КИБЕРПРОТЕКТ

КИБЕР Бэкап

Версия 18.6

Руководство пользователя

Редакция: 01.07.2026

Авторское право

© 2026 ООО «Киберпротект».

ООО «Киберпротект» является правообладателем данного документа.

Все права защищены.

Распространение измененных версий данного руководства, а также переработанных материалов, входящих в данное руководство, запрещено без явного разрешения владельца авторских прав.

ДОКУМЕНТ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ДОКУМЕНТ НЕ ПРЕДПОЛАГАЕТ ОБЯЗАТЕЛЬСТВ И/ИЛИ ГАРАНТИЙ ПРАВООБЛАДАТЕЛЯ ОТНОСИТЕЛЬНО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, НАСКОЛЬКО ТАКОЕ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ДОПУСКАЕТСЯ ЗАКОНОМ, ВКЛЮЧАЯ, СРЕДИ ПРОЧЕГО, ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ, УДОВЛЕТВОРИТЕЛЬНОГО КАЧЕСТВА, ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ.

Содержание

1 Издания и лицензии Кибер Бэкап ... 16
1.1 Пробная версия ... 17
2 Установка ... 18
2.1 Компоненты ... 18
2.1.1 Сервер управления ... 18
2.1.2 Агенты ... 18
2.1.3 Узел хранения ... 21
2.1.4 Другие компоненты ... 21
2.2 Требования к программному обеспечению ... 22
2.2.1 Поддерживаемые веб-браузеры ... 23
2.2.2 Поддерживаемые операционные системы и среды ... 23
2.2.3 Поддерживаемые платформы виртуализации ... 29
2.2.4 Поддерживаемые почтовые сервисы ... 35
2.2.5 Поддерживаемые СУБД ... 35
2.2.6 Поддерживаемые версии приложений Microsoft ... 36
2.2.7 Необходимые пакеты для ОС Linux ... 36
2.2.8 Совместимость с ОС Astra Linux SE ... 42
2.2.9 Совместимость с программами шифрования ... 44
2.2.10 Поддерживаемые интеграции со службами каталогов ... 45
2.3 Системные требования ... 46
2.3.1 Рекомендуемые конфигурации оборудования для сервера управления ... 48
2.4 Поддержка файловых систем ... 57
2.5 Настройки прокси-сервера ... 60
2.5.1 В Windows ... 60
2.5.2 В ОС Linux ... 61
2.6 Развертывание Кибер Бэкап ... 62
2.6.1 Установка сервера управления ... 63
2.6.2 Настройка отказоустойчивого кластера ... 72
2.6.3 Добавление машин через веб-интерфейс ... 86
2.6.4 Установка агентов ... 95
2.6.5 Автоматическая установка или автоматическое удаление ... 167
2.6.6 Регистрация агента вручную ... 181
2.6.7 Установка и настройка узла хранения ... 183
2.6.8 Проверка наличия обновлений программного обеспечения ... 192
2.6.9 Управление лицензиями ... 192

© ООО Киберпротект, 2026

2.7 Автоматическое обнаружение машин ... 193
2.7.1 Принципы работы ... 194
2.7.2 Предварительные требования ... 195
2.7.3 Процесс обнаружения машины ... 195
2.7.4 Автоматическое и ручное обнаружение ... 196
2.7.5 Управление обнаруженными машинами ... 200
2.7.6 Устранение неисправностей при автоматическом обнаружении ... 201
2.8 Обновление виртуальных устройств ... 202
2.8.1 Порядок обновления виртуального устройства ... 202
2.9 Обновление агентов ... 203
2.9.1 Порядок обновления агентов локально через установочный файл ... 203
2.9.2 Порядок обновления агентов из веб-консоли Кибер Бэкап ... 204
2.10 Обновление Кибер Бэкап ... 205
2.11 Удаление продукта ... 208
2.11.1 В Windows ... 208
2.11.2 В ОС Linux ... 208
2.11.3 Удаление агента для VMware (виртуальное устройство) ... 209
2.11.4 Удаление машин из веб-консоли Кибер Бэкап ... 209
3 Веб-консоль Кибер Бэкап ... 210
3.1 В Windows ... 210
3.2 В ОС Linux ... 211
3.3 Смена языка ... 211
3.4 Настройка веб-браузера для выполнения встроенной проверки подлинности Windows ... 211
3.4.1 Настройка Microsoft Edge, Opera и Google Chrome ... 211
3.4.2 Настройка Mozilla Firefox ... 212
3.4.3 Добавление консоли к списку веб-узлов локальной интрасети ... 212
3.4.4 Добавление консоли к списку доверенных веб-узлов ... 214
3.5 Настройки сертификата SSL ... 217
3.5.1 Использование самозаверяющих сертификатов ... 217
3.5.2 Использование сертификата, выданного доверенным центром сертификации ... 218
3.6 Режимы отображения списка устройств ... 220
3.6.1 Простой режим ... 220
3.6.2 Табличный режим ... 220
4 План защиты и модули ... 224
4.1 Создание плана защиты ... 224
4.1.1 Порядок создания плана защиты ... 224
4.2 Разрешение конфликтов плана ... 225

© ООО Киберпротект, 2026

4.2.1 Применение нескольких планов к устройству ... 225
4.2.2 Разрешение конфликтов плана ... 225
4.3 Операции с планами защиты ... 227
4.3.1 Доступные действия с планами защиты ... 227
4.3.2 Создание плана ... 228
4.3.3 Импорт плана ... 229
4.3.4 Просмотр сведений о плане ... 229
4.3.5 Запуск резервного копирования по требованию ... 229
4.3.6 Остановка выполнения плана ... 230
4.3.7 Изменение плана ... 231
4.3.8 Применение плана к устройству или группе устройств ... 233
4.3.9 Отзыв плана с устройства ... 234
4.3.10 Просмотр журнала действий с планом ... 235
4.3.11 Оповещения ... 237
4.3.12 Клонирование плана ... 237
4.3.13 Экспорт плана ... 237
4.3.14 Включение / отключение плана ... 238
4.3.15 Удаление плана ... 238
4.3.16 Групповые действия с планами ... 239
4.4 Активная защита (Active Protection) ... 240
4.4.1 Технические требования и ограничения службы Active Protection ... 241
4.4.2 Active Protection для Windows ... 241
4.4.3 Active Protection для Linux ... 245
5 Группы устройств ... 248
5.1 Встроенные группы ... 248
5.2 Пользовательские группы ... 248
5.3 Операции со статическими группами ... 249
5.3.1 Создание статических групп ... 249
5.3.2 Добавление устройств в статические группы ... 250
5.3.3 Удаление устройств из статических групп ... 252
5.4 Операции с динамическими группами ... 253
5.4.1 Создание динамических групп ... 253
5.4.2 Условия поиска ... 254
5.4.3 Операторы ... 261
5.5 Применение плана защиты к группе ... 262
5.6 Переименование группы ... 262
5.7 Удаление группы ... 263

© ООО Киберпротект, 2026

6 Резервное копирование **264**
6.1 Агент 266
6.2 Типы резервных копий 266
6.3 Модуль резервного копирования: памятка 267
6.3.1 Ограничения 271
6.4 Выбор данных для резервного копирования 272
6.4.1 Выбор всей машины 272
6.4.2 Выбор файлов и папок 273
6.4.3 Выбор дисков и томов 275
6.4.4 Выбор конфигурации ESXi 277
6.5 Выбор места сохранения 278
6.5.1 Поддерживаемые расположения 278
6.5.2 О разделе Зона безопасности 283
6.5.3 О продуктах Кибер Инфраструктура и Кибер Хранилище 286
6.6 Расписание 287
6.6.1 Схема резервного копирования 288
6.6.2 Дополнительные параметры расписания 289
6.6.3 Планирование по событиям 290
6.6.4 Условия запуска 293
6.7 Правила хранения 299
6.7.1 Что ещё нужно знать 300
6.8 Защита паролем 301
6.8.1 Настройка защиты паролем в планах защиты 301
6.8.2 Особенности защиты паролем 301
6.9 Преобразование в виртуальную машину 302
6.9.1 Методы преобразования 302
6.9.2 Важная информация о преобразовании 302
6.9.3 Преобразование в виртуальную машину в плане защиты 304
6.9.4 Как работает обычное преобразование в виртуальную машину 305
6.10 Репликация 306
6.10.1 Примеры использования 306
6.10.2 Поддерживаемые расположения 306
6.10.3 Включение репликации резервных копий 308
6.10.4 Замечания по использованию узла хранения 309
6.11 Запуск резервного копирования вручную 309
6.12 Одновременное резервное копирование 312
6.12.1 Зачем выполнять одновременное резервное копирование 312

© ООО Киберпротект, 2026

6.12.2 Что нужно для выполнения одновременного резервного копирования ... 313
6.12.3 Включение одновременного резервного копирования ... 314
6.12.4 Запуск одновременного резервного копирования ... 315
6.12.5 Ограничение общего количества планов для файлового и дискового резервного копирования ... 315
6.12.6 Ограничение общего количества виртуальных машин ... 315
6.12.7 Ограничение общего количества планов для почтовых ящиков и баз данных PostgreSQL ... 317
6.13 Резервное копирование виртуальных машин без использования локальной сети (LAN-free backup) ... 318
6.13.1 Резервное копирование без использования локальной сети (LAN-free backup) для oVirt ... 318
6.13.2 Резервное копирование без использования локальной сети (LAN-free backup) для VMware ... 324
6.14 Параметры резервного копирования ... 335
6.14.1 Доступность параметров резервного копирования ... 335
6.14.2 Оповещения ... 341
6.14.3 Консолидация резервных копий ... 342
6.14.4 Имя файла резервной копии ... 343
6.14.5 Формат резервной копии ... 347
6.14.6 Проверка резервных копий ... 348
6.14.7 Функция Changed Block Tracking (CBT) ... 349
6.14.8 Способ резервного копирования кластера ... 350
6.14.9 Уровень сжатия ... 352
6.14.10 Многопоточность ... 352
6.14.11 Уведомления по электронной почте ... 353
6.14.12 Обработка ошибок ... 354
6.14.13 Быстрое инкрементное/дифференциальное резервное копирование ... 355
6.14.14 Фильтры файлов ... 356
6.14.15 Моментальные снимки резервных копий на уровне файлов ... 358
6.14.16 Сокращение журнала Microsoft SQL Server ... 358
6.14.17 Создание моментальных снимков LVM ... 359
6.14.18 Точки подключения ... 359
6.14.19 Многотомные моментальные снимки ... 360
6.14.20 Производительность и окно резервного копирования ... 361
6.14.21 Команды до и после процедуры ... 365
6.14.22 Команды до и после захвата данных ... 367

© ООО Киберпротект, 2026

6.14.23 Моментальные снимки оборудования SAN ... 370
6.14.24 Планирование ... 370
6.14.25 Посекторное резервное копирование ... 371
6.14.26 Деление ... 371
6.14.27 Управление лентами ... 372
6.14.28 Действие при сбое плана ... 378
6.14.29 Условия запуска задания ... 378
6.14.30 Служба теневого копирования томов (VSS) ... 379
6.14.31 Служба теневого копирования томов (VSS) для виртуальных машин ... 380
6.14.32 Еженедельное резервное копирование ... 381
6.14.33 Журнал событий Windows ... 381
7 Восстановление ... 382
7.1 Восстановление: памятка ... 382
7.2 Создание загрузочных носителей ... 383
7.3 Восстановление машины ... 384
7.3.1 Физическая машина ... 384
7.3.2 Восстановление физической машины в виртуальную ... 386
7.3.3 Виртуальная машина ... 388
7.3.4 Восстановление дисков с помощью загрузочного носителя ... 390
7.3.5 Использование компонента Универсальное восстановление (Universal Restore) ... 391
7.4 Восстановление файлов ... 394
7.4.1 Восстановление файлов с помощью веб-интерфейса ... 394
7.4.2 Восстановление файлов с помощью загрузочного носителя ... 396
7.4.3 Извлечение файлов из локальных резервных копий ... 397
7.5 Восстановление конфигурации ESXi ... 398
7.6 Параметры восстановления ... 399
7.6.1 Доступность параметров восстановления ... 399
7.6.2 Проверка резервных копий ... 401
7.6.3 Режим загрузки ... 401
7.6.4 Дата и время для файлов ... 402
7.6.5 Обработка ошибок ... 402
7.6.6 Исключения файлов ... 403
7.6.7 Безопасность на уровне файлов ... 404
7.6.8 Flashback ... 404
7.6.9 Восстановление полного пути ... 404
7.6.10 Точки подключения ... 404
7.6.11 Производительность ... 405

© ООО Киберпротект, 2026

7.6.12 Команды до и после процедуры ... 405
7.6.13 Управление лентами ... 407
7.6.14 Изменение идентификатора безопасности ... 407
7.6.15 Управление питанием ВМ ... 408
7.6.16 Журнал событий Windows ... 408
7.6.17 Включить после восстановления ... 408
8 Операции с резервными копиями ... 410
8.1 Подключение томов из резервной копии ... 410
8.1.1 Требования ... 410
8.1.2 Сценарии использования ... 410
8.2 Экспорт резервных копий ... 411
8.3 Удаление резервных копий ... 413
8.4 Обработка данных вне хоста (off-host) ... 413
8.4.1 Репликация резервных копий ... 414
8.4.2 Проверка резервных копий ... 416
8.4.3 Очистка от устаревших резервных копий ... 420
8.4.4 Преобразование резервных копий в виртуальные машины ... 421
9 Вкладка «Планы» ... 423
10 Вкладка «Хранилища резервных копий» ... 425
11 Загрузочный носитель ... 427
11.1 Загрузочный носитель ... 427
11.2 Создавать ли загрузочный носитель или скачать готовый? ... 427
11.3 Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE? ... 428
11.3.1 На основе Linux ... 428
11.3.2 На основе WinPE ... 428
11.4 Мастер создания загрузочных носителей ... 429
11.4.1 Цели использования мастера создания носителей ... 429
11.4.2 Загрузочные носители на основе Linux ... 429
11.4.3 Загрузочный носитель на основе WinPE ... 446
11.5 Подключение к машине, загружаемой с носителя ... 450
11.5.1 Настройка сети ... 450
11.5.2 Локальное подключение ... 451
11.5.3 Удаленное подключение ... 451
11.6 Регистрация носителя на сервере управления ... 451
11.6.1 Регистрация носителя в пользовательском интерфейсе носителя ... 451
11.7 Операции с загрузочным носителем ... 453
11.7.1 Настройка режима отображения ... 454

© ООО Киберпротект, 2026

11.7.2 Резервное копирование ... 454
11.7.3 Восстановление ... 455
11.7.4 Управление дисками ... 456
11.8 Настройка устройств iSCSI ... 469
11.9 Диспетчер восстановления при загрузке (Startup Recovery Manager) ... 470
11.9.1 Активация Диспетчера восстановления при загрузке ... 470
11.9.2 Что происходит при активации Диспетчера восстановления при загрузке ... 471
11.9.3 Деактивация Диспетчера восстановления при загрузке ... 472
11.10 PXE-сервер Киберпротект ... 472
11.10.1 Установка PXE-сервера ... 472
11.10.2 Настройка машины на загрузку с PXE ... 473
11.10.3 Работа в подсетях ... 474
12 Защита приложений, сервисов, баз данных ... 475
12.1 Защита приложений Microsoft ... 475
12.1.1 Защита Microsoft SQL Server и Microsoft Exchange Server ... 475
12.1.2 Защита Microsoft SharePoint ... 475
12.1.3 Защита контроллера домена ... 476
12.1.4 Восстановление приложений ... 476
12.1.5 Предварительные требования ... 477
12.1.6 Резервное копирование баз данных Microsoft SQL Server и Microsoft Exchange Server ... 479
12.1.7 Резервное копирование с поддержкой приложений ... 485
12.1.8 Резервная копия почтового ящика ... 487
12.1.9 Восстановление баз данных Microsoft SQL Server ... 488
12.1.10 Восстановление баз данных Microsoft Exchange Server ... 492
12.1.11 Восстановление почтовых ящиков Exchange и элементов почтового ящика ... 495
12.1.12 Изменение учетных данных для доступа к Microsoft SQL Server или Microsoft Exchange Server ... 501
12.2 Защита CommuniGate Pro ... 502
12.2.1 Зачем создавать резервную копию CommuniGate Pro ... 502
12.2.2 Что необходимо для резервного копирования CommuniGate Pro? ... 502
12.2.3 Возможности ... 503
12.2.4 Известные проблемы и ограничения ... 503
12.2.5 Предварительные требования для защиты CommuniGate Pro ... 503
12.2.6 Установка CommuniGate Pro ... 508
12.2.7 Резервное копирование CommuniGate Pro ... 512
12.2.8 Восстановление CommuniGate Pro ... 527
12.2.9 Удаление CommuniGate Pro ... 531

© ООО Киберпротект, 2026

12.3 Защита VK WorkMail и VK WorkDisk ... 532
12.3.1 Зачем обеспечивать защиту VK WorkMail и VK WorkDisk ... 532
12.3.2 Что необходимо для резервного копирования ... 532
12.3.3 Возможности ... 533
12.3.4 Установка VK WorkMail ... 534
12.3.5 Резервное копирование VK WorkMail и VK WorkDisk ... 540
12.3.6 Восстановление VK WorkMail и VK WorkDisk ... 551
12.3.7 Обновление токена VK WorkMail ... 557
12.4 Защита Mailion ... 558
12.4.1 Возможности ... 559
12.4.2 Известные проблемы и ограничения ... 559
12.4.3 Установка Mailion ... 559
12.4.4 Резервное копирование данных Mailion ... 563
12.4.5 Восстановление данных Mailion ... 566
12.5 Защита Oracle Database ... 569
12.5.1 Защита Oracle Database предыдущих версий ... 570
12.6 Защита баз данных PostgreSQL ... 584
12.6.1 Что необходимо для резервного копирования ... 585
12.6.2 Возможности ... 585
12.6.3 Предварительная настройка PostgreSQL ... 586
12.6.4 Установка и настройка ... 589
12.6.5 Резервное копирование PostgreSQL ... 591
12.6.6 Восстановление баз данных PostgreSQL ... 594
12.6.7 Ограничения ... 599
12.6.8 Известные проблемы и их решения ... 600
12.7 Защита данных MySQL и MariaDB ... 601
12.7.1 Настройка резервного копирования с поддержкой приложений ... 602
12.7.2 Восстановление данных из резервной копии с поддержкой приложений ... 603
12.8 Защита баз данных Ред База Данных ... 607
12.8.1 Предварительная настройка базы данных ... 608
12.8.2 Создание плана резервного копирования ... 608
12.8.3 Разблокировка базы данных ... 610
12.9 Защита баз данных MongoDB ... 610
12.9.1 Настройка резервного копирования баз данных MongoDB ... 611
12.9.2 Восстановление данных из резервной копии ... 616
12.10 Защита Kubernetes ... 616
12.10.1 Зачем защищать Kubernetes ... 616

© ООО Киберпротект, 2026

12.10.2 Что необходимо для резервного копирования Kubernetes? 616
12.10.3 Возможности 617
12.10.4 Установка агента для Kubernetes 617
12.10.5 Подготовка кластера Kubernetes 619
12.10.6 Создание служебной учетной записи для агента Kubernetes 620
12.10.7 Подготовка файла kubeconfig 625
12.10.8 Добавление кластера Kubernetes 626
12.10.9 Резервное копирование Kubernetes 628
12.10.10 Восстановление Kubernetes 635
12.10.11 Резервное копирование постоянных томов в хранилище Кибер Бэкап 641
12.11 Защита SAP HANA 645
12.11.1 Поддерживаемые версии SAP HANA 645
12.11.2 Резервное копирование физических серверов 645
12.11.3 Резервное копирование виртуальных серверов 649
12.11.4 Восстановление всего сервера 649
12.11.5 Восстановление базы данных с помощью SAP HANA Studio 650
13 Специальные операции с виртуальными машинами 659
13.1 Запуск виртуальной машины из резервной копии (мгновенное восстановление) 659
13.1.1 Примеры использования 659
13.1.2 Предварительные требования 659
13.1.3 Запуск машины 660
13.1.4 Удаление машины 661
13.1.5 Финализация машины 661
13.2 Работа в VMware vSphere 662
13.2.1 Репликация виртуальных машин 662
13.2.2 Использование локально присоединенного хранилища 669
13.2.3 Привязка виртуальной машины 670
13.2.4 Поддержка миграции VM 672
13.2.5 Управление средами виртуализации 673
13.2.6 Просмотр статуса резервного копирования в клиенте vSphere 674
13.2.7 Агент для VMware: необходимые привилегии 675
13.2.8 Предельное количество виртуальных машин для резервного копирования 690
13.2.9 Одновременное восстановление 691
13.3 Использование моментальных снимков оборудования SAN 691
13.3.1 Смысл использования моментальных снимков оборудования SAN 692
13.3.2 Что необходимо для использования моментальных снимков оборудования SAN? 692
13.3.3 Настройка хранилища данных YADRO TATLIN.UNIFIED 693

© ООО Киберпротект, 2026

13.3.4 Требования для хранилища данных NetApp SAN ... 699
13.3.5 Настройка Huawei OceanStor (Dorado) ... 701
13.3.6 Настройка машины с агентом для VMware (Windows) ... 707
13.3.7 Регистрация хранилища данных SAN на сервере управления ... 712
13.3.8 Настройка машины с агентом для oVirt ... 714
13.4 Резервное копирование кластеризованных машин Hyper-V ... 717
13.4.1 Высокая доступность восстановленной машины ... 717
13.5 Миграция машины ... 717
13.5.1 Миграция Linux-машины с логическими томами (LVM) ... 720
13.6 Увеличение объёма ОЗУ виртуального устройства ... 721
13.7 Резервное копирование облачных виртуальных машин без доступа к гипервизору ... 721
13.7.1 Требования к сети ... 722
14 Мониторинг, отчёты и аудит ... 723
14.1 Панель мониторинга "Обзор" ... 723
14.1.1 Виджет "Резервные копии" ... 724
14.1.2 Виджет "Статус защиты" ... 724
14.1.3 Виджет "Нет последних резервных копий" ... 725
14.2 Панель мониторинга "Оповещения" ... 726
14.2.1 Файл настройки оповещений ... 727
14.2.2 Изменение степени серьёзности оповещения, отключение оповещения ... 727
14.2.3 Перезапуск службы сервера управления в ОС Windows ... 727
14.2.4 Перезапуск службы сервера управления в ОС Linux ... 728
14.3 Панель мониторинга "Действия" ... 728
14.3.1 Порядок изменения периода хранения сведений о действиях ... 729
14.4 Отчёты ... 729
14.4.1 Обзор вкладки "Отчёты" ... 730
14.4.2 Варианты отчётов ... 730
14.4.3 Основные операции с отчётами ... 731
14.5 Журнал аудита ... 739
14.5.1 Основной поиск событий ... 740
14.5.2 Расширенный поиск событий ... 740
14.5.3 Использование сохранённых поисковых запросов ... 742
14.5.4 Регистрируемые события ... 743
14.6 Настройка внешнего мониторинга ... 751
14.6.1 Настройка OpenTelemetry Collector ... 751
14.6.2 Настройка Prometheus в качестве источника данных ... 753
14.6.3 Настройка Grafana Loki в качестве источника данных ... 757

© ООО Киберпротект, 2026

14.6.4 Настройка системы мониторинга Grafana ... 761
15 Ленточные устройства ... 766
15.1 Типы и свойства лент ... 766
15.1.1 Перезаписываемые ленты ... 766
15.1.2 Ленты типа WORM ... 767
15.1.3 Аппаратная защита от записи ... 767
15.1.4 Чистящие ленты ... 768
15.1.5 Ленты неизвестного типа ... 768
15.2 Поддержка резервного копирования на ленту ... 768
15.2.1 Совместимость с RSM и программным обеспечением других поставщиков ... 769
15.2.2 Поддерживаемое оборудование ... 769
15.2.3 База данных управления лентами ... 769
15.2.4 Параметры записи на ленты ... 770
15.2.5 Связанные с лентой параметры резервного копирования ... 772
15.2.6 Параллельные операции ... 772
15.2.7 Ограничения ... 773
15.3 Начало работы с ленточным устройством ... 774
15.3.1 Резервное копирование машины на локально подключенное ленточное устройство ... 774
15.3.2 Резервное копирование на ленточное устройство, подключенное к узлу хранения ... 775
15.3.3 Восстановление с ленточного устройства из операционной системы ... 777
15.3.4 Восстановление с загрузочного носителя из локально прикрепленного ленточного устройства ... 778
15.3.5 Восстановление с помощью загрузочного носителя с ленточного устройства, прикрепленного к узлу хранения ... 779
15.4 Управление лентами ... 780
15.4.1 Обнаружение ленточных устройств ... 780
15.4.2 Пулы лент ... 780
15.4.3 Операции с пулами ... 782
15.4.4 Операции с лентами ... 783
15.4.5 Ограничения ... 787
15.4.6 Ограничения ... 787
15.4.7 Перемещение ... 788
15.4.8 Ограничения ... 788
15.4.9 Утилита для работы с лентами ... 789
15.4.10 Перемещение ... 790
15.4.11 Ручная очистка ленточных приводов ... 799
16 Настройки системы ... 800

© ООО Киберпротект, 2026

16.1 Уведомления по электронной почте ... 800
16.2 Почтовый сервер ... 801
16.3 Безопасность ... 802
16.3.1 Завершить сеансы работы неактивных пользователей через ... 802
16.3.2 Показать уведомление о последнем входе текущего пользователя ... 802
16.3.3 Предупреждать об истечении срока действия локального пароля или пароля домена 802
16.4 Обновления ... 802
16.5 Параметры резервного копирования по умолчанию ... 803
16.6 Настройка PAM-модуля ... 803
16.6.1 Установленные библиотеки ... 803
16.6.2 Используемая конфигурация ... 803
16.6.3 Предупреждение о редактировании конфигурационного файла ... 803
16.7 Управление журналом аудита ... 804
16.7.1 Очистка журнала аудита ... 804
16.8 Отправка записей журнала аудита на Syslog-сервер ... 804
16.8.1 Предварительные требования для протокола TLS ... 804
16.8.2 Настройка отправки записей на Syslog-сервер ... 805
17 Управление учетными записями пользователей и отделами организации ... 806
17.1 Отделы и административные учетные записи ... 806
17.1.1 Отделы ... 806
17.1.2 Административные учетные записи ... 806
17.1.3 Какие учетные записи могут быть административными? ... 806
17.1.4 Роли административной учетной записи ... 807
17.1.5 Наследование ролей ... 807
17.1.6 Администраторы по умолчанию ... 808
17.1.7 Административная учетная запись в нескольких отделах ... 809
17.1.8 Добавление машин в отделы ... 809
17.2 Добавление административных учетных записей ... 809
17.3 Создание отделов ... 814
18 Диагностика неполадок ... 815
Глоссарий ... 816
Указатель ... 818

© ООО Киберпротект, 2026

1 Издания и лицензии Кибер Бэкап

Для Кибер Бэкап 18 доступны следующие типы лицензий:

- **Кибер Бэкап 18 для рабочей станции**,
- **Кибер Бэкап 18 для физического сервера**,
- **Кибер Бэкап 18 для платформы виртуализации**,
- **Кибер Бэкап 18 для почтового ящика**,
- **Кибер Бэкап 18 для СУБД PostgreSQL**,
- **Кибер Бэкап 18 универсальная лицензия**.

Кроме того, доступны следующие редакции:

- **Стандартная** редакция подходит для резервного копирования данных в ИТ-инфраструктурах небольшого размера, в которых резервные копии отправляются в целевые хранилища напрямую без использования узла хранения, не требуется глобальная дедупликация, не требуется дифференциация ролей администратора, не используются ленточные носители.
- **Расширенная** редакция предназначена для крупных ИТ-инфраструктур, где требуется защита физических серверов, рабочих станций, виртуальных машин и приложений. Включает централизованное управление, глобальную дедупликацию данных, поддержку ленточных носителей, позволяет создавать организационные единицы и добавлять администраторов для них, а также содержит другие расширенные функции.

Лицензии на рабочие станции, физические серверы и платформы виртуализации доступны в двух редакциях: **Стандартная** и **Расширенная**.

Лицензии на почтовые ящики, СУБД PostgreSQL и универсальная лицензия доступны только в одной редакции: **Расширенная**.

Для использования Кибер Бэкап в кластере хостов виртуализации VMware ESXi или MS Hyper-V необходимо для каждого хоста в кластере иметь лицензии одного типа (**Для платформы виртуализации** или **Универсальная лицензия**) и одной редакции (**Стандартная** или **Расширенная**). Смешивание лицензий разных типов или редакций не допускается. Подробнее см. в статье базы знаний Особенности лицензирования резервного копирования виртуальных машин.

Все лицензии являются бессрочными. Приобретаемые лицензии распространяются на основную версию продукта, а также на все прошлые и будущие минорные обновления основной версии. Более подробную информацию о лицензиях см. в статье Лицензирование.

Чтобы управлять лицензиями в своей среде, в веб-консоли Кибер Бэкап последовательно выберите пункты **Настройки** > **Лицензии**.

Кроме того, можно управлять лицензиями для каждой отдельной машины. Для этого в веб-консоли Кибер Бэкап выберите нужную машину и последовательно выберите пункты **Устройство** > **Сведения** > **Лицензия**.

© ООО Киберпротект, 2026

1.1 Пробная версия

Перед покупкой лицензии можно воспользоваться пробной версией Кибер Бэкап. Она позволит оценить все возможности продукта без ограничений в течение 30 дней.

© ООО Киберпротект, 2026

2 Установка

2.1 Компоненты

Кибер Бэкап состоит из сервера управления, агентов, а также различных вспомогательных компонентов. Все компоненты должны быть установлены в одной сети.

2.1.1 Сервер управления

Сервер управления является центральным компонентом. Он отвечает за обмен данными с агентами Кибер Бэкап, управляет планами защиты и предоставляет пользователям веб-интерфейс.

Сервер управления можно установить на машине с ОС Windows или Linux. Установка сервера управления на машине с ОС Windows позволяет удаленно развертывать агенты на других компьютерах.

2.1.2 Агенты

Агенты – это приложения, которые устанавливаются на рабочие нагрузки и выполняют резервное копирование данных, их восстановление и другие операции.

Перед выполнением любой операции защиты агенты обращаются к серверу управления для проверки предварительных требований. Подключение к серверу управления необходимо для развертывания новых планов защиты. Если план защиты уже развернут, агент продолжает выполнять операции защиты на протяжении 30 дней после утраты связи с сервером управления.

Выберите агент в зависимости от того, для какого именно объекта нужно создать резервную копию. В таблице ниже приведены основные сведения, которые помогут вам принять решение.

Обратите внимание: агент для Windows устанавливается вместе с агентом для Exchange, агентом для SQL, агентом для Active Directory и агентом для Oracle. Например, установив агент для SQL, вы также сможете создавать резервные копии всей машины.

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?
Физические машины		
Диски, тома и файлы на физических машинах под управлением Windows	Агент для Windows	На машину, резервная копия которой будет создана.
Диски, тома и файлы на физических машинах под управлением Linux	Агент для Linux	

© ООО Киберпротект, 2026

Приложения		
Базы данных PostgreSQL, Postgres Pro, Patroni, Platform V Pangolin, Proxima DB, Jatoba, Tantor	Агент для PostgreSQL	На машину с сервером PostgreSQL или на другую машину, у которой есть сетевой доступ к PostgreSQL.
Ред База Данных	Агент для Windows или агент для Linux	На машину с СУБД Ред База Данных.
Базы данных MySQL/MariaDB	Агент для MySQL/MariaDB	На машину с сервером MySQL/MariaDB.
Базы данных MongoDB	Агент для Windows или агент для Linux	На машину с сервером MongoDB или на другую машину, у которой есть сетевой доступ к MongoDB.
Базы данных SQL Server	Агент для SQL	На машину с Microsoft SQL Server.
Машины под управлением Oracle Database	Агент для Oracle	На машину с запущенной Oracle Database.
Базы данных SAP HANA*	Агент для Linux	На машину с SAP HANA.
Пространства имен и постоянные тома Kubernetes	Агент для Kubernetes	На машину с ОС Linux, у которой есть сетевой доступ к кластеру Kubernetes.
Данные CommuniGate Pro	Агент для CommuniGate Pro	На машину с CommuniGate Pro или на другую машину, у которой есть сетевой доступ к CommuniGate Pro.
Данные VK WorkMail и VK WorkDisk	Агент для VK WorkMail	На машину, у которой есть сетевой доступ к VK WorkMail.
Базы данных и почтовые ящики Exchange	Агент для Exchange	На машину с ролью почтового ящика Microsoft Exchange Server.** Если требуется резервное копирование только почтового ящика, агент может быть установлен на любой машине с ОС Windows, которая имеет сетевой доступ к машине, на которой включена роль клиентского доступа Microsoft Exchange Server.
Машины с Microsoft SharePoint	Агент для SQL и агент для Windows	На серверы баз данных, серверы веб-интерфейса и серверы приложений.
Машины с доменными	Агент для Active	На контроллер домена.

© ООО Киберпротект, 2026

службами Active Directory	Directory	
Виртуальные машины		
Виртуальные машины VMware ESXi	Агент для VMware (Windows)	На машину Windows с сетевым доступом к vCenter Server и хранилищу виртуальных машин.***
	Агент для VMware (виртуальное устройство)	В среду виртуализации в виде виртуального устройства.
Виртуальные машины oVirt, ROSA Virtualization, zVirt, Red Hat Virtualization, РЕД Виртуализация, HOSTVM	Агент для oVirt	
Виртуальные машины SpaceVM	Агент для SpaceVM	
Виртуальные машины ECP VeiL	Агент для ECP VeiL	
Виртуальные машины Кибер Инфраструктуры	Агент для Кибер Инфраструктуры	
Виртуальные машины OpenStack, РУСТЭК, VK Cloud	Агент для OpenStack	
Виртуальные машины Basis DynamiX Enterprise	Агент для Basis DynamiX Enterprise	
Виртуальные машины OpenNebula, ПК СВ "Брест", ПО "Альт Виртуализация", Система группового управления "Горизонт-ВС"	Агент для OpenNebula	
Виртуальные машины Hyper-V	Агент для Hyper-V	На хост Hyper-V.
Виртуальные машины в среде Windows Azure	Агент для Windows или агент для Linux****	На машину, резервная копия которой будет создана.
Виртуальные машины, размещенные в Amazon EC2		
Виртуальные машины на хосте Citrix XenServer		На машину, резервная копия которой будет создана.*****
Виртуальные машины Red Hat Virtualization (RHV/RHEV)		

© ООО Киберпротект, 2026

Виртуальные машины на основе ядра (KVM)		
Виртуальные машины Oracle		
Виртуальные машины Nutanix AHV		

* Также поддерживается защита СУБД SAP HANA, которая установлена в виртуальную машину VMware ESXi. Подробные сведения см. в разделе "Резервное копирование виртуальных серверов" (стр. 649).

** В ходе установки агент для Exchange проверяет достаточность свободного пространства на машине, где он запущен. При выполнении фрагментарного восстановления временно необходимо свободное пространство в объеме, равном 15 процентам от объема самой большой базы данных Exchange.

*** Если ваш ESXi использует SAN-хранилище, установите агент на машине, подключенной к тому же SAN-хранилищу. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Подробные инструкции см. в разделе "Резервное копирование без использования локальной сети посредством Windows-агента для VMware" (стр. 332).

**** Для выполнения операций защиты установите агент для операционной системы, которая используется в гостевой системе (агент Windows или агент Linux).

***** Лицензия **Кибер Бэкап 18 Стандартная для платформы виртуализации** не подходит для лицензирования данных ВМ. Необходимо использовать либо лицензию **Кибер Бэкап 18 Расширенная для платформы виртуализации** для лицензирования хоста виртуализации, либо лицензии **Кибер Бэкап 18 для рабочей станции или физического сервера** для лицензирования каждой ВМ как физической машины.

2.1.3 Узел хранения

Узел хранения – это сервер, предназначенный для оптимизации использования различных ресурсов, требуемых для защиты корпоративных данных. Это достигается путем организации и управления хранилищами, выделенными для корпоративных резервных копий.

Узел хранения можно установить на машине с ОС Windows или Linux.

2.1.4 Другие компоненты

Компонент	Функция	Куда его следует установить?
Компоненты для удаленной установки	Сохраняет пакеты установки агента в локальную папку.	На машине Windows с сервером управления.

© ООО Киберпротект, 2026

Мастер создания загрузочных носителей	Создает загрузочный носитель.	На машине с ОС Windows или Linux.
Программа командной строки	Предоставляет интерфейс командной строки.	На машине с ОС Windows или Linux.
Мониторинг Защиты Данных	Позволяет пользователям отслеживать выполнение запущенных задач в области уведомлений ОС Windows.	На машине с ОС Windows.
PXE-сервер	Активирует загрузку машин на загрузочный носитель по сети.	На машине под управлением ОС Windows.

2.2 Требования к программному обеспечению

В этом разделе приведены требования к программному обеспечению, необходимому для установки и работы Кибер Бэкап и его компонентов:

- к операционным системам и средам (см. раздел "Поддерживаемые операционные системы и среды" (стр. 23)), в том числе:
  - к наличию дополнительных пакетов для работы в среде ОС Linux (см. раздел "Необходимые пакеты для ОС Linux" (стр. 36));
  - к настройкам для поддержки ОС Astra Linux SE (см. раздел "Совместимость с ОС Astra Linux SE" (стр. 42));
- к веб-браузерам для работы с интерфейсом пользователя (см. раздел "Поддерживаемые веб-браузеры" (стр. 23)).

Также в разделе приведены сведения о программном обеспечении, которое поддерживается в качестве защищаемых рабочих нагрузок:

- об операционных системах (см. раздел "Агенты" (стр. 23));
- о платформах виртуализации (см. раздел "Поддерживаемые платформы виртуализации" (стр. 29));
- о почтовых сервисах (см. раздел "Поддерживаемые почтовые сервисы" (стр. 35));
- о СУБД (см. раздел "Поддерживаемые СУБД" (стр. 35));
- о приложениях Microsoft (см. раздел "Поддерживаемые версии приложений Microsoft" (стр. 36)).

Кроме этого, в разделе указаны требования к поддерживаемым программам шифрования (см. раздел "Совместимость с программами шифрования" (стр. 44)) и службам каталогов (см. раздел "Поддерживаемые интеграции со службами каталогов" (стр. 45)).

© ООО Киберпротект, 2026

2.2.1 Поддерживаемые веб-браузеры

Веб-интерфейс сервиса резервного копирования поддерживает перечисленные ниже браузеры:

- Яндекс Браузер 25.2 или более поздней версии
- Google Chrome 134 или более поздней версии
- Opera 118 или более поздней версии
- Mozilla Firefox 136 или более поздней версии
- Microsoft Edge 133 или более поздней версии

В других веб-браузерах интерфейс пользователя может отображаться неправильно или могут быть недоступны некоторые функции.

2.2.2 Поддерживаемые операционные системы и среды

2.2.2.1 Агенты

В разделе указаны поддерживаемые операционные системы для машин, на которые устанавливаются агенты защиты (подробнее в разделе "Компоненты" (стр. 18)). Часть агентов предоставляется в виде виртуального устройства, и для их развертывания требуется лишь среда виртуализации.

Агент для Windows

Агент устанавливается непосредственно на защищаемое устройство.

- Windows Server 2012 R2 (64-разрядные версии) – все выпуски, включая Storage Server;
- Windows Server 2016–2022 (64-разрядные версии) – все выпуски, кроме Nano Server;
- Windows 10/11 (64-разрядные версии) – все выпуски.

Агент для SQL, агент для Exchange, агент для Active Directory

Агент для SQL устанавливается на машину с Microsoft SQL Server.

Агент для Exchange устанавливается на машину с ролью почтового ящика Microsoft Exchange Server (подробнее в разделе "Компоненты" (стр. 18)).

Агент для Active Directory устанавливается на контроллер домена.

- Windows Server 2012 R2 (64-разрядные версии) – все выпуски, включая Storage Server;
- Windows Server 2016–2022 (64-разрядные версии) – все выпуски, кроме Nano Server;
- Windows 10/11 (64-разрядные версии) – все выпуски.

Поддерживаемые версии Microsoft SQL Server, Microsoft Exchange Server и Microsoft Active Directory приведены в разделе "Поддерживаемые версии приложений Microsoft" (стр. 36).

© ООО Киберпротект, 2026

Агент для VMware (Windows)

Агент устанавливается на машину с ОС Windows с сетевым доступом к vCenter Server и хранилищу виртуальных машин.

Этот агент предоставляется в виде приложения Windows для работы в любой из перечисленных выше операционных систем для агента для Windows.

Список поддерживаемых версий VMware приведен в разделе "Поддерживаемые платформы виртуализации" (стр. 29).

Используйте этот агент в случаях, когда необходимо настроить резервное копирование без использования локальной сети (LAN-free backup), когда доступен свободный сервер на базе Windows либо требуется развертывание на этой ОС. Во всех прочих сценариях рекомендуется задействовать агенты на базе виртуального устройства, как описано ниже в данном разделе.

Агент для Oracle

Агент устанавливается на машину с Oracle Database.

- Windows Server 2012 R2 – выпуски Standard, Enterprise, Datacenter и Web (x64);
- Linux: все ядра и дистрибутивы, которые поддерживаются агентом для Linux (перечислены ниже).

Поддерживаемые версии СУБД приведены в разделе "Защита Oracle Database" (стр. 569).

Агент для MySQL/MariaDB

Агент для MySQL/MariaDB устанавливается непосредственно на машину с СУБД вместе с агентом для Linux. Поддерживает те же ОС, что и агент для Linux. Список поддерживаемых версий для MySQL/MariaDB приведен в разделе "Поддерживаемые СУБД" (стр. 35).

Агент для Linux

Агент устанавливается непосредственно на защищаемое устройство.

Поддерживаемые ОС:

- Astra Linux Special Edition 1.6 - 1.8.3;
- Astra Linux Common Edition 2.12;
- Альт Сервер 9, 10, 11;
- Альт Рабочая станция 9, 10, 11;
- Альт 8, 10 СП;
- РЕД ОС 7.2, 7.3, 8;
- РОСА «КОБАЛЬТ» 7.9, «ХРОМ» 12.5;
- Red Hat Enterprise Linux версии с 7.x по 8.x, кроме конфигураций со Stratis;

© ООО Киберпротект, 2026

- Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS;
- SUSE Linux Enterprise Server 12, 15, 15.5 — поддерживается в файловых системах, за исключением Btrfs;
- Debian 10, 11, 12;
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3, 9 Stream, 10 Stream;
- Oracle Linux 8.0, 8.1, 8.2, 8.3, 9.5 — Unbreakable Enterprise Kernel и Red Hat Compatible Kernel;
- AlterOS 7.5, 9.5;
- ОСнова 2.7 – 2.10, 3.0.

Указанные ОС поддерживаются только с версиями ядра от 3.0 до 6.14 и glibc версии 2.17 и новее.

Перед установкой продукта в системе, в которой не используется диспетчер пакетов RPM, такой как Ubuntu, необходимо установить этот диспетчер вручную, например, выполнив следующую команду (в качестве привилегированного пользователя): apt-get install rpm

Агент для PostgreSQL

Агент устанавливается на машину с сервером PostgreSQL или на машину, у которой есть сетевой доступ к серверу PostgreSQL.

Поддерживаемые ОС Windows:

- Windows Server 2012 R2 (x64);
- Windows Server 2016–2022;
- Windows 10 (x64);
- Windows 11.

Поддерживаемые ОС Linux:

- Astra Linux Special Edition 1.6 – 1.8;
- РЕД ОС 7.2, 7.3, 8;
- РОСА «КОБАЛЬТ» 7.9, «ХРОМ» 12.5;
- Альт Сервер 9, 10;
- ОСнова 2.7 – 2.10, 3.0;
- Red Hat Enterprise Linux версии с 7.x по 8.x, кроме конфигураций со Stratis;
- Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS;
- SUSE Linux Enterprise Server 12, 15, 15.5 — поддерживается в файловых системах, за исключением Btrfs;
- Debian 10, 11, 12;
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3, 9 Stream, 10 Stream.

Указанные ОС поддерживаются только с версиями ядра от 3.0 до 6.14.

© ООО Киберпротект, 2026

Перед установкой продукта в системе, в которой не используется диспетчер пакетов RPM, такой как Ubuntu, необходимо установить этот диспетчер вручную, например выполнив следующую команду в качестве суперпользователя: apt-get install rpm

Поддерживаемые виды и версии СУБД приведены в разделе "Защита баз данных PostgreSQL" (стр. 584).

Агент для CommuniGate Pro, агент для VK WorkMail, агент для Mailion

Агенты устанавливаются на машину с целевой системой или на машину, у которой есть сетевой доступ к целевой системе.

- Windows — все ОС, которые поддерживаются агентом для Windows.
- Linux — все ядра и дистрибутивы, которые поддерживаются агентом для Linux.

Список поддерживаемых версий почтовых сервисов приведен в разделе "Поддерживаемые почтовые сервисы" (стр. 35).

Агент для Hyper-V

Агент устанавливается на хост Hyper-V.

- Windows Server 2012 R2 (64-разрядные версии) — все выпуски с активной ролью Hyper-V, включая Server Core;
- Windows Server 2016 - 2022 (64-разрядные версии) — все выпуски с активной ролью Hyper-V, кроме Nano Server;
- Windows 10/11 (64-разрядные версии) — все выпуски с активной ролью Hyper-V.

Список поддерживаемых версий платформы Hyper-V приведен в разделе "Поддерживаемые платформы виртуализации" (стр. 29).

Агенты, предоставляемые в виде виртуальных устройств

Агенты устанавливаются в виде виртуального устройства с предустановленной поддерживаемой ОС.

- Агент для VMware;
- Агент для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация);
- Агент для SpaceVM;
- Агент для ECP VeiL;
- Агент для OpenStack;
- Агент для Basis DynamiX Enterprise;
- Агент для OpenNebula;
- Агент для Proxmox VE.

© ООО Киберпротект, 2026

Список поддерживаемых версий платформ виртуализации приведен в разделе "Поддерживаемые платформы виртуализации" (стр. 29).

2.2.2.2 Сервер управления

ПО сервера управления должно быть установлено на аппаратную платформу, оснащённую одной из указанных ниже операционных систем. Информация о возможных конфигурациях аппаратной платформы приведена в разделе "Рекомендуемые конфигурации оборудования для сервера управления" (стр. 48).

Более подробные сведения о сервере управления приведены в разделе "Компоненты" (стр. 18).

Поддерживаемые версии ОС Windows

- Windows Server 2016 – 2022 (64-разрядные версии) — все выпуски, кроме Nano Server
- Windows 11 (64-разрядные версии) — все выпуски

Поддерживаемые ядра Linux и готовые дистрибутивы

Агент устанавливается непосредственно на защищаемое устройство.

Поддерживаемые ОС:

- Astra Linux Special Edition 1.6 – 1.8.3;
- Astra Linux Common Edition 2.12;
- Альт Сервер 9, 10, 11;
- Альт Рабочая станция 9, 10, 11;
- Альт 8, 10 СП;
- РЕД ОС 7.2, 7.3, 8;
- РОСА «КОБАЛЬТ» 7.9, «ХРОМ» 12.5;
- Red Hat Enterprise Linux версии с 7.x по 8.x, кроме конфигураций со Stratis;
- Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS;
- SUSE Linux Enterprise Server 12, 15, 15.5 — поддерживается в файловых системах, за исключением Btrfs;
- Debian 10, 11, 12;
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3, 9 Stream, 10 Stream;
- Oracle Linux 8.0, 8.1, 8.2, 8.3, 9.5 — Unbreakable Enterprise Kernel и Red Hat Compatible Kernel;
- AlterOS 7.5, 9.5;
- ОСнова 2.7 – 2.10, 3.0.

Указанные ОС поддерживаются только с версиями ядра от 3.0 до 6.14 и glibc версии 2.17 и новее.

© ООО Киберпротект, 2026

Перед установкой продукта в системе, в которой не используется диспетчер пакетов RPM, такой как Ubuntu, необходимо установить этот диспетчер вручную, например, выполнив следующую команду (в качестве привилегированного пользователя): apt-get install rpm

2.2.2.3 Узел хранения

ПО узла хранения должно быть установлено на аппаратную платформу, оснащённую одной из указанных ниже операционных систем. Более подробные сведения об узле хранения приведены в разделе "Компоненты" (стр. 18).

Поддерживаемые версии ОС Windows

- Windows Server 2012 R2 (64-разрядные версии) — все выпуски, включая Storage Server;
- Windows Server 2016 - 2022 (64-разрядные версии) — все выпуски, кроме Nano Server;
- Windows 10/11 (64-разрядные версии) — все выпуски.

Поддерживаемые ядра Linux и готовые дистрибутивы

Агент устанавливается непосредственно на защищаемое устройство.

Поддерживаемые ОС:

- Astra Linux Special Edition 1.6 - 1.8.3;
- Astra Linux Common Edition 2.12;
- Альт Сервер 9, 10, 11;
- Альт Рабочая станция 9, 10, 11;
- Альт 8, 10 СП;
- РЕД ОС 7.2, 7.3, 8;
- РОСА «КОБАЛЬТ» 7.9, «ХРОМ» 12.5;
- Red Hat Enterprise Linux версии с 7.x по 8.x, кроме конфигураций со Stratis;
- Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS;
- SUSE Linux Enterprise Server 12, 15, 15.5 — поддерживается в файловых системах, за исключением Btrfs;
- Debian 10, 11, 12;
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3, 9 Stream, 10 Stream;
- Oracle Linux 8.0, 8.1, 8.2, 8.3, 9.5 — Unbreakable Enterprise Kernel и Red Hat Compatible Kernel;
- AlterOS 7.5, 9.5;
- ОСнова 2.7 - 2.10, 3.0.

Указанные ОС поддерживаются только с версиями ядра от 3.0 до 6.14 и glibc версии 2.17 и новее.

© ООО Киберпротект, 2026

Перед установкой продукта в системе, в которой не используется диспетчер пакетов RPM, такой как Ubuntu, необходимо установить этот диспетчер вручную, например, выполнив следующую команду (в качестве привилегированного пользователя): apt-get install rpm

2.2.3 Поддерживаемые платформы виртуализации

В следующей таблице приведены платформы виртуализации, для которых можно выполнять резервное копирование с помощью Кибер Бэкап.

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
Киберпротект		
Кибер Инфраструктура версии с 6.0 по 6.5.2	+	+
HOSTVM		
HOSTVM 4	+	+
РЕД СОФТ		
РЕД Виртуализация 7.2, 7.3, 7.3.2, 8.0*	+	+
РОСА		
ROSA Virtualization 2.0, 2.1, 3.0**	+	+
РУСТЭК		
РУСТЭК 2.6	+	+
VK Cloud		
VK Cloud 4.0	+	+
zVirt		
zVirt 3.0, 3.1, 3.2, 3.3, 4.0, 4.1, 4.2, 4.3, Max, 4.4, 4.5, 5.0	+	+
SpaceVM		
SpaceVM с 6.0.5 по 6.5.8	+	+

© ООО Киберпротект, 2026

ECP VeiL		
ECP VeiL с 4.7 по 5.1.10	+	+
Basis DynamiX Enterprise		
Basis DynamiX Enterprise версии 3.8.8 – 4.1, 4.3	+	+
Proxmox Virtual Environment		
Proxmox Virtual Environment версии 7.2, 7.3, 7.4, 8.4.0, 9.0.3	+	+
ПК СВ "Брест"		
ПК СВ "Брест", основанный на версии OpenNebula 6.0.0.2	+	+
Альт Виртуализация		
Альт Виртуализация 10, основанная на версии OpenNebula 6.2.0.1 Альт Виртуализация PVE версии 10.2, 11	+	+
Система группового управления "Горизонт-ВС"		
Система группового управления "Горизонт-ВС" версии 1.8.3 и выше	+	+
VMware		
Версии VMware vSphere: 6.5, 6.7, 7.0, 8.0 – 8.0 Update 3 **Выпуски VMware vSphere:** VMware vSphere Essentials VMware vSphere Essentials Plus VMware vSphere Standard VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (бесплатная низкоуровневая оболочка ESXi)***		+
VMware Server (VMware Virtual Server) VMware Workstation VMware ACE		+

© ООО Киберпротект, 2026

VMware Player		
Microsoft		
Windows Server 2012 R2 с Hyper-V Microsoft Hyper-V Server 2012 R2 Windows 10 с Hyper-V Windows Server 2016 с Hyper-V – все варианты установки, кроме Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 с Hyper-V – все варианты установки, кроме Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 с Hyper-V – все варианты установки, кроме Nano Server****	+	+
Microsoft Virtual PC 2004 и 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
oVirt		
oVirt 4.2, 4.3, 4.4, 4.5	+	+
OpenStack		
От Ussuri до Zed, а также Caracal и Dalmatian	+	+
OpenNebula		
OpenNebula версии 6.0.0.2	+	+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6		Только полностью виртуализированные (известные также как HVM) гостевые системы. Паравиртуализированные (известные также как PV) гостевые системы не поддерживаются.
Red Hat и Linux		

© ООО Киберпротект, 2026

Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1, 4.2, 4.3, 4.4		+
Виртуальные машины на основе ядра (KVM)		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Только полностью виртуализированные (известные также как HVM) гостевые системы. Паравиртуализированные (известные также как PV) гостевые системы не поддерживаются.
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x-20180425.x		+
Amazon		
Экземпляры Amazon EC2		+
Microsoft Azure		
Виртуальные машины Azure		+

* Для систем РЕД Виртуализация технология Changed Block Tracking (CBT) не поддерживается.

** Для ROSA Virtualization 3.0 не поддерживается восстановление ВМ с ОС на основе CentOS в новую ВМ на платформу VMware.

*** Резервное копирование на уровне гипервизора не поддерживается для vSphere Hypervisor, так как в этом продукте доступ к удаленному интерфейсу командной строки (RCLI) возможен исключительно в режиме «только для чтения». Агент работает в течение пробного периода vSphere Hypervisor до введения серийного ключа. После введения серийного ключа агент перестает работать.

**** Резервное копирование с поддержкой приложений не поддерживается.

© ООО Киберпротект, 2026

2.2.3.1 Ограничения

- **Отказоустойчивые машины**

  Агент для VMware выполняет резервное копирование отказоустойчивой машины, только если в VMware vSphere включена отказоустойчивость. При выполнении обновления с более ранней версии vSphere достаточно отключить и снова включить отказоустойчивость для каждой машины. При использовании более ранней версии vSphere установите агент в гостевой операционной системе.
- **Резервное копирование дисков и томов**

  Для резервного копирования виртуальным устройством дисков и томов ВМ можно использовать только правило политики [Disk N] (см. раздел "Выбор дисков и томов" (стр. 275)).
- **Независимые диски и RDM-диски**

  Агент для VMware не создает резервные копии RDM-дисков в режиме физической совместимости или независимых дисков. При выполнении резервного копирования агент пропускает эти диски и добавляет предупреждения в журнал. Чтобы не получать эти предупреждения, следует исключить из плана защиты независимые диски и RDM-диски в режиме физической совместимости. Если необходимо выполнить резервное копирование этих дисков или данных на этих дисках, установите агент в гостевой операционной системе.
- **Диски прямого доступа**

  Агенты для Hyper-V не выполняют резервного копирования дисков прямого доступа. Во время резервного копирования агент пропускает эти диски и добавляет предупреждения в журнал. Чтобы не получать эти предупреждения, следует исключить из плана защиты диски прямого доступа. Если необходимо выполнить резервное копирование этих дисков или данных на этих дисках, установите агент в гостевой операционной системе.
- **Кластеризация гостевых систем Hyper-V**

  Агент для Hyper-V не поддерживает резервное копирование виртуальных машин Hyper-V, которые являются узлами отказоустойчивого кластера Windows Server. Моментальный снимок VSS на уровне хоста может даже временно отключить внешний диск кворума от кластера. Если необходимо выполнить резервное копирование этих машин, установите агенты в гостевых операционных системах.
- **Подключение iSCSI в гостевой ОС**

  Агент для VMware и агент для Hyper-V не выполняют резервное копирование томов логического устройства, подключенных инициатором iSCSI, который работает в этой гостевой операционной системе. Поскольку у гипервизоров ESXi и Hyper-V нет никакой информации о таких томах, эти тома не включаются в моментальные снимки на уровне гипервизора, а их резервное копирование пропускается без предупреждений. Чтобы создать резервную копию этих томов или данных на этих томах, установите агент в гостевой операционной системе.
- **Машины Linux с логическими томами (LVM)**

  Агент для VMware и агент для Hyper-V не поддерживают указанные ниже операции для машин Linux с LVM:

© ООО Киберпротект, 2026

- Миграция P2V и V2P. Используйте агент для Linux или загрузочный носитель, чтобы создать резервную копию, и загрузочный носитель для восстановления.
- Запуск виртуальной машины из резервной копии, созданной агентом для Linux или загрузочным носителем.
- Преобразование резервной копии, созданной агентом для Linux или загрузочным носителем, в виртуальную машину.

- **Зашифрованные виртуальные машины** (эта функциональная возможность представлена в VMware vSphere 6.5)
  - Резервное копирование зашифрованных виртуальных машин выполняется в незашифрованном состоянии.
  - Восстановленные виртуальные машины всегда являются незашифрованными.
  - При резервном копировании виртуальных машин рекомендуем также шифровать виртуальную машину, на которой запущен агент для VMware. В противном случае операции с зашифрованными машинами могут выполняться медленнее, чем ожидается. Примените **политику шифрования ВМ** к машине агента, используя веб-клиент vSphere.
  - Резервное копирование зашифрованных виртуальных машин будет выполнено по локальной сети, даже если настроен режим транспорта сети SAN для агента. Агент выполнит возврат из реплики, используя транспорт NBD, поскольку VMware не поддерживает транспорт сети SAN для резервного копирования зашифрованных виртуальных дисков.
- **Безопасная загрузка** (эта функциональная возможность представлена в VMware vSphere 6.5)

  Безопасная загрузка отключается после восстановления виртуальной машины как новой виртуальной машины. По окончании восстановления можно вручную включить этот параметр.
- **Резервное копирование конфигурации ESXi** не поддерживается для VMware vSphere 7.0 и новее.
- **Виртуальные диски типа Direct LUN виртуальных машин oVirt и аналогичных систем виртуализации**

  При резервном копировании виртуальных машин систем виртуализации oVirt, ROSA Virtualization, zVirt, Red Hat Virtualization, РЕД Виртуализация и HOSTVM виртуальные диски типа Direct LUN не включаются в резервные копии.
- **Сортировка дисков виртуальных машин oVirt и аналогичных систем виртуализации**

  При резервном копировании только выбранных дисков виртуальных машин систем виртуализации oVirt, ROSA Virtualization, zVirt и РЕД Виртуализация необходимо включить сортировку дисков ВМ на виртуальном устройстве с агентом. Для этого в файле /etc/Acronis/VirtualWare.config установите значение 1 параметру DiskSortingEnabled. Например:

```
<key name="oVirt">
...
<value name="DiskSortingEnabled" type="Tdword">1</value>
...
</key>
```


© ООО Киберпротект, 2026

2.2.4 Поддерживаемые почтовые сервисы

Кибер Бэкап позволяет выполнять резервное копирование следующих почтовых сервисов:

- CommuniGate Pro 6.3.14 - 6.5.2 (см. раздел "Защита CommuniGate Pro" (стр. 502)).
- VK WorkMail 25.4 (см. раздел "Защита VK WorkMail и VK WorkDisk" (стр. 532)).
- Mailion 2.3 (см. раздел "Защита Mailion" (стр. 558)).
- Microsoft Exchange Server (см. раздел "Защита приложений Microsoft" (стр. 475)):
  - Microsoft Exchange Server 2016-2019 – все выпуски;
  - Microsoft Exchange Server 2013 – все выпуски, накопительный пакет обновления 1 (CU1) или более поздней версии.

2.2.5 Поддерживаемые СУБД

Кибер Бэкап позволяет выполнять резервное копирование следующих систем управления базами данных:

- СУБД Ред База Данных 3.0 – 5.1
- PostgreSQL 11–17;
- PostgreSQL для 1С;
- Postgres Pro Standard 11–17;
- Postgres Pro Enterprise 11–17;
- Patroni 3.0 – 3.2.1;
- Platform V Pangolin SE 6.1.7 (требуются дополнительные настройки на машине с агентом, подробнее см. статью базы знаний);
- Proxima DB 2.0, 3.0;
- СУБД Jatoba 5 (в случае возникновения ошибки при подключении экземпляра PostgreSQL для гранулярного восстановления см. статью базы знаний);
- СУБД Tantor 14–17;
- Arenadata Prosperity 4.0.
- MariaDB 10.4
- MySQL 8.0 и новее
- MongoDB 6.0

  Поддержка через "Команды до и после процедуры" (стр. 365).
- Microsoft SQL Server 2012–2019
- Oracle Database 11-19 – все выпуски
- SAP HANA 2.0 SPS 03, установленная в RHEL 7.6 на физической машине или виртуальной машине VMware ESXi

© ООО Киберпротект, 2026

Поскольку SAP HANA не поддерживает восстановление контейнеров баз данных с несколькими арендаторами с использованием моментальных снимков хранилища, данное решение поддерживает контейнеры SAP HANA с базой данных только одного арендатора.

2.2.6 Поддерживаемые версии приложений Microsoft

2.2.6.1 Поддерживаемые версии Microsoft Active Directory

Поддерживается резервное копирование контроллеров домена Active Directory, развернутых на серверах следующих версий:

- Microsoft Windows Server 2016-2022 – все выпуски, кроме Nano Server;
- Microsoft Windows Server 2012 R2 – все выпуски, включая Storage Server.

2.2.6.2 Поддерживаемые версии Microsoft Exchange Server

- Microsoft Exchange Server 2016-2019 – все выпуски;
- Microsoft Exchange Server 2013 – все выпуски, накопительный пакет обновления 1 (CU1) или более поздней версии.

2.2.6.3 Поддерживаемые версии Microsoft SharePoint

Кибер Бэкап поддерживает резервное копирование баз данных SQL Server, используемых локально установленными продуктами SharePoint следующих версий:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2 (необходима ферма восстановления SharePoint для прикрепления баз данных)

Защита данных SharePoint в Microsoft 365 не поддерживается.

Резервные копии или базы данных, из которых извлекаются данные, должны происходить из той же версии SharePoint, что и версия, где установлен SharePoint Explorer.

2.2.6.4 Поддерживаемые версии Microsoft SQL Server

- Microsoft SQL Server 2012-2019.

2.2.7 Необходимые пакеты для ОС Linux

Чтобы добавить необходимые модули к ядру Linux, программе установки требуются перечисленные ниже пакеты Linux:

© ООО Киберпротект, 2026

- Пакет с заголовками или исходными кодами ядра. Версия пакета должна соответствовать версии ядра.
- Набор компиляторов GNU Compiler Collection (GCC). Версия GCC должна быть той же, с которой было скомпилировано ядро.
- Инструмент Make.
- Интерпретатор Perl.
- Инструмент mokutil. Необходим для определения режима загрузки ОС (UEFI с Secure Boot, UEFI без Secure Boot, BIOS).
- Библиотеки libelf-dev, libelf-devel или elfutils-libelf-devel с установленным параметром CONFIG_UNWINDER_ORC=y. Библиотеки необходимы для сборки ядер не ниже 4.15. Для некоторых дистрибутивов их необходимо установить отдельно от заголовков ядра.

Для корректного формирования и выгрузки отчётов в ОС ALT Linux также требуется набор шрифтов, включая следующие пакеты:

- fonts-ttf-ms;
- fonts-ttf-liberation;
- fonts-ttf-dejavu;
- fonts-ttf-PTAstra;
- fonts-ttf-paratype-pt-*.

Примечание
Названия вышеуказанных пакетов зависят от используемого дистрибутива ОС Linux.

В ОС Red Hat Enterprise Linux и CentOS пакеты обычно устанавливаются программой установки. В других дистрибутивах вы должны сами установить пакеты, если они не установлены или это не те версии, которые требуются.

2.2.7.1 Установлены ли необходимые пакеты?

Чтобы проверить, установлены ли пакеты, сделайте следующее:

1. Выполните следующую команду, чтобы узнать версию ядра и необходимую версию GCC:

   ```
   $ cat /proc/version
   ```

   Эта команда возвращает примерно такие строки: Linux version 2.6.35.6 и gcc version 4.5.1
2. Выполните следующие команды, чтобы узнать, установлен ли инструмент Make и компилятор GCC:

   ```
   $ make -v
   $ gcc -v
   ```

   Для gcc убедитесь, что команда возвращает ту же версию, что и в параметре версия gcc в шаге 1. Для инструмента make просто проверьте, что команда выполняется.

© ООО Киберпротект, 2026

3. Проверьте, установлена ли соответствующая версия пакетов для создания модулей ядра.
   - В Red Hat Enterprise Linux и CentOS выполните следующую команду:

     ```
     $ yum list installed | grep kernel-devel
     ```

   - В Ubuntu выполните следующие команды:

     ```
     $ dpkg --get-selections | grep linux-headers
     $ dpkg --get-selections | grep linux-image
     ```

   В каждом из этих случаев убедитесь в том, что версии такие же, как в параметре Linux version в шаге 1.
4. Чтобы выяснить, установлен ли интерпретатор Perl, выполните следующую команду:

   ```
   $ perl --version
   ```

   Если на экране отображаются сведения о версии Perl, это означает, что интерпретатор установлен.
5. Проверьте, установлен ли инструмент mokutil.
   - В Red Hat Enterprise Linux и CentOS выполните следующую команду:

     ```
     $ yum list installed | grep mokutil
     ```

   - В Ubuntu выполните следующую команду:

     ```
     $ dpkg --get-selections | grep mokutil
     ```

6. В Red Hat Enterprise Linux и CentOS выполните следующую команду, чтобы проверить, установлена ли библиотека elfutils-libelf-devel:

   ```
   $ yum list installed | grep elfutils-libelf-devel
   ```

   Если на экране отображаются сведения о версии библиотеки, это означает, что библиотека установлена.

2.2.7.2 Установка пакетов из репозитория

В следующей таблице указано, как установить необходимые пакеты в различных дистрибутивах Linux.

Дистрибутив Linux	Имена пакетов	Как установить
Red Hat Enterprise Linux	kernel-devel gcc make elfutils-libelf-devel	Программа установки загрузит и установит пакеты автоматически по вашей подписке на Red Hat.

© ООО Киберпротект, 2026

<table>
<tr><td></td><td>perl
mokutil</td><td>Выполните следующие команды:
<pre>$ yum install perl
$ yum install mokutil</pre></td></tr>
<tr><td rowspan="2">CentOS</td><td>kernel-devel
gcc
make
elfutils-libelf-devel</td><td>Программа установки загрузит и установит пакеты автоматически.</td></tr>
<tr><td>perl
mokutil</td><td>Выполните следующие команды:
<pre>$ yum install perl
$ yum install mokutil</pre></td></tr>
<tr><td>Ubuntu
Debian</td><td>linux-headers
linux-image
rpm
gcc
make
perl
mokutil</td><td>Выполните следующие команды:
<pre>$ sudo apt-get update
$ sudo apt-get install linux-headers-$(uname -r)
$ sudo apt-get install linux-image-$(uname -r)
$ sudo apt-get install rpm
$ sudo apt-get install gcc-<версия>
$ sudo apt-get install make
$ sudo apt-get install perl
$ sudo apt-get install mokutil</pre></td></tr>
<tr><td>SUSE Linux
OpenSUSE</td><td>kernel-source
gcc
make
perl
mokutil</td><td>Выполните следующие команды:
<pre>$ sudo zypper install kernel-source
$ sudo zypper install gcc
$ sudo zypper install make
$ sudo zypper install perl
$ sudo zypper install mokutil</pre>Для OpenSUSE 12.3:
<pre>$ cd /usr/src/linux
$ sudo make oldconfig && make modules_prepare
&& make prepare</pre></td></tr>
<tr><td>Astra Linux</td><td>rpm
gcc
make
linux-headers
mokutil
zstd
libnss3

Дополнительно для</td><td>Выполните следующие команды:
<pre>$ sudo apt install rpm
$ sudo apt install gcc
$ sudo apt install make
$ sudo apt-get install linux-headers-`uname -r`
$ sudo apt-get install mokutil
$ sudo apt-get install zstd
$ sudo apt-get install libnss3</pre></td></tr>
</table>

© ООО Киберпротект, 2026

	ядер версии 5.10 и новее:
	flex
	bison
		`$ sudo apt install flex`
		`$ sudo apt install bison`
		
		Если используется Astra SE, пакеты необходимо установить с диска разработчика для текущей версии Astra.

ALT Linux	kernel-source
	kernel-headers-modules
	gcc
	make
	kmod-sign
	mokutil
	fonts-ttf-ms
	fonts-ttf-liberation
	fonts-ttf-dejavu
	fonts-ttf-PTAstra
	fonts-ttf-paratype-pt-*
		Выполните следующие команды:
		
		`$ su -`
		`# apt-get install kernel-source-<x.x>`
		`(где <x.x> - версия ядра)`
		`# apt-get install kernel-headers-modules-std-def`
		`# apt-get install gcc`
		`# apt-get install make`
		`# apt-get install kmod-sign`
		`# apt-get install mokutil`
		`# apt-get install fonts-ttf-ms`
		`# apt-get install fonts-ttf-liberation`
		`# apt-get install fonts-ttf-dejavu`
		`# apt-get install fonts-ttf-PTAstra`
		`# apt-get install fonts-ttf-paratype-pt-*`
		
		Если версия пакетов в репозитории новее версии текущего ядра, необходимо также обновить ядро:
		
		`$ su -`
		`# apt-get update`
		`# apt-get dist-upgrade`
		`# update-kernel`
		
		После этого перезагрузите систему.

РЕД ОС	kernel-lt-devel
	kernel-lt-headers
	mokutil
		Выполните следующие команды:
		
		`$ sudo yum install kernel-lt-devel`
		`$ sudo yum install kernel-lt-headers`
		`$ sudo yum install gcc`
		`$ sudo yum install make`
		`$ sudo yum install mokutil`
		
		Желательно также полностью обновить систему:
		
		`$ sudo yum update`
		
		И затем перезагрузить ее.

Пакеты будут загружены из репозитория дистрибутива и установлены.

Примечание

Для разных операционных систем на основе Linux названия этих пакетов могут отличаться.

© ООО Киберпротект, 2026

Для других дистрибутивов Linux обратитесь к документации по дистрибутиву, чтобы выяснить точные имена необходимых пакетов и способы их установки.

2.2.7.3 Установка пакетов вручную

Возможно, необходимо будет установить пакеты **вручную**, если:

- У машины нет активной подписки на Red Hat или подключения к Интернету.
- Программе установки не удается найти версию kernel-devel или gcc, соответствующую версии ядра. Если доступная версия kernel-devel новее версии ядра, необходимо обновить ядро или установить соответствующую версию kernel-devel вручную.
- Необходимые пакеты имеются в локальной сети, и вы не хотите тратить время на автоматический поиск и загрузку.

Загрузите пакеты из своей локальной сети или с веб-сайта надежного третьего поставщика и установите, как описано ниже.

- В Red Hat Enterprise Linux и CentOS выполните следующую команду как привилегированный пользователь:

  ```
  $ rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

- В Ubuntu выполните следующую команду:

  ```
  $ sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

Пример установки пакетов вручную

Для установки необходимых пакетов выполните следующие шаги.

1. Узнайте версии ядра и GCC. Например:

   ```
   $ cat /proc/version
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. Получите пакеты kernel-devel и gcc, которые соответствуют этой версии ядра:

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. Получите пакет make:

   ```
   make-3.82-3.fc14.i686
   ```

4. Установите пакеты, выполнив следующую команду как привилегированный пользователь:

   ```
   $ rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
   $ rpm -ivh gcc-4.5.1.fc14.i686.rpm
   $ rpm -ivh make-3.82-3.fc14.i686
   ```


© ООО Киберпротект, 2026

Все эти пакеты можно указать в одной команде rpm. Установка этих пакетов может потребовать установки дополнительных пакетов для разрешения зависимостей.

Дополнительные пакеты для ОС Linux

Для резервного копирования в сетевые папки на машине с установленным агентом для Linux необходимо иметь установленные дополнительные пакеты Linux. Например, для CentOS 7 должны быть установлены следующие пакеты (в зависимости от места сохранения резервных копий):

МЕСТО СОХРАНЕНИЯ	НЕОБХОДИМЫЙ КОМПОНЕНТ LINUX
SMB NTLM	cifs-utils
SMB with Kerberos	cifs-utils keyutils
NFS	nfs-utils

2.2.8 Совместимость с ОС Astra Linux SE

В этом разделе собраны сведения об особенностях использования продукта Кибер Бэкап на машинах с ОС Astra Linux Special Edition, в которой включены мандатное управлением доступом (МРД) и мандатный контроль целостности (МКЦ). Эти механизмы обеспечивают защиту конфиденциальности информации и целостности ОС и ее приложений. Подробные сведения о работе МРД и МКЦ см. в документации Astra Linux.

2.2.8.1 Установка компонентов Кибер Бэкап

- Если включено только МРД, установку необходимо выполнять с привилегиями администратора от имени пользователя из группы astra-admin, используя минимальный уровень конфиденциальности и пустой набор категорий конфиденциальности.
- Если включен только МКЦ, установку необходимо выполнять с привилегиями администратора от имени пользователя из группы astra-admin, используя максимальный уровень целостности.
- Если включены как МРД, так и МКЦ, установку необходимо выполнять с привилегиями администратора от имени пользователя из группы astra-admin, используя минимальный уровень конфиденциальности, пустой набор категорий конфиденциальности и максимальный уровень целостности.

Пример установки при включенных МРД и МКЦ:

```
myuser@astra-smol1-7-3:~$ id
uid=1000(myuser) gid=1000(myuser) groups=...(astra-admin)...
myuser@astra-smol1-7-3:~$ pdp-id
Уровень конф.=0(Уровень_0), Уровень целостности:63(Высокий), Категории=0x0(Нет)
Роли=()
myuser@astra-smol1-7-3:~$ chmod +x CyberBackup_18_64-bit.x86_64
myuser@astra-smol1-7-3:~$ sudo update-initramfs -u -k all
```


© ООО Киберпротект, 2026

```
myuser@astra-smol1-7-3:~$ sudo reboot
myuser@astra-smol1-7-3:~$ sudo ./CyberBackup_18_64-bit.x86_64
...
```

2.2.8.2 Резервное копирование дисков и томов

Резервное копирование выполняется обычным образом, так как оно осуществляется на уровне блочных устройств.

2.2.8.3 Резервное копирование файлов и папок

Резервное копирование выполняется обычным образом, так как агент защиты запущен с привилегиями администратора и обладает полным доступом ко всем файловым системам.

2.2.8.4 Восстановление дисков и томов

Восстановление выполняется обычным образом, так как оно осуществляется на уровне блочных устройств.

2.2.8.5 Восстановление файлов и папок

При восстановлении Кибер Бэкап пытается назначить изначальные мандатные метки восстановленным файлам и папкам, однако какие мандатные метки получат восстановленные объекты в итоге, зависит от правил, действующих в ОС с включенными МРД и МКЦ.

Предупреждение
При восстановлении файлов и папок с мандатными метками на файловую систему, не поддерживающую МРД и МКЦ, мандатные метки не восстанавливаются.

Для сохранения изначальных мандатных меток файлов и папок при восстановлении из резервной копии необходимо назначать PARSEC-привилегию PARSEC_CAP_UNSAFE_SETXATTR агенту защиты на время восстановления.

Чтобы назначить эту привилегию агенту, выполните следующие действия на целевой машине:

1. Измените файл /etc/systemd/system/acronis_mms.service так, как показано ниже:

   ```
   ...
   [Service]
   CapabilitiesParsec=PARSEC_CAP_UNSAFE_SETXATTR
   ...
   ```

2. Выполните следующие команды:

   ```
   systemctl daemon-reload
   systemctl restart acronis_mms.service
   ```


© ООО Киберпротект, 2026

3. Запишите 1 в файл /parsecfs/unsecure_setxattr, чтобы привилегия PARSEC_CAP_UNSAFE_ SETXATTR вступила в силу, например:

```
echo 1 | sudo tee /parsecfs/unsecure_setxattr
```

Примечание
После перезагрузки машины в файл /parsecfs/unsecure_setxattr записывается 0.

2.2.8.6 Репликация резервных копий

При репликации резервных копий их tibx-файлам назначаются мандатные метки по правилам, действующим в ОС с включенными МРД и МКЦ.

2.2.8.7 Узел хранения

Узел хранения устанавливается как компонент Кибер Бэкап и работает обычным образом.

2.2.8.8 Пользователи организации и ее отделов

Учетные данные пользователей, созданных на машине с сервером управления, используются для аутентификации пользователей организации и ее отделов в веб-панели Кибер Бэкап. Кибер Бэкап не учитывает, какие уровни конфиденциальности, категории конфиденциальности, уровни целостности и PARSEC-привилегии назначены этим пользователям на уровне ОС.

2.2.9 Совместимость с программами шифрования

Нет ограничений на резервное копирование и восстановление данных, зашифрованных программой шифрования на уровне файлов.

Программы шифрования на уровне дисков шифруют данные в реальном времени. Поэтому данные, содержащиеся в резервной копии, не шифруются. Программы шифрования на уровне дисков часто меняют области системы: загрузочные записи, таблицы разделов или таблицы файловой системы. Эти факторы влияют на резервное копирование и восстановление на уровне дисков, а также на возможность загрузки восстановленной системы и доступа ее к Зоне безопасности.

Можно создать резервную копию данных, зашифрованных при помощи указанных ниже программ шифрования на уровне файлов:

- Шифрование дисков Microsoft BitLocker,
- McAfee Endpoint Encryption,
- PGP Whole Disk Encryption.

Для надежного восстановления на уровне дисков следуйте общим правилам и рекомендациям по конкретному продукту.

© ООО Киберпротект, 2026

2.2.9.1 Типичные правила установки

Рекомендуется установить программу шифрования перед установкой агентов защиты.

2.2.9.2 Способ использования Зоны безопасности

Зона безопасности не должна быть зашифрована на уровне дисков. Это единственный способ использования Зоны безопасности:

1. Установите программу шифрования, а затем установите агент.
2. Создайте Зону безопасности.
3. Исключите Зону безопасности при шифровании диска или его томов.

2.2.9.3 Общее правило резервного копирования

Позволяет выполнить резервное копирование на уровне дисков операционной системы. Не пытайтесь выполнить резервное копирование с использованием загрузочного носителя.

2.2.9.4 Процедуры восстановления для конкретных программ

Шифрование дисков Microsoft BitLocker

Как восстановить систему, зашифрованную функцией BitLocker:

1. Загрузите машину с загрузочного носителя.
2. Восстановите систему. Восстановленные данные будут незашифрованы.
3. Перезагрузите восстановленную систему.
4. Включите функцию BitLocker.

Если необходимо восстановить только один раздел диска, выполните восстановление из операционной системы. При восстановлении с использованием загрузочного носителя восстановленный раздел может не распознаваться системой Windows.

McAfee Endpoint Encryption и PGP Whole Disk Encryption

Можно восстановить шифрованный системный раздел, используя только загрузочный носитель.

Если восстановленную систему не удастся загрузить, восстановите основную загрузочную запись, как описано в статье базы знаний Майкрософт по ссылке https://support.microsoft.com/kb/2622803

2.2.10 Поддерживаемые интеграции со службами каталогов

Кибер Бэкап позволяет добавлять пользователей и группы пользователей из следующих служб каталогов:

© ООО Киберпротект, 2026

- Active Directory,
- Samba DC,
- FreeIPA,
- ALD Pro,
- РЕД АДМ.

Добавленные пользователи могут использовать свои учётные записи в службах каталогов для входа в веб-консоль Кибер Бэкап. Кроме того, им можно назначать привилегии для работы в Кибер Бэкап.

Процедура добавления учётных записей описана в разделе "Добавление административных учетных записей" (стр. 809).

2.3 Системные требования

В таблице ниже представлены требования к дисковому пространству и памяти для типичных сценариев установки компонентов продукта Кибер Бэкап. Установка выполняется с настройками по умолчанию.

Устанавливаемые компоненты	Для установки необходимо место на диске	Минимальный используемый объем памяти
Сервер управления	См. раздел "Рекомендуемые конфигурации оборудования для сервера управления" (стр. 48).	
Узел хранения и агент для ОС Windows Примечания: • поддерживается только 64-разрядная платформа; • для использования функции дедупликации требуется минимум 8 ГБ ОЗУ (дополнительные сведения см. в разделе "Рекомендации по дедупликации" (стр. 190)).	1,1 ГБ	330 МБ
Агент для ОС Windows	850 МБ	150 МБ
Агент для ОС Windows и один из следующих агентов: • агент для Microsoft SQL Server; • агент для Microsoft Exchange.	950 МБ	170 МБ
Агент для ОС Windows и один из следующих агентов: • агент для VMware (ОС Windows); • агент для Hyper-V.	1170 МБ	180 МБ
Агент для ОС Linux	2,0 ГБ	130 МБ

© ООО Киберпротект, 2026

Агент для oVirt (виртуальное устройство zVirt/ROSA Virtualization/РЕД Виртуализация)	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.
Агент для oVirt (для ОС Linux при использовании аппаратных снимков уровня СХД)	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.
Агент для SpaceVM	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.
Агент для ECP VeiL	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.
Агент для OpenStack	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.
Агент для Basis DynamiX Enterprise	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.
Агент для OpenNebula	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.
Агент для VMware	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.

Во время резервного копирования агент обычно занимает около 350 МБ памяти (значение получено при резервном копировании тома размером 500 ГБ). Максимальное потребление памяти может достигать 2 ГБ в зависимости от объема и типа обрабатываемых данных.

Для восстановления экземпляра базы данных PostgreSQL требуется не менее 4 ГБ памяти.

Для резервного копирования больших архивов (600 ГБ или больше) требуется 1 ГБ ОЗУ на каждый терабайт архива.

Для загрузочного носителя или восстановления диска с перезагрузкой требуется не менее 1 ГБ памяти.

© ООО Киберпротект, 2026

Объем компонентов Кибер Бэкап с учетом файлов журналов может достигать 2 ГБ.

Производительность сервера управления зависит от сценария его установки. По умолчанию сервер управления устанавливается с локальной СУБД SQLite, что накладывает ограничения на его производительность и возможности. Для повышения производительности рекомендуется использовать СУБД PostgreSQL или Microsoft SQL Server, установленную на отдельную машину. СУБД PostgreSQL можно использовать для сервера управления на машине с ОС Linux, а СУБД Microsoft SQL Server – для сервера управления на машине с ОС Windows. Подробнее о сценариях установки см. в разделе "Рекомендуемые конфигурации оборудования для сервера управления" (стр. 48).

2.3.1 Рекомендуемые конфигурации оборудования для сервера управления

В этом разделе описаны рекомендуемые конфигурации оборудования для различных сценариев установки сервера управления.

2.3.1.1 Сервер управления на машине с ОС Linux или Windows, использующий СУБД SQLite

Требования к оборудованию

Для работы сервера управления и размещения его баз данных необходимы следующие ресурсы:

- как минимум 6 ядер ЦП (для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 8 ядер),
- 16 ГБ ОЗУ,
- не менее 200 ГБ дискового пространства на SSD-диске.

Внимание
Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от типа, версии и редакции используемой ОС.

Рекомендуемая конфигурация продукта Кибер Бэкап

В продукте Кибер Бэкап, развернутом на оборудовании с описанными выше характеристиками, рекомендуется:

- Использовать не более 6 000 лицензий (для повышения производительности рекомендуется использовать одну корпоративную лицензию, в которую включены все необходимые агенты и виртуальные устройства).

  Для установок Кибер Бэкап с большим количеством контролируемых ресурсов рекомендуется добавлять лицензии до регистрации агентов и добавления устройств.
- Добавлять не более 6 000 устройств (физических и виртуальных машин, почтовых ящиков, баз данных и других ресурсов, отображаемых в веб-консоли Кибер Бэкап в разделе **Устройства**).

© ООО Киберпротект, 2026

- Добавлять не более 50 виртуальных устройств (virtual appliance).
- Включать в общий план не более 100 устройств (общий план включает в себя отдельные устройства), для большего количества устройств используйте групповые планы.
- Включать в групповой план не более 500 устройств (групповой план включает в себя группы устройств).
- Создавать не более 500 общих и групповых планов.
- Выполнять не более 500 одновременных операций резервного копирования и восстановления.
- Создавать не более 500 отделов.
- Использовать не более 10 уровней в иерархии отделов.
- Создавать в отделе не более 300 подотделов одного уровня.

Кроме того, общее количество записей в таблице resources БД службы учетных записей (Account Server) не должно превышать 60 000. Чем ближе общее количество записей к этой границе, тем ниже производительность сервера управления.

Внимание
При несоблюдении этих рекомендаций производительность сервера управления может заметно снизиться.

Примечание
Реальная производительность сервера управления зависит от профиля нагрузки. Например, в случае, когда виртуальные машины размещены в кластерах, включающих в себя большое количество серверов, производительность может быть значительно меньше, чем в случае, когда серверы не объединены в кластеры или кластеры содержат небольшое количество серверов.

Дополнительная настройка

Дополнительная настройка машины с ОС Linux

Для обеспечения высокой производительности сервера управления и СУБД параметрам, ограничивающим использование ресурсов ОС, необходимо назначить достаточно большие значения. Например, на машине с ОС CentOS 7 это можно сделать следующим образом:

1. В конфигурационный файл /etc/sysctl.conf добавьте следующие строки:

```
fs.file-max = 6553500
kernel.pid_max = 4194303
kernel.threads-max = 4194303
```

2. В конфигурационный файл /etc/security/limits.conf добавьте следующие строки:

```
* soft nproc 65535
* hard nproc 65535
```


© ООО Киберпротект, 2026

```
* soft nofile 65535
* hard nofile 65535
```

Примечание
Параметры, указанные в файлах в каталоге /etc/security/limits.d/, могут переопределять параметры, указанные в файле /etc/security/limits.conf.

3. Перезагрузите машину:

```
reboot
```

Дополнительная настройка машины с ОС Windows

- Количество портов, входящих в диапазон динамических портов для протокола TCP, должно быть в 1,5-2 раза больше общего количества агентов и виртуальных устройств, зарегистрированных в Кибер Бэкап.

  Текущий диапазон динамических портов можно просмотреть с помощью команды netsh int ipv4 show dynamicport tcp, например:

```
netsh int ipv4 show dynamicport tcp

Protocol tcp Dynamic Port Range
---------------------------------
Start Port      : 49152
Number of Ports : 16384
```

  Задать новый диапазон динамических портов можно с помощью команды netsh int ipv4 set dynamicport tcp start=<start_port> num=<number_of_ports>, где <start_port> задает начальный порт, а <number_of_ports> – количество портов.
- Антивирусное ПО может замедлять работу сервера управления. В таком случае нужно настроить антивирус.

Дополнительная настройка продукта Кибер Бэкап на машине с ОС Linux

Для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется увеличить лимиты на количество одновременно открытых файлов для служб сервера управления и изменить уровень детализации сообщений в журналах событий с DEBUG на INFO.

Например, если сервер управления установлен на машину с ОС CentOS 7, лимит на количество одновременно открытых файлов для службы acronis_asm и уровень детализации сообщений в журналах можно изменить следующим образом:

1. Узнайте путь к скрипту запуска службы acronis_asm, просмотрев ее unit-файл:

```
cat /etc/systemd/system/acronis_asm.service
<...>
```


© ООО Киберпротект, 2026

```
ExecStart=/usr/sbin/acronis_asm
<...>
```

2. Задайте новый лимит в скрипте запуска службы /usr/sbin/acronis_asm, заменив строку

```
ulimit -n 1024
```

на

```
ulimit -n 10240
```

и сохранив изменение.

3. Измените уровень детализации сообщений в файлах /usr/lib/Acronis/AccountServer/account_server.json и /usr/lib/Acronis/BackupManager/backup_manager.yml:

```
...
 chronica:
   level: "INFO"
...
```

4. Перезапустите службу:

```
systemctl restart acronis_asm
```

2.3.1.2 Сервер управления на машине с ОС Linux, использующий СУБД PostgreSQL

Требования к оборудованию

Машина для сервера управления

Для работы сервера управления необходимы следующие ресурсы:

- как минимум 6 ядер ЦП (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 12 ядер);
- как минимум 16 ГБ ОЗУ (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 32 ГБ);
- не менее 150 ГБ дискового пространства на SSD-диске (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется не менее 300 ГБ);
- подключение к сети, поддерживающее скорость передачи данных от 30 МБ/с (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 50 МБ/с).

Внимание
Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от версии и редакции используемой ОС Linux.

© ООО Киберпротект, 2026

Машина для PostgreSQL

Для работы СУБД PostgreSQL и размещения баз данных сервера управления необходимы следующие ресурсы:

- как минимум 4 ядра ЦП (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 8 ядер);
- как минимум 16 ГБ ОЗУ (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 32 ГБ);
- не менее 200 ГБ дискового пространства на SSD-диске (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется не менее 300 ГБ);
- подключение к сети, поддерживающее скорость передачи данных от 30 МБ/с (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 50 МБ/с).

Внимание
Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от версии и редакции используемой ОС Linux.

Рекомендуемая конфигурация продукта Кибер Бэкап

В продукте Кибер Бэкап, развернутом на оборудовании с описанными выше характеристиками, рекомендуется:

- Использовать не более 8 000 лицензий (для повышения производительности рекомендуется использовать одну корпоративную лицензию, в которую включены все необходимые агенты и виртуальные устройства).

  Для установок Кибер Бэкап с большим количеством контролируемых ресурсов рекомендуется добавлять лицензии до регистрации агентов и добавления устройств.
- Добавлять не более 20 000 почтовых ящиков или 8 000 других устройств (физических и виртуальных машин, баз данных и других ресурсов, отображаемых в веб-консоли Кибер Бэкап в разделе **Устройства**).

  Добавить до 60 000 почтовых ящиков или до 20 000 ВМ можно при соблюдении дополнительных условий (см. разделы "Резервное копирование больших объемов данных" (стр. 545) и "Предельное количество виртуальных машин для резервного копирования" (стр. 690)).
- Добавлять не более 50 виртуальных устройств (virtual appliance).
- Включать в общий план не более 100 устройств (общий план включает в себя отдельные устройства), для большего количества устройств используйте групповые планы.
- Включать в групповой план не более 500 устройств (групповой план включает в себя группы устройств).
- Создавать не более 500 общих и групповых планов.
- Выполнять не более 500 одновременных операций резервного копирования и восстановления.
- Создавать не более 500 отделов.

© ООО Киберпротект, 2026

- Использовать не более 10 уровней в иерархии отделов.
- Создавать в отделе не более 300 подотделов одного уровня.

Кроме того, общее количество записей в таблице resources БД службы учетных записей (Account Server) не должно превышать 100 000. Чем ближе общее количество записей к этой границе, тем ниже производительность сервера управления.

Внимание
При несоблюдении этих рекомендаций производительность сервера управления может заметно снизиться.

Примечание
Реальная производительность сервера управления зависит от профиля нагрузки. Например, в случае, когда виртуальные машины размещены в кластерах, включающих в себя большое количество серверов, производительность может быть значительно меньше, чем в случае, когда серверы не объединены в кластеры или кластеры содержат небольшое количество серверов.

Дополнительная настройка

Дополнительная настройка машин для сервера управления и СУБД PostgreSQL

Для обеспечения высокой производительности сервера управления и СУБД параметрам, ограничивающим использование ресурсов ОС, необходимо назначить достаточно большие значения. Например, на машине с ОС CentOS 7 это можно сделать следующим образом:

1. В конфигурационный файл /etc/sysctl.conf добавьте следующие строки:

```
fs.file-max = 6553500
kernel.pid_max = 4194303
kernel.threads-max = 4194303
```

2. В конфигурационный файл /etc/security/limits.conf добавьте следующие строки:

```
* soft nproc 65535
* hard nproc 65535
* soft nofile 65535
* hard nofile 65535
```

Примечание
Параметры, указанные в файлах в каталоге /etc/security/limits.d/, могут переопределять параметры, указанные в файле /etc/security/limits.conf.

3. Перезагрузите машину:

```
reboot
```


© ООО Киберпротект, 2026

Дополнительная настройка СУБД PostgreSQL

Для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется изменить ряд параметров в конфигурационном файле postgresql.conf:

```
<...>
max_connections = 600
shared_buffers = [4-8]GB [~20-25% от ОЗУ]
work_mem = 8MB
checkpoint_timeout = 20min
random_page_cost = 1.2
effective_cache_size = 16GB [~50% от ОЗУ]
autovacuum_vacuum_scale_factor = 0.05
autovacuum_analyze_scale_factor = 0.02
statement_timeout = 1800000
idle_session_timeout = 1800000
<...>
```

Примечание
Минимальное значение параметра max_connections – 200, рекомендуемое значение для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств – 600.

Подробнее о параметрах настройки СУБД см. в официальной документации PostgreSQL.

После изменения параметров необходимо перезагрузить PostgreSQL, например:

```
systemctl restart postgresql-15
```

Дополнительная настройка продукта Кибер Бэкап

Для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется увеличить лимиты на количество одновременно открытых файлов для служб сервера управления и изменить уровень детализации сообщений в журналах событий с DEBUG на INFO.

Например, если сервер управления установлен на машину с ОС CentOS 7, лимит на количество одновременно открытых файлов для службы acronis_asm и уровень детализации сообщений в журналах можно изменить следующим образом:

1. Узнайте путь к скрипту запуска службы acronis_asm, просмотрев ее unit-файл:

   ```
   cat /etc/systemd/system/acronis_asm.service
   <...>
   ExecStart=/usr/sbin/acronis_asm
   <...>
   ```

2. Задайте новый лимит в скрипте запуска службы /usr/sbin/acronis_asm, заменив строку

© ООО Киберпротект, 2026

```
ulimit -n 1024
```

на

```
ulimit -n 10240
```

и сохранив изменение.

3. Измените уровень детализации сообщений в файлах /usr/lib/Acronis/AccountServer/account_server.json и /usr/lib/Acronis/BackupManager/backup_manager.yml:

```
...
 chronica:
  level: "INFO"
...
```

4. Перезапустите службу:

```
systemctl restart acronis_asm
```

2.3.1.3 Сервер управления на машине с ОС Windows, использующий СУБД Microsoft SQL Server

Требования к оборудованию

Машина для сервера управления

Для работы сервера управления необходимы следующие ресурсы:

- как минимум 6 ядер ЦП (для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 8 ядер),
- 16 ГБ ОЗУ,
- не менее 150 ГБ дискового пространства.

Внимание
Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от версии и редакции используемой ОС Windows.

Машина для Microsoft SQL Server

Для работы СУБД Microsoft SQL Server и размещения баз данных сервера управления необходимы следующие ресурсы:

- 4 ядра ЦП,
- 16 ГБ ОЗУ,
- не менее 100 ГБ дискового пространства.

© ООО Киберпротект, 2026

Внимание
Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от версии и редакции используемой ОС Windows.

Рекомендуемая конфигурация продукта Кибер Бэкап

В продукте Кибер Бэкап, развернутом на оборудовании с описанными выше характеристиками, рекомендуется:

- Использовать не более 8 000 лицензий (для повышения производительности рекомендуется использовать одну корпоративную лицензию, в которую включены все необходимые агенты и виртуальные устройства).

  Для установок Кибер Бэкап с большим количеством контролируемых ресурсов рекомендуется добавлять лицензии до регистрации агентов и добавления устройств.
- Добавлять не более 8 000 устройств (физических и виртуальных машин, почтовых ящиков, баз данных и других ресурсов, отображаемых в веб-консоли Кибер Бэкап в разделе **Устройства**).
- Добавлять не более 50 виртуальных устройств (virtual appliance).
- Включать в общий план не более 100 устройств (общий план включает в себя отдельные устройства).
- Включать в групповой план не более 500 устройств (групповой план включает в себя группы устройств).
- Создавать не более 500 общих и групповых планов.
- Выполнять не более 500 одновременных операций резервного копирования и восстановления.
- Создавать не более 500 отделов.
- Использовать не более 10 уровней в иерархии отделов.
- Создавать в отделе не более 300 подотделов одного уровня.

Кроме того, общее количество записей в таблице resources БД службы учетных записей (Account Server) не должно превышать 60 000. Чем ближе общее количество записей к этой границе, тем ниже производительность сервера управления.

Внимание
При несоблюдении этих рекомендаций производительность сервера управления может заметно снизиться.

Примечание
Реальная производительность сервера управления зависит от профиля нагрузки. Например, в случае, когда виртуальные машины размещены в кластерах, включающих в себя большое количество серверов, производительность может быть значительно меньше, чем в случае, когда серверы не объединены в кластеры или кластеры содержат небольшое количество серверов.

© ООО Киберпротект, 2026

Дополнительная настройка

Дополнительная настройка машины для сервера управления

- Количество портов, входящих в диапазон динамических портов для протокола TCP, должно быть в 1,5-2 раза больше общего количества агентов и виртуальных устройств, зарегистрированных в Кибер Бэкап.

  Текущий диапазон динамических портов можно просмотреть с помощью команды netsh int ipv4 show dynamicport tcp, например:

  ```
  netsh int ipv4 show dynamicport tcp

  Protocol tcp Dynamic Port Range
  ---------------------------------
  Start Port      : 49152
  Number of Ports : 16384
  ```

  Задать новый диапазон динамических портов можно с помощью команды netsh int ipv4 set dynamicport tcp start=<start_port> num=<number_of_ports>, где <start_port> задает начальный порт, а <number_of_ports> – количество портов.
- Антивирусное ПО может замедлять работу сервера управления. В таком случае нужно настроить антивирус.

2.4 Поддержка файловых систем

Агент защиты может создать резервную копию любой файловой системы, доступной из операционной системы, в которой установлен агент. Например, агент для Windows может выполнить резервное копирование и восстановление файловой системы ext4, если соответствующий драйвер установлен в Windows.

В следующей таблице представлена сводная информация о файловых системах, в отношении которых можно выполнять резервное копирование и восстановление. Ограничения применяются как к агентам, так и к загрузочным носителям.

Файловая система	Поддержка			Ограничения
	Агенты	Загрузочный носитель WinPE	Загрузочные носители на основе Linux	
FAT16/32	Все агенты	+	+	Без ограничений
NTFS		+	+	
ext2/ext3/ext4		+	+	

© ООО Киберпротект, 2026

JFS	Агент для Linux	-	+	• Файлы невозможно исключить из резервной копии диска • Невозможно включить быстрое инкрементное/дифференциальное резервное копирование
ReiserFS3		-	+	
ReiserFS4		-	+	• Файлы невозможно исключить из резервной копии диска • Невозможно включить быстрое инкрементное/дифференциальное резервное копирование • Невозможно изменить размер томов при выполнении восстановления
ReFS	Все агенты	+	+	
XFS		+	+	• Файлы невозможно исключить из резервной копии диска • Невозможно включить быстрое инкрементное/дифференциальное резервное копирование • Невозможно изменить размер томов при выполнении восстановления • Восстановление файлов с резервной копии, которая хранится на ленточном накопителе, не поддерживается
Linux SWAP	Агент	-	+	Без ограничений

© ООО Киберпротект, 2026

	для Linux			
exFAT	Все агенты	+	+ Если резервная *копия хранится в* файловой системе exFAT, загрузочный носитель невозможно использовать для восстановления.	• Поддерживается только резервное копирование дисков/томов • Файлы невозможно исключить из резервной копии • Отдельные файлы невозможно восстановить из резервной копии • Невозможно изменить размер томов при выполнении восстановления

Программное обеспечение автоматически перейдет к посекторному резервному копированию для дисков с нераспознанными или неподдерживаемыми файловыми системами. Посекторное резервное копирование возможно для любой файловой системы, которая:

- основана на блоках;
- занимает один диск;
- имеет стандартную схему разделов MBR/GPT.

Если файловая система не соответствует этим требованиям, процесс резервного копирования завершится сбоем.

2.4.0.1 Дедупликация данных

ОС Windows Server 2012 R2 и более поздних версий позволяет включить функцию дедупликации данных для тома NTFS. Дедупликация данных дает возможность уменьшить объем используемого пространства тома путем однократного сохранения повторяющихся фрагментов файлов на томе.

Предусмотрена возможность создавать резервные копии и восстанавливать тома с включенной дедупликацией данных на уровне диска без каких-либо ограничений. Поддерживается резервное копирование на уровне файлов (за исключением использования поставщика VSS). Для восстановления файлов с резервной копии диска запустите виртуальную машину с резервной копии или подключите резервную копию на машине под управлением Windows Server 2012 R2 или более поздней версии и скопируйте файлы с подключенного тома.

Функциональные средства дедупликации данных Windows Server не имеют никакого отношения к функциональным средствам дедупликации Кибер Бэкапа.

© ООО Киберпротект, 2026

2.5 Настройки прокси-сервера

Агенты защиты могут передавать данные через прокси-сервер HTTP/HTTPS. Сервер должен функционировать через HTTP-тоннель без сканирования или изменения трафика HTTP. Промежуточные прокси-серверы не поддерживаются.

2.5.1 В Windows

Если прокси-сервер настроен в Windows (**Панель управления** > **Свойства браузера** > **Подключения**), то программа установки считает настройки прокси-сервера из реестра и использует их автоматически. Кроме того, можно задать настройки прокси-сервера во время установки (см. "Установка агентов" (стр. 95)) или указать их заранее, используя процедуру, описанную ниже. С помощью той же процедуры эти параметры можно изменить после установки.

Указание параметров прокси-сервера в Windows

1. Создайте новый текстовый документ и откройте его в текстовом редакторе, например Notepad.
2. Скопируйте и вставьте в этот файл следующие строки:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Замените proxy.company.com именем хоста или IP-адресом прокси-сервера, а 000001bb – шестнадцатеричным значением номера порта. Например, 000001bb соответствует номеру порта 443.
4. Если на прокси-сервере необходимо пройти аутентификацию, вместо строк proxy_login и proxy_password укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.
5. Сохраните документ с именем **proxy.reg**.
6. Запустите файл от имени администратора.
7. Подтвердите изменение реестра Windows.
8. Если агент защиты еще не установлен, то можно установить его сейчас. В противном случае можно перезапустить агент (см. п. 14).
9. Откройте файл **%programdata%\Acronis\Agent\etc\aakore.yaml** в текстовом редакторе.
10. Найдите раздел **env** или создайте его и добавьте следующие строки:

© ООО Киберпротект, 2026

```
env:
http-proxy: proxy_login:proxy_password@proxy_address:port
https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. Замените proxy_login и proxy_password учетными данными прокси-сервера, а proxy_address:port - адресом и номером порта прокси-сервера.
12. В меню **Пуск** нажмите **Выполнить**, введите: **cmd** и нажмите **OK**.
13. Перезапустите службу aakore, используя следующие команды:

```
net stop aakore
net start aakore
```

14. Перезапустите агент, используя следующие команды:

```
net stop mms
net start mms
```

2.5.2 В ОС Linux

Запустите файл установки с параметрами --http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN--http-proxy-password=PASSWORD. Чтобы изменить параметры прокси-сервера после установки, используйте описанную ниже процедуру.

Именение параметров прокси-сервера в Linux

1. Откройте файл **/etc/Acronis/Global.config** в текстовом редакторе.
2. Выполните одно из следующих действий:
   - Если параметры прокси-сервера были заданы во время установки агента, найдите следующий раздел:

     ```
     <key name="HttpProxy">
       <value name="Enabled" type="Tdword">"1"</value>
       <value name="Host" type="TString">"ADDRESS"</value>
       <value name="Port" type="Tdword">"PORT"</value>
       <value name="Login" type="TString">"LOGIN"</value>
       <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - В противном случае скопируйте приведенные выше строки и вставьте в файл между тегами <registry name="Global">...</registry>.
3. Замените АДРЕС новым именем хоста или IP-адресом прокси-сервера, а ПОРТ — номером порта в десятичном формате.
4. Если на прокси-сервере необходимо пройти аутентификацию, вместо дескрипторов ИМЯ ВХОДА и ПАРОЛЬ укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.
5. Сохраните файл.

© ООО Киберпротект, 2026

6. Откройте файл **/opt/acronis/etc/aakore.yaml** в текстовом редакторе.
7. Найдите раздел **env** или создайте его и добавьте следующие строки:

```
env:
http-proxy: proxy_login:proxy_password@proxy_address:port
https-proxy: proxy_login:proxy_password@proxy_address:port
```

8. Замените proxy_login и proxy_password учетными данными прокси-сервера, а proxy_address:port - адресом и номером порта прокси-сервера.
9. Перезапустите службу aakore, используя следующую команду:

```
sudo service aakore restart
```

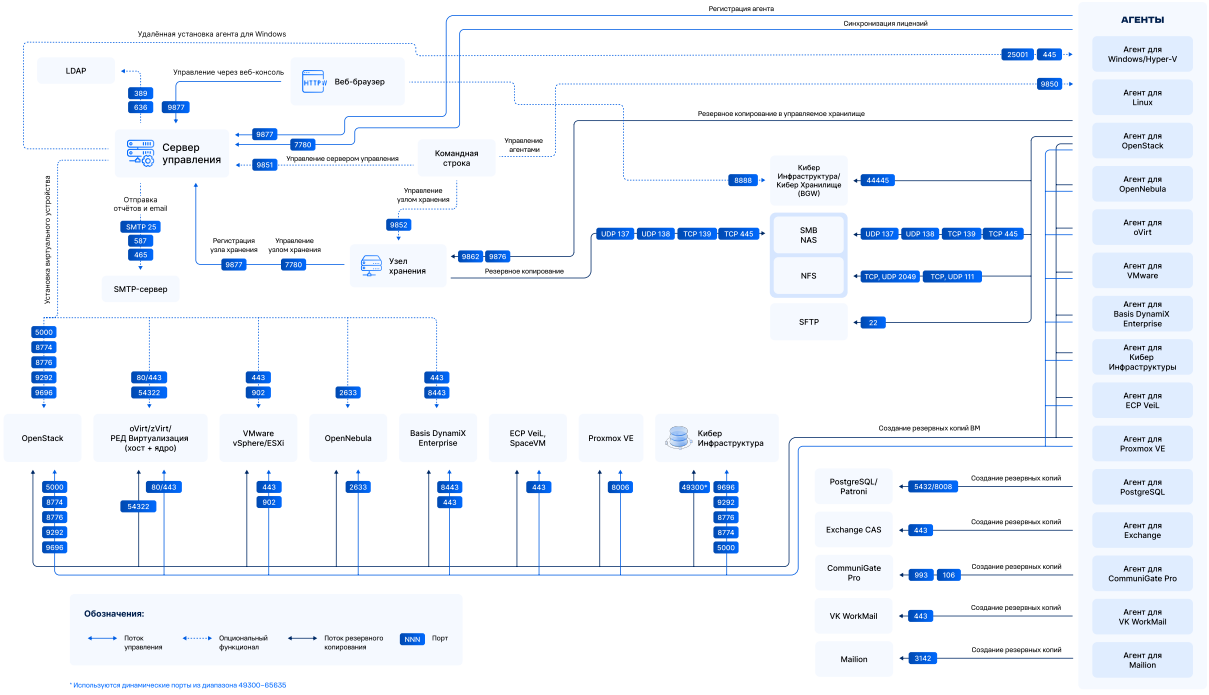
10. Перезапустите агент, выполнив следующую команду в любом каталоге:

```
sudo service acronis_mms restart
```

2.6 Развертывание Кибер Бэкап

Развертывание Кибер Бэкап включает в себя установку ряда программных компонентов, которые описаны в разделе Компоненты.

На схеме ниже показано взаимодействие основных компонентов продукта.



Описание подключений по указанным портам приведено в Базе знаний.

© ООО Киберпротект, 2026

2.6.1 Установка сервера управления

2.6.1.1 Установка в ОС Windows

Установка сервера управления

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.
4. Не меняйте настройку по умолчанию **Установите агент защиты и сервер управления**.
5. Выполните любое из следующих действий:
   - Нажмите **Установить**.

     Это самый легкий способ установить продукт. Для большинства параметров установки будут использоваться значения по умолчанию.

     По умолчанию устанавливаются следующие компоненты:
     - Сервер управления
     - Компоненты для удаленной установки
     - Агент для Windows
     - Другие агенты (агент для Hyper-V, агент для Exchange, агент для SQL и агент для Active Directory), если на машине обнаружен соответствующий гипервизор или приложение
     - Мастер создания загрузочных носителей
     - Программа командной строки
     - Мониторинг Защиты Данных
   - Щелкните **Настройка параметров установки**, чтобы настроить программу установки.

     Можно будет выбрать компоненты для установки и указать дополнительные параметры. Дополнительную информацию см. в разделе «Настройка параметров установки».
   - Щелкните **Создать MST- и MSI-файлы для автоматической установки**, чтобы извлечь пакеты установки. Проверьте и при необходимости измените настройки установки, которые будут добавлены в MST-файл, затем нажмите кнопку **Создать**. Для этой процедуры не требуется никаких дополнительных шагов.

     Чтобы развернуть агенты через групповую политику, см. раздел «Развертывание агентов с использованием групповой политики».
6. Приступите к установке.
7. После завершения установки нажмите кнопку **Закрыть**.

Настройка параметров установки в ОС Windows

В этом разделе описаны настройки, которые можно изменить при установке.

© ООО Киберпротект, 2026

Общие параметры

- Устанавливаемые компоненты

Компонент	Описание
Сервер управления	Сервер управления – это центр управления всеми резервными копиями.
Агент для Windows	Этот агент создает резервную копию дисков, томов и файлов. Он устанавливается на машинах Windows. Он устанавливается в любом случае (не подлежит выбору).
Агент для Hyper-V	Этот агент создает резервную копию виртуальных машин Hyper-V. Он устанавливается на хостах Hyper-V. Если этот компонент выбран, и на машине обнаружена роль Hyper-V, он будет установлен.
Агент для SQL	Этот агент создает резервную копию баз данных SQL Server. Он устанавливается на машинах с Microsoft SQL Server. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для Exchange	Этот агент создает резервную копию баз данных и почтовых ящиков Exchange. Он устанавливается на машинах с ролью почтового ящика Microsoft Exchange Server. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для Active Directory	Этот агент создает резервную копию данных доменных служб Active Directory. Он устанавливается на контроллерах домена. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для VMware (Windows)	Этот агент создает резервную копию виртуальных машин VMware. Он устанавливается на виртуальных машинах Windows с сетевым доступом к vCenter Server. Если этот компонент выбран, он будет установлен.
Агент для Oracle	Этот агент создает резервную копию баз данных Oracle. Он устанавливается на машинах с Oracle Database. Если этот компонент выбран, он будет установлен.
Агент для PostgreSQL	Этот агент создает резервную копию баз данных PostgreSQL. Если этот компонент выбран, он будет установлен.
Узел хранения	Этот компонент используется для организации управляемых хранилищ и дедупликации резервных копий. Он устанавливается на машину с агентом для Windows.
Мониторинг Защиты Данных	Этот компонент позволяет пользователю отслеживать выполнение запущенных заданий в области уведомлений, приостанавливать

© ООО Киберпротект, 2026

	запуск планов защиты, устанавливать особые пароли для резервных копий машины. Он устанавливается на машинах Windows. Если этот компонент выбран, он будет установлен.
Программа командной строки	Кибер Бэкап поддерживает интерфейс командной строки с утилитой acrocmd. acrocmd не содержит никаких инструментов, которые физически выполняют команды. Она просто обеспечивает интерфейс командной строки для компонентов Кибер Бэкап – агентов и сервера управления. Если этот компонент выбран, он будет установлен.

- Папка, в которую будет установлен продукт.
- Учетная запись, с использованием которой будут запускаться службы.

  Можно выбрать один из следующих вариантов:
  - **Использовать учетные записи пользователя службы** (по умолчанию для службы агента)

    Учетные записи пользователя услуги – это системные учетные записи Windows, которые используются для запуска служб. Преимущество этой настройки состоит в том, что политики безопасности домена не влияют на права пользователей этих учетных записей. По умолчанию агент запускается в учетной записи **Локальная система**.
  - **Создать учетную запись** (по умолчанию для службы сервера управления и службы узла хранения)

    Учетные записи будут иметь имена **Киберпротект Agent User**, **CMS User** и **CSN User** для агента, сервера управления и служб узла хранения соответственно.
  - **Использовать следующую учетную запись**

    При установке продукта на контроллер домена программа установки предложит указать существующие учетные записи (или ту же учетную запись) для каждой службы. В целях безопасности программа установки не может автоматически создавать учетные записи на контроллере домена.

    Эта настройка также позволяет использовать на сервере управления существующий сервер Microsoft SQL, установленный на другой машине, а также проверку подлинности Windows для SQL Server.

  При выборе параметра **Создать учетную запись** или **Использовать следующую учетную запись** убедитесь, что политики безопасности домена не повлияют на права соответствующих учетных записей. Если права пользователя не были заданы для учетной записи при установке, данный компонент может работать неправильно или вообще не работать.

Права, требуемые для учетной записи входа

На машине Windows агент запускается как Managed Machine Service (MMS). Для надлежащей работы агента учетная запись, под которой запускается агент, должна иметь специальные права. Поэтому пользователю MMS необходимо назначить следующие права:

1. Учетная запись должна входить в группы **Операторы архива** и **Администраторы**. На контроллере домена пользователь должен входить в группу **Администраторы домена**.

© ООО Киберпротект, 2026

2. Предоставляется разрешение **Полный доступ** в отношении папки %PROGRAMDATA%\Acronis и ее подпапок.
3. Разрешение **Полный доступ** в отношении определенных разделов реестра в следующем разделе: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis.
4. Назначены следующие права пользователя:
   - Вход в качестве службы
   - Настройка квот памяти для процесса
   - Замена маркера уровня процесса
   - Изменение параметров среды оборудования

Пользователь узла хранения должен иметь права локального администратора на машине с установленным узлом хранения Киберпротект.

Назначение прав пользователя

Ниже описаны инструкции по назначению прав пользователя (в этом примере используется право пользователя **Вход в качестве службы**, однако все действия идентичны и для других прав пользователя):

1. Войдите на компьютер с учетной записью с правами администратора.
2. В разделе **Панель управления** откройте **Администрирование** (или щелкните Win+R, введите **control admintools** и нажмите клавишу "ВВОД"), затем откройте **Локальная политика безопасности**.
3. Разверните **Локальные политики** и щелкните **Назначение прав пользователя**.
4. В правой панели щелкните правой кнопкой мыши **Вход в качестве службы** и выберите **Свойства**.
5. Чтобы добавить нового пользователя, нажмите кнопку **Добавление пользователя или группы...**.
6. В окне **выбора пользователей, компьютеров, учетных записей служб или групп** найдите пользователя, которого необходимо ввести, и щелкните **OK**.
7. Чтобы сохранить изменения, щелкните **OK** в разделе "Свойства" (**Вход в качестве службы**).

Внимание
Убедитесь, что пользователь, добавленный в правило **Вход в качестве службы**, не указан в политике **Отказать во входе в качестве службы** в разделе **Локальная политика безопасности**.

Обратите внимание, что не рекомендуется вручную менять учетные записи входа после окончания установки.

Установка сервера управления

- База данных, которая должна использоваться сервером управления. По умолчанию используется встроенная база данных SQLite.
  Можно выбрать любую из указанных ниже версий Microsoft SQL Server:

© ООО Киберпротект, 2026

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017 (в Windows)
- Microsoft SQL Server 2019 (в Windows)

Выбранный экземпляр может использоваться и другими программами.

Если для экземпляра используется имя по умолчанию – **MSSQLSERVER** – необходимо указать только имя машины, на которой расположен этот экземпляр. Если используется настраиваемое имя экземпляра, необходимо указать имя машины и имя экземпляра.

Перед выбором установленного на другой машине экземпляра убедитесь, что на этой машине включены служба обозревателя SQL Server и протокол TCP/IP. Инструкции по запуску службы браузера SQL Server см. на странице http://msdn.microsoft.com/en-us/library/ms189093.aspx. Включить протокол TCP/IP можно с помощью аналогичной процедуры.

- База данных, которая должна использоваться службой сканирования. Служба сканирования может использовать ту же базу данных Microsoft SQL Server, которая указана для сервера управления, или отдельную базу данных PostrgeSQL Server. Службу сканирования невозможно использовать со встроенной базой данных SQLite.
- Порт, который будет использоваться веб-браузером для доступа к серверу управления (по умолчанию 9877) и порт, который будет использоваться для связи между компонентами продукта (по умолчанию 7780). Изменение последнего порта после установки потребует перерегистрации всех компонентов.

  Брандмауэр Windows настраивается автоматически при установке. Если используется другой брандмауэр, убедитесь, что порты открыты как для входящих, так и для исходящих запросов, проходящих через этот брандмауэр.

2.6.1.2 Установка в Linux

Подготовка

1. В системе, в которой не используется диспетчер пакетов RPM, необходимо установить этот диспетчер вручную. Как привилегированный пользователь выполните команду (например):

   ```
   apt-get install rpm
   ```

2. Убедитесь в том, что на машине установлены необходимые пакеты Linux.
3. Дайте разрешение на исполнение установочному файлу. Выполните следующую команду:

   ```
   chmod +x CyberBackup_*
   ```


© ООО Киберпротект, 2026

Подготовка к установке в ОС Astra Linux SE

Перед установкой продукта в ОС Astra Linux SE ознакомьтесь с разделом "Совместимость с ОС Astra Linux SE" (стр. 42) и выполните следующие шаги. Предполагается, что включен режим замкнутой программной среды.

1. Распакуйте дистрибутив:

   ```
   tar --xattrs --xattrs-include=* -xvf CyberBackup_18_64-bit.x86_64.tar
   ```

2. Запустите файл установки с правами привилегированного пользователя:

   ```
   ./CyberBackup_18_64-bit.x86_64
   ```

3. Обновите образы initramfs:

   ```
   update-initramfs -u -k all
   ```

4. Перезагрузите систему.

Подготовка СУБД PostgreSQL/Patroni

Если планируется использовать СУБД PostgreSQL или кластерную конфигурацию Patroni для сервера управления, выполните следующие шаги:

1. Установите PostgreSQL на машину, предназначенную для сервера управления, либо на отдельную машину. Для установки можно использовать:
   - PostgreSQL или Postgres Pro версии 14, 15, 16, 17, 18;
   - Platform V Pangolin SE 6.1.7;
   - СУБД Jatoba 5;
   - СУБД Tantor 14–17.

   Пример установки PostgreSQL 15 в ОС CentOS 7:

   ```
   yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
   yum install -y postgresql15-server
   /usr/pgsql-15/bin/postgresql-15-setup initdb
   systemctl enable postgresql-15
   systemctl start postgresql-15
   ```

2. На машину с PostgreSQL установите пакет postgresql-contrib, например:

   ```
   yum -y install postgresql15-contrib
   ```

   Версия пакета должна соответствовать версии PostgreSQL.
3. При установке сервера управления необходимо будет указать учетные данные пользователя с привилегиями LOGIN и SUPERUSER. От его имени будет настроена СУБД PostgreSQL. Если

© ООО Киберпротект, 2026

такой пользователь есть, можно использовать его учетные данные. Если такого пользователя нет, зайдите на машину с PostgreSQL от имени администратора и создайте его. Например:

```
sudo -u postgres psql -c "CREATE ROLE cyberbackup WITH LOGIN SUPERUSER
PASSWORD '69c64fee29d24024b219578ecd9f5d88';"
```

Для подключения сервера управления к PostgreSQL в процессе установки будет автоматически создан пользователь cyberprotect.

4. Измените конфигурационный файл postgresql.conf так, как показано в примерах ниже.
   - PostgreSQL и сервер управления на одной машине.

     ```
     <...>
     listen_addresses = '127.0.0.1'
     max_connections = 600
     password_encryption = scram-sha-256
     <...>
     ```

   - PostgreSQL и сервер управления на разных машинах.

     ```
     <...>
     listen_addresses = '10.10.10.10'
     max_connections = 600
     password_encryption = scram-sha-256
     <...>
     ```

     В этом примере 10.10.10.10 – это IP-адрес машины с PostgreSQL.

   Примечание
   - Минимальное значение параметра max_connections – 200, рекомендуемое значение для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств – 600.
   - Подробные сведения о возможных значениях параметра listen_addresses см. в документации установленной версии PostgreSQL.

   После внесения изменений перезагрузите PostgreSQL. Например:

   ```
   systemctl restart postgresql-15
   ```

5. Настройте аутентификацию в PostgreSQL для сервера управления.
   a. На машине с PostgreSQL измените файл pg_hba.conf так, как показано в примерах.
      - PostgreSQL и сервер управления на одной машине.

        ```
        # TYPE  DATABASE      USER          ADDRESS              METHOD
        # "local" is for Unix domain socket connections only
        local   all           all                              peer
        # Cyber Backup connections
        host    all           cyberbackup     127.0.0.1/32     scram-sha-256
        host    all           cyberprotect    127.0.0.1/32     scram-sha-256
        <...>
        ```


© ООО Киберпротект, 2026

В этом примере cyberbackup – пользователь, с помощью привилегий которого СУБД PostgreSQL будет настроена при установке, а cyberprotect – пользователь, от имени которого сервер управления будет подключаться к PostgreSQL.

- PostgreSQL и сервер управления на разных машинах.

```
# TYPE  DATABASE      USER          ADDRESS              METHOD
# "local" is for Unix domain socket connections only
local   all           all                                peer
# Cyber Backup connections
host    all           cyberbackup     10.10.10.11/32     scram-sha-256
host    all           cyberprotect    10.10.10.11/32     scram-sha-256
<...>
```

В этом примере cyberbackup – пользователь, с помощью привилегий которого СУБД PostgreSQL будет настроена при установке, а cyberprotect – пользователь, от имени которого сервер управления будет подключаться к PostgreSQL. Кроме того, 10.10.10.11 – IP-адрес машины, предназначенной для сервера управления.

Примечание

- Сервер управления не поддерживает локальные подключения к базам данных PostgreSQL через доменные сокеты Unix (тип подключения local в pg_hba.conf).
- Сервер управления поддерживает подключения к базам данных PostgreSQL только по протоколу IPv4.
- Кроме метода аутентификации scram-sha-256, сервер управления также поддерживает методы аутентификации md5 и trust.

b. Примените изменения. Например:

```
systemctl reload postgresql-15
```

6. В случае размещения PostgreSQL и сервера управления на разных машинах:
   - брандмауэр должен разрешать подключения с машины, предназначенной для сервера управления, к машине с PostgreSQL через TCP-порт, используемый PostgreSQL (5432 по умолчанию);
   - время на машинах должно быть синхронизировано.

   Предупреждение
   Не переводите системное время вперед и обратно при работе Кибер Бэкап.

7. Убедитесь, что с машины, предназначенной для сервера управления, можно подключаться к PostgreSQL с учетными данными созданного ранее пользователя.
   - PostgreSQL и сервер управления на одной машине.

```
[root@cb-mn-srv ~]# psql -h 127.0.0.1 -U cyberbackup -d postgres
Пароль пользователя cyberbackup:
psql (15.0)
```


© ООО Киберпротект, 2026

```
Введите "help", чтобы получить справку.

postgres=#
```

- PostgreSQL и сервер управления на разных машинах.

```
[root@cb-mn-srv ~]# psql -h 10.10.10.10 -U cyberbackup -d postgres
Пароль пользователя cyberbackup:
psql (15.0)
Введите "help", чтобы получить справку.

postgres=#
```

Для использования кластерной конфигурации Patroni произведите аналогичную настройку машин PostgreSQL и обратитесь к официальной документации Patroni для настройки кластера. Для установки можно использовать Patroni версии 3.0 – 3.2.1.

Установка

Для установки сервера управления необходимо как минимум 4 ГБ свободного места на диске.

Установка сервера управления

1. Запустите файл установки (файл .i686 или .x86_64) как привилегированный пользователь:

   ```
   ./CyberBackup_18_64-bit.x86_64
   ```

2. Примите условия лицензионного соглашения.
3. [Необязательно] Выберите компоненты, которые требуется установить.

   По умолчанию устанавливаются следующие компоненты:

   - Сервер управления
   - Агент для Linux
   - Мастер создания загрузочных носителей
4. Выберите систему управления базами данных (СУБД) для сервера управления – SQLite или PostgreSQL/Patroni. По умолчанию выбрана встроенная СУБД SQLite.

   Внимание
   СУБД PostgreSQL/Patroni должна быть подготовлена до установки сервера управления по приведенной выше инструкции.

5. [Для СУБД PostgreSQL/Patroni] Укажите сведения для подключения и аутентификации:
   - **Хост** – IPv4-адрес или DNS-имя машины с PostgreSQL/балансировщиком нагрузки кластера Patroni. По умолчанию установлено значение localhost.
   - **Порт** – порт для подключения к PostgreSQL/Patroni. По умолчанию установлено значение 5432.

© ООО Киберпротект, 2026

- **Пользователь** и **Пароль** – имя и пароль пользователя для подключения к PostgreSQL/Patroni. Необходимо указать учетные данные пользователя, который был создан при подготовке СУБД. По умолчанию указан пользователь postgres.

6. Укажите порт, который будет использоваться в веб-браузере для доступа к серверу управления. Значение по умолчанию составляет 9877.
7. Укажите порт, который будет использоваться для обмена данными между компонентами продукта. По умолчанию установлено значение 7780.
8. Нажмите кнопку **Далее**, чтобы продолжить установку.

Примечание
Мастер установки может потребовать пакет openjdk-8-jre-headless. Устанавливать его не нужно.

9. По окончании установки выберите **Открыть веб-консоль**, затем нажмите кнопку **Выход**. Веб-консоль Кибер Бэкап откроется в веб-браузере по умолчанию.

2.6.2 Настройка отказоустойчивого кластера

В этом разделе приведены описание типовой архитектуры и пример настройки двухузлового отказоустойчивого кластера для программного обеспечения резервного копирования и восстановления данных Кибер Бэкап в операционной системе Ред ОС 7.3 Муром. В качестве программного обеспечения для поддержания целостности кластера и выполнения сигнальных функций используется Corosync, а для управления ресурсами кластера – Pacemaker.

В разделе описываются общие принципы настройки кластера Pacemaker/Corosync, перечень и рекомендуемые настройки ресурсов кластера для Кибер Бэкап, пример настройки типового двухузлового кластера на физических серверах с выделенной виртуальной машиной-свидетелем.

Подход, используемый в данном разделе, может быть применен как при построении кластеров высокой доступности, расположенных целиком на одной площадке, так и при построении катастрофоустойчивых кластеров, распределенных по нескольким центрам обработки данных.

Данный раздел не является руководством по программному обеспечению Pacemaker/Corosync и не заменяет техническую документацию по указанным продуктам.

2.6.2.1 Архитектура

Компоненты кластера

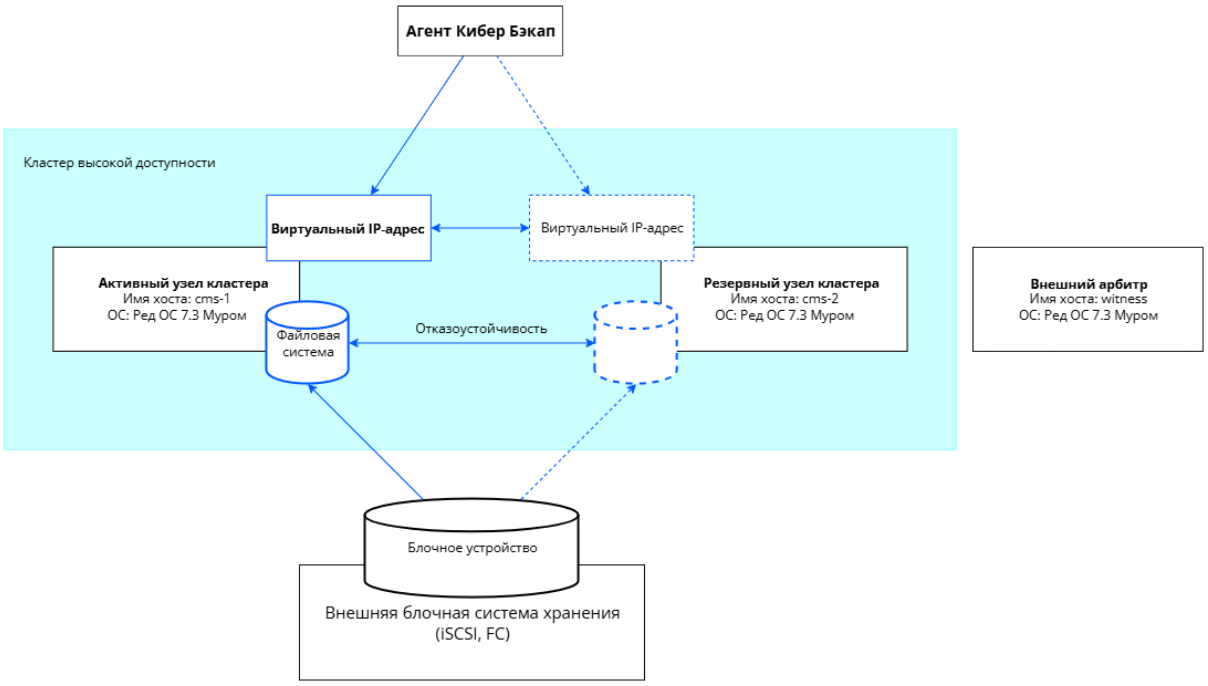
В разделе рассмотрен способ кластеризации Кибер Бэкап, включающий задействование следующих компонентов:

- Два аппаратных сервера с выделенными IPMI-интерфейсами;
- Внешняя блочная система хранения, доступная по протоколу iSCSI;
- Выделенный сервер, предпочтительно виртуализованный для кворумного устройства (так называемый "свидетель" или "арбитр").

© ООО Киберпротект, 2026

Кластер Кибер Бэкап является классическим отказоустойчивым кластером с общими разделяемыми дисками и виртуальным IP-адресом сервиса. Целостность кластера обеспечивается механизмами Stonith с использованием функционала IPMI и защитой от split brain при помощи внешнего арбитра.

Схема компонентов кластера:



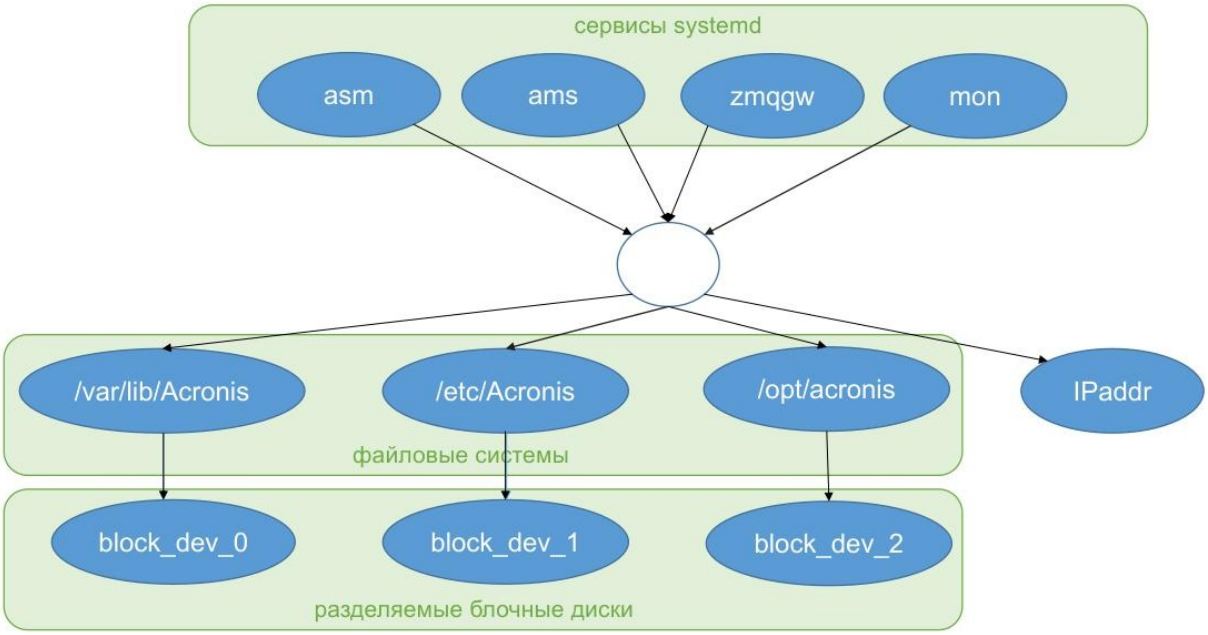
Ресурсы кластера

Для функционирования кластера необходимо настроить следующие типы кластерных ресурсов:

- Разделяемые блочные дисковые устройства;
- Перемещаемые файловые системы;
- Перемещаемый (виртуальный) IP-адрес, также называемый vIP (Virtual IP);
- Службы Кибер Бэкап;
- IPMI-ресурсы.

Дерево зависимостей ресурсов кластера изображено на следующем рисунке.

© ООО Киберпротект, 2026



2.6.2.2 Развертывание и настройка

Настройка сети

Требования к организации сети

Узлам кластера, IPMI-интерфейсам и внешнему арбитру должны быть назначены статические адреса IPv4. Адреса узлов кластера и перемещаемый IP-адрес должны находиться в одном сегменте сети. Адреса внешнего арбитра и IPMI-интерфейсов могут находиться в отдельных сегментах сети, доступных с использованием сетевой маршрутизации, но также должна быть обеспечена сетевая связность со стороны узлов кластера.

Тип	ОС	Имя хоста	IP-адрес	IPMI-интерфейс	Виртуальный IP-адрес	Описание
Узел кластера	РЕД ОС 7.3.3 x64	cms-1	10.77.44.58/22	10.77.0.58/22	10.77.44.57/22	Первый узел кластера для сервера управления Кибер Бэкап. Вариант установки: "сервер минимальный".
	РЕД ОС 7.3.3 x64	cms-2	10.77.44.59/22	10.77.0.59/22		Второй узел кластера для сервера управления Кибер Бэкап. Вариант

© ООО Киберпротект, 2026

						установки: "сервер минимальный".
Арбитр	РЕД ОС 7.3.3 x64	witness	10.77.44.61/22	–	–	Арбитр с кворумным устройством для предотвращения split brain. Вариант установки: "сервер минимальный". Допустимо использование виртуальной машины.

Настройка сетевых интерфейсов

На всех узлах кластера и арбитре настройте статические сетевые адреса, шлюз по умолчанию и адреса серверов имен (файл /etc/sysconfig/network-scripts/ifcfg-ens3):

```
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
NAME=ens3
DEVICE=ens3
ONBOOT=yes
IPADDR=10.77.44.58
PREFIX=22
GATEWAY=10.77.44.1
DNS1=10.77.29.101
DNS2=10.77.29.10
```

В файл /etc/hosts на узлах кластера и арбитре добавьте записи с остальными компонентами кластера, чтобы целостность кластера не зависела от стабильности работы внешних DNS-серверов:

```
10.77.44.57 cms    # Virtual (floating) cluster IP address
10.77.44.58 cms-1  # Node 1 static address
10.77.44.59 cms-2  # Node 2 static address
10.77.44.61 witness # Cluster witness with quorum device
```

Перезагрузите серверы и проверьте:

- Наличие статических адресов на интерфейсах;
- Наличие маршрута по умолчанию;
- Сетевую связность между всеми компонентами кластера.

© ООО Киберпротект, 2026

```
[root@cms-1 network-scripts]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 56:6f:93:3c:00:64 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.77.44.58/22 brd 10.77.47.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::546f:93ff:fe3c:64/64 scope link
       valid_lft forever preferred_lft forever

[root@cms-1 ~]# ip route
default via 10.77.44.1 dev ens3 proto static metric 100
10.77.44.0/22 dev ens3 proto kernel scope link src 10.77.44.58 metric 100
```

Подготовка узлов кластера

Установка кластерного программного обеспечения

Установите программное обеспечение для кластера, используя следующую таблицу.

Тип	Имя хоста	Команды
Узел кластера	cms-1	# dnf update # dnf install pcs pacemaker corosync corosync-qdevice lsyncd # dnf install iscsi-initiator-utils
Узел кластера	cms-2	# dnf update # dnf install pcs pacemaker corosync corosync-qdevice lsyncd # dnf install iscsi-initiator-utils
Арбитр	witness	# dnf update # dnf install pcs corosync-qnetd

Отключение SELinux

Для отключения SELinux на узлах кластера и арбитре выполните следующую команду:

```
setenforce 0
```

В конфигурационном файле /etc/selinux/config измените значение **enforcing** на **disabled**:

© ООО Киберпротект, 2026

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Настройка доступа по SSH-ключам

Для root настройте доступ между узлами кластера по SSH-ключам:

```
[root@cms-1 ~]# ssh-copy-id root@cms-2

[root@cms-2 ~]# ssh-copy-id root@cms-1
```

Настройка lsyncd

На первом узле кластера (cms-1) создайте конфигурационные файлы для автоматической двунаправленной синхронизации следующих системных файлов:

- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/security/acronisagent.conf

Конфигурационный файл lsyncd (/etc/lsyncd.conf):

```
settings {
    logfile = "/var/log/lsyncd.log"
}

sync {
    default.rsyncssh,
    source = "/etc",
    host = "cms-2",
    targetdir = "/etc",
    delete = 'false',
    rsync = {
        update = "true",
        whole_file = "true",
        _extra = {
            "--include-from=/etc/lsyncd.list",
            "--exclude=*"
        }
```


© ООО Киберпротект, 2026

```
    }
}

sync {
    default.rsyncssh,
    source = "/etc/security",
    host = "cms-2",
    targetdir = "/etc/security",
    delete = 'false',
    rsync = {
        update = "true",
        whole_file = "true",
        _extra = {
            "--include=acronisagent.conf",
            "--exclude=*"
        }
    }
}
```

Создайте список файлов для синхронизации (/etc/lsyncd.list):

```
passwd
shadow
group
```

Перезапустите сервис lsyncd:

```
systemctl enable lsyncd --now
```

Выполните аналогичную процедуру на втором узле кластера (cms-2). В конфигурационном файле /etc/lsyncd.conf необходимо изменить имя хоста на cms-1.

Настройка кластера

Пользователь hacluster

На узлах кластера и арбитре задайте пароль для пользователя **hacluster**:

```
passwd hacluster
```

Кластерные службы

На узлах кластера добавьте запуск кластерных служб при перезагрузке:

```
systemctl enable pcsd pacemaker corosync
```

Инициализация кластера

На всех узлах кластера и на свидетеле запустите pscd:

© ООО Киберпротект, 2026

```
systemctl start pcsd
```

На одном из узлов кластера выполните команды по инициализации кластера:

```
pcs host auth cms-1 cms-2 -u hacluster # Запросит пароль hacluster
pcs cluster setup CyberBackup cms-1 cms-2
pcs cluster enable --all
pcs cluster start --all
```

где cms-1 и cms-2 – имена узлов кластера; CyberBackup – имя кластера.

Настройка арбитра

Инициализируйте на арбитре кворумное устройство и запустите pcsd:

```
[root@witness ~]# pcs qdevice setup model net --enable --start
Quorum device 'net' initialized
quorum device enabled
Starting quorum device...
quorum device started

[root@witness ~]# systemctl enable pcsd --now
Created symlink /etc/systemd/system/multi-user.target.wants/pcsd.service →
/usr/lib/systemd/system/pcsd.service.
```

Активируйте и запустите corosync-qdevice на каждом узле кластера:

```
[root@cms-1 ~]# systemctl enable corosync-qdevice
Created symlink /etc/systemd/system/multi-user.target.wants/corosyncqdevice.
service → /usr/lib/systemd/system/corosync-qdevice.service.
```

Для инициализации и настройки кворумного устройства на одном из узлов кластера выполните следующие команды:

```
[root@cms-1 ~]# pcs host auth witness
Username: hacluster
Password:
witness: Authorized

[root@cms-1 ~]# pcs quorum device add model net host=witness algorithm=ffsplit
Setting up qdevice certificates on nodes...
cms-1: Succeeded
cms-2: Succeeded
Enabling corosync-qdevice...
cms-1: corosync-qdevice enabled
cms-2: corosync-qdevice enabled
Sending updated corosync.conf to nodes...
cms-1: Succeeded
cms-2: Succeeded
```


© ООО Киберпротект, 2026

```
cms-1: Corosync configuration reloaded
Starting corosync-qdevice...
cms-2: corosync-qdevice started
cms-1: corosync-qdevice started

[root@cms-1 ~]# pcs quorum status
Quorum information
------------------
Date:             Thu Nov 16 21:50:29 2023
Quorum provider:  corosync_votequorum
Nodes:            2
Node ID:          1
Ring ID:          1.6a
Quorate:          Yes

Votequorum information
----------------------
Expected votes:   3
Highest expected: 3
Total votes:      3
Quorum:           2
Flags:            Quorate Qdevice

Membership information
----------------------
Nodeid      Votes    Qdevice      Name
1          1      A,V,NMW     cms-1 (local)
2          1      A,V,NMW     cms-2
0          1      Qdevice
```

Настройка механизма stonith / fencing

Для обеспечения целостности разделяемых данных в кластере существует механизм, называемый stonith или fencing. В случае сетевой недоступности неисправного узла кластера он всё еще может выполнять доступ к разделяемым данным, поэтому уцелевшая часть кластера должна иметь механизм для предотвращения доступа узла кластера, не отвечающего на запросы. Чаще всего это реализуется с помощью аппаратных средств, например, перезагрузка узла при помощи интерфейса управления IPMI, временного прерывания подачи питания через управляемые устройства распределения питания PDU (Power Distribution Unit), отключение портов узла на LAN/SAN-коммутаторах и т.п. Возможно использование одновременно несколько fencing-методов.

Внимание
Промышленная эксплуатация кластера без настроенного механизма stonith / fencing недопустима и ведет к риску порчи данных.

Ниже приведен вариант настройки fencing с использованием IPMI-совместимых модулей управления физического сервера.

© ООО Киберпротект, 2026

1. Включите механизм fencing:

```
pcs property set stonith-enabled=true
```

2. Установите на узлы кластера пакет с fencing-агентом:

```
dnf install fence-agents-ipmilan
```

3. Для каждого узла кластера создайте fencing-ресурс:

```
pcs stonith create cms1_ipmi fence_ipmilan pcmk_host_list="cms-1" \
    ip=10.77.0.58 username=testuser password=acd123 privlvl=operator \
    lanplus=1 op monitor interval=60s

pcs stonith create cms2_ipmi fence_ipmilan pcmk_host_list="cms-2" \
    ip=10.77.0.59 username=testuser password=acd123 privlvl=operator \
    lanplus=1 op monitor interval=60s
```

   Все параметры, доступные при создании fencing-ресурса, можно уточнить следующей командой:

```
pcs stonith describe fence_ipmilan
```

4. Создайте правила, запрещающие fencing-ресурсу для отключения узла запускаться на этом же самом узле:

```
pcs constraint location cms1_ipmi avoids cms-1
pcs constraint location cms2_ipmi avoids cms-2
```

5. Работа механизма fencing должна быть протестирована как отдельно, так и при тестировании отработки сценариев отказа кластером. Ручное тестирование интеграции возможно с использованием следующей команды, которая должна перезагрузить сервер cms-1 с использованием IPMI-интерфейса:

```
[root@cms-2 ~]# stonith_admin --reboot cms-1
```

   В тестовых кластерах, которые не содержат данных, представляющих ценность и используются только с целью проверки совместимости или отработки какой-либо гипотезы, допустимо отключение механизма fencing. Такие кластеры могут быть целиком реализованы внутри виртуальных машин и не иметь работающего механизма fencing. В таком случае его необходимо отключить:

```
pcs property set stonith-enabled=false
```

Монтирование блочных iSCSI-устройств

Выполните подключение блочных iSCSI-устройств на одном из узлов кластера. Сканируйте доступные из системы устройства с именем хоста iscsi-tgt.

© ООО Киберпротект, 2026

```
[root@cms-1 ~]# iscsiadm --mode discovery --type st --portal iscsi-tgt --login
10.77.44.62:3260,1 iqn.2003-01.org.linux-iscsi.iscsitgt.
x8664:sn.bfbc1ebb624c
Logging in to [iface: default, target: iqn.2003-01.org.linux-iscsi.iscsitgt.
x8664:sn.bfbc1ebb624c, portal: 10.77.44.62,3260]
Login to [iface: default, target: iqn.2003-01.org.linux-iscsi.iscsitgt.
x8664:sn.bfbc1ebb624c, portal: 10.77.44.62,3260] successful.
```

Проверьте наличие активных iSCSI-сессий до целевого устройства и отключите автоматическое подключение iSCSI-клиентом дисков с внешней системы хранения:

```
[root@cms-2 ~]# iscsiadm --mode session
tcp: [1] 10.77.44.62:3260,1 iqn.2003-01.org.linux-iscsi.iscsitgt.
x8664:sn.bfbc1ebb624c (non-flash)

[root@cms-2 ~]# iscsiadm --mode node --portal iscsi-tgt --op update \
    --name node.startup --value manual
```

Проверьте доступность новых блочных устройств:

```
[root@cms-1 ~]# lsblk
NAME    MAJ:MIN  RM  SIZE  RO  TYPE  MOUNTPOINTS
...
sdc       8:32     0   5G     0   disk
sdd       8:48     0   100G   0   disk
sde       8:64     0   20G    0   disk
...
```

Отформатируйте новые диски в ext4 и смонтируйте файловые системы:

```
[root@cms-1 ~]# mkfs.ext4 -m 0 -L etc /dev/sdc
[root@cms-1 ~]# mkfs.ext4 -m 0 -L var /dev/sdd
[root@cms-1 ~]# mkfs.ext4 -m 0 -L opt /dev/sde

[root@cms-1 ~]# mkdir -p /etc/Acronis /opt/acronis /var/lib/Acronis
[root@cms-2 ~]# mkdir -p /etc/Acronis /opt/acronis /var/lib/Acronis

[root@cms-1 ~]# mount /dev/sdc /etc/Acronis
[root@cms-1 ~]# mount /dev/sdd /var/lib/Acronis
[root@cms-1 ~]# mount /dev/sde /opt/acronis

[root@cms-1 ~]# lsblk -f
NAME              FSTYPE     FSVER     LABEL     UUID
FSAVAIL     FSUSE%   MOUNTPOINTS
...
sdc               ext4 1.0 etc cdbcd761-01fc-4f13-ad48-
cdcee09a6dd2 4,8G 0% /etc/Acronis
sdd               ext4 1.0 var eda7bfbb-edd8-4af3-b866-
1bdfa26879d6 97,7G 0% /var/lib/Acronis
sde               ext4 1.0 opt 1fa314b9-765f-460a-b0ef-
```


© ООО Киберпротект, 2026

```
9f3c56c0dd81 19,5G 0% /opt/acronis
...
```

Кластерные ресурсы и файловые системы

На одном из узлов кластера создайте кластерные ресурсы:

```
pcs resource create rsc_shared_disks ocf:heartbeat:iscsi udev="no" \
    portal=10.77.44.62 target=iqn.2003-01.org.linux-iscsi.iscsi-tgt.x8664:sn.bfbc1ebb624c \
    op monitor interval=60s timeout=30s

pcs resource create rsc_fs_etc ocf:heartbeat:Filesystem \
    device="/dev/disk/by-uuid/cdbcd761-01fc-4f13-ad48-cdcee09a6dd2" \
    directory="/etc/Acronis" fstype="ext4" options="lazytime" \
    force_unmount="true" \
    op monitor interval=60 timeout=60 OCF_CHECK_LEVEL=20 \
    meta migration-threshold=2 failure-timeout=1d

pcs resource create rsc_fs_var ocf:heartbeat:Filesystem \
    device="/dev/disk/by-uuid/eda7bfbb-edd8-4af3-b866-1bdfa26879d6" \
    directory="/var/lib/Acronis/" fstype="ext4" options="lazytime" \
    force_unmount="true" \
    op monitor interval=60 timeout=60 OCF_CHECK_LEVEL=20 \
    meta migration-threshold=2 failure-timeout=1d

pcs resource create rsc_fs_opt ocf:heartbeat:Filesystem \
    device="/dev/disk/by-uuid/1fa314b9-765f-460a-b0ef-9f3c56c0dd81" \
    directory="/opt/acronis" fstype="ext4" options="lazytime" \
    force_unmount="true" \
    op monitor interval=60 timeout=60 OCF_CHECK_LEVEL=20 \
    meta migration-threshold=2 failure-timeout=1d

pcs constraint colocation set rsc_fs_etc rsc_fs_var rsc_fs_opt \
    sequential=false set rsc_shared_disks setoptions id=col_fs

pcs constraint order set rsc_shared_disks set rsc_fs_etc rsc_fs_var \
    rsc_fs_opt sequential=false require-all=true setoptions id=ord_fs
```

Установка Кибер Бэкап

Установите Кибер Бэкап на узле с примонтированными файловыми системами стандартным образом (см. раздел "Установка" (стр. 18)). После успешной установки сервера управления Кибер Бэкап необходимо установить его также на второй узел. Для этого остановите службы Кибер Бэкап и переместите файловые системы на второй узел:

```
[root@cms-1 ~]# systemctl stop acronis_ams
[root@cms-1 ~]# systemctl stop acronis_asm
[root@cms-1 ~]# systemctl stop acronis_zmqgw
[root@cms-1 ~]# systemctl stop acronis_monitoring_service
[root@cms-1 ~]# pcs resource move rsc_shared_disks --autodelete
```


© ООО Киберпротект, 2026

```
[root@cms-1 ~]# pcs status
Cluster name: CyberBackup
Cluster Summary:
    * Stack: corosync (Pacemaker is running)
    * Current DC: cms-1 (version 2.1.6-1.el7-6fdc9deea29) - partition with quorum
    * Last updated: Wed Nov  1 09:58:45 2023 on cms-1
    * Last change:  Wed Nov  1 09:58:43 2023 by root via crm_resource on cms-1
    * 2 nodes configured
    * 9 resource instances configured

Node List:
    * Online: [ cms-1 cms-2 ]

Full List of Resources:
    * rsc_shared_disks    (ocf::custom:iscsi):    Started cms-2
    * rsc_fs_etc  (ocf::heartbeat:Filesystem):    Started cms-2
    * rsc_vip (ocf::heartbeat:IPaddr2):    Started cms-1
    * rsc_fs_var  (ocf::heartbeat:Filesystem):    Started cms-2
    * rsc_fs_opt  (ocf::heartbeat:Filesystem):    Started cms-2

Daemon Status:
    corosync: active/enabled
    pacemaker: active/enabled
    pcsd: active/enabled
```

Кластерные ресурсы и службы Кибер Бэкап

Создайте кластерные ресурсы для служб Кибер Бэкап на одном из узлов кластера.

Внимание

В параметре **portal** ресурса rsc_vip обязательно укажите IP-адрес, а не доменное имя.

```
pcs resource create rsc_vip ocf:heartbeat:IPaddr2 \
    ip="10.77.44.57" cidr_netmask="22" \
    op monitor interval="30"

pcs resource create rsc_ams systemd:acronis_ams \
    op start interval=0 timeout=60 \
    op stop interval=0 timeout=60 \
    op monitor interval=10 \
    meta target-role=Started \
    migration-threshold=2 failure-timeout=1d


pcs resource create rsc_asm systemd:acronis_asm \
    op start interval=0 timeout=60 \
    op stop interval=0 timeout=60 \
    op monitor interval=10 \
    meta target-role=Started \
```


© ООО Киберпротект, 2026

```
    migration-threshold=2 failure-timeout=1d


pcs resource create rsc_mon systemd:acronis_monitoring_service \
    op start interval=0 timeout=60 \
    op stop interval=0 timeout=60 \
    op monitor interval=10 \
    meta target-role=Started \
    migration-threshold=2 failure-timeout=1d


pcs resource create rsc_zmqgw systemd:acronis_zmqgw \
    op start interval=0 timeout=60 \
    op stop interval=0 timeout=60 \
    op monitor interval=10 \
    meta target-role=Started \
    migration-threshold=2 failure-timeout=1d

pcs constraint colocation set rsc_ams rsc_asm rsc_mon rsc_zmqgw \
        sequential=false set rsc_fs_etc rsc_fs_var rsc_fs_opt setoptions \
        id=col_services

pcs constraint order set rsc_fs_etc rsc_fs_var rsc_fs_opt sequential=false \
        require-all=true set rsc_ams rsc_asm rsc_mon rsc_zmqgw sequential=false \
        setoptions id=ord_services

pcs constraint colocation add rsc_vip with rsc_ams id=col_vip


[root@cms-2 ~]# pcs resource cleanup

[root@cms-2 ~]# pcs  status
Cluster name: CyberBackup
Cluster Summary:
    * Stack: corosync (Pacemaker is running)
    * Current DC: cms-1 (version 2.1.6-1.el7-6fdc9deea29) - partition with quorum
    * Last updated: Wed Nov  1 10:04:32 2023 on cms-2
    * Last change:  Wed Nov  1 09:58:43 2023 by root via crm_resource on cms-1
    * 2 nodes configured
    * 9 resource instances configured

Node List:
    * Online: [ cms-1 cms-2 ]

Full List of Resources:
    * rsc_shared_disks    (ocf::custom:iscsi):    Started cms-2
    * rsc_fs_etc  (ocf::heartbeat:Filesystem):    Started cms-2
    * rsc_vip (ocf::heartbeat:IPaddr2):    Started cms-2
    * rsc_fs_var  (ocf::heartbeat:Filesystem):    Started cms-2
    * rsc_fs_opt  (ocf::heartbeat:Filesystem):    Started cms-2
    * rsc_ams (systemd:acronis_ams):   Started cms-2
    * rsc_asm (systemd:acronis_asm):   Started cms-2
```


© ООО Киберпротект, 2026

```
    * rsc_mon (systemd:acronis_monitoring_service):    Started cms-2
    * rsc_zmqgw   (systemd:acronis_zmqgw):     Started cms-2

Daemon Status:
    corosync: active/enabled
    pacemaker: active/enabled
    pcsd: active/enabled
```

Убедитесь, что авторизация в веб-консоли по публичному адресу или его имени http://cms:9877 проходит успешно.

Подключение агентов

Для корректной работы клиентов после переключения активного узла кластера необходимо, чтобы регистрация агентов была выполнена с использованием плавающего кластерного адреса сервера управления. Данный адрес соответствует адресу, указанному в кластерном ресурсе rsc_vip.

Если агент ранее был зарегистрирован на некластеризованном сервере управления, то необходимо выполнить его перерегистрацию с явным указанием кластерного адреса. Пример перерегистрации агента из клиентской Linux-системы с использованием одноразового токена:

```
root@cbclient:~# /usr/lib/Acronis/RegisterAgentTool/RegisterAgent --
operation unregister
Success.
200
null

root@cbclient:~# /usr/lib/Acronis/RegisterAgentTool/RegisterAgent --
operation register --address cms --token 8D77-CEDC-433B
Success.
200
null
```

В этом примере:

- cms – кластерное доменное имя или vIP-адрес сервера управления;
- 8D77-CEDC-433B – токен, полученный в консоли управления Кибер Бэкап для регистрации агента.

Подробное описание дополнительных возможностей и вариантов регистрации агентов см. в отдельной статье.

2.6.3 Добавление машин через веб-интерфейс

Чтобы приступить к добавлению машины на сервер управления, щелкните **Физические и виртуальные машины** > **Добавить**.

© ООО Киберпротект, 2026

Если сервер управления установлен в Linux, будет предложено выбрать программу установки в соответствии с типом машины, которую нужно добавить. После скачивания программы установки запустите ее локально на этой машине.

Операции, описанные далее в этом разделе, возможны, если сервер управления установлен в Windows. В большинстве случаев развертывание агента на выбранной машине выполняется без вывода сообщений.

2.6.3.1 Добавление машины с ОС Windows

Подготовка

1. Для установки на удаленной машине, *не* входящей в домен Active Directory, контроль учетных записей (UAC) на этой машине должен быть *отключен*. Чтобы получить дополнительную информацию о том, как отключить его, выберите Требования к контролю учетных записей пользователей (UAC) > "Как отключить UAC".
2. По умолчанию для выполнения удаленной установки на любой машине Windows требуются учетные данные встроенной учетной записи администратора. Для удаленной установки с использованием учетных данных другого администратора, ограничения удаленного контроля учетных записей (UAC) должны быть *отключены*. Чтобы получить дополнительную информацию о том, как отключить их, выберите Требования к контролю учетных записей пользователей (UAC) > "Порядок отключения ограничений удаленного контроля учетных записей (UAC)".
3. Общий доступ к файлам и принтерам на удаленной машине должен быть *включен*. Для получения доступа к этому параметру выберите **Панель управления > Брандмауэр Windows** (**Брандмауэр Защитника Windows** в Windows 10) **> Центр управления сетями и общим доступом > Изменить дополнительные параметры общего доступа**.
4. Кибер Бэкап использует TCP-порты **445**, **25001** и **43234** для удаленной установки.

   Порт **445** открывается автоматически при выборе параметра "Общий доступ к файлам и принтерам". В брандмауэре Windows порты 43234 и 25001 открыты автоматически. При использовании другого брандмауэра убедитесь, что эти три порта открыты (добавлены в исключения) как для входящих, так и исходящих запросов.

   По окончанию удаленной установки порт **25001** автоматически закрывается брандмауэром Windows. Если в дальнейшем нужно обновлять агент удаленно, порты **445** и **43234** должны быть открыты. В брандмауэре Windows порт **25001** открывается и закрывается автоматически в ходе каждого обновления. Если используется другой брандмауэр, сохраните все эти порты открытыми.

© ООО Киберпротект, 2026

Примечание
Удаленная установка не поддерживается для контроллеров домена. Процедуру установки агента защиты на контроллер домена см. в разделе "Установка агентов в ОС Windows вручную" (стр. 95). Необходимо настроить параметры установки, выбрав в разделе **Учетная запись для входа службы агента** параметр **Использовать следующую учетную запись**. Дополнительную информацию об этом параметре см. в разделе "Настройка параметров установки в ОС Windows" (стр. 63).

Компоненты для удаленной установки

Для установки агентов на удаленные машины используются компоненты для удаленной установки, размещенные на сервере управления. В зависимости от операционной системы машины, на которой работает сервер управления, компоненты размещаются в следующих локальных папках:

- %ProgramFiles%\Acronis\RemoteInstallationFiles\installation_files\<номер сборки продукта> (ОС Windows; задается в разделе реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\RemoteInstallationFiles\<номер сборки продукта>**),
- /usr/lib/Acronis/RemoteInstallationFiles/installation_files/<номер сборки продукта> (ОС Linux).

На сервер управления с ОС Windows компоненты для удаленной установки устанавливаются по умолчанию. Ручная установка компонентов может понадобиться в следующих случаях:

- Компоненты не были установлены при установке сервера управления на машину с ОС Windows.
- Используется сервер управления, установленный на машину с ОС Linux.
- Компоненты были удалены с сервера управления.

Порядок размещения компонентов на сервере управления с ОС Linux

1. На веб-консоли Кибер Бэкап щелкните значок учетной записи в правом верхнем углу и выберите пункт **Загрузки**.
2. Щелкните **Офлайн-установщик для Windows (64-bit)** и получите установщик продукта.
3. Загрузите установщик продукта на машину с ОС Windows и запустите его.
4. В мастере установки продукта нажмите **Создание MST- и MSI-файлов для автоматической установки**.
5. В разделе **Устанавливаемые компоненты** выберите компоненты **Сервер управления**, **Компоненты для удаленной установки** и **Агент для Windows** и извлеките их файлы.
6. На сервере управления создайте папку x64 в папке /usr/lib/Acronis/RemoteInstallationFiles/installation_files/<номер сборки продукта>, а затем разместите извлеченные ранее файлы в созданной папке.
7. Убедитесь, что в папке /usr/lib/Acronis/RemoteInstallationFiles/installation_files есть файл web_installer.exe. При необходимости в разделе **Загрузки** веб-консоли Кибер Бэкап получите файл онлайн-установщика для Windows, сохраните его в эту папку и переименуйте в web_installer.exe.

© ООО Киберпротект, 2026

8. Перезапустите службу Acronis Management Server с помощью команды systemctl restart acronis_ams.

Агент развертывания

Чтобы установить агентов защиты на удаленных машинах из веб-консоли Кибер Бэкап, в вашей среде должен быть установлен хотя бы один агент защиты для Windows. Этот агент будет служить как агент развертывания для удаленной установки, а также будет подключаться к серверу управления и целевой удаленной машине.

При развертывании сервера управления на машине с ОС Windows, как правило, устанавливается агент защиты, который можно использовать как агент развертывания. При использовании сервера управления на машине с ОС Linux необходимо установить агента защиты на одну из имеющихся машин с ОС Windows.

Примечание
При установке агентов защиты на нескольких машинах агент защиты для Windows может также использоваться как агент обнаружения.

Принцип работы агента развертывания:

1. Агент развертывания подключается к серверу управления и получает файл web_installer.exe.
2. Агент развертывания подключается к удаленной машине по имени хоста или IP-адресу этой машины с использованием указанных вами учетных данных администратора, а затем передает на эту машину файл web_installer.exe.
3. Файл web_installer.exe выполняется на удаленной машине в автоматическом режиме.
4. В зависимости от области требуемой установки веб-установщик получает дополнительные компоненты с сервера управления, а затем устанавливает их на целевую машину с использованием команды msiexec.

   В зависимости от операционной системы машины, на которой работает сервер управления, компоненты размещаются в следующих локальных папках:
   - %ProgramFiles%\Acronis\RemoteInstallationFiles\installation_files\<номер сборки продукта> (ОС Windows; задается в разделе реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\RemoteInstallationFiles\<номер сборки продукта>**),
   - /usr/lib/Acronis/RemoteInstallationFiles/installation_files/<номер сборки продукта> (ОС Linux).
5. По окончании установки агент удаленной машины регистрируется на сервере управления.

Добавление машины

1. Щелкните **Физические и виртуальные машины** > **Добавить**.
2. Щелкните **Windows** или кнопку, соответствующую приложению, которое необходимо защитить.
   В зависимости от того, какая кнопка нажата, будет выбран один из следующих вариантов:
   - Агент для Windows
   - Агент для Hyper-V

© ООО Киберпротект, 2026

- Агент для SQL + агент для Windows
- Агент для Exchange + агент для Windows

  Если при наличии хотя бы одного зарегистрированного агента для Exchange щелкнуть **Microsoft Exchange Server** > **Почтовые ящики Exchange**, будет выполнен переход непосредственно к шагу 6.
- Агент для Active Directory + агент для Windows

3. Выберите агент развертывания.
4. Укажите имя хоста или IP-адрес целевой машины и учетные данные учетной записи с правами администратора на этой машине.

   Удаленная установка должна выполняться пользователем со встроенной учетной записью администратора. Если нужно использовать другую учетную запись пользователя, искомый пользователь должен входить в группу "Администраторы". Кроме того, необходимо внести изменения в реестр на машине, которая добавляется, согласно инструкциям по следующей ссылке: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.
5. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
6. Нажмите **Установить**.
7. Если на шаге 2 вы выбрали **Microsoft Exchange Server** > **Почтовые ящики Exchange**, укажите машину, на которой включена роль сервера **Client Access** (CAS) Microsoft Exchange Server. Дополнительную информацию см. в разделе «Резервное копирование почтовых ящиков».

Требования к контролю учетных записей пользователей (UAC)

На машине с ОС Windows, которая не входит в домен Active Directory, для операций централизованного управления (включая удаленную установку) необходимо, чтобы контроль учетных записей пользователей (UAC) и ограничения удаленного контроля учетных записей пользователей были отключены.

Порядок отключения UAC

1. Откройте редактор реестра.
2. Найдите следующий раздел реестра: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
3. Для параметра **EnableLUA** измените значение на **0**.
4. Перезапустите машину.

Порядок отключения ограничений удаленного контроля учетных записей (UAC)

© ООО Киберпротект, 2026

1. Откройте редактор реестра.
2. Найдите следующий раздел реестра: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Для параметра **LocalAccountTokenFilterPolicy** измените значение на **1**.

   Если параметр **LocalAccountTokenFilterPolicy** не существует, создайте его как DWORD (32 бита). Дополнительную информацию об этом значении см. в документации Microsoft по следующей ссылке: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Примечание
Из соображений безопасности после выполнения операции управления (например, удаленной установки) рекомендуется вернуть для обеих настроек их исходные значения: **EnableLUA=1** и **LocalAccountTokenFilterPolicy = 0**

2.6.3.2 Добавление машины с ОС Linux

1. Щелкните **Физические и виртуальные машины** > **Добавить**.
2. Щелкните **Linux**. Будет загружен файл установки.
3. На машине, которую нужно защитить, запустите программу установки локально.

2.6.3.3 Добавление vCenter или хоста ESXi

Добавить vCenter или автономный хост ESXi на сервер управления можно четырьмя способами:

- Развертывание агента для VMware (виртуальное устройство)

  Этот способ рекомендуется в большинстве случаев. Виртуальное устройство будет автоматически развернуто на каждом хосте, находящемся под управлением указанной системы vCenter. Можно выбрать хосты и настроить параметры виртуальных устройств.
- Установка агента для VMware (Windows)

  Возможно, вы решите установить агент для VMware на физической машине с ОС Windows в целях резервного копирования с помощью третьей машины или без использования локальной сети.
  - **Резервное копирование с помощью третьей машины**

    Используйте в том случае, если нагрузка на рабочие хосты ESXi так велика, что запускать на них виртуальные устройства нежелательно.
  - **Резервное копирование без использования локальной сети**

    Если с ESXi используется SAN-хранилище, установите агент на машину, подключенную к той же сети SAN. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Подробные инструкции см. в разделе "Резервное копирование без использования локальной сети посредством Windows-агента для VMware" (стр. 332).

  Если сервер управления выполняется в Windows, агент будет автоматически развернут на указанной машине. В противном случае необходимо установить агент вручную.

© ООО Киберпротект, 2026

- Регистрация установленного агента для VMware

  Это необходимый этап после переустановки сервера управления. Кроме того, можно зарегистрировать и настроить агент для VMware (виртуальное устройство, развернутое из шаблона OVF). Агент можно подключить только к одному vCenter Server или автономному хосту ESXi.
- Настройка уже зарегистрированного агента для VMware

  Это необходимый этап после установки агента для VMware (Windows) вручную или развертывания программно-аппаратного комплекса Кибер Бэкап. Кроме того, можно связать уже настроенный агент для VMware с другим сервером vCenter Server или автономным хостом ESXi.

Развертывание агента для VMware (виртуальное устройство) через веб-интерфейс

1. Щелкните **Физические и виртуальные машины** > **Добавить**.
2. Щелкните **VMware ESXi**.
3. Выберите **Разверните виртуальное устройство на каждом хосте vCenter**.
4. Укажите адрес и учетные данные для доступа к vCenter Server или автономному хосту ESXi. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями на хосте vCenter Server или ESXi.
5. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
6. [Необязательно] Щелкните **Настройки**, чтобы настроить параметры развертывания:
   - хосты ESXi, на которых необходимо развернуть агент (только если на предыдущем шаге был указан сервер vCenter Server);
   - имя виртуального устройства;
   - хранилище данных, в котором будет находиться устройство;
   - пул ресурсов или контейнер vApp, в котором будет содержаться устройство;
   - сеть, к которой будет подключен сетевой адаптер виртуального устройства;
   - настройки сети виртуального устройства. Можно выбрать автоматическую настройку DHCP или вручную указать значения, включая статический IP-адрес.
7. Щелкните **Развернуть**.

Установка агента для VMware (Windows)

Подготовка

Выполните инструкции по подготовке, описанные в разделе "Добавление машины с ОС Windows" (стр. 87).

© ООО Киберпротект, 2026

Установка

1. Щелкните **Физические и виртуальные машины** > **Добавить**.
2. Щелкните **VMware ESXi**.
3. Выберите **Удаленно установить на машине под управлением Windows**.
4. Выберите агент развертывания.
5. Укажите имя хоста или IP-адрес целевой машины и учетные данные учетной записи с правами администратора на этой машине.
6. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.
   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
7. Щелкните **Подключиться**.
8. Укажите адрес и учетные данные для vCenter Server или автономного хоста ESXi, а затем щелкните **Подключиться**. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями на хосте vCenter Server или ESXi.

   Примечание
   Агент можно подключить только к одному vCenter Server или автономному хосту ESXi. Если требуется подключить еще один автономный хост ESXi, то необходимо развернуть новый агент.
9. Щелкните **Установить**.

Регистрация установленного агента для VMware

В этом разделе описана регистрация агента для VMware через веб-интерфейс.

Альтернативные способы регистрации указаны ниже.

- Можно зарегистрировать агент для VMware (виртуальное устройство), указав сервер управления в интерфейсе виртуального устройства. См. шаг 3 в теме "Настройка виртуального устройства" раздела Развертывание агента для VMware (виртуальное устройство) из шаблона OVF.
- Агент для VMware (Windows) регистрируется при его локальной установке.

Регистрация агента для VMware

1. Щелкните **Физические и виртуальные машины** > **Добавить**.
2. Щелкните **VMware ESXi**.
3. Выберите **Зарегистрировать уже установленный агент**.

© ООО Киберпротект, 2026

4. Выберите агент развертывания.
5. При регистрации *агента для VMware (Windows)* укажите имя хоста или IP-адрес машины, на которой установлен агент, и данные учетной записи с правами администратора на этой машине.

   При регистрации *агента для VMware (виртуальное устройство)* укажите имя хоста или IP-адрес виртуального устройства и учетные данные сервера vCenter Server или автономного хоста ESXi, на котором работает устройство.
6. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
7. Щелкните **Подключиться**.
8. Укажите имя хоста либо IP-адрес сервера vCenter Server или хоста ESXi и учетные данные для доступа к нему, а затем щелкните **Подключение**. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями на хосте vCenter Server или ESXi.
9. Щелкните **Зарегистрировать**, чтобы зарегистрировать агент.

Настройка уже зарегистрированного агента для VMware

В этом разделе описан порядок связывания агента для VMware с vCenter Server или ESXi в веб-интерфейсе. Как вариант, это можно сделать в консоли агента для VMware (виртуальное устройство).

Эта процедура позволяет изменить существующую связь агента с vCenter Server или ESXi. Как вариант, это можно сделать в агенте для VMware (виртуальное устройство) или последовательно выбрав пункты **Настройки** > **Агенты** > агент > **Подробнее** > **vCenter/ESXi**.

Настройка агента для VMware

1. Щелкните **Физические и виртуальные машины** > **Добавить**.
2. Щелкните **VMware ESXi**.
3. В данном программном обеспечении отображается ненастроенный агент для VMware, который идет первым в алфавитном порядке.

   Если настроены все агенты, зарегистрированные на сервере управления, щелкните **Настроить уже зарегистрированный агент**. После этого в программе отобразится агент, который идет первым в алфавитном порядке.
4. При необходимости щелкните **Машина с агентом** и выберите агент для настройки.
5. Укажите или измените имя хоста либо IP-адрес сервера vCenter Server или хоста ESXi и учетные данные для доступа к ним. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми

© ООО Киберпротект, 2026

привилегиями на хосте vCenter Server или ESXi.

6. Щелкните **Настроить**, чтобы сохранить изменения.

2.6.4 Установка агентов

В этом разделе приводятся инструкции по установке и развертыванию агентов для таких программных компонентов, как операционные системы, платформы виртуализации, Кибер Инфраструктура и некоторых других. Установка агентов для защиты приложений, почтовых сервисов и баз данных рассматривается в разделе "Защита приложений, сервисов, баз данных" (стр. 475).

После установки и развертывания необходимых агентов убедитесь, что устройство, предназначенное к защите, доступно в веб-консоли в разделе "Устройства". Затем можно приступать непосредственно к резервному копированию (подробнее об этом см. в разделе "Резервное копирование" (стр. 264)).

2.6.4.1 Установка агентов в ОС Windows вручную

Установка агента для Windows, агента для Hyper-V, агента для Exchange, агента для SQL или агента для Active Directory

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.
4. Выберите **Установить агент защиты**.
5. Выполните любое из следующих действий:
   - Нажмите **Установить**.

     Это самый легкий способ установить продукт. Для большинства параметров установки будут использоваться значения по умолчанию.

     По умолчанию устанавливаются следующие компоненты:
     - Агент для Windows
     - Другие агенты (агент для Hyper-V, агент для Exchange, агент для SQL и агент для Active Directory), если на машине обнаружен соответствующий гипервизор или приложение
     - Мастер создания загрузочных носителей
     - Программа командной строки
     - Мониторинг Защиты Данных
   - Щелкните **Настройка параметров установки**, чтобы настроить программу установки.

     Можно будет выбрать компоненты для установки и указать дополнительные параметры. Дополнительную информацию см. в разделе «Настройка параметров установки».
   - Щелкните **Создать MST- и MSI-файлы для автоматической установки**, чтобы извлечь пакеты установки. Проверьте и при необходимости измените настройки установки, которые

© ООО Киберпротект, 2026

будут добавлены в MST-файл, затем нажмите кнопку **Создать**. Для этой процедуры не требуется никаких дополнительных шагов.

Чтобы развернуть агенты через групповую политику, выполните действия, указанные в разделе «Развертывание агентов с использованием групповой политики».

6. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:
   a. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   b. Укажите учетные данные администратора сервера управления или маркер регистрации.

      Дополнительную информацию о создании маркера регистрации см. в разделе "Развертывание агентов с использованием групповой политики" (стр. 179).
   c. Нажмите кнопку **Готово**.
7. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе "Отделы и административные учетные записи" (стр. 806).
8. Приступите к установке.
9. После завершения установки нажмите кнопку **Закрыть**.
10. Если установлен агент для Exchange, можно будет выполнять резервное копирование баз данных Exchange. Чтобы создать резервную копию почтовых ящиков Exchange, откройте веб-консоль Кибер Бэкап, щелкните **Добавить** > **Microsoft Exchange Server** > **Почтовые ящики Exchange** и укажите машину, на которой включена роль сервера **клиентского доступа** (CAS) Microsoft Exchange Server. Дополнительную информацию см. в разделе «Резервное копирование почтовых ящиков».

Порядок установки агента для VMware (Windows), агента для Oracle или агента для Exchange на машину без сервера Microsoft Exchange Server

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.
4. Выберите **Установить агент защиты**, затем щелкните **Настройка параметров установки**.
5. Рядом с пунктом **Устанавливаемые компоненты** щелкните **Изменить**.
6. Установите флажок, соответствующий агенту, который необходимо установить. Снимите флажки для компонентов, которые не нужно устанавливать. Чтобы продолжить, нажмите кнопку **Готово**.
7. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:
   a. Перейдите на **Сервер управления Кибер Бэкап** и щелкните **Указать**.

© ООО Киберпротект, 2026

b. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.

c. Укажите учетные данные администратора сервера управления или маркер регистрации.

   Дополнительную информацию о создании маркера регистрации см. в разделе "Развертывание агентов с использованием групповой политики" (стр. 179).

d. Нажмите кнопку **Готово**.

8. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе "Отделы и административные учетные записи" (стр. 806).

9. [Необязательно] Измените другие настройки установки, как описано в разделе «Настройка параметров установки».
10. Нажмите **Установить**, чтобы продолжить установку.
11. После завершения установки нажмите кнопку **Закрыть**.
12. [Только при установке агента для VMware (Windows)] Выполните процедуру, которая описана в разделе «Настройка уже зарегистрированного агента для VMware».
13. [Только при установке агента для Exchange] Откройте веб-консоль Кибер Бэкап, щелкните **Добавить** > **Microsoft Exchange Server** > **Почтовые ящики Exchange** и укажите машину, на которой включена роль сервера **клиентского доступа** (CAS) Microsoft Exchange Server. Дополнительную информацию см. в разделе «Резервное копирование почтовых ящиков».

2.6.4.2 Установка агентов в ОС Linux вручную

Подготовка

1. В системе, в которой не используется диспетчер пакетов RPM, необходимо установить этот диспетчер вручную. Как привилегированный пользователь выполните команду (например):

   ```
   apt-get install rpm
   ```

2. Убедитесь в том, что на машине установлены необходимые пакеты Linux.
3. Дайте разрешение на исполнение установочному файлу. Выполните следующую команду:

   ```
   chmod +x CyberBackup_*
   ```

Подготовка к установке в ОС Astra Linux SE

Перед установкой продукта в ОС Astra Linux SE ознакомьтесь с разделом "Совместимость с ОС Astra Linux SE" (стр. 42) и выполните следующие шаги. Предполагается, что включен режим замкнутой программной среды.

© ООО Киберпротект, 2026

1. Распакуйте дистрибутив:

```
tar --xattrs --xattrs-include=* -xvf CyberBackup_18_64-bit.x86_64.tar
```

2. Запустите файл установки с правами привилегированного пользователя:

```
./CyberBackup_18_64-bit.x86_64
```

3. Обновите образы initramfs:

```
update-initramfs -u -k all
```

4. Перезагрузите систему.

Установка

Для установки агента для Linux необходимо как минимум 2,0 ГБ свободного места на диске.

Установка агента для Linux

1. Запустите файл установки (файл .i686 или .x86_64) как привилегированный пользователь:

```
./CyberBackup_18_64-bit.x86_64
```

2. Примите условия лицензионного соглашения.
3. Укажите устанавливаемые компоненты:
   a. Снимите флажок **Сервер управления Кибер Бэкап**.
   b. Установите флажки для агентов, которые необходимо установить. Доступны следующие агенты:
      - **Агент для Linux (базовый агент)**;
      - **Агент для Oracle**;
      - **Агент для PostgreSQL**;
      - **Агент для MySQL/MariaDB**;
      - **Агент для Kubernetes**;
      - **Агент для oVirt**;
      - **Агент для CommuniGate Pro**;
      - **Агент для VK WorkMail**;
      - **Агент для Mailion**;
      - **Rescue Media Builder (компонент необходим для удаленного восстановления всей машины и дисков).**

      Для агентов для Oracle, PostgreSQL, MySQL/MariaDB, Kubernetes, oVirt, CommuniGate Pro, VK WorkMail также требуется установленный агент для Linux.
   c. Нажмите кнопку **Далее**.

© ООО Киберпротект, 2026

4. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:
   a. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   b. Укажите имя пользователя и пароль администратора сервера управления.

      Если в вашей организации есть отделы, установка учетных данных может понадобиться, чтобы добавить машину в отдел, которым управляет указанный администратор. Дополнительные сведения см. в разделе "Отделы и административные учетные записи" (стр. 806).
   c. Нажмите кнопку **Далее**.
5. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов, затем нажмите клавишу **ВВОД**.

   Этот запрос появляется, если учетная запись, указанная в предыдущем шаге, является администратором одного отдела или организации как минимум с одним отделом.

   Примечание
   Если в процессе установки возникнет ошибка сборки модуля ядра "Не удалось построить модуль ядра SnapAPI. Операции с резервными копиями на уровне дисков будут недоступны", продолжите установку. После завершения установки решите проблему с помощью статьи базы знаний Сборка модуля SnapAPI для Linux.
6. Если на машине включена безопасная загрузка UEFI, выводится сообщение о том, что необходимо перезагрузить систему после установки. Запомните пароль, который следует использовать (пароль привилегированного пользователя).

   Примечание
   В процессе установки создается новый ключ, который используется для подписи модулей ядра. Необходимо зарегистрировать этот ключ в списке владельцев ключей машины (Machine Owner Key, MOK), перезапустив машину. Если не зарегистрировать ключ, агент не будет работать. Если безопасная загрузка UEFI включена после установки агента, повторите установку, включая шаг 6.
7. После завершения установки выполните одно из следующих действий.
   - Нажмите кнопку **Перезапустить**, если в предыдущем шаге вам было предложено перезапустить систему.

     Во время перезапуска системы выберите управление ключом владельца машины (MOK), выберите **Зарегистрировать MOK** и зарегистрируйте ключ, используя пароль, предложенный в предыдущем шаге.
   - В противном случае нажмите **Выход**.

Сведения об устранении неполадок представлены в файле /usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL.

© ООО Киберпротект, 2026

2.6.4.3 Ручная установка агента для VMware (виртуальное устройство) из шаблона OVF

Перед началом

Системные требования для агента

По умолчанию виртуальному устройству назначается 4 ГБ ОЗУ и 2 виртуальных ЦП. Для большинства операций этого достаточно. Чтобы повысить производительность резервного копирования в случае, когда ожидается, что скорость передачи трафика резервного копирования превысит 100 МБ в секунду (например, в сетях с пропускной способностью 10 Гбит/с), рекомендуем повысить объем ОЗУ до 8 ГБ и использовать 4 виртуальных ЦП.

Виртуальные диски устройства занимают не более 6 ГБ. Формат диска («толстый» или «тонкий») не влияет на производительность устройства.

Сколько агентов необходимо?

Несмотря на то, что одно виртуальное устройство может защитить всю среду vSphere, рекомендуется развернуть по одному виртуальному устройству на каждый кластер vSphere (или на каждый хост при отсутствии кластера). Это позволит ускорить процессы резервного копирования, поскольку устройство с помощью транспорта HotAdd может присоединить диски, для которых созданы резервные копии. В этом случае трафик резервного копирования направляется от одного локального диска к другому.

Вполне нормально одновременно использовать виртуальное устройство и агент для VMware (Windows), когда они подключены к одному vCenter Server *или* разным хостам ESXi. Избегайте сценариев, когда один агент подключен к хосту ESXi напрямую, а другой агент подключен к vCenter Server, который управляет этим хостом ESXi.

Если у вас несколько агентов, не рекомендуем использовать локальное хранилище данных (т. е. хранить резервные копии на виртуальных дисках, добавленных в виртуальное устройство). Дополнительную информацию см. в разделе «Использование локально присоединенного хранилища».

Отключить автоматический DRS для агента

Если виртуальное устройство развернуто в кластере vSphere, убедитесь, что для него отключено автоматическое применение vMotion. В настройках DRS кластера включите уровни автоматизации отдельной виртуальной машины. После этого задайте параметру **Уровень автоматизации** виртуального устройства значение **Отключено**.

Развертывание шаблона OVF

Расположение шаблона OVF

Шаблон OVF содержит один OVF-файл и два VMDK-файла.

© ООО Киберпротект, 2026

Загрузить шаблон виртуального устройства OVF для VMware можно на сайте компании.

Развертывание шаблона OVF

1. Убедитесь, что файлы шаблона OVF доступны с машины, на которой выполняется клиент vSphere.
2. Запустите клиент vSphere и выполните вход на сервер vCenter Server.
3. Разверните шаблон OVF.
   - При настройке хранилища данных выберите общее хранилище данных, если оно существует. Формат диска («толстый» или «тонкий») не имеет значения, поскольку не влияет на производительность устройства.
   - При настройке сетевых подключений выберите сеть с сервером управления.

Настройка виртуального устройства

1. **Запуск виртуального устройства**

   В клиенте vSphere откройте раздел **Инвентаризация**, щелкните правой кнопкой имя виртуального устройства и выберите команду **Питание** > **Включить**. Выберите вкладку **Консоль**.
2. **Прокси-сервер**

   Если в вашей сети есть прокси-сервер:
   a. Чтобы запустить командную оболочку, в пользовательском интерфейсе виртуального устройства нажмите клавиши CTRL+SHIFT+F2.
   b. Откройте файл **/etc/Acronis/Global.config** в текстовом редакторе.
   c. Выполните одно из следующих действий:
      - Если параметры прокси-сервера были заданы во время установки агента, найдите следующий раздел:

        ```
        <key name="HttpProxy">
          <value name="Enabled" type="Tdword">"1"</value>
          <value name="Host" type="TString">"ADDRESS"</value>
          <value name="Port" type="Tdword">"PORT"</value>
          <value name="Login" type="TString">"LOGIN"</value>
          <value name="Password" type="TString">"PASSWORD"</value>
        </key>
        ```

      - В противном случае скопируйте приведенные выше строки и вставьте в файл между тегами <registry name="Global">...</registry>.
   d. Замените АДРЕС новым именем хоста или IP-адресом прокси-сервера, а ПОРТ – номером порта в десятичном формате.
   e. Если на прокси-сервере необходимо пройти аутентификацию, вместо дескрипторов ИМЯ ВХОДА и ПАРОЛЬ укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.
   f. Сохраните файл.

© ООО Киберпротект, 2026

g. Откройте файл **/opt/acronis/etc/aakore.yaml** в текстовом редакторе.

h. Найдите раздел **env** или создайте его и добавьте туда следующие строки:

```
env:
 http-proxy: proxy_login:proxy_password@proxy_address:port
 https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Вместо proxy_login и proxy_password укажите учетные данные прокси-сервера, а вместо proxy_address:port – адрес и номер порта прокси-сервера.

j. Выполните команду **reboot**.

В противном случае пропустите этот шаг.

3. **Сетевые настройки**

   Сетевое подключение агента настраивается автоматически с помощью протокола DHCP. Чтобы изменить конфигурацию по умолчанию, в подразделе **eth0** раздела **Параметры агента** нажмите кнопку **Изменить** и укажите нужные сетевые настройки.

4. **vCenter/ESX(i)**

   В окне **Параметры агента** в области **vCenter/ESX(i)** нажмите кнопку **Изменить** и укажите имя или IP-адрес vCenter Server. Агент сможет выполнять резервное копирование и восстановление любых виртуальных машин, управляемых vCenter Server.

   Если vCenter Server не используется, укажите имя или IP-адрес хоста ESXi, резервное копирование и восстановление виртуальных машин которого необходимо выполнить. Обычно резервное копирование происходит быстрее, когда агент создает резервные копии виртуальных машин, размещенных на его собственном хосте.

   Укажите учетные данные, которые будут использоваться агентом для подключения к vCenter Server или ESXi. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями на хосте vCenter Server или ESXi.

   С помощью команды **Проверить подключение** можно проверить правильность учетных данных для доступа.

5. **Сервер управления**

   a. На **сервере управления** в разделе **Параметры агента** щелкните **Изменить**.

   b. В разделе **Имя/IP-адрес сервера** выберите **Локальное**. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.

   c. В полях **Имя пользователя** и **Пароль** укажите имя пользователя и пароль администратора сервера управления.

6. **Часовой пояс**

   В разделе **Виртуальная машина** в подразделе **Часовой пояс** нажмите кнопку **Изменить**. Выберите свой часовой пояс, чтобы запланированные операции выполнялись в правильное время.

   После изменения часового пояса перезагрузите виртуальное устройство.

7. **[Необязательно] Локальные хранилища данных**

© ООО Киберпротект, 2026

К виртуальному устройству можно присоединить дополнительный диск, чтобы агент для VMware мог сохранять резервные копии на этом локально присоединенном хранилище.

Добавьте диск, изменив параметры виртуальной машины и нажав кнопку **Обновить**. Ссылка **Создать хранилище** станет доступной. Щелкните эту ссылку, выберите диск и задайте для него метку.

Обновление агента для VMware (виртуальное устройство)

Порядок обновления агента для VMware (виртуального устройства) с веб-консоли Кибер Бэкап

1. Щелкните **Настройки** > **Агенты**.

   В программе будет выведен список машин. Машины с агентами устаревших версий будут помечены оранжевым восклицательным знаком.
2. Выберите машины, на которых нужно обновить агенты. Машины должны быть включены.
3. Щелкните **Обновить агент**.

Примечание
При выполнении обновления все выполняющиеся резервные копии завершатся сбоем.

Порядок обновления агента для VMware (виртуальное устройство) версий, более ранних, чем 12.5.23094

1. Удалите агент для VMware (виртуальное устройство), как описано в разделе "Удаление продукта". В шаге 5 удалите агент из раздела **Настройки** > **Агенты**, даже если вы планируете установить агент снова.
2. Разверните агент для VMware (виртуальное устройство), как описано в разделе "Развертывание шаблона OVF".
3. Настройте агент для VMware (виртуальное устройство), как описано в разделе "Настройка виртуального устройства".

   Чтобы восстановить локальное хранилище данных, в шаге 7 выполните следующие действия:

   a. Добавьте на виртуальное устройство диск с локальным хранилищем данных.

   b. Последовательно выберите пункты **Обновить** > **Создать хранилище** > **Подключить**.

   c. В программе отображается оригинальная **буква** и **метка** диска. Не меняйте их.

   d. Нажмите кнопку **OK**.

   В результате планы защиты, примененные к старому агенту, автоматически применяются к новому агенту.
4. Для планов с включенным резервным копированием с поддержкой приложений необходимо заново ввести учетные данные гостевой ОС. Измените эти планы и заново введите учетные данные.
5. Для планов, которые выполняют резервное копирование конфигурации ESXi, необходимо заново ввести пароль привилегированного пользователя (root). Измените эти планы и заново введите пароль.

© ООО Киберпротект, 2026

2.6.4.4 Установка агента для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация)

Для развертывания агента oVirt вам понадобятся установленные и настроенные системы:

- Система управления виртуализацией (например, ROSA Virtualization).
- Решение Кибер Бэкап.

Вы можете установить агент двумя способами:

- Автоматически из интерфейса Кибер Бэкап.
- Вручную, используя установочный файл агента oVirt в формате OVA.

После установки настройте агент в системе управления виртуализацией (например, ROSA Virtualization) и создайте план защиты ваших виртуальных устройств в Кибер Бэкап.

Настройка LDAP-аутентификации для агента для zVirt

Система управления виртуализацией zVirt, благодаря интеграции с системой управления учетными данными и доступом Keycloack, позволяет подключать службы каталогов (например, Active Directory, FreeIPA или SambaDC), предоставлять доступ в ее порталы пользователям служб каталогов, разрешать им выполнение операций. Список поддерживаемых служб каталогов см. в документации zVirt.

Для того чтобы можно было использовать учетные данные пользователя службы каталогов при настройке виртуального устройства (агента для zVirt), необходимо выполнить следующие действия:

1. На портале Keycloack подключите необходимую службу каталогов согласно инструкции в документации zVirt.
2. Подготовьте учетные данные пользователя службы каталога. Можно использовать существующего пользователя или создать нового.
3. На портале администрирования zVirt:
   a. В разделе **Управление** > **Пользователи** добавьте пользователя службы каталогов. При добавлении в поле **Поиск** необходимо выбрать **internalsso (...)**.
   b. Предоставьте добавленному пользователю такие же разрешения, как у пользователя admin.
4. Убедитесь, что можно войти на портал управления zVirt с учетными данными этого пользователя.

После выполнения этих действий можно будет использовать учетные данные пользователя службы каталогов для автоматической или ручной настройки виртуального устройства. Имя пользователя необходимо указать в формате <name>@internalsso.

© ООО Киберпротект, 2026

Автоматическая установка агента для oVirt

Примечание
Убедитесь, что у сервера управления есть доступ к дистрибутиву через сеть Интернет. Если доступ есть, переходите сразу к установке агента (п.4 и далее).
Если у сервера управления нет интернет-доступа к дистрибутиву, вначале загрузите дистрибутив вручную на хост с вашими виртуальными машинами, для которых вы будете использовать Кибер Бэкап, по SSH или другим доступным способом, и положите в папку (см. п.3), не распаковывая его.

Чтобы установить агент, выполните действия:

1. Перейдите на сайт Киберпротект в раздел Загрузки.
2. В категории **Дополнительные файлы** щелкните **Пакет установки агента для oVirt**.
3. Загрузите файл дистрибутива агента для oVirt и положите его в папку на сервере управления Кибер Бэкап:
   - C:\ProgramData\Acronis\VaDeployer\va-images (Windows),
   - /var/lib/Acronis/VaDeployer/va-images (Linux).
4. Войдите в веб-консоль Кибер Бэкап.
5. Добавьте лицензию:
   a. Откройте раздел **Параметры > Лицензии**.
   b. Нажмите кнопку **Добавить ключи**.
   c. В поле введите один или несколько лицензионных ключей в формате XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX.
   d. Нажмите кнопку **Добавить**.
   e. Обновите страницу: на всплывающем окне нажмите **Обновить сейчас**.
6. Добавьте виртуальное устройство:
   a. Откройте раздел **Устройства** > **Физические и виртуальные машины**.
   b. В правом верхнем углу окна нажмите кнопку **Добавить**.
   c. В окне **Добавить устройства** в разделе **Хосты виртуализации** выберите один из вариантов в зависимости от системы oVirt, которую вы используете:
      - Red Hat Virtualization (oVirt),
      - ROSA Virtualization (oVirt),
      - zVirt (oVirt),
      - РЕД Виртуализация (oVirt).
   d. В открывшемся окне введите параметры сервера.
      Например, если вы выбрали ROSA Virtualization (oVirt), укажите имя или IP-адрес сервера ROSA Virtualization (например, https://my-ovirt), имя пользователя (например, admin@internal) и пароль доступа к ROSA Virtualization.

© ООО Киберпротект, 2026

Примечание
При установке агента в систему управления виртуализацией zVirt имя пользователя службы каталогов необходимо указать в формате <name>@internalsso. Подробные сведения см. в разделе "Настройка LDAP-аутентификации для агента для zVirt" (стр. 104).

e. В списке выберите доменное имя или IP-адрес сервера управления Кибер Бэкап.

f. Нажмите кнопку **Настройки**.

g. В окне дополнительных настроек задайте имя виртуального устройства, выберите кластер, домен и сеть, с которыми будет взаимодействовать виртуальное устройство.
Если вы хотите автоматически получить сетевые параметры по DHCP, установите флажок.

h. Нажмите кнопку **Развернуть**.

Агент будет установлен и появится в системе oVirt в списке виртуальных машин под именем ovirt_virtual_appliance.

Ручная установка агента для oVirt

Чтобы установить агент вручную, выполните действия:

1. Скачайте дистрибутив агента oVirt (файл формата OVA).
2. Загрузите дистрибутив на хост с вашими виртуальными машинами, для которых вы будете использовать Кибер Бэкап, по SSH или другим доступным способом.
3. Распакуйте архив, выполнив команду bzip2 -d <полное имя файла с версией>.ova. Например: bzip2 -d OVirtAppliance_v15.0.25879.ova.
4. Войдите в систему ROSA Virtualization через браузер.
5. В списке ресурсов выберите **Виртуальные машины**.
6. В меню действий над виртуальными машинами выберите **Импорт**.
7. В открывшейся форме задайте следующие параметры:
   - Дата-центр, в котором находится хост, на который вы загрузили OVA-файл.
   - Источник: Виртуальное устройство (OVA).
   - Имя хоста, на который вы загрузили OVA-файл.
   - Путь к файлу - полный путь к директории, в которую вы загрузили OVA-файл.
8. Нажмите кнопку **Загрузить**.
   Загруженный OVA-файл появится в списке Виртуальные машины источника.
   Внимание! Если OVA-файл с дистрибутивом агента не появился в списке, убедитесь, что вы указали корректный путь к файлу и что архив с дистрибутивом не поврежден.
9. Выберите OVA-файл ovirt_virtual_appliance в списке и переместите его в список **Виртуальные машины для импорта**.
10. Нажмите кнопку **Далее**.
11. В открывшемся окне укажите домен и кластер, в который вы хотите установить агент.

© ООО Киберпротект, 2026

12. Нажмите на имя виртуального устройства.
    Раскроется меню.
13. Выберите вкладку **Сетевые интерфейсы**.
14. Задайте имя сети ovirtmgmt и профиль ovirtmgmt.
15. Нажмите кнопку **OK**.

Выполненные действия должны привести к следующим результатам:

Агент oVirt будет установлен и появится в списке виртуальных машин под именем ovirt_virtual_appliance.

Настройка агента в ROSA Virtualization

Независимо от того, каким способом вы установили агент ROSA Virtualization (oVirt), необходимо его настроить.

Чтобы настроить агент в ROSA Virtualization, выполните действия:

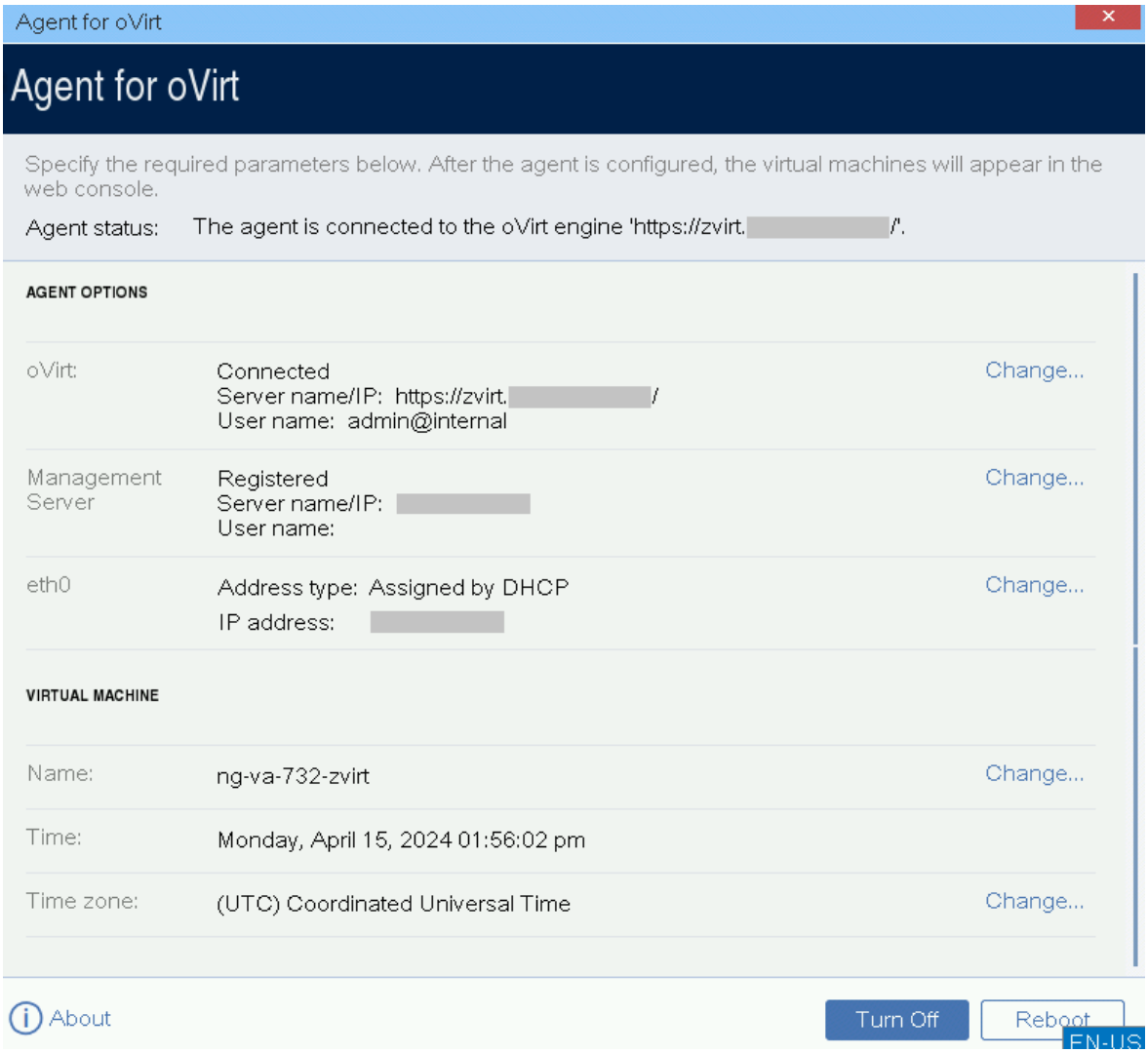
1. Войдите в систему ROSA Virtualization через браузер.
2. В списке ресурсов выберите **Виртуальные машины**.
3. В списке виртуальных машин выберите **ovirt_virtual_appliance**.
4. В меню выберите **Консоль** и откройте консоль. Вы увидите интерфейс настройки агента ROSA Virtualization (oVirt).
5. В консоли выбирайте параметр, нажимайте на кнопку **Change**, чтобы изменять его значение. Нажимайте кнопку **OK** чтобы сохранять изменения.
   Настройте следующие параметры:
   - **oVirt**
     Укажите имя или адрес сервера ROSA Virtualization, на который вы устанавливаете агент (например, https://my-ovirt), имя пользователя (например, admin@internal) и пароль доступа к ROSA Virtualization. Нажмите **Check connection** чтобы проверить соединение. Ошибки при подключении могут указывать как на некорректность введенных данных, так и на проблемы с сетью.

     Примечание
     При настройке агента для системы управления виртуализацией zVirt имя пользователя службы каталогов необходимо указать в формате <name>@internalsso. Подробные сведения см. в разделе "Настройка LDAP-аутентификации для агента для zVirt" (стр. 104).

   - **Management Server**
     Укажите имя или IP-адрес компьютера, на котором установлено решение Кибер Бэкап, имя пользователя и пароль доступа к нему.
   - **Eth0**
     Если необходимо, задайте параметры сетевого интерфейса, для которого вы будете использовать агент (IP-адрес, маску сети, шлюз и DNS). По умолчанию используется DHCP.

© ООО Киберпротект, 2026

- **Name**
  Если необходимо, измените имя агента. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.
- **Time zone**
  Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.



Выполненные действия должны привести к следующим результатам в веб-консоли Кибер Бэкап:

- в разделе **Настройки** > **Агенты** отобразится агент ROSA Virtualization (oVirt),
- в разделе **Устройства** появится подраздел oVirt.

© ООО Киберпротект, 2026

2.6.4.5 Развертывание резервного копирования для Кибер Инфраструктуры

Общие сведения

Для развертывания резервного копирования для продукта Кибер Инфраструктура вам понадобятся установленные и настроенные системы:

- Решение Кибер Инфраструктура версии с 6.0 по 6.5.2.
- Решение Кибер Бэкап.

Установка проводится в несколько этапов:

- Создание и регистрация пользователя.
- Установка виртуального устройства.
- Подключение виртуального устройства к серверу управления.

Известные проблемы и ограничения

- Восстановление невозможно, если выполнено резервное копирование машины, на которой находятся сервер управления и агент. Восстановление с Кибер Инфраструктурой компьютера с системным диском, на котором находится сервер управления, завершается ошибкой: Не удалось подключиться к службе ядра агента на этом компьютере.
- Виртуальное устройство оперирует данными обо всех виртуальных машинах во всех доменах, вне зависимости от того в каком домене оно развернуто, и передает их серверу управления, в то время как пользователь не должен иметь доступ за пределы своего домена. В результате сервер управления имеет доступ к машинам за пределами домена виртуального устройства. Эти машины доступны для резервного копирования, но восстановление в домены за пределами виртуального устройства невозможно.

Создание и регистрация пользователя

Для настройки виртуального устройства необходимо создать специального пользователя в Кибер Инфраструктуре и предоставить ему доступ ко всем проектам с виртуальными машинами, для которых требуется выполнять резервное копирование и восстановление. Этого пользователя можно создать в любом домене и назначить ему любую роль.

Для получения подробной информации об управлении пользователями см. раздел «Управление доменами, пользователями и проектами» в руководстве администратора продукта Кибер Инфраструктура.

Чтобы предоставить пользователю доступ ко всем проектам домена, выполните следующие действия на сервере управления Кибер Инфраструктуры:

© ООО Киберпротект, 2026

1. Подготовьтесь для работы с интерфейсом командной строки OpenStack с правами администратора системы:
   a. Создайте RC-файл для OpenStack, в котором указаны учетные данные администратора системы.

      ```
      su - vstoradmin
      kolla-ansible post-deploy
      exit
      ```

   b. Задайте переменные среды, необходимые для клиента командной строки OpenStack.

      ```
      . /etc/kolla/admin-openrc.sh
      ```

2. Предоставьте пользователю доступ.

   ```
   openstack --insecure user set --project <project> --project-domain <project-domain> --domain <user-domain> <username>
   openstack --insecure role add --domain <project-domain> --user <username> --user-domain <user-domain> admin --inherited
   ```

   В этих командах:
   - <project-domain> — имя целевого домена с проектами, к которым будет предоставлен доступ.
   - <project> — имя любого проекта из целевого домена.
   - <user-domain> — имя домена пользователя, которому будет предоставлен доступ.
   - <username> — имя пользователя Кибер Инфраструктуры. Виртуальное устройство будет использовать этого пользователя для резервного копирования и восстановления виртуальных машин в проектах целевого домена.

При необходимости можно просмотреть роли, назначенные пользователю Кибер Инфраструктуры.

- Команда openstack --insecure role assignment list --user <username> --names выводит только те роли, которые назначены пользователю <username> явно, например:

  ```
  openstack --insecure role assignment list --user johndoe --names
  +--------------+-----------------+-------+---------+-------------+--------+-----------+
  | Role         | User            | Group | Project | Domain      | System | Inherited |
  +--------------+-----------------+-------+---------+-------------+--------+-----------+
  | admin        | johndoe@Default |       |         | MyNewDomain |        | True      |
  | compute      | johndoe@Default |       |         | Default     |        | True      |
  | domain_admin | johndoe@Default |       |         | Default     |        | True      |
  | domain_admin | johndoe@Default |       |         | Default     |        | False     |
  +--------------+-----------------+-------+---------+-------------+--------+-----------+
  ```

- Команда openstack --insecure role assignment list --user <username> --names --effective выводит список всех ролей, назначенных пользователю <username> как явно, так и неявно, например:

  ```
  openstack --insecure role assignment list --user johndoe --names --effective
  +--------------+-----------------+-------+-----------------+---------+--------+-----------+
  ```


© ООО Киберпротект, 2026

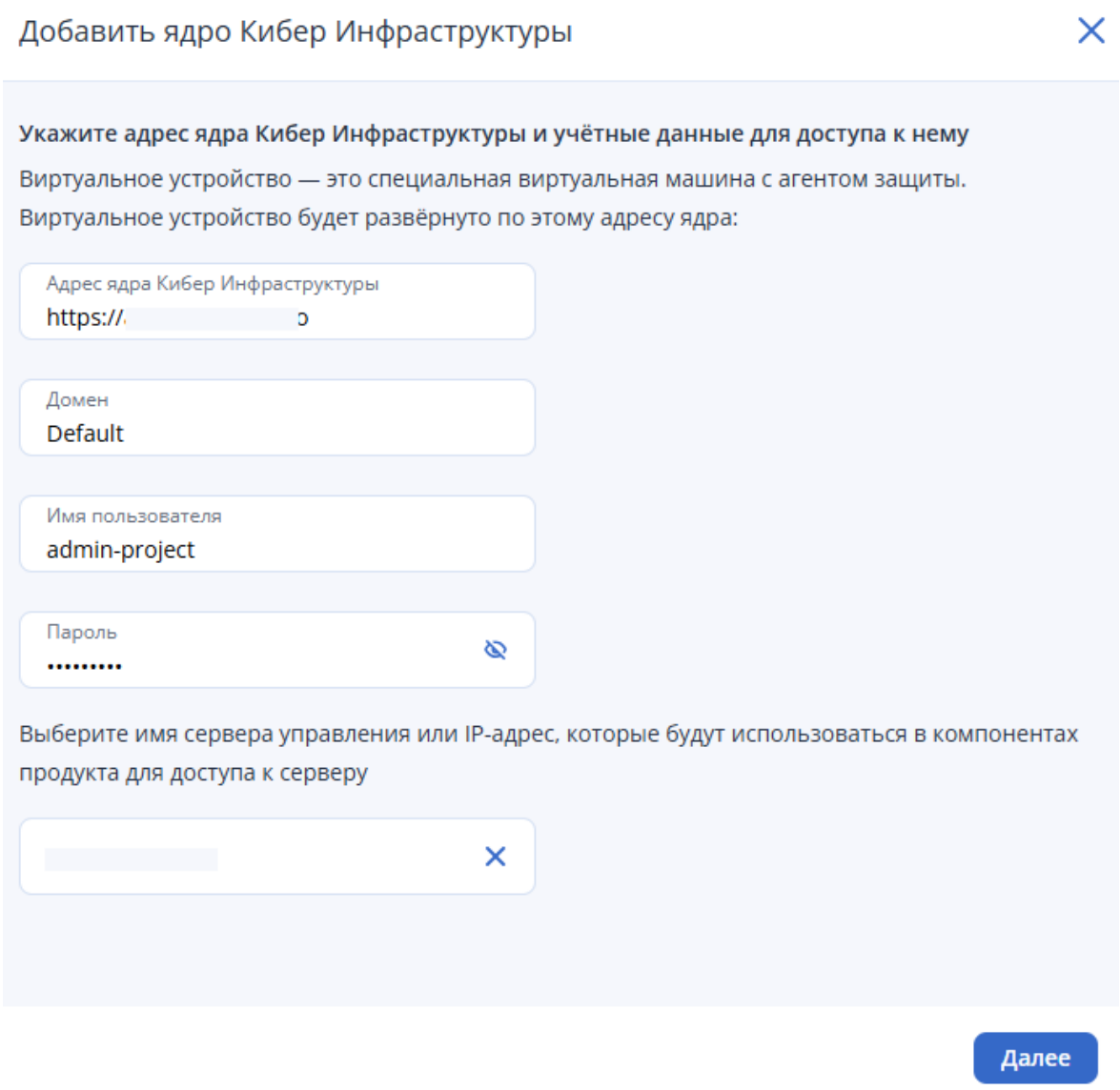
```
| Role         | User            | Group | Project        | Domain  | System | Inherited |
+--------------+-----------------+-------+----------------+---------+--------+-----------+
| domain_admin | johndoe@Default |       |                | Default |        | False     |
| compute      | johndoe@Default |       | admin@Default  |         |        | True      |
| compute      | johndoe@Default |       | service@Default |        |        | True      |
| domain_admin | johndoe@Default |       | admin@Default  |         |        | True      |
| domain_admin | johndoe@Default |       | service@Default |        |        | True      |
| project_user | johndoe@Default |       | service@Default |        |        | True      |
| member       | johndoe@Default |       | service@Default |        |        | True      |
| reader       | johndoe@Default |       | service@Default |        |        | True      |
| project_user | johndoe@Default |       | admin@Default  |         |        | True      |
| member       | johndoe@Default |       | admin@Default  |         |        | True      |
| reader       | johndoe@Default |       | admin@Default  |         |        | True      |
| project_user | johndoe@Default |       |                | Default |        | False     |
| member       | johndoe@Default |       |                | Default |        | False     |
| reader       | johndoe@Default |       |                | Default |        | False     |
+--------------+-----------------+-------+----------------+---------+--------+-----------+
```

Автоматическая установка агента для Кибер Инфраструктуры

Чтобы добавить хост Кибер Инфраструктуры на сервер управления и автоматически развернуть агент, выполните следующие шаги в веб-интерфейсе Кибер Бэкап:

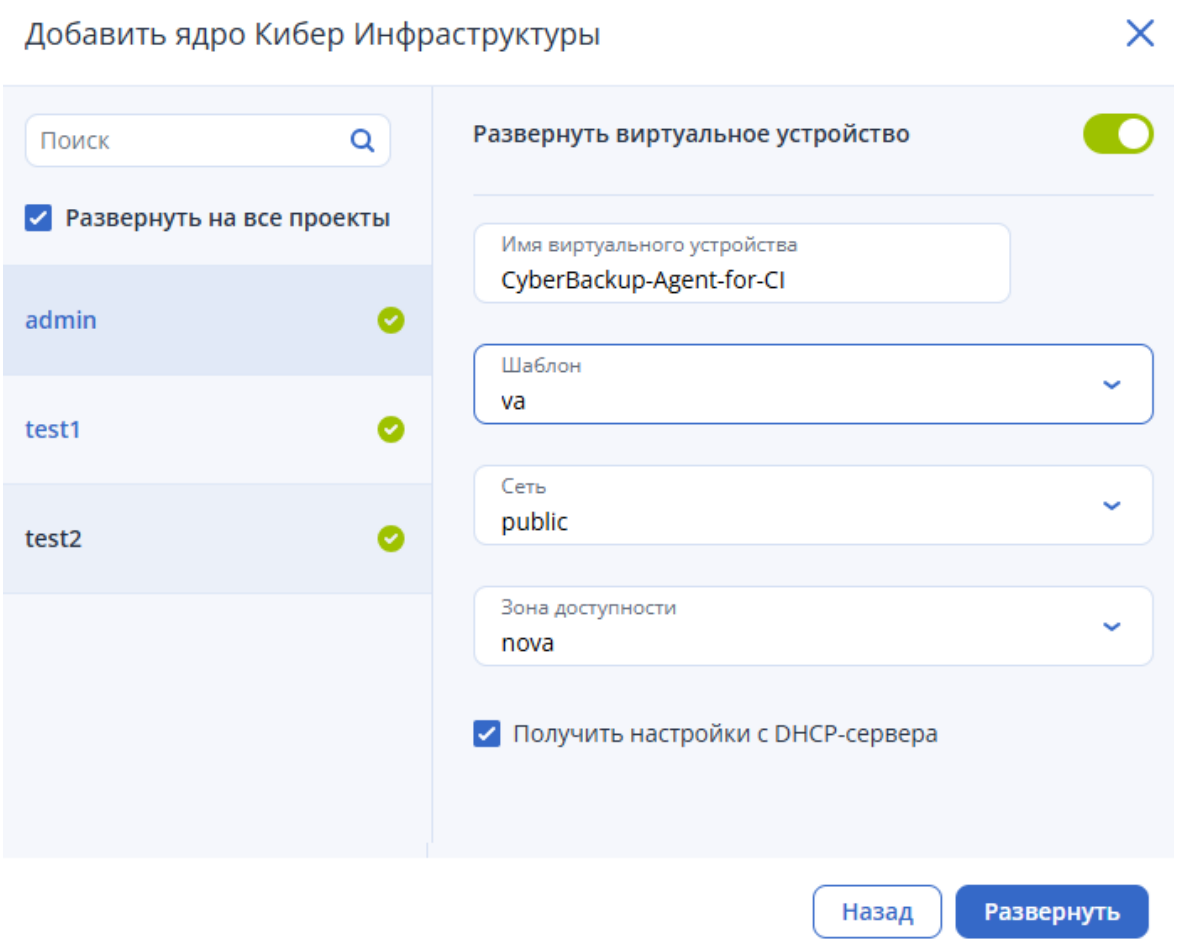
1. На вкладке **Устройства** > **Физические и виртуальные машины** щелкните **Добавить**. Появится окно **Добавить устройства**.
2. В разделе **Платформы виртуализации** выберите **Кибер Инфраструктура**. Откроется окно **Добавить ядро Кибер Инфраструктуры**.

© ООО Киберпротект, 2026



3. В поле **Адрес ядра Кибер Инфраструктуры** укажите адрес сервера управления Кибер Инфраструктуры.
4. В поле **Домен** укажите домен Кибер Инфраструктуры.
5. В соответствующих полях укажите имя пользователя и пароль пользователя в Кибер Инфраструктуре с правами в целевом домене (см. раздел "Создание и регистрация пользователя" (стр. 109)).
6. Нажмите **Далее**. Откроется окно **Добавить ядро Кибер Инфраструктуры**.

© ООО Киберпротект, 2026



7. Для каждого необходимого проекта включите ползунок **Развернуть виртуальное устройство** и укажите параметры виртуального устройства:
   - **Имя виртуального устройства**.
   - **Шаблон**. Необходимо минимум 4 ГБ ОЗУ, 2 ядра ЦП и 8 ГБ дискового пространства.
   - **Сеть**. Должна обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап.
   - **Зона доступности**.
8. При необходимости можно снять флажок **Получить настройки с DHCP-сервера** и указать параметры сети вручную.
9. Указав необходимые параметры, нажмите **Развернуть**.

В Кибер Инфраструктуре будет создано виртуальное устройство, в которое будет установлен агент. При этом архив агента с именем "CIAppliance_v<версия>.zip" будет загружен с официального сайта Киберпротект. Если это невозможно, архив агента будет взят локально с машины, на которой установлен сервер управления Киберпротект: из директории C:\ProgramData\Acronis\VaDeployer\va-images (в ОС Windows) или из директории /var/lib/Acronis/VaDeployer/va-images (в ОС Linux).

Перейдите в **Настройки** > **Агенты** и убедитесь, что в списке появился агент для резервного копирования Кибер Инфраструктуры.

© ООО Киберпротект, 2026

Установка агента для Кибер Инфраструктуры вручную

Чтобы установить агент:

1. Скачайте дистрибутив для резервного копирования с Кибер Инфраструктурой (архив формата ZIP, например CIAppliance.zip), распакуйте его, извлеките файл CIAppliance.qcow2.
2. В Кибер Инфраструктуре перейдите в **Вычисления** > **Виртуальные машины** > **Образы** и нажмите **Добавить образ**.
3. В поле **Файл образа** укажите путь к нужному образу виртуальной машины.
4. При необходимости в поле **Имя** измените наименование образа.
5. В поле **Выберите дистрибутив ОС** укажите нужный дистрибутив и нажмите **Добавить**.
6. Перейдите на вкладку **Виртуальные машины** и нажмите **Создать виртуальную машину**.
7. В разделе **Образ** нажмите **Укажите** и в открывшемся окне выберите необходимый образ.
8. В разделе **Тип ВМ** нажмите **Укажите** и в открывшемся окне выберите тип ВМ. Для промышленных сборок рекомендуется выбрать тип ВМ, содержащий как минимум 2 ЦП и 4 ГБ памяти.
9. В разделе **Сетевые интерфейсы** нажмите **Укажите** и в открывшемся окне выберите подходящий сетевой интерфейс. Нажмите **Добавить** и в поле **Сеть** выберите нужный сетевой интерфейс. Убедитесь, что виртуальное устройство имеет доступ к внутренним сетям кластера со следующими типами трафика (сети и назначенные им типы трафика можно просмотреть в разделе **Инфраструктура** > **Сети**):
   - **VM backups**,
   - **Compute API**,
   - **Storage** (не обязательно).

   Доступ к **VM backups** разрешает передачу данных от виртуальной машины к резервным копиям и обратно. Доступ к **Compute API** позволяет использовать дополнительные возможности, например, взаимодействие с OpenStack, создание моментальных снимков резервных копий.
10. Введите имя виртуальной машины и по окончании ввода данных нажмите **Развернуть**.
11. Перейдите снова в раздел **Виртуальные машины** и убедитесь, что имя виртуальной машины появилось в списке виртуальных машин.

Примечание
Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

Подключение виртуального устройства к серверу управления

1. Перейдите в **Вычисления** > **Виртуальные машины**.
2. В списке виртуальных машин выберите имя виртуальной машины и перейдите в **Консоль**.

© ООО Киберпротект, 2026

3. В поле **Server name/IP** введите адрес сервера управления Кибер Инфраструктуры в формате https://<address>:5000.
4. В поле **User domain name** укажите имя системного домена.
5. В остальных полях укажите нужные параметры, нажмите **Check connection**, чтобы проверить соединение и затем **OK**.
6. В открывшемся окне **Register agent** укажите данные для подключения к серверу управления Кибер Бэкап и нажмите **OK**.
7. В открывшемся окне **Rename Agent for Cyber Infrastructure** введите имя агента Кибер Инфраструктуры и нажмите **Отправить комбинацию клавиш**.
8. По окончании настроек откройте Кибер Бэкап и выберите вкладку **Устройства**. Убедитесь, что в подменю слева появилась вкладка **Кибер Инфраструктура**.
9. Перейдите в **Настройки** > **Агенты** и убедитесь, что в списке агентов появился агент для резервного копирования Кибер Инфраструктуры.

2.6.4.6 Ручная установка агента для SpaceVM

Для развертывания агента для SpaceVM и настройки его интеграции с Кибер Бэкап вам понадобятся установленные и настроенные системы:

- Система SpaceVM версии с 6.0.5 по 6.5.8.
- Решение Кибер Бэкап.

Планирование количества агентов для SpaceVM

Чтобы создавать резервные копии всех виртуальных машин, как правило, нужно развернуть несколько агентов для SpaceVM. Это связано с тем, что агенты могут получить доступ только к пулам данных, подключенным к серверу (хосту), на котором развернут агент.

Если вы используете только локальные пулы данных, разверните по одному агенту для SpaceVM на каждом сервере.

Если вы используете общие пулы данных, доступные на всех серверах, достаточно развернуть один агент для SpaceVM.

Дополнительные агенты также могут потребоваться в ситуации, когда в системе имеется очень большое число виртуальных машин, и суммарное время создания резервных копий окажется слишком большим.

Процедура развертывания

Выполняйте действия по развертыванию агента для SpaceVM в следующем порядке:

1. "Установка сервера управления" (стр. 63).
2. "Установка агента для SpaceVM" (стр. 117).
3. "Создание плана защиты" (стр. 224).

© ООО Киберпротект, 2026

Известные проблемы и ограничения

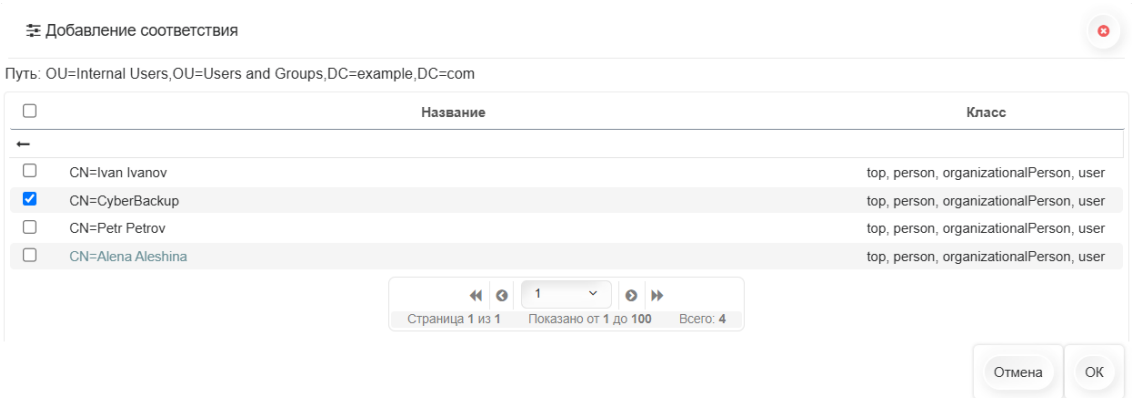
1. Текущие версии платформы SpaceVM не позволяют осуществлять резервное копирование следующих типов виртуальных машин:
   - виртуальные машины, являющиеся "тонким клоном", в которых уже после операции создания "тонкого клона" был изменен набор дисков;
   - виртуальные машины с SCSI-контроллером типа lsilogic.
2. Текущие версии платформы SpaceVM не поддерживают резервное копирование с хранилищ LVM ввиду ограничений самой платформы - моментальные снимки на хранилищах этого типа невозможны.
3. Резервное копирование доступно лишь для виртуальных машин в пределах той локации, в которой развернуто виртуальное устройство. Если виртуальное устройство расположено на любом хосте в пределах одной локации, резервное копирование доступно для:
   - виртуальных машин, расположенных на всех хранилищах того же хоста;
   - всех виртуальных машин, которые находятся на сетевых хранилищах всех хостов в пределах этой локации.
4. Виртуальные машины, являющиеся "тонким клоном", можно восстановить только в новые ВМ.

Настройка LDAP-аутентификации для агента для SpaceVM

Если система виртуализации использует службу каталогов для аутентификации пользователей, то перед развертыванием агента выполните дополнительную настройку службы:

1. В веб-панели управления системой виртуализации перейдите в раздел **Безопасность** > **Службы каталогов**.
2. Щелкните по имени службы каталогов и перейдите в раздел **Соответствия**.
3. Нажмите **Добавить соответствие** и выполните следующие действия в окне **Добавление соответствия**:
   a. Укажите имя для соответствия.
   b. Выберите роли **Администратор** и **Администратор безопасности**.
   c. [Необязательно] Введите описание соответствия.
   d. Нажмите **Добавить объекты LDAP** и добавьте LDAP-объект, представляющий пользователя, от имени которого агент будет выполнять операции резервного копирования и восстановления в системе виртуализации. При необходимости можно добавить LDAP-объект, представляющий группу, в которую входит требуемый пользователь.
   Чтобы просмотреть дочерние LDAP-объекты некоторого LDAP-объекта, щелкните по его имени в списке. Чтобы добавить LDAP-объект, поставьте галочку рядом с его именем и нажмите **OK**.
   Пример для Active Directory:

© ООО Киберпротект, 2026



e. Нажмите **OK**, чтобы завершить создание соответствия.

4. Убедитесь, что пользователь, для которого создано соответствие, может войти в веб-панель управления системой виртуализации и обладает в ней указанными ролями.

Установка агента для SpaceVM

Чтобы установить агент для SpaceVM, выполните следующие действия:

1. Загрузите **Пакет установки агента для SpaceVM** (архив формата ZIP) с сайта Киберпротект и извлеките из архива файл пакета (например, xxx.ova).
2. Войдите в систему SpaceVM через браузер.
3. В консоли управления SpaceVM в меню слева перейдите в раздел **Хранилища** > **Файлы**.
4. В верхнем меню выберите **Загрузить из файловой системы**.
5. В файловой системе выберите распакованный на первом шаге файл, далее выберите пул данных, по возможности доступный на всех хостах, и нажмите **OK**.
6. После завершения загрузки файла нажатием на имя файла раскройте его свойства.
7. В верхнем меню выберите **Обновить информацию**, подтвердите свое решение нажатием на кнопку **Да**.
8. В верхнем меню выберите **Конфигурация копии ВМ**.
9. В открывшемся окне выберите **Восстановление ВМ**, укажите узел, на который вы хотите восстановить виртуальную машину, нажмите **OK**.
10. После завершения создания виртуальной машины на указанном узле в меню слева перейдите в раздел **Виртуальные машины**.
11. В списке виртуальных машин выберите созданную виртуальную машину. Имя виртуальной машины по умолчанию CyberBackup_Agent_for_SpaceVM. Если вы планируете развернуть несколько виртуальных машин, рекомендуется переименовать каждую из них.
12. В открывшемся окне запустите эту виртуальную машину нажатием на стрелку в верхнем меню.
13. Подключитесь к консоли виртуальной машины: на мини-экране ВМ выберите **VNC** или **Spice**.
14. После завершения запуска виртуальной машины в консоли переходите по ссылкам **Change...** для настройки параметров:

© ООО Киберпротект, 2026

a. Укажите адрес контроллера SpaceVM (например, https://space.my-company.ru), имя пользователя (например, admin) и пароль доступа к SpaceVM.

   Если система SpaceVM использует службу каталогов для аутентификации пользователей, установите флажок **Use LDAP-authentication**.

   Нажмите **Check connection**, чтобы проверить соединение. Ошибки при подключении могут указывать как на некорректность введенных данных, так и на проблемы с сетью.

b. Укажите имя или IP-адрес сервера управления – компьютера, на котором установлено решение Кибер Бэкап, имя пользователя и пароль доступа к нему.

c. Если необходимо, задайте параметры сетевого интерфейса Eth0 (IP-адрес, маску сети, шлюз и DNS). По умолчанию используется DHCP.

d. Если вы планируете развернуть несколько агентов для SpaceVM, измените имя агента для SpaceVM. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.

e. Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

15. При необходимости установите агент на других серверах, выполняя шаги установки из этой инструкции.

Выполненные действия должны привести к следующим результатам:

- В веб-консоли Кибер Бэкап в разделе **Настройки** > **Агенты** отобразится агент для SpaceVM;
- В веб-консоли Кибер Бэкап в разделе **Устройства** появятся устройства SpaceVM.

2.6.4.7 Ручная установка агента для ECP VeiL

Для развертывания агента для ECP VeiL и настройки его интеграции с Кибер Бэкап вам понадобятся установленные и настроенные системы:

- Система ECP VeiL версии с 4.7 по 5.1.10
- Решение Кибер Бэкап.

Планирование количества агентов для ECP VeiL

Чтобы создавать резервные копии всех виртуальных машин, как правило, нужно развернуть несколько агентов для ECP VeiL. Это связано с тем, что агенты могут получить доступ только к пулам данных, подключенным к серверу (хосту), на котором развернут агент.

Если вы используете только локальные пулы данных, разверните по одному агенту для ECP VeiL на каждом сервере.

Если вы используете общие пулы данных, доступные на всех серверах, достаточно развернуть один агент для ECP VeiL.

Дополнительные агенты также могут потребоваться в ситуации, когда в системе имеется очень большое число виртуальных машин, и суммарное время создания резервных копий окажется слишком большим.

© ООО Киберпротект, 2026

Процедура развертывания

Выполняйте действия по развертыванию агента для ECP VeiL в следующем порядке:

1. "Установка сервера управления" (стр. 63).
2. "Установка агента для ECP VeiL" (стр. 120).
3. "Создание плана защиты" (стр. 224).

Известные проблемы и ограничения

1. Текущие версии платформы ECP VeiL не позволяют осуществлять резервное копирование следующих типов виртуальных машин:
   - виртуальные машины, являющиеся "тонким клоном", в которых уже после операции создания "тонкого клона" был изменен набор дисков;
   - виртуальные машины с SCSI-контроллером типа lsilogic.
2. Текущие версии платформы ECP VeiL не поддерживают резервное копирование с хранилищ LVM ввиду ограничений самой платформы - моментальные снимки на хранилищах этого типа невозможны.
3. Версии ECP VeiL 4.x.x не поддерживают резервное копирование виртуальных машин, которые расположены на пулах хранения ZFS. Поддержка резервного копирования таких виртуальных машин реализована в ECP VeiL, начиная с версии 5.1.4.
4. Резервное копирование доступно лишь для виртуальных машин в пределах той локации, в которой развернуто виртуальное устройство. Если виртуальное устройство расположено на любом хосте в пределах одной локации, резервное копирование доступно для:
   - виртуальных машин, расположенных на всех хранилищах того же хоста;
   - всех виртуальных машин, которые находятся на сетевых хранилищах всех хостов в пределах этой локации.

Если вышеперечисленные ограничения являются для вас критичными, пожалуйста, обратитесь в службу поддержки НИИ «Масштаб».

Настройка LDAP-аутентификации для агента для ECP Veil

Если система виртуализации использует службу каталогов для аутентификации пользователей, то перед развертыванием агента выполните дополнительную настройку службы:

1. В веб-панели управления системой виртуализации перейдите в раздел **Безопасность** > **Службы каталогов**.
2. Щелкните по имени службы каталогов и перейдите в раздел **Соответствия**.
3. Нажмите **Добавить соответствие** и выполните следующие действия в окне **Добавление соответствия**:
   a. Укажите имя для соответствия.
   b. Выберите роли **Администратор** и **Администратор безопасности**.

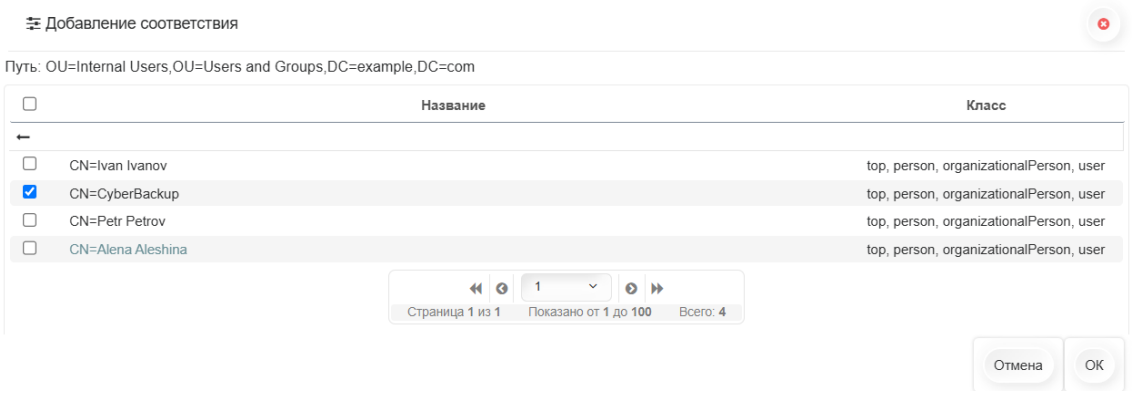
© ООО Киберпротект, 2026

c. [Необязательно] Введите описание соответствия.

d. Нажмите **Добавить объекты LDAP** и добавьте LDAP-объект, представляющий пользователя, от имени которого агент будет выполнять операции резервного копирования и восстановления в системе виртуализации. При необходимости можно добавить LDAP-объект, представляющий группу, в которую входит требуемый пользователь.

   Чтобы просмотреть дочерние LDAP-объекты некоторого LDAP-объекта, щелкните по его имени в списке. Чтобы добавить LDAP-объект, поставьте галочку рядом с его именем и нажмите **OK**.

   Пример для Active Directory:



e. Нажмите **OK**, чтобы завершить создание соответствия.

4. Убедитесь, что пользователь, для которого создано соответствие, может войти в веб-панель управления системой виртуализации и обладает в ней указанными ролями.

Установка агента для ECP VeiL

Чтобы установить агент для ECP VeiL, выполните следующие действия:

1. Загрузите **Пакет установки агента для ECP VeiL** (архив формата ZIP), с сайта Киберпротект и извлеките из архива файл пакета (например, xxx.ova).
2. Войдите в систему ECP VeiL через браузер.
3. В консоли управления ECP VeiL в меню слева перейдите в раздел **Хранилища** > **Файлы**.
4. В верхнем меню выберите **Загрузить из файловой системы**.
5. В файловой системе выберите распакованный на первом шаге файл, далее выберите пул данных, по возможности доступный на всех хостах, и нажмите **OK**.
6. После завершения загрузки файла нажатием на имя файла раскройте его свойства.
7. В верхнем меню выберите **Обновить информацию**, подтвердите свое решение нажатием на кнопку **Да**.
8. В верхнем меню выберите **Конфигурация копии ВМ**.
9. В открывшемся окне выберите **Восстановление ВМ**, укажите узел, на который вы хотите восстановить виртуальную машину, нажмите кнопку **Отправить**.
10. После завершения создания виртуальной машины на указанном узле в меню слева перейдите в раздел **Виртуальные машины**.

© ООО Киберпротект, 2026

11. В списке виртуальных машин выберите созданную виртуальную машину. Имя виртуальной машины по умолчанию CyberBackup_Agent_for_ECP_VeiL. Если вы планируете развернуть несколько виртуальных машин, рекомендуется переименовать каждую из них.
12. В открывшемся окне запустите эту виртуальную машину нажатием на стрелку в верхнем меню.
13. Подключитесь к консоли виртуальной машины: на мини-экране ВМ выберите **VNC** или **Spice**.
14. После завершения запуска виртуальной машины в консоли переходите по ссылкам **Change...** для настройки параметров:
    a. Укажите адрес контроллера ECP VeiL (например, https://my-veil.my-company.ru), имя пользователя (например, admin) и пароль доступа к ECP VeiL.

       Если система ECP Veil использует службу каталогов для аутентификации пользователей, установите флажок **Use LDAP-authentication**.

       Нажмите **Check connection**, чтобы проверить соединение. Ошибки при подключении могут указывать как на некорректность введенных данных, так и на проблемы с сетью.
    b. Укажите имя или IP-адрес сервера управления – компьютера, на котором установлено решение Кибер Бэкап, имя пользователя и пароль доступа к нему.
    c. Если необходимо, задайте параметры сетевого интерфейса Eth0 (IP-адрес, маску сети, шлюз и DNS). По умолчанию используется DHCP.
    d. Если вы планируете развернуть несколько агентов для ECP VeiL, измените имя агента для ECP VeiL. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.
    e. Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.
15. При необходимости установите агент на других серверах, выполняя шаги установки из этой инструкции.

Выполненные действия должны привести к следующим результатам:

- В веб-консоли Кибер Бэкап в разделе **Настройки** > **Агенты** отобразится агент для ECP VeiL;
- В веб-консоли Кибер Бэкап в разделе **Устройства** появятся устройства ECP VeiL.

2.6.4.8 Установка агента для OpenStack

Общие сведения

Кибер Бэкап поддерживает резервное копирование и восстановление виртуальных машин OpenStack и РУСТЭК.

Резервная копия такой виртуальной машины содержит ее параметры и моментальный снимок ее дисков. Такую резервную копию можно восстановить на любой совместимый по версии хост. Восстановление будет выполнено в новую виртуальную машину, которая будет создана с необходимыми параметрами и к которой будут подключены моментальные снимки дисков.

Поддерживаемые конфигурации

Вам понадобятся установленные и настроенные системы:

© ООО Киберпротект, 2026

- Решение Кибер Бэкап 16 или новее.
- Одна из следующих платформ виртуализации:
  - OpenStack;
  - РУСТЭК.

    Подробнее о поддерживаемых версиях платформ виртуализации см. раздел "Поддерживаемые платформы виртуализации" (стр. 29).

Планирование количества агентов

Если в системе имеется очень большое число виртуальных машин, то суммарное время создания резервных копий может быть слишком велико. В этом случае можно развернуть несколько виртуальных устройств с агентами на одном проекте OpenStack или РУСТЭК.

Производительность резервного копирования одного агента можно настроить с помощью параметра **Планирование** плана защиты (см. "Планирование" (стр. 370)).

Установка

Для работы Кибер Бэкап с платформами виртуализации OpenStack и РУСТЭК необходимо установить агент для OpenStack. В процессе установки происходит добавление хоста OpenStack (или РУСТЭК) на сервер управления Кибер Бэкап и развертывание на хосте виртуального устройства (виртуальная машина с агентом Кибер Бэкап).

Порядок установки для OpenStack

1. Установка агента для OpenStack в автоматическом режиме или вручную.

Порядок установки для РУСТЭК

1. Подготовка хостов РУСТЭК.
2. Установка агента для OpenStack в автоматическом режиме или вручную.

Известные проблемы и ограничения

- Не поддерживается резервное копирование виртуальных машин с эфемерными дисками.
- Не поддерживается восстановление в текущую виртуальную машину.

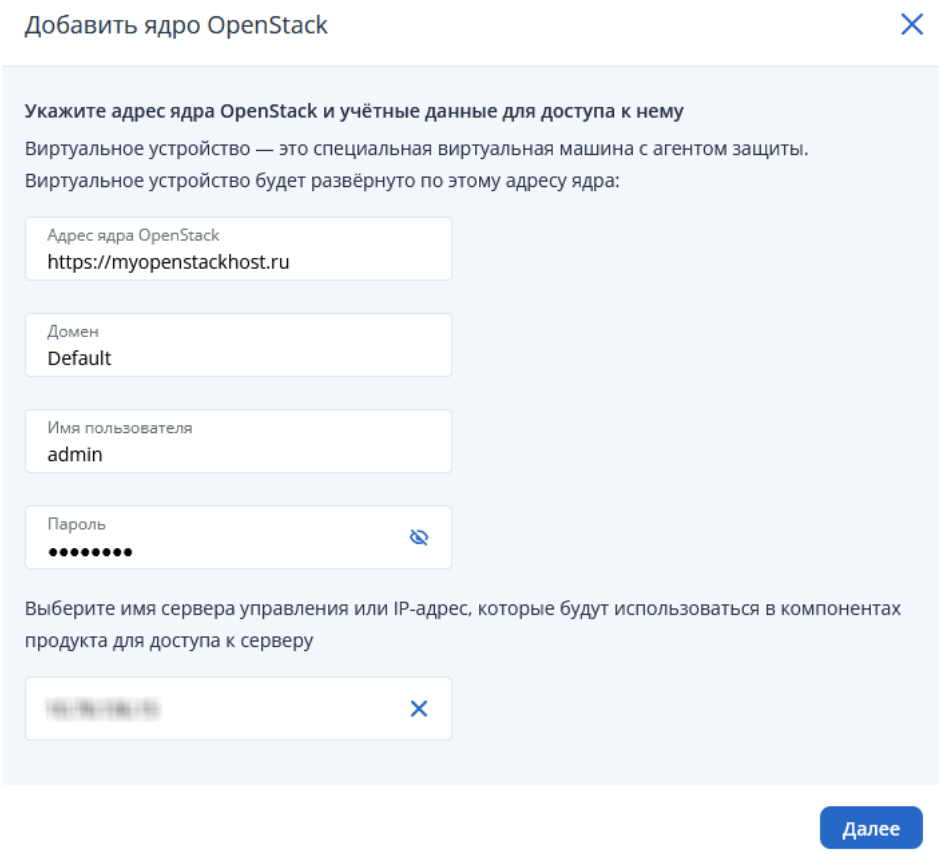
Автоматическая установка агента для OpenStack

Примечание
При установке агента для OpenStack для РУСТЭК вначале необходимо выполнить подготовку хоста РУСТЭК.

Для автоматической установки агента выполните следующие шаги в веб-интерфейсе Кибер Бэкап:

© ООО Киберпротект, 2026

1. На вкладке **УСТРОЙСТВА** > **Физические и виртуальные машины** щелкните **Добавить**. Появится окно **Добавить устройства**.
2. В разделе **ХОСТЫ ВИРТУАЛИЗАЦИИ** щелкните **OpenStack**. Откроется окно **Добавить ядро OpenStack**.

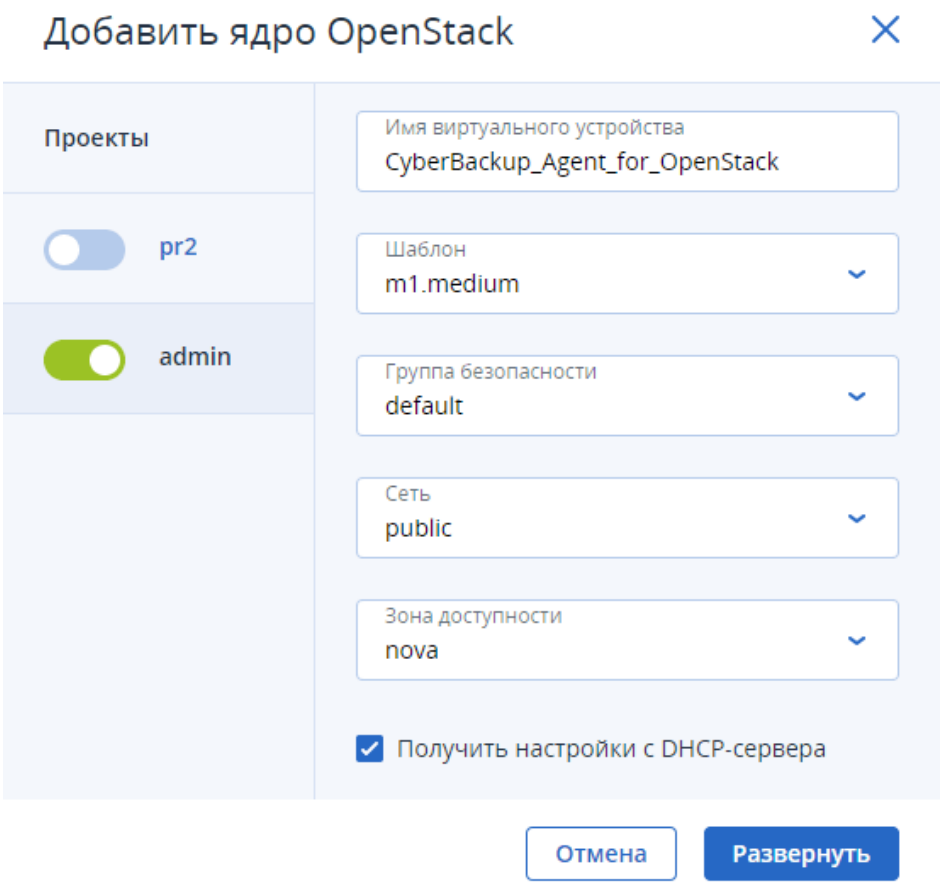


3. В поле **Адрес ядра OpenStack** укажите адрес хоста OpenStack (РУСТЭК) с префиксом протокола. Например, https://myopenstackhost.ru/. Поддерживаются протоколы HTTP и HTTPS. Вдобавок можно указать порт, например, https://myopenstackhost.ru:12345 (по умолчанию используется порт 5000) или токен, например, https://myopenstackhost.ru/identity.
4. В поле **Домен** укажите домен с проектами, в которых находятся требуемые виртуальные машины.
5. В соответствующих полях укажите имя пользователя и пароль администратора проектов с требуемыми виртуальными машинами.
6. В выпадающем списке выберите сервер управления Кибер Бэкап, к которому будет подключен устанавливаемый агент. При этом, если сервер управления находится в одном домене Active Directory с хостом OpenStack (РУСТЭК), его можно выбрать по имени. В остальных случаях его необходимо выбрать по IP-адресу.
7. Укажите дополнительные параметры, щелкнув **Далее** внизу справа. Появится список проектов в указанном домене хоста. Ползунками отметьте необходимые. Для каждого из отмеченных проектов будет создано свое виртуальное устройство. Щелкнув название проекта, можно выбрать параметры соответствующего виртуального устройства:

© ООО Киберпротект, 2026

- **Имя**. Должно удовлетворять требованиям к именам виртуальных машин OpenStack (РУСТЭК).
- **Шаблон (Flavor)**. Необходимо минимум 4 ГБ ОЗУ, 2 ядра ЦП и 8 ГБ дискового пространства.
- **Группа безопасности**. Должна разрешать подключения к указанному серверу управления по протоколам TCP и ICMP.
- **Сеть**. Должна обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап и с контроллером OpenStack (РУСТЭК) через конечную точку (endpoint) identity (keystone). При необходимости можно снять флажок **Получить настройки с DHCP-сервера** и указать параметры сети вручную.
- **Зона доступности**.

Например:



8. Указав необходимые параметры, нажмите **Развернуть**.

На указанном хосте будет создано виртуальное устройство, в которое будет установлен агент. При этом архив агента с именем "OpenStackAppliance_v<версия>.zip" будет загружен с официального сайта Киберпротект. Если это невозможно, архив агента будет взят локально с машины, на которой установлен сервер управления: из директории C:\ProgramData\Acronis\VaDeployer\va-images на ОС Windows и из директории /var/lib/Acronis/VaDeployer/va-images на ОС Linux.

© ООО Киберпротект, 2026

Запустившись автоматически, агент подключится к серверу управления, и виртуальные машины из выбранных проектов на хосте OpenStack (РУСТЭК) отобразятся в списке **УСТРОЙСТВА** > **OpenStack**. После этого их можно будет добавлять к планам защиты обычным способом.

Примечание
В планах защиты таких виртуальных машин необходимо отключать функцию **Active Protection** (**Активная защита**).

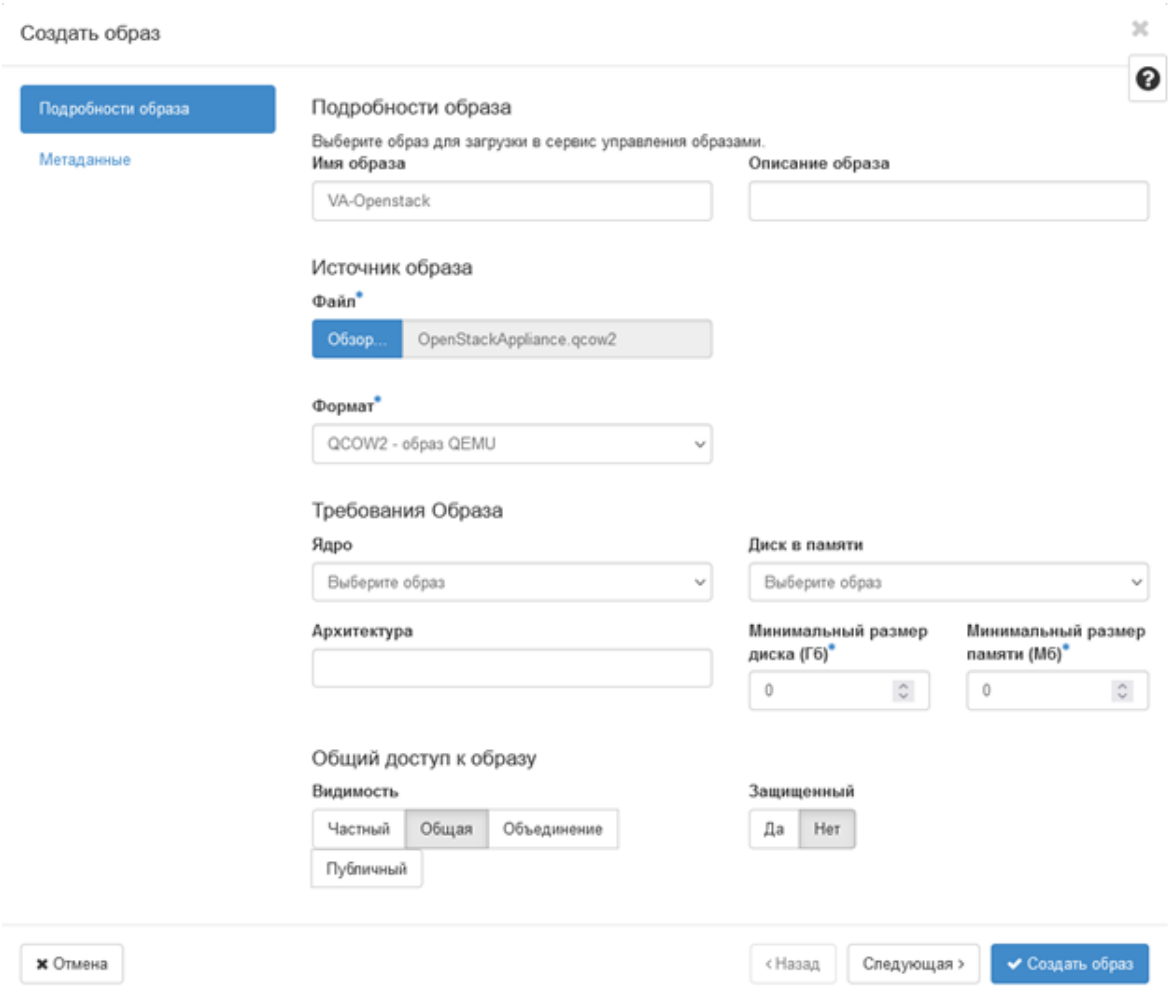
Установка агента для OpenStack вручную

Примечание
При установке агента для OpenStack для РУСТЭК вначале необходимо выполнить подготовку хоста РУСТЭК.

Чтобы установить агент для OpenStack вручную, выполните следующие шаги:

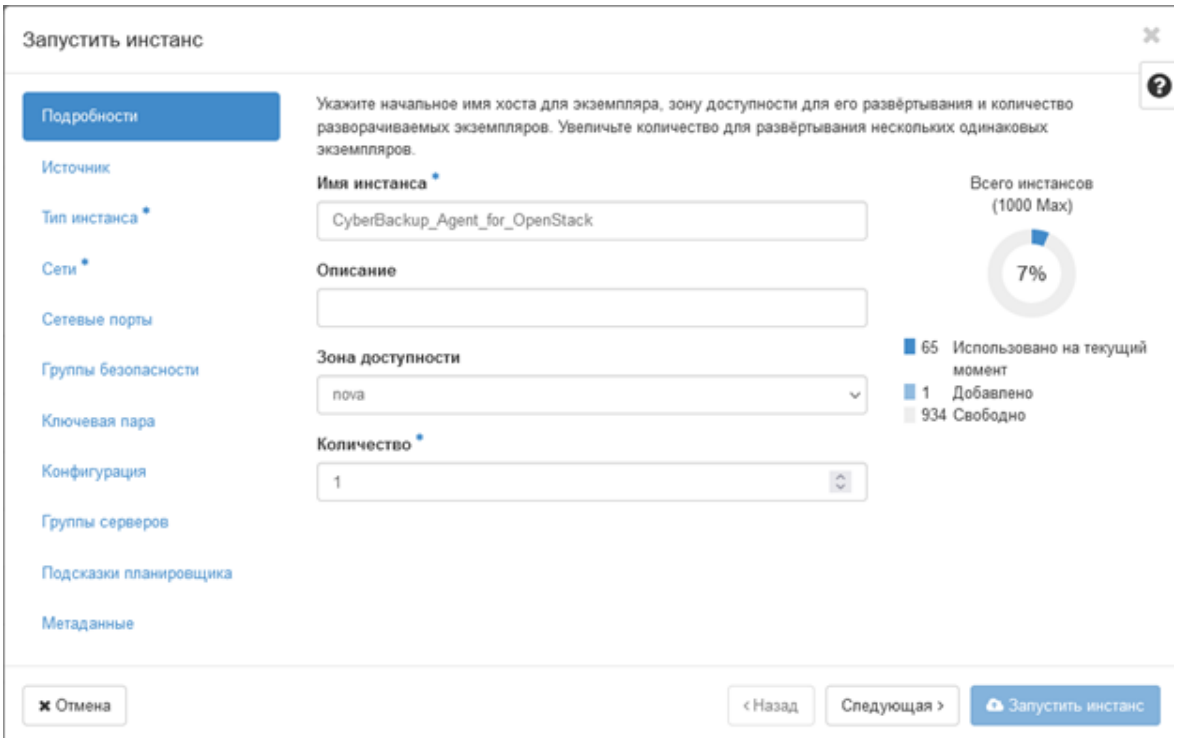
1. Загрузите **Пакет установки агента для OpenStack** с сайта Киберпротект.
2. Распакуйте образ виртуального устройства (например, OpenStackAppliance.qcow2).
3. В панели управления OpenStack перейдите на вкладку **Вычислительные ресурсы** > **Образы** и нажмите **Создать образ**.
4. В поле **Источник образа** укажите путь к распакованному образу виртуального устройства.

© ООО Киберпротект, 2026

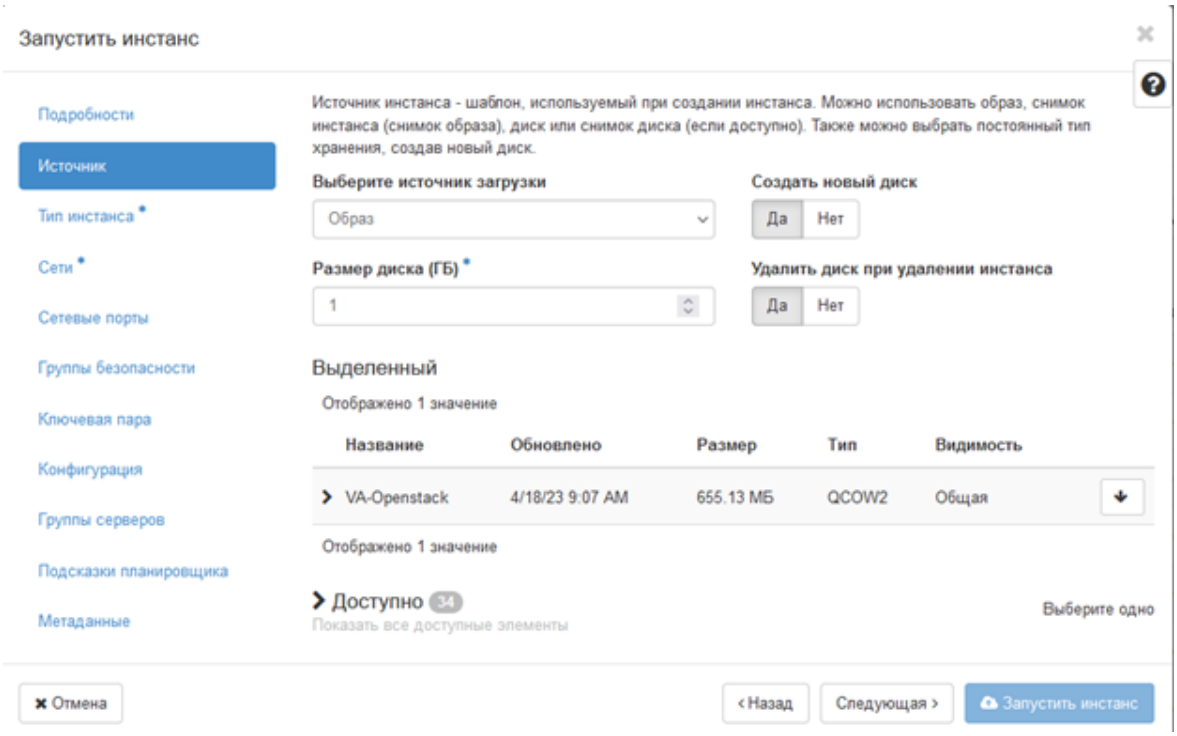


5. В поле **Формат** выберите **QCOW2 - образ QEMU**. По окончании ввода данных нажмите **Создать образ**.
6. Перейдите на вкладку **Вычислительные ресурсы** > **Инстансы** и выберите **Запустить инстанс**.

© ООО Киберпротект, 2026

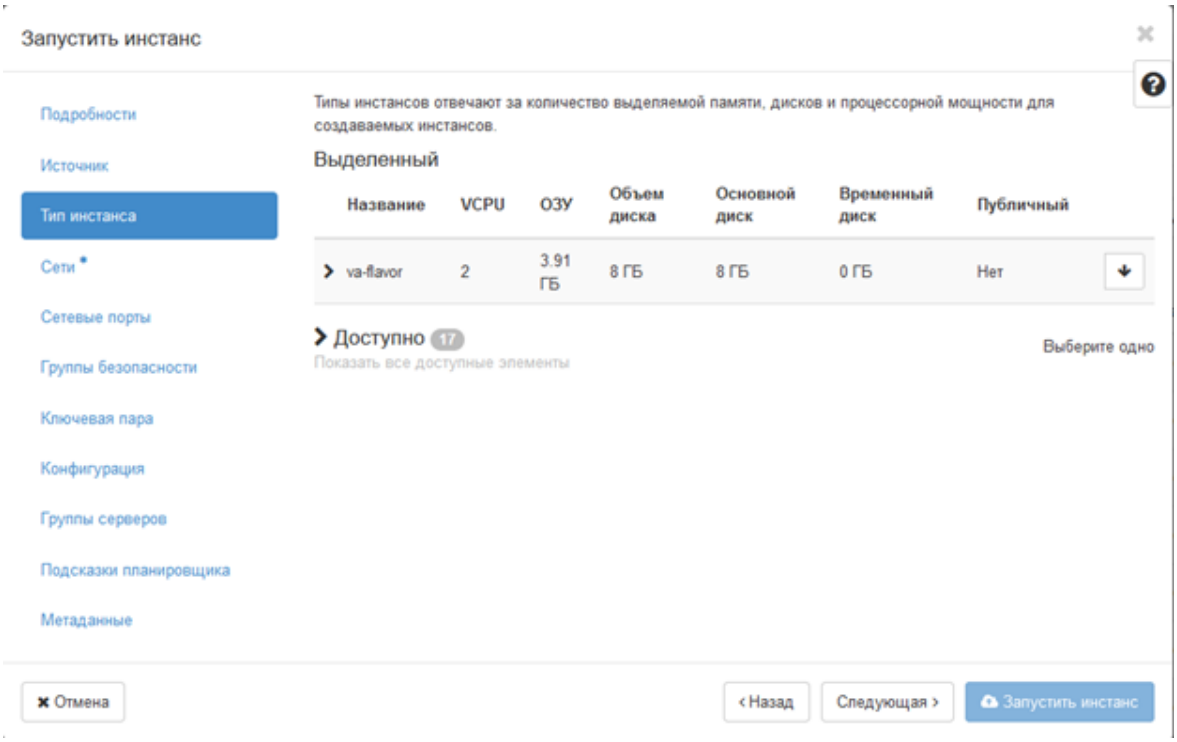


7. Укажите имя инстанса и зону доступности.
8. Выберите источник загрузки **Образ** и укажите образ виртуального устройства.

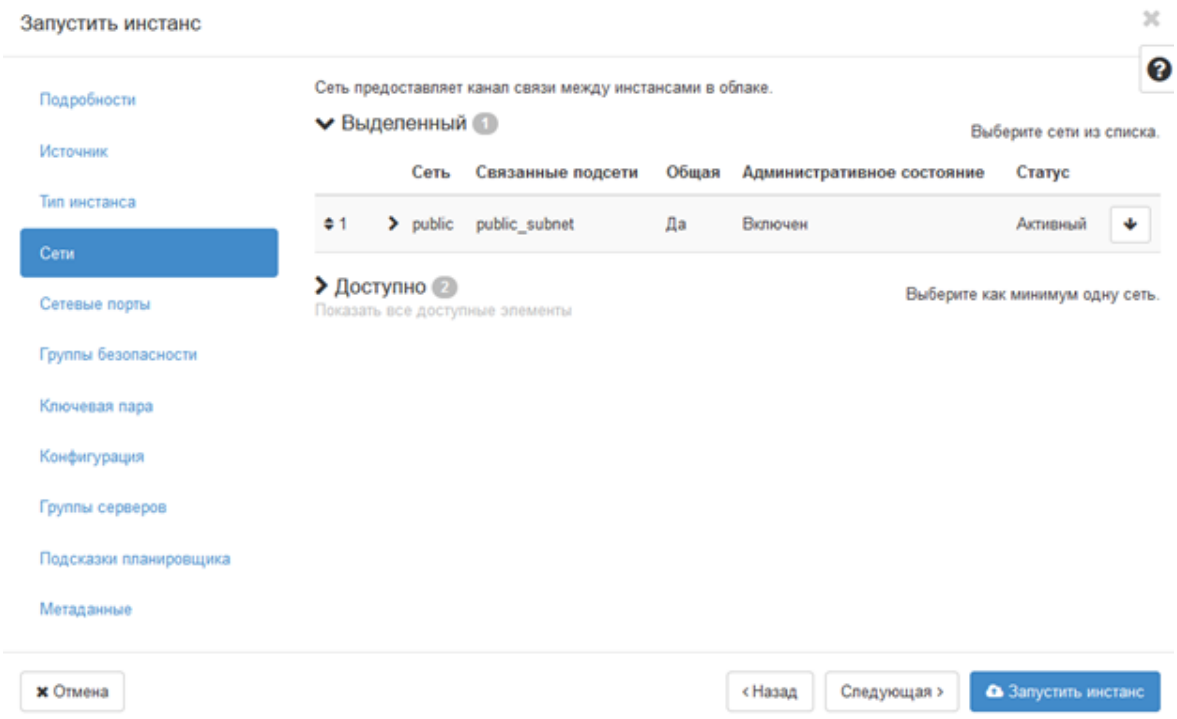


9. Укажите параметры виртуальной машины на вкладке **Тип инстанса**. Для промышленных сборок рекомендуется указывать не менее 2 ЦП и не менее 4 ГБ памяти.

© ООО Киберпротект, 2026



10. На вкладке **Сети** укажите подходящие сеть и группу безопасности. Сеть должна обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап и с контроллером OpenStack через конечную точку (endpoint) identity (keystone). Группа должна разрешать подключения к серверу управления по протоколам TCP и ICMP.



11. По окончании ввода данных нажмите **Запустить инстанс**.
12. Перейдите на экран **Вычислительные ресурсы** > **Инстансы** и убедитесь, что имя машины с агентом появилось в списке виртуальных машин.

© ООО Киберпротект, 2026

13. Дождитесь запуска ВМ, откройте ее консоль и задайте параметры агента:
    - **OpenStack**. Укажите адрес хоста-контроллера OpenStack с префиксом протокола. Например, https://myopenstackhost.ru/. Поддерживаются протоколы HTTP и HTTPS. Вдобавок можно указать порт, например, https://myopenstackhost.ru:12345 (по умолчанию используется порт 5000) или токен, например, https://myopenstackhost.ru/identity.

      Кроме того, укажите домен с проектами, в которых находятся требуемые виртуальные машины. В соответствующих полях укажите имя пользователя и пароль администратора проектов с требуемыми виртуальными машинами.
    - **Management Server**. Укажите DNS-имя или IP-адрес сервера управления Кибер Бэкап, имя пользователя и пароль.
    - **Eth0**. Если необходимо, задайте параметры сетевого интерфейса, который будет использоваться агентом (IP-адрес, маску сети, шлюз, DNS-серверы и WINS-серверы). По умолчанию используется автоконфигурация посредством DHCP.
    - **Name**. Если необходимо, измените имя агента. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.
    - **Time zone**. Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

Выполненные действия должны привести к следующим результатам:

- В разделе **Настройки** > **Агенты** отобразится агент для OpenStack.
- В веб-консоли Кибер Бэкап в разделе **Устройства** появится подраздел **OpenStack**.

Подготовка хостов РУСТЭК к установке агента

Перед установкой агента на хост РУСТЭК необходимо добавить на этот хост политики для новой роли "cyberbackup" и создать пользователя с этой ролью.

Выполните следующие шаги:

- Загрузите архив cyberbackup-policy.tar.bz2 на один из узлов платформы РУСТЭК и распакуйте его:

