КИБЕРПРОТЕКТ

КИБЕР Бэкап

Версия 17.0

Руководство пользователя

Редакция: 21.05.2024

Заявление об авторских правах

Содержание

1 Выпуски и лицензирование Кибер Бэкап **17**

2 Установка **18**

2.1 Обзор установки 18

2.1.1 Локальное развертывание 18

2.2 Компоненты 18

2.2.1 Агенты 18

2.2.2 Другие компоненты 21

2.3 Требования к программному обеспечению 22

2.3.1 Поддерживаемые веб-браузеры 22

2.3.2 Поддерживаемые операционные системы и среды 23

2.3.3 Поддерживаемые версии Microsoft Exchange Server 29

2.3.4 Поддерживаемые версии Microsoft SharePoint 29

2.3.5 Поддерживаемые платформы виртуализации 30

2.3.6 Пакеты Linux 35

2.3.7 Совместимость с программами шифрования 39

2.3.8 Поддерживаемые системы управления базами данных 40

2.3.9 Совместимость с ОС Astra Linux SE 41

2.4 Требования к системе 43

2.4.1 Рекомендуемые конфигурации оборудования для сервера управления 44

2.5 Поддержка файловых систем 53

2.6 Настройки прокси-сервера 55

2.6.1 В Windows 55

2.6.2 В ОС Linux 57

2.7 Локальное развертывание 58

2.7.1 Установка сервера управления 58

2.7.2 Добавление машин через веб-интерфейс 67

2.7.3 Локальная установка агентов 79

2.7.4 Автоматическая установка или автоматическое удаление 84

2.7.5 Стандартные параметры 85

2.7.6 Параметры установки сервера управления 89

2.7.7 Параметры установки агента 89

2.7.8 Параметры установки узла хранения 90

2.7.9 Регистрация машин вручную 95

2.7.10 Проверка наличия обновлений программного обеспечения 98

2.7.11 Управление лицензиями 98

2.8 Автоматическое обнаружение машин ... 100
2.8.1 Принципы работы ... 101
2.8.2 Предварительные требования ... 101
2.8.3 Процесс обнаружения машины ... 102
2.8.4 Автоматическое и ручное обнаружение ... 103
2.8.5 Управление обнаруженными машинами ... 107
2.8.6 Устранение неисправностей ... 108
2.9 Развертывание агента для VMware (виртуальное устройство) из шаблона OVF ... 109
2.9.1 Перед началом ... 109
2.9.2 Развертывание шаблона OVF ... 110
2.9.3 Настройка виртуального устройства ... 111
2.9.4 Обновление агента для VMware (виртуальное устройство) ... 113
2.10 Развертывание агента для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация) ... 113
2.10.1 Автоматическая установка oVirt ... 114
2.10.2 Установка oVirt вручную ... 115
2.10.3 Настройка агента в ROSA Virtualization ... 116
2.11 Развертывание резервного копирования для Кибер Инфраструктуры ... 118
2.11.1 Общие сведения ... 118
2.11.2 Известные проблемы и ограничения ... 118
2.11.3 Создание и регистрация пользователя ... 118
2.11.4 Установка виртуального устройства для Кибер Инфраструктуры ... 120
2.11.5 Подключение виртуального устройства к серверу управления ... 121
2.12 Развертывание агента для SpaceVM ... 121
2.12.1 Планирование количества агентов для SpaceVM ... 122
2.12.2 Процедура развертывания ... 122
2.12.3 Известные проблемы и ограничения ... 122
2.12.4 Установка агента для SpaceVM ... 122
2.13 Развертывание агента для ECP VeiL ... 124
2.13.1 Планирование количества агентов для ECP VeiL ... 124
2.13.2 Процедура развертывания ... 124
2.13.3 Известные проблемы и ограничения ... 124
2.13.4 Установка агента для ECP VeiL ... 125
2.14 Развертывание агента для OpenStack (РУСТЭК) ... 126
2.14.1 Подготовка хостов РУСТЭК к установке агента ... 126
2.14.2 Установка агента для OpenStack (РУСТЭК) вручную ... 127
2.15 Развертывание резервного копирования для Базис.DynamiX ... 131
2.15.1 Общие сведения ... 131

2.15.2 Известные проблемы и ограничения ... 131
2.15.3 Установка Базис.DynamiX ... 132
2.16 Развертывание агентов с использованием групповой политики ... 134
2.16.1 Предварительные требования ... 134
2.16.2 Шаг 1. Формирование маркера регистрации ... 134
2.16.3 Шаг 2. Создание MST-преобразования и извлечение пакета установки ... 135
2.16.4 Шаг 3. Настройка объектов групповой политики ... 135
2.17 Обновление виртуальных устройств ... 136
2.17.1 Локальные развертывания ... 136
2.18 Обновление агентов ... 137
2.19 Модернизация с предыдущих версий продукта ... 138
2.20 Удаление продукта ... 141
2.20.1 В Windows ... 141
2.20.2 В ОС Linux ... 141
2.20.3 Удаление агента для VMware (виртуальное устройство) ... 142
2.20.4 Удаление машин из веб-консоли Кибер Бэкап ... 142
2.21 Установка агентов ... 142
2.21.1 В Windows ... 142
2.21.2 В ОС Linux ... 144
3 Доступ к веб-консоли Кибер Бэкап ... 146
3.1 Локальное развертывание ... 146
3.1.1 В Windows ... 146
3.1.2 В ОС Linux ... 147
3.2 Смена языка ... 147
3.3 Настройка веб-браузера для выполнения встроенной проверки подлинности Windows ... 147
3.3.1 Настройка Microsoft Edge, Opera и Google Chrome ... 147
3.3.2 Настройка Mozilla Firefox ... 148
3.3.3 Добавление консоли к списку веб-узлов локальной интрасети ... 148
3.3.4 Добавление консоли к списку доверенных веб-узлов ... 150
3.4 Настройки сертификата SSL ... 153
3.4.1 Использование самозаверяющих сертификатов ... 153
3.4.2 Использование сертификата, выданный доверенным центром сертификации ... 154
4 Представление веб-консоли Кибер Бэкап ... 156
5 План защиты и модули ... 157
5.1 Создание плана защиты ... 157
5.2 Разрешение конфликтов плана ... 158
5.2.1 Применение нескольких планов к устройству ... 158

5.2.2 Разрешение конфликтов плана ... 158
5.3 Операции с планами защиты ... 159
5.3.1 Доступные действия с планами защиты ... 159
6 Резервное копирование ... 168
6.1 Модуль резервного копирования: памятка ... 170
6.1.1 Ограничения ... 172
6.2 Выбор данных для резервного копирования ... 174
6.2.1 Выбор всей машины ... 174
6.2.2 Выбор файлов и папок ... 174
6.2.3 Выбор дисков и томов ... 176
6.2.4 Выбор конфигурации ESXi ... 179
6.3 Выбор места назначения ... 180
6.3.1 Поддерживаемые расположения ... 180
6.3.2 Расширенный выбор вариантов хранения ... 181
6.3.3 О программе Зона безопасности ... 182
6.3.4 О программе Кибер Инфраструктура ... 186
6.4 Расписание ... 187
6.4.1 Схема резервного копирования ... 187
6.4.2 Дополнительные параметры расписания ... 189
6.4.3 Планирование по событиям ... 189
6.4.4 Условия запуска ... 192
6.5 Правила хранения ... 199
6.5.1 Что еще нужно знать ... 200
6.6 Защита паролем ... 201
6.6.1 Настройка защиты паролем в планах защиты ... 201
6.6.2 Защита паролем как свойство машины ... 201
6.6.3 Особенности защиты паролем ... 203
6.7 Преобразование в виртуальную машину ... 203
6.7.1 Методы преобразования ... 203
6.7.2 Важная информация о преобразовании ... 204
6.7.3 Преобразование в виртуальную машину в плане защиты ... 205
6.7.4 Как работает обычное преобразование в виртуальную машину ... 206
6.8 Репликация ... 207
6.8.1 Примеры использования ... 208
6.8.2 Поддерживаемые расположения ... 208
6.8.3 Рекомендации для пользователей с лицензией Advanced ... 209
6.9 Запуск резервного копирования вручную ... 209

6.10 Параметры резервного копирования ... 210
6.10.1 Доступность параметров резервного копирования ... 210
6.10.2 Оповещения ... 213
6.10.3 Консолидация резервных копий ... 213
6.10.4 Имя файла резервной копии ... 214
6.10.5 Формат резервной копии ... 218
6.10.6 Проверка резервных копий ... 220
6.10.7 Функция Changed Block Tracking (CBT) ... 221
6.10.8 Способ резервного копирования кластера ... 221
6.10.9 Уровень сжатия ... 223
6.10.10 Уведомления по электронной почте ... 223
6.10.11 Обработка ошибок ... 224
6.10.12 Быстрое инкрементное/дифференциальное резервное копирование ... 226
6.10.13 Фильтры файлов ... 226
6.10.14 Моментальные снимки резервных копий на уровне файлов ... 228
6.10.15 Сокращение журнала ... 229
6.10.16 Создание моментальных снимков LVM ... 229
6.10.17 Точки подключения ... 230
6.10.18 Многотомные моментальные снимки ... 231
6.10.19 Производительность и окно резервного копирования ... 231
6.10.20 Команды до и после процедуры ... 235
6.10.21 Команды до и после захвата данных ... 237
6.10.22 Моментальные снимки оборудования SAN ... 239
6.10.23 Планирование ... 240
6.10.24 Посекторное резервное копирование ... 241
6.10.25 Деление ... 241
6.10.26 Управление лентами ... 242
6.10.27 Действия при сбое задания ... 247
6.10.28 Условия запуска задания ... 247
6.10.29 Служба теневого копирования томов (VSS) ... 248
6.10.30 Служба теневого копирования томов (VSS) для виртуальных машин ... 249
6.10.31 Еженедельное резервное копирование ... 250
6.10.32 Журнал событий Windows ... 250
7 Восстановление ... **251**
7.1 Восстановление: памятка ... 251
7.2 Создание загрузочных носителей ... 251
7.3 Восстановление машины ... 252

7.3.1 Физическая машина ... 252
7.3.2 Восстановление физической машины в виртуальную ... 254
7.3.3 Виртуальная машина ... 256
7.3.4 Восстановление дисков с помощью загрузочного носителя ... 258
7.3.5 Использование Universal Restore ... 259
7.4 Восстановление файлов ... 262
7.4.1 Восстановление файлов с помощью веб-интерфейса ... 262
7.4.2 Восстановление файлов с помощью загрузочного носителя ... 264
7.4.3 Извлечение файлов из локальных резервных копий ... 264
7.5 Восстановление конфигурации ESXi ... 265
7.6 Параметры восстановления ... 266
7.6.1 Доступность параметров восстановления ... 266
7.6.2 Проверка резервных копий ... 268
7.6.3 Режим загрузки ... 268
7.6.4 Дата и время для файлов ... 269
7.6.5 Обработка ошибок ... 270
7.6.6 Исключения файлов ... 270
7.6.7 Безопасность на уровне файлов ... 271
7.6.8 Flashback ... 271
7.6.9 Восстановление полного пути ... 271
7.6.10 Точки подключения ... 272
7.6.11 Производительность ... 272
7.6.12 Команды до и после процедуры ... 272
7.6.13 Управление лентами ... 274
7.6.14 Изменение идентификатора безопасности ... 274
7.6.15 Управление питанием ВМ ... 275
7.6.16 Журнал событий Windows ... 275
7.6.17 Включить после восстановления ... 276
8 Операции с резервными копиями ... 277
8.1 Вкладка «Хранилище резервных копий» ... 277
8.2 Подключение томов из резервной копии ... 278
8.2.1 Требования ... 278
8.2.2 Сценарии использования ... 278
8.3 Экспорт резервных копий ... 279
8.4 Удаление резервных копий ... 281
9 Вкладка «Планы» ... 282
9.1 Обработка данных Off-host ... 283

9.1.1 Репликация резервной копии ... 283
9.1.2 Проверка ... 285
9.1.3 Очистка ... 287
9.1.4 Преобразование в виртуальную машину ... 288
10 Загрузочный носитель ... 290
10.1 Загрузочный носитель ... 290
10.2 Создавать ли загрузочный носитель или скачать готовый? ... 290
10.3 Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE? ... 291
10.3.1 На основе Linux ... 291
10.3.2 На основе WinPE ... 291
10.4 Мастер создания загрузочных носителей ... 292
10.4.1 Цели использования мастера создания носителей ... 292
10.4.2 32- или 64-разрядная версия ... 292
10.4.3 Загрузочные носители на основе Linux ... 292
10.4.4 Объект высшего уровня ... 301
10.4.5 Объект переменной ... 301
10.4.6 Тип элемента управления ... 302
10.4.7 Загрузочный носитель на основе WinPE ... 308
10.5 Подключение к машине, загружаемой с носителя ... 314
10.5.1 Настройка сети ... 314
10.5.2 Локальное подключение ... 315
10.5.3 Удаленное подключение ... 315
10.6 Регистрация носителя на сервере управления ... 315
10.6.1 Регистрация носителя в пользовательском интерфейсе носителя ... 315
10.7 Операции с загрузочным носителем ... 316
10.7.1 Настройка режима отображения ... 317
10.7.2 Резервное копирование ... 317
10.7.3 Восстановление ... 319
10.7.4 Управление дисками ... 319
10.7.5 Простой том ... 326
10.7.6 Составной том ... 326
10.7.7 Чередующийся том ... 327
10.7.8 Зеркальный том ... 327
10.7.9 Зеркальный чередующийся том ... 327
10.7.10 RAID-5 ... 327
10.8 Настройка устройств iSCSI ... 332
10.9 Восстановление при загрузке ... 333

10.9.1 Активация Восстановление при загрузке ... 334
10.9.2 Что происходит при активации Восстановление при загрузке ... 334
10.9.3 Деактивация Восстановление при загрузке ... 334
10.10 PXE-сервер Киберпротект ... 335
10.10.1 Установка PXE-сервера ... 335
10.10.2 Настройка машины на загрузку с PXE ... 336
10.10.3 Работа в подсетях ... 336
11 Защита приложений Microsoft ... 338
11.1 Защита Microsoft SQL Server и Microsoft Exchange Server ... 338
11.2 Защита Microsoft SharePoint ... 338
11.3 Защита контроллера домена ... 339
11.4 Восстановление приложений ... 339
11.5 Предварительные требования ... 340
11.5.1 Общие требования ... 340
11.5.2 Дополнительные требования для операций резервного копирования с поддержкой приложений ... 341
11.6 Резервное копирование базы данных ... 342
11.6.1 Выбор баз данных SQL ... 342
11.6.2 Выбор данных Exchange Server ... 343
11.6.3 Защита группы Always On Availability Groups (AAG) ... 344
11.6.4 Защита групп обеспечения доступности базы данных (DAG) ... 346
11.7 Резервное копирование с поддержкой приложений ... 348
11.7.1 Почему нужно использовать резервное копирование с поддержкой приложений? ... 348
11.7.2 Что необходимо для использования резервного копирования с поддержкой приложений? ... 349
11.7.3 Требуемые права пользователя ... 349
11.8 Резервная копия почтового ящика ... 350
11.8.1 Выбор почтовых ящиков сервера Exchange ... 351
11.8.2 Требуемые права пользователя ... 351
11.9 Восстановление баз данных SQL ... 351
11.9.1 Восстановление системных баз данных ... 354
11.9.2 Подключение баз данных SQL Server ... 355
11.10 Восстановление баз данных Exchange ... 355
11.10.1 Подключение баз данных Exchange Server ... 358
11.11 Восстановление почтовых ящиков Exchange и элементов почтового ящика ... 358
11.11.1 Восстановление на Exchange Server ... 359
11.11.2 Восстановить в Office 365 ... 359

11.11.3 Восстановление почтовых ящиков ... 360
11.11.4 Восстановление элементов почтовых ящиков ... 362
11.11.5 Копирование библиотек Microsoft Exchange Server ... 365
11.12 Изменение учетных данных для доступа к SQL Server или Exchange Server ... 365
12 Защита почтовых ящиков Office 365 ... 367
12.1 Зачем создавать резервную копию почтовых ящиков Office 365? ... 367
12.2 Что необходимо для резервного копирования почтовых ящиков? ... 367
12.3 Восстановление ... 367
12.4 Ограничения ... 368
12.5 Выбор почтовых ящиков ... 368
12.6 Восстановление почтовых ящиков и элементов почтовых ящиков ... 369
12.6.1 Восстановление почтовых ящиков ... 369
12.6.2 Восстановление элементов почтовых ящиков ... 370
12.7 Изменение учетных данных для доступа к Office 365 ... 371
12.8 Получение идентификатора и секрета приложения ... 371
13 Защита CommuniGate Pro ... 374
13.1 Зачем создавать резервную копию CommuniGate Pro ... 374
13.2 Что необходимо для резервного копирования CommuniGate Pro? ... 374
13.3 Возможности ... 374
13.3.1 Резервное копирование ... 374
13.3.2 Восстановление ... 374
13.4 Известные проблемы и ограничения ... 375
13.5 Предварительные требования для защиты CommuniGate Pro ... 375
13.5.1 Выключение ограничений на количество сессий ... 375
13.5.2 Инициализация соединения вручную ... 376
13.5.3 Установка прав пользователя ... 377
13.5.4 Разрешение подключения агента к серверу CommuniGate Pro ... 379
13.5.5 Устранение неполадок при подключении ... 379
13.6 Установка CommuniGate Pro ... 380
13.6.1 Установка агента CommuniGate Pro ... 381
13.6.2 Добавление хоста CommuniGate Pro ... 382
13.7 Резервное копирование CommuniGate Pro ... 384
13.7.1 Создание плана защиты для CommuniGate Pro ... 385
13.7.2 Настройка плана защиты для CommuniGate Pro ... 389
13.7.3 Резервное копирование данных CommuniGate Pro ... 390
13.7.4 Резервные копии CommuniGate Pro ... 392
13.8 Восстановление CommuniGate Pro ... 394

13.9 Удаление CommuniGate Pro ... 398
14 Защита VK WorkMail ... 399
14.1 Зачем обеспечивать защиту VK WorkMail ... 399
14.2 Что необходимо для резервного копирования ... 399
14.3 Возможности ... 399
14.4 Установка VK WorkMail ... 399
14.4.1 Установка агента для VK WorkMail ... 400
14.4.2 Настройка в панели администрирования VK WorkMail ... 402
14.4.3 Добавление хоста VK WorkMail ... 403
14.5 Резервное копирование VK WorkMail ... 405
14.5.1 Резервное копирование данных пользователей VK WorkMail ... 405
14.5.2 Резервное копирование сервера VK WorkMail ... 409
14.5.3 Особенности резервного копирования VK WorkMail на ленты ... 411
14.6 Восстановление VK WorkMail ... 412
14.6.1 Восстановление данных пользователей VK WorkMail ... 412
14.6.2 Просмотр писем VK WorkMail ... 415
14.6.3 Восстановление сервера VK WorkMail ... 418
14.7 Обновление токена VK WorkMail ... 418
15 Защита Oracle Database ... 420
16 Защита баз данных PostgreSQL ... 421
17 Защита данных MySQL и MariaDB ... 422
17.0.1 Ограничения ... 422
17.0.2 Известные проблемы и ограничения ... 423
17.1 Настройка резервного копирования с поддержкой приложений ... 423
17.2 Восстановление данных из резервной копии с поддержкой приложений ... 424
17.2.1 Восстановление всего сервера ... 425
17.2.2 Восстановление экземпляров ... 425
17.2.3 Восстановление баз данных ... 425
17.2.4 Восстановление таблиц ... 427
18 Защита баз данных Ред База Данных ... 429
19 Защита баз данных MongoDB ... 430
19.1 Настройка резервного копирования баз данных MongoDB ... 430
19.1.1 Предварительные требования ... 430
19.1.2 Настройка удаленного подключения к базе данных MongoDB ... 430
19.1.3 Создание скрипта с командами для утилиты mongodump ... 431
19.1.4 Создание плана резервного копирования ... 432
19.2 Восстановление данных из резервной копии ... 435

20 Защита Kubernetes ... **436**
20.1 Зачем защищать Kubernetes ... 436
20.2 Что необходимо для резервного копирования Kubernetes? ... 436
20.3 Возможности ... 437
20.4 Известные проблемы и ограничения ... 437
20.5 Установка Kubernetes ... 437
20.5.1 Установка сервера управления ... 437
20.5.2 Установка агента для Kubernetes ... 437
20.5.3 Добавление кластера Kubernetes ... 439
20.6 Резервное копирование Kubernetes ... 440
20.6.1 Предварительные требования ... 440
20.6.2 Создание плана защиты ... 440
20.6.3 Создание групп ... 444
20.7 Восстановление Kubernetes ... 445
21 Специальные операции с виртуальными машинами ... **448**
21.1 Запуск виртуальной машины из резервной копии (мгновенное восстановление) ... 448
21.1.1 Примеры использования ... 448
21.1.2 Предварительные требования ... 448
21.1.3 Запуск машины ... 449
21.1.4 Удаление машины ... 450
21.1.5 Финализация машины ... 450
21.2 Работа в VMware vSphere ... 451
21.2.1 Репликация виртуальных машин ... 451
21.2.2 Резервное копирование без использования локальной сети ... 458
21.2.3 Использование моментальных снимков оборудования SAN ... 461
21.2.4 Использование локально присоединенного хранилища ... 466
21.2.5 Привязка виртуальной машины ... 467
21.2.6 Поддержка миграции VM ... 469
21.2.7 Управление средами виртуализации ... 470
21.2.8 Просмотр статуса резервного копирования в клиенте vSphere ... 471
21.2.9 Агент для VMware: необходимые привилегии ... 472
21.3 Резервное копирование кластеризованных машин Hyper-V ... 477
21.3.1 Высокая доступность восстановленной машины ... 477
21.4 Ограничение общего количества виртуальных машин, для которых одновременно выполняется резервное копирование ... 478
21.5 Миграция машины ... 479
21.5.1 Миграция Linux-машины с логическими томами (LVM) ... 482

21.6 Виртуальные машины Windows Azure и Amazon EC2 ... 482
21.6.1 Требования к сети ... 483
22 Защита SAP HANA ... 484
23 Отказоустойчивый кластер Кибер Бэкап ... 485
24 Active Protection (Активная защита) ... 486
24.1 Настройка модуля Active Protection ... 487
24.1.1 Принцип работы ... 487
24.1.2 Действие при обнаружении ... 487
24.1.3 Защита сетевых папок ... 488
24.1.4 Защита на стороне сервера (внешняя защита сетевых папок) ... 488
24.1.5 Самозащита ... 488
24.1.6 Выявление процессов майнинга криптовалют ... 489
24.1.7 Исключения ... 490
25 Оценка уязвимостей ... 491
25.1 Поддерживаемые продукты Microsoft и сторонние продукты ... 491
25.1.1 Поддерживаемые продукты Microsoft ... 491
25.1.2 Поддерживаемые продукты для Windows от сторонних разработчиков ... 493
25.2 Настройка модуля Оценка уязвимостей ... 493
25.2.1 Объект сканирования ... 493
25.2.2 Расписание ... 493
25.3 Просмотр обнаруженных уязвимостей ... 494
26 Группы устройств ... 496
26.1 Встроенные группы ... 496
26.2 Пользовательские группы ... 496
26.3 Создание статической группы ... 497
26.4 Добавление устройств в статические группы ... 497
26.5 Создание динамической группы ... 498
26.5.1 Условия поиска ... 498
26.5.2 Операторы ... 505
26.6 Применение плана защиты к группе ... 506
27 Мониторинг и отчеты ... 507
27.1 Панель мониторинга "Обзор" ... 507
27.1.1 Кибер Бэкап ... 508
27.1.2 Статус защиты ... 508
27.1.3 Нет недавних резервных копий ... 509
27.2 Вкладка «Действия» ... 510
27.3 Отчеты ... 511

27.4 Настройка важности оповещений ... 514
27.4.1 Файл настройки оповещений ... 515
28 Расширенный выбор вариантов хранения ... 516
28.1 Ленточные устройства ... 516
28.1.1 Что такое ленточное устройство? ... 516
28.1.2 Поддержка резервного копирования на ленту ... 516
28.1.3 Начало работы с ленточным устройством ... 522
28.1.4 Управление лентами ... 527
28.2 Узлы хранения ... 538
28.2.1 Установка узла хранения и службы каталогизации ... 538
28.2.2 Добавление управляемого хранилища ... 539
28.2.3 Дедупликация ... 541
28.2.4 Защита хранилища паролем ... 544
28.2.5 Каталогизация ... 545
28.3 Настройка сервера управления для Huawei OceanStor (Dorado) ... 547
29 Настройки системы ... 555
29.1 Уведомления по электронной почте ... 555
29.2 Почтовый сервер ... 556
29.3 Безопасность ... 557
29.3.1 Завершить сеансы работы неактивных пользователей через ... 557
29.3.2 Показать уведомление о последнем входе текущего пользователя ... 557
29.3.3 Предупреждать об истечении срока действия локального пароля или пароля домена 557
29.4 Обновления ... 557
29.5 Параметры резервного копирования по умолчанию ... 558
29.6 Настройка анонимной регистрации ... 558
29.7 Настройка PAM-модуля ... 559
29.7.1 Установленные библиотеки ... 559
29.7.2 Используемая конфигурация ... 559
29.7.3 Предупреждение о редактировании конфигурационного файла ... 559
30 Управление учетными записями пользователей и отделами организации ... 560
30.1 Локальное развертывание ... 560
30.1.1 Отделы и учетные записи администратора ... 560
30.1.2 Добавление учетных записей администратора ... 563
30.1.3 Создание отделов ... 564
31 Устранение неисправностей ... 565
Глоссарий ... 566
Указатель ... 568

1 Выпуски и лицензирование Кибер Бэкап

Кибер Бэкап доступен в следующих выпусках:

- Cyber Backup 17 Standard Server – Кибер Бэкап для физического сервера.
- Cyber Backup 17 Standard Workstation – Кибер Бэкап для рабочей станции.
- Cyber Backup 17 Standard Virtual Host – Кибер Бэкап для платформы виртуализации.
- Cyber Backup 17 Standard Mailbox 5, 25, 100 mailboxes – Кибер Бэкап для почтовых ящиков (5, 25, 100 почтовых ящиков).
- Cyber Backup 17 Advanced Server – Кибер Бэкап Расширенная редакция для физического сервера.
- Cyber Backup 17 Advanced Workstation – Кибер Бэкап Расширенная редакция для рабочей станции.
- Cyber Backup 17 Advanced Universal – Кибер Бэкап Расширенная редакция для универсальной платформы.
- Cyber Backup 17 Advanced Virtual Host – Кибер Бэкап Расширенная редакция для платформы виртуализации.
- Cyber Backup 17 Advanced PostgreSQL – Кибер Бэкап Расширенная редакция для PostgreSQL.
- Cyber Backup 17 Advanced Kubernetes – Кибер Бэкап Расширенная редакция для Kubernetes.
- Cyber Backup 17 Advanced Mailbox 5, 25, 100 mailboxes – Кибер Бэкап Расширенная для почтовых ящиков (5, 25, 100 почтовых ящиков).

Все выпуски Кибер Бэкап лицензированы по количеству защищенных рабочих нагрузок и их типу (рабочая станция, сервер и виртуальный хост). Выпуски Кибер Бэкап доступны как с бессрочными лицензиями, так и с лицензиями на подписку.

Выпуски Кибер Бэкап Расширенная редакция, а также все выпуски Кибер Бэкап для почтовых ящиков доступны в пробной версии сроком на один месяц.

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**.

Примечание
От выпуска зависят функции продукта. Выпуски Кибер Бэкап Расширенная редакция обладают полным функционалом в отличие от базового функционала в выпусках Кибер Бэкап.

2 Установка

2.1 Обзор установки

Кибер Бэкап Сервер управления – это центр управления всеми резервными копиями. При локальном развертывании он устанавливается в локальной сети.

Сервер управления Кибер Бэкап отвечает за обмен данными с агентами Кибер Бэкап и выполняет общие функции управления планом. Перед выполнением любого действия защиты агенты обращаются к серверу управления для проверки предварительных требований. Иногда подключение к серверу управления утрачивается, что препятствует развертыванию новых планов защиты. Однако если план защиты уже развернут на машине, агент продолжает выполнять операции защиты на протяжении 30 дней после утраты связи с сервером управления.

Необходимо установить агент защиты на каждой машине, для которой планируется создать резервную копию.

2.1.1 Локальное развертывание

Локальное развертывание подразумевает установку всех компонентов продукта в локальной сети. Это единственный способ развертывания, доступный по бессрочной лицензии. Кроме того, этот способ необходимо использовать, если машины не подключены к Интернету.

2.1.1.1 Расположение сервера управления

Сервер управления можно установить на машине с ОС Windows или Linux.

Рекомендуется установка в Windows, так как это позволит развертывать агенты с сервера управления на других машинах. Лицензия Advanced позволяет создавать организационные единицы и добавлять администраторов для них. Таким способом можно делегировать управление защитой другим пользователям, для которых разрешения на доступ явным образом ограничены соответствующими отделами.

Установка в Linux рекомендуется в средах на основе исключительно систем Linux. Агент потребуется установить локально на машинах, резервное копирование которых необходимо выполнять.

2.2 Компоненты

2.2.1 Агенты

Агенты – это приложения, выполняющие резервное копирование данных, их восстановление и другие операции на машинах под управлением Кибер Бэкап.

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?	Доступность агента локально
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		+
Приложения			
Базы данных SQL	Агент для SQL	На машину с сервером Microsoft SQL Server.	+
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 а любой машине с ОС Windows, которая имеет сетевой доступ к машине, на которой включена роль клиентского доступа Microsoft Exchange Server.	+
Почтовые ящики Microsoft Office 365	Агент для Office 365	На машину с Windows, которая подключена к Интернету.	+
Машины с доменными службами Active Directory	Агент для Active Directory	На контроллер домена.	+
Машины под	Агент для Oracle	На машину с запущенной	+

управлением Oracle Database		Oracle Database.	
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)	На хост ESXi.	+
Виртуальные машины Hyper-V	Агент для Hyper-V	На хост Hyper-V.	+
Виртуальные машины oVirt, ROSA Virtualization, zVirt, Red Hat Virtualization, РЕД Виртуализация	Агент для oVirt	На хост oVirt.	+
Виртуальные машины SpaceVM	Агент для SpaceVM	На хост SpaceVM.	+
Виртуальные машины ECP VeiL	Агент для ECP VeiL	На хост ECP VeiL.	+
Виртуальные машины OpenStack	Агент для OpenStack	На хост OpenStack.	+
Виртуальные машины Базис.Dynamix	Агент для Базис.Dynamix	На хост Базис.Dynamix.	+
Виртуальные машины в среде Windows Azure	То же самое, что и для физических машин***	На машину, резервная копия которой будет создана.	+
Виртуальные машины, размещенные в Amazon EC2			+
Виртуальные машины на хосте Citrix XenServer			+****
Виртуальные машины Red Hat Virtualization (RHV/RHEV)			

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

*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».

***Виртуальная машина считается виртуальной, если ее резервная копия была создана с использованием внешнего агента. Если агент установлен в гостевой системе, то операции резервного копирования и восстановления выполняются точно так же, как и на виртуальной машине.

****При наличии лицензии Advanced Virtual Host для Кибер Бэкап эти виртуальные машины считаются виртуальными (используется лицензия для каждого хоста). При наличии лицензии Virtual Host для Кибер Бэкап эти виртуальные машины считаются физическими (используется лицензия для каждого хоста).

2.2.2 Другие компоненты

Компонент	Функция	Куда его следует установить?	Доступность Локально
Сервер управления	Управляет агентами. Предоставляет пользователям веб-интерфейс.	На машине с ОС Windows или Linux.	+
Компоненты для удаленной установки	Сохраняет пакеты установки агента в локальную папку.	На машине Windows с сервером управления.	+
Мастер создания	Создает загрузочный носитель.	На машине с ОС Windows или Linux.	+

загрузочных носителей			
Программа командной строки	Предоставляет интерфейс командной строки.	На машине с ОС Windows или Linux.	+
Мониторинг Защиты Данных	Позволяет пользователям отслеживать резервные копии вне веб-интерфейса.	На машине с ОС Windows.	+
Узел хранения	Хранение резервных копий. Требуется для каталогизации и дедупликации.	На машине с ОС Windows или Linux.	+
Служба каталога	Выполняет каталогизации резервных копий на узлах хранения.	На машине под управлением ОС Windows.	+
PXE-сервер	Активирует загрузку машин на загрузочный носитель по сети.	На машине под управлением ОС Windows.	+

2.3 Требования к программному обеспечению

2.3.1 Поддерживаемые веб-браузеры

Веб-интерфейс сервиса резервного копирования поддерживает перечисленные ниже браузеры:

- Яндекс Браузер 21 или более поздней версии
- Google Chrome 90 или более поздней версии
- Opera 77 или более поздней версии
- Mozilla Firefox 86 или более поздней версии
- Microsoft Edge 112 или более поздней версии

В других веб-браузерах (включая браузеры Safari, запущенные в других операционных системах) может неправильно отображаться интерфейс пользователя или могут быть недоступны некоторые функции.

2.3.2 Поддерживаемые операционные системы и среды

2.3.2.1 Агенты

Агент для Windows

- Windows 7 с пакетом обновления 1 (SP1) и более поздних версий
- Windows Server 2008 R2 – выпуски Standard, Enterprise, Datacenter, Foundation и Web
- Windows 8/8.1 – все выпуски (x86, x64), за исключением выпусков Windows RT
- Windows Server 2012/2012 R2 – все выпуски
- Windows Storage Server 2008 R2/2012/2012 R2/2016
- Windows 10 – выпуски Home, Pro, Education, Enterprise, IoT Enterprise и LTSC (прежнее название LTSB)
- Windows Server 2016 – все варианты установки, кроме Nano Server
- Windows Server 2019 – все варианты установки, кроме Nano Server
- Windows Server 2022 – все варианты установки, кроме Nano Server

Агент для SQL, агент для Exchange (для резервного копирования базы данных и резервного копирования с поддержкой приложений), агент для Active Directory

Каждый из этих агентов можно установить на машине с любой из перечисленных выше операционных систем и поддерживаемой версией соответствующего приложения. Есть следующие исключения:

- Agent для SQL не поддерживается в локальном развертывании в Windows 7 выпусков "Начальная" и "Домашняя" (x86, x64)

Агент для Exchange (для резервного копирования почтового ящика)

Этот агент можно установить на машине с или без Microsoft Exchange Server.

- Windows 7 – все выпуски
- Windows Server 2008 R2 – выпуски Standard, Enterprise, Datacenter, Foundation и Web
- Windows 8/8.1 – все выпуски (x86, x64), за исключением выпусков Windows RT
- Windows Server 2012/2012 R2 – все выпуски
- Windows Storage Server 2008 R2/2012/2012 R2
- Windows 10 – выпуски Home, Pro, Education и Enterprise
- Windows Server 2016 – все варианты установки, кроме Nano Server
- Windows Server 2019 – все варианты установки, кроме Nano Server
- Windows Server 2022 – все варианты установки, кроме Nano Server

Агент для Office 365

- Windows Server 2008 R2 – выпуски Standard, Enterprise, Datacenter, Foundation и Web
- Windows 8/8.1 – все выпуски (только x64), кроме выпусков Windows RT
- Windows Server 2012/2012 R2 – все выпуски
- Windows Storage Server 2008 R2/2012/2012 R2/2016 (только x64)
- Windows 10 – выпуски Home, Pro, Education и Enterprise (только x64)
- Windows Server 2016 – все варианты установки (только x64), кроме Nano Server
- Windows Server 2019 – все варианты установки (только x64), кроме Nano Server
- Windows Server 2022 – все варианты установки (только x64), кроме Nano Server

Агент для Oracle

- Windows Server 2008 R2 – выпуски Standard, Enterprise, Datacenter и Web (x86, x64)
- Windows Server 2012 R2 – выпуски Standard, Enterprise, Datacenter и Web (x86, x64)
- Linux: все ядра и дистрибутивы, которые поддерживаются агентом для Linux (перечислены ниже)

Агент для Linux

Linux с версией ядра от 3.0 до 6.7 и glibc версии 2.3.4 или более поздней, включая следующие дистрибутивы x86 и x86_64:

- Astra Linux 1.6, 1.7.0, 1.7.1, 1.7.2, 1.7.3, 1.7.4, 1.7.5, 1.8
- Альт Сервер 9, 10
- Альт Рабочая станция 9, 10
- Альт 8 СП
- РЕД ОС 7.2, 7.3, 8
- РОСА «КОБАЛЬТ» 7.9
- Red Hat Enterprise Linux 7.x, 8.0*, 8.1*, 8.2*, 8.3*
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS
- SUSE Linux Enterprise Server 12 – поддерживается в файловых системах, за исключением Btrfs
- SUSE Linux Enterprise Server 15
- Debian 10, 11
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3
- Oracle Linux 7.x, 8.0, 8.1, 8.2, 8.3 – Unbreakable Enterprise Kernel и Red Hat Compatible Kernel
- AlmaLinux 7.x, 8.x*

- AlterOS 7.5
- ОСнова 2.7

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

* Конфигурации со Stratis не поддерживаются.

Агент для VMware (виртуальное устройство)

Этот агент предоставляется в качестве виртуального устройства для запуска на хосте ESXi.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0, 8.0 Update 2

Агент для VMware (Windows)

Этот агент предоставляется в виде приложения Windows для работы в любой из перечисленных выше операционных систем для агента для Windows, но с исключением: 32-разрядные операционные системы не поддерживаются.

Агент для Hyper-V

- Windows Server 2008 R2 с ролью Hyper-V, включая режим установки Server Core
- Microsoft Hyper-V Server 2008 R2
- Windows Server 2012/2012 R2 с ролью Hyper-V, включая режим установки Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (только x64) с Hyper-V
- Windows 10 – выпуски Pro, Education и Enterprise с Hyper-V
- Windows Server 2016 с ролью Hyper-V – все варианты установки, кроме Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 с ролью Hyper-V – все варианты установки, кроме Nano Server
- Microsoft Hyper-V Server 2019

Агент для PostgreSQL

Поддерживаемые операционные системы Windows

- Windows Server 2008 R2 (x64)
- Windows Server 2012 R2 (x64)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows 7 (x64)

- Windows 8 или 8.1 (x64)
- Windows 10 (x64)

Поддерживаемые операционные системы Linux с версией ядра от 3.0 и выше

- Astra Linux 1.6 и выше
- РЕД ОС 7.2, 7.3, 8
- РОСА «КОБАЛЬТ» 7.9
- Альт Сервер 9, 10
- ОСнова 2.7
- Red Hat Enterprise Linux 7.x и выше
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS
- SUSE Linux Enterprise Server 12 и выше
- Debian 10 и выше
- CentOS 7.x и выше

Поддерживаемые системы управления базами данных

- PostgreSQL 11, 12, 13, 14, 15, 16
- Postgres Pro Standard 11, 12, 13, 14, 15, 16
- Postgres Pro Enterprise 11, 12, 13, 14, 15, 16
- Patroni 3.0-3.2.1
- Proxima DB 2.0
- СУБД Jatoba (без поддержки подключения томов и гранулярного восстановления)
- СУБД Tantor

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

Агент для oVirt (виртуальное устройство zVirt/ROSA Virtualization/РЕД Виртуализация)

Этот агент предоставляется в качестве виртуального устройства.

Поддерживаемые системы управления средами виртуализации

- oVirt 4.2, 4.3, 4.4, 4.5
- ROSA Virtualization 2.0, 2.1
- zVirt 3.0, 3.1, 3.2, 3.3, 4.0, 4.1
- Red Hat Virtualization 4.2, 4.3, 4.4
- РЕД Виртуализация 7.2, 7.3

Агент для SpaceVM (виртуальное устройство)

Этот агент предоставляется в качестве виртуального устройства.

Поддерживаемые системы

- SpaceVM версии от 6.0.5 до 6.4.1

Агент для ECP VeiL (виртуальное устройство)

Этот агент предоставляется в качестве виртуального устройства.

Поддерживаемые системы

- ECP VeiL версии от 4.7 до 5.1

Агент OpenStack (виртуальное устройство)

Этот агент предоставляется в качестве виртуального устройства.

Поддерживаемые системы управления средами виртуализации

- РУСТЭК 2.6
- OpenStack выпусков от Ussuri до Zed

Агент для Базис.Dynamix (виртуальное устройство)

Этот агент предоставляется в качестве виртуального устройства.

Поддерживаемые системы управления средами виртуализации

- Базис.Dynamix версии 3.8.8 и выше

2.3.2.2 Сервер управления (только в локальных развертываниях)

В Windows

Windows 7 – все выпуски (x86, x64)

Windows Server 2008 R2 – выпуски Standard, Enterprise, Datacenter и Foundation

Windows 8/8.1 – все выпуски (x86, x64), за исключением выпусков Windows RT

Windows Server 2012/2012 R2 – все выпуски

Windows Storage Server 2008 R2/2012/2012 R2/2016

Windows 10 – выпуски Home, Pro, Education, Enterprise, IoT Enterprise и LTSC (прежнее название LTSB)

Windows Server 2016 – все варианты установки, кроме Nano Server

Windows Server 2019 – все варианты установки, кроме Nano Server

Windows Server 2022 – все варианты установки, кроме Nano Server

В ОС Linux

Linux с версией ядра от 3.0 до 6.7 и glibc версии 2.3.4 или более поздней, включая следующие дистрибутивы x86_64:

Astra Linux 1.6, 1.7.0, 1.7.1, 1.7.2, 1.7.3, 1.7.4, 1.7.5, 1.8

Альт Сервер 9, 10

Альт Рабочая станция 9, 10

Альт 8 СП

РЕД ОС 7.2, 7.3, 8

РОСА «КОБАЛЬТ» 7.9

Red Hat Enterprise Linux 7.x, 8.0*, 8.1*, 8.2*, 8.3*

Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS

SUSE Linux Enterprise Server 12 – поддерживается в файловых системах, за исключением Btrfs

SUSE Linux Enterprise Server 15

Debian 10, 11

CentOS 7.x, 8.0, 8.1, 8.2, 8.3

Oracle Linux 7.x, 8.0, 8.1, 8.2, 8.3 – Unbreakable Enterprise Kernel и Red Hat Compatible Kernel

AlmaLinux 7.x, 8.x*

AlterOS 7.5

ОСнова 2.7

* Конфигурации со Stratis не поддерживаются.

2.3.2.3 Узел хранения (только в локальных развертываниях)

Внимание
Поддерживаются только 64-битные версии перечисленных операционных систем.

В Windows

- Windows 7
- Windows Server 2008 R2 – выпуски Standard, Enterprise, Datacenter и Foundation
- Windows 8/8.1 – все выпуски, кроме Windows RT
- Windows Server 2012/2012 R2 – все выпуски
- Windows Storage Server 2008 R2/2012/2012 R2/2016

- Windows 10 – выпуски Home, Pro, Education, Enterprise, и IoT Enterprise
- Windows Server 2016 – все варианты установки, кроме Nano Server
- Windows Server 2019 – все варианты установки, кроме Nano Server
- Windows Server 2022 – все варианты установки, кроме Nano Server

В Linux

Linux с версией ядра от 3.0 до 6.7 и glibc версии 2.3.4 или более поздней, включая:

- Astra Linux 1.6, 1.7.0, 1.7.1, 1.7.2, 1.7.3, 1.7.4, 1.7.5, 1.8
- Альт Сервер 9, 10
- Альт Рабочая станция 9, 10
- Альт 8 СП
- РЕД ОС 7.2, 7.3, 8
- РОСА «КОБАЛЬТ» 7.9
- Red Hat Enterprise Linux 7.x, 8.0, 8.1, 8.2, 8.3
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS
- SUSE Linux Enterprise Server 12 – поддерживается в файловых системах, за исключением Btrfs
- SUSE Linux Enterprise Server 15
- Debian 10, 11
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3
- Oracle Linux 7.x, 8.0, 8.1, 8.2, 8.3 – Unbreakable Enterprise Kernel и Red Hat Compatible Kernel
- AlmaLinux 7.x, 8.x
- AlterOS 7.5
- ОСнова 2.7

2.3.3 Поддерживаемые версии Microsoft Exchange Server

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

2.3.4 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.

2.3.5 Поддерживаемые платформы виртуализации

В следующей таблице приведены поддерживаемые платформы виртуализации.

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
HOSTVM		
HOSTVM 4	+	+
РЕД СОФТ		
РЕД Виртуализация 7.2, 7.3	+	+
РОСА		
ROSA Virtualization 2.0, 2.1	+	+
РУСТЭК		
РУСТЭК 2.6	+	+
zVirt		
zVirt 3.0, 3.1, 3.2, 3.3, 4.0, 4.1	+	+
VMware		
Версии VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0, 8.0 Update 2 **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 VMware Player		+
Microsoft		
Windows Server 2008 R2 с Hyper-V Microsoft Hyper-V Server 2008 R2 Windows Server 2012/2012 R2 с Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) с Hyper-V 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	+	+
Microsoft Virtual PC 2004 и 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
oVirt		
oVirt 4.2, 4.3, 4.4, 4.5	+	+
SpaceVM		

SpaceVM от 6.0.5 до 6.4.1	+	+
ECP VeiL		
ECP VeiL от 4.7 до 5.1	+	+
OpenStack		
От Ussuri до Zed	+	+
Базис.Dynamix		
Базис.Dynamix версии 3.8.8.	+	+
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		
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)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
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		+

* В этих редакциях транспорт HotAdd для виртуальных дисков поддерживается в vSphere 5.0 и более поздней версии. В версии 4.1 резервные копии могут выполняться медленнее.

** 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.

2.3.5.1 Ограничения

- **Отказоустойчивые машины**

  Агент для VMware выполняет резервное копирование отказоустойчивой машины, только если в VMware vSphere 6.0 и более поздней версии 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.
- **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:
  - 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.

2.3.6 Пакеты Linux

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

- 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.
- Библиотеки libelf-dev, libelf-devel или elfutils-libelf-devel для сборки ядер не ниже 4.15 и настроены с параметром CONFIG_UNWINDER_ORC=y. Для некоторых дистрибутивов их необходимо установить отдельно от заголовков ядра.

Имена этих пакетов зависят от используемого дистрибутива 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.

2.3.6.1 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.
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. 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.

2.3.6.2 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.
	perl	Выполните следующую команду: `$ yum install perl`
CentOS	kernel-devel gcc make elfutils-libelf-devel	Программа установки загрузит и установит пакеты автоматически.
	perl	Выполните следующую команду: `$ yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Выполните следующие команды:
		`$ sudo apt-get update`
		`$ sudo apt-get install linux-headers-$(uname -r)`
		`$ sudo apt-get install linux-image-$(uname -r)`
		`$ sudo apt-get install gcc-<версия>`
		`$ sudo apt-get install make`
		`$ sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source
	gcc
	make
	perl
		Выполните следующие команды:
		`$ sudo zypper install kernel-source`
		`$ sudo zypper install gcc`
		`$ sudo zypper install make`
		`$ sudo zypper install perl`
		Для OpenSUSE 12.3:
		`$ cd /usr/src/linux`
		`$ sudo make oldconfig && make modules_prepare && make prepare`

Astra Linux	rpm
	gcc
	make
	linux-headers
	Дополнительно для ядер версии 5.10 и новее:
	flex
	bison
		Выполните следующие команды:
		`$ sudo apt install rpm`
		`$ sudo apt install gcc`
		`$ sudo apt install make`
		`$ sudo apt-get install linux-headers-`uname -r``
		`$ 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
		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`
		Если версия пакетов в репозитории новее версии текущего ядра, необходимо также обновить ядро:
		`$ su -`
		`# apt-get update`
		`# apt-get dist-upgrade`

		`# update-kernel` И перезагрузите систему.

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

Пакеты будут загружены из репозитория дистрибутива и установлены.

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

2.3.6.3 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
   ```

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

2.3.7 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 на лету. 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 Зона 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.

2.3.7.1 Типичные правила установки

Настоятельно рекомендуется установить программу шифрования перед установкой агентов защиты.

2.3.7.2 Способ использования Зона безопасности

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

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

2.3.7.3 Общее правило резервного копирования

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

2.3.7.4 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

2.3.8 Поддерживаемые системы управления базами данных

Кибер Бэкап совместим со следующими системами управления базами данных:

- СУБД Ред База Данных 3.0
- PostgreSQL 11, 12, 13, 14, 15, 16
- Postgres Pro Standard 11, 12, 13, 14, 15, 16
- Postgres Pro Enterprise 11, 12, 13, 14, 15, 16
- Patroni 3.0-3.2.1

- Proxima DB 2.0
- СУБД Jatoba (без поддержки подключения томов и гранулярного восстановления)
- СУБД Tantor
- MongoDB
- Microsoft SQL Server 2012, 2014, 2016, 2017, 2019
- Oracle Database 11g и 12c, все выпуски

  Поддерживаются только конфигурации с одним экземпляром.
- SAP HANA 2.0 SPS 03, установленная в RHEL 7.6 на физической машине или виртуальной машине VMware ESXi

  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.

2.3.9 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.

2.3.9.1 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_16_64-bit.x86_64
myuser@astra-smol1-7-3:~$ sudo update-initramfs -u -k all
myuser@astra-smol1-7-3:~$ sudo reboot
```

```
myuser@astra-smol1-7-3:~$ sudo ./CyberBackup_16_64-bit.x86_64
...
```

2.3.9.2 Резервное копирование дисков и томов

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

2.3.9.3 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.

2.3.9.4 Восстановление дисков и томов

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

2.3.9.5 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
   ```

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.

2.3.9.6 Репликация резервных копий

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

2.3.9.7 Узел хранения

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

2.3.9.8 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.

2.4 Требования к системе

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

Устанавливаемые компоненты	Для установки необходимо место на диске	Минимальный используемый объем памяти
Агент для Windows	850 МБ	150 МБ
Агент для Windows и один из следующих агентов: • Агент для SQL • Агент для Exchange	950 МБ	170 МБ
Агент для Windows и один из следующих агентов: • Агент для VMware (Windows) • Агент для Hyper-V	1170 МБ	180 МБ
Агент для Office 365	500 МБ	170 МБ
Агент для Linux	2,0 ГБ	130 МБ
Только для локальных развертываний		

Сервер управления в Windows	1,7 ГБ	200 МБ
Сервер управления в Linux	1,5 ГБ	200 МБ
Сервер управления и агент для Windows	2,4 ГБ	360 МБ
Сервер управления и агенты на машине с ОС Windows, Microsoft SQL Server, Microsoft Exchange Server и доменными службами Active Directory	3,35 ГБ	400 МБ
Сервер управления и агент для Linux	4,0 ГБ	340 МБ
Узел хранения и агент для Windows • только 64-разрядная платформа • Для использования функции дедупликации требуется минимум 8 ГБ ОЗУ. Дополнительные сведения см. в разделе «Рекомендации по дедупликации».	1,1 ГБ	330 МБ

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 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.

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. 44).

2.4.1 Рекомендуемые конфигурации оборудования для сервера управления

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

2.4.1.1 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:

- добавлять не более 6 000 устройств (устройства – это физические и виртуальные машины, почтовые ящики, базы данных и т. д., то есть все то, что отображается в веб-консоли Кибер Бэкап в разделе **Устройства**);
- включать в общий план не более 250 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;
- использовать не более 6 000 лицензий (для повышения производительности рекомендуется использовать одну корпоративную лицензию, в которую включены все необходимые агенты и виртуальные устройства);
- 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.

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.shmmax = 100663296
   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
   ```

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.

Например, если сервер управления установлен на машину с ОС CentOS 7, лимит на количество одновременно открытых файлов для службы acronis_asm 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

   ```
   ulimit -n 1024
   ```

   на

   ```
   ulimit -n 10240
   ```

   и сохранив изменение.

3. Перезапустите службу:

   ```
   systemctl restart acronis_asm
   ```

2.4.1.2 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 продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 8 ядер);
- как минимум 16 ГБ ОЗУ (для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 24 ГБ);
- не менее 150 ГБ дискового пространства на SSD-диске;
- подключение к сети, поддерживающее скорость передачи данных от 30 МБ/с (для установок продукта 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.

Машина для PostgreSQL

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

- как минимум 4 ядра ЦП (для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 6-8 ядер);
- 16 ГБ ОЗУ;
- не менее 200 ГБ дискового пространства на SSD-диске;
- подключение к сети, поддерживающее скорость передачи данных от 30 МБ/с (для установок продукта 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:

- добавлять не более 8 000 устройств (устройства – это физические и виртуальные машины, почтовые ящики, базы данных и т. д., то есть все то, что отображается в веб-консоли Кибер Бэкап в разделе **Устройства**);
- включать в общий план не более 500 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;

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

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.shmmax = 100663296
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
```

Дополнительная настройка СУБД PostgreSQL

В конфигурационном файле postgresql.conf параметру max_connections необходимо назначить достаточно большое значение, например:

```
<...>
max_connections = 600
<...>
```

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

После изменения параметра 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.

Например, если сервер управления установлен на машину с ОС CentOS 7, лимит на количество одновременно открытых файлов для службы acronis_asm 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

   ```
   ulimit -n 1024
   ```

   на

   ```
   ulimit -n 10240
   ```

   и сохранив изменение.

3. Перезапустите службу:

```
systemctl restart acronis_asm
```

2.4.1.3 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.

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:

- добавлять не более 8 000 устройств (устройства – это физические и виртуальные машины, почтовые ящики, базы данных и т. д., то есть все то, что отображается в веб-консоли Кибер Бэкап в разделе **Устройства**);
- 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;
- использовать не более 8 000 лицензий (для повышения производительности рекомендуется использовать одну корпоративную лицензию, в которую включены все необходимые агенты и виртуальные устройства);
- 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.

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 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.

2.5 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.

<table>
<tr><th rowspan="2">Файловая система</th><th colspan="3">Поддержка</th><th rowspan="2">Ограничения</th></tr>
<tr><th>Агенты</th><th>Загрузочный носитель WinPE</th><th>Загрузочные носители на основе Linux</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Все агенты</td><td>+</td><td>+</td><td rowspan="3">Без ограничений</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>+</td></tr>
<tr><td>JFS</td><td rowspan="2">Агент для Linux</td><td>-</td><td>+</td><td rowspan="2">• Файлы невозможно исключить из резервной копии диска
• Невозможно включить быстрое инкрементное/дифференциальное резервное копирование</td></tr>
<tr><td>ReiserFS3</td><td>-</td><td>+</td></tr>
</table>

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 для Linux	-	+	Без ограничений
exFAT	Все агенты	+	+ Если резервная *копия хранится в* файловой	• Поддерживается только резервное копирование дисков/томов • Файлы невозможно исключить из резервной копии

			системе exFAT, загрузочный носитель невозможно использовать для восстановления.	• 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.

2.5.0.1 Дедупликация данных

ОС Windows Server 2012 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 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.

2.6 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.

2.6.1 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 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:

```
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
```

2.6.2 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.
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:

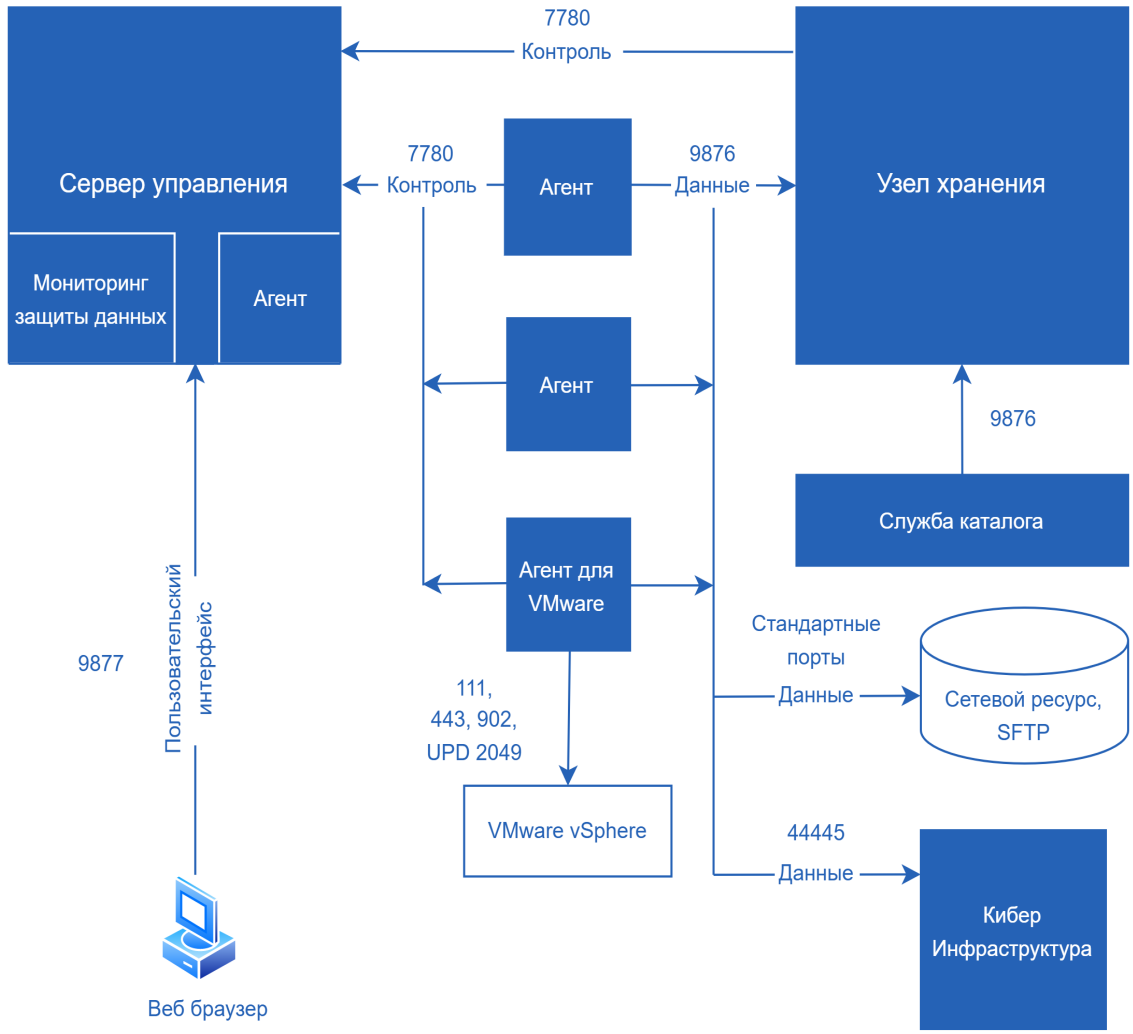
   ```
   sudo service aakore restart
   ```

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

```
sudo service acronis_mms restart
```

2.7 Локальное развертывание

Локальное развертывание включает в себя ряд программных компонентов, которые описаны в разделе Компоненты. На указанной ниже диаграмме показано взаимодействие компонентов и портов, которые требуются для этого взаимодействия. Стрелки направлены от тех компонентов, которые инициируют подключение.



2.7.1 Установка сервера управления

2.7.1.1 Установка в ОС Windows

Установка сервера управления

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щелкните **Язык установки**.
3. Примите условия лицензионного соглашения.
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**.

2.7.1.2 Настройка параметров установки

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

Общие параметры

- Устанавливаемые компоненты

Компонент	Описание
Сервер управления	Сервер управления – это центр управления всеми резервными

	копиями. При локальном развертывании он устанавливается в локальной сети.
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 Office 365	Этот агент создает резервную копию почтовых ящиков Microsoft Office 365 в локальном хранилище. Он устанавливается на машинах Windows. 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 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. Он устанавливается на машинах с Oracle Database. 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 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** (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**.
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 ASN 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:

  - 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.

2.7.1.3 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. Если требуется установить агент для Linux вместе с сервером управления, 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 также выполните следующие шаги. Предполагается, что включен режим замкнутой программной среды.

1. Распакуйте дистрибутив:

   ```
   tar --xattrs --xattrs-include=* -xvf CyberBackup_16_64-bit.x86_64.tar
   ```

2. Запустите файл установки с правами привилегированного пользователя:

```
./CyberBackup_16_64-bit.x86_64
```

3. Обновите образы initramfs:

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

4. Перезагрузите систему.

Подготовка СУБД PostgreSQL

Если планируется использовать СУБД PostgreSQL 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 или 16.

   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. Зайдите на машину с PostgreSQL от имени пользователя с привилегиями администратора. Создайте пользователя в PostgreSQL, от имени которого сервер управления будет подключаться к PostgreSQL, задайте для него пароль и назначьте ему привилегии LOGIN и SUPERUSER. Например:

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

   При установке сервера управления необходимо будет указать учетные данные созданного пользователя.

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
<...>
```

В этом примере cyberbackup — 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
<...>
```

В этом примере cyberbackup — пользователь, от имени которого сервер управления будет подключаться к PostgreSQL; 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)
     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=#
     ```

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_16_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. По умолчанию выбрана встроенная СУБД SQLite.

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

5. [Для СУБД PostgreSQL] Укажите сведения для подключения и аутентификации:
   - **Хост** – IPv4-адрес или DNS-имя машины с PostgreSQL. По умолчанию установлено значение localhost.
   - **Порт** – порт для подключения к PostgreSQL. По умолчанию установлено значение 5432.
   - **Пользователь** и **Пароль** – имя и пароль пользователя для подключения к PostgreSQL. Необходимо указать учетные данные пользователя, который был создан при подготовке PostgreSQL. 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.

2.7.2 Добавление машин через веб-интерфейс

Чтобы приступить к добавлению машины на сервер управления, щелкните **Все устройства** > **Добавить**.

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.

2.7.2.1 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.

Примечание
Удаленная установка не поддерживается для контроллеров домена. Процедуру установки агента защиты на контроллер домена см. в разделе "Установка в ОС Windows" (стр. 79). 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" (стр. 59).

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.
- Необходимо добавить 32-разрядную машину на 64-разрядный сервер управления или наоборот.
- Необходимо обновить агента на 32-разрядной машине с 64-разрядного сервера управления или наоборот.

Порядок размещения компонентов на сервере управления с ОС Windows

Если необходимо разместить компоненты с такой же разрядностью, как у сервера управления, используйте установщик продукта с соответствующей разрядностью. В противном случае используйте процедуру, приведенную ниже.

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)** или **Офлайн-установщик для Windows (32-bit)** и получите установщик продукта.
3. Загрузите установщик продукта на сервер управления и запустите его.
4. В мастере установки продукта нажмите **Сгенерировать .MST**.
5. В разделе **Устанавливаемые компоненты** выберите компоненты **Сервер управления**, **Компоненты для удаленной установки** и **Агент для Windows** и извлеките их файлы.
6. В зависимости от разрядности компонентов создайте папку x64 или x86 в папке %ProgramFiles%\Acronis\RemoteInstallationFiles\installation_files\<номер сборки продукта> и сохраните извлеченные файлы в созданную папку.
7. Убедитесь, что в папке %ProgramFiles%\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.
8. Перезапустите службу Acronis Service Manager с помощью Windows-оснастки «Службы».

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)** или **Офлайн-установщик для Windows (32-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** (в случае, если разрядности ОС машины и установщика продукта совпадают) или **Сгенерировать .MST** (в случае, если разрядности ОС машины и установщика продукта не совпадают).
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 в зависимости от разрядности компонентов создайте папку x64 или x86 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.
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 **Все устройства** > **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
   - 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
   - Агент для Office 365
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.

Как отключить UAC

Выберите один из следующих вариантов в зависимости от операционной системы.

- **В ОС Windows более ранней версии, чем Windows 8:**
  Выберите **Панель управления > Просмотр по: Мелкие значки > Учетные записи пользователей > Изменение параметров контроля учетных записей** и передвиньте ползунок на пункт **Никогда не уведомлять**. Перезапустите машину.
- **В любой операционной системе Windows**:
  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)

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**

2.7.2.2 Добавление машины с ОС Linux

1. Щелкните **Все устройства** > **Добавить**.
2. Щелкните **Linux**. Будет загружен файл установки.
3. На машине, которую нужно защитить, запустите программу установки локально.

2.7.2.3 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».

  Если сервер управления выполняется в Windows, агент будет автоматически развернут на указанной машине. В противном случае необходимо установить агент вручную.
- Регистрация установленного агента для VMware

  Это необходимый этап после переустановки сервера управления. Кроме того, можно зарегистрировать и настроить агент для VMware (виртуальное устройство), развернутое с шаблона OVF.
- 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 **Все устройства** > **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 Windows».

Установка

1. Щелкните **Все устройства** > **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.
9. Щелкните **Установить**, чтобы установить агент.

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 **Все устройства** > **Добавить**.
2. Щелкните **VMware ESXi**.
3. Выберите **Зарегистрировать уже установленный агент**.
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 **Все устройства** > **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 привилегиями на хосте vCenter Server или ESXi.
6. Щелкните **Настроить**, чтобы сохранить изменения.

2.7.2.4 Добавление хостов OpenStack (РУСТЭК)

Начиная с версии 16, Кибер Бэкап поддерживает резервное копирование и восстановление виртуальных машин OpenStack, а также РУСТЭК.

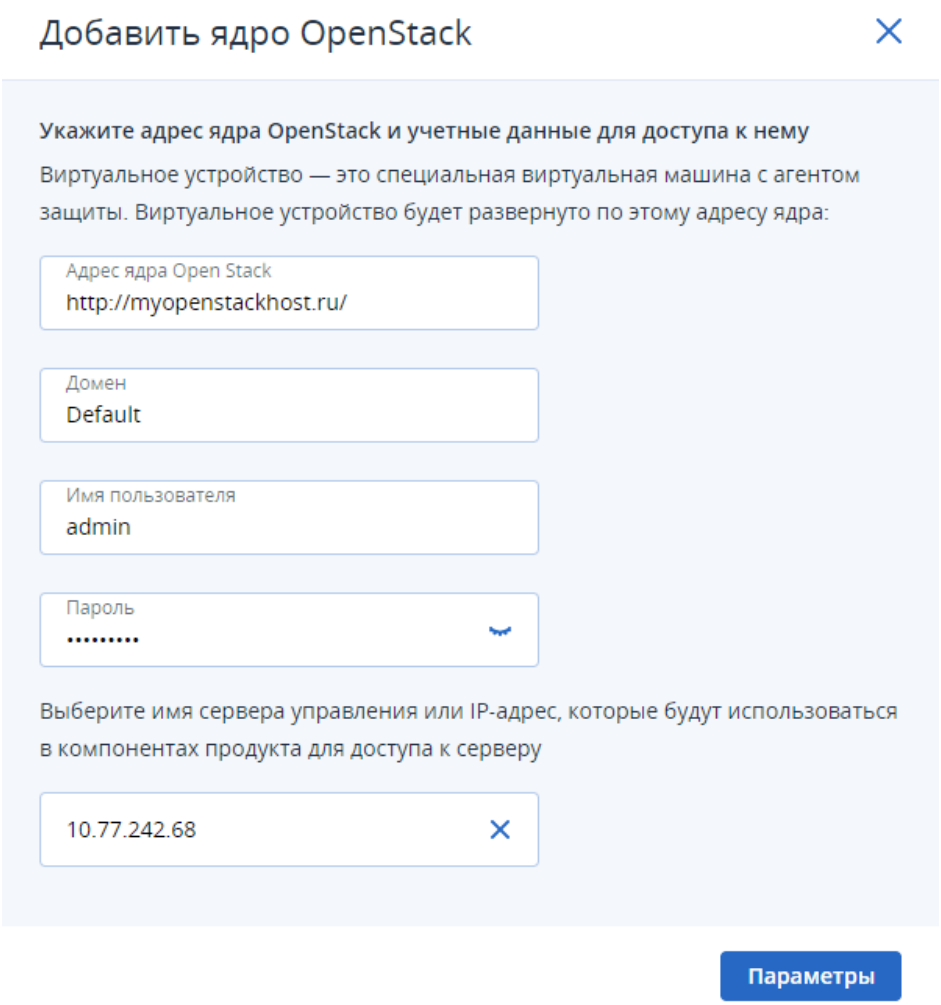
Резервная копия такой виртуальной машины содержит ее параметры и моментальный снимок ее дисков. Такую резервную копию можно восстановить на любой совместимый по версии хост. При восстановлении будет создана новая виртуальная машина с необходимыми параметрами, к которой будут подключены моментальные снимки дисков.

Для работы с виртуальными машинами хост OpenStack (РУСТЭК) необходимо предварительно добавить на сервер управления Кибер Бэкап. При этом на хосте будет развернуто виртуальное устройство – виртуальная машина с агентом Кибер Бэкап.

Производительность резервного копирования одного агента задана параметром **Планирование** плана защиты (см. "Параметры резервного копирования" (стр. 210)). Можно развернуть несколько виртуальных устройств с агентами для одного проекта OpenStack (РУСТЭК).

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

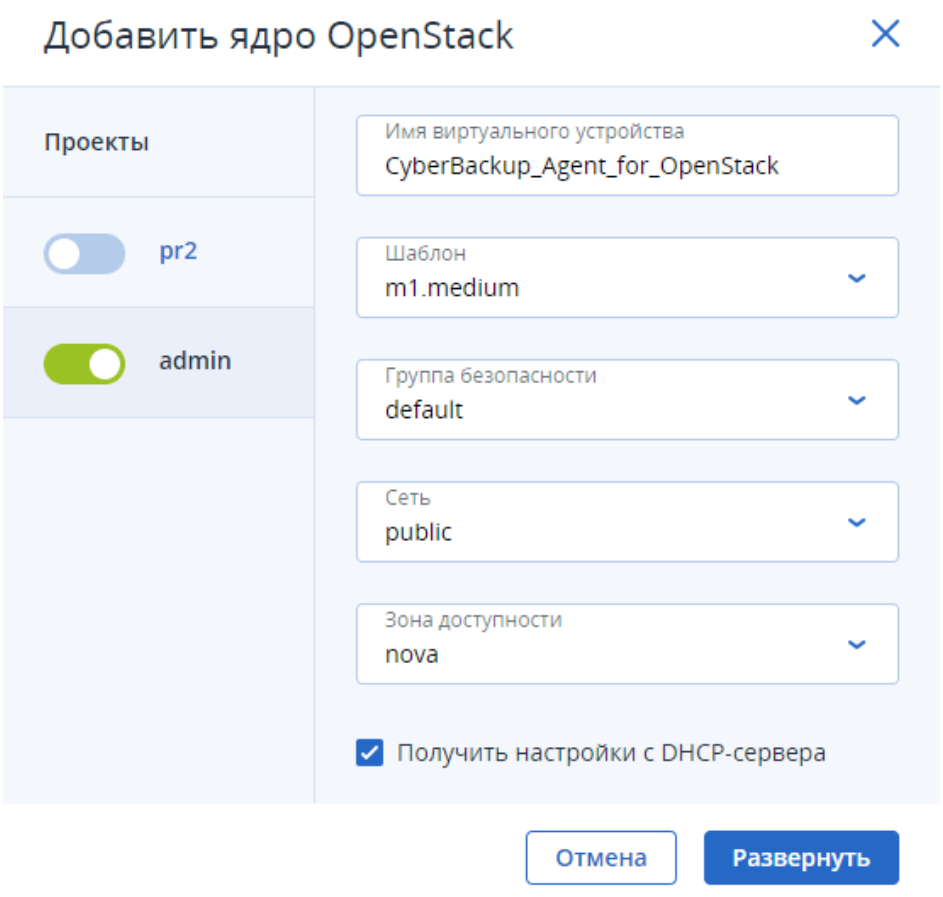
1. На вкладке **УСТРОЙСТВА** > **Все устройства** щелкните **Добавить**. Появится окно **Добавить устройства**.
2. В разделе **ХОСТЫ ВИРТУАЛИЗАЦИИ** щелкните **OpenStack**. Откроется окно **Добавить ядро OpenStack**.



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 **Параметры** 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:
   - **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 AMS и с контроллером OpenStack (РУСТЭК) через оконечную точку /identity. 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.

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, как описано в данном руководстве.

Примечание
В планах защиты таких виртуальных машин необходимо отключать функции **Active Protection** и **Оценка уязвимостей**.

Также агент можно установить вручную в панели управления OpenStack или РУСТЭК (см. раздел "Установка агента для OpenStack (РУСТЭК) вручную" (стр. 127)).

2.7.3 Локальная установка агентов

2.7.3.1 Установка в ОС Windows

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, щелкните **Язык установки**.
3. Примите условия лицензионного соглашения.
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 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".

      Если вы не являетесь администратором сервера управления, машину можно зарегистрировать и в этом случае. Для этого выберите параметр **Подключиться без проверки подлинности**. Это можно сделать, если на сервере управления разрешена анонимная регистрации (имейте в виду, что она может быть отключена).
   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 «Администраторы и отделы».
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 Office 365, 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, щелкните **Язык установки**.
3. Примите условия лицензионного соглашения.
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**.
   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".

      Если вы не являетесь администратором сервера управления, машину можно зарегистрировать и в этом случае. Для этого выберите параметр **Подключиться без проверки подлинности**. Это можно сделать, если на сервере управления разрешена анонимная регистрации (имейте в виду, что она может быть отключена).
   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 «Администраторы и отделы».
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».

2.7.3.2 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_*
```

Подготовка к установке в ОС Astra Linux SE

Перед установкой продукта в ОС Astra Linux SE также выполните следующие шаги. Предполагается, что включен режим замкнутой программной среды.

1. Распакуйте дистрибутив:

```
tar --xattrs --xattrs-include=* -xvf CyberBackup_16_64-bit.x86_64.tar
```

2. Запустите файл установки с правами привилегированного пользователя:

```
./CyberBackup_16_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_16_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 CommuniGate Pro**
      - **Агент для VK WorkMail**

- **Rescue Media Builder (компонент необходим для удаленного восстановления всей машины и дисков)**

Для агентов для Oracle, PostgreSQL, MySQL/MariaDB, Kubernetes, CommuniGate Pro, VK WorkMail также требуется установленный агент для Linux.

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 имя пользователя и пароль администратора сервера управления или выберите анонимную регистрацию.

      Если в вашей организации есть отделы, установка учетных данных может понадобиться, чтобы добавить машину в отдел, которым управляет указанный администратор. При анонимной регистрации машина всегда добавляется в организацию. Дополнительные сведения см. в разделе «Администраторы и отделы».

      Если анонимная регистрация на сервере управления отключена, необходимо указать учетные данные.

   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.**

2.7.4 Автоматическая установка или автоматическое удаление

2.7.4.1 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 «Установка агентов с помощью групповой политики».

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.

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 поле **Разрядность компонента** выберите **32-разрядная версия** или **64-разрядная версия**.
4. В разделе **Устанавливаемые компоненты** выберите компоненты, которые требуется установить. Пакеты установки для этих компонентов будут извлечены из программы установки.
5. Проверьте и при необходимости измените параметры установки, которые будут добавлены в MST-файл.
6. Нажмите кнопку **Создать**.

В результате создается MST-файл, а установочные MSI-пакеты и CAB-пакеты извлекаются в указанную папку.

Установка продукта с использованием преобразования MST

Выполните следующую команду:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

В этой формуле:

- <имя пакета> – это имя MSI-файла. Этот файл имеет имя **AB_AIP.msi** или **AB_AIP64.msi** в зависимости от разрядности операционной системы.

- <имя преобразования> – это имя преобразования. Этот файл имеет имя **AB_AIP.msi.mst** или **AB_AIP64.msi.mst** в зависимости от разрядности операционной системы.

Например, msiexec /i 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_AIP.msi** или **AB_AIP64.msi** в зависимости от разрядности операционной системы.

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 ab64.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 ab64.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
```

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

2.7.5 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	32-разрядная/64-разрядная	Сервер управления
WebConsole	AcronisCentralizedManagementServer	32-разрядная/64-разрядная	Веб-консоль
ComponentRegisterFeature	AcronisCentralizedManagementServer	32-разрядная/64-разрядная	Компоненты для удаленной установки
AgentsCoreComponents		32-разрядная/64-разрядная	Компоненты Core для агентов
BackupAndRecoveryAgent	AgentsCoreComponents	32-разрядная/64-разрядная	Агент для Windows
ArxAgentFeature	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Агент для Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Агент для SQL
ARADAgentFeature	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Агент для Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Агент для Oracle
ArxOnlineAgentFeature	AgentsCoreComponents	32-разрядная/64-разрядная	Агент для Office 365
AcronisESXSupport	AgentsCoreComponents	32-разрядная/64-разрядная	Агент для VMware (Windows)

HyperVAgent	AgentsCoreComponents	32-разрядная/64-разрядная	Агент для Hyper-V
ESXVirtualAppliance		32-разрядная/64-разрядная	Агент для VMware (виртуальное устройство)
CommandLineTool		32-разрядная/64-разрядная	Программа командной строки
TrayMonitor	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Мониторинг Защиты Данных
BackupAndRecoveryBootableComponents		32-разрядная/64-разрядная	Мастер создания загрузочных носителей
PXEServer		32-разрядная/64-разрядная	PXE-сервер
StorageServer	BackupAndRecoveryAgent	64-разрядная версия	Узел хранения
CatalogBrowser	Обновление 111 или более поздней версии для JRE 8	64-разрядная версия	Служба каталога

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, узел хранения и служба каталогизации, указанные в параметре ADDLOCAL, будут зарегистрированы на

этом сервере управления. Порт должен быть обязательно указан, если он отличается от установленного по умолчанию (9877).

Если анонимная регистрация на сервере управления отключена, 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>

Отдел в организации. Агенты, узел хранения и служба каталогизации, 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.

2.7.6 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>

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.

2.7.7 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.

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.

2.7.8 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.

2.7.8.1 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>
   ```

   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	Описание компонента

AcronisCentralizedManagementServer	Сервер управления
BackupAndRecoveryAgent	Агент для Linux
BackupAndRecoveryBootableComponents;	Мастер создания загрузочных носителей

Если данный параметр не указан, устанавливаются все перечисленные ниже компоненты.

--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. 63).

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>

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.

Если анонимная регистрация на сервере управления отключена, 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.

- --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.

```
./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
```

2.7.9 Регистрация машин 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.

Порядок регистрации машины

В командной строке машины, на которой установлен агент, выполните одну из следующих команд:

- Порядок анонимной регистрации машины

```
<path to the registration tool> -o register -a <management server address:port>
```

- <путь к инструменту регистрации> – это:
  - в ОС Windows: %ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe
  - в Linux: /usr/lib/Acronis/RegisterAgentTool/RegisterAgent

  <адрес сервера управления:порт> – это имя хоста или IP-адрес машины, на которой установлен сервер управления Кибер Бэкап. Если используется порт по умолчанию (9877), необязательно указывать его явно.

  Этот параметр доступен, только если на сервере управления включена анонимная регистрация. Если она отключена, необходимо зарегистрировать машину под конкретной учетной записью администратора или с помощью маркера регистрации. Дополнительную информацию об анонимной регистрации см. в разделе Настройка анонимной регистрации.

- Порядок регистрации машины под конкретной учетной записью администратора

  ```
  <path to the registration tool> -o register -a <management server address:port> -u <user name> -p <password>
  ```

  - <имя пользователя> и <пароль> – учетные данные учетной записи администратора, для которой будет зарегистрирован агент.

- Чтобы зарегистрировать машину в специальном отделе, укажите идентификатор отдела:

  ```
  <path to the registration tool> -o register -a <management server address:port> --tenant <unit ID>
  ```

  - Чтобы узнать идентификатор отдела, на веб-консоли Кибер Бэкап щелкните **Настройки** > **Учетные записи**, выберите нужный отдел и щелкните **Сведения**.

    Если анонимная регистрация отключена на сервере управления, необходимо добавить учетные данные для учетной записи администратора:

    ```
    <path to the registration tool> -o register -a <management server address:port> u <user name> -p <password> --tenant <unit ID>
    ```

Внимание
Администраторы могут только регистрировать агенты на их уровне в иерархии организации. Администраторы отдела могут регистрировать агенты в собственных отделах и их подотделах. Администраторы организации могут регистрировать агенты во всех отделах. Дополнительную информацию о разных учетных записях администратора см. в разделе Управление учетными записями пользователей и отделами организации.

- Порядок регистрации машины с использованием маркера регистрации

  ```
  <path to the registration tool> -o register -a <management server address:port> --token <token>
  ```

  - 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".

Отмена регистрации машины

В командной строке машины, на которой установлен агент, выполните следующую команду:

```
<path to the registration tool> -o unregister
```

2.7.9.1 Примеры

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a https://10.250.144.179:9877
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword --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
```

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a https://10.250.144.179:9877
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword --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
```

2.7.9.2 Пароли со специальными символами или пробелами

Если пароль содержит специальные символы или пробелы, заключите его в кавычки при вводе в командной строке.

