КИБЕРПРОТЕКТ

КИБЕР Бэкап Старт



Руководство пользователя

Редакция: 03.10.2026

© ООО «Киберпротект», 2026

ООО «Киберпротект» является правообладателем данного документа.

Все права защищены.

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

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

Оглавление

Введение **1**

Что такое Кибер Бэкап Старт? 1

Системные требования и список поддерживаемых носителей 2

Минимальные системные требования 2

Поддерживаемые операционные системы 2

Поддерживаемые файловые системы 3

Поддерживаемые носители данных 3

Установка и удаление Кибер Бэкап Старт 4

Активация Кибер Бэкап Старт 5

Сведения о пробной версии 7

Обновление Кибер Бэкап Старт 7

Техническая поддержка 8

Приступая к работе. **9**

Язык интерфейса пользователя 9

Защита системы 9

Резервное копирование компьютера или сервера 10

Как создать загрузочный носитель 12

Резервное копирование всех данных 12

Что такое резервное копирование всего компьютера или сервера? 12

Создание Пакета для восстановления 14

Резервное копирование файлов 17

Клонирование жесткого диска 18

Восстановление компьютера или сервера 20

Учетная запись Киберпротект 23

Начало работы с Кибер Облаком 25

Как мы обеспечиваем защиту ваших данных 25

Сведения о подписке 26

Основные понятия **27**

Разница между резервными копиями файлов и дисков и разделов 29

Полные, инкрементные и дифференциальные резервные копии 30

Выбор места хранения резервных копий 34

Подготовка нового диска к резервному копированию 35

FTP-подключение 35

Настройки проверки подлинности 36

Присвоение имен файлам резервных копий . . . 37
Интеграция с ОС Windows . . . 37
Мастеры . . . 38
Вопросы и ответы по резервному копированию, восстановлению и клонированию . . . 40

Резервное копирование данных . . . 42

Резервное копирование дисков и разделов . . . 42
Резервное копирование файлов и папок . . . 44
Резервное копирование мобильных устройств . . . 46
Параметры резервного копирования . . . 48
Планирование . . . 49
Параметры ежедневного резервного копирования . . . 50
Параметры еженедельного резервного копирования . . . 51
Параметры ежемесячного резервного копирования . . . 51
Настройка параметров запуска по событию . . . 51
Схемы резервного копирования . . . 52
Схема с одной версией . . . 54
Схема с цепочкой версий . . . 54
Пользовательские схемы . . . 55
Уведомления при резервном копировании . . . 60
Исключение элементов из резервной копии . . . 62
Режим создания образа . . . 64
Защита резервных копий . . . 64
Защита резервных копий в онлайн-хранилище . . . 66
Команды до и после резервного копирования . . . 66
Редактирование пользовательских команд, выполняемых при резервном копировании . . . 67
Разделение резервной копии . . . 67
Проверка резервной копии . . . 68
Обработка ошибок . . . 69
Обработка ошибок для резервных копий и реплик в облаке . . . 70
Параметры безопасности файлов для создаваемой резервной копии . . . 71
Выключение компьютера . . . 72
Производительность операций резервного копирования . . . 72
Параметры питания ноутбука . . . 75
Сети Wi-Fi для резервного копирования в Кибер Облако . . . 75
Операции с резервными копиями . . . 76
Меню операций резервного копирования . . . 76
Действия и статистика резервного копирования . . . 79

Сортировка резервных копий в списке . . . 80
Репликация резервных копий в Кибер Облако . . . 81
Защита реплицированных данных . . . 82
Проверка резервных копий . . . 82
Резервное копирование в разные хранилища . . . 82
Добавление существующей резервной копии в список . . . 83
Очистка резервных копий, версий и реплик . . . 83
Удаление данных из Кибер Облака . . . 86
Восстановление данных . . . 88
Восстановление дисков и разделов . . . 88
Восстановление системы после аварии . . . 88
Попытка определения причины сбоя . . . 88
Подготовка к восстановлению . . . 89
Восстановление системы на тот же диск . . . 90
Восстановление системы на новый диск при работе с загрузочного носителя . . . 96
Восстановление дисков и разделов . . . 106
Свойства раздела . . . 108
Интерфейс UEFI . . . 109
Способ миграции . . . 116
Восстановление динамических и GPT-дисков и томов . . . 123
Пример восстановления в систему UEFI . . . 125
Настройка порядка загрузки в BIOS или UEFI BIOS . . . 126
Восстановление дисков из Кибер Облака . . . 128
Восстановление системы из Кибер Облака . . . 130
Восстановление файлов и папок . . . 139
Поиск в содержимом резервных копий . . . 141
Параметры восстановления . . . 142
Режим восстановления диска . . . 143
Команды до и после восстановления . . . 143
Редактирование пользовательских команд, выполняемых при восстановлении . . . 143
Параметры проверки . . . 144
Перезагрузка компьютера . . . 144
Параметры восстановления файлов . . . 144
Параметры перезаписи файлов . . . 145
Производительность операций восстановления . . . 145
Уведомления при восстановлении . . . 146
Архивирование данных. . . . 148
Что такое архивирование данных . . . 148

Что исключается из архивов . . . 149
Чем архивирование в облако отличается от резервного копирования в онлайн-хранилище . . . 149
Удаление дубликатов . . . 150
Создание архивов . . . 151
Параметры архивирования данных . . . 152
Доступ к архивным файлам . . . 152
Клонирование и перенос диска . . . 154
Утилита клонирования дисков . . . 154
Мастер клонирования дисков . . . 155
Создание разделов вручную . . . 157
Исключение элементов из клонирования . . . 159
Способ миграции . . . 160
Система загружается с помощью BIOS, MBR, UEFI не поддерживается . . . 161
Система, загружаемая с помощью BIOS, MBR, поддержка UEFI . . . 161
Система загружается с помощью BIOS, MBR, без Windows . . . 162
Система загружается с помощью BIOS, GPT, UEFI поддерживается . . . 163
Система загружается с помощью BIOS, GPT, без Windows . . . 163
Система загружается с помощью UEFI, MBR, UEFI не поддерживается . . . 164
Система загружается с помощью UEFI, MBR, UEFI поддерживается . . . 164
Система на основе UEFI, MBR, Windows отсутствует . . . 165
Система загружается с помощью UEFI, GPT, UEFI поддерживается . . . 166
Система, загружаемая с помощью UEFI, GPT, без Windows . . . 166
Перенос системы с жесткого диска на твердотельный накопитель . . . 167
Что делать, если Кибер Бэкап Старт не распознает твердотельный накопитель . . . 168
Перенос системы на твердотельный накопитель методом резервного копирования и восстановления . . . 169
Инструменты . . . 172
Мастер создания загрузочных носителей . . . 172
Как создать загрузочный носитель . . . 174
Загрузочный носитель: параметры запуска . . . 175
Добавление драйверов в существующий WIM-образ . . . 177
Создание ISO-файла из WIM-файла . . . 178
Проверка загрузочного носителя на возможность использования в случае необходимости . . . 179
Выбор видеорежима при загрузке с загрузочного носителя . . . 183
Восстановление при загрузке . . . 184
Экспериментальный режим . . . 186
Использование Экспериментального режима . . . 188
Параметры и уведомления Экспериментального режима . . . 191

Примеры использования Экспериментального режима . . . 192
Зона безопасности Киберпротект . . . 194
Создание и изменение зоны безопасности Киберпротект . . . 195
Расположение зоны безопасности Киберпротект . . . 195
Размер зоны безопасности Киберпротект . . . 197
Защита зоны безопасности Киберпротект . . . 198
Удаление зоны безопасности Киберпротект . . . 199
Добавление нового жесткого диска . . . 200
Выбор жесткого диска . . . 200
Выбор метода инициализации . . . 201
Создание разделов . . . 202
Настройки раздела . . . 203
Средства обеспечения безопасности и конфиденциальности . . . 205
Очистка диска . . . 205
Выбор источника . . . 207
Выбор алгоритма . . . 207
Заключительные действия . . . 211
Очистка системы . . . 212
Настройки очистки . . . 214
Параметры очистки по умолчанию . . . 215
Отдельные параметры очистки . . . 216
Просмотр . . . 220
Состояние операции очистки . . . 221
Подключение резервной копии . . . 221
Отключение резервной копии . . . 222
Работа с VHD(X)-файлами . . . 223
Преобразование резервных копий, созданных в ПО Киберпротект . . . 224
Импорт и экспорт параметров резервного копирования . . . 224
Устранение неисправностей. . . . 226
Создание отчетов о системе . . . 226
Сбор аварийных дампов . . . 228

Введение

Что такое Кибер Бэкап Старт?

Кибер Бэкап Старт — это комплексное решение для киберзащиты, которое обеспечивает безопасность всей вашей информации. С его помощью можно создавать резервные копии документов, фотографий, сообщений электронной почты, выбранных разделов или целого диска, включая операционную систему, приложения, настройки и все данные. Одним из его основных преимуществ является сочетание функций защиты данных и обеспечения безопасности.

Резервные копии позволяют восстановить систему компьютера или сервера при потере данных, случайном удалении важных файлов и папок или полном отказе жесткого диска.

Функция резервного копирования в онлайн-хранилище позволяет хранить файлы и диски в Кибер Облаке. Данные будут защищены даже в случае потери, кражи или поломки компьютера, и при необходимости их можно будет полностью восстановить на новое устройство.

Кибер Бэкап Старт поставляется в двух редакциях:

- расширенной с поддержкой ПК и серверов,
- стандартной с поддержкой ПК.

Основные функции

- *Резервное копирование дисков в локальное хранилище и в Кибер Облако*
- *Резервное копирование файлов в локальное хранилище и в Кибер Облако*
- *Загрузочный носитель*
- *Клонирование жесткого диска*
- *Архивирование данных*
- *Средства обеспечения безопасности и конфиденциальности*

> **Примечание**
>
> Невозможно создать резервные копии в Кибер Облаке с помощью восстановления при загрузке и загрузочного носителя.

Подробнее о защите компьютера или сервера см. в разделе *Защита системы*.

Системные требования и список поддерживаемых носителей

Минимальные системные требования

Для работы Кибер Бэкап Старт необходимо следующее оборудование.

- Процессор Intel Core 2 Duo 2 ГГц или аналогичный с поддержкой инструкций SSE.
- 2 ГБ ОЗУ.
- 4 ГБ свободного пространства на системном жестком диске.
- Дисковод CD-RW/DVD-RW или USB-накопитель для создания загрузочного носителя.
  - Для загрузочного носителя на базе Linux требуется около 660 МБ свободного пространства.
  - Для загрузочного носителя на базе Windows требуется около 700 МБ свободного пространства.
- Монитор с разрешением экрана не менее 1300x700 пикселей.
- Мышь или другое указывающее устройство (рекомендуется).

Предупреждение

Для развертываний на виртуальных машинах не гарантируется успешное резервное копирование и восстановление.

Другие требования

- Подключение к Интернету требуется для активации продукта и работы всех функций, использующих Кибер Облако. Дополнительные сведения см. в разделе *Активация Кибер Бэкап Старт*.
- Для запуска Кибер Бэкап Старт необходимы права администратора.

Поддерживаемые операционные системы

Кибер Бэкап Старт был испытан в следующих операционных системах:

- Windows Server 2025 — выпуски Standard и Datacenter,
- Windows Server 2022 — выпуски Standard и Datacenter,
- Windows Server 2019 — выпуски Standard и Datacenter,

- Windows 11,
- Windows 10.

Примечание

- Бета-версии не поддерживаются.
- Выпуски Windows Embedded, IoT, Windows 10 LTSB, Windows 10 LTSC и Windows 10 в S-режиме не поддерживаются.

Кибер Бэкап Старт также позволяет создать загрузочный диск CD-R/DVD-R или USB-накопитель для резервного копирования и восстановления дисков или разделов на компьютере с любым процессором Intel или AMD и любой операционной системой для ПК, включая Linux.

Работа программного обеспечения на прочих системах Windows не гарантируется.

Предупреждение

Успешное восстановление гарантируется только для поддерживаемых операционных систем. Для других операционных систем можно создать резервные копии в посекторном режиме, но они могут перестать загружаться после восстановления.

Поддерживаемые файловые системы

- NTFS;
- Ext2/Ext3/Ext4;
- ReiserFS3 (только резервное копирование и восстановление дисков или разделов);
- Linux Swap (только резервное копирование и восстановление дисков или разделов);
- FAT16/32/exFAT (без изменения размера при восстановлении дисков и разделов, клонировании).

Если файловая система повреждена или не поддерживается, Кибер Бэкап Старт копирует все секторы диска подряд.

Поддерживаемые носители данных

- Жесткие диски (HDD).
- Твердотельные накопители (SSD).
- Сетевые устройства хранения.

- FTP-серверы с поддержкой передачи файлов в пассивном режиме. При резервном копировании на FTP-сервер резервные копии будут разделены на файлы размером 2 ГБ.
- Устройства хранения USB 1.1/2.0/3.0, USB-C, eSATA, FireWire (IEEE-1394), SCSI и PC Card.

Ограничения на операции с динамическими дисками:

- Создание зоны безопасности Киберпротект на динамических дисках не поддерживается.
- Невозможно восстановить динамический том как динамический том, изменив размер вручную.
- Клонирование динамических дисков не поддерживается.

Установка и удаление Кибер Бэкап Старт

Как установить Кибер Бэкап Старт

1. Скачайте файл установки Кибер Бэкап Старт в личном кабинете. Доступ появится после покупки или запроса пробной версии продукта.
2. Запустите файл установки.

   Прежде чем начать процесс установки, Кибер Бэкап Старт проверяет наличие более новой версии на веб-сайте. Если новая версия доступна, она будет предложена для установки.
3. Нажмите **Установить**, чтобы начать установку.

   Кибер Бэкап Старт будет установлен на системный раздел (обычно C:).
4. После завершения установки нажмите кнопку **Запустить приложение**.
5. Прочитайте и примите условия лицензионных соглашений Кибер Бэкап Старт и Bonjour.

   Программа Bonjour будет установлена на компьютер для расширенной поддержки устройств NAS. Ее можно будет удалить в любой момент.
6. Если в вашей учетной записи уже есть лицензия продукта Кибер Бэкап Старт, то продукт будет активирован автоматически после входа в учетную запись.

   В случае отсутствия подходящей лицензии в учетной записи, вам будет предложено ввести лицензионный ключ и активировать продукт вручную.

   Если у вас нет лицензионного ключа, продукт можно будет использовать в пробном режиме в течение 30 дней.

> **Примечание**

Вы можете приобрести лицензии Кибер Бэкап Старт на веб-сайте Киберпротект.

Как выполнить восстановление после ошибки Кибер Бэкап Старт

Если Кибер Бэкап Старт перестает работать или возникают ошибки, возможно, повреждены файлы программы. Чтобы решить эту проблему, необходимо восстановить программу. Для этого запустите еще раз установщик Кибер Бэкап Старт. Он обнаружит Кибер Бэкап Старт на компьютере и предложит изменить или удалить ее.

Как удалить Кибер Бэкап Старт полностью

Windows 11

Нажмите **Пуск** → **Параметры** → **Приложения** → **Приложения и возможности** → **Cyber Backup Start** → **Удалить**.

Windows 10

Нажмите **Пуск** → **Параметры** → **Приложения** → **Cyber Backup Start** → **Удалить**.

Затем следуйте инструкциям на экране. После этого необходимо перезагрузить компьютер для завершения задания.

Примечание

Если использовалась *Зона безопасности*, то в открывшемся окне выберите необходимые действия с зоной.

Активация Кибер Бэкап Старт

Для использования Кибер Бэкап Старт требуется активация через Интернет. Без активации полностью функциональная версия продукта работает в течение 30 дней. Если активация не выполнена до окончания этого срока, все функции программы, кроме восстановления, становятся недоступны.

Если программа не может подключиться к серверу активации продукта Киберпротект, убедитесь, что ваш компьютер подключен к Интернету, перейдите в раздел **Учетная запись** и нажмите **Повторить попытку**, чтобы повторить попытку подключения к серверу активации Киберпротект.

Проблема неудавшейся активации лицензии

Возможные причины проблемы «Не удалось активировать лицензию»:

- Превышено максимальное количество компьютеров с установленным продуктом Кибер Бэкап Старт.

  Например, у вас есть одна лицензия для одного компьютера и вы устанавливаете Кибер Бэкап Старт на втором компьютере.

  Решения:

  - Введите новый лицензионный ключ. Если у вас его нет, вы можете приобрести новую лицензию на веб-сайте Киберпротект.
  - Перенесите лицензию на новый компьютер со старого, где продукт уже активирован. Для этого войдите в вашу учетную запись Киберпротект, перейдите в раздел **Продукты** и нажмите **Управлять**.

    Обратите внимание, что на старом компьютере Кибер Бэкап Старт будет деактивирован.

- Вы переустановили ОС Windows или поменяли оборудование на компьютере.

  Например, вы могли поставить новую материнскую плату или процессор. Активация будет потеряна, поскольку Кибер Бэкап Старт воспринимает компьютер как новый.

  Решение: Чтобы заново активировать Кибер Бэкап Старт на компьютере, следуйте инструкциям в статье Базы знаний.

Управление лицензиями и подписками в Личном кабинете

Вы можете управлять лицензиями и подписками в Личном кабинете. Вы можете делать следующее:

- Перемещать лицензии между компьютерами;
- Удалять лицензии с компьютеров;
- Разрешать конфликты активации продукта, включая проблему неудавшейся активации лицензии;
- Покупать новые лицензии.

Как управлять лицензиями и подписками:

1. Перейдите на страницу https://account.cyberprotect.ru/ и выполните вход в учетную запись Киберпротект.
2. Перейдите в раздел **Продукты** и выберите Кибер Бэкап Старт.

Сведения о пробной версии

Общие ограничения

Пробная версия Кибер Бэкап Старт работает только в течение 30 дней. Она имеет следующие ограничения:

- *Клонирование дисков* отключено;
- При загрузке с загрузочного носителя доступно только восстановление.

Кибер Облако

Кибер Облако — это облачное хранилище Киберпротект. В течение пробного периода у вас будет 1 ТБ в облачном хранилище. Вы можете использовать это пространство для хранения резервных копий и архивов. После завершения пробного периода Кибер Облако работает в режиме «только восстановление» в течение 30 дней. По окончании этого периода вы не сможете пользоваться сервисом Кибер Облако и все ваши данные будут удалены из сервиса.

Покупка полной версии

Полную версию можно приобрести на веб-сайте Киберпротект.

Обновление Кибер Бэкап Старт

Когда обновление для Кибер Бэкап Старт будет доступно на веб-сайте Киберпротект, вы сможете его скачать. Если на компьютере установлена предыдущая версия программы Кибер Бэкап Старт, можно установить новую версию поверх старой, не удаляя программы. Если же установлена еще более старая версия, рекомендуется сначала удалить ее.

Резервные копии, созданные в предыдущей версии Кибер Бэкап Старт, полностью совместимы с новой версией продукта. После обновления все имеющиеся резервные копии будут автоматически добавлены в список резервных копий.

Резервные копии, созданные более новой версией программы, могут быть несовместимы с предыдущими версиями. Если вернуть Кибер Бэкап Старт к предыдущей версии, то, скорее всего, придется заново создавать резервные копии с помощью старой версии. Настоятельно рекомендуется создавать новый загрузочный носитель после каждого обновления версии Кибер Бэкап Старт.

Как приобрести полную версию

Купить полную версию можно на веб-сайте Киберпротект.

Как обновить Кибер Бэкап Старт

1. Запустите Кибер Бэкап Старт.
2. На боковой панели нажмите **Учетная запись**.

   Если доступна новая версия, вы увидите соответствующее сообщение рядом с текущим номером сборки.
3. Щелкните **Загрузить и установить**.

   > **Примечание**
   >
   > Прежде чем начать загрузку, убедитесь, что брандмауэр не блокирует процесс загрузки.

4. Когда новая версия будет загружена, щелкните **Установить сейчас**.

Для автоматической проверки обновлений перейдите в раздел **Параметры** и установите флажок **При запуске автоматически проверять наличие обновлений**.

Техническая поддержка

За помощью в использовании Кибер Бэкап Старт обращайтесь по адресу https://cyberprotect.ru/support/.

Приступая к работе

Язык интерфейса пользователя

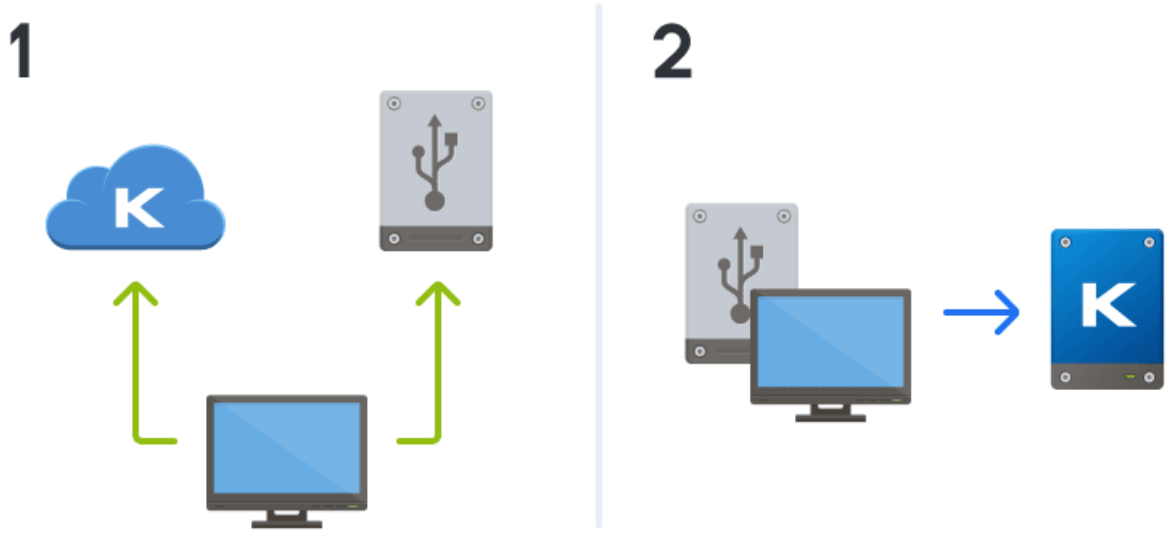
Перед началом работы выберите предпочитаемый язык пользовательского интерфейса Кибер Бэкап Старт. По умолчанию язык устанавливается в соответствии с языком отображения Windows.

Как изменить язык пользовательского интерфейса:

1. Запустите Кибер Бэкап Старт.
2. В разделе **Параметры** выберите предпочитаемый язык из списка.

Защита системы

1. *Резервное копирование компьютера или сервера*.
2. *Создайте загрузочный носитель*.



Рекомендуется протестировать загрузочный носитель, как описано в разделе *Проверка загрузочного носителя на возможность использования в случае необходимости*.

Резервное копирование компьютера или сервера

Когда необходимо создавать резервную копию?

Создавайте новую версию резервной копии после каждого значимого события в системе.

Примеры таких событий:

- Вы приобрели новый компьютер.
- Вы переустановили ОС Windows на компьютере.
- Вы настроили все параметры системы (дату, время, язык и т. д.) и установили на новый компьютер все нужные программы.
- Важное обновление системы.

> **Примечание**
>
> Чтобы убедиться, что диск в нормальном состоянии, перед резервным копированием рекомендуется выполнить проверку на вирусы. Используйте для этого антивирусную программу. Учтите, что эта операция часто занимает много времени.

Как создать резервную копию компьютера?