  ```
  # tar -xvf cyberbackup-policy.tar.bz2
  ```

- Выполните сценарий Ansible из архива:

  ```
  # ansible-playbook -i /var/lib/rustack-ansible/inventory.yml cyberbackup-policy/main.yml -vv
  ```

- Примените новые политики, запустив конфигуратор РУСТЭК:

  ```
  rustackctl
  ```

- Выберите пункт меню **Изменить политики служб**.

© ООО Киберпротект, 2026

- После завершения процедуры вручную создайте пользователя "cyberbackup" с новой ролью "cyberbackup" в проекте "cyberbackup":

  ```
  # openstack project create --os-cloud rustack_system --domain default cyberbackup
  # openstack user create --os-cloud rustack_system --password <passwd> --enable --project cyberbackup --domain default cyberbackup
  # openstack role add --os-cloud rustack_system --user cyberbackup --project cyberbackup cyberbackup
  ```

  где <passwd> – пароль для пользователя "cyberbackup".
- При необходимости откройте этому пользователю полный доступ через портал:

  ```
  # openstack role add --os-cloud rustack_system --user cyberbackup --user-domain default --system all cyberbackup
  # openstack role add --os-cloud rustack_system --user cyberbackup --user-domain default --domain default cyberbackup
  # openstack role add --os-cloud rustack_system --user cyberbackup --user-domain default --domain default --inherited cyberbackup
  ```

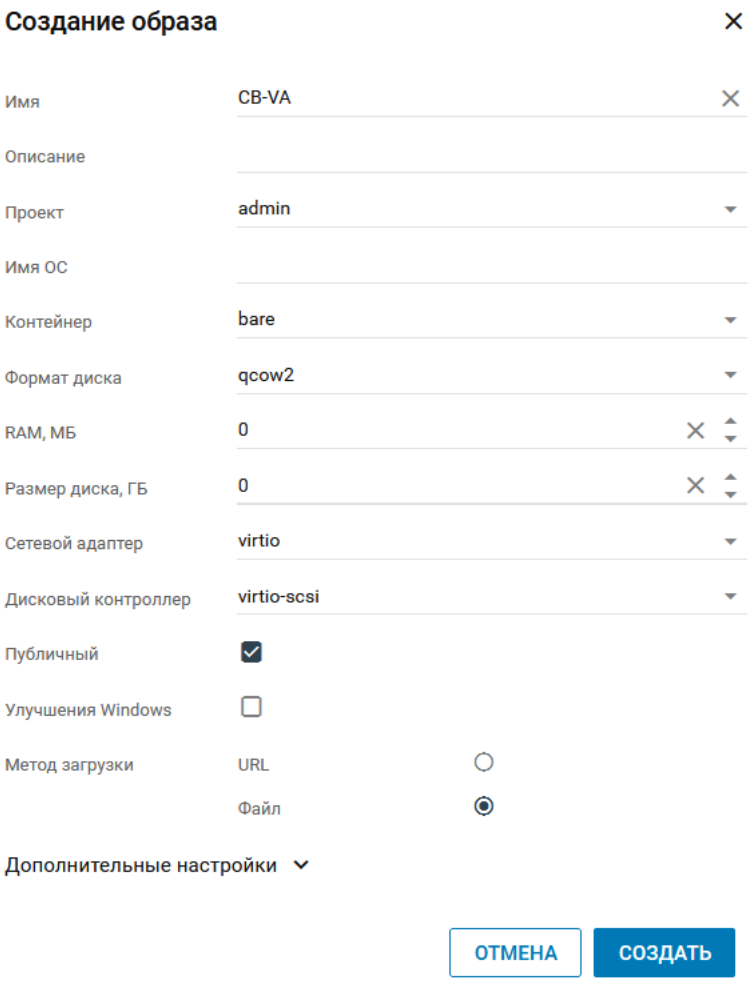
Установка агента для РУСТЭК вручную

Чтобы установить агент для РУСТЭК вручную, выполните следующие шаги:

1. Загрузите **Пакет установки агента для OpenStack** с сайта Киберпротект.
2. Распакуйте образ виртуального устройства (например, OpenStackAppliance.qcow2).
3. В панели управления РУСТЭК перейдите в раздел **Копии и образы** > **Образы** и нажмите **Создать**.
4. В окне **Создание образа** задайте параметры образа:
   - В поле **Имя** введите имя образа.
   - Убедитесь, что в поле **Формат диска** выбрано значение **qcow2**.
   - В поле **Метод загрузки** выберите значение **Файл**.

   По окончании ввода данных нажмите **Создать**.

© ООО Киберпротект, 2026



5. В списке образов выберите созданный образ и нажмите **Загрузить образ**.
6. В окне **Загрузка образа** укажите путь к распакованному образу виртуального устройства и нажмите **Загрузить**.
7. Перейдите в раздел **Виртуальные машины** и нажмите **Создать**.
8. В окне **Создание виртуальной машины** задайте параметры виртуальной машины (ВМ):
   - В поле **Имя** введите имя ВМ.
   - В поле **ОС** укажите образ виртуального устройства.
   - В поле **Конфигурация** выберите конфигурацию ВМ. Для промышленных сред рекомендуется выбирать конфигурации, в которых указано не менее 4 ЦП и не менее 4 ГБ памяти.
   - В поле **Размер диска** укажите размер диска ВМ. Для промышленных сред рекомендуется указывать не менее 8 ГБ.
   - В поле **Сети** выберите сеть, к которой будет подключена ВМ. Сеть должна обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап и с контроллером РУСТЭК через конечную точку (endpoint) identity (keystone).
   - В поле **Профили безопасности** укажите профиль, разрешающий подключение ВМ к серверу управления по протоколам TCP и ICMP.

   По окончании ввода данных нажмите **Создать**.

© ООО Киберпротект, 2026

9. Перейдите в раздел **Виртуальные машины** и убедитесь, что имя ВМ с агентом появилось в списке виртуальных машин.
10. Дождитесь запуска ВМ, откройте ее консоль и задайте параметры агента:
    - **OpenStack**. Укажите адрес хоста-контроллера РУСТЭК с префиксом протокола. Например, https://myrustackhost.ru/. Поддерживаются протоколы HTTP и HTTPS. Вдобавок можно указать порт, например, https://myrustackhost.ru:12345 (по умолчанию используется порт 5000) или токен, например, https://myrustackhost.ru/identity.

      Кроме того, укажите домен с проектами, в которых находятся требуемые виртуальные машины. В соответствующих полях укажите имя пользователя и пароль администратора проектов с требуемыми виртуальными машинами.

© ООО Киберпротект, 2026

- **Management Server**. Укажите DNS-имя или IP-адрес сервера управления Кибер Бэкап, имя пользователя и пароль.
- **Eth0**. Если необходимо, задайте параметры сетевого интерфейса, который будет использоваться агентом (IP-адрес, маску сети, шлюз, DNS-серверы и WINS-серверы). По умолчанию используется автоконфигурация посредством DHCP.
- **Name**. Если необходимо, измените имя агента. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.
- **Time zone**. Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

Выполненные действия должны привести к следующим результатам:

- В разделе **Настройки** > **Агенты** отобразится агент для OpenStack.
- В веб-консоли Кибер Бэкап в разделе **Устройства** появится подраздел **OpenStack**.

2.6.4.9 Ручная установка агента для VK Cloud

Для развертывания агента VK Cloud вам понадобятся установленные и настроенные системы:

- Платформа виртуализации VK Cloud версии 4.0;
- Решение Кибер Бэкап 17 или новее.

Перед установкой агента для VK Cloud требуется предварительная настройка пользователя VK Cloud в зависимости от типа облачной платформы.

Предварительная настройка VK Cloud

Настройка для публичной облачной платформы

В панели администратора VK Cloud убедитесь, что включен доступ к API у пользователя, который будет взаимодействовать с виртуальным устройством.

См. также документацию разработчика.

Настройка для частной облачной платформы

Выполните следующие действия:

1. Выполните авторизацию в OpenStack с помощью команды:

   ```
   source openrc.sh
   ```

2. Создайте нового пользователя, выполнив команду:

   ```
   openstack user create --password user_password user_name
   ```

   где user_password – пароль пользователя,

© ООО Киберпротект, 2026

user_name – имя пользователя.

Запомните или запишите ID пользователя.

3. Отобразите список проектов с помощью команды:

```
openstack project list
```

4. Найдите в списке нужный проект и получите информацию об этом проекте, выполнив команду:

```
openstack project show project_name
```

где project_name – название проекта.

5. Добавьте созданного пользователя в проект с правами mcs_co_owner с помощью команды:

```
openstack role add --project project_ID --project-domain project_domain_ID --user user_ID mcs_co_owner
```

где project_ID – ID проекта,

user_ID – ID пользователя.

В зависимости от вашей конфигурации, в качестве project_domain_ID выберите ID домена проекта или укажите ID домена по умолчанию: default.

См. также документацию разработчика.

Установка агента для VK Cloud

Для установки обратитесь к разделу "Установка агента для VK Cloud" (стр. 134).

Установка агента для VK Cloud

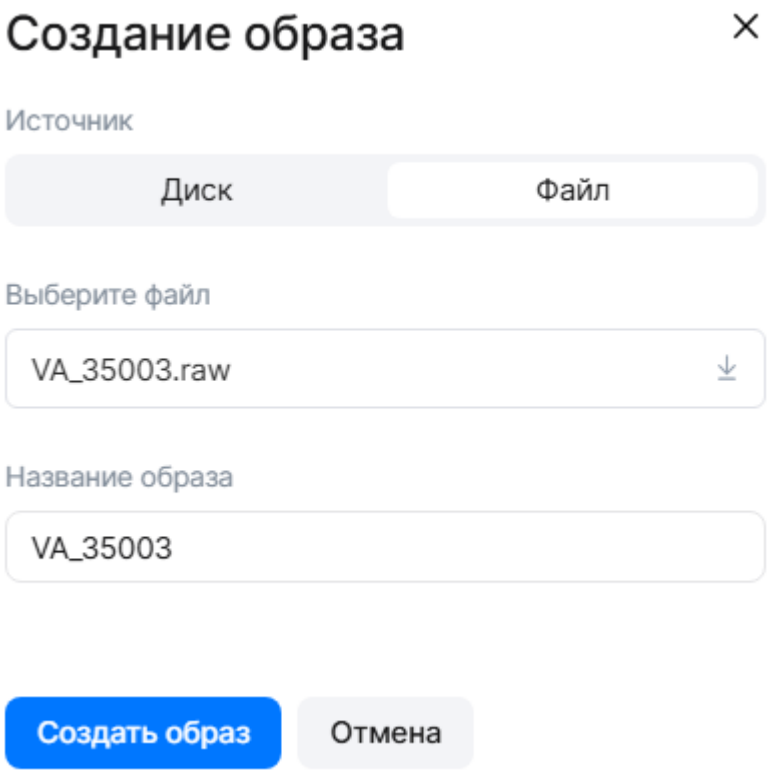
Чтобы установить агент для VK Cloud вручную, выполните следующие шаги:

1. Загрузите **Пакет установки агента для OpenStack** с сайта Киберпротект и распакуйте его.
2. Подготовьте образ виртуального устройства в формате RAW с помощью утилиты qemu-img:

```
qemu-img convert -f qcow2 -O raw OpenStackAppliance.qcow2 OpenStackAppliance.raw
```

3. Войдите в личный кабинет VK Cloud.
4. Импортируйте подготовленный образ в VK Cloud:
   a. Перейдите в раздел **Облачные вычисления** > **Образы** и нажмите **Создать**.
   b. В окне **Создание образа** укажите параметры импортируемого образа:
      i. В поле **Источник** выберите **Файл**.
      ii. В поле **Выберите файл** укажите путь к файлу образа в формате RAW.
      iii. В поле **Название образа** введите имя образа.

© ООО Киберпротект, 2026

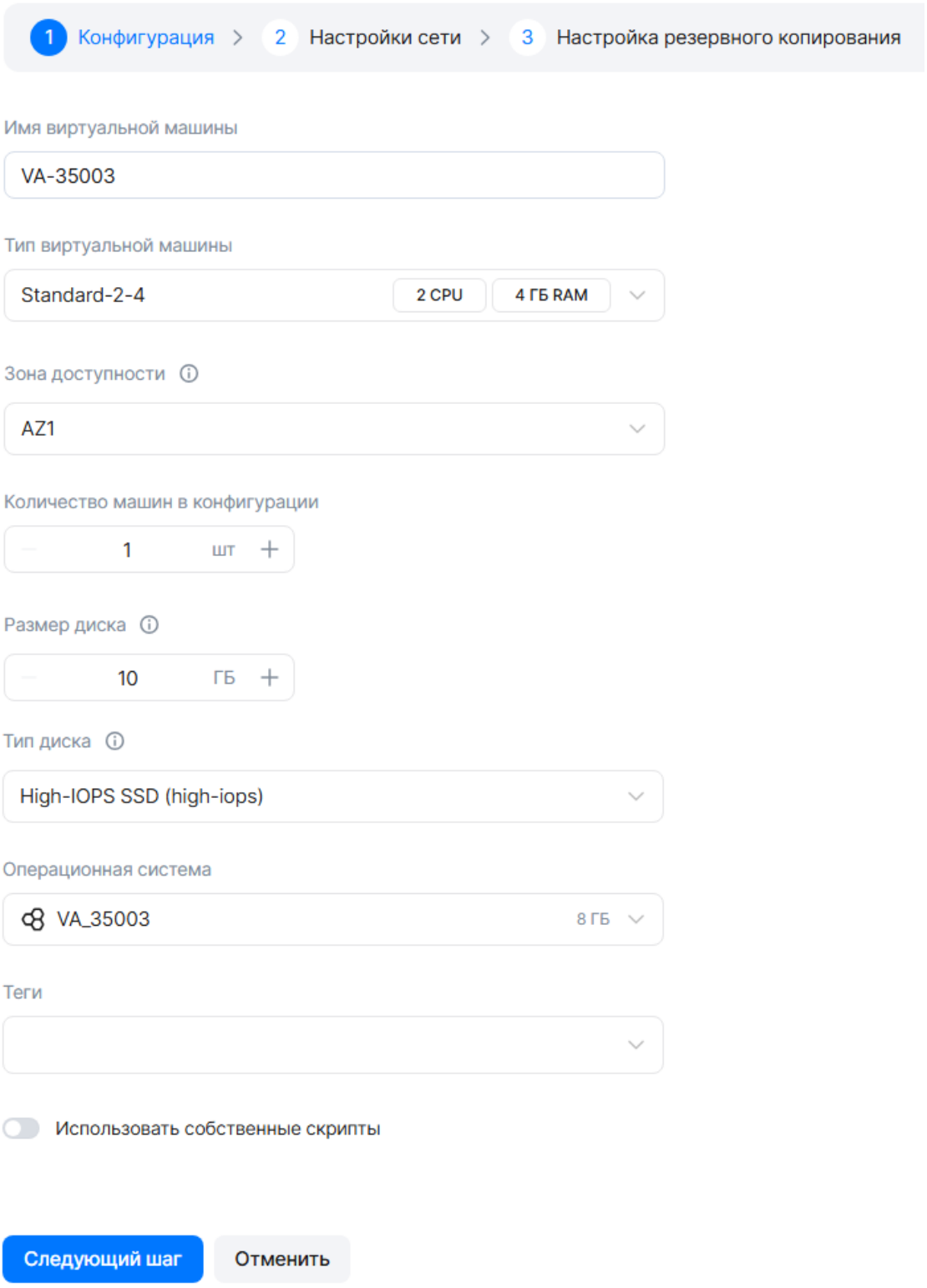


c. Нажмите **Создать образ**.

5. Создайте ВМ на основе импортированного ранее образа:
   a. Перейдите в раздел **Облачные вычисления** > **Образы**, щелкните значок многоточия рядом с образом и выберите **Создать ВМ из образа** в появившемся меню. Откроется мастер создания ВМ.
   b. На шаге **Конфигурация** укажите конфигурационные параметры ВМ:
      i. В поле **Имя виртуальной машины** введите имя ВМ.
      ii. В поле **Тип виртуальной машины** выберите тип ВМ. Для промышленной среды рекомендуется использовать тип ВМ, в котором указано не менее 2 ЦП и не менее 4 ГБ памяти.
      iii. В поле **Зона доступности** выберите необходимую зону.
      iv. В поле **Количество машин в конфигурации** укажите значение 1.
      v. В поле **Размер диска** задайте размер диска ВМ.
      vi. В поле **Тип диска** выберите тип диска ВМ.
      vii. Убедитесь, что в поле **Операционная система** выбран образ ВМ, который был импортирован ранее.

      По окончании ввода нажмите **Следующий шаг**.

© ООО Киберпротект, 2026



c. На шаге **Настройки сети** задайте сетевую конфигурацию ВМ:
   i. В поле **Сеть** выберите сеть, к которой будет подключена ВМ. Эта сеть должна обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап и с контроллером VK Cloud.

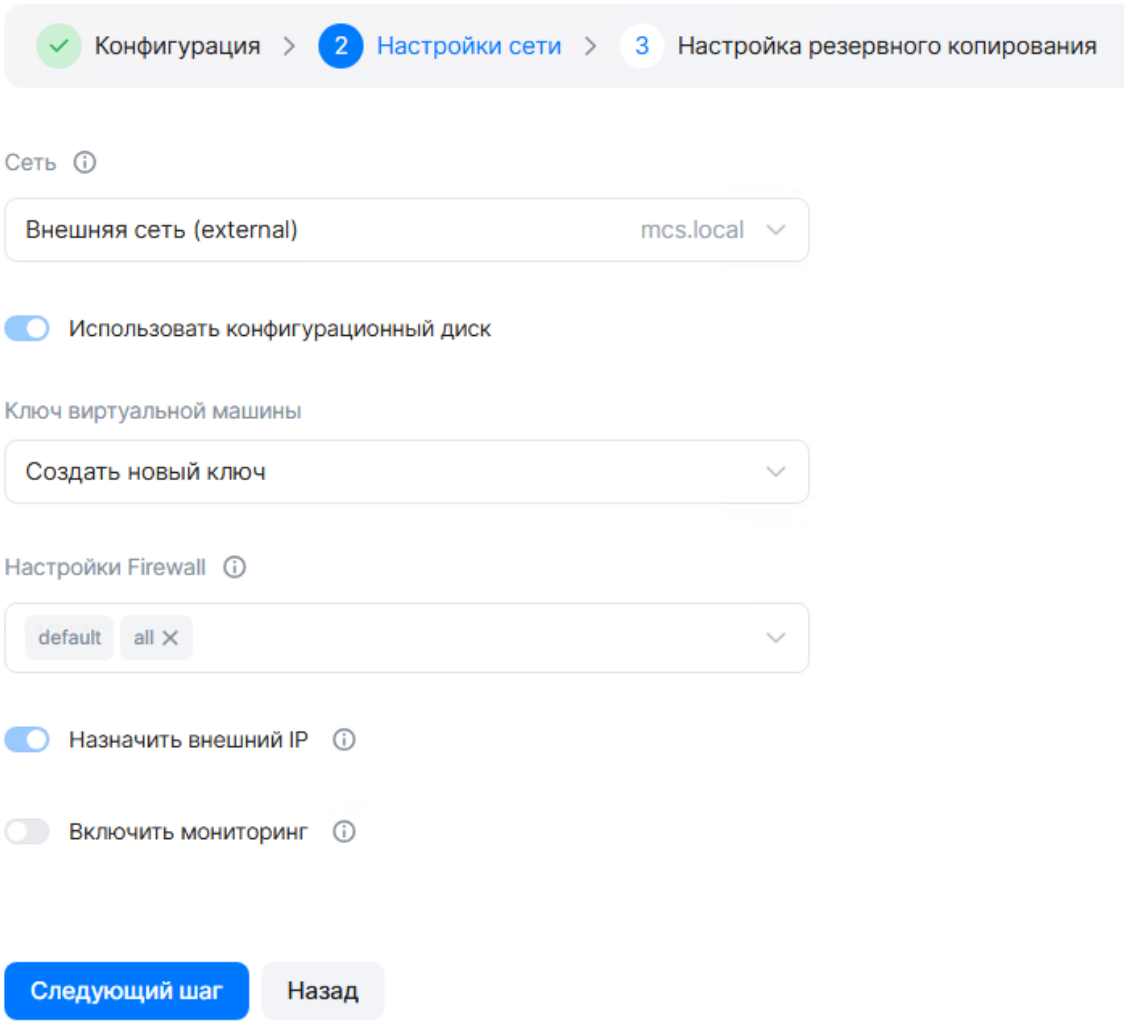
© ООО Киберпротект, 2026

ii. В поле **Ключ виртуальной машины** укажите SSH-ключ для доступа к ВМ.

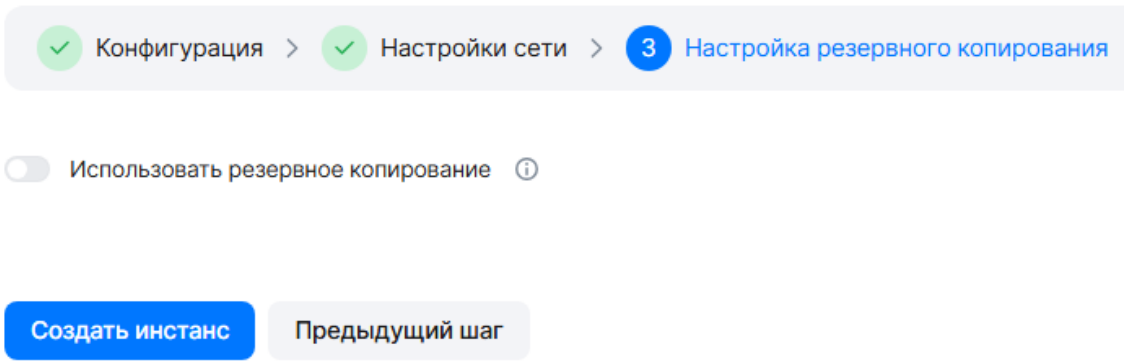
iii. В поле **Настройки Firewall** выберите группы безопасности.

iv. При необходимости передвиньте переключатель **Назначить внешний IP** в положение "вкл".

По окончании ввода нажмите **Следующий шаг**.



d. На шаге **Настройка резервного копирования** нажмите **Создать инстанс**.

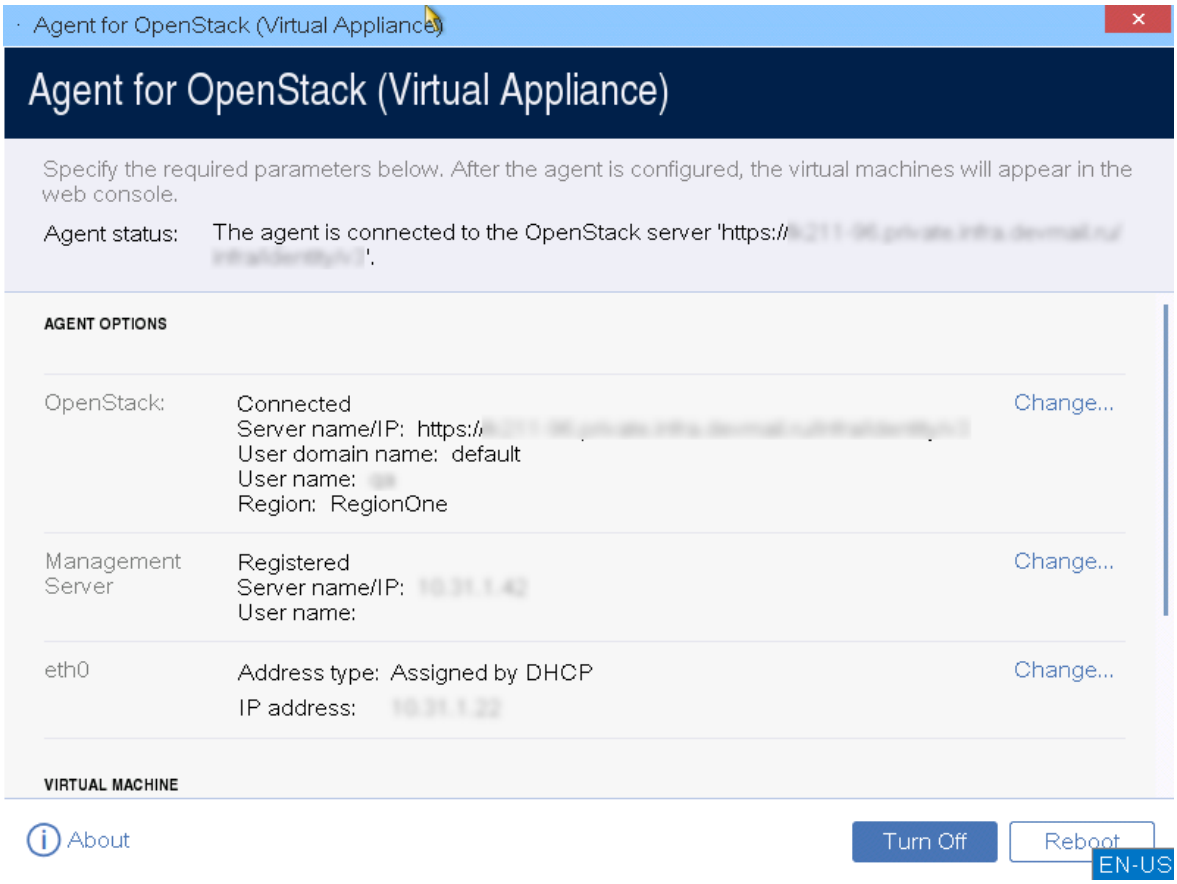


© ООО Киберпротект, 2026

e. Перейдите в раздел **Облачные вычисления** > **Виртуальные машины** и убедитесь, что имя машины с агентом появилось в списке виртуальных машин.

6. Получите URL-адрес API для аутентификации, который будет использоваться виртуальным устройством для взаимодействия с VK Cloud:
   a. Щелкните имя пользователя вверху справа и выберите **Настройки проекта**.
   b. Перейдите на вкладку **Доступ по API**.
   c. Запомните или запишите значение поля **Auth URL**.
7. Дождитесь запуска ВМ, откройте ее консоль и задайте параметры агента:
   - **OpenStack**. Укажите URL-адрес API для аутентификации. Кроме того, укажите домен с проектами, в которых находятся требуемые виртуальные машины. В соответствующих полях укажите имя пользователя и пароль администратора проектов с требуемыми виртуальными машинами.
   - **Management Server**. Укажите DNS-имя или IP-адрес сервера управления Кибер Бэкап, имя пользователя и пароль.
   - **eth0**. Если необходимо, задайте параметры сетевого интерфейса, который будет использоваться агентом (IP-адрес, маску сети, шлюз, DNS-серверы и WINS-серверы). По умолчанию используется автоконфигурация посредством DHCP.
   - **Name**. Если необходимо, измените имя агента. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.
   - **Time zone**. Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

© ООО Киберпротект, 2026



Выполненные действия должны привести к следующим результатам:

- В разделе **Настройки** > **Агенты** отобразится агент для OpenStack (VK Cloud).
- В веб-консоли Кибер Бэкап в разделе **Устройства** появится подраздел **OpenStack (VK Cloud)**.

2.6.4.10 Установка агента для Basis DynamiX Enterprise

Общие сведения

1. Для резервного копирования данных Basis DynamiX Enterprise понадобятся установленные и настроенные продукты:
   - Кибер Бэкап версии 17 или выше с лицензией Кибер Бэкап Расширенная редакция для платформы виртуализации (подробнее о лицензиях см. "Издания и лицензии Кибер Бэкап" (стр. 16));
   - Basis DynamiX Enterprise версии с 3.8.8 – 4.1, 4.3.
2. Для корректной работы Кибер Бэкап и Basis DynamiX Enterprise виртуальное устройство должно отвечать следующим минимальным требованиям:
   - Количество центральных процессоров (CPU): 2;
   - Объем ОЗУ: 4 ГБ;
   - Объем диска: 8 ГБ.

© ООО Киберпротект, 2026

Известные проблемы и ограничения

- Резервное копирование включённых ВМ поддерживается с версии 4.1.
- Не поддерживается подключение более 9 дисков к ВМ Basis DynamiX Enterprise 3.8.8 – 4.0.0 из-за ограничений платформы.
- Не поддерживается подключение более 8 сетевых адаптеров к ВМ Basis DynamiX Enterprise 3.8.8 – 4.0.0 из-за ограничений платформы.
- При развертывании агента не отслеживается прогресс передачи диска.
- После создания мгновенного снимка невозможно отключить вновь присоединенные или созданные диски от ВМ.
- Резервное копирование дисков с данными объемом более 100 ГБ может завершаться с ошибкой.
- Не поддерживается резервное копирование виртуальной машины, если к ней подключены диски из разных пулов.
- Не поддерживается резервное копирование виртуальной машины, если диски ВМ подключены к разным SEP.

Автоматическая установка агента для Basis DynamiX Enterprise

Установка Basis DynamiX Enterprise включает в себя следующие шаги:

1. Установка сервера управления Кибер Бэкап.
2. Подключение виртуального устройства Basis DynamiX Enterprise к серверу управления Кибер Бэкап.

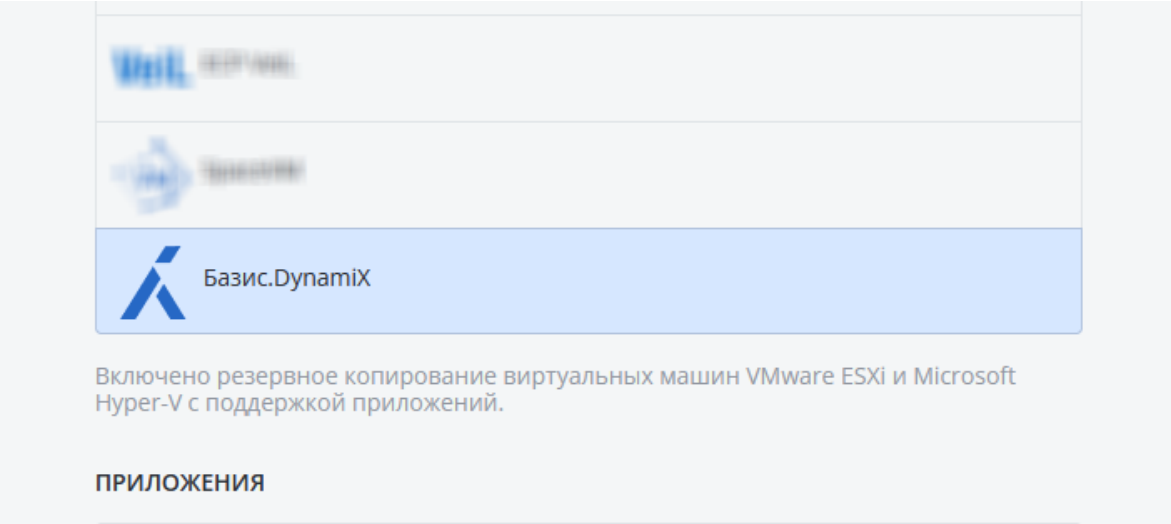
Установка сервера управления Кибер Бэкап

Для установки сервера управления Кибер Бэкап обратитесь к разделу "Установка сервера управления" (стр. 63).

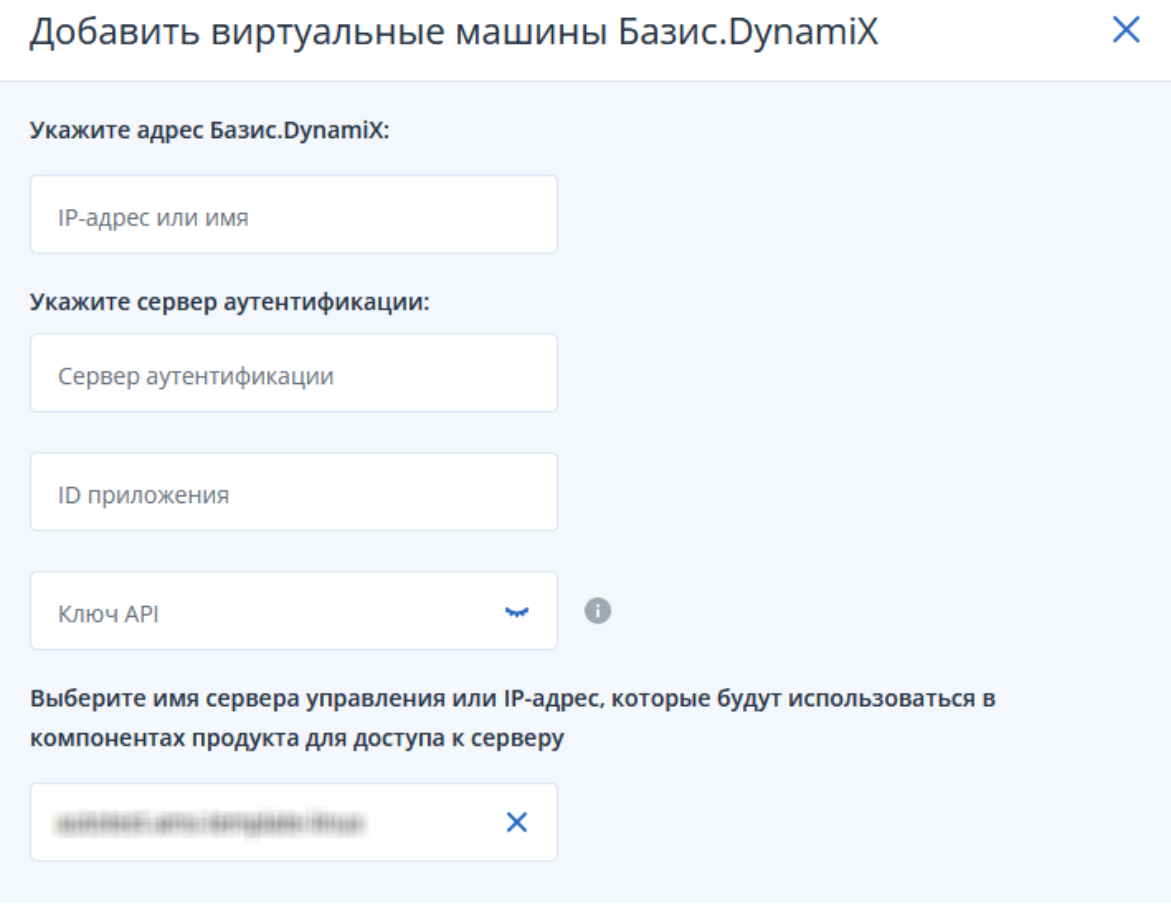
Подключение виртуального устройства Basis DynamiX Enterprise к серверу управления Кибер Бэкап

1. В веб-консоли Кибер Бэкап перейдите: **Устройства** > **Физические и виртуальные машины**.
2. Справа вверху щелкните **Добавить** и выберите в списке Basis DynamiX Enterprise.

© ООО Киберпротект, 2026



3. Укажите IP-адрес или имя для Basis DynamiX Enterprise, данные сервера аутентификации и укажите данные для доступа к серверу управления.



Для получения ID приложения и ключа API выполните следующие действия:

a. Перейдите на портал управления авторизацией SSO, например: sso.your_domain_name.domain.
b. Авторизуйтесь под именем пользователя, от имени которого будут выполняться запросы к REST API платформы (посредством токена JWT).

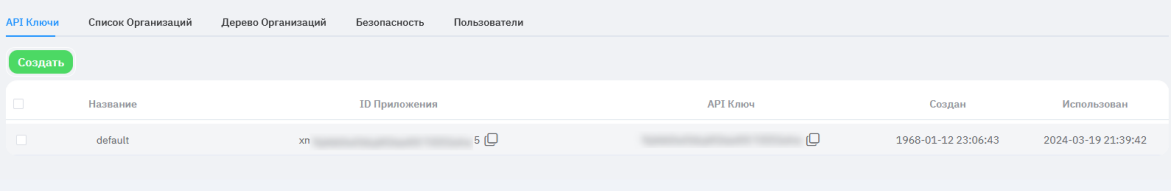
© ООО Киберпротект, 2026

Примечание
Пользователь должен иметь права **Admin** в учетной записи Basis DynamiX Enterprise.

c. Перейдите на вкладку **API Ключи** и нажмите **Создать**.

d. Введите название ключа и нажмите **Enter**.

e. Введите ID приложения и API ключ с экрана в соответствующие строки.



После заполнения полей нажмите **Далее** и дождитесь окончания подключения.

4. Перейдите в **Устройства** > **Basis DynamiX Enterprise** и убедитесь, что подключенное устройство отображается корректно.
5. Перейдите в **Настройки** > **Агенты** и убедитесь, что в списке агентов появился агент для резервного копирования.

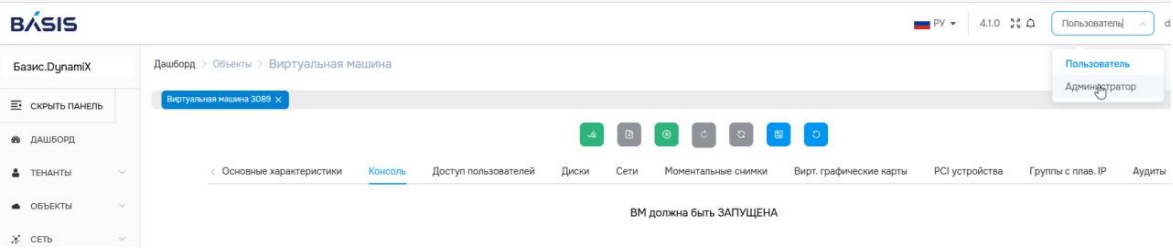
   Если операция подключения завершилась с ошибкой, проверьте сетевые настройки, соединение с сервером управления и настройки подключения к платформе Basis DynamiX Enterprise.

Примечание
Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

Установка агента для Basis DynamiX Enterprise вручную

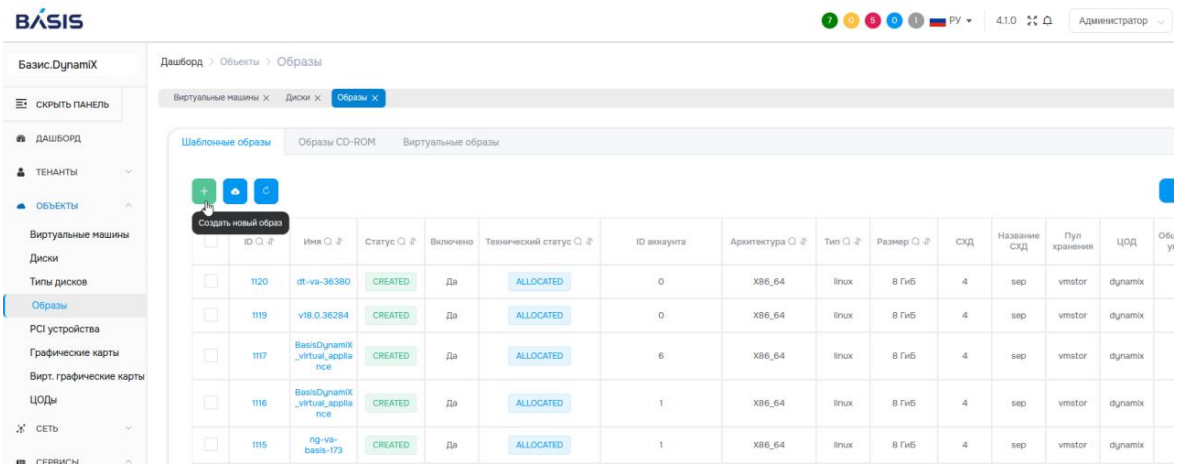
Для установки вручную агента для Basis DynamiX выполните следующие действия:

1. Скачайте пакет установки агента Basis DynamiX с сайта Киберпротект (файл формата .qcow2, например: BasisDynamixAppliance.qcow2).
2. В панели управления системой виртуализации Basis DynamiX перейдите в режим администратора.

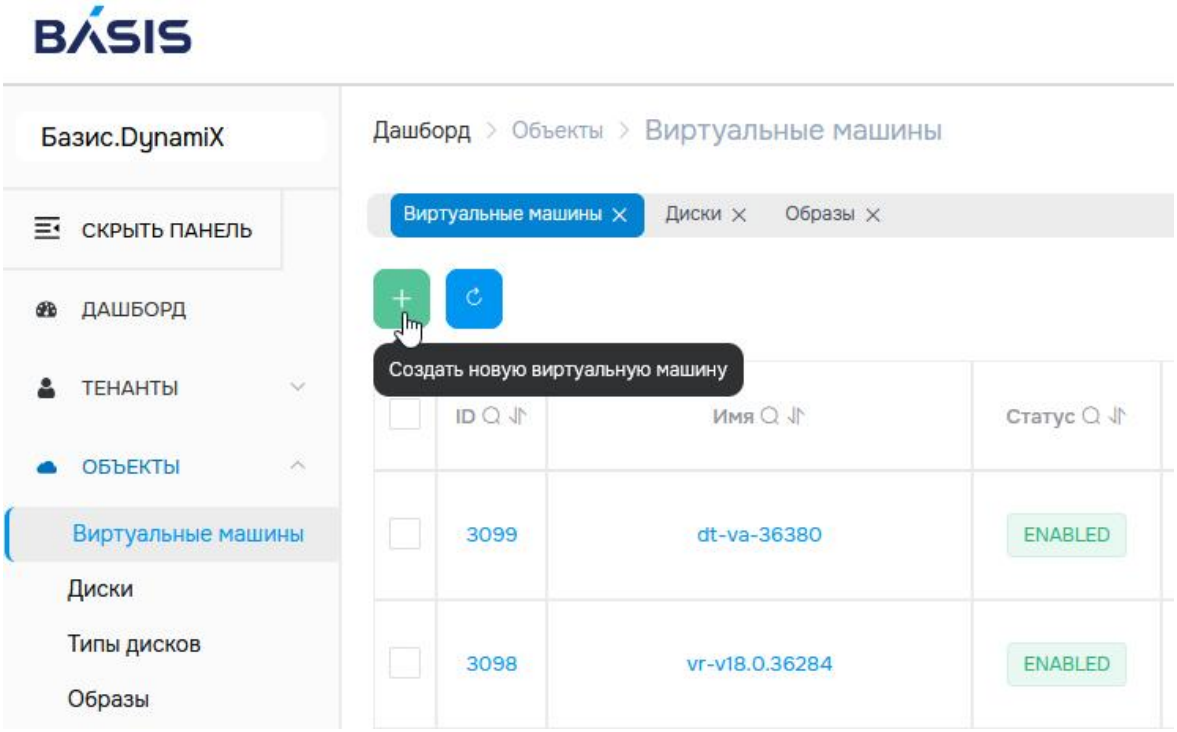


3. Перейдите в раздел **Объекты** > **Образы** и нажмите **Создать новый образ**.

© ООО Киберпротект, 2026

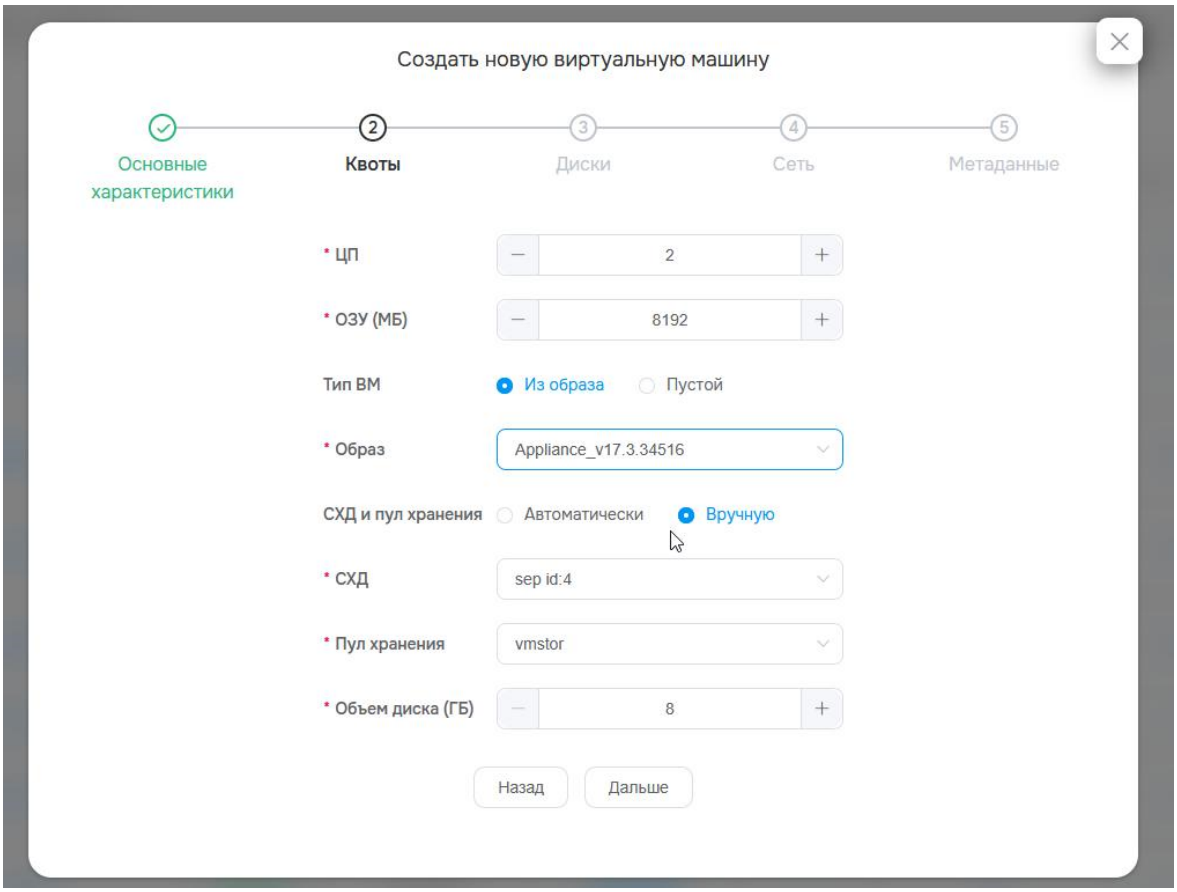


4. В окне создания образа укажите путь к пакету установки агента Basis DynamiX (подробнее см. в документации Basis DynamiX).
5. Перейдите в раздел **Виртуальные машины** и нажмите **Создать новую виртуальную машину**.



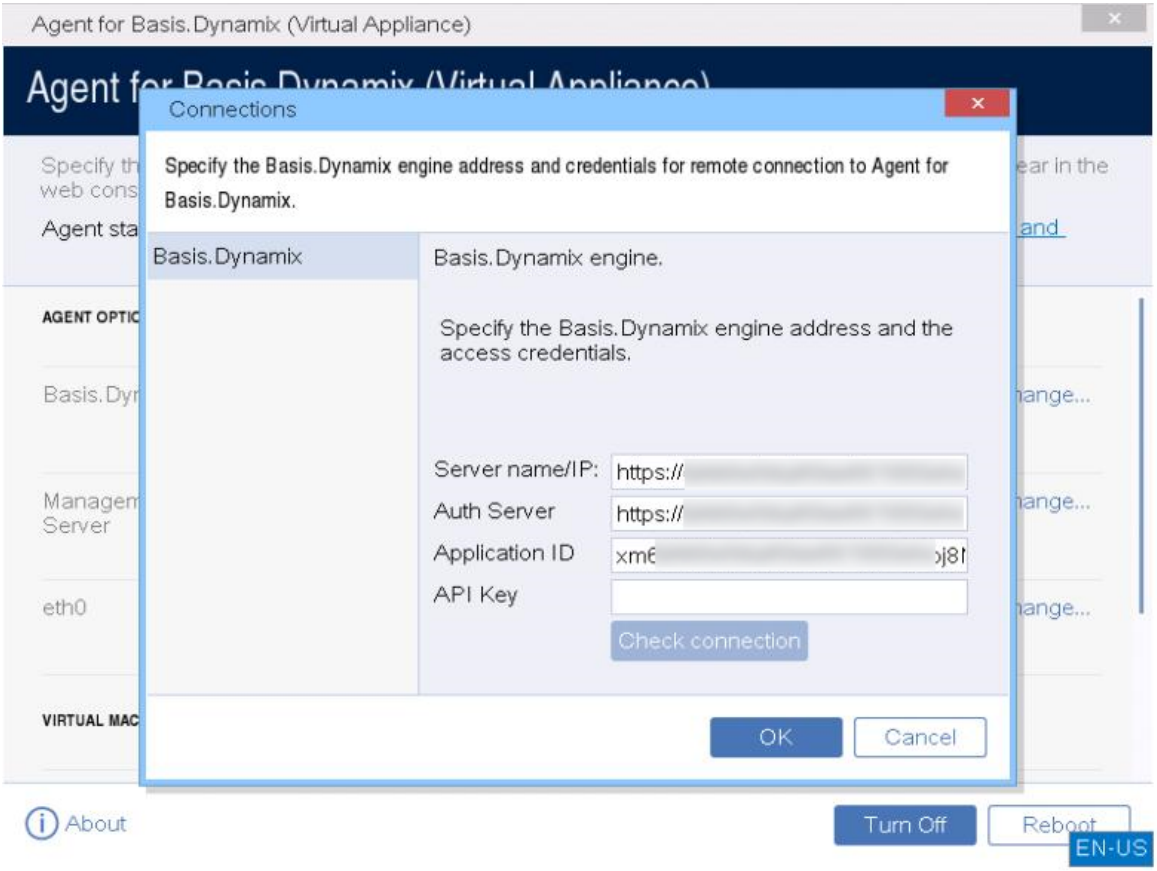
© ООО Киберпротект, 2026

6. В окне создания виртуальной машины на шаге **Квоты** укажите созданный ранее образ ВМ.



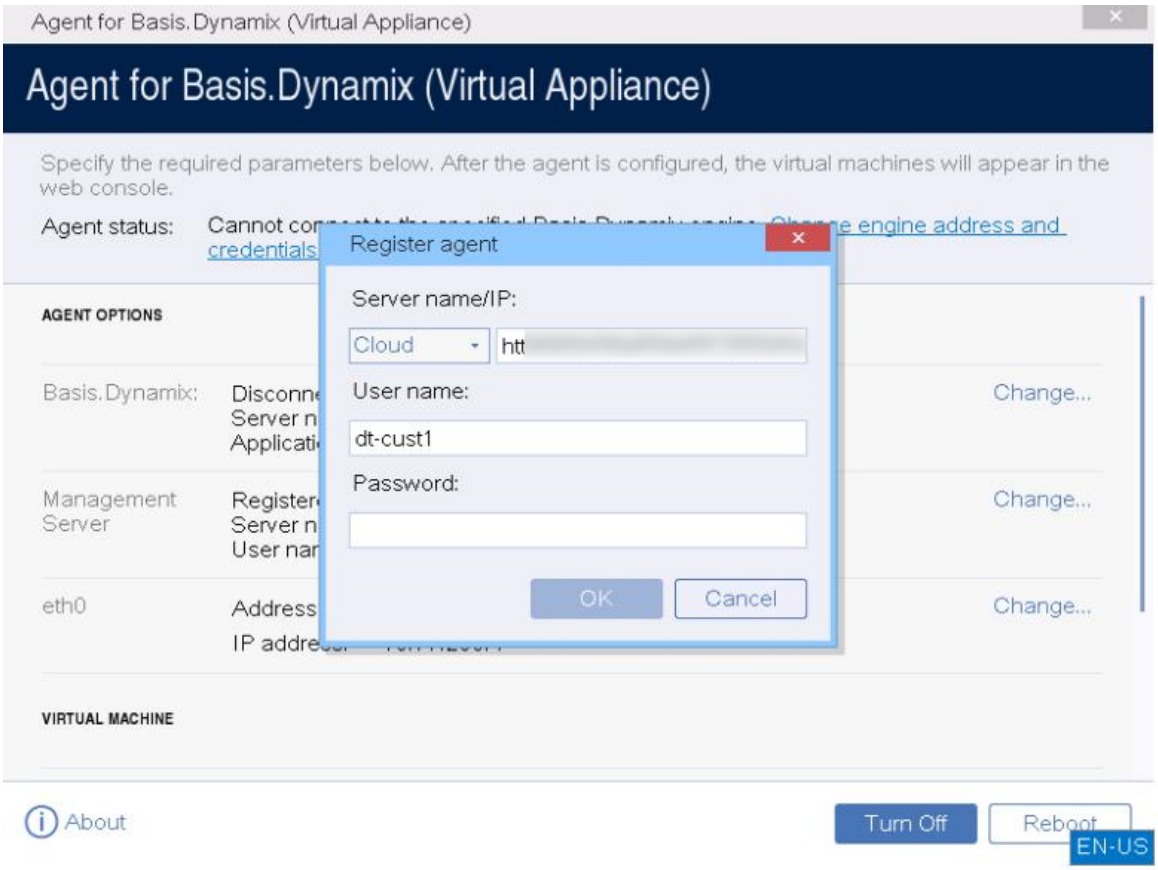
7. Укажите остальные настройки для создания шаблона на основе образа виртуального устройства согласно документации Basis DynamiX.
8. Подключитесь к консоли виртуальной машины.
9. В разделе **Basis.Dynamix** нажмите **Change** и укажите IP-адрес сервера платформы виртуализации, ID приложения и ключ API (информацию о получении ID приложения и ключа API см. в разделе "Автоматическая установка агента для Basis DynamiX Enterprise" (стр. 140)).

© ООО Киберпротект, 2026



10. В разделе **Management Server** нажмите **Change** и укажите IP-адрес сервера управления Кибер Бэкап и учетные данные для подключения к нему.

© ООО Киберпротект, 2026



11. Перезапустите виртуальную машину.
12. Убедитесь, что в разделе **Устройства** веб-консоли Кибер Бэкап отображаются устройства Basis DynamiX.

2.6.4.11 Установка агента для OpenNebula

Предварительные требования

1. Для развёртывания агента OpenNebula вам понадобятся установленные и настроенные системы:
   - Решение Кибер Бэкап версии 17.2 или выше с лицензией Кибер Бэкап Расширенная редакция для платформы виртуализации (подробнее о лицензиях см. "Издания и лицензии Кибер Бэкап" (стр. 16));
   - Система управления виртуализацией (например, ПК СВ "Брест").
2. Поддерживаются следующие системы управления виртуализацией:
   - OpenNebula версии 6.0.0.2;
   - ПК СВ "Брест", основанный на OpenNebula версии 6.0.0.2;
   - Альт Виртуализация 10, основанная на версии OpenNebula 6.2.0.1;
   - Система группового управления "Горизонт-ВС" версии 1.8.3 и выше.

© ООО Киберпротект, 2026

3. Для корректной работы Кибер Бэкап и OpenNebula виртуальное устройство должно отвечать следующим минимальным требованиям:
   - Количество процессоров (vCPU): 2;
   - Объём ОЗУ: 4 ГБ;
   - Объём диска: 64 ГБ.

Процедура установки

Вы можете установить агент двумя способами:

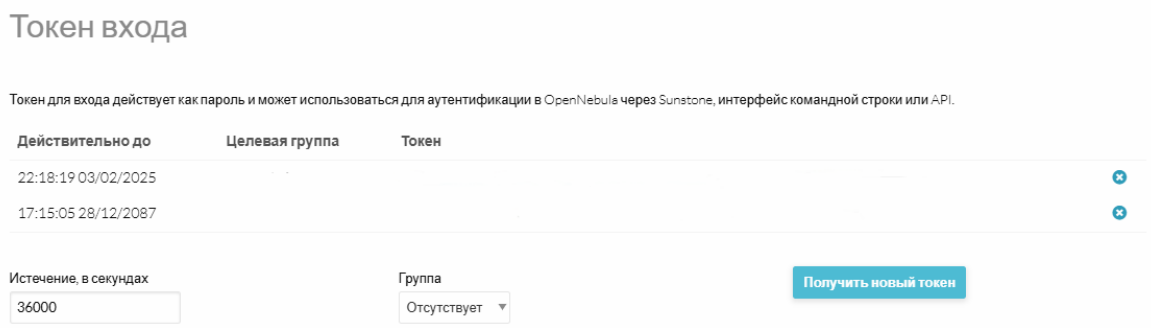
- Автоматически из интерфейса Кибер Бэкап (см. "Автоматическая установка агента для OpenNebula" (стр. 148)).
- Вручную, используя установочный файл агента OpenNebula (см. "Установка агента для OpenNebula вручную" (стр. 151)).

После установки агента создайте план защиты ваших виртуальных устройств в Кибер Бэкап.

Настройка токена входа

По умолчанию срок жизни нового токена входа для пользователя составляет 36 000 секунд (10 часов). Чтобы изменить срок жизни токена входа, выполните следующие действия:

1. В панели управления системой виртуализации перейдите в раздел **Система** > **Пользователи**.
2. Выберите пользователя, с помощью которого Кибер Бэкап будет подключаться к системе виртуализации.
3. Перейдите в раздел **Аутентификация** и выберите **Управление токенами входа**.
4. В поле **Истечение, в секундах** укажите необходимое значение и нажмите **Получить новый токен**.



Используйте токен при установке агента.

Известные проблемы и ограничения

- Не поддерживается резервное копирование RAW-дисков.
- Диски в системных хранилищах (System_DS) LVM_LVM обрабатываются как RAW-диски. Из-за ограничений платформы у таких хранилищ не поддерживается создание моментальных снимков диска и создание "тонких" дисков.

© ООО Киберпротект, 2026

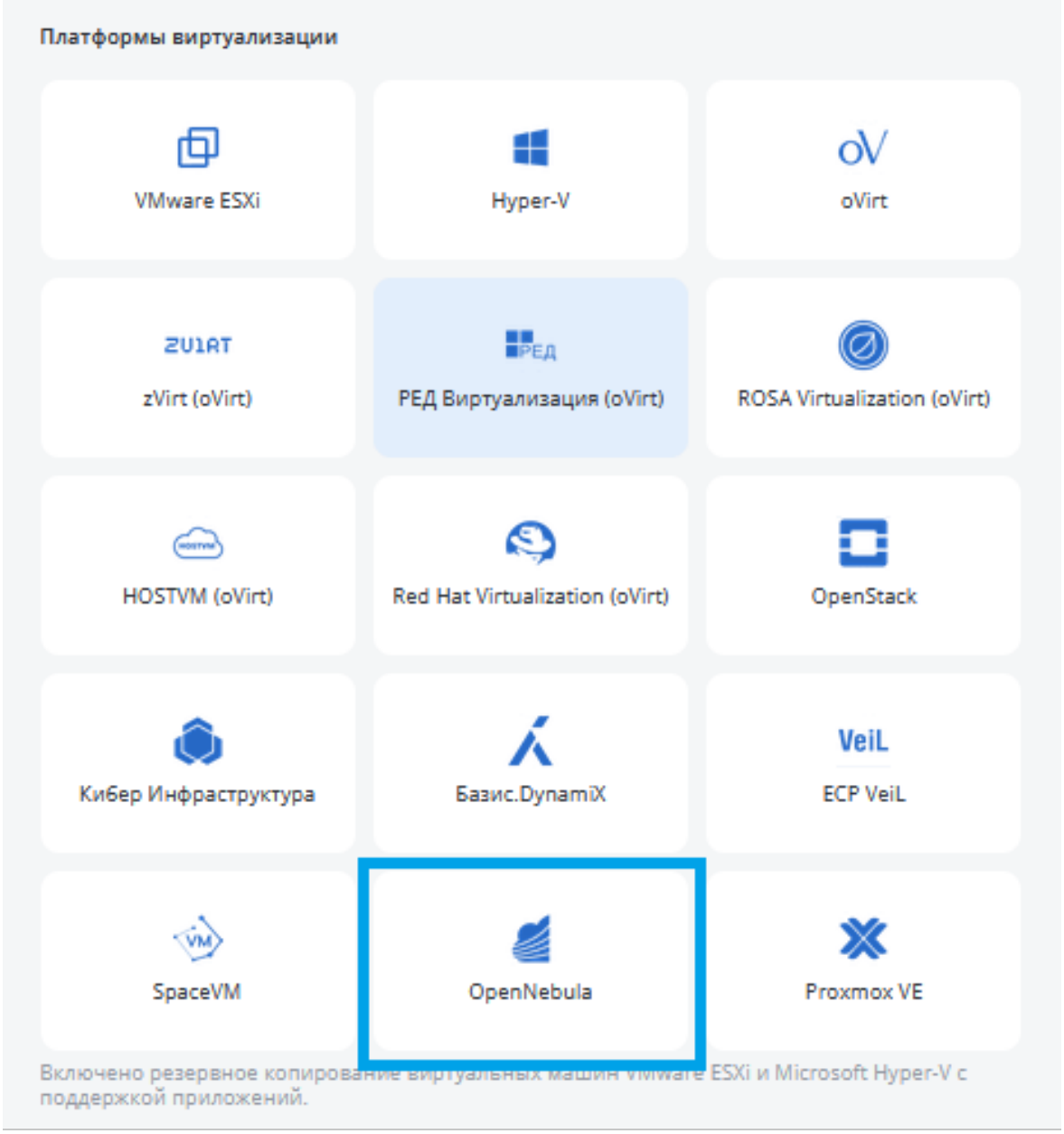
- Из-за ограничений платформы создание моментальных снимков диска в хранилищах BREST_LVM не поддерживается. Резервное копирование виртуальных машин в таких хранилищах также не поддерживается.
- Резервное копирование в LVM-хранилищах на платформе OpenNebula версии 6.0.0.2 и ниже (например, ПК СВ "Брест", основанный на OpenNebula версии 6.0.0.2 и ниже) не гарантируется из-за ограничения самой платформы: размещение виртуального устройства в LVM-хранилище может приводить к сбоям в дисковых операциях.
- Не поддерживается резервное копирование временных дисков.
- Не поддерживаются CD/DVD-диски.
- Не поддерживается восстановление дисков, использующих интерфейс SATA. Из-за ограничений платформы SATA-диски обрабатываются как SCSI-диски.
- Не поддерживается восстановление ВМ с дисками VirtIO. Диски VirtIO обрабатываются как SCSI-диски.
- Из-за ограничений платформы виртуальное устройство с агентом запускается как служебная ВМ. По этой причине дискреционный режим работы платформы виртуализации характеризуется следующими особенностями:
  - ВМ запускается от имени системного пользователя Oneadmin;
  - Необходимо разворачивать виртуальное устройство путем ручной загрузки образа, если нет возможности использовать в системе запуск виртуального устройства как служебной ВМ;
  - Не работает отложенный запуск ВМ.

Автоматическая установка агента для OpenNebula

Для автоматической установки агента для OpenNebula выполните следующие действия:

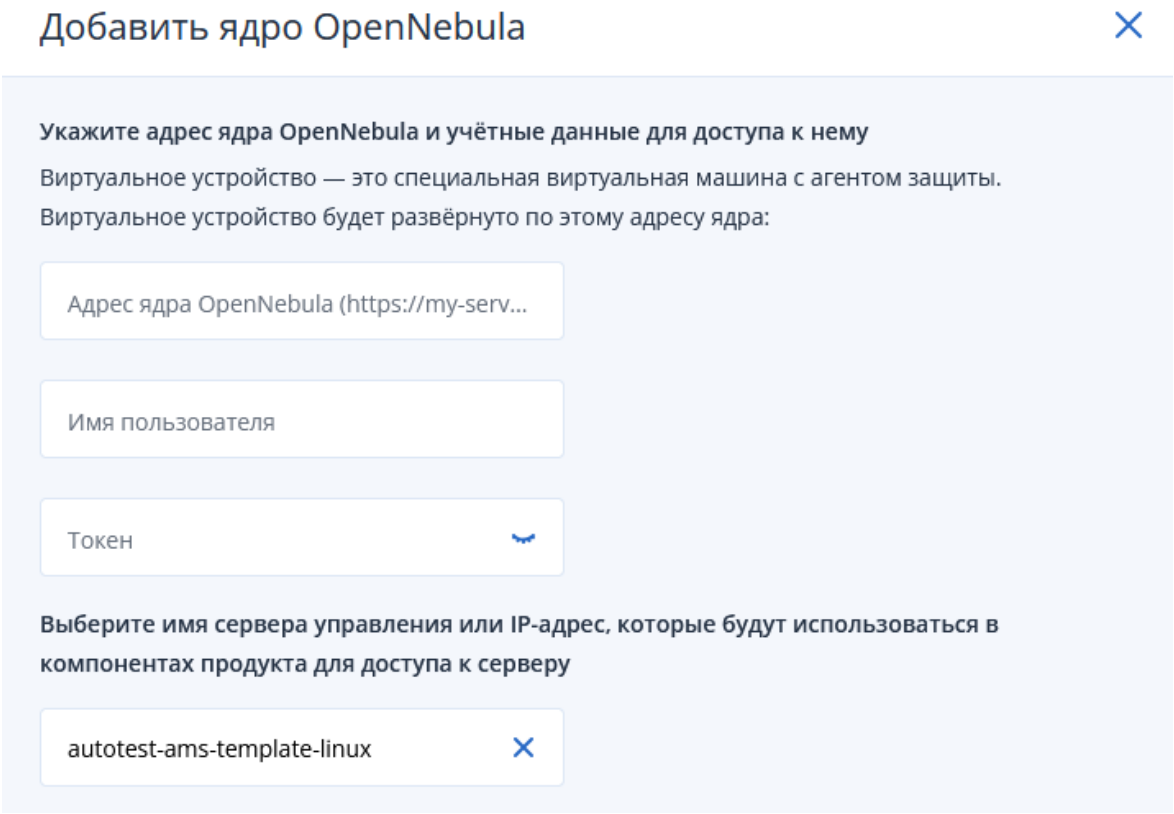
© ООО Киберпротект, 2026

1. В консоли Кибер Бэкап в разделе **Устройства** щёлкните **Добавить** и выберите OpenNebula.



2. Укажите адрес платформы, данные пользователя и сетевые настройки.

© ООО Киберпротект, 2026



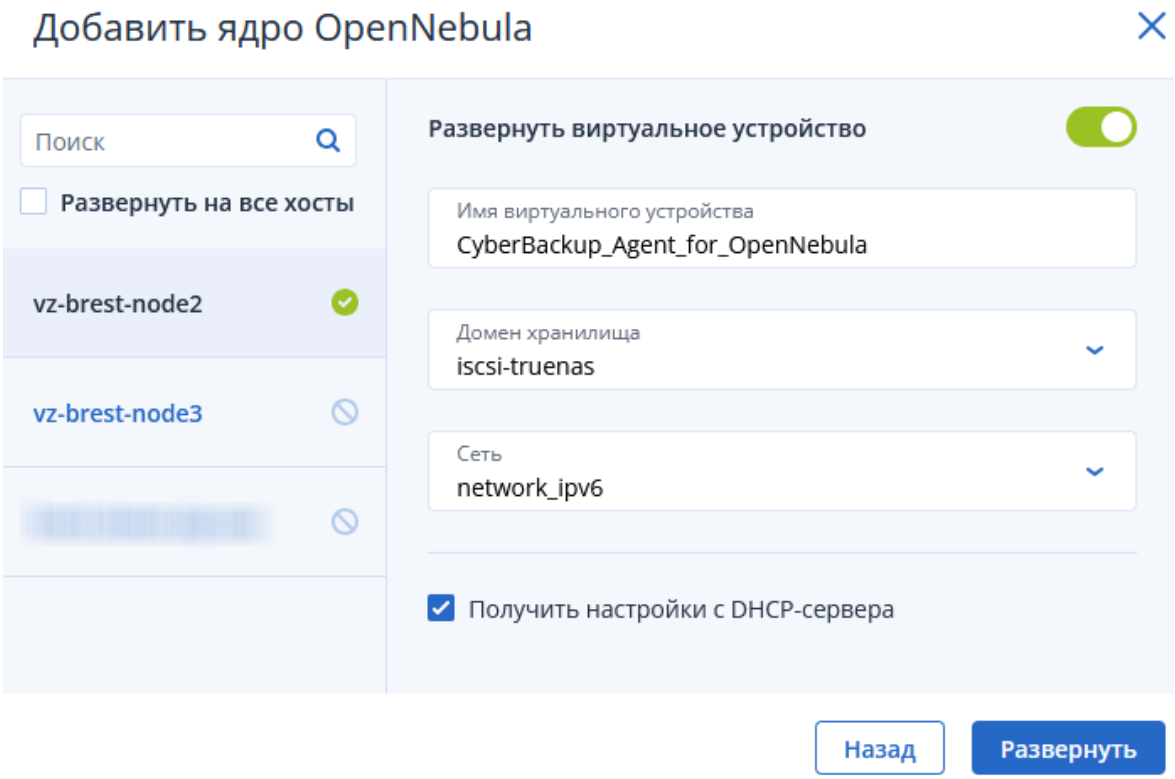
- В поле **Адрес ядра OpenNebula** укажите URL-адрес для доступа к серверу платформы виртуализации. В качестве этого адреса в OpenNebula используется конечная точка (например, для платформы ПК СВ "Брест" для получения точки доступа перейдите в **Инфраструктура** -> **Зоны**).

  Примечание
  Убедитесь, что в конфигурационном файле OpenNebula oned.conf адрес прослушивания для порта открыт в диапазоне с 127.0.0.0 до 0.0.0.0 или укажите конкретный IP-адрес.

- В поле **Имя пользователя** укажите имя пользователя (логин), с помощью которого Кибер Бэкап будет подключаться к системе виртуализации.
- В поле **Токен** укажите токен входа (см. "Настройка токена входа" (стр. 147)).
- В нижнем поле укажите доменное имя или IP-адрес сервера управления Кибер Бэкап.

3. Нажмите **Далее** и укажите дополнительные параметры.

© ООО Киберпротект, 2026



Задайте имя виртуального устройства, выберите кластер, домен и сеть, с которыми будет взаимодействовать виртуальное устройство. Если необходимо, укажите сетевые настройки вручную, сняв флажок **Получить настройки с DHCP-сервера**.

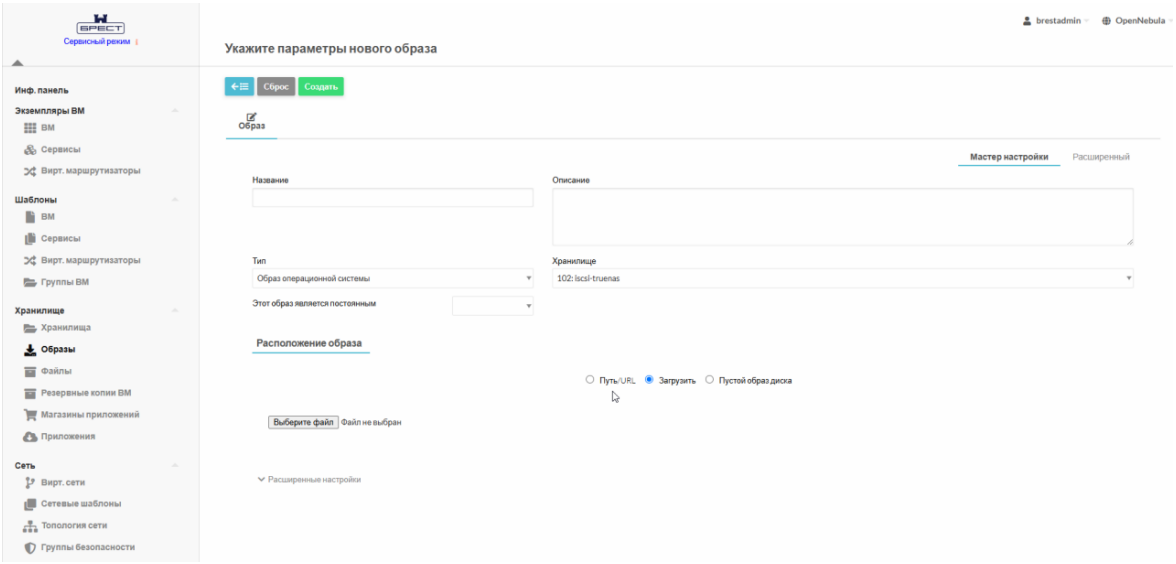
4. Нажмите **Развернуть** и дождитесь завершения процедуры развертывания. Убедитесь, что виртуальное устройство с агентом появилось в интерфейсе платформы виртуализации в списке виртуальных машин.

Установка агента для OpenNebula вручную

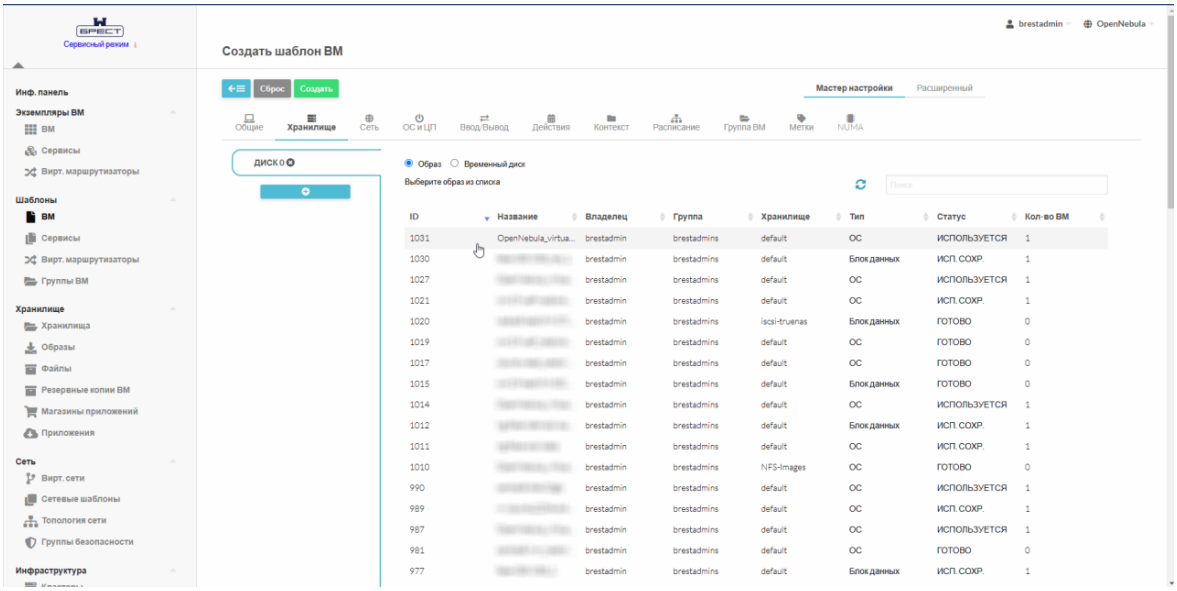
Для установки вручную агента для OpenNebula выполните следующие действия:

1. Скачайте пакет установки агента OpenNebula с сайта Киберпротект (файл формата .qcow2, например: OpenNebulaAppliance.qcow2).
2. Распакуйте образ виртуального устройства.
3. В панели управления системой виртуализации (например, ПК СВ "Брест") перейдите в раздел **Хранилище** -> **Образы**.
4. Отметьте флажок **Загрузить** и далее щелкните **Выберите файл**.

© ООО Киберпротект, 2026

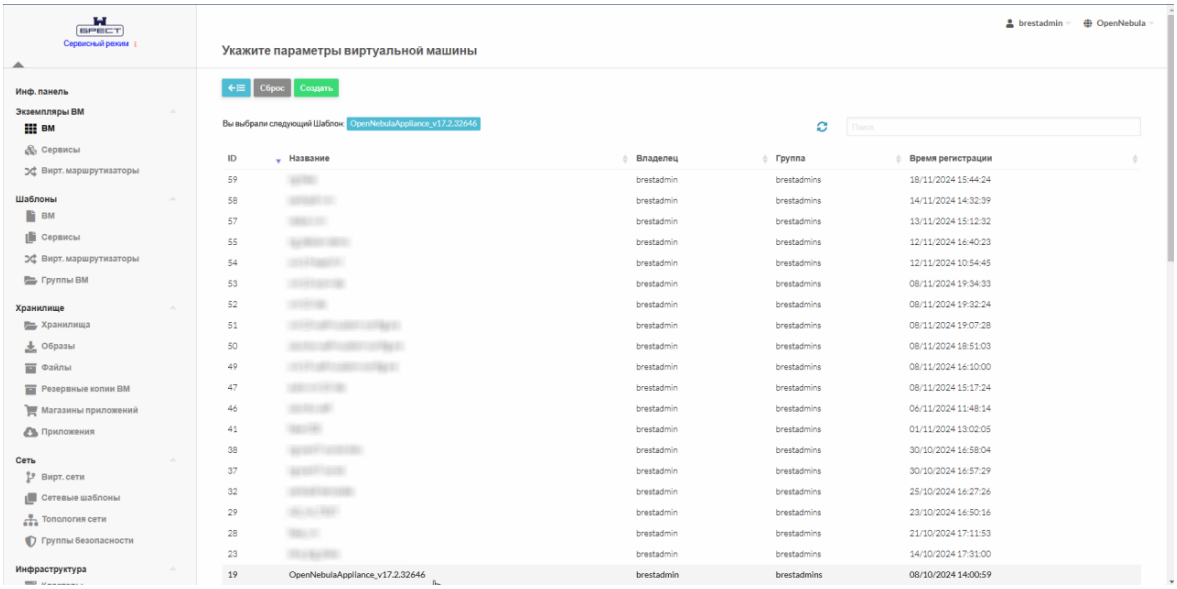


5. Укажите скачанный файл образа виртуального устройства и подтвердите загрузку.
6. Перейдите в раздел **Шаблоны** -> **ВМ** и нажмите **Создать**.

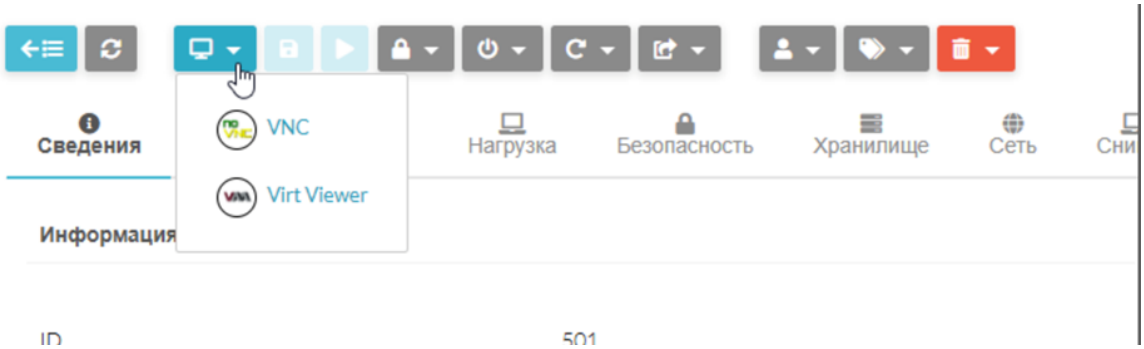


7. Выберите из списка появившееся виртуальное устройство и укажите необходимые настройки для создания шаблона на основе образа виртуального устройства.
8. Перейдите в список виртуальных машин **Экземпляры ВМ** -> **ВМ** и отметьте в списке появившийся там шаблон.

© ООО Киберпротект, 2026

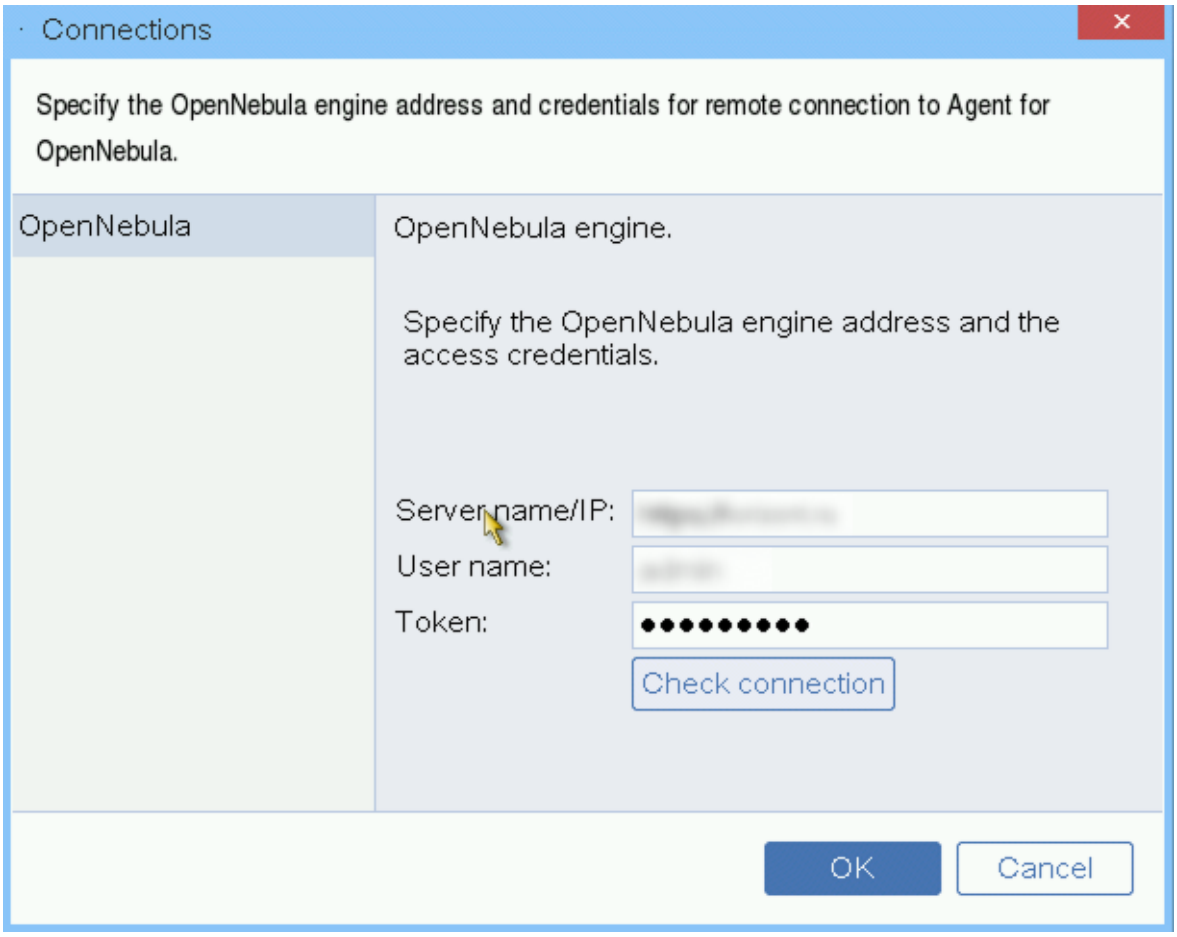


9. Щелкните **Создать** и подтвердите создание ВМ на основе выбранного шаблона и укажите необходимые настройки, в том числе:
   - Количество процессоров CPU: не менее 2;
   - Количество памяти RAM: не менее 4 Гб;
   - Объем жесткого диска: не менее 8 Гб.
10. Убедитесь, что виртуальное устройство с агентом Кибер Бэкап для OpenNebula появилось в списках ВМ.
11. Подключитесь к консоли виртуальной машины: в панели управления ВМ нажмите **VNC**. Отобразится меню интеграции с OpenNebula.



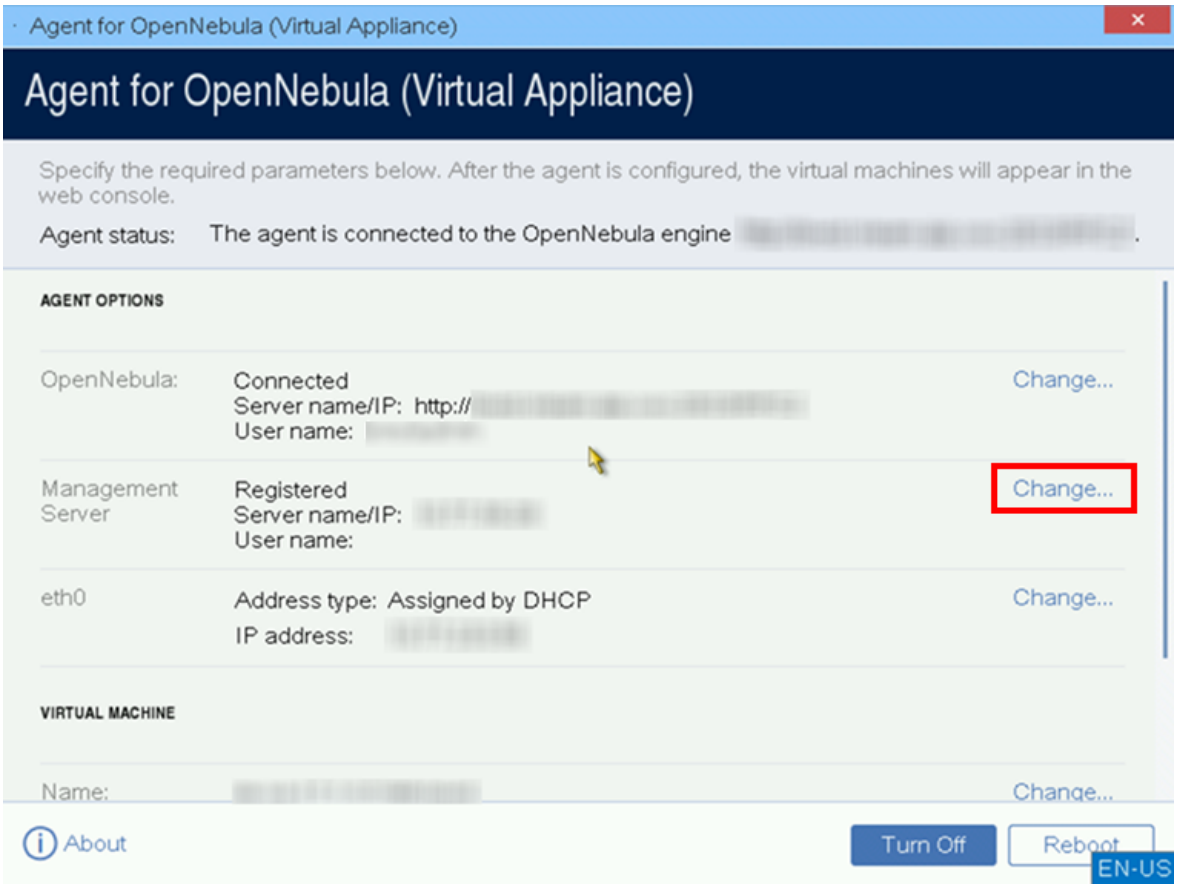
12. В разделе **OpenNebula** нажмите **Change** и укажите IP-адрес сервера платформы виртуализации, имя пользователя и токен входа (см. "Настройка токена входа" (стр. 147)).

© ООО Киберпротект, 2026



13. В разделе **Management Server** нажмите **Change** и укажите IP-адрес сервера управления Кибер Бэкап и учетные данные для подключения к нему.

© ООО Киберпротект, 2026



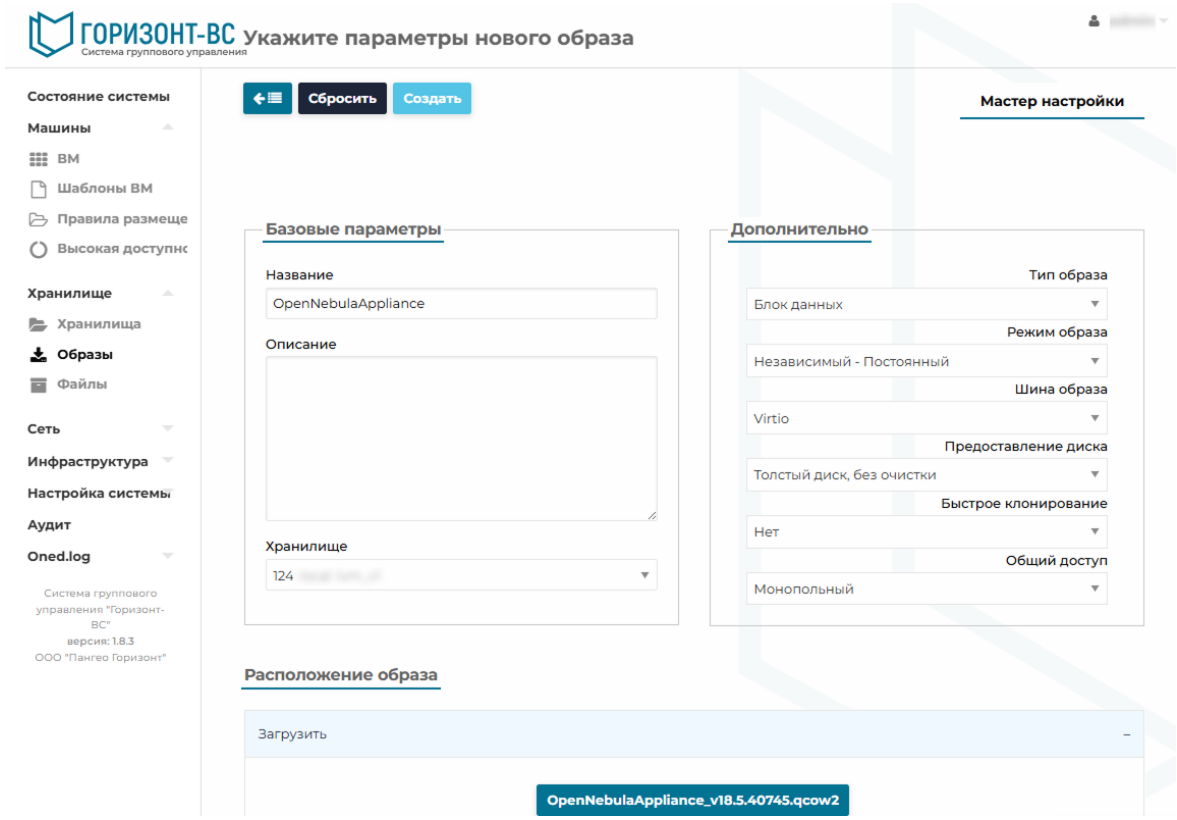
14. Перезапустите виртуальную машину.
15. Убедитесь, что в разделе **Устройства** веб-консоли Кибер Бэкап отображаются устройства OpenNebula.

Установка агента для OpenNebula вручную в СГУ "Горизонт-ВС"

Для установки вручную агента для OpenNebula в Системе группового управления "Горизонт-ВС" выполните следующие действия:

1. Скачайте пакет установки агента OpenNebula с сайта Киберпротект (файл формата .qcow2, например: OpenNebulaAppliance.qcow2).
2. В панели управления Системы группового управления "Горизонт-ВС" перейдите в раздел **Хранилище** > **Образы**.
3. Щёлкните значок плюса в верхнем меню и заполните поля в появившейся форме. При этом в блоке **Дополнительно** для параметра **Тип образа** выберите значение **Блок данных**.
4. В блоке **Расположение образа** нажмите **Загрузить файл** и выберите скачанный на шаге 1 файл с пакетом установки агента OpenNebula. В результате название выбранного файла будет отображено в области кнопки **Загрузить файл**.
5. Щёлкните **Создать** в верхнем меню.

© ООО Киберпротект, 2026



6. Подключитесь по SSH к машине с Системой группового управления "Горизонт-ВС" и выполните команду:

```
bhcs
```

7. Создайте файл с шаблоном виртуальной машины:

```
mcedit <имя_файла_с_шаблоном>
```

Где:

- <имя_файла_с_шаблоном> – имя создаваемого файла с шаблоном виртуальной машины (например, template).

8. В созданном файле укажите текст конфигурации:

```
NAME = <имя_файла_с_шаблоном>
AUTOSTART = "0"
CONTEXT = [
 NETWORK = "YES",
 SSH_PUBLIC_KEY = "$USER[SSH_PUBLIC_KEY]" ]
CPU = "1"
DISK = [
 CACHE = "none",
 IMAGE = "<имя_загруженного_с_сайта_файла>",
 IMAGE_UNAME = "admin" ]
FEATURES = [
 GUEST_AGENT = "yes" ]
```


© ООО Киберпротект, 2026

```
GRAPHICS = [
  LISTEN = "0.0.0.0",
  TYPE = "VNC" ]
INPUT = [
  BUS = "usb",
  TYPE = "tablet" ]
LOGO = "images/logos/redos.svg"
MEMORY = "4096"
NIC = [
  MODEL = "virtio",
  NETWORK = "Public",
  NETWORK_UNAME = "admin" ]
OS = [
  ARCH = "x86_64",
  AUTOSTART = "NO",
  BIOS = "LEGACY",
  BOOTMENU = "NO",
  HA = "NO",
  SMBIOS_MODE = "sysinfo" ]
SYSINFO=[
  VENDOR_INFO="yes",
  VM_INFO="yes"
]
USB_CONTROLLER = "XHCI"
VCPU = "2"
VGA_ADAPTER = [
  ACCEL3D = "no",
  HEADS = "1",
  MODEL = "qxl",
  RENDERNODE = "" ]
```

В тексте конфигурации замените значения параметров NAME и IMAGE, где:

- <имя_файла_с_шаблоном> – имя создаваемого на шаге 7 файла с шаблоном виртуальной машины (например, template);
- <имя_загруженного_с_сайта_файла> – имя файла с пакетом установки агента OpenNebula, загруженного на шаге 1 (например, OpenNebulaAppliance).

9. Завершите создание шабона, выполнив команду:

```
onetemplate create <имя_файла_с_шаблоном>
```

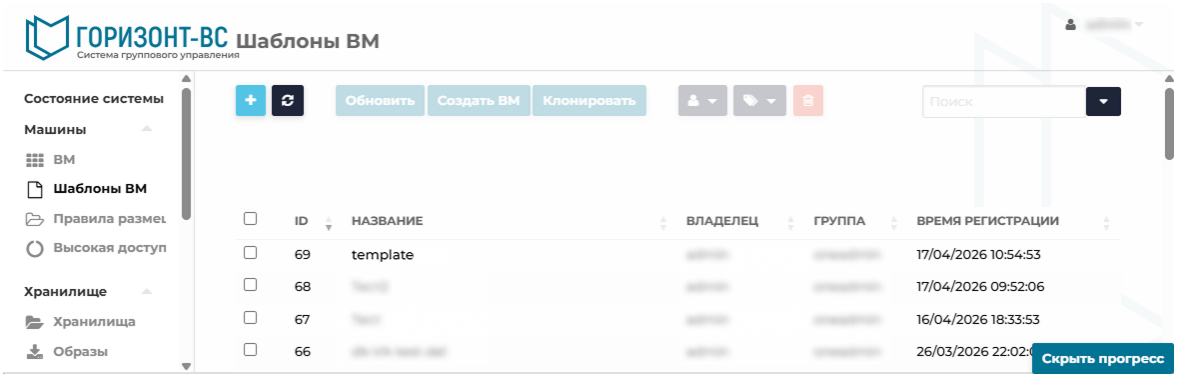
Где:

- <имя_файла_с_шаблоном> – имя создаваемого файла с шаблоном виртуальной машины (например, template).

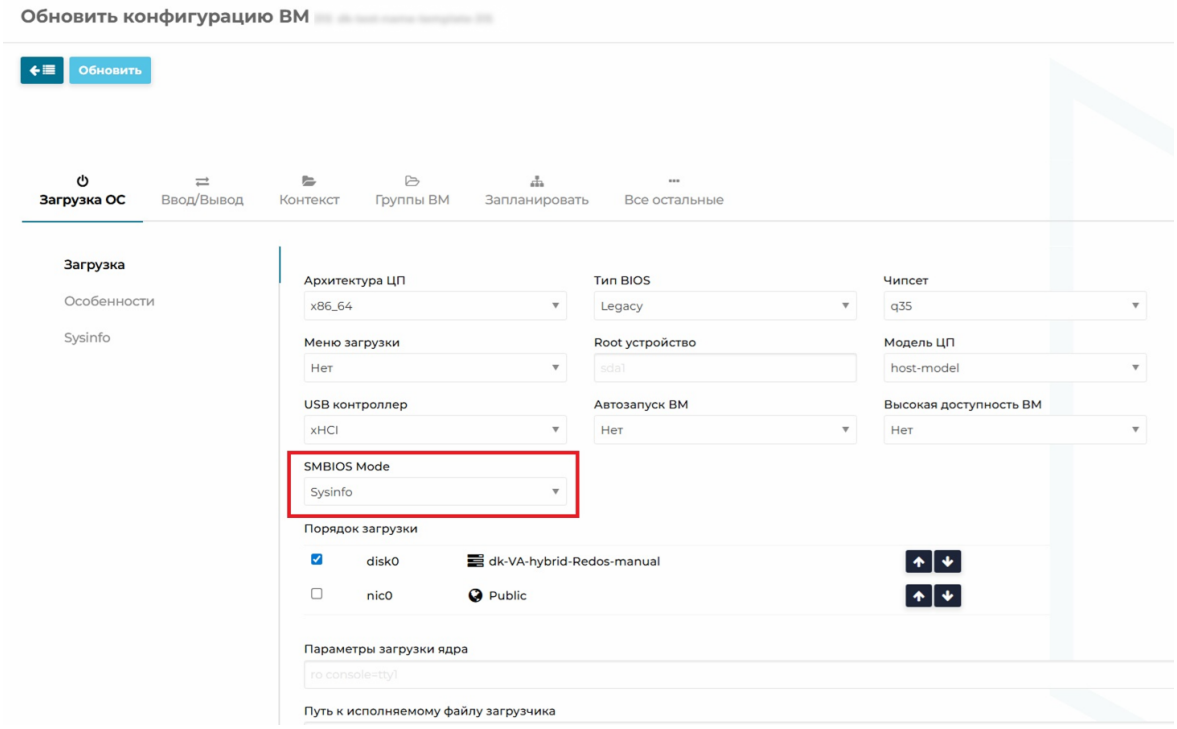
Убедитесь в отображении номера созданного шаблона в ответе команды (например, ID: 69).

10. В панели управления Системы группового управления "Горизонт-ВС" перейдите в раздел **Машины** > **Шаблоны ВМ**.
11. Убедитесь в отображении созданного шаблона в списке. Для поиска воспользуйтесь номером созданного шабона из предыдущего шага.

© ООО Киберпротект, 2026

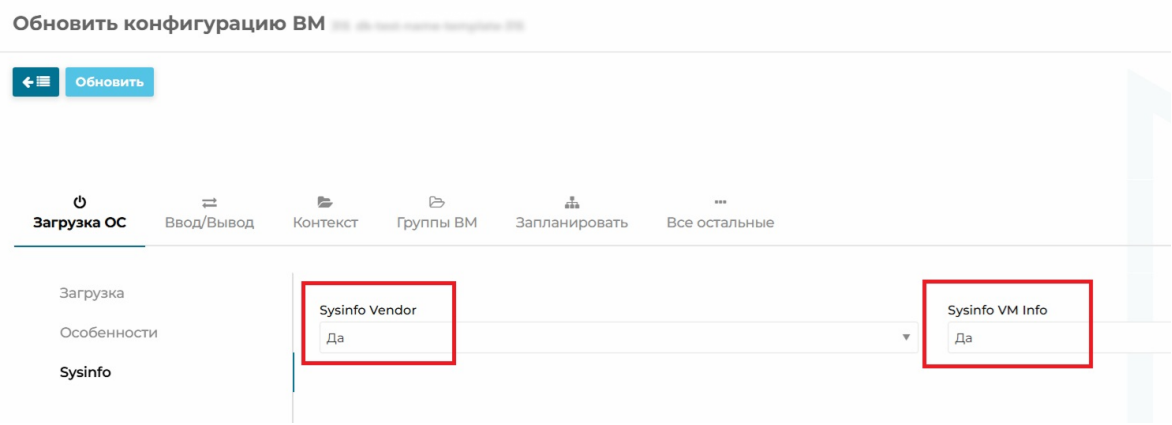


12. Перейдите в раздел **Машины** > **ВМ**.
13. Щёлкните значок плюса в верхнем меню, выберите созданный шаблон и нажмите **Создать**. Дождитесь окончания процесса создания виртуальной машины и отображения её в списке виртуальных машин со статусом **Запущено**.
14. Выберите созданную вирутуальную машину в списке и отключите её питание.
15. После отключения питания виртуальной машины в верхнем меню перейдите в раздел **Конфигурация** и щёлкните **Обновить конфигурацию**.
16. В верхнем меню перейдите в раздел **Загрузка ОС**, на панели слева выберите **Загрузка**. После этого для параметра **SMBIOS Mode** установите значение **Sysinfo**.

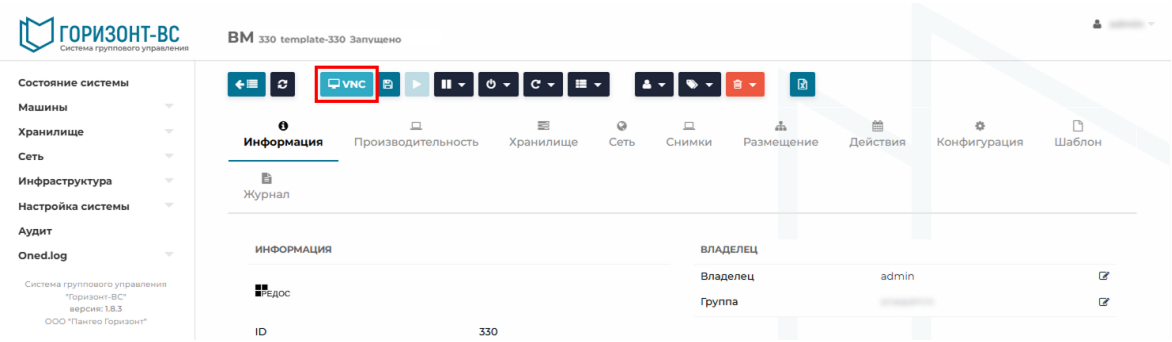


17. На панели слева выберите **Sysinfo** и установите для параметров **Sysinfo Vendor** и **Sysinfo VM Info** значение **Да**. Затем щёлкните **Обновить**.

© ООО Киберпротект, 2026

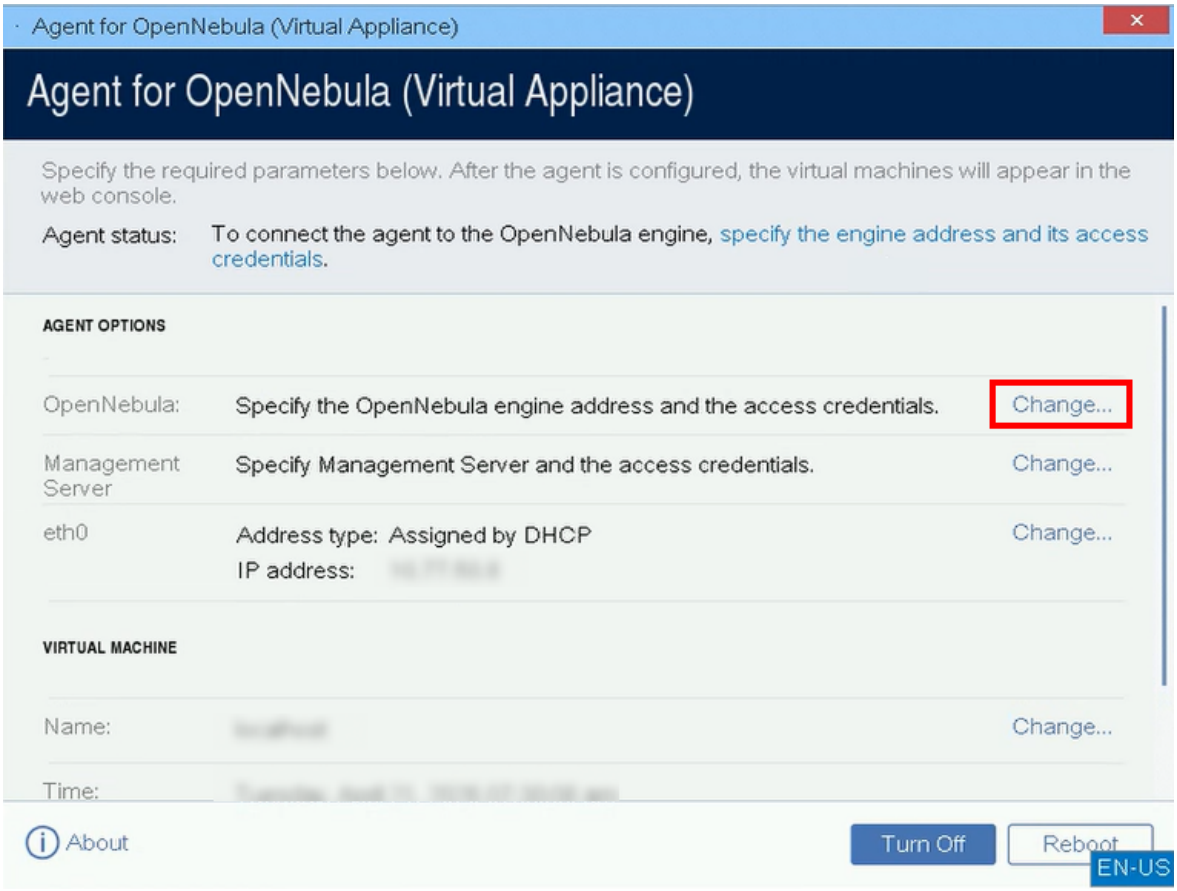


18. Запустите виртуальную машину.
19. Подключитесь к консоли виртуальной машины, щёлкнув **VNC** в верхнем меню.



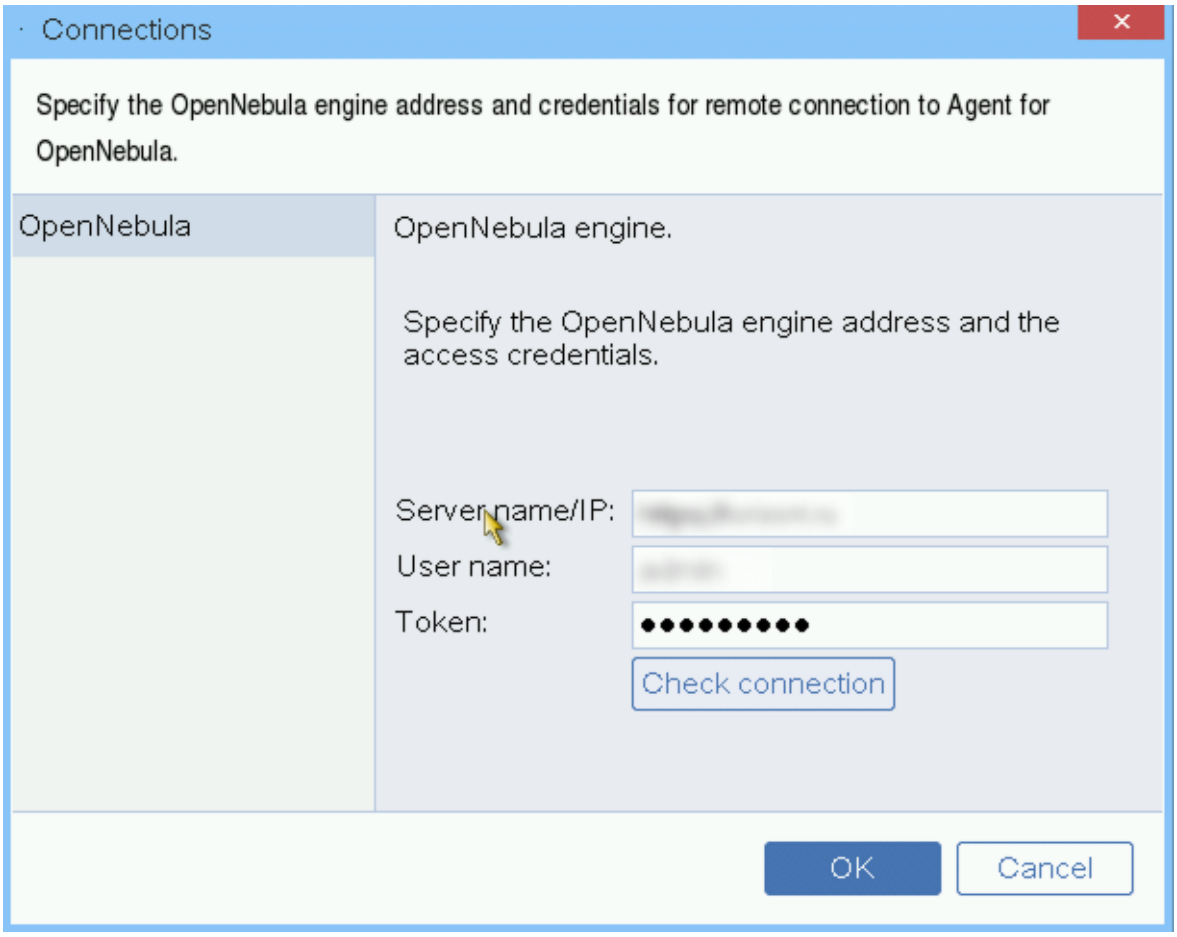
20. В разделе **OpenNebula** нажмите **Change**.

© ООО Киберпротект, 2026



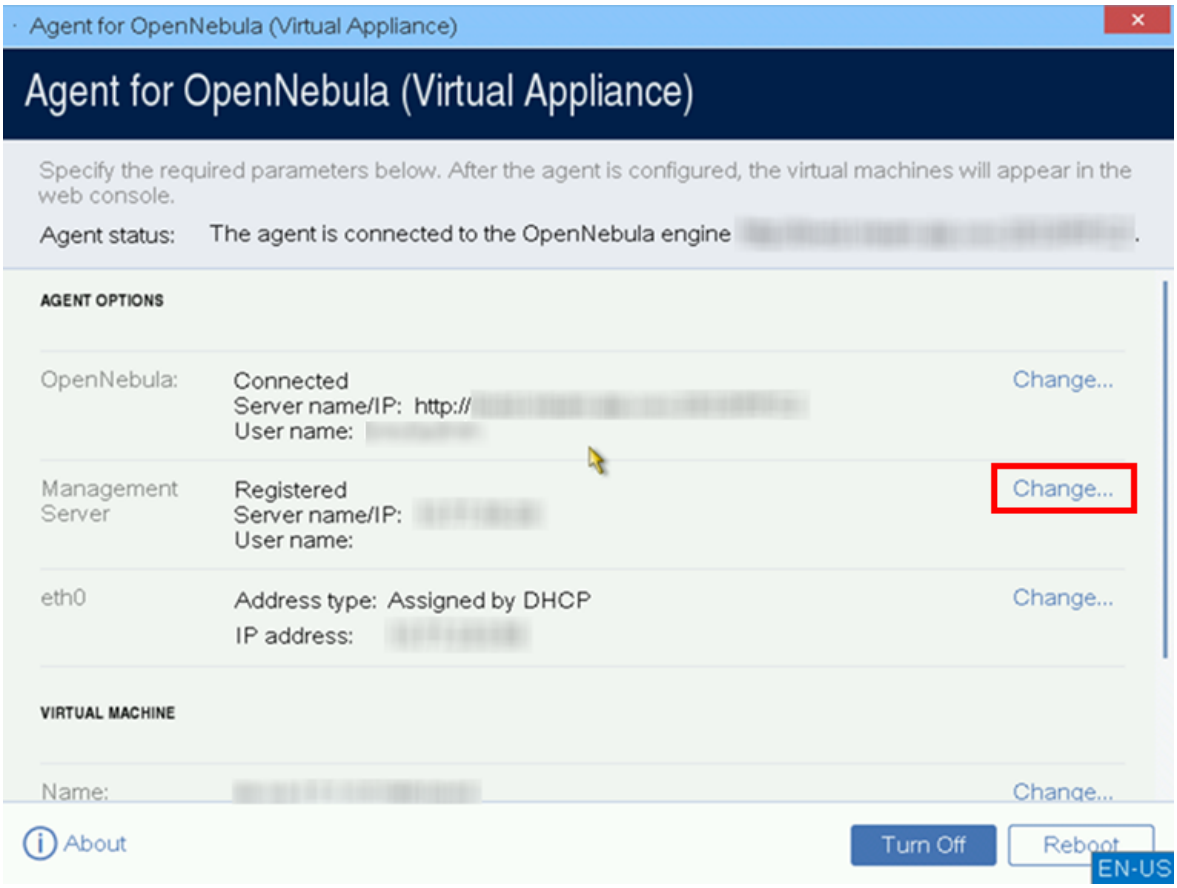
21. В появившемся окне укажите IP-адрес сервера Системы группового управления "Горизонт-ВС", имя пользователя и токен входа (см. "Настройка токена входа" (стр. 147)).

© ООО Киберпротект, 2026



22. В разделе **Management Server** нажмите **Change** и укажите IP-адрес сервера управления Кибер Бэкап и учётные данные для подключения к нему.

© ООО Киберпротект, 2026



23. Убедитесь, что в разделе **Настройки** > **Агенты** веб-консоли Кибер Бэкап отображается созданное виртуальное устройство.

2.6.4.12 Установка агента для Proxmox

Для работы с виртуальными машинами на хосте Proxmox необходимо развернуть виртуальное устройство – виртуальную машину с агентом Кибер Бэкап.

Общие сведения

1. Для резервного копирования и восстановления данных Proxmox VE понадобятся установленные и настроенные продукты:
   - Кибер Бэкап версии 18 или выше с лицензией Кибер Бэкап Расширенная редакция для платформы виртуализации (подробнее о лицензиях см. "Издания и лицензии Кибер Бэкап" (стр. 16));
   - Система управления виртуализацией.
2. Поддерживаются следующие системы управления виртуализацией:
   - Proxmox Virtual Environment;
   - Альт Виртуализация редакции PVE.

   Подробнее о поддерживаемых версиях вышеуказанных продуктов см. раздел "Поддерживаемые платформы виртуализации" (стр. 29).

© ООО Киберпротект, 2026

3. Для корректной работы Кибер Бэкап и Proxmox VE виртуальное устройство должно отвечать следующим минимальным требованиям:
   - Количество центральных процессоров (CPU): 2;
   - Объем ОЗУ: 4 ГБ;
   - Объем диска: 8 ГБ.

Планирование количества агентов для Proxmox

Агент для Proxmox контролирует виртуальные машины только на том сервере Proxmox, на котором он установлен. Для резервного копирования всех виртуальных машин в кластере необходимо развернуть агенты на каждом сервере Proxmox.

Известные проблемы и ограничения

- Из-за ограничений системы Proxmox VE при восстановлении виртуальной машины в новую ВМ необходимо в настройках новой ВМ указывать не более четырех виртуальных процессоров. Для увеличения производительности ВМ в консоли Proxmox VE можно увеличить количество ядер для данной ВМ.
- Виртуальное устройство поддерживает следующие типы контроллеров: VirtIO SCSI, VirtIO SCSI Single, LSI 53C895A, VMware PVSCSI.
- Для аутентификации пользователя на виртуальном устройстве доступны следующие методы: LDAP и Linux PAM Standard Authentication. Подробнее см. в документации Proxmox VE.
- В ряде случаев Proxmox дублирует UUID-идентификаторы SMBIOS в виртуальных машинах. Такие ВМ не отображаются в списках в Кибер Бэкап. В таких случаях необходимо вручную изменить идентификаторы на уникальные.
- Хранилища iSCSI/kernel, iSCSI/libiscsi и Ceph/RBD не поддерживаются.
- Совместимость продукта Кибер Бэкап с хранилищами CephFS, Proxmox Backup и BTRFS не проверялась.

Установка агента для Proxmox вручную

Чтобы установить вручную агент для Proxmox, выполните следующие действия:

1. Загрузите пакет установки агента Proxmox с сайта Киберпротект (файл формата .qcow2, например: ProxmoxAppliance.qcow2).
2. Войдите как администратор в панель управления системы виртуализации Proxmox VE.
3. Создайте виртуальную машину без подключенных дисков:
   a. В верхнем левом углу панели управления нажмите **Create VM**.
   b. Укажите следующие данные в окне создания ВМ:
      i. На вкладке **General** задайте имя ВМ.
      ii. На вкладке **OS** выберите пункт **Do not use any media**.
      iii. На вкладке **System** в поле **SCSI Controller** выберите один из поддерживаемых контроллеров: VirtIO SCSI, VirtIO SCSI Single, LSI 53C895A, VMware PVSCSI.

© ООО Киберпротект, 2026

iv. На вкладке **Disks** удалите диск, который предлагается создать вместе с ВМ.

v. На вкладке **CPU** в поле **Cores** укажите минимум 2 ядра процессора.

vi. На вкладке **Memory** укажите минимум 4 ГБ оперативной памяти.

Укажите остальные настройки согласно документации Proxmox VE (ссылка на документацию находится в правом верхнем углу панели управления).

4. Загрузите диск установки агента на сервер системы виртуализации Proxmox VE. Например, выполните команду:

```
cd /mnt/pve/nfsproxmox/template
wget адрес_архива/ProxmoxAppliance.qcow2
```

5. Подключите диск агента для ранее созданной ВМ. Например, выполните команду:

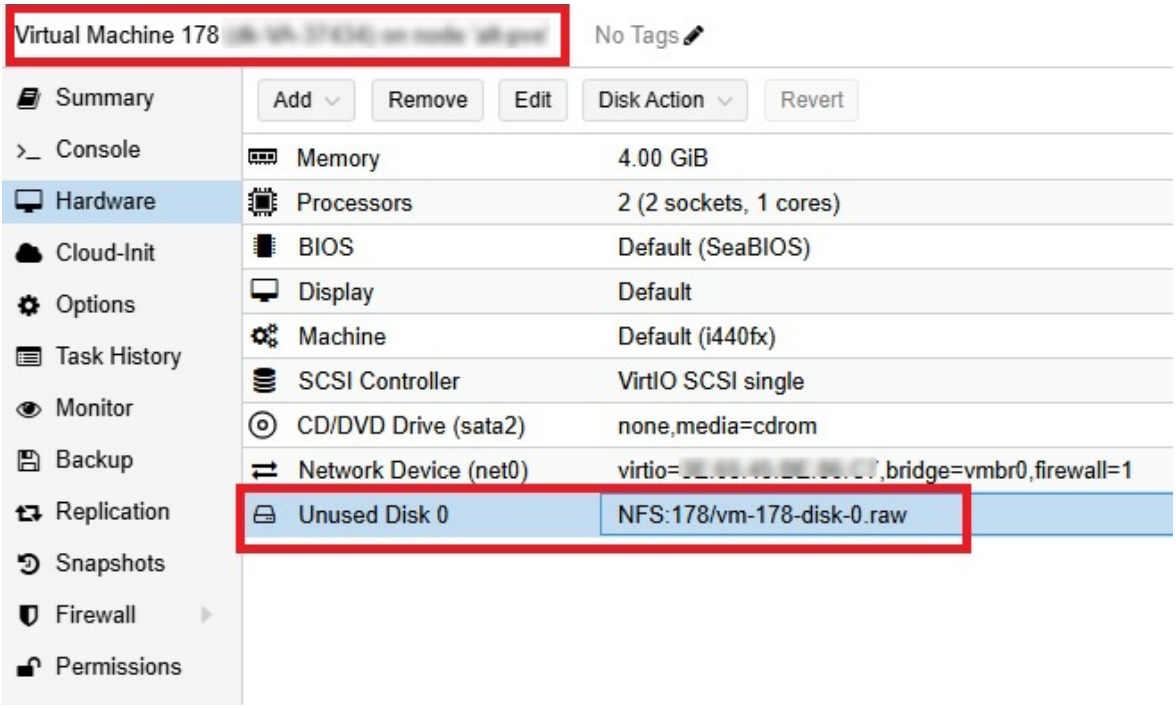
```
qm importdisk 178 ProxmoxAppliance.qcow2 NFS
```

Где:

- 178 – ID виртуальной машины, созданной на шаге 3 данной инструкции;
- ProxmoxAppliance.qcow2 – имя пакета установки агента;
- NFS – имя хранилища в Proxmox, куда будет помещён диск.

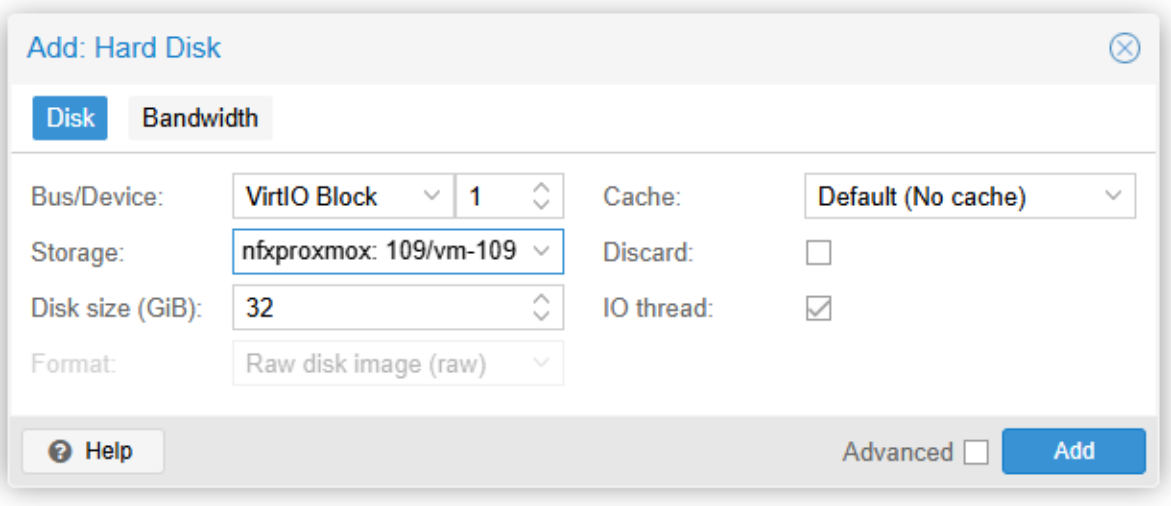
6. Выберите в списке созданную виртуальную машину и перейдите в раздел **Hardware**.

7. Откройте подключенный диск с именем **Unused Disk 0**.



© ООО Киберпротект, 2026

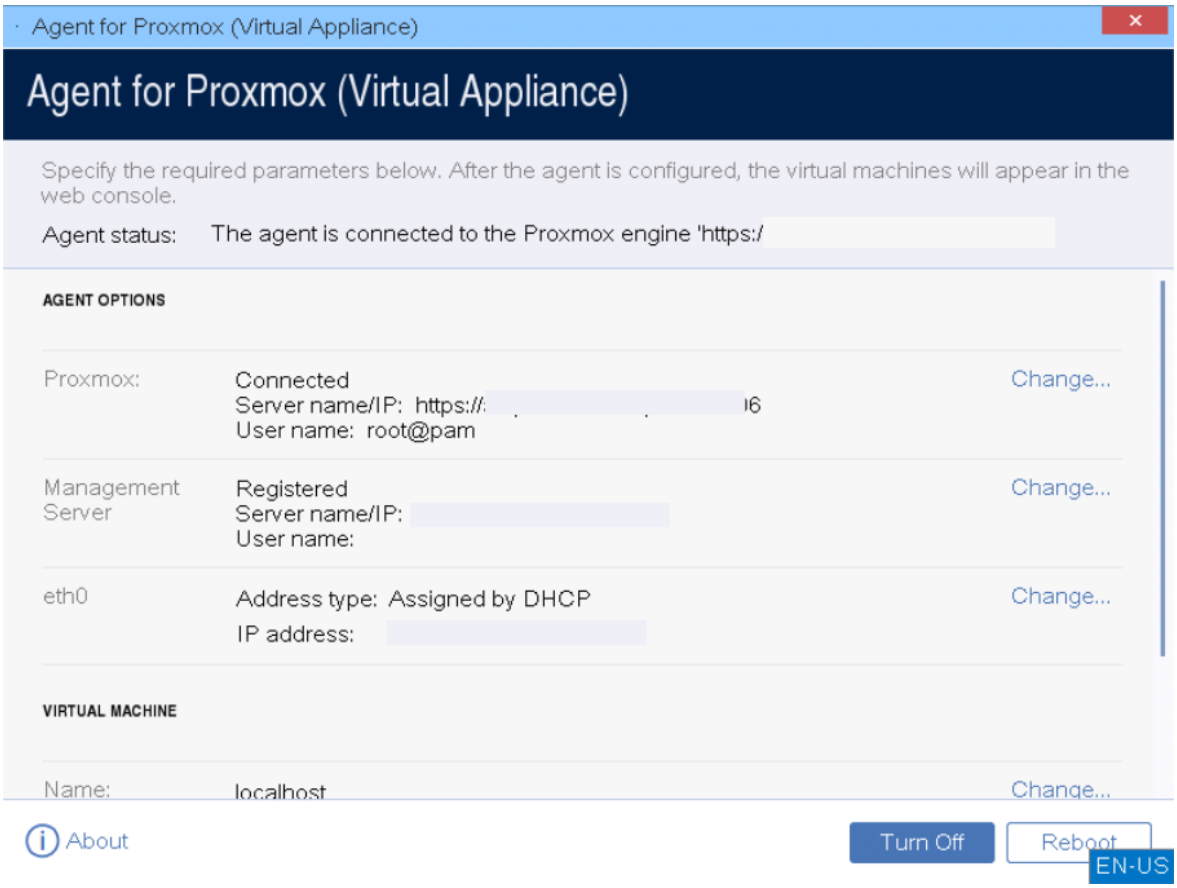
8. В поле **Bus/Device** выберите **VirtIO Block**.



9. Установите для нового диска первый приоритет в порядке загрузки:
   a. Выберите в списке виртуальную машину и нажмите **Options**.
   b. Выберите **Boot Order** и нажмите **Edit**.
   c. Перенесите диск, импортированный из пакета установки, на первое место в списке и поставьте для него галочку **Enabled**.
10. Подключитесь к консоли виртуальной машины.
11. В разделе **Proxmox** нажмите **Change** и укажите:
    - URL-адрес системы виртуализации Proxmox VE в формате https://<IP-адрес>:8006

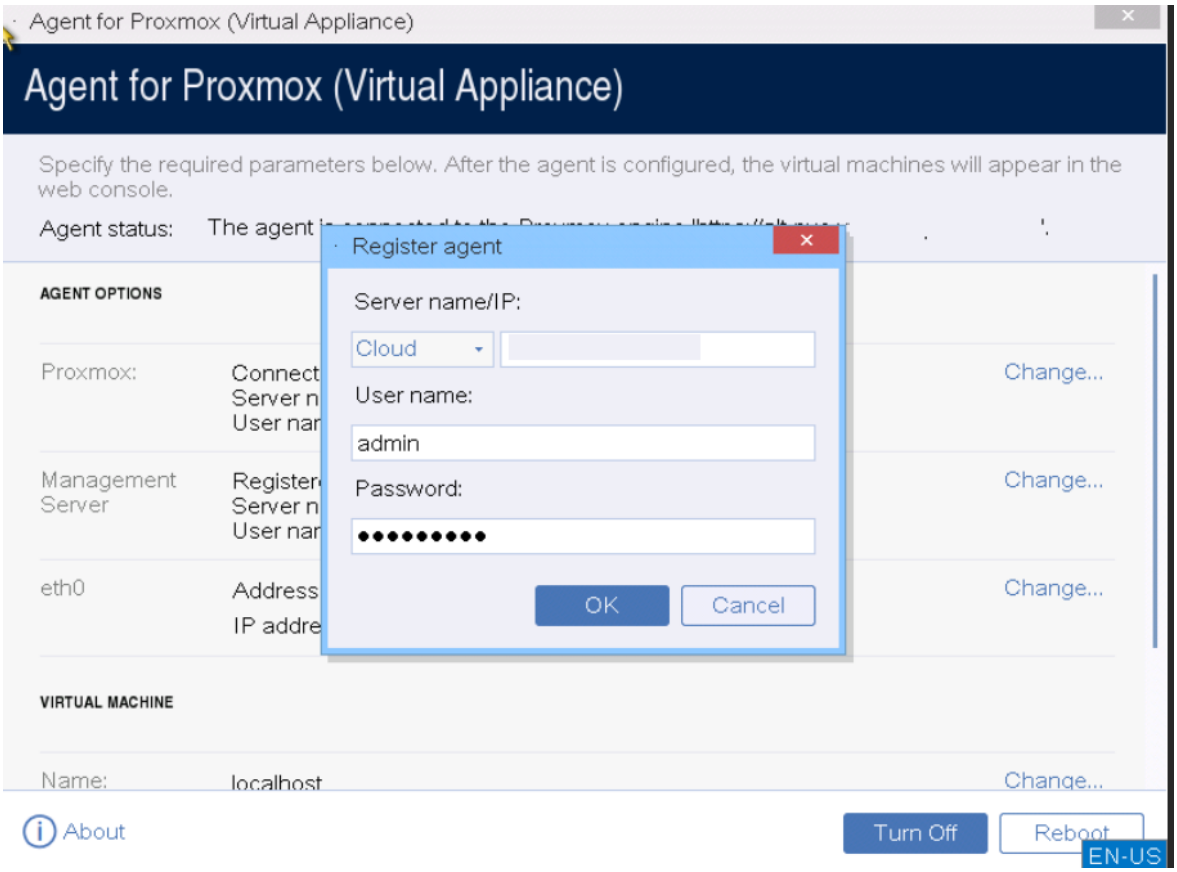
      Где:
      - <IP-адрес> – IP-адрес системы виртуализации Proxmox VE;
      - 8006 – порт подключения.
    - имя пользователя и пароль администратора.

© ООО Киберпротект, 2026



12. В разделе **Management Server** нажмите **Change** и укажите IP-адрес сервера управления Кибер Бэкап и учетные данные для подключения к нему.

© ООО Киберпротект, 2026



13. Перезапустите виртуальную машину.
14. Убедитесь, что в разделе **Устройства** веб-консоли Кибер Бэкап отображаются устройства Proxmox VE.

2.6.5 Автоматическая установка или автоматическое удаление

2.6.5.1 Автоматическая установка или автоматическое удаление в Windows

В этом разделе показано, как установить или удалить Кибер Бэкап в автоматическом режиме на машине с Windows, используя установщик Windows (программа msiexec). В домене Active Directory можно также выполнять автоматическую установку с помощью групповой политики: см. раздел "Развертывание агентов с использованием групповой политики" (стр. 179).

При установке можно использовать файл, называемый **преобразованием** (MST-файл). Преобразование – это файл с параметрами установки. В качестве альтернативного варианта можно указать параметры прямо в командной строке.

Предварительные требования

В этом режиме установки требуется распространяемый компонент Microsoft Visual C++ 2022 версии не ниже 14.42.34438. Проверьте наличие этого компонента на машине или установите его перед выполнением установки Кибер Бэкап. После установки пакета может потребоваться

© ООО Киберпротект, 2026

перезагрузка. Распространяемый пакет Microsoft Visual C++ можно скачать по ссылке https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Создание MST-преобразования и извлечение пакетов установки

1. Войдите как администратор и запустите программу установки.
2. Щелкните **Создать MST- и MSI-файлы для автоматической установки**.
3. В разделе **Устанавливаемые компоненты** выберите компоненты, которые требуется установить. Пакеты установки для этих компонентов будут извлечены из программы установки.
4. Проверьте и при необходимости измените параметры установки, которые будут добавлены в MST-файл.
5. Нажмите кнопку **Создать**.

В результате создается MST-файл, а установочные MSI-пакеты и CAB-пакеты извлекаются в указанную папку.

Установка или удаление продукта с использованием преобразования MST

Чтобы установить продукт, выполните следующую команду:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Чтобы удалить продукт, выполните следующую команду:

```
msiexec /x <package name> TRANSFORMS=<transform name>
```

В этих командах:

- <имя пакета> – это имя MSI-файла. Этот файл имеет имя **AB_AIP64.msi**.
- <имя преобразования> – это имя преобразования. Этот файл имеет имя **AB_AIP64.msi.mst**.

Примеры

- Установка продукта с использованием преобразования MST.

  ```
  msiexec /i AB_AIP64.msi TRANSFORMS=AB_AIP64.msi.mst
  ```

- Удаление продукта с использованием преобразования MST.

  ```
  msiexec /x AB_AIP64.msi TRANSFORMS=AB_AIP64.msi.mst
  ```

Установка или удаление продукта с указанием параметров вручную

Выполните следующую команду:

```
msiexec /i <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

<имя пакета> – это имя MSI-файла. Этот файл имеет имя **AB_AIP64.msi**.

© ООО Киберпротект, 2026

Доступные параметры и их значения описаны в разделе «Параметры автоматической установки или автоматического удаления».

Примеры

- Установка сервера управления и компонентов для удаленной установки.

```
msiexec.exe /i AB_AIP64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en CMS_USE_SYSTEM_ACCOUNT=1
```

- Установка агента для Windows, программы командной строки и программы Мониторинг Защиты Данных. Регистрация машины с агентом на ранее установленном сервере управления.

```
msiexec.exe /i AB_AIP64.msi /l*v my_log.txt /qn
ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonit
or TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
```

- Удаление всех компонентов продукта и их настроек.

```
msiexec.exe /i AB_AIP64.msi /l*v my_log.txt /qn TARGETDIR="C:\Program Files\Acronis"
REMOVE=ALL DELETE_ALL_SETTINGS=1
```

Параметры автоматической установки или автоматического удаления

В этом разделе описаны параметры, которые используются при автоматической установке или автоматическом удалении в Windows.

Кроме этих параметров можно использовать другие параметры msiexec, как описано по ссылке https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Параметры установки

Стандартные параметры

ADDLOCAL= <список компонентов>

Компоненты для установки, разделенные запятыми без символов пробела. Все указанные компоненты необходимо извлечь из программы установки до установки.

Полный список компонентов указан ниже.

Компонент	Необходимо установить вместе с	Разрядность	Имя / описание компонента
AcronisCentralizedManagementServer	WebConsole	64-разрядная	Сервер управления

© ООО Киберпротект, 2026

WebConsole	AcronisCentralizedManagementServer	64-разрядная	Веб-консоль
ComponentRegisterFeature	AcronisCentralizedManagementServer	64-разрядная	Компоненты для удаленной установки
AgentsCoreComponents		64-разрядная	Компоненты Core для агентов
BackupAndRecoveryAgent	AgentsCoreComponents	64-разрядная	Агент для Windows
ArxAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для Exchange
ArsAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для SQL
ARADAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для Oracle
AcronisESXSupport	AgentsCoreComponents	64-разрядная	Агент для VMware (Windows)
HyperVAgent	AgentsCoreComponents	64-разрядная	Агент для Hyper-V
ESXVirtualAppliance		64-разрядная	Агент для VMware (виртуальное устройство)
CommandLineTool		64-разрядная	Программа командной строки
TrayMonitor	BackupAndRecoveryAgent	64-разрядная	Мониторинг Защиты Данных

© ООО Киберпротект, 2026

BackupAndRecoveryBootableComponents		64-разрядная	Мастер создания загрузочных носителей
PXEServer		64-разрядная	PXE-сервер
StorageServer	BackupAndRecoveryAgent	64-разрядная	Узел хранения
CommunigateAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для CommuniGate Pro
PostgreSqlAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для PostgreSQL
WorkmailAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для VK WorkMail

TARGETDIR=<путь>

Папка, в которую будет установлен продукт.

REBOOT=ReallySuppress

Если данный параметр указан, перезапуск машины запрещен.

CURRENT_LANGUAGE=<ИД языка>

Язык продукта. Доступные значения: en, en_GB, ru.

REGISTRATION_ADDRESS=<имя или IP-адрес хоста>:<порт>

Имя хоста или IP-адрес машины, на которой установлен сервер управления. Агенты и узел хранения, указанные в параметре ADDLOCAL, будут зарегистрированы на этом сервере управления. Порт должен быть обязательно указан, если он отличается от установленного по умолчанию (9877).

Необходимо указать параметр REGISTRATION_TOKEN или параметры REGISTRATION_LOGIN и REGISTRATION_PASSWORD.

REGISTRATION_TOKEN=<маркер>

Маркер регистрации, сгенерированный на веб-консоли Кибер Бэкап, как описано в разделе Развертывание агентов с использованием групповой политики.

REGISTRATION_LOGIN=<имя пользователя> и REGISTRATION_PASSWORD=<пароль>

Имя пользователя и пароль администратора сервера управления.

REGISTRATION_TENANT=<идентификатор отдела>

© ООО Киберпротект, 2026

Отдел в организации. Агенты и узел хранения, указанные в параметре ADDLOCAL, будут добавлены в этот отдел.

Чтобы узнать идентификатор отдела, на веб-консоли Кибер Бэкап щелкните **Настройки** > **Учетные записи**, выберите нужный отдел и щелкните **Подробнее**.

Этот параметр не работает без параметра REGISTRATION_TOKEN или параметров REGISTRATION_LOGIN и REGISTRATION_PASSWORD. В этом случае компоненты будут добавлены в организацию.

Если данный параметр не указан, компоненты будут добавлены в организацию.

REGISTRATION_REQUIRED={0,1}

Результат установки при сбое регистрации. Если значение равно 1, установка завершится сбоем. Если значение равно 0, установка завершается успешно, даже если компонент не зарегистрирован.

REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY= <значение открытого ключа>

Эти взаимоисключающие параметры определяют метод проверки сертификата сервера управления при регистрации. Проверьте сертификат, и таким образом вы проверите подлинность сервера управления для предотвращения атак MITM.

Если значение равно 1, для проверки подлинности используется системный центр сертификации или пакет центра сертификации, который прилагается к продукту. Если указан закрепленный открытый ключ, он используется для проверки подлинности. Если значение равно 0 или параметры не указаны, проверка сертификатов не выполняется, но трафик регистрации остается зашифрованным.

/l*v <файл журнала>

Если данный параметр указан, журнал установки в режиме подробного протоколирования сохраняется в указанный файл. Файл журнала можно использовать для анализа проблем с установкой.

Параметры установки сервера управления

WEB_SERVER_PORT=<номер порта>

Порт, который будет использоваться в веб-браузере для доступа к серверу управления. По умолчанию это порт 9877.

ZMQ_PORT=<номер порта>

Порт, который будет использоваться для обмена данными между компонентами продукта. По умолчанию это порт 7780.

SQL_INSTANCE=<экземпляр>

© ООО Киберпротект, 2026

База данных, которая должна использоваться сервером управления. Можно выбрать любую версию Microsoft SQL Server 2012, Microsoft SQL Server 2014 или Microsoft SQL Server 2016. Выбранный экземпляр может использоваться и другими программами.

Без этого параметра будет использоваться встроенная база данных SQLite.

SQL_USER_NAME=<имя пользователя> и SQL_PASSWORD=<пароль>

Учетные данные учетной записи для входа на Microsoft SQL Server. Сервер управления использует эти учетные данные для подключения к выбранному экземпляру SQL Server. Если эти параметры не выбраны, сервер управления будет использовать учетные данные учетной записи службы сервера управления (**CMS User**).

Учетная запись, под которой запущена служба сервера управления

Укажите один из следующих параметров:

- CMS_USE_SYSTEM_ACCOUNT={0,1}
  Если задано значение 1, будет использоваться системная учетная запись.
- CMS_CREATE_NEW_ACCOUNT={0,1}
  Если задано значение 1, будет создана новая учетная запись.
- CMS_SERVICE_USERNAME=<имя пользователя> и CMS_SERVICE_PASSWORD=<пароль>
  Будет использоваться указанная учетная запись.

Параметры установки агента

HTTP_PROXY_ADDRESS=<IP-адрес> и HTTP_PROXY_PORT=<порт>

Прокси-сервер HTTP, который будет использоваться агентом. Если эти параметры не заданы, не будет использовано ни одного прокси-сервера.

HTTP_PROXY_LOGIN=<имя входа> и HTTP_PROXY_PASSWORD=<пароль>

Учетные данные для прокси-сервера HTTP. Используйте эти параметры, если сервер требует проверки подлинности.

HTTP_PROXY_ONLINE_BACKUP={0,1}

SET_ESX_SERVER={0,1}

Если задано значение 0, устанавливаемый агент для VMware не будет подключаться к vCenter Server или хосту ESXi. После установки продолжайте действия, как указано в разделе «Настройка уже зарегистрированного агента для VMware».

Если задано значение 1, укажите следующие параметры:

ESX_HOST=<имя хоста или IP-адрес>

Имя хоста или IP-адрес vCenter Server или хоста ESXi.

ESX_USER=<имя пользователя> и ESX_PASSWORD=<пароль>

Учетные данные для доступа к vCenter Server или хосту ESXi.

© ООО Киберпротект, 2026

Учетная запись, с которой будет запускаться служба агента

Укажите один из следующих параметров:

- MMS_USE_SYSTEM_ACCOUNT={0,1}
  Если задано значение 1, будет использоваться системная учетная запись.
- MMS_CREATE_NEW_ACCOUNT={0,1}
  Если задано значение 1, будет создана новая учетная запись.
- MMS_SERVICE_USERNAME=<имя пользователя> и MMS_SERVICE_PASSWORD=<пароль>
  Будет использоваться указанная учетная запись.

Параметры установки узла хранения

Учетная запись, с которой будет запускаться служба узла агента

Укажите один из следующих параметров:

- CSN_USE_SYSTEM_ACCOUNT={0,1}
  Если задано значение 1, будет использоваться системная учетная запись.
- CSN_CREATE_NEW_ACCOUNT={0,1}
  Если задано значение 1, будет создана новая учетная запись.
- CSN_SERVICE_USERNAME=<имя пользователя> и CSN_SERVICE_PASSWORD=<пароль>
  Будет использоваться указанная учетная запись.

Параметры удаления

REMOVE={<список компонентов>|ALL}

Компоненты для удаления, разделенные запятыми без символов пробела.

Доступные компоненты описаны ранее в этом разделе.

Если задано значение ALL, все компоненты продукта будут удалены. Кроме того, можно указать следующий параметр:

DELETE_ALL_SETTINGS={0,1}

Если задано значение 1, журналы продукта, задачи и настройки конфигурации будут удалены.

2.6.5.2 Автоматическая установка или автоматическое удаление в Linux

В этом разделе описан порядок установки или удаления Кибер Бэкап в автоматическом режиме на машинах под управлением Linux с использованием командной строки.

Порядок установки или удаления продукта

1. Откройте приложение терминала.
2. Выполните следующую команду:

```
<package name> -a <parameter 1> ... <parameter N>
```


© ООО Киберпротект, 2026

Здесь <имя пакета> – это имя пакета установки (файла .i686 или .x86_64).

3. [Только при установке агента для Linux] Если на машине включена безопасная загрузка UEFI, выводится сообщение о том, что необходимо перезагрузить систему после установки. Запомните пароль, который следует использовать (пароль привилегированного пользователя). Во время перезапуска системы выберите управление ключом владельца машины (MOK), выберите **Зарегистрировать MOK** и зарегистрируйте ключ, используя рекомендуемый пароль.

Если безопасная загрузка UEFI включена после установки агента, повторите установку, включая шаг 3. В противном случае последующие операции резервного копирования завершатся сбоем.

Параметры установки

Стандартные параметры

{-a|--auto}

Установить или удалить компоненты продукта без участия пользователя. Чтобы использовать этот параметр при установке агента, необходимо также указать учетную запись, под которой агент будет зарегистрирован в службе Cyber Protect. Для этого можно использовать параметр --token или параметры --login и --password.

{-i |--id=} <список компонентов>

Компоненты для установки, разделенные запятыми без символов пробела.

Для установки доступны указанные ниже компоненты:

Компонент	Необходимо установить вместе с	Описание компонента
AcronisCentralizedManagementServer		Сервер управления
BackupAndRecoveryAgent		Агент для Linux
BackupAndRecoveryBootableComponents;		Мастер создания загрузочных носителей
CommunigateAgentFeature	BackupAndRecoveryAgent	Агент для CommuniGate Pro
K8sAgentFeature	BackupAndRecoveryAgent	Агент для Kubernetes
PostgreSqlAgentFeature	BackupAndRecoveryAgent	Агент для PostgreSQL
WorkmailAgentFeature	BackupAndRecoveryAgent	Агент для VK WorkMail

Если данный параметр не указан, устанавливаются все перечисленные выше компоненты.

© ООО Киберпротект, 2026

--language= <ИД языка>

Язык продукта. Доступные значения: en, en_GB, de, ru.

{-d|--debug}

Если данный параметр указан, журнал установки записывается в режиме подробного протоколирования. Журнал расположен в файле **/var/log/trueimage-setup.log**.

{-t|--strict}

Если данный параметр указан, любое предупреждение при установке приведет к сбою установки. Если данный параметр не указан, установка успешно выполняется, даже при наличии предупреждений.

{-n|--nodeps}

Если параметр указан, отсутствие требуемых пакетов Linux не будет принято во внимание при установке.

Параметры установки сервера управления

{-W |--web-server-port=} <номер порта>

Порт, который будет использоваться в веб-браузере для доступа к серверу управления. По умолчанию это порт 9877.

--ams-tcp-port= <номер порта>

Порт, который будет использоваться для обмена данными между компонентами продукта. По умолчанию это порт 7780.

{-P | --force-postgres}

Если параметр указан, то для установки будет использована СУБД PostgreSQL вместо встроенной СУБД SQLite. Перед установкой сервера управления PostgreSQL необходимо подготовить, как описано в разделе "Установка в Linux" (стр. 67).

Используйте следующие параметры, чтобы указать сведения для подключения к PostgreSQL:

--postgres-user=<имя пользователя>

Имя пользователя для подключения к PostgreSQL. Необходимо указать имя пользователя, который был создан при подготовке PostgreSQL.

--postgres-password=<пароль пользователя>

Пароль пользователя для подключения к PostgreSQL. Необходимо указать пароль пользователя, который был создан при подготовке PostgreSQL.

--postgres-host=<IP-адрес или DNS-имя>

IP-адрес или DNS-имя машины с PostgreSQL.

--postgres-port=<номер порта>

© ООО Киберпротект, 2026

Порт для подключения к PostgreSQL.

Параметры установки агента

Укажите один из следующих параметров:

- --skip-registration
  - Не регистрировать агент на сервере управления.
- {-C |--ams=} <имя хоста или IP-адрес>
  - Имя хоста или IP-адрес машины, на которой установлен сервер управления. Агент будет зарегистрирован на этом сервере управления.

Если установить агент и сервер управления одной командой, агент будет зарегистрирован на этом сервере управления независимо от значения параметра -C.

Необходимо указать параметр token parameter или параметры login и password.

--token= <маркер>

Маркер регистрации, сгенерированный на веб-консоли Кибер Бэкап, как описано в разделе Развертывание агентов с использованием групповой политики.

{-g |--login=} <имя пользователя> и {-w |--password=}<пароль>

Учетные данные администратора сервера управления.

--unit= <идентификатор отдела>

Отдел в организации. Агент будет добавлен в этот отдел.

Чтобы узнать идентификатор отдела, на веб-консоли Кибер Бэкап щелкните **Настройки** > **Учетные записи**, выберите нужный отдел и щелкните **Подробнее**.

Если данный параметр не указан, агент будет добавлен в организацию.

--reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}

Метод проверки сертификата сервера управления при регистрации. Проверьте сертификат, и таким образом вы проверите подлинность сервера управления для предотвращения атак MITM.

Если задано значение https, или параметр не указан, проверка сертификата не выполняется, но трафик регистрации остается зашифрованным. Если задано значение, *отличное от*https, для проверки подлинности используется системный центр сертификации или пакет центра сертификации, который прилагается к продукту или закрепленному открытому ключу соответственно.

--reg-transport-pinned-public-key= <значение открытого ключа>

Значение закрепленного открытого ключа. Этот параметр должен быть указан вместе с параметром --reg-transport=https-pinned-public-key или вместо него.

© ООО Киберпротект, 2026

- --http-proxy-host= <IP-адрес> и --http-proxy-port=<порт>
- --http-proxy-login= <имя входа> и --http-proxy-password=<пароль>
  - Учетные данные для прокси-сервера HTTP. Используйте эти параметры, если сервер требует проверки подлинности.
- --no-proxy-to-ams
  - Агент защиты подключится к серверу управления без использования прокси-сервера, который указан параметрами --http-proxy-host и --http-proxy-port.

Параметры удаления

{-u|--uninstall}

Удаляет продукт.

--purge

Удаляет журналы продукта, задачи и настройки конфигурации.

Параметры информации

{-?|--help}

Показано описание параметров.

--usage

Показывает краткое описание использования команды.

{-v|--version}

Показывает версию пакета установки.

--product-info

Показывает имя продукта и версию пакета установки.

--components-list

Показывает список компонент продукта, включенных в пакет установки.

--snapapi-list

Показывает список версий модуля Snap API, включенных в пакет установки. Данный модуль обеспечивает создание моментальных снимков тома.

Примеры

- Установка сервера управления.

```
./CyberBackup_17_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Установка сервера управления, указание нестандартных портов.

© ООО Киберпротект, 2026

```
./CyberBackup_17_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --web-server-port 6543 --ams-tcp-port 8123
```

- Установка сервера управления с использованием СУБД PostgreSQL.

```
./CyberBackup_17_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --force-postgres --postgres-user=cyberbackup --postgres-password=69c64fee29d24024b219578ecd9f5d88 --postgres-host=127.0.0.1 --postgres-port=5432
```

- Установка агента для Linux и его регистрация на указанном сервере управления.

```
./CyberBackup_17_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 --login root --password 123456
```

- Установка агента для Linux и его регистрация на указанном сервере управления в указанном отделе.

```
./CyberBackup_17_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 --login root --password 123456 -unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

- Удаление Кибер Бэкап.

```
./CyberBackup_17_64-bit.x86_64 -a -u
```

2.6.5.3 Развертывание агентов с использованием групповой политики

Агент для Windows можно централизованно устанавливать (или развертывать) на машинах в составе домена Active Directory с помощью групповой политики.

В этом разделе описывается настройка объекта групповой политики для развертывания агентов на машинах во всем домене или в его организационной единице.

Каждый раз при входе машины в домен результирующий объект групповой политики проверяет, установлен и зарегистрирован ли на ней агент.

Предварительные требования

Перед развертыванием агента убедитесь в том, что выполнены перечисленные ниже условия.

- Имеется домен Active Directory, контроллер которого работает под управлением Microsoft Windows Server.
- Вы входите в состав группы **Администраторы домена**.
- Вы загрузили программу установки **Все агенты для установки в Windows**. Ссылка для скачивания доступна на странице **Добавить устройства** на веб-консоли Кибер Бэкап.
- Выполнены предварительные условия для автоматической установки агента в среде Windows (см. "Автоматическая установка или автоматическое удаление в Windows" (стр. 167)).

© ООО Киберпротект, 2026

Шаг 1. Формирование маркера регистрации

Маркер регистрации передает ваше удостоверение в программу установки, не сохраняя имя входа и пароль для веб-консоли Кибер Бэкап. Это позволяет зарегистрировать любое количество машин в учетной записи. Чтобы обеспечить более высокий уровень безопасности, маркер имеет ограниченный срок действия.

Формирование маркера регистрации

1. Войдите в веб-консоль Кибер Бэкап с учетными данными той учетной записи, для которой необходимо назначить машины.
2. Щелкните **Физические и виртуальные машины** > **Добавить**.
3. Прокрутите вниз до поля **Маркер регистрации** и нажмите кнопку **Создать**.
4. Укажите срок действия маркера и нажмите кнопку **Создать маркер**.
5. Скопируйте маркер или запишите его. Сохраните маркер, если он понадобится в будущем.

   Для просмотра уже сформированных маркеров и управления ими можно щелкнуть **Управление активными маркерами**. Имейте в виду, что из соображений безопасности в этой таблице не отображаются полные значения маркеров.

Шаг 2. Создание MST-преобразования и извлечение пакета установки

1. Войдите как администратор на любую машину в домене.
2. Создайте общую папку, в которой будут находиться пакеты установки. Убедитесь, что у пользователей домена есть доступ к этой папке (для этого можно, например, оставить значение параметра общего доступа по умолчанию для категории **Все**).
3. Запустите программу установки.
4. Щелкните **Создать MST- и MSI-файлы для автоматической установки**.
5. Проверьте и при необходимости измените параметры установки, которые будут добавлены в MST-файл. Указывая способ подключения к серверу управления, выберите **Используйте маркер регистрации** и введите сгенерированный маркер.
6. Щелкните **Продолжить**.
7. В поле **Сохранить файлы в** укажите путь к созданной папке.
8. Нажмите кнопку **Создать**.

В результате будет сформировано MST-преобразование, а установочные MSI-пакеты и CAB-пакеты будут извлечены в созданную вами папку.

Шаг 3. Настройка объектов групповой политики

1. Войдите на контроллер домена с правами администратора домена. Если в домене больше одного контроллера, это можно сделать на любом из них.
2. Если вы планируете развернуть агент в рамках организационной единицы, она должна быть создана до начала установки. В противном случае пропустите этот шаг.

© ООО Киберпротект, 2026

3. В меню **Пуск** выберите пункт **Администрирование**, а затем щелкните **Управление групповой политикой**.
4. Правой кнопкой мыши щелкните имя домена или организационной единицы, а затем щелкните **Создать объект GPO в этом домене и связать его**.
5. Назовите новый объект групповой политики **Агент для Windows**.
6. Откройте объект групповой политики **Агент для Windows** для изменения. Чтобы сделать это, в разделе **Объекты групповой политики** щелкните правой кнопкой мыши объект групповой политики, а затем щелкните **Изменить**.
7. В оснастке «Редактор объектов групповой политики» разверните узел **Конфигурация компьютера**.
8. Разверните узел **Политики** > **Конфигурация программ**.
9. Щелкните правой кнопкой мыши узел **Установка программ**, выберите пункт **Создать**, затем щелкните **Пакет**.
10. Выберите MSI-пакет установки агента в созданной ранее общей папке и нажмите кнопку **Открыть**.
11. В диалоговом окне **Развертывание программ** выберите **особый**, затем нажмите кнопку **OK**.
12. На вкладке **Изменения** нажмите кнопку **Добавить** и выберите созданное ранее MST-преобразование.
13. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Развертывание программ**.

2.6.6 Регистрация агента вручную

Помимо регистрации машины на сервере управления Кибер Бэкап при установке агента, можно также зарегистрировать ее в интерфейсе командной строки. Это может понадобиться, например, когда агент установлен, но при этом не удалось выполнить автоматическую регистрацию, или необходимо зарегистрировать существующую машину под новой учетной записью.

Перед регистрацией в Windows убедитесь, что были выполнены предварительные условия для автоматической установки (см. "Автоматическая установка или автоматическое удаление в Windows" (стр. 167)).

Порядок регистрации агента

В командной строке машины, на которой установлен агент, выполните одну из следующих команд:

- Регистрация агента по учетной записи администратора

  ```
  <путь_к_программе_регистрации> -o register -a <адрес_сервера_управления:порт> -u <имя_пользователя> -p <пароль>
  ```

  <имя_пользователя> и <пароль> – учетные данные учетной записи администратора, для которой будет зарегистрирован агент.
- Регистрация агента в отделе по идентификатору отдела

© ООО Киберпротект, 2026

```
<путь_к_программе_регистрации> -o register -a <адрес_сервера_управления:порт> -u
<имя_пользователя> -p <пароль> --tenant <идентификатор_отдела>
```

Чтобы узнать идентификатор отдела, в веб-консоли Кибер Бэкап щелкните **Настройки** > **Учетные записи**, выберите нужный отдел и щелкните **Сведения**.

Администраторы могут регистрировать агентов только на своём уровне в иерархии организации. Администраторы отдела могут регистрировать агентов в собственных отделах и их подотделах. Администраторы организации могут регистрировать агентов во всех отделах. Дополнительную информацию о разных учетных записях администратора см. в разделе "Управление учетными записями пользователей и отделами организации" (стр. 806).

- Регистрация агента по маркеру регистрации

```
<путь_к_программе_регистрации> -o register -a <адрес_сервера_управления:порт> --token
<маркер_регистрации>
```

Маркер регистрации – это последовательность из 12 символов, разделенных дефисами на три части. Дополнительную информацию о создании маркера регистрации см. в разделе "Развертывание агентов с использованием групповой политики" (стр. 179).

Отмена регистрации агента

В командной строке машины, на которой установлен агент, выполните следующую команду:

```
<путь_к_программе_регистрации> -o unregister
```

2.6.6.1 Примеры

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspasswd
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspasswd --tenant 590b1dd7-8adb-11ea-bf44-
0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o unregister
```


© ООО Киберпротект, 2026

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a https://10.250.144.179:9877 -u johndoe -p johnspasswd
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a https://10.250.144.179:9877 -u johndoe -p johnspasswd --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a https://10.250.144.179:9877 --token 34F6-8C39-4A5C
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

2.6.6.2 Ввод паролей со специальными символами или пробелами

Если пароль содержит специальные символы или пробелы, заключите его в кавычки при вводе в командной строке.

```
<путь_к_программе_регистрации> -o register -a <адрес_сервера_управления:порт> -u <имя_пользователя> -p "<пароль>"
```

Пример для Windows:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a https://10.250.144.179:9877 -u johndoe -p "johns passwd"
```

В случае ошибок:

1. Зашифруйте пароль в формате Base64.
2. В командной строке укажите зашифрованный пароль, добавив параметр -b или --base64.

Пример для Windows:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

2.6.7 Установка и настройка узла хранения

Узел хранения – это сервер, предназначенный для оптимизации использования различных ресурсов (таких как объем корпоративного хранилища, пропускная способность сети или загрузка процессоров производственных серверов), требуемых для защиты корпоративных данных. Это достигается путем организации и управления хранилищами, выделенными для корпоративных резервных копий (см. "Добавление управляемого хранилища" (стр. 187)).

© ООО Киберпротект, 2026

Один из сценариев использования узла хранения – обеспечить централизованный доступ к ленточным накопителям или библиотекам, например, для резервного копирования и восстановления данных с нескольких устройств на один и тот же ленточный накопитель или библиотеку (управляемое хранилище на ленте).

Другим вариантом использования является включение расширенных возможностей дедупликации, когда данные на нескольких устройствах могут быть сопоставлены друг с другом (дедуплицированы) и храниться в едином расположении (управляемом хранилище с включенной дедупликацией).

Примечание
Для всех резервных копий в формате TIBX по умолчанию включена дедупликация в архиве (подробнее см. раздел "Дедупликация в архиве" (стр. 348)).

2.6.7.1 Установка узла хранения

Перед установкой узла хранения убедитесь, что машина соответствует системным требованиям.

Порядок установки узла хранения в ОС Linux

Подготовка

1. В системе, в которой не используется диспетчер пакетов RPM, необходимо установить этот диспетчер вручную. Как привилегированный пользователь выполните команду (например):

   ```
   apt-get install rpm
   ```

2. Убедитесь в том, что на машине установлены необходимые пакеты Linux.
3. Дайте разрешение на исполнение установочному файлу. Выполните следующую команду:

   ```
   chmod +x CyberBackup_*
   ```

Подготовка к установке в ОС Astra Linux SE

Перед установкой продукта в ОС Astra Linux SE ознакомьтесь с разделом "Совместимость с ОС Astra Linux SE" (стр. 42) и выполните следующие шаги. Предполагается, что включен режим замкнутой программной среды.

1. Распакуйте дистрибутив:

   ```
   tar --xattrs --xattrs-include=* -xvf CyberBackup_18_64-bit.x86_64.tar
   ```

2. Запустите файл установки с правами привилегированного пользователя:

   ```
   ./CyberBackup_18_64-bit.x86_64
   ```

3. Обновите образы initramfs:

© ООО Киберпротект, 2026

```
update-initramfs -u -k all
```

4. Перезагрузите систему.

Установка

1. Запустите файл установки (файл .i686 или .x86_64) как привилегированный пользователь:

```
./CyberBackup_18_64-bit.x86_64
```

2. Примите условия лицензионного соглашения.
3. Укажите устанавливаемые компоненты:
   a. Снимите флажок **Сервер управления**.
   b. Установите флажок **Узел хранения**. Флажок **Агент для Linux** будет установлен автоматически.
   c. Нажмите кнопку **Далее**.
4. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:
   a. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   b. Укажите учетные данные администратора сервера управления или маркер регистрации.
      Дополнительную информацию о создании маркера регистрации см. в разделе "Развертывание агентов с использованием групповой политики" (стр. 179).
   c. Нажмите кнопку **Далее**.
5. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов, затем нажмите клавишу **ВВОД**.
   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе "Отделы и административные учетные записи" (стр. 806).

   Примечание
   Если в процессе установки возникнет ошибка сборки модуля ядра "Не удалось построить модуль ядра SnapAPI. Операции с резервными копиями на уровне дисков будут недоступны", продолжите установку. После завершения установки решите проблему с помощью статьи базы знаний Сборка модуля SnapAPI для Linux.

6. Если на машине включена безопасная загрузка UEFI, выводится сообщение о том, что необходимо перезагрузить систему после установки. Запомните пароль, который следует использовать (пароль привилегированного пользователя).

© ООО Киберпротект, 2026

Примечание
В процессе установки создается новый ключ, который используется для подписи модулей ядра. Необходимо зарегистрировать этот ключ в списке владельцев ключей машины (Machine Owner Key, MOK), перезапустив машину. Если не зарегистрировать ключ, агент не будет работать. Если безопасная загрузка UEFI включена после установки агента, повторите установку, включая шаг 6.

7. После завершения установки выполните одно из следующих действий.
   - Нажмите кнопку **Перезапустить**, если на предыдущем шаге вам было предложено перезапустить систему.

     Во время перезапуска системы выберите управление ключом владельца машины (MOK), выберите **Зарегистрировать MOK** и зарегистрируйте ключ, используя пароль, предложенный на предыдущем шаге.
   - В противном случае нажмите **Выход**.

Сведения об устранении неполадок представлены в файле /usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL.

Порядок установки узла хранения в ОС Windows

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.
4. Щелкните **Настройка параметров установки**.
5. В разделе **Устанавливаемые компоненты** щелкните **Изменить**.
6. Выберите устанавливаемые компоненты:
   - Для установки узла хранения установите флажок **Узел хранения**. Флажок **Агент для Windows** будет установлен автоматически.
   - Если на этой машине не нужно устанавливать другие компоненты, снимите соответствующие флажки.

   Чтобы продолжить, нажмите кнопку **Готово**.
7. Укажите сервер управления, на котором будут зарегистрированы компоненты:
   a. Перейдите на **Сервер управления Кибер Бэкап** и щелкните **Указать**.
   b. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   c. Укажите учетные данные администратора сервера управления или маркер регистрации.

      Дополнительную информацию о создании маркера регистрации см. в разделе "Развертывание агентов с использованием групповой политики" (стр. 179).
   d. Нажмите кнопку **Готово**.

© ООО Киберпротект, 2026

8. При поступлении запроса выберите, добавлять ли машину с узлом хранения в организацию или в один из отделов.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе "Отделы и административные учетные записи" (стр. 806).
9. [Необязательно] Измените другие настройки установки, как описано в разделе "Настройка параметров установки в ОС Windows" (стр. 63).
10. Нажмите **Установить**, чтобы продолжить установку.
11. После завершения установки нажмите кнопку **Закрыть**.

2.6.7.2 Добавление управляемого хранилища

Управляемое хранилище может быть организовано:

- В локальной папке.
  - На жестком диске, локальном по отношению к узлу хранения.
  - На хранилище SAN, которое операционная система определяет как локально подключенное устройство.
- В сетевой папке.
  - В общей папке SMB/CIFS.
  - На хранилище SAN, которое операционная система определяет как сетевую папку.
  - На устройстве NAS.
- В ленточном устройстве, локально подключенном к узлу хранения.

  Хранилища на основе ленточных устройств создаются в виде пулов лент. Один пул лент присутствует по умолчанию. При необходимости можно создать другие пулы лент, как описано далее в этом разделе.

Репликация резервной копии с использованием управляемого хранилища имеет свои особенности (см. разделы "Репликация" (стр. 306) и "Замечания по использованию узла хранения" (стр. 309)).

Порядок создания управляемого хранилища в локальной или сетевой папке

1. Выполните одно из следующих действий:
   - Щелкните **Хранилища резервных копий** > **Добавить расположение**, затем щелкните **Узел хранения**.
   - При создании плана защиты щелкните **Место сохранения резервной копии** > **Добавить хранилище**, затем щелкните **Узел хранения**.
   - Щелкните **Настройки** > **Узел хранения**, выберите узел хранения, который будет управлять расположением, затем щелкните **Добавить хранилище**.
2. В поле **Имя** укажите уникальное имя для хранилища. «Уникальный» означает, что не должно быть другого расположения с тем же именем, которое управляется тем же узлом хранения.

© ООО Киберпротект, 2026

3. [Необязательно] Выберите узел хранения, который будет управлять этим хранилищем. Если вы выбрали последний параметр в шаге 1, вы не сможете изменять узел хранения.
4. Выберите имя узла хранения или IP-адрес, которые будут использоваться агентом для доступа к хранилищу.

   По умолчанию выбрано имя узла хранения. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою доступа. Чтобы изменить эту настройку позже, щелкните **Хранилища резервных копий** > **Хранилище** > **Изменить**, затем измените значение поля **Адрес**.
5. Введите путь к папке или выберите ее в проводнике.
6. Нажмите кнопку **Готово**. Программа проверит доступ к указанной папке.
7. [Необязательно] Включите дедупликацию резервных копий в хранилище.

   Дедупликация минимизирует трафик резервного копирования и уменьшает размеры резервных копий в хранилище, удаляя дублированные блоки на диске.

   Дополнительную информацию об ограничениях дедупликации см. в разделе "Ограничения дедупликации" (стр. 189).
8. [Только если включена дедупликация] Укажите или измените значение в поле **Путь к базе данных дедупликации**.

   Это должна быть папка на жестком диске, локальном по отношению к узлу хранения. Для повышения производительности системы рекомендуется создавать базу данных дедупликации и управляемое хранилище на разных дисках.

   Дополнительную информацию о базе данных дедупликации см. в разделе "Рекомендации по дедупликации" (стр. 190).
9. [Необязательно] Укажите, нужно ли защитить хранилище паролем. Все данные, которые записываются в это хранилище, будут защищены. При чтении пароль будет подставлен узлом хранения незаметно для пользователя.

   Подробнее см. в разделе "Защита хранилища паролем" (стр. 189).
10. Нажмите кнопку **Готово**, чтобы создать хранилище.

Для создания управляемого хранилища на ленточном устройстве

1. Щелкните **Хранилища резервных копий** > **Добавить хранилище**, или при создании плана защиты щелкните **Место сохранения резервной копии** > **Добавить хранилище**.
2. Выберите **Ленты**.
3. [Необязательно] Выберите узел хранения, который будет управлять этим хранилищем.
4. Выполните действия, описанные в разделе "Создание пула" (стр. 782), начиная с шага 4.

Примечание
По умолчанию агенты используют имя узла хранения для доступа к управляемому хранилищу на основе ленточных устройств. Чтобы агенты использовали IP-адрес узла хранения, щелкните **Хранилища резервных копий** > **Хранилище** > **Изменить**, затем измените значение поля **Адрес**.

Рекомендация по переподключению хранилищ

© ООО Киберпротект, 2026

Управляемые хранилища рекомендуется переподключать к узлам хранения с той же ОС, что и при отключении хранилищ. В противном случае переподключение может занять долгое время.

2.6.7.3 Защита хранилища паролем

Если для хранилища установлена защита паролем, то при подключении хранилища к другому узлу хранения потребуется ввести пароль. Если носитель хранилища украден или доступ к нему получил неавторизованный пользователь, злоумышленник не сможет получить доступ к содержимому хранилища без доступа к узлу хранения.

Эта защита паролем не имеет ничего общего с защитой паролем резервной копии, которая задана в плане защиты и выполняется агентом. Если резервная копия уже защищена паролем, защита паролем на стороне узла хранения применяется поверх защиты паролем, выполненной агентом.

Для существующих управляемых хранилищ включение этой опции невозможно. Защита хранилища паролем поддерживается только для формата резервных копий "Версия 11" (см. раздел "Формат резервной копии" (стр. 347)).

Как защитить хранилище паролем

На этапе развертывания управляемого хранилища (см. раздел "Добавление управляемого хранилища" (стр. 187)) укажите и подтвердите пароль, который будет служить ключом защиты.

Поддерживаются следующие уровни защиты хранилища: **Базовый**, **Средний**, **Высокий**.

Чем выше уровень защиты, тем лучше будут защищены резервные копии.

Пароль на диске не хранится. Такая схема защиты позволяет обезопасить резервные копии от несанкционированного доступа, но восстановить утраченный пароль невозможно.

2.6.7.4 Дедупликация

В разделе описаны особенности дедупликации резервных копий на узле хранения. О дедупликации в архиве см. раздел "Дедупликация в архиве" (стр. 348).

Ограничения дедупликации

Общие ограничения

Дедупликация резервных копий на узле хранения поддерживается только для формата резервных копий "Версия 11" (см. раздел "Формат резервной копии" (стр. 347)).

Не поддерживается дедупликация резервных копий, защищенных паролем. Чтобы одновременно использовать и дедупликацию, и защиту паролем, не защищайте резервные копии, но укажите для них хранилище, где поддерживается как дедупликация, так и защита паролем.

Резервное копирование на уровне дисков

Дедупликация дисковых блоков не выполняется, если размер единицы выделения памяти (также называемый размером кластера или блока) тома не кратен 4 КБ.

© ООО Киберпротект, 2026

Примечание
Размер единицы выделения памяти у большинства томов NTFS и ext3 равен 4 КБ. Это позволяет выполнять дедупликацию на уровне блоков. Другие примеры подходящих размеров единиц выделения памяти – 8 КБ, 16 КБ и 64 КБ.

Резервное копирование на уровне файлов

Дедупликация файла не выполняется, если файл защищен паролем.

Дедупликация и потоки данных NTFS

В файловой системе NTFS у файла может быть один или несколько связанных с ним дополнительных наборов данных, которые часто называют *альтернативными потоками данных*.

При создании резервной копии такого файла также создается копия альтернативных потоков данных. Однако эти потоки никогда не дедуплицируются, даже если дедуплицирован сам файл.

Рекомендации по дедупликации

Наиболее важные факторы, влияющие на скорость дедупликации:

- скорость доступа к базе данных дедупликации;
- объем оперативной памяти узла хранения;
- количество дедуплицирующих хранилищ, созданное в узле хранения.

Для увеличения производительности дедупликации следуйте рекомендациям ниже.

Размещайте базу данных дедупликации и дедуплицирующее хранилище на разных физических носителях.

В базе данных дедупликации содержатся хэш-значения всех элементов, которые хранятся в хранилище, кроме тех, которые не могут дедуплицироваться (например, файлы, защищенные паролем).

Для увеличения скорости доступа к базе данных дедупликации база данных и хранилище должны быть размещены на разных физических носителях.

Рекомендуется выделить специальные устройства для хранилища и базы данных. Если это невозможно, по крайней мере не размещайте хранилище или базу данных на диске с операционной системой. При работе операционной системы выполняется большое количество операций чтения/записи на жесткий диск, что существенно замедляет процесс дедупликации.

Выбор диска для базы данных дедупликации

- База данных должна находиться на стационарном диске. Не пытайтесь разместить базу данных дедупликации на внешних съемных носителях.

© ООО Киберпротект, 2026

- Чтобы минимизировать время доступа к базе данных, сохраните ее на диске, подключенном напрямую, а не на подключенном сетевом томе. Задержка в сети может существенно снизить производительность дедупликации.
- Примерный объем дискового пространства, необходимого для базы данных дедупликации, вычисляется по следующей формуле:

$$S = U * 90 / 65536 + 10$$

В этой формуле

S – размер диска в ГБ;

U – планируемый объем уникальных данных в хранилище дедуплицированных данных (ГБ).

Например, если планируемый объем уникальных данных в хранилище дедуплицированных данных U = 5 ТБ, для базы данных дедупликации потребуется объем свободного пространства не менее

$$S = 5000 * 90 / 65536 +10 = 17 ГБ$$

Выбор диска для дедуплицирующего хранилища

Для предотвращения потери данных рекомендуется использовать RAID 10, 5 или 6. RAID 0 не рекомендуется, поскольку не является отказоустойчивым. RAID 1 не рекомендуется из-за относительно низкой скорости. Можно использовать как локальные диски, так и SAN.

От 40 до 160 МБ ОЗУ на 1 ТБ уникальных данных

По достижении ограничения дедупликация выполняться не будет, а резервное копирование и восстановление продолжат выполняться. Если вы добавите ОЗУ в узел хранения после следующего резервного копирования, дедупликация восстановится. В общем, чем больше ОЗУ, тем больше размер томов с уникальными данными, которые можно сохранить.

Одно дедуплицирующее хранилище на каждый узел хранения

Настоятельно рекомендуется создавать только одно дедуплицирующее хранилище на узле хранения. В противном случае весь доступный объем ОЗУ будет распределен пропорционально количеству хранилищ.

Отсутствие приложений, конкурирующих за ресурсы

На машине с узлом хранения не должны быть запущены приложения, требующие большого количества системных ресурсов, например, системы управления базами данных (СУБД) или системы планирования ресурсов предприятия (ERP).

Многоядерный процессор с тактовой частотой не менее 2,5 ГГц

Рекомендуется использовать процессор с количеством ядер не менее 4 и тактовой частотой не менее 2,5 ГГц.

© ООО Киберпротект, 2026

Достаточное свободное пространство в хранилище

Для дедупликации в месте сохранения требуется столько же свободного пространства, сколько занимают данные резервной копии сразу после сохранения в хранилище. Без выполнения сжатия или дедупликации в источнике это значение равно размеру исходных данных, резервная копия которых создана во время данной операции резервного копирования.

Высокоскоростная локальная сеть

Рекомендуется скорость локальной сети 1 Гбит. Это позволит программе выполнить 5-6 операций резервного копирования параллельно с дедупликацией без заметного снижения скорости.

Выполните резервное копирование типичной машины перед резервным копированием нескольких машин со сходным содержимым.

При резервном копировании нескольких машин со сходным содержимым рекомендуется сначала выполнить резервное копирование одной машины и подождать завершения индексирования данных резервной копии. После этого резервное копирование остальных машин будет выполняться быстрее за счет эффективной дедупликации. Поскольку резервная копия первой машины была проиндексирована, большая часть данных уже находится в хранилище дедуплицированных данных.

Выполняйте резервное копирование разных машин в разное время.

При резервном копировании большого количества машин распределите операции резервного копирования по времени. Для этого необходимо создать несколько планов защиты с различными расписаниями.

2.6.8 Проверка наличия обновлений программного обеспечения

Эта функциональность доступна только для администраторов организации.

При каждом входе в веб-консоль Кибер Бэкап может проверять, доступна ли новая версия на веб-сайте Киберпротект. Если новая версия доступна, в веб-консоли Кибер Бэкап отображается ссылка на ее скачивание в нижней части каждой страницы на вкладках **Устройства**, **Планы** и **Хранилища резервных копий**. Ссылка также доступна на странице **Настройки** > **Агенты**.

Чтобы отключить автоматические проверки наличия обновлений (включены по умолчанию), измените системную настройку **Обновления**.

Чтобы проверить наличие обновлений вручную, щелкните значок вопроса в верхнем правом углу, затем щелкните **О программе** > **Проверить обновления**.

2.6.9 Управление лицензиями

Лицензирование Кибер Бэкап основано на количестве ресурсов, подлежащих резервному копированию. Подробнее о лицензиях см. в разделе "Издания и лицензии Кибер Бэкап" (стр. 16).

© ООО Киберпротект, 2026

Чтобы приступить к использованию Кибер Бэкап, необходимо добавить на сервер управления хотя бы один лицензионный ключ. Лицензия автоматически назначается машине при применении плана защиты.

Кроме того, лицензии можно назначить и отозвать вручную. Ручные операции с лицензиями доступны только для администраторов организации.

Порядок доступа к странице «Лицензии»

1. Выполните одно из следующих действий:
   - Щелкните **Настройки**.
   - Щелкните значок учетной записи в правом верхнем углу.
2. Щелкните **Лицензии**.

Добавление лицензионного ключа

1. Щелкните **Добавить ключи**.
2. Введите лицензионные ключи.
3. Нажмите кнопку **Добавить**.

2.6.9.1 Управление лицензиями

Назначение лицензии машине

1. Выберите лицензию.

   В программе отобразятся лицензионные ключи, соответствующие выбранной лицензии.
2. Выберите ключ, который нужно назначить.
3. Щелкните **Назначить**.

   В программе отобразятся машины, которым можно назначить выбранный ключ.
4. Выберите машину и нажмите кнопку **Готово**.

Отзыв лицензии для машины

1. Выберите лицензию.

   В программе отобразятся лицензионные ключи, соответствующие выбранной лицензии. Машина, которой назначен ключ, указана в столбце **Кому назначено**.
2. Выберите лицензионный ключ, который нужно отозвать.
3. Щелкните **Отозвать**.
4. Подтвердите операцию.

   Отозванный ключ останется в списке лицензионных ключей. Его можно назначить другой машине.

2.7 Автоматическое обнаружение машин

Функциональность обнаружения машин позволяет выполнять указанные ниже действия.

© ООО Киберпротект, 2026

- Автоматизировать процесс установки агентов защиты и регистрации машины за счет автоматического выявления машин в домене Active Directory (AD) или локальной сети.
- Устанавливать и обновлять агент защиты на нескольких машинах.
- Использовать синхронизацию с Active Directory для уменьшения затрат, связанных с выделением ресурсов и управлением машиной в большой среде AD.

Внимание
Обнаружение машины может выполняться только агентами, установленными на машинах Windows. В настоящее время агент обнаружения может обнаружить не только машины Windows, однако удаленная установка программного обеспечения возможна только на машинах Windows. Если в вашей среде нет машин с установленным агентом, то функция автоматического обнаружения будет скрыта: раздел **Несколько устройств** будет скрыт в мастере **добавления нового устройства**.

После добавления машин на веб-консоль они подразделяются на указанные ниже категории.

- **Обнаружено**: обнаруженные машины без установленного агента защиты.
- **Управляемое**: машины, на которых установлен агент защиты.
- **Незащищенные**: машины, к которым не применен план защиты. Под незащищенными машинами подразумеваются как обнаруженные, так и управляемые машины без примененного плана защиты.
- **Защищено**: машины, к которым применен план защиты.

2.7.1 Принципы работы

При сканировании локальной сети агент обнаружения использует указанные ниже технологии. Обнаружение NetBIOS, Web Service Discovery (WSD) и таблица Address Resolution Protocol (ARP). Агент пытается получить следующие параметры для каждой машины:

- Имя (короткое/имя хоста NetBIOS)
- FQDN
- Домен/рабочая группа
- IP-адреса IPv4/IPv6
- MAC-адреса
- Операционная система (имя/версия/семейство)
- Категория машины (рабочая станция/сервер/контроллер домена)

Когда Active Directory выполняет сканирование, агент дополнительно извлекает параметр "Организационная единица" и более подробную информацию об имени и операционной системе. Он не получает IP-адреса и MAC-адреса.

© ООО Киберпротект, 2026

2.7.2 Предварительные требования

Прежде чем запустить обнаружение машин, необходимо установить агент защиты хотя бы на одной машине в локальной сети (см. "Установка агентов" (стр. 95)), чтобы использовать его как агент обнаружения.

Если вы планируете выполнить обнаружение машин в домене Active Directory, необходимо установить агент как минимум на одной машине в этом домене. Этот агент будет использоваться как агент обнаружения при сканировании Active Directory.

Для успешной удаленной установки агента защиты на машине Windows Server 2012 R2 должно быть установлено обновление KB2999226.

2.7.3 Процесс обнаружения машины

В приведенной ниже схеме указаны основные этапы процесса обнаружения машины.

Как правило, весь процесс автоматического обнаружения состоит из следующих этапов:

© ООО Киберпротект, 2026

1. Выберите метод обнаружения машины:
   - Сканирование Active Directory
   - Сканирование локальной сети
   - Вручную: добавление машины по ее IP-адресу или имени хоста или импорт списка машин из файла

   Первые два метода позволяют автоматически отфильтровывать результаты, чтобы исключить машины с установленными агентами.

   При обнаружении машины вручную выполняется модернизация и перерегистрация существующих агентов. При автоматическом обнаружении с использованием той же учетной записи агент просто обновляется до последней версии (при необходимости). Если используется другая учетная запись, агент обновляется и перерегистрируется в клиенте, которому принадлежит учетная запись.
2. Выберите машины для добавления из списка, полученного в результате выполнение предыдущего действия.
3. Выберите способ добавления машин:
   - Агент защиты и дополнительные компоненты устанавливаются на машинах. Кроме того, они регистрируются на веб-консоли.
   - Машины регистрируются на веб-консоли (если они уже имеют установленный агент).
   - Машины добавляются на веб-консоль службы со статусом **Неуправляемое** без установки каких-либо агентов или компонентов.

   Если для добавления машины вы выбрали один из первых двух методов, можно также выбрать план защиты из существующих планов и применить его к машинам.
4. Укажите учетные данные пользователя с правами администратора на выбранных машинах.
5. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
6. Проверьте, что можете подключиться к машинам, используя указанные учетные данные.

В следующих темах вы получите более подробную информацию о процедуре обнаружения.

2.7.4 Автоматическое и ручное обнаружение

Прежде чем запустить обнаружение, убедитесь, что соблюдены предварительные требования.

Обнаружение машин

1. На веб-консоли выберите пункты **Устройства** > **Физические и виртуальные машины**.
2. Нажмите кнопку **Добавить**.
3. В области **Несколько устройств** щелкните **Windows-only (Только для Windows)**. Откроется мастер обнаружения

© ООО Киберпротект, 2026

4. [Если в вашей организации есть отделы] Выберите отдел. Затем в **агенте обнаружения** вы сможете выбрать агенты, связанные с выбранным отделом и его дочерними отделами.
5. Выберите агент обнаружения, который выполнит сканирование для обнаружения машин.
6. Выберите метод обнаружения:
   - **Поиск в Active Directory**. Убедитесь, что машина с агентом обнаружения входит в домен Active Directory.
   - **Сканировать локальную сеть**. Если выбранному агенту обнаружения не удалось найти никаких машин, выберите другой агент обнаружения.
   - **Укажите вручную или импортируйте из файла**. Вручную определите машины для добавления или импортируйте их из текстового файла.
7. [Если выбран метод обнаружения Active Directory] Выберите метод поиска машин:
   - **В списке организационной единицы**. Выбор группы машин для добавления.
   - **По запросу диалекта LDAP**. Запрос диалект LDAP для выбора машин. **База поиска** определяет места поиска, а **Фильтр** позволяет указать критерий выбора машины.
8. [Если выбран метод обнаружения Active Directory или локальной сети] Используйте список для выбора машин, которые необходимо добавить.

   [Если выбран ручной метод обнаружения] Укажите IP-адреса машины или имена хостов либо импортируйте список машины из текстового файла. Файл должен содержать IP-адреса/имена хостов, по одному на строку. Ниже приводим пример файла:

   ```
   156.85.34.10
   156.85.53.32
   156.85.53.12
   EN-L00000100
   EN-L00000101
   ```

   После добавления адресов машины вручную или их импорте из файла агент попытается выполнить команду ping в отношении добавленных машин и определить их доступность.
9. Выберите действие, которое должно предприниматься после обнаружения:
   - **Установить агенты и зарегистрировать машины**. Компоненты для установки на машинах можно выбрать, щелкнув **Выбор компонентов**. Дополнительную информацию см. в разделе Выбор компонентов для установки. Одновременно можно установить до 100 агентов.

     На экране **Выбор компонентов** укажите учетную запись, с которой будут запускаться службы. Для этого укажите **Учетная запись для входа службы агента**. Можно выбрать один из следующих вариантов:
     - **Использовать учетные записи пользователя услуги** (по умолчанию для службы агента)

       Учетные записи пользователя услуги – это системные учетные записи Windows, которые используются для запуска служб. Преимущество этой настройки состоит в том, что политики безопасности домена не влияют на права пользователей этих учетных записей. По умолчанию агент запускается в учетной записи **Локальная система**.
     - **Создать учетную запись**

       Имя учетной записи будет использоваться в качестве Agent User для агента.

© ООО Киберпротект, 2026

- **Использовать следующую учетную запись**

  При установке агента на контроллер домена система предложит указать существующие учетные записи (или ту же учетную запись) для агента. Из соображений безопасности система не может автоматически создавать учетные записи на контроллере домена.

Внимание
При установке агента на контроллер домена необходимо выбрать вариант **Использовать следующую учетную запись**, иначе установка завершится ошибкой.

При выборе параметра **Создать учетную запись** или **Использовать следующую учетную запись** убедитесь, что политики безопасности домена не повлияют на права соответствующих учетных записей. Если права пользователя не были заданы для учетной записи при установке, данный компонент может работать неправильно или вообще не работать.

- **Зарегистрировать машины с установленными агентами**. Этот параметр используется, если агент уже установлен на машинах и необходимо только зарегистрировать их в Кибер Бэкап. Если на машинах не найдено агента, они добавляются как машины со статусом **Неуправляемое**.
- **Добавить как неуправляемые машины**. Агент не устанавливается на машинах. Вы сможете просмотреть их на веб-консоли и установить или зарегистрировать агент позже.

[Если выбрано действие после обнаружения **Установить агенты и зарегистрировать машины**] **При необходимости перезагрузите машину**: если выбран этот параметр, машина перезапускается столько раз, сколько необходимо для завершения установки.

Перезапуск машины может потребоваться в одном из следующих случаев:

- Все предварительно требуемые компоненты установлены. Необходимо перезапустить машину для продолжения установки.
- Установка завершена, но необходимо перезапустить машину, поскольку некоторые файлы были заблокированы при установке.
- Установка завершена, но необходимо перезапустить машину, поскольку на ней есть другие ранее установленные программы.

[Если выбран параметр **При необходимости перезагрузите машину**] **Не перезапускать, если пользователь в системе**: если этот параметр включен, машина не будет автоматически перезапускаться, когда в системе есть активный пользователь. То есть, если для установки потребуется перезапуск, когда пользователь работает, система не перезапускается.

Если необходимые компоненты были установлены, но перезапуск не выполнялся по причине активного пользователя в системе, то для завершения установки агента необходимо перезапустить машину и запустить установку снова.

Если агент был установлен, а перезапуск не выполнялся, необходимо перезагрузить машину.

[Если в вашей организации есть отделы] **Отдел для регистрации машины**: выберите отдел, в котором будут зарегистрированы машины.

© ООО Киберпротект, 2026

Если выбрано одно из первых двух действий после обнаружения, то также есть возможность применить план защиты к машинам. При наличии нескольких планов защиты, необходимо выбрать конкретный план для использования.

10. Укажите учетные данные пользователя с правами администратора для всех машин.

Внимание
Обратите внимание, что удаленная установка агента работает без каких-либо подготовительных действий только в том случае, когда указаны учетные данные встроенной учетной записи администратора (это первая учетная запись, созданная при установке системы). Если вы намерены создать настраиваемую учетную запись администратора, необходимо вручную выполнить дополнительные подготовительные операции, как описано в разделе Добавление машины с ОС Windows > "Подготовка".

11. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.
    По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
12. Система проверяет подключение ко всем машинам. Если не удастся установить подключение к некоторым машинам, можно изменить учетные данные для них.

При запуске процесса обнаружения машин соответствующее задание появится в действии **Обнаружение машин** (**Панель мониторинга** > **Действия**).

2.7.4.1 Выбор компонентов для установки

В таблице ниже приводится описание обязательных и дополнительных компонентов:

Компонент	Описание
Обязательный компонент	
Агент для Windows	Этот агент создает резервную копию дисков, томов и файлов. Он устанавливается на машинах Windows. Он устанавливается в любом случае (не подлежит выбору).
Дополнительные компоненты	
Агент для Hyper-V	Этот агент создает резервную копию виртуальных машин Hyper-V. Он устанавливается на хостах Hyper-V. Если этот компонент выбран, и на машине обнаружена роль Hyper-V, он будет установлен.
Агент для SQL	Этот агент создает резервную копию баз данных SQL Server. Он устанавливается на машинах с Microsoft SQL Server. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.

© ООО Киберпротект, 2026

Агент для Exchange	Этот агент создает резервную копию баз данных и почтовых ящиков Exchange. Он устанавливается на машинах с ролью почтового ящика Microsoft Exchange Server. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для Active Directory	Этот агент создает резервную копию данных доменных служб Active Directory. Он устанавливается на контроллерах домена. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для VMware (Windows)	Этот агент создает резервную копию виртуальных машин VMware. Он устанавливается на виртуальных машинах Windows с сетевым доступом к vCenter Server. Если этот компонент выбран, он будет установлен.
Агент для Oracle	Этот агент создает резервную копию баз данных Oracle. Он устанавливается на машинах с Oracle Database. Если этот компонент выбран, он будет установлен.
Мониторинг Защиты Данных	Этот компонент позволяет пользователю отслеживать выполнение запущенных заданий в области уведомлений, приостанавливать запуск планов защиты, устанавливать особые пароли для резервных копий машины. Он устанавливается на машинах с Oracle Database. Если этот компонент выбран, он будет установлен.
Инструмент командной строки	Кибер Бэкап поддерживает интерфейс командной строки с утилитой acrocmd. acrocmd не содержит никаких инструментов, которые физически выполняют команды. Она просто обеспечивает интерфейс командной строки для компонентов Кибер Бэкап – агентов и сервера управления. Если этот компонент выбран, он будет установлен.
Мастер создания загрузочных носителей	Этот компонент позволяет пользователям создать загрузочный носитель. Он устанавливается на машинах Windows (если выбрано).

2.7.5 Управление обнаруженными машинами

По окончании процесса обнаружения все обнаруженные машины отображаются в разделе **Устройства** > **Необслуживаемые машины**.

Этот раздел разбит на подразделы согласно используемым методам обнаружения. Полный список параметров машины показан ниже (зависит от метода обнаружения).

Имя	Описание
Имя	Имя машины. Если не удастся обнаружить имя машины, будет отображаться ее IP-адрес.

© ООО Киберпротект, 2026

IP-адрес	IP-адрес машины.
Тип обнаружения	Метод обнаружения, использованный для выявления машины.
Организационная единица	Организационная единица в Active Directory, которой принадлежит машина. Этот столбец отображается при просмотре списка машин в разделе **Необслуживаемые машины** > **Active Directory**.
Операционная система	Операционная система, которая установлена на машине.

В разделе **Исключения** можно добавить машины, которые должны быть пропущены в процессе обнаружения. Например, если нет необходимости обнаруживать определенные машины, добавьте их в этот список.

Чтобы добавить машину в раздел **Исключения**, выберите ее в списке и щелкните **Добавить в исключения**. Чтобы удалить машину из раздела **Исключения**, выберите пункты **Необслуживаемые машины** > **Исключения**, выберите машину и щелкните **Удалить из исключений**.

Для установки агента защиты и регистрации группы обнаруженных машин в Кибер Бэкап можно выбрать их в списке и щелкнуть **Установить и зарегистрировать**. В открытом мастере также можно назначить план защиты группе машин.

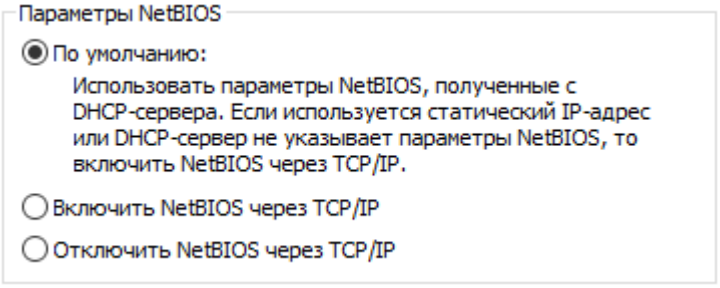
Те машины, на которых установлен агент защиты, отображаются в разделе **Устройства** > **Машины с агентами**.

Чтобы проверить статус защиты, откройте раздел **Панель мониторинга** > **Обзор** и добавьте виджет Статус защиты или виджет Обнаруженная машина.

2.7.6 Устранение неисправностей при автоматическом обнаружении

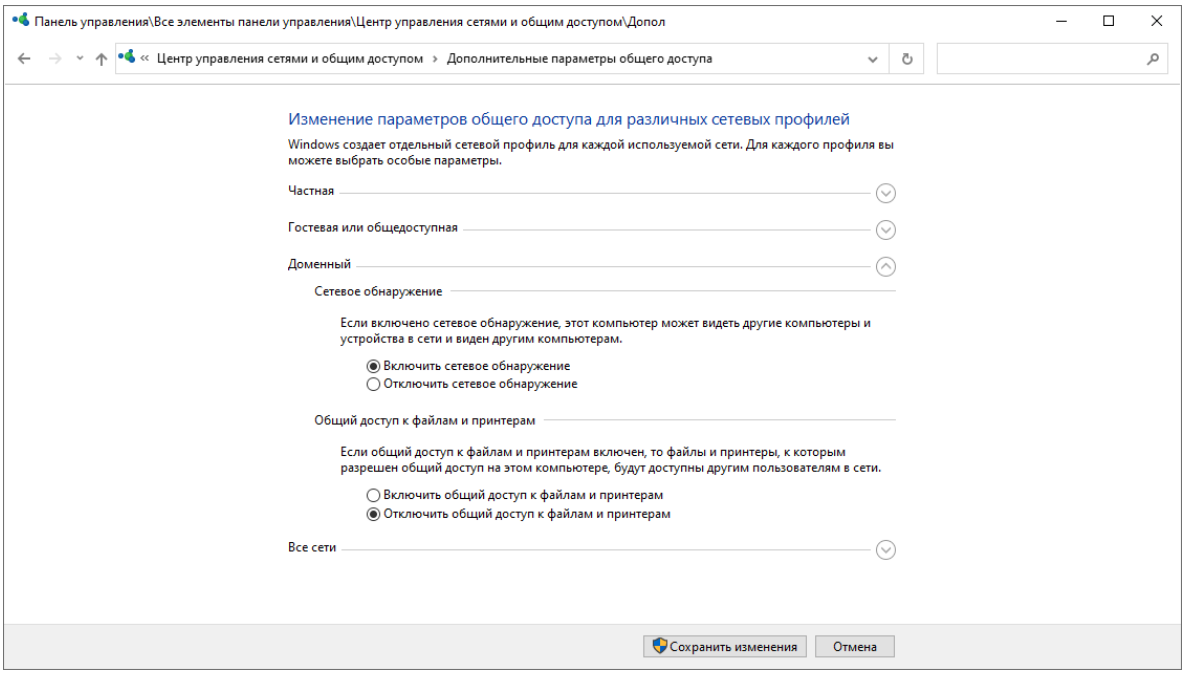
Если есть какие-либо проблемы с функциональностью автоматического обнаружения, выполните указанные ниже действия.

- Проверьте, что протокол "NetBIOS через TCP/IP" включен или задан по умолчанию.



- Выберите **Панель управления** > **Центр управления сетями и общим доступом** > **Дополнительные параметры общего доступа** и включите обнаружение сети.

© ООО Киберпротект, 2026



- Проверьте, что служба **Хост поставщика функции обнаружения** запущена на машине, которая выполняет обнаружение, и на машинах, которые должны быть доступны для обнаружения.
- Проверьте, что служба **Публикация ресурсов обнаружения функции** запущена на машинах, которые должны быть доступны для обнаружения.

2.8 Обновление виртуальных устройств

В разделе описан порядок обновления агентов для платформ виртуализации.

Рекомендуется выполнять обновление агентов вне расписания резервного копирования. Все операции, выполняемые агентом во время его обновления, завершатся сбоем.

2.8.1 Порядок обновления виртуального устройства

1. Обновите сервер управления. Подробнее об этом см. раздел "Обновление Кибер Бэкап" (стр. 205).
2. Скачайте пакет обновления агента.
3. Сохраните файлы tar.bz2 в указанный ниже каталог на машине сервера управления:
   - Windows: C:\Program Files\Acronis\VirtualAppliances\va-updates
   - Linux: /usr/lib/Acronis/VirtualAppliances/va-updates
4. Для отображения списка виртуальных устройств в веб-консоли Кибер Бэкап выберите **Настройки** > **Агенты**.

   Для устаревших виртуальных устройств рядом с версией агента будет отображён оранжевый треугольник с восклицательным знаком.
5. Выберите виртуальные устройства, которые необходимо обновить. Эти виртуальные устройства должны быть включены.

© ООО Киберпротект, 2026

6. Нажмите **Обновление агента**.
   Ход выполнения обновления показан на вкладке **Панель мониторинга** > **Действия**.
7. После завершения обновления откройте вкладку **Сведения** виртуального устройства.
   Проверьте версию устройства и статус подключения к платформе виртуализации.

Примечание
Агент для VMware (виртуальное устройство) версии более ранней, чем 15.24426 (выпущена в сентябре 2020 года), обновляется как агент, установленный на машине (см. раздел "Обновление агентов" (стр. 203)).

2.9 Обновление агентов

Рекомендуется выполнять обновление агентов вне расписания резервного копирования. Все операции, выполняемые агентом во время его обновления, завершатся сбоем.

Агент, установленный на машине с ОС Linux, можно обновить, запустив новую версию его установочного файла.

Агент, установленный на машине с ОС Windows, можно обновить, запустив новую версию его установочного файла или из веб-консоли Кибер Бэкап.

Для работы функций Кибер Бэкап на машинах с ОС Windows требуется распространяемый компонент Microsoft Visual C++ 2022 версии не ниже 14.42.34438. Проверьте наличие этого компонента на машине или установите его перед обновлением агента. После установки может потребоваться перезагрузка. Распространяемый пакет Microsoft Visual C++ можно скачать по ссылке https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Примечание
Обновление агентов для виртуализации описано в разделе "Обновление виртуальных устройств" (стр. 202).

Проверка версии агента

1. В веб-консоли Кибер Бэкап перейдите в раздел **Настройки** > **Агенты**.
2. Посмотрите данные в столбце **Версия агента**.

2.9.1 Порядок обновления агентов локально через установочный файл

1. Обновите сервер управления. Подробнее об этом см. раздел "Обновление Кибер Бэкап" (стр. 205).
2. Скачайте установщик новой версии агента.
3. Запустите установщик на машине с агентом устаревшей версии.
4. Примите лицензионное соглашение и нажмите **Обновить**.

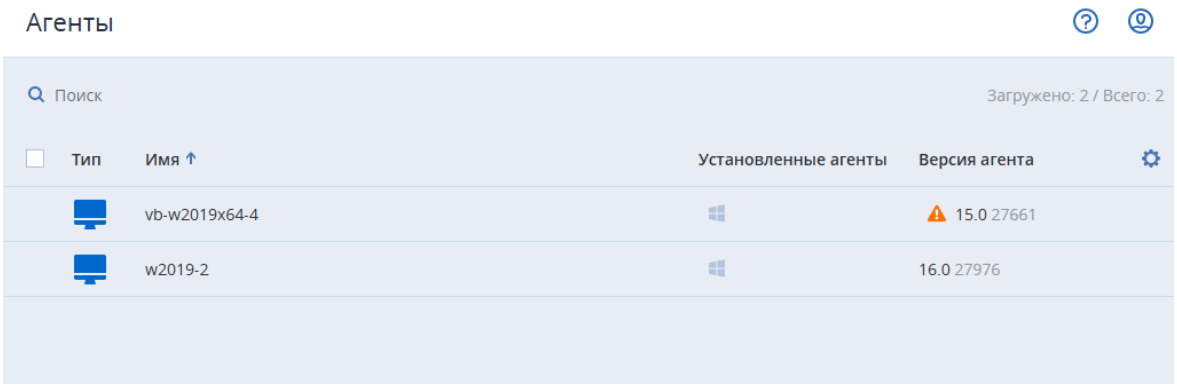
© ООО Киберпротект, 2026

5. Для агентов на машинах с ОС Linux далее см. раздел "Установка агентов в ОС Linux вручную" (стр. 97).
6. Для агентов на машинах с ОС Windows далее см. раздел "Установка агентов в ОС Windows вручную" (стр. 95).

2.9.2 Порядок обновления агентов из веб-консоли Кибер Бэкап

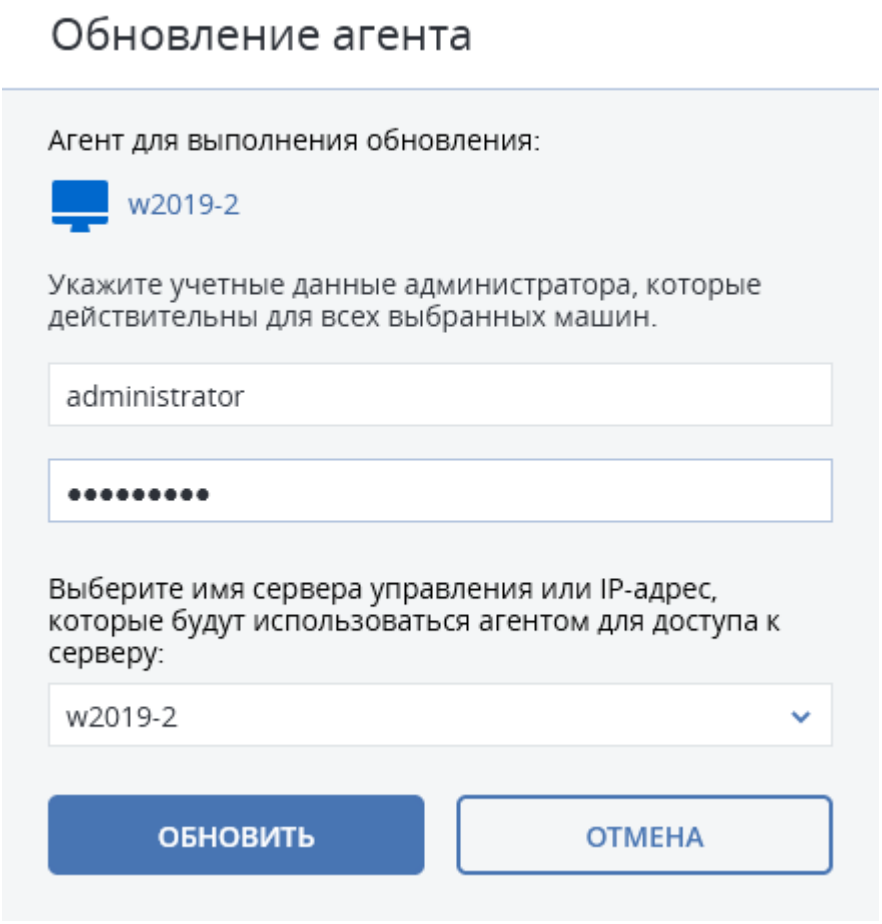
1. Обновите сервер управления и узел хранения (подробнее см. раздел "Обновление Кибер Бэкап" (стр. 205)).
2. Убедитесь, что на машине с сервером управления есть пакеты установки (подробнее см. раздел "Добавление машины с ОС Windows" (стр. 87)).
3. В веб-консоли Кибер Бэкап последовательно выберите пункты **Настройки** > **Агенты**.

   В программе будет выведен список машин. Машины с агентами устаревших версий будут помечены оранжевым восклицательным знаком.



4. Выберите машины, на которых нужно обновить агенты. Машины должны быть включены.
5. Щелкните **Обновление агента**.

© ООО Киберпротект, 2026



6. Выберите агент развертывания.
7. Укажите данные учетной записи с правами администратора на целевой машине.

   Внимание
   Пароль учетной записи не должен быть пустым.

8. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
9. Ход выполнения обновления отображается на вкладке **Действия**.

2.10 Обновление Кибер Бэкап

Обновление Кибер Бэкап до последней версии можно выполнить с предварительным удалением предыдущей версии продукта или без удаления.

Обновление без удаления текущей версии продукта доступно начиная с Кибер Бэкап 15 обновление 2.6 (сборка 27146 и более поздней версии). Продукты более ранних версий невозможно обновить напрямую.

© ООО Киберпротект, 2026

Внимание
Перед обновлением настоятельно рекомендуем создать резервную копию системы. Это позволит выполнить возврат к оригинальной конфигурации в случае сбоя обновления.

Порядок обновления с версии Кибер Бэкап 15 обновление 2.5 или более ранней

Обновление на машине с версией Кибер Бэкап 15 обновление 2.5 или более ранней выполняется в два этапа:

1. Обновление Кибер Бэкап до версии 15 обновление 2.6 или более поздней (до 17.1 включительно).
2. Обновление Кибер Бэкап до версии 17.2 и выше.

Все обновления выполняйте, используя порядок обновления с предыдущей версии Кибер Бэкап.

Порядок обновления с предыдущей версии Кибер Бэкап

1. Обновление сервера управления и узла хранения.
2. Обновление агентов Кибер Бэкап.

Обновление сервера управления и узла хранения выполняется посредством установщика Кибер Бэкап новой версии.

Обновление агента Кибер Бэкап можно выполнить с помощью установщика новой версии Кибер Бэкап (см. следующий пункт "Обновление с предыдущей версии Кибер Бэкап") или через веб-консоль (см. раздел "Обновление агентов" (стр. 203)).

Внимание
Обновляйте агенты Кибер Бэкап только после того, как обновили сервер управления и узел хранения.

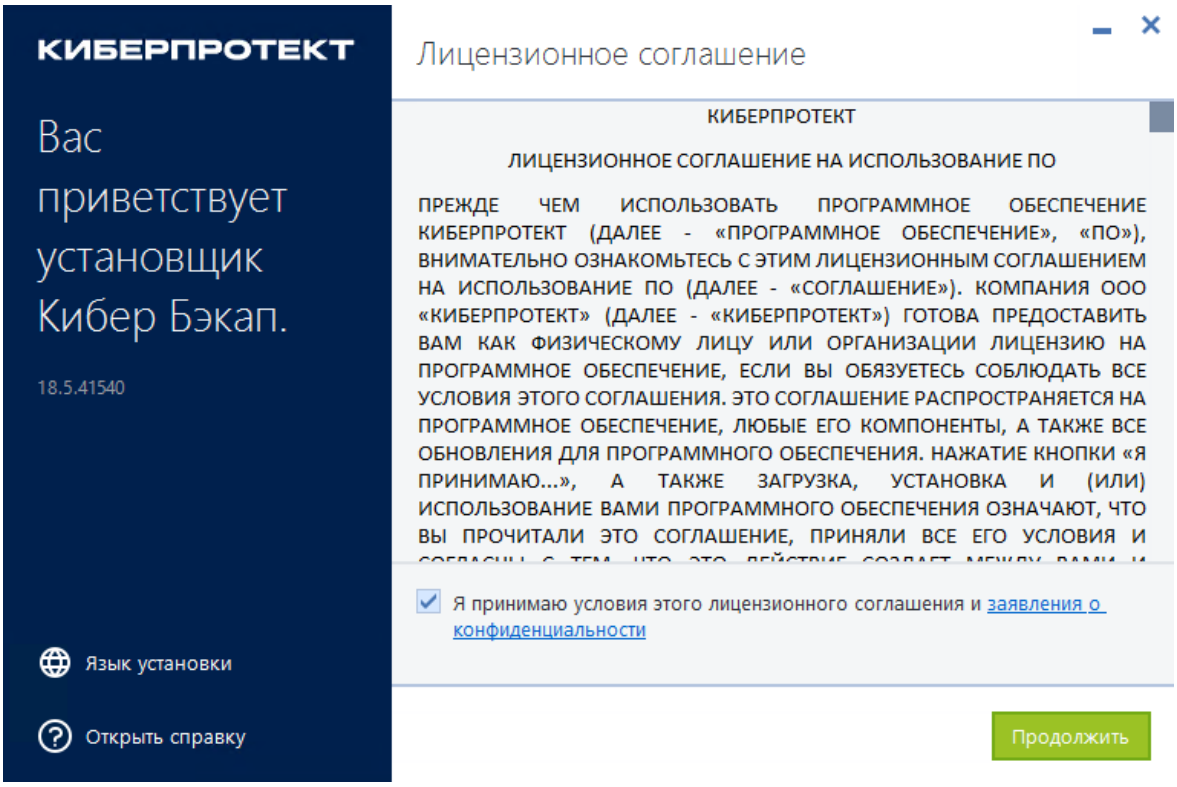
Сервер управления новой версии поддерживает агенты только одного предшествующего крупного релиза. При этом возможности новой версии недоступны для таких агентов.

Обновление агентов не влияет на существующие резервные копии и их настройки.

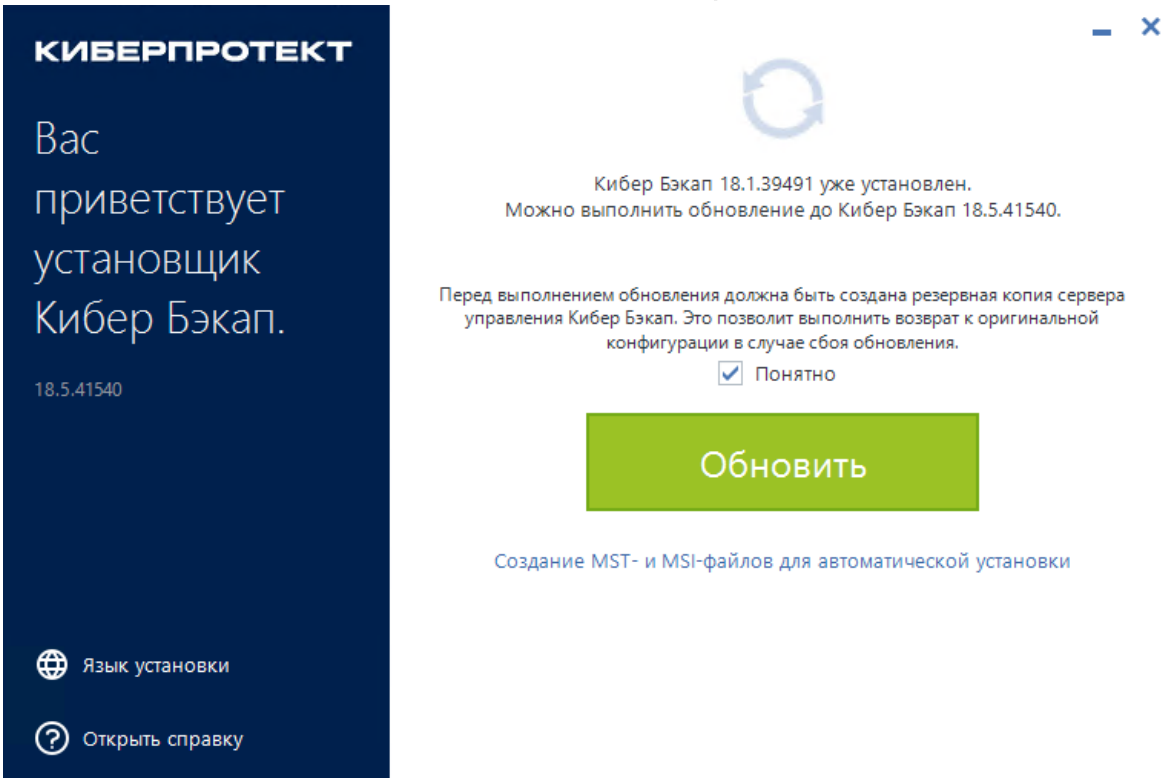
Обновление с предыдущей версии Кибер Бэкап

1. Запустите установщик на машине с сервером управления или узлом хранения. При необходимости можно изменить язык отображения сообщений во время обновления, нажав **Язык установки**.

© ООО Киберпротект, 2026



2. Примите условия лицензионного соглашения и нажмите **Продолжить**.



3. Для продолжения подтвердите, что прочитали рекомендацию о создании резервной копии сервера управления. После этого нажмите **Обновить**.

Установленная на вашем компьютере версия Кибер Бэкап будет обновлена.

© ООО Киберпротект, 2026

2.11 Удаление продукта

Чтобы удалить с машины отдельные компоненты продукта, запустите программу установки, перейдите к изменению продукта и отмените выбор компонентов, которые больше не нужны. Ссылки на программы установки доступны на странице **Загрузки** (щелкните значок учетной записи в правом верхнем углу и выберите пункт **Загрузки**).

Если нужно удалить все компоненты продукта с машины, следуйте приведенным ниже инструкциям.

Предупреждение
Выбирайте компоненты для удаления с осторожностью.

Если удалить сервер управления по ошибке, веб-консоль Кибер Бэкап станет недоступной и вы больше не сможете выполнять резервное копирование и восстановление машин, зарегистрированных на удаленном сервере управления.

2.11.1 В Windows

1. Войдите как администратор.
2. Откройте **Панель управления** и выберите **Программы и компоненты** > **Кибер Бэкап** > **Удалить**.
3. [Необязательно] Установите флажок **Удалить журналы и параметры конфигурации**.
   Не устанавливайте этот флажок, если удаляете агент и планируете установить его снова. Если установить флажок, машина может быть дуплицирована на веб-консоли Кибер Бэкап. При этом резервные копии старой машины могут быть не связаны с новой машиной.
4. Подтвердите операцию.

2.11.2 В ОС Linux

1. В качестве привилегированного пользователя выполните **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Необязательно] Установите флажок **Очистить все следы продукта (удалить журналы продукта и параметры конфигурации)**.
   Не устанавливайте этот флажок, если удаляете агент и планируете установить его снова. Если установить флажок, машина может быть дуплицирована на веб-консоли Кибер Бэкап. При этом резервные копии старой машины могут быть не связаны с новой машиной.
3. Подтвердите операцию.

© ООО Киберпротект, 2026

2.11.3 Удаление агента для VMware (виртуальное устройство)

1. Запустите клиент vSphere и выполните вход на сервер vCenter Server.
2. Если виртуальное устройство включено, щелкните его правой кнопкой мыши, а затем щелкните **Питание** > **Выключить питание**. Подтвердите операцию.
3. Если виртуальное устройство использует локально присоединенное хранилище на виртуальном диске и нужно сохранить данные на диске, выполните указанные ниже действия.
   a. Щелкните виртуальное устройство правой кнопкой мыши и выберите пункт **Изменить настройки**.
   b. Выберите диск с хранилищем и щелкните **Удалить**. В разделе **Параметры удаления** нажмите кнопку **Удалить из виртуальной машины**.
   c. Нажмите кнопку **OK**.

   В результате диск остается в хранилище данных. Можно подключить диск к другому виртуальному устройству.
4. Щелкните виртуальное устройство правой кнопкой мыши и выберите пункт **Удалить с диска**. Подтвердите операцию.

2.11.4 Удаление машин из веб-консоли Кибер Бэкап

После удаления агента его регистрация на сервере управления будет отменена. Кроме того, из веб-консоли Кибер Бэкап будет автоматически удалена запись о машине, на которой был установлен агент.

Если при выполнении этой операции подключение к серверу управления будет утрачено (например, из-за проблемы в сети), агент может удалиться, но его машина при этом может продолжать отображаться на веб-консоли. В этом случае необходимо удалить машину из веб-консоли службы вручную.

Порядок удаления машины из веб-консоли вручную

1. На веб-консоли Кибер Бэкап последовательно выберите пункты **Настройки** > **Агенты**.
2. Выберите машину, на которой установлен агент.
3. Щелкните **Удалить**.

© ООО Киберпротект, 2026

3 Веб-консоль Кибер Бэкап

Веб-консоль является основным инструментом управления продуктом Кибер Бэкап.

Для доступа к веб-консоли Кибер Бэкап введите адрес страницы входа в адресной строке веб-браузера, а затем выполните вход, как описано ниже.

Адрес страницы входа – это IP-адрес или имя машины, на которой установлен сервер управления:

- localhost:9877 – С сервера управления можно автоматически войти в систему от имени текущего пользователя.
- ams_IP:9877 – При входе по IP-адресу сервера управления всегда нужно указывать имя пользователя и пароль.
- ams_hostname:9877 – При входе по имени хоста сервера управления всегда нужно указывать имя пользователя и пароль.

На одном TCP-порту поддерживаются оба протокола (HTTP и HTTPS). Внести изменения в эту настройку можно при установке сервера управления. По умолчанию используется порт 9877.

Сервер управления можно настроить таким образом, чтобы запретить доступ к веб-консоли Кибер Бэкап по HTTP и использовать сторонний сертификат SSL.

3.1 В Windows

Если сервер управления установлен в ОС Windows, существует два способа войти на веб-консоль Кибер Бэкап.

- Щелкните **Войти**, чтобы войти как текущий пользователь Windows.

  Это самый простой способ входа с машины, на которой установлен сервер управления.

  Если сервер управления установлен на другой машине, этот способ работает при условии, что:

  - Машина, с которой выполняется вход, находится в одном домене Active Directory с сервером управления.
  - Вы вошли как пользователь домена.

  Рекомендуется настроить веб-браузер для выполнения встроенной проверки подлинности Windows. В противном случае веб-браузер запросит имя пользователя и пароль. Однако этот параметр можно отключить.
- Щелкните **Ввести имя пользователя и пароль**, а затем укажите имя пользователя и пароль.

В любом случае учетная запись должна находиться в списке администраторов сервера управления. По умолчанию этот список содержит группу **Администраторы** на машине, где работает сервер управления. Дополнительные сведения см. в разделе "Отделы и административные учетные записи" (стр. 806).

Порядок отключения параметра входа под учетной записью текущего пользователя Windows

1. На машине с установленным сервером управления перейдите в папку C:\Program Files\Acronis\AccountServer.

© ООО Киберпротект, 2026

2. Откройте файл **account_server.json** для редактирования.
3. Перейдите к разделу "connectors" и удалите следующие строки:

```
{
"type": "sspi",
"name": "1 Windows Integrated Logon",
"id": "sspi",
"config": {}
},
```

4. Перезапустите службу Киберпротект Service Manager, как описано в разделе Использование сертификата, выданного доверенным центром сертификации.

3.2 В ОС Linux

Если на сервере управления установлена ОС Linux, укажите имя пользователя и пароль учетной записи, которая включена в список администраторов сервера управления. По умолчанию в этот список входит только пользователь **root** на машине с запущенным сервером управления. Также в список администраторов можно добавить учетные записи других пользователей, в том числе из домена Active Directory. Дополнительные сведения см. в разделе "Отделы и административные учетные записи" (стр. 806).

3.3 Смена языка

После входа в систему можно изменить язык веб-интерфейса, щелкнув значок учетной записи в правом верхнем углу.

3.4 Настройка веб-браузера для выполнения встроенной проверки подлинности Windows

Выполнение встроенной проверки подлинности Windows возможно при наличии доступа к веб-консоли Кибер Бэкап с машины с запущенной Windows и любого поддерживаемого браузера.

Рекомендуется настроить веб-браузер для выполнения встроенной проверки подлинности Windows. В противном случае веб-браузер запросит имя пользователя и пароль.

3.4.1 Настройка Microsoft Edge, Opera и Google Chrome

Если машина, на которой запущен браузер, находится в одном домене Active Directory с машиной, на которой работает сервер управления, добавьте страницу входа консоли к списку веб-узлов **локальной интрасети**.

В противном случае, добавьте страницу входа консоли к списку **надежных веб-узлов** и включите параметр **Автоматический вход в систему с текущим пользователем и паролем**.

© ООО Киберпротект, 2026

См. пошаговые инструкции далее в этом разделе. Поскольку эти браузеры используют параметры Windows, возможна их настройка с помощью групповой политики в домене Active Directory.

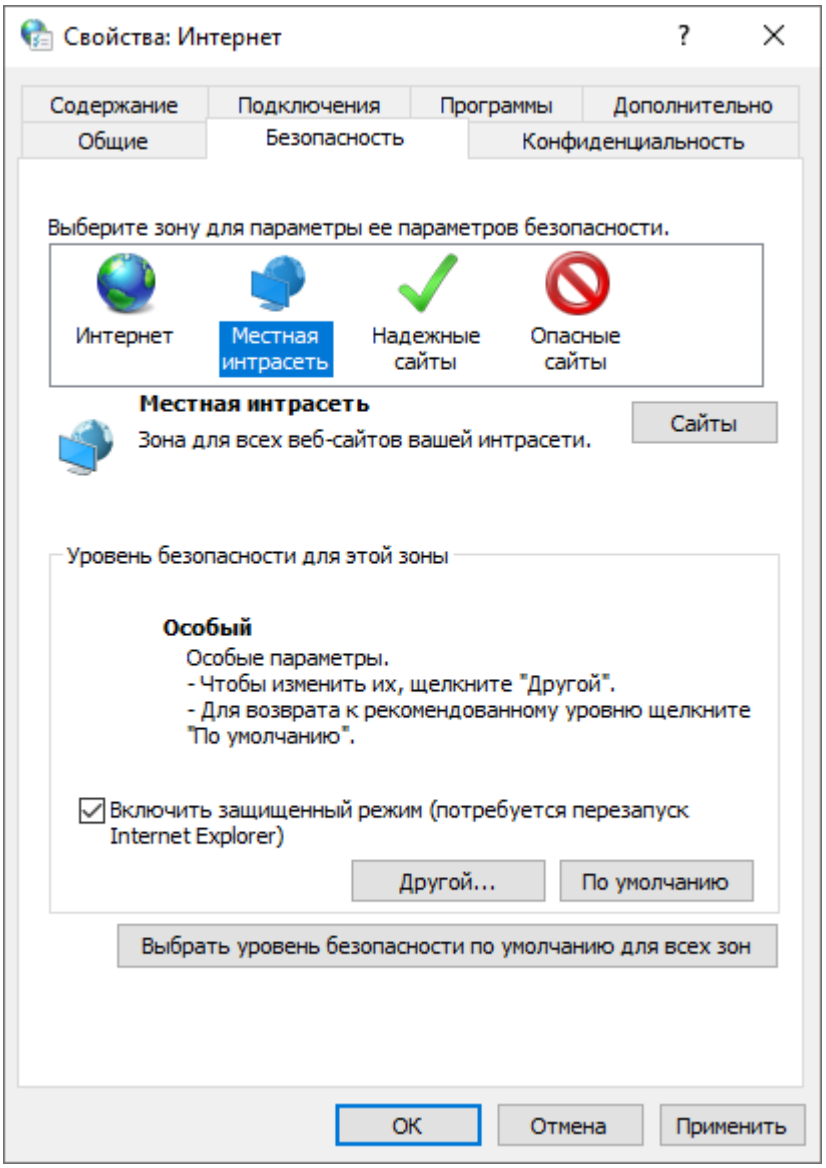
3.4.2 Настройка Mozilla Firefox

1. В Firefox перейдите на URL-адрес about:config, а затем нажмите кнопку **Я принимаю возможные риски**.
2. В поле Поиск выполните поиск настройки **network.negotiate-auth.trusted-uris**.
3. Дважды щелкните настройку, а затем введите адрес страницы входа в веб-консоль Кибер Бэкап в одном из форматов, указанных в разделе "Веб-консоль Кибер Бэкап" (стр. 210). Например, https://localhost:9877 или http://localhost:9877.
4. Повторите шаги 2-3 для настройки network.automatic-ntlm-auth.trusted-uris.
5. Закройте окно about:config.

3.4.3 Добавление консоли к списку веб-узлов локальной интрасети

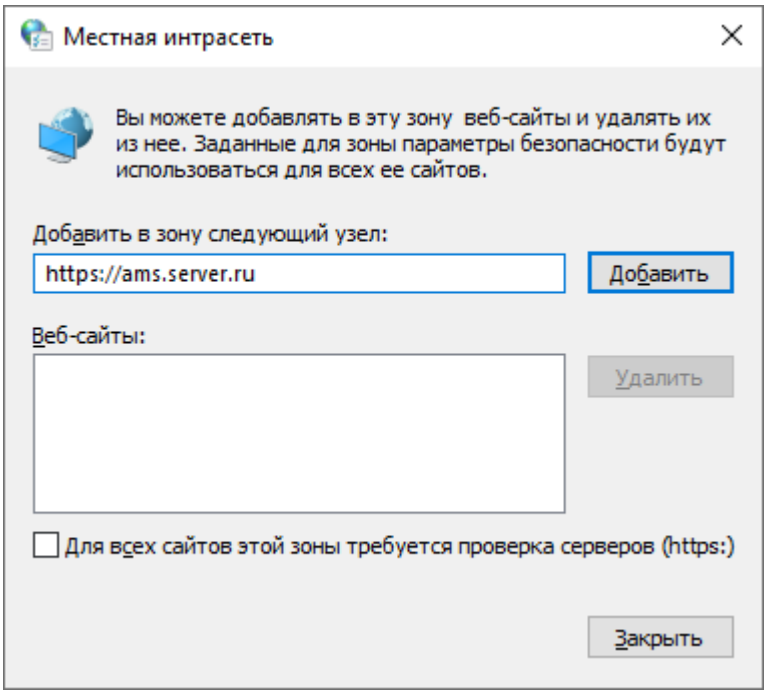
1. Выберите **Панель управления** > **Свойства браузера**.
2. Во вкладке **Безопасность** выберите **Местная интрасеть**.

© ООО Киберпротект, 2026



3. Нажмите кнопку **Сайты** и далее **Дополнительно**.
4. В поле **Добавить в зону следующий узел** введите адрес страницы входа на веб-консоль Кибер Бэкап, а затем щелкните **Добавить**.

© ООО Киберпротект, 2026

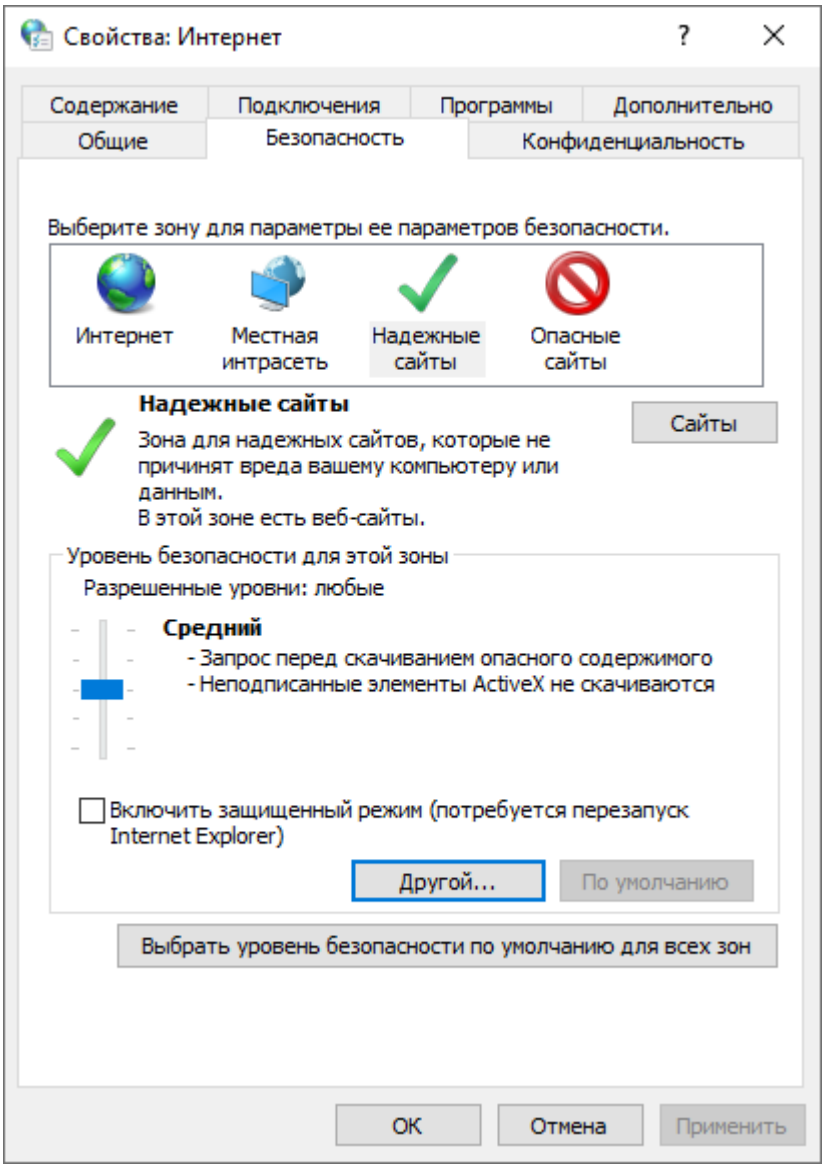


5. Нажмите кнопку **Закрыть**.
6. Нажмите кнопку **OK** и далее **Применить**.

3.4.4 Добавление консоли к списку доверенных веб-узлов

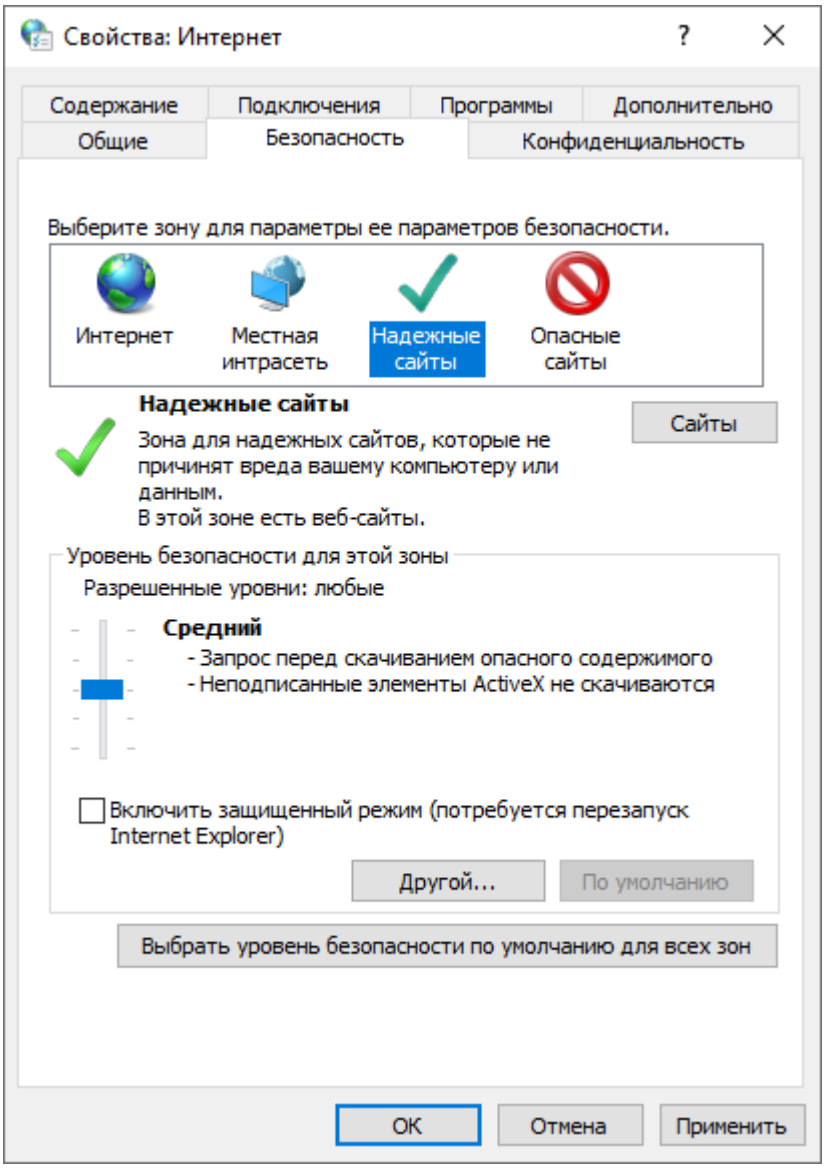
1. Выберите **Панель управления** > **Свойства браузера**.
2. Во вкладке **Безопасность** выберите **Надежные сайты**, а затем нажмите **Другой**.