```
<path to the registration tool> -o register -a <management server address:port> -u <user name> -p <"password">
```

Пример (для Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a https://10.250.144.179:9877 -u johndoe -p "johns password"
```

Если не удалось устранить ошибку:

1. Зашифруйте пароль в формат base64 на портале https://www.base64encode.org/.
2. В командной строке укажите зашифрованный пароль, используя параметры "-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==
```

2.7.10 Проверка наличия обновлений программного обеспечения

Эта функциональность доступна только для администраторов организации.

При каждом входе на веб-консоль Кибер Бэкап проверяет, доступна ли новая версия на веб-сайте Киберпротект. Если новая версия доступна, на веб-консоли Кибер Бэкап отображается ссылка на ее скачивание в нижней части каждой страницы на вкладках **Устройства**, **Планы** и **Хранилище резервных копий**. Ссылка также доступна на странице **Настройки** > **Агенты**.

Чтобы включить или отключить автоматические проверки наличия обновлений, измените системную настройку **Обновления**.

Чтобы проверить обновления вручную, щелкните значок вопроса в верхнем правом углу > **О программе** > **Проверить обновления** или значок вопроса > **Проверить обновления**.

2.7.11 Управление лицензиями

Лицензирование Кибер Бэкап основано на количестве физических машин и хостов виртуализации, подлежащих резервному копированию. Можно использовать как подписки, так и бессрочные лицензии. Период действия подписки начинается с момента ее регистрации на сайте Киберпротект.

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**.
4. Чтобы активировать подписку, необходимо выполнить вход. Если вы ввели хотя бы один ключ подписки, введите адрес электронной почты и пароль своей учетной записи Киберпротект, а затем нажмите кнопку **Вход**. Если вы ввели только бессрочные ключи, пропустите это действие.
5. Нажмите кнопку **Готово**.

Примечание
Если вы уже зарегистрировали ключи подписки, сервер управления может импортировать их из вашей учетной записи Киберпротект. Чтобы синхронизировать ключи подписки, щелкните **Синхронизация** и выполните вход.

2.7.11.1 Управление бессрочными лицензиями

Назначение бессрочной лицензии машине

1. Выберите бессрочную 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 бессрочной лицензии для машины

1. Выберите бессрочную 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.

2.7.11.2 Управление лицензиями по подписке

Назначение лицензии по подписке машине

1. Выберите лицензию по подписке.

   В программе отобразятся машины, которым уже назначена выбранная лицензия.
2. Щелкните **Назначить**.

   В программе отобразятся машины, которым можно назначить выбранную лицензию.
3. Выберите машину и нажмите кнопку **Готово**.

Отзыв лицензии по подписке для машины

1. Выберите лицензию по подписке.

   В программе отобразятся машины, которым уже назначена выбранная лицензия.
2. Выберите машину, для которой необходимо отозвать лицензию.
3. Щелкните **Отозвать лицензию**.
4. Подтвердите операцию.

2.8 Автоматическое обнаружение машин

Функциональность обнаружения машин позволяет выполнять указанные ниже действия.

- 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.

2.8.1 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.

2.8.2 Предварительные требования

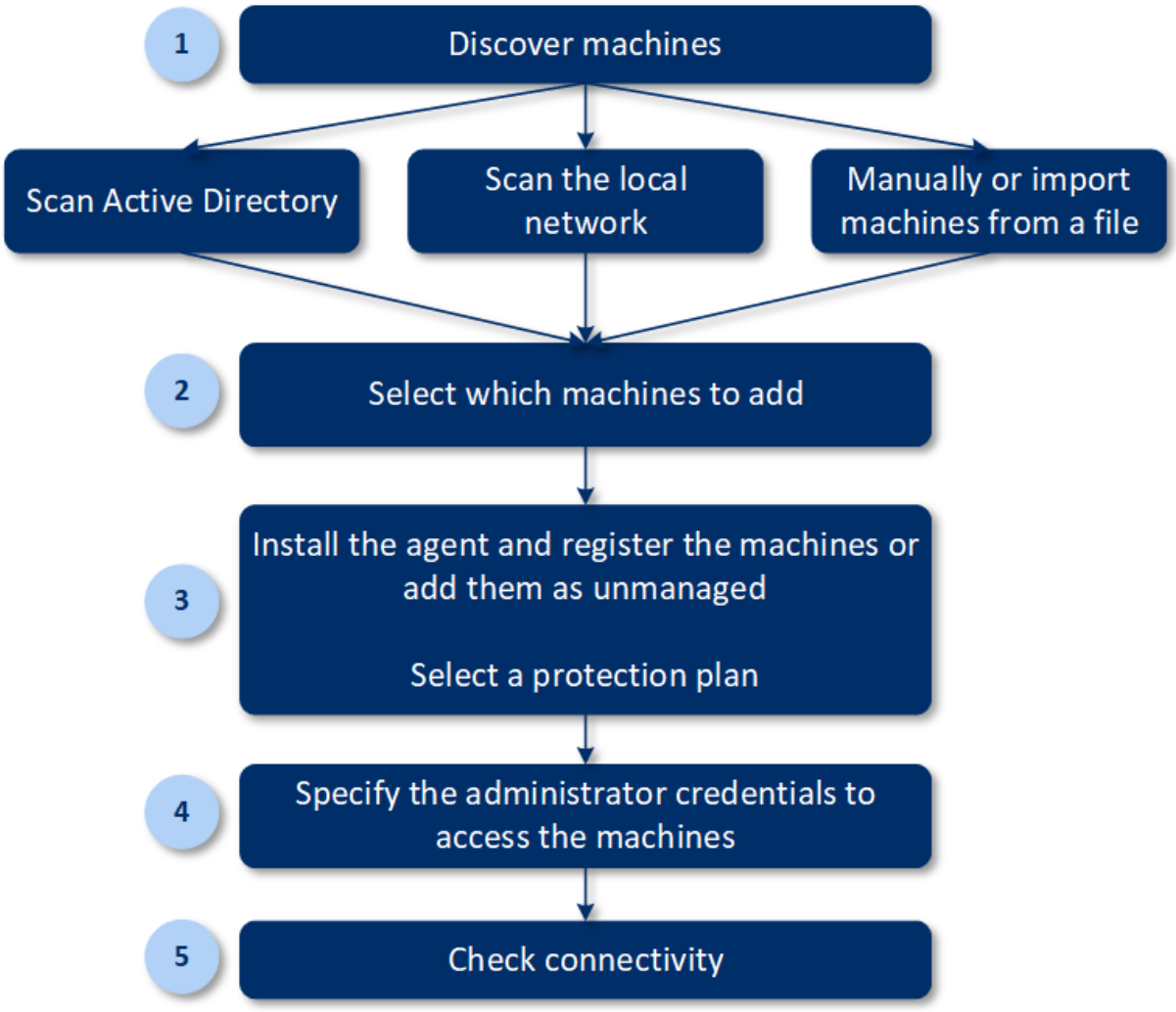
Прежде чем запустить обнаружение машин, необходимо установить агент защиты хотя бы на одной машине в локальной сети, чтобы использовать его как агент обнаружения.

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.

2.8.3 Процесс обнаружения машины

В приведенной ниже схеме указаны основные этапы процесса обнаружения машины.



Как правило, весь процесс автоматического обнаружения состоит из следующих этапов:

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.

2.8.4 Автоматическое и ручное обнаружение

Прежде чем запустить обнаружение, убедитесь, что соблюдены предварительные требования.

Обнаружение машин

1. На веб-консоли выберите пункты **Устройства** > **Все устройства**.
2. Нажмите кнопку **Добавить**.
3. В области **Несколько устройств** щелкните **Windows-only (Только для Windows)**. Откроется мастер обнаружения
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.
     - **Использовать следующую учетную запись**

       При установке агента в контроллере 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.

     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.

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**).

2.8.4.1 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.
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 Office 365	Этот агент создает резервную копию почтовых ящиков Microsoft Office 365 в локальном хранилище. Он устанавливается на машинах Windows. 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. Он устанавливается на машинах с Oracle Database. 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).

2.8.5 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.
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.

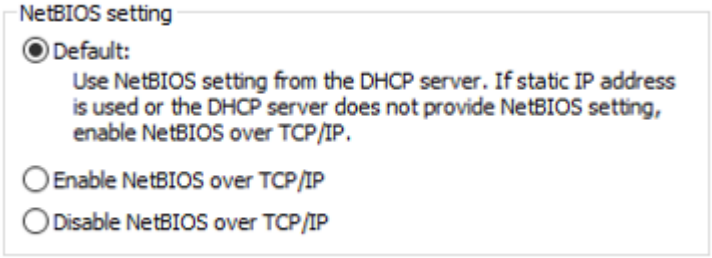
Те машины, на которых установлен агент защиты, отображаются в разделе **Устройства** > **Машины с агентами**.

Чтобы проверить статус защиты, откройте раздел **Панель мониторинга** > **Обзор** и добавьте виджет Статус защиты или виджет Обнаруженная машина.

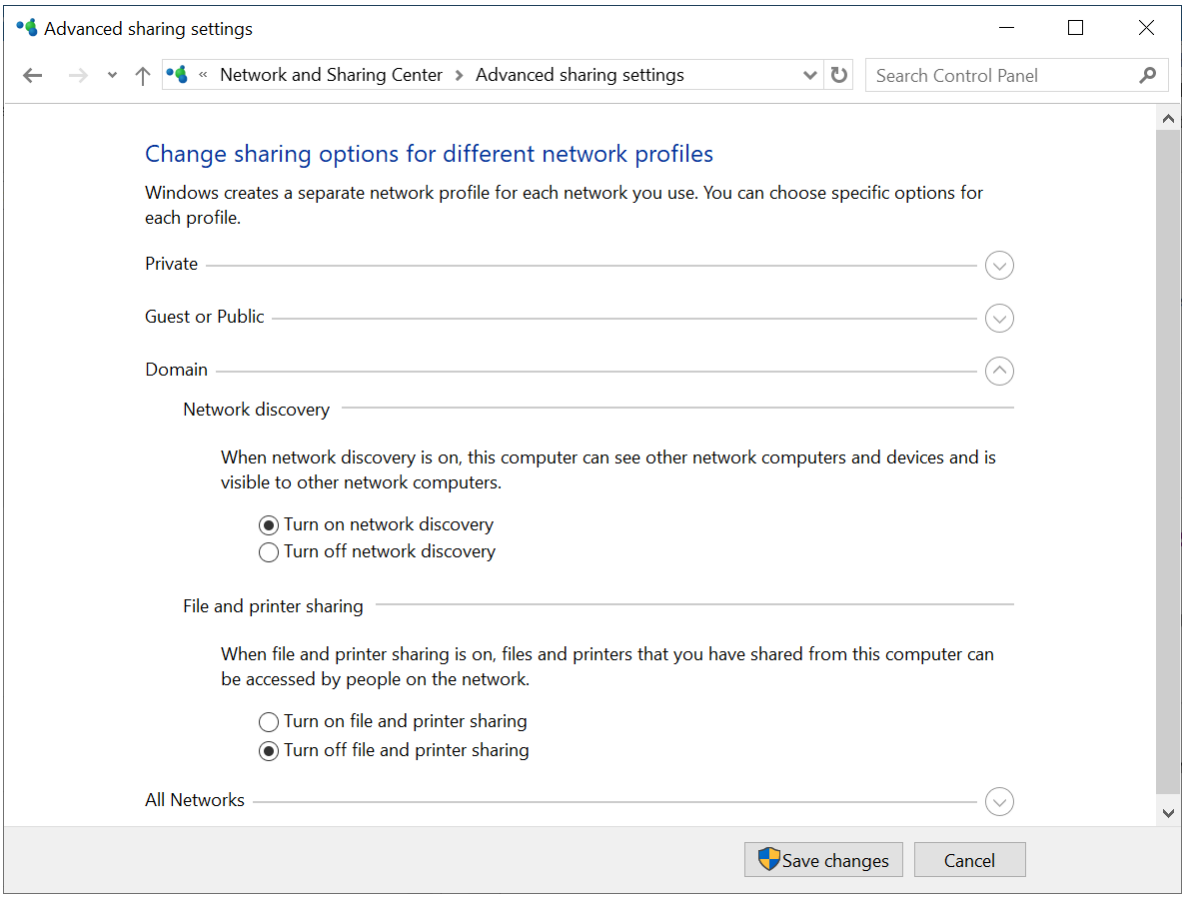
2.8.6 Устранение неисправностей

Если есть какие-либо проблемы с функциональностью автоматического обнаружения, выполните указанные ниже действия.

- Проверьте, что протокол "NetBIOS over TCP/IP" включен или задан по умолчанию.



- Выберите **Панель управления** > **Центр управления сетями и общим доступом** > **Дополнительные параметры общего доступа** и включите обнаружение сети.



- 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.

2.9 Развертывание агента для VMware (виртуальное устройство) из шаблона OVF

2.9.1 Перед началом

2.9.1.1 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 ТБ. Формат диска («толстый» или «тонкий») не влияет на производительность устройства.

2.9.1.2 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».

2.9.1.3 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**.

2.9.2 Развертывание шаблона OVF

2.9.2.1 Расположение шаблона OVF

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

В локальных развертываниях

После установки сервера управления пакет виртуального устройства OVF располагается в папке **%ProgramFiles%\Acronis\ESXAppliance** (в ОС Windows) or **/usr/lib/Acronis/ESXAppliance** (в ОС Linux).

2.9.2.2 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 в локальных развертываниях выберите сеть с сервером управления.

2.9.3 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.

   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** выполните действие:

      - Для локального развертывания выберите **Локальное**. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.

   c. В полях **Имя пользователя** и **Пароль** выполните действие:

      - Для локального развертывания 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**

   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.

2.9.4 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.

2.10 Развертывание 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.

2.10.1 Автоматическая установка 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 > Все устройства**
   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.

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

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**.

Выполненные действия должны привести к следующим результатам:

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

2.10.2 Установка oVirt вручную

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.
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.

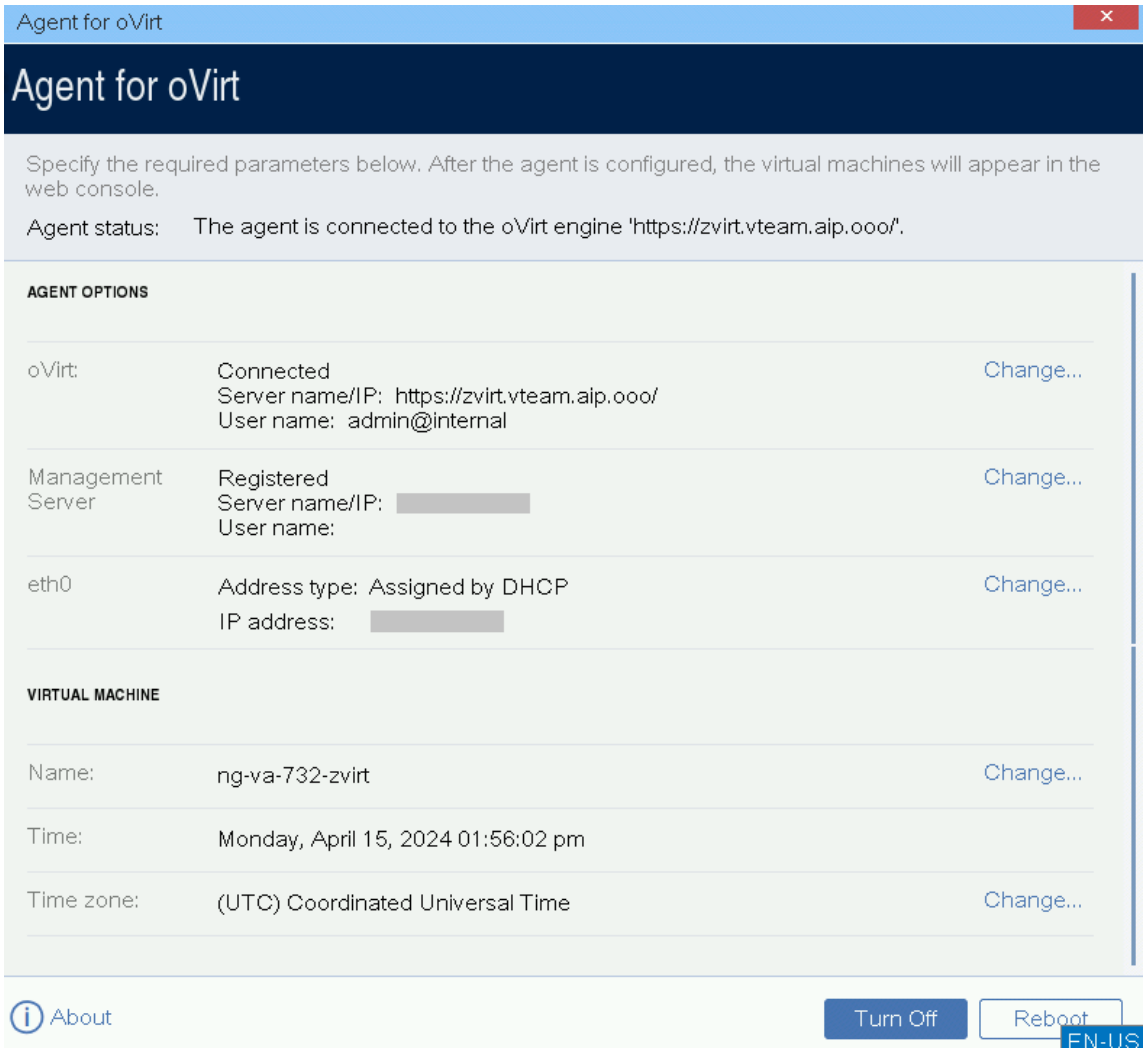
2.10.3 Настройка агента в ROSA Virtualization

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 значения параметров.
6. Нажмите кнопку **OK** чтобы сохранять изменения.
7. 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.
   - **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.
- **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 ROSA Virtualization (oVirt).
- В веб-консоли Кибер Бэкап в разделе Устройства появится подраздел oVirt.

2.11 Развертывание резервного копирования для Кибер Инфраструктуры

2.11.1 Общие сведения

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

- Решение Кибер Инфраструктура 4.7.
- Решение Кибер Бэкап.

Установка проводится в несколько этапов:

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

2.11.2 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.*

* См. также Известные проблемы версии 16.5.

2.11.3 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:

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
+--------------+-----------------+-------+-----------------+---------+--------+-----------+
| 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     |
+--------------+-----------------+-------+-----------------+---------+--------+-----------+
```

2.11.4 Установка виртуального устройства для Кибер Инфраструктуры

Установка виртуального устройства проводится в ручном режиме.

Чтобы установить виртуальное устройство, выполните действия:

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 **Вычисления** > **Виртуальные машины** > **Образы** и нажмите **Добавить образ**.
3. В поле **Файл образа** укажите путь к нужному образу виртуальной машины.
4. В поле **Имя** введите наименование виртуальной машины.
5. В поле **Выберите дистрибутив ОС** укажите нужный дистрибутив для виртуальной машины.
6. Перейдите на вкладку **Виртуальные машины** и выберите **Создать виртуальную машину**.
7. В поле **Образ** укажите нужный образ виртуальной машины.
8. Укажите параметры виртуальной машины на вкладке **Тип ВМ**. Для промышленных сборок рекомендуется указывать не менее 2-х ЦП и не менее 4 Гб памяти.
9. На вкладке **Сетевые интерфейсы** укажите подходящий сетевой интерфейс. Нажмите **Добавить** и выберите нужный сетевой интерфейс. Убедитесь, что сеть виртуального устройства имеет доступ к внутренним интерфейсам кластера (это можно сделать в меню **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 **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.

2.11.5 Подключение виртуального устройства к серверу управления

1. Перейдите **Вычисления** > **Виртуальные машины**.
2. В списке виртуальных машин выберите имя виртуальной машины и перейдите в **Консоль**.
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 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 **Cyber Infrastructure**.
9. Перейдите в **Настройки > Агенты** и убедитесь, что в списке агентов появился агент для резервного копирования Кибер Инфраструктуры.

2.12 Развертывание агента для SpaceVM

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

- Система SpaceVM версии 6.0.5 и выше.
- Решение Кибер Бэкап.

2.12.1 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.

2.12.2 Процедура развертывания

Выполняйте действия по развертыванию агента для SpaceVM в следующем порядке:

1. "Установка сервера управления" (стр. 58).
2. "Установка агента для SpaceVM" (стр. 122).
3. "Создание плана защиты" (стр. 157).

2.12.3 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.

2.12.4 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:
    a. Укажите адрес контроллера SpaceVM (например, https://space.my-company.ru), имя пользователя (например, admin) и пароль доступа к SpaceVM. 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.

2.13 Развертывание 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 от 4.7 до 5.1.
- Решение Кибер Бэкап.

2.13.1 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.

2.13.2 Процедура развертывания

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

1. "Установка сервера управления" (стр. 58).
2. "Установка агента для ECP VeiL" (стр. 125).
3. "Создание плана защиты" (стр. 157).

2.13.3 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».

2.13.4 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**.
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. 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.

2.14 Развертывание агента для OpenStack (РУСТЭК)

Для развертывания агента OpenStack вам понадобятся установленные и настроенные системы:

- Одна из следующих платформ виртуализации:
  - OpenStack выпусков от Ussuri до Zed,
  - РУСТЭК 2.6.
- Решение Кибер Бэкап 16.5 или новее.

Перед установкой агента на хост РУСТЭК, необходимо на данном хосте добавить политики для новой роли cyberbackup и создать пользователя с этой ролью. Подробнее см. в разделе "Подготовка хостов РУСТЭК к установке агента" (стр. 126).

Агент для OpenStack можно установить следующими путями:

- Добавить хост OpenStack или РУСТЭК на сервере управления в веб-интерфейсе Кибер Бэкап как описано в разделе "Добавление хостов OpenStack (РУСТЭК)" (стр. 76).
- Установить агент вручную в панели управления OpenStack (РУСТЭК) как описано далее.

2.14.1 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**.
- 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
```

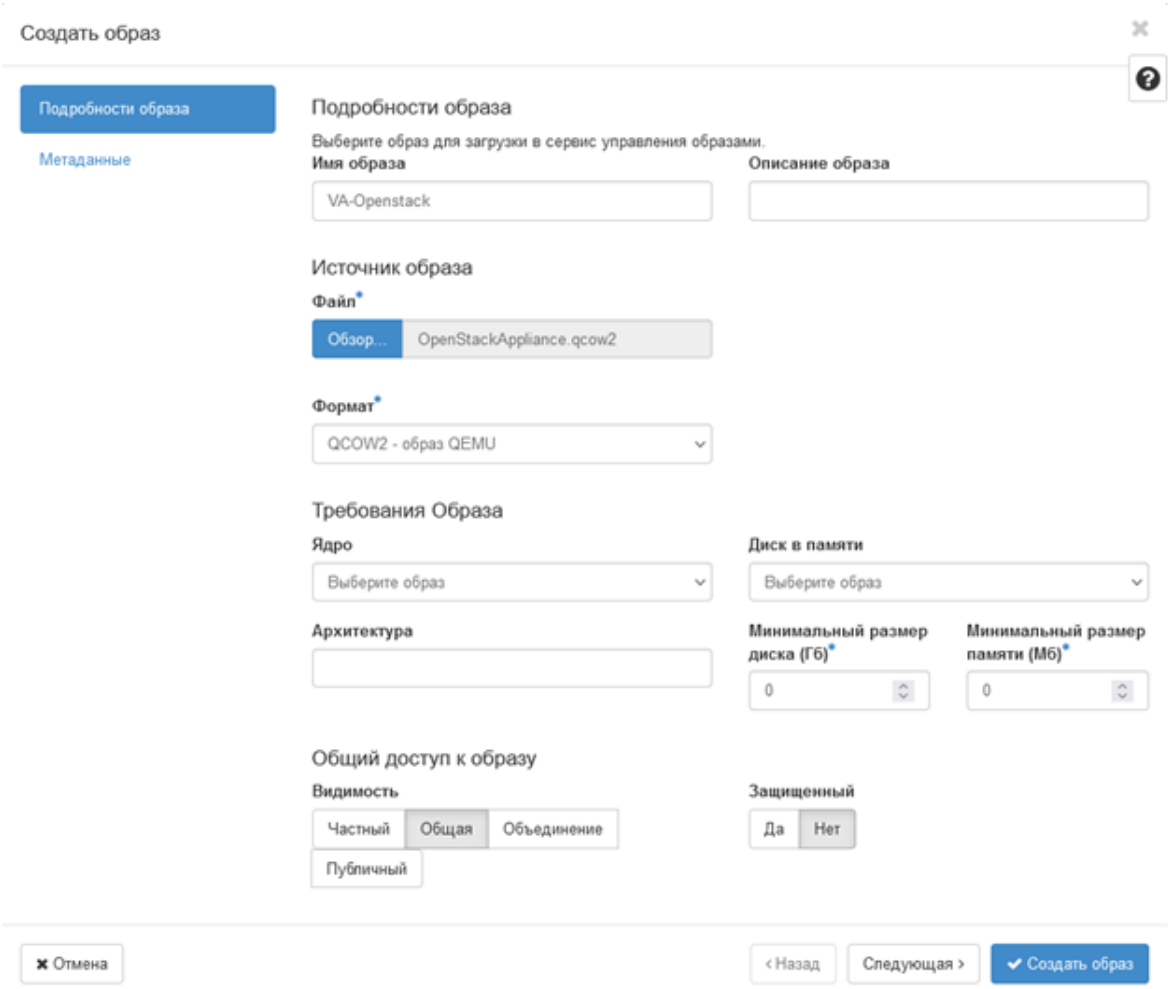
  где <passwd> – пароль для пользователя "cyberbackup".
- При необходимости откройте этому пользователю полный доступ через портал:

```
# 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
```

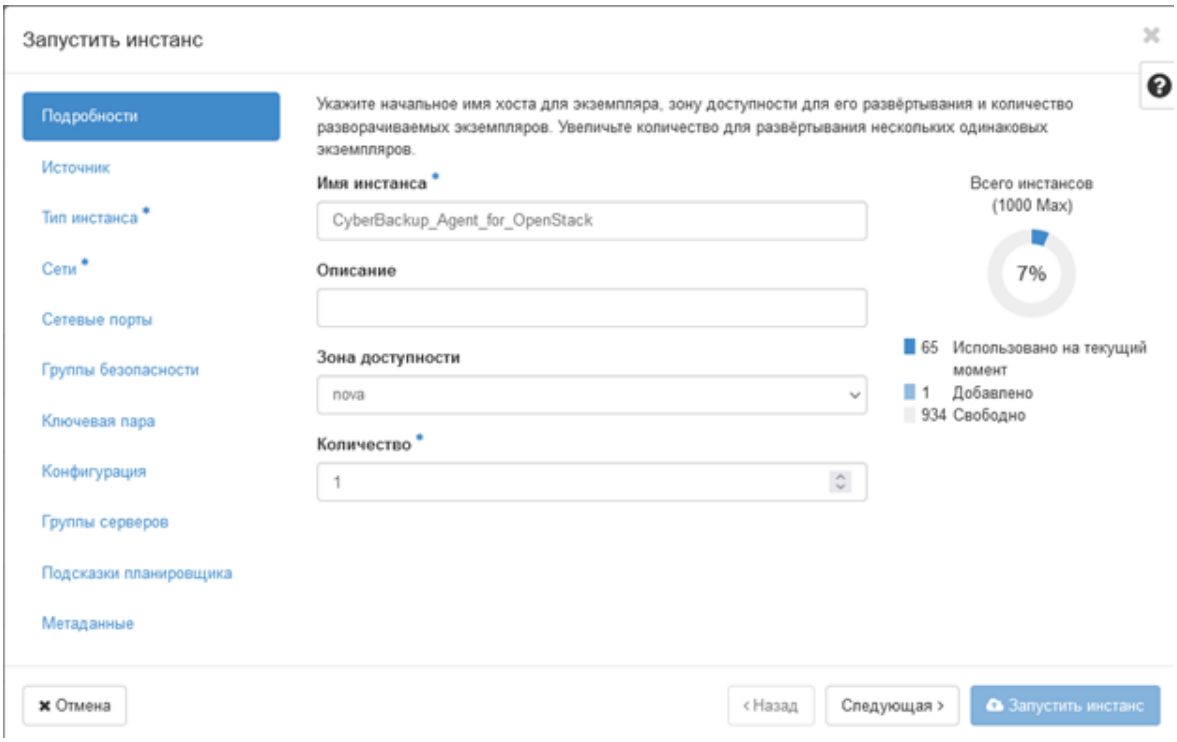
2.14.2 Установка агента для OpenStack (РУСТЭК) вручную

Чтобы установить агент OpenStack (РУСТЭК) вручную, выполните следующие шаги:

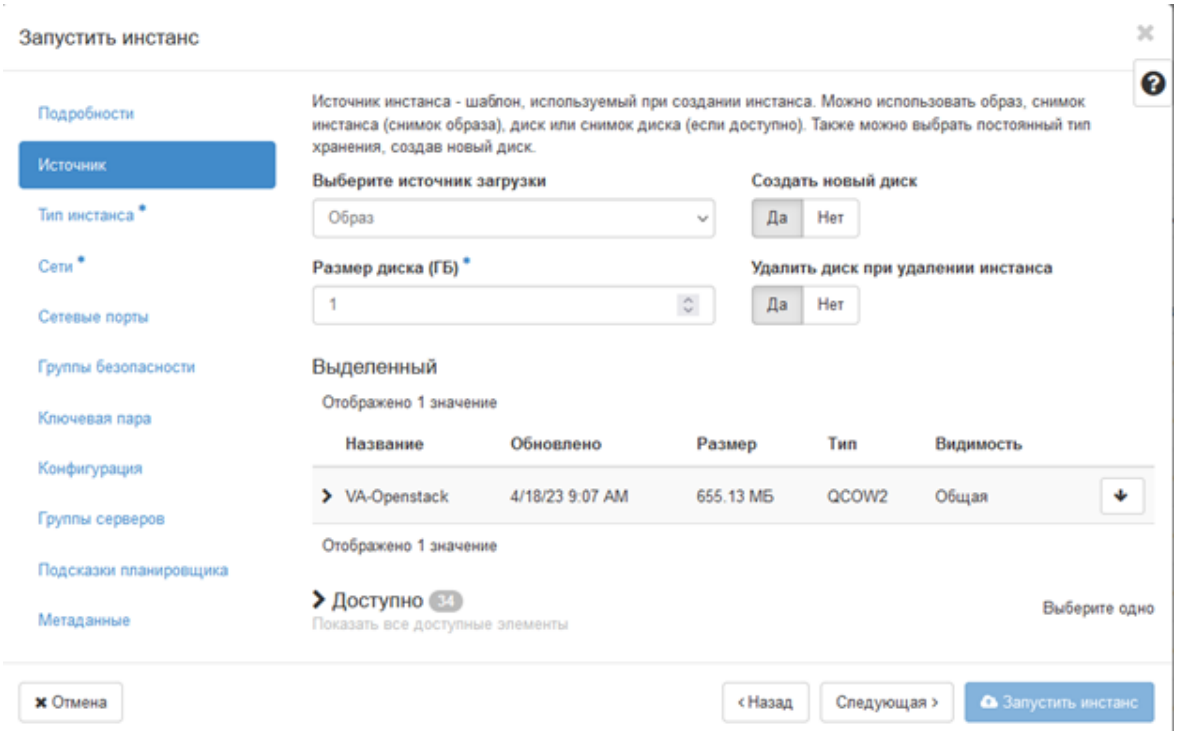
1. Загрузите **Пакет установки агента для OpenStack** с сайта Киберпротект.
2. Распакуйте образ виртуального устройства OpenStackAppliance.qcow2.
3. В панели управления OpenStack (РУСТЭК) перейдите на вкладку **Вычислительные ресурсы** > **Образы** и нажмите **Создать образ**.
4. В поле **Источник образа**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



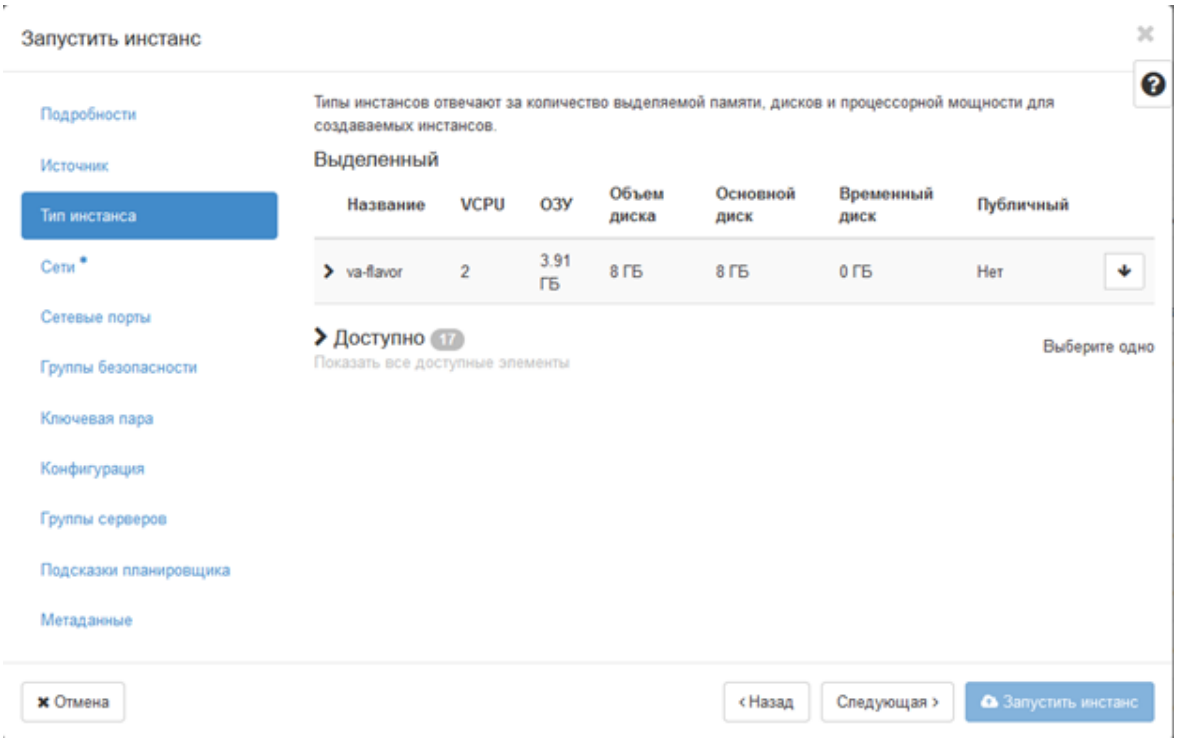
5. В поле **Формат** выберите **QCOW2 - образ QEMU**. По окончании ввода данных нажмите **Создать образ**.
6. Перейдите на вкладку **Вычислительные ресурсы** > **Инстансы** и выберите **Запустить инстанс**.



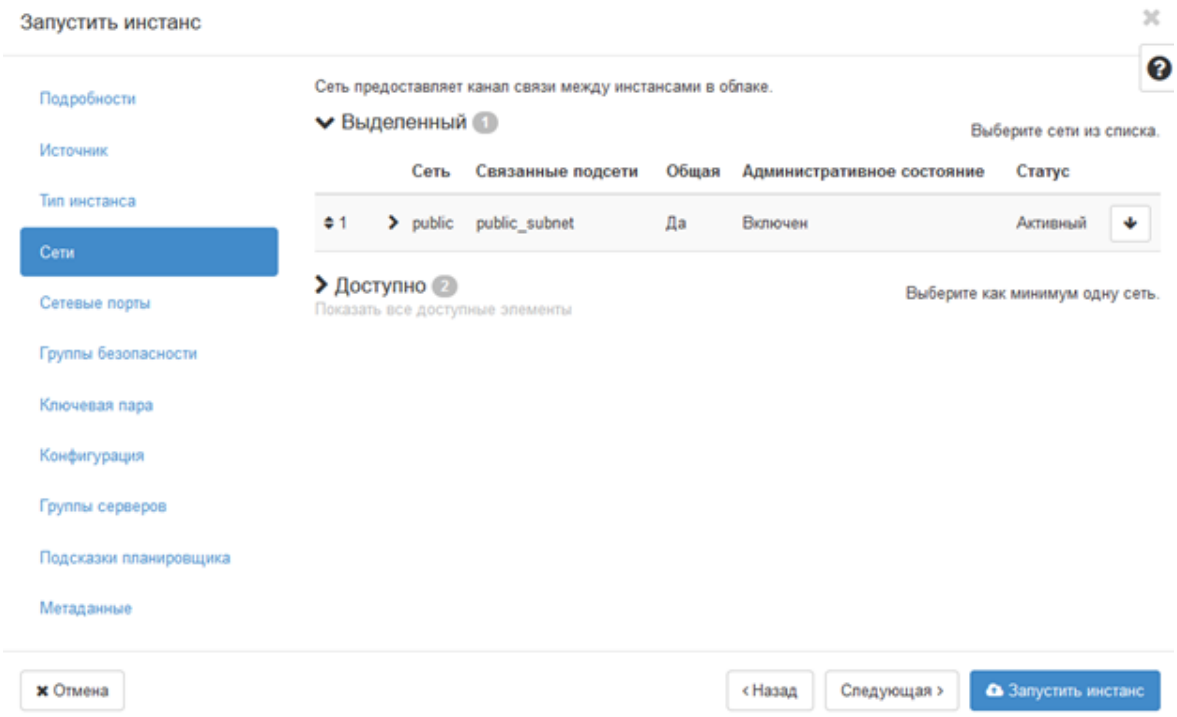
7. Укажите имя инстанса и зону доступности.
8. Выберите источник загрузки "Образ" и укажите образ виртуального устройства.



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



10. На вкладке **Сети** укажите подходящий сетевой интерфейс и группу безопасности. Группа должна разрешать подключения к указанному 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.

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

2.15 Развертывание резервного копирования для Базис.DynamiX

2.15.1 Общие сведения

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

2.15.2 Известные проблемы и ограничения

- Не поддерживается подключение более 9 дисков к ВМ Базис.Dynamix из-за ограничений платформы.
- Не поддерживается подключение более 8 сетевых адаптеров к ВМ Базис.Dynamix из-за ограничений платформы.
- При развертывании агента не отслеживается прогресс передачи диска.
- Нельзя выполнить клонирование включенной машины.
- 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.

См. также Проблемы, актуальные для Кибер Бэкап 17.

2.15.3 Установка Базис.DynamiX

Установка Базис.DynamiX включает в себя следующие шаги:

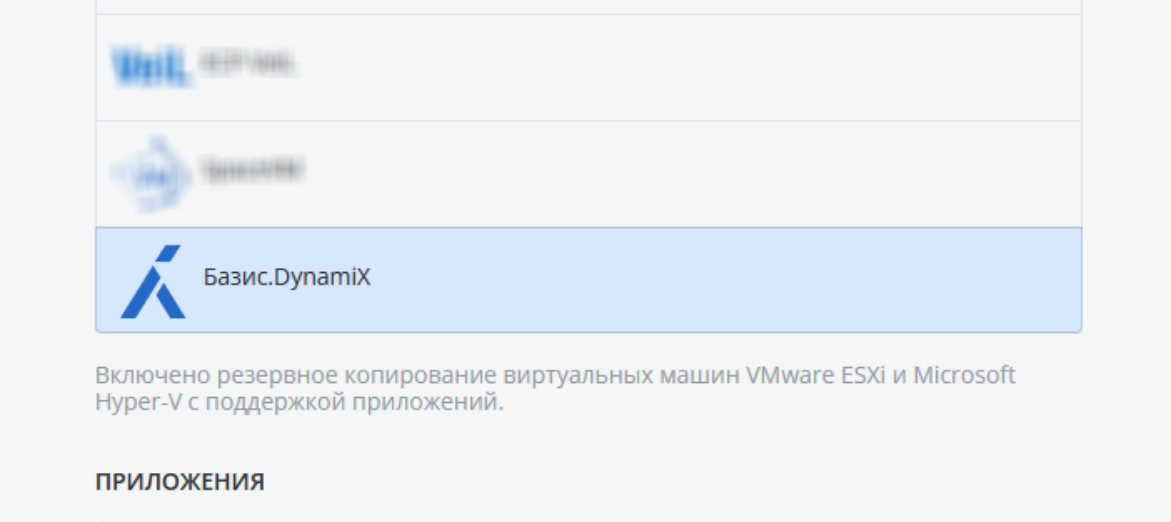
1. Установка сервера управления Кибер Бэкап.
2. Подключение виртуального устройства Базис.DynamiX к серверу управления Кибер Бэкап.

2.15.3.1 Установка сервера управления Кибер Бэкап

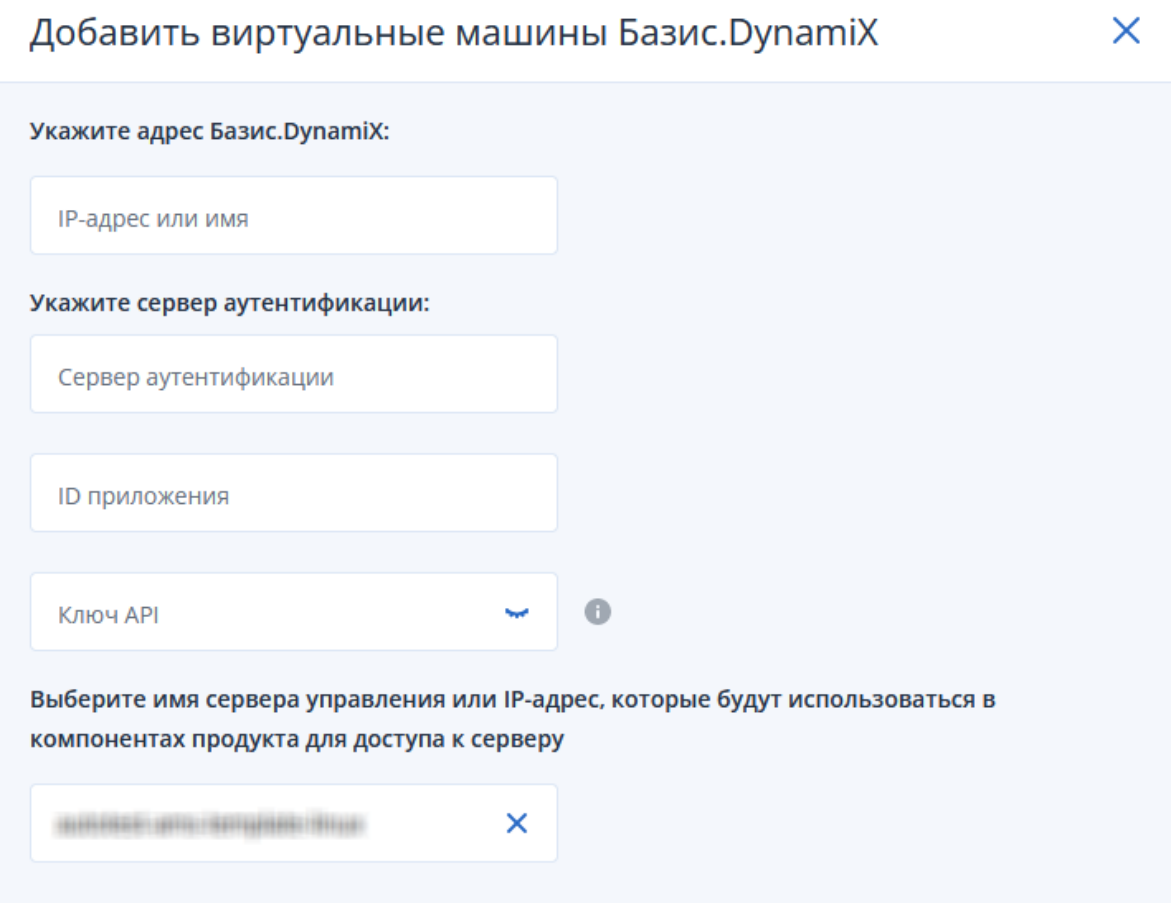
Для установки сервера управления Кибер Бэкап обратитесь к разделу "Установка сервера управления" (стр. 58).

2.15.3.2 Подключение виртуального устройства Базис.DynamiX к серверу управления Кибер Бэкап

1. В веб-консоли Кибер Бэкап перейдите: **Устройства** > **Все устройства**.
2. Справа вверху щелкните **Добавить** и выберите в списке Базис.DynamiX.



3. Укажите IP-адрес или имя для Базис.DynamiX, 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.

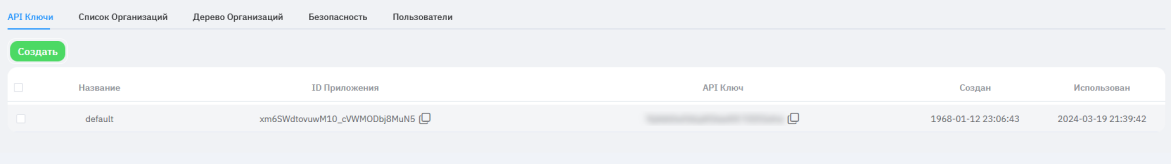
b. Авторизуйтесь под именем пользователя, от имени которого будут выполняться запросы к REST API платформы (посредством токена JWT).

> **Примечание**
> Пользователь должен иметь права **Admin** в учетной записи Базис.DynamiX.

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** > **Базис.Dynamix** 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 Базис.DynamiX.

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

2.16 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.

2.16.1 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.

2.16.2 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 на веб-консоль Кибер Бэкап с учетными данными той учетной записи, для которой необходимо назначить машины.
2. Щелкните **Все устройства** > **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.

2.16.3 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.

2.16.4 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.
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. В Windows Server 2008 R2:

- Разверните узел **Конфигурация программ**.

В Windows Server 2012 или более поздних версий:

- 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**.

2.17 Обновление виртуальных устройств

2.17.1 Локальные развертывания

Порядок обновления агента для VMware (виртуальное устройство) с версии более ранней, чем 15.24426 (выпущена в сентябре 2020 года), описан в разделе "Обновление агентов" (стр. 137).

Порядок обновления виртуального устройства версии 15.24426 или более поздней

1. Скачайте пакет обновления,
2. Сохраните файлы tar.bz в указанный ниже каталог на машине сервера управления:
   - Windows: C:\Program Files\Acronis\VirtualAppliances\va-updates
   - Linux: /usr/lib/Acronis/VirtualAppliances/va-updates
3. На веб-консоли Кибер Бэкап последовательно выберите пункты **Настройки** > **Агенты**.
   В программе будет выведен список машин. Машины с устаревшими виртуальными устройствами будут помечены оранжевым восклицательным знаком.
4. Выберите машины, на которых нужно обновить виртуальные устройства. Эти машины должны быть включены.
5. Щелкните **Обновить агент**.
6. Выберите агент развертывания.
7. Укажите учетные данные учетной записи с правами администратора на целевой машине.
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-сервер не может преобразовать имя хоста в IP-адрес, что приводит к ошибке при регистрации виртуального устройства.

Ход выполнения обновления показан на вкладке **Действия**.

Примечание
При выполнении обновления все выполняющиеся резервные копии завершатся сбоем.

2.18 Обновление агентов

2.18.0.1 Предварительные требования

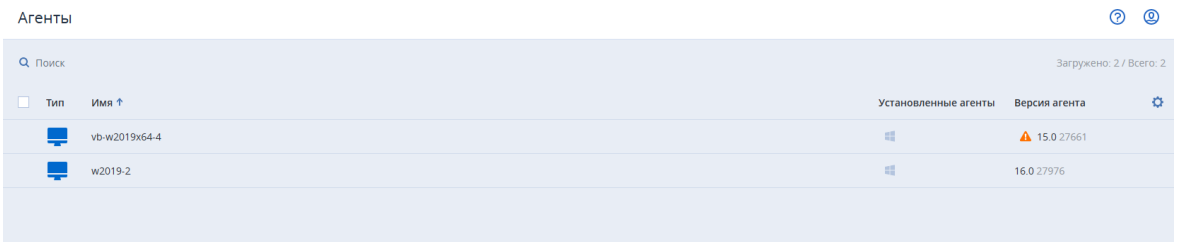
Для работы функций Кибер Бэкап на машинах Windows требуется распространяемый компонент Microsoft Visual C++ 2017. Проверьте наличие этого компонента на машине или установите его перед обновлением агента. После установки может потребоваться перезагрузка. Распространяемый пакет Microsoft Visual C++ можно скачать по ссылке https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Чтобы найти версию агента, выберите машину и нажмите кнопку **Сведения**.

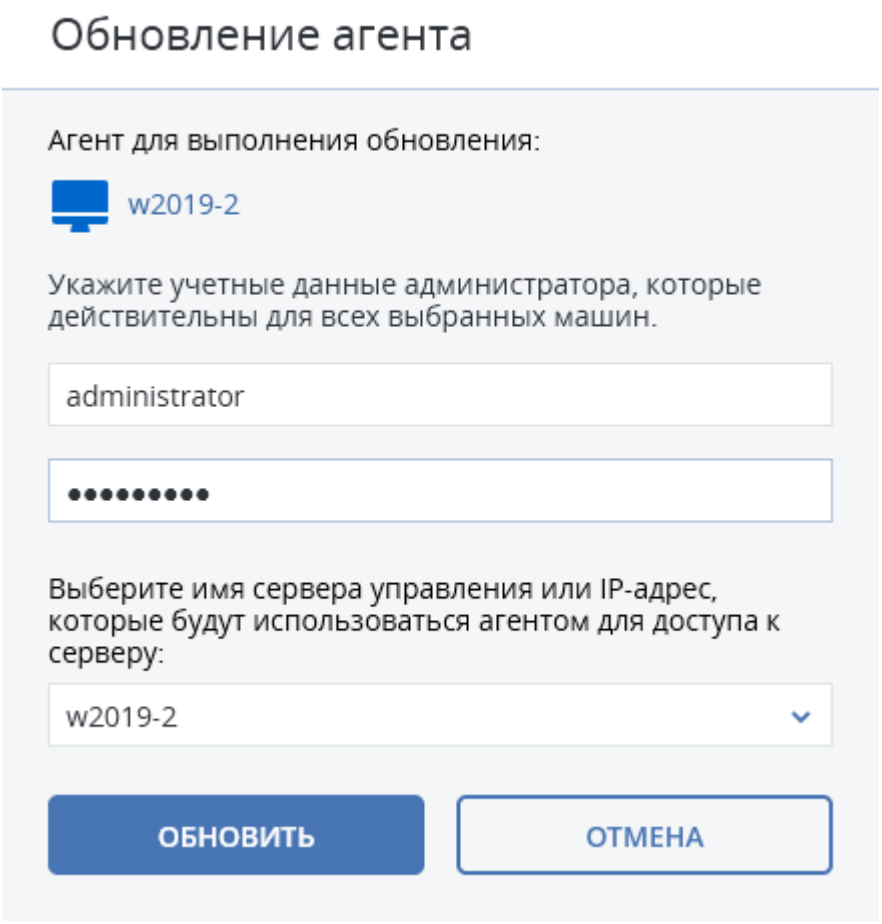
Можно обновить агенты, используя веб-консоль Кибер Бэкап или повторив их установку любым доступным способом. Чтобы одновременно обновить несколько агентов, используйте указанную ниже процедуру.

Порядок обновления агентов с веб-консоли Кибер Бэкап

1. [Только в локальных развертываниях] Обновите сервер управления и узел хранения. Подробнее об этом см. Модернизация с предыдущих версий продукта.
2. [Только в локальных развертываниях] Убедитесь, что на машине с сервером управления есть пакеты установки. Чтобы узнать о конкретных действиях, выберите «Добавление машины с ОС Windows» > «Пакеты установки».
3. На 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**.



6. Выберите агент развертывания.
7. Укажите учетные данные учетной записи с правами администратора на целевой машине.
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**.

Примечание
При выполнении обновления все выполняющиеся резервные копии завершатся сбоем.

2.19 Модернизация с предыдущих версий продукта

Можно выполнить модернизацию до последней версии непосредственно на машине с более ранней версией Кибер Бэкап или с предварительным удалением предыдущей версии продукта.

Непосредственная модернизация доступна, только начиная с Кибер Бэкап 12.5 с обновлением 5 (сборка 16225 и более поздней версии). Продукты более ранних версий невозможно модернизировать напрямую.

Внимание
Перед выполнением модернизации настоятельно рекомендуем создать резервную копию системы. Это позволит выполнить возврат к оригинальной конфигурации в случае сбоя модернизации.

Порядок обновления с предыдущей версии Кибер Бэкап

1. Обновление сервера управления (AMS) и узла хранения (ASN).
2. Обновление агента 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 или через веб-консоль. Для обновления агента посредством установщика см. следующий пункт ("Обновление с предыдущей версии Кибер Бэкап"). Для обновления агента посредством веб-консоли обратитесь к разделу "Обновление агентов" (стр. 137).

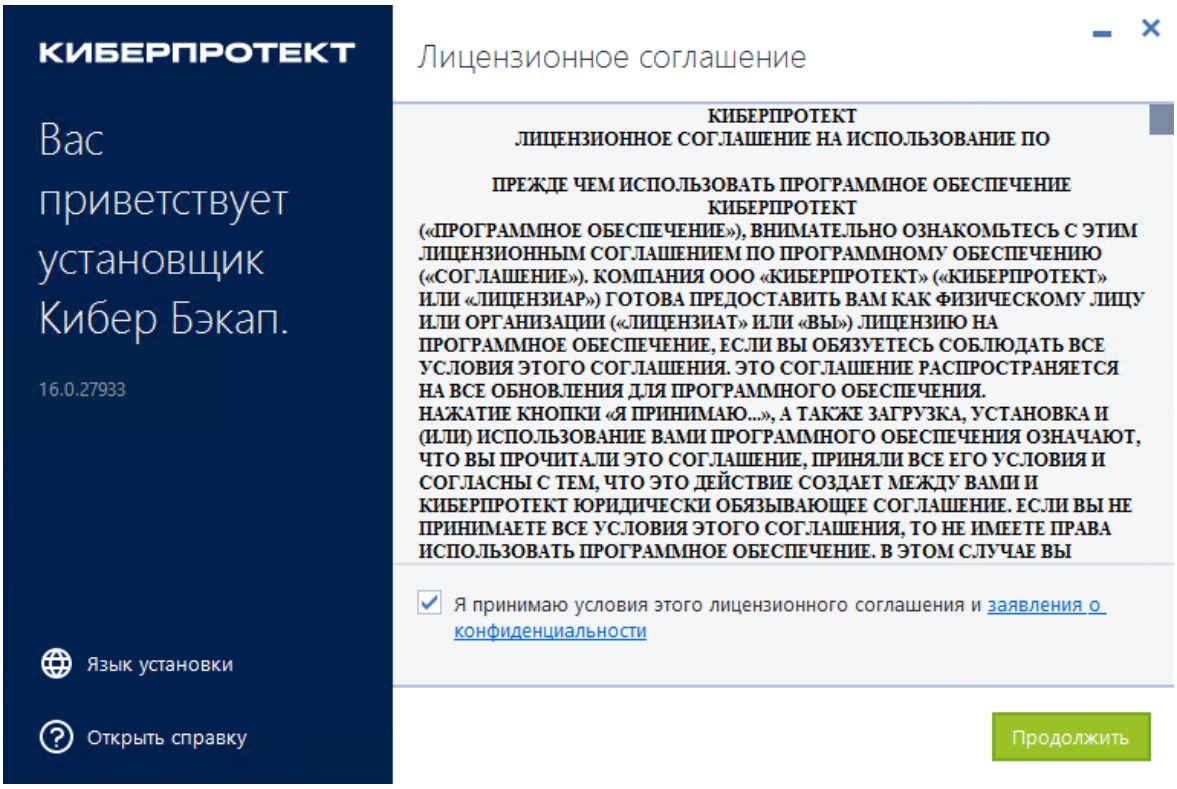
Внимание
Обновляйте агента Кибер Бэкап только после того, как обновили сервер управления и узел хранения.

Сервер управления в Кибер Бэкап 16.5 обратно совместим с агентами версий 12.5 и 15 и поддерживает их. Однако эти агенты не поддерживают функции Кибер Бэкап 16.5.

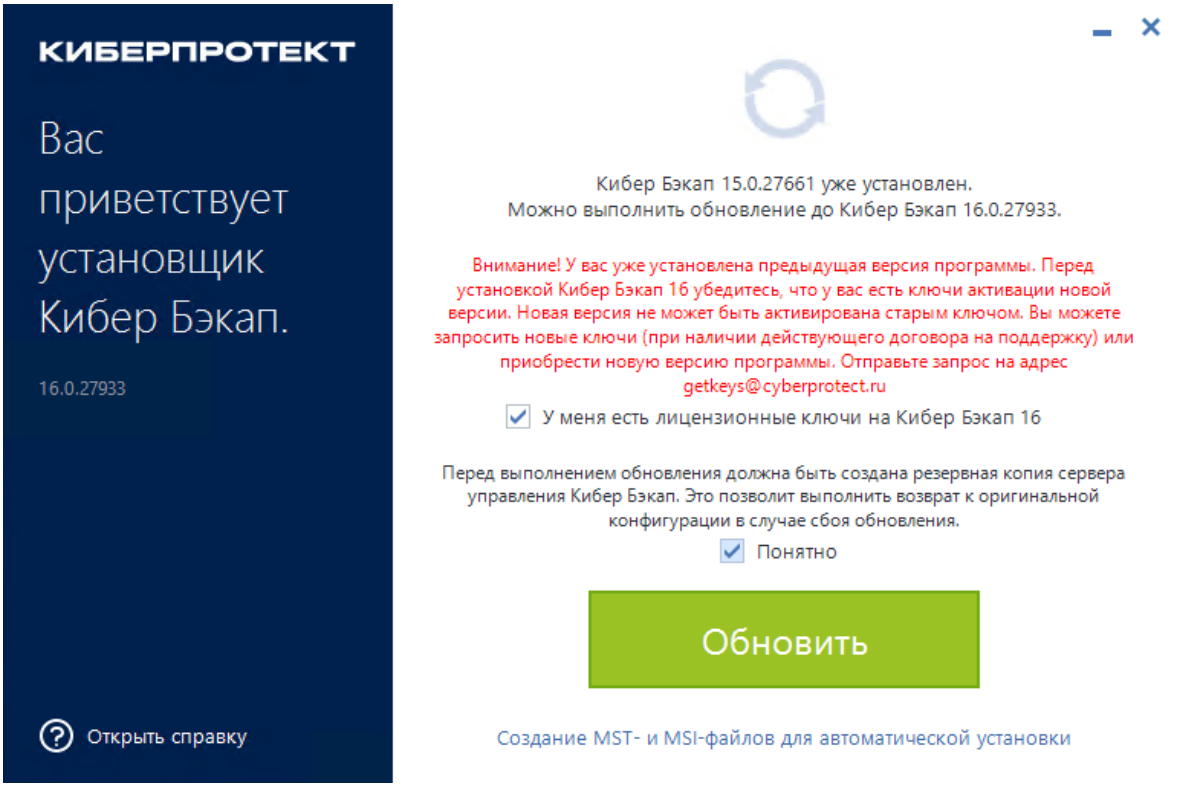
Модернизация агентов не влияет на существующие резервные копии и их настройки.

Обновление с предыдущей версии Кибер Бэкап

1. Запустите установщик на машине с сервером управления или узлом хранения. Для продолжения установки вам потребуется принять лицензионное соглашение.



2. При необходимости можно изменить язык отображения сообщений во время обновления, нажав **Язык установки**. После выбора языка установки нажмите **Продолжить**.
3. Для продолжения установки обновления подтвердите наличие у вас лицензии на новую версию Кибер Бэкап.



Для продолжения подтвердите также, что прочитали рекомендацию о создании резервной копии сервера управления. После этого нажмите **Обновить**. Установленная на вашем компьютере версия Кибер Бэкап будет обновлена.

2.20 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
В локальных развертываниях 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.

2.20.1 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.

2.20.2 В ОС Linux

1. В качестве привилегированного пользователя выполните **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Необязательно] Установите флажок **Удалить все элементы трассировки продукта (журналы, задания, хранилища, параметры конфигурации продукта)**.

   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.

2.20.3 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.

2.20.4 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**.

2.21 Установка агентов

2.21.1 В Windows

1. Убедитесь в том, что машина подключена к Интернету.
2. Войдите как администратор и запустите программу установки.

3. [Необязательно] Щелкните **Настройка параметров установки** и внесите нужные изменения (при необходимости):
   - Изменение устанавливаемых компонентов (например, отмена установки программы командной строки).
   - Изменение метода регистрации машины в службе Кибер Бэкап. Можно изменить параметр **Использовать консоль Кибер Бэкап** (по умолчанию) на **Использовать учетные данные** или **Использовать маркер регистрации**.
   - Изменение пути установки.
   - Изменение учетной записи для службы агента.
   - Проверка или изменение имени хоста или IP-адреса, порта и учетных данных прокси-сервера. Если прокси-сервер включен в Windows, он определяется и используется автоматически.
4. Нажмите **Установить**.
5. [Только при установке агента для VMware] Укажите адрес и учетные данные доступа для сервера vCenter Server или автономного хоста ESXi, для которых агент будет создавать резервные копии виртуальных машин, и нажмите кнопку **Готово**. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями на хосте vCenter Server или ESXi.
6. [Только при установке на контроллер домена] Укажите учетную запись пользователя, под которой будет работать служба агента, и нажмите кнопку **Готово**. В целях безопасности программа установки не может автоматически создавать учетные записи на контроллере домена.
7. Если на шаге 3 вы не меняли способ регистрации по умолчанию (**Использовать консоль Кибер Бэкап**), дождитесь появления экрана регистрации и перейдите к следующему шагу. Если нет, дополнительных действий не требуется.
8. Выполните одно из следующих действий:
   - Щелкните **Зарегистрировать машину**. В открывшемся окне браузера войдите на веб-консоль Кибер Бэкап, проверьте регистрационные данные и щелкните **Подтвердить регистрацию**.
   - Щелкните **Показать регистрационные сведения**. В программе установки будет показана ссылка на регистрацию и код регистрации. Можно скопировать их и пройти все необходимые этапы регистрации на другой машине. В этом случае необходимо будет ввести код регистрации в форме регистрации. Код регистрации действует только один час.

     В качестве альтернативного варианта доступ к форме регистрации можно получить следующим образом: выберите **Все устройства** > **Добавить**, прокрутите вниз до поля **Регистрация по коду** и нажмите кнопку **Регистрация**.

9. **Примечание**
   Не выходите из программы установки до подтверждения регистрации. Чтобы начать регистрацию заново, необходимо перезапустить программу установки и щелкнуть **Зарегистрировать машину**.

   Это приведет к тому, что машина будет назначена учетной записи, которая была использована для входа на веб-консоль Кибер Бэкап.

2.21.2 В ОС Linux

1. Убедитесь в том, что машина подключена к Интернету.
2. Запустите файл установки от имени суперпользователя.
   Если в сети включен прокси-сервер, при запуске файла укажите имя хоста или IP-адрес и порт сервера в следующем формате: --http-proxy-host=АДРЕС --http-proxy-port=ПОРТ --http-proxy-login=ИМЯ ВХОДА--http-proxy-password=ПАРОЛЬ.
   Чтобы изменить метод регистрации машины в службе Кибер Бэкап, используемый по умолчанию, запустите установочный файл с одним из следующих параметров:
   - --register-with-credentials: запрашивать имя пользователя и пароль при установке;
   - --token=STRING: использовать маркер регистрации;
   - --skip-registration: пропустить регистрацию.
3. Установите флажки для агентов, которые необходимо установить. Доступны следующие агенты:
   - **Агент для Linux**
   - **Агент для Virtuozzo**
   - **Агент для Oracle**
   - **Агент для MySQL/MariaDB**

   Агент для Virtuozzo, Агент для Oracle, Агент для MySQL/MariaDB невозможно установить без агента для Linux.
4. Если вы оставили метод регистрации по умолчанию в шаге 2, перейдите к следующему шагу. В противном случае введите имя пользователя и пароль для службы Кибер Бэкап или дождитесь регистрации машины с использованием маркера.
5. Выполните одно из следующих действий:
   - Щелкните **Зарегистрировать машину**. В открывшемся окне браузера войдите на веб-консоль Кибер Бэкап, проверьте регистрационные данные и щелкните **Подтвердить регистрацию**.
   - Щелкните **Показать регистрационные сведения**. В программе установки будет показана ссылка на регистрацию и код регистрации. Можно скопировать их и пройти все необходимые этапы регистрации на другой машине. В этом случае необходимо будет ввести код регистрации в форме регистрации. Код регистрации действует только один час.

В качестве альтернативного варианта доступ к форме регистрации можно получить следующим образом: выберите **Все устройства** > **Добавить**, прокрутите вниз до поля **Регистрация по коду** и нажмите кнопку **Регистрация**.

6. **Примечание**
   Не выходите из программы установки до подтверждения регистрации. Чтобы начать регистрацию заново, необходимо будет перезапустить программу установки и повторить процедуру установки.

   Это приведет к тому, что машина будет назначена учетной записи, которая была использована для входа на веб-консоль Кибер Бэкап.
7. 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
   Во время установки создается новый ключ для подписания модуля snapapi. Этот ключ регистрируется как ключ владельца машины (Machine Owner Key, MOK). Для регистрации этого ключа необходимо перезапустить систему. Если не зарегистрировать ключ, агент не будет работать. Если безопасная загрузка UEFI включена после установки агента, повторите установку, включая шаг 6.

8. 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.**

3 Доступ к веб-консоли 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.

3.1 Локальное развертывание

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.

3.1.1 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. 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 находится в списке администраторов сервера управления. По умолчанию этот список содержит группу **Администраторы** на машине, где работает сервер управления. Дополнительные сведения см. в разделе «Администраторы и отделы».

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.

2. Откройте файл **account_server.json** для редактирования.
3. Перейдите к разделу "connectiors" и удалите следующие строки:

```
{
"type": "sspi",
"name": "1 Windows Integrated Logon",
"id": "sspi",
"config": {}
},
```

4. Перейдите к разделу "checksum" и измените значение "sum" следующим образом:

```
"sum": "FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. Перезапустите службу Киберпротект Service Manager Service, как описано в разделе Использование сертификата, выданного доверенным центром сертификации.

3.1.2 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 «Администраторы и отделы».

3.2 Смена языка

После входа в систему можно изменить язык веб-интерфейса, щелкнув значок учетной записи в правом верхнем углу.

3.3 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.

3.3.1 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**.

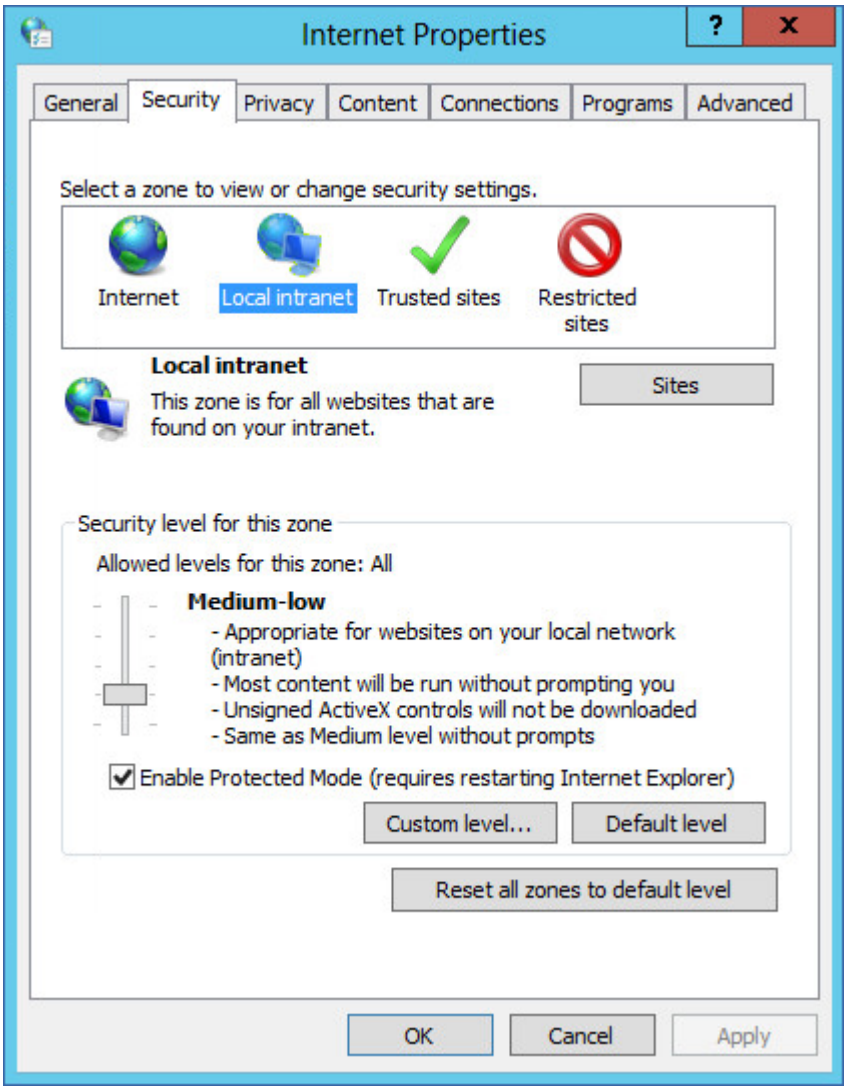
См. пошаговые инструкции далее в этом разделе. Поскольку эти браузеры используют параметры Windows, возможна их настройка с помощью групповой политики в домене Active Directory.

3.3.2 Настройка Mozilla Firefox

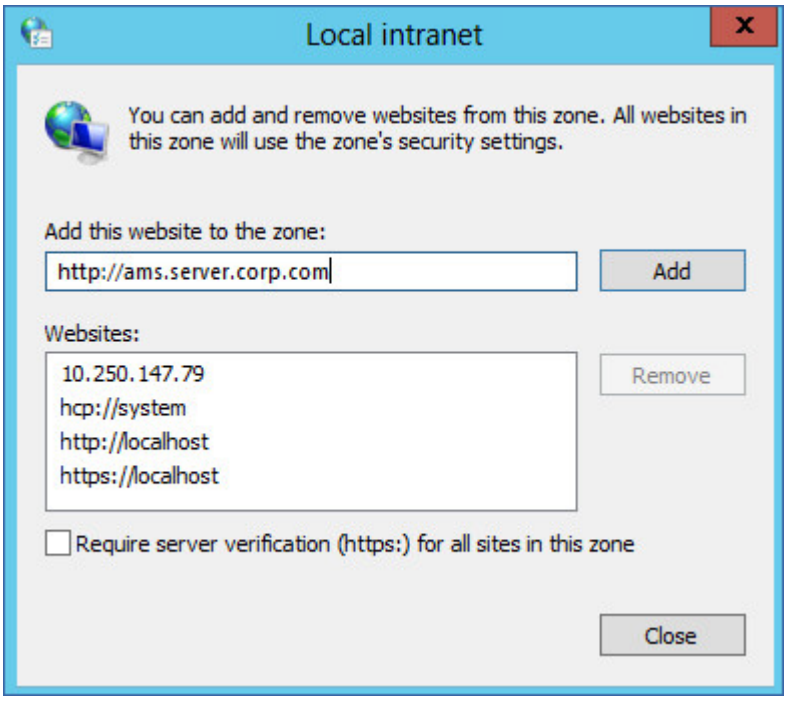
1. В Firefox перейдите на URL-адрес about:config, а затем нажмите кнопку **Я принимаю возможные риски**.
2. В поле Поиск выполните поиск настройки **network.negotiate-auth.trusted-uris**.
3. Дважды щелкните настройку, а затем введите адрес страницы входа в веб-консоль Кибер Бэкап в одном из форматов, указанных в разделе "Доступ к веб-консоли Кибер Бэкап" (стр. 146). 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.

3.3.3 Добавление консоли к списку веб-узлов локальной интрасети

1. Выберите **Панель управления** > **Настройки Интернета**.
2. Во вкладке **Безопасность** выберите **Локальная интрасеть**.



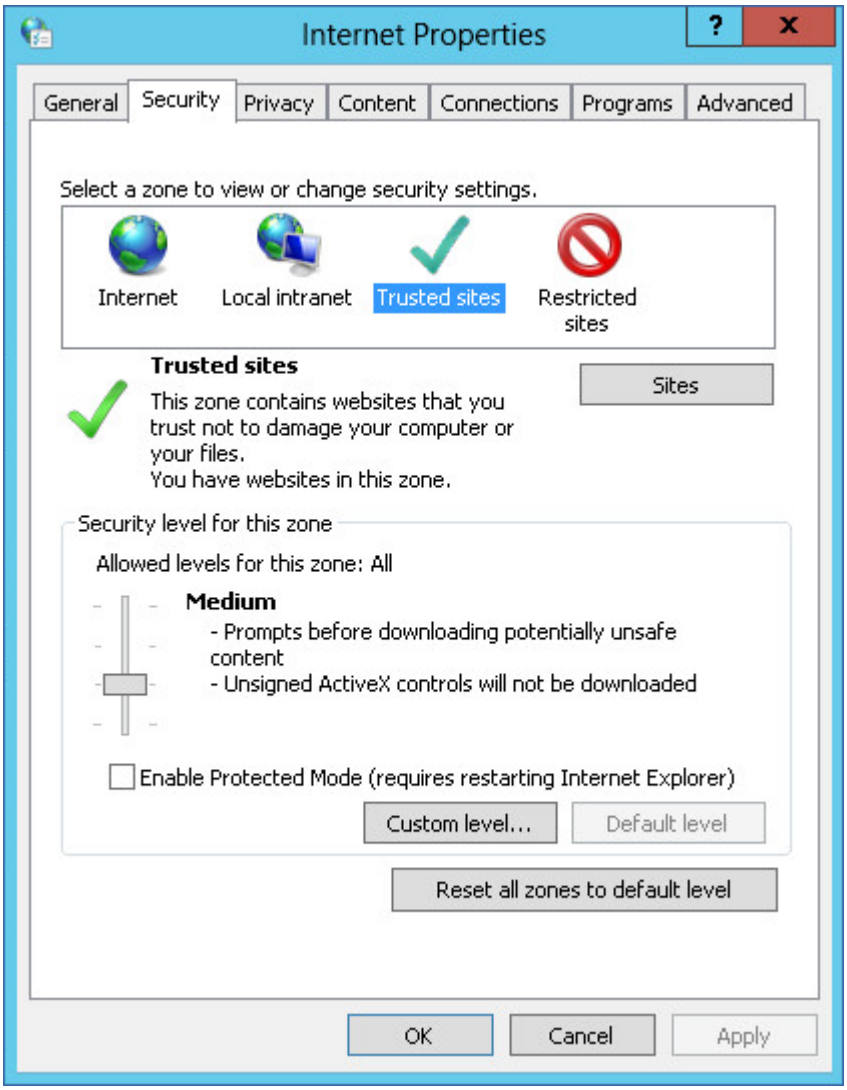
3. Нажмите кнопку **Веб-узлы**.
4. В поле **Добавить этот веб-сайт в зону** введите адрес страницы входа на веб-консоль Кибер Бэкап, а затем щелкните **Добавить**.



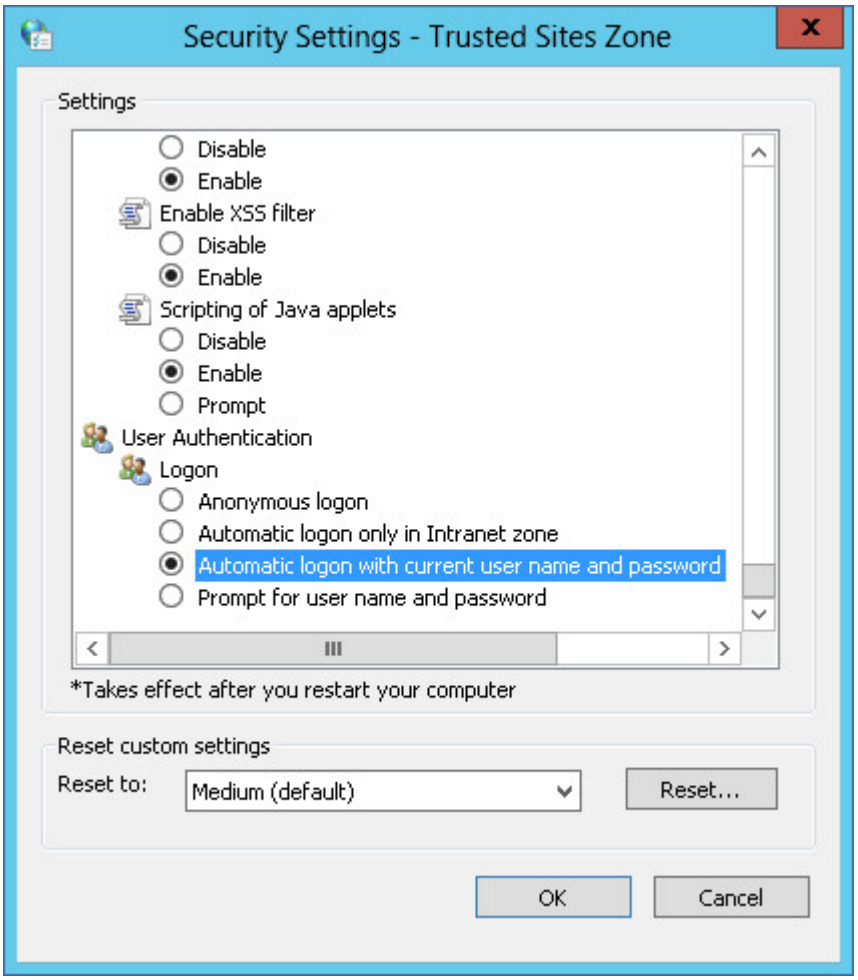
5. Нажмите кнопку **Закрыть**.
6. Нажмите кнопку **OK**.

3.3.4 Добавление консоли к списку доверенных веб-узлов

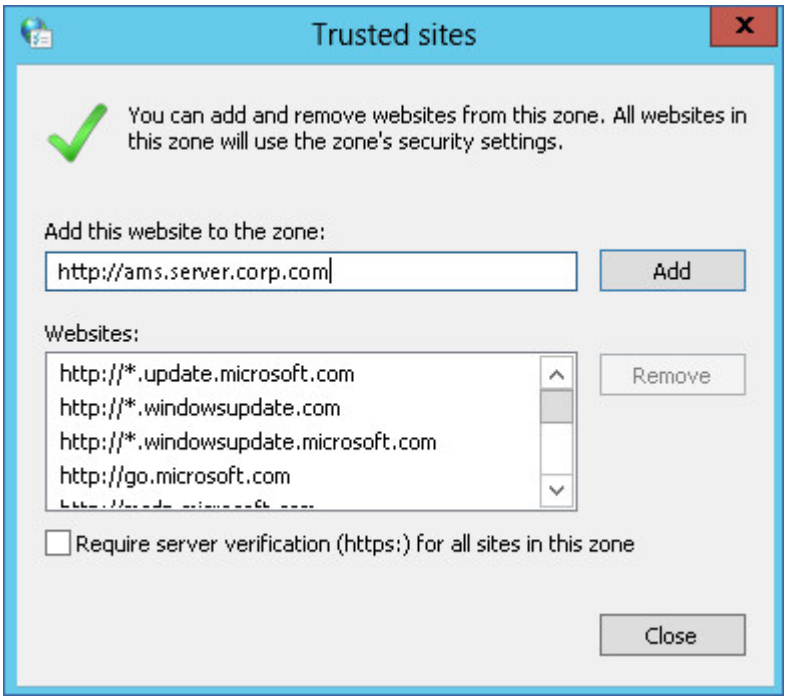
1. Выберите **Панель управления** > **Настройки Интернета**.
2. Во вкладке **Безопасность** выберите **Доверенные веб-узлы**, а затем нажмите **Пользовательский уровень**.



3. В группе **Учетные данные** выберите **Автоматический вход в систему с текущим именем пользователя и паролем**, а затем нажмите кнопку **OK**.



4. Во вкладке **Безопасность**, при выбранных **Доверенных веб-узлах**, нажмите **Веб-узлы**.
5. В поле **Добавить этот веб-сайт в зону** введите адрес страницы входа на веб-консоль Кибер Бэкап, а затем щелкните **Добавить**.



6. Нажмите кнопку **Закрыть**.
7. Нажмите кнопку **OK**.

3.4 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, таким как GoDaddy, Comodo или 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.

3.4.1 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**.

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
```

3.4.2 Использование сертификата, выданный 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)
   - 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
```

Порядок перезапуска службы Киберпротект Service Manager в Linux

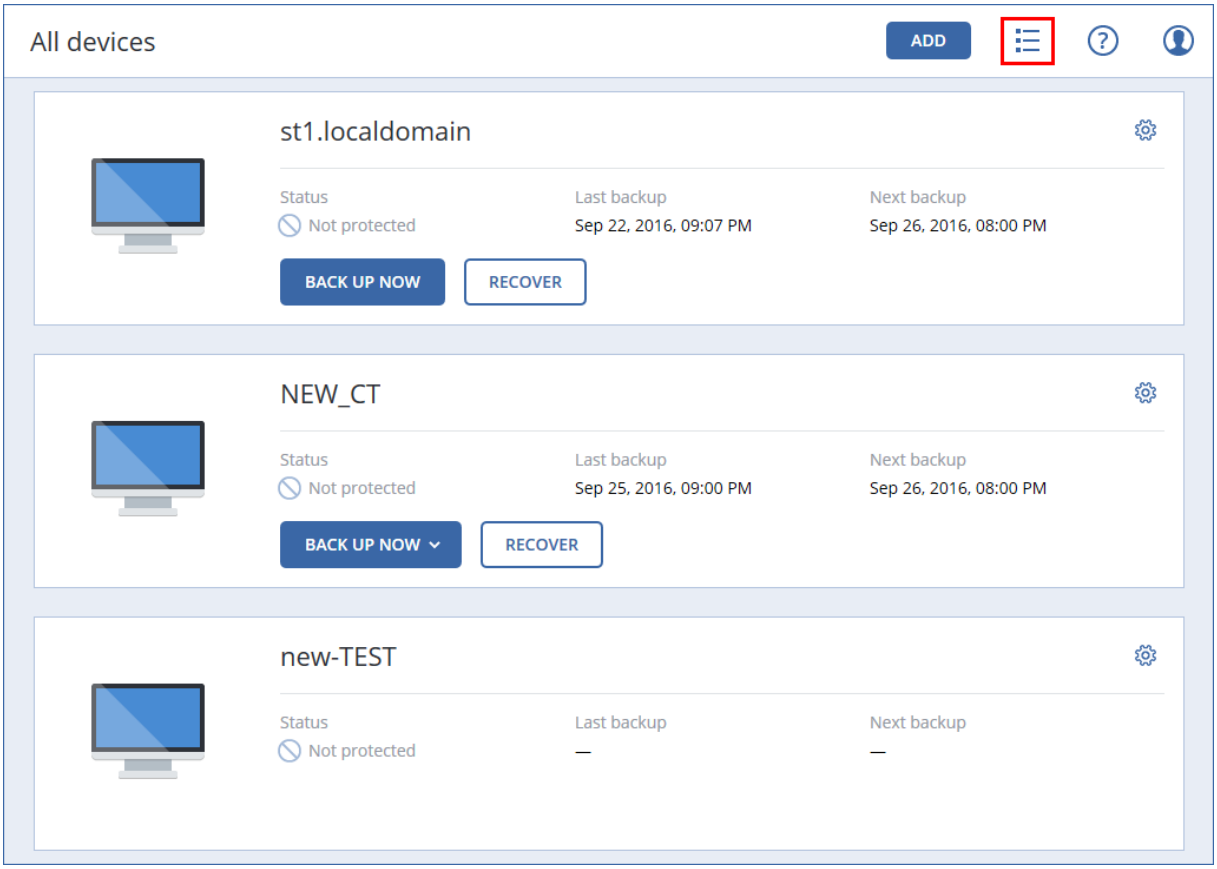
1. Откройте **приложение терминала**.
2. Выполните следующую команду в любом каталоге:

```
sudo service acronis_asm restart
```

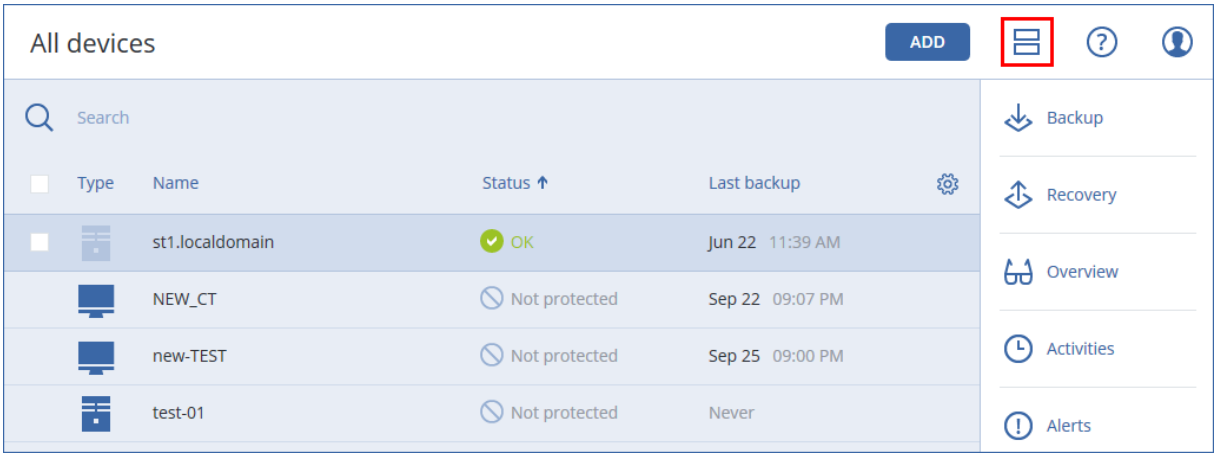
4 Представление веб-консоли Кибер Бэкап

Веб-консоль Кибер Бэкап имеет два представления – простое и табличное. Для переключения между ними используется значок в правом верхнем углу.

В этом небольшом представлении поддерживается небольшое количество машин.



Табличное представление включается автоматически, когда появляются машины в большом количестве.



В обоих представлениях доступен один и тот же набор функций и операций. В этом документе описан порядок вызова различных команд из табличного представления.

5 План защиты и модули

План защиты – это план, объединяющий в себе несколько модулей защиты данных, включая указанные ниже:

- "Резервное копирование" (стр. 168) – позволяет создавать резервную копию источников данных в локальном хранилище данных.
- Active Protection – позволяет выполнять проверку компьютеров встроенным средством защиты от вредоносных программ.
- "Оценка уязвимостей" (стр. 491) – проверяет установленные на ваших компьютерах продукты Microsoft и сторонних производителей на наличие уязвимостей и уведомляет вас о них.

Создавая гибкие планы для разных потребностей бизнеса, различные модули можно включить и отключить, задать их настройки.

5.1 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 применен.

Рассмотрим первый способ.

Порядок создания плана защиты

1. На веб-консоли Кибер Бэкап выберите пункты **Устройства** > **Все устройства**.
2. Выберите машины, для которых нужно обеспечить защиту.
3. Щелкните **Защитить**, а затем **Создать план**. Откроется план защиты с настройками по умолчанию.
4. [Необязательно] Для изменения имени плана защиты щелкните значок карандаша рядом с именем.
5. [Необязательно] Для включения или отключения модуля плана защиты щелкните переключатель рядом с именем модуля.
6. [Необязательно] Для настройки параметров модуля щелкните соответствующий раздел плана защиты.
7. После этого щелкните **Создать**.

Модуль Резервное копирование можно выполнить по требованию. Для этого щелкните **Запустить сейчас**.

Для настройки модуля Active Protection см. "Настройка модуля Active Protection" (стр. 487).

Для настройки модуля Оценка уязвимостей см. "Настройка модуля Оценка уязвимостей" (стр. 493)

5.2 Разрешение конфликтов плана

План защиты может иметь одно из указанных ниже состояний.

- **Активный**: план, который назначен устройствам и выполнен на них.
- **Неактивный**: план, который назначен устройствам, но отключен и не выполнен на них.

5.2.1 Применение нескольких планов к устройству

К одному устройству можно применить несколько планов защиты. В результате получится комбинация разных планов защиты, назначенных одному устройству. Планы защиты можно объединить, только если у них нет общих модулей. Если есть модули, которые одновременно включены в нескольких планах резервного копирования, необходимо будет разрешить конфликты между ними.

5.2.2 Разрешение конфликтов плана

5.2.2.1 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.

- Создайте новый план, примените его и отключите все примененные конфликтующие планы.
- Создайте новый план и отключите его.

При редактировании нового плана на устройстве или устройствах с уже примененными планами, которые конфликтуют с внесенными изменениями, можно разрешить конфликт одним из указанных ниже способов.

- Сохраните изменения в план и отключите все уже примененные конфликтующие планы.
- Сохраните изменения, внесенные в план, и отключите его.

5.2.2.2 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.

5.2.2.3 Проблемы с лицензией

Назначенная квота на устройстве должна обеспечивать выполнение, обновление и применение плана защиты. Чтобы разрешить проблему с лицензией, выполните одно из указанных ниже действий:

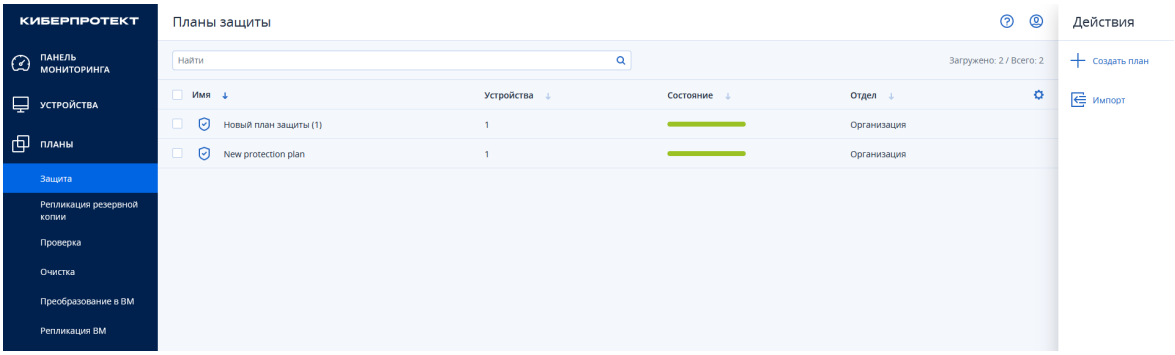
- Отключите модули, которые не поддерживаются назначенной квотой, и продолжите использовать план защиты.
- Измените назначенную квоту вручную: откройте раздел **Устройства**> **<конкретное устройство>** > **Подробнее** > **Квота службы**. После этого отзовите существующую квоту и назначьте новую.

5.3 Операции с планами защиты

5.3.1 Доступные действия с планами защиты

Действия с планами доступны на вкладке **Планы** основного меню веб-консоли. Для просмотра возможных действий с планами выполните следующее:

1. Откройте веб-консоль.
2. Перейдите на вкладку **Планы** для просмотра списка планов.



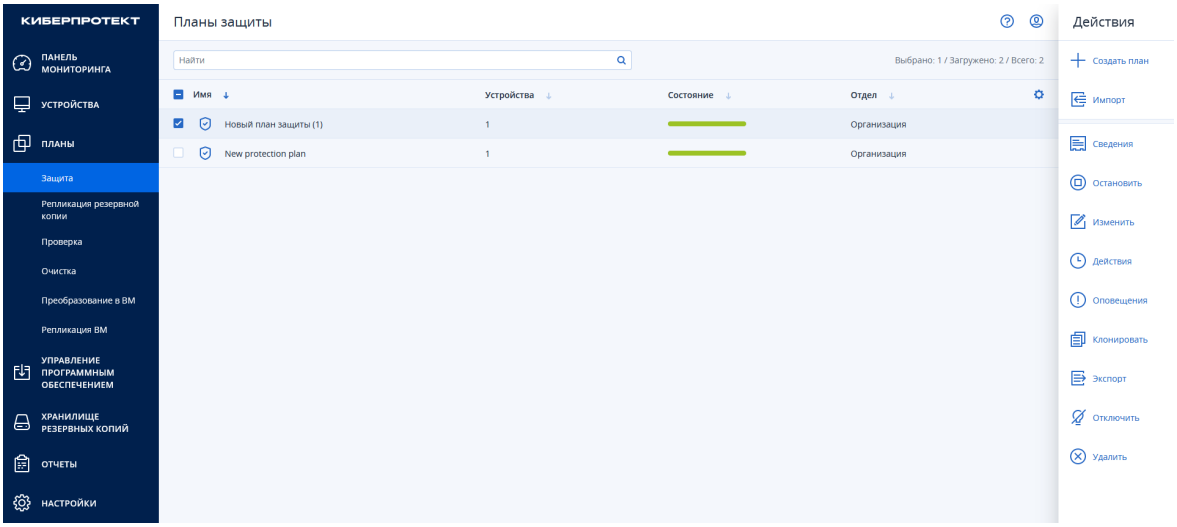
Справа отображается меню действий с планами. Из этого меню вы можете:

- Создать план
- Импортировать план

> **Примечание**
> Импортировать можно только те планы защиты, которые созданы в Кибер Бэкап 15 и 16.

3. Отметьте план в списке по вашему выбору. Справа в меню дополнительно появится список

действий с выбранным планом.



С выбранным планом можно выполнить указанные ниже действия.

- Просмотреть сведения о плане
- Остановить выполнение плана
- Переименовать план
- Изменить план
- Включить / отключить план
- Применить план к устройствам или группе устройств
- Отозвать план с устройства
- Клонировать план
- Экспортировать план
- Удалить план.

Примечание
Одно и то же действие с планами может быть доступно из разных вкладок меню действий с планами.