Предусмотрено два варианта защиты системы:

- **Резервное копирование всего ПК** (рекомендуется)

  Кибер Бэкап Старт создаст резервную копию всех внутренних жестких дисков в дисковом режиме. Резервная копия будет содержать операционную систему, установленные программы, системные настройки и все личные данные, включая фотографии, музыку и документы. Дополнительные сведения см. в разделе *Резервное копирование всех данных на компьютере*.

- **Резервное копирование системного диска**

  Можно выбрать создание резервной копии системного раздела или всего системного диска. Дополнительные сведения см. в разделе *Резервное копирование дисков и разделов*.

Выполните следующие действия:

1. Запустите Кибер Бэкап Старт.
2. На боковой панели нажмите **Резервное копирование**.

   Если резервная копия создается впервые, откроется окно настройки резервного копирования. Если у вас уже есть резервные копии в списке, щелкните **Добавить копию**.

3. Щелкните значок **Изменить источник** и выберите **Весь компьютер**.

   Чтобы создать резервную копию только системного диска, щелкните **Диски и разделы**, затем выберите системный раздел (обычно C:) и раздел «Зарезервировано системой» (если есть).

4. Щелкните значок **Выбор хранилища** и выберите хранилище для создаваемой резервной копии (см. рекомендации ниже).

5. Нажмите кнопку **Создать копию**.

После этого в списке резервных копий появится новая панель резервной копии. Чтобы создать новую версию резервной копии впоследствии, выберите панель резервной копии из списка и щелкните **Создать копию**.

Где следует хранить резервные копии диска?

- **Хорошо** — обычный внутренний жесткий диск.
- **Лучше** — *Зона безопасности*. Это специальный защищенный раздел на локальном жестком диске для хранения резервных копий.
- **Рекомендуется** — *Кибер Облако* или внешний жесткий диск.

Дополнительные сведения см. в разделе *Выбор места хранения резервных копий*.

Сколько необходимо версий резервной копии?

В большинстве случаев нужны 2–3 *версии резервных копий* всего содержимого ПК или системного диска, самое большее — 4–6 (сведения о времени создания резервных копий см. выше). Количество версий можно контролировать с помощью правил автоматической очистки. Дополнительные сведения см. в разделе *Пользовательские схемы*.

Помните, что первая версия резервной копии (полная версия) является самой важной. Она имеет наибольший размер, поскольку содержит все данные, хранящиеся на диске. Последующие версии резервной копии (инкрементные и дифференциальные версии) могут быть организованы по различным схемам. Эти версии содержат только измененные данные. Поэтому они зависят от полной версии резервной копии и полная версия так важна.

По умолчанию резервная копия диска создается с применением инкрементной схемы. Эта схема оптимальна в большинстве случаев.

Примечание

Для опытных пользователей: рекомендуется создать 2–3 полных версии резервной копии и сохранить их на различных устройствах. Этот метод гораздо более надежен.

Как создать загрузочный носитель

Загрузочный носитель — это диск CD/DVD, флеш-накопитель USB или другой съемный носитель, с которого можно запустить Кибер Бэкап Старт, если ОС Windows не загружается. Носитель можно сделать загрузочным с помощью программы Мастер создания загрузочных носителей.

Как создать загрузочный носитель:

1. Вставьте диск CD/DVD или подключите USB-накопитель (флеш-накопитель USB или внешний жесткий диск / твердотельный накопитель).
2. Запустите Кибер Бэкап Старт.
3. На боковой панели щелкните **Инструменты** и выберите **Мастер создания загрузочных носителей**.
4. На первом шаге выберите **Простой**.
5. Выберите устройство, которое будет использоваться для создания загрузочного носителя.
6. Нажмите кнопку **Приступить**.

Как использовать загрузочный носитель:

Загрузочный носитель используется для восстановления компьютера, когда ОС Windows не запускается.

1. Подключите загрузочный носитель к компьютеру (вставьте диск CD/DVD или подключите USB-накопитель).
2. Измените порядок загрузки в BIOS так, чтобы сделать загрузочный носитель первым устройством загрузки.

   Дополнительные сведения см. в разделе *Настройка порядка загрузки в BIOS*.
3. Загрузите компьютер с загрузочного носителя и выберите Кибер Бэкап Старт.

   Когда Кибер Бэкап Старт загрузится, его можно будет использовать для восстановления компьютера.

Дополнительные сведения см. в разделе *Мастер создания загрузочных носителей*.

Резервное копирование всех данных

Что такое резервное копирование всего компьютера или сервера?

Резервное копирование всего компьютера или сервера — это самый простой способ создать резервную копию всего содержимого ПК. Этот вариант рекомендуется в случае, если вы не уверены, какие данные следует защитить. Если требуется создать резервную копию только системного раздела, см. дополнительные сведения в разделе *Резервное копирование дисков и разделов*.

Если в качестве типа резервного копирования выбран «Весь компьютер», то Кибер Бэкап Старт создает резервную копию всех внутренних жестких дисков в дисковом режиме. Резервная копия будет содержать операционную систему, установленные программы, системные настройки и все личные данные, включая фотографии, музыку и документы.

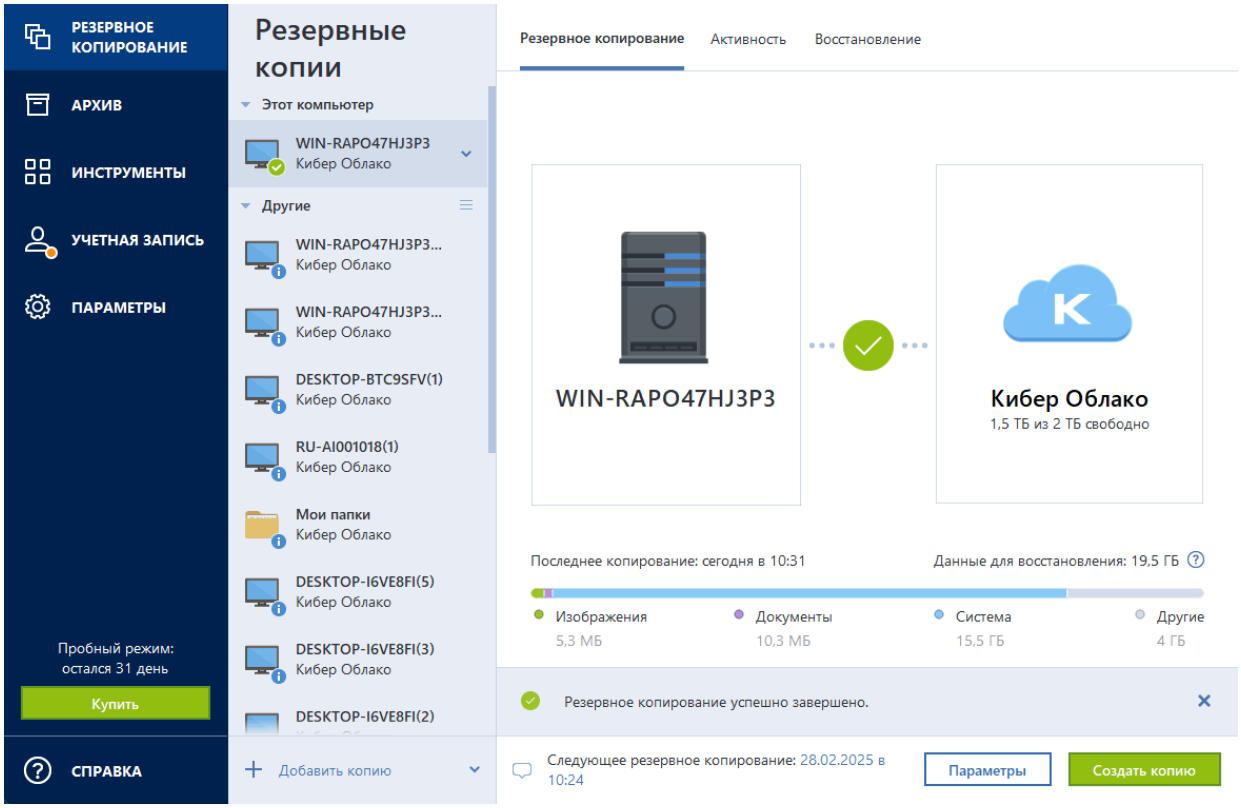
Восстановление из резервной копии всего компьютера также упрощено. Требуется только выбрать дату, к которой необходимо вернуть данные. Кибер Бэкап Старт восстанавливает все данные из резервной копии в исходное расположение. Также вы можете выбрать новое место для восстановления или восстановить отдельные диски, разделы, файлы и папки. Дополнительные сведения см. в разделе *Резервное копирование файлов и папок*.

Если резервная копия всего компьютера содержит динамические диски, то восстановление данных выполняется в режиме раздела. Это означает, что вы можете выбрать отдельные разделы и изменить путь восстановления. Дополнительные сведения см. в разделе *Восстановление динамических и GPT-дисков и томов*.

Как создать резервную копию всего компьютера

1. Запустите Кибер Бэкап Старт.
2. На боковой панели нажмите **Резервное копирование**.
3. Щелкните значок «плюс» в нижней части списка резервных копий.
4. Щелкните значок **Изменить источник** и выберите **Весь компьютер**.
5. Щелкните значок **Выбор хранилища** и выберите место для сохранения резервной копии.

   Резервную копию компьютера рекомендуется создавать в Кибер Облаке либо в локальном или сетевом хранилище. Дополнительные сведения см. в разделе *Выбор места хранения резервных копий*.



6. [Необязательно] Выберите **Параметры**, чтобы задать параметры резервного копирования. Дополнительные сведения см. в разделе *Параметры резервного копирования*.
7. Нажмите кнопку **Создать копию**.

Примечание

При резервном копировании данных в Кибер Облако создание первой резервной копии может занять длительное время. Последующие операции резервного копирования должны происходить намного быстрее, так как через Интернет будут передаваться только изменения в файлах.

Создание Пакета для восстановления

Чтобы восстановить компьютер после сбоя, необходимо иметь два ключевых компонента: резервную копию системного диска и загрузочный носитель. Как правило, эти компоненты разделены. Например, резервная копия системы хранится на внешнем диске или в Кибер Облаке, а загрузочный носитель представляет собой небольшой флеш-накопитель USB. Пакет для восстановления объединяет оба компонента, чтобы у вас было одно устройство, на котором есть все необходимое для восстановления компьютера в случае сбоя. Это внешний жесткий диск, на котором находятся файлы, необходимые для загрузки компьютера в режиме восстановления, и резервная копия системного раздела, всего компьютера или любого диска.

Резервная копия, входящая в Пакет для восстановления, может содержать любые данные, нуждающиеся в защите, и обновляться в соответствии с настройками *расписания*. Более того, внешний жесткий диск не будет полностью занят Пакетом для восстановления. Загрузочный носитель занимает всего 2 ГБ дискового пространства, а остальное место может использоваться под резервную копию системного раздела или всего компьютера в составе Пакета для восстановления, а также любые другие данные, в том числе другие резервные копии, личные данные, фотографии и т. п. Однако не следует хранить больше одного Пакета для восстановления на одном внешнем жестком диске.

Неважно, сколько резервных копий находится на внешнем жестком диске, для восстановления компьютера нужен только один Пакет для восстановления. Загрузочный носитель работает с любой резервной копией системного раздела или всего компьютера, если они созданы для того же компьютера или компьютеров с той же конфигурацией.

В качестве устройства для Пакета для восстановления можно использовать:

- **внешний жесткий диск**

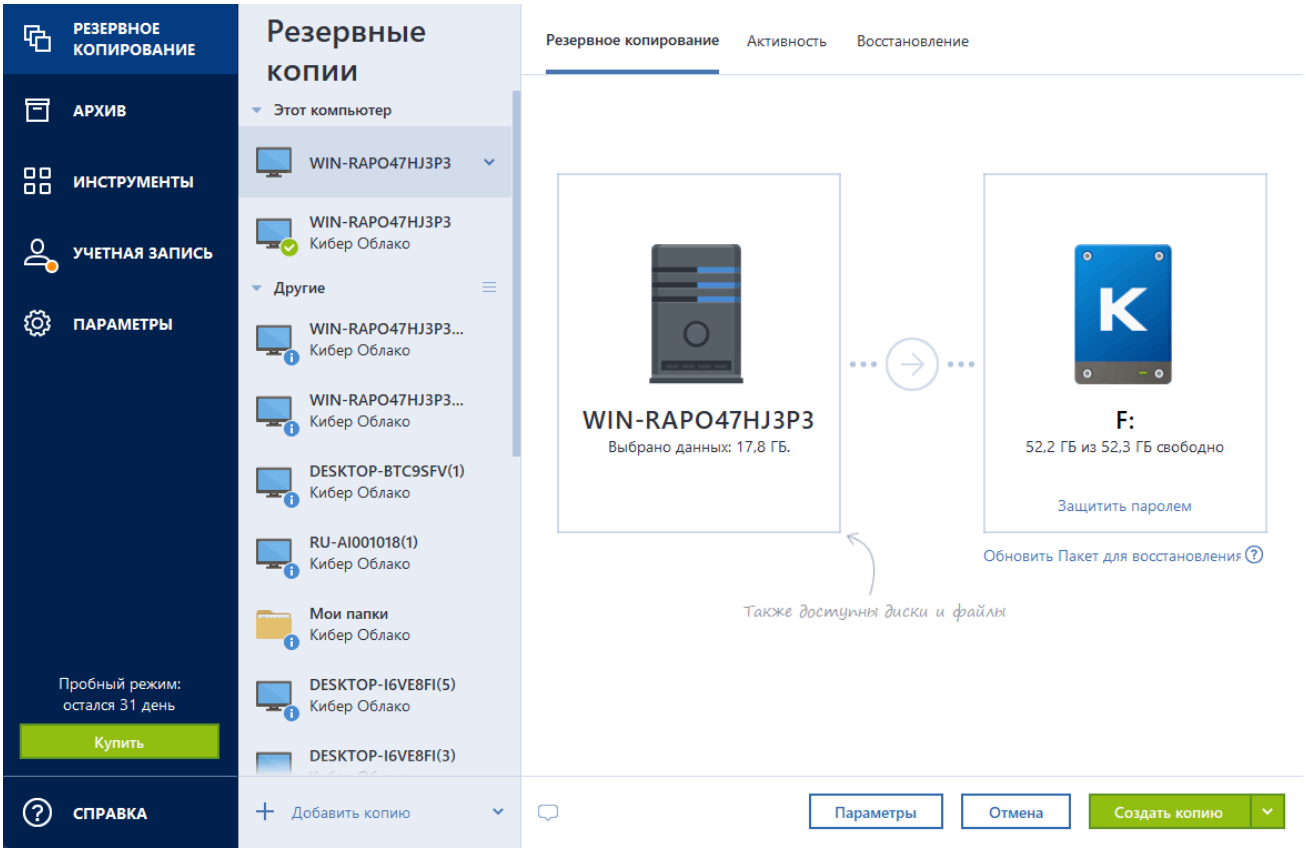
  Диск должен иметь размер более 32 ГБ и файловую систему NTFS, FAT32 или exFAT. Если на диске другая файловая система, Кибер Бэкап Старт предложит отформатировать диск.

- **флеш-накопитель USB**

  Флеш-накопитель должен иметь формат MBR и размер не менее 32 ГБ. Если используется флеш-накопитель GPT, Кибер Бэкап Старт предложит преобразовать его в MBR. Обратите внимание, что флеш-накопители поддерживаются только в Windows 10 (сборка 1703 и выше) и Windows 11.

Как создать Пакет для восстановления:

Если при настройке резервного копирования системного раздела, всего компьютера или любого диска выбрать в качестве места назначения внешний жесткий диск, Кибер Бэкап Старт предложит создать Пакет для восстановления.



1. Щелкните **Создать копию** или **Создать Пакет для восстановления**.
2. В открывшемся окне щелкните **Создать**.

   Кибер Бэкап Старт создаст небольшой раздел на выбранном диске и запишет туда загрузочные файлы. Для этого будет уменьшен размер одного из существующих томов. Если это не GPT-диск с файловой системой NTFS, FAT32 или exFAT, Кибер Бэкап Старт предложит отформатировать диск. Учтите, что при форматировании диска все данные на нем будут удалены.
3. После успешной записи загрузочных файлов на диск он преобразуется в загрузочный носитель, который можно использовать для восстановления компьютера. Чтобы завершить создание Пакета для восстановления, необходимо сохранить на этот диск резервную копию системного раздела, всего компьютера или любого диска. Для этого щелкните **Создать копию**. Если вы пропускаете этот шаг, не забудьте позже создать резервную копию на этом диске. Дополнительные сведения см. в разделе *Резервное копирование дисков и разделов*.

   Когда Пакет для восстановления готов, его можно использовать для восстановления компьютера. Дополнительные сведения см. в разделе *Восстановление системы на тот же диск*.

Каждый раз при настройке резервного копирования на внешнее устройство с Пакетом для восстановления Кибер Бэкап Старт будет проверять его версию. Если доступна более новая версия Пакета для восстановления, Кибер Бэкап Старт предложит обновить Пакет для восстановления на внешнем устройстве.

Резервное копирование файлов

Чтобы защитить только документы, фотографии, музыку и видеозаписи, нет необходимости выполнять резервное копирование всего раздела, содержащего эти файлы. Можно создать резервные копии отдельных файлов и папок и сохранить их в хранилищах следующих типов:

- Локальное или сетевое хранилище.

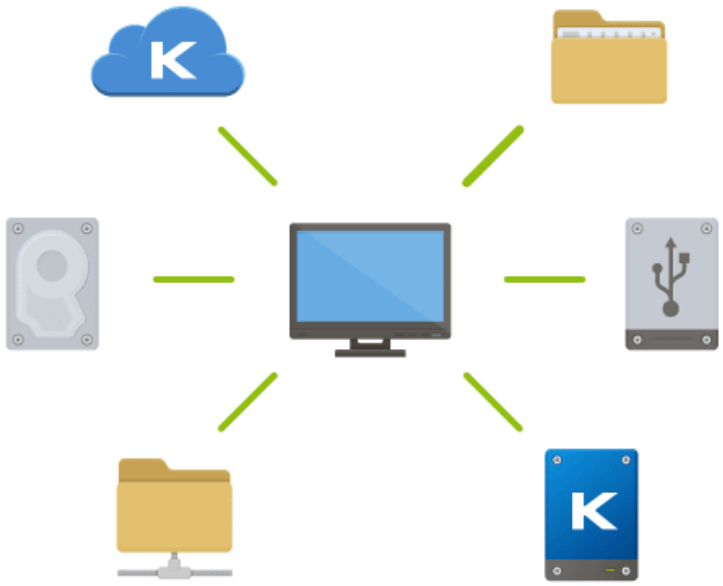
  Это простой и быстрый вариант. Используйте его для защиты файлов, которые редко изменяются.

- *Кибер Облако*

  Это надежный вариант. Используйте его для защиты важных файлов, а также файлов, к которым необходим доступ для других устройств или пользователей.

  Чтобы использовать Кибер Облако, необходима учетная запись Киберпротект и подписка на сервис Кибер Облако.

  Дополнительные сведения см. в разделе *Сведения о подписке*.



Как выполнить резервное копирование файлов и папок:

1. Запустите Кибер Бэкап Старт.
2. На боковой панели нажмите **Резервное копирование**.
3. Щелкните значок «плюс» в нижней части списка резервных копий.

4. Щелкните значок **Изменить источник** и выберите **Файлы и папки**.
5. В открывшемся окне установите флажки напротив нужных файлов и папок и нажмите кнопку **ОК**.
6. Щелкните значок **Выбор хранилища** и выберите место назначения резервной копии.
    - **Кибер Облако** — войдите в свою учетную запись и нажмите кнопку **ОК**.
    - **Внешний диск** — если к компьютеру подключен внешний диск, его можно выбрать из списка.
    - **NAS** — выберите устройство NAS из списка обнаруженных устройств NAS. Если устройство NAS всего одно, Кибер Бэкап Старт по умолчанию предложит его как место хранения резервных копий.
    - **Обзор** — выберите место назначения в дереве папок.
7. Нажмите кнопку **Создать копию**.

Дополнительные сведения см. в разделе *Резервное копирование файлов и папок*.

Клонирование жесткого диска

Зачем это нужно?

Когда на жестком диске начинает не хватать свободного места, можно приобрести новый диск большей емкости и перенести на него все данные. Обычная операция копирования не делает новый жесткий диск идентичным старому. Например, если открыть проводник Windows и скопировать все файлы и папки на новый жесткий диск, Windows не загрузится с нового диска. Утилита клонирования диска позволяет не только скопировать все данные, но и сделать Windows загружаемой на новом жестком диске.



Перед началом операции

Рекомендуется сразу установить целевой (новый) диск в место планируемого использования, а исходный диск — в другое место, например во внешний USB-корпус. Это особенно важно для ноутбуков.

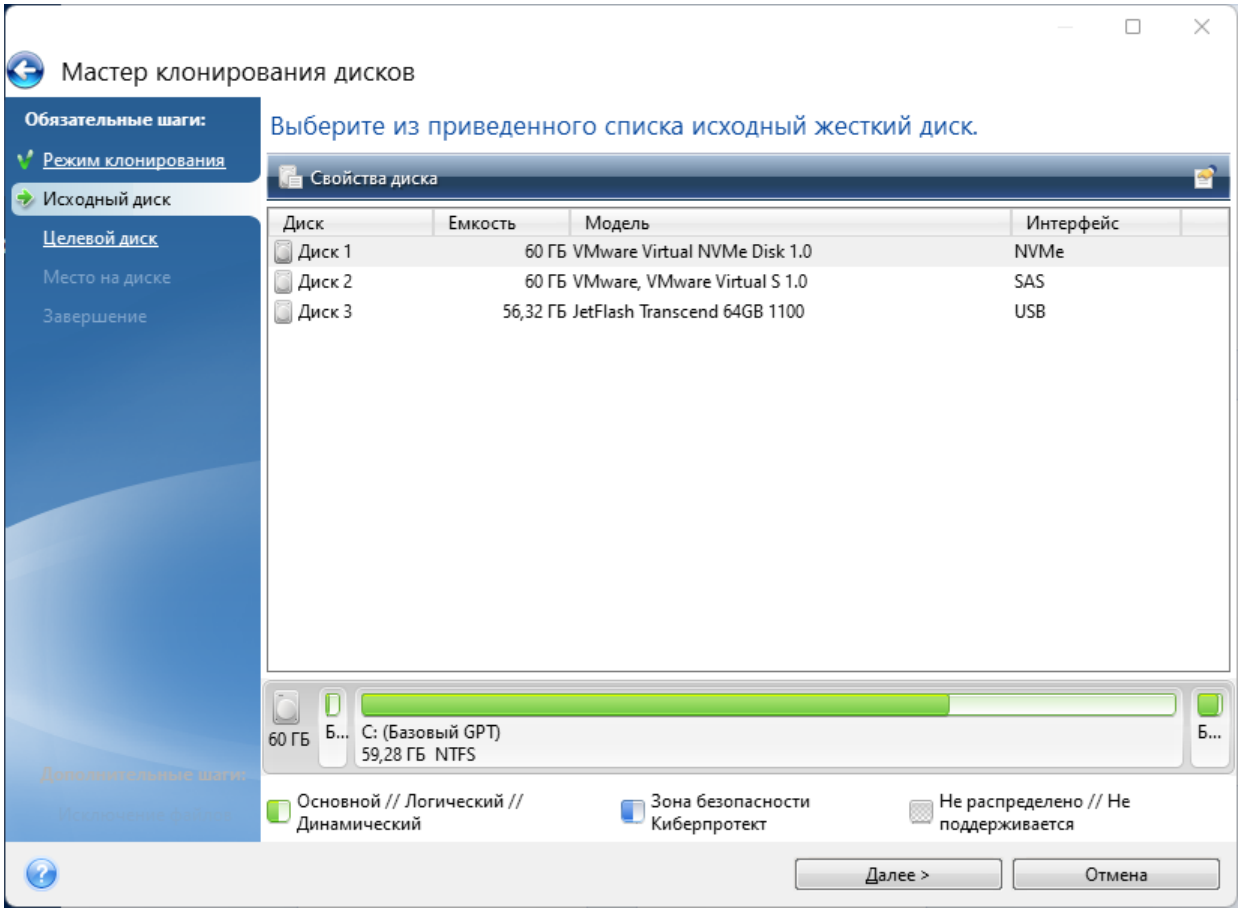
> **Примечание**
>
> Рекомендуется, чтобы старый и новый диски работали в одном режиме контроллера (например, IDE или AHCI). Иначе компьютер может не загружаться с нового жесткого диска.