© ООО Киберпротект, 2026



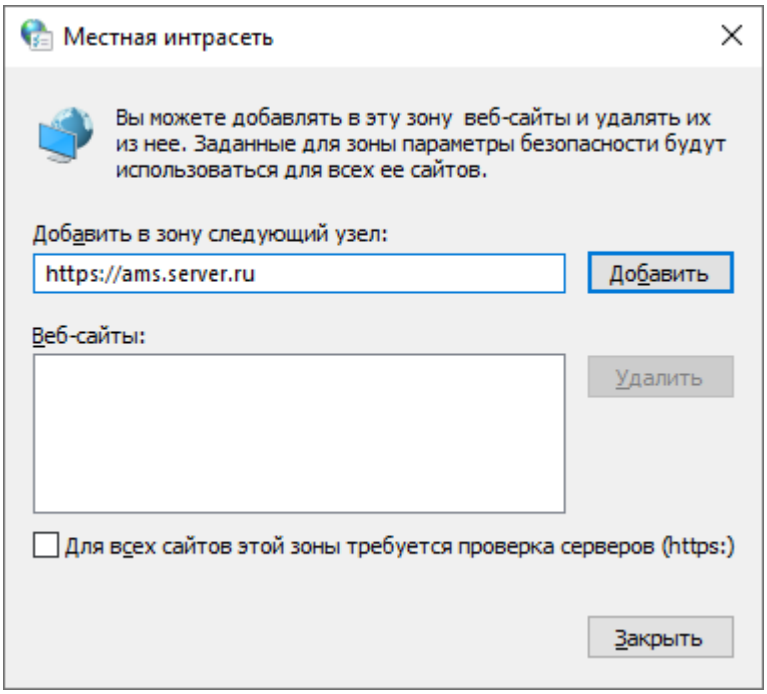
3. В группе **Проверка подлинности пользователя** выберите **Автоматический вход в сеть с текущим именем пользователя и паролем**, а затем нажмите кнопку **OK** и далее **Применить**.

© ООО Киберпротект, 2026



4. Во вкладке **Безопасность** при выбранной зоне **Надежные сайты** нажмите **Сайты**.
5. В поле **Добавить в зону следующий узел** введите адрес страницы входа на веб-консоль Кибер Бэкап, а затем щелкните **Добавить**.

© ООО Киберпротект, 2026



6. Нажмите кнопку **Закрыть**.
7. Нажмите кнопку **Применить**.

3.5 Настройки сертификата SSL

В этом разделе затронуты следующие темы:

- Настройка агента защиты, который использует самозаверяющий сертификат SSL, сгенерированный сервером управления.
- Замена самозаверяющего сертификата SSL, созданного сервером управления, на сертификат, выписанный доверенным центром сертификации (например, GlobalSign). В этом случае сертификат, используемый сервером управления, будет доверенным на любой машине. Оповещение безопасности браузера не будет появляться при входе в веб-консоль Кибер Бэкап по HTTPS.

При необходимости можно настроить сервер управления таким образом, чтобы запретить доступ к веб-консоли Кибер Бэкап по HTTP и перенаправлять всех пользователей через HTTPS.

3.5.1 Использование самозаверяющих сертификатов

Порядок настройки агента защиты в Windows

1. На машине с агентом откройте редактор реестра.
2. Найдите следующий раздел реестра: **HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions.**
3. Задайте параметру **VerifyPeer** значение **0**.
4. Убедитесь, что параметру **VerifyHost** задано значение **0**.

© ООО Киберпротект, 2026

5. Перезапустите Managed Machine Service (MMS):
   a. В меню **Пуск** щелкните **Запустить**, а затем введите **cmd**
   b. Нажмите кнопку **OK**.
   c. Выполните следующие команды:

```
net stop mms
net start mms
```

Порядок настройки агента защиты в Linux

1. На машине с агентом откройте файл **/etc/Acronis/BackupAndRecovery.config** для редактирования**.**
2. Перейдите к разделу **CurlOptions** и задайте параметру **VerifyPeer** значение **0**. Убедитесь, что параметру **VerifyHost** задано значение **0**.
3. Сохраните внесенные изменения.
4. Перезапустите Managed Machine Service (MMS), выполнив следующую команду в любом каталоге:

```
sudo service acronis_mms restart
```

Порядок настройки виртуального устройства

1. Подключитесь к консоли виртуального устройства.

   Примечание
   Чтобы запустить командную оболочку, нажмите клавиши CTRL+SHIFT+F2.

2. Откройте файл **/etc/Acronis/BackupAndRecovery.config** для редактирования.
3. Перейдите к разделу **CurlOptions** и задайте параметрам **VerifyHost** и **VerifyPeer** значение **0**, например:

```
<value name="VerifyHost" type="Tdword">"0"</value>
<value name="VerifyPeer" type="Tdword">"0"</value>
```

4. Сохраните внесенные изменения.
5. Перезапустите виртуальное устройство.

3.5.2 Использование сертификата, выданного доверенным центром сертификации

Порядок изменения настроек сертификата SSL

1. Убедитесь, что у вас есть:
   - Файл сертификата (в формате .pem)
   - Файл с закрытым ключом для сертификата (обычно в формате .key)

© ООО Киберпротект, 2026

- Парольная фраза закрытого ключа (если ключ зашифрован)

2. Скопируйте файлы на машину, на которой запущен сервер управления.
3. На этой машине откройте указанный ниже файл конфигурации с текстовым редактором:
   - В ОС Windows: **%ProgramData%\Acronis\ApiGateway\api_gateway.json**
   - В ОС Linux: **/var/lib/Acronis/ApiGateway/api_gateway.json**
4. Найдите следующий раздел:

```
"tls": {
   "cert_file": "cert.pem",
   "key_file": "key.pem",
   "passphrase": "",
   "auto_redirect": false
}
```

5. Между двойными кавычками в строке "cert_file" укажите полный путь к файлу сертификата. Пример:
   - В Windows (обратите внимание на символы косой черты): "cert_file": "C:/certificate/local-domain.ams.pem"
   - В ОС Linux: "cert_file": "/home/user/local-domain.ams.pem"
6. Между двойными кавычками в строке "key_file" укажите полный путь к файлу закрытого ключа. Пример:
   - В Windows (обратите внимание на символы косой черты): "key_file": "C:/certificate/private.key"
   - В ОС Linux: "key_file": "/home/user/private.key"
7. Если закрытый ключ зашифрован, укажите его парольную фразу между двойными кавычками в строке "passphrase". Пример: "passphrase": "my secret passphrase"
8. Чтобы запретить доступ к веб-консоли Кибер Бэкап по HTTP и перенаправлять всех пользователей через HTTPS, измените значение "auto_redirect" с false на true. В противном случае пропустите этот шаг.
9. Сохраните файл **api_gateway.json**.

Внимание
Будьте внимательны, чтобы не удалить в файле конфигурации ни одной запятой, скобки и двойной кавычки.

10. Перезапустите службу Киберпротект Service Manager, как описано ниже.

Порядок перезапуска службы Киберпротект Service Manager в Windows

1. В меню **Пуск** выберите команду **Выполнить** и введите: **cmd**
2. Нажмите кнопку **OK**.
3. Выполните следующие команды:

```
net stop asm
net start asm
```


© ООО Киберпротект, 2026

Порядок перезапуска службы Киберпротект Service Manager в Linux

1. Откройте **приложение терминала**.
2. Выполните следующую команду в любом каталоге:

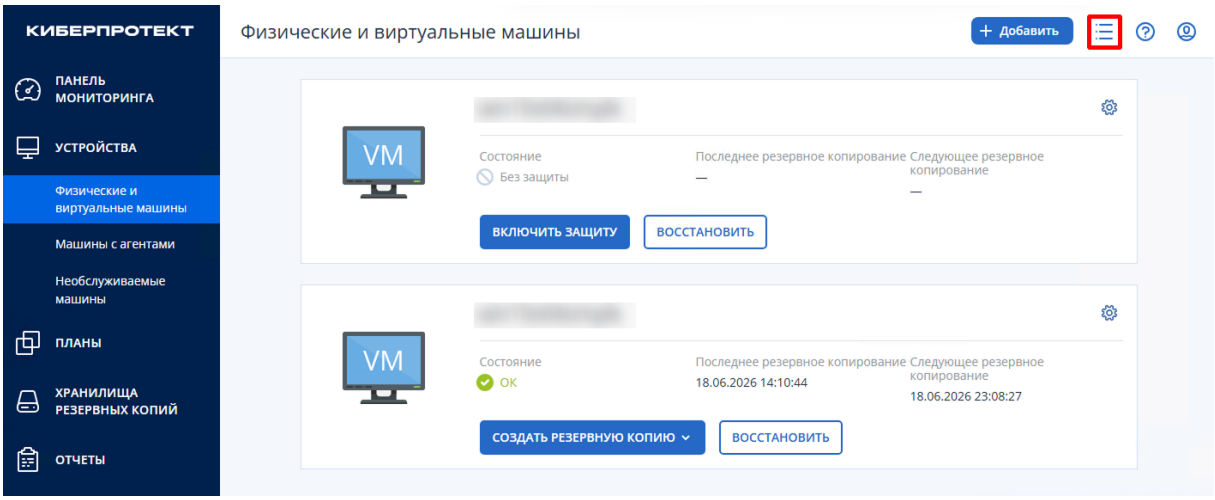
```
sudo service acronis_asm restart
```

3.6 Режимы отображения списка устройств

Список устройств в веб-консоли Кибер Бэкап можно отображать в **простом** и **табличном** режимах. Они различаются только типом представления данных. Набор доступных функций и операций при этом один и тот же.

3.6.1 Простой режим

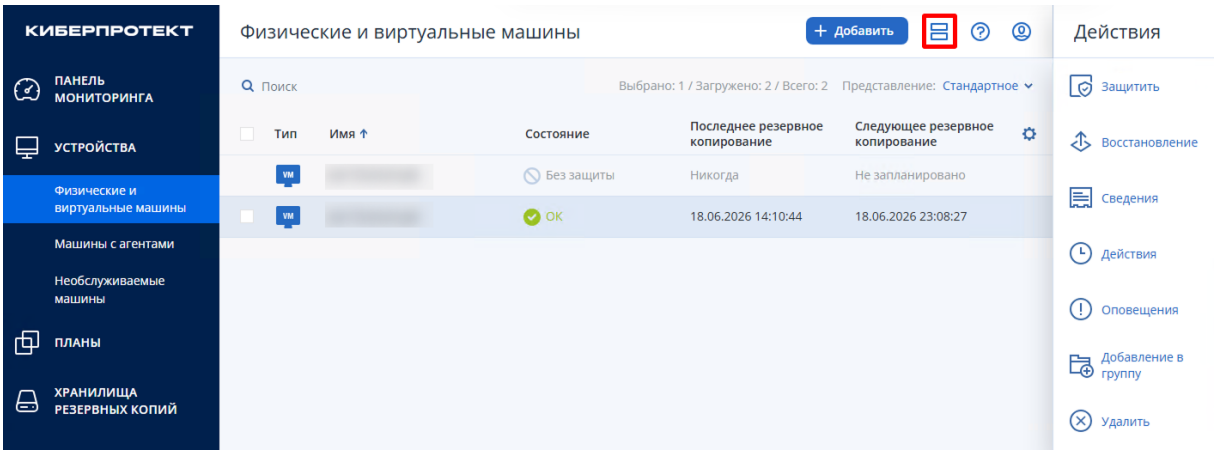
Пример отображения устройств в простом режиме приведён на рисунке ниже. Для переключения на табличный режим отображения щёлкните значок в правом верхнем углу веб-консоли.



3.6.2 Табличный режим

Пример отображения устройств в табличном режиме приведён на рисунке ниже. Для переключения на простой режим отображения щёлкните значок в правом верхнем углу веб-консоли.

© ООО Киберпротект, 2026



3.6.2.1 Настройка представлений в табличном режиме

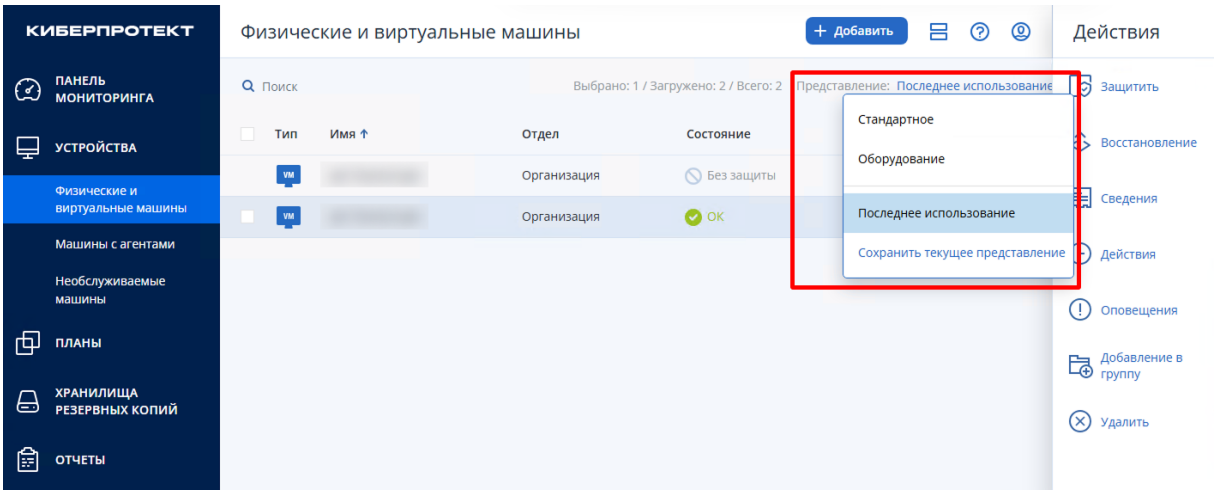
Кибер Бэкап в табличном режиме позволяет отображать только нужные столбцы с данными об устройствах. Доступны как предустановленные варианты представлений, так и возможность создания собственного (пользовательского) представления.

Чтобы выбрать представление, в верхней строке веб-консоли нажмите текущее название и в выпадающем списке выберите нужный вариант:

- **Стандартное** (значение по умолчанию). Отображаются столбцы: **Тип**, **Имя**, **Состояние**, **Последнее резервное копирование**, **Следующее резервное копирование**.
- **Оборудование**. Отображаются столбцы: **Тип**, **Имя**.
- **Последнее использование**. Отображаются столбцы, выбранные пользователем в предыдущий раз (кроме сохранённых наборов).

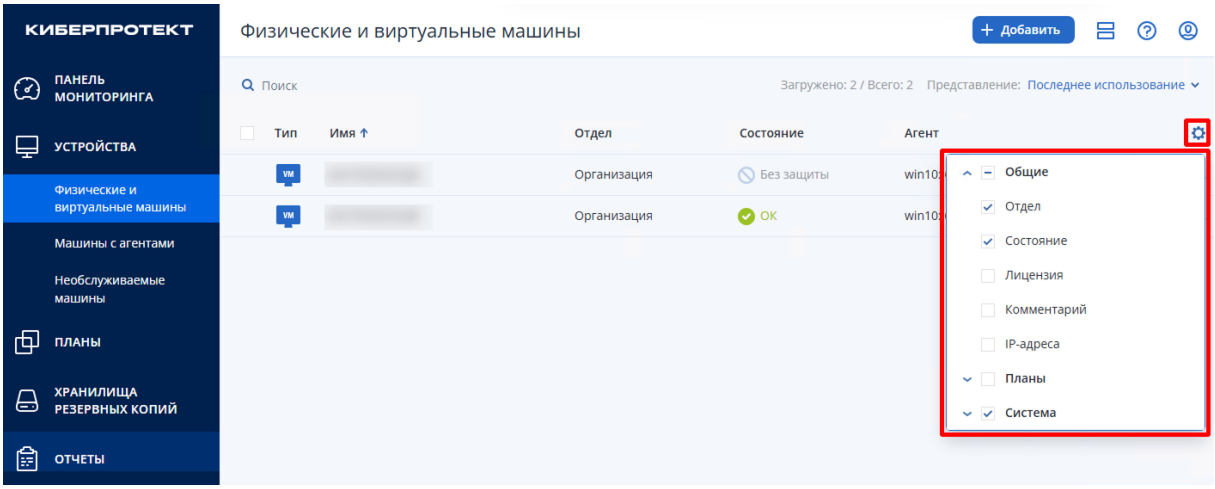
> **Примечание**
> Данный вариант отображается, если пользователь настроил, но не сохранил собственный набор столбцов.

- Пользовательское представление (отображается название пользовательского представления после его сохранения).



© ООО Киберпротект, 2026

Чтобы настроить пользовательский набор столбцов, щёлкните значок шестерёнки в правом верхнем углу веб-консоли и в выпадающем списке отметьте нужные столбцы или их группы.

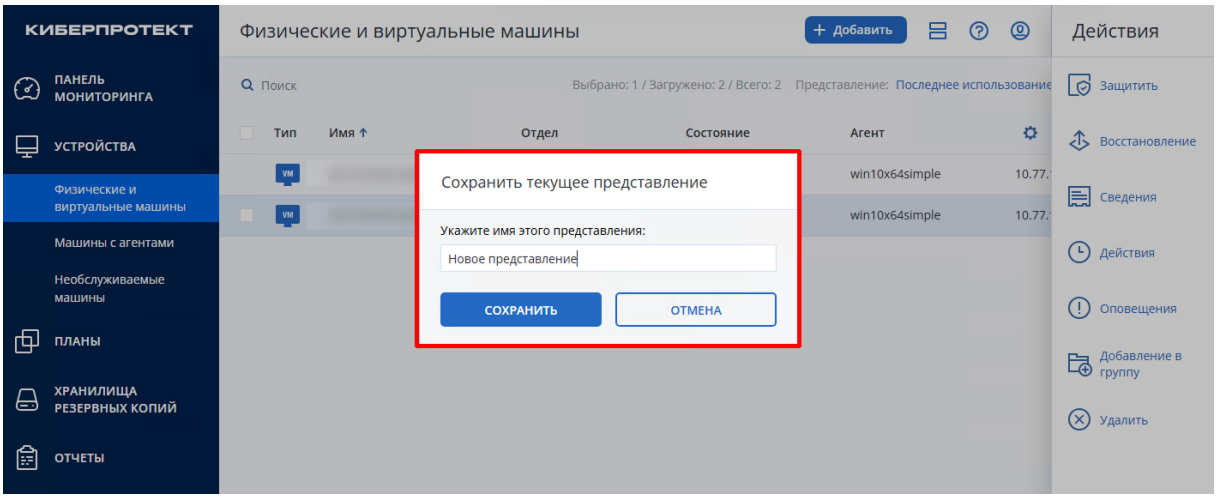


В результате выбранные столбцы будут отображены в таблице, а в верхней строке веб-консоли название представления поменяется на **Последнее использование**.

3.6.2.2 Сохранение пользовательских представлений

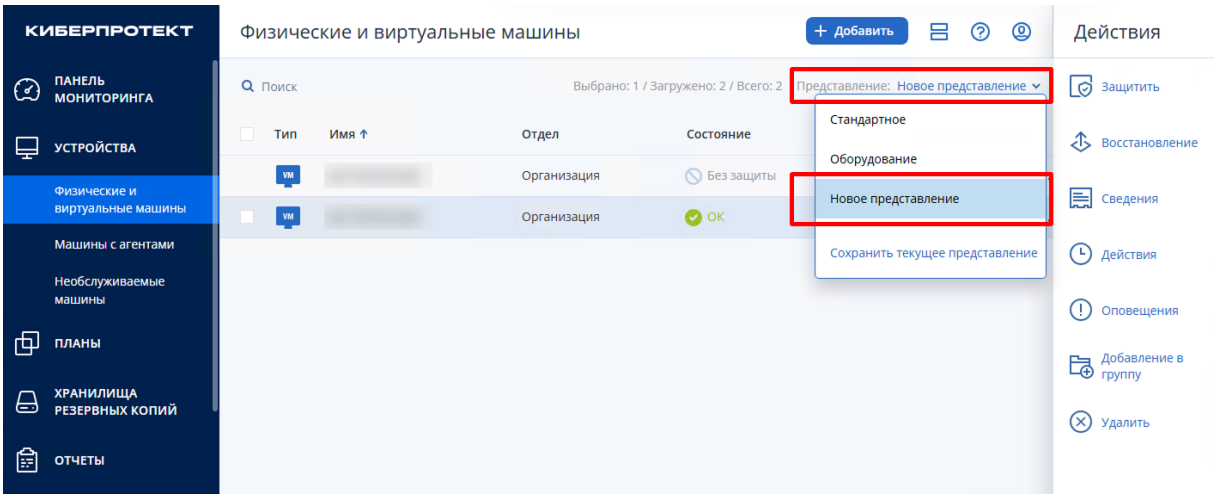
Пользовательский набор отображаемых столбцов можно сохранить. Для этого выполните следующие действия:

1. В верхней строке веб-консоли нажмите название текущего представления.
2. В выпадающем меню нажмите **Сохранить текущее представление**.
3. В окне **Сохранить текущее представление** введите название для нового представления и нажмите **Сохранить**.



В результате пользовательское представление будет сохранено и появится в списке представлений. Также его название появится в верхней строке веб-консоли.

© ООО Киберпротект, 2026



3.6.2.3 Удаление пользовательских представлений

Для удаления пользовательского представления выполните следующие действия:

1. В верхней строке веб-консоли нажмите название текущего представления.
2. В выпадающем меню выберите представление и нажмите значок крестика в его строке.

В результате пользовательское представление будет удалено. Если оно использовалось в момент удаления, система автоматически переключится на **Стандартное** представление.

© ООО Киберпротект, 2026

4 План защиты и модули

План защиты – это план, объединяющий в себе модули защиты данных, указанные ниже:

- "Резервное копирование" (стр. 264) – позволяет создавать резервную копию источников данных в выбранном хранилище данных.
- "Активная защита (Active Protection)" (стр. 240) – позволяет выполнять проверку компьютеров встроенным средством защиты от вредоносных программ.

Создавая гибкие планы для разных потребностей бизнеса, модули можно включить и отключить, задать их настройки.

4.1 Создание плана защиты

План защиты можно применить к нескольким машинам на этапе его создания или позже. При создании плана система проверяет операционную систему и тип устройства (например, рабочая станция, виртуальная машина и т. д.) и показывает только те модули плана, которые применимы к вашим устройствам.

План защиты можно создать одним из двух способов, которые описаны ниже.

- В разделе **Устройства**: при выборе устройства или устройств для защиты с последующим созданием плана для них.
- В разделе **Планы**: при создании плана с последующим выбором машин, к которым он будет применён.

Рассмотрим первый способ.

4.1.1 Порядок создания плана защиты

1. В веб-консоли Кибер Бэкап выберите **Устройства** > **Физические и виртуальные машины**.
2. Выберите машины, для которых нужно обеспечить защиту.
3. Щёлкните **Защитить**, а затем **Создать план**. Откроется план защиты с настройками по умолчанию.
4. [Необязательно] Для изменения имени плана защиты щёлкните значок карандаша рядом с именем.

   Примечание
   Для хранения имени плана может использоваться не более 128 байт. Тип используемых символов влияет на занимаемый ими объём: символ латиницы или цифра занимает 1 байт, символ русского алфавита – 2 байта, эмодзи – 4 байта и более.

5. [Необязательно] Для включения или отключения модуля плана защиты щёлкните переключатель рядом с именем модуля.
6. [Необязательно] Для настройки параметров модуля щёлкните соответствующий раздел плана

© ООО Киберпротект, 2026

защиты.

7. После этого щёлкните **Создать**.

Модуль **Резервное копирование** можно выполнить по требованию. Для этого щёлкните **Запустить сейчас** (подробнее см. в разделе "Запуск резервного копирования вручную" (стр. 309)).

Для настройки модуля Active Protection см. раздел "Активная защита (Active Protection)" (стр. 240).

4.2 Разрешение конфликтов плана

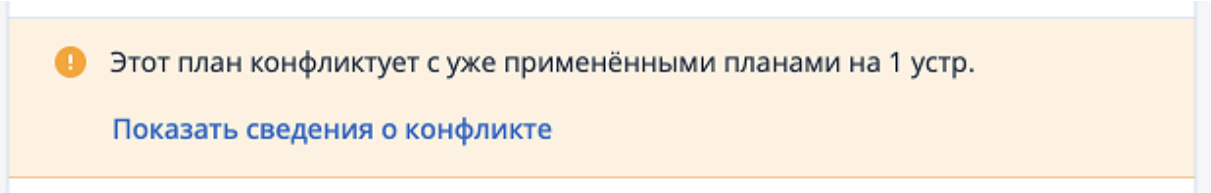
План защиты может иметь одно из указанных ниже состояний.

- **Активный**: план, который назначен устройствам и выполняется на них.
- **Неактивный**: план, который назначен устройствам, но отключен и не выполняется на них.

4.2.1 Применение нескольких планов к устройству

К одному устройству можно применить несколько планов защиты с модулем **Резервное копирование**. Планы с модулем **Active Protection (Активная защита)** применяются с ограничением: этот модуль можно применить к одному устройству только один раз. Например, можно применить план защиты с модулями **Active Protection (Активная защита)** и **Резервное копирование** и другой план, в котором включен только модуль **Резервное копирование**.

При попытке применения нескольких планов защиты с модулем **Active Protection (Активная защита)** возникнет конфликт. В этом случае Кибер Бэкап отобразит уведомление:



4.2.2 Разрешение конфликтов плана

4.2.2.1 План конфликтует с уже примененными планами.

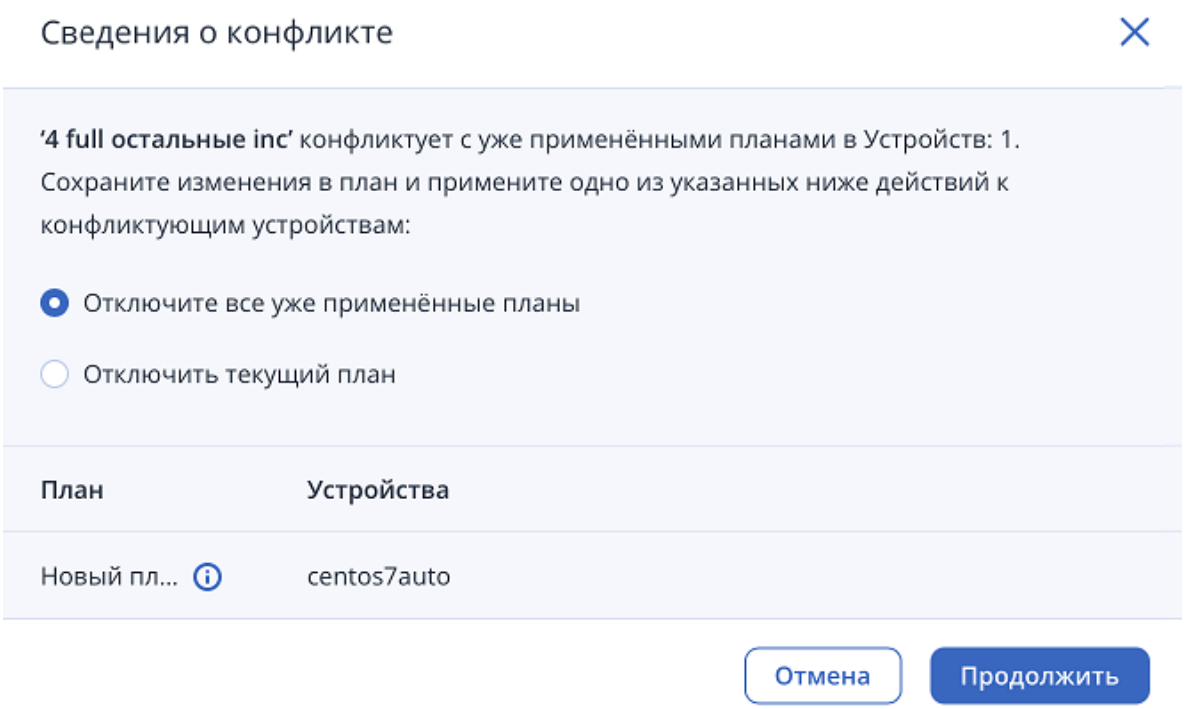
При создании нового плана на устройстве или устройствах с уже примененными планами, которые конфликтуют с новым планом, можно разрешить конфликт одним из указанных ниже способов.

При попытке сохранить план Кибер Бэкап предложит следующие варианты:

- Создать новый план, применить его и отключить все примененные ранее конфликтующие планы.

© ООО Киберпротект, 2026

- Отключить созданный план.



При редактировании плана на устройстве или устройствах с уже примененными другими планами, которые конфликтуют с внесенными изменениями, можно разрешить конфликт одним из способов:

- Сохранить изменения, внесенные в редактируемый план, и отключить все уже примененные ранее конфликтующие планы.
- Отключить редактируемый план с внесенными изменениями.

4.2.2.2 План устройства конфликтует с планом группы

При попытке назначить новый план устройству из группы устройств с назначенным планом группы, система потребует разрешить конфликт посредством одного из следующих действий:

- Удаление устройства из группы и применение нового плана к устройству.
- Применение нового плана ко всей группе или изменение текущего плана группы.

4.2.2.3 Проблемы с лицензией

Назначенная лицензия на устройстве должна обеспечивать выполнение, обновление и применение плана защиты. Чтобы разрешить проблему с лицензией, выполните одно из действий:

- Отключите модули, которые не поддерживаются назначенной лицензией, и продолжите использовать план защиты.
- Измените назначенную лицензию вручную: откройте раздел **Устройства** > **'конкретное устройство'** > **Сведения** > **Лицензия**. После этого отзовите существующую лицензию и назначьте новую.

© ООО Киберпротект, 2026

4.3 Операции с планами защиты

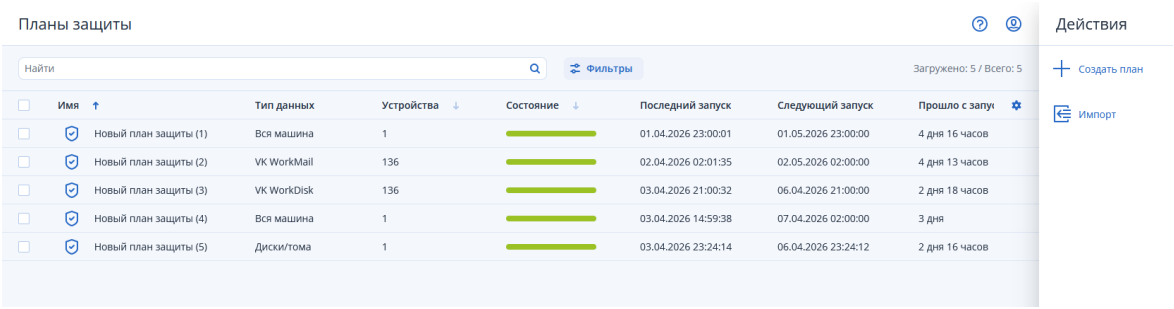
4.3.1 Доступные действия с планами защиты

Действия с планами доступны на вкладке **Планы** основного меню веб-консоли.

Внимание
Вкладка **Планы** доступна при использовании расширенной редакции лицензии продукта. Подробнее о лицензиях см. в разделе "Издания и лицензии Кибер Бэкап" (стр. 16).

Для просмотра возможных действий с планами выполните следующее:

1. Откройте веб-консоль.
2. Перейдите на вкладку **Планы** > **Защита** для просмотра списка планов.



   Список планов можно сортировать по столбцам **Имя**, **Устройства**, **Состояние** и **Отдел**. Кроме того, список можно фильтровать по названию плана или его части (указав его в строке поиска), а также по типу защищаемых данных, состоянию плана и используемым хранилищам (нажав **Фильтры**, выбрав необходимые параметры и нажав **Применить**).

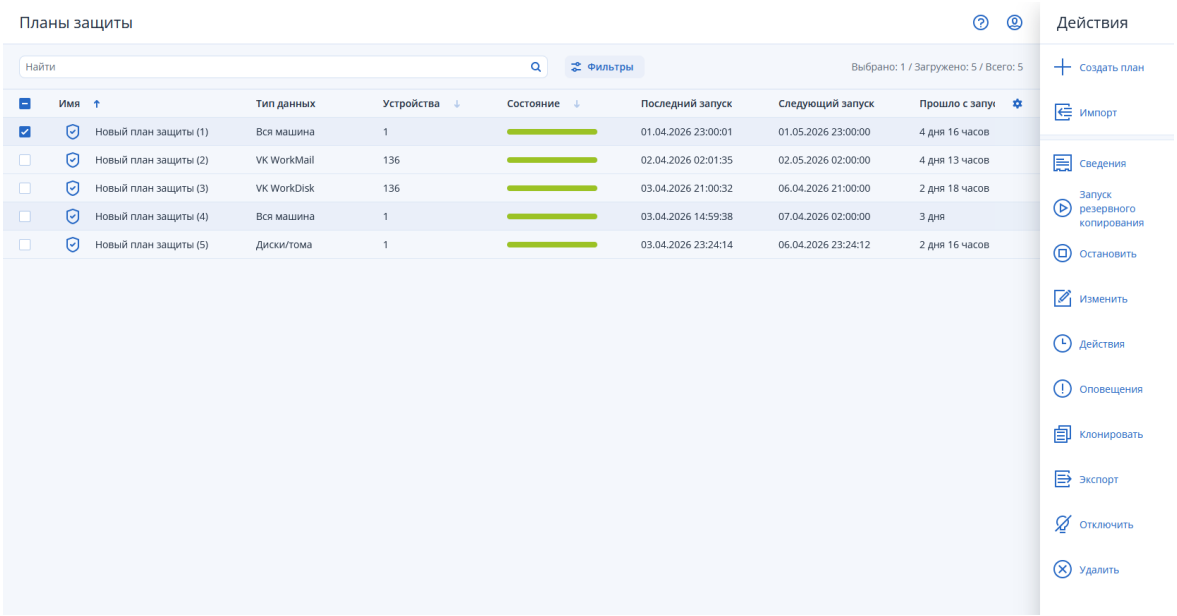
   Справа отображается меню действий с планами. Без выбора плана из этого меню вы можете:

   - создать план;
   - импортировать план.

3. Отметьте план в списке по вашему выбору. Справа в меню появится список действий с

© ООО Киберпротект, 2026

выбранным планом.



С выбранным планом можно выполнить указанные ниже действия:

- просмотреть сведения о плане;
- запустить резервное копирование по требованию;
- остановить выполнение плана;
- изменить план;
- применить план к устройствам или группе устройств;
- отозвать план с устройства;
- просмотреть журнал действий с планом;
- просмотреть оповещения, связанные с планом;
- клонировать план;
- экспортировать план;
- включить или отключить план;
- удалить план.

Примечание
Одно и то же действие с планами может быть доступно из разных вкладок меню действий с планами.

Примечание
Ряд действий с планами доступен также из вкладки **Устройства** основного меню веб-консоли.

4.3.2 Создание плана

Информацию о создании плана защиты см. в разделе "Создание плана защиты" (стр. 224).

© ООО Киберпротект, 2026

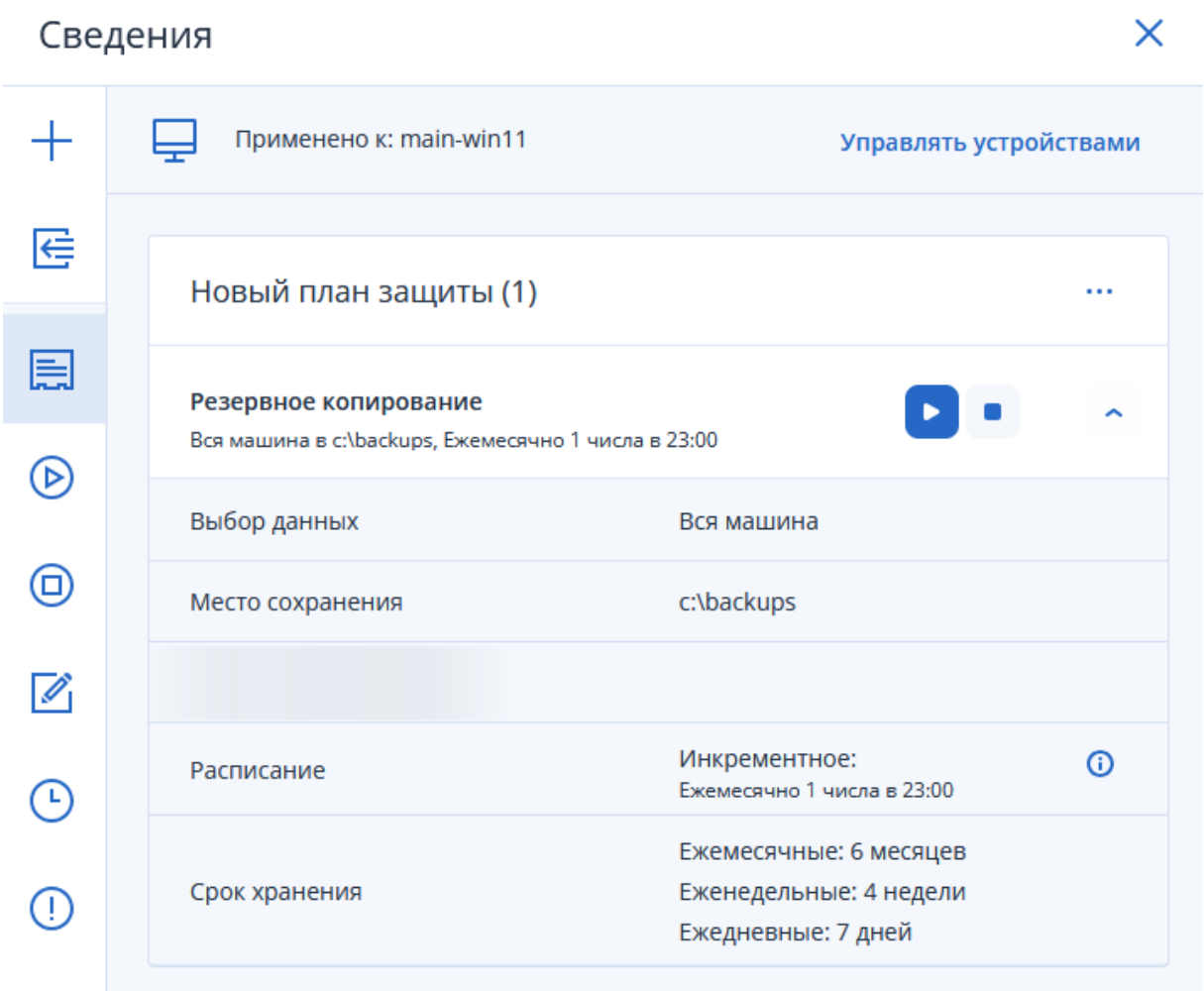
4.3.3 Импорт плана

1. Щелкните **Импорт** в меню действий с планом.
2. Выберите файл с планом и нажмите **Открыть**. План будет добавлен в список планов.

Примечание
Импортировать можно только те планы защиты, которые созданы в Кибер Бэкап 15 и более поздних версиях.

4.3.4 Просмотр сведений о плане

Для просмотра сведений о плане щелкните **Сведения** в меню справа. Отобразится вкладка сведений о плане.



4.3.5 Запуск резервного копирования по требованию

Запуск резервного копирования по требованию описан в разделе "Запуск резервного копирования вручную" (стр. 309).

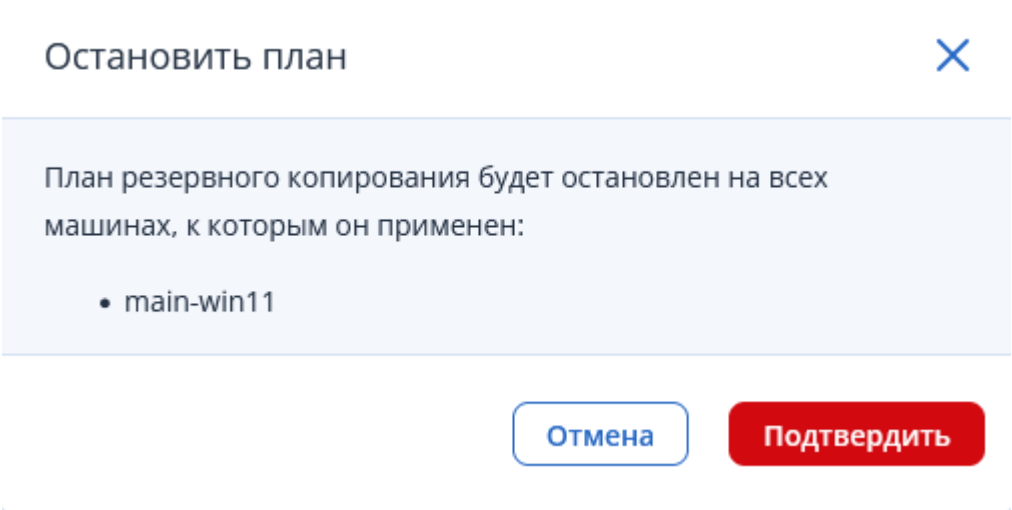
© ООО Киберпротект, 2026

4.3.6 Остановка выполнения плана

Для отмены выполняющегося резервного копирования остановите выполнение плана. Остановку выполнения плана можно произвести любым из следующих способов.

Остановка выполнения плана из меню действий с планом

1. Щелкните **Остановить** в меню действий с планом. Откроется окно подтверждения.



2. Нажмите **Подтвердить**. План будет остановлен.

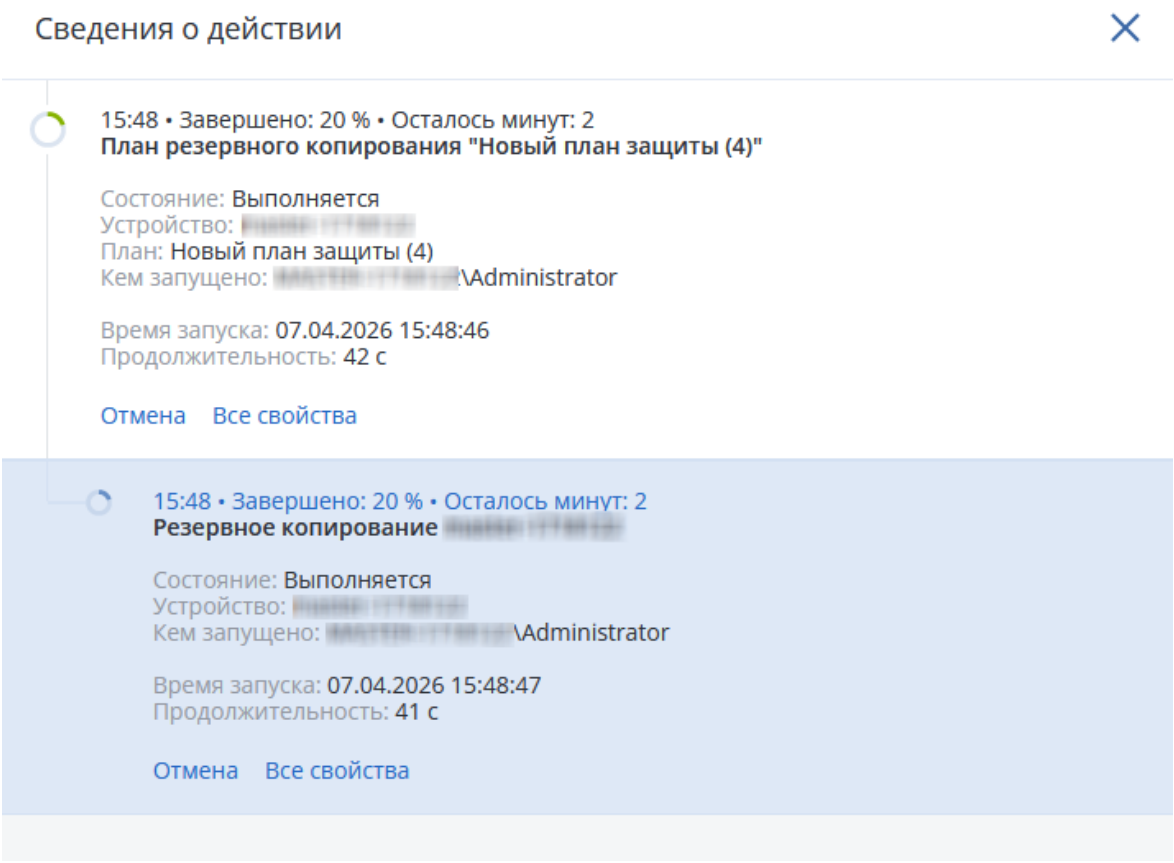
Остановка выполнения плана из вкладки Сведения

1. В меню действий с планом щелкните **Сведения**.
2. Нажмите на значок остановки плана.
3. Нажмите **Подтвердить** в окне подтверждения. План будет остановлен.

Остановка выполнения плана из меню Устройства

1. Перейдите в меню **Устройства**.
2. Отметьте в списке машину с выполняющимся планом и нажмите в меню справа **Действия**.
3. В списке действий выберите требуемое и нажмите **Отмена**.

© ООО Киберпротект, 2026

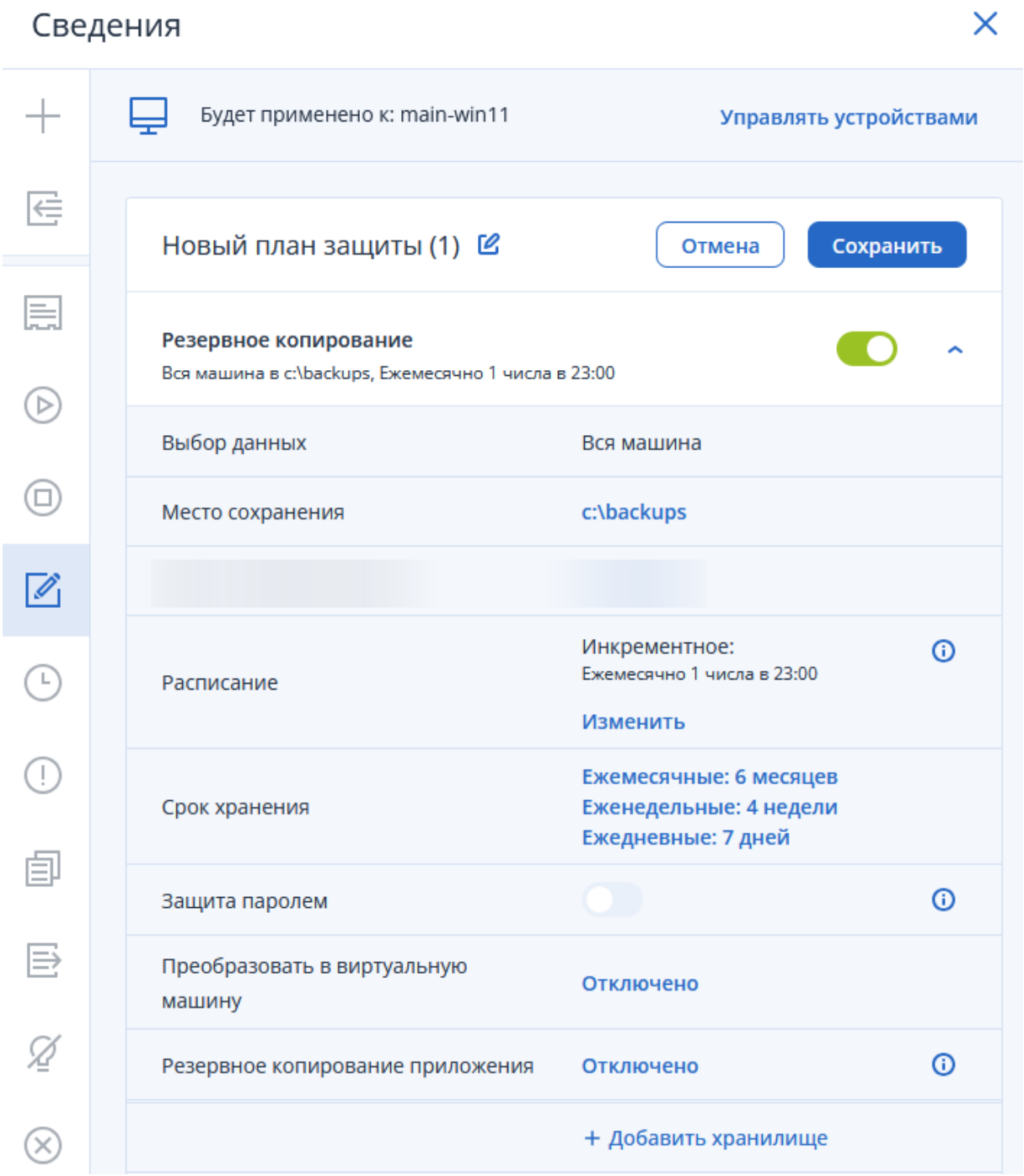


План будет остановлен и появится сообщение об отмене операции.

4.3.7 Изменение плана

Щелкните **Изменить** в меню действий с планом. Откроется вкладка с параметрами плана.

© ООО Киберпротект, 2026



На вкладке можно сделать в т. ч. следующие изменения:

- переименовать план;
- изменить место сохранения резервных копий;
- изменить расписание выполнения плана;
- изменить срок хранения резервных копий;
- изменить дополнительные параметры резервного копирования.

Или (через вкладку **Устройства**):

© ООО Киберпротект, 2026

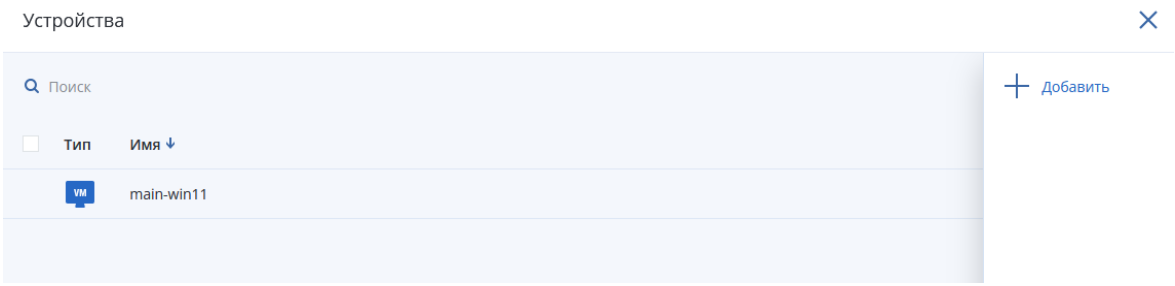
1. Чтобы изменить план защиты для всех машин, к которым он применен, выберите одну из них. В противном случае выберите машины, для которых необходимо изменить план защиты.
2. Щелкните **Защитить**.
3. Выберите план защиты, который необходимо изменить.
4. Щелкните значок многоточия рядом с именем плана резервного копирования и выберите команду **Изменить**.
5. Чтобы изменить параметры плана защиты, щелкните соответствующий раздел на его панели.
6. Щелкните **Сохранить изменения**.
7. Чтобы изменить план защиты для всех машин, к которым он применен, щелкните **Применить изменения к этому плану защиты**. Или щелкните **Создать новый план защиты только для выбранных устройств**.

4.3.7.1 Переименование плана

1. Щелкните **Изменить** в меню действий с планом. Откроется вкладка с параметрами плана.
2. Нажмите на значок редактирования рядом с наименованием плана.
3. Введите в открывшемся окне новое наименование плана и нажмите **Продолжить**. План будет сохранен под новым именем.

4.3.8 Применение плана к устройству или группе устройств

1. В списке планов отметьте план, который вы хотите применить к устройству или устройствам.
2. В меню действий с планом щелкните **Изменить**.
3. Во вкладке параметров плана нажмите **Управлять устройствами**.



4. Нажмите **Добавить**.
5. В списке устройств отметьте одно или несколько устройств, к которым требуется применить план.
6. Щелкните **Добавить** и затем **Готово**.

Или (через вкладку **Устройства**):

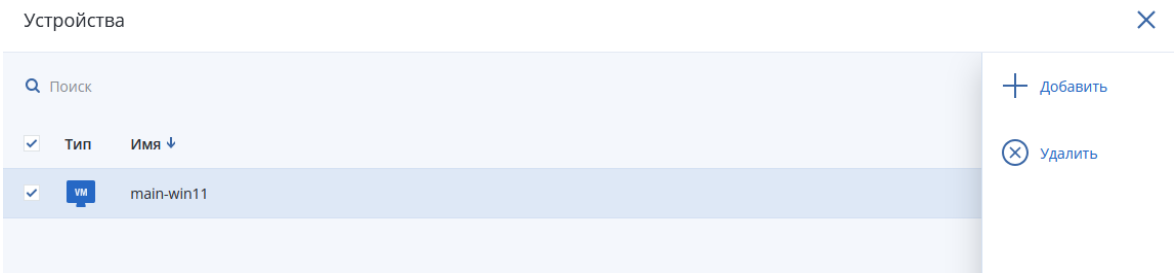
1. Выберите машины, для которых нужно обеспечить защиту.
2. Щелкните **Защитить**. Если план защиты уже применен к выбранным машинам, щелкните **Добавить план**.

© ООО Киберпротект, 2026

3. В программе отображаются ранее созданные планы защиты.
4. Выберите необходимую защиту и щелкните **Применить**.

4.3.9 Отзыв плана с устройства

1. В списке планов отметьте план, который вы хотите отозвать с устройства.
2. В меню действий с планом щелкните **Изменить**.
3. На вкладке **Изменить** нажмите **Управлять устройствами**. Появится список устройств, к которым применен план.
4. В списке устройств отметьте устройство, с которого хотите отозвать план.



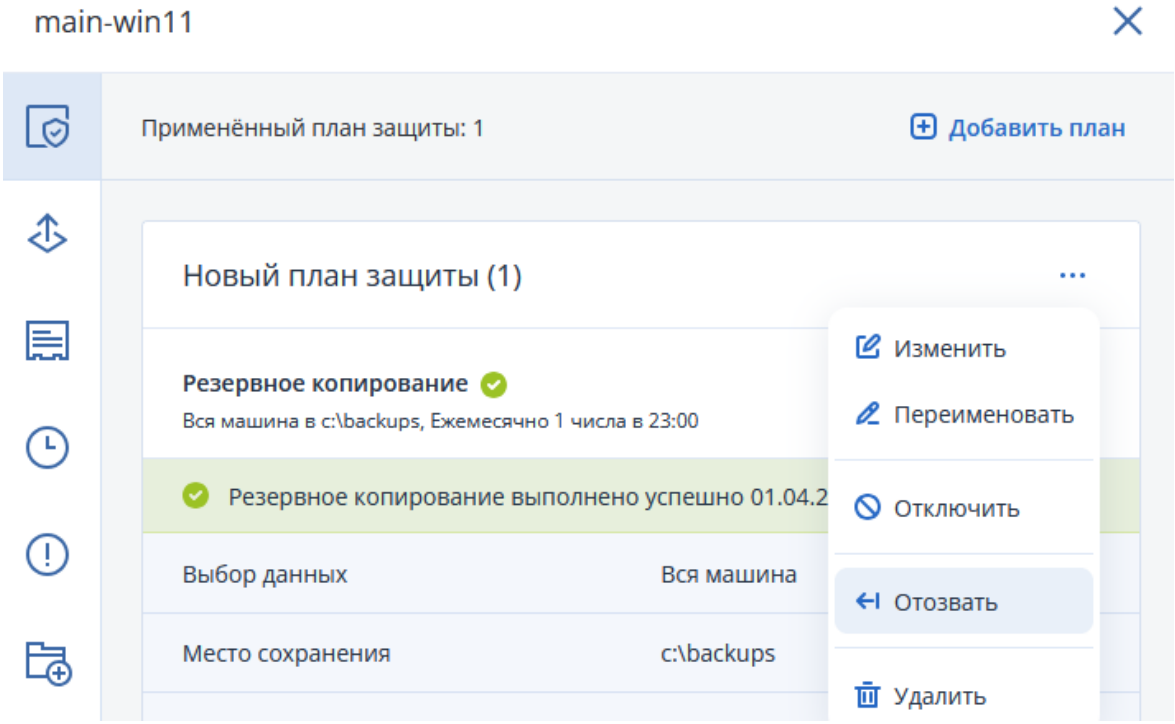
5. Щелкните **Удалить** и затем **Готово**.
6. Нажмите **Сохранить** для сохранения изменений.

Или (через вкладку **Устройства**):

1. Выберите машины, для которых нужно отозвать план защиты.
2. Щелкните **Защитить**.
3. Если для машин применено несколько планов защиты, выберите тот из них, который необходимо отозвать.

© ООО Киберпротект, 2026

4. Щелкните значок многоточия рядом с именем плана защиты и выберите команду **Отозвать**.



Отозванный план больше не применяется к устройствам.

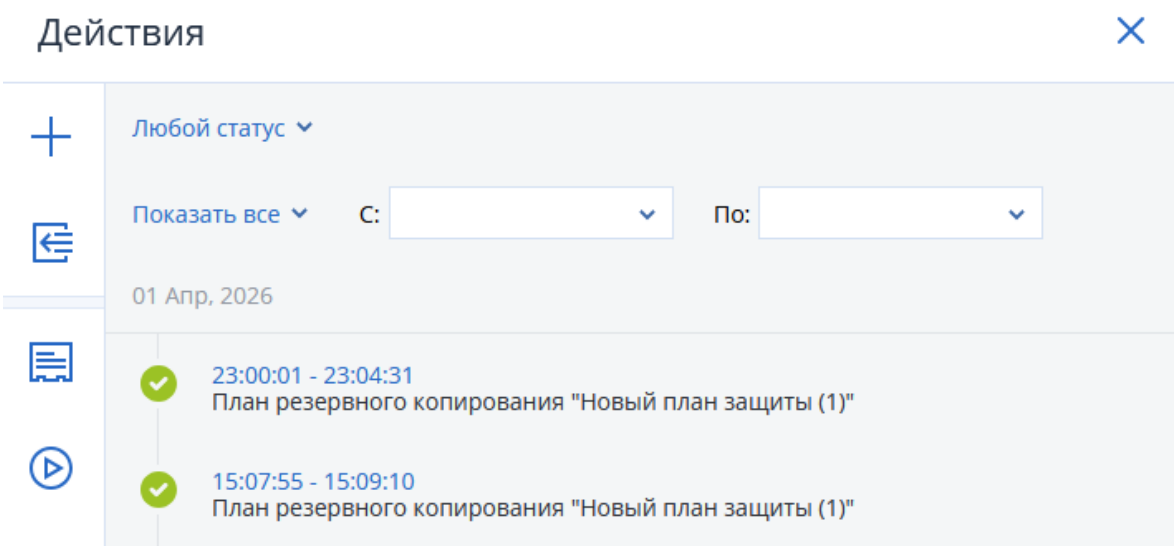
Это действие удобно для администраторов, которым не нужно быстро защитить то же самое устройство тем же планом защиты. Для восстановления защиты, которая обеспечивалась отозванным планом, администратор должен знать имя этого плана, выбрать его из списка доступных планов, а затем заново применить план к желаемому устройству.

4.3.10 Просмотр журнала действий с планом

Для просмотра журнала действий с выбранным планом резервного копирования выполните следующие шаги:

1. Щелкните **Действия** в меню действий с планом. В результате будет отображён список всех действий с планом.

© ООО Киберпротект, 2026



2. Для просмотра более детальной информации нажмите на выбранную запись о действии. После этого будет открыто окно **Сведения о действии**, в котором будут отображены детальные данные.

Примечание
Записи о действиях, связанных с планами защиты, также отображаются во вкладке **Панель мониторинга** > **Действия** (см. подробнее раздел "Панель мониторинга "Действия"" (стр. 728)).

Доступна фильтрация записей о действиях:

- по статусу;
- по временному интервалу.

Для фильтрации записей о действиях с планом по статусу нажмите **Любой статус** и в выпадающем списке выберите один из вариантов:

- любой статус;
- выполняется;
- выполнено с предупреждениями;
- успешно;
- с ошибками.

Для фильтрации записей о действиях с планом по временному интервалу можно:

- выбрать произвольные даты диапазона в полях **С** и **По**;
- нажать **Другой период** и в выпадающем списке выбрать один из вариантов:
  - показать все;
  - последние 24 часа;

© ООО Киберпротект, 2026

- предыдущая неделя;
- предыдущий месяц.

В случае отсутствия записей в соответствии с примененным фильтром будет отображено сообщение "Нет действий".

Для снятия фильтра нажмите на значок крестика в полях **С** и **По**.

4.3.11 Оповещения

Для просмотра оповещений, связанных с выбранным планом защиты, щелкните **Оповещения** в меню действий с планом. В результате будут отображены оповещения (при их наличии) или сообщение "Нет оповещений" (при их отсутствии).

Для удаления выбранного оповещения нажмите **Очистить** в области соответствующего оповещения. Для удаления всех оповещений по выбранному плану защиты нажмите **Очистить все**.

Примечание
Оповещения, связанные с планами защиты, также отображаются во вкладке **Панель мониторинга** > **Оповещения** (см. подробнее раздел "Панель мониторинга "Оповещения"" (стр. 726)).

Внимание
При удалении оповещений в меню действий с планом защиты они также удаляются и из оповещений во вкладке **Панель мониторинга**.

4.3.12 Клонирование плана

Клонирование плана позволяет быстро перенести параметры плана на другое устройство по вашему выбору.

1. В списке планов отметьте план, который вы хотите клонировать для другого устройства.
2. Щелкните **Клонирование** в меню действий с планом. Откроется вкладка создания плана защиты с выбором устройства.
3. Нажмите **Добавить устройство**.
4. Выберите устройство из списка и нажмите **Добавить**.
5. Назначьте имя плану и нажмите **Сохранить**. План с действующими параметрами будет применен к выбранному устройству.

4.3.13 Экспорт плана

Экспорт плана позволяет сохранить план в файл в формате JSON.

1. Щелкните **Экспорт** в меню действий с планом.
2. Введите имя файла и нажмите **Сохранить**. План вместе с параметрами будет сохранен в файл.

© ООО Киберпротект, 2026

4.3.14 Включение / отключение плана

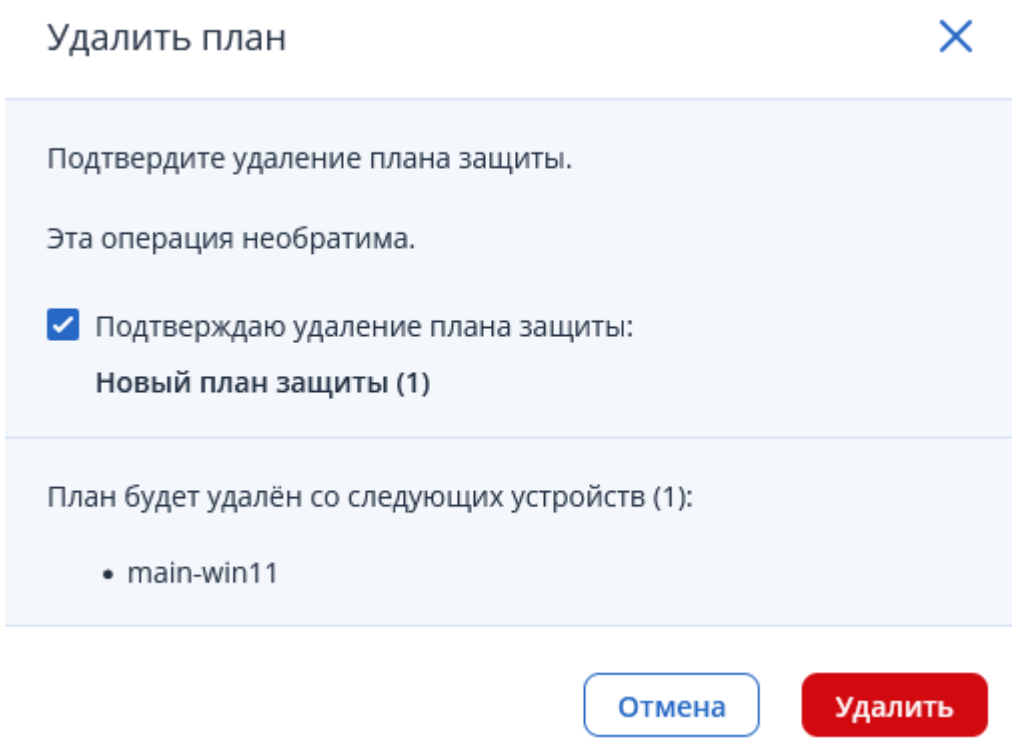
1. Нажмите **Включить** или **Отключить** в меню действий с планом. Сразу после нажатия совершится выбранное действие.

Отключенный план не будет выполняться на устройстве, к которому он применен.

Это действие удобно для администраторов, которые планируют защитить то же самое устройство тем же планом защиты позже. Поскольку план не отзывается с устройства, для восстановления защиты администратору необходимо только заново включить план.

4.3.15 Удаление плана

1. Щелкните **Удалить** в меню действий с планом.
2. В открывшемся окне подтвердите удаление плана, отметив поле подтверждения.



3. Нажмите **Удалить**. План будет удален из списка планов.

Или (через вкладку **Устройства**):

1. Выберите любую машину, для которой применен план защиты, который необходимо удалить.
2. Щелкните **Защитить**.
3. Если для машины применено несколько планов защиты, выберите тот из них, который необходимо удалить.
4. Щелкните значок многоточия рядом с именем плана защиты и выберите команду **Удалить**.

© ООО Киберпротект, 2026

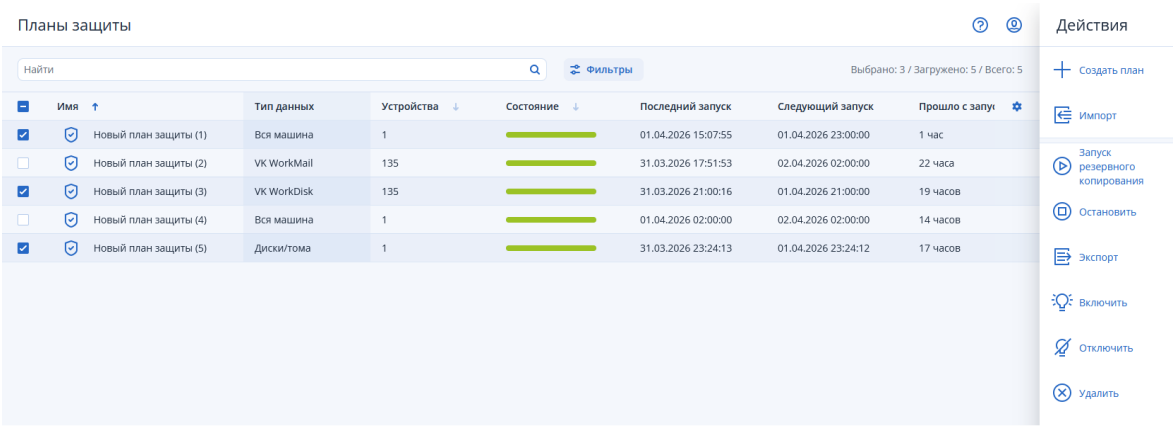
5. В результате план защиты будет отозван для всех машин и полностью удален из веб-интерфейса.

4.3.16 Групповые действия с планами

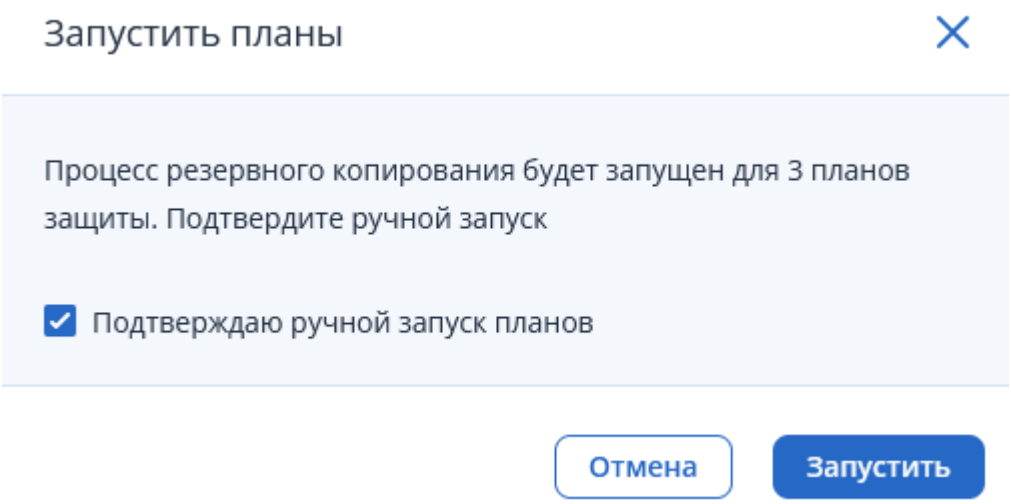
Начиная с версии 18.5 в Кибер Бэкап доступны групповые действия с планами защиты.

Внимание
Перед выполнением групповых действий с планами защиты убедитесь, что включено одновременное резервное копирование (подробнее см. раздел "Одновременное резервное копирование" (стр. 312)).

1. Отметьте в списке планов защиты нужные планы.



2. В меню справа выберите действие, которое необходимо совершить с выбранными планами, и щелкните его.
3. В открывшемся окне подтвердите выбранное действие.



4. Дождитесь окончания операции.

© ООО Киберпротект, 2026

Примечание
Одновременный запуск большого количества планов может приводить к снижению производительности резервного копирования. Во избежание этого запускайте планы небольшими группами.

Обзор групповых действий с планами доступен на вкладке **Панель мониторинга** -> **Действия**.

4.4 Активная защита (Active Protection)

Active Protection – это отдельный модуль в плане защиты, который отслеживает процессы, запущенные на защищённом компьютере. Когда процесс сторонней программы пытается шифровать файлы или запускает математические вычисления в фоновом режиме, похищая вычислительную мощность и увеличивая сетевой трафик, Active Protection создаёт оповещение и выполняет дополнительные действия в соответствии с заданными настройками.

Также Active Protection предотвращает неавторизованные изменения собственных процессов, записей реестра, исполняемых и конфигурационных файлов и резервных копий, расположенных в локальных папках.

Для распознавания вредоносных процессов Active Protection использует поведенческий анализ. Active Protection сравнивает цепочку действий, выполняемых процессом, с цепочками событий, записанных в базе данных шаблонов вредоносного поведения. Такой подход позволяет обнаруживать новые вредоносные программы по их типичному поведению.

Служба Active Protection доступна для машин с ОС Windows (подробнее см. в разделе "Active Protection для Windows" (стр. 241)) и с ОС Linux (подробнее см. в разделе "Active Protection для Linux" (стр. 245)).

Примечание
Для использования службы Active Protection на машине – источнике данных должен быть установлен агент для Windows или для Linux. В случае отсутствия на ней агента для Windows или для Linux или при резервном копировании виртуальной машины в безагентном режиме служба Active Protection должна оставаться выключенной в настройках плана защиты.

Возможности службы Active Protection в зависимости от установленной на машине операционной системы приведены в таблице.

Функция	Машина с ОС Windows	Машина с ОС Linux
Действие при обнаружении	+	+
Исключения	+	+
Выявление процессов майнинга криптовалют	+	-

© ООО Киберпротект, 2026

Самозащита	+	-
Защита сетевых папок	+	-
Защита на стороне сервера (внешняя защита сетевых папок)	+	-

4.4.1 Технические требования и ограничения службы Active Protection

4.4.1.1 Active Protection для Windows

Служба Active Protection доступна для машин со следующими операционными системами семейства Windows:

- Windows Server 2012 R2 (64-разрядные версии) — все выпуски;
- Windows Server 2016–2022 (64-разрядные версии) — все выпуски, кроме Nano Server;
- Windows 10 (64-разрядные версии) — выпуски Home, Pro, Education, Enterprise, IoT Enterprise и LTSC (прежнее название LTSB);
- Windows 11 (64-разрядные версии) — все выпуски.

На машине должен быть установлен агент для Windows.

4.4.1.2 Active Protection для Linux

Служба Active Protection доступна во всех операционных системах, поддерживающих агент для Linux (см. раздел "Агенты" (стр. 23)), с учётом следующих требований и ограничений:

- Ядро Linux должно поддерживать установку драйвера file_protection_linux.
- Ядра Linux новее версии 4.9 должны поддерживать технологию трассировки ftrace (Function Tracer).
- Не поддерживается совместная работа модуля с ПО Kaspersky Endpoint Security для Linux. Если включен модуль, блокируется установка Kaspersky Endpoint Security для Linux. Если включено ПО Kaspersky Endpoint Security для Linux, блокируется работа модуля.
- Не поддерживается работа модуля в ОС Astra Linux 1.7.x с ядром версии 6.1.90, а также ОС Astra Linux 1.8.x с ядрами версий 6.1.90, 6.6.28.
- Не поддерживается работа модуля в ОС Debian, Ubuntu, Astra Linux с защищёнными (hardened) ядрами.

На машине должен быть установлен агент для Linux.

4.4.2 Active Protection для Windows

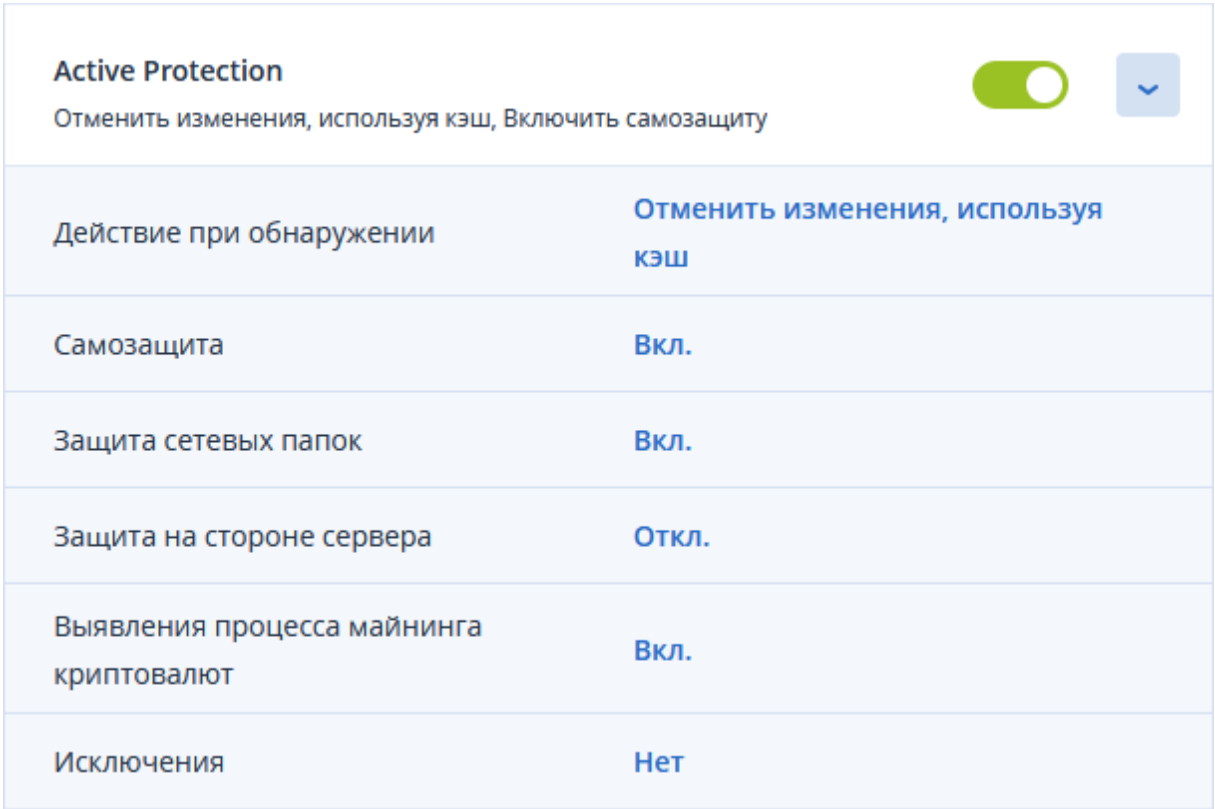
На машине с ОС Windows служба Active Protection обеспечивает защиту компьютера от вредоносных программ и имеет следующие настройки:

© ООО Киберпротект, 2026

- **Действие при обнаружении**;
- **Самозащита**;
- **Защита сетевых папок**;
- **Защита на стороне сервера**;
- **Выявления процессов майнинга криптовалют**;
- **Исключения**.

По умолчанию служба Active Protection выключена. Чтобы активировать её, в веб-консоли Кибер Бэкап перейдите на вкладку **Планы** > **Защита**, выберите план защиты из списка и на панели **Действия** щёлкните **Изменить** (либо создайте новый план защиты, подробнее см. раздел "Создание плана защиты" (стр. 224)), затем переведите соответствующий переключатель в положение **Включено**.

Для перехода к настройкам параметров службы Active Protection нажмите на стрелку справа от переключателя. Вид окна настроек службы Active Protection на машине с ОС Windows приведён на рисунке.



4.4.2.1 Действие при обнаружении

Параметр **Действие при обнаружении** определяет действие, которое будет выполняться при обнаружении подозрительной активности.

Для настройки параметра выполните следующие действия:

© ООО Киберпротект, 2026

1. Щёлкните в области строки **Действие при обнаружении**.
2. Выберите действие:
   - **Только уведомить** – программа создаст оповещение о процессе.
   - **Остановить процесс** – программа создаст оповещение о процессе и остановит процесс.
   - **Отменить изменения, используя кэш** (значение по умолчанию) – программа создаст оповещение, остановит процесс и отменит внесённые в файл изменения, используя кэш службы.
3. Для сохранения выбранной настройки нажмите **Готово**.

4.4.2.2 Самозащита

Параметр **Самозащита** предотвращает несанкционированные изменения в собственных процессах программного обеспечения, записях реестра, исполняемых и конфигурационных файлах и резервных копиях, расположенных в локальных папках.

Примечание
Значение по умолчанию: **Вкл.** (включено). Отключение параметра **Самозащита** не рекомендуется.

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Самозащита**.
2. При необходимости переведите переключатель в положение **Вкл.** (включено).
3. [Необязательно] Установите флажок **Разрешить определённым процессам изменять резервные копии**.

   Нажмите **Добавить** и укажите процессы, которым разрешено изменять файлы резервных копий, даже если эти файлы защищены системой самозащиты. Это полезно, например, при удалении файлов резервных копий или перемещении их в другое место с помощью скрипта.

   Если функция **Разрешить определённым процессам изменять резервные копии** отключена, файлы резервных копий могут быть изменены только процессами, подписанными поставщиком программного обеспечения для резервного копирования. Это позволяет программному обеспечению применять правила хранения и удалять резервные копии, когда пользователь запрашивает это через веб-интерфейс. Другие процессы, независимо от того, подозрительные они или нет, не могут изменять резервные копии.

   Эта возможность относится к файлам резервных копий, которые имеют расширения .tibx, .tib, .tia и расположены в локальных папках.
4. Для сохранения настроек нажмите **Готово**.

4.4.2.3 Защита сетевых папок

Параметр **Защита сетевых папок** позволяет защитить сетевые папки, назначенные как локальные диски, от локальных вредоносных процессов.

© ООО Киберпротект, 2026

Этот параметр применяется к папкам, к которым предоставляется общий доступ по протоколам SMB или NFS.

Если файл изначально был расположен на подключённом диске, он не может быть сохранён в исходное местоположение при извлечении из кэша с помощью действия **Отменить изменения, используя кэш**. Вместо этого он будет сохранён в папку, указанную в настройках параметра.

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Защита сетевых папок**.
2. При необходимости переведите переключатель в положение **Вкл.** (включено).
3. [Необязательно] Укажите адрес локальной папки для сохранения восстановленных файлов. Если указанная папка не существует, она будет создана.

   Примечание
   Сетевые папки, включая папки на подключённых дисках, не поддерживаются.

4. Для сохранения настроек нажмите **Готово**.

Значение по умолчанию: **Вкл.** (включено).

4.4.2.4 Защита на стороне сервера (внешняя защита сетевых папок)

Параметр **Защита на стороне сервера** определяет, будут ли защищены сетевые папки, к которым предоставлен общий доступ, от внешних входящих подключений с других серверов в сети, которые потенциально могут представлять угрозы.

Значение по умолчанию: **Откл.** (отключено).

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Защита на стороне сервера**.
2. При необходимости переведите переключатель в положение **Вкл.** (включено).
3. [Необязательно] щёлкните по вкладке **Доверенные**, нажмите **Добавить** и укажите имя пользователя и IP-адрес для подключения, которому разрешено изменять любые данные.
4. [Необязательно] щёлкните по вкладке **Заблокировано**, нажмите **Добавить** и укажите имя пользователя и IP-адрес для подключения, которому не разрешено изменять никакие данные.
5. Для сохранения настроек нажмите **Готово**.

4.4.2.5 Выявление процессов майнинга криптовалют

Параметр **Выявление процессов майнинга криптовалют** позволяет обнаруживать вредоносное программное обеспечение для майнинга криптовалют, снижающее производительность полезных приложений и увеличивающее потребление электроэнергии, что в результате может привести к сбоям системы и даже повреждению оборудования. Рекомендуется добавить вредоносные программы для майнинга в список вредоносных процессов для предотвращения их запуска.

Значение по умолчанию: **Откл.** (отключено).

© ООО Киберпротект, 2026

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Выявление процессов майнинга криптовалют**.
2. При необходимости переведите переключатель в положение **Вкл.** (включено).
3. Выберите действие, которое будет выполняться при обнаружении активности майнинга криптовалют:
   - **Только уведомить** – программа создаст оповещение о подозрительном процессе.
   - **Остановить процесс** – программа создаст оповещение и останавливает подозрительный процесс.
4. Для сохранения настроек нажмите **Готово**.

4.4.2.6 Исключения

Параметр **Исключения** позволяет свести к минимуму ресурсы, используемые для поведенческого анализа, и исключить так называемые ложные срабатывания, когда доверенная программа рассматривается как программа-вымогатель.

Данный параметр позволяет создать:

- список доверенных процессов, которые никогда не будут рассматриваться как вредоносные программы;
- список процессов, запуск которых всегда будет заблокирован, пока на компьютере включен модуль Active Protection.

Примечание
Процессы, подписанные корпорацией Майкрософт, всегда являются надёжными.

Значение по умолчанию: **Нет** (списки доверенных и заблокированных процессов пустые).

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Исключения**.
2. [Необязательно] Щёлкните по вкладке **Доверенные** и укажите:
   - Полный путь к исполняемому файлу процесса, который никогда не будет рассматриваться как вредоносная программа.
   - Полный путь к папке, в которой не будут отслеживаться изменения файлов.
3. [Необязательно] Щёлкните по вкладке **Заблокировано** и укажите полный путь к исполняемому файлу процесса, который всегда будет заблокирован.
4. Для сохранения настроек нажмите **Готово**.

4.4.3 Active Protection для Linux

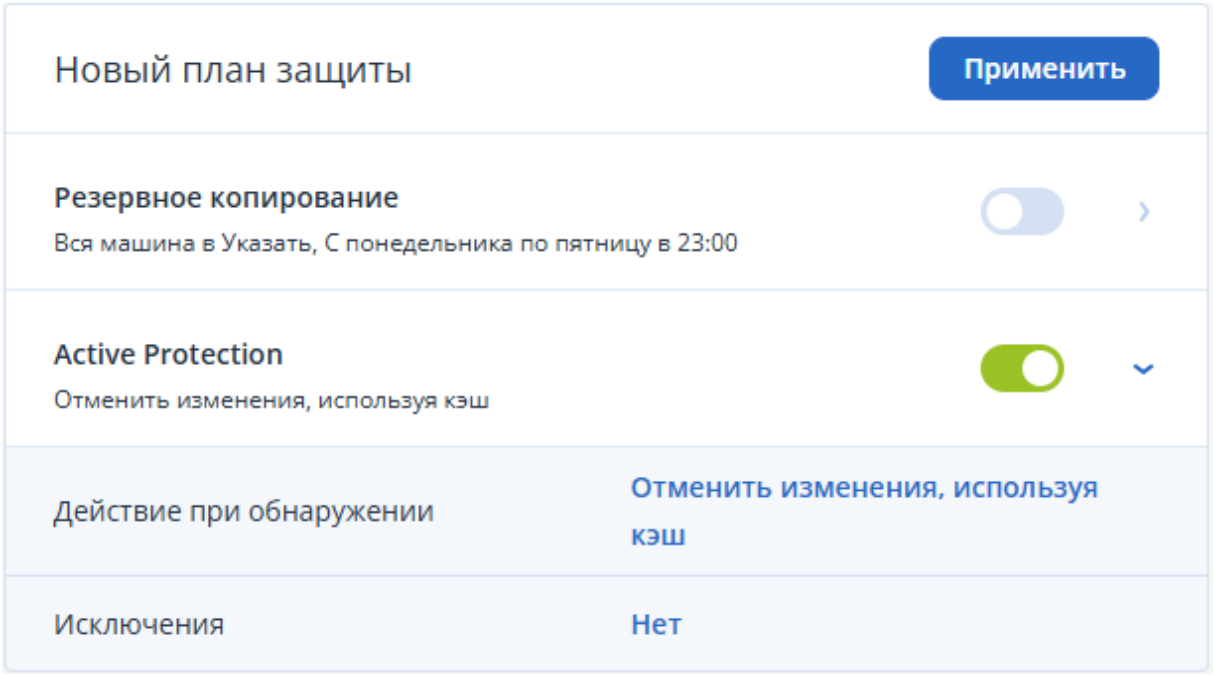
На машине с ОС Linux служба Active Protection обеспечивает защиту компьютера от вредоносных программ и имеет следующие настройки:

© ООО Киберпротект, 2026

- **Действие при обнаружении**;
- **Исключения**.

По умолчанию служба Active Protection выключена. Чтобы активировать её, в веб-консоли Кибер Бэкап перейдите на вкладку **Планы** > **Защита**, выберите план защиты из списка и на панели **Действия** щёлкните **Изменить** (либо создайте новый план защиты, подробнее см. раздел "Создание плана защиты" (стр. 224)), затем переведите соответствующий переключатель в положение **Включено**.

Для перехода к настройкам параметров службы Active Protection нажмите на стрелку справа от переключателя. Вид окна настроек службы Active Protection на машине с ОС Linux приведён на рисунке.



4.4.3.1 Действие при обнаружении

Параметр **Действие при обнаружении** определяет действие, которое будет выполняться при обнаружении подозрительной активности.

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Действие при обнаружении**.
2. Выберите действие:
   - **Только уведомить** – программа создаст оповещение о процессе.
   - **Остановить процесс** – программа создаст оповещение о процессе и остановит процесс.
   - **Отменить изменения, используя кэш** (значение по умолчанию) – программа создаст оповещение, остановит процесс и отменит внесённые в файл изменения, используя кэш

© ООО Киберпротект, 2026

службы.

3. Для сохранения выбранной настройки нажмите **Готово**.

4.4.3.2 Исключения

Параметр **Исключения** позволяет свести к минимуму ресурсы, используемые для поведенческого анализа, и исключить так называемые ложные срабатывания, когда доверенная программа рассматривается как программа-вымогатель.

Данный параметр позволяет создать:

- список доверенных процессов, которые никогда не будут рассматриваться как вредоносные программы;
- список процессов, запуск которых всегда будет заблокирован, пока на компьютере включен модуль Active Protection.

Значение по умолчанию: **Нет** (списки доверенных и заблокированных процессов пустые).

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Исключения**.
2. [Необязательно] Щёлкните по вкладке **Доверенные** и укажите:
   - Полный путь к исполняемому файлу процесса, который никогда не будет рассматриваться как вредоносная программа.
   - Полный путь к папке, в которой не будут отслеживаться изменения файлов.
3. [Необязательно] Щёлкните по вкладке **Заблокировано** и укажите полный путь к исполняемому файлу процесса, который всегда будет заблокирован.
4. Для сохранения настроек нажмите **Готово**.

© ООО Киберпротект, 2026

5 Группы устройств

Группы устройств призваны обеспечить простое управление большим количеством зарегистрированных устройств.

Вы можете применить план защиты к группе. После появления нового устройства в группе, это устройство будет защищено планом. Если устройство удалено из группы, оно больше не будет защищено планом. Если план применим к группе, нельзя отменить его применение к одному из членов группы, только ко всей группе.

В группу могут быть добавлены устройства только одного типа. Например в **Hyper-V** вы можете создать группу виртуальных машин Hyper-V. В разделе **Машины с агентами** можно создать группу машин с установленными агентами. В разделе **Физические и виртуальные машины** невозможно создать группу.

Одно устройство может входить в несколько групп.

5.1 Встроенные группы

После регистрации устройства оно появляется в одной из встроенных корневых групп на вкладке **Устройства**.

Корневые группы *невозможно* редактировать или удалить. *Невозможно* применить план к корневым группам.

Некоторые корневые группы содержат встроенные подкорневые группы. Такие группы *невозможно* редактировать или удалить. Однако *возможно* применить планы к подкорневым встроенным группам.

5.2 Пользовательские группы

Защита всех устройств во встроенной группе с помощью одного плана защиты может быть неудовлетворительной из-за разных ролей машин. У каждого отдела есть свои данные для резервного копирования. Для некоторых данных резервные копии требуется создавать часто, тогда как для других – пару раз в год. Поэтому может потребоваться создать различные планы защиты, применяющиеся на разных группах машин. В этом случае следует рассмотреть возможность создания пользовательских групп.

Пользовательская группа может включать одну или несколько вложенных групп. Любую пользовательскую группу можно изменить или удалить. Существует несколько типов пользовательских групп.

- **Статические группы**

  Статические группы содержат машины, добавленные вручную. Состав статической группы меняется, только если вы специально добавите или удалите машину.

  Пример: Вы создали пользовательскую группу для отдела бухгалтерии и вручную добавили в группу машины бухгалтеров. Когда к этой группе будет применен план защиты, машины

© ООО Киберпротект, 2026

сотрудников бухгалтерии будут защищены. Если в отдел пришел новый сотрудник, следует включить его машину в эту группу вручную.

- **Динамические группы**

  Динамические группы содержат машины, добавленные автоматически в соответствии с поисковыми критериями, определенными при создании группы. Состав динамической группы меняется автоматически. Машина остается в группе до тех пор, пока отвечает заданным критериям.

  Пример 1. Имена хостов машин, принадлежащих к отделу бухгалтерии, содержат слово «бухгалтерия». Достаточно задать часть имени машины в качестве критерия членства в группе и применить к этой группе план защиты. Машина нового бухгалтера добавляется в группу сразу после регистрации. Таким образом она будет автоматически защищена.

  Пример 2. Отдел бухгалтерии формирует отдельную организационную единицу Active Directory (OU). Укажите организационную единицу бухгалтерии как критерий членства в группе и примените к данной группе план защиты. Машина нового бухгалтера добавляется в группу сразу после регистрации и добавления к организационной единице независимо от того, какое действие выполняется первым. Таким образом она будет автоматически защищена.

5.3 Операции со статическими группами

Со статическими группами доступны следующие операции:

- создание (см. далее в этом разделе);
- добавление устройств в группы и удаление из них (см. далее в этом разделе);
- применение плана защиты к группе (подробнее см. в разделе "Применение плана защиты к группе" (стр. 262));
- переименование (подробнее см. в разделе "Переименование группы" (стр. 262));
- удаление (подробнее см. в разделе "Удаление группы" (стр. 263)).

5.3.1 Создание статических групп

Для создания статической группы выполните следующие действия:

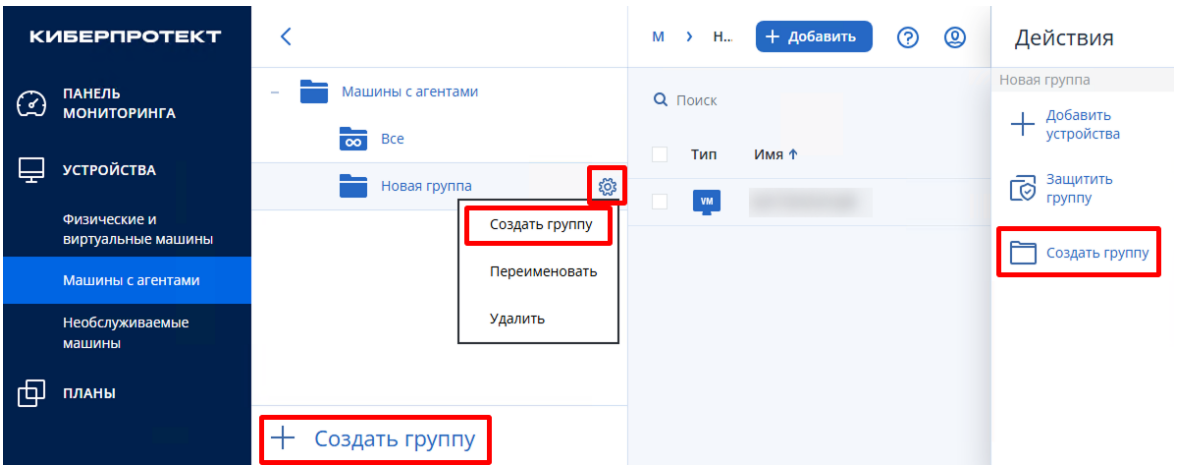
1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Машины с агентами**.
2. Выберите группу, внутри которой необходимо создать статическую группу.

   Примечание
   Доступно для встроенной корневой группы, а также пользовательских групп.

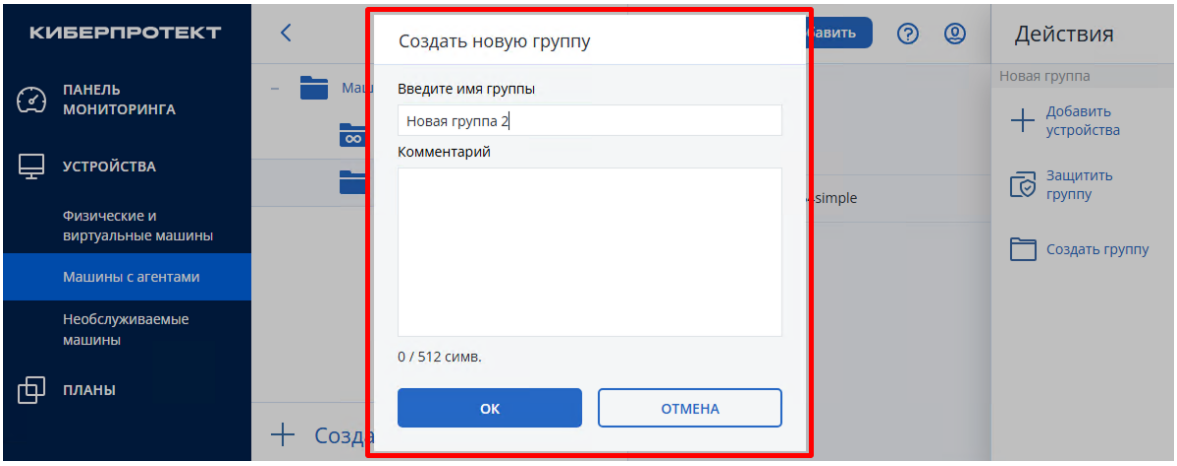
3. Выполните одно из указанных действий:
   - Нажмите на значок шестерёнки и в выпадающем меню выберите **Создать группу**.
   - В нижней части веб-консоли нажмите **Создать группу**.

© ООО Киберпротект, 2026

- Справа на панели **Действия** щёлкните **Создать группу** (доступно, если родительская группа не пустая).



4. В окне **Создать новую группу** введите имя группы. При необходимости добавьте комментарий длиной до 512 символов.
5. Нажмите **OK**.



В результате новая группа будет отображена в списке групп.

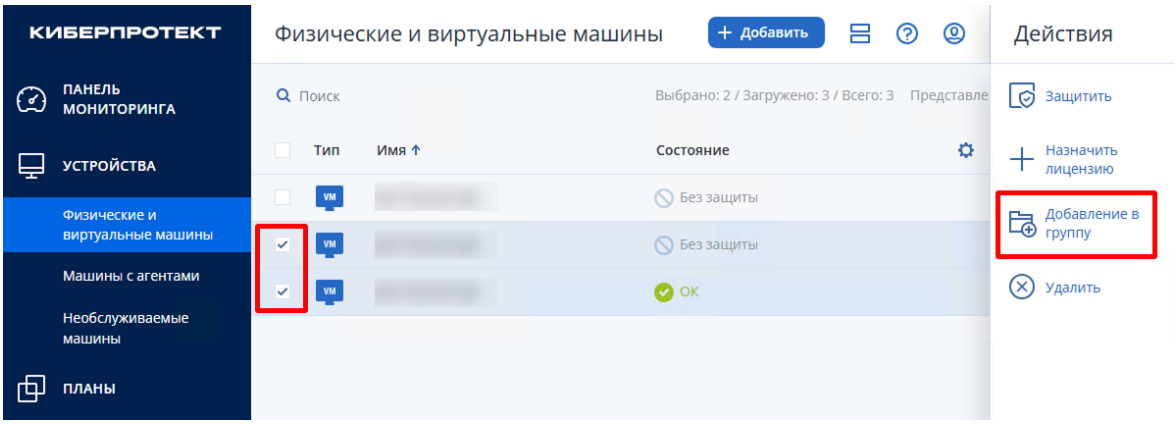
5.3.2 Добавление устройств в статические группы

Добавить устройства в статическую группу можно несколькими способами.

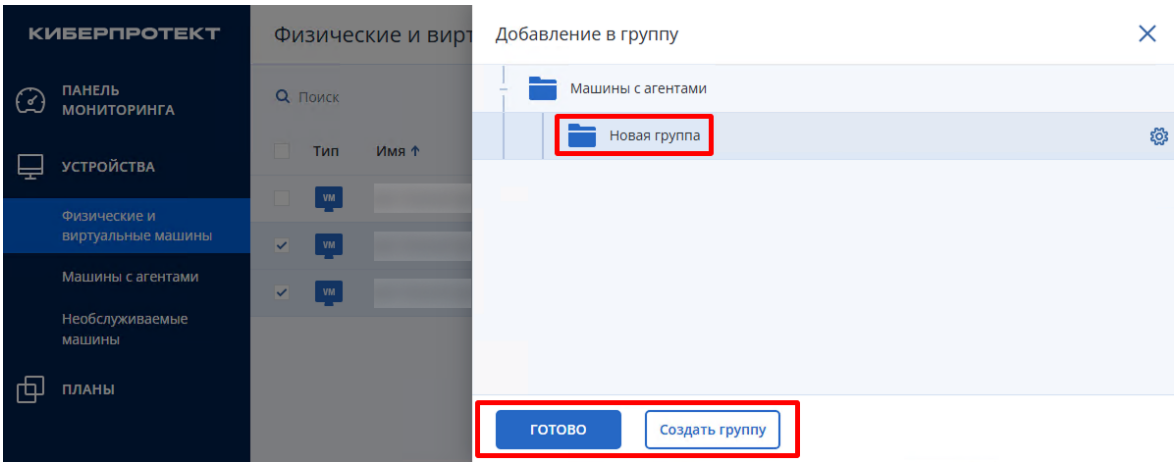
Способ 1 (через раздел Физические и виртуальные машины)

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Физические и виртуальные машины**.
2. Установите флажки напротив выбранных машин.
3. Справа на панели **Действия** щёлкните **Добавление в группу**.

© ООО Киберпротект, 2026



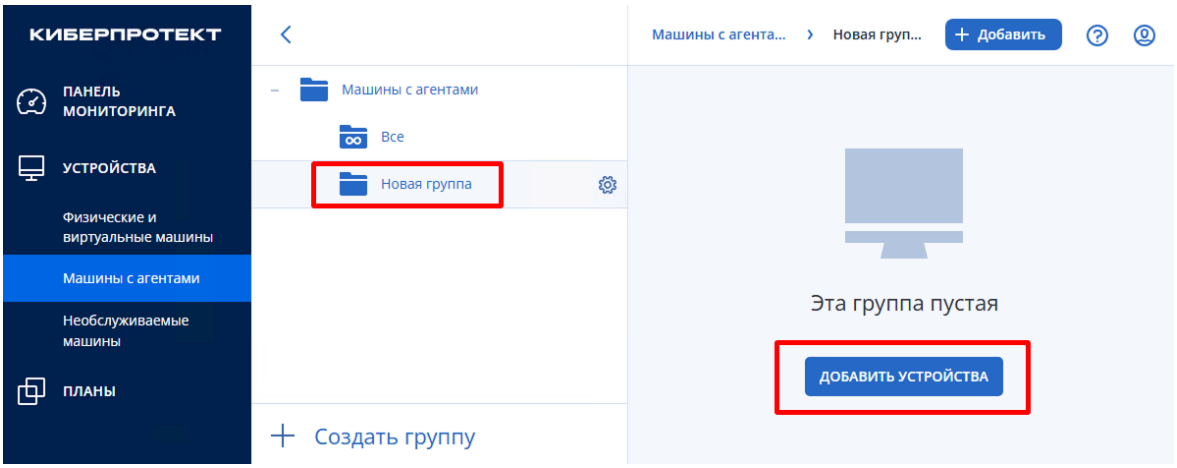
4. [Для добавления в существующую группу] Выберите группу и нажмите **Готово**.
5. [Для добавления в новую группу] Выберите группу, внутри которой будет создана новая группа, и нажмите **Создать группу**. Затем в окне **Создать новую группу** введите имя группы. При необходимости добавьте комментарий длиной до 512 символов.



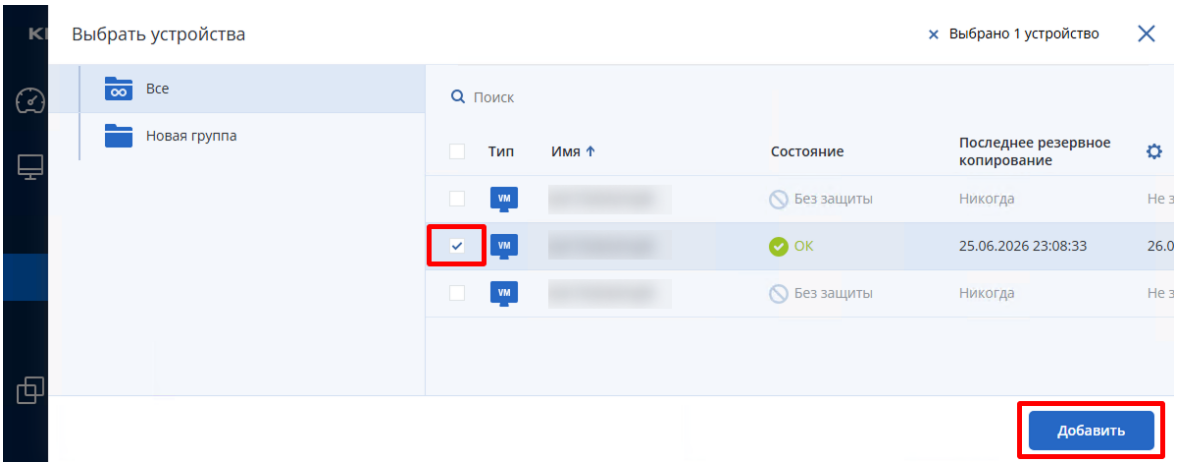
Способ 2 (через раздел Машины с агентами)

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Машины с агентами**.
2. Выберите группу.
3. Нажмите **Добавить устройства** (если в группе есть устройства, кнопка отображается на панели **Действия**, если в группе нет устройств – в области справа рядом с сообщением **Эта группа пустая**).

© ООО Киберпротект, 2026



4. В области **Выбрать устройства** установите флажки напротив выбранных машин и нажмите **Добавить**.



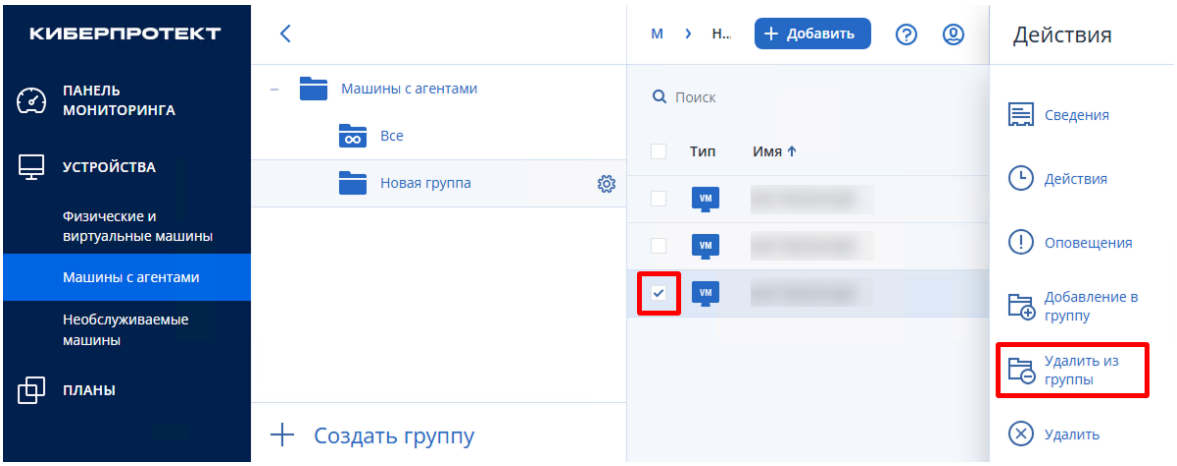
В результате выбранные устройства будут добавлены в статическую группу.

5.3.3 Удаление устройств из статических групп

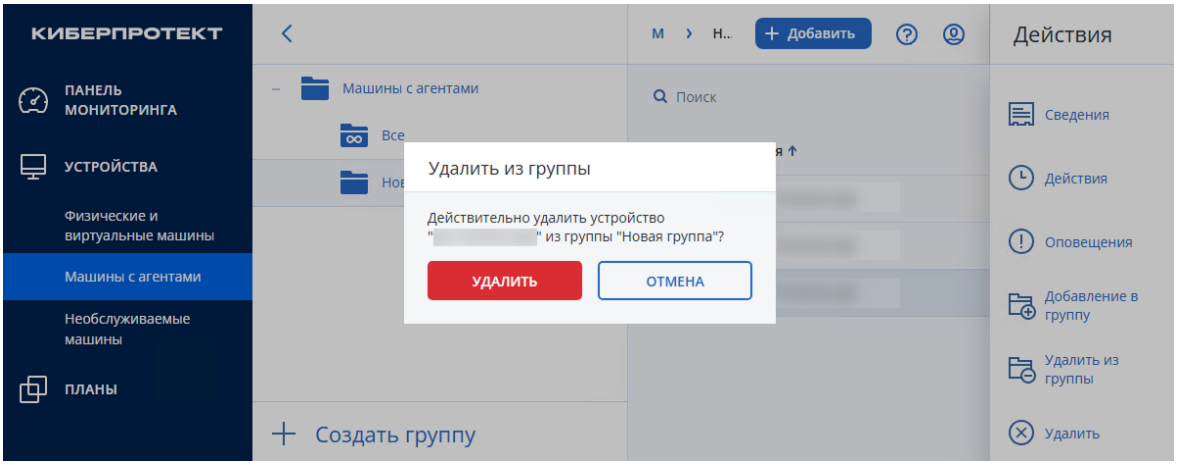
Для удаления устройств из статической группы выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Машины с агентами**.
2. Выберите группу, из которой нужно удалить устройства.
3. Установите флажки напротив выбранных машин.
4. Справа на панели **Действия** щёлкните **Удалить из группы**.

© ООО Киберпротект, 2026



5. В окне **Удалить из группы** подтвердите удаление, щёлкнув **Удалить**.



В результате выбранные устройства будут удалены из статической группы.

5.4 Операции с динамическими группами

С динамическими группами доступны следующие операции:

- создание (см. далее в этом разделе);
- применение плана защиты к группе (подробнее см. в разделе "Применение плана защиты к группе" (стр. 262));
- переименование (подробнее см. в разделе "Переименование группы" (стр. 262));
- удаление (подробнее см. в разделе "Удаление группы" (стр. 263)).

5.4.1 Создание динамических групп

Для создания динамической группы выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Машины с агентами**.
2. В поле поиска введите условие выбора устройств для добавления в группу и нажмите **Поиск**.

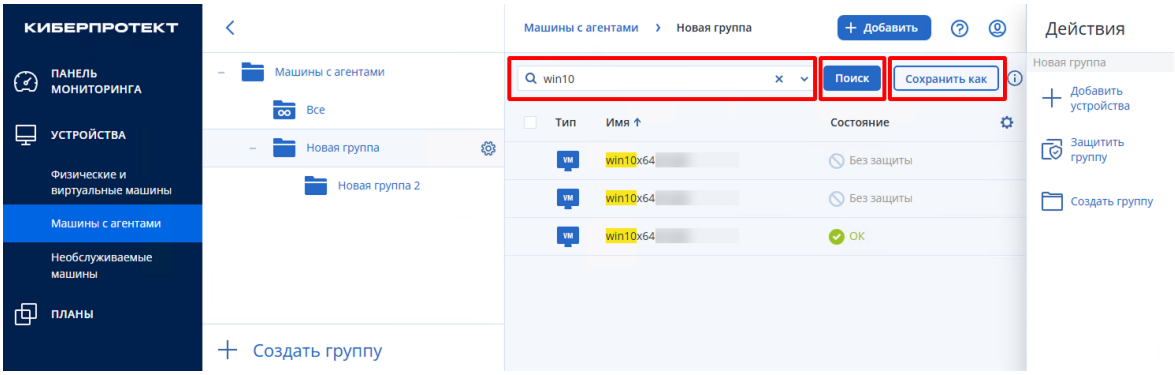
© ООО Киберпротект, 2026

Если не задать критерии поиска, по умолчанию будет выполнен поиск по имени. Критерии можно комбинировать с помощью операторов (они должны быть указаны в явном виде, например, name LIKE '%name%' AND comment = '').

Примечание

- Некоторые критерии поиска не поддерживаются при создании группы, см. таблицу в разделе "Условия поиска" ниже.
- Не поддерживается создание динамических групп на основе поиска во встроенной группе **Виртуальные устройства**.

3. Если результаты поиска удовлетворительны, нажмите **Сохранить как** (справа от поля поиска).



4. В окне **Создать новую группу** введите имя группы. При необходимости добавьте комментарий длиной до 512 символов.
5. Нажмите **OK**.

В результате динамическая группа будет создана, а устройства, соответствующие критериям поиска, будут добавлены в неё автоматически.

5.4.2 Условия поиска

Доступные условия поиска приведены в следующей таблице.

Критерий	Значение	Примеры поисковых запросов	Поддерживается для создания группы
name	• Имя хоста для физических машин • Имя для виртуальных машин • Имя базы данных • Адрес электронной почты для почтовых ящиков	name = 'en-00'	Да
comment	Комментарий для	comment = 'important machine'	Да

© ООО Киберпротект, 2026

	устройства. Значение по умолчанию: • Для физических машин с ОС Windows описание компьютера считывается в свойствах компьютера в Windows. • Пусто для других устройств. Чтобы просмотреть комментарий, в разделе **Устройства** выберите устройство и щелкните **Подробнее**, затем перейдите к разделу **Комментарий**. Чтобы добавить или изменить комментарий, щелкните **Добавить** или **Изменить**.	comment = '' (все машины без комментария)	
ip	IP-адрес (только для физических машин).	ip RANGE ('10.250.176.1','10.250.176.50')	Да Только при поиске с оператором RANGE
memorySize	Размер ОЗУ в мегабайтах (МиБ).	memorySize < 1024	Да
insideVm	Виртуальная машина с агентами в ней. Возможные значения: • true • false	insideVm = true	Да
tzOffset	Смещение часового пояса машины в минутах.	tzOffset = 120	Да
osName	Название операционной системы.	osName LIKE '%Windows 10%'	Да

© ООО Киберпротект, 2026

osType	Тип операционной системы. Возможные значения: • 'windows' • 'linux'	osType IN ('linux')	Да
osProductType	Тип продукта операционной системы. Возможные значения: • 'dc' Означает контроллер домена. • 'server' • 'workstation'	osProductType = 'server'	Да
osSp	Пакет обновления операционной системы.	osSp = 1	Да
osVersionMajor	Основной номер версии операционной системы.	osVersionMajor = 1	Да
osVersionMinor	Дополнительный номер версии операционной системы.	osVersionMinor = 1	Да
isOnline	Доступность машины. Возможные значения: • true • false	isOnline = true	Нет
tenant	Название отдела, которому принадлежит устройство.	tenant = 'Unit 1'	Да
tenantId	Идентификатор отдела, которому принадлежит устройство. Для получения идентификатора отдела напротив пункта **Устройства** выберите устройство и выберите пункт **Сведения** > **Все**	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	Да

© ООО Киберпротект, 2026

	свойства. Идентификатор отобразится в поле ownerId.		
state	Состояние устройства. Возможные значения: • 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'	state = 'backup'	Нет
status	Состояние ресурса. Возможные значения: • 'notProtected' • 'ok' • 'warning' • 'error' • 'critical'	status = 'ok'	Нет
protectedByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором. Для получения идентификатора плана нажмите **Планы** > **Резервное копирование**, выберите план,	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет

© ООО Киберпротект, 2026

	нажмите на диаграмму в колонке **Статус** и затем нажмите на статус. Будет создан новый поиск с идентификатором плана.		
okByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором и со статусом **OK**.	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
errorByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором и со статусом **Ошибка**.	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
warningByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором и со статусом **Предупреждение**.	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
runningByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором и со статусом **Выполняется**.	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
interactionByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором и со статусом **Требуется вмешательство**.	interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
ou	Машины, которые принадлежат к указанной организационной	ou IN ('RnD', 'Computers')	Да

© ООО Киберпротект, 2026

	единице Active Directory.		
id	Идентификатор устройства. Для получения идентификатора устройства напротив пункта **Устройства** выберите устройство и выберите пункт **Сведения** > **Все свойства**. Идентификатор отобразится в поле Id.	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Да Только при указании двух и более идентификаторов устройств
lastBackupTime	Дата и время последнего успешного создания резервной копии. Формат данных следующий:'ГГГГ-ММ-ДД ЧЧ:ММ'.	lastBackupTime > '2016-03-11' lastBackupTime <= '2016-03-11 00:15' lastBackupTime is null	Нет
lastBackupTryTime	Время последней попытки резервного копирования. Формат данных следующий:'ГГГГ-ММ-ДД ЧЧ:ММ'.	lastBackupTryTime >= '2016-03-11'	Нет
nextBackupTime	Время следующего резервного копирования. Формат данных следующий:'ГГГГ-ММ-ДД ЧЧ:ММ'.	nextBackupTime >= '2016-03-11'	Нет
agentVersion	Версия установленного агента защиты.	agentVersion LIKE '12.0.*'	Да
hostId	Внутренний идентификатор агента защиты. Для получения идентификатора агента	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Да

© ООО Киберпротект, 2026

	защиты напротив пункта **Устройства** выберите машину и щелкните **Сведения** > **Все свойства**. Используйте значение "id" свойства agent.		
resourceType	Тип ресурса. Возможные значения: • 'machine' • 'virtual_machine.vmwesx' • 'virtual_machine.mshyperv' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen'	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	Да
hasAsz	Агент защиты на физической машине с Зоной безопасности. Возможные значения: • true • false	hasAsz=true	Да
chassis	Тип корпуса машины. Возможные значения: • unknown • laptop • desktop • server • other	chassis="laptop"	Да
tagName	• Теги vSphere Tags виртуальных машин VMware. Отображаются только в разделе **УСТРОЙСТВА** -> **VMware**. • Теги виртуальных машин oVirt. Отображаются	tagName = 'Tag 1'	Да

© ООО Киберпротект, 2026

	только в разделе **УСТРОЙСТВА** -> **oVirt**.		

Примечание

Если пропустить значение для часов и минут, начальное время будет в формате ГГГГ-ММ-ДД 00:00, а конечное время – в формате ГГГГ-ММ-ДД 23:59:59. Например, lastBackupTime = 2020-02-20 означает, что в результаты поиска будут включены все резервные копии из интервала lastBackupTime >= 2020-02-20 00:00 и lastBackup time <= 2020-02-20 23:59:59

5.4.3 Операторы

Доступные операторы приведены в следующей таблице.

Оператор	Значение	Примеры
AND	Логический оператор конъюнкции.	name like 'en-00' AND tenant = 'Unit 1'
OR	Логический оператор дизъюнкции.	state = 'backup' OR state = 'interactionRequired'
NOT	Логический оператор отрицания.	NOT(osProductType = 'workstation')
LIKE 'шаблон подстановочного символа'	Этот оператор используется для проверки того, соответствует ли выражение шаблону подстановочного символа. В этом параметре не учитывается регистр. Могут быть использованы следующие операторы подстановочного знака: • "*" (звёздочка) или "%" (знак процента) могут заменять собой произвольное число символов, включая их отсутствие. • "_" (нижнее подчеркивание) может заменять собой один символ.	name LIKE 'en-00' name LIKE '*en-00' name LIKE '*en-00*' name LIKE 'en-00_'
IN (<значение1>,... <значениеN>)	Этот оператор используется для проверки того, соответствует ли выражение любому значению из указанного списка значений. В	osType IN ('windows', 'linux')

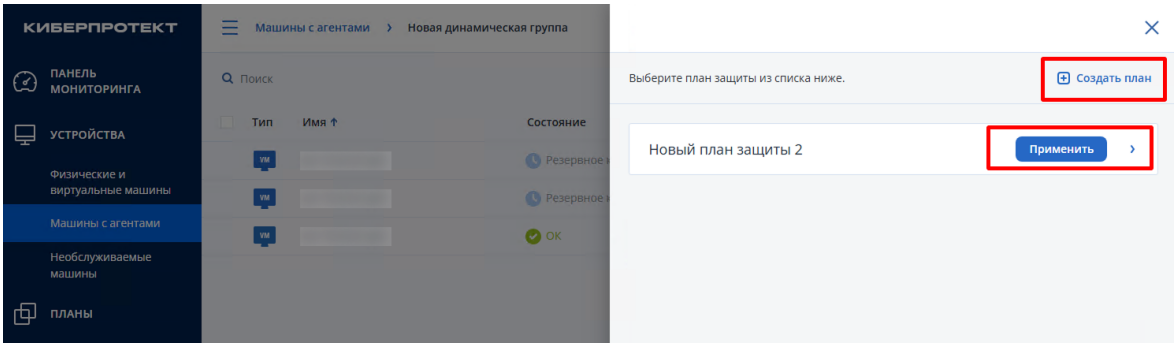
© ООО Киберпротект, 2026

	этом параметре учитывается регистр.	
RANGE(<starting_value>, <ending_value>)	Этот оператор используется для проверки того, находится ли значение в диапазоне значений (включительно).	ip RANGE ('10.250.176.1','10.250.176.50')

5.5 Применение плана защиты к группе

Для применения плана защиты к статической или динамической группе выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Машины с агентами**.
2. Выберите группу, к которой необходимо применить план защиты.
3. Справа на панели **Действия** щёлкните **Защитить группу**.
   В результате отобразится список планов защиты, которые можно применить к группе.
4. Выполните одно из следующих действий:
   - [Для применения существующего плана] Щёлкните **Применить**, при необходимости нажмите на иконку со стрелкой для просмотра информации о плане защиты.
   - [Для создания нового плана] Щёлкните **Создать план** и создайте новый план защиты, как описано в разделе "Резервное копирование" (стр. 264).



В результате план защиты будет применён к группе устройств.

5.6 Переименование группы

Для переименования статической или динамической группы выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Машины с агентами**.
2. Выберите группу и нажмите на значок шестерёнки рядом с её названием.
3. В выпадающем меню выберите **Переименовать**.
4. В окне **Переименовать группу** введите новое имя группы. При необходимости добавьте комментарий длиной до 512 символов.
5. Нажмите **OK**.

© ООО Киберпротект, 2026

В результате новое название группы будет отображено в списке групп.

5.7 Удаление группы

Для удаления статической или динамической группы выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Машины с агентами**.
2. Выберите группу и нажмите на значок шестерёнки рядом с её названием.
3. В выпадающем меню выберите **Удалить**.
4. В окне **Удалить группу** подтвердите удаление, нажав **Удалить**.

В результате группа будет удалена, а применённые к ней планы резервного копирования будут отозваны.

© ООО Киберпротект, 2026

6 Резервное копирование

В разделе описывается дисковое и файловое резервное копирование серверов и виртуальных машин. О защите данных разнообразных инфраструктур см. в разделе "Защита приложений, сервисов, баз данных" (стр. 475).

Для резервного копирования данных необходимо создать план их защиты. План защиты с включенным модулем **Резервное копирование** – это набор правил, определяющий способ защиты указанных данных на конкретной машине.

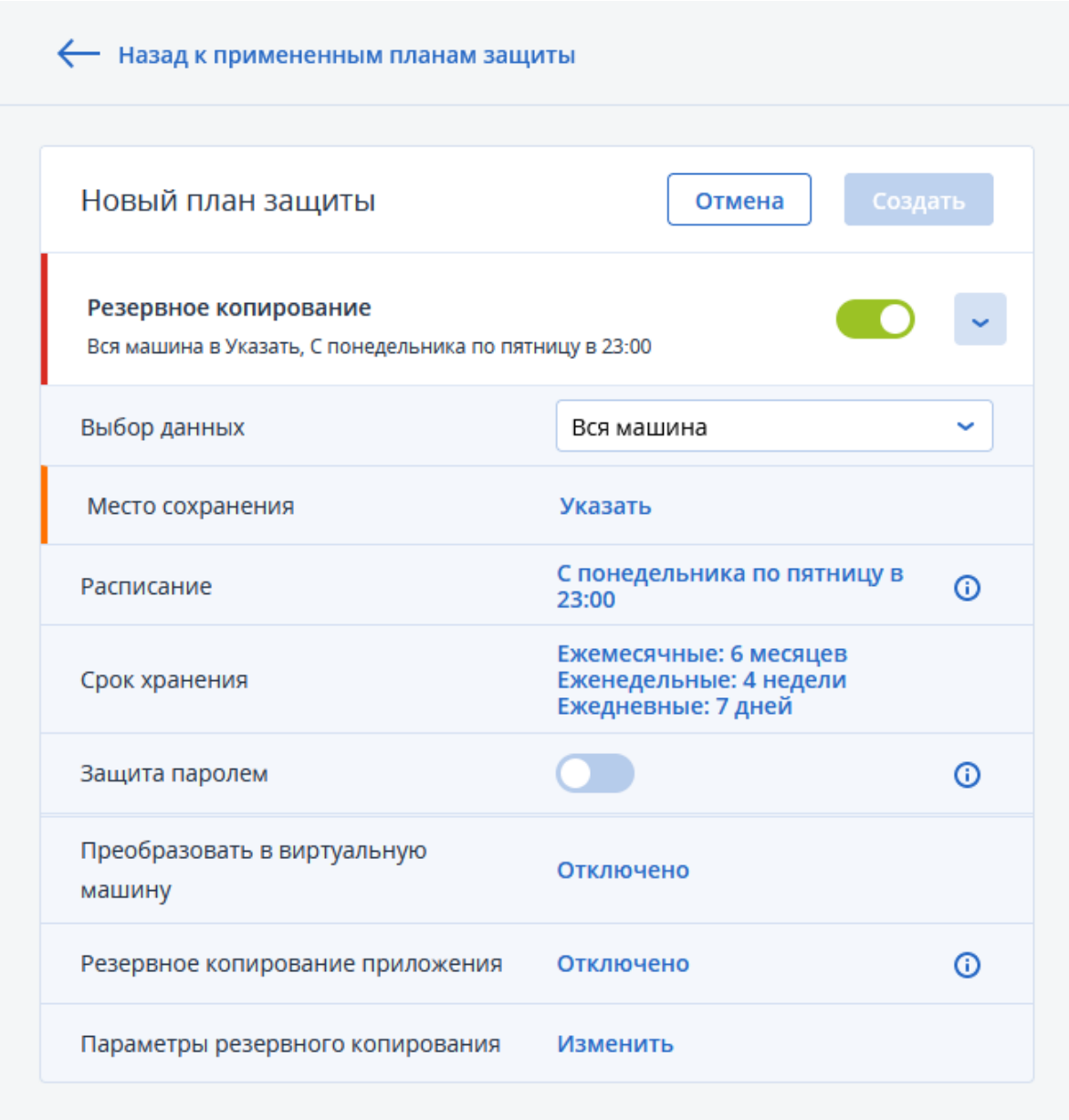
План защиты можно применить к нескольким машинам на этапе его создания или позже.

Примечание
При наличии только стандартных лицензий план защиты можно применить к одному или нескольким устройствам, выбранным вручную. Назначить план защиты для группы устройств невозможно.

Порядок создания первого плана защиты с включенным модулем "Резервное копирование"

1. Выберите машины, резервные копии которых необходимо создать.
2. Щелкните **Защитить**.
   В программе выводятся планы защиты, которые применены к машине. Если для машины еще не назначено ни одного плана, будет предложено применить план защиты по умолчанию. Можно задать настройки по собственному усмотрению и применить этот план или создать новый.

© ООО Киберпротект, 2026



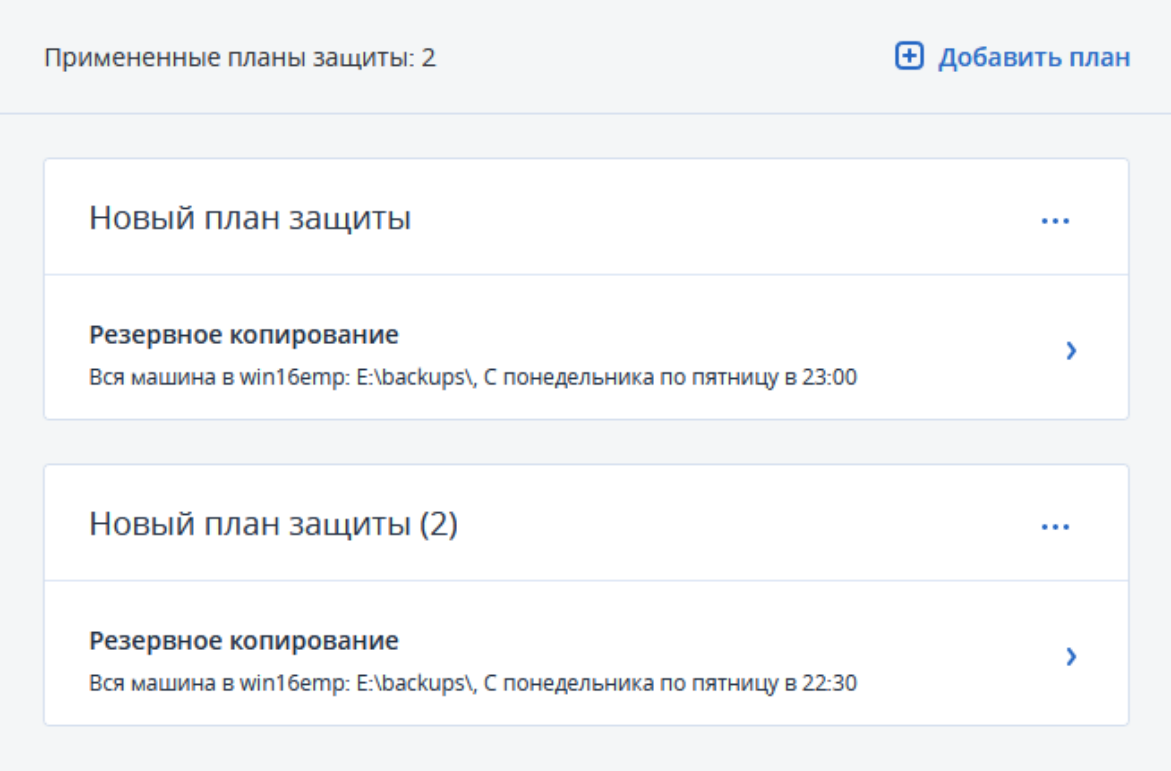
3. Чтобы создать новый план, щелкните **Создать план**. Включите модуль **Резервное копирование** и откатите настройки.
4. [Необязательно] Для изменения имени плана защиты щелкните имя по умолчанию.
5. [Необязательно] Чтобы изменить параметры модуля **Резервное копирование**, щелкните соответствующий раздел панели плана защиты.
6. [Необязательно] Чтобы изменить параметры резервного копирования, щелкните **Изменить** рядом с **Параметры резервного копирования**.
7. Нажмите кнопку **Создать**.

Порядок применения существующего плана резервного копирования

© ООО Киберпротект, 2026

1. Выберите машины, резервные копии которых необходимо создать.
2. Щелкните **Защитить**. Если к выбранным машинам уже применен стандартный план защиты, щелкните **Добавить план**.

   В программе отображаются ранее созданные планы защиты.



3. Выберите план защиты для применения.
4. Нажмите кнопку **Применить**.

6.1 Агент

Агент – это основная часть ПО Кибер Бэкап. Агенты управляют всеми процессами резервного копирования (подробнее см. "Развертывание Кибер Бэкап" (стр. 62)).

Агент устанавливается в ту программную среду, в которой находятся защищаемые объекты (см. "Установка агентов" (стр. 95)).

Основные функции агента реализуются при его работе в рамках одного или нескольких планов защиты (см. "План защиты и модули" (стр. 224)).

Агент Кибер Бэкап может выполнять резервное копирование данных в режиме многозадачности. Многозадачность агента заключается в его способности выполнять одновременное резервное копирование нескольких элементов в рамках различных планов защиты (см. "Одновременное резервное копирование" (стр. 312)).

6.2 Типы резервных копий

Кибер Бэкап работает со следующими типами резервных копий:

© ООО Киберпротект, 2026

- **Полная** – содержит все исходные данные и является самодостаточной. Для восстановления такой резервной копии не требуется доступ к каким-либо другим. Первая резервная копия, создаваемая планом защиты, всегда полная.
- **Инкрементная** – содержит изменения данных с момента создания последней резервной копии любого типа. Для восстановления инкрементной резервной копии нужна вся цепочка предыдущих копий, от которых она зависит, вплоть до исходной полной.
- **Дифференциальная** – содержит изменения данных с момента создания последней полной резервной копии. Для восстановления дифференциальной резервной копии нужна полная резервная копия, от которой она зависит.

При настройке схемы резервного копирования можно выбрать комбинацию используемых типов резервных копий (подробнее см. в разделе "Расписание" (стр. 287)).

6.3 Модуль резервного копирования: памятка

В таблице ниже вкратце описаны доступные параметры модуля "Резервное копирование". С ее помощью вы сможете легко создать план, который лучше всего отвечает вашим потребностям.

ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ	ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ Способы выбора	МЕСТО СОХРАНЕНИЯ	РАСПИСАНИЕ Схемы резервного копирования	ВРЕМЯ ХРАНЕНИЯ
Диски/тома (физические машины)	Напрямую Правила политики Фильтры файлов	Локальная папка Сетевая папка* Сервер SFTP* NFS* Кибер Инфраструктура или Кибер Хранилище* Зона безопасности* Управляемое хранилище* Ленточное устройство*	Всегда инкрементное* Всегда полное Еженедельно полное, ежедневно инкрементное Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS) Настраиваемый вариант (П-Д-И)	По возрасту резервной копии (одно правило на набор резервных копий) По количеству резервных копий По общему размеру резервных копий* Хранить бессрочно
Диски/тома (виртуальные машины)	Правила политики Фильтры файлов	Локальная папка Сетевая папка* Сервер SFTP*		

© ООО Киберпротект, 2026

		NFS* Кибер Инфраструктура или Кибер Хранилище* Управляемое хранилище* Ленточное устройство*		
Файлы (только физические машины)	Напрямую Правила политики Фильтры файлов	Локальная папка Сетевая папка* Сервер SFTP* NFS* Кибер Инфраструктура или Кибер Хранилище* Зона безопасности* Управляемое хранилище* Ленточное устройство	Всегда полное Еженедельно полное, ежедневно инкрементное Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS) Всегда инкрементное* Настраиваемый вариант (П-Д-И)	
Конфигурация ESXi	Напрямую	Локальная папка Сетевая папка* Сервер SFTP NFS*		
Базы данных SQL	Напрямую	Локальная папка Сетевая папка* Кибер Инфраструктура или Кибер Хранилище* Управляемое хранилище* Ленточное	Всегда полное Еженедельно полное, ежедневно инкрементное Настраиваемый вариант (П-И)	

© ООО Киберпротект, 2026

Базы данных Exchange	Напрямую	устройство		
Почтовые ящики Exchange	Напрямую	Локальная папка Сетевая папка* Кибер Инфраструктура или Кибер Хранилище* Управляемое хранилище*	Всегда инкрементное	
Базы данных Oracle	Команды до и после процедуры Резервное копирование сервера Oracle	Локальная папка Сетевая папка* Сервер SFTP* NFS* Кибер Инфраструктура или Кибер Хранилище* Зона безопасности* Управляемое хранилище* Ленточное устройство*	Всегда полное	
Базы данных PostgreSQL	Напрямую	Локальная папка Сетевая папка* Сервер SFTP NFS* Кибер Инфраструктура или Кибер Хранилище* Управляемое хранилище*	Всегда полное Еженедельно полное, ежедневно инкрементное Настраиваемый вариант (П-И)	По возрасту резервной копии (одно правило на набор резервных копий) По количеству резервных копий Хранить бессрочно
Данные CommuniGate Pro	Напрямую		Всегда полное Всегда инкрементное Еженедельно полное, ежедневно инкрементное	

© ООО Киберпротект, 2026

Данные VK WorkMail и VK WorkDisk	Напрямую	Локальная папка Сетевая папка* Сервер SFTP NFS* Кибер Инфраструктура или Кибер Хранилище* Управляемое хранилище* Ленточное устройство	Всегда полное Всегда инкрементное Еженедельно полное, ежедневно инкрементное	
Данные Kubernetes	Напрямую	Локальная папка Сетевая папка* Сервер SFTP NFS* Кибер Инфраструктура или Кибер Хранилище* Управляемое хранилище*	Всегда полное Всегда инкрементное Еженедельно полное, ежедневно инкрементное Настраиваемый вариант (П-И)	
Ред База Данных	Команды до и после процедуры	Локальная папка Сетевая папка* Сервер SFTP* NFS* Кибер Инфраструктура или Кибер Хранилище* Зона безопасности* Управляемое хранилище* Ленточное устройство*	Всегда полное	По возрасту резервной копии (одно правило на набор резервных копий) По количеству резервных копий По общему размеру резервных копий* Хранить бессрочно
Серверы SAP HANA	Команды до и после процедуры		Всегда полное Всегда инкрементное	

© ООО Киберпротект, 2026

* См. ограничения ниже.

6.3.1 Ограничения

6.3.1.1 Сетевая папка

Для резервного копирования в сетевые папки на машине с установленным агентом для Linux необходимо иметь установленные дополнительные пакеты Linux. Например, для CentOS 7 должны быть установлены следующие пакеты (в зависимости от места сохранения резервных копий):

МЕСТО СОХРАНЕНИЯ	НЕОБХОДИМЫЙ КОМПОНЕНТ LINUX
SMB NTLM	cifs-utils
SMB with Kerberos	cifs-utils keyutils
NFS	nfs-utils

Для более подробной информации об установке пакетов см. Пакеты Linux.

Примечание
Для разных операционных систем на основе Linux названия этих пакетов могут отличаться.

6.3.1.2 Сервер SFTP и ленточное устройство

- Эти хранилища не могут использоваться для резервных копий с поддержкой приложений.
- Схема резервного копирования **Всегда инкрементное** недоступна при выполнении резервного копирования в эти хранилища.
- Правило хранения **По общему размеру резервных копий** недоступно для этих хранилищ.

6.3.1.3 NFS

- Резервное копирование в общие папки NFS недоступно в Windows.
- Схема резервного копирования **Всегда инкрементное** для файлов (физических машин) недоступна при выполнении резервного копирования в общие папки NFS.

6.3.1.4 Кибер Инфраструктура или Кибер Хранилище

Для подробной информации см. раздел "О продуктах Кибер Инфраструктура и Кибер Хранилище" (стр. 286).

6.3.1.5 Зона безопасности

- Схема резервного копирования **Всегда инкрементное** для файлов (физических машин) недоступна при выполнении резервного копирования в зону безопасности.

© ООО Киберпротект, 2026

6.3.1.6 Управляемое хранилище

- Управляемое хранилище с активированной функцией дедупликации или защитой паролем не может быть выбрано в качестве места хранения:
  - если используется схема резервного копирования **Всегда инкрементное**,
  - если используется формат резервной копии **Версии 12**,
  - для резервных копий почтовых ящиков Exchange.
- Правило хранения **По общему размеру резервных копий** недоступно для управляемых хранилищ с активированной функцией дедупликации.

6.3.1.7 Всегда инкрементное

- Схема резервного копирования **Всегда инкрементное** недоступна при выполнении резервного копирования на SFTP-сервер или ленточное устройство.

6.3.1.8 По общему размеру резервных копий

- Правило хранения **По общему размеру резервных копий** недоступно:
  - Если используется схема резервного копирования **Всегда инкрементное**
  - При выполнении резервного копирования на SFTP-сервер, ленточное устройство или управляемое хранилище с активированной функцией дедупликации.

6.4 Выбор данных для резервного копирования

6.4.1 Выбор всей машины

Чтобы настроить резервное копирование всей машины, в области **Выбор данных** плана выберите **Вся машина**.

Для физической или виртуальной машины с агентом, установленным в гостевой ОС, резервная копия всей машины – это резервная копия всех ее несъёмных дисков. В таких сценариях в план необходимо добавлять объекты из раздела **Устройства** -> **Машины с агентами**. Задание по резервному копированию будет выполнено агентом в гостевой ОС.

Для виртуальной машины без агента резервная копия всей машины – это резервная копия всех ее несъёмных дисков, которые попадают в снимок ВМ, а также данных о конфигурации ВМ (ЦП, ОЗУ, дисках, сетевых адаптерах и прочем). В таких сценариях в план необходимо добавлять объекты из подраздела соответствующей системы виртуализации в разделе **Устройства**, например, **oVirt** или **OpenNebula**. Задание по резервному копированию будет выполнено агентом для данной системы виртуализации с помощью снимка ВМ на уровне гипервизора.

© ООО Киберпротект, 2026

Примечание
Одна и та же машина может отображаться в разных местах раздела **Устройства**, поскольку данные о ней поступают от разных агентов Кибер Бэкап. Например, если у виртуальной машины VMware есть агент в гостевой ОС и для неё же есть агент на уровне гипервизора, она будет отображаться в подразделах **Устройства** -> **Машины с агентами** и **Устройства** -> **VMware**. Резервное копирование первого из этих ресурсов будет выполнено агентом в гостевой ОС, второго – агентом на уровне гипервизора.

Примечание
Внешние диски, такие как USB-накопители или другие съемные носители, не включаются в резервную копию всей машины. Для них необходимо настроить резервное копирование дисков и томов (подробнее см. в разделе "Выбор дисков и томов" (стр. 275)).

6.4.2 Выбор файлов и папок

Резервное копирование на уровне файлов доступно для физических и виртуальных машин, если для них настроено резервное копирование с помощью агента, установленного в гостевой системе.

Для восстановления операционной системы резервной копии на уровне файлов недостаточно. Выберите этот способ, если необходимо сохранять только определенные данные (например, текущий проект). Это позволит уменьшить размер архива и тем самым сократить потребность в дисковом пространстве.

Есть два способа выбора файлов: напрямую на каждой машине или с помощью правил политики. Для каждого из этих способов выбор можно уточнить с помощью фильтров файлов.

6.4.2.1 Выбор напрямую на машине

1. В области **Выбор данных** выберите вариант **Файлы/папки**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **Напрямую**.
4. Для каждой машины, включенной в план защиты, выполните указанные ниже действия.
   a. Щелкните **Выбрать файлы и папки**.
   b. Щелкните **Локальная папка** или **Сетевая папка**.
      Общая папка должна быть доступна с выбранной машины.
   c. Перейдите к требуемым файлам и папкам или введите путь и нажмите кнопку со стрелкой.
      Если потребуется, укажите имя пользователя и пароль для доступа к общей папке.
      Резервное копирование папки с анонимным доступом не поддерживается.
   d. Выберите файлы и папки.
   e. Нажмите кнопку **Готово**.

© ООО Киберпротект, 2026

6.4.2.2 Использование правил политики

1. В области **Элементы для резервного копирования** выберите вариант **Файлы/папки**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **С использованием правил политики**.
4. Выберите готовые правила, введите собственные или используйте оба варианта.

   Правила политики будут применены ко всем машинам, которые входят в план защиты. Если на машине при запуске резервного копирования отсутствуют объекты, соответствующие хотя бы одному правилу, копирование завершится сбоем.
5. Нажмите кнопку **Готово**.

Правила выбора для Windows

- Полный путь к файлу или папке, например **D:\Work\Text.doc** или **C:\Windows**.
- Шаблоны
  - [All Files] позволяет выбрать все файлы на всех томах машины.
  - [All Profiles Folder] позволяет выбрать папку, в которой хранятся все профили пользователей (обычно это **C:\Users** или **C:\Documents and Settings**).
- Переменные среды:
  - %ALLUSERSPROFILE% позволяет выбрать папку, в которой хранятся общие данные всех профилей пользователей (обычно это **C:\ProgramData** или **C:\Documents and Settings\All Users**).
  - %PROGRAMFILES% позволяет выбрать папку с файлами программ (например, **C:\Program Files**).
  - %WINDIR% позволяет выбрать папку, в которой находится система Windows (например, **C:\Windows**).

  Можно использовать другие переменные среды или их сочетание с текстом. Например, чтобы выбрать папку Java в папке Program Files, введите **%PROGRAMFILES%\Java**.

Правила выбора для Linux

- Полный путь к файлу или каталогу. Например, чтобы создать резервную копию файла **file.txt** в томе **/dev/hda3**, подключенном к каталогу **/home/usr/docs**, введите **/dev/hda3/file.txt** или **/home/usr/docs/file.txt**.
  - /home позволяет выбрать домашний каталог обычных пользователей.
  - /root позволяет выбрать домашний каталог привилегированного пользователя.
  - /usr позволяет выбрать каталог для всех пользовательских программ.
  - /etc позволяет выбрать каталог с конфигурационными файлами системы.
- Шаблоны

© ООО Киберпротект, 2026

- [All Files] позволяет выбрать все файлы во всех каталогах машины.
- [All Profiles Folder] позволяет выбрать каталог **/home**. В этой папке по умолчанию размещены все профили пользователя.

6.4.3 Выбор дисков и томов

Резервная копия диска содержит копию диска или тома в запакованном виде. Из такой копии можно восстановить отдельные диски, тома или файлы. Резервная копия всей машины — это резервная копия со всеми ее несъемными дисками.

Есть два способа выбора дисков/томов: напрямую на каждой машине или с помощью правил политики. Исключить файлы из резервной копии можно с помощью фильтров файлов.

6.4.3.1 Выбор напрямую на машине

Возможность выбора дисков и томов напрямую доступна только для физических машин. Чтобы включить прямой выбор дисков и томов на виртуальной машине, необходимо установить агент Киберзащиты в ее гостевой операционной системе.

1. В области **Выбор данных** выберите вариант **Диски/тома**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **Напрямую**.
4. Для каждой из машин, которая включена в план защиты, установите флажки рядом с дисками и томами, которые требуется скопировать.
5. Нажмите кнопку **Готово**.

6.4.3.2 Использование правил политики

1. В области **Выбор данных** выберите вариант **Диски/тома**.
2. Нажмите **Элементы для резервного копирования**.
3. Выберите готовые правила, введите собственные или используйте оба варианта.

   Правила политики будут применены ко всем машинам, которые входят в план защиты. Если на машине при запуске резервного копирования отсутствуют объекты, соответствующие хотя бы одному правилу, копирование завершится сбоем.
4. Нажмите кнопку **Ок**.

Правила для Windows и Linux

- [Все тома] позволяет выбрать все тома машин с Windows и все подключенные тома машин с Linux.
- [Фиксированные тома (физические машины)] позволяет выбрать все тома физических машин, кроме съемных носителей. К фиксированным томам относятся тома на устройствах SCSI, ATAPI, ATA, SSA, SAS и SATA, а также RAID-массивы.

© ООО Киберпротект, 2026

- [BOOT+SYSTEM] выбирает системный том и загрузочный том. Это сочетание соответствует минимальному набору данных, который необходим для восстановления операционной системы из резервной копии.
- [Disk 1] позволяет выбрать первый диск машины, включая все тома на нем. Чтобы выбрать другой диск, введите соответствующий номер.

Примечание
Для резервного копирования виртуальным устройством дисков и томов ВМ можно использовать только правило политики [Disk 1].

Правила только для Windows

- Буква диска (например, **C:**) обозначает том с указанной буквой.
- [BOOT+SYSTEM DISK] выбирает все тома диска, на котором расположены загрузочный и системный том. Если загрузочный том и системный том располагаются на разных дисках, ничего не будет выбрано. Это правило действует только для физических машин.

Правила только для Linux

- /dev/hda1 обозначает первый том на первом жестком диске IDE.
- /dev/sda1 обозначает первый том на первом жестком диске SCSI.
- /dev/md1 обозначает первый жесткий диск в программном RAID-массиве.

Чтобы выбрать другие базовые тома, введите /dev/xdyN, где:

- x обозначает тип диска;
- y обозначает номер диска (a – первый, b – второй и т. д.);
- N обозначает номер тома.

Чтобы выбрать логический том, укажите путь к нему, отображаемый после выполнения команды ls /dev/mapper в учетной записи привилегированного пользователя. Пример:

```
[root@localhost ~]# ls /dev/mapper/
control vg_1-lv1 vg_1-lv2
```

В выходных данных отображаются два логических тома, **lv1** и **lv2**, принадлежащие к группе томов **vg_1**. Для создания резервных копий этих томов введите:

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

6.4.3.3 Что содержится в резервных копиях томов или дисков

Резервная копия диска или тома хранит **файловую систему** целиком и включает всю информацию, необходимую для загрузки операционной системы. Из таких резервный копий можно восстанавливать целые диски или тома, а также отдельные папки и файлы.

© ООО Киберпротект, 2026

Если включен параметр резервного копирования **посекторное копирование (бесформатный режим)**, то в резервной копии диска сохраняются все сектора диска. Посекторное резервное копирование может использоваться для резервного копирования дисков с неопознанными или неподдерживаемыми файловыми системами и другими нестандартными форматами данных.

Windows

Резервная копия тома хранит все файлы и папки выбранного тома независимо от их атрибутов (включая скрытые и системные файлы), загрузочную запись, таблицу размещения файлов (FAT), если она есть, а также корневую и нулевую дорожки жесткого диска с основной загрузочной записью (MBR).

Резервная копия диска сохраняет все тома выбранного диска (включая скрытые разделы, например специальные скрытые разделы, предназначенные для хранения ПО поставщика) и нулевую дорожку жесткого диска с основной загрузочной записью (MBR).

Следующие элементы *не входят* в резервную копию диска или тома (а также в резервную копию на уровне файлов):

- Файл подкачки (pagefile.sys) и файл, в котором сохраняется содержимое ОЗУ, когда машина переходит в режим гибернации (hiberfil.sys). После восстановления эти файлы будут созданы повторно в соответствующем месте с нулевым размером.
- При выполнении резервного копирования в операционной системе (а не на загрузочном носителе или при резервном копировании виртуальных машин на уровне гипервизора):
  - Теневое хранилище Windows. Путь к нему определяется значением реестра **VSS Default Provider** в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup. Это означает, что в ОС Windows резервное копирование Windows Restore Points не производится.
  - Файлы и папки, указанные в ключе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot, если включен параметр резервного копирования **Volume Shadow Copy Service (VSS)** (см. "Служба теневого копирования томов (VSS)" (стр. 379)).

Linux

Резервная копия тома хранит все файлы и папки выбранного тома независимо от их атрибутов, загрузочную запись и суперблок файловой системы.

Резервное копирование диска сохраняет все тома диска, а также нулевую дорожку с основной загрузочной записью.

6.4.4 Выбор конфигурации ESXi

Резервная копия конфигурации хоста ESXi позволяет восстановить хост ESXi на «голое железо». Восстановление выполняется с загрузочного носителя.

© ООО Киберпротект, 2026

Виртуальные машины, которые выполняются на данном хосте, не включены в резервную копию. Создать для них резервную копию и восстановить их можно отдельно.

В резервную копию конфигурации хоста входят следующие элементы:

- Разделы загрузчика и активного загрузочного блока данного хоста.
- Состояние хоста (конфигурация виртуальной сети и хранилища данных, ключи SSL, сетевые настройки сервера и информация локального пользователя).
- Расширения и исправления, установленные или поэтапно устанавливаемые на хосте.
- Файлы журнала.

Предварительные требования

- В разделе **Профиль безопасности** конфигурации хоста ESXi должен быть включен SSH.
- Необходимо знать пароль учетной записи «root» хоста ESXi.

Ограничения

- Резервное копирование конфигурации ESXi не поддерживается для VMware vSphere 7.0 и новее.
- Для корректной загрузки восстановленной конфигурации ESXi рекомендуется отключить параметр **Безопасная загрузка** (Secure boot) в настройках хоста.

Порядок выбора конфигурации ESXi

1. Щелкните **Устройства** > **Физические и виртуальные машины**, после чего выберите хосты ESXi, для которых необходимо создать резервную копию.
2. Нажмите кнопку **Резервное копирование**.
3. В поле **Выбор данных**, выберите **Конфигурация ESXi**.
4. В поле **Пароль пользователя root ESXi** укажите пароль для учетной записи root на каждом выбранном хосте или примените один пароль ко всем хостам.

6.5 Выбор места сохранения

Для выбора хранилища резервных копий

1. Нажмите **Место сохранения резервной копии**.
2. Выполните одно из следующих действий:
   - Выберите использованное ранее или предопределенное хранилище резервных копий.
   - Нажмите **Добавить хранилище** и затем укажите новое хранилище резервных копий.

6.5.1 Поддерживаемые расположения

Виды поддерживаемых хранилищ резервных копий приведены в таблицах ниже.

© ООО Киберпротект, 2026

Вид хранилища	СУБД			
	PostgreSQL	Microsoft SQL Server	MySQL	БД Microsoft Exchange Server
Локальная папка	+	+	+	+
Сетевая папка	+	+	+	+
Папка NFS	+	-	-	-
SFTP	+	-	-	-
Узел хранения	+	+	-	+
Кибер Инфраструктура или Кибер Хранилище	+	+	+	+
Зона безопасности	-	-	-	-
Ленты	+	+	-	+

Вид хранилища	Виртуальные машины, защищённые в безагентном режиме								
	VMware	Hyper-V	oVirt, zVirt, HOSTVM, ROSA Virtualization	OpenStack, VK Cloud	OpenNebula, ПК СВ "Брест"	ECP VeiL, Space VM	Basis Dynamix Enterprise	Proxmox Virtual Environment	Кибер Инфраструктура
Локальная папка	+	+	+	-	-	-	-	-	-
Сетевая папка	+	+	+	+	+	+	+	+	+
Папка NFS	+	-	+	+	+	+	+	+	+
SFTP	+	+	+	+	+	+	+	+	+
Узел хранения	+	+	+	+	+	+	+	+	+
Кибер Инфраструктура или Кибер Хранилище	+	+	+	+	+	+	+	+	+
Зона безопаснос	-	-	-	-	-	-	-	-	-

© ООО Киберпротект, 2026

ти									
Ленты	+	+	+	+	+	+	+	+	+

Вид хранилища	ESXi-конфигурация	Физические и виртуальные машины с установленным агентом		Почтовые ящики				Kubernetes
		Windows	Linux	VK WorkMail	CommuniGate Pro	Mailion	Почтовые ящики Microsoft Exchange Server	
Локальная папка	+	+	+	+	+	+	+	+
Сетевая папка	+	+	+	+	+	+	+	+
Папка NFS	+	-	+	+	+	+	-	+
SFTP	+	+	+	+	+	+	-	+
Узел хранения	-	+	+	+	+	+	+	+
Кибер Инфраструктура или Кибер Хранилище	-	+	+	+	+	+	+	+
Зона безопасности	+	+	+	-	-	-	-	-
Ленты	-	+	+	+	-	-	-	+

- **Локальная папка**

  Если выбрана одна машина, перейдите на ней в соответствующую папку или введите путь.

  Если выбрано несколько машин (или их статическая или динамическая группа), введите путь к папке. Резервные копии будут сохраняться в этой папке на каждой из выбранных физических машин либо на машине, на которой установлен агент для виртуальных машин. Если папка не существует, она будет создана.
- **Сетевая папка**

  Это папка, общий доступ к которой предоставлен посредством SMB/CIFS/DFS.

© ООО Киберпротект, 2026

Перейдите к требуемой общей папке или введите путь к ней в следующем формате:

- Для общих папок SMB/CIFS: \\<имя_хоста>\<путь>\ или smb://<имя_хоста>/<путь>/
- Для папок DFS: \\<полное доменное имя DNS>\<корневой каталог DFS>\<путь>

  Например, \\example.company.com\shared\files

После этого нажмите кнопку со стрелкой. Если потребуется, укажите имя пользователя и пароль для доступа к общей папке. Эти учетные данные можно изменить в любое время. Для этого щелкните значок ключа рядом с именем папки.

Резервное копирование в папку с анонимным доступом не поддерживается.

Примечание

Перед выполнением резервного копирования в сетевую папку убедитесь, что на компьютере с агентом Linux установлены необходимые пакеты. Подробнее см. Модуль резервного копирования: памятка > Ограничения.

- **Папка NFS** (доступна для машин под управлением Linux)

  Перейдите к требуемой папке NFS или введите путь к ней в следующем формате:

  nfs://<имя хоста>/<экспортированная папка>:/<подпапка>

  После этого нажмите кнопку со стрелкой.

  Невозможно выполнить резервное копирование в папку NFS, защищенную паролем.
- **SFTP**

  Введите имя или IP-адрес сервера SFTP Поддерживаются следующие форматы:

  sftp://<сервер>
  sftp://<сервер>/<папка>

  После введения имя пользователя и пароля вы можете просматривать папки на сервере.

  В любом формате также можно указать порт, имя пользователя и пароль:

  sftp://<сервер>:<порт>/<папка>
  sftp://<имя пользователя>@<сервер>:<порт>/<папка>
  sftp://<имя пользователя>:<пароль>@<сервер>:<порт>/<папка>

  Если номер порта не указан, используется порт 22.

  Пользователи, для которых настроен доступ к SFTP без пароля, могут выполнять резервное копирование на SFTP.

  Резервное копирование на FTP-сервер не поддерживается.
- **Узел хранения**

  Узел хранения – это сервер, предназначенный для оптимизации использования различных ресурсов (таких как объем корпоративного хранилища, пропускная способность сети или загрузка процессоров производственных серверов), требуемых для защиты корпоративных данных. Это достигается путем организации хранилищ и управления хранилищами, выделенными для корпоративных резервных копий (управляемыми хранилищами).

  Выберите предварительно созданное хранилище или создайте новое, нажав **Добавить хранилище** > **Узел хранения**. Информацию о настройках см. в разделе «Добавление управляемого хранилища».

© ООО Киберпротект, 2026

Если потребуется, укажите имя пользователя и пароль для доступа к узлу хранения. Члены указанных ниже групп Windows на машине с установленным узлом хранения имеют доступ ко всем управляемым хранилищам на узле хранения:

- **Администраторы**
- **Киберпротект ASN Remote Users**

  Эта группа создается автоматически при установке узла хранения. По умолчанию эта группа пустая. Можно добавить пользователей в эту группу вручную.

- **Кибер Инфраструктура / Кибер Хранилище**

  Кибер Инфраструктура и Кибер Хранилище – это высоконадежные программно-определяемые хранилища данных с избыточностью данных и автоматическим самовосстановлением. Эти хранилища данных можно настроить как шлюз для хранения резервных копий в Yandex Cloud или в одном из ряда решений для хранения данных, совместимых с S3 или Swift. В хранилищах также может использоваться сервер NFS. Дополнительную информацию см. в разделе "О продуктах Кибер Инфраструктура и Кибер Хранилище" (стр. 286).

- **Зона безопасности** (доступно, если этот раздел присутствует на каждой из выбранных машин)

  Зона безопасности – это безопасный раздел на диске машины, для которой создана резервная копия. Перед настройкой резервной копии этот раздел необходимо создать вручную. Информацию о создании раздела Зона безопасности, его преимуществах и ограничениях см. в разделе Информация о разделе Зона безопасности.

- **Лента**

  Если ленточное устройство подключено к машине, для которой создается резервная копия, или к узлу хранения, в списке хранилищ указывается заданный по умолчанию пул лент. Этот пул создается автоматически.

  Выберите заданный по умолчанию пул или создайте новый, нажав **Добавить хранилище** > **Лента**. Информацию о настройках пула см. в «Создание пула».

  Для хранения данных на лентах используйте подходящий тип ленты. Подробнее о типах лент в разделе "Типы и свойства лент" (стр. 766).

- **Определяется сценарием** (доступно для машин под управлением Windows)

  Резервную копию каждой машины можно хранить в папке, определенной сценарием. Поддерживаются сценарии на языках JScript, VBScript или Python.

  Примечание
  Для использования сценариев Python на машины с агентами необходимо вручную установить Python версии 3.5 или новее.

  При развертывании плана защиты на каждой машине будет выполнен заданный сценарий. Выходными данными сценария для каждой машины является путь к локальной или сетевой папке. Если папка не существует, она будет создана. Действует следующее ограничение: сценарии на языке Python не могут создавать папки в сетевых папках. На вкладке **Хранилища резервных копий** каждая папка показана в виде отдельного хранилища резервных копий.

© ООО Киберпротект, 2026

В поле **Тип сценария** выберите тип сценария (**JScript**, **VBScript** или **Python**), а затем импортируйте или скопируйте и вставьте сценарий. Для сетевых папок укажите учетные данные доступа с правами чтения/записи

Например, следующий сценарий JScript выводит расположение хранилища резервных копий для машины в формате \\bkpsrv\<имя_машины>:

```
WScript.echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
```

В результате резервные копии каждой машины будут сохранены в папке с тем же именем на сервере **bkpsrv**.

6.5.2 О разделе Зона безопасности

Зона безопасности – это безопасный раздел на диске машины, для которой была создана резервная копия. В нем могут храниться резервные копии дисков или файлов этой машины.

Если на диске произойдет физический сбой, резервные копии в разделе Зона безопасности могут быть утрачены. Поэтому Зона безопасности не должна быть единственным хранилищем резервных копий. В корпоративных средах Зону безопасности можно представить как вспомогательное хранилище резервных копий, когда обычное хранилище временно недоступно или подключено через медленный или загруженный канал.

6.5.2.1 Почему нужно использовать раздел Зона безопасности?

Зона безопасности:

- Обеспечивает восстановление диска на тот же диск, на котором находится резервная копия диска.
- Обеспечивает экономный и удобный метод защиты данных при неправильной работе программного обеспечения или ошибках, вызванных человеческим фактором.
- Устраняет необходимость в отдельном носителе или сетевом подключении для резервного копирования или восстановления данных.
- Может служить основным местом сохранения при использовании репликации резервных копий.

6.5.2.2 Ограничения

- Зона безопасности – это раздел на базовом диске. Зону безопасности невозможно организовать на динамическом диске или создать как логический том (управляемый LVM).
- Файловая система раздела Зона безопасности имеет формат FAT32. Поскольку в FAT32 действует ограничение 4 ГБ на размер файлов, то резервные копии большего размера разбиваются на части при сохранении в Зону безопасности. Это не влияет на процедуру резервного копирования и его скорость.

© ООО Киберпротект, 2026

- Зона безопасности не поддерживает формат одного файла резервной копии[1]. При изменении места сохранения на Зону безопасности в плане защиты, который имеет схему резервного копирования **Всегда инкрементное**, данная схема заменяется схемой **Еженедельно полное, ежедневно инкрементное**.

6.5.2.3 Преобразование диска в результате создания раздела Зона безопасности

- Зона безопасности всегда создается в конце жесткого диска.
- Если в конце диска нераспределенного пространства нет или недостаточно, но существует нераспределенное пространство между томами, то эти тома будут перемещены, чтобы добавить больше нераспределенного пространства в конец диска.
- Если все незанятое пространство собрано, но его не хватает, то программа заберет свободное пространство из томов по выбору, пропорционально уменьшив их размер.
- Тем не менее на томе должно быть свободное пространство для работы операционной системы и приложений, например для создания временных файлов. Программа не будет уменьшать размер тома, на котором свободное пространство меньше или равно 25 % общего объема тома. Только если все тома на диске будут иметь 25 % или меньше свободного пространства, программа продолжит пропорциональное уменьшение томов.

Как следует из приведенных выше соображений, не рекомендуется указывать максимальный возможный размер раздела Зона безопасности. Следствием этого будет отсутствие свободного пространства на любом томе, что может привести к нестабильной работе операционной системы или приложений либо даже к невозможности их запуска.

Внимание
Для перемещения или изменения размера тома, с которого загружена операционная система, потребуется перезагрузка.

6.5.2.4 Порядок создания Зоны безопасности

1. Выберите машину, на которой необходимо создать Зону безопасности.
2. Щелкните **Сведения** > **Создать Зону безопасности**.
3. В разделе **Диск Зоны безопасности** щелкните **Выбрать**, выберите жесткий диск (если их несколько), на котором нужно создать Зону безопасности.

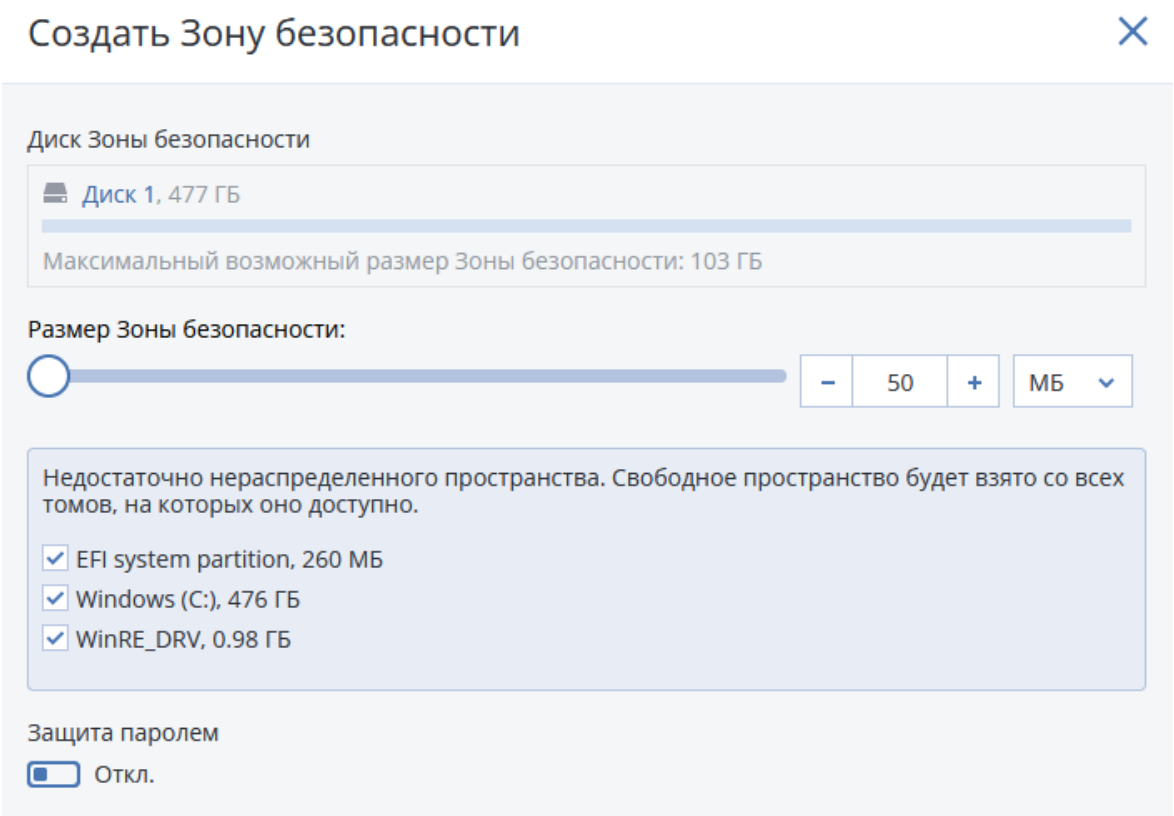
   Программа рассчитает максимальный возможный размер Зоны безопасности.

[1]Новый формат резервных копий, в котором начальная полная и последующие инкрементные резервные копии сохраняются в одном TIB-файле вместо цепочки файлов. Преимуществом этого формата является скорость инкрементного метода; при этом он лишен основного недостатка – сложностей, связанных с удалением устаревших копий. Программа помечает блоки, которые используются такими копиями, как свободные, и записывает на их место новые резервные копии. В результате очистка выполняется очень быстро и с минимальным потреблением ресурсов. Формат резервной копии в виде одного файла недоступен при резервном копировании в хранилища, которые не поддерживают операции произвольного чтения и записи, например, на сервера SFTP.

© ООО Киберпротект, 2026

4. Введите размер Зоны безопасности или перетащите ползунок, чтобы выбрать любой размер в диапазоне между минимальным и максимальным.

   Минимальный размер составляет около 50 МБ в зависимости от геометрии жесткого диска. Максимальный размер складывается из размера нераспределенного пространства и суммарного свободного пространства всех томов диска.
5. Если всего нераспределенного пространства не хватает для указанного размера, то программа заберет свободное пространство от существующих томов. По умолчанию выбраны все тома. Чтобы исключить некоторые тома, щелкните **Выбрать тома**. В противном случае пропустите этот шаг.



6. [Необязательно] Включите переключатель **Защита паролем** и укажите пароль.

   Этот пароль потребуется для доступа к резервным копиям, расположенным в Зоне безопасности. Для резервного копирования в раздел Зона безопасности пароль не требуется, за исключением случая, когда резервное копирование выполняется в системе, загруженной с загрузочного носителя.
7. Нажмите кнопку **Создать**.

   Программа покажет предполагаемую структуру разделов. Нажмите кнопку **OK**.
8. Подождите, пока программа создаст Зону безопасности.

После этого Зону безопасности можно выбрать в разделе **Место сохранения** при создании плана защиты.

© ООО Киберпротект, 2026

6.5.2.5 Порядок удаления Зоны безопасности

1. Выберите машину с разделом Зона безопасности.
2. Нажмите **Сведения**.
3. Щелкните значок шестерни рядом с разделом **Зона безопасности**, затем щелкните **Удалить**.
4. [Дополнительно] Укажите тома, на которые будет добавлено пространство, которое занимала Зона безопасности. По умолчанию выбраны все тома.

   Пространство будет распределено между выбранными томами поровну. Если ни один том не выбран, освобожденное пространство становится нераспределенным.

   Для изменения размера тома, с которого загружена операционная система, потребуется перезагрузка.
5. Щелкните **Удалить**.

В результате Зона безопасности будет удалена вместе со всеми содержащимися в ней резервными копиями.

6.5.3 О продуктах Кибер Инфраструктура и Кибер Хранилище

Кибер Бэкап поддерживает интеграцию с продуктами Кибер Инфраструктура (версии 6.5.2 и новее) и Кибер Хранилище (версии 6.7 и новее).

6.5.3.1 Развертывание

Чтобы использовать продукт Кибер Инфраструктура или Кибер Хранилище, разверните его локально на вычислительном оборудовании без виртуализации. Чтобы воспользоваться всеми преимуществами данного продукта, необходимо по крайней мере пять физических серверов. Если нужна только функциональность шлюза резервного копирования (Backup Gateway), можно использовать один физический или виртуальный сервер либо настроить кластер шлюзов с максимально большим количеством серверов.

Убедитесь, что настройки времени синхронизированы между сервером управления Кибер Бэкапа и Кибер Инфраструктурой или Кибер Хранилищем. Настройки времени для Кибер Инфраструктуры или Кибер Хранилища можно задать при развертывании. Синхронизация времени по протоколу NTP включена по умолчанию.

Можно развернуть несколько экземпляров Кибер Инфраструктуры или Кибер Хранилища и зарегистрировать их на одном сервере управления.

6.5.3.2 Регистрация

Регистрация сервера управления Кибер Бэкап выполняется в веб-интерфейсе Кибер Инфраструктуры или Кибер Хранилища. Кибер Инфраструктуру или Кибер Хранилище могут зарегистрировать только администраторы организации и только в данной организации. После регистрации хранилище становится доступным всем отделам организации. Его можно добавить в качестве хранилища резервных копий в любой отдел или организацию.

© ООО Киберпротект, 2026

Обратная операция (отмена регистрации) выполняется в интерфейсе Кибер Бэкап. Щелкните **Настройки** > **Узлы хранения**, щелкните требуемый экземпляр Кибер Инфраструктуры или Кибер Хранилища, а затем щелкните **Удалить**.

6.5.3.3 Добавление хранилища резервных копий

В отдел или организацию можно добавить только по одному хранилищу резервных копий на каждый экземпляр Кибер Инфраструктуры или Кибер Хранилища. Хранилище, добавленное на уровне отдела, доступно в этом отделе и администраторам организации. Хранилище, добавленное на уровне организации, доступно только администраторам организации.

При добавлении хранилища вы создаете и вводите его имя. Если понадобится добавить существующее хранилище на новый или другой сервер управления, установите флажок **Использовать существующее хранилище в Кибер Инфраструктуре или Кибер Хранилище**, щелкните **Обзор** и выберите хранилище в списке.

Если на сервере управления зарегистрировано несколько экземпляров Кибер Инфраструктуры или Кибер Хранилища, можно выбрать нужный экземпляр при добавлении хранилища.

6.5.3.4 Ограничения для Кибер Инфраструктуры и Кибер Хранилища

- Невозможно выполнить прямой доступ к Кибер Инфраструктуре или Кибер Хранилищу с загрузочного носителя. Для работы с Кибер Инфраструктурой или Кибер Хранилищем зарегистрируйте носитель на сервере управления и управляйте им из веб-консоли Кибер Бэкап.
- Доступ к Кибер Инфраструктуре или Кибер Хранилищу через интерфейс командной строки невозможен.
- Резервное копирование в Кибер Инфраструктуру или Кибер Хранилище недоступно для конфигураций ESXi.
- После окончания резервного копирования в некоторых случаях размер больших архивов может обновляться с задержкой.

6.5.3.5 Документация

Документация продуктов доступна по следующим ссылкам:

- Кибер Инфраструктура,
- Кибер Хранилище.

6.6 Расписание

В расписании используются настройки времени (включая часовой пояс) операционной системы, в которой установлен агент. Инструкции по настройке агентов приведены в главе "Установка" (стр. 18).

© ООО Киберпротект, 2026

Пример: если план защиты, который применен к нескольким машинам в разных часовых поясах, запланирован к запуску в 21:00, то процесс резервного копирования на каждой машине начнется в 21:00 по местному времени данной машины.

6.6.1 Схема резервного копирования

Можно выбрать одну из стандартных схем резервного копирования или создать собственную. Схема входит в состав плана защиты и содержит расписание и методы создания резервных копий.

В разделе **Схема резервного копирования** выберите один из перечисленных ниже вариантов.

- [Только резервные копии на уровне дисков] **Всегда инкрементное**

  По умолчанию резервное копирование выполняется ежедневно с понедельника по пятницу. Можно выбрать время для запуска резервного копирования.

  Чтобы сменить частоту создания резервной копии, перетащите ползунок и задайте расписание резервного копирования.

  Для резервных копий используется новый формат резервной копии в виде одного файла[1].

  Эта схема недоступна при выполнении резервного копирования на SFTP-сервер или в зону безопасности.
- **Всегда полное**

  По умолчанию резервное копирование выполняется ежедневно с понедельника по пятницу. Можно выбрать время для запуска резервного копирования.

  Чтобы сменить частоту создания резервной копии, перетащите ползунок и задайте расписание резервного копирования.

  Каждый раз создаются полные резервные копии.
- **Еженедельно полное, ежедневно инкрементное**

  По умолчанию резервное копирование выполняется ежедневно с понедельника по пятницу. Дни недели и время запуска резервного копирования можно изменить.

  Раз в неделю создается полная резервная копия. Остальные копии будут инкрементными. Время создания полной резервной копии определяется параметром **Еженедельное резервное копирование** (щелкните значок шестеренки и выберите **Параметры резервного копирования** > **Еженедельное резервное копирование**).
- **Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS)**

  Схема GFS (Grandfather-Father-Son) или "дед-отец-сын" – иерархическая политика резервного копирования, при которой для разных типов резервных копий определяются различные периодичность создания и сроки хранения. Например: резервные копии уровня "сын"

[1]Новый формат резервных копий, в котором начальная полная и последующие инкрементные резервные копии сохраняются в одном TIB-файле вместо цепочки файлов. Преимуществом этого формата является скорость инкрементного метода; при этом он лишен основного недостатка – сложностей, связанных с удалением устаревших копий. Программа помечает блоки, которые используются такими копиями, как свободные, и записывает на их место новые резервные копии. В результате очистка выполняется очень быстро и с минимальным потреблением ресурсов. Формат резервной копии в виде одного файла недоступен при резервном копировании в хранилища, которые не поддерживают операции произвольного чтения и записи, например, на сервера SFTP.

© ООО Киберпротект, 2026

(инкрементные) создаются ежедневно и хранятся одну неделю, резервные копии уровня "отец" (дифференциальные) создаются каждую неделю и хранятся один месяц, резервные копии уровня "дед" (полные) создаются ежемесячно и хранятся год.

По умолчанию инкрементное резервное копирование выполняется ежедневно с понедельника по пятницу; дифференциальное резервное копирование выполняется каждую субботу; полное резервное копирование выполняется в первый день каждого месяца. Это расписание и время запуска резервного копирования можно изменить. Для установки сроков хранения требуется настроить правила хранения (см. раздел "Правила хранения" (стр. 299)).

Данная схема резервного копирования отображается как схема **Пользовательская** на панели плана защиты.

Примечание

При выборе этой схемы при создании резервных копий на лентах рекомендуется включить параметр **Использовать наборы лент в пуле лент, выбранных для резервного копирования** в окне **Параметры резервного копирования** > **Управление лентами** (см. "Управление лентами" (стр. 372)). Рекомендуется выбрать **Использовать отдельный набор лент** с шаблоном **День недели**.

В таком случае для каждого дня недели будет использоваться отдельная лента. Резервные копии, созданные в понедельник, будут храниться на одной ленте. Резервные копии, созданные во вторник, будут храниться на другой ленте. И так далее.

- **Другое**

  Задайте расписания для полных, дифференциальных и инкрементных резервных копий.

  Дифференциальное резервное копирование не выполняется для данных SQL и Exchange.

Для любой схемы резервного копирования можно запланировать резервное копирование по событиям, а не по времени. Для этого выберите тип события в настройках расписания. Дополнительную информацию см. в разделе «Расписание по событиям».

6.6.2 Дополнительные параметры расписания

Для каждого места сохранения можно выполнить следующие действия:

- Задайте условия запуска резервного копирования так, чтобы запланированное резервное копирование выполнялось только при соблюдении этих условий. Дополнительную информацию см. в разделе «Условия запуска».
- Задать интервал дат, в течение которого будет использоваться указанное расписание. Установите флажок **Выполнять план в диапазоне дат** и укажите диапазон дат.
- Отключить расписание. Когда расписание отключено, правила хранения не применяются за исключением случая, при котором резервное копирование запущено вручную.
- Настроить задержку с момента запланированного времени. Значение задержки для каждой машины выбирается случайно и находится в диапазоне от нуля до максимального значения, которое вы укажете. Параметр может быть полезен для резервного копирования нескольких машин в сетевое хранилище, чтобы избежать чрезмерной загрузки сети.

© ООО Киберпротект, 2026

Щелкните значок шестеренки, затем последовательно выберите пункты **Параметры резервного копирования** > **Планирование задач**. Установите флажок **Распределять время запуска резервного копирования по доступному времени**, затем укажите максимальную задержку. Продолжительность задержки для каждой машины определяется при применении плана защиты к машине и остается неизменной до тех пор, пока в плане защиты не будет изменено максимальное значение задержки.

- Щелкните **Подробнее**, чтобы получить доступ к указанным ниже параметрам:
  - **Если машина выключена, выполнить пропущенные задания при ее загрузке** (по умолчанию отключено)
  - **Отключить переход в спящий режим или режим гибернации при выполнении резервного копирования** (по умолчанию включено)

    Этот параметр действует только для машин с ОС Windows.
  - **Выйти из спящего режима или режима гибернации для запуска запланированного резервного копирования** (отключено по умолчанию)

    Этот параметр действует только для машин с ОС Windows. Этот параметр не действует, когда машина выключена, т. е. данный параметр не использует функциональность Wake-on-LAN.

6.6.3 Планирование по событиям

При составлении расписания для плана защиты выберите тип события в настройках расписания. Резервное копирование будет запущено, как только произойдет событие.

Можно выбрать одно из следующих событий

- **С заданной периодичностью**

  Через определенное время после завершения последнего успешного резервного копирования в рамках одного плана защиты. Укажите период времени.

  Примечание
  Расписание составляется на основе успешно выполненных операций резервного копирования. При сбое операции резервного копирования планировщик не будет запускать задание заново, пока оператор не запустит план вручную, и он не будет выполнен без сбоев.

- **При входе пользователя в учетную запись**

  По умолчанию резервное копирование запустится при входе в учетную запись любого пользователя. Вместо любого пользователя можно указать конкретную учетную запись.
- **При выходе пользователя из учетной записи**

  По умолчанию резервное копирование запустится при выходе из учетной записи любого пользователя. Вместо любого пользователя можно указать конкретную учетную запись.

© ООО Киберпротект, 2026

Примечание
Резервное копирование не будет запущено при завершении работы системы, поскольку завершение работы не эквивалентно выходу из учетной записи.

- **При запуске системы**
- **При завершении работы системы**
- **По событию в журнале событий Windows**
  Вы должны указать свойства события.

В следующей таблице перечислены события, доступные для различных данных в ОС Windows и Linux.

ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ	С заданной периодичностью	При входе пользователя в учетную запись	При выходе пользователя из учетной записи	При запуске системы	При завершении работы системы	По событию в журнале событий Windows
Диски/тома или файлы (физические машины)	Windows, Linux	Windows	Windows	Windows, Linux	Windows	Windows
Диски/тома (виртуальные машины)	Windows, Linux	-	-	-	-	-
Конфигурация ESXi	Windows, Linux	-	-	-	-	-
Базы данных и почтовые ящики Exchange	Windows	-	-	-	-	Windows
Базы данных SQL	Windows	-	-	-	-	Windows

6.6.3.1 По событию в журнале событий Windows

Можно запланировать запуск резервного копирования в случае записи определенного события в один из журналов событий Windows (**журнал приложения**, **журнал безопасности** или **системный**

© ООО Киберпротект, 2026

журнал).

Например, можно задать план защиты, по которому аварийное полное резервное копирование данных будет запускаться автоматически, как только ОС Windows обнаружит вероятность отказа жесткого диска.

Для обзора событий и просмотра свойств событий используйте встраиваемое **Средство просмотра событий**, доступное в консоли **Управление компьютером**. Журнал **Безопасность** может быть открыт только из-под учетной записи, которая входит в группу **«Администраторы»**.

Свойства событий

Имя журнала

Указывает имя журнала. Выберите имя стандартного журнала (**Приложение**, **Безопасность** или **Система**) из списка или введите имя журнала. Пример: **Microsoft Office Sessions**

Источник события

Указывает источник события. Как правило, это программа или компонент системы, который вызвал событие. Пример: **диск**.

Любой источник событий с указанной строкой запустит запланированное резервное копирование. Этот параметр не является регистрозависимым. Таким образом, если указана строка "служб", то источники событий **Диспетчер служб** и **Служба времени** вызовут резервное копирование.

Тип события

Указывает тип события: **Ошибка**, **Предупреждение**, **Информация**, **Успех аудита** или **Ошибка аудита**.

Идентификатор события

Указывает номер события, который обычно определяет тип событий среди событий из одного источника.

Например, событие **Ошибка** с источником события **диск** и идентификатором события **7** происходит в случае, если ОС Windows обнаруживает плохой блок на диске, а событие **Ошибка** с источником события **диск** и идентификатором события **15** – в случае, если диск еще недоступен.

Пример. Аварийное резервное копирование при обнаружении «плохого блока»

Появление одного или нескольких плохих блоков на жестком диске обычно означает, что диск скоро выйдет из строя. Предположим, требуется план защиты, который создаст резервную копию данных жесткого диска в такой ситуации.

Если ОС Windows обнаруживает плохой блок на жестком диске, это событие записывается в журнал **Система** с источником события **диск** и номером события **7**, тип этого события – **ошибка**.

Во время создания плана введите или выберите следующее в разделе **Расписание**.

© ООО Киберпротект, 2026

- **Имя журнала**: **Система**
- **Источник события**: **диск**
- **Тип события**: **Ошибка**
- **Идентификатор события**: **7**

Внимание
Чтобы убедиться в том, что резервное копирование будет выполнено несмотря на присутствие плохих блоков, необходимо настроить резервное копирование на пропуск плохих блоков. Для этого в разделе **Параметры резервного копирования** выберите **Обработка ошибок** и установите флажок **Пропуск поврежденных секторов**.

6.6.4 Условия запуска

Такие настройки делают планировщик более гибким, позволяя выполнять резервное копирование в соответствии с определенными условиями. Если условий несколько, для запуска резервного копирования все они должны выполняться одновременно. Начальные условия не действуют, если резервная копия запущена вручную.

Для доступа к этим настройкам щелкните **Показать больше** при настройке расписания для плана защиты.

Поведение планировщика заданий в случае, если событие происходит, а одно или несколько условий не выполнено, определяется параметром резервного копирования Условия запуска резервного копирования. Чтобы предусмотреть случаи, когда условия не выполняются в течение слишком долгого времени и дальнейшая отсрочка резервного копирования становится рискованной, можно установить временной промежуток, после которого задание запустится независимо от условия.

В следующей таблице перечислены условия запуска, доступные для различных данных в ОС Windows и Linux.

ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ	Диски/тома или файлы (физические машины)	Диски/тома (виртуальные машины)	Конфигурация ESXi	Базы данных и почтовые ящики Exchange	Базы данных SQL
Пользователь неактивен	Windows	-	-	-	-
Хост хранилища резервных копий доступен	Windows, Linux	Windows, Linux	Windows, Linux	Windows	Windows
Пользователи завершили сеанс	Windows	-	-	-	-

© ООО Киберпротект, 2026

В интервале времени	Windows, Linux	Windows, Linux	-	-	-
Сэкономить заряд батареи	Windows	-	-	-	-
Не запускать при работе на лимитном подключении	Windows	-	-	-	-
Не запускать при подключении к следующим сетям Wi-Fi	Windows	-	-	-	-
Проверить IP-адрес устройства	Windows	-	-	-	-

6.6.4.1 Пользователь неактивен

«Пользователь неактивен» означает, что машина заблокирована или на экране отражается заставка.

Пример

Запускать резервное копирование на машине каждый день в 21:00 – желательно, когда пользователь неактивен. Если в 23:00 пользователь все еще активен, все равно запустить резервное копирование.

- Расписание: Ежедневно, запускать каждый день. Запускать в: **21:00**.
- Условие: **Пользователь неактивен**.
- Условия запуска резервного копирования: **Ждать выполнения условий, все равно запустить резервное копирование через 2** часа.

В результате:

1. Если пользователь становится неактивным до 21:00, резервное копирование начинается в 21:00.

2. Если пользователь становится неактивным между 21:00 и 23:00, резервное копирование выполняется сразу после того, как пользователь стал неактивным.

3. Если пользователь все еще активен в 23:00, резервное копирование начинается в 23:00.

6.6.4.2 Хост хранилища резервных копий доступен

Строка «Хост хранилища резервных копий доступен» означает, что машина, служащая назначением для хранения резервных копий, доступна в сети.

© ООО Киберпротект, 2026

Данное условие эффективно для сетевых папок и хранилищ под управлением узла хранения.

Данное условие перекрывает доступность хоста, а не доступность самого хранилища. Например, если хост доступен, но отсутствует доступ к сетевой папке на хосте или учетные данные для доступа к папке недействительны, условия все еще считаются соблюденными.

Пример

Резервное копирование данных в сетевую папку выполняется каждый рабочий день в 21:00. Если машина, на которой находится папка, в это время недоступна (например, из-за профилактических работ), вам необходимо пропустить резервное копирование и ждать запланированного запуска на следующий рабочий день.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: **21:00**.
- Условие: **Хост хранилища резервных копий доступен**.
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

1. Если в 21:00 хост местоположения доступен, резервное копирование начнет выполняться вовремя.

2. Если в 21:00 хост с хранилищем недоступен, резервное копирование будет выполнено в следующий рабочий день, когда хост будет доступен.

3. Если хост с хранилищем вообще недоступен по рабочим дням в 21:00, задание вообще не будет выполняться.

6.6.4.3 Пользователи завершили сеанс

Позволяет поставить выполнение резервного копирования на ожидание до тех пор, пока все пользователи не выйдут из системы Windows.

Пример

Запуск резервного копирования в 20:00 каждую пятницу, желательно, когда все пользователи завершили сеанс. Если один из пользователей все еще находится в системе в 23:00, все равно запустить резервное копирование

- Расписание: Еженедельно, по пятницам. Запускать в: **20:00**.
- Условие: **Пользователи завершили сеанс**.
- Условия запуска резервного копирования: **Ждать выполнения условий**, **все равно запустить резервное копирование через 3** часа.

В результате:

1. Если все пользователи выходят из системы к 20:00, резервное копирование начинает выполняться в 20:00.

© ООО Киберпротект, 2026

2. Если последний пользователь выходит из системы между 20:00 и 23:00, резервное копирование начинает выполняться сразу после выхода пользователя из системы.

3. Если хотя бы один пользователь все еще активен в 23:00, резервное копирование начинается в 23:00.

6.6.4.4 В интервале времени

Ограничивает время запуска резервного копирования определенным интервалом.

Пример

Для резервного копирования данных пользователей и серверов компания использует разные области на одном и том же сетевом устройстве хранения. Рабочий день начинается в 8:00 и заканчивается в 17:00. Копирование данных пользователя должно начинаться, как только пользователи выйдут из системы, но не раньше 16:30. Каждый день в 23:00 начинается резервное копирование серверов компании. К этому времени резервное копирование пользовательских данных должно закончиться, чтобы освободить пропускную способность сети. Считается, что резервное копирование данных пользователей занимает не больше часа, так что самое позднее время начала резервного копирования – 22:00. Если в заданный период времени пользователь все еще находится в системе или выходит из системы в любое другое время, резервное копирование пользовательских данных не производится, то есть, резервное копирование пропускается.

- Событие: **При выходе пользователя из системы**. Укажите учетную запись пользователя: **Любой пользователь**.
- Условие: **В интервале времени** от **16:30** до **22:00**.
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

(1) Если пользователь выходит из системы между 16:30:00и 22:00:00, задание резервного копирования запускается сразу после выхода пользователя из системы.

(2) Если пользователь выходит из системы в любое другое время, резервное копирование пропускается.

6.6.4.5 Сэкономить заряд батареи

Предотвращает резервное копирование, если устройство (ноутбук или планшетный ПК) не подключено к источнику питания. В зависимости от значения параметра резервного копирования Условия запуска резервного копирования пропущенное резервное копирование запускается или не запускается после подключения устройства к источнику питания. Доступны следующие параметры:

- **Не запускать при работе от батареи**
  Резервное копирование запускается, только если устройство подключено к источнику питания.
- **Запускать при работе от батареи, если уровень ее заряда больше**

© ООО Киберпротект, 2026

Резервное копирование запускается, если устройство подключено к источнику питания или если уровень заряда аккумуляторной батареи больше указанного значения.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство не подключено к источнику питания (например, пользователь допоздна задерживается на собрании), уместно не выполнять резервное копирование до тех пор, пока устройство не будет подключено к источнику питания. Это позволит сэкономить заряд батареи.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.
- Условие: **Сэкономить заряд батареи**, **Не запускать при работе от батареи**.
- Условия запуска резервного копирования: **Ожидайте выполнения условий**.

В результате:

(1) Если в 21:00 устройство подключено к источнику питания, резервное копирование начнется немедленно.

(2) Если в 21:00 устройство работает от аккумуляторной батареи, резервное копирование начнется как только устройство будет подключено к источнику питания.

6.6.4.6 Не запускать при работе на лимитном подключении

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если устройство подключено к Интернету через лимитное подключение в Windows. Дополнительную информацию о лимитных подключениях в Windows см. по ссылке https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

Дополнительная мера предотвращения резервного копирования через мобильные точки доступа: если включено условие **Не запускать при работе на лимитном подключении**, условие **Не запускать при подключении к следующим сетям Wi-Fi** включается автоматически. По умолчанию указаны следующие сетевые имена: "android", "phone", "mobile" и "modem". Эти имена можно удалить из списка, щелкнув значок X.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство подключено к Интернету через лимитное подключение (например, пользователь в командировке), возможно, предпочтительнее будет не выполнять резервное копирование, дождавшись запланированного запуска на следующий рабочий день. Это позволит сэкономить сетевой трафик.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.
- Условие: **Не запускать при работе на лимитном подключении**
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

© ООО Киберпротект, 2026

(1) Если в 21:00 устройство не подключено к Интернету через лимитное подключение, резервное копирование начнется немедленно.

(2) Если в 21:00 устройство подключено к Интернету через лимитное подключение, резервное копирование начнется на следующий рабочий день.

(3) Если устройство всегда подключено к Интернету через лимитное подключение по рабочим дням 21:00, то резервное копирование вообще не запускается.

6.6.4.7 Не запускать при подключении к следующим сетям Wi-Fi

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если устройство подключено к любой указанной беспроводной сети. Можно указать имена сети Wi-Fi, также известные как идентификаторы беспроводной сети (SSID).

Это ограничение применяется ко всем сетям, которые содержат указанное имя (с учетом регистра) как подстроку в своем имени. Например, если в качестве сетевого имени указать "phone", резервная копия не запустится, если устройство подключено к любой из указанных ниже сетей: "John's iPhone", "phone_wifi", или "my_PHONE_wifi".

Это условие полезно, чтобы предотвратить резервное копирование, когда устройство подключено к Интернету через мобильную точку доступа.

Дополнительная мера предотвращения резервного копирования через мобильные точки доступа: условие **Не запускать при подключении к следующим сетям Wi-Fi** включается автоматически при включении условия **Не запускать при работе на лимитном подключении**. По умолчанию указаны следующие сетевые имена: "android", "phone", "mobile" и "modem". Эти имена можно удалить из списка, щелкнув значок X.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство подключено к Интернету через мобильную точку доступа (например, ноутбук подключен через мобильный телефон в режиме модема), возможно, предпочтительнее будет не выполнять резервное копирование, дождавшись запланированного запуска на следующий рабочий день.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.
- Условие: **Не запускать при подключении к следующим сетям**, **Сетевое имя**: <SSID сети доступа>.
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

(1) Если в 21:00 машина не подключена к указанной сети, резервное копирование начнется немедленно.

(2) Если в 21:00 машина подключена к указанной сети, резервное копирование начнется на следующий рабочий день.

© ООО Киберпротект, 2026

(3) Если машина всегда подключено к указанным сетям по рабочим дням 21:00, то резервное копирование вообще не запускается.

6.6.4.8 Проверить IP-адрес устройства

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если любой из IP-адресов устройства находится в указанном диапазоне IP-адресов или вне этого диапазона. Доступны следующие параметры:

- **Запустить, если вне диапазона IP-адресов**
- **Запустить, если в диапазоне IP-адресов**

В обоих параметрах можно указать разные диапазоны. Поддерживаются только адреса IPv4.

Это условие позволяет избежать затрат на передачу больших объемов данных, если пользователь физически находится на большом расстоянии. Кроме того, оно помогает предотвратить резервное копирование через подключение VPN.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство подключено к корпоративной сети через VPN-туннель (например, пользователь работает из дома), уместно не выполнять резервное копирование до тех пор, пока устройство не будет в офисе.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.
- Условие: **Проверить IP-адрес устройства**, **Запустить, если вне диапазона IP-адресов**, **От**: <начало диапазона IP-адресов VPN>, **До**: <конец диапазона IP-адресов VPN>.
- Условия запуска резервного копирования: **Ожидайте выполнения условий**.

В результате:

(1) Если в 21:00 IP-адрес машины не будет находится в указанном диапазоне, резервное копирование запустится немедленно.

(2) Если в 21:00 IP-адрес машины будет находится в указанном диапазоне, резервное копирование запустится как только устройство получит IP-адрес вне диапазона IP-адресов VPN.

(3) Если IP-адрес машины всегда находится в указанном диапазоне по рабочим дням в 21:00, резервное копирование вообще не будет выполняться.

6.7 Правила хранения

Для настройки правил хранения резервных копий выполните следующие действия:

1. Нажмите **Срок хранения**.
2. В разделе **Очистка** выберите один из перечисленных ниже вариантов:

© ООО Киберпротект, 2026

- **По сроку хранения** (по умолчанию)

  Укажите, в течение какого срока нужно хранить резервные копии, созданные планом защиты. По умолчанию правила хранения задаются отдельно для каждого набора резервных копий[1]. Чтобы использовать одно правило для всех резервных копий, щёлкните **Переключиться на одно правило для всех наборов резервных копий**.
- **По числу резервных копий**

  Укажите максимальное количество хранимых резервных копий.
- **По общему размеру резервных копий**

  Укажите максимальный общий размер резервных копий.

  Данная настройка доступна только для формата резервных копий "Версия 11" (см. раздел "Формат резервной копии" (стр. 347)).

  Данная настройка недоступна в схеме резервного копирования **Всегда инкрементное** или при резервном копировании на сервер SFTP или на ленточное устройство.
- **Хранить резервные копии неограниченное время**

3. Выберите время для запуска очистки:
   - **После резервного копирования** (по умолчанию)

     Правила хранения будут применены после создания новой резервной копии.
   - **До резервного копирования**

     Правила хранения будут применены до создания новой резервной копии.

     Эта настройка недоступна при резервном копировании кластеров Microsoft SQL Server или сервера Microsoft Exchange.
4. Нажмите кнопку **Готово**.

В результате правила хранения резервных копий будут установлены.

6.7.1 Что ещё нужно знать

- Последняя резервная копия, созданная согласно плану защиты, сохраняется в любом случае, даже если это нарушает правило хранения. Не пытайтесь удалить единственную резервную копию, применяя правила хранения перед резервным копированием.

---

[1]Группа резервных копий, к которым можно применить отдельное правило хранения. Для настраиваемой схемы резервного копирования наборы резервных копий соответствуют методам резервного копирования (полный, дифференциальный и инкрементный). Во всех других случаях используются ежемесячный, ежедневный, еженедельный и почасовой наборы резервного копирования. Ежемесячная резервная копия – это первая копия, которая создается после начала месяца. Еженедельная резервная копия создается в день недели, который задан с помощью параметра Еженедельная резервная копия (щелкните значок шестеренки и последовательно выберите пункты Параметры резервного копирования > Еженедельная резервная копия). Если еженедельная копия является первой с начала месяца, она считается ежемесячной. В этом случае еженедельная резервная копия создается в назначенный день на следующей неделе. Ежедневная резервная копия – это первая копия, которая создается после начала дня, если только она не является ежемесячной или еженедельной. Почасовая резервная копия – это первая копия, которая создается после начала часа, если только она не является ежемесячной, еженедельной или ежедневной

© ООО Киберпротект, 2026

- Резервные копии, которые хранятся на ленточном накопителе, не удаляются физически до перезаписи данных на ленте.
- Если в соответствии со схемой резервного копирования и форматом резервного копирования каждая резервная копия хранится в отдельном файле, этот файл не может быть удалён до окончания времени существования всех зависимых от него резервных копий (инкрементных и дифференциальных). Для хранения резервных копий, удаление которых отложено, требуется дополнительное место на диске. Кроме того, возраст, количество или размер резервных копий могут превышать указанные вами значения.

  Это поведение можно изменить, используя опцию резервного копирования "Консолидация резервных копий" (стр. 342).
- Правила хранения – составная часть плана защиты. Они прекращают действовать для резервных копий машины, как только с неё отозван или удалён план защиты или когда сама машина удалена с сервера управления. Если вам больше не нужны резервные копии, созданные данным планом, удалите их, как описано в разделе "Удаление резервных копий" (стр. 413).

6.8 Защита паролем

Внимание
Если пароль утерян, восстановить защищённые резервные копии будет невозможно.

6.8.1 Настройка защиты паролем в планах защиты

Чтобы включить защиту паролем, укажите соответствующие параметры при создании плана защиты. После применения плана защиты изменить их будет невозможно. Чтобы использовать другие настройки защиты паролем, создайте новый план защиты.

Определение настроек защиты паролем в планах защиты

1. На панели плана защиты переведите переключатель **Защита паролем** в положение **Включено**.
2. Укажите и подтвердите пароль.
3. Выберите один из следующих уровней защиты паролем:
   - **Базовый** – резервные копии будут защищены паролем с уровнем защиты **Базовый**.
   - **Средний** – резервные копии будут защищены паролем с уровнем защиты **Средний**.
   - **Высокий** – резервные копии будут защищены паролем с уровнем защиты **Высокий**.
4. Нажмите кнопку **OK**.

6.8.2 Особенности защиты паролем

Чем выше уровень защиты паролем, тем дольше выполняется план защиты.

© ООО Киберпротект, 2026

Пароль не сохраняется на диске или в резервных копиях. Это позволяет обезопасить данные резервной копии от несанкционированного доступа, но восстановление утраченного пароля невозможно.

6.9 Преобразование в виртуальную машину

Преобразование в виртуальную машину возможно только для резервных копий на уровне дисков. Если в резервной копии есть системный том и вся информация, необходимая для запуска операционной системы, то созданная виртуальная машина может запускаться без стороннего содействия. В противном случае можно добавить ее виртуальные диски на другую виртуальную машину.

6.9.1 Методы преобразования

- **Обычное преобразование**

  Есть два способа настроить регулярное преобразование:

  - **Включить преобразование в план защиты**

    Преобразование будет выполняться после каждого резервного копирования (если настроено для первичного хранилища) или после каждой репликации (если настроено для второго и последующих хранилищ).
  - **Создать отдельный план преобразования**

    Этот метод позволяет указать отдельное расписание преобразования.
- **Восстановить на новую виртуальную машину**

  Этот метод позволяет выбрать диски для восстановления и задать настройки для каждого виртуального диска. Этот метод позволяет выполнять преобразование только один раз или время от времени, например, для выполнения миграции с физической машины на виртуальную.

6.9.2 Важная информация о преобразовании

6.9.2.1 Поддерживаемые типы виртуальных машин

Преобразование резервной копии в виртуальную машину можно выполнить в том же агенте, который использовался для ее создания, или в другом агенте.

Чтобы выполнить преобразование в VMware ESXi или Hyper-V, необходимо иметь хост ESXi или Hyper-V и агент защиты (агент для VMware или агент для Hyper-V), который управляет этим хостом.

Преобразование в файлы VHDX предполагает, что файлы будут подключаться к виртуальной машине Hyper-V как виртуальные диски.

В следующей сводной таблице указаны типы виртуальных машин, которые могут быть созданы теми или иными агентами:

Тип ВМ	Агент для VMware	Агент для Hyper-V	Агент для Windows	Агент для Linux

© ООО Киберпротект, 2026

VMware ESXi	+	-	-	-
Microsoft Hyper-V	-	+	-	-
VMware Workstation	+	+	+	+
Файлы VHDX	+	+	+	+

6.9.2.2 Ограничения

- Агент для Windows, агент для VMware (Windows) и агент для Hyper-V не могут преобразовать резервные копии, которые хранятся в системе NFS.
- Резервные копии, которые хранятся в системе NFS или на сервере SFTP, невозможно преобразовать в рамках отдельного плана преобразования.
- Резервные копии, которые хранятся в Зона безопасности, могут быть преобразованы только агентом, который выполняется та той же машине.
- Резервные копии с логическими томами Linux (LVM) можно преобразовать, только если они созданы агентом для VMware или агентом для Hyper-V и ориентированы на один гипервизор. Преобразование между различными гипервизорами не поддерживается.
- При преобразовании резервных копий машины Windows в файлы VMware Workstation или VHDX полученная виртуальная машина наследует тип ЦП от машины, которая выполняет преобразование. В результате этого в гостевой операционной системе устанавливаются соответствующие драйверы ЦП. Если гостевая система запускается на хосте с ЦП другого типа, в гостевой системе отображается ошибка драйвера. Обновите этот драйвер вручную.

6.9.2.3 Регулярное преобразование в ESXi и Hyper-V по сравнению с запуском виртуальной машины с резервной копии

Обе операции предоставляют в ваше распоряжение виртуальную машину, которую можно запустить за считанные секунды в случае сбоя оригинальной машины.

Для регулярного преобразования требуются ресурсы ЦП и памяти. Файлы виртуальной машины постоянно занимают место в хранилище данных. Если рабочий хост используется для преобразования, это может быть непрактично. Однако производительность виртуальной машины ограничена только ресурсами хоста.

Во втором случае ресурсы потребляются только в том случае, когда виртуальная машина запущена. Место на хранилище данных требуется только для того, чтобы сохранить изменения в виртуальных дисках. Однако виртуальная машина может работать медленно, поскольку хост работает с виртуальными дисками не напрямую, а через агент, который считывает данные с резервной копии. Кроме того, виртуальная машина является временной. Сделать машину постоянной можно только для ESXi.

© ООО Киберпротект, 2026

6.9.3 Преобразование в виртуальную машину в плане защиты

Можно настроить преобразование в виртуальную машину с любой резервной копии или хранилища репликации, указанных в плане защиты. Преобразование будет выполняться после каждого резервного копирования или репликации.

Информацию о предварительных требованиях и ограничениях см. в разделе «Важная информация о преобразовании».

Порядок настройки преобразования в виртуальную машину в плане защиты

1. Определите, с какого хранилища резервных копий необходимо выполнить преобразование.
2. На панели плана защиты для этого хранилища щелкните **Преобразовать в виртуальную машину**.
3. Включите параметр **Преобразование**.
4. В поле **Преобразовать в** выберите тип целевой виртуальной машины. Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **Файлы VHDX**
5. Выполните одно из следующих действий:
   - Для VMware ESXi и Hyper-V: щелкните **Хост**, выберите целевой хост, а затем укажите новый шаблон имени машины.
   - Для виртуальных машин других типов: в поле **Путь** укажите расположение для сохранения файлов виртуальной машины и шаблон имени файла.

   Имя по умолчанию – **[Имя машины]_converted**.
6. [Необязательно] Щелкните **Агенты, которые будут выполнять преобразование** и выберите агент.

   Это может быть агент, который выполняет резервное копирование (по умолчанию), или агент, установленный на другой машине. В последнем случае необходимо сохранить резервные копии в общем хранилище, например в сетевой папке, чтобы другая машина могла получить к нему доступ.
7. [Необязательно] Для VMware ESXi и Hyper-V можно также выполнить следующие действия:
   - Щелкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для данной виртуальной машины.
   - Измените режим распределения ресурса дисков. По умолчанию задана настройка **Экономное** для VMware ESXi и **Динамически расширяемое** для Hyper-V.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.
8. Нажмите кнопку **Готово**.

© ООО Киберпротект, 2026

6.9.4 Как работает обычное преобразование в виртуальную машину

То, как выполняются повторные преобразования, зависит от того, где нужно создать виртуальную машину.

- **Если нужно сохранить виртуальную машину как набор файлов:** при каждом преобразовании виртуальная машина будет повторно создаваться с нуля.
- **Если нужно создать виртуальную машину на сервере виртуализации:** при преобразовании инкрементной или дифференциальной резервной копии программа обновляет существующую виртуальную машину, а не создает ее заново. Обычно такое преобразование происходит быстрее. Таким образом снижается загруженность сети и потребление ресурсов ЦП хоста, на котором выполняется преобразование. Если обновление виртуальной машины невозможно, программа воссоздает ее с нуля.

Ниже подробно описаны оба случая.

6.9.4.1 Если нужно сохранить виртуальную машину как набор файлов

В результате первого преобразования будет создана новая виртуальная машина. При каждом последующем преобразовании эта машина будет повторно создаваться с нуля. Сначала старая машина временно переименовывается. Затем создается новая виртуальная машина с предыдущим именем старой машины. Если эта операция завершается успешно, старая машина удаляется. При сбое операции новая машина удаляется, а старой машине возвращается предыдущее имя. Таким образом, после преобразования всегда остается одна машина. Однако на время преобразования необходимо дополнительное дисковое пространство для размещения временной машины.

6.9.4.2 Если нужно создать виртуальную машину на сервере виртуализации

В результате первого преобразования создается новая виртуальная машина. Все последующие преобразования выполняются следующим образом.

- Если с момента последнего преобразования выполнялось *полное резервное копирование*, виртуальная машина создается заново с нуля, как описано ранее в этом разделе.
- В противном случае существующая виртуальная машина обновляется в соответствии с изменениями, которые произошли после последнего преобразования. Если обновление невозможно (например, удалены промежуточные моментальные снимки, см. ниже), виртуальная машина создается заново.

Промежуточные моментальные снимки

Чтобы иметь возможность обновить виртуальную машину, программа хранит несколько ее промежуточных моментальных снимков Эти моментальные снимки имеют имена **Backup…** и **Replica…**; их необходимо хранить. Ненужные моментальные снимки удаляются автоматически.

© ООО Киберпротект, 2026

Последний моментальный снимок **Replica...** соответствует результату последнего преобразования. Можно перейти к этому моментальному снимку, чтобы вернуть машину в это состояние, например если после работы с машиной нужно отменить внесенные изменения.

Другие моментальные снимки предназначены для внутреннего использования программой.

6.10 Репликация

В данном разделе описана репликация резервных копий, которая включена в план защиты. Информацию о создании отдельного плана репликации см. в разделе "Обработка данных вне хоста (off-host)" (стр. 413).

Если включить репликацию резервных копий, то каждая резервная копия копируется в другое хранилище сразу же после создания. Если более ранние резервные копии не были реплицированы (например, из-за сбоя сетевого подключения), программа также реплицирует все резервные копии, появившиеся после последней успешной репликации.

Реплицированные резервные копии не зависят от резервных копий, оставшихся в исходном хранилище и наоборот. Можно восстановить данные из любой резервной копии без доступа к другим хранилищам.

6.10.1 Примеры использования

- **Надёжное аварийное восстановление**

  Храните резервные копии локально (для немедленного восстановления) и удалённо (чтобы защитить резервные копии при отказе локального хранилища данных или стихийных бедствиях).
- **Сохранение только последних точек восстановления**

  Удалите старые резервные копии из быстродействующего запоминающего устройства в соответствии с правилами резервного копирования, чтобы без необходимости не использовать ёмкость хранения данных.

6.10.2 Поддерживаемые расположения

Возможные расположения источников и целевых хранилищ резервных копий при репликации приведены в таблицах ниже.

Источник репликации	Целевое хранилище репликации				
	Локальная папка	Сетевая папка	Папка NFS	SFTP-сервер	Зона безопасности
Локальная папка	+	+	+*	+	+
Сетевая папка	+	+	+*	+	+
Папка NFS	+	+	+*	+	+

© ООО Киберпротект, 2026

SFTP-сервер	+	+	+*	+	+
Зона безопасности	+	+	+*	+	+
Ленточное устройство	-	-	-	-	-
Хранилище под управлением узла хранения с дедупликацией	+	+	+*	+	+
Хранилище под управлением узла хранения без дедупликации	+	+	+*	+	+
Хранилище под управлением узла хранения с лентами	-	-	-	-	-
Кибер Инфраструктура или Кибер Хранилище	+	+	+*	+	+

* Только для ОС Linux.

Источник репликации	**Целевое хранилище репликации**				
	Ленточное устройство	**Хранилище под управлением узла хранения**			**Кибер Инфраструктура или Кибер Хранилище**
		с дедупликацией	**без дедупликации**	**с лентами**	
Локальная папка	+	+*	+	+	+
Сетевая папка	+	+*	+	+	+
Папка NFS	+	+*	+	+	+
SFTP-сервер	+	+*	+	+	+
Зона безопасности	+	+*	+	+	+
Ленточное устройство	-	-	-	-	-
Хранилище под управлением узла хранения с дедупликацией	+	+*	+	+	+
Хранилище под управлением узла хранения без дедупликации	+	+*	+	+	+
Хранилище под	-	-	-	-	-

© ООО Киберпротект, 2026

управлением узла хранения с лентами					
Кибер Инфраструктура или Кибер Хранилище	+	+*	+	+	+

* Только для резервных копий формата "Версия 11". Подробнее о форматах резервных копий см. раздел "Формат резервной копии" (стр. 347).

Примечание
Хранилище под управлением узла хранения с включённой дедупликацией не рекомендуется использовать для постоянной репликации. Дедупликация является длительным и ресурсоёмким процессом, который может привести к снижению скорости репликации, если в качестве источника реплицируемых данных используется хранилище под управлением узла хранения с дедупликацией.

Дополнительные условия использования хранилища под управлением узла хранения см. в разделе "Замечания по использованию узла хранения" (стр. 309).

6.10.3 Включение репликации резервных копий

Для включения репликации резервных копий выполните следующие действия:

1. На панели плана резервного копирования щёлкните **Добавить хранилище**.
   Элемент управления **Добавить хранилище** отображается только в том случае, если поддерживается репликация *из* последнего выбранного хранилища.
2. Укажите хранилище, в которое будет проведена репликация резервных копий.
3. [Необязательно] В поле **Срок хранения** измените правила хранения для указанного хранилища, как описано в разделе "Правила хранения" (стр. 299).
4. [Необязательно] В поле **Преобразовать в VM** укажите настройки преобразования в виртуальную машину, как описано в разделе "Преобразование в виртуальную машину" (стр. 302).
5. [Необязательно] Щёлкните значок шестерёнки > **Производительность и окно резервного копирования**, затем задайте окно резервного копирования для выбранного расположения, как описано в разделе "Производительность и окно резервного копирования" (стр. 361). Эти настройки определят производительность репликации.
6. [Необязательно] Повторите шаги 1-5 для всех хранилищ, где необходимо реплицировать резервные копии. Можно использовать до пяти последовательных хранилищ (включая основное).

© ООО Киберпротект, 2026

6.10.4 Замечания по использованию узла хранения

6.10.4.1 Репликация резервных копий между управляемыми хранилищами

Репликация резервной копии из одного управляемого хранилища в другое выполняется узлом хранения.

6.10.4.2 Ограничения

- Репликация резервных копий *из* ленточного устройства, подключенного к узлу хранения, не поддерживается.
- Репликация резервных копий *из* хранилища, управляемого узлом хранения, в Зону безопасности не поддерживается.
- Репликация резервных копий *в* управляемое хранилище с включенной дедупликацией не поддерживается для резервных копий, имеющих формат резервной копии **Версии 12**.

Примечание
Не рекомендуется использовать для постоянной репликации. Дедупликация является длительным и ресурсоёмким процессом, который может привести к снижению скорости репликации, если в качестве источника реплицируемых данных используется хранилище под управлением узла хранения с дедупликацией.

6.10.4.3 Какая машина выполняет операцию?

Репликация резервной копии *из* любого хранилища инициируется агентом, создавшим резервную копию, и выполняется:

- этим агентом, если хранилище *не* управляется узлом хранения;
- соответствующим узлом хранения, если хранилище является управляемым.

Как следует из вышеуказанного, операция будет выполнена только в том случае, если машина с агентом включена.

6.11 Запуск резервного копирования вручную

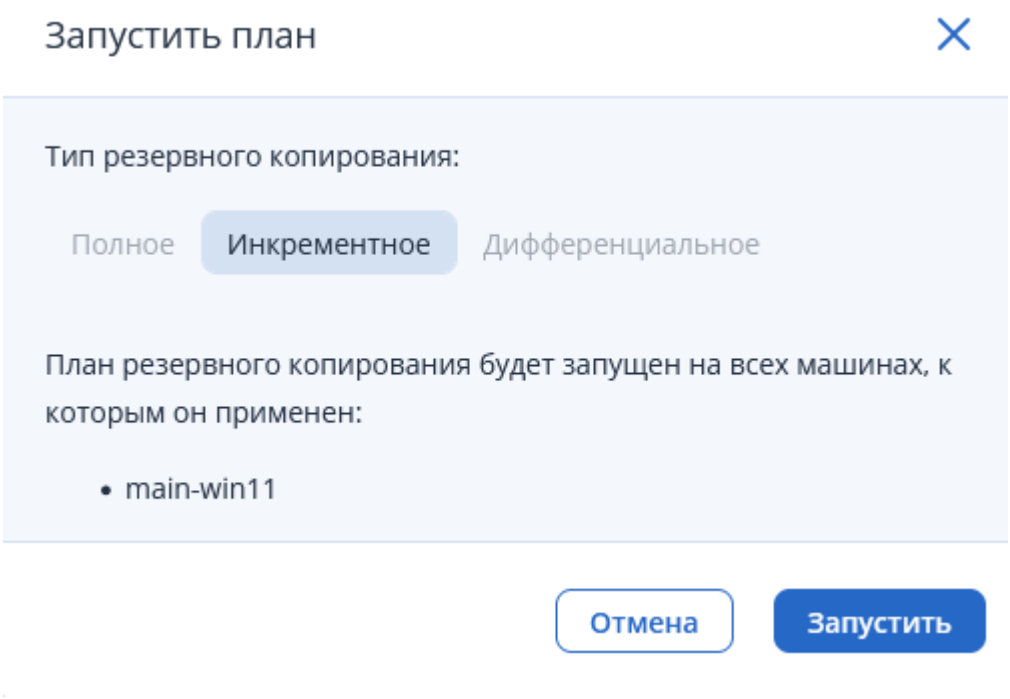
Можно не дожидаться запуска резервного копирования по расписанию и запустить его немедленно. Немедленный запуск резервного копирования можно осуществить несколькими способами.

Запуск резервного копирования из меню действий с планом

1. Во вкладке **Планы** -> **Защита** отметьте план в списке.
2. Щелкните **Запуск резервного копирования** в меню действий с планом.

© ООО Киберпротект, 2026

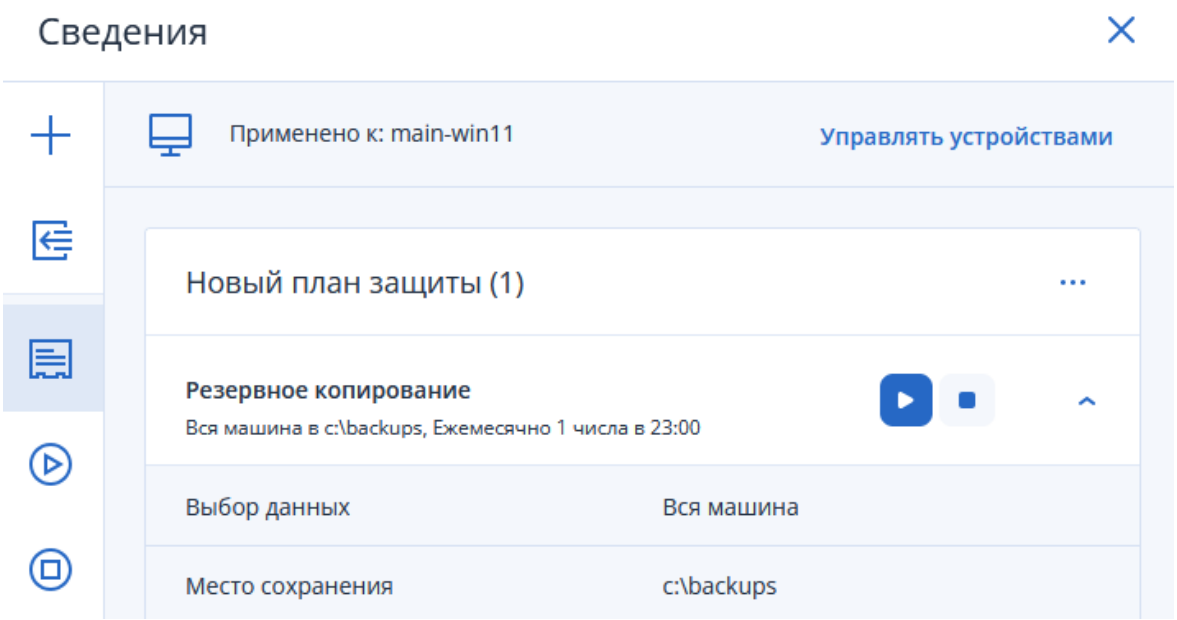
3. Выберите тип резервного копирования (доступно, если в плане предусматривается резервное копирование с сочетанием разных его типов).



4. Нажмите кнопку **Запустить**. Дождитесь окончания резервного копирования.

Запуск резервного копирования из вкладки Сведения

1. Отметьте план в списке и в меню действий с планом перейдите на вкладку **Сведения**.



2. Нажмите кнопку с символом воспроизведения.
3. Выберите тип резервного копирования (доступно, если в плане предусматривается резервное

© ООО Киберпротект, 2026

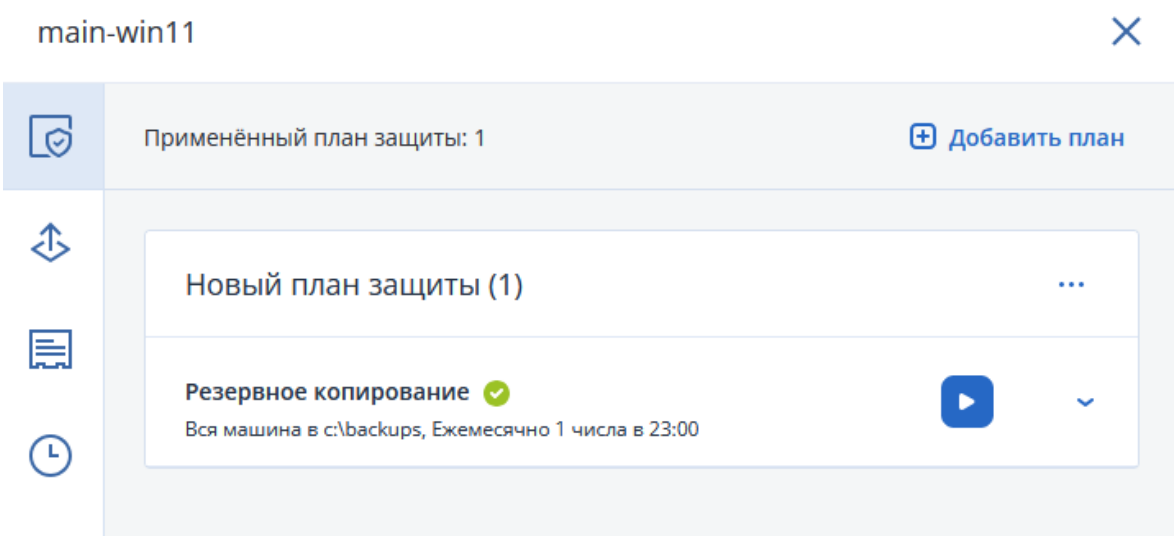
копирование с сочетанием разных его типов).

4. Нажмите кнопку **Запустить**. Дождитесь окончания резервного копирования.

Запуск резервного копирования из меню Устройства

1. Перейдите в меню **Устройства**.
2. Отметьте в списке одну машину или несколько машин и нажмите в меню справа **Защитить**.
3. Выберите нужный план и нажмите кнопку с символом воспроизведения.

Примечание
При выборе нескольких машин в списке будут отображены только те планы, которые являются общими для всех выбранных машин.



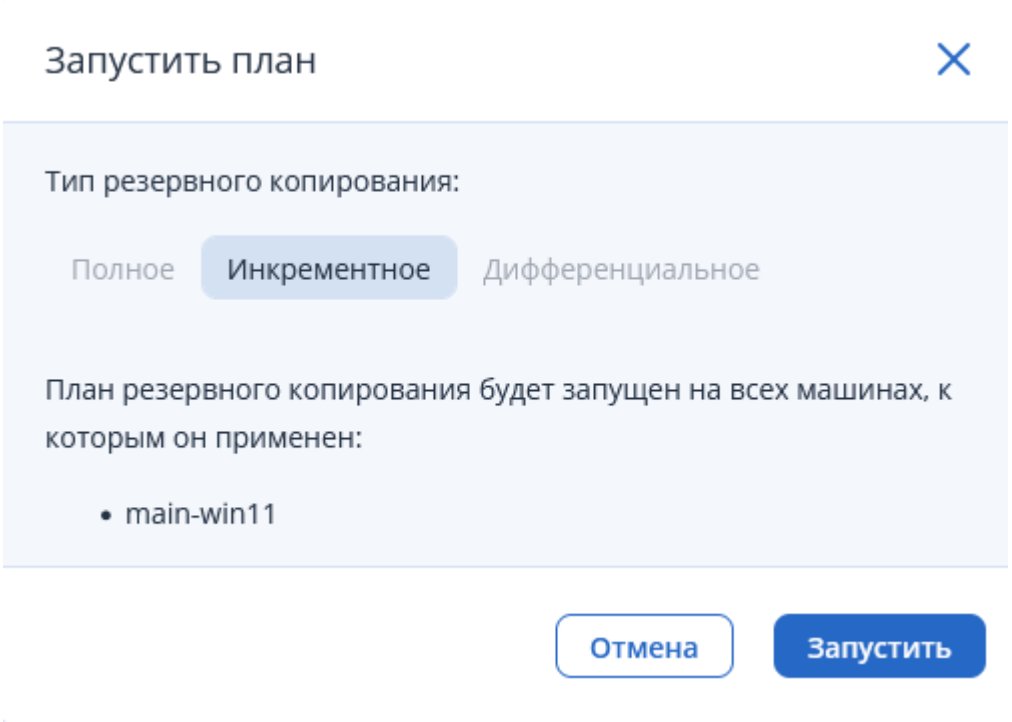
Если к машине применено несколько планов, нажмите кнопку запуска у каждого из тех, которые необходимо выполнить сейчас.

Примечание
Одновременный запуск большого количества планов может приводить к снижению производительности резервного копирования. Во избежание этого запускайте планы небольшими группами.

Внимание
Запуск по требованию нескольких планов одновременно требует включения одновременного резервного копирования. Для включения одновременного файлового и дискового резервного копирования необходимо настроить конфигурационный файл (см. "Одновременное резервное копирование" (стр. 312)).

4. Выберите тип резервного копирования (доступно, если в плане предусматривается резервное копирование с сочетанием разных его типов).

© ООО Киберпротект, 2026



5. Нажмите кнопку **Запустить**. Дождитесь окончания резервного копирования.

Первая резервная копия, созданная планом защиты, всегда является полной.

Прогресс выполнения резервного копирования отображается в столбце **Действия** для выбранной машины или на вкладке **Панель мониторинга** -> **Действия** основного меню.

Пока выполняется план, кнопка запуска будет неактивна. Остановка выполняющегося в данный момент резервного копирования в рамках плана описана в разделе "Операции с планами защиты" (стр. 227).

6.12 Одновременное резервное копирование

6.12.1 Зачем выполнять одновременное резервное копирование

Одновременное резервное копирование одним агентом позволяет нескольким планам защиты выполняться параллельно в том случае, когда они работают с одним и тем же типом данных. Одновременное резервное копирование является реализацией многозадачности агента в резервном копировании Кибер Бэкап (см. "Агент" (стр. 266)). Это способно значительно ускорить выполнение операций.

В Кибер Бэкап одновременное резервное копирование доступно для следующих элементов:

- локальные диски, файлы и папки;
- сетевые файлы и папки;
- виртуальные машины;

© ООО Киберпротект, 2026

- почтовые ящики Microsoft Exchange;
- экземпляры баз данных PostgreSQL.

  В Кибер Бэкап начиная с версии 17.3 доступно одновременное файловое (см. "Выбор файлов и папок" (стр. 273)) и дисковое (см. "Выбор дисков и томов" (стр. 275)) резервное копирование, выполняемое одним агентом.

  По умолчанию эта функция отключена.

6.12.2 Что нужно для выполнения одновременного резервного копирования

В таблице ниже представлены условия одновременного резервного копирования данных различных элементов в зависимости от их типа.

Элементы для резервного копирования	Особенности	Количество планов защиты	Возможность одновременного резервного копирования	Необходимость включения одновременного резервного копирования
Почтовые ящики	Разные почтовые ящики	Один или несколько	Да	Нет
Экземпляры баз данных PostgreSQL	Разные экземпляры	Один или несколько	Да	Нет
Виртуальные машины	Разные ВМ	Один или несколько	Да	Нет
	Разные диски одной ВМ	Несколько	Нет	Нет
Локальные диски	Разные диски одной машины	Несколько	Да	Да
	Один диск одной машины			Да

© ООО Киберпротект, 2026

Локальные файлы и папки	Разные диски одной машины	Несколько	Да	Да
	Один диск одной машины			Да
Сетевые файлы и папки (SMB/CIFS и NFS)	Разные файлы одного ресурса	Несколько	Да	Да

Для того, чтобы иметь возможность выполнять одновременное файловое и дисковое резервное копирование, необходимо включить его, выполнив настройку конфигурационного файла Кибер Бэкап.

6.12.3 Включение одновременного резервного копирования

Конфигурационный файл по умолчанию расположен на машине с агентом по адресу: C:\Program Files\Acronis\BackupAndRecovery\settings.config (для Windows) и /usr/lib/Acronis/BackupAndRecovery/settings.config (для Linux). Добавьте в него значение simultaneous_backups как показано далее:

```
<mms>

 <default>

   <backup>
    <simultaneous_backups>10</simultaneous_backups>

.....
```

Число в конфигурационном файле (в этом примере 10) – это параметр, задающий максимальное количество одновременно выполняемых планов. По умолчанию параметр simultaneous_backups не внесен в конфигурационный файл, что соответствует его значению, равному 1. Установка ограничения на число одновременно выполняемых планов для различных типов данных описана далее в соответствующих разделах.

Внимание

- После внесения изменений в конфигурацию агента его необходимо перезапустить.
- При обновлении агента пользовательское значение параметра simultaneous_backups не сохраняется. После обновления его нужно задать повторно.

© ООО Киберпротект, 2026

6.12.4 Запуск одновременного резервного копирования

Включение одновременного резервного копирования позволяет планам с файловым и дисковым резервным копированием выполняться одновременно.

Вы также можете запустить одновременное резервное копирование вручную. Запуск вручную выполняется в веб-консоли (см. "Запуск резервного копирования вручную" (стр. 309)).

Перед запуском создайте необходимые планы (см. "Создание плана защиты" (стр. 224)) с дисковым или файловым резервным копированием или убедитесь, что такие планы уже созданы (см. "Вкладка «Планы»" (стр. 423)).

6.12.5 Ограничение общего количества планов для файлового и дискового резервного копирования

Конфигурационный файл по умолчанию расположен по адресу: C:\Program Files\Acronis\BackupAndRecovery\settings.config (для Windows) и /usr/lib/Acronis/BackupAndRecovery/settings.config (для Linux). Укажите в нем необходимое значение параметра simultaneous_backups, задающего максимальное количество одновременно выполняемых планов:

```
<mms>

 <default>

   <backup>
    <simultaneous_backups>10</simultaneous_backups>

.....
```

В этом примере число указано равным 10. Если это число указано достаточно большим и ресурсов агента для одновременного резервного копирования не хватает, количество одновременно выполняемых планов будет автоматически скорректировано агентом.

Внимание

- После внесения изменений в конфигурацию агента его необходимо перезапустить.
- При обновлении агента пользовательское значение параметра simultaneous_backups не сохраняется. После обновления его нужно задать повторно.

6.12.6 Ограничение общего количества виртуальных машин

Параметр резервного копирования **Планирование** определяет количество виртуальных машин, для которых агент может одновременно создавать резервные копии при выполнении данного плана защиты.

© ООО Киберпротект, 2026

Если несколько планов защиты пересекаются по времени, указанные в их параметрах числа суммируются. Хотя суммарное количество программным образом ограничено до 10, пересечение планов может влиять на производительность резервного копирования, а также оказывать избыточную нагрузку на хранилище хоста и виртуальной машины.

Вы можете дополнительно ограничить общее количество виртуальных машин, для которых агенты для систем управления виртуализацией (например, VMware или Hyper-V) могут одновременно создавать резервные копии.

Примечание
Одновременное резервное копирование виртуальных машин для VMware/Hyper-V работает в том числе при размещении агента на физическом сервере.

Установка ограничения на общее количество виртуальных машин, для которых может создавать резервные копии агент для VMware (Windows) или агент для Hyper-V

1. На машине, на которой запущен агент, создайте новый текстовый документ и откройте его в текстовом редакторе, например в Блокноте.
2. Скопируйте и вставьте в этот файл следующие строки:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLi
mits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Вместо 00000001 укажите нужное ограничение в шестнадцатеричном формате. Например 00000001 означает 1, а 0000000A – 10.
4. Сохраните документ под именем **limit.reg**.
5. Запустите файл от имени администратора.
6. Подтвердите изменение реестра Windows.
7. Выполните указанные ниже действия, чтобы перезапустить агент.
   a. В меню **Пуск** выберите команду **Выполнить** и введите: **cmd**
   b. Нажмите кнопку **OK**.
   c. Выполните следующие команды:

```
net stop mms
net start mms
```

Установка ограничения на общее количество виртуальных машин, для которых может создавать резервные копии агент для VMware (виртуальное устройство) или агент для среды виртуализации (Linux)

Эта процедура применяется в отношении следующих агентов, предоставляемых в виде виртуального устройства:

© ООО Киберпротект, 2026

- агент для VMware;
- агент для системы управления виртуализацией, используемый совместно с агентом для Linux.

Для установки ограничения выполните следующие действия.

1. На машине, на которой запущен агент, откройте консоль управления.
   - **Агент для VMware (виртуальное устройство)**: в пользовательском интерфейсе виртуального устройства нажмите клавиши CTRL+SHIFT+F2.
   - **Агент для среды виртуализации (Linux)**: войдите с учетными данными пользователя root на машину, на которой запущено устройство Кибер Бэкап. Пароль совпадает с паролем для веб-консоли Кибер Бэкап.
2. Откройте файл **/etc/Acronis/MMS.config** в текстовом редакторе, например в **vi**.
3. Найдите следующий раздел:

   ```
   <key name="SimultaneousBackupsLimits">
     <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
   </key>
   ```

4. Вместо 10 укажите нужное ограничение в десятичном формате.
5. Сохраните файл.
6. Перезапустите агент.
   - **Агент для VMware (виртуальное устройство)**: выполните команду reboot.
   - **Агент для среды виртуализации (Linux)**: выполните указанные ниже команды.

     ```
     sudo service acronis_mms restart
     ```

6.12.7 Ограничение общего количества планов для почтовых ящиков и баз данных PostgreSQL

Конфигурационный файл по умолчанию расположен по адресу: /opt/acronis/etc/generic-backup-agent/generic-backup-agent.json. В параметре maxTasks укажите максимальное количество одновременно выполняемых планов (по умолчанию 5):

```
"maxTasks": 5
```

Внимание
После внесения изменений в конфигурацию агента его необходимо перезапустить.

© ООО Киберпротект, 2026

6.13 Резервное копирование виртуальных машин без использования локальной сети (LAN-free backup)

В том случае, если по каким-то причинам вы не можете использовать локальную сеть для резервного копирования виртуальных машин или она становится узким местом в вашей системе, можно настроить резервное копирование без использования локальной сети.

6.13.1 Резервное копирование без использования локальной сети (LAN-free backup) для oVirt

Резервное копирование без использования локальной сети в системах oVirt/zVirt поддерживается в следующих продуктах:

- Кибер Бэкап версии 17.3 и выше;
- oVirt версии 4.2 и выше;
- zVirt версии 4.2 и выше.

© ООО Киберпротект, 2026

6.13.1.1 Схема резервного копирования без использования локальной сети

На этой схеме:

- **ВМ CMS** – виртуальная машина с установленным сервером управления Кибер Бэкап (CMS);
- **Виртуальное устройство** – виртуальное устройство для взаимодействия с Кибер Бэкап и oVirt/zVirt;

© ООО Киберпротект, 2026

- **BM** – целевая виртуальная машина для выполнения резервной копии, расположена на системе виртуализации oVirt/zVirt;
- **Node** – вычислительный узел (хост) системы виртуализации oVirt/zVirt;
- **------** – отображает подключение сети управления;
- **<------- >** – отображает направление трафика;
- **iSCSI,FC** – устройство хранения резервных копий;
- **Подключение диска к виртуальному устройству** – подключение диска к виртуальному устройству через настроенную сеть хранения данных на системе виртуализации (диск RDM (прямой LUN), диск, представленный через iSCSI или из локального хранилища).

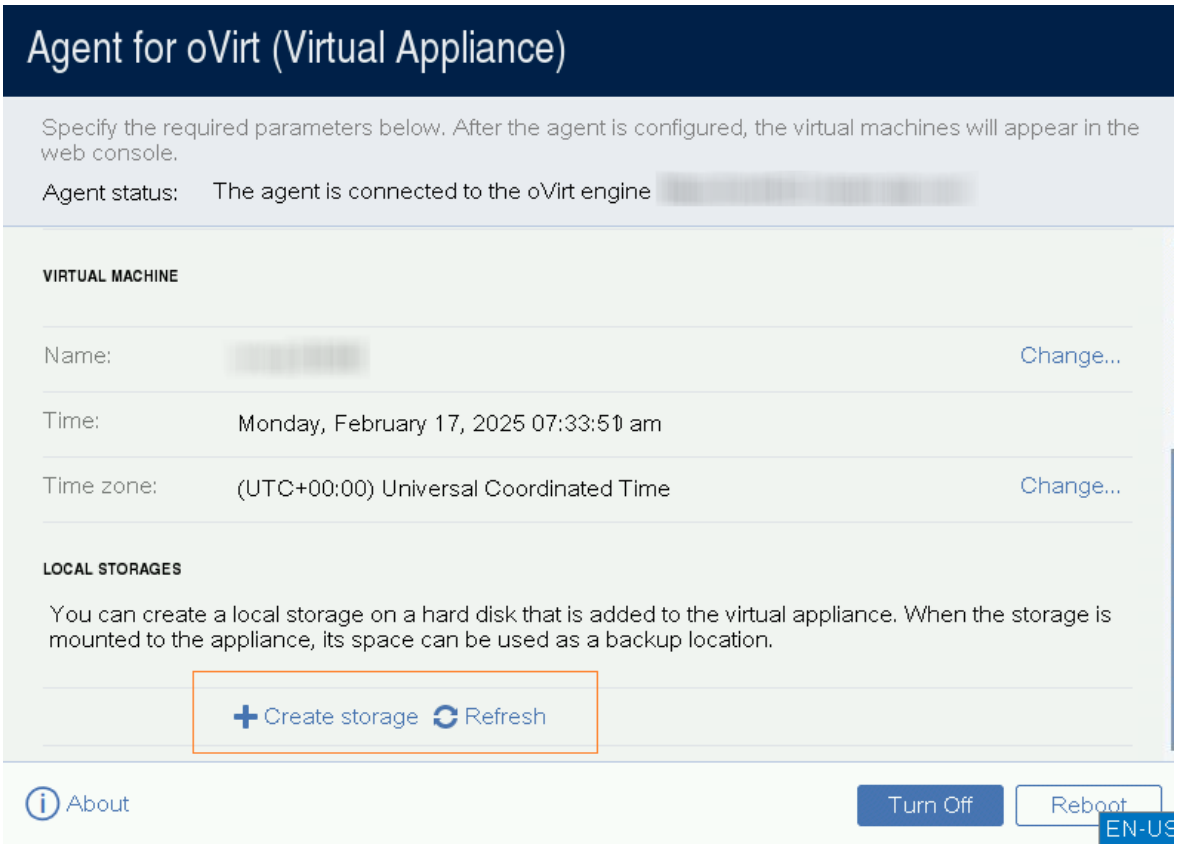
6.13.1.2 Настройка и подключение диска к виртуальному устройству

1. Установите виртуальное устройство (virtual appliance) для системы виртуализации oVirt/zVirt.
2. Убедитесь, что виртуальное устройство успешно подключено к системе виртуализации и серверу управления (CMS).
3. Добавьте новый диск к виртуальному устройству с помощью графического интерфейса oVirt/zVirt. Этот диск может быть представлен как диск iSCSI или FC. Размер диска должен составлять не менее 10 ГБ.

   Внимание
   Для виртуального устройства (virtual appliance) любой подключенный к нему диск представляется как Local Storages. Этот термин следует отличать от локального хранилища zVirt, которое не рекомендовано к использованию в продуктовой среде.

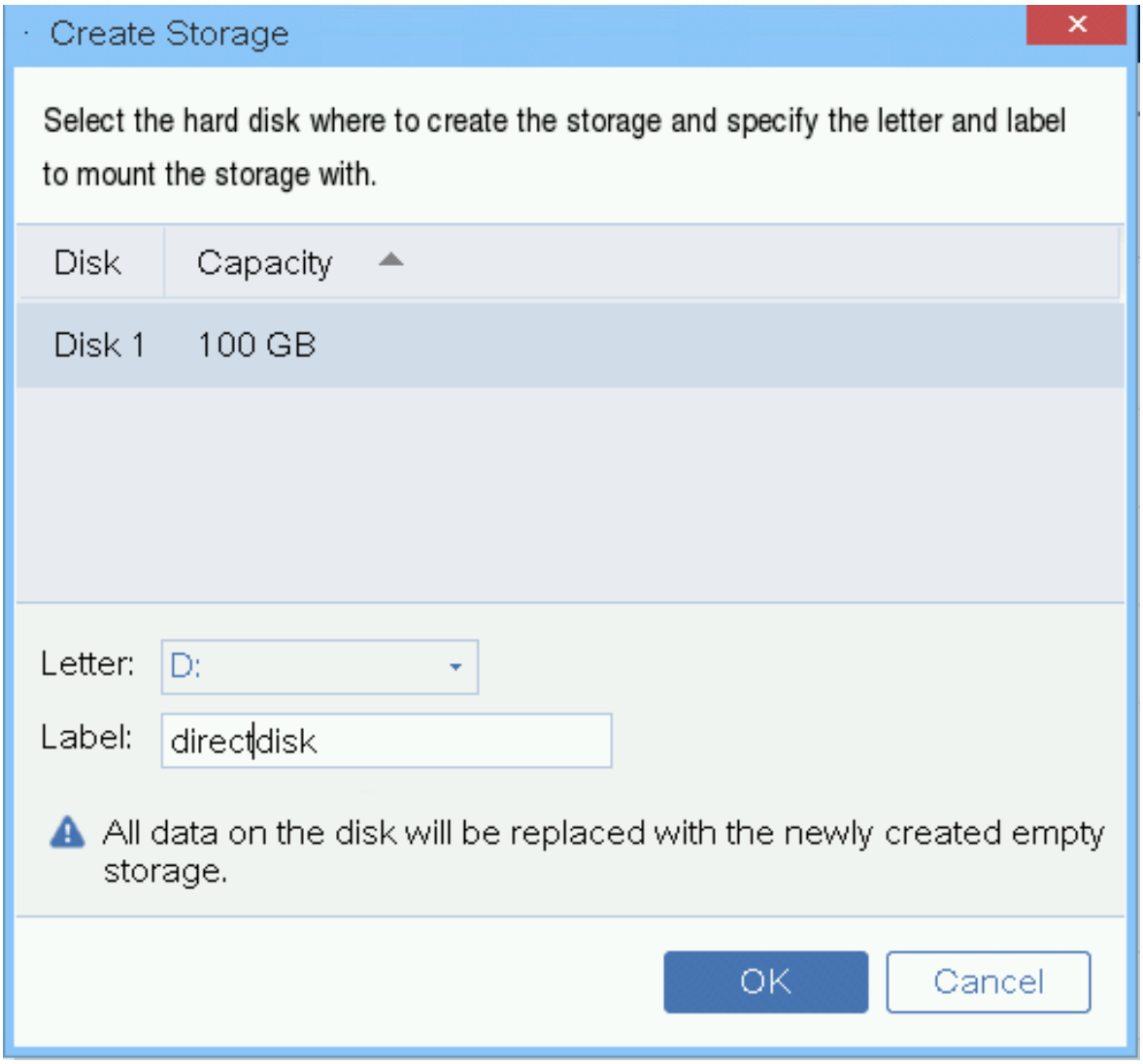
4. Перейдите в консоль виртуального устройства.
5. В веб-интерфейсе виртуального устройства в меню **Local Storages** нажмите на ссылку **Refresh**.

© ООО Киберпротект, 2026

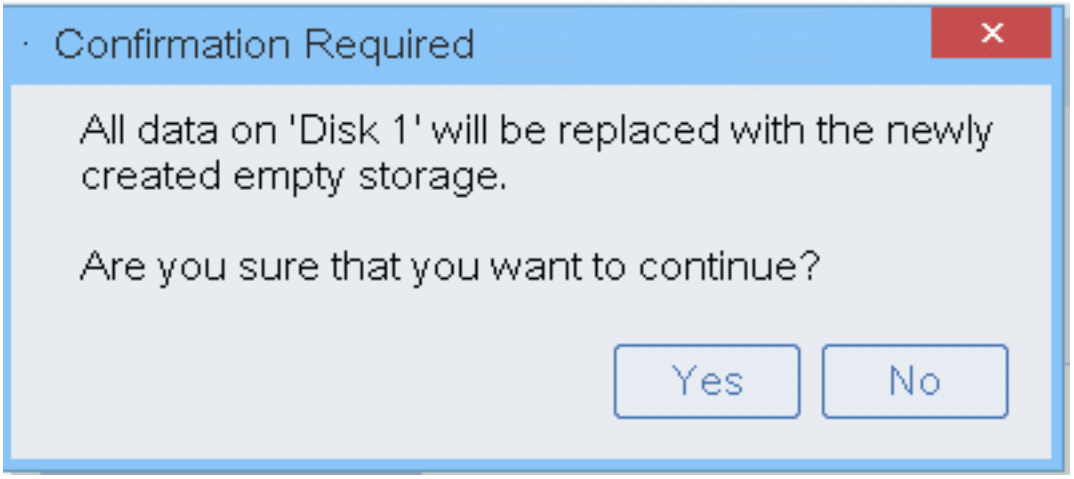


6. Ссылка **Create Storage** станет активной, нажмите на эту ссылку. Выберите диск и укажите для него метку. Длина метки ограничена 16 символами в связи с ограничениями файловой системы.

© ООО Киберпротект, 2026

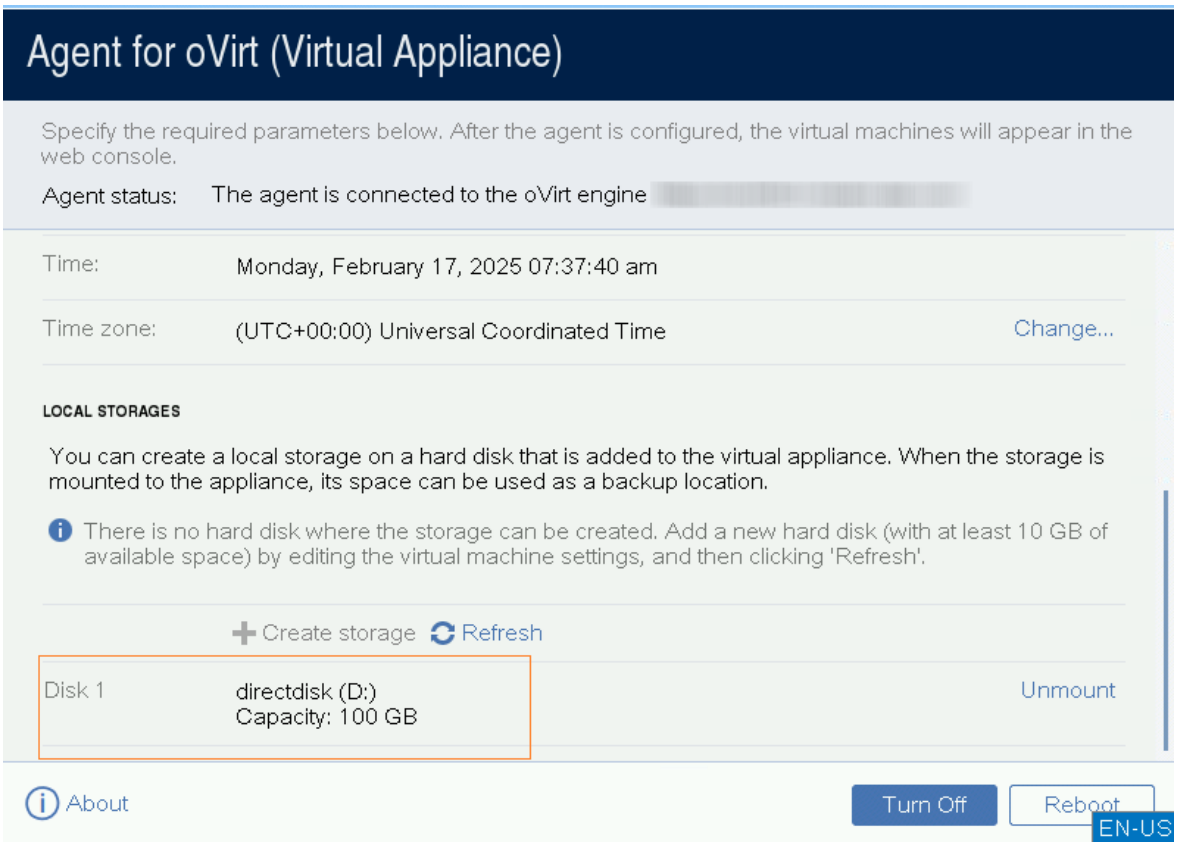


7. Подтвердите добавление диска.



8. В интерфейсе виртуального устройства убедитесь, что диск был успешно добавлен к виртуальному устройству.