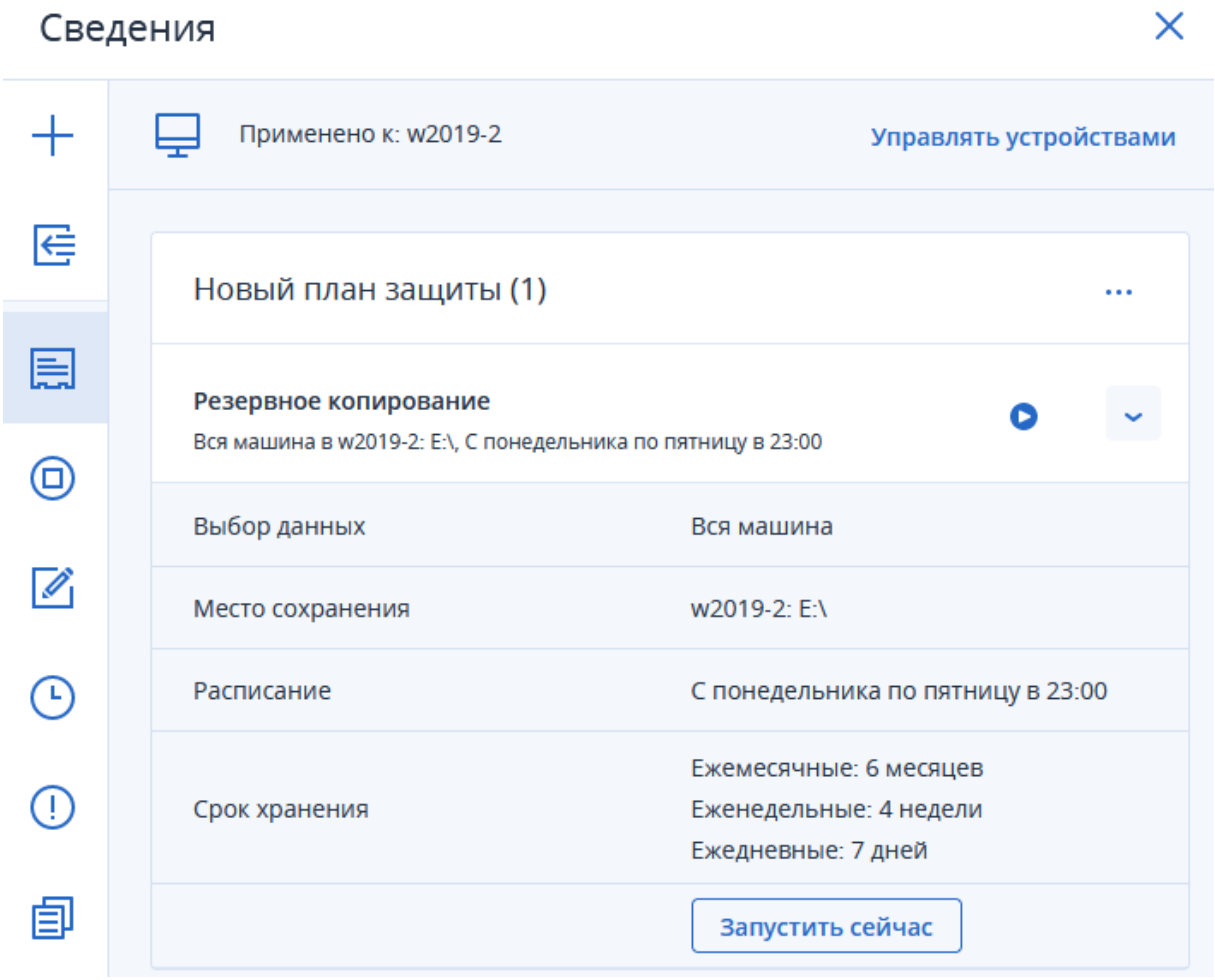
Примечание
Ряд действий с планами доступен также из вкладки **Устройства** основного меню веб-консоли.

Создание плана защиты

Информацию о создании плана защиты см. в разделе "Создание плана защиты" (стр. 157).

Просмотр сведений о плане

Для просмотра сведений о плане щелкните **Сведения** в меню справа. Отобразится вкладка сведений о плане.



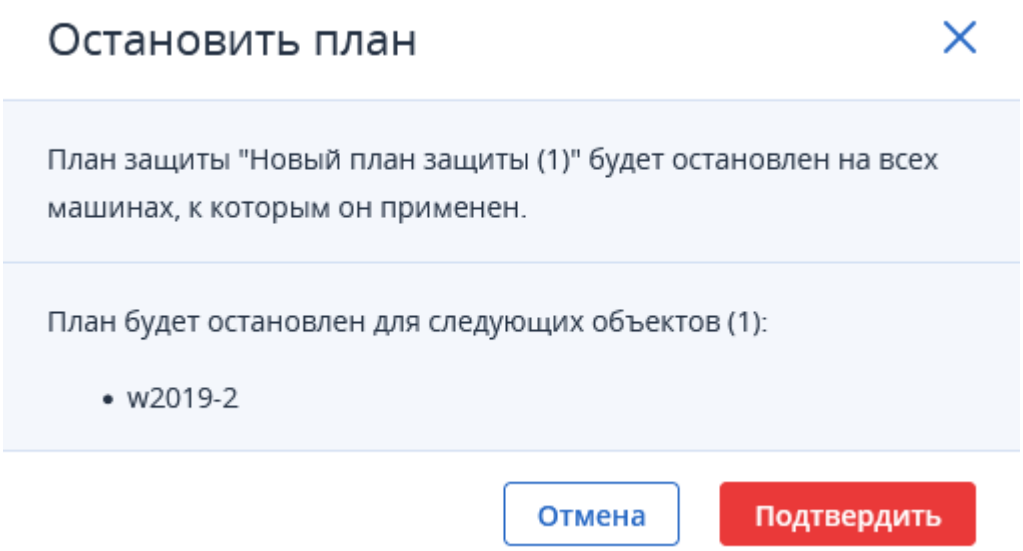
На этой вкладке также можно:

- Применить план к устройству
- Отозвать план с устройства
- Переименовать план
- Изменить план
- Отключить план
- Удалить план
- Запустить резервное копирование по требованию.

Подробнее об этих действиях см. далее.

Остановка выполнения плана

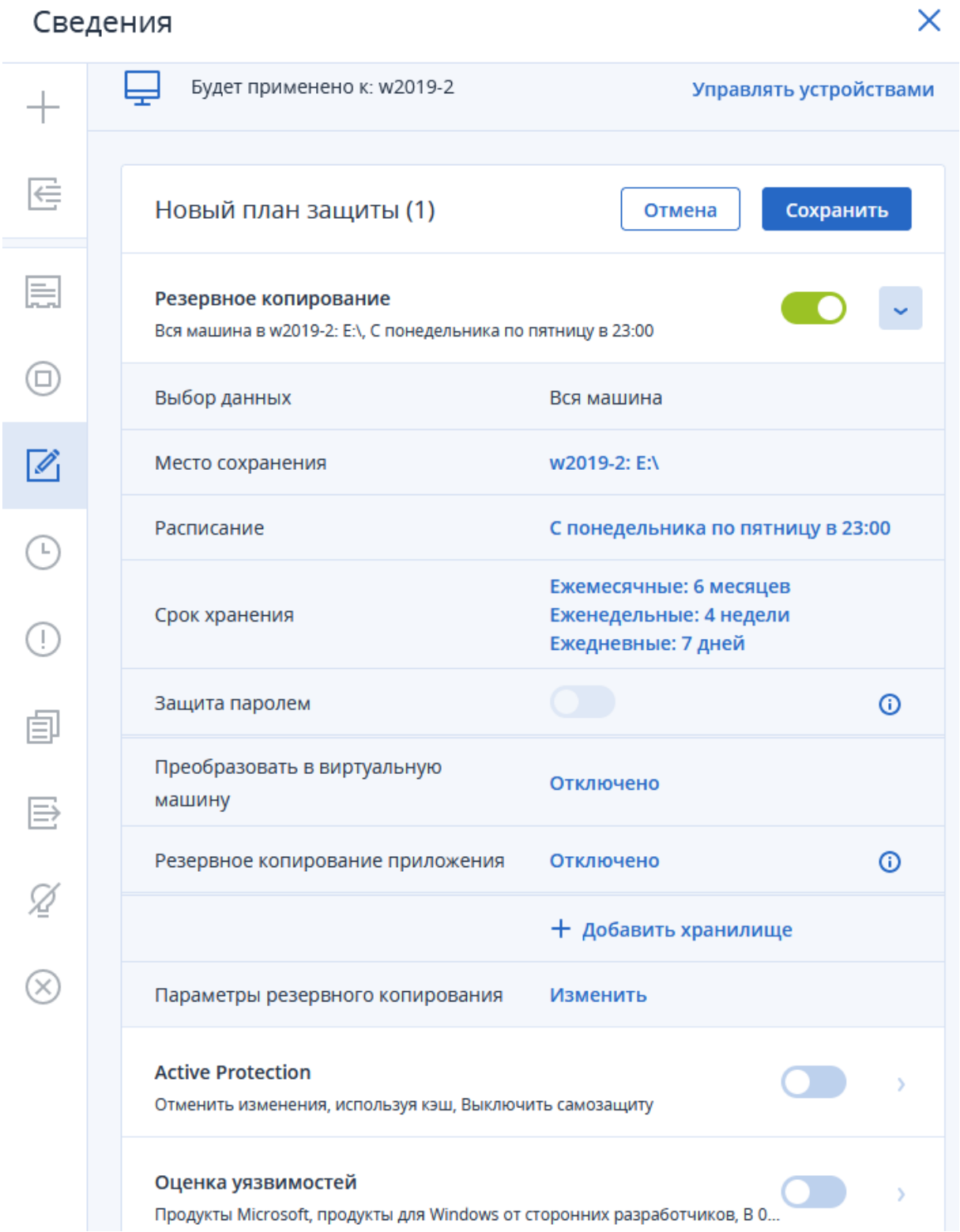
1. Щелкните **Остановить** в меню действий с планом. Откроется окно подтверждения.



2. Нажмите **Подтвердить**. План будет остановлен.

Изменение плана

Щелкните **Изменить** в меню действий с планом. Откроется вкладка с параметрами плана.



На вкладке можно сделать следующие изменения:

- Применить план к устройству (см. далее)
- Отозвать план с устройства (см. далее)

- Изменить место сохранения резервных копий
- Изменить расписание выполнения плана
- Изменить срок хранения резервных копий
- Изменить дополнительные параметры резервного копирования

Или (через вкладку **Устройства**):

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**.

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.

Включение / отключение плана

1. Нажмите **Включить** / **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.

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 устройство или устройства, 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**.
3. В программе отображаются ранее созданные планы защиты.
4. Выберите необходимую защиту и щелкните **Применить**.

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**.

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.
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.

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.

Импорт плана

1. Щелкните **Импорт** в меню действий с планом.
2. Выберите файл с планом и нажмите **Открыть**. План будет добавлен в список планов.

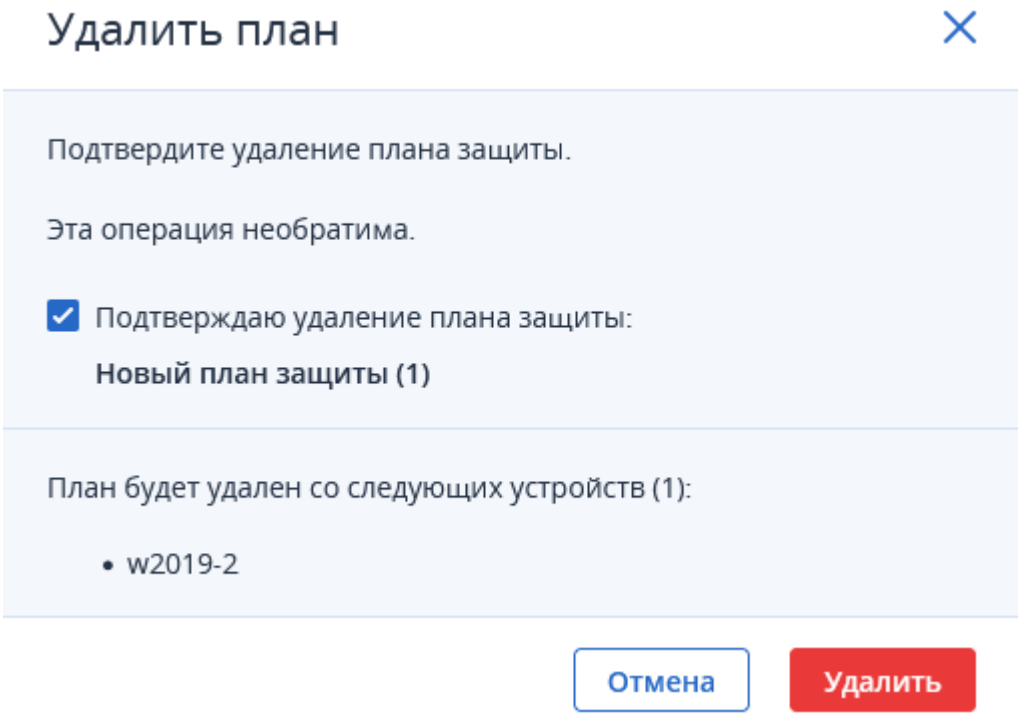
Экспорт плана

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.

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**.
5. В результате план защиты будет отозван для всех машин и полностью удален из веб-интерфейса.

6 Резервное копирование

План защиты с включенным модулем "Резервное копирование" – это набор правил, определяющий способ защиты указанных данных на конкретной машине.

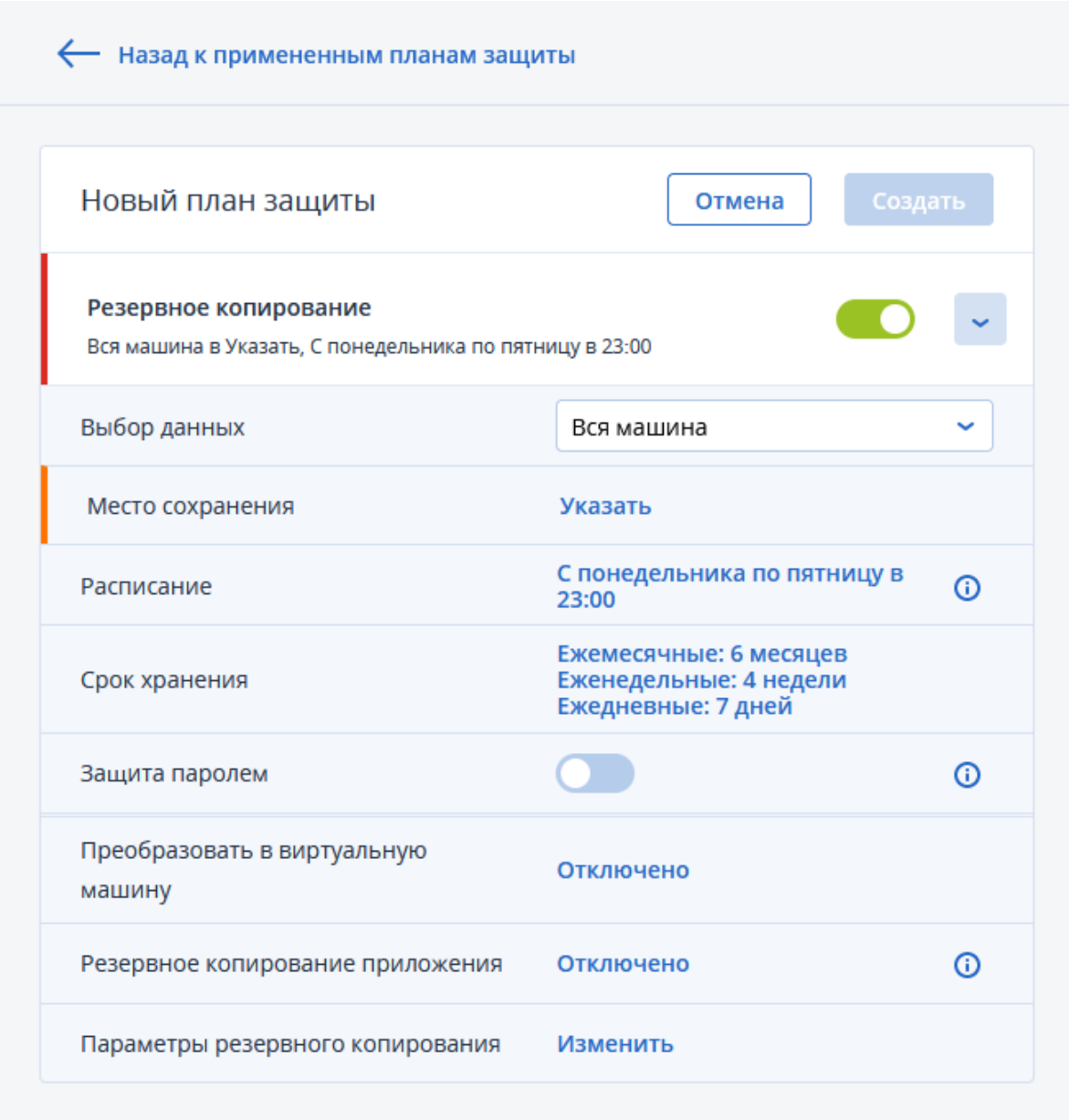
План защиты можно применить к нескольким машинам на этапе его создания или позже.

Примечание
Если в локальных развертываниях на сервере управления есть только стандартные лицензии, план защиты нельзя применить к нескольким физическим машинам. Для каждой физической машины должен быть свой собственный план защиты.

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.

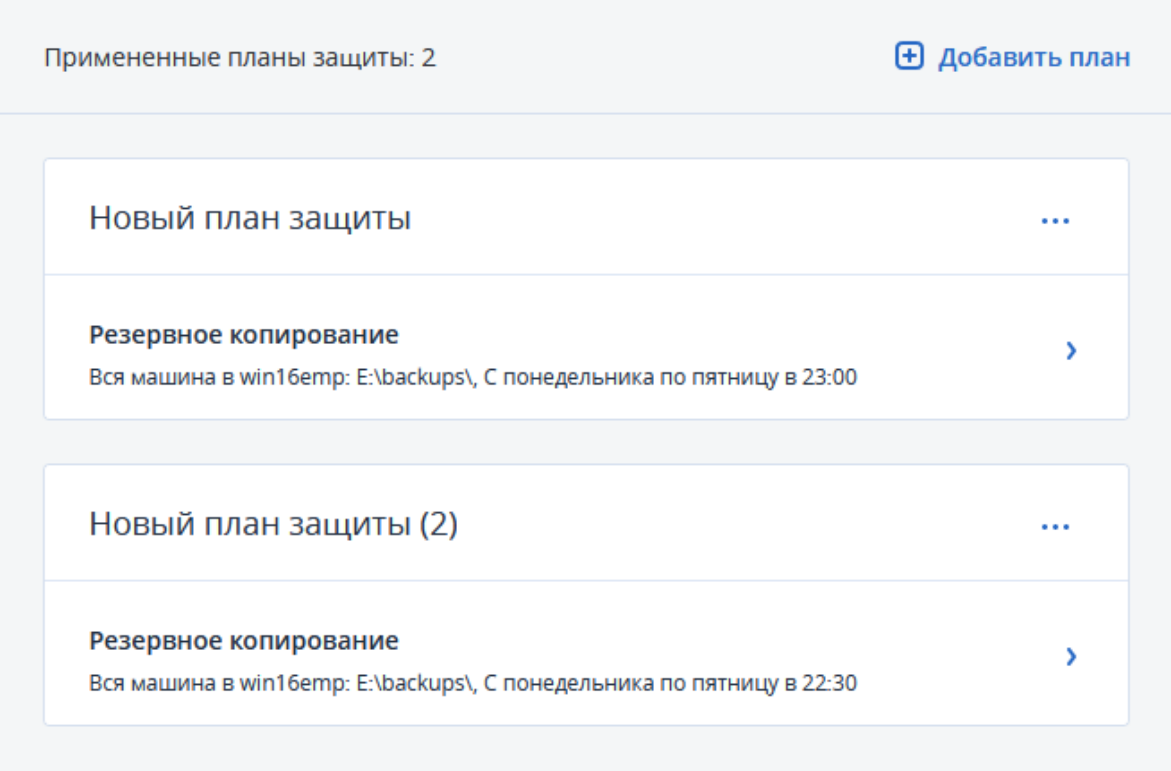


3. Чтобы создать новый план, щелкните **Создать план**. Включите модуль **Резервное копирование** и откатите настройки.
4. [Необязательно] Для изменения имени плана защиты щелкните имя по умолчанию.
5. [Необязательно] Чтобы изменить параметры модуля "Резервное копирование", щелкните соответствующий раздел 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

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 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*	Всегда инкрементное* Всегда полное Еженедельно полное, ежедневно	По возрасту резервной копии (одно правило на набор резервных

		Кибер Инфраструктура* Зона безопасности* Управляемое хранилище* Ленточное устройство*	инкрементное Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS) Настраиваемый вариант (П-Д-И)	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* NFS* Кибер Инфраструктура* Управляемое хранилище* Ленточное устройство*		
Файлы (только физические машины)	Напрямую Правила политики Фильтры файлов	Локальная папка Сетевая папка* Сервер SFTP* NFS* Кибер Инфраструктура* 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* Управляемое хранилище* Ленточное устройство	Всегда полное Еженедельно полное, ежедневно инкрементное Настраиваемый вариант (П-И)	
Базы данных Exchange	Напрямую			
Почтовые ящики Exchange	Напрямую	Локальная папка Сетевая папка* Кибер Инфраструктура* Управляемое хранилище*	Всегда инкрементное	По возрасту резервной копии (одно правило на набор резервных копий) По количеству резервных копий Хранить бессрочно
Почтовые ящики Office 365	Напрямую			

* См. ограничения ниже.

6.1.1 Ограничения

6.1.1.1 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 назначения резервных копий):

МЕСТО НАЗНАЧЕНИЯ	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.

6.1.1.2 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.

6.1.1.3 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.

6.1.1.4 Кибер Инфраструктура

Для более подробной информации о Кибер Инфраструктура см. раздел "О программе Кибер Инфраструктура" (стр. 186).

6.1.1.5 Зона безопасности

- Схема резервного копирования **Всегда инкрементное** для файлов (физических машин) недоступна при выполнении резервного копирования в зону безопасности.

6.1.1.6 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 и Office 365.

- Правило хранения **По общему размеру резервных копий** недоступно для управляемых хранилищ с активированной функцией дедупликации.

6.1.1.7 Всегда инкрементное

- Схема резервного копирования **Всегда инкрементное** недоступна при выполнении резервного копирования на SFTP-сервер или ленточное устройство.

6.1.1.8 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.

6.2 Выбор данных для резервного копирования

6.2.1 Выбор всей машины

Резервная копия всей машины – это резервная копия всех ее несъемных дисков.

Чтобы настроить такое резервное копирование, в области **Выбор данных** выберите **Вся машина**.

Примечание
Внешние диски, такие как USB-накопители или другие съемные носители, не включаются в резервную копию всей машины. Для резервного копирования таких дисков настройте резервное копирование дисков и томов. Дополнительные сведения о резервном копировании дисков см. в разделе "Выбор дисков и томов" (стр. 176).

6.2.2 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.

6.2.2.1 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**.

6.2.2.2 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
  - [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.

6.2.3 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.

6.2.3.1 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**.

6.2.3.2 Использование правил политики

1. В области **Элементы для резервного копирования** выберите вариант **Диски/тома**.
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 для Windows и Linux

- [All Volumes] позволяет выбрать все тома машин с Windows и все подключенные тома машин с Linux.
- [Fixed Volumes (physical machines)] 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.
- [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.

Правила только для Windows

- Буква диска (например, **C:**) обозначает том с указанной буквой.
- [ЗАГРУЗОЧНЫЙ+СИСТЕМНЫЙ ДИСК (физические машины)] 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

6.2.3.3 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.

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. 248)).

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.

6.2.4 Выбор конфигурации ESXi

Резервная копия конфигурации хоста ESXi позволяет восстановить хост ESXi на «голое железо». Восстановление выполняется с загрузочного носителя.

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.
- Для корректной загрузки восстановленной конфигурации ESXi рекомендуется отключить параметр **Безопасная загрузка** (Secure boot) в настройках хоста.

Порядок выбора конфигурации ESXi

1. Щелкните **Устройства** > **Все устройства**, 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.

6.3 Выбор места назначения

Внимание
Некоторые из функций, описанные в этом разделе, доступны только для локальных развертываний.

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.

6.3.1 Поддерживаемые расположения

- **Локальная папка**

  Если выбрана одна машина, перейдите на ней в соответствующую папку или введите путь.

  Если выбрано несколько машин, 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.

  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.

- **Кибер Инфраструктура**

  Кибер Инфраструктура – это высоконадежное программно-определяемое хранилище данных с избыточностью данных и автоматическим самовосстановлением. Это хранилище данных можно настроить как шлюз для хранения резервных копий в Microsoft Azure или в одном из ряда решений для хранения данных, совместимых с S3 или Swift. В хранилище также может

использоваться сервер NFS. Дополнительную информацию см. в разделе О продукте Кибер Инфраструктура.

- **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.

- **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.

- **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.

6.3.2 Расширенный выбор вариантов хранения

Определяется сценарием (доступно для машин под управлением Windows)

Можно хранить резервную копию каждой машины в папке, определенной сценарием. Программное обеспечение поддерживает сценарии на языках JScript, VBScript или Python 3.5. При развертывании плана защиты программа выполняет сценарий на каждой машине. 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 **Хранилище резервных копий** каждая папка показана в виде отдельного хранилища резервных копий.

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

Пример. 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**.

- **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».

  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.
- **Лента**

  Если ленточное устройство подключено к машине, для которой создана резервная копия или к узлу хранения, в списке хранилище 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».

6.3.3 О программе Зона безопасности

Зона безопасности – это безопасный раздел на диске машины, для которой создана резервная копия. В этом разделе могут храниться диски или файлы этой машины.

Если на диске произойдет физический сбой, резервные копии в разделе Зона безопасности могут быть утрачены. Поэтому Зона безопасности не должен быть единственным хранилищем резервных копий. В корпоративных средах Зона безопасности можно представить как вспомогательное хранилище резервных копий, когда обычное хранилище временно недоступно или подключено через медленный или загруженный канал.

6.3.3.1 Почему нужно использовать раздел Зона безопасности?

Зона безопасности:

- обеспечивает восстановление того же диска, на котором находится резервная копия этого 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; Это особенно полезно для пользователей, которые меняют место расположения.
- Может служить первичным назначением при использовании репликации резервных копий.

6.3.3.2 Ограничения

- Зона безопасности – это раздел на базовом диске. Его 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 раздел Зона безопасности. Это не влияет на процедуру резервного копирования и его скорость.
- Зона безопасности не поддерживает формат одного файла резервной копии[1]. При изменении назначения на раздел Зона безопасности в плане защиты, который имеет схему резервного копирования **Всегда инкрементное**, данная схема заменяется схемой **Еженедельно полное, ежедневно инкрементное**.

6.3.3.3 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.

---

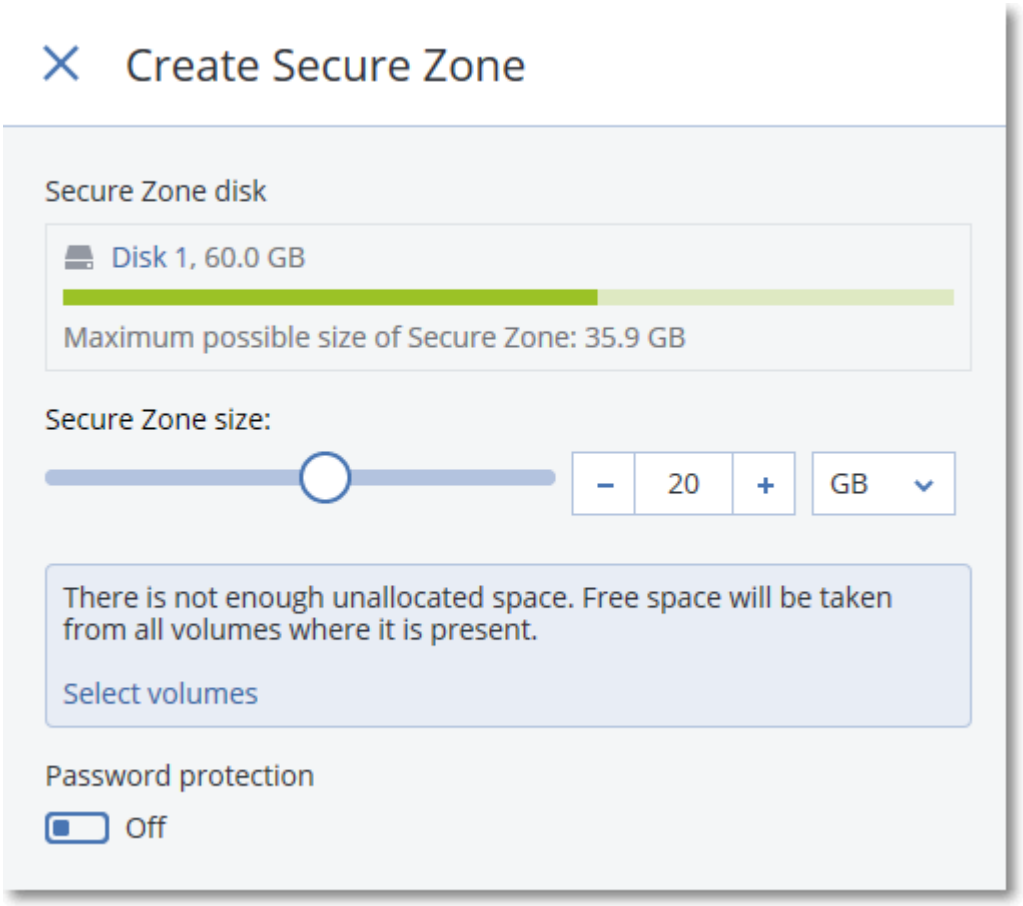
[1]Новый формат резервных копий, в котором начальная полная и последующие инкрементные резервные копии сохраняются в одном TIB-файле вместо цепочки файлов. Преимуществом этого формата является скорость инкрементного метода; при этом он лишен основного недостатка – сложностей, связанных с удалением устаревших 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.

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.

6.3.3.4 Порядок создания Зона безопасности

1. Выберите машину, на которой необходимо создать раздел Зона безопасности.
2. Щелкните **Сведения** > **Создать Зона безопасности** .
3. В разделе **Диск Зона безопасности** щелкните **Выбрать**, выберите жесткий диск (если их несколько), на котором нужно создать зону.
   Программа рассчитает максимальный возможный размер раздела Зона безопасности.
4. Введите размер Зона безопасности или перетащите ползунок, чтобы выбрать любой размер в диапазоне между минимальным и максимальным.
   Минимальный размер зоны 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.

   Для доступа к резервным копиям, расположенным в разделе Зона безопасности, необходимо будет указать пароль. 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 раздел Зона безопасности.

После этого раздел Зона безопасности можно выбрать в разделе **Место сохранения** при создании плана защиты.

6.3.3.5 Порядок удаления Зона 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 раздел Зона безопасности будет удален вместе со всеми содержащимися в нем резервными копиями.

6.3.4 О программе Кибер Инфраструктура

Кибер Бэкап 17 поддерживает интеграцию с Кибер Инфраструктура 3.5 с обновлением 5 или более поздних версий.

6.3.4.1 Развертывание

Чтобы использовать Кибер Инфраструктура, разверните его на «голом железе» в локальном месте. Чтобы воспользоваться всеми преимуществами данного продукта, необходимо по крайней мере пять физических серверов. Если нужна только функциональность шлюза, можно использовать один физический или виртуальный сервер либо настроить кластер шлюзов с максимально большим количеством серверов.

Убедитесь, что настройки времени синхронизированы между сервером управления и Кибер Инфраструктура. Настройки времени для КиберИнфраструктура можно настроить при развертывании. Синхронизация времени по протоколу NTP включена по умолчанию.

Можно развернуть несколько экземпляров Кибер Инфраструктура и зарегистрировать их на одном сервере управления.

6.3.4.2 Регистрация

Регистрация выполняется в веб-интерфейсе Кибер Инфраструктура. Кибер Инфраструктура 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.

Обратная операция (отмена регистрации) выполняется в интерфейсе Кибер Бэкап. Щелкните **Настройки** > **Узлы хранения**, щелкните требуемый экземпляр Кибер Инфраструктура, а затем щелкните **Удалить**.

6.3.4.3 Добавление хранилища резервных копий

В отдел или организацию можно добавить только по одному хранилищу резервных копий на каждый экземпляр Кибер Инфраструктура. 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...**, щелкните **Обзор** и выберите хранилище в списке.

Если на сервере управления зарегистрировано несколько экземпляров Кибер Инфраструктура, можно выбрать экземпляр Инфраструктура при добавлении хранилища.

6.3.4.4 Ограничения для Кибер Инфраструктура

- Невозможно выполнить прямой доступ к Кибер Инфраструктура с загрузочного носителя. Для работы с Кибер Инфраструктура зарегистрируйте носитель на сервере управления и управляйте им с веб-консоли Кибер Бэкап.
- Доступ к Кибер Инфраструктура через интерфейс командной строки невозможен.
- Резервное копирование в Кибер Инфраструктура недоступно для конфигураций ESXi.
- После окончания резервного копирования в некоторых случаях размер больших архивов может обновляться с задержкой.

6.3.4.5 Документация

Полный набор документации по Кибер Инфраструктура доступен на веб-сайте Киберпротект.

6.4 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).

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.

6.4.1 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)**

  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.

  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. 242)). 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.

- **Пользовательские**

[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.

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».

6.4.2 Дополнительные параметры расписания

Для каждого места назначения 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.

  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.

6.4.3 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.

  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	-	-	-	-	-
Почтовые ящики Office 365	Windows	-	-	-	-	Windows
Базы данных и почтовые ящики Exchange	Windows	-	-	-	-	Windows
Базы данных SQL	Windows	-	-	-	-	Windows

6.4.3.1 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 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**.

- **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**.

6.4.4 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	Почтовые ящики Office 365	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	Windows
Пользователи завершили сеанс	Windows	-	-	-	-	-
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	-	-	-	-	-

6.4.4.1 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.

6.4.4.2 Хост хранилища резервных копий доступен

Строка «Хост хранилища резервных копий доступен» означает, что машина, служащая назначением для хранения резервных копий, доступна в сети.

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.

6.4.4.3 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.

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.

6.4.4.4 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.

6.4.4.5 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**
  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.

6.4.4.6 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:

(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.

6.4.4.7 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.

(3) Если машина всегда подключено к указанным сетям по рабочим дням 21:00, то резервное копирование вообще не запускается.

6.4.4.8 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.

6.5 Правила хранения

Внимание
Некоторые из функций, описанные в этом разделе, доступны только для локальных развертываний.

1. Нажмите **Срок хранения**.
2. В разделе **Очистка** выберите один из перечисленных ниже вариантов.

- **По возрасту резервной копии** (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, щелкните **Перейти на использование одного правила для всех наборов резервных копий**.
- **По количеству резервных копий**

  Укажите максимальное количество хранимых резервных копий.
- **По общему размеру резервных копий**

  Укажите максимальный общий размер резервных копий.

  Данная настройка недоступна в схеме резервного копирования **Всегда инкрементное** или при резервном копировании на сервер SFTP или на ленточное устройство.
- **Хранить резервные копии неопределенно долго**

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.

6.5.1 Что еще 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.
- Резервные копии, которые хранятся на ленточном накопителе, не удаляется 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 удален до окончания времени существования всех зависимых от него резервных копий (инкрементных и дифференциальных). Для хранения резервных копий, удаление которых отложено, требуется

[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

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 резервной копии».

- Правила хранения – составная часть плана защиты. Они прекращают действовать для резервных копий машины, как только с нее отозван или удален 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".

6.6 Защита паролем

Внимание
Если вы забыли или потеряли пароль, восстановить защищенные резервные копии невозможно.

6.6.1 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 включите переключатель **Защита паролем**.
2. Укажите и подтвердите пароль.
3. Выберите один из следующих уровней защиты паролем:
   - **Низкий** – резервные копии будут защищены паролем с уровнем защиты **Низкий**.
   - **Средний** – резервные копии будут защищены паролем с уровнем защиты **Средний**.
   - **Высокий** – резервные копии будут защищены паролем с уровнем защиты **Высокий**.
4. Нажмите кнопку **OK**.

6.6.2 Защита паролем как свойство машины

Этот параметр предназначен для администраторов, которые работают с резервными копиями нескольких машин. Если необходим уникальный пароль защиты для каждой машины, или нужно защитить паролем отдельные резервные копии независимо от настроек плана защиты, сохраните настройки защиты паролем на каждой машине в отдельности. Резервные копии будут защищены с уровнем защиты **Высокий**.

Сохранение настроек защиты паролем на машине влияет на планы защиты следующим образом:

- **Планы защиты, которые уже применены к машине.** Если настройки защиты паролем в плане отличаются, резервное копирование завершится сбоем.

- **Планы защиты, которые будут применены к машине позже.** Настройки защиты паролем, сохраненные на машине, переопределят аналогичные настройки плана защиты. Паролем будут защищаться все резервные копии, даже если это отключено в плане защиты.

Это можно использовать на машине с запущенным агентом для VMware. Однако следует соблюдать осторожность, если к одному серверу vCenter Server подключено несколько агентов для VMware. Настройки защиты паролем должны быть одинаковы для всех агентов, поскольку между ними имеет место процесс распределения нагрузки.

После сохранения настроек защиты паролем их можно изменить или сбросить, как описано ниже.

Внимание
Если план защиты, который выполняется на этой машине, уже создал резервные копии, изменение настроек защиты паролем приведет к сбою этого плана. Чтобы продолжить резервное копирование, создайте новый план.

Сохранение настроек защиты паролем на машине

1. Войдите как администратор (в Windows) или пользователь root (в Linux).
2. Выполните следующий сценарий:
   - В Windows: <путь_установки>**\PyShell\bin\acropsh.exe -m manage_creds --set-password** <пароль_защиты>

     Здесь <путь_установки> – это путь к установленному агенту. По умолчанию в локальных развертываниях используется путь **%ProgramFiles%\Acronis** .
   - В Linux: **/usr/sbin/acropsh -m manage_creds --set-password** <пароль_защиты>

Сброс настроек защиты паролем на машине

1. Войдите как администратор (в Windows) или пользователь root (в Linux).
2. Выполните следующий сценарий:
   - В Windows: <путь_установки>**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     Здесь <путь_установки> – это путь к установленному агенту. По умолчанию в локальных развертываниях используется путь **%ProgramFiles%\Acronis** .
   - В Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Порядок изменения настроек защиты паролем с использованием программы Мониторинг Защиты Данных

1. Войдите в систему как администратор в Windows.
2. Щелкните значок **Мониторинг Защиты Данных** в области уведомлений Windows.
3. Выберите значок шестеренки.
4. Выберите пункт **Защита паролем**.
5. Выполните одно из следующих действий:

- Установите **пароль для этой машины**. Укажите и подтвердите пароль защиты.
- Выберите пункт **Использовать настройки защиты паролем, указанные в плане защиты**.

6. Нажмите кнопку **OK**.

6.6.3 Особенности защиты паролем

Чем выше уровень защиты паролем, тем дольше выполняется план защиты.

Пароль не сохраняется на диске или в резервных копиях. Это позволяет обезопасить данные резервной копии от несанкционированного доступа, но восстановление утраченного пароля невозможно.

6.7 Преобразование в виртуальную машину

Внимание
Некоторые из функций, описанные в этом разделе, доступны только для локальных развертываний.

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.

6.7.1 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.

6.7.2 Важная информация о преобразовании

6.7.2.1 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
VMware ESXi	+	-	-	-
Microsoft Hyper-V	-	+	-	-
VMware Workstation	+	+	+	+
Файлы VHDX	+	+	+	+

6.7.2.2 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.

6.7.2.3 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.

6.7.3 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**.

6.7.4 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.

6.7.4.1 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.

6.7.4.2 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.

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.

6.8 Репликация

Внимание
Некоторые из функций, описанные в этом разделе, доступны только для локальных развертываний.

В данном разделе описана репликация резервных копий, которая включена в план защиты. Информацию о создании отдельного плана репликации см. в разделе «Обработка данных Off-host».

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.

6.8.1 Примеры использования

- **Надежное аварийное восстановление**

  Храните резервные копии локально (для немедленного восстановления) и удаленно (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 емкость хранения данных.

6.8.2 Поддерживаемые расположения

Можно выполнить репликацию резервной копии *из* любого указанного ниже расположения:

- Локальная папка
- Сетевая папка
- Зона безопасности
- SFTP-сервер
- Хранилище под управлением узла хранения

Можно выполнить репликацию резервной копии *в* любое указанное ниже расположение:

- Локальная папка
- Сетевая папка
- SFTP-сервер
- Хранилище под управлением узла хранения
- Ленточное устройство

Включение репликации резервных копий

1. На панели плана резервного копирования щелкните **Добавить хранилище**.

   Элемент управления **Добавить хранилище** отображается только в том случае, если поддерживается репликация *из*последнего выбранного хранилища.
2. Укажите хранилище, в котором будет проведена репликация резервных копий.
3. [Необязательно] В поле **Срок хранения** измените правила хранения для указанного хранилища, как описано в разделе «Правила хранения».
4. [Необязательно] В поле **Преобразовать в VM**укажите настройки преобразования в виртуальную машину, как описано в «Преобразование в виртуальную машину».
5. [Необязательно] Щелкните значок шестерни > **Производительность и окно резервного копирования**, затем задайте окно резервного копирования для выбранного расположения, как описано в теме «Производительность и окно резервного копирования». 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).

6.8.3 Рекомендации для пользователей с лицензией Advanced

6.8.3.1 Ограничения

- Репликация резервных копий *из* хранилища, управляемого узлом хранения, на локальную папку не поддерживается. Локальной папкой называется папка на машине с агентом, создавшим резервную копию.
- Репликация резервных копий *в* управляемое хранилище с включенной дедупликацией не поддерживается для резервных копий, имеющих формат резервной копии **Версии 12**.

6.8.3.2 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.

6.8.3.3 Репликация резервных копий между управляемыми хранилищами

Репликация резервной копии из одного управляемого хранилища в другое выполняется узлом хранения.

Если для целевого хранилища включена дедупликация (возможно, на другом узле хранения), узел хранения источника отправляет только те блоки данных, которые отсутствуют в целевом хранилище. Другими словами, узел хранения, как и агент, выполняет дедупликацию в источнике. Это помогает уменьшить сетевой трафик при репликации данных между географически разделенными узлами хранения.

6.9 Запуск резервного копирования вручную

1. Выберите машину, для которой применен хотя бы один план защиты.
2. Нажмите кнопку **Резервное копирование**.
3. Если применено несколько планов защиты, выберите один из них.
4. Выполните одно из следующих действий:
   - Щелкните **Запустить сейчас**. Будет создана инкрементная резервная копия.

- Если схема резервного копирования содержит несколько методов резервного копирования, можно выбрать метод для использования. Щелкните стрелку на кнопке **Запустить сейчас**, а затем выберите **«Полная», «Инкрементная»** или **«Дифференциальная»**.

Первая резервная копия, созданная планом защиты, всегда является полной.

Прогресс выполнения резервного копирования отображается в столбце **Состояние** для выбранной машины.

6.10 Параметры резервного копирования

Внимание
Некоторые из функций, описанные в этом разделе, доступны только для локальных развертываний.

Чтобы изменить параметры резервного копирования, щелкните значок шестерни рядом с именем плана защиты и щелкните **Параметры резервного копирования**.

6.10.1 Доступность параметров резервного копирования

Набор доступных параметров резервного копирования зависит от следующих факторов:

- 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 или сетевая папка).

В следующей таблице представлены обобщенные сведения по доступности параметров резервного копирования.

	Резервное копирование на уровне дисков		Резервное копирование на уровне файлов		Виртуальные машины		SQL и Exchange
	Windows	Linux	Windows	Linux	ESXi	Hyper-V	Windows
Оповещения	+	+	+	+	+	+	+
Консолидация резервных копий	+	+	+	+	+	+	-
Имя файла резервной копии	+	+	+	+	+	+	+
Формат резервной копии	+	+	+	+	+	+	+

Проверка резервных копий	+	+	+	+	+	+	+
Функция Changed Block Tracking (CBT)	+	-	-	-	+	+	+
Способ резервного копирования кластера	-	-	-	-	-	-	+
Уровень сжатия	+	+	+	+	+	+	+
Уведомления по электронной почте	+	+	+	+	+	+	+
Обработка ошибок							
Повтор операции при возникновении ошибки	+	+	+	+	+	+	+
Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений)	+	+	+	+	+	+	+
Пропуск поврежденных секторов	+	+	+	+	+	+	-
Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины	-	-	-	-	+	+	-
Быстрое инкрементное/дифференциальное резервное копирование	+	+	-	-	-	-	-
Фильтры файлов	+	+	+	+	+	+	-
Моментальные снимки резервных копий на уровне файлов	-	-	+	+	-	-	-
Сокращение журнала	-	-	-	-	+	+	Только SQL
Создание моментальных снимков LVM	-	+	-	-	-	-	-

Точки подключения	-	-	+	-	-	-	-
Многотомные моментальные снимки	+	+	+	+	-	-	-
Производительность и окно резервного копирования	+	+	+	+	+	+	+
Команды до и после процедуры	+	+	+	+	+	+	+
Команды до и после захвата данных	+	+	+	+	+	-	+
Моментальные снимки оборудования SAN	-	-	-	-	+	-	-
Планирование							
Распределять время запуска по доступному времени	+	+	+	+	+	+	+
Ограничить число одновременно выполняющихся операций резервного копирования	-	-	-	-	+	+	-
Посекторное резервное копирование	+	+	-	-	+	+	-
Деление	+	+	+	+	+	+	+
Управление лентами	+	+	+	+	+	+	+
Действия при сбое задания	+	+	+	+	+	+	+
Условия запуска задания	+	+	+	+	+	+	+
Служба теневого копирования томов (VSS)	+	-	+	-	-	+	+
Служба теневого копирования томов (VSS) для виртуальных машин	-	-	-	-	+	+	-
Еженедельное резервное	+	+	+	+	+	+	+

копирование							
Журнал событий Windows	+	-	+	-	+	+	+

6.10.2 Оповещения

6.10.2.1 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.

6.10.3 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 назначения 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 () 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.

6.10.4 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.

6.10.4.1 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 **Хранилище резервных копий**.

6.10.4.2 Где можно просмотреть имена файлов резервных копий?

Выберите вкладку **Хранилище 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 **Хранилище резервных копий** в столбце **Имя**.

6.10.4.3 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**).

6.10.4.4 Имя файла резервной копии по умолчанию

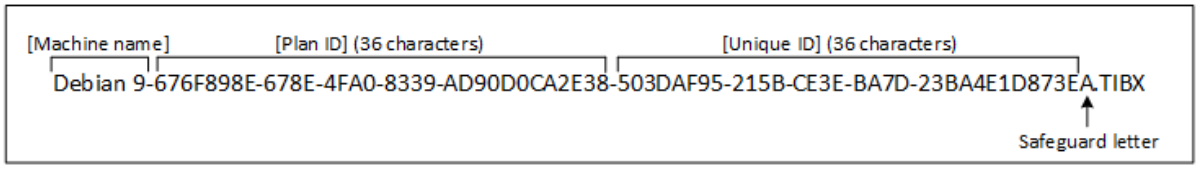
Имя файла резервной копии по умолчанию имеет вид [Имя машины]-[Идентификатор плана]-[Уникальный идентификатор]A.

Имя файла резервной копии по умолчанию для почтового ящика имеет вид [Идентификатор почтового ящика]_почтовый ящик_[Идентификатор плана]A.

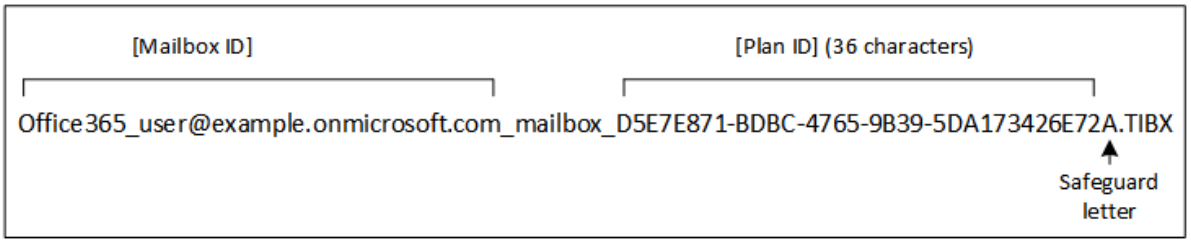
Имя состоит из следующих переменных:

- [Имя машины] Эта переменная заменяется именем машины (такое же имя отображается на веб-консоли Кибер Бэкап) для всех типов резервных копий данных, за исключением почтовых ящиков Office 365. Для почтовых ящиков Office 365 она заменяется именем участника-пользователя (UPN) почтового ящика.
- [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.



На приведенной ниже диаграмме показано имя по умолчанию файла резервной копии для почтового ящика.



6.10.4.5 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
...
```

6.10.4.6 Использование переменных

Кроме переменных, используемых по умолчанию, можно использовать переменную [Имя плана], которая заменяется именем плана защиты.

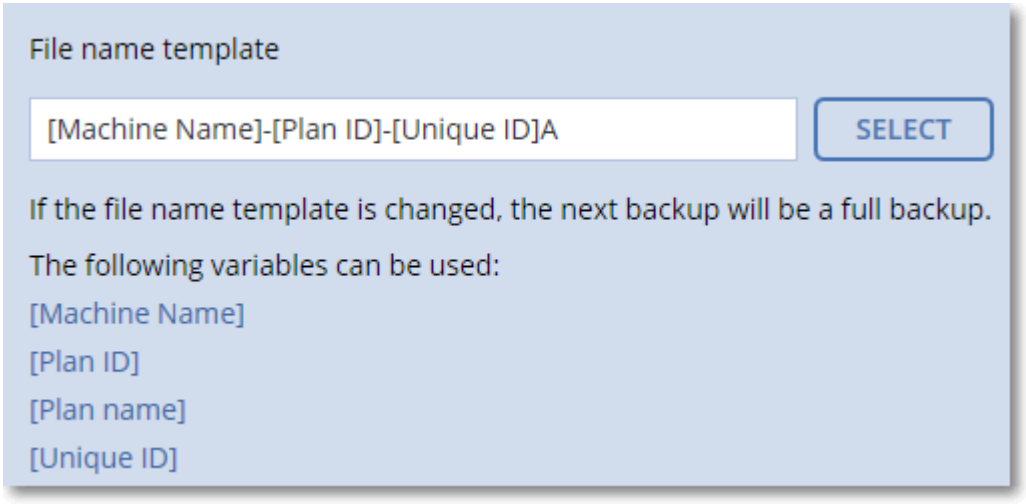
Если выбрано резервное копирование нескольких машин или почтовых ящиков, имя файла резервной копии должно содержать переменную [Имя машины], [Идентификатор почтового ящика] или [Уникальный идентификатор].

6.10.4.7 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.

6.10.4.8 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.

Примечание
Кнопка **Выбрать** доступна только для планов защиты, которые созданы и применены для одного устройства.

6.10.5 Формат резервной копии

Этот параметр определяет формат резервных копий, созданных планом защиты. Он доступен только для планов защиты, которые используют устаревший формат резервных копий "Версия 11". В этом случае его можно изменить на новый формат "Версия 12". После этого изменения параметр станет недоступен.

Этот параметр *не* применим к резервным копиям почтового ящика. Резервные копии почтового ящика всегда имеют новый формат.

Значение по умолчанию: **Автоматический выбор**.

Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:

- **Автоматический выбор**
  Будет использоваться формат "Версия 12", за исключением случаев, когда план защиты добавляет резервные копии к уже созданным в продукте более ранней версии.
- **Версия 12**
  В большинстве случаев для быстрого резервного копирования и восстановления рекомендуется новый формат. Каждая цепочка резервных копий (полного или дифференциального

копирования, и всех зависящих от них инкрементных резервных копий) сохраняется в один файл TIBX.

С этим форматом правило хранения **По общему размеру резервных копий** не применимо.

- **Версия 11**

  Возможность использовать устаревший формат сохранена для обеспечения обратной совместимости. Это позволит добавлять резервные копии к уже созданным в продукте более ранней версии.

  Также используйте этот формат (с любой схемой резервного копирования, за исключением **Всегда инкрементное**) для полного, инкрементного и дифференциального резервного копирования в отдельные файлы.

  Этот формат выбирается автоматически, если местом назначения резервной копии (или местом назначения репликации) является управляемое хранилище с включенной дедупликацией. Если изменить формат на **Версию 12**, резервное копирование не будет выполнено.

Примечание
Невозможно создать резервную копию групп обеспечения доступности баз данных (DAG), используя формат архива "Версия 11". Резервное копирование группы обеспечения доступности баз данных поддерживается только в формате "Версия 12".

6.10.5.1 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 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).	

6.10.5.2 Изменение формата резервной копии на "Версия 12" (TIBX)

При изменении формата резервной копии с версии 11 (формат .tib) на версию 12 (формат .tibx) имеет место 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 **Хранилище резервных копий**. Их можно удалить вручную.
- Старые локальные резервные копии будут занимать пространство в пределах квоты **Локальная резервная копия** до тех пор, пока не вы не удалите их вручную.
- Если местом назначения резервной копии (или местом назначения репликации) является управляемое хранилище с включенной дедупликацией, операции резервного копирования завершатся сбоем.

6.10.5.3 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 TIBX. Не нужно включать ее в параметрах резервного копирования. Отключить ее также невозможно.

6.10.6 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.

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.

6.10.7 Функция Changed Block Tracking (CBT)

Этот параметр применим для резервных копий на уровне дисков для виртуальных и физических машин, работающих под управлением Windows. Он также применим к резервным копиям баз данных Microsoft SQL Server и Microsoft Exchange Server.

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.

6.10.8 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.

6.10.8.1 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. 344).

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.

6.10.8.2 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. 346).

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.

6.10.8.3 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**
  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.

6.10.9 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.

6.10.10 Уведомления по электронной почте

Этот параметр позволяет задать уведомления по электронной почте о событиях, которые возникают во время резервного копирования.

Этот параметр доступен только в локальных развертываниях.

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
   - [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.

6.10.11 Обработка ошибок

Эти параметры позволяют указать, как должны обрабатываться ошибки, возникшие во время резервного копирования.

6.10.11.1 В случае ошибки повторить попытку

Значение по умолчанию: **Включено. Количество попыток: 30. Интервал между попытками: 30 секунд.**

Если возникла устранимая ошибка, программа будет продолжать попытки выполнить операцию. 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 назначения 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.

6.10.11.2 Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений)

Значение по умолчанию: **Включено**.

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.

6.10.11.3 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.

6.10.11.4 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).

6.10.12 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.

6.10.13 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.

6.10.13.1 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**).

  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**

6.10.13.2 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**.

6.10.13.3 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 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.

6.10.14 Моментальные снимки резервных копий на уровне файлов

Этот параметр действует только 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.

6.10.15 Сокращение журнала

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.

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 тот момент времени, когда этим программным обеспечением была создана резервная копия. Журналы транзакций резервного копирования создаются встроенным модулем архивации Microsoft SQL Server. Можно будет применить журналы транзакций после восстановления и таким образом восстановить базу данных в состояние на любой момент времени.

6.10.16 Создание моментальных снимков LVM

Этот параметр действует только для физических машин.

Этот параметр действует только для резервного копирования на уровне дисков томов, управляемых диспетчера 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.

6.10.17 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.)

- 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**.

6.10.18 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:

- 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.

6.10.19 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.

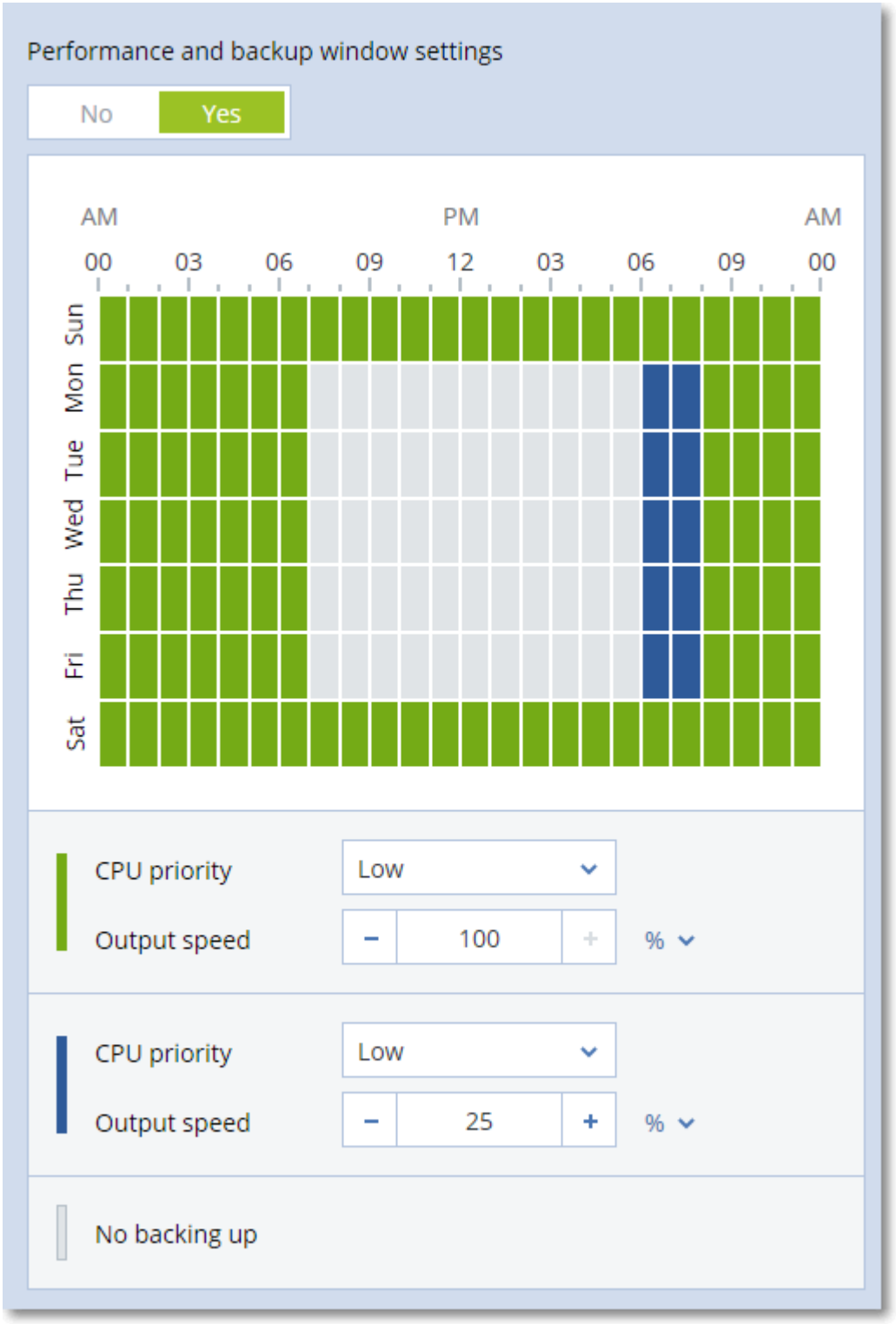
Даже если запланированные резервные копии заблокированы, резервное копирование можно запустить вручную. Для него будут использоваться параметры производительности последнего часа, когда процессы резервного копирования были разрешены.

6.10.19.1 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.



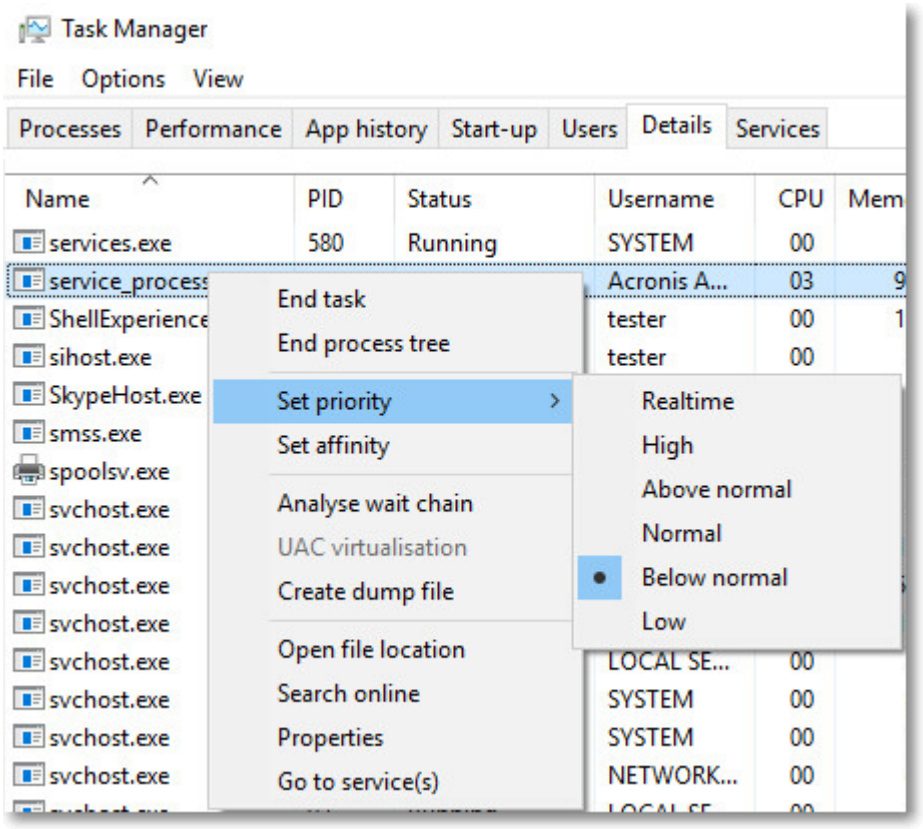
6.10.19.2 Приоритет ЦП

Этот параметр задает приоритет процесса резервного копирования (**service_process.exe**) в операционной системе Windows.

Доступные значения:

- **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.



6.10.19.3 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 в том случае, если агент выполняется в Windows.

- В КБ/секунду (для всех мест назначения).

6.10.20 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.

Программа не поддерживает интерактивные команды, то есть команды, которые требуют пользовательского ввода (например, pause).

6.10.20.1 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 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 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.

6.10.20.2 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 найдите пакетный файл.
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 резервное копирование 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 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**.

6.10.21 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="4"><---------- 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></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.

6.10.21.1 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).
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 выполнения команды. Прерывать резервное копирование при сбое команды.	Выполнить захват данных после команды независимо от результатов ее выполнения (успешно или ошибка).	Н/Д	Выполнить захват данных одновременно с выполнением команды и независимо от результатов выполнения команды.

* Команда считается сбойной, если код завершения не равен нулю.

6.10.21.2 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	Установить	Снять	Установить	Снять

резервное копирование при сбое команды*				
Не продолжать создание резервной копии до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				
	Предустановка Продолжить резервное копирование только после успешного выполнения команды.	Продолжить резервное копирование после команды независимо от результатов ее выполнения (успешно или ошибка).	Н/Д	Продолжить резервное копирование одновременно с выполнением команды и независимо от результатов выполнения команды.

* Команда считается сбойной, если код завершения не равен нулю.

6.10.22 Моментальные снимки оборудования SAN

Эта опция эффективна для резервного копирования виртуальных машин VMware ESXi.

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. Моментальный снимок хранится все время резервного копирования.

Если этот параметр включен, содержимое виртуального диска будет прочитано с моментального снимка SAN. Моментальный снимок VMware будет создан и сохранен на небольшое время, чтобы привести виртуальные диски в согласованное состояние. Если чтение с моментального снимка SAN невозможно, резервное копирование завершится ошибкой.

Перед подключением этой опции проверьте и выполните все требования, указанные в разделе «Использование моментальных снимков оборудования SAN».

6.10.23 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.

Значение по умолчанию:

- Локальное развертывание: **Начинать все операции резервного копирования строго по расписанию.**

Для этого укажите Учетная запись для входа службы агента. 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.
- **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.
  Резервное копирование физических машин запустится точно в соответствии с расписанием.

6.10.24 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.

6.10.25 Деление

Этот параметр применим для следующих схем резервного копирования: **Всегда полное**, **Еженедельно полное, ежедневно инкрементное**, **/Ежемесячное полное, еженедельное дифференциальное, дневное инкрементное (GFS)/** и **Пользовательские**.

Этот параметр позволяет выбрать метод разделения резервных копий на фрагменты.

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 резервной копии" (стр. 283)), разделенной 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.

6.10.26 Управление лентами

Эти параметры применимы только при резервном копировании на ленточное устройство.

6.10.26.1 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.

Этот функционал недоступен для резервных копий ВМ на лентах, созданных без физического агента.

Дополнительные файлы располагаются в следующих местах:

- 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 файлов недоступно, если размер архива резервной копии менее 500 КБ.

6.10.26.2 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.

6.10.26.3 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.

6.10.26.4 Перезаписать ленту в автономном ленточном устройстве при создании полной резервной копии

Значение по умолчанию: **Отключено**.

Параметр применяется только к изолированным ленточным устройствам. Если этот параметр включен, лента, вставленная в устройство, будет перезаписываться каждый раз при создании полной резервной копии.

6.10.26.5 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.

6.10.26.6 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.

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.

6.10.26.7 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:

- **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.

6.10.26.8 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 года**, **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.

  Примечание
  Этот параметр рекомендуется включать при выборе схемы **Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS)** (см. "Расписание" (стр. 187)).
  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**
  При выборе этого варианта возможно указание собственного правила для организации наборов лент. Правило может содержать следующие переменные:

Синтаксис переменной	Описание переменной	Доступные значения
[Имя ресурса]	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 ресурса]	Резервные копии каждого типа машин будут храниться на отдельном наборе лент.	Экземпляры сервера, сервер, рабочая станция, физическая машина, виртуальная машина VMware, виртуальная машина Virtual-PC, виртуальная машина виртуального сервера, виртуальная машина Hyper-V, виртуальная машина Parallels, виртуальная машина XEN, виртуальная машина KVM, виртуальная машина RHEV,
[День месяца]	Резервные копии, созданные в каждый день месяца, будут	01, 02, 03, ..., 31

	храниться на отдельном наборе лент.	
[День недели]	Резервные копии, созданные в каждый день недели, будут храниться на отдельном наборе лент.	Воскресенье, Понедельник, Вторник, Среда, Четверг, Пятница, Суббота
[Месяц]	Резервные копии, созданные в каждый месяц года, будут храниться на отдельном наборе лент.	Январь, Февраль, Март, Апрель, Май, Июнь, Июль, Август, Сентябрь, Октябрь, Ноябрь, Декабрь
[Год]	Резервные копии, созданные за год, будут храниться на отдельном наборе лент.	2017, 2018, ...

- Например, при указании правила [Имя ресурса]-[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 Понедельник для ленты 1, Вторник для ленты 2 и т. д. и указании [День недели] в параметрах резервного копирования надлежащая лента будет использована в соответствующий день недели.

6.10.27 Действия при сбое задания

Этот параметр определяет поведение программы при сбое запланированного плана защиты. Этот параметр не действует, 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**.

6.10.28 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.**

6.10.28.1 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.

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.

6.10.28.2 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.

6.10.29 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 программный поставщик 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.

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.

6.10.29.1 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.

6.10.30 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 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.

6.10.31 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**.

6.10.32 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**.

7 Восстановление

7.1 Восстановление: памятка

В таблице ниже кратко описаны доступные методы восстановления. С ее помощью вы сможете выбрать способ, который лучше всего отвечает вашим потребностям.

Объект восстановления	Метод восстановления
Физическая машина (Windows или Linux)	Использование веб-интерфейса Использование загрузочного носителя
Виртуальная машина (VMware или Hyper-V)	Использование веб-интерфейса Использование загрузочного носителя
Конфигурация ESXi	Использование загрузочного носителя
Файлы и папки	Использование веб-интерфейса Использование загрузочного носителя Извлечение файлов из локальных резервных копий
Базы данных SQL	Использование веб-интерфейса
Базы данных Exchange	Использование веб-интерфейса
Почтовые ящики Exchange	Использование веб-интерфейса
Почтовые ящики Office 365	Использование веб-интерфейса
Базы данных PostgreSQL	Использование веб-интерфейса
Базы данных Oracle	Использование инструмента Oracle Explorer

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. Чтобы загрузить файл, щелкните значок учетной записи в правом верхнем углу и выберите **Загрузки** > **Загрузочный носитель**.
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.
   - 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.

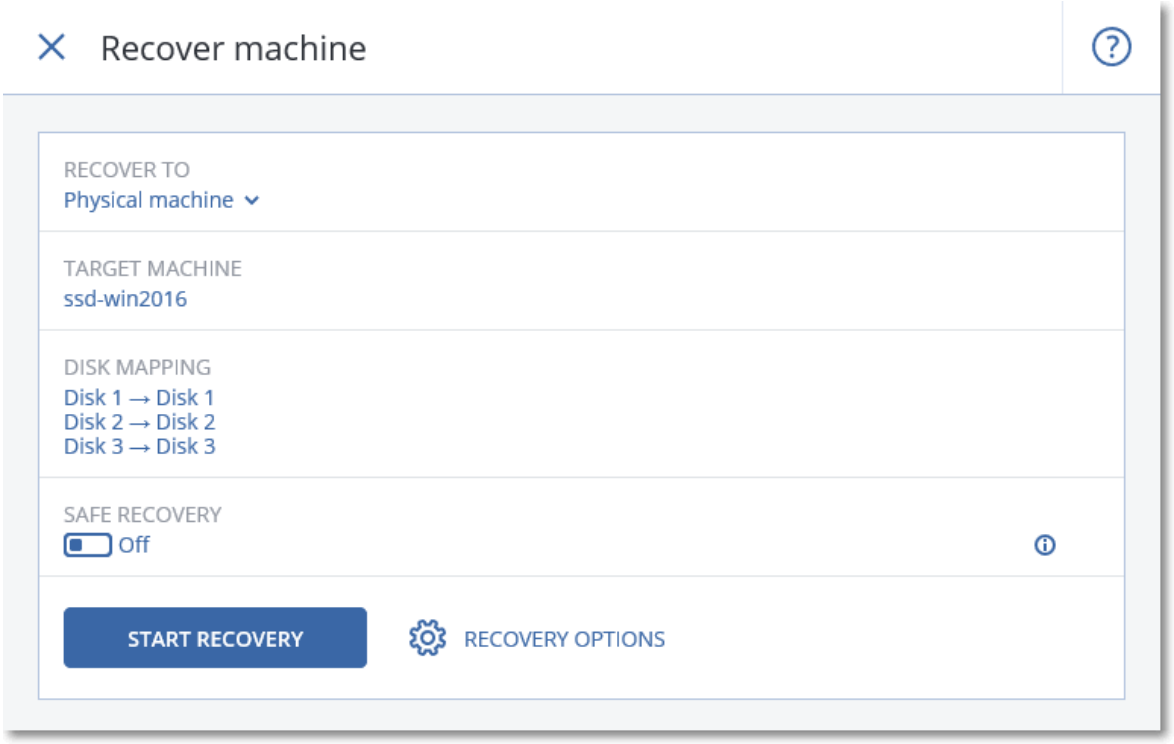
Для восстановления операционной системы потребуется перезагрузка. Вы можете перезапустить машину автоматически или присвоить ей статус **Требуется вмешательство**. Восстановленная операционная система автоматически запускается.

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 Хранилище резервных копий.
   - Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя».
4. Последовательно выберите пункты **Восстановление** > **Вся машина**.

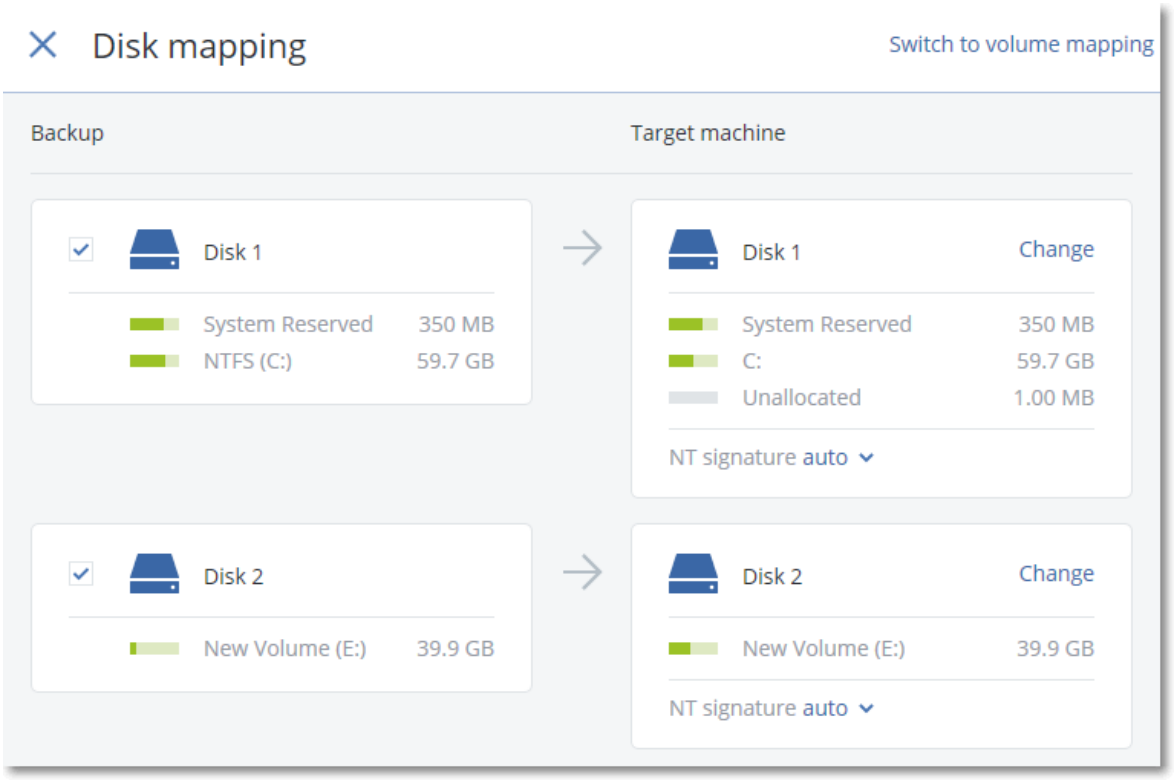
Программное обеспечение автоматически сопоставит диски из резервной копии с дисками целевой машины.

Чтобы выполнить восстановление в другую виртуальную машину, щелкните **Целевая машина** и выберите включенную целевую машину.



5. Если результат сопоставления вас не удовлетворяет или если выполнить сопоставление не удалось, нажмите **Сопоставление дисков**, чтобы сопоставить диски заново вручную.

   Раздел сопоставления также позволяет вам выбирать отдельные диски или тома для восстановления. Вы можете переключаться между восстановлением дисков и томов посредством ссылки **Переключиться на...** в верхнем правом углу.



6. Щелкните **Запуск восстановления**.
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 с использованием веб-интерфейса. Эту операцию можно выполнить, если установлен и зарегистрирован хотя бы один агент для VMware или агент для Hyper-V.

Для восстановления физической Linux-машины с логическими томами (LVM) в виртуальную см. раздел Миграция Linux-машины с логическими томами (LVM).

Дополнительную информацию о миграции P2V см. в разделе «Миграция машины».

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.

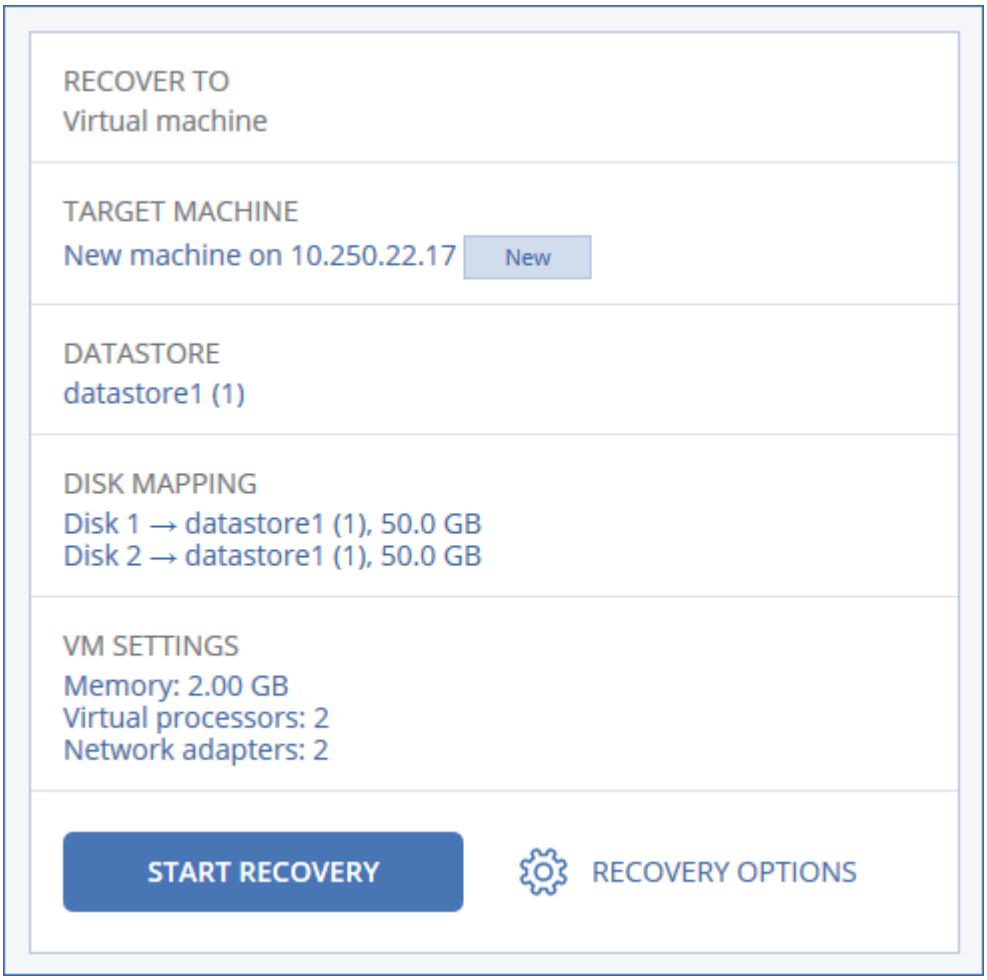
   Если машина отключена, точки восстановления не отображаются. Выполните любое из следующих действий:

   - Если резервная копия расположена в общем хранилище данных (т .е. другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите машину, которая подключена,

а затем выберите точку восстановления.

- Выберите точку восстановления на вкладке Хранилище резервных копий.
- Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя».

4. Последовательно выберите пункты **Восстановление** > **Вся машина**.
5. В поле **Восстановить в** выберите пункт **Виртуальная машина**.
6. Щелкните **Целевая машина**.
   a. Выберите гипервизор (**VMware ESXi** или **Hyper-V**).
      Должен быть установлен хотя один агент для VMware или агент для Hyper-V.
   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** для ESXi 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**.



8. Щелкните **Запуск восстановления**.
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 Хранилище 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.

   Если это имеет место, продолжите с шага 4 в разделе «Физическая машина». В противном случае рекомендуется выполнить миграцию V2P, используя загрузочный носитель.
4. Данное программное обеспечение автоматически выбирает исходную машину в качестве целевой.

   Чтобы выполнить восстановление на другую виртуальную машину, выберите **Целевая машина** и выполните следующие действия:

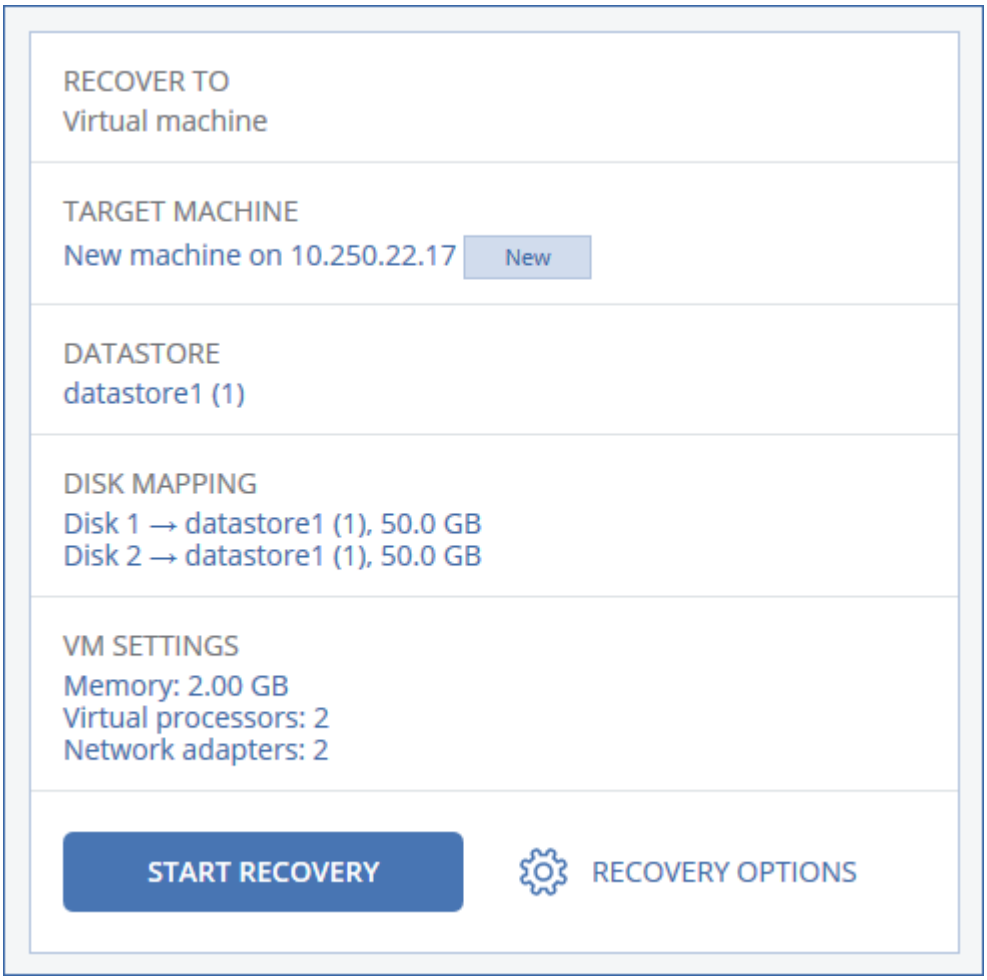
   a. Выберите гипервизор.

   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** для ESXi или **Путь** для Hyper-V, затем выберите хранилище данных для виртуальной машины.
   - Щелкните **Сопоставление дисков**, 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**.



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.
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 Universal Restore

Новейшие версии операционных систем сохраняют загружаемость при восстановлении на отличающееся оборудование или платформы VMware и Hyper-V. Если восстановленная операционная система не загружается, используйте средство Universal Restore, чтобы обновить драйверы и модули, необходимые для загрузки системы.

Universal Restore можно применить к операционным системам Windows и Linux.

Порядок использования Universal Restore

1. Загрузите машину с загрузочного носителя.
2. Щелкните **Применение Universal Restore**.
3. Если на машине несколько операционных систем, выберите, к какой из них следует применить Universal Restore.
4. [Только для Windows] Настройка дополнительных настроек.
5. Нажмите кнопку **OK**.

7.3.5.1 Universal Restore в Windows

Подготовка

Подготовьте драйверы

Прежде чем применять 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 компонент Universal Restore.

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 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**.
- Если драйверы находятся в сетевой папке или на загрузочном носителе, укажите путь к этой папке, нажав кнопку **Добавить папку**.

Кроме того, Universal Restore 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.

Universal Restore 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. Universal Restore выполняет также поиск драйвера сетевого адаптера. После его обнаружения Universal Restore передает путь к найденному драйверу операционной системе. Если на машине установлено несколько сетевых интерфейсных плат, Universal Restore 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.

Процесс Universal Restore

Указав требуемые настройки, нажмите кнопку **OK**.

Если Universal Restore 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 Universal Restore. 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.

После этого пользователь сможет настроить сетевое подключение и указать драйверы для видеоадаптера, USB и других устройств.

7.3.5.2 Universal Restore в Linux

Universal Restore может применяться к операционным системам Linux с версией ядра 3.0 или более поздней.

Если Universal Restore применяется к операционной системе Linux, обновляется временная файловая система, известная как начальный электронный диск (initrd). Это обеспечивает загрузку операционной системы на новом оборудовании.

Universal Restore добавляет к начальному электронному диску модули для нового оборудования (включая драйверы устройств). Обычно все необходимые модули обнаруживаются в папке **/lib/modules**. Если Universal Restore не может найти нужный модуль, имя файла модуля записывается в журнал.

Universal Restore может изменить конфигурацию загрузчика GRUB. Возможно, для этого потребуется обеспечить загружаемость системы, если структура томов новой машины отличается от исходной машины.

Universal Restore 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 Universal Restore сохраняет его копию в той же папке. Имя копии — это имя файла с прибавлением суффикса **_acronis_backup.img**. При запуске Universal Restore 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

1. Выберите машину, на которой ранее располагались данные, которые необходимо восстановить.
2. Щелкните **Восстановление**.

3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если выбрана физическая машина или машина в автономном режиме, то точки восстановления не отображаются. Выполните одно из следующих действий:

   - [Рекомендуется] 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 Хранилище резервных копий.
   - Использовать загрузочный носитель.
4. Последовательно выберите пункты **Восстановление** > **Файлы/папки**.
5. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов и папок.

   Можно использовать один или несколько подстановочных символов (* и ?). Подробную информацию об использовании подстановочных символов см. в разделе «Фильтры файлов».
6. Выберите файлы, которые необходимо восстановить.
7. Чтобы сохранить файлы как ZIP-файл, нажмите кнопку **Загрузить**, выберите расположение для сохранения данных и нажмите кнопку**Сохранить**. В противном случае пропустите этот шаг.

   Загрузка недоступна, если среди выбранных элементов есть папки или общий размер выбранных файлов превышает 100 МБ.
8. Нажмите кнопку **Восстановить**.

   В поле **Восстановить в** будет отображаться один из следующих вариантов:

   - Машина, на которой изначально были файлы, которые необходимо восстановить (если на этой машине установлен агент).
   - Машина, на которой установлен агент для VMware или агент для Hyper-V (если файлы изначально находятся на виртуальной машине ESXi или Hyper-V).

   Это целевая машина для восстановления. При необходимости можно выбрать другую машину.
9. В поле **Путь** выберите целевое место восстановления. Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:

   - Исходное расположение (при восстановлении на исходную машину)
   - Локальная папка на целевой машине

     Примечание
     Символьные ссылки не поддерживаются.
   - Сетевая папка, которая доступна с целевой машины.
10. Нажмите кнопку **Запуск восстановления**.
11. Выберите один из вариантов перезаписи файла:

    - **Перезаписывать существующие файлы**
    - **Перезаписывать существующий файл, если он старше**

- **Не перезаписывать существующие файлы**

Ход выполнения восстановления показан на вкладке **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.
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:
   <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 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	SQL и Excha

							машины	nge
	Windows	Linux	Загрузочный носитель	Windows	Linux	Загрузочный носитель	ESXi, Hyper-V	Windows
Проверка резервных копий	+	+	+	+	+	+	+	+
Режим загрузки	+	-	-	-	-	-	+	-
Дата и время для файлов	-	-	-	+	+	+	-	-
Обработка ошибок	+	+	+	+	+	+	+	+
Исключения файлов	-	-	-	+	+	+	-	-
Flashback	+	+	+	-	-	-	+	-
Восстановление полного пути	-	-	-	+	+	+	-	-
Точки подключения	-	-	-	+	-	-	-	-
Производительность	+	+	-	+	+	-	+	+
Команды до и после процедуры	+	+	-	+	+	-	+	+
Изменение идентификатора безопасности	+	-	-	-	-	-	-	-
Управление питанием ВМ	-	-	-	-	-	-	+	-
"Управление лентами" (стр. 274)	-	-	-	+	+	-	-	-

Журнал событий Windows	+	-	-	+	-	-	Только Hyper-V	+
Включить после восстановления	-	-	-	-	-	+	-	-

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**

  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 попытку

Значение по умолчанию: **Включено. Количество попыток: 30. Интервал между попытками: 30 секунд.**

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 технической поддержки 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. 227).

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.

7.6.7 Безопасность на уровне файлов

Этот параметр действует только при восстановлении файлов томов NTFS с диска и резервных копий на уровне файлов.

Этот параметр определяет, должны ли восстанавливаться разрешения NTFS вместе с файлами.

Значение по умолчанию: **Включено**.

Можно выбрать восстановление разрешений или наследование файлами их разрешений NTFS из 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**.

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

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.
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 8.1 и 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.

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. 262)).

7.6.17 Включить после восстановления

Этот параметр применим при работе с загрузочного носителя.

Значение по умолчанию: **Отключено**.

Этот параметр позволяет загрузить машину с восстановленной операционной системой без вмешательства пользователя.

8 Операции с резервными копиями

8.1 Вкладка «Хранилище резервных копий»

На вкладке **Хранилище 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 **Хранилище резервных копий**. Чтобы добавить другую папку (например, съемное USB-устройство) в список хранилищ резервных копий, щелкните **Обзор** и укажите путь к папке.

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 «Хранилище резервных копий»

1. На вкладке **Хранилище 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.

8.2 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.

8.2.1 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.

8.2.2 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

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 **Компьютер** (**Этот компьютер** в Windows 8.1 и более поздней версии).
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.

8.3 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 резервного копирования.

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 Хранилище 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 назначения экспорта.
8. Нажмите кнопку **Запустить**.

8.4 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 **Все устройства** 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 **Хранилище 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.

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. 159).

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.

9.1 Обработка данных 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.

Разграничение планов сканирования 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 настройка вынесенного агента.

Если вы используете узел хранения, установка вынесенного агента на ту же машину не имеет смысла.

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.

9.1.1 Репликация резервной копии

При применении плана репликации к резервной копии, разделенной на фиксированные фрагменты (см. раздел "Деление" (стр. 241)), реплицированная копия объединяется в общий архив.

9.1.1.1 Поддерживаемые расположения

В следующей таблице представлены хранилища резервных копий, поддерживаемые планами репликации резервных копий.

Хранилище резервных копий	Поддерживается в качестве источника	Поддерживается в качестве назначения
Локальная папка	+	+
Сетевая папка	+	+

Папка NFS	-	-
Зона безопасности	-	-
Сервер SFTP	-	-
Управляемое хранилище*	+	+
Ленточное устройство	-	+

* Проверьте ограничения, описанные в теме "Рекомендации для пользователей с лицензией Advanced" (стр. 209).

Порядок создания плана репликации резервных копий

1. Щелкните **Планы** > **Репликация резервных копий**.
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 выполнит репликацию.
   Можно выбрать любого агента, который имеет доступ к источнику и месту назначения хранилища резервной копии.
5. Щелкните **Элементы для репликации** и выберите резервные копии для репликации 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. Щелкните **Место назначения** и укажите место назначения.
7. [Дополнительно] В разделе **Порядок репликации** выберите резервные копии для репликации. Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:
   - **Все резервные копии** (по умолчанию)
   - **Только полные резервные копии**
   - **Только последнее резервное копирование**
8. [Дополнительно] Щелкните **Расписание**, а затем измените расписание.
9. [Необязательно] Щелкните **Правила хранения**, а затем укажите правила хранения для целевого расположения, как описано в разделе «Правила хранения».
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 щелкните значок шестеренки.
12. Нажмите кнопку **Создать**.

9.1.2 Проверка

Проверка это операция по определению возможности восстановления данных из резервной копии.

Проверка хранилища резервных копий проверяет все резервные копии, расположенные в хранилище.

9.1.2.1 Принципы работы

В планах проверки предусмотрено два метода проверки. Если выбрать оба метода, операции будут выполняться последовательно.

- **Вычисление контрольной суммы для каждого блока данных, сохраненных в резервной копии**
  Дополнительную информацию о проверке путем расчета 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. Чтобы использовать этот метод, необходимо иметь хост ESXi или Hyper-V и агент защиты (агент для VMware или агент для Hyper-V), который управляет этим хостом.
  Агент запускает виртуальную машину с резервной копии и подключается к VMware Tools или службе Hyper-V Heartbeat для проверки успешности запуска операционной системы. При сбое подключения агент пытается подключится каждые две минуты. Всего предпринимается пять попыток подключения. Если ни одна из попыток не будет успешной, проверка завершится сбоем.
  Независимо от количества планов проверки и проверенных резервных копий агент, который выполняет планы проверки, одновременно запускает одну виртуальную машину. Как только результат проверки становится известным, агент удаляет виртуальную машину и запускает следующую.

Если не удается выполнить проверку, можно просмотреть подробные сведения в разделе **Действия** на вкладке **Обзор**.

9.1.2.2 Поддерживаемые расположения

В следующей таблице представлены хранилища резервных копий, поддерживаемые планами проверки.

Хранилище резервных копий	Вычисление контрольной суммы	Запуск VM
Локальная папка	+	+
Сетевая папка	+	+
Папка NFS	-	-

Зона безопасности	-	-
Сервер SFTP	-	-
Управляемое хранилище	+	+
Ленточное устройство	+	-
Кибер Инфраструктура	+	+

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 нажмите на имя по умолчанию.
4. Щелкните **Агент**, а затем выберите агент, который выполнит проверку.

   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. Щелкните **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 на проверку. Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:
   - **Все резервные копии**
   - **Только последнее резервное копирование**
7. [Необязательно] Нажмите **Порядок проверки** и затем выберите любой из указанных ниже методов:
   - **Проверка контрольной суммы**

     Программное обеспечение вычислит контрольную сумму для каждого блока данных резервной копии.
   - **Запуск как виртуальной машины**

     Программное обеспечение запустит виртуальную машину из каждой резервной копии.
8. Если выбрать **Запуск как виртуальной машины**:
   a. Щелкните **Целевая машина** и выберите тип виртуальной машины (ESXi или Hyper-V), хост и шаблон имени машины.

      По умолчанию установлено имя **[Имя машины]_validate**.
   b. Нажмите **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для виртуальной машины.

c. [Необязательно] Измените режим распределения ресурсов диска.

   По умолчанию задана настройка **Экономное** для VMware ESXi и **Динамически расширяемое** для Hyper-V.

d. Чтобы получить правильный результат проверки, не выключайте **Сигнал пульса ВМ**. Этот переключатель предназначен для будущих выпусков.

e. [Необязательно] Щелкните **Настройки ВМ**, чтобы изменить размер памяти и сетевые подключения виртуальной машины.

   По умолчанию виртуальная машина *не* подключена к сети, а размер памяти виртуальной машины соответствует размеру памяти оригинальной машины.

9. [Дополнительно] Щелкните **Расписание**, а затем измените расписание.
10. Если резервные копии, выбранные в разделе **Элементы для проверки**, защищены паролем, включите переключатель **Пароль резервной копии** и укажите пароль. В противном случае пропустите этот шаг.
11. [Дополнительно] Для изменения параметров плана щелкните значок шестеренки.
12. Нажмите кнопку **Создать**.

9.1.3 Очистка

Очистка – это операция, которая удаляет устаревшие резервные копии в соответствии с правилами хранения.

9.1.3.1 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».
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**.

9.1.4 Преобразование в виртуальную машину

Можно создать отдельный план для преобразования 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.

   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**.

10 Загрузочный носитель

Внимание
Некоторые из функций, описанные в этом разделе, доступны только для локальных развертываний.

10.1 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.

10.2 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 Universal Restore. Вы не 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 в локальном развертывании, 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.

10.3 Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE?

10.3.1 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.

10.3.2 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:

- 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 назначения резервной копии оптический носитель, например CD, DVD или диск Blu-ray (BD).

10.4 Мастер создания загрузочных носителей

Мастер создания загрузочных носителей – это специальное средство для создания загрузочных носителей. Он доступен только для локальных развертываний.

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.

10.4.1 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 в локальном развертывании, необходимо будет создать собственный загрузочный носитель, используя для этого мастер создания загрузочных носителей.

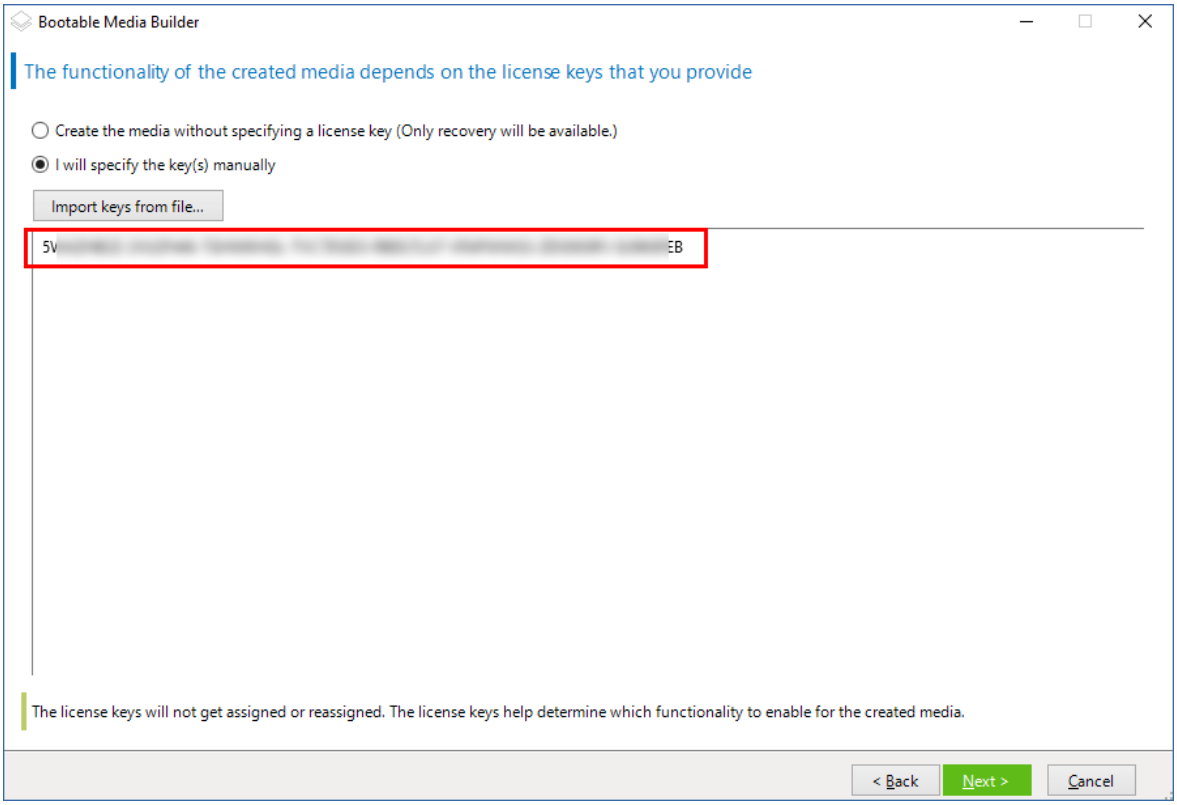
10.4.2 32- или 64-разрядная версия

Мастер создания загрузочных носителей позволяет создавать носители как с 32-разрядными, так и 64-разрядными компонентами. В большинстве случаев для загрузки машины, которая использует интерфейс UEFI, требуется 64-разрядный носитель.

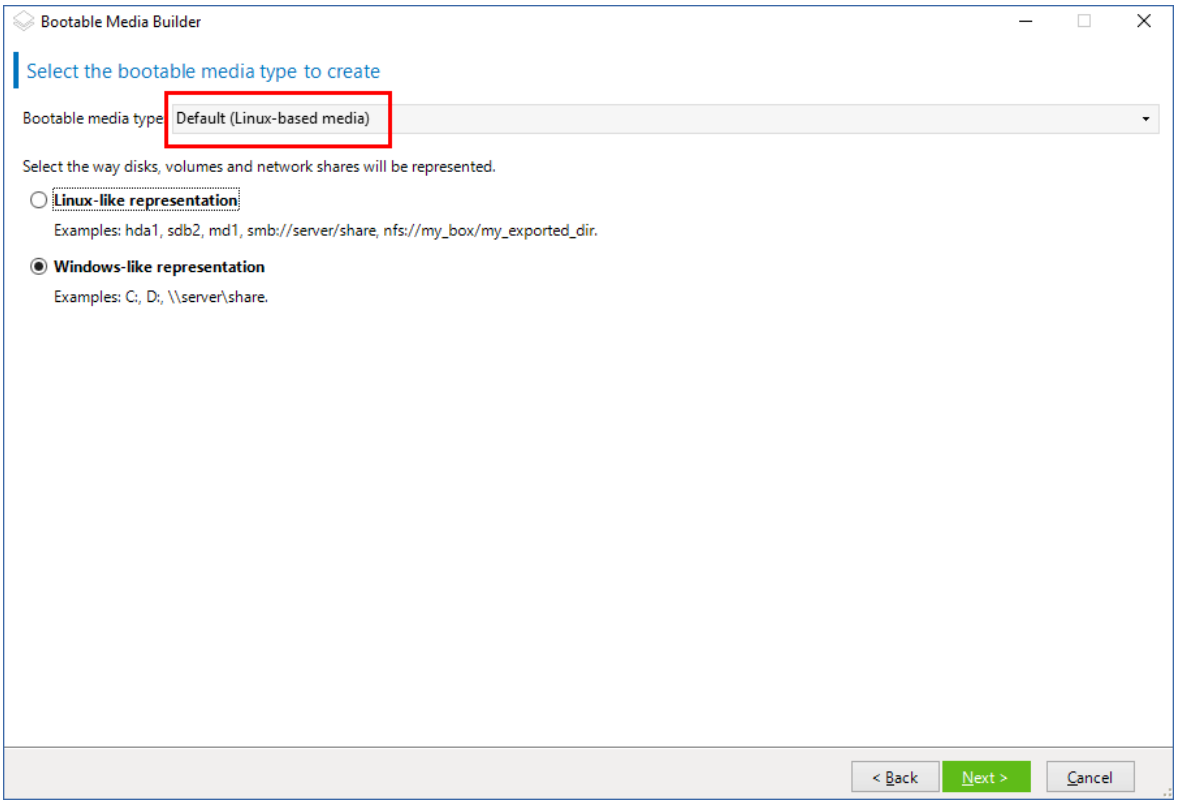
10.4.3 Загрузочные носители на основе Linux

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 Universal Restore.



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).



4. [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**

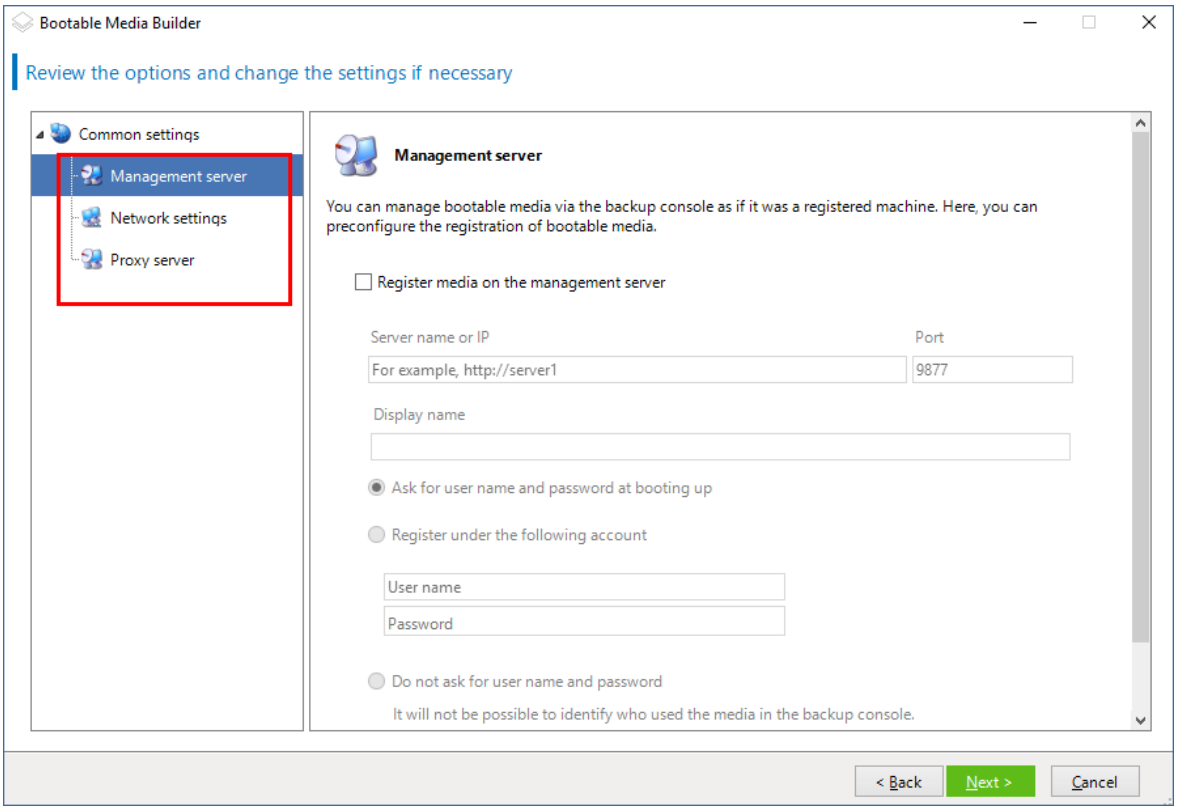
   Дополнительную информацию о доступных параметрах см. в разделе Параметры ядра.
5. [Дополнительно] Выберите язык, который будет использоваться в загрузочном носителе.
6. Выберите компоненты, которые будут размещены на носителе: загрузочный агент Кибер Бэкап и (или) Universal Restore, если вы планируете восстанавливать систему на отличающееся оборудование.

   Загрузочный агент позволяет выполнить операции резервного копирования, восстановления и управления дисками на любом ПК-совместимом оборудовании, включая "голое железо".

   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.
7. [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.

8. [Необязательно] Чтобы автоматизировать операции загрузочного агента, установите флажок **Использовать следующий сценарий**. Затем выберите один из сценариев и задайте его параметры.
9. [Необязательно] Выберите способ регистрации носителя на сервере управления при загрузке. Дополнительную информацию о настройках регистрации см. в разделе Сервер управления.



10. [Необязательно] Укажите сетевые настройки: настройки TCP/IP для назначения сетевым адаптерам машины.
11. [Необязательно] Укажите сетевой порт: TCP-порт, который прослушивается загрузочным агентом для приема входящих подключений.
12. [Необязательно] Если в сети включен прокси-сервер, укажите его имя хоста или IP-адрес и порт.
13. 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.
14. [Необязательно] Добавьте системные драйверы Windows для использования компонентом Universal Restore. Это окно отображается в том случае, если компонент Universal Restore добавлен на носитель и выбран носитель, отличный от WDS и RIS.
15. При необходимости укажите имя хоста или IP-адрес и учетные данные для WDS или RIS либо путь к ISO-файлу носителя.

16. Проверьте настройки в итоговом окне и щелкните **Приступить**.

10.4.3.1 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

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.

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.

10.4.3.2 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**);
- 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 **Хранилище 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.

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.

10.4.4 Объект высшего уровня

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).

10.4.5 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,	Нет	Значение по умолчанию элемента управления. Если пара не указана, значением по умолчанию

	multiString, password или enum число, еслитуре является number, spinner или checkbox		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).
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.

10.4.6 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.
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",
                "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
        }
    }
}
```