Клонирование диска

1. На боковой панели щелкните **Инструменты** и выберите **Клонирование диска**.
2. На шаге **Режим клонирования** рекомендуем выбрать режим переноса **Автоматически**. В этом случае размеры разделов будут пропорционально изменены в соответствии с размером нового жесткого диска. Режим **Вручную** предоставляет большую гибкость. Дополнительные сведения о ручном режиме см. в разделе *Мастер клонирования дисков*.

   > **Примечание**
   >
   > Если программа обнаружит на компьютере два диска, один из которых содержит разделы, а другой — нет, она автоматически распознает диск с разделами как исходный, а диск без разделов как целевой. В этом случае следующие шаги будут пропущены и откроется итоговое окно клонирования.

3. На шаге **Исходный диск** выберите диск, который необходимо клонировать.



4. На шаге **Целевой диск** выберите диск, на который будут перенесены клонированные данные.

> **Примечание**
>
> Если на одном из дисков разделы отсутствуют, программа сама определит, что данный диск является целевым, и текущий шаг будет пропущен.

5. На шаге **Завершение** убедитесь, что настроенные параметры соответствуют вашим целям, и нажмите кнопку **Приступить**.

По умолчанию Кибер Бэкап Старт выключает компьютер после завершения процесса клонирования. Это позволит извлечь один из жестких дисков.

Восстановление компьютера или сервера

Восстановление системного диска — важная операция. Перед началом работы рекомендуется прочитать подробные описания в следующих разделах справки:

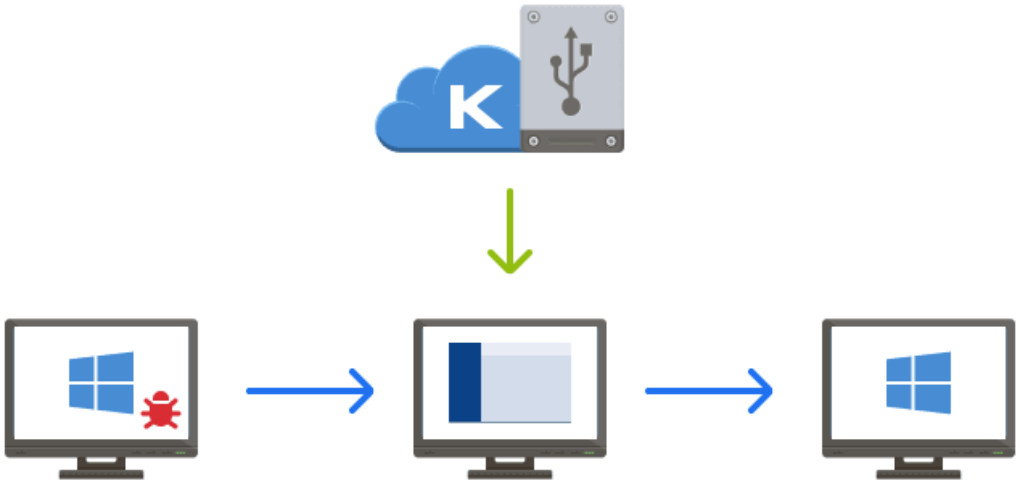
- *Попытка определения причины сбоя*

- *Подготовка к восстановлению*
- *Восстановление системы на тот же диск*

Рассмотрим два разных случая:

1. Windows работает неправильно, но Кибер Бэкап Старт запускается.
2. Windows не запускается (например, если при включении компьютера на экране отображается что-то необычное).

Случай 1. Как восстановить компьютер, если Windows работает неправильно?

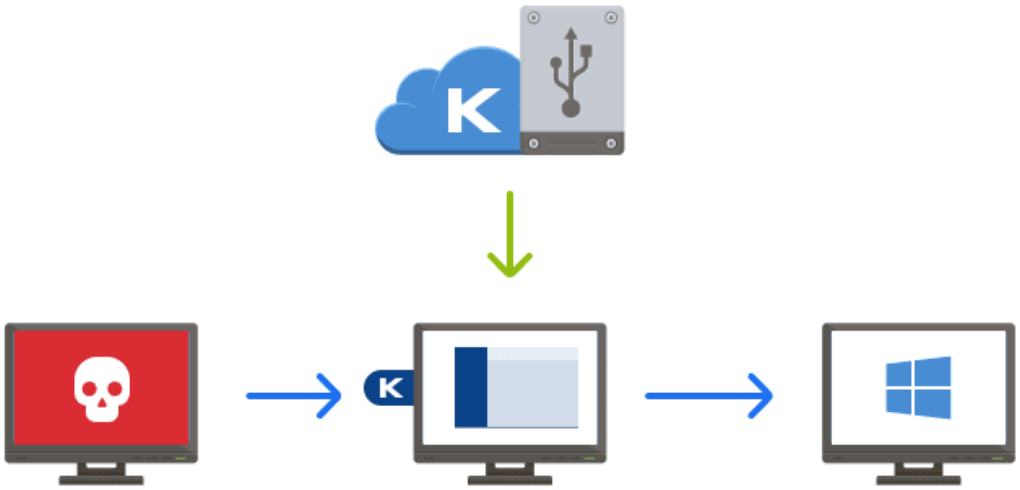


1. Запустите Кибер Бэкап Старт.
2. На боковой панели нажмите **Резервное копирование**.
3. Выберите из списка резервную копию, содержащую системный диск. Резервная копия может располагаться в локальном или сетевом хранилище либо в Кибер Облаке.
4. На правой панели нажмите **Восстановление**.
5. Выберите версию резервной копии (состояние данных на определенную дату и время).
6. Выберите для восстановления системный раздел и раздел «Зарезервировано системой» (если есть).
7. Нажмите кнопку **Восстановить**.

Примечание

Для завершения операции Кибер Бэкап Старт должен перезагрузить систему.

Случай 2. Как восстановить компьютер, если Windows не запускается?



1. Подключите загрузочный носитель к компьютеру и запустите специальную автономную версию Кибер Бэкап Старт.

   Дополнительные сведения см. в разделах *Как создать загрузочный носитель* и *Настройка порядка загрузки в BIOS или UEFI BIOS*.

2. На экране приветствия выберите **Мои диски** в раздел **Восстановить**.

3. Выберите резервную копию системного диска, которая будет использоваться для восстановления. Щелкните резервную копию правой кнопкой мыши и выберите **Восстановить**.

   Если резервная копия не отображается, нажмите кнопку **Обзор** и укажите путь к резервной копии вручную. В том же окне можно подключиться к Кибер Облаку и выбрать резервную копию в онлайн-хранилище. Дополнительные сведения см. в разделе *Восстановление системы из Кибер Облака*.

4. На шаге **Метод восстановления** выберите **Восстановить диски или разделы**.

5. На шаге **Объект восстановления** выберите системный раздел (обычно диск C). Обратите внимание, что системный раздел обозначен флагами Pri, Act. Также выберите раздел «Зарезервировано системой» (если есть).

6. Можно оставить все параметры разделов без изменений и нажать кнопку **Завершить**.
7. Ознакомьтесь с перечнем операций и нажмите кнопку **Приступить**.
8. После завершения операции выйдите из автономной версии Кибер Бэкап Старт, извлеките загрузочный носитель (если есть) и загрузите компьютер с восстановленного системного раздела. Когда вы убедитесь, что ОС Windows восстановлена до нужного состояния, восстановите исходный порядок загрузки.

Учетная запись Киберпротект

Учетная запись Киберпротект необходима для использования возможностей продукта Кибер Бэкап Старт. Например, учетная запись нужна при следующих действиях:

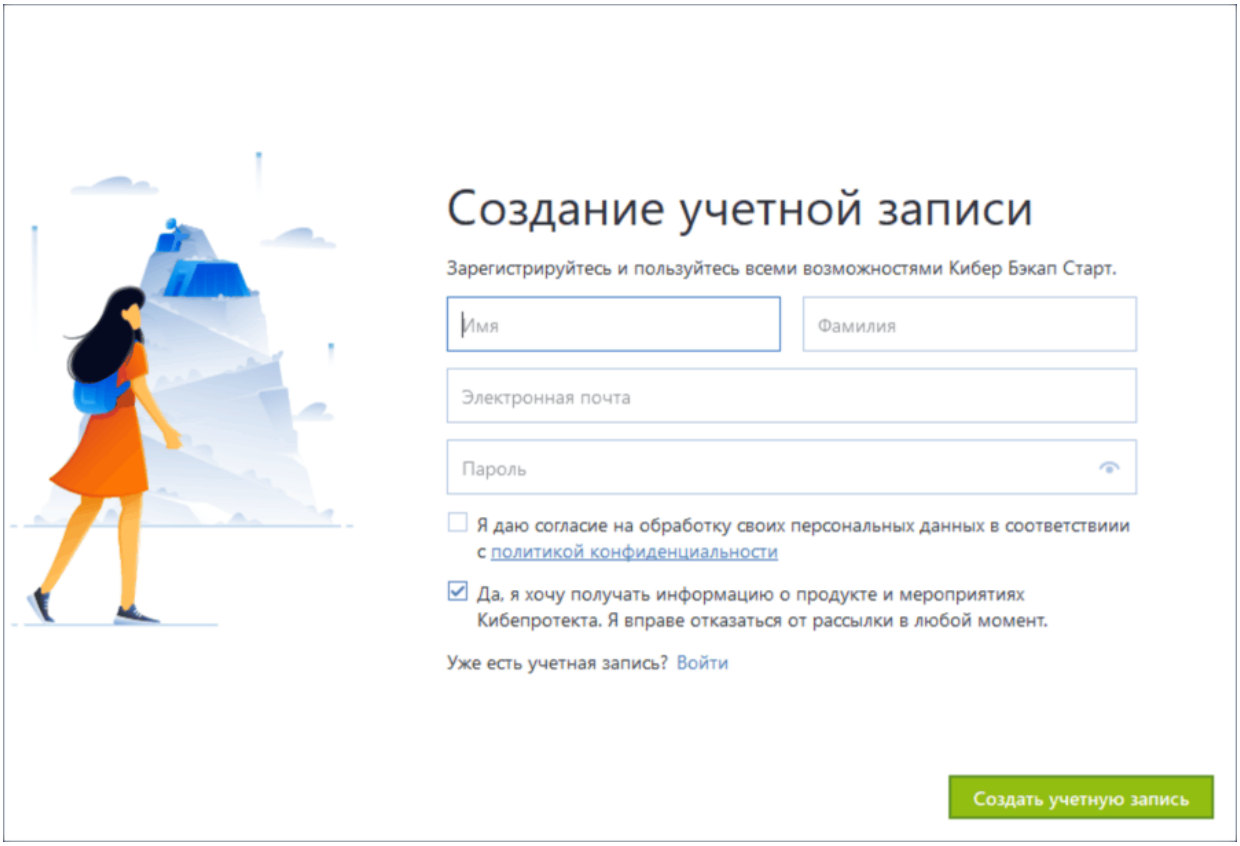
- активация продукта Кибер Бэкап Старт;
- резервное копирование в Кибер Облако;
- архивация данных в Кибер Облако.

Учетная запись Киберпротект обычно создается в следующих случаях:

- покупка продукта Киберпротект;
- регистрация продукта Киберпротект при его установке.

Как создать учетную запись Киберпротект:

1. В форме регистрации укажите требуемые данные, примите условия использования и при желании подпишитесь на новости и специальные предложения.



2. На указанный адрес электронной почты будет отправлено сообщение. Откройте его и подтвердите создание учетной записи.

Примечание

Для безопасности личных данных используйте надежный пароль, защищайте его от попадания в руки злоумышленников и время от времени меняйте его.

Как выполнить вход со своей учетной записью Киберпротект:

1. Запустите Кибер Бэкап Старт.
2. Введите адрес электронной почты и пароль, которые вы указали при создании вашей учетной записи, после чего нажмите **Войти**.

Как выйти из учетной записи Киберпротект:

1. На боковой панели нажмите **Учетная запись**.
2. Щелкните ваш адрес электронной почты, затем выберите **Выход**.

Начало работы с Кибер Облаком

Удаленное хранилище

Кибер Облако — это защищенное удаленное хранилище для:

- резервных копий файлов и папок;
- резервных копий разделов и дисков;
- реплик резервных копий;
- архивов.

Поскольку файлы находятся в удаленном хранилище, они будут защищены даже в случае кражи компьютера или пожара в доме. В случае аварии или повреждения данных вы сможете восстановить файлы и даже все содержимое компьютера.

С помощью одной учетной записи можно сохранить данные с нескольких компьютеров.

Чтобы использовать Кибер Облако, необходима подписка на продукт Кибер Бэкап Старт. Подробнее см. в разделе *Сведения о подписке*.

Веб-интерфейс Кибер Облака

Веб-интерфейс Кибер Облака позволяет просматривать и восстанавливать данные, которые хранятся в Кибер Облаке. Для работы с веб-интерфейсом можно использовать любой компьютер, подключенный к Интернету.

Для доступа к веб-интерфейсу Кибер Облака, войдите в учетную запись Киберпротект и перейдите в раздел **Резервные копии**.

Как мы обеспечиваем защиту ваших данных

При использовании Кибер Облака в качестве хранилища вам нужна уверенность в том, что ваши личные файлы не попадут в руки злоумышленников. Возможно, вас особенно беспокоит безопасность использования мобильного устройства, поскольку все данные будут передаваться через Интернет.

Мы гарантируем сохранность ваших данных. Прежде всего мы используем протоколы с шифрованием (SSL, TLS) для передачи всех данных как через Интернет, так и по локальной сети. Для доступа к данным выполните вход в свою учетную запись, указав адрес электронной почты и пароль. Вы также можете выбрать использование только защищенных сетей Wi-Fi для резервного копирования данных. В этом случае данные будут в полной безопасности при передаче в Кибер Облако. Выберите защищенные сети Wi-Fi для резервного копирования (см. *Сети Wi-Fi для резервного копирования в Кибер Облако*) в разделе **Параметры**.

Сведения о подписке

Для работы функций Кибер Бэкап Старт, использующих Кибер Облако (таких как резервное копирование в онлайн-хранилище и облачное архивирование), требуется подписка на продукт Кибер Бэкап Старт. Оформить подписку можно на веб-сайте Киберпротект.

Примечание

На Кибер Облако распространяется наша политика лицензирования. Дополнительные сведения см. на странице https://cyberprotect.ru/licensing.

Пробная версия

При активации пробной версии продукта ваша учетная запись автоматически получает 1 ТБ в хранилище и бесплатную подписку на Кибер Бэкап Старт в течение пробного периода. Подробнее см. в разделе *Сведения о пробной версии*.

Полная версия

Подписку на Кибер Бэкап Старт можно купить на веб-сайте Киберпротект.

Основные понятия

Этот раздел содержит общие сведения об основных принципах работы программы.

Резервное копирование и восстановление

Резервное копирование — создание копий данных для **восстановления** оригинала в случае утраты.

Резервные копии в основном используются в двух случаях:

- Для восстановления операционной системы, если она повреждена или не запускается (так называемое аварийное восстановление). Дополнительные сведения о защите компьютера от аварий см. в разделе *Защита системы*.
- Для восстановления определенных файлов и папок после случайного удаления или повреждения.

Кибер Бэкап Старт предоставляет решение для обоих случаев, создавая резервные копии как дисков и разделов, так и файлов.

Методы восстановления

- **Полное восстановление** можно выполнить в исходное или новое хранилище.

  Если выбрано исходное хранилище, то данные в нем полностью перезаписываются данными из резервной копии. При выборе нового хранилища данные просто копируются в него из резервной копии.

- **Инкрементное восстановление** выполняется только в исходное хранилище и только из облачной резервной копии. Перед запуском восстановления файлы в исходном хранилище сравниваются с файлами в резервной копии по атрибутам, таким как размер файла и дата последнего изменения. Несовпадающие файлы помечаются для восстановления, а все остальные игнорируются. Таким образом, в отличие от полного восстановления, Кибер Бэкап Старт восстанавливает только измененные файлы. Этот метод значительно сокращает время восстановления и экономит трафик при восстановлении из Кибер Облака.

Версии резервной копии

Версии резервной копии — это файл или файлы, создаваемые в процессе каждой операции резервного копирования. Количество созданных версий равно количеству выполненных операций резервного копирования. Таким образом, версия представляет собой момент времени, на который можно восстановить систему или данные.

Версии представляют собой полные, инкрементные и дифференциальные резервные копии — см.

раздел *Полное, инкрементное и дифференциальное резервное копирование*.

Версии резервных копий аналогичны версиям файлов. Понятие версий файлов знакомо пользователям, применяющим функцию Windows «Предыдущие версии файлов». Эта функция позволяет вернуть файл в состояние на определенный момент времени. Версия резервной копии позволяет восстановить данные аналогичным образом.

Клонирование диска

В ходе этой операции выполняется копирование всего содержимого одного диска на другой диск. Например, это может быть необходимо, если требуется перенести операционную систему, приложения и данные на новый диск большей емкости. Это можно сделать двумя способами.

- Использовать утилиту клонирования диска.
- Создать резервную копию старого диска, а затем восстановить ее на новый диск.

Формат файла резервной копии

Кибер Бэкап Старт обычно сохраняет резервные копии в собственном формате TIBX с применением сжатия. Данные из резервных копий в TIBX-файлах можно восстановить только с помощью Кибер Бэкап Старт в Windows или в среде восстановления.

Проверка резервной копии

Функция проверки резервной копии позволяет убедиться, что резервная копия не повреждена и данные можно восстановить. При создании резервной копии программа добавляет к блокам данных контрольные суммы. Целостность файла резервной копии проверяется путем пересчета контрольной суммы данных и сравнения полученной суммы со значением из резервной копии. Если все сравниваемые значения совпадают, значит файл резервной копии не поврежден.

Планирование

Данные, восстанавливаемые из резервных копий, должны содержать актуальную информацию, поэтому резервные копии должны регулярно обновляться. Планируйте создание резервных копий, чтобы оно выполнялось автоматически на регулярной основе.

Удаление резервных копий

Для удаления ненужных резервных копий и их версий рекомендуется использовать средства программы Кибер Бэкап Старт. Дополнительные сведения см. в разделе *Удаление резервных копий и их версий*.

Кибер Бэкап Старт хранит сведения о резервных копиях в базе метаданных. Поэтому при удалении ненужных файлов резервных копий в проводнике Windows сведения об этих резервных копиях не

удаляются из базы данных. Это приведет к ошибкам, когда программа попытается выполнить операции с резервными копиями, которых больше не существует.

Разница между резервными копиями файлов и дисков и разделов

При резервном копировании файлов и папок сжимаются и сохраняются только файлы и дерево папок.

Резервные копии дисков и разделов отличаются от резервных копий файлов и папок. Кибер Бэкап Старт сохраняет точный моментальный снимок диска или раздела. Эта процедура называется созданием резервной копии диска.

Что содержится в резервной копии диска или раздела?

Резервная копия диска или раздела содержит все данные, хранящиеся на нем.

1. Нулевая дорожка жесткого диска с основной загрузочной записью (MBR) (только в резервных копиях MBR-дисков).
2. Один или несколько разделов, включая следующие.
    1. Загрузочный код.
    2. Метаданные файловой системы, включая служебные файлы, таблицу размещения файлов (FAT) и загрузочную запись раздела.
    3. Данные файловой системы, включая операционную систему (системные файлы, реестр, драйверы), данные пользователей и приложения.
3. Раздел «Зарезервировано системой», если есть.
4. Системный раздел EFI, если есть (только в резервных копиях GPT-дисков).

Что исключается из резервных копий дисков?

Чтобы уменьшить размер резервной копии и ускорить её создание, по умолчанию Кибер Бэкап Старт сохраняет только те сектора жесткого диска, в которых содержатся данные.

Кибер Бэкап Старт исключает из резервной копии диска следующие файлы:

- `pagefile.sys`
- `hiberfil.sys` (файл, в котором хранится содержимое ОЗУ при переходе компьютера в режим гибернации)

Этот метод по умолчанию можно изменить, включив посекторный режим. В этом случае Кибер Бэкап

Старт копирует все сектора жесткого диска, а не только те, которые содержат данные.

Кроме того, при резервном копировании системного раздела или диска в Кибер Облако Кибер Бэкап Старт исключает следующие данные:

- Папка Temp, обычное расположение:
  - `C:\Windows\Temp\`
  - `C:\Users\<username>\AppData\Local\Temp`
- Папка `System Volume Information` (обычное расположение — `C:\System Volume Information\`)
- Корзина
- Временные данные веб-браузера:
  - Временные файлы Интернета
  - Файлы cookie
  - Журнал
  - Кэш
- Файлы TIB и TIBX
- TMP-файлы
- Файлы с расширением .~

Полные, инкрементные и дифференциальные резервные копии

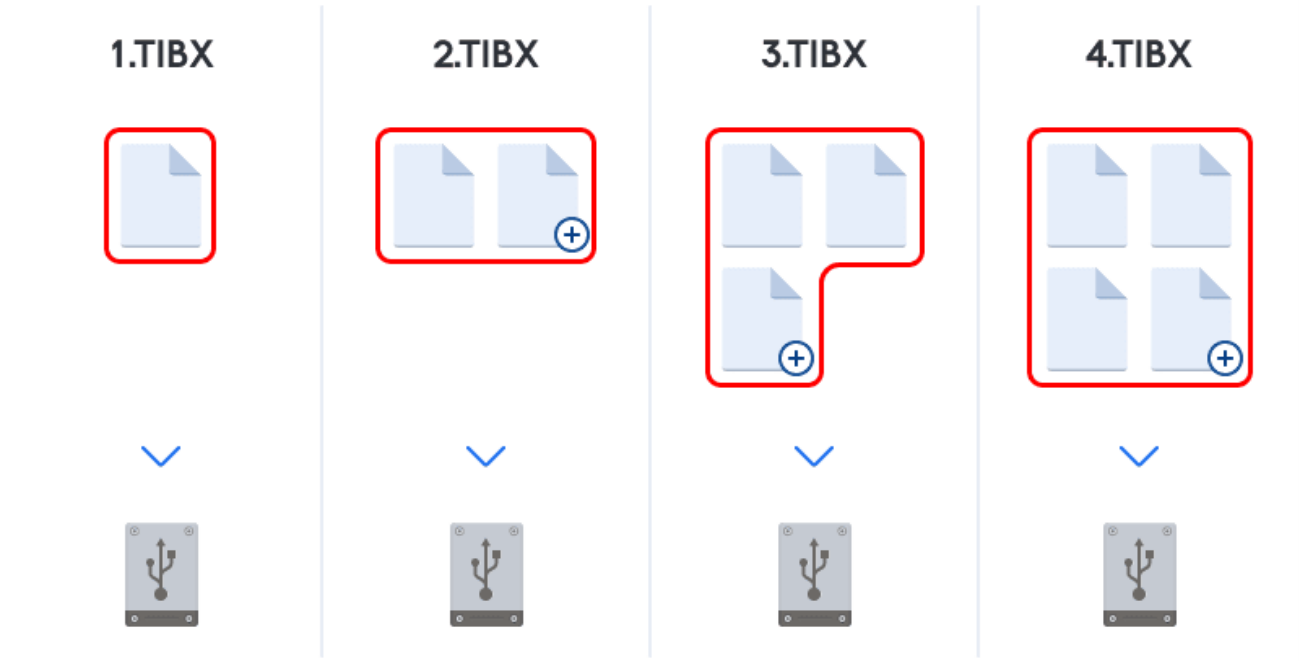
Кибер Бэкап Старт предлагает три метода резервного копирования: полное, инкрементное и дифференциальное.