© ООО Киберпротект, 2026

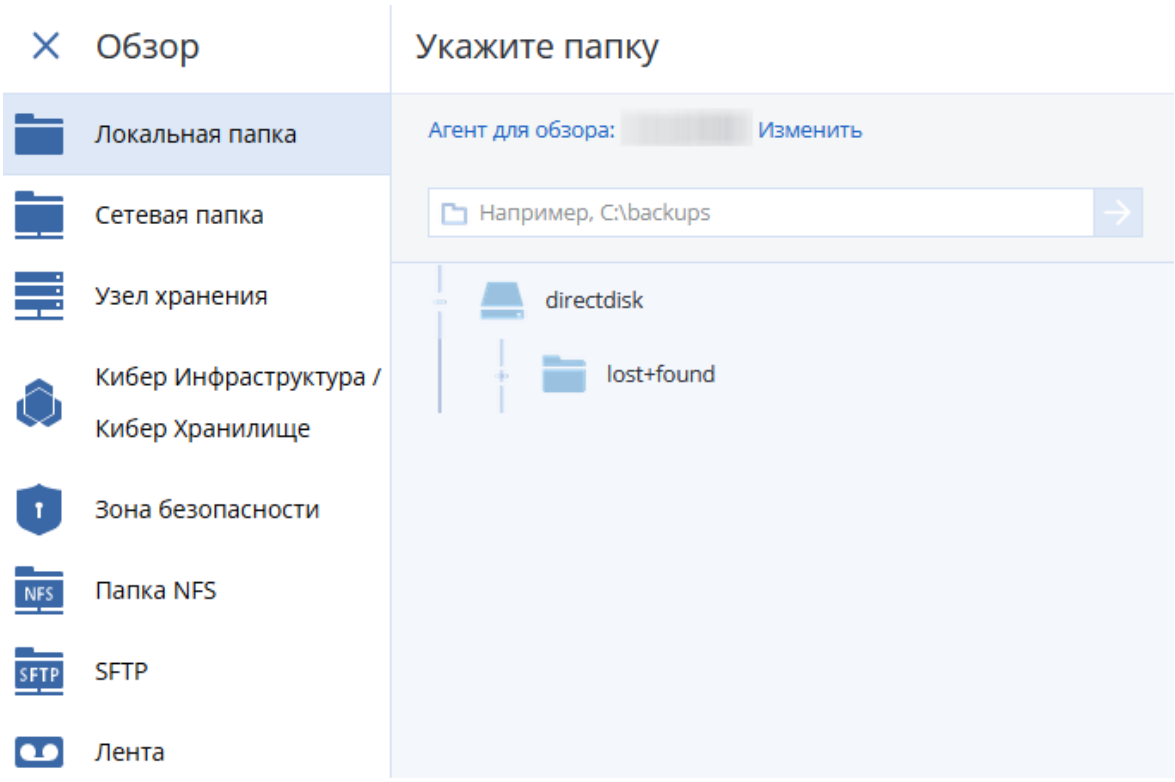


6.13.1.3 Подключение локального диска виртуального устройства в Кибер Бэкап

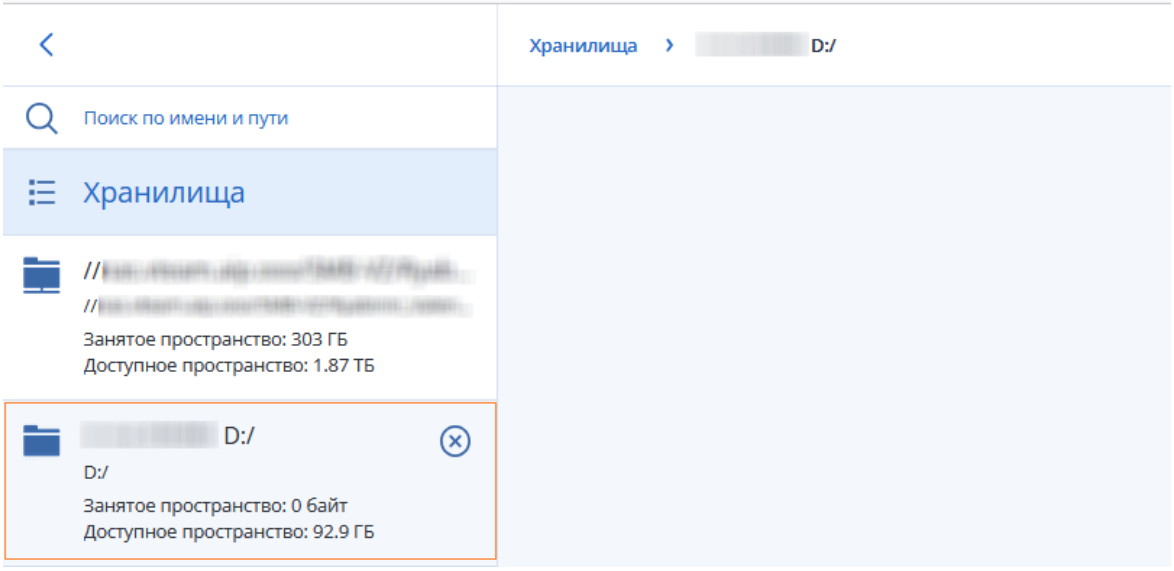
Для подключения выполните следующие действия:

1. Убедитесь, что виртуальное устройство (virtual appliance) установлено и подключено к oVirt/Zvirt.
2. В веб-консоли (Кибер Бэкап) перейдите в меню **Хранилище резервных копий** и на вкладке **Действия** выберите ссылку **Добавить хранилище**.
3. На вкладке **Обзор** рядом с **Агент для обзора** щелкните **Изменить**, выберите нужное виртуальное устройство и нажмите **OK**. Далее выберите **Локальная папка** и после отображения дерева подключенных дисков выберите необходимый диск на виртуальном устройстве.

© ООО Киберпротект, 2026



4. После успешного добавления в разделе **Хранилище резервных копий** отобразится новое хранилище для резервных копий.



6.13.2 Резервное копирование без использования локальной сети (LAN-free backup) для VMware

Резервное копирование виртуальных машин без использования локальной сети можно организовать с помощью виртуального устройства для VMware или Windows-агента для VMware. Подробные сведения см. в соответствующих подразделах.

© ООО Киберпротект, 2026

6.13.2.1 Резервное копирование без использования локальной сети посредством виртуального устройства для VMware

Схема резервного копирования без использования локальной сети

На этой схеме:

© ООО Киберпротект, 2026

- **ВМ CMS** – виртуальная машина с установленным сервером управления Кибер Бэкап (CMS);
- **Виртуальное устройство** – виртуальное устройство для взаимодействия с Кибер Бэкап и vCenter/ESXi;
- **ВМ** – целевая виртуальная машина для создания резервной копии, расположена в системе виртуализации VMware;
- **Узел** – ESXi-сервер;
- **------** – отображает подключение сети управления;
- **<------- >** – отображает направление трафика;
- **iSCSI, FC** – устройство хранения резервных копий;
- **Подключение диска к ВУ** – подключение диска к виртуальному устройству через настроенную сеть хранения данных в системе виртуализации (диск RDM).

При использовании этой схемы виртуальное устройство создает резервные копии виртуальных машин, получая данные из хранилищ данных VMware, которые размещены в СХД и подключены к ESX-серверу виртуального устройства через сеть хранения данных. Резервные копии размещаются на локальном диске виртуального устройства, который представляет собой отдельный LUN, доступный через сеть хранения данных и подключенный к виртуальному устройству как RDM-диск.

Предварительные требования

- Развернута и настроена сеть хранения данных (SAN) на основе iSCSI или Fibre Channel; к этой сети подключена система хранения данных (СХД).
- Серверы ESXi, помимо сети управления, также подключены к сети хранения данных.
- Хранилища данных VMware (datastores) для дисков виртуальных машин размещены в СХД.
- Для хранения резервных копий виртуальных машин в СХД выделена и экспортирована в виде LUN часть дискового пространства.

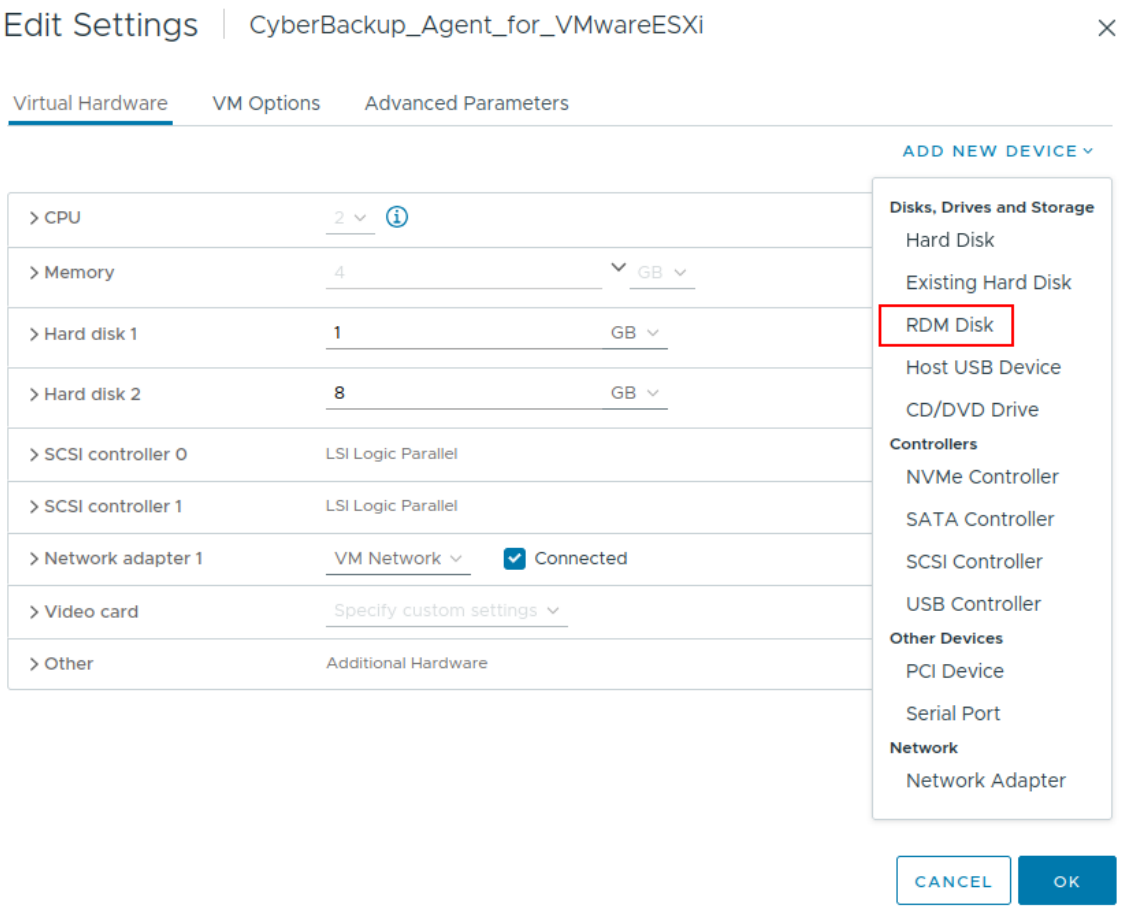
Настройка и подключение диска к виртуальному устройству

1. Создайте виртуальное устройство (virtual appliance) для системы виртуализации VMware.
2. Убедитесь, что виртуальное устройство успешно подключено к системе виртуализации и серверу управления (CMS).
3. Убедитесь, что ESX-сервер, на котором расположено виртуальное устройство, подключен к сети хранения данных.

   Примечание
   Для подключения к сети хранения данных на основе iSCSI на ESXi-сервере должен быть установлен программный iSCSI-адаптер, а для подключения к сети хранения данных на основе Fibre Channel – аппаратный HBA-адаптер.

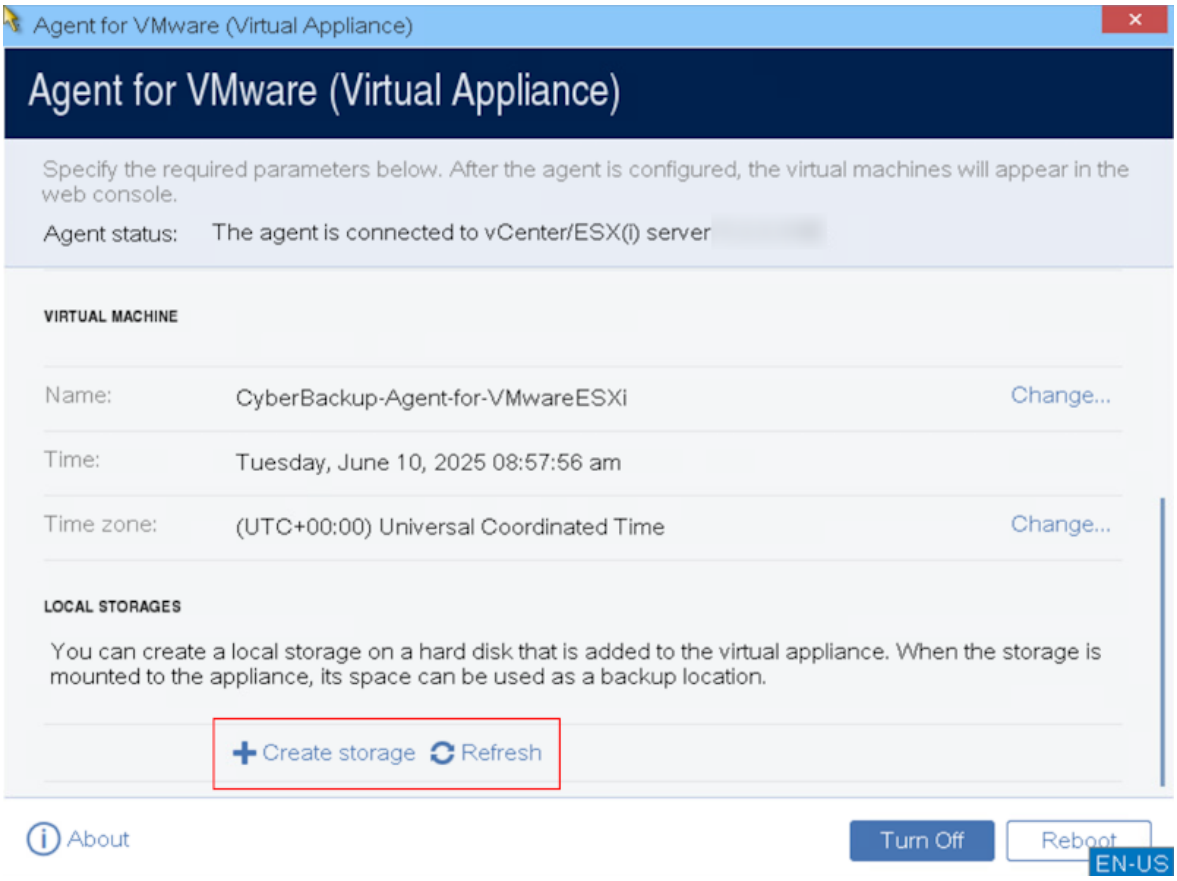
4. Подключите LUN, предназначенный для хранения резервных копий, к виртуальному устройству как RDM-диск с помощью веб-интерфейса vCenter/ESXi.

© ООО Киберпротект, 2026



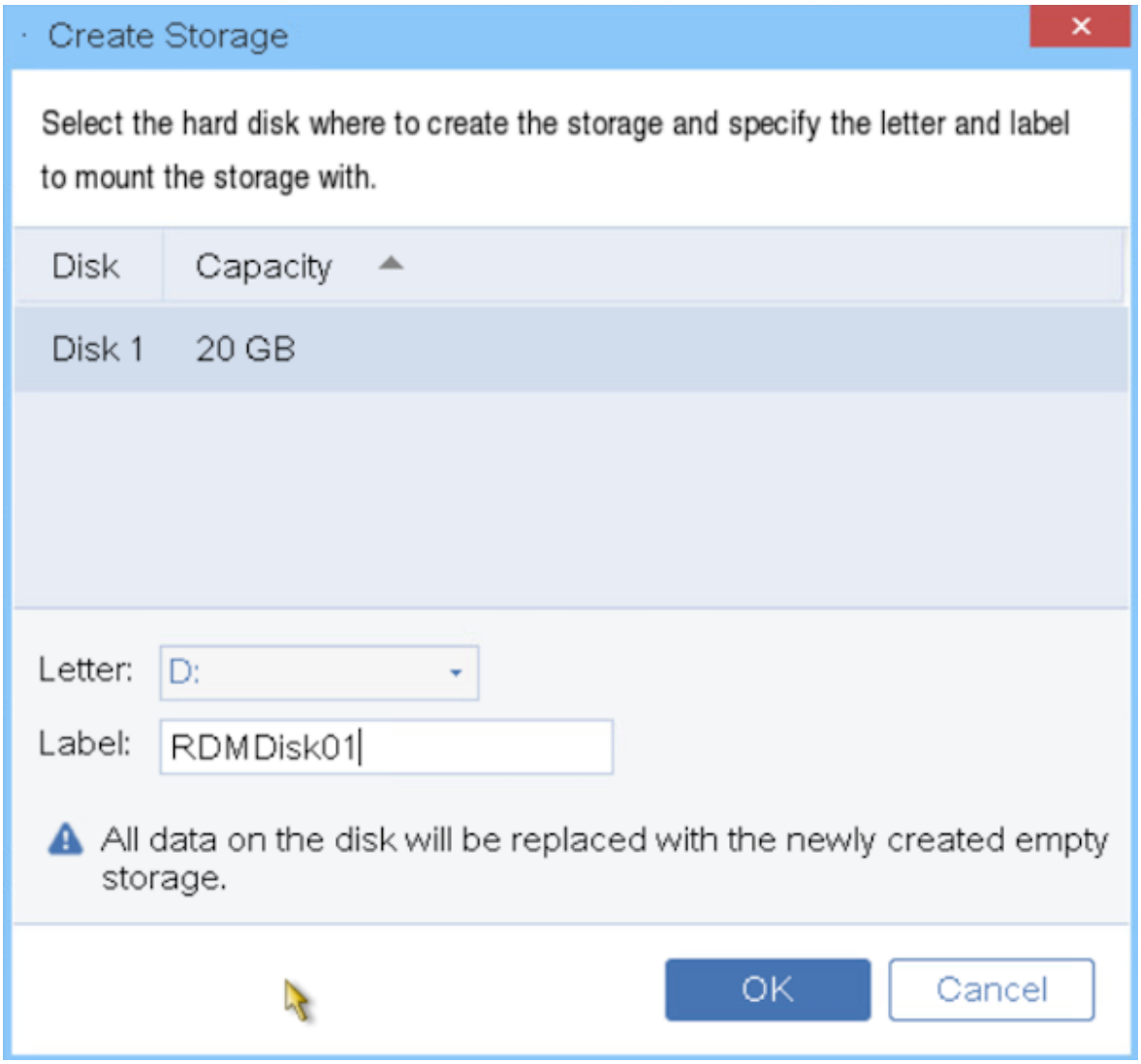
5. Перейдите в консоль виртуального устройства.
6. В интерфейсе виртуального устройства в разделе **Local Storages** нажмите **Refresh**.

© ООО Киберпротект, 2026

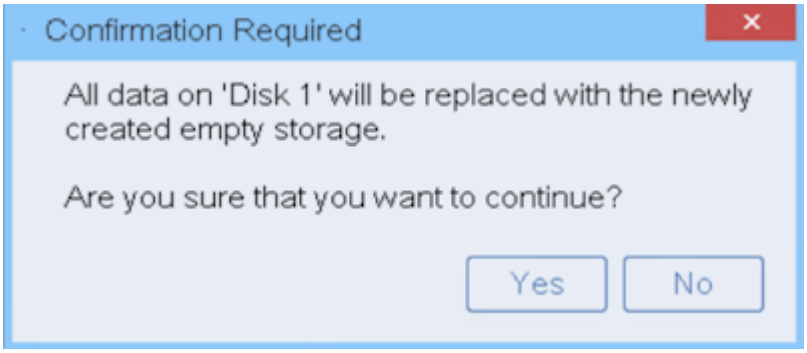


7. Когда ссылка **Create Storage** станет активной, нажмите на нее. Выберите диск и укажите для него метку. Длина метки ограничена 16 символами в связи с ограничениями файловой системы.

© ООО Киберпротект, 2026

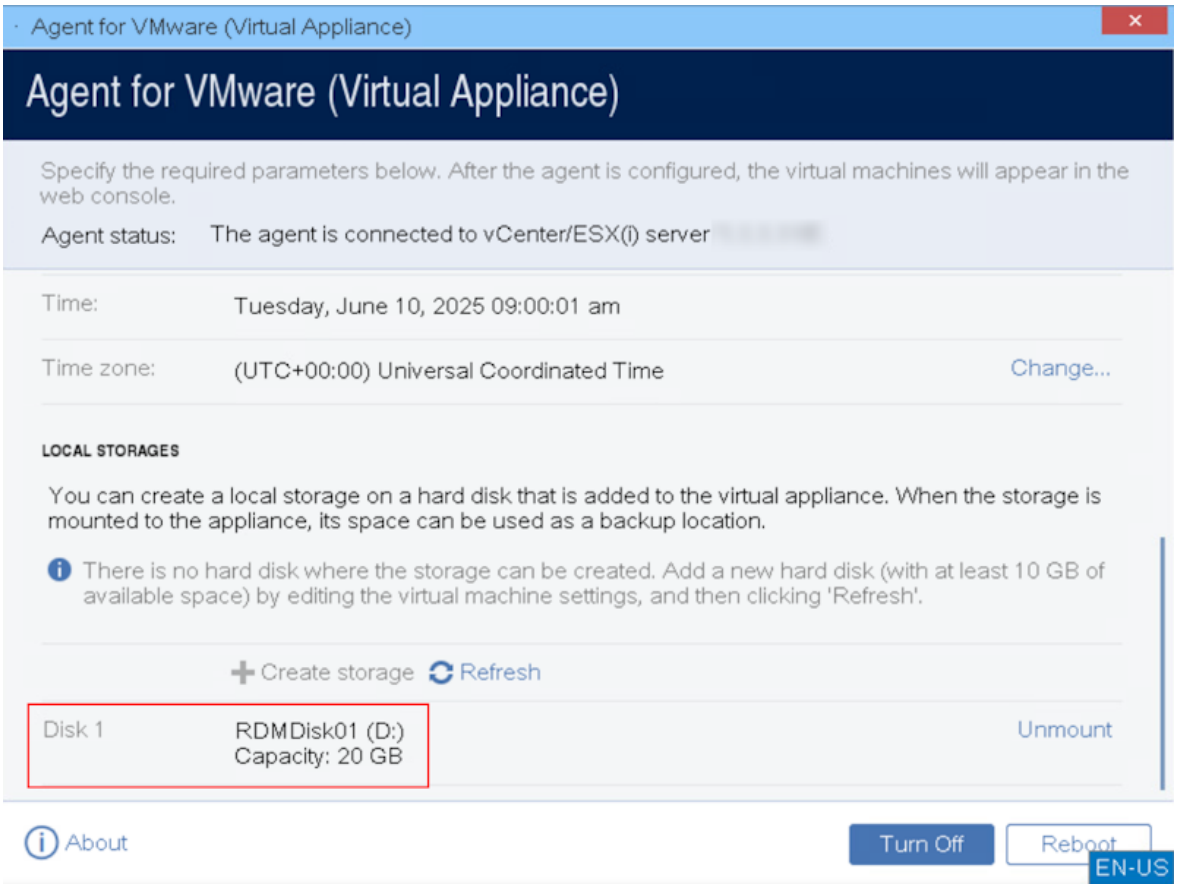


8. Подтвердите добавление диска.



9. В интерфейсе виртуального устройства убедитесь, что диск был успешно добавлен к виртуальному устройству.

© ООО Киберпротект, 2026

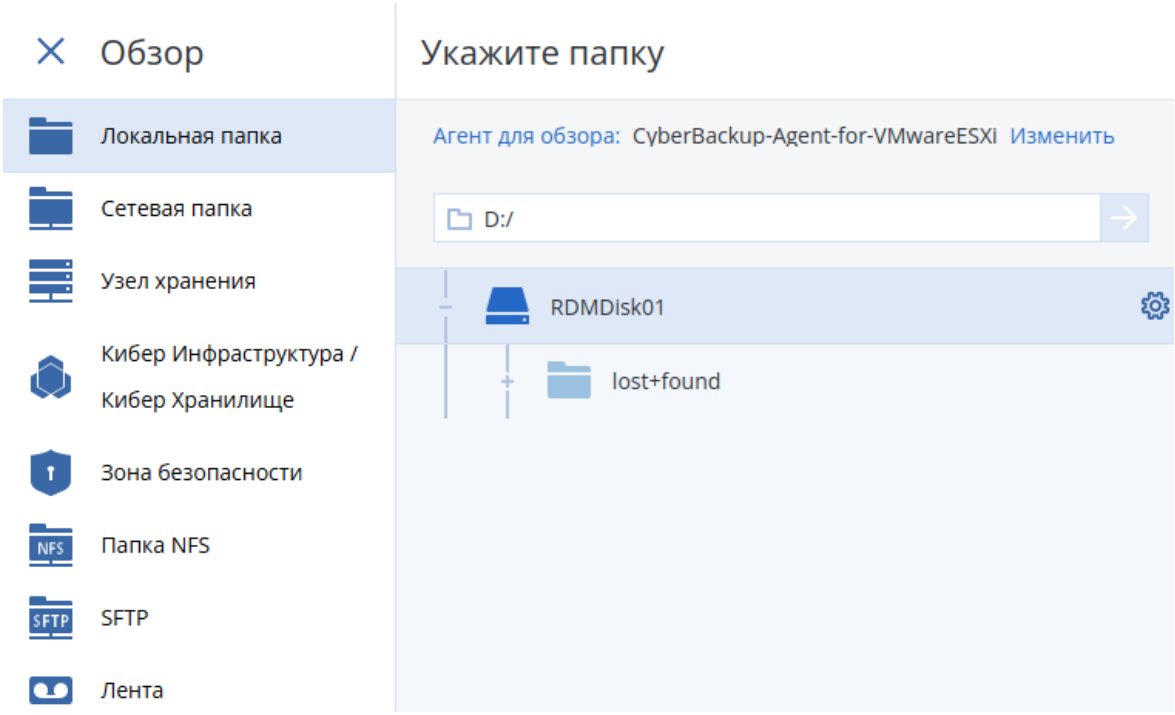


Подключение локального диска виртуального устройства в Кибер Бэкап

Для подключения выполните следующие действия:

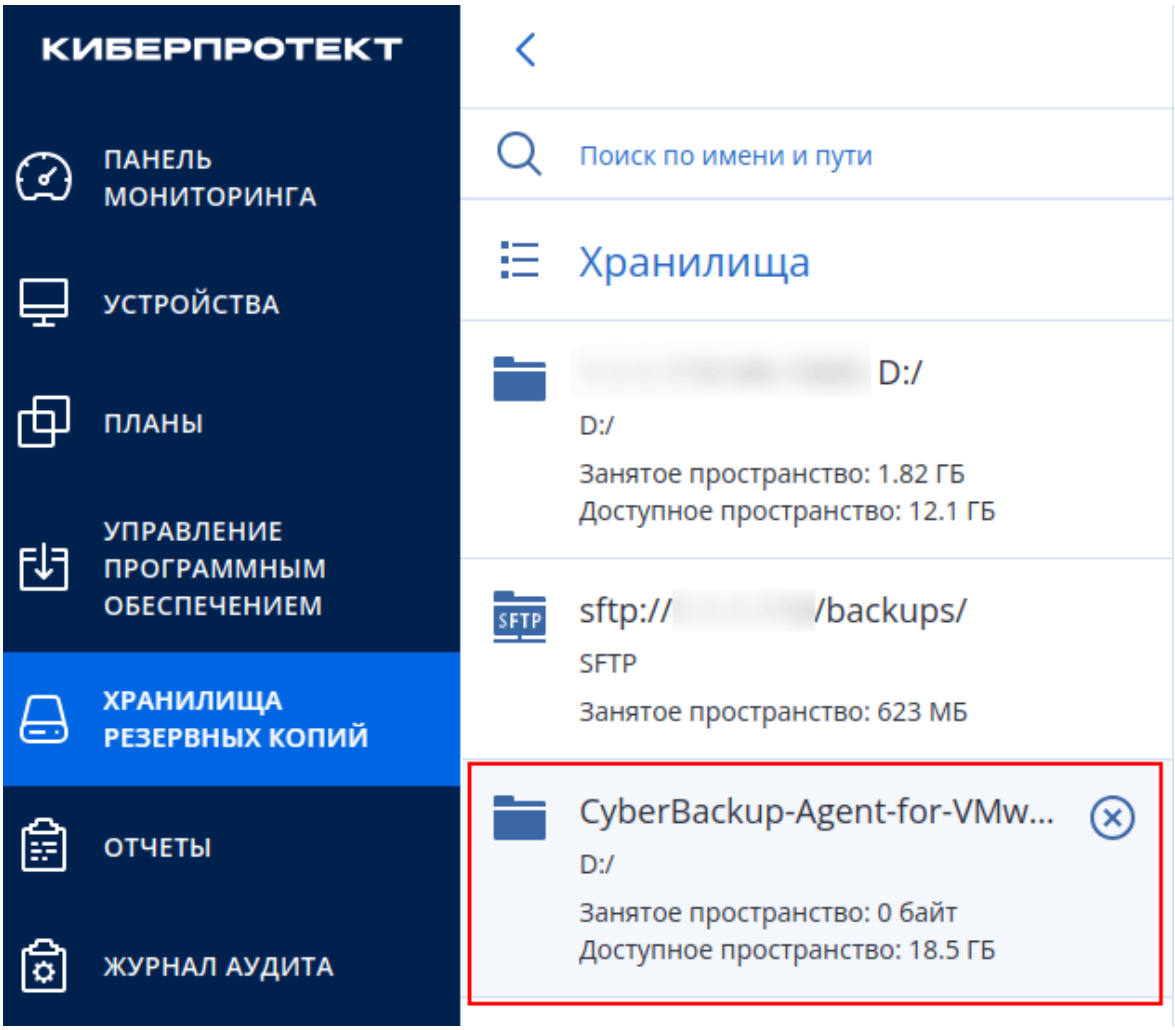
1. В веб-консоли Кибер Бэкап перейдите в раздел **Хранилища резервных копий** и на вкладке **Действия** щелкните ссылку **Добавить хранилище**.
2. На вкладке **Обзор** рядом с **Агент для обзора** щелкните **Изменить**, выберите нужное виртуальное устройство и нажмите **OK**. Далее выберите **Локальная папка** и после отображения дерева подключенных дисков выберите необходимый диск виртуального устройства.

© ООО Киберпротект, 2026



3. После успешного добавления в **Хранилища резервных копий** отобразится новое хранилище для резервных копий.

© ООО Киберпротект, 2026



Добавленное хранилище можно будет использовать в плане резервного копирования виртуальных машин, при исполнении которого данные будут передаваться только через сеть хранения данных.

Примечание
Резервное копирование в это хранилище может выполняться только тем виртуальным устройством (агентом), к которому подключен RDM-диск. Для других виртуальных устройств (агентов) хранилище недоступно.

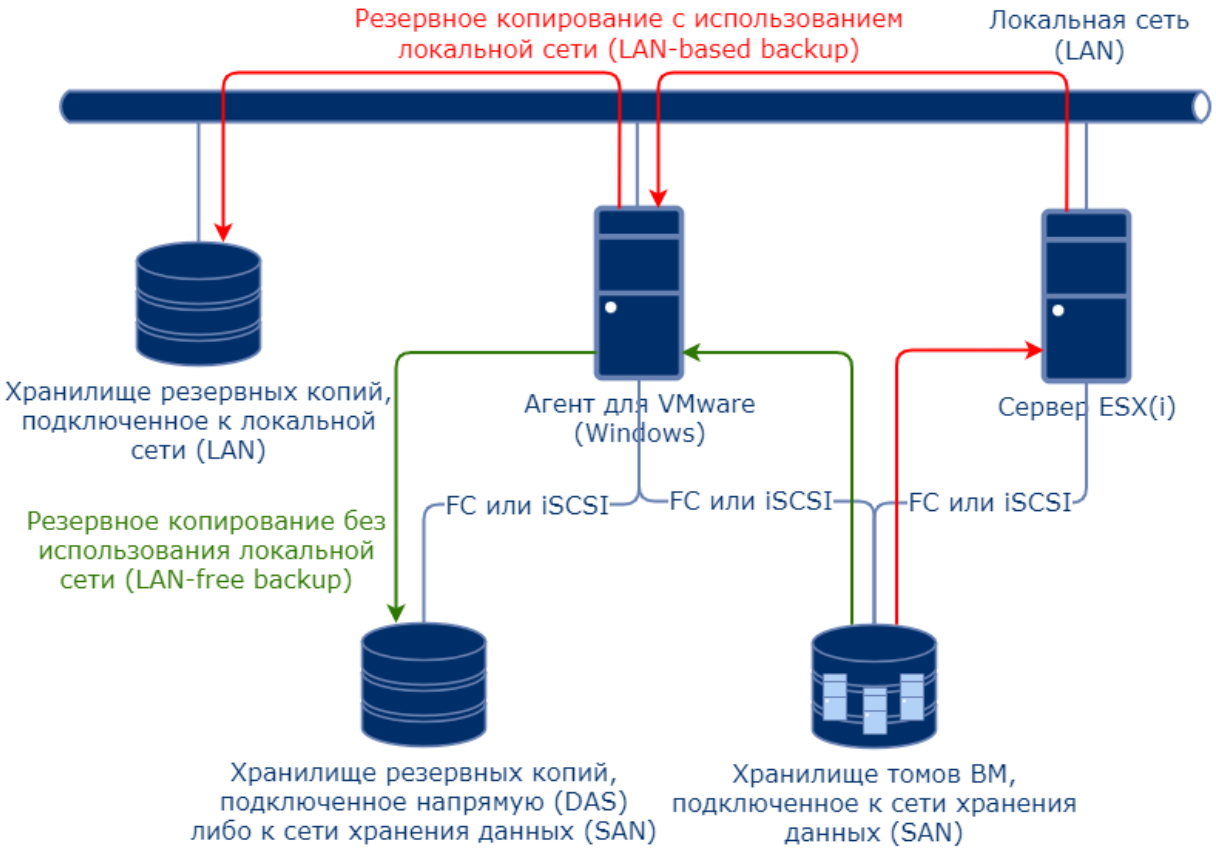
6.13.2.2 Резервное копирование без использования локальной сети посредством Windows-агента для VMware

Если нагрузка на производственные хосты ESXi слишком велика и запуск виртуальных устройств нежелателен, можно установить агент для VMware (Windows) на физическую машину за пределами инфраструктуры ESXi.

Если с ESXi используется SAN-хранилище, установите агент на машину, подключенную к той же сети SAN. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Эта возможность называется резервным копированием без использования локальной сети.

© ООО Киберпротект, 2026

На следующем рисунке показано резервное копирование с использованием и без использования локальной сети. Доступ к виртуальным машинам без использования локальной сети возможен при наличии оптоволоконного канала (FC) или сети хранения данных (SAN) iSCSI. Чтобы полностью исключить передачу резервных копий данных по локальной сети, храните резервные копии на локальном диске машины с установленным агентом или в присоединенном хранилище SAN.



Порядок включения прямого доступа к хранилищу данных для агента

1. Установите агент для VMware на машину Windows, на которой есть сетевой доступ к vCenter Server.
2. Подключите к машине логическое устройство, на котором расположено хранилище данных. Примите во внимание следующие соображения:
   - Используйте тот же протокол (iSCSI или FC), который использовался для подключения хранилища данных к ESXi.
   - Логическое устройство *не должно* инициализироваться. Вместо этого оно должно появиться как «автономный» диск в разделе **Управление дисками**. Если Windows инициализирует логическое устройство, оно может быть повреждено и стать нечитаемым для VMware vSphere.

     Чтобы избежать инициализации логического устройства, для параметра **Политика SAN** автоматически устанавливается значение **Перевод в автономное состояние всех ресурсов** во время установки агента для VMware (Windows).

© ООО Киберпротект, 2026

В результате агент будет использовать режим транспорта сети SAN для доступа к виртуальным дискам, т. е. он будет посекторно считывать секторы логического устройства по iSCSI/FC, не распознавая файловой системы VMFS (которая неизвестна для Windows).

Ограничения

- В vSphere агент не может использовать режим транспорта SAN, если одни диски ВМ расположены в VMware Virtual Volume (VVol), а другие – на других томах. Резервное копирование таких виртуальных машин приведет к сбою.
- Резервное копирование зашифрованных виртуальных машин (эта функциональная возможность представлена в VMware vSphere 6.5) будет выполняться по локальной сети, даже если настроен режим транспорта сети SAN для агента. Агент выполнит возврат из реплики, используя транспорт NBD, поскольку VMware не поддерживает транспорт сети SAN для резервного копирования зашифрованных виртуальных дисков.

Пример

Если используется сеть хранения данных (SAN) iSCSI, настройте инициатор iSCSI на машине с Windows, на которой установлен агент для VMware.

Настройка политики SAN

1. Войдите как администратор, откройте командную строку, введите diskpart и нажмите клавишу **Ввод**.
2. Введите san и нажмите клавишу **Ввод**. Убедитесь, что отображается **Политика SAN: Перевод в состояние "вне сети" общих ресурсов**.
3. Если для политики SAN задано другое значение:
   a. Введите san policy=offlineall.
   b. Нажмите клавишу **Ввод**.
   c. Чтобы проверить правильность применения настройки, выполните шаг 2.
   d. Перезапустите машину.

Настройка инициатора iSCSI

1. Последовательно выберите пункты **Панель управления** > **Администрирование** > **Инициатор iSCSI**.

   Примечание
   Чтобы найти приложение **Администрирование**, возможно, необходимо будет изменить представление **панели управления** на отличное от **Главная** или **Категория** или воспользоваться поиском.

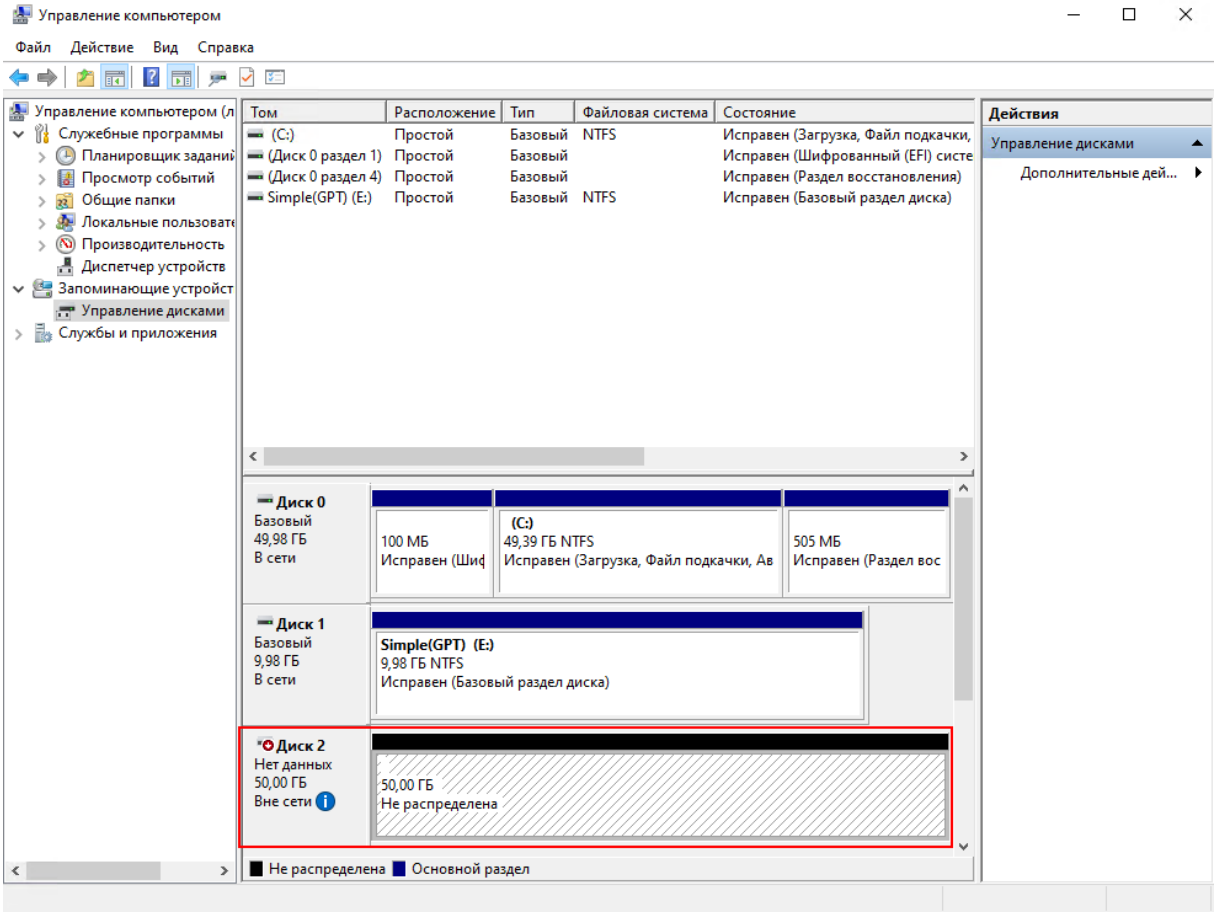
2. Если инициатор iSCSI Microsoft запускается впервые, подтвердите, что необходимо запустить службу инициатора iSCSI (Microsoft).
3. На вкладке **Цели** введите полное доменное имя или IP-адрес целевого устройства SAN и щелкните **Быстрое подключение**.

© ООО Киберпротект, 2026

4. Выберите логическое устройство, на котором расположено хранилище данных, и нажмите кнопку **Подключить**.

   Если логическое устройство не отображается, убедитесь, что распределение зон на целевом устройстве iSCSI позволяет машине, на которой выполняется агент, получить доступ к логическому устройству. Машину необходимо добавить в список разрешенных инициаторов iSCSI в этом целевом объекте.
5. Нажмите кнопку **OK**.

Готовое логическое устройство SAN должно появиться в разделе **Управление дисками**, как показано на снимке экрана ниже.



6.14 Параметры резервного копирования

Чтобы изменить параметры резервного копирования, щёлкните **Изменить** в меню действий с планом, затем в блоке **Параметры резервного копирования** нажмите **Изменить**.

6.14.1 Доступность параметров резервного копирования

Набор доступных параметров резервного копирования зависит от следующих факторов:

© ООО Киберпротект, 2026

- среда, в которой работает агент (Windows, Linux);
- тип данных, для которых выполняется резервное копирование (диски, файлы, виртуальные машины, данные приложения);
- место назначения резервной копии (локальная папка, сетевая папка и т. д.).

В следующих таблицах представлены обобщенные сведения по доступности параметров резервного копирования.

Параметр резервного копирования	СУБД			Резервное копирование на уровне файлов и дисков		
	PostgreSQL	MySQL	БД Microsoft Exchange Server	Windows	Linux	ESXi
"Функция Changed Block Tracking (CBT)" (стр. 349)	-	-	-	-	-	-
"Быстрое инкрементное/дифференциальное резервное копирование" (стр. 355)	-	-	-	-	-	-
"Действие при сбое плана" (стр. 378)	-	+	+	+	+	-
"Деление" (стр. 371)	+	+	+	+	+	-
"Еженедельное резервное копирование" (стр. 381)	+	+	+	+	+	+
"Журнал событий Windows" (стр. 381)	-	+	+	+	+	-
"Имя файла резервной копии" (стр. 343)	+	+	+	+	+	+
"Команды до и после процедуры" (стр. 365)	+	+	+	+	+	-
"Команды до и после захвата данных" (стр. 367)	-	-	-	-	-	-
"Консолидация резервных копий" (стр. 342)	-	+	+	+	+	+
"Многотомные моментальные снимки" (стр. 360)	-	-	-	-	-	-

© ООО Киберпротект, 2026

"Создание моментальных снимков LVM" (стр. 359)	-	-	-	-	-	-
"Моментальные снимки оборудования SAN" (стр. 370)	-	-	-	-	-	-
"Многопоточность" (стр. 352)	+	-	-	-	-	-
"Обработка ошибок" (стр. 354)	-	+	+	+	+	+
"Оповещения" (стр. 341)	-	+	+	+	+	+
"Планирование" (стр. 370)	-	-	-	-	-	-
"Посекторное резервное копирование" (стр. 371)	-	-	-	-	-	-
"Проверка резервных копий" (стр. 348)	-	+	+	+	+	+
"Производительность и окно резервного копирования" (стр. 361)	-	+	+	+	+	-
"Служба теневого копирования томов (VSS)" (стр. 379)	-	-	-	-	-	-
"Служба теневого копирования томов (VSS) для виртуальных машин" (стр. 380)	-	-	-	-	-	-
"Уведомления по электронной почте" (стр. 353)	-	+	+	+	+	+
"Уровень сжатия" (стр. 352)	+	+	+	+	+	+
"Условия запуска задания" (стр. 378)	-	+	+	+	+	+
"Фильтры файлов" (стр. 356)	-	-	-	-	-	-
"Управление лентами" (стр. 372)	+	+	+	+	+	+
"Способ резервного копирования кластера" (стр. 350)	+	-	+	-	-	-

© ООО Киберпротект, 2026

Резервное копирование приложений	-	+	-	-	-	-
Кластер почтовых агентов	-	-	-	-	-	-
Преобразование в виртуальную машину	-	-	-	Только для резервного копирования на уровне дисков.	Только для резервного копирования на уровне дисков.	Только для резервного копирования на уровне дисков.

Параметр резервного копирования	**Физические и виртуальные машины**					
	VMware, Hyper-V	**oVirt**	**OpenStack**	**OpenNebula**	**ECP VeiL, SpaceVM**	**Basis DynamiX Enterprise**
"Функция Changed Block Tracking (CBT)" (стр. 349)	+	+	+	+	+	+
"Быстрое инкрементное/дифференциальное резервное копирование" (стр. 355)	+	+	+	+	+	+
"Действие при сбое плана" (стр. 378)	+	+	+	+	+	+
"Деление" (стр. 371)	+	+	+	+	+	+
"Еженедельное резервное копирование" (стр. 381)	+	+	+	+	+	+
"Журнал событий Windows" (стр. 381)	+	+	+	+	+	+
"Имя файла резервной копии" (стр. 343)	+	+	+	+	+	+
"Команды до и после процедуры" (стр. 365)	+	+	+	+	+	+
"Команды до и после захвата данных" (стр. 367)	+	+	+	+	+	+
"Консолидация резервных копий" (стр. 342)	-	-	-	-	-	-
"Многотомные моментальные снимки" (стр. 360)	+	+	+	+	+	+

© ООО Киберпротект, 2026

"Создание моментальных снимков LVM" (стр. 359)	+	+	+	+	+	+
"Моментальные снимки оборудования SAN" (стр. 370)	+	+	+	+	+	+
"Многопоточность" (стр. 352)	-	-	-	-	-	-
"Обработка ошибок" (стр. 354)	+	+	+	+	+	+
"Оповещения" (стр. 341)	+	+	+	+	+	+
"Планирование" (стр. 370)	+	+	+	+	+	+
"Посекторное резервное копирование" (стр. 371)	+	+	+	+	+	+
"Проверка резервных копий" (стр. 348)	+	+	+	+	+	+
"Производительность и окно резервного копирования" (стр. 361)	+	+	+	+	+	+
"Служба теневого копирования томов (VSS)" (стр. 379)	+	+	+	+	+	+
"Служба теневого копирования томов (VSS) для виртуальных машин" (стр. 380)	+	+	+	+	+	+
"Уведомления по электронной почте" (стр. 353)	+	+	+	+	+	+
"Уровень сжатия" (стр. 352)	+	+	+	+	+	+
"Условия запуска задания" (стр. 378)	+	+	+	+	+	+
"Фильтры файлов" (стр. 356)	+	+	+	+	+	+
"Управление лентами" (стр. 372)	+	+	+	+	+	+
"Способ резервного копирования кластера" (стр. 350)	-	-	-	-	-	-
Резервное копирование приложений	-	-	-	-	-	-
Кластер почтовых агентов	-	-	-	-	-	-
Преобразование в виртуальную машину	+	+	+	+	+	+

© ООО Киберпротект, 2026

Параметр резервного копирования	Приложения			
	VK WorkMail	CommuniGate Pro	Почтовые ящики Microsoft Exchange Server	Kubernetes
"Функция Changed Block Tracking (CBT)" (стр. 349)	-	-	-	-
"Быстрое инкрементное/дифференциальное резервное копирование" (стр. 355)	-	-	-	-
"Действие при сбое плана" (стр. 378)	-	-	+	-
"Деление" (стр. 371)	+	-	+	+
"Еженедельное резервное копирование" (стр. 381)	+	+	+	+
"Журнал событий Windows" (стр. 381)	-	-	+	-
"Имя файла резервной копии" (стр. 343)	+	+	+	+
"Команды до и после процедуры" (стр. 365)	-	-	+	-
"Команды до и после захвата данных" (стр. 367)	-	-	-	-
"Консолидация резервных копий" (стр. 342)	-	-	-	-
"Многотомные моментальные снимки" (стр. 360)	-	-	-	-
"Создание моментальных снимков LVM" (стр. 359)	-	-	-	-
"Моментальные снимки оборудования SAN" (стр. 370)	-	-	-	-
"Многопоточность" (стр. 352)	-	-	-	-
"Обработка ошибок" (стр. 354)	-	+	+	+
"Оповещения" (стр. 341)	-	-	+	-
"Планирование" (стр. 370)	-	-	-	-
"Посекторное резервное	-	-	-	-

© ООО Киберпротект, 2026

копирование" (стр. 371)				
"Проверка резервных копий" (стр. 348)	-	-	+	-
"Производительность и окно резервного копирования" (стр. 361)	-	-	+	-
"Служба теневого копирования томов (VSS)" (стр. 379)	-	-	-	-
"Служба теневого копирования томов (VSS) для виртуальных машин" (стр. 380)	-	-	-	-
"Уведомления по электронной почте" (стр. 353)	-	-	+	-
"Уровень сжатия" (стр. 352)	+	+	+	+
"Условия запуска задания" (стр. 378)	-	-	+	-
"Фильтры файлов" (стр. 356)	-	-	-	-
"Управление лентами" (стр. 372)	+	-	+	+
"Способ резервного копирования кластера" (стр. 350)	-	-	-	-
Резервное копирование приложений	-	-	-	-
Кластер почтовых агентов	+	+	-	-
Преобразование в виртуальную машину	-	-	-	-

6.14.2 Оповещения

6.14.2.1 За указанное количество дней подряд не создано успешно ни одной резервной копии.

Значение по умолчанию: **Отключено**.

Этот параметр определяет, будет ли создаваться оповещение, если за указанный период времени планом защиты не будет успешно создано ни одной резервной копии. Помимо процессов резервного копирования, которые завершились сбоем, программа считает резервные копии, которые не выполняются по расписанию (отсутствующие резервные копии).

Оповещения создаются для конкретной машины и отображаются на вкладке **Оповещения**.

Можно задать количество дней подряд без созданных резервных копий. По истечении указанного периода будет сформировано уведомление.

© ООО Киберпротект, 2026

6.14.3 Консолидация резервных копий

Этот параметр определяет, нужно ли консолидировать резервные копии при очистке или при полном удалении цепочек резервных копий.

Значение по умолчанию: **Отключено**.

Консолидация – это процесс объединения двух и более последовательных резервных копий в одну резервную копию.

Если этот параметр включен, то резервная копия, которая должна быть удалена при очистке, консолидируется со следующей зависимой резервной копией (инкрементная или дифференциальная).

В противном случае данная резервная копия сохраняется до тех пор, пока все зависимые резервные копии не станут предметом для удаления. Это поможет избежать потенциально долгой консолидации, но требует дополнительного пространства для хранения резервных копий, удаление которых откладывается. Возраст или количество резервных копий могут превысить значения, заданные в правилах хранения.

Внимание
Необходимо учитывать, что консолидация – это просто один из методов удаления, но не альтернатива удалению. Итоговая резервная копия не будет содержать данные, которые присутствовали в удаленной резервной копии и отсутствовали в оставшейся инкрементной или дифференциальной резервной копии.

Этот параметр *не действует* в любом из следующих случаев:

- Местом сохранения резервной копии является ленточное устройство.
- Используется схема резервного копирования **Всегда инкрементное**.
- Используется формат резервной копии **Версии 12**.

Резервные копии, хранимые на лентах, невозможно консолидировать. Резервные копии, сохраненные в виде одного файла (форматы версий 11 и 12) всегда консолидированы, поскольку их внутренняя структура позволяет ускорить и упростить консолидацию.

Однако если используется формат версии 12 и при этом есть несколько цепочек резервных копий (каждая цепочка хранится в отдельном файле), консолидация работает только для последней цепочки. Все цепочки, за исключением первой, удаляются. Первая цепочка сжимается до минимально необходимого размера для хранения метаданных (~12 КБ). Эти метаданные требуются, чтобы обеспечить согласованность данных при одновременном выполнении операций чтения и записи. Сразу же после применения правила хранения резервные копии, входящие в эти цепочки, исчезают из графического интерфейса пользователя, хотя физически они существуют до удаления всей цепочки.

Во всех остальных случаях резервные копии, удаление которых отложено, помечаются значком корзины (

© ООО Киберпротект, 2026

) в графическом пользовательском интерфейсе. Если удалить такую резервную копию, щелкнув значок X, будет выполнена консолидация. Резервные копии, которые хранятся на ленточном накопителе, удаляются из графического интерфейса пользователя только при перезаписи или удалении данных на ленте.

6.14.4 Имя файла резервной копии

Этот параметр определяет имена файлов резервных копий, создаваемые планом защиты.

Эти имена можно увидеть в диспетчере файлов при обзоре хранилища резервной копии.

6.14.4.1 Что такое файл резервной копии?

В зависимости от схемы резервного копирования и используемого формата резервной копии каждый план защиты создает один или несколько файлов в хранилище резервной копии. В следующей таблице перечислены файлы, которые могут быть созданы на каждой машине или почтовом ящике.

	Всегда инкрементное	**Другие схемы резервного копирования**
Формат резервной копии **Версии 11**	Один файл TIB и один файл метаданных XML	Несколько файлов TIB и один файл метаданных XML (традиционный формат)
Формат резервной копии **Версии 12**	Один файл TIBX на каждую цепочку резервных копий (полное или дифференциальное резервное копирование и все зависящие от них инкрементные резервные копии).	

Все файлы имеют одинаковое имя с добавлением метки времени или порядкового номера, или без них. При создании или редактировании плана защиты можно задать такое имя (называемое именем файла резервной копии).

Примечание
Метка времени добавляется в имя файла резервной копии только в формате резервного копирования "Версия 11".

После изменения имени файла резервной копии следующей будет полная резервная копия, если не указано имя файла существующей резервной копии той же машины. В последнем случае будет создана полная, инкрементная или дифференциальная резервная копия в соответствии с расписанием плана защиты.

Обратите внимание, что можно задать имена файлов резервных копий для хранилищ, обзор которых невозможно выполнить с помощью диспетчера файлов (например, ленточного устройства). Это целесообразно в том случае, если требуется просмотр пользовательских имен на вкладке **Хранилища резервных копий**.

© ООО Киберпротект, 2026

6.14.4.2 Где можно просмотреть имена файлов резервных копий?

Выберите вкладку **Хранилища резервных копий**, а затем выберите группу резервных копий.

- Имя файла по умолчанию отображаются на панели **Подробности**.
- Если имена файлов заданы не по умолчанию, они отобразятся непосредственно на вкладке **Хранилища резервных копий** в столбце **Имя**.

6.14.4.3 Ограничения для имени файла резервной копии

- Имя файла резервной копии не должно заканчиваться цифрой.

  Чтобы имя не заканчивалось цифрой, в конце имени резервной копии по умолчанию добавляется буква «A». При создании пользовательского имени убедитесь, что оно не заканчивается цифрой. При использовании переменных имя не должно заканчиваться на переменную, поскольку она может заканчиваться цифрой.
- Имя файла резервной копии не должно содержать следующие символы: **()&?*$<>»:\|/#%**, символы окончания строки (**\n**) и знаки табуляции (**\t**).

6.14.4.4 Имя файла резервной копии по умолчанию

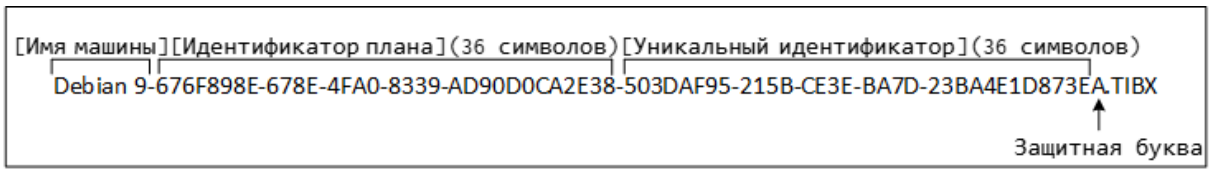
Имя файла резервной копии по умолчанию имеет вид [Имя машины]-[Идентификатор плана]-[Уникальный идентификатор]A.

Имя файла резервной копии по умолчанию для почтового ящика имеет вид [Идентификатор почтового ящика]_почтовый ящик_[Идентификатор плана]A.

Имя состоит из следующих переменных:

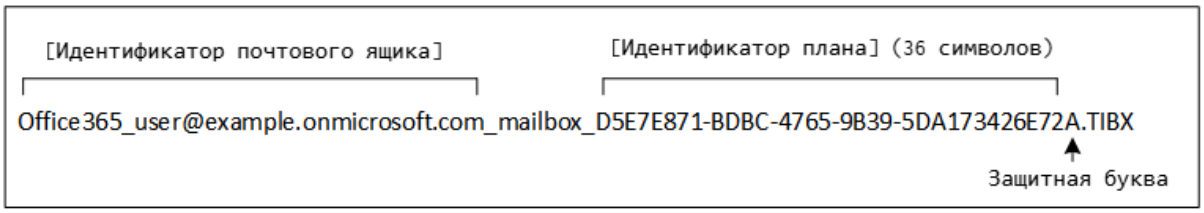
- [Имя машины] Эта переменная заменяется именем машины (такое же имя отображается на веб-консоли Кибер Бэкап) для всех типов резервных копий данных.
- [Идентификатор плана] Эта переменная заменяется уникальным идентификатором плана защиты. При переименовании плана это значение не изменяется.
- [Уникальный идентификатор] Эта переменная заменяется уникальным идентификатором выбранной машины или почтового ящика. При изменении имени машины или UPN почтового ящика это значение не изменяется.
- [Идентификатор почтового ящика] Эта переменная заменяется UPN почтового ящика.
- Защитная буква «A» добавляется для того, чтобы имя файла не заканчивалось цифрой.

На приведенной ниже диаграмме показано имя по умолчанию файла резервной копии.



© ООО Киберпротект, 2026

На приведенной ниже диаграмме показано имя по умолчанию файла резервной копии для почтового ящика.



6.14.4.5 Имена без переменных

Если вы измените имя файла резервной копии на MyBackup, файлы резервной копии будут выглядеть как в следующих примерах. Оба примера предполагают, что ежедневные инкрементальные резервные копирования запланированы в 14:40, начиная с 13 сентября 2016 года.

Для формата "Версия 12" со схемой резервного копирования **Всегда инкрементное**:

```
MyBackup.tibx
```

Для формата "Версии 12" с другими схемами резервного копирования:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Для формата "Версия 11" со схемой резервного копирования **Всегда инкрементное**:

```
MyBackup.xml
MyBackup.tib
```

Для формата "Версии 11" с другими схемами резервного копирования:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

6.14.4.6 Использование переменных

Кроме переменных, используемых по умолчанию, можно использовать переменную [Имя плана], которая заменяется именем плана защиты.

Если выбрано резервное копирование нескольких машин или почтовых ящиков, имя файла резервной копии должно содержать переменную [Имя машины], [Идентификатор почтового ящика] или [Уникальный идентификатор].

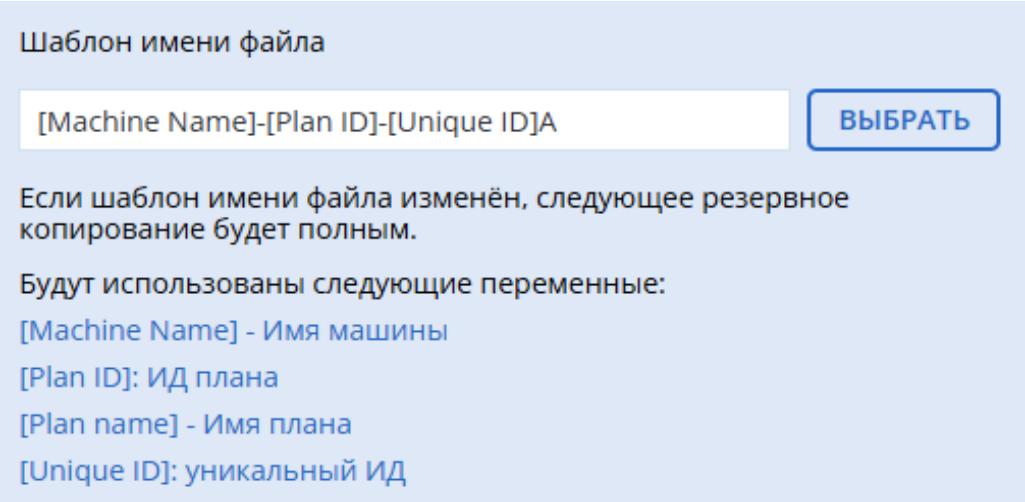
© ООО Киберпротект, 2026

6.14.4.7 Сравнение имени файла резервной копии и упрощенного именования файлов

Используя обычный текст и/или переменные можно создать такие же имена файлов, как и в более ранних версиях Кибер Бэкап. Однако упрощенные имена файлов не могут быть созданы заново – в версии 12 имя файла содержит отметку времени, если не используется формат одного файла.

6.14.4.8 Примеры использования

- **Просмотр дружественных к пользователю имен файлов**
  При обзоре хранилища с помощью диспетчера файлов легко отличить резервные копии.
- **Продолжение существующей последовательности резервных копий**
  Предположим, что план защиты применен к одной машине и необходимо удалить эту машину из веб-консоли Кибер Бэкап или удалить агент вместе с его настройками конфигурации. После повторного добавления машины или переустановки агента можно применить план защиты для продолжения выполнения резервного копирования в ту же резервную копию или последовательность резервных копий. Просто перейдите к этому параметру, щелкните **Выбрать** и выберите требуемую резервную копию.
  Кнопка **Обзор** позволяет показать резервные копии в хранилище, выбранном в разделе **Место сохранения резервной копии** на панели плана защиты. Обзор невозможно выполнить за пределами этого хранилища.



- **Переход с предыдущих версий продукта**
  Если при обновлении плана защиты до новой версии он не был автоматически перенесен, создайте план заново и примените его к старому файлу резервной копии. Если для резервного копирования выбрана только одна машина, щелкните **Обзор** и выберите требуемую резервную копию. Если для резервного копирования выбраны несколько машин, заново создайте старое имя файла резервной копии с использованием переменных.

© ООО Киберпротект, 2026

Примечание
Кнопка **Выбрать** доступна только для планов защиты, которые созданы и применены для одного устройства.

6.14.5 Формат резервной копии

Этот параметр показывает формат резервных копий, созданных планом защиты. Он доступен только для уже созданных планов защиты, в которых для сохранения резервных копий используются управляемые хранилища с защитой паролем (см. раздел "Защита хранилища паролем" (стр. 189)) или с включенной дедупликацией (см. раздел "Дедупликация" (стр. 189)).

Существуют следующие форматы:

- **Версия 12**. Формат, который используется по умолчанию во всех сценариях резервного копирования и восстановления, кроме сценария с сохранением резервных копий в управляемые хранилища с защитой паролем или с включенной дедупликацией.
- **Версия 11**. Этот формат выбирается автоматически, если местом сохранения резервной копии (или репликации) является управляемое хранилище с защитой паролем или с включенной дедупликацией. Для изменения формата на "Версия 12" обратитесь к статье ниже.

  Создание резервных копий почтовых ящиков и групп обеспечения доступности баз данных (DAG) в этом формате не поддерживается.

  Примечание
  Вариант **Автоматический выбор** в данный момент не поддерживается.

6.14.5.1 Формат резервной копии и файлы резервных копий

Для хранилищ резервных копий, обзор которых можно выполнить с помощью диспетчера файлов (например, локальные или сетевые папки), формат резервных копий определяет количество файлов и их расширение. Можно назначить имена файлов используя опцию имя файла резервной копии. В следующей таблице перечислены файлы, которые создаются на каждой машине или почтовом ящике, и доступные данные для резервного копирования.

	Всегда инкрементное	**Другие схемы резервного копирования**	**Источник данных**
Формат резервной копии **Версии 11**	Один файл TIB и один файл метаданных XML	Несколько файлов TIB и один файл метаданных XML (традиционный формат)	Файлы и папки, физическая машина, виртуальная машина, Microsoft SQL Server и Microsoft Exchange Server
Формат резервной копии **Версии 12**	Один файл TIBX на каждую цепочку резервных копий (полное или дифференциальное резервное копирование и все зависящие от них инкрементные резервные копии).		Все поддерживаемые источники данных

© ООО Киберпротект, 2026

6.14.5.2 Изменение формата резервной копии на формат "Версия 12"

Для корректного перехода резервных копий с формата "Версия 11" на формат "Версия 12" укажите местом сохранения резервной копии хранилище, которое не защищено паролем и для которого выключена дедупликация. При этом происходит следующее:

- Следующая резервная копия будет полной.
- В хранилищах резервных копий, которые доступны для обзора в диспетчере файлов (например, локальные или сетевые папки), создается новый файл с расширением TIBX. Новый файл имеет имя исходного файла с добавлением суффикса **_v12A**.
- Правила хранения и репликации применяются только к новым резервным копиям.
- Старые резервные копии не удаляются и остаются доступными на вкладке **Хранилища резервных копий**. Их можно удалить вручную.

6.14.5.3 Дедупликация в архиве

Формат "Версия 12" поддерживает дедупликацию в архиве, которая обеспечивает указанные ниже преимущества.

- Существенно меньший размер резервной копии со встроенной дедупликацией на уровне блоков для любого типа данных.
- Эффективная обработка жестких ссылок обеспечивает отсутствие дублированных элементов в хранилище данных.
- Фрагментирование на основе хэша.

Примечание
Дедупликация в архиве включена по умолчанию для всех резервных копий в формате "Версия 12". Для отключения дедупликации обратитесь к статье в базе знаний Отключение внутренней дедупликации архива на стороне агента.

Не рекомендуется отключать дедупликацию, кроме случаев использования системы хранения данных со встроенной поддержкой дедупликации.

6.14.6 Проверка резервных копий

Проверка – это операция по определению возможности восстановления данных из резервной копии. Если этот параметр включен, то каждая резервная копия, созданная в соответствии с планом защиты, проверяется непосредственно после создания. Эта операция выполняется агентом защиты.

Значение по умолчанию: **Отключено**.

При проверке вычисляется контрольная сумма для каждого блока данных, который можно восстановить из данной резервной копии.

© ООО Киберпротект, 2026

Проверка – это длительный процесс даже при инкрементном или дифференциальном резервном копировании небольших объемов данных. Причина заключается в том, что во время операции проверяются не только данные, физически присутствующие в резервной копии, но и все данные, которые восстанавливаются при выборе этой резервной копии. Это требует доступа к созданным ранее резервным копиям.

Хотя успешная проверка означает высокую вероятность восстановления данных, проверяются не все факторы, влияющие на процесс восстановления. При резервном копировании операционной системы рекомендуем выполнить тестовое восстановление с загрузочного носителя на запасной жесткий диск или запустить виртуальную машину из резервной копии в среде ESXi или Hyper-V.

6.14.7 Функция Changed Block Tracking (CBT)

Этот параметр применим к следующим ресурсам:

- резервным копиям на уровне дисков для:
  - физических машин с ОС Windows,
  - виртуальных машин;
- резервным копиям баз данных:
  - Microsoft SQL Server,
  - Microsoft Exchange Server.

Этот параметр применим к следующим платформам виртуализации:

- VMware ESXi версии 6.5 и выше,
- Hyper-V Server 2012 R2 и выше,
- oVirt версии 4.5 и выше,
- zVirt версии 4.1 и выше,
- ROSA Virtualization 3.0.

Примечание
Для успешного применения параметра в средах виртуализации oVirt (zVirt, ROSA Virtualization) в настройках диска виртуальной машины активируйте флаг **Включить инкрементное резервное копирование**. Использовать технологию CBT можно только для виртуальных дисков формата QCOW.

Значение по умолчанию: **Включено**.

Этот параметр определяет, будет ли использоваться технология Changed Block Tracking (CBT) при выполнении инкрементного или дифференциального резервного копирования.

Технология CBT ускоряет процесс резервного копирования. Изменения содержимого диска или базы данных постоянно отслеживаются на уровне блоков. При запуске резервного копирования изменения могут быть незамедлительно сохранены в резервную копию.

© ООО Киберпротект, 2026

6.14.8 Способ резервного копирования кластера

Этот параметр относится к резервному копированию групп доступности Always On (AAG) в Microsoft SQL Server, групп обеспечения доступности баз данных (DAG) в Microsoft Exchange Server и кластера баз данных PostgreSQL на базе Patroni.

Параметр действует только в случае, если для резервного копирования выбрана сама группа доступности или кластер, а не отдельные содержащиеся в них узлы или базы данных. Если вы выберете отдельные элементы, содержащиеся в группе или кластере, то будут созданы резервные копии только выбранных копий элементов.

6.14.8.1 Настройка параметра для групп доступности Always On (AAG)

Чтобы параметр действовал для групп доступности Always On (AAG), агент для SQL должен быть установлен на всех узлах AAG. Дополнительные сведения о резервном копировании групп доступности Always On см. в разделе "Защита группы Always On Availability Groups (AAG)" (стр. 481).

Значение по умолчанию: **Дополнительная реплика, если возможно**.

Можно выбрать один из следующих вариантов:

- **Дополнительная реплика, если возможно**
  Если все дополнительные реплики отключены от сети, создается резервная копия основной реплики. Резервное копирование основной реплики может замедлить работу SQL Server, но будет обеспечено самое актуальное состояние данных в резервной копии.
- **Дополнительная реплика**
  Если все дополнительные реплики отключены, резервное копирование не будет выполнено. Создание резервной копии дополнительной реплики не влияет на производительность сервера SQL и позволяет расширить окно резервного копирования. Однако пассивные реплики могут содержать не самые последние данные, так как часто настроены на асинхронное обновление (с отставанием).
- **Основная реплика**
  Если основная реплика отключена, резервное копирование не будет выполнено. Резервное копирование основной реплики может замедлить работу SQL Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

Независимо от значения данного параметра, для обеспечения целостности базы данных, программа пропускает базы данных, которые до начала резервного копирования не находятся в состоянии **СИНХРОНИЗИРОВАНО** или **СИНХРОНИЗАЦИЯ**. Если пропущены все базы данных, резервное копирование не будет выполнено.

© ООО Киберпротект, 2026

6.14.8.2 Настройка параметра для групп обеспечения доступности баз данных (DAG) в Microsoft Exchange Server

Чтобы параметр действовал, агент для Exchange должен быть установлен на всех узлах DAG. Дополнительные сведения о резервном копировании групп обеспечения доступности баз данных см. в разделе "Защита групп обеспечения доступности базы данных (DAG)" (стр. 483).

Значение по умолчанию: **Пассивная копия, если возможно**.

Можно выбрать один из следующих вариантов:

- **Пассивная копия, если возможно**
  Если все пассивные копии выключены, создается резервная копия активной копии. Резервное копирование активной копии может замедлить работу Exchange Server, но будет обеспечено самое актуальное состояние данных в резервной копии.
- **Пассивная копия**
  Если все пассивные копии выключены, резервное копирование завершится сбоем. Создание резервной копии пассивных копий не влияет на производительность Exchange Server и позволяет расширить окно резервного копирования. Однако пассивные копии могут содержать не самые последние данные, так как часто настроены на асинхронное обновление (с отставанием).
- **Активная копия**
  Если активная копия выключена, резервное копирование завершится сбоем. Резервное копирование активной копии может замедлить работу Exchange Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

Независимо от значения данного параметра, для обеспечения целостности базы данных, программа пропускает базы данных, которые до начала резервного копирования не находятся в состоянии **ИСПРАВНА** или **АКТИВНА**. Если пропущены все базы данных, резервное копирование не будет выполнено.

6.14.8.3 Настройка параметра для кластера баз данных PostgreSQL на базе Patroni

Значение по умолчанию: **Реплика, если возможно**.

Можно выбрать один из следующих вариантов:

- **Реплика, если возможно**
  Выполняется резервная копия баз данных с подчиненных узлов. Если все подчиненные узлы выключены, создается резервная копия с главного узла. Резервное копирование главного узла может замедлить работу PostgreSQL, но в резервной копии будут самые актуальные данные.
- **Реплика**
  Выполняется резервная копия баз данных только с подчиненных узлов.
- **Лидер**

© ООО Киберпротект, 2026

Выполняется резервная копия баз данных только с главного узла. Резервное копирование главного узла может замедлить работу PostgreSQL, но в резервной копии будут самые актуальные данные.

6.14.9 Уровень сжатия

Этот параметр определяет уровень сжатия данных при резервном копировании. Доступные уровни: **Отсутствует**, **Обычное**, **Высокое**, **Максимальное**.

Значение по умолчанию: **Обычное**.

Чем выше уровень сжатия, тем больше времени занимает процесс резервного копирования, но созданная резервная копия занимает меньше места. В данный момент уровни "Высокое" и "Максимальное" работают аналогичным образом.

Оптимальный уровень сжатия данных зависит от типа копируемых данных. Даже максимальное сжатие не уменьшит значительно размер резервной копии, состоящей из уже сжатых файлов, например JPG, PDF или MP3. Но такие форматы, как DOC или XLS, сжимаются хорошо.

6.14.10 Многопоточность

Этот параметр позволяет указать способ использования многопоточности при резервном копировании PostgreSQL.

Примечание
Режим многопоточности работает только для экземпляров PostgreSQL. Для кластеров Patroni этот режим недоступен.

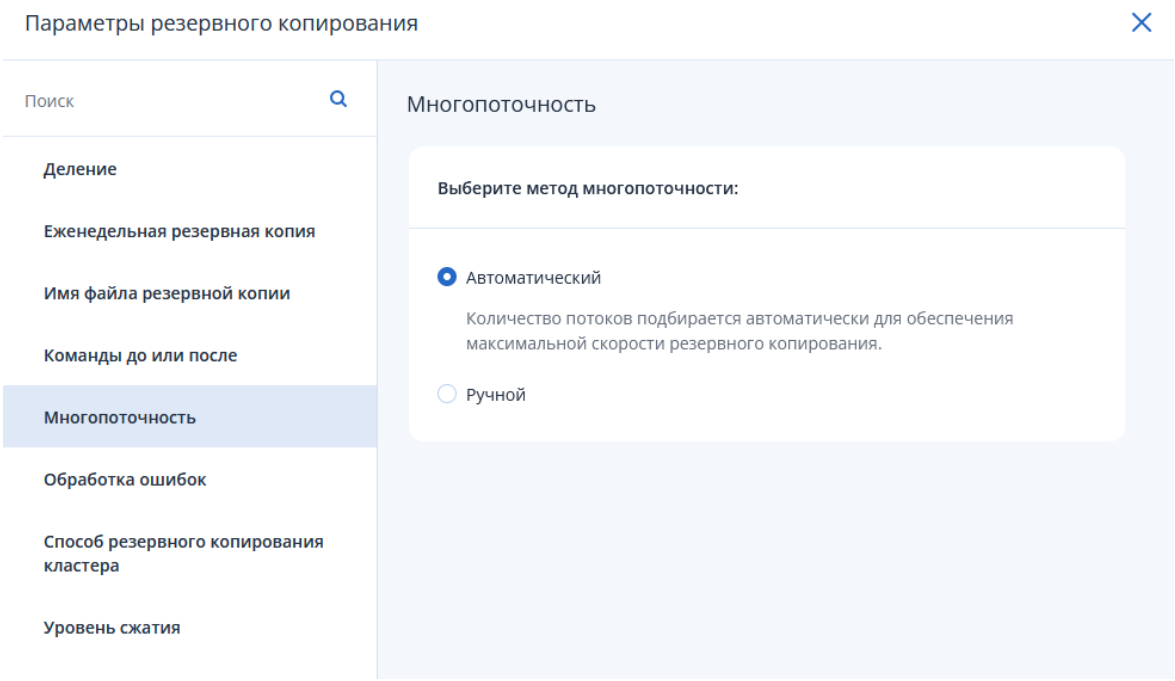
6.14.10.1 Предварительные требования

Агент для PostgreSQL должен быть установлен на тот же сервер, где находится экземпляр PostgreSQL.

6.14.10.2 Настройка

1. В меню **Параметры резервного копирования** щелкните **Многопоточность**.
2. Выберите один из двух следующих вариантов:
   a. **Автоматический**. Значение в автоматическом режиме: 16.
   b. **Ручной**. Установите с помощью кнопок управления необходимое число потоков в диапазоне от 1 до 32.
      При установке количества потоков вручную примите во внимание следующие обстоятельства:
      - увеличение числа потоков создает дополнительную нагрузку на дисковую подсистему;
      - во избежание создания узких мест в системе, увеличивайте число потоков только в том случае, если в результате общая скорость выполнения плана повышается.

© ООО Киберпротект, 2026



3. Нажмите **Сохранить**.

6.14.11 Уведомления по электронной почте

Этот параметр позволяет задать уведомления по электронной почте о событиях, которые возникают во время резервного копирования.

Значение по умолчанию: **Используйте настройки системы.**

Можно использовать системные настройки или переопределить их, заменив на пользовательские значения, относящееся только к данному плану. Системные настройки устанавливаются, как описано в разделе «Уведомления по электронной почте».

Внимание
При изменении системных настроек изменяются все планы защиты, в которых используются системные настройки.

Прежде чем включать этот параметр, убедитесь, что установлены настройки **Почтовый сервер**.

Порядок настройки уведомлений по электронной почте для плана защиты

1. Выберите **Настроить параметры для этого плана защиты**.
2. В поле **Адрес электронной почты получателя** введите адрес электронной почты получателя. Можно указать несколько адресов, разделяя их точкой с запятой.
3. [Необязательно] В поле **Тема** измените тему уведомления по электронной почте.
   Можно использовать следующие переменные:
   - [Оповещение] – сводка оповещений
   - [Устройство] – имя устройства

© ООО Киберпротект, 2026

- [План] – название плана, для которого создано оповещение.
- [Сервер управления] – имя хоста машины, на которой установлен сервер управления.
- [Отдел] – название отдела, которому принадлежит машина.

Тема по умолчанию: [Оповещение] **Устройство:** [устройство] **План:** [План]

4. Установите флажки для событий, о которых необходимо получать уведомления. Их можно выбрать из списка всех оповещений, которые возникают во время резервного копирования, сгруппированных по степени серьезности.

6.14.12 Обработка ошибок

Эти параметры позволяют указать, как должны обрабатываться ошибки, возникшие во время резервного копирования.

6.14.12.1 В случае ошибки повторить операцию

Значение по умолчанию: **Включено. Количество попыток: 30. Интервал между попытками: 30 секунд.**

Если возникла устранимая ошибка, программа будет продолжать попытки выполнить операцию. При повторном запуске дозапись в резервную копию продолжается с места прерывания.

Задайте временной интервал и количество попыток. Попытки будут прекращены в случае, если операция будет успешно выполнена, ИЛИ после указанного максимального числа попыток.

Например, если место сохранения резервной копии в сети станет недоступным, программа будет выполнять попытки подключения каждые 30 секунд, но не более 30 раз. Попытки будут прекращены, когда подключение будет восстановлено ИЛИ число попыток достигнет указанного максимума.

В этом случае фактическое количество попыток не ограничено, а время ожидания до возврата ошибки о сбое резервного копирования рассчитывается по следующей формуле: (300 секунд + **Интервал между попытками**) * (**Количество попыток** + 1).

Примеры:

- Со значениями по умолчанию для сбоя резервного копирования должно пройти (300 секунд + 30 секунд) * (300 + 1) = 99330 секунд, или ~27,6 часов.
- Если параметру **Количество попыток** задано значение 1, а параметру **Интервал между попытками** – значение 1, сбой резервного копирования должен произойти через (300 секунд + 1 секунда) * (1 + 1) = 602 секунды или ~10 минут.

Если рассчитанное время ожидания превышает 30 минут, а передача данных еще не началась, для фактического времени ожидания устанавливается время 30 минут.

6.14.12.2 Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений)

Значение по умолчанию: **Включено**.

© ООО Киберпротект, 2026

В режиме без вывода сообщений ситуации, требующие вмешательства пользователя, разрешаются автоматически (за исключением обработки поврежденных секторов, что задается отдельным параметром). Если операция не может быть продолжена без вмешательства пользователя, она не будет выполнена. Дополнительные сведения об операции, включая информацию об ошибках (если они есть), см. в журнале операций.

6.14.12.3 Пропуск поврежденных секторов

Значение по умолчанию: **Отключено**.

Если этот параметр отключен, каждый раз, когда встречается поврежденный сектор, действию резервного копирования будет назначено состояние **Требуется вмешательство пользователя**. Чтобы создать резервную копию данных с диска, который быстро выходит из строя, включите параметр пропуска поврежденных секторов. Резервное копирование неповрежденных данных будет выполнено, после чего можно подключить резервную копию диска и извлечь исправные файлы на другой диск.

6.14.12.4 Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины

Значение по умолчанию: **Включено. Количество попыток: 3. Интервал между попытками: 5 минут.**

Если не удастся создать моментальный снимок виртуальной машины, программа будет продолжать попытки выполнить операцию. Задайте временной интервал и количество попыток. Попытки будут прекращены, как только операция будет успешно выполнена ИЛИ по достижении указанного максимального количества попыток (в зависимости от того, что наступит раньше).

6.14.13 Быстрое инкрементное/дифференциальное резервное копирование

Этот параметр работает для инкрементных и дифференциальных резервных копий на уровне дисков.

Этот параметр не работает (всегда отключен) для томов с файловыми системами JFS, ReiserFS3, ReiserFS4, ReFS или XFS.

Значение по умолчанию: **Включено**.

Инкрементная или дифференциальная резервная копия содержит только изменения данных. Чтобы ускорить процесс резервного копирования, программа определяет, есть ли изменения в файле по размеру, дате и времени последнего изменения файла. Если эта функция отключена, то программа будет сравнивать все содержимое файла с тем содержимым, которое сохранено в резервной копии.

© ООО Киберпротект, 2026

6.14.14 Фильтры файлов

Фильтры позволяют включить в резервную копию или исключить из нее только определенные файлы и папки.

Фильтры файлов доступны как для резервных копий на уровне файлов, так и для резервных копий на уровне дисков, если не указано иначе.

Фильтры файлов не работают для динамических дисков (томов LVM или LDM) или виртуальной машины, резервная копия которой создана агентом для VMware или агентом для Hyper-V в режиме без использования агента.

Включение фильтров файлов

1. В плане защиты разверните модуль **Резервное копирование**.
2. В разделе **Параметры резервного копирования** щелкните **Изменить**.
3. Выберите **Фильтры файлов**.
4. Воспользуйтесь любыми из перечисленных ниже вариантов.

6.14.14.1 Включение или исключение файлов, соответствующих определенным критериям

Есть два параметра с противоположными принципами действия.

- **Создавать резервные копии файлов, соответствующих следующим критериям**
  Пример: Если выбрать резервное копирование всей машины и указать в качестве условия фильтрации **C:\File.exe**, будет создана резервная копия только этого файла.
- **Не создавать резервные копии файлов, соответствующих следующим критериям**
  Пример: Если выбрать резервное копирование всей машины и указать в качестве условия фильтрации **C:\File.exe**, будет пропущен только этот файл.

Оба параметра можно использовать одновременно. При этом второй имеет приоритет над первым (т. е. если указать **C:\File.exe** в обоих полях, этот файл будет пропущен при резервном копировании).

Условия

- **Полный путь**
  Укажите полный путь к файлу или папке, начиная с буквы диска (при резервном копировании ОС Windows) или с корневого каталога (при резервном копировании Linux).
  Как в Windows, так и в Linux, в пути к файлу или папке можно использовать косую черту (например, **C:/Temp/File.tmp**). В Windows также можно использовать традиционную обратную косую черту (например, **C:\Temp\File.tmp**).

© ООО Киберпротект, 2026

Внимание
Если операционная система машины, для которой создается резервная копия, определена неправильно при резервном копировании на уровне дисков, фильтры полного пути к файлу не будут работать. Для фильтра исключения будет показано предупреждение. Если есть фильтр включения, резервное копирование завершится сбоем.

Фильтр полного пути включает в себя букву диска (в ОС Windows) или корневой каталог (в ОС Linux). Пример полного пути к файлу: **C:\Temp\File.tmp**. Фильтр, который включает в себя букву диска или корневой каталог, например **C:\Temp\File.tmp** или **C:\Temp***, вызовет предупреждение или сбой.

Фильтр, в котором не используется буква диска или корневой каталог (например, **Temp*** или **Temp\File.tmp**), или фильтр, который начинается со звездочки (например, ***C:**), не приводит к возврату предупреждения или сбою. Если операционная система машины, для которой создана резервная копия, определена неправильно, фильтры обоих типов не будут работать.

- **Имя**
  Укажите имя файла или папки, например **Document.txt**. Будут выбраны все файлы и папки с этим названием.

В условиях *не* учитывается регистр символов. Например, путь **C:\Temp** включает варианты **C:\TEMP**, **C:\temp** и т. п.

В условии можно использовать любое количество подстановочных символов (*, ** и ?). Эти символы можно использовать как в полном пути, так и в имени файла или папки.

Звездочка (*) замещает 0 или несколько символов имени файла. Например, условие **Doc*.txt** включает в себя файлы **Doc.txt** и **Document.txt**

[Только резервные копии в формате **версия 12**] Две звездочки (*) замещают 0 или несколько символов в имени или пути файла, включая символ косой черты. Например, критерий ****/Docs/**.txt** соответствует всем TXT-файлам во всех подпапках всех папок **Docs**.

Вопросительный знак (?) замещает в имени файла ровно один символ. Например, условие **Doc?.txt** включает в себя файлы **Doc1.txt** и **Docs.txt**, но не включает файлы **Doc.txt** и **Doc11.txt**

6.14.14.2 Исключить скрытые файлы и папки

Этот параметр действует только в файловых системах, совместимых с Windows. Установите этот флажок, чтобы пропускать файлы и папки с атрибутом **Скрытый**. Если скрыта папка, будет исключено все ее содержимое, включая файлы без атрибута **Скрытый**.

6.14.14.3 Исключить системные файлы и папки

Этот параметр действует только в файловых системах, совместимых с Windows. Установите этот флажок, чтобы пропустить файлы и папки с атрибутом **Системный**. Если данный атрибут назначен

© ООО Киберпротект, 2026

папке, будет исключено все ее содержимое, включая файлы без атрибута **Системный**.

Примечание
Просматривать атрибуты файлов и папок можно в их свойствах или с помощью команды attrib. Дополнительные сведения можно получить в центре справки и поддержки Windows.

6.14.15 Моментальные снимки резервных копий на уровне файлов

Этот параметр действует только для резервной копии на уровне файлов.

Этот параметр определяет, выполнять последовательное резервное копирование файлов или делать моментальный снимок данных.

Примечание
Файлы, которые хранятся в сетевых папках, при создании резервной копии всегда копируются по одному.

Значение по умолчанию:

- Если для резервного копирования выбраны только машины с ОС Linux: **Не создавать моментальный снимок.**
- В противном случае: **По возможности создавать моментальный снимок.**

Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:

- **По возможности создавать моментальный снимок**
  Прямое резервное копирование файлов, если создание моментального снимка невозможно.
- **Всегда создавать моментальный снимок**
  Моментальный снимок позволяет выполнять резервное копирование всех файлов, включая те, которые открыты с монопольным доступом. Все файлы в резервной копии будут сохранены в состоянии на данный момент времени. Выберите эту настройку только в случае, если эти факторы имеют важное значение, т. е. резервное копирование файлов без создания моментального снимка лишено смысла. Если моментальный снимок не может быть сделан, резервное копирование завершится ошибкой.
- **Не создавать моментальный снимок**
  Всегда выполнять прямое резервное копирование файлов. Попытка резервного копирования файлов, открытых с монопольным доступом, приведет к ошибке чтения. Файлы в резервной копии могут быть не синхронизированы по времени.

6.14.16 Сокращение журнала Microsoft SQL Server

Этот параметр применим для резервного копирования баз данных Microsoft SQL Server и резервного копирования на уровне дисков с включенным резервным копированием приложения Microsoft SQL Server.

© ООО Киберпротект, 2026

Этот параметр определяет, будут ли сокращаться журналы транзакций SQL Server после успешного резервного копирования.

Значение по умолчанию: **Включено**.

Если этот параметр включен, базу данных можно восстановить только по состоянию на момент создания резервной копии этим программным обеспечением. Отключите этот параметр, если вы создаёте резервные копии журналов транзакции встроенным модулем резервного копирования Microsoft SQL Server. Можно будет применить журналы транзакций после восстановления и таким образом восстановить базу данных в состояние на любой момент времени (Point-in-Time Recovery, PITR).

Убедитесь, что резервные копии журналов транзакций регулярно создаются модулем резервного копирования Microsoft SQL Server и переполнения диска не происходит.

6.14.17 Создание моментальных снимков LVM

Этот параметр действует только для физических машин.

Этот параметр действует только для резервного копирования томов на уровне дисков, управляемых диспетчером логических томов Linux (LVM). Такие тома также называются логическими томами.

Этот параметр определяет способ создания моментального снимка логического тома. Программа резервного копирования может выполнить это самостоятельно или воспользоваться для этого диспетчером логических томов Linux (LVM).

Значение по умолчанию: **С помощью программы для резервного копирования**.

- **С помощью программы для резервного копирования**. Данные моментального снимка хранятся в основном в ОЗУ. Так резервное копирование выполняется быстрее, а в группе томов не требуется нераспределенное пространство. Поэтому рекомендуется изменять заранее заданное значение только при возникновении неполадок с резервным копированием логических томов.
- **С помощью LVM**. Моментальный снимок сохраняется в нераспределеном пространстве группы тома. При отсутствии нераспределенного пространства моментальный снимок будет создан программой резервного копирования.

Моментальный снимок используется только при выполнении операции резервного копирования и автоматически удаляется после её окончания. Временные файлы не сохраняются.

6.14.18 Точки подключения

Этот параметр действует только в Windows для резервной копии на уровне файлов любого источника данных, который включает в себя подключенные тома или общие тома кластера.

Этот параметр работает только в случае, если для резервного копирования выбрана папка, которая в иерархии папок находится выше точки подключения. (Точка подключения – это папка, к которой логически подключен дополнительный том.)

© ООО Киберпротект, 2026

- Если такая папка (родительская папка) выбрана для резервного копирования, и включен параметр **Точки подключения**, все файлы на подключенном томе будут включены в резервную копию. Если параметр **Точки подключения** отключен, точка подключения в резервной копии будет пуста.

  При восстановлении родительской папки содержимое точки подключения восстанавливается, когда для восстановления включен параметр **Точки подключения**.
- Если выбрана сама точка подключения или любая папка в подключенном томе, выбранные папки рассматриваются как обыкновенные. Их резервное копирование будет выполняться независимо от состояния параметра **Точки подключения**, а восстановление – независимо от **Точки подключения** для восстановления.

Значение по умолчанию: **Отключено**.

Примечание
Можно создавать резервные копии виртуальных машин Hyper-V, расположенных на общем томе кластера, путем резервного копирования нужных файлов или всего тома на уровне файлов. Просто отключите виртуальные машины, чтобы их резервное копирование выполнялось согласованно.

Пример

Предположим, что папка **C:\Data1** является точкой подключения для подключенного тома. Этот том содержит папки **Folder1** и **Folder2**. Вы создаете план защиты для резервной копии ваших данных на уровне файлов.

Если установить флажок для тома C и включить параметр **Точки подключения**, в папке **C:\Data1** в резервной копии будут находиться **Folder1** и **Folder2**. При восстановлении данных с резервной копии помните о правильном использовании параметра **Точки подключения** для восстановления.

Если установить флажок для тома C и отключить параметр **Точки подключения**, папка **C:\Data1** в резервной копии будет пустой.

Если установить флажок для **Data1**, папки **Folder1** или **Folder2**, отмеченные папки будут включены в копию как обыкновенные папки независимо от параметра **Точки подключения**.

6.14.19 Многотомные моментальные снимки

Этот параметр применим для резервных копий физических и виртуальных машин, работающих под управлением Windows или Linux, с установленным в этих ОС агентом.

Этот параметр применяется к резервному копированию дисков. Также этот параметр применим к резервному копированию файлов, если оно выполняется посредством создания моментального снимка. (Параметр «Моментальный снимок файлов» указывает, будет ли создан моментальный снимок при резервном копировании на уровне файлов).

Этот параметр определяет, создаются моментальные снимки нескольких томов одновременно или последовательно.

Значение по умолчанию:

© ООО Киберпротект, 2026

- Если хотя бы одна машина под управлением Windows выбрана для резервного копирования: **Включено**.
- Если не выбрано ни одной машины (это имеет место, когда вы начинаете создавать план защиты на странице **Планы** > **Резервная копия**): **Включено**.
- В противном случае: **Отключено**.

Если этот параметр включен, то моментальные снимки всех томов, для которых выполняется резервное копирование, создаются одновременно. Используйте этот параметр для создания синхронизированных по времени резервных копий данных, расположенных на нескольких томах, например в базе данных Oracle.

Если этот параметр отключен, то моментальные снимки томов будут созданы последовательно. В результате, если данные расположены на нескольких томах, результирующие резервные копии могут быть не синхронизированы по времени.

6.14.20 Производительность и окно резервного копирования

Позволяет задавать один из трех уровней производительности резервного копирования (высокий, низкий, запрещено) для каждого часа недели. Таким образом можно определить окно времени, в течение которого разрешено запускать и выполнять процессы резервного копирования. Высокий и низкий уровни производительности настраиваются в плане приоритета процесса и скорости вывода.

Этот параметр можно настроить отдельно для каждого хранилища, указанного в плане защиты. Чтобы настроить этот параметр для хранилища репликации, щелкните значок шестерни рядом с именем хранилища и щелкните **Производительность и окно резервного копирования**.

Этот параметр действует только для резервного копирования и репликации резервной копии. Команды после резервного копирования и другие операции, входящие в план защиты (проверка, преобразование в виртуальную машину), запускаются независимо от значения этого параметра.

Значение по умолчанию: **Отключено**.

Если этот параметр отключен, процессы резервного копирования разрешено запускать в любое время с указанными ниже параметрами (при этом не имеет значения, было ли изменено предустановленное значение параметра):

- Приоритет ЦП: **Низкий** (соответствует значению **Ниже среднего**).
- Скорость вывода: **Без ограничений**.

Если этот параметр включен, запланированные резервные копии разрешаются или блокируются согласно параметрам, указанным для текущего часа. В начале часа блокировки резервного копирования процесс резервного копирования автоматически останавливается; появляется соответствующее оповещение.

Даже если запланированные резервные копии заблокированы, резервное копирование можно запустить вручную. Для него будут использоваться параметры производительности последнего часа, когда процессы резервного копирования были разрешены.

© ООО Киберпротект, 2026

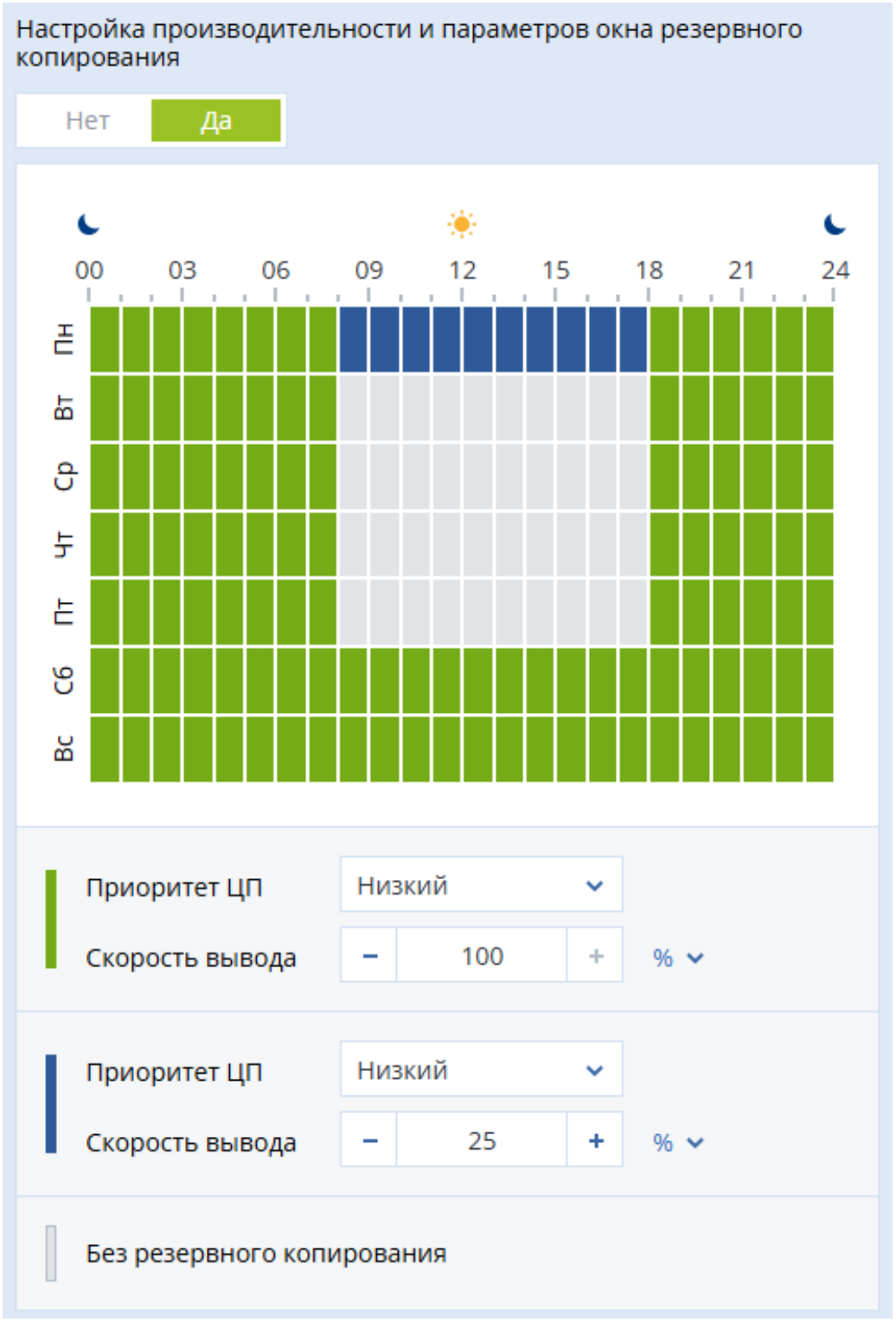
6.14.20.1 Окно резервного копирования

Каждый прямоугольник представляет один час в пределах рабочего дня. По щелчку прямоугольника можно поочередно переходить между указанными состояниями:

- **Зеленый:** резервное копирование разрешено с параметрами, указанными в зеленом разделе ниже.
- **Синий:** резервное копирование разрешено с параметрами, указанными в синем разделе ниже. Это состояние недоступно, если для формата резервной копии задано значение **Версия 11**.
- **Серый:** резервное копирование заблокировано.

Чтобы одновременно изменить состояние нескольких прямоугольников, щелкните один из них и расширьте выделение путем перетаскивания.

© ООО Киберпротект, 2026



6.14.20.2 Приоритет ЦП

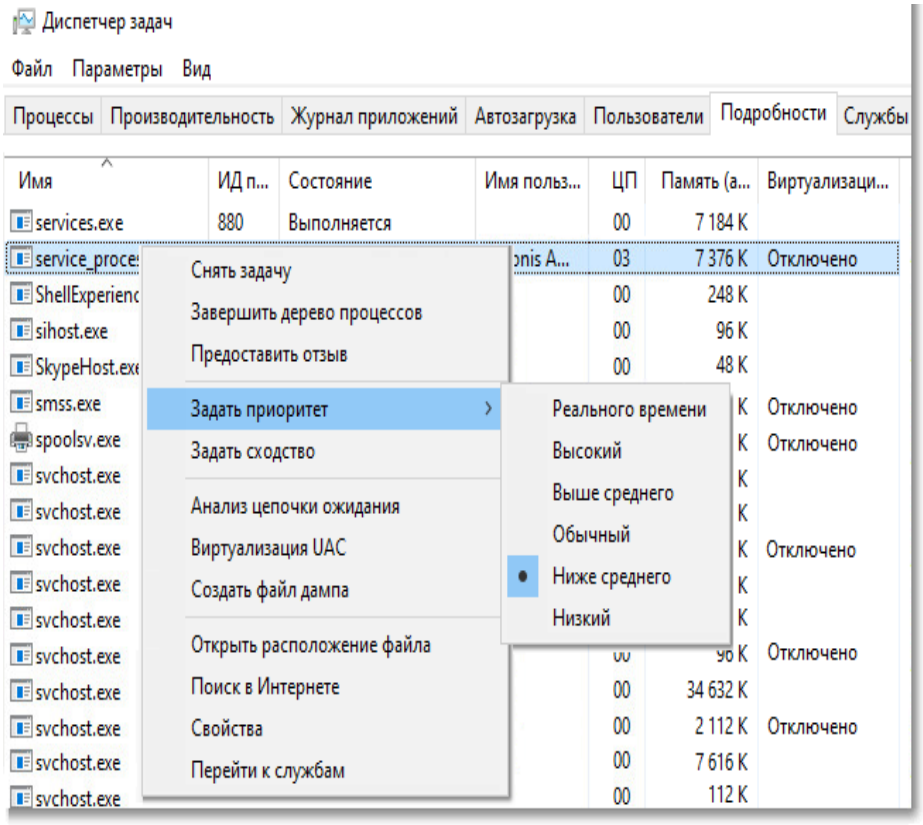
Этот параметр задает приоритет процесса резервного копирования (**service_process.exe**) в операционной системе Windows.

Доступные значения:

© ООО Киберпротект, 2026

- **Низкий**: соответствует значению **Ниже среднего**.
- **Обычный**: соответствует значению **Обычный**.
- **Высокий**: соответствует значению **Высокий**.

Приоритет процесса, выполняющегося в системе, определяет количество выделенных ему ресурсов ЦП и системы. Понижение приоритета резервного копирования освободит часть ресурсов для других приложений. Повышение приоритета копирования ускорит процесс создания резервных копий за счет того, что операционная система выделит программе резервного копирования больше ресурсов, например ресурсов ЦП. Однако результат будет зависеть от общего использования процессора и других факторов, например от скорости ввода-вывода диска и загруженности сети.



6.14.20.3 Скорость вывода при резервном копировании

Этот параметр позволяет ограничить скорость записи на жесткий диск (при выполнении резервного копирования в локальную папку) или скорость передачи данных резервной копии по сети (при резервном копировании в сетевую папку).

Если этот параметр включен, можно указать максимально разрешенную скорость вывода:

- В процентах от оценочной скорости записи на целевом жестком диске (при резервном копировании в локальную папку) или оценочной максимальной скорости сетевого подключения (при резервном копировании сетевой папки).

  Эта настройка работает только для Windows-агентов.

© ООО Киберпротект, 2026

- В КБ/секунду (для всех мест сохранения).

  Эта настройка работает для Windows- и Linux-агентов.

Примечание
Если одновременно запущено несколько процессов резервного копирования, итоговая скорость вывода определяется как сумма скоростей вывода этих процессов.

6.14.21 Команды до и после процедуры

Этот параметр позволяет определить команды, которые должны выполняться автоматически перед выполнением процедуры резервного копирования или после нее.

Следующая схема иллюстрирует порядок выполнения команд до и после процедуры.

Команда до резервного копирования	Резервное копирование	Команда после резервного копирования

Примеры использования команд до и после процедуры:

- Удаление некоторых временных файлов с диска до начала резервного копирования.
- Настройка антивирусной программы стороннего производителя для запуска до начала резервного копирования.
- Выборочное копирование резервных копий в другое хранилище. Этот параметр может быть полезен, поскольку операция репликации, заданная в плане защиты, копирует каждую резервную копию архива в указанные хранилища.

Агент выполняет репликацию после выполнения команды после резервного копирования.

Кибер Бэкап не поддерживает интерактивные команды, то есть команды, которые требуют пользовательского ввода (например, pause).

6.14.21.1 Команда до резервного копирования

Как указать команду или пакетный файл, которые будут выполнены перед началом резервного копирования

1. Включите переключатель **Выполнение команды до резервного копирования**.
2. В поле **Команда...** введите команду или укажите путь к пакетному файлу на машине с агентом. Кибер Бэкап не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).

© ООО Киберпротект, 2026

Примечание
Если в плане указана интерактивная команда, то такой план после запуска может навсегда остаться в состоянии "Выполняется", а его выполнение нельзя будет остановить через веб-интефейс Кибер Бэкап. Чтобы остановить выполнение плана в такой ситуации, на каждой целевой машине плана необходимо принудительно завершить процесс этой команды (см. дочерние процессы процесса агента Кибер Бэкап) и перезапустить агент.

3. В поле **Рабочий каталог** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите аргументы выполнения команды (если необходимо).
5. В зависимости от желаемого результата выберите соответствующие параметры из описанных в таблице ниже.
6. Нажмите кнопку **Готово**.

Флажок	**Выбор**			
Не запускать план, если не удается выполнить команду*	Установить	Снять	Установить	Снять
Выполнить план по окончании выполнения команды	Установить	Установить	Снять	Снять
Результат				
	По умолчанию Выполнить резервное копирование только после успешного выполнения команды. Прерывать резервное копирование при сбое команды.	Выполнить резервное копирование после команды независимо от результатов ее выполнения (успешно или ошибка).	Н/Д	Выполнить резервное копирование одновременно с выполнением команды и независимо от результатов выполнения команды.

* Команда считается сбойной, если код завершения не равен нулю. При сбое команды план не перезапускается даже при включенном параметре "Действие при сбое плана" (стр. 378).

© ООО Киберпротект, 2026

6.14.21.2 Команда после резервного копирования

Как указать команду или исполняемый файл, которые будут выполнены после завершения резервного копирования

1. Включить переключатель **Выполнение команды после резервного копирования**.
2. В поле **Команда...** введите команду или укажите путь к пакетному файлу на машине с агентом.
3. В поле **Рабочий каталог** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости аргументы выполняемой команды.
5. Установите флажок **Прерывать резервное копирование при сбое команды**, если для вас важно успешное выполнение команды. Считается, что команда не выполнена, если код выхода не равен нулю. При сбое выполнения команды состоянию резервной копии будет задано значение **Ошибка**.

   Если флажок не установлен, результат выполнения команды не влияет на успешность выполнения резервного копирования. Можно отследить результат выполнения команды, изучив информацию на вкладке **Действия**.
6. Нажмите кнопку **Готово**.

6.14.22 Команды до и после захвата данных

Этот параметр позволяет задать команды, которые должны выполняться автоматически до и после захвата данных (т. е. создание моментального снимка данных). Захват данных выполняется в начале процедуры резервного копирования.

Следующая схема иллюстрирует порядок выполнения команд до и после захвата данных.

<table>
<tr><td></td><td colspan="3"><---------- Резервная копия ----------></td><td></td></tr>
<tr><td>Команда до резервного копирования</td><td>Команда до захвата данных</td><td>Захват данных</td><td>Команда после захвата данных</td><td>Команда после резервного копирования</td></tr>
</table>

Если включен параметр «Служба теневого копирования томов (VSS)», то последовательность выполнения команд и операций Microsoft VSS будет следующей:

Команды «до захвата данных» -> приостановка VSS -> захват данных -> возобновление VSS -> команды «после захвата данных».

Использование команд до и после захвата данных предоставляет возможность приостановки и возобновления базы данных или приложения, которые несовместимы с VSS. Поскольку захват данных выполняется за считанные секунды, время простоя базы данных или приложения сводится к минимуму.

© ООО Киберпротект, 2026

Команды после захвата данных работают только в случае, если включен параметр «Многотомные моментальные снимки» (см. раздел "Многотомные моментальные снимки" (стр. 360)).

6.14.22.1 Команда до захвата данных

Как указать команду или пакетный файл, которые будут выполнены до захвата данных

1. Включите переключатель **Выполнение команды до захвата данных**.
2. В поле **Команда...** введите команду или найдите пакетный файл. Программа не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).

   Примечание
   Если в плане указана интерактивная команда, то такой план после запуска может навсегда остаться в состоянии "Выполняется", а его выполнение нельзя будет остановить через веб-интефейс Кибер Бэкап. Чтобы остановить выполнение плана в такой ситуации, на каждой целевой машине плана необходимо принудительно завершить процесс этой команды (см. дочерние процессы процесса агента Кибер Бэкап) и перезапустить агент.

3. В поле **Рабочая папка** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите аргументы выполнения команды (если необходимо).
5. В зависимости от желаемого результата выберите соответствующие параметры из описанных в таблице ниже.
6. Нажмите кнопку **Готово**.

Флажок	**Выбор**			
Прерывать резервное копирование при сбое команды*	Установить	Снять	Установить	Снять
Не выполнять захват данных до полного выполнения команды	Установить	Установить	Снять	Снять
Результат				
	Предустановка Выполнить захват данных только после успешного	Выполнить захват данных после команды независимо от	Н/Д	Выполнить захват данных одновременно с выполнением

© ООО Киберпротект, 2026

	выполнения команды. Прерывать резервное копирование при сбое команды.	результатов ее выполнения (успешно или ошибка).		команды и независимо от результатов выполнения команды.

* Команда считается сбойной, если код завершения не равен нулю.

6.14.22.2 Команда после захвата данных

Как указать команду или пакетный файл, которые будут выполнены после захвата данных

1. Включите переключатель **Выполнение команды после захвата данных**.
2. В поле **Команда...** введите команду или найдите пакетный файл. Программа не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).
3. В поле **Рабочая папка** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите аргументы выполнения команды (если необходимо).
5. В зависимости от желаемого результата выберите соответствующие параметры из описанных в таблице ниже.
6. Нажмите кнопку **Готово**.

Флажок	**Выбор**			
Прерывать резервное копирование при сбое команды*	Установить	Снять	Установить	Снять
Не продолжать создание резервной копии до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				
	Предустановка Продолжить резервное копирование только после	Продолжить резервное копирование после команды независимо от	Н/Д	Продолжить резервное копирование одновременно с выполнением

© ООО Киберпротект, 2026

	успешного выполнения команды.	результатов ее выполнения (успешно или ошибка).		команды и независимо от результатов выполнения команды.

* Команда считается сбойной, если код завершения не равен нулю.

6.14.23 Моментальные снимки оборудования SAN

Эта опция эффективна для резервного копирования виртуальных машин VMware ESXi и oVirt.

Значение по умолчанию: **Отключено**.

Этот параметр определяет, будет ли использоваться технология моментальных снимков SAN при выполнении резервного копирования.

Если эта опция отключена, содержимое виртуального диска будет прочитано с моментального снимка VMware/oVirt. Моментальный снимок хранится все время резервного копирования.

Если этот параметр включен, содержимое виртуального диска будет прочитано с моментального снимка SAN. Моментальный снимок будет создан и сохранен на небольшое время, чтобы привести виртуальные диски в согласованное состояние. Если чтение с моментального снимка SAN невозможно, резервное копирование завершится с ошибкой.

Перед подключением этой опции проверьте и выполните все требования, указанные в разделе «Использование моментальных снимков оборудования SAN».

6.14.24 Планирование

Этот параметр определяет, запускаются ли процессы резервного копирования по расписанию или с задержкой, а также количество виртуальных машин, для которых резервное копирование выполняется одновременно.

Можно выбрать один из следующих вариантов:

- **Начинать все операции резервного копирования строго по расписанию**
  Резервное копирование физических машин запустится точно в соответствии с расписанием. Резервные копии виртуальных машин будут создаваться поочередно.
- **Распределять время запуска по доступному времени**
  Резервные копии физических машин будут запущены с задержкой от запланированного времени. Значение задержки для каждой машины выбирается случайно и находится в диапазоне от нуля до максимального значения, которое вы укажете. Параметр может быть полезен для резервного копирования нескольких машин в сетевое хранилище, чтобы избежать чрезмерной загрузки сети. Продолжительность задержки для каждой машины определяется при применении плана защиты к машине и остается неизменной до тех пор, пока в плане защиты не будет изменено максимальное значение задержки.
  Резервные копии виртуальных машин будут создаваться поочередно.

© ООО Киберпротект, 2026

- **Ограничить число одновременно выполняющихся операций резервного копирования на уровне**

  Этот параметр доступен только в том случае, если план защиты применен к нескольким виртуальным машинам. Этот параметр определяет количество виртуальных машин, для которых агент может одновременно создавать резервные копии при выполнении данного плана защиты.

  Если в соответствии с планом защиты агенту необходимо начать резервное копирование нескольких машин сразу, он выберет две машины. (Чтобы оптимизировать производительность резервного копирования, агент пытается подобрать машины, хранящиеся в различных хранилищах.) После завершения создания любой из первых двух резервных копий агент выберет третью машину и т. д.

  Количество виртуальных машин, для которых агент будет создавать резервные копии одновременно, можно изменить. Максимальное значение равно 10. Однако если агент выполняет несколько планов защиты, которые пересекаются по времени, указанные в их параметрах числа суммируются. Вы можете ограничить общее количество виртуальных машин, для которых агент может одновременно создавать резервные копии, вне зависимости от количества выполняемых планов резервного копирования.

6.14.25 Посекторное резервное копирование

Этот параметр действует только при резервном копировании на уровне дисков.

Этот параметр определяет, создавать ли точную копию диска или тома на физическом уровне.

Значение по умолчанию: **Отключено**.

Если этот параметр включен, создается резервная копия всех секторов диска или тома, включая нераспределенное пространство и те сектора, в которых нет данных. Размер полученной в результате резервной копии будет равен размеру диска, для которого создается резервная копия (если параметру Уровень сжатия задано значение **Отсутствует**). Программное обеспечение автоматически перейдет к посекторному резервному копированию для дисков с нераспознанными или неподдерживаемыми файловыми системами.

Примечание
Невозможно будет восстановить данные приложения из резервных копий, созданных в посекторном режиме.

6.14.26 Деление

Этот параметр применим для следующих схем резервного копирования:

- **Всегда инкрементное**;
- **Всегда полное**;
- **Еженедельно полное, ежедневно инкрементное**;

© ООО Киберпротект, 2026

- **Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS)**;
- **Другое**.

Этот параметр позволяет выбрать метод разделения резервных копий на фрагменты.

Примечание
Параметр не используется для Кибер Инфраструктуры и Кибер Хранилища.

Значение по умолчанию: **Автоматически**.

Доступны следующие настройки:

- **Автоматически**

  Резервная копия будет разделена на части, если:
  - размер копии превышает максимальный размер файла, который поддерживается в выбранном хранилище;
  - копия не помещается на остаток текущей ленты.

  Примечание
  В том случае, когда в хранилище используется файловая система NTFS и агент для Windows, резервная копия будет разделена на части, если её размер превышает 200 ГБ.

- **Постоянный размер**

  Введите или выберите из предлагаемых вариантов нужный размер файла.

При применении плана репликации к резервной копии (см. раздел "Репликация резервных копий" (стр. 414)), разделённой на фиксированные фрагменты, реплицированная копия объединяется в общий архив.

Примечание
При редактировании плана новое значение параметра применяется только после удаления всех резервных копий, сделанных со старым значением.

6.14.27 Управление лентами

Эти параметры применимы только при резервном копировании на ленточное устройство.

6.14.27.1 Включить восстановление файлов из образов дисков на лентах

Значение по умолчанию: **Отключено**.

Если этот флажок установлен, при каждом резервном копировании программа создает дополнительные файлы на жестком диске машины, к которой подсоединено ленточное устройство. Восстановление файлов из резервных копий дисков возможно до тех пор, пока эти дополнительные файлы будут в порядке. Файлы автоматически удаляются при стирании, удалении или перезаписи ленты с соответствующими резервными копиями.

Дополнительные файлы располагаются в следующих местах:

© ООО Киберпротект, 2026

- В ОС Windows: %PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation.
- В ОС Linux: /var/lib/Acronis/BackupAndRecovery/TapeLocation.

Пространство, занимаемое этими дополнительными файлами, зависит от количества файлов в соответствующей резервной копии. Для полной резервной копии диска, содержащей примерно 20 000 файлов (обычная резервная копия диска рабочей станции), дополнительные файлы занимают около 150 МБ. Полная резервная копия сервера, содержащая 250 000 файлов, может создать около 700 МБ дополнительных файлов. Поэтому, если вы уверены, что восстановление отдельных файлов не потребуется, можно не устанавливать этот флажок для экономии дискового пространства.

Если дополнительные файлы не были созданы в процессе резервного копирования или были удалены, их все равно можно создать, повторно просканировав ленты, на которых хранится резервная копия.

Примечание
Восстановление дополнительных файлов недоступно, если размер архива резервной копии менее 500 КБ.

6.14.27.2 Вернуть ленту в слот после каждого успешного создания резервной копии каждой машины

Значение по умолчанию: **Включено**.

Если этот параметр отключен, лента будет оставаться в приводе после завершения операции, в которой используется лента. В ином случае программное обеспечение вернет ленту в слот, в котором она находилась до операции. Если, согласно плану защиты, за созданием резервной копии следуют другие операции (например, ее проверка или репликация в другое хранилище), лента будет возвращена в слот после завершения этих операций.

Если включен этот параметр, а также параметр **Извлечь ленты после успешного резервного копирования каждой машины**, лента будет извлечена.

6.14.27.3 Извлечь ленты после каждого успешного резервного копирования каждой машины

Значение по умолчанию: **Отключено**.

Если установлен этот флажок, программа будет извлекать ленты после любого успешного резервного копирования каждой машины. Если, согласно плану защиты, за созданием резервной копии следуют другие операции (например, ее проверка или репликация в другое хранилище), ленты будут извлечены после завершения этих операций.

6.14.27.4 Перезаписать ленту в автономном ленточном устройстве при создании полной резервной копии

Значение по умолчанию: **Отключено**.

© ООО Киберпротект, 2026

Параметр применяется только к изолированным ленточным устройствам. Если этот параметр включен, лента, вставленная в устройство, будет перезаписываться каждый раз при создании полной резервной копии.

6.14.27.5 Используйте следующие ленточные устройства и приводы

Этот параметр позволяет указать ленточные устройства и приводы лент, используемые данным планом защиты.

Пул лент включает в себя ленты со всех ленточных устройств, подключенных к машине, будь то узел хранения или машина, на которой установлен агент защиты, или обе эти машины. Если в качестве хранилища резервных копий выбран пул лент, это означает, что косвенно выбрана и машина, к которой подключены ленточные устройства. По умолчанию резервные копии можно записать на ленты в любом приводе лент на любом ленточном устройстве, подключенном к этой машине. Если некоторые устройства или приводы отсутствуют или не работают должным образом, план защиты будет использовать доступные устройства и приводы.

Можно щелкнуть **Только выбранные устройства и приводы** и выбрать ленточные устройства и приводы в списке. При выборе всего устройства выбираются все его приводы. Это означает, что любой из этих приводов может использоваться планом защиты. Если выбранное устройство или привод отсутствуют или не работают должным образом, а никаких других устройств не выбрано, резервное копирование завершится сбоем.

Этот параметр позволяет управлять процессами резервного копирования, которые выполняются несколькими агентами, в большую библиотеку ленточных носителей с несколькими приводами. Например, резервное копирование большого файлового сервера или большой общей папки может не запуститься, если несколько агентов выполняют резервное копирование машин в одном окне резервного копирования, поскольку агенты могут занимать все приводы. Если разрешить агентам использовать, например, приводы 2 и 3, привод 1 будет зарезервирован для агента, который выполняет резервное копирование общей папки.

6.14.27.6 С несколькими потоками

Значение по умолчанию: **Отключено**.

Использование нескольких потоков позволяет распределить данные с одного агента на несколько потоков, а затем одновременно записать эти потоки на разные ленточные носители. Это позволяет создавать резервные копии быстрее и особенно полезно в тех случаях, когда производительность агента выше производительности ленточного устройства.

Флажок **С несколькими потоками** доступен только в том случае, если в параметре **Только выбранные устройства и приводы** выбрано несколько ленточных устройств. Количество выбранных ленточных устройств равно количеству одновременных потоков от агента. Если при запуске резервного копирования какое-либо из этих устройств будет недоступно, резервное копирование завершится сбоем.

© ООО Киберпротект, 2026

Для восстановления с многопотоковой резервной копии или с многопотоковой и мультиплексированной резервной копии понадобится как минимум такое же количество приводов, которое было использовано при создании этой резервной копии.

Невозможно изменить настройки многопоточности в существующем плане защиты. Чтобы использовать другие настройки или изменить выбранные ленточные устройства, создайте новый план защиты.

Многопоточность доступна как для локально подключенных ленточных устройств, так и ленточных устройств, подключенных к узлу хранения.

6.14.27.7 Мультиплексирование

Значение по умолчанию: **Отключено**.

Мультиплексирование позволяет записывать потоки данных с нескольких агентов на один ленточный носитель. Это способствует улучшению использования быстрых ленточных устройств. По умолчанию коэффициент мультиплексирования (количество агентов, которые отправляют данные на один ленточный носитель) равен 2. Его можно увеличить до 10.

Мультиплексирование полезно для больших сред, в которых выполняется множество операций резервного копирования. Оно не повысит производительность единичных процессов резервного копирования.

Чтобы получить максимально возможную быстроту резервного копирования в большой среде, необходимо проанализировать производительность агентов, сети и ленточных устройств. После этого необходимо задать соответствующий коэффициент мультиплексирования. При этом следует избежать чрезмерного мультиплексирования. Например, если агенты передают данные со скоростью 70 Мбит/с, а скорость записи на ленточное устройство составляет 250 Мбит/с, то при отсутствии проблем (задержек) в сети установите для коэффициента мультиплексирования значение 3. Если для коэффициента мультиплексирования задать значение 4, это приведет к излишнему мильтиплексированию и снижению производительности резервного копирования. Как правило, значение коэффициента мультиплексирования задается в диапазоне от 2 до 5.

Резервные копии, созданные с использованием мультиплексирования, восстанавливаются медленнее. Это обусловлено их структурой. Чем выше коэффициент мультиплексирования, тем медленнее будет восстановление. Одновременное восстановление нескольких резервных копий, записанных на одну мультиплексированную ленту, не поддерживается.

Можно выбрать одно или несколько ленточных устройств для мультиплексирования или использовать мультиплексирование с любым доступным ленточным устройством. Мультиплексирование недоступно для ленточных устройств, подключенных локально.

Невозможно изменить настройки мультиплексирования в существующем плане защиты. Чтобы использовать другие настройки, создайте новый план защиты.

В плане защиты можно использовать следующие комбинации многопоточности и мультиплексирования:

© ООО Киберпротект, 2026

- **Настройки многопоточности и мультиплексирования отключены.**
  Каждый агент отправляет данные на одно ленточное устройство.
- **Выбрана только многопоточность.**
  Каждый агент одновременно отправляет данные как минимум на два ленточных устройства.
- **Выбрано только мультиплексирование.**
  Каждый агент отправляет данные на ленточное устройство, которое одновременно принимает потоки от нескольких агентов. Максимальное количество потоков, которые может принять ленточное устройство, задается в плане защиты. Его невозможно изменить «на ходу».
- **Настройки многопоточности и мультиплексирования выбраны.**
  Каждый агент отправляет данные как минимум на два ленточных устройства, которые одновременно принимают потоки от нескольких агентов.

Ленточное устройство единовременно может записывать только один тип резервной копии (с мультиплексированием или без мультиплексирования) в зависимости от того, какой план защиты запущен первым.

6.14.27.8 Использовать наборы лент в пуле лент, выбранных для резервного копирования

Значение по умолчанию: **Отключено**.

Ленты внутри одного пула можно объединить в так называемые **наборы лент**.

Если оставить этот параметр отключенным, резервное копирование данных будет выполнено на все ленты, принадлежащие пулу. Если включить этот параметр, можно разделить резервные копии в соответствии с предварительно определенными или пользовательскими правилами.

- **Используйте отдельный набор лент для каждого** (выберите правило: **Тип резервной копии**, **Тип устройства**, **Имя устройства**, **День месяца**, **День недели**, **Месяц**, **Год**, **Дата**).
  При выборе этого варианта возможна организация наборов лент в соответствии с предопределенным правилом. Например, можно указать отдельные наборы лент для каждого дня недели или хранить резервные копии каждой машины на отдельном наборе лент.
  Правило **Имя устройства** не работает, если используется режим мультиплексирования.

  Примечание
  Этот параметр рекомендуется включать при выборе схемы **Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS)** (см. "Расписание" (стр. 287)).
  Рекомендуется выбрать шаблон **День недели**.
  В таком случае для каждого дня недели будет использоваться отдельная лента. Резервные копии, созданные в понедельник, будут храниться на одной ленте. Резервные копии, созданные во вторник, будут храниться на другой ленте. И так далее.

- **Укажите настраиваемое правило для наборов лент**.

© ООО Киберпротект, 2026

При выборе этого варианта возможно указание собственного правила для организации наборов лент. Правило может содержать следующие переменные:

Синтаксис переменной	Описание переменной	Доступные значения
[Имя устройства]	Резервные копии на каждой машине будут храниться на отдельном наборе лент.	Имена машин, зарегистрированных на сервере управления.
[Тип резервной копии]	Полные, инкрементные и дифференциальные резервные копии будут храниться на отдельных наборах лент.	full, inc, diff
[Тип устройства]	Резервные копии каждого типа машин будут храниться на отдельном наборе лент.	Server essentials, Server, Workstation, VMware Virtual Machine, Virtual-PC Virtual Machine, Virtual Server Virtual Machine, Hyper-V Virtual Machine, XEN Virtual Machine, KVM Virtual Machine, RHEV Virtual Machine.
[День месяца]	Резервные копии, созданные в каждый день месяца, будут храниться на отдельном наборе лент.	01, 02, 03, ..., 31
[День недели]	Резервные копии, созданные в каждый день недели, будут храниться на отдельном наборе лент.	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
[Месяц]	Резервные копии, созданные в каждый месяц года, будут храниться на отдельном наборе лент.	January, February, March, April, May, June, July, August, September, October, November, December
[Год]	Резервные копии, созданные за год, будут храниться на отдельном наборе лент.	2017, 2018, ...
[Дата]	Резервные копии, созданные в определённую дату, будут храниться на отдельном наборе лент.	Дата в формате [Год].[Месяц].[День месяца] Где: ◦ [Год] – значение, доступное для переменной [Год]. ◦ [Месяц] – значение, доступное для переменной

© ООО Киберпротект, 2026

		[Месяц]. ◦ [День месяца] – значение, доступное для переменной [День месяца]. Пример: 2025.December.18

- Например, при указании правила [Имя устройства]-[Тип резервной копии] будет создан отдельный набор лент для каждой полной, инкрементной и дифференциальной резервной копии каждой машины, к которой применим план защиты.

Возможно указать набор лент для отдельных лент. В данном случае программное обеспечение сначала запишет резервные копии на ленты, значение набора лент которых совпадает со значением выражения, указанного в плане защиты. После чего при необходимости будут взяты другие ленты этого пула. Если пул пополняемый, после этого будут использованы ленты из пула **Свободные ленты**.

Например, при указании набора лент Monday для ленты 1, Tuesday для ленты 2 и т. д. и указании [День недели] в параметрах резервного копирования надлежащая лента будет использована в соответствующий день недели.

6.14.28 Действие при сбое плана

Этот параметр определяет поведение программы при сбое запланированного плана защиты. Этот параметр не действует для планов с параметром "Команды до и после процедуры" (стр. 365) или если план защиты запущен вручную.

Если этот параметр включен, то программа попытается еще раз выполнить план защиты. Можно задать временной интервал между попытками и количеством попыток. Попытки будут прекращены, когда задание будет выполнено успешно ИЛИ количество попыток достигнет указанного предела.

Значение по умолчанию: **Отключено**.

6.14.29 Условия запуска задания

Этот параметр применим в операционных системах Windows и Linux.

Этот параметр определяет поведение программы в момент, когда должно начаться выполнение задания (наступает запланированное время или событие, указанное в расписании), но не выполнено одно или несколько условий. Дополнительную информацию об условиях см. в разделе «Условия запуска».

Значение по умолчанию: **Дождитесь, пока будут выполнены все условия в расписании.**

6.14.29.1 Ожидать выполнения условий расписания

С этой настройкой планировщик начинает отслеживать условия и запускает задание, как только условия выполняются. Если условия не выполняются, задание не запускается.

© ООО Киберпротект, 2026

Чтобы предусмотреть случаи, когда условия не выполняются в течение слишком долгого времени и дальнейшая отсрочка задания становится рискованной, можно установить интервал времени, после которого задание запустится независимо от условия. Установите флажок **Запустить задание в любом случае через** и укажите интервал времени. Задание запустится, если будут выполнены условия или истечет максимальное время задержки.

6.14.29.2 Пропустить задание

Задержка выполнения задания может быть недопустима, например, если его необходимо выполнить точно в заданное время. В этом случае имеет смысл пропустить задание, а не ждать выполнения условий, особенно если задания выполняются сравнительно часто.

6.14.30 Служба теневого копирования томов (VSS)

Этот параметр работает только в операционных системах Windows.

Этот параметр указывает, должен ли поставщик службы теневого копирования томов (VSS) уведомлять VSS-совместимые приложения о предстоящем запуске резервного копирования. Это обеспечивает согласованное состояние всех данных, используемых приложениями. В частности, завершение всех транзакций в момент создания моментального снимка данных программным обеспечением резервного копирования. Согласованность данных, в свою очередь, обеспечивает восстановление приложения в корректном состоянии и возможность использования сразу после восстановления.

Значение по умолчанию: **Включено**. **Автоматический выбор поставщика моментальных снимков**.

Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:

- **Автоматически выбирать поставщика моментальных снимков**

  Автоматический выбор из следующих вариантов: аппаратный поставщик моментальных снимков, программные поставщики моментальных снимков и программный поставщик теневого копирования (Microsoft).
- **Использовать программного поставщика теневого копирования (Microsoft)**

  Мы рекомендуем выбрать этот параметр при резервном копировании серверов приложений (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint или Active Directory).

Отключите этот параметр, если база данных несовместима с VSS. Процесс создания моментальных снимков ускорится, но согласованность данных приложений, в которых имеются незавершенные транзакции, не гарантируется. Можно использовать Команды до и после захвата данных, чтобы обеспечить согласованность данных, для которых выполняется резервное копирование. Например, укажите команды до захвата данных, которые приостановят работу базы данных и перенесут содержимое всех временных хранилищ для обеспечения корректного выполнения транзакций, укажите команды после захвата данных, которые возобновят операции базы данных после выполнения моментального снимка.

© ООО Киберпротект, 2026

Примечание
Если этот параметр включен, резервное копирование файлов и папок, указанных в ключе реестра **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**, не выполняется. В частности, не выполняется резервное копирование файлов данных Outlook (.ost), поскольку они указаны в значении **OutlookOST** данного ключа.

6.14.30.1 Включить полное резервное копирование VSS

Если этот параметр включен, журналы Microsoft Exchange Server и других приложений, поддерживающих VSS (кроме Microsoft SQL Server), будут сокращаться каждый раз после полного, инкрементного или дифференциального резервного копирования на уровне дисков.

Значение по умолчанию: **Отключено**.

Оставьте параметр отключенным в следующих случаях:

- Если для резервного копирования данных Exchange Server используется агент для Exchange или ПО сторонних производителей. В этом случае усечение журналов помешает последующему резервному копированию журналов транзакций.
- Если для резервного копирования данных SQL Server используется программное обеспечение сторонних производителей. Программа стороннего производителя будет воспринимать получившуюся резервную копию диска как «свою собственную» полную резервную копию. В результате следующее дифференциальное резервное копирование данных SQL Server завершится ошибкой. Резервное копирование будет завершаться ошибкой, пока программа стороннего производителя не создаст следующую собственную полную резервную копию.
- Если на машине работают другие VSS-совместимые приложения, журналы которых необходимо хранить по какой-либо причине.

При включении этого параметра не происходит усечения журналов Microsoft SQL Server. Чтобы сократить журнал SQL Server после выполнения резервного копирования, включите параметр резервного копирования Сокращение журнала Microsoft SQL Server.

6.14.31 Служба теневого копирования томов (VSS) для виртуальных машин

Этот параметр определяет, следует ли создавать замороженные моментальные снимки виртуальных машин. Чтобы создать замороженный моментальный снимок, программное обеспечение резервного копирования применяет VSS в виртуальной машине, используя VMware Tools или Hyper-V Integration Services.

Значение по умолчанию: **Включено**.

Если этот параметр включен, то транзакции всех приложений с поддержкой VSS, которые запущены на виртуальной машине, завершаются перед созданием моментального снимка. Если после нескольких попыток, количество которых определено параметром "Обработка ошибок", не удается создать замороженный моментальный снимок и резервное копирование приложений

© ООО Киберпротект, 2026

отключено, создается обычный моментальный снимок. Если включено резервное копирование приложений, то резервное копирование завершается сбоем.

Если этот параметр отключен, создается обычный моментальный снимок. Будет создана резервная копия виртуальной машины с защитой от сбоев. Рекомендуем не выключать этот параметр даже на время и даже для виртуальных машин, на которых не выполняются приложения с поддержкой VSS. В противном случае невозможно будет гарантировать даже однородность файловой системы в рамках созданной резервной копии.

Примечание
Этот параметр не влияет на виртуальные машины oVirt, SpaceVM, ECP VeiL, а также OpenStack. Для них заморозка зависит от того, установлены ли инструменты масштабирования на виртуальной машине.

6.14.32 Еженедельное резервное копирование

Этот параметр определяет то, какие процессы резервного копирования считаются «еженедельными» в правилах хранения и схемах резервного копирования. «Еженедельная» резервная копия – это первая копия, которая создается после начала недели.

Значение по умолчанию: **Понедельник**.

6.14.33 Журнал событий Windows

Этот параметр работает только в ОС Windows.

Этот параметр указывает, должны ли агенты записывать события операций резервного копирования в журнал событий приложений Windows (чтобы просмотреть этот журнал, запустите файл eventvwr.exe или выберите **Панель управления** > **Администрирование** > **Просмотр событий**). События содержат статус и время завершения операции; события можно фильтровать.

Значение по умолчанию: **Отключено**.

© ООО Киберпротект, 2026

7 Восстановление

7.1 Восстановление: памятка

Кибер Бэкап поддерживает множество сценариев восстановления:

- универсальное восстановление физических и виртуальных машин;
- восстановление физической машины в виртуальную;
- миграцию при восстановлении виртуальных машин;
- мгновенное восстановление виртуальных машин;
- гранулярное восстановление данных (файлов, дисков, баз данных, почтовых ящиков и т. д.).

В таблице ниже описаны данные, доступные для гранулярного восстановления.

Тип агента	Источник данных	Гранулярность
Для операционной системы	Linux, Windows	Диск/том, папка, файл
Для платформы виртуализации (на уровне гипервизора)	VMware, Hyper-V, oVirt, zVirt, ROSA, HOSTVM, Red Hat Virtualization, Basis DynamiX, РЕД Виртуализация, ECP Veil, SpaceVM, Кибер Инфраструктура, OpenStack, VK Cloud, OpenNebula, Брест	Диск/том, папка, файл
Для СУБД	Microsoft SQL Server, Oracle Database, SAP HANA, Ред База Данных, PostgreSQL и СУБД на ее основе	База данных
	MySQL, MariaDB	База данных, таблица
Для платформы коммуникаций	Microsoft Exchange Server, VK WorkMail, Mailion, CommuniGate Pro	Почтовый ящик, сообщение

Кибер Бэкап поддерживает различные методы восстановления. В таблице ниже кратко описаны доступные методы для каждой целевой системы.

Объект восстановления	Метод восстановления
Физическая машина (Windows или Linux)	Использование веб-интерфейса Использование загрузочного носителя
Виртуальная машина	Использование веб-интерфейса
Конфигурация ESXi	Использование загрузочного носителя
Файлы и папки	Использование веб-интерфейса

© ООО Киберпротект, 2026

	Использование загрузочного носителя Извлечение файлов из локальных резервных копий
Базы данных Microsoft SQL Server	Использование веб-интерфейса
Базы данных Microsoft Exchange Server	Использование веб-интерфейса
Почтовые ящики Microsoft Exchange Server	Использование веб-интерфейса
Базы данных PostgreSQL	Использование веб-интерфейса
Базы данных Oracle	Использование инструмента Oracle Explorer
Данные CommuniGate Pro	Использование веб-интерфейса
Данные VK WorkMail и VK WorkDisk	Использование веб-интерфейса
Данные Mailion	Использование веб-интерфейса
Данные Kubernetes	Использование веб-интерфейса
Данные MySQL и MariaDB	Использование веб-интерфейса
Ред База Данных	Использование веб-интерфейса
Серверы SAP HANA	Использование веб-интерфейса

7.2 Создание загрузочных носителей

Загрузочный носитель – это компакт-диск, DVD-диск, флэш-накопитель USB или другой съемный носитель, с помощью которого можно запустить агент, не используя операционную систему. Основная задача, для которой применяются такие носители, – восстановление операционной системы, которую не удается загрузить.

Мы настоятельно рекомендуем создать и протестировать загрузочный носитель сразу же после первого создания резервных копий дисков. Кроме того, рекомендуется повторно создавать носитель после каждого основного обновления агента защиты.

С помощью одного носителя можно восстановить как ОС Windows, так и Linux.

Создание загрузочного носителя в Windows и Linux

1. Загрузите ISO-файл загрузочного носителя с веб-сайта Киберпротект.
2. Выполните любое из следующих действий:
   - Запишите компакт- или DVD-диск, используя ISO-файл.
   - Создайте загрузочный флэш-накопитель USB, используя ISO-файл и один из бесплатных инструментов, доступных в Интернете.

     Для машин с UEFI используйте ISO to USB или RUFUS, для машин с BIOS – Win32DiskImager. В Linux можно воспользоваться утилитой dd.

© ООО Киберпротект, 2026

- Подключите ISO-файл в качестве CD/DVD-дисковода к виртуальной машине, которую требуется восстановить.

Кроме того, можно создать загрузочный носитель, используя Мастер создания загрузочных копий.

7.3 Восстановление машины

7.3.1 Физическая машина

В этом разделе описано восстановление физических машин через веб-интерфейс.

Используйте вместо веб-интерфейса загрузочный носитель, если вам необходимо восстановить:

- Любую операционную систему на «голое железо» либо на отключенной машине.
- Структуру логических томов (тома созданы диспетчером логических томов в ОС Linux). Носитель позволяет автоматически воссоздать структуру логических томов.

Для восстановления операционной системы потребуется перезагрузка. Вы можете перезапустить машину автоматически или присвоить ей статус **Требуется вмешательство**. Восстановленная операционная система автоматически запускается.

Восстановление физической машины

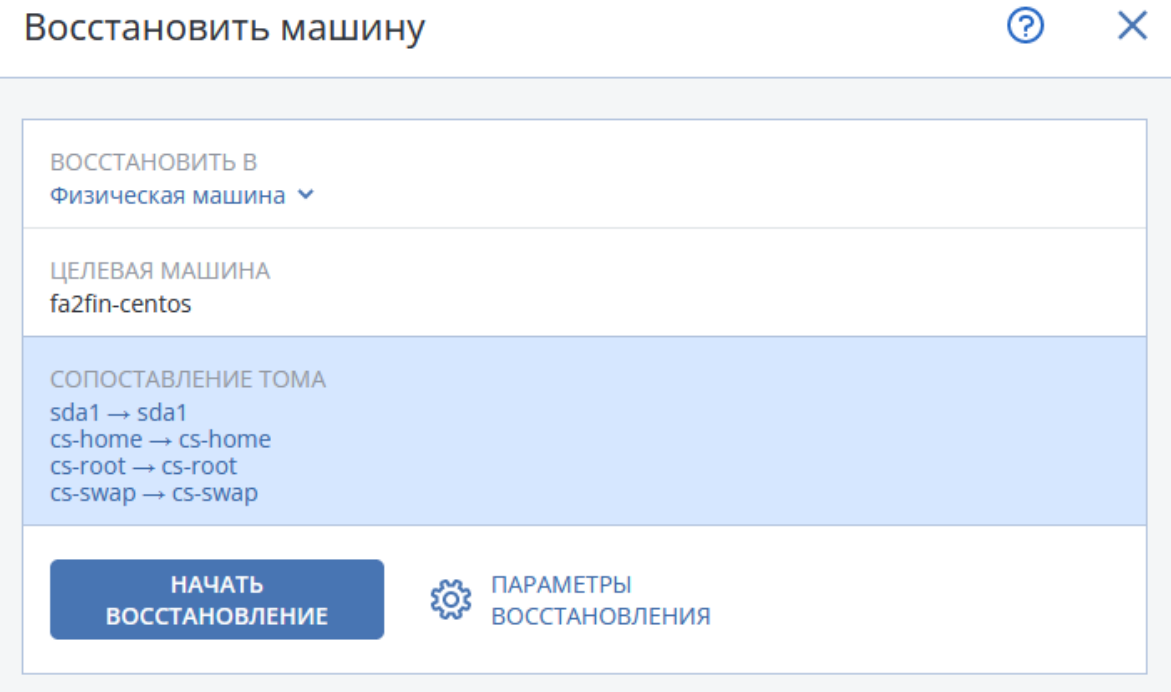
1. Выберите машину, для которой есть резервная копия.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните любое из следующих действий:
   - Если резервная копия расположена в общем хранилище данных (т. е. другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилища резервных копий.
   - Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя».
4. Последовательно выберите пункты **Восстановление** > **Вся машина**.

   Программное обеспечение автоматически сопоставит диски из резервной копии с дисками целевой машины.

   Чтобы выполнить восстановление в другую виртуальную машину, щелкните **Целевая машина** и выберите включенную целевую машину.

© ООО Киберпротект, 2026



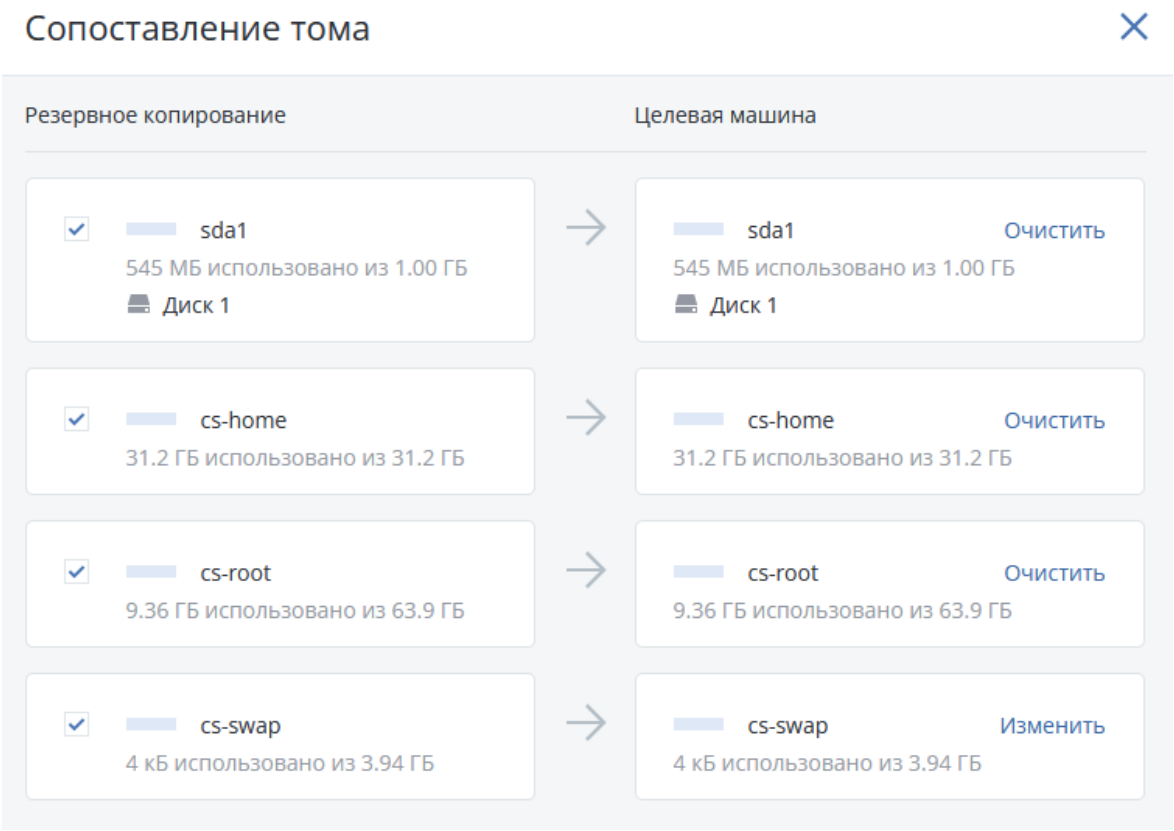
5. Если результат сопоставления вас не удовлетворяет или если выполнить сопоставление не удалось, нажмите **Сопоставление тома**, чтобы сопоставить диски заново вручную.

   Раздел сопоставления также позволяет вам выбирать отдельные диски или тома для восстановления.

Примечание

Автоматическое сопоставление томов возможно только в последовательном порядке при условии, что конфигурации целевой машины и машины-источника одинаковы. Если конфигурации машин различаются, сопоставить тома можно только в ручном режиме.

© ООО Киберпротект, 2026



6. Щелкните **Начать восстановление**.
7. Подтвердите перезапись дисков версиями из резервной копии. Укажите, следует ли автоматически перезапустить машину.

Ход выполнения восстановления показан на вкладке **Действия**.

7.3.2 Восстановление физической машины в виртуальную

В этом разделе описано восстановление физической машины в качестве виртуальной (P2V) с использованием веб-интерфейса. Эту операцию можно выполнить, если установлен и зарегистрирован хотя бы один агент для целевой платформы виртуализации.

Доступные места восстановления и ограничения восстановления P2V см. в разделе "Миграция машины" (стр. 717).

Для восстановления физической Linux-машины с логическими томами (LVM) в виртуальную см. раздел "Миграция Linux-машины с логическими томами (LVM)" (стр. 720).

Восстановление физической машины как виртуальной

1. Выберите машину, для которой есть резервная копия.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

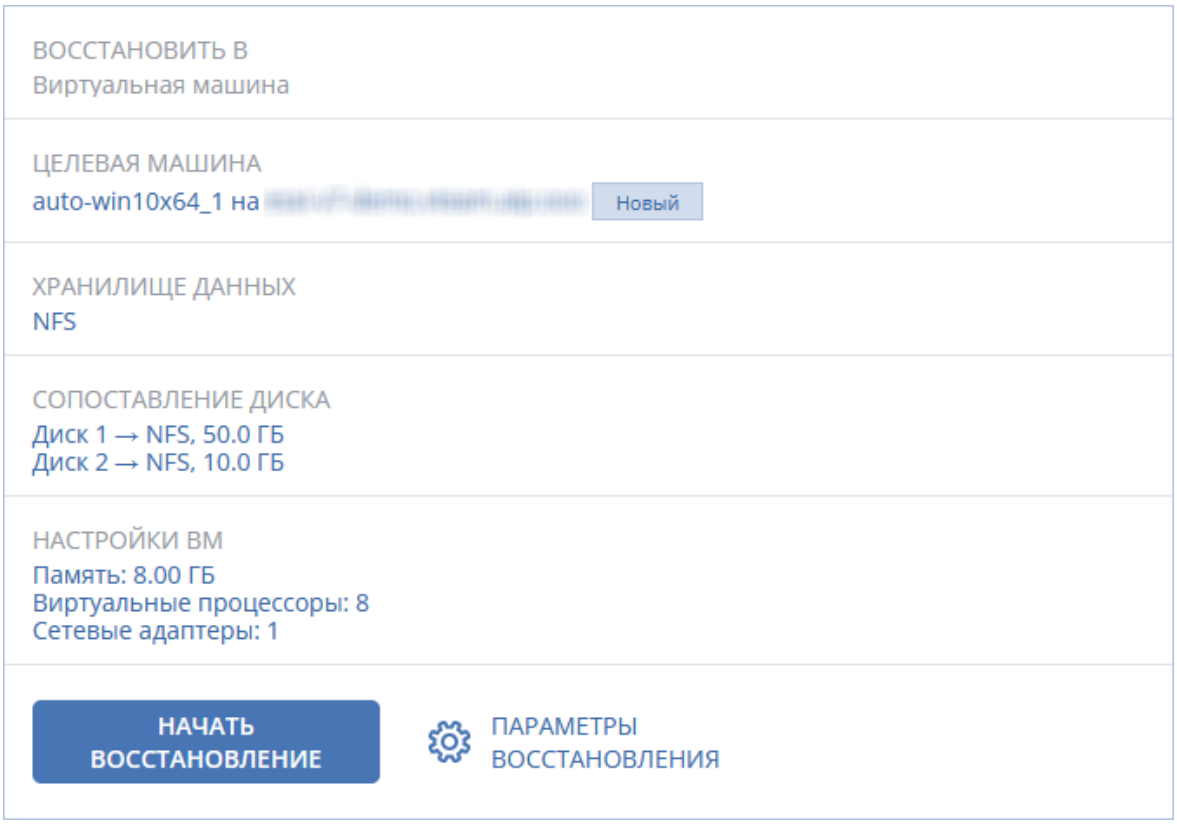
© ООО Киберпротект, 2026

Если машина отключена, точки восстановления не отображаются. Выполните любое из следующих действий:

- Если резервная копия расположена в общем хранилище данных (другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите машину, а затем выберите точку восстановления.
- Выберите точку восстановления на вкладке Хранилища резервных копий.
- Восстановите машину, как описано в разделе "Восстановление дисков с помощью загрузочного носителя" (стр. 390).

4. Последовательно выберите пункты **Восстановление** > **Вся машина**.
5. В поле **Восстановить в** выберите пункт **Виртуальная машина**.
6. Щелкните **Целевая машина**.
   a. В выпадающем списке выберите тип целевой виртуальной машины.
      Должен быть установлен хотя бы один агент для выбранного типа виртуальной машины.
   b. Выберите машину, в которую будут выполняться восстановление: новая или существующая. Выбор новой машины предпочтительнее, поскольку для нее не требуется, чтобы конфигурация диска целевой машины в точности соответствовала конфигурации диска в резервной копии.
   c. Выберите хост и укажите имя новой машины или выберите существующую целевую машину.
   d. Нажмите кнопку **OK**.
7. [Необязательно] При восстановлении в новую машину также можно выполнить следующие действия:
   - Щелкните **Хранилище данных** (или **Путь** для Hyper-V) и выберите хранилище данных для данной виртуальной машины.
   - Щелкните **Сопоставление дисков**, чтобы выбрать хранилище данных, интерфейс и режим распределения для каждого виртуального диска. Раздел сопоставления также позволяет выбирать отдельные диски для восстановления.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.

© ООО Киберпротект, 2026



8. Щелкните **Начать восстановление**.
9. При восстановлении в существующую виртуальную машину подтвердите перезапись дисков.

Ход выполнения восстановления показан на вкладке **Действия**.

7.3.3 Виртуальная машина

Восстановление на виртуальную машину выполняется, только когда машина остановлена. Программа останавливает машину без запроса. После завершения восстановления машину потребуется запустить вручную.

Это поведение можно изменить, используя параметр восстановления «Управление питанием ВМ» (выберите **Параметры восстановления** > **Управление питанием ВМ**).

Восстановление виртуальной машины

1. Выполните одно из следующих действий:
   - Выберите машину, для которой создана резервная копия, выберите **Восстановление** и выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилища резервных копий.
2. Последовательно выберите пункты **Восстановление** > **Вся машина**.
3. Чтобы выполнить восстановление на физическую машину, в списке **Восстановить в** выберите пункт **Физическая машина**. В противном случае пропустите этот шаг.

   Восстановление в физическую машину возможно только в том случае, если конфигурация целевой машины в точности соответствует конфигурации диска в данной резервной копии.

© ООО Киберпротект, 2026

В этом случае продолжите с шага 4 в разделе «Физическая машина». В противном случае рекомендуется выполнить миграцию виртуальной машины в физическую (V2P), используя загрузочный носитель.

4. По умолчанию исходная машина выбирается в качестве целевой.

   Чтобы выполнить восстановление на другую виртуальную машину, выберите **Целевая машина** и выполните следующие действия:

   a. Выберите гипервизор.

   b. Выберите машину, в которую будет выполняться восстановление: новая или существующая.

   Примечание
   Виртуальные машины OpenStack можно восстанавливать только в новые ВМ.

   c. Выберите хост и укажите имя новой машины или выберите существующую целевую машину.

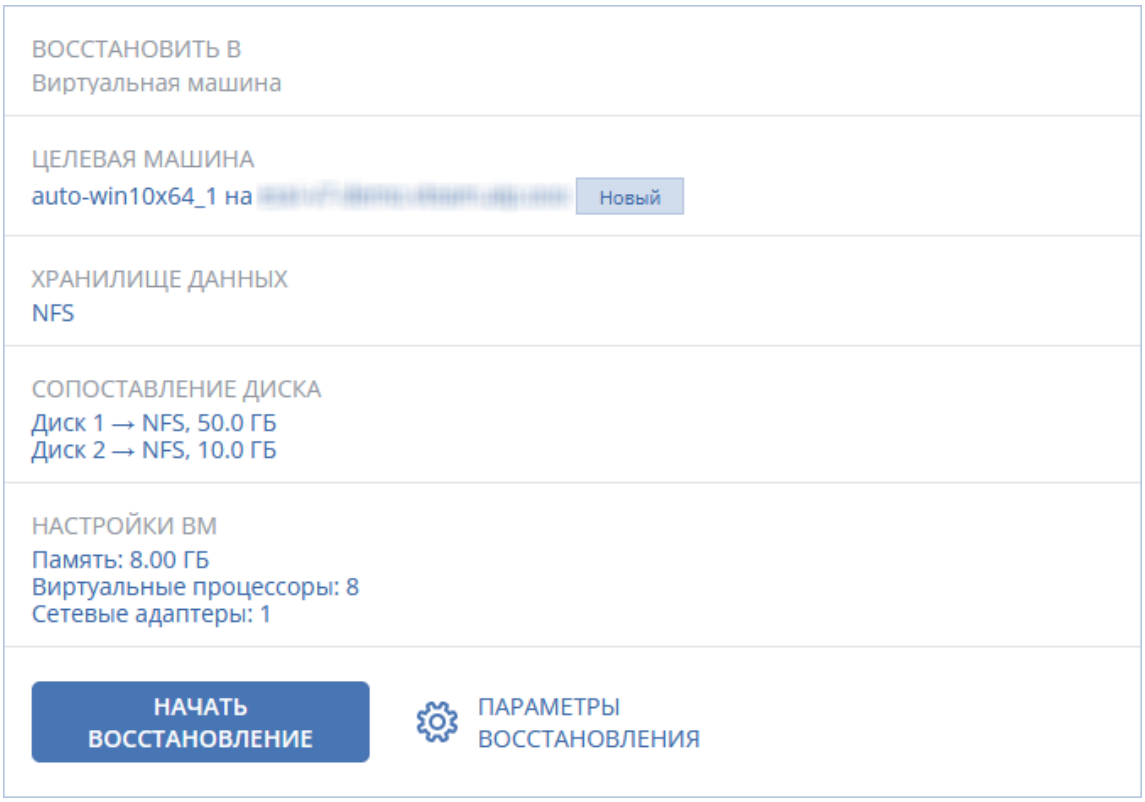
   d. Нажмите кнопку **OK**.

5. [Необязательно] При восстановлении в новую машину также можно выполнить следующие действия:

   - Щелкните **Хранилище данных** (или **Путь** для Hyper-V) и выберите хранилище данных для виртуальной машины.
   - Щелкните **Сопоставление диска**, чтобы выбрать интерфейс и режим распределения для каждого виртуального диска. Раздел сопоставления также позволяет выбирать отдельные диски для восстановления.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.

   Примечание
   При необходимости ВМ можно восстановить без сетевых адаптеров. Исключение составляет система OpenStack и продукты на её основе (Кибер Инфраструктура, VK Cloud), ВМ в которых всегда должны иметь хотя бы один сетевой адаптер.

© ООО Киберпротект, 2026



6. Щелкните **Начать восстановление**.
7. При восстановлении в существующую виртуальную машину подтвердите перезапись дисков.

Ход выполнения восстановления показан на вкладке **Действия**.
При восстановлении виртуальной машины OpenStack из резервной копии будут созданы только диски и сетевой порт виртуальной машины, если:

- в конфигурации OpenStack используется единственная внешняя сеть без подсетей и внешний DHCP-сервер (автоматическое восстановление виртуальной машины невозможно из-за ограничений OpenStack);
- виртуальную машину OpenStack не удается восстановить из-за ошибок ПО OpenStack (например, нет доступных хостов для запуска виртуальной машины).

В таком случае используйте восстановленные диски, чтобы создать новую ВМ вручную из командной строки OpenStack (подробнее см. в официальной документации OpenStack).

7.3.4 Восстановление дисков с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя».

Порядок восстановления дисков с помощью загрузочного носителя

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.

© ООО Киберпротект, 2026

3. Если в вашей сети включен прокси-сервер, щелкните **Инструменты** > **Прокси-сервер** и укажите имя хоста/IP-адрес и порт прокси-сервера. В противном случае пропустите этот шаг.
4. На экране приветствия нажмите кнопку **Восстановить**.
5. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
6. Укажите хранилище резервных копий.
   - Чтобы восстановить данные из локальной или сетевой папки, укажите ее в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **OK**, чтобы подтвердить выбор.
7. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
8. В разделе **Содержимое резервной копии** выберите диски, которые нужно восстановить. Нажмите кнопку **OK**, чтобы подтвердить выбор.
9. В разделе **Место восстановления** программное обеспечение автоматически сопоставит выбранные диски с целевыми.

   Если выполнить сопоставление не удалось или его результат вас не устраивает, сопоставьте диски заново вручную.

   Примечание
   Изменение структуры дисков может повлиять на загружаемость операционной системы. Если вы не уверены в полном успехе, используйте исходную структуру дисков машины.
10. [Только для ОС Linux] Если на машине, резервная копия которой создавалась, имелись логические тома (LVM), а вам необходимо воспроизвести исходную структуру LVM, выполните перечисленные ниже действия:
    a. Убедитесь, что количество дисков на целевой машине и емкость каждого диска равны аналогичным значениям исходной машины, а затем щелкните **Применить RAID/LVM**.
    b. Просмотрите структуру томов, а затем нажмите кнопку **Применить RAID/LVM**, чтобы создать ее.
11. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
12. Нажмите кнопку **OK**, чтобы начать восстановление.

7.3.5 Использование компонента Универсальное восстановление (Universal Restore)

Новейшие версии операционных систем сохраняют загружаемость при восстановлении на отличающееся оборудование или платформы виртуализации. Если восстановленная операционная система не загружается, используйте компонент Универсальное восстановление (Universal Restore), чтобы обновить драйверы и модули, необходимые для загрузки системы.

Компонент можно применить к операционным системам Windows и Linux.

Порядок использования компонента Универсальное восстановление (Universal Restore)

© ООО Киберпротект, 2026

1. Загрузите машину с загрузочного носителя.
2. Щелкните **Использовать Universal Restore**.
3. Если на машине несколько операционных систем, выберите, к какой из них следует применить данный компонент.
4. [Только для Windows] Настройка дополнительных настроек.
5. Нажмите кнопку **OK**.

7.3.5.1 Компонент Универсальное восстановление (Universal Restore) в Windows

Подготовка

Подготовьте драйверы

Прежде чем применять компонент Универсальное восстановление (Universal Restore) к операционной системе Windows, удостоверьтесь в наличии драйверов для нового контроллера жестких дисков и набора микросхем. Эти драйверы являются критическими для запуска операционной системы. Используйте компакт-диски или DVD-диски, предоставленные поставщиками аппаратных средств, или загрузите драйверы с веб-сайта поставщика. Файлы драйверов должны иметь расширение *.inf. В случае загрузки драйверов в форматах EXE, CAB или ZIP получите их с помощью стороннего приложения.

Наилучшим решением является хранение драйверов для всех аппаратных средств, используемых в организации, в едином репозитории с сортировкой по типу устройств или аппаратным конфигурациям. Копию репозитория можно хранить на DVD-диске или флэш-накопителе, поместить нужные драйверы на загрузочный носитель или создать пользовательский загрузочный носитель с требуемыми драйверами (а также файлами конфигурации сети) для каждого сервера. Или можно просто указывать путь к репозиторию каждый раз, когда используется данный компонент.

Проверьте наличие доступа к драйверам в загрузочной среде

Убедитесь в наличии доступа к устройству с драйверами при работе с загрузочного носителя. Используйте носитель на основе WinPE, если устройство доступно в Windows, но носитель на основе Linux не обнаружил его.

Настройки компонента Универсальное восстановление (Universal Restore)

Автоматический поиск драйверов

Укажите, где программа должна искать драйверы слоя абстрагирования оборудования (HAL), контроллера жестких дисков и сетевых адаптеров.

- Если драйверы находятся на диске от производителя или другом съемном носителе, установите флажок **Поиск на съемных носителях**.

© ООО Киберпротект, 2026

- Если драйверы находятся в сетевой папке или на загрузочном носителе, укажите путь к этой папке, нажав кнопку **Добавить папку**.

Кроме того, компонент выполнит поиск драйверов в папке, используемой по умолчанию для хранения драйверов Windows. Ее расположение определяется значением реестра **DevicePath** в разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Обычно это папка WINDOWS/inf.

Компонент выполнит рекурсивный поиск во всех папках, вложенных в указанную папку, обнаружит наиболее подходящие драйверы HAL и контроллера жестких дисков из всех имеющихся и установит их в операционную систему. Компонент выполняет также поиск драйвера сетевого адаптера. После его обнаружения компонент передает путь к найденному драйверу операционной системе. Если на машине установлено несколько сетевых интерфейсных плат, компонент попытается настроить драйверы всех плат.

Драйверы запоминающих устройств для обязательной установки

Этот параметр необходим в следующих случаях.

- На компьютере установлен особый контроллер запоминающего устройства, например RAID (особенно NVIDIA RAID) или адаптер Fibre Channel.
- Система перенесена на виртуальную машину, которая использует контроллер жесткого диска SCSI. Используйте драйверы SCSI, предоставленные в пакете программного обеспечения виртуализации, или загрузите последние версии драйверов с веб-сайта разработчика программного обеспечения.
- Если не удалось загрузить систему с помощью автоматического поиска драйверов.

Укажите нужные драйвер, нажав кнопку **Добавить драйвер**. Указанные драйверы будут установлены, даже если программа найдет лучший драйвер, с выдачей соответствующего предупреждения.

Применение компонента Универсальное восстановление (Universal Restore)

Указав требуемые настройки, нажмите кнопку **OK**.

Если компоненту не удается найти совместимый драйвер в указанных расположениях, будет выведено сообщение о проблемном устройстве. Выполните одно из следующих действий:

- Добавьте драйвер в любое из ранее указанных расположений и нажмите кнопку **Повторить**.
- Если вы не помните расположения, нажмите кнопку **Пропустить**, чтобы продолжить процесс. При неудовлетворительном результате заново примените компонент. При настройке операции укажите необходимый драйвер.

После загрузки Windows начнется стандартная процедура установки новых устройств. Драйвер сетевого адаптера будет установлен без уведомлений при наличии у него подписи Microsoft Windows. В противном случае Windows попросит подтвердить установку неподписанного драйвера.

© ООО Киберпротект, 2026

После этого пользователь сможет настроить сетевое подключение и указать драйверы для видеоадаптера, USB и других устройств.

7.3.5.2 Компонент Универсальное восстановление (Universal Restore) в Linux

Компонент Универсальное восстановление (Universal Restore) может применяться к операционным системам Linux с версией ядра 3.0 или более поздней.

Если компонент применяется к операционной системе Linux, обновляется временная файловая система, известная как начальный электронный диск (initrd). Это обеспечивает загрузку операционной системы на новом оборудовании.

Компонент добавляет к начальному электронному диску модули для нового оборудования (включая драйверы устройств). Обычно все необходимые модули обнаруживаются в папке **/lib/modules**. Если компонент не может найти нужный модуль, имя файла модуля записывается в журнал.

Компонент может изменить конфигурацию загрузчика GRUB. Возможно, для этого потребуется обеспечить загружаемость системы, если структура томов новой машины отличается от исходной машины.

Компонент никогда не изменяет ядро Linux.

Возврат к исходному начальному RAM-диску

При необходимости можно вернуться к исходному начальному RAM-диску.

Начальный RAM-диск хранится в файле на машине. Перед первым обновлением начального RAM-диска компонент сохраняет его копию в той же папке. Имя копии – это имя файла с прибавлением суффикса **_acronis_backup.img**. При запуске компонента более одного раза (например, после добавления недостающих драйверов) эта копия не перезаписывается.

Чтобы вернуться к исходному начальному RAM-диску, выполните любое из следующих действий.

- Измените имя копии соответствующим образом. Например, выполните команду, подобную следующей:

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- Укажите копию в строке **initrd** конфигурации загрузчика GRUB.

7.4 Восстановление файлов

7.4.1 Восстановление файлов с помощью веб-интерфейса

С помощью веб-консоли Кибер Бэкап можно восстановить файлы, которые ранее были расположены на физической или виртуальной машине с установленным агентом, или на машине,

© ООО Киберпротект, 2026

защищённой с помощью виртуального устройства (virtual appliance).

Восстановить файлы можно:

- на физическую или виртуальную машину с агентом (как на исходную, так и на другую);
- путём сохранения их в сетевое хранилище, из которого впоследствии их можно будет извлечь;
- загрузив их с помощью веб-консоли на машину, в которой открыта веб-консоль.

7.4.1.1 Порядок восстановления файлов

1. В веб-консоли Кибер Бэкап перейдите во вкладку **Устройства**.
2. Выберите машину, файлы которой необходимо восстановить.
3. Щелкните **Восстановление**.
4. Выберите точку восстановления, нажав на соответствующие дату и время точки восстановления.

   Примечание
   Если резервные копии хранятся в нескольких хранилищах, то точки восстановления будут отфильтрованы по хранилищу. Для выбора хранилища установите флажок напротив имени хранилища в списке **Хранилище резервных копий**.

   Если физическая или виртуальная машина с установленным агентом отключена, то значок машины будет серого цвета, а точки восстановления не будут отображены. В этом случае выполните одно из предлагаемых в веб-консоли действий:
   - [Рекомендуется] Если резервная копия расположена в общем хранилище данных (т. е. другие агенты могут получить к ней доступ), щёлкните **Выбор машины**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке **Хранилища резервных копий**.
   - Используйте загрузочный носитель (подробнее см. в разделе "Восстановление файлов с помощью загрузочного носителя" (стр. 396)).
5. Нажмите кнопку **Восстановление** и выберите **Файлы/папки**.
6. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов и папок.

   Можно использовать один или несколько подстановочных символов (* и ?), подробнее см. в разделе "Фильтры файлов" (стр. 356).
7. Отметьте флажками папки и файлы, которые необходимо восстановить.
8. Если требуется сохранить выбранные папки и файлы на машине, с помощью которой открыта веб-консоль Кибер Бэкап, нажмите кнопку **Загрузить** (иначе пропустите этот шаг). В результате выбранные файлы будут загружены в компьютер.

   Примечание
   Если выбрана папка или несколько файлов, загрузка будет выполнена в виде ZIP-архива.

© ООО Киберпротект, 2026

Внимание
Если общий размер выбранных файлов превышает 100 МБ, загрузка будет недоступна.

9. Если требуется восстановить выбранные папки и файлы на машину с установленным агентом, или чтобы сохранить файлы в сетевом хранилище, доступном машине с агентом (который будет выполнять восстановление), нажмите кнопку **Восстановить**.
10. Выберите целевую машину в блоке **Восстановить в**, нажав на отображаемое имя машины, затем в предложенном списке выберите машину с установленным агентом и нажмите **OK**.
11. В случае отображения окна **Укажите учётные данные** введите имя пользователя и пароль учётной записи для доступа к хранилищу с выбранной резервной копией.
12. В блоке **Путь** установите флажок для выбора целевого места на машине, куда будут сохранены восстанавливаемые файлы. Доступные варианты:
    - Исходное расположение (доступно только при восстановлении на исходную физическую или виртуальную машину с установленным агентом).
    - Пользовательское расположение, нажав **Обзор**, можно выбрать:
      - локальную папку на машине с агентом, с помощью которой осуществляется восстановление;
      - сетевую папку, доступную для машины с агентом, с помощью которой выполняется восстановление.
13. Нажмите кнопку **Начать восстановление**.
14. Выберите один из вариантов восстановления файлов:
    - **Перезаписывать существующие файлы**.
    - **Перезаписывать существующие файлы более новыми**.
    - **Не перезаписывать существующие файлы**.
15. Установите или снимите флажок **При необходимости перезагрузить машину**.
16. Нажмите кнопку **Продолжить**.

Ход выполнения восстановления будет отображаться справа во всплывающей области **Сведения о действии**, а также в разделе **Панель мониторинга** > **Действия**.

7.4.2 Восстановление файлов с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя».

Восстановление файлов с помощью загрузочного носителя

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
3. Если в вашей сети включен прокси-сервер, щелкните **Инструменты** > **Прокси-сервер** и укажите имя хоста/IP-адрес и порт прокси-сервера. В противном случае пропустите этот шаг.

© ООО Киберпротект, 2026

4. На экране приветствия нажмите кнопку **Восстановить**.
5. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
6. Укажите хранилище резервных копий.
   - Чтобы восстановить данные из локальной или сетевой папки, укажите ее в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **OK**, чтобы подтвердить выбор.
7. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
8. В области **Содержимое резервной копии** выберите **Файлы/папки**.
9. Выберите данные, которые необходимо восстановить. Нажмите кнопку **OK**, чтобы подтвердить выбор.
10. В разделе **Место восстановления** укажите нужную папку. При желании можно запретить перезапись более новых версий файлов или исключить некоторые файлы из списка восстанавливаемых.
11. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
12. Нажмите кнопку **OK**, чтобы начать восстановление.

Примечание
Хранилище на ленте занимает много места и может не соответствовать ОЗУ при повторном сканировании или восстановлении с использованием загрузочного носителя на основе Linux или WinPE. Для Linux нужно будет подключить другое хранилище для сохранения данных на диске или ресурсе общего доступа. Для Windows PE пока нет решения этой проблемы.

7.4.3 Извлечение файлов из локальных резервных копий

Можно просмотреть содержимое резервных копий и извлечь необходимые файлы.

7.4.3.1 Требования

- Эта функциональность доступна только в Windows при использовании проводника.
- На машине, на которой выполняется поиск резервной копии, должен быть установлен агент защиты.
- Файловая система, для которой создается резервная копия, должна иметь один из следующих типов: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS или HFS+.
- Резервная копия должна хранится в локальной папке или в сетевой папке (SMB/CIFS).

Порядок извлечения файлов из резервной копии

1. Перейдите в хранилище резервных копий, используя проводник.
2. Дважды щелкните файл резервной копии. Файлы имеют имена на основе следующего шаблона:

© ООО Киберпротект, 2026

<имя машины> - <GUID плана защиты>

3. Если резервная копия защищена паролем, укажите его. В противном случае пропустите этот шаг.

   В проводнике отображаются точки восстановления.
4. Дважды щелкните точку восстановления.

   В проводнике отображаются данные, для которых созданы резервные копии.
5. Обзор требуемой папки.
6. Скопируйте требуемые файлы в любую папку в файловой системе.

7.5 Восстановление конфигурации ESXi

Чтобы восстановить конфигурацию ESXi, необходим загрузочный носитель на основе Linux. Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя».

Если при восстановлении конфигурации ESXi на хост, который не является исходным, исходный хост ESXi все еще подключен к vCenter Server, отключите и удалите этот хост из vCenter Server, чтобы избежать неожиданных проблем при восстановлении. Чтобы сохранить исходный хост вместе с восстановленным, можно снова добавить его по окончании восстановления.

Виртуальные машины, которые выполняются на данном хосте, не включены в резервную копию конфигурации ESXi. Создать для них резервную копию и восстановить их можно отдельно.

Порядок восстановления конфигурации ESXi

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Щелкните **Локальное управление этой машиной**.
3. На экране приветствия нажмите кнопку **Восстановить**.
4. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
5. Укажите хранилище резервных копий.
   - Укажите папку в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **OK**, чтобы подтвердить выбор.
6. В поле **Показать** выберите **Конфигурации ESXi**.
7. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
8. Нажмите кнопку **OK**.
9. В разделе **Диски для новых хранилищ данных** выполните следующие действия:
   - В поле **Восстановить ESXi в** выберите диск, на который будет восстановлена конфигурация хоста. При восстановлении конфигурации на исходный хост исходный диск выбирается по умолчанию.
   - [Необязательно] В поле **Использовать для новых хранилищ данных** выберите диски, в которых будут созданы новые хранилища данных. Будьте внимательны, поскольку все

© ООО Киберпротект, 2026

данные на выбранных дисках могут быть утрачены. Чтобы сохранить виртуальные машины в существующих хранилищах данных, не выбирайте никакие диски.

10. Если для новых хранилищ данных выбраны какие-либо диски, выберите метод создания хранилища данных в поле **Создание новых хранилищ данных**: **Создать одно хранилище данных на диск** или **Создать одно хранилище на всех выбранных жестких дисках**.
11. [Необязательно] В разделе **Сопоставление сети** измените результат автоматического сопоставления виртуальных коммутаторов, присутствующих в резервной копии, с физическими сетевыми картами.
12. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
13. Нажмите кнопку **OK**, чтобы начать восстановление.

7.6 Параметры восстановления

Чтобы изменить параметры восстановления, щелкните **Параметры восстановления** при настройке восстановления.

7.6.1 Доступность параметров восстановления

Набор доступных параметров восстановления зависит от следующих факторов.

- Среда, в которой работает агент, выполняющий восстановление (Windows, Linux или загрузочный носитель).
- Тип данных, для которых выполняется восстановление (диски, файлы, виртуальные машины, данные приложения).

Следующая таблица включает в себя общие сведения о доступности параметров восстановления.

	Диски			**Файлы**			**Виртуальные машины**	**SQL и Exchange**
	Windows	Linux	Загрузочный носитель	Windows	Linux	Загрузочный носитель	ESXi, Hyper-V	Windows
Проверка резервных копий	+	+	+	+	+	+	+	+
Режим загрузки	+	-	-	-	-	-	+	-
Дата и время для файлов	-	-	-	+	+	+	-	-

© ООО Киберпротект, 2026

Обработка ошибок	+	+	+	+	+	+	+	+
Исключения файлов	-	-	-	+	+	+	-	-
Безопасность на уровне файлов	-	-	-	+	-	-	-	-
Flashback	+	+	+	-	-	-	+	-
Восстановление полного пути	-	-	-	+	+	+	-	-
Точки подключения	-	-	-	+	-	-	-	-
Производительность	+	+	-	+	+	-	+	+
Команды до и после процедуры	+	+	-	+	+	-	+	+
Изменение идентификатора безопасности	+	-	-	-	-	-	-	-
Управление питанием ВМ	-	-	-	-	-	-	+	-
"Управление лентами" (стр. 407)	-	-	-	+	+	-	-	-
Журнал событий Windows	+	-	-	+	-	-	Только Hyper-V	+
Включить после восстановления	-	-	-	-	-	+	-	-

© ООО Киберпротект, 2026

7.6.2 Проверка резервных копий

Этот параметр определяет, выполнять ли проверку резервной копии на повреждения перед восстановлением из нее данных. Эта операция выполняется агентом защиты.

Значение по умолчанию: **Отключено**.

При проверке резервной копии тома вычисляется контрольная сумма для каждого блока данных, сохраненного в резервной копии.

Проверка – это длительный процесс даже при инкрементном или дифференциальном резервном копировании небольших объемов данных. Причина заключается в том, что во время операции проверяются не только данные, физически присутствующие в резервной копии, но и все данные, которые восстанавливаются при выборе этой резервной копии. Это требует доступа к созданным ранее резервным копиям.

7.6.3 Режим загрузки

Этот параметр работает при восстановлении физической или виртуальной машины с резервной копии на уровне дисков, которая содержит операционную систему Windows.

Этот параметр позволяет выбрать режим загрузки (BIOS или UEFI), который Windows будет использовать после восстановления. Если режим загрузки исходной машины отличается от выбранного режима загрузки, программа:

- Инициализирует диск, на который восстанавливается системный том в соответствии с выбранным режимом загрузки (MBR для BIOS, GPT для UEFI).
- Адаптирует операционную систему Windows для запуска в выбранном режиме загрузки.

Значение по умолчанию: **Как и в целевой машине.**

Можно выбрать один из следующих вариантов:

- **Как и в целевой машине**

  Агент, запущенный на целевой машине, определяет режим загрузки, который в настоящее время используется Windows, и вносит изменения в соответствии с обнаруженным режимом загрузки.

  Это наиболее безопасное значение, которое автоматически приводит к созданию загрузочной системы, если только не применяются указанные ниже ограничения. Поскольку параметр **Режим загрузки** отсутствует на загрузочном носителе, агент на носителе всегда работает таким образом, словно это значение выбрано.
- **Как и в машине, для которой есть резервная копия**

  Агент, запущенный на целевой машине, считывает режим загрузки с резервной копии и вносит изменения в соответствии этим режимом загрузки. Это помогает восстановить систему на другой машине, даже если на этой машине используется другой режим загрузки, а затем заменить диск на машине, для которой создана резервная копия.
- **BIOS**

© ООО Киберпротект, 2026

Агент, запущенный на целевой машине, вносит изменения для использования BIOS.

- **UEFI**

  Агент, запущенный на целевой машине, вносит изменения для использования UEFI.

После изменения параметра будет повторно выполнена процедура сопоставления диска. Это займет некоторое время.

7.6.3.1 Рекомендации

Чтобы передать Windows между UEFI и BIOS, выполните указанные ниже действия:

- Восстановите весь диск, на котором расположен системный том. При восстановлении только системного тома поверх существующего тома агент не сможет правильно инициализировать целевой диск.
- Помните, что BIOS не позволяет использовать более 2 ТБ дискового пространства.

7.6.3.2 Ограничения

- Перенос между UEFI и BIOS поддерживается для 64-разрядных операционных систем Windows и Windows Server.
- Перенос между UEFI и BIOS не поддерживается, если резервная копи хранится на ленточном устройстве.

Если перенос системы между UEFI и BIOS не поддерживается, агент работает так, словно выбрана настройка **Как и в машине, для которой есть резервная копия**. Если целевая машина поддерживает как UEFI, так и BIOS, необходимо вручную включить режим загрузки, соответствующий исходной машине. Иначе система не загрузится.

7.6.4 Дата и время для файлов

Этот параметр применим только при восстановлении файлов.

Этот параметр определяет, получить ли дату и время восстановленных файлов из резервной копии или присвоить файлам текущую дату и время.

Если этот параметр включен, файлам будет назначена текущая дата и время.

Значение по умолчанию: **Отключено**.

7.6.5 Обработка ошибок

Они позволяют указать, как должны обрабатываться ошибки, возникшие при восстановлении.

7.6.5.1 В случае ошибки повторить операцию

Значение по умолчанию: **Включено. Количество попыток: 30. Интервал между попытками: 30 секунд.**

© ООО Киберпротект, 2026

Если возникла устранимая ошибка, программа будет продолжать попытки выполнить операцию. Задайте временной интервал и количество попыток. Попытки будут прекращены, как только операция будет успешно выполнена ИЛИ по достижении указанного максимального количества попыток (в зависимости от того, что наступит раньше).

7.6.5.2 Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений)

Значение по умолчанию: **Отключено**.

В режиме без вывода сообщений программа автоматически разрешает ситуации, требующие вмешательства пользователя. Если операция не может быть продолжена без вмешательства пользователя, она не будет выполнена. Дополнительные сведения об операции, включая информацию об ошибках (если они есть), см. в журнале операций.

7.6.5.3 Сохранить сведения о системе при сбое восстановления с перезагрузкой

Этот параметр применим для диска или тома восстановления на физическую машину с Windows или Linux.

Значение по умолчанию: **Отключено**.

Если этот параметр включен, можно указать папку на локальном диске (включая устройства флэш-памяти или жесткие диски (HDD), подсоединенные к целевой машине) или на сетевой папке, в которую будут сохраняться журналы, сведения о системе и файлы аварийных дампов. Этот файл поможет сотрудникам сопровождения ПО определить проблему.

7.6.6 Исключения файлов

Этот параметр применим только при восстановлении файлов.

Этот параметр определяет файлы и папки, которые будут пропущены в процессе восстановления и по причине этого исключены из списка восстановленных элементов.

Каждое условие об исключении файлов (имя файла, путь к файлу или маска) указывается в отдельном поле, при указывании можно использовать один или несколько подстановочных символов (* и ?). Подробную информацию об использовании подстановочных символов см. в разделе "Условия" (стр. 356).

Примечание
Исключения переопределяют выбор элементов данных для восстановления. Например, если выбрать восстановление файла MyFile.tmp, но при этом исключить все TMP-файлы, файл MyFile.tmp не будет восстановлен.

© ООО Киберпротект, 2026

7.6.7 Безопасность на уровне файлов

Этот параметр действует для файловых систем, поддерживающих атрибуты безопасности (например, NTFS), при восстановлении файлов с диска и резервных копий на уровне файлов.

Этот параметр определяет, должны ли восстанавливаться атрибуты безопасности вместе с файлами.

Значение по умолчанию: **Включено**.

Можно выбрать восстановление атрибутов безопасности или наследование файлами их атрибутов безопасности от папки, в которую они восстанавливаются.

7.6.8 Flashback

Этот параметр действует при восстановлении дисков и томов на физических и виртуальных машинах.

Если этот параметр включен, восстанавливаются только различия между данными в резервной копии и данными на целевом диске. Это ускоряет восстановление данных на диск, для которого создана резервная копия, особенно если структура тома данного диска не изменена. Данные сравниваются на уровне блоков.

Сравнение данных на уровне блоков – это длительная операция для физических машин. При наличии быстрого подключения к хранилищу резервных копий на восстановление всего диска потребуется меньше времени, чем на вычисления разницы в данных. Поэтому мы рекомендуем включать этот параметр только при медленном подключении к хранилищу резервных копий (например, если резервная копия расположена на удаленной сетевой папке).

При восстановлении физической машины предварительно задана настройка **Отключено**.

При восстановлении виртуальной машины предварительно задана настройка **Включено**.

7.6.9 Восстановление полного пути

Этот параметр действует только при восстановлении из резервной копии на уровне файлов.

Если этот параметр включен, в целевом хранилище воссоздается полный путь к файлу.

Значение по умолчанию: **Отключено**.

7.6.10 Точки подключения

Этот параметр действует только в Windows для восстановления данных с резервной копии на уровне файлов.

Включите этот параметр для восстановления файлов и папок, которые хранятся на подключенных томах и резервные копии которых создавались с включенным параметром Точки подключения.

Значение по умолчанию: **Отключено**.

© ООО Киберпротект, 2026

Этот параметр работает только в том случае, если для восстановления выбрана папка, которая в иерархии папок находится выше точки подключения. Если для восстановления выбраны папки в точке подключения или сама точка подключения, выбранные элементы будут восстановлены независимо от значения параметра **Точки подключения**.

Примечание
Помните, что, если том не подключен в момент восстановления, данные будут восстановлены напрямую в папку, которая была точкой подключения во время резервного копирования.

7.6.11 Производительность

Этот параметр определяет приоритет процесса восстановления в операционной системе.

Доступные значения:

- **Низкий**: соответствует значению **Ниже среднего**.
- **Обычный**: соответствует значению **Обычный**.
- **Высокий**: соответствует значению **Высокий**.

Значение по умолчанию: **Обычный**.

Приоритет процесса, выполняющегося в системе, определяет количество выделенных ему ресурсов ЦП и системы. Понизив приоритет восстановления, можно освободить часть ресурсов для других приложений. Повышение приоритета восстановления может ускорить процесс восстановления за счет выделения операционной системой большего объема ресурсов приложению, выполняющему восстановление. Однако результат будет зависеть от общей загрузки процессора и других факторов, например скорости ввода-вывода диска и сетевого трафика.

7.6.12 Команды до и после процедуры

Этот параметр позволяет определить команды, которые должны выполняться автоматически перед выполнением процедуры восстановления данных и после нее.

Пример использования команд до и после процедуры:

- Запустите команду **Checkdisk**, чтобы найти и исправить логические ошибки файловой системы, физические ошибки или поврежденные сектора до запуска восстановления или после его окончания.

Программа не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).

Команда после восстановления не будет выполнена, если восстановление заканчивается перезагрузкой.

7.6.12.1 Команда, выполняемая перед восстановлением

Как указать команду или пакетный файл, выполняемый перед началом восстановления

© ООО Киберпротект, 2026

1. Включите переключатель **Выполнение команды до восстановления**.
2. В поле **Команда...** введите команду или найдите пакетный файл. Программа не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).
3. В поле **Рабочая папка** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите аргументы выполнения команды (если необходимо).
5. В зависимости от желаемого результата выберите соответствующие параметры из описанных в таблице ниже.
6. Нажмите кнопку **Готово**.

Флажок	**Выбор**			
Прервать восстановление при сбое команды*	Установить	Снять	Установить	Снять
Не начинать восстановление до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				
	Предустановка Выполнить восстановление только после успешного выполнения команды. Прервать восстановление при сбое команды.	Выполнить восстановление после выполнения команды независимо от результатов ее выполнения (успешно или ошибка).	Н/Д	Выполнить восстановление параллельно с выполнением команды независимо от результата ее выполнения.

* Команда считается сбойной, если код завершения не равен нулю.

7.6.12.2 Команда после восстановления

Как указать команду или исполняемый файл, которые будут выполнены после завершения восстановления

1. Включите переключатель **Выполнение команды после восстановления**.
2. В поле **Команда...** введите команду или найдите пакетный файл.

© ООО Киберпротект, 2026

3. В поле **Рабочая папка** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости аргументы выполняемой команды.
5. Установите флажок **Прерывать восстановление при сбое команды**, если для вас важно успешное выполнение программы. Считается, что команда не выполнена, если код выхода не равен нулю. При сбое выполнения команды статусу восстановления будет задано значение **Ошибка**.

   Если флажок не установлен, результат выполнения команды не влияет на успешность выполнения восстановления. Можно отследить результат выполнения команды, изучив информацию на вкладке **Действия**.
6. Нажмите кнопку **Готово**.

Примечание
Команда после восстановления не будет выполнена, если восстановление заканчивается перезагрузкой.

7.6.13 Управление лентами

Можно использовать указанные ниже параметры восстановления управления лентами.

7.6.13.1 Использование кэша диска для ускорения восстановления

Значение по умолчанию: **Отключено**.

Настоятельно рекомендуем использовать параметр **Используйте кэш диска, чтобы ускорить восстановление** при восстановлении файлов из архива изображения. В противном случае операция восстановления может занять много времени. При использовании этого параметра лента читается последовательно без прерываний и перемоток.

7.6.14 Изменение идентификатора безопасности

Этот параметр действует при восстановлении ОС Windows Server 2012 R2 или более ранних версий.

Этот параметр не работает, если восстановление в виртуальную машину выполняется агентом для VMware или агентом для Hyper-V.

Значение по умолчанию: **Отключено**.

Это программное обеспечение может генерировать уникальный идентификатор безопасности (SID компьютера) для восстановленной операционной системы. Этот параметр требуется только для обеспечения работоспособности программного обеспечения сторонних производителей, в котором используется SID компьютера.

© ООО Киберпротект, 2026

Корпорация Майкрософт не поддерживает официально изменение SID в развернутых или восстановленных системах. Это означает, что, используя этот параметр, вы принимаете на себя весь риск.

7.6.15 Управление питанием ВМ

Эти параметры применяются, если восстановление на виртуальную машину выполняется агентом для VMware или агентом для Hyper-V.

7.6.15.1 Выключать целевые виртуальные машины при запуске восстановления

Значение по умолчанию: **Включено**.

Невозможно выполнить восстановление в существующую виртуальную машину, если она включена, поэтому машина выключается автоматически при запуске восстановления. Пользователи будут отключены от этой машины, а любые несохраненные данные потеряны.

Снимите флажок, соответствующий этому параметру, если предпочитаете вручную выключать виртуальные машины перед восстановлением.

7.6.15.2 Включите целевую виртуальную машину по окончании восстановления.

Значение по умолчанию: **Отключено**.

После восстановления машины из резервной копии на другой машине существует вероятность появления копии существующей машины в сети. На всякий случай включите восстановленную виртуальную машину вручную после принятия всех необходимых мер предосторожности.

7.6.16 Журнал событий Windows

Этот параметр работает только в ОС Windows.

Этот параметр указывает, должны ли агенты записывать события операций восстановления в журнал событий приложений Windows (чтобы просмотреть этот журнал, запустите файл eventvwr.exe или выберите **Панель управления** > **Администрирование** > **Просмотр событий**). События содержат статус и время завершения операции; события можно фильтровать.

Значение по умолчанию: **Отключено**.

Примечание
Параметр работает только для операций восстановления файлов (см. раздел "Восстановление файлов" (стр. 394)).

7.6.17 Включить после восстановления

Этот параметр применим при работе с загрузочного носителя.

© ООО Киберпротект, 2026

Значение по умолчанию: **Отключено**.

Этот параметр позволяет загрузить машину с восстановленной операционной системой без вмешательства пользователя.

© ООО Киберпротект, 2026

8 Операции с резервными копиями

8.1 Подключение томов из резервной копии

Подключение томов из резервной копии на уровне дисков позволяет получить доступ к томам так же, как и к физическим дискам.

Подключение томов в режиме чтения/записи позволяет менять содержимое резервной копии, то есть сохранять, перемещать, создавать и удалять файлы или папки и запускать исполняемые сценарии, состоящие из одного файла. В этом режиме программное обеспечение создает инкрементную резервную копию, которая содержит изменения, внесенные в содержимое резервной копии. Помните, что ни одного из этих изменений не будет в последующих резервных копиях.

8.1.1 Требования

- Эта функциональность доступна только в Windows при использовании проводника.
- На машине, которая выполняет операцию подключения, должен быть установлен агент для Windows.
- Файловая система, для которой создана резервная копия, должна поддерживаться в той версии Windows, которая выполняется на данной машине.
- Резервная копия должна хранится в локальной папке, сетевой папке (SMB/CIFS) или в Зоне безопасности.

8.1.2 Сценарии использования

- **Предоставление общего доступа к данным**

  Можно легко предоставить общий доступ к подключенным томам по сети.
- **Временное решение по восстановлению базы данных**

  Подключите том, который содержит базу данных SQL, из вышедшей недавно из строя машины. Это предоставит доступ к базе данных до восстановления этой машины. Этот подход можно использовать для фрагментарного восстановления данных Microsoft SharePoint, используя SharePoint Explorer.
- **Обработка ошибок**

  Сбой восстановления с возможностью восстановления размера тома может происходить по причине ошибки в файловой системе, для которой создана резервная копия. Подключите резервную копию в режиме чтения/записи. После этого проверьте подключенный том на наличие ошибок, используя команду **chkdsk /r**. После исправления ошибок и создания новой инкрементной резервной копии восстановите систему из этой резервной копии.

Порядок подключения тома из резервной копии

© ООО Киберпротект, 2026

1. Перейдите в хранилище резервных копий, используя проводник.
2. Дважды щелкните файл резервной копии. По умолчанию файлы имеют имена на основе следующего шаблона:

   <имя машины> - <GUID плана защиты>
3. Если резервная копия защищена паролем, укажите его. В противном случае пропустите этот шаг.

   В проводнике отображаются точки восстановления.
4. Дважды щелкните точку восстановления.

   В проводнике отображаются тома, для которых созданы резервные копии.

   Примечание

   Дважды щелкните том для обзора его содержимого. Можно скопировать файлы и папки из резервной копии в любую папку в файловой системе.
5. Правой кнопкой мыши щелкните том для подключения, затем выберите один из следующих пунктов меню:
   - **Подключить**
   - **Подключить в режиме «только чтение»**
6. Если резервная копия хранится в сетевой папке, укажите учетные данные для доступа. В противном случае пропустите этот шаг.

   Программа подключит выбранный том. Данному тому назначается первая неиспользованная буква.

Порядок отключения тома

1. В проводнике откройте **Этот компьютер**.
2. Правой кнопкой мыши щелкните подключенный том.
3. Нажмите **Отключить**.
4. Если том подключен в режиме чтения/записи и его содержимое было изменено, выберите, создавать ли инкрементную резервную копию с этими изменениями. В противном случае пропустите этот шаг.

   Программа отключит выбранный том.

8.2 Экспорт резервных копий

При экспорте в указанном хранилище создается самодостаточная копия резервной копии. Исходная резервная копия остается без изменений. Экспорт позволяет выделить определенную резервную копию из цепочки инкрементных и дифференциальных резервных копий для быстрого восстановления и записать ее на съемный носитель для использования в других целях.

Результатом операции экспорта всегда является полная резервная копия. Чтобы выполнить репликацию всей цепочки резервных копий в другое хранилище и сохранить несколько точек восстановления, используйте план репликации резервных копий.

© ООО Киберпротект, 2026

Имя файла экспортированной резервной копии зависит от значения параметра формат резервной копии:

- Для формата **Версия 12** с любой схемой резервного копирования имя файла резервной копии будет таким же, как и имя файла оригинальной резервной копии, плюс порядковый номер. Если несколько резервных копий одной цепочки экспортируются в одно хранилище, имена файлов (за исключением первого) в конце дополняются порядковым номером из четырех цифр.
- Для формата **Версии 11** со схемой резервного копирования **Всегда инкрементное** имя файла резервной копии в точности соответствует имени файла исходной резервной копии. Если несколько резервных копий одной цепочки экспортируются в одно хранилище, то каждая операция экспорта перезаписывает ранее экспортированную резервную копию.
- Для формата **Версия 11** с другими схемами резервного копирования имя файла резервной копии будет таким же, как и имя файла оригинальной резервной копии, плюс метка времени. Метки времени экспортированных резервных копий соответствуют времени выполнения экспорта.

Экспортированная резервная копия наследует настройки защиты паролем и сам пароль от исходной резервной копии. При экспорте защищенной резервной копии необходимо указать пароль.

Порядок экспорта резервной копии

1. Выберите машину, для которой есть резервная копия.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните любое из следующих действий:
   - Если резервная копия расположена в общем хранилище данных (т .е. другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилища резервных копий.
4. Щелкните значок шестерни, затем щелкните **Экспорт**.
5. Выберите агент, который будет выполнять экспорт.
6. Если резервная копия защищена паролем, укажите его. В противном случае пропустите этот шаг.
7. Укажите место сохранения экспорта.
8. Нажмите кнопку **Запустить**.

© ООО Киберпротект, 2026

8.3 Удаление резервных копий

Предупреждение
При удалении резервной копии все ее данные удаляются окончательно. Удаленные данные невозможно восстановить.

Порядок удаления резервных копий машины, которая включена и присутствует на веб-консоли Кибер Бэкап

1. На вкладке **Физические и виртуальные машины** выберите машину, резервные копии которой необходимо удалить.
2. Щелкните **Восстановление**.
3. Выберите хранилище, в котором расположены резервные копии для удаления.
4. Выполните одно из следующих действий:
   - Чтобы удалить одну резервную копию, выберите резервную копию для удаления, щелкните значок шестерни и выберите пункт **Удалить**.
   - Чтобы удалить все резервные копии в выбранном хранилище, щелкните **Удалить все**.
5. Подтвердите операцию.

Порядок удаления резервных копий любой машины

1. На вкладке **Хранилища резервных копий** выберите хранилище, из которого необходимо удалить резервные копии.
   В программном обеспечении отображаются все резервные копии, которые разрешено просматривать в выбранном хранилище для вашей учетной записи. Резервные копии объединены по группам. Группы имеют имена на основе следующего шаблона:
   <имя машины> - <имя плана защиты>
2. Выберите группу.
3. Выполните одно из следующих действий:
   - Чтобы удалить одну резервную копию, щелкните **Показать резервные копии**, выберите резервную копию для удаления, щелкните значок шестерни и выберите пункт **Удалить**.
   - Чтобы удалить выбранную группу, щелкните **Удалить**.
4. Подтвердите операцию.

8.4 Обработка данных вне хоста (off-host)

Большинство действий, предусмотренных в плане резервного копирования, например, репликация, проверка и применение правил хранения, выполняются агентом резервного копирования. Это увеличивает рабочую нагрузку на машину, на которой запущен агент, даже после завершения процесса резервного копирования.

© ООО Киберпротект, 2026

Разграничение планов репликации, проверки, очистки и преобразования резервных копий в виртуальные машины повышает гибкость и предоставляет следующие возможности:

- выбор другого агента/агентов для выполнения таких операций;
- планирование выполнения таких операций на часы наименьшей загрузки для снижения использования полосы пропускания;
- перенесение выполнения таких операций на нерабочие часы, если в ваши планы не входит установка выделенного агента для обработки данных.

Если вы используете узел хранения, то для обработки данных вне хоста можно использовать выделенный агент, поставляемый в комплекте с узлом хранения.

В отличие от планов резервного копирования и репликации ВМ, которые используют настройки времени, заданные на машинах с агентами, планы обработки данных вне хоста запускаются в соответствии с настройками времени на машине сервера управления.

8.4.1 Репликация резервных копий

При применении плана репликации к резервной копии, разделённой на фиксированные фрагменты (см. раздел "Деление" (стр. 371)), реплицированная копия объединяется в общий архив.

8.4.1.1 Поддерживаемые расположения

В таблицах ниже представлены хранилища резервных копий, поддерживаемые планами репликации резервных копий.

Источник репликации	**Целевое хранилище репликации**			
	Локальная папка	**Хранилище под управлением узла хранения**		
		с дедупликацией	**без дедупликации**	**с лентами**
Локальная папка	+	+*	+	+
Сетевая папка	+	+*	+	+
Хранилище под управлением узла хранения с дедупликацией	+	+*	+	+
Хранилище под управлением узла хранения без дедупликации	+	+*	+	+
Хранилище под управлением узла хранения с лентами	+	+*	+	+
Зона безопасности	+	+*	+	+
Папка NFS	-	-	-	-

© ООО Киберпротект, 2026

SFTP-сервер	-	-	-	-
Кибер Инфраструктура или Кибер Хранилище	+	+*	+	+

* Только для резервных копий формата "Версия 11". Подробнее о форматах резервных копий см. раздел "Формат резервной копии" (стр. 347).

Источник репликации	Целевое хранилище репликации			
	Сетевая папка	Папка NFS	SFTP-сервер	Кибер Инфраструктура или Кибер Хранилище
Локальная папка	+	-	-	+
Сетевая папка	+	-	-	+
Хранилище под управлением узла хранения с дедупликацией	+	-	-	+
Хранилище под управлением узла хранения без дедупликации	+	-	-	+
Хранилище под управлением узла хранения с лентами	+	-	-	+
Зона безопасности	+	-	-	+
Папка NFS	-	-	-	-
SFTP-сервер	-	-	-	-
Кибер Инфраструктура или Кибер Хранилище	+	-	-	+

Примечание
Хранилище под управлением узла хранения с включённой дедупликацией не рекомендуется использовать для постоянной репликации. Дедупликация является длительным и ресурсоёмким процессом, который может привести к снижению скорости репликации, если в качестве источника реплицируемых данных используется хранилище под управлением узла хранения с дедупликацией.

Дополнительные условия использования хранилища под управлением узла хранения см. в разделе "Замечания по использованию узла хранения" (стр. 309).

8.4.1.2 Порядок создания плана репликации резервных копий

Для создания плана репликации резервных копий выполните следующие действия:

© ООО Киберпротект, 2026

1. Щёлкните **Планы** > **Репликация резервной копии**.
2. Нажмите **Создать план**.

   В программе отобразится новый шаблон плана.
3. [Необязательно] Для изменения имени плана нажмите на имя по умолчанию.
4. Щёлкните **Агент**, а затем выберите агента, который выполнит репликацию.

   Можно выбрать любого агента, который имеет доступ к источнику и месту сохранения хранилища резервной копии.
5. Щёлкните **Элементы для репликации** и выберите резервные копии для репликации этим планом.

   Используя переключатель **Расположения** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии защищены паролем, пароль для всех должен быть одинаков. Для резервных копий, для которых используются разные пароли, создайте отдельные планы.
6. Щёлкните **Место сохранения** и укажите место сохранения.
7. [Дополнительно] В разделе **Порядок преобразования** выберите резервные копии для репликации. Можно выбрать один из следующих вариантов:
   - **все резервные копии** (по умолчанию),
   - **только полные резервные копии**,
   - **только последняя резервная копия**.
8. [Дополнительно] Щёлкните **Расписание**, а затем измените расписание.
9. [Необязательно] Щёлкните **Правила хранения**, а затем укажите правила хранения для целевого расположения, как описано в разделе "Правила хранения" (стр. 299).
10. Если резервные копии, выбранные в **Элементы для репликации**, защищены паролем, включите переключатель **Пароль резервной копии** и укажите пароль. В противном случае пропустите этот шаг.
11. [Дополнительно] Для изменения параметров плана щёлкните значок шестеренки.
12. Нажмите кнопку **Создать**.

8.4.2 Проверка резервных копий

Проверка – это операция по определению возможности восстановления данных из резервной копии.

Проверка хранилища резервных копий проверяет все резервные копии, расположенные в хранилище.

8.4.2.1 Методы проверки резервных копий

В планах проверки предусмотрено два метода проверки резервных копий. Если выбрать оба метода, операции будут выполняться последовательно.

© ООО Киберпротект, 2026

- **Вычисление контрольной суммы для каждого блока данных, сохранённого в резервной копии**

  Дополнительную информацию о проверке путём определения контрольной суммы см. в разделе Проверка резервных копий.
- **Запуск виртуальной машины из резервной копии**

  Этот метод работает только для резервных копий дисков, содержащих операционную систему (Windows или Linux). Резервная копия может быть создана на физическом сервере или на виртуальном сервере поддерживаемой среды виртуализации. Чтобы использовать этот метод, необходимо иметь хост ESXi или Hyper-V и агент защиты (агент для VMware или агент для Hyper-V соответственно), который управляет этим хостом. В этой среде будет запущена виртуальная машина из проверяемой резервной копии.

  Агент запускает виртуальную машину из резервной копии и подключается к VMware Tools или службе Hyper-V Heartbeat для проверки успешности запуска операционной системы. При сбое подключения агент пытается подключиться каждые две минуты. Всего предпринимается пять попыток подключения. Если ни одна из попыток не будет успешной, проверка завершится сбоем, подробные сведения будут доступны во вкладке **Панель мониторинга** > **Действия**.

  Независимо от количества планов проверки и проверенных резервных копий агент, который выполняет планы проверки, одновременно запускает одну виртуальную машину. При этом добавляемые к запускаемой машине диски подключаются напрямую из хранилища резервных копий без переноса в среду виртуализации. Как только результат проверки становится известным, агент удаляет виртуальную машину и запускает следующую.

8.4.2.2 Поддерживаемые расположения

В следующей таблице представлены хранилища резервных копий, поддерживаемые планами проверки.

Хранилище резервных копий	Вычисление контрольной суммы	Запуск виртуальной машины
Локальная папка	+	+
Сетевая папка	+	+
Папка NFS	-	-
Зона безопасности	-	-
Сервер SFTP	-	-
Управляемое хранилище	+	+
Ленточное устройство	+	-
Кибер Инфраструктура или Кибер Хранилище	+	+

© ООО Киберпротект, 2026

8.4.2.3 Порядок создания нового плана проверки

1. Нажмите **Планы** > **Проверка**.
2. Нажмите **Создать план**.

   В программе отобразится новый шаблон плана.
3. [Необязательно] Для изменения имени плана проверки нажмите на имя по умолчанию, далее в открывшемся окне введите новое имя и нажмите **OK**.
4. Щёлкните **Агент**, а затем выберите агент, который выполнит проверку, и нажмите **OK**.

   Для удобства воспользуйтесь поиском по имени агента, введя его имя в соответствующее поле.

   Для настройки отображаемых столбцов с информацией об агентах нажмите на значок шестерёнки и установите флажки для отображаемых столбцов.

   Для выполнения проверки посредством запуска виртуальной машины из резервной копии выберите агент для VMware или агент для Hyper-V. В противном случае выберите любой агент, который зарегистрирован на сервере управления и имеет доступ к хранилищу резервной копии.
5. Щёлкните **Элементы для проверки** и выберите резервные копии для проверки этим планом.

   Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии защищены паролем, пароль для всех должен быть одинаков. Для резервных копий, для которых используются разные пароли, создайте отдельные планы.
6. [Необязательно] В **Объект проверки**, выберите резервные копии для проверки. Можно выбрать один из следующих вариантов:
   - **Все резервные копии**;
   - **Только последняя резервная копия**.
7. [Необязательно] Нажмите **Порядок проверки** и затем выберите метод, переведя соответствующий переключатель в положение **Вкл.** (можно выбрать оба метода):
   - **Проверка контрольной суммы**

     Программное обеспечение вычислит контрольную сумму для каждого блока данных резервной копии.
   - **Запустить как виртуальную машину**

     Программное обеспечение запустит виртуальную машину из каждой резервной копии.
8. Если выбран вариант **Запустить как виртуальную машину**, дополнительно выполните следующие шаги:
   a. Щёлкните **Целевая машина** и выберите тип виртуальной машины (ESXi или Hyper-V), хост и шаблон имени машины.

      По умолчанию установлено имя **[Machine Name]_validate**.
   b. Нажмите **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для виртуальной машины.
   c. Для получения результата проверки используется опция **Сигнал пульса ВМ**, которая получает статус пульса виртуальный машины от гостевой операционной системы через

© ООО Киберпротект, 2026

инструментарий гипервизора (VMware Tools или Hyper-V Integration Services). Опция включена по умолчанию и не может быть выключена.

d. [Необязательно] Щёлкните **Настройки ВМ**, чтобы изменить размер памяти и сетевые подключения виртуальной машины.

Примечание
По умолчанию виртуальная машина *не* подключена к сети, а размер памяти виртуальной машины соответствует размеру памяти оригинальной машины. При необходимости подключения виртуальной машины к сети будьте осторожны во избежание создания помех другим машинам.

9. [Необязательно] Щёлкните **Расписание**, а затем укажите требуемые параметры расписания и нажмите **Готово**.
10. Если резервные копии, выбранные в разделе **Элементы для проверки**, защищены паролем, установите пароль, щёлкнув по переключателю **Пароль резервной копии**. В противном случае пропустите этот шаг.
11. [Необязательно] Для настройки действий при сбое плана щёлкните значок шестерёнки, выберите **Действие при сбое плана** и установите требуемые параметры, после чего нажмите **Готово**.
12. [Необязательно] Для настройки команд, которые должны выполняться до или после плана проверки, щёлкните значок шестерёнки, выберите **Команды до и после** и установите требуемые параметры, после чего нажмите **Готово**.
13. [Необязательно] Для настройки повторного выполнения плана проверки в случае сбоев щёлкните значок шестерёнки, выберите **Обработка ошибок** и установите требуемые параметры, после чего нажмите **Готово**.
14. [Необязательно] Для настройки приоритета резервного копирования щёлкните значок шестерёнки, выберите **Производительность** и установите требуемые параметры, после чего нажмите **Готово**.
15. Нажмите кнопку **Создать**.

В результате выполненных действий план проверки будет создан, а его имя будет отображено в списке **Планы проверки**.

8.4.2.4 Порядок проверки резервных копий

Проверка резервных копий с использованием созданного плана проверки может быть выполнена:

- по расписанию;
- по требованию (доступно как для планов с настроенным расписанием, так и без него).

Проверка резервных копий по расписанию

При выполнении проверки по расписанию процесс будет выполняться автоматически в заданнное время.

© ООО Киберпротект, 2026

Для просмотра результатов проверки перейдите в **Планы** > **Проверка**, выберите план проверки и щёлкните **Действия**.

Проверка резервных копий по требованию

Чтобы выполнить проверку резервной копии по требованию, выполните следующие действия:

1. Щёлкните **Планы** > **Проверка**.
2. Выберите в списке план проверки.
3. На панели **Действия** нажмите **Запустить сейчас**.

В результате выполненных действий будет начат процесс проверки резервных копий в соответствии с используемым планом.

Для просмотра статуса выполнения проверки щёлкните **Действия**. В случае возникновения ошибок соответствующие сообщения будут отображены в этом разделе.

8.4.3 Очистка от устаревших резервных копий

Очистка – это операция, которая удаляет устаревшие резервные копии в соответствии с правилами хранения.

8.4.3.1 Поддерживаемые расположения

Планы очистки поддерживаются всеми хранилищами резервных копий, за исключением папок NFS, SFTP-серверов и Зона безопасности.

Порядок создания нового плана очистки

1. Щелкните **Планы** > **Очистка**.
2. Нажмите **Создать план**.
   В программе отобразится новый шаблон плана.
3. [Необязательно] Для изменения имени плана нажмите на имя по умолчанию.
4. Щелкните **Агент**, а затем выберите агента, который будет выполнять очистку.
   Можно выбрать любой агент, который имеет доступ к расположению резервного копирования.
5. Щелкните **Элементы для очистки**, затем выберите резервные копии, которые будут очищены этим планом.
   Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.
   Если выбранные резервные копии защищены паролем, пароль для всех должен быть одинаков. Для резервных копий, для которых используются разные пароли, создайте отдельные планы.
6. [Дополнительно] Щелкните **Расписание**, а затем измените расписание.
7. [Дополнительно] Щелкните **Правило хранения**, а затем укажите правила хранения, как описано в разделе «Правила хранения».

© ООО Киберпротект, 2026

8. Если резервные копии, выбранные в **Элементы для очистки** защищены паролем, включите переключатель **Пароль резервной копии** и укажите пароль. В противном случае пропустите этот шаг.
9. [Дополнительно] Для изменения параметров плана щелкните значок шестеренки.
10. Нажмите кнопку **Создать**.

8.4.4 Преобразование резервных копий в виртуальные машины

Можно создать отдельный план для преобразования резервной копии в виртуальную машину и запустить его вручную или по расписанию.

Информацию о предварительных требованиях и ограничениях см. в разделе «Важная информация о преобразовании».

Порядок создания плана для преобразования в виртуальную машину

1. Щелкните **Планы** > **Преобразование в ВМ**.
2. Нажмите **Создать план**.
   В программе отобразится новый шаблон плана.
3. [Необязательно] Для изменения имени плана нажмите на имя по умолчанию.
4. В поле **Преобразовать в** выберите тип целевой виртуальной машины. Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **Файлы VHDX**

   Примечание
   Для экономии дискового пространства при каждом преобразовании в файлы VHDX выполняется перезапись файлов VHDX в целевом расположении, созданном при предыдущем преобразовании.
5. Выполните одно из следующих действий:
   - Для VMware ESXi и Hyper-V: щелкните **Хост**, выберите целевой хост, а затем укажите новый шаблон имени машины.
   - Для виртуальных машин других типов: в поле **Путь** укажите расположение для сохранения файлов виртуальной машины и шаблон имени файла.

   Имя по умолчанию – **[Имя машины]_converted**.
6. Щелкните **Агент**, а затем выберите агент, который выполнит преобразование.
7. Щелкните **Элементы для преобразования**, выберите резервные копии, которые данный план преобразует в виртуальные машины.

© ООО Киберпротект, 2026

Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

Если выбранные резервные копии защищены паролем, пароль для всех должен быть одинаков. Для резервных копий, для которых используются разные пароли, создайте отдельные планы.

8. [Только для VMware ESXi и Hyper-V] Щелкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для данной виртуальной машины.
9. [Необязательно] Для VMware ESXi и Hyper-V можно также выполнить следующие действия:
   - Измените режим распределения ресурса дисков. По умолчанию задана настройка **Экономное** для VMware ESXi и **Динамически расширяемое** для Hyper-V.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.
10. [Дополнительно] Щелкните **Расписание**, а затем измените расписание.
11. Если резервные копии, выбранные в **Элементы для преобразования** защищены паролем, включите переключатель **Пароль резервной копии** и укажите пароль. В противном случае пропустите этот шаг.
12. [Дополнительно] Для изменения параметров плана щелкните значок шестеренки.
13. Нажмите кнопку **Создать**.

© ООО Киберпротект, 2026

9 Вкладка «Планы»

При наличии лицензии Кибер Бэкап расширенная редакция планами защиты и прочими планами можно управлять на вкладке **Планы**.

Каждый раздел вкладки **Планы** содержит все планы конкретного типа. Доступны следующие разделы

- Защита
- Репликация резервной копии
- Проверка
- Очистка
- Преобразование в ВМ
- Репликация ВМ
- Загрузочный носитель. В этом разделе показаны планы защиты, которые созданы для машин, загружаемых с загрузочных носителей, и применяются только к этим машинам.

На вкладке **Планы** также можно выполнять операции с планами. В каждом разделе вкладки можно создавать, редактировать, отключать, включать, удалять, запускать и отслеживать выполнение плана.

Список действий с планами находится в меню справа. По умолчанию из этого меню вы можете:

Создать план - создает план защиты с выбранными параметрами;

Импорт - позволяет импортировать план из файла;

Для просмотра свойств и настройки уже существующего плана отметьте нужный план в списке планов. Справа появится дополнительное меню действий с планами. В меню содержатся следующие пункты:

- **Сведения** - показывает сведения о выбранном плане;
- **Остановить** - позволяет остановить выполнение выбранного плана;
- **Изменить** - позволяет изменить параметры выбранного плана;
- **Действия** - предоставляет сведения о действиях с выбранным планом;
- **Оповещения** - предоставляет список оповещений относительно выбранного плана;
- **Клонировать** - позволяет применить выбранный план вместе с параметрами к другому устройству;
- **Экспорт** - позволяет сохранить план в файл;
- **Отключить** (**Включить**) - отключает (включает) план;
- **Удалить** - удаляет план.

Подробнее об этом см. в разделе "Операции с планами защиты" (стр. 227).

© ООО Киберпротект, 2026

Клонирование и остановка доступны только для планов защиты. В отличие от остановки резервного копирования на вкладке **Устройства**, при остановке плана защиты будут остановлены процессы создания резервных копий на всех устройствах, к которым он применен.

Также возможно экспортировать план в файл и импортировать предварительно экспортированный план.

© ООО Киберпротект, 2026

10 Вкладка «Хранилища резервных копий»

На вкладке **Хранилища резервных копий** показаны резервные копии всех машин, которые когда-либо были зарегистрированы на сервере управления. Сюда входят отключенные машины и машины, которые больше не зарегистрированы.

Резервные копии, которые хранятся в общем расположении (например на общем ресурсе SMB или NFS) видимы всем пользователям, которые имеют разрешение на чтение в данном расположении.

В ОС Windows файлы резервных копий наследуют разрешения на доступ от родительской папки. Поэтому мы рекомендуем ограничить разрешения на чтение для этой папки.

Хранилища резервных копий, которые используются в планах защиты, автоматически добавляются на вкладку **Хранилища резервных копий**. Чтобы добавить хранилище, а также локальную или сетевую папку, узел хранения, Кибер Инфраструктуру и прочее, щёлкните **Добавить хранилище** и следуйте инструкции.

Предупреждение
Не пытайтесь редактировать файлы резервной копии вручную, поскольку это может привести к повреждению файла и сделать резервные копии нестабильными. Кроме того, мы рекомендуем экспортировать резервные копии или реплицировать их, а не перемещать их файлы вручную.

Порядок выбора точки восстановления на вкладке «Хранилища резервных копий»

1. На вкладке **Хранилища резервных копий** выберите хранилище резервных копий.
   В программном обеспечении отображаются все резервные копии, которые разрешено просматривать в выбранном хранилище для вашей учетной записи. Резервные копии объединены по группам. Группы имеют имена на основе следующего шаблона:
   <имя машины> - <имя плана защиты>
2. Выберите группу, с которой необходимо восстановить данные.
3. [Необязательно] Щелкните **Изменить** рядом с полем **Машина для обзора** и выберите другую машину. Обзор некоторых резервных копий могут выполнить только определенные агенты. Например, чтобы просмотреть резервные копии баз данных Microsoft SQL Server, необходимо выбрать машину с запущенным агентом для SQL.

   Внимание
   Имейте в виду, что расположение, указанное в поле **Машина для обзора**, является расположением по умолчанию для восстановления с резервной копии физической машины. После того как вы выберете точку восстановления и щелкните **Восстановление**, дважды проверьте настройку **Целевая машина**, чтобы убедиться в правильности указанной машины, в которую будут выполнено восстановление. Чтобы изменить целевое место восстановления, укажите другую машину в поле **Машина для обзора**.
4. Щелкните **Показать резервные копии**.
5. Выберите точку восстановления.

© ООО Киберпротект, 2026

Примечание

Точку восстановления можно также выбрать, нажав **Устройства** > <устройство> > **Восстановление** (см. "Восстановление" (стр. 382)).

© ООО Киберпротект, 2026

11 Загрузочный носитель

11.1 Загрузочный носитель

Загрузочный носитель представляет собой физический носитель (компакт-диск, DVD-диск, флеш-накопитель USB или другой съемный носитель, распознаваемый BIOS машины в качестве загрузочного устройства), который позволяет запускать агент Кибер Бэкап в среде Linux или среде предустановки Windows (WinPE) без помощи операционной системы.

Загрузочный носитель чаще всего используется в следующих случаях:

- Восстановление операционной системы, которая не может запуститься.
- Доступ к данным, сохранившимся после повреждения системы и их резервного копирования.
- Развертывание операционной системы на "голое железо".
- Создание базовых или динамических томов на "голом железе".
- Посекторное резервное копирование диска с неподдерживаемой файловой системой.
- Резервное копирование в автономном режиме любых данных, которые не удалось скопировать в онлайн-режиме, например, из-за блокировки запущенным приложением или ограничения доступа.

Кроме того, машину можно загрузить с использованием сетевой загрузки с помощью PXE-сервера Киберпротект, службы развертывания Windows (WDS) или службы удаленной установки (RIS). Эти серверы с загружаемыми загрузочными компонентами также могут рассматриваться как один из видов загрузочных носителей. С помощью одного мастера можно создать загрузочный носитель, настроить PXE-сервер или службы WDS/RIS.

11.2 Создавать ли загрузочный носитель или скачать готовый?

Используя мастер создания загрузочных носителей, можно создать собственный загрузочный носитель (на основе Linux или на основе WinPE) для компьютеров Windows или Linux. Чтобы создать полнофункциональный загрузочный носитель, необходимо указать лицензионный ключ Кибер Бэкап. Если не указать этот ключ, с загрузочного носителя можно будет выполнить только операции восстановления.

Примечание
Загрузочный носитель не поддерживает гибридные диски.

Кроме того, можно скачать готовый загрузочный носитель (только на основе Linux) с веб-сайта Киберпротект. Скачанный загрузочный носитель можно использовать только для операций восстановления и доступа к инструменту Универсальное восстановление (Universal Restore). Вы не

© ООО Киберпротект, 2026

сможете создавать резервные копии данных, проверять или экспортировать резервные копии, выполнять операции управления дисками или использовать сценарии с ними.

Примечание
Готовый загрузочный носитель не поддерживает узел хранения, хранилища на ленте и хранилища SFTP. Если вы намерены использовать эти хранилища, необходимо будет создать собственный загрузочный носитель, используя для этого мастер создания загрузочных носителей.

Можно записать скачанный ISO-файл на CD/DVD-диск или создать загрузочный флэш-накопитель USB, используя один из бесплатных инструментов, доступных в Интернете. Для машин с UEFI используйте ISO to USB или RUFUS, для машин с BIOS –Win32DiskImager. В Linux можно воспользоваться утилитой dd.

11.3 Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE?

11.3.1 На основе Linux

Загрузочный носитель на основе Linux содержит загружаемый агент Кибер Бэкап на основе ядра Linux. Этот агент может выполнять загрузку и операции на любом PC-совместимом оборудовании, включая «голое железо» и машины с поврежденными или неподдерживаемыми файловыми системами. Операции можно настраивать и контролировать в локальном или удаленном режиме на веб-консоли Кибер Бэкап.

11.3.2 На основе WinPE

Загрузочный носитель на основе WinPE содержит минимальную систему Windows, которая называется среда предустановки Windows (WinPE), и подключаемый модуль Киберпротект для WinPE, то есть модификацию агента Кибер Бэкап, запускаемую в среде предустановки.

WinPE – самое удобное загрузочное решение в больших средах с разнообразным оборудованием.

Преимущества:

- Использование Кибер Бэкап в среде предустановки Windows предоставляет больше возможностей, чем применение загрузочного носителя на основе Linux. После загрузки среды WinPE на ПК-совместимом оборудовании можно использовать не только агент Кибер Бэкап, но и команды и сценарии PE и другие подключаемые модули, добавленные в среду PE.
- С помощью загрузочного носителя на основе PE удается решить некоторые проблемы, свойственные загрузочным носителям Linux, например поддержку определенных RAID-контроллеров или только определенных уровней RAID-массивов. Носители на основе WinPE 2.x и последующих версий позволяют динамическую загрузку необходимых драйверов устройств.

Ограничения:

© ООО Киберпротект, 2026

- загрузочные носители на основе версий WinPE ниже 4.0 не позволяют выполнять начальную загрузку компьютеров, на которых используется единый интерфейс EFI (UEFI).
- При загрузке машины с загрузочного носителя для среды PE невозможно выбрать в качестве места сохранения резервной копии оптический носитель, например CD, DVD или диск Blu-ray (BD).

11.4 Мастер создания загрузочных носителей

Мастер создания загрузочных носителей – это специальное средство для создания загрузочных носителей.

Мастер создания загрузочных носителей устанавливается по умолчанию при установке сервера управления. Его можно установить отдельно на любой машине с ОС Windows или Linux. Поддерживаются те же операционные системы, что и для соответствующих агентов.

В большинстве случаев для загрузки машины, которая использует интерфейс UEFI, требуется 64-разрядный носитель.

11.4.1 Цели использования мастера создания носителей

Готовый загрузочный носитель, доступный для скачивания на веб-сайте Киберпротект, можно использовать только для восстановления. Этот носитель основан на ядре Linux. В отличие от среды Windows PE, он не позволяет вводить пользовательские драйверы на лету.

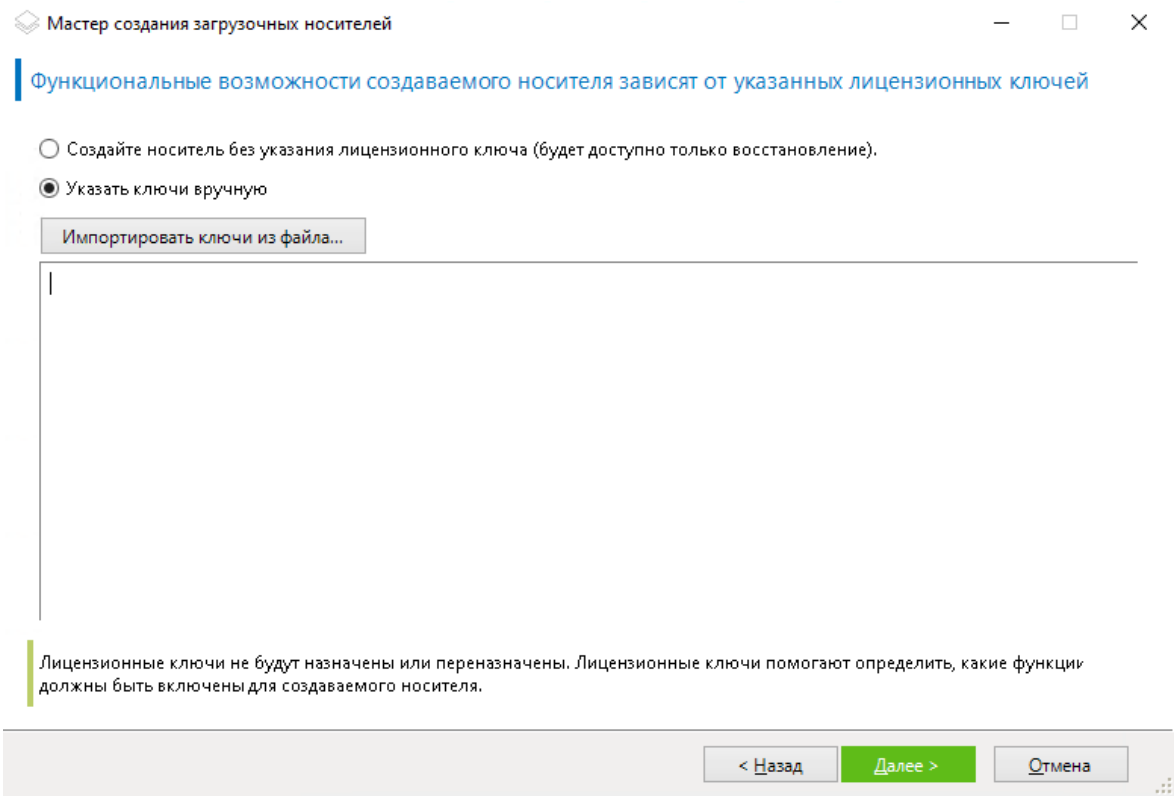
- С помощью мастера создания загрузочных носителей можно создавать настраиваемые полнофункциональные загрузочные носители на основе Linux или WinPE с функциями резервного копирования.
- Помимо создания физического загрузочного носителя, можно передать его компоненты в службах развертывания Windows (WDS) и использовать загрузку по сети.
- Готовый загрузочный носитель не поддерживает узел хранения, хранилища на ленте и хранилища SFTP. Если вы намерены использовать эти хранилища, необходимо будет создать собственный загрузочный носитель, используя для этого мастер создания загрузочных носителей.

11.4.2 Загрузочные носители на основе Linux

Как создать загрузочный носитель на основе Linux

1. Запустите **Мастер создания загрузочных носителей**.
2. Чтобы создать полнофункциональный загрузочный носитель, укажите лицензионный ключ Кибер Бэкап. Этот ключ используется для определения функций, которые будут представлены на загрузочном носителе. Лицензии не будут отзываться.
   Если не указать лицензионный ключ, полученный загрузочный носитель можно использовать только для операций восстановления и доступа к компоненту Универсальное восстановление (Universal Restore).

© ООО Киберпротект, 2026

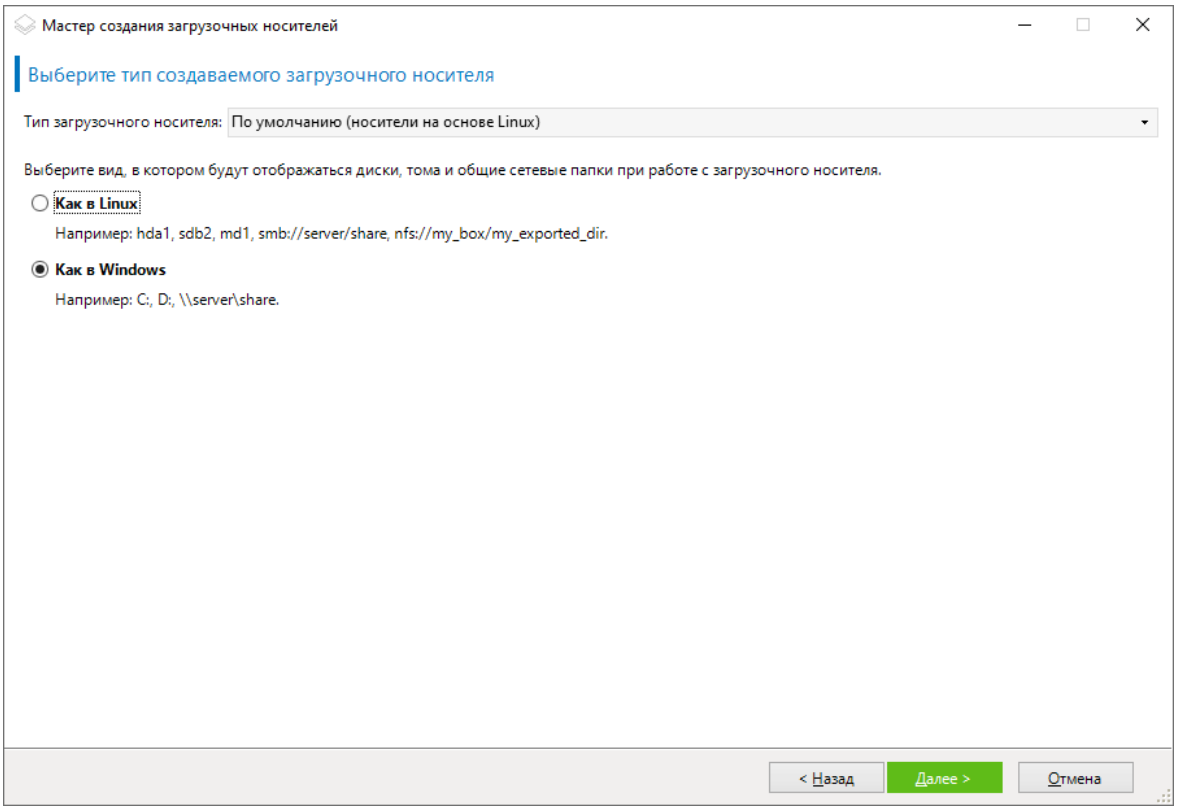


3. Выберите **Тип загрузочного носителя: По умолчанию (носители на основе Linux)**.

   Выберите способ представления томов и сетевых ресурсов:

   - На носителе с представлением томов по типу Linux тома отображаются как, например, hda1 и sdb2. Перед началом восстановления предпринимается попытка реконструировать MD-устройства и LVM (диспетчер логических томов).
   - На носителе с представлением томов по типу Windows тома отображаются как, например, C: и D:. Он обеспечивает доступ к динамическим томам (LDM).

© ООО Киберпротект, 2026

4. 

5. [Необязательно] Укажите параметры ядра Linux. Несколько параметров разделяются пробелами.

   Например, чтобы включить выбор режима дисплея для загрузочного агента при каждом запуске носителя, введите: **vga=ask**

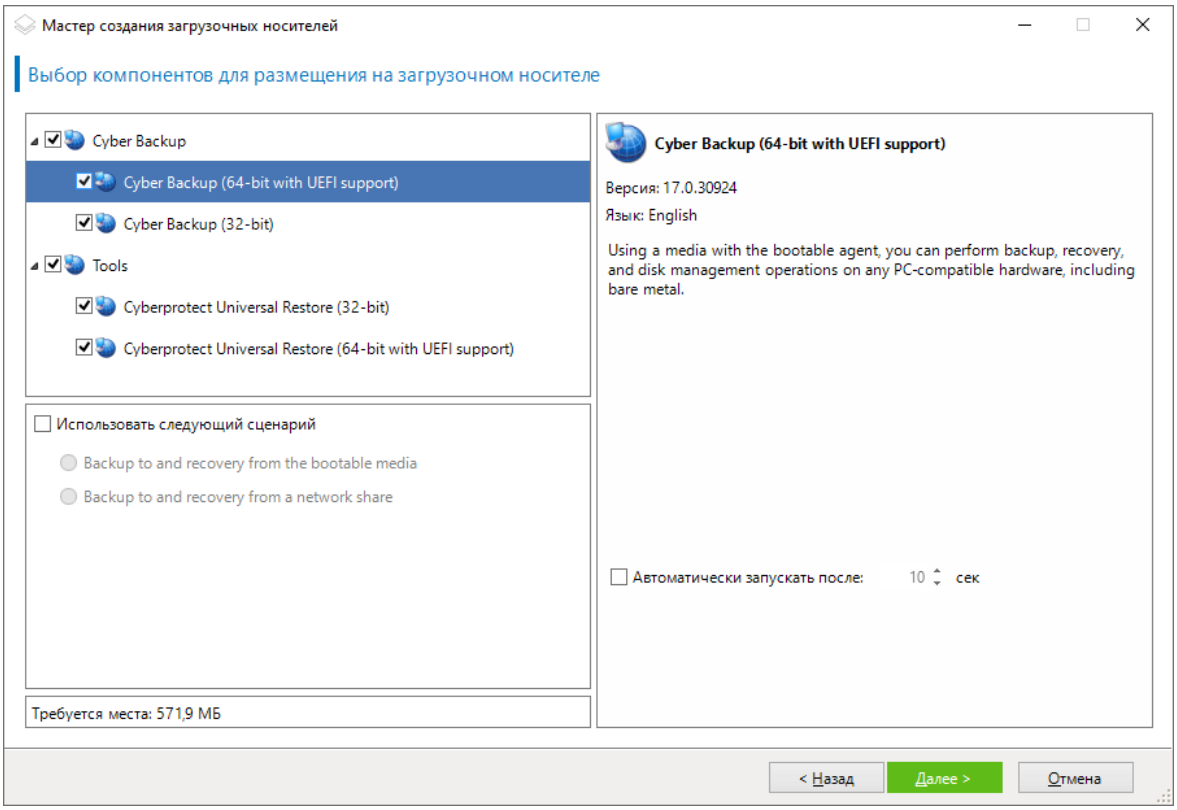
   Дополнительную информацию о доступных параметрах см. в разделе Параметры ядра.
6. [Дополнительно] Выберите язык, который будет использоваться в загрузочном носителе.
7. Выберите компоненты, которые будут размещены на носителе: загрузочный агент Кибер Бэкап и (или) Универсальное восстановление (Universal Restore), если вы планируете восстанавливать систему на отличающееся оборудование.

   Загрузочный агент позволяет выполнить операции резервного копирования, восстановления и управления дисками на любом ПК-совместимом оборудовании, включая "голое железо".

   Компонент Универсальное восстановление (Universal Restore) позволяет загружать операционную систему, восстановленную на отличающееся оборудование или на виртуальную машину. Этот инструмент находит и устанавливает драйверы для устройств, необходимых для запуска операционной системы, таких как контроллеры памяти, системная плата или набор микросхем.
8. [Необязательно] Укажите время ожидания для меню загрузки и компонент, который будет автоматически запускаться по истечении этого времени. Для этого щелкните нужный компонент в левой верхней панели и задайте интервал для него. Это позволяет автоматически выполнять операции на рабочем месте при загрузке из WDS или RIS.

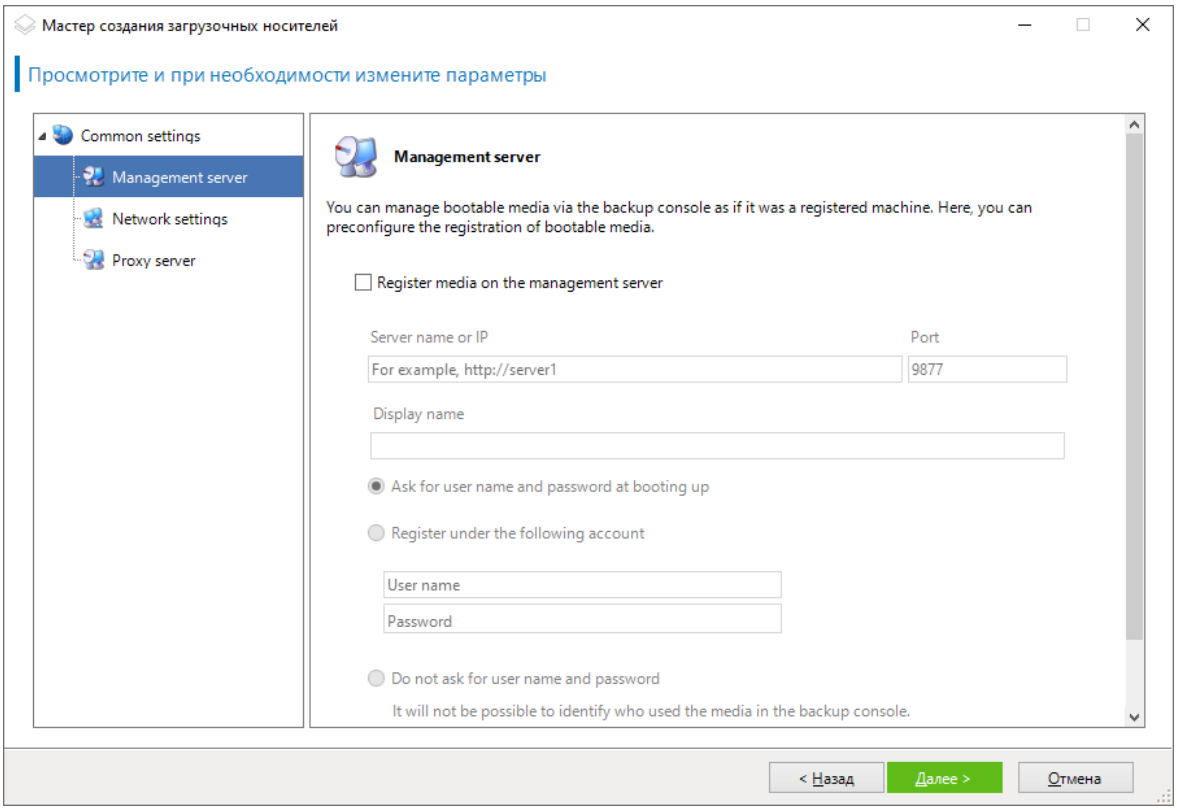
   Если эта настройка не задана, загрузчик ждет, пока вы выберете, загружать ли операционную систему (если есть) или компонент.

© ООО Киберпротект, 2026



9. [Необязательно] Чтобы автоматизировать операции загрузочного агента, установите флажок **Использовать следующий сценарий**. Затем выберите один из сценариев и задайте его параметры.
10. [Необязательно] Выберите способ регистрации носителя на сервере управления при загрузке. Дополнительную информацию о настройках регистрации см. в разделе Сервер управления.

© ООО Киберпротект, 2026



11. [Необязательно] Укажите сетевые настройки: настройки TCP/IP для назначения сетевым адаптерам машины.
12. [Необязательно] Укажите сетевой порт: TCP-порт, который прослушивается загрузочным агентом для приема входящих подключений.
13. [Необязательно] Если в сети включен прокси-сервер, укажите его имя хоста или IP-адрес и порт.
14. Выберите тип носителя. Можно сделать следующее:
    - Создайте ISO-образ. Затем можно записать его на CD/DVD-диск, использовать для создания загрузочного флэш-накопителя USB или подключить его к виртуальной машине.
    - Создайте ZIP-файл.
    - Передать выбранные компоненты на PXE-сервер Киберпротект.
    - Загрузить выбранные компоненты на WDS/RIS.
15. [Необязательно] Добавьте системные драйверы Windows для использования компонентом Универсальное восстановление (Universal Restore). Это окно отображается в том случае, если компонент добавлен на носитель и выбран носитель, отличный от WDS и RIS.
16. При необходимости укажите имя хоста или IP-адрес и учетные данные для WDS или RIS либо путь к ISO-файлу носителя.
17. Проверьте настройки в итоговом окне и щелкните **Приступить**.

© ООО Киберпротект, 2026

11.4.2.1 Параметры ядра

Это окно позволяет указывать параметры для ядра Linux. Они будут применены автоматически при запуске загрузочного носителя.

Обычно эти параметры используются при наличии проблем с работой загрузочных носителей. Как правило, это поле оставляется пустым.

Кроме того, можно указать любой из этих параметров, нажав клавишу F11 в меню загрузки.

Параметры

Если задается несколько параметров, они должны быть разделены пробелами.

acpi=off

Отключает интерфейс ACPI. Этот параметр может использоваться при наличии проблем с определенной конфигурацией оборудования.

noapic

Отключает расширенный программируемый контроллер прерываний Advanced Programmable Interrupt Controller (APIC). Этот параметр может использоваться при наличии проблем с определенной конфигурацией оборудования.

vga=ask

Предлагает указать видеорежим для графического пользовательского интерфейса загрузочного носителя. Если параметр **vga** не задан, то видеорежим определяется автоматически.

vga=*mode_number*

Задает видеорежим для графического пользовательского интерфейса загрузочного носителя. Номер режима задается параметром *mode_number* в шестнадцатеричном формате, например **vga=0x318**

Разрешение экрана и количество цветов, соответствующее номеру режима, может различаться на разных машинах. Рекомендуется в качестве значения **номер_режима** сначала использовать параметр *vga=ask*.

quiet

Отключает отображение загрузочных сообщений при загрузке ядра Linux и запускает консоль управления после загрузки ядра.

Этот параметр указан неявно при создании загрузочного носителя, однако его можно удалить из меню загрузки.

Без этого параметра будут отображаться все сообщения загрузки, потом появится командная строка. Чтобы запустить консоль управления из командной строки, запустите следующую команду: **/bin/product**

nousb

© ООО Киберпротект, 2026

Отключает загрузку подсистемы USB.

nousb2

Отключает поддержку USB 2.0. Устройства USB 1.1 при наличии этого параметра продолжают работать. Этот параметр позволяет использовать некоторые USB-устройства в режиме USB 1.1, если они не работают в режиме USB 2.0.

nodma

Отключает прямой доступ к памяти access (DMA) для всех жестких дисков IDE. Предотвращает зависание ядра с некоторым оборудованием.

nofw

Отключает поддержку интерфейса FireWire (IEEE1394).

nopcmcia

Отключает распознавание оборудования PCMCIA.

nomouse

Отключает поддержку мыши.

module_name **=off**

Отключает модуль, имя которого задано параметром *module_name*. Например, чтобы отключить использование модуля SATA, задайте параметр **sata_sis=off**

pci=bios

Включает принудительное использование BIOS PCI вместо непосредственного доступа к устройству. Этот параметр может потребоваться, если машина имеет нестандартный мост хоста PCI.

pci=nobios

Отключает использование BIOS PCI. Будут разрешены только прямые методы доступа к оборудованию. Этот параметр может понадобиться, если загрузочный носитель не загружается. Это может вызывать BIOS.

pci=biosirq

Использует вызовы BIOS PCI для получения таблицы маршрутизации прерываний. Этот параметр может понадобиться, если ядру не удается выделять запросы на прерывания (IRQ) или не удается обнаружить вторичные шины PCI на материнской плате.

Эти вызовы могут работать на некоторых машинах неправильно. Однако это может быть единственный способ получения таблицы маршрутизации прерываний.

LAYOUTS=en-US, de-DE, fr-FR, ...

Задает раскладки клавиатуры, которые можно использовать в графическом интерфейсе пользователя загрузочного носителя.

© ООО Киберпротект, 2026

Если данный параметр не указан, могут использоваться только две раскладки: «Английский (США)» и раскладка, которая соответствует языку, выбранному в меню загрузки носителя.

Укажите один из следующих параметров:

Бельгийский: **be-BE**

Чешский: **cz-CZ**

Английский: **en-GB**

Английский (США): **en-US**

Французский: **fr-FR**

Французский (Швейцария): **fr-CH**

Немецкий: **de-DE**

Немецкий (Швейцария): **de-CH**

Итальянский: **it-IT**

Польский: **pl-PL**

Португальский: **pt-PT**

Португальский (Бразилия): **pt-BR**

Русский: **ru-RU**

Сербский (кириллица): **sr-CR**

Сербский (латиница): **sr-LT**

Испанский: **es-ES**

При работе на загрузочном носителе, используйте CTRL + SHIFT для перехода по доступным раскладкам.

11.4.2.2 Сценарии на загрузочных носителях

Для того, чтобы на загрузочном носителе выполнялся определенный набор операций, укажите сценарий при создании носителя в Bootable Media Builder. При каждой загрузке носителя вместо отображения пользовательского интерфейса начнется выполнение сценария.

Выберите один из предопределенных сценариев или создайте пользовательский сценарий в соответствии со стандартами создания сценариев.

Предопределенный сценарий

Bootable Media Builder предоставляет следующие предопределенные сценарии:

- резервное копирование данных на загрузочный носитель и восстановление данных с загрузочного носителя (**entire_pc_local**);

© ООО Киберпротект, 2026

- резервное копирование данных в сетевую папку и восстановление данных из сетевой папки (**entire_pc_share**);

Сценарии находятся на машине, на которой установлено приложение Bootable Media Builder, в следующих папках:

- В ОС Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- В ОС Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Резервное копирование данных на загрузочный носитель и восстановление данных с загрузочного носителя

Сценарий создаст резервную копию машины на загрузочном носителе или восстановит машину из последней резервной копии, созданной этим сценарием на том же носителе. При запуске сценарий отправит пользователю запрос с возможностью выбора между созданием резервной копии, восстановлением из резервной копии и запуском пользовательского интерфейса.

В Bootable Media Builder вы можете указать пароль, который сценарий будет использовать для защиты резервных копий или доступа к ним.

Резервное копирование данных в сетевую папку и восстановление данных из сетевой папки

Сценарий создаст резервную копию машины в сетевой папке или восстановит машину из последней резервной копии, расположенной в сетевой папке. При запуске сценарий отправит пользователю запрос с возможностью выбора между созданием резервной копии, восстановлением из резервной копии и запуском пользовательского интерфейса.

В Bootable Media Builder укажите следующие параметры сценария:

1. путь к сетевой папке;
2. имя пользователя и пароль для доступа в сетевую папку;
3. [Необязательно] имя файла резервной копии. Значением по умолчанию является **AutoBackup** (Автоматическое резервное копирование). Если вы хотите, чтобы сценарий добавлял резервные копии к уже существующим резервным копиям, или провести восстановление из резервной копии с заданным пользователем именем, измените значение по умолчанию на имя файла желаемой резервной копии.

   Как узнать имя файла резервной копии

   a. На веб-консоли Кибер Бэкап последовательно выберите пункты **Хранилища резервных копий** > **Хранилища**.
   b. Выберите сетевую папку (нажмите **Добавить хранилище**, если нужной папки нет в списке).
   c. Выберите резервную копию.
   d. Нажмите **Сведения**. Имя файла отобразиться в поле **Имя файла резервной копии**.
4. [Необязательно] пароль, который сценарий будет использовать для защиты резервных копий или доступа к ним.

© ООО Киберпротект, 2026

Пользовательские сценарии

Внимание
Создание пользовательских сценариев требует знания команд оболочки Bash и формата JavaScript Object Notation (JSON). Если вы не знакомы с командной оболочкой Bash, хороший учебник можно найти по ссылке http://www.tldp.org/LDP/abs/html. Спецификация JSON доступна на сайте http://www.json.org.

Файлы сценария

Сценарий должен быть расположен в указанных ниже каталогах на машине, в которой установлен мастер создания загрузочных носителей:

- В ОС Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- В ОС Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Сценарий должен состоять из по меньшей мере трех файлов:

- **<файл_сценария>.sh** – файл со сценарием Bash. При создании сценария используйте только ограниченный набор команд оболочки, который вы можете найти по ссылке https://busybox.net/downloads/BusyBox.html. Также могут быть использованы следующие команды:
  - acrocmd – утилита командной строки для создания резервной копии и восстановления
  - product – команда, запускающая пользовательский интерфейс загрузочного носителя

  Этот файл и все другие включенные в сценарий дополнительные файлы (например, посредством использования команды с точкой) должны быть расположены в подпапке **bin**. В сценарии укажите дополнительные пути к файлам в виде **/ConfigurationFiles/bin/<файл>**.
- **autostart** – файл для запуска **<файл_сценария>.sh**. Содержимое файла должно быть следующим:

  ```
  #!/bin/sh
  . /ConfigurationFiles/bin/variables.sh
  . /ConfigurationFiles/bin/<script_file>.sh
  . /ConfigurationFiles/bin/post_actions.sh
  ```
- **autostart.json** – файл формата JSON, содержащий следующее:
  - Имя сценария и описания будут отображаться в мастере создания загрузочных носителей.
  - Имена переменных сценария должны быть настроены через мастер создания загрузочных носителей.
  - Параметры элементов управления, которые будут отображены в Bootable Media Builder для каждой переменной.

Структура autostart.json

Объект высшего уровня

© ООО Киберпротект, 2026

Пара		Требуется	Описание
Имя	**Тип значения**		
displayName	строка	Да	Имя сценария, которое будет отображаться в Bootable Media Builder.
description	строка	Нет	Описание сценария, которое будет отображаться в Bootable Media Builder.
timeout	число	Нет	Время ожидания (в секундах) для меню загрузки перед запуском сценария. Если пара не указана, время ожидания составит десять секунд.
variables	объект	Нет	Любые переменные для **<файл_сценария>.sh**, которые вы хотите сконфигурировать посредством Bootable Media Builder. Значение должно быть указано в виде набора следующих пар: идентификатор строки переменной и объект переменной (см. в таблице ниже).