10.4.6.1 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 хранятся 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.

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.
   - **Не спрашивайте имя пользователя и пароль**

     Если анонимная регистрация на сервере управления не отключена, машина регистрируется анонимно.

На вкладке **Действия** веб-консоли Кибер Бэкап не отображаются пользователи, которые использовали носитель.

На веб-консоли Кибер Бэкап носитель будет доступен в разделе организации.

В интерфейсе загрузочного носителя будет возможно изменить имя пользователя и пароль, перейдя по пути **Инструменты** > **Зарегистрировать носитель на сервере управления**.

10.4.6.2 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,
- 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.

10.4.6.3 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.

- Порт по умолчанию
- Текущий используемый порт
- Новый порт (введите номер порта)

Если порт не был предварительно настроен, агент использует порт 9876.

10.4.6.4 Драйверы для Universal Restore

При создании загрузочного носителя есть возможность добавить на него драйверы Windows. Эти драйверы будут использоваться компонентом Universal Restore для загрузки системы Windows, перенесенной на отличающееся оборудование.

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 операции 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

1. Выберите INF-файл.
2. Нажмите кнопку **Удалить**.

10.4.7 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 пакета Windows AIK или комплекта средств для развертывания и оценки Windows (ADK).

10.4.7.1 PE-образы на основе WinRE

Создание образов на основе WinRE поддерживается для следующих операционных систем:

- Windows 7 (64-разрядная версия)
- Windows 8, 8.1, 10 (32-разрядная и 64-разрядная версии)
- Windows Server 2012, 2016, 2019 (64-разрядная версия)

10.4.7.2 PE-образы

После установки пакета Windows AIK или комплекта средств для развертывания и оценки Windows (ADK), мастер создания загрузочных носителей поддерживает дистрибутивы WinPE, основанные на любом из следующих ядер:

- Windows 7 (PE 3.0) с дополнением для Windows 7 SP1 (PE 3.1) или без него
- Windows 8 (PE 4.0)

- Windows 8.1 (PE 5.0)
- Windows 10 (PE для Windows 10)

Мастер создания загрузочных носителей поддерживает как 32-разрядные, так и 64-разрядные дистрибутивы WinPE. 32-разрядные дистрибутивы WinPE могут работать и на 64-разрядном оборудовании. Однако 64-разрядный дистрибутив требуется для загрузки машины, которая использует интерфейс UEFI.

Для работы образов среды предустановки на основе WinPE 4 (и более поздних версий) требуется около 1 ГБ ОЗУ.

Примечание
Функции управления дисками недоступны для загрузочных носителей на основе Windows PE 4.0 и более поздних версий. Поэтому управление дисками поддерживается для Windows 7 и операционных систем более ранних версий. Для выполнения операций управления дисками в ОС Windows 8 и более поздних версий необходимо установить Управление Дисками.

10.4.7.3 Подготовка WinPE 2.x и 3.x

Для создания или изменения образов PE 2.x или 3.x необходимо установить мастер создания загрузочных носителей на машину, на которую установлен пакет автоматической установки Windows (AIK). Если у вас нет машины с AIK, подготовьте ее следующим образом.

Как подготовить машину с AIK

1. Загрузите и установите пакет Windows AIK.
   Набор средств автоматизированной установки (AIK) для Windows 7 (PE 3.0):
   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=ru
   Набор средств автоматизированной установки (AIK) для Windows 7 SP1 (PE 3.1):
   http://www.microsoft.com/download/en/details.aspx?id=5188
   Системные требования для установки приведены по указанным выше ссылкам.
2. [Необязательно] Запишите WAIK на DVD или скопируйте на флэш-накопитель.
3. Установите платформу Microsoft .NET Framework из этого пакета (NETFXx86 или NETFXx64 в зависимости от оборудования).
4. Установите средство синтаксического анализа Microsoft Core XML (MSXML) 5.0 или 6.0 из этого набора.
5. Установите пакет Windows AIK из этого набора.
6. Установите мастер создания загрузочных носителей на этой же машине.

Рекомендуется ознакомиться со справкой, идущей в комплекте с пакетом Windows AIK. Чтобы открыть документацию, в меню «Пуск» выберите **Microsoft Windows AIK > Документация**.

10.4.7.4 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 развертывания и оценки Windows (ADK). Если у вас нет машины с ADK, подготовьте ее следующим образом.

Как подготовить машину с ADK

1. Загрузите программу установки комплекта средств для развертывания и оценки (ADK).

   Комплект средств для развертывания и оценки Windows (ADK) для Windows 8 (PE 4.0): http://www.microsoft.com/en-us/download/details.aspx?id=30652.

   Комплект средств для развертывания и оценки Windows (ADK) для Windows 8.1 (PE 5.0): http://www.microsoft.com/ru-ru/download/details.aspx?id=39982.

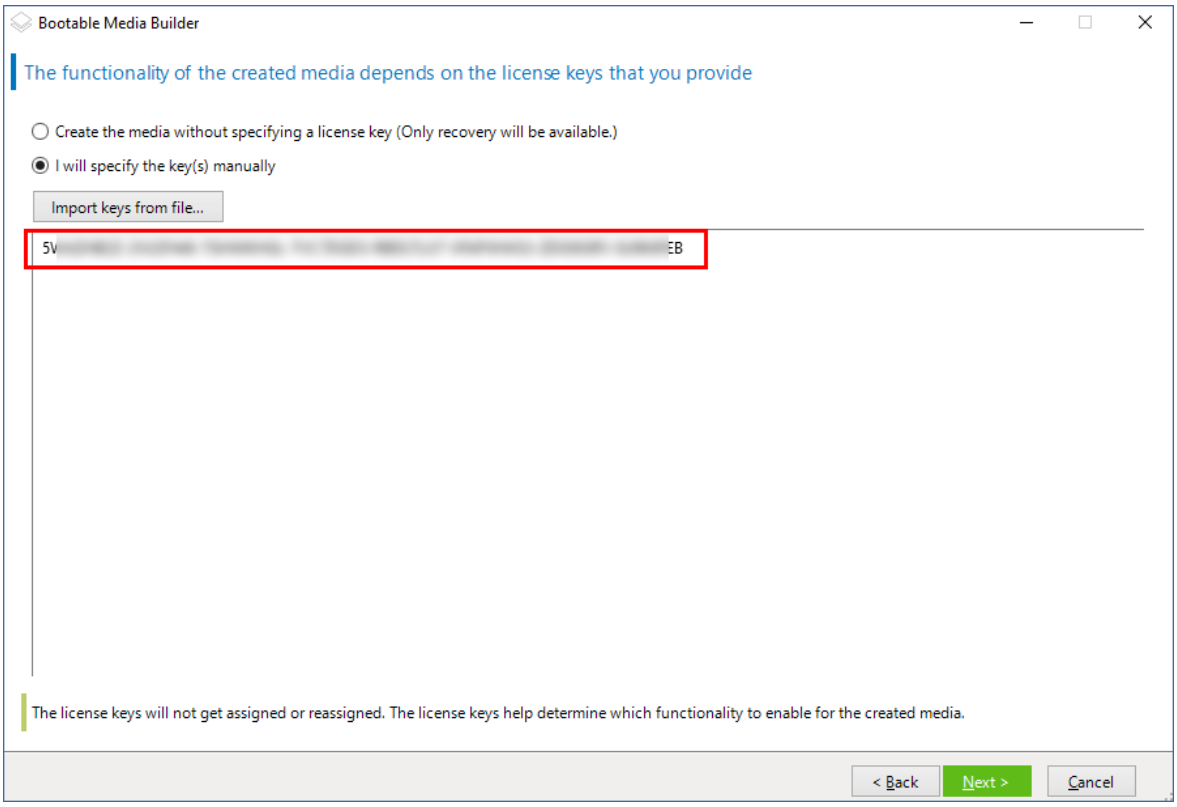
   Комплект средств для развертывания и оценки Windows (ADK) для Windows 10 (PE для Windows 10): https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx.

   Системные требования для установки приведены по указанным выше ссылкам.
2. Установите комплект ADK на машине.
3. Установите мастер создания загрузочных носителей на этой же машине.

10.4.7.5 Добавление подключаемого модуля Киберпротект к WinPE

Порядок добавление 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 Universal Restore.



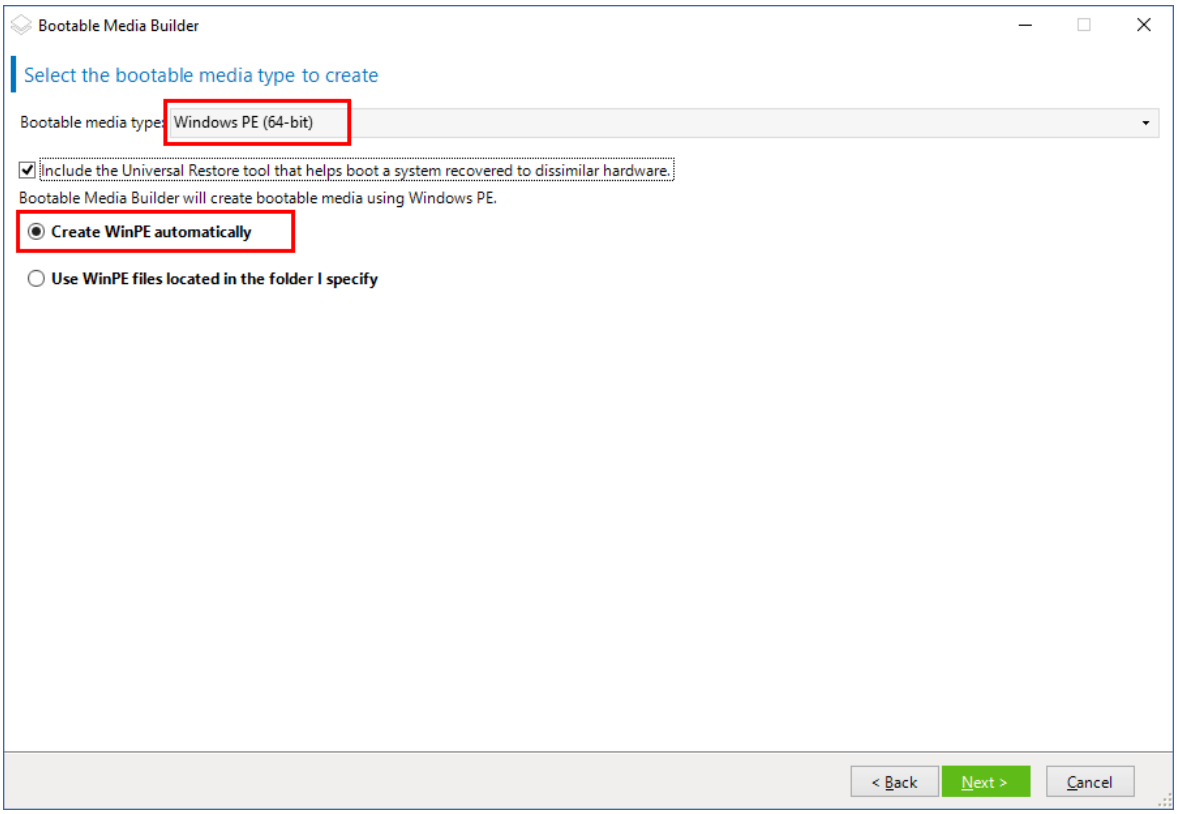
3. Выберите **Тип загрузочного носителя: Windows PE** или **Тип загрузочного носителя: Windows PE (64-разрядный)**. 64-разрядный носитель требуется для загрузки машины, которая использует интерфейс UEFI.

   Если выбран вариант **Тип загрузочного носителя: Windows PE**, сначала выполните указанные ниже действия.

   - Выберите **Загрузить подключаемый модуль для WinPE (32-разрядный)**.
     Для загрузки модуля выполните одно из следующих действий:
     - Перейдите на страницу загрузки и выберите **Плагин Windows PE** для вашей версии Кибер Бэкап.
     - В веб-консоли щелкните значок профиля (в правом верхнем углу), затем нажмите **Загрузки** и далее выберите **Плагин для Win PE (32-bit)**.
   - Сохраните подключаемый модуль в папке **%PROGRAM_ FILES%\Acronis\BootableComponents\WinPE32**.

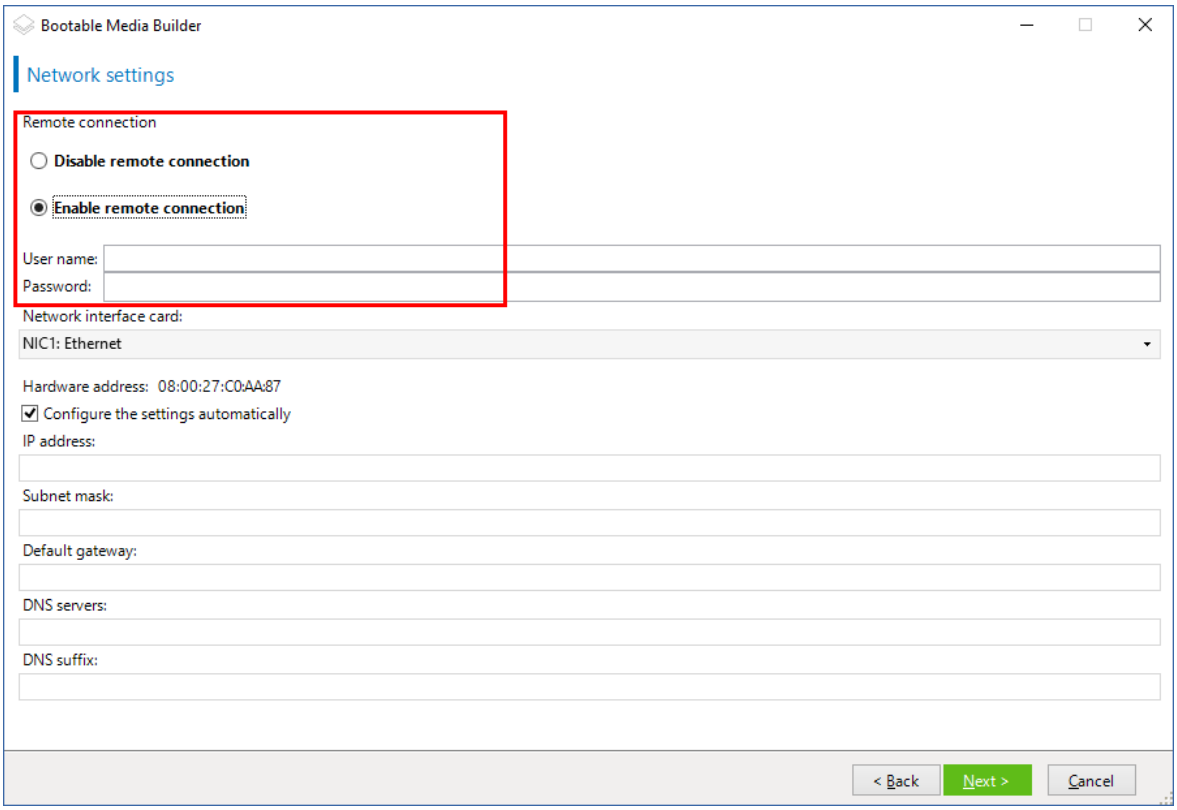
   Если планируется восстановить операционную систему на компьютере с другим оборудованием или на виртуальной машине и необходимо обеспечить загружаемость системы, установите флажок **Включить средство Universal Restore...**
4. Выберите пункт **Создать WinPE автоматически**.

   Программа запускает соответствующий сценарий и переходит к следующему окну.



5. Выберите язык, который будет использоваться в загрузочном носителе.
6. Выберите, разрешить или запретить удаленное 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 удаленное подключение через интерфейс командной строки можно будет выполнить без ввода учетных данных.

   Эти учетные данные также необходимы при регистрации носителя на сервере управления с веб-консоли Кибер Бэкап.



[Необязательно] Выберите

7. Укажите сетевые настройки для сетевых адаптеров машины или выберите автоконфигурацию DHC.
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. Добавьте 32-разрядные драйверы, если вы используете 32-разрядный дистрибутив WinPE, или 64-разрядные драйверы, если вы используете 64-разрядный дистрибутив WinPE.

   Кроме того, можно будет указать добавленные драйверы при настройке компонента Universal Restore для Windows. Для использования Universal Restore добавьте 32-разрядные или 64-разрядные драйверы в зависимости от того, какую ОС Windows вы планируете восстанавливать – 32-разрядную или 64-разрядную.

   Как добавить драйверы

   - Щелкните **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 щелкните **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.

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.

Дополнительные сведения о настройке среды предустановки Windows PE 2.x и 3.x см. в руководстве пользователя для этой среды (Winpe.chm). Сведения о настройке среды Windows PE 4.0 и более поздних версий доступны в библиотеке Microsoft TechNet.

10.5 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.

10.5.1 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.

10.5.1.1 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.

Если требуется удалить VLAN, щелкните соответствующую сеть VLAN и нажмите кнопку **Удалить VLAN**.

10.5.2 Локальное подключение

Для непосредственной работы на машине, загружаемой с носителя, щелкните **Локальное управление этой машиной** в окне загрузки.

10.5.3 Удаленное подключение

Для удаленного подключения к носителю зарегистрируйте его на сервере управления, как описано в разделе «Регистрация носителя на сервере управления».

10.6 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, Восстановление 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.

10.6.1 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**.
3. В поле **Зарегистрировать в** 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. В полях **Имя пользователя** и **Пароль** введите учетные данные учетной записи, которая 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.
5. 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.
6. Нажмите кнопку **OK**.

10.7 Операции с загрузочным носителем

Операции с загрузочным носителем подобны операциям резервного копирования и восстановления, которые выполняются при запущенной операционной системе. Отличие 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 назначения 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.

10.7.1 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**.

10.7.2 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 диски или раздел по его размеру или метке.

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.

10.7.3 Восстановление

Операция восстановления доступна как на загрузочных носителях, созданных с помощью мастера создания загрузочных носителей, так и на скачанные 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.
10. [Необязательно] Настройте параметры восстановления.
11. Проверьте правильность настроек и нажмите кнопку **OK**.

Примечание
Для восстановления данных на отличающееся оборудование необходимо использовать Киберпротект Universal Restore. Компонент Киберпротект Universal Restore недоступен, если резервная копия находится в Зоне безопасности.

10.7.4 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
Функции управления дисками недоступны для загрузочных носителей на основе Windows PE 4.0 и более поздних версий. Поэтому управление дисками поддерживается для Windows 7 и операционных систем более ранних версий. Для выполнения операций управления дисками в ОС Windows 8 и более поздних версий необходимо установить Управление Дисками.

Порядок выполнения операций управления дисками

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.

10.7.4.1 Поддержка файловых систем

Загрузочный носитель поддерживает управление диском со следующими файловыми системами:

- FAT 16/32,
- NTFS.

10.7.4.2 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.

10.7.4.3 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.

10.7.4.4 Операции с дисками

Используя загрузочный носитель, можно выполнить следующие операции управления диском:

- 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 будут 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.

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, будут 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.

   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 будут отменена.
9. Если выбран вариант, предусматривающий копирование NT-подписи, подождите, пока выполнится операция и перезагрузится компьютер, а затем отключите жесткий диск источника или жесткий диск назначения 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 будут 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. ПреобразованиеMBR-диска из динамического в базовый с помощью операции **Преобразовать в базовый**.
2. Преобразование базовых дисков MBR в GPT с помощью операции **Преобразовать в GPT**.
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 будут 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.

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, операций 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;
- в мультизагрузочных системах – загружаемость системы, которая была **отключена от сети** во время операции.

10.7.4.5 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

10.7.5 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.

10.7.6 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.

10.7.7 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.

10.7.8 Зеркальный том

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.

10.7.9 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.

10.7.10 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
   - 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 диски назначения.
   - Для основного тома укажите нераспределенное пространство на выбранном диске.
   - Для простого/составного тома выберите один или несколько дисков назначения.
   - Для зеркального тома выберите два целевых диска.
   - Для составного тома выберите два или более дисков назначения.
   - 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 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 будут 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 будут 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 будут 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.

   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 операцию 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 будут 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 будут 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 будут отменена.

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 будут отменена.

10.7.10.1 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**.

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.

10.8 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 кладку **Обнаружение**.
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.

10.9 Восстановление при загрузке

Восстановление 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.

Восстановление 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 Восстановление при загрузке можно «на ходу» выполнять резервное копирование.

На машинах с установленным загрузчиком GRUB пользователь не нажимает клавишу F11, а выбирает Startup Recovery Manager в меню загрузки.

10.9.1 Активация Восстановление при загрузке

На машине, где запущен агент для Windows или агент для Linux, Восстановление при загрузке можно активировать с помощью веб-консоли Кибер Бэкап.

Порядок активации Восстановление при загрузке на веб-консоли Кибер Бэкап

1. Выберите машину, на которой нужно активировать Восстановление при загрузке.
2. Нажмите **Сведения**.
3. Включите переключатель **Восстановление при загрузке** .
4. Дождитесь, пока программа активирует Восстановление при загрузке.

Порядок активации Восстановление при загрузке на машине без агента

1. Загрузите машину с загрузочного носителя.
2. Щелкните **Инструменты** > **Активировать Восстановление при загрузке** .
3. Дождитесь, пока программа активирует Восстановление при загрузке.

10.9.2 Что происходит при активации Восстановление при загрузке

Активация включает при загрузке подсказку «Press F11 for Startup Recovery Manager...» (при отсутствии загрузчика GRUB) или добавляет пункт «Восстановление при загрузке» в меню загрузчика GRUB (при его наличии).

Примечание
Для активации Восстановление 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 Восстановление 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 Восстановление при загрузке. В противном случае измените конфигурацию этого загрузчика вручную после активации.

10.9.3 Деактивация Восстановление 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).

10.10 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.

Ограничение:

PXE-сервер Киберпротект не поддерживает загрузчик UEFI.

10.10.1 Установка PXE-сервера

Порядок установки PXE-сервера

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щелкните **Язык установки**.
3. Примите условия лицензионного соглашения.
4. Щелкните **Настройка параметров установки**.
5. Рядом с пунктом **Устанавливаемые компоненты** щелкните **Изменить**.
6. Установите флажок **PXE Server**. Если на этой машине не нужно устанавливать другие компоненты, снимите соответствующие флажки. Чтобы продолжить, нажмите кнопку **Готово**.
7. [Необязательно] Измените другие настройки установки.

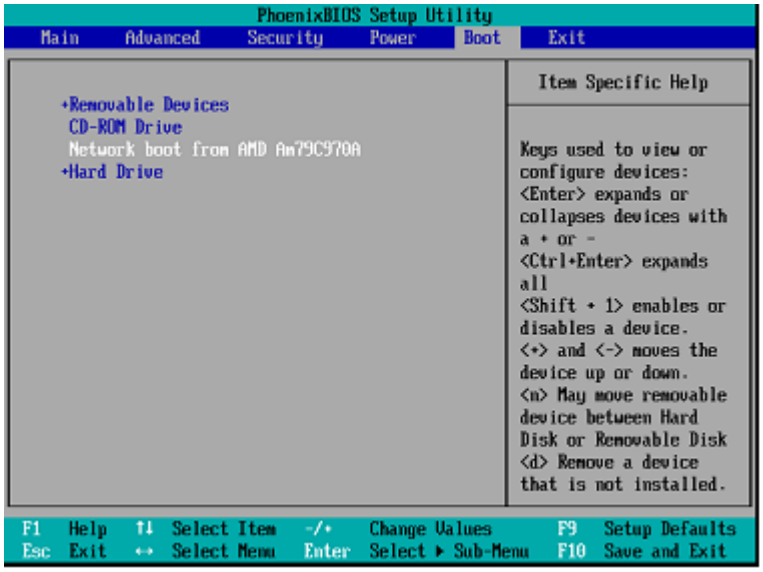
8. Нажмите **Установить**, чтобы продолжить установку.
9. После завершения установки нажмите кнопку **Закрыть**.

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.

10.10.2 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.

10.10.3 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.

11 Защита приложений Microsoft

Внимание
Некоторые из функций, описанные в этом разделе, доступны только для локальных развертываний.

11.1 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 или на Microsoft Office 365. Резервное копирование почтовых ящиков поддерживается для Microsoft Exchange Server 2013 и более поздних версий.

11.2 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.

11.3 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.

11.4 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 или Office 365*	Вся машина Базы данных в запущенный Exchange Базы данных как файлы Фрагментарное восстановление в запущенный Exchange или Office 365*	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	-

* Фрагментарное восстановление также доступно из резервной копии почтового ящика.

11.5 Предварительные требования

Перед настройкой резервного копирования приложений убедитесь, что перечисленные ниже требования выполнены.

Чтобы проверить состояние модуля записи VSS, используйте команду vssadmin list writers.

11.5.1 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. Если используется Exchange 2010 или более поздней версии, то оболочка Windows PowerShell должна иметь по крайней мере версию 2.0.
- Установлена платформа Microsoft .NET Framework.

  Если используется Exchange 2007, то Microsoft .NET Framework должна иметь по крайней мере версию 2.0.

  Если используется Exchange 2010 или более поздней версии, то Microsoft .NET Framework должна иметь по крайней мере версию 3.5.
- 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.

11.5.2 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 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.

11.5.2.1 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).

11.5.2.2 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.
- Для Hyper-V 2008 R2: в качестве гостевой операционной системы используется Windows Server 2008 R2 или 2012.
- 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 и более поздних версий: виртуальная машина не имеет контрольных точек.
  - Для Hyper-V 2012 и более поздних версий: виртуальная машина имеет контроллер SCSI (проверьте **Настройки** > **Оборудования**).

11.6 Резервное копирование базы данных

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.

11.6.1 Выбор баз данных SQL

Резервная копия базы данных SQL 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 SQL. Усечение журнала SQL можно отключить в параметрах плана защиты.

Порядок выбора баз данных SQL

1. Нажмите **Устройства** > **Microsoft SQL**.

   /Программное обеспечение отобразит дерево групп Always On Availability Groups (AAG) сервера 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 AAGs, машины, на которых запущен 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 которых запущен 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 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.

11.6.2 Выбор данных Exchange Server

В таблице ниже приведены основные сведения о том, какие именно данные Microsoft Exchange Server можно выбрать для резервного копирования, а также о минимальных правах пользователя, которые для этого необходимы.

Версия Exchange	Элементы данных	Права пользователя
2007	Группы хранения	Участие в группе ролей **Администраторы организации Exchange**
2010/2013/2016/2019	Базы данных, Группы обеспечения доступности баз данных (DAG)	Участие в группе ролей **Управление сервером**.

При полном резервном копировании в копию включаются все выбранные данные Exchange Server.

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 Server

1. Нажмите **Устройства** > **Microsoft Exchange**.

   Программное обеспечение отобразит дерево групп обеспечения доступности баз данных (DAG) Exchange Server, машины, на которых запущен Microsoft Exchange Server, и базы данных Exchange Server. 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 которых запущен сервер Microsoft Exchange, будет создана резервная копия всех баз данных, подключенных к серверу Exchange.
   - 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**.

11.6.3 Защита группы Always On Availability Groups (AAG)

11.6.3.1 Обзор решений для SQL Server высокой доступности

Функция отказоустойчивой кластеризации Windows Server (WSFC) позволяет настроить SQL-сервер с высоким уровнем доступности посредством избыточности на уровне экземпляра (экземпляр отказоустойчивого кластера, FCI) или на уровне базы данных (AlwaysOn Availability Group, AAG). Оба метода можно сочетать.

В экземпляре отказоустойчивого кластера базы данных SQL 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.

11.6.3.2 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.

11.6.3.3 Сколько требуется агентов для резервного копирования и восстановления данных кластера?

Для успешного резервного копирования и восстановления данных кластера необходимо установить агент для SQL на каждом узле кластера WSFC.

11.6.3.4 В AAG включено резервное копирование баз данных

1. Установите агент для SQL 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 SQL на остальных узлах выберите AAG, нажмите **Сведения**, после чего нажмите **Установить агент** возле каждого узла.

2. Выберите AAG или набор баз данных для создания резервной копии в соответствии с инструкциями Выбор баз данных SQL.

   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».

11.6.3.5 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 "Хранилище 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 SQL» (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 исключить целевую базу данных из AAG перед восстановлением. Либо можно просто восстановить базу данных как новую базу, не входящую в AAG. После завершения восстановления можно воссоздать исходную конфигурацию AAG.

11.6.4 Защита групп обеспечения доступности базы данных (DAG)

11.6.4.1 Обзор кластеров Exchange Server

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 или групп хранения 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.

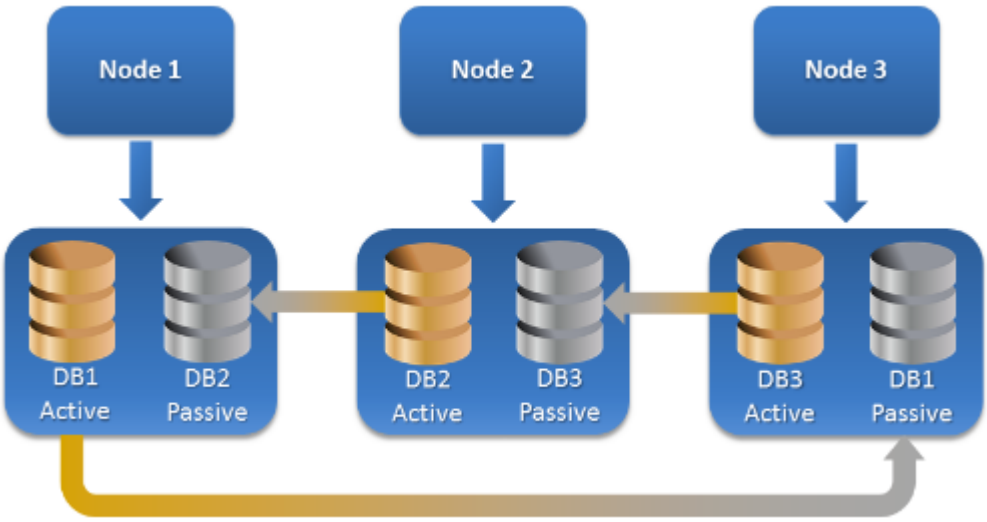
11.6.4.2 Резервное копирование с поддержкой кластеров

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.

11.6.4.3 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.

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.



11.6.4.4 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.

11.6.4.5 Создание резервной копии данных кластера Exchange

1. При создании плана защиты выберите DAG в соответствии с инструкциями в разделе "Выбор данных 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.

11.6.4.6 Восстановление данных кластера Exchange

1. Выберите точку восстановления для базы данных, которую необходимо восстановить. Резервное копирование всего кластера для восстановления невозможно.

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 "Хранилище 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.

11.7 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 приложений** для дополнительной защиты данных этих приложений.

11.7.1 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 восстановления 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.

11.7.2 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 **Хранилище резервных копий**, а затем выберите эту машину в списке **Машина для обзора**.

Другие требования перечислены в разделах «Предварительные требования» и «Необходимые права пользователя».

11.7.3 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 Exchange Server:
  Exchange 2007: Данная учетная запись должна входить в группу **Администраторы** на данной машине, а также в группу ролей **Администраторы организации Exchange**.
  Exchange 2010 и более поздней версии: Данная учетная запись должна входить в группу **Администраторы** на данной машине, а также в группу ролей **Управление организацией**.
- 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).

11.8 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**.

В результате почтовый ящик будет находиться по пути **Устройства** > **Microsoft Exchange** > **Почтовые ящики**.

11.8.1 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**.

11.8.2 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.

Минимальные требуемые права пользователя:

- Учетная запись должна входить в группы ролей **Управление сервером** и **Управление получателями**.
- Для учетной записи должна быть включена роль управления **ApplicationImpersonation** для всех пользователей или групп пользователей, к почтовым ящикам которых будет обращаться агент.
  Информацию о настройке роли управления **ApplicationImpersonation** см. в следующей статье базы знаний Microsoft: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

11.9 Восстановление баз данных SQL

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

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 Хранилище 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 незафиксированных транзакций восстановленной базы данных, хранящихся в журналах транзакций. Вы не сможете восстановить дополнительные журналы транзакций из резервных копий в собственном формате Microsoft SQL.

   - **Не работает (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.

   - **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 Хранилище 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 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**.

11.9.1 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».

11.9.1.1 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.

11.9.2 Подключение баз данных SQL Server

В этом разделе описывается процедура подключения базы данных в SQL Server с помощью среды SQL Server Management Studio. Одновременно может быть подключена только одна база данных.

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 Microsoft SQL Server Management Studio.
2. Подключитесь к требуемому экземпляру 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 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 SQL Server из резервной копии.
7. Когда все файлы будут найдены, нажмите кнопку **OK**.

11.10 Восстановление баз данных Exchange

В этом разделе описано восстановление из резервных копий базы данных и резервных копий с поддержкой приложений.

Можно восстановить данные Exchange Server в работающий Exchange Server. Это может быть исходный Exchange Server или Exchange Server 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 Server можно выбрать для восстановления, а также о минимальных правах пользователя, которые для этого необходимы.

Версия Exchange	Элементы данных	Права пользователя
2007	Группы хранения	Участие в группе ролей **Администраторы организации Exchange**.
2010/2013/2016/2019	Базы данных	Участие в группе ролей **Управление сервером**.

Базы данных (группы хранения) 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 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).

В нижеуказанной процедуре как базы данных, так и группы хранения описываются термином «базы данных».

Для восстановления баз данных Exchange на запущенный сервер Exchange Server

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 Хранилище 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 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 Хранилище 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**.

11.10.1 Подключение баз данных 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 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 Server и локальную группу администраторов для данного целевого сервера.

Подробную информацию о том, как подключить базы данных, см. в следующих статьях:

- Для Exchange 2010 (или более поздней версии): http://technet.microsoft.com/en-us/library/aa998871.aspx
- Для Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

11.11 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 или на Microsoft Office 365.

Можно восстановить следующие элементы:

- почтовые ящики (за исключением архивированных почтовых ящиков);
- общие папки;
- элементы общих папок;
- папки электронной почты;

- сообщения электронной почты;
- события календаря;
- задания;
- контакты;
- записи журнала;
- Примечание

Чтобы найти эти элементы, можно воспользоваться поиском.

11.11.1 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.

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.

11.11.1.1 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.

11.11.2 Восстановить в Office 365

Восстановление можно выполнить из резервных копий Microsoft Exchange Server 2013 и более поздних версий.

Если почтовый ящик восстанавливается в существующий почтовый ящик Office 365, существующие элементы не затрагиваются, а восстановленные элементы помещаются рядом с ними.

При восстановлении одного почтового ящика необходимо выбрать целевой ящик Office 365. При восстановлении нескольких почтовых ящиков в рамках одной операции восстановления программное обеспечение попытается восстановить каждый почтовый ящик в почтовый ящик пользователя с таким же именем. Если пользователь не найден, почтовый ящик пропускается. Если некоторые почтовые ящики будут пропущены, восстановление продолжится с предупреждением. Если все почтовые ящики будут пропущены, восстановление завершится сбоем.

Дополнительную информацию о восстановлении Office 365 см. в разделе «Защита почтовых ящиков Office 365».

11.11.3 Восстановление почтовых ящиков

Порядок восстановления почтовых ящиков из резервной копии с поддержкой приложений или резервной копии базы данных

1. [Только при восстановлении из базы данных в Office 365] Если агент для Office 365 не установлен на машине с Exchange Server, резервная копия которой создается, выполните одно из указанных ниже действий:
   - Если в вашей организации нет агента для Office 365, установите агент для Office 365 на машине, для которой создана резервная копия, или на другой машине с такой же версией Microsoft Exchange Server.
   - Если в вашей организации уже есть агент для Office 365, скопируйте библиотеки с машины, для которой создана резервная копия, или с другой машины с такой же версией Microsoft Exchange Server на машину с агентом Office 365, как описано в разделе «Копирование библиотек Microsoft Exchange».
2. 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.
3. Щелкните **Восстановление**.
4. 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

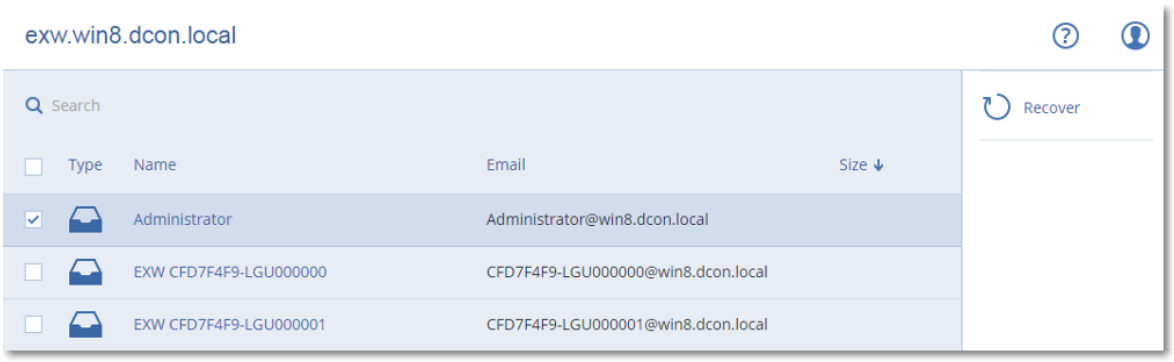
Exchange или агент для VMware, а затем выберите точку восстановления.

- Выберите точку восстановления на вкладке Хранилище резервных копий.

Вместо выключенной исходной машины восстановление будет выполнено машиной, которая выбранная для просмотра одним из двух указанных выше действий.

5. Щелкните **Восстановление** > **Почтовые ящики Exchange**.
6. Выберите почтовые ящики, которые необходимо восстановить.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.



7. Нажмите кнопку **Восстановить**.
8. [Только при восстановлении в Office 365]:
   a. В поле **Восстановить в** выберите пункт **Microsoft Office 365**.
   b. [Если в шаге 6 выбран только один почтовый ящик] В поле **Целевой почтовый ящик** укажите целевой почтовый ящик.
   c. Щелкните **Запуск восстановления**.

   Для этой процедуры не требуется никаких дополнительных шагов.

   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 использоваться для доступа к машине. Требования к этой учетной записи указаны в разделе «Требуемые права пользователя».
10. [Необязательно] Чтобы изменить автоматически выбранную базу данных, щелкните **База данных для воссоздания отсутствующих почтовых ящиков**.
11. Щелкните **Запуск восстановления**.

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 Хранилище 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 8-11 вышеописанной процедуры.

11.11.4 Восстановление элементов почтовых ящиков

Порядок восстановления элементов почтовых ящиков из резервной копии с поддержкой приложений или резервной копии базы данных

1. [Только при восстановлении из базы данных в Office 365] Если агент для Office 365 не установлен на машине с Exchange Server, резервная копия которой создается, выполните одно из указанных ниже действий:
   - Если в вашей организации нет агента для Office 365, установите агент для Office 365 на машине, для которой создана резервная копия, или на другой машине с такой же версией Microsoft Exchange Server.
   - Если в вашей организации уже есть агент для Office 365, скопируйте библиотеки с машины, для которой создана резервная копия, или с другой машины с такой же версией Microsoft Exchange Server на машину с агентом Office 365, как описано в разделе «Копирование библиотек Microsoft Exchange».
2. 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.
3. Щелкните **Восстановление**.
4. 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

Exchange или агент для VMware, а затем выберите точку восстановления.

- Выберите точку восстановления на вкладке Хранилище резервных копий.

Вместо выключенной исходной машины восстановление будет выполнено машиной, которая выбранная для просмотра одним из двух указанных выше действий.

5. Щелкните **Восстановление** > **Почтовые ящики Exchange**.
6. Щелкните почтовый ящик, в котором изначально содержались элементы, которые необходимо восстановить.
7. Выберите элементы, которые необходимо восстановить.

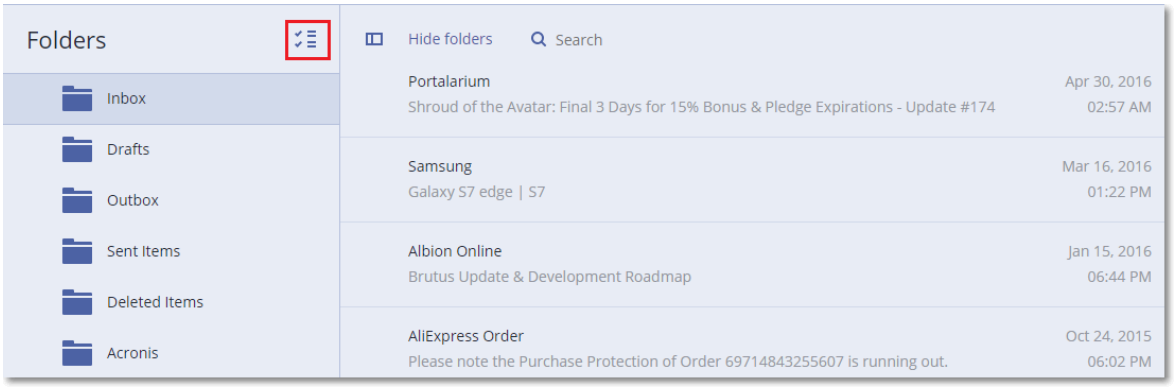
   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

   - 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.



8. Нажмите кнопку **Восстановить**.
9. Чтобы выполнить восстановление в Office 365, выберите **Microsoft Office 365** в поле **Восстановить в**.

   Чтобы выполнить восстановление на Exchange Server, сохраните значение по умолчанию **Microsoft Exchange** в поле **Восстановить в**.
10. [Только при восстановлении на Exchange Server] 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.
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».

11. 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.
12. [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**.
13. Щелкните **Запуск восстановления**.

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 Хранилище 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.

   Когда выбрано это сообщение электронной почты, можно щелкнуть **Показать содержимое**, чтобы показать его содержимое, включая вложения.

Примечание
Чтобы загрузить вложенный файл, щелкните его имя.

Когда выбрано это 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 9-13 вышеописанной процедуры.

11.11.5 Копирование библиотек Microsoft Exchange Server

При восстановлении почтовых ящиков Exchange или элементов почтовых ящиков в Office 365, возможно, необходимо будет скопировать указанные ниже библиотеки с машины, для которой создана резервная копия, или с другой машины с такой же версией Microsoft Exchange Server на машину с агентом для Office 365.

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.

11.12 Изменение учетных данных для доступа к SQL Server или Exchange Server

Можно изменить учетные данные для доступа к SQL Server или Exchange Server без переустановки агента.

Для изменения учетных данных для доступа к SQL Server или 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 SQL Server или Exchange Server, для которых необходимо изменить учетные данные.
3. Щелкните **Укажите учетные данные**
4. Укажите новые учетные данные для доступа, а затем щелкните **OK**.

Для изменения учетных данных Exchange Server для доступа к резервной копии почтового ящика

1. Щелкните **Устройства** > **Microsoft Exchange** и разверните узел **Почтовые ящики**.
2. Выберите Microsoft Exchange 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 Защита почтовых ящиков Office 365

Внимание
Информация, приведенная в данном разделе, действительна для локальных развертываний Кибер Бэкап.

12.1 Зачем создавать резервную копию почтовых ящиков Office 365?

Несмотря на то что Microsoft Office 365 – это облачный сервис, регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователя. Удаленные элементы можно восстановить из резервной копии, даже если период хранения в Office 365 истек. Кроме того, можно сохранить локальную копию почтовых ящиков Office 365, если это необходимо в соответствии с нормативными требованиями.

12.2 Что необходимо для резервного копирования почтовых ящиков?

Для выполнения резервного копирования почтовых ящиков Office 365 необходимо иметь роль глобального администратора в Microsoft Office 365.

Порядок добавления организации Microsoft Office 365

1. Установите агент для Office 365 на машине Windows, которая подключена к Интернету. В организации должен быть только один агент для Office 365.
2. На веб-консоли Кибер Бэкап щелкните **Microsoft Office 365**.
3. В открывшемся окне введите идентификатор приложения, секрет приложения и идентификатор клиента Microsoft 365. Дополнительную информацию о том, как их найти см. в разделе Получение идентификатора и секрета приложения.
4. Щелкните **Войти**.

После этого элементы данных вашей организации появятся на веб-консоли Кибер Бэкап на странице **Microsoft Office 365**.

12.3 Восстановление

Из резервной копии почтового ящика можно восстановить следующие элементы:

- почтовые ящики;
- папки электронной почты;
- сообщения электронной почты;
- события календаря;

- задания;
- контакты;
- записи журнала;
- Примечание

Чтобы найти эти элементы, можно воспользоваться поиском.

Восстановление может выполняться в почтовый ящик Microsoft Office 365 или на запущенный сервер Exchange Server.

Если почтовый ящик восстанавливается в существующий почтовый ящик Office 365, существующие элементы с одинаковыми идентификаторами перезаписываются. Если почтовый ящик восстанавливается в существующий почтовый ящик Exchange Server, существующие элементы остаются без изменений. Восстановленные элементы помещаются рядом с ним.

При восстановлении элементов почтового ящика перезапись не происходит. Вместо этого в целевой папке заново создается полный путь к элементу почтового ящика.

12.4 Ограничения

- Если план защиты применен к более чем 500 почтовым ящикам, это может привести к снижению производительности резервного копирования. Чтобы защитить большое количество почтовых ящиков, создайте несколько планов защиты и запланируйте их запуск в разное время.
- Невозможно создать резервную копию архивированных почтовых ящиков (**архив на месте**).
- В резервную копию почтового ящика входят только те папки, которые видны для пользователей. Папка **Элементы с возможностью восстановления** и ее подпапки (**Удаления**, **Версии**, **Очистки**, **Аудит**, **DiscoveryHold**, **Ведение журнала календаря**) не входят в резервную копию почтового ящика.
- Невозможно выполнить восстановление в новый почтовый Office 365. Сначала необходимо создать нового пользователя Office 365, затем восстановить элементы в почтовый ящик этого пользователя.
- Восстановление в учетную запись другой организации Microsoft Office 365 не поддерживается.
- Некоторые типы или свойства, которые поддерживаются в Office 365, могут не поддерживаться Exchange Server. Они будут пропущены при восстановлении на Exchange Server.

12.5 Выбор почтовых ящиков

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана защиты как требуется.

Порядок выбора почтовых ящиков

1. Щелкните **Microsoft Office 365**.
2. Войдите в Microsoft Office 365 как глобальный администратор при поступлении соответствующего запроса
3. Выберите почтовые ящики, для которых необходимо создать резервные копии.
4. Нажмите кнопку **Резервное копирование**.

12.6 Восстановление почтовых ящиков и элементов почтовых ящиков

12.6.1 Восстановление почтовых ящиков

1. [Только при восстановлении в Exchange Server] Убедитесь, что существует пользователь Exchange с таким же именем входа, как и пользователь, почтовый ящик которого восстанавливается. В противном случае создайте пользователя. Другие требования для этого пользователя доступны в теме«Восстановление почтовых ящиков Exchange и элементов почтового ящика» раздела «Требования для учетных записей пользователя».
2. Щелкните **Устройства** > **Microsoft Office 365**.
3. 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 Хранилище резервных копий и щелкните **Показать резервные копии**.
4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
5. Последовательно выберите пункты **Восстановление** > **Почтовый ящик**.
6. Чтобы выполнить восстановление на Exchange Server, выберите **Microsoft Exchange** в поле **Восстановить в**. Продолжите восстановление, как описано в разделе «Восстановление почтовых ящиков», начиная с шага 9. Для этой процедуры не требуется никаких дополнительных шагов.

   Чтобы выполнить восстановление в Office 365, сохраните установленное по умолчанию значение **Microsoft Office 365** в поле **Восстановить в**.
7. Раздел **Целевой почтовый ящик** позволяет просмотреть, изменить или указать целевой почтовый ящик.

   По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует, необходимо указать целевой почтовый ящик.
8. Щелкните **Запуск восстановления**.

12.6.2 Восстановление элементов почтовых ящиков

1. [Только при восстановлении в Exchange Server] Убедитесь, что существует пользователь Exchange с таким же именем входа, как и пользователь, элементы почтового ящика которого восстанавливаются. В противном случае создайте пользователя. Другие требования для этого пользователя доступны в теме«Восстановление почтовых ящиков Exchange и элементов почтового ящика» раздела «Требования для учетных записей пользователя».
2. Щелкните **Устройства** > **Microsoft Office 365**.
3. 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 Хранилище резервных копий и щелкните **Показать резервные копии**.
4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
5. Последовательно выберите пункты **Восстановление** > **Сообщения электронной почты**.
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.

   Когда выбрано это 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 
7. Нажмите кнопку **Восстановить**.
8. Чтобы выполнить восстановление на Exchange Server, выберите **Microsoft Exchange** в поле **Восстановить в**.

   Чтобы выполнить восстановление в Office 365, сохраните установленное по умолчанию значение **Microsoft Office 365** в поле **Восстановить в**.

[Только при восстановлении на Exchange Server] 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 машины, на которой включена роль **Клиентский доступ** Microsoft Exchange Server. 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 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, необходимо указать целевой почтовый ящик.
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**.
12. Щелкните **Запуск восстановления**.

12.7 Изменение учетных данных для доступа к Office 365

Можно изменить учетные данные для доступа к Office 365 без переустановки агента.

Для изменения учетных данных для доступа к Office 365

1. Щелкните **Устройства** > **Microsoft Office 365**.
2. Выберите организацию Office 365.
3. Щелкните **Укажите учетные данные**
4. Введите идентификатор приложения, секрет приложения и идентификатор клиента Microsoft 365. Дополнительную информацию о том, как их найти см. в разделе Получение идентификатора и секрета приложения.
5. Щелкните **Войти**.

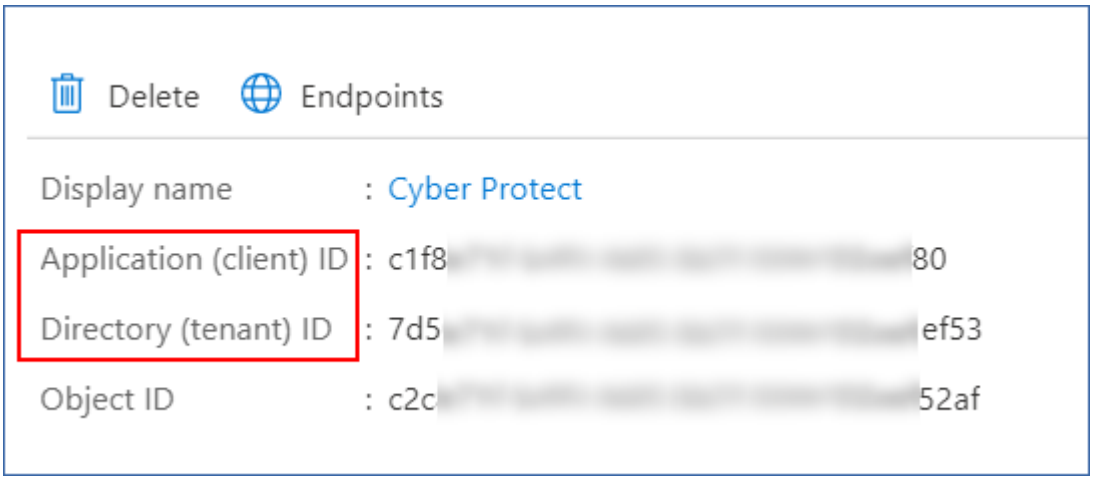
12.8 Получение идентификатора и секрета приложения

Чтобы использовать современный метод аутентификации для Office 365, необходимо создать настраиваемое приложение в Azure Active Directory и предоставить ему конкретные разрешения API. Таким образом вы получите **идентификатор приложения**, **секрет приложения** и **идентификатор каталога (клиента)**, который необходимо ввести на веб-консоли Кибер Бэкап.

Порядок создания приложения в Azure Active Directory

1. Войдите на портал Azure как администратор.
2. Последовательно выберите пункты **Azure Active Directory** > **Регистрации приложения**, а затем щелкните **Новая регистрация**.
3. Укажите имя настраиваемого приложения, например Кибер Бэкап.
4. В поле **Supported Account types (Поддерживаемые типы учетных записей)** выберите **Accounts in this organizational directory only (Учетные записи только в каталоге этой организации)**.
5. Щелкните **Зарегистрироваться**.

Приложение создано. На портале Azure перейдите на страницу **Обзор** приложения и проверьте идентификатор приложения (клиента) и каталога (пользователя клиента).



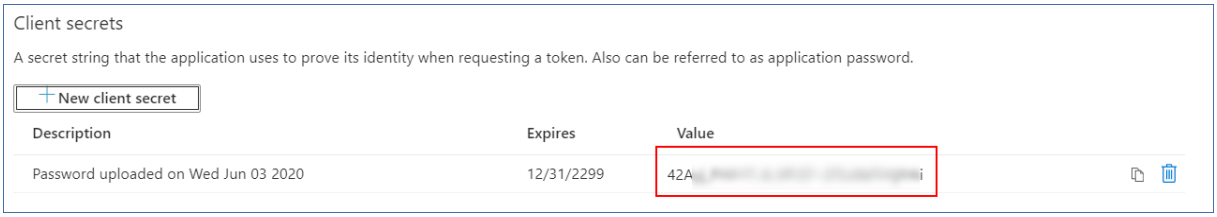
Дополнительную информацию о процедуре создания приложения на портале Azure см. в документации Microsoft.

Порядок предоставления приложению необходимых разрешений API

1. На портале Azure откройте раздел **Разрешения API** и щелкните **Добавить разрешение**.
2. Откройте вкладку **APIs my organization uses** (API в моей организации) и найдите **Office 365 Exchange Online**.
3. Щелкните **Office 365 Exchange Online**, а затем щелкните **Разрешения приложения**.
4. Установите флажок **full_access_as_app**, а затем щелкните **Добавить разрешения**.
5. В разделе **Разрешения API** щелкните **Добавить разрешение**.
6. Выберите **Microsoft Graph**.
7. Выберите **Разрешения приложения**.
8. Разверните вкладку **Каталог** и установите флажок **Directory.Read.All** . Щелкните **Добавить разрешения**.
9. Отметьте все разрешения, а затем щелкните **Предоставить согласие администратора для <имя вашей программы>**.
10. Для подтверждения выбранного варианта щелкните **Да**.

Порядок создания секрета приложения

1. На портале Azure найдите ваше приложение и выберите пункты **Certificates & secrets (Сертификаты и секреты)** > **New client secret (Новый секрет клиента)**.
2. В открывшемся диалогом окне в поле "Expires: (Истекает:)" выберите **Never (Никогда)** и щелкните **Добавить**.
3. Проверьте секрет приложения в поле **Значение** и убедитесь, что помните его.



Дополнительную информацию о секрете приложения см. в документации Microsoft.

13 Защита CommuniGate Pro

13.1 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.

13.2 Что необходимо для резервного копирования CommuniGate Pro?

Для резервного копирования данных CommuniGate Pro понадобятся установленные и настроенные продукты:

- Кибер Бэкап 15U2.7 или новее с лицензией Кибер Бэкап Расширенная.
- CommuniGate Pro.

Для выполнения резервного копирования требуется установка агента.

Поддерживается установка агентов для следующих операционных систем:

- Windows.
- Linux.

13.3 Возможности

13.3.1 Резервное копирование

1. Автоматическая и ручная синхронизация ресурсов.
2. Резервное копирование данных.
3. Резервное копирование по расписанию.
4. Поддержка многоуровневого резервного копирования.
5. Перезапись данных хранилища по выбору.
6. Настраиваемые правила очистки хранилища.

13.3.2 Восстановление

Из резервной копии можно восстановить следующие элементы:

- почтовые ящики, включая папки и вложения,
- контакты,
- календари,
- заметки,
- задачи,
- настройки учетной записи.

13.4 Известные проблемы и ограничения

- Восстановление в новый хост возможно в случае, если на нем заранее создан домен с исходным именем. Восстановление в домен с новым именем невозможно.
- Резервные копии можно сохранять только в локальных папках (подробнее см. в разделе "Выбор места назначения" (стр. 180)).

См. также Известные проблемы версии 16.5.

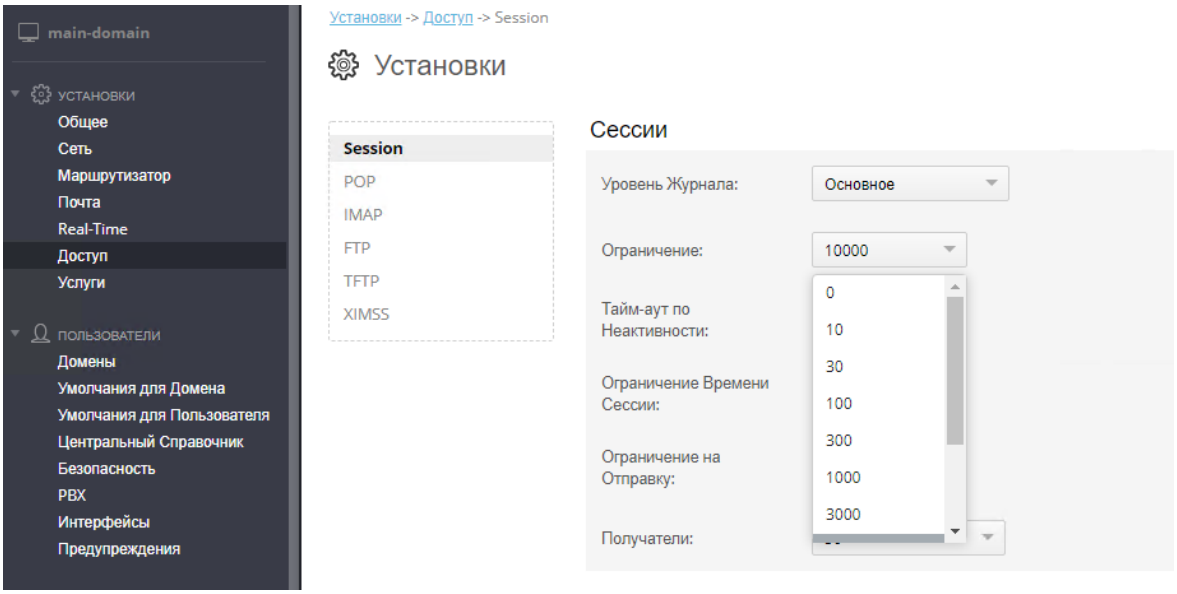
13.5 Предварительные требования для защиты CommuniGate Pro

Перед началом использования защиты CommuniGate Pro потребуется выполнить некоторые действия.

13.5.1 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.

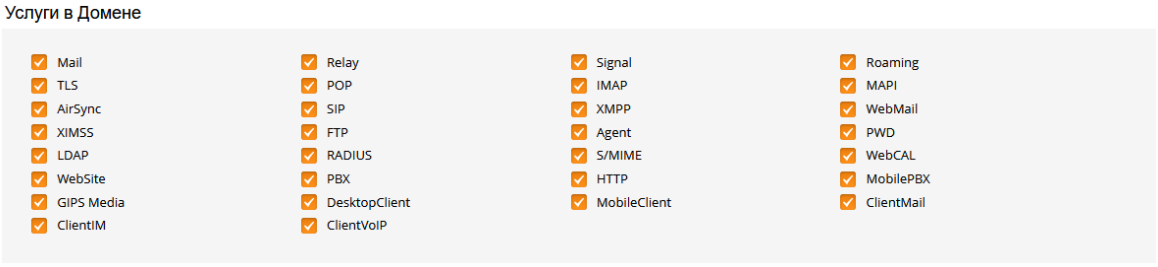


4. Нажмите **Модифицировать**, чтобы сохранить изменения.

13.5.2 Инициализация соединения вручную

Для инициализации соединения Кибер Бэкап с CommuniGate Pro (например, если интерфейс командной строки недоступен) может потребоваться выполнить следующие действия:

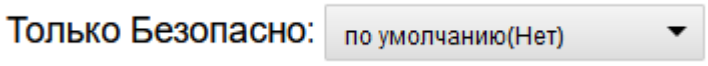
1. Откройте CommuniGate Pro.
2. Перейдите в **Пользователи** -> **Умолчания для Домена** и убедитесь, что услуга PWD включена.



3. Перейдите в **Пользователи** -> **Домены** -> **<Имя_домена>** -> **Установки Домена** и убедитесь, что в настройках домена включена услуга PWD.

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.

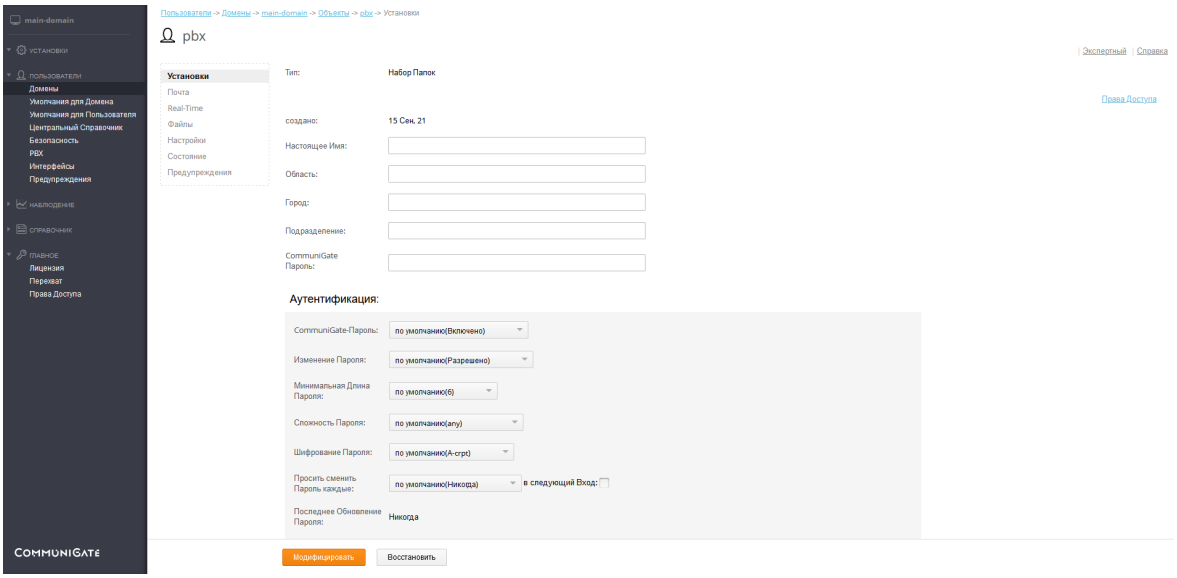
13.5.3 Установка прав пользователя

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:

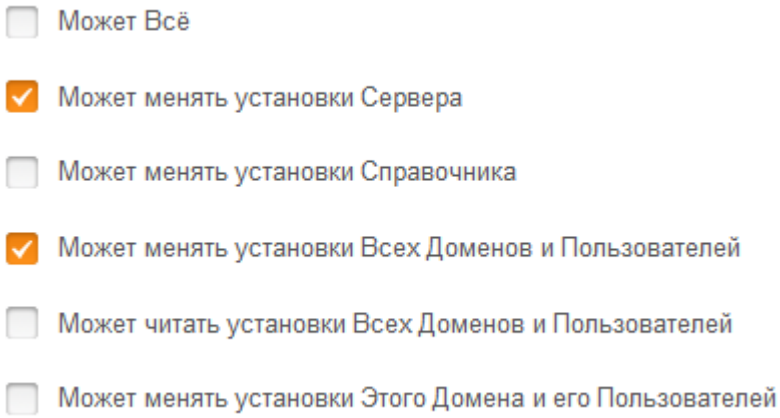
1. Откройте CommuniGate Pro.
2. Перейдите **Пользователи** -> **Домены** -> **Имя главного домена**.
3. Щелкните по имени пользователя в списке объектов.
4. На странице настроек пользователя нажмите справа вверху **Права доступа**.



5. Установите права пользователя следующим образом:

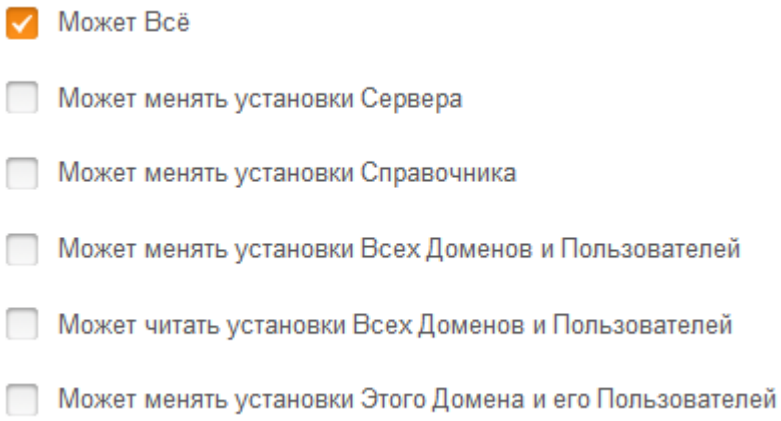
   Может менять установки Сервера и

   Может менять установки всех Доменов и Пользователей



   или

   Может Всё



6. Для сохранения изменений нажмите **Модифицировать**.

13.5.4 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.

13.5.5 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:

```
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
)
```

13.6 Установка CommuniGate Pro

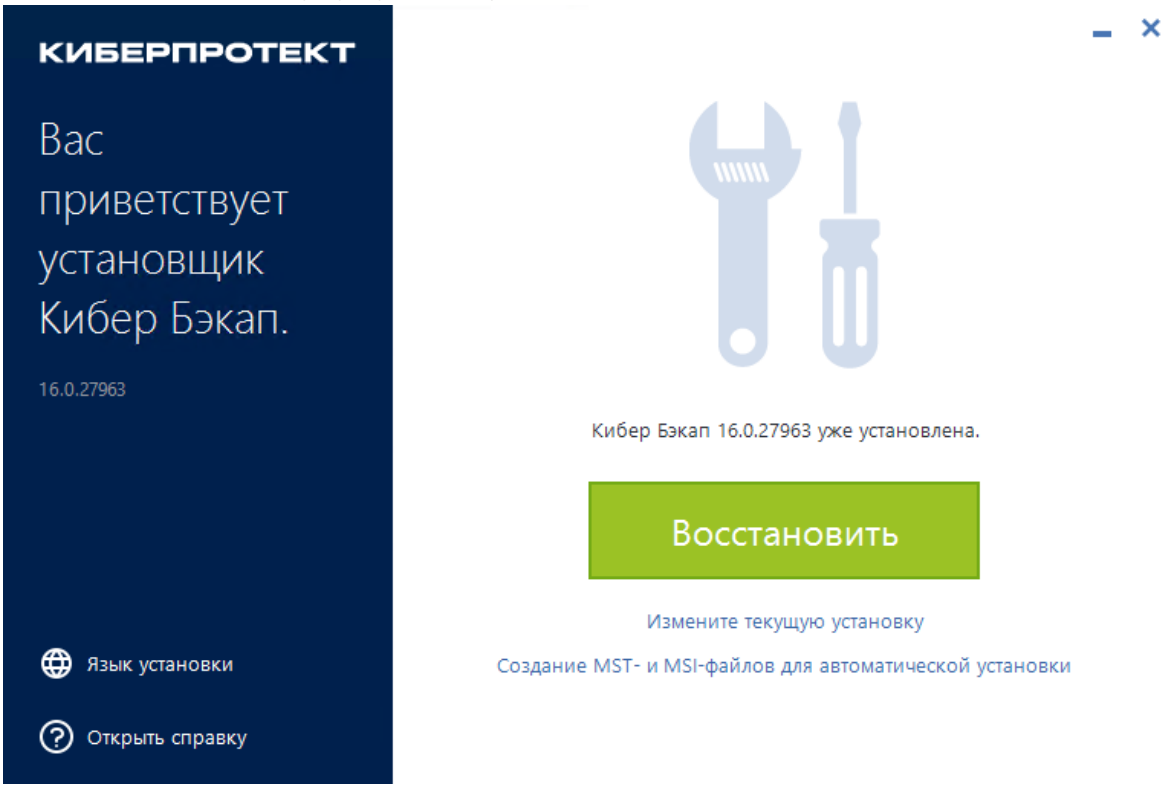
Установка CommuniGate Pro включает в себя установку агента для Кибер Бэкап и добавление хоста CommuniGate Pro. Добавление хоста возможно лишь после установки агента.