Полное резервное копирование

Результат операции полного резервного копирования (называемый также полной версией резервной копии) содержит все данные, существовавшие на момент создания резервной копии.

Пример: каждый день вы пишете одну страницу документа и создаете резервную копию этого документа методом полного резервного копирования. Кибер Бэкап Старт сохраняет весь документ каждый раз, когда вы запускаете резервное копирование.

`1.tibx`, `2.tibx`, `3.tibx`, `4.tibx` — это файлы полных версий резервной копии.



Полная версия резервной копии образует основу для последующих инкрементных и дифференциальных резервных копий. Ее также можно использовать в качестве автономной резервной копии. Создание автономной полной резервной копии может быть оптимальным решением, если вы часто возвращаете систему в исходное состояние или не хотите управлять разными версиями резервных копий.

Восстановление: В приведенном выше примере, чтобы восстановить всю работу из файла `4.tibx`, нужна только одна версия резервной копии — `4.tibx`.

Инкрементное резервное копирование

Результат операции инкрементного резервного копирования (называемый также инкрементной версией резервной копии) содержит только те файлы, которые изменились с момента ПОСЛЕДНЕЙ ОПЕРАЦИИ РЕЗЕРВНОГО КОПИРОВАНИЯ.

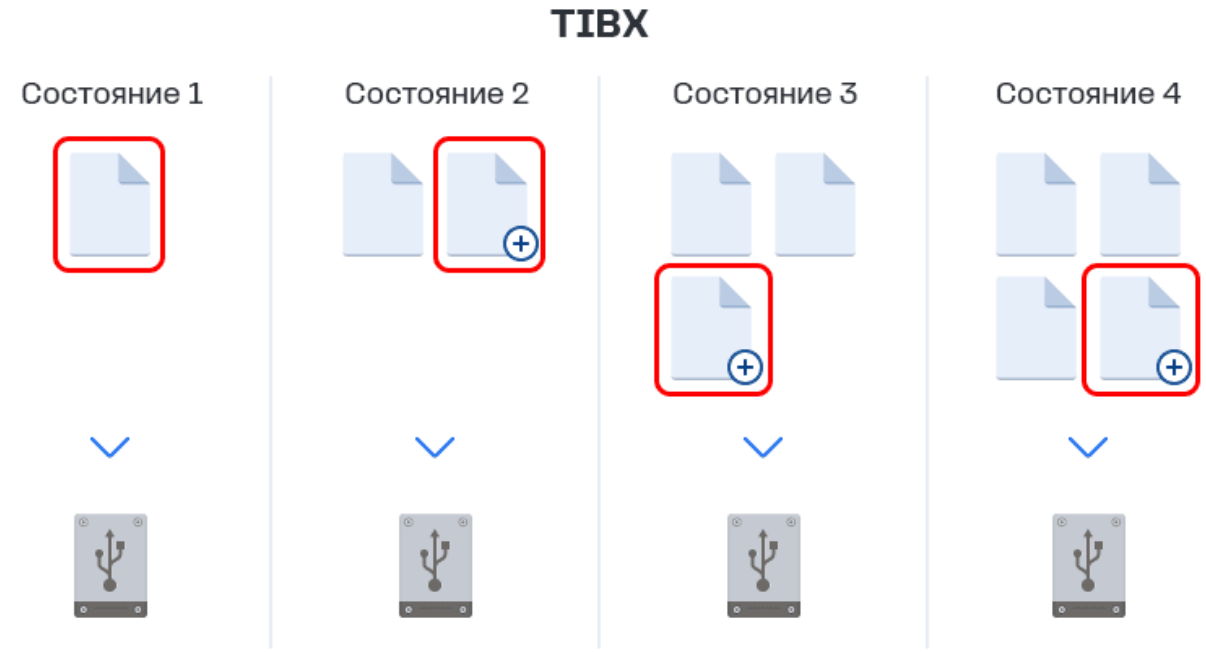
Пример: каждый день вы пишете одну страницу документа и создаете резервную копию методом инкрементного резервного копирования. Кибер Бэкап Старт сохраняет новую страницу каждый раз, когда вы запускаете резервное копирование.

Примечание

Сначала всегда создается полная версия резервной копии.

- `tibx` — это файл резервной копии, который содержит полную версию резервной копии, а также инкрементные версии резервной копии.

- Состояние 1 — это полная версия резервной копии.
- Состояние 2, Состояние 3 и Состояние 4 — это инкрементные версии резервной копии.



Инкрементные резервные копии наиболее полезны, если нужно часто создавать версии резервных копий и иметь возможность вернуться к состоянию на определенный момент времени. Как правило, инкрементные версии резервной копии существенно меньше полных или дифференциальных. С другой стороны, инкрементные версии резервной копии требуют больше работы от программы при восстановлении.

Восстановление: В приведенном выше примере, чтобы восстановить всю работу из файла tibx, нужны все версии резервной копии. При утере или повреждении инкрементной версии резервной копии все последующие инкрементные версии резервной копии оказываются бесполезными.

Дифференциальное резервное копирование

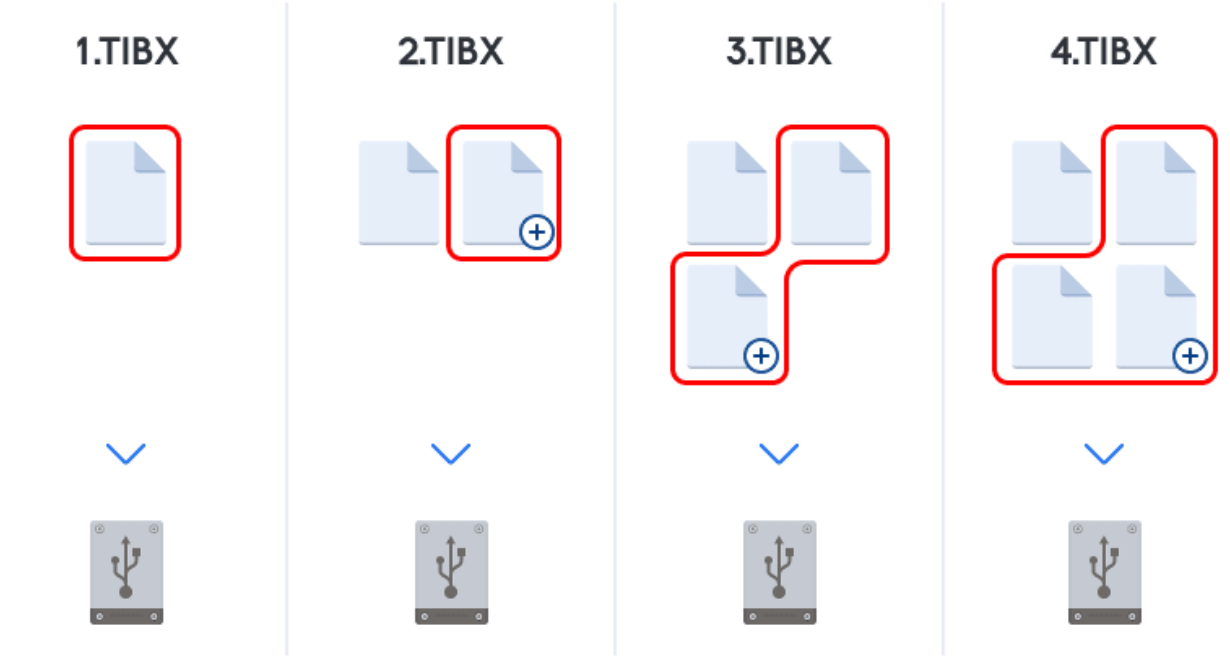
Результат операции дифференциального резервного копирования (называемый также дифференциальной версией резервной копии) содержит только те файлы, которые изменились с момента СОЗДАНИЯ ПОСЛЕДНЕЙ ПОЛНОЙ РЕЗЕРВНОЙ КОПИИ.

Пример: каждый день вы пишете одну страницу документа и создаете резервную копию методом дифференциального резервного копирования. Кибер Бэкап Старт сохраняет весь документ, кроме первой страницы, хранящейся в полной версии резервной копии.

Примечание

Сначала всегда создается полная версия резервной копии.

- `1.tibx` — это файл полной версии резервной копии.
- `2.tibx`, `3.tibx`, `4.tibx` — это файлы дифференциальных версий резервной копии.



Дифференциальный метод является промежуточным между двумя предыдущими. Он требует меньше времени и места для хранения по сравнению с полным методом, но больше по сравнению с инкрементным. Для восстановления данных из дифференциальной версии резервной копии Кибер Бэкап Старт требуется только дифференциальная версия и последняя полная версия. Поэтому восстановление из дифференциальной версии будет проще и надежней, чем из инкрементной.

Восстановление: В приведенном выше примере, чтобы восстановить всю работу из файла 4.tibx, нужны две версии резервной копии — 1.tibx и 4.tibx.

Чтобы выбрать метод резервного копирования, необходимо задать пользовательскую схему резервного копирования. Дополнительные сведения см. в разделе *Пользовательские схемы*.

Примечание

Инкрементная или дифференциальная резервная копия, созданная после дефрагментации диска, может иметь значительно больший размер, чем обычная. Это вызвано тем, что программа дефрагментации изменяет местоположение файлов на диске и эти изменения отражаются в резервной копии. Поэтому после дефрагментации диска рекомендуется заново создать полную резервную копию.

Changed Block Tracking (CBT)

Технология CBT ускоряет процесс резервного копирования при создании локальных инкрементных или дифференциальных версий резервных копий дисков. Изменения в содержимом диска непрерывно отслеживаются на уровне блоков. При запуске резервного копирования изменения могут быть сразу сохранены в резервной копии.

Выбор места хранения резервных копий

Кибер Бэкап Старт поддерживает большой набор устройств хранения (см. *Поддерживаемые носители данных*).

Хотя хранение резервных копий на локальном жестком диске является самым простым вариантом, мы рекомендуем хранить резервные копии в удаленном хранилище, так как это повышает безопасность данных.

Рекомендуемые хранилища:

1. **Кибер Облако**
2. **Внешний диск**

   Если вы планируете использовать внешний жесткий диск USB с настольным компьютером, рекомендуется подключить диск к заднему разъему с помощью короткого кабеля.
3. **Домашний файловый сервер, NAS или NDAS**

   Проверьте, обнаруживает ли Кибер Бэкап Старт выбранное хранилище резервных копий как в Windows, так и при загрузке с загрузочного носителя.

   Чтобы получить доступ к устройству хранения NDAS, в большинстве случаев потребуется указать идентификатор устройства NDAS (20 символов) и ключ записи (5 символов). Ключ записи позволяет использовать устройство NDAS в режиме записи (например, для сохранения резервных копий). Обычно идентификатор устройства и ключ записи напечатаны на наклейке, находящейся на нижней стороне устройства NDAS или внутри упаковки. Если наклейки нет, обратитесь к производителю устройства NDAS для получения этой информации.
4. **Сетевая папка**

   > **См. также**
   >
   > *Настройки проверки подлинности*.

5. **FTP-сервер**

См. также

FTP-подключение.

Подготовка нового диска к резервному копированию

Кибер Бэкап Старт может не распознать новый внутренний или внешний жесткий диск. В этом случае используйте средства операционной системы, чтобы установить для диска статус **Оперативный**, а затем инициализировать его.

Как изменить статус диска на оперативный:

1. Откройте **Управление дисками**. Для этого выберите **Панель управления** → **Система и безопасность** → **Администрирование**, запустите **Управление компьютером** и щелкните **Управление дисками**.
2. Найдите диск, помеченный как **Автономный**. Щелкните диск правой кнопкой мыши и выберите **Оперативный**.
3. Статус диска будет изменен на **Оперативный**. После этого вы сможете инициализировать диск.

Как инициализировать диск:

1. Откройте **Управление дисками**. Для этого выберите **Панель управления** → **Система и безопасность** → **Администрирование**, запустите **Управление компьютером** и щелкните **Управление дисками**.
2. Найдите диск, помеченный как **Не инициализирован**. Щелкните диск правой кнопкой мыши и выберите **Инициализировать диск**.
3. Выберите для диска таблицу разделов — MBR или GPT и нажмите кнопку **ОК**.
4. [Не обязательно] Чтобы создать том на диске, щелкните диск правой кнопкой мыши, выберите **Новый простой том** и следуйте указаниям мастера для настройки нового тома. Чтобы создать еще один том, повторите операцию.

FTP-подключение

Кибер Бэкап Старт позволяет сохранять резервные копии на FTP-серверах.

Чтобы создать новое FTP-подключение, при выборе хранилища резервных копий щелкните **Обзор**, откройте папку **Мои FTP-подключения** и выберите **Новое FTP-подключение**. В открывшемся окне укажите следующие данные.

- Путь к FTP-серверу, например: my.server.com
- Порт
- Имя пользователя

- Пароль

Для проверки настроек нажмите кнопку **Проверить подключение**. Компьютер попытается установить подключение к указанному FTP-серверу. Если при проверке удалось установить подключение, нажмите кнопку **Подключить**, чтобы добавить FTP-подключение.

Созданное FTP-подключение появится в дереве папок. Выберите подключение и перейдите к хранилищу резервных копий, которое следует использовать.

Примечание

- Простое открытие корневой папки FTP-сервера не открывает ваш домашний каталог.
- Для восстановления данных непосредственно с FTP-сервера резервная копия должна состоять из файлов размером не более 2 ГБ каждый. Поэтому при резервном копировании непосредственно на FTP-сервер Кибер Бэкап Старт разбивает резервную копию на файлы размером 2 ГБ. Если резервная копия сохраняется на жесткий диск с целью последующей передачи на FTP-сервер, можно разбить ее на файлы по 2 ГБ, установив нужный размер файла в параметрах резервного копирования.
- FTP-сервер должен поддерживать передачу файлов в пассивном режиме.

Настройки проверки подлинности

В большинстве случаев при подключении к удаленному компьютеру необходимо ввести учетные данные для доступа к общему сетевому ресурсу. Например, это возможно при выборе хранилища резервных копий. Окно **Настройки проверки подлинности** отображается автоматически при выборе сетевого имени компьютера.

При необходимости укажите имя пользователя и пароль, затем нажмите кнопку **Проверить подключение**. Если проверка прошла успешно, нажмите **Подключиться**.

Устранение неисправностей

При создании сетевого общего ресурса для использования в качестве хранилища резервных копий обеспечьте выполнение по крайней мере одного из следующих условий.

- Учетная запись Windows имеет пароль на компьютере, где находится общая папка.
- Защищенный паролем общий доступ выключен в Windows.

В противном случае подключиться к общей папке будет невозможно.

Присвоение имен файлам резервных копий

Имя файла резервной копии содержит только имя резервной копии и инкрементный номер. Оно не содержит дополнительной информации, такой как метод резервного копирования, номер цепочки резервных копий, номер версии резервной копии или номер тома.

Имя резервной копии может выглядеть следующим образом:

1. `my_documents.tibx`
2. `my_documents_0001.tibx`
3. `my_documents_0002.tibx`
4. `my_documents_0003.tibx`

Полные и дифференциальные резервные копии хранятся в отдельных файлах, а инкрементные резервные копии автоматически добавляются в файлы полных резервных копий, которым они соответствуют.

Интеграция с ОС Windows

В процессе установки Кибер Бэкап Старт устанавливает тесную интеграцию с операционной системой Windows. Такое слияние позволяет максимально расширить возможности компьютера.

Кибер Бэкап Старт интегрирует следующие компоненты:

- Элементы Кибер Бэкап Старт в меню **Пуск** Windows
- Команды контекстного меню

Меню «Пуск» Windows

В меню **Пуск** отображаются команды, инструменты и утилиты Кибер Бэкап Старт. Они предоставляют доступ к функциональным возможностям Кибер Бэкап Старт, не требуя запуска приложения.

Центр области уведомлений

Когда Кибер Бэкап Старт открыт, в нём можно просматривать статус любой операции. Но поскольку некоторые операции, такие как резервное копирование, могут занимать длительное время, нет необходимости держать открытой Кибер Бэкап Старт, чтобы узнать результат.

Центр области уведомлений содержит все последние уведомления в одном месте и позволяет в любой момент просматривать состояние важных операций, не открывая программы Кибер Бэкап Старт. В центре области уведомлений Кибер Бэкап Старт отображаются следующие уведомления: информация

о результатах операций резервного копирования и другие важные уведомления из программы Кибер Бэкап Старт. Центр области уведомлений сворачивается и скрывается под значком Кибер Бэкап Старт в области уведомлений.

Команды контекстного меню

Для доступа к командам контекстного меню откройте проводник, щелкните правой кнопкой мыши по выбранным элементам, наведите курсор на **Cyber Backup Start** и выберите нужную команду.

- Чтобы создать новую резервную копию файлов, щелкните **Новая резервная копия файлов**.
- Чтобы создать новую резервную копию дисков, щелкните **Новая резервная копия дисков**.
- Чтобы проверить резервную копию (файл TIBX), выберите **Проверить**.

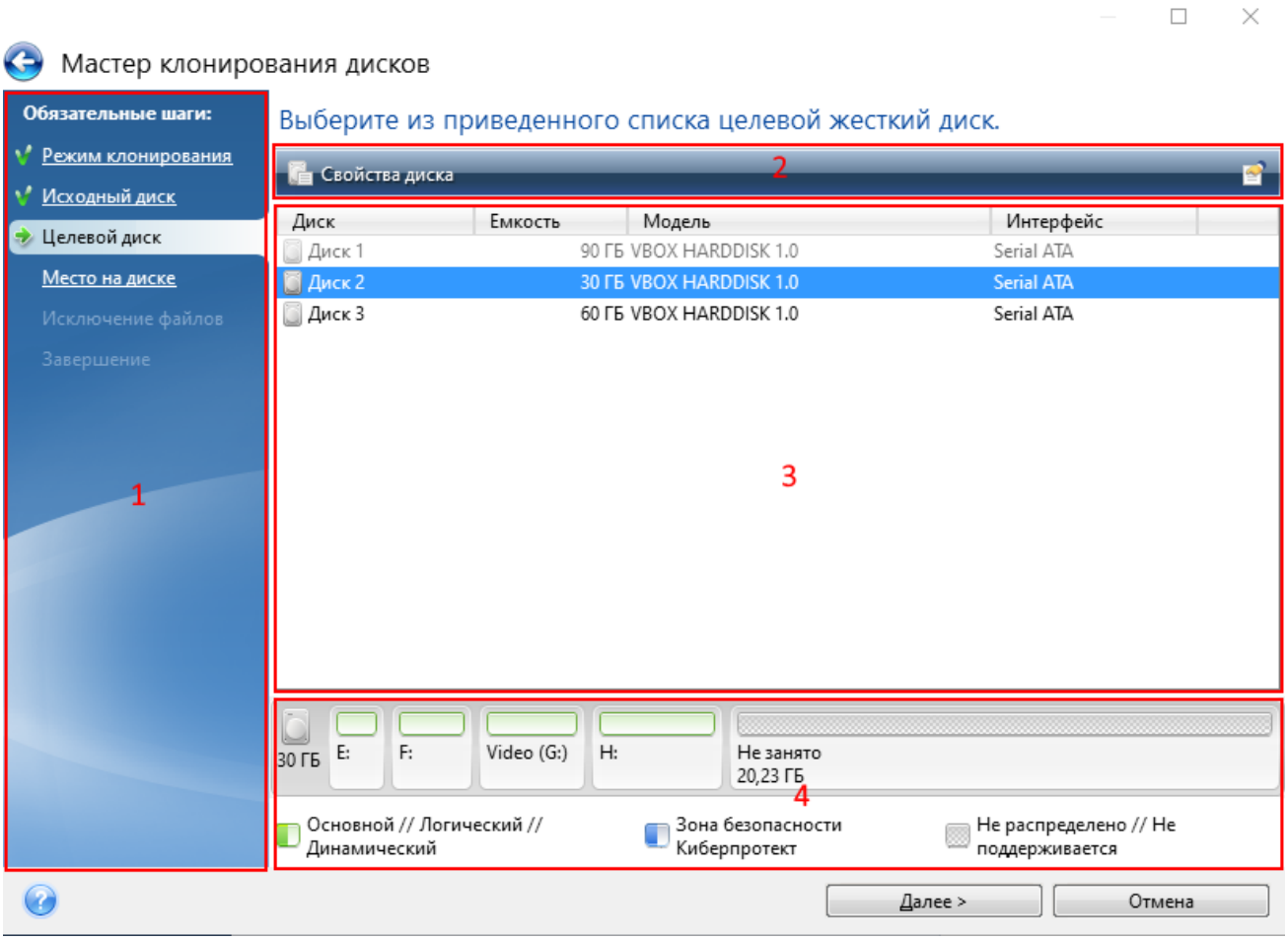
Восстановление файлов в проводнике

1. В проводнике дважды щелкните файл резервной копии (TIBX) с данными, которые необходимо восстановить.
2. Скопируйте или перетащите нужные файлы и папки в любое расположение на компьютере, как если бы они хранились на обычном диске.

Мастеры

При использовании инструментов и утилит, доступных в Кибер Бэкап Старт, часто применяются различные мастеры, помогающие выполнять операции.

Для примера см. снимок экрана ниже.



Окно мастера обычно содержит следующие области:

1. Это список шагов для завершения операции. Завершенные шаги отмечаются зелеными флажками. Зеленая стрелка указывает текущий шаг. После выполнения всех шагов программа отображает итоговое окно на последнем шаге **Завершение**. Проверьте сводку и нажмите кнопку **Приступить**, чтобы начать операцию.

2. На этой панели инструментов находятся кнопки для управления объектами, выбранными в области 3.

   Например:

   - **Сведения** — отображает окно с подробными сведениями о выбранной резервной копии.
   - **Свойства** — отображает окно свойств выбранного элемента.
   - **Создать новый раздел** — отображает окно, в котором можно настроить параметры нового раздела.
   - **Столбцы** — позволяет выбрать, какие столбцы таблицы и в каком порядке следует отображать.

3. Это главная область, в которой выбираются элементы и изменяются параметры.
4. В этой области отображается дополнительная информация об элементе, выбранном в области 3.