Объект переменной

Пара		Требуется	Описание
Имя	**Тип значения**		
displayName	строка	Да	Имя переменной, использованное в **<файл_сценария>.sh**.
type	строка	Да	Тип элемента управления, отображенный в Bootable Media Builder. Этот элемент управления используется для конфигурирования значения переменной. Список всех поддерживаемых типов см. в таблице ниже.
description	строка	Да	Метка элемента управления, отображаемая над элементом управления в Bootable Media Builder.
default	строка, если type является string, multiString, password или enum число, еслиtype является number,	Нет	Значение по умолчанию элемента управления. Если пара не указана, значением по умолчанию будет являться пустая строка или ноль, в зависимости от типа элемента управления. Значением по умолчанию для флажка может быть 0 (флажок не установлен) или 1 (флажок установлен).

© ООО Киберпротект, 2026

	spinner или checkbox		
order	число (не отрицательное)	Да	Порядок элементов управления в Bootable Media Builder. Чем выше значение, тем ниже расположен элемент управления относительно других элементов управления, указанных в **autostart.json**. Изначальным значение должен быть 0.
min (только для spinner)	число	Нет	Минимальное значение элемента управления «счетчик» в поле счетчика. Если пара не указана, значением будет 0.
max (только для spinner)	число	Нет	Максимальное значение элемента управления «счетчик» в поле счетчика. Если пара не указана, значением будет 100.
step (только для spinner)	число	Нет	Значение шага элемента управления «счетчик» в поле счетчика. Если пара не указана, значением будет 1.
items (только для enum)	массив строк	Да	Значения для раскрывающегося списка.
required (для string, multiString, password и enum)	число	Нет	Указывает, может ли значение элемента управления быть пустым (0) или нет (1). Если пара не указана, значение элемента управления может быть пустым.

Тип элемента управления

Имя	Описание
string	Текстовое поле высотой в одну строку и без ограничений ширины, используемое для введения или редактирования коротких строк.
multiString	Текстовое поле высотой в несколько строк и без ограничений ширины, используемое для введения или редактирования коротких строк.
password	Текстовое поле высотой в одну строку и без ограничений ширины, используемое для безопасного введения пароля.
number	Текстовое поле высотой в одну строку, с допустимым введением только числовых значений, используемое для введения или редактирования чисел.

© ООО Киберпротект, 2026

spinner	Текстовое поле высотой в одну строку, с допустимым введением только числовых значений, используемое для введения или редактирования чисел, с элементом управления «счетчик». Также называется полем счетчика.
enum	Стандартный выпадающий список с фиксированным набором предварительно указанных значений.
checkbox	Поле флажка с двумя положениями – флажок установлен и флажок не установлен.

Указанный ниже пример **autostart.json** содержит все возможные типы элементов управления, которые могут быть использованы для конфигурирования переменных для файла **<файл_сценария>.sh**.

```
{
    "displayName": "Имя автоматически запускаемого сценария",
    "description": «Это – описание автоматически запускаемого сценария",
    "variables": {
        "var_string": {
            "displayName": "VAR_STRING",
            "type": "string", "order": 1,
            "description": «Это – элемент управления 'string':", "default": "Hello, world!"
        },
        "var_multistring": {
            "displayName": "VAR_MULTISTRING",
            "type": "multiString", "order": 2,
            "description": «Это – элемент управления 'multiString':",
            "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
        },
        "var_number": {
            "displayName": "VAR_NUMBER",
            "type": "number", "order": 3,
            "description": "Это – элемент управления 'number':", "default": 10
        },
        "var_spinner": {
            "displayName": "VAR_SPINNER",
```


© ООО Киберпротект, 2026

```
                "type": "spinner", "order": 4,
                "description": "Это – элемент управления 'spinner':",
                "min": 1, "max": 10, "step": 1, "default": 5
            },
            "var_enum": {
                "displayName": "VAR_ENUM",
                "type": "enum", "order": 5,
                "description": "Это – элемент управления 'enum':",
                "items": ["первый", "второй", "третий"], "default": "второй"
            },
            "var_password": {
                "displayName": "VAR_PASSWORD",
                "type": "password", "order": 6,
                "description": "Это – элемент управления 'password':", "default": "qwe"
            },
            "var_checkbox": {
                "displayName": "VAR_CHECKBOX",
                "type": "checkbox", "order": 7,
                "description": "Это – элемент управления 'checkbox'", "default": 1
            }
        }
}
```

11.4.2.3 Сервер управления

При создании загрузочного носителя есть возможность предварительно сконфигурировать регистрацию носителя на сервере управления.

Регистрация носителя позволит выполнять операции управления с загрузочным носителем посредством веб-консоли Кибер Бэкап, как с зарегистрированной машиной. Кроме удобства удаленного доступа это дает системному администратору возможность отслеживать все операции, выполняемые на загрузочном носителе. Операции находятся на вкладке **Действия**, где можно увидеть, кто и когда начал выполнение операции.

Если регистрация не была предварительно сконфигурирована, остается возможность зарегистрировать носитель после загрузки с него машины.

© ООО Киберпротект, 2026

Как выполнить предварительную конфигурацию регистрации на сервере управления.

1. Установите флажок **Зарегистрировать носитель на сервере управления**.
2. В строке **Имя или IP-адрес сервера** укажите имя хоста или IP-адрес машины, на которой установлен сервер управления. Используйте один из следующих форматов.
   - http://<сервер>. Например, http://10.250.10.10 или http://server1
   - <IP-адрес>. Например, 10.250.10.10
   - <имя хоста>. Например, server1 или server1.example.com
3. В строке **Порт** укажите порт, который будет использоваться для доступа к серверу управления. Значение по умолчанию составляет 9877.
4. В строке **Отображаемое имя** укажите имя, которое будет отображаться для этой машины на веб-консоли Кибер Бэкап. Если это поле будет оставлено пустым, в качестве отображаемого имени будет указано одно из следующих.
   - Если машина ранее была зарегистрирована на сервере управления, у нее будет то же имя.
   - В ином случае будет использовано полное доменное имя (FQDN) или IP-адрес машины.
5. Выберите учетную запись, которая будет использована для регистрации носителя на сервере управления. Доступны следующие параметры:
   - **Спрашивать имя пользователя и пароль при загрузке**

     Учетные данные необходимо вводить при каждой загрузке машины с носителя.

     Для выполнения регистрации учетная запись должна находится в списке администраторов сервера управления (**Настройки** > **Учетные записи**). На веб-консоли Кибер Бэкап носитель будет доступен в разделе организации или конкретного отдела в соответствии с правами, которые предоставлены данной учетной записи.

     В интерфейсе загрузочного носителя будет возможно изменить имя пользователя и пароль, перейдя по пути **Инструменты** > **Зарегистрировать носитель на сервере управления**.
   - **Зарегистрироваться под следующей учетной записью**

     Машина будет регистрироваться автоматически при каждой загрузке с носителя.

     Указанная учетная запись должна находится в списке администраторов сервера управления (**Настройки** > **Учетные записи**). На веб-консоли Кибер Бэкап носитель будет доступен в разделе организации или конкретного отдела в соответствии с правами, которые предоставлены данной учетной записи.

     В интерфейсе загрузочного носителя будет *невозможно* сменить параметры регистрации.

11.4.2.4 Сетевые настройки

При создании загрузочного носителя можно предварительно настроить сетевые подключения, которые будут использоваться загрузочным агентом. Предварительно настроить можно следующие параметры:

- IP-адрес,
- маску подсети,

© ООО Киберпротект, 2026

- шлюз,
- DNS-сервер,
- WINS-сервер.

После запуска загрузочного агента на машине конфигурация применяется к сетевому адаптеру машины. Если параметры не были предварительно настроены, агент использует автонастройку DHCP. Также вы можете задать сетевые параметры вручную при запуске загрузочного агента на машине.

Предварительная настройка нескольких сетевых подключений

Можно предварительно настроить параметры TCP/IP вплоть до десяти сетевых адаптеров. Чтобы убедиться, что каждому сетевому адаптеру будут назначены соответствующие параметры, создайте носитель на сервере, для которого настраивается носитель. При выборе существующего сетевого адаптера в окне мастера ее настройки выбираются для сохранения на носителе. MAC-адрес каждого существующего сетевого адаптера также сохраняется на носителе.

Параметры, кроме MAC-адреса, можно изменить или при необходимости настроить для несуществующего сетевого адаптера.

После запуска загрузочного агента на сервере он получает список доступных сетевых адаптеров. Этот список сортируется по слотам, которые занимают сетевые адаптеры: чем ближе к процессору, тем выше в списке.

Загрузочный агент назначает каждому известному сетевому адаптеру соответствующие настройки, идентифицируя адаптеры по MAC-адресам. После настройки сетевых адаптеров с известными MAC-адресами оставшимся сетевым адаптерам назначаются настройки, созданные для несуществующих сетевых адаптеров, начиная с верхнего неназначенного адаптера.

Загрузочный носитель можно настроить для любой машины, а не только для той, на которой он был создан. Для этого настройте сетевые адаптеры в соответствии с порядком их слотов на нужной машине: NIC1 занимает ближайший к процессору слот, NIC2 – следующий слот и т. д. При запуске загрузочного агента на этой машине он не найдет сетевых адаптеров с известными MAC-адресами и настроит адаптеры в том порядке, который вы указали.

Пример

Загрузочный агент может использовать один из сетевых адаптеров для связи с консолью управления через производственную сеть. Для этого подключения можно выполнить автоматическую настройку. Объемные данные для восстановления можно передавать через второй сетевой адаптер, включенный в выделенную резервную сеть посредством статических настроек TCP/IP.

11.4.2.5 Сетевой порт

Во время создания загрузочного носителя можно предварительно настроить сетевой порт, который будет прослушиваться загрузочным агентом на наличие входящего подключения от утилиты acrocmd. Можно выбрать один из указанных ниже вариантов.

© ООО Киберпротект, 2026

- Порт по умолчанию
- Текущий используемый порт
- Новый порт (введите номер порта)

Если порт не был предварительно настроен, агент использует порт 9876.

11.4.2.6 Драйверы для компонента Универсальное восстановление (Universal Restore)

При создании загрузочного носителя есть возможность добавить на него драйверы Windows. Эти драйверы будут использоваться компонентом Универсальное восстановление (Universal Restore) для загрузки системы Windows, перенесенной на отличающееся оборудование.

Компонент Универсальное восстановление (Universal Restore) можно будет настроить для следующих целей:

- для поиска на носителе драйверов, наилучшим образом подходящих для целевого оборудования;
- для получения драйверов устройств хранения данных, явно заданных с носителя. Это необходимо, если целевое оборудование оснащено специфическим контроллером запоминающего устройства (таким как SCSI, RAID или адаптер Fiber Channel) для жесткого диска.

Драйверы будут размещены в видимой папке Drivers на загрузочном носителе. Драйверы не загружаются в ОЗУ целевой машины, поэтому носитель должен оставаться вставленным или подключенным в течение всей работы компонента Универсальное восстановление (Universal Restore).

Добавить драйверы на загрузочный носитель можно при создании съемного носителя, его ISO-образа или подключаемого носителя, такого как флэш-накопитель. Драйверы невозможно загрузить в WDS или RIS.

Драйверы можно добавить в список только в группах путем добавления INF-файлов или папок, содержащих такие файлы. Выбор отдельных драйверов из INF-файлов невозможен, однако мастер создания загрузочных носителей отображает содержимое файла для сведений.

Чтобы добавить драйверы

1. Щелкните **Добавить** и перейдите к INF-файлу или папке, содержащей INF-файлы.
2. Выберите INF-файл или папку.
3. Нажмите кнопку **OK**.

Драйверы можно удалить из списка только в группах путем удаления INF-файлов.

Чтобы удалить драйверы

© ООО Киберпротект, 2026

1. Выберите INF-файл.
2. Нажмите кнопку **Удалить**.

11.4.3 Загрузочный носитель на основе WinPE

Мастер создания загрузочных носителей предоставляет два способа интеграции Кибер Бэкап с WinPE:

- Создание ISO-образа PE с подключаемым модулем с нуля.
- Добавление подключаемого модуля Киберпротект к WIM-файлу для использования в будущем (ручное создание ISO-образа, добавление других средств к образу и т. д.).

Можно создать PE-образы на основе WinRE без какой-либо дополнительной подготовки или создать PE-образы после установки комплекта средств для развёртывания и оценки Windows (ADK).

11.4.3.1 PE-образы на основе WinRE

Создание образов на основе WinRE поддерживается для следующих операционных систем:

- Windows 10–11 (64-разрядные версии);
- Windows Server 2016–2025 (64-разрядные версии).

11.4.3.2 PE-образы

После установки пакета Windows AIK или комплекта средств для развёртывания и оценки Windows (ADK) мастер создания загрузочных носителей поддерживает дистрибутивы WinPE, основанные на любой из следующих ОС:

- Windows 10 (PE для Windows 10);
- Windows 11 (PE для Windows 11).

Мастер создания загрузочных носителей поддерживает 64-разрядные дистрибутивы WinPE для загрузки машин, которые используют интерфейс UEFI.

Для работы образов среды предустановки на основе WinPE 4 (и более поздних версий) требуется около 1 ГБ ОЗУ.

Примечание
Для выполнения операций управления дисками в ОС Windows 10 и более поздних версий необходимо установить Управление Дисками.

11.4.3.3 Подготовка WinPE 4.0 и более поздние версии

Для создания или изменения образов PE 4 или более поздних версий установите мастер создания загрузочных носителей на машину с установленным комплектом средств для развёртывания и оценки Windows (ADK). Если у вас нет машины с ADK, подготовьте её следующим образом.

© ООО Киберпротект, 2026

Как подготовить машину с ADK

1. Загрузите программу установки комплекта средств для развёртывания и оценки (ADK).

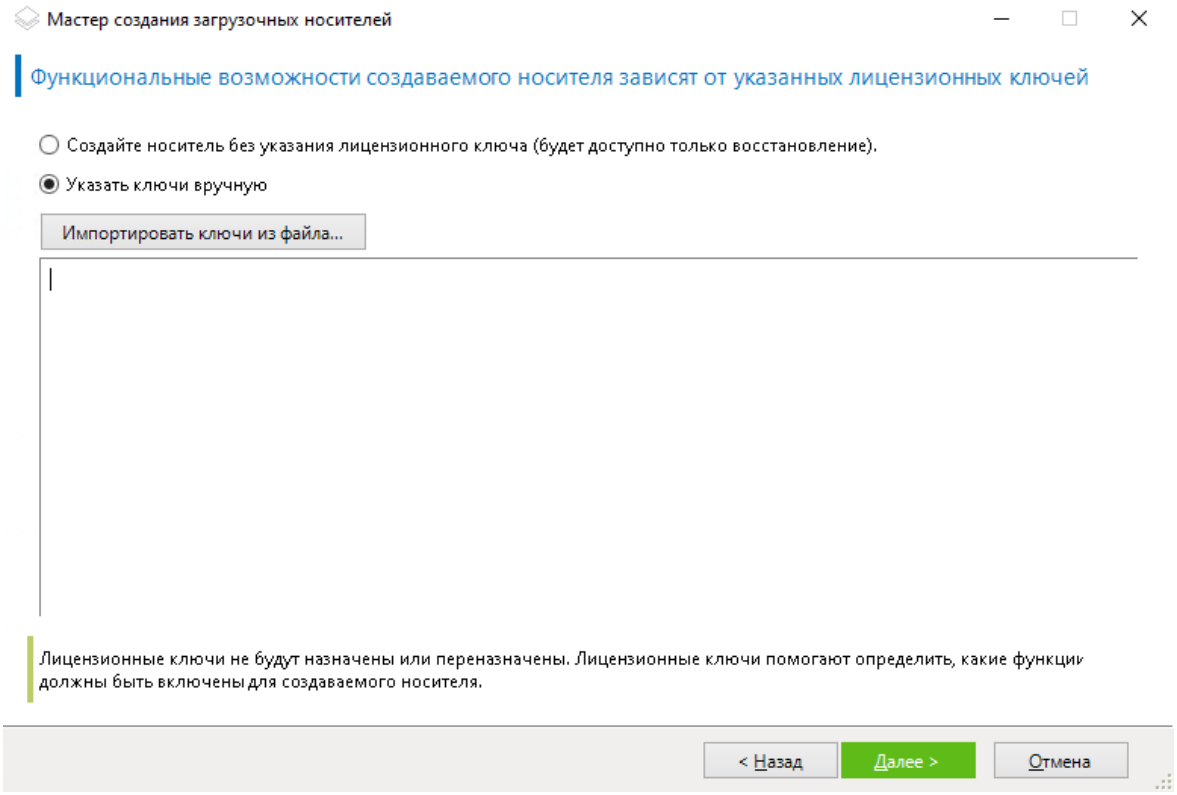
   Скачайте комплект средств для развёртывания и оценки Windows (ADK) для Windows с официальной страницы: https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install.

   Системные требования для установки приведены по указанной выше ссылке.
2. Установите комплект ADK на машине.
3. Установите мастер создания загрузочных носителей на этой же машине.

11.4.3.4 Добавление подключаемого модуля Киберпротект к WinPE

Порядок добавления подключаемого модуля Киберпротект к WinPE

1. Запустите мастер создания загрузочных носителей.
2. Чтобы создать полнофункциональный загрузочный носитель, укажите лицензионный ключ Кибер Бэкап. Этот ключ используется для определения функций, которые будут представлены на загрузочном носителе. Лицензии не будут отзываться. Если не указать лицензионный ключ, полученный загрузочный носитель можно использовать только для операций восстановления и доступа к компоненту Универсальное восстановление (Universal Restore).

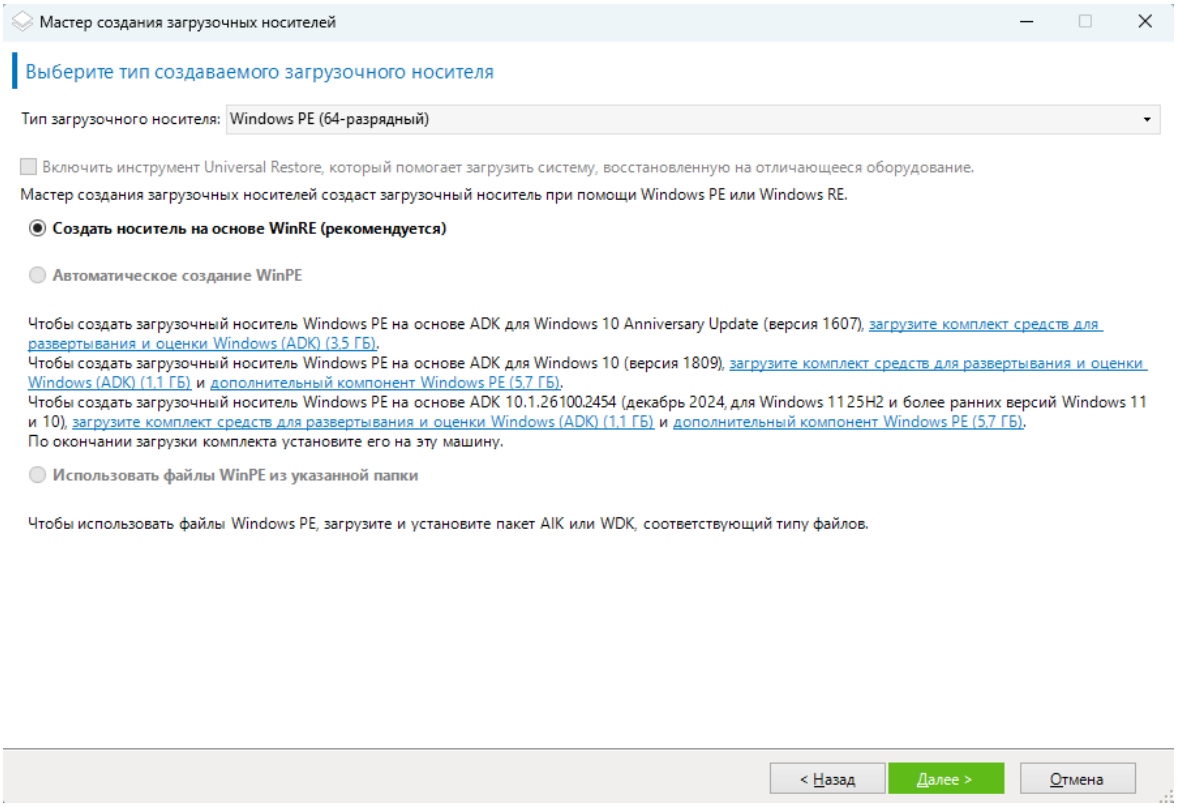


3. Выберите **Тип загрузочного носителя: Windows PE (64-разрядный)**.

   Если планируется восстановить операционную систему на компьютере с другим оборудованием или на виртуальной машине и необходимо обеспечить загружаемость системы, установите флажок **Включить инструмент Universal Restore...**
4. Выберите **Создать носитель на основе WinRE (рекомендуется)**.

© ООО Киберпротект, 2026

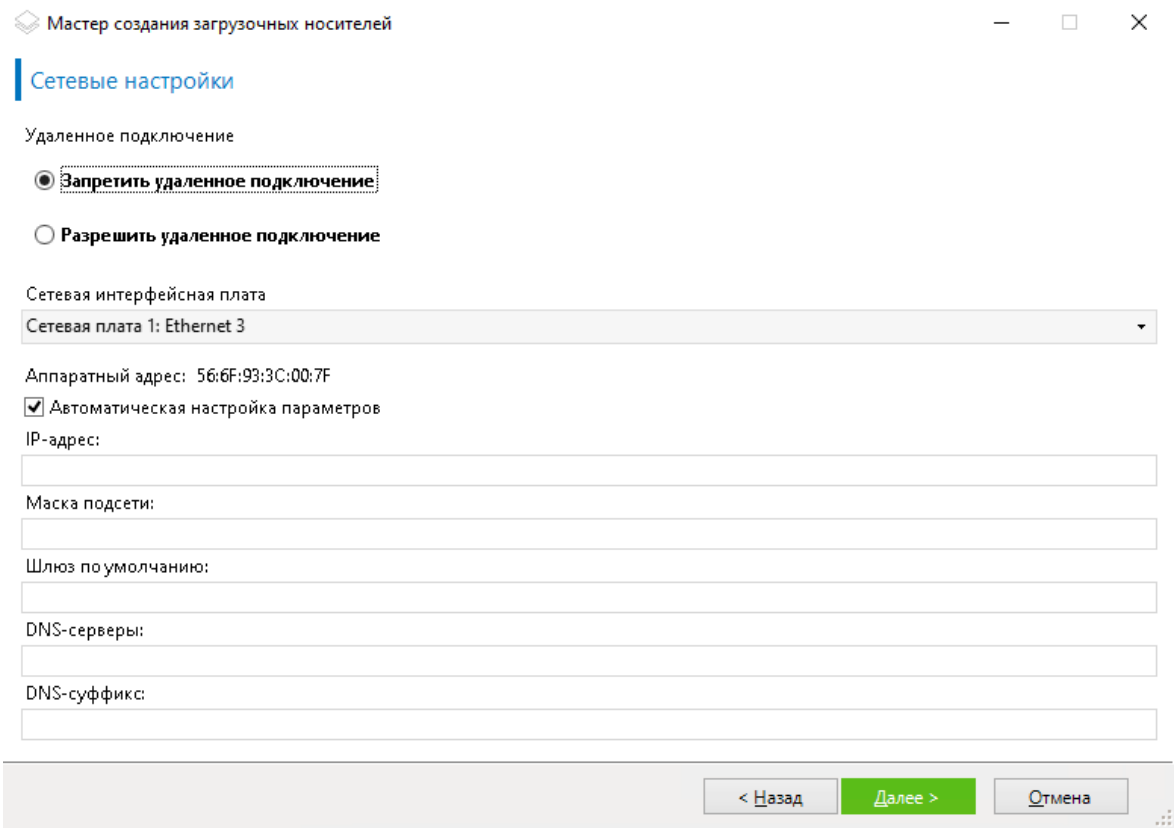
Программа запустит соответствующий сценарий и перейдёт к следующему окну.



5. Выберите язык, который будет использоваться в загрузочном носителе.
6. Выберите, разрешить или запретить удалённое подключение к машине, загружаемой с носителя. Если подключение разрешено, введите имя пользователя и пароль, которые должны быть указаны в командной строке в случае, когда утилита acrocmd выполняется на другой машине. Можно оставить эти поля пустыми. В этом случае удалённое подключение через интерфейс командной строки можно будет выполнить без ввода учётных данных.

   Эти учётные данные также необходимы при регистрации носителя на сервере управления с веб-консоли Кибер Бэкап.

© ООО Киберпротект, 2026



7. Укажите сетевые настройки для сетевых адаптеров машины или выберите автоконфигурацию DHCP.
8. [Необязательно] Выберите способ регистрации носителя на сервере управления при загрузке. Дополнительную информацию о настройках регистрации см. в разделе Сервер управления.
9. [Необязательно] Укажите драйверы Windows, которые нужно добавить к Windows PE.

   После загрузки Windows PE на машину эти драйверы помогут получить доступ к устройствам, на которых расположена резервная копия.

   Кроме того, можно будет указать добавленные драйверы при настройке компонента Универсальное восстановление (Universal Restore) для Windows.

   Как добавить драйверы

   - Щёлкните **Добавить** и задайте путь к INF-файлу для соответствующего контроллера SCSI, RAID или SATA, сетевого адаптера, ленточного устройства или другого устройства.
   - Повторите эту процедуру для каждого драйвера, который необходимо записать на носитель WinPE.
10. Выберите, следует ли создать ISO- или WIM-образ либо загрузить носитель на сервер (WDS или RIS).
11. Задайте полный путь к полученному файлу образа, включая его имя, или укажите сервер и задайте имя пользователя и пароль для доступа к нему.
12. Проверьте настройки в итоговом окне и щёлкните **Приступить**.
13. Запишите ISO-образ на CD- или DVD-диск, используя стороннюю программу, или подготовьте загрузочный флэш-накопитель.

После загрузки машины в WinPE агент запустится автоматически.

© ООО Киберпротект, 2026

Чтобы создать образ среды предустановки (ISO-файл) из получившегося WIM-файла

- Замените в папке Windows PE файл boot.wim, используемый по умолчанию, созданным WIM-файлом. Например, введите:

  ```
  copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
  ```

- Используйте инструмент **Oscdimg**. Например, введите:

  ```
  oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
  ```

Предупреждение
Не копируйте этот пример. Введите команду вручную.

11.5 Подключение к машине, загружаемой с носителя

После загрузки машины с загрузочного носителя терминал машины отображает окно загрузки с IP-адресами, полученными от сервера DHCP или установленными в соответствии с предварительно заданными значениями.

11.5.1 Настройка сети

Чтобы изменить сетевые параметры для текущего сеанса, щелкните **Настроить параметры сети** в окне запуска. Появится окно **Сетевые параметры**, где можно задать сетевые настройки для каждого сетевого адаптера (NIC) машины.

Изменения, внесенные во время сеанса, будут потеряны после перезагрузки машины.

11.5.1.1 Добавление VLAN

В окне **Сетевые параметры** можно добавить виртуальные локальные сети (VLAN). Используйте эту функцию, если требуется доступ к хранилищу резервных копий, включенному в определенную сеть VLAN.

В основном сети VLAN используются для разделения локальной сети на сегменты. Сетевой адаптер, подключенный к порту *доступа* коммутатора, всегда имеет доступ к сети VLAN, указанной в настройках порта. Сетевой адаптер, подключенный к *магистральному* порту коммутатора, имеет доступ к сетям VLAN, указанным в настройках порта, только в случае, если сети VLAN заданы в сетевых параметрах.

Включение доступа к сети VLAN через магистральный порт

1. Щелкните **Добавить VLAN**.
2. Выберите сетевой адаптер, обеспечивающий доступ к локальной сети с нужной сетью VLAN.
3. Укажите идентификатор VLAN.

После щелчка на **OK** появится новая запись в списке сетевых адаптеров.

© ООО Киберпротект, 2026

Если требуется удалить VLAN, щелкните соответствующую сеть VLAN и нажмите кнопку **Удалить VLAN**.

11.5.2 Локальное подключение

Для непосредственной работы на машине, загружаемой с носителя, щелкните **Локальное управление этой машиной** в окне загрузки.

11.5.3 Удаленное подключение

Для удаленного подключения к носителю зарегистрируйте его на сервере управления, как описано в разделе «Регистрация носителя на сервере управления».

11.6 Регистрация носителя на сервере управления

Регистрация загрузочного носителя позволит выполнять операции управления с загрузочным носителем посредством веб-консоли Кибер Бэкап, как с зарегистрированной машиной. Это применимо ко всем загрузочным носителям вне зависимости от метода загрузки (физический носитель, Диспетчер восстановления при загрузке, Киберпротект PXE Server, WDS или RIS).

Регистрация носителей возможна только при наличии на сервере управления хотя бы одной расширенной лицензии Кибер Бэкап.

Носитель можно зарегистрировать в пользовательском интерфейсе носителя.

Параметры регистрации могут быть предварительно настроены в опции Сервер управления Bootable Media Builder. Если все параметры регистрации настроены предварительно, носитель автоматически отображается на веб-консоли Кибер Бэкап. Если некоторые параметры настроены предварительно, некоторые шаги описанной далее процедуры могут быть недоступны.

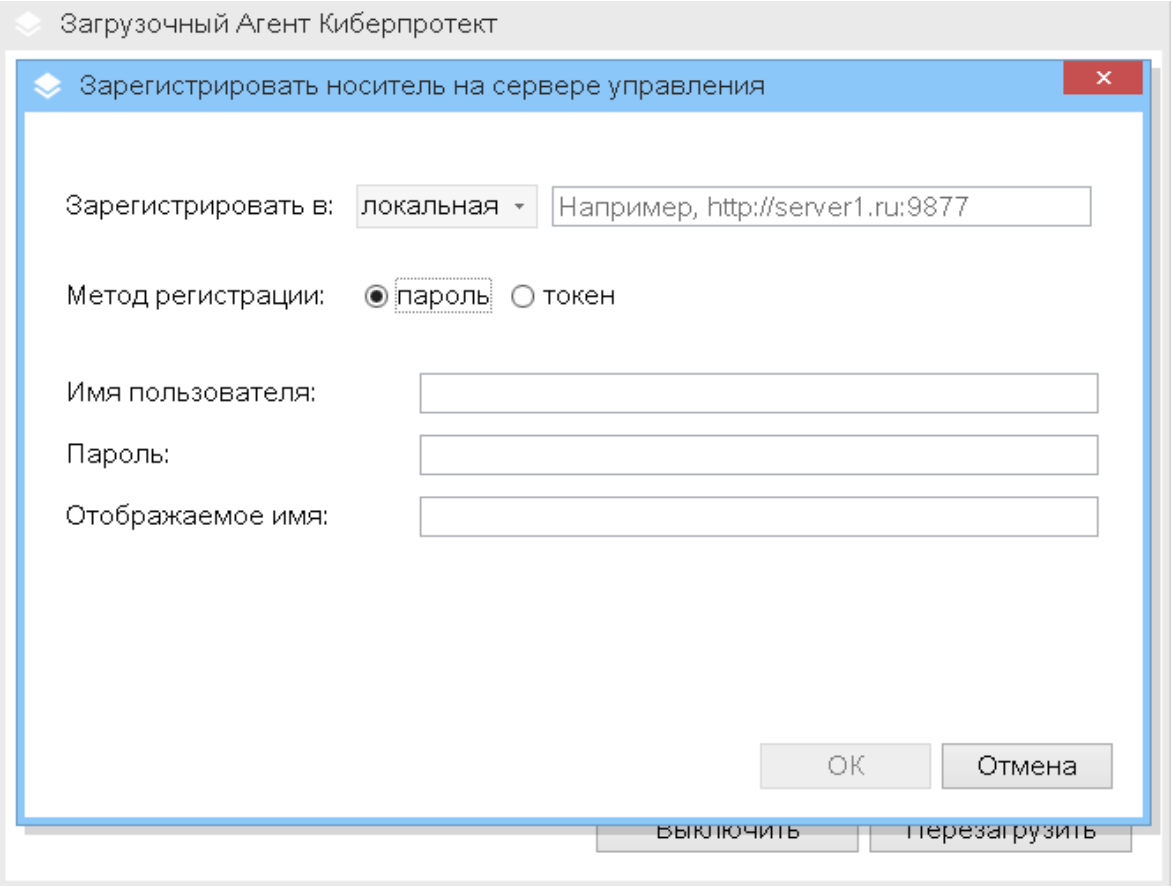
11.6.1 Регистрация носителя в пользовательском интерфейсе носителя

Носитель можно создать или загрузить с использованием Bootable Media Builder.

Регистрация носителя в пользовательском интерфейсе носителя

1. Загрузите машину с носителя.
2. Выполните одно из следующих действий:
   - В окне запуска в поле **Сервер управления** нажмите **Редактировать**.
   - В интерфейсе загрузочного носителя нажмите **Инструменты** > **Зарегистрировать носитель на сервере управления**.

© ООО Киберпротект, 2026



3. В поле **Зарегистрировать в** выберите **Локальная** и укажите имя хоста или IP-адрес машины, на которой установлен сервер управления. Используйте один из следующих форматов.
   - http://<сервер>. Например, http://10.250.10.10 или http://server.
   - <IP-адрес>. Например, 10.250.10.10.
   - <имя хоста>. Например, server или server.example.com.
4. Выберите метод регистрации: пароль или токен. Информацию о создании токена см. в разделе "Развертывание агентов с использованием групповой политики" (стр. 179).
5. При регистрации по токену укажите его в поле **Регистрационный токен** и перейдите к шагу 8.
6. При регистрации по паролю в полях **Имя пользователя** и **Пароль** введите учетные данные учетной записи, которая находится в списке администраторов сервера управления (**Настройки** > **Учетные записи**). В веб-консоли Кибер Бэкап носитель будет доступен в разделе организации или конкретного отдела в соответствии с правами, которые предоставлены данной учетной записи.
7. В строке **Отображаемое имя** укажите имя, которое будет отображаться для этой машины в веб-консоли Кибер Бэкап. Если это поле будет оставлено пустым, в качестве отображаемого имени будет указано одно из следующих:
   - Если машина ранее была зарегистрирована на сервере управления, у нее будет то же имя.
   - В ином случае будет использовано полное доменное имя (FQDN) или IP-адрес машины.
8. Нажмите кнопку **OK**.

© ООО Киберпротект, 2026

11.7 Операции с загрузочным носителем

Операции с загрузочным носителем подобны операциям резервного копирования и восстановления, которые выполняются при запущенной операционной системе. Отличия состоят в следующем:

1. Если используется загрузочный носитель с представлением томов по типу Windows, том имеет такую же букву диска, как в Windows. Томам, которые не имеют букв диска в Windows (например, том "Зарезервировано системой"), присваиваются свободные буквы в порядке их следования на диске.

   Если загрузочный носитель не обнаруживает ОС Windows на машине или обнаруживает несколько систем, всем томам (даже если они не имеют букв дисков), присваиваются буквы в порядке их следования на диске. Поэтому буквы томов могут отличаться от букв томов, отображаемых в Windows. Например, диск D: на загрузочном носителе может соответствовать диску E: в Windows.

   Примечание
   Рекомендуем назначить уникальные имена томам.

2. Загрузочный носитель с представлением томов по типу Linux отображает локальные диски и тома как отключенные (sda1, sda2...).
3. Резервным копиям, созданным с помощью загрузочного носителя, присваиваются упрощенные имена файлов. Стандартные имена назначаются резервным копиям только в случае, если эти резервные копии добавляются к существующему архиву со стандартными именами файлов или если место сохранения не поддерживает упрощенные имена файлов.
4. Загрузочному носителю с представлением томов по типу Linux не удается записать резервные копии на том в формате NTFS. При необходимости сделать это переключитесь на носитель с представлением томов по типу Windows. Чтобы перейти к представлениям томов загрузочного носителя, щелкните **Инструменты** > **Изменить представление томов**.
5. Задания невозможно запланировать в расписании. Если требуется повторить операцию, настройте ее с нуля.
6. Время существования журнала ограничено текущим сеансом. Весь журнал или отфильтрованные записи журнала можно сохранить в файл.
7. Централизованные хранилища не отображаются в дереве папок окна **Архив**.

   Для доступа к управляемому хранилищу введите следующую строку в поле **Путь**:

   bsp://адрес_узла/имя_хранилища/

   Для доступа к неуправляемому централизованному хранилищу введите полный путь к папке хранилища.

   После ввода учетных данных для доступа будет отображен список архивов, расположенных в хранилище.

© ООО Киберпротект, 2026

11.7.1 Настройка режима отображения

Для машины, которая загружается с загрузочного носителя Linux, режим отображения определяется автоматически в зависимости от конфигурации оборудования (характеристик монитора и видеоплаты). Если видеорежим определен неправильно, сделайте следующее.

1. В меню загрузки нажмите клавишу F11.
2. В командной строке введите следующее: **vga=ask**, а затем продолжите загрузку.
3. Из списка поддерживаемых видеорежимов выберите нужный. Для этого введите его номер (например, **318**) и нажмите клавишу **ВВОД**.

Чтобы не выполнять эту процедуру каждый раз при загрузке данной аппаратной конфигурации, создайте загрузочный носитель заново с номером режима (в вышеуказанном примере **vga=0x318**), указанным в окне **Параметры ядра**.

11.7.2 Резервное копирование

Создать резервную копию данных можно только с использованием загрузочного носителя, который создан в мастере создания загрузочных носителей, и лицензионного ключа Кибер Бэкап. Информацию о том, как создать загрузочный носитель, см. в разделах Загрузочные носители на основе Linux или Загрузочный носитель на основе Windows-PE соответственно.

Порядок восстановления данных с помощью загрузочного носителя

1. Выполните загрузку с загрузочного носителя Киберпротект.
2. Чтобы создать резервную копию локальной машины, щелкните **Локальное управление этой машиной**. Для удаленных подключений см. раздел Регистрация носителя на сервере управления.
3. Щелкните **Создать резервную копию сейчас**.
4. Для создания резервной копии автоматически выбираются все несъемные диски. Чтобы изменить данные для резервного копирования, щелкните **Элементы для резервного копирования**, а затем выберите желаемые диски или томы.

   При выборе данных для резервного копирования может выводиться следующее сообщение: "*Эту машину нельзя выбрать напрямую. На машине установлена предыдущая версия агента. Чтобы выбрать эту машину для резервного копирования, используйте правила политики".* Сообщение об этой проблеме с графическим интерфейсом пользователя можно проигнорировать. Выберите отдельные диски или томы, для которых необходимо создать резервные копии.

   Примечание
   Если используется загрузочный носитель на основе Linux, буквы диска могут отличаться от букв диска в Windows. Попробуйте определить необходимый диск или раздел по его размеру или метке.

© ООО Киберпротект, 2026

5. Если необходимо выполнить резервное копирование файлов или папок (а не дисков), перейдите к области **Файлы** в разделе **Данные для резервного копирования**.

   С помощью загрузочного носителя можно создать только резервную копию дисков/разделов и файлов/папок. Другие типы резервного копирования, например, резервное копирование базы данных, можно выполнить только в запущенной операционной системе.
6. Щелкните **Хранилище** и выберите место сохранения резервной копии.
7. Укажите хранилище и имя для резервной копии.
8. Укажите тип резервной копии. Если это первая резервная копия в этом хранилище, будет создана полная резервная копия. Если же создается очередная резервная копия, для экономии места можно выбрать параметр **Инкрементное** или **Дифференциальное**.
9. [Необязательно] Чтобы проверить файл резервной копии, выберите **Проверить резервную копию сразу после создания**.
10. [Необязательно] Укажите параметры резервного копирования, которые могут вам понадобиться, например, пароль для файла резервной копии, разбивка резервной копии или обработка ошибок.
11. Нажмите кнопку **OK**, чтобы начать резервное копирование.

    Загрузочный носитель считывает данные с диска, сжимает их в файл .tib, а затем записывает этот файл в выбранное хранилище. Он не создает моментальный снимок диска, поскольку нет запущенных приложений.
12. В появившемся окне можно проверить статус задания резервного копирования и просмотреть дополнительную информацию о резервном копировании.

11.7.3 Восстановление

Операция восстановления доступна как на загрузочных носителях, созданных с помощью мастера создания загрузочных носителей, так и на скачанных готовых загрузочных носителях.

Порядок восстановления данных с помощью загрузочного носителя

1. Выполните загрузку с загрузочного носителя Киберпротект.
2. Чтобы восстановить данные на локальную машину, щелкните **Локальное управление этой машиной**. Для удаленных подключений см. раздел Регистрация носителя на сервере управления.
3. Нажмите кнопку **Восстановить**.
4. В разделе **Объект восстановления** щелкните **Выбрать данные**.
5. Щелкните **Обзор** и выберите хранилище резервных копий.
6. Выберите файл резервной копии, на основе которой необходимо выполнить восстановление.
7. В левой нижней панели выберите файлы и тома (или файлы и папки), которые необходимо восстановить, и нажмите кнопку **OK**.
8. [Необязательно] Настройте правила перезаписи.
9. [Необязательно] Настройте исключения восстановления.

© ООО Киберпротект, 2026

10. [Необязательно] Настройте параметры восстановления.
11. Проверьте правильность настроек и нажмите кнопку **OK**.

Примечание
Для восстановления данных на отличающееся оборудование необходимо использовать компонент Универсальное восстановление (Universal Restore). Он недоступен, если резервная копия находится в Зоне безопасности.

11.7.4 Управление дисками

С помощью загрузочного носителя Киберпротект можно подготовить конфигурацию диска/тома для восстановления образов тома, резервная копия которых создана Кибер Бэкап.

Иногда, когда том скопирован и его образ помещен в безопасное хранилище, конфигурация дисков машины может измениться из-за замены жесткого диска или отказа оборудования. В таких случаях можно воссоздать необходимую конфигурацию диска таким образом, чтобы можно было восстановить образ тома точно таким, каким он был раньше, или с определенными изменениями диска или структуры томов на усмотрение пользователя.

Соблюдайте все необходимые меры предосторожности, чтобы избежать возможной потери данных.

Внимание
Все операции с дисками и томами создают определенный риск повреждения данных. Операции с системой, загрузочными томами или томами с данными должны выполняться очень аккуратно во избежание проблем с процессом загрузки или хранением данных жесткого диска.
Операции с жесткими дисками и томами занимают определенное время и в случае потери питания во время процедуры (непреднамеренного выключения машины или случайного нажатия кнопки Reset) могут привести к повреждению томов и потере данных.

Операции управления диском можно выполнить на «голом железе» на машине, которая перестала загружаться или работает не под управлением Windows. Вам понадобится загрузочный носитель, который создан в мастере создания загрузочных носителей с использованием лицензионного ключа Кибер Бэкап. Информацию о том, как создать загрузочный носитель, см. в разделах Загрузочные носители на основе Linux или Загрузочный носитель на основе Windows-PE соответственно.

Примечание
Для выполнения операций управления дисками в ОС Windows 10 и более поздних версий необходимо установить Управление Дисками.

Порядок выполнения операций управления дисками

© ООО Киберпротект, 2026

1. Выполните загрузку с загрузочного носителя Киберпротект.
2. Для работы с локальной машиной щелкните **Локальное управление этой машиной**. Для удаленных подключений см. раздел Регистрация носителя на сервере управления.
3. Щелкните **Управление дисками**.

Примечание
Операции по управлению дисками при загрузке с загрузочных носителей могут работать неправильно, если на машине настроены дисковые пространства.

11.7.4.1 Поддержка файловых систем

Загрузочный носитель поддерживает управление диском со следующими файловыми системами:

- FAT 16/32,
- NTFS.

11.7.4.2 Основные меры предосторожности

Во избежание возможного повреждения структуры тома или диска или потери данных следует принимать все необходимые меры предосторожности и следовать приведенным ниже простым рекомендациям.

1. Создайте резервную копию диска, на котором планируете создавать тома и управлять ими. Создание резервной копии самых важных данных на другом жестком диске, общем сетевом ресурсе или съемном носителе позволит работать с томами диска, не опасаясь за сохранность данных.
2. Проверьте диск, чтобы убедиться в его полной функциональности и отсутствии поврежденных секторов и ошибок файловой системы.
3. Не выполняйте операции с дисками/томами во время работы других программ, осуществляющих доступ к дискам на низком уровне.

11.7.4.3 Выбор операционной системы для управления дисками

На машине с двумя или несколькими операционными системами представление дисков и томов зависит от того, какая операционная система сейчас запущена. Один том в разных операционных системах может иметь разные буквы.

При выполнении операции управления дисками необходимо указать структуру диска, для которой будет отображаться операционная система. Для этого щелкните имя операционной системы рядом с меткой **Структура диска** и выберите нужную операционную систему в открывшемся окне.

11.7.4.4 Операции с дисками

Используя загрузочный носитель, можно выполнить следующие операции управления диском:

© ООО Киберпротект, 2026

- Инициализация диска: инициализация нового оборудования, добавленного в систему.
- Клонирование базового диска: передача всех данных с базового MBR-диска источника на целевой диск.
- Преобразование диска: MBR в GPT: преобразование таблицы разделов MBR в GPT.
- Преобразование диска: GPT в MBR: преобразование таблицы разделов GPT в MBR
- Преобразование диска: базовый в динамический: преобразование базового диска в динамический
- Преобразование диска: динамический в базовый: преобразование динамического диска в базовый.

Инициализация диска

Загрузочный носитель отображает неинициализированный диск в виде серого блока с серым значком, означающим, что диск не может использоваться системой.

Порядок инициализации диска

1. Правой кнопкой мыши щелкните нужный диск и выберите пункт **Инициализировать**.
2. В окне **Инициализация диска** задайте схему разделов диска (MBR или GPT) и тип диска (базовый или динамический).
3. После нажатия кнопки **OK** будет добавлена ожидающая операция инициализации диска.
4. Чтобы выполнить добавленную операцию, подтвердите ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.
5. После инициализации пространство диска останется нераспределенным. Чтобы использовать его, необходимо создать том на нем.

Клонирование базового диска

Располагая полнофункциональным загрузочным диском на основе Linux, можно клонировать базовые MBR-диски. Клонирование диска недоступно на готовых загрузочных носителях, которые можно скачать, или на загрузочных носителях, созданных без использования лицензионного ключа.

Клонирование базовых дисков с носителя

1. Выполните загрузку с загрузочного носителя Киберпротект.
2. Чтобы клонировать диск локальной машины, щелкните **Локальное управление этой машиной**. Для удаленных подключений см. раздел Регистрация носителя на сервере управления.
3. Щелкните **Управление дисками**.
4. Отобразятся доступные диски. Правой кнопкой мыши щелкните диск, который необходимо клонировать, и щелкните **Клонировать базовый диск**.

Примечание
Можно клонировать только полные диски. Клонирование разделов недоступно.

© ООО Киберпротект, 2026

5. Отображается список возможных целевых дисков. Программа позволяет выбрать целевой диск, если его емкость будет достаточной для хранения всех данных диска-источника без потерь. Выберите целевой диск, а затем щелкните **Далее**.

   Если целевой диск имеет больший размер, можно клонировать его "как есть" или изменить размеры томов диска-источника с соблюдением пропорций (вариант по умолчанию), чтобы не оставлять нераспределенное пространство на целевом диске.
   Если целевой диск имеет меньший размер, доступно только пропорциональное изменение размера. Если безопасное клонирование невозможно даже с использованием пропорционального изменения размера, вы не сможете продолжить операцию.

   Внимание
   Если на целевом диске есть данные, будет выведено следующее предупреждение: "*Выбран целевой диск с данными. Данные на его томах будут перезаписаны*". Если продолжить операцию, все данные, которые в данный момент содержатся на целевом диске, будут безвозвратно утрачены.

6. Выберите, нужно ли копировать NT-подпись.

   При клонировании диска, который содержит системный том, необходимо сохранить загружаемость операционной системы на томе целевого диска. Это означает, что у операционной системы должны быть данные системного тома (например, буква тома) и эти данные должны совпадать с NT-подписью, которая хранится в записи MBR-диска. Однако два диска с одинаковой NT-подписью не могут корректно работать под управлением одной операционной системы.

   При наличии двух дисков с одинаковой NT-подписью, на одном из которых находится системный том машины, при загрузке операционная система запускается с первого диска, обнаруживает такую же подпись на втором диске, затем автоматически формирует новую уникальную NT-подпись и назначает ее второму диску. В результате буквы всех томов на втором диске будут утеряны, все пути на этом диске станут недействительными и программы не смогут найти свои файлы. Операционная система на этом диске не сможет загружаться.

   Чтобы сохранить загружаемость системы на томе целевого диска, можно выбрать одно из указанных ниже действий:

   a. **Копировать NT-подпись**: укажите целевой диск с NT-подписью исходного диска, которая соответствует ключам реестра, которые также будут скопированы на целевой диск.

      Для этого установите флажок **Копировать NT-подпись**.
      Появится следующее предупреждение: *"Если на жестком диске есть операционная система, необходимо до следующего запуска машины удалить с нее диск-источник или целевой диск. В противном случае ОС будет запущена с первого из двух дисков, а ОС на втором диске станет незагружаемой.*
      Флажок **Выключите машину после завершения операции** устанавливается и снимается автоматически.

   b. **Оставить подпись NT**: для сохранения прежней подписи целевого диска и обновления операционной системы в соответствии с этой подписью.

© ООО Киберпротект, 2026

Для этого при необходимости снимите флажок **Копировать NT-подпись**.

Флажок **Выключите машину после завершения операции** снимается автоматически.

7. Щелкните **Завершить**, чтобы добавить ожидающую операцию клонирования диска.
8. В окне **Ожидающие операции** щелкните Подтвердить, а затем – **Продолжить**. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.
9. Если выбран вариант, предусматривающий копирование NT-подписи, подождите, пока выполнится операция и перезагрузится компьютер, а затем отключите жесткий диск источника или целевой жесткий диск на машине.

Преобразование диска: MBR в GPT

Преобразование базового MBR-диска в базовый GPT-диск нужно в тех случаях, когда требуется:

- более 4 основных томов на одном диске;
- дополнительная защита диска от возможных повреждений данных.

Внимание
Базовый MBR-диск, который содержит загрузочный том с текущей запущенной операционной системой, невозможно преобразовать в GPT.

Порядок преобразования базового MBR-диска в базовый GPT-диск

1. Правой кнопкой мыши щелкните диск, который необходимо клонировать, и щелкните **Преобразовать в GPT**.
2. Нажатие кнопки **OK** добавит ожидающую операцию преобразования MBR в GPT.
3. Чтобы выполнить добавленную операцию, подтвердите ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Примечание
На диске с GPT-разделами в конце области разделов выделяется место для области резервного копирования, в которой хранятся копии заголовка GPT и таблицы разделов. Если диск заполнен и размер тома невозможно уменьшить автоматически, операция преобразования MBR-диска в GPT не произойдет.
Данная операция необратима. Если на MBR-диске есть основной том и сначала диск преобразуется в GPT, а затем обратно в MBR, том станет логическим и не сможет использоваться как системный.

Преобразование динамического диска MBR в GPT

Загрузочный носитель не поддерживает прямое преобразование динамических дисков MBR в GPT. Однако можно достичь цели посредством следующих преобразований:

1. Преобразование MBR-диска из динамического в базовый с помощью операции **Преобразовать в базовый**.
2. Преобразование базовых дисков MBR в GPT с помощью операции **Преобразовать в GPT**.

© ООО Киберпротект, 2026

3. Преобразование GPT-диска из базового в динамический с помощью операции **Преобразовать в динамический**.

Преобразование диска: GPT в MBR

Если планируется установить операционную систему, которая не поддерживает GPT-диски, их можно преобразовать в MBR-диски.

Внимание
Базовый GPT-диск, который содержит загрузочный том с текущей запущенной операционной системой, невозможно преобразовать в MBR.

Порядок преобразования GPT в MBR

1. Правой кнопкой мыши щелкните диск, который необходимо клонировать, и щелкните **Преобразовать в MBR**.
2. Если нажать кнопку **OK**, будет добавлена ожидающая операция преобразования GPT в MBR.
3. Чтобы выполнить добавленную операцию, подтвердите ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Примечание
После выполнения операции тома на этом диске станут логическими. Это изменение необратимо.

Преобразование диска из базового в динамический

Необходимость преобразовать базовый диск в динамический может возникнуть, если:

- планируется использовать диск как часть группы динамических дисков;
- для хранения данных требуется более высокий уровень надежности дисков.

Порядок преобразования базового диска в динамический

1. Правой кнопкой мыши щелкните диск, который необходимо преобразовать, и щелкните **Преобразовать в динамический**.
2. Нажмите кнопку **OK**.

Преобразование будет выполнено незамедлительно, и в случае необходимости машина будет перезапущена.

© ООО Киберпротект, 2026

Примечание
Динамический диск занимает последний мегабайт физического диска для хранения базы данных, включая четырехуровневое описание (том-компонент-раздел-диск) для каждого динамического тома. Если при преобразовании базового диска в динамический окажется, что базовый диск полностью заполнен и размер его томов невозможно уменьшить автоматически, операция завершится ошибкой.
Преобразование дисков с системными томами занимает определенное время, и в случае потери питания во время процедуры (непреднамеренного выключения машины или случайного нажатия кнопки Reset) диск может стать незагружаемым.

В отличие от диспетчера дисков Windows, эта программа гарантирует загружаемость **автономной ОС** на диске после выполнения операции.

Преобразование диска из динамического в базовый

Иногда требуется преобразовать динамические диски обратно в базовые (например, чтобы использовать операционную систему, не поддерживающую динамические диски).

Порядок преобразования динамического диска в базовый

1. Правой кнопкой мыши щелкните диск, который необходимо преобразовать, затем щелкните **Преобразовать в базовый**.
2. Нажмите кнопку **OK**.

Преобразование будет выполнено незамедлительно, и в случае необходимости машина будет перезапущена.

Примечание
Эта операция недоступна для динамических дисков с томами следующих типов: составные (Spanned), чередующиеся (Striped) и RAID-5.

После преобразования последние 8 МБ дискового пространства будут зарезервированы для будущего преобразования диска из базового в динамический. В некоторых случаях возможный размер нераспределенного пространства и предлагаемый максимальный размер тома могут отличаться (например, если размер одного зеркала определяет размер другого или последние 8 МБ диска зарезервированы для будущего преобразования диска из базового в динамический).

Примечание
Преобразование дисков с системными томами занимает некоторое время, и в случае потери питания, случайного выключения машины или нажатия кнопки Reset во время процедуры диск может стать незагружаемым.

В отличие от диспетчера дисков Windows, эта программа гарантирует:

- безопасное преобразование динамического диска в базовый, если на нем содержатся тома **с данными** для простых и зеркальных томов;

© ООО Киберпротект, 2026

- в мультизагрузочных системах – загружаемость системы, которая была **отключена от сети** во время операции.

11.7.4.5 Операции с томами

Используя загрузочный носитель, можно выполнить следующие операции с томами:

- Создать том: создает новый том.
- Удалить том: удаляет выбранный том.
- Активировать: выбранный том становится активным, чтобы машина могла загружаться с помощью установленной здесь ОС.
- Изменить букву: изменяет букву выбранного тома.
- Изменить метку: изменяет метку выбранного тома
- Форматировать том: форматирует том в файловую систему определенного типа

Типы динамических томов

Простой том

Том, созданный из свободного пространства на одном физическом диске. Он может состоять из одной области на диске или из нескольких областей, виртуально объединенных диспетчером логических дисков (LDM). Он не обеспечивает ни дополнительной надежности, ни улучшения скорости, ни увеличения размера.

Составной том

Том, созданный из свободного места на диске, виртуально связанного LDM из нескольких физических дисков. В один том можно включить до 32 дисков, обойдя таким образом аппаратные ограничения размера. Но если хотя бы один диск выйдет из строя, все данные будут потеряны. При этом ни одну часть составного тома нельзя удалить, не разрушив весь том. Таким образом, составной том не обеспечивает ни дополнительной надежности, ни улучшенной скорости ввода-вывода.

Чередующийся том

Том (называемый также RAID 0), который состоит из полос данных одинакового размера, записанных через каждый диск тома. Поэтому, для создания чередующегося тома необходимо два или более динамических дисков. Диски в чередующемся томе не обязательно должны быть идентичными, но на каждом диске, который планируется включить в том, должно быть доступное неиспользуемое пространство. Размер тома будет зависеть от размера наименьшего пространства. Доступ к данным на чередующемся томе обычно осуществляется быстрее, чем доступ к тем же данным на одном физическом диске, так как ввод-вывод распределяется более чем по одному диску.

Чередующиеся тома создаются для улучшения производительности, но не надежности – они не содержат избыточной информации.

Зеркальный том

© ООО Киберпротект, 2026

Устойчивый к сбоям том, также называемый RAID 1, данные которого дублируются на два идентичных физических диска. Все данные с одного диска копируются на другой диск, обеспечивая избыточность данных. Зеркальным можно сделать почти любой том, включая системные и загрузочные тома, и, если один из дисков выйдет из строя, доступ к данным все равно можно будет получить с оставшихся дисков. К сожалению, аппаратные ограничения на размер и производительность при использовании зеркальных томов еще строже.

Зеркальный чередующийся том

Устойчивый к сбоям том, также иногда называемый RAID 1+0, сочетающий преимущества высокой скорости ввода-вывода чередующегося тома и надежность зеркального тома. Недостатком остается неотъемлемое следствие зеркальной архитектуры – низкое соотношение размера диска к размеру тома.

RAID-5

Устойчивый к сбоям диск, данные которого чередуются по всему массиву из трех или более дисков. Идентичность дисков необязательна, но на них должны быть одинакового размера блоки нераспределенного пространства, доступного на каждом диске тома. Четность (вычисляемое значение, с помощью которого можно реконструировать данные в случае сбоя) также чередуется по всему дисковому массиву и всегда хранится на другом диске отдельно от данных. В случае сбоя физического диска часть тома RAID-5, которая на нем находилась, можно воссоздать на основе оставшихся данных и четности. Том RAID-5 обеспечивает надежность и позволяет обойти ограничения размера физических дисков с более высоким соотношением размера диска к размеру тома, чем у зеркальных томов.

Создание тома

Новый том может потребоваться, чтобы:

- восстановить имеющуюся резервную копию именно в той конфигурации, которая существовала в момент копирования;
- хранить отдельно коллекции аналогичных файлов, например коллекцию MP3-файлов или видеофайлов на отдельном томе;
- хранить резервные копии (образы) других томов и дисков в специальном томе;
- установить ОС (или файл подкачки) на новом томе;
- добавить новое оборудование к машине.

Порядок создания тома

1. Правой кнопкой мыши щелкните любое нераспределенное пространство на диске, затем щелкните **Создать том**. Откроется мастер **Создание тома**.
2. Выберите тип тома. Доступны следующие параметры:
   - Базовый
   - Простой/составной
   - Чередующийся

© ООО Киберпротект, 2026

- Зеркальный
- RAID-5

Если текущая операционная система не поддерживает выбранный тип тома, будет возвращено предупреждение, а кнопка **Далее** будет отключена. Чтобы продолжить, необходимо выбрать другой тип тома.

3. Укажите нераспределенное пространство или выберите целевые диски.
   - Для основного тома укажите нераспределенное пространство на выбранном диске.
   - Для простого/составного тома выберите один или несколько целевых дисков.
   - Для зеркального тома выберите два целевых диска.
   - Для составного тома выберите два или более целевых дисков.
   - Для тома RAID-5 выберите три целевых диска

   Если создается **динамический** том и для его создания выбирается один или несколько **базовых** дисков, появится предупреждение о том, что выбранный диск будет автоматически преобразован в динамический.
4. Задание размера тома.

   Максимальное значение обычно соответствует максимально возможному объему нераспределенного пространства. В некоторых случаях предлагаемое максимальное значение может быть другим – например, если размер одного зеркала определяет размер другого или последние 8 МБ диска зарезервированы для будущего преобразования диска из базового в динамический.

   Можно выбрать расположение нового основного тома на диске, если объем нераспределенного пространства на этом диске превышает объем тома.
5. Настройка параметров тома.

   Можно задать **букву** тома (по умолчанию это будет первая свободная буква алфавита), а при необходимости и **метку** (по умолчанию метка не назначается). Кроме того, необходимо указать **файловую систему** и **размер кластера**.

   Возможные варианты типа файловой системы:
   - FAT16 (недоступен, если размер тома превышает 2 ГБ);
   - FAT32 (недоступен, если размер тома превышает 2 ТБ);
   - NTFS
   - Оставить том неформатированным.

   Задавая размер кластера, можно выбрать любое из предустановленных значений для каждой файловой системы. Размер кластера, который предлагается по умолчанию, наилучшим образом соответствует тому с выбранной файловой системой. Если задать размер кластера 64 КБ для FAT16/FAT32 или 8-64 КБ для NTFS, Windows сможет подключить том, но некоторые программы (например, программы установки) могут неправильно вычислить пространство на диске.

   Если создается основной том, который можно сделать системным, можно будет выбрать тип тома – **Основной** (**Активный основной**) или **Логический**. Обычно для установки операционной

© ООО Киберпротект, 2026

системы на том выбирается тип **Основной**. Выберите **Активный** (значение по умолчанию), если нужно установить на этом томе операционную систему для загрузки при запуске машины. Если кнопка **Основной** не нажата, параметр **Активный** будет отключен. Если том предполагается использовать для хранения данных, выберите тип **Логический**.

Примечание
На базовом диске может быть до четырех основных томов. Если они уже существуют, необходимо будет преобразовать диск в динамический. В противном случае параметры **Активный** и **Основной** будут отключены, и можно будет выбрать только тип тома **Логический**.

6. В окне **Ожидающие операции** щелкните **Подтвердить**, а затем – **Продолжить**. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Удаление тома

Порядок удаления тома

1. Правой кнопкой мыши щелкните том, который необходимо удалить.
2. Щелкните **Удалить том**.

Примечание
Вся информация об этом томе будет утрачена без возможности восстановления.

3. После нажатия кнопки **OK** будет добавлена ожидающая операция удаления тома.
4. Чтобы выполнить добавленную операцию, подтвердите ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Когда том удаляется, освобожденное пространство добавляется к нераспределенному дисковому пространству, Можно использовать его для создания нового тома или для изменения типа другого тома.

Активный том

Если основных томов несколько, необходимо указать один из них в качестве загрузочного. Для этого необходимо сделать том активным. Диск может иметь только один активный том.

Порядок установки тома как активного

1. Правой кнопкой мыши щелкните нужный основной том на основном MBR-диске, а затем щелкните **Пометить активным**.

   Если в системе нет других активных томов, будет добавлена ожидающая операция указания активного тома. Если в системе есть еще один активный том, появится предупреждение о том, что сначала нужно перевести прежний активный том в пассивное состояние.

© ООО Киберпротект, 2026

Примечание
Когда появляется новый активный том, буква прежнего активного тома может измениться и некоторые из установленных программ могут перестать работать.

2. После нажатия кнопки **OK** в очередь будет добавлена операция установки активного тома.

Примечание
Даже если в новом активном томе есть операционная система, в некоторых случаях будет невозможно загрузить машины с него. Необходимо подтвердить, что вы хотите сделать том активным.

3. Чтобы выполнить добавленную операцию, подтвердите ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Изменение буквы тома

При загрузке операционная система Windows назначает буквы (C:, D: и т. д.) томам жестких дисков. Эти буквы используются приложениями и операционными системами для поиска файлов и папок в томах. Подключение дополнительного диска, а также создание и удаление тома на существующем диске может привести к изменению конфигурации системы. В результате некоторые приложения могут начать работать неправильно, а пользовательские файлы нельзя будет автоматически найти и открыть. Чтобы этого избежать, можно вручную изменить буквы томов, назначенные автоматически операционной системой.

Порядок изменения буквы тома, назначенной операционной системой

1. Правой кнопкой мыши щелкните нужный том и выберите пункт **Изменить букву**.
2. В окне **Изменить букву** выберите новую букву.
3. После нажатия кнопки **OK** будет добавлена ожидающая операция назначения буквы тома.
4. Чтобы выполнить добавленную операцию, подтвердите ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Изменение метки тома

Метка тома необязательна. Метка тома – это имя, которое присваивается тому для простоты опознания.

Порядок изменения метки тома

1. Правой кнопкой мыши щелкните нужный том и выберите пункт **Изменить метку**.
2. Введите новую метку в текстовом поле окна **Изменить метку** .
3. После нажатия кнопки **OK** будет добавлена ожидающая операция изменения метки тома.
4. Чтобы выполнить добавленную операцию, подтвердите ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

© ООО Киберпротект, 2026

Форматирование тома

Форматирование тома может потребоваться, если вы хотите изменить файловую систему тома в следующих целях:

- для экономии дополнительного пространства, которое иначе теряется из-за размеров кластеров в файловых системах FAT16 и FAT32;
- для быстрого и более или менее надежного способа уничтожения данных, содержащихся в этом томе.

Порядок форматирования тома

1. Правой кнопкой мыши щелкните нужный том и выберите пункт **Формат**.
2. Выберите размер кластера и файловую систему. Возможные варианты типа файловой системы:
   - FAT16 (недоступен, если размер тома превышает 2 ГБ);
   - FAT32 (недоступен, если размер тома превышает 2 ТБ);
   - NTFS.
3. После нажатия кнопки **OK** будет добавлена ожидающая операция форматирования тома.
4. Чтобы выполнить добавленную операцию, подтвердите ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

11.7.4.6 Ожидающие операции

Все операции считаются ожидающими, пока вы не введете и не подтвердите команду **Подтвердить**. Таким образом вы можете контролировать все запланированные операции, проверять все назначенные изменения, а при необходимости и отменять любые операции до их исполнения (при необходимости).

В представлении **Управление дисками** содержится панель инструментов со значками для запуска таких действий, как **Отменить**, **Вернуть** и **Подтвердить** для ожидающих операций. Эти действия можно также выполнить в меню **Управление дисками**.

Все запланированные операции добавляются к списку ожидающих операций.

Действие **Отменить** позволяет отменить последнюю операцию в списке. Это действие доступно для непустого списка.

Действие **Вернуть** позволяет восстановить последнюю ожидающую операцию, которая была отменена.

Действие **Подтвердить** позволяет перейти в окно **Ожидающие операции**, где можно просмотреть список ожидающих операций.

Чтобы выполнить их, щелкните **Приступить**.

© ООО Киберпротект, 2026

Примечание
После выбора операции **Приступить** отменить какое-либо действие или операцию невозможно.

Чтобы не подтверждать операцию, щелкните **Отмена**. После отмены никакие изменения в список ожидающих операций не вносятся. Если выйти из программы, не подтвердив операции, ожидающие выполнения, эти операции будут отменены.

11.8 Настройка устройств iSCSI

В этом разделе описана настройка устройств iSCSI при работе с загрузочного носителя. После выполнения описанных ниже этапов можно использовать эти устройства так, как если бы они были подключены локально к машине, загружаемой с помощью загрузочного носителя.

Целевой сервер iSCSI (или **целевой портал**) – это сервер, на котором находится устройство iSCSI. **Целевое устройство iSCSI** – это компонент на целевом сервере; этот компонент обеспечивает совместное использование устройства и составляет список инициаторов iSCSI, которым разрешен доступ к устройству. **Инициатор iSCSI** – это компонент на машине; этот компонент обеспечивает взаимодействие между машиной и целевым устройством iSCSI. При настройке доступа к устройству iSCSI на машине, загруженной с помощью загрузочного носителя, необходимо указать целевой портал iSCSI устройства, а также один из инициаторов iSCSI, перечисленный на целевом устройстве. Если в целевом объекте предоставлен общий доступ к нескольким устройствам, вы получите доступ ко всем ним.

Для добавления устройства iSCSI на загрузочный носитель на основе Linux

1. Нажмите **Инструменты** > **Настроить устройства iSCSI/NDAS**.
2. Нажмите кнопку **Добавить хост**.
3. Укажите IP-адрес и порт портала целевого устройства iSCSI, а также имя любого инициатора iSCSI, который разрешил доступ к устройству.
4. Если хост требует проверки подлинности, укажите имя пользователя и пароль.
5. Нажмите кнопку **OK**.
6. Выберите целевое устройство iSCSI в списке и нажмите кнопку **Подключиться**.
7. Если в настройках целевого устройства iSCSI включена проверка подлинности CHAP, поступит запрос на учетные данные для доступа к целевому устройству iSCSI. Укажите имя пользователя и секрет целевого устройства, которые указаны в настройках целевого устройства iSCSI. Нажмите кнопку **OK**.
8. Нажмите кнопку **Закрыть**, чтобы закрыть окно.

Для добавления устройства iSCSI на загрузочный носитель на основе PE

1. Нажмите **Инструменты** > **Запустить установку iSCSI**.
2. Выберите вкладку **Обнаружение**.

© ООО Киберпротект, 2026

3. Под пунктом **Целевые порталы** нажмите кнопку **Добавить**, а затем укажите IP-адрес и порт портала целевого устройства iSCSI. Нажмите кнопку **OK**.
4. Откройте вкладку **Общие**, нажмите кнопку **Изменить**, а затем укажите имя инициатора iSCSI, который разрешил доступ к устройству.
5. Откройте вкладку **Цели**, нажмите кнопку **Обновить**, выберите целевое устройство iSCSI в списке, а затем нажмите кнопку **Подключить**. Нажмите кнопку **OK**, чтобы подключиться к целевому устройству iSCSI.
6. Если в настройках целевого устройства iSCSI включена проверка подлинности CHAP, отобразится ошибка **Сбой аутентификации**. В этом случае щелкните **Подключиться**, затем щелкните **Дополнительно**, установите флажок **Включить вход CHAP** и укажите имя пользователя и секрет целевого устройства, которые указаны в настройках целевого устройства iSCSI. Нажмите кнопку **OK**, чтобы закрыть окно, затем нажмите кнопку **OK**, чтобы подключиться к целевому устройству iSCSI.
7. Нажмите кнопку **OK**, чтобы закрыть окно.

11.9 Диспетчер восстановления при загрузке (Startup Recovery Manager)

Диспетчер восстановления при загрузке — это загрузочный компонент, находящийся на системном диске Windows или в разделе /boot Linux и настроенный на запуск во время загрузки системы при нажатии клавиши F11. При его использовании не требуется отдельный носитель или сетевое подключение для запуска загрузочной утилиты аварийного восстановления.

Диспетчер восстановления при загрузке особенно полезен для мобильных пользователей. В случае сбоя перезагрузите машину, дождитесь появления запроса «Press F11 for Startup Recovery Manager...» и нажмите клавишу F11. Программа запустится, и можно будет выполнить восстановление.

Кроме того, с помощью Диспетчера можно «на ходу» выполнять резервное копирование.

Некоторые производители оборудования резервируют за клавишей F11 при включении или перезагрузке компьютера загрузку других компонентов, например, старт загрузочного меню. В этом случае сначала выберите в меню соответствующий пункт (например, **Киберпротект Loader**). Далее последует старт загрузчика Киберпротект, и на экране появится подсказка; после этого нажмите вновь F11 для запуска Диспетчера.

На машинах с установленным загрузчиком GRUB пользователь не нажимает клавишу F11, а выбирает **Startup Recovery Manager** в меню загрузки.

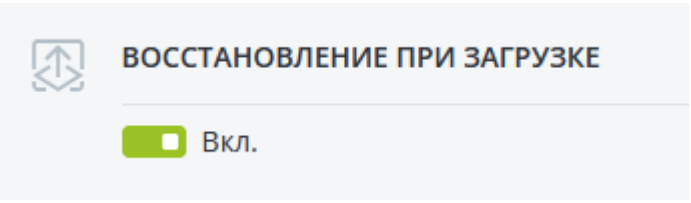
11.9.1 Активация Диспетчера восстановления при загрузке

На машине, где запущен агент для Windows или агент для Linux, Диспетчер восстановления при загрузке можно активировать с помощью веб-консоли Кибер Бэкап.

Порядок активации Диспетчера восстановления при загрузке на веб-консоли Кибер Бэкап

© ООО Киберпротект, 2026

1. Выберите машину, на которой нужно активировать Диспетчер восстановления при загрузке.
2. Нажмите **Сведения**.
3. Включите переключатель **Восстановление при загрузке**.



4. Дождитесь окончания активации.

Порядок активации Диспетчера восстановления при загрузке на машине без агента

1. Загрузите машину с загрузочного носителя.
2. Щелкните **Инструменты** > **Активировать Восстановление при загрузке**.
3. Дождитесь окончания активации.

11.9.2 Что происходит при активации Диспетчера восстановления при загрузке

Активация включает при загрузке подсказку «Press F11 for Startup Recovery Manager...» (при отсутствии загрузчика GRUB) или добавляет пункт **Startup Recovery Manager** в меню загрузчика GRUB (при его наличии).

В некоторых случаях при нажатии клавиши F11 используется встроенный в оборудование загрузчик меню. Тогда дождитесь старта встроенного загрузчика, в его меню выберите пункт с загрузчиком Киберпротект. В процессе старта с загрузчика Киберпротект при нажатии клавиши F11 активируется загрузка Диспетчера.

Примечание
Для активации Диспетчера восстановления при загрузке системный диск (или раздел /boot в Linux) должен иметь по крайней мере 100 МБ свободного пространства.

За исключением случая, когда используется загрузчик GRUB и он установлен в основную загрузочную запись (MBR), активация Диспетчера восстановления при загрузке перезаписывает основную загрузочную запись (MBR) своим собственным загрузочным кодом. Таким образом, при использовании загрузчиков сторонних производителей может потребоваться их повторное активирование.

В ОС Linux при использовании загрузчика, отличного от GRUB (такого как LILO), возможна его установка в загрузочную запись корневого (или загрузочного) раздела Linux вместо MBR до активации Диспетчера восстановления при загрузке. В противном случае измените конфигурацию этого загрузчика вручную после активации.

© ООО Киберпротект, 2026

11.9.3 Деактивация Диспетчера восстановления при загрузке

Деактивация выполняется аналогично активации.

Деактивация отключает подсказку «Press F11 for Startup Recovery Manager...» при загрузке (или пункт меню в GRUB).

Если **Восстановление при загрузке** не активировано, для восстановления системы, которая не смогла загрузиться, требуется выполнить одно из следующих действий:

- загрузить машину с отдельного загрузочного носителя;
- использовать сеть, чтобы загрузиться с PXE-сервера или службы удаленной установки Microsoft (RIS).

11.10 PXE-сервер Киберпротект

PXE-сервер Киберпротект служит для загрузки машин в загрузочные компоненты Киберпротект через сеть.

Загрузка по сети:

- устраняет потребность в специалисте для установки загрузочного носителя в систему, которая должна быть загружена;
- при групповых операциях снижает количество времени, требуемого для загрузки нескольких машин, по сравнению с использованием физического загрузочного носителя.

Загрузочные компоненты загружаются на PXE-сервер Киберпротект при помощи мастера создания загрузочных носителей Киберпротект. Чтобы загрузить загрузочные компоненты, запустите мастер создания загрузочных носителей и следуйте пошаговым инструкциям, описанным в разделе «Загрузочные носители на основе Linux».

Загрузка нескольких машин с PXE-сервера Киберпротект имеет смысл, если в сети присутствует DHCP-сервер. При этом сетевые интерфейсы загруженных машин автоматически получат IP-адреса.

11.10.1 Установка PXE-сервера

Примечание
PXE-сервер может быть установлен только на машине с ОС Windows.

Порядок установки PXE-сервера

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.

© ООО Киберпротект, 2026

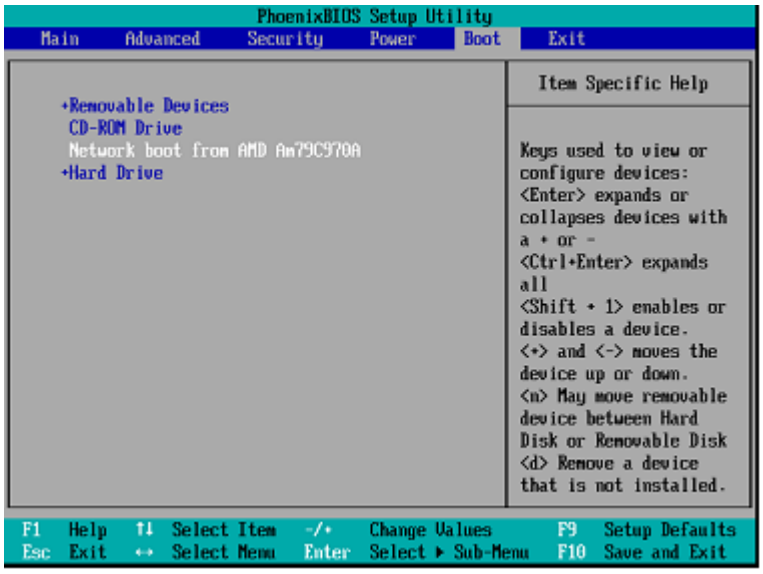
4. Щёлкните **Настройка параметров установки**.
5. Рядом с пунктом **Устанавливаемые компоненты** щёлкните **Изменить**.
6. Установите флажок **PXE-сервер**. Если на этой машине не нужно устанавливать другие компоненты, снимите соответствующие флажки. Чтобы продолжить, нажмите кнопку **Готово**.
7. [Необязательно] Измените другие настройки установки.
8. Нажмите **Установка**, чтобы продолжить установку.
9. После завершения установки нажмите кнопку **Закрыть**.

PXE-сервер Киберпротект запускается в виде службы сразу же после установки. Позже он автоматически стартует при каждом запуске операционной системы. Остановить или запустить PXE-сервер можно так же, как службу Windows.

11.10.2 Настройка машины на загрузку с PXE

В случае «голого железа» достаточно, чтобы система BIOS машины поддерживала сетевую загрузку.

На тех машинах, операционная система которых расположена на жестком диске, система BIOS должна быть настроена так, чтобы сетевая интерфейсная плата была первым загрузочным устройством либо чтобы она предшествовала жесткому диску в приоритете загрузки. На следующем примере показана одна из приемлемых конфигураций BIOS. Если в машину не вставлен загрузочный носитель, будет производиться загрузка по сети.



В некоторых версиях BIOS необходимо сохранить изменения BIOS после включения сетевой интерфейсной платы, чтобы плата появилась в списке загрузочных устройств.

Если установлено несколько сетевых интерфейсных плат, убедитесь, что к плате, поддерживаемой BIOS, подключен сетевой кабель.

© ООО Киберпротект, 2026

11.10.3 Работа в подсетях

Чтобы Киберпротект PXE-сервер мог работать в другой подсети (подключенной через коммутатор), необходимо настроить коммутатор для передачи трафика PXE. IP-адреса PXE-сервера настраиваются отдельно для каждого интерфейса с помощью вспомогательной службы IP таким же способом, как адреса DHCP-сервера. Дополнительные сведения см. на странице https://support.microsoft.com/en-us/help/257579/pxe-clients-do-not-receive-an-ip-address-from-a-dhcp-server.

© ООО Киберпротект, 2026

12 Защита приложений, сервисов, баз данных

В разделе описаны способы резервного копирования и восстановления данных различных приложений, сервисов и баз данных.

12.1 Защита приложений Microsoft

12.1.1 Защита Microsoft SQL Server и Microsoft Exchange Server

Есть два метода для защиты этих приложений:

- **Резервная копия базы данных**

  Это резервное копирование на уровне файлов базы данных и метаданных, связанных с ней. Базы данных можно восстановить в запущенное приложение или как файлы.
- **Резервное копирование с поддержкой приложений**

  Это резервное копирование на уровне дисков, при котором также выполняется сбор метаданных приложений. Эти метаданные позволяют выполнить обзор и восстановление данных приложений, не восстанавливая весь диск или том. Диск или том также можно восстановить полностью. Это означает, что можно использовать единое решение и один план защиты как для аварийного восстановления, так и для защиты данных.

Для Microsoft Exchange Server вы можете выбрать **Резервное копирование почтового ящика**. При выборе данной опции будут созданы резервные копии отдельных почтовых ящиков посредством протокола Exchange Web Services. Почтовые ящики или элементы почтового ящика могут быть восстановлены на запущенный Exchange Server. Резервное копирование почтовых ящиков поддерживается для Microsoft Exchange Server 2013 и более поздних версий.

12.1.2 Защита Microsoft SharePoint

Ферма Microsoft SharePoint состоит из серверов веб-интерфейса, на которых выполняются службы SharePoint, серверов баз данных, на которых выполняется Microsoft SQL Server и (необязательно) серверов приложений, которые разгружают серверы веб-интерфейса от некоторых служб SharePoint. Некоторые серверы веб-интерфейса и серверы приложений могут быть идентичны друг другу.

Чтобы защитить всю ферму SharePoint, выполните указанные ниже действия:

- Создайте резервные копии серверов базы данных, выполнив резервное копирование с поддержкой приложений.
- Создайте резервные копии всех уникальных серверов веб-интерфейса и серверов приложений, выполнив обычное резервное копирование на уровне дисков.

Резервные копии всех серверов должны быть выполнены по одному расписанию.

Чтобы защитить только содержимое, можно создать резервные копии баз данных по отдельности.

© ООО Киберпротект, 2026

12.1.3 Защита контроллера домена

Машину под управлением доменных служб Active Directory можно защитить резервным копированием с поддержкой приложений. Если домен содержит несколько контроллеров домена, то при восстановлении одного из них выполняется непринудительное восстановление; при этом откат USN не выполняется после восстановления.

12.1.4 Восстановление приложений

В таблице приведена сводка доступных методов восстановления приложений.

	Из резервной копии базы данных	**Из резервной копии с поддержкой приложений**	**Из резервной копии диска**
Microsoft SQL Server	Базы данных в запущенный экземпляр SQL Server Базы данных как файлы	Вся машина Базы данных в запущенный экземпляр SQL Server Базы данных как файлы	Вся машина
Microsoft Exchange Server	Базы данных в запущенный Exchange Базы данных как файлы Фрагментарное восстановление в запущенный Exchange*	Вся машина Базы данных в запущенный Exchange Базы данных как файлы Фрагментарное восстановление в запущенный Exchange*	Вся машина
Серверы базы данных Microsoft SharePoint	Базы данных в запущенный экземпляр SQL Server Базы данных как файлы Фрагментарное восстановление с использованием SharePoint Explorer	Вся машина Базы данных в запущенный экземпляр SQL Server Базы данных как файлы Фрагментарное восстановление с использованием SharePoint Explorer	Вся машина
Интерфейсные веб-серверы Microsoft SharePoint	-	-	Вся машина
Доменные службы Active Directory	-	Вся машина	-

© ООО Киберпротект, 2026

* Фрагментарное восстановление также доступно из резервной копии почтового ящика.

12.1.5 Предварительные требования

Перед настройкой резервного копирования приложений убедитесь, что перечисленные ниже требования выполнены.

Чтобы проверить состояние модуля записи VSS, используйте команду vssadmin list writers.

12.1.5.1 Общие требования

Для Microsoft SQL Server убедитесь, что выполнены указанные ниже требования:

- Запущен хотя бы один экземпляр Microsoft SQL Server.
- Модуль записи SQL для VSS включен.

Для Microsoft Exchange Server убедитесь, что выполнены указанные ниже требования:

- Запущена служба банка данных Microsoft Exchange.
- Установлена оболочка Windows PowerShell версии 2.0 или новее.
- Установлена платформа Microsoft .NET Framework версии 3.5 или новее.
- Модуль записи Exchange для VSS включен.

Примечание
Для работы агента для Exchange требуется временное хранилище данных. По умолчанию временные файлы находятся в папке %ProgramData%\Acronis\Temp. Убедитесь, что объем свободного пространства на томе, где расположена папка %ProgramData%, составляет как минимум 15 % от размера базы данных Exchange. Как вариант, можно изменить расположение временных файлов перед созданием резервных копий Exchange.

На контроллере домена убедитесь, что:

- Модуль записи Active Directory для VSS включен.

При создании плана защиты убедитесь в следующем:

- Для физических машин включен параметр резервного копирования Служба теневого копирования томов (VSS).
- Для виртуальных машин включен параметр резервного копирования Служба теневого копирования томов (VSS) для виртуальных машин.

12.1.5.2 Дополнительные требования для операций резервного копирования с поддержкой приложений

При создании плана защиты убедитесь, что для резервного копирования выбран параметр **Вся машина**. В плане защиты необходимо отключить параметр резервного копирования **Sector-by-sector (Посекторно)**; в противном случае невозможно будет восстановить данные приложения из

© ООО Киберпротект, 2026

таких резервных копий. Если данный план выполнен в режиме **Sector-by-sector (Посекторно)** из-за автоматического перехода в этот режим, то и в этом случае восстановить данные приложения будет невозможно.

Требования для виртуальных машин ESXi

Если приложение выполняется на виртуальной машине, резервная копия которой создана агентом для VMware, убедитесь, что выполнены следующие условия:

- Виртуальная машина для резервного копирования соответствует требованиям совместимого с приложениями резервного копирования и восстановления, которые перечислены в статье «Windows Backup Implementations (Реализации резервного копирования Windows)» из документации к VMware: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html.
- На машине установлен и обновлен набор утилит VMware Tools.
- Учетные записи пользователей (UAC) отключены на машине. Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).

Требования для виртуальных машин Hyper-V

Если приложение выполняется на виртуальной машине, резервная копия которой создана агентом для Hyper-V, убедитесь, что выполнены следующие условия:

- В качестве гостевой операционной системы используется Windows Server.
- Виртуальная машина не имеет динамических дисков.
- Между хостом Hyper-V и гостевой операционной системой установлено сетевое подключение. Это необходимо для выполнения удаленных запросов WMI в виртуальной машине.
- Учетные записи пользователей (UAC) отключены на машине. Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).
- Конфигурация виртуальной машины соответствует следующем критерию:
  - Службы интеграции Hyper-V установлены и обновлены. Должно быть установлено критическое обновление, доступное по ссылке https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - В настройках виртуальной машины включен параметр **Управление** > **Службы интеграции** > **Резервное копирование (контрольная точка тома)**.
  - Для Hyper-V 2012 R2 и более поздних версий: виртуальная машина не имеет контрольных точек.
  - Для Hyper-V 2012 R2 и более поздних версий: виртуальная машина имеет контроллер SCSI (проверьте **Настройки** > **Оборудования**).

© ООО Киберпротект, 2026

12.1.6 Резервное копирование баз данных Microsoft SQL Server и Microsoft Exchange Server

Прежде чем приступить к созданию резервных копий баз данных, убедитесь, что выполнены требования, перечисленные в разделе "Предварительные требования".

Выберите базы данных, как указано ниже, а затем укажите другие настройки плана защиты как требуется.

12.1.6.1 Выбор баз данных Microsoft SQL Server

Резервная копия базы данных Microsoft SQL Server содержит файлы базы (.mdf, .ndf), журналы (.ldf) и другие связанные файлы. Их резервные копии создаются с помощью службы SQL Writer. Она должна быть запущена в момент, когда служба теневого копирования томов (VSS) отправляет запрос на резервное копирование или восстановление.

После каждого успешного резервного копирования выполняется сокращение журналов транзакций Microsoft SQL Server. Усечение журнала Microsoft SQL Server можно отключить в параметрах плана защиты.

Порядок выбора баз данных Microsoft SQL Server

1. Нажмите **Устройства** > **Microsoft SQL**.

   Программное обеспечение отобразит дерево групп Always On Availability Groups (AAG) сервера Microsoft SQL Server, машины, на которых запущен Microsoft SQL Server, экземпляры SQL Server и базы данных.
2. Перейдите к данным, для которых требуется создать резервные копии.

   Разверните узлы дерева или дважды щелкните элементы списка, расположенного справа от дерева.
3. Выберите данные, резервную копию которых необходимо создать. Выберите AAG, машины, на которых запущен Microsoft SQL Server, экземпляры SQL Server или отдельные базы данных.
   - При выборе AAG, для всех баз данных, включенных в выбранную AAG, будет создана резервная копия. Дополнительные сведения о резервном копировании групп AAG или отдельных баз данных AAG см. в разделе Защита групп Always On Availability Groups (AAG).
   - При выборе машины, на которой запущен Microsoft SQL Server, будет создана резервная копия всех баз данных, подключенных к экземпляру SQL Server.
   - При выборе экземпляра SQL Server, для всех баз данных, подключенных к выбранному экземпляру, будет создана резервная копия.
   - Если выбрать отдельные базы, будут созданы резервные копии только для них.
4. Нажмите кнопку **Резервное копирование**. Если потребуется, введите учетные данные для доступа к Microsoft SQL Server. Соответствующая учетная запись должна входить в группу **Операторы архива** или **Администраторы** на этой машине, а также иметь роль **системный администратор** в каждом из экземпляров, для которых создается резервная копия.

© ООО Киберпротект, 2026

12.1.6.2 Выбор данных Microsoft Exchange Server

В таблице ниже приведены основные сведения о том, какие именно данные Exchange можно выбрать для резервного копирования.

Версия Exchange	Элементы данных
2013/2016/2019	Базы данных, группы обеспечения доступности баз данных (DAG)

При полном резервном копировании в копию включаются все выбранные данные Exchange.

Инкрементная резервная копия содержит измененные блоки файлов баз данных, файлы контрольных точек, а также небольшое количество файлов журналов, более новых по отношению к соответствующим контрольным точкам базы. Поскольку в резервную копию включаются изменения, внесенные в базу данных, добавлять в нее все записи из журналов транзакций с момента предыдущего резервного копирования не нужно. После восстановления воспроизводится только журнал, более новый, чем контрольная точка. Это позволяет ускорить восстановление и обеспечить резервное копирование базы, даже если включено циклическое ведение журнала.

После каждого успешного резервного копирования выполняется усечение файлов журнала транзакций.

Порядок выбора данных Exchange

1. Нажмите **Устройства** > **Microsoft Exchange**.

   Программное обеспечение отобразит дерево групп обеспечения доступности баз данных (DAG) Exchange, машины, на которых запущен Exchange, и базы данных Exchange. Если агент для Exchange настроен, как описано в разделе «Резервное копирование почтовых ящиков», в этом дереве также отображаются почтовые ящики.
2. Перейдите к данным, для которых требуется создать резервные копии.

   Разверните узлы дерева или дважды щелкните элементы списка, расположенного справа от дерева.
3. Выберите данные, резервную копию которых необходимо создать.
   - При выборе DAG создаются резервные копии одной из копий каждой кластеризованной базы данных. Дополнительные сведения о резервном копировании групп DAG см. в разделе «Защита групп обеспечения доступности базы данных (DAG)».
   - При выборе машины, на которой запущен сервер Exchange, будет создана резервная копия всех баз данных, подключенных к серверу.
   - Если выбрать отдельные базы, будут созданы резервные копии только для них.
   - Если агент для Exchange настроен, как описано в разделе «Резервное копирование почтовых ящиков», можно выбрать почтовые ящики для резервного копирования.
4. Если потребуется, введите учетные данные для доступа к информации.
5. Щелкните **Защитить**.

© ООО Киберпротект, 2026

12.1.6.3 Защита группы Always On Availability Groups (AAG)

Обзор решений высокой доступности для Microsoft SQL Server

Функция отказоустойчивой кластеризации Windows Server (WSFC) позволяет настроить Microsoft SQL Server с высоким уровнем доступности посредством избыточности на уровне экземпляра (экземпляр отказоустойчивого кластера, FCI) или на уровне базы данных (Always On Availability Group, AAG). Оба метода можно сочетать.

В экземпляре отказоустойчивого кластера базы данных Microsoft SQL Server расположены в общем хранилище. Доступ к этому хранилищу возможен только с активного узла кластера. При сбое активного узла происходит переход, и активным становится другой узел.

В группе обеспечения доступности все реплики баз данных располагаются на разных узлах. Если основная реплика становится недоступна, основная роль назначается дополнительной реплике, расположенной на другом узле.

Таким образом, уже сами кластеры являются решением по аварийному восстановлению. Однако в некоторых случаях кластеры не могут обеспечить защиту данных: например, при логическом повреждении базы данных, отсутствии копии или реплики какой-то базы данных в кластере или отказе всего кластера.

Поддерживаемые конфигурации кластеров

Это программное обеспечение поддерживает *только* группы обеспечения доступности Always On SQL Server (AAG) для SQL Server 2012 или более поздних версий. Прочие конфигурации кластеров, такие как, например, Failover Cluster Instances, зеркальное отображение базы данных и доставка журналов, *не* поддерживаются.

Сколько требуется агентов для резервного копирования и восстановления данных кластера?

Для успешного резервного копирования и восстановления данных кластера необходимо установить агент для Microsoft SQL Server на каждом узле кластера WSFC.

В AAG включено резервное копирование баз данных

1. Установите агент для Microsoft SQL Server на каждый узел кластера WSFC.

   Примечание
   После установки агента на одном из узлов программное обеспечение отобразит AAG и ее узлы в поле **Устройства** > **Microsoft SQL** > **Базы данных**. Для установки агента для Microsoft SQL Server на остальных узлах выберите AAG, нажмите **Сведения**, после чего нажмите **Установить агент** возле каждого узла.

© ООО Киберпротект, 2026

2. Выберите AAG или набор баз данных для создания резервной копии в соответствии с инструкциями "Выбор баз данных Microsoft SQL Server" (стр. 479).

   Чтобы создать резервную копию всех баз данных AAG, необходимо выбрать саму AAG. Чтобы создать резервную копию набора баз данных, определите этот набор во всех узлах AAG.

   Предупреждение
   Набор баз данных должен быть одним на всех узлах. Если хотя бы один набор будет отличаться от всех остальных или будет определен не на всех узлах, резервное копирование кластера будет работать неправильно.

3. Настройте параметр резервного копирования «Способ резервного копирования кластера».

Восстановление баз данных, включенных в AAG

1. Выберите базы данных, которые необходимо восстановить, а затем выберите желаемую точку восстановления данных.

   При переходе **Устройства** > **Microsoft SQL** > **Базы данных**, выборе кластеризованной базы данных и нажатии **Восстановить**, программное обеспечение отобразит только те точки восстановления, которые соответствуют временам создания резервной копии выбранной копии базы данных.

   Самый легкий способ просмотра всех точек восстановления кластеризованной базы данных – выбор резервной копии всей AAG на вкладке "Хранилища резервных копий". Имена резервных копий AAG помечены особым значком и составляются по следующему шаблону: <имя AAG> - <имя плана защиты>.
2. Для конфигурирования восстановления выполните действия, описанные в разделе "Восстановление баз данных Microsoft SQL Server" (стр. 488) (начиная с шага 5).

   Программное обеспечение автоматически определяет узел кластера, на который будут восстановлены данные. Имя узла отображается в поле **Восстановить на**. Вы можете вручную изменить целевой узел.

   Внимание
   База данных, включенная в группу Always On Availability Group, не может быть перезаписана во время восстановления, поскольку это запрещено правилами Microsoft SQL Server. Необходимо восстановить базу данных как новую, не входящую в AAG. После завершения восстановления можно воссоздать исходную конфигурацию AAG.

Рекомендуется следующая последовательность действий, чтобы восстановить базу данных, входящую в AAG:

1. Восстановить базу данных как новую (то есть под другим именем и в отдельную пустую папку).
2. Проверить восстановленную базу данных средствами SQL Server Management Studio.
3. Удалить старую базу данных.

© ООО Киберпротект, 2026

4. Переименовать восстановленную базу данных.
5. Добавить восстановленную базу данных в AAG.

12.1.6.4 Защита групп обеспечения доступности базы данных (DAG)

Обзор кластеров Exchange

Основная идея кластеров Exchange – обеспечить высокую доступность базы данных с быстрым переходом к реплике и без потери данных. Обычно для этого одна или несколько копий баз данных находятся на элементах (узлах) кластера. В случае отказа узла кластера, на котором находится активная копия базы данных, или самой активной копии базы данных, другой узел кластера, содержащий пассивную копию, автоматически берет на себя операции с отказавшего узла и предоставляет доступ к службам Exchange с минимальным простоем. Таким образом, уже сами кластеры являются решением по аварийному восстановлению.

Однако в некоторых случаях решение с использованием отказоустойчивых кластеров не может обеспечить защиту данных: например, при логическом повреждении базы данных, отсутствии копии или реплики какой-то базы данных в кластере или отказе всего кластера.

Резервное копирование с поддержкой кластеров

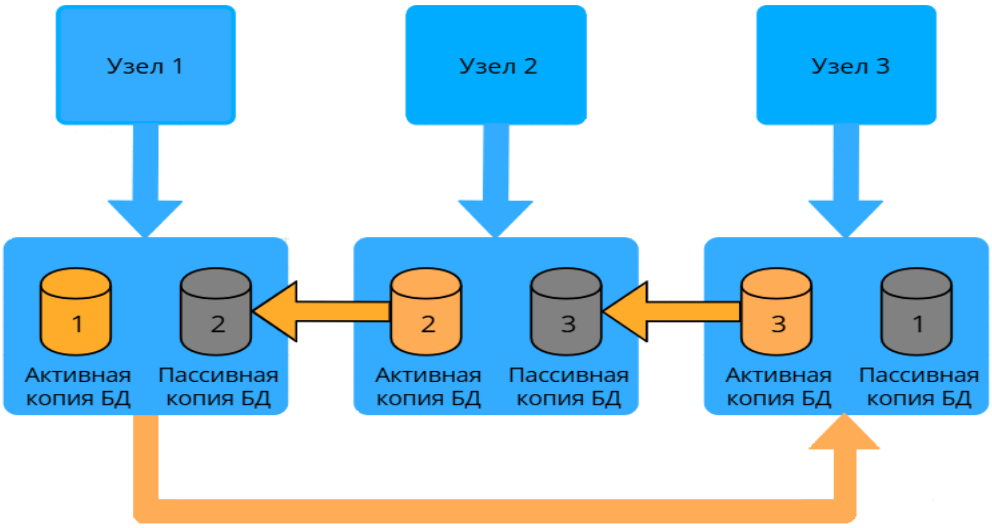
Используя резервное копирование с поддержкой кластеров, вы создаете только одну копию кластеризированных данных. Если данные меняют свое расположение в кластере (например, из-за переключения или перехода к реплике), программное обеспечение отслеживает все перемещения этих данных и благополучно создает их резервную копию.

Поддерживаемые конфигурации кластеров

Резервное копирование с поддержкой кластеров поддерживается *только* для группы обеспечения доступности баз данных (DAG) в Microsoft Exchange Server 2013 или более поздних версиях. При этом поддерживаются базы данных с включенной функцией MetaCache Database (MCDB), в том числе гранулярное восстановление писем из таких баз данных.

Группа DAG включает до 16 серверов почтовых ящиков Exchange. На любом узле может располагаться копия базы данных почтовых ящиков с любого другого узла. Каждый узел может содержать пассивные и активные копии базы данных. Может быть создано до 16 копий каждой базы данных.

© ООО Киберпротект, 2026



Сколько требуется агентов для резервного копирования и восстановления данных кластера?

Для успешного резервного копирования и восстановления кластеризованных баз данных необходимо установить агент для Exchange на каждом узле кластера Exchange.

Примечание

После установки агента на одном из узлов веб-консоль Кибер Бэкап отобразит DAG и ее узлы в поле **Устройства** > **Microsoft Exchange** > **Базы данных**. Для установки агента для Exchange на остальных узлах выберите DAG, нажмите **Сведения**, после чего нажмите **Установить агент** возле каждого узла.

Создание резервной копии данных кластера Exchange

1. При создании плана защиты выберите DAG в соответствии с инструкциями в разделе "Выбор данных Microsoft Exchange Server".
2. Настройте параметр резервного копирования «Способ резервного копирования кластера».
3. Укажите другие необходимые настройки плана защиты.

Внимание

Для резервного копирования с поддержкой кластеров необходимо выбрать саму группу обеспечения доступности баз данных. Если выбрать отдельные узлы или базы данных в группе обеспечения доступности баз данных, то будет создана резервная копия только для выбранных элементов, а параметр **Способ резервного копирования кластера** будет проигнорирован.

Восстановление данных кластера Exchange

1. Выберите точку восстановления для базы данных, которую необходимо восстановить. Резервное копирование всего кластера для восстановления невозможно.

© ООО Киберпротект, 2026

Если в разделе **Устройства** > **Microsoft Exchange** > **Базы данных** > <имя кластера> > <имя узла> выбрать копию кластеризованной базы данных и нажать кнопку **Восстановить**, в программном обеспечении будут показаны только те точки восстановления, которые соответствуют времени создания резервной копии выбранной копии базы данных.

Самый легкий способ просмотра всех точек восстановления кластеризованной базы данных – выбор соответствующей резервной копии на вкладке "Хранилища резервных копий".

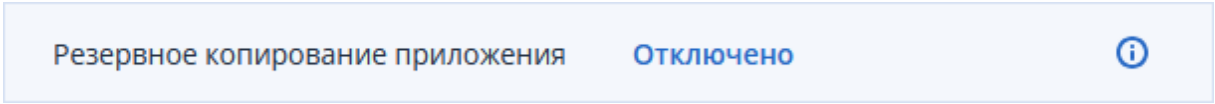
2. Выполните действия, описанные в разделе «Восстановление баз данных Exchange», начиная с шага 5.

   Программное обеспечение автоматически определяет узел кластера, на который будут восстановлены данные. Имя узла отображается в поле **Восстановить на**. Вы можете вручную изменить целевой узел.

12.1.7 Резервное копирование с поддержкой приложений

Резервная копия на уровне дисков с поддержкой приложений доступна для физических машин, виртуальных машин ESXi и виртуальных машин Hyper-V.

При резервном копировании машины, на которой выполняется Microsoft SQL Server, Microsoft Exchange Server или доменные службы Active Directory, включите **Резервное копирование приложения** для дополнительной защиты данных этих приложений.



12.1.7.1 Почему нужно использовать резервное копирование с поддержкой приложений?

Используя резервное копирование с поддержкой приложений, вы обеспечиваете следующее:

1. Резервные копии приложений в согласованном состоянии, поэтому доступны немедленно после восстановления машины.
2. Можно восстановить базы данных SQL и Exchange, почтовые ящики и элементы почтовых ящиков без восстановления всей машины.
3. После каждого успешного резервного копирования выполняется сокращение журналов транзакций SQL. Усечение журнала SQL можно отключить в параметрах плана защиты. Журналы транзакций Exchange сокращаются только на виртуальных машинах. Чтобы урезать размер журналов транзакций Exchange на физической машине, можно включить параметр полного резервного копирования VSS.
4. Если домен содержит несколько контроллеров домена, то при восстановлении одного из них выполняется непринудительное восстановление; при этом откат USN не выполняется после восстановления.

© ООО Киберпротект, 2026

12.1.7.2 Что необходимо для использования резервного копирования с поддержкой приложений?

На физической машине кроме агента для Windows должен быть установлен агент для SQL и (или) агент для Exchange.

На виртуальной машине наличие установленного агента не требуется. Предполагается, что резервная копия виртуальной машины создана агентом для VMware (Windows) или агентом для Hyper-V.

Агент для VMware (виртуальное устройство) и агент для VMware (Linux) может создать резервные копии с поддержкой приложений, но не может восстановить из них данные приложения. Чтобы восстановить данные приложения с резервных копий, созданных этими агентами, необходимо иметь агент для VMware (Windows), агент для SQL или агент для Exchange на машине с доступом к хранилищу, в котором хранятся резервные копии. При настройке восстановления данных приложения выберите точку восстановления на вкладке **Хранилища резервных копий**, а затем выберите эту машину в списке **Машина для обзора**.

Другие требования перечислены в разделах «Предварительные требования» и «Необходимые права пользователя».

12.1.7.3 Требуемые права пользователя

Резервные копии с поддержкой приложений содержат метаданные приложений с поддержкой VSS, которые представлены на диске. Чтобы агент мог получить доступ к метаданным, для него необходима учетная запись с соответствующими правами, которые перечислены ниже. Пользователю поступает запрос на указание учетной записи при включении резервного копирования приложений.

- Для SQL Server:

  Соответствующая учетная запись должна входить в группу **Операторы архива** или **Администраторы** на этой машине, а также иметь роль **sysadmin** в каждом из экземпляров, для которых создается резервная копия.
- Для Active Directory:

  Данная учетная запись должна быть администратором домена.

Дополнительные требования для виртуальных машин

Если приложение выполняется на виртуальной машине, резервная копия которой создана агентом для VMware или агентом для Hyper-V, убедитесь, что на этой машине отключен контроль учетных записей (UAC). Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).

© ООО Киберпротект, 2026

12.1.8 Резервная копия почтового ящика

Резервное копирование почтовых ящиков поддерживается для Microsoft Exchange Server 2013 и более поздних версий.

Резервная копия почтового ящика доступна, если на сервере управления зарегистрирован по меньшей мере один агент для Exchange. Этот агент должен быть установлен на машине, которая находится в одном лесу Active Directory с сервером Microsoft Exchange Server.

Перед выполнением резервного копирования почтовых ящиков вы должны подключить агент для Exchange к машине с серверной ролью (CAS) **Client Access** сервера Microsoft Exchange Server. В Exchange 2016 и более поздних версиях роль CAS не устанавливается отдельно. Она устанавливается автоматически как часть роли сервера почтовых ящиков. Таким образом, можно подключить агент к любому серверу, которому присвоена **роль почтовых ящиков**.

Как подключить агент для Exchange к CAS

1. Нажмите **Устройства** > **Добавить**.
2. Нажмите **Microsoft Exchange Server**.
3. Щелкните **Почтовые ящики Exchange**.

   Если на сервере управления не зарегистрировано ни одного агента для Exchange, программное обеспечение попросит вас установить агент. После установки повторите эту процедуру с шага 1.
4. [Необязательно] Если на сервере управления зарегистрировано несколько агентов для Exchange, щелкните **Агент** и измените агент, который выполнит резервное копирование.
5. На сервере **Client Access Server** укажите полное доменное имя машины (FQDN), на которой включена роль **Клиентский доступ** Microsoft Exchange Server.

   В Exchange 2016 и более поздних версиях службы клиентского доступа автоматически устанавливаются в рамках роли сервера почтовых ящиков. Таким образом, можно указать любой сервер, которому присвоена **роль почтовых ящиков**. В этом разделе подобный сервер обозначается аббревиатурой CAS.
6. В пункте **Тип аутентификации**, выберите тип аутентификации, используемый CAS. Можно выбрать **Kerberos** (по умолчанию) или **Базовый**.
7. [Только для базовой аутентификации] Выберите используемый протокол. Можно выбрать **HTTPS** (по умолчанию) или **HTTP**.
8. [Только для базовой аутентификации с протоколом HTTPS] Если CAS использует сертификат SSL, полученный от сертифицирующей организации, и вы желаете, чтобы программное обеспечение проверяло сертификат SSL при подключении к CAS, установите флажок **Проверять сертификат SSL**. В противном случае пропустите этот шаг.
9. Укажите учетные данные учетной записи, которые будут использоваться для доступа к CAS. Требования к этой учетной записи указаны в разделе «Требуемые права пользователя».
10. Нажмите кнопку **Добавить**.

© ООО Киберпротект, 2026

В результате почтовый ящик будет находиться по пути **Устройства** > **Microsoft Exchange** > **Почтовые ящики**.

12.1.8.1 Выбор почтовых ящиков сервера Exchange

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана защиты как требуется.

Выбор почтовых ящиков Exchange

1. Нажмите **Устройства** > **Microsoft Exchange**.
   Программное обеспечение отобразит дерево баз данных и почтовых ящиков Exchange
2. Нажмите **Почтовые ящики**, после чего выберите почтовые ящики, для которых необходимо создать резервные копии.
3. Нажмите кнопку **Резервное копирование**.

12.1.8.2 Требуемые права пользователя

Чтобы получить доступ к почтовым ящикам, агенту для Exchange необходима учетная запись с соответствующими правами. При настройке различных операций с почтовыми ящиками пользователю поступает запрос на указание учетной записи.

Членство учетной записи в группе ролей **Управление организацией** позволяет получить доступ к любому почтовому ящику, включая почтовые ящики, которые будут созданы в будущем.

12.1.9 Восстановление баз данных Microsoft SQL Server

В этом разделе описано восстановление из резервных копий базы данных и резервных копий с поддержкой приложений.

Можно восстановить базы данных SQL в экземпляр SQL Server, если на машине с этим экземпляром установлен агент для SQL. Для этого потребуется указать данные учетной записи, которая входит в группу **Операторы архива** или **Администраторы** на этой машине, а также имеет роль **sysadmin** на целевом экземпляре.

Базы данных также можно восстанавливать в виде файлов. Это может быть полезным при необходимости извлечь данные для интеллектуального анализа данных, аудита или дальнейшей обработки с использованием инструментов сторонних поставщиков. Можно присоединить файлы базы данных SQL к экземпляру SQL Server, как описано в теме «Подключение баз данных SQL Server».

Если используется только агент для VMware (Windows), то единственный доступный метод восстановления – восстановить базы данных как файлы. Невозможно восстановить базы данных с помощью агента для VMware (виртуальное устройство).

Системные базы данных восстанавливаются в целом так же, как и пользовательские. Особенности этой процедуры описаны в разделе «Восстановление системных баз данных».

Восстановление базы данных в запущенный экземпляр SQL Server

© ООО Киберпротект, 2026

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft SQL** и затем выберите базы данных, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для SQL, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилища резервных копий.

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления баз данных SQL.
4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** > **Базы данных SQL**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** > **Базы данных в экземпляр**.
5. По умолчанию данные восстанавливаются в исходных базах. Если исходная база данных не существует, она будет создана. Можно выбрать другой экземпляр сервера SQL Server (запущенный на той же машине), в который требуется восстановить базы данных.

   Восстановление данных в другой базе на том же экземпляре
   a. Щелкните имя базы данных.
   b. В поле **Восстановить в** выберите вариант **Новая база данных**.
   c. Укажите имя новой базы данных.
   d. Укажите путь к новой базе данных и журналу. В указанной папке не должно быть файлов исходной базы данных и ее журналов. В противном случае возникнет ошибка из-за конфликта новых и существующих файлов с идентичными именами.
6. [Необязательно] [Недоступно для базы данных, восстановленной в свой исходный экземпляр как новая база данных] Чтобы изменить состояние базы данных после восстановления, щелкните ее имя и выберите один из перечисленных ниже вариантов.
   - **Готово к использованию (RESTORE WITH RECOVERY)** (по умолчанию)

     После завершения восстановления база данных будет готова к использованию. Пользователи будут иметь к ней полный доступ. Программа выполнит откат всех

© ООО Киберпротект, 2026

незафиксированных транзакций восстановленной базы данных, хранящихся в журналах транзакций. Вы не сможете восстановить дополнительные журналы транзакций из резервных копий в собственном формате Microsoft SQL.

- **В нерабочем состоянии (RESTORE WITH NORECOVERY)**

  Использовать базу данных после завершения восстановления будет невозможно. Пользователи не будут иметь к ней доступа. Программа сохранит все незафиксированные транзакции восстановленной базы данных. Вы сможете восстановить дополнительные журналы транзакций из резервных копий в собственном формате Microsoft SQL и таким образом достичь нужной точки восстановления (Point-in-Time Recovery, PITR).

  Восстановление дополнительных журналов транзакций из резервных копий в формате Microsoft SQL Server доступно при отключении в плане резервного копирования параметра "Сокращение журнала Microsoft SQL Server" (стр. 358). Сведения о восстановлении журналов транзакций см. в документации Microsoft.

- **Только чтение (RESTORE WITH STANDBY)**

  После завершения восстановления база данных будет доступна пользователям только для чтения. Программа выполнит откат всех незафиксированных транзакций. Однако действия по откату будут сохранены во временный резервный файл, чтобы можно было вернуть базу данных в состояние до восстановления.

  Это значение в основном используется для определения точки во времени, где произошла ошибка SQL Server.

7. Щелкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке **Действия**.

Восстановление баз данных SQL в виде файлов

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft SQL** и затем выберите базы данных, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для SQL или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилища резервных копий.

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления баз данных SQL.

© ООО Киберпротект, 2026

4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** > **Базы данных SQL**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить как файлы**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** > **Базы данных как файлы**.
5. Нажмите **Обзор** и затем выберите локальную или сетевую папку, в которую требуется сохранить файлы.
6. Щелкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке **Действия**.

12.1.9.1 Восстановление системных баз данных

Все системные базы данных экземпляра восстанавливаются одновременно. При восстановлении системных баз программа автоматически перезапускает целевой экземпляр в однопользовательском режиме. После завершения восстановления программа перезапускает экземпляр и восстанавливает другие базы данных (если есть).

При восстановлении системной базы данных также обращайте внимание на перечисленные ниже моменты.

- Системные базы данных можно восстановить только на экземпляре той же версии, что и исходный.
- Системные базы данных всегда восстанавливаются в состоянии «готово к использованию».

Восстановление базы данных master

В число системных баз данных входит база **master**. В базе данных **master** содержатся сведения обо всех базах данных экземпляра. Это означает, что база данных **master** в резервной копии содержит информацию о базах данных, существовавших в экземпляре на момент резервного копирования. После восстановления базы данных **master** может потребоваться следующее.

- Базы данных, которые появились в экземпляре после выполнения резервного копирования, становятся невидимыми для экземпляра. Чтобы снова перевести их в режим эксплуатации, прикрепите их к экземпляру вручную с помощью SQL Server Management Studio.
- Базы данных, которые были удалены после выполнения резервного копирования, отображаются в экземпляре как находящиеся в автономном режиме. Удалите эти базы данных с помощью SQL Server Management Studio.

12.1.9.2 Подключение баз данных Microsoft SQL Server

В этом разделе описывается процедура подключения базы данных в Microsoft SQL Server с помощью среды SQL Server Management Studio. Одновременно может быть подключена только одна база данных.

© ООО Киберпротект, 2026

Для подключения базы данных необходимо иметь любое из следующих разрешений: **CREATE DATABASE** (Создание базы данных), **CREATE ANY DATABASE** (Создание любой базы данных) или **ALTER ANY DATABASE** (Изменение любой базы данных). Обычно эти разрешения предоставляются роли **sysadmin** экземпляра.

Как подключить базу данных

1. Запустите среду SQL Server Management Studio.
2. Подключитесь к требуемому экземпляру Microsoft SQL Server и разверните его.
3. Правой кнопкой мыши щелкните пункт **Базы данных** и щелкните **Подключить**.
4. Нажмите кнопку **Добавить**.
5. В диалоговом окне **Поиск файлов баз данных** найдите и выберите MDF-файл базы данных.
6. В разделе **Сведения о базе данных** убедитесь, что остальные файлы базы данных (NDB-файлы и LDF-файлы) также найдены.

   Подробнее. Файлы базы данных Microsoft SQL Server могут быть не найдены автоматически, если:
   - Они находятся в расположении, отличном от расположения по умолчанию, или они не находятся в одной папке с основным файлом базы данных (MDF). Решение: Укажите путь к требуемым файлам вручную в столбце **Путь к текущему файлу**.
   - Вы восстановили неполный набор файлов, составляющих базу данных. Решение: Восстановите отсутствующие файлы базы данных Microsoft SQL Server из резервной копии.
7. Когда все файлы будут найдены, нажмите кнопку **OK**.

12.1.10 Восстановление баз данных Microsoft Exchange Server

В этом разделе описано восстановление из резервных копий базы данных и резервных копий с поддержкой приложений.

Можно восстановить данные Exchange в работающий Exchange. Это может быть исходный Exchange или Exchange той же версии, выполняющийся на машине с таким же полным доменным именем (FQDN). Агент для Exchange должен быть установлен на целевой машине.

В таблице ниже приведены основные сведения о том, какие именно данные Exchange можно выбрать для восстановления, а также о минимальных правах пользователя, которые для этого необходимы.

Версия Exchange	Элементы данных	Права пользователя
2013/2016/2019	Базы данных	Участие в группе ролей **Управление сервером**.

Базы данных также можно восстанавливать в виде файлов. Файлы баз данных и журналы транзакций извлекаются из резервной копии в указанную папку. Это может оказаться полезно, если необходимо извлечь данные для аудита или дальнейшей обработки средствами сторонних

© ООО Киберпротект, 2026

производителей либо в случае, когда выполнить восстановление по какой-либо причине не удается и требуется обходное решение для подключения баз данных вручную.

Если используется только агент для VMware (Windows), то единственный доступный метод восстановления – восстановить базы данных как файлы. Невозможно восстановить базы данных с помощью агента для VMware (виртуальное устройство).

Для восстановления баз данных Exchange на запущенный сервер Exchange

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft Exchange** > **Базы данных** и затем выберите базы данных, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилища резервных копий.

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления данных Exchange.
4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** > **Базы данных Exchange**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** > **Базы данных на сервер Exchange**.
5. По умолчанию данные восстанавливаются в исходных базах. Если исходная база данных не существует, она будет создана.

   Восстановление данных в другой базе
   a. Щелкните имя базы данных.
   b. В поле **Восстановить в** выберите вариант **Новая база данных**.
   c. Укажите имя новой базы данных.
   d. Укажите путь к новой базе данных и журналу. В указанной папке не должно быть файлов

© ООО Киберпротект, 2026

исходной базы данных и ее журналов.

6. Щелкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке **Действия**.

Восстановление баз данных Exchange в виде файлов

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft Exchange** > **Базы данных** и затем выберите базы данных, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилища резервных копий.

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления данных Exchange.
4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** > **Базы данных Exchange**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить как файлы**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** > **Базы данных как файлы**.
5. Нажмите **Обзор** и затем выберите локальную или сетевую папку, в которую требуется сохранить файлы.
6. Щелкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке **Действия**.

12.1.10.1 Подключение баз данных Microsoft Exchange Server

После восстановления файлов базы данных можно включить базы данных, подключив их. Подключение выполняется с использованием консоли управления Exchange, диспетчера Exchange или командной консоли Exchange.

Восстановленные базы данных будут в состоянии «Неправильное отключение». База данных в состоянии «Неправильное отключение» может быть подключена системой, если она

© ООО Киберпротект, 2026

восстанавливается в исходное хранилище (то есть, информация об исходной базе данных присутствует в Active Directory). Если база данных восстанавливается в другое расположение (в новую базу данных или базу данных восстановления), она не может быть подключена, пока не будет приведена в состояние «чистого отключения» с помощью команды Eseutil /r <Enn>. <Enn> указывает префикс файлов журнала для базы данных (или группы хранения, содержащей эту базу данных), где необходимо применить файлы журнала транзакций.

Учетной записи, которая используется для подключения базы данных, необходимо делегировать роль администратора сервера Exchange и локальную группу администраторов для данного целевого сервера.

Подробную информацию о том, как подключить базы данных, см. в статье по ссылке http://technet.microsoft.com/en-us/library/aa998871.aspx.

12.1.11 Восстановление почтовых ящиков Exchange и элементов почтового ящика

В этом разделе описана процедура восстановления почтовых ящиков Exchange и элементов почтового ящика из резервных копий базы данных, резервных копий с поддержкой приложений и из резервных копий почтового ящика. Почтовые ящики или элементы почтового ящика могут быть восстановлены на запущенный Exchange Server.

Можно восстановить следующие элементы:

- почтовые ящики, в том числе архивные;
- общие папки;
- элементы общих папок;
- папки электронной почты;
- сообщения электронной почты;
- события календаря;
- задания;
- контакты;
- записи журнала;
- заметки.

Чтобы найти эти элементы, можно воспользоваться поиском.

12.1.11.1 Восстановление на Exchange Server

Фрагментарное восстановление можно выполнить в Microsoft Exchange Server 2013 и более поздних версиях. Исходная резервная копия может содержать базы данных или почтовые ящики любой поддерживаемой версии Exchange.

© ООО Киберпротект, 2026

Фрагментарное восстановление может быть выполнено агентом для Exchange или агентом для VMware (Windows). Целевой Exchange Server и машина с выполняющимся агентом должны быть в одном лесу Active Directory.

Если почтовый ящик восстанавливается в существующий почтовый ящик, существующие элементы с одинаковыми идентификаторами перезаписываются.

При восстановлении элементов почтового ящика перезапись не происходит. Вместо этого в целевой папке заново создается полный путь к элементу почтового ящика.

Требования к учетным записям пользователей

Почтовый ящик, восстанавливаемый из резервной копии, должен иметь связанную с ним учетную запись пользователя в Active Directory.

Пользовательские почтовые ящики и их содержимое можно восстановить, только если *включены* связанные с ними учетные записи пользователей. Общие почтовые ящики, почтовые ящики помещения и оборудования могут быть восстановлены, только если соответствующие учетные записи пользователей *отключены*.

Почтовый ящик, не соответствующий этим условиям, при восстановлении будет пропущен.

Если некоторые почтовые ящики будут пропущены, восстановление продолжится с предупреждением. Если все почтовые ящики будут пропущены, восстановление завершится сбоем.

12.1.11.2 Восстановление почтовых ящиков

Порядок восстановления почтовых ящиков из резервной копии с поддержкой приложений или резервной копии базы данных

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений: в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft Exchange** > **Базы данных** и затем выберите базу данных, в которой изначально располагались данные, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. В этом случае воспользуйтесь одним из перечисленных ниже способов.
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для

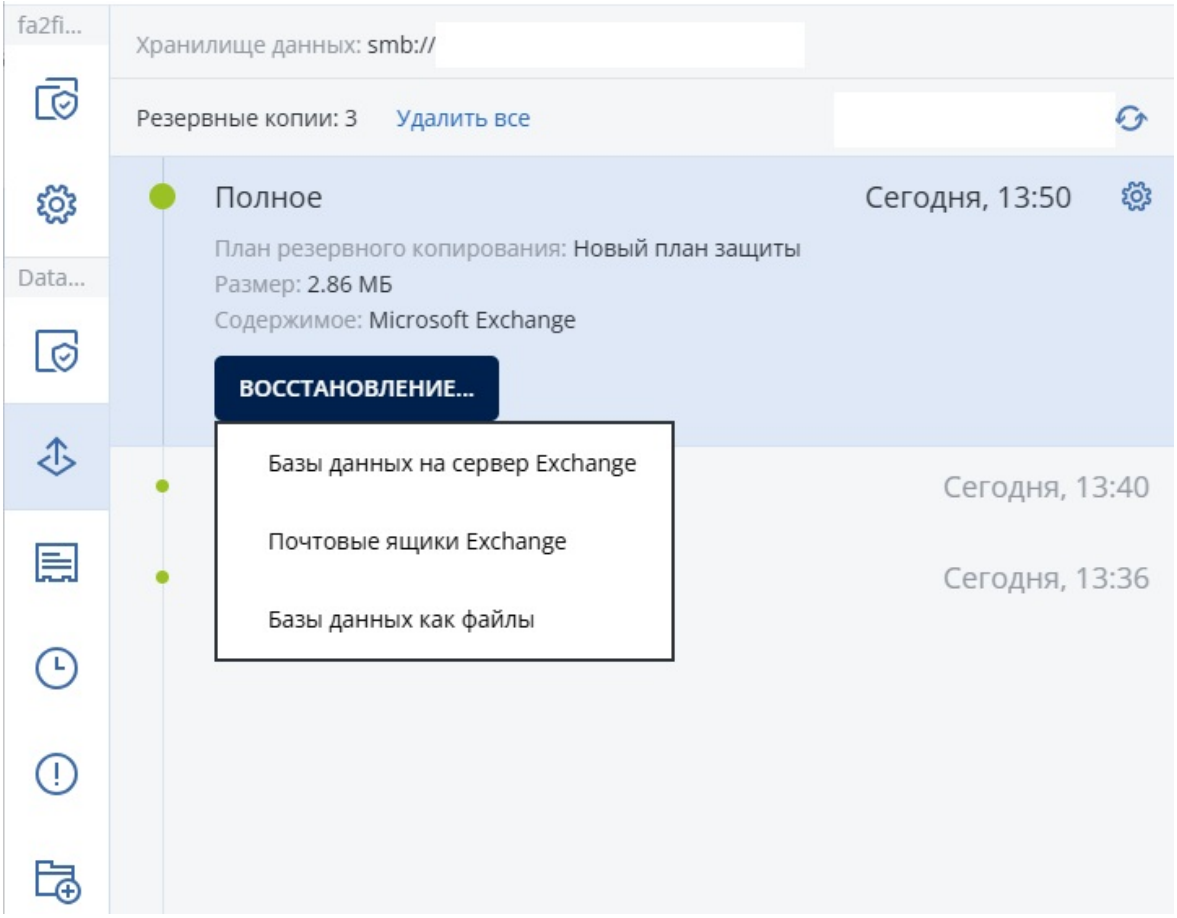
© ООО Киберпротект, 2026

Exchange или агент для VMware, а затем выберите точку восстановления.

- Выберите точку восстановления на вкладке Хранилища резервных копий.

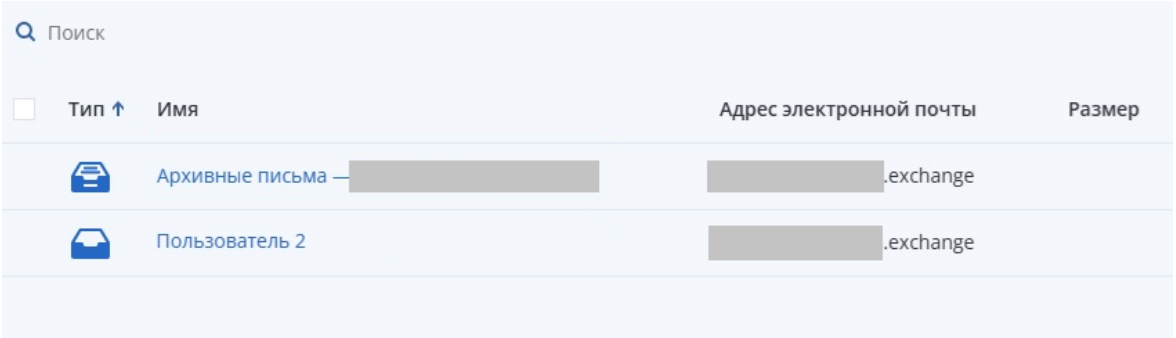
  Вместо выключенной исходной машины восстановление будет выполнено машиной, которая выбрана для просмотра одним из двух указанных выше действий.

4. Щелкните **Восстановление** > **Почтовые ящики Exchange**.



5. Выберите почтовые ящики, которые необходимо восстановить. Архивные почтовые ящики имеют специальную иконку и имя, состоящее из названия архива писем и псевдонима пользователя.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.



6. Нажмите кнопку **Восстановить**.

© ООО Киберпротект, 2026

Чтобы выбрать или изменить целевую машину, щелкните **Целевая машина с Microsoft Exchange Server**. Это действие позволит восстановить машину, на которой не запущен агент для Exchange.

Укажите полное доменное имя (FQDN) машины, на которой включена роль **Клиентский доступ** (в Microsoft Exchange Server 2013) или **Роль почтовых ящиков** (в Microsoft Exchange Server 2016 или более поздних версиях). Эта машина должна принадлежать тому же лесу Active Directory, что и машина, которая выполняет восстановление.

7. При поступлении соответствующего запроса укажите данные учетной записи, которая будет использоваться для доступа к машине. Требования к этой учетной записи указаны в разделе «Требуемые права пользователя».
8. При восстановлении архивных почтовых ящиков щелкните **База данных для воссоздания отсутствующих почтовых ящиков** и укажите активную базу данных.
9. Нажмите **Начать восстановление**.

Ход выполнения восстановления показан на вкладке **Действия**.

Порядок восстановления почтового ящика из резервной копии почтового ящика

1. Нажмите **Устройства** > **Microsoft Exchange** > **Почтовые ящики**.
2. Выберите почтовый ящик для восстановления и щелкните **Восстановить**.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.

   Если почтовый ящик был удален, выберите его на вкладке Хранилища резервных копий и щелкните **Показать резервные копии**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
4. Последовательно выберите пункты **Восстановление** > **Почтовый ящик**.
5. Выполняйте шаги 7-9 вышеописанной процедуры.

12.1.11.3 Восстановление элементов почтовых ящиков

Порядок восстановления элементов почтовых ящиков из резервной копии с поддержкой приложений или резервной копии базы данных

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений: в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft Exchange** > **Базы данных** и затем выберите базу данных, в которой изначально располагались данные, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

© ООО Киберпротект, 2026

Если машина отключена, точки восстановления не отображаются. В этом случае воспользуйтесь одним из перечисленных ниже способов.

- [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange или агент для VMware, а затем выберите точку восстановления.
- Выберите точку восстановления на вкладке Хранилища резервных копий.

Вместо выключенной исходной машины восстановление будет выполнено машиной, которая выбранная для просмотра одним из двух указанных выше действий.

4. Щелкните **Восстановление** > **Почтовые ящики Exchange**.
5. Щелкните почтовый ящик, в котором изначально содержались элементы, которые необходимо восстановить.
6. Выберите элементы, которые необходимо восстановить.

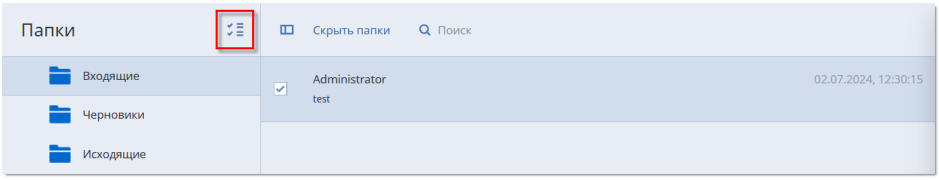
   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

   - Для сообщений электронной почты: выполните поиск по теме, отправителю, получателю и дате.
   - Для событий: выполните поиск по заголовку и дате.
   - Для задач: выполните поиск по теме и дате.
   - Для контактов: выполните поиск по имени, адресу электронной почты и номеру телефона.

   Когда выбрано это сообщение электронной почты, можно щелкнуть **Показать содержимое**, чтобы показать его содержимое, включая вложения.

   Примечание
   Чтобы загрузить вложенный файл, щелкните его имя.

   Чтобы иметь возможность выбрать папки, щелкните значок восстановления папок.



7. Нажмите кнопку **Восстановить**.
8. Чтобы выполнить восстановление на Exchange Server, сохраните значение по умолчанию **Microsoft Exchange** в поле **Восстановить в**.

   Чтобы выбрать или изменить целевую машину, щелкните **Целевая машина с Microsoft Exchange Server**. Это действие позволит восстановить машину, на которой не запущен агент для Exchange.

   Укажите полное доменное имя (FQDN) машины, на которой включена роль **Клиентский доступ** (в Microsoft Exchange Server 2013) или **Роль почтовых ящиков** (в Microsoft Exchange Server 2016 или более поздних версиях). Эта машина должна принадлежать тому же лесу Active Directory, что и машина, которая выполняет восстановление.
9. При поступлении соответствующего запроса укажите данные учетной записи, которая будет

© ООО Киберпротект, 2026

использоваться для доступа к машине. Требования к этой учетной записи указаны в разделе «Требуемые права пользователя».

10. Раздел **Целевой почтовый ящик** позволяет просмотреть, изменить или указать целевой почтовый ящик.

    По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует или выбрана целевая машина, которая не является исходной, необходимо указать целевой почтовый ящик.

    При восстановлении архивного почтового ящика укажите действующий почтовый ящик, в который будут восстановлены данные.
11. [Только при восстановлении сообщений электронной почты] В поле **Целевая папка** просмотрите или измените целевую папку в целевом почтовом ящике. По умолчанию выбрана папка **Восстановленные элементы**. Из-за ограничений Microsoft Exchange события, задачи, примечания и контакты восстанавливаются в их оригинальное расположение независимо от папки, заданной параметром **Целевая папка**.
12. Нажмите **Начать восстановление**.

Ход выполнения восстановления показан на вкладке **Действия**.

Порядок восстановления элемента почтового ящика из резервной копии почтового ящика

1. Нажмите **Устройства** > **Microsoft Exchange** > **Почтовые ящики**.
2. Выберите почтовый ящик, в котором изначально содержались элементы, которые необходимо восстановить, и нажмите кнопку **Восстановить**.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.

   Если почтовый ящик был удален, выберите его на вкладке Хранилища резервных копий и щелкните **Показать резервные копии**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
4. Последовательно выберите пункты **Восстановление** > **Сообщения электронной почты**.
5. Выберите элементы, которые необходимо восстановить.

   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

   - Для сообщений электронной почты: выполните поиск по теме, отправителю, получателю и дате.
   - Для событий: выполните поиск по заголовку и дате.
   - Для задач: выполните поиск по теме и дате.
   - Для контактов: выполните поиск по имени, адресу электронной почты и номеру телефона.

   Если выбрано сообщение электронной почты, можно щелкнуть **Показать содержимое**, чтобы показать его содержимое, включая вложения.

Примечание
Чтобы загрузить вложенный файл, щелкните его имя.

© ООО Киберпротект, 2026

Если выбрано сообщение электронной почты, можно щелкнуть **Отправить как сообщение электронной почты**, чтобы отправить сообщение по адресу электронной почты. Сообщение отправляется с адреса электронной почты администратора учетной записи.

Чтобы иметь возможность выбрать папки, щелкните значок восстановления папок .

6. Нажмите кнопку **Восстановить**.
7. Выполните шаги 8-12 вышеописанной процедуры.

12.1.11.4 Копирование библиотек Microsoft Exchange Server

Скопируйте указанные ниже файлы в соответствии с версией Microsoft Exchange Server, для которой создана резервная копия.

Версия Microsoft Exchange Server	Ленточные библиотеки	Хранилище по умолчанию
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

Библиотеки необходимо поместить в папку **%ProgramData%\Acronis\ese**. Если папка не существует, создайте ее вручную.

12.1.12 Изменение учетных данных для доступа к Microsoft SQL Server или Microsoft Exchange Server

Можно изменить учетные данные для доступа к Microsoft SQL Server или Microsoft Exchange Server без переустановки агента.

Для изменения учетных данных для доступа к Microsoft SQL Server или Microsoft Exchange Server

1. Щелкните **Устройства**, а затем щелкните **Microsoft SQL** или **Microsoft Exchange**.
2. Выберите группу обеспечения доступности Always On, группу обеспечения доступности баз данных, экземпляр Microsoft SQL Server или Microsoft Exchange Server, для которых необходимо изменить учетные данные.
3. Щелкните **Укажите учетные данные**
4. Укажите новые учетные данные для доступа, а затем щелкните **OK**.

© ООО Киберпротект, 2026

Для изменения учетных данных Microsoft Exchange Server для доступа к резервной копии почтового ящика

1. Щелкните **Устройства** > **Microsoft Exchange** и разверните узел **Почтовые ящики**.
2. Выберите Microsoft Exchange Server для которого необходимо изменить учетные данные для доступа.
3. Щелкните **Настройки**.
4. Ниже поля **Учетная запись администратора Exchange** укажите новые учетные данные для доступа, а затем щелкните **Сохранить**.

12.2 Защита CommuniGate Pro

12.2.1 Зачем создавать резервную копию CommuniGate Pro

С помощью Кибер Бэкап можно выполнять резервное копирование данных CommuniGate Pro. При использовании Кибер Бэкап и CommuniGate Pro регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователя. Удаленные элементы можно восстановить из резервной копии.

12.2.2 Что необходимо для резервного копирования CommuniGate Pro?

Для резервного копирования данных CommuniGate Pro понадобятся установленные и настроенные продукты:

- Кибер Бэкап 15 обновление 2.7 или новее с лицензией Кибер Бэкап для почтового ящика. Информацию о лицензиях см. в разделе "Издания и лицензии Кибер Бэкап" (стр. 16).
- CommuniGate Pro.
  Поддерживаемые версии CommuniGate Pro указаны в разделе "Поддерживаемые почтовые сервисы" (стр. 35).

Для выполнения резервного копирования требуется установка агента.

Поддерживается установка агентов для следующих операционных систем:

- Windows,
- Linux.

Полный список поддерживаемых операционных систем Windows и Linux см. в разделе "Агенты" (стр. 23).

© ООО Киберпротект, 2026

12.2.3 Возможности

12.2.3.1 Резервное копирование

- Автоматическая и ручная синхронизация ресурсов.
- Резервное копирование данных и настроек.
- Резервное копирование по расписанию.
- Поддержка многоуровневого резервного копирования.
- Перезапись данных хранилища по выбору.
- Настраиваемые правила очистки хранилища.
- Поддержка кластерных конфигураций.

12.2.3.2 Восстановление

- Гранулярное восстановление, или восстановление следующих элементов:
  - серверы (в случае файлового или дискового резервного копирования);
  - почтовые ящики (включая папки, права на них, письма и вложения);
  - письма;
  - контакты;
  - календари;
  - заметки;
  - задачи;
  - настройки учетной записи.
- Восстановление в исходное и новое месторасположение (сервер, домен, пользователь).
- Поиск элементов в резервной копии.

12.2.4 Известные проблемы и ограничения

- Восстановление на новый хост возможно в случае, если на нем заранее создан домен с исходным именем. Восстановление в домен с новым именем невозможно.
- Не поддерживается сохранение резервных копий на подключенное к узлу хранения ленточное устройство.
- Резервное копирование и восстановление настроек пользователя ограничено резервным копированием и восстановлением его системных настроек.

12.2.5 Предварительные требования для защиты CommuniGate Pro

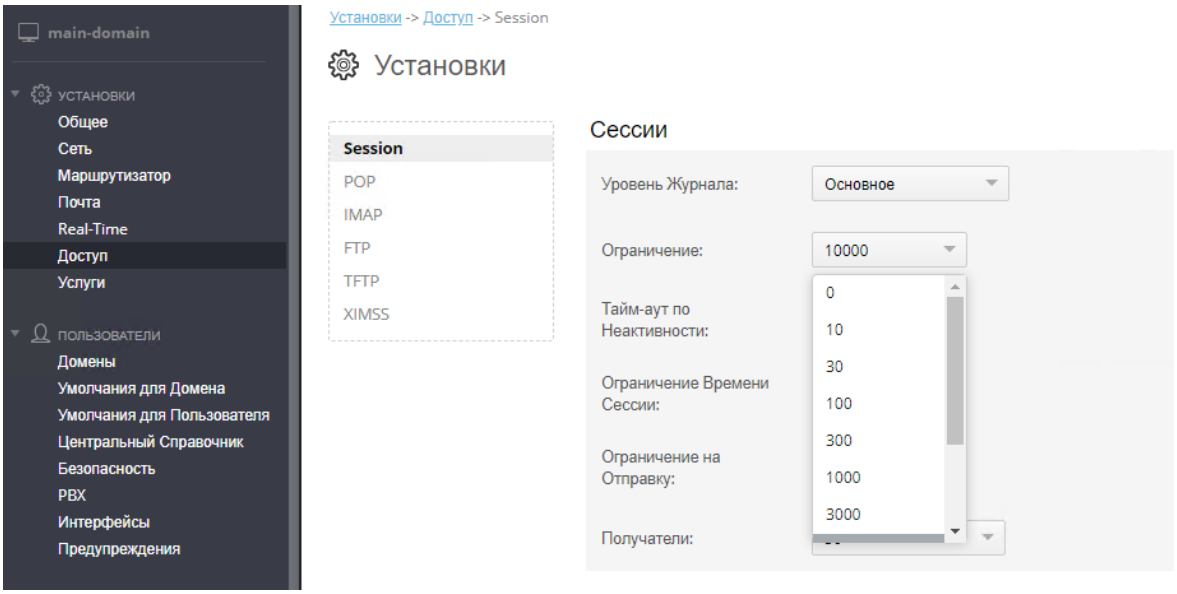
Перед началом использования защиты CommuniGate Pro потребуется выполнить некоторые действия.

© ООО Киберпротект, 2026

12.2.5.1 Выключение ограничений на количество сессий

Необходимо выключить ограничения на количество сессий в сервере CommuniGate, иначе резервное копирование может завершаться с ошибкой. Для выключения ограничений выполните следующие действия:

1. Откройте CommuniGate Pro.
2. Перейдите в **Установки** -> **Доступ**.
3. В подразделе **Сессии** в поле **Ограничение** установите значение, равное 10000.

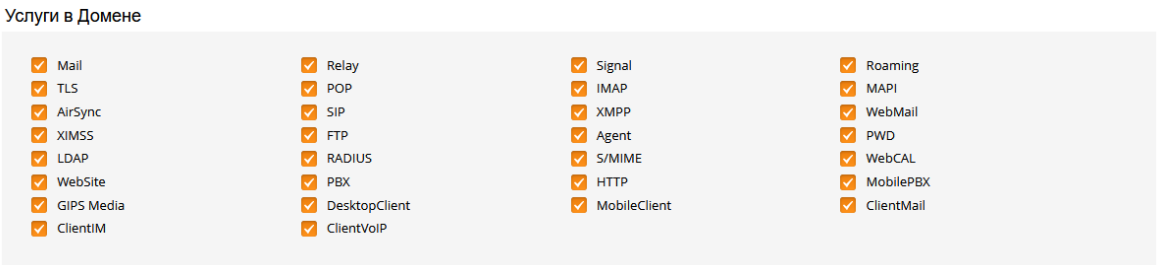


4. Нажмите **Модифицировать**, чтобы сохранить изменения.

12.2.5.2 Инициализация соединения вручную

Для инициализации соединения Кибер Бэкап с CommuniGate Pro (например, если интерфейс командной строки недоступен) может потребоваться выполнить следующие действия:

1. Откройте CommuniGate Pro.
2. Перейдите в **Пользователи** -> **Умолчания для Домена** и убедитесь, что услуга PWD включена.

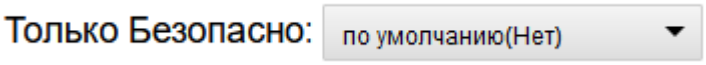


3. Перейдите в **Пользователи** -> **Домены** -> **<Имя_домена>** -> **Установки Домена** и убедитесь, что в настройках домена включена услуга PWD.

© ООО Киберпротект, 2026

4. Перейдите в **Умолчания для пользователя** -> **Установки** и убедитесь, что в настройках пользователя включена услуга PWD.

5. Перейдите в **Умолчания для пользователя** -> **Установки** и выберите **Нет** в параметре **Только безопасно**.



6. Для сохранения изменений нажмите **Модифицировать**.
7. Щелкните **Пользователи** и выберите из списка пользователя (домен), который используется для подключения к Кибер Бэкап.
8. Убедитесь, что в настройках пользователя (домена), используемого для подключения к Кибер Бэкап, включены все опции PWD.

12.2.5.3 Установка прав пользователя

Для того, чтобы выполнять резервное копирование и восстановление из резервных копий в CommuniGate Pro, пользователь, от имени которого они выполняются, должен обладать следующими свойствами:

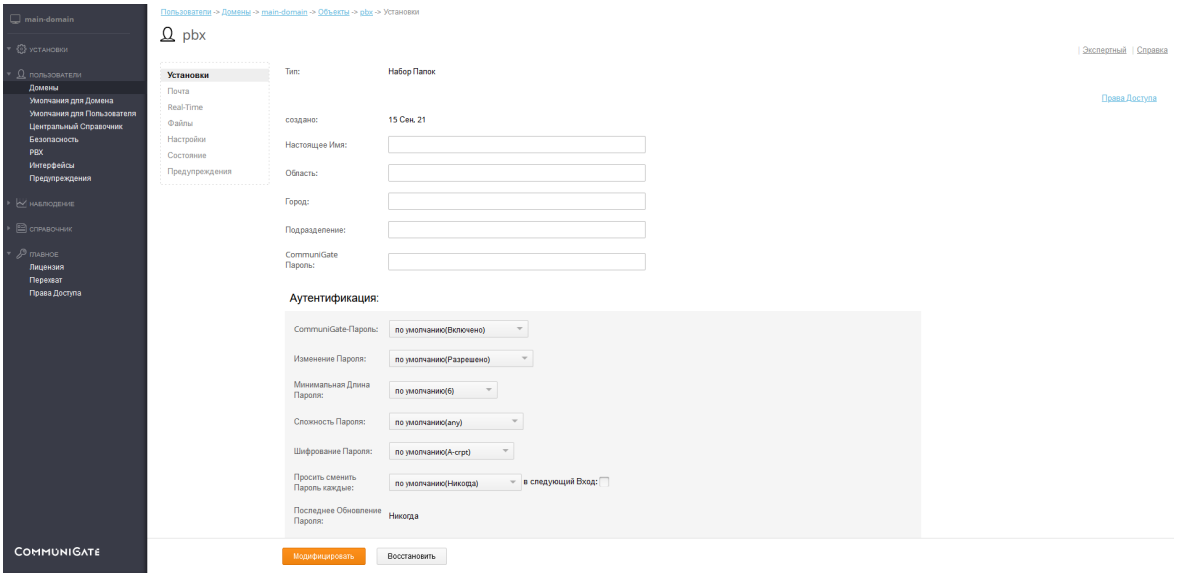
- Пользователь должен принадлежать главному домену.
- Права пользователя должны позволять ему менять установки сервера, а также всех доменов и пользователей.

Установка прав пользователя:

1. Откройте CommuniGate Pro.
2. Перейдите в **Пользователи** -> **Домены** -> **Имя главного домена**.

© ООО Киберпротект, 2026

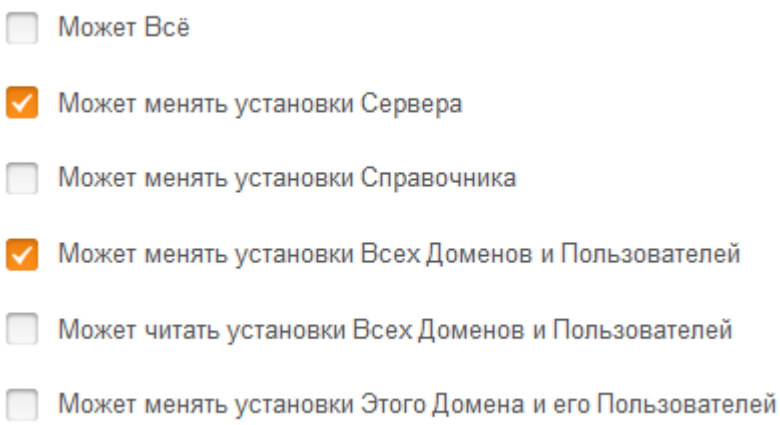
3. Щелкните по имени пользователя в списке объектов.
4. На странице настроек пользователя нажмите справа вверху **Права доступа**.



5. Установите права пользователя следующим образом:

   Может менять установки Сервера и

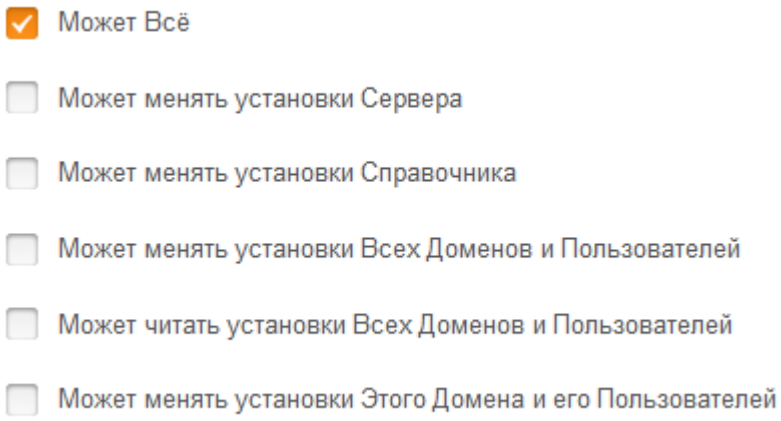
   Может менять установки всех Доменов и Пользователей



   или

   Может Всё

© ООО Киберпротект, 2026



6. Для сохранения изменений нажмите **Модифицировать**.

12.2.5.4 Разрешение подключения агента к серверу CommuniGate Pro

Для успешной работы агент должен иметь возможность подключаться к серверу CommuniGate Pro через TCP-порты 106 и 993 (по умолчанию):

1. Через порт 106 по протоколу PWD происходит базовое подключение для регистрации и определения параметров сервера.
2. Через порт 993 по протоколу IMAP происходит резервное копирование и восстановлении данных.

В настройках сетевого экрана сервера CommuniGate Pro откройте эти порты и разрешите подключение от агента через них.

12.2.5.5 Устранение неполадок при подключении

При возникновении проблем с регистрацией или резервным копированием CommuniGate Pro выполните следующие проверки:

1. Проверка сетевой доступности.

   На машине с агентом CommuniGate Pro выполните следующие команды:

   ```
   ping mx.company.local
   telnet mx.company.local 106
   telnet mx.company.local 993
   ```

   где mx.company.local – имя или IP-адрес сервера CommuniGate Pro.
2. Проверка прав доступа.

   Подключитесь к CommuniGate Pro в режиме командной строки:

   ```
   telnet mx.company.local 106
   ```

   Выполните команды:

© ООО Киберпротект, 2026

```
user postmaster
pass password
LISTDOMAINS
```

где:

- postmaster – имя учетной записи администратора, которую использует агент для подключения к CommuniGate Pro;
- password – пароль учетной записи администратора.

Ответ на каждую команду должен сопровождаться кодом 200.

Пример:

```
% telnet ys-cgp-fe1 106
Trying 10.10.100.10...
Connected to ys-cgp-fe1.
Escape character is '^]'.
200 fe1.domain.name CommuniGate Pro PWD Server 6.3.33 ready <18.1712221326@main-
domain>
user postmaster
300 please send the PASS
pass password
200 login OK, proceed
LISTDOMAINS
200 data follow
(
fe1.domain.name,
fe2,
host-domain,
qwe.domain.name,
test1.domain.name,
test2.domain.name
)
```

12.2.6 Установка CommuniGate Pro

Установка CommuniGate Pro включает в себя установку агента Кибер Бэкап и добавление хоста CommuniGate Pro. Добавление хоста возможно лишь после установки агента.

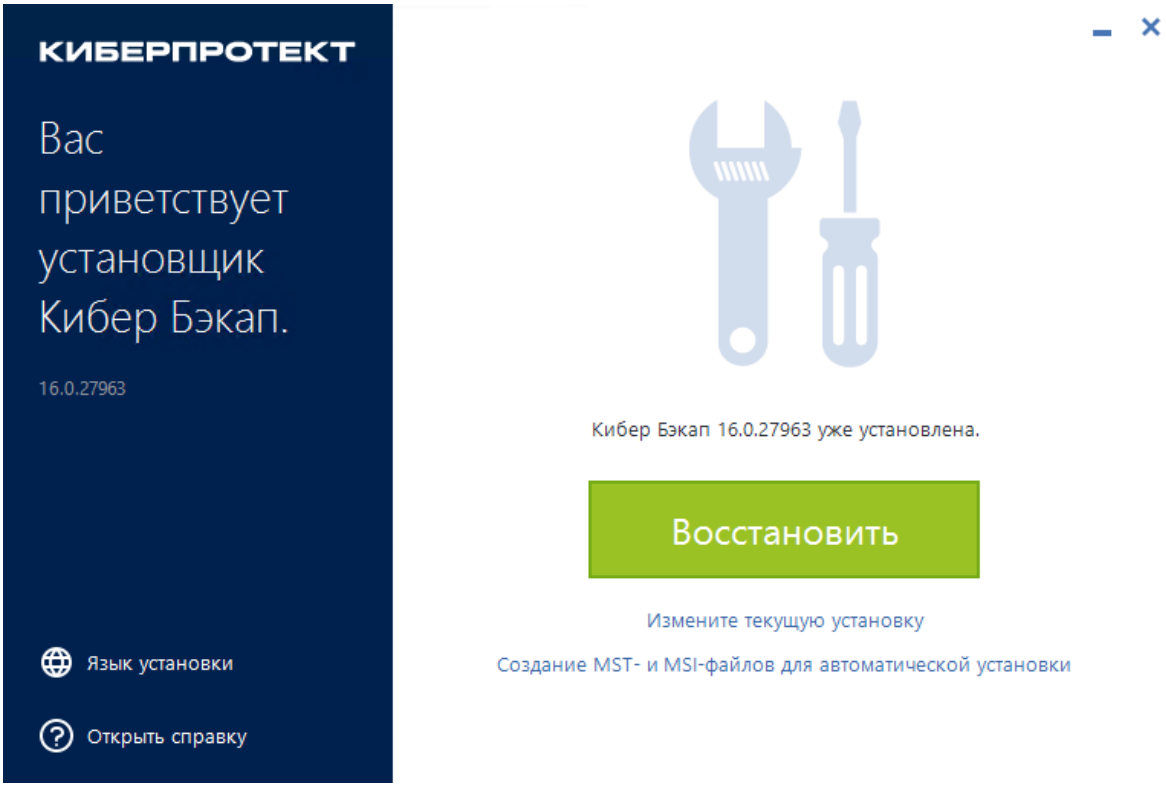
Агент может быть установлен на машину с почтовым сервером или на отдельно стоящую машину.

Для каждого хоста должен быть установлен отдельный агент.

© ООО Киберпротект, 2026

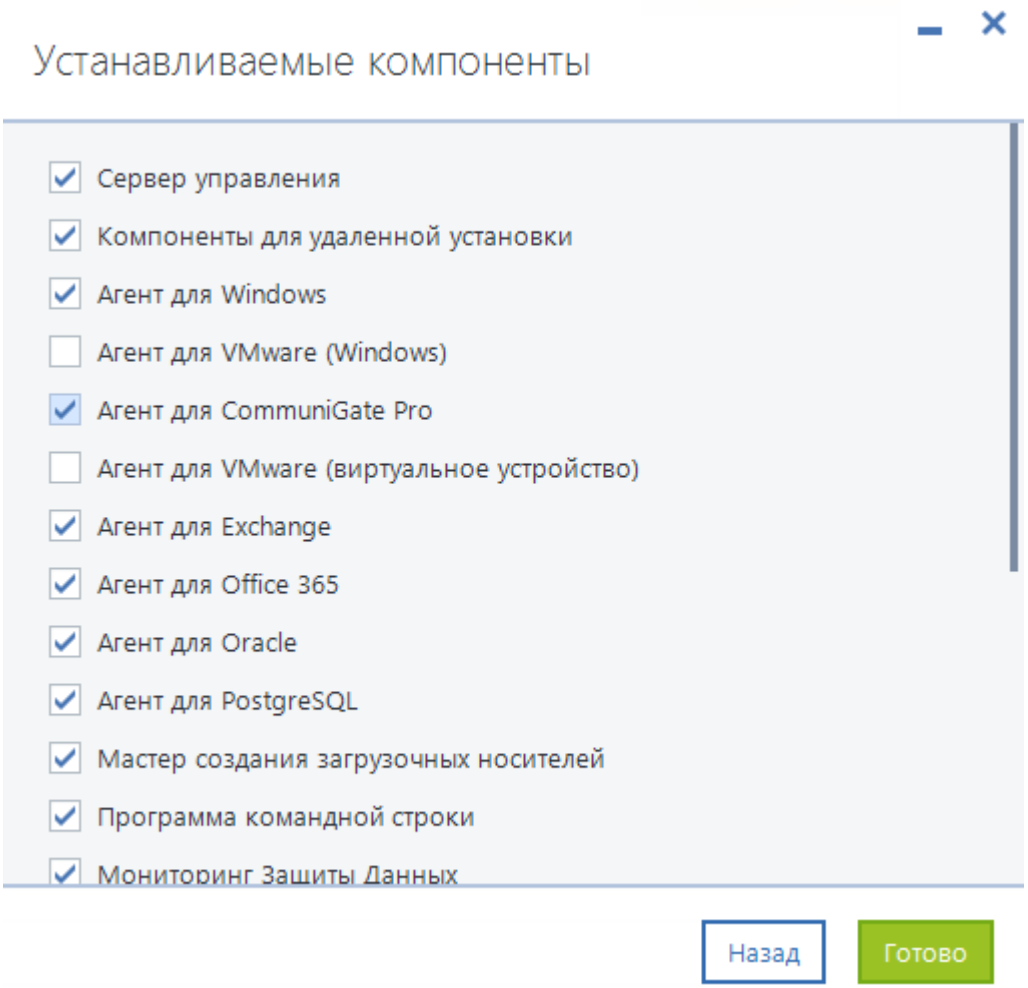
12.2.6.1 Установка агента для CommuniGate Pro

1. Запустите установщик Кибер Бэкап.
2. Выберите **Измените текущую установку**



© ООО Киберпротект, 2026

3. Отметьте в списке **Агент для CommuniGate Pro**.



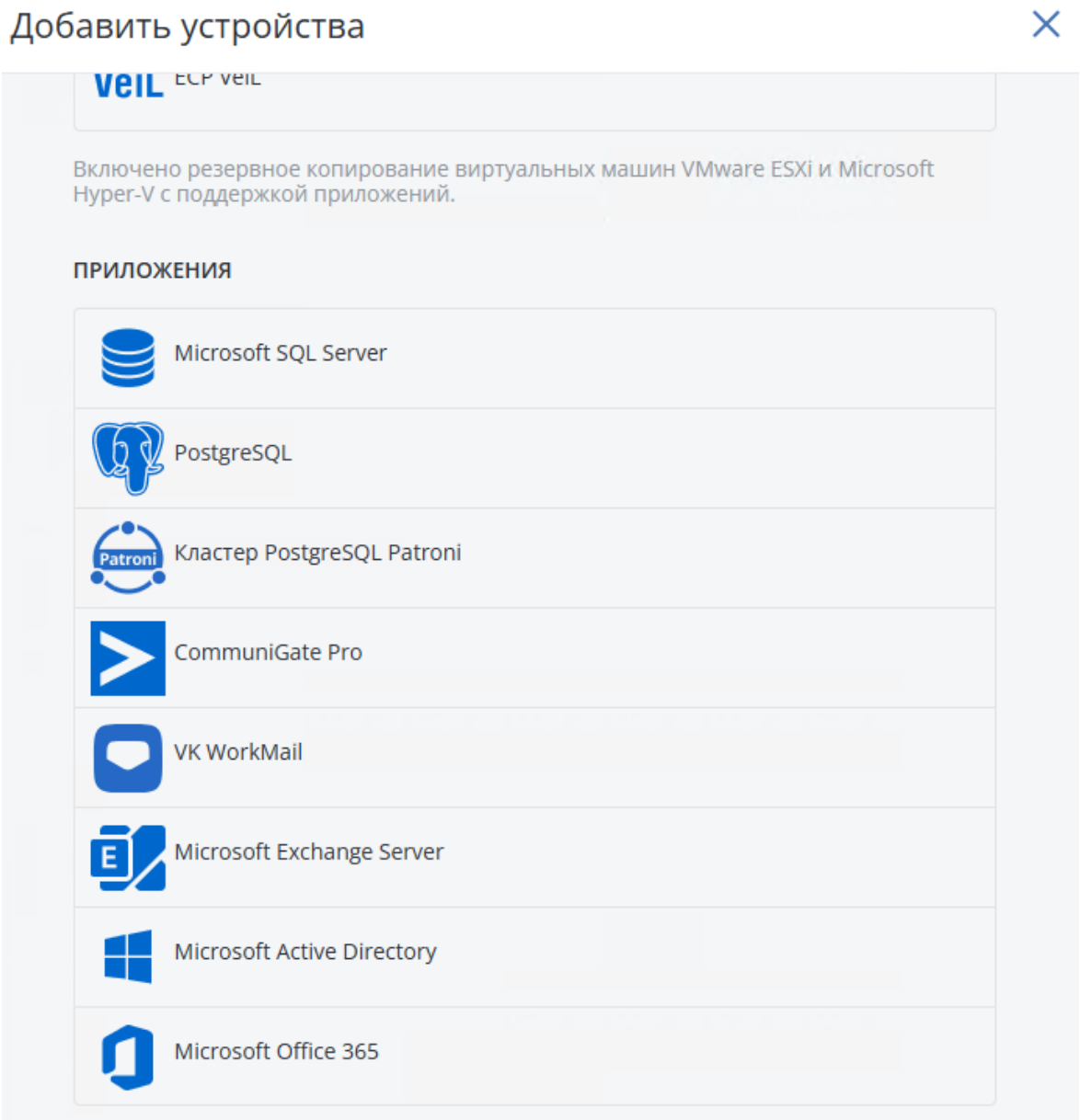
4. Щелкните **Готово**.

12.2.6.2 Добавление хоста CommuniGate Pro

1. В веб-консоли перейдите на вкладку **Устройства** в главном меню слева и нажмите в правом верхнем углу **Добавить**.

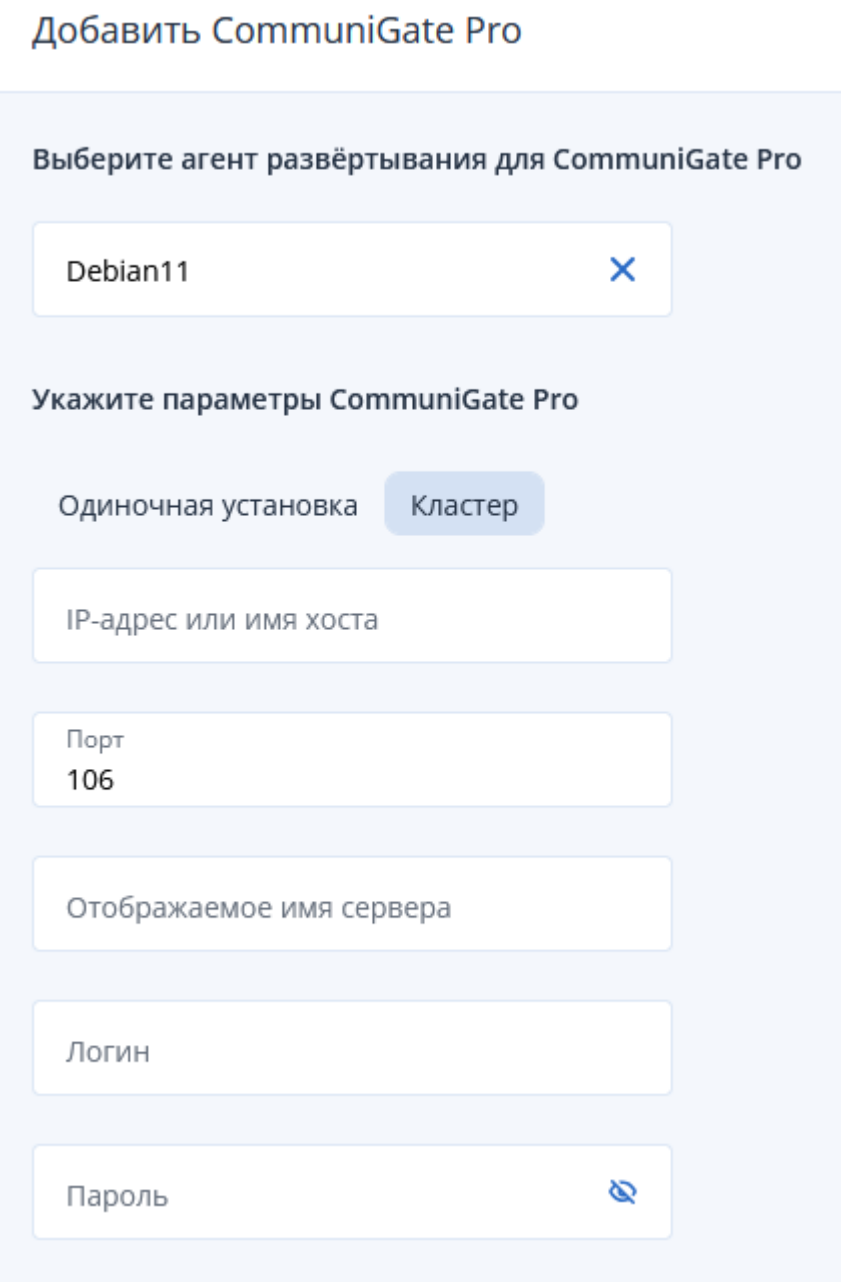
© ООО Киберпротект, 2026

2. В окне добавления нового устройства в подразделе **Приложения** щелкните **CommuniGate Pro**.



3. Заполните поля:
   - в поле подраздела **Выберите агент развертывания для CommuniGate Pro** укажите имя компьютера, на котором установлен агент CommuniGate Pro;
   - в полях подраздела **Укажите параметры CommuniGate Pro** укажите параметры сервера CommuniGate Pro:
     - выберите **Одиночная установка** в случае одиночного сервера или **Кластер** в случае серверного кластера;
     - в поле **IP-адрес или имя хоста** укажите IP-адрес или имя регистрируемого сервера;
     - в поле **Отображаемое имя сервера** укажите имя, под которым сервер будет отображаться в системе;
     - в полях **Логин** и **Пароль** укажите имя и пароль пользователя сервера CommuniGate Pro.

© ООО Киберпротект, 2026



4. По окончании ввода данных нажмите **Добавить**.
5. Убедитесь, что новое устройство отображается в разделе **Устройства** веб-консоли.

12.2.7 Резервное копирование CommuniGate Pro

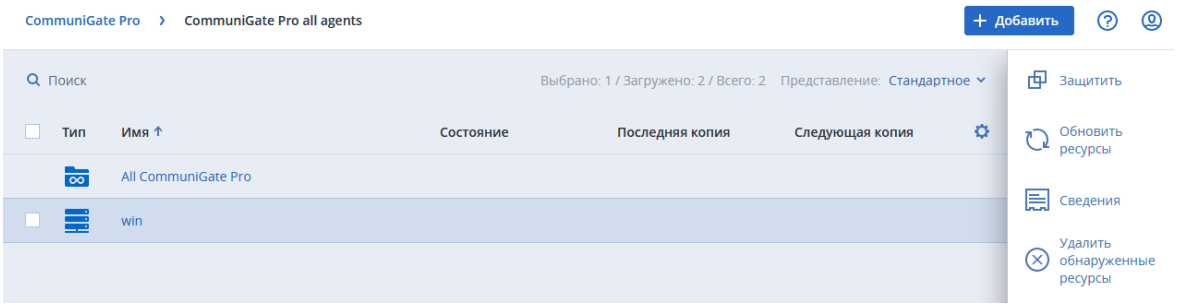
Резервное копирование данных CommuniGate Pro позволяет защитить домены и отдельные почтовые ящики. Для защиты данных необходимо сначала создать план защиты.

12.2.7.1 Создание плана защиты для CommuniGate Pro

Для создания плана защиты выполните следующие действия:

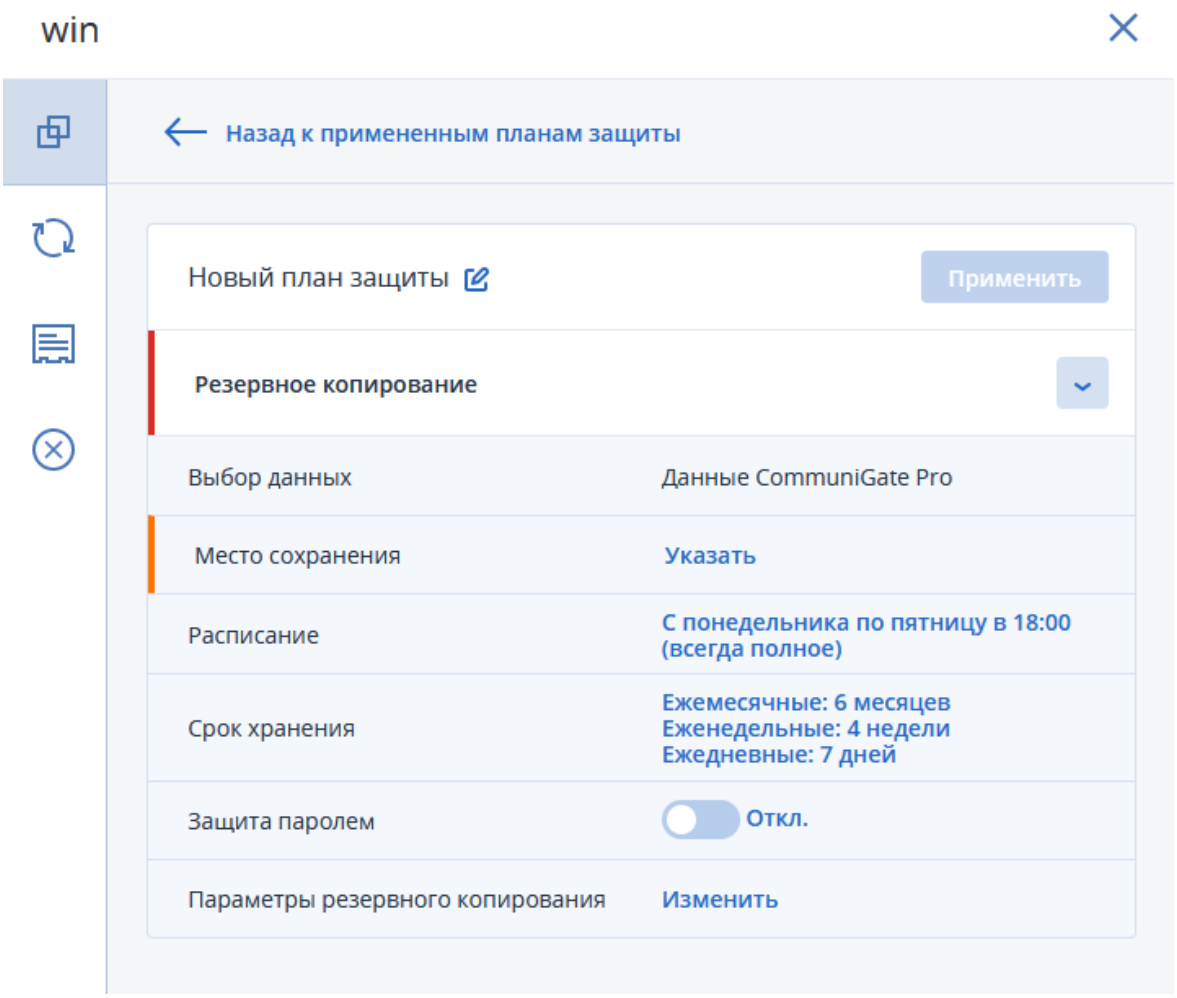
© ООО Киберпротект, 2026

1. Перейдите в **Устройства**.
2. Выберите из списка устройство, которое вы хотите защитить, и щелкните по строке, в которой находится это устройство.
3. Перейдите на вкладку справа **Защитить**.



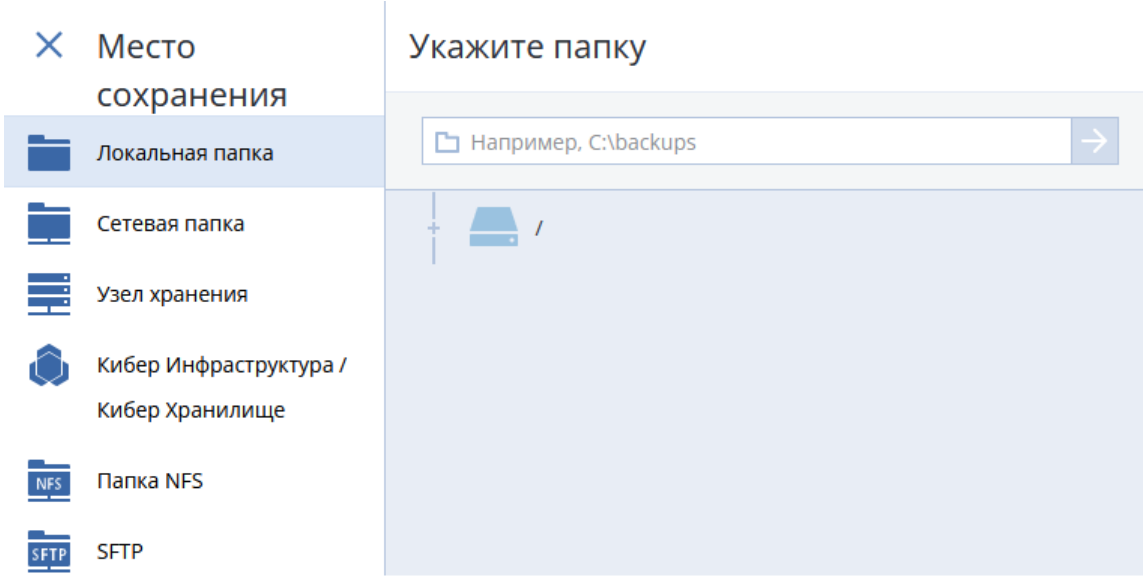
4. Нажмите **Создать план**.

Откроется окно создания плана.



© ООО Киберпротект, 2026

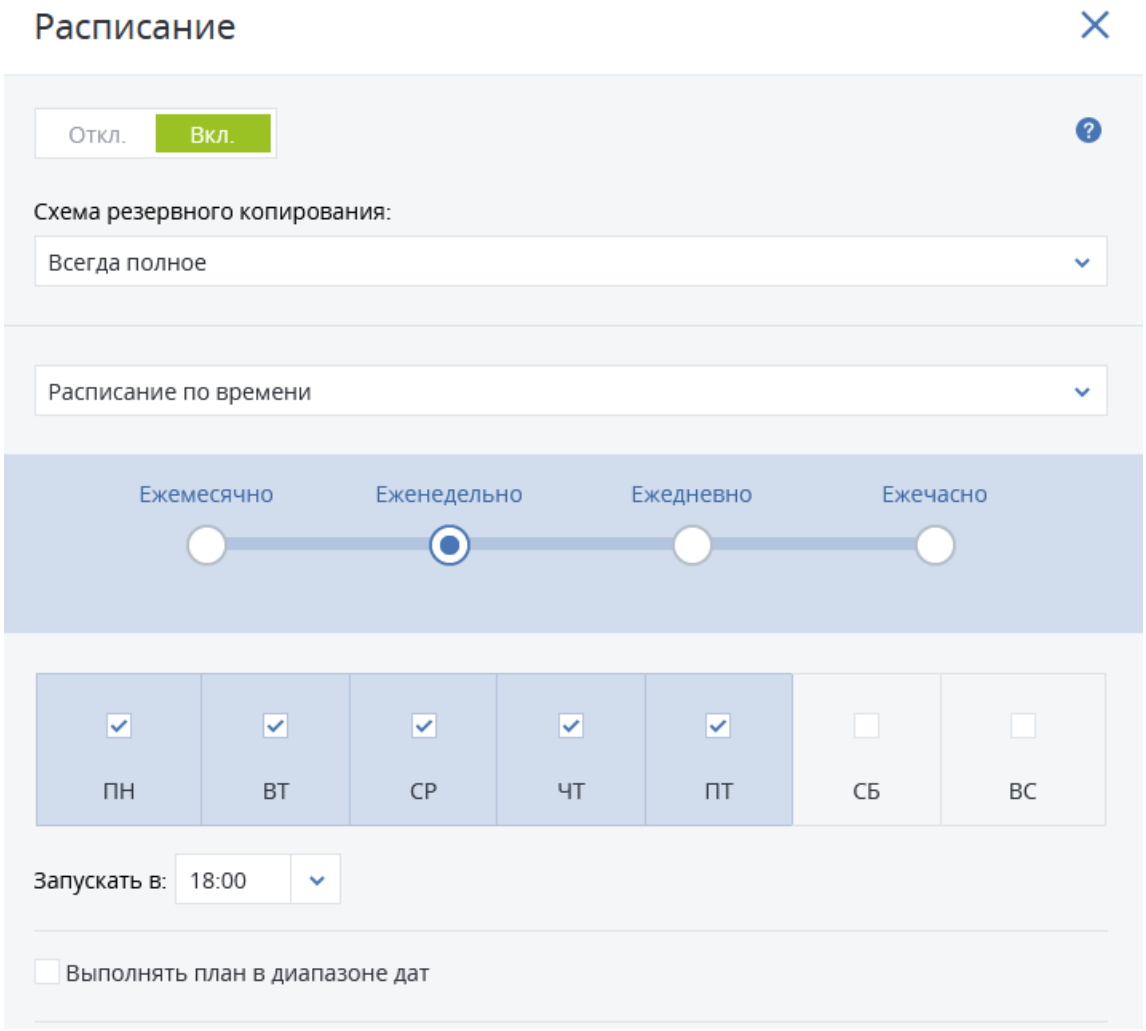
5. Заполните данные в окне создания плана защиты:
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.



   Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места сохранения" (стр. 278).

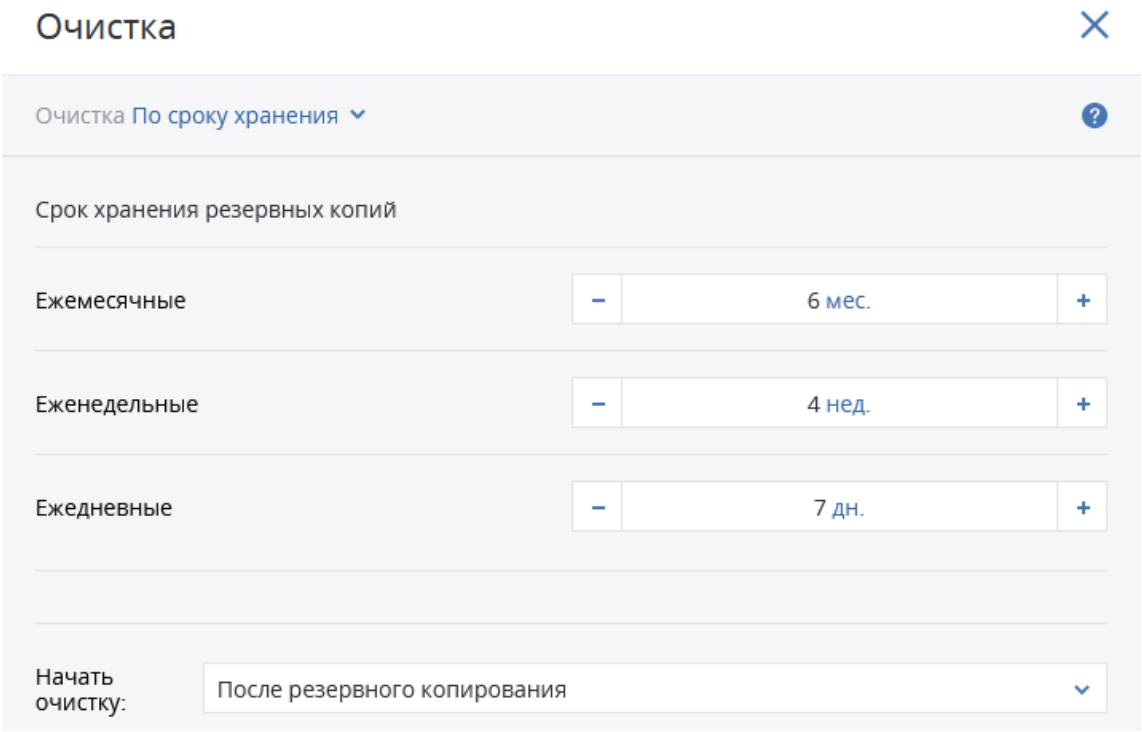
© ООО Киберпротект, 2026

- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.

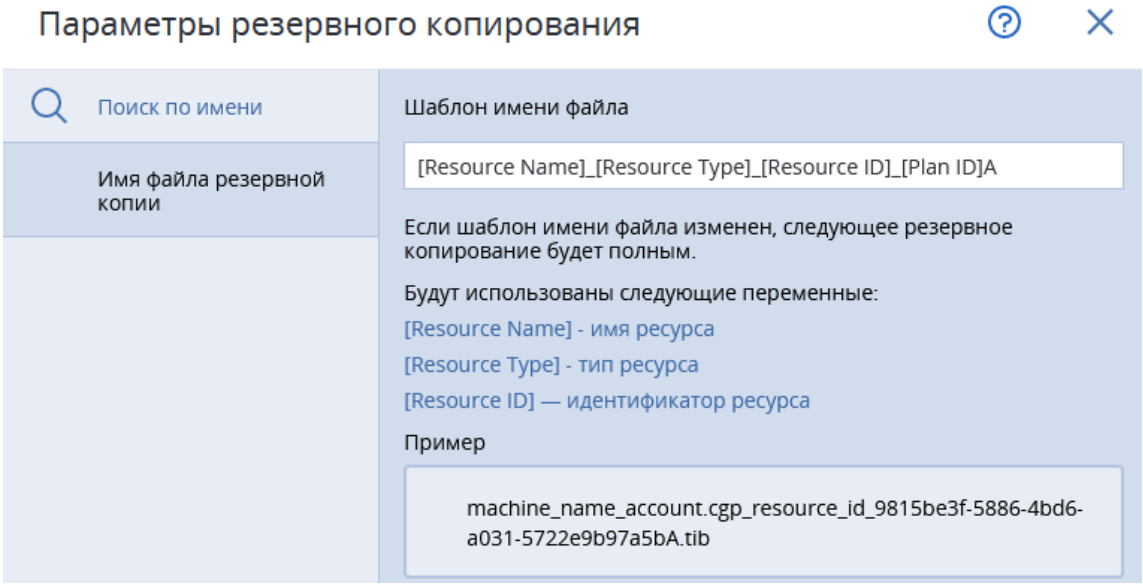


- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.

© ООО Киберпротект, 2026



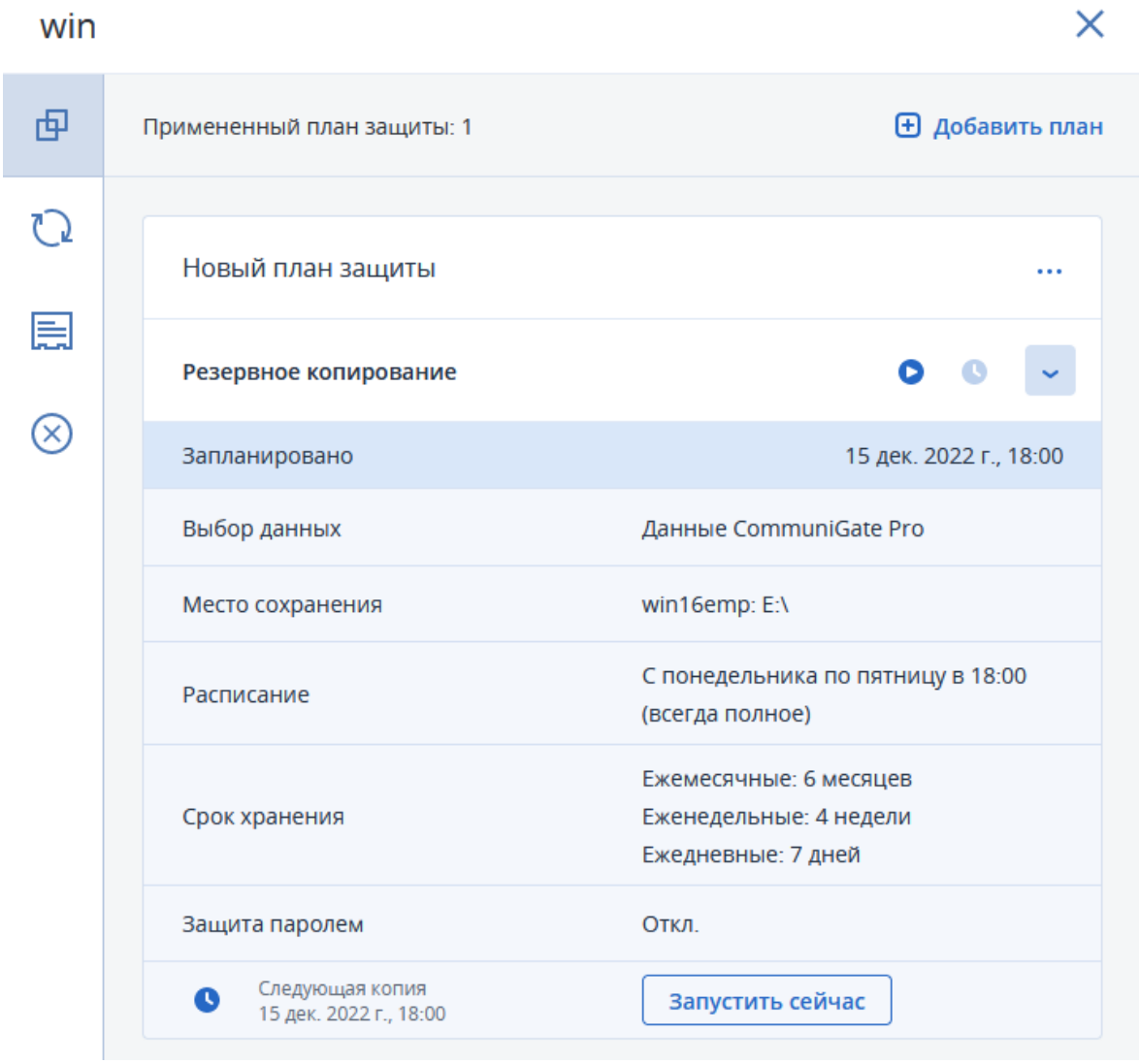
- [Необязательно] В поле **Параметры резервного копирования** укажите параметры для автоматического наименования файла резервного копирования.



  Обратите внимание на то, что в случае изменения этих параметров следующее резервное копирование будет полным.

6. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов.

© ООО Киберпротект, 2026



См. также информацию в разделе "План защиты и модули" (стр. 224).

12.2.7.2 Настройка плана защиты для CommuniGate Pro

Для настройки плана защиты CommuniGate Pro перейдите на вкладку **Планы** в меню веб-консоли.

Отметьте план, который вы хотите настроить. В меню справа появится список действий, доступных для этого плана.

В меню доступны следующие действия:

- **Сведения** – подробные сведения о плане;
- **Остановить** – остановка выполнения плана;
- **Изменить** – изменение плана;
- **Действия** – список действий, связанных с планом;
- **Оповещения** – список оповещений, связанных с планом;

© ООО Киберпротект, 2026

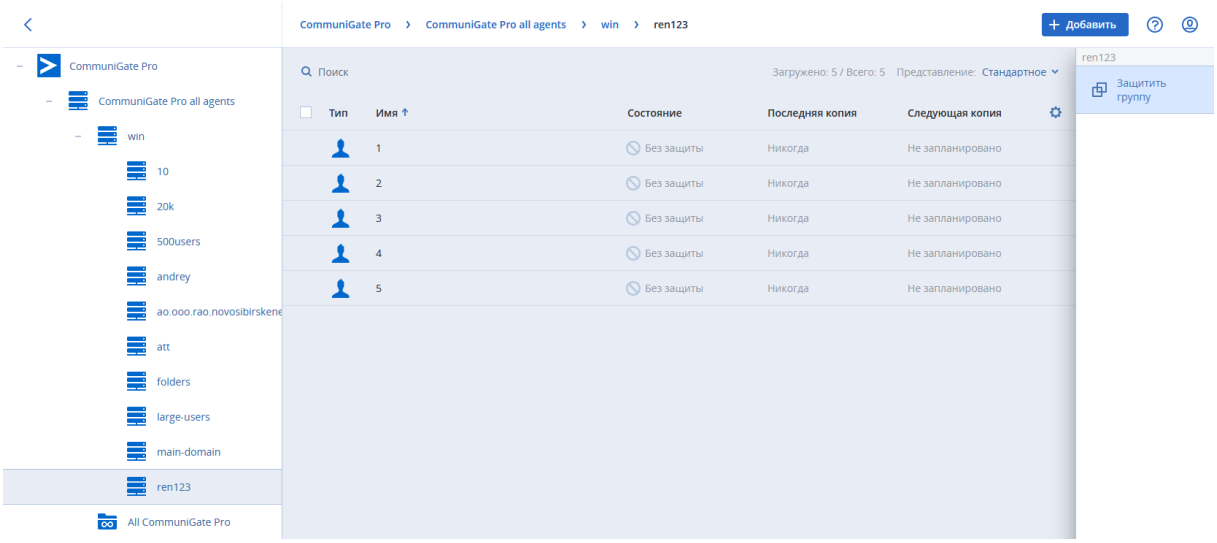
- **Клонировать** – клонирование плана на другое устройство;
- **Экспорт** – экспорт плана в файл;
- **Отключение (Включение)** – включение/отключение плана одной кнопкой;
- **Удаление** – удаление плана.

Подробнее о действиях с планами защиты см. в разделе "Операции с планами защиты" (стр. 227).

12.2.7.3 Резервное копирование данных CommuniGate Pro

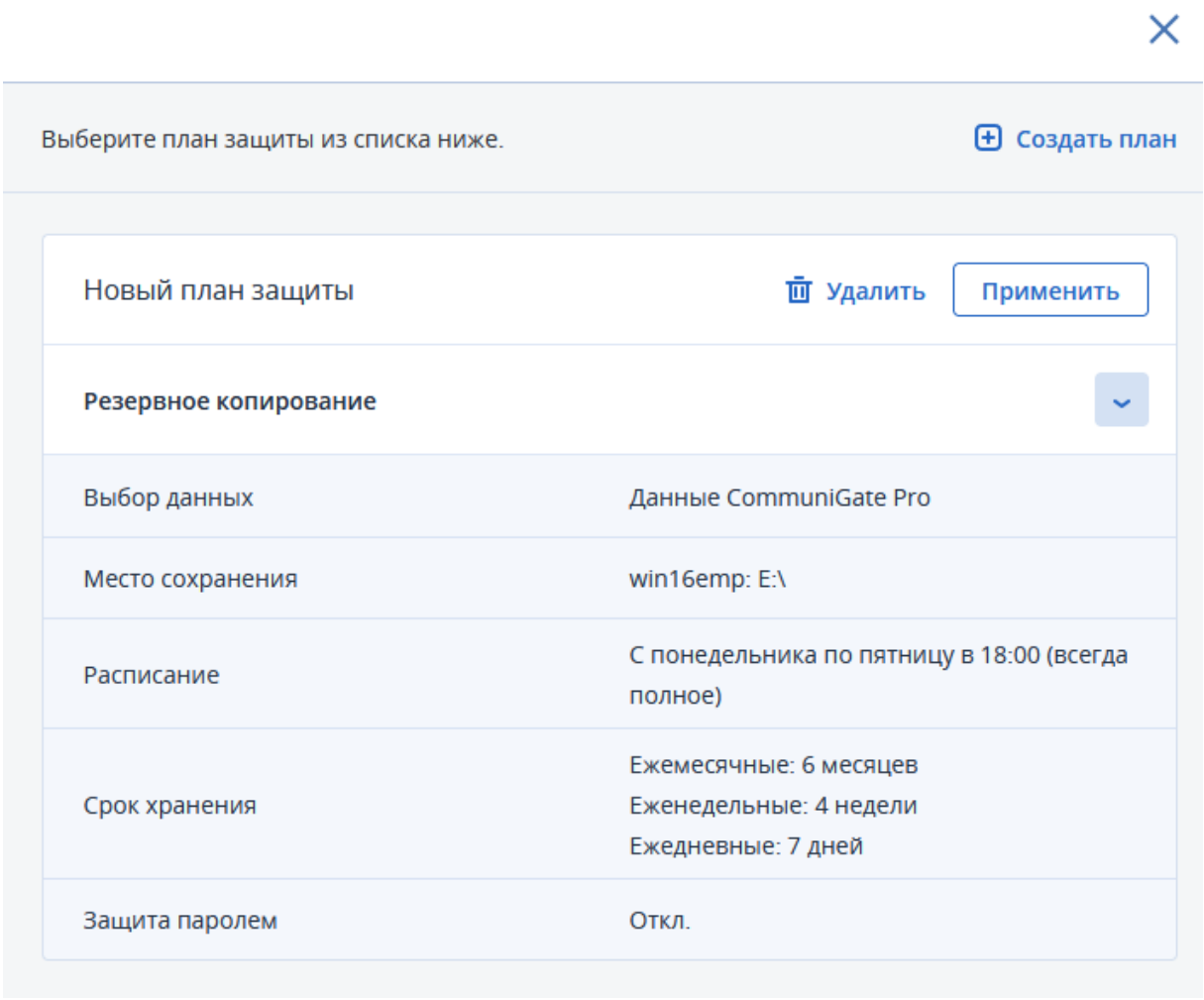
Резервное копирование домена

Чтобы защитить домен, в списке доменов щелкните по строке, содержащей название домена, и перейдите на вкладку **Защитить группу** в меню справа.



В окне выбора плана защиты в списке планов защиты выберите подходящий план и щелкните **Применить**.

© ООО Киберпротект, 2026

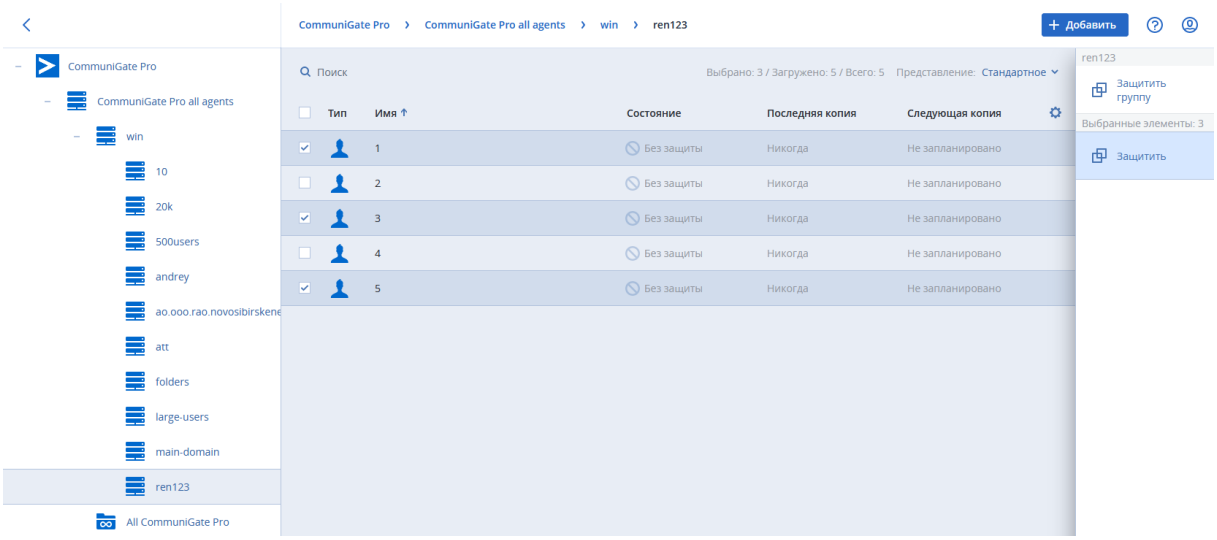


Резервное копирование почтового ящика

Чтобы защитить почтовый ящик, раскройте список почтовых ящиков в домене, щелкните по строке, содержащей имя домена, и перейдите на вкладку **Защитить** в меню справа.

Чтобы выбрать несколько почтовых ящиков, входящих в домен, щелкните по домену, затем отметьте флажок в окошке рядом с полем **Тип** и снимите флажки с почтовых ящиков, которые вы не хотите защищать. Перейдите на вкладку **Защитить** в меню справа.

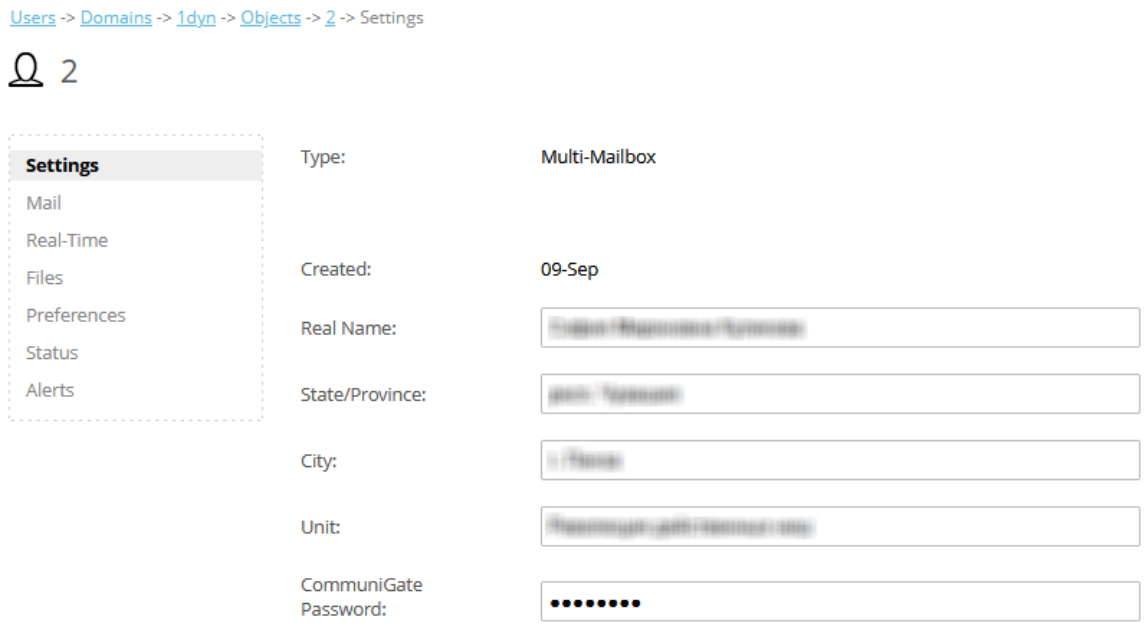
© ООО Киберпротект, 2026



В окне выбора плана защиты в списке планов защиты выберите подходящий план и щелкните **Применить**.

Примечание

Защита настроек пользователя выполняется вместе с защитой его данных (почтового ящика). При этом защита касается только системных настроек. Эти настройки расположены в панели администратора CommuniGate Pro на следующей странице: **Users** -> **Domains** -> **Domain_name** -> **Objects** -> **Object_name** -> **Settings**.



Резервное копирование по требованию

Резервное копирование по требованию представляет собой запуск выбранного плана защиты вне очереди. Чтобы выполнить резервное копирование по требованию:

© ООО Киберпротект, 2026

- щелкните по строке, содержащей название почтового ящика или домена
- перейдите на вкладку **Защитить** для почтового ящика или **Защитить группу** для домена в меню справа
- в строке **Резервное копирование** или в нижней части вкладки нажмите кнопку **Запустить сейчас**.

12.2.7.4 Резервное копирование больших объемов данных CommuniGate Pro

В Кибер Бэкап для резервного копирования данных CommuniGate Pro большого объема существуют следующие возможности:

- Резервное копирование с использованием нескольких агентов.
- Резервное копирование кластерных конфигураций.

Использование нескольких агентов

Для резервного копирования большого количества данных можно использовать сразу несколько агентов.

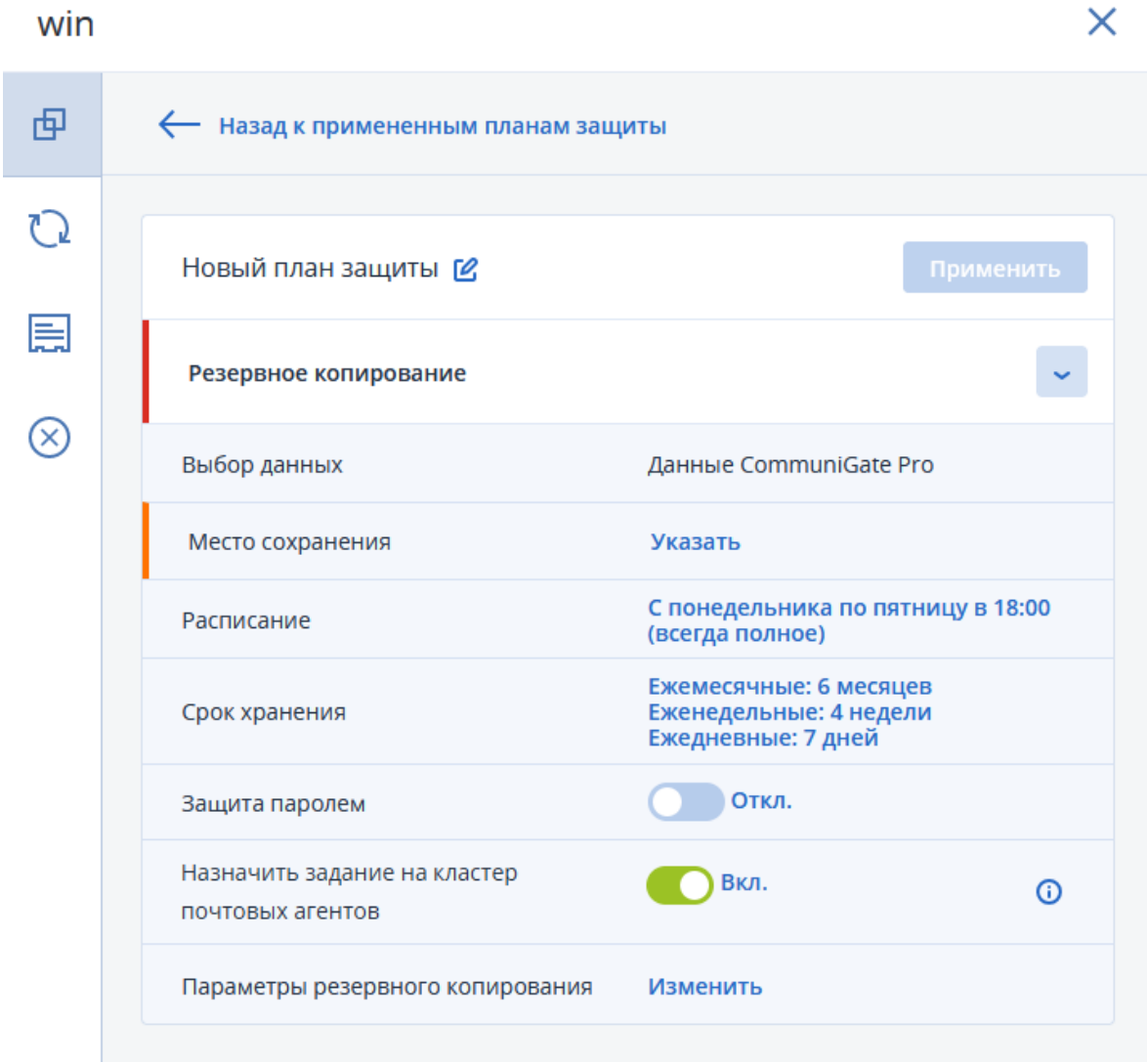
Для этого выполните следующие действия:

1. Зарегистрируйте необходимое количество агентов CommuniGate Pro (см. раздел "Установка CommuniGate Pro" (стр. 508)). Агенты должны быть версии 17.3 или новее.
2. Создайте план резервного копирования для агентов. В резервном копировании будут участвовать все агенты CommuniGate Pro, зарегистрированные в Кибер Бэкап.

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** -> **CommuniGate Pro**.
2. Выберите ресурсы CommuniGate Pro, для которых вы хотите создать план защиты.
3. На вкладке справа нажмите **Защитить** или **Защитить группу** (если выбрана группа почтовых ресурсов).

© ООО Киберпротект, 2026



4. Введите данные в окне создания плана защиты:
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, SFTP, папка NFS (только для Linux).

     Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места сохранения" (стр. 278).
   - В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.
   - В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.
   - В поле **Назначить задание на кластер почтовых агентов** включите переключатель, чтобы назначить план защиты всем зарегистрированным агентам.
   - [Необязательно] В поле **Параметры резервного копирования** укажите метод разбиения резервных копий на меньшие по размеру фрагменты, параметры обработки ошибок и уровень сжатия резервных копий.

© ООО Киберпротект, 2026

5. По окончании настройки плана нажмите **Применить**.

При резервном копировании несколькими агентами балансировка нагрузки происходит в режиме циклического перебора (round robin).

Резервное копирование кластеров CommuniGate Pro

При необходимости обслуживания большого количества (более 150–200 тыс.) почтовых ящиков пользователей или в случае серьезной сетевой нагрузки становится целесообразным использовать многосерверные кластерные конфигурации.

Кибер Бэкап поддерживает резервное копирование и восстановление серверных кластеров CommuniGate Pro.

Требования

Для резервного копирования кластерных конфигураций вам понадобятся установленные и настроенные системы:

- Кибер Бэкап версии 18.0 и выше;
- CommuniGate Pro версии не ниже 6.5.2.

Поддерживаются операционные системы:

- Windows;
- Linux.

Возможности

- Поддержка динамических и статических кластеров.
- Обнаружение ресурсов автоматически и вручную.
- Все операции, включая обнаружение ресурсов, резервное копирование и восстановление, используют любой из доступных серверов кластера. При неисправности какого-либо сервера следующая операция будет выполнена на одном из доступных серверов кластера.
- При необходимости любой сервер кластера может быть зарегистрирован как отдельный сервер. В этом случае будут доступны как домены кластера, так и локальные домены сервера.
- Поддерживается полное и инкрементальное резервное копирование.
- Поддерживается резервное копирование сервера (с помощью дискового и файлового резервного копирования).
- Доступен поиск по именам пользователей в архиве, при условии что имя пользователя содержится в имени архива.

© ООО Киберпротект, 2026

Ограничения

- Агент Кибер Бэкап может работать только с одним сервером (хостом) CommuniGate Pro.
- Все серверы кластера должны иметь доступ к агенту. Если агент не имеет доступа к какому-либо серверу, этот сервер будет помечен как **offline**.
- Все серверы кластера должны разрешать авторизацию одного и того же пользователя с одним и тем же паролем.
- Не поддерживается работа через балансировщик нагрузки кластера.
- При обнаружении ресурсов доступны только ресурсы динамического кластера. Ресурсы, принадлежащие определенному серверу, недоступны для обнаружения.
- Для резервного копирования доступны только домены, принадлежащие динамическому кластеру. Домены, принадлежащие определенному серверу, недоступны для резервного копирования.
- Не поддерживается резервное копирование сервера в кластерной конфигурации (также см. главу "Возможности").

Установка

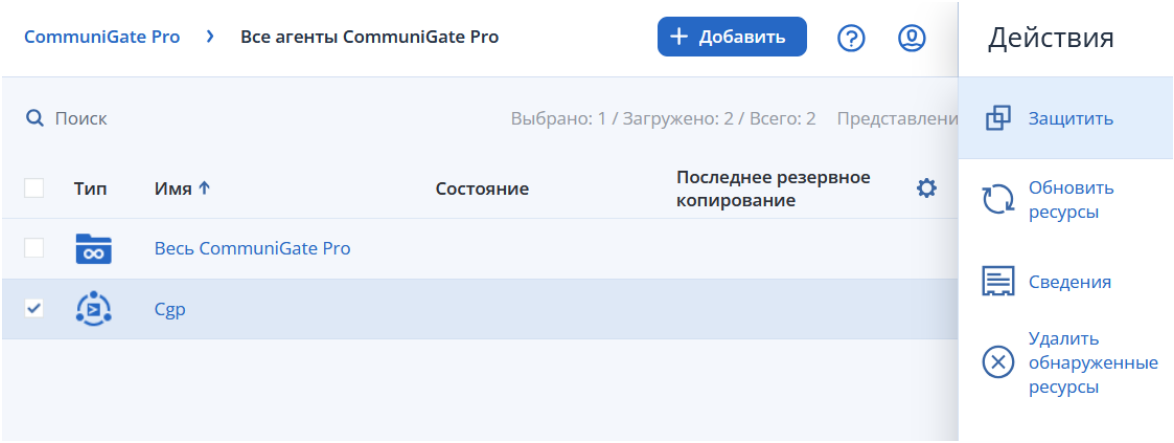
Для установки см. раздел "Установка CommuniGate Pro" (стр. 508).

Для регистрации кластера CommuniGate Pro укажите данные любого сервера, входящего в кластер. Этот сервер должен быть доступен для агента. Процесс регистрации кластерного сервера аналогичен процессу регистрации одиночного сервера.

Резервное копирование кластера

Для резервного копирования кластера выполните следующие действия:

1. В веб-консоли перейдите на вкладку **Устройства** -> **CommuniGate Pro**.
2. Выберите в списке кластер, который хотите защитить.



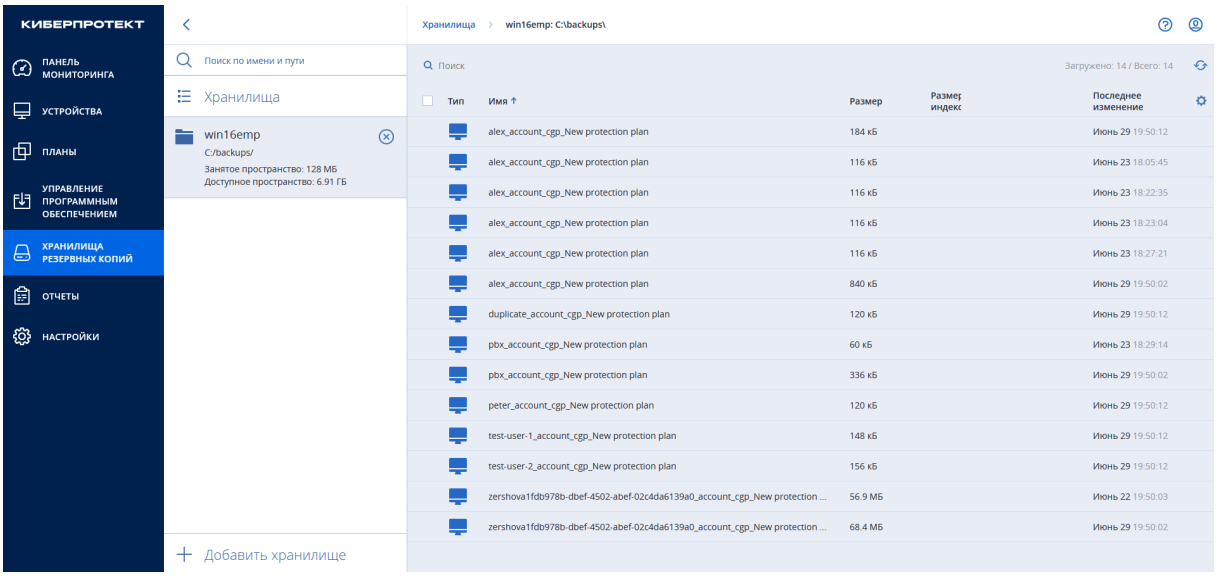
3. [Необязательно] Для обнаружения новых ресурсов нажмите **Обновить ресурсы**.
4. Щелкните в меню справа **Защитить**.
5. Создайте новый план защиты или выберите существующий.

© ООО Киберпротект, 2026

6. Укажите необходимые настройки плана. Поддерживаются следующие места сохранения: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SMTP.
7. По окончании настройки плана нажмите **Применить**.

12.2.7.5 Резервные копии CommuniGate Pro

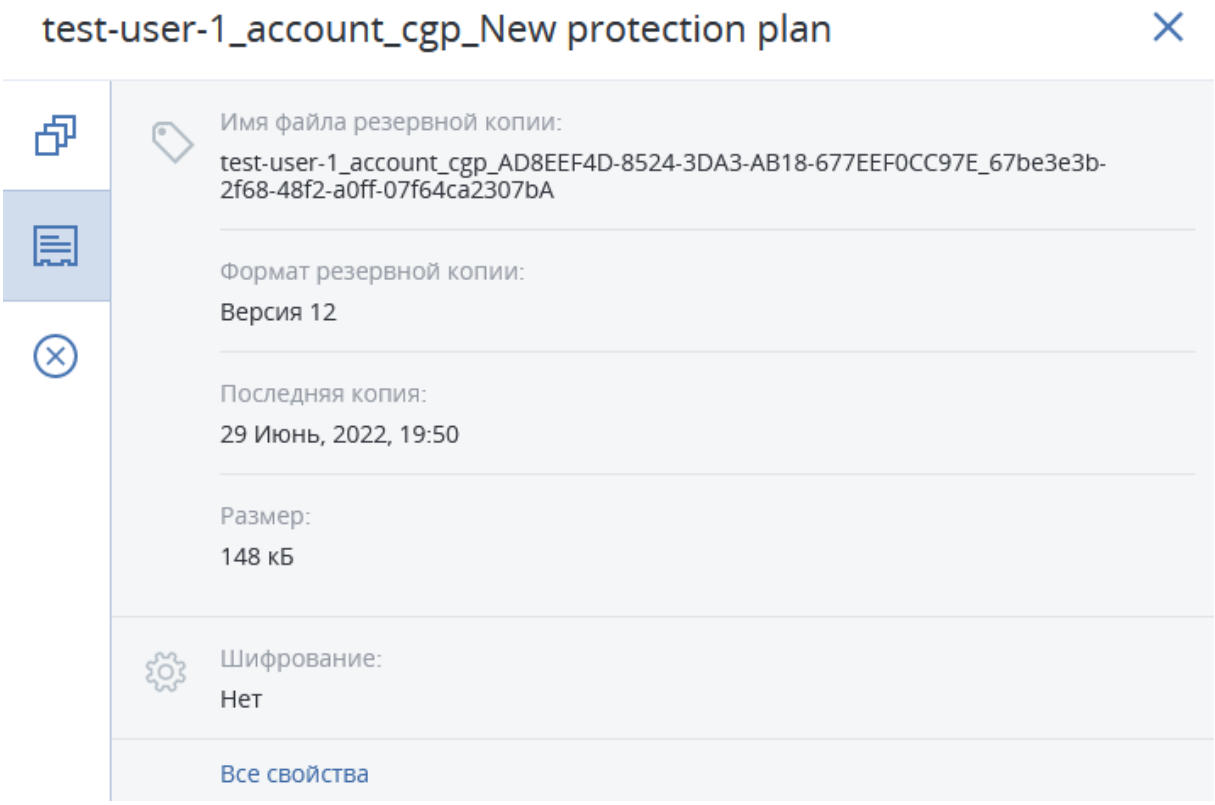
Чтобы посмотреть список резервных копий компьютеров, перейдите на вкладку **Хранилища резервных копий**.



Чтобы посмотреть список резервных копий для компьютера, щелкните на строку с названием компьютера и затем перейдите на вкладку **Показать резервные копии** в меню справа. Откроется список резервных копий. Из этого меню также можно восстановить одну из резервных копий для этого компьютера.

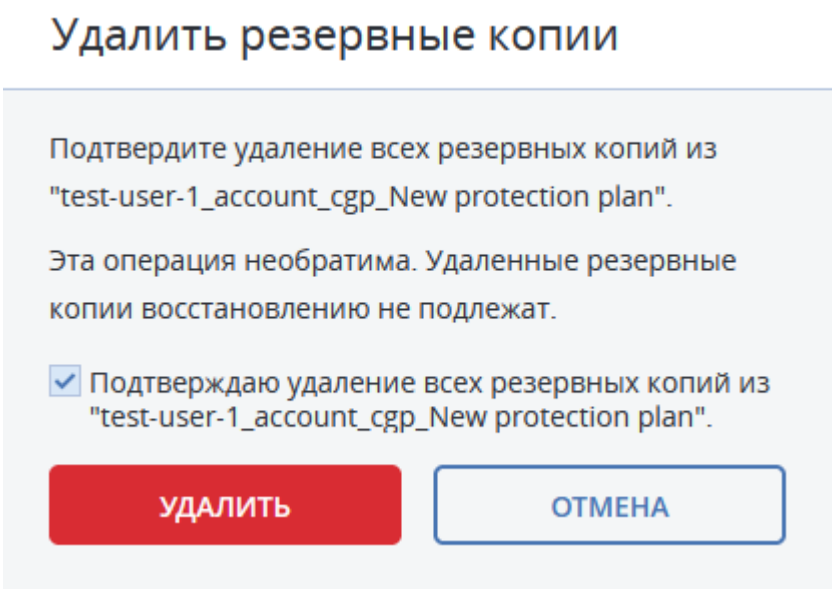
Чтобы посмотреть сведения о резервной копии, щелкните по строке, содержащей название резервной копии, и перейдите на вкладку **Сведения** в меню справа.

© ООО Киберпротект, 2026



Подробная информация доступна по ссылке **Все свойства**.

Чтобы удалить резервную копию, перейдите на вкладку **Удалить** в меню справа.



Для подтверждения удаления отметьте флажок в поле и нажмите **Удалить**. Выбранная резервная копия после удаления исчезнет из списка резервных копий.

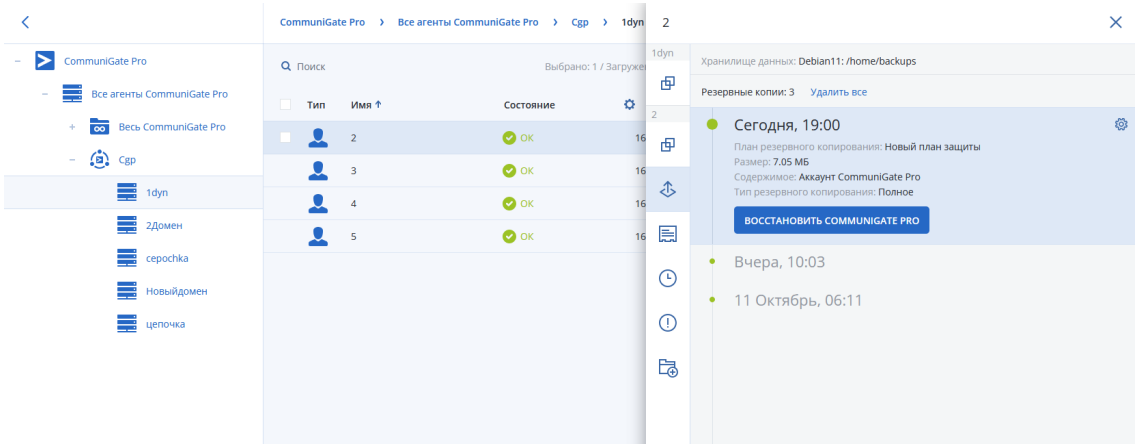
Для удаления резервной копии см. также Восстановление CommuniGate Pro.

© ООО Киберпротект, 2026

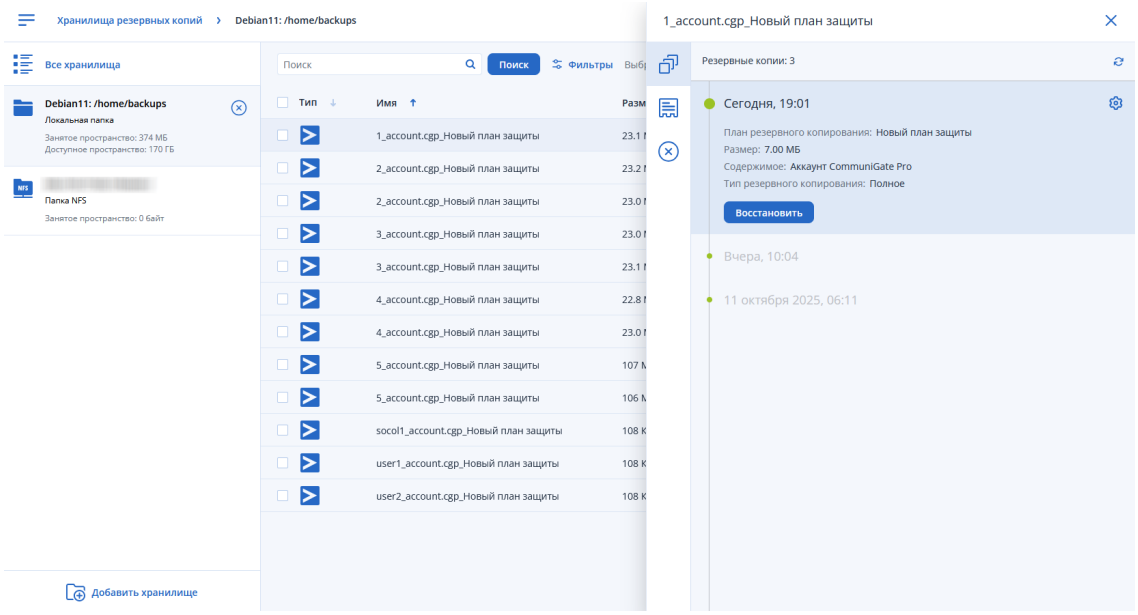
12.2.8 Восстановление CommuniGate Pro

Восстановление данных CommuniGate Pro

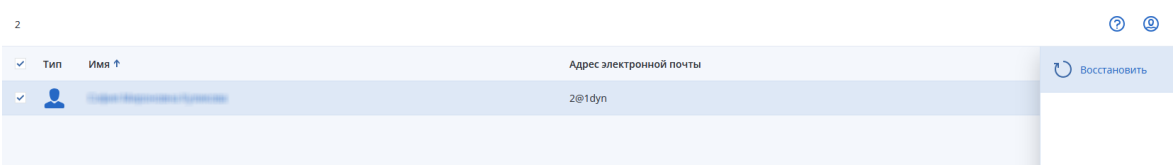
1. Выполните одно из следующих действий:
   a. Перейдите в **Устройства** -> **CommuniGate Pro**, щелкните кластер, сервер или домен, данные в котором хотите восстановить, выберите в списке нужный аккаунт (учетную запись), справа в меню щелкните **Восстановление** и далее **Восстановить CommuniGate Pro**.



   b. Перейдите в **Хранилище резервных копий**, щелкните хранилище с резервными копиями, выберите в списке нужный аккаунт и нажмите **Восстановить**.

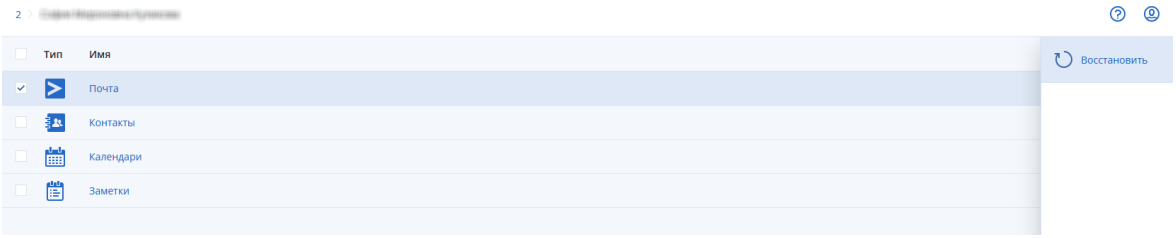


2. Для восстановления всех данных пользователя отметьте галочкой имя пользователя и нажмите **Восстановить**. Иначе просто щелкните имя пользователя.



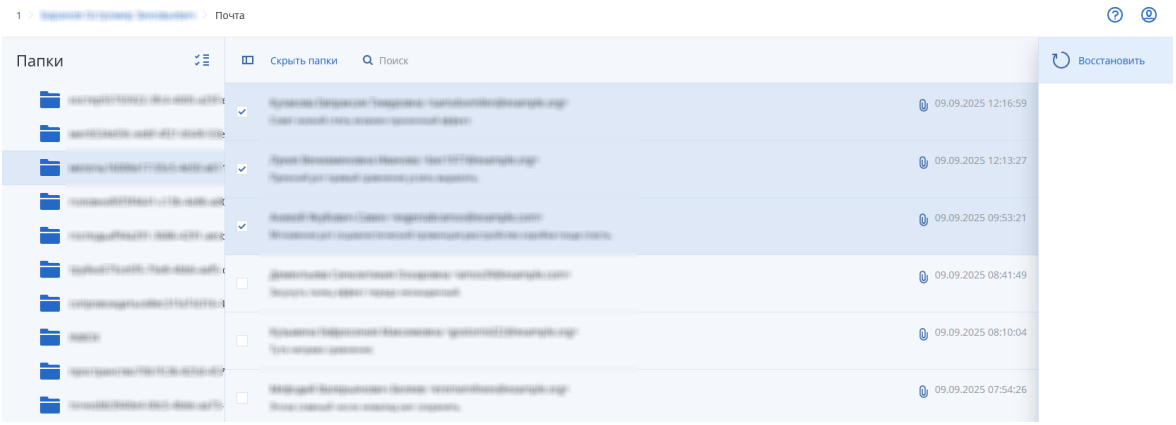
© ООО Киберпротект, 2026

3. Для восстановления всех данных одного типа отметьте галочкой тип восстанавливаемых данных (**Почта**, **Контакты**, **Календари**, **Заметки**).



Для восстановления определенных данных щелкните на названии типа нужных данных (например, **Почта**) и далее в списке отметьте галочками те данные (например, письма), которые необходимо восстановить.

Примечание
Восстановление на новый сервер можно выполнить только при восстановлении всех данных пользователя или всех данных одного типа.

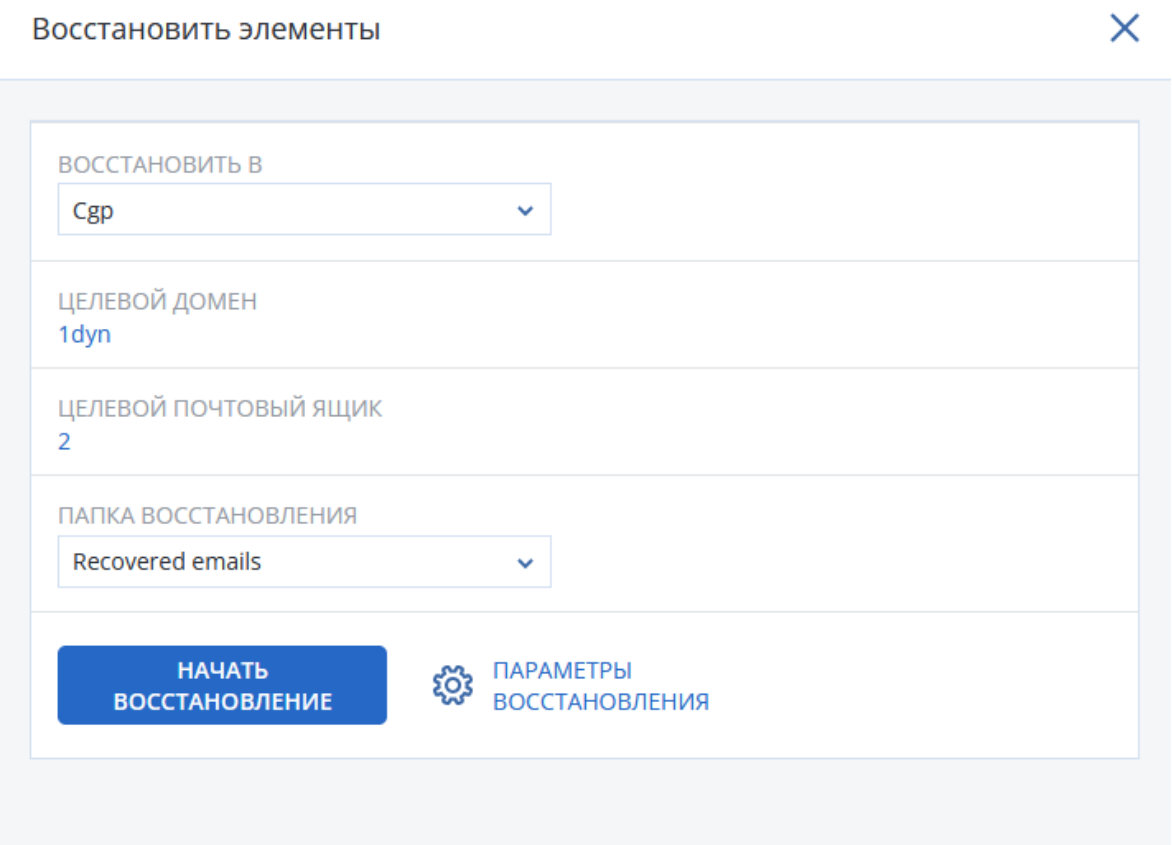


Для просмотра содержимого письма нажмите справа **Показать содержимое**. Для скачивания вложения щелкните по этому вложению.

Для поиска нажмите значок поиска сверху. Для почты доступен расширенный поиск, для его настройки нажмите значок выпадающего списка в строке поиска.

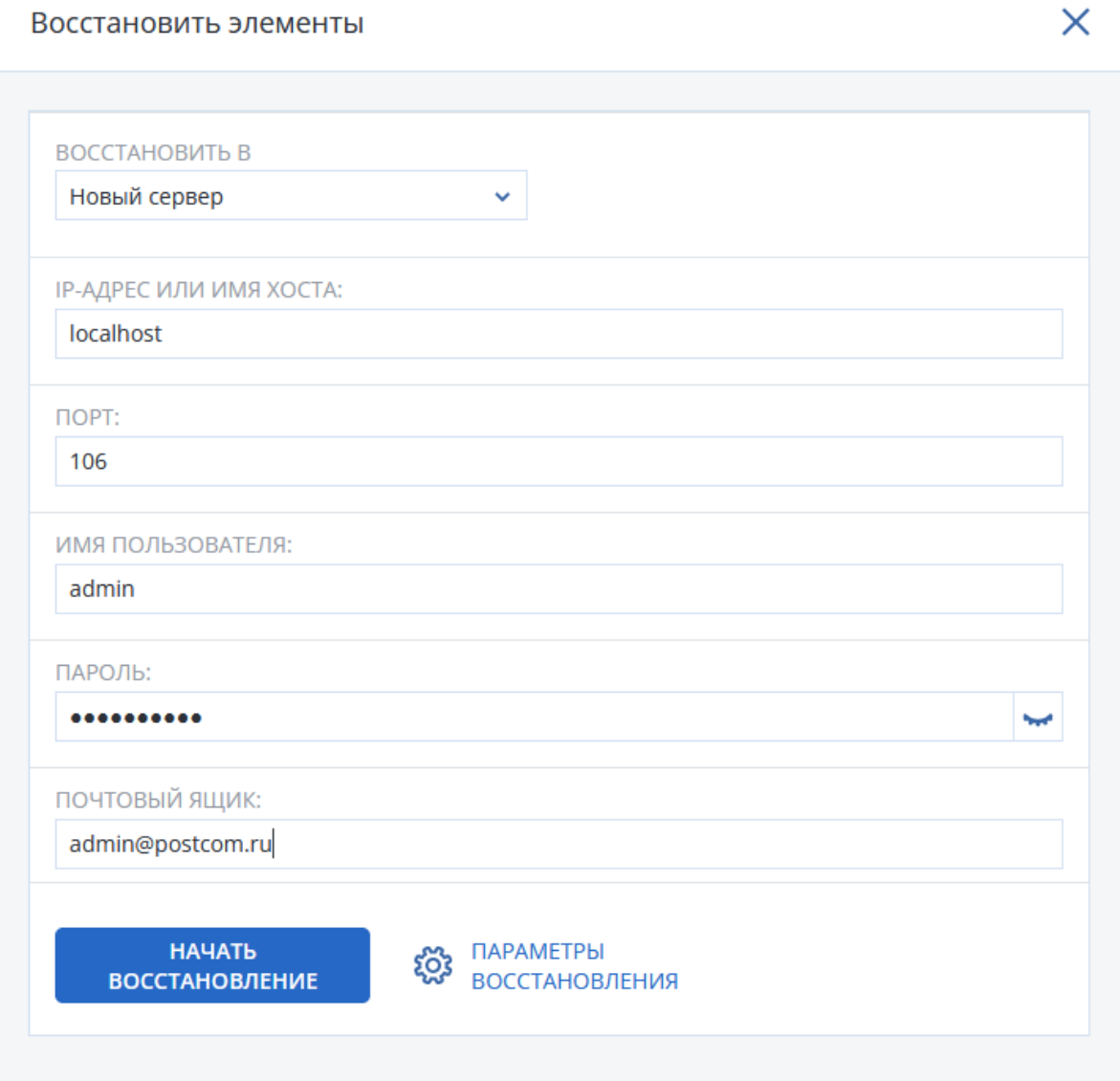
4. Нажмите **Восстановить**.
5. На экране **Восстановить элементы** укажите место для восстановления:
   a. Существующий сервер или новый сервер;
   b. Домен (из существующих);
   c. Почтовый ящик (из существующих);
   d. Папка для восстановления (если происходит восстановление выбранных вами данных одного типа).

© ООО Киберпротект, 2026



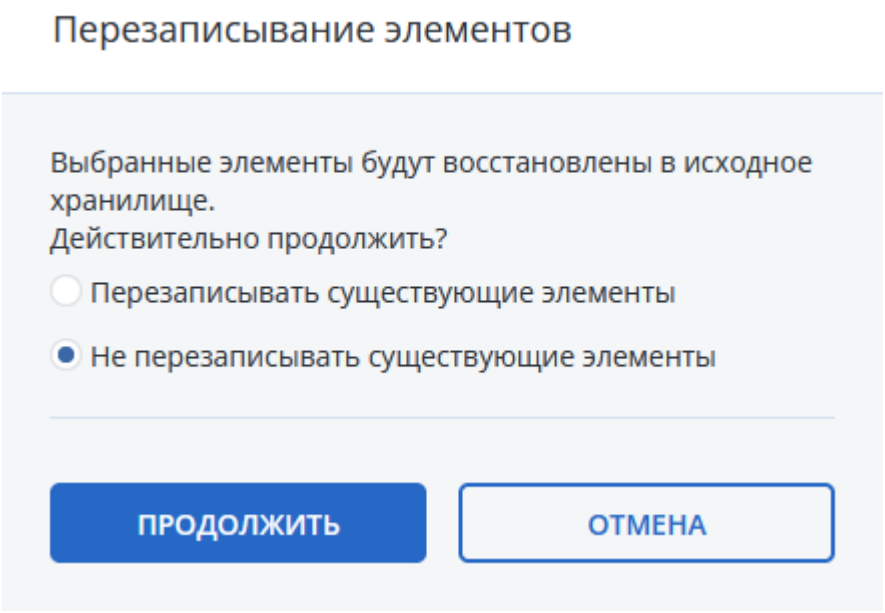
При восстановлении на новый сервер укажите параметры нового хранилища.

© ООО Киберпротект, 2026



6. Закончив выбор, нажмите **Начать восстановление**.
7. На экране **Перезаписывание элементов** подтвердите или отклоните перезапись существующих данных при восстановлении.

© ООО Киберпротект, 2026



Примечание
Перезапись draft не работает должным образом из-за ограничений в CommuniGate Pro.

Внимание
При выборе перезаписи существующие данные будут уничтожены!

Примечание
При перезаписи уничтожены будут данные, совпадающие с данными из архива. Если в почтовых ящиках с момента создания последней резервной копии появились новые данные, то они не будут уничтожены.

Ход выполнения восстановления показан на вкладке **Действия**.

На вкладке **Восстановление** доступно также удаление резервной копии.

Удаление резервной копии

1. Щелкните резервную копию, которую хотите удалить.
2. Щелкните значок настройки справа вверху.
3. Нажмите **Удалить**.

Чтобы удалить все резервные копии, во вкладке **Восстановление** щелкните ссылку **Удалить все**.

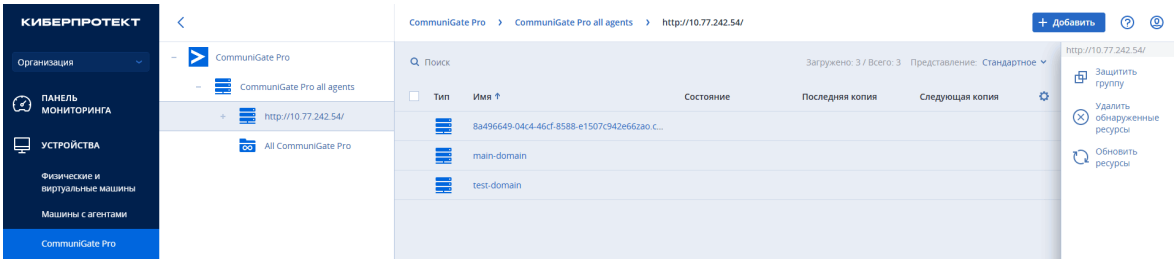
12.2.9 Удаление CommuniGate Pro

Вы можете удалить хост CommuniGate Pro отдельно, не удаляя сам агент и резервные копии.

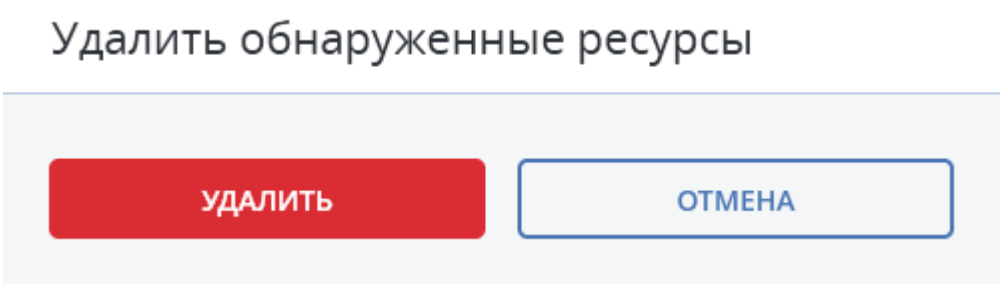
Порядок удаления хоста CommuniGate Pro

© ООО Киберпротект, 2026

1. В веб-консоли перейдите на вкладку **Устройства -> CommuniGate Pro**.
2. Отметьте хост CommuniGate Pro в списке.
3. В меню справа щелкните **Удалить обнаруженные ресурсы**.



В окне подтверждения удаления нажмите **Удалить**.



4. Устройство будет удалено из списка.

Примечание
Удаление машины не затрагивает агента и хранящиеся на ней резервные копии.

12.3 Защита VK WorkMail и VK WorkDisk

12.3.1 Зачем обеспечивать защиту VK WorkMail и VK WorkDisk

VK WorkMail – масштабируемое и отказоустойчивое решение корпоративного класса для работы с почтой, календарем, контактами и для просмотра документов.

VK WorkDisk – облачное хранилище, которое предоставляет возможность безопасного хранения и обмена файлами внутри организации.

С помощью Кибер Бэкап можно выполнять резервное копирование данных VK WorkMail и VK WorkDisk. Резервное копирование данных VK WorkDisk производится для пользователей, которые используют почтовый сервис VK WorkMail. При использовании Кибер Бэкап регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователей и различных сбоев. Удаленные элементы можно восстановить из резервной копии.

12.3.2 Что необходимо для резервного копирования

Для резервного копирования данных VK WorkMail понадобятся установленные и настроенные продукты:

© ООО Киберпротект, 2026

- Кибер Бэкап 16.5 или новее с лицензией Кибер Бэкап для почтового ящика (список лицензий см. в разделе "Издания и лицензии Кибер Бэкап" (стр. 16)).
- VK WorkMail.

Для резервного копирования данных VK WorkDisk понадобятся установленные и настроенные продукты:

- Кибер Бэкап 17.1 или новее с лицензией Кибер Бэкап для почтового ящика (список лицензий см. в разделе "Издания и лицензии Кибер Бэкап" (стр. 16)).
- VK WorkMail с подключенными ресурсами VK WorkDisk.

Поддерживаемые версии VK WorkMail указаны в разделе "Поддерживаемые почтовые сервисы" (стр. 35).

Для лицензирования VK WorkDisk используется лицензия VK WorkMail. Она автоматически подключается при создании плана защиты данных пользователя VK WorkDisk.

Для выполнения резервного копирования требуется установка агента.

Поддерживается установка агента для следующих операционных систем:

- Windows,
- Linux.

Полный список поддерживаемых операционных систем Windows и Linux см. в разделе "Агенты" (стр. 23).

12.3.3 Возможности

Кибер Бэкап обеспечивает резервное копирование и восстановление:

- данных пользователя VK WorkMail (почтовый ящик, календарь, профиль пользователя и адресная книга пользователя),

  Примечание
  При резервном копировании профиля пользователя создаются копии следующих настроек пользователя: Имя отправителя, Автоответчик, Уведомления, Отправка писем, После удаления письма, Адресная книга, Права доступа к почте.
  Резервное копирование файлов, прикрепленных к событиям в календаре, происходит при резервном копировании VK WorkDisk пользователя. При резервном копировании календаря создаются только копии ссылок прикрепленных событий на место хранения событий в VK WorkDisk пользователя.

- отдельных писем пользователей VK WorkMail,
- глобальных адресных книг VK WorkMail,
- данных пользователя VK WorkDisk,
- серверов VK WorkMail и VK WorkDisk.

© ООО Киберпротект, 2026

Также возможно скачивать отдельные файлы или данные пользователей из существующих резервных копий.

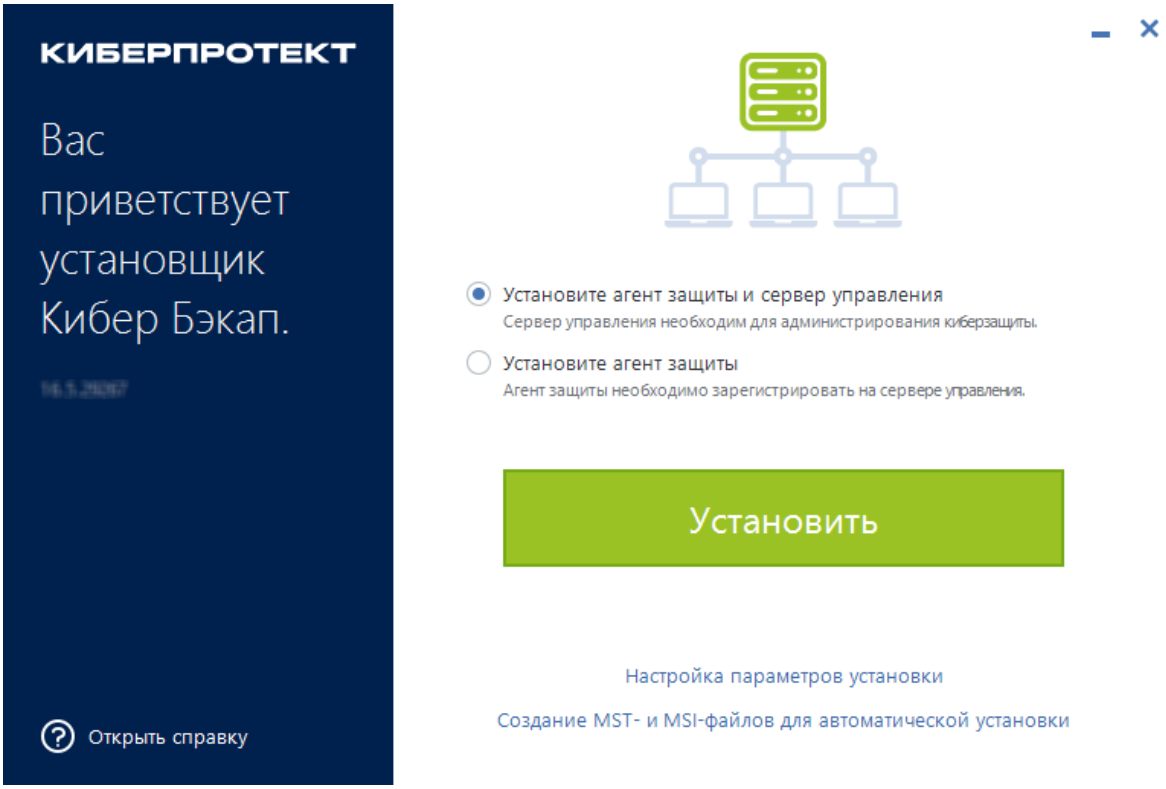
12.3.4 Установка VK WorkMail

Установка VK WorkMail включает в себя установку агента Кибер Бэкап и добавление хоста VK WorkMail. Добавление хоста возможно лишь после установки агента.

12.3.4.1 Установка агента для VK WorkMail

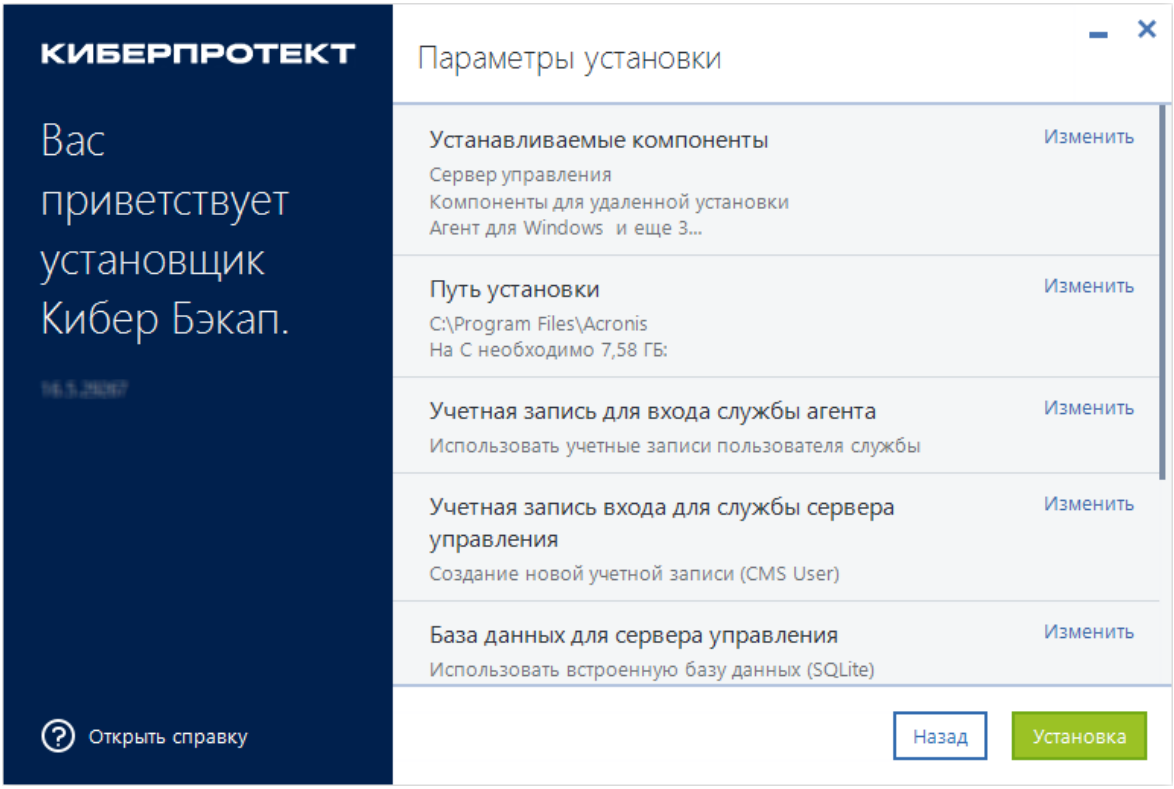
В этом разделе рассмотрена установка агента Кибер Бэкап для Windows. Для установки агента для Linux обратитесь к разделу "Установка агентов в ОС Linux вручную" (стр. 97).

1. Запустите установщик Кибер Бэкап.
2. Выберите **Настройка параметров установки**.