Агент может быть установлен на машину с почтовым сервером или на отдельно стоящую машину.

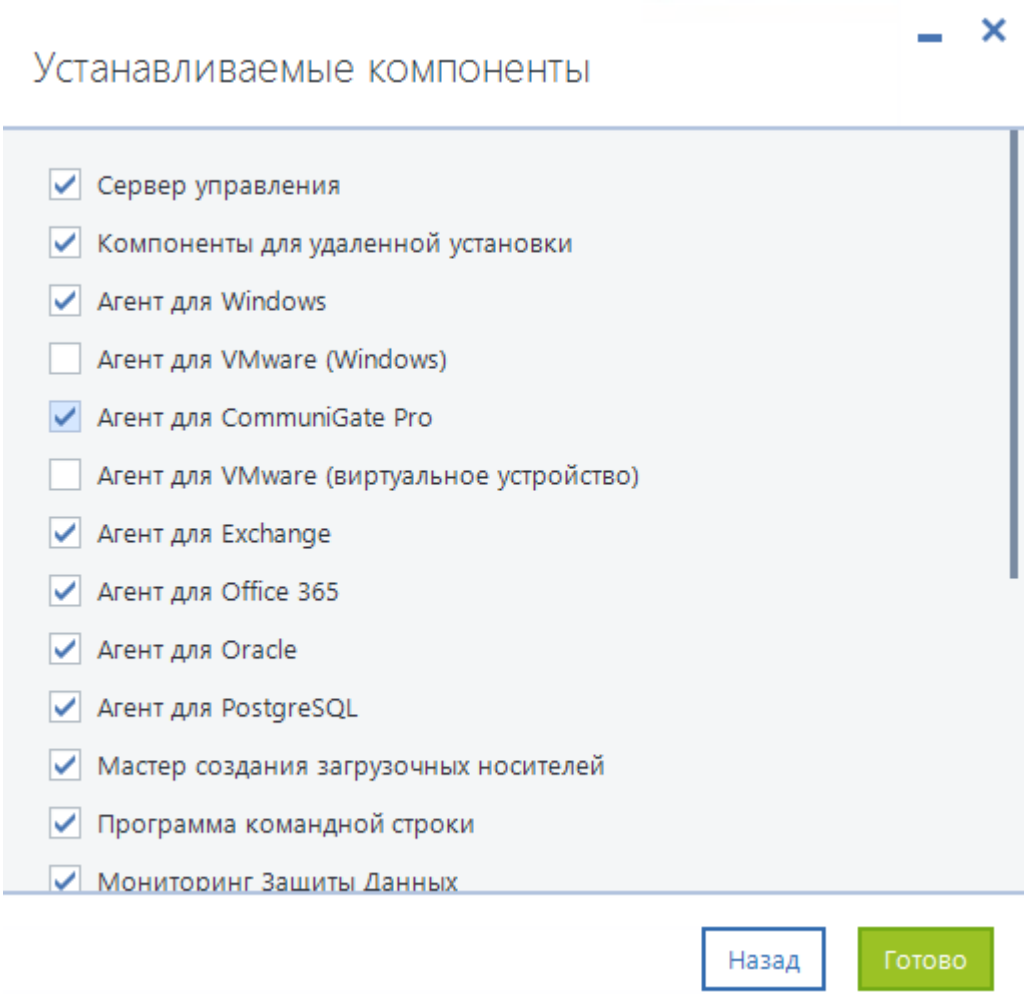
Для каждого хоста должен быть установлен отдельный агент.

13.6.1 Установка агента CommuniGate Pro

1. Запустите установщик Кибер Бэкап.
2. Выберите **Измените текущую установку**



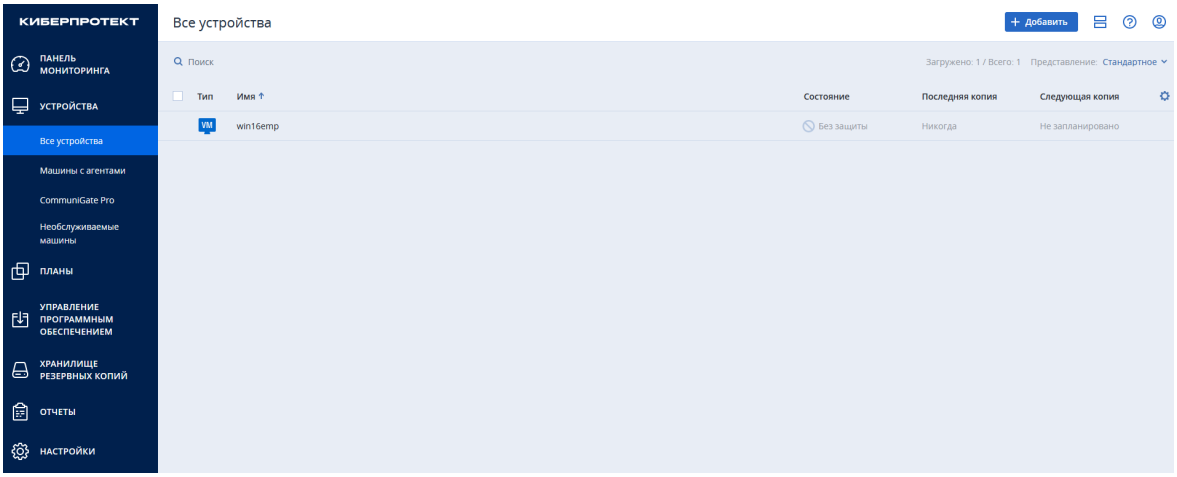
3. Отметьте в списке **Агент для CommuniGate Pro**.



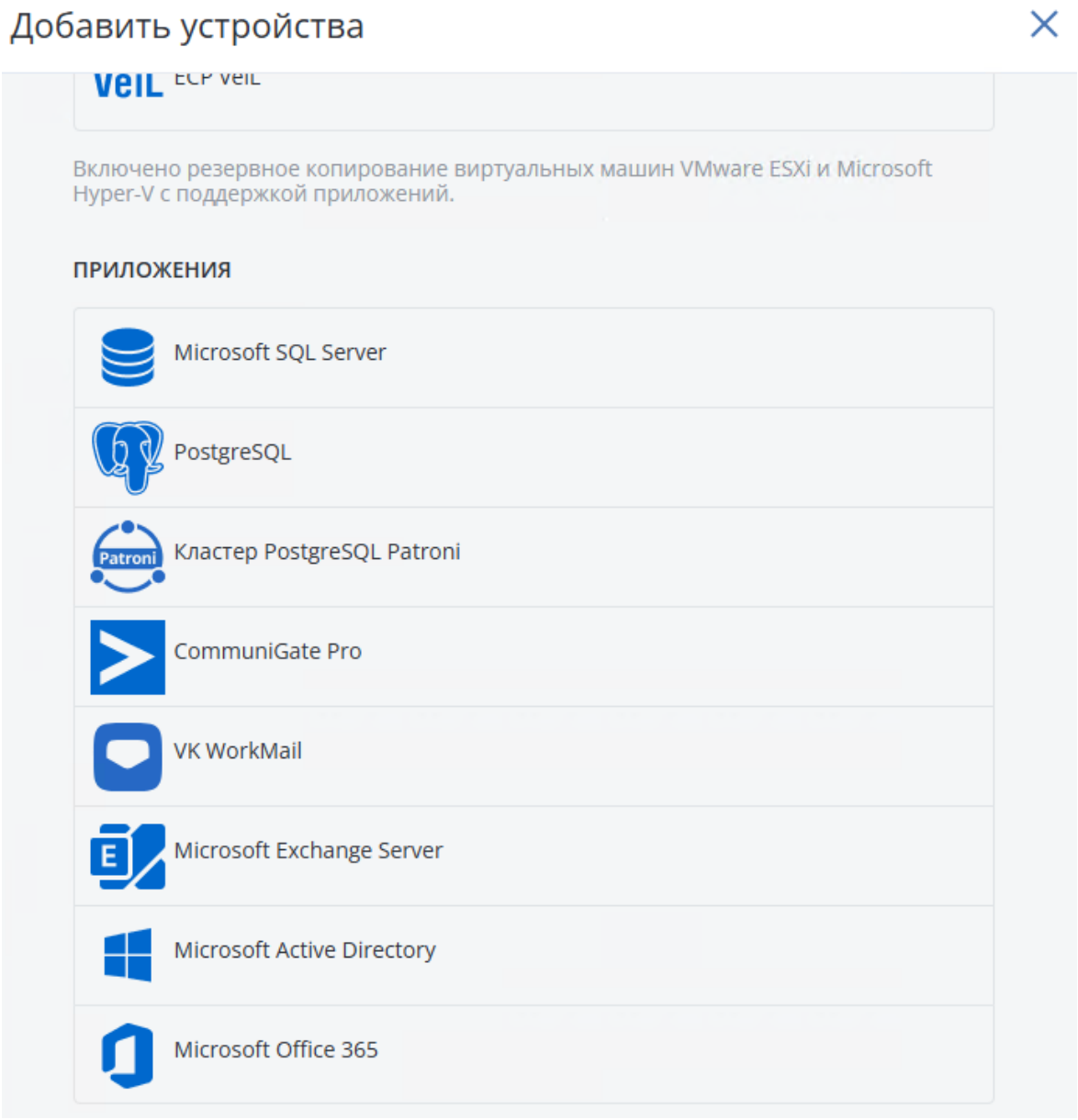
4. Щелкните **Готово**.

13.6.2 Добавление хоста CommuniGate Pro

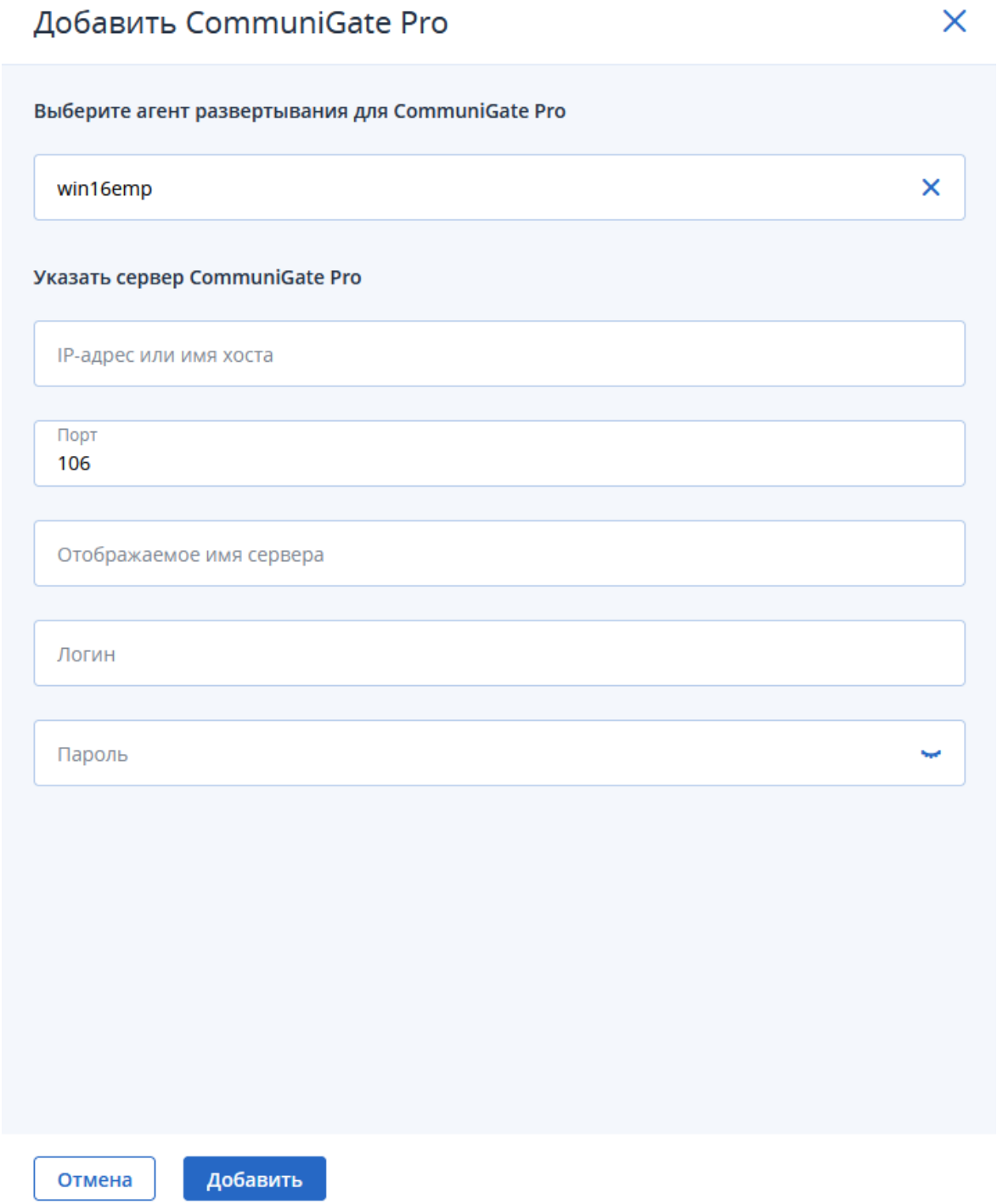
1. В веб-консоли перейдите на вкладку **Устройства** и нажмите в правом верхнем углу **Добавить**.



2. В окне добавления нового устройства щелкните CommuniGate Pro.



3. Заполните поля:
   - в поле **Выберите агент развертывания для CommuniGate Pro** укажите имя компьютера, на котором установлен агент CommuniGate Pro
   - в поле **Указать сервер CommuniGate Pro** укажите IP-адрес или имя сервера CommuniGate Pro
   - в поле **Отображаемое имя сервера** укажите имя, под которым сервер будет отображаться в системе
   - в полях **Логин** и **Пароль** укажите имя и пароль пользователя.



4. По окончании ввода данных нажмите **Добавить**.

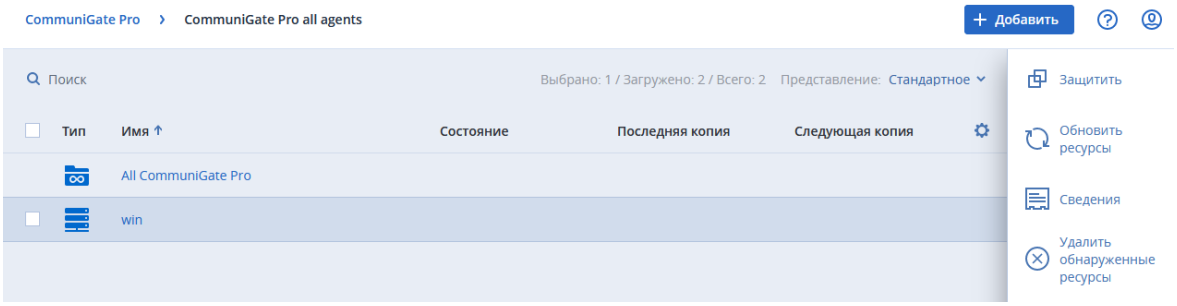
13.7 Резервное копирование CommuniGate Pro

Резервное копирование данных CommuniGate Pro позволяет защитить домены и отдельные почтовые ящики. Для защиты данных необходимо сначала создать план защиты.

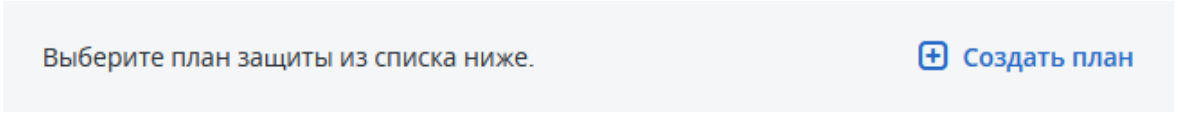
13.7.1 Создание плана защиты для CommuniGate Pro

Для создания плана защиты выполните следующие действия:

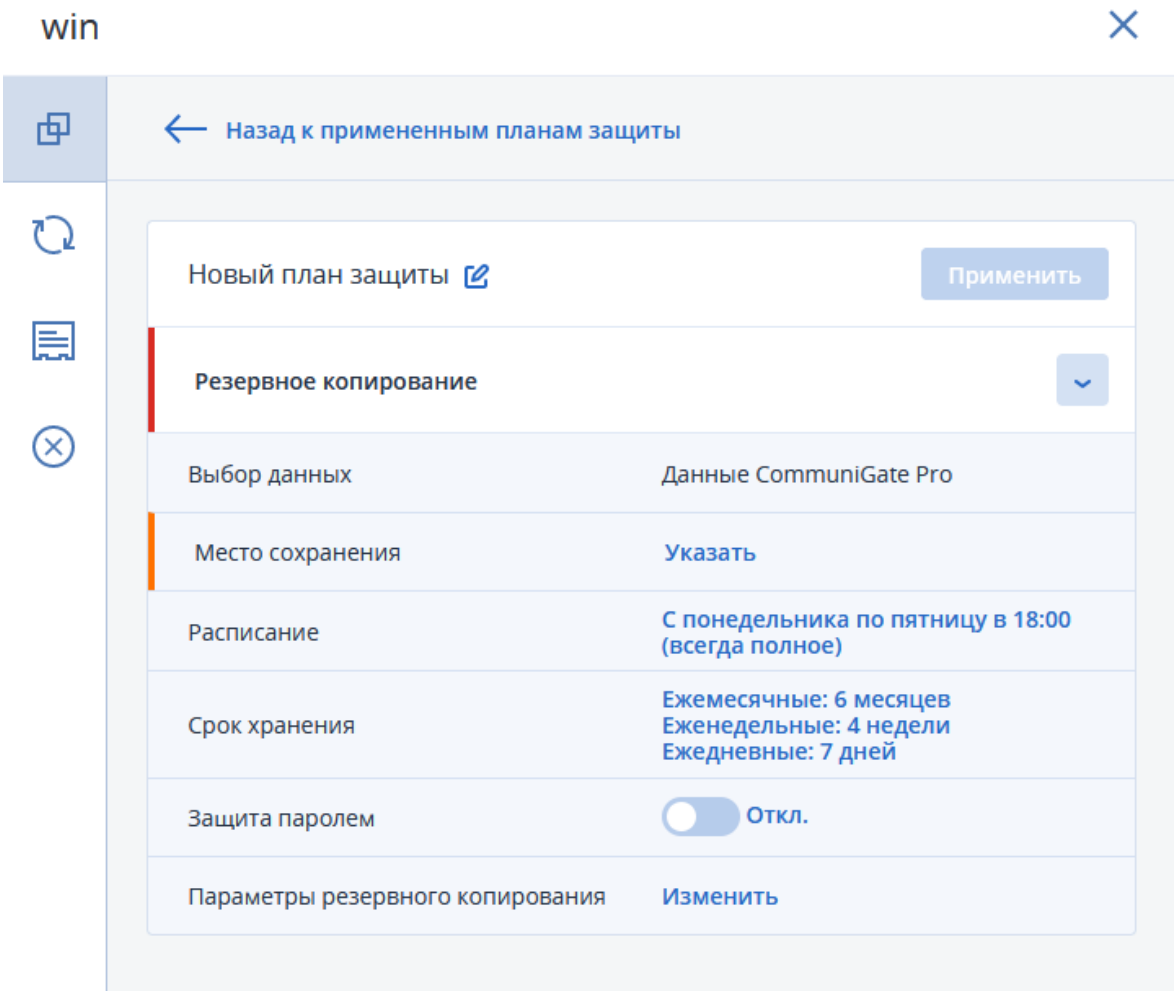
1. Перейдите в **Устройства**.
2. Выберите из списка устройство, которое вы хотите защитить, и щелкните по строке, в которой находится это устройство.
3. Перейдите на вкладку справа **Защитить**.



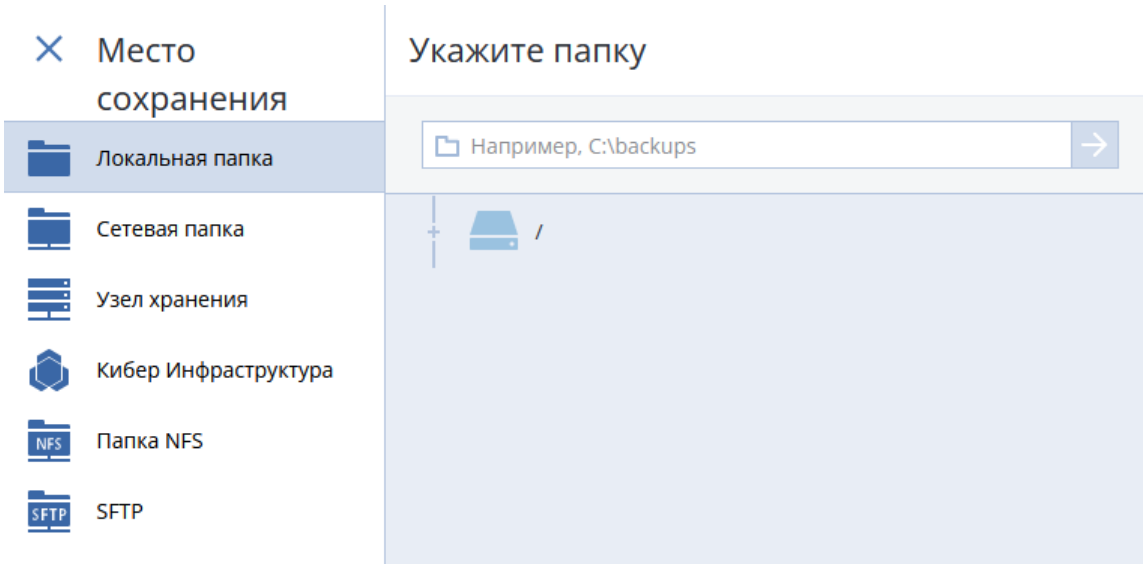
4. Нажмите **Создать план**.



Откроется окно создания плана.

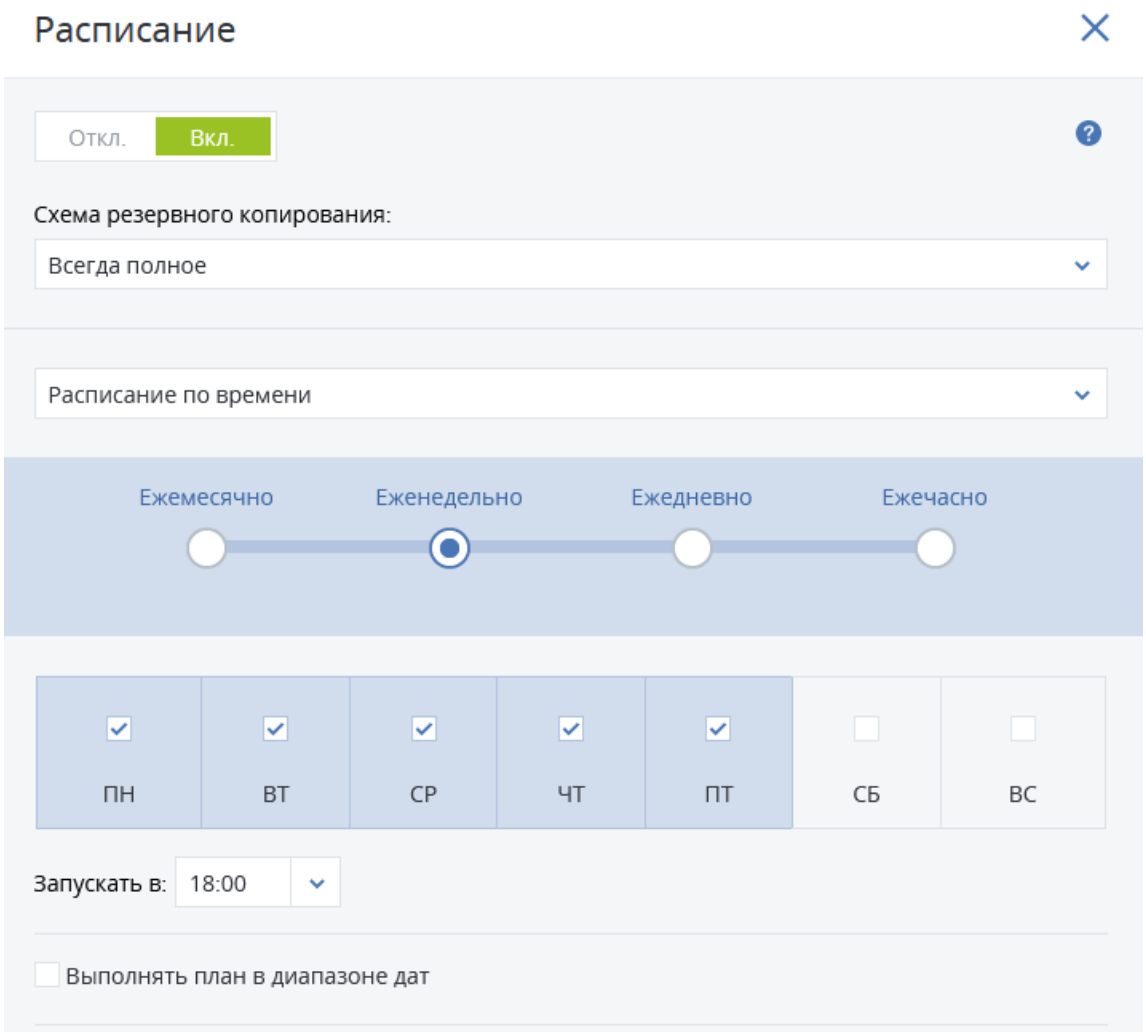


5. Заполните данные в окне создания плана защиты:
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура, папка NFS, SFTP.

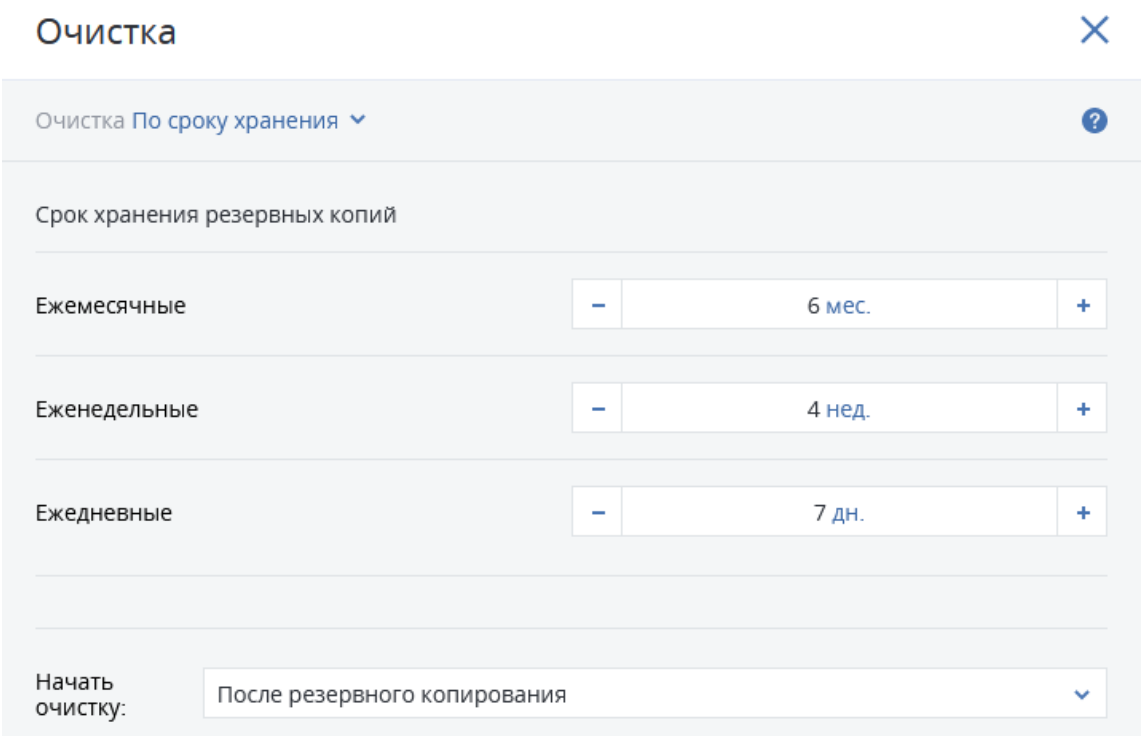


Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места назначения" (стр. 180).

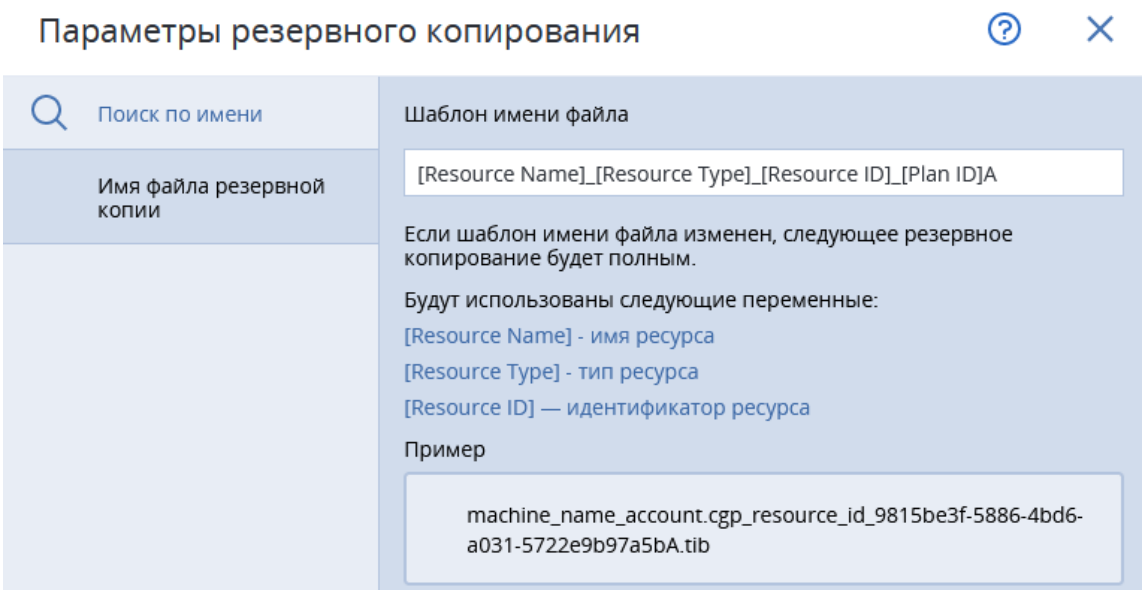
- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.



- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.

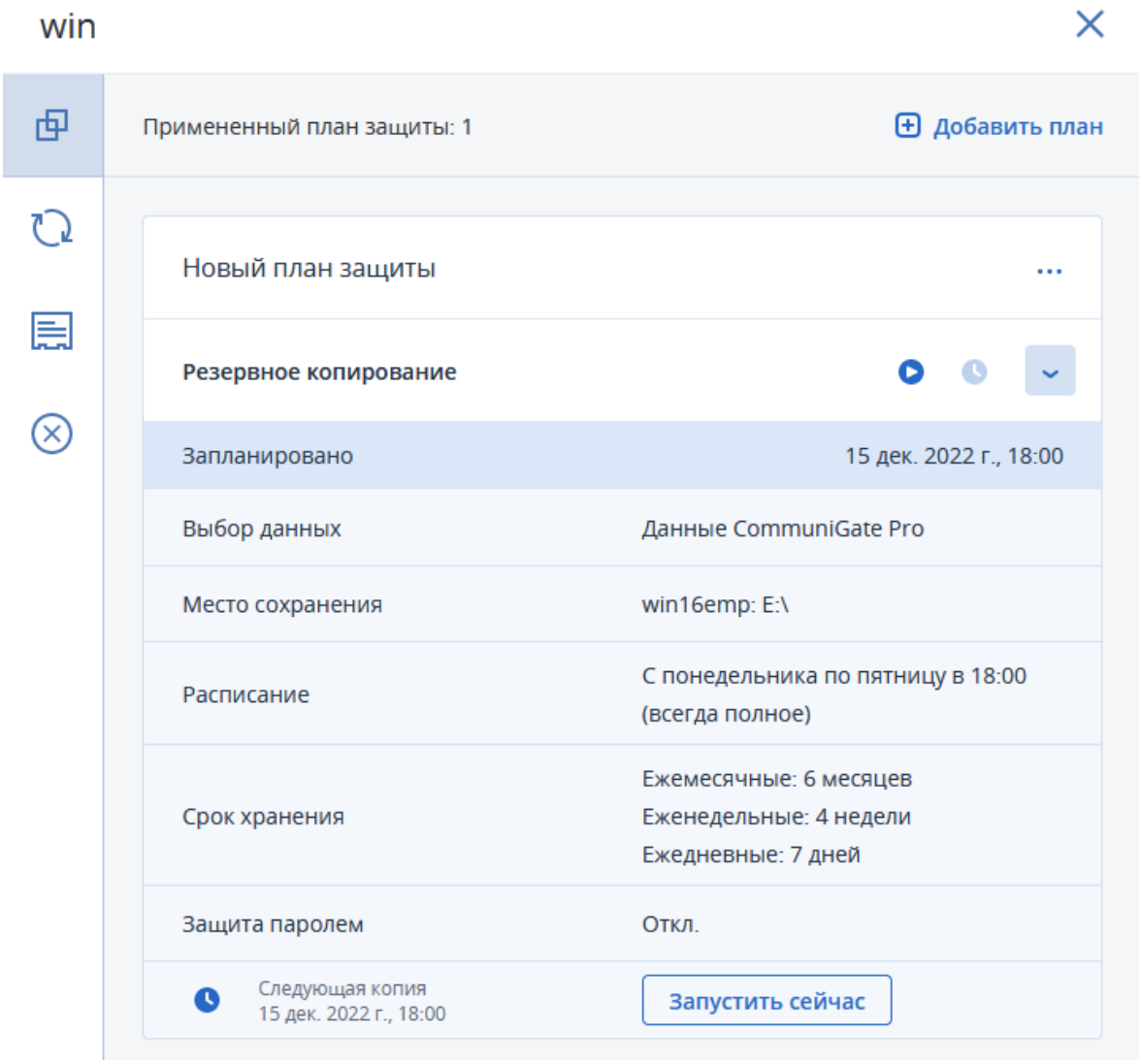


- [Необязательно] В поле **Параметры резервного копирования** укажите параметры для автоматического наименования файла резервного копирования.



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.



См. также информацию в разделе "План защиты и модули" (стр. 157).

13.7.2 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;

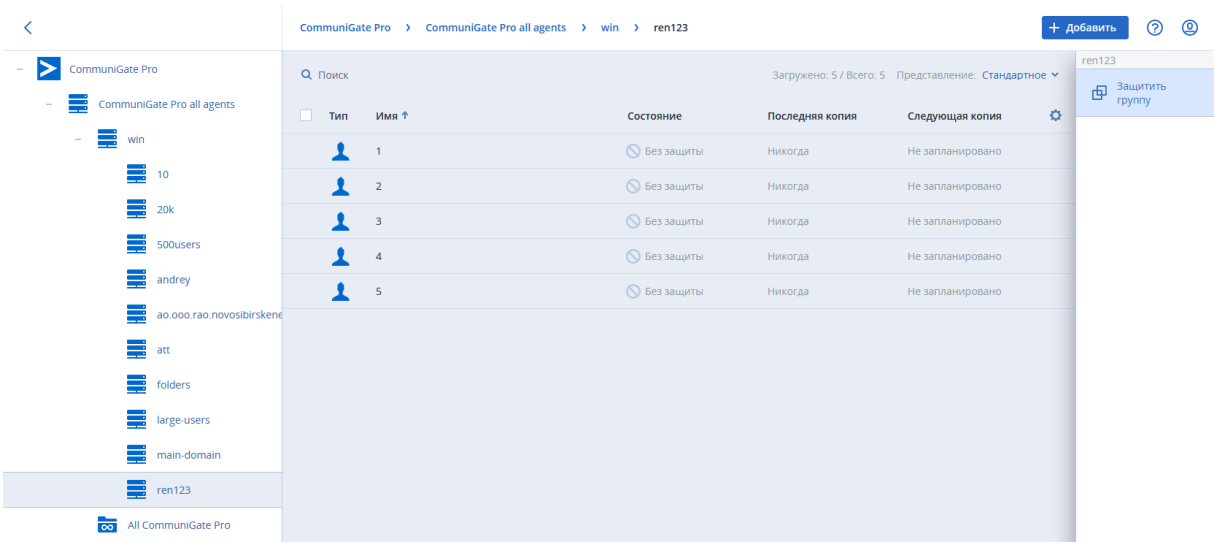
- **Клонировать** - Клонирование плана на другое устройство;
- **Экспорт** - Экспорт плана в файл;
- **Отключение (Включение)** - Включение/отключение плана одной кнопкой;
- **Удаление** - Удаление плана.

Подробнее о действиях с планами защиты см. в разделе "Операции с планами защиты" (стр. 159).

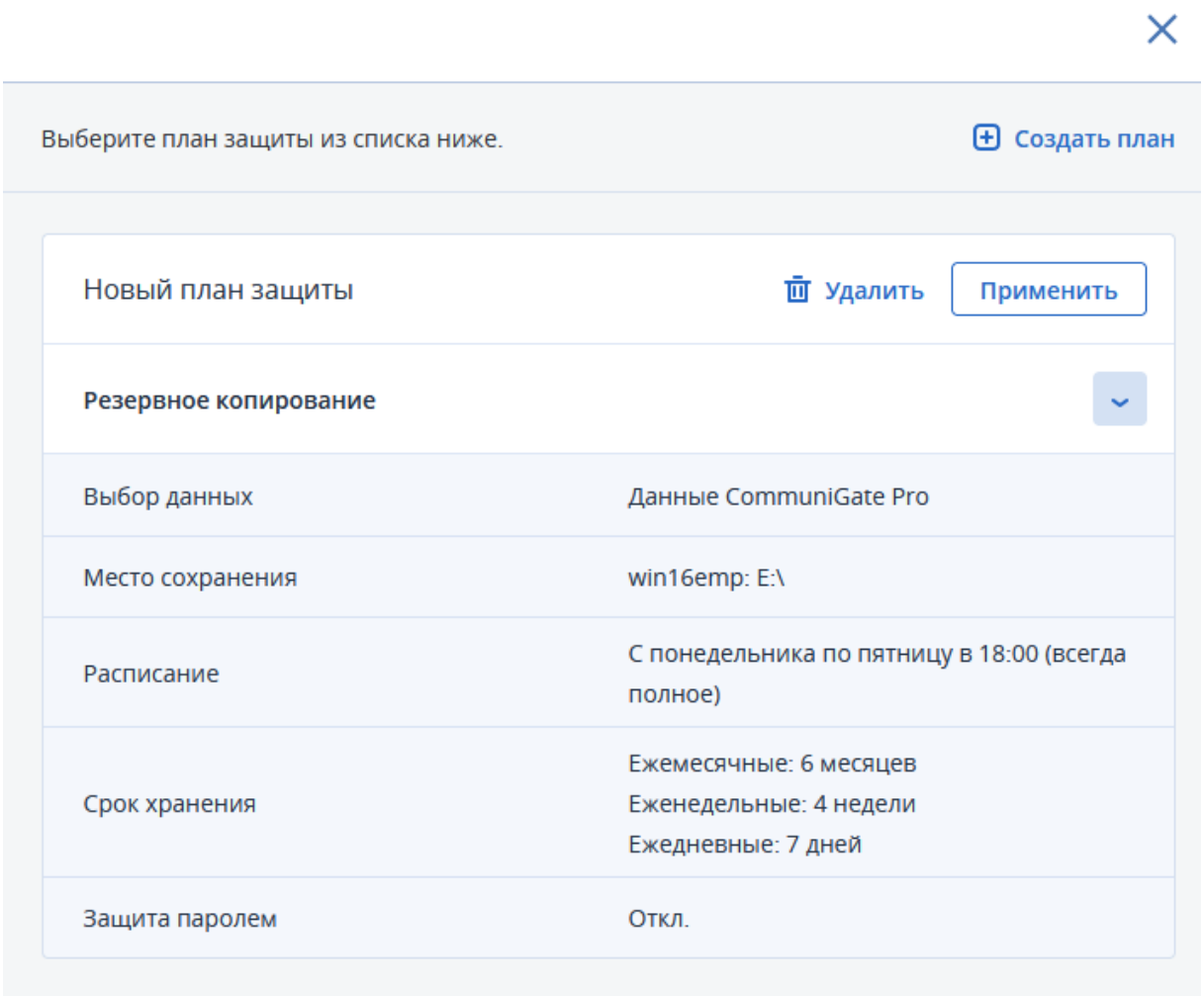
13.7.3 Резервное копирование данных CommuniGate Pro

Резервное копирование домена

Чтобы защитить домен, в списке доменов щелкните по строке, содержащей название домена, и перейдите на вкладку **Защитить группу** в меню справа.



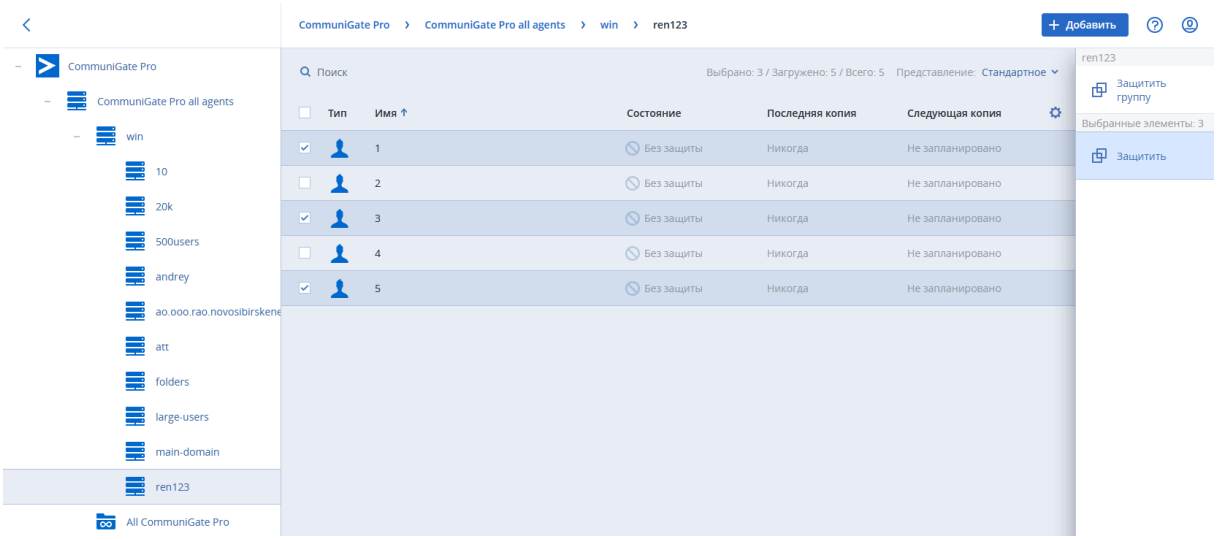
В окне выбора плана защиты в списке планов защиты выберите подходящий план и щелкните **Применить**.



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.



В окне выбора плана защиты в списке планов защиты выберите подходящий план и щелкните **Применить**.

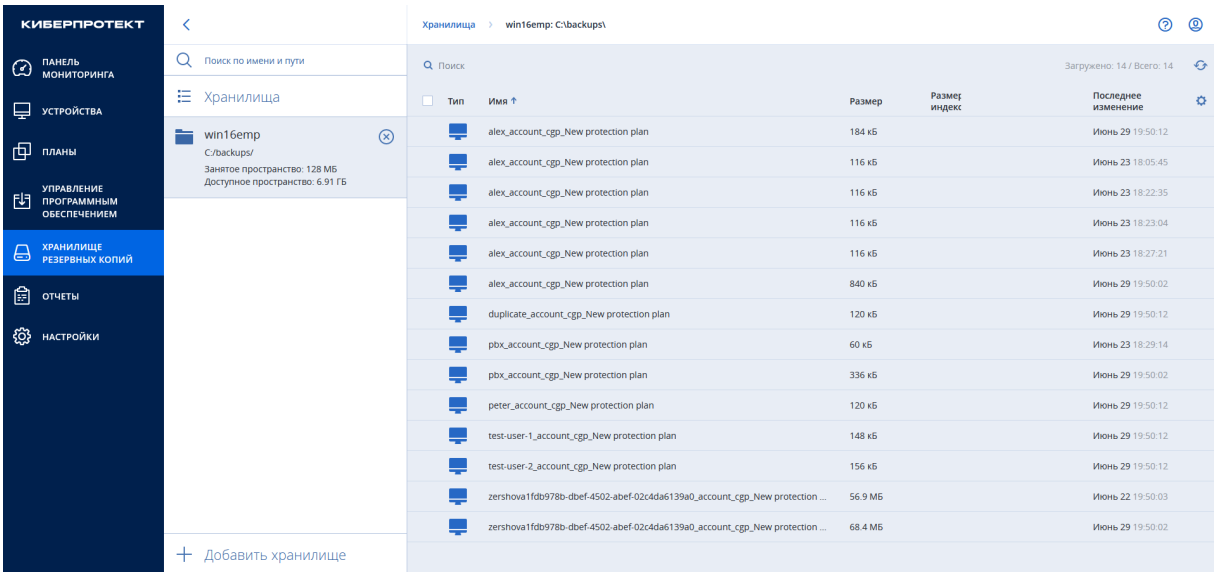
Резервное копирование по требованию

Резервное копирование по требованию представляет собой запуск выбранного плана защиты вне очереди. Чтобы выполнить резервное копирование по требованию:

- 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**.

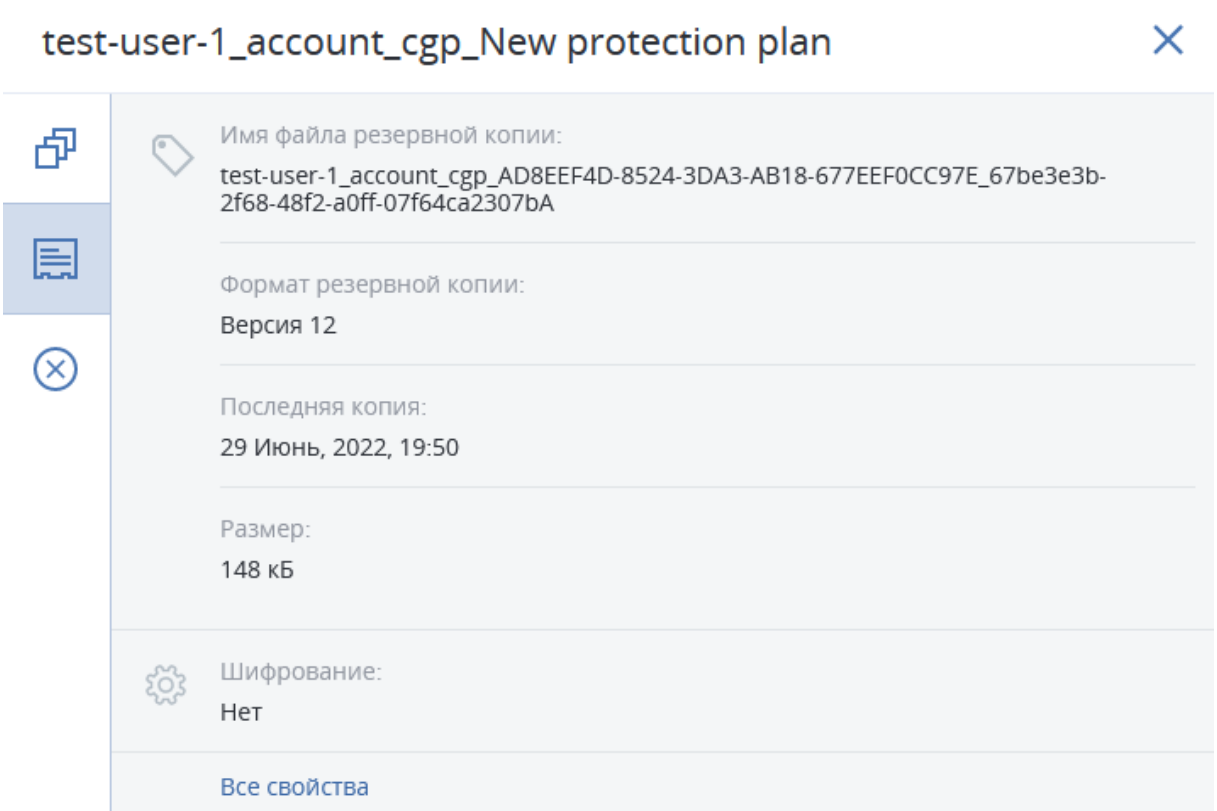
13.7.4 Резервные копии CommuniGate Pro

Чтобы посмотреть список резервных копий компьютеров, перейдите на вкладку **Хранилище резервных копий**.



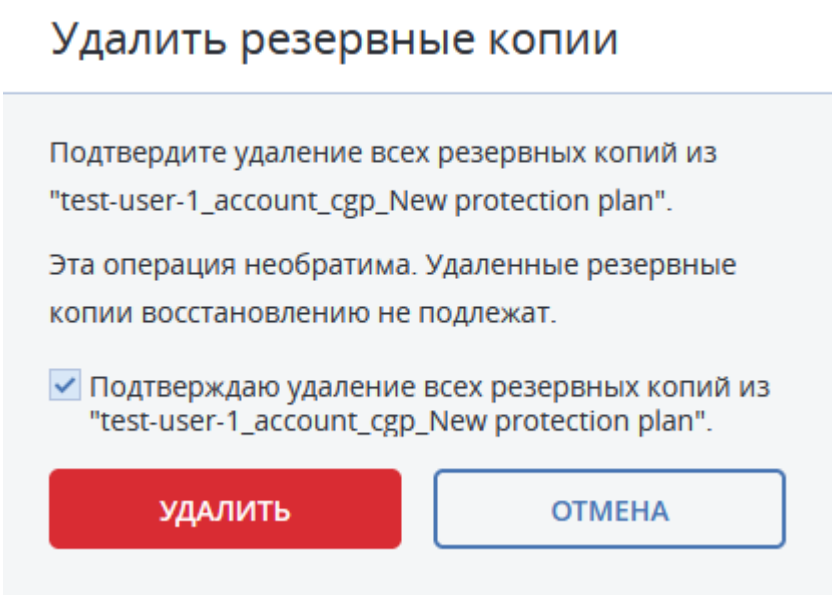
Чтобы посмотреть список резервных копий для компьютера, щелкните на строку с названием компьютера и затем перейдите на вкладку **Показать резервные копии** в меню справа. Откроется список резервных копий. Из этого меню также можно восстановить одну из резервных копий для этого компьютера.

Чтобы посмотреть сведения о резервной копии, щелкните по строке, содержащей название резервной копии, и перейдите на вкладку **Сведения** в меню справа.



Подробная информация доступна по ссылке **Все свойства**.

Чтобы удалить резервную копию, перейдите на вкладку **Удалить** в меню справа.



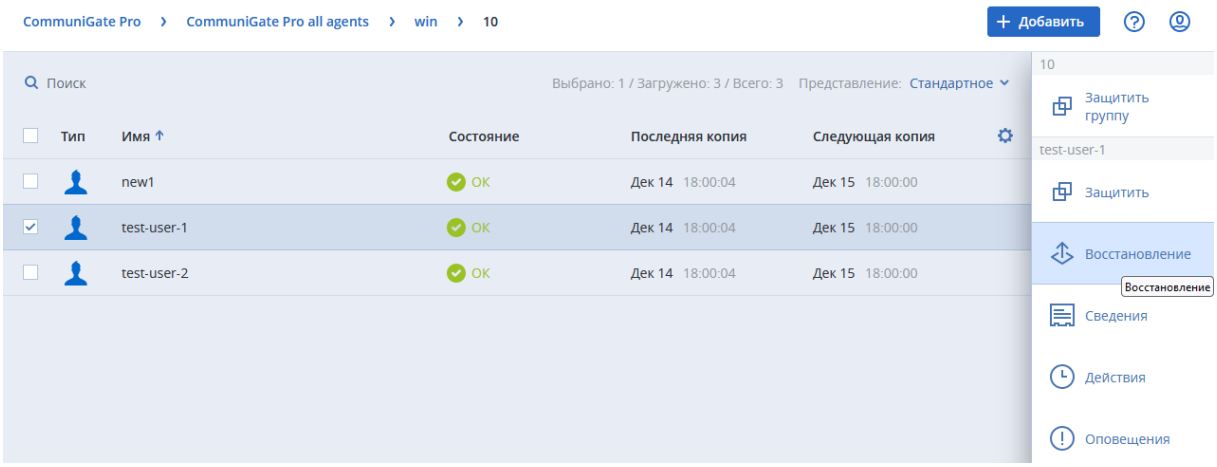
Для подтверждения удаления отметьте флажок в поле и нажмите **Удалить**. Выбранная резервная копия после удаления исчезнет из списка резервных копий.

Для удаления резервной копии см. также Восстановление CommuniGate Pro.

13.8 Восстановление CommuniGate Pro

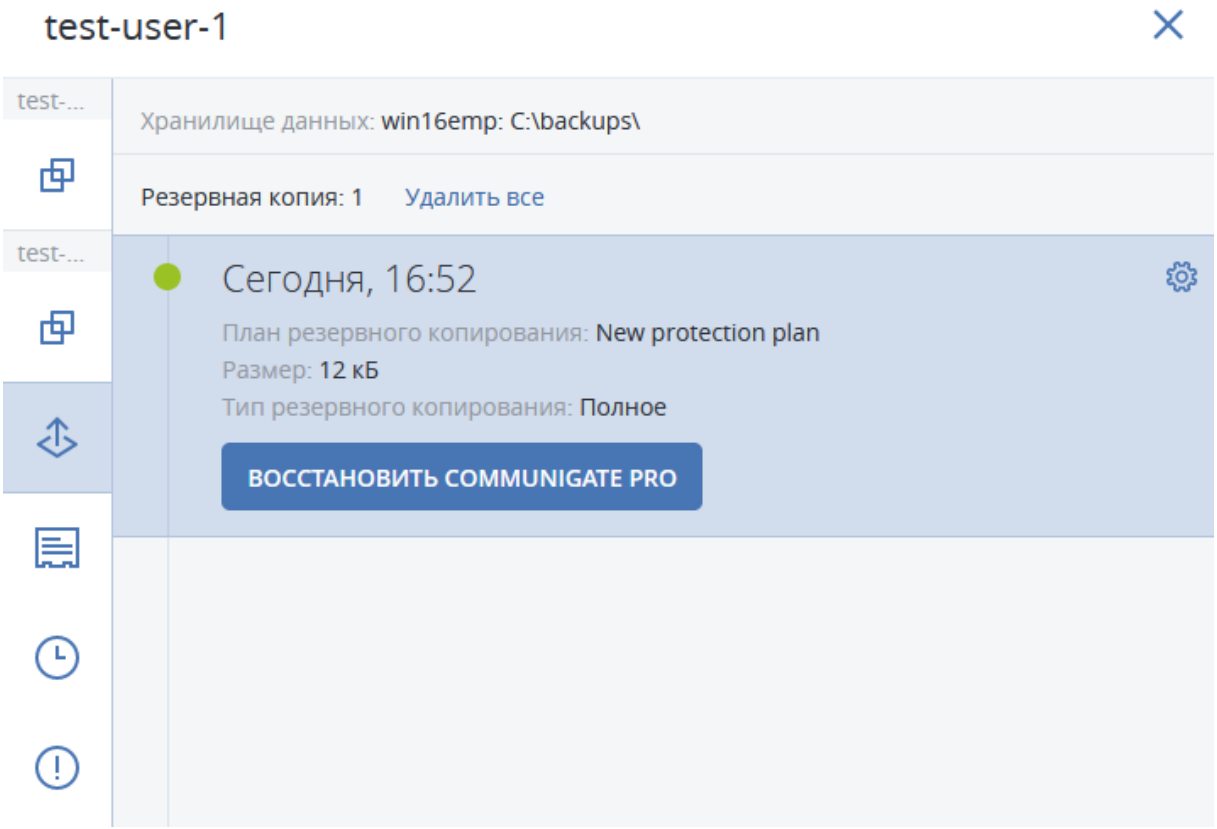
Порядок восстановления почтового ящика из резервной копии

1. Перейдите в **Устройства**.
2. Щелкните домен который хотите восстановить.
3. Выберите почтовый ящик в домене, который хотите восстановить.



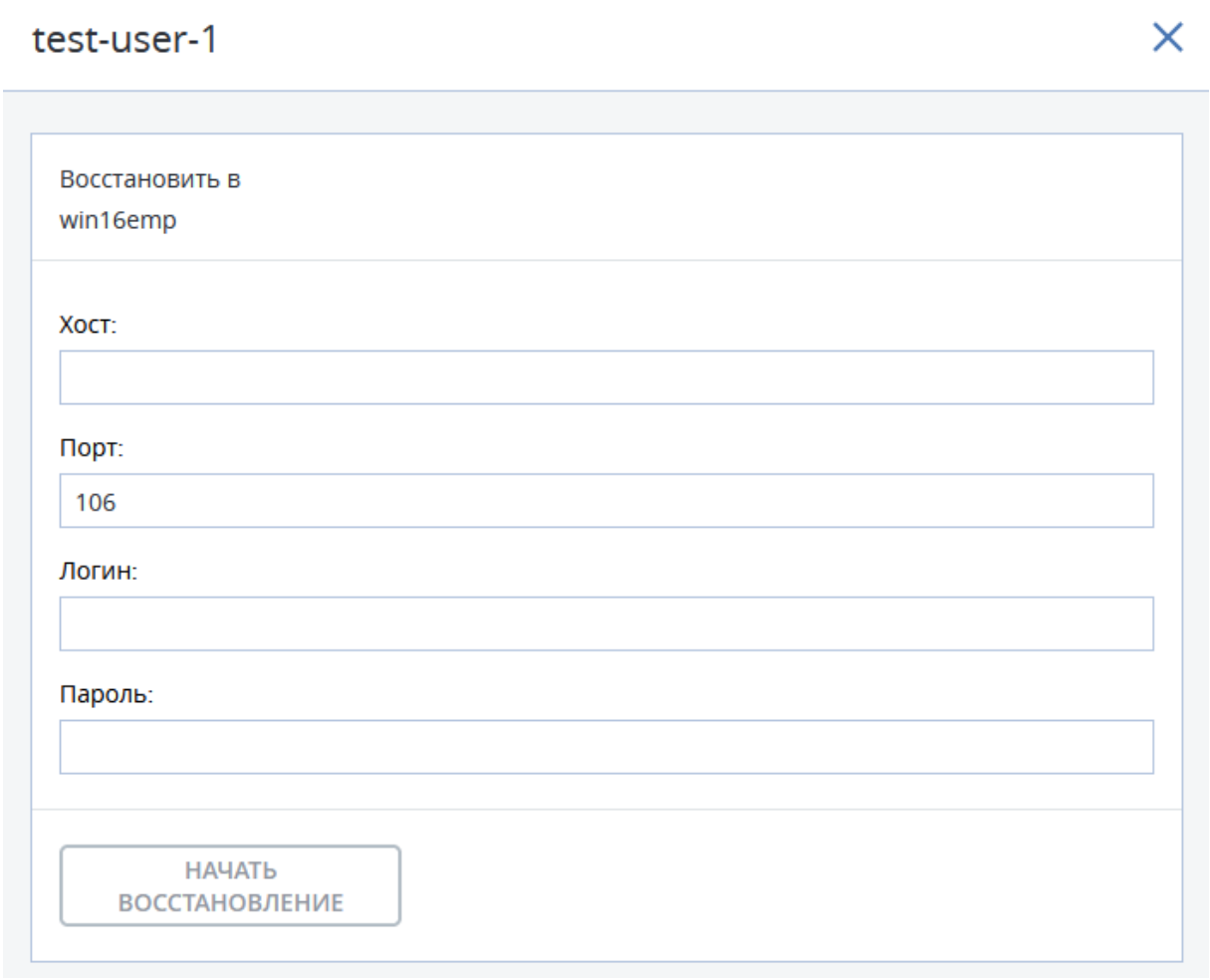
4. Перейдите на вкладку **Восстановление** справа в меню.

5. В списке резервных копий выберите резервную копию, которую хотите восстановить, и нажмите **Восстановить CommuniGate Pro**.



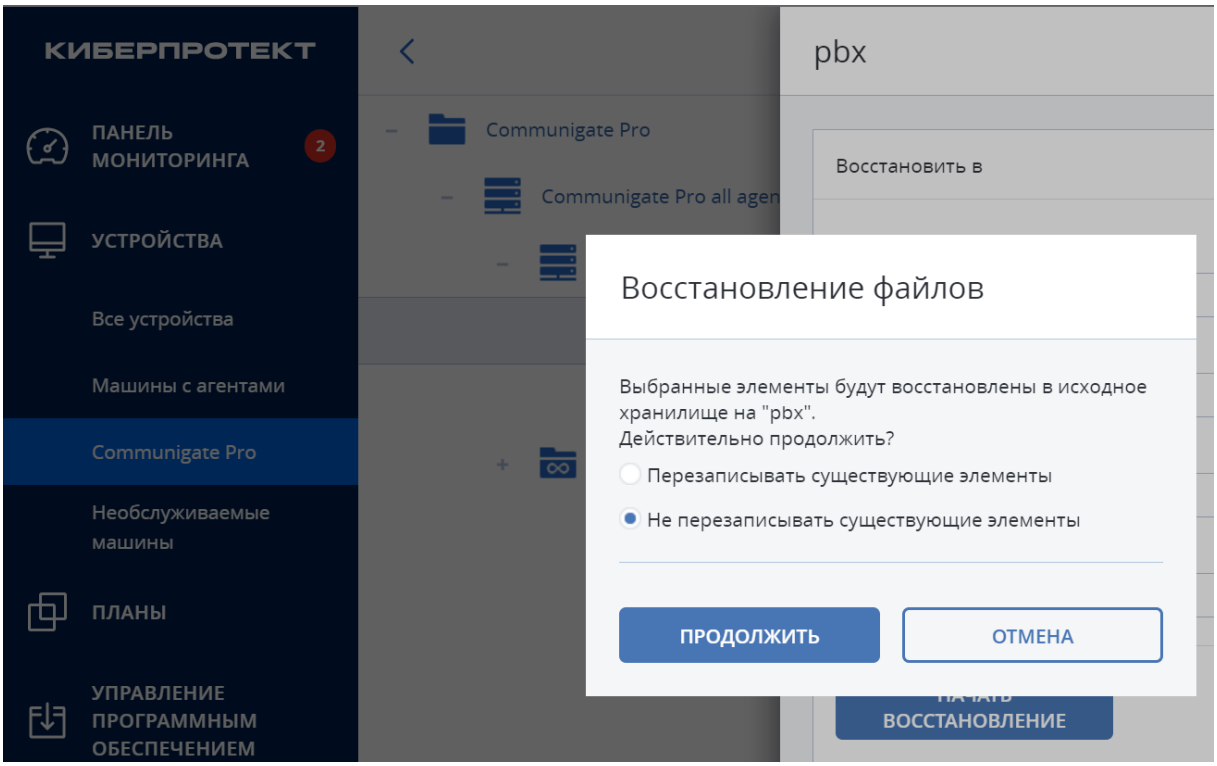
6. Заполните поля в новом окне. Укажите данные для места восстановления:

- адрес хоста, куда хотите восстановить данные
- логин и пароль пользователя.



7. По окончании ввода данных нажмите **Начать восстановление**.

При появлении окна выбора перезаписи данных, отметьте, хотите ли вы перезаписать существующие данные или хотите оставить уже существующую копию этих данных.



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.

После этого нажмите **Продолжить**. Данные из резервной копии будут восстановлены в указанное вами место.

Ход выполнения восстановления показан на вкладке **Действия**.

На вкладке **Восстановление** доступно также удаление резервной копии.

Чтобы удалить резервную копию:

- щелкните на резервную копию, которую хотите удалить
- щелкните значок настройки справа вверху
- нажмите **Удалить**.

Чтобы удалить все резервные копии, во вкладке **Восстановление** щелкните ссылку **Удалить все**.

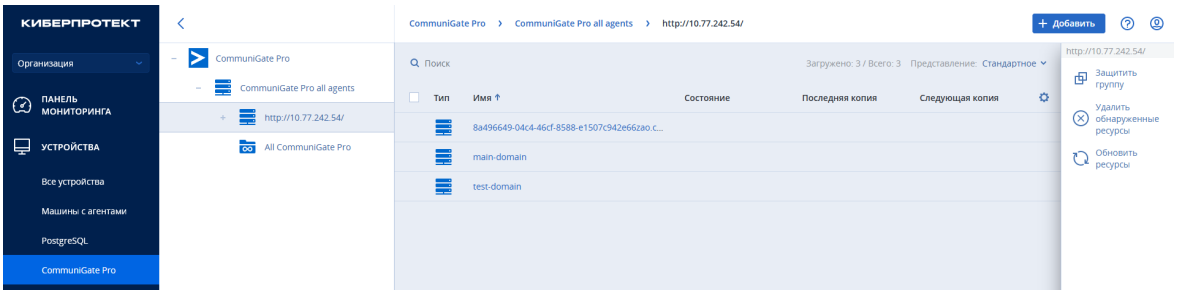
См. также Резервные копии CommuniGate Pro.

13.9 Удаление CommuniGate Pro

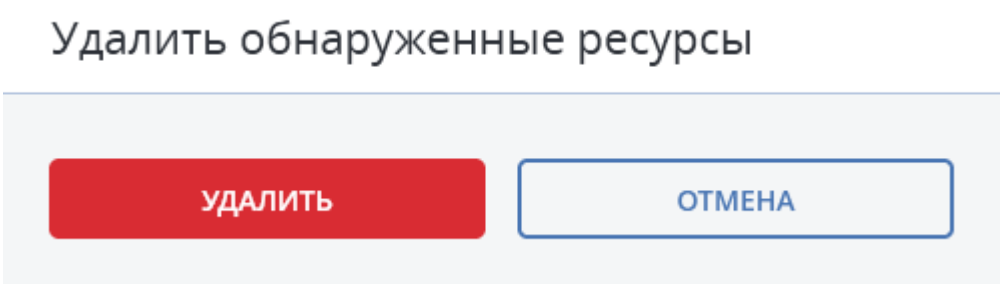
Вы можете удалить хост CommuniGate Pro отдельно, не удаляя сам агент и резервные копии.

Порядок удаления хоста CommuniGate Pro

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.

14 Защита VK WorkMail

14.1 Зачем обеспечивать защиту VK WorkMail

VK WorkMail - это масштабируемое и отказоустойчивое решение корпоративного класса для работы с почтой, календарем, контактами и для просмотра документов. С помощью Кибер Бэкап можно выполнять резервное копирование данных 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.

14.2 Что необходимо для резервного копирования

Для резервного копирования данных VK WorkMail понадобятся установленные и настроенные продукты:

- Кибер Бэкап 16.5 или новее с лицензией для почтовых ящиков (список лицензий см. в разделе "Выпуски и лицензирование Кибер Бэкап" (стр. 17)).
- VK WorkMail.

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).

14.3 Возможности

Кибер Бэкап обеспечивает резервное копирование и восстановление:

- почтовых ящиков пользователей VK WorkMail,
- отдельных писем пользователей VK WorkMail,
- сервера VK WorkMail.

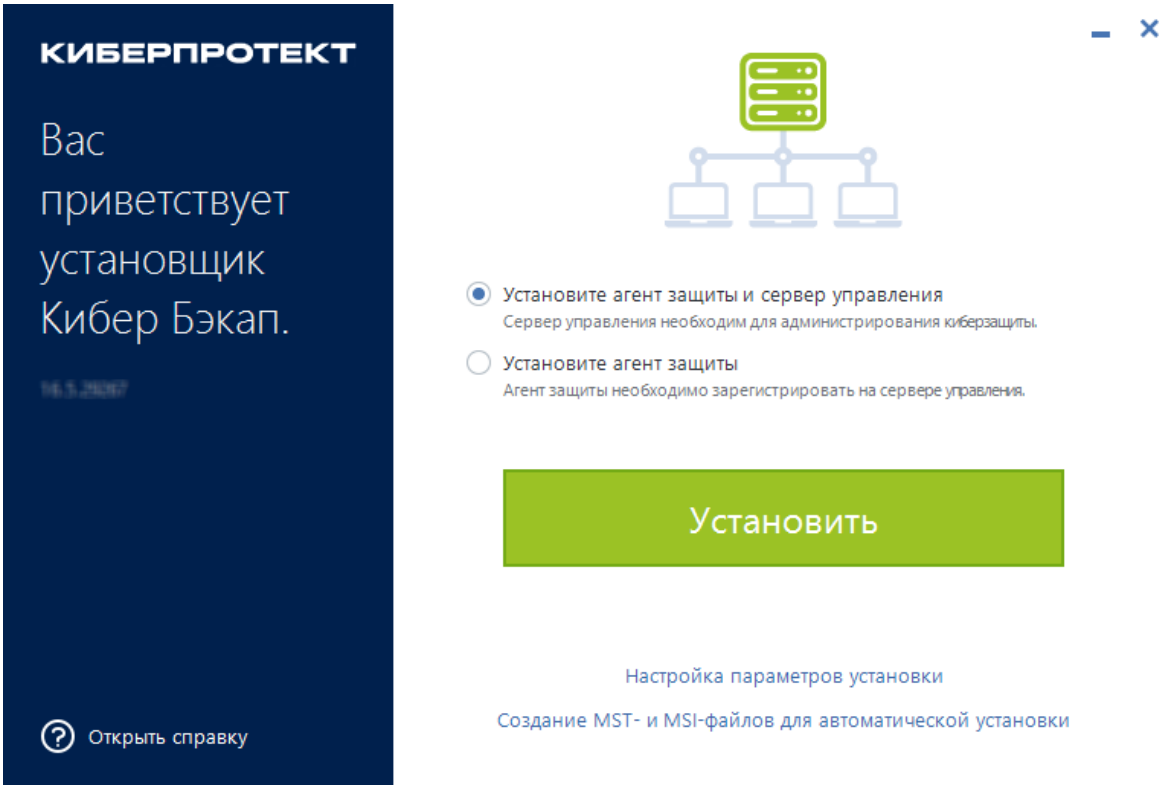
14.4 Установка VK WorkMail

Установка VK WorkMail включает в себя установку агента Кибер Бэкап и добавление хоста VK WorkMail. Добавление хоста возможно лишь после установки агента.

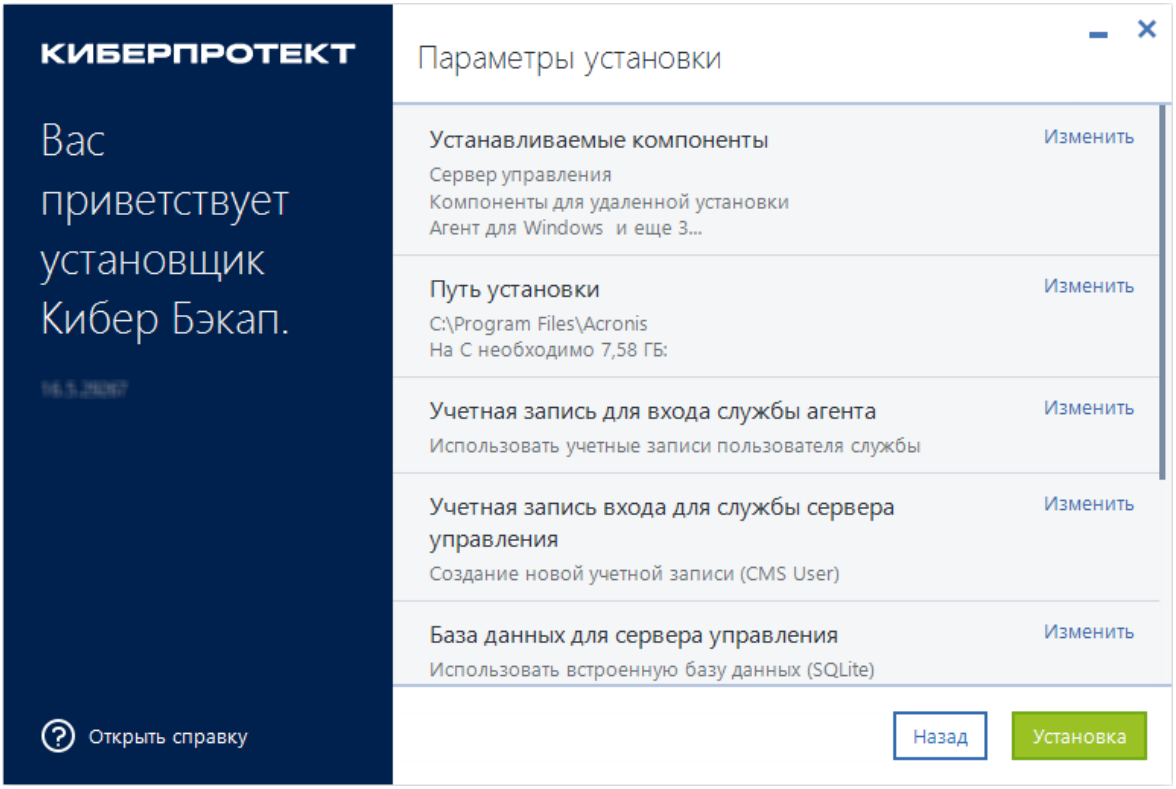
14.4.1 Установка агента для VK WorkMail

В этом разделе рассмотрена установка агента Кибер Бэкап для Windows. Для установки агента для Linux обратитесь к разделу "Установка в Linux" (стр. 81).

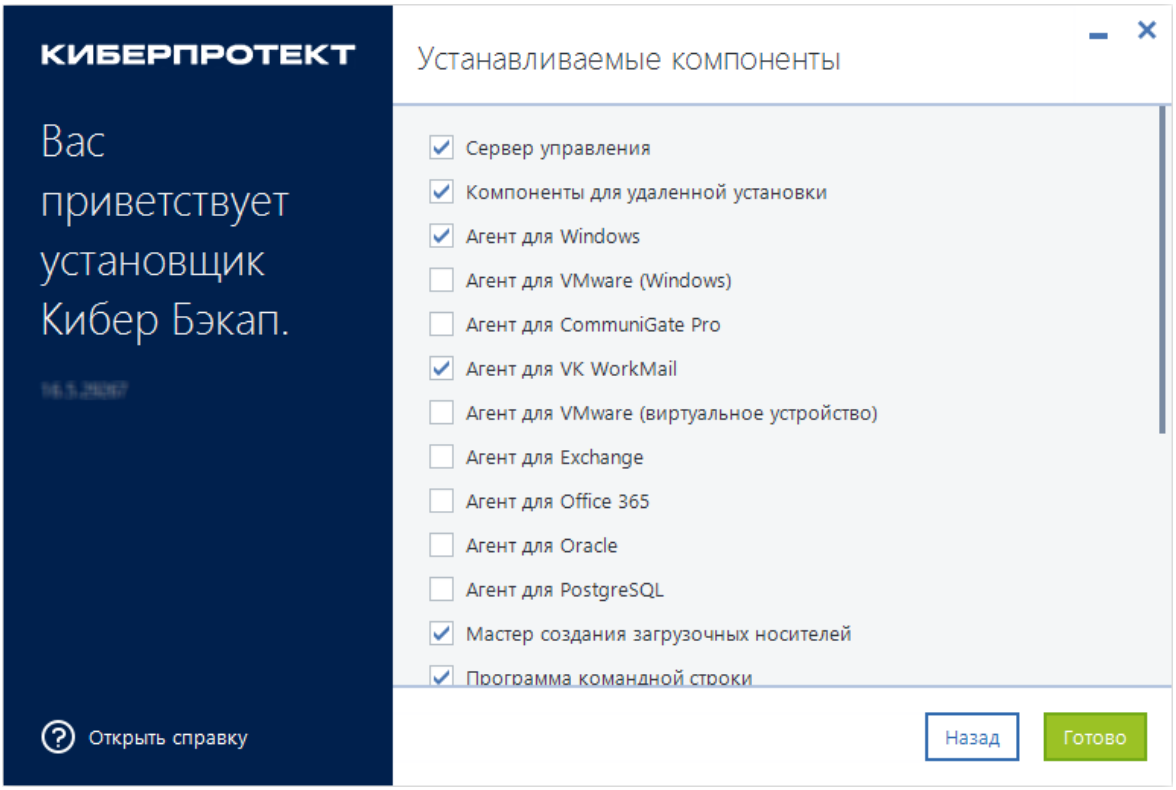
1. Запустите установщик Кибер Бэкап.
2. Выберите **Настройка параметров установки**.



3. В блоке **Устанавливаемые компоненты** выберите **Изменить**.



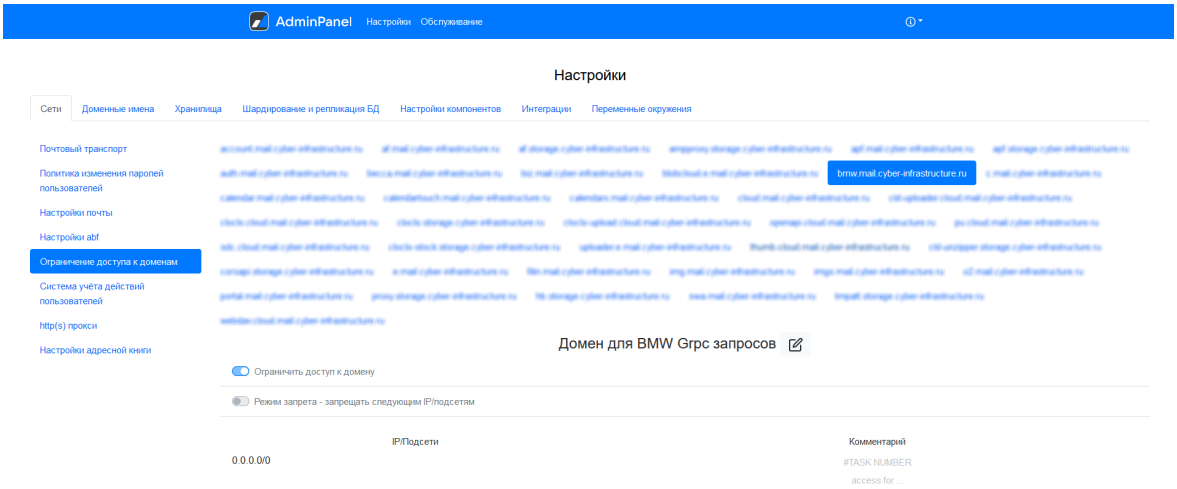
4. Отметьте в списке **Агент для VK WorkMail**.



5. Щелкните **Готово**.

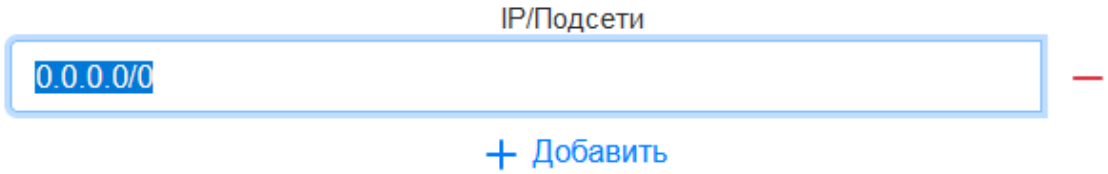
14.4.2 Настройка в панели администрирования VK WorkMail

1. Укажите настройки в панели администрирования VK WorkMail аналогично следующему примеру:

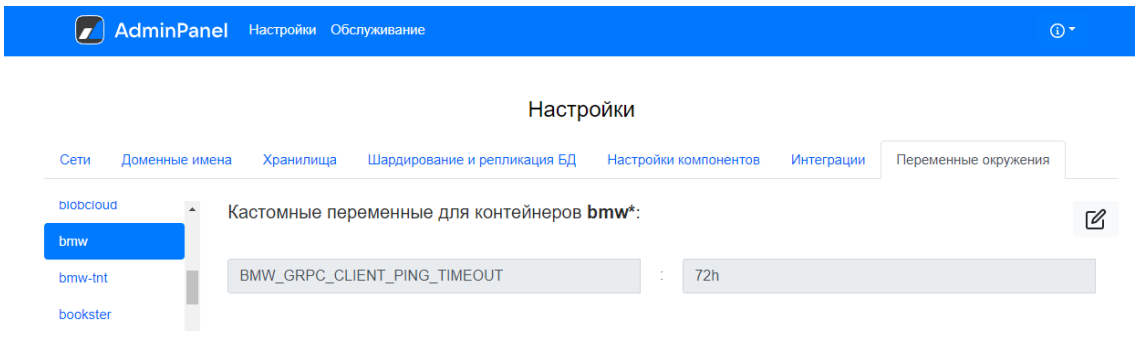


2. Для настройки IP-адреса нажмите значок редактирования

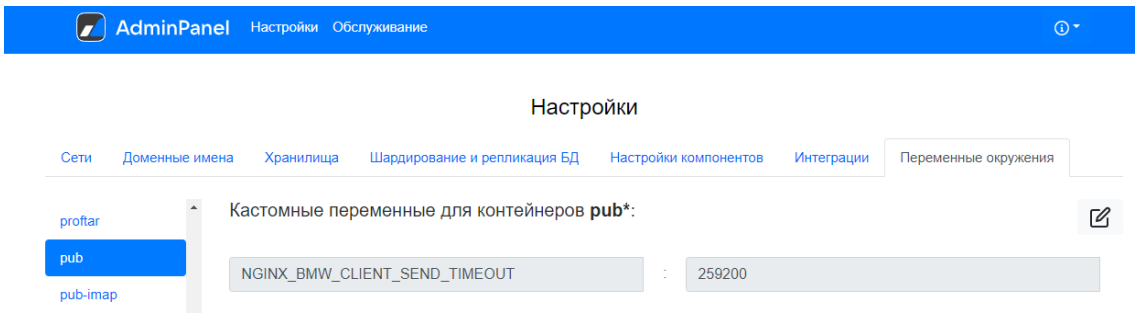
и введите IP-адрес компьютера, на который установлен агент для VK WorkMail.



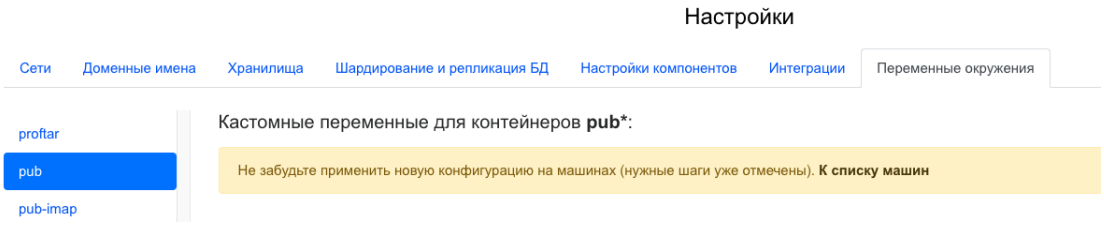
3. Нажмите **Сохранить**.
4. Добавьте переменные окружения:
   a. Перейдите в раздел **Настройки** и откройте вкладку **Переменные окружения**.
   b. В списке слева выберите контейнер **bmw**, создайте переменную BMW_GRPC_CLIENT_PING_TIMEOUT и укажите для нее значение 72h.



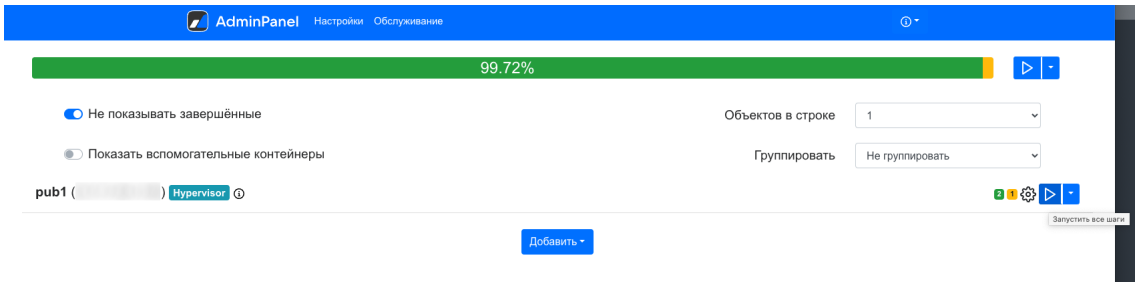
c. В списке слева выберите контейнер **pub**, создайте переменную NGINX_BMW_CLIENT_SEND_TIMEOUT и укажите для нее значение 259200.



d. Откройте экран со списком машин, перейдя по ссылке **К списку машин**.

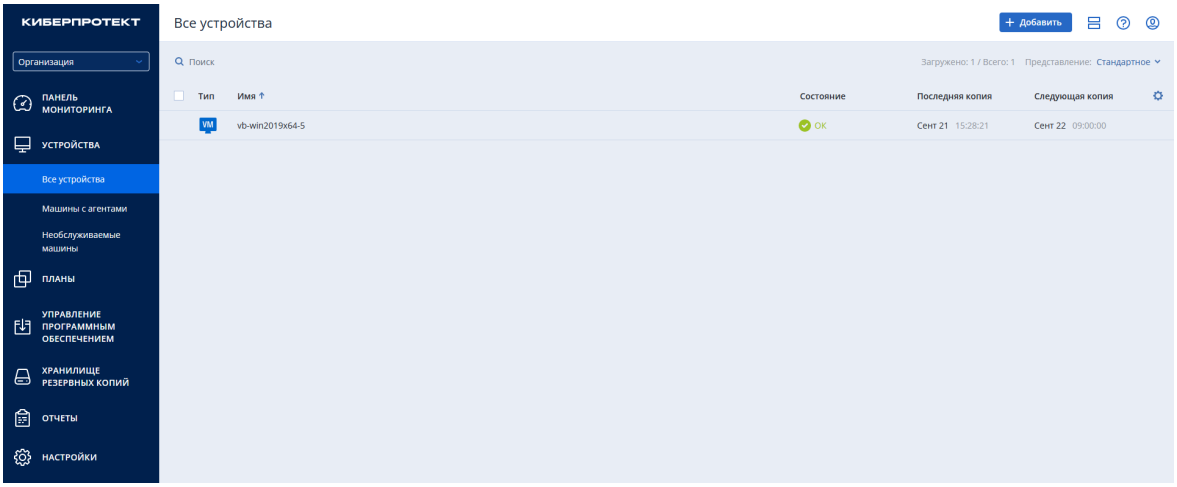


e. Примените изменения для обоих типов контейнеров, нажав на значок запуска  .