Вопросы и ответы по резервному копированию, восстановлению и клонированию

- **Системный раздел имеет размер 150 ГБ, но на этом разделе занято только 80 ГБ. Что будет включено в резервную копию?** По умолчанию Кибер Бэкап Старт копирует только те сектора жесткого диска, которые содержат данные, поэтому в резервную копию будет включено только 80 ГБ. При необходимости можно выбрать посекторный режим. Такой режим резервного копирования требуется только в особых случаях. Дополнительные сведения см. в разделе *Режим создания образа*. При резервном копировании в посекторном режиме программа копирует как используемые, так и неиспользуемые сектора жесткого диска, поэтому размер файла резервной копии, как правило, получается значительно больше.
- **Будут ли включены в резервную копию системного диска драйверы, документы, изображения и т. п.?** Да, такая резервная копия будет содержать драйверы, а также содержимое папки «Мои документы» и ее подпапок, если вы не меняли стандартного расположения этой папки. Если в компьютере только один жесткий диск, то такая резервная копия будет содержать всю операционную систему, приложения и данные.
- **Старый жесткий диск в моем ноутбуке почти заполнен. Был приобретен новый жесткий диск большей емкости. Как перенести на него систему Windows, программы и данные?** Можно либо клонировать старый жесткий диск на новый, либо сделать резервную копию старого диска и восстановить ее на новом. Выбор оптимального метода, как правило, зависит от структуры разделов на старом жестком диске.
- **Я хочу перенести старый системный жесткий диск на твердотельный накопитель. Можно ли это сделать?** Да, Кибер Бэкап Старт предоставляет такую функцию. Дополнительные сведения о процедуре см. в разделе *Перенос системы с жесткого диска на твердотельный накопитель*.
- **Какой метод переноса системы на новый диск лучше: клонирование или резервное копирование и восстановление?** Метод резервного копирования и восстановления дает больше гибкости. В любом случае настоятельно рекомендуется сделать резервную копию старого жесткого диска, даже если вы выберете метод клонирования. Это может сохранить данные в случае, если что-либо произойдет с исходным жестким диском во время клонирования. Например, были случаи, когда пользователи выбирали не тот диск в качестве целевого и таким образом уничтожали все данные на системном диске. Кроме того, еще одна резервная копия может использоваться для создания избыточности и повышения безопасности.

- **Какую резервную копию следует создавать: раздела или всего диска?** В большинстве случаев лучше создать резервную копию всего диска. Однако в некоторых случаях рекомендуется резервное копирование раздела. Например, у вашего ноутбука один жесткий диск с двумя разделами: системным разделом (буква диска C) и разделом данных (буква диска D). В системном разделе хранятся рабочие документы в папке **Мои документы** и ее подпапках. В разделе данных хранятся видеофайлы, изображения и музыка. Если вы хотите выполнить резервное копирование только системного раздела, нет необходимости создавать резервную копию всего диска. В этом случае будет достаточно резервной копии системного раздела. Также, если вы хотите выполнить резервное копирование только своих данных (без системных файлов), можно создать резервную копию файлов. Однако рекомендуется сделать как минимум одну резервную копию целого диска, если позволяет емкость хранилища резервных копий.
- **Есть ли поддержка RAID-массивов?** Кибер Бэкап Старт поддерживает аппаратные RAID-массивы всех распространенных типов. Также поддерживаются конфигурации с программными RAID-массивами на динамических дисках. Загрузочный носитель поддерживает большинство распространенных аппаратных контроллеров RAID. Если стандартный загрузочный носитель не распознает RAID-массив как единый том, на носителе нет соответствующих драйверов. В этом случае можно создать загрузочный носитель на основе WinPE и добавить на него нужные драйверы (в расширенном режиме).
- **Что делать, если устройство NAS не определяется при загрузке с загрузочного носителя?** В случае если устройство NAS работает через протокол Bonjour, то в загрузочных носителях на основе Linux или WinPE устройство NAS не определяется. Чтобы устройство NAS определилось в загрузочном носителе на основе WinPE, переключите устройство NAS на протокол UPnP. Если такой возможности нет или загрузочный носитель на основе Linux, обратитесь к устройству NAS как к обычной сетевой папке. В процессе подключения к устройству NAS может потребоваться ввод учетных данных.

Резервное копирование данных

Резервное копирование дисков и разделов

В отличие от резервных копий файлов резервные копии дисков и разделов содержат все данные, хранящиеся на них. Этот тип резервного копирования обычно используется для создания точной копии системного раздела или всего системного диска. Такая резервная копия позволяет восстановить систему, если Windows работает неправильно или не запускается.

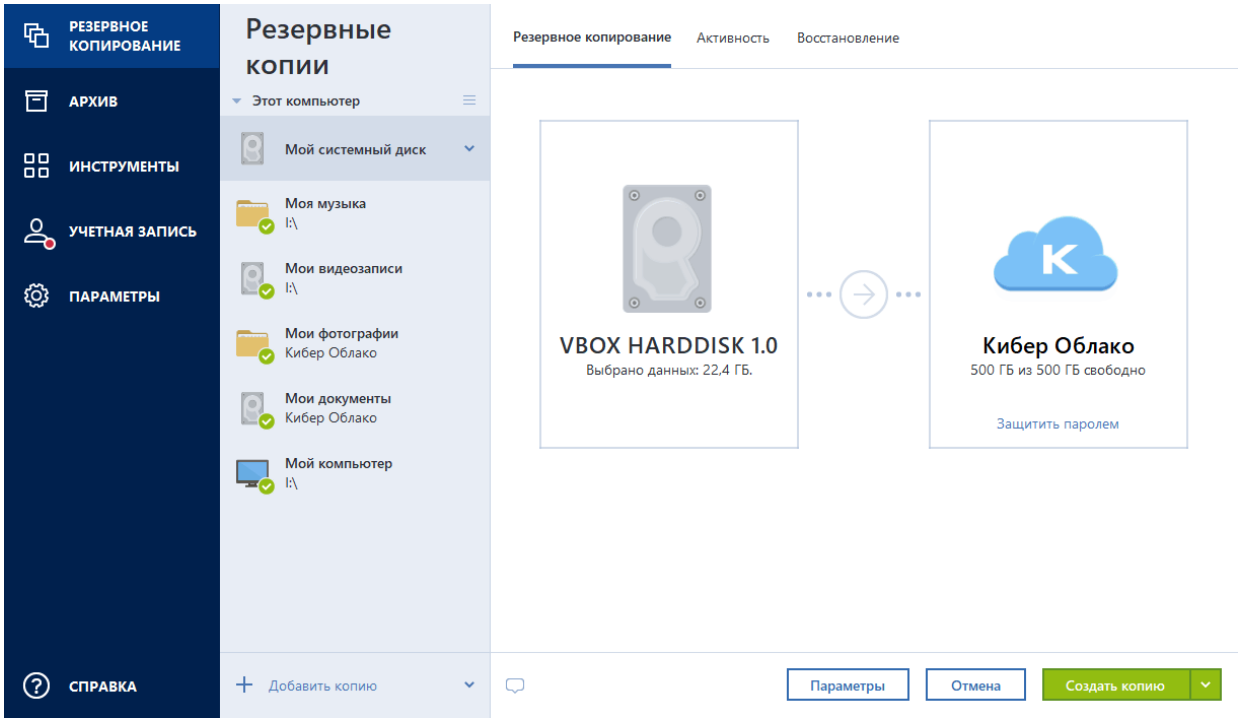
> **Примечание**
>
> Не используйте загрузочные носители на основе ОС Linux, если у вас в системе есть разделы с файловой системой ExFAT или необходимо сделать резервную копию такого раздела. Также см. ограничения в разделе *Восстановление дисков и разделов*.

Как выполнить резервное копирование разделов или дисков:

1. Запустите Кибер Бэкап Старт.
2. На боковой панели нажмите **Резервное копирование**.
3. Щелкните **Добавить копию**.
4. [Необязательно] Чтобы переименовать резервную копию, щелкните стрелку рядом с именем резервной копии, выберите **Переименовать** и введите новое имя.
5. Щелкните область **Изменить источник** и выберите **Диски и разделы**.
6. В открывшемся окне установите флажки напротив нужных разделов и дисков и нажмите кнопку **ОК**.

   Чтобы просмотреть скрытые разделы, щелкните **Полный список разделов**.

   > **Примечание**
   >
   > Для резервного копирования динамических дисков можно использовать только режим раздела.



7. Щелкните область **Выбор хранилища** и выберите место для сохранения резервной копии.

   - **Кибер Облако** — войдите в свою учетную запись и нажмите кнопку **ОК**.
   - **Внешний диск** — если к компьютеру подключен внешний диск, его можно выбрать из списка.
   - **NAS** — выберите устройство NAS из списка обнаруженных устройств NAS. Если устройство NAS всего одно, Кибер Бэкап Старт по умолчанию предложит его как место хранения резервных копий.
   - **Обзор** — выберите место назначения в дереве папок.

   Примечание

   По возможности избегайте хранения резервных копий системных разделов на динамических дисках, так как восстановление системного раздела происходит в среде Linux. Linux и Windows по-разному работают с динамическими дисками. Это может вызвать проблемы при восстановлении.

8. [Необязательно] Выберите **Параметры**, чтобы задать параметры резервного копирования. Дополнительные сведения см. в разделе *Параметры резервного копирования*.

9. [Необязательно] Щелкните значок **Добавить комментарий** и введите комментарий к версии резервной копии. Комментарии к резервной копии помогут найти нужную версию позже при восстановлении данных.

10. Выполните одно из следующих действий.
    - Чтобы немедленно выполнить резервное копирование, щелкните **Создать копию**.
    - Чтобы выполнить резервное копирование позже или по расписанию, щелкните стрелку справа от кнопки **Создать копию**, а затем щелкните **Позже**.

Примечание

- При резервном копировании данных в Кибер Облако создание первой резервной копии может занять длительное время. Последующие операции резервного копирования должны происходить намного быстрее, так как через Интернет будут передаваться только изменения в файлах.
- После запуска резервного копирования в онлайн-хранилище можно закрыть программу Кибер Бэкап Старт. Процесс резервного копирования продолжится в фоновом режиме. Если приостановить резервное копирование, выключить компьютер или разорвать подключение к Интернету, то резервное копирование возобновится после нажатия «Создать копию» или после того, как будет восстановлено подключение к Интернету. Прерывание резервного копирования не приведет к передаче ваших данных дважды.

Резервное копирование файлов и папок

Чтобы защитить документы, фотографии, музыкальные и видеофайлы, нет необходимости выполнять резервное копирование всего раздела, содержащего эти файлы. Можно создать резервные копии определенных файлов и папок.

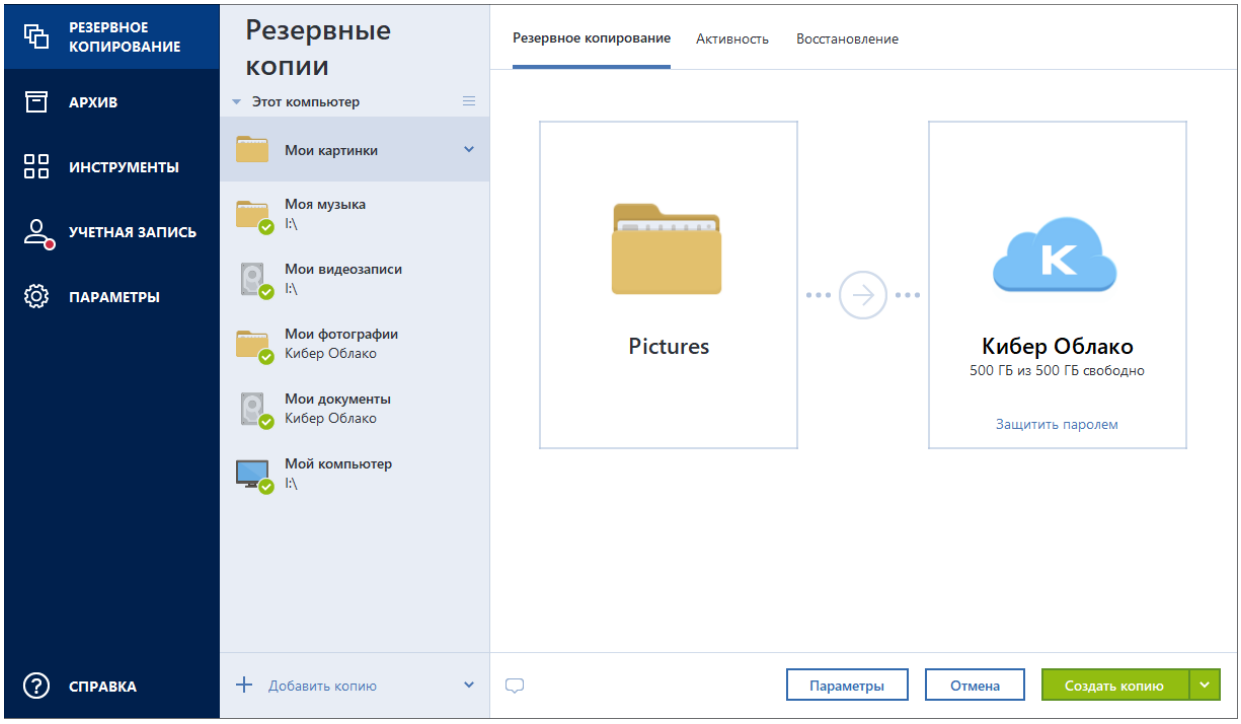
Важно

Перед резервным копированием файлов не создается моментальный снимок. Из-за этого в резервной копии не сохраняются файлы, занятые системой или открытые в приложениях. Так, например, не получится создать резервную копию файлов в системных папках. Поэтому перед резервным копированием файлов убедитесь, что они не заняты системой и не открыты в приложениях.

Как выполнить резервное копирование файлов и папок:

1. Запустите Кибер Бэкап Старт.
2. На боковой панели нажмите **Резервное копирование**.
3. Щелкните **Добавить копию**.

4. [Необязательно] Чтобы переименовать резервную копию, щелкните стрелку рядом с именем резервной копии, выберите **Переименовать** и введите новое имя.
5. Щелкните область **Изменить источник** и выберите **Файлы и папки**.
6. В открывшемся окне установите флажки напротив нужных файлов и папок и нажмите кнопку **ОК**.



7. Щелкните область **Выбор хранилища** и выберите место для сохранения резервной копии.
   - **Внешний диск** — если к компьютеру подключен внешний диск, его можно выбрать из списка.
   - **NAS** — выберите устройство NAS из списка обнаруженных устройств NAS. Если устройство NAS всего одно, Кибер Бэкап Старт по умолчанию предложит его как место хранения резервных копий.
   - **Обзор** — выберите место назначения в дереве папок.
8. [Необязательно] Выберите **Параметры**, чтобы задать параметры резервного копирования. Дополнительные сведения см. в разделе *Параметры резервного копирования*.
9. [Необязательно] Щелкните значок **Добавить комментарий** и введите комментарий к версии резервной копии. Комментарии к резервной копии помогут найти нужную версию позже при восстановлении данных.
10. Выполните одно из следующих действий.
    - Чтобы немедленно выполнить резервное копирование, щелкните **Создать копию**.
    - Чтобы выполнить резервное копирование позже или по расписанию, щелкните стрелку вниз

справа от кнопки **Создать копию**, а затем щелкните **Позже**.

Примечание

При резервном копировании данных в Кибер Облако создание первой резервной копии может занять длительное время. Последующие операции резервного копирования должны происходить намного быстрее, так как через Интернет будут передаваться только изменения в файлах.

Резервное копирование мобильных устройств

Резервная копия мобильного устройства позволяет защитить и восстановить данные на мобильном устройстве в случае их повреждения или потери. С помощью резервной копии можно также перенести личные данные со старого мобильного устройства на новое.

Чтобы создать резервную копию мобильных данных на ПК, выполните следующие шаги в Кибер Бэкап Старт на ПК, а также в мобильном приложении:

1. Убедитесь, что исходное мобильное устройство и целевой ПК подключены к одной и той же сети Wi-Fi.
2. На ПК запустите Кибер Бэкап Старт и выполните следующие шаги:
    1. На боковой панели нажмите **Резервное копирование**.
    2. Щёлкните **Добавить резервную копию**.
    3. Наведите курсор мыши на имя ПК. Когда оно сменится на **Источник резервной копии**, нажмите на него.
    4. В окне **Источник резервной копии** щёлкните **Мобильное устройство**. Появится QR-код.

       Не закрывайте это окно.
3. На мобильном устройстве откройте приложение и выполните следующие шаги:
    1. Нажмите **НАСТРОЙКА** для создания первой резервной копии или **+** для создания новой резервной копии.
    2. Выберите ПК в качестве места назначения резервной копии.
    3. Нажмите **Сканировать QR-код**, отсканируйте QR-код на экране ПК и дождитесь, пока мобильное устройство подключится к компьютеру.
    4. Выберите категории данных, которые будут скопированы или пропустите этот шаг, чтобы создать резервную копию всех данных.

5. Если требуется автоматически выполнять резервное копирование изменений данных (например, новых фотографий), включите параметр **Непрерывное резервное копирование**. Если он отключен, новые данные будут копироваться только при нажатии **СОЗДАТЬ РЕЗЕРВНУЮ КОПИЮ**.
6. [Необязательно] Включите включите шифрование резервной копии. В этом случае:
    1. Введите пароль шифрования.
    2. [Необязательно] Снимите флажок **Сохранить пароль**. В этом случае пароль придется вводить при каждом доступе к резервной копии.
    3. Нажмите кнопку **ШИФРОВАТЬ**.
7. Нажмите **СОЗДАТЬ РЕЗЕРВНУЮ КОПИЮ**.
8. Разрешите мобильному приложению доступ к данным, резервная копия которых создается.

После запуска резервного копирования отслеживать его ход можно как в мобильном приложении, так и на ПК. Предупреждения и сообщения об ошибках будут отображаться только в мобильном приложении.

После завершения резервного копирования данные будут загружены на компьютер.

Изменение места хранения резервных копий мобильных устройств на ПК

По умолчанию резервные копии мобильных устройств хранятся в папке `C:\ProgramData\Acronis Mobile Backup Data\acronis-local-data\`. Чтобы изменить расположение по умолчанию:

1. На вкладке **Настройки** найдите параметр **Хранилище резервных копий мобильных устройств**.
2. Щёлкните **Изменить** → **Выбрать хранилище** и выберите новое расположение для резервных копий. Можно выбрать расположение только на внутренних жестких дисках.

Чтобы вернуть исходное расположение, нажмите **Восстановить значения по умолчанию** на вкладке **Настройки**.

После изменения хранилища папка `acronis-local-data` будет перемещена в выбранное расположение. На время этой операции текущие задания резервного копирования мобильных устройств будут приостановлены и возобновлены после её завершения. Все новые резервные копии мобильного устройства будут сохраняться в новом расположении.

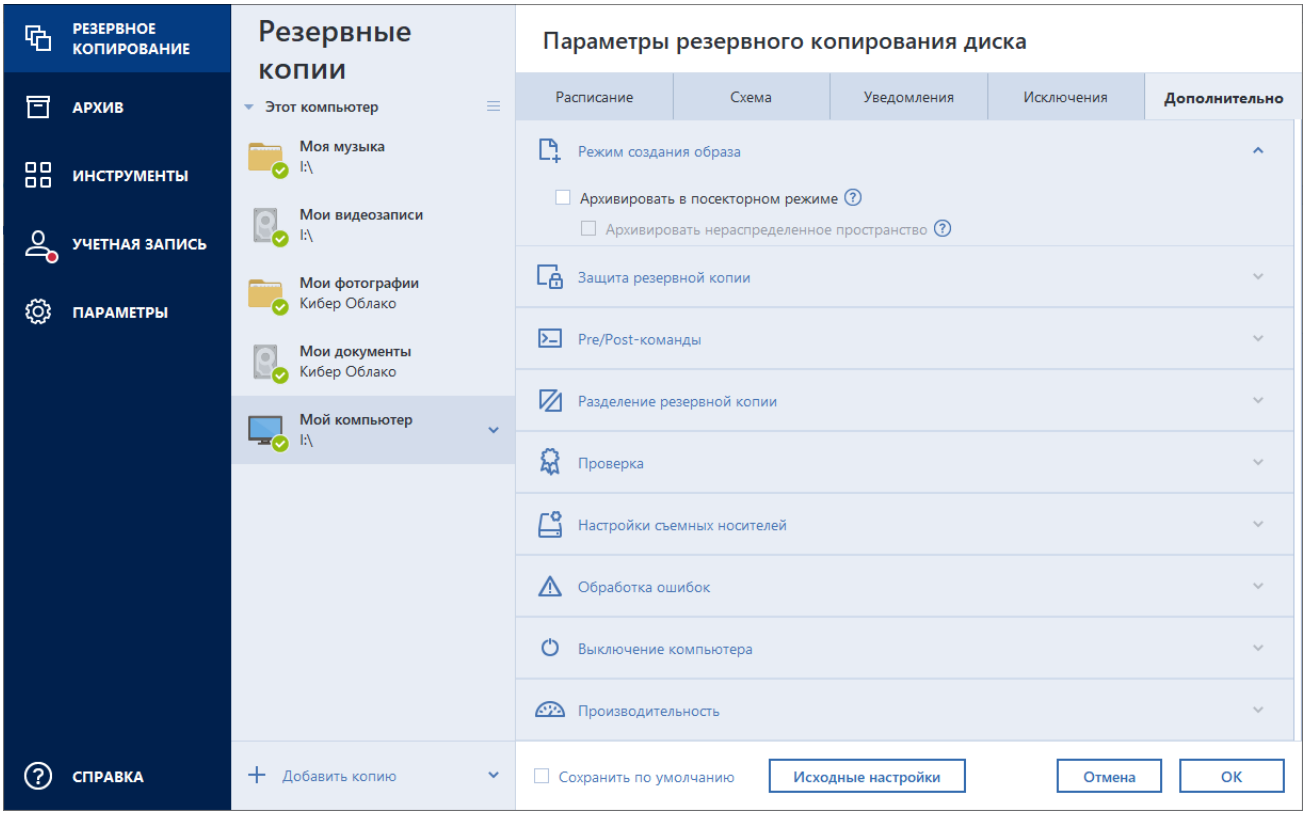
> **Примечание**
>
> Резервные копии мобильных устройств всегда хранятся в одной папке и не могут быть разделены.

Параметры резервного копирования

При создании резервной копии можно изменить дополнительные параметры и настроить процесс резервного копирования. Чтобы открыть окно параметров, выберите источник и место назначения для резервной копии, затем нажмите **Параметры**.

Следует учитывать, что параметры для каждого типа резервного копирования (на уровне дисков, на уровне файлов, в онлайн-хранилище) являются полностью независимыми и их следует настраивать отдельно.

После установки приложения все параметры будут установлены в начальные значения. Параметры можно изменить только на время выполнения текущей операции резервного копирования или для всех последующих операций. Установите флажок **Сохранить по умолчанию**, чтобы применить измененные настройки ко всем последующим операциям резервного копирования.