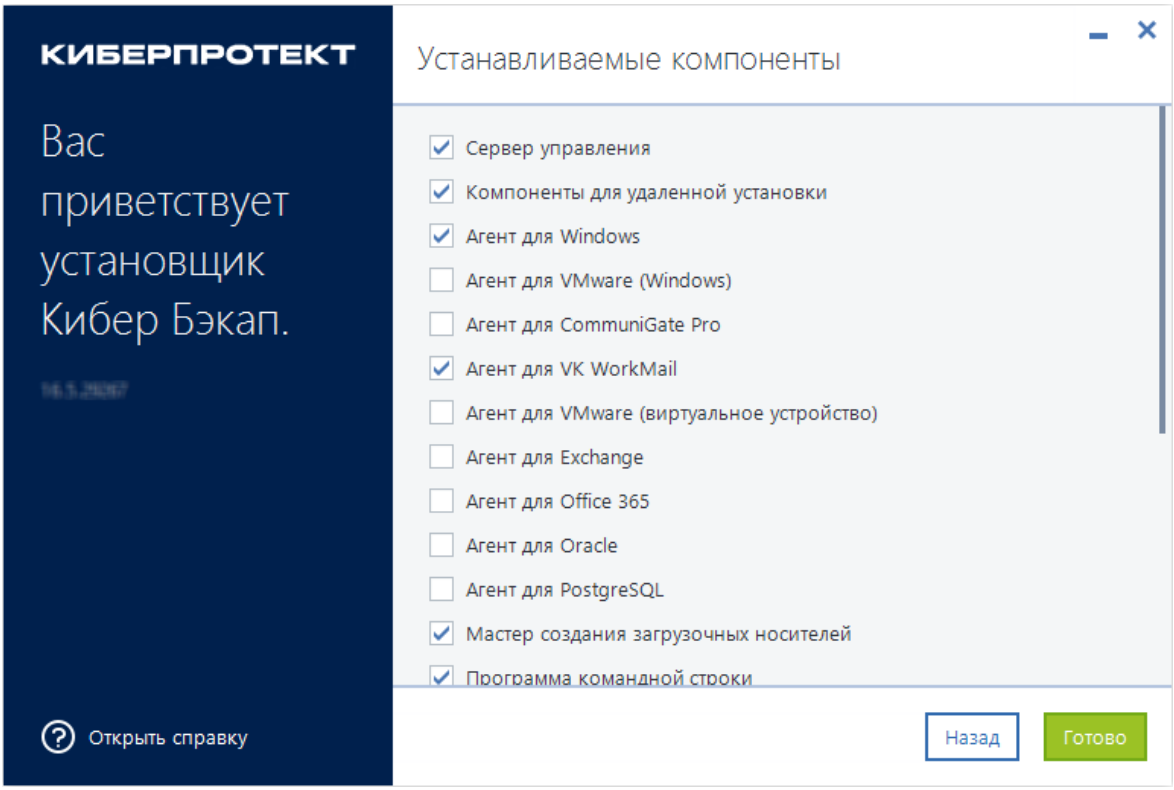


3. В блоке **Устанавливаемые компоненты** выберите **Изменить**.

© ООО Киберпротект, 2026



4. Отметьте в списке **Агент для VK WorkMail**.

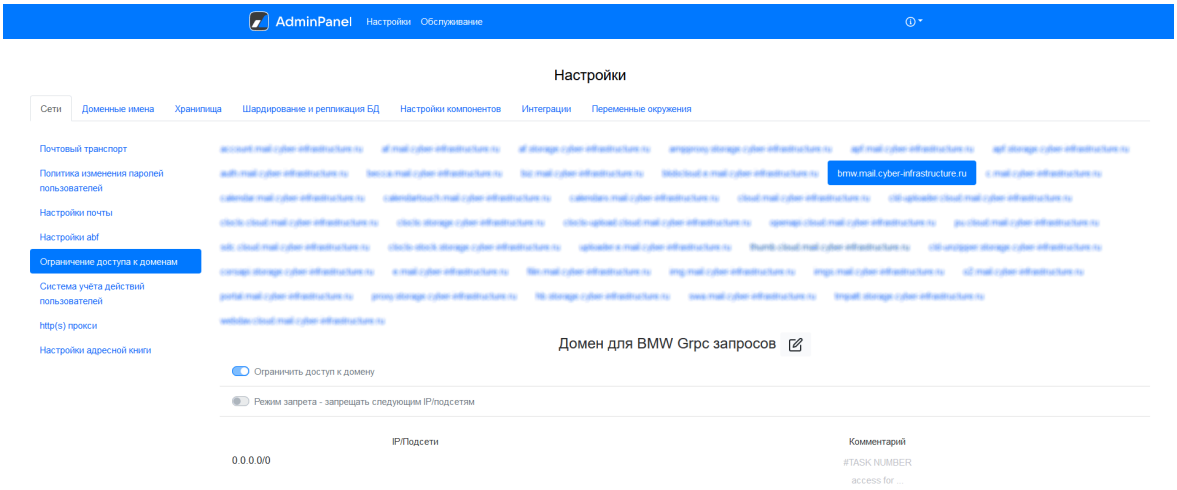


5. Щелкните **Готово**.

© ООО Киберпротект, 2026

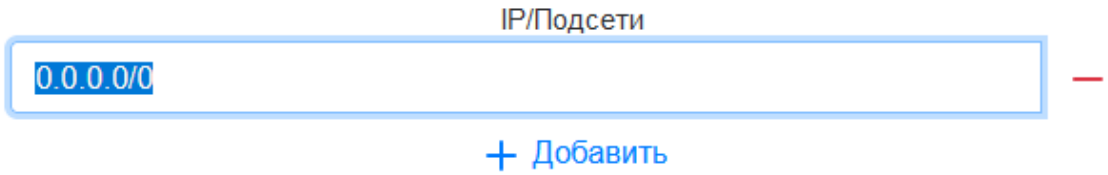
12.3.4.2 Настройка в панели администрирования VK WorkMail

1. Укажите настройки в панели администрирования VK WorkMail аналогично следующему примеру:



2. Для настройки IP-адреса нажмите значок редактирования

и введите IP-адрес компьютера, на который установлен агент для VK WorkMail.

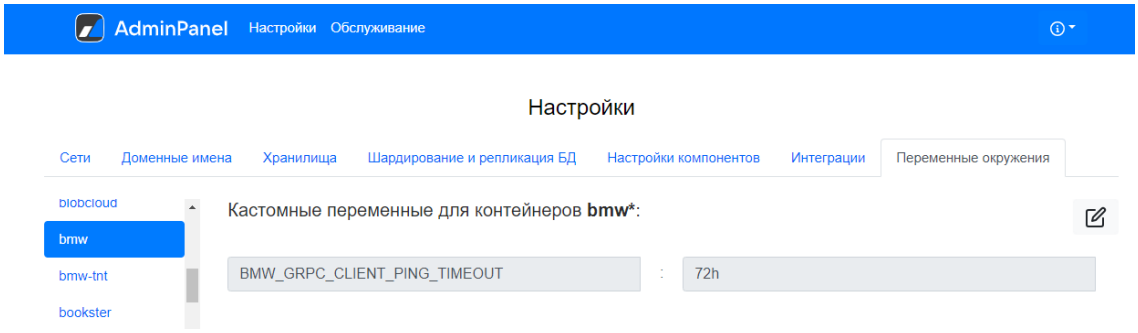


3. Нажмите **Сохранить**.
4. Добавьте переменные окружения:
   a. Перейдите в раздел **Настройки** и откройте вкладку **Переменные окружения**.
   b. В списке слева выберите контейнер **bmw** и создайте следующие переменные:
      - BMW_GRPC_CLIENT_PING_TIMEOUT, значение 72h. Переменная устанавливает время ожидания новой ленты при заполнении предыдущей.
      - BMW_GRPC_MAX_MESSAGE_SIZE_MB, значение 256. Переменная устанавливает максимальный размер писем для резервного копирования и восстановления.
      - AMELI_WORKERS, значение 10. Переменная необходима для ускорения взаимодействия VK WorkMail и Кибер Бэкап.

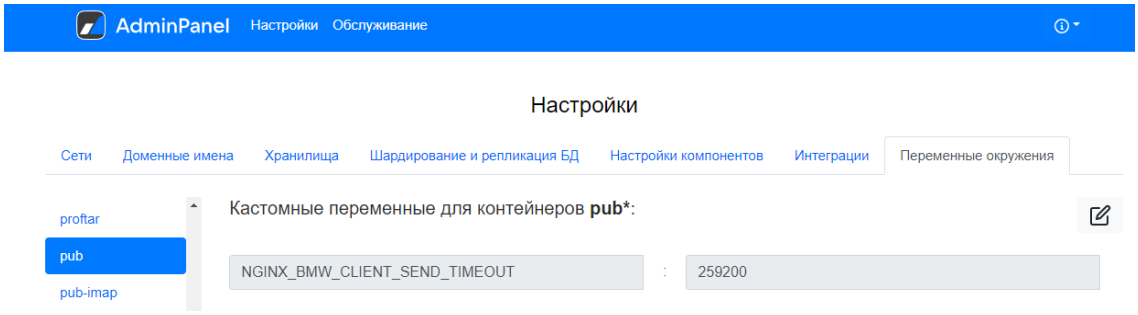
      Примечание
      Для VK WorkMail 26.2 и новее необходимо создавать переменную AMELI_BACKUPER_THREADS.

© ООО Киберпротект, 2026

- BMW_MESCALITO_RESTORE_FIBERS, значение зависит от конфигурации, его необходимо запросить у сотрудников технической поддержки платформы VK WorkSpace. Переменная необходима для восстановления почтовых ящиков, в которых есть письма с вложениями большого размера.
- [VK WorkMail 26.1 и новее] BMW_GRPC_DISABLE_DEPRECATED_METHODS, значение false. Переменная используется для отключения проверок на использование устаревших методов удалённого вызова процедур.

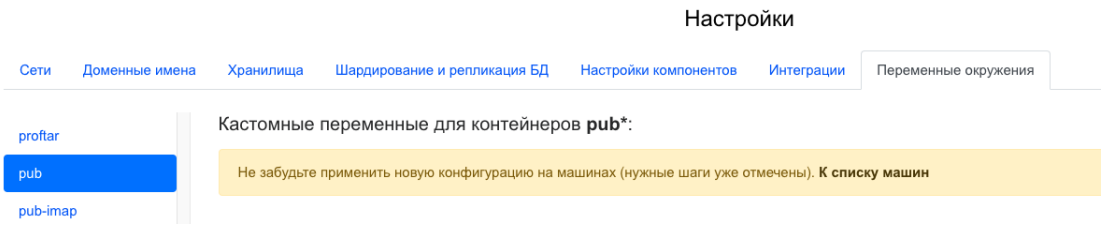


c. В списке слева выберите контейнер **pub**, создайте переменную NGINX_BMW_CLIENT_SEND_TIMEOUT и укажите для нее значение 259200.



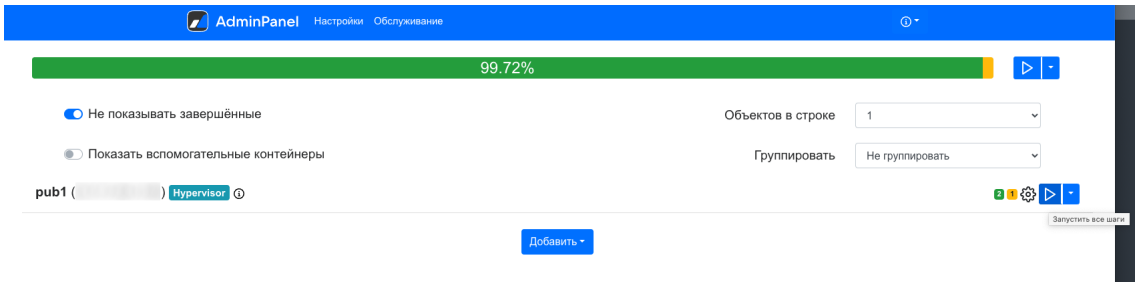
d. В списке слева выберите контейнер **stz-skel-ss**, создайте переменную ZEPTO_WRITABLE_BUCKETS. Значение зависит от конфигурации, его необходимо запросить у сотрудников технической поддержки платформы VK WorkSpace. Переменная необходима для восстановления почтовых ящиков, в которых есть письма с вложениями большого размера.

e. Откройте экран со списком машин, перейдя по ссылке **К списку машин**.



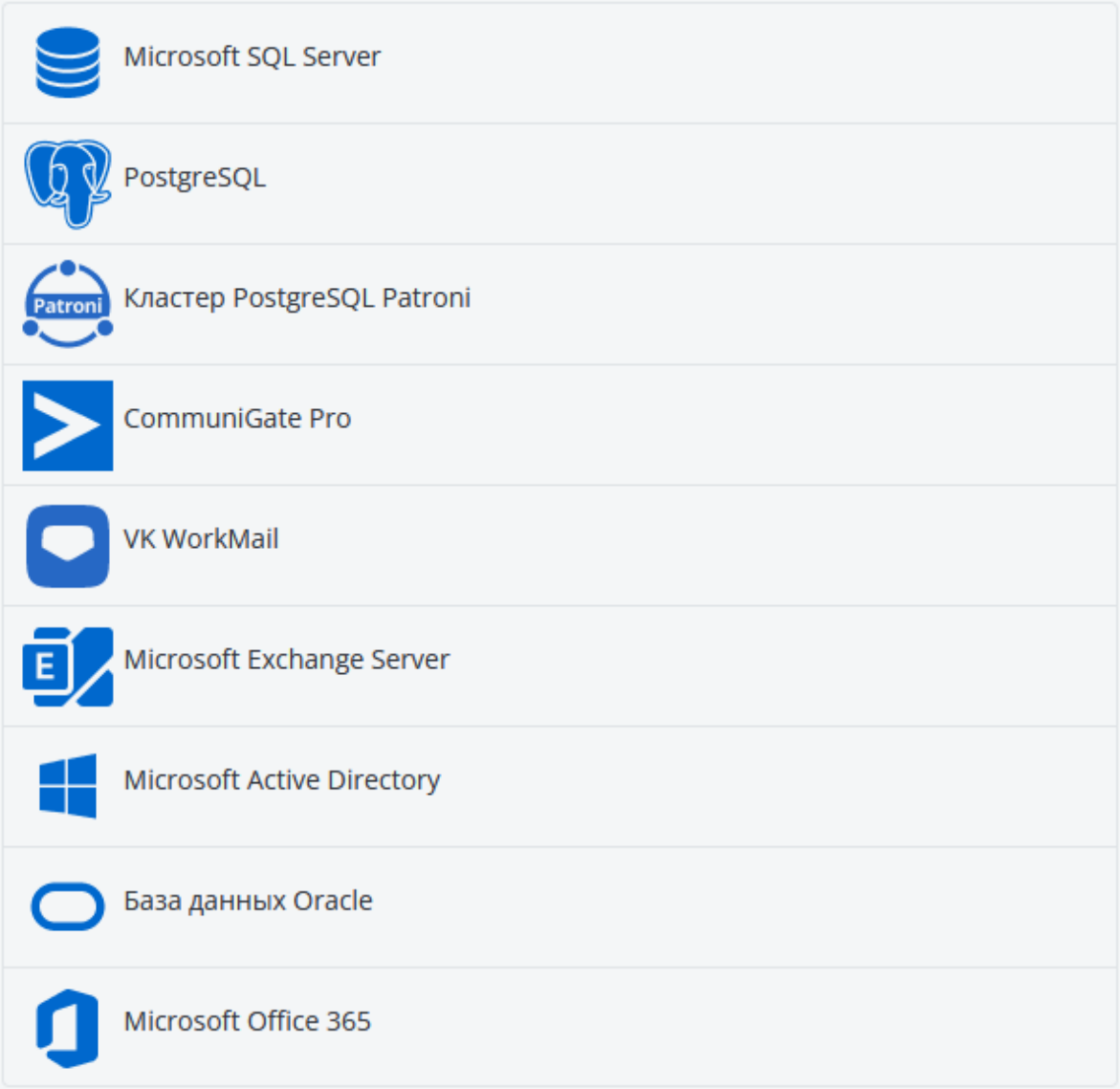
f. Примените изменения для обоих типов контейнеров, нажав на значок запуска .

© ООО Киберпротект, 2026



12.3.4.3 Добавление хоста VK WorkMail

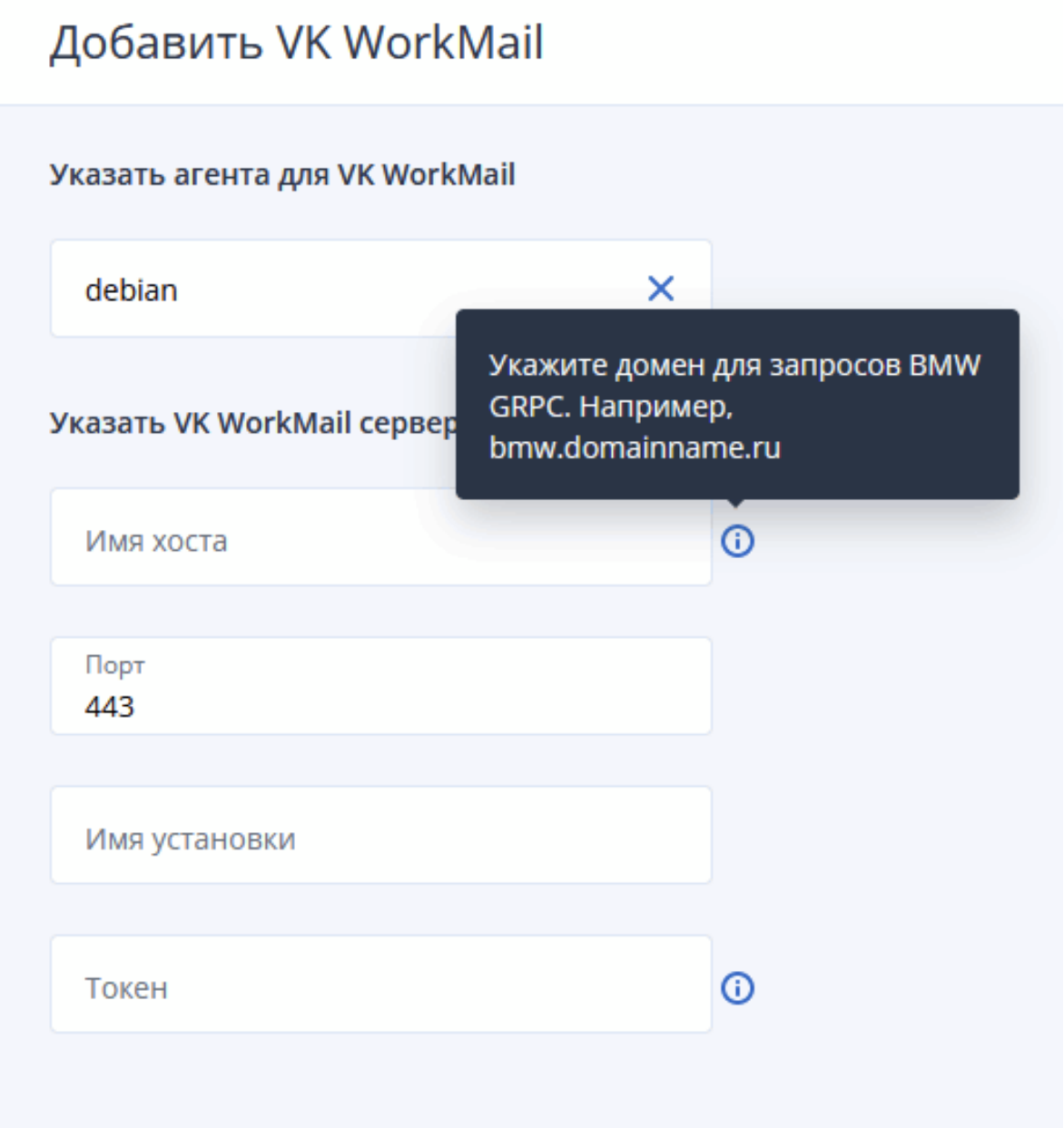
1. В веб-консоли перейдите на вкладку **Устройства** главного меню слева и нажмите в правом верхнем углу **Добавить**.
2. В окне добавления нового устройства щелкните VK WorkMail.



3. Заполните поля:

© ООО Киберпротект, 2026

- в поле **Указать агента для VK WorkMail** выберите из списка имя компьютера, на котором установлен агент или начните вводить имя для поиска;
- в поле **Указать VK WorkMail сервер** укажите домен для запросов BMW GRPC, например, bmw.domainname.ru;
- в поле **Порт** укажите номер порта;
- в поле **Имя установки** укажите имя текущей установки;
- в поле **Токен** укажите токен, выданный вам администратором. Получение токенов описано в документации VK WorkMail.



4. По окончании ввода данных нажмите **Добавить**.

© ООО Киберпротект, 2026

12.3.5 Резервное копирование VK WorkMail и VK WorkDisk

Глобальная адресная книга VK WorkMail определяется в Кибер Бэкап как дополнительный пользователь с именем «адресная книга name@domain». Резервное копирование глобальных адресных книг VK WorkMail происходит аналогично резервному копированию данных пользователей VK WorkMail.

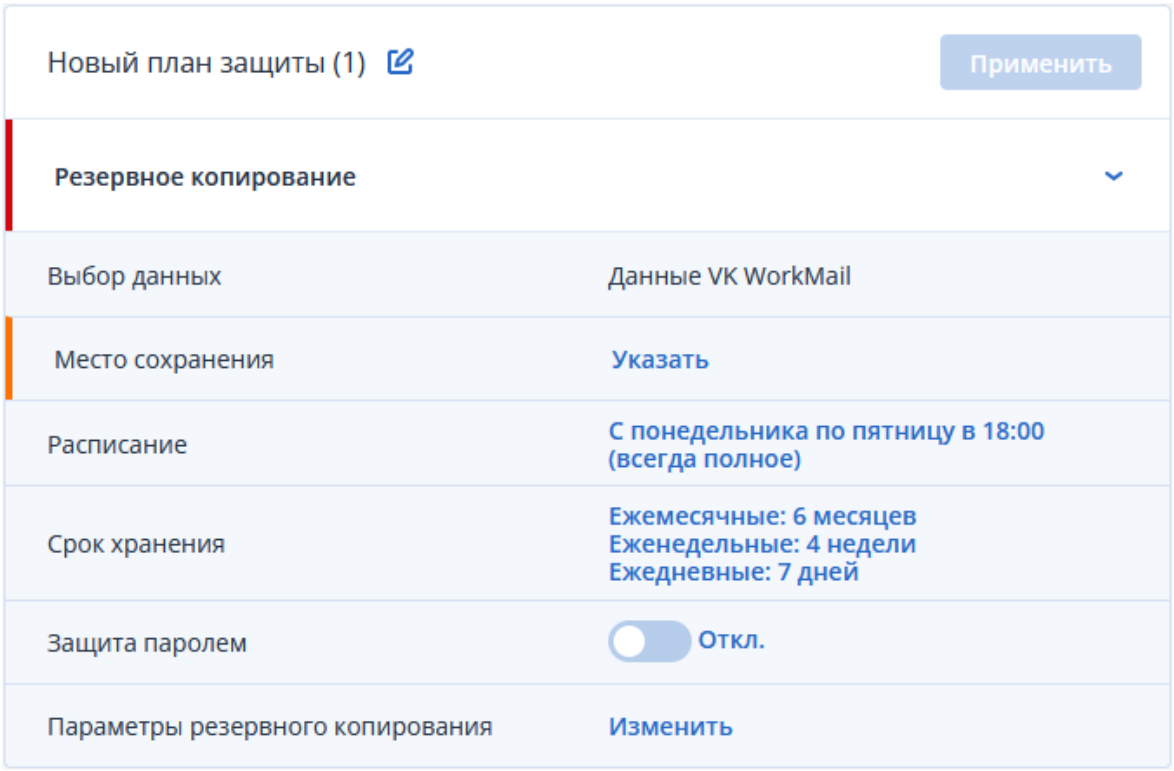
12.3.5.1 Резервное копирование данных пользователей VK WorkMail

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** -> **VK WorkMail**.
2. Выберите из списка обнаруженных ресурсов VK WorkMail пользователя, для которого вы хотите создать защиту, и щелкните по строке, в которой находится имя этого пользователя.

   Примечание
   Для резервного копирования глобальной адресной книги VK WorkMail выберите пользователя с именем «адресная книга name@domain».

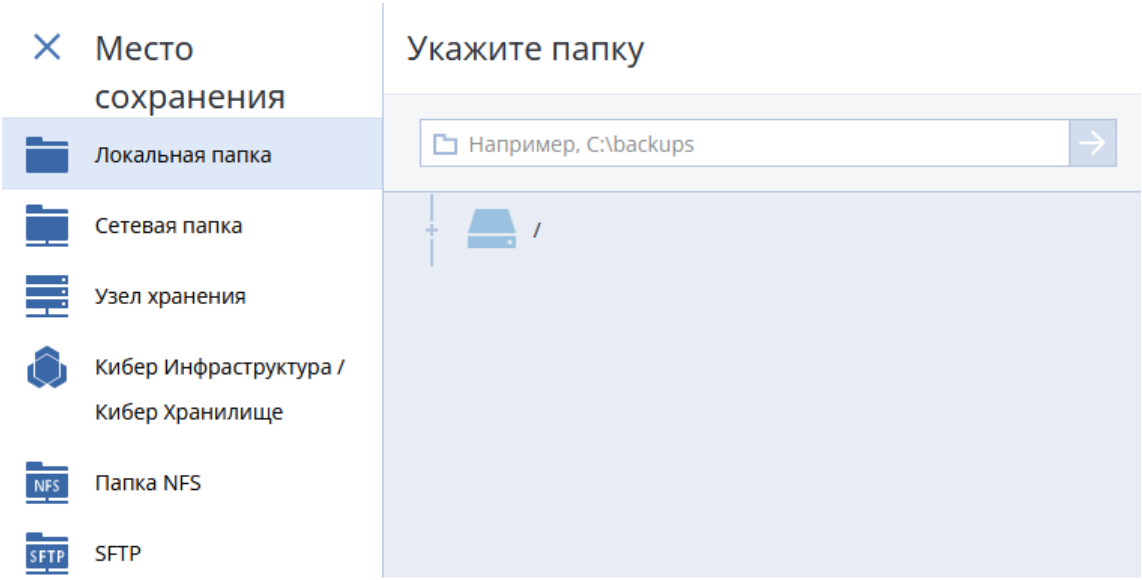
3. Перейдите на вкладку справа **Защитить** для защиты почтового ящика или группы почтовых ящиков (домена).



4. Заполните данные в окне создания плана защиты:
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел

© ООО Киберпротект, 2026

хранения (в том числе на ленты), Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.

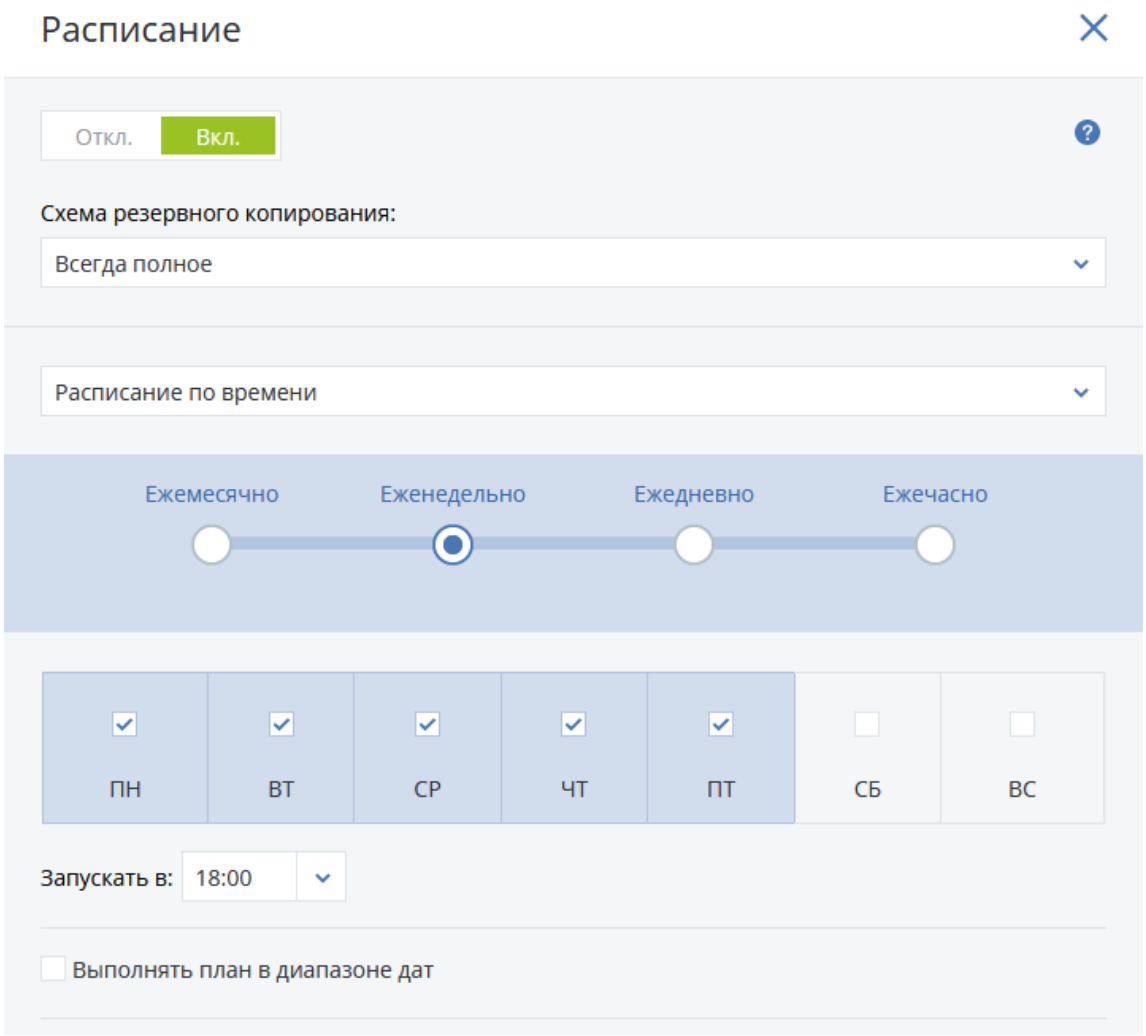


Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места сохранения" (стр. 278).

Внимание
Для резервного копирования на ленты через узел хранения выполните шаги из раздела "Особенности резервного копирования VK WorkMail и VK WorkDisk на ленты" (стр. 550).

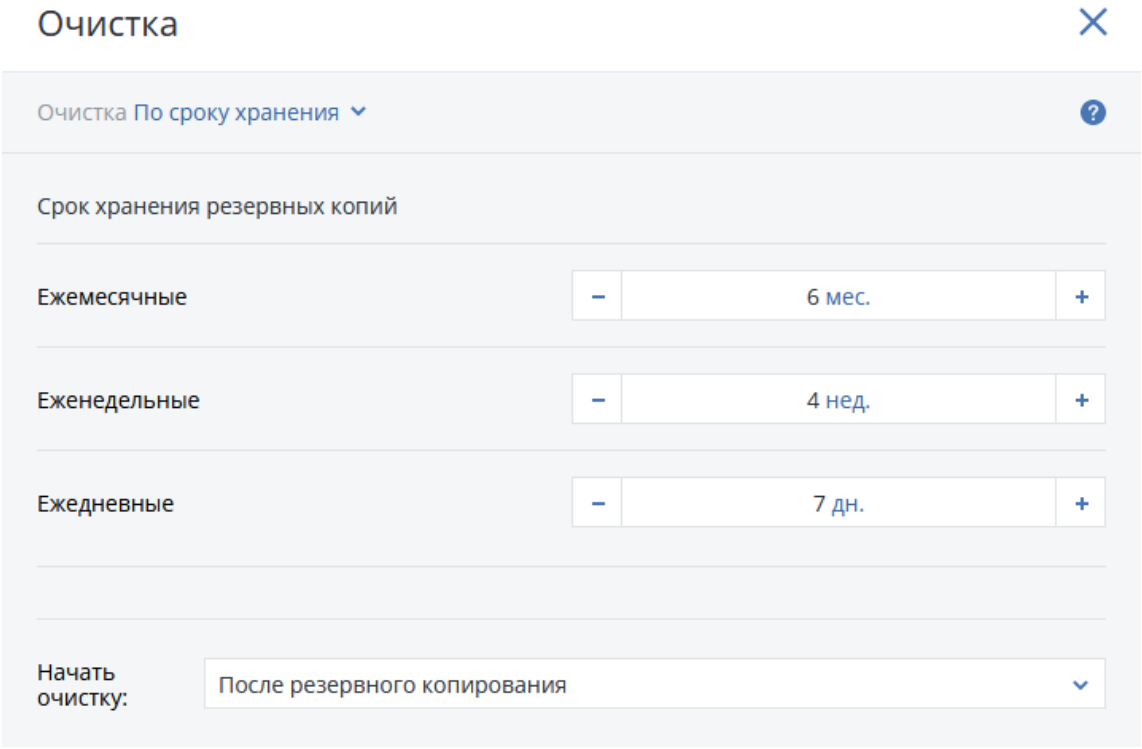
© ООО Киберпротект, 2026

- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.

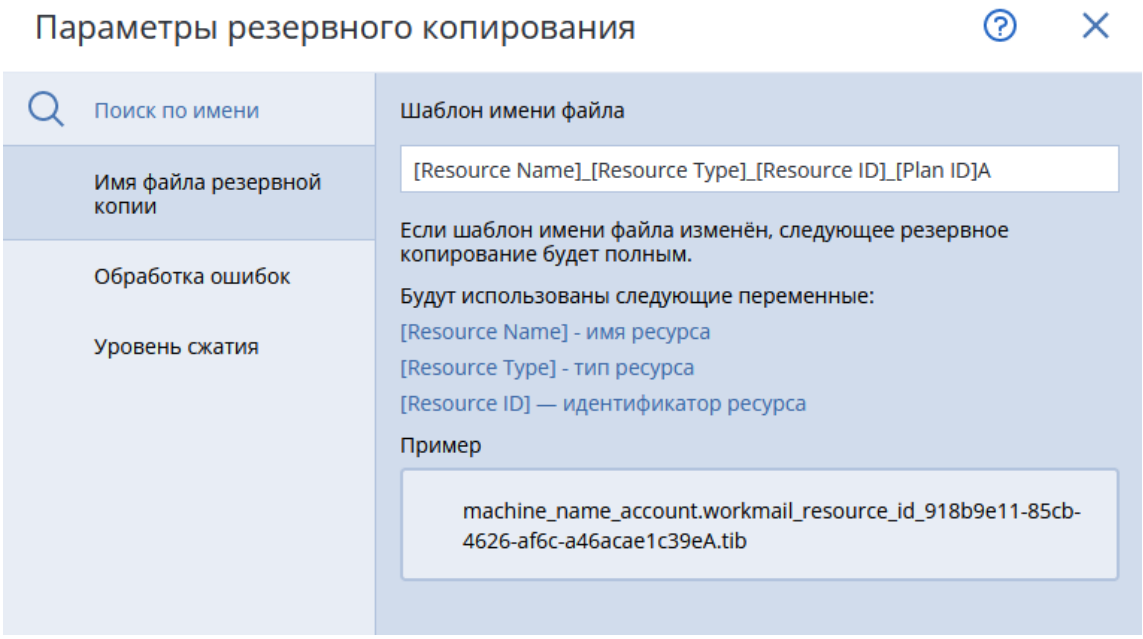


- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.

© ООО Киберпротект, 2026



- [Необязательно] В поле **Параметры резервного копирования** укажите параметры обработки ошибок и уровень сжатия резервных копий.



5. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов и будет применен к выбранным доменам или почтовым ящикам.

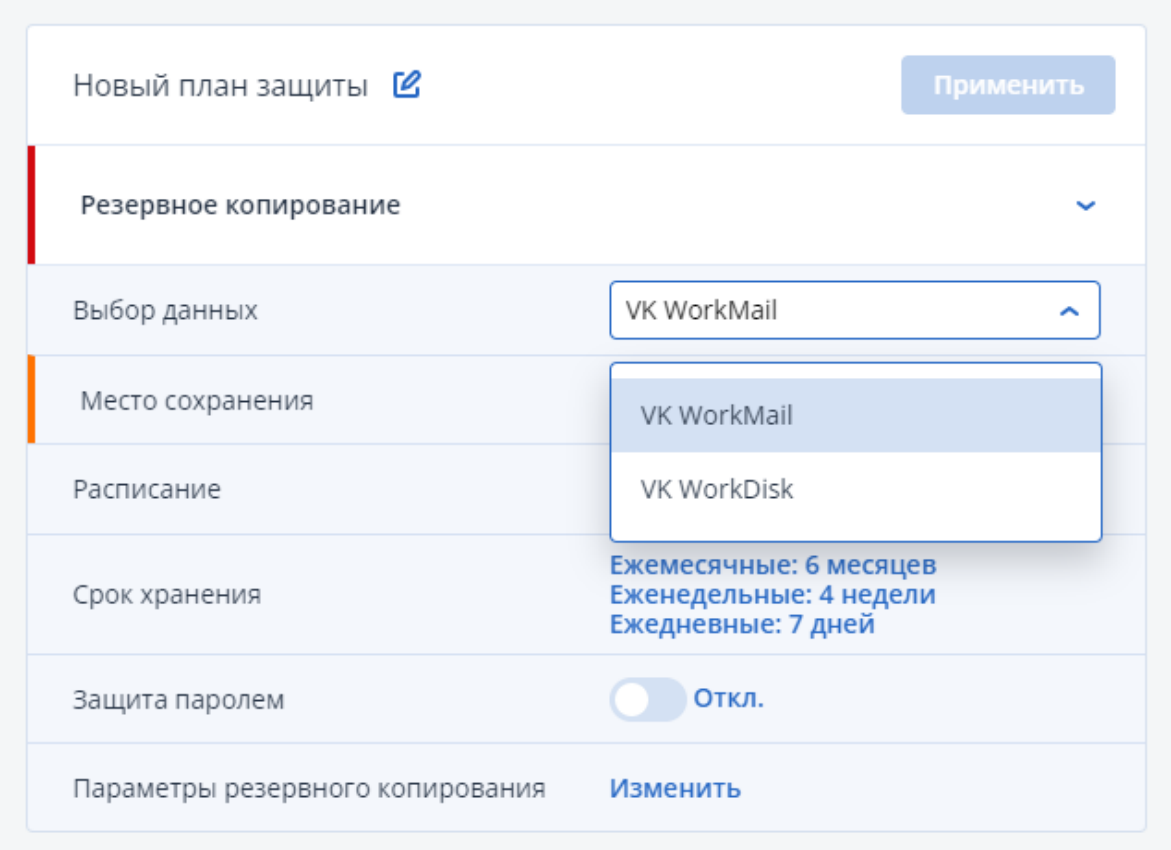
См. также информацию в разделе "План защиты и модули" (стр. 224).

12.3.5.2 Резервное копирование данных пользователей VK WorkDisk

Для создания плана защиты выполните следующие действия:

© ООО Киберпротект, 2026

1. Перейдите в **Устройства** -> **VK WorkMail**.
2. Выберите из списка пользователя, данные которого вы хотите защитить, и щелкните по строке, в которой находится имя этого пользователя.
3. Перейдите на вкладку справа **Защитить** для защиты данных VK WorkDisk.



4. Заполните данные в окне создания плана защиты:
   - В поле **Выбор данных** выберите **VK WorkDisk**.
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения (в том числе на ленты), Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.

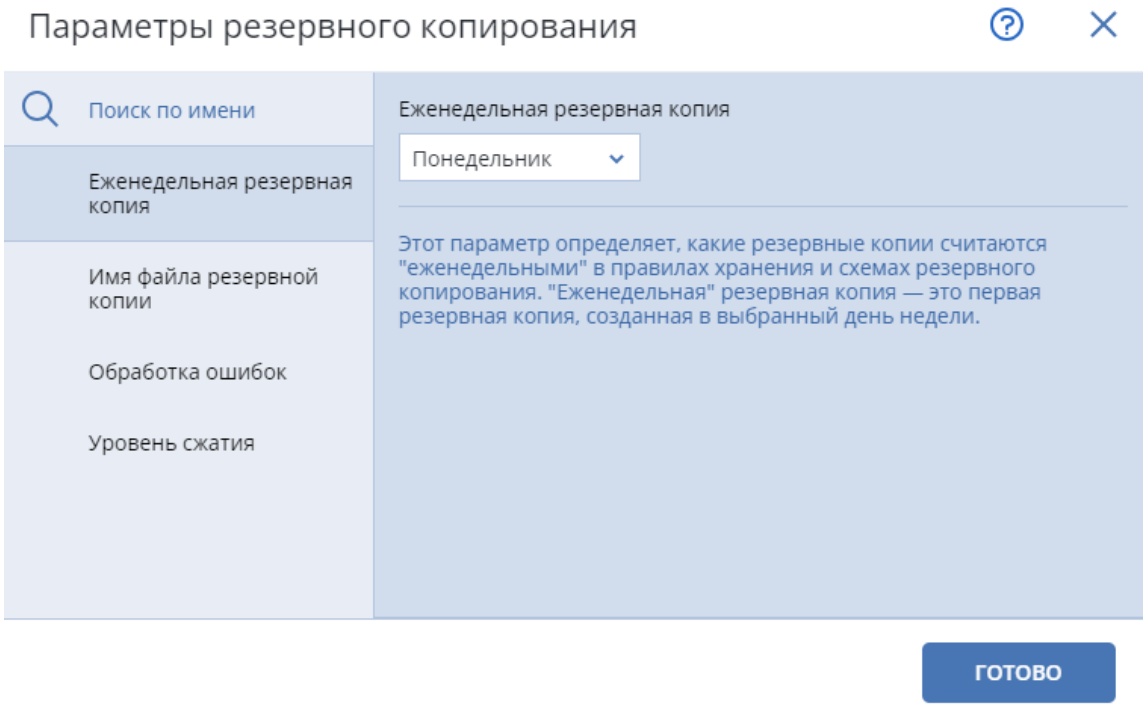
     Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места сохранения" (стр. 278).

     Внимание
     Для резервного копирования на ленты через узел хранения выполните шаги из раздела "Особенности резервного копирования VK WorkMail и VK WorkDisk на ленты" (стр. 550).

   - В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.
   - В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.

© ООО Киберпротект, 2026

- [Необязательно] В поле **Параметры резервного копирования** укажите день недели для создания еженедельной копии, параметры обработки ошибок и уровень сжатия резервных копий.



5. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов и будет применен к данным VK WorkMail выбранного пользователя.

См. также информацию в разделе "План защиты и модули" (стр. 224).

12.3.5.3 Резервное копирование больших объемов данных

При резервном копировании большого количества почтовых ящиков (до 60 000) рекомендуется соблюдать следующие условия:

- Иметь особую лицензию для резервного копирования больших объемов данных.
- Установить сервер управления на машину с ОС Linux, использующую СУБД PostgreSQL (см. раздел "Сервер управления на машине с ОС Linux, использующий СУБД PostgreSQL" (стр. 51)).
- Производить резервное копирование с помощью "Группы устройств" (стр. 248). В каждой группе должно быть не более 2 000 почтовых ящиков.
- Использовать один агент VK WorkMail не более чем для 12 000 почтовых ящиков. Для увеличения производительности можно установить до десяти агентов VK WorkMail на каждый кластер (см. раздел "Установка VK WorkMail" (стр. 534)).
- Использовать для хранения резервных копий Кибер Инфраструктуру. Кроме того, при количестве резервных копий до 150 000, можно использовать сетевую папку.

Использование нескольких агентов для одновременного резервного копирования данных

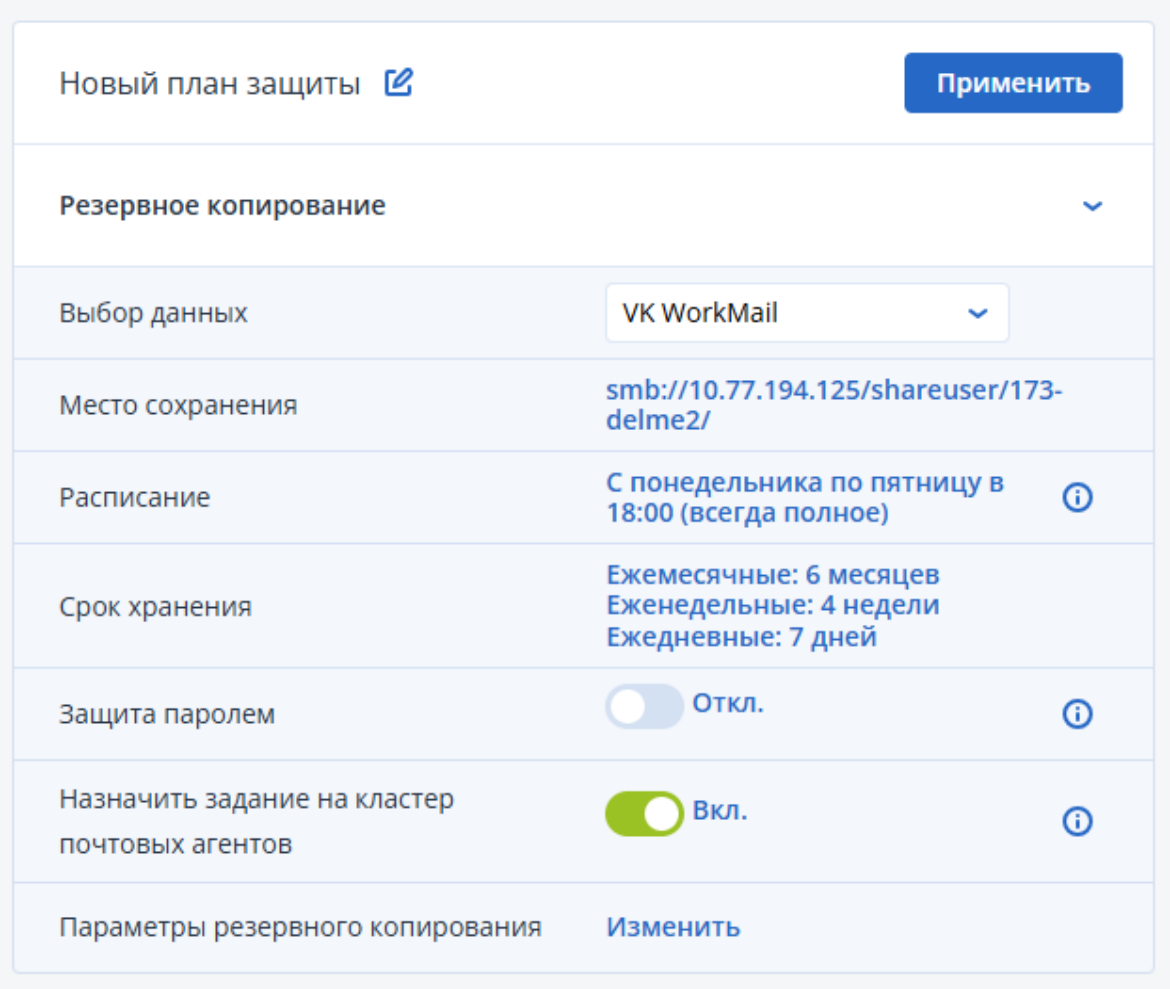
Для резервного копирования более 6 000 почтовых ящиков можно использовать сразу несколько агентов. Для этого выполните следующие действия:

© ООО Киберпротект, 2026

1. Зарегистрируйте необходимое количество агентов VK WorkMail (см. раздел "Установка VK WorkMail" (стр. 534)). Агенты должны быть версии 17.3 или новее.
2. Создайте план резервного копирования для агентов. В резервном копировании будут участвовать все агенты VK WorkMail, зарегистрированные в Кибер Бэкап.

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** -> **VK WorkMail**.
2. Выберите ресурсы VK WorkMail или VK WorkDisk, для которых вы хотите создать план защиты.
3. На вкладке справа нажмите **Защитить** или **Защитить группу**, если выбрана группа почтовых ресурсов.



4. Введите данные в окне создания плана защиты:
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: сетевая папка, узел хранения (в том числе на ленты), Кибер Инфраструктура / Кибер Хранилище, SFTP, папка NFS (только для Linux). Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места сохранения" (стр. 278).
   - В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.

© ООО Киберпротект, 2026

- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.
- В поле **Назначить задание на кластер почтовых агентов** включите переключатель, чтобы назначить план защиты всем зарегистрированным агентам.
- [Необязательно] В поле **Параметры резервного копирования** укажите метод разбиения резервных копий на меньшие по размеру фрагменты, параметры обработки ошибок и уровень сжатия резервных копий.

5. По окончании настройки плана нажмите **Применить**.

При резервном копировании несколькими агентами балансировка нагрузки происходит в режиме циклического перебора (round robin).

12.3.5.4 Резервное копирование серверов VK WorkMail и VK WorkDisk

Резервное копирование сервера VK WorkDisk происходит автоматически при резервном копировании сервера VK WorkMail, к которому подключен сервер VK WorkDisk.

Для резервного копирования сервера VK WorkMail на нем должен быть установлен агент для Linux.

Для создания плана защиты сервера VK WorkMail выполните действия по аналогии со следующим примером.

Предварительные действия

1. Загрузите скрипт.
2. Загрузите файлы программы.
3. Прочитайте инструкцию.

Примечание
Компания Киберпротект предоставляет протестированную на совместимость версию программы VK WorkMail. Для установки последней версии программы обратитесь к официальному разработчику.

Резервное копирование

Настройте план резервного копирования в соответствии с инструкцией, как описано далее.

1. Скопируйте в директорию, например в /tmp, файлы программы: mnt-backup и tars.
2. Задайте права на выполнение:

   ```
   chmod +x /tmp/mnt-backup
   ```

3. В скрипте pre-command.sh укажите необходимые пути:

   ```
   script_dir=/tmp
   main_dir=/home/backup1
   ```

   здесь script_dir – путь к mnt-backup, main_dir – путь, куда будут сохраняться базы данных.

© ООО Киберпротект, 2026

4. Запустите скрипт вручную до создания плана защиты, чтобы получить пути, которые нужно защитить и которые необходимо добавить в исключения (exclude) задачи резервного копирования:

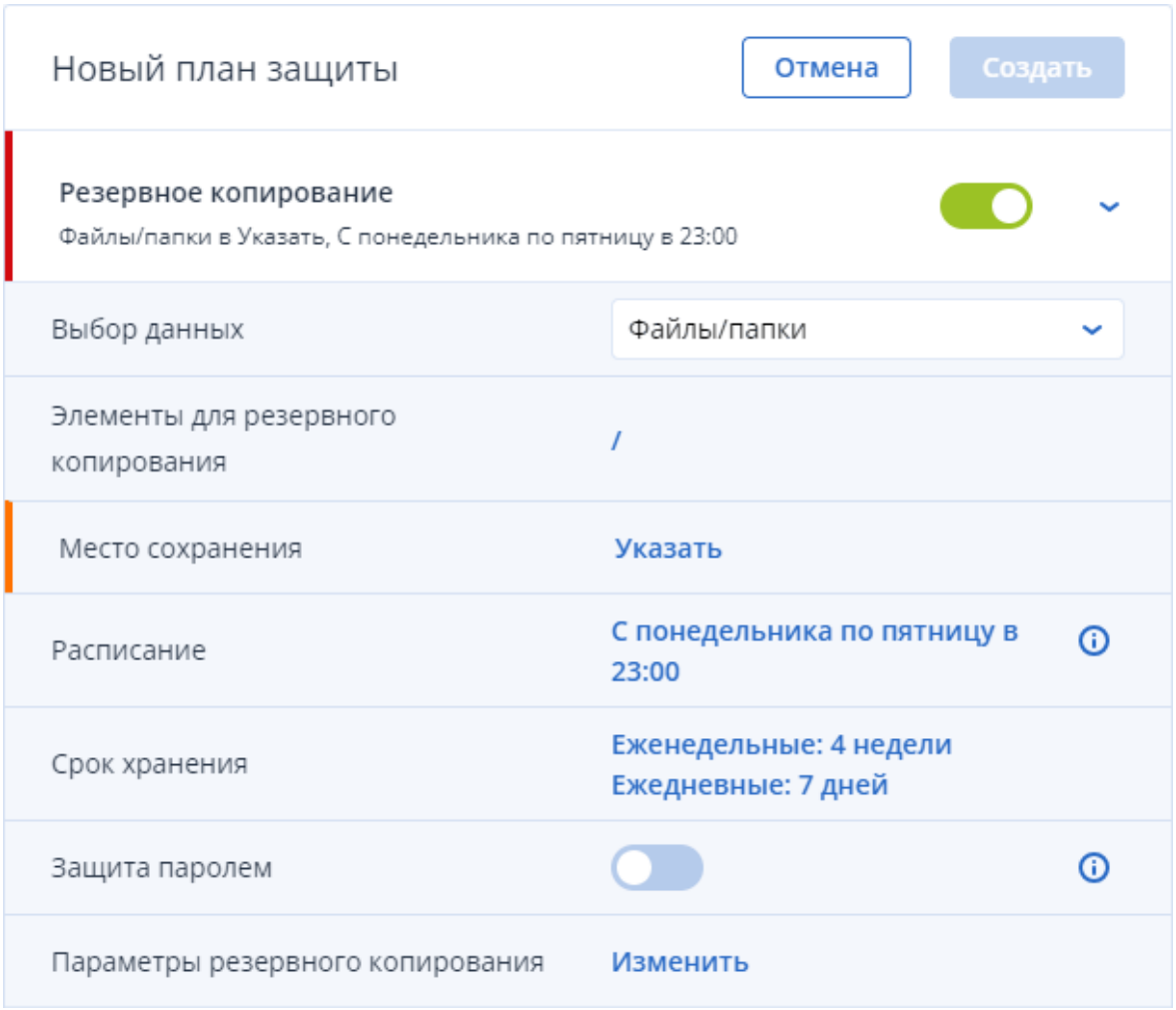
```
chmod +x pre-command.sh
./pre-command.sh
```

В результате в папке /home/backup1/latest появятся файлы:

- pathToStore.txt – содержит пути, которые нужно защитить,
- pathToExclude.txt – содержит абсолютные пути, которые нужно добавить в исключения задачи резервного копирования,
- README.txt – содержит результат запуска скриптов.

Для формирования пути используется /opt/mailOnPremise, а также те части, которые находятся в файле.

5. Перейдите в веб-консоли: **Устройства** -> **Физические и виртуальные машины**.
6. Выберите из списка сервер VK WorkMail, который вы хотите защитить, и щелкните по строке, в которой находится это устройство.
7. Перейдите на вкладку справа **Защитить**.



© ООО Киберпротект, 2026

8. В поле **Выбор данных** выберите **Файлы/папки**.
9. В поле **Элементы для резервного копирования** выберите **С помощью правил политики**.
10. В поле **Добавить правило** поочередно укажите корневые директории тех путей, которые находятся в файле pathToStore.txt, например:

    ```
    /var
    /etc
    /opt
    /home
    ```

    или просто поставьте знак корня

    ```
    /
    ```

11. Нажмите **OK**.
12. Перейдите в **Параметры резервного копирования** -> **Фильтры файлов** -> **Выполнять резервное копирование только файлов, соответствующих следующим критериям**.
13. Укажите пути по маске **со звездочкой** (*) из файла pathToStore.txt:

    ```
    /var/lib/docker/*
    /home/deployer/*
    /opt/mailOnPremise/
    /etc/systemd/system/onpremise-*
    /etc/systemd/system/deployer.service
    /home/backup1/latest/*
    ```

14. Перейдите в **Параметры резервного копирования** -> **Фильтры файлов** -> **Не выполнять резервное копирование файлов, соответствующих следующим критериям**.
15. Добавьте абсолютные пути из файла pathToExclude.txt:

    ```
    /opt/mailOnPremise/dockerVolumes/ussug1/tarantool
    /opt/mailOnPremise/dockerVolumes/evdokia-tar1/tarantool
    /opt/mailOnPremise/dockerVolumes/filters-tar1/tarantool
    /opt/mailOnPremise/dockerVolumes/abookpdd-tar1/tarantool
    /opt/mailOnPremise/dockerVolumes/mstatqueue-tar1/tarantool
    /opt/mailOnPremise/dockerVolumes/search-reindex-queue1/tarantool
    /opt/mailOnPremise/dockerVolumes/cldudb-proxy1/tarantool
    /opt/mailOnPremise/dockerVolumes/autoreplylimiter1/tarantool
    /opt/mailOnPremise/dockerVolumes/stpath-tar1/tarantool
    /opt/mailOnPremise/dockerVolumes/attfiledb1/tarantool
    ...
    ```

16. Перейдите в **Параметры резервного копирования** -> **Команды до или после** -> **Выполнение команды до резервного копирования** и включите переключатель: **Да**.
17. В поле **Команда или путь к файлу пакета на машине с агентом** вставьте:

    ```
    ./pre-command.sh
    ```


© ООО Киберпротект, 2026

18. В поле **Рабочий каталог** вставьте путь, где лежит скрипт pre-command.sh, например:

```
/tmp
```

19. Нажмите **Готово**.

Внимание
Поскольку вы используете команды "до или после", убедитесь, что код возврата скрипта от VK возвращает корректное значение. В противном случае, возможна неверная интерпретация результатов резервного копирования.

12.3.5.5 Особенности резервного копирования VK WorkMail и VK WorkDisk на ленты

Функционал autoinventory

Перед резервным копированием на ленты через узел хранения необходимо отключить функционал autoinventory в файле tape_devices.xml:

```
<autoinventory>
  <enabled value="0"/>
</autoinventory>
```

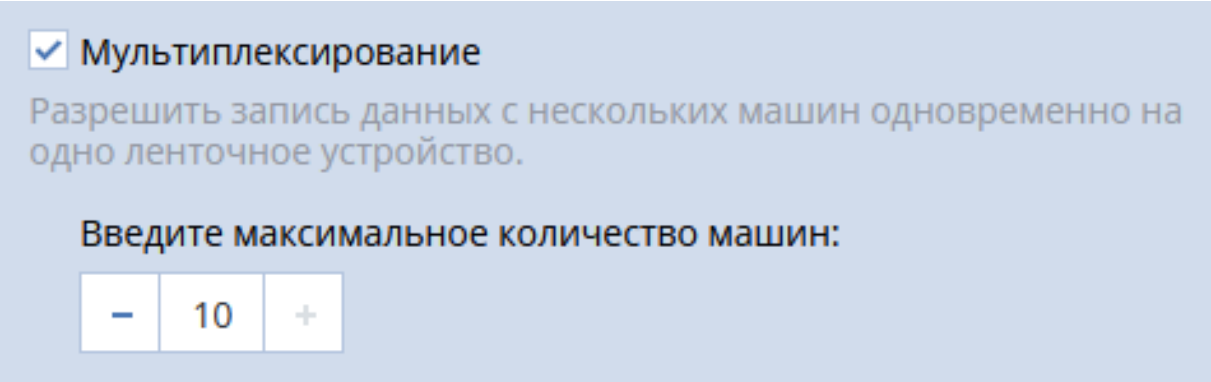
и перезапустить службу узла хранения.

- В ОС Windows отредактируйте файл C:\ProgramData\Acronis\BackupAndRecovery\ARSM\Configuration\tape_devices.xml. Затем перезапустите службу **Cyberprotect Storage Node Service** в приложении **Службы**.
- В ОС Linux отредактируйте файл /var/lib/Acronis/BackupAndRecovery/ARSM/Configuration/tape_devices.xml. Затем выполните команду

```
systemctl restart acronis_storageserver
```

Мультиплексирование

Мультиплексирование должно быть включено. Максимальное количество машин должно быть не менее 10. Подробнее о мультиплексировании см. в разделе "Управление лентами" (стр. 372).



© ООО Киберпротект, 2026

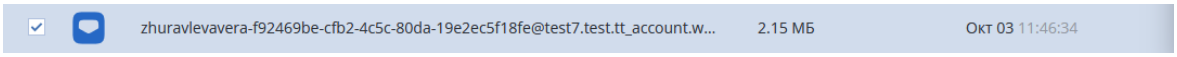
12.3.6 Восстановление VK WorkMail и VK WorkDisk

Восстановление глобальных адресных книг VK WorkMail происходит аналогично восстановлению данных пользователей VK WorkMail.

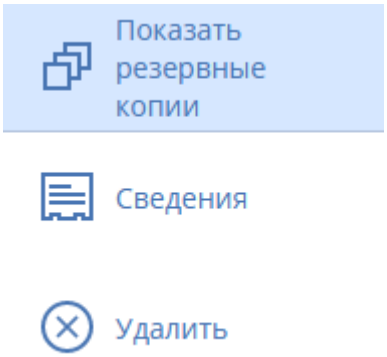
12.3.6.1 Восстановление данных пользователей VK WorkMail

Чтобы восстановить данные пользователей VK WorkMail, выполните следующие действия:

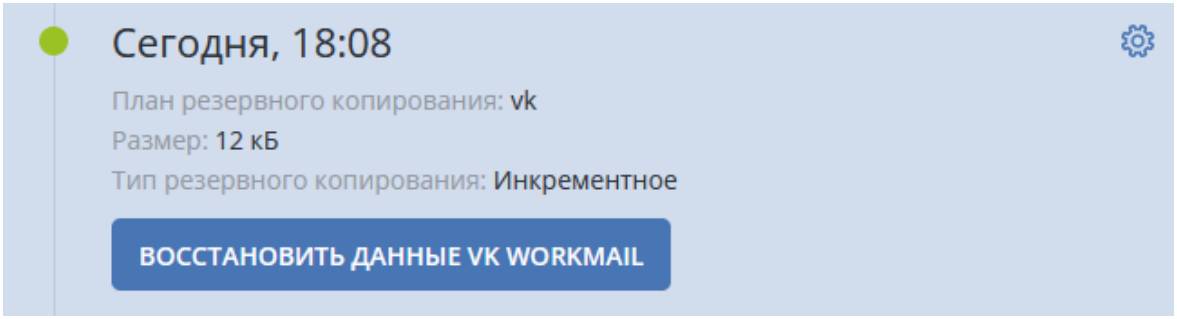
1. Перейдите в **Хранилища резервных копий** в главном меню слева.
2. Выберите в списке нужную резервную копию.



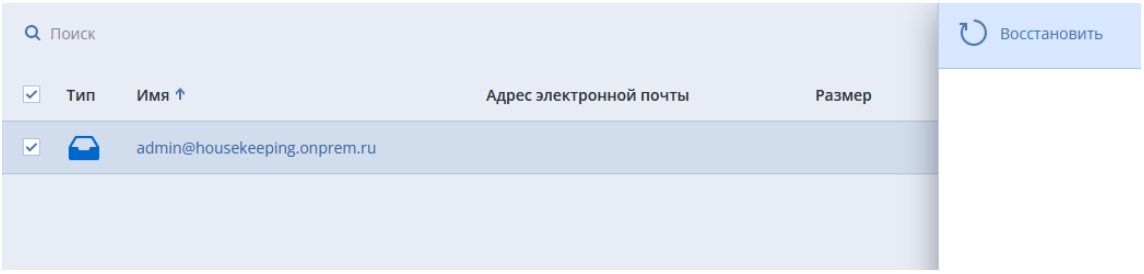
3. Выберите справа **Показать резервные копии**.



4. Нажмите **Восстановить данные VK WorkMail**.

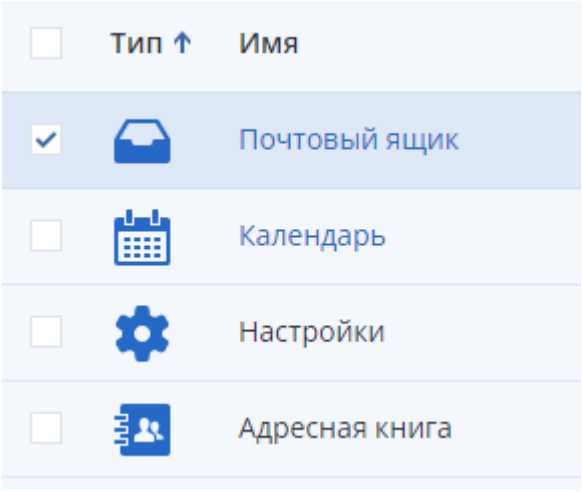


5. Выберите данные для восстановления:
   - Если необходимо восстановить весь почтовый ящик, отметьте галочкой в списке имя почтового ящика, затем выберите справа **Восстановить**.

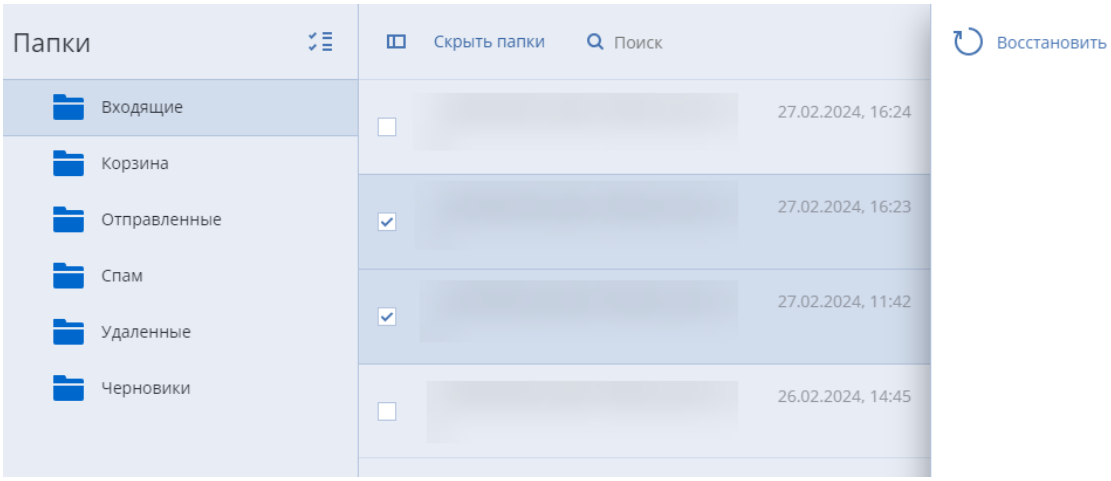


© ООО Киберпротект, 2026

- Если необходимо восстановить отдельные ресурсы пользователя, нажмите на имя резервной копии. Можно выбрать только один тип ресурса для восстановления. Выберите ресурс и нажмите справа **Восстановить**.



- Если необходимо восстановить отдельные письма или события календаря, нажмите на **Почтовый ящик** или **Календарь** и выберите данные, затем нажмите справа **Восстановить**.



6. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
7. Укажите место восстановления.

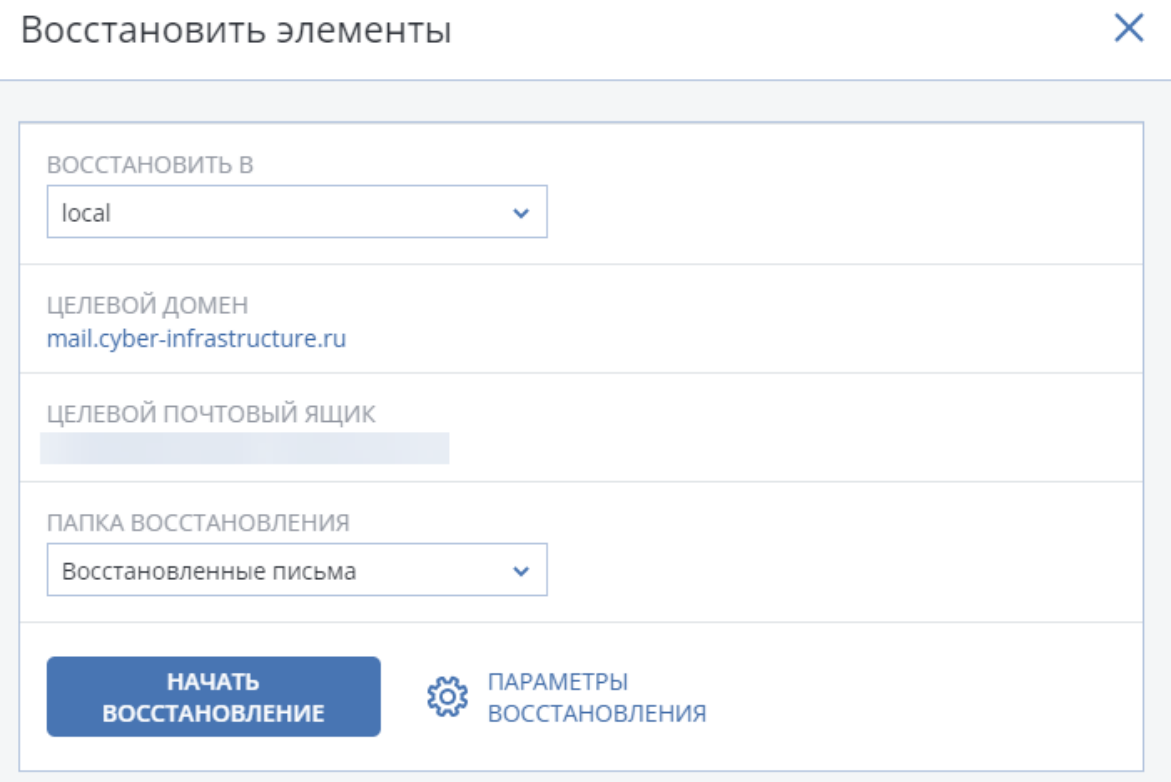
Примечание

При восстановлении только профиля пользователя невозможно выбрать пользователя, отличного от оригинального.

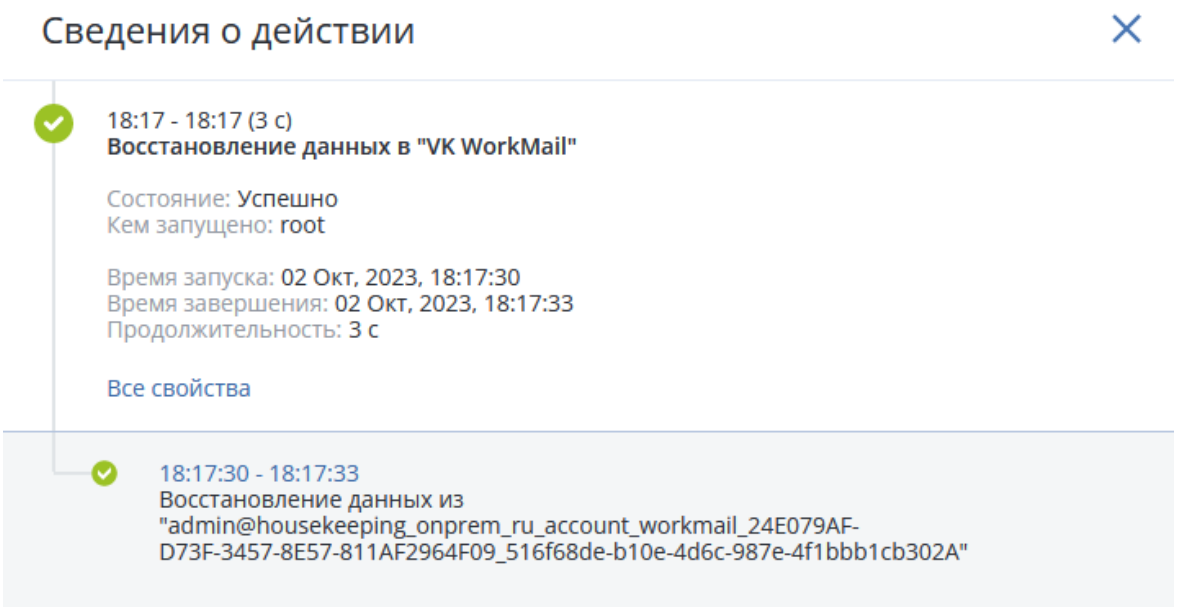
При восстановлении полного аккаунта пользователя в другого пользователя восстановление профиля будет пропускаться. Остальные данные будут восстановлены.

Проверьте правильность заполнения полей и затем нажмите **Начать восстановление**.

© ООО Киберпротект, 2026



8. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.



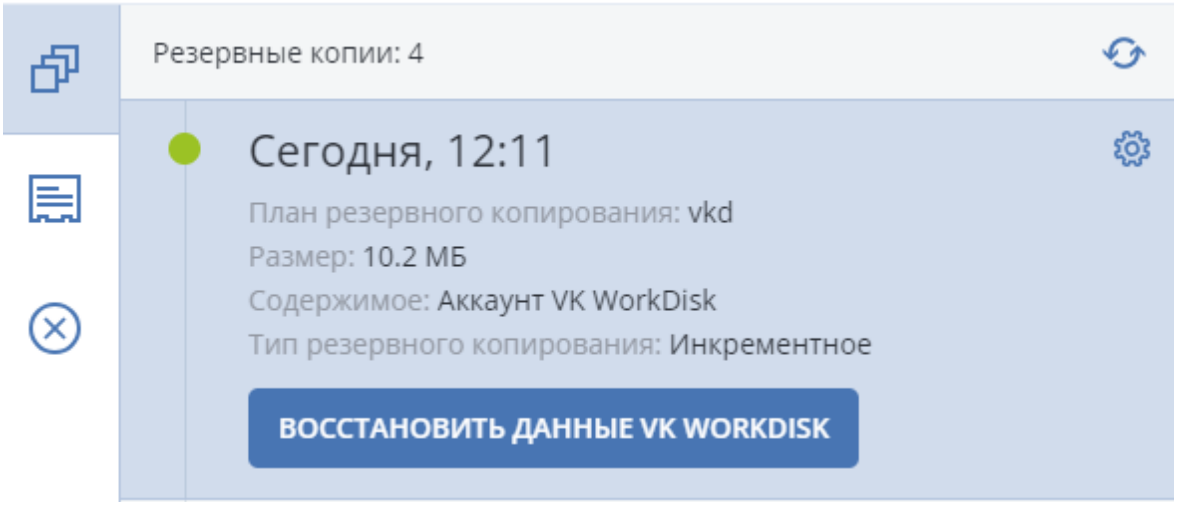
12.3.6.2 Восстановление данных пользователей VK WorkDisk

Чтобы восстановить данные пользователей VK WorkDisk, выполните следующие действия:

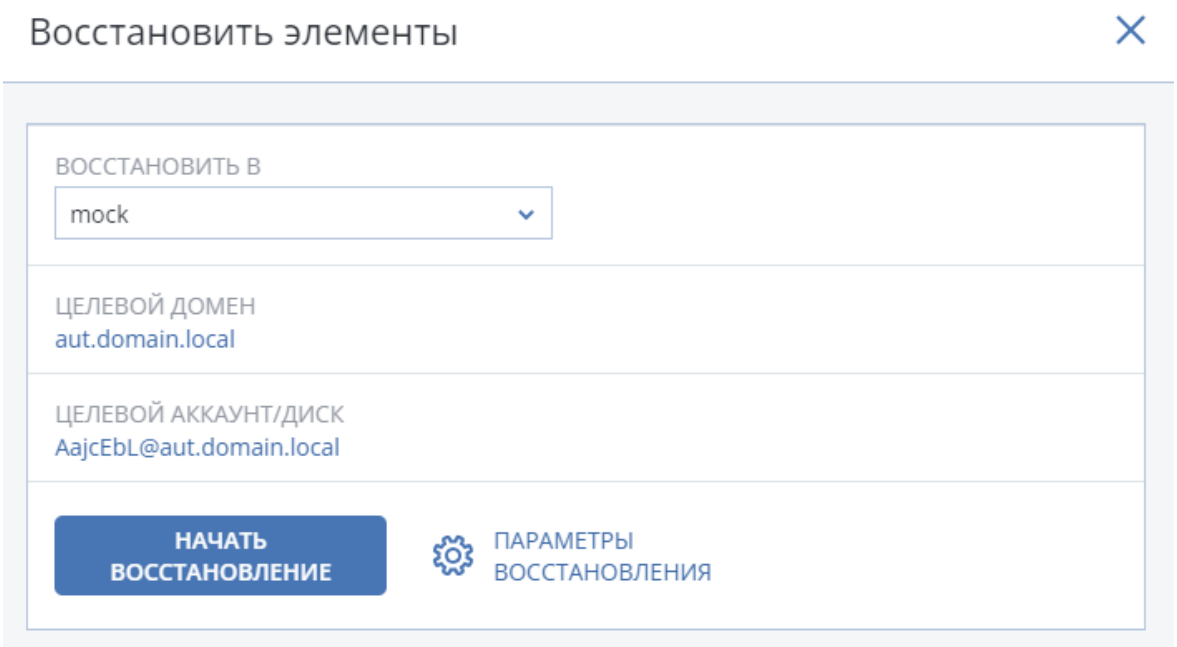
1. Перейдите в **Хранилища резервных копий** и выберите в списке нужную резервную копию.
2. Выберите справа **Показать резервные копии**.

© ООО Киберпротект, 2026

3. Нажмите **Восстановить данные VK WorkDisk**.



4. Выберите данные для восстановления; затем выберите справа **Восстановить**.
5. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
6. Проверьте правильность заполнения полей и затем нажмите **Начать восстановление**.



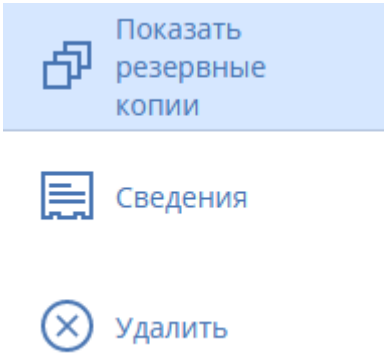
7. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.

12.3.6.3 Просмотр писем VK WorkMail

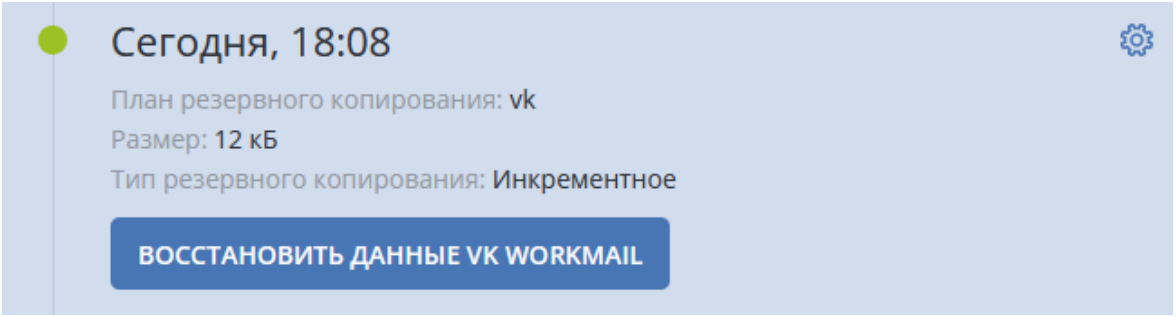
Чтобы просмотреть письма пользователя VK WorkMail, выполните следующие действия:

1. Перейдите в **Хранилища резервных копий** в главном меню слева.
2. Выберите нужное хранилище, щелкните в списке нужную резервную копию.
3. Выберите справа **Показать резервные копии**.

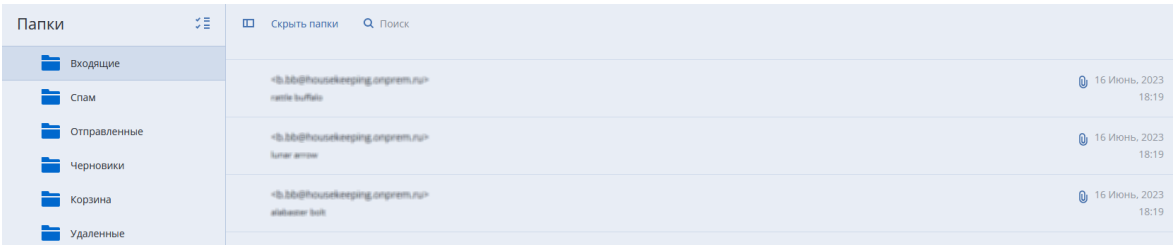
© ООО Киберпротект, 2026



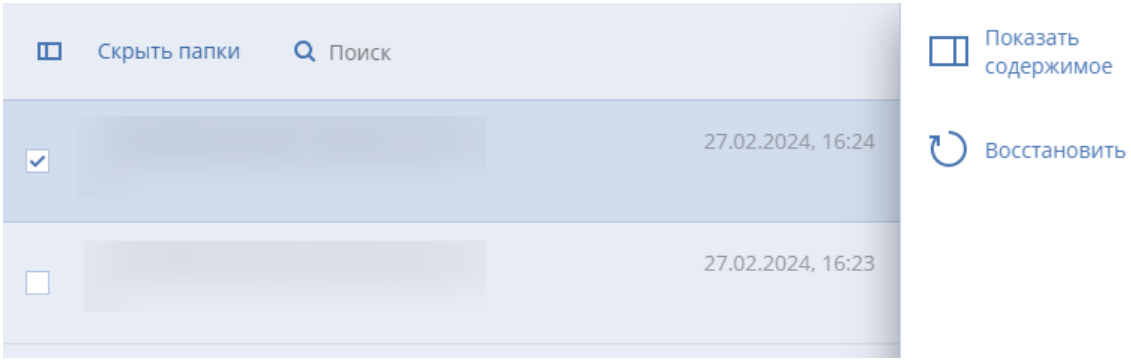
4. Щелкните **Восстановить данные VK WorkMail**.



5. Нажмите имя пользователя в виде ссылки. Откроется список папок с письмами этого пользователя.

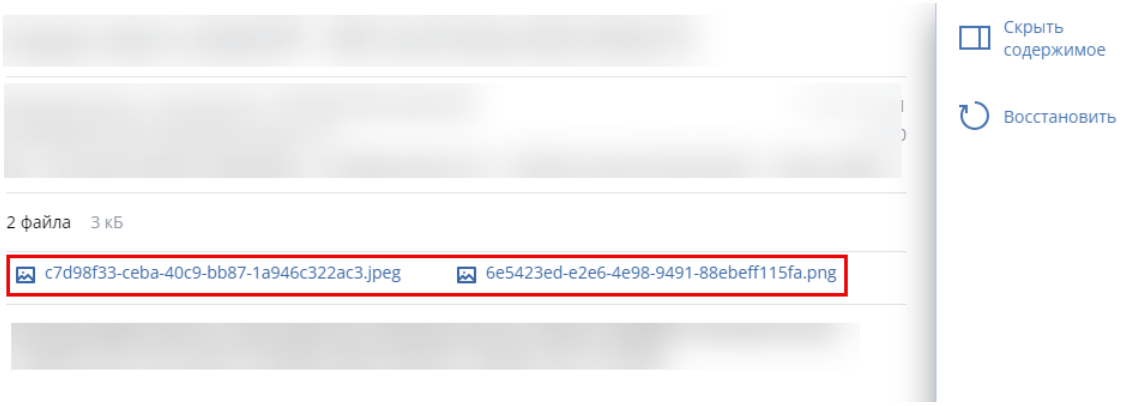


6. Выберите из списка нужное письмо, отметьте его галочкой.
7. Для просмотра содержимого письма нажмите справа **Показать содержимое**. Данная возможность недоступна для писем, хранящихся на лентах.



8. Для скачивания файла, приложенного к письму, щелкните по нему.

© ООО Киберпротект, 2026



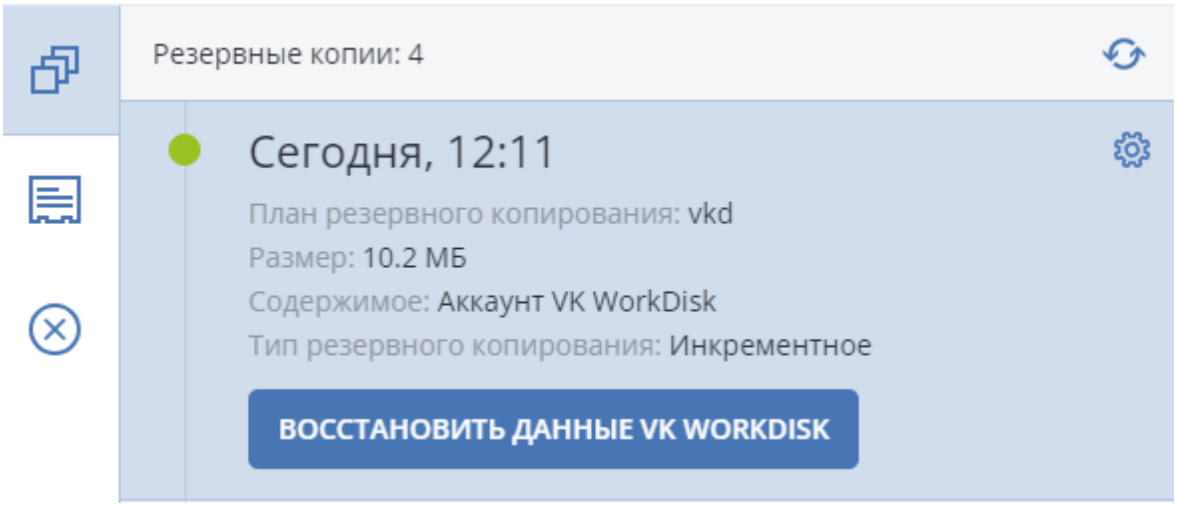
12.3.6.4 Скачивание файлов из архива VK WorkDisk

Перед скачиванием данных рекомендуется увеличить время ожидания до автоматического выхода по причине неактивности пользователя в настройках Кибер Бэкап. Для этого перейдите в **Настройки** -> **Настройки системы** -> **Безопасность** и либо уберите галочку **Завершить сеансы работы неактивных пользователей через**, либо установите время, которого точно хватит для скачивания данных.

Внимание
Если во время скачивания файла произойдет автоматический выход пользователя из веб-консоли, файл придется скачивать заново.

Чтобы скачать файлы из архива VK WorkDisk, выполните следующие действия:

1. Перейдите в **Хранилища резервных копий**.
2. Выберите нужное хранилище, щелкните в списке нужную резервную копию.
3. Выберите справа **Показать резервные копии**.
4. Нажмите **Восстановить данные VK WorkDisk**.



5. Нажмите имя пользователя в виде ссылки. Откроется список с данными пользователя.

© ООО Киберпротект, 2026

6. Отметьте в списке нужные элементы галочкой. Количество выбранных элементов не должно превышать 150. Папка с файлами или диск целиком считаются за один элемент.
7. Для скачивания файлов нажмите **Загрузить**.

   Не выходите из окна просмотра архива и не переходите на другие точки восстановления до окончания скачивания данных. Чтобы воспользоваться другими функциями Кибер Бэкап, используйте новую вкладку браузера, иначе скачивание файла может быть прервано.

Примечание
Скачивание файлов из архива VK WorkDisk не поддерживается для резервных копий, расположенных на лентах.

12.3.6.5 Восстановление серверов VK WorkMail и VK WorkDisk

Восстановление данных на новую машину

Восстановление сервера VK WorkDisk происходит автоматически при восстановлении сервера VK WorkMail, к которому подключен сервер VK WorkDisk.

Для восстановления резервной копии сервера VK WorkMail, созданной по инструкции в разделе "Резервное копирование серверов VK WorkMail и VK WorkDisk" (стр. 547), выполните следующие действия:

1. Выключите исходную машину.
2. Для новой машины установите такой же IP-адрес, как для исходной.
3. Установите на новую машину агент Кибер Бэкап для Linux.
4. Восстановите данные в соответствующие директории, следуя шагам в разделе "Восстановление гипервизора" инструкции, предоставленной VK.

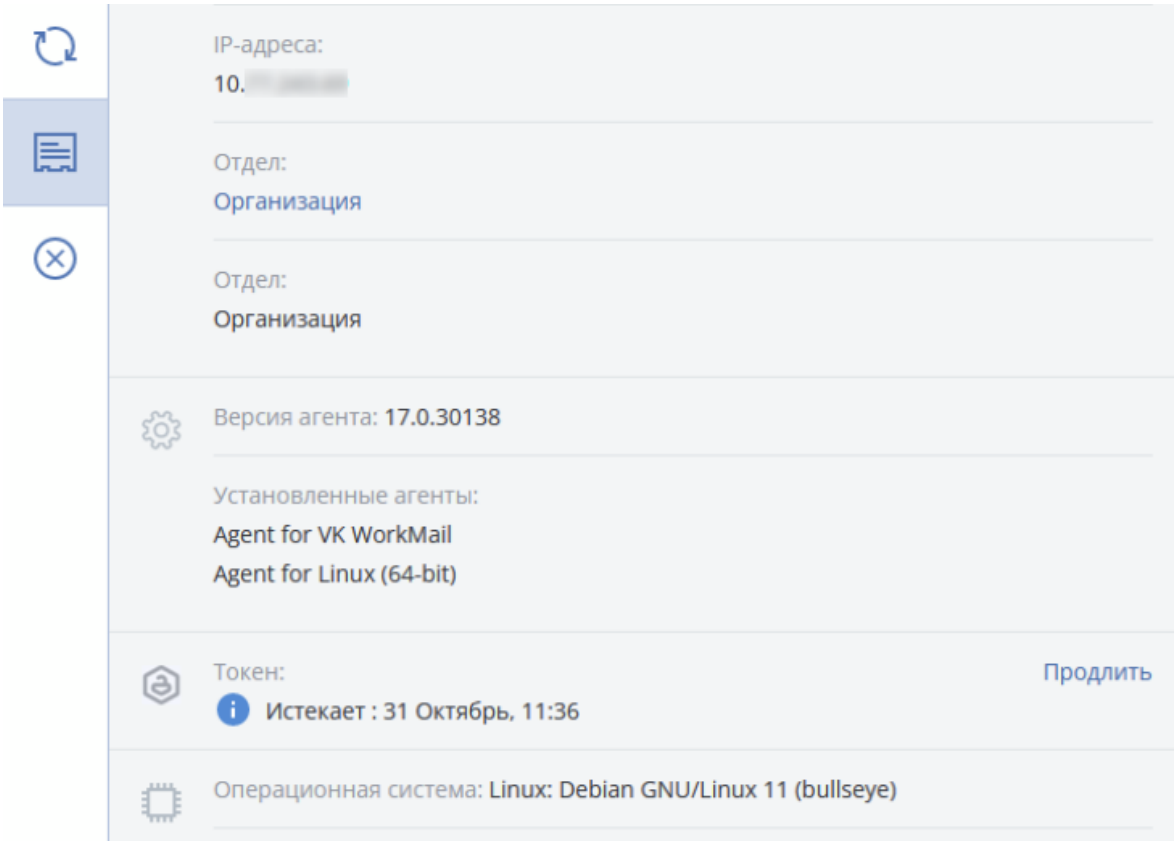
12.3.7 Обновление токена VK WorkMail

Для обнаружения, резервного копирования и восстановления данных устройства VK WorkMail Кибер Бэкап использует gRPC API, предоставляемый VK WorkMail, при обращениях к которому Кибер Бэкап передает токен для авторизации запросов. Токен обладает ограниченным сроком действия, поэтому его необходимо заблаговременно обновлять. Кибер Бэкап будет оповещать пользователей за месяц до истечения срока действия токена, а также при истечении этого срока.

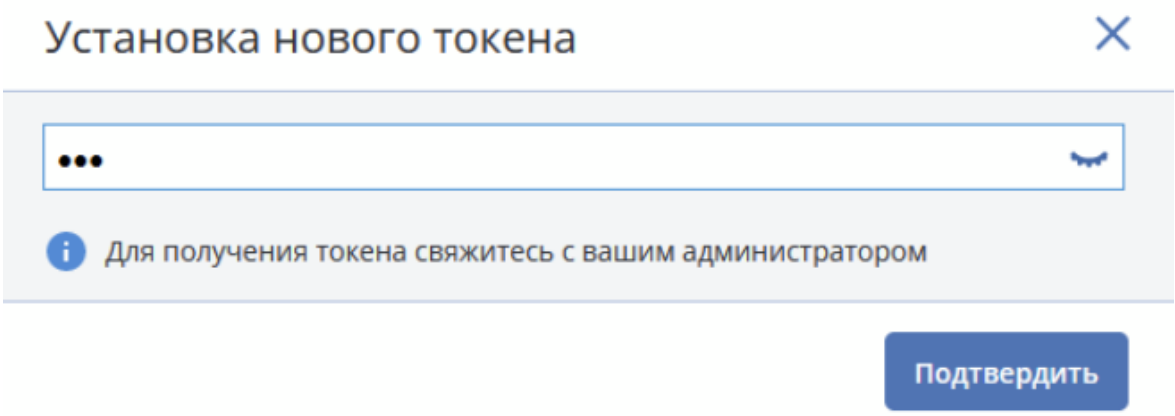
Чтобы узнать дату окончания срока действия токена и обновить его при необходимости, выполните следующие шаги:

1. В веб-консоли перейдите на экран **Устройства** > **VK WorkMail** и выберите нужное устройство.
2. В правой панели перейдите на вкладку **Сведения**. В разделе **Токен** будет отображена дата окончания срока действия токена.

© ООО Киберпротект, 2026



Если необходимо обновить токен, щелкните **Продлить**, укажите новый токен и нажмите **Подтвердить**.



12.4 Защита Mailion

Mailion – почтовая система, ориентированная на крупные коммерческие и государственные организации.

Для резервного копирования данных Mailion понадобятся установленные и настроенные продукты:

- Кибер Бэкап 18.0 или новее с лицензией Кибер Бэкап для почтового ящика (список лицензий см. в разделе "Издания и лицензии Кибер Бэкап" (стр. 16)).
- Почтовый сервис Mailion.

© ООО Киберпротект, 2026

Поддерживаемые версии Mailion указаны в разделе "Поддерживаемые почтовые сервисы" (стр. 35).

Для выполнения резервного копирования требуется установка агента Mailion.

Поддерживается установка агента для следующих операционных систем:

- Windows,
- Linux.

Полный список поддерживаемых операционных систем Windows и Linux см. в разделе "Агенты" (стр. 23).

12.4.1 Возможности

Кибер Бэкап обеспечивает резервное копирование и восстановление:

- данных пользователя Mailion (электронные сообщения с форматированием и флагами, вложения, папки со структурой подпапок, настройки, календари и события календарей, контакты, задачи);
- тенанта Mailion (как группу пользователей);
- параметры общего доступа;
- почтовых ящиков ресурсов.

После выполнения резервного копирования в архиве можно посмотреть содержимое отдельных папок и писем, а также события и задачи в календаре.

12.4.2 Известные проблемы и ограничения

- Не поддерживается резервное копирование на ленты.
- Для восстановления структуры тенанта необходимо восстановить данные специального пользователя Tenant Catalog.
- Восстановить почтовый ящик пользователя можно только в пространство этого пользователя.
- Для восстановления данных пользователя на другой сервер Mailion надо предварительно восстановить на этот сервер тенант, в котором находится пользователь.

12.4.3 Установка Mailion

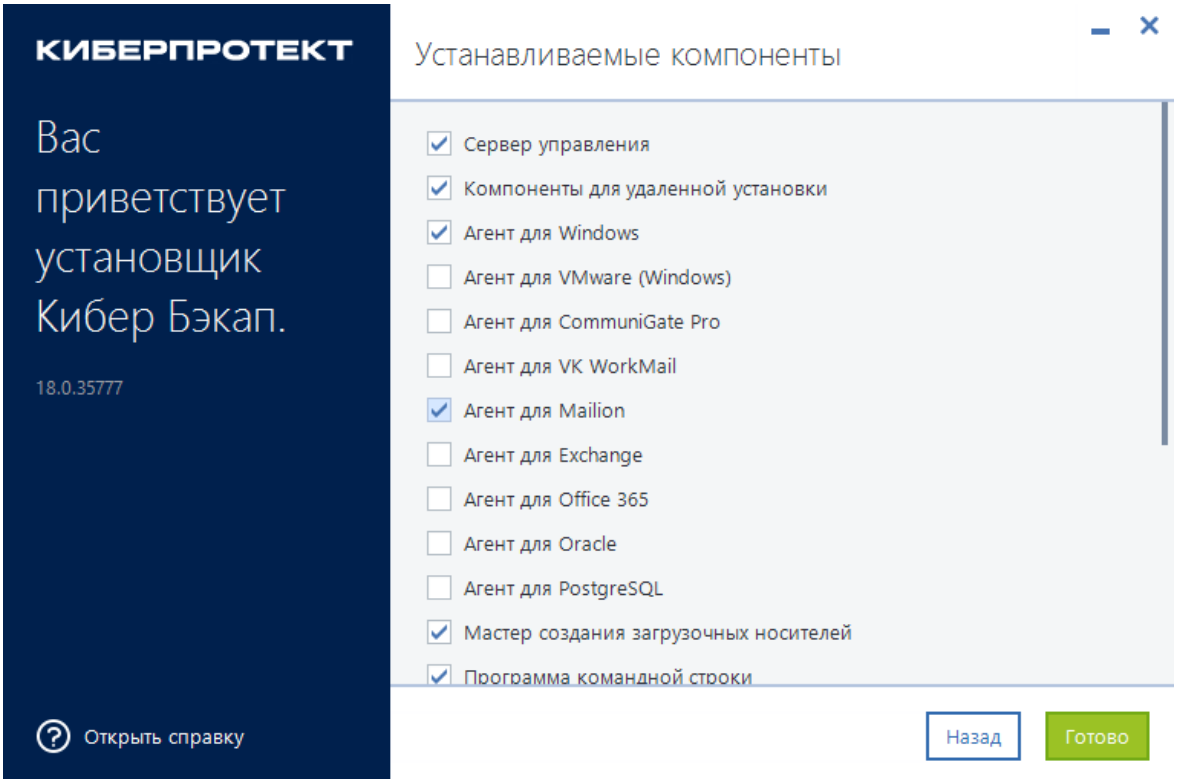
Установка Mailion включает в себя установку агента Кибер Бэкап и добавление хоста Mailion. Добавление хоста возможно лишь после установки агента.

12.4.3.1 Установка агента для Mailion

В этом разделе рассмотрена установка агента Кибер Бэкап для Windows. Для установки агента для Linux обратитесь к разделу "Установка агентов в ОС Linux вручную" (стр. 97).

© ООО Киберпротект, 2026

1. Запустите установщик Кибер Бэкап.
2. Выберите **Настройка параметров установки**.
3. В блоке **Устанавливаемые компоненты** выберите **Изменить**.
4. Отметьте в списке **Агент для Mailion**.

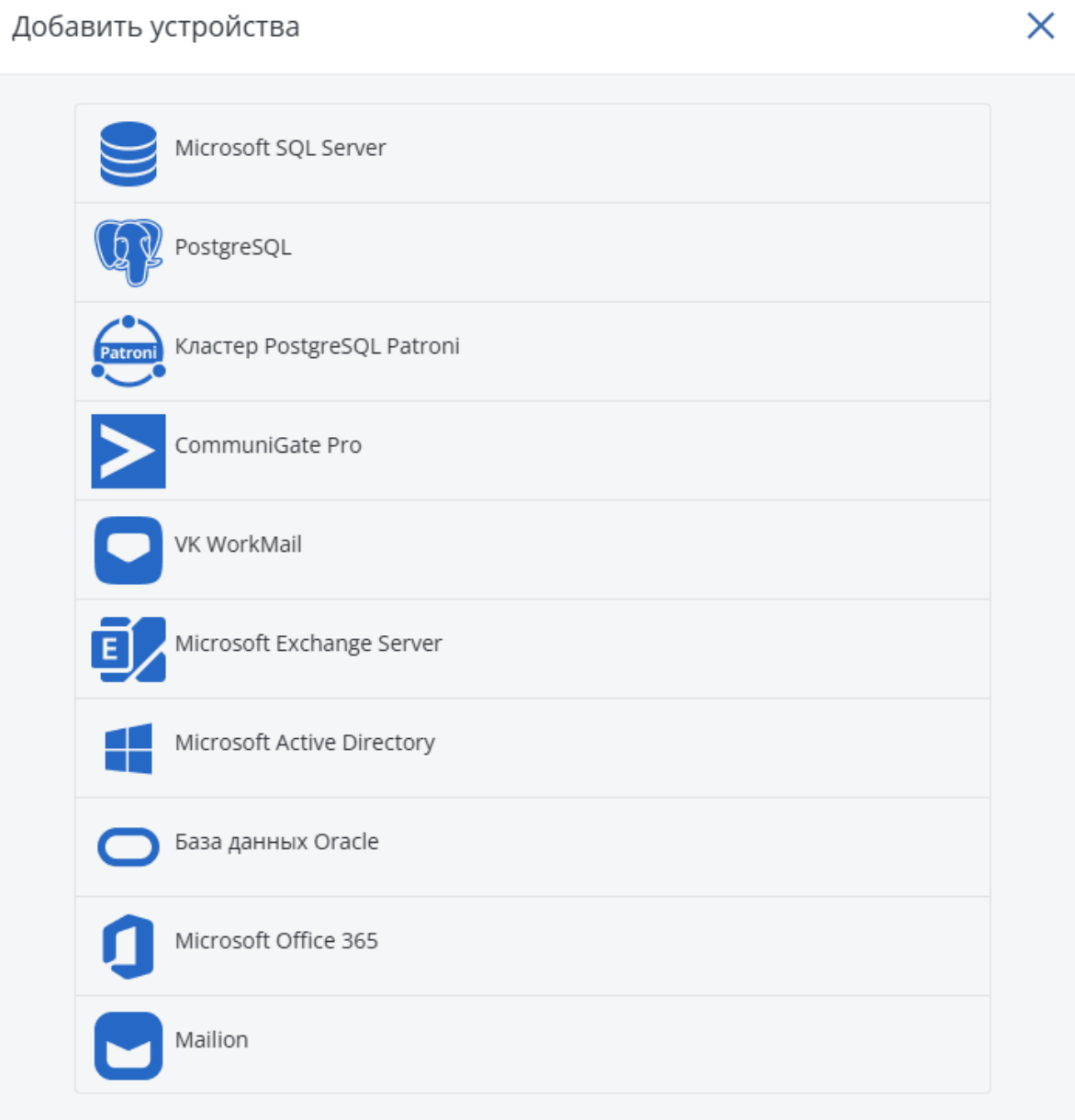


5. Нажмите **Готово**, затем нажмите **Установка**.

12.4.3.2 Добавление хоста Mailion

1. В веб-консоли перейдите на вкладку **Устройства** и нажмите в правом верхнем углу **Добавить**.
2. В окне добавления нового устройства щелкните **Mailion**.

© ООО Киберпротект, 2026

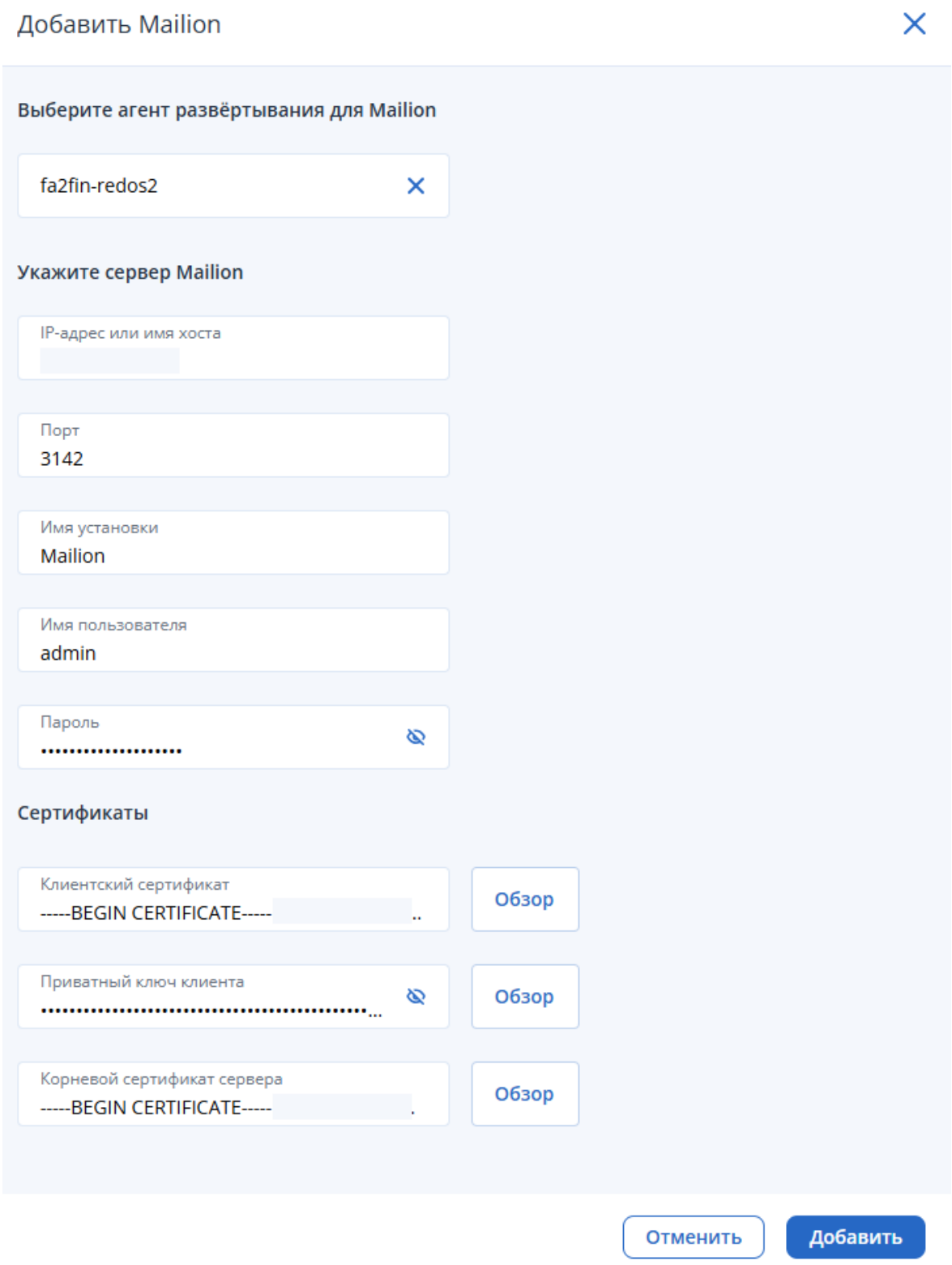


3. В поле **Выберите агент развертывания для Mailion** выберите из списка имя компьютера, на котором установлен агент или начните вводить имя для поиска.
4. В разделе **Укажите сервер Mailion**:
   - в поле **IP-адрес или имя хоста** укажите IP-адрес или имя сервера Mailion;
   - в поле **Порт** укажите порт для подключения к службам резервного копирования Mailion (порт по умолчанию, 3142);
   - в поле **Имя установки** укажите имя, под которым хост будет отображаться в системе;
   - в полях **Имя пользователя** и **Пароль** укажите данные специальной учетной записи backuper с правами на резервное копирование в системе Mailion.
5. В разделе **Сертификаты** укажите файлы сертификатов в формате PEM, созданные при установке и настройке сервера Mailion (для получения сертификатов обратитесь к администратору почтовой системы Mailion):

© ООО Киберпротект, 2026

- **Клиентский сертификат**. Нажмите **Обзор** и укажите личный сертификат пользователя, учетные данные которого используются для подключения к Mailion.
- **Приватный ключ клиента**. Нажмите **Обзор** и укажите закрытый ключ для клиентского сертификата.
- **Корневой сертификат сервера**. Нажмите **Обзор** и укажите Wildcard SSL-сертификат, выпущенный в аккредитованном центре сертификации для используемого экземпляра Mailion.

© ООО Киберпротект, 2026



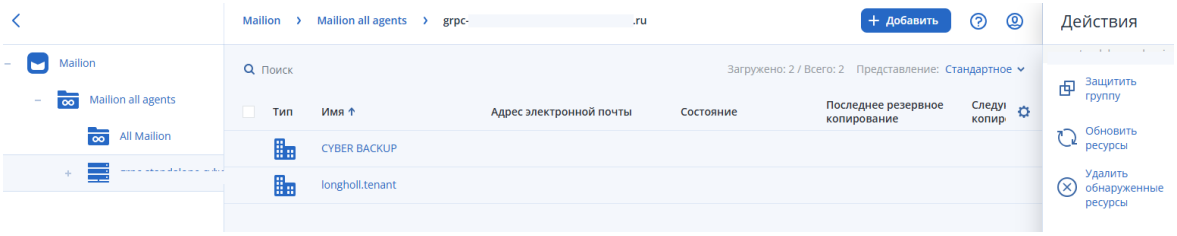
6. По окончании ввода данных нажмите **Добавить**.

12.4.4 Резервное копирование данных Mailion

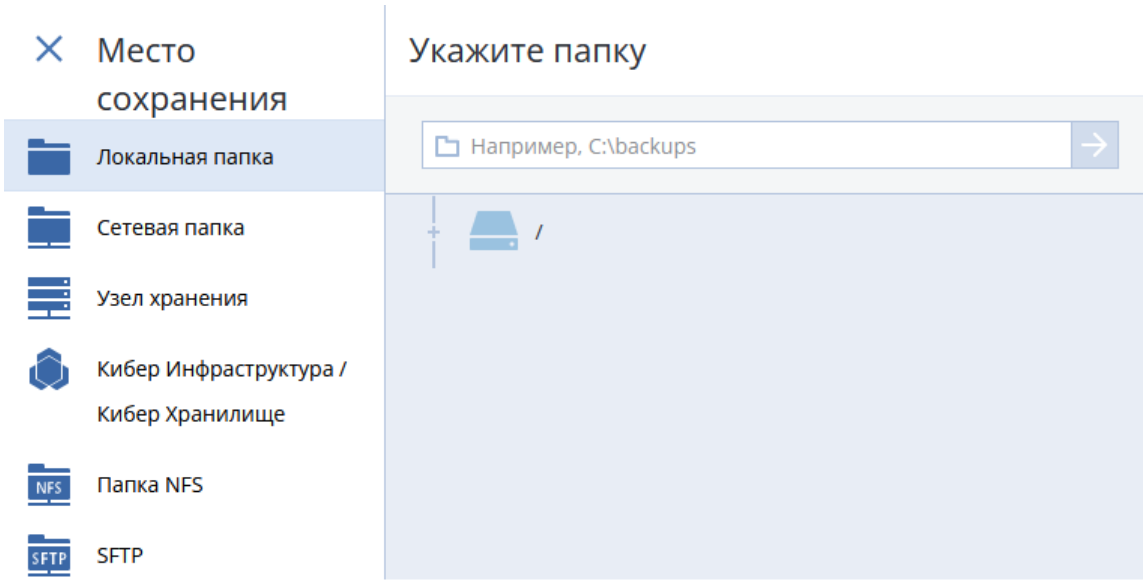
Для создания плана защиты выполните следующие действия:

© ООО Киберпротект, 2026

1. Перейдите в **Устройства** -> **Mailion**.
2. Выберите из списка данные Mailion, которые вы хотите защитить.
3. Перейдите на вкладку справа **Защитить** для защиты данных пользователя или **Защитить группу** для защиты тенанта и пользователей в нем.



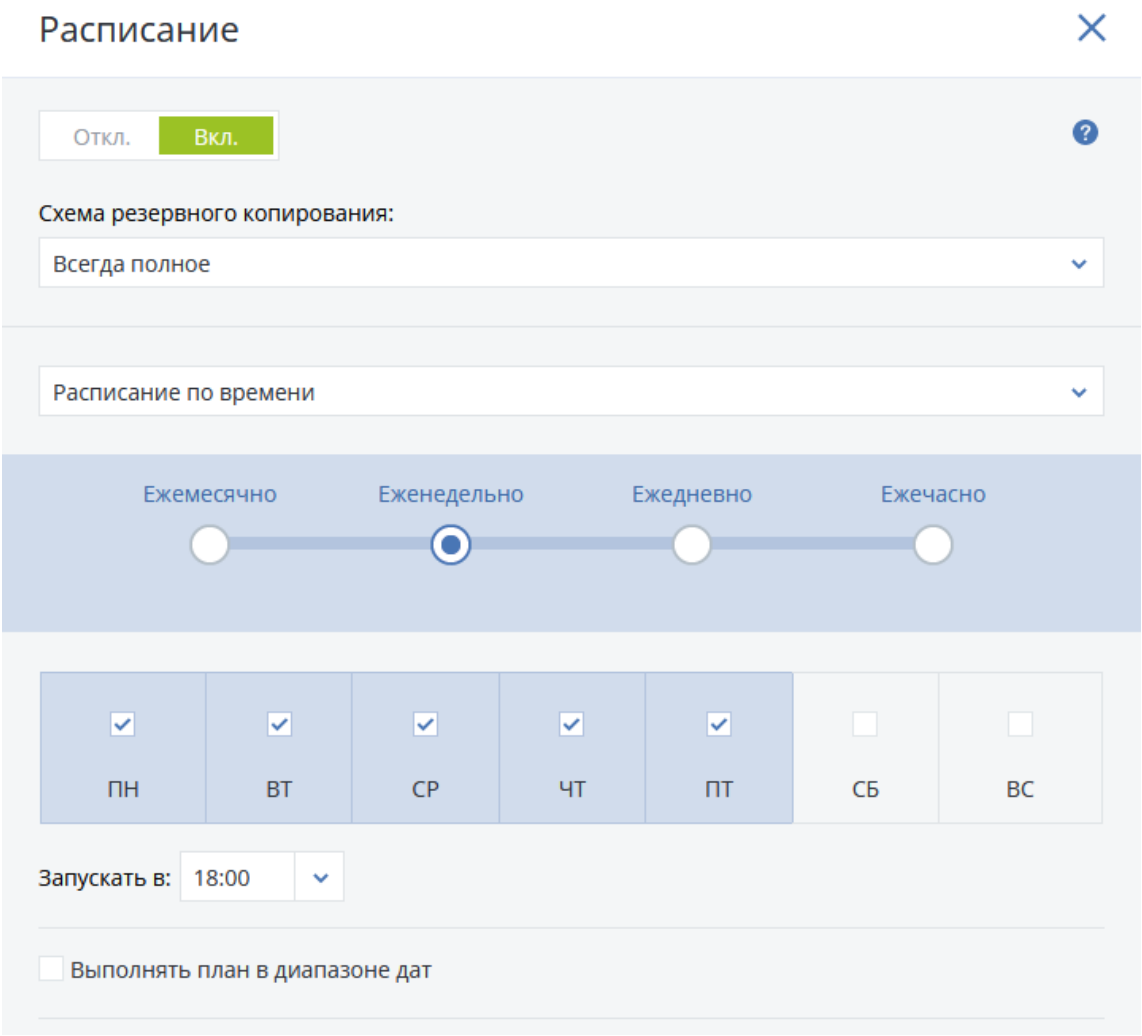
4. Заполните данные в окне создания плана защиты:
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.



   Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места сохранения" (стр. 278).

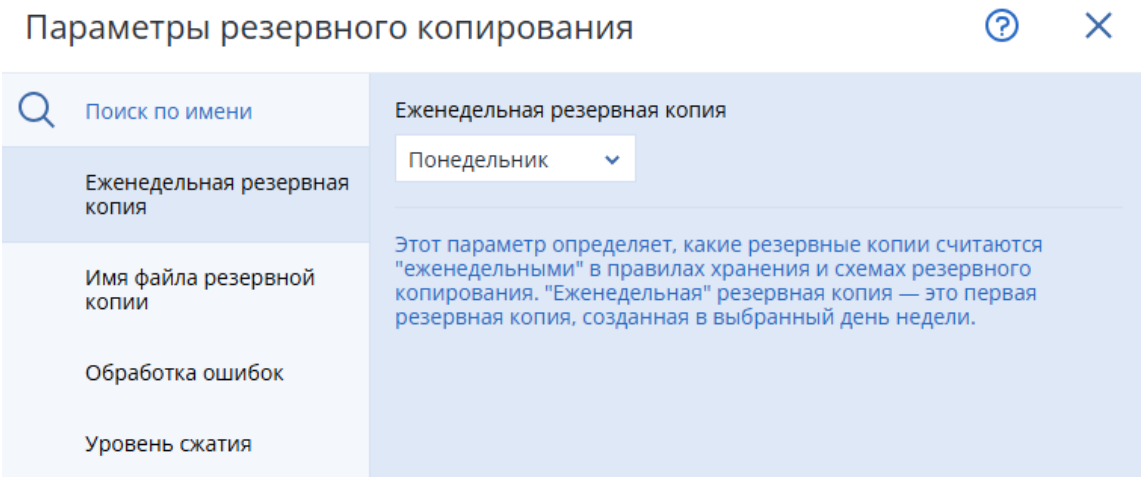
© ООО Киберпротект, 2026

- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.



- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.
- В поле **Назначить задание на кластер почтовых агентов** включите переключатель, чтобы назначить план защиты всем зарегистрированным агентам Mailion.
- [Необязательно] В поле **Параметры резервного копирования** укажите параметры обработки ошибок и уровень сжатия резервных копий.

© ООО Киберпротект, 2026



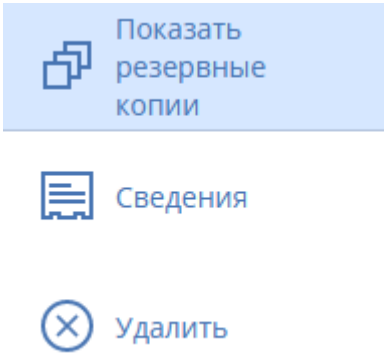
5. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов и будет применен к выбранным данным.

См. также информацию в разделе "План защиты и модули" (стр. 224).

12.4.5 Восстановление данных Mailion

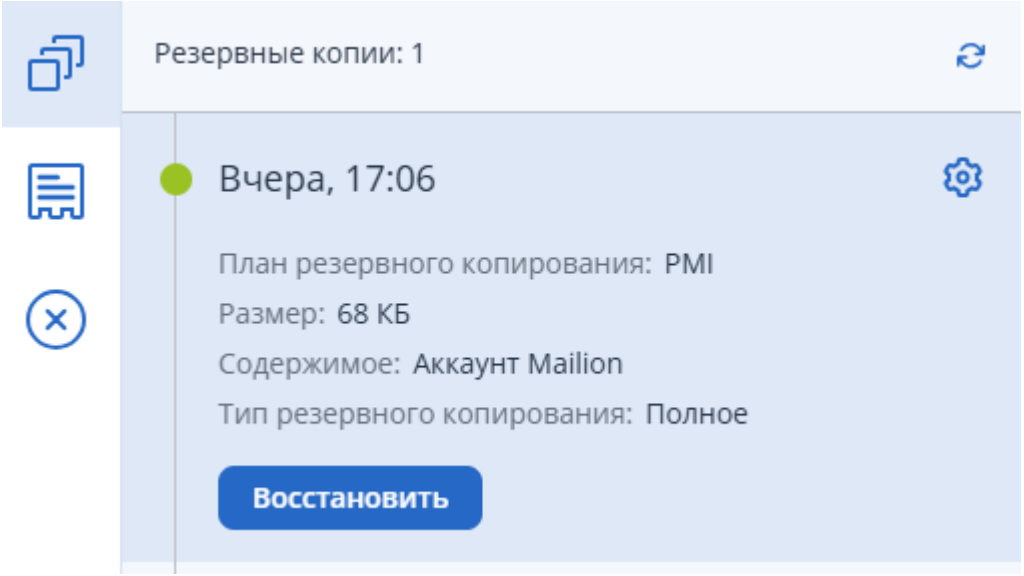
Чтобы восстановить данные Mailion, выполните следующие действия:

1. Перейдите в **Хранилище резервных копий** и выберите в списке нужные данные.
2. Выберите справа **Показать резервные копии**.

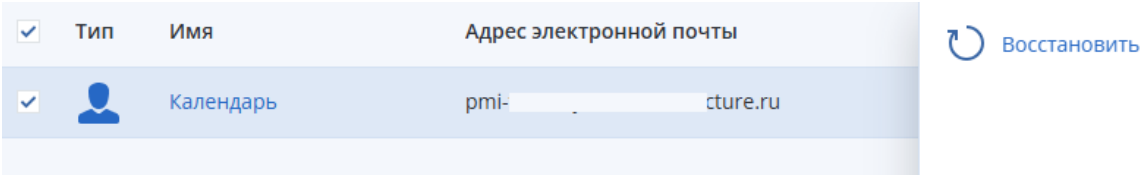


3. Нажмите **Восстановить**.

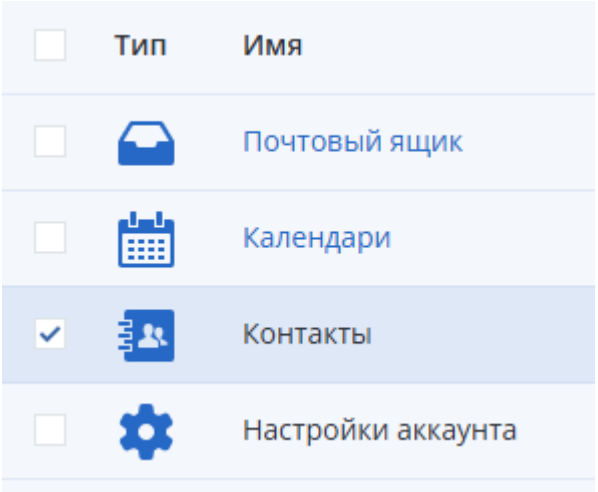
© ООО Киберпротект, 2026



4. Выберите данные для восстановления:
   - Если необходимо восстановить весь почтовый ящик, отметьте галочкой в списке имя почтового ящика, затем выберите справа **Восстановить**.



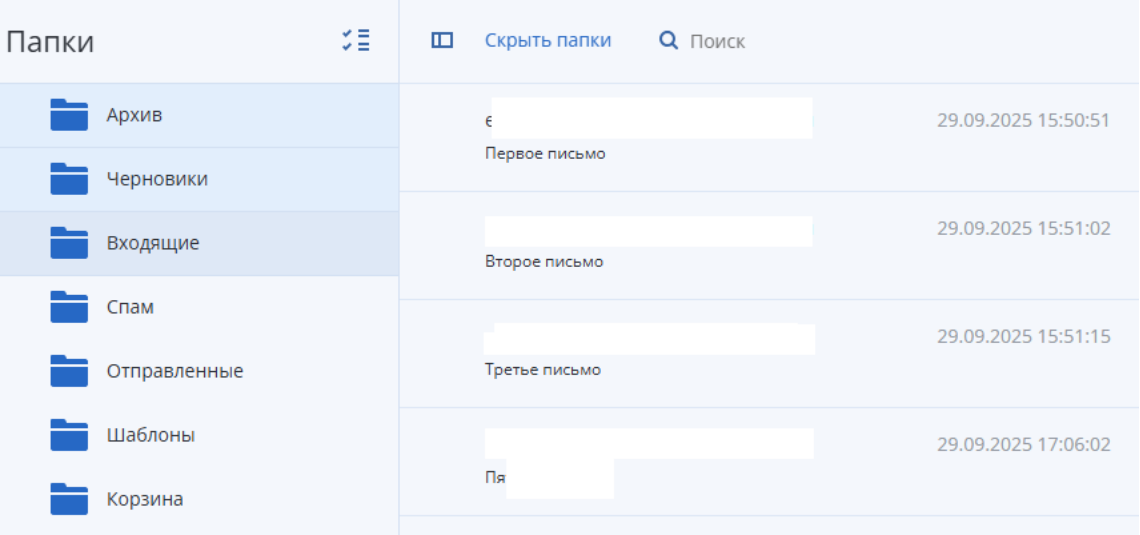
   - Если необходимо восстановить отдельные ресурсы пользователя, нажмите на имя резервной копии. Можно выбрать только один тип ресурса для восстановления. Выберите ресурс и нажмите справа **Восстановить**.



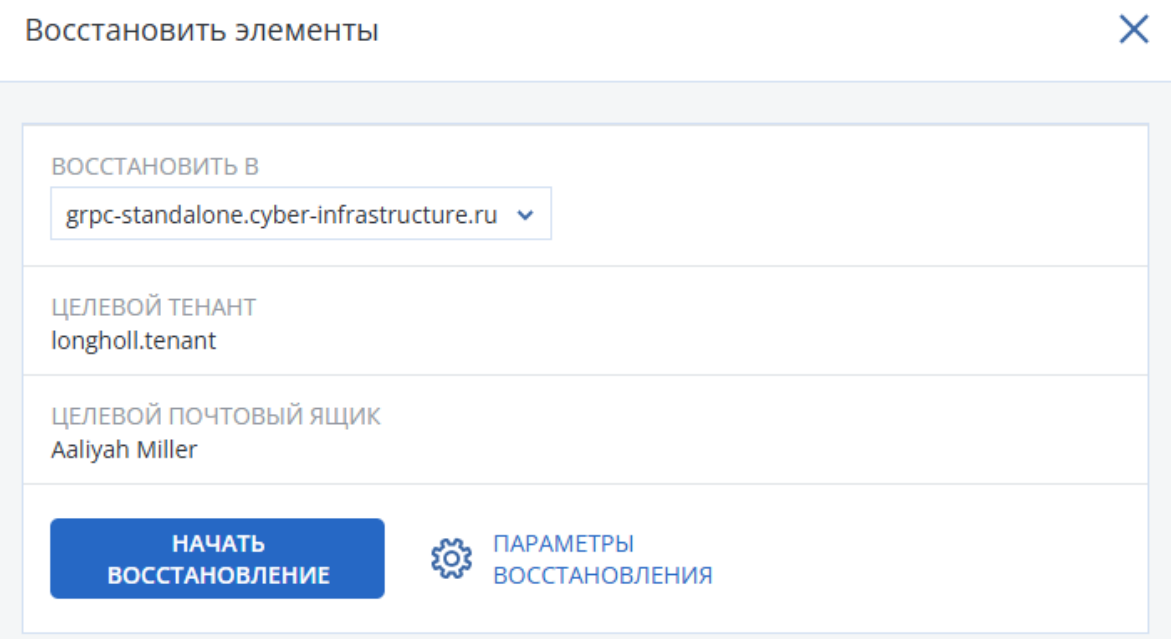
   - Если необходимо восстановить отдельные письма, нажмите на **Почтовый ящик** и выберите

© ООО Киберпротект, 2026

данные, затем нажмите справа **Восстановить**.

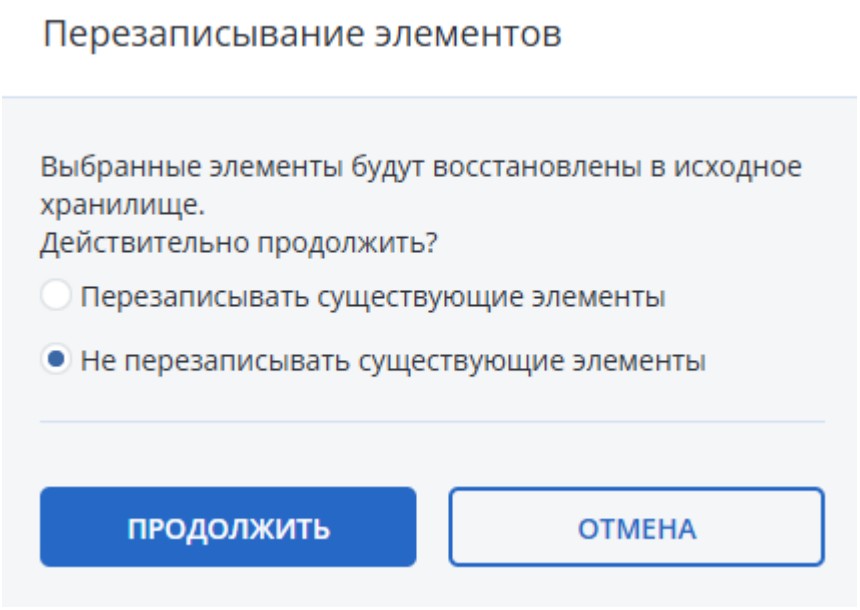


5. Укажите место восстановления. Возможные варианты:
   - Текущий сервер.
   - Новый сервер. Если сервер еще не зарегистрирован в Кибер Бэкап, укажите данные нового сервера как при установке (см. раздел "Установка Mailion" (стр. 559)).



6. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
7. Проверьте правильность заполнения полей и затем нажмите **Начать восстановление**.
8. При восстановлении на текущий сервер укажите признак перезаписывания данных и нажмите **Продолжить**.

© ООО Киберпротект, 2026



9. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.

12.5 Защита Oracle Database

Поддержка резервного копирования баз данных Oracle версий 11-19 осуществляется с помощью команд, выполняемых до и после резервного копирования, в связке с ПО RMAN. Команды позволяют вызывать ПО RMAN для создания первичных резервных копий БД Oracle через интерфейс Кибер Бэкап в рамках планов резервного копирования. При этом сохраняется вся функциональность Кибер Бэкап, доступная для файлового резервного копирования.

В качестве команд до и после резервного копирования можно использовать скрипты ОС и RMAN. Примеры приведены в статье базы знаний.

Примечание
Для работы с Oracle Database версий старше 12 не требуется устанавливать агент для Oracle, как описано в разделе "Защита Oracle Database предыдущих версий" (стр. 570). Для таких версий необходим только агент для Linux (см. "Установка агентов в ОС Linux вручную" (стр. 97)).

Это позволит использовать все преимущества RMAN, включая:

- Различные типы резервного копирования:
  - Full Backup,
  - Incremental Backup,
  - Differential Backup,
  - Cumulative Backup,
  - Archivelog Backup.

© ООО Киберпротект, 2026

- Выполнение резервного копирования как промышленных БД, так и копий горячего резерва (Standby).
- Выполнение резервного копирования БД в конфигурации кластера Oracle RAC.
- Восстановление на заданные точки во времени (Point-in-Time Recovery, PITR):
  - с указанием времени в различных вариантах,
  - с указанием номера изменения БД (SCN).

12.5.1 Защита Oracle Database предыдущих версий

В данном разделе описано, как настроить резервное копирование баз данных Oracle следующих версий:

- Oracle Database 11g, все выпуски;
- Oracle Database 12c, все выпуски.

Поддерживаются только конфигурации с одним экземпляром.

Условия для резервного копирования

Для резервного копирования баз данных Oracle понадобится Кибер Бэкап 15 или новее с лицензией «Кибер Бэкап для физического сервера» на каждый экземпляр Oracle Database, резервное копирование которого вы планируете выполнять (список лицензий см. в разделе "Издания и лицензии Кибер Бэкап" (стр. 16)).

Для выполнения резервного копирования нужно установить агент Кибер Бэкап для операционной системы, которую вы используете (Windows или Linux), а также агент для Oracle. Список поддерживаемых операционных систем см. в разделе "Агенты" (стр. 23).

Предварительные требования для резервных копий машин Windows с поддержкой приложений описаны в разделе "Предварительные требования" (стр. 477).

12.5.1.1 Методы резервного копирования

Решение Кибер Бэкап предоставляет два метода защиты данных Oracle. Оба метода позволяют использовать функциональность управления резервными копиями: централизованное управление, репликация, хранение, уведомления электронной почты и другие возможности.

Резервное копирование сервера

Создайте резервную копию всего сервера Oracle, используя резервное копирование с поддержкой приложений для согласованности состояния базы данных Oracle с приложениями.

Преимущества:

- Меньшее директивное время восстановления при сбое всего сервера.
- Резервное копирование полностью настраивается в графическом интерфейсе пользователя. Не обязательно иметь навыки работы с Oracle Recovery Manager (RMAN).

© ООО Киберпротект, 2026

- Имея резервную копию всего сервера, можно легко создать виртуальную машину, которая развертывается за считанные секунды и заменяет исходный сервер.

Ограничения:

- База данных должна храниться в обычной файловой системе, поддерживаемой программой резервного копирования. Разделы без форматирования и тома Oracle Automatic Storage Management (ASM) не поддерживаются.

Резервное копирование базы данных

Создайте резервную копию базы данных Oracle с помощью Oracle Recovery Manager (RMAN) в локальной папке, затем создайте резервную копию полученных файлов в другом хранилище, сохранив в локальной папке только последние резервные копии RMAN. Решение предоставляет сценарии RMAN, которые могут автоматически запускаться до резервного копирования файлов. Поэтому всю процедуру можно настроить и выполнить в одном рабочем процессе. При этом не требуется навыков создания сценариев RMAN.

Преимущества:

- Поддержка баз данных, которые хранятся на необработанных разделах или томах Oracle Automatic Storage Management (ASM).

Ограничения:

- Большее директивное время восстановления при сбое всего сервера.

Сравнительная характеристика

Показатель	Резервное копирование сервера	Резервное копрование базы данных
Директивное время восстановления при сбое всего сервера	Меньше	Больше
Возможность запускать виртуальный сервер Oracle	Да, ESX или Hyper-V	Нет
Поддержка разделов без форматирования/ASM	Нет	Да
Поддержка распространения базы данных на несколько томов	Да	Да
Простота использования	Резервное копирование полностью настраивается в графическом интерфейсе пользователя. Нет	Необходимо настроить отдельные планы резервного копирования для полных резервных копий

© ООО Киберпротект, 2026

	необходимости знать RMAN.	архивированного журнала.

12.5.1.2 Методы восстановления

Восстановление сервера

Восстановление всего сервера на момент времени создания резервной копии. При восстановлении сервера на "голое железо" Oracle Database восстанавливается среди других данных и будет в согласованном состоянии.

Преимущества:

- Самый быстрый и простой способ аварийного восстановления.
- Позволяет выполнить миграцию физической машины на виртуальную (P2V), а также воспользоваться другими методами репликации или миграции сервера Oracle.
- Не обязательно иметь навыки работы с Oracle Recovery Manager (RMAN).

Восстановление с использованием Oracle Explorer

Восстанавливайте файлы данных по состоянию на определенный момент времени, используя инструмент Oracle Explorer, который входит в состав решения. Данный инструмент использует RMAN и включает в себя целый ряд полезных параметров RMAN в удобном пользовательском интерфейсе. Этот инструмент позволяет выполнить восстановление как с резервных копий с поддержкой приложений, так и с резервных копий баз данных.

Преимущества:

- Позволяет выполнить фрагментарное восстановление данных Oracle на определенный момент времени непосредственно с резервных копий с поддержкой приложений.
- Не обязательно иметь навыки работы с Oracle Recovery Manager (RMAN).

Ограничения:

- При восстановлении с резервных копий баз данных может потребоваться двухэтапный процесс.

Восстановление с использованием сценариев

Восстанавливайте базу данных по состоянию на время создания последней резервной копии с локально сохраненных резервных копий RMAN. Для такого восстановления решение предоставляет сценарий RMAN. Чтобы восстановить базу данных по состоянию на время создания предыдущей резервной копии RMAN, сначала восстановите эту резервную копию RMAN из резервной копии на уровне файлов, а затем используйте сценарии для восстановления базы данных.

Те же самые операции восстановления можно выполнить с файлами данных и файлом управления. Это решение предоставляет отдельные сценарии для этих операций восстановления.

© ООО Киберпротект, 2026

Кроме того, это решение предоставляет отдельные сценарии для восстановления по состоянию на настраиваемый момент времени. Этот момент времени можно задать, указав точную дату и время или номер системного изменения (SCN).

Преимущества:

- Можно настроить восстановление в расширенных сценариях.

Ограничения:

- Для выполнения настройки требуется знание RMAN.
- Может потребоваться двухэтапный процесс восстановления.

12.5.1.3 Общие ограничения

- Кластеры Oracle Real Application (RAC) не поддерживаются.
- Поддерживаются только конфигурации базы данных с одним экземпляром.
- Невозможно создать резервную копию отдельных подключаемых баз данных (pluggable database, PDB). Для них резервные копии создаются как часть контейнерной базы данных (container database, CDB).
- База данных должна быть в режиме ARCHIVELOG (флаг **NOARCHIVELOG** отключен).

  Базу данных в режиме NOARCHIVELOG можно скопировать только в закрытом состоянии, а решение для резервного копирования рассчитано на то, чтобы создавать резервные копии баз данных без простоя. Если включенная база данных работает в этом режиме, а RMAN больше невозможно использовать, при попытке создать резервную копию на уровне дисков будет возвращена ошибка VSS.

  Чтобы избежать этой ошибки, остановите и закройте базу данных командой до захвата данных и перезапустите базу данных командой после захвата данных. Можно будет восстановить весь сервер, но восстановление через Oracle Explorer будет недоступно.

12.5.1.4 Установка

Компоненты программного обеспечения для резервного копирования

Чтобы защитить данные Oracle, необходимы следующие компоненты:

- **Сервер управления** позволяет централизованно управлять несколькими машинами: создавать планы резервного копирования, отслеживать их выполнение, развертывать агенты и выполнять другие действия. Его можно установить на машине с Windows или Linux, которая имеет сетевой доступ ко всем управляемым машинам.

  Чтобы установить сервер управления, выполните действия, описанные в разделе "Установка сервера управления" (стр. 63).
- **Агенты** необходимы для резервного копирования серверов и баз данных.
  - Чтобы защитить физический или виртуальный сервер, на котором работает Oracle Database, установите на этот компьютер **Агент для Oracle**. **Агент для Windows** или **Агент для Linux** (в

© ООО Киберпротект, 2026

зависимости от операционной системы сервера) и **агент для Oracle** должны быть установлены на физической машине с Oracle Database. В Linux **Агент для Oracle** использует тот же установщик, что и **Агент для Linux**.

- **Oracle Explorer** предназначен для фрагментарного восстановления данных Oracle. Этот компонент входит в состав агента для Oracle.

Чтобы установить агенты, выполните действия, описанные в разделе "Установка агентов" (стр. 95).

- **Python 3** на машине с агентом для Oracle необходим для резервного копирования и восстановления Oracle Database. Путь к интерпретатору Python (python для Linux или python.exe для Windows) должен быть добавлен в переменную окружения PATH.

Сценарии интеграции с Oracle RMAN

Эти сценарии автоматически устанавливаются вместе с агентом для Oracle.

Эти сценарии устанавливаются в следующую папку:

- В Windows: **%ProgramFiles%\Acronis\Oracle**.
- В Linux: **/usr/lib/Acronis/Oracle**.

Далее эта папка называется <папка расположения сценариев>.

Список сценариев

В таблице ниже перечислены предоставляемые сценарии.

Имя сценария	Для Windows или Linux?	Описание
main.py	Windows, Linux	Основной сценарий, который выполняет все операции, связанные с резервным копированием и восстановлением Oracle. Не предназначен для независимого использования.
main.cfg	Windows, Linux	Конфигурационный файл содержит параметры доступа к базе данных и другие параметры, которые являются общими для других сценариев. Это – единственный файл, в который может потребоваться внести изменения. Этот файл расположен в следующей папке: • В Windows: **%ProgramData%\Acronis\Oracle\Config** • В Linux: **/var/lib/Acronis/Oracle/Config**
backup_full_pre.bat	Windows	Вызывает основной сценарий для создания полной резервной копии базы данных утилитой RMAN.
backup_full_pre.sh	Linux	

© ООО Киберпротект, 2026

backup_incr_pre.bat	Windows	Вызывает основной сценарий для создания резервной копии архивированных журналов утилитой RMAN.
backup_incr_pre.sh	Linux	
restore_disaster.bat	Windows	Вызывает основной сценарий для восстановления всей базы данных до последнего доступного состояния.
restore_disaster.sh	Linux	
restore_datafiles.bat	Windows	Вызывает основной сценарий для восстановления файлов данных до последнего доступного состояния (полное восстановление).
restore_datafiles.sh	Linux	
restore_controlfile.bat	Windows	Вызывает основной сценарий для восстановления файла управления до последнего доступного состояния.
restore_controlfile.sh	Linux	
restore_to-point-in-time.bat	Windows	Вызывает основной сценарий для восстановления базы данных до состояния на определенный момент времени в прошлом (неполное восстановление). Такой момент времени указывается датой и временем в следующем формате: гггг-мм-дд:чч24:мм:сс.
restore_to-point-in-time.sh	Linux	
restore_to-scn.bat	Windows	Вызывает основной сценарий для восстановления базы данных до состояния на определенный момент времени в прошлом (неполное восстановление). Такой момент времени задается номером системного изменения (SCN).
restore_to-scn.sh	Linux	
last_log.bat	Windows	Вызывает основной сценарий, чтобы показать его последний журнал.
last_log.sh	Linux	
***.rman**	Windows, Linux	Сценарии RMAN для различных операций. Не предназначен для независимого использования.
***.sql**	Windows, Linux	Сценарии SQL*Plus для различных операций. Не предназначен для независимого использования.
Other	Windows, Linux	Вспомогательные сценарии. Не предназначен для независимого использования.

© ООО Киберпротект, 2026

Параметры конфигурации

В этом разделе перечислены параметры, которые можно изменить в файле **main.cfg**. Эти параметры влияют только на резервное копирование базы данных. Резервное копирование сервера не использует эти параметры.

- BACKUP_DIR: локальная папка, в которой будут храниться резервные копии RMAN.

  На диске, на котором вы хотите хранить резервные копии RMAN, должно быть достаточно свободного места для двух копий базы данных.

  Путь по умолчанию: **C:\local_rman_backups** в Windows и **/tmp/local_rman_backups** в Linux.

  Примечание
  В Windows используйте две обратные косые черты вместо одной. Например, путь по умолчанию: **C:\\local_rman_backups**.

- TARGET: строка подключения для базы данных.

  Значение по умолчанию: **/**. Если задано это значение, сценарий выполняет вход в Oracle с использованием аутентификации операционной системы.

  Примечание
  Поддерживается только аутентификация операционной системы. В Windows данный сценарий использует учетную запись, с которой запускается служба агента. В Linux данный сценарий использует значение переменной ORACLE_USER (см. далее в этом разделе). Как в Windows, так и в Linux учетная запись, которую вы указываете, должна иметь системную привилегию SYSDBA в Oracle. Чтобы предоставить эту привилегию, добавьте пользователя в группу ORA_DBA.

  Чтобы использовать проверку подлинности базы данных, укажите строку подключения в следующем формате:

  В этом выражении

  - <имя_пользователя>/<пароль> – это учетные данные сценария, который будет использоваться для входа в Oracle. Эта учетная запись должна иметь системную привилегию SYSDBA в Oracle.
  - <идентификатор подключения> – это идентификатор подключения Oracle Net. Это может быть имя сетевой службы, имя службы базы данных или имя сетевой службы. Идентификатор подключения требуется в Oracle Database Engine 12 для того, чтобы строка подключения указывала на контейнерную базу данных (CDB), а не на подключаемую базу данных (PDB).

  Пример. Чтобы для подключения к базе данных, которая имеет псевдоним Oracle Net FLEETDB, сценарий использовал имя пользователя, для параметра TARGET введите значение HR/password@FLEETDB.

В Linux может потребоваться дополнительно изменить указанные ниже переменные среды Oracle, чтобы они соответствовали фактическим настройкам Oracle Database:

© ООО Киберпротект, 2026

- ORACLE_BASE: корень дерева каталогов Oracle Database. Значение по умолчанию: /u01/app/oracle. Чтобы узнать фактическое значение, выполните команду env | grep ORACLE_ BASE под учетной записью, которая имеет системную привилегию SYSDBA в Oracle.
- ORACLE_HOME: расположение конкретной установки Oracle Database. Значение по умолчанию: /u01/app/oracle/product/12.1.0.2/db_1/. Чтобы узнать фактическое значение, выполните команду env | grep ORACLE_HOME под учетной записью, которая имеет системную привилегию SYSDBA в Oracle.
- ORACLE_SID: системный идентификатор базы данных. Значение по умолчанию orcl. Чтобы узнать фактическое значение, выполните команду env | grep ORACLE_SID под учетной записью, которая имеет системную привилегию SYSDBA в Oracle.
- ORACLE_USER: учетная запись, которую RMAN и SQL*Plus используют для входа в Oracle, когда параметр TARGET имеет значение / (см. описание параметра TARGET выше). Значение по умолчанию: oracle. Учетная запись, которую вы указываете, должна иметь системную привилегию SYSDBA в Oracle. Кроме того, эта учетная запись должна входить в группу **acronis** . Эта группа автоматически создается во время установки агента для Oracle и определяется в файле /etc/passwd. Если учетная запись ORACLE_USER не входит в группу **acronis**, используйте команду groupadd чтобы добавить ее.
- RMAN_PATH: каталог с утилитой RMAN.

  Значение по умолчанию: $ORACLE_HOME/bin. Чтобы узнать фактическое значение, выполните команду which rman под учетной записью, которая имеет системную привилегию SYSDBA в Oracle. Например, если команда возвращает строку /u01/app/oracle/product/12.1.0.2/db_ 1/lib/rman, задайте переменной RMAN_PATH значение $ORACLE_HOME/lib.

12.5.1.5 Резервное копирование базы данных Oracle

Подготовка

Выберите локальную папку, в которой будут храниться резервные копии RMAN. На диске, выделенном для хранения резервных копий RMAN, должно быть достаточно свободного пространства для двух копий базы данных. Не выбирайте тот же диск, на котором хранится база данных.

Путь по умолчанию: **C:\local_rman_backups** в Windows и **/tmp/local_rman_backups** в Linux. Чтобы изменить этот путь, измените значение параметра BACKUP_DIR в файле **main.cfg** как описано в разделе "Параметры конфигурации" (стр. 576).

Если папка не существует, создайте ее вручную заранее. Указанные ниже пользователи должны иметь разрешение на чтение в отношении этой папки:

1. Учетная запись, с которой выполняется служба агента.
2. Учетная запись, с которой выполняется служба экземпляра (OracleService<Идентификатор базы данных>).
3. [Только в Linux] Суперпользователь.

При необходимости измените другие параметры конфигурации сценария.

© ООО Киберпротект, 2026

Создание планов резервного копирования

Чтобы создать резервную копию базы данных Oracle, создайте один или несколько планов резервного копирования. Один из них является обязательным: сначала создается полная резервная копия RMAN, затем создается полная резервная копия полученных файлов в другое хранилище. Другой план является дополнительным: сначала создается резервная копия архивированных журналов RMAN, затем создается инкрементная резервная копия полученных файлов в том же самом хранилище и с таким же именем файла, как и у полной резервной копии. Используйте второй план для резервного копирования архивированных журналов чаще, чем для создания резервной копии базы данных.

Прежде чем приступить к созданию резервных копий архивированных журналов, сначала необходимо создать полную резервную копию RMAN. Пока не будет создана полная резервная копия, невозможно будет восстановить базу данных. Если по расписанию первым запускается инкрементное резервное копирование, запустите перед ним создание полной резервной копии вручную.

Порядок создания плана резервного копирования для полных резервных копий

Следуйте указанным ниже инструкциям:

1. В области **Элементы для резервного копирования** выберите вариант **Файлы/папки**. Выберите папку для хранения резервных копий RMAN.
2. В разделе **Расписание** > **Схема резервного копирования** выберите **Всегда полное** или **Пользовательская**.
3. Укажите расписание резервного копирования. Если выбрана схема резервного копирования **Пользовательская**, укажите в этом разделе только расписание полного резервного копирования.

   Рекомендуем создавать полные резервные копии один раз в неделю.
4. В разделе параметров резервного копирования выполните следующие действия:
   a. Щелкните **Имя файла резервной копии** и измените шаблон измени файла. Не используйте переменные [Plan ID] и [Plan name].

      Запомните или запишите указанный шаблон, поскольку вам нужно будет задать то же самое значение во втором плане резервного копирования.
   b. Щелкните **Pre/post-команды**.
   c. Включите переключатель **Выполнение команды до резервного копирования**.
   d. Укажите следующие настройки.

      [В Windows]

      - В поле **Команда** введите <папка со сценариями>\backup_full_pre.bat.
      - В поле **Рабочая директория** введите <папка со сценариями>.

      [В Linux]

© ООО Киберпротект, 2026

- В поле **Команда** введите /<папка со сценариями>/backup_full_pre.sh.
- В поле **Рабочая директория** введите /<папка со сценариями>/.

Порядок создания плана резервного копирования для резервных копий архивированного журнала

Следуйте указанным ниже инструкциям:

1. В области **Элементы для резервного копирования** выберите **Файлы/папки**. Выберите папку для хранения резервных копий RMAN.
2. В области **Место сохранения** выберите то же самое хранилище резервных копий, в котором хранятся полные резервные копии.
3. В разделе **Расписание** > **Схема резервного копирования** выберите **Пользовательская**.
4. Измените расписание резервного копирования для полных резервных копий. Поскольку в этом случае нет необходимости создавать полные резервные копии, они должны быть полностью исключены из расписания.

   Рекомендуем изменить расписание на **По событию в журнале событий Windows** и оставить другие параметры без изменений.
5. Укажите расписание резервного копирования для инкрементных резервных копий.

   Мы рекомендуем создавать инкрементные резервные копии каждый день недели, кроме дня, выбранного для полных резервных копий.
6. В разделе параметров резервного копирования выполните следующие действия:
   a. Щелкните **Имя файла резервной копии** и укажите такой же шаблон имени файла, который используется для полных резервных копий.
   b. Щелкните **Pre/post-команды**.
   c. Включите переключатель **Выполнение команды до резервного копирования**.
   d. Укажите следующие настройки.

      [В Windows]
      - В поле **Команда** введите <папка со сценариями>\backup_incr_pre.bat.
      - В поле **Рабочая директория** введите <папка со сценариями>.

      [В Linux]
      - В поле **Команда** введите /<папка со сценариями>/backup_incr_pre.sh.
      - В поле **Рабочая директория** введите /<папка со сценариями>/.

12.5.1.6 Резервное копирование сервера

При создании плана защиты сервера с базой данных Oracle следуйте инструкции:

1. Выберите всю машину. В противном случае невозможно будет создать резервную копию с поддержкой приложений.
2. Щелкните **Резервное копирование приложения** и включите переключатель **Oracle Database**.
3. В разделе параметров резервного копирования выполните следующие действия:

© ООО Киберпротект, 2026

a. Убедитесь, что параметр **Многотомные моментальные снимки** включен.

b. [Только для Windows] Убедитесь, что для физических машин включен параметр резервного копирования **Служба теневого копирования томов (VSS)**. Рекомендуем не менять установленное по умолчанию **Автоматически выбирать поставщика моментальных снимков**, если на то нет причин.

Эти настройки обеспечивают правильную фиксацию и запись базы данных при создании моментального снимка. В результате резервная копия приложения будет полностью согласованной.

Дополнительную информацию о резервном копировании см. в разделе "Резервное копирование" (стр. 264).

12.5.1.7 Восстановление всего сервера

1. Выполните действия, как описано в разделе "Восстановление машины" (стр. 384).
2. Если за период времени, прошедшего с момента создания резервной копии, с которой выполнено восстановление, есть доступные журналы (например, они могут храниться на отдельном неуправляемом томе или по отдельности в разных местах), после восстановления сервера восстановите их к последнему актуальному состоянию с помощью RMAN.

12.5.1.8 Восстановление баз данных Oracle с использованием Oracle Explorer

Oracle Explorer

Oracle Explorer может взаимодействовать только с агентом для Oracle, который установлен на том же сервере.

- В Windows Oracle Explorer расположен в папке **%ProgramFiles%\Acronis\OracleExplorer**. Чтобы запустить этот инструмент, можно использовать ярлык, созданный на рабочем столе после установки агента для Oracle.
- В Linux запустите /usr/lib/Acronis/OracleExplorer/oracle_explorer.sh.

Oracle Explorer восстанавливает данные Oracle в два этапа. На первом этапе восстанавливаются требуемые файлы Oracle (файлы данных, файл параметров сервера, контрольный файл и архивированные журналы) из резервной копии с поддержкой приложений или из резервной копии базы данных. Если эти файлы не нужно восстанавливать, этот шаг можно пропустить. Затем инструмент вызывает команду восстановления RMAN, которая применяет журналы отката и выполняет другие операции, чтобы привести базу данных в нужное состояние.

Порядок восстановления данных Oracle

1. Запустите Oracle Explorer.
2. Выберите хранилище резервных копий. Если потребуется, укажите имя пользователя и пароль для доступа к хранилищу.

© ООО Киберпротект, 2026

3. Выберите резервную копию. Если потребуется, укажите пароль для зашифрованной резервной копии.
4. Выберите точку восстановления и базу данных для восстановления.
5. Выберите файлы Oracle для восстановления из резервной копии. Если эти файлы не нужно восстанавливать, пропустите этот шаг.

   Рекомендуется выбрать табличные пространства и архивированные журналы. При восстановлении контрольного файла необходимо будет создать новое олицетворение базы данных. При восстановлении файла параметров сервера будут утрачены изменения, внесенные в параметры экземпляра после создания резервной копии.

   Если выбран вариант восстановления журналов архива, выберите журналы для восстановления.

   Файлы Oracle всегда будут восстанавливаться в исходное хранилище и перезаписываться.
6. [Необязательно] Выберите параметры восстановления:
   - Момент времени, по состоянию на который будет восстанавливаться база данных.

     Это может быть восстановление до последнего доступного состояния (полное восстановление) или восстановление до момента времени в прошлом (неполное восстановление). Такой момент времени указывается через дату и время из интервала между точкой восстановления, выбранной раньше, и текущим моментом или через номер системного изменения (SCN).
   - Определяет, открывать ли базу данных после восстановления.

     Не открывайте базу данных, если вы планируете выполнять ручные операции восстановления, используя RMAN.
   - Определяет, сбрасывать ли журналы.

     Этот параметр необходимо использовать с осторожностью, поскольку при сбросе журналов отката создается новое олицетворения базы данных. Это может обусловить ограничения для отката базы данных к предыдущему олицетворению.
   - Учетная запись, с которой выполняется восстановление.
   - Файлы базы данных также можно восстановить без запуска операции восстановления RMAN, если вы планируете выполнить восстановление позже.

   Далее в этом разделе описан ряд основных сценариев восстановления с рекомендуемыми параметрами, которые можно выбрать в каждом случае.

Восстановление до последнего состояния

Используйте эту процедуру, если файлы данных потеряны или повреждены, а также при сбоях базы данных, относящихся к другим типам. Предполагается, что контрольный файл и файл параметров сервера рабочие.

Этот сценарий также можно использовать, чтобы привести базу данных в актуальное состояние после восстановления всего сервера с более старой резервной копии на уровне диска.

В этом сценарии при необходимости выберите **Табличные пространства** и **Журналы архива**. В параметрах восстановления выберите **Восстановить к последнему доступному состоянию**, не

© ООО Киберпротект, 2026

снимайте флажок **Открыть базу данных после восстановления** и не устанавливайте флажок **Сбросить журналы**.

Восстановление по состоянию на более ранний момент времени

Используйте эту процедуру, когда база данных функционирует должным образом, но вам нужно откатить ее к предыдущему состоянию.

В этом сценарии при необходимости выберите **Табличные пространства** и **Журналы архива**. В параметрах восстановления выберите **Восстановить на момент времени** или **Восстановить до номера системного изменения (SCN)**; укажите дату и время или SCN, по состоянию на которые необходимо восстановить базу данных; не снимайте флажок **Открыть базу данных после восстановления** и установите флажок **Сбросить журналы**.

12.5.1.9 Восстановление данных Oracle с помощью сценариев

Восстановление резервной копии RMAN из резервной копии на уровне файлов

Выполните эту операцию в следующих ситуациях:

- Последняя резервная копия RMAN потеряна или повреждена.
- Необходимо восстановить базу данных до состояния на предыдущий момент времени.

Порядок восстановления:

Выполните действия, как описано в разделе "Восстановление файлов с помощью веб-интерфейса" (стр. 394).

Восстановление данных Oracle с резервной копии RMAN

Аварийное восстановление базы данных Oracle

Этот метод применяется для восстановления всего сервера или диска, на котором установлена Oracle Database при отсутствии ее резервной копии на уровне дисков. Этот метод делает базу данных согласованной с состоянием резервной копии RMAN.

Порядок восстановления:

1. Переустановите операционную систему или перейдите на другой сервер, который работает надлежащим образом. Если операционная система работает нормально, пропустите этот шаг.
2. Переустановите Oracle Database.
3. Создайте новую базу данных с тем же именем и в том же месте, как и та, которую необходимо восстановить.
4. Восстановите нужную резервную копию RMAN из резервной копии на уровне файлов, как описано ранее в этом разделе.

   При выполнении восстановления с самой последней резервной копии RMAN, которая не повреждена, пропустите этот шаг.
5. [В Windows] В командной строке введите cd <папка расположения сценариев>.

© ООО Киберпротект, 2026

[В Linux] В терминале введите cd /<папка расположения сценариев>.

6. Запустите файл **restore_disaster.bat** (в Windows) или **restore_disaster.sh** (в Linux).

Полное восстановление базы данных

Используйте этот метод, если база данных не работает или повреждена после создания последней резервной копии. Чтобы воспользоваться этим методом, контрольный файл и файл параметров сервера должны быть неповрежденными.

Порядок восстановления:

1. Восстановите нужную резервную копию RMAN из резервной копии на уровне файлов, как описано ранее в этом разделе.

   При выполнении восстановления с самой последней резервной копии RMAN, которая не повреждена, пропустите этот шаг.
2. [В Windows] В командной строке введите cd <папка расположения сценариев>.

   [В Linux] В терминале введите cd /<папка расположения сценариев>.
3. Запустите файл **restore_datafiles.bat** (в Windows) или **restore_datafiles.sh** (в Linux).

Восстановление контрольного файла

Используйте этот метод, если контрольный файл потерян или поврежден после создания последней резервной копии.

Порядок восстановления:

1. Восстановите нужную резервную копию RMAN из резервной копии на уровне файлов, как описано ранее в этом разделе.

   При выполнении восстановления с самой последней резервной копии RMAN, которая не повреждена, пропустите этот шаг.
2. [В Windows] В командной строке введите cd <папка расположения сценариев>.

   [В Linux] В терминале введите cd /<папка расположения сценариев>.
3. Запустите файл **restore_controlfile.bat** (в Windows) или **restore_controlfile.sh** (в Linux).
4. Создайте полную резервную копию.

   При восстановлении контрольного файла журналы сбрасываются, поэтому следующая резервная копия должна быть полной.

Восстановление по состоянию на настраиваемый момент времени (неполное восстановление)

Этот метод позволяет восстановить базу данных на настраиваемый момент времени (Point-in-Time Recovery, PITR). Этот момент времени можно указать следующими способами:

- Точная дата и время. Доступный диапазон от момента создания резервной копии RMAN до текущего момента.
- Номер системного изменения (SCN). Доступный диапазон от времени, записанного в файле **scn.in** до последнего значения времени, доступного в архивированных журналах.

  Файл **scn.in** хранится в папке с резервными копиями RMAN. Как правило, SCN в этом файле несет информацию о моменте времени последней резервной копии.

© ООО Киберпротект, 2026

Чтобы узнать последнее значение SCN из архивированных журналов, выполните следующие действия:

a. В командной строке (в Windows) или в терминале (в Linux) введите sqlplus / as sysdba, чтобы войти в Oracle.
b. Введите select max(next_change#)-1 from v$archived_log;

Порядок восстановления:

1. Восстановите нужную резервную копию RMAN из резервной копии на уровне файлов, как описано ранее в этом разделе. Это приведет к перезаписи файла **scn.in**.

   При выполнении восстановления с самой последней резервной копии RMAN, которая не повреждена, пропустите этот шаг.
2. [В Windows] В командной строке введите cd <папка расположения сценариев>.

   [В Linux] В терминале введите cd /<папка расположения сценариев>.
3. Выполните любое из следующих действий:
   - Чтобы выполнить восстановление на определенный момент времени, запустите restore_to-point-in-time.bat <момент времени> (в Windows) или restore_to-point-in-time.sh<момент времени> (в Linux).

     Переменная <момент времени> должна быть указана в следующем формате: yyyy-mm-dd:hh24:mi:ss.
   - Чтобы выполнить восстановление по состоянию на определенный SCN, запустите restore_to-scn.bat <SCN> (в Windows) или restore_to-scn.sh <SCN> (в Linux).

   Если дата и время (SCN) не указаны, восстановление выполняется на момент времени, который определен номером SCN, указанным в файле **scn.in**.
4. Создайте полную резервную копию.

   При неполном восстановлении журналы сбрасываются, поэтому следующая резервная копия должна быть полной.

12.6 Защита баз данных PostgreSQL

Кибер Бэкап поддерживает резервное копирование экземпляров (instances) PostgreSQL, Postgres Pro, а также кластера PostgreSQL на базе Patroni.

Вы можете выполнять резервное копирование баз данных PostgreSQL следующих версий:

- PostgreSQL 11–17;
- PostgreSQL для 1С;
- Postgres Pro Standard 11–17;
- Postgres Pro Enterprise 11–17;
- Patroni 3.0 – 3.2.1;
- Platform V Pangolin SE 6.1.7 (требуются дополнительные настройки на машине с агентом, подробнее см. статью базы знаний);

© ООО Киберпротект, 2026

- Proxima DB 2.0, 3.0;
- СУБД Jatoba 5 (в случае возникновения ошибки при подключении экземпляра PostgreSQL для гранулярного восстановления см. статью базы знаний);
- СУБД Tantor 14–17;
- Arenadata Prosperity 4.0.

12.6.1 Что необходимо для резервного копирования

Для резервного копирования баз данных PostgreSQL понадобятся установленные и настроенные продукты:

- Кибер Бэкап 15 или новее с лицензией «Кибер Бэкап для СУБД PostgreSQL» на каждый экземпляр PostgreSQL, резервное копирование которого вы планируете выполнять (список лицензий см. в разделе "Издания и лицензии Кибер Бэкап" (стр. 16)). Одна лицензия для PostgreSQL распространяется на один экземпляр или на один кластер Patroni.
- PostgreSQL.

Для выполнения резервного копирования нужно установить агент Кибер Бэкап для операционной системы, которую вы используете (агент для Windows или агент для Linux), а также агент для PostgreSQL.

При установке агента для PostgreSQL к используемым операционным системам предъявляются более высокие требования, которые изложены в разделе "Агенты" (стр. 23).

Объем ОЗУ машины, на которую будет установлен агент для PostgreSQL, должен составлять не менее 4 ГБ.

12.6.2 Возможности

1. Кибер Бэкап поддерживает следующие виды резервного копирования:
   - полное резервное копирование;
   - инкрементное резервное копирование;
   - резервное копирование журнала транзакций.

   Примечание
   До версии 18.5 в Кибер Бэкап под инкрементным резервным копированием понималось резервное копирование журнала транзакций. Начиная с версии 18.5, инкрементное резервное копирование основано на отслеживании фактических изменений в файлах баз данных. Резервное копирование журнала транзакций выделено в отдельную схему.

   Полное резервное копирование означает резервное копирование кластеров с базами данных. На одном сервере может быть несколько кластеров.

© ООО Киберпротект, 2026

Примечание
При резервном копировании данные сразу записываются в целевое хранилище резервных копий. Промежуточное хранение предварительных данных на источнике не используется.

2. Кибер Бэкап поддерживает в качестве хранилищ резервных копий:
   - локальные папки;
   - сетевые папки;
   - NFS;
   - SFTP;
   - узлы хранения;
   - ленты.
3. Кибер Бэкап поддерживает следующие варианты расписания резервного копирования:
   - всегда полное;
   - еженедельно полное, ежедневно инкрементное;
   - еженедельно полное, ежедневно журнал транзакций;
   - еженедельно полное, ежедневно инкрементное, ежечасно журнал транзакций;
   - другое (пользовательская схема).

   Подробнее о схемах см. подраздел "Схемы резервного копирования" в разделе "Резервное копирование PostgreSQL" (стр. 591).
4. Кибер Бэкап поддерживает следующие варианты восстановления PostgreSQL:
   - восстановление экземпляра PostgreSQL в виде файлов;
   - подключение экземпляра PostgreSQL из архива;
   - восстановление отдельных баз данных в dump-файлы, исходные или новые базы данных;
   - восстановление отдельных баз данных на определенный момент времени (Point-in-Time Recovery, PITR).

12.6.3 Предварительная настройка PostgreSQL

12.6.3.1 Создание учетной записи пользователя на сервере PostgreSQL

Создайте учетную запись пользователя на сервере PostgreSQL, с помощью которой Кибер Бэкап будет подключаться к PostgreSQL.

Учетная запись должна обладать привилегией SUPERUSER.

Например, можно использовать команду:

```
CREATE USER <replicator> SUPERUSER PASSWORD <password>
```

Где:

© ООО Киберпротект, 2026

- <replicator> – имя учетной записи;
- <password> – пароль учетной записи.

Если планируется работать с кластером PostgreSQL, то на всех узлах кластера должна быть создана учетная запись с одинаковым именем и паролем.

Примечание
В случае изменения данных этой учетной записи на сервере PostgreSQL, для корректного обновления данных в конфигурационных файлах Кибер Бэкап рекомендуется использовать специальную утилиту (см. раздел "Известные проблемы и их решения" (стр. 600)).

12.6.3.2 Настройка аутентификации в PostgreSQL

Чтобы настроить соединение между Кибер Бэкап и PostgreSQL, внесите изменения в конфигурационные файлы postgresql.conf и pg_hba.conf. По умолчанию конфигурационные файлы находятся в каталоге с данными кластера базы данных.

Настройка конфигурационного файла postgresql.conf

Добавьте в файл postgresql.conf параметр listen_addresses и укажите, с каких адресов (агентов) возможно подключение к экземпляру PostgreSQL, например:

```
listen_addresses = 0.0.0.0
```

За более подробной информацией о параметре listen_addresses обратитесь к официальной документации PostgreSQL (например, параметры подключений).

Настройка конфигурационного файла pg_hba.conf

Укажите в файле pg_hba.conf параметры аутентификации с помощью новых записей.

Каждая запись в pg_hba.conf обозначает тип соединения, диапазон IP-адресов клиента (если он соотносится с типом соединения), имя базы данных, имя пользователя и способ аутентификации, который будет использован для соединения. Первая запись с подходящими параметрами применяется для аутентификации пользователя.

Значения полей:

TYPE

Тип подключения. Значение local управляет подключениями через Unix-сокеты. Без подобной записи подключения через Unix-сокеты невозможны. Значение host управляет подключениями, устанавливаемыми по TCP/IP.

DATABASE

Определяет, каким именам баз данных соответствует эта запись. Значение all определяет, что подходят все базы данных. Значение replication показывает, что запись соответствует, если запрашивается подключение для физической репликации (имейте в виду, что для таких

© ООО Киберпротект, 2026

подключений не выбирается какая-то конкретная база данных). Несколько имён баз данных можно указать, разделяя их запятыми. Файл, содержащий имена баз данных, можно указать, поставив знак @ в начале его имени.

USER

Указывает, какому имени (или именам) пользователя базы данных соответствует эта запись. Значение all показывает, что запись соответствует всем пользователям. Несколько имён пользователей можно указать, разделяя их запятыми. Файл, содержащий имена пользователей, можно указать, поставив знак @ в начале его имени.

ADDRESS

Указывает адрес (или адреса) клиентской машины, которым соответствует данная запись. Это поле может содержать имя компьютера, диапазон IP-адресов или одно из ключевых слов.

Диапазон IP-адресов указывается в виде начального адреса диапазона, дополненного косой чертой (/) и длиной маски CIDR. Длина маски задаёт количество старших битов клиентского IP-адреса, которые должны совпадать с битами IP-адреса диапазона. Биты, находящиеся правее, в указанном IP-адресе должны быть нулевыми. Между IP-адресом, знаком / и длиной маски CIDR не должно быть пробельных символов.

METHOD

Метод-аутентификации.

Чтобы к PostgreSQL можно было подключаться с логином и паролем, укажите значение md5.

Для учетной записи пользователя PostgreSQL, с помощью которой происходит соединение с программой Кибер Бэкап (см. раздел "Предварительные требования" (стр. 477)), укажите метод аутентификации trust.

За более подробной информацией о конфигурационном файле pg_hba.conf обратитесь к официальной документации PostgreSQL (например, файл pg_hba.conf).

Примеры записей

Записи для подключения агента с этого же сервера по адресу 127.0.0.1 для пользователя replicator:

```
# TYPE DATABASE      USER         ADDRESS       METHOD
host       all         replicator     127.0.0.1/32    trust
host       replication   replicator     127.0.0.1/32    trust
```

Записи для подключения агента с другого сервера с адресом 10.10.10.100 для любого пользователя локальной системы по TCP/IP:

```
# TYPE   DATABASE      USER        ADDRESS           METHOD
host       all         all         10.10.10.100/32     md5
host       replication    all         10.10.10.100/32     md5
```

Пример файла pg_hba.conf с необходимыми записями:

© ООО Киберпротект, 2026

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             replicator      127.0.0.1/32            trust
host    all             all             0.0.0.0/0               md5
host    all             all             127.0.0.1/32            ident
# IPv6 local connections:
host    all             all             ::1/128                 ident
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     replicator      127.0.0.1/32            trust
host    replication     all             0.0.0.0/0               md5
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 ident
```

Внимание

Для настройки аутентификации при переходе с версии Кибер Бэкап 15 Обновление 2.6 или Кибер Бэкап Обновление 2.7 на Кибер Бэкап 16 обратитесь к разделу Известные проблемы и их решения.

После внесения изменений в файлы конфигурации перезапустите службу PostgreSQL:

```
systemctl restart postgresql
```

12.6.4 Установка и настройка

Установка и настройка включает в себя следующие шаги:

1. Установка сервера управления.
2. Установка агента для PostgreSQL и агента Кибер Бэкап для операционной системы, которую вы используете (Windows или Linux).
3. Добавление в веб-консоли Кибер Бэкап устройства PostgreSQL.

12.6.4.1 Установка сервера управления

Для установки сервера управления обратитесь к разделу "Установка сервера управления" (стр. 63).

12.6.4.2 Установка агентов для PostgreSQL

Агент для PostgreSQL может быть установлен как на сервер, на котором находятся базы данных PostgreSQL, так и на другую машину.

Если вы устанавливаете агент для PostgreSQL на другую машину:

© ООО Киберпротект, 2026

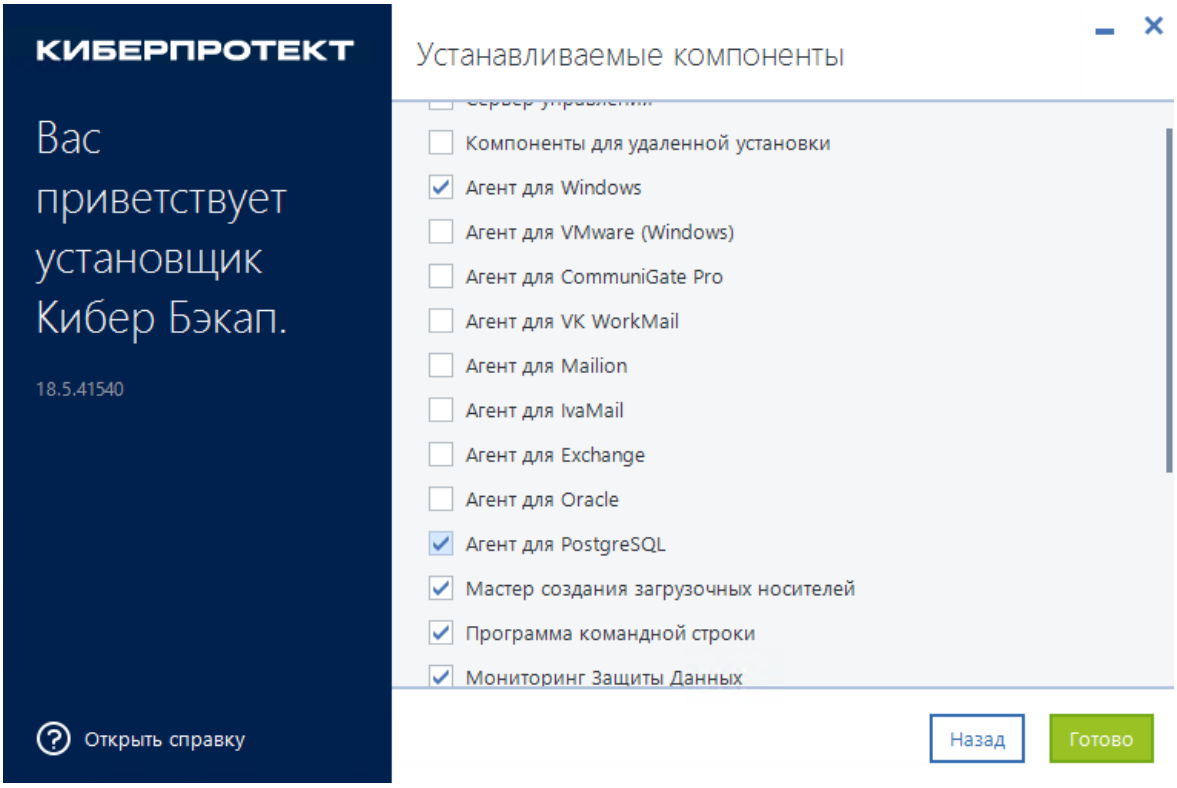
1. Убедитесь, что машина с агентом и сервер PostgreSQL смогут обмениваться данными по сети. Откройте необходимые порты, настройте соединение, если требуется – настройте прокси-сервер.
2. На сервере PostgreSQL разрешите локальные входящие соединения типа replication.
3. Для гранулярного восстановления баз данных PostgreSQL на машине с агентом должен быть установлен экземпляр PostgreSQL той же версии, что и восстанавливаемый.
4. Обратите внимание, что восстановление экземпляра PostgreSQL в виде файлов возможно только на машину с агентом и в присоединенные к ней сетевые папки (см. раздел "Восстановление экземпляра PostgreSQL в виде файлов" (стр. 594)).

Установка агента для PostgreSQL

Агент для PostgreSQL необходимо устанавливать совместно с агентом для операционной системы, которую вы используете (Windows или Linux).

В этом разделе рассмотрена установка агента для PostgreSQL на машину с ОС Windows. Для установки агента для PostgreSQL на машину с ОС Linux обратитесь к разделу "Установка агентов в ОС Linux вручную" (стр. 97).

1. Запустите установщик Кибер Бэкап.
2. Выберите **Настройка параметров установки**.
3. В блоке **Устанавливаемые компоненты** выберите **Изменить**.
4. Отметьте в списке **Агент для PostgreSQL**.



5. Нажмите **Готово**, затем нажмите **Установка**.

© ООО Киберпротект, 2026

Примечание
Для СУБД Platform V Pangolin также выполните шаги, приведённые в статье Базы знаний.

12.6.4.3 Добавление в веб-консоли Кибер Бэкап устройства PostgreSQL

1. В веб-консоли Кибер Бэкап в разделе **Устройства** нажмите **Добавить**.
2. В блоке **Приложения** выберите:
   - **PostgreSQL**, если необходимо добавить сервер PostgreSQL.
   - **Кластер PostgreSQL Patroni**, если необходимо добавить кластер PostgreSQL.
3. В поле выбора агента из выпадающего списка выберите агент развёртывания для PostgreSQL. Выбранный агент будет использоваться для резервного копирования и восстановления данных сервера или кластера PostgreSQL.
4. Укажите настройки соединения с PostgreSQL:
   a. имя хоста или IP-адрес сервера PostgreSQL;
   b. порт подключения (по умолчанию для сервера PostgreSQL используется порт 5432, для кластера PostgreSQL – порт 8008);
   c. имя пользователя учётной записи для подключения к PostgreSQL;
   d. пароль учётной записи для подключения к PostgreSQL.

   Убедитесь, что при настройке параметров аутентификации вы настроили метод аутентификации **trust**.
5. [Необязательно] Введите произвольный комментарий.
6. Нажмите кнопку **Добавить**.

В списке устройств отобразится раздел PostgreSQL с добавленным сервером или кластером.

Для кластера PostgreSQL в разделе **Сведения** отобразится информация об IP-адресах/именах узлов, доступности (**Online**/**Offline**) и статусах узлов (**Leader**/**Replica**).

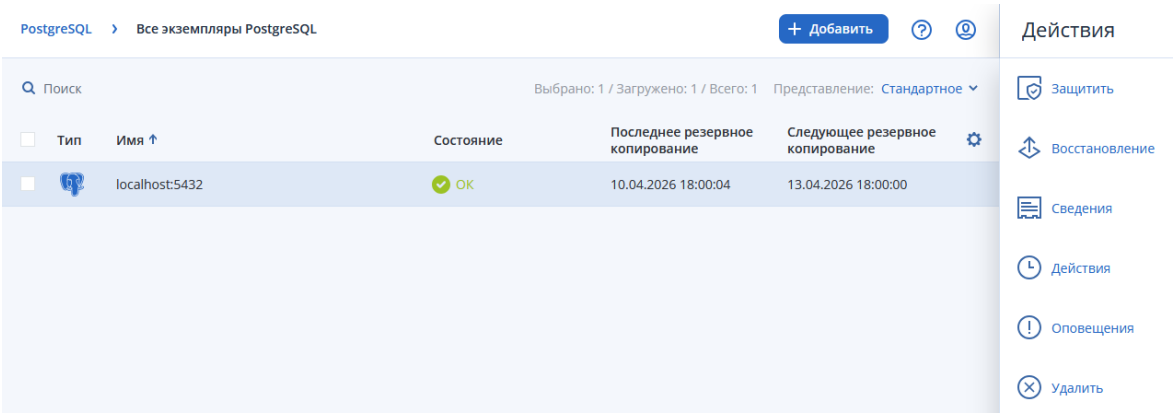
12.6.5 Резервное копирование PostgreSQL

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** > **PostgreSQL**.
2. Выберите экземпляр PostgreSQL, который вы хотите защитить.

© ООО Киберпротект, 2026

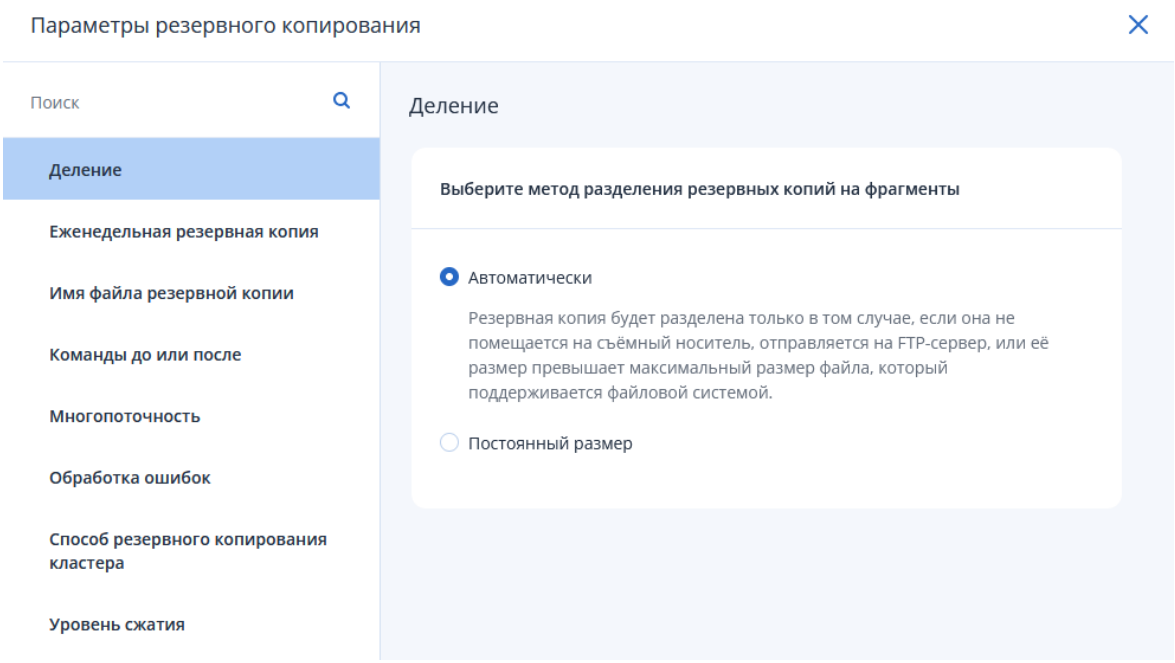
3. Перейдите на вкладку справа **Защитить**.



4. В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.

   Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места сохранения" (стр. 278).
5. В поле **Расписание** укажите схему и периодичность выполнения резервного копирования. Подробнее о расписании см. в разделе "Расписание" (стр. 287). В текущей версии доступны полное резервное копирование, инкрементное резервное копирование и резервное копирование журнала транзакций. Подробнее о схемах см. далее подраздел "Схемы резервного копирования".
6. В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища. Подробнее см. в разделе "Правила хранения" (стр. 299).
7. При необходимости защитите резервные копии паролем. Подробнее см. в разделе "Защита паролем" (стр. 301).
8. [Необязательно] В поле **Параметры резервного копирования** нажмите **Изменить** и укажите следующие параметры:
   - **Деление**. Выберите метод разделения резервных копий на меньшие по размеру фрагменты.
   - **Еженедельная резервная копия**. Укажите день недели для создания еженедельной копии.
   - **Имя файла резервной копии**. Укажите шаблон для наименований файлов резервных копий.
   - **Команды до или после**. Укажите команды, которые должны выполняться перед резервным копированием или после него.
   - **Многопоточность**. Выберите вариант использования многопоточности.
   - **Обработка ошибок**. Укажите порядок обработки ошибок, возникающих при резервном копировании.
   - **Способ резервного копирования кластера**. Подробнее см. в разделе "Способ резервного копирования кластера" (стр. 350).
   - **Управление лентами**. Укажите порядок записи резервных копий на ленточные устройства.
   - **Уровень сжатия**. Укажите уровень сжатия данных при резервном копировании.

© ООО Киберпротект, 2026



Подробнее см. в разделе "Параметры резервного копирования" (стр. 335).

9. Нажмите **Применить**. Новый план защиты появится в списке планов.

В результате вы сможете:

- выполнять резервное копирование баз данных PostgreSQL;
- выполнять восстановление баз данных PostgreSQL из резервных копий.

12.6.5.1 Схемы резервного копирования

Примечание
Начиная с версии 18.5 в Кибер Бэкап для инкрементного резервного копирования требуется, чтобы агент располагался на одной машине с экземпляром PostgreSQL.

В Кибер Бэкап для PostgreSQL реализованы следующие схемы резервного копирования:

- **Всегда полное**. При этой схеме всегда выполняется полное резервное копирование.
- **Еженедельно полное, ежедневно инкрементное**. В версиях Кибер Бэкап ранее 18.5 в этой схеме вместо инкрементного резервного копирования выполнялось резервное копирование журнала транзакций. Если агент для PostgreSQL установлен на машине, на которой нет баз данных, то резервное копирование всегда будет полным.
- **Еженедельно полное, ежедневно журнал транзакций**. Эта схема в версии Кибер Бэкап ранее 18.5 называлась **Еженедельно полное, ежедневно инкрементное**.
- **Еженедельно полное, ежедневно инкрементное, ежечасно журнал транзакций**. Эта схема доступна начиная с версии Кибер Бэкап 18.5. Если агент для PostgreSQL установлен на машине, на которой нет баз данных, вместо инкрементного резервного копирования будет совершаться

© ООО Киберпротект, 2026

полное.

- **Другое**. Эта схема является пользовательской.

Примечание
Инкрементное резервное копирование выполняется только для экземпляров PostgreSQL. Для кластеров Patroni этот тип резервного копирования недоступен.

Особенности использования

- Если выполнить обновление сервера управления, это приведет к следующим изменениям:
  - схема резервного копирования **Еженедельно полное, ежедневно инкрементное** сменит свое название на **Еженедельно полное, ежедневно журнал транзакций**;
  - в интерфейсе веб-консоли **Хранилища резервных копий** названия резервных копий **Инкрементное** останутся неизменными;
  - в схеме резервного копирования **Другое** изменится название с **Инкрементное резервное копирование** на **Резервное копирование журналов транзакций**;
  - при дальнейших запусках **Журнал транзакций** будет отображаться в резервных копиях как **Инкрементальное** (новый тип резервного копирования не будет поддерживаться).
- Если выполнить обновление агента, это приведет к следующим изменениям:
  - все старые инкрементные резервные копии останутся с названием **Инкрементное**;
  - при первом запуске схемы **Журнал транзакций** будет выполнено полное резервное копирование; при последующих запусках будет выполняться резервное копирование по схеме **Журнал транзакций**.
- Если правилами хранения установлены такие сроки хранения, при которых резервные копии должны быть удалены, одна резервная копия журнала транзакций всё равно сохранится.
- После смены лидера в кластере Patroni следующее резервное копирование будет полным.

12.6.6 Восстановление баз данных PostgreSQL

Восстановление всех поддерживаемых версий баз данных PostgreSQL, а также кластера PostgreSQL на базе Patroni происходит по единому сценарию.

Кибер Бэкап поддерживает следующие варианты восстановления баз данных:

- "Восстановление экземпляра PostgreSQL в виде файлов" (стр. 594).
- "Подключение экземпляра PostgreSQL из архива" (стр. 595).
- "Гранулярное восстановление баз данных PostgreSQL" (стр. 597).

12.6.6.1 Восстановление экземпляра PostgreSQL в виде файлов

Для восстановления всего экземпляра PostgreSQL в виде файлов:

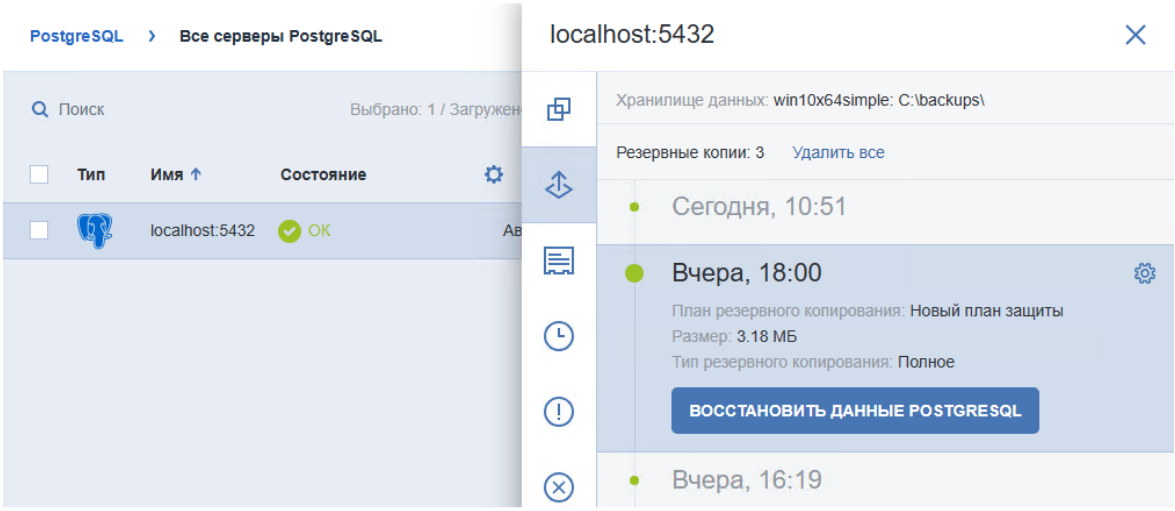
1. Перейдите в **Устройства** > **PostgreSQL**.
2. Выберите экземпляр PostgreSQL, который нужно восстановить.

© ООО Киберпротект, 2026

3. Перейдите на вкладку справа **Восстановление**.

> **Примечание**
> Либо перейдите в **Хранилища резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

4. Выберите нужную копию для восстановления и нажмите **Восстановить данные PostgreSQL**.



5. Выберите архив и нажмите справа **Восстановить как файлы**.
6. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
7. Выберите место для восстановления файлов. Возможные варианты: локальные папки машины, на которой установлен агент, и присоединенные к ней сетевые папки.
8. Проверьте остальные настройки и нажмите **Начать восстановление**.

Ход выполнения восстановления показан на вкладке **Действия**.

После успешного восстановления на машине под управлением ОС Windows необходимо подключить восстановленные файлы к PostgreSQL, как описано в статье Подключение баз данных PostgreSQL после восстановления.

12.6.6.2 Подключение экземпляра PostgreSQL из архива

Подключение экземпляра PostgreSQL из архива может понадобиться для просмотра содержимого резервной копии или других операций с базой данных средствами PostgreSQL.

Предварительные требования:

- Для восстановления баз данных из одного экземпляра PostgreSQL в другой экземпляр PostgreSQL на машинах с экземплярами должны совпадать операционная система, версия и редакция PostgreSQL.
- В случае если агент установлен не на сервере с экземпляром PostgreSQL, на машине с агентом должен быть установлен экземпляр PostgreSQL той же версии, что и восстанавливаемый.

© ООО Киберпротект, 2026

- На машине с агентом PostgreSQL в конфигурационном файле /opt/acronis/var/dsp.database.pg/postgresql-agent.json в секции server > recovery_instance > binaries необходимо указать путь к исполняемым файлам PostgreSQL. Например:

```
"recovery_instance": {
   "run_as_user": "postgres",
   "binaries": ["/usr/pgsql-15/bin/postgres"]
}
```

  Далее перезапустите службу агента PostgreSQL:

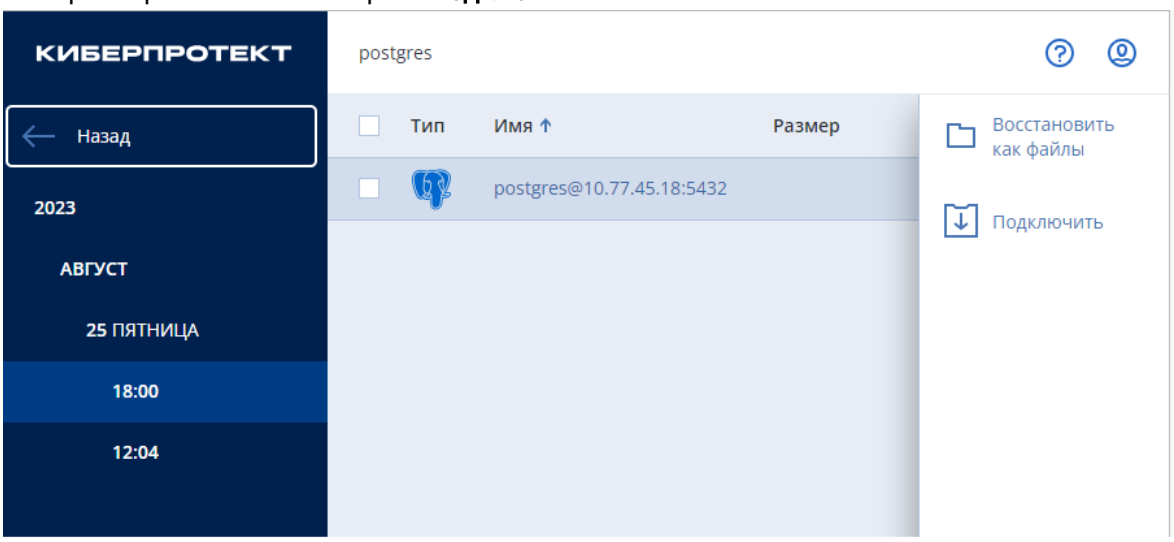
```
systemctl restart aakore
systemctl restart acronis_mms
```

Для подключения экземпляра PostgreSQL из архива:

1. Перейдите в **Устройства** > **PostgreSQL**.
2. Выберите экземпляр PostgreSQL, который нужно подключить.
3. Перейдите на вкладку справа **Восстановление**.

   Примечание
   Либо перейдите в **Хранилища резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

4. Выберите нужный архив для подключения и нажмите **Восстановить данные PostgreSQL**.
5. Выберите архив и нажмите справа **Подключить**.



6. Проверьте настройки и нажмите **Монтировать**.
7. Подключитесь к восстановленной базе данных и совершите необходимые действия средствами PostgreSQL.
8. Перейдите в **Панель Мониторинга** > **Действия** и выберите операцию подключения базы данных. Прервите подключение архива базы данных.

© ООО Киберпротект, 2026

12.6.6.3 Гранулярное восстановление баз данных PostgreSQL

Гранулярное восстановление доступно только для баз данных PostgreSQL, установленных на машинах под управлением ОС Linux. Доступно восстановление отдельных баз данных из единого архива резервной копии.

Восстановление на определенный момент времени (Point-in-Time Recovery, PITR) доступно только для резервных копий журналов транзакций.

Предварительные требования:

- Для восстановления баз данных из одного экземпляра PostgreSQL в другой экземпляр PostgreSQL на машинах с экземплярами должны совпадать операционная система, версия и редакция PostgreSQL.
- В случае если агент установлен не на сервере с экземпляром PostgreSQL, на машине с агентом должен быть установлен экземпляр PostgreSQL той же версии, что и восстанавливаемый.
- На машине с агентом PostgreSQL в конфигурационном файле /opt/acronis/var/dsp.database.pg/postgresql-agent.json в секции server > recovery_instance > binaries необходимо указать путь к исполняемым файлам PostgreSQL. Например:

  ```
  "recovery_instance": {
    "run_as_user": "postgres",
    "binaries": ["/usr/pgsql-15/bin/postgres"]
  }
  ```

  Далее перезапустите службу агента PostgreSQL:

  ```
  systemctl restart aakore
  systemctl restart acronis_mms
  ```

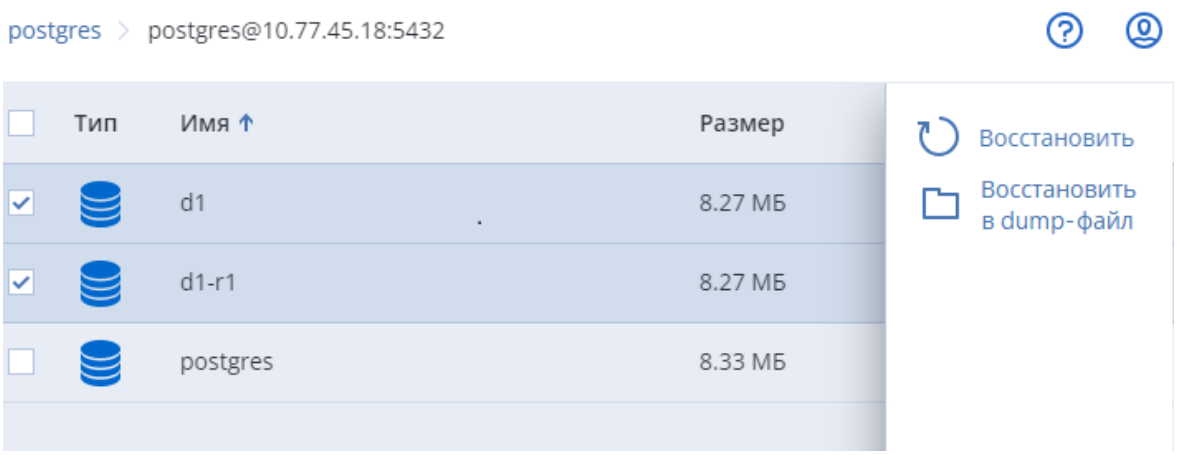
Для восстановления отдельных баз данных PostgreSQL:

1. Перейдите в **Устройства** > **PostgreSQL**.
2. Выберите экземпляр PostgreSQL, из которого вы хотите восстановить базы данных.
3. Перейдите на вкладку справа **Восстановление**.

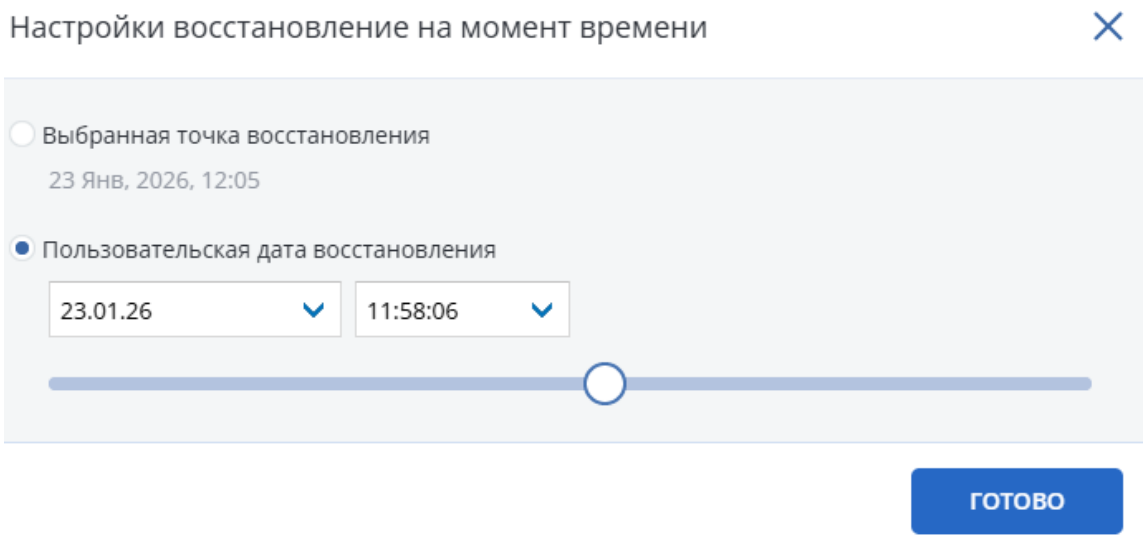
   Примечание
   Либо перейдите в **Хранилища резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

4. Нажмите на имя резервной копии и выберите необходимые для восстановления базы из архива.

© ООО Киберпротект, 2026



5. Выберите способ восстановления:
   - Если необходимо сразу восстановить выбранные базы из архива, нажмите справа **Восстановить**.
   - Если необходимо сохранить выбранные базы из архива в отдельные dump-файлы, нажмите справа **Восстановить в dump-файл**.
6. [Если выбрано восстановление баз из архива] Укажите следующие настройки:
   - Выберите время восстановления. Можно оставить время создания резервной копии или указать время между созданием предыдущей резервной копии и выбранной (PITR).



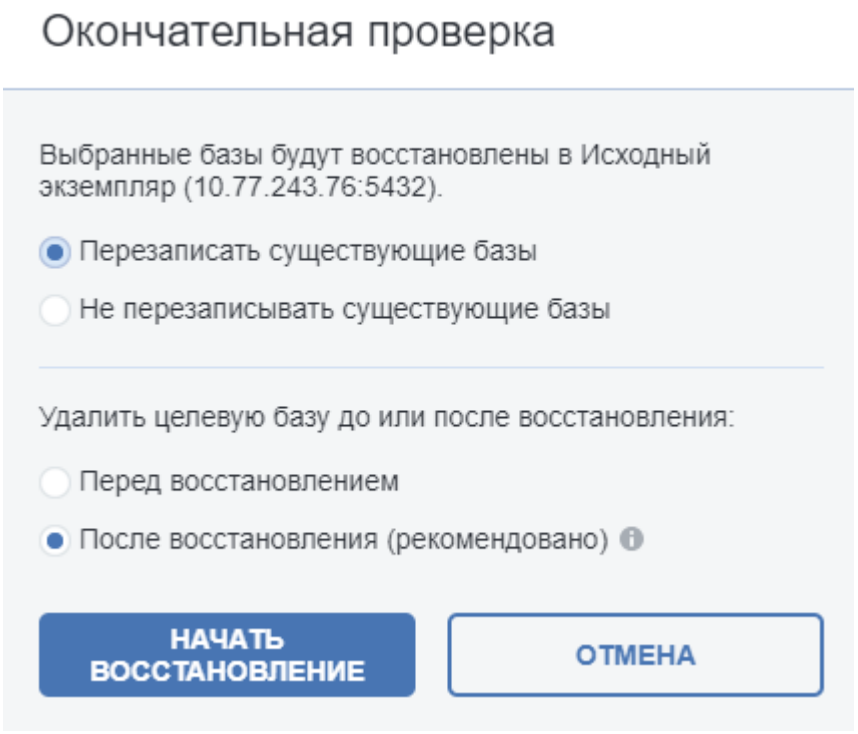
   - Экземпляр PostgreSQL, куда будет происходить восстановление.

     Примечание
     Версия экземпляра PostgreSQL, куда будет происходить восстановление, должна быть не ниже восстанавливаемой. Редакции экземпляров PostgreSQL должны совпадать. Экземпляр, созданный из кластеризованного экземпляра, можно восстановить на некластеризованный экземпляр и наоборот.

   - Для каждой выбранной базы из архива укажите место для восстановления. Возможные варианты: в исходную базу, в новую базу.

© ООО Киберпротект, 2026

7. [Если выбрано сохранение баз данных в dump-файлы] Укажите следующие настройки:
   - Выберите время восстановления. Можно оставить время создания резервной копии или указать время между созданием предыдущей резервной копии и выбранной (PITR).
   - Место хранения dump-файлов.
8. Нажмите **Начать восстановление**.
9. [Если выбрано восстановление в исходную базу данных] Укажите порядок восстановления баз данных и нажмите **Начать восстановление**.



Ход выполнения восстановления показан на вкладке **Действия**.

12.6.7 Ограничения

- Не поддерживается полное резервное копирование баз данных PostgreSQL в хранилище под управлением узла хранения с включенной дедупликацией резервных копий.
- Не поддерживается резервное копирование баз данных PostgreSQL в защищенное паролем хранилище под управлением узла хранения.
- Не поддерживается гранулярное восстановление на машинах под управлением ОС Windows.
- Не поддерживается гранулярное восстановление для резервных копий на ленточных накопителях.
- При репликации архива диапазон восстановления на момент времени (PITR) доступен только на исходном архиве.
- При копировании в другую папку архива диапазон восстановления на момент времени утрачивается в новом расположении.

© ООО Киберпротект, 2026

12.6.8 Известные проблемы и их решения

12.6.8.1 Настройка аутентификации

Если вы выполняли настройку аутентификации PostgreSQL в Кибер Бэкап 15 версий Обновление 2.6 или Обновление 2.7 в соответствии с инструкцией в разделе "Предварительная настройка PostgreSQL" (стр. 586) и впоследствии перешли на версию Кибер Бэкап 16, резервное копирование PostgreSQL может завершаться с ошибкой.

```
{"error": "FATAL: no pg_hba.conf entry for host "10.77.242.110", user "postgres", database "template1", no encryption (SQLSTATE 28000)",
"request-id": "bff753db-34f0-4ee9-bbda-d429f45b4ea3",
"service": "PostgreSQL",
"serviceMsg": "FATAL: no pg_hba.conf entry for host "10.77.242.110", user "postgres", database "template1", no encryption (SQLSTATE 28000)"}
```

Решение

В пункте IPv4 local connections файла pg_hba.conf укажите настройки так, как показано в следующем примере:

host all all 127.0.0.1/32 trust

host all all 0.0.0.0/0 md5.

После того, как вы изменили настройки, перезапустите PostgreSQL.

Примечание
Укажите ip-адреса в соответствии со своей конфигурацией.

12.6.8.2 Изменение данных учетной записи пользователя, с помощью которой происходит соединение с PostgreSQL

В некоторых случаях при обновлении Кибер Бэкап или при изменении пароля пользователя средствами PostgreSQL, новый пароль для учетной записи пользователя не обновляется автоматически во всех конфигурационных файлах Кибер Бэкап.

Решение

Для корректного изменения данных учетной записи используйте утилиту, которая устанавливает новые имя пользователя и пароль во всех конфигурационных файлах Кибер Бэкап.

Выполните команду:

```
/usr/lib/Acronis/AMS/postgresql_credentials_changer 'postgres_username' 'postgres_password'
```

Где:

© ООО Киберпротект, 2026

- postgres_username – имя учетной записи;
- postgres_password – пароль учетной записи.

После успешного изменения данных отображается сообщение Successfully changed PostgreSQL credentials in CyberBackup configs.

12.6.8.3 Слоты репликации

Резервное копирование по расписанию останавливается с ошибкой после нескольких созданий, запусков по расписанию и удалений планов резервного копирования.

```
ОШИБКА: используются все слоты репликации (SQLSTATE 53400)
ОШИБКА: syntax error (SQLSTATE 42601)
```

Решение

Удалите ненужные слоты репликации вручную, используя следующие команды:

- Получить все слоты:
  select * from pg_replication_slots where slot_name like 'cp%'
- Удалить слот:
  select pg_drop_replication_slot('cp_3odiqs5psps0knx0bgjz3g_dsuqc5akrjsnln9fhr6srg')

12.7 Защита данных MySQL и MariaDB

Данные MySQL или MariaDB можно защитить с помощью резервного копирования на уровне дисков с поддержкой приложений. При этом собираются метаданные приложения и обеспечивается детальное восстановление на уровне экземпляра, базы данных или таблицы.

Примечание
Резервное копирование данных MySQL или MariaDB с поддержкой приложений доступно при выборе одного из вариантов лицензии Кибер Бэкап Расширенная.

Защита данных СУБД MySQL и MariaDB поддерживается начиная с версии Кибер Бэкап 15 обновление 2.7.

Поддерживаемые версии MySQL и MariaDB указаны в разделе "Поддерживаемые СУБД" (стр. 35).

Чтобы защитить физическую или виртуальную машину, на которой запущены экземпляры MySQL или MariaDB, с помощью резервного копирования с поддержкой приложений, необходимо установить агент для MySQL/MariaDB на этой машине. Агент для MySQL/MariaDB устанавливается вместе с агентом для Linux.

Загрузка установочного файла агента для Linux

1. Войдите в веб-консоль Кибер Бэкап.
2. Нажмите на значок учетной записи в правом верхнем углу и затем выберите **Загрузки**.

© ООО Киберпротект, 2026

3. Выберите **Установщик для Linux**.

   Установочный файл будет загружен на ваш компьютер. Чтобы установить агент, выполните действия, как описано в разделе "Установка агентов" (стр. 95) или "Автоматическая установка или автоматическое удаление в Linux" (стр. 174). Убедитесь, что вы выбрали опцию **Агент для MySQL/MariaDB**.

12.7.0.1 Известные проблемы и ограничения

- Кластеры MySQL или MariaDB не поддерживаются.
- Экземпляры MySQL или MariaDB, работающие в контейнерах Docker, не поддерживаются.
- Экземпляры MySQL или MariaDB, работающие в операционных системах, использующих файловую систему BTRFS, не поддерживаются.
- Системные базы данных (sys, mysql, information-schema, и performance_schema) и базы данных, которые не содержат никаких таблиц, не могут быть восстановлены в запущенные экземпляры. Однако эти базы данных могут быть восстановлены в виде файлов при восстановлении всего экземпляра.
- Восстановление из резервных копий, хранящихся в Зоне безопасности, не поддерживается.
- Восстановление из резервных копий, расположенных на узлах хранения, не поддерживается.
- Восстановление в целевые базы данных, настроенные с использованием символических ссылок, не поддерживается. Вы можете восстановить резервные копии баз данных как новые базы данных, изменив их имя.

Если у вас возникли проблемы при восстановлении данных из защищенных паролем общих ресурсов Samba, выйдите из веб-консоли, а затем снова войдите в нее. Выберите нужную точку восстановления, а затем нажмите **Базы данных MySQL/MariaDB**. Не нажимайте **Вся машина** или **Файлы/папки**.

12.7.1 Настройка резервного копирования с поддержкой приложений

Предварительные требования

- На выбранной машине должен быть запущен хотя бы один экземпляр MySQL или MariaDB.
- На компьютере, на котором запущен экземпляр MySQL или MariaDB, агент защиты должен быть запущен от имени пользователя root.
- Резервное копирование с поддержкой приложений доступно только в том случае, если в плане защиты в качестве источника резервного копирования выбрано **Вся машина**.
- Опция резервного копирования **Sector-by-sector (Посекторно)** должна быть отключена в плане защиты. В противном случае восстановить данные приложения будет невозможно.

Для настройки резервного копирования с поддержкой приложений

© ООО Киберпротект, 2026

1. В веб-консоли Кибер Бэкап выберите один или несколько компьютеров, на которых запущены экземпляры MySQL или MAriaDB. На каждом компьютере может быть один или несколько экземпляров.
2. Создайте план защиты с включенным модулем резервного копирования.
3. В разделе **Выбор данных** выберите **Вся машина**.
4. Нажмите **Резервное копирование приложения**, а затем включите параметр **Сервер MySQL/MariaDB**.
5. Выберите способ указания экземпляров MySQL или MariaDB:
   - **Для всех рабочих нагрузок**

     Используйте этот параметр, если вы запускаете экземпляры с одинаковыми конфигурациями на нескольких серверах. Для всех экземпляров будут использоваться одни и те же параметры подключения и учетные данные доступа.
   - **Для конкретных рабочих нагрузок**

     Используйте этот параметр, чтобы указать параметры подключения и учетные данные доступа для каждого экземпляра.
6. Для настройки параметров подключения и учетных данных доступа нажмите **Добавить экземпляр**.
   a. Выберите тип соединения, а затем укажите следующие данные:
      - [Для сокета TCP] IP-адрес и порт.
      - [Для сокета Unix] путь к сокету.
   b. Укажите данные учетной записи пользователя, которая имеет следующие привилегии для экземпляра:
      - FLUSH_TABLES или RELOAD для всех баз данных и таблиц(*.*)
      - SELECT для information_schema.tables
   c. Нажмите **OK**.
7. Нажмите **Готово**.

12.7.2 Восстановление данных из резервной копии с поддержкой приложений

Из резервной копии с поддержкой приложений можно восстановить экземпляры, базы данных и таблицы MySQL или MariaDB. Также можно восстановить весь сервер, на котором запущены экземпляры, или восстановить файлы и папки с этого сервера.

В таблице ниже приведены все варианты восстановления.

Что восстановить	Опция восстановления	Путь восстановления
Сервер MySQL Сервер	Вся машина	Компьютер*, на котором установлен агент для Linux

© ООО Киберпротект, 2026

Что восстановить	Опция восстановления	Путь восстановления
MariaDB		
Сервер MySQL Сервер MariaDB	Файлы или папки	Компьютер*, на котором установлен агент для Linux
Экземпляр	Файлы	Компьютер*, на котором установлен агент для MySQL/MariaDB
База данных	Та же база данных Новая база данных	Компьютер*, на котором установлен агент для MySQL/MariaDB • Исходный экземпляр • Другой экземпляр • Исходная база данных • Новая база данных
Таблица	Та же таблица Новая таблица	Компьютер*, на котором установлен агент для MySQL/MariaDB • Исходный экземпляр • Другой экземпляр • Исходная база данных • Исходная таблица • Новая таблица

* С точки зрения резервного копирования, виртуальная машина с агентом внутри рассматривается как физическая машина.

12.7.2.1 Восстановление всего сервера

Чтобы узнать, как восстановить весь сервер, на котором запущены экземпляры MySQL или MariaDB, обратитесь к разделу "Восстановление машины" (стр. 384).

12.7.2.2 Восстановление экземпляров

Из резервной копии с поддержкой приложений можно восстановить экземпляры MySQL или MariaDB в виде файлов.

Восстановление экземпляра

1. В веб-консоли Кибер Бэкап выберите компьютер, на котором изначально находились данные, которые вы хотите восстановить.
2. Нажмите **Восстановление**.
3. Выберите точку восстановления. Обратите внимание, что точки восстановления отфильтрованы по месторасположению.

   Если компьютер находится в автономном режиме, точки восстановления не отображаются. Выполните одно из следующих действий:

© ООО Киберпротект, 2026

- Если местом резервного копирования является облако или общее хранилище (то есть, к нему могут получить доступ другие агенты), нажмите **Выбрать машину**, выберите компьютер в сети, на котором установлен агент для MySQL/MariaDB, а затем выберите точку восстановления.
- Выберите точку восстановления на вкладке **Хранилища резервных копий**.

Машина, выбранная для просмотра в любом из вышеуказанных действий, становится целевой машиной для восстановления.

4. Выберите **Восстановить** > **Базы данных MySQL/MariaDB**.
5. Выберите экземпляр, который вы хотите восстановить, а затем нажмите **Восстановить как файлы**.
6. В разделе **Путь** выберите каталог, в который будут восстановлены файлы.
7. Щелкните **Начать восстановление**.

12.7.2.3 Восстановление баз данных

Из резервной копии с поддержкой приложений можно восстановить базы данных в запущенные экземпляры MySQL или MariaDB.

1. В веб-консоли Кибер Бэкап выберите компьютер, на котором изначально находились данные, которые вы хотите восстановить.
2. Нажмите **Восстановление**.
3. Выберите точку восстановления. Обратите внимание, что точки восстановления отфильтрованы по месторасположению.

   Если компьютер находится в автономном режиме, точки восстановления не отображаются. Выполните одно из следующих действий:

   - Если местом резервного копирования является облако или общее хранилище (то есть, к нему могут получить доступ другие агенты), нажмите **Выбрать машину**, выберите компьютер в сети, на котором установлен агент для MySQL/MariaDB, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке **Хранилища резервных копий**.

   Машина, выбранная для просмотра в любом из вышеуказанных действий, становится целевой машиной для восстановления.
4. Выберите **Восстановить** > **Базы данных MySQL/MariaDB**.
5. Щелкните имя нужного экземпляра, чтобы перейти к его базам данных.
6. Выберите одну или несколько баз данных, которые вы хотите восстановить.
7. Нажмите **Восстановление**.
8. Нажмите **Целевой экземпляр MySQL/MariaDB** для указания параметров подключения и учетных данных доступа к целевому экземпляру.

© ООО Киберпротект, 2026

- Проверьте экземпляр, в который вы хотите восстановить данные. По умолчанию выбран исходный экземпляр.
- Укажите данные учетной записи пользователя, которая может получить доступ к целевому экземпляру. Эта учетная запись пользователя должна иметь следующие привилегии для всех баз данных и таблиц (*.*):
  - INSERT
  - CREATE
  - DROP
  - LOCK_TABLES
  - ALTER
  - SELECT
- Нажмите **OK**.

9. Проверьте целевую базу данных.

   По умолчанию выбрана исходная база данных.

   Чтобы восстановить базу данных как новую, щелкните имя целевой базы данных и измените его. Это действие доступно только при восстановлении одной базы данных.
10. В разделе **Перезапись существующих баз данных** выберите режим перезаписи.

    По умолчанию перезапись включена, и резервная база данных заменит целевую базу данных с тем же именем.

    Если перезапись отключена, резервная база данных будет пропущена во время операции восстановления и не заменит целевую базу данных с тем же именем.
11. Щелкните **Начать восстановление**.

12.7.2.4 Восстановление таблиц

Из резервной копии с поддержкой приложений можно восстановить таблицы в запущенные экземпляры MySQL или MariaDB.

1. В веб-консоли Кибер Бэкап выберите компьютер, на котором изначально находились данные, которые вы хотите восстановить.
2. Нажмите **Восстановление**.
3. Выберите точку восстановления. Обратите внимание, что точки восстановления отфильтрованы по месторасположению.

   Если компьютер находится в автономном режиме, точки восстановления не отображаются. Выполните одно из следующих действий:
   - Если местом резервного копирования является облако или общее хранилище (то есть, к нему могут получить доступ другие агенты), нажмите **Выбрать машину**, выберите компьютер в сети, на котором установлен агент для MySQL/MariaDB, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке **Хранилища резервных копий**.

© ООО Киберпротект, 2026

Машина, выбранная для просмотра в любом из вышеуказанных действий, становится целевой машиной для восстановления.

4. Выберите **Восстановить** > **Базы данных MySQL/MariaDB**.
5. Щелкните имя нужного экземпляра, чтобы перейти к его базам данных.
6. Щелкните имя нужной базы данных, чтобы перейти к ее таблицам.
7. Выберите одну или несколько таблиц, которые вы хотите восстановить.
8. Нажмите **Восстановление**.
9. Нажмите **Целевой экземпляр MySQL/MariaDB** для указания параметров подключения и учетных данных доступа к целевому экземпляру.
   - Проверьте экземпляр, в который вы хотите восстановить данные. По умолчанию выбран исходный экземпляр.
   - Укажите данные учетной записи пользователя, которая может получить доступ к целевому экземпляру. Эта учетная запись пользователя должна иметь следующие привилегии для всех баз данных и таблиц (*.*):
     - INSERT
     - CREATE
     - DROP
     - LOCK_TABLES
     - ALTER
     - SELECT
   - Нажмите **OK**.
10. Проверьте целевую таблицу.

    По умолчанию выбрана исходная таблица.

    Чтобы восстановить таблицу как новую, щелкните имя целевой таблицы и измените его. Это действие доступно только при восстановлении одной таблицы.
11. В разделе **Перезапись существующих таблиц** выберите режим перезаписи.

    По умолчанию перезапись включена, и резервная копия таблицы заменит целевую таблицу с тем же именем.

    Если перезапись отключена, резервная копия таблицы будет пропущена во время операции восстановления и не заменит целевую таблицу с тем же именем.
12. Нажмите кнопку **Начать восстановление**.

12.8 Защита баз данных Ред База Данных

Защита данных СУБД Ред База Данных поддерживается начиная с версии Кибер Бэкап 15 обновление 2.7.

Поддерживаемые версии Ред База Данных указаны в разделе "Поддерживаемые СУБД" (стр. 35).

© ООО Киберпротект, 2026

12.8.1 Предварительная настройка базы данных

При настройке резервного копирования базы данных СУБД Ред База Данных рекомендуется заблокировать базы данных на время резервного копирования. При такой блокировке основной файл базы данных замораживается, изменения при этом фиксируются во временном файле дельты. После окончания резервного копирования основной файл базы данных разблокируется, и временный файл дельты и основной файл базы данных объединяются.

12.8.1.1 Скачивание скриптов

Скачайте скрипты для блокировки базы данных (БД) на время резервного копирования.

12.8.1.2 Разархивирование скриптов

Распакуйте скачанные файлы conf.sh (Linux) и conf.bat (Windows) в рабочий каталог скриптов.

12.8.1.3 Настройка конфигурации

Укажите в файле conf.* следующие параметры:

- **RDB** – каталог установки СУБД;
- **DBNAME** – путь к файлу БД или псевдоним (database alias);
- **USER** – имя пользователя для подключения к БД;
- **PASS** – пароль;
- **NBL_DIR** – путь к каталогу с файлом журнала.

12.8.1.4 Разрешение запуска скриптов блокировки и разблокировки

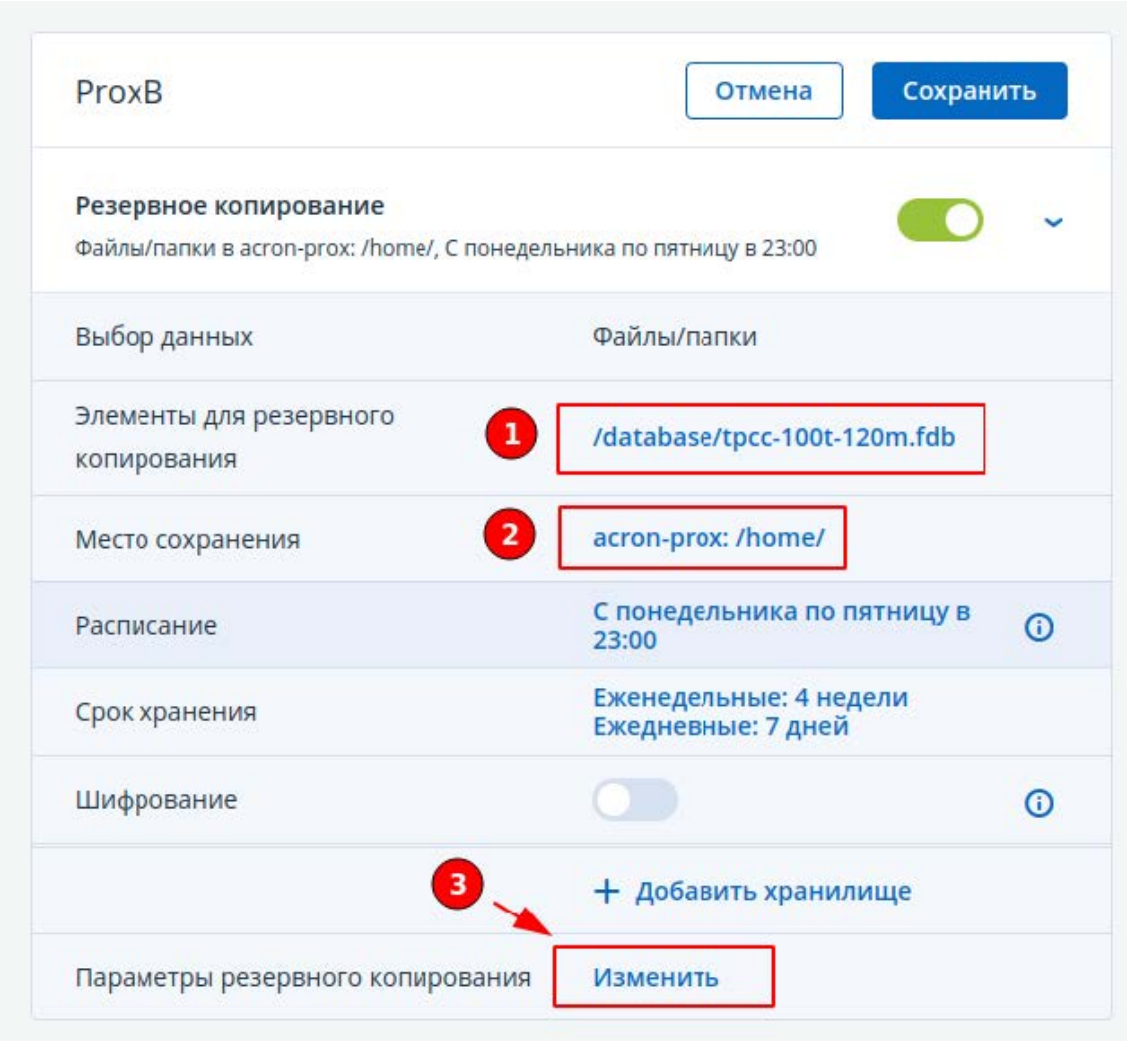
В случае использования ОС Linux необходимо задать права на выполнение для скриптов блокировки и разблокировки. Для этого перейдите в рабочий каталог скриптов и выполните следующие команды:

```
chmod +x ./lock.sh
chmod +x ./unlock.sh
```

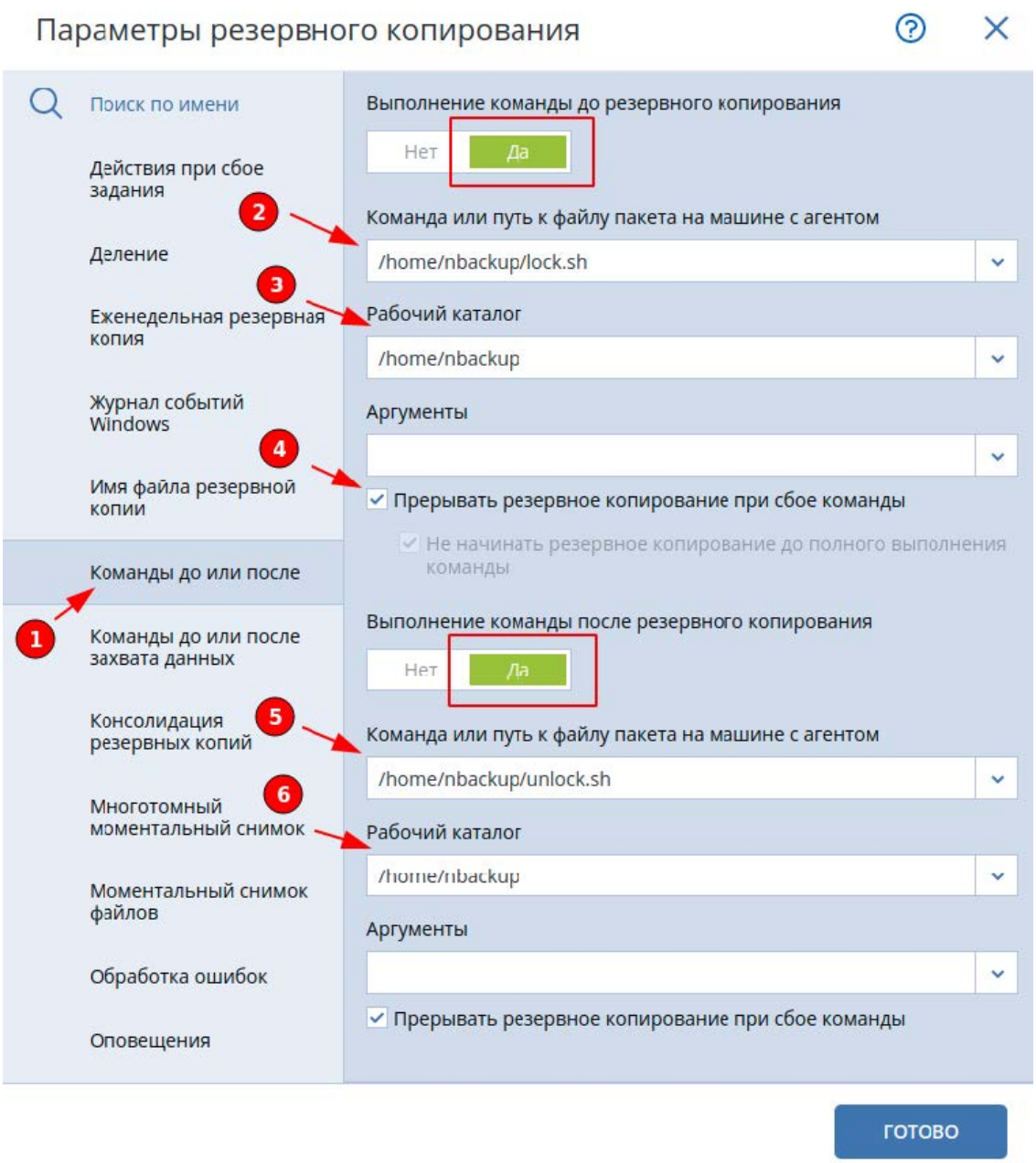
12.8.2 Создание плана резервного копирования

При настройке плана резервного копирования укажите пути к файлам скриптов и к рабочему каталогу как показано далее:

© ООО Киберпротект, 2026



© ООО Киберпротект, 2026



12.8.3 Разблокировка базы данных

После восстановления базы данных из резервной копии, она будет заблокирована. Для разблокировки **восстановленной копии** выполните команду:

```
nbackup -user USER_NAME -pass PASS -F /path/to/db_copy.fdb
```

12.9 Защита баз данных MongoDB

Данные MongoDB можно защитить с помощью резервного копирования с использованием встроенных инструментов MongoDB (например, утилит mongodump и mongorestore). При этом

© ООО Киберпротект, 2026

обеспечивается восстановление на уровне серверов СУБД, баз данных и коллекций MongoDB.

Защита данных MongoDB поддерживается начиная с версии Кибер Бэкап 15 обновление 2.7.

Поддерживаемые версии MongoDB указаны в разделе "Поддерживаемые СУБД" (стр. 35).

Чтобы защитить физическую или виртуальную машину, на которой запущен экземпляр MongoDB, необходимо установить агент для Windows или агент для Linux (в зависимости от операционной системы сервера).

Агент защиты может быть установлен как на хост, на котором находятся базы данных MongoDB, так и на другой хост. Если вы устанавливаете агент защиты на другой хост, убедитесь, что хосты с агентом и MongoDB могут обмениваться данными по сети.

Чтобы установить агент защиты, выполните действия, как описано в разделе "Установка агентов" (стр. 95) или "Автоматическая установка или автоматическое удаление в Linux" (стр. 174).

12.9.1 Настройка резервного копирования баз данных MongoDB

Для резервного копирования баз данных MongoDB используйте план защиты со скриптом, в котором описаны команды для встроенного инструмента MongoDB – утилиты mongodump.

12.9.1.1 Предварительные требования

- Агент защиты и утилита mongodump должны находиться на одном хосте.
- В случае если база данных находится на отдельном хосте, настройте доступ утилиты mongodump к базе данных MongoDB.

12.9.1.2 Настройка удаленного подключения к базе данных MongoDB

Для настройки удаленного подключения необходимо задать значение параметра bindIp:

1. Отредактируйте конфигурационный файл /etc/mongod.conf, например, добавьте строки:

```
...
net:
  port: 27017
  bindIp: 0.0.0.0
...
```

2. Перезапустите сервер MongoDB:

```
systemctl restart mongod.service
```

Подробнее см. в официальной документации MongoDB.

12.9.1.3 Создание скрипта с командами для утилиты mongodump

В скрипте необходимо указать параметры для утилиты mongodump. Подробнее см. в официальной документации MongoDB.

© ООО Киберпротект, 2026

Пример скрипта:

```
#!/bin/bash

# Exit on error:
set -e

epoch_time=$(date +%s)
script_dir=$(pwd)
main_dir=/home/mongo_dump
backup_dir=${main_dir}/latest
info_file=${backup_dir}/README.txt
error_file=${backup_dir}/ERROR.txt

host_db="localhost:27017"
mongo_db_name="my-db"
mongo_db_collection="my-collection"

if [ ! -d ${backup_dir} ]; then
  mkdir -p ${backup_dir}
  echo -e "${epoch_time}\n$(date -d @${epoch_time})" > ${info_file}
  echo -e "$(date -d @${epoch_time}): ${backup_dir} doesnt exist and has been created now. Restart
backup task" >> ${error_file}
  echo "$(date -d @${epoch_time}): ${backup_dir} doesnt exist and has been created now. Restart
backup task" >&2
  exit 1
else
  # For move existing old data to a new dir
  mv ${backup_dir} ${main_dir}/$(head -n 1 ${info_file})
  # Or comment mv above and delete existing files:
  # rm -rf ${backup_dir}
  # Re-create backup dir:
  mkdir -p ${backup_dir}
fi

cd ${script_dir}

echo -e "${epoch_time}\n$(date -d @${epoch_time})" > ${info_file}
echo -e "\n\nRun: /usr/bin/mongodump --host=${host_db} --db ${mongo_db_name} --
collection=${mongo_db_collection} --out ${backup_dir}" >> ${info_file}
/usr/bin/mongodump --host=${host_db} --db=${mongo_db_name} --collection=${mongo_db_
collection} --out ${backup_dir} >> ${info_file} 2>&1
```

где:

- localhost:27017 – имя хоста развертывания MongoDB;
- my-db – имя базы данных MongoDB;
- my-collection – имя коллекции базы данных MongoDB;
- /home/mongo_dump/latest – место хранения резервной копии;

© ООО Киберпротект, 2026

- README.txt – файл с результатами работы скрипта;
- ERROR.txt – файл с ошибками при сбое в работе скрипта.

Пример содержимого файла README.txt:

```
1694175355
Fri Sep  8 15:15:55 MSK 2023

Run: /usr/bin/mongodump --host=localhost:27017 --db my-db --collection=my-collection --out
/home/mongo_dump/latest
Unknown or unsupported stacktrace method requested: generic_fp. Ignoring it
2023-09-08T15:15:56.014+0300    writing my-db.my-collection to /home/mongo_dump/latest/my-
db/my-collection.bson
2023-09-08T15:15:56.015+0300    done dumping my-db.my-collection (11 documents)
```

12.9.1.4 Создание плана резервного копирования

Для создания плана защиты выполните следующие действия:

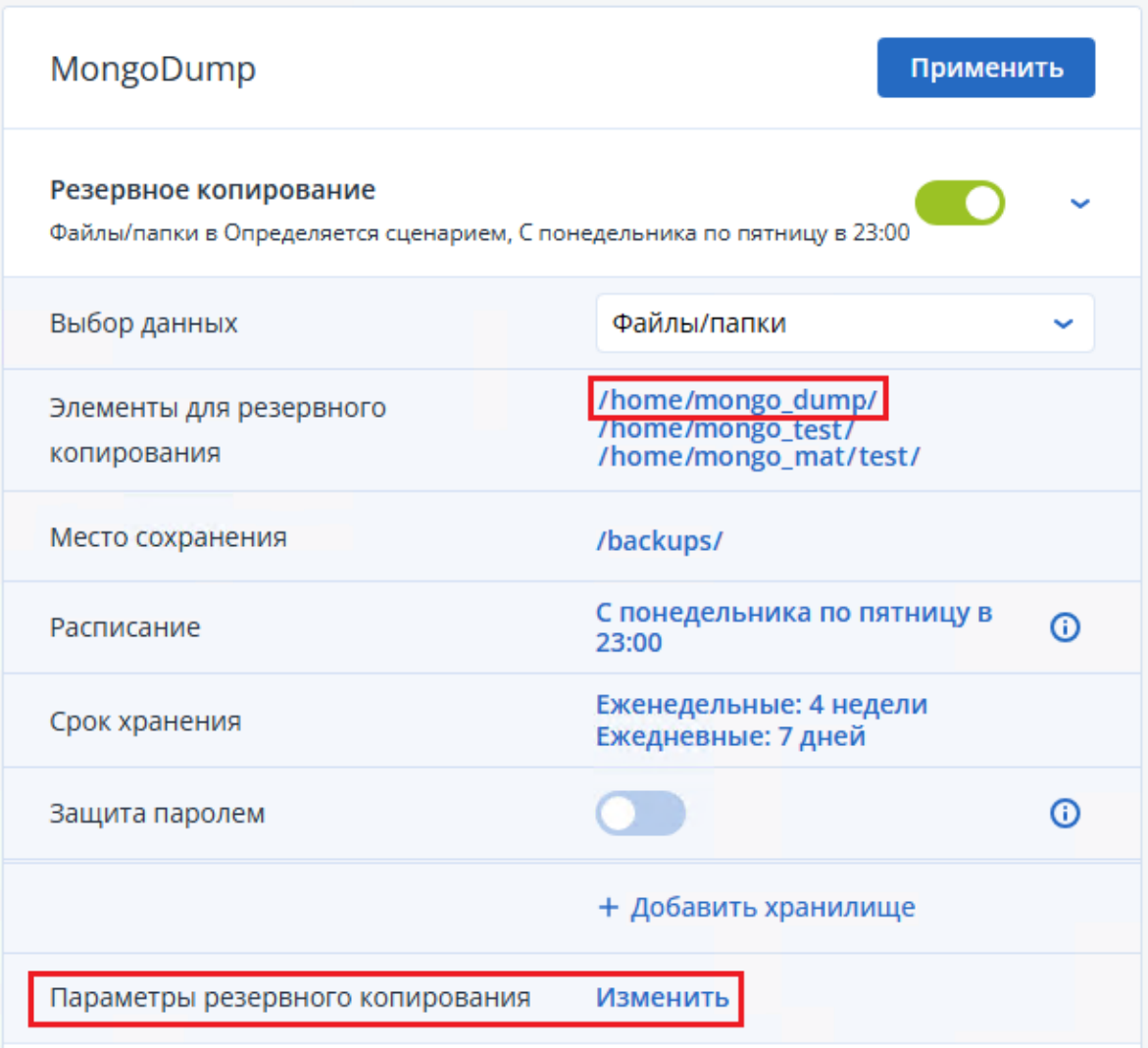
1. Перейдите в **Устройства** и выберите машину с базой данных MongoDB, которую вы хотите защитить.
2. Перейдите на вкладку справа **Защитить**.
3. В разделе **Выбор данных** укажите данные для резервного копирования. Возможные варианты:
   - Вся машина. Обратите внимание, что внешние диски не включаются в резервную копию всей машины (подробнее см. в разделе "Выбор всей машины" (стр. 272)).
   - Диски/тома.
   - Файлы/папки.

   В поле **Элементы для резервного копирования** нажмите **Указать** и выберите данные для резервного копирования. Папки, указанные в поле **Элементы для резервного копирования**, должны существовать до запуска резервного копирования (дочерние элементы могут быть созданы в ходе выполнения скрипта).

   Место хранения резервной копии из скрипта (например, /home/mongo_dump/latest) должно попадать в список данных для резервного копирования (либо явно, либо как дочерний элемент).
4. В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий.

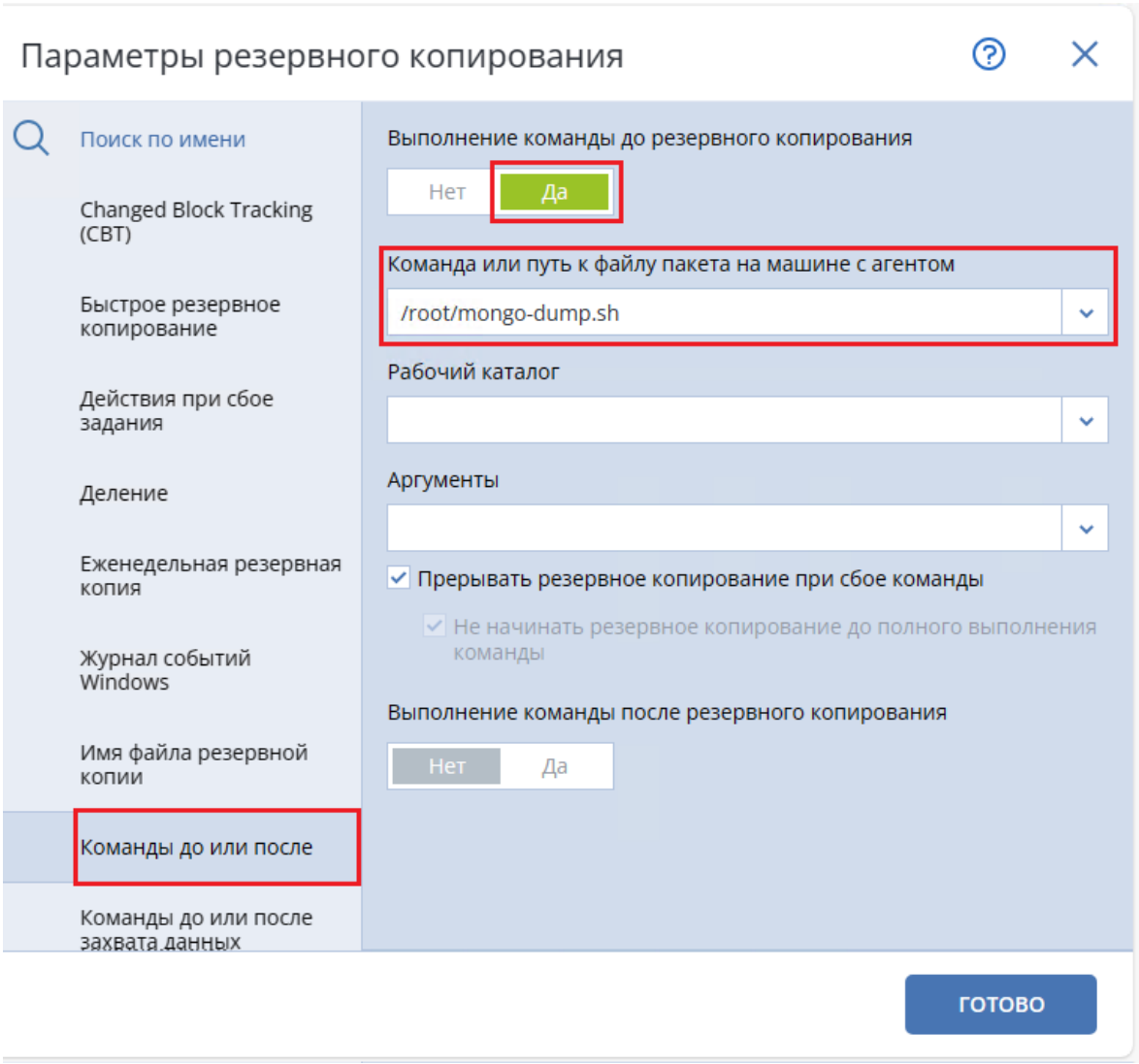
© ООО Киберпротект, 2026

5. В поле **Параметры резервного копирования** нажмите **Изменить**.



6. Выберите параметр **Команды до или после** (Также можно использовать параметр **Команды до или после захвата данных**). Включите переключатель **Выполнение команды до резервного копирования** и укажите путь до файла со скриптом с командами для утилиты mongodump:

© ООО Киберпротект, 2026



Примечание

Если работа утилиты mongodump завершается ошибкой (например, если mongodump не смогла установить соединение с базой данных), то при установленном флажке **Прерывать резервное копирование при сбое команды** Кибер Бэкап не начинает резервное копирование и отображает в интерфейсе сообщение об ошибке.

Однако, если утилита mongodump завершает работу без ошибки (return code = 0), то в Кибер Бэкап такая операция помечается как успешно выполненная при любых результатах работы mongodump.

Рекомендуем проверять результаты работы утилиты mongodump (например, в файле README.txt), чтобы убедиться, что резервная копия создана успешно.

Нажмите **Готово**.

7. При необходимости укажите другие параметры плана защиты. Подробнее см. в разделе "Резервное копирование" (стр. 264).
8. Нажмите **Применить**.

© ООО Киберпротект, 2026

Новый план защиты появится в списке планов.

12.9.2 Восстановление данных из резервной копии

Для восстановления данных из резервной копии используйте утилиту mongorestore. Подробнее см. в официальной документации MongoDB.

Пример:

```
# /usr/bin/mongorestore --host="localhost:27017" --db=my-db --collection=my-collection
/home/mongo_dump/restored_my-db/my-collection.bson
```

где:

- localhost:27017 — имя хоста развертывания MongoDB;
- my-db — конечная база данных для восстановления;
- my-collection — коллекция базы данных для восстановления;
- /home/mongo_dump/restored_my-db/my-collection.bson — место хранения и файл резервной копии.

12.10 Защита Kubernetes

12.10.1 Зачем защищать Kubernetes

С помощью Кибер Бэкап можно выполнять резервное копирование пространств имен и постоянных томов Kubernetes. При использовании Кибер Бэкап и Kubernetes регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователя и различных сбоев. Удаленные и поврежденные элементы можно восстановить из резервной копии.

12.10.2 Что необходимо для резервного копирования Kubernetes?

Для резервного копирования данных Kubernetes понадобятся установленные и настроенные продукты:

- Кибер Бэкап версии 17 или выше с лицензией Кибер Бэкап Расширенная редакция универсальная лицензия.
- Kubernetes версии 1.24 или выше.
  - Для создания моментальных снимков томов в кластере Kubernetes должны быть установлены CSI-драйвер с поддержкой функции Snapshot и контроллер моментальных снимков томов (см. раздел "Подготовка кластера Kubernetes" (стр. 619)).
  - Из кластера должен быть доступ к Docker-репозиторию https://registry.cyberprotect.ru/registry. В случае среды без доступа в Интернет можно разместить Docker-образ, необходимый агенту для Kubernetes, во внутреннем Docker-репозитории (см. раздел "Резервное копирование постоянных томов в хранилище Кибер Бэкап" (стр. 641)).

© ООО Киберпротект, 2026

Примечание
Защита каждого кластера Kubernetes требует отдельной лицензии Кибер Бэкап Расширенная редакция универсальная лицензия. Информацию о лицензиях см. в разделе "Издания и лицензии Кибер Бэкап" (стр. 16).

Для выполнения резервного копирования требуется установка агента.

Поддерживается установка агентов для следующих операционных систем:
Поддерживаемые операционные системы Linux с версией ядра от 3.0 до 6.12

- Astra Linux Special Edition 1.6 – 1.8
- РЕД ОС 7.2, 7.3, 8
- РОСА «КОБАЛЬТ» 7.9
- Альт Сервер 9, 10
- ОСнова 2.7 – 2.10, 3.0
- Red Hat Enterprise Linux версии с 7.x по 8.x, кроме конфигураций со Stratis
- Ubuntu 20.04 LTS, 22.04 LTS
- SUSE Linux Enterprise Server 12, 15, 15.5 — поддерживается в файловых системах, за исключением Btrfs
- Debian 10, 11, 12
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3, 9 Stream, 10 Stream

Перед установкой продукта в системе, в которой не используется диспетчер пакетов RPM, такой как Ubuntu, необходимо установить этот диспетчер вручную, например, выполнив следующую команду в качестве суперпользователя: apt-get install rpm.

12.10.3 Возможности

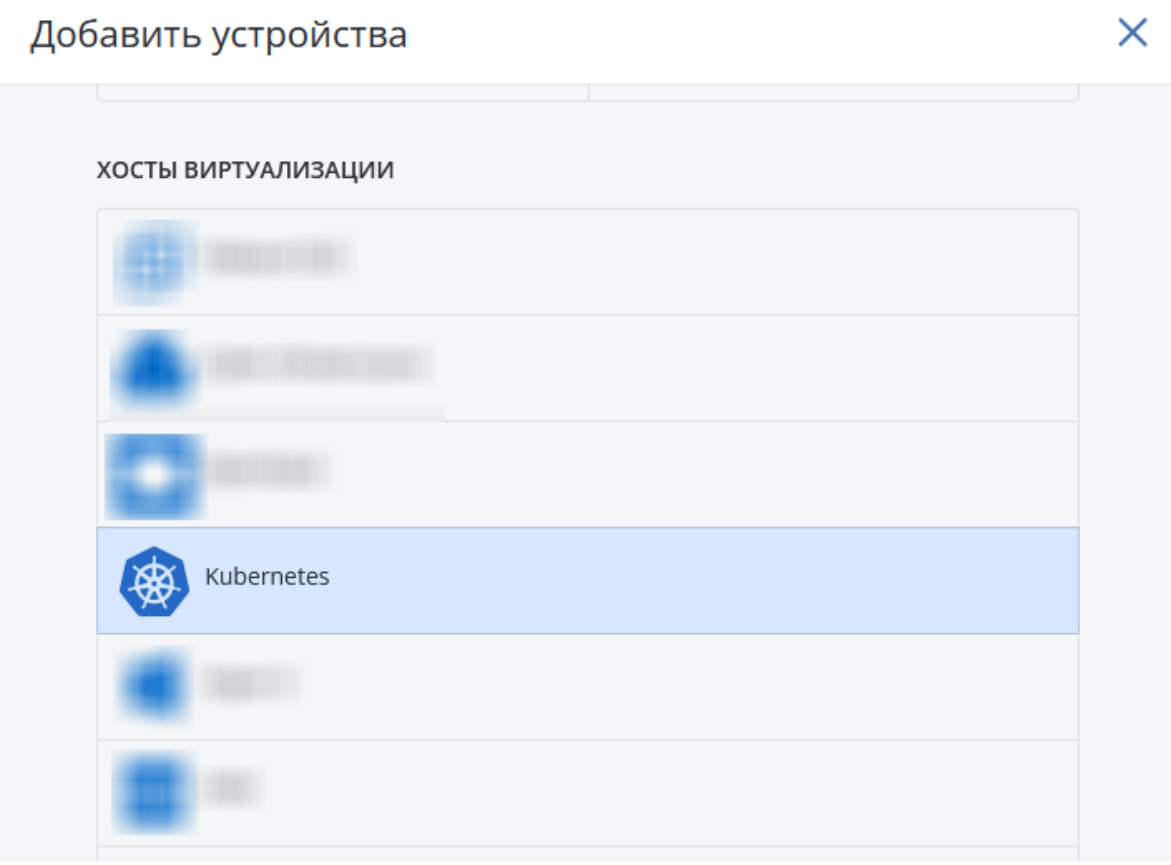
Кибер Бэкап позволяет выполнять резервное копирование и восстановление пространств имен, групп пространств имен и постоянных томов Kubernetes.

12.10.4 Установка агента для Kubernetes

Установите агент для Kubernetes:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Физические и виртуальные машины**.
2. Справа вверху щелкните **Добавить** и выберите в списке Kubernetes.

© ООО Киберпротект, 2026



3. Выберите **Скачать и установить Кибер Бэкап агент для Kubernetes** и укажите место сохранения установщика.

4. Запустите установщик Кибер Бэкап от имени привилегированного пользователя на сервере, на котором планируете установить агент.
5. Следуя инструкциям на экране, установите агент для Linux, агент для Kubernetes и, если необходимо, прочие компоненты.

См. также "Установка агентов в ОС Linux вручную" (стр. 97).

© ООО Киберпротект, 2026

Если агенту не удалось подключиться к серверу управления, выполните это подключение вручную, как описано в статье Ручная регистрация агента на сервере управления.

12.10.5 Подготовка кластера Kubernetes

Перед добавлением кластера в Кибер Бэкап подготовьте его, как описано в этом разделе.

12.10.5.1 Требования к CSI-драйверу

Для создания моментальных снимков томов в кластере должен быть установлен CSI-драйвер с поддержкой функции Snapshot.

Для резервного копирования томов в хранилище Кибер Бэкап CSI-драйвер должен поддерживать функцию Raw Block. Если ваш драйвер её не поддерживает, то следует добавить аннотацию в соответствующие ему объекты VolumeSnapshotClass:

```
kubectl annotate volumesnapshotclass <volume_snapshot_class_name> cyberprotect.ru/convert-to-block-mode=false
```

Список CSI-драйверов и сведения о поддерживаемых ими функциях см. в документации разработчика Kubernetes.

12.10.5.2 Установка контроллера моментальных снимков томов

Установите контроллер моментальных снимков томов, если он еще не установлен. Сведения об установке см. в статье. Подробные сведения о моментальных снимках томов см. в документации Kubernetes.

В процессе добавления кластера в веб-консоль управления агент для Kubernetes проверяет наличие установленного контроллера с помощью запроса в API-интерфейс Kubernetes, аналогичного следующей команде:

```
kubectl get volumesnapshots -n kube-system
```

В случае успешного выполнения запроса считается, что контроллер установлен.

Если в кластере есть несколько классов моментальных снимков томов (VolumeSnapshotClass), то каждый класс хранилища (StorageClass) необходимо привязать к одному из них с помощью аннотации:

```
kubectl annotate storageclass <storage_class_name> cyberprotect.ru/volume-snapshot-class=<volume_snapshot_class_name>
```

В этой команде storage_class_name – имя класса хранилища, volume_snapshot_class_name – имя класса моментальных снимков томов.

В классе моментальных снимков томов, который будет использоваться агентом для Kubernetes, в поле deletionPolicy должно быть установлено значение Delete. Если это не так, то будет

© ООО Киберпротект, 2026

использоваться созданная автоматически копия класса, в которой в поле deletionPolicy установлено значение Delete.

12.10.6 Создание служебной учетной записи для агента Kubernetes

Перед добавлением кластера Kubernetes в Кибер Бэкап создайте в нем служебную учетную запись для агента Kubernetes.

1. Создайте файл prepare-cluster.yaml с содержимым, приведенным ниже.

   prepare-cluster.yaml

```
apiVersion: v1
kind: Namespace
metadata:
  name: cyberprotect
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: cyberprotect
  namespace: cyberprotect
---
apiVersion: v1
kind: Secret
metadata:
 name: cyberprotect
 namespace: cyberprotect
 annotations:
  kubernetes.io/service-account.name: cyberprotect
type: kubernetes.io/service-account-token
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-discovery-generic
rules:
# Get cluster id
- apiGroups: [""]
  resources: ["namespaces"]
  resourceNames: ["kube-system"]
  verbs: ["get"]
# List nodes
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["list"]
# List namespaces
- apiGroups: [""]
  resources: ["namespaces"]
  verbs: ["list"]
# List storage classes
- apiGroups: ["storage.k8s.io"]
```


© ООО Киберпротект, 2026

```
  resources: ["storageclasses"]
  verbs: ["list"]
# List cluster resources
- apiGroups: ["*"]
  resources: ["*"]
  verbs: ["list"]
# Create cyberprotect namespace
- apiGroups: [""]
  resources: ["namespaces"]
  verbs: ["create"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-discovery-generic
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-discovery-generic
  apiGroup: rbac.authorization.k8s.io
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: cyberprotect-discovery-volume-backup
  namespace: cyberprotect
rules:
# Manage pods
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["*"]
# Manage jobs
- apiGroups: ["batch"]
  resources: ["jobs"]
  verbs: ["*"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: cyberprotect-discovery-volume-backup
  namespace: cyberprotect
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: Role
  name: cyberprotect-discovery-volume-backup
```


© ООО Киберпротект, 2026

```
  apiGroup: rbac.authorization.k8s.io
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-backup-generic
rules:
# List cluster resources
- apiGroups: ["*"]
  resources: ["*"]
  verbs: ["list"]
# Get persistent volume claims
- apiGroups: [""]
  resources: ["persistentvolumeclaims"]
  verbs: ["get"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-backup-generic
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-backup-generic
  apiGroup: rbac.authorization.k8s.io
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-backup-snapshotter
rules:
# Manage volume snapshots
- apiGroups: ["snapshot.storage.k8s.io"]
  resources: ["*"]
  verbs: ["*"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-backup-snapshotter
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-backup-snapshotter
  apiGroup: rbac.authorization.k8s.io
```


© ООО Киберпротект, 2026

```
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-backup-data-mover
rules:
# Create/delete pods, services and persistent volume claims. Execute commands in pods.
- apiGroups: [""]
  resources: ["pods", "pods/exec", "services", "persistentvolumeclaims"]
  verbs: ["create", "get", "delete"]
# Watch events
- apiGroups: [""]
  resources: ["events"]
  verbs: ["watch"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-backup-data-mover
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-backup-data-mover
  apiGroup: rbac.authorization.k8s.io
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-restore
rules:
# Manage namespaces
- apiGroups: [""]
  resources: ["namespaces"]
  verbs: ["create", "get", "update", "delete"]
# Manage core resources
- apiGroups: [""]
  resources: ["*"]
  verbs: ["*"]
# Manage workloads
- apiGroups: ["apps"]
  resources: ["*"]
  verbs: ["*"]
# Manage other cluster resources
- apiGroups: ["*"]
  resources: ["*"]
  verbs: ["create", "get", "update", "delete", "deletecollection"]
---
apiVersion: rbac.authorization.k8s.io/v1
```


© ООО Киберпротект, 2026

```
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-restore
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-restore
  apiGroup: rbac.authorization.k8s.io
```

2. Создайте в кластере ресурсы, перечисленные в файле prepare-cluster.yaml:

```
kubectl create -f prepare-cluster.yaml
```

3. Разрешите запуск привилегированных подов в пространстве имён cyberprotect:

```
kubectl label --overwrite ns cyberprotect pod-security.kubernetes.io/enforce=privileged
```

4. Получите и сохраните токен служебной учетной записи cyberprotect:

```
kubectl -n cyberprotect describe secret cyberprotect
```

12.10.6.1 Дополнительные действия для кластера Deckhouse

Разрешите запуск привилегированных подов в пространстве имён cyberprotect:

```
kubectl label --overwrite ns cyberprotect security.deckhouse.io/pod-policy=privileged
```

12.10.6.2 Для защиты системных пространств имен кластера Deckhouse

1. Создайте ресурс Secret с токеном для служебной учетной записи deckhouse:

```
apiVersion: v1
kind: Secret
metadata:
 name: deckhouse-secret
 namespace: d8-system
 annotations:
  kubernetes.io/service-account.name: deckhouse
type: kubernetes.io/service-account-token
```

2. Выполните следующую команду:

```
kubectl -n d8-system describe secret deckhouse-secret
```

3. Получите и сохраните токен служебной ученой записи deckhouse:

© ООО Киберпротект, 2026

```
root@k8s-d-node1:/home/myuser# kubectl -n d8-system describe secret deckhouse-secret
Name:       deckhouse-secret
Namespace:    d8-system
Labels:      <none>
Annotations:  kubernetes.io/service-account.name: deckhouse
              kubernetes.io/service-account.uid: 1db29c03-13d5-4a9d-a084-00348b739b05

Type:  kubernetes.io/service-account-token

Data
====
ca.crt:    1107 bytes
namespace:  9 bytes
token:     <...>
```

12.10.7 Подготовка файла kubeconfig

Перед добавлением кластера Kubernetes в Кибер Бэкап подготовьте конфигурационный файл kubeconfig.

Процедура подготовки файла далее описана для двух случаев:

- создание резервной копии и восстановление пользовательских пространств имен Kubernetes;
- создание резервной копии и восстановление системных пространств имен Deckhouse.

12.10.7.1 Подготовка файла в случае защиты пользовательских пространств имен Kubernetes

1. Загрузите на рабочую машину файл конфигурации kubeconfig по умолчанию. Путь к файлу конфигурации по умолчанию – /etc/kubernetes/admin.conf.
2. Внесите в файл следующие изменения:
   - замените имя исходной служебной учетной записи (например, admin) на cyberprotect;
   - замените сертификат для аутентификации пользователя (client-certificate-data: <...>) на токен (token: <...>), который был подготовлен в разделе "Создание служебной учетной записи для агента Kubernetes" (стр. 620).
3. Сохраните внесенные изменения.

Пример файла, который должен получиться в итоге:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: <...>
    server: https://192.168.1.100:6443
  name: myk8scluster
contexts:
- context:
```


© ООО Киберпротект, 2026

```
    cluster: myk8scluster
    user: cyberprotect
  name: default
current-context: default
kind: Config
preferences: {}
users:
- name: cyberprotect
  user:
    token: <...>
```

12.10.7.2 Подготовка файла в случае защиты системных пространств имен Deckhouse

1. Загрузите на рабочую машину файл kubeconfig по умолчанию.
2. Внесите в файл следующие изменения:
   - замените имя исходной служебной учетной записи (например, kubernetes-admin) на deckhouse;
   - замените сертификат для аутентификации пользователя (client-certificate-data: <...>) на токен (token: <...>), который был подготовлен в разделе "Создание служебной учетной записи для агента Kubernetes" (стр. 620).
3. Сохраните внесенные изменения.