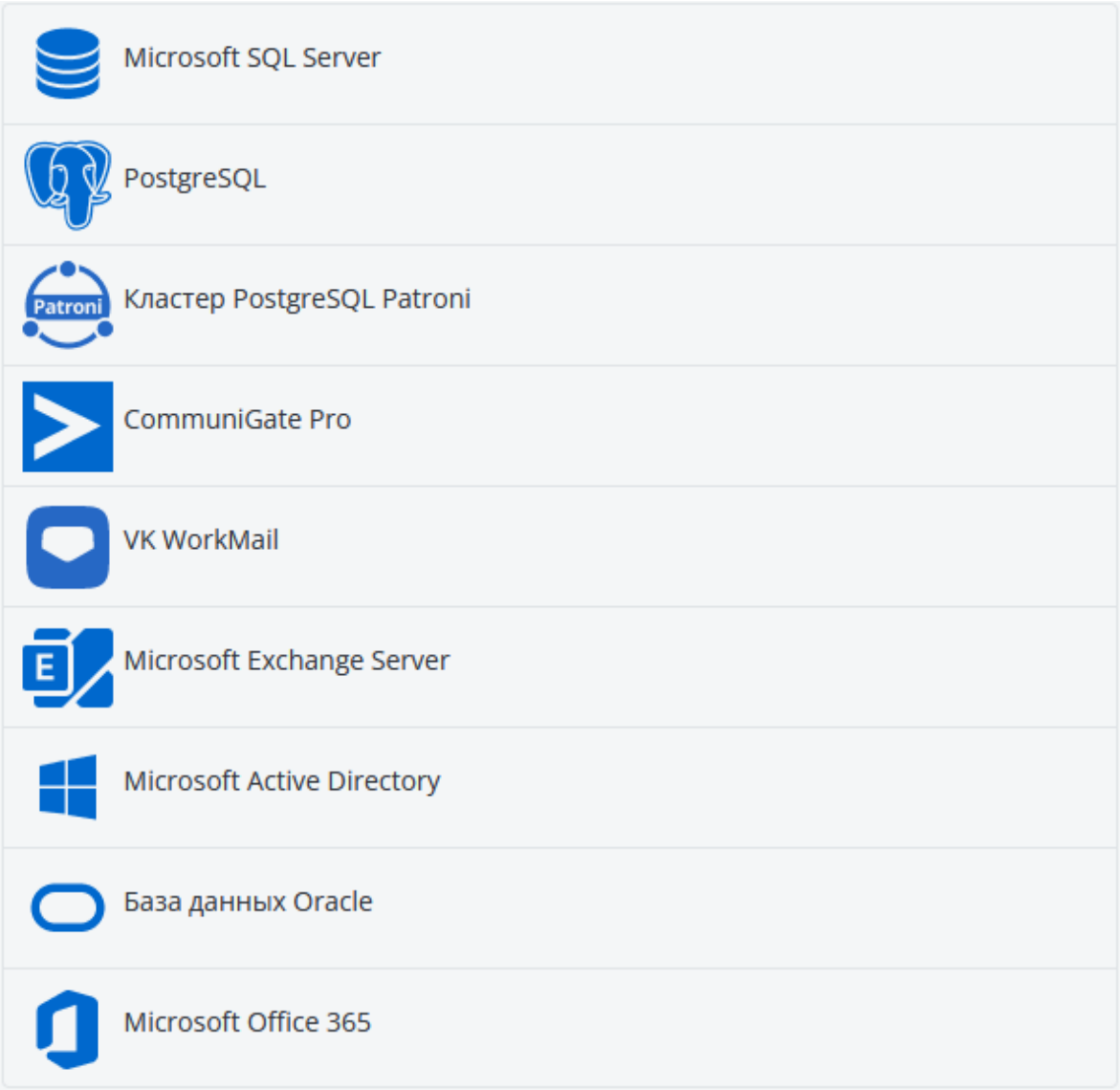


14.4.3 Добавление хоста VK WorkMail

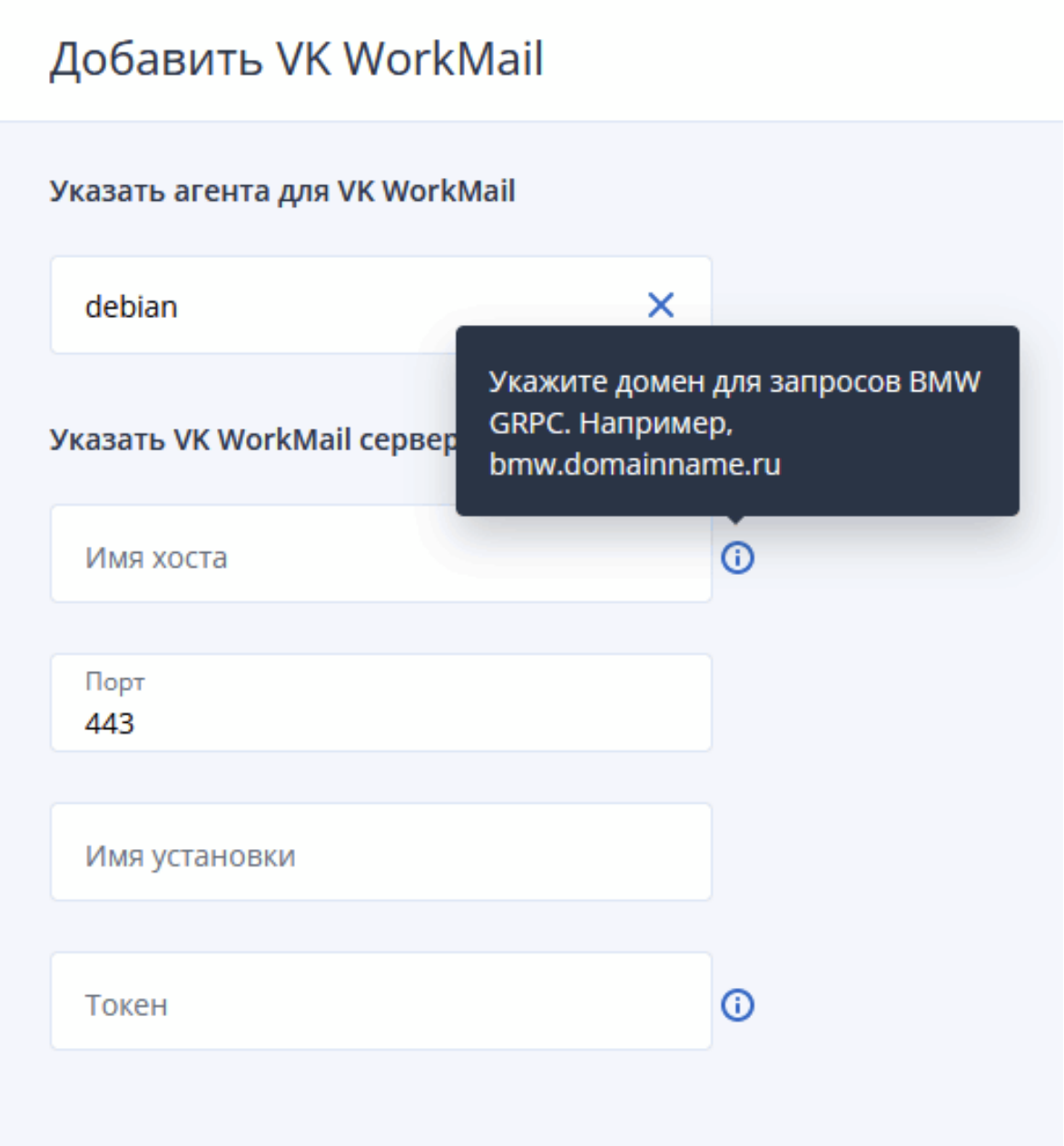
1. В веб-консоли перейдите на вкладку **Устройства** и нажмите в правом верхнем углу **Добавить**.



2. В окне добавления нового устройства щелкните VK WorkMail.



3. Заполните поля:
   - 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.



4. По окончании ввода данных нажмите **Добавить**.

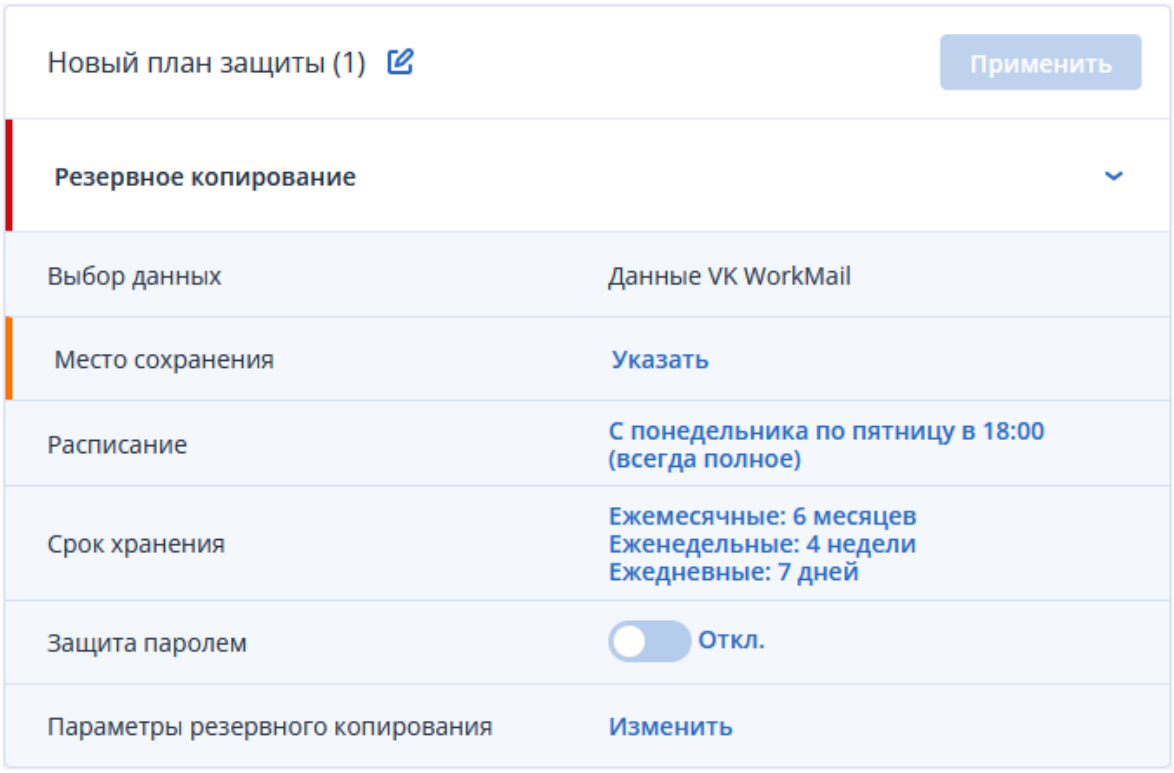
14.5 Резервное копирование VK WorkMail

14.5.1 Резервное копирование данных пользователей VK WorkMail

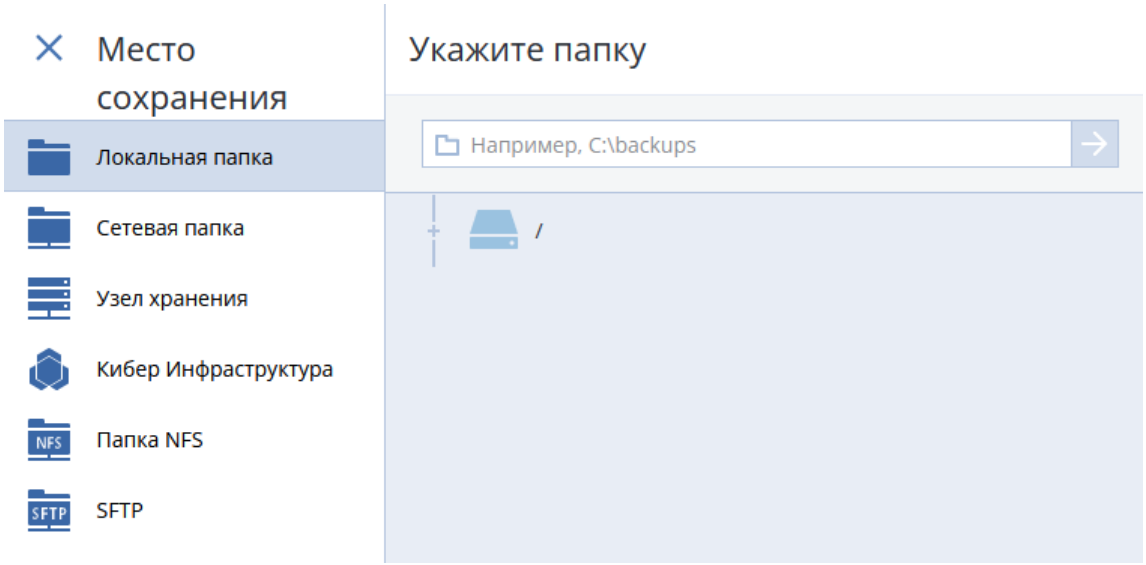
Для создания плана защиты выполните следующие действия:

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.

3. Перейдите на вкладку справа **Защитить** для защиты почтового ящика или группы почтовых ящиков (домена).



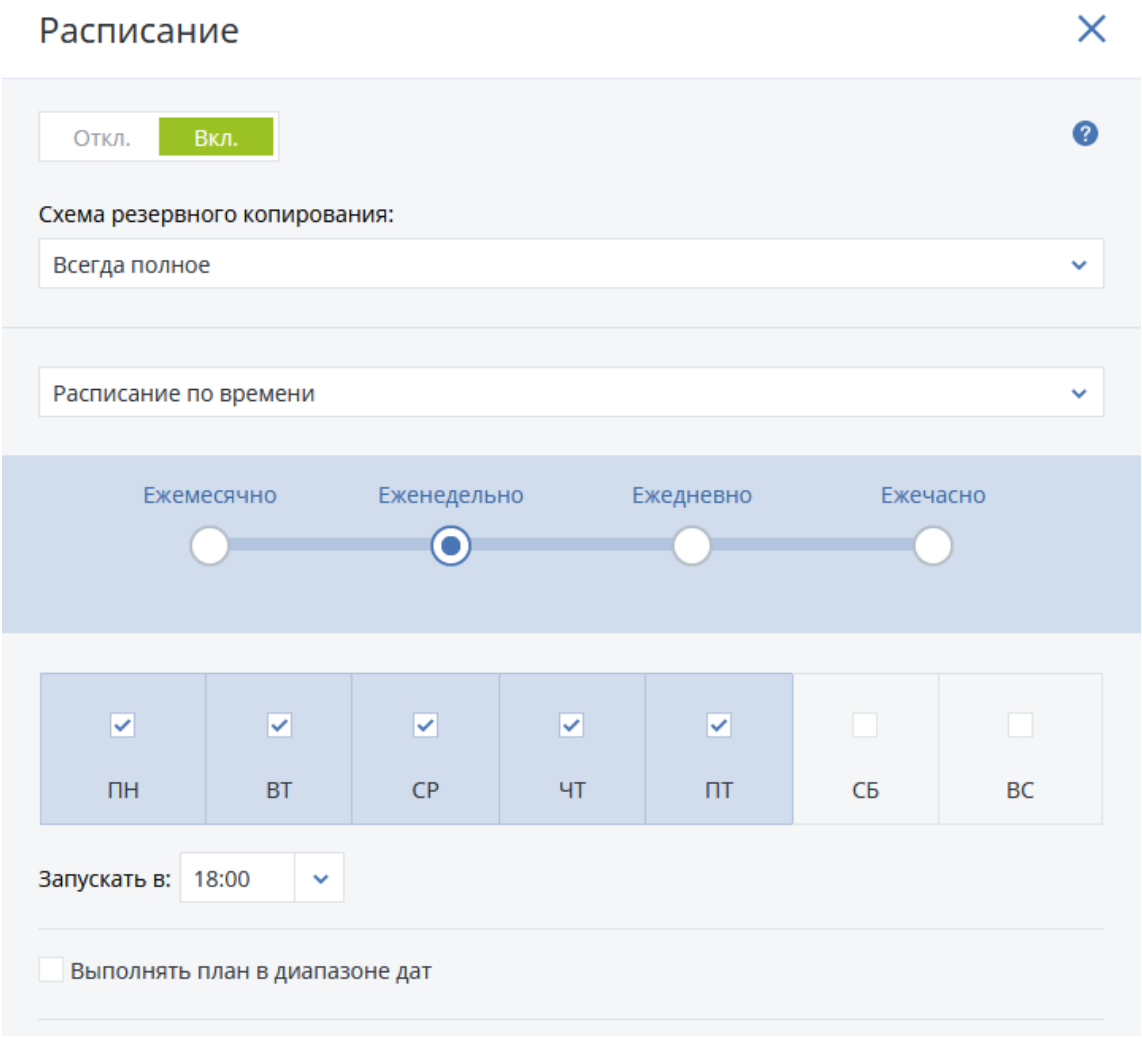
4. Заполните данные в окне создания плана защиты:
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура, папка NFS, SFTP.



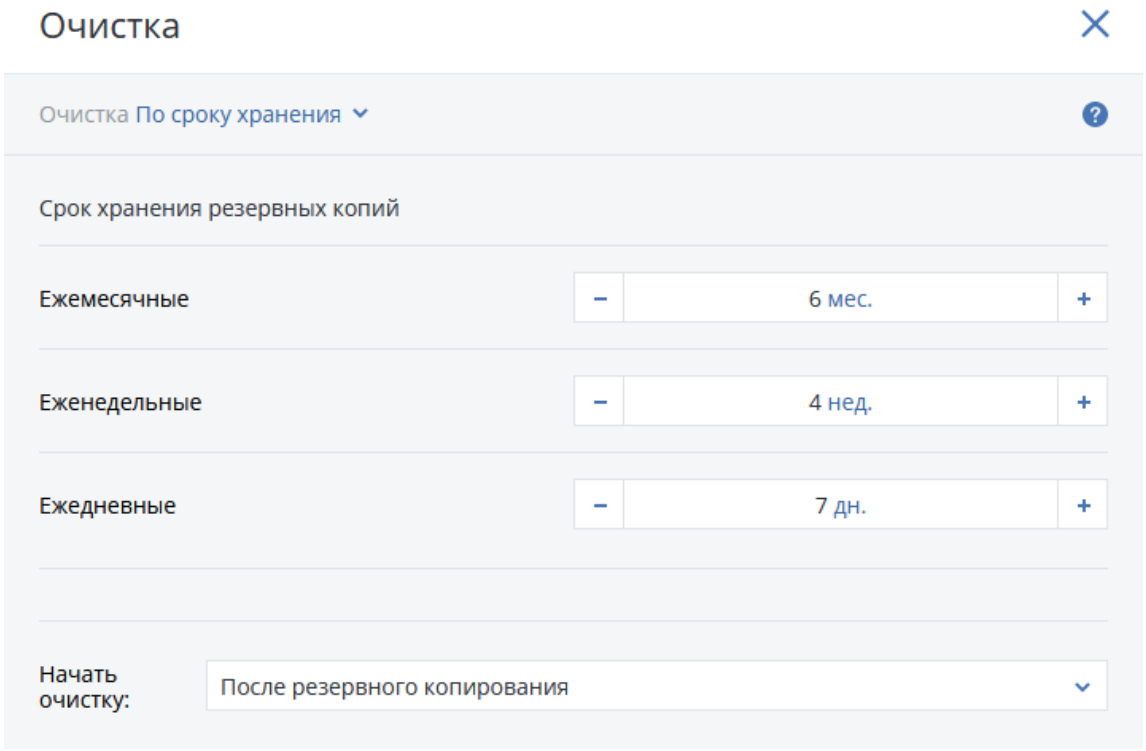
   Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места назначения" (стр. 180).

Внимание
Для резервного копирования на ленты через узел хранения выполните шаги из раздела "Особенности резервного копирования VK WorkMail на ленты" (стр. 411).

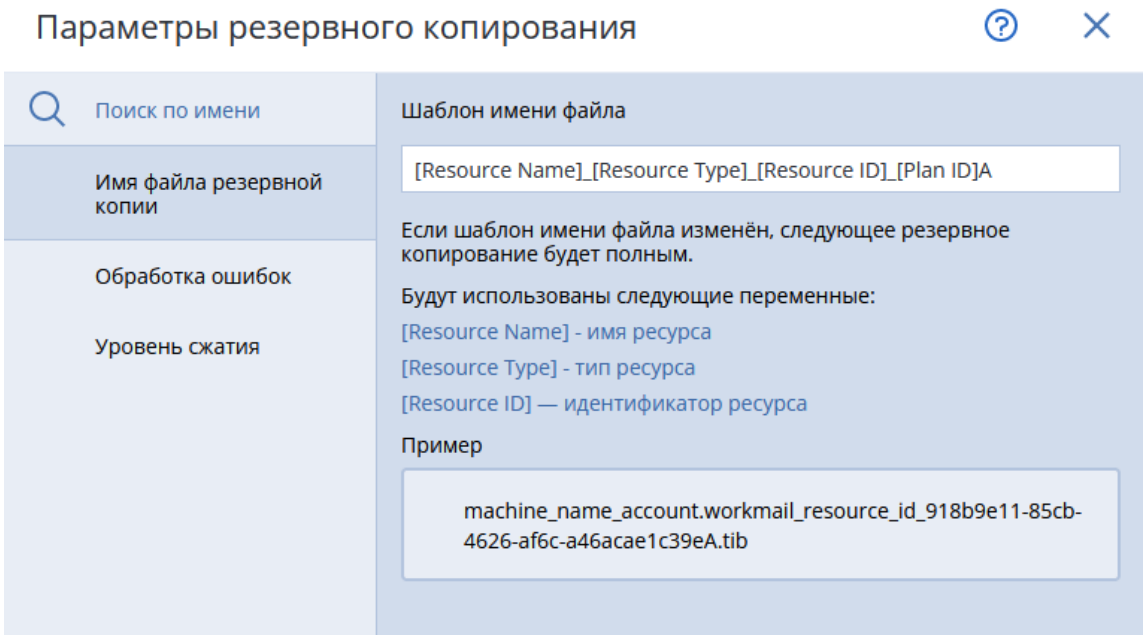
- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.



- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.



- [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. 157).

14.5.2 Резервное копирование сервера VK WorkMail

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, предоставленные VK.
3. Прочитайте инструкцию, предоставленную VK.

Резервное копирование

Настройте план резервного копирования в соответствии с инструкцией, предоставленной VK, как описано далее.

1. Скопируйте в директорию, например в /tmp, файлы программы, предоставленные VK: 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
   ```

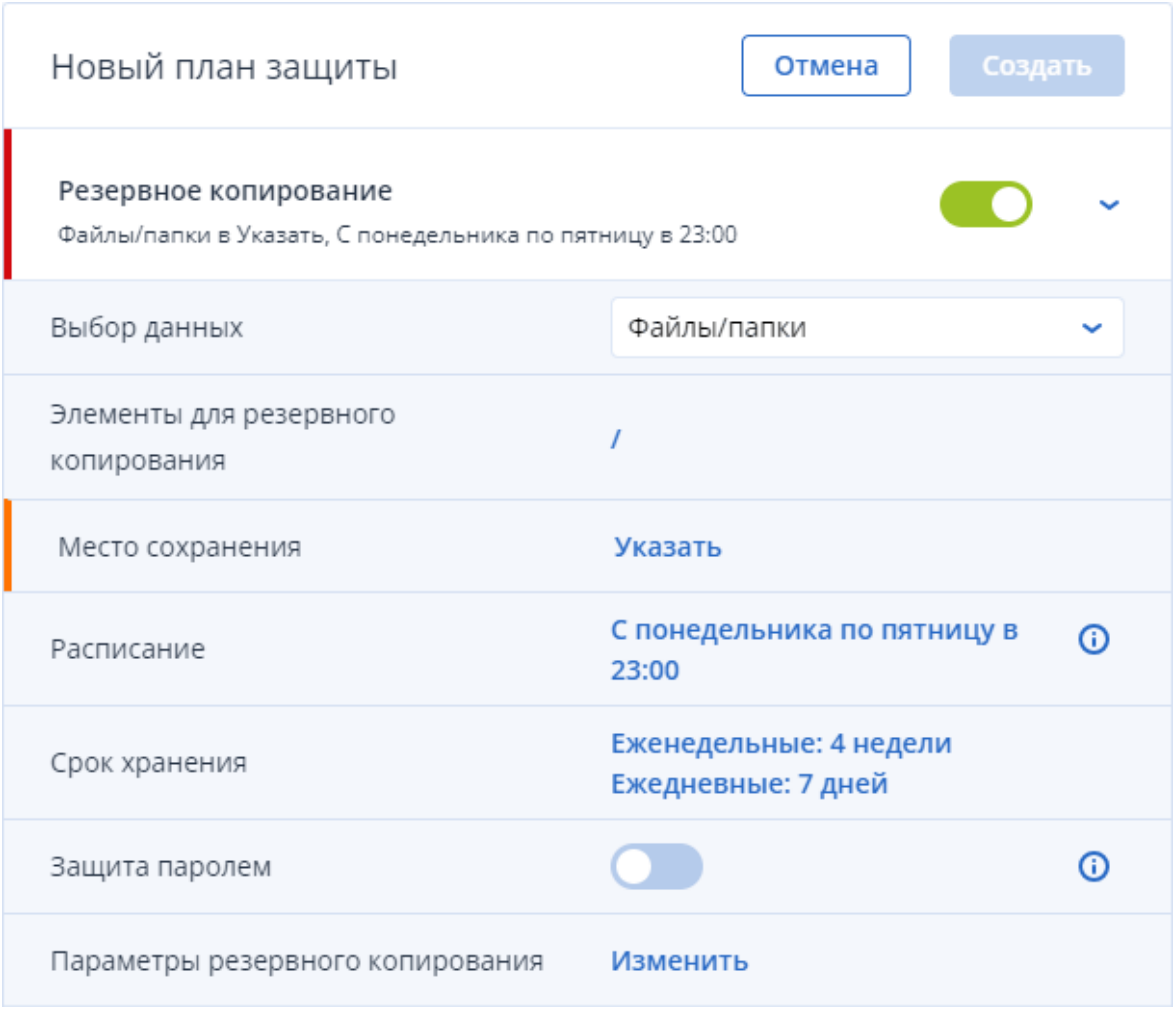
   здесь script_dir – путь к mnt-backup, main_dir – путь, куда будут сохраняться базы данных.
4. Запустите скрипт вручную до создания плана защиты, чтобы получить пути, которые нужно защитить и которые необходимо добавить в исключения (exclude) задачи резервного копирования:

   ```
   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** -> **Все устройства**.

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**.



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
```

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.

14.5.3 Особенности резервного копирования VK WorkMail 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>
```

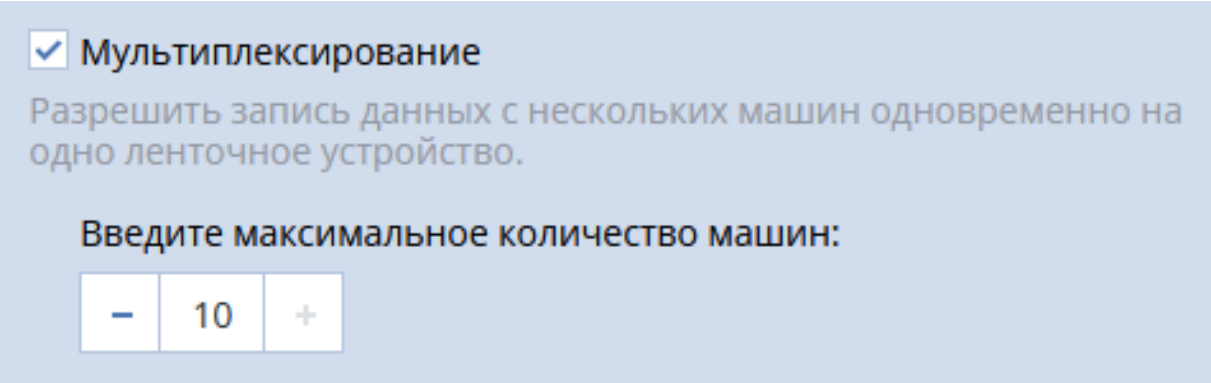
и перезапустить службу узла хранения.

- 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. 242).

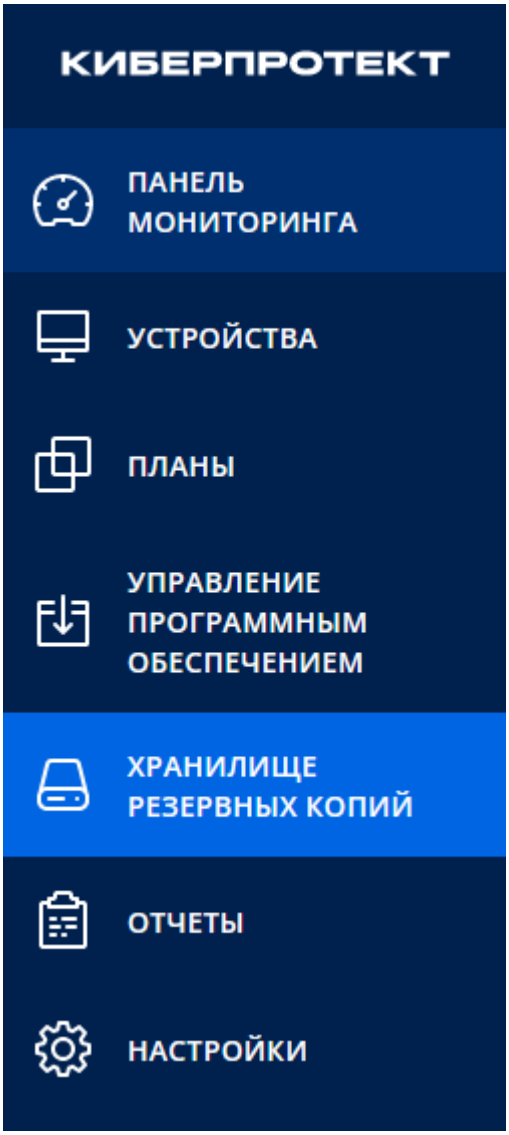


14.6 Восстановление VK WorkMail

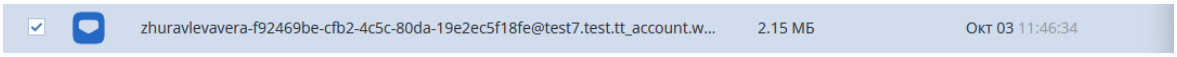
14.6.1 Восстановление данных пользователей VK WorkMail

Чтобы восстановить данные пользователей VK WorkMail, выполните следующие действия:

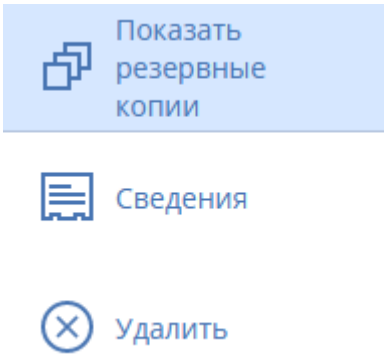
1. Перейдите в **Хранилище резервных копий**.



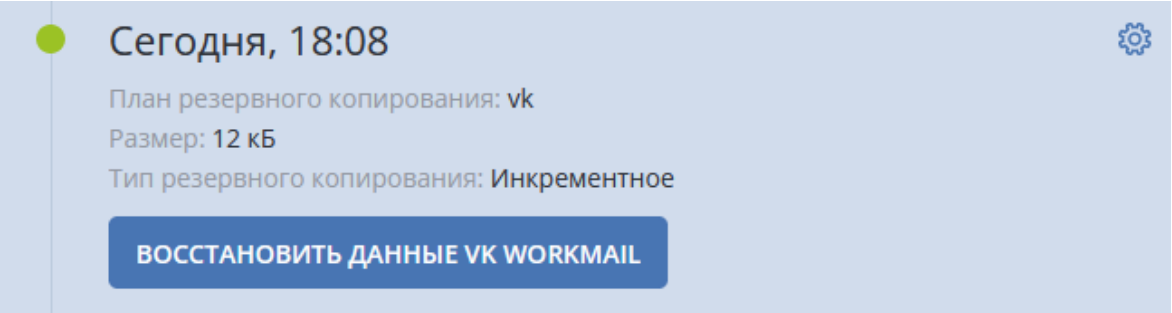
2. Выберите в списке нужную резервную копию.



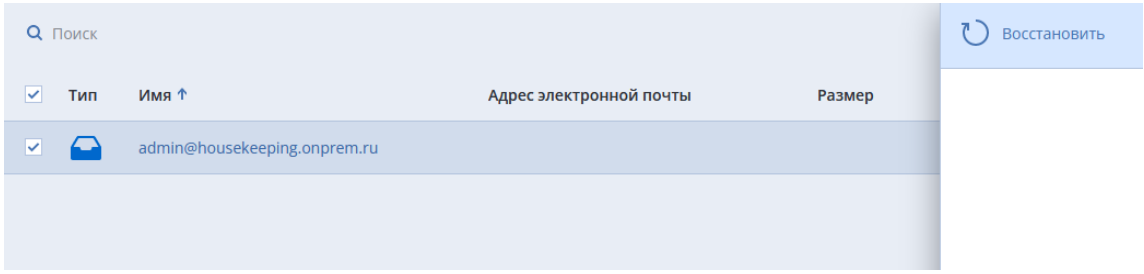
3. Выберите справа **Показать резервные копии**.



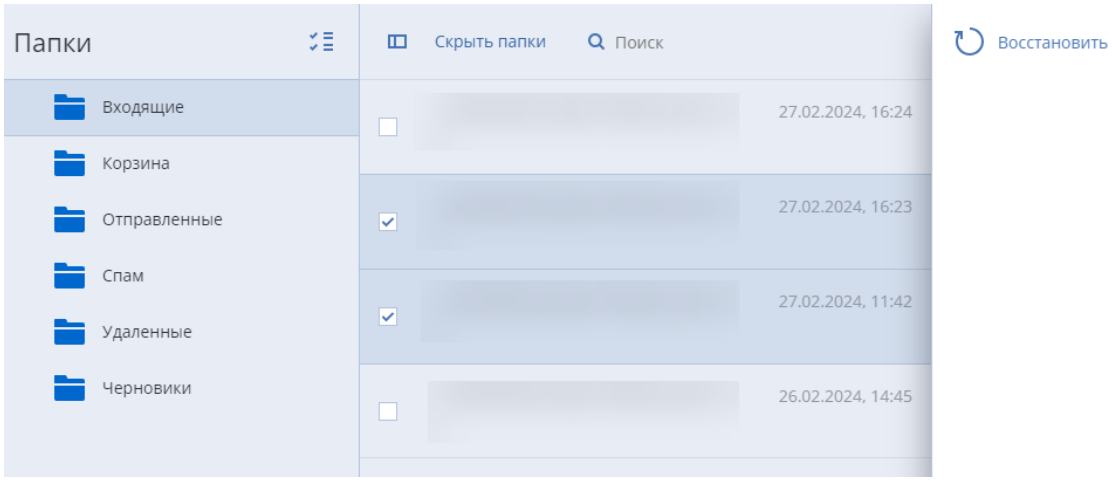
4. Нажмите **Восстановить данные VK WorkMail**.



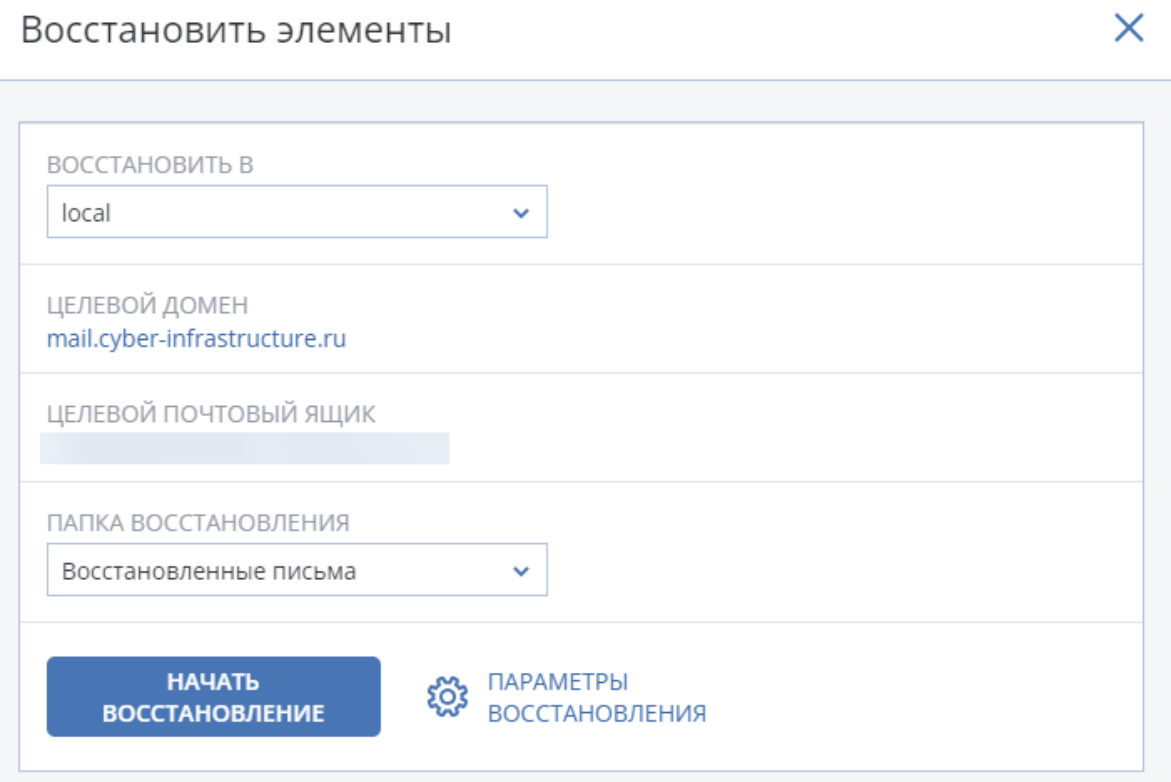
5. Выберите данные для восстановления:
   - Если необходимо восстановить весь почтовый ящик, отметьте галочкой в списке имя почтового ящика, затем выберите справа **Восстановить**.



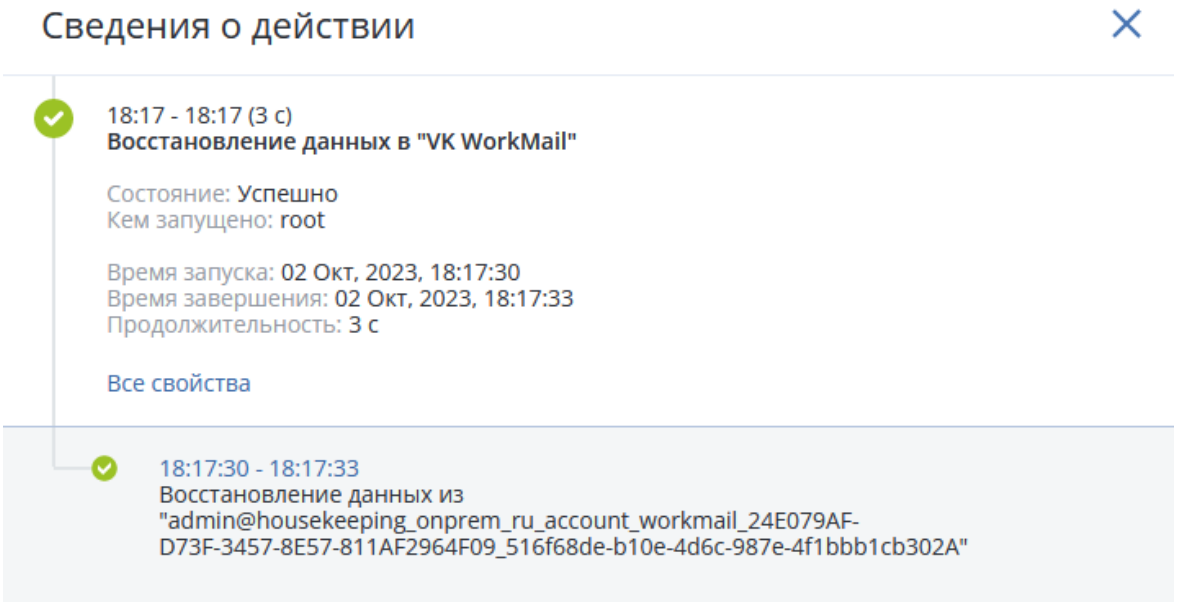
   - Если необходимо восстановить отдельные письма, нажмите на имя резервной копии и выберите письма, затем нажмите справа **Восстановить**.



6. Проверьте правильность заполнения полей и затем нажмите **Начать восстановление**.



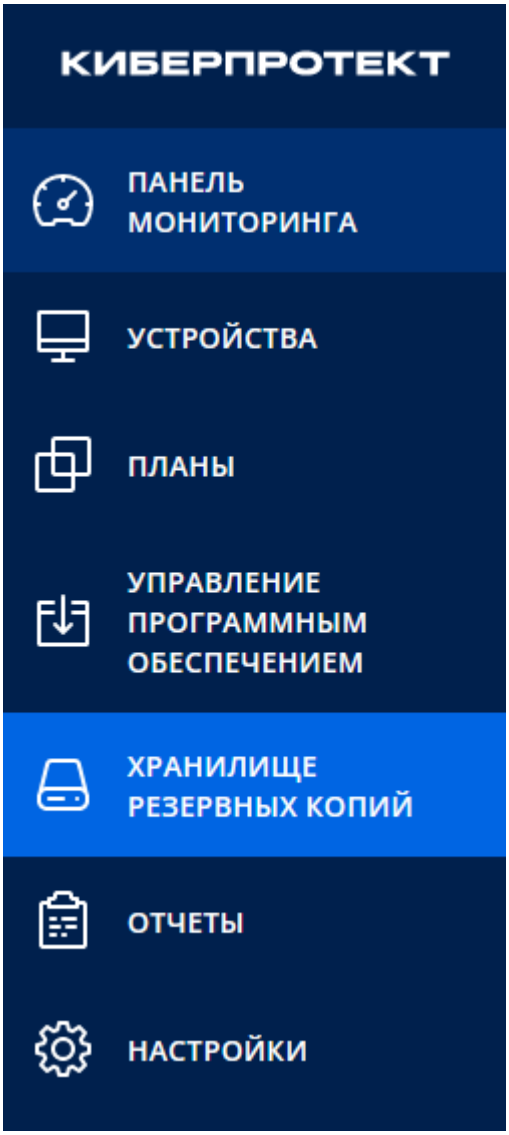
7. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.



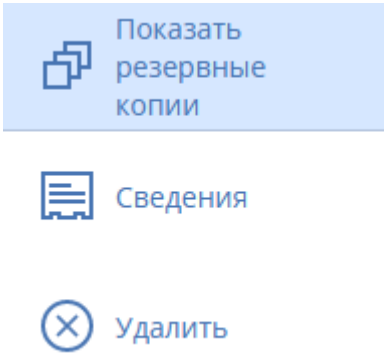
14.6.2 Просмотр писем VK WorkMail

Чтобы просмотреть письма пользователя VK WorkMail, выполните следующие действия:

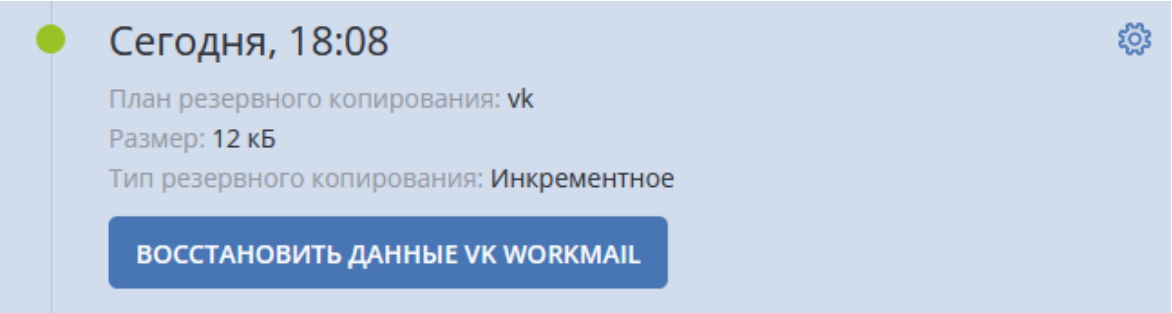
1. Перейдите в **Хранилище резервных копий**.



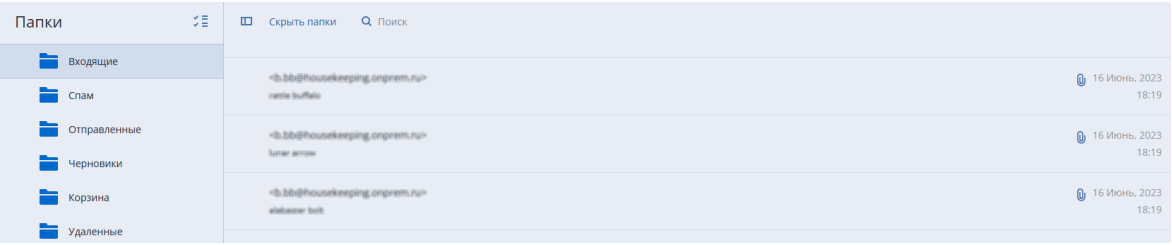
2. Выберите нужное хранилище, щелкните в списке нужную резервную копию.
3. Выберите справа **Показать резервные копии**.



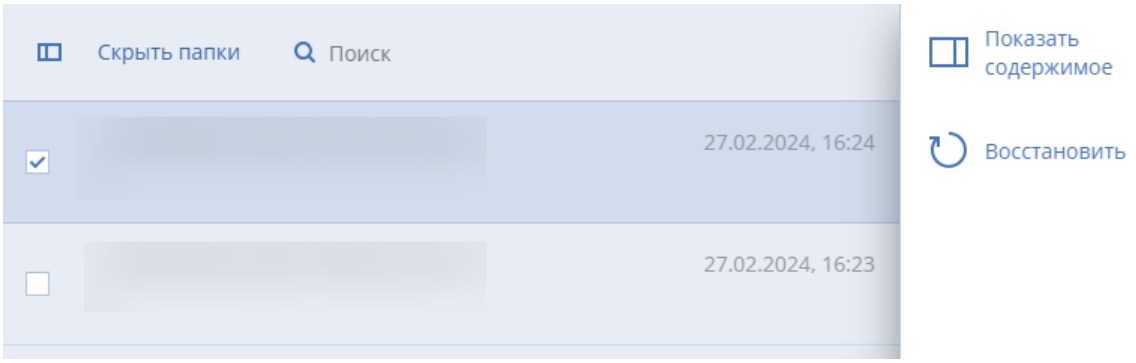
4. Щелкните **Восстановить данные VK WorkMail**.



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.

14.6.3 Восстановление сервера VK WorkMail

14.6.3.1 Восстановление данных на новую машину

Для восстановления резервной копии сервера VK WorkMail, созданной по инструкции в разделе "Резервное копирование сервера VK WorkMail" (стр. 409), выполните следующие действия:

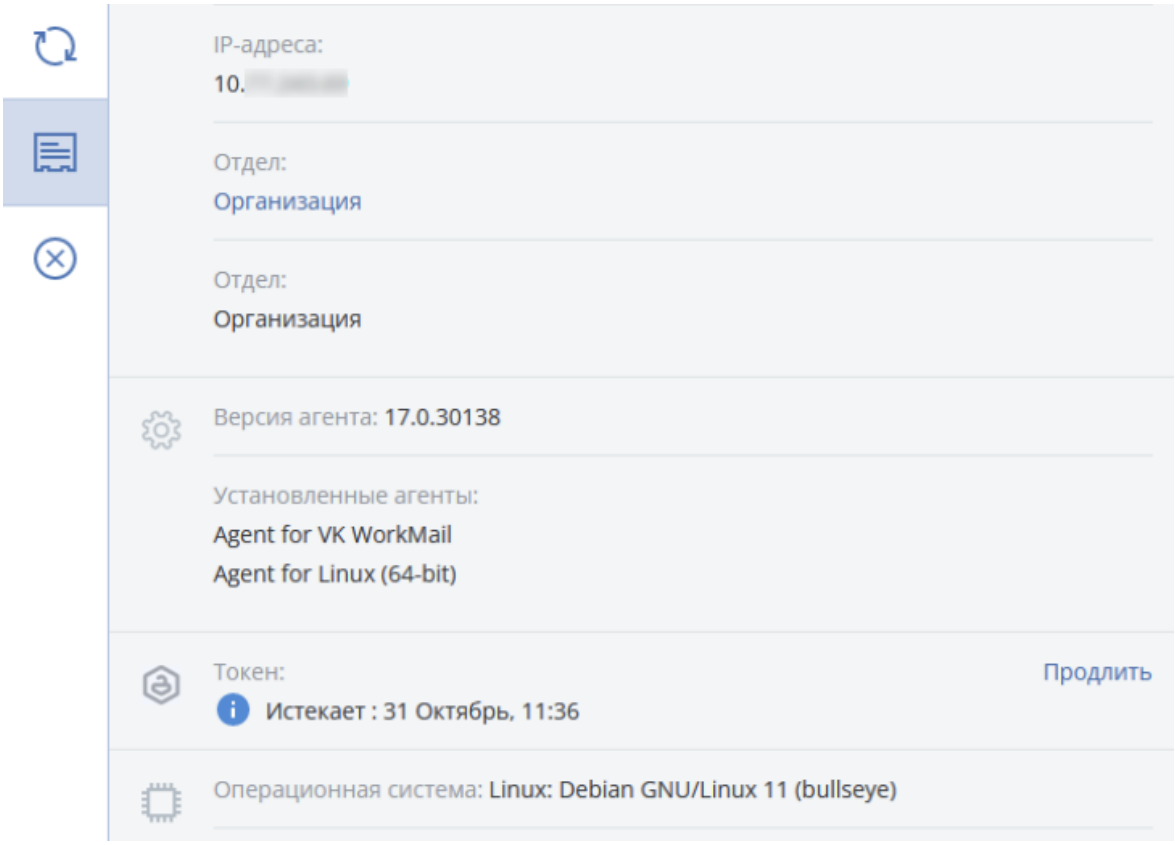
1. Выключите исходную машину.
2. Для новой машины установите такой же IP-адрес, как для исходной.
3. Установите на новую машину агент Кибер Бэкап для Linux.
4. Восстановите данные в соответствующие директории, следуя шагам в разделе "Восстановление гипервизора" инструкции, предоставленной VK.

14.7 Обновление токена VK WorkMail

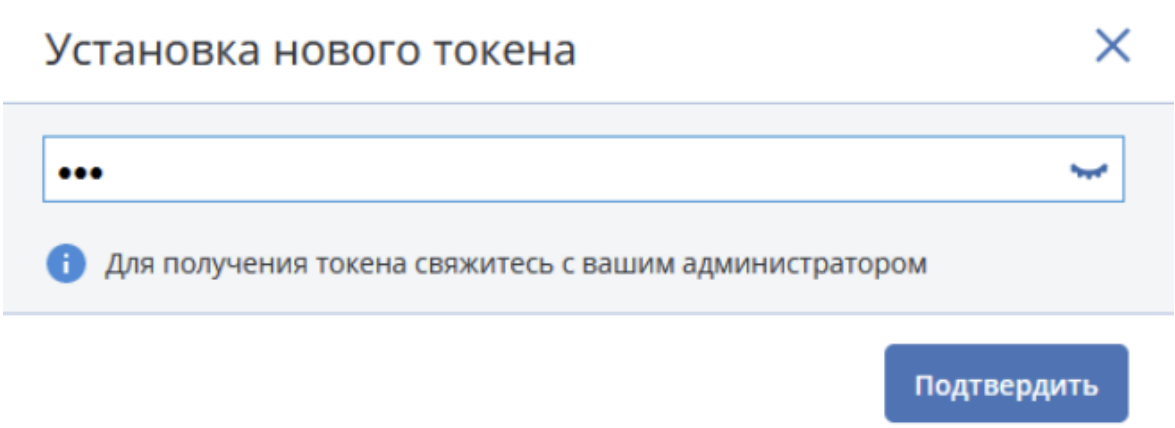
Для обнаружения, резервного копирования и восстановления данных устройства VK WorkMail Кибер Бэкап использует gRPC API, предоставляемый VK WorkMail, при обращениях к которому Кибер Бэкап передает токен для авторизации запросов. Токен обладает ограниченным сроком действия, поэтому его необходимо заблаговременно 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.



Если необходимо обновить токен, щелкните **Продлить**, укажите новый токен и нажмите **Подтвердить**.



15 Защита Oracle Database

Защита Oracle Database описана в отдельном документе, который доступен по ссылке https://docs.cyberprotect.ru/ru-RU/CyberBackup/16.5/OracleBackup.pdf.

16 Защита баз данных PostgreSQL

Установка и настройка компонентов программы для резервного копирования баз PostgreSQL, Postgres Pro и кластера PostgreSQL на базе Patroni описаны в отдельном документе, который доступен по ссылке https://docs.cyberprotect.ru/ru-RU/CyberBackup/16.5/PostgreSQLBackup.pdf.

17 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.

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 (64-разрядная версия).

Чтобы загрузить установочный файл агента для Linux (64-бит)

1. Войдите в веб-консоль Кибер Бэкап.
2. Нажмите на значок учетной записи в правом верхнем углу и затем выберите **Загрузки**.
3. Выберите **Агент для Linux (64-бит)**.

   Установочный файл будет загружен на ваш компьютер. Чтобы установить агента, выполните действия, как описано в разделе "Установка агентов" (стр. 142) или "Автоматическая установка или автоматическое удаление в Linux" (стр. 91). Убедитесь, что вы выбрали опцию Агент для MySQL/MariaDB.

17.0.1 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.

17.0.2 Известные проблемы и ограничения

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***.

* См. также Известные проблемы версии 16.5.

17.1 Настройка резервного копирования с поддержкой приложений

17.1.0.1 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

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**.

17.2 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 MariaDB	Вся машина	Компьютер*, на котором установлен агент для Linux
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

Что восстановить	Опция восстановления	Путь восстановления
		• Новая таблица

* С точки зрения резервного копирования, виртуальная машина с агентом внутри рассматривается как физическая машина.

17.2.1 Восстановление всего сервера

Чтобы узнать, как восстановить весь сервер, на котором запущены экземпляры MySQL или MariaDB, обратитесь к разделу "Восстановление машины" (стр. 252).

17.2.2 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:

   - 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 **Хранилище 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**.

17.2.3 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 **Хранилище 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.
   - 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**.

17.2.4 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 **Хранилище 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. 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**.

18 Защита баз данных Ред База Данных

Установка и настройка компонентов программы для резервного копирования баз данных Ред База Данных описаны в отдельном документе, который доступен по ссылке https://docs.cyberprotect.ru/ru-RU/CyberBackup/16.5/RedBDBackup.pdf.

19 Защита баз данных MongoDB

Данные MongoDB можно защитить с помощью резервного копирования с использованием встроенных инструментов MongoDB (например, утилит mongodump и mongorestore). При этом обеспечивается восстановление на уровне серверов СУБД, баз данных и коллекций MongoDB.

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. 142) или "Автоматическая установка или автоматическое удаление в Linux" (стр. 91).

19.1 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.

19.1.1 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.

19.1.2 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.

19.1.3 Создание скрипта с командами для утилиты mongodump

В скрипте необходимо указать параметры для утилиты mongodump. Подробнее см. в официальной документации MongoDB.