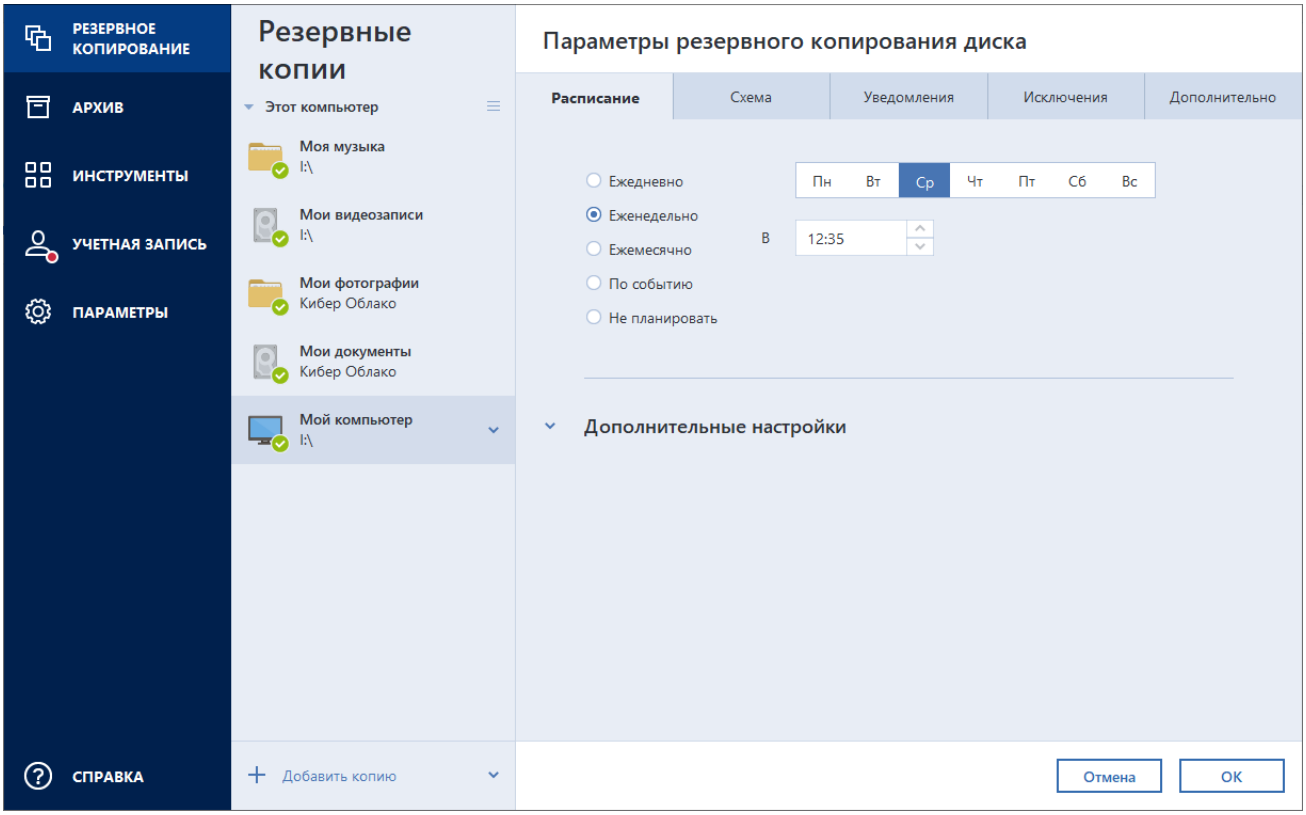


Чтобы вернуть все измененные параметры в исходные значения, заданные после установки продукта, нажмите кнопку **Исходные настройки**. Обратите внимание, что это приведет к сбросу параметров только для текущего резервного копирования. Чтобы сбросить параметры для будущих операций резервного копирования, щелкните **Исходные настройки**, установите флажок **Сохранить по умолчанию** и нажмите кнопку **ОК**.

Планирование

Расположение: **Параметры** → **Расписание**

На вкладке **Расписание** можно указать настройки планирования резервного копирования и проверки.



Можно задать расписание для регулярного создания или проверки резервных копий.

- **Ежедневно** (см. *Параметры ежедневного резервного копирования*) — операция будет выполняться один раз в день или чаще.
- **Еженедельно** (см. *Параметры еженедельного резервного копирования*) — операция будет выполняться один или несколько раз в неделю по выбранным дням.
- **Ежемесячно** (см. *Параметры ежемесячного резервного копирования*) — операция будет выполняться один или несколько раз в месяц по выбранным числам.
- **По событию** (см. *Настройка параметров запуска по событию*) — операция будет выполнена при наступлении события.
- **Не планировать** — для текущей операции планировщик будет отключен. В этом случае резервное копирование или проверка будут запущены только при нажатии кнопки **Создать копию** или выборе элемента меню операций резервного копирования **Проверить последнюю версию** или **Проверить все версии**.

Дополнительные настройки

Нажмите **Дополнительные настройки**, чтобы задать следующие дополнительные настройки резервного копирования и проверки:

- **Копировать, только если компьютер заблокирован или запущена экранная заставка** — установите этот флажок, чтобы отложить выполнение запланированной операции до того времени, когда компьютер не будет использоваться (будет отображаться заставка, или компьютер будет заблокирован). Для расписания проверки этот параметр будет называться **Запускать проверку только при простое компьютера**.
- **Предотвращать переход компьютера в спящий режим/гибернацию** — установите этот флажок, чтобы резервное копирование, занимающее длительное время, не прерывалось переходом компьютера в режим сна или гибернации.
- **Пробуждать компьютер из спящего режима/гибернации** — установите этот флажок, чтобы компьютер выходил из спящего режима или гибернации для выполнения запланированной операции.
- **Выполнять пропущенные операции при запуске системы с задержкой (в минутах)** — установите этот флажок, чтобы пропущенные операции принудительно выполнялись при следующем запуске системы, если в запланированное время компьютер был выключен.

  Кроме того, можно задать время задержки, чтобы резервное копирование начиналось через определенное время после запуска системы. Например, чтобы начать резервное копирование через 20 минут после запуска системы, введите *20* в соответствующее поле.
- **Выполнять пропущенные операции после подключения внешнего устройства** [необязательно, при планировании резервного копирования на флеш-накопитель USB или проверки резервной копии, расположенной на флеш-накопителе USB] — установите этот флажок, чтобы пропущенные операции выполнялись при подключении флеш-накопителя USB, если в запланированное время он был отключен.

Параметры ежедневного резервного копирования

Можно настроить следующие параметры для резервных копий, создаваемых или проверяемых ежедневно.

- **Каждые** — выберите ежедневную периодичность из раскрывающегося списка (например, каждые 2 часа).
- **Один раз в день** — операция запускается один раз в день в указанное время.
- **Два раза в день** — операция запускается два раза в день. Выберите время для каждой из двух операций.

Описание **Дополнительных настроек** см. в разделе *Планирование*.

Параметры еженедельного резервного копирования

Можно настроить следующие параметры для резервных копий, создаваемых или проверяемых еженедельно.

- **Дни недели** — выберите дни для запуска операции.
- **В** — задайте время запуска операции.

Описание **Дополнительных настроек** см. в разделе *Планирование*.

Параметры ежемесячного резервного копирования

Можно настроить следующие параметры для резервных копий, создаваемых или проверяемых ежемесячно.

- **Каждые** — выберите номер и день недели из раскрывающегося списка. Например, выберите **Каждый первый понедельник** для запуска операции в первый понедельник каждого месяца.
- **В выбранные дни месяца** — укажите даты для резервного копирования. Например, можно запланировать запуск операции на 10-е число и последний день месяца.
- **В** — задайте время запуска операции.

Описание дополнительных настроек см. в разделе *Планирование*.

Настройка параметров запуска по событию

Можно настроить следующие параметры для резервных копий, создаваемых или проверяемых при определенном событии.

- **Только один раз в день** — установите этот флажок, чтобы операция запускалась только при первом наступлении указанного события в текущий день.
- Укажите событие, при наступлении которого будет выполняться создание или проверка резервной копии.
    - **После подключения внешнего устройства** — операция будет запускаться каждый раз при подключении к компьютеру внешнего устройства (флеш-накопителя USB или внешнего жесткого диска), которое ранее использовалось в качестве места назначения резервной копии. Обратите внимание, что ОС Windows должна распознать устройство как внешнее.
    - **Входе пользователя** — операция будет запускаться каждый раз, когда текущий пользователь выполняет вход в ОС.

- **Выходе пользователя** — операция будет запускаться каждый раз, когда текущий пользователь выходит из ОС.
- **Завершение работы или перезагрузка системы** — операция будет запускаться каждый раз при выключении или перезагрузке компьютера.
- **Запуск системы с задержкой (в минутах)** — операция будет запускаться с указанным временем задержки при каждом запуске ОС.

Описание дополнительных настроек см. в разделе *Планирование*.

Схемы резервного копирования

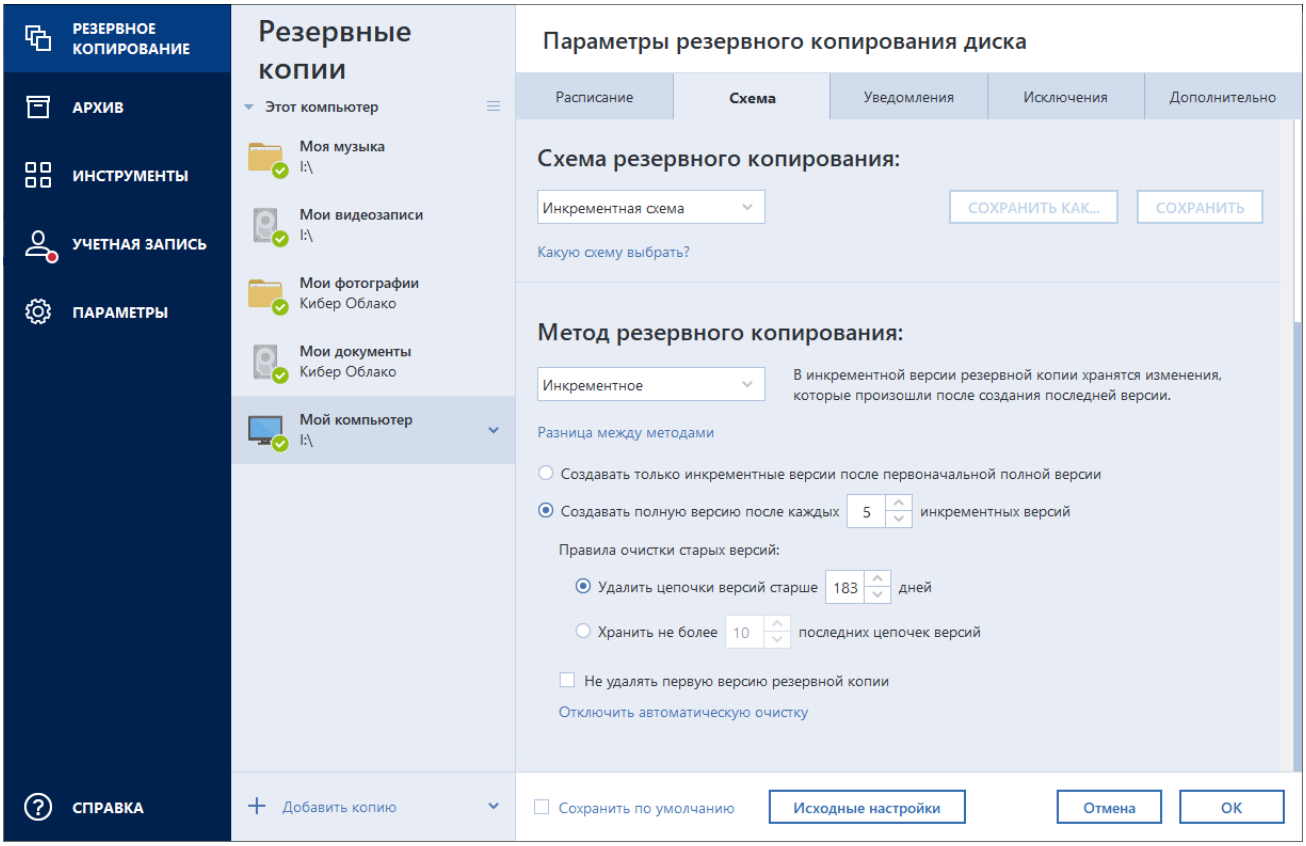
Расположение: **Параметры** → **Схема**

Сочетание схем резервного копирования и планировщика помогает создать собственную стратегию резервного копирования. Применение схем резервного копирования оптимизирует использование пространства хранилища резервных копий, повышает надежность хранения данных и автоматически удаляет устаревшие версии резервной копии.

> **Примечание**
>
> Для резервных копий в онлайн-хранилище схема резервного копирования установлена по умолчанию и не может быть изменена. После создания первой полной резервной копии создаются только инкрементные версии.

Схема резервного копирования определяет следующие параметры:

- *Методы резервного копирования*, используемые при создании версий резервной копии (полное, дифференциальное или инкрементное).
- Последовательность версий резервной копии, созданных с использованием различных методов.
- Правила удаления версий.



Схемы резервного копирования, доступные в Кибер Бэкап Старт:

- **Схема с одной версией** (см. *Схема с одной версией*) — позволяет использовать хранилище резервных копий минимального размера.
- **Схема с цепочкой версий** (см. *Схема с цепочкой версий*) — оптимальная схема для многих случаев.
- **Инкрементная схема** — выберите для создания полной версии через каждые пять инкрементных версий. Эта схема установлена по умолчанию.
- **Дифференциальная схема** — выберите для создания только дифференциальных резервных копий после начальной полной резервной копии.
- **Пользовательская схема** (см. *Пользовательские схемы*) — выберите, чтобы настроить схему резервного копирования вручную.

Можно легко изменить схему резервного копирования для существующей резервной копии. Это не повлияет на целостность цепочек резервных копий, поэтому можно будет восстановить свои данные с любой предыдущей версии резервной копии.

Схема с одной версией

Эта схема аналогична резервному копированию дисков и файлов (за исключением параметров планировщика).

Программа создает полную версию резервной копии и перезаписывает ее каждый раз по расписанию или при запуске резервного копирования вручную. В этом процессе старая версия удаляется только после создания новой.

> **Примечание**
>
> Самый первый файл останется для вспомогательных целей, но в нем не будет ваших данных. Не удаляйте его!

Параметры планировщика для резервного копирования дисков: ежемесячно.

Параметры планировщика для резервного копирования файлов: ежедневно.

Результат: одна актуальная полная версия резервной копии.

Требуемое дисковое пространство: минимальное.

Схема с цепочкой версий

У этой схемы есть различия при резервном копировании дисков и файлов.

Цепочка версий резервных копий дисков

Сначала программа создает первую полную версию резервной копии. Эта версия хранится до тех пор, пока не будет удалена вручную. После этого по заданному расписанию (или при резервном копировании вручную) программа создает 1 полную версию и 5 дифференциальных версий резервной копии, затем снова 1 полную версию и 5 дифференциальных версий резервной копии и т. д. Версии хранятся в течение 6 месяцев. По истечении этого срока программа проверяет, можно ли удалить старые версии резервной копии (за исключением первой полной версии). Все зависит от минимального количества версий (восемь) и согласованности цепочек версий. Программа удаляет самые старые версии по одной после создания новых версий тем же самым методом (например, самая старая дифференциальная версия будет удалена только после создания самой новой дифференциальной версии). При этом сначала удаляются самые старые дифференциальные версии, а затем самая старая полная версия.

Параметры планировщика резервного копирования: ежемесячно.

Результат: у вас будут ежемесячные версии резервной копии за последние 6 месяцев плюс исходная полная версия резервной копии, которая может храниться в течение более продолжительного периода.

Требуемое дисковое пространство: зависит от количества версий и их размеров.

Цепочка версий резервных копий файлов

Согласно заданному расписанию (или при выполнении резервного копирования вручную) программа создает 1 полную версию и 6 инкрементных версий резервной копии, затем снова 1 полную версию и 6 инкрементных версий резервной копии и так далее. Версии хранятся в течение 1 месяца. По истечении этого срока программа проверяет, можно ли удалить самые старые версии резервной копии. Все зависит от согласованности цепочки версий резервных копий. Для поддержания согласованности после создания очередной аналогичной цепочки версий программа удаляет самые старые версии по цепочкам «1 полная + 6 инкрементных версий».

Параметры планировщика резервного копирования: ежедневно.

Результат: в наличии версии резервной копии за каждый день прошедшего месяца.

Требуемое дисковое пространство: зависит от количества версий и их размеров.

Пользовательские схемы

Кибер Бэкап Старт позволяет создавать собственные схемы резервного копирования. За основу можно взять готовые схемы резервного копирования. Внесите необходимые изменения в выбранную готовую схему и сохраните измененную схему как новую.

> **Примечание**
>
> Существующие предустановленные схемы резервного копирования перезаписать нельзя.

Также можно создавать пользовательские схемы резервного копирования с нуля, на основе версий полных, дифференциальных или инкрементных резервных копий.

Для начала в соответствующем поле необходимо выбрать метод резервного копирования.

- *Полное*

  При выборе этого метода создаются только полные резервные копии.

- *Инкрементное*

  Будут созданы цепочки версий резервной копии с одной полной версией и несколькими инкрементными.

  Настройте параметры схемы резервного копирования:

  - **Создавать только инкрементные версии после первоначальной полной версии** — будет создана только одна цепочка версий резервной копии. В этом случае автоматическая очистка будет недоступна.

- **Создавать полную версию после каждых [n] инкрементных версий** — будут созданы несколько цепочек версий резервной копии. Этот вариант более надежный, но для его реализации требуется больше дискового пространства.

- *Дифференциальное*

  Будут созданы цепочки версий резервной копии с одной полной версией и несколькими дифференциальными.

  Настройте параметры схемы резервного копирования:

  - **Создавать только дифференциальные версии после первоначальной полной версии** — будет создана только одна цепочка версий резервной копии. В этом случае автоматическая очистка будет недоступна.
  - **Создавать полную версию после каждых [n] дифференциальных версий** — будут созданы несколько цепочек версий резервной копии. Этот вариант более надежный, но для его реализации требуется больше дискового пространства.

Включить автоматическую очистку:

- **Правила очистки старых версий** — чтобы устаревшие версии удалялись автоматически, настройте одно из следующих правил.
  - **Удалять версии, с момента создания которых прошло более [n] дней** [только при использовании метода полного резервного копирования] — этот параметр ограничивает срок хранения версий резервной копии. Все версии старше указанного срока автоматически удаляются.
  - **Хранить не более [n] последних версий** [только при использовании метода полного резервного копирования] — этот параметр ограничивает максимальное количество хранимых версий резервной копии. Когда количество версий резервной копии превысит заданное значение, самая старая версия будет автоматически удалена.
  - **Удалять цепочки версий старше [n] дней** [только при инкрементном и дифференциальном резервном копировании] — этот параметр ограничивает срок хранения цепочек версий резервной копии. Самая старая цепочка версий удаляется только когда последняя версия резервной копии в этой цепочке будет старше указанного срока.
  - **Хранить не более [n] последних цепочек версий** [при инкрементном и дифференциальном резервном копировании] — этот параметр ограничивает максимальное количество хранимых цепочек версий резервной копии. Когда количество цепочек версий резервной копии превысит заданное значение, самая старая цепочка будет автоматически удалена.
- **Не удалять первую версию резервной копии** — установите этот флажок, чтобы сохранить первоначальное состояние данных. Программа создаст две первоначальные полные версии

резервной копии. Первая версия не будет подлежать автоматическому удалению и будет храниться до ее удаления вручную. При выборе инкрементного или дифференциального метода первая цепочка резервной копии будет начинаться со второй полной версии резервной копии. Соответственно, только третья версия резервной копии будет инкрементной или дифференциальной. Если этот параметр выбран для полного метода, название **Хранить не более [n] последних версий** меняется на **Хранить не более 1+[n] последних версий**.

Управление пользовательскими схемами резервного копирования

Если что-либо изменить в существующей схеме резервного копирования, измененную схему можно сохранить как новую. В этом случае нужно будет указать новое имя для этой схемы резервного копирования.

- Существующие пользовательские схемы можно перезаписывать.
- Существующие предустановленные схемы резервного копирования перезаписать нельзя.
- В имени схемы допустимы любые символы, разрешенные ОС в именах файлов. Максимальная длина имени схемы резервного копирования — 255 символов.
- Создать можно не более 16 пользовательских схем резервного копирования.

После создания пользовательской схемы резервного копирования ее можно использовать при настройке резервного копирования, как любую другую существующую схему.

Также пользовательскую схему резервного копирования можно использовать, не сохраняя. В этом случае она будет доступна только для резервной копии, в которой она была создана, а для других резервных копий воспользоваться ею не удастся.

Если пользовательская схема резервного копирования больше не требуется, ее можно удалить. Чтобы удалить схему, выберите ее в списке схем резервного копирования, нажмите кнопку **Удалить**, а затем подтвердите удаление в окне **Удалить схему**.

Примечание

Предустановленные системные схемы резервного копирования не удаляются.

Примеры пользовательских схем

1. Резервное копирование всего компьютера — «Две полных версии»

Ситуация: вы хотите защитить все данные на своем компьютере с двумя полными версиями и обновлять резервную копию раз в месяц. Посмотрим, как сделать это с помощью пользовательской схемы резервного копирования.

1. Начните настройку резервного копирования всего ПК. Дополнительные сведения см. в разделе *Резервное копирование всех данных на компьютере*.
2. Убедитесь, что в качестве источника резервной копии выбран весь ПК.
3. Нажмите кнопку **Параметры**, откройте вкладку **Расписание**, щелкните **Ежемесячно** и укажите день месяца (например, 20-й). Версия резервной копии будет создаваться ежемесячно в указанный день. Затем укажите время запуска операции резервного копирования.
4. Откройте вкладку **Схема**, после чего выберите **Пользовательская схема**, а не **Инкрементная схема**.
5. В поле **Метод резервного копирования** выберите из раскрывающегося списка пункт **Полное**.
6. Для ограничения количества версий нажмите **Хранить не более [n] последних версий**, введите или выберите **2** и нажмите кнопку **ОК**.

   В этом случае программа будет создавать новую версию ежемесячно в 20-й день месяца. Поле создания третьей версии самая старая версия будет автоматически удаляться.
7. Проверьте заданные параметры и нажмите **Создать копию**. Если нужно, чтобы первое резервное копирование было запущено только во время, заданное в планировщике, щелкните стрелку вниз справа от кнопки **Создать копию** и выберите из раскрывающегося списка пункт **Позже**.

2. Резервное копирование файлов «Ежедневная инкрементная версия + недельная полная версия»

Ситуация: у вас имеются файлы или папки, с которыми вы работаете каждый день. Вам требуется сохранять результаты ежедневной работы и иметь возможность восстановить состояние данных на любой день в течение последних трех недель. Посмотрим, как сделать это с помощью пользовательской схемы резервного копирования.

1. Начните настройку файловой резервной копии. Дополнительные сведения см. в разделе *Резервное копирование файлов и папок*.
2. Щелкните **Параметры**, откройте вкладку **Расписание**, выберите **Ежедневно** и укажите время запуска операции резервного копирования. Например, если вы заканчиваете ежедневную работу в 20:00, укажите это время или чуть более позднее (20:05) в качестве времени запуска.
3. Откройте вкладку **Схема**, после чего выберите **Пользовательская схема**, а не **Инкрементная схема**.
4. В поле **Метод резервного копирования** выберите пункт **Инкрементное** из раскрывающегося списка.
5. Щелкните **Создавать полную версию после каждых [n] инкрементных версий** и введите или выберите значение **6**.

   В этом случае программа сначала создаст полную начальную версию резервной копии (независимо от настройки процесса резервного копирования первая версия резервной копии

всегда будет полной), а затем 6 инкрементных версий день за днем. После этого снова будут созданы 1 полная версия и 6 инкрементных, и т. д. Таким образом, каждая новая полная версия будет создаваться ровно через неделю.

6. Чтобы ограничить время хранения версий, щелкните **Включить автоматическую очистку**.
7. Щелкните **Удалять цепочки версий старше [n] дней**, введите или выберите **21** и нажмите кнопку **ОК**.
8. Проверьте заданные параметры и нажмите **Создать копию**. Если нужно, чтобы первое резервное копирование было запущено только во время, указанное в расписании, щелкните стрелку вниз справа от кнопки **Создать копию** и выберите из раскрывающегося списка пункт **Позже**.

3. Резервное копирование дисков «Полная версия каждые 2 месяца + дифференциальная версия дважды в месяц»

Ситуация: требуется выполнять резервное копирование системного раздела дважды в месяц и создавать новую полную версию резервной копии каждые 2 месяца. Посмотрим, как сделать это с помощью пользовательской схемы резервного копирования.