Пример файла, который должен получиться в итоге:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: <...>
    server: https://10.11.12.13:6443
  name: deckhouse
contexts:
- context:
    cluster: deckhouse
    user: deckhouse
  name: deckhouse@deckhouse
current-context: deckhouse@deckhouse
kind: Config
preferences: {}
users:
- name: deckhouse
  user:
    token: <...>
```

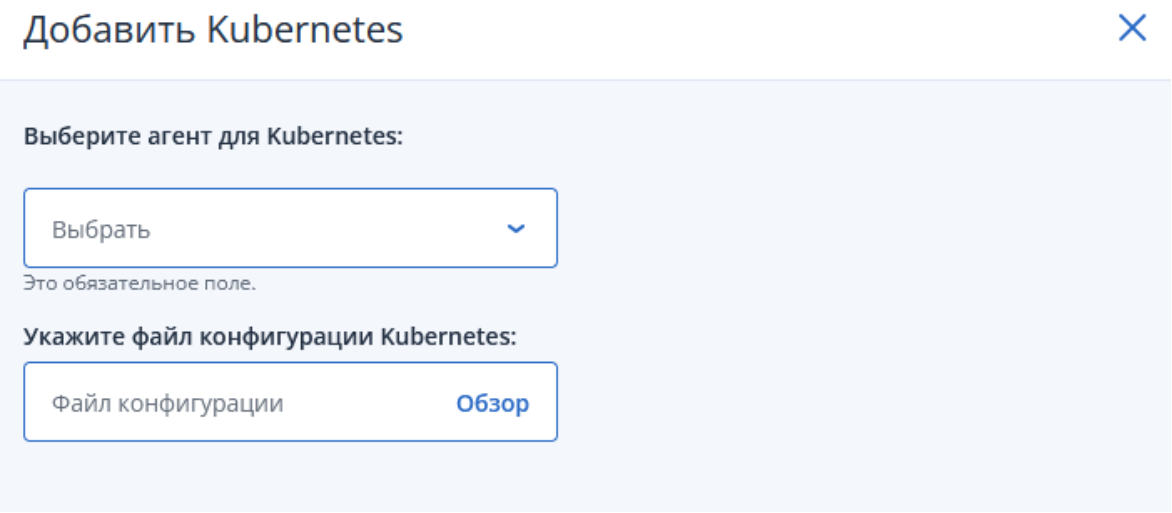
12.10.8 Добавление кластера Kubernetes

Добавьте кластер Kubernetes в Кибер Бэкап:

© ООО Киберпротект, 2026

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Физические и виртуальные машины**.
2. Справа вверху щелкните **Добавить** и выберите в списке **Kubernetes**.
3. Выберите **Добавить кластер Kubernetes**.

4. Укажите агент для Kubernetes, для которого будет выполнена регистрация, и файл конфигурации kubeconfig, который был подготовлен в разделе "Подготовка файла kubeconfig" (стр. 625).
   Для подключения к кластеру Kubernetes файл конфигурации должен содержать адрес кластера, имя пользователя и токен.



   После заполнения полей нажмите **Добавить** и дождитесь окончания установки.
5. В веб-консоли перейдите в раздел **Устройства** и убедитесь, что кластер Kubernetes добавлен в вашу конфигурацию.
6. В веб-консоли перейдите в раздел **Настройки** > **Агенты** и убедитесь, что агент для Kubernetes отображается в списке агентов.

© ООО Киберпротект, 2026

12.10.9 Резервное копирование Kubernetes

12.10.9.1 Предварительные требования

Перед резервным копированием убедитесь, что вы выполнили следующие действия:

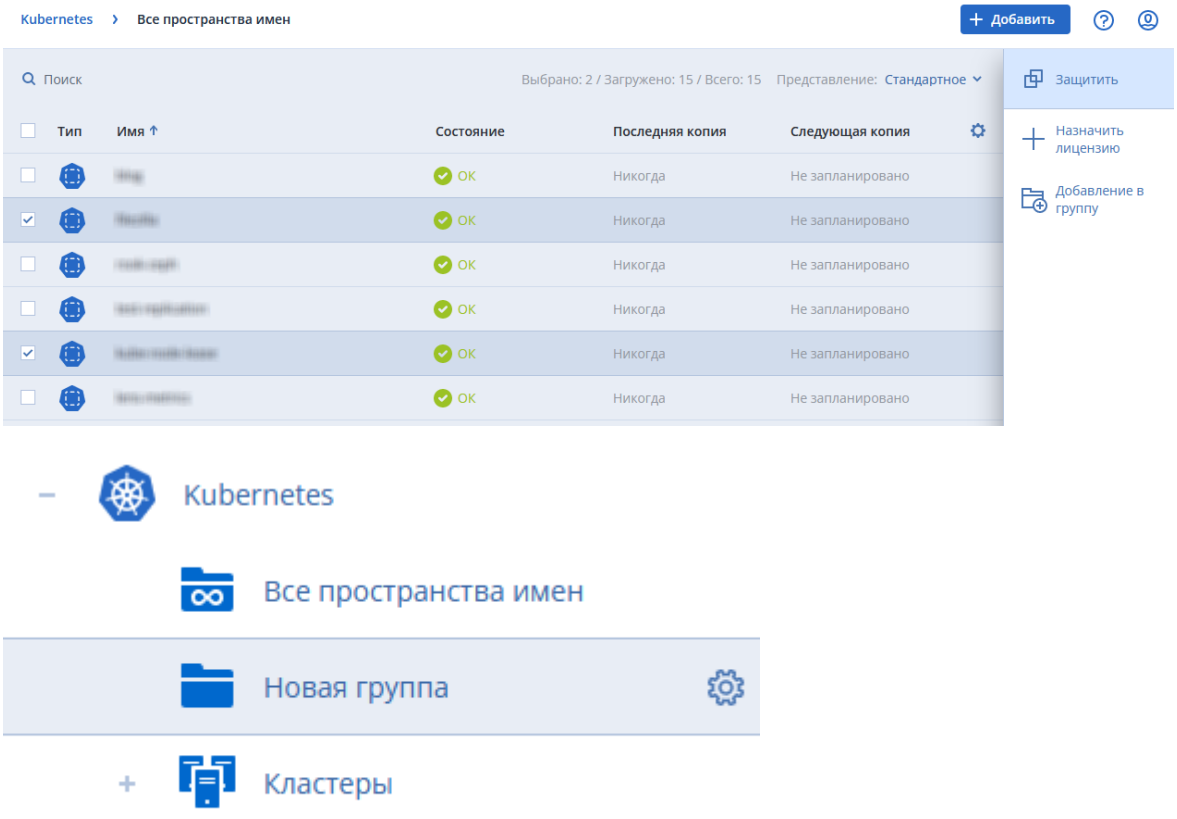
1. Установка агента Кибер Бэкап для Kubernetes и подключение кластера Kubernetes к Серверу управления (см. "Установка агента для Kubernetes" (стр. 617) и "Добавление кластера Kubernetes" (стр. 626)).
2. Настройка хранилища. Настройте ваше хранилище для работы с Кибер Бэкап и Kubernetes.

12.10.9.2 Создание плана защиты

Создание плана защиты из веб-консоли возможно двумя способами: через пункт веб-консоли **Устройства** и через пункт **Планы** (см. также "Создание плана защиты" (стр. 224)).

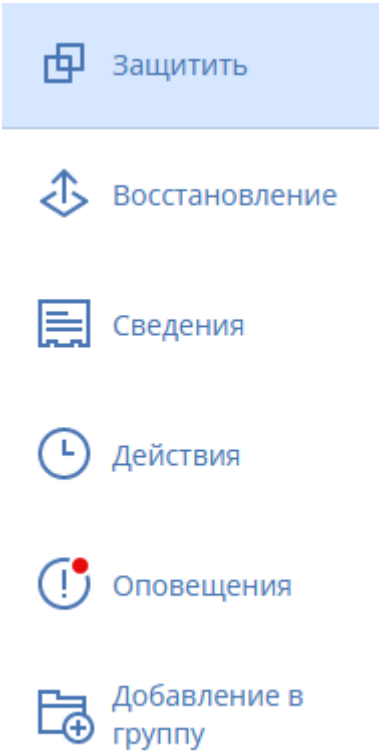
Создание плана через пункт веб-консоли Устройства

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** > **Kubernetes**.
2. Выберите пространства имен (или группу с пространствами имен) для защиты.

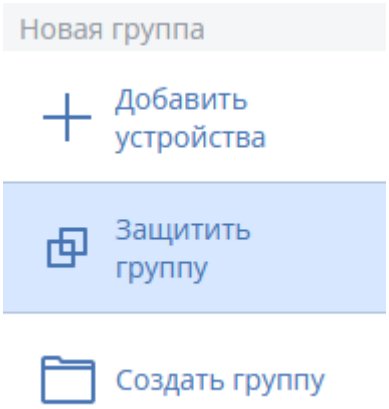


3. Нажмите справа вверху **Защитить**.

© ООО Киберпротект, 2026

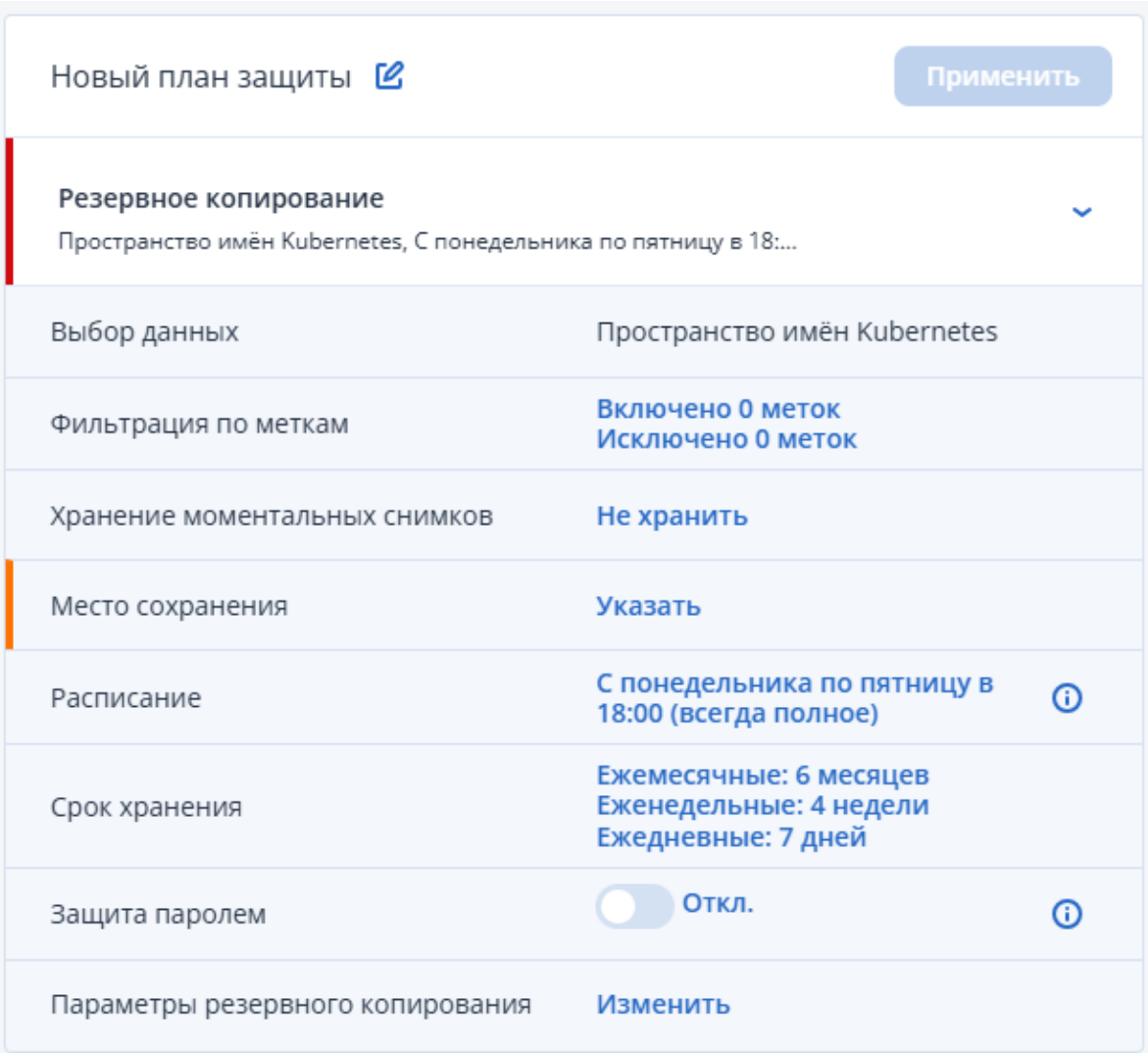


Для защиты группы выберите **Защитить группу**.



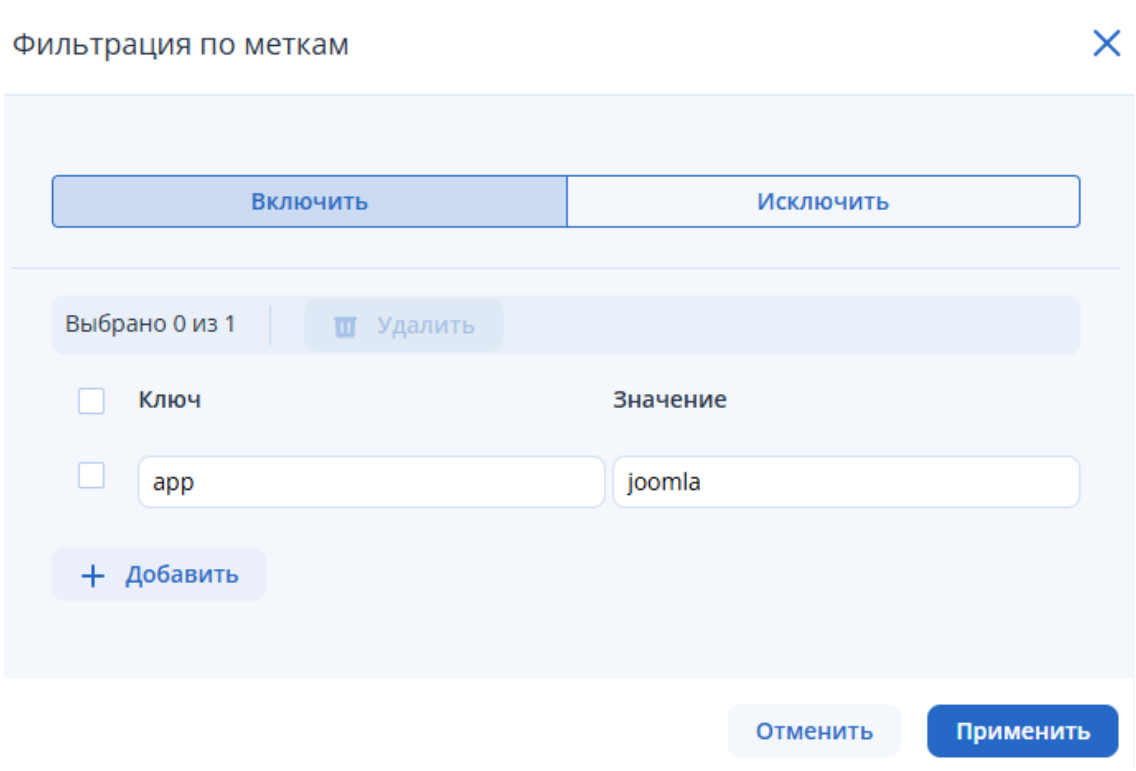
4. Щелкните **Создать план** (если план не применен) или **Добавить план** (если какой-либо план в данный момент применен).
5. Выберите необходимые вам настройки плана защиты, заполнив соответствующие поля:

© ООО Киберпротект, 2026



a. **Фильтрация по меткам**. Укажите метки ресурсов Kubernetes, по которым ресурсы будут включаться в план защиты.

© ООО Киберпротект, 2026



Особенности резервного копирования в рамках плана защиты с метками:

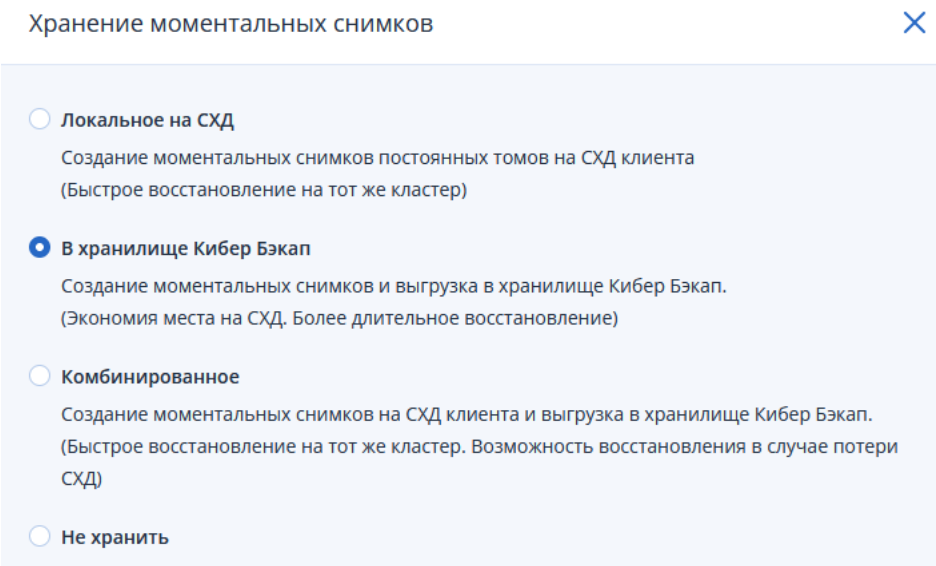
- В резервную копию попадает не только ресурс с включающей меткой, но и вся цепочка связанных с ним ресурсов. Например, для цепочки ресурсов Deployment → ReplicaSet → Pod при указании включающей метки ресурса Pod Кибер Бэкап производит резервное копирование только ресурса Deployment, при этом попадает в резервную копию и восстанавливается вся цепочка ресурсов.

  Примечание
  Восстановление цепочек зависимостей ресурсов Custom Resources может работать некорректно.

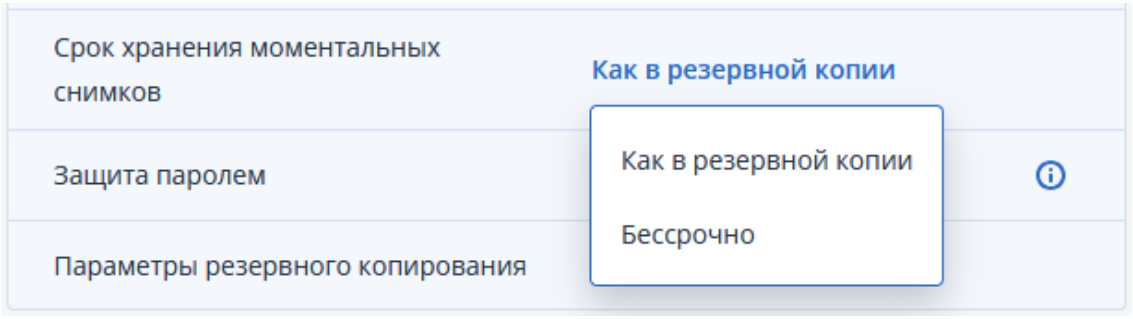
- Ресурс, который имеет как включающую, так и исключающую метку, не будет включен в план защиты.
- Для резервного копирования постоянного тома должна присутствовать включающая метка самого тома (Persistent Volume) или запроса на хранилище тома (Persistent Volume Claim). При резервном копировании постоянного тома в резервную копию всегда включаются ресурсы Persistent Volume, Persistent Volume Claim и Storage Class.
- Если в плане защиты включено хранение моментальных снимков, то в резервную копию включаются ресурсы Volume Snapshot, Volume Snapshot Class и Volume Snapshot Content.

b. **Хранение моментальных снимков**. Укажите место, где будут сохраняться моментальные снимки.

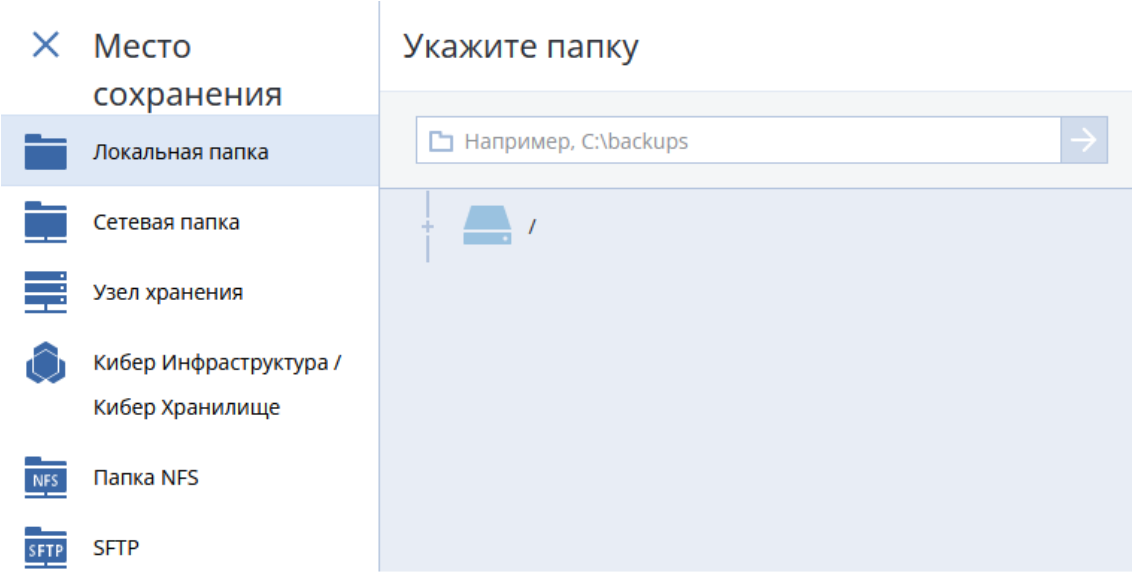
© ООО Киберпротект, 2026



При выборе варианта хранения **Локальное на СХД** укажите также срок хранения моментальных снимков в появившейся области **Срок хранения моментальных снимков**.



c. **Место сохранения**. В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.



© ООО Киберпротект, 2026

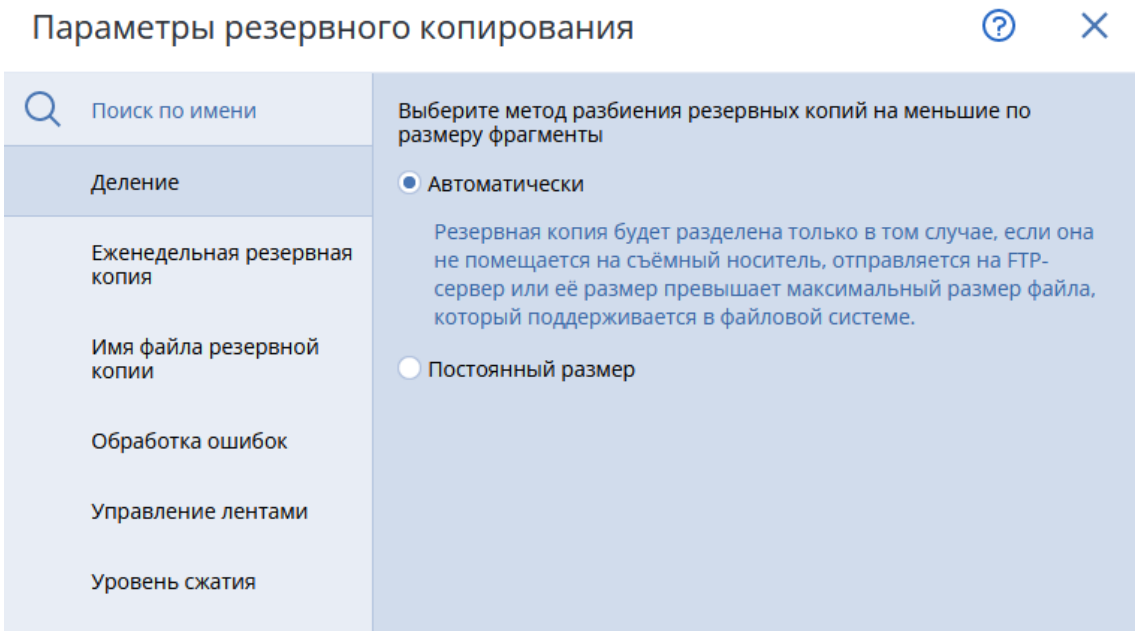
Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места сохранения" (стр. 278).

d. [Необязательно] **Расписание**. Задайте расписание резервного копирования.

e. [Необязательно] **Срок хранения**. Укажите срок хранения резервных копий.

f. [Необязательно] **Защита паролем**. Активируйте защиту паролем при необходимости.

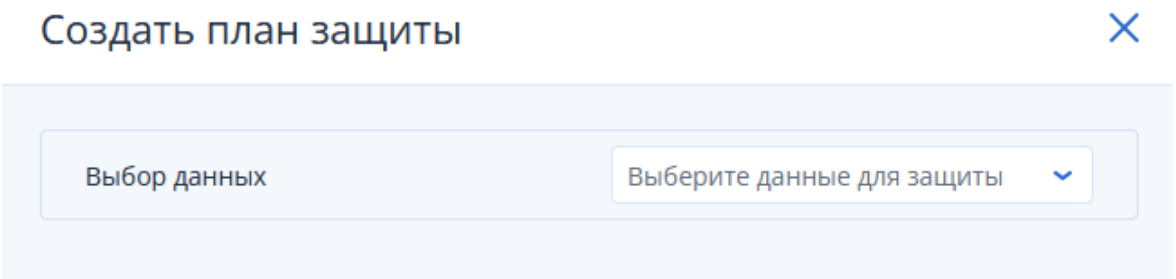
g. [Необязательно] **Параметры резервного копирования**. Выберите параметры резервного копирования (см. также "Параметры резервного копирования" (стр. 335)).



6. Нажмите **Применить**.

Создание плана через пункт веб-консоли Планы

1. В веб-консоли перейдите в раздел **Планы** > **Защита**.
2. Нажмите справа вверху **Создать план**.
3. В открывшемся окне в строке **Выбор данных** выберите из списка **Kubernetes**.



4. В окне создания плана настройте план нужным вам образом и нажмите **Создать**.

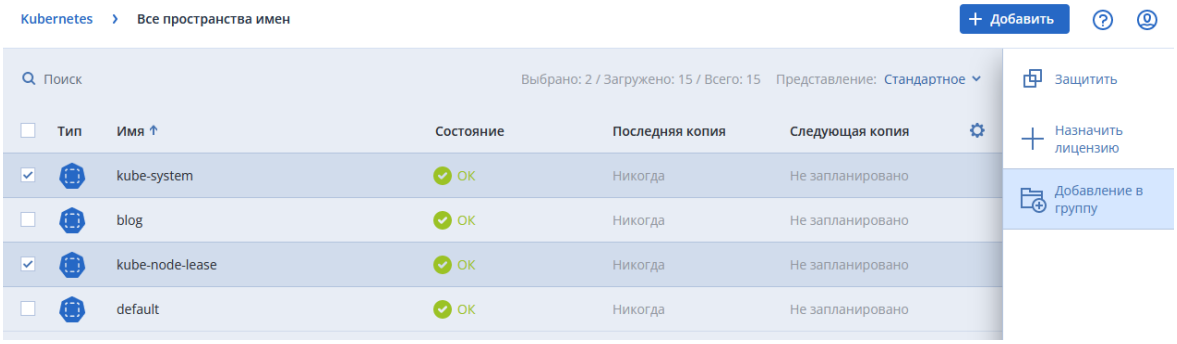
© ООО Киберпротект, 2026

12.10.9.3 Создание групп

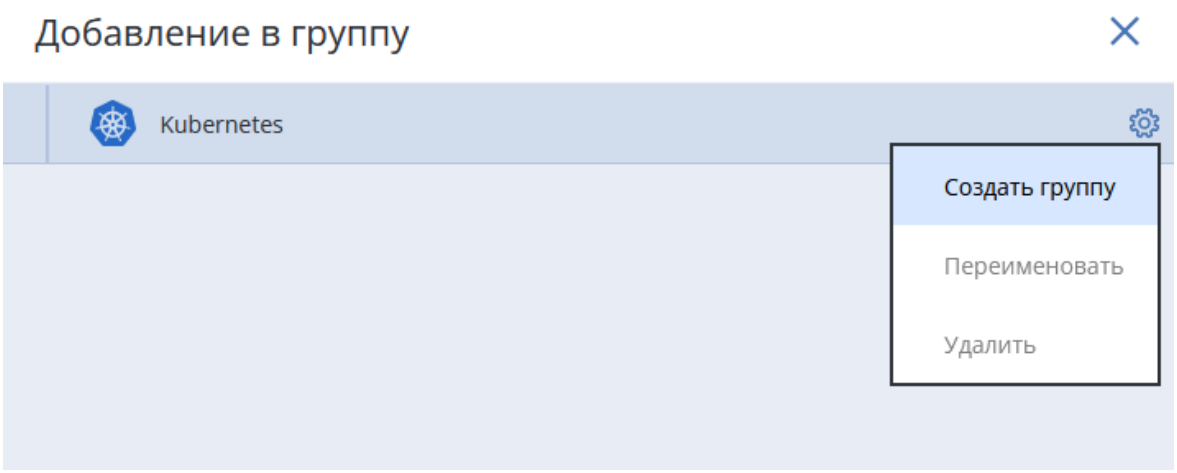
С Кибер Бэкап вы можете создавать и защищать не только отдельные пространства имен, но и группы пространств имен.

Для создания группы пространств имен выполните следующие действия:

1. В веб-консоли перейдите в раздел **Устройства** > **Kubernetes**.
2. Отметьте в списке устройства, которые хотите добавить в группу, и щелкните справа **Добавление в группу**.

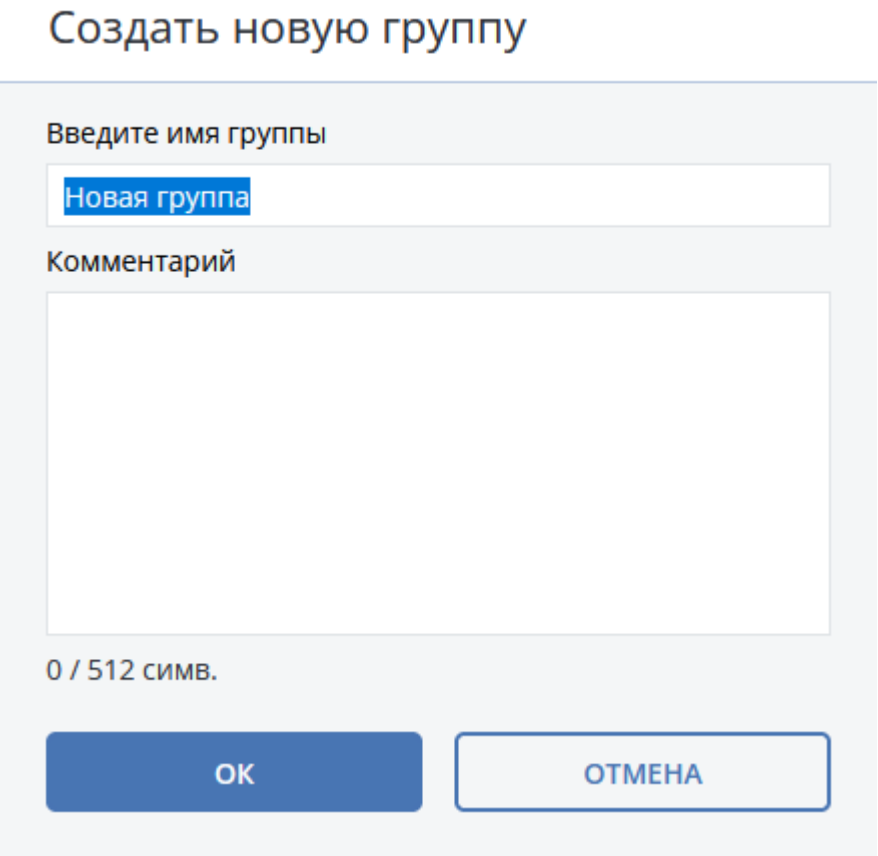


3. Щелкните значок шестеренки и выберите **Создать группу**.



4. Введите имя группы; если требуется, добавьте комментарий и нажмите **OK**.

© ООО Киберпротект, 2026



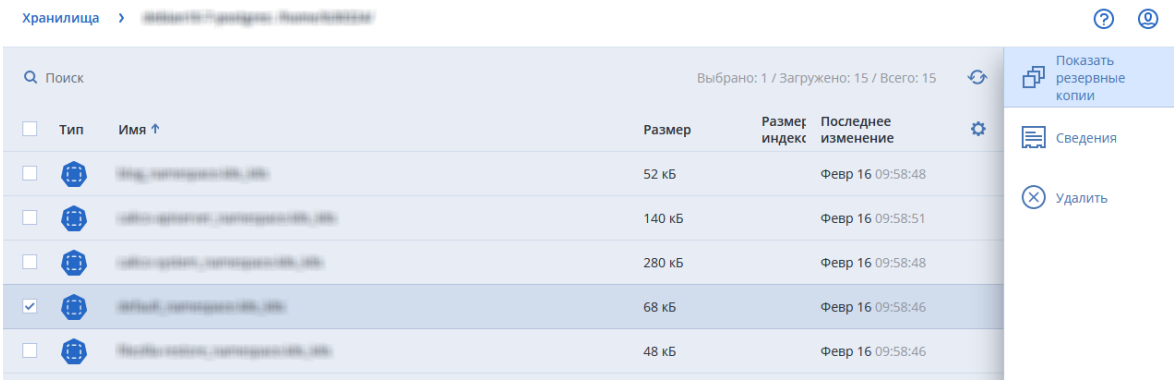
5. Нажмите **Готово**.

12.10.10 Восстановление Kubernetes

Перед восстановлением убедитесь, что место хранения резервных копий доступно, а резервные копии, из которых вы хотите выполнить восстановление, были созданы успешно.

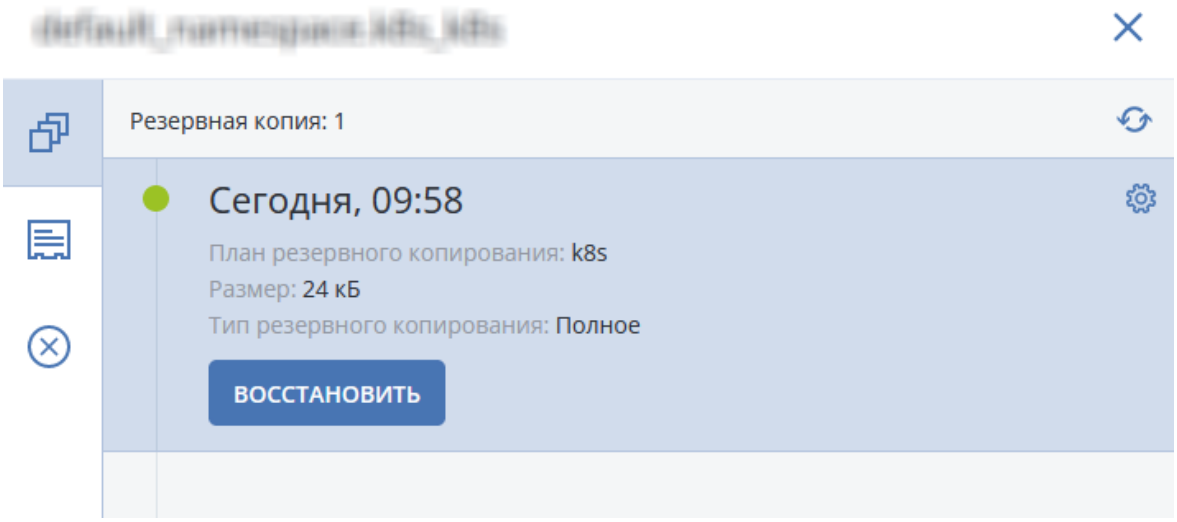
Восстановление пространства имен и постоянных томов Kubernetes из меню Резервные копии

1. В веб-консоли перейдите в раздел **Хранилища резервных копий** и выберите хранилище с резервными копиями Kubernetes.
2. В списке резервных копий Kubernetes отметьте нужную вам и нажмите справа вверху **Показать резервные копии**.



© ООО Киберпротект, 2026

3. Выберите нужную резервную копию из списка и нажмите **Восстановить**.



4. Для восстановления щелкните **Восстановить все пространство**.

   Для просмотра списка постоянных томов щелкните **Постоянные тома**.

   Для просмотра сведений о конфигурации:

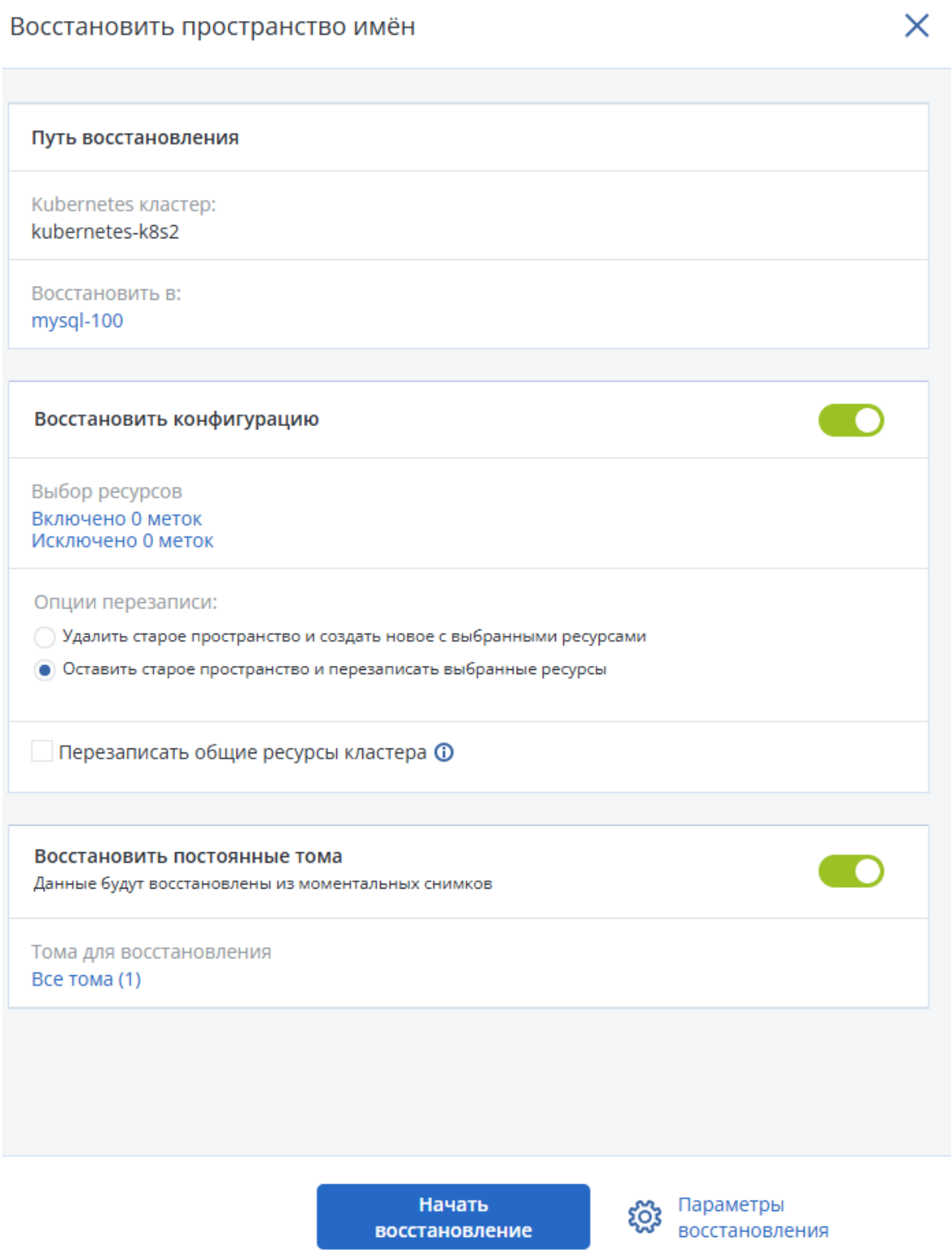
   a. щелкните **Конфигурация**;

   b. отметьте в списке необходимый элемент;

   c. нажмите справа **Открыть YAML** для просмотра сведений или **Скачать** для сохранения файла со сведениями.

5. Укажите параметры восстановления.

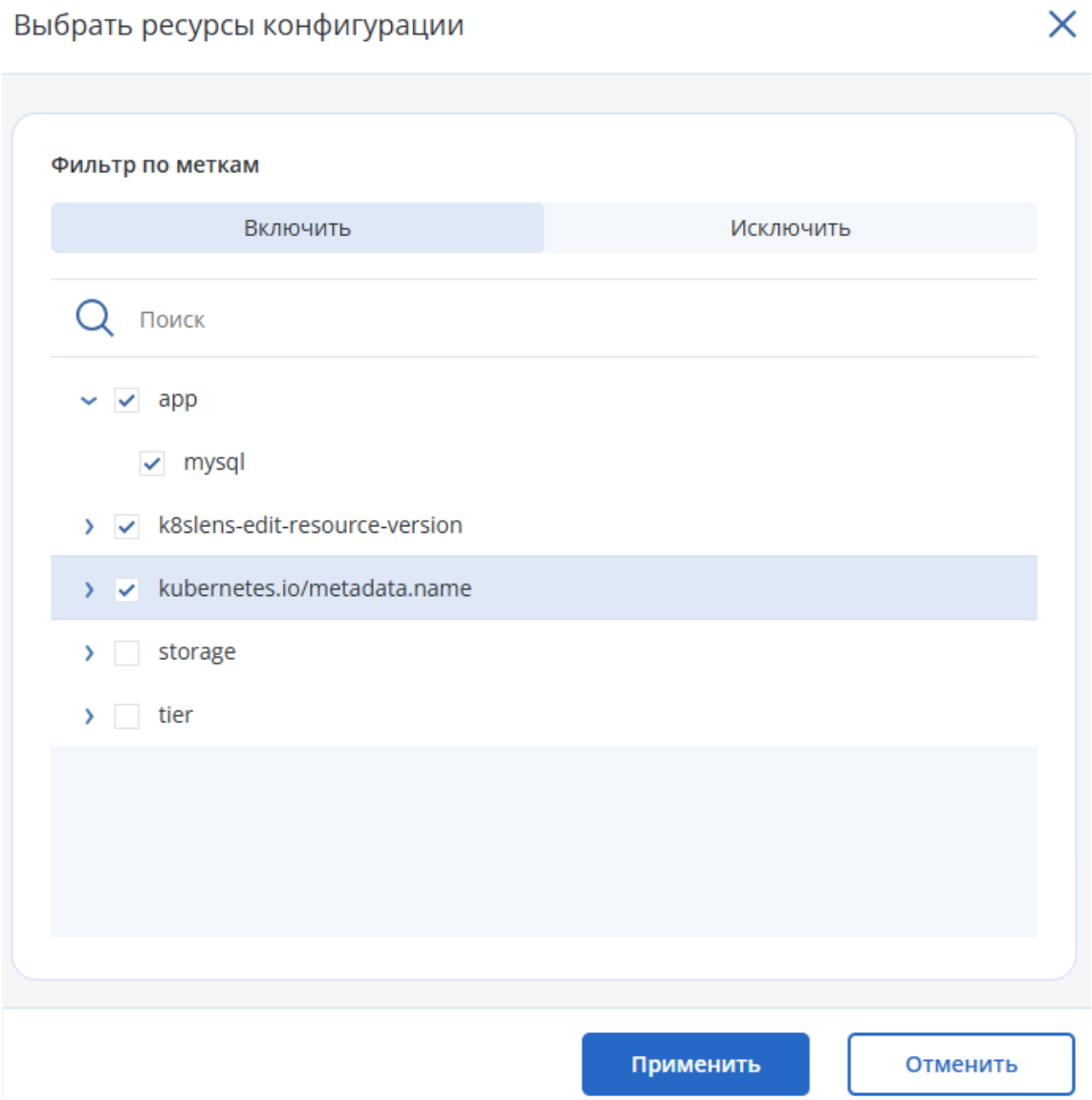
© ООО Киберпротект, 2026



- Укажите место для восстановления резервной копии. Выберите установленное по умолчанию место или укажите новое.
- Для восстановления конфигурации в области **Восстановить конфигурацию** укажите нужный вариант и передвиньте ползунок.

© ООО Киберпротект, 2026

- Для восстановления с фильтрацией по меткам щелкните раздел **Выбор ресурсов**. Укажите метки ресурсов, которые необходимо восстановить:



Особенности восстановления с фильтраций по меткам:

- Восстанавливается не только ресурс с включающей меткой, но и вся цепочка связанных с ним ресурсов.

  Примечание
  Восстановление цепочек зависимостей ресурсов Custom Resources может работать некорректно.

- Ресурс, который имеет как включающую, так и исключающую метку, не будет восстановлен.
- Для восстановления постоянного тома должна присутствовать включающая метка самого тома (Persistent Volume) или запроса на хранилище тома (Persistent Volume Claim). При восстановлении постоянного тома всегда восстанавливаются ресурсы Persistent Volume,

© ООО Киберпротект, 2026

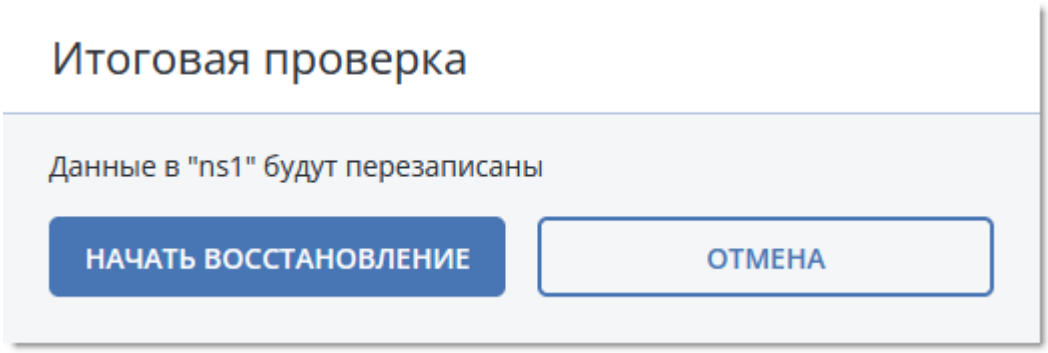
Persistent Volume Claim и Storage Class (так же восстанавливаются ресурсы Volume Snapshot, Volume Snapshot Class и Volume Snapshot Content, если они присутствуют в резервной копии).

- Для восстановления всех постоянных томов передвиньте ползунок в области **Восстановить постоянные тома**. При необходимости измените параметры восстановления томов, такие как имя тома и класс хранения, нажав **Все тома**.

  Примечание
  При восстановлении тома с новым именем исходный том не удаляется из кластера.

  Сведения о том, как восстановить только выбранные постоянные тома, не восстанавливая при этом пространство имен, см. в подразделе "Восстановление постоянных томов из меню **Резервные копии**".
- [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.

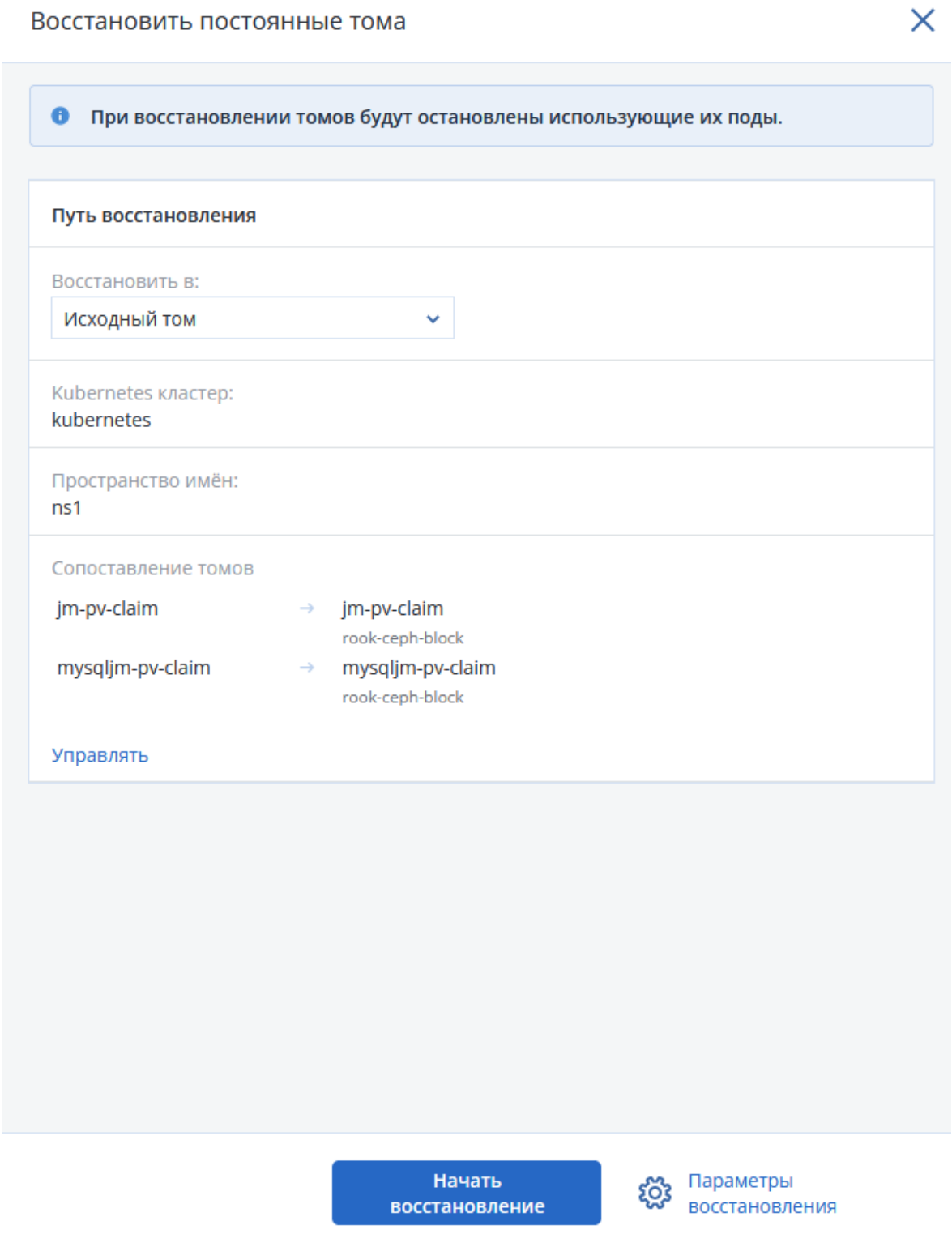
6. Нажмите **Начать восстановление**. Подтвердите еще раз восстановление в открывшемся окне и дождитесь его окончания.



Восстановление постоянных томов из меню Резервные копии

1. В веб-консоли перейдите в раздел **Хранилища резервных копий** и выберите хранилище с резервными копиями Kubernetes.
2. В списке резервных копий Kubernetes отметьте нужную вам и нажмите справа вверху **Показать резервные копии**.
3. Выберите нужную резервную копию из списка и нажмите **Восстановить**.
4. Щелкните **Постоянные тома** и выберите тома, которые необходимо восстановить.
5. Справа вверху щелкните **Восстановить постоянные тома**.
6. Укажите параметры восстановления.

© ООО Киберпротект, 2026



- Укажите место для восстановления резервной копии. Выберите установленное по умолчанию место или укажите новое.
- При необходимости измените имена и классы хранения восстанавливаемых томов, щелкнув **Управлять** в разделе **Сопоставление томов**.

© ООО Киберпротект, 2026

Примечание
Автоматическое сопоставление томов возможно только в последовательном порядке при условии, что конфигурации целевой машины и машины-источника одинаковы. Если конфигурации машин различаются, сопоставить тома можно только в ручном режиме.

Примечание
При восстановлении тома с новым именем исходный том не удаляется из кластера.

- [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.

7. Нажмите **Начать восстановление**. Подтвердите еще раз восстановление в открывшемся окне и дождитесь его окончания.

Примечание
Для корректного восстановления убедитесь, что конфигурационный файл kubeconfig подготовлен необходимым образом (подробнее см. "Подготовка файла kubeconfig" (стр. 625)).

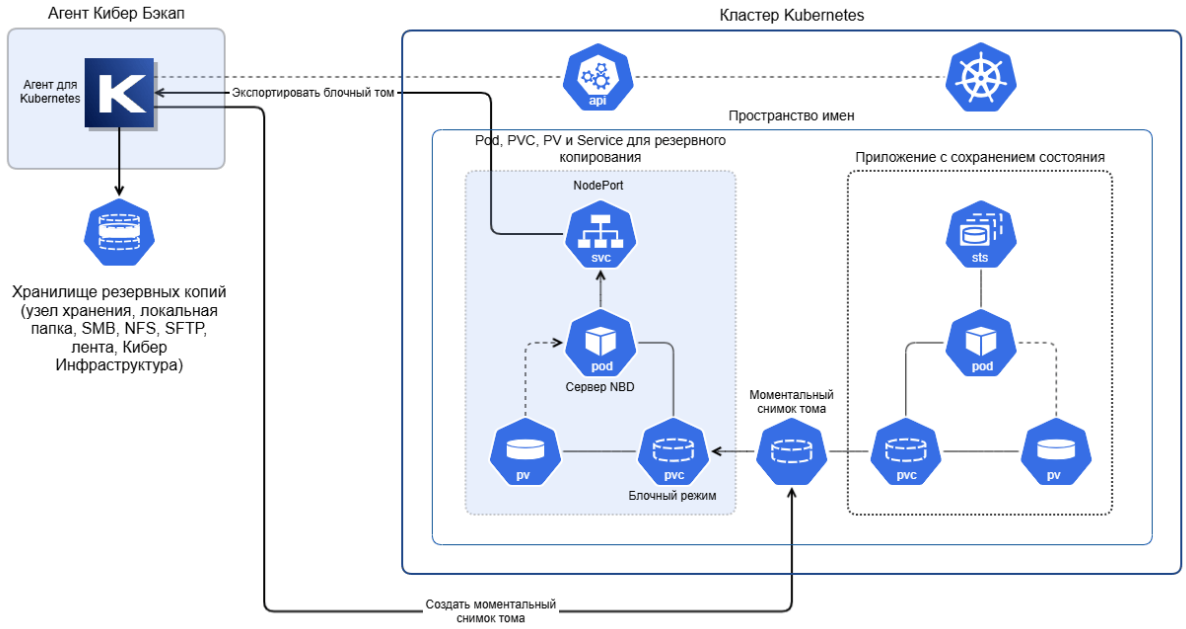
12.10.11 Резервное копирование постоянных томов в хранилище Кибер Бэкап

12.10.11.1 Резервное копирование

Резервное копирование постоянного тома (PersistentVolume) в хранилище Кибер Бэкап выполняется следующим образом:

1. Создается моментальный снимок исходного тома (VolumeSnapshotContent).
2. На основе моментального снимка создается временный том в блочном режиме или в режиме файловой системы (при наличии аннотации cyberprotect.ru/convert-to-block-mode=false в VolumeSnapshotClass).
3. В служебном пространстве имён cyberprotect создается временный под (Pod) с сервером NBD/NFS на основе Docker-образа k8s-backup-and-restore, к которому подключен временный том.
4. Создается сервис (Service) типа NodePort, посредством которого агент для Kubernetes может получить данные временного тома. В случае недоступности сервиса агент использует механизм port forwarding.
5. Агент для Kubernetes получает данные временного тома, создается резервная копия тома в хранилище Кибер Бэкап.
6. По завершении создания резервной копии сервис, временные под и том удаляются. Моментальный снимок тома удаляется при использовании режима хранения моментальных снимков тома **В хранилище Кибер Бэкап** либо оставляется в кластере при использовании режима **Комбинированное**.

© ООО Киберпротект, 2026

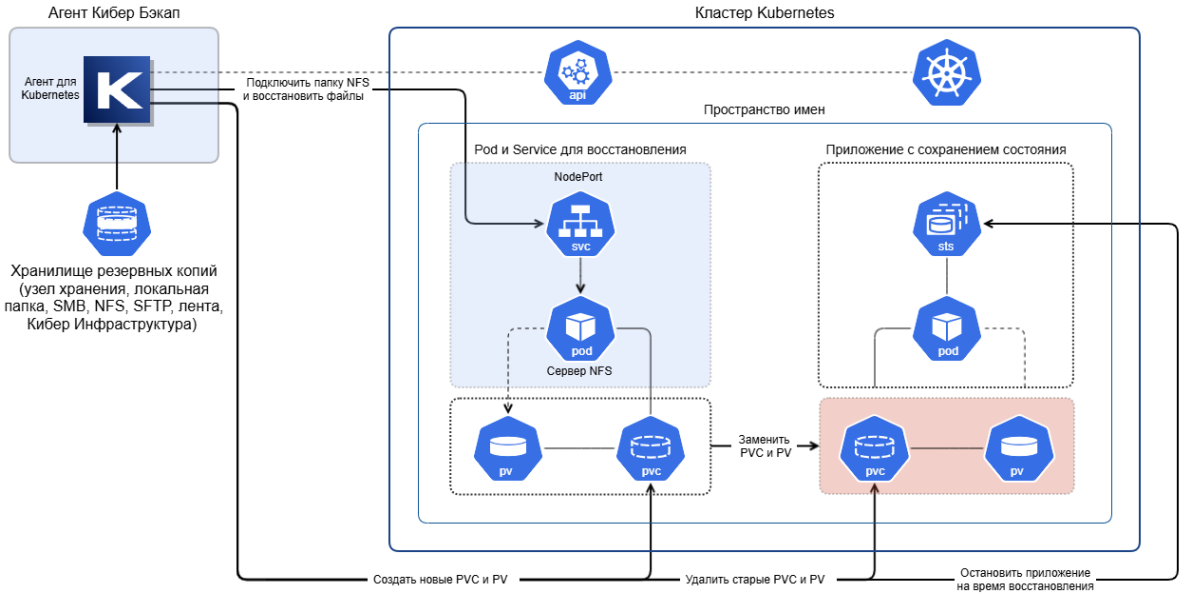


12.10.11.2 Восстановление из резервной копии

Восстановление тома из размещенной в хранилище Кибер Бэкап резервной копии происходит следующим образом:

1. Останавливаются использующие восстанавливаемый том приложения (число реплик устанавливается равным нулю или удаляются поды).
2. В служебном пространстве имён cyberprotect создаются новый том и временный под (Pod) с сервером NFS; при этом старый том удаляется, если его имя совпадает с именем нового тома.
3. Создается сервис типа NodePort, посредством которого агент для Kubernetes может записать данные из резервной копии на новый том. В случае недоступности сервиса агент использует механизм port forwarding.
4. Агент для Kubernetes монтирует папку NFS и записывает данные из резервной копии на новый том.
5. Сервис и временный под (Pod) удаляются. Объект PersistentVolumeClaim тома переносится в целевое пространство имён.
6. Новый том подключается к требуемым подам, восстанавливается исходное число реплик приложений.

© ООО Киберпротект, 2026



12.10.11.3 Требования

- Для создания моментальных снимков томов в кластере Kubernetes должен быть установлен CSI-драйвер с поддержкой функции Snapshot.

  Для резервного копирования томов в хранилище Кибер Бэкап CSI-драйвер должен поддерживать функцию Raw Block. Если ваш драйвер её не поддерживает, то следует добавить аннотацию в соответствующие ему объекты VolumeSnapshotClass:

  ```
  kubectl annotate volumesnapshotclass <volume_snapshot_class_name>
  cyberprotect.ru/convert-to-block-mode=false
  ```

  Список CSI-драйверов и сведения о поддерживаемых ими функциях см. в документации разработчика Kubernetes.
- Из кластера должен быть доступен Docker-репозиторий, из которого можно получить Docker-образ k8s-backup-and-restore. По умолчанию используется публичный Docker-репозиторий компании Киберпротект registry.cyberprotect.ru/registry.
- Сервисная учетная запись cyberprotect должна обладать правами на запуск пода в привилегированном режиме в целевом пространстве имен.

12.10.11.4 Настройка доступа в Docker-репозиторий в закрытой среде

При отсутствии доступа в Docker-репозиторий по умолчанию (например, если Кибер Бэкап используется в среде без доступа в Интернет) можно загрузить из него Docker-образ k8s-backup-and-restore и разместить его в Docker-репозитории, который доступен в пределах закрытой среды. Например:

1. На машине, на которой есть доступ к Docker-репозиторию по умолчанию и на которой установлен Docker, получите Docker-образ и сохраните его в виде tar-архива:

© ООО Киберпротект, 2026

```
CYBERPROTECT_REGISTRY=registry.cyberprotect.ru/registry
IMAGE_NAME=k8s-backup-and-restore
IMAGE_TAG=1.0

docker pull ${CYBERPROTECT_REGISTRY}/${IMAGE_NAME}:${IMAGE_TAG}
docker save -o ${IMAGE_NAME}_${IMAGE_TAG}.tar ${CYBERPROTECT_
REGISTRY}/${IMAGE_NAME}:${IMAGE_TAG}
```

2. Разместите tar-архив на машине, на которой есть доступ к внутреннему Docker-репозиторию и на которой установлен Docker.
3. Отправьте Docker-образ во внутренний Docker-репозиторий:

```
CYBERPROTECT_REGISTRY=registry.cyberprotect.ru/registry
IMAGE_NAME=k8s-backup-and-restore
IMAGE_TAG=1.0

INTERNAL_REGISTRY=<YOUR_INTERNAL_DOCKER_REGISTRY>
INTERNAL_IMAGE_NAME=${IMAGE_NAME}
INTERNAL_IMAGE_TAG=${IMAGE_TAG}

docker image load -i ${IMAGE_NAME}_${IMAGE_TAG}.tar
docker tag ${CYBERPROTECT_REGISTRY}/${IMAGE_NAME}:${IMAGE_TAG} ${INTERNAL_
REGISTRY}/${INTERNAL_IMAGE_NAME}:${INTERNAL_IMAGE_TAG}
docker push ${INTERNAL_REGISTRY}/${INTERNAL_IMAGE_NAME}:${INTERNAL_IMAGE_
TAG}
```

4. Укажите новое имя Docker-образа в конфигурационном файле агента для Kubernetes /opt/acronis/etc/dsp.k8s/k8s-agent.json в поле cluster_config.docker_image.
5. В конфигурационном файле агента для Kubernetes укажите учетные данные для доступа во внутренний Docker-репозиторий, использовав один из следующих способов:
   - **Base64-строка с учетными данными для доступа во внутренний Docker-репозиторий**
     a. Получите строку с учетными данными в формате Base64, выполнив команду:

     ```
     kubectl create secret docker-registry regcred \
      --docker-server=<YOUR_INTERNAL_DOCKER_REGISTRY> \
      --docker-username=<YOUR_DOCKER_USER> \
      --docker-password=<YOUR_DOCKER_PASSWORD> \
      --docker-email=<YOUR_DOCKER_EMAIL> \
      --dry-run=server -o json | jq '.data.".dockerconfigjson"' -r
     ```

     b. Укажите строку из вывода команды в поле cluster_config.docker_image_pull_secret конфигурационного файла агента для Kubernetes /opt/acronis/etc/dsp.k8s/k8s-agent.json.
   - **Файл с учетными данными для доступа во внутренний Docker-репозиторий**
     a. Создайте файл с учетными данными, выполнив команду:

     ```
     kubectl create secret docker-registry regcred \
      --docker-server=<YOUR_INTERNAL_DOCKER_REGISTRY> \
      --docker-username=<YOUR_DOCKER_USER> \
     ```


© ООО Киберпротект, 2026

```
 --docker-password=<YOUR_DOCKER_PASSWORD> \
 --docker-email=<YOUR_DOCKER_EMAIL> \
 -dry-run=server -o json | jq '.data.".dockerconfigjson"' -r | base64 -d > <YOUR_DOCKER_
CREDENTIALS_FILE.json>
```

b. Разместите полученный файл с учетными данными на машине с агентом для Kubernetes.

c. Укажите путь к файлу с учетными данными в поле cluster_config.docker_image_pull_secret конфигурационного файла агента для Kubernetes /opt/acronis/etc/dsp.k8s/k8s-agent.json.

6. Перезапустите агент для Kubernetes:

```
/opt/acronis/aakore restart --unit dsp.k8s
```

12.11 Защита SAP HANA

В этом разделе описывается решение для создания согласованных резервных копий серверов с SAP HANA. Это решение позволяет восстанавливать серверы SAP HANA до состояния bare-metal, на том же или другом оборудовании, переносить их с физической машины на виртуальную и наоборот.

Кибер Бэкап использует механизм подготовки моментальных снимков SAP HANA для создания согласованных с приложениями резервных копий всего сервера SAP HANA на уровне дисков. Это решение дает следующие преимущества:

- Восстановление на "голое железо" на то же или другое оборудование с поддержкой LVM.
- Преобразование физического в виртуальное и виртуального в физическое, включая преобразование в виртуальную машину по расписанию.
- Практически мгновенное восстановление путем запуска виртуальной машины VMware ESXi из резервной копии сервера SAP HANA.

12.11.1 Поддерживаемые версии SAP HANA

Поддерживаемые версии SAP HANA указаны в разделе "Поддерживаемые СУБД" (стр. 35).

12.11.2 Резервное копирование физических серверов

12.11.2.1 Предварительные условия

- В вашей среде установлен сервер управления Кибер Бэкап. См. раздел "Установка сервера управления" (стр. 63).
- Вы можете войти на сервер управления с помощью поддерживаемого браузера. См. раздел "Веб-консоль Кибер Бэкап" (стр. 210).
- Агент Кибер Бэкап для Linux установлен на компьютере с SAP HANA и добавлен на сервер управления. См. раздел "Добавление машины с ОС Linux" (стр. 91).

© ООО Киберпротект, 2026

- Компьютеру, на котором работает SAP HANA, назначена лицензия: Расширенная редакция для физического сервера.

12.11.2.2 Установка сценариев

- Загрузите файл https://download.cyberprotect.ru/releases/AcronisDataProtection/SAP-HANA-modules.tar
- Распакуйте файл:

```
tar -xvf SAP-HANA-modules.tar
```

- Предоставьте права на исполняемый файл сценарию установки:

```
sudo chmod 777 setup.sh
```

- Запустите сценарий установки:

```
setup.sh
```

12.11.2.3 Настройка доступа к базам данных

1. Перейдите в каталог:

```
cd /usr/lib/Acronis/SAPHANA/bash/
```

2. Укажите учетные данные доступа с помощью команд, приведенных ниже.

   Пользователь, чьи учетные данные вы указываете, должен иметь права Администратора резервного копирования и права чтения каталогов в соответствующем экземпляре.

   - Чтобы добавить данные учетной записи, указав имя пользователя и пароль

     ```
     sudo ./config.sh ADD -i <instance_number> -d <database> -u <user> -p <password>
     ```

     Данные учетной записи, добавленные вами, будут сохранены в /var/lib/Acronis/SAPHANA/Config/config.yaml и будут доступны только пользователю root. Пароль будет закодирован в base64 и не зашифрован.

   - Чтобы добавить пользователя из безопасного хранилища пользователей

     ```
     sudo ./config.sh ADD -i <instance_number> -d <database> -U <key>
     ```

   - Чтобы удалить учетные данные для определенной базы данных

     ```
     ./config.sh REMOVE -i <instance_number> -d <database>
     ```

   - Чтобы просмотреть список добавленных учетных данных

     ```
     sudo ./config.sh LIST
     ```


© ООО Киберпротект, 2026

- Чтобы просмотреть учетные данные для определенной базы данных

  ```
  sudo ./config.sh GET -i <instance_number> -d <database>
  ```

3. Укажите путь установки SAP HANA:

   ```
   sudo ./config.sh SET_INSTALL_PATH --install_path <path>
   ```

   Здесь <path> – это путь к файлу sapservices, который используется в SAP HANA для отслеживания места установки баз данных. Путь по умолчанию – /usr/sap.

12.11.2.4 Создание плана резервного копирования

В соответствии с вашими требованиями к защите сервера создайте план резервного копирования для всего сервера SAP HANA, как описано в разделе "Резервное копирование" (стр. 264).

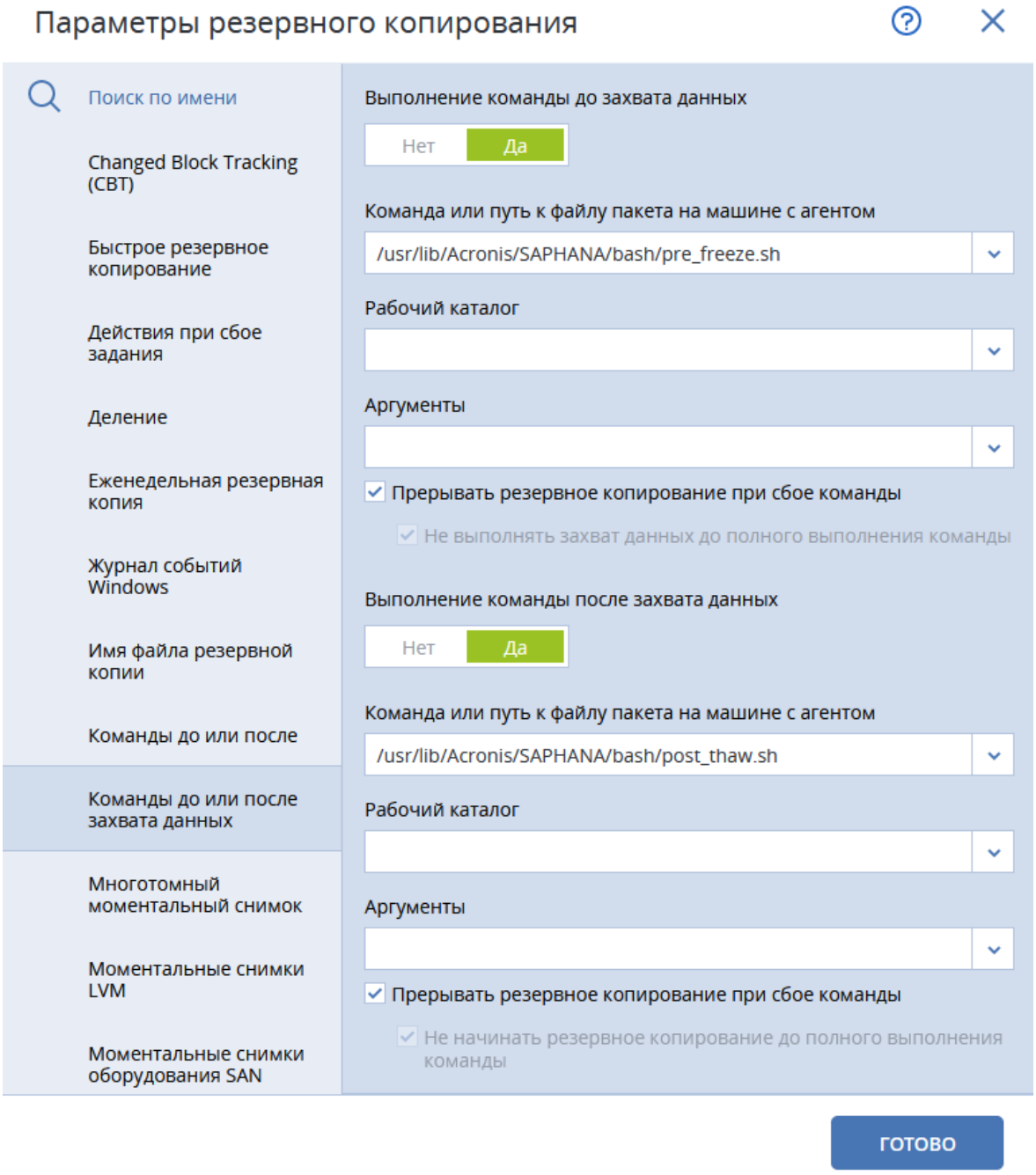
При создании плана:

1. Нажмите **Изменить** рядом с опцией **Параметры резервного копирования**, а затем выберите параметр **Команды до или после захвата данных**.
2. Активируйте переключатель **Выполнение команды до захвата данных**.
3. В поле **Команда или путь к файлу пакета на машине с агентом** введите путь к сценарию предварительного захвата данных:

   ```
   /usr/lib/Acronis/SAPHANA/bash/pre_freeze.sh
   ```

4. Активируйте переключатель **Выполнение команды после захвата данных**.
5. В поле **Команда или путь к файлу пакета на машине с агентом** введите путь к сценарию последующего захвата данных:
   -
     ```
     /usr/lib/Acronis/SAPHANA/bash/post_thaw.sh
     ```
     - если вы не хотите усекать журналы
   -
     ```
     /usr/lib/Acronis/SAPHANA/bash/post_thaw_with_truncate_logs.sh
     ```
     - если вы хотите усекать журналы после каждого резервного копирования. Этот измененный сценарий удалит журналы повторов после успешного закрытия моментального снимка.

© ООО Киберпротект, 2026



6. Выберите параметр **Многотомный моментальный снимок** и убедитесь, что он включен.
7. Нажмите **Готово**.
8. При необходимости укажите другие параметры плана резервного копирования, а затем нажмите **Создать**.

План резервного копирования будет создан и применен к вашему серверу SAP HANA. Резервные копии, созданные с помощью этого плана, будут содержать согласованную базу данных, при этом будут использоваться мощные функциональные возможности, которые предусмотрены для всех резервных копий на уровне дисков.

© ООО Киберпротект, 2026

12.11.3 Резервное копирование виртуальных серверов

12.11.3.1 Предварительные условия

- Виртуальная машина VMware ESXi работает под управлением SAP HANA и имеет установленные инструменты VMware.
- В вашей среде установлен сервер управления Кибер Бэкап. См. раздел "Установка сервера управления" (стр. 63).
- Вы можете войти на сервер управления с помощью поддерживаемого браузера. См. раздел "Веб-консоль Кибер Бэкап" (стр. 210).
- Агент Кибер Бэкап для VMware установлен в VMware vSphere или на компьютере с Windows и добавлен на сервер управления. См. раздел "Добавление vCenter или хоста ESXi" (стр. 91).
- ESXi, на котором размещена виртуальная машина под управлением SAP HANA, назначена лицензия: Расширенная редакция для физического сервера.

12.11.3.2 Дальнейшие шаги

Войдите в гостевую систему и выполните процедуры "Установка сценариев" и "Настройка доступа к базам данных", описанные в разделе "Резервное копирование физических серверов" (стр. 645).

Создайте план резервного копирования для резервного копирования всего сервера SAP HANA в соответствии с вашими требованиями к защите сервера, как описано в разделе "Резервное копирование" (стр. 264). Для виртуальных машин не нужно указывать команды предварительного и последующего сбора данных. Сценарии будут автоматически вызываться инструментами VMware каждый раз, когда требуется моментальный снимок с остановкой. Однако убедитесь, что параметр **Многотомный моментальный снимок** включен.

Чтобы включить или отключить усечение журнала, отредактируйте файл /usr/sbin/post-thaw-script. По умолчанию этот сценарий вызывает /usr/lib/Acronis/SAPHANA/bash/post_thaw.sh, что означает, что журналы не усекаются. Чтобы включить усечение, измените строку /usr/lib/Acronis/SAPHANA/bash/post_thaw.sh на /usr/lib/Acronis/SAPHANA/bash/post_thaw_with_truncate_logs.sh.

12.11.4 Восстановление всего сервера

Восстановите физический или виртуальный сервер, как описано в разделе "Восстановление машины" (стр. 384).

Если вы хотите запустить виртуальную машину VMware ESXi из резервной копии, действуйте, как описано в разделе "Запуск виртуальной машины из резервной копии (мгновенное восстановление)" (стр. 659).

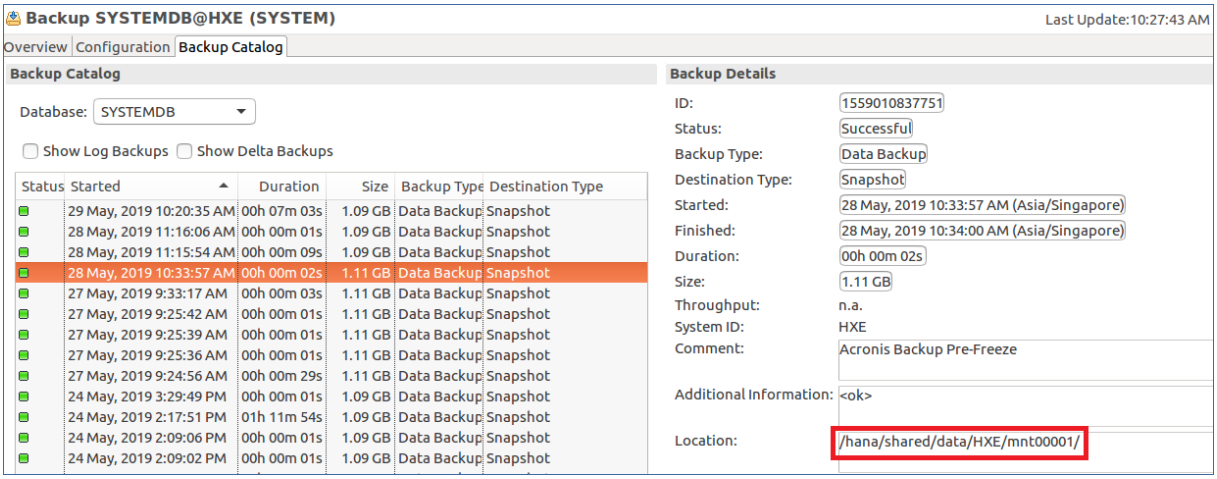
© ООО Киберпротект, 2026

12.11.5 Восстановление базы данных с помощью SAP HANA Studio

Если нет необходимости восстанавливать весь сервер, вы можете вернуть базу данных к моментальному снимку с помощью собственных инструментов SAP HANA. Ниже приведены примеры восстановления базы данных из моментальных снимков HANA, созданных во время выполнения команд предварительного сбора данных.

Эти моментальные снимки можно распознать по комментарию "Pre-Freeze" (Предварительная заморозка) в сведениях о резервном копировании, например, в каталоге резервных копий SAP HANA.

Перед началом восстановления отметьте папку, в которой находятся моментальные снимки:

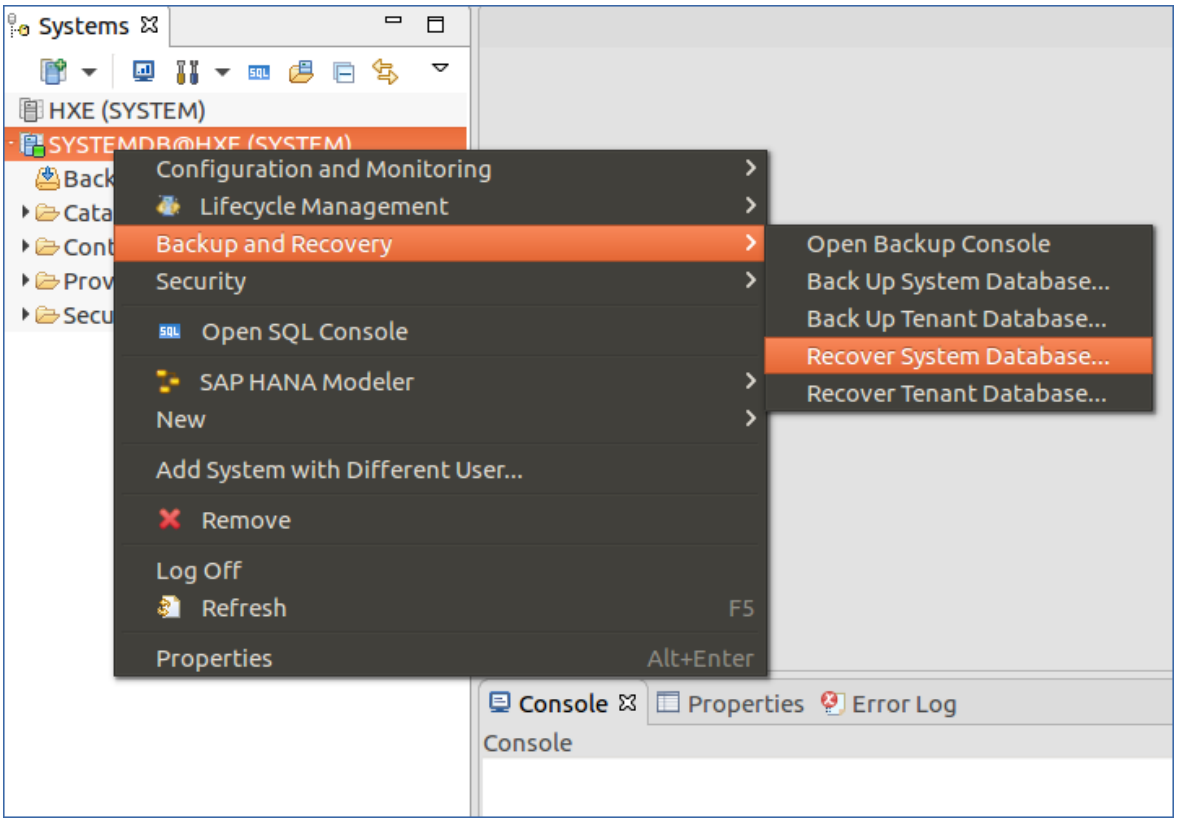


Во время восстановления мы сначала восстановим папку, содержащую моментальный снимок, а затем вернем базы данных к этому моментальному снимку с помощью SAP HANA Studio.

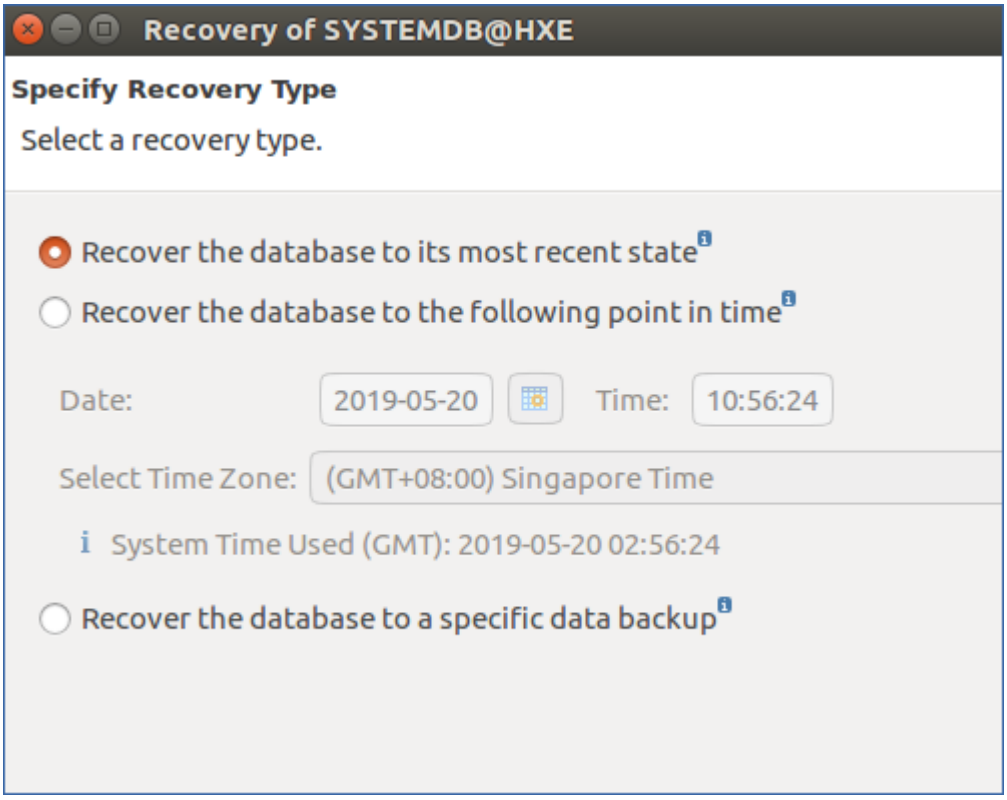
12.11.5.1 Восстановление из последней резервной копии

1. Остановите службы SAP.
   a. Откройте терминал и переключитесь на пользователя SAP HANA: su <sid>adm. Например, su hxeadm.
   b. Наберите HDB stop.
2. Восстановите папку, в которой находятся моментальные снимки из самой последней резервной копии, созданной Кибер Бэкап. Процедура восстановления описана в разделе "Восстановление файлов с помощью веб-интерфейса" (стр. 394).
3. Запустите SAP HANA Studio.
4. Щелкните правой кнопкой мыши на системной базе данных, а затем выберите **Backup and Recovery** (Резервное копирование и восстановление) > **Recover System Database...** (Восстановить системную базу данных).

© ООО Киберпротект, 2026

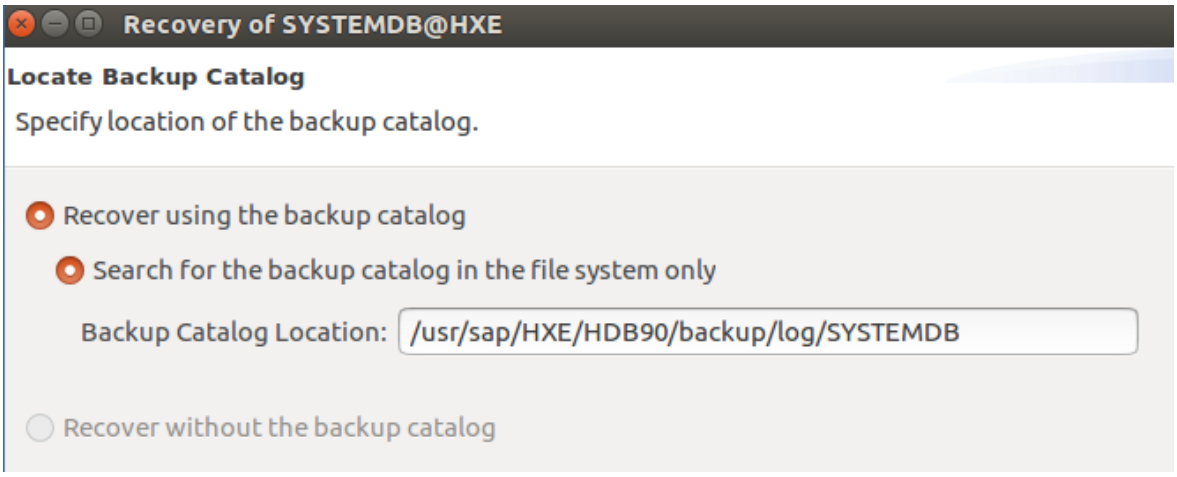


5. Выберите **Recover the database to its most recent state** (Восстановить базу данных до ее последнего состояния).

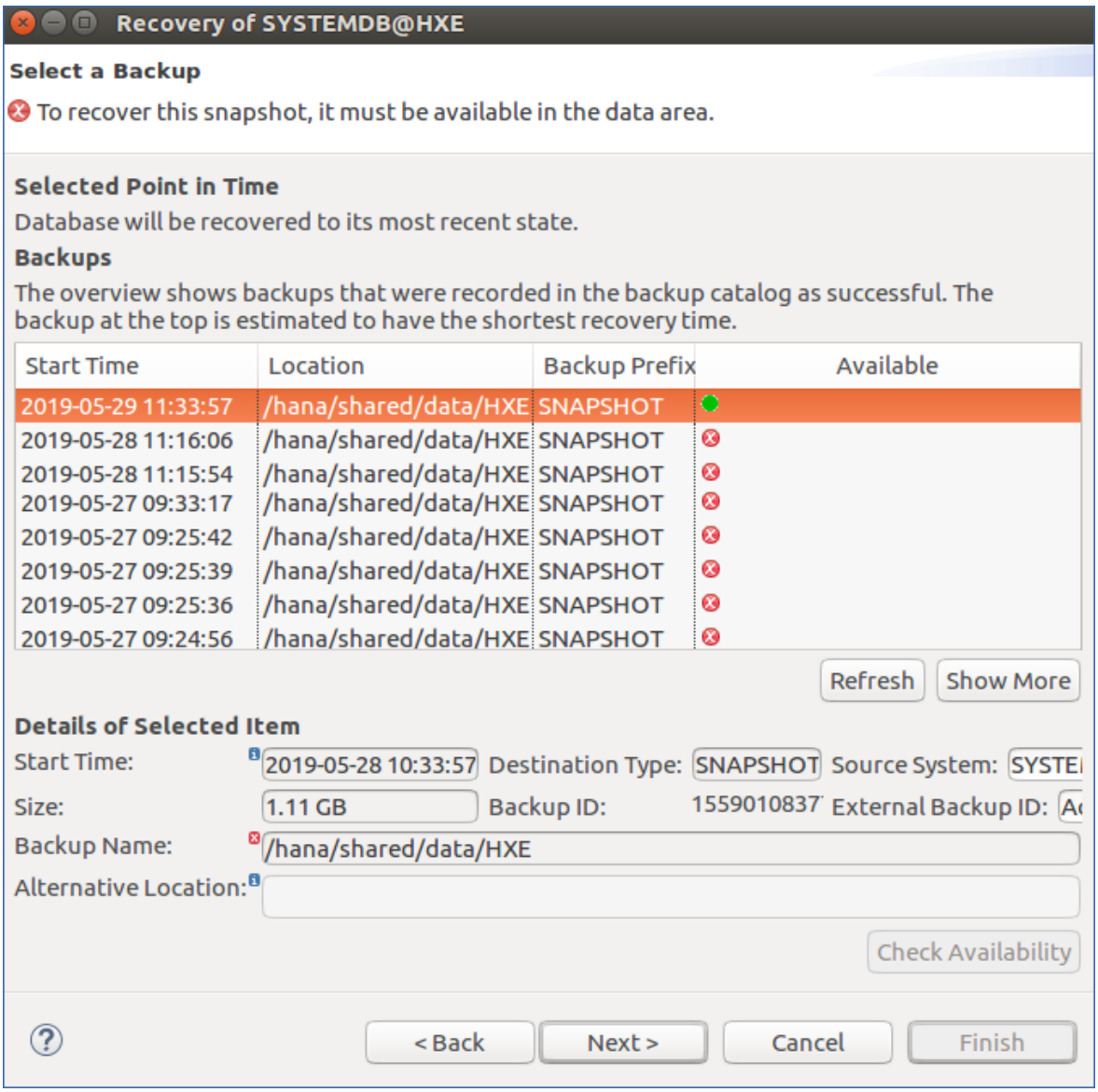


6. Проверьте путь к каталогу резервных копий и при необходимости измените его.

© ООО Киберпротект, 2026

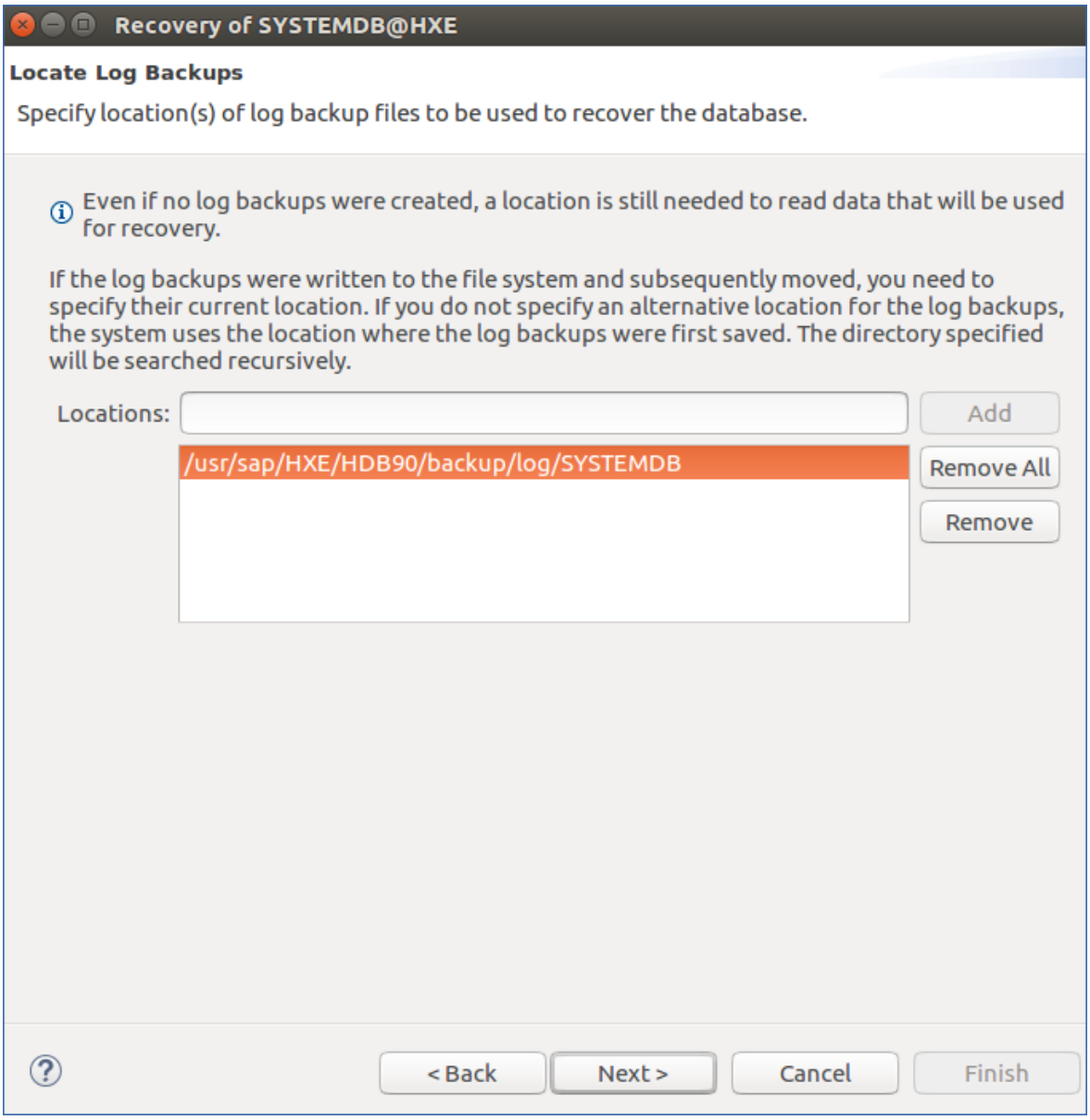


7. Последний снимок должен быть доступен, поскольку он был восстановлен на шаге 2. Если это не так, нажмите **Refresh** (Обновить).



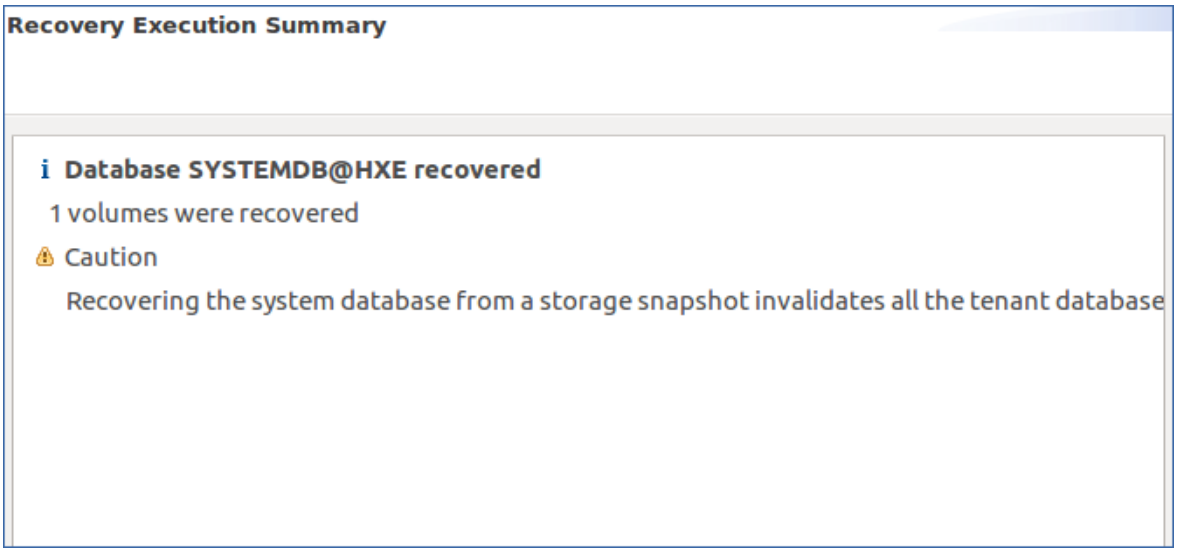
8. Проверьте путь к файлам журнала и при необходимости измените его.

© ООО Киберпротект, 2026

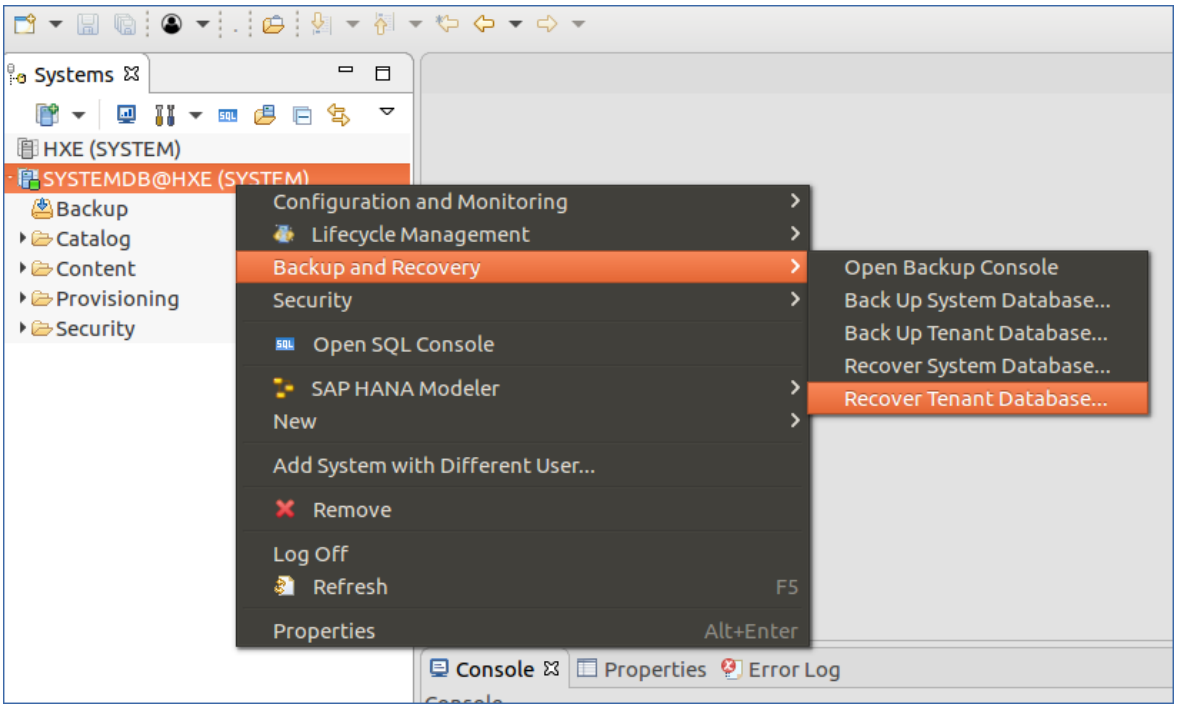


9. На шаге **Other Settings** (Прочие настройки) оставьте настройки по умолчанию и нажмите **Next** (Далее).
10. Проверьте параметры восстановления и нажмите **Finish** (Завершить). После успешного восстановления будет отображено сообщение о базе данных клиента.

© ООО Киберпротект, 2026



11. Щелкните правой кнопкой мыши по системной базе данных, а затем выберите **Backup and Recovery** (Резервное копирование и восстановление) > **Recover Tenant Database...** (Восстановить клиентскую базу данных).



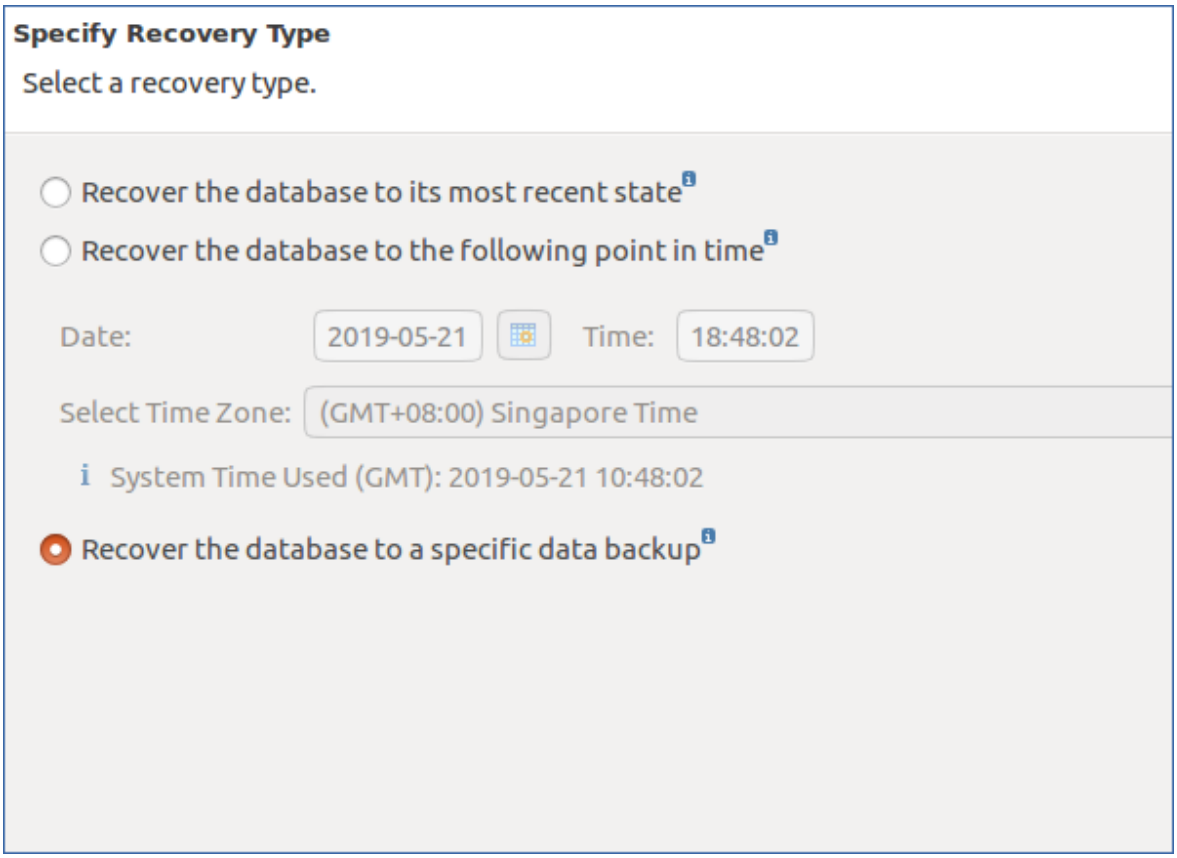
12. Повторите шаги 5-10 для клиентской базы данных.
13. После успешного восстановления откройте терминал, переключитесь на пользователя SAP HANA, а затем введите HDB start.

12.11.5.2 Восстановление из определенной резервной копии

1. Запустите SAP HANA studio и войдите в системную базу данных.

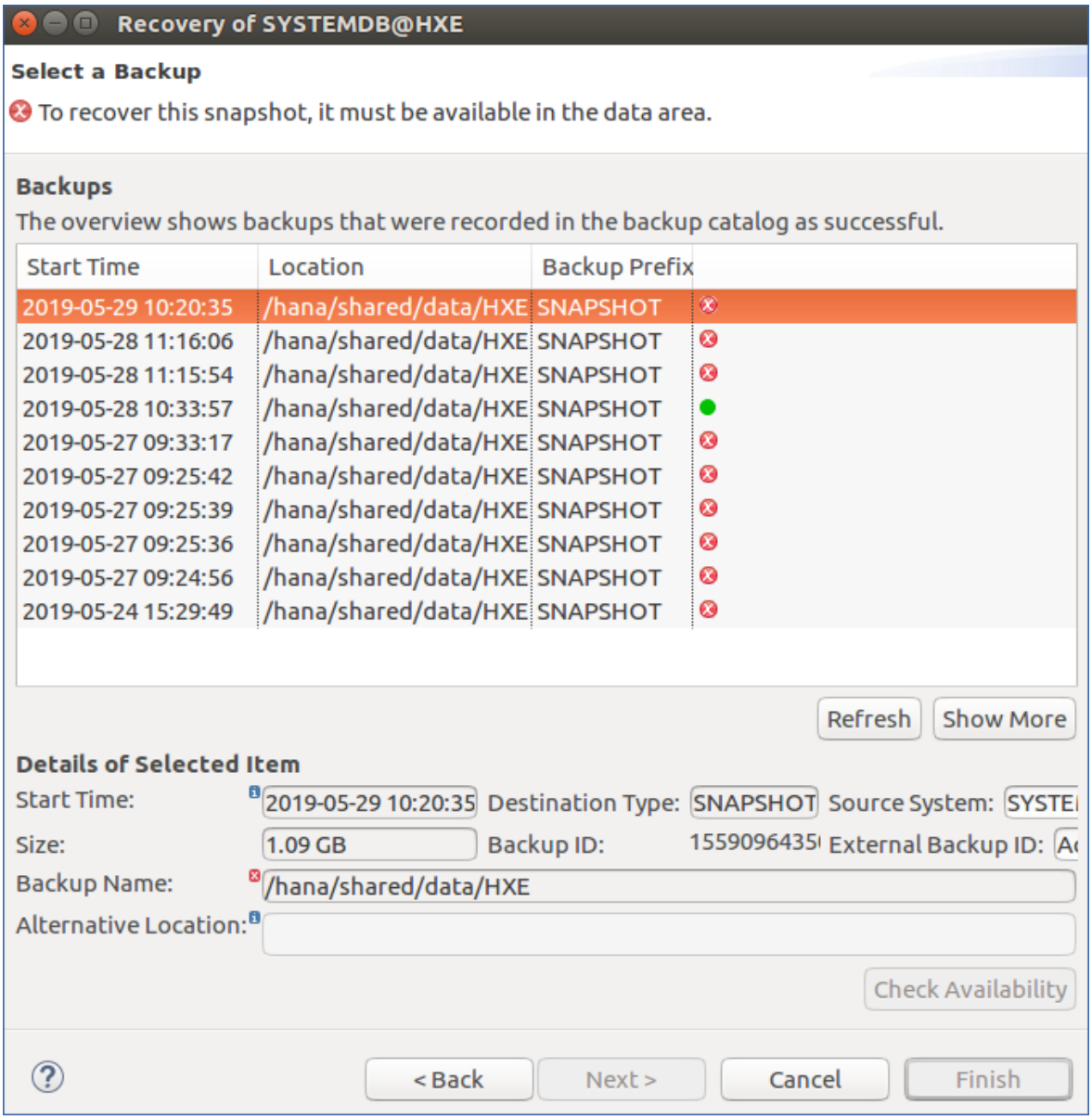
© ООО Киберпротект, 2026

2. Щелкните правой кнопкой мыши на системной базе данных, а затем выберите **Backup and Recovery** (Резервное копирование и восстановление) > **Recover System Database...** (Восстановить системную базу данных).
3. Выберите **Recover the database to a specific data backup** (Восстановить базу данных из определенной резервной копии), а затем щелкните **Next** (Далее).



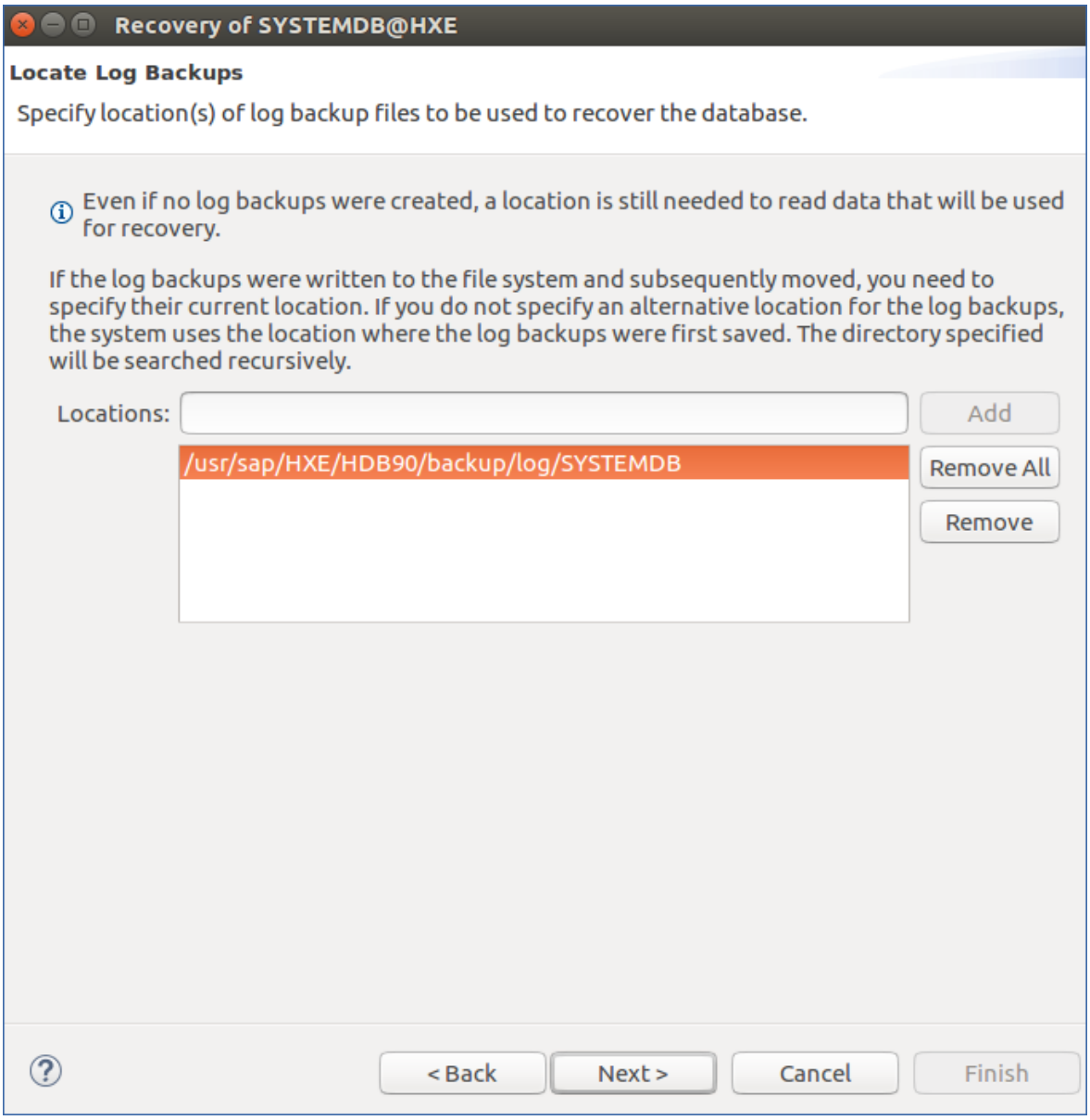
4. Выберите **Recover using the backup catalog** (Восстановить с использованием каталога резервных копий). Проверьте путь к каталогу резервных копий и при необходимости измените его.
5. В каталоге резервных копий моментальные снимки отображаются как недоступные. Выберите моментальный снимок, к которому нужно вернуть базу данных, и отметьте **Start Time** (Время начала) моментального снимка.
6. Восстановите папку, в которой находятся снимки, из резервной копии, созданной в момент, соответствующий значению **Start Time** (Время начала). Процедура восстановления описана в разделе "Восстановление файлов с помощью веб-интерфейса" (стр. 394).
7. Вернитесь в каталог резервных копий и нажмите **Refresh** (Обновить). Выбранный снимок теперь отображается как доступный. Выберите этот снимок и нажмите **Next** (Далее).

© ООО Киберпротект, 2026



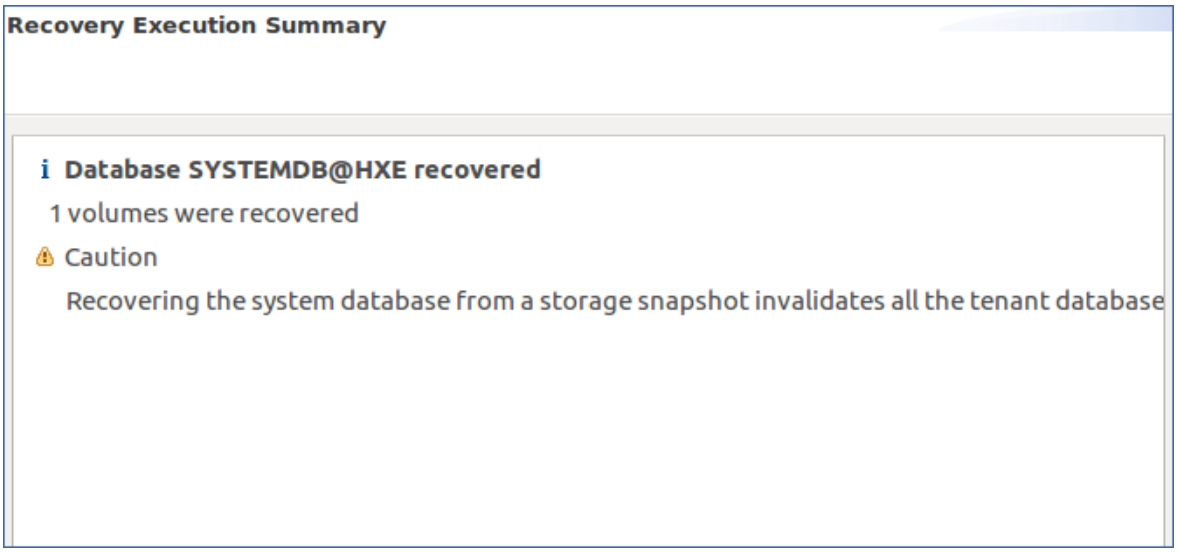
8. Проверьте путь к файлам журнала и при необходимости измените его.

© ООО Киберпротект, 2026

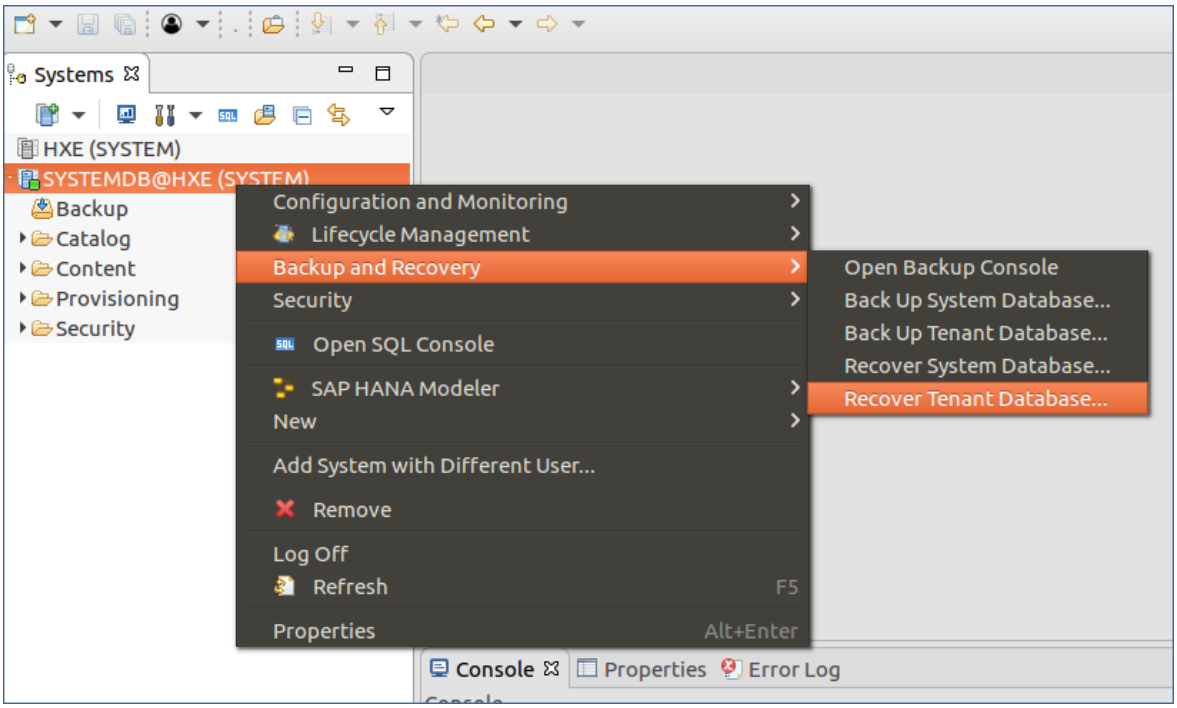


9. На шаге **Other Settings** (Прочие настройки) оставьте настройки по умолчанию и нажмите **Next** (Далее).
10. Проверьте параметры восстановления и нажмите **Finish** (Завершить). После успешного восстановления будет отображено сообщение о базе данных клиента.

© ООО Киберпротект, 2026



11. Щелкните правой кнопкой мыши по системной базе данных, а затем выберите **Backup and Recovery** (Резервное копирование и восстановление) > **Recover Tenant Database...** (Восстановить клиентскую базу данных).



12. Повторите шаги 3-4 и 7-10 для клиентской базы данных.
13. После успешного восстановления откройте терминал, переключитесь на пользователя SAP HANA, а затем введите HDB start.

© ООО Киберпротект, 2026

13 Специальные операции с виртуальными машинами

13.1 Запуск виртуальной машины из резервной копии (мгновенное восстановление)

Можно запустить виртуальную машину с резервной копии на уровне дисков, которая содержит операционную систему. Эта операция, которая также известна как мгновенное восстановление, позволяет ускорить виртуальный сервер за считанные секунды. Виртуальные диски эмулируются непосредственно с резервной копии и поэтому не занимают место в хранилище данных. Место хранения требуется только для того, чтобы сохранить изменения в виртуальных дисках.

Рекомендуем запустить эту временную виртуальную машину на срок до трех дней. После этого можно полностью удалить ее или преобразовать в обычную виртуальную машину (финализировать) без простоя.

Пока существует временная виртуальная машина, правила хранения нельзя применить к резервной копии, которая используется этой машиной. Резервные копии исходной машины могут продолжать выполняться.

13.1.1 Примеры использования

- **Аварийное восстановление**
  Мгновенное восстановление виртуальной машины, на которой произошел сбой.
- **Тестирование резервного копирования**
  Запустите машину с резервной копии и убедитесь в том, что гостевая ОС и приложения работают правильно.
- **Доступ к данным приложения**
  Когда машина запущена, воспользуйтесь встроенными инструментами управления в приложении, чтобы получить доступ к требуемым данным и извлечь их.

13.1.2 Предварительные требования

- В службе Защиты Данных необходимо зарегистрировать хотя бы один агент для VMware или агент для Hyper-V.
- Резервная копия может храниться в сетевой папке, на узле хранения или в локальной папке машины, на которой установлен агент для VMware или агент для Hyper-V. Сетевая папка должна быть доступной с данной машины. Виртуальную машину невозможно запустить из резервной копии, хранящейся на сервере SFTP, на ленточном устройстве или в зоне безопасности.
- Резервная копия должна содержать всю машину или все тома, которые необходимы для запуска операционной системы.
- Могут использоваться резервные копии физических и виртуальных машин.

© ООО Киберпротект, 2026

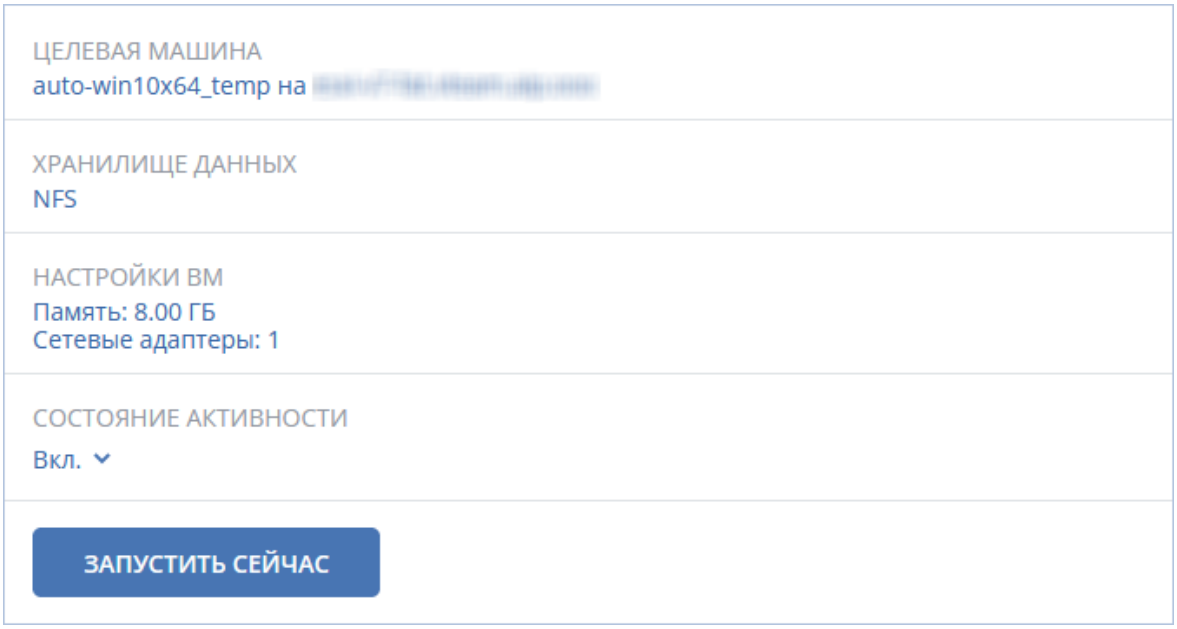
- Резервные копии с логическими томами Linux (LVM) должны создаваться агентом для VMware или агентом для Hyper-V. При этом тип виртуальной машины должен быть идентичен типу исходной машины (ESXi или Hyper-V).

Примечание
Мгновенное восстановление из резервной копии физической Linux-машины с логическими томами (LVM) не поддерживается.

13.1.3 Запуск машины

1. Выполните одно из следующих действий:
   - Выберите машину, для которой создана резервная копия, выберите **Восстановление** и выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилища резервных копий.
2. Щелкните **Запустить как ВМ**.

   Программа автоматически выберет хост и другие требуемые параметры.



3. [Необязательно] Щелкните **Целевая машина**, затем измените тип виртуальной машины (ESXi или Hyper-V), хост или имя виртуальной машины.
4. [Необязательно] Щелкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для виртуальной машины.

   Изменения, внесенные в виртуальные диски, накапливаются, пока машина запущена. Убедитесь, что в выбранном хранилище данных достаточно свободного пространства. Если вы намерены сохранить эти изменения, сделав виртуальную машину постоянной, выберите хранилище данных, подходящее для запуска машины в рабочей среде.
5. [Необязательно] Щелкните **Настройки ВМ**, чтобы изменить размер памяти и сетевые подключения виртуальной машины.

© ООО Киберпротект, 2026

6. [Необязательно] Выберите состояние активности ВМ (**Включено**/**Выключено**).
7. Щелкните **Запустить сейчас**.

В результате этого машина появляется в веб-интерфейсе с одним из следующих значков: или

. Такие виртуальные машины невозможно выбрать для резервного копирования.

13.1.4 Удаление машины

Не рекомендуется удалять временную виртуальную машину непосредственно в vSphere/Hyper-V. Это может привести к возникновению артефактов в веб-интерфейсе. Кроме того, резервная копия, с которой запускалась машина, может быть заблокирована в течении некоторого времени (невозможно будет ее удалить согласно правилам хранения).

Порядок удаления виртуальной машины, которая запущена из резервной копии

1. На вкладке **Физические и виртуальные машины** выберите машину, которая запущена из резервной копии.
2. Щелкните **Удалить**.

Машина будет удалена из веб-интерфейса. Она также удаляется из инвентаря и хранилища данных vSphere или Hyper-V. Все изменения данных, которые были внесены, когда машина была запущена, будут утрачены.

13.1.5 Финализация машины

Когда виртуальная машина запущена из резервной копии, содержимое виртуальных дисков берется непосредственно из этой резервной копии. Поэтому при утрате подключения к хранилищу резервных копий или агенту защиты машина становится недоступной или даже повреждается.

Эту машину можно сделать постоянной, то есть восстановить все ее виртуальные диски вместе с изменениями, внесенными при работе машины, в хранилище данных, в котором хранятся эти изменения. Этот процесс называется финализацией.

Финализация выполняется без простоя. При выполнении финализации виртуальная машина *не* выключается.

Расположение окончательных виртуальных жестких дисков определяется в параметрах операции Запустить как ВМ (**Хранилище данных** для ESXi или **Путь** для Hyper-V). Прежде чем запускать финализацию, убедитесь, что свободное место, возможности предоставления общего доступа и производительность этого хранилища данных позволяют запустить машину в рабочей среде.

Порядок финализации машины, которая запущена из резервной копии

1. На вкладке **Физические и виртуальные машины** выберите машину, которая запущена из резервной копии.

© ООО Киберпротект, 2026

2. Щелкните **Финализировать**.
3. [Необязательно] Укажите новое имя для данной машины.
4. [Необязательно] Измените режим распределения ресурсов диска. По умолчанию задана настройка **Экономное**.
5. Щелкните **Финализировать**.

Имя машины сразу же меняется. Ход выполнения восстановления показан на вкладке **Действия**. После выполнения восстановления значок машины меняется на значок постоянной виртуальной машины.

13.1.5.1 Полезная информация о финализации

Сравнение финализации и обычного восстановления

Процесс финализации выполняется медленнее обычного восстановления по указанным ниже причинам:

- При выполнении финализации агент в случайном порядке выбирает разные части резервной копии. При восстановлении всей машины агент считывает данные из резервной копии последовательно.
- Если при выполнении финализации запущена виртуальная машина, агент считывает данные из резервной копии более часто. Это необходимо для одновременной поддержки обоих процессов. При обычном восстановлении виртуальная машина останавливается.

13.2 Работа в VMware vSphere

В этом разделе описаны операции, характерные для среды VMware vSphere.

13.2.1 Репликация виртуальных машин

Репликация доступна только для виртуальных машин VMware ESXi.

Репликация – это процесс создания точной копии (реплики) виртуальной машины с последующей поддержкой реплики в синхронизированном состоянии с исходной машиной. Репликация критически важных машин позволяет всегда иметь копию этой машины в готовом к запуску состоянии.

Репликацию можно запустить вручную или по расписанию, которое определяется пользователем. Первая репликация является полной (выполняется копирование всей машины). Все последующие репликации являются инкрементными и выполняются с помощью функции Changed Block Tracking, если этот параметр не отключен.

13.2.1.1 Репликация и резервное копирование

В отличие от запланированных процессов резервного копирования, в реплику сохраняется только актуальное на момент создания реплики состояние. Для реплики необходимо пространство

© ООО Киберпротект, 2026

хранилища данных, а резервные копии могут храниться на более дешевых хранилищах данных.

Однако включение реплики выполняется гораздо быстрее, чем восстановление и запуск виртуальной машины из резервной копии. Включенная реплика работает быстрее виртуальной машины, запущенной из резервной копии и не загружает агент для VMware.

13.2.1.2 Примеры использования

- **Репликация виртуальных машин на удаленную площадку.**

  Репликация позволяет сохранить работоспособность при частичном или полном отказе центра обработки данных. Это возможно за счет клонирования виртуальных машин с основной площадки на вторичную площадку. Эта вторичная площадка обычно располагается на удаленном оборудовании, которое не подвергается воздействию тех факторов окружающей среды, инфраструктурных или иных факторов, которые могли привести к отказу основной площадки.
- **Репликация виртуальных машин в рамках одной площадки (с одного хоста/хранилища данных на другой хост/другое хранилище данных).**

  Репликацию на месте можно использовать в сценариях High Availability и аварийного восстановления.

13.2.1.3 Действия, которые можно выполнить с репликой

- **Проверка реплики**

  Реплика будет включена для тестирования. Чтобы проверить правильность работы реплики, воспользуйтесь клиентом vSphere или другими инструментами. При выполнении тестирования репликация приостанавливается.
- **Переход к реплике**

  Переход к реплике – это перенос рабочей нагрузки с исходной виртуальной машины на ее реплику. При выполнении перехода к реплике репликация приостанавливается.
- **Резервное копирование реплики**

  Как для резервного копирования, так и для репликации необходим доступ к виртуальным дискам. Это влияет на производительность работы хоста, на котором запущена виртуальная машина. Если необходимо иметь и реплику, и резервные копии виртуальной машины, то, чтобы не создавать дополнительную нагрузку для рабочего хоста, реплицируйте машину на другой хост и задайте резервные копии данной реплики.

13.2.1.4 Ограничения

Невозможно выполнить репликацию указанных ниже типов виртуальных машин:

- Машины, которые запущены из резервных копий.
- Реплики виртуальных машин.

© ООО Киберпротект, 2026

13.2.1.5 Создание плана репликации

План репликации необходимо создать отдельно для каждой машины. Невозможно применить существующий план к другим машинам.

Порядок создания плана репликации

1. Выберите виртуальную машину для репликации.
2. Щелкните **Репликация**.

   В программе отображается новый шаблон плана репликации.
3. [Необязательно] Чтобы изменить имя плана репликации, щелкните имя по умолчанию.
4. Щелкните **Целевая машина** и выполните указанные ниже действия:
   a. Выберите, создавать ли новую или использовать уже существующую реплику исходной машины.
   b. Выберите хост ESXi и укажите имя новой реплики или выберите существующую реплику.

      Новая реплика будет иметь имя по умолчанию **[Имя первоначальной машины]_replica**.
   c. Нажмите кнопку **OK**.
5. [Только при репликации на новую машину] Щелкните **Хранилище данных** и выберите хранилище данных для виртуальной машины.
6. [Необязательно] Щелкните **Расписание**, чтобы изменить расписание репликации.

   По умолчанию репликация выполняется ежедневно с понедельника по пятницу. Можно выбрать время для запуска репликации.

   Чтобы изменить частоту выполнения репликации, перетащите ползунок и задайте расписание.

   Можно также выполнить следующие действия:
   - Задать интервал дат, в течение которого будет использоваться указанное расписание. Установите флажок **Выполнять план в диапазоне дат** и укажите диапазон дат.
   - Отключить расписание. В этом случае репликацию можно запустить вручную.
7. [Необязательно] Щелкните значок шестерни, чтобы изменить параметры репликации.
8. Нажмите кнопку **Применить**.
9. [Необязательно] Чтобы запустить план вручную, щелкните **Запустить сейчас** на панели плана.

В результате выполнения плана репликации реплика виртуальной машины появляется в списке **Физические и виртуальные машины** с указанным ниже значком:

13.2.1.6 Тестирование реплики

Порядок подготовки реплики к тестированию

1. Выберите реплику для тестирования.
2. Щёлкните **Тестировать реплику**.

© ООО Киберпротект, 2026

3. Щёлкните **Начать тестирование**.
4. Выберите, подключить ли включённую реплику к сети. По умолчанию реплика не подключена к сети.

   Для возможности остановки тестирования реплики в блоке **Сетевое подключение** выберите **Подключить при включённом питании**. В противном случае кнопка **Остановить тестирование** будет неактивна.
5. [Необязательно] Если выбрано подключение реплики к сети, установите флажок **Остановить исходную виртуальную машину**, чтобы остановить исходную виртуальную машину до включения реплики.
6. Нажмите кнопку **Запустить**.

Порядок остановки тестирования реплики

1. Выберите реплику, для которой выполняется тестирование.
2. Щёлкните **Тестировать реплику**.
3. Щёлкните **Остановить тестирование**.
4. Подтвердите операцию.

13.2.1.7 Переход к реплике

Переход с машины к реплике

1. Выберите реплику, к которой необходимо перейти.
2. Щелкните **Действия с репликой**.
3. Щелкните **Переход к реплике**.
4. Выберите, подключить ли включенную реплику к сети. По умолчанию реплика будет подключена к той же сети, что и исходная машина.
5. [Необязательно] Если выбрано подключение реплики к сети, снимите флажок **Остановить исходную виртуальную машину**, чтобы не выключать исходную виртуальную машину.
6. Нажмите кнопку **Запустить**.

При выполнении перехода к реплике можно выбрать одно из указанных ниже действий:

- **Остановить переход к реплике**

  Остановите переход к реплике, если исходная машина исправлена. Реплика будет выключена. Репликация будет продолжена.
- **Выполнить окончательный переход на реплику**

  Эта мгновенная операция позволяет удалить флаг «реплика» из виртуальной машины, чтобы сделать репликацию невозможной. Чтобы продолжить репликацию, измените план репликации таким образом, чтобы эта машина была выбрана как исходная.
- **Возврат из реплики**

  Выполните возврат из реплики, если выполнен переход на площадку, которая не предназначена для непрерывных операций. Реплика будет восстановлена на исходную или новую виртуальную

© ООО Киберпротект, 2026

машину. По окончании восстановления на исходную машину она включается и репликация продолжается. Если выбрано восстановление на новую машину, измените план репликации таким образом, чтобы эта машина была выбрана как исходная.

Остановка перехода к реплике

Порядок остановки перехода к реплике

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Остановить переход к реплике**.
4. Подтвердите операцию.

Выполнение окончательного перехода на реплику

Порядок выполнения окончательного перехода на реплику

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Окончательный переход на реплику**.
4. [Необязательно] Измените имя виртуальной машины.
5. [Необязательно] Установите флажок **Остановить исходную виртуальную машину**.
6. Нажмите кнопку **Запустить**.

Возврат из реплики

Порядок выполнения возврата из реплики

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Возврат из реплики**.

   Данное программное обеспечение автоматически выбирает исходную машину в качестве целевой.
4. [Необязательно] Щелкните **Целевая машина** и выполните следующие действия:
   a. Выберите новую или существующую машину для возврата из реплики.
   b. Выберите хост ESXi и укажите имя новой машины или выберите существующую машину.
   c. Нажмите кнопку **OK**.
5. [Необязательно] При возврате из реплики на новую машину также можно выполнить следующие действия:
   - Щелкните **Хранилище данных**, чтобы выбрать хранилище данных для виртуальной машины.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.

© ООО Киберпротект, 2026

6. [Необязательно] Щелкните **Параметры восстановления**, чтобы изменить параметры возврата из реплики.
7. Щелкните **Запуск восстановления**.
8. Подтвердите операцию.

13.2.1.8 Параметры репликации

Чтобы изменить параметры репликации, щелкните значок шестерни рядом с именем плана репликации и нажмите кнопку **Параметры репликации**.

Функция Changed Block Tracking (CBT)

Этот параметр подобен параметру резервного копирования «Changed Block Tracking (CBT)».

Распределение ресурсов диска

Этот параметр определяет настройки распределения ресурсов диска для реплики.

Значение по умолчанию: **Экономное распределение**.

Доступны следующие значения: **Экономное распределение**, **Неэкономное распределение**, **Сохранить первоначальную настройку**.

Обработка ошибок

Этот параметр подобен параметру резервного копирования «Обработка ошибок».

Команды до и после процедуры

Этот параметр подобен параметру резервного копирования «Команды до и после процедуры».

Служба теневого копирования томов (VSS) для виртуальных машин

Этот параметр подобен параметру резервного копирования «Служба теневого копирования томов (VSS) для виртуальных машин».

13.2.1.9 Параметры возврата из реплики

Чтобы изменить параметры возврата из реплики, щелкните **Параметры восстановления** при настройке возврата из реплики.

Обработка ошибок

Этот параметр подобен параметру восстановления Обработка ошибок.

Производительность

Этот параметр подобен параметру восстановления Производительность.

© ООО Киберпротект, 2026

Команды до и после процедуры

Этот параметр подобен параметру восстановления Команды до и после процедуры.

Управление питанием ВМ

Этот параметр подобен параметру восстановления Управление питанием ВМ.

13.2.1.10 Сохранение первоначальной реплики

Чтобы ускорить репликацию в удаленное расположение и сэкономить пропускную способность сети, можно выполнить сохранение реплики.

Внимание
Для сохранения реплики агент для VMware (виртуальное устройство) должен работать на целевом хосте ESXi.

Сохранение первоначальной реплики

1. Выполните одно из следующих действий:
   - Если исходную виртуальную машину можно выключить, сделайте это, а затем перейдите к шагу 4.
   - Если исходную виртуальную машину нельзя выключить, перейдите к следующему шагу.
2. Создайте план репликации.

   При создании плана в разделе **Целевая машина** выберите пункт **Создать реплику** и хост ESXi, на котором размещена первоначальная машина.
3. Запустите план однократно.

   На исходном хосте ESXi будет создана реплика.
4. Экспортируйте файлы виртуальной машины (или реплики) на внешний жесткий диск.
   a. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.
   b. Подключите клиент vSphere к исходному хосту vCenter\ESXi.
   c. Выберите только что созданную реплику в списке.
   d. Щелкните **Файл** > **Экспорт** > **Экспорт шаблона OVF**.
   e. В поле **Папка** укажите папку на внешнем жестком диске.
   f. Нажмите кнопку **OK**.
5. Перенесите жесткий диск в удаленное расположение.
6. Импортируйте реплику на целевой хост ESXi.
   a. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.
   b. Подключите клиент vSphere к целевому хосту vCenter\ESXi.
   c. Щелкните **Файл** > **Развернуть шаблон OVF**.

© ООО Киберпротект, 2026

d. В поле **Развернуть из файла или URL-адреса** укажите шаблон, экспортированный на шаге 4.

e. Завершите процедуру импорта.

7. Измените план репликации, созданный на шаге 2. В поле **Целевая машина** выберите **Существующая реплика**, а затем выберите импортированную реплику.

В результате программа продолжит обновлять реплику. Все репликации будут инкрементными.

13.2.2 Использование локально присоединенного хранилища

К агенту для виртуального устройства VMware можно подключить дополнительный диск, чтобы агент мог создавать резервные копии в этом локальном хранилище. Этот подход устраняет сетевой трафик между агентом и хранилищем резервных копий.

Виртуальное устройство, которое выполняется на одном хосте или в одном кластере с виртуальными машинами, для которых созданы резервные копии, имеет прямой доступ к хранилищам данных, в которых расположены эти машины. Это означает, что устройство может присоединить диски, для которых созданы резервные копии, используя транспорт HotAdd. В этом случае трафик резервного копирования направляется от одного локального диска к другому. Если хранилище данных подключено как **диск/логическое устройство (LUN)**, а не как **NFS**, резервная копия будет работать без использования локальной сети. В случае хранилища данных NFS, будет иметь место сетевой трафик между хранилищем данных и хостом.

При использовании локально присоединенного хранилища предполагается, что агент всегда создает резервную копию для одних и тех же машин. Если несколько агентов работают в рамках vSphere и один или несколько из них используют локально присоединенные хранилища, необходимо вручную привязать каждый агент ко всем машинам, для которых он должен создавать резервные копии. В противном случае, если сервер управления произведет перераспределение машин среди агентов, резервные копии машин могут оказаться рассредоточенными по нескольким хранилищам.

Можно добавить хранилище к уже работающему агенту или сделать это при развертывании агента из шаблона OVF.

Как прикрепить хранилище к уже работающему агенту

1. В списке VMware vSphere щелкните правой кнопкой мыши агент для виртуального устройства VMware.
2. Добавьте диск путем внесения изменений в параметры виртуальной машины. Размер диска должен составлять по меньшей мере 10 ГБ.

   Предупреждение
   Необходимо соблюдать осторожность при добавлении уже существующего диска. После создания хранилища все данные, содержавшиеся ранее на этом диске, будут потеряны.

3. Перейдите на консоль виртуального устройства. Ссылка **Создать хранилище** доступна в нижней части экрана. Если этого не происходит, нажмите **Обновить**.

© ООО Киберпротект, 2026

4. Нажмите ссылку **Создать хранилище**, выберите диск и укажите для него метку. Длина метки ограничена 16 символами в связи с ограничениями файловой системы.

Как выбрать локально присоединенное хранилище в качестве места сохранения резервной копии

При создании плана защиты в области **Место сохранения резервной копии** выберите **Локальные папки** и введите букву диска, соответствующую локально присоединенному хранилищу, например **D:**.

13.2.3 Привязка виртуальной машины

В этом разделе показано, как сервер управления организует работу нескольких агентов в VMware vCenter.

Нижеуказанный алгоритм распределения работает как для виртуальных устройств, так и для агентов, установленных в Windows.

13.2.3.1 Алгоритм распределения

Виртуальные машины автоматически равномерно распределяются между агентами для VMware. Под равномерностью имеется в виду, что все агенты управляют равным количеством машин. Объем пространства, занимаемого в хранилище виртуальной машиной, не учитывается.

При выборе агента для машины программное обеспечение пытается оптимизировать общую производительность системы. В частности, программное обеспечение учитывает расположение агента и виртуальной машины. Предпочтительным является агент, размещенный на том же хосте. Если на том же хосте агента нет, по возможности выбирается агент из того же кластера.

Когда виртуальная машина назначается агенту, все централизованные резервные копии этой машины делегируются этому агенту.

13.2.3.2 Перераспределение

Перераспределение происходит каждый раз, когда нарушается этот баланс, или, точнее, когда дисбаланс нагрузки между агентами достигает 20 процентов. Это может произойти при добавлении или удалении машины или агента, при переносе машины на другой хост или в другой кластер или если машина привязывается к агенту вручную. В этом случае сервер управления перераспределяет машины с помощью того же алгоритма.

Например, вы понимаете, что для необходимой пропускной способности требуется больше агентов, и развертываете в кластере дополнительное виртуальное устройство. Сервер управления назначит новому агенту наиболее подходящие машины. Нагрузка на старые агенты уменьшится.

Если агент удаляется с сервера управления, то машины, назначенные этому агенту, распределяются между оставшимися агентами. Однако этого не произойдет, если агент поврежден или вручную удален из vSphere. Перераспределение начнется только после удаления такого агента из веб-интерфейса.

© ООО Киберпротект, 2026

13.2.3.3 Просмотр результата распределения

Можно просмотреть результат автоматического распределения:

- в столбце **Агент** для каждой виртуальной машины в разделе **Физические и виртуальные машины**;
- в разделе **Назначенные виртуальные машины** на панели **Сведения** при выборе агента в разделе **Настройки** > **Агенты**.

13.2.3.4 Привязка вручную

Привязка агента для VMware позволяет исключить виртуальную машину из этого процесса распределения, указав агент, который должен всегда выполнять резервное копирование этой машины. Общий баланс будет поддерживаться, но конкретная машина может быть передана другому агенту только в случае удаления исходного агента.

Порядок привязки машины к агенту

1. Выберите машину.
2. Нажмите **Сведения**.

   В разделе **Назначенные агенты** программное обеспечение отобразит агент, который в данный момент управляет выбранной машиной.
3. Нажмите **Изменить**.
4. Выберите **Вручную**.
5. Выберите агент, к которому вы хотите привязать машину.
6. Нажмите кнопку **Сохранить**.

Как отвязать машину от агента

1. Выберите машину.
2. Нажмите **Сведения**.

   В разделе **Назначенные агенты** программное обеспечение отобразит агент, который в данный момент управляет выбранной машиной.
3. Нажмите **Изменить**.
4. Выберите **Автоматически**.
5. Нажмите кнопку **Сохранить**.

13.2.3.5 Отключение автоматического назначения для агента

Для отключения автоматического назначения для агента VMware, чтобы исключить его из процесса распределения, укажите список машин, для которых этот агент должен выполнять резервное копирование. Прочие агенты будут поддерживать общий баланс.

© ООО Киберпротект, 2026

Невозможно отключить автоматическое назначение для агента при отсутствии прочих зарегистрированных агентов или при отключенном автоматическом назначении для прочих агентов.

Отключение автоматического назначения для агента

1. Щелкните **Настройки** > **Агенты**.
2. Выберите агент для VMware, для которого вы хотите отключить автоматическое назначение.
3. Нажмите **Сведения**.
4. Отключите **Автоматическое назначение**, нажав на переключатель.

13.2.3.6 Примеры использования

- Привязка вручную может быть удобна, если необходимо, чтобы агент для VMware (Windows) создал резервную копию конкретной (очень большой) машины через оптоволоконный канал, тогда как резервные копии других машин создаются виртуальными устройствами.
- Привязка вручную необходима при использовании моментальных снимков оборудования SAN. Привяжите агент для VMware (Windows), для которого сконфигурированы моментальные снимки оборудования SAN, к машинам, расположенным в хранилище данных SAN.
- Виртуальные машины необходимо привязать к агенту, если к агенту локально прикреплено хранилище.
- Отключение автоматического назначения дает возможность убедиться в том, что резервное копирование конкретной машины гарантировано будет проходить по указанному вами расписанию. Агент, отвечающий за резервное копирование только одной машины, не может быть привлечен к резервному копированию других машин в запланированное время.
- Отключение автоматического назначения полезно при наличии нескольких географически разделенных хостов ESXi. При отключении автоматического назначения и последующей привязке виртуальных машин на каждом хосте к агенту, запущенному на том же хосте вы можете быть уверены, что агент не будет выполнять резервное копирование машин, запущенных на удаленных хостах ESXi, что позволит сэкономить сетевой трафик.

13.2.4 Поддержка миграции VM

В этом разделе рассказывается об особенностях миграции виртуальных машин в среде vSphere, включая перемещение виртуальных машин между узлами ESXi, входящими в кластер vSphere.

13.2.4.1 vMotion

vMotion перемещает состояние и конфигурацию виртуальной машины на другой хост. При этом диски машины остаются в той же папке общего хранилища данных.

- Функциональная возможность vMotion агента для VMware (виртуальное устройство) не поддерживается и отключена.

© ООО Киберпротект, 2026

- Функциональная возможность vMotion виртуальной машины отключена при выполнении резервного копирования. Выполнение резервного копирования будет продолжено после завершения миграции.

13.2.4.2 Storage vMotion

Storage vMotion перемещает диски виртуальной машины из одного хранилища данных в другое.

- Функциональная возможность Storage vMotion агента для VMware (виртуальное устройство) не поддерживается и отключена.
- Функциональная возможность Storage vMotion виртуальной машины отключена при выполнении резервного копирования. Процессы резервного копирования продолжат выполняться после миграции.

13.2.5 Управление средами виртуализации

Можно просмотреть среды vSphere и Hyper-V в их собственном представлении. После установки и регистрации соответствующего агента в разделе **Устройства** появляются вкладки **VMware** или **Hyper-V**.

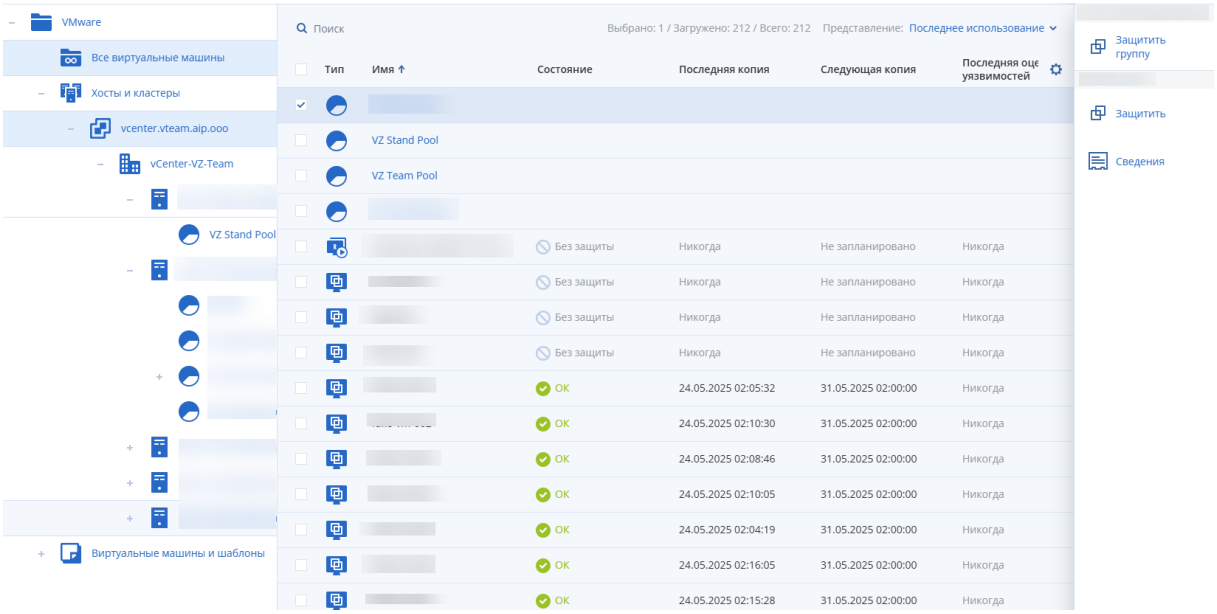
На вкладке **VMware** выполните резервное копирование следующих объектов инфраструктуры vSphere:

- Центр обработки данных
- Папка
- Кластер
- Хост ESXi
- Пул ресурсов

Каждый из этих объектов инфраструктуры работает как группа объектов для виртуальных машин. При применении плана защиты к любому из этих объектов группы создается резервная копия для всех виртуальных машин, которые входят в этот план. Можно создать резервную копию выбранных машин группы, щелкнув **Защитить**, или машин родительской группы, в которую входит выбранная группа, щелкнув **Защитить группу**.

Например, вы выбрали кластер, а затем – пул ресурсов в нем. Если щелкнуть **Защитить**, будет создана резервная копия для всех виртуальных машин в выбранном пуле ресурсов. Если щелкнуть **Защитить группу**, будет создана резервная копия для всех виртуальных машин в кластере.

© ООО Киберпротект, 2026



Можно изменить учетные данные доступа vCenter Server или автономного хоста ESXi без переустановки агента.

Изменение учетных данных доступа vCenter Server или хоста ESXi

1. В разделе **Устройства** выберите **VMware**.
2. Выберите **Хосты и кластеры**.
3. В списке **Хосты и кластеры** (справа от дерева **Хосты и кластеры**) выберите vCenter Server или автономный хост ESXi, который был указан при установке агента для VMware.
4. Нажмите **Сведения**.
5. В области **Учетные данные** выберите имя пользователя.
6. Укажите новые учетные данные для доступа, а затем щелкните **OK**.

13.2.6 Просмотр статуса резервного копирования в клиенте vSphere

Можно просмотреть статус резервного копирования и время создания последней резервной копии виртуальной машины в клиенте vSphere.

Эти сведения появляются в сводке по виртуальной машине (**Сводка** > **Настраиваемые атрибуты**/**Аннотации**/**Примечания** в зависимости от типа клиента и версии vSphere). Можно также включить столбцы **Последняя резервная копия** и **Состояние резервного копирования** на вкладке **Виртуальные машины** для любого хоста, ЦОД, папки, пула ресурсов или для всего экземпляра vCenter Server.

Для предоставления этих атрибутов, помимо прав, описанных в разделе «Агент для VMware – необходимые привилегии», агенту для VMware должны быть предоставлены следующие права:

© ООО Киберпротект, 2026

- **Глобальные** > **Управление настраиваемыми атрибутами**
- **Глобальные** > **Настройка настраиваемых атрибутов**

13.2.7 Агент для VMware: необходимые привилегии

В этом разделе описаны права, необходимые для операций с виртуальными машинами ESXi, а также для развертывания виртуальных устройств.

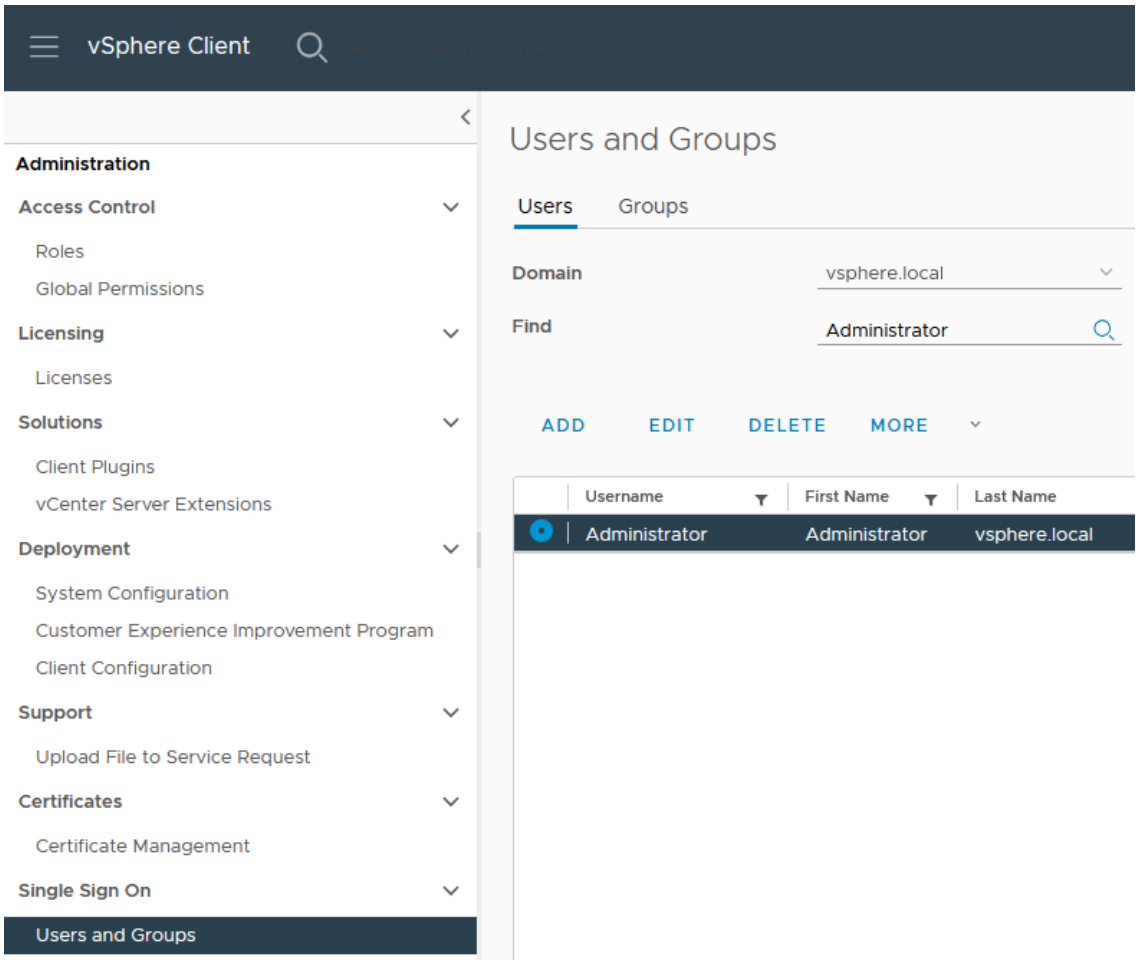
Для выполнения любой операции с объектами vCenter (например, виртуальными машинами, хостами ESXi, кластерами, хостами vCenter и т. д.) агент для VMware выполняет аутентификацию на хосте vCenter или ESXi с учетными данными vSphere, которые указаны пользователем. Учетная запись vSphere, которая используется агентом для VMware для подключения к vSphere, должна иметь необходимые права на всех уровнях инфраструктуры vSphere, начиная с уровня vCenter.

Укажите учетную запись vSphere с необходимыми правами при установке или настройке агента для VMware. Чтобы изменить учетную запись позже, см. информацию в разделе «Управление средами виртуализации».

Порядок подготовки пользователя vSphere с необходимыми правами:

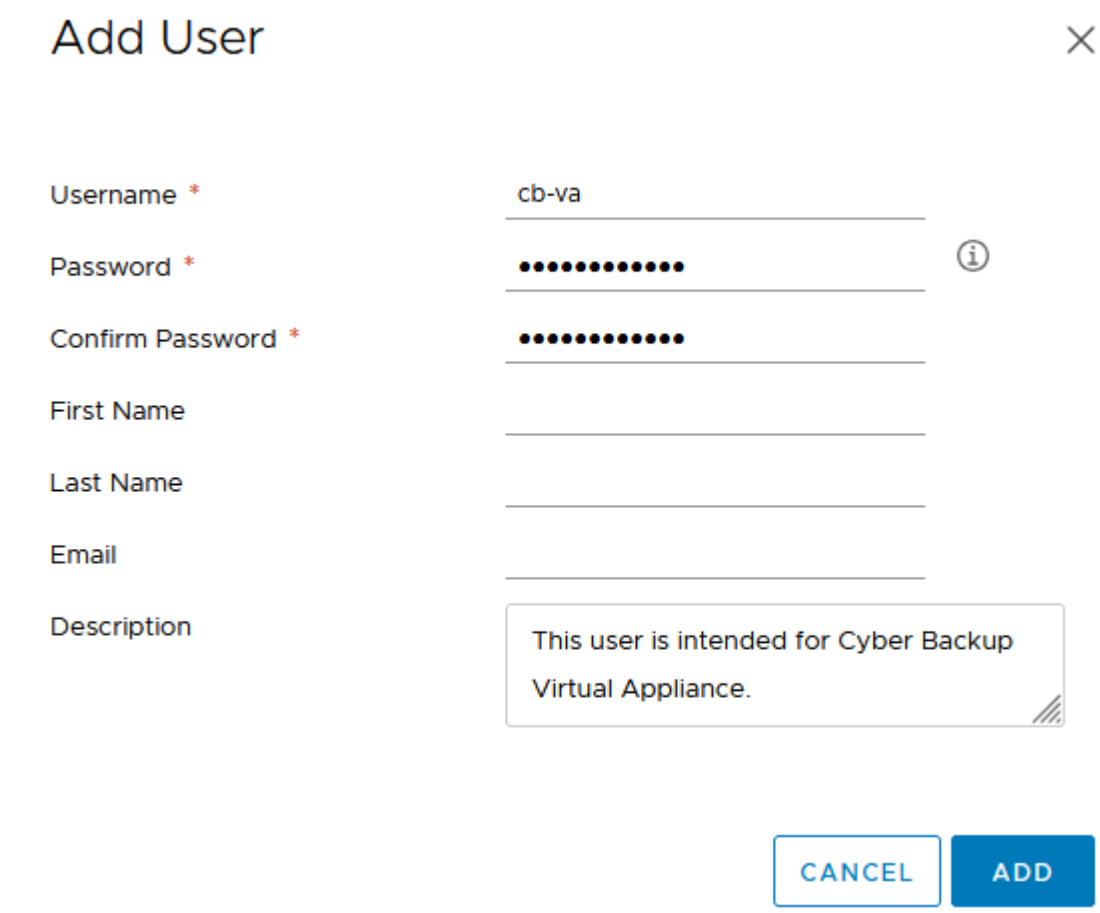
1. Подключитесь к vCenter с помощью веб-клиента vSphere, использовав учетные данные администратора.
2. Создайте пользователя:
   a. Перейдите в раздел **Administration** > **Single Sign On** > **Users and Groups** (Администрирование > Единый вход > Пользователи и группы), выберите вкладку **Users** (Пользователи) и нажмите **ADD** (ДОБАВИТЬ).

© ООО Киберпротект, 2026

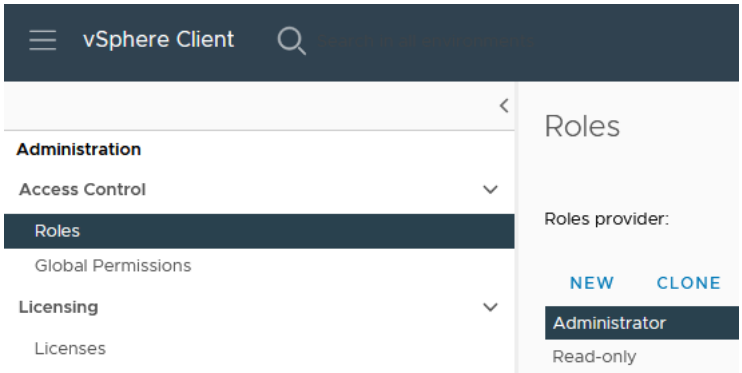


b. В окне **Add User** (Добавление пользователя) укажите имя пользователя и пароль, затем нажмите **ADD** (ДОБАВИТЬ).

© ООО Киберпротект, 2026



3. Создайте роль:
   a. Перейдите в раздел **Administration** > **Access Control** > **Roles** (Администрирование > Контроль доступа > Роли) и нажмите **NEW** (НОВАЯ).



   b. Укажите имя роли и выберите следующие привилегии:
      - **Cryptographic operations** > **Add disk** (Операции шифрования > Добавить диск (доступно начиная с vSphere 6.5)),
      - **Cryptographic operations** > **Direct Access** (Операции шифрования > Прямой доступ (доступно начиная с vSphere 6.5)),
      - **Datastore** > **Allocate space** (Хранилище данных > Распределение пространства),

© ООО Киберпротект, 2026

- **Datastore** > **Browse datastore** (Хранилище данных > Обзор хранилища данных),
- **Datastore** > **Configure datastore** (Хранилище данных > Настройка хранилища данных),
- **Datastore** > **Low level file operations** (Хранилище данных > Низкоуровневые файловые операции),
- **Global** > **Disable methods** (Глобальные > Методы отключения),
- **Global** > **Enable methods** (Глобальные > Методы включения),
- **Global** > **Licenses** (Глобальные > Лицензии),
- **Global** > **Manage custom attributes** (Глобальные > Управление настраиваемыми атрибутами),
- **Global** > **Set custom attribute** (Глобальные > Задание настраиваемых атрибутов),
- **Host** > **Configuration** > **Storage partition configuration** (Хост > Конфигурация > Конфигурация раздела хранения данных),
- **Host** > **Configuration** > **Virtual machine autostart configuration** (Хост > Конфигурация > Конфигурация автозапуска ВМ),
- **Host** > **Configuration** > **Advanced settings** (Хост > Конфигурация > Расширенные настройки),
- **Host** > **Configuration** > **Connection** (Хост > Конфигурация > Подключение),
- **Host** > **Configuration** > **System management** (Хост > Конфигурация > Управление системой),
- **Host** > **Inventory** > **Modify cluster** (Хост > Инвентарь > Изменение кластера),
- **Host** > **Local operations** > **Create virtual machine** (Хост > Локальные операции > Создание ВМ),
- **Host** > **Local operations** > **Delete virtual machine** (Хост > Локальные операции > Удаление ВМ),
- **Host** > **Local operations** > **Reconfigure virtual machine** (Хост > Локальные операции > Перенастройка ВМ),
- **Network** > **Assign network** (Сеть > Назначение сети),
- **Resource** > **Assign virtual machine to resource pool** (Ресурс > Назначение ВМ пулу ресурсов),
- **vApp** > **Add virtual machine** (vApp > Добавление виртуальной машины),
- **vApp** > **Import** (vApp > Импорт),
- **Virtual machine** > **Change configuration** > **Acquire disk lease** (Виртуальная машина > Изменение конфигурации > Аренда диска),
- **Virtual machine** > **Change configuration** > **Add existing disk** (Виртуальная машина > Изменение конфигурации > Добавление существующего диска),
- **Virtual machine** > **Change configuration** > **Add new disk** (Виртуальная машина > Изменение конфигурации > Добавление нового диска),
- **Virtual machine** > **Change configuration** > **Add or remove device** (Виртуальная машина > Изменение конфигурации > Добавление или удаление устройства),

© ООО Киберпротект, 2026

- **Virtual machine** > **Change configuration** > **Advanced configuration** (Виртуальная машина > Изменение конфигурации > Дополнительная конфигурация),
- **Virtual machine** > **Change configuration** > **Change CPU count** (Виртуальная машина > Изменение конфигурации > Изменение числа ЦП),
- **Virtual machine** > **Change configuration** > **Change Memory** (Виртуальная машина > Изменение конфигурации > Управление ОЗУ),
- **Virtual machine** > **Change configuration** > **Change Settings** (Виртуальная машина > Изменение конфигурации > Изменение настроек),
- **Virtual machine** > **Change configuration** > **Remove disk** (Виртуальная машина > Изменение конфигурации > Удаление диска),
- **Virtual machine** > **Change configuration** > **Rename** (Виртуальная машина > Изменение конфигурации > Переименование),
- **Virtual machine** > **Change configuration** > **Set annotation** (Виртуальная машина > Изменение конфигурации > Настройка аннотации),
- **Virtual machine** > **Change configuration** > **Toggle disk change tracking** (Виртуальная машина > Изменение конфигурации > Включение/выключение отслеживания изменений диска),
- **Virtual machine** > **Edit Inventory** > **Create from existing** (Виртуальная машина > Редактирование инвентаря > Создание из существующей),
- **Virtual machine** > **Edit Inventory** > **Create new** (Виртуальная машина > Редактирование инвентаря > Создание новой),
- **Virtual machine** > **Edit Inventory** > **Move** (Виртуальная машина > Редактирование инвентаря > Перемещение),
- **Virtual machine** > **Edit Inventory** > **Register** (Виртуальная машина > Редактирование инвентаря > Регистрация),
- **Virtual machine** > **Edit Inventory** > **Remove** (Виртуальная машина > Редактирование инвентаря > Удаление),
- **Virtual machine** > **Edit Inventory** > **Unregister** (Виртуальная машина > Редактирование инвентаря > Отмена регистрации),
- **Virtual machine** > **Guest operations** > **Guest operation modifications** (Виртуальная машина > Гостевые операции > Изменения гостевых операций),
- **Virtual machine** > **Guest operations** > **Guest operation program execution** (Виртуальная машина > Гостевые операции > Выполнение программы гостевой операции),
- **Virtual machine** > **Guest operations** > **Guest operation queries** (Виртуальная машина > Гостевые операции > Запросы гостевой операции),
- **Virtual machine** > **Interaction** > **Configure CD media** (Виртуальная машина > Взаимодействие > Настройка носителя CD),
- **Virtual machine** > **Interaction** > **Connect devices** (Виртуальная машина > Взаимодействие > Подключение устройств),
- **Virtual machine** > **Interaction** > **Console interaction** (Виртуальная машина > Взаимодействие > Взаимодействие с консолью),

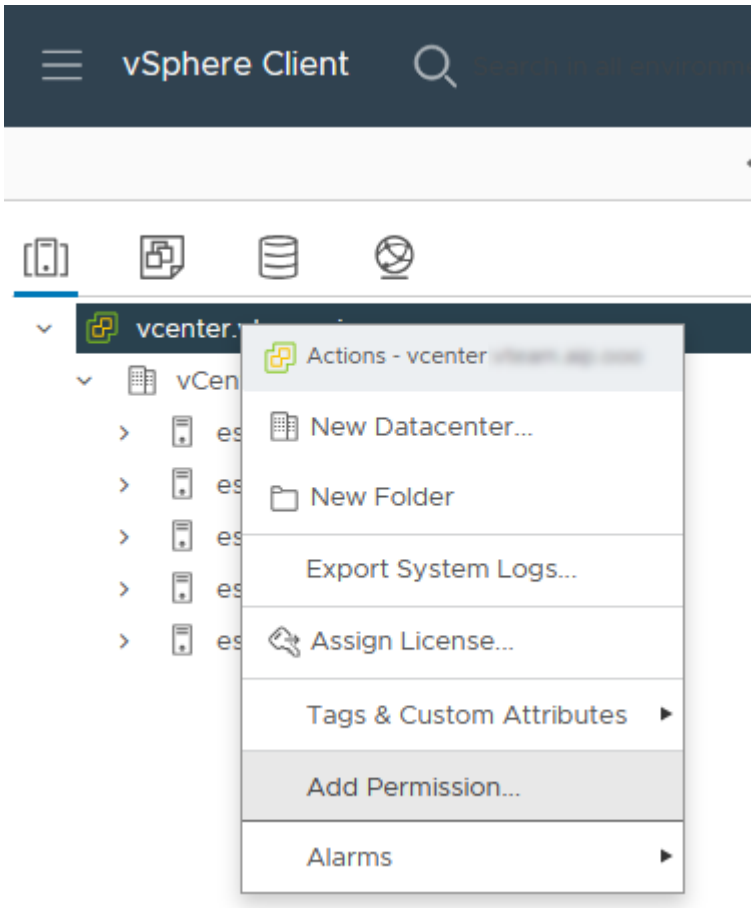
© ООО Киберпротект, 2026

- **Virtual machine** > **Interaction** > **Guest operating system management by VIX API** (Виртуальная машина > Взаимодействие > Управление гостевой операционной системой с помощью API VIX),
- **Virtual machine** > **Interaction** > **Power off** (Виртуальная машина > Взаимодействие > Отключение),
- **Virtual machine** > **Interaction** > **Power on** (Виртуальная машина > Взаимодействие > Включение),
- **Virtual machine** > **Provisioning** > **Allow disk access** (Виртуальная машина > Распределение > Разрешение доступа к диску),
- **Virtual machine** > **Provisioning** > **Allow read-only disk access** (Виртуальная машина > Распределение > Разрешение доступа к диску только для чтения),
- **Virtual machine** > **Provisioning** > **Allow virtual machine download** (Виртуальная машина > Распределение > Разрешение загрузки ВМ),
- **Virtual machine** > **Snapshot management** > **Create snapshot** (Виртуальная машина > Управление моментальными снимками > Создание моментального снимка),
- **Virtual machine** > **Snapshot management** > **Remove snapshot** (Виртуальная машина > Управление моментальными снимками > Удаление моментального снимка).

c. Нажмите **CREATE** (СОЗДАТЬ) для завершения создания роли.

4. Назначьте пользователю роль на уровне vCenter:
   a. Перейдите в раздел **Inventory** > **Hosts and Clusters** (Инвентарь > Хосты и кластеры) и щелкните правой кнопкой мыши vCenter.

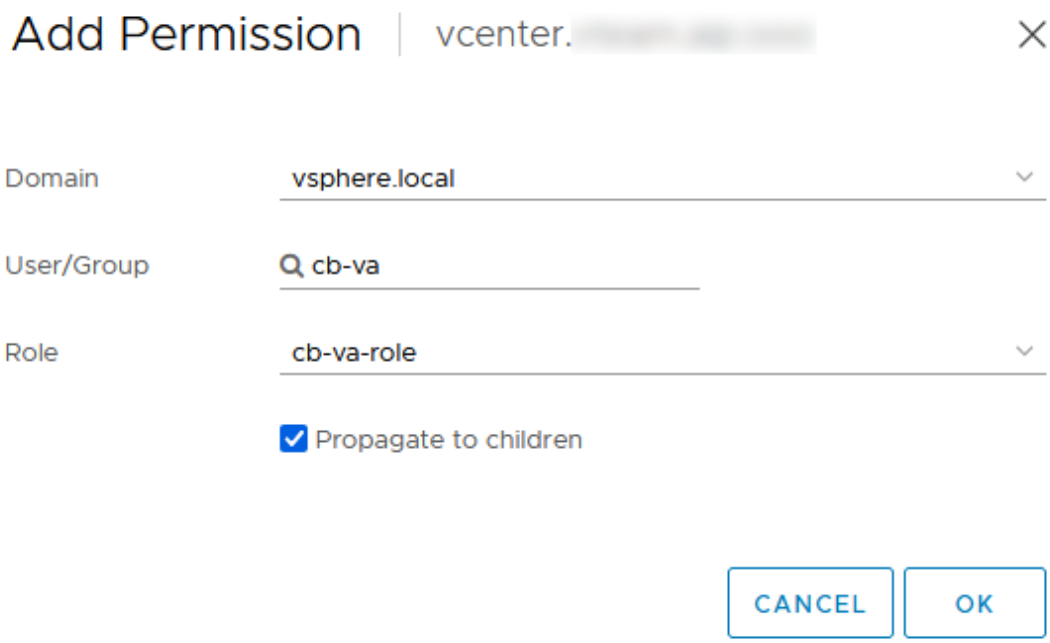
© ООО Киберпротект, 2026



b. В меню выберите **Add Permission** (Добавить право).

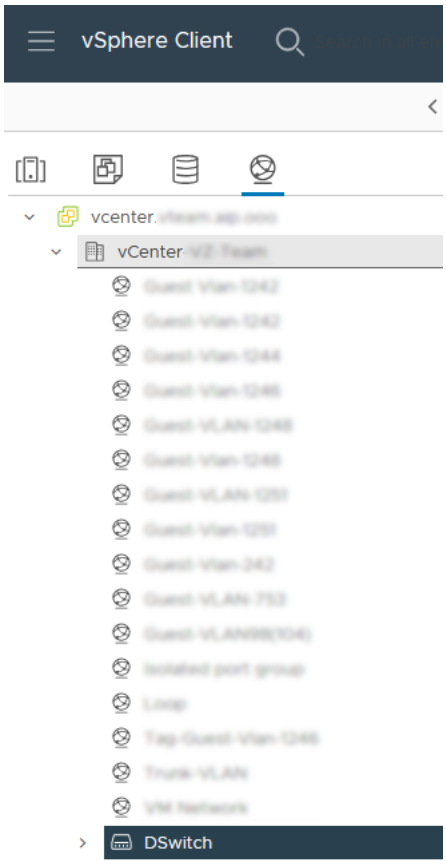
c. В окне **Add Permission** (Добавить право) выберите пользователя и роль, которые были созданы на предыдущих шагах, затем установите флажок **Propagate to children** (Распространить на дочерние элементы) и нажмите **OK**.

© ООО Киберпротект, 2026

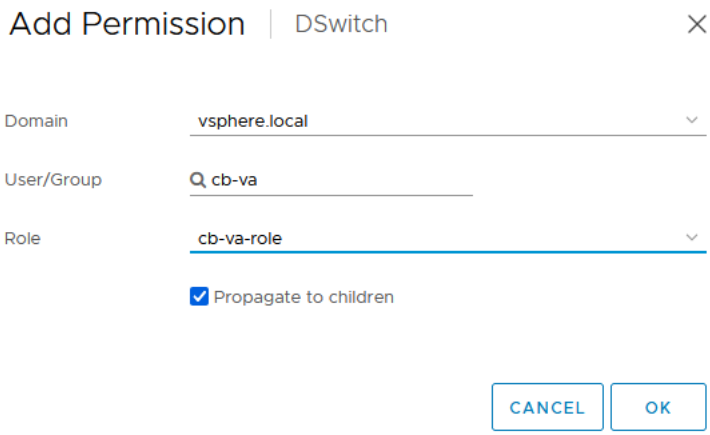


5. Назначьте пользователю роль на уровне распределенного виртуального коммутатора (dvSwitch):
   a. Перейдите в раздел **Inventory** > **Networking** (Инвентарь > Сеть) и щелкните правой кнопкой мыши распределенный виртуальный коммутатор, который будет использоваться при восстановлении в новую ВМ, затем щелкните **Add Permission** (Добавить право).

© ООО Киберпротект, 2026



b. В окне **Add Permission** (Добавить право) выберите пользователя и роль, которые были созданы на предыдущих шагах, затем установите флажок **Propagate to children** (Распространить на дочерние элементы) и нажмите **OK**.



В таблице перечислены необходимые привилегии и приведены сведения о том, как они используются.

© ООО Киберпротект, 2026

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
Cryptographic operations (Операции шифрования (доступно начиная с vSphere 6.5))	**Add disk** (Добавить диск)	+*				
	Direct Access (Прямой доступ)	+*				
Datastore (Хранилище данных)	**Allocate space** (Распределение пространства)		+	+	+	+
	Browse datastore (Обзор хранилища данных)				+	+
	Configure datastore (Настройка хранилища данных)	+	+	+	+	+
	Low level file operations (Низкоуровневые файловые операции)				+	+
Global (Глобальные)	**Licenses** (Лицензии)	+	+	+	+	
	Disable methods (Методы отключения)	+	+	+		
	Enable methods (Методы включения)	+	+	+		

© ООО Киберпротект, 2026

Объект	Привилегия	Операция				
		Резервное копирование ВМ	Восстановление в новую ВМ	Восстановление в существующую ВМ	Запуск ВМ из резервной копии	Развертывание виртуального устройства
	Manage custom attributes (Управление настраиваемыми атрибутами)	+	+	+		
	Set custom attribute (Задание настраиваемых атрибутов)	+	+	+		
Host > **Configuration** (Хост > Конфигурация)	**VM autostart configuration** (Конфигурация автозапуска ВМ)					+
	Storage partition configuration (Конфигурация раздела хранения данных)				+	
Host > **Inventory** (Хост > Инвентарь)	**Modify cluster** (Изменение кластера)					+
Host > **Local operations** (Хост > Локальные операции)	**Create VM** (Создание ВМ)				+	+
	Delete VM (Удаление ВМ)				+	+
	Reconfigure VM (Перенастройка ВМ)				+	+
Network (Сеть)	**Assign network** (Назначение сети)		+	+	+	+

© ООО Киберпротект, 2026

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
Resource (Ресурс)	**Assign VM to resource pool** (Назначение ВМ пулу ресурсов)		+	+	+	+
Virtual machine > **Change configuration** (Виртуальная машина > Изменение конфигурации)	**Add existing disk** (Добавление существующего диска)	+	+		+	
	Add new disk (Добавление нового диска)		+	+	+	+
	Add or remove device (Добавление или удаление устройства)		+		+	+
	Advanced configuration (Дополнительная конфигурация)	+	+	+		+
	Change CPU count (Изменение числа ЦП)		+			
	Toggle disk change tracking (Включение/выключение отслеживания изменений диска)	+		+		
	Acquire disk lease (Аренда диска)	+		+		

© ООО Киберпротект, 2026

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
	Change memory (Управление ОЗУ)		+			
	Remove disk (Удаление диска)	+	+	+	+	
	Rename (Переименование)		+			
	Set annotation (Настройка аннотации)				+	
	Change settings (Изменение настроек)		+	+	+	
Virtual machine > **Guest Operations** (Виртуальная машина > Гостевые операции)	**Guest Operation Program Execution** (Выполнение программы гостевой операции)	+**				+
	Guest Operation Queries (Запросы гостевой операции)	+**				+
	Guest Operation Modifications (Изменения гостевых операций)	+**				

© ООО Киберпротект, 2026

Объект	Привилегия	Операция				
		Резервное копирование ВМ	Восстановление в новую ВМ	Восстановление в существующую ВМ	Запуск ВМ из резервной копии	Развертывание виртуального устройства
Virtual machine > **Interaction** (Виртуальная машина > Взаимодействие)				+	+	
	Configure CD media (Настройка носителя CD)		+	+		
	Connect devices (Подключение устройств)		+	+		
	Console interaction (Взаимодействие с консолью)					+
	Guest operating system management by VIX API (Управление гостевой операционной системой с помощью API VIX)				+	+
	Power off (Отключение)			+	+	+
Power on (Включение)		+	+	+	+	
Virtual machine > **Edit Inventory** (Виртуальная машина >	**Create from existing** (Создание из существующей)		+	+	+	

© ООО Киберпротект, 2026

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
Редактирование инвентаря)						
	Create new (Создание новой)		+	+	+	+
	Move (Перемещение)					+
	Register (Регистрация)				+	
	Remove (Удаление)		+	+	+	+
	Unregister (Отмена регистрации)				+	
Virtual machine > **Provisioning** (Виртуальная машина > Распределение)	**Allow disk access** (Разрешение доступа к диску)		+	+	+	
	Allow read-only disk access (Разрешение доступа к диску только для чтения)	+		+		
	Allow virtual machine download (Разрешение загрузки ВМ)	+	+	+	+	
Virtual machine > **Snapshot management** (Виртуальн	**Create snapshot** (Создание моментального снимка)	+		+	+	+

© ООО Киберпротект, 2026

Объект	Привилегия	Операция				
		Резервное копирование ВМ	Восстановление в новую ВМ	Восстановление в существующую ВМ	Запуск ВМ из резервной копии	Развертывание виртуального устройства
ая машина > Управление моментальными снимками)						
	Remove snapshot (Удаление моментального снимка)	+		+	+	+
vApp	**Add virtual machine** (Добавление ВМ)				+	
	Import (Импорт)					+

* Эта привилегия требуется только для резервного копирования зашифрованных машин.

** Эта привилегия требуется только для резервных копий с поддержкой приложений.

13.2.8 Предельное количество виртуальных машин для резервного копирования

Кибер Бэкап позволяет защитить до 20 000 виртуальных машин в одной конфигурации VMware vSphere.

Для этого необходимо соблюдать следующие условия:

- Иметь особую лицензию для резервного копирования больших объемов данных.
- Установить сервер управления на машину с ОС Linux, использующую СУБД PostgreSQL (см. раздел "Сервер управления на машине с ОС Linux, использующий СУБД PostgreSQL" (стр. 51)).
- Производить резервное копирование с помощью "Группы устройств" (стр. 248). В каждой группе должно быть не более 500 виртуальных машин.
- Агент для VMware (виртуальное устройство) должен иметь как минимум 6 центральных процессоров и 16 ГБ ОЗУ.
- Использовать один агент на кластер VMware vSphere.
- Агент должен подключаться к vCenter Server с правами доступа только на свой кластер (видеть объекты только своего кластера). Подробнее см. в статье базы знаний.

© ООО Киберпротект, 2026

- При резервном копировании на ленты использовать не более 5 потоков для одного агента (см. раздел "Управление лентами" (стр. 372)).
- Производить одновременное резервное копирование не более 50 виртуальных машин (см. раздел "Ограничение общего количества виртуальных машин" (стр. 315)).
- Использовать для хранения резервных копий Кибер Инфраструктуру. Кроме того, при количестве резервных копий до 150 000, можно использовать сетевую папку.

Наибольшая производительность резервного копирования достигается при следующих конфигурациях VMware vSphere:

- не более 2 000 виртуальных машин в одном кластере;
- не более 10 кластеров;
- пропускная способность сети не менее 300 Мбит/с.

13.2.9 Одновременное восстановление

Один агент может выполнять восстановление нескольких виртуальных машин параллельно, что является реализацией многозадачности агента Кибер Бэкап (см. раздел "Агент" (стр. 266)). Одновременное восстановление позволяет повысить суммарную скорость восстановления одним агентом.

Для выполнения одновременного восстановления воспользуйтесь разделами "Виртуальная машина" (стр. 388) или "Восстановление физической машины в виртуальную" (стр. 386) и по очереди запускайте восстановление требуемых виртуальных машин. Каждый последующий запуск можно выполнять, не дожидаясь завершения предыдущего действия.

При выполнении одновременного восстановления необходимо следить за использованием агентом вычислительных ресурсов. При необходимости увеличьте количество виртуальных процессоров и памяти для агента (виртуального устройства). Нехватка вычислительных ресурсов может привести к деградации функциональности резервного копирования и восстановления (вплоть до сбоев).

13.3 Использование моментальных снимков оборудования SAN

Кибер Бэкап позволяет использовать моментальные снимки оборудования SAN при резервном копировании виртуальных машин платформ виртуализации VMware и oVirt (zVirt).

Для платформы виртуализации VMware поддерживаются следующие системы хранения данных:

- YADRO TATLIN.UNIFIED,
- NetApp,
- Huawei OceanStor (Dorado).

© ООО Киберпротект, 2026

Для платформы виртуализации oVirt (zVirt) поддерживается система хранения данных YADRO TATLIN.UNIFIED.

13.3.1 Смысл использования моментальных снимков оборудования SAN

Агенту требуются моментальные снимки виртуальных машин для выполнения согласованного резервного копирования. Агент считывает содержимое виртуального диска с моментального снимка диска, поэтому моментальный снимок должен храниться в течение всего процесса резервного копирования.

По умолчанию агент использует встроенные моментальные снимки приложения VMware, созданные хостом ESXi. Во время хранения снимка файлы виртуального диска находятся в режиме «только чтение» и хост записывает все внесенные на диск изменения в отдельные разностные файлы. После завершения процесса резервного копирования хост удаляет моментальные снимки, то есть, объединяет разностные файлы с файлами виртуального диска.

Хранение и удаление моментальных снимков влияет на производительность виртуальной машины. На виртуальных дисках большого объема с быстрым изменением данных эти операции занимают много времени и приводят к падению производительности. В исключительных случаях при одновременном проведении резервного копирования нескольких машин, возрастающий объем разностных файлов может привести к чрезмерному заполнению хранилища данных и привести к отключению всех виртуальных машин.

Вы можете снизить использование ресурсов гипервизором разгрузкой моментальных снимков в SAN. В данном случае последовательность операций будет следующей.

1. ESXi выполняет моментальный снимок VMware в начале процесса резервного копирования для согласования виртуальных дисков.
2. SAN создает моментальный снимок оборудования тома или LUN, содержащих виртуальную машину, и моментальный снимок VMware. Эта операция, как правило, займет несколько секунд.
3. ESXi удаляет моментальный снимок VMware. Агент для VMware считывает содержимое виртуального диска с моментального снимка оборудования SAN.

Моментальный снимок VMware сохраняется в течение нескольких секунд, поэтому снижение производительности виртуальной машины минимально.

13.3.2 Что необходимо для использования моментальных снимков оборудования SAN?

Для использования моментальных снимков оборудования SAN при резервном копировании виртуальных машин VMware убедитесь в выполнении следующих условий.

© ООО Киберпротект, 2026

- Установлена расширенная редакция лицензии Кибер Бэкап.
- Выполнена настройка в соответствии с описанием в разделе "Настройка хранилища данных YADRO TATLIN.UNIFIED" (стр. 693).
- Хранилище SAN NetApp соответствует требованиям, описанным в разделе "Требования для хранилища данных NetApp SAN" (стр. 699).
- Выполнена настройка в соответствии с описанием в разделе "Настройка Huawei OceanStor (Dorado)" (стр. 701).
- Машина, на которой запущен агент для VMware (Windows), сконфигурирована в соответствии с описанием в разделе "Настройка машины с агентом для VMware (Windows)" (стр. 707).
- Выполнена регистрация хранилища SAN в соответствии с описанием в разделе "Регистрация хранилища данных SAN на сервере управления" (стр. 712).
- [При наличии агентов для VMware, не принимавших участие в вышеуказанной регистрации] Виртуальные машины в хранилище SAN назначены агентам с подключенным SAN, как описано в разделе "Привязка виртуальной машины" (стр. 670).
- Параметр резервного копирования "Моментальные снимки оборудования SAN" (стр. 370) включен в плане резервного копирования.

Для использования моментальных снимков оборудования SAN при резервном копировании виртуальных машин oVirt убедитесь в выполнении следующих условий.

- Установлена расширенная редакция лицензии Кибер Бэкап.
- Выполнена настройка в соответствии с описанием в разделе "Настройка хранилища данных YADRO TATLIN.UNIFIED" (стр. 693).
- Произведена настройка машины, на которой запущен агент для oVirt, в соответствии с описанием в разделе "Настройка машины с агентом для oVirt" (стр. 714).
- Параметр резервного копирования "Моментальные снимки оборудования SAN" (стр. 370) включен в плане резервного копирования.

13.3.3 Настройка хранилища данных YADRO TATLIN.UNIFIED

Кибер Бэкап поддерживает системы хранения YADRO TATLIN.UNIFIED. В этом разделе описана настройка и подключение этих устройств к Кибер Бэкап для выполнения резервного копирования виртуальных машин в среде VMware и zVirt (oVirt) с использованием аппаратных моментальных снимков.

13.3.3.1 Поддерживаемые конфигурации

Поддерживается оборудование, имеющее интерфейс подключения с iSCSI-протоколом.

Ограничения

- Не поддерживается создание аппаратных моментальных снимков для ресурсов, включенных в группу ресурсов.

© ООО Киберпротект, 2026

- Недоступно восстановление виртуальных машин локальным агентом для oVirt для Linux; для этого используйте агент, предоставляемый в виде виртуального устройства.

Следующие ограничения приведены из расчета на одну систему хранения или из расчета на одновременное выполнение резервного копирования виртуальных машин:

- Количество виртуальных машин, для которых выполняется резервное копирование, не должно превышать 40.
- Суммарное количество дисков виртуальных машин, для которых выполняется резервное копирование, не должно превышать 40.
- Число аппаратных моментальных снимков не должно превышать 40, если для одной виртуальной машины предполагается наличие нескольких аппаратных моментальных снимков.

Следующие ограничения приведены из расчета на одного агента или из расчета на одновременное выполнение резервного копирования виртуальных машин:

- Количество виртуальных машин, для которых выполняется резервное копирование, не должно превышать 10.
- Число аппаратных моментальных снимков не должно превышать 10, если для одной виртуальной машины предполагается наличие нескольких аппаратных моментальных снимков.

13.3.3.2 Настройка

Настройка хранилища данных состоит из следующих этапов:

1. Установка агента для VMware или агента для oVirt.
2. Настройка машины с агентом.
3. Подключение LUN к хостам виртуализации.
4. Подготовка пользователя.
5. Подключение к серверу управления.

Установка агента

Примечание
Для резервного копирования моментальных снимков на уровне СХД необходимо устанавливать агенты для VMware или oVirt посредством установщика Кибер Бэкап.

Установка агента для VMware

Для установки агента для VMware обратитесь к разделу "Установка агентов в ОС Windows вручную" (стр. 95).

Установка агента для oVirt

Для установки локального агента для oVirt для Linux выполните следующие действия:

© ООО Киберпротект, 2026

1. Запустите установщик Кибер Бэкап.
2. Примите лицензионное соглашение.
3. В списке компонентов для установки отметьте флажком **Agent for Linux** (**Агент для Linux**) и **Agent for oVirt** (**Агент для oVirt**).
   Отметьте в списке **Management Server** (**Сервер управления**), если установка сервера управления выполняется на локальную машину.
4. Нажмите **Далее**.
5. Укажите при необходимости свои параметры для подключения. Если вы выбрали установку сервера управления на локальную машину, укажите порты для подключения или оставьте имеющиеся по умолчанию (рекомендуется). Если у вас уже установлен сервер управления, укажите имя или IP-адрес машины с сервером управления.
6. Нажмите **Далее**.
7. Дождитесь окончания установки.

В случае успешной установки в разделе **Устройства** появится подраздел **oVirt**.

Настройка машины с агентом

Для настройки машины с агентом для VMware выполните шаги из раздела "Настройка машины с агентом для VMware (Windows)" (стр. 707).

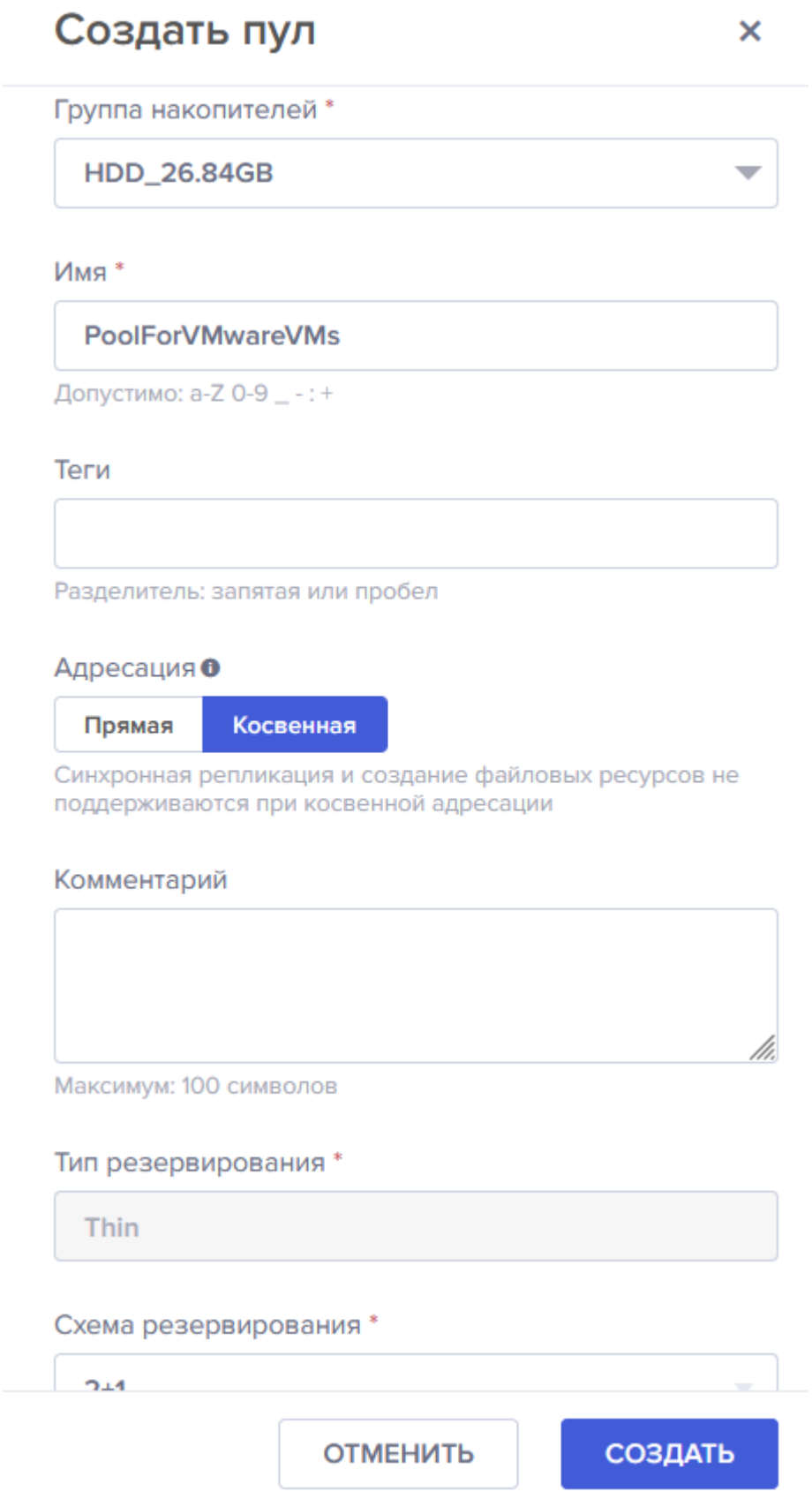
Для настройки машины с агентом для oVirt выполните шаги из раздела "Настройка машины с агентом для oVirt" (стр. 714).

© ООО Киберпротект, 2026

Создание и подключение к хостам виртуализации ресурса (LUN) для размещения дисков виртуальных машин

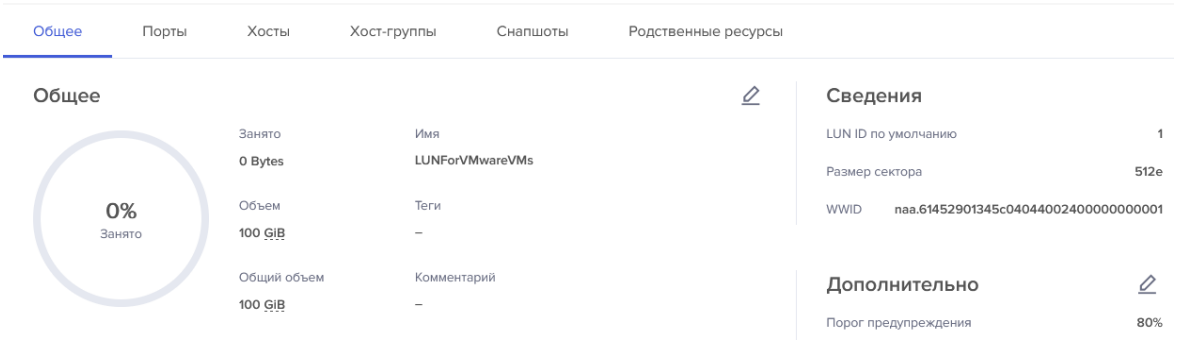
© ООО Киберпротект, 2026

1. В хранилище данных YADRO TATLIN.UNIFIED создайте пул с косвенной адресацией.



© ООО Киберпротект, 2026

2. В пуле создайте блочный ресурс (LUN) необходимого размера для размещения дисков виртуальных машин. При создании ресурса выберите размер сектора **512e** (рекомендовано для VMware).

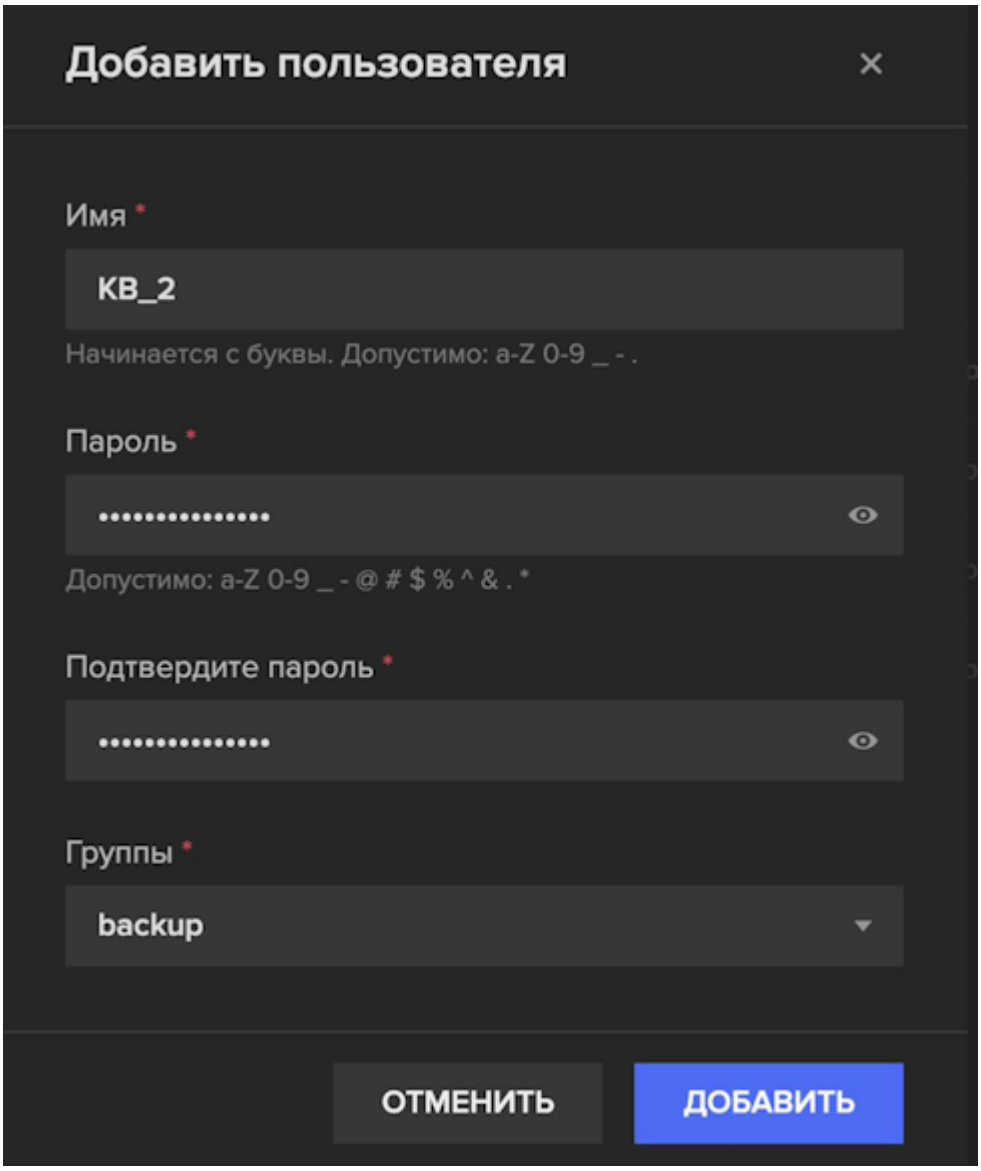


3. Подключите ресурс (LUN) по протоколу iSCSI к хостам виртуализации в качестве хранилища виртуальных дисков. Сведения о том, как выполнить подключение, см. в документации системы хранения.

Подготовка пользователя для подключения к API системы хранения данных

В системе хранения данных YADRO TATLIN.UNIFIED создайте пользователя, добавьте его в группу **backup** и сохраните его учетные данные. Эти учетные данные будут использоваться сервером управления Кибер Бэкап для подключения к API системы хранения данных.

© ООО Киберпротект, 2026



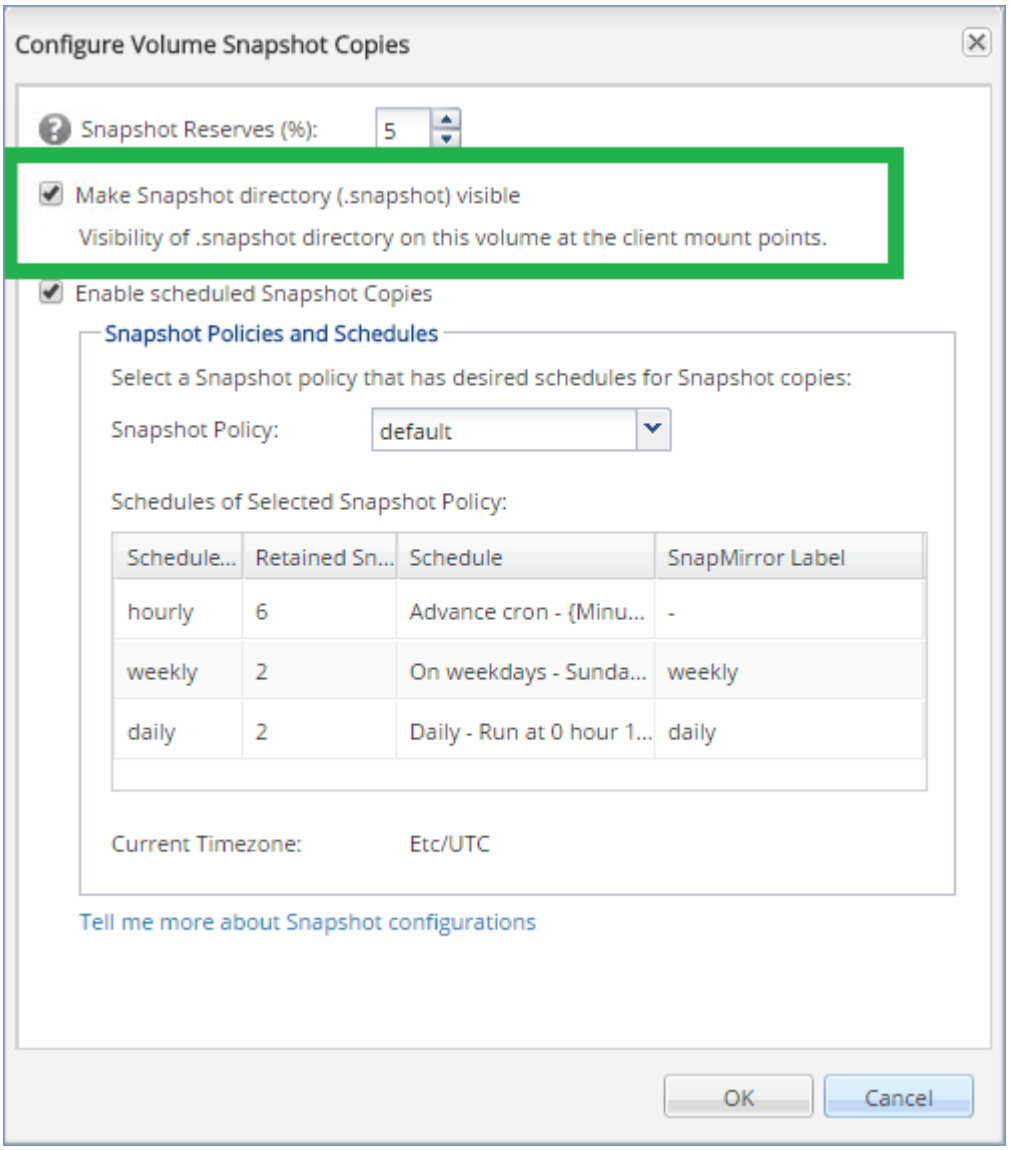
Подключение к серверу управления

Подключите систему хранения данных YADRO TATLIN.UNIFIED к серверу управления Кибер Бэкап согласно описанию в разделе "Регистрация хранилища данных SAN на сервере управления" (стр. 712).

13.3.4 Требования для хранилища данных NetApp SAN

- Хранилище SAN должно использовать хранилище данных NFS или iSCSI.
- SAN должен работать с ПО Data ONTAP версии 8.1 или более новой в режиме **Clustered Data ONTAP (cDOT)**. Режим **7-mode** не поддерживается.
- В менеджере системы NetApp OnCommand System Manager должен быть установлен флажок **Моментальные копии** > **Конфигурирование** > **Сделать видимой папку моментальных копий (.snapshot)** для тома, в котором находится хранилище данных.

© ООО Киберпротект, 2026

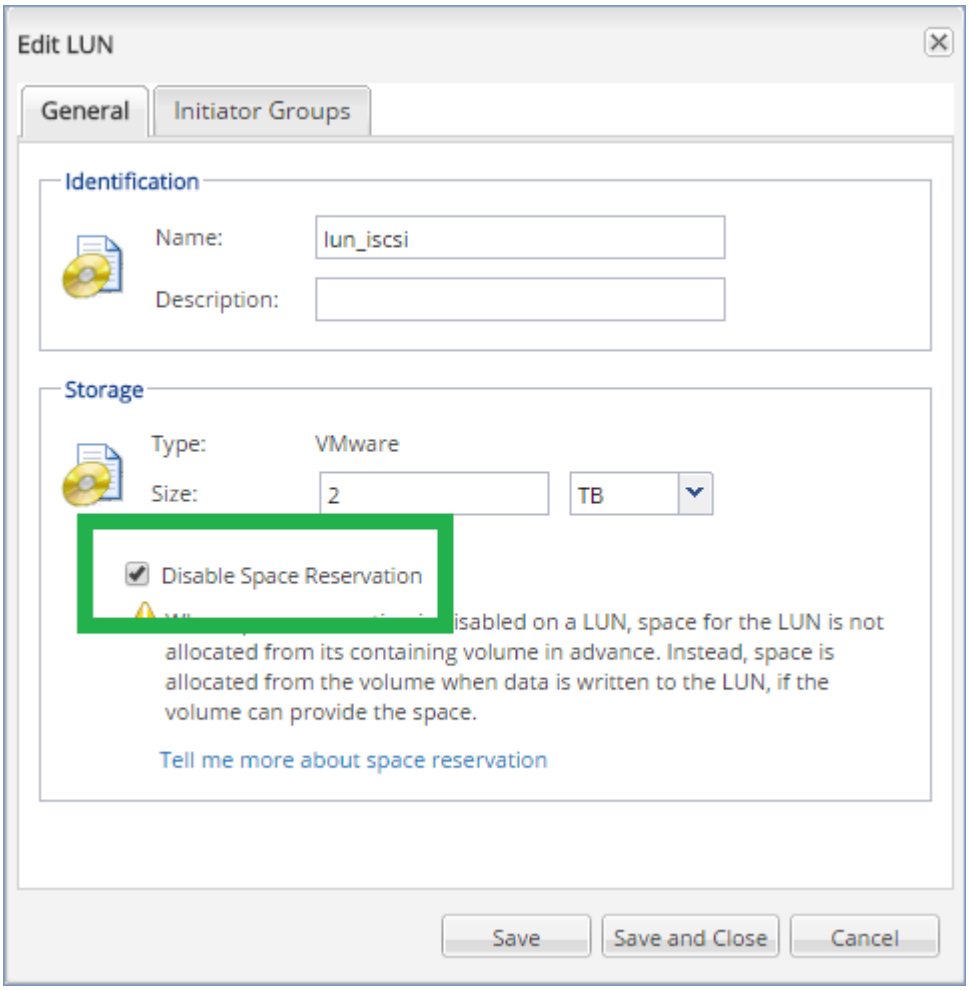


- [Для хранилищ данных NFS] На указанной при создании хранилища данных виртуальной машине должен быть разрешен доступ к общим папкам NFS для клиентов Windows NFSv3. Доступ можно разрешить посредством следующей команды:

  ```
  vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
  ```

  Дополнительные сведения см. в документе с рекомендациями NetApp: https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices
- [Для хранилищ данных iSCSI] В менеджере системы NetApp OnCommand должен быть установлен флажок **Отключить резервирование пространства** для iSCSI LUN, в котором находится хранилище данных.

© ООО Киберпротект, 2026



13.3.5 Настройка Huawei OceanStor (Dorado)

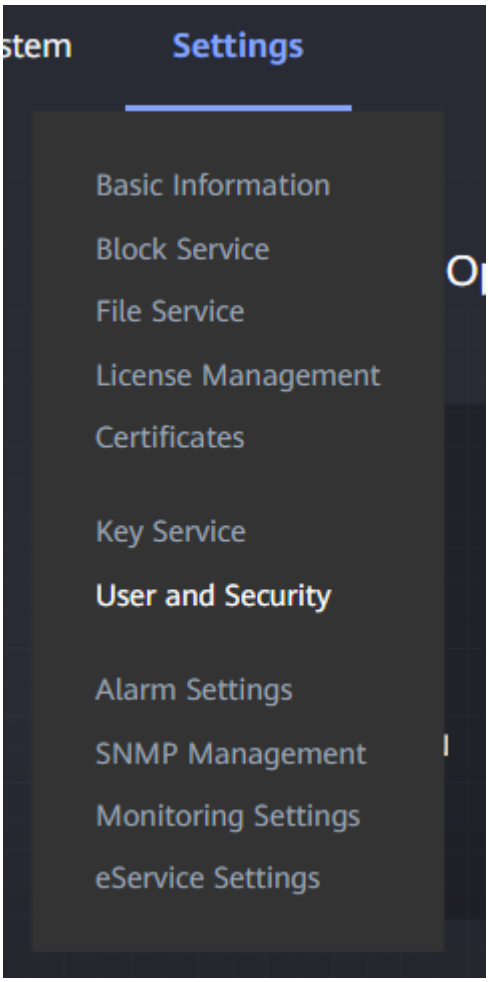
Кибер Бэкап поддерживает системы хранения семейства Huawei OceanStor (Dorado). В этом разделе описана настройка и подключение этих устройств к Кибер Бэкап для создания аппаратных моментальных снимков в среде VMware.

13.3.5.1 Настройка пользователя в Dorado

Для настройки пользователя в Dorado выполните следующие действия:

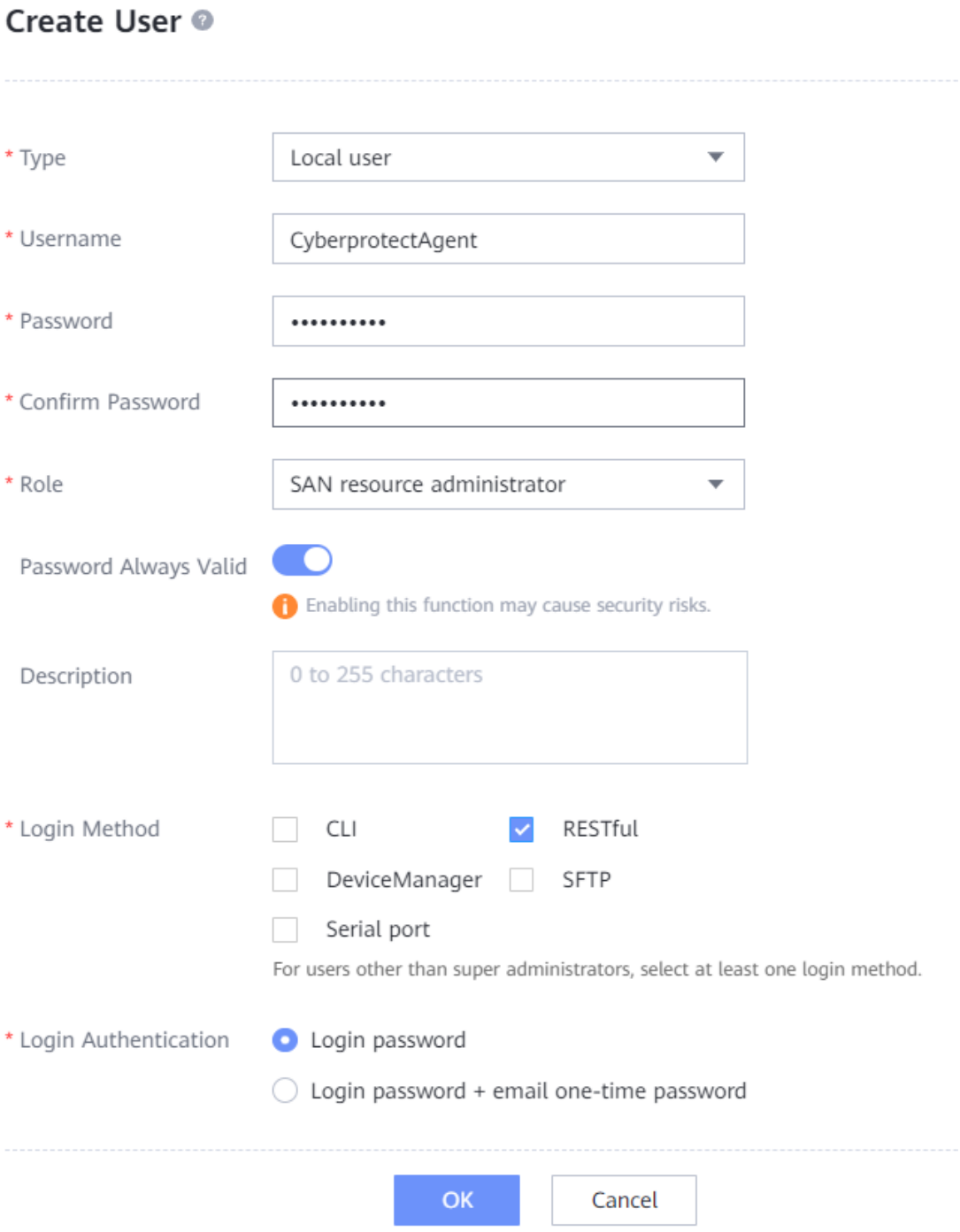
- В настройках **План резервного копирования** укажите параметр **SAN hardware snapshot**: **yes**.
- На вкладке **Settings** перейдите в раздел **User and Security** и нажмите **Create User**.

© ООО Киберпротект, 2026

- 

- Заполните поля как показано далее:

© ООО Киберпротект, 2026



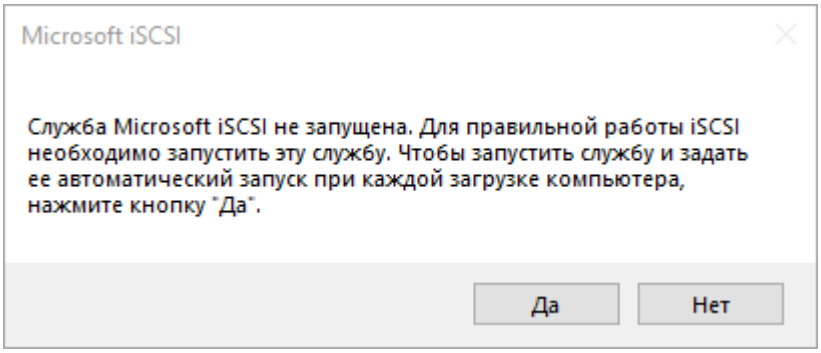
- В поле **Role** укажите одну из двух следующих ролей (встроенных групп):
  - Administrator
  - Super administrator
- По окончании ввода данных нажмите **OK**.

© ООО Киберпротект, 2026

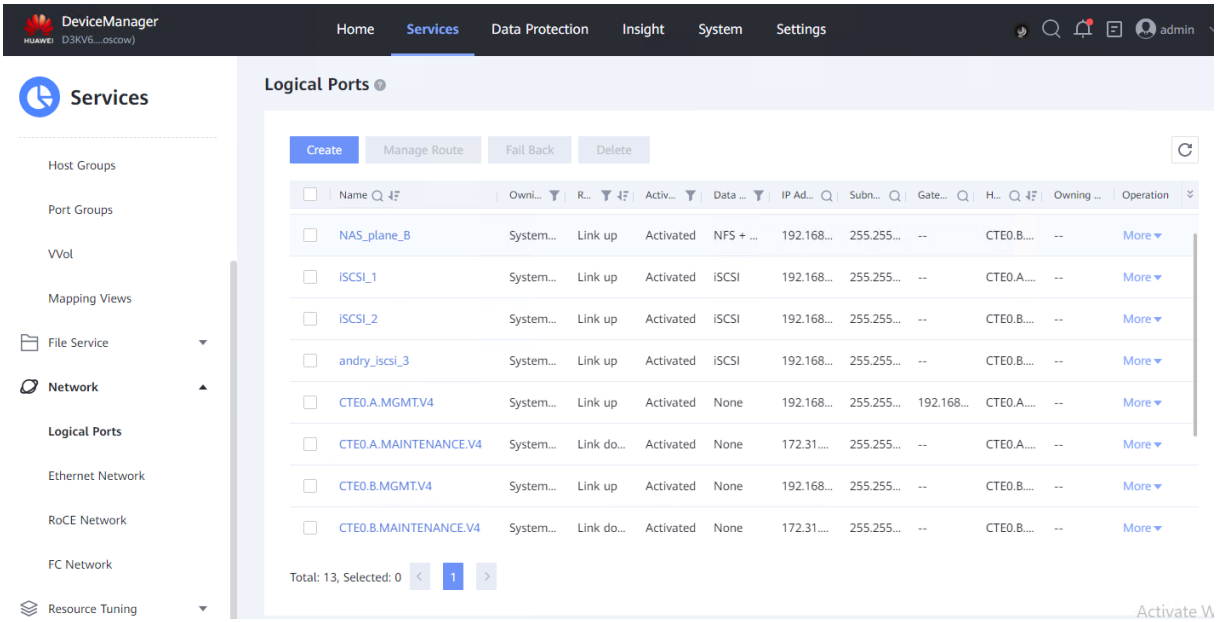
13.3.5.2 Настройка iSCSI-доступа

Нажмите **Пуск** - > **Средства администрирования Windows** - > **iSCSI Initiator**. Или в меню **Пуск** выберите **Выполнить** (или нажмите одновременно **Win** + **R**) и наберите **iscsicpl.exe**, а затем нажмите **OK** или Enter.

Если служба не была запущена, появится предложение запустить службу, выберите **Да**.



Убедитесь, что у устройства Dorado есть доступ хотя бы к одному из портов Logical Ports iSCSI. При этом порт в Logical Ports может быть отличен от порта, который используется в ESXi.



Убедитесь, что IQN инициатора уникально. Это актуально в случае, если машины были клонированы.

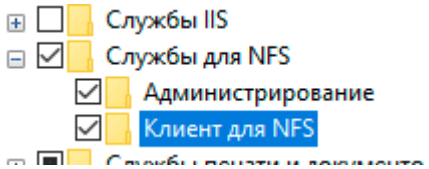
13.3.5.3 Настройка NFS

Убедитесь, что хотя бы одна сетевая карта (подсеть) имеет доступ к NFS устройства Dorado. NFS Dorado должна располагаться в той же подсети, в которой находится ESXi.

На клиентском компьютере под управлением Windows выполните следующие действия:

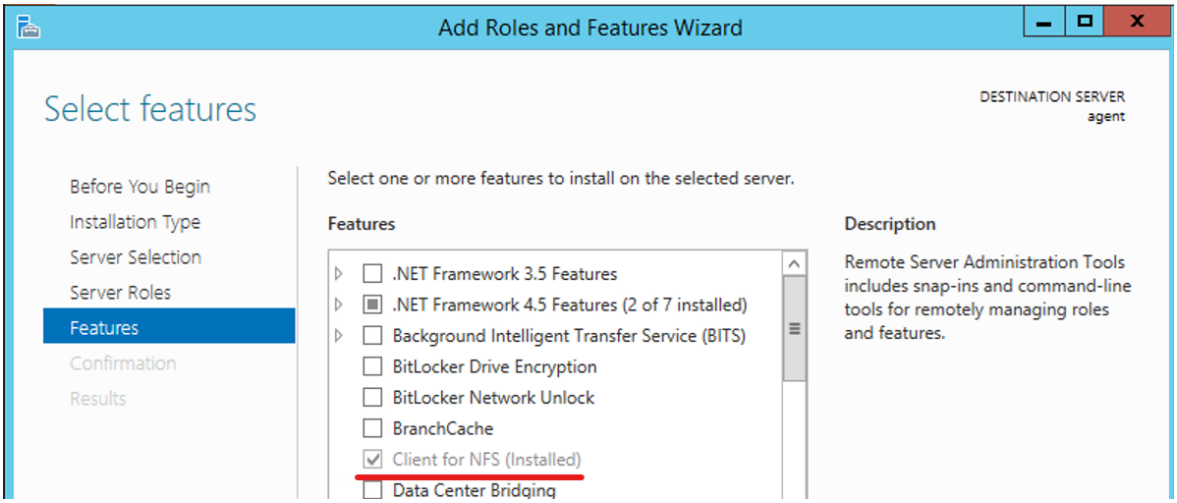
© ООО Киберпротект, 2026

1. Нажмите **Пуск** - > **Выполнить** (или нажмите одновременно **Win** + **R**).
2. Наберите **optionalfeatures.exe** и нажмите **OK** или Enter.
3. Отметьте пункт **Клиент для NFS** и нажмите **OK**.



Для сервера под управлением Windows выполните следующие действия:

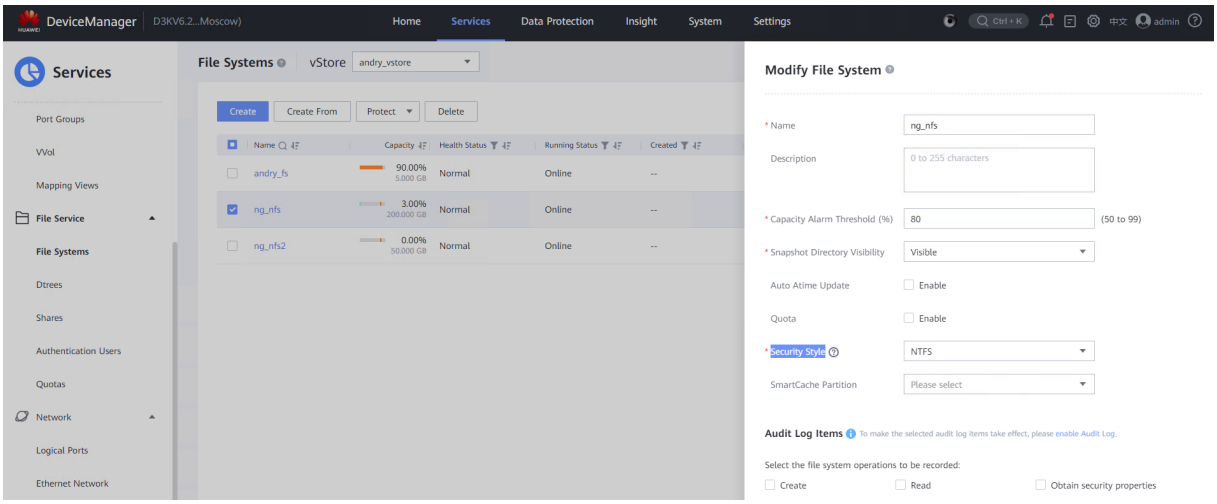
1. Нажмите **Пуск** - > **Выполнить** (или нажмите одновременно **Win** + **R**).
2. Наберите **optionalfeatures.exe** и нажмите **OK** или **Enter**.
3. Убедитесь, что на сервере установлен компонент **Клиент для NFS**. Иначе отметьте пункт **Клиент для NFS** и установите компонент (инструкции по установке см. в документации Microsoft).



13.3.5.4 Настройка CIFS

При создании общей папки SMB в секции **File Systems** в панели управления Dorado в поле **Security Style** выберите пункт **NTFS**.

© ООО Киберпротект, 2026



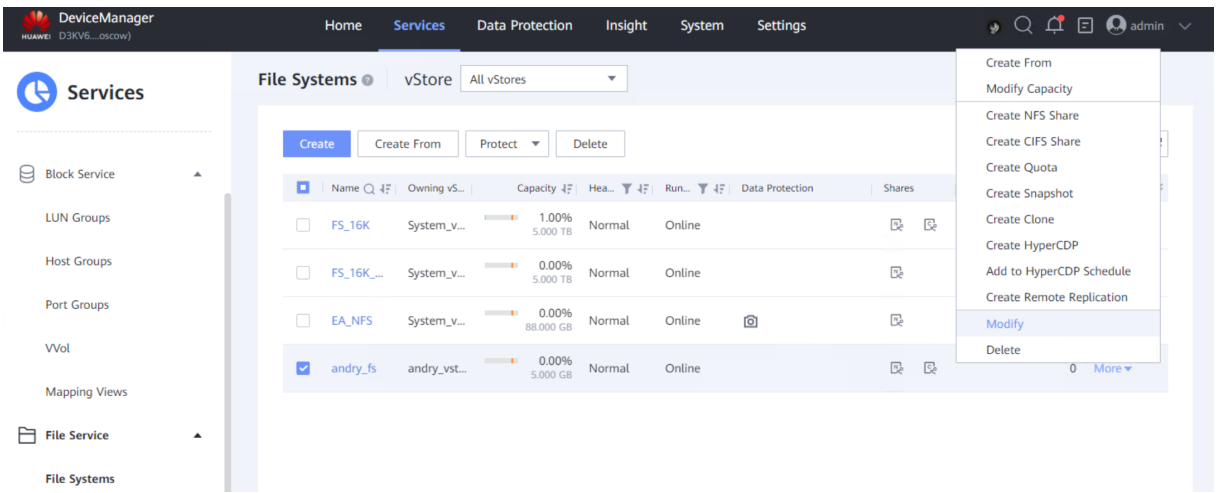
Рекомендуется в настройках общей папки прописывать доступ к машине с агентом. Убедитесь, что общая папка SMB доступна для чтения/записи штатными средствами.

13.3.5.5 Настройка анонимного UID и анонимного GID

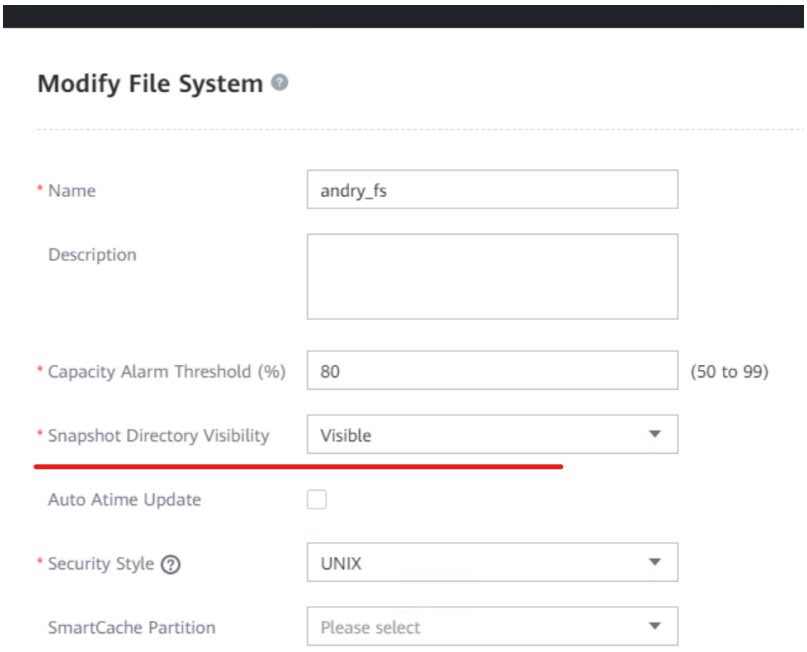
1. На компьютере, где находится агент для VMware (Windows) откройте реестр Windows: нажмите одновременно **Win+R**, а затем наберите **regedit.exe** и нажмите **OK** или Enter.
2. Откройте HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default
3. Создайте новый элемент **DWORD** с названием **AnonymousUID** и установите его значение на **0** (или другое значение UID для пользователя Unix).
4. Создайте новый элемент **DWORD** с названием **AnonymousGID** и установите его значение на **0** (или другое значение GID для пользователя Unix).
5. Перезагрузите компьютер.

Убедитесь, что IP-адрес агента находится в списке разрешенных для раздела ресурсов и у него есть права read-write.

Убедитесь, что **Snapshot Directory Visibility** файловой системы включен.



© ООО Киберпротект, 2026



13.3.5.6 Подключение к серверу управления

Для подключения к серверу управления выполните шаги по настройке Dorado из раздела "Регистрация хранилища данных SAN на сервере управления" (стр. 712).

13.3.5.7 Известные проблемы и ограничения

1. Возможность резервного копирования через NFS существует лишь для компьютеров под управлением Windows 10.
2. Аппаратные моментальные снимки поддерживаются только для VMware.
3. Проверяется наличие NFS-клиента, если в хранилище находится хотя бы одна файловая система NFS.
4. Проверяется наличие iSCSI-инициатора, если в хранилище находится хотя бы одно логическое устройство (LUN).
5. Не удается выполнить резервное копирование виртуальной машины с пустым диском.
6. Не удается выполнить резервное копирование, если диск виртуальной машины находится не в аппаратном хранилище.

13.3.6 Настройка машины с агентом для VMware (Windows)

В зависимости от использования хранилища SAN в качестве хранилища данных NFS или iSCSI см. соответствующий раздел ниже.

13.3.6.1 Настройка инициатора iSCSI

Убедитесь, что выполнены все последующие условия:

© ООО Киберпротект, 2026

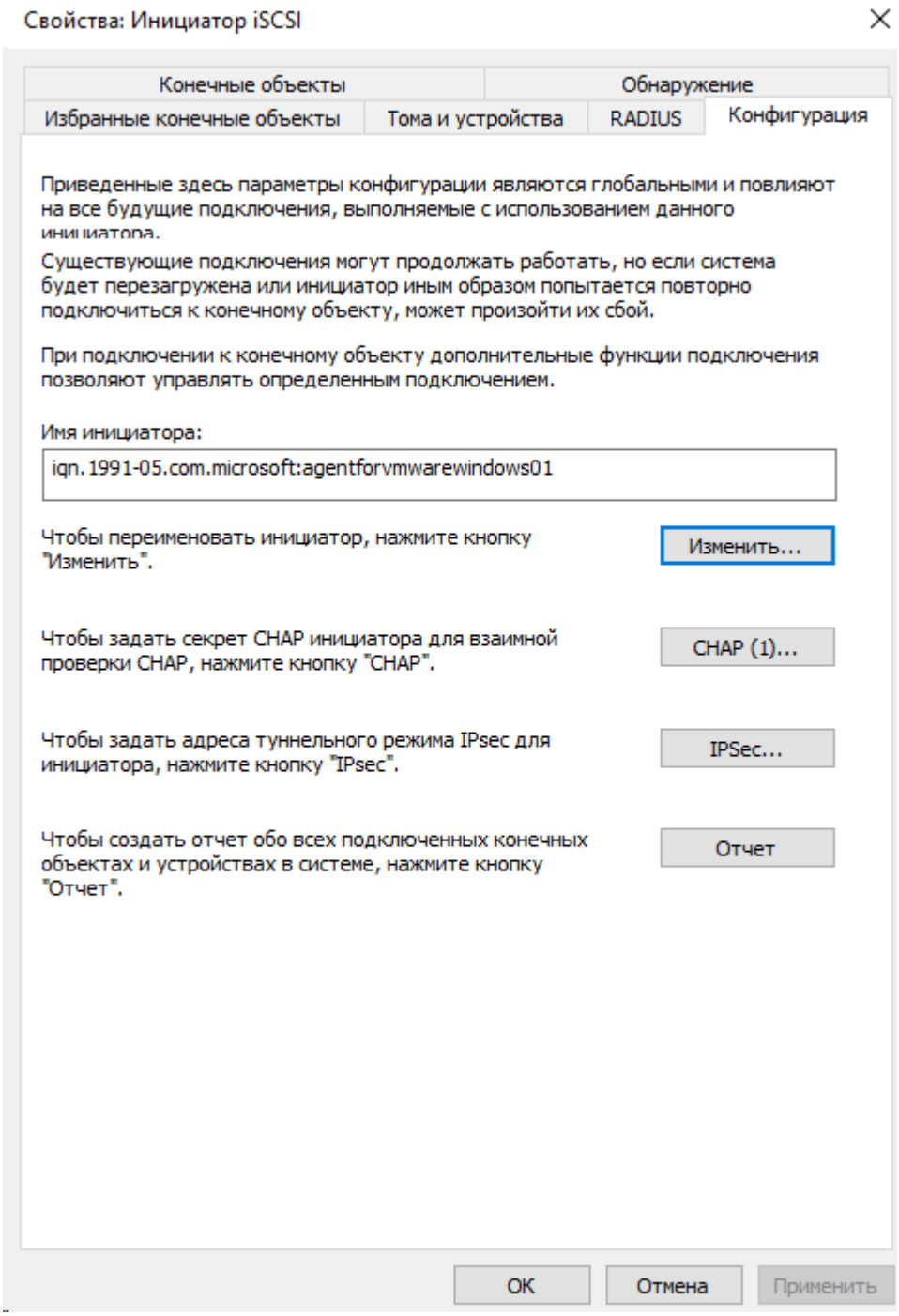
- Инициатор iSCSI установлен.
- Тип запуска службы инициатора iSCSI (Microsoft) имеет значение **Автоматически** или **Вручную**. Это можно сделать в оснастке **Службы**.
- Инициатор iSCSI настроен как описано в примере раздела "Резервное копирование без использования локальной сети посредством Windows-агента для VMware" (стр. 332).

13.3.6.2 Настройка iSCSI-инициатора для СХД YADRO TATLIN.UNIFIED

Выполните следующие действия для каждой машины с агентом:

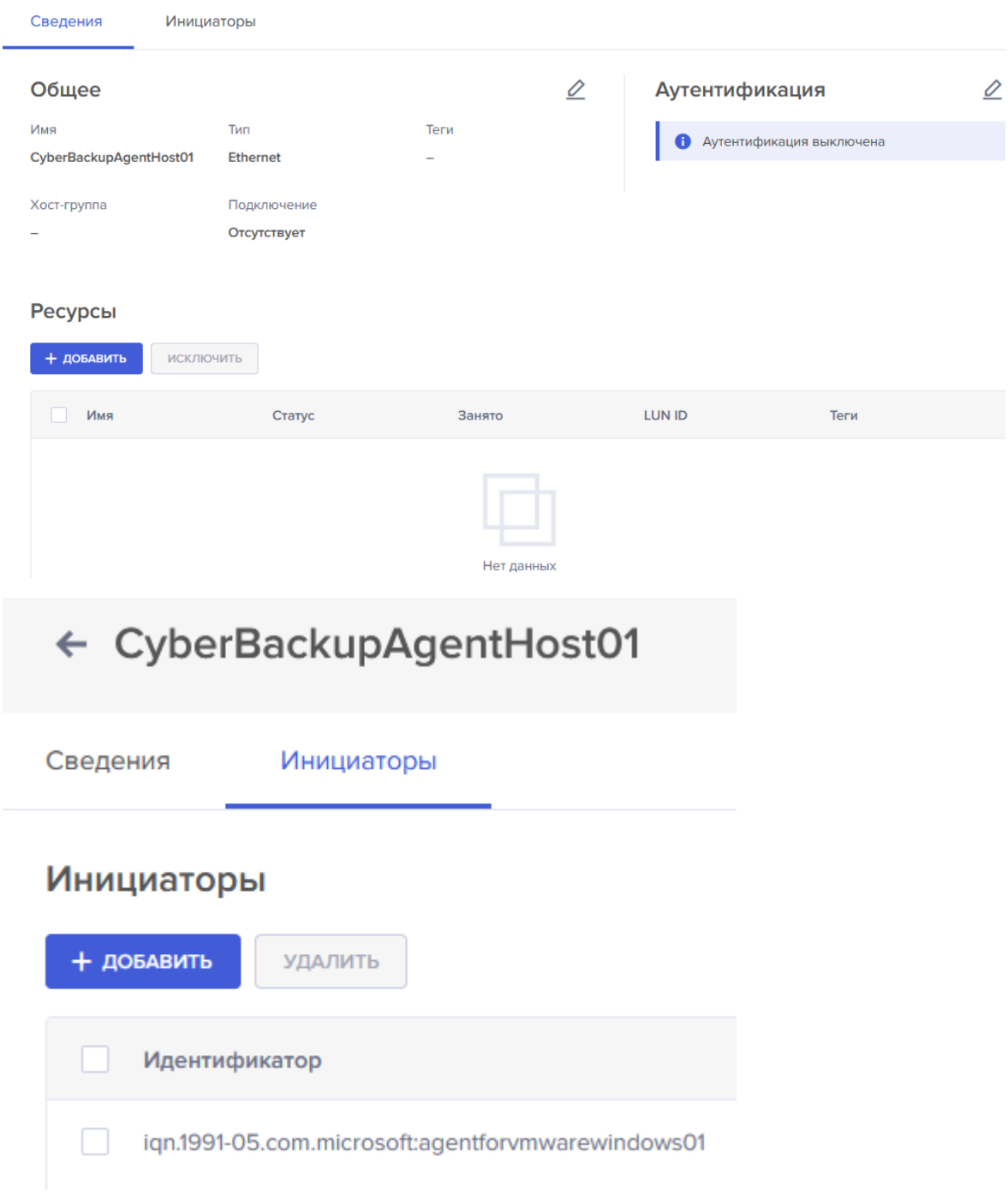
1. В консоли управления службами укажите тип запуска **Автоматически** или **Вручную** для службы инициатора Майкрософт iSCSI.
2. Запустите приложение **Инициатор iSCSI** и на вкладке **Конфигурация** получите IQN-имя iSCSI-инициатора машины.

© ООО Киберпротект, 2026



3. В хранилище данных YADRO TATLIN.UNIFIED создайте хост с именем **CyberBackupAgentHost<уникальный_суффикс>** и добавьте для него IQN-имя iSCSI-инициатора машины. Ресурсы добавлять не нужно.

© ООО Киберпротект, 2026



Добавленный хост будет использоваться для предоставления агенту доступа к моментальным снимкам, создаваемым в хранилище данных.

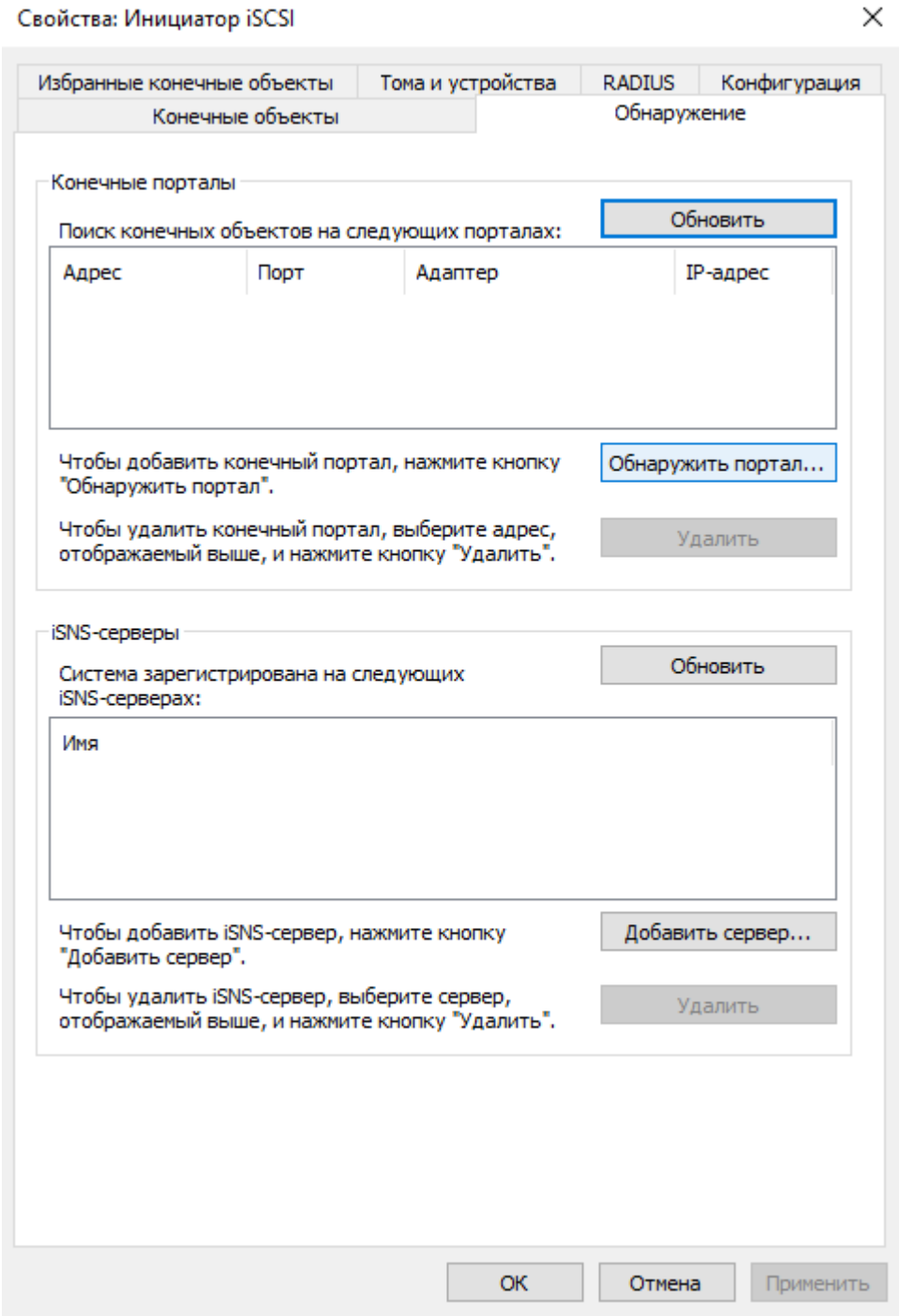
Примечание

При резервном копировании Кибер Бэкап автоматически добавляет (для хоста) и удаляет временные ресурсы (LUN), которые создаются на основе моментальных снимков ресурса с дисками виртуальных машин.

4. Проверьте, что iSCSI-инициатор может подключиться к хранилищу данных. Для этого в приложении **Инициатор iSCSI** на вкладке **Обнаружение** добавьте портал обнаружения

© ООО Киберпротект, 2026

хранилища данных, перейдите на вкладку **Конечные объекты** и подключитесь к обнаруженному конечному объекту.



13.3.6.3 Настройка NFS-клиента

Убедитесь, что выполнены все последующие условия:

- Установлен **Клиент для NFS**.
- NFS-клиент настроен на анонимный доступ. Это можно сделать следующим образом:

© ООО Киберпротект, 2026

a. Откройте редактор реестра.

b. Найдите следующий раздел реестра: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**

c. В этом ключе создайте новый параметр **DWORD** с именем **AnonymousUID** и задайте ему значение, равное 0.

d. В этом же ключе создайте новый параметр **DWORD** с именем **AnonymousGID** и задайте ему значение, равное 0.

e. Перезапустите машину.

13.3.7 Регистрация хранилища данных SAN на сервере управления

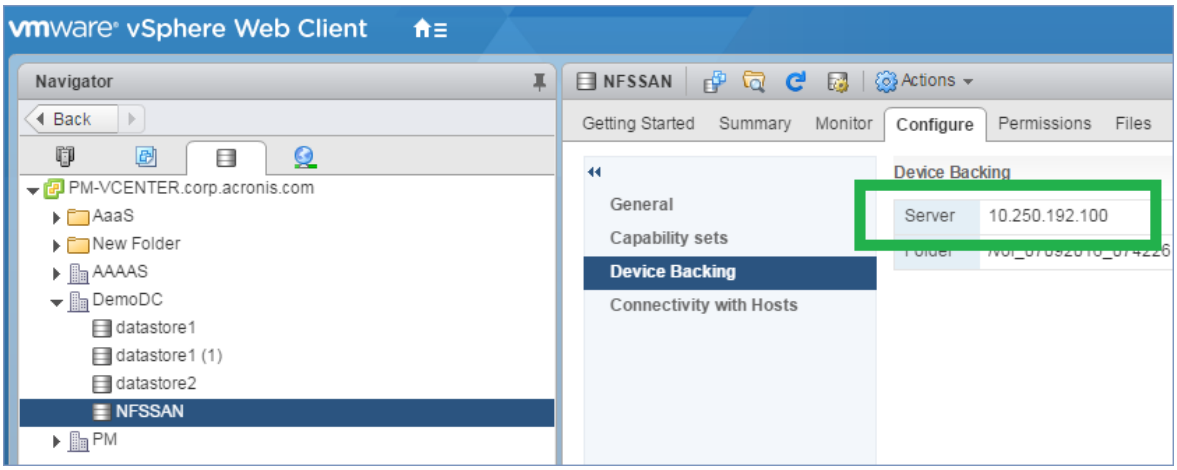
13.3.7.1 Регистрация хранилища данных YADRO TATLIN.UNIFIED

1. Перейдите в раздел **Настройки** > **Хранилище данных SAN** и нажмите **Добавить хранилище**.
2. В поле **Имя** укажите имя для хранилища.
3. В раскрывающемся списке **Выберите тип SAN** выберите тип хранилища данных **YADRO Tatlin.Unified**.
4. В поле **Имя или IP-адрес хоста** укажите DNS-имя или IP-адрес для подключения к API хранилища данных.
5. В полях **Имя пользователя** и **Пароль** укажите учетные данные пользователя для подключения к API хранилища данных. Сведения о подготовке пользователя см. в разделе "Настройка хранилища данных YADRO TATLIN.UNIFIED" (стр. 693).
6. Выберите от одного до нескольких агентов, которым будет предоставлен доступ на чтение к этому хранилищу данных.
7. Нажмите **Добавить**.

13.3.7.2 Регистрация хранилища данных NetApp

1. Нажмите **Настройки** > **Хранилище данных SAN**.
2. Нажмите **Добавить хранилище**.
3. [Необязательно] В **Имя** измените имя хранилища.
   Это имя будет отображено на вкладке **Хранилище данных SAN**.
4. В **Имя хоста или IP-адрес** укажите виртуальную машину хранилища NetApp Storage Virtual Machine (SVM, также называемое систематизатором), которая была указана при создании хранилища данных.
   Для нахождения требуемой информации в веб-клиенте VMware vSphere выберите хранилище данных и затем нажмите **Настроить** > **Резервная копия устройства**. Имя хоста или IP-адрес отобразится в поле **Сервер**.

© ООО Киберпротект, 2026



5. В полях **Имя пользователя** и **Пароль** укажите учетные данные администратора SVM.

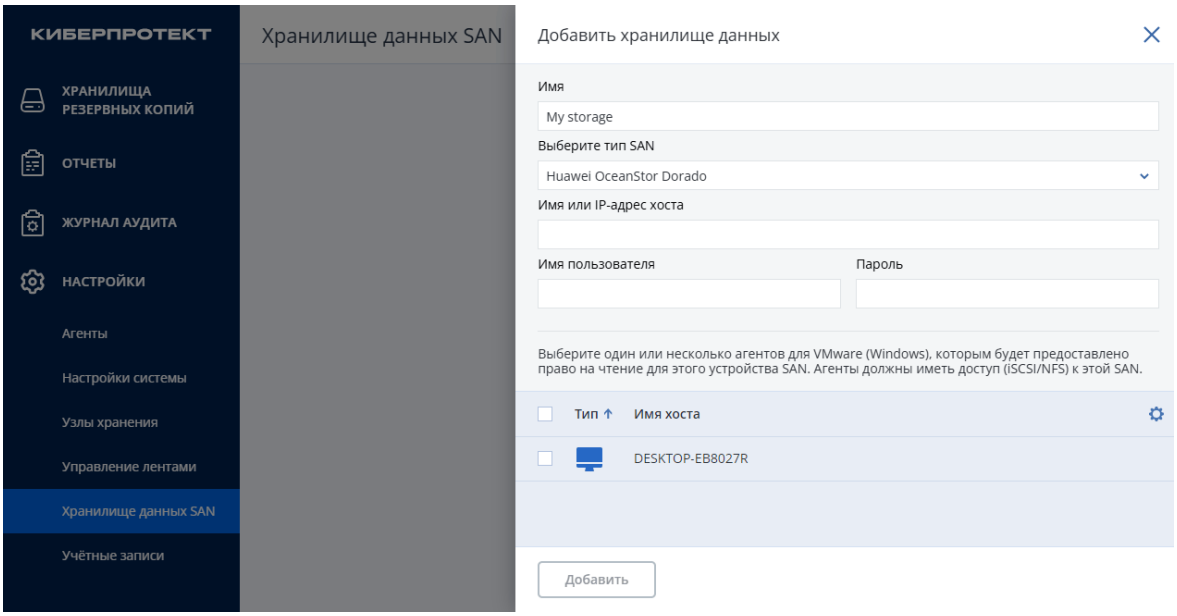
Внимание
Указанная учетная запись должна иметь права локального администратора SVM, а не права администратора менеджера системы NetApp.

Выберите существующего пользователя или создайте нового. Второе можно сделать в менеджере системы NetApp OnCommand по пути **Настройки** > **Безопасность** > **Пользователи**.

6. Выберите один или несколько агентов для VMware (Windows), которым будет предоставлено право на чтение для устройства SAN.
7. Нажмите **Добавить**.

13.3.7.3 Регистрация хранилища данных Huawei OceanStor (Dorado)

1. Перейдите в веб-консоль Кибер Бэкап.
2. В разделе **Настройки** -> **Хранилище данных SAN** нажмите **Добавить хранилище**.



© ООО Киберпротект, 2026

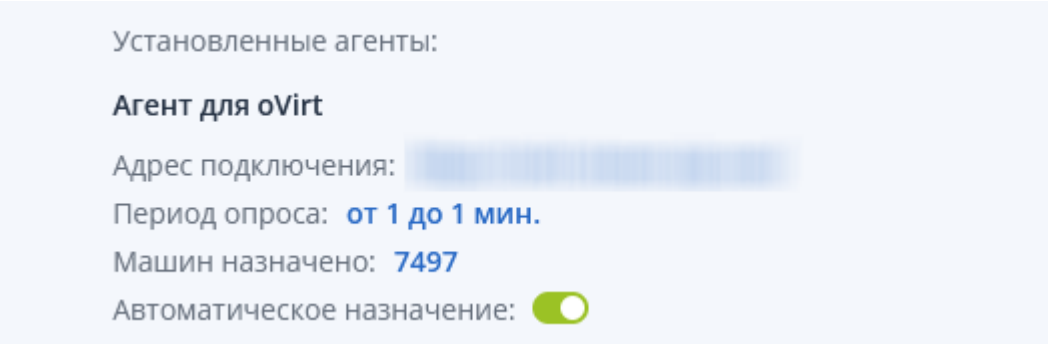
3. Укажите параметры в окне **Добавить хранилище данных**:
   - В поле **Имя** укажите название устройства;
   - В поле **Выберите тип SAN** укажите **Huawei OceanStor Dorado**;
   - В поле **Имя или IP-адрес хоста** укажите IP-адрес веб-интерфейса устройства;
   - В полях **Имя пользователя** и **Пароль** укажите логин и пароль пользователя.
4. Выберите один или несколько агентов для VMware (Windows), которым будет предоставлено право на чтение для этого устройства SAN.
5. Нажмите **Добавить**.

13.3.8 Настройка машины с агентом для oVirt

13.3.8.1 Регистрация агента

Для регистрации агента выполните следующие действия:

1. В веб-консоли перейдите в меню **Настройки** -> **Агенты**.
2. В списке отметьте машину с агентом и нажмите справа **Сведения**.
3. В блоке **Агент для oVirt** щелкните значение в строке **Адрес подключения**.



4. В открывшемся окне введите адрес сервера и данные учетной записи для подключения к платформе виртуализации (например, https://zvirt.company.ru) и нажмите **Применить**.
5. В строке **Машин назначено** отображается количество назначенных машин для резервного копирования. Щелкните по значению в строке и просмотрите открывшийся список. Убедитесь, что все необходимые машины назначены. По умолчанию включено автоматическое назначение машин; если необходимо, назначьте машины вручную.

Для повышения производительности при одновременном резервном копировании рекомендуется для машины с агентом для oVirt использовать минимум 16 ГБ ОЗУ и 4 ядра ЦП.

13.3.8.2 Настройка агента

Чтобы настроить машину с агентом для oVirt, выполните следующие действия (на примере РЕД ОС 8, в других ОС названия пакетов могут отличаться):

© ООО Киберпротект, 2026

1. Установите пакет qemu-img:

```
dnf install qemu-img
```

2. Установите пакет lvm2:

```
dnf install lvm2
```

3. Отключите автоматическую активацию томов LVM в конфигурационном файле /etc/lvm/lvm.conf, добавив в секцию activation следующую строку:

```
auto_activation_volume_list = []
```

4. Отключите в LVM фильтрацию устройств по devices file, раскомментировав в файле /etc/lvm/lvm.conf параметр use_devicesfile и установив его значение равным 0:

```
use_devicesfile = 0
```

5. Установите пакет iscsi-initiator-utils:

```
dnf install iscsi-initiator-utils
```

6. Включите автозапуск службы iscsid:

```
systemctl enable iscsid iscsi --now
```

7. Создайте файл /etc/iscsi/iscsid_auth.conf и добавьте в него строки:

```
[DEFAULTS]
InitiatorName=<имя инициатора iSCSI>
```

Где <имя инициатора iSCSI> – строка из файла /etc/iscsi/initiatorname.iscsi.

8. Установите пакет для multipathd:

```
dnf install device-mapper-multipath
```

9. Создайте конфигурационный файл /etc/multipath.conf с содержимым:

```
defaults {
  user_friendly_names no
}
```

10. Перезапустите службу multipathd:

```
systemctl restart multipathd
```

Для работы агента с системой виртуализации oVirt может потребоваться сертификат SSL.

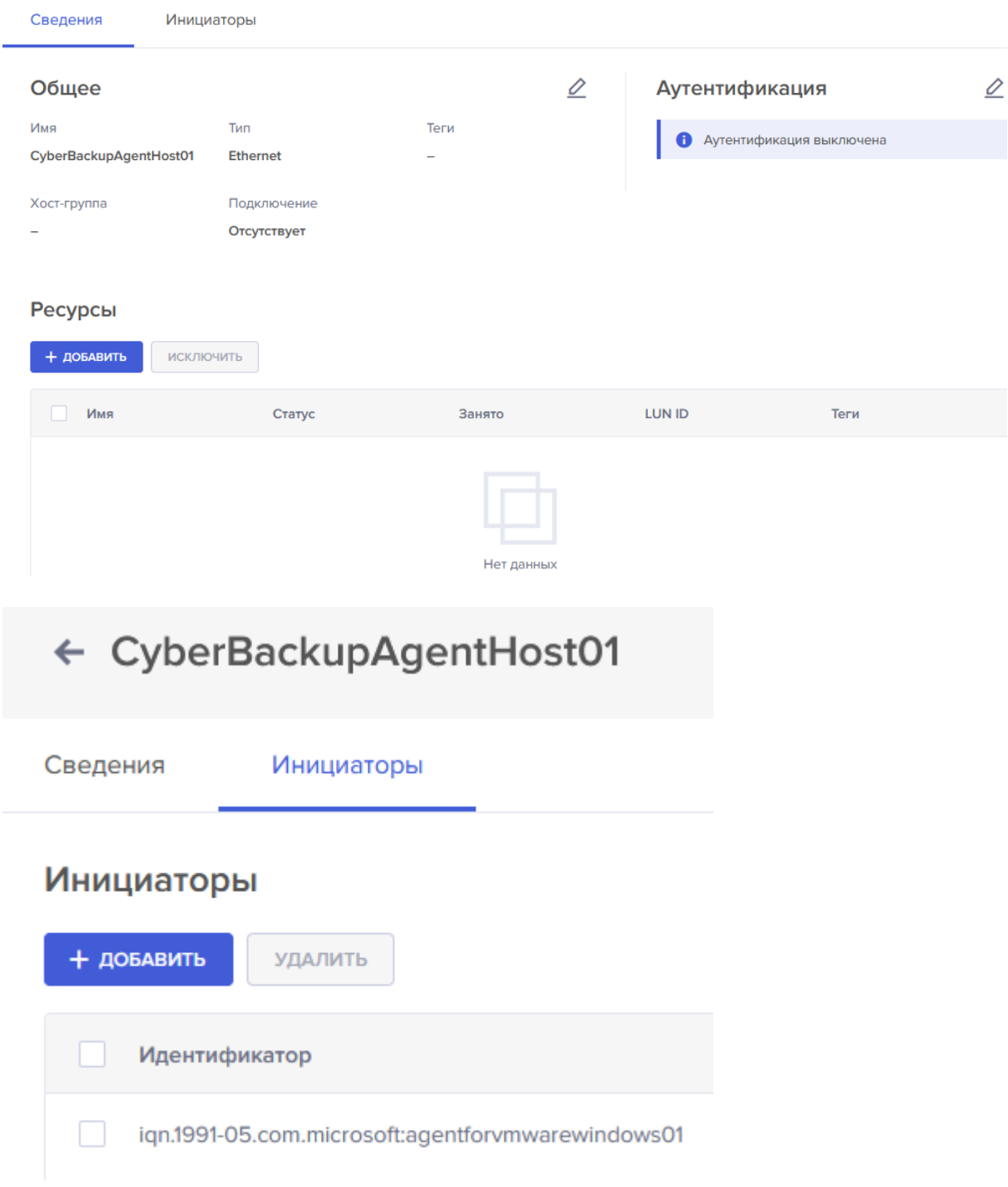
Установите сертификат SSL или в файле /etc/Acronis/VirtualWare.config под поле </registry> добавьте строку:

© ООО Киберпротект, 2026

```
<value name="IgnoreSslErrors" type="Tdword">"1"</value>
```

13.3.8.3 Создание хоста

В хранилище данных YADRO TATLIN.UNIFIED создайте хост с именем **CyberBackupAgentHost<уникальный_суффикс>** и добавьте для него IQN-имя iSCSI-инициатора машины. Ресурсы добавлять не нужно.



© ООО Киберпротект, 2026

13.3.8.4 Известные проблемы и ограничения

- Недоступно восстановление виртуальных машин локальным агентом для oVirt для Linux; для этого используется виртуальное устройство для oVirt (для его установки см. раздел "Установка агента для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация)" (стр. 104)).

13.4 Резервное копирование кластеризованных машин Hyper-V

В кластере Hyper-V виртуальные машины могут мигрировать между узлами кластера. Следуйте приведенным ниже рекомендациям для настройки правильного резервного копирования кластеризованных машин Hyper-V.

1. Машина должна быть доступна для резервного копирования независимо от того, на какой узел она переносится. Чтобы убедиться в том, что агент для Hyper-V имеет доступ к машине на любом узле, необходимо запустить службу агента под учетной записью пользователя домена с правами администратора на каждом из узлов кластера (см. "Установка агентов" (стр. 95)). Рекомендуется указать такую учетную запись для службы агента в процессе установки агента для Hyper-V.
2. Установите агент для Hyper-V на каждом узле кластера.
3. Зарегистрируйте все агенты на сервере управления.

13.4.1 Высокая доступность восстановленной машины

При восстановлении резервных копий дисков на *существующей* виртуальной машине Hyper-V свойство высокой доступности данной машины остается без изменений.

Если вы восстанавливаете диски с резервной копии на *новую* виртуальную машину Hyper-V или выполняете преобразование в виртуальную машину Hyper-V в рамках плана защиты, полученная в результате машина не будет высокодоступной. Она считается запасной и обычно выключена. Если машину необходимо использовать в производственной среде, можно настроить для нее свойство высокой доступности с помощью оснастки **Управление отказоустойчивым кластером**.

13.5 Миграция машины

Можно выполнить миграцию машины, восстановив ее резервную копию на машину, которая не является исходной.

Доступные варианты выполнения миграции приведены в следующей таблице.

© ООО Киберпротект, 2026

Тип виртуальной машины	Доступные места восстановления									
	Физическая машина	Виртуальная машина Кибер Инфраструктура	Виртуальная машина VMware ESXi	Виртуальная машина Hyper-V	Виртуальная машина oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация)	Виртуальная машина SpaceVM	Виртуальная машина ECP VeiL	Виртуальная машина OpenStack[1]	Виртуальная машина Basis DynamiX Enterprise[1]	Виртуальная машина OpenNebula (ПК СВ "Брест")
Физическая машина	+	-	+	+	+	+	+	+	+	+
Виртуальная машина Кибер Инфраструктура	-	+	+	-	+	+	+	+	+	+
Виртуальная машина Basis DynamiX Enterprise	-	+	+	-	+	+	+	+	+	+
Виртуальная машина VMware ESXi	+	+	+	+	+	+	+	+	+	+
Виртуальная машина	+	-	+	+	+	+	+	+	+	+

© ООО Киберпротект, 2026

Hyper-V										
Виртуальная машина oVirt	+	+	+	+	+	+	+	+	+	+
Виртуальная машина Space VM	+	+	+	+	+	+	+	+	+	+
Виртуальная машина ECP VeiL	+	+	+	+	+	+	+	+	+	+
Виртуальная машина OpenStack	-	+	+	-	+	+[2]	+[2]	+	+	+
Виртуальная машина OpenNebula	+	+	+	+	+	+	+	+	+	+

[1] Платформы OpenStack и Basis DynamiX Enterprise наряду с KVM используют драйверы VirtIO и VirtIO SCSI для сети и дисков. Для миграции виртуальной машины на ОС Windows или Linux на OpenStack или Basis DynamiX Enterprise необходимо установить в нее драйверы VirtIO и VirtIO SCSI, агент QEMU Guest Agent, cloud-init и убедиться, что они работают. Необходимо учитывать, что драйверы VirtIO могут по-разному работать на различных выпусках ОС Windows и версиях OpenStack и Basis DynamiX Enterprise. Подготовленная машина может не запускаться на платформах из-за особенностей настройки гипервизора, флагов ЦП или несовместимости драйверов. Рекомендуется использовать готовые образы ОС Windows, например, от Cloudbase. Дополнительные сведения для машин на ОС Windows приведены в руководстве OpenStack.

[2] Только машины на ОС Linux с дисками с интерфейсом NVMe.

Инструкции о выполнении миграции см. в следующих разделах:

© ООО Киберпротект, 2026

- Миграция систем с физической машины на виртуальную (P2V): Миграция систем с физической машины на виртуальную
- Миграция систем с виртуальной машины на виртуальную (V2V): Виртуальная машина
- Миграция систем с виртуальной машины на физическую (V2P): Виртуальная машина или Восстановление дисков с помощью загрузочного носителя

Хотя можно выполнить миграцию V2P в веб-интерфейсе, в определенных случаях рекомендуется использовать загрузочный носитель. Иногда вы можете создать носитель для миграции в ESXi или Hyper-V.

Носитель позволяет выполнить следующие действия:

- Выполнить миграцию P2V и миграцию V2V машины Linux с логическими томами (LVM). Используйте агент для Linux или загрузочный носитель, чтобы создать резервную копию, и загрузочный носитель для восстановления.
- Предоставить драйверы для определенного оборудования, которое имеет критически важное значения для загружаемости системы.

13.5.1 Миграция Linux-машины с логическими томами (LVM)

Для миграции физической или виртуальной Linux-машины, у которой есть логические тома (LVM), в виртуальную или физическую машину, необходимо следующее:

1. резервная копия исходной машины должна быть создана с помощью агента, установленного внутри данной машины;

   Примечание
   Резервная копия виртуальной машины, созданная агентом для соответствующей системы виртуализации, не может быть использована для данного вида миграции.

2. восстановление должно выполняться с помощью загрузочного носителя;
3. в процессе восстановления нужно воспроизвести исходную структуру логических томов.

Миграция Linux-машины, у которой есть логические тома (LVM)

1. Убедитесь, что у вас есть резервная копия машины, которая была создана агентом, установленным внутри исходной машины.
2. Загрузите целевую машину, используя загрузочный носитель.
3. Убедитесь, что в интерфейсе загрузочного носителя используется способ представления дисков и томов как в Linux.
4. Запустите мастер восстановления, выберите резервную копию исходной машины и выберите диски для восстановления.
5. Удостоверьтесь, что количество и емкость дисков целевой машины равны или превосходят количество и емкость дисков исходной машины.
6. Воспроизведите на целевой машине такую же структуру логических томов, как на исходной

© ООО Киберпротект, 2026

машине. Для этого нажмите кнопку **Применить RAID/LVM**.

7. Завершите процесс восстановления.

   Если операционная система на целевой машине не загружается после восстановления, используйте универсальное восстановление для решения этой проблемы.

13.6 Увеличение объёма ОЗУ виртуального устройства

Для повышения производительности операций резервного копирования и восстановления объём ОЗУ виртуального устройства (virtual appliance) может быть увеличен. При этом размер его диска должен быть достаточным для размещения как аварийного дампа памяти (при его формировании), так и файлов журналов. В противном случае файл дампа может занять всё дисковое пространство, что приведёт к некорректной работе или полному отказу функций резервного копирования и восстановления виртуальных машин.

Начиная с Кибер Бэкап версии 18.5, объём диска для вновь создаваемых виртуальных устройств по умолчанию составляет 64 ГБ (ранее – 8 ГБ).

У виртуальных устройств, созданных в более ранних версиях Кибер Бэкап, после обновления до версии 18.5 размер диска остаётся прежним. В этом случае для расширения дискового пространства рекомендуется переустановить виртуальное устройство, используя новые образы (подробнее см. в разделе "Установка агентов" (стр. 95)), либо выполнить инструкции, приведённые в статье базы знаний.

13.7 Резервное копирование облачных виртуальных машин без доступа к гипервизору

Чтобы создать резервную копию виртуальной машины без доступа к гипервизору (т. е. находящейся в облаке), установите агент защиты на такой машине. Операции резервного копирования и восстановления выполняются точно так же, как и на физической машине.

Отличие от физической машины состоит в том, что виртуальные машины, находящиеся в облаке, невозможно загрузить с загрузочного носителя. Если необходимо выполнить восстановление в новую виртуальную машину, следуйте указанной ниже процедуре.

Порядок восстановления машины как виртуальной машины в облаке:

1. Создайте новую виртуальную машину из образа или шаблона в используемом облаке. Новая машина должна иметь такую же конфигурацию диска, как и машина, которую необходимо восстановить.
2. Установите агент для Windows или агент для Linux на новой машине.
3. Восстановите машину из резервной копии, как описано в разделе Физическая машина. При настройке восстановления выберите новую машину в качестве целевой.

© ООО Киберпротект, 2026

13.7.1 Требования к сети

Агенты, установленные на машинах, для которых выполняется резервное копирование, должны иметь возможность обмениваться данными с сервером управления по сети.

- Если и агенты, и сервер управления установлены в одном облаке, то никаких дополнительных действий не требуется, так как все машины уже находятся в одной сети.
- Если сервер управления находится вне облака, то машины внутри облака не будут иметь доступа к локальной сети, в которой установлен сервер управления. Чтобы агенты, установленные на таких машинах, могли связываться с сервером управления, необходимо создать подключение виртуальной частной сети (VPN) между локальной и облачной сетями.

  Запросите у вашего поставщика облачной инфраструктуры, чей сервис вы используете, инструкции по созданию подключений VPN, аналогичные инструкциям, приведённым ниже:
  - Windows Azure: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal;
  - Amazon EC2: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw.

© ООО Киберпротект, 2026

14 Мониторинг, отчёты и аудит

Панель мониторинга **Обзор** даёт возможность отслеживать текущее состояние защищённой инфраструктуры.

Раздел **Отчёты** даёт возможность создавать запланированные отчёты и отчёты по требованию с данными о защищённой инфраструктуре. Этот раздел доступен только при наличии лицензии Кибер Бэкап Расширенная редакция.

Раздел **Журнал аудита** содержит сведения о событиях, произошедших в Кибер Бэкап вследствие действий пользователей или работы системных компонентов.

14.1 Панель мониторинга "Обзор"

Панель мониторинга **Обзор** предоставляет ряд настраиваемых виджетов для обзора защищенной инфраструктуры. Вы можете выбирать из более чем 20 виджетов, представленных в виде круговых диаграмм, таблиц, графиков, линейчатых диаграмм и списков. У виджетов есть активные элементы, на которые можно щелкнуть для исследования возникших неполадок, их диагностики и устранения. Информация, представленная в виджетах, обновляется каждые пять минут.

Расширенная лицензия также позволяет скачать текущее состояние панели мониторинга или отправить его по электронной почте в файле формата .pdf и (или) .xlsx. Для отправки данных панели мониторинга по электронной почте убедитесь в том, что у вас сконфигурированы настройки почтового сервера.

Доступные виджеты зависят от выпуска Кибер Бэкап. Ниже перечислены виджеты, которые отображаются по умолчанию:

Виджет	Доступность	Описание
Статус защиты	Доступно во всех выпусках	Показывает текущее состояние защиты для всех машин.
Действия	Доступно во всех выпусках	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Сводка по активным оповещениям	Доступно во всех выпусках	Показывает сводную информацию об активных оповещениях по их типу и уровню серьезности.
Устройства	Доступно во всех выпусках	Показывает подробную информацию об устройствах в вашей среде.
Подробная информация об активных оповещениях	Доступно во всех выпусках	Показывает подробную информацию об активных оповещениях.
Сводные данные о хранилищах	Доступно во всех выпусках	Показывает подробную информацию о хранилищах резервных копий.

Порядок добавления виджета

Щелкните **Добавить виджет** и выполните одно из следующих действий:

© ООО Киберпротект, 2026

- Щелкните виджет, который необходимо добавить. Виджет будет добавлен с настройками по умолчанию.
- Чтобы изменить виджет перед его добавлением, щелкните значок карандаша, когда виджет выбран. После изменения виджета щелкните **Готово**.

Порядок изменения расположения виджетов на панели мониторинга

Перетащите виджеты, щелкнув их имена.

Порядок изменения виджета

Щелкните значок карандаша рядом с именем виджета. Изменение виджета позволяет переименовать его, изменить диапазон времени, задать фильтры и сгруппировать строки.

Порядок удаления виджета

Щелкните значок X рядом с именем виджета.

14.1.1 Виджет "Резервные копии"

В этом виджете отображается общая информация о размере резервных копий .

В верхней строке отображается текущая статистика:

- **Резервная копия создана сегодня**: суммарный размер резервных копий в точках восстановления за последние 24 часа

В нижней строке показана общая статистика:

- Сжатый размер всех резервных копий

14.1.2 Виджет "Статус защиты"

В этом виджете показано текущее состояние защиты для всех машин.

Машина может быть в одном из следующих состояний:

- **Защищенные**: машины, для которых применен план защиты.
- **Незащищенные**: машины, для которых не применен план защиты. Под ними подразумеваются как обнаруженные, так и управляемые машины без примененного плана защиты.
- **Управляемое**: машины с установленным агентом защиты.
- **Обнаружено**: машины без установленного агента защиты.

Если щелкнуть состояние машины, для получения более подробной информации откроется список машин, которые имеют данное состояние.

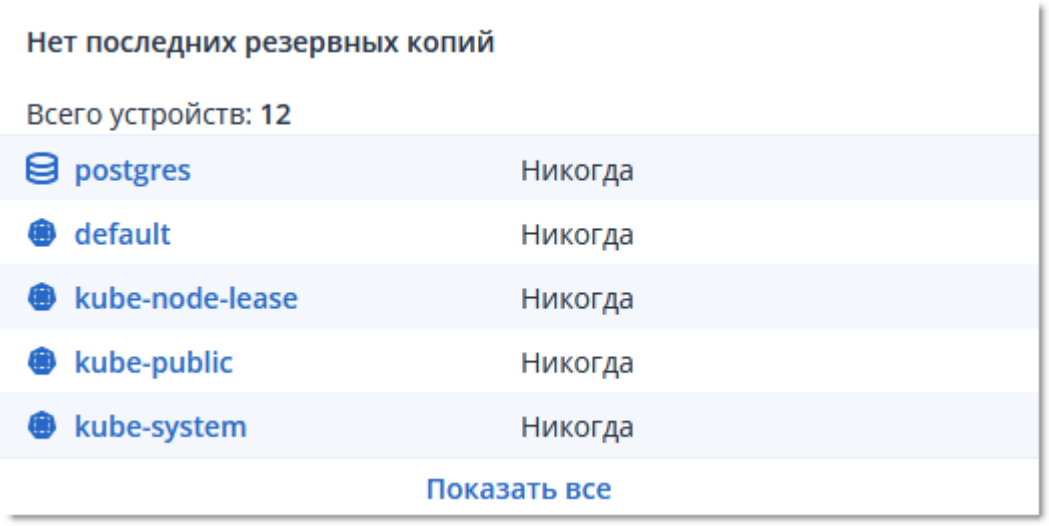
14.1.2.1 Обнаруженные машины

В этом виджете показан список машин, обнаруженных за указанный период времени.

© ООО Киберпротект, 2026

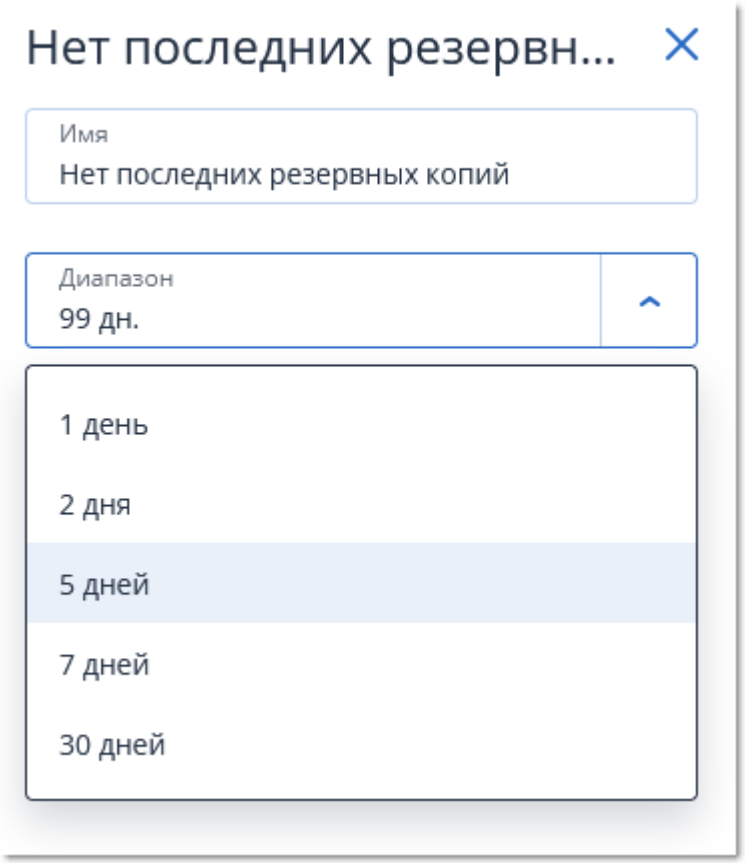
14.1.3 Виджет "Нет последних резервных копий"

Этот виджет показывает рабочие нагрузки с применяемыми планами защиты, дата последнего успешного резервного копирования которых была ранее диапазона времени, указанного в настройках виджета.



Когда вы добавляете этот виджет, по умолчанию он отображает информацию за последние 5 дней. Вы можете использовать раскрывающееся меню, чтобы выбрать другой период или ввести количество дней вручную. Максимальное количество дней, которое вы можете ввести, составляет 99.

© ООО Киберпротект, 2026



14.2 Панель мониторинга "Оповещения"

Оповещение – это сообщение, предупреждающее о текущей или потенциальной проблеме. Оповещения можно использовать разными способами:

- Раздел **Оповещения** на вкладке **Обзор** позволяет быстро определять и решать проблемы путём мониторинга текущих оповещений.

  Примечание
  При поиске оповещений нельзя указывать в запросах непарные скобки, а также указывать символы перед парными скобками.

- В области виджета **Устройства** состояние устройства основывается на оповещениях. Колонка **Состояние** позволяет фильтровать устройства с проблемами.
- При настройке уведомлений по электронной почте можно выбрать, какие оповещения запустят уведомление.

Оповещение может иметь одну из следующих степеней серьёзности:

- **Критично**;
- **Ошибка**;
- **Предупреждение**.

© ООО Киберпротект, 2026

Можно изменить степень серьёзности оповещения или полностью отключить их с помощью файла настройки оповещений, как описано ниже. Эта операция требует перезапуска службы сервера управления.

Изменение степени серьёзности оповещения не повлияет на уже созданные оповещения.

14.2.1 Файл настройки оповещений

Файл настройки оповещений расположен на машине, где работает сервер управления.

- В Windows: <путь_установки>\AlertManager\alert_manager.yaml.

  Здесь <путь_установки> – путь установки сервера управления. По умолчанию используется %ProgramFiles%\Acronis.
- В ОС Linux: /usr/lib/Acronis/AlertManager/alert_manager.yaml

Файл имеет структуру YAML-документа. Каждое оповещение – это элемент в списке alertTypes.

Ключ name идентифицирует оповещение.

Ключ severity определяет уровень серьёзности оповещения. Он может иметь одно из следующих значений: critical (критично), error (ошибка) или warning (предупреждение).

Дополнительный ключ enabled определяет, включено ли оповещение. Значение должно быть true или false. По умолчанию (этот ключ не задан) все оповещения включены.

14.2.2 Изменение степени серьёзности оповещения, отключение оповещения

Для изменения степени серьёзности оповещения или его отключения выполните шаги:

1. На машине, на которой установлен сервер управления, откройте в текстовом редакторе файл **alert_manager.yaml**.
2. Найдите оповещение, которое необходимо изменить или отключить.
3. Выполните одно из следующих действий:
   - Чтобы изменить уровень серьёзности оповещения, измените значение ключа severity.
   - Чтобы отключить оповещение, добавьте ключ enabled и задайте для него значение false.
4. Сохраните файл.
5. Перезапустите службу сервера управления, как описано ниже.

14.2.3 Перезапуск службы сервера управления в ОС Windows

Для перезапуска службы сервера управления в ОС Windows выполните следующие шаги:

1. В меню **Пуск** операционной системы выберите команду **Выполнить** и введите: cmd.
2. Нажмите кнопку **OK**.
3. Выполните следующие команды:

© ООО Киберпротект, 2026

```
net stop acrmngsrv
net start acrmngsrv
```

В результате выполненных действий служба сервера управления будет перезапущена в ОС Windows.

14.2.4 Перезапуск службы сервера управления в ОС Linux

Для перезапуска службы сервера управления в ОС Linux выполните следующие шаги:

1. Откройте **приложение терминала**.
2. Выполните следующую команду:

```
sudo service acronis_ams restart
```

В результате выполненных действий служба сервера управления будет перезапущена в ОС Linux.

14.3 Панель мониторинга "Действия"

На вкладке **Действия** представлен обзор текущих и последних действий. По умолчанию период хранения составляет 180 дней.

Чтобы настроить содержимое вкладки **Действия**, щёлкните значок шестерни и выберите столбцы, которые нужно отобразить.

Чтобы ход выполнения действия отображался в реальном времени, установите флажок **Обновлять автоматически**.

Внимание
Частое обновление нескольких действий снижает производительность сервера управления.

Поиск действий в списке можно выполнить по указанным ниже критериям:

- **Имя устройства**:
  машина, на которой выполнено действие.
- **Кем запущено**:
  учётная запись, от имени которой запущено действие.
- **Название плана**:
  наименование плана защиты.

Кроме того, можно отфильтровать действия по следующим свойствам:

- **Состояние**:
  например, "Успешно", "С ошибками", "Выполняется", "Отменено".
- **Тип**:
  например, "Применение плана", "Удаление резервных копий", "Установка обновлений программного обеспечения".

© ООО Киберпротект, 2026

- **Время**:
  например, действия за последние сутки / неделю / месяц или действия в течение указанного периода времени в пределах периода хранения по умолчанию.

14.3.1 Порядок изменения периода хранения сведений о действиях

1. На машине с запущенной службой сервера управления откройте следующий файл конфигурации в текстовом редакторе:
   - В ОС Windows: %Program Files%\Acronis\TaskManager\task_manager.yaml.
   - В ОС Linux: /usr/lib/Acronis/TaskManager/task_manager.yaml.
2. Найдите следующий раздел:

```
database:
connection-string: ""
run-cleanup-at: "23:59"
cleanup-batch-size: 10
max-cleanup-retries: 10
log-queries: false
max-transaction-retries: 10
shards:
- connection-string: sqlite://task-manager.sqlite
days-to-keep: 180
space: "default"
key: "00000000-0000-0000-0000-000000000000"
```

3. Установите нужное значение параметра days-to-keep.

   Примечание
   Существенное изменение продолжительности периода хранения не рекомендуется: сильное уменьшение может привести к удалению незавершённых активностей, а сильное увеличение – к снижению производительности сервера управления.

4. Перезапустите службу Киберпротект Service Manager, как описано в разделе Использование сертификата, выданного доверенным центром сертификации.

В результате период хранения сведений о действиях будет изменён.

14.4 Отчёты

При наличии лицензии Кибер Бэкап Расширенная редакция в веб-консоли доступна вкладка **Отчёты**, на которой можно просматривать, создавать и настраивать отчёты.

В отчёт попадают те данные, которые отображаются с помощью элементов их визуального представления на панели мониторинга (виджетов). Отчёт можно сформировать, используя предустановленный набор виджетов или же задав собственный пользовательский набор. Для получения отчёта сохраните его в виде файла (файлы XLSX будут содержать исходные цифровые данные).

© ООО Киберпротект, 2026

Примечание

Вы можете настроить отчёты только для отделов, которыми вы управляете. Подробнее об управлении отделами см. в разделе "Управление учетными записями пользователей и отделами организации" (стр. 806).

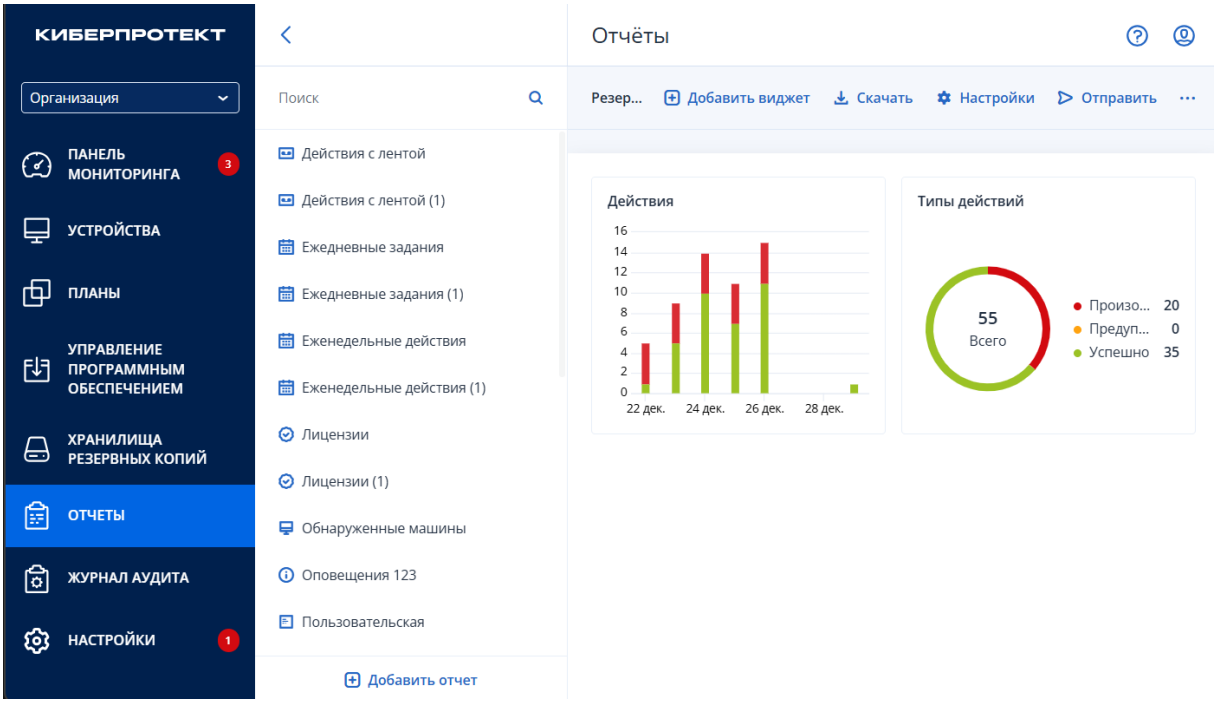
Отчёты могут быть отправлены по электронной почте или загружены по расписанию или по требованию. Для отправки отчётов по электронной почте убедитесь в том, что у вас сконфигурированы настройки Почтового сервера. При создании отчёта с использованием стороннего программного обеспечения настройте сохранение отчётов в формате XLSX в указанную папку.

14.4.1 Обзор вкладки "Отчёты"

В средней части окна программы отображается список созданных отчётов, отсортированный по их имени. Чтобы скрыть панель со списком отчётов, нажмите на иконку со стрелкой в верхней части панели. В результате список отчётов будет скрыт. Чтобы вернуть отображение списка отчётов, щёлкните иконку с тремя горизонтальными линиями (слева от слова "Отчёты").

В правой области окна программы для выбранного отчёта отображаются его элементы визуального представления данных в виде виджетов, а также меню действий с отчётом.

Общий вид вкладки **Отчёты** приведён на рисунке ниже.



14.4.2 Варианты отчётов

В таблице перечислены отчёты по умолчанию.

© ООО Киберпротект, 2026

Имя отчёта	Описание
Действия с лентой	Показывает список лент, которые использовались в течение последних 24 часов.
Ежедневные задания	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Еженедельные действия	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Лицензии	Показывает сводную информацию о доступных лицензиях.
Обнаруженные машины	Показывает все машины, обнаруженные в сети организации.
Оповещения	Показывает оповещения, выполненные за указанный период времени.
Хранилища	Показывает статистику использования хранилищ резервных копий за указанный период времени.
Резервные копии	Показывает подробную информацию о текущих резервных копиях и точках восстановления.
Сводка	Показывает сводную информацию об устройствах, защищённых за указанный период времени.
Текущий статус	Показывает текущий статус вашей среды.
Пользовательская	Позволяет создать пустой отчёт и настроить его.

14.4.3 Основные операции с отчётами

С отчётами можно выполнить следующие операции:

- просмотреть отчёт;
- добавить новый отчёт;
- добавить в отчёт элемент визуального представления данных;
- настроить порядок отображения в отчёте элементов визуального представления данных;
- удалить из отчёта элемент визуального представления данных;
- сохранить файл отчёта на текущей машине;
- переименовать отчёт;
- изменить диапазон времени для всех виджетов, включённых в отчёт;
- запланировать сохранение и (или) отправку отчёта по электронной почте;
- отправить файл отчёта по электронной почте по требованию;
- создать копию отчёта;

© ООО Киберпротект, 2026

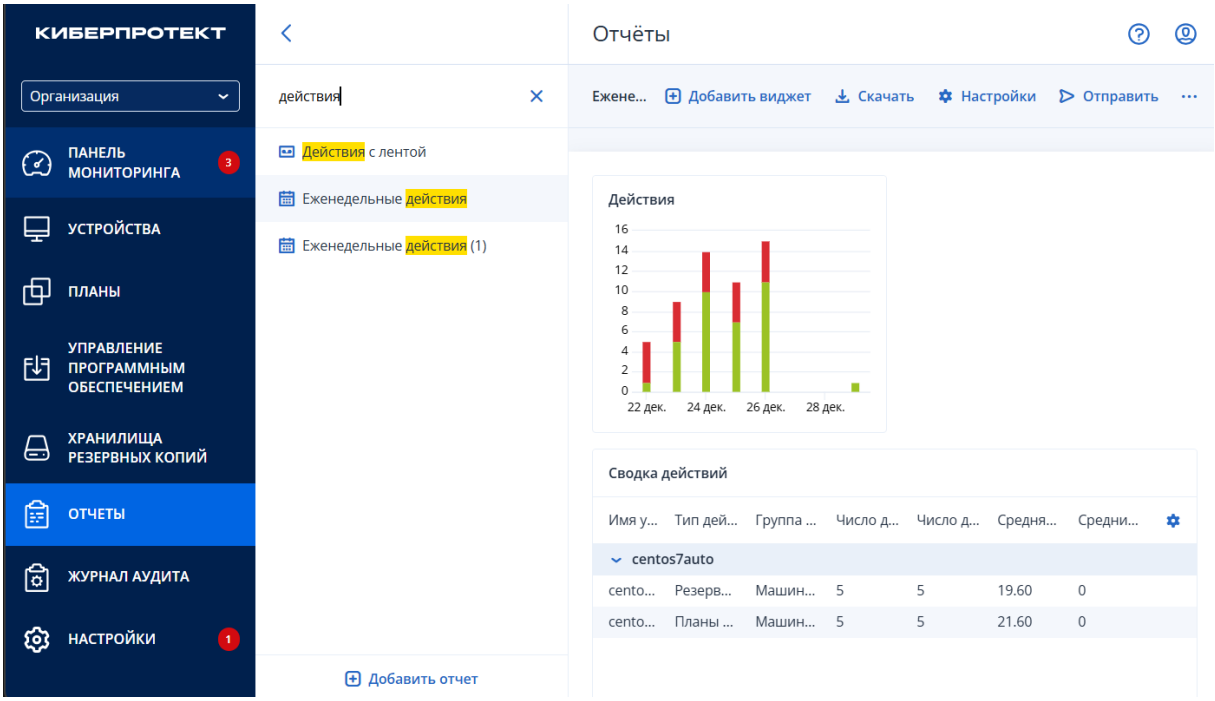
- экспортировать структуру отчёта;
- импортировать структуру отчёта;
- создать дамп данных отчёта;
- удалить отчёт.

14.4.3.1 Просмотр отчёта

Для просмотра отчёта щёлкните его имя в списке. В результате в правой области окна программы для выбранного отчёта будут отображены его элементы визуального представления данных в виде виджетов, а также меню действий с отчётом.

Виджеты являются интерактивными элементами. Например, некоторые из них позволяют получить больше информации при наведении курсора на отображаемые в диаграммах данные и нажатии на них.

Для поиска нужного отчёта введите его имя в строку поиска. Во время ввода будут отображаться отчёты, имя которых соответствует введённой комбинации символов.



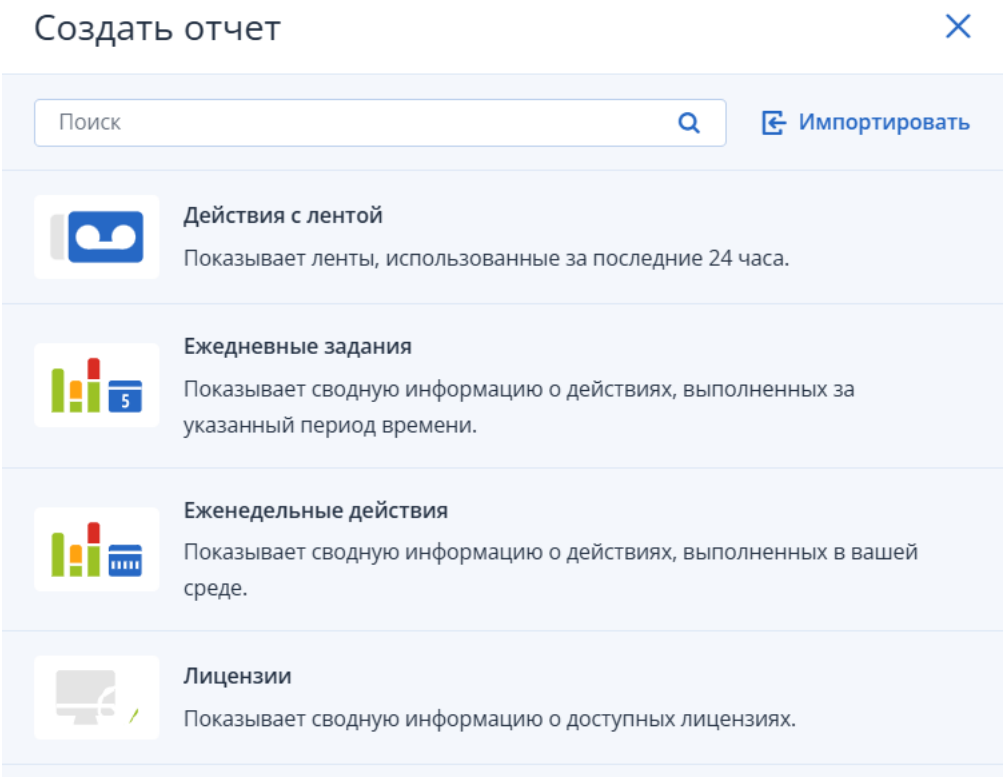
14.4.3.2 Порядок добавления отчёта

Вы можете добавить отчёт с предопределённым набором элементов визуального представления данных в виде виджетов или настроить пользовательский отчёт со своим набором.

Чтобы добавить отчёт, выполните следующие шаги:

1. В нижней части панели со списком отчётов щёлкните **Добавить отчёт**.
2. В открывшемся окне выберите тип отчёта, щёлкнув его имя.

© ООО Киберпротект, 2026



В результате новый отчёт будет добавлен, его имя будет отображено в списке отчётов, а в нижней правой части окна появится сообщение **Отчёт создан**.

Примечание
При создании отчёту присваивается имя по умолчанию, соответствующее выбранному типу отчёта. При необходимости отчёт можно переименовать (см. далее в статье).

Примечание
Структура отчёта типа **Пользовательская** не содержит предустановленных элементов визуального представления данных в виде виджетов, их необходимо добавить в отчёт самостоятельно (см. далее в статье).

14.4.3.3 Добавление в отчёт элемента визуального представления данных

Элементы визуального представления данных в виде виджетов можно добавить в любой отчёт, для этого выполните следующие шаги:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Добавить виджет**.
3. В открывшемся окне выберите виджет, щёлкнув его имя.
   В результате выбранный элемент визуального представления данных будет добавлен в интерфейс отчёта, а в нижнем правом углу окна программы появится всплывающее сообщение **Виджет добавлен**.

© ООО Киберпротект, 2026

Примечание
Новый элемент будет отображаться в верхней части отчёта. При необходимости его можно переместить (см. далее в статье).

4. [Необязательно] Настройте виджет, для этого нажмите кнопку **Настроить** в области выбранного виджета и выполните необходимые настройки.

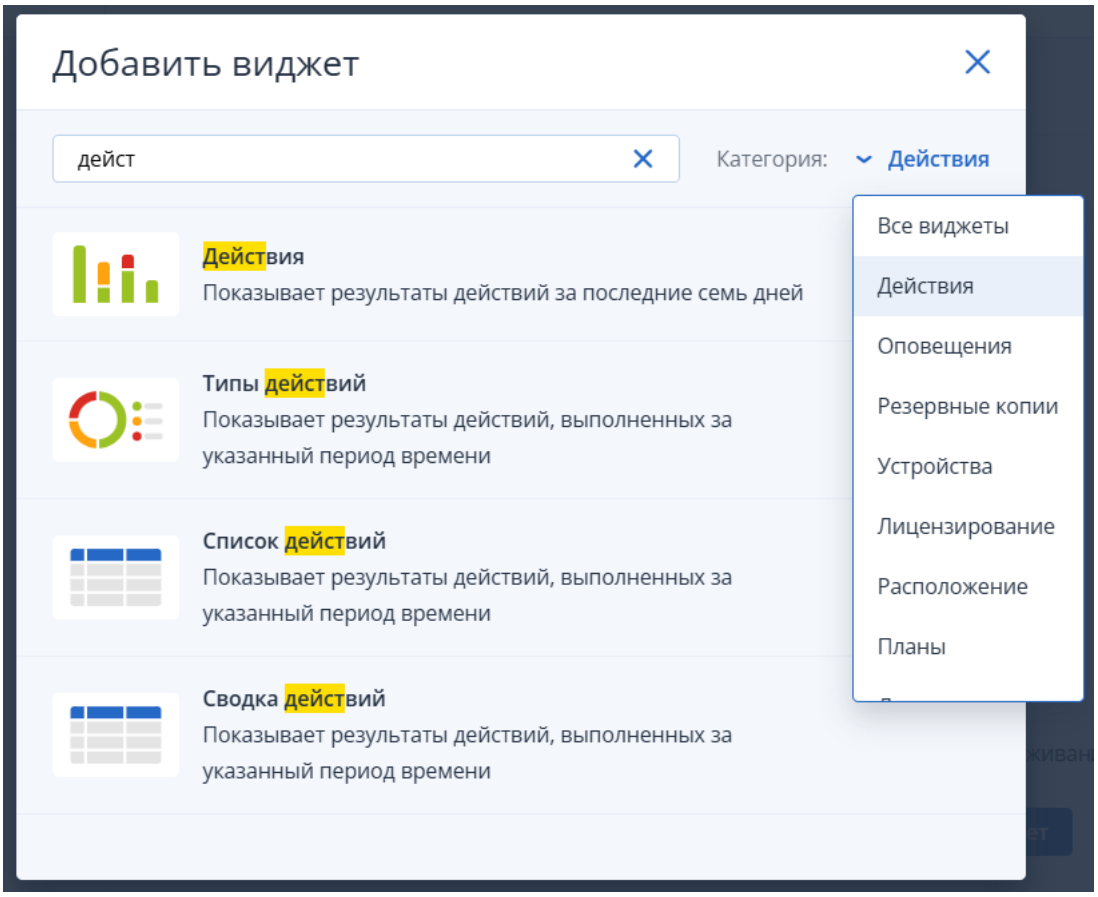
Примечание
Для разных видов виджетов предусмотрены различные настройки.

Для поиска виджета при его добавлении Вы можете:

- ввести его имя в строку поиска (во время ввода будут отображаться виджеты, имя которых соответствует введённой комбинации символов);
- настроить отображение виджетов определённой категории, выбрав её в выпадающем списке **Категория** в верхней правой части окна;
- просмотреть виджеты доступных категорий поочерёдно, щёлкнув по имени категории для разворачивания или сворачивания списка её виджетов.

Примечание
При использовании нескольких методов поиска виджета их условия применяются вместе. Например, при вводе названия виджета в строке поиска и выборе категории будут отображены виджеты, соответствующие обоим условиям.

© ООО Киберпротект, 2026



14.4.3.4 Настройка порядка отображения в отчёте элементов визуального представления данных

Чтобы настроить в отчёте порядок отображения элементов визуального представления данных, наведите курсор на название виджета и, зажав левую клавишу мыши, переместите его на новое место.

14.4.3.5 Удаление из отчёта элемента визуального представления данных

Чтобы удалить из отчёта элемент визуального представления данных, нажмите в его области значок крестика.

В результате элемент будет удалён, а внизу справа появится всплывающее сообщение **Виджет удалён**.

Примечание
Данную операцию можно отменить, нажав **Отмена** в области всплывающего сообщения.

14.4.3.6 Сохранение файла отчёта на текущей машине

Можно сохранить файл выбранного отчёта на машине, с помощью которой открыта веб-консоль. Для этого выполните следующие шаги:

© ООО Киберпротект, 2026

1. Нажмите кнопку **Скачать** на панели меню выбранного отчёта.
2. Выберите один из вариантов:
   - Excel и PDF (будут скачаны два файла: один в формате XLSX, другой – в формате PDF);
   - Excel (будет скачан один файл в формате XLSX);
   - PDF (будет скачан один файл в формате PDF).

   В результате выполненных действий отчёт будет сохранён на текущей машине.

14.4.3.7 Переименование отчёта

Чтобы переименовать отчёт, выполните следующие действия:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Настройки**.
3. Введите новое имя отчёта в поле **Имя**.
4. Нажмите кнопку **Сохранить**.

В результате выполненных действий отчёт будет переименован.

14.4.3.8 Изменение диапазона времени для всех элементов визуального представления данных, включённых в отчёт

Чтобы настроить отображение данных за определённый период времени в элементах визуального представления, выполните следующие шаги:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Настройки**.
3. Выберите значение в выпадающем списке **Диапазон**.
4. Нажмите кнопку **Сохранить**.

В результате в элементах визуального представления данных будет отображена информация за выбранный период времени.

14.4.3.9 Планирование сохранения и (или) отправки файла с отчётом по электронной почте

Сохранение файла с отчётом или отправка его по электронной почте, либо оба действия одновременно могут выполняться по установленному расписанию.

Для того чтобы установить расписание, выполните шаги:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Настройки**.
3. Переведите переключатель **Запланировано** в положение **Включено**.

© ООО Киберпротект, 2026

4. Установите флажки для требуемых действий (можно выбрать оба варианта):
   - **отправлять отчёт по электронной почте**;
   - **сохранить как файл на сервере управления**.

   В зависимости от выбора укажите адрес электронной почты, путь к папке или и то, и другое.

   Внимание
   Для отправки отчётов по электронной почте убедитесь в том, что у вас сконфигурированы настройки Почтового сервера.

5. Выберите формат формат отчёта: PDF, XLSX или и то, и другое.
6. Выберите язык в выпадающем списке (доступны русский и английский).
7. Настройте отчётный период (ежемесячно, еженедельно или ежедневно).
8. Укажите дни и время сохранения и (или) отправления отчёта.
9. Нажмите кнопку **Сохранить**.

14.4.3.10 Отправление файла с отчётом по электронной почте по требованию

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Отправить**.

Внимание
Для отправки отчётов по электронной почте убедитесь в том, что у вас сконфигурированы настройки Почтового сервера.

14.4.3.11 Создание копии отчёта

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите значок многоточия (...) в правом верхнем углу.
3. Выберите **Клонировать**.

В результате будет создана копия отчёта, его имя будет отображаться в списке отчётов, а в нижнем правом углу окна программы появится всплывающее сообщение **Отчёт создан**.

14.4.3.12 Экспорт структуры отчёта

Вы можете экспортировать структуру отчёта (набор виджетов и настройки расписания) в файл JSON. Это может оказаться полезным при переустановке сервера управления или для копирования структуры отчёта на другой сервер управления.

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите значок многоточия (...) в правом верхнем углу.

© ООО Киберпротект, 2026

3. Выберите **Экспорт**.

В результате на машине, с помощью которой открыта веб-консоль, будет будет сохранён файл JSON с параметрами отчёта.

14.4.3.13 Импорт структуры отчёта

Вы можете импортировать структуру отчёта (набор виджетов и настройки расписания) из файла JSON. Это может оказаться полезным при переустановке сервера управления или для копирования структуры отчёта из другого сервера управления.

Чтобы импортировать структуру отчёта, нажмите кнопку **Добавить отчёт** внизу списка отчётов. Затем в открывшемся окне нажмите **Импортировать** и выберите файл со структурой отчёта. В результате выполненных действий отчёт с импортированной структурой будет добавлен, а в нижнем правом углу окна программы появится всплывающее сообщение **Отчёт создан**.

14.4.3.14 Дамп данных отчёта

Вы можете сохранить дамп данных отчёта в файл CSV. Дамп содержит все данные отчёта (без фильтрации) за определённый промежуток времени.

ПО динамически генерирует дамп данных. При указании большого промежутка времени выполнение данного действия может занять продолжительное время.
Для сохранения дампа данных отчёта выполните шаги:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите значок многоточия (...) в правом верхнем углу.
3. Выберите **Данные дампа**.
4. В открывшемся окне в поле **Расположение** укажите путь к папке для файла CSV.
5. В поле **Диапазон времени** выберите диапазон времени.
6. Нажмите кнопку **Сохранить**.

В результате выполненных действий файл CSV будет сохранён в указанную папку.

14.4.3.15 Удаление отчёта

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите значок многоточия (...) в правом верхнем углу.
3. Выберите **Удалить отчёт**.
4. Подтвердите действие, нажав кнопку **Удаление** во всплывающем окне **Удалить отчёт**.

В результате выполненных действий отчёт будет удалён.

© ООО Киберпротект, 2026

14.5 Журнал аудита

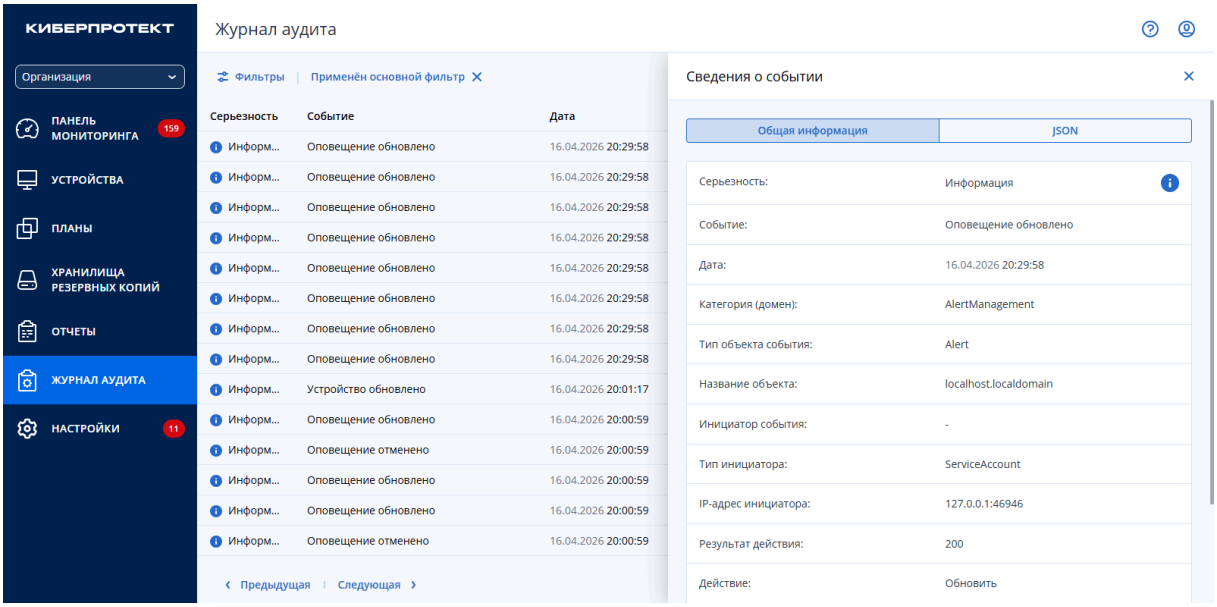
Журнал аудита содержит сведения о событиях, произошедших в Кибер Бэкап вследствие действий пользователей или работы системных компонентов (подробнее см. в разделе "Регистрируемые события" (стр. 743)).

По умолчанию журнал аудита хранится в базе данных продукта, однако при необходимости записи журнала можно отправлять на Syslog-сервер (см. "Отправка записей журнала аудита на Syslog-сервер" (стр. 804)).

Чтобы просмотреть список событий, перейдите в раздел **Журнал аудита**. Он доступен, только если включено сохранение событий аудита. События отображаются постранично с сортировкой по дате и времени в обратном порядке (от более новых к более старым). Для переключения между страницами используйте кнопки **< Предыдущая** и **Следующая >** внизу слева. Для настройки количества отображаемых записей журнала выберите значение в списке **Показывать строк:** или введите в поле ввода произвольное значение.

Для настройки отображения информации о событиях щёлкните шестерёнку вверху справа и в открывшемся окне установите или снимите флажки для выбранных столбцов. После этого внесённые изменения будут применены. Для закрытия окна щёлкните вне его области.

Для просмотра сведений о событии щёлкните по нему в списке.



На вкладке **Общая информация** будут отображены сведения о выбранном событии. При необходимости на вкладке **JSON** можно просмотреть подробные сведения о событии в формате JSON, а также скопировать их, нажав соответствующую кнопку.

Срок хранения записи в журнале – 90 дней. Записи, срок хранения которых истёк, удаляются автоматически. Кроме того, очистить журнал аудита можно вручную (см. "Управление журналом аудита" (стр. 804)).

© ООО Киберпротект, 2026

14.5.1 Основной поиск событий

Чтобы найти события с помощью основного поиска, выполните следующие действия:

1. Щёлкните **Фильтры** над списком событий и перейдите на вкладку **Основной**.
2. Укажите от одного до нескольких критериев поиска:
   - название отдела,
   - уровень важности события (можно выбрать от одного до нескольких значений в выпадающем списке, в котором приведены все возможные значения),
   - период времени (можно выбрать один из предопределённых периодов или вручную указать его начало и окончание),
   - тип объекта события (можно выбрать от одного до нескольких значений в выпадающем списке, в котором приведены все возможные значения),
   - объект события,
   - инициатор события,
   - тип инициатора события (можно выбрать от одного до нескольких значений в выпадающем списке, в котором приведены все возможные значения),
   - IP-адрес инициатора события.
3. Нажмите **Применить** для отображения результатов.

14.5.2 Расширенный поиск событий

Чтобы найти события с помощью расширенного поиска, выполните следующие действия:

1. Щёлкните **Фильтры** над списком событий и перейдите на вкладку **Расширенный**.
2. Введите поисковый запрос. Параметры и операторы, которые можно использовать в запросе, приведены в таблицах ниже.
3. Нажмите **Применить** для отображения результатов.

Кроме параметров и операторов, можно использовать круглые скобки для группировки условий поиска, например:

```
(status = '204' OR status = '200') AND action = 'Login'
```

Параметры расширенного поиска

Параметр	Описание	Примеры
uuid	Идентификатор события. Идентификатор можно узнать, просмотрев JSON-представление события.	• uuid = '0193c41a-6f13-7aa4-8448-2cad89f23385'
tenant_name	Название отдела.	• tenant_name = 'Accounting'

© ООО Киберпротект, 2026

Параметр	Описание	Примеры
src_ip	IP-адрес и порт инициатора события.	• src_ip LIKE '192.168.10.10%'
level	Уровень важности события. Возможные значения: • info – информация; • warning – предупреждение; • critical – критично; • error – ошибка.	• level = 'warning'
obj_name	Имя объекта события.	• obj_name = 'WIN2019X64-5\\Administrator'
obj_domain	Категория (область) события. Возможные значения можно узнать, просмотрев JSON-представления событий.	• obj_domain = 'TaskManagement'
obj_type	Название типа объекта события. Возможные значения можно узнать, просмотрев JSON-представления событий.	• obj_type = 'Task'
obj_subtype	Название подтипа объекта события. Возможные значения можно узнать, просмотрев JSON-представления событий.	• obj_subtype = 'Backup::Disks'
action	Название действия. Возможные значения можно узнать, просмотрев JSON-представления событий.	• action IN ('Login', 'Logout')
status	Результат действия.	• status = '200'
principal_type	Название типа инициатора события. Возможные значения: • User – инициатором события является пользователь; • ServiceAccount – инициатором события является системный компонент.	• principal_type = 'User'
principal_name	Имя инициатора события.	• principal_name LIKE '%admin%'
event.timestamp	Дата и время события. Операторы поиска **<**, **>**, **=**, **!=**, **IN**, **NOT IN** и **LIKE** не поддерживаются.	• event.timestamp <= '2024-11-30 12:00:00Z' • event.timestamp >= '2024-11-30 12:00:00Z'

Операторы расширенного поиска

Оператор	Описание	Примеры
<параметр> = <значение>	Оператор сравнения "равно".	• level = 'warning'

© ООО Киберпротект, 2026

Оператор	Описание	Примеры
<параметр> != <значение>	Оператор сравнения "не равно".	• level != 'info'
<параметр> < <значение>	Оператор сравнения "меньше".	• status < '400'
<параметр> > <значение>	Оператор сравнения "больше".	• status > '200'
<параметр> <= <значение>	Оператор сравнения "меньше или равно".	• event.timestamp <= '2024-11-30 12:00:00Z'
<параметр> >= <значение>	Оператор сравнения "больше или равно".	• event.timestamp >= '2024-11-30 12:00:00Z'
<выражение> AND <выражение>	Логический оператор "И".	• src_ip LIKE '192.168.10.10%' AND level = 'info'
<выражение> OR <выражение>	Логический оператор "ИЛИ".	• level = 'critical' OR level = 'warning'
<параметр> IN (<значение 1>, ..., <значение n>)	Проверяет, присутствует ли значение параметра в заданном наборе значений.	• level IN ('critical', 'warning')
<параметр> NOT IN (<значение 1>, ..., <значение n>)	Проверяет, отсутствует ли значение параметра в заданном наборе значений.	• level NOT IN ('critical', 'warning')
<параметр> LIKE <шаблон значения>	Проверяет, соответствует ли значение параметра указанному шаблону (регистр символов не учитывается). В шаблоне можно использовать знак процента (**%**), который подменяет любую, в том числе и пустую, последовательность символов.	• principal_name LIKE '%admin%'

14.5.3 Использование сохранённых поисковых запросов

Чтобы сохранить поисковый запрос, нажмите **Сохранить как шаблон**, введите имя и при необходимости описание запроса и нажмите **Сохранить**.

Сохранённый запрос можно выполнить, выбрав его в поле **Шаблон фильтрации** и нажав **Применить**. Для удаления сохраненного запроса щёлкните значок корзины рядом с его именем и нажмите **Удалить** в окне подтверждения удаления.

© ООО Киберпротект, 2026

14.5.4 Регистрируемые события

В журнале аудита Кибер Бэкап фиксируются события следующих категорий:

- назначение статусов оповещениям;
- регистрация агентов;
- аутентификация и авторизация;
- действия с планами защиты;
- действия с устройствами и их группами;
- резервное копирование;
- действия с пользователями и группами;
- действия с хранилищами;
- действия с архивами.

Более подробная информация о записываемых в журнал событиях приведена в таблицах ниже.

14.5.4.1 События назначения статусов оповещениям

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Оповещение создано (Alert created)	Информация (info)	Имя ресурса	Alert	-	200
Оповещение обновлено (Alert updated)	Информация (info)	Имя ресурса	Alert	-	200
Оповещение отменено (Alert reset)*	Информация (info)	Имя ресурса	Alert	Имя пользователя	204

* При использовании массового действия с оповещениями, например, **Очистить всё**, для каждого оповещения будет создана отдельная запись в журнале аудита.

14.5.4.2 События регистрации агентов

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Регистрация агента завершена (Agent registration complete)	Информация (info)	Имя агента (имя хоста)	Agent	-	200
Регистрация агента	Информация	Имя агента	Agent	-	200

© ООО Киберпротект, 2026

отозвана (Agent unregistered) **Примечание** При отмене регистрации через командную строку или при удалении продукта.	(info)	(имя хоста)			
Регистрация агента отозвана (Agent unregistered) **Примечание** При удалении машины через веб-консоль (подробнее см. в разделе "Удаление продукта" (стр. 208)).	Информация (info)	Имя агента (имя хоста)	Agent	Имя пользователя, инициировавшего удаление агента	200

14.5.4.3 События аутентификации и авторизации

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Успешный вход в систему (Logged in)	Информация (info)	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	Session	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	200
Не удалось войти в систему (Fail to log in)	Предупреждение (warning)	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	Session	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	401
Успешный выход из системы (Logged out)	Информация (info)	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux:	Session	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux:	200

© ООО Киберпротект, 2026

		имя пользователя.		имя пользователя.	

14.5.4.4 События при действиях с планами защиты

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
План защиты создан (Backup plan created)	Информация (info)	Имя плана	Policy	Имя пользователя	20x
План защиты обновлён (Backup plan updated)	Информация (info)	Имя плана	Policy	Имя пользователя	20x
План защиты удалён (Backup plan deleted)	Информация (info)	Имя плана	Policy	Имя пользователя	204
Статус установки плана (Plan deployment state)	Информация (info)	Имя плана	Policy	-	200
Политика применена к устройству (Policy applied to workload)	Информация (info)	Имя плана	PolicyApplication	Имя пользователя	20x

14.5.4.5 События при действиях с устройствами и их группами

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Устройство создано (Workload created)	Информация (info)	Имя ресурса	Workload	-	200
Устройство обновлено (Workload updated)	Информация (info)	Имя ресурса	Workload	-	200
Устройство удалено (Workload deleted)	Информация (info)	Имя ресурса	Workload	-	200

© ООО Киберпротект, 2026

Группа устройств создана (Workload group created)	Информация (info)	Имя группы	GroupMembership	Имя пользователя	201
Участники добавлены в статическую группу устройств (Workload static group member added)	Информация (info)	Имя группы	GroupMembership	-	200
Участники добавлены в динамическую группу устройств (Workload dynamic group member added)	Информация (info)	Имя группы	GroupMembership	-	200
Участники удалены из статической группы устройств (Workload static group member removed)	Информация (info)	Имя группы	GroupMembership	-	200
Участники удалены из динамической группы устройств (Workload dynamic group member removed)	Информация (info)	Имя группы	GroupMembership	-	200
Группа устройств удалена (Workload group deleted)	Информация (info)	Имя группы	GroupMembership	Имя пользователя	200

14.5.4.6 События резервного копирования

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия

© ООО Киберпротект, 2026

Резервное копирование помещено в очередь (Backup queued)	Информация (info)	Имя ресурса	Task	Если тип инициатора – **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора – **ServiceAccount**: '-'.	200
Резервное копирование назначено агенту (Backup assigned to agent)	Информация (info)	Имя ресурса	Task	Если тип инициатора – **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора – **ServiceAccount**: '-'.	200
Ошибка при назначении резервного копирования агенту (Error assigning backup to agent)	Предупреждение (warning), если задача завершена с кодом warning. Критично (critical)*, если задача завершена с кодом error.	Имя ресурса	Task	Имя пользователя	500
Резервное копирование начато (Backup started)	Информация (info)	Имя ресурса	Task	Если тип инициатора – **User**: • имя хоста и имя пользователя	200

© ООО Киберпротект, 2026

				(для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора – **ServiceAccount**: '-'.	
Резервное копирование выполнено (Backup completed)	Информация (info)	Имя ресурса	Task	Если тип инициатора – **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора – **ServiceAccount**: '-'.	200
Резервное копирование завершилось с предупреждением (Backup finished with warning)	Предупреждение (warning), если задача завершена с кодом warning. Критично (critical)*, если задача завершена с кодом error.	Имя ресурса	Task	Если тип инициатора – **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора – **ServiceAccount**: '-'.	200
Резервное копирование завершилось с ошибкой (Backup failed)	Предупреждение (warning), если задача завершена с кодом warning. Критично (critical)*, если задача	Имя ресурса	Task	Если тип инициатора – **User**: • имя хоста и имя пользователя	500

© ООО Киберпротект, 2026

	завершена с кодом error.			(для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора – **ServiceAccount**: '-'.	
Задача на восстановление создана (Recovery task created)	Информация (info)	-	Activity	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	200
Задача на восстановление запущена (Recovery task started)	Информация (info)	Имя ресурса	Activity	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	200
Задача на восстановление выполнена (Recovery task completed)	Информация (info)	Имя ресурса	Activity	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	200

14.5.4.7 События действий с пользователями и группами

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Изменение привилегий пользователя/группы (User/group privileges updated)	Информация (info)	-/BUILTIN (для группы Administrators)	UserPrivileges	Имя пользователя	200

14.5.4.8 События действий с хранилищами

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Хранилище создано (Storage	Информация (info)	Имя хранилища	Vault	-	200

© ООО Киберпротект, 2026

created)					
Хранилище обновлено (Storage updated)	Информация (info)	Имя хранилища	Vault	• Имя пользователя (если тип инициатора – **User**); • '-' (если тип инициатора – **ServiceAccount**).	200
Хранилище удалено (Storage deleted)	Информация (info)	Имя хранилища	Vault	-	200

14.5.4.9 События действий с архивами

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Архив создан (Archive created)	Информация (info)	Имя файла резервной копии	Archive	-	200
Архив обновлён (Archive updated)	Информация (info)	Имя файла резервной копии	Archive	-	200
Архив удалён (Archive deleted)	Информация (info)	Имя файла резервной копии	Archive	-	200
Точка восстановления создана (Recovery point created)	Информация (info)	Имя точки восстановления*	RecoveryPoint	-	200
Точка восстановления удалена (Recovery point deleted)	Информация (info)	Имя точки восстановления*	RecoveryPoint	-	200

* Имя точки восстановления в формате <ГГГГ>-<ММ>-<ДД> <чч>:<мм>:<сс> <смещение> UTC.

В этом выражении:

- <ГГГГ> – год четырьмя цифрами (например, 2026).
- <ММ> – месяц двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 06).
- <ДД> – день двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 02).

© ООО Киберпротект, 2026

- <чч> – часы двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 09).
- <мм> – минуты двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 07).
- <сс> – минуты двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, 05).
- <смещение> – смещение времени относительно UTC (например, +0000).

Пример имени точки восстановления: 2026-06-02 09:07:05 +0000 UTC.

14.6 Настройка внешнего мониторинга

Кибер Бэкап позволяет с помощью OpenTelemetry Collector передавать различные данные телеметрии в системы внешнего мониторинга.

Далее в разделе будет рассмотрена настройка для системы мониторинга Grafana.

Настройка состоит из следующих шагов:

1. Создание учётной записи администратора с ролью **Оператор мониторинга** (см. раздел "Отделы и административные учетные записи" (стр. 806)).
2. Настройка OpenTelemetry Collector.
3. Настройка источников данных для системы мониторинга (см. разделы "Настройка Prometheus в качестве источника данных" (стр. 753) и "Настройка Grafana Loki в качестве источника данных" (стр. 757)).
4. Настройка системы мониторинга Grafana (см. раздел "Настройка системы мониторинга Grafana" (стр. 761)).

14.6.1 Настройка OpenTelemetry Collector

Настройка производится на машине с сервером управления Кибер Бэкап и состоит из следующих шагов:

- Настройка Memory Limiter. Memory Limiter позволяет OpenTelemetry Collector корректно работать с данными телеметрии, не выходя при этом за рамки потребления оперативной памяти.
- Настройка данных телеметрии. В данные телеметрии необходимо добавить специальные метаданные для её идентификации в системах внешнего мониторинга.

14.6.1.1 Настройка Memory Limiter

1. Откройте конфигурационный файл config.yml:
   - в ОС Linux: /usr/lib/Acronis/OpenTelemetryCollector/config.yml;
   - в ОС Windows: C:\Program Files\Acronis\OpenTelemetryCollector\config.yml.
2. Измените значения параметров memory_limiter на следующие:

© ООО Киберпротект, 2026

```
processors:
  memory_limiter:
    check_interval: 1s
    limit_mib: 500
    spike_limit_mib: 100
```

3. Добавьте параметр memory_limiter в раздел service.pipelines:

```
service:
  pipelines:
    metrics:
      receivers: [otlp]
      processors: [batch, memory_limiter]
      exporters: [file/metrics]
    logs:
      receivers: [otlp]
      processors: [batch, memory_limiter]
      exporters: [file/metrics]
```

Внимание
memory_limiter необходимо добавить и для metrics, и для logs.

14.6.1.2 Настройка данных телеметрии

1. Откройте конфигурационный файл config.yml:
   - в ОС Linux: /usr/lib/Acronis/OpenTelemetryCollector/config.yml;
   - в ОС Windows: C:\Program Files\Acronis\OpenTelemetryCollector\config.yml.
2. Добавьте параметр resource в раздел Processor:

```
processors:
  resource:
    attributes:
    - key: ru.cyberprotect.cb.stand.name
      action: upsert
      value: YOUR_VALUE
```

где ru.cyberprotect.cb.stand.name и YOUR_VALUE – метаданные, по которым системы внешнего мониторинга смогут идентифицировать метрики и записи журналов.

Внимание
Значения метаданных должны быть уникальны и при этом иметь низкую кардинальность.

3. Добавьте параметр resource в раздел service:pipelines:

```
service:
  pipelines:
    metrics:
      receivers: [otlp]
```


© ООО Киберпротект, 2026

```
    processors: [batch, memory_limiter, resource]
    exporters: [file/metrics]
  logs:
    receivers: [otlp]
    processors: [batch, memory_limiter, resource]
    exporters: [file/metrics]
```

Внимание
resource необходимо добавить и для metrics, и для logs.

14.6.2 Настройка Prometheus в качестве источника данных

Настройка Prometheus в качестве источника данных состоит из следующих шагов:

1. Настройка OpenTelemetry Collector для предоставления двух специальных точек доступа (далее – конечная точка) /metrics:
   - с метриками сервера управления Кибер Бэкап;
   - с метриками внутренней телеметрии.
2. Настройка Node Exporter или Windows Exporter в зависимости от используемой ОС.
3. Настройка Prometheus для сбора метрик.

14.6.2.1 Настройка OpenTelemetry Collector

Добавление конечной точки с метриками сервера управления Кибер Бэкап

1. Откройте конфигурационный файл config.yml:
   - в ОС Linux: /usr/lib/Acronis/OpenTelemetryCollector/config.yml;
   - в ОС Windows: C:\Program Files\Acronis\OpenTelemetryCollector\config.yml.
2. Добавьте в раздел exporters конечную точку:

```
exporters:
  prometheus:
    endpoint: 0.0.0.0:8889
    resource_to_telemetry_conversion:
      enabled: true
```

   где 0.0.0.0:8889 – строка, указывающая IP-адрес и порт для конечной точки /metrics.
3. Добавьте конечную точку в раздел service.pipelines:

```
service:
  pipelines:
    metrics:
      receivers: [otlp]
      processors: [batch, memory_limiter, resource]
      exporters: [file/metrics, prometheus]
```


© ООО Киберпротект, 2026

Теперь основные метрики OpenTelemetry Collector доступны на конечной точке /metrics в стандартом формате Prometheus.

Добавление конечной точки для внутренней телеметрии

OpenTelemetry Collector может предоставлять различную информацию о своей работе в виде метрик. Это позволяет наблюдать за его работой и реагировать на проблемы.

Для настройки внутренней телеметрии:

1. Откройте конфигурационный файл config.yml:
   - в ОС Linux: /usr/lib/Acronis/OpenTelemetryCollector/config.yml;
   - в ОС Windows: C:\Program Files\Acronis\OpenTelemetryCollector\config.yml.
2. Добавьте в раздел service.telemetry данные конечной точки:

```
service:
  telemetry:
    resource:
      ru.cyberprotect.cb.stand.name: YOUR_VALUE
```

Внимание
YOUR_VALUE – значение атрибута ru.cyberprotect.cb.stand.name, указанное при настройке данных телеметрии (см. подраздел "Настройка данных телеметрии" в разделе "Настройка внешнего мониторинга" (стр. 751)).

Теперь внутренние метрики OpenTelemetry Collector будут доступны по адресу http://127.0.0.1:8888/metrics.

При необходимости укажите IP-адрес и порт для конечной точки в разделе service.telemetry:

```
service:
  telemetry:
    resource:
      ru.cyberprotect.cb.stand.name: YOUR_VALUE
    metrics:
      readers:
        - pull:
            exporter:
              prometheus:
                host: '0.0.0.0'
                port: 8890
```

Внимание
YOUR_VALUE – значение атрибута ru.cyberprotect.cb.stand.name, указанное при настройке данных телеметрии (см. подраздел "Настройка данных телеметрии" в разделе "Настройка внешнего мониторинга" (стр. 751)).

host и port – IP-адрес и порт, по которым доступна конечная точка /metrics.

© ООО Киберпротект, 2026

Перезапустите службу сервера управления Кибер Бэкап.

14.6.2.2 Настройка Node Exporter

В ОС Linux для сбора различных системных метрик вроде загрузки ЦП, использования памяти и сетевой статистики можно использовать специальный инструмент – Node Exporter.

Скачайте актуальную версию Node Exporter, распакуйте и запустите:

```
# NOTE: Replace the URL with one from the above mentioned "downloads" page.
# Node Exporter is available for multiple OS targets and architectures.
# Downloads are available at:
# https://github.com/prometheus/node_exporter/releases/download/v<VERSION>/node_exporter-
<VERSION>.<OS>-<ARCH>.tar.gz
#
# <VERSION>, <OS>, and <ARCH> are placeholders:
# - <VERSION>: Release version (e.g., 1.10.2)
# - <OS>: Operating system (e.g., linux, darwin, freebsd)
# - <ARCH>: Architecture (e.g., amd64, arm64, 386)
#
# For this example, we will use Node Exporter version 1.10.2 for a Linux system with amd64
architecture.

wget https://github.com/prometheus/node_exporter/releases/download/v1.10.2/node_exporter-
1.10.2.linux-amd64.tar.gz
tar xvfz node_exporter-1.10.2.linux-amd64.tar.gz
cd node_exporter-1.10.2.linux-amd64
./node_exporter
```

Все необходимые коллекторы для сбора метрик базовой контрольной панели включены по умолчанию. После запуска Node Exporter будет предоставлять метрики на конечной точке /metrics через порт 9100.

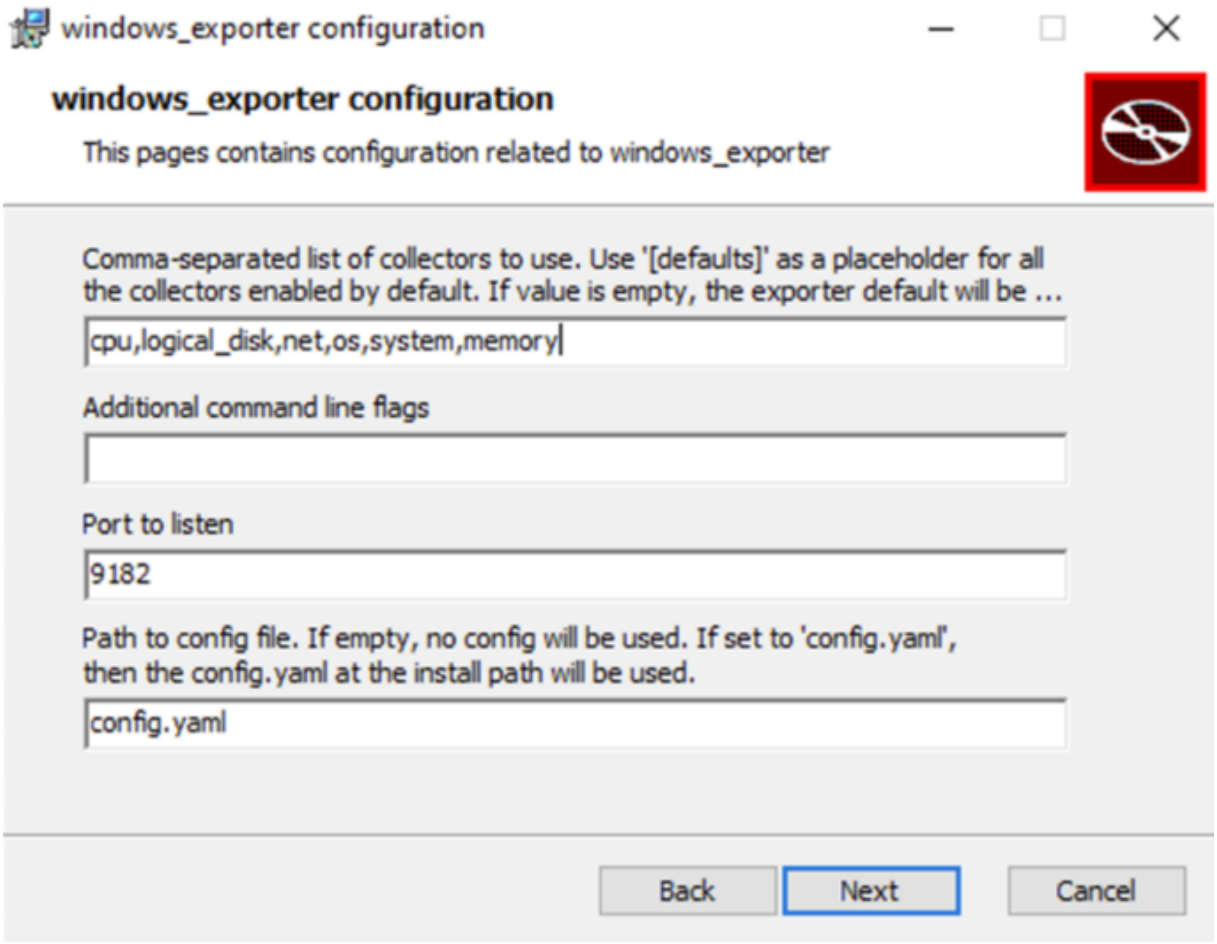
14.6.2.3 Настройка Windows Exporter

В ОС Windows для сбора различных системных метрик вроде загрузки ЦП, использования памяти и сетевой статистики можно использовать специальный инструмент – Windows Exporter.

Windows Exporter распространяется в виде .msi-установщика; скачайте актуальную версию и установите.

При установке укажите необходимые для работы коллекторы (через запятую): cpu, logical_disk, net, os, system, memory и укажите порт (по умолчанию 9182):

© ООО Киберпротект, 2026



После установки Windows Exporter будет предоставлять метрики на конечной точке /metrics через порт 9182.

14.6.2.4 Настройка Prometheus для сбора метрик

Добавьте параметры метрик в Prometheus. Например, при использовании ОС Linux:

```
scrape_configs:
  - job_name: 'cb-otel-collector'
    static_configs:
      - targets: ['otel-collector:8889']
    metrics_path: '/metrics'

  - job_name: 'cb-otel-collector-internal-telemetry'
    static_configs:
      - targets: ['otel-collector:8888']
    metrics_path: '/metrics'

  - job_name: 'cb-node-exporter'
    static_configs:
      - targets: ['node-exporter:9100']
    metrics_path: '/metrics'
```


© ООО Киберпротект, 2026

При использовании ОС Windows вместо cb-node-exporter укажите cb-windows-exporter с соответствующим портом 9182:

```
scrape_configs:
 - job_name: 'windows-node-exporter'
   static_configs:
    - targets: ['windows-exporter:9182']
   metrics_path: '/metrics'
```

Внимание
Значения otel-collector, node-exporter и windows-exporter необходимо заменить на действительные IP-адреса.

Перезапустите Prometheus:

```
# systemctl reload prometheus
```

В результате Prometheus будет собирать все необходимые метрики.

14.6.3 Настройка Grafana Loki в качестве источника данных

Настройка Grafana Loki в качестве источника данных состоит из двух шагов:

1. Настройка OpenTelemetry Collector для экспорта записей журналов в Grafana Loki.
2. Настройка Grafana Loki для корректного приёма записей журналов от OpenTelemetry Collector.

14.6.3.1 Настройка OpenTelemetry Collector для экспорта записей журналов в Grafana Loki

Настройка для Grafana Loki без аутентификации

1. Откройте конфигурационный файл config.yml:
   - в ОС Linux: /usr/lib/Acronis/OpenTelemetryCollector/config.yml;
   - в ОС Windows: C:\Program Files\Acronis\OpenTelemetryCollector\config.yml.
2. Добавьте OTLP-экспортер для Grafana Loki в раздел exporters:

   ```
   exporters:
    otlphttp/loki:
     endpoint: http://<loki-addr>/otlp
   ```

   Где http://<loki-addr>/otlp URL-адрес Grafana Loki.
3. Включите OTLP-экспортер в раздел service.pipelines:

   ```
   service:
    pipelines:
     logs:
   ```


© ООО Киберпротект, 2026

```
    receivers: [..., filelog/task-manager, filelog/alert-manager]
    processors: [..., batch, memory_limiter, resource]
    exporters: [..., otlphttp/loki]
```

В строке receivers укажите службы, которые будут отправлять записи журналов в Grafana Loki. Список доступных служб указан ниже.

В строке processors необходимо добавить batch, memory_limiter и resource.

Перезапустите службу сервера управления Кибер Бэкап.

Настройка для Grafana Loki с аутентификацией

1. Откройте конфигурационный файл config.yml:
   - в ОС Linux: /usr/lib/Acronis/OpenTelemetryCollector/config.yml;
   - в ОС Windows: C:\Program Files\Acronis\OpenTelemetryCollector\config.yml.
2. Добавьте расширение basicauth в конфигурацию:

```
extensions:
  basicauth/otlp:
    client_auth:
      username: username
      password: password
```

3. Включите OTLP-экспортер с указанием расширения basicauth в раздел exporters:

```
exporters:
  otlphttp/loki:
    auth:
      authenticator: basicauth/otlp
    endpoint: http://<loki-addr>/otlp
```

   Где http://<loki-addr>/otlp URL-адрес Grafana Loki.
4. Включите OTLP-экспортер в раздел service.pipelines:

```
service:
  extensions: [basicauth/otlp]
  pipelines:
    logs:
      receivers: [..., filelog/task-manager, filelog/alert-manager]
      processors: [..., batch, memory_limiter, resource]
      exporters: [..., otlphttp/loki]
```

   В строке receivers укажите службы, которые будут отправлять записи журналов в Grafana Loki. Список доступных служб указан ниже.

   В строке processors необходимо добавить batch, memory_limiter и resource.

Перезапустите службу сервера управления Кибер Бэкап.

© ООО Киберпротект, 2026

14.6.3.2 Настройка Grafana Loki для корректного приема записей журналов от OpenTelemetry Collector

Актуальные версии Loki поддерживают формат OpenTelemetry для приёма записей журналов. Для корректного приема записей журналов в Loki должна быть включена работа с структурированными метаданными (по умолчанию включено в Loki 3.0 и более поздних версиях).

Установите параметр allow_structured_metadata в значение true в конфигурационном файле Loki:

```
limits_config:
  allow_structured_metadata: true
```

14.6.3.3 Список служб, которые можно добавить для отправки записей журналов в Grafana Loki

Ниже перечислены службы, которые можно добавить в список для отправки записей журналов в Grafana Loki:

Служба	Строка для добавления службы	Описание
AccountServer	filelog/account-server	Управляет доступом и лицензированием
AgentGateway	filelog/agent-gateway	Прослушивает входящие регистрации агентов
AgentManager	filelog/agent-manager	Управляет машинами зарегистрированных агентов
AlertManager	filelog/alert-manager	Хранит информацию об оповещениях
AMS	filelog/ams-without-level, filelog/ams-with-level	Осуществляет централизованное управление агентами
ApiGateway	filelog/api-gateway	Выступает единой точкой входа в сеть, обеспечивает маршрутизацию, аутентификацию и управление сессиями
AppBackupGrpmAddon	filelog/app-backup-grpm-addon	Дополнение GRPM для резервного копирования приложений
ArchiveServer	filelog/archive-server_json, filelog/archive-	Предоставляет REST API для работы с архивами и элементами внутри архивов; используется только в сценариях интеграции с хранилищем на базе Кибер

© ООО Киберпротект, 2026

	server_plain-text	Инфраструктуры
BackupAssistantGrpmAddon	filelog/backup-assistant-grpm-addon	Дополнение GRPM для планов защиты (файлы, диски, машины)
BackupManager	filelog/backup-manager	Отвечает за управление ресурсами и политиками в обобщённом виде
CatalogManager	filelog/catalog-manager	Является частью функции поиска. Отвечает за проверку поисковых запросов и назначение их браузеру каталога. REST API в основном задействуется при использовании графического интерфейса пользователя (веб-консоль)
CredStore	filelog/cred-store	Управление секретами
EventStore	filelog/event-store	Отвечает за чтение событий из очереди с последующим сохранением их в своей БД и отправкой в SIEM. Является частью аудит-системы
FilerManager	filelog/filer-manager	Служба управления сетевыми хранилищами данных. На текущий момент поддерживает работу с SAN (Storage Area Network)
GrpmAtpAddon	filelog/grpm-atp-addon	Отвечает за реализацию внутреннего GRPM API для политик активной защиты
LegacyAppsService	filelog/legacy-apps-service	Дополнение GRPM для резервного копирования данных Microsoft Exchange Server и Microsoft SQL Server
MonitoringCollector	filelog/monitoring-collector	Участвует в системе мониторинга Кибер Бэкап
MonitoringServer	filelog/monitoring-server	Участвует в системе мониторинга Кибер Бэкап
NatsServer	filelog/nats-server	Отвечает за журнал аудита в Кибер Бэкап
Scheduler	filelog/scheduler	Служба управления расписаниями
ServiceManager	filelog/service-manager	Обеспечивает работу служб сервера управления Кибер Бэкап
TaskManager	filelog/task-manager	API для очереди задач, управления жизненным циклом задач и их шагов, доступа и поиска задач
TcpTunnels	filelog/tcp-tunnels	Набор служб для управления TCP-туннелями и другими WebSocket-соединениями (или другими прокси-серверами)
UpdateService	filelog/update-	Предоставляет информацию о доступных версиях

© ООО Киберпротект, 2026

	service	Кибер Бэкап
VaDeployer	filelog/va-deployer	Отвечает за развертывание виртуальных устройств со стороны службы управления
VaultManager	filelog/vault-manager	Отвечает за метаинформацию о хранилищах, архивах и резервных копиях, отслеживает согласованность данных и управляет соответствующими операциями (CRUD)
WebServer	filelog/web-server	Используется для передачи запросов к центральному серверу управления
WsProxy	filelog/ws-proxy	Набор служб для управления TCP-туннелями
ZmqGw	filelog/zmq-gw-without-level, filelog/zmq-gw-with-level	Обеспечивает связь между агентами и сервером управления Кибер Бэкап

14.6.4 Настройка системы мониторинга Grafana

Для корректной работы системы мониторинга Grafana с Кибер Бэкап необходимо выполнить следующие действия:

1. Установить плагин Infinity (скачайте плагин с официального сайта).
2. Создать и настроить источники данных для панели мониторинга.
3. Произвести импорт и настройку панели мониторинга.

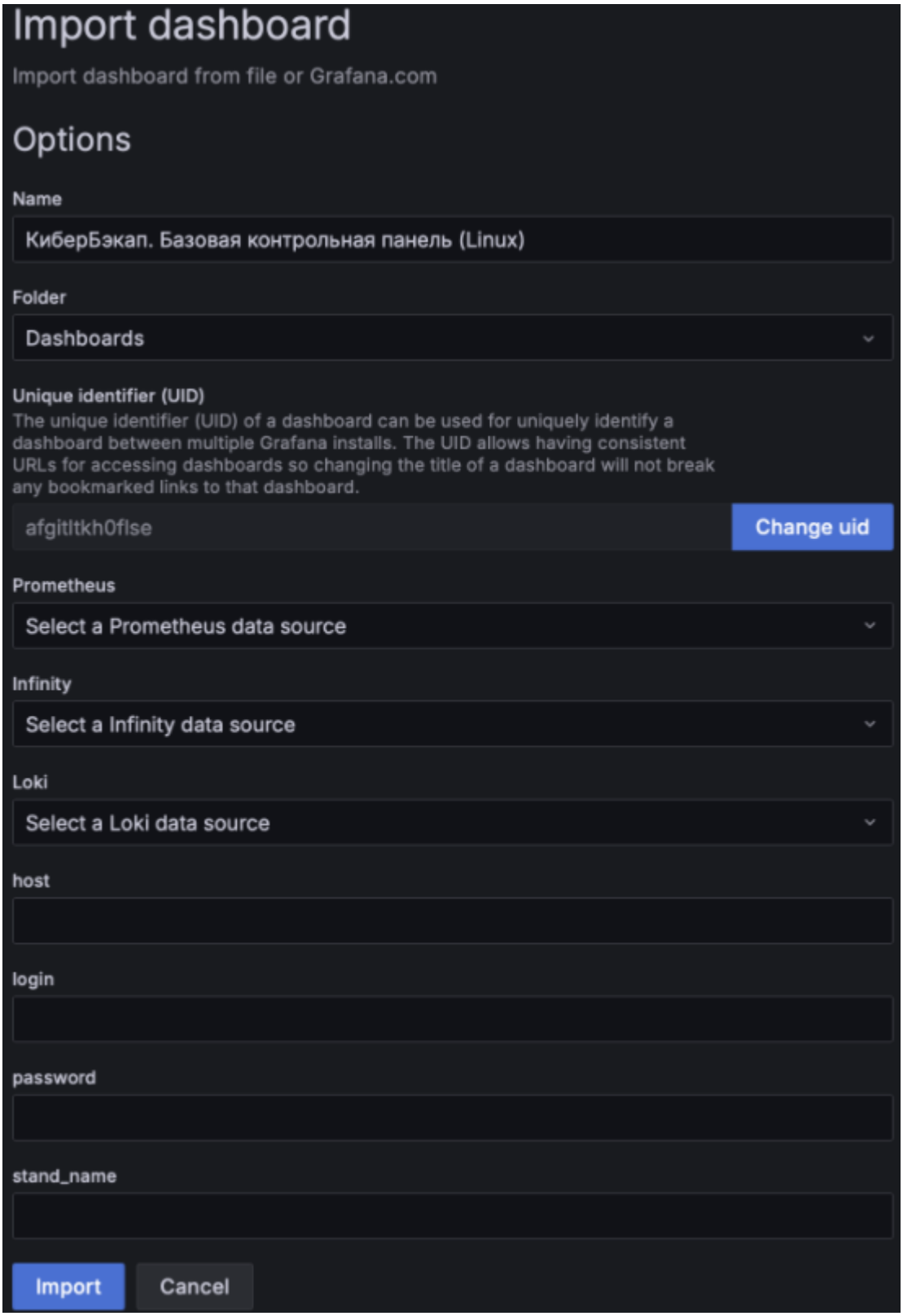
14.6.4.1 Создание и настройка источников данных для панели мониторинга

- Создайте источник данных Infinity. Для создания обратитесь к документации разработчика).
- Создайте источник данных Prometheus (см. раздел "Настройка Prometheus в качестве источника данных" (стр. 753)).
- Создайте источник данных Grafana Loki и подключите его к экземпляру Grafana Loki (см. раздел "Настройка Grafana Loki в качестве источника данных" (стр. 757)).

14.6.4.2 Импорт и настройка панели мониторинга

1. Скачайте файл с панелью мониторинга в зависимости от ОС, на которой работает сервер управления Кибер Бэкап:
   - ОС Linux;
   - ОС Windows.
2. Импортируйте панель мониторинга в платформу Grafana с помощью стандартного механизма платформы.
3. Заполните поля меню импорта.

© ООО Киберпротект, 2026



- **Name**. Укажите наименование панели мониторинга.
- **Folder**. Укажите папку, в которую будет импортирована панель мониторинга.
- **Prometheus**. Выберите из выпадающего списка источник данных, связанный с вашим экземпляром Prometheus.

© ООО Киберпротект, 2026

- **Infinity**. Выберите из выпадающего списка источник данных Infinity.
- **Loki**. Выберите из выпадающего списка источник данных, связанный с вашим экземпляром Grafana Loki.
- **host**. Укажите адрес и порт веб-консоли Кибер Бэкап. Например, http://host:9877
- **login**. Укажите имя учетной записи с ролью **Оператор мониторинга** (см. раздел "Отделы и административные учетные записи" (стр. 806)).
- **password**. Укажите пароль от учетной записи с ролью **Оператор мониторинга**.
- **stand_name**. Введите значение атрибута ru.cyberprotect.cb.stand.name, указанное при настройке данных телеметрии (см. подраздел "Настройка данных телеметрии" в разделе "Настройка внешнего мониторинга" (стр. 751)).

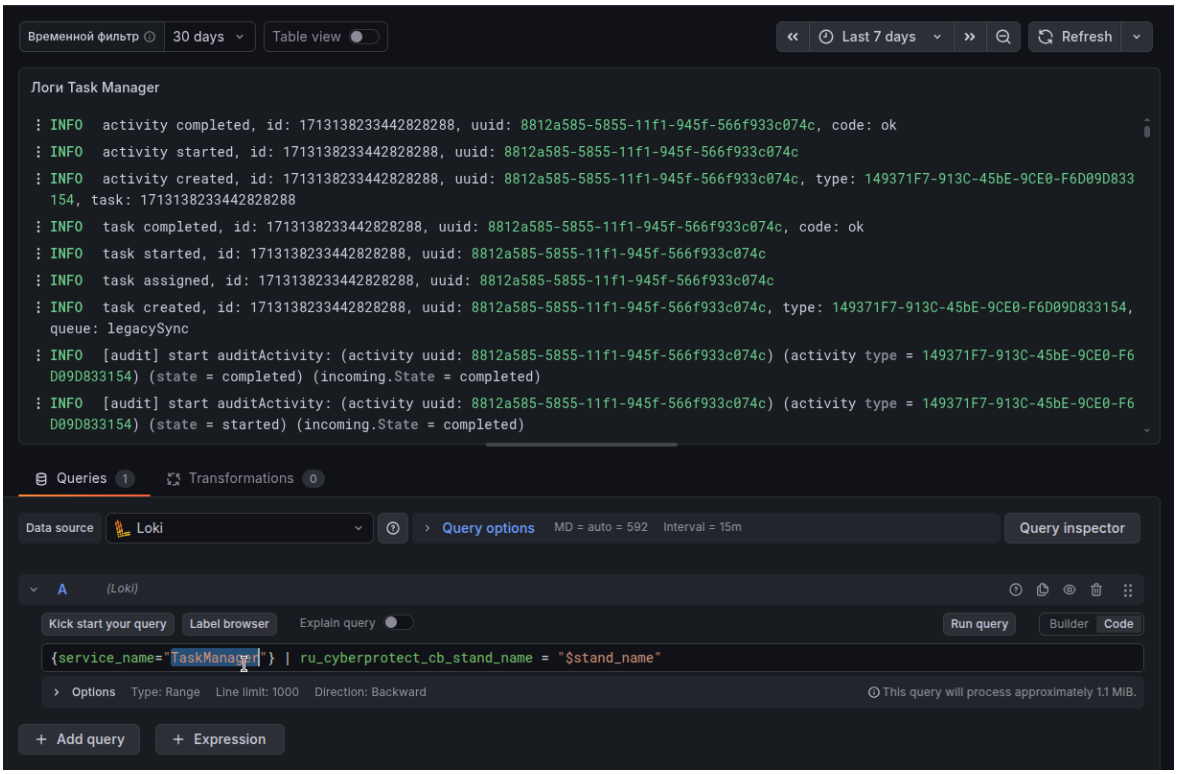
14.6.4.3 Настройка панелей платформы Grafana

Настройка панелей с журналами

Для каждой службы необходимо добавить отдельную панель. Чтобы добавить панель с журналами:

1. Скопируйте существующую панель с журналами и вставьте копию в панель мониторинга.
2. Перейдите в режим редактирования панели и в поле **service_name** укажите необходимую службу и значение атрибута ru.cyberprotect.cb.stand.name, указанное при настройке данных телеметрии (см. подраздел "Настройка данных телеметрии" в разделе "Настройка внешнего мониторинга" (стр. 751)). Служба должна быть указана при настройке OpenTelemetry Collector (см. раздел "Настройка Grafana Loki в качестве источника данных" (стр. 757)).

© ООО Киберпротект, 2026



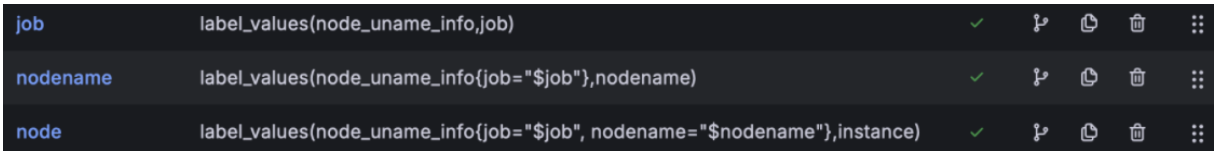
3. Сохраните изменения.

Повторите действия для каждой необходимой службы.

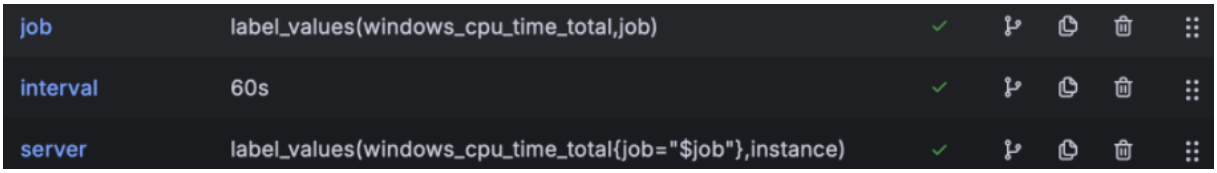
Настройка системных панелей

Системные панели используют метрики, полученные из Node Exporter или Windows Exporter. Метрики Node Exporter отличаются от метрик Windows Exporter, поэтому для PromQL-запросов используются разные переменные.

Для ОС Linux используются переменные job, nodename и node.



Для ОС Windows используются переменные job, interval и server.



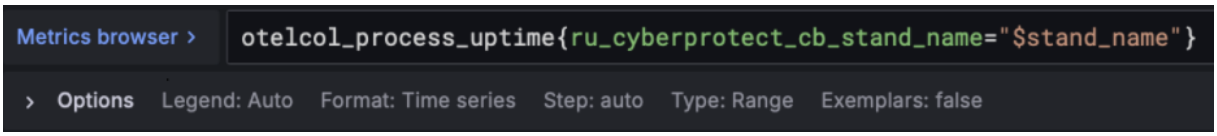
При необходимости измените значения переменных.

Настройка панели с временем доступности

Панель времени доступности отображает время работы сервера управления Кибер Бэкап.

© ООО Киберпротект, 2026

По умолчанию панель использует метрику otelcol_process_uptime, ассоциированную со значением атрибута ru.cyberprotect.cb.stand.name, которое было указано при настройке данных телеметрии (см. подраздел "Настройка данных телеметрии" в разделе "Настройка внешнего мониторинга" (стр. 751)).



Настройка панелей с журналами

Для работы с журналами используется атрибут ru.cyberprotect.cb.stand.name, которой был указан при настройке данных телеметрии (см. подраздел "Настройка данных телеметрии" в разделе "Настройка внешнего мониторинга" (стр. 751)).

Для корректной работы панели в Grafana Loki должна быть включена работа с структурированными метаданными.

© ООО Киберпротект, 2026

15 Ленточные устройства

Лента – носитель (картридж с магнитной лентой) для записи и хранения данных.

Чистящая лента – лента, предназначенная для технического обслуживания ленточных приводов.

Ленточное устройство – общий термин, обозначающий оборудование для работы с лентами. Включает как ленточные библиотеки, так и автономные ленточные приводы.

Ленточный привод – устройство чтения данных с лент и записи данных на ленты.

Ленточная библиотека – автоматизированная система хранения данных большой емкости, содержащая следующие компоненты:

- множество слотов хранения для размещения лент;
- один или несколько ленточных приводов;
- механизм для автоматического перемещения лент между слотами и приводами.

Библиотека может содержать и другие компоненты, например, устройства чтения штрихкодов или принтеры штрихкодов.

В следующих разделах описано использование ленточных устройств для хранения резервных копий.

15.1 Типы и свойства лент

Кибер Бэкап поддерживает следующие известные типы носителей:

- перезаписываемые ленты;
- ленты типа WORM (write-once-read-many – однократная запись, множественное чтение);
- чистящие ленты.

Кроме того, Кибер Бэкап поддерживает работу с лентами, которые не удалось отнести ни к одному из известных типов (см. далее подраздел "Ленты неизвестного типа").

Кибер Бэкап обеспечивает совместимость со многими ленточными устройствами. По вопросам поддержки конкретного оборудования см. соответствующую документацию.

15.1.1 Перезаписываемые ленты

Перезаписываемые ленты являются основным типом ленточных носителей в Кибер Бэкап для резервного копирования. Используйте их для хранения информации, которую предполагается перезаписывать.

Особенности перезаписываемых лент:

- неограниченное количество циклов записи;
- используются по умолчанию для резервного копирования;

© ООО Киберпротект, 2026

- могут иметь аппаратную защиту от записи.

Перезаписываемые ленты используются по умолчанию для автоматического пополнения пользовательских пулов.

15.1.2 Ленты типа WORM

Ленты этого типа предназначены для записи неизменяемых архивов. Используйте эти ленты для хранения резервных копий, которые не будут меняться в течение всего срока хранения.

Кибер Бэкап поддерживает запись данных на пустые и на частично заполненные WORM-ленты. При этом операции перезаписи и стирания данных будут предотвращаться.

Для лент WORM предусмотрено автоматическое пополнение пользовательских пулов. Для его включения в существующем пуле перейдите в **Настройки** -> **Управление лентами** -> **Пулы лент** -> **Пользовательский пул** -> **Правка пула** и отметьте флажком пункт **Носителями однократной записи (тип WORM)**.

Внимание
Данные, записанные на WORM-ленты, нельзя будет впоследствии перезаписать или стереть.

15.1.2.1 Использование WORM-носителей для архивного хранения

Для архивного хранения на WORM-лентах создайте отдельный пул. Используйте этот пул для создания неизменяемых архивов. Включите для этого пула автоматическое пополнение WORM-лентами или перенесите их в него вручную.

Создайте план защиты для WORM-лент. При его выполнении автоматически будет выбрана WORM-лента с доступным местом.

При необходимости WORM-ленты будут автоматически добавляться из пула **Свободные ленты**.

Примечание
При назначении плана защиты убедитесь, что в библиотеке достаточно пустых WORM-лент.

15.1.3 Аппаратная защита от записи

Перезаписываемые ленты и ленты WORM оснащены аппаратной защиты от записи.

С включенной защитой на ленте невозможно выполнять следующие действия:

- записывать и перезаписывать данные;
- стирать существующие данные.

Внимание
Физическое положение переключателя защиты от записи имеет приоритет по отношению к настройкам программы.

© ООО Киберпротект, 2026

При расхождении данных о положении переключателя с данными программы выполните инвентаризацию.

15.1.4 Чистящие ленты

Эти специальные ленты предназначены для профилактической очистки ленточных приводов.

Особенности чистящих лент:

- автоматически определяются и остаются в пуле **Нераспознанные ленты**;
- имеют ограниченный ресурс (до 50 циклов очистки);
- не могут использоваться для хранения данных;
- не перемещаются в другие пулы.

Оставшийся ресурс каждой ленты автоматически отслеживается после каждой процедуры очистки.

15.1.5 Ленты неизвестного типа

Этот статус лента получает в том случае, если в результате инвентаризации Кибер Бэкап не удается автоматически установить ее тип. При этом такие ленты все равно можно использовать для операций резервного копирования.

По умолчанию в Кибер Бэкап ленты неизвестного типа обрабатываются как перезаписываемые.

При каждом взаимодействии с такой лентой будет вновь автоматически выполняться попытка идентификации.

Ленты этого типа можно размещать в пользовательских пулах и автоматически пополнять ими эти пулы.

15.2 Поддержка резервного копирования на ленту

Агенты защиты могут выполнять резервное копирование данных на ленточное устройство напрямую или через узел хранения. В любом случае обеспечивается полностью автоматическая работа ленточного устройства. Если ленточное устройство с несколькими накопителями подключено к узлу хранения, несколько агентов могут одновременно выполнять резервное копирование на магнитные ленты.

Внимание
Для корректной работы необходимо, чтобы доступ к ленточным устройствам и управление ими осуществлялись только через продукт Кибер Бэкап. Любые действия, выполняемые в обход продукта, могут привести к ошибкам.

© ООО Киберпротект, 2026

15.2.1 Совместимость с RSM и программным обеспечением других поставщиков

15.2.1.1 Сосуществование с программным обеспечением других поставщиков

Невозможно работать с лентами на машине, на которой установлено программное обеспечение других поставщиков с фирменными средствами управления лентами. Для использования лент на таких машинах необходимо удалить или отключить программное обеспечение других поставщиков.

15.2.1.2 Взаимодействие с диспетчером съемных носителей Windows (RSM)

Агенты защиты и узлы хранения не используют RSM. При обнаружении ленточного устройства они отключают устройство от RSM (если они не используются другим программным обеспечением). Чтобы работать с ленточным устройством, убедитесь, что устройство не включается в RSM ни пользователями, ни программным обеспечением других поставщиков. Если ленточное устройство включено в RSM, повторите процедуру распознавания ленточного устройства.

15.2.2 Поддерживаемое оборудование

Кибер Бэкап поддерживает внешние устройства SCSI. Это устройства, подключаемые к Fibre Channel или с помощью интерфейсов SCSI, iSCSI, Serial Attached SCSI (SAS). Кроме того, Кибер Бэкап поддерживает ленточные устройства, подключенные через USB.

В ОС Windows Кибер Бэкап может выполнять резервное копирование на ленточное устройство, даже если не установлены драйверы для соответствующего устройства смены носителей. Такое ленточное устройство отображается в **диспетчере устройств** как **неизвестный сменщик носителей**. Однако драйверы для накопителей устройства должны быть установлены. В Linux и при загрузке с носителя резервное копирование на ленточное устройство без драйверов невозможно.

Распознавание устройств, подключенных к IDE или SATA, не гарантируется. Это зависит от того, установлены ли в операционной системе необходимые драйверы.

Чтобы узнать, поддерживается ли то или иное устройство, используйте инструмент совместимости оборудования. Можно отправить отчет с результатами теста в Киберпротект.

15.2.3 База данных управления лентами

Информация обо всех ленточных устройствах, подключенных к машине, хранится в базе метаданных управления лентами. Путь к базе данных по умолчанию:

© ООО Киберпротект, 2026

- В ОС Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database**.
- В ОС Linux: **/var/lib/Acronis/BackupAndRecovery/ARSM/Database**.

Размер базы данных зависит от количества резервных копий, которые хранятся на ленточных носителях, и приблизительно равен 10 МБ на каждые сто резервных копий. База данных может быть больше, если библиотека ленточных носителей содержит тысячи резервных копий. В таком случае, возможно, потребуется сохранить базу данных ленточных носителей на другом томе.

База данных также хранит:

- Информацию о чистящих носителях и их местоположении;
- Счетчики использованных и оставшихся циклов очистки;
- Историю выполненных операций очистки.

Как изменить расположение базы данных в Windows

1. Остановите службу MMS.
   Если ленточные носители подключены к узлу хранения, остановите службу storagenode.
2. Переместите файлы из расположения по умолчанию в новое расположение.
3. В реестре найдите ключ HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings.
4. Укажите новый путь к каталогу в значении реестра **ArsmDmlDbProtocol**. Строка может содержать до 32765 символов.
5. Запустите службу MMS или storagenode.

Как изменить расположение базы данных в Linux

1. Остановите службу acronis_mms.
   Если ленточные носители подключены к узлу хранения, остановите службу storageserver.
2. Переместите файлы из расположения по умолчанию в новое расположение.
3. Откройте файл конфигурации **/etc/Acronis/ARSM.config** в текстовом редакторе.
4. Найдите строку <value name="ArsmDmlDbProtocol" type="TString">.
5. Измените путь под этой строкой.
6. Сохраните файл.
7. Запустите службу acronis_mms или storageserver.

15.2.4 Параметры записи на ленты

Параметры записи на ленту (размер блока данных и размер кэша) позволяют выполнить тонкую настройку программного обеспечения для получения максимальной производительности. Для записи на ленту требуются оба параметра, но обычно необходимо настроить только размер блока данных. Оптимальное значение зависит от типа ленточного устройства и от данных, подлежащих резервному копированию, например, от количества файлов и их размера.

© ООО Киберпротект, 2026

Примечание
Программа читает ленту блоками данных такого же размера, который использовался для записи данных на ленту. Если ленточное устройство не поддерживает этот размер блоков данных, чтение завершится сбоем.

Параметры заданы на каждой машине, к которой подключено ленточное устройство. Это может быть машина, на которой установлен агент или узел хранения. На машине под управлением Windows настройка выполняется в реестре. На машине Linux она выполняется в файле конфигурации **/etc/Acronis/BackupAndRecovery.config**.

В Windows создайте соответствующие разделы реестра и их значения DWORD. На машине Linux добавьте следующий текст в конце файла конфигурации непосредственно перед тегом </registry>:

```
<key name="TapeLocation">
   <value name="WriteCacheSize" type="Dword">
      "value"
   </value>
   <value name="DefaultBlockSize" type="Dword">
      "value"
   </value>
</key>
```

DefaultBlockSize

Это размер блока данных (в байтах), используемый для записи на ленты.

Возможные значения: 65536, 131072, 262144, 524288, 1048576. Рекомендуемое значение: 65536 или 262144.

Если данное значение равно 0 или параметр отсутствует, размер блока данных определяется следующим образом:

- В Windows данное значение принимается от драйвера ленточного устройства.
- В Linux данное значение составляет **64 КБ**.

Раздел реестра (на машине под управлением Windows): **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize**

Строка в файле /etc/Acronis/BackupAndRecovery.config (на машине под управлением Linux):

```
   <value name="DefaultBlockSize" type="Dword">
      "value"
   </value>
```

Если указанное значение не принимается ленточным устройством, то программа делит его на два до тех пор, пока не будет достигнуто приемлемое значение или значение 32 байта. Если приемлемое значение не найдено, то программа умножает указанное значение на два до тех пор,

© ООО Киберпротект, 2026

пока не будет достигнуто приемлемое значение или значение 1 МБ. Если ни одно значение не принимается диском, резервное копирование завершится сбоем.

WriteCacheSize

Это размер буфера (в байтах), используемый для записи на ленты.

Возможные значения: 65536, 131072, 262144, 524288, 1048576, но не меньше значения параметра **DefaultBlockSize**. Рекомендуемое значение: 4 * **DefaultBlockSize**.

Если значение составляет 0 или данный параметр отсутствует, размер буфера составляет **1 МБ**. Если операционная система не поддерживает это значение, то программа делит его на два до тех пор, пока не будет достигнуто приемлемое значение или значение параметра **DefaultBlockSize**. Если значение, поддерживаемое операционной системой, не найдено, резервное копирование завершится сбоем.

Раздел реестра (на машине под управлением Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

Строка в файле /etc/Acronis/BackupAndRecovery.config (на машине под управлением Linux):

```
<value name="WriteCacheSize" type="Dword">
   "value"
</value>
```

Если указать ненулевое значение, которое не поддерживается операционной системой, резервное копирование завершится сбоем.

15.2.5 Связанные с лентой параметры резервного копирования

Настраиваемые параметры резервного копирования Управление лентами позволяют определить следующие возможности.

- Следует ли включить восстановление файлов из образов дисков на лентах.
- Следует ли возвращать ленты в слот после выполнения плана защиты.
- Следует ли извлекать ленты после завершения резервного копирования.
- Следует ли использовать свободную ленту для каждой резервной копии.
- Следует ли перезаписывать данные на ленте при создании полной резервной копии (только для изолированных ленточных устройств).
- Следует ли использовать наборы лент для различения использованных лент, например, для резервных копий, созданных в разные дни недели или для резервных копий разных типов машин.

15.2.6 Параллельные операции

Кибер Бэкап может одновременно выполнять операции с различными компонентами ленточного устройства. В ходе операции с накопителем (резервное копирование, восстановление, повторное

© ООО Киберпротект, 2026

сканирование или стирание) можно запустить операцию, в которой используется устройство смены носителей (перемещение ленты в другой слот или извлечение ленты), и наоборот. Если в библиотеке ленточных носителей больше одного накопителя, можно запустить операцию с одним накопителем во время операции с другим. Например, несколько машин могут одновременно выполнять резервное копирование или восстановление, используя разные устройства одной и той же библиотеки ленточных носителей.

Операция обнаружения новых ленточных устройств может выполняться одновременно с любой другой операцией. Во время инвентаризации недоступны никакие другие операции, кроме обнаружения новых ленточных устройств.

Очистка привода может выполняться параллельно с операциями на других приводах. Очищаемый привод блокируется на время операции (обычно 2-5 минут).

Операции, которые нельзя выполнить параллельно, помещаются в очередь.

15.2.7 Ограничения

Существуют следующие ограничения использования ленточных устройств:

1. Резервное копирование и репликация резервных копий почтовых ящиков Microsoft Exchange на ленты не поддерживаются.
2. Невозможно выполнить резервное копирование физических и виртуальных машин с поддержкой приложений.
3. Консолидация резервных копий на лентах невозможна. В результате схема резервного копирования **Всегда инкрементное** недоступна при резервном копировании на ленты.
4. Дедупликация резервных копий на лентах невозможна.
5. Кибер Бэкап не может автоматически перезаписать ленту с резервными копиями, которые не удалены, а также в тех случаях, когда на других лентах есть зависимые резервные копии.
6. Резервное копирование невозможно, если требуется очистка привода. Используйте операцию "Очистка привода" для профилактического обслуживания в промежутках между резервным копированием.
7. Чистящие носители не могут быть использованы для операций с данными и не могут быть перемещены из пула **Нераспознанные ленты**.
8. Восстановление из резервной копии на ленте под управлением операционной системы невозможно, если это восстановление требует перезагрузки операционной системы. Для такого восстановления используйте загрузочный носитель.
9. Можно проверить любые резервные копии на лентах, однако выбрать для проверки целое хранилище на ленте или ленточное устройство невозможно.
10. Управляемое хранилище на лентах невозможно защитить паролем. Вместо этого защитите паролем резервные копии.
11. При репликации резервных копий на ленты не поддерживается мультиплексирование (см. "Управление лентами" (стр. 372)).

© ООО Киберпротект, 2026

12. Устройства, использующие протокол NDMP (Network Data Management Protocol), не поддерживаются.
13. Принтеры штрихкодов не поддерживаются.
14. Ленты, форматированные в файловую систему Linear Tape File System (LTFS), не поддерживаются.
15. Если при резервном копировании на ленте заканчивается свободное место, продолжить копирование можно только на пустую ленту.
16. Резервное копирование на какой-либо из накопителей ленточной библиотеки невозможно, если требуется очистка данного накопителя или очистка уже выполняется.

    Для успешного выполнения операций резервного копирования рекомендуется регулярно выполнять очистку накопителей ленточной библиотеки в промежутках между операциями.
17. Не рекомендуется использовать в ленточных библиотеках кассеты без бар-кодов. Использование таких кассет может приводить к сбоям.

15.3 Начало работы с ленточным устройством

15.3.1 Резервное копирование машины на локально подключенное ленточное устройство

15.3.1.1 Предварительные требования

- Ленточное устройство должно быть подключено к машине в соответствии с инструкциями производителя.
- На машине установлен агент защиты.

15.3.1.2 Перед резервным копированием

1. Загрузите ленты в ленточное устройство.
2. Войдите на веб-консоль Кибер Бэкап.
3. В разделе **Настройки** > **Управление лентами** разверните узел машины и щелкните **Ленточные устройства**.
4. Убедитесь, что отображается подключенное ленточное устройство. Если нет, нажмите кнопку **Поиск устройств**.
5. Проведите инвентаризацию лент:
   a. Щелкните имя ленточного устройства.
   b. Щелкните **Инвентаризация** для обнаружения загруженных лент. Оставьте включенным параметр **Полная инвентаризация**. Не включайте функцию **Перенести нераспознанные или импортированные ленты в пул «Свободные ленты»**. Щелкните **Начать инвентаризацию сейчас**.

      Результат: Загруженные ленты перенесены в соответствующие пулы, как указано в разделе «Инвентаризация».

© ООО Киберпротект, 2026

Примечание
Полная инвентаризация всего ленточного устройства может занять длительное время.

c. Если загруженные ленты перенесены в пул **Нераспознанные ленты** или **Импортированные ленты**, но требуются для резервного копирования, переместите такие ленты в пул **Свободные ленты** вручную.

Примечание
Ленты, отправленные в пул **Импортированные ленты**, содержат резервные копии, записанные ПО Кибер Бэкап. Перед перемещением таких лент в пул **Свободные ленты** убедитесь, что эти резервные копии больше не нужны.

15.3.1.3 Резервное копирование

Создайте план защиты, как описано в разделе Резервное копирование. Затем укажите хранилище резервных копий, щелкнув **Пул лент**.

15.3.1.4 Результаты

- Для доступа к хранилищу, где будут созданы резервные копии, выберите **Хранилища резервных копий** > **Пул лент**.
- Ленты с резервными копиями будут перемещены в пул.

15.3.2 Резервное копирование на ленточное устройство, подключенное к узлу хранения

15.3.2.1 Предварительные требования

- Узел хранения должен быть зарегистрирован на сервере управления.
- Ленточное устройство должно быть подключено к узлу хранения в соответствии с инструкциями производителя.

15.3.2.2 Перед резервным копированием

1. Загрузите ленты в ленточное устройство.
2. Войдите в веб-консоль Кибер Бэкап.
3. Щелкните **Настройки** > **Управление лентами**, разверните узел с именем узла хранения и щелкните **Ленточные устройства**.
4. Убедитесь, что отображается подключенное ленточное устройство. Если нет, нажмите кнопку **Поиск устройств**.
5. Проведите инвентаризацию лент:

© ООО Киберпротект, 2026

a. Щелкните имя ленточного устройства.

b. Щелкните **Инвентаризация** для обнаружения загруженных лент. Оставьте включенным параметр **Полная инвентаризация**. Не включайте функцию **Переместить нераспознанные или импортированные пулы лент в пул «Свободные ленты»**. Щелкните **Начать инвентаризацию сейчас**.

   Результат: Загруженные ленты перенесены в соответствующие пулы, как указано в разделе «Инвентаризация».

   Примечание
   Полная инвентаризация всего ленточного устройства может занять длительное время.

c. Если загруженные ленты перенесены в пул **Нераспознанные ленты** или **Импортированные ленты**, но требуются для резервного копирования, переместите такие ленты в пул **Свободные ленты** вручную.

   Примечание
   Ленты, отправленные в пул **Импортированные ленты**, содержат резервные копии, записанные ПО Кибер Бэкап. Перед перемещением таких лент в пул **Свободные ленты** убедитесь, что эти резервные копии больше не нужны.

d. Определите, что требуется сделать: выполнить резервное копирование в пул или создать новый пул.

   Наличие нескольких пулов позволяет использовать отдельный набор лент для каждой машины или каждого отдела компании.

e. Если выбранный пул может, при необходимости, принимать ленты из пула **Свободные ленты**, пропустите этот шаг.

   В противном случае перенесите ленты из пула **Свободные ленты** в выбранный пул.

   Примечание
   Чтобы узнать, может ли пул принимать ленты из пула **Свободные ленты**, щелкните пул, а затем щелкните **Правка пула**.

15.3.2.3 Резервное копирование

Создайте план защиты, как описано в разделе Резервное копирование. При указании хранилища резервных копий выберите пул лент.

15.3.2.4 Результаты

- Для доступа к хранилищу, где будут созданы резервные копии, выберите **Хранилища резервных копий**, затем выберите пул лент.
- После завершения резервного копирования ленты с резервными копиями будут перемещены в выбранный пул.

© ООО Киберпротект, 2026

15.3.2.5 Советы по дальнейшему использованию библиотеки ленточных носителей

- Полная инвентаризация не требуется каждый раз, когда загружается новая лента. Для экономии времени используйте процедуру, описанную в разделе «Инвентаризация», подраздел «Сочетание быстрой и полной инвентаризации».
- В той же библиотеке ленточных носителей можно создать другие пулы и выбрать любой из них в качестве места сохранения резервных копий.

15.3.3 Восстановление с ленточного устройства из операционной системы

Как выполнить восстановление с ленточного устройства из операционной системы

1. Войдите в веб-консоль Кибер Бэкап.
2. Нажмите **Устройства** и выберите машину, для которой есть резервная копия.
3. Щелкните **Восстановление**.
4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
5. Данное ПО отобразит список лент, необходимых для восстановления. Отсутствующие ленты помечены как неактивные. Если в ленточном устройстве есть пустые слоты, загрузите эти ленты в устройство.
6. Настройте другие параметры восстановления.
7. Нажмите **Запуск восстановления**, чтобы запустить операцию восстановления.
8. Если какие-либо из необходимых лент не загружены, программа отобразит сообщение с идентификатором нужной ленты. Необходимо сделать следующее:
   a. Загрузите ленту.
   b. Выполните быструю инвентаризацию.
   c. Нажмите **Панель мониторинга** > **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.
   d. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

15.3.3.1 Если не отображаются резервные копии, хранящиеся на лентах

Это может означать, что база данных с содержимым лент не найдена или повреждена.

Для восстановления базы данных выполните следующие действия.

© ООО Киберпротект, 2026

1. Выполните быструю инвентаризацию.

   Предупреждение
   Во время инвентаризации *не* включайте функцию **Перенести нераспознанные и импортированные ленты в пул «Свободные ленты»**. Если этот переключатель включен, можно потерять все резервные копии.

2. Проведите Повторное сканирование пула **Нераспознанные ленты**. В результате будет получено содержимое загруженных лент.
3. Если какие-либо из обнаруженных резервных копий продолжаются на других лентах, которые еще не сканировались, загрузите эти ленты по запросу и выполните их повторное сканирование.

15.3.4 Восстановление с загрузочного носителя из локально прикрепленного ленточного устройства

Как выполнить восстановление с загрузочного носителя из локально прикрепленного ленточного устройства

1. Загрузите в ленточное устройство ленты, необходимые для восстановления.
2. Загрузите машину с загрузочного носителя.
3. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
4. Если ленточное устройство подключено с использованием интерфейса iSCSI, настройте устройство, как описано в «Настройка устройств iSCSI и NDAS».
5. Щелкните **Управление лентами**.
6. Нажмите кнопку **Инвентаризация**.
7. В **Объекты для инвентаризации** выберите ленточное устройство.
8. Нажмите **Запуск** для запуска инвентаризации.
9. После завершения инвентаризации нажмите **Закрыть**.
10. Нажмите **Действия** > **Восстановить**.
11. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
12. Разверните **Ленточные устройства**, а затем выберите необходимое устройство. Система запросит подтверждение повторного сканирования. Нажмите **Да**.
13. Выберите пул **Нераспознанные ленты**.
14. Выберите ленты для повторного сканирования. Чтобы выбрать все ленты пула, установите флажок рядом с заголовком столбца **Имя ленты**.
15. Если ленты содержат защищенную паролем резервную копию, установите соответствующий флажок и укажите пароль для резервной копии в поле **Пароль**. Если пароль не указан или недействителен, резервная копия не будет обнаружена. Помните об этом в случае, если после

© ООО Киберпротект, 2026

повторного сканирования резервные копии не обнаружены.

Подсказка. Если ленты содержат несколько резервных копий, защищенных разными паролями, необходимо повторить сканирование несколько раз, поочередно указывая пароли.

16. Нажмите **Запуск** для запуска повторного сканирования. В результате будет получено содержимое загруженных лент.
17. Если какие-либо из обнаруженных резервных копий продолжаются на других лентах, которые еще не сканировались, загрузите эти ленты по запросу и выполните их повторное сканирование.
18. После завершения повторного сканирования нажмите кнопку **OK**.
19. В **представлении «Архив»** выберите резервную копию, затем выберите данные, которые требуется восстановить. После нажатия кнопки **OK** на странице **Восстановление данных** отобразится список лент, необходимых для восстановления. Отсутствующие ленты помечены как неактивные. Если в ленточном устройстве есть пустые слоты, загрузите эти ленты в устройство.
20. Настройте другие параметры восстановления.
21. Нажмите кнопку **OK**, чтобы начать восстановление.
22. Если какие-либо из необходимых лент не загружены, программа отобразит сообщение с идентификатором нужной ленты. Необходимо сделать следующее:
    a. Загрузите ленту.
    b. Выполните быструю инвентаризацию.
    c. Нажмите **Обзор** > **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.
    d. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

15.3.5 Восстановление с помощью загрузочного носителя с ленточного устройства, прикрепленного к узлу хранения

Как выполнить восстановление с помощью загрузочного носителя с ленточного устройства, прикрепленного к узлу хранения

1. Загрузите в ленточное устройство ленты, необходимые для восстановления.
2. Загрузите машину с загрузочного носителя.
3. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
4. Нажмите кнопку **Восстановить**.
5. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
6. В поле **Путь** введите bsp://<адрес узла хранения>/<имя пула>/, где <адрес узла хранения> – это IP-адрес узла хранения, содержащего нужную резервную копию, а <имя пула> – имя пула лент. Нажмите кнопку **OK** и укажите учетные данные для доступа к пулу.

© ООО Киберпротект, 2026

7. Выберите резервную копию, а затем данные для восстановления. После нажатия кнопки **OK** на странице **Восстановление данных** отобразится список лент, необходимых для восстановления. Отсутствующие ленты помечены как неактивные. Если в ленточном устройстве есть пустые слоты, загрузите эти ленты в устройство.
8. Настройте другие параметры восстановления.
9. Нажмите кнопку **OK**, чтобы начать восстановление.
10. Если какие-либо из необходимых лент не загружены, программа отобразит сообщение с идентификатором нужной ленты. Необходимо сделать следующее:
    a. Загрузите ленту.
    b. Выполните быструю инвентаризацию.
    c. Нажмите **Обзор** > **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.
    d. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

15.4 Управление лентами

15.4.1 Обнаружение ленточных устройств

При обнаружении ленточных устройств программа резервного копирования находит ленточные устройства, подключенные к машине, и помещает информацию о них в базу данных управления лентами. Обнаруженные ленточные устройства отключаются от RSM.

Как правило, ленточное устройство обнаруживается автоматически сразу же после подключения устройства к машине, на которой установлен продукт. Однако вам может потребоваться обнаружение ленточных устройств в следующих случаях:

- После подключения или повторного подключения ленточного устройства.
- После установки или переустановки программы резервного копирования на машине, к которой подключено ленточное устройство.

Как обнаружить ленточные устройства

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину, к которой подключено ленточное устройство.
3. Выберите **Поиск устройств**. Будут отображены подключенные ленточные устройства, их накопители и слоты.

15.4.2 Пулы лент

В программе резервного копирования используются пулы лент, представляющие собой логические группы лент. В Кибер Бэкап предустановлены следующие пулы лент (служебные пулы):

© ООО Киберпротект, 2026

- **Нераспознанные ленты**;
- **Импортированные ленты**;
- **Свободные ленты**.

Для размещения резервных копий в хранилищах используются пользовательские пулы, в том числе пользовательский пул по умолчанию. Предусмотрена возможность создания собственных пользовательских пулов.

Ленты можно перемещать между пулами. Подробнее об этом см. раздел "Перемещение в другой пул" (стр. 784).

15.4.2.1 Служебные пулы

Нераспознанные ленты

Пул содержит ленты, которые записывались сторонними приложениями. Для записи на такие ленты их необходимо явным образом переместить в пул **Свободные ленты**. Переместить ленты из этого пула в какой-либо другой, кроме пула **Свободные ленты**, нельзя.

Импортированные ленты

Пул содержит ленты, которые записывались программой Кибер Бэкап в ленточном устройстве, подключенном к другому узлу хранения или агенту. Для записи на такие ленты их необходимо явным образом переместить в пул **Свободные ленты**. Переместить ленты из этого пула в какой-либо другой, кроме пула **Свободные ленты**, нельзя.

Свободные ленты

Пул содержит свободные (пустые) ленты. В этот пул можно вручную перемещать ленты из других пулов.

При переносе ленты в пул **Свободные ленты** программа Кибер Бэкап удаляет информацию о резервных копиях на ней. Чтобы восстановить резервные копии, выполните повторное сканирование.

Пул используется по умолчанию для резервного копирования, когда не требуется создавать собственные пулы. Обычно он применяется к одному ленточному устройству с небольшим числом лент.

15.4.2.2 Пользовательские пулы

Для разделения резервных копий с различными данными необходимо создать несколько пулов. Например, можно создать пользовательские пулы для разделения:

- резервных копий разных отделов компании;
- резервных копий разных машин;
- резервных копий системных томов и пользовательских данных.

© ООО Киберпротект, 2026

15.4.3 Операции с пулами

15.4.3.1 Создание пула

Для создания пользовательского пула выполните следующие действия:

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которым прикреплено ленточное устройство, и затем нажмите **Пулы лент** около необходимой машины.
3. Нажмите **Создать пул**.
4. Введите имя пула.
5. [Необязательно] Настройте автоматическое пополнение, выбрав один из следующих вариантов:
   - Снимите флажок **Пополнять автоматически из пула "Свободные ленты"** для ручного управления носителями.
   - Оставьте флажок **Пополнять автоматически из пула "Свободные ленты"** и выберите тип лент, которыми создаваемый пул будет автоматически пополняться:
     - **Перезаписываемыми носителями** (по умолчанию) – стандартные операции;
     - **Носителями однократной записи (тип WORM)** – для архивного хранения неизменяемых данных.

   Примечание
   При выборе по умолчанию (**Перезаписываемыми носителями**) для автопополнения из пула **Свободные ленты** также будут использоваться ленты неизвестного типа.
6. Нажмите **Создать**.

15.4.3.2 Изменение пула

Примечание
Изменение параметров доступно только для пользовательского пула. Параметры служебного пула изменению не подлежат.

Как изменить пул

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Выберите требуемый пользовательский пул и нажмите кнопку **Правка пула**.
4. Можно изменить имя или настройки пула. Дополнительные сведения о настройках пула см. в

© ООО Киберпротект, 2026

разделе Создание пула.

5. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

15.4.3.3 Удаление пула

Можно удалять только созданные пользовательские пулы. Нельзя удалить служебные пулы лент (**Нераспознанные ленты**, **Импортированные ленты** и **Свободные ленты**), а также **Пул по умолчанию**.

Перед удалением пула выполните следующие действия:

- Переместите все ленточные носители в другой пул. Переместите ленты в пул **Свободные ленты** или воспользуйтесь процедурой стирания, если ленты содержат неактуальные данные.
- Внесите изменения в планы защиты, в которых данный пул указан в качестве хранилища резервных копий. В противном случае выполнение этих планов защиты завершится сбоем.

Как удалить пул

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство, и затем нажмите **Пулы лент** около необходимой машины.
3. Выберите требуемый пул и нажмите кнопку **Удалить**.
4. Подтвердите удаление пула.

15.4.4 Операции с лентами

15.4.4.1 Перемещение в другой слот

Используйте эту операцию в следующих ситуациях:

- необходимо извлечь несколько лент из ленточного устройства одновременно;
- ленточное устройство не имеет устройства оперативной смены носителя, и извлекаемые ленты находятся в слотах несъемных магазинов.

Необходимо переместить ленты в слоты одного магазина, а затем извлечь магазин вручную.

Порядок перемещения ленты в другой слот

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимую ленту, а затем выберите требуемую ленту.
4. Нажмите **Переместить в слот**.
5. Выберите новый слот, в который нужно перенести выбранную ленту.
6. Нажмите **Переместить**, чтобы начать операцию.

© ООО Киберпротект, 2026

15.4.4.2 Перемещение в другой пул

Операция позволяет перенести одну или несколько лент из одного пула в другой.

Существуют следующие возможности:

- "Ограничения" (стр. 787);
- "Ограничения" (стр. 787);
- "Ограничения" (стр. 788) (с помощью специальной утилиты).

Внимание
Чистящие ленты всегда отображаются в пуле **Нераспознанные ленты**; перенести их в другой пул нельзя.

Допустимое перемещение лент

В таблицах ниже приводятся разрешенные перемещения лент между пулами в зависимости от типа перемещаемых лент, находящихся в них.

Перезаписываемые ленты

Исходный пул / Целевой пул		**Пользовательские пулы**	**Служебные пулы**		
			Свободные ленты	**Нераспознанные ленты**	**Импортированные ленты**
Пользовательские пулы		Перемещение: • пустые ленты – через веб-консоль • ленты с данными – через командную строку	Перемещение	-	-
Служебные пулы	**Свободные ленты**	Перемещение (как пустые) Автоматическое пополнение	-	-	-
	Импортированные ленты	Сканирование	Перемещение	-	-
	Нераспознанные ленты	Сканирование	Перемещение	-	-

© ООО Киберпротект, 2026

Ленты WORM

Исходный пул / Целевой пул		Пользовательские пулы	Служебные пулы		
			Свободные ленты	Нераспознанные ленты	Импортированные ленты
Пользовательские пулы		Перемещение: • пустые ленты – через веб-консоль • ленты с данными – через командную строку	Перемещение (только пустые)	-	-
Служебные пулы	**Свободные ленты**	Перемещение Автоматическое пополнение	-	-	-
	Импортированные ленты	Сканирование	Перемещение	-	-
	Нераспознанные ленты	Сканирование	Перемещение	-	-

Особенности перемещения WORM-лент:

- Пустые WORM-ленты можно перемещать между всеми пулами;
- WORM-ленты с данными можно перемещать между пользовательскими пулами;
- При перемещении в пул **Свободные ленты** данные на WORM-лентах не удаляются.

Чистящие ленты

Исходный пул / Целевой пул		Пользовательские пулы	Служебные пулы		
			Свободные ленты	Нераспознанные ленты	Импортированные ленты
Пользовательские пулы		-	-	-	-
Служебные пулы	**Свободные ленты**	-	-	-	-
	Импортированные ленты	-	-	-	-

© ООО Киберпротект, 2026

	Нераспознанные ленты	-	-	-	-

Ограничения для чистящих носителей:

- Можно перемещать только между слотами хранения;
- Используйте очистку привода для контролируемой очистки.

Ленты неизвестного типа

Исходный пул / Целевой пул		**Пользовательские пулы**	**Служебные пулы**		
			Свободные ленты	**Нераспознанные ленты**	**Импортированные ленты**
Пользовательские пулы		Перемещение: • пустые ленты – через веб-консоль • ленты с данными – через командную строку	Перемещение	-	-
Служебные пулы	**Свободные ленты**	Перемещение Автоматическое пополнение	-	-	-
	Импортированные ленты	Сканирование	Перемещение	-	-
	Нераспознанные ленты	Сканирование	Перемещение	-	-

Перемещение лент в пул "Свободные ленты"

Если требуется повторно использовать ленты, на которых содержатся старые и ненужные резервные копии или просто оптимизировать ваше пространство, используйте перемещение лент в пул **Свободные ленты**.

Операция производится только с выбранными лентами. Тем не менее, информация о резервных копиях порой содержится и на других (созависимых) лентах. Перед непосредственным выполнением операции происходит автоматический поиск и обнаружение таких лент.

© ООО Киберпротект, 2026

Предупреждение
При переносе ленты с резервными копиями в пул **Свободные ленты** Кибер Бэкап удаляет информацию об этих резервных копиях на перемещаемой ленте и на созависимых лентах. Для восстановления удаленной информации потребуется повторное сканирование ленты.

15.4.5 Ограничения

- Ленты WORM с данными нельзя перенести из пользовательского пула в пул **Свободные ленты**.
- Перемещение носителей выполняется в соответствии с таблицами допустимого перемещения.

Перемещение

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство, и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Переместить в пул**.
5. Выберите пул **Свободные ленты**.
6. Нажмите **Переместить** для сохранения изменений.

Ход выполнения перемещения отображается в разделе **Панель мониторинга** -> **Действия**.

Перемещение пустых лент между пулами

Операция может потребоваться при необходимости перераспределения ресурсов между пользовательскими пулами: пополнение пулов, балансировка нагрузки и т. д.

Внимание
Операция применяется только к лентам, не содержащим данных резервных копий.

Перед выполнением операции проводится автоматическая проверка отсутствия данных на лентах. При обнаружении лент с данными или лент, занятых другими операциями, операция будет продолжена, а эти ленты исключены из операции. Исключенные ленты останутся в своих исходных пулах. Если при проверке на всех лентах будут обнаружены данные, операция будет отменена. Для перемещения лент с данными используйте утилиту командной строки.

15.4.6 Ограничения

- Отсутствие данных резервных копий на лентах;
- Перемещение носителей выполняется в соответствии с таблицами допустимого перемещения.

© ООО Киберпротект, 2026

15.4.7 Перемещение

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство, и затем нажмите **Пулы лент** около необходимой машины.
3. [Необязательно] Нажмите **Создать новый пул**, если требуется создать другой пул для выбранных лент. Выполните действия, описанные в разделе "Создание пула" (стр. 782).
4. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
5. Нажмите **Переместить в пул**.
6. Выберите пул, в который необходимо перенести ленты.
7. Нажмите **Переместить** для сохранения изменений.

Ход выполнения перемещения отображается в разделе **Панель мониторинга** -> **Действия**.

Перемещение лент с данными между пулами

Операция может потребоваться при необходимости изменить логическую структуру хранения данных резервных копий, провести балансировку нагрузки между разными пулами и т. д. Выполняется при наличии на лентах данных резервных копий.

Внимание
Для выполнения операции необходима специализированная утилита командной строки. Для ее использования требуется соответствующая квалификация администратора.

Предупреждение
На время операции необходимо приостановить все остальные выполняющиеся операции (в том числе, резервного копирования и восстановления), использующие информацию о связанных носителях, архивах и резервных копиях.

15.4.8 Ограничения

- Операция выполняется с использованием специальной утилиты, выполнение операции через веб-консоль невозможно;
- Перемещение носителей возможно только между пользовательскими пулами;
- Перемещение носителей выполняется в соответствии с таблицами допустимого перемещения;
- Максимальное количество перемещаемых лент за одну операцию: 1000 (выбранные и созависимые суммарно);
- Все перемещаемые ленты должны принадлежать исходному пулу.

Во время операции производится проверка созависимых данных на других лентах. После выполнения операции имеющиеся созависимости будут сохранены.

© ООО Киберпротект, 2026

15.4.9 Утилита для работы с лентами

Для перемещения используйте утилиту для работы с лентами tape_ctl, которая поставляется вместе с продуктом Кибер Бэкап и устанавливается вместе с узлом хранения или агентом.

Для запуска утилиты используйте командную строку. Запуск командной строки может выполняться от имени любого пользователя.

По умолчанию утилита расположена по следующему пути:

- C:\Program Files\Acronis\ARSM (в Windows);
- /usr/lib/Acronis/ARSM (в Linux).

Примечание
Запускайте утилиту на том узле хранения, который управляет перемещаемыми лентами. Они размещены в ленточной библиотеке, подключенной к указанному узлу хранения.

Для перемещения лент используйте синтаксис следующего вида:

```
tape_ctl move-data-tapes --address=<IP-адрес:порт> --user=<имя_пользователя> --password=<пароль> --source-pool=<исходный_пул> --target-pool=<целевой_пул> --all-tapes | --data-tapes=<ШТРИХКОД01,...,ШТРИХКОД99> | --tapes-file=<путь_к_файлу> [--force] [--dry-run] [--log-file=<имя_файла>]
```

В выражении для перемещения должны присутствовать следующие обязательные параметры:

- move-data-tapes – режим перемещения лент с данными;
- --address=<IP-адрес:порт> – IP-адрес или имя хоста и порт сервера управления;
- --user=<имя_пользователя> – имя пользователя учетной записи на сервере управления с привилегиями администратора;
- --password=<пароль> – пароль пользователя учетной записи на сервере управления с привилегиями администратора;
- --source-pool=<исходный_пул> – идентификатор исходного пользовательского пула;
- --target-pool=<целевой_пул> – идентификатор целевого пользовательского пула;
- Один из следующих параметров, указывающих ленты для перемещения:
  - --tapes-file=<путь_к_файлу> – путь к файлу со списком лент (штрихкодов) для перемещения;
  - --data-tapes=<ШТРИХКОД01,...,ШТРИХКОД99> – список лент (штрихкодов);
  - --all-tapes – ключ для перемещения всех лент из исходного пула.

При необходимости укажите дополнительные параметры:

- --force – принудительное выполнение операции без запроса подтверждения;
- --dry-run – режим симуляции (анализ без выполнения фактического перемещения);
- --log-file=<имя_файла> – файл журнала операции.

© ООО Киберпротект, 2026

Получение идентификатора пула

Для получения идентификатора пула выполните следующие действия:

1. В веб-консоли выберите нужный пул и щелкните справа **Сведения**.
2. Нажмите **Все свойства**.
3. В строке **poolid** прочтите значение идентификатора.

Файл со списком для перемещения

Если вам удобнее перечислить перемещаемые ленты в отдельном файле, создайте файл со списком таких лент и затем укажите его при использовании команды перемещения.

Файл со списком лент для перемещения должен соответствовать следующим требованиям:

- Текстовый файл в формате UTF-8;
- Одна лента на строку (штрихкод ленты);
- Файл должен содержать хотя бы одну не пустую и не комментированную строку с именем ленты.

Примечание
Пустые строки игнорируются. Строки, начинающиеся с символа #, считаются комментариями и также игнорируются. Ленты с дублирующимися именами обрабатываются как одна.

Пример содержимого файла:

```
# Список лент для перемещения
ШТРИХКОД01
ШТРИХКОД03
# Эта лента временно исключена
# ШТРИХКОД07
ШТРИХКОД11
```

15.4.10 Перемещение

Для непосредственного перемещения лент используйте приведенные ниже команды.

- Перемещение всех лент в целевой пул:

  ```
  tape_ctl move-data-tapes --address=<IP-адрес:порт> --user=<имя_пользователя> --password=<пароль> --source-pool=<исходный_пул> --target-pool=<целевой_пул> --all-tapes
  ```

  Пример:

  ```
  # tape_ctl move-data-tapes --address=192.168.1.10:9877 --user=root --password=1q2w3e --source-pool=0084691A-75F9-4DE5-B3DE-C65043507A2C --target-pool=2FF802EA-220B-4BD7-A416-8D4C1F7AC538 --all-tapes
  ```

- Перемещение указанных лент в целевой пул без запроса подтверждения:

© ООО Киберпротект, 2026

```
tape_ctl move-data-tapes --address=<IP-адрес:порт> --user=<имя_пользователя> --password=<пароль> --force --source-pool=<исходный_пул> --target-pool=<целевой_пул> --data-tapes=<ШТРИХКОД01,...,ШТРИХКОД99>
```

Пример:

```
# tape_ctl move-data-tapes --address=192.168.1.10:9877 --user=root --password=1q2w3e --force --source-pool=0084691A-75F9-4DE5-B3DE-C65043507A2C --target-pool=2FF802EA-220B-4BD7-A416-8D4C1F7AC538 --data-tapes=BARCODE01,BARCODE02
```

- Предварительный анализ лент из списка в файле без фактического перемещения и с записью действий в журнал:

```
tape_ctl move-data-tapes --address=<IP-адрес:порт> --user=<имя_пользователя> --password=<пароль> --dry-run --source-pool=<исходный_пул> --target-pool=<целевой_пул> --tapes-file=<путь_к_файлу> --log-file=<имя_файла>
```

Пример:

```
# tape_ctl move-data-tapes --address=192.168.1.10:9877 --user=root --password=1q2w3e --dry-run --source-pool=0084691A-75F9-4DE5-B3DE-C65043507A2C --target-pool=2FF802EA-220B-4BD7-A416-8D4C1F7AC538 --tapes-file=/tmp/tape-barcodes.txt --log-file=/tmp/tape-movement.log
```

- Перемещение указанных лент без запроса подтверждения и с записью действий в журнал:

```
tape_ctl move-data-tapes --address=<IP-адрес:порт> --user=<имя_пользователя> --password=<пароль> --force --source-pool=<исходный_пул> --target-pool=<целевой_пул> --data-tapes=<ШТРИХКОД01,...,ШТРИХКОД99> --log-file=<имя_файла>
```

Пример:

```
# tape_ctl move-data-tapes --address=192.168.1.10:9877 --user=root --password=1q2w3e --force --source-pool=0084691A-75F9-4DE5-B3DE-C65043507A2C --target-pool=2FF802EA-220B-4BD7-A416-8D4C1F7AC538 --data-tapes=BARCODE01,BARCODE02 --log-file=/tmp/tape-movement.log
```

Предупреждение

Не прерывайте процесс перемещения лент – это может привести к нарушению целостности данных на них. В случае сбоя или ошибки при перемещении, для восстановления целостности данных может понадобиться выполнить повторное сканирование перемещаемых лент.

В случае ошибки проверьте правильность указания параметров в командной строке и правильность оформления файла со списком. Убедитесь, что нет других препятствий для выполнения перемещения (см. подраздел "Ограничения").

© ООО Киберпротект, 2026

15.4.10.1 Инвентаризация

Операция инвентаризации обнаруживает ленты, загружаемые в ленточное устройство, и присваивает имена лентам, у которых их нет.

Существует два вида инвентаризации: ручная и автоматическая.

Ручная инвентаризация

Ручная инвентаризация запускается по требованию пользователя.

Методы инвентаризации

Существует два метода ручной инвентаризации.

Быстрая инвентаризация

Агент или узел хранения сканируют штрихкоды лент и проверяют наличие в системе информации об этих лентах. Если информация о ленте обнаружена (лента ранее использовалась в этой системе), Кибер Бэкап распознает ленту и автоматически возвращает её в соответствующий пул.

Если информация о ленте отсутствует (лента новая или использовалась в другой системе), она направляется в пул **нераспознанных лент**.

Используйте этот метод для распознания лент, которые используются одним и тем же ленточным устройством, подключенным к одной и той же машине.

Если ленточная библиотека не поддерживает сканирование штрихкодов, все ленты направляются в пул **нераспознанных лент**. В этом случае для распознания лент выполните полную инвентаризацию или используйте **комбинацию быстрой и полной инвентаризации**, как описано далее в этом разделе.

Полная инвентаризация

В процессе полной инвентаризации агент или узел хранения анализирует информацию, считанную с инвентаризируемых лент, и определяет следующие параметры:

- тип ленты и ее характеристики;
- содержимое лент и доступное пространство;
- состояние аппаратной защиты от записи.

В следующих таблицах показано, в какие пулы направляются ленты после полной инвентаризации.

Использовал ленту	Считывает ленту	В какой пул направляется лента
Агент	Тот же агент	Пул, где лента была раньше

© ООО Киберпротект, 2026

	Другой агент	**Импортированные ленты**
	Узел хранения	**Импортированные ленты**
Узел хранения	Тот же узел хранения	Пул, где лента была раньше
	Другой узел хранения	**Импортированные ленты**
	Агент	**Импортированные ленты**
Приложение для резервного копирования стороннего производителя	Агент или узел хранения	**Нераспознанные ленты**

Ленты, отличные от обычных заполненных, направляются в пулы, соответствующие типу ленты.

Тип ленты	В какой пул направляется лента
Пустая лента	**Свободные ленты**
Чистящая лента	**Нераспознанные ленты**

Комбинация быстрой и полной инвентаризации

Полная инвентаризация всего ленточного устройства может занять длительное время. Если требуется инвентаризация только нескольких лент, сделайте следующее.

1. Выполните быструю инвентаризацию ленточного устройства.
2. Щелкните пул **нераспознанных лент**. Найдите ленты, которые нужно инвентаризировать, и отметьте, в каких слотах они находятся.
3. Выполните полную инвентаризацию этих слотов.

Что делать после инвентаризации

Если вы хотите создавать резервные копии на лентах, которые были помещены в пул **нераспознанных лент** или пул **импортированных лент**, переместите их в пул **свободных лент**, а затем в пользовательский пул. Если пул, в котором вы хотите создавать резервные копии, пополняем, можно оставить ленты в пуле **свободных лент**.

Если требуется восстановление с ленты, которая была помещена в пул **нераспознанных лент** или **импортированных лент**, необходимо повторно сканировать эту ленту. Лента будет перемещена в пул, который вы выбрали во время повторного сканирования, и резервные копии, которые хранятся на ленте, появятся в хранилище.

Последовательность действий

© ООО Киберпротект, 2026

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину, к которой подключено ленточное устройство, а затем выберите ленточное устройство, для которого необходимо выполнить инвентаризацию.
3. Нажмите кнопку **Инвентаризация**.
4. [Необязательно] Для выбора быстрой инвентаризации отключите функцию **Полная инвентаризация**.
5. [Необязательно] Включите функцию **Перенести неопознанные и импортированные ленты в пул «Свободные ленты»**.

   Предупреждение
   Подключайте эту функцию только в том случае, если вы абсолютно уверены, что данные, которые хранятся на лентах, больше не нужны и ленты можно перезаписать.

6. Нажмите **Начать инвентаризацию сейчас** для запуска инвентаризации.

Автоинвентаризация

Автоинвентаризация – это инвентаризация, работающая в фоновом режиме. Она выполняется для своевременного обнаружения изменений в ленточных устройствах и поддержания их актуального статуса. Автоинвентаризация и инвентаризация не работают вместе.

Автоинвентаризация имеет меньший приоритет по сравнению с обычной инвентаризацией. Если на текущий момент работает инвентаризация или есть инвентаризации, ждущие своей очереди на выполнение, автоинвентаризация не запускается. Если запустить инвентаризацию, то выполняющаяся на текущий момент автоинвентаризация будет прервана.

Автоинвентаризация запускается периодически согласно параметрам настройки. Настройка периода выполнения автоинвентаризации производится в конфигурационном файле tape_devices.xml. Расположение конфигурационного файла: C:\ProgramData\Acronis\BackupAndRecovery\ARSM\Configuration (в Windows) и /var/lib/Acronis/BackupAndRecovery/ARSM/Configuration (в Linux). Вы можете настроить параметр **autoinventory** самостоятельно. Атрибут **period** параметра **autoinventory** настраивается в следующих границах: от 3 до 7200 (в секундах). По умолчанию этот параметр составляет 180.

```
<autoinventory>
  <enabled value="1"/>
  <period value="180"/>
 </autoinventory>
```

15.4.10.2 Повторное сканирование

Сведения о содержимом лент хранятся в особой базе данных. В ходе операции повторного сканирования выполняется чтение содержимого лент и, если содержимое не соответствует информации, имеющейся в базе данных, обновляется база данных. Резервные копии, обнаруженные в результате этой операции, помещаются в заданный пул.

© ООО Киберпротект, 2026

За одну операцию можно просканировать ленты из одного пула.

Для повторного сканирования лент с многопотоковой резервной копией или с многопотоковой и мультиплексированной резервной копией понадобится как минимум такое же количество приводов, которое было использовано при создании этой резервной копии. Такие резервные копии невозможно заново отсканировать, используя автономное ленточное устройство.

Повторное сканирование рекомендуется в следующих случаях:

- Если база данных узла хранения или управляемой машины потеряна или повреждена;
- Если сведения о ленте в базе данных устарели (например, содержимое ленты было изменено другим узлом хранения или агентом);
- Если требуется получить доступ к резервным копиям, сохраненным на лентах при работе с загрузочным носителем;
- Если по ошибке удалены сведения о ленте из базы данных. При повторном сканировании удаленной ленты резервные копии, сохраненные на ней, вновь появляются в базе данных и становятся доступными для восстановления данных;
- Если резервные копии были удалены из ленты вручную или с помощью правил хранения, но нужно сделать их доступными для восстановления данных. Перед повторным сканированием такой ленты извлеките ее, удалите сведения о ней из базы данных, а затем снова вставьте ленту в устройство.

Порядок повторного сканирования лент

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Ленточные устройства** около необходимой машины.
3. Выберите ленточное устройство, в которое загружены ленты.
4. Выполните быструю инвентаризацию.

   Примечание
   Во время инвентаризации *не* включайте функцию **Перенести нераспознанные и импортированные ленты в пул «Свободные ленты»**.

5. Выберите пул **Нераспознанные ленты**. После быстрой инвентаризации большинство лент направляется именно в этот пул. Также возможно повторное сканирование лент из любого другого пула.
6. Выберите отдельные ленты для индивидуального сканирования.
7. Нажмите **Повторное сканирование**.
8. Выберите пул, в который будут помещаться резервные копии после обнаружения.
   - Для лент из пользовательского пула – только текущий пул (целевой пул изменить нельзя);
   - Для лент из служебных пулов – любой пользовательский пул.
9. При необходимости установите флажок **Включить восстановление файлов из образов дисков на лентах**.

© ООО Киберпротект, 2026

Подробнее. Если этот флажок установлен, программа создает специальные дополнительные файлы на жестком диске машины, к которой подсоединено ленточное устройство. Восстановление файлов из резервных копий дисков возможно до тех пор, пока эти дополнительные файлы будут в порядке. Обязательно установите флажок, если ленты содержат резервные копии с поддержкой приложений. В противном случае вы не сможете восстановить данные приложений из этих резервных копий.

10. Нажмите **Запуск повторного сканирования** для запуска повторного сканирования.

Результат: Повторно отсканированные ленты перемещаются в выбранный пул. Резервные копии, сохраненные на лентах, находятся в этом пуле. Если резервная копия расположена на нескольких лентах, то вторая лента будет отсканирована автоматически и резервная копия будет добавлена в пул.

15.4.10.3 Переименование

Если программой обнаружена новая лента, ей автоматически назначается имя в следующем формате: **Лента XXX**, где **XXX** – уникальный номер. Ленты нумеруются последовательно. Операция переименования позволяет вручную изменить имя ленты.

Порядок переименования лент

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимую ленту, а затем выберите требуемую ленту.
4. Нажмите **Переименовать**.
5. Введите новое имя выбранной ленты.
6. Нажмите **Переименовать** для сохранения изменений.

15.4.10.4 Стирание

Внимание
Операцию стирания отменить невозможно.

Если лента находилась в пуле **Нераспознанные ленты** или **Импортированные ленты**, то после стирания она будет перемещена в пул **Свободные ленты**. Лента, размещенная в любом другом пуле, не перемещается.

Ленты WORM не могут быть стерты независимо от содержимого.

Ленты с включенной аппаратной защитой от записи требуют предварительного снятия защиты.

Порядок стирания лент

© ООО Киберпротект, 2026

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Стереть**. Система попросит подтвердить операцию.
5. Выберите способ стирания:
   - **Быстрое стирание**. Удаляются заголовки резервных копий, а из базы данных удаляется информация об этих резервных копиях. Информация о самой ленте сохраняется в базе данных.
   - **Полное стирание**. Физически удаляются все резервные копии, сохраненные на ленте, а из базы данных удаляется информация об этих резервных копиях. Однако информация о самой ленте сохраняется в базе данных.
6. Нажмите **Стереть**, чтобы начать операцию.

15.4.10.5 Извлечение

Для успешного извлечения ленты из библиотеки ленточных носителей библиотека ленточных носителей должна иметь устройство оперативной смены носителя (mail-slot), которое не должно быть блокировано пользователем или другой программой.

Порядок извлечения лент

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Извлечь**. Программа попросит ввести описание ленты. Рекомендуется описать физическое место, в котором будут храниться ленты. Во время восстановления программа покажет это описание, и вы легко найдете ленты.
5. Нажмите кнопку **Извлечь**, чтобы начать операцию.

После того как лента извлечена вручную или автоматически, рекомендуется написать на ленте ее имя.

15.4.10.6 Удаление

В ходе операции удаления из базы данных удаляются данные о резервных копиях, хранимых на выбранной ленте, и о самой ленте.

Можно удалить только автономную (извлеченную) ленту.

Порядок удаления ленты

© ООО Киберпротект, 2026

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимую ленту, а затем выберите требуемую ленту.
4. Нажмите кнопку **Удалить**. Система попросит подтвердить операцию.
5. Нажмите **Удалить**, чтобы удалить ленту.

Действия в случае удаления ленты по ошибке

В отличие от стертой ленты, данные из удаленной ленты не удаляются физически. Поэтому можно вновь сделать доступными резервные копии, сохраненные на такой ленте. Выполните следующие действия.

1. Загрузите ленту в ленточное устройство.
2. Выполните быструю инвентаризацию, чтобы обнаружить ленту.

   Примечание
   Во время инвентаризации *не* включайте функцию **Перенести нераспознанные и импортированные ленты в пул «Свободные ленты»**.

3. Выполните повторное сканирование, чтобы сопоставить данные, сохраненные на лентах, с базой данных.

15.4.10.7 Указание набора лент

Данная операция позволяет указать набор лент.

Набор лент представляет собой группу лент одного пула.

В отличие от указания набора лент в параметрах резервного копирования, где допустимо использование переменных, здесь допустимо указание только строковых значений.

Выполнение данной операции приведет к созданию программным обеспечением резервной копии *указанных* лент в соответствии с определенным правилом (например, для сохранений резервных копий за понедельник на ленте 1, резервных копий за вторник на ленте 2 и т. д.). Укажите определенный набор лент для каждой требуемой ленты и затем укажите тот же тип лент или используйте соответствующие переменные в параметрах резервного копирования.

В вышеупомянутом примере следует указать набор лент Monday для ленты 1, Tuesday для ленты 2 и т. д. В параметрах резервного копирования укажите [День недели]. В данном случае надлежащая лента будет использована в соответствующий день недели.

Порядок указания набора лент для одной или нескольких лент

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство, и затем нажмите **Пулы лент** около необходимой машины.

© ООО Киберпротект, 2026

3. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Набор лент**.
5. Введите имя набора лент. Если для указанных лент уже был задан набор лент, он будет заменен. Для исключения лент из набора лент без перемещения их в другой набор удалите существующее имя набора лент.
6. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

15.4.11 Ручная очистка ленточных приводов

Ручная очистка осуществляется с помощью специальных чистящих носителей (см. раздел "Типы и свойства лент" (стр. 766)).

Рекомендуется регулярно проводить очистку ленточных приводов для профилактики ошибок оборудования.

Примечание
Операцию очистки нельзя отменить после ее начала.

Чтобы очистить ленточный привод, выполните следующие действия:

1. Нажмите **Настройки** > **Управление лентами**.
2. Под необходимой машиной нажмите **Ленточные устройства** и далее выберите ленточную библиотеку, а затем ленточный привод.
3. На панели **Действия** нажмите **Выполнить очистку**.
4. Выберите чистящий носитель из списка доступных. Система показывает количество оставшихся циклов очистки для каждого носителя.

   Примечание
   Кибер Бэкап определяет количество оставшихся циклов очистки после первого применения чистящего носителя.

5. Нажмите **Очистить**.

Очистка привода занимает 2-5 минут. Привод недоступен во время очистки.

© ООО Киберпротект, 2026

16 Настройки системы

Чтобы получить доступ к этим настройкам, щелкните **Настройки** > **Настройки системы**.

Раздел **Настройки системы** видим только для администраторов организации.

16.1 Уведомления по электронной почте

Можно задать глобальные настройки, общие для всех уведомлений, отправляемых по электронной почте с сервера управления.

В окне Параметры восстановления по умолчанию пользователь может переопределить эти параметры исключительно для событий, возникающих во время резервного копирования. В этом случае глобальные настройки будут иметь силу для операций, не являющихся операциями резервного копирования.

При создании плана защиты можно выбрать настройки, которые будут использоваться: глобальные настройки или настройки, указанные в параметрах резервного копирования по умолчанию. Можно переопределить их, заменив на пользовательские значения, относящееся только к данному плану.

Внимание
При изменении глобальных настроек уведомлений по электронной почте будут изменены все планы защиты, в которых используются глобальные настройки.

Перед настройкой этих параметров обязательно настройте параметры **почтового сервера**.

Для определения глобальных настроек почтовых уведомлений

1. Выберите **Настройки** > **Настройки системы** > **Уведомления по электронной почте**.
2. В поле **Адрес электронной почты получателя** введите адрес электронной почты получателя. Можно указать несколько адресов, разделяя их точкой с запятой.
3. [Необязательно] В поле **Тема** измените тему уведомления по электронной почте.
   Можно использовать следующие переменные:
   - [Оповещение] – сводка оповещений
   - [Устройство] – имя устройства
   - [План] – название плана, для которого создано оповещение.
   - [Сервер управления] – имя хоста машины, на которой установлен сервер управления.
   - [Отдел] – название отдела, которому принадлежит машина.

   Тема по умолчанию: [Оповещение] **Устройство:** [устройство] **План:** [План]
4. [Необязательно] Установите флажок **Ежедневные краткие сведения об активных оповещениях**, а затем выполните следующие действия:

© ООО Киберпротект, 2026

a. Укажите время отправки кратких сведений.

b. [Необязательно] Установите флажок **Не отправлять сообщения «Нет активных оповещений»** .

5. [Необязательно] Выберите язык, который будет использоваться в уведомлениях по электронной почте.
6. Установите флажки для событий, о которых необходимо получать уведомления. Их можно выбрать из списка всех возможных оповещений, сгруппированных по степени серьезности.
7. Нажмите кнопку **Сохранить**.

16.2 Почтовый сервер

Можно указать почтовый сервер, который будет использоваться для отправки уведомлений с сервера управления.

Выбор почтового сервера

1. Последовательно выберите пункты **Настройки** > **Настройки системы** > **Почтовый сервер**.
2. В разделе **Почтовая служба** выберите один из перечисленных ниже пунктов.
   - **Пользовательские**
   - **Gmail**

     В учетной записи Gmail должен быть включен параметр **Ненадежные приложения**. Дополнительную информацию см. по ссылке https://support.google.com/accounts/answer/6010255.
   - **Yahoo Mail**
   - **Outlook.com**
3. [Только для пользовательской почтовой службы] Задайте указанные ниже настройки.
   - В поле **Сервер SMTP** введите имя сервера исходящей почты (SMTP).
   - В поле **Порт SMTP** укажите порт сервера исходящей почты. По умолчанию это порт 25.
   - Укажите, следует ли использовать шифрование SSL или TLS. Выберите **Нет**, чтобы отключить шифрование.
   - Если SMTP требует выполнять проверку подлинности, установите флажок **Для сервера SMTP требуется проверка подлинности**, а затем укажите учетные данные учетной записи, которая будет использоваться для отправки сообщений. Если вы не уверены, требует ли сервер SMTP проверки подлинности, обратитесь за помощью к сетевому администратору или поставщику услуг электронной почты.
4. [Только для Gmail, Yahoo Mail и Outlook.com] Укажите данные учетной записи, которая будет использоваться для отправки сообщений.
5. [Только для пользовательской почтовой службы] В поле **Отправитель** введите имя отправителя. Это имя будет указываться в поле **От** уведомлений по электронной почте. Если оставить это поле пустым, в сообщениях будет указана учетная запись, заданная на шаге 3 или 4.

© ООО Киберпротект, 2026

6. [Необязательно] Щелкните **Отправить тестовое сообщение**, чтобы проверить, правильно ли работают уведомления по электронной почте с заданными настройками. Введите адрес электронной почты, на который следует отправить тестовое сообщение.

16.3 Безопасность

Эти параметры позволяют повысить безопасность Кибер Бэкап.

16.3.1 Завершить сеансы работы неактивных пользователей через

Этот параметр позволяет указать время ожидания до автоматического выхода по причине неактивности пользователя. Когда до истечения времени ожидания остается одна минута, программа выводит пользователю запрос на подтверждение активности. Если этот запрос останется без ответа, будет выполнен выход из программы по тайм-ауту с потерей всех несохраненных изменений.

Значение по умолчанию: **Включено. Тайм-аут: 10 минут**.

16.3.2 Показать уведомление о последнем входе текущего пользователя

Этот параметр позволяет показать дату и время последнего успешного входа пользователя, количество сбоев аутентификации с момента последнего успешного входа и IP-адрес, с которого был выполнен последний успешный вход. Эта информация отображается в нижней части экрана при каждом входе пользователя.

Значение по умолчанию: **Отключено**.

16.3.3 Предупреждать об истечении срока действия локального пароля или пароля домена

Этот параметр позволяет отображать срок истечения пароля пользователя для доступа к серверу управления Кибер Бэкап. Это локальный пароль или пароль домена, с которым пользователь входит на машину с установленным сервером управления. Время до окончания срока действия пароля отображается в нижней части экрана и в меню учётной записи в верхнем правом углу.

Значение по умолчанию: **Отключено**.

16.4 Обновления

Этот параметр определяет, будет ли Кибер Бэкап проверять наличие новой версии при каждом входе администратора организации на веб-консоль Кибер Бэкап.

Значение по умолчанию: **Включено**.

Если этот параметр отключен, администратор может проверить обновления вручную, как описано в разделе «Проверка наличия обновлений программного обеспечения».

© ООО Киберпротект, 2026

16.5 Параметры резервного копирования по умолчанию

Параметры резервного копирования по умолчанию являются общими для всех планов защиты на сервере управления. Администратор организации может изменить используемое по умолчанию значение параметра, изменив его предопределенное значение. Новое значение будет использовано по умолчанию для всех планов защиты, которые будут созданы на этой машине после внесения изменения.

При создании плана защиты пользователь может переопределить значение по умолчанию своим значением, которое будет действовать только для данного плана.

Для изменения используемых по умолчанию параметров

1. Войдите в веб-консоль Кибер Бэкап как администратор организации.
2. Нажмите **Настройки** > **Настройки системы**.
3. Увеличьте область раздела **Параметры резервного копирования по умолчанию**.
4. Выберите параметр и внесите необходимые изменения.
5. Нажмите кнопку **Сохранить**.

16.6 Настройка PAM-модуля

Эти параметры позволяют повысить безопасность пользователя в Кибер Бэкап.

16.6.1 Установленные библиотеки

Перед началом настройки убедитесь в том, что в системе пользователя установлены библиотеки pam_tally2.so или pam_faillock.so

16.6.2 Используемая конфигурация

При настройке используйте конфигурационный файл /etc/pam.d/acronisagent.

Соблюдайте осторожность при изменении конфигурационных файлов. Поскольку блокировка PAM обрабатывается через account_server, а не напрямую через PAM, трудно учитывать каждый аспект конфигурации PAM, поэтому при отображении ошибок входа в систему могут возникнуть несоответствия.

16.6.3 Предупреждение о редактировании конфигурационного файла

В случае, если пользователь редактировал конфигурационный файл в Кибер Бэкап, все дальнейшие действия он предпринимает на свой страх и риск. Киберпротект не несет никакой

© ООО Киберпротект, 2026

ответственности за любые последствия, возникшие в результате самостоятельного изменения пользователем конфигурационных файлов.

16.7 Управление журналом аудита

Журнал аудита отключен по умолчанию. Включить его (как и снова отключить) может администратор с помощью переключателя **Сохранять события аудита** в разделе **НАСТРОЙКИ** > **Аудит** > **Журнал аудита**.

Примечание
При обновлении продукта состояние журнала аудита сохраняется: если он был включен на момент обновления, он останется включен, и наоборот.

16.7.1 Очистка журнала аудита

Очистить журнал аудита можно вручную в разделе **НАСТРОЙКИ** > **Аудит** > **Журнал аудита**:

- щелкнув **Очистить** возле значения размера журнала;
- отметив флажок **Удалить события аудита без возможности восстановления** при отключении журнала.

16.8 Отправка записей журнала аудита на Syslog-сервер

По умолчанию журнал аудита хранится в базе данных продукта Кибер Бэкап, однако для централизованного хранения и обработки можно настроить отправку записей журнала аудита на удаленный Syslog-сервер. Для отправки записей может использоваться протокол TCP, UDP или TLS.

Примечание
При отключении журнала аудита передача событий на Syslog-сервер прекращается. Настройки, указанные в этом разделе, становятся недоступны.

16.8.1 Предварительные требования для протокола TLS

Если для отправки записей планируется использовать протокол TLS, то перед настройкой должны быть выполнены следующие требования:

- Для сервера управления Кибер Бэкап подготовлены сертификат и закрытый ключ. Сертификат заверен корневым или промежуточным удостоверяющим центром (УЦ).
- Для Syslog-сервера подготовлены сертификат и закрытый ключ. Сертификат заверен корневым УЦ. В поле сертификата IPAddress указан IP-адрес Syslog-сервера, или в поле DNSname указано его DNS-имя.

© ООО Киберпротект, 2026

- Сертификат и закрытый ключ Syslog-сервера загружены на Syslog-сервер и указаны в его настройках.
- Файл цепочки сертификатов для проверки сертификата сервера управления Кибер Бэкап загружен на Syslog-сервер и указан в его настройках.
- Подготовлен сертификат УЦ, которым был заверен сертификат Syslog-сервера.

Подробные сведения о подготовке сертификатов и настройке Syslog-сервера см. в документации используемого в вашем окружении Syslog-сервера.

16.8.2 Настройка отправки записей на Syslog-сервер

Для настройки выполните следующие действия:

1. Перейдите в раздел **Настройки** > **Аудит** > **Syslog** и переведите переключатель **Передавать журнал аудита на Syslog сервер** в состояние "вкл".
2. Укажите параметры подключения к Syslog-серверу:
   - **Адрес удаленного сервера**. IP-адрес или DNS-имя Syslog-сервера.
   - **Порт**. Порт Syslog-сервера.
   - **Протокол**. Протокол для подключения к Syslog-серверу. Можно указать **TCP**, **UDP** или **TLS**.
   - **Формат сообщения**. Формат, в котором будут отправляться сообщения. Можно указать **CEF (RFC 3164)** или **Syslog**.
   - [Только для протокола TLS] **TLS Certificate**. Сертификат сервера управления Кибер Бэкап в формате PEM. Этот сертификат будет использоваться Syslog-сервером для проверки подлинности сервера управления Кибер Бэкап.
   - [Только для протокола TLS] **TLS Key**. Закрытый ключ сертификата сервера управления Кибер Бэкап. Ключ должен быть указан в формате PEM.
   - [Только для протокола TLS] **TLS CA Certificate**. Сертификат удостоверяющего центра (УЦ), которым заверен сертификат Syslog-сервера. Сертификат УЦ должен быть указан в формате PEM. Этот сертификат будет использоваться сервером управления Кибер Бэкап при проверке подлинности Syslog-сервера.
3. Нажмите **Отправить тестовое сообщение** и убедитесь, что сообщение получено Syslog-сервером.

   Примечание
   При использовании протокола UDP сообщение об ошибке отправки будет показано только в том случае, когда хост, на котором установлен Syslog-сервер, недоступен.

4. Нажмите **Сохранить**.

После настройки запись о каждом новом событии будет сохраняться в журнал аудита, а также отправляться на указанный Syslog-сервер.

© ООО Киберпротект, 2026

17 Управление учетными записями пользователей и отделами организации

Функциональные возможности, описанные в этом разделе, доступны только для администраторов организации.

Чтобы получить доступ к этим настройкам, щелкните **Настройки** > **Учетные записи**.

17.1 Отделы и административные учетные записи

Для управления отделами и административными учетными записями в веб-консоли Кибер Бэкап последовательно выберите пункты **Настройки** > **Учетные записи**. На панели **Учетные записи** отображается группа **Организация** с деревом отделов (при их наличии), а также список административных учетных записей на выбранном уровне иерархии.

17.1.1 Отделы

Группа **Организация** автоматически создается при установке сервера управления. При наличии лицензии Кибер Бэкап Расширенная можно создать дочерние группы, называемые отделами, которые, как правило, соответствуют отделам или подразделениям организации, и добавить в них административные учетные записи. Таким способом можно делегировать управление защитой другим пользователям, для которых разрешения на доступ явным образом ограничены соответствующими отделами. Информацию о том, как создать отдел, см. в разделе "Создание отделов" (стр. 814).

Каждый отдел может иметь дочерние отделы. Учетные записи родительского отдела имеют одинаковые права во всех дочерних отделах. Группа **Организация** – это родительская группа верхнего уровня. Учетные записи на этом уровне имеют одинаковые права во всех ее отделах.

17.1.2 Административные учетные записи

Если учетная запись пользователя позволяет ему войти в веб-консоль Кибер Бэкап, то такая учетная запись является административной (управляющей).

В веб-консоли Кибер Бэкап любой пользователь с административной учетной записью может просматривать все элементы на уровне иерархии своего отдела, а также управлять ими. Например, административная учетная запись в *организации* имеет доступ к верхнему уровню, а соответственно, и доступ ко всем отделам этой организации. Напротив, административная учетная запись в определенном *отделе* может получить доступ только к данному отделу и своим дочерним отделам.

17.1.3 Какие учетные записи могут быть административными?

Если на машине установлен сервер управления, любому локальному пользователю, пользователю домена или группе пользователей можно предоставить административную учетную запись

© ООО Киберпротект, 2026

(поддерживаемые службы каталогов приведены в разделе "Поддерживаемые интеграции со службами каталогов" (стр. 45)).

Информацию о добавлении административной учетной записи на сервере управления см. в разделе "Добавление административных учетных записей" (стр. 809).

17.1.4 Роли административной учетной записи

Каждой административной учетной записи назначается роль с предварительно определенными правами, которые необходимы для выполнения определенных заданий. Роли административной учетной записи перечислены ниже:

- **Администратор**:
  роль предоставляет полный административный доступ к организации или отделу.
- **Оператор мониторинга**:
  роль предоставляет доступ к инструментам мониторинга системы Кибер Бэкап. Роль позволяет создавать виджеты, просматривать уведомления о сбоях, действиях в системе, детали запущенных процессов, список агентов и узлов хранения, разрешает собирать данные диагностики Кибер Бэкап. Эта роль не позволяет изменять или запускать планы резервного копирования и восстанавливать резервные копии.
- **Только для чтения**:
  роль предоставляет доступ только для чтения по отношению к веб-консоли Кибер Бэкап. Эта роль позволяет только собирать диагностические данные, такие как системные отчеты. Роль «Только для чтения» не позволяет выполнять обзор резервных копий.
- **Аудитор**:
  роль предоставляет доступ только для чтения по отношению к вкладке **Действия** и разделу **Журнал аудита** в веб-консоли Кибер Бэкап. Дополнительную информацию об этом см. в разделах "Панель мониторинга "Действия"" (стр. 728) и "Журнал аудита" (стр. 739). Эта роль не позволяет собирать или экспортировать какие-либо данные, включая системную информацию сервера управления.

Все изменения, внесенные в роли, отображаются на вкладке **Действия**.

17.1.5 Наследование ролей

Роли в родительском отделе наследуются дочерними отделами. Если для одной учетной записи пользователя назначены разные роли в родительском и дочернем отделах, эта учетная запись будет иметь обе роли.

Кроме того, роли можно явно назначить определенной учетной записи пользователя или наследовать от группы пользователей. Таким образом, учетная запись пользователя может иметь специально назначенную роль и наследованную роль.

Если учетная запись пользователя имеет различные роли (назначенные и (или) наследованные), такой пользователь может получить доступ и выполнять действия, разрешенные одной из этих

© ООО Киберпротект, 2026

ролей. Например, учетная запись пользователя с назначенной ролью «Только для чтения» и наследованной ролью «Администратор» будет иметь права администратора.

Внимание
В веб-консоли Кибер Бэкап показаны только роли, которые явно назначены для текущего отдела. Никакие возможные отличия от наследованных ролей не отображаются. Во избежание возможных проблем с наследованными ролями настоятельно рекомендуем назначать роли «Администратор», «Только для чтения» и «Аудитор» отдельным учетным записям или группам.

17.1.6 Администраторы по умолчанию

17.1.6.1 В Windows

При установке сервера управления на машине происходит следующее:

- Группа пользователей **Acronis Centralized Admins** создается на машине.
  На контроллере домена группе присваивается имя *DCNAME* **$ Acronis Centralized Admins**. *DCNAME* означает имя NetBIOS контроллера домена.
- Все члены группы **Администраторы** добавляются в группу **Acronis Centralized Admins**. Если данная машина входит в домен, но не является контроллером домена, локальные пользователи (не входят в домен) исключаются. В контроллере домена нет пользователей, не принадлежащих к данному домену.
- Группы **Acronis Centralized Admins** и **Администраторы** добавляются к серверу управления как **администраторы организации**. Если данная машина входит в домен, но не является контроллером домена, группа **Администраторы** не добавляется. Это необходимо, чтобы локальные пользователи (не входят в домен) не стали администраторами организации.

Можно удалить группу **«Администраторы»** из списка администраторов организации. Однако группу **Acronis Centralized Admins** невозможно удалить. В том маловероятном случае, когда удалены все администраторы организации, в Windows можно добавить учетную запись в группу **Acronis Centralized Admins**, а затем войти в веб-консоль Кибер Бэкап, используя эту учетную запись.

17.1.6.2 В ОС Linux

При установке сервера управления на машину пользователь **root** добавляется на сервер управления в качестве **администратора организации**.

Можно добавить других пользователей Linux в список администраторов сервера управления, как описано далее, а затем удалить пользователя **root** из этого списка. В том маловероятном случае, когда удалены все администраторы организации, можно перезапустить службу acronis_asm. В результате пользователь **root** будет автоматически заново добавлен в качестве администратора организации.

В Linux вы можете также добавлять пользователей и назначать им роли (подробнее о добавлении пользователей см. раздел "Добавление административных учетных записей" (стр. 809)).

© ООО Киберпротект, 2026

17.1.7 Административная учетная запись в нескольких отделах

Для учетной записи можно предоставить права на управление в любом количестве отделов. Для такой учетной записи, а также для административных учетных записей на уровне организации в веб-консоли Кибер Бэкап отображается селектор отдела. Этот селектор позволяет пользователю с этой учетной записью по отдельности просмотреть каждый отдел и выполнить управление.

Учетная запись, которая имеет разрешения на все отделы в организации, не имеет разрешений для организации. Административные учетные записи на уровне организации необходимо явно добавить в группу **Организация**.

17.1.8 Добавление машин в отделы

Когда администратор добавляет машину с помощью веб-интерфейса, она добавляется в отдел, управляемый администратором. Если администратор управляет несколькими отделами, машина добавляется в отдел, выбранный с помощью селектора. Следовательно, администратору необходимо выбрать отдел перед тем, как щелкнуть **Добавить**.

При локальной установке агентов администратор предоставляет свои учетные данные. Машина добавляется в отдел, управляемый администратором. Если администратор управляет несколькими отделами, установщик попросит выбрать, в какой отдел добавить машину.

17.2 Добавление административных учетных записей

Примечание
Эта функция недоступна в Стандартной редакции.

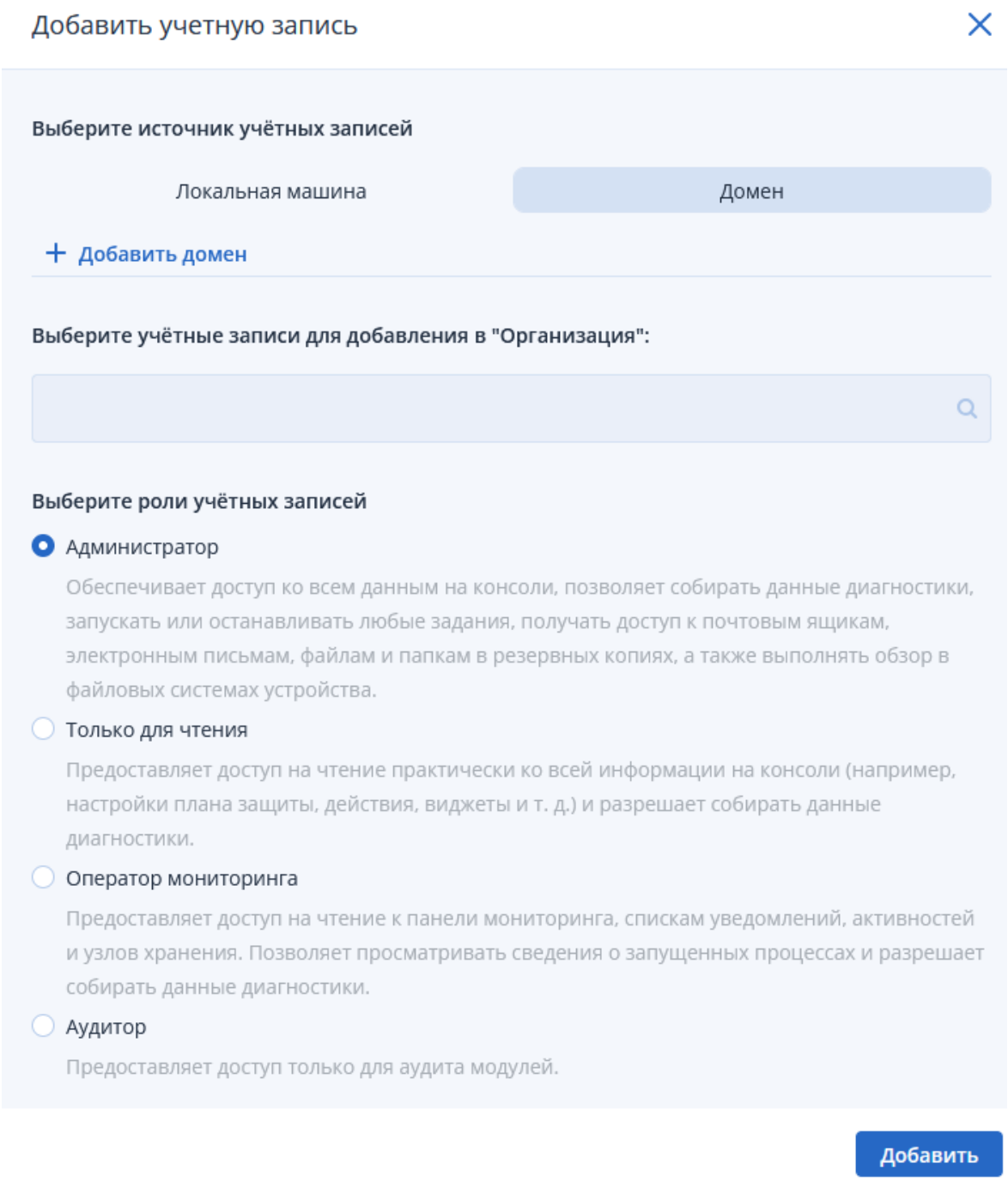
Порядок добавления учетных записей

1. Щелкните **Настройки** > **Учетные записи**.
   В веб-консоли отобразится список администраторов сервера управления и дерево отделов (при его наличии).
2. Выберите **Организация** или выберите отдел, в котором необходимо добавить административную учетную запись.
3. Нажмите кнопку **Добавить учетную запись**. Вы можете добавить пользователей домена следующих служб каталогов: Active Directory, Samba DC, FreeIPA, ALD Pro, РЕД АДМ.
4. Выберите локальную машину или домен, содержащий учетные записи, которые необходимо добавить.

   Примечание
   Для добавления учетных записей из домена необходимо сначала добавить сам домен.

   На вкладке **Домен** нажмите **Добавить домен**.

© ООО Киберпротект, 2026



Для добавления домена необходимо создать LDAP-подключение (или LDAPS-подключение). Укажите параметры этого подключения:

- **Имя домена**. Введите полное имя домена службы каталогов, например: company.ru.
- **Имя контроллера домена**. Укажите полное DNS-имя или IP-адрес сервера, на котором работает контроллер домена, например: dc1.company.ru или 192.168.1.10.
- **Служба каталогов**. Выберите **Active Directory**, **FreeIPA** или **Samba DC**. Для ALD Pro выберите **FreeIPA**, для РЕД АДМ – **Samba DC**.

© ООО Киберпротект, 2026

- **Порт**. Укажите порт подключения к службе каталогов. Для обычного подключения порт по умолчанию – 389. Для подключения, защищенного посредством протокола SSL (LDAPS), порт по умолчанию – 636. Если указать значение 0, то будет автоматически использован порт по умолчанию в зависимости от типа подключения.
- **Имя служебной учетной записи в службе каталога**. Введите имя учетной записи пользователя (с учетом регистра) для подключения к службе каталогов:
  - для FreeIPA или ALD Pro укажите имя в DN-формате, например: uid=ivanivanov,cn=users,cn=accounts,dc=company,dc=ru;
  - для Active Directory, РЕД АДМ или Samba DC укажите имя в формате COMPANYRU\User или User@company.ru, где COMPANYRU – NetBIOS-имя домена службы каталогов, company.ru – полное DNS-имя домена службы каталогов, User – имя учетной записи пользователя домена службы каталогов.

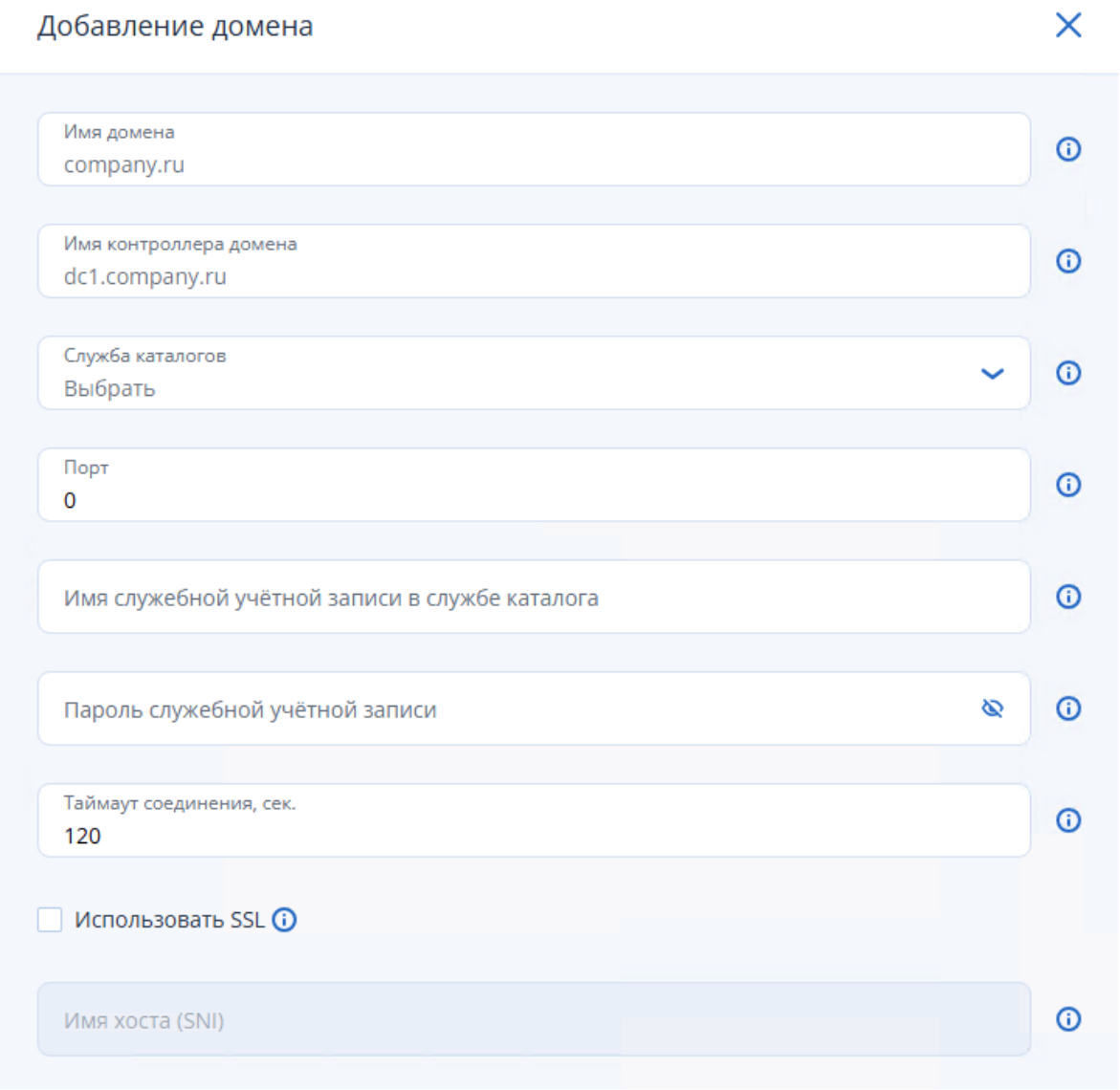
Внимание
Пользователь должен обладать правами на чтение объектов каталога и их свойств.

- **Пароль служебной учетной записи**. Введите пароль от учетной записи для подключения к службе каталогов.
- [Необязательно] **Таймаут соединения, сек**. Введите значение промежутка времени в секундах, в течение которого будет выполняться попытка подключения. По умолчанию это время составляет 120 с.
- **Использовать SSL**. Установите этот флажок, если необходимо использовать протокол SSL для подключения к службе каталогов (LDAPS-подключение).

Примечание
Чтобы использовать это подключение, необходимо настроить SSL-сертификат.

При установке этого флажка также появляется поле **Имя хоста (SNI)**. С его помощью можно задать указанное в сертификате имя хоста (SNI), с которым осуществляется TLS-соединение.

© ООО Киберпротект, 2026



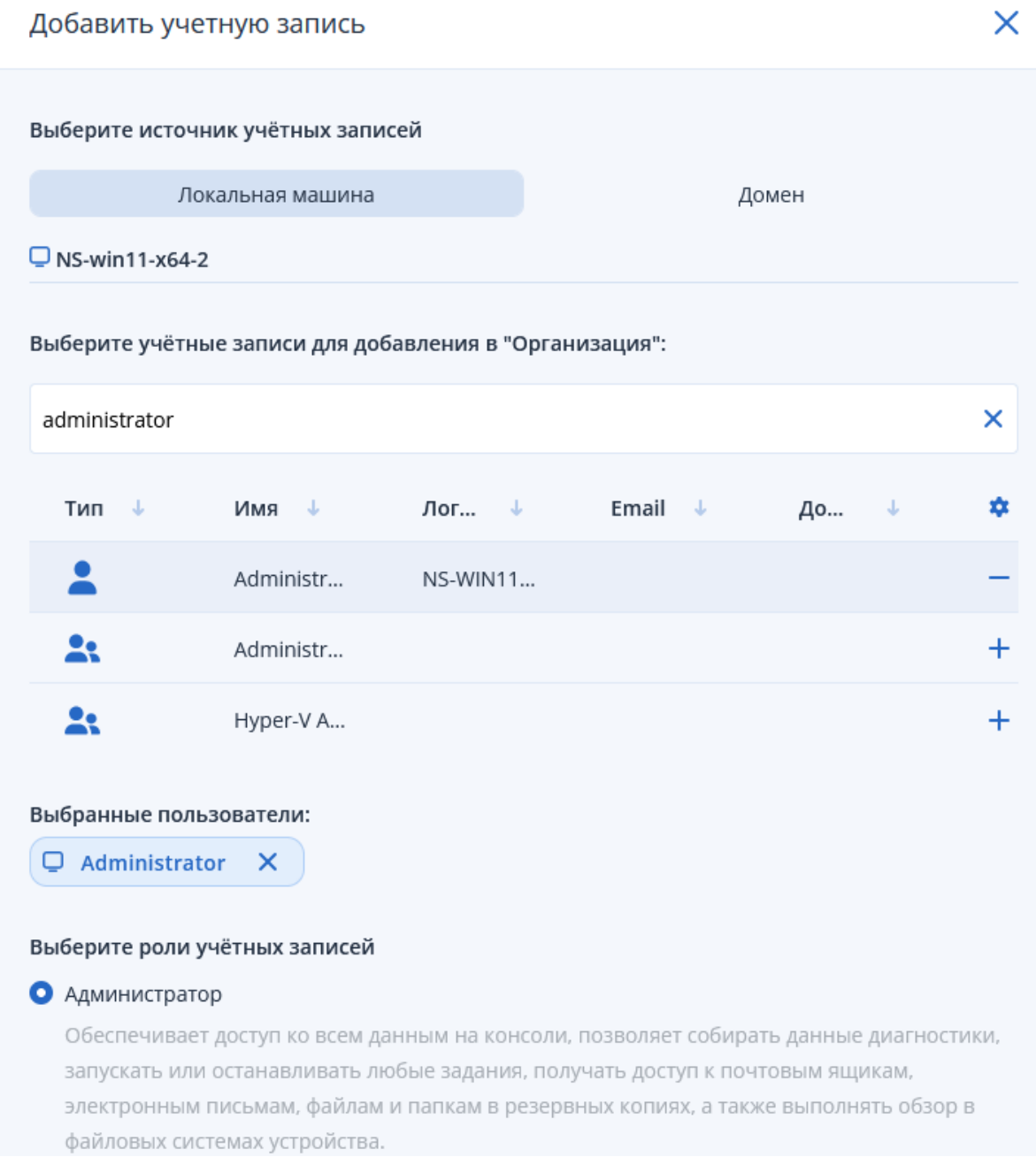
По окончании заполнения полей нажмите **Добавить** и дождитесь завершения процедуры добавления домена. Если процесс добавления не удается завершить успешно, проверьте настройки подключения.

5. Выполните поиск пользователя или группы пользователей. Поиск можно выполнять по следующим данным пользователя: имя пользователя, имя учетной записи, адрес электронной почты.
6. Нажмите «+» рядом с именем пользователя или группы.

Примечание

Из больших доменов (более 10 000 пользователей) или из доменов с группами высокого уровня вложенности (третьего уровня и выше) рекомендуется добавлять пользователей по одному. Или просто добавьте группу, в которую входят все необходимые пользователи.

© ООО Киберпротект, 2026



7. Выберите роль для учетной записи. Подробнее о ролях учетной записи см. в разделе "Отделы и административные учетные записи" (стр. 806).
8. Повторите шаги 4-7 для всех пользователей или групп, которые необходимо добавить.
9. По окончании нажмите **Добавить**.
10. [Только в Linux для локальных пользователей] Добавьте имена пользователей в Киберпротект Linux Pluggable Authentication Module (PAM), как описано ниже.

Порядок добавления имен пользователя в Киберпротект Linux PAM

1. На машине, где работает сервер управления, в текстовом редакторе откройте файл **/etc/security/acronisagent.conf** от имени привилегированного пользователя.

© ООО Киберпротект, 2026

2. В этом файле введите имена пользователей, которые добавлены как администраторы сервера управления. В каждой строке должно быть по одному имени.

   Примечание
   Указывайте в файле только имена локальных пользователей.

3. Сохраните и закройте файл.

17.3 Создание отделов

1. Щелкните **Настройки** > **Учетные записи**.
2. В веб-консоли отобразится список администраторов сервера управления и дерево отделов (при его наличии).
3. Выберите **Организация** или выберите родительский отдел для нового отдела.
4. Нажмите **Создать отдел**.
5. Укажите имя нового отдела и затем нажмите **Создать**.

© ООО Киберпротект, 2026

18 Диагностика неполадок

В этом разделе объясняется, как сохранить журналы агента и сервера управления в ZIP-файлы. Эти журналы помогут сотрудникам сопровождения ПО определить проблему в случае неудачного резервного копирования или других операций, не удавшихся по неясной причине.

Получение журналов агентов

1. Выполните одно из следующих действий:
   - В разделе **Устройства** выберите машину, на которой необходимо собрать журналы, и нажмите кнопку **Действия**.
   - В разделе **Настройки** > **Агенты** выберите машину, на которой необходимо собрать журналы, и нажмите кнопку **Сведения**.
2. Нажмите кнопку **Сбор сведений о системе**.
3. При появлении соответствующего запроса в веб-браузере укажите место сохранения файла.

Получение журналов сервера управления

Выполните следующие действия:

1. В разделе **Панель мониторинга** > **Действия** нажмите кнопку **Собрать сведения о системе сервера управления** в нижней части экрана.
2. В открывшемся окне **Требуется подтверждение** нажмите кнопку **Собрать**.
3. При появлении соответствующего запроса в веб-браузере укажите место сохранения файла.

Получить журнал сервера управления возможно без установки агентов.

© ООО Киберпротект, 2026

Глоссарий

В

Восстановление при загрузке

Модификация загрузочного агента, которая находится на системном диске и запускается во время загрузки при нажатии клавиши F11. Восстановление при загрузке устраняет необходимость в загрузочном носителе или сетевом подключении для запуска утилиты аварийного восстановления. Восстановление при загрузке особенно полезно для мобильных пользователей. В случае сбоя пользователь перезагружает машину, нажимает F11 при появлении подсказки «Press F11 for Startup Recovery Manager...» и выполняет восстановление данных так же, как с обычного загрузочного носителя. Ограничение: требуется повторная активация загрузчиков, кроме загрузчиков Windows и GRUB.

Д

Дифференциальное резервное копирование

В дифференциальной резервной копии хранятся только те данные, которые отличаются от содержимого последней версии полной резервной копии. Для восстановления данных из нее необходим доступ к дифференциальной резервной копии.

И

Инкрементная резервная копия

Резервная копия, в которой хранятся изменения, произведенные в данных относительно самой поздней резервной копии. Для восстановления данных из нее необходим доступ к другим резервным копиям.

Н

Набор резервных копий

Группа резервных копий, к которым можно применить отдельное правило хранения. Для настраиваемой схемы резервного копирования наборы резервных копий соответствуют методам резервного копирования (полный, дифференциальный и инкрементный). Во всех других случаях используются ежемесячный, ежедневный, еженедельный и почасовой наборы резервного копирования. Ежемесячная резервная копия – это первая копия, которая создается после начала месяца. Еженедельная резервная копия создается в день недели, который задан с помощью параметра Еженедельная резервная копия (щелкните значок шестеренки и последовательно выберите пункты Параметры резервного копирования > Еженедельная резервная копия). Если еженедельная копия является первой с начала месяца, она считается ежемесячной. В этом случае еженедельная резервная копия создается в назначенный день на следующей неделе. Ежедневная резервная копия – это первая копия, которая создается после начала дня, если только она не является ежемесячной или еженедельной. Почасовая резервная копия – это первая копия, которая создается после начала часа, если только она не является ежемесячной, еженедельной или ежедневной

П

Полная резервная копия

Самостоятельная резервная копия, содержащая все необходимые данные. Для

© ООО Киберпротект, 2026

восстановления данных из нее не нужен доступ к какой-либо другой резервной копии.

У

Управляемое хранилище

Узел хранения обеспечивает управление хранилищем резервных копий. Физически управляемое хранилище может находиться на общем сетевом ресурсе, в сети хранения данных (SAN), в сетевом хранилище данных (NAS), на локальном жестком диске узла хранения или в библиотеке ленточных носителей, локально подключенной к узлу хранения. Узел хранения выполняет очистку и проверку (если таковые включены в план защиты) для каждой резервной копии в управляемом хранилище. Вы можете указать дополнительные операции, которые должен выполнять узел хранения (дедупликация, защита паролем).

Ф

Формат резервной копии в виде одного файла

Новый формат резервных копий, в котором начальная полная и последующие инкрементные резервные копии сохраняются в одном TIB-файле вместо цепочки файлов. Преимуществом этого формата является скорость инкрементного метода; при этом он лишен основного недостатка – сложностей, связанных с удалением устаревших копий. Программа помечает блоки, которые используются такими копиями, как свободные, и записывает на их место новые резервные копии. В результате очистка выполняется очень быстро и с минимальным потреблением ресурсов. Формат резервной копии в виде одного файла недоступен при резервном копировании в хранилища, которые не поддерживают операции произвольного чтения и записи, например, на сервера SFTP.

© ООО Киберпротект, 2026

Указатель

A

Active Protection для Linux 245

Active Protection для Windows 241

D

DefaultBlockSize 771

F

Flashback 404

L

Linux 183, 277

M

McAfee Endpoint Encryption и PGP Whole Disk Encryption 45

Microsoft Exchange Server 351

Microsoft SQL Server 350-351

N

NFS 271

O

Oracle Explorer 580

P

PE-образы 446

PE-образы на основе WinRE 446

PXE-сервер Киберпротект 472

R

RAID-5 464

S

Storage vMotion 673

V

vMotion 672

W

Windows 182, 277

WriteCacheSize 772

А

Автоинвентаризация 794

Автоматическая установка агента для Basis DynamiX Enterprise 140

Автоматическая установка агента для OpenNebula 148

Автоматическая установка агента для OpenStack 122

Автоматическая установка агента для oVirt 105

Автоматическая установка агента для Кибер Инфраструктуры 111

Автоматическая установка или автоматическое удаление 167

Автоматическая установка или автоматическое удаление в Linux 174

Автоматическая установка или автоматическое удаление в Windows 167

© ООО Киберпротект, 2026

Автоматический поиск драйверов 392

Автоматическое и ручное обнаружение 196

Автоматическое обнаружение машин 193

Авторское право 2

Агент 266

Агент для CommuniGate Pro, агент для VK WorkMail, агент для Mailion 26

Агент для Hyper-V 26

Агент для Linux 24

Агент для MySQL/MariaDB 24

Агент для Oracle 24

Агент для PostgreSQL 25

Агент для SQL, агент для Exchange, агент для Active Directory 23

Агент для VMware

необходимые привилегии 675

Агент для VMware (Windows) 24

Агент для Windows 23

Агент развертывания 89

Агенты 18, 23

Агенты, предоставляемые в виде виртуальных устройств 26

Активная защита (Active Protection) 240

Активный том 466

Алгоритм распределения 670

Архитектура 72

Б

База данных управления лентами 769

Безопасность 802

Безопасность на уровне файлов 404

Быстрое инкрементное/дифференциальное резервное копирование 355

В

В AAG включено резервное копирование баз данных 481

В Windows 60, 208

В интервале времени 296

В ОС Linux 61, 208

В случае ошибки повторить операцию 354, 402

Важная информация о преобразовании 302

Ввод паролей со специальными символами или пробелами 183

Веб-консоль Кибер Бэкап 210

Вернуть ленту в слот после каждого успешного создания резервной копии каждой машины 373

Взаимодействие с диспетчером съемных носителей Windows (RSM) 769

Виджет "Нет последних резервных копий" 725

Виджет "Резервные копии" 724

Виджет "Статус защиты" 724

Виртуальная машина 388

Вкладка «Планы» 423

Вкладка «Хранилища резервных копий» 425

Включение или исключение файлов, соответствующих определенным критериям 356

Включите целевую виртуальную машину по окончании восстановления. 408

Включить восстановление файлов из образов дисков на лентах 372

Включить полное резервное копирование VSS 380

© ООО Киберпротект, 2026

Включить после восстановления 408

Возврат из реплики 666

Возврат к исходному начальному RAM-диску 394

Восстановление 382, 455

памятка 382

Восстановление CommuniGate Pro 527

Восстановление Kubernetes 635

Восстановление VK WorkMail и VK WorkDisk 551

Восстановление баз данных 605

Восстановление баз данных Microsoft Exchange Server 492

Восстановление баз данных Microsoft SQL Server 488

Восстановление баз данных Oracle с использованием Oracle Explorer 580

Восстановление баз данных PostgreSQL 594

Восстановление баз данных, включенных в AAG 482

Восстановление базы данных master 491

Восстановление базы данных с помощью SAP HANA Studio 650

Восстановление всего сервера 580, 604, 649

Восстановление данных Mailion 566

Восстановление данных Oracle с помощью сценариев 582

Восстановление данных Oracle с резервной копии RMAN 582

Восстановление данных из резервной копии 616

Восстановление данных из резервной копии с поддержкой приложений 603

Восстановление данных кластера Exchange 484

Восстановление данных пользователей VK WorkDisk 553

Восстановление данных пользователей VK WorkMail 551

Восстановление дисков с помощью загрузочного носителя 390

Восстановление до последнего состояния 581

Восстановление из определенной резервной копии 654

Восстановление из последней резервной копии 650

Восстановление конфигурации ESXi 398

Восстановление машины 384

Восстановление на Exchange Server 495

Восстановление по состоянию на более ранний момент времени 582

Восстановление полного пути 404

Восстановление почтовых ящиков 496

Восстановление почтовых ящиков Exchange и элементов почтового ящика 495

Восстановление приложений 476

Восстановление резервной копии RMAN из резервной копии на уровне файлов 582

Восстановление с загрузочного носителя из локально прикрепленного ленточного устройства 778

Восстановление с ленточного устройства из операционной системы 777

Восстановление с помощью загрузочного носителя с ленточного устройства, прикрепленного к узлу хранения 779

Восстановление серверов VK WorkMail и VK WorkDisk 557

Восстановление системных баз данных 491

© ООО Киберпротект, 2026

Восстановление таблиц 606

Восстановление файлов 394

Восстановление файлов с помощью веб-интерфейса 394

Восстановление файлов с помощью загрузочного носителя 396

Восстановление физической машины в виртуальную 386

Восстановление экземпляра PostgreSQL в виде файлов 594

Восстановление экземпляров 604

Восстановление элементов почтовых ящиков 498

Всегда инкрементное 272

Встроенные группы 248

Выбор баз данных Microsoft SQL Server 479

Выбор всей машины 272

Выбор данных Microsoft Exchange Server 480

Выбор данных для резервного копирования 272

Выбор дисков и томов 275

Выбор компонентов для установки 199

Выбор конфигурации ESXi 277

Выбор места сохранения 278

Выбор напрямую на машине 273, 275

Выбор операционной системы для управления дисками 457

Выбор почтовых ящиков сервера Exchange 488

Выбор файлов и папок 273

Выключать целевые виртуальные машины при запуске восстановления 408

Выполнение окончательного перехода на реплику 666

Выполните резервное копирование типичной машины перед резервным копированием нескольких машин со сходным содержимым. 192

Выполняйте резервное копирование разных машин в разное время. 192

Высокая доступность восстановленной машины 717

Высокоскоростная локальная сеть 192

Г

Где можно просмотреть имена файлов резервных копий? 344

Гранулярное восстановление баз данных PostgreSQL 597

Группы устройств 248

Д

Дата и время для файлов 402

Дедупликация 189

Дедупликация в архиве 348

Дедупликация данных 59

Действие при сбое плана 378

Действия, которые можно выполнить с репликой 663

Деление 371

Диагностика неполадок 815

Диспетчер восстановления при загрузке (Startup Recovery Manager) 470

Добавление vCenter или хоста ESXi 91

Добавление VLAN 450

Добавление административных учетных записей 809

Добавление кластера Kubernetes 626

© ООО Киберпротект, 2026

Добавление консоли к списку веб-узлов локальной интрасети 212

Добавление консоли к списку доверенных веб-узлов 214

Добавление машин через веб-интерфейс 86

Добавление машины 89

Добавление машины с ОС Linux 91

Добавление машины с ОС Windows 87

Добавление подключаемого модуля Киберпротект к WinPE 447

Добавление управляемого хранилища 187

Добавление хранилища резервных копий 287

Документация 287

Дополнительная настройка 49, 53, 57

Дополнительная настройка машин для сервера управления и СУБД PostgreSQL 53

Дополнительная настройка машины для сервера управления 57

Дополнительная настройка машины с ОС Linux 49

Дополнительная настройка машины с ОС Windows 50

Дополнительная настройка продукта Кибер Бэкап 50, 54

Дополнительная настройка СУБД PostgreSQL 54

Дополнительные параметры расписания 289

Дополнительные требования для виртуальных машин 486

Дополнительные требования для операций резервного копирования с поддержкой приложений 477

Достаточное свободное пространство в хранилище 192

Доступность параметров восстановления 399

Доступность параметров резервного копирования 335

Доступные действия с планами защиты 227

Драйверы для компонента Универсальное восстановление (Universal Restore) 445

Драйверы запоминающих устройств для обязательной установки 393

Другие компоненты 21

Е

Еженедельное резервное копирование 381

Если не отображаются резервные копии, хранящиеся на лентах 777

Если нужно создать виртуальную машину на сервере виртуализации 305

Если нужно сохранить виртуальную машину как набор файлов 305

Ж

Журнал аудита 739

Журнал событий Windows 381, 408

З

За указанное количество дней подряд не создано успешно ни одной резервной копии. 341

Завершить сеансы работы неактивных пользователей через 802

Загрузочные носители на основе Linux 429

Загрузочный носитель 427

Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE? 428

Загрузочный носитель на основе WinPE 446

© ООО Киберпротект, 2026

Замечания по использованию узла хранения 309

Запуск виртуальной машины из резервной копии (мгновенное восстановление) 659

Запуск машины 660

Запуск резервного копирования вручную 309

Защита CommuniGate Pro 502

Защита Kubernetes 616

Защита Mailion 558

Защита Microsoft SharePoint 475

Защита Microsoft SQL Server и Microsoft Exchange Server 475

Защита Oracle Database 569

Защита Oracle Database предыдущих версий 570

Защита SAP HANA 645

Защита VK WorkMail и VK WorkDisk 532

Защита баз данных MongoDB 610

Защита баз данных PostgreSQL 584

Защита баз данных Ред БД 607

Защита групп обеспечения доступности базы данных (DAG) 483

Защита группы Always On Availability Groups (AAG) 481

Защита данных MySQL и MariaDB 601

Защита контроллера домена 476

Защита паролем 301

Защита приложений Microsoft 475

Защита приложений, сервисов, баз данных 475

Защита хранилища паролем 189

Зеркальный том 463

Зеркальный чередующийся том 464

Зона безопасности 271

И

Известные проблемы и их решения 600

Извлечение 797

Извлечение файлов из локальных резервных копий 397

Извлечь ленты после каждого успешного резервного копирования каждой машины 373

Издания и лицензии Кибер Бэкап 16

Изменение буквы тома 467

Изменение идентификатора безопасности 407

Изменение метки тома 467

Изменение пула 782

Изменение учетных данных для доступа к Microsoft SQL Server или Microsoft Exchange Server 501

Изменение формата резервной копии на формат "Версия 12" 348

Имена без переменных 345

Именение параметров прокси-сервера в Linux 61

Имя файла резервной копии 343

Имя файла резервной копии по умолчанию 344

Инвентаризация 792

Инициализация диска 458

Инициализация кластера 78

Исключения файлов 403

Исключить системные файлы и папки 357

Исключить скрытые файлы и папки 357

© ООО Киберпротект, 2026

Использование компонента Универсальное восстановление (Universal Restore) 391

Использование кэша диска для ускорения восстановления 407

Использование локально присоединенного хранилища 669

Использование моментальных снимков оборудования SAN 691

Использование нескольких агентов 521

Использование переменных 345

Использование правил политики 274-275

Использование самозаверяющих сертификатов 217

Использование сертификата, выданного доверенным центром сертификации 218

Использование сохранённых поисковых запросов 742

Использовать наборы лент в пуле лент, выбранных для резервного копирования 376

Используемая конфигурация 803

Используйте следующие ленточные устройства и приводы 374

К

Как работает обычное преобразование в виртуальную машину 305

Кибер Инфраструктура или Кибер Хранилище 271

Кластерные ресурсы и службы Кибер Бэкап 84

Кластерные ресурсы и файловые системы 83

Кластерные службы 78

Клонирование базового диска 458

Команда до захвата данных 368

Команда до резервного копирования 365

Команда после восстановления 406

Команда после захвата данных 369

Команда после резервного копирования 367

Команда, выполняемая перед восстановлением 405

Команды до и после захвата данных 367

Команды до и после процедуры 365, 405, 667-668

Компонент Универсальное восстановление (Universal Restore) в Linux 394

Компонент Универсальное восстановление (Universal Restore) в Windows 392

Компоненты 18

Компоненты для удаленной установки 88

Компоненты кластера 72

Компоненты программного обеспечения для резервного копирования 573

Консолидация резервных копий 342

Копирование библиотек Microsoft Exchange Server 501

Л

Ленточные устройства 766

Локальное подключение 451

М

Мастер создания загрузочных носителей 429

Машина для PostgreSQL 52

Машина для сервера управления 51, 55

Методы преобразования 302

Методы проверки резервных копий 416

Миграция Linux-машины с логическими

© ООО Киберпротект, 2026

томами (LVM) 720

Миграция машины 717

Многопоточность 352

Многотомные моментальные снимки 360

Многоядерный процессор с тактовой частотой не менее 2,5 ГГц 191

Модуль резервного копирования

памятка 267

Моментальные снимки оборудования SAN 370

Моментальные снимки резервных копий на уровне файлов 358

Мониторинг, отчёты и аудит 723

Монтирование блочных iSCSI-устройств 81

Мультиплексирование 375

Н

На основе Linux 428

На основе WinPE 428

Назначение прав пользователя 66

Настройка Grafana Loki в качестве источника данных 757

Настройка Huawei OceanStor (Dorado) 701

Настройка LDAP-аутентификации для агента для ECP Veil 119

Настройка LDAP-аутентификации для агента для SpaceVM 116

Настройка LDAP-аутентификации для агента для zVirt 104

Настройка lsyncd 77

Настройка Microsoft Edge, Opera и Google Chrome 211

Настройка Mozilla Firefox 212

Настройка PAM-модуля 803

Настройка Prometheus в качестве источника данных 753

Настройка агента в ROSA Virtualization 107

Настройка арбитра 79

Настройка веб-браузера для выполнения встроенной проверки подлинности Windows 211

Настройка виртуального устройства 101

Настройка внешнего мониторинга 751

Настройка доступа по SSH-ключам 77

Настройка защиты паролем в планах защиты 301

Настройка кластера 78

Настройка конфигурационного файла pg_hba.conf 587

Настройка конфигурационного файла postgresql.conf 587

Настройка машины на загрузку с PXE 473

Настройка машины с агентом для oVirt 714

Настройка машины с агентом для VMware (Windows) 707

Настройка механизма stonith / fencing 80

Настройка отказоустойчивого кластера 72

Настройка отправки записей на Syslog-сервер 805

Настройка параметров установки в ОС Windows 63

Настройка плана защиты для CommuniGate Pro 517

Настройка режима отображения 454

Настройка резервного копирования баз данных MongoDB 611

Настройка резервного копирования с поддержкой приложений 602

© ООО Киберпротект, 2026

Настройка сетевых интерфейсов 75

Настройка сети 74, 450

Настройка системы мониторинга Grafana 761

Настройка уже зарегистрированного агента для VMware 94

Настройка устройств iSCSI 469

Настройка хранилища данных YADRO TATLIN.UNIFIED 693

Настройки компонента Универсальное восстановление (Universal Restore) 392

Настройки прокси-сервера 60

Настройки сертификата SSL 217

Настройки системы 800

Начало работы с ленточным устройством 774

Не запускать при подключении к следующим сетям Wi-Fi 298

Не запускать при работе на лимитном подключении 297

Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений) 354, 403

Необходимые пакеты для ОС Linux 36

О

О продуктах Кибер Инфраструктура и Кибер Хранилище 286

О разделе Зона безопасности 283

Обзор кластеров Exchange 483

Обзор решений высокой доступности для Microsoft SQL Server 481

Обнаружение ленточных устройств 780

Обнаруженные машины 724

Обновление агента для VMware (виртуальное устройство) 103

Обновление агентов 203

Обновление виртуальных устройств 202

Обновление Кибер Бэкап 205

Обновление токена VK WorkMail 557

Обновления 802

Обработка данных вне хоста (off-host) 413

Обработка ошибок 354, 402, 667

Общее правило резервного копирования 45

Общие ограничения 189, 573

Общие параметры 64

Общие требования 477

Объект высшего уровня 438

Объект переменной 439

Ограничение общего количества виртуальных машин 315

Ограничение общего количества планов для почтовых ящиков и баз данных PostgreSQL 317

Ограничение общего количества планов для файлового и дискового резервного копирования 315

Ограничения 33, 271, 278, 283, 303, 334, 402, 599, 663, 773

Ограничения дедупликации 189

Ограничения для имени файла резервной копии 344

Ограничения для Кибер Инфраструктуры и Кибер Хранилища 287

Одно дедуплицирующее хранилище на каждый узел хранения 191

Одновременное восстановление 691

Одновременное резервное копирование 312

Ожидать выполнения условий расписания 378

© ООО Киберпротект, 2026

Ожидающие операции 468

Окно резервного копирования 362

Операторы 261

Операции с динамическими группами 253

Операции с дисками 457

Операции с загрузочным носителем 453

Операции с лентами 783

Операции с планами защиты 227

Операции с пулами 782

Операции с резервными копиями 410

Операции с томами 463

Операции со статическими группами 249

Оповещения 341

Основной поиск событий 740

Основные меры предосторожности 457

Основные операции с отчётами 731

Особенности защиты паролем 301

Особенности резервного копирования VK WorkMail и VK WorkDisk на ленты 550

Остановка перехода к реплике 666

От 40 до 160 МБ ОЗУ на 1 ТБ уникальных данных 191

Отделы и административные учетные записи 806

Отключение SELinux 76

Отключение автоматического назначения для агента 671

Отключить автоматический DRS для агента 100

Отправка записей журнала аудита на Syslog-сервер 804

Отсутствие приложений, конкурирующих за ресурсы 191

Отчёты 729

Очистка от устаревших резервных копий 420

П

Панель мониторинга "Действия" 728

Панель мониторинга "Обзор" 723

Панель мониторинга "Оповещения" 726

Параллельные операции 772

Параметры 434

Параметры автоматической установки или автоматического удаления 169

Параметры возврата из реплики 667

Параметры восстановления 399

Параметры записи на ленты 770

Параметры информации 178

Параметры конфигурации 576

Параметры резервного копирования 335

Параметры резервного копирования по умолчанию 803

Параметры репликации 667

Параметры удаления 174, 178

Параметры установки 169, 175

Параметры установки агента 173, 177

Параметры установки сервера управления 172, 176

Параметры установки узла хранения 174

Параметры ядра 434

Перед началом 100

Перед резервным копированием 774-775

Перезаписать ленту в автономном ленточном устройстве при создании полной резервной копии 373

© ООО Киберпротект, 2026

Переименование 796

Переименование группы 262

Перемещение в другой пул 784

Перемещение в другой слот 783

Перемещение лент в пул Свободные ленты 786

Перемещение лент с данными между пулами 788

Перемещение пустых лент между пулами 787

Перераспределение 670

Переход к реплике 665

План защиты и модули 224

План конфликтует с уже примененными планами. 225

План устройства конфликтует с планом группы 226

Планирование 370

Планирование количества агентов для ECP VeiL 118

Планирование количества агентов для SpaceVM 115

Планирование по событиям 290

По общему размеру резервных копий 272

По событию в журнале событий Windows 291

Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины 355

Повторное сканирование 794

Подготовка 67, 87, 92, 184, 392, 577

Подготовка WinPE 4.0 и более поздние версии 446

Подготовка к установке в ОС Astra Linux SE 68, 97, 184

Подготовка кластера Kubernetes 619

Подготовка СУБД PostgreSQL 68

Подготовка узлов кластера 76

Подготовка файла kubeconfig 625

Подготовка хостов РУСТЭК к установке агента 129

Подготовьте драйверы 392

Поддерживаемое оборудование 769

Поддерживаемые веб-браузеры 23

Поддерживаемые версии ОС Windows 27

Поддерживаемые версии приложений Microsoft 36

Поддерживаемые интеграции со службами каталогов 45

Поддерживаемые конфигурации кластеров 481, 483

Поддерживаемые операционные системы и среды 23

Поддерживаемые платформы виртуализации 29

Поддерживаемые почтовые сервисы 35

Поддерживаемые расположения 278, 306, 414, 417, 420

Поддерживаемые СУБД 35

Поддерживаемые типы виртуальных машин 302

Поддерживаемые ядра Linux и готовые дистрибутивы 27

Поддержка миграции VM 672

Поддержка резервного копирования на ленту 768

Поддержка файловых систем 57, 457

Подключение агентов 86

Подключение баз данных Microsoft Exchange Server 494

© ООО Киберпротект, 2026

Подключение баз данных Microsoft SQL Server 491

Подключение к машине, загружаемой с носителя 450

Подключение томов из резервной копии 410

Подключение экземпляра PostgreSQL из архива 595

Показать уведомление о последнем входе текущего пользователя 802

Полезная информация о финализации 662

Пользователи завершили сеанс 295

Пользователь hacluster 78

Пользователь неактивен 294

Пользовательские группы 248

Пользовательские пулы 781

Пользовательские сценарии 438

Порядок обновления агента для VMware (виртуального устройства) с веб-консоли Кибер Бэкап 103

Порядок обновления агента для VMware (виртуальное устройство) версий, более ранних, чем 12.5.23094 103

Порядок обновления агентов из веб-консоли Кибер Бэкап 204

Порядок обновления агентов локально через установочный файл 203

Порядок создания Зоны безопасности 284

Порядок удаления Зоны безопасности 286

Порядок установки узла хранения в ОС Linux 184

Порядок установки узла хранения в ОС Windows 186

Посекторное резервное копирование 371

Почему нужно использовать раздел Зона безопасности? 283

Почему нужно использовать резервное копирование с поддержкой приложений? 485

Почтовый сервер 801

Права, требуемые для учетной записи входа 65

Правила выбора для Linux 274

Правила выбора для Windows 274

Правила для Windows и Linux 275

Правила только для Linux 276

Правила только для Windows 276

Правила хранения 299

Предварительная настройка PostgreSQL 586

Предварительная настройка базы данных 608

Предварительная настройка нескольких сетевых подключений 444

Предварительные требования 179, 195, 278, 477, 659, 774-775

Предварительные требования для защиты CommuniGate Pro 503

Предварительные требования для протокола TLS 804

Предельное количество виртуальных машин для резервного копирования 690

Предопределенный сценарий 436

Предупреждать об истечении срока действия локального пароля или пароля домена 802

Предупреждение о редактировании конфигурационного файла 803

Преобразование в виртуальную машину 302

Преобразование в виртуальную машину в плане защиты 304

Преобразование динамического диска MBR в GPT 460

© ООО Киберпротект, 2026

Преобразование диска

GPT в MBR 461

MBR в GPT 460

Преобразование диска в результате создания раздела Зона безопасности 284

Преобразование диска из базового в динамический 461

Преобразование диска из динамического в базовый 462

Преобразование резервных копий в виртуальные машины 421

Привязка виртуальной машины 670

Привязка вручную 671

Применение компонента Универсальное восстановление (Universal Restore) 393

Применение нескольких планов к устройству 225

Применение плана защиты к группе 262

Пример 294-299

Пример установки пакетов вручную 41

Пример. Аварийное резервное копирование при обнаружении «плохого блока» 292

Примеры 178, 182

Примеры записей 588

Примеры использования 306, 346, 659, 663, 672

Принципы работы 194

Приоритет ЦП 363

Проблемы с лицензией 226

Проверить IP-адрес устройства 299

Проверка наличия обновлений программного обеспечения 192

Проверка резервных копий 348, 401, 416

Проверьте наличие доступа к драйверам в загрузочной среде 392

Производительность 405, 667

Производительность и окно резервного копирования 361

Пропуск поврежденных секторов 355

Пропустить задание 379

Просмотр писем VK WorkMail 554

Просмотр результата распределения 671

Просмотр статуса резервного копирования в клиенте vSphere 674

Простой том 463

Процедура развертывания 115, 119

Процедуры восстановления для конкретных программ 45

Процесс обнаружения машины 195

Пулы лент 780

Р

Работа в VMware vSphere 662

Работа в подсетях 474

Разблокировка базы данных 610

Развертывание 286

Развертывание агента для VMware (виртуальное устройство) через веб-интерфейс 92

Развертывание агентов с использованием групповой политики 179

Развертывание и настройка 74

Развертывание Кибер Бэкап 62

Развертывание резервного копирования для Кибер Инфраструктуры 109

Развертывание шаблона OVF 100-101

© ООО Киберпротект, 2026

Размещайте базу данных дедупликации и дедуплицирующее хранилище на разных физических носителях. 190

Разрешение конфликтов плана 225

Расписание 287

Расположение шаблона OVF 100

Распределение ресурсов диска 667

Расширенный поиск событий 740

Регистрация 286

Регистрация агента вручную 181

Регистрация носителя в пользовательском интерфейсе носителя 451

Регистрация носителя на сервере управления 451

Регистрация установленного агента для VMware 93

Регистрация хранилища данных SAN на сервере управления 712

Регистрируемые события 743

Регулярное преобразование в ESXi и Hyper-V по сравнению с запуском виртуальной машины с резервной копии 303

Режим загрузки 401

Режимы отображения списка устройств 220

Резервная копия почтового ящика 487

Резервное копирование 264, 454, 775-776

Резервное копирование CommuniGate Pro 512

Резервное копирование PostgreSQL 591

Резервное копирование VK WorkMail и VK WorkDisk 540

Резервное копирование баз данных Microsoft SQL Server и Microsoft Exchange Server 479

Резервное копирование базы данных Oracle 577

Резервное копирование без использования локальной сети (LAN-free backup) для oVirt 318

Резервное копирование без использования локальной сети (LAN-free backup) для VMware 324

Резервное копирование без использования локальной сети посредством Windows-агента для VMware 332

Резервное копирование без использования локальной сети посредством виртуального устройства для VMware 325

Резервное копирование больших объемов данных 545

Резервное копирование больших объемов данных CommuniGate Pro 521

Резервное копирование виртуальных машин без использования локальной сети (LAN-free backup) 318

Резервное копирование виртуальных серверов 649

Резервное копирование данных CommuniGate Pro 518

Резервное копирование данных Kubernetes 628

Резервное копирование данных Mailion 563

Резервное копирование данных в сетевую папку и восстановление данных из сетевой папки 437

Резервное копирование данных на загрузочный носитель и восстановление данных с загрузочного носителя 437

Резервное копирование данных пользователей VK WorkDisk 543

Резервное копирование данных

© ООО Киберпротект, 2026

пользователей VK WorkMail 540

Резервное копирование кластеризованных машин Hyper-V 717

Резервное копирование кластеров CommuniGate Pro 523

Резервное копирование машины на локально подключенное ленточное устройство 774

Резервное копирование на ленточное устройство, подключенное к узлу хранения 775

Резервное копирование на уровне дисков 189

Резервное копирование на уровне файлов 190

Резервное копирование облачных виртуальных машин без доступа к гипервизору 721

Резервное копирование постоянных томов в хранилище Кибер Бэкап 641

Резервное копирование с поддержкой кластеров 483

Резервное копирование с поддержкой приложений 485

Резервное копирование сервера 579

Резервное копирование серверов VK WorkMail и VK WorkDisk 547

Резервное копирование физических серверов 645

Резервные копии CommuniGate Pro 525

Результаты 775-776

Рекомендации 402

Рекомендации по дедупликации 190

Рекомендуемая конфигурация продукта Кибер Бэкап 48, 52, 56

Рекомендуемые конфигурации оборудования для сервера управления 48

Репликация 306

Репликация виртуальных машин 662

Репликация и резервное копирование 662

Репликация резервных копий 414

Ресурсы кластера 73

Ручная инвентаризация 792

Ручная очистка ленточных приводов 799

Ручная установка агента для ECP VeiL 118

Ручная установка агента для oVirt 106

Ручная установка агента для SpaceVM 115

Ручная установка агента для VK Cloud 133

Ручная установка агента для VMware (виртуальное устройство) из шаблона OVF 100

С

С несколькими потоками 374

Свойства событий 292

Связанные с лентой параметры резервного копирования 772

Сервер SFTP и ленточное устройство 271

Сервер управления 18, 27, 442

Сервер управления на машине с ОС Linux или Windows, использующий СУБД SQLite 48

Сервер управления на машине с ОС Linux, использующий СУБД PostgreSQL 51

Сервер управления на машине с ОС Windows, использующий СУБД Microsoft SQL Server 55

Сетевой порт 444

Сетевые настройки 443

Системные требования 46

© ООО Киберпротект, 2026

Системные требования для агента 100

Скачивание файлов из архива VK WorkDisk 556

Сколько агентов необходимо? 100

Сколько требуется агентов для резервного копирования и восстановления данных кластера? 481, 484

Скорость вывода при резервном копировании 364

Служба теневого копирования томов (VSS) 379

Служба теневого копирования томов (VSS) для виртуальных машин 380, 667

Служебные пулы 781

Смысл использования моментальных снимков оборудования SAN 692

Советы по дальнейшему использованию библиотеки ленточных носителей 777

Совместимость с RSM и программным обеспечением других поставщиков 769

Совместимость с ОС Astra Linux SE 42

Совместимость с программами шифрования 44

Создавать ли загрузочный носитель или скачать готовый? 427

Создание MST-преобразования и извлечение пакетов установки 168

Создание загрузочных носителей 383

Создание и регистрация пользователя 109

Создание моментальных снимков LVM 359

Создание отделов 814

Создание плана защиты 224

Создание плана защиты для CommuniGate Pro 512

Создание плана резервного копирования 608

Создание плана репликации 664

Создание планов резервного копирования 578

Создание пула 782

Создание резервной копии данных кластера Exchange 484

Создание служебной учетной записи для агента Kubernetes 620

Создание тома 464

Сокращение журнала Microsoft SQL Server 358

Составной том 463

Сосуществование с программным обеспечением других поставщиков 769

Сохранение первоначальной реплики 668

Сохранить сведения о системе при сбое восстановления с перезагрузкой 403

Специальные операции с виртуальными машинами 659

Список сценариев 574

Способ использования Зоны безопасности 45

Способ резервного копирования кластера 350

Сравнение имени файла резервной копии и упрощенного именования файлов 346

Сравнение финализации и обычного восстановления 662

Стандартные параметры 169, 175

Стирание 796

Структура autostart.json 438

Схема резервного копирования 288

Сценарии интеграции с Oracle RMAN 574

Сценарии использования 410

Сценарии на загрузочных носителях 436

Сэкономить заряд батареи 296

© ООО Киберпротект, 2026

Т

Тестирование реплики 664

Технические требования и ограничения службы Active Protection 241

Тип элемента управления 440

Типичные правила установки 45

Типы и свойства лент 766

Типы динамических томов 463

Типы резервных копий 266

Точки подключения 359, 404

Требования 397, 410

Требования для виртуальных машин ESXi 478

Требования для виртуальных машин Hyper-V 478

Требования для хранилища данных NetApp SAN 699

Требования к контролю учетных записей пользователей (UAC) 90

Требования к оборудованию 48, 51, 55

Требования к организации сети 74

Требования к программному обеспечению 22

Требования к сети 722

Требования к учетным записям пользователей 496

Требуемые права пользователя 486, 488

У

Уведомления по электронной почте 353, 800

Увеличение объёма ОЗУ виртуального устройства 721

Удаление 797

Удаление CommuniGate Pro 531

Удаление агента для VMware (виртуальное устройство) 209

Удаление группы 263

Удаление машин из веб-консоли Кибер Бэкап 209

Удаление машины 661

Удаление продукта 208

Удаление пула 783

Удаление резервных копий 413

Удаление тома 466

Удаленное подключение 451

Узел хранения 21, 28

Указание набора лент 798

Указание параметров прокси-сервера в Windows 60

Управление дисками 456

Управление журналом аудита 804

Управление лентами 372, 407, 780

Управление лицензиями 192-193

Управление обнаруженными машинами 200

Управление питанием ВМ 408, 668

Управление средами виртуализации 673

Управление учетными записями пользователей и отделами организации 806

Управляемое хранилище 272

Уровень сжатия 352

Условия 356

Условия запуска 293

Условия запуска задания 378

Условия поиска 254

Установка 18, 71, 93, 185, 573

© ООО Киберпротект, 2026

Установка CommuniGate Pro 508

Установка Mailion 559

Установка PXE-сервера 472

Установка VK WorkMail 534

Установка агента для Basis DynamiX Enterprise 139

Установка агента для Basis DynamiX Enterprise вручную 142

Установка агента для ECP VeiL 120

Установка агента для Kubernetes 617

Установка агента для OpenNebula 146

Установка агента для OpenNebula вручную 151

Установка агента для OpenNebula вручную в СГУ "Горизонт-ВС" 155

Установка агента для OpenStack 121

Установка агента для OpenStack вручную 125

Установка агента для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация) 104

Установка агента для Proxmox 162

Установка агента для Proxmox вручную 163

Установка агента для SpaceVM 117

Установка агента для VK Cloud 134

Установка агента для VMware (Windows) 92

Установка агента для Кибер Инфраструктуры вручную 114

Установка агента для РУСТЭК вручную 130

Установка агентов 95

Установка агентов в ОС Linux вручную 97

Установка агентов в ОС Windows вручную 95

Установка в Linux 67

Установка в ОС Windows 63

Установка и настройка 589

Установка и настройка узла хранения 183

Установка или удаление продукта с использованием преобразования MST 168

Установка или удаление продукта с указанием параметров вручную 168

Установка Кибер Бэкап 83

Установка кластерного программного обеспечения 76

Установка пакетов вручную 41

Установка пакетов из репозитория 38

Установка сервера управления 63, 66

Установка узла хранения 184

Установленные библиотеки 803

Установлены ли необходимые пакеты? 37

Устранение неисправностей при автоматическом обнаружении 201

Ф

Файл настройки оповещений 727

Файлы сценария 438

Физическая машина 384

Фильтры файлов 356

Финализация машины 661

Формат резервной копии 347

Формат резервной копии и файлы резервных копий 347

Форматирование тома 468

Функция Changed Block Tracking (CBT) 349, 667

© ООО Киберпротект, 2026

Х

Хост хранилища резервных копий доступен 294

Ц

Цели использования мастера создания носителей 429

Ч

Чередующийся том 463

Что ещё нужно знать 300

Что необходимо для использования моментальных снимков оборудования SAN? 692

Что необходимо для использования резервного копирования с поддержкой приложений? 486

Что содержится в резервных копиях томов или дисков 276

Что такое файл резервной копии? 343

Ш

Шаг 1. Формирование маркера регистрации 180

Шаг 2. Создание MST-преобразования и извлечение пакета установки 180

Шаг 3. Настройка объектов групповой политики 180

Шифрование дисков Microsoft BitLocker 45

Э

Экспорт резервных копий 411

© ООО Киберпротект, 2026