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;
- 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)
```

19.1.4 Создание плана резервного копирования

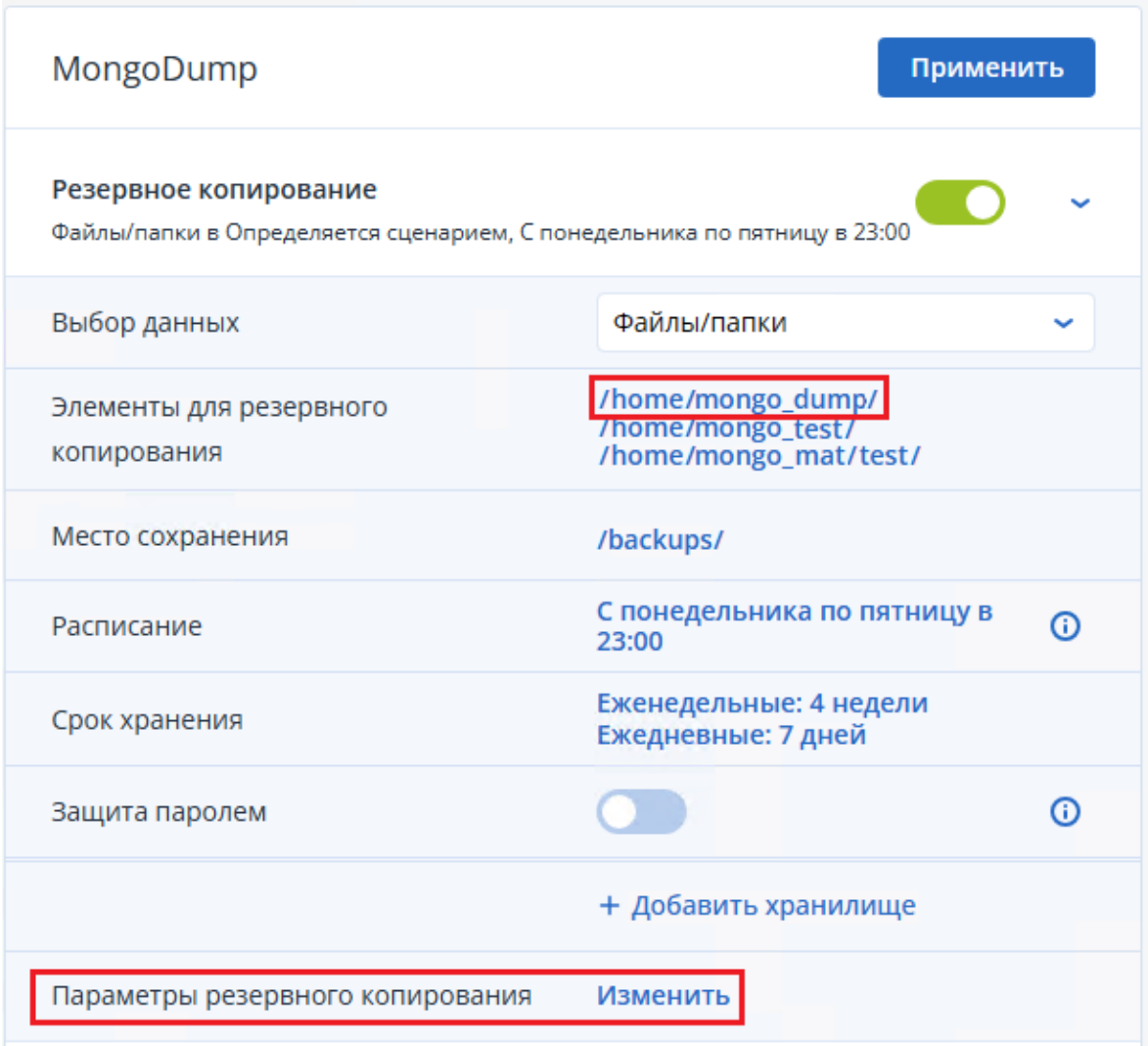
Для создания плана защиты выполните следующие действия:

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. 174)).
   - Диски/тома.
   - Файлы/папки.

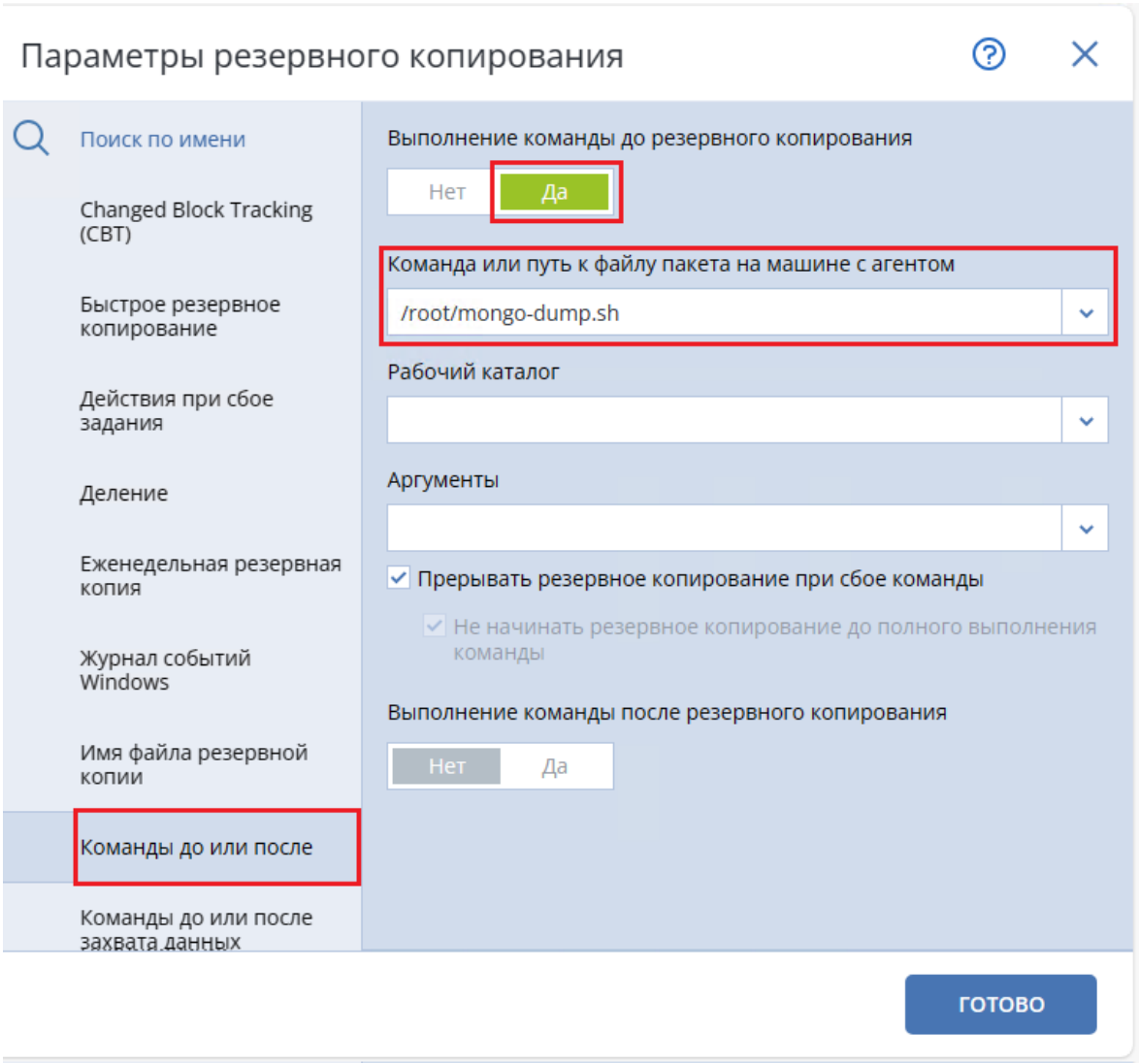
   В поле **Элементы для резервного копирования** нажмите **Указать** и выберите данные для резервного копирования. Папки, указанные в поле **Элементы для резервного копирования**, должны существовать до запуска резервного копирования (дочерние элементы могут быть созданы в ходе выполнения скрипта).

   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.

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:



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. 168).
8. Нажмите **Применить**.

Новый план защиты появится в списке планов.

19.2 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.

20 Защита Kubernetes

20.1 Зачем защищать Kubernetes

С помощью Кибер Бэкап можно выполнять резервное копирование пространств имен 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.

20.2 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 для Kubernetes или Кибер Бэкап Расширенная редакция для универсальной платформы.
- Kubernetes версии 1.24 или выше.

Примечание
Защита каждого кластера Kubernetes требует отдельной лицензии Кибер Бэкап Расширенная редакция для Kubernetes или Кибер Бэкап Расширенная редакция для универсальной платформы. Информацию о лицензиях Кибер Бэкап см. в разделе "Выпуски и лицензирование Кибер Бэкап" (стр. 17)

Для выполнения резервного копирования требуется установка агента.

Поддерживается установка агентов для следующих операционных систем:
Поддерживаемые операционные системы Linux с версией ядра от 3.0 и выше

- Astra Linux 1.6 и выше
- РЕД ОС 7.2, 7.3, 8
- РОСА «КОБАЛЬТ» 7.9
- Альт Сервер 9, 10
- ОСнова 2.7
- Red Hat Enterprise Linux 7.x и выше
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS
- SUSE Linux Enterprise Server 12 и выше
- Debian 10 и выше
- CentOS 7.x и выше

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.

20.3 Возможности

Кибер Бэкап позволяет выполнять резервное копирование и восстановление пространств имен, групп пространств имен и постоянных томов Kubernetes.

20.4 Известные проблемы и ограничения

- Восстановление постоянных томов в текущей версии Кибер Бэкап ограничено поддержкой моментальных снимков.

См. также Проблемы, актуальные для Кибер Бэкап 17.

20.5 Установка Kubernetes

Установка Kubernetes включает в себя следующие шаги:

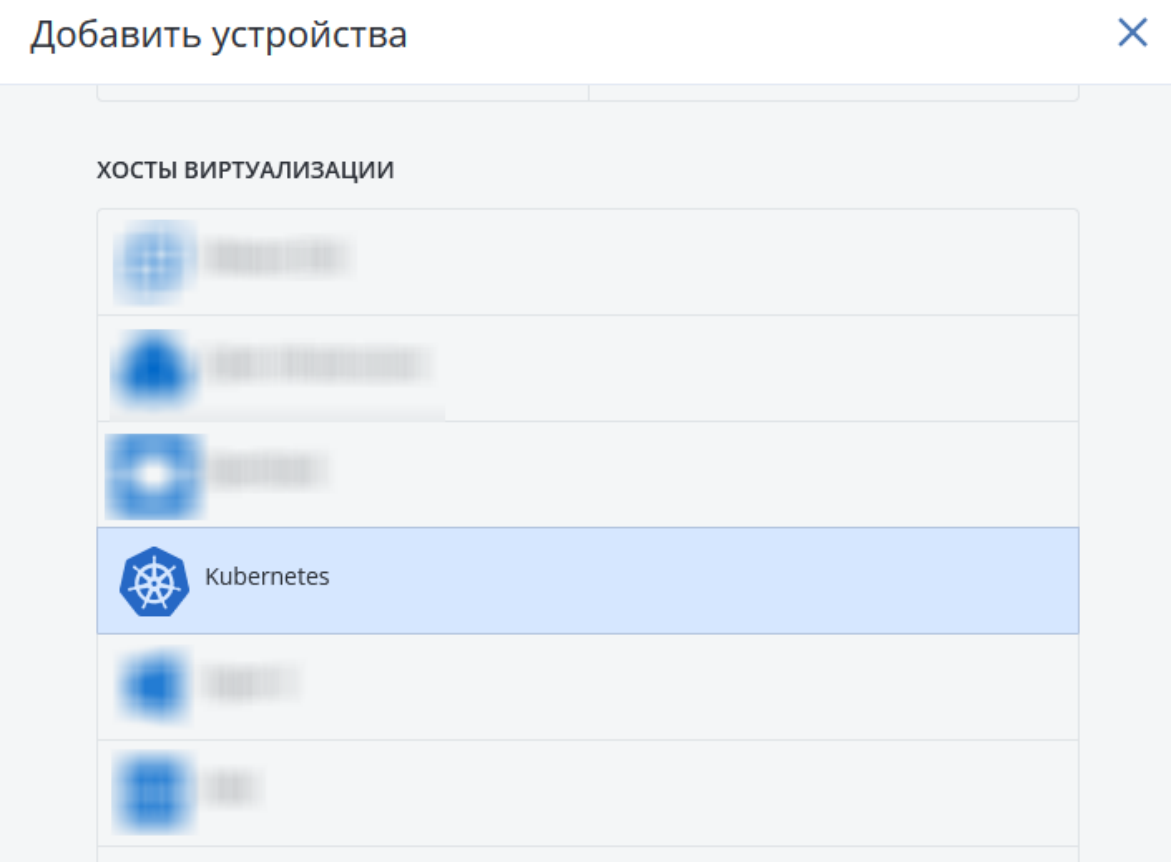
1. Установка сервера управления.
2. Установка агента Кибер Бэкап для Kubernetes.
3. Добавление кластера Kubernetes.

20.5.1 Установка сервера управления

Для установки сервера управления обратитесь к разделу "Установка сервера управления" (стр. 58).

20.5.2 Установка агента для Kubernetes

1. В веб-консоли Кибер Бэкап перейдите: **Устройства** -> **Все устройства**.
2. Справа вверху щелкните **Добавить** и выберите в списке Kubernetes.



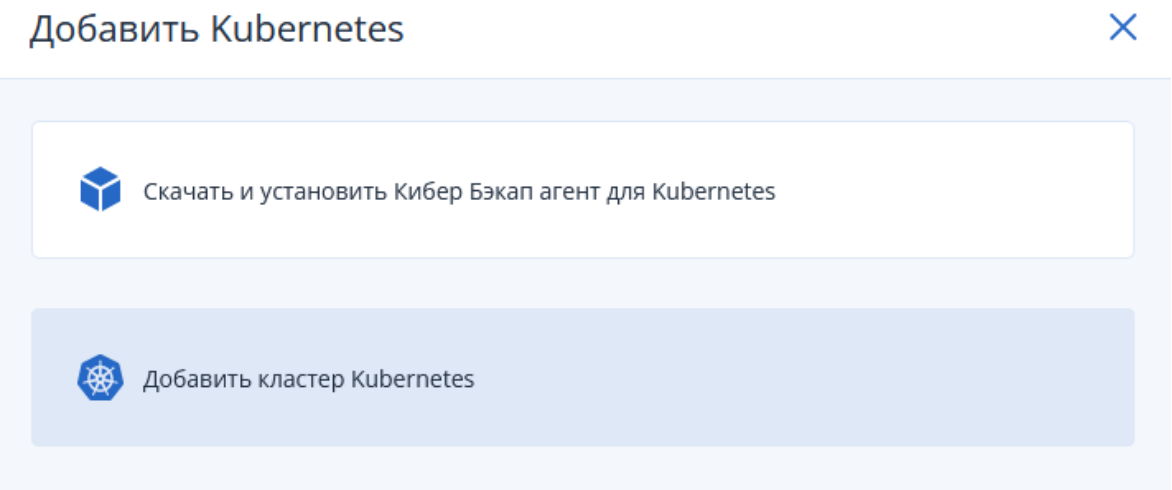
3. Выберите **Скачать и установить Кибер Бэкап агент для Kubernetes** и укажите место сохранения установщика.

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 в Linux" (стр. 81).

20.5.3 Добавление кластера Kubernetes

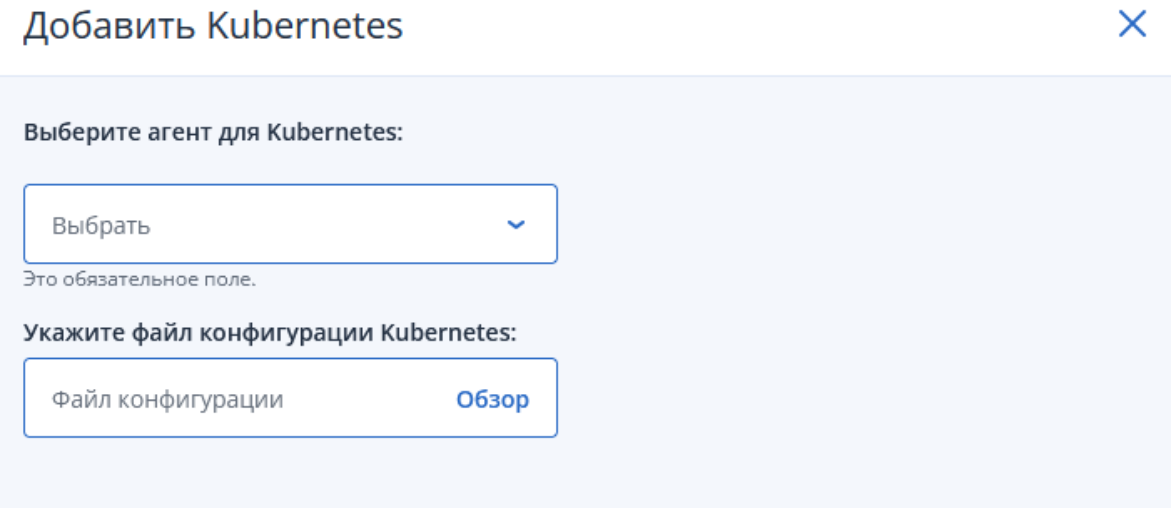
1. В веб-консоли Кибер Бэкап перейдите **Устройства** -> **Все устройства**.
2. Справа вверху щелкните **Добавить** и выберите в списке **Kubernetes**.
3. Выберите **Добавить кластер Kubernetes**.



4. Укажите агент для Kubernetes, для которого будет выполнена регистрация, и файл конфигурации для Kubernetes.

   Для подключения к кластеру Kubernetes файл конфигурации должен содержать адрес, имя пользователя и клиентский сертификат. Пользователь должен иметь роль **kubeadm:cluster-admins** или **cluster-admin** для полного доступа ко всем API кластера.

   Путь к файлу конфигурации по умолчанию: /etc/kubernetes/admin.conf.



   После заполнения полей нажмите **Добавить** и дождитесь окончания установки.
5. В веб-консоли перейдите в **Устройства** и убедитесь, что кластер Kubernetes добавлен в вашу конфигурацию.
6. В веб-консоли перейдите: **Настройки** > **Агенты** и убедитесь, что агент для Kubernetes отображается в списке агентов.

Если агенту не удалось подключиться к серверу управления, выполните это подключение вручную, как описано в статье Ручная регистрация агента на сервере управления.

20.6 Резервное копирование Kubernetes

20.6.1 Предварительные требования

Перед резервным копированием убедитесь, что вы выполнили следующие действия:

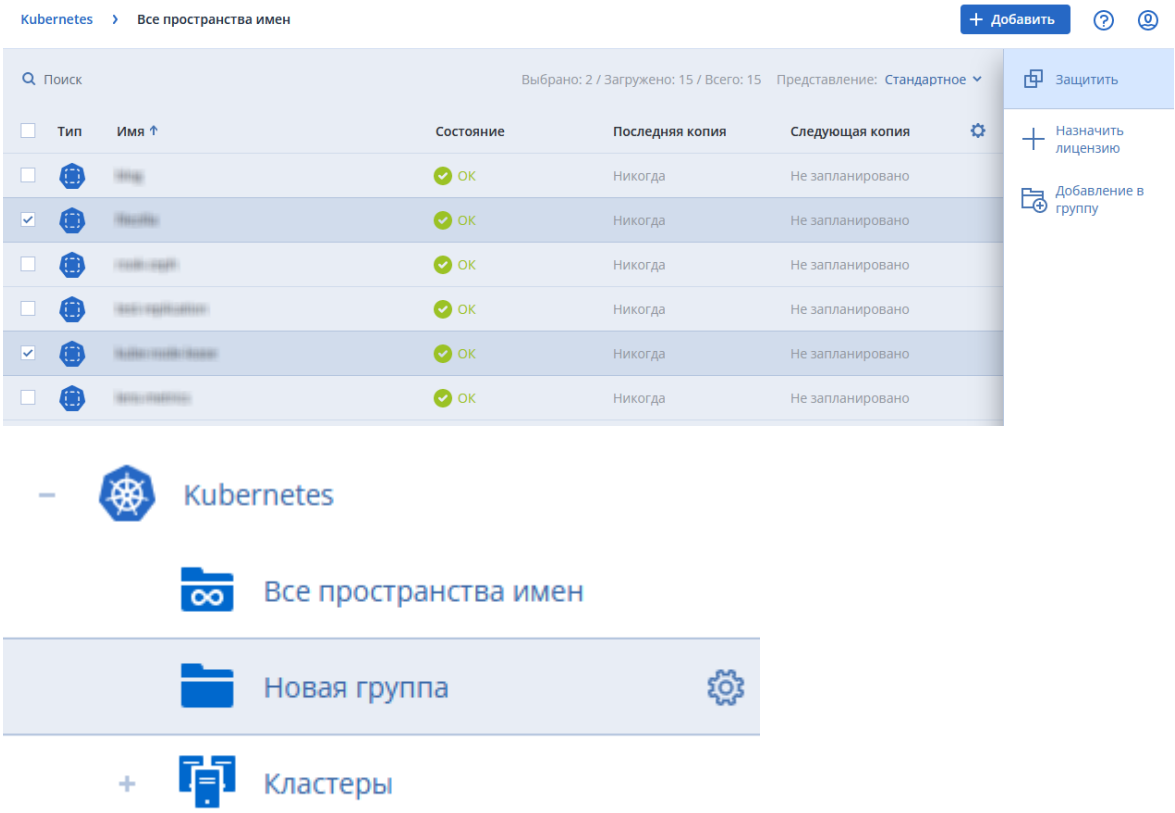
1. Установка агента Кибер Бэкап для Kubernetes и подключение кластера Kubernetes к Серверу управления (см. "Установка Kubernetes" (стр. 437)).
2. Настройка хранилища. Настройте ваше хранилище для работы с Кибер Бэкап и Kubernetes.

20.6.2 Создание плана защиты

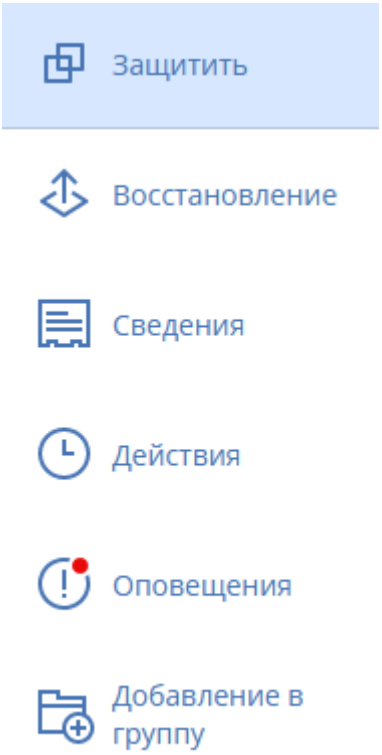
Создание плана защиты из веб-консоли возможно двумя способами: через пункт веб-консоли **Устройства** и через пункт **Планы** (см. также "Создание плана защиты" (стр. 157)).

Создание плана через пункт веб-консоли Устройства

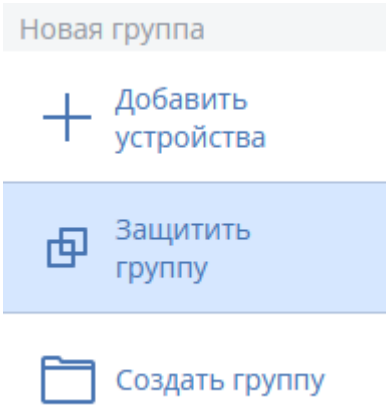
1. В веб-консоли Кибер Бэкап перейдите **Устройства** -> **Kubernetes**.
2. Выберите пространства имен (или группу с пространствами имен) для защиты.



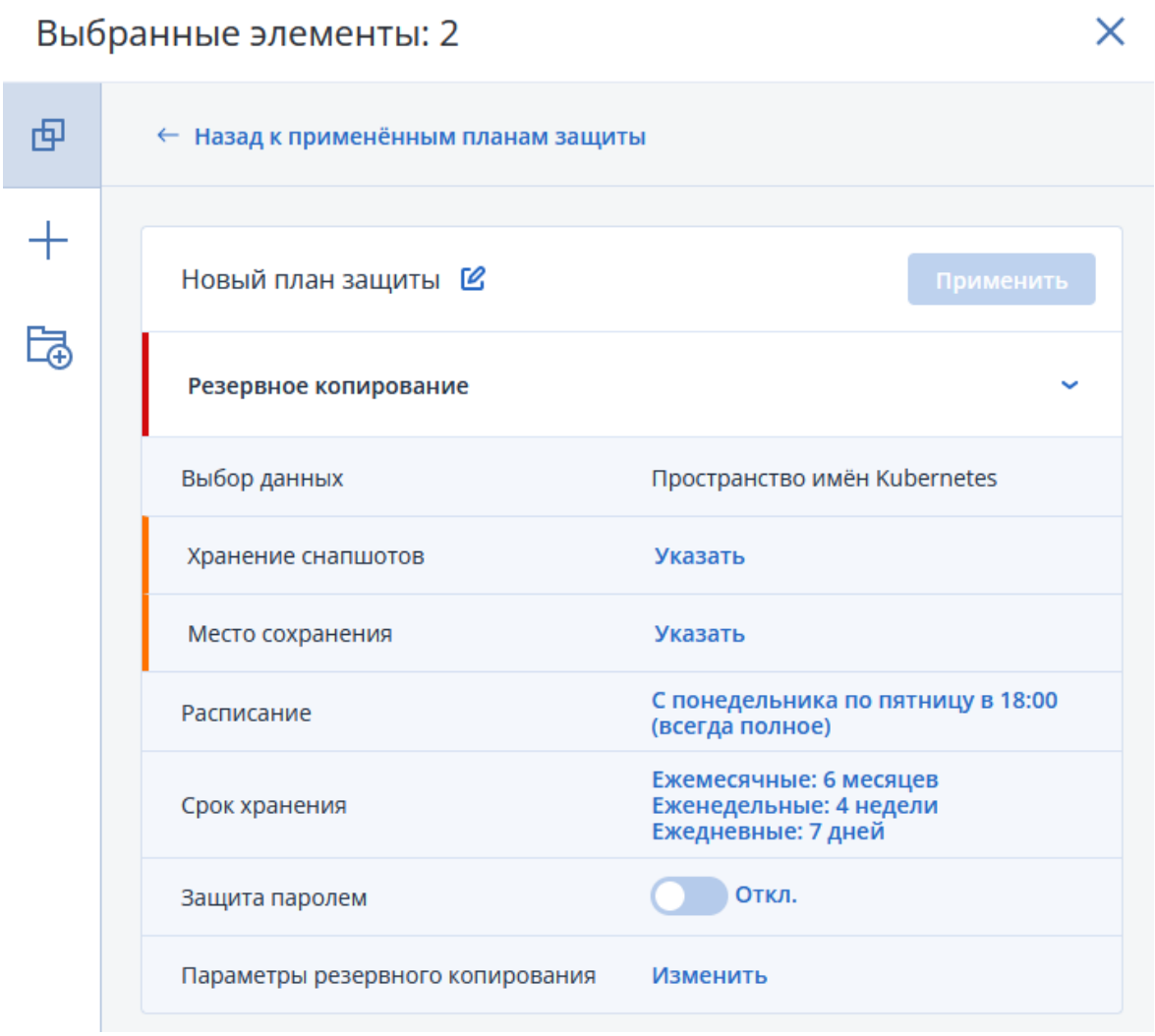
3. Нажмите справа вверху **Защитить**.



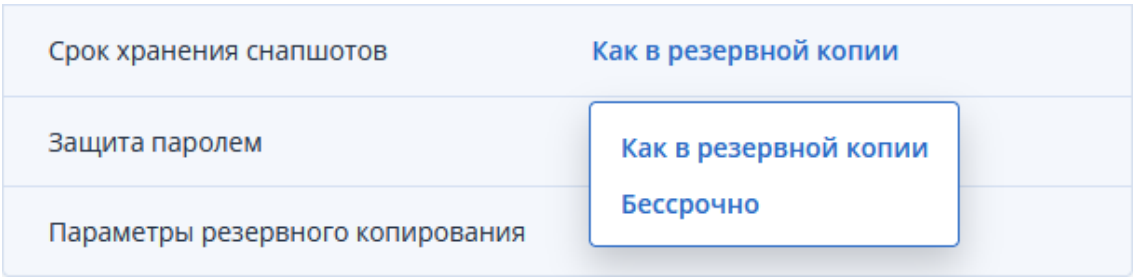
Для защиты группы выберите **Защитить группу**.



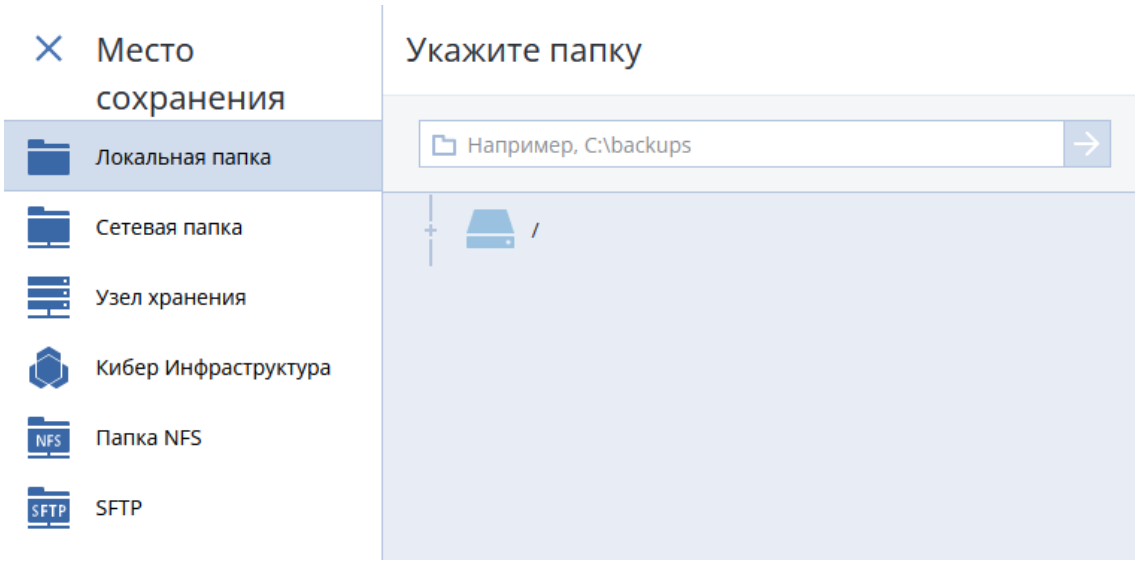
4. Щелкните **Создать план** (если план не применен) или **Добавить план** (если какой-либо план в данный момент применен).
5. Выберите необходимые вам настройки плана защиты, заполнив соответствующие поля:



a. **Хранение снапшотов**. Укажите место, где будут сохраняться моментальные снимки. При выборе варианта хранения **Локальное на СХД** укажите также срок хранения моментальных снимков в появившейся области **Срок хранения снапшотов**.



b. **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, папка NFS, SFTP.



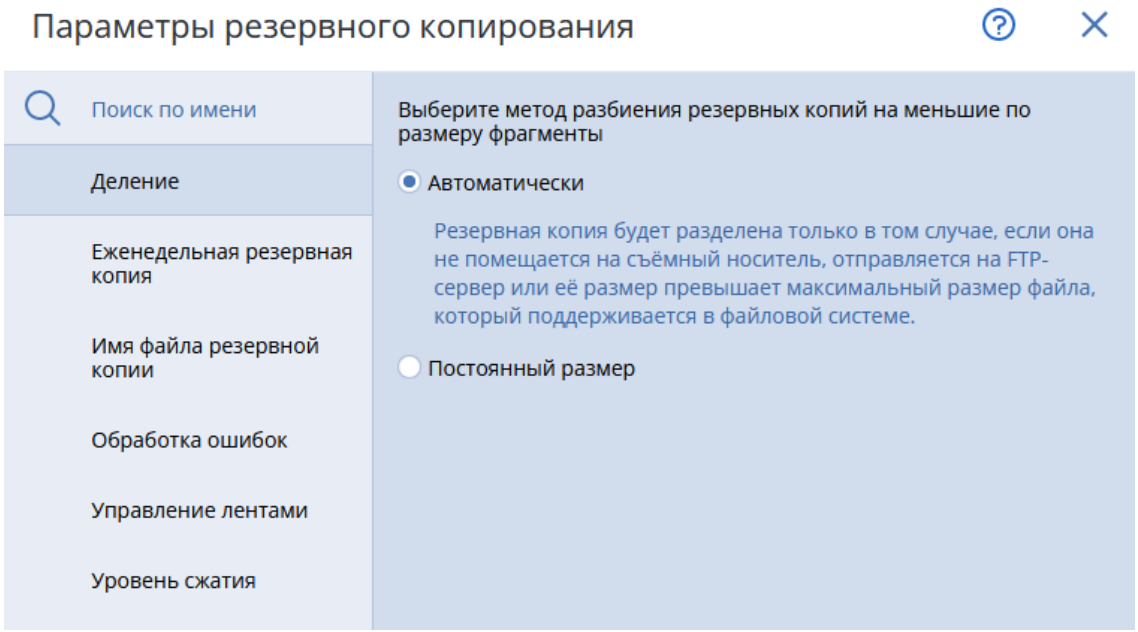
Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места назначения" (стр. 180).

c. [Необязательно] **Расписание**. Задайте расписание резервного копирования.

d. [Необязательно] **Срок хранения**. Укажите срок хранения резервных копий.

e. [Необязательно] **Защита паролем**. Активируйте защиту паролем при необходимости.

f. [Необязательно] **Параметры резервного копирования**. Выберите параметры резервного копирования (см. также "Параметры резервного копирования" (стр. 210)).

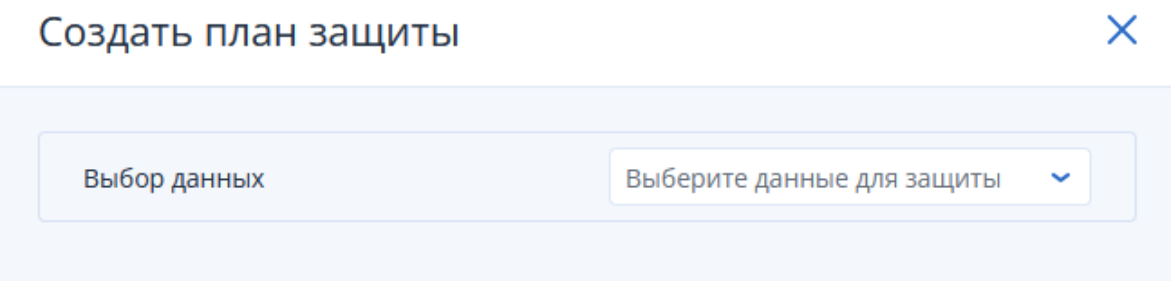


6. Нажмите **Применить**.

Создание плана через пункт веб-консоли Планы

1. В веб-консоли перейдите: **Планы** -> **Защита**.
2. Нажмите справа вверху **Создать план**.

3. В открывшемся окне в строке **Выбор данных** выберите из списка **Kubernetes**.



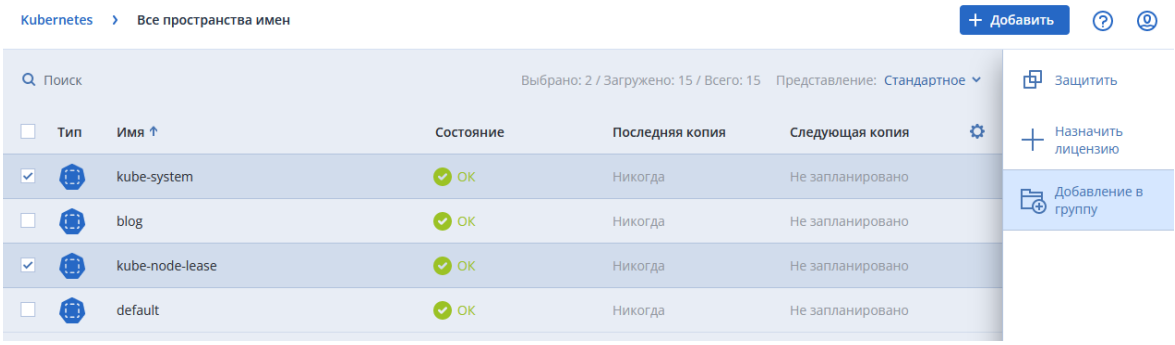
4. В окне создания плана настройте план нужным вам образом и нажмите **Создать**.

20.6.3 Создание групп

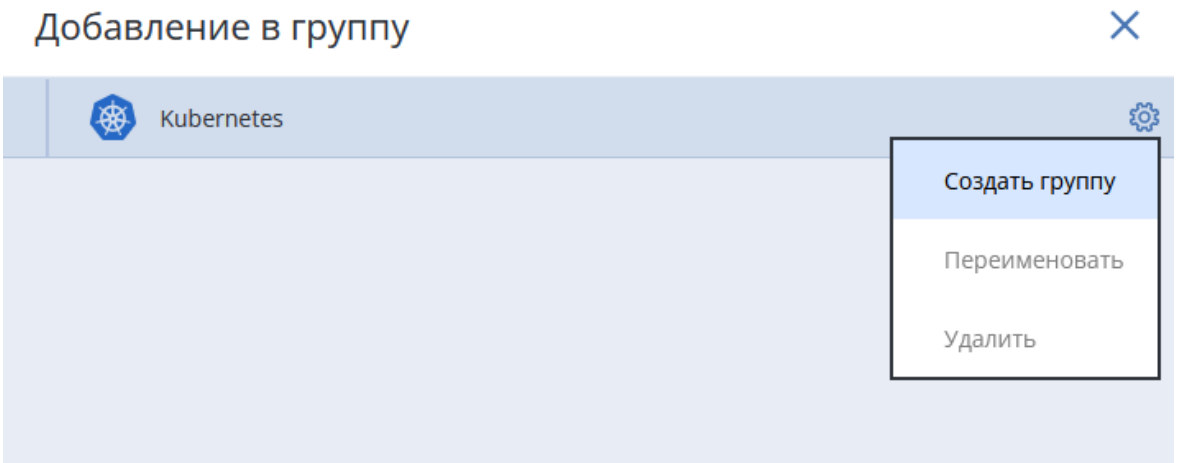
С Кибер Бэкап вы можете создавать и защищать не только отдельные пространства имен, но и группы пространств имен.

Для создания группы пространств имен выполните следующие действия:

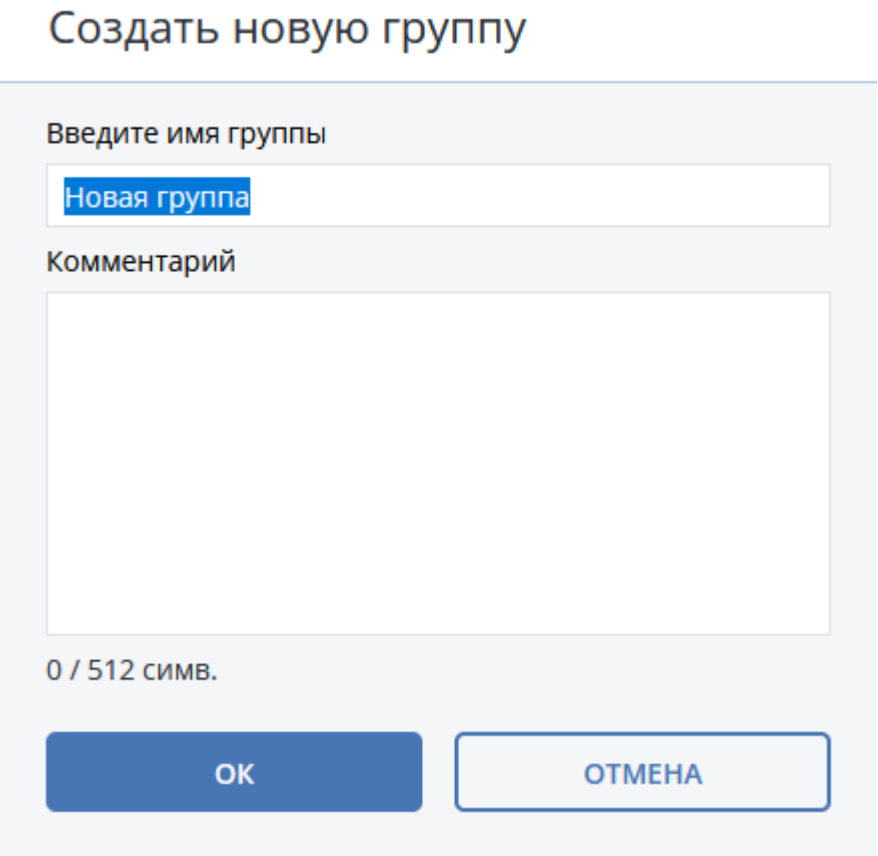
1. В веб-консоли перейдите: **Устройства** -> **Kubernetes**.
2. Отметьте в списке устройства, которые хотите добавить в группу, и щелкните справа **Добавление в группу**.



3. Щелкните значок шестеренки и выберите **Создать группу**.



4. Введите имя группы; если требуется, добавьте комментарий и нажмите **OK**.



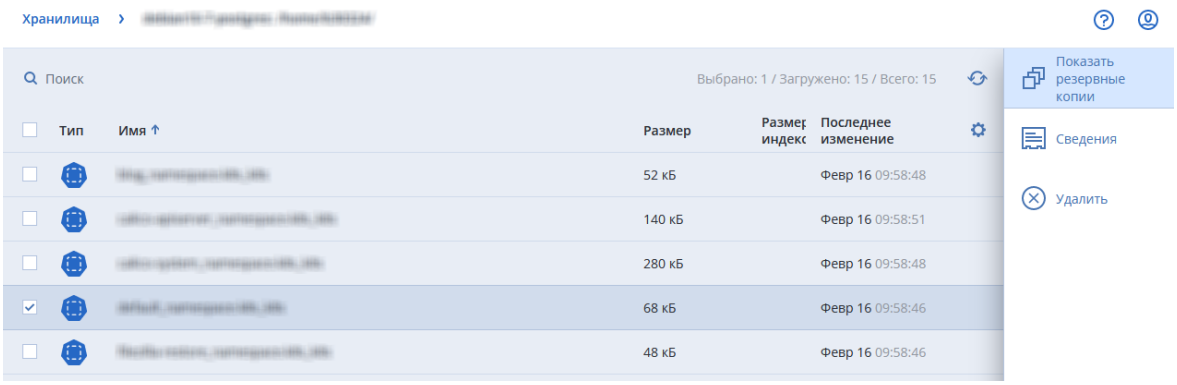
5. Нажмите **Готово**.

20.7 Восстановление Kubernetes

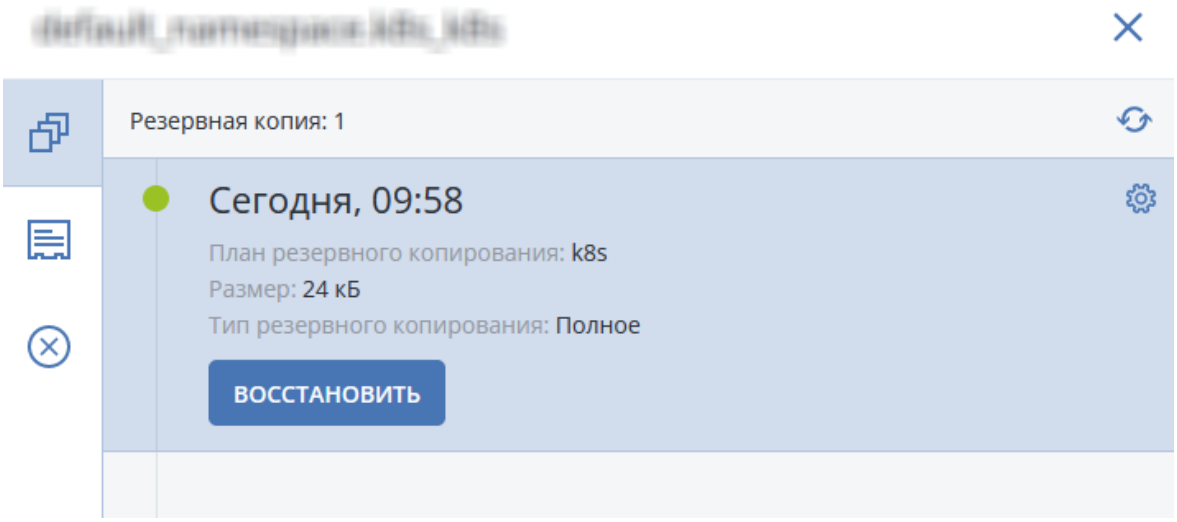
Перед восстановлением убедитесь, что место хранения резервных копий доступно, а резервные копии, из которых вы хотите выполнить восстановление, были созданы успешно.

Восстановление пространства имен из меню Резервные копии

1. В веб-консоли перейдите в **Хранилище резервных копий**.
2. В списке резервных копий пространств имен отметьте нужную вам и нажмите справа вверху **Показать резервные копии**.



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**.

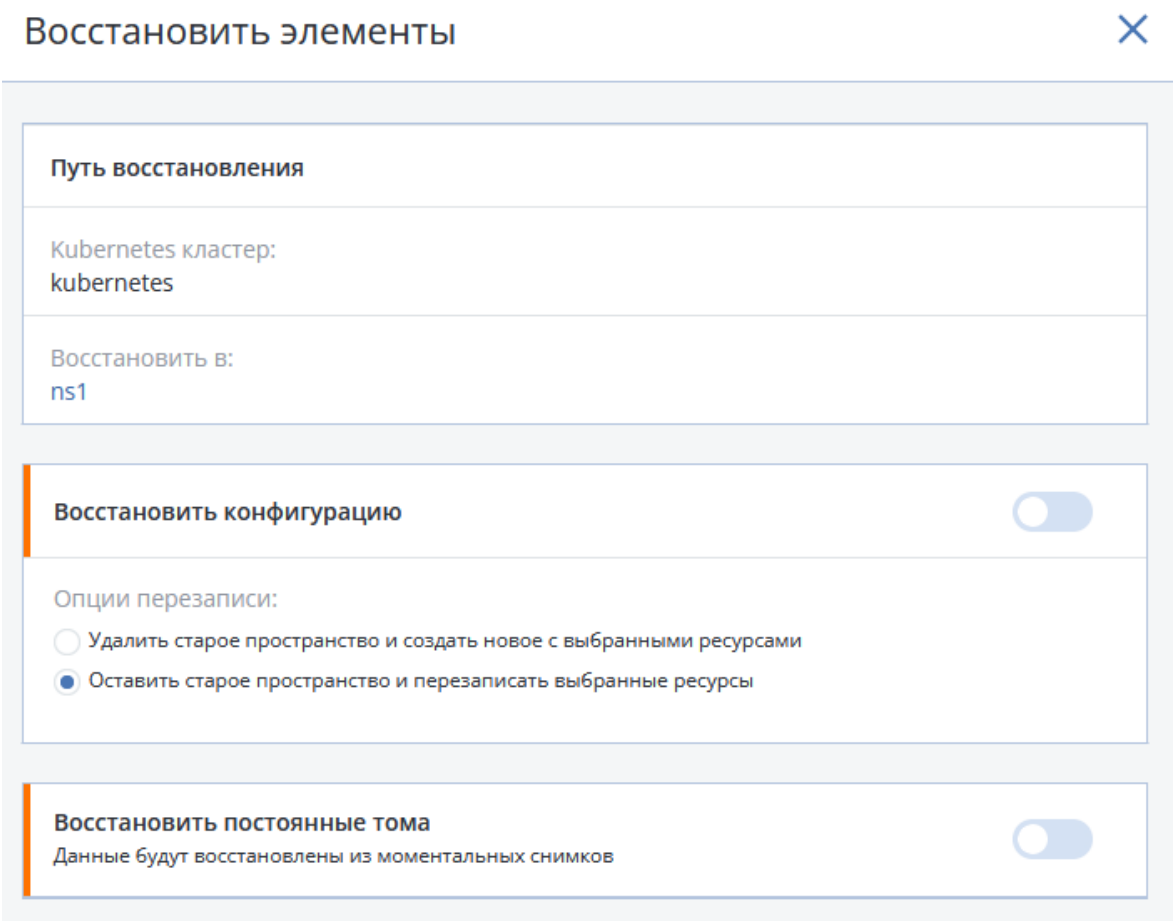
   Для просмотра сведений о конфигурации:

   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.



- 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.
- Для восстановления постоянных томов передвиньте ползунок в области **Восстановить постоянные тома**.

6. Нажмите **Начать восстановление** и дождитесь его окончания.

21 Специальные операции с виртуальными машинами

21.1 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.

21.1.1 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.

21.1.2 Предварительные требования

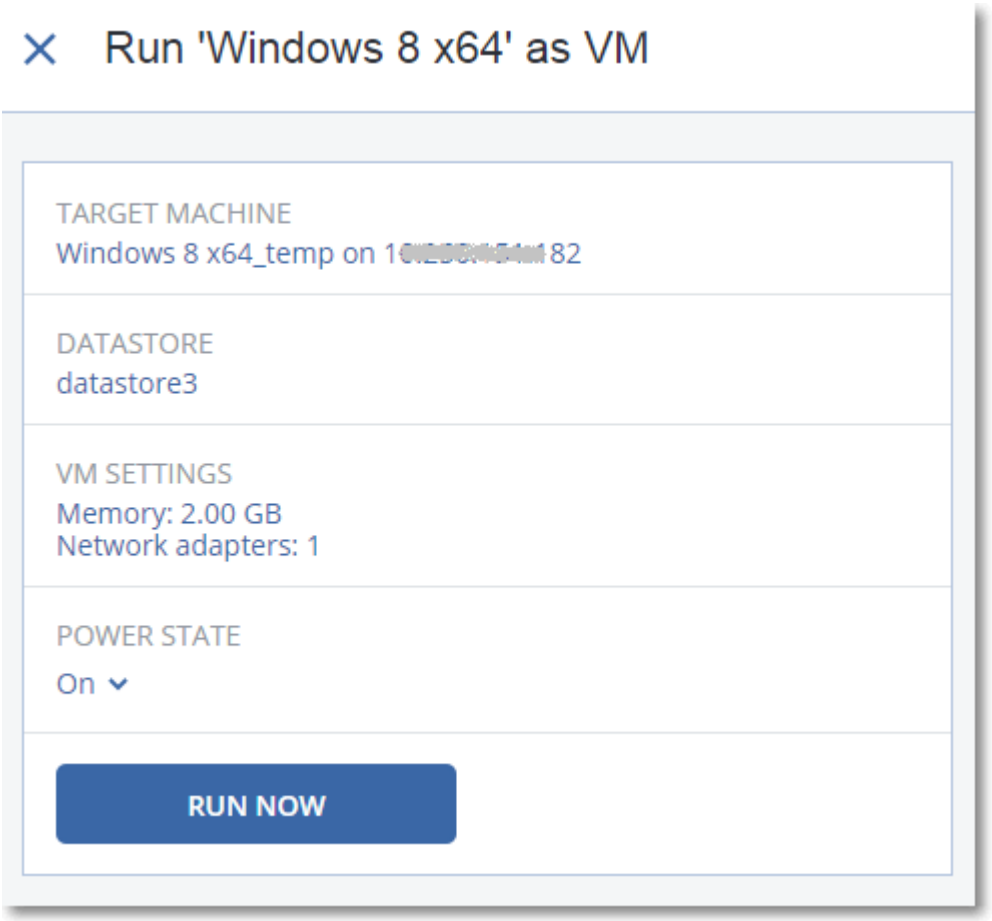
- В службе Защиты Данных необходимо зарегистрировать хотя бы один агент для VMware или агент для Hyper-V.
- Резервная копия может храниться в сетевой папке, на узле хранения или в локальной папке машины, на которой установлен агент для VMware или агент для Hyper-V. Сетевая папка должна быть доступной 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. Нельзя использовать резервные копии *контейнеров* Virtuozzo.
- 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.

21.1.3 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 Хранилище 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.
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.

21.1.4 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 **Все устройства** 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.

21.1.5 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.

Примечание
Финализация не поддерживается для Hyper-V, который выполняется в Windows Server 2008 R2 и Microsoft Hyper-V Server 2008 R2, поскольку в этих версиях Hyper-V отсутствует необходимый API.

Порядок финализации машины, которая запущена из резервной копии

1. На вкладке **Все устройства** выберите машину, которая запущена из резервной копии.
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.

21.1.5.1 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.

21.2 Работа в VMware vSphere

В этом разделе описаны операции, характерные для среды VMware vSphere.

21.2.1 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.

21.2.1.1 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 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.

21.2.1.2 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.

21.2.1.3 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.

21.2.1.4 Ограничения

Невозможно выполнить репликацию указанных ниже типов виртуальных машин:

- Отказоустойчивые машины, которые выполняются в ESXi 5.5 и более ранних версий.
- Машины, которые запущены из резервных копий.
- Реплики виртуальных машин.

21.2.1.5 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 **Все устройства** с указанным ниже значком: 

21.2.1.6 Тестирование реплики

Порядок подготовки реплики к тестированию

1. Выберите реплику для тестирования.
2. Щелкните **Тестировать реплику**.
3. Щелкните **Начать тестирование**.
4. Выберите, подключить ли включенную реплику к сети. По умолчанию реплика не будут подключена к сети.
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. Щелкните **Тестировать реплику**.
3. Щелкните **Остановить тестирование**.
4. Подтвердите операцию.

21.2.1.7 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 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**.
6. [Необязательно] Щелкните **Параметры восстановления**, чтобы изменить параметры возврата из реплики.
7. Щелкните **Запуск восстановления**.
8. Подтвердите операцию.

21.2.1.8 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».

21.2.1.9 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.

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.

21.2.1.10 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**.

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.

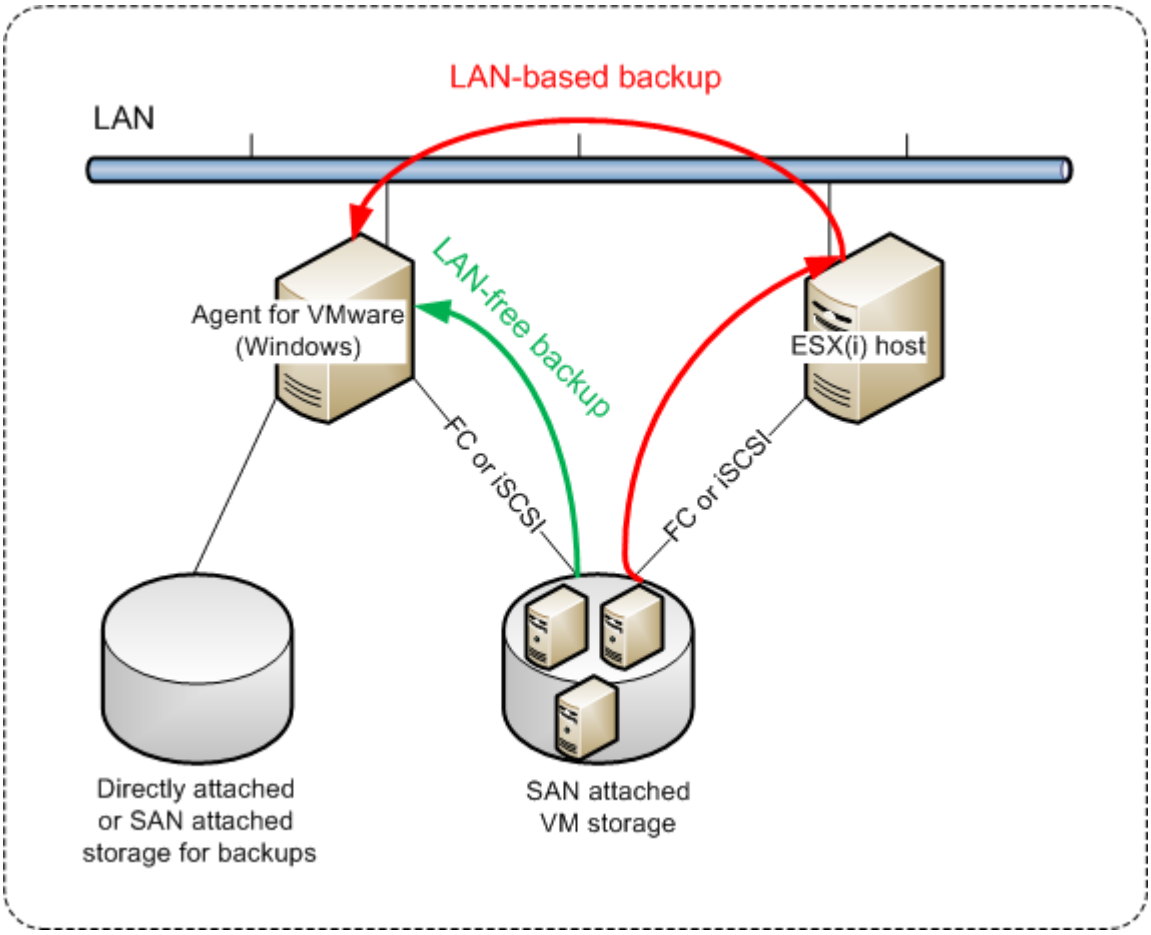
В результате программа продолжит обновлять реплику. Все репликации будут инкрементными.

21.2.2 Резервное копирование без использования локальной сети

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.

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 появится 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 Policy** автоматически устанавливается значение**Перевод в автономное состояние всех ресурсов** во время установки агента для VMware (Windows).

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).

21.2.2.1 Ограничения

- В vSphere 6.0 и более поздней версии 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.

21.2.2.2 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: На экране отобразится Перевод в автономное состояние всех 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**.

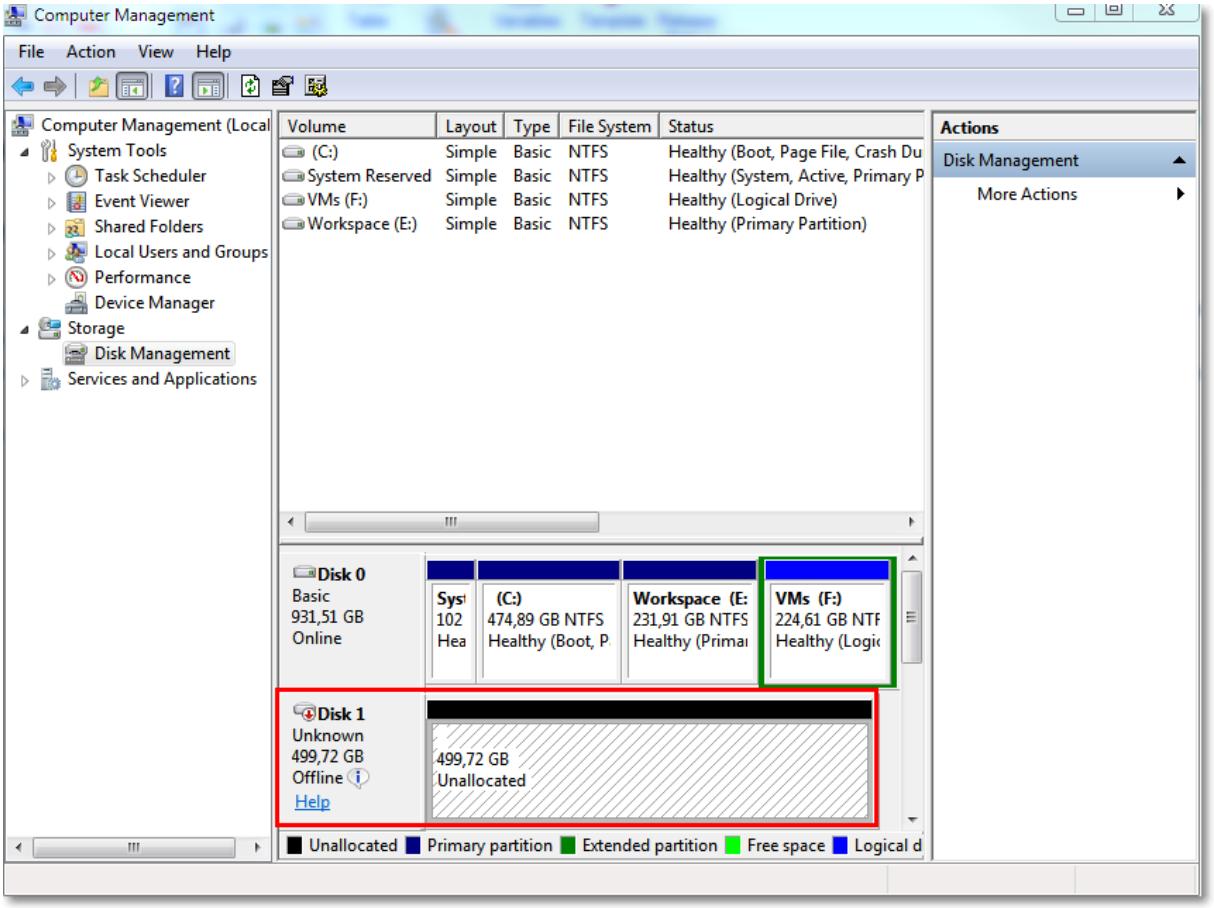
   Примечание
   Чтобы найти приложение **Администрирование**, возможно, необходимо будет изменить представление **панели управления** на отличное от **Главная** или **Категория** или воспользоваться поиском.

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**.
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 появится в разделе **Управление дисками**, как показано на снимке экрана ниже.



21.2.3 Использование моментальных снимков оборудования SAN

Если VMware vSphere использует систему хранения Storage area network (SAN) в качестве хранилища данных, вы можете подключить агент для VMware (Windows) для использования моментальных снимков оборудования SAN при выполнении резервного копирования.

Внимание
Поддерживается только хранилище данных SAN NetApp.

21.2.3.1 Смысл использования моментальных снимков оборудования SAN

Агенту для VMware требуются моментальные снимки виртуальных машин для выполнения согласованного резервного копирования. Агент считывает содержимое виртуального диска с

моментального снимка диска, поэтому моментальный снимок должен хранится 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.

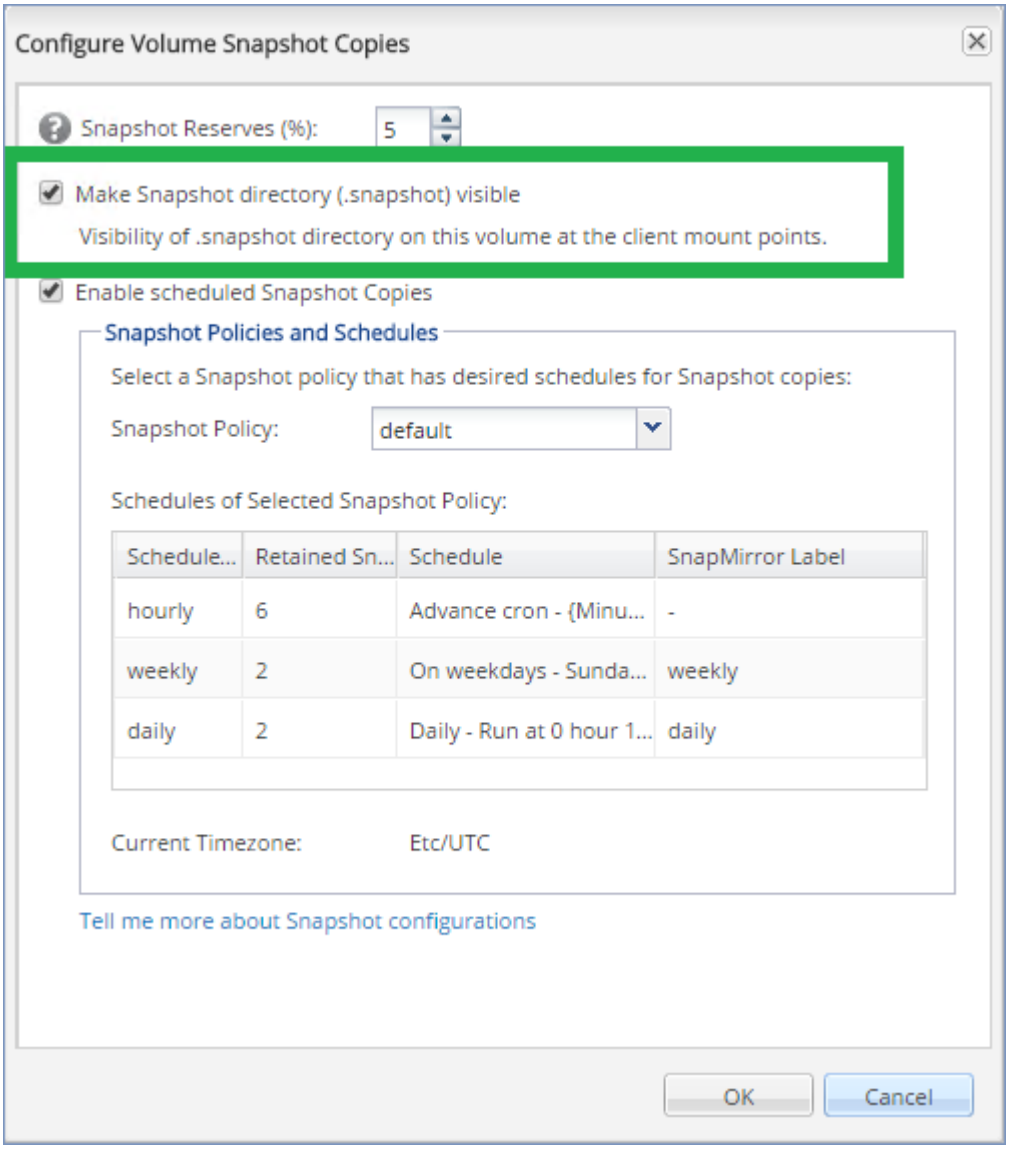
21.2.3.2 Что необходимо для использования моментальных снимков оборудования SAN?

Для использования моментальных снимков оборудования SAN при резервном копировании виртуальных машин убедитесь в выполнении следующих условий.

- Хранилище SAN NetApp соответствует требованиям, описанным в «Требования хранилища SAN NetApp».
- Машина, на которой запущен агент для VMware (Windows) сконфигурирована в соответствии с описанным в «Настройка машины, на которой работает агент для VMware».
- Хранилище SAN зарегистрировано на сервере управления.
- [При наличии агентов для VMware, не принимавших участие в вышеуказанной регистрации] Виртуальные машины в хранилище SAN назначены агентам с подключенным SAN, как описано в «Привязка виртуальной машины».
- Опция резервного копирования Моментальные снимки оборудования SAN включена в параметрах плана резервного копирования.

21.2.3.3 Требуется хранилище 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.

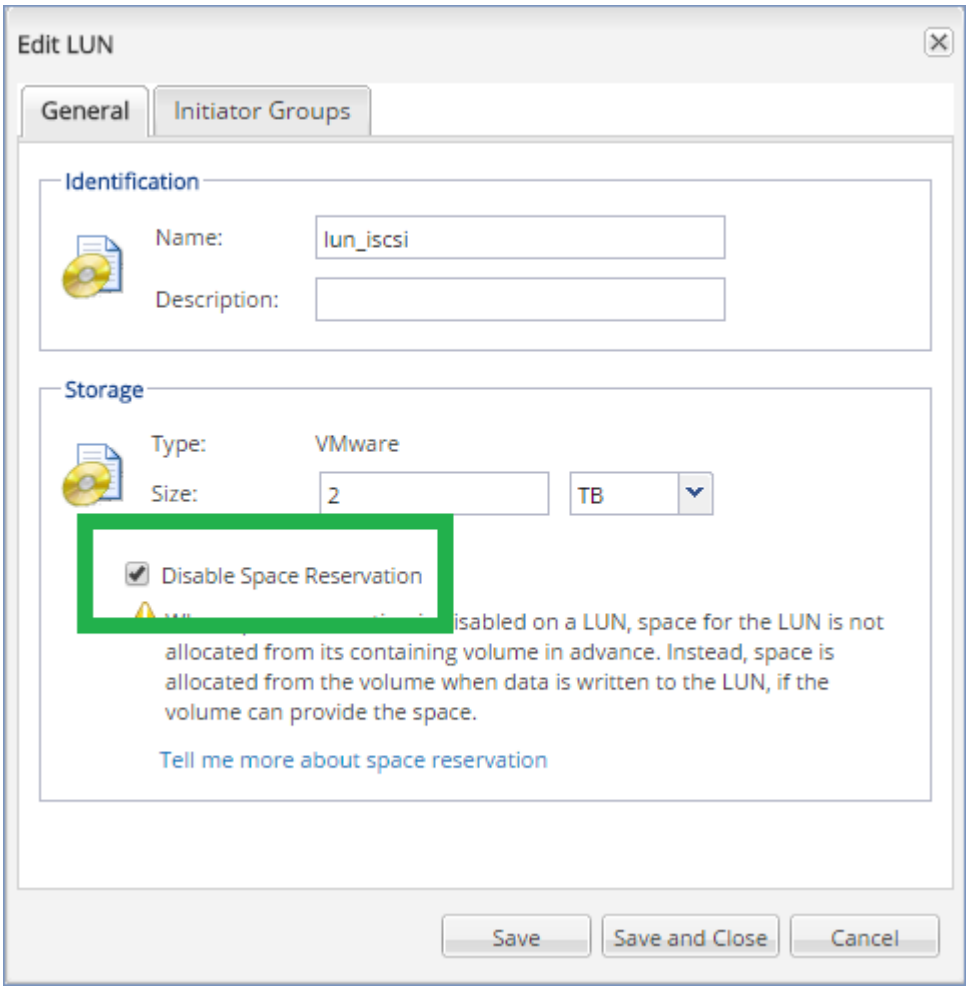


- [Для хранилищ данных NFS] На указанной при создании хранилища данных виртуальной должен быть разрешен доступ до общих папок NFS для клиентов Windows NFSv3. Доступ можно разрешить посредством следующей команды:

```
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.



21.2.3.4 Настройка машины, на которой работает агент для VMware

В зависимости от использования хранилища SAN в качестве хранилища данных NFS или iSCSI см. соответствующий раздел ниже.

Настройка инициатора iSCSI

Убедитесь, что выполнены все последующие условия:

- Инициатор iSCSI установлен.
- Тип запуска службы инициатора iSCSI (Microsoft) имеет значение **Автоматический** или **Ручной**. Это можно сделать в оснастке **Службы**.
- Инициатор iSCSI настроен как описано в примере раздела «Резервное копирование без использования локальной сети».

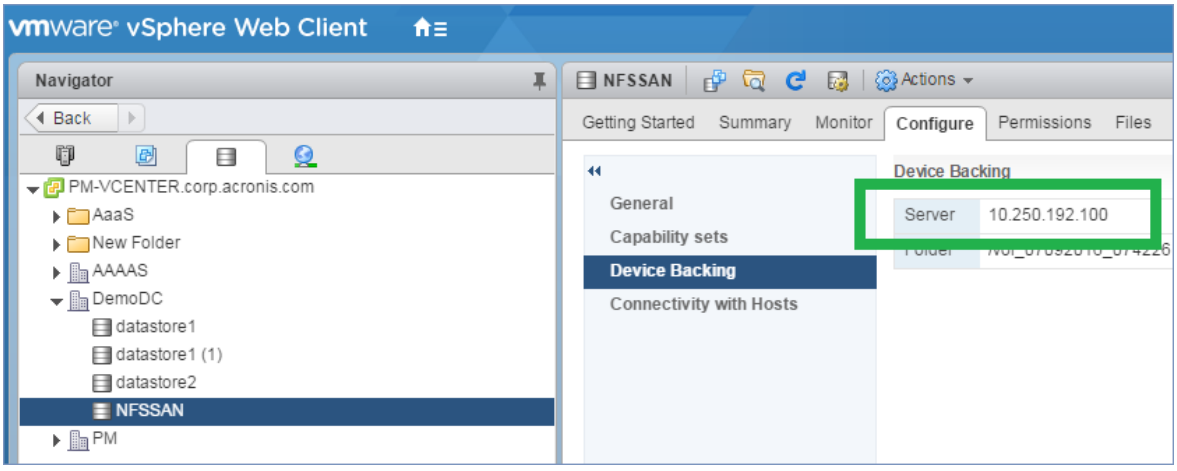
Настройка NFS-клиента

Убедитесь, что выполнены все последующие условия:

- **Службы для NFS** Microsoft (в Windows Server 2008 R2) или **Клиент для NFS** (в Windows Server 2012 и более поздних версиях) установлены.
- NFS-клиент настроен на анонимный доступ. Это можно сделать следующим образом:
  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.

21.2.3.5 Регистрация хранилища данных SAN на сервере управления.

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**.



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. Для создания нового пользователя в менеджере системы NetApp OnCommand перейдите по пути **Настройки** > **Безопасность** > **Пользователи** и создайте нового пользователя.

6. Выберите один или несколько агентов для VMware (Windows), которым будет предоставлено право на чтение для устройства SAN.
7. Нажмите кнопку **Добавить**.

21.2.4 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 агентаиз 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**.
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 назначения 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:**.

21.2.5 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.

21.2.5.1 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.

21.2.5.2 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.

21.2.5.3 Просмотр результата распределения

Можно просмотреть результат автоматического распределения:

- в столбце **Агент** для каждой виртуальной машины в разделе **Все устройства**;
- в разделе **Назначенные виртуальные машины** на панели **Сведения** при выборе агента в разделе **Настройки** > **Агенты**.

21.2.5.4 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**.

21.2.5.5 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.

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.

21.2.5.6 Примеры использования

- Привязка вручную может быть удобна если необходимо, чтобы агент для VMware (Windows) создал резервную копию конкретной (очень большой) машины через волоконный 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.

21.2.6 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.

21.2.6.1 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.
- Функциональная возможность vMotion виртуальной машины отключена при выполнении резервного копирования. Выполнение резервного копирования будет продолжено после завершения миграции.

21.2.6.2 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.

21.2.7 Управление средами виртуализации

Можно просмотреть среды vSphere, Hyper-V и Virtuozzo в их собственном представлении. После установки и регистрации соответствующего агента в разделе **Устройства** появляются вкладки **VMware**, **Hyper-V** или **Virtuozzo**.

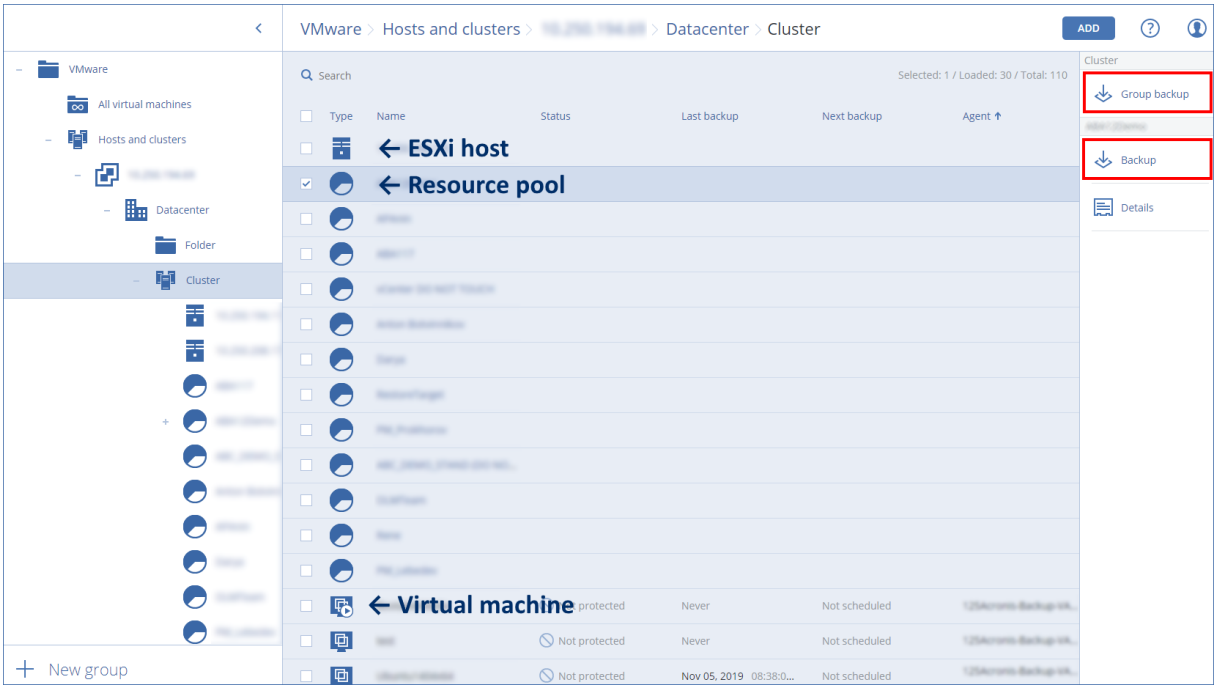
На вкладке **VMware** выполните резервное копирование следующих объектов инфраструктуры vSphere:

- 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 **Резервное копирование**, или машин родительской группы, в которую входит выбранная группа, щелкнув **Групповое резервное копирование**.

Например, вы выбрали кластер, а затем – пул ресурсов в нем. Если щелкнуть **Резервное копирование**, будет создана резервная копия для всех виртуальных машин в выбранном пуле

ресурсов. Если щелкнуть **Групповое резервное копирование**, будет создана резервная копия для всех виртуальных машин в кластере.



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**.

21.2.8 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:

- **Глобальные** > **Управление настраиваемыми атрибутами**
- **Глобальные** > **Настройка настраиваемых атрибутов**

21.2.9 Агент для VMware: необходимые привилегии

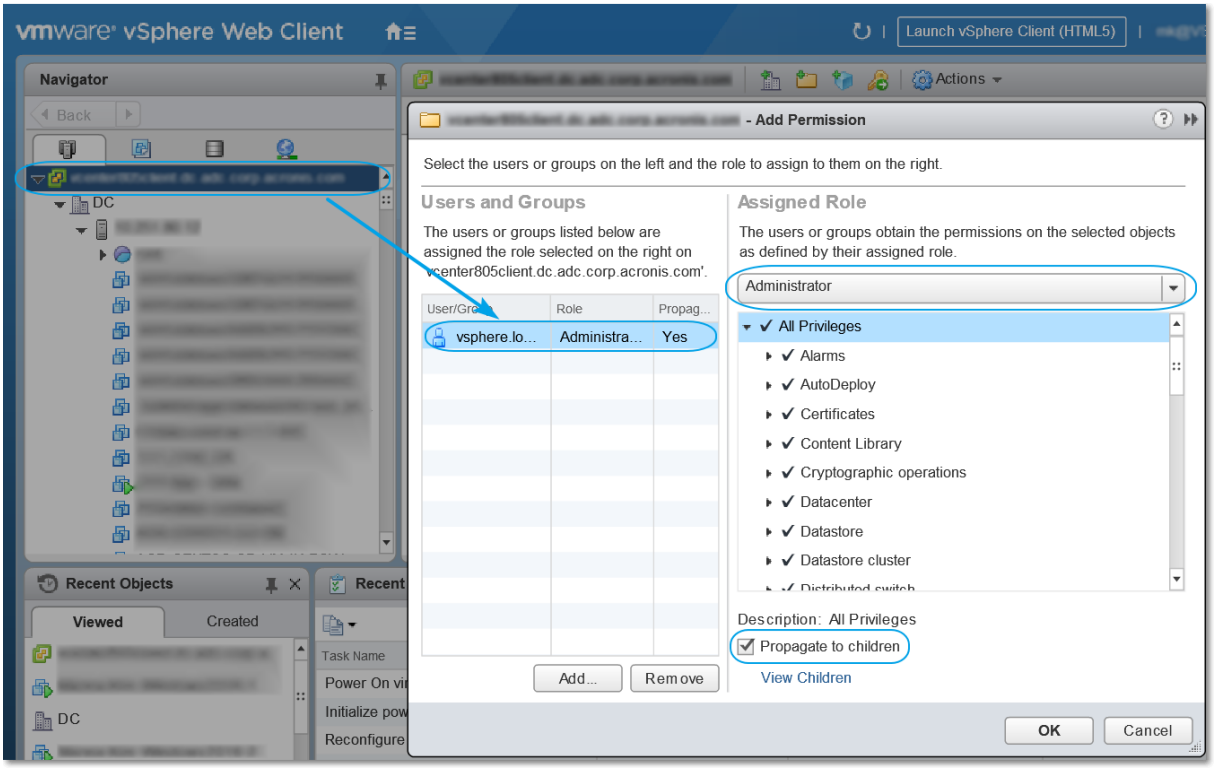
В этом разделе описаны права, необходимые для операций с виртуальными машинами ESXi, а также для развертывания виртуальных устройств.

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 назначения прав пользователю vSphere на уровне vCenter

1. Войдите в веб-клиент vSphere.
2. Щелкните правой кнопкой мыши vCenter, затем щелкните **Добавить право**.
3. Выберите или добавьте нового пользователя с требуемой ролью (роль должна включать в себя все требуемые разрешения с таблицей ниже).
4. Выберите параметр **Propagate to children (Распространить на дочерние элементы)**.



		Операция				
Объект	**Привилегия**	**Резервное копирование ВМ**	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
Операции шифрования (начиная с vSphere 6.5)	**Добавить диск**	+*				
	Прямой доступ	+*				
Хранилище данных	**Распределение пространства**		+	+	+	+
	Обзор хранилища данных				+	+
	Настройка хранилища данных	+	+	+	+	+

	Низкоуровневые файловые операции				+	+
Глобальные	Лицензии	+	+	+	+	
	Методы отключения	+	+	+		
	Методы включения	+	+	+		
	Управление настраиваемыми атрибутами	+	+	+		
	Задать настраиваемый атрибут	+	+	+		
Хост > Конфигурация	Конфигурация автозапуска ВМ					+
	Конфигурация раздела хранения данных				+	
Хост > Инвентаризация	Изменение кластера					+
Хост > Локальные операции	Создание ВМ				+	+
	Удаление ВМ				+	+
	Перенастройка ВМ				+	+
Сеть	Назначение сети		+	+	+	+
Ресурс	Назначение ВМ пулу ресурсов		+	+	+	+

Импорт	**Добавить виртуальную машину**				+	
	vApp					+
Виртуальная машина > Конфигурация	**Добавление существующего диска**	+	+		+	
	Добавление нового диска		+	+	+	+
	Добавление или удаление устройства		+		+	+
	Дополнительно	+	+	+		+
	Изменение числа ЦП		+			
	Отслеживание изменений диска	+		+		
	Аренда диска	+		+		
	Память		+			
	Удаление диска	+	+	+	+	
	Переименование		+			
	Настройка аннотации				+	
	Настройки		+	+	+	
Виртуальная машина > Гостевые операции	**Выполнение программы гостевой операции**	+**				+
	Запросы гостевой операции	+**				+

	Изменения гостевых операций	+**				
Виртуальная машина > Взаимодействие	**Получение контрольного билета гостя** (в vSphere 4.1 и 5.0)				+	+
	Настройка носителя CD		+	+		
	Подключение устройств		+	+		
	Взаимодействие с консолью					+
	Управление гостевой операционной системой с помощью API VIX (в vSphere 5.1 и более поздних версий)				+	+
	Отключение			+	+	+
	Включение		+	+	+	+
Виртуальная машина > Инвентаризация	**Создание из существующей**		+	+	+	
	Создание новой		+	+	+	+
	Перемещение					+
	Регистрация				+	
	Удаление		+	+	+	+
	Отмена регистрации				+	

Виртуальная машина > Распределение	**Разрешение доступа к диску**		+	+	+	
	Разрешение доступа к диску только для чтения	+		+		
	Разрешение загрузки ВМ	+	+	+	+	
Виртуальная машина > Состояние	**Создание моментального снимка**	+		+	+	+
	Удаление снимка	+		+	+	+

* Эта привилегия требуется только для резервного копирования зашифрованных машин.

** Эта привилегия требуется только резервных копий с поддержкой приложений.

21.3 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.

   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.

21.3.1 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**.

21.4 Ограничение общего количества виртуальных машин, для которых одновременно выполняется резервное копирование

Параметр резервного копирования Планирование определяет количество виртуальных машин, для которых агент может одновременно создавать резервные копии при выполнении данного плана защиты.

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 агент для VMware или агент для Hyper-V может одновременно создавать резервные копии.

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 VMware (Linux)

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 VMware (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 VMware (Linux)**: выполните указанные ниже команды.

     ```
     sudo service acronis_mms restart
     ```

21.5 Миграция машины

Можно выполнить миграцию машины, восстановив ее резервную копию на машину, которая не является исходной.

Доступные варианты выполнения миграции приведены в следующей таблице.

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 Базис.Dynamix1
Физическая машина	+	-	+	+	+	+	+	+	+
Виртуальная машина Кибер Инфраструктура	-	+	+	-	+	+	+	+	+
Виртуальная машина VMware ESXi	+	+	+	+	+	+	+	+	+
Виртуальная машина Hyper-V	+	-	+	+	+	+	+	+	+
Виртуальная машина oVirt	+	+	+	+	+	+	+	+	+
Виртуальная машин	+	+	+	+	+	+	+	+	+

a SpaceVM									
Виртуальная машина ECP VeiL	+	+	+	+	+	+	+	+	+
Виртуальная машина OpenStack	-	+	+	-	+	+[2]	+[2]	+	+

[1] Платформы OpenStack и Базис.Dynamix 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 Базис.Dynamix 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 Базис.Dynamix. 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:

- 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.

21.5.1 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 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.

21.6 Виртуальные машины Windows Azure и Amazon EC2

Чтобы создать резервную копию виртуальной машины Windows Azure или Amazon EC2, установите агент защиты на 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 Windows Azure и Amazon EC2 невозможно загрузить с загрузочного носителя. Если необходимо выполнить восстановление в новую виртуальную машину Windows Azure или Amazon EC2, следуйте указанной ниже процедуре.

Порядок восстановления машины как виртуальной машины Windows Azure или Amazon EC2

1. Создайте новую виртуальную машину из образа/шаблона в Windows Azure или Amazon EC2. 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.

21.6.1 Требования к сети

Агенты, установленные на машинах, для которых выполняется резервное копирование, должны иметь возможность обмениваться данными с сервером управления по сети.

21.6.1.1 Локальное развертывание

- Если и агенты, и сервер управления установлены в облаке Azure/EC2, все машины уже находятся в одной сети. Никаких дополнительных действий не требуется.
- Если сервер управления находится вне облака Azure/EC2, то машины в облаке не будут иметь доступа к локальной сети, в которой он установлен. Чтобы агенты, установленные на таких машинах, могли связываться с сервером управления, необходимо создать подключение виртуальной частной сети (VPN) между локальной и облачной (Azure/EC2) сетями. Инструкции по созданию подключений VPN см. в следующих статьях:

  Amazon EC2: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

  Windows Azure: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

22 Защита SAP HANA

Защита SAP HANA описана в отдельном документе, который доступен по ссылке https://docs.cyberprotect.ru/ru-RU/CyberBackup/16.5/SapHanaBackup.pdf.

23 Отказоустойчивый кластер Кибер Бэкап

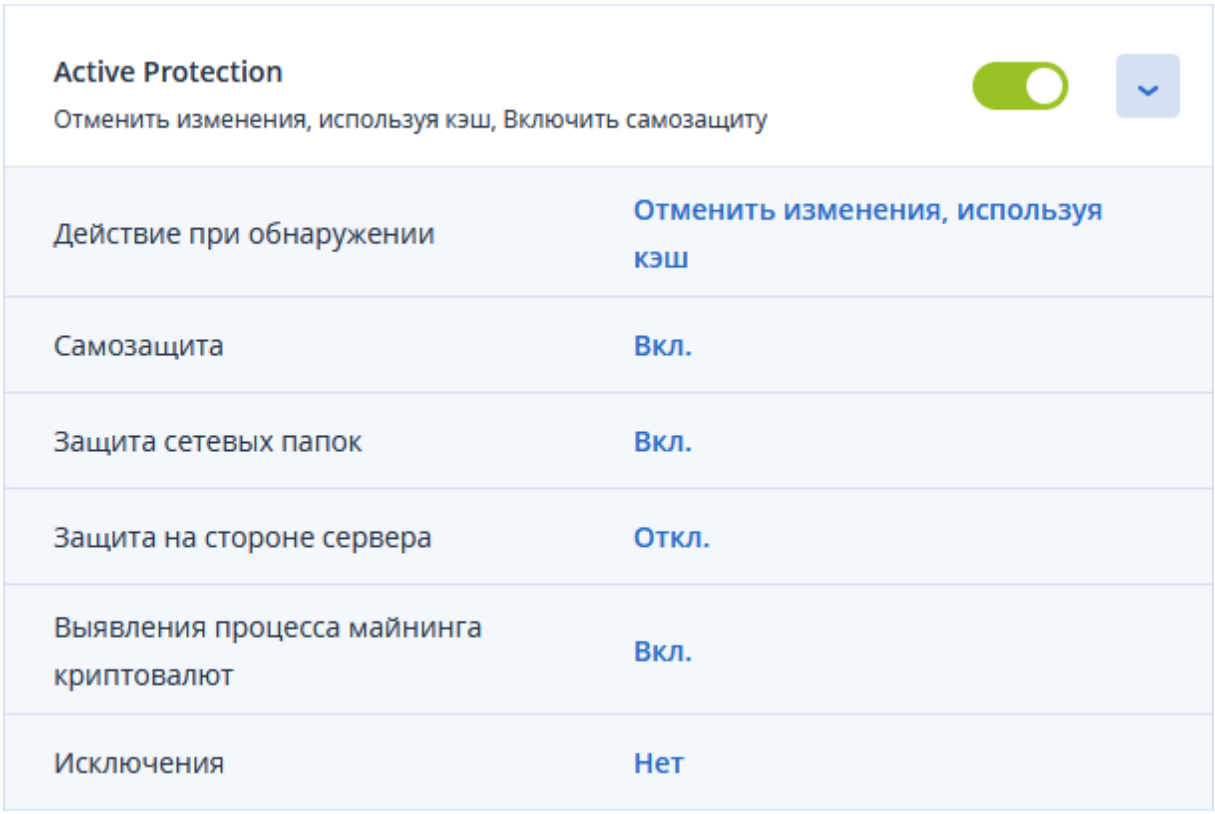
Пример настройки отказоустойчивого кластера сервера управления Кибер Бэкап в операционной системе РЕД ОС описан в отдельном документе.

24 Active Protection (Активная защита)

Служба Active Protection обеспечивает защиту компьютера от вредоносных программ, таких как вирусы-вымогатели и программы майнинга криптовалют. Вирусы-вымогатели шифруют файлы и требуют платы от пользователя за ключ расшифровки. Программы майнинга криптовалют запускают математические вычисления в фоновом режиме, тем самым похищая вычислительную мощность и сетевой трафик.

Active Protection – это отдельный модуль в плане защиты. Этот модуль имеет следующие настройки:

- Действие при обнаружении
- Самозащита
- Защита сетевых папок
- Защита на стороне сервера
- Обнаружение процессов майнинга криптовалют
- Исключения



Служба Active Protection доступна для машин со следующими операционными системами:

- Операционные системы для настольных компьютеров: Windows 7 с пакетом обновления 1 (SP1) и более поздних версий

Для машин с ОС Windows 7 должны быть установлены обновления: KB2533623 и KB3063858 для 32-битных или для 64-битных систем

- Серверные операционные системы: Windows Server 2008 R2 и более поздних версий.

На машине должен быть установлен агент для Windows.

Для более подробного ознакомления с возможностями Active Protection см. "Настройка модуля Active Protection" (стр. 487).

24.1 Настройка модуля Active Protection

24.1.1 Принцип работы

Active Protection отслеживает процессы, запущенные на защищенном компьютере. Когда процесс сторонней программы пытается шифровать файлы или добывать криптовалюту, Active Protection создает оповещение и выполняет дополнительные действия, если они указаны в настройках.

Вдобавок 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 активной защите обнаруживать новые вредоносные программы по их типичному поведению.

Значение по умолчанию: **Вкл** (включено).

24.1.2 Действие при обнаружении

В поле **Действие при обнаружении** выберите действие, которое будет выполняться при обнаружении подозрительной активности и затем нажмите **Готово**.

Вы можете выбрать один из следующих вариантов:

- **Только уведомить**

  Программа создаст оповещение о процессе.
- **Остановить процесс**

  Программа создаст оповещение о процессе и остановит процесс.
- **Отменить изменения, используя кэш**

  Программа создаст оповещение, остановит процесс и отменит изменения в файле, используя служебный кэш.

Значение по умолчанию: **Отменить изменения, используя кэш**.

24.1.3 Защита сетевых папок

Параметр **Защитите сетевые папки, назначенные как локальные диски** позволяет защитить от локальных вредоносных процессов сетевые папки, назначенные как локальные диски.

Этот параметр применяется к папкам, к которым предоставляется общий доступ по протоколам SMB или NFS.

Если файл изначально был расположен на подключенном диске, он не может быть сохранен в исходное местоположение при извлечении из кэша с помощью действия **Отменить изменения, используя кэш**. Вместо этого он будет сохранен в папку, указанную в настройках этой опции. Папка по умолчанию:

```
C:\ProgramData\Acronis\Restored Network Files
```

Если эта папка не существует, она будет создана. Если вы хотите изменить этот путь, укажите другую локальную папку. Сетевые папки, включая папки на подключенных дисках, не поддерживаются.

Значение по умолчанию: **Вкл**(включено).

24.1.4 Защита на стороне сервера (внешняя защита сетевых папок)

Этот параметр определяет, будут ли защищены от вредоносных программ сетевые папки, к которым вы предоставляете общий доступ, от внешних входящих подключений с других серверов в сети, которые потенциально могут представлять угрозы.

Значение по умолчанию: **Выкл** (выключено).

24.1.4.1 Настройка доверенных и заблокированных подключений

На вкладке **Доверенные** вы можете указать соединения, которым разрешено изменять любые данные. Необходимо указать имя пользователя и IP-адрес.

На вкладке **Заблокировано** вы можете указать соединения, которые не смогут изменять никакие данные. Необходимо указать имя пользователя и IP-адрес.

24.1.5 Самозащита

Параметр **Самозащита** предотвращает несанкционированные изменения в собственных процессах программного обеспечения, записях реестра, исполняемых и конфигурационных файлах и резервных копиях, расположенных в локальных папках. Мы не рекомендуем отключать эту функцию.

Значение по умолчанию: **Вкл** (включено).

24.1.5.1 Разрешить процессам изменять резервные копии

Параметр **Разрешить определенным процессам изменять резервные копии** можно задействовать, когда включена **Самозащита**.

Эта возможность относится к файлам, которые имеют расширения .tibx, .tib, .tia и расположены в локальных папках.

В настройках параметра можно указать процессы, которым разрешено изменять файлы резервных копий, даже если эти файлы защищены системой самозащиты. Это полезно, например, если вы удаляете файлы резервных копий или перемещаете их в другое место с помощью скрипта.

Если параметр отключен, 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.

Если эта функция включена, вы можете разрешить другим процессам изменять резервные копии. Укажите полный путь к исполняемому файлу процесса, начиная с буквы диска.

Значение по умолчанию: **Выключено**.

24.1.6 Выявление процессов майнинга криптовалют

Включение этого параметра позволяет обнаруживать вредоносное программное обеспечение для майнинга криптовалют.

Вредоносные программы для майнинга снижают производительность полезных приложений, увеличивают потребление электроэнергии, могут привести к сбоям системы и даже повреждению оборудования. Мы рекомендуем вам добавить вредоносные программы для майнинга в список вредоносных процессов, чтобы предотвратить их запуск.

Значение по умолчанию: **Вкл** (включено).

24.1.6.1 Настройки выявления процессов майнинга криптовалют

Выберите действие, которое программа будет выполнять при обнаружении активности майнинга криптовалют, а затем нажмите кнопку **Готово**. Вы можете выбрать один из следующих вариантов:

- **Только уведомить**
  Программа создает предупреждение о подозрительном процессе.
- **Остановить процесс**
  Программа создает предупреждение и останавливает подозрительный процесс.

Значение по умолчанию: **Остановить процесс**.

24.1.7 Исключения

Чтобы свести к минимуму ресурсы, используемые для поведенческого анализа, и исключить так называемые ложные срабатывания, когда доверенная программа рассматривается как программа-вымогатель, вы можете задать следующие настройки:

- На вкладке **Доверенные** вы можете указать:
  - Процессы, которые никогда не будут рассматриваться как вредоносные программы. Процессы, подписанные корпорацией Майкрософт, всегда являются надежными.
  - Папки, в которых не будут отслеживаться изменения файлов.
- На вкладке **Заблокировано** вы можете указать процессы, которые всегда будут заблокированы. Эти процессы не смогут запуститься до тех пор, пока на компьютере включен модуль Active Protection.

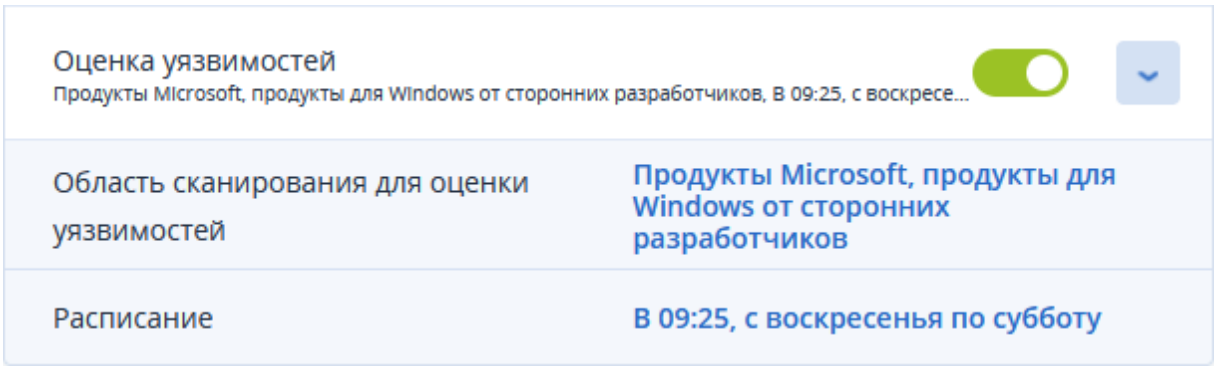
  Укажите полный путь к исполняемому файлу процесса, начиная с буквы диска. Например:

  ```
  C:\Windows\Temp\er76s7sdkh.exe
  ```

Значение по умолчанию: **Нет** (по умолчанию исключения не определены).

25 Оценка уязвимостей

Оценка уязвимостей – это процесс выявления, количественной оценки и определения приоритетов обнаруженных уязвимостей в системе. Используя модуль Оценка уязвимостей в плане защиты, вы можете сканировать свои компьютеры на наличие уязвимостей и проверять, обновлены ли операционные системы и установленные приложения и работают ли они должным образом.



Сканирование с оценкой уязвимостей поддерживается для компьютеров, работающих под управлением операционных систем Windows.

Процесс оценки уязвимостей состоит из следующих этапов:

1. Вы создаете план защиты с включенным модулем Оценка уязвимостей (см. раздел "Создание плана защиты" (стр. 157)), указываете настройки модуля Оценка уязвимостей (см. раздел "Настройка модуля Оценка уязвимостей" (стр. 493)) и назначаете план компьютерам.
2. Система по расписанию или по запросу отправляет агентам защиты команду на запуск сканирования с оценкой уязвимостей.
3. Агенты получают команду и запускают сканирование компьютеров на наличие уязвимостей.
4. После завершения сканирования с оценкой уязвимостей агенты создают результаты сканирования и отправляют их в Службу мониторинга.
5. Служба мониторинга обрабатывает данные от агентов и отображает результаты в списке найденных уязвимостей.

Вы можете отслеживать результаты сканирования с оценкой уязвимостей в разделе **Панель мониторинга** > **Обзор** > **Действия**.

25.1 Поддерживаемые продукты Microsoft и сторонние продукты

25.1.1 Поддерживаемые продукты Microsoft

ОС Windows

- Windows 7 (выпуски Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

ОС Windows Server

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office и связанные компоненты

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Компоненты, связанные с ОС Windows

- Internet Explorer
- Microsoft EDGE
- Проигрыватель Windows Media
- Платформа .NET Framework
- Visual Studio и приложения
- Компоненты операционной системы

Серверные приложения

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Sharepoint Server 2016

25.1.2 Поддерживаемые продукты для Windows от сторонних разработчиков

Служба Кибер Бэкап поддерживает оценку уязвимостей и исправление широкого диапазона сторонних приложений, включая инструменты совместной работы и клиенты VPN, которые имеют первоочередное значение для сценариев удаленной работы.

25.2 Настройка модуля Оценка уязвимостей

Вы можете указать следующие настройки в модуле Оценка уязвимостей.

25.2.1 Объект сканирования

Вы можете сканировать на наличие уязвимостей:

- Компьютеры с Windows:
  - **Продукты Microsoft**
  - **Продукты для Windows от сторонних разработчиков**.

25.2.2 Расписание

Задайте расписание проверки выбранных компьютеров с оценкой уязвимостей:

Запланируйте запуск задания, используя указанные ниже события.

- **Расписание по времени**: задание запускается в указанное время.
- **При входе пользователя в систему**: по умолчанию задание запускается при входе любого пользователя в систему. Можно изменить эту настройку в тех случаях, когда необходимо, чтобы задание мог инициировать только определенный пользователь.
- **При выходе пользователя из системы**: по умолчанию задание запускается при выходе любого пользователя из системы. Можно изменить эту настройку в тех случаях, когда необходимо, чтобы задание мог инициировать только определенный пользователь.

  Примечание
  Задание не будет запускаться при выключении системы. Выключение системы и выход из системы – это разные события в настройке расписания.

- **При запуске системы**: задание запускается при запуске операционной системы.
- **При выключении системы**: задание запускается при выключении операционной системы.

Настройка по умолчанию: **Расписание по времени**.

Тип расписания:

- **Ежемесячные**: выберите месяцы и недели или дни месяца для запуска задания.
- **Ежедневные**: выберите дни недели для запуска задания.
- **Ежечасно**: выберите дни недели, количество повторений и интервал времени для запуска задания.

Настройка по умолчанию: **Ежедневные**.

Запускать в: выберите точное время запуска задания.

Запускать в пределах диапазона дат: задайте диапазон, в течение которого будет действовать расписание.

Условия запуска: укажите все условия, которые одновременно должны быть удовлетворены для запуска задания.

Можно задать следующие дополнительные условия запуска:

- **Распределять время запуска заданий по доступному времени**: этот параметр позволяет задать интервал времени для выполнения задания, чтобы избежать проблем с загрузкой сети. Можно указать задержку в часах или минутах. Например, если для времени запуска по умолчанию задано 10:00 с задержкой 60 минут, задание будет запущено между 10:00 и 11:00.
- **Если компьютер выключен, выполнить пропущенные задания при его загрузке**
- **Отключить переход в спящий режим или режим гибернации при выполнении задания**
- **Выйти из спящего режима или режима гибернации для запуска запланированного задания**
- **Пользователь неактивен**
- **Пользователи завершили сеанс**
- **В интервале времени**: укажите интервалы запуска задания.
- **Сэкономить заряд батареи**: укажите параметры запуска задания в зависимости от состояния батареи компьютера.
- **Не запускать при работе на лимитном подключении**
- **Не запускать при подключении к следующим сетям Wi-Fi**: введите названия сетей Wi-Fi, при подключении к которым запуск задания не состоится.
- **Проверить IP-адрес устройства**: введите диапазон IP-адресов и условия запуска задания в зависимости от принадлежности IP-адреса компьютера к указанному вами диапазону.
- **Если условия запуска не выполнены, все равно запустить задание через**: укажите период времени, по истечении которого задание будет запущено независимо от выполнения других условий запуска.

По окончании задания условий нажмите **Готово**.

25.3 Просмотр обнаруженных уязвимостей

Обнаруженные уязвимости вы можете просмотреть в разделе **Управление программным обеспечением** > **Уязвимости**.

Название	Описание
Название	Название уязвимости.
Затронутые продукты	Программные продукты, для которых были обнаружены уязвимости.
Машины	Количество затронутых машин.
Серьезность	Серьезность обнаруженной уязвимости по общей системе оценки уязвимостей (CVSS): • **Критический**: 9 - 10 CVSS • **Высокий**: 7 - 9 CVSS • **Средний**: 3 - 7 CVSS • **Низкий**: 0 - 3 CVSS • **Нет**
Опубликовано	Дата и время публикации уязвимости в базе данных общеизвестных уязвимостей (CVE).
Обнаружено	Дата первого обнаружения уязвимости.

Вы можете найти описание обнаруженной уязвимости, щелкнув по ее названию в списке.

26 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 **Все устройства** невозможно создать группу.

Одно устройство может входить в несколько групп.

26.1 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.

26.2 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

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.

26.3 Создание статической группы

1. Нажмите **Устройства** и выберите встроенную группу, которая содержит устройства, для которых вы хотите создать статическую группу.
2. Нажмите на значок шестеренки около группы, в которой вы хотите создать группу.
3. Нажмите кнопку **Новая группа**.
4. Укажите имя группы и затем нажмите кнопку **OK**.

   Новая группа появится на дереве групп.

26.4 Добавление устройств в статические группы

1. Щелкните **Устройства** и выберите устройства для добавления в группу.
2. Нажмите кнопку **Добавить в группу**.

   Программное обеспечение отобразит дерево групп, в которые можно добавить выбранное устройство.
3. Если требуется создать новую группу, выполните следующие действия. В противном случае пропустите этот шаг.
   a. Выберите группой, в которой необходимо создать группу.
   b. Нажмите кнопку **Новая группа**.
   c. Укажите имя группы и затем нажмите кнопку **OK**.
4. Выберите группу, в которую необходимо добавить устройство, а затем нажмите кнопку **Выполнено**.

Другой способ добавить устройства в статическую группу – выбрать группу и щелкнуть **Добавить устройства**.

26.5 Создание динамической группы

1. Нажмите **Устройства** и выберите группу, которая содержит устройства, для которых необходимо создать динамическую группу.
2. Выполните поиск устройств с помощью поля поиска. Можно использовать составные условия поиска и операторы, описанные ниже.
3. Щелкните **Сохранить как** рядом с полем поиска.

Примечание
Определенные критерии поиска не поддерживаются для создания группы. См. таблицу в разделе "Условия поиска" ниже.

4. Укажите имя группы и затем нажмите кнопку **OK**.

26.5.1 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
parameters.MacAddress	MAC-адрес.	parameters.MacAddress LIKE "00-22-4D-50-25-E5"	Да
comment	Комментарий для устройства. Значение по умолчанию: • Для физических машин с ОС Windows описание	comment = 'important machine' comment = '' (все машины без комментария)	Да

	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**.		
ip	IP-адрес (только для физических машин).	ip RANGE ('10.250.176.1','10.250.176.50')	Да
cpuArch	Архитектура CPU. Возможные значения: • "x64" • "x86"	cpuArch = "x64"	Да
memorySize	Размер ОЗУ в мегабайтах (МиБ).	memorySize < 1024	Да
cpuName	Имя ЦП.	cpuName LIKE '%XEON%'	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
parameters.Architecture	Архитектура операционной	parameters.Architecture = "x86"	Да

	системы. Возможные значения: • "x86" • "x64"		
osName	Название операционной системы.	osName LIKE '%Windows 10%'	Да
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,	tenant = 'Unit 1'	Да

	которому принадлежит устройство.		
tenantId	Идентификатор отдела, которому принадлежит устройство. Для получения идентификатора отдела напротив пункта **Устройства** выберите устройство и выберите пункт **Сведения** > **Все свойства**. Идентификатор отобразится в поле ownerId.	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	Да
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'	status = 'ok'	Нет

	• 'error' • 'critical'		
protectedByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором. Для получения идентификатора плана нажмите **Планы** > **Резервное копирование**, выберите план, нажмите на диаграмму в колонке **Статус** и затем нажмите на статус. Будет создан новый поиск с идентификатором плана.	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
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	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет

	защиты с указанным идентификатором и со статусом **Выполняется**.		
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 единице Active Directory.	ou IN ('RnD', 'Computers')	Да
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
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 защиты напротив пункта **Устройства** выберите машину и щелкните **Сведения** > **Все свойства**. Используйте значение "id" свойства agent.	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Да
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

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

26.5.2 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: • * или % Астериск или знак процента могут заменять собой ни одного, один или несколько символов. • _ 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 этом параметре учитывается регистр.	osType IN ('windows', 'linux')
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')

26.6 Применение плана защиты к группе

1. Щелкните **Устройства**, а затем выберите встроенную группу, содержащую в себе группу, к которой необходимо применить план защиты.

   В программе будет выведен список дочерних групп.
2. Выберите группу, к которой необходимо применить план защиты.
3. Щелкните **Групповое резервное копирование**.

   В программе выводится список планов защиты, которые можно применить к группе.
4. Выполните одно из следующих действий:
   - Разверните существующий план защиты, а затем щелкните **Применить**.
   - Щелкните **Создать новый** и создайте новый план защиты, как описано в теме Резервное копирование.

27 Мониторинг и отчеты

Панель мониторинга **Обзор** дает возможность отслеживать текущее состояние защищенной инфраструктуры.

Раздел **Отчеты** дает возможность создавать запланированные отчеты и отчеты по требованию с данными о защищенной инфраструктуре. Этот раздел доступен только при наличии лицензии Advanced.

27.1 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.

Лицензия Advanced 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:

- 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.

27.1.1 Кибер Бэкап

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

27.1.2 Статус защиты

27.1.2.1 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.

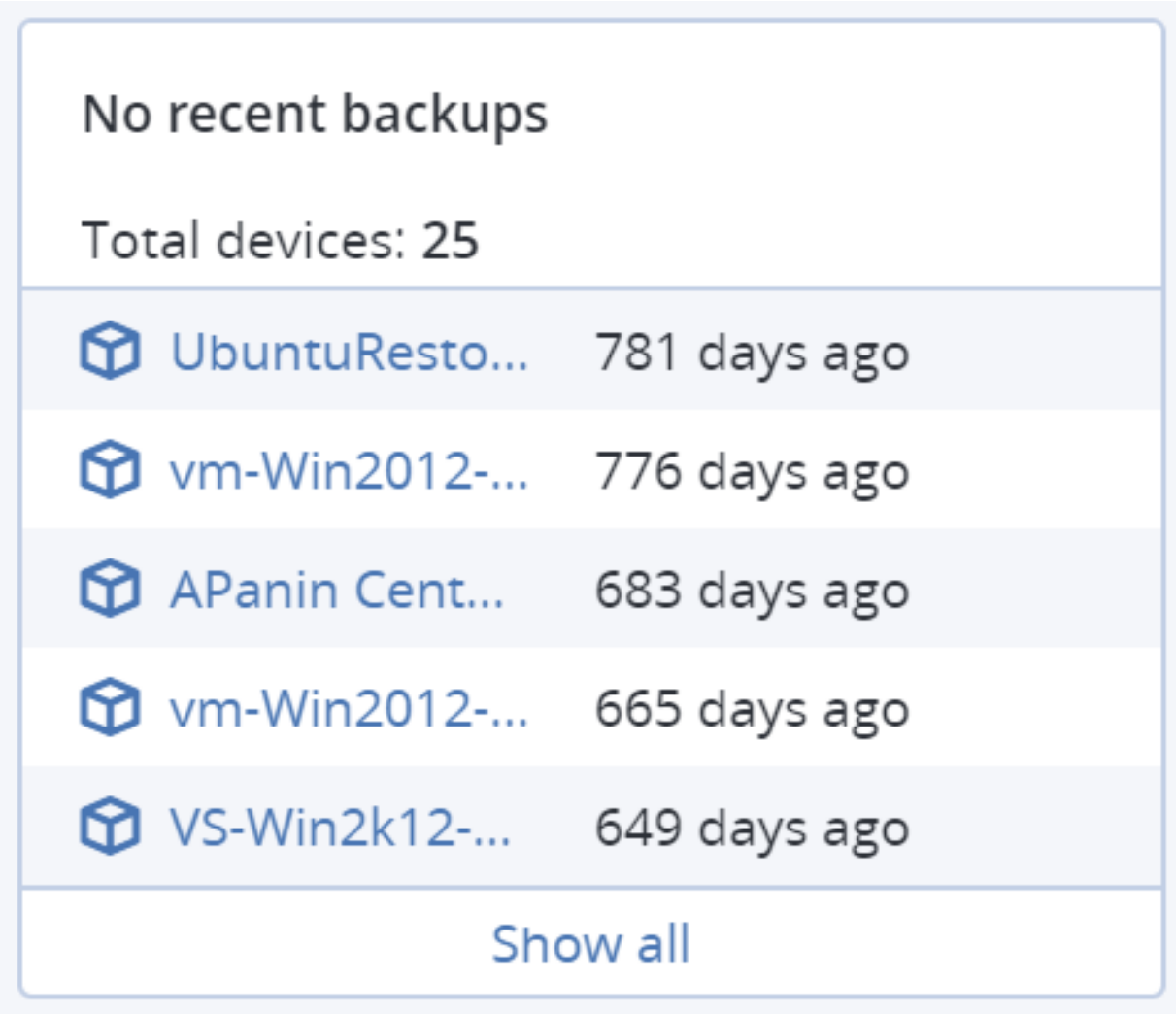
Если щелкнуть состояние машины, для получения более подробной информации откроется список машин, которые имеют данное состояние.

27.1.2.2 Обнаруженные машины

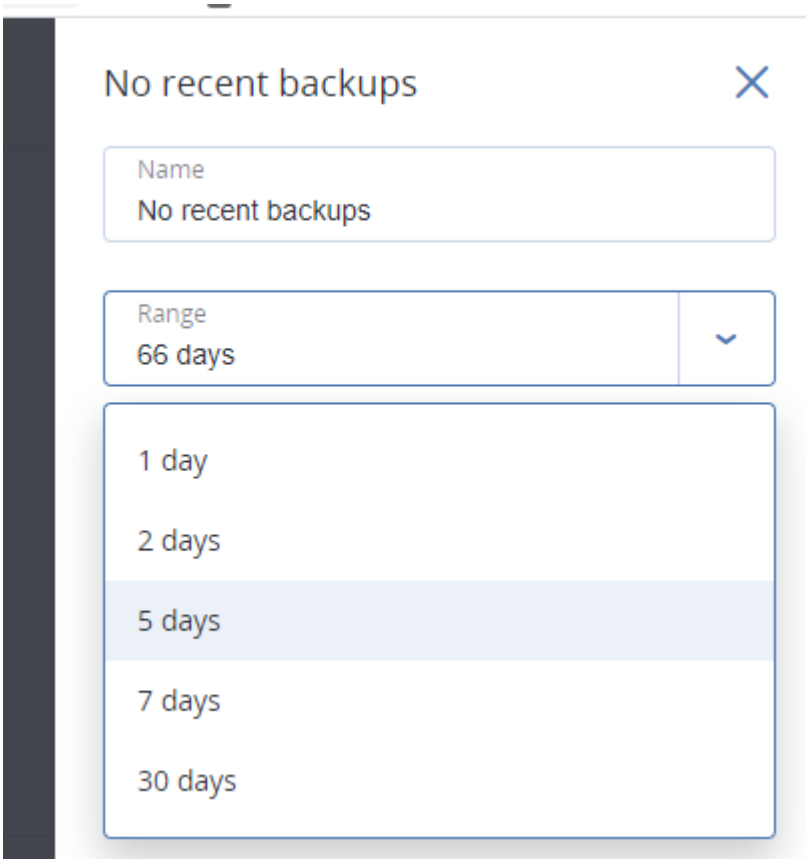
В этом виджете показан список машин, обнаруженных за указанный период времени.

27.1.3 Нет недавних 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.



По умолчанию, когда вы добавляете этот виджет, 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 180.



27.2 Вкладка «Действия»

На вкладке **Действия** предоставлен обзор текущих и последних действий. По умолчанию период хранения составляет 180 дней.

Чтобы настроить содержимое вкладки **Действия**, щелкните значок шестерни и выберите столбцы, которые нужно отобразить.

Чтобы ход выполнения действия отображался в реальном времени, установите флажок **Обновлять автоматически**. Однако 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**:
  это учетная запись, от имени которой запущено действие.

Кроме того, можно отфильтровать действия по следующим свойствам:

- **Состояние**:
  например, «Успешно», «Сбой», «Выполняется», «Отменено».
- **Тип**:
  например, «Применение плана», «Удаление резервных копий», «Установка обновлений

программного обеспечения».

- **Время**:
  например, последние действия, действия за последние 24 часа или действия в течение указанного периода времени в пределах периода хранения по умолчанию.

Порядок изменения периода хранения

1. На машине с выполняющимся сервером 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 понижение может привести к удалению незавершенных активностей, а сильное повышение к снижению производительности сервера управления.

4. Перезапустите службу Киберпротект Service Manager Service, как описано в разделе Использование сертификата, выданного доверенным центром сертификации.

27.3 Отчеты

Вы можете использовать предварительно созданные отчеты или создать пользовательский отчет. Отчет может включать набор виджетов панели мониторинга.

Вы можете только настроить отчеты для отделов, которыми вы управляете.

Отчеты могут быть отправлены по электронной почте или загружены по расписанию. Для отправки отчетов по электронной почте убедитесь в том, что у вас сконфигурированы настройки Почтового сервера. При создании отчета с использованием стороннего программного обеспечения запланируйте сохранение отчетов в формате .xlsx в указанную папку.

Доступные отчеты зависят от выпуска Кибер Бэкап. Ниже перечислены отчеты по умолчанию

Имя отчета	Доступность	Описание
Оповещения	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает оповещения, выполненные за указанный период времени.
Резервные копии	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает подробную информацию о текущих резервных копиях и точках восстановления.
Текущий статус	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает текущий статус вашей среды.
Ежедневные задания	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Обнаруженные машины	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает все машины, обнаруженные в сети организации.
Лицензии	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает сводную информацию о доступных лицензиях.
Хранилища	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает статистику использования хранилищ резервных копий за указанный период времени.
Сводные данные	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает сводную информацию об устройствах, защищенных за указанный период времени.
Действия с лентой	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает список лент, которые использовались в течение последних 24 часов.

Еженедельные действия	Кибер Бэкап Advanced Кибер Бэкап Advanced	Показывает сводную информацию о действиях, выполненных за указанный период времени.

27.3.0.1 Основные операции с отчетами

- Для просмотра отчета щелкните его имя.
- Чтобы выполнить дополнительные операции в отчете, щелкните значок многоточия (...). Такие же операции доступны из отчета.

Порядок добавления отчета

1. Щелкните **Добавить отчет**.
2. Выполните одно из следующих действий:
   - Чтобы добавить предопределенный отчет, щелкните его имя.
   - Чтобы добавить настраиваемый отчет, щелкните **Пользовательский**. В список отчетов добавляется новый отчет с именем **Пользовательский**. Откройте этот отчет и добавьте в него виджеты.
3. [Необязательно] Для изменения положения виджетов перетащите их.
4. [Необязательно] Измените отчет, как описано ниже.