1. Начните настройку резервной копии диска. См. раздел *Резервное копирование дисков и разделов*.
2. Выберите системный раздел (обычно C:) в качестве источника резервного копирования.
3. Щелкните **Параметры**, откройте вкладку **Расписание**, щелкните **Ежемесячно** и укажите, например, 1-й и 15-й дни месяца. Версия резервной копии будет создаваться примерно каждые 2 недели. Затем укажите время запуска операции резервного копирования.
4. Откройте вкладку **Схема**, после чего выберите **Пользовательская схема**, а не **Инкрементная схема**.
5. В поле **Метод резервного копирования** выберите из раскрывающегося списка пункт **Дифференциальное**.
6. Щелкните **Создавать полную версию после каждых [n] дифференциальных версий** и введите или выберите значение **3**.

   В этом случае программа сначала создаст исходную полную версию резервной копии (независимо от настройки процесса резервного копирования первая версия резервной копии всегда будет полной), а затем 3 дифференциальных версии с интервалом примерно две недели. После этого снова будут созданы 1 полная версия и 3 дифференциальных и т. д. Таким образом, новая полная версия будет создаваться каждые два месяца.
7. Чтобы ограничить время хранения версий, щелкните **Включить автоматическую очистку**.
8. Щелкните **Удалять цепочки версий старше [n] дней**, введите или выберите **120** и нажмите кнопку **ОК**.
9. Проверьте заданные параметры и нажмите **Создать копию**. Если нужно, чтобы первое резервное копирование было запущено только во время, заданное в планировщике, щелкните стрелку вниз

справа от кнопки **Создать копию** и выберите из раскрывающегося списка пункт **Позже**.

Уведомления при резервном копировании

Расположение: **Параметры** → **Уведомления**

Иногда резервное копирование или восстановление может длиться час или более. Кибер Бэкап Старт может уведомлять о завершении операции по электронной почте. Также возможна отправка дубликатов сообщений, выдаваемых в процессе работы программы, и полного журнала операции после ее завершения.

По умолчанию отправка любых уведомлений отключена.

Порог свободного объема дискового пространства

Можно настроить получение уведомлений, когда свободное пространство в хранилище резервных копий станет меньше указанного порогового значения. Если после запуска резервного копирования Кибер Бэкап Старт обнаружит, что свободного пространства в выбранном хранилище резервных копий меньше, чем было указано, то программа не будет начинать процесс резервного копирования, а немедленно уведомит об этом, выведя соответствующее сообщение. Это сообщение предлагает три варианта действий: игнорировать и продолжать резервное копирование, выбрать другое хранилище для резервной копии или отменить резервное копирование.

Если свободное пространство станет меньше указанного значения в ходе выполнения резервного копирования, программа отобразит такое же сообщение, и потребуется принять одно из этих решений.

Кибер Бэкап Старт может отслеживать свободное пространство на следующих устройствах хранения: локальных жестких дисках, накопителях и дисках USB, общих сетевых папках (SMB). Оповещение о достижении порога свободного пространства не работает для FTP-серверов.

Как установить порог свободного пространства:

1. Установите флажок **Показывать уведомление при недостатке свободного пространства на диске**.
2. Введите пороговое значение в поле **Уведомлять, когда свободного места на диске останется меньше**.

> **Примечание**
>
> Сообщение не будет показано, если в настройках **Обработка ошибок** установлен флажок **Не показывать сообщения и диалоговые окна во время выполнения операции**.

Уведомление по электронной почте

1. Установите флажок **Отправлять по электронной почте уведомления о состоянии операции**.
2. Настройте параметры электронной почты:
   - Введите адрес электронной почты в поле **Кому**. Можно указать несколько адресов, разделяя их точкой с запятой.
   - Укажите сервер исходящей почты (SMTP) в поле **Настройки сервера**.
   - Укажите порт сервера исходящей почты. По умолчанию используется порт 25.
   - Выберите нужный метод шифрования для сообщений электронной почты.
   - При необходимости установите флажок **Проверка подлинности SMTP** и введите имя пользователя и пароль в соответствующие поля.
3. Чтобы проверить правильность настроек, нажмите кнопку **Отправить тестовое сообщение**.

Если не удается отправить тестовое сообщение:

1. Щелкните **Расширенные настройки**.
2. Настройте дополнительные параметры электронной почты:
   - Введите адрес электронной почты отправителя в поле **От**. Если вы не знаете, какой адрес указывать, наберите любой адрес в стандартном формате, например *aaa@bbb.com*.
   - При необходимости измените тему сообщения в поле **Тема**.

     Чтобы упростить мониторинг статуса резервной копии, можно добавить самую важную информацию в тему сообщений. Можно ввести следующие текстовые подписи:

     - %BACKUP_NAME% — имя резервной копии
     - %COMPUTER_NAME% — имя компьютера, на котором было запущено резервное копирование
     - %OPERATION_STATUS% — результат резервного копирования или другой операции

       Например:

       ```
       Статус резервной копии %BACKUP_NAME%: %OPERATION_STATUS% (%COMPUTER_NAME%)
       ```
   - Установите флажок **Логин для сервера входящей почты** и укажите под ним сервер входящей почты (POP3).
   - Укажите порт сервера входящей почты. По умолчанию используется порт 110.

3. Снова нажмите кнопку **Отправить тестовое сообщение**.

Дополнительные параметры уведомления:

- **Отправлять уведомления об успешном завершения операции** — установите этот флажок для отправки уведомлений о завершении процесса.
- **Отправлять уведомления при возникновении ошибки операции** — установите этот флажок для отправки уведомлений о сбое процесса.
- **Оповещать о необходимости вмешательства пользователя** — установите этот флажок для отправки уведомлений с сообщениями операции.
- **Присоединять к уведомлению полный журнал** — установите этот флажок для отправки уведомлений с полным журналом операций.

> **Примечание**
>
> Вы будете получать уведомления по электронной почте только для определенной резервной копии.

Исключение элементов из резервной копии

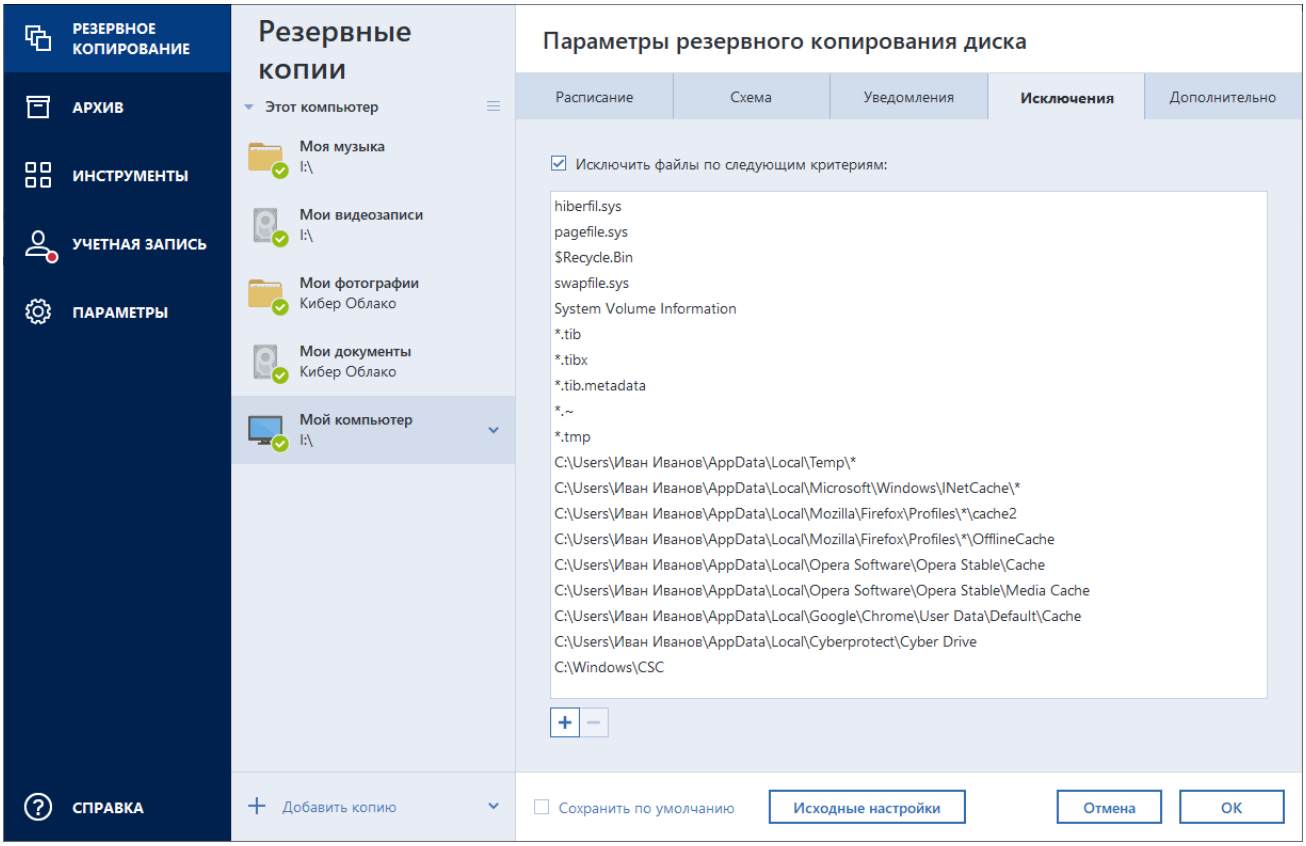
Расположение: **Параметры** → **Исключения**

Если необходимо исключить ненужные файлы из резервной копии, укажите соответствующие типы файлов на вкладке **Исключения** окна параметров резервного копирования. Можно указать исключения для резервных копий дисков, резервных копий файлов или резервных копий в онлайн-хранилище.

Если вы выбираете конкретный файл для резервного копирования, он не может быть исключен параметрами исключения. Эти параметры применяются только к файлам, расположенным в разделе, на диске или внутри папки, которые выбраны для резервного копирования.

Использование параметров исключений по умолчанию

После установки приложения для всех параметров исключений установлены первоначальные значения. Параметры можно изменить только на время выполнения текущей операции резервного копирования или для всех последующих операций. Установите флажок **Сохранить по умолчанию**, чтобы применить измененные настройки ко всем последующим операциям резервного копирования. Чтобы вернуть все измененные параметры к значениям, которые были изначально заданы при установке продукта, нажмите кнопку **Исходные настройки**.



Что и как можно исключить

Можно исключить файлы, соответствующие определенным критериям. Для этого установите флажок **Исключить файлы по следующим критериям**, щелкните значок «плюс» и введите критерий исключения.

Примечание

Не рекомендуется исключать скрытые и системные файлы из резервных копий системного раздела.

Как добавить критерий исключения:

- Имя файла можно ввести полностью:
  - `file.ext` — все файлы с данным именем и расширением будут исключены из резервной копии.
  - `C:\file.ext` — файл `file.ext` на диске C: будет исключен.
- Можно ввести подстановочные знаки (* и ?):
  - `*.ext` — все файлы с расширением EXT будут исключены.
  - `??name.ext` — все файлы с расширением EXT, имеющие шесть букв в имени (которое начинается с любых двух символов (??) и заканчивается на *name*), будут исключены.

- Чтобы исключить папку из резервной копии на уровне диска, щелкните значок «плюс», нажмите кнопку с многоточием и выберите исключаемую папку в дереве каталогов, а затем нажмите кнопку **ОК**.

Чтобы удалить критерий, добавленный по ошибке, выберите его и щелкните значок «минус».

Режим создания образа

Расположение: **Параметры** → **Дополнительно** → **Режим создания образа**

Этот параметр недоступен для резервного копирования в Кибер Облако.

Эти параметры можно использовать для создания точных копий целых разделов или жестких дисков, а не только секторов, содержащих данные. Например, это может быть полезно при резервном копировании раздела или диска с операционной системой, которую не поддерживает Кибер Бэкап Старт. Обратите внимание, что в этом режиме время обработки увеличивается, а размер файла резервной копии, как правило, больше.

- Чтобы создать посекторную резервную копию, установите флажок **Архивировать в посекторном режиме**.
- Чтобы включить в резервную копию все нераспределенное пространство диска, установите флажок **Архивировать нераспределенное пространство**.

  Этот флажок доступен только при установленном флажке **Архивировать в посекторном режиме**.

Защита резервных копий

Расположение: **Параметры** → **Дополнительно** → **Защита резервной копии**

> **Примечание**
>
> Этот раздел относится к локальным и сетевым резервным копиям. Сведения о защите облачных резервных копий см. в разделе *Защита резервных копий в онлайн-хранилище*.

По умолчанию защиты паролем для резервных копий нет, но можно настроить пароли для защиты файлов резервных копий.

> **Примечание**
>
> Нельзя изменить параметры защиты для существующей резервной копии.

Как защитить резервную копию:

1. Введите пароль для резервной копии в соответствующее поле. Рекомендуется использовать сложный пароль длиной более семи символов, содержащий как буквы (прописные и строчные), так и цифры.

   > **Примечание**
   >
   > Извлечь пароль невозможно. Необходимо запомнить пароль, заданный для защиты резервной копии.

2. Чтобы подтвердить ранее введенный пароль, снова введите его в соответствующее поле.
3. [Дополнительный шаг] Чтобы усилить защиту конфиденциальных данных, можно использовать дополнительную защиту, уровень которой может быть указан. Для выбора оптимального соотношения производительности и степени защиты можно использовать следующие уровни защиты: низкий, средний и высокий.

   В большинстве случаев достаточно использовать низкий уровень защиты. Чем выше уровень защиты, тем лучше защищены данные. Однако использование более высоких уровней защиты значительно замедляет процесс резервного копирования.

   Если необходимо использовать дополнительную защиту, выберите один из трех вариантов:

   - **Низкий** — для использования низкого уровня защиты;
   - **Средний** — для использования среднего уровня защиты;
   - **Высокий** — для использования высокого уровня защиты.

   Если дополнительная защита не нужна и достаточно защитить резервную копию паролем, выберите **Нет**.
4. Указав все параметры резервного копирования, нажмите кнопку **ОК**.

Как получить доступ к резервной копии, защищенной паролем

Кибер Бэкап Старт запрашивает пароль при каждой попытке изменения резервной копии:

- Восстановить данные из резервной копии
- Изменить настройки
- Подключить
- Переместить

Для доступа к резервной копии необходимо ввести правильный пароль. В целях безопасности отсутствует возможность восстановить потерянные пароли.

Защита резервных копий в онлайн-хранилище

Расположение: **Параметры** → **Дополнительно** → **Защита резервной копии**

Данные в Кибер Облаке можно дополнительно защитить с помощью пароля. В этом случае при резервном копировании данные будут защищены паролем с высокой степенью защиты, а затем сохранены в Кибер Облаке. Для работы с резервной копией программе необходим пароль, который должен быть указан при настройке резервного копирования в онлайн-хранилище. Вы можете задать любой желаемый набор символов. Пароль вводится с учетом регистра.

Предупреждение

Пароль резервной копии в онлайн-хранилище нельзя восстановить. Необходимо запомнить пароль, заданный для защиты резервной копии.

При попытке доступа к защищенным паролем данным программа попросит ввести пароль.

Примечание

Обратите внимание, что нельзя задать или изменить пароль для уже существующей резервной копии в онлайн-хранилище.

Команды до и после резервного копирования

Расположение: **Параметры** → **Дополнительно** → **Pre/Post-команды**

Этот параметр недоступен для резервного копирования в Кибер Облако.

Вы можете указать команды или пакетные файлы, которые будут автоматически выполняться до и после процесса резервного копирования.

Например, может потребоваться запустить или остановить определенные процессы Windows или проверить данные перед запуском резервного копирования.

Как указать команды (пакетные файлы):

- Установите флажок **Использовать пользовательские команды**.
- В поле **Pre-команда** выберите команду, которая будет выполняться перед запуском резервного копирования. Чтобы создать новую команду или выбрать пакетный файл, нажмите кнопку **Изменить**.
- В поле **Post-команда** выберите команду, которая будет выполняться после завершения резервного копирования. Чтобы создать новую команду или выбрать пакетный файл, нажмите кнопку

Изменить.

Не пытайтесь выполнить интерактивные команды, то есть команды, требующие вмешательства пользователя (например, **pause**). Они не поддерживаются.

Редактирование пользовательских команд, выполняемых при резервном копировании

Чтобы указать пользовательские команды, которые будут выполняться перед операцией резервного копирования или после,

- В поле **Команда** введите команду вручную или выберите ее из списка. Чтобы выбрать пакетный файл, нажмите кнопку **...**.
- В поле **Рабочая папка** введите путь для выполнения команды или выберите его из списка использованных путей.
- В поле **Аргументы** введите или выберите из списка аргументы исполняемой команды.

Отключение параметра **Не выполнять операции до завершения исполнения команды**, включенного по умолчанию для команд, выполняемых перед резервным копированием, позволит процессу резервного копирования выполняться одновременно с пользовательскими командами.

Параметр **При возникновении ошибки отменить выполнение операции** (включен по умолчанию) прервет процедуру при возникновении каких-либо ошибок, произошедших во время выполнения команды.

Чтобы проверить созданную команду, нажмите кнопку **Тест команды**.

Разделение резервной копии

Расположение: **Параметры** → **Дополнительно** → **Разделение резервной копии**

> **Примечание**
>
> Кибер Бэкап Старт не может разделить уже существующие резервные копии. Резервные копии могут быть разделены только во время создания.

Этот параметр недоступен для резервного копирования в Кибер Облако.

Резервные копии большого размера можно разделить на несколько файлов, вместе составляющих исходную резервную копию. Резервную копию также можно разделить для записи на съемные носители.

Параметр по умолчанию — **Автоматически**. С этим параметром Кибер Бэкап Старт действует следующим образом.

При создании резервной копии на жестком диске:

- Если на выбранном диске достаточно места и его файловая система поддерживает файлы с размером, соответствующим прогнозируемому размеру файла резервной копии, то будет создан один файл резервной копии.
- Если на диске достаточно места, но его файловая система не поддерживает прогнозируемый размер файла, резервная копия будет автоматически разделена на несколько файлов.
- Если свободного пространства на жестком диске недостаточно, программа выдаст сообщение и будет ждать вашего решения. Попробуйте освободить дополнительное пространство на диске и продолжить или выберите другой диск.

Проверка резервной копии

Расположение: **Параметры** → **Дополнительно** → **Проверка**

Этот параметр недоступен для резервного копирования в Кибер Облако.

Можно указать следующие параметры:

- **Проверять резервную копию каждый раз после ее создания** — установите этот флажок, чтобы проверять целостность версии резервной копии сразу после выполнения резервного копирования. Рекомендуется включать этот параметр при резервном копировании критически важных данных или системного диска.
    - **Проверять только последнюю версию разнородной резервной копии** — быстрая проверка последнего экземпляра резервной копии.
    - **Проверять резервную копию целиком**
- **Проверять резервную копию по расписанию** — установите этот флажок, чтобы запланировать проверку резервных копий для гарантии их работоспособности.
    - **Последнюю версию разнородной резервной копии после ее завершения**
    - **Резервную копию целиком после ее завершения**

    По умолчанию используются следующие параметры:
    - **Периодичность** — ежемесячно.
    - **День** — дата создания резервной копии.
    - **Время** — время начала резервного копирования плюс 15 минут.

Также можно настроить запуск проверки вручную через контекстное меню резервной копии.

Для этого щелкните резервную копию правой кнопкой мыши и выберите:

- **Проверить все версии**
- **Проверить последнюю версию**

  Пример: операция резервного копирования начата 15 июля в 12:00. Версия резервной копии была создана в 12:05. Проверка этой версии будет начата в 12:15, если компьютер находится в режиме отображения «заставки». В противном случае проверка не будет выполнена. Очередная проверка будет запущена через месяц, 15 августа в 12:15. Как и раньше, компьютер должен находиться в режиме отображения «заставки». Та же операция повторится 15 сентября и так далее.

  Вы можете изменить параметры, заданные по умолчанию, и установить собственное расписание. Дополнительные сведения см. в разделе *Планирование*.

Обработка ошибок

Расположение: **Параметры** → **Дополнительно** → **Обработка ошибок**

Если в Кибер Бэкап Старт возникает ошибка при выполнении резервного копирования, процесс резервного копирования останавливается и появляется сообщение, ожидающее ответа пользователя о том, как поступить с этой ошибкой. Можно настроить политику обработки ошибок, чтобы Кибер Бэкап Старт не прерывал процесс резервного копирования, а обрабатывал ошибку в соответствии с заданным набором правил и продолжал работу.

> **Примечание**
>
> Этот раздел относится к резервным копиям, использующим локальное или сетевое место назначения. Параметры обработки ошибок для резервных копий, использующих Кибер Облако в качестве места назначения, см. в разделе *Обработка ошибок для резервных копий и реплик в облаке*.

Как настроить политику обработки ошибок:

1. Настройте политику обработки ошибок:

   - **Не показывать сообщения и диалоговые окна во время выполнения операции** — выберите этот параметр, чтобы игнорировать ошибки при выполнении операций резервного копирования. Это полезно в тех случаях, когда нет возможности контролировать процесс.
   - **Игнорировать ошибки чтения дефектных секторов** — этот параметр доступен только для резервного копирования дисков и разделов. Он позволяет успешно завершить резервное копирование, даже если на жестком диске имеются поврежденные секторы.

     Рекомендуется установить этот флажок, если имеется неисправность жесткого диска, например:

- Жесткий диск издает щелчки или скрежет при работе.
- Система S.M.A.R.T. обнаружила проблемы с жестким диском и выдала рекомендацию как можно быстрее выполнить резервное копирование.

Если не установить этот флажок, может произойти сбой резервного копирования из-за поврежденных секторов на диске.

- **При недостатке места в Зоне безопасности Киберпротект удалять самую старую резервную копию** (включено по умолчанию). Рекомендуется установить этот флажок, если планируется выполнять резервное копирование в Зону безопасности по расписанию в отсутствие пользователя. В противном случае, если во время операции резервного копирования в Зоне безопасности заканчивается место, Кибер Бэкап Старт приостанавливает резервное копирование и запрашивает действие пользователя. Диалоговое окно появляется даже при включенном параметре **Не показывать сообщения и диалоговые окна во время выполнения операции**.
- **Повторить попытку в случае неудачного резервного копирования**. Этот параметр позволяет автоматически повторить попытку резервного копирования, если по какой-либо причине его выполнить не удастся. Можно указать количество попыток и временной интервал между попытками. Обратите внимание, что если не устранить ошибку, препятствующую резервному копированию, то резервная копия не будет создана.

> **Примечание**
>
> Запланированные операции резервного копирования не будут запускаться до завершения всех попыток.

2. Нажмите кнопку **ОК**.

Обработка ошибок для резервных копий и реплик в облаке

Можно настроить Кибер Бэкап Старт на повтор неудачных операций резервного копирования и репликации в облако.

Настройка количества повторных попыток и временного интервала между ними:

1. В разделе **Резервное копирование** выберите облачную резервную копию, нажмите **Параметры** и перейдите на вкладку **Дополнительно**.
2. В разделе **Обработка ошибок** установите флажок **Повторить попытку в случае неудачного резервного копирования**, затем выберите количество попыток (от 1 до 99) и интервал между ними.
3. Нажмите кнопку **ОК**.

Новая настройка будет применяться ко всем последующим операциям резервного копирования и репликации в облако для выбранного объекта резервной копии.

> **Примечание**
>
> Запланированные операции резервного копирования не будут запускаться до завершения всех повторных попыток.

Параметры безопасности файлов для создаваемой резервной копии

Расположение: **Параметры** → **Дополнительно** → **Параметры безопасности файлов**

> **Примечание**
>
> Этот параметр доступен только для резервного копирования на уровне файлов при использовании Зоны безопасности Киберпротект.

Можно указать параметры безопасности для резервных копий файлов.

- **Сохранять параметры безопасности файлов в резервных копиях** — выберите этот пункт, чтобы сохранить все настройки безопасности файлов (разрешения, присвоенные группам или пользователям) для последующего восстановления.

  По умолчанию файлы и папки сохраняются в резервной копии со всеми исходными параметрами безопасности Windows (разрешениями чтения, записи и выполнения для каждого пользователя или группы пользователей, установленными в настройках файла **Свойства** → **Безопасность**). При восстановлении файла/папки на компьютер, где нет пользователя, указанного в разрешениях, такой файл может оказаться недоступным для чтения или редактирования.

  Чтобы этого не произошло, можно запретить сохранение параметров безопасности файлов в резервных копиях. Тогда восстановленные файлы/папки будут наследовать разрешения той папки, в которую они восстановлены (родительской папки или диска, если они восстановлены в корневой каталог).

  Параметры безопасности также можно отключить во время восстановления, даже если они сохраняются в резервной копии. Результат будет тот же.

- **Хранить файлы в резервных копиях в расшифрованном виде** (по умолчанию отключено) — выберите этот параметр, если в создаваемой резервной копии имеются зашифрованные файлы и нужно, чтобы они были доступны любому пользователю после восстановления. В противном случае восстановленные файлы/папки будут доступны только пользователю, который их зашифровал. Снятие шифрования полезно также, если предполагается восстановление

зашифрованных файлов на другом компьютере.

Если функция шифрования, имеющаяся в Windows XP и более поздних операционных системах, не используется, просто игнорируйте этот параметр. (Шифрование файлов/папок устанавливается в разделе **Свойства** → **Общие** → **Дополнительные атрибуты** → **Шифровать содержимое для защиты данных**).

Выключение компьютера

Расположение: **Параметры** → **Дополнительно** → **Выключение компьютера**

Можно настроить следующие параметры:

- **Остановить все текущие операции при выключении компьютера** — если попытаться завершить работу компьютера в то время, как Кибер Бэкап Старт осуществляет продолжительные операции, например, резервное копирование диска, то такие операции не позволят выключить компьютер. Если установить этот флажок, то Кибер Бэкап Старт будет автоматически останавливать все свои текущие операции перед выключением компьютера. Это может занять несколько минут. Остановленные процессы резервного копирования возобновятся при следующем запуске Кибер Бэкап Старт.
- **Выключить компьютер после окончания резервного копирования** — выберите этот параметр, если настраиваемый процесс резервного копирования может занимать длительное время. В этом случае не нужно ждать завершения операции. Программа выполнит запланированное резервное копирование и автоматически выключит компьютер.

  Этот параметр полезен и для планирования резервного копирования. Например, необходимо создавать резервные копии каждый рабочий день по вечерам для сохранения всей работы. Запланируйте резервное копирование и установите флажок. В этом случае можно закончить работу и уйти, зная, что будет создана резервная копия критических данных, а компьютер будет выключен.

Производительность операций резервного копирования

Расположение резервных копий с локальным местом назначения: **Параметры** → **Дополнительно** → **Производительность**.

Уровень сжатия

Выберите уровень сжатия создаваемой резервной копии.

- **Нет** — данные будут скопированы без сжатия, что существенно увеличит размер файла резервной копии.

- **Обычный** — рекомендуемый уровень сжатия данных (установлен по умолчанию).
- **Высокий** — более высокий уровень сжатия, но более длительное время создания резервной копии.
- **Максимальный** — максимальный уровень сжатия, но самое длительное время создания резервной копии.

Примечание

- Оптимальный уровень сжатия данных зависит от типа файлов, сохраняемых в резервной копии. Например, даже максимальный уровень сжатия незначительно снизит размер резервной копии, если она содержит изначально сжатые файлы, такие как JPG, PDF или MP3.
- Уровень сжатия уже существующих резервных копий нельзя изменить.

Приоритет операции

Изменение приоритета операции резервного копирования или восстановления может ускорить или замедлить процесс (в зависимости от того, был ли приоритет повышен или понижен), но также существенно влияет на производительность других выполняющихся программ. Приоритет каждого протекающего в системе процесса определяет долю выделяемых этому процессу системных ресурсов и процессорного времени. Понижение приоритета операции освободит часть ресурсов для других выполняемых компьютером задач. Повышение приоритета резервного копирования или восстановления, напротив, может ускорить процесс за счет отбора ресурсов у параллельных задач. Насколько будет выражен этот эффект, зависит от общей загрузки процессора и других факторов.

Приоритеты операции

- **Низкий** (выбран по умолчанию) — процесс резервного копирования или восстановления будет выполняться медленнее, но скорость работы других программ будет выше.
- **Обычный** — процесс резервного копирования или восстановления будет выполняться наравне с другими процессами системы.
- **Высокий** — процесс резервного копирования или восстановления будет происходить быстрее за счет уменьшения производительности других программ. Учтите, что при выборе этого варианта Кибер Бэкап Старт может использовать 100 % ресурсов компьютера.

Скорость загрузки данных

При резервном копировании в Кибер Облако можно изменить скорость передачи данных для Кибер Бэкап Старт. Установите скорость подключения, которая позволит использовать Интернет без раздражающего замедления работы.

Чтобы задать скорость подключения, выберите один из следующих параметров.

- **Максимальный** — максимальная скорость передачи данных в этой конфигурации системы.
- **Ограничить до** — можно указать максимальное значение для скорости загрузки данных.

Моментальный снимок для резервного копирования

> **Предупреждение**
>
> Это параметр только для опытных пользователей. Не меняйте значение по умолчанию, если вы не уверены в выборе.

В процессе резервного копирования диска или раздела, который часто занимает много времени, некоторые из копируемых файлов могут быть заблокированы либо использоваться или изменяться. Например, вы можете работать над документом и время от времени сохранять его. Если бы Кибер Бэкап Старт выполнял резервное копирование файлов по очереди, то открытый файл, скорее всего, изменился бы с момента начала резервного копирования, а затем был бы сохранен в резервной копии с другой временной отметкой. Таким образом данные в резервной копии были бы несогласованными. Во избежание этого Кибер Бэкап Старт создает так называемый моментальный снимок, фиксирующий данные в состоянии на определенный момент времени. Это делается перед началом резервного копирования и гарантирует согласованность данных.

Выберите вариант из списка **Моментальный снимок для резервной копии**.

- **Без моментального снимка** — моментальный снимок не будет создан. Файлы будут обрабатываться по очереди, как в обычной операции копирования.
- **VSS** — этот параметр выбран по умолчанию для резервных копий дисков и всего компьютера и гарантирует согласованность данных.

  > **Предупреждение**
  >
  > Для резервного копирования системы рекомендуется только этот вариант. После восстановления из резервной копии, созданной с другим типом моментального снимка, компьютер может не запуститься.

- **Моментальный снимок Киберпротект** — моментальный снимок будет создан с помощью драйвера Киберпротект, используемого в предыдущих версиях Кибер Бэкап Старт.
- **VSS без модулей записи** — это параметр по умолчанию для резервного копирования на уровне файлов. Модули записи VSS — это специальные компоненты VSS, которые уведомляют

приложения о создании моментального снимка, чтобы приложения подготовили свои данные. Модули записи необходимы для приложений, которые выполняют большое количество операций с файлами и требуют согласованности, например, для баз данных. Поскольку подобные приложения не устанавливаются на домашних компьютерах, использовать модули записи нет необходимости. Кроме того, это сокращает время резервного копирования файлов.

Параметры питания ноутбука

Расположение: **Параметры** → **Экономия заряда**

> **Примечание**
>
> Этот параметр доступен только на компьютерах с аккумулятором (ноутбуки, компьютеры с ИБП).

Долговременное резервное копирование способно довольно быстро разрядить аккумулятор. При работе на ноутбуке в отсутствие постоянного источника питания или в случае, если компьютер переключился на ИБП после отключения электричества, имеет смысл экономить заряд аккумулятора.

Как сэкономить заряд аккумулятора:

На боковой панели нажмите **Параметры** → **Экономия заряда**, установите флажок **Не выполнять резервное копирование при заряде аккумулятора менее** и с помощью ползунка задайте уровень заряда аккумулятора для запуска режима экономии.

Если этот параметр включен, то при отключении компьютера от сети питания или переходе на ИБП после отключения электричества и при оставшемся заряде аккумулятора равном или меньшем, чем заданный уровень, все текущие операции резервного копирования приостанавливаются, а запланированные не запускаются. После включения компьютера в сеть или восстановления подачи питания приостановленное резервное копирование возобновится. Запланированные операции резервного копирования, которые были пропущены из-за включения этого параметра, также запустятся.

Этот параметр не блокирует функцию резервного копирования полностью. В любой момент можно запустить резервное копирование вручную.

Сети Wi-Fi для резервного копирования в Кибер Облако

Расположение: **Параметры** → **Сети Wi-Fi для резервного копирования**

При резервном копировании в Кибер Облако вас может беспокоить безопасность личных данных во время передачи по незащищенным сетям Wi-Fi. Чтобы устранить риск кражи личных данных, настоятельно рекомендуется использовать только защищенные сети Wi-Fi.

Как защитить данные:

1. На боковой панели щелкните **Параметры** → **Сети Wi-Fi для резервного копирования** и выберите **Задать сети**.
2. В окне **Сети Wi-Fi для резервного копирования**, которое содержит все доступные и сохраненные недоступные сети Wi-Fi, установите флажки напротив сетей, которые следует использовать для резервного копирования данных.

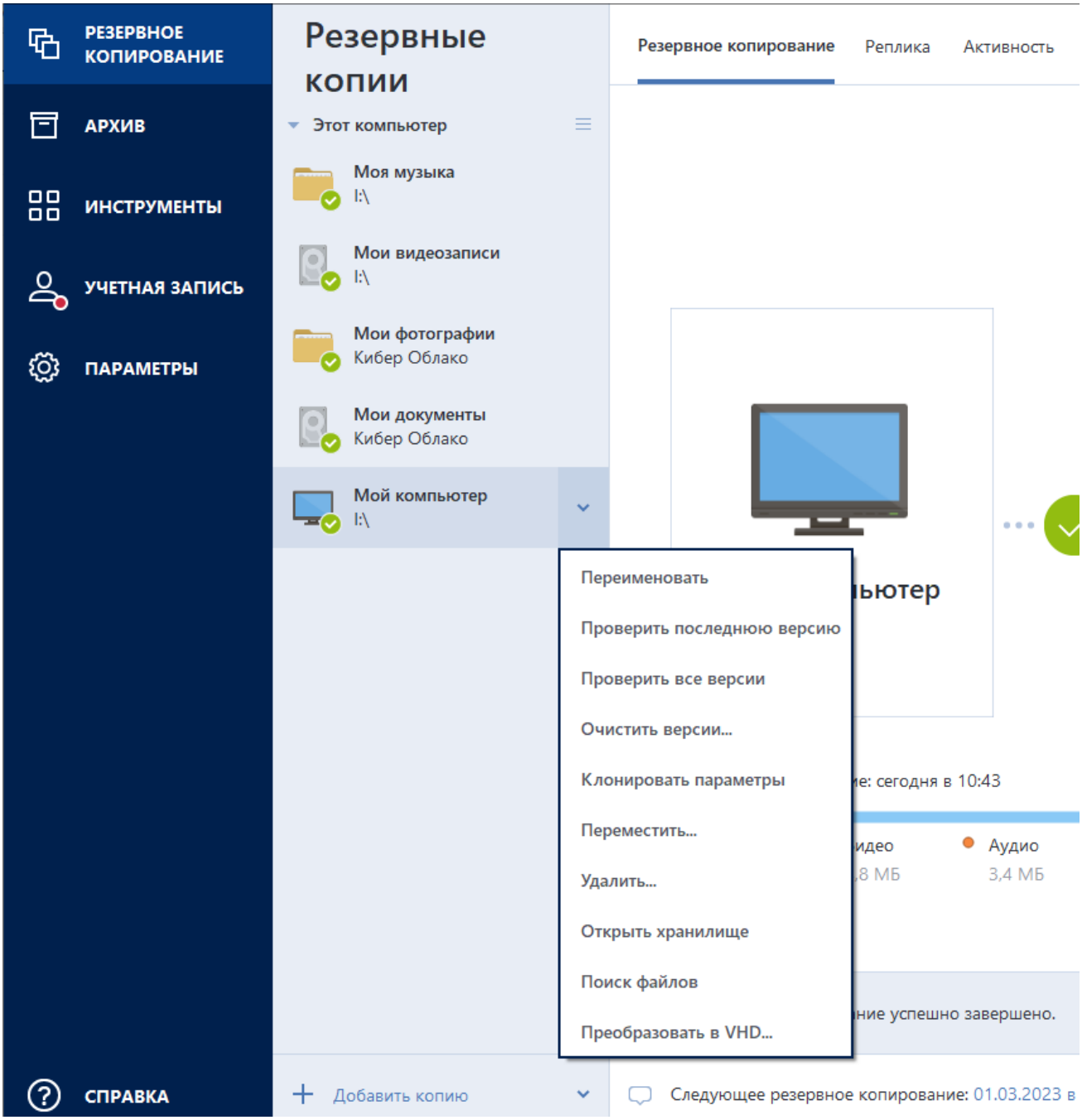
Если сети выбраны и компьютер теряет подключение к одной из них, все текущие операции резервного копирования приостанавливаются, а запланированные не запускаются. После подключения компьютера к любой из этих сетей приостановленное резервное копирование возобновится. Запланированные операции резервного копирования, которые были пропущены из-за включения этого параметра, также запустятся.

Чтобы использовать новую сеть Wi-Fi для резервного копирования данных, достаточно выбрать ее в окне **Сети Wi-Fi для резервного копирования**. Это можно делать каждый раз, когда необходимо использовать новую сеть.

Операции с резервными копиями

Меню операций резервного копирования

Меню операций резервного копирования предоставляет быстрый доступ к дополнительным операциям, которые можно выполнить с выбранной резервной копией.



Меню операций резервного копирования может содержать следующие элементы.

- **Переименовать** — позволяет задать новое имя для резервной копии в списке. Для переименования щелкните в меню **Переименовать**, введите новое имя и нажмите клавишу `Enter`.

  Применение нового имени для резервной копии полностью завершается в результате синхронизации после запуска следующего резервного копирования. В случае с Кибер Облаком процесс полной синхронизации может длиться около часа. Из-за этого не рекомендуется выполнять другие операции с резервной копией (например, удаление резервной копии) до завершения синхронизации.

- **Перенастроить** (для резервных копий, добавленных в список вручную) — настройка параметров резервных копий, созданных предыдущей версией программы. Этот пункт может также появиться для резервных копий, которые были созданы на другом компьютере и добавлены в список резервных копий без импорта настроек.

  Без настроек не удастся обновить резервную копию нажатием кнопки **Создать копию**. Кроме того, невозможно изменить или клонировать параметры резервного копирования.

- **Перенастроить** (для резервных копий в онлайн-хранилище) — привязка выбранной резервной копии к текущему компьютеру. Для этого щелкните данный пункт и измените параметры резервного копирования. Обратите внимание, что на одном компьютере может быть активна только одна резервная копия в онлайн-хранилище.

- **Проверить последнюю версию** — запуск быстрой проверки последней части резервной копии.

- **Проверить все версии** — запуск проверки всех экземпляров резервной копии.

- **Очистить версии** — позволяет удалить ненужные версии резервной копии.

- **Клонировать параметры** — создание пустой панели резервной копии с параметрами исходной копии и именем **(1) [имя исходной резервной копии]**. Измените параметры, сохраните их и нажмите кнопку **Создать копию** на панели клонированной резервной копии.

- **Переместить** — перемещение всех файлов резервной копии в другое хранилище. Последующие версии резервной копии будут сохранены в новое хранилище.

  Если изменить место сохранения в параметрах резервного копирования, в новое хранилище будут сохранены только новые версии. Более ранние версии останутся в старом хранилище.

- **Удалить** — в зависимости от типа резервной копии можно либо полностью удалить ее из хранилища, либо выбрать удаление только панели резервной копии. Если удаляется только панель, файлы резервной копии остаются на месте и в дальнейшем эту копию можно будет добавить в список. Обратите внимание, что, если удалить резервную копию полностью, отменить удаление будет невозможно.

- **Открыть хранилище** — открытие папки с файлами резервных копий.

- **Поиск файлов** — позволяет найти отдельный файл или папку, введя имя в поле поиска.

- **Преобразовать в VHD** (для резервных копий на уровне дисков) — преобразование выбранной версии резервной копии Киберпротект (TIBX-файл) в формат виртуального жесткого диска (VHD(X)-файл). Исходная версия резервной копии не будет изменена.

Действия и статистика резервного копирования

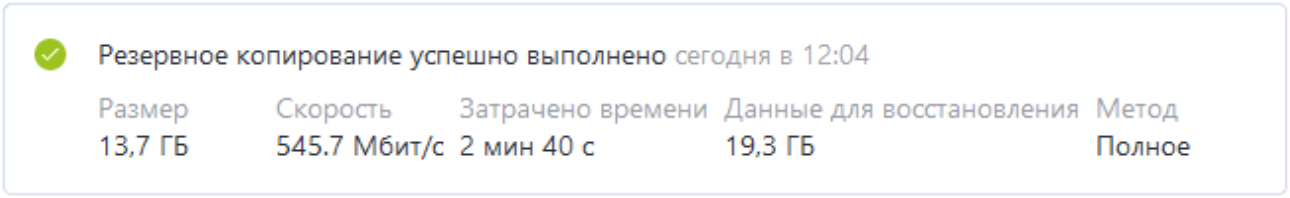
На вкладках **Активность** и **Резервное копирование** можно найти дополнительные сведения о резервной копии, такие как история резервного копирования и типы файлов в резервной копии. Вкладка **Активность** содержит список выполненных операций с выбранной резервной копией, начиная с ее создания, а также статусы операций и статистику. Это удобно, когда требуется узнать состояние резервного копирования в фоновом режиме, например, количество и статус запланированных операций, размер скопированных данных, результаты проверки резервной копии и т. д.

При создании первой версии резервной копии на вкладке **Резервное копирование** наглядно отображается ее содержимое по типам файлов.

Вкладка «Активность»

Как просмотреть действия с резервной копией:

1. На боковой панели нажмите **Резервное копирование**.
2. Выберите в списке резервную копию, историю действий которой нужно просмотреть.
3. Перейдите на вкладку **Активность**.



Что можно просматривать и анализировать:

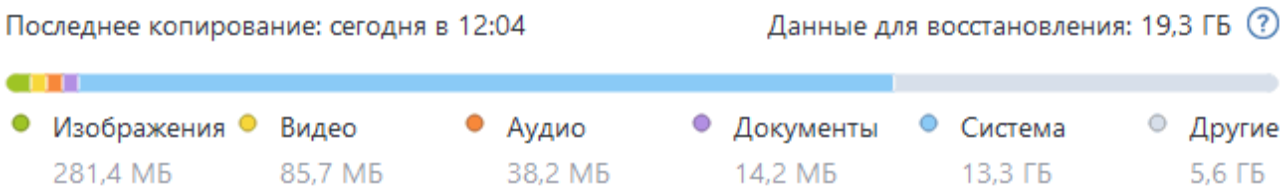
- Операции резервного копирования и их статусы (успешно, сбой, отменено, прервано и т. д.)
- Операции с резервной копией и их статусы
- Сообщения об ошибках
- Комментарии к резервным копиям
- Подробные сведения об операции резервного копирования, включая:
  - **Размер** — размер данных текущей версии резервной копии в файле резервной копии .tibx. Размер зависит от уровня сжатия, выбранного в настройках резервной копии, метода и схемы резервного копирования.
  - **Скорость** — скорость операции резервного копирования.
  - **Затрачено времени** — время, потраченное на операцию резервного копирования.
  - **Данные для восстановления** — размер данных, которые можно восстановить из текущей

версии резервной копии.

- **Метод** — метод резервного копирования (полное, инкрементное или дифференциальное).

Вкладка «Резервное копирование»

После создания резервной копии можно просмотреть статистику по типам файлов в последней версии резервной копии.



Наведите курсор на цветной сегмент, чтобы узнать количество файлов и общий размер по каждой категории данных:

- Изображения
- Видеофайлы
- Аудиофайлы
- Документы
- Системные файлы
- Другие типы файлов, включая скрытые системные файлы

Сортировка резервных копий в списке

По умолчанию резервные копии сортируются по дате создания от самой последней до самой старой. Для изменения порядка выберите нужный тип сортировки в верхней части списка резервных копий. Существуют следующие варианты.

Команда		**Описание**
Сортировать по	Имя	Эта команда сортирует все резервные копии в алфавитном порядке. Для изменения порядка на обратный выберите **Z -> A**.
	Дата создания	Эта команда сортирует все резервные копии в порядке от самой новой до самой старой. Для изменения порядка на обратный выберите **Сначала старые**.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Команда		Описание
	Дата обновления	Эта команда сортирует все резервные копии по дате последней версии. Чем новее последняя версия резервной копии, тем выше будет эта копия в списке. Для изменения порядка на обратный выберите **Сначала давние**.
	Размер	Эта команда сортирует все резервные копии по размеру от самой большой до самой малой. Для изменения порядка на обратный выберите **Сначала маленькие**.
	Тип источника	Эта команда сортирует все резервные копии по типу источника.
	Тип места назначения	Эта команда сортирует все резервные копии по типу хранилища.

Репликация резервных копий в Кибер Облако

Зачем нужна репликация?

Хотя резервное копирование защищает данные, рекомендуется также реплицировать все локальные резервные копии в Кибер Облако для защиты от случайного повреждения на компьютере. Конечно, можно создать два плана резервного копирования: в локальное хранилище и в Кибер Облако. Но автоматическая репликация позволяет сэкономить время на настройку планов резервного копирования, а создание реплики выполняется быстрее, чем создание второй резервной копии. Реплика представляет собой дубликат резервной копии. Она может использоваться для восстановления и доступна из любого места.

Активация репликации

Репликация неактивна по умолчанию. Ее можно активировать для любой локальной резервной копии диска, раздела или всего компьютера, которая использует локальное место назначения (внешний или внутренний диск), настроенное в Кибер Бэкап Старт. Репликацию можно активировать на особой вкладке плана резервного копирования.

Как активировать репликацию резервной копии в Кибер Облако:

1. Выберите из списка резервную копию, которую необходимо реплицировать, и откройте вкладку **Реплика**.
2. Нажмите **Реплицировать**. Теперь репликация активирована и запустится при создании обычной резервной копии. Кибер Бэкап Старт можно закрыть. Процессы резервного копирования и репликации продолжатся в фоновом режиме.
3. [Необязательно] Нажмите **Параметры** → **Дополнительно** → **Репликация в Кибер Облако**, чтобы *настроить параметры очистки* Кибер Облака для оптимизации использования хранилища.

Защита реплицированных данных

Реплицированные данные загружаются в Кибер Облако с использованием защищенного протокола SSL.

В облаке данные хранятся в соответствии с настройками защиты. Если пароль не задан, реплицированные данные хранятся в незащищенном виде. В противном случае данные защищаются паролем с высокой степенью защиты.

Проверка резервных копий

Процедура проверки определяет, можно ли будет восстановить данные из резервной копии.

Например, важно выполнять проверку резервных копий перед восстановлением системы. Если запустить восстановление из поврежденной резервной копии, процесс завершится сбоем и компьютер может перестать загружаться. Рекомендуется выполнить проверку резервных копий системного раздела с загрузочного носителя. Остальные резервные копии можно проверить в Windows. См. также разделы *Подготовка к восстановлению* и *Основные понятия*.

Как проверить всю резервную копию в Windows:

1. Запустите Кибер Бэкап Старт и щелкните **Резервное копирование** на боковой панели.
2. В списке резервных