Порядок изменения отчета

1. Щелкните значок многоточия (...) рядом с именем отчета и щелкните **Настройки**.
2. Внесите изменения в отчет. Можно сделать следующее:
   - Переименовать отчет.
   - Изменить диапазон времени для всех виджетов, включенных в отчет.
   - Запланировать отправку отчета по электронной почте в формате PDF и (или) XLSX.
3. Нажмите кнопку **Сохранить**.

Порядок поставки отчета в расписание

1. Выберите отчет и затем нажмите **Запланировать**.
2. Включите переключатель **Отправить запланированный отчет**.
3. Выберите: отправлять отчеты по электронной почте, сохранять в папку, и то, и другое. В зависимости от выбора укажите адрес электронной почты, путь к папке или и то, и другое.
4. Выберите формат отчета: .pdf, .xlsx или и то, и другое.
5. Выберите отчетный период: 1 день, 7 дней или 30 дней.
6. Выберите дни и время отправки/сохранения отчета.
7. Нажмите кнопку **Сохранить**.

27.3.0.2 Экспорт и импорт структуры отчета

Вы можете экспортировать и импортировать структуру отчета (набор виджетов и настройки расписания) в файл .json. Это может оказаться полезным при переустановке сервера управления или для копирования структуры отчета на другой сервер управления.

Для экспорта структуры отчета выберите отчет и затем нажмите **Экспорт**.

Для импорта структуры отчета нажмите **Создать отчет** и затем нажмите **Импорт**.

27.3.0.3 Дамп данных отчета

Вы можете сохранить дамп данных отчета в файл .csv. Дамп содержит все данные отчета (без фильтрации) за определенный промежуток времени.

ПО динамически генерирует дамп данных. При указании большого промежутка времени данное действие может долго выполняться.

Дамп данных отчета

1. Выберите отчет и затем нажмите **Открыть**.
2. Щелкните значок многоточия (...) в правом верхнем углу, а затем щелкните **Данные дампа**.
3. В **Хранилище** укажите путь к папке для файла .csv.
4. В **Диапазон времени** укажите диапазон времени.
5. Нажмите кнопку **Сохранить**.

27.4 Настройка важности оповещений

Оповещение – это сообщение, предупреждающее о текущей или потенциальной проблеме. Можно использовать оповещения разными способами:

- Раздел **Оповещения** на вкладке **Обзор** позволяет быстро определять и решать проблемы путем мониторинга текущих оповещений.
- В области **Устройства** статус устройства основывается на оповещениях. Колонка **Статус** позволяет фильтровать устройства с проблемами.
- При настройке уведомлений по электронной почте можно выбрать, какие оповещения запустят уведомление.

Оповещение может иметь одну из следующих степеней серьезности:

- **Критическая**
- **Ошибка**
- **Предупреждение**

Можно изменить степень серьезности оповещения или полностью отключить их с помощью файла настройки оповещений, как описано ниже. Эта операция требует перезапуска сервера управления.

Изменение степени серьезности оповещения не повлияет на уже созданные оповещения.

27.4.1 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 серьезности оповещения. Он может иметь одно из следующих значений: критическаяошибкапредупреждение.

Дополнительный ключ enabled определяет, включено ли оповещение. Значение должно быть true или false. По умолчанию (этот ключ не задан) все оповещения включены.

Для изменения степени серьезности оповещения или его отключения

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 серьезности 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.

Для перезапуска службы сервера управления в ОС Windows

1. В меню **Пуск** выберите команду **Выполнить** и введите: **cmd**
2. Нажмите кнопку **OK**.
3. Выполните следующие команды:

```
net stop acrmngsrv
net start acrmngsrv
```

Для перезапуска службы сервера управления в ОС Linux

1. Откройте **приложение терминала**.
2. Выполните следующую команду в любом каталоге:

```
sudo service acronis_ams restart
```

28 Расширенный выбор вариантов хранения

28.1 Ленточные устройства

В следующих разделах подробно описано использование ленточных устройств для хранения резервных копий.

28.1.1 Что такое ленточное устройство?

Ленточное устройство – общий термин, который обозначает библиотеку ленточных носителей или изолированный ленточный носитель.

Библиотека ленточных носителей (автоматизированная библиотека) – устройство хранения большой емкости, содержащее следующие элементы:

- одно или несколько ленточных устройств;
- слоты для лент (до нескольких тысяч);
- одно или несколько устройств смены носителей (робототехнических механизмов) для перемещения лент между слотами и ленточными устройствами.

Библиотека может содержать и другие компоненты, например устройства чтения штрихкодов или принтеры штрихкодов.

Автоматический загрузчик – это особая разновидность библиотеки ленточных носителей. Он содержит один привод, несколько слотов, устройство смены носителей и устройство чтения штрихкодов (дополнительно).

Изолированное ленточное устройство (называемое также **стримером**) содержит один слот и в каждый момент времени может содержать только одну ленту.

28.1.2 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.

28.1.2.1 Совместимость с RSM и программным обеспечением других поставщиков

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.

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.

28.1.2.2 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.

28.1.2.3 База данных управления лентами

Информация обо всех ленточных устройствах, подключенных к машине, хранится в базе метаданных управления лентами. Путь к базе данных по умолчанию:

- 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.

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.

28.1.2.4 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.

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. 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

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 пока, пока не будет достигнуто приемлемое значение или значение 32 байт. Если приемлемое значение не найдено, то программа умножает указанное значение на два до тех пока, 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. 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, но не меньше значения параметра **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 пока, 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.

28.1.2.5 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.

28.1.2.6 Параллельные операции

Кибер Бэкап может одновременно выполнять операции с различными компонентами ленточного устройства. В ходе операции с накопителем (резервное копирование, восстановление, повторное 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.

Операции, которые нельзя выполнить параллельно, помещаются в очередь.

28.1.2.7 Ограничения

Существуют следующие ограничения использования ленточных устройств:

1. Ленточные устройства не поддерживаются, если машина загружается с 32-разрядного загрузочного носителя на базе Linux.
2. Невозможно создать резервную копию следующих типов данных на лентах: Почтовые ящики Microsoft Office 365, почтовые ящики Microsoft Exchange.
3. Невозможно выполнить резервное копирование физических и виртуальных машин с поддержкой приложений.
4. Консолидация резервных копий на лентах невозможна. В результате, схема резервного копирования **Всегда инкрементное** недоступна при резервном копировании на ленты.
5. Дедупликация резервных копий на лентах невозможна.
6. Программа не может автоматически перезаписать ленту с резервными копиями, которые не удалены, а также в тех случаях, когда на других лентах есть зависимые резервные копии.

   Единственное исключение из этого правила составляют случаи, когда включен параметр «Перезаписать ленту в автономном ленточном устройстве при создании полной резервной копии».
7. Восстановление из резервной копии на ленте под управлением операционной системы невозможно, если это восстановление требует перезагрузки операционной системы. Для такого восстановления используйте загрузочный носитель.
8. Можно проверить любые резервные копии на лентах, однако выбрать для проверки целое хранилище на ленте или ленточное устройство невозможно.
9. Управляемое хранилище на лентах невозможно защитить паролем. Вместо этого защитите паролем резервные копии.
10. При репликации резервных копий на ленты не поддерживается мультиплексирование (см. "Управление лентами" (стр. 242)).
11. Устройства, использующие протокол NDMP (Network Data Management Protocol), не поддерживаются.
12. Принтеры штрихкодов не поддерживаются.
13. Ленты, форматированные в файловую систему Linear Tape File System (LTFS), не поддерживаются.
14. Если при резервном копировании на ленте заканчивается свободное место, продолжить копирование можно только на пустую ленту.
15. 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.
16. Не рекомендуется использовать в ленточных библиотеках кассеты без бар-кодов. Использование таких кассет может приводить к сбоям.

28.1.3 Начало работы с ленточным устройством

28.1.3.1 Резервное копирование машины на локально подключенное ленточное устройство

Предварительные требования

- Ленточное устройство должно быть подключено к машине в соответствии с инструкциями производителя.
- На машине установлен агент защиты.

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 **Обнаружить устройства**.
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».

      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 программой Киберпротект. Перед перемещением таких лент в пул **Свободные ленты** убедитесь, что эти резервные копии больше не нужны.

Резервное копирование

Создайте план защиты, как описано в разделе Резервное копирование. Затем укажите хранилище резервных копий, щелкнув **Пул лент**.

Результаты

- Для доступа к хранилищу, где будут созданы резервные копии, выберите **Хранилище резервных копий** > **Пул лент**.
- Ленты с резервными копиями будут перемещены в пул.

28.1.3.2 Резервное копирование на ленточное устройство, подключенное к узлу хранения

Предварительные требования

- Узел хранения должен быть зарегистрирован на сервере управления.
- Ленточное устройство должно быть подключено к узлу хранения в соответствии с инструкциями производителя.

Перед резервным копированием

1. Загрузите ленты в ленточное устройство.
2. Войдите на 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 **Обнаружить устройства**.
5. Проведите инвентаризацию лент:
   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 программой Киберпротект. 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.

   Подробнее. Наличие нескольких пулов позволяет использовать отдельный набор лент для каждой машины или каждого отдела компании. Разные пулы помогают не путать резервные копии, находящиеся на одной ленте, но созданные с помощью разных планов защиты.

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.

   Подсказка. Чтобы узнать, может ли пул принимать ленты из пула **Свободные ленты**, щелкните пул, а затем щелкните **Информация**.

Резервное копирование

Создайте план защиты, как описано в разделе Резервное копирование. При указании хранилища резервных копий выберите созданный пул ленты.

Результаты

- Для доступа к хранилищу, где будут созданы резервные копии, выберите **Резервные копии**, затем выберите имя созданного пула ленты.
- Ленты с резервными копиями будут перемещены в выбранный пул.

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 назначения резервных копий.

28.1.3.3 Восстановление с ленточного устройства из операционной системы

Как выполнить восстановление с ленточного устройства из операционной системы

1. Войдите на 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 **Обзор** > **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.
   d. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

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.

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.

28.1.3.4 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 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.

28.1.3.5 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.
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.

28.1.4 Управление лентами

28.1.4.1 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 отключены от RSM.

Как правило, ленточное устройство обнаруживается автоматически сразу же после подключения устройства к машине, на которой установлен продукт. Однако вам может потребоваться определение 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 **Обнаружение ленточных устройств**. Будут отображены подключенные ленточные устройства, их накопители и слоты.

28.1.4.2 Пулы лент

В программе резервного копирования используются пулы лент, представляющие собой логические группы лент. Программное обеспечение содержит следующие стандартные пулы лент: **Нераспознанные ленты**, **Импортированные ленты** и **Свободные ленты**. Кроме того, предусмотрена возможность создания собственных пользовательских пулов.

Пул и пользовательские пулы также используются в качестве хранилищ резервных копий.

Предварительно заданные 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 помечает ее как пустую. Если лента содержит резервные копии, они помечаются значком  . Когда программа начнет перезаписывать ленту, данные, связанные с резервными копиями, будут удалены из базы данных.

Пул используется по умолчанию для резервного копирования, когда не требуется создавать собственные пулы. Обычно он применяется к одному ленточному устройству с небольшим числом лент.

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.

28.1.4.3 Операции с пулами

Создание пула

Как создать 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. Нажмите **Создать пул**.
4. Введите имя пула.
5. [Необязательно] Снимите флажок напротив пункта **Автоматически брать ленты из пула «Свободные ленты»...**. Если флажок снят, только ленты, включенные в пул в определенный момент, будут использоваться для резервного копирования.
6. Нажмите кнопку **Создать**.

Изменение пула

Можно изменить параметры пула.

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 пул и нажмите кнопку **Редактировать пул**.
4. Можно изменить имя или настройки пула. Дополнительные сведения о настройках пула см. в разделе Создание пула.
5. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

Удаление пула

Можно удалять только пользовательские пулы. Нельзя удалить предварительно заданные пулы лент (**Нераспознанные ленты**, **Импортированные ленты** и **Свободные ленты**).

Примечание
После удаления пула не забудьте внести 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. Выберите пул, в который будут перемещаться ленты из удаляемого пула после удаления.
5. Нажмите кнопку **OK**, чтобы удалить пул.

28.1.4.4 Операции с лентами

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.

Перемещение в другой пул

Операция позволяет перенести одну или несколько лент из одного пула в другой.

При переносе ленты в пул **Свободные ленты** программа помечает ее как пустую. Если лента содержит резервные копии, они помечаются значком  . Когда программа начнет перезаписывать ленту, данные, связанные с резервными копиями, будут удалены из базы данных.

Примечание о перемещении лент с резервными копиями:

Перед перемещением лент с резервными копиями из одного пула резервного копирования в другой рекомендуется выполнить одно из следующих действий:

- удалить архивы из хранилища, связанного с пулом, из которого происходит перемещение;
- выполнить очистку лент;
- переместить ленты в пул **Свободные ленты**.

Иначе в хранилище, связанном с предыдущим пулом, все еще могут отображаться архивы, относящиеся к перемещенной ленте. В таком случае удалите их вручную.

Примечания о конкретных типах лент:

- В пул **Свободные ленты** нельзя перенести защищенные от записи и однократно записанные ленты WORM (Write-Once-Read-Many – однократная запись, множественное чтение).
- Чистящие ленты всегда отображаются в пуле **Нераспознанные ленты**; перенести их в другой пул нельзя.

Порядок переноса лент в другой 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. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Переместить в пул**.
5. [Необязательно] Нажмите **Создать новый пул**, если требуется создать другой пул для выбранных лент. Выполните действия, описанные в разделе «Создание пула».
6. Выберите пул, в который необходимо перенести ленты.
7. Нажмите **Переместить** для сохранения изменений.

Инвентаризация

Операция инвентаризации обнаруживает ленты, загружаемые в ленточное устройство, и присваивает имена лентам, у которых их нет.

Методы инвентаризации

Существует два метода инвентаризации.

Быстрая инвентаризация

Агент или узел хранения сканирует штрихкоды лент. С помощью штрихкодов программное обеспечение может быстро вернуть ленту в пул, где она находилась раньше.

Используйте этот метод для распознания лент, которые используются одним и тем же ленточным устройством, подключенным к одной и той же машине. Другие ленты будут направлены в пул **нераспознанных лент**.

Если в библиотеке ленточных носителей нет обработчика штрихкода, все ленты направляются в пул **нераспознанных лент**. Для распознания лент выполните полную инвентаризацию или используйте комбинацию быстрой и полной инвентаризации, как описано далее в этом разделе.

Полная инвентаризация

Агент или узел хранения считывает теги, записанные ранее, и анализирует прочую информацию о содержимом загружаемых лент. Выберите этот метод для распознания пустых лент и лент, записанных программным обеспечением, на любом ленточном устройстве и любой машине.

В следующей таблице показаны пулы, куда направляются ленты в результате полной инвентаризации.

Кто использовал ленту	Кто считывает ленту	В какой пул направляется лента
Агент	Тот же агент	Пул, где лента была раньше
	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 стороннего производителя для резервного копирования	Агент или узел хранения	**Нераспознанные ленты**

Ленты определенных типов направляются в определенные пулы.

Тип ленты	В какой пул направляется лента
Пустая лента	**Свободные ленты**

Пустая лента, защищенная от записи	**Нераспознанные ленты**
Очистка ленты	**Нераспознанные ленты**

Быструю инвентаризацию можно применять только к целым ленточным устройствам. Полную инвентаризацию можно применять к целым ленточным устройствам, отдельным приводам и слотам. Однако для автономных ленточных устройств всегда выполняется полная инвентаризация, даже если выбрана быстрая инвентаризация.

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

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.

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.

За одну операцию можно просканировать ленты из одного пула. Для операции могут быть выбраны только ленты устройств, находящихся в оперативном режиме.

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 направляются именно в этот пул. Также возможно повторное сканированиелюбого другого пула.
6. /[Необязательно] Выберите отдельные ленты для индивидуального сканирования./
7. Нажмите **Повторное сканирование**.
8. Выберите пул, в которое будут помещаться резервные копии после обнаружения..
9. При необходимости установите флажок **Включить восстановление файлов из образов дисков на лентах**.

   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. Если ленты содержат защищенные паролем резервные копии, установите соответствующий флажок и укажите пароль для этих резервных копий в поле пароля. Если пароль не указан или недействителен, резервные копии не будет обнаружены. Помните об этом в случае, если после повторного сканирования резервные копии не обнаружены.

    Подсказка. Если ленты содержат несколько резервных копий, защищенных разными паролями, необходимо повторить сканирование несколько раз, поочередно указывая пароли.
11. Нажмите **Запуск повторного сканирования** для запуска повторного сканирования.

Результат: Выбранные ленты перемещаются в выбранный пул. Резервные копии, сохраненные на лентах находятся в этом пуле. Резервная копия, расположенная на нескольких лентах, не появится в пуле, пока не будут повторно сканированы все эти ленты.

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.

Стирание

При стирании 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.

Если стертая лента находилась в пуле **Нераспознанные ленты** или **Импортированные ленты**, она перемещается в пул **Свободные ленты**. Лента, размещенная в любом другом пуле, не перемещается.

Порядок стирания 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 **Стереть**. Система попросит подтвердить операцию.
5. Выберите способ стирания: быстрый или полный.
6. Нажмите кнопку **Стереть**, чтобы начать операцию.

   Подробнее. Операцию стирания отменить невозможно.

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.

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

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.

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 Понедельник для ленты 1, Вторник 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.
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.

28.2 Узлы 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).

28.2.1 Установка узла хранения и службы каталогизации

Перед установкой узла хранения убедитесь, что машина соответствует системным требованиям.

Мы рекомендуем устанавливать узел хранения и службу каталогов на отдельные машины. Системные требования к машине, на которой установлена служба каталогизации, описаны в разделе «Лучшие практики каталогизации».

Порядок установки узла хранения и (или) службы каталогизации

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щелкните **Язык установки**.
3. Примите условия лицензионного соглашения.
4. Щелкните **Установить агент защиты**.
5. Щелкните **Настройка параметров установки**.
6. Рядом с пунктом **Устанавливаемые компоненты** щелкните **Изменить**.
7. Выберите устанавливаемые компоненты:
   - Для установки узла хранения установите флажок **Узел хранения**. Флажок **Агент для Windows** будет установлен автоматически.

- Для установки службы каталогов установите флажок **Служба каталогов**.
- Если на этой машине не нужно устанавливать другие компоненты, снимите соответствующие флажки.

Чтобы продолжить, нажмите кнопку **Готово**.

8. 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".

      Если вы не являетесь администратором сервера управления, машину можно зарегистрировать и в этом случае. Для этого выберите параметр **Подключиться без проверки подлинности**. Это можно сделать, если на сервере управления разрешена анонимная регистрации (имейте в виду, что она может быть отключена).
   d. Нажмите кнопку **Готово**.
9. При поступлении запроса выберите, добавлять ли машину с узлом хранения и (или) службой каталогизации 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 «Администраторы и отделы».
10. [Необязательно] Измените другие настройки установки, как описано в разделе «Настройка параметров установки».
11. Нажмите **Установить**, чтобы продолжить установку.
12. После завершения установки нажмите кнопку **Закрыть**.

28.2.2 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.

Порядок создания управляемого хранилища в локальной или сетевой папке

1. Выполните одно из следующих действий:
   - Щелкните **Хранилище 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** > **Узла 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.
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 **Хранилище 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».
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».
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».

10. [Необязательно] Выберите, нужно ли каталогизировать резервные копии, сохраненные в данном хранилище. Каталог данных позволяет легко найти требуемую версию данных и выбрать ее для восстановления.

    Если на сервере управления зарегистрировано несколько служб каталогизации, можно выбрать службу каталогизации, которая выполнит каталогизацию резервных копий, которые находятся в хранилище.

    Каталогизацию можно включить или отключить позже, как описано в разделе «Включение или отключение каталогизации».
11. Нажмите кнопку **Готово**, чтобы создать хранилище.

Для создания управляемого хранилища на ленточном устройстве

1. Щелкните **Хранилище 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», 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 **Хранилище резервных копий** > хранилище > **Изменить**, затем измените значение поля **Адрес**.

28.2.3 Дедупликация

28.2.3.1 Ограничения дедупликации

Общие ограничения

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.

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.

28.2.3.2 Рекомендации по дедупликации

Дедупликация – это сложный процесс, зависящий от многих факторов.

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.
- 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

$$S = 5000 * 90 / 65536 +10 = 17 \text{ ГБ}$$

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.

Достаточное свободное пространство в хранилище

Для дедупликации в месте назначения 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.

28.2.4 Защита хранилища паролем

Если для хранилища установлена защита паролем, то все данные, которые в него заносятся, будут защищены. 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.

Как защитить хранилище паролем

1. Укажите и подтвердите слово (пароль), которое будет служить ключом защиты.
   В слове учитывается регистр. Это слово потребуется только при подключении хранилища к другому узлу хранения.
2. Выберите один из следующих уровней защиты паролем:
   - **Низкий** – содержимое хранилища будет защищено паролем с уровнем защиты **Низкий**.
   - **Средний** – содержимое хранилища будет защищено паролем с уровнем защиты **Средний**.
   - **Высокий** – содержимое хранилища будет защищено паролем с уровнем защиты **Высокий**.
3. Нажмите кнопку **OK**.

Чем выше уровень защиты паролем, тем лучше будут защищены резервные копии.

Слово на диске не хранится. Такая схема защиты позволяет обезопасить резервные копии от несанкционированного доступа, но восстановить утраченное слово невозможно.

28.2.5 Каталогизация

28.2.5.1 Каталог данных

Каталог данных позволяет легко найти требуемую версию данных и выбрать ее для восстановления. В каталоге данных отображаются данные в управляемых хранилищах, для которых включена каталогизация.

Раздел **Каталог** появляется на вкладке **Хранилища резервных копий** только в том случае, если по меньшей мере одна служба каталога зарегистрирована на сервере управления. Информацию по установке сервиса каталога см. по ссылке «Installing a storage node and a cataloging service (Установка узла хранения и службы каталогизации)».

Раздел **Каталог** видим только для администраторов организации.

Ограничения

Каталогизация поддерживается только для резервных копий физических машин на уровне файлов и резервных копий виртуальных машин.

В каталоге не отображаются следующие данные:

- данные резервных копий, защищенных паролем;
- данные, резервная копия которых находится на ленточных носителях;
- Данные, резервная копия которых создана Кибер Бэкап версий, предшествующих 12.5

Выбор данных резервной копии для восстановления

1. Щелкните **Хранилище резервных копий** > **Каталог**.
2. Если на сервере управления зарегистрированы несколько служб каталогизации, выберите службу каталогизации, которая выполнит каталогизацию резервных копий, которые находятся в хранилище.

   Примечание
   Чтобы узнать, какая служба каталогизирует хранилище, выберите хранилище в **Хранилище резервных копий** > **Хранилища** > **Хранилища**, после чего щелкните **Сведения**.

3. В программном обеспечении отобразятся машины, резервные копии которых находятся в управляемых хранилищах, каталогизированных выбранной службой каталогизации.
   Выберите данные для восстановления через обзор или поиск.
   - **Обзор**

     Дважды щелкните машину, чтобы посмотреть резервные копии дисков, томов, папок и файлов.

Чтобы восстановить диск, выберите диск, обозначенный следующим значком: 

Чтобы восстановить том, дважды щелкните диск с этим томом и выберите том.

Чтобы восстановить файлы и папки, найдите том в месте его расположения. Через обзор можно найти тома, которые отмечены значком папки: 

- **Поиск**

  В поле поиска введите информацию, которая позволит идентифицировать требуемые данные (это может быть имя машины, файла или папки либо метка диска), после чего нажмите кнопку **Поиск**.

  Можно использовать подстановочные символы звездочки (*) и вопросительного знака (?).

  Как результат поиска отобразится список резервных копий данных, имена которых полностью или частично совпадают с введенным значением.

4. По умолчанию данные будут возвращены к состоянию на момент времени создания последней резервной копии. Если выбран один элемент, для выбора точки восстановления можно использовать кнопку **Версии**.
5. Выбрав необходимые данные, выполните один из следующих вариантов.
   - Нажмите **Восстановление**, после чего сконфигурируйте параметры операции восстановления в соответствии с описанным на странице«Recovery» (Восстановление).
   - [Только для файлов и папок] Если вы хотите сохранить файл в виде архива с расширением .zip, нажмите кнопку **Загрузить**, выберите, куда вы хотите сохранить данные, и затем нажмите кнопку **Сохранить**.

28.2.5.2 Рекомендации по каталогизации

Для увеличения производительности каталогизации следуйте рекомендациям ниже.

Установка

Мы рекомендуем устанавливать службу каталогов и узел хранения на отдельные машины. В противном случае, эти компоненты будут конкурировать с ресурсами ЦП и ОЗУ.

Если на сервере управления зарегистрированы несколько узлов хранения, одной службы каталогов будет достаточно без потери производительности индексирования и поиска. Например, если наблюдается работа каталогизации в режиме 24/7 (что означает отсутствие пауз между действиями каталогизации), установите еще одну службу каталогов на отдельную машину. Затем удалите некоторые управляемые хранилища и заново создайте их с новой службой каталогов. Резервные копии, сохраненные в этих хранилищах, будут оставаться без изменений.

Требования к системе

Параметр	Минимальное значение	Рекомендуемое значение

Количество ядер ЦП	2	4 и более
ОЗУ	8 ГБ	16 ГБ и более
Жесткий диск	Жесткий диск 7200 об/мин	SSD (твердотельный накопитель)
Сетевое подключение между машиной с узлом хранения и машиной со службой каталогов	100 Мбит/с	1 Гбит/с

28.2.5.3 Включение или отключение каталогизации

Если каталогизация включена для управляемого расположения, содержимое каждой резервной копии, перенаправляемой в хранилище, добавляется в каталог данных сразу же после ее создания.

Каталогизацию можно включить при добавлении управляемого расположения или позже. После включения каталогизации все резервные копии, которые сохранены в хранилище и не были каталогизированы ранее, будут каталогизированы после следующего процесса резервного копирования в хранилище.

Процесс каталогизации может занимать продолжительное время, особенно при выполнении резервного копирования большого количества машин в одно хранилище. Отключить каталогизацию можно в любое время. Каталогизация резервных копий, созданных до отключения, будет выполнена. Новые созданные резервные не будут каталогизироваться.

Порядок настройки каталогизации для существующего хранилища

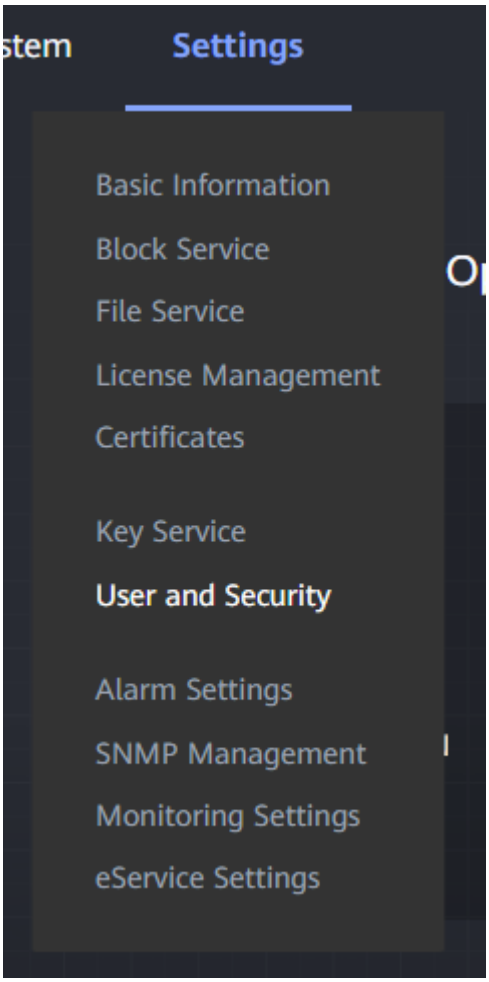
1. Щелкните **Хранилище резервных копий** > **Хранилища**.
2. Щелкните **Хранилища**, а затем выберите управляемое расположение, для которого необходимо настроить каталогизацию.
3. Щелкните **Изменить**.
4. Включите или выключите переключатель **Служба каталогизации**.
5. Нажмите кнопку **Готово**.

28.3 Настройка сервера управления для Huawei OceanStor (Dorado)

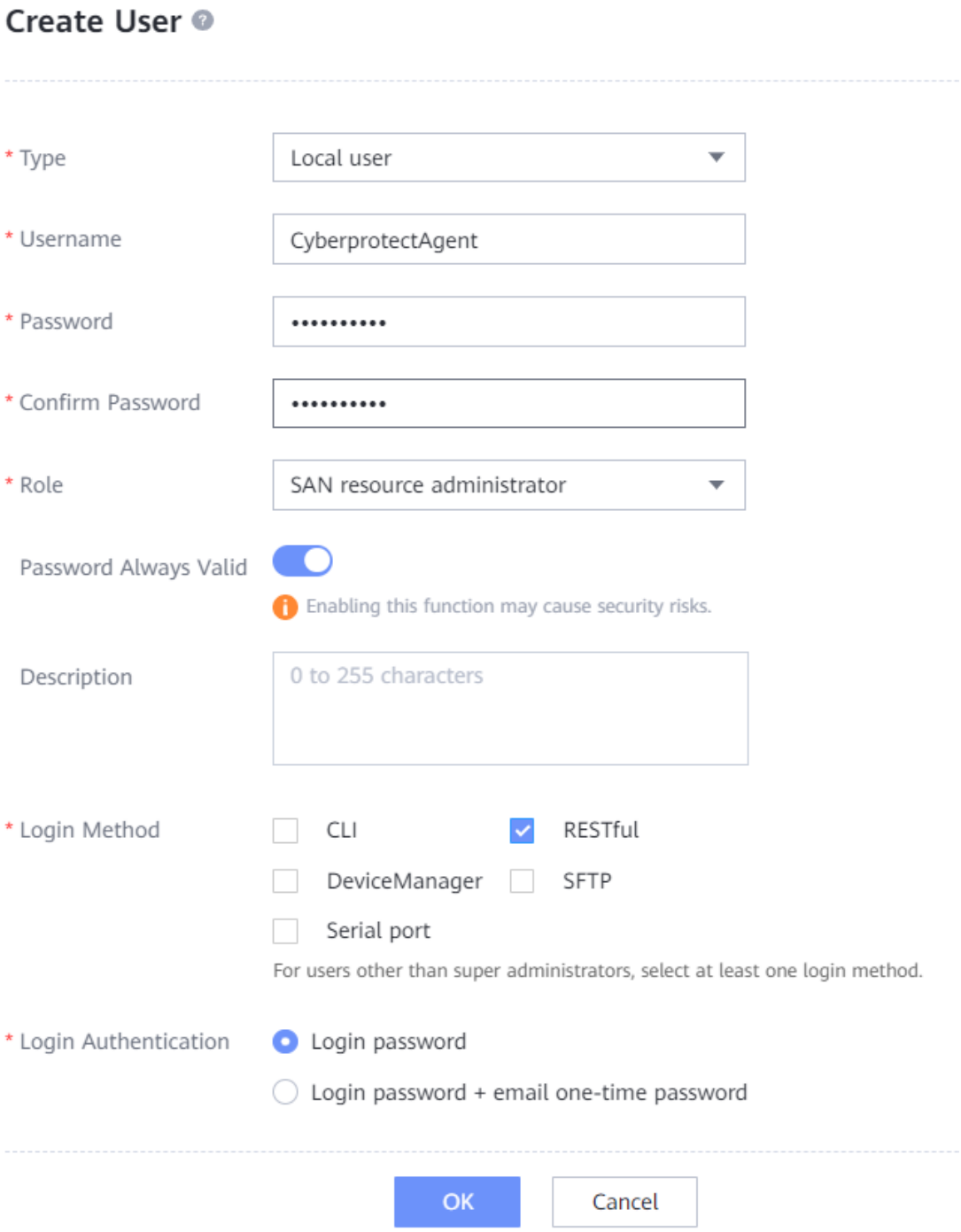
Кибер Бэкап поддерживает системы хранения семейства Huawei OceanStor (Dorado). В этом разделе описана настройка сервера управления для устройств хранения Huawei OceanStor (Dorado).

28.3.0.1 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**.
- 

- Заполните поля как показано далее:

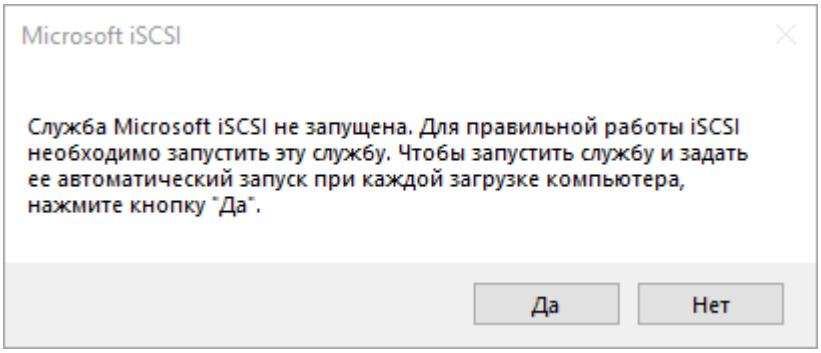


- В поле Role укажите одну из двух следующих ролей (встроенных групп):
  - Administrator
  - Super administrator
- По окончании ввода данных нажмите **OK**.

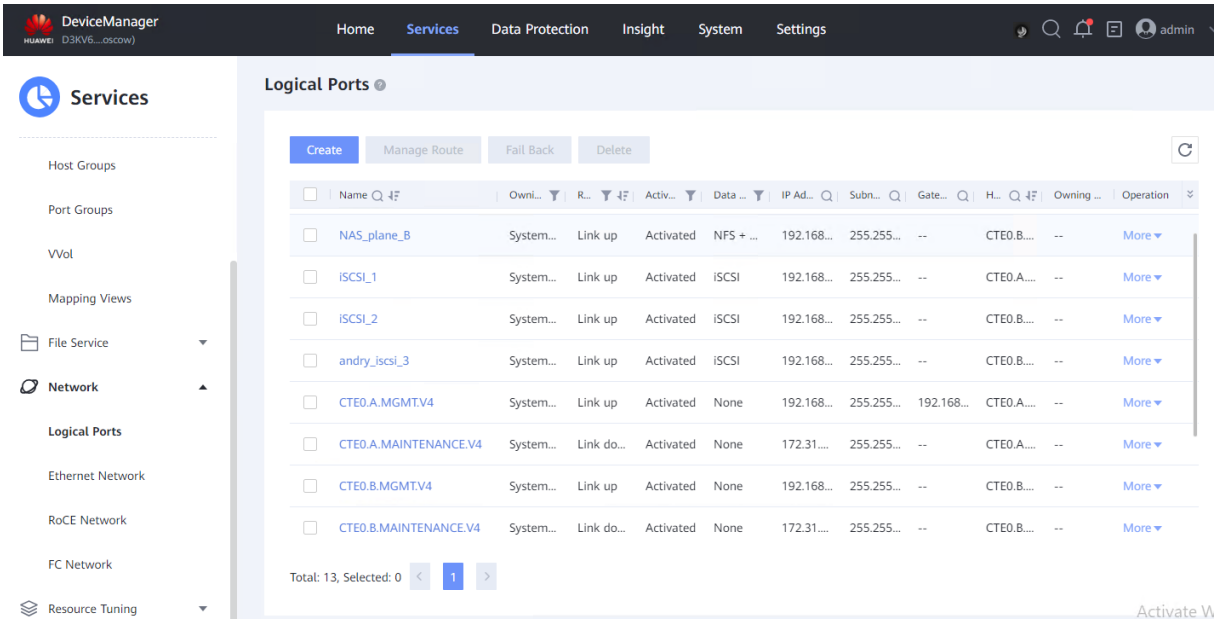
28.3.0.2 Настройка iSCSI доступа

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.



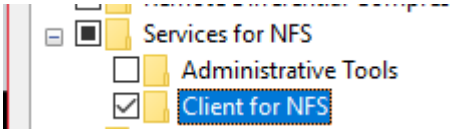
Убедитесь, что имя IQN инициатор уникально. Это актуально в случае, если машины были клонированы.

28.3.0.3 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.

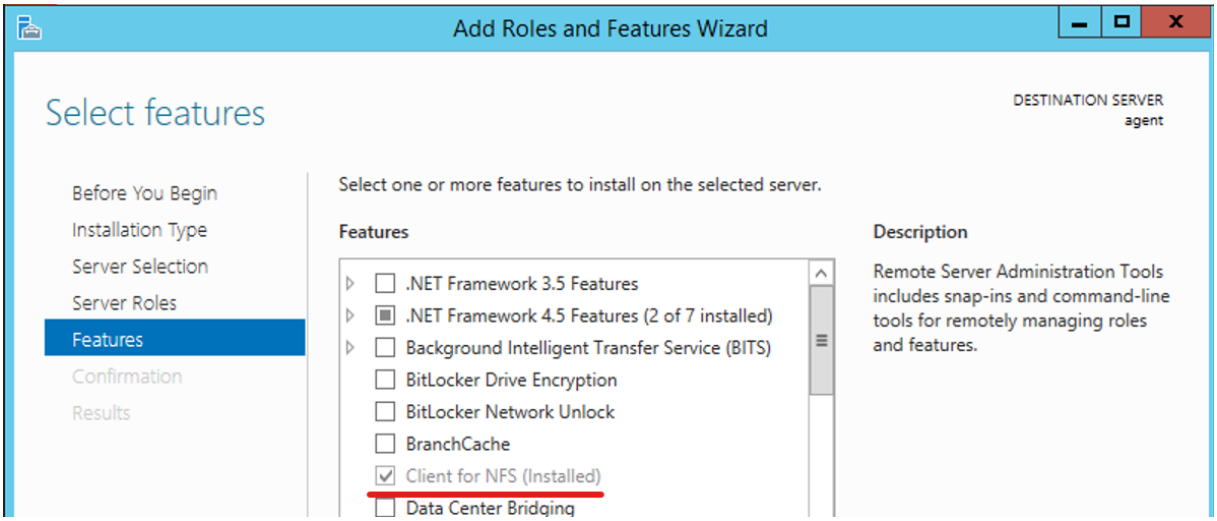
На клиентском компьютере под управлением Windows выполните следующие действия:

- Нажмите **Пуск** - > **Выполнить** (или нажмите одновременно **Win** + **R**).
- Наберите **optionalfeatures.exe** и нажмите **OK** или Enter.
- Отметьте пункт **Clients for NFS** и нажмите **OK**.



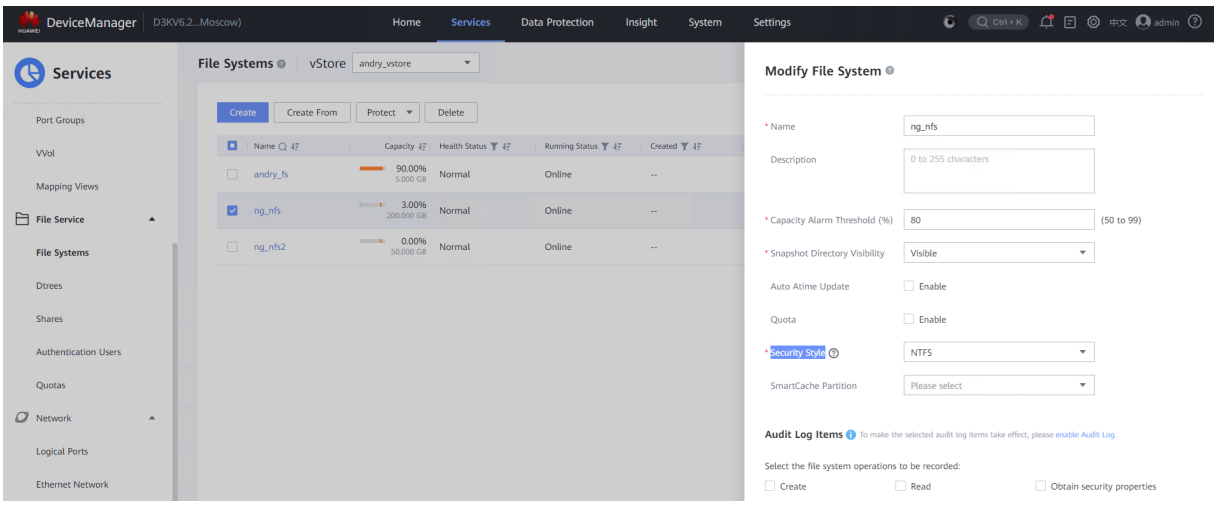
Для сервера под управлением Windows выполните следующие действия:

- Нажмите **Пуск** - > **Выполнить** (или нажмите одновременно **Win** + **R**).
- Наберите **optionalfeatures.exe** и нажмите **OK** или Enter.
- Отметьте пункт **Clients for NFS (Installed)** и нажмите **OK**.



28.3.0.4 Настройка CIFS

При создании общей папки SMB в секции **File Systems** в панели управления Dorado в поле **Security Style** выберите пункт **NTFS**.



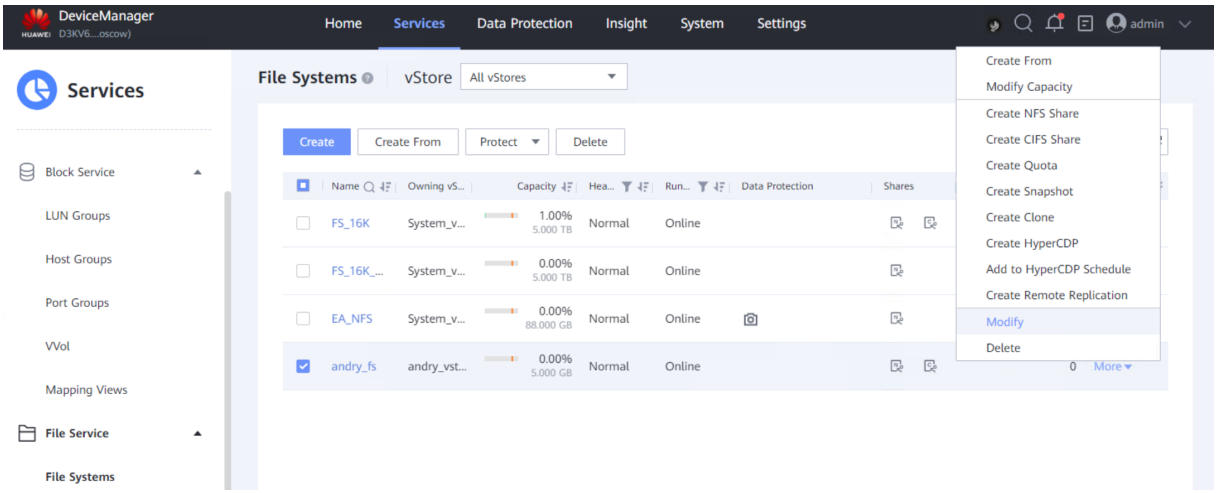
Рекомендуется в настройках общей папки прописывать доступ к машине с агентом. Убедитесь, что общая папка SMB доступна для чтения/записи штатными средствами.

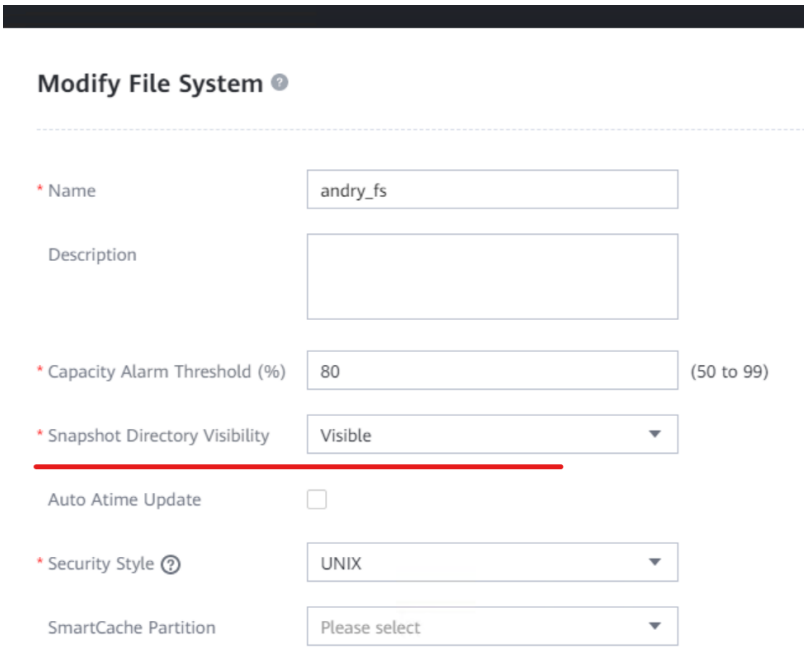
28.3.0.5 Настройка анонимного UID и анонимного GID.

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.

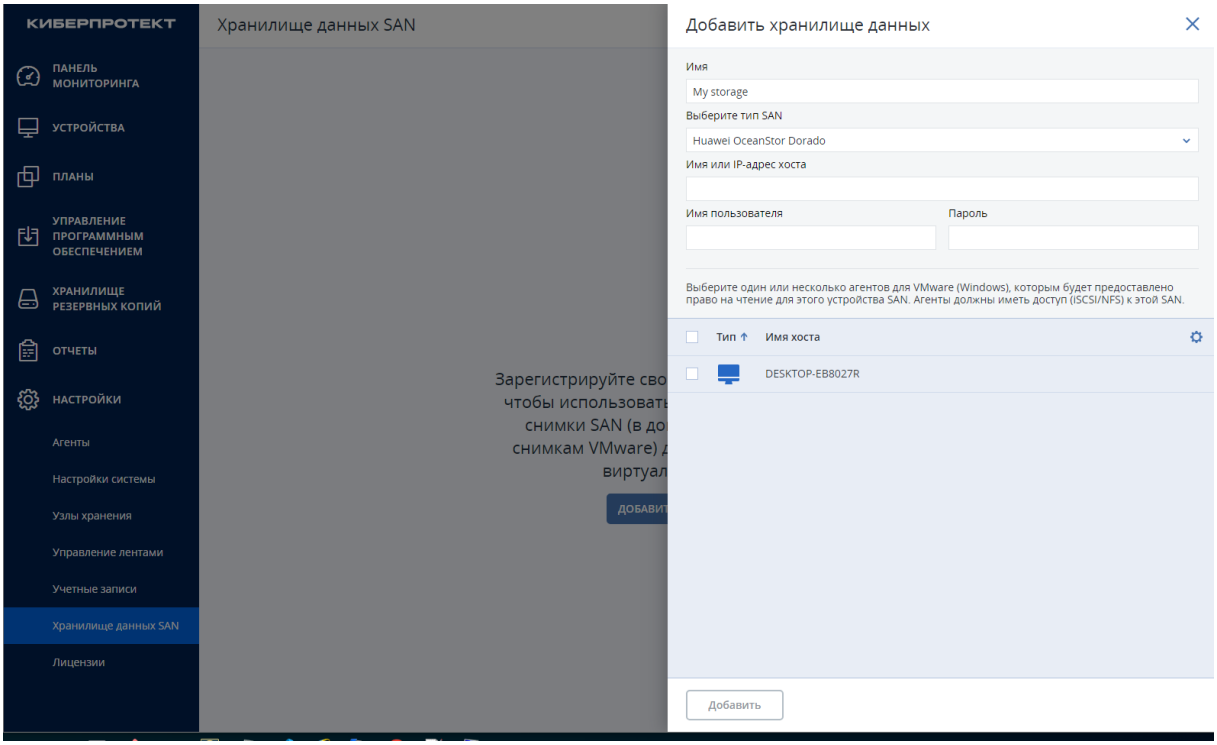
Убедитесь, что **Snapshot Directory Visibility** файловой системы включен.





28.3.0.6 Общие настройки

1. Перейдите в веб-консоль Кибер Бэкап.
2. В веб-консоли в разделе **Настройки** → **Хранилище данных SAN** нажмите **Добавить хранилище**



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.
- По окончании ввода данных нажмите **Добавить**.

28.3.0.7 Известные проблемы и ограничения*

1. Возможность резервного копирования через NFS существует лишь для компьютеров под управлением Windows 10..
2. Проверяется наличие NFS-клиента, если в хранилище находится хотя бы одна файловая система NFS.
3. Проверяется наличие iSCSI-инициатора, если в хранилище находится хотя бы одно логическое устройство (LUN).
4. Не удается выполнить резервное копирование виртуальной машины с пустым диском.
5. Не удается выполнить резервное копирование, если диск виртуальной машины находится не в аппаратном хранилище.

* См. также Известные проблемы версии 16.5.

29 Настройки системы

Эти настройки доступны только в локальных развертываниях.

Чтобы получить доступ к этим настройкам, щелкните **Настройки** > **Настройки системы**.

Раздел **Настройки системы** видим только для администраторов организации.

29.1 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:

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**.

29.2 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.

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.

29.3 Безопасность

Эти параметры позволяют повысить безопасность локального развертывания Кибер Бэкап.

29.3.1 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.**

29.3.2 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**.

29.3.3 Предупреждать об истечении срока действия локального пароля или пароля домена

Этот параметр позволяет отображать срок истечения пароля пользователя для доступа к Кибер Бэкап Management Server. Это локальный пароль или пароль домена, с которым пользователь входит на машину, на которой установлен сервер управления. Время до окончания срока действия пароля отображается в нижней части экрана и в меню учетной записи в верхнем правом углу.

Значение по умолчанию: **Отключено**.

29.4 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».

29.5 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 на 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**.

29.6 Настройка анонимной регистрации

В ходе локальной установки агента программа установки предложит зарегистрировать машину на сервере управления анонимно, т. е. подключиться без проверки подлинности. Анонимная регистрация также выполняется, если для сервера управления в параметре GUI агента для VMware (виртуальное устройство) указаны неправильные учетные данные. Анонимная регистрация позволяет администратору сервера делегировать установку агента пользователям.

Можно отключить анонимную регистрацию на сервере управления. В таком случае для регистрации устройства всегда необходимо будет указывать действительное имя и пароль администратора сервера управления. Если пользователь выберет анонимную регистрацию, произойдет сбой регистрации. Регистрация загрузочного носителя, предварительно настроенного с параметром **Не спрашивать имя пользователя и пароль**, также будет отклонена. При автоматической установке необходимо будет указать маркер регистрации в файле преобразования (.mst) или как параметр команды msiexec.

Порядок отключения анонимной регистрации на сервере управления

1. Войдите на машину с установленным сервером управления.
2. На этой машине откройте указанный ниже файл конфигурации в текстовом редакторе:
   - В ОС Windows: **%ProgramData%\Acronis\ApiGateway\api_gateway.json**
   - В ОС Linux: **/var/lib/Acronis/ApiGateway/api_gateway.json**
3. Найдите следующий раздел:

```
"auth": {
 "anonymous_role": {
  "enabled": true
 }
},
```

Если сервер управления обновлен со сборки 11010 или более ранней, этот раздел отсутствует. Скопируйте и вставьте его в начало файла сразу после открывающей скобки {.

4. Замените значение true на значение false.
5. Сохраните файл **api_gateway.json**.

Внимание
Будьте внимательны, чтобы не удалить в файле конфигурации ни одной запятой, скобки и двойной кавычки.

6. Перезапустите службу Киберпротект Service Manager Service, как описано в разделе Использование сертификата, выданного доверенным центром сертификации.

29.7 Настройка PAM-модуля

Эти параметры позволяют повысить безопасность пользователя в Кибер Бэкап.

29.7.1 Установленные библиотеки

Перед началом настройки убедитесь в том, что в системе пользователя установлены библиотеки pam_tally2.so или pam_faillock.so

29.7.2 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.

29.7.3 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 ответственности за любые последствия, возникшие в результате самостоятельного изменения пользователем конфигурационных файлов.

30 Управление учетными записями пользователей и отделами организации

30.1 Локальное развертывание

Функциональные возможности, описанные в этом разделе, доступны только для администраторов организации.

Чтобы получить доступ к этим настройкам, щелкните **Настройки** > **Учетные записи**.

30.1.1 Отделы и учетные записи администратора

Для управления отделами и учетными записями администратора на веб-консоли Кибер Бэкап последовательно выберите пункты **Настройки** > **Агенты**. На панели **Учетные записи** отображается группа **Организация** с деревом отделов (при наличии), а также список учетных записей администраторов на выбранном уровне иерархии.

30.1.1.1 Отделы

Группа **Организация** автоматически создается при установке сервера управления. При наличии лицензии Кибер Бэкап Advanced можно создать дочерние группы, называемые отделами, которые, как правило, соответствуют отделам или подразделениям организации, и добавить в них учетные записи администраторов. 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.

Каждый отдел может иметь дочерние отделы. Учетные записи администраторов родительского отдела имеют одинаковые права во всех дочерних отделах. Группа **Организация** – это родительская группа верхнего уровня. Учетные записи администратора на этом уровне имеют одинаковые права во всех ее отделах.

30.1.1.2 Учетные записи администратора

Любой пользователь, учетная запись которого позволяет войти на веб-консоль Кибер Бэкап, является администратором.

На веб-консоли Кибер Бэкап любой пользователь с учетной записью администратора может просматривать все элементы на уровне иерархии своего отдела, а также управлять ими. Например, учетная запись администратора в *организации* имеет доступ к верхнему уровню, а соответственно и доступ ко всем отделам этой организации. Напротив, учетная запись администратора в определенном *отделе* может получить доступ только к данному отделу и своим дочерним отделам.

30.1.1.3 Какие учетные записи могут иметь роль администратора?

Если на машине Windows, включенной в домен Active Directory, установлен сервер управления, любому локальному пользователю, пользователю домена или группе пользователей можно предоставить права администратора. В противном случае, права администратора можно предоставить только локальным пользователям и группам.

Информацию о добавлении учетной записи администратора на сервере управления см. в разделе Добавление учетных записей администратора.

30.1.1.4 Роли учетной записи администратора

Каждой учетной записи администратора назначается роль с предварительно определенными правами, которые необходимы для выполнения определенных заданий. Роли учетной записи администратора 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 и содержимого резервных копий почтовых ящиков.
- **Аудитор**:
  роль предоставляет доступ только для чтения по отношению к вкладке **Действия** на веб-консоли Кибер Бэкап. Дополнительную информацию об этой вкладке см. в разделе Вкладка «Действия». Эта роль не позволяет собирать или экспортировать никаких данных, включая системную информацию сервера управления.

Все изменения, внесенные в роли, отображаются на вкладке **Действия**.

30.1.1.5 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 ролей. Например, учетная запись пользователя с назначенной ролью «Только для чтения» и наследованной ролью «Администратор» будет иметь права администратора.

Внимание
На 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.

30.1.1.6 Администраторы по умолчанию

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.

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 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 Active Directory и назначать им роли (подробнее о добавлении пользователей см. "Добавление учетных записей администратора" (стр. 563)).

Для обнаружения домена Active Directory используется команда dnsdomainname. Она определяет имя домена в автоматическом режиме. Если домен все же определен неверно, то для того, чтобы исправить его обнаружение, создайте вручную конфигурационный файл cyber_domain.conf по пути /etc/security/ и укажите в нем имя домена. Домен в файле может быть указан только один; он должен быть указан без дополнительных символов (например, пробелов) и строго в первой строчке файла. Если этот файл создан, то значение, указанное в нем, становится приоритетным при определении домена. Если файл был создан, но домен в нем не указан, это равнозначно тому, что такой домен не существует. В этом случае вы сможете добавить лишь локальных пользователей.

30.1.1.7 Учетная запись администратора в нескольких отделах

Для учетной записи можно предоставить права администратора в любом количестве отделов. Для такой учетной записи, а также для учетных записей администраторов на уровне организации на 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. Учетные записи администраторов на уровне организации необходимо явно добавить в группу **Организация**.

30.1.1.8 Как заполнить отделы данными о машинах?

Когда администратор добавляет машину с помощью веб-интерфейса, она добавляется в отдел, управляемый администратором. Если администратор управляет несколькими отделами, машина добавляется 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.

30.1.2 Добавление учетных записей администратора

Примечание
Эта функция недоступна в выпусках Standard и Essentials.

Порядок добавления учетных записей

1. Щелкните **Настройки** > **Учетные записи**.
   Программное обеспечение отобразит список администраторов сервера управления и дерево отделов (при его наличии).
2. Выберите **Организация** или выберите отдел, в котором необходимо добавить администратора.

3. Нажмите кнопку **Добавить учетную запись**.
4. В окне **Домен** выберите домен, содержащий учетные записи, которые необходимо добавить. Если сервер управления не входит в домен Active Directory, могут быть добавлены только локальные пользователи. В Linux вы также можете добавить пользователей домена Active Directory.

   Если для доступа к домену Active Directory потребуется указать данные учетной записи, введите имя учетной записи администратора домена и пароль. Имя учетной записи указывайте в формате DOMAINNAME0\Administrator или Administrator@domain.name, где DOMAINNAME0 – NetBIOS-имя домена, domain.name – DNS-имя домена, Administrator – имя учетной записи администратора домена Active Directory.
5. Выполните поиск имени пользователя или имени группы пользователей.
6. Нажмите «+» рядом с именем пользователя или группы.
7. Выберите роль для учетной записи.
8. Повторите шаги 4-6 для всех пользователей или групп, которые необходимо добавить.
9. По окончании нажмите **Готово**.
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.
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.

30.1.3 Создание отделов

1. Щелкните **Настройки** > **Учетные записи**.
2. Программное обеспечение отобразит 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**.

31 Устранение неисправностей

В этом разделе объясняется, как сохранить журнал агента в ZIP-файл. Этот файл поможет сотрудникам технической поддержки определить проблему в случае неудачного резервного копирования по неясной причине.

Получение журналов

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 **Подробнее**.
2. Нажмите кнопку **Сбор сведений о системе**.
3. При появлении соответствующего запроса в веб-браузере укажите место сохранения файла.

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

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.

Указатель

#

32- или 64-разрядная версия 292

A

Active Protection (Активная защита) 486

D

DefaultBlockSize 519

F

Flashback 271

L

Linux 97, 179

M

McAfee Endpoint Encryption и PGP Whole Disk Encryption 40

Microsoft Exchange Server 222

Microsoft SQL Server 221, 223

N

NFS 173

P

PE-образы 308

PE-образы на основе WinRE 308

PXE-сервер Киберпротект 335

R

RAID-5 327

S

Storage vMotion 470

U

Universal Restore в Linux 262

Universal Restore в Windows 260

V

vMotion 470

W

Windows 97, 178

WriteCacheSize 519

A

Автоматическая установка oVirt 114

Автоматическая установка или автоматическое удаление 84

Автоматическая установка или автоматическое удаление в Linux 91

Автоматическая установка или автоматическое удаление в Windows 84

Автоматический поиск драйверов 260

Автоматическое и ручное обнаружение 103

Автоматическое обнаружение машин 100

Агент OpenStack (виртуальное устройство) 27

Агент для ECP Veil 27

Агент для Exchange (для резервного копирования почтового ящика) 23

Агент для Hyper-V 25

Агент для Linux 24

Агент для Office 365 24

Агент для Oracle 24

Агент для oVirt (виртуальное устройство) 26

Агент для PostgreSQL 25

Агент для SpaceVM 27

Агент для SQL, агент для Exchange (для резервного копирования базы данных и резервного копирования с поддержкой приложений), агент для Active Directory 23

Агент для VMware

необходимые привилегии 472

Агент для VMware (Windows) 25

Агент для VMware (виртуальное устройство) 25

Агент для Windows 23

Агент для Базис.Dynamix (виртуальное устройство) 27

Агент развертывания 70

Агенты 18, 23

Администраторы по умолчанию 562

Активация Восстановление при загрузке 334

Активный том 330

Алгоритм распределения 467

Б

База данных управления лентами 517

Безопасность 557

Безопасность на уровне файлов 271

Быстрое инкрементное/дифференциальное резервное копирование 226

В

В AAG включено резервное копирование баз данных 345

В Windows 27, 55, 141-142, 146, 562

В интервале времени 195

В локальных развертываниях 110

В ОС Linux 28, 57, 141, 144, 147, 562

В случае ошибки повторить попытку 224, 270

Важная информация о преобразовании 204

Вернуть ленту в слот после каждого успешного создания резервной копии каждой машины 242

Взаимодействие с диспетчером съемных носителей Windows (RSM) 517

Виртуальная машина 256

Виртуальные машины Windows Azure и Amazon EC2 482

Вкладка «Действия» 510

Вкладка «Планы» 282

Вкладка «Хранилище резервных копий» 277

Включение или исключение файлов, соответствующих определенным критериям 226

Включение или отключение каталогизации 547

Включите целевую виртуальную машину по окончании восстановления. 275

Включить восстановление файлов из образов дисков на лентах 242

Включить полное резервное копирование VSS 249

Включить после восстановления 276

Возврат из реплики 455

Возврат к исходному начальному RAM-диску 262

Восстановить в Office 365 359

Восстановление 251, 319, 367

памятка 251

Восстановление CommuniGate Pro 394

Восстановление Kubernetes 445

Восстановление VK WorkMail 412

Восстановление баз данных 425

Восстановление баз данных Exchange 355

Восстановление баз данных SQL 351

Восстановление баз данных, включенных в AAG 345

Восстановление базы данных master 354

Восстановление всего сервера 425

Восстановление данных из резервной копии 435

Восстановление данных из резервной копии с поддержкой приложений 424

Восстановление данных кластера Exchange 347

Восстановление данных пользователей VK WorkMail 412

Восстановление дисков с помощью загрузочного носителя 258

Восстановление конфигурации ESXi 265

Восстановление машины 252

Восстановление на Exchange Server 359

Восстановление полного пути 271

Восстановление почтовых ящиков 360, 369

Восстановление почтовых ящиков Exchange и элементов почтового ящика 358

Восстановление почтовых ящиков и элементов почтовых ящиков 369

Восстановление при загрузке 333

Восстановление приложений 339

Восстановление с загрузочного носителя из локально прикрепленного ленточного устройства 525

Восстановление с ленточного устройства из операционной системы 524

Восстановление с помощью загрузочного носителя с ленточного устройства, прикрепленного к узлу хранения 527

Восстановление сервера VK WorkMail 418

Восстановление системных баз данных 354

Восстановление таблиц 427

Восстановление файлов 262

Восстановление файлов с помощью веб-интерфейса 262

Восстановление файлов с помощью загрузочного носителя 264

Восстановление физической машины в виртуальную 254

Восстановление экземпляров 425

Восстановление элементов почтовых ящиков 362, 370

Всегда инкрементное 174

Встроенные группы 496

Выбор баз данных SQL 342

Выбор всей машины 174

Выбор данных Exchange Server 343

Выбор данных для резервного копирования 174

Выбор данных резервной копии для восстановления 545

Выбор дисков и томов 176

Выбор компонентов для установки 106

Выбор конфигурации ESXi 179

Выбор места назначения 180

Выбор напрямую на машине 174, 176

Выбор операционной системы для управления дисками 321

Выбор почтовых ящиков 368

Выбор почтовых ящиков сервера Exchange 351

Выбор файлов и папок 174

Выключать целевые виртуальные машины при запуске восстановления 275

Выполнение окончательного перехода на реплику 455

Выполните резервное копирование типичной машины перед резервным копированием нескольких машин со сходным содержимым. 544

Выполняйте резервное копирование разных машин в разное время. 544

Выпуски и лицензирование Кибер Бэкап 17

Высокая доступность восстановленной машины 477

Высокоскоростная локальная сеть 544

Г

Где можно просмотреть имена файлов резервных копий? 215

Группы устройств 496

Д

Дамп данных отчета 514

Дата и время для файлов 269

Деактивация Восстановление при загрузке 334

Дедупликация 541

Дедупликация в архиве 220

Дедупликация данных 55

Действия при сбое задания 247

Действия, которые можно выполнить с репликой 452

Деление 241

Добавление vCenter или хоста ESXi 73

Добавление VLAN 314

Добавление консоли к списку веб-узлов локальной интрасети 148

Добавление консоли к списку доверенных веб-узлов 150

Добавление машин через веб-интерфейс 67

Добавление машины 71

Добавление машины с ОС Linux 73

Добавление машины с ОС Windows 68

Добавление подключаемого модуля Киберпротект к WinPE 310

Добавление управляемого хранилища 539

Добавление устройств в статические группы 497

Добавление учетных записей администратора 563

Добавление хостов OpenStack (РУСТЭК) 76

Добавление хранилища резервных копий 186

Документация 187

Дополнительная настройка 46, 49, 52

Дополнительная настройка машин для сервера управления и СУБД PostgreSQL 49

Дополнительная настройка машины для сервера управления 52

Дополнительная настройка машины с ОС Linux 46

Дополнительная настройка машины с ОС Windows 46

Дополнительная настройка продукта Кибер Бэкап 47, 50

Дополнительная настройка СУБД PostgreSQL 50

Дополнительные параметры расписания 189

Дополнительные требования для виртуальных машин 349

Дополнительные требования для операций резервного копирования с поддержкой приложений 341

Достаточное свободное пространство в хранилище 543

Доступ к веб-консоли Кибер Бэкап 146

Доступность параметров восстановления 266

Доступность параметров резервного копирования 210

Доступные действия с планами защиты 159

Драйверы для Universal Restore 307

Драйверы запоминающих устройств для обязательной установки 261

Другие компоненты 21

Е

Еженедельное резервное копирование 250

Если не отображаются резервные копии, хранящиеся на лентах 525

Если нужно создать виртуальную машину на сервере виртуализации 207

Если нужно сохранить виртуальную машину как набор файлов 206

Ж

Журнал событий Windows 250, 275

З

За указанное количество дней подряд не создано успешно ни одной резервной копии. 213

Завершить сеансы работы неактивных пользователей через 557

Загрузочные носители на основе Linux 292

Загрузочный носитель 290

Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE? 291

Загрузочный носитель на основе WinPE 308

Запуск виртуальной машины из резервной копии (мгновенное восстановление) 448

Запуск машины 449

Запуск резервного копирования вручную 209

Зачем создавать резервную копию почтовых ящиков Office 365? 367

Защита CommuniGate Pro 374

Защита Kubernetes 436

Защита Microsoft SharePoint 338

Защита Microsoft SQL Server и Microsoft Exchange Server 338

Защита Oracle Database 420

Защита SAP HANA 484

Защита VK WorkMail 399

Защита баз данных MongoDB 430

Защита баз данных PostgreSQL 421

Защита баз данных Ред БД 429

Защита групп обеспечения доступности базы данных (DAG) 346

Защита группы Always On Availability Groups (AAG) 344

Защита данных MySQL и MariaDB 422

Защита контроллера домена 339

Защита паролем 201

Защита паролем как свойство машины 201

Защита почтовых ящиков Office 365 367

Защита приложений Microsoft 338

Защита хранилища паролем 544

Заявление об авторских правах 2

Зеркальный том 327

Зеркальный чередующийся том 327

Зона безопасности 173

И

Извлечение 536

Извлечение файлов из локальных резервных копий 264

Извлечь ленты после каждого успешного резервного копирования каждой машины 243

Изменение буквы тома 330

Изменение идентификатора безопасности 274

Изменение метки тома 331

Изменение пула 529

Изменение учетных данных для доступа к Office 365 371

Изменение учетных данных для доступа к SQL Server или Exchange Server 365

Изменение формата резервной копии на "Версия 12" (TIBX) 219

Имена без переменных 216

Именение параметров прокси-сервера в Linux 57

Имя файла резервной копии 214

Имя файла резервной копии по умолчанию 215

Инвентаризация 531

Инициализация диска 321

Исключения файлов 270

Исключить системные файлы и папки 228

Исключить скрытые файлы и папки 228

Использование Universal Restore 259

Использование кэша диска для ускорения восстановления 274

Использование локально присоединенного хранилища 466

Использование моментальных снимков оборудования SAN 461

Использование переменных 217

Использование правил политики 175-176

Использование самозаверяющих сертификатов 153

Использование сертификата, выданный доверенным центром сертификации 154

Использовать наборы лент в пуле лент, выбранных для резервного копирования 245

Используемая конфигурация 559

Используйте следующие ленточные устройства и приводы. 243

К

Как заполнить отделы данными о машинах? 563

Как работает обычное преобразование в виртуальную машину 206

Какая машина выполняет операцию? 209

Какие учетные записи могут иметь роль администратора? 561

Каталог данных 545

Каталогизация 545

Кибер Бэкап 508

Кибер Инфраструктура 173

Клонирование базового диска 322

Команда до захвата данных 237

Команда до резервного копирования 235

Команда после восстановления 274

Команда после захвата данных 238

Команда после резервного копирования 236

Команда, выполняемая перед восстановлением 273

Команды до и после захвата данных 237

Команды до и после процедуры 235, 272, 456-457

Компоненты 18

Компоненты для удаленной установки 69

Консолидация резервных копий 213

Копирование библиотек Microsoft Exchange Server 365

Л

Ленточные устройства 516

Локальная установка агентов 79

Локальное подключение 315

Локальное развертывание 18, 58, 146, 483, 560

Локальные развертывания 136

М

Мастер создания загрузочных носителей 292

Машина для PostgreSQL 48

Машина для сервера управления 47, 51

Методы инвентаризации 531

Методы преобразования 203

Миграция Linux-машины с логическими томами (LVM) 482

Миграция машины 479

Многотомные моментальные снимки 231

Многоядерный процессор с тактовой частотой не менее 2,5 ГГц 543

Модернизация с предыдущих версий продукта 138

Модуль резервного копирования

памятка 170

Моментальные снимки оборудования SAN 239

Моментальные снимки резервных копий на уровне файлов 228

Мониторинг и отчеты 507

Мультиплексирование 244

Н

На основе Linux 291

На основе WinPE 291

Назначение прав пользователя 62

Наследование ролей 561

Настройка Microsoft Edge, Opera и Google Chrome 147

Настройка Mozilla Firefox 148

Настройка NFS-клиента 465

Настройка PAM-модуля 559

Настройка агента в ROSA Virtualization 116

Настройка анонимной регистрации 558

Настройка важности оповещений 514

Настройка веб-браузера для выполнения встроенной проверки подлинности Windows 147

Настройка виртуального устройства 111

Настройка защиты паролем в планах защиты 201

Настройка инициатора iSCSI 464

Настройка машины на загрузку с PXE 336

Настройка машины, на которой работает агент для VMware 464

Настройка модуля Active Protection 487

Настройка модуля Оценка уязвимостей 493

Настройка параметров установки 59

Настройка плана защиты для CommuniGate Pro 389

Настройка режима отображения 317

Настройка резервного копирования баз данных MongoDB 430

Настройка резервного копирования с поддержкой приложений 423

Настройка сервера управления для Huawei OceanStor (Dorado) 547

Настройка сети 314

Настройка уже зарегистрированного агента для VMware 76

Настройка устройств iSCSI 332

Настройки Universal Restore 260

Настройки прокси-сервера 55

Настройки сертификата SSL 153

Настройки системы 555

Начало работы с ленточным устройством 522

Не запускать при подключении к следующим сетям Wi-Fi 198

Не запускать при работе на лимитном подключении 197

Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений) 225, 270

Нет недавних резервных копий 509

О

О программе Зона безопасности 182

О программе Кибер Инфраструктура 186

Обзор кластеров Exchange Server 346

Обзор решений для SQL Server высокой доступности 344

Обзор установки 18

Обнаружение ленточных устройств 527

Обнаруженные машины 508

Обновление агента для VMware (виртуальное устройство) 113

Обновление агентов 137

Обновление виртуальных устройств 136

Обновление токена VK WorkMail 418

Обновления 557

Обработка данных Off-host 283

Обработка ошибок 224, 270, 456-457

Общее правило резервного копирования 40

Общие ограничения 541

Общие параметры 59

Общие требования 340

Объект высшего уровня 301

Объект переменной 301

Ограничение общего количества виртуальных машин, для которых одновременно выполняется резервное копирование 478

Ограничения 33, 172, 179, 183, 204, 209, 269, 368, 453, 460, 521, 545

Ограничения дедупликации 541

Ограничения для имени файла резервной копии 215

Ограничения для Кибер Инфраструктура 187

Одно дедуплицирующее хранилище на каждый узел хранения 543

Ожидать выполнения условий расписания 248

Ожидающие операции 331

Окно резервного копирования 232

Операторы 505

Операции с дисками 321

Операции с загрузочным носителем 316

Операции с лентами 530

Операции с планами защиты 159

Операции с пулами 529

Операции с резервными копиями 277

Операции с томами 326

Оповещения 213

Основные меры предосторожности 320

Основные операции с отчетами 513

Особенности защиты паролем 203

Особенности резервного копирования VK WorkMail на ленты 411

Остановка перехода к реплике 455

От 40 до 160 МБ ОЗУ на 1 ТБ уникальных данных 543

Отделы 560

Отделы и учетные записи администратора 560

Отказоустойчивый кластер Кибер Бэкап 485

Отключение автоматического назначения для агента 469

Отключить автоматический DRS для агента 110

Отсутствие приложений, конкурирующих за ресурсы 543

Отчеты 511

Оценка уязвимостей 491

Очистка 287

П

Пакеты Linux 35

Панель мониторинга "Обзор" 507

Параллельные операции 520

Параметры 296

Параметры автоматической установки или автоматического удаления 85

Параметры возврата из реплики 457

Параметры восстановления 266

Параметры записи на ленты 518

Параметры информации 94

Параметры резервного копирования 210

Параметры резервного копирования по умолчанию 558

Параметры репликации 456

Параметры удаления 90, 94

Параметры установки 85, 91

Параметры установки агента 89, 93

Параметры установки сервера управления 89, 92

Параметры установки узла хранения 90

Параметры ядра 296

Пароли со специальными символами или пробелами 98

Перед началом 109

Перед резервным копированием 522-523

Перезаписать ленту в автономном ленточном устройстве при создании полной резервной копии 243

Переименование 535

Перемещение в другой пул 530

Перемещение в другой слот 530

Перераспределение 467

Переход к реплике 454

План защиты и модули 157

План конфликтует с уже примененными планами. 158

План устройства конфликтует с планом группы 158

Планирование 240

Планирование количества агентов для ECP VeiL 124

Планирование количества агентов для SpaceVM 122

Планирование по событиям 189

По общему размеру резервных копий 174

По событию в журнале событий Windows 191

Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины 225

Повторное сканирование 534

Подготовка 63, 68, 74, 81, 260

Подготовка WinPE 2.x и 3.x 309

Подготовка WinPE 4.0 и более поздние версии 310

Подготовка к установке в ОС Astra Linux SE 63, 82

Подготовка СУБД PostgreSQL 64

Подготовка хостов РУСТЭК к установке агента 126

Подготовьте драйверы 260

Поддерживаемое оборудование 517

Поддерживаемые веб-браузеры 22

Поддерживаемые версии Microsoft Exchange Server 29

Поддерживаемые версии Microsoft SharePoint 29

Поддерживаемые конфигурации кластеров 344, 346

Поддерживаемые операционные системы и среды 23

Поддерживаемые платформы виртуализации 30

Поддерживаемые продукты Microsoft 491

Поддерживаемые продукты Microsoft и сторонние продукты 491

Поддерживаемые продукты для Windows от сторонних разработчиков 493

Поддерживаемые расположения 180, 208, 283, 285, 287

Поддерживаемые системы управления базами данных 40

Поддерживаемые типы виртуальных машин 204

Поддержка миграции VM 469

Поддержка резервного копирования на ленту 516

Поддержка файловых систем 53, 320

Подключение баз данных Exchange Server 358

Подключение баз данных SQL Server 355

Подключение виртуального устройства к серверу управления 121

Подключение к машине, загружаемой с носителя 314

Подключение томов из резервной копии 278

Показать уведомление о последнем входе текущего пользователя 557

Полезная информация о финализации 451

Получение идентификатора и секрета приложения 371

Пользователи завершили сеанс 195

Пользователь неактивен 194

Пользовательские группы 496

Пользовательские пулы 529

Пользовательские сценарии 300

Порядок обновления агента для VMware (виртуального устройства) с веб-консоли Кибер Бэкап 113

Порядок обновления агента для VMware (виртуальное устройство) версий, более ранних, чем 12.5.23094 113

Порядок создания Зона безопасности 184

Порядок удаления Зона безопасности 185

Посекторное резервное копирование 241

Последовательность действий 533

Почему нужно использовать раздел Зона безопасности? 182

Почему нужно использовать резервное копирование с поддержкой приложений? 348

Почтовый сервер 556

Права, требуемые для учетной записи входа 61

Правила выбора для Linux 176

Правила выбора для Windows 175

Правила для Windows и Linux 177

Правила только для Linux 177

Правила только для Windows 177

Правила хранения 199

Предварительная настройка нескольких сетевых подключений 306

Предварительно заданные пулы 528

Предварительные требования 101, 134, 137, 179, 340, 448, 522-523

Предварительные требования для защиты CommuniGate Pro 375

Предопределенный сценарий 298

Представление веб-консоли Кибер Бэкап 156

Предупреждать об истечении срока действия локального пароля или пароля домена 557

Предупреждение о редактировании конфигурационного файла 559

Преобразование в виртуальную машину 203, 288

Преобразование в виртуальную машину в плане защиты 205

Преобразование динамического диска MBR в GPT 324

Преобразование диска

- GPT в MBR 324
- MBR в GPT 323

Преобразование диска в результате создания раздела Зона безопасности 183

Преобразование диска из базового в динамический 325

Преобразование диска из динамического в базовый 325

Привязка виртуальной машины 467

Привязка вручную 468

Применение нескольких планов к устройству 158

Применение плана защиты к группе 506

Пример 194-199

Пример установки пакетов вручную 38

Пример. Аварийное резервное копирование при обнаружении «плохого блока» 192

Примеры 95, 97

Примеры использования 208, 217, 448, 452, 469

Принципы работы 101, 285

Приоритет ЦП 233

Проблемы с лицензией 159

Проверить IP-адрес устройства 199

Проверка 285

Проверка наличия обновлений программного обеспечения 98

Проверка резервных копий 220, 268

Проверьте наличие доступа к драйверам в загрузочной среде 260

Производительность 272, 457

Производительность и окно резервного копирования 231

Пропуск поврежденных секторов 225

Пропустить задание 248

Просмотр обнаруженных уязвимостей 494

Просмотр писем VK WorkMail 415

Просмотр результата распределения 468

Просмотр статуса резервного копирования в клиенте vSphere 471

Простой том 326

Процедура развертывания 122, 124

Процедуры восстановления для конкретных программ 40

Процесс Universal Restore 261

Процесс обнаружения машины 102

Пулы лент 528

Р

Работа в VMware vSphere 451

Работа в подсетях 336

Развертывание 186

Развертывание агента для ECP VeiL 124

Развертывание агента для OpenStack (РУСТЭК) 126

Развертывание агента для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация) 113

Развертывание агента для SpaceVM 121

Развертывание агента для VMware (виртуальное устройство) из шаблона OVF 109

Развертывание агента для VMware (виртуальное устройство) через веб-интерфейс 73

Развертывание агентов с использованием групповой политики 134

Развертывание резервного копирования для Базис.DynamiX 131

Развертывание резервного копирования для Кибер Инфраструктуры 118

Развертывание шаблона OVF 110

Размещайте базу данных дедупликации и дедуплицирующее хранилище на разных физических носителях. 542

Разрешение конфликтов плана 158

Расписание 187

Расположение сервера управления 18

Расположение шаблона OVF 110

Распределение ресурсов диска 456

Расширенный выбор вариантов хранения 181, 516

Регистрация 186

Регистрация машин вручную 95

Регистрация носителя в пользовательском интерфейсе носителя 315

Регистрация носителя на сервере управления 315

Регистрация установленного агента для VMware 75

Регистрация хранилища данных SAN на сервере управления. 465

Регулярное преобразование в ESXi и Hyper-V по сравнению с запуском виртуальной машины с резервной копии 205

Режим загрузки 268

Резервная копия почтового ящика 350

Резервное копирование 168, 317, 523-524

Резервное копирование CommuniGate Pro 384

Резервное копирование VK WorkMail 405

Резервное копирование базы данных 342

Резервное копирование без использования локальной сети 458

Резервное копирование данных CommuniGate Pro 390

Резервное копирование данных Kubernetes 440

Резервное копирование данных в сетевую папку и восстановление данных из сетевой папки 299

Резервное копирование данных на загрузочный носитель и восстановление данных с загрузочного носителя 299

Резервное копирование данных пользователей VK WorkMail 405

Резервное копирование кластеризованных машин Hyper-V 477

Резервное копирование машины на локально подключенное ленточное устройство 522

Резервное копирование на ленточное устройство, подключенное к узлу хранения 523

Резервное копирование на уровне дисков 541

Резервное копирование на уровне файлов 542

Резервное копирование с поддержкой кластеров 346

Резервное копирование с поддержкой приложений 348

Резервное копирование сервера VK WorkMail 409

Резервные копии CommuniGate Pro 392

Результаты 523-524

Рекомендации 269

Рекомендации для пользователей с лицензией Advanced 209

Рекомендации по дедупликации 542

Рекомендации по каталогизации 546

Рекомендуемая конфигурация продукта Кибер Бэкап 45, 48, 51

Рекомендуемые конфигурации оборудования для сервера управления 44

Репликация 207

Репликация виртуальных машин 451

Репликация и резервное копирование 452

Репликация резервной копии 283

Репликация резервных копий между управляемыми хранилищами 209

Роли учетной записи администратора 561

С

С несколькими потоками 244

Свойства событий 191

Связанные с лентой параметры резервного копирования 520

Сервер SFTP и ленточное устройство 173

Сервер управления 304

Сервер управления (только в локальных развертываниях) 27

Сервер управления на машине с ОС Linux или Windows, использующий СУБД SQLite 45

Сервер управления на машине с ОС Linux, использующий СУБД PostgreSQL 47

Сервер управления на машине с ОС Windows, использующий СУБД Microsoft SQL Server 51

Сетевой порт 307

Сетевые настройки 306

Системные требования для агента 109

Сколько агентов необходимо? 110

Сколько требуется агентов для резервного копирования и восстановления данных кластера? 345, 347

Скорость вывода при резервном копировании 234

Служба теневого копирования томов (VSS) 248

Служба теневого копирования томов (VSS) для виртуальных машин 249, 456

Смена языка 147

Смысл использования моментальных снимков оборудования SAN 461

Советы по дальнейшему использованию библиотеки ленточных носителей 524

Совместимость с RSM и программным обеспечением других поставщиков 517

Совместимость с ОС Astra Linux SE 41

Совместимость с программами шифрования 39

Создавать ли загрузочный носитель или скачать готовый? 290

Создание MST-преобразования и извлечение пакетов установки 84

Создание динамической группы 498

Создание загрузочных носителей 251

Создание и регистрация пользователя 118

Создание моментальных снимков LVM 229

Создание отделов 564

Создание плана защиты 157

Создание плана защиты для CommuniGate Pro 385

Создание плана репликации 453

Создание пула 529

Создание резервной копии данных кластера Exchange 347

Создание статической группы 497

Создание тома 328

Сокращение журнала 229

Составной том 326

Сосуществование с программным обеспечением других поставщиков 517

Сохранение первоначальной реплики 457

Сохранить сведения о системе при сбое восстановления с перезагрузкой 270

Специальные операции с виртуальными машинами 448

Способ использования Зона безопасности 40

Способ резервного копирования кластера 221

Сравнение имени файла резервной копии и упрощенного именования файлов 217

Сравнение финализации и обычного восстановления 451

Стандартные параметры 85, 91

Статус защиты 508

Стирание 536

Структура autostart.json 301

Схема резервного копирования 187

Сценарии использования 278

Сценарии на загрузочных носителях 298

Сэкономить заряд батареи 196

Т

Тестирование реплики 454

Тип элемента управления 302

Типичные правила установки 39

Типы динамических томов 326

Точки подключения 230, 272

Требования 265, 278

Требования для виртуальных машин ESXi 341

Требования для виртуальных машин Hyper-V 341

Требования к контролю учетных записей пользователей (UAC) 72

Требования к оборудованию 45, 47, 51

Требования к программному обеспечению 22

Требования к сети 483

Требования к системе 43, 546

Требования к учетным записям пользователей 359

Требуемые права пользователя 349, 351

Требуется хранилище данных NetApp SAN 463

У

Уведомления по электронной почте 223, 555

Удаление 537

Удаление CommuniGate Pro 398

Удаление агента для VMware (виртуальное устройство) 142

Удаление машин из веб-консоли Кибер Бэкап 142

Удаление машины 450

Удаление продукта 141

Удаление пула 530

Удаление резервных копий 281

Удаление тома 329

Удаленное подключение 315

Узел хранения (только в локальных развертываниях) 28

Узлы хранения 538

Указание набора лент 537

Указание параметров прокси-сервера в Windows 56

Управление бессрочными лицензиями 99

Управление дисками 319

Управление лентами 242, 274, 527

Управление лицензиями 98

Управление лицензиями по подписке 100

Управление обнаруженными машинами 107

Управление питанием BM 275, 457

Управление средами виртуализации 470

Управление учетными записями пользователей и отделами организации 560

Управляемое хранилище 173

Уровень сжатия 223

Условия 227

Условия запуска 192

Условия запуска задания 247

Условия поиска 498

Установка 18, 66, 74, 82, 546

Установка CommuniGate Pro 380

Установка Kubernetes 437

Установка oVirt вручную 115

Установка PXE-сервера 335

Установка VK WorkMail 399

Установка агента для ECP VeiL 125

Установка агента для OpenStack (РУСТЭК) вручную 127

Установка агента для SpaceVM 122

Установка агента для VMware (Windows) 74

Установка агентов 142

Установка Базис.DynamiX 132

Установка в Linux 63, 81

Установка в ОС Windows 58, 79

Установка виртуального устройства для Кибер Инфраструктуры 120

Установка или удаление продукта с указанием параметров вручную 85

Установка пакетов вручную 38

Установка пакетов из репозитория 36

Установка продукта с использованием преобразования MST 84

Установка сервера управления 58, 62

Установка узла хранения и службы каталогизации 538

Установленные библиотеки 559

Установлены ли необходимые пакеты? 35

Устранение неисправностей 108, 565

Учетная запись администратора в нескольких отделах 563

Учетные записи администратора 560

Ф

Файл настройки оповещений 515

Файлы сценария 300

Физическая машина 252

Фильтры файлов 226

Финализация машины 450

Формат резервной копии 218

Формат резервной копии и файлы резервных копий 219

Форматирование тома 331

Функция Changed Block Tracking (CBT) 221, 456

Х

Хост хранилища резервных копий доступен 194

Ц

Цели использования мастера создания носителей 292

Ч

Чередующийся том 327

Что делать после инвентаризации 533

Что еще нужно знать 200

Что необходимо для использования моментальных снимков оборудования SAN? 462

Что необходимо для использования резервного копирования с поддержкой приложений? 349

Что необходимо для резервного копирования почтовых ящиков? 367

Что происходит при активации Восстановление при загрузке 334

Что содержится в резервных копиях томов или дисков 178

Что такое ленточное устройство? 516

Что такое файл резервной копии? 214

Ш

Шаг 1. Формирование маркера регистрации 134

Шаг 2. Создание MST-преобразования и извлечение пакета установки 135

Шаг 3. Настройка объектов групповой политики 135

Шифрование дисков Microsoft BitLocker 40

Э

Экспорт и импорт структуры отчета 514

Экспорт резервных копий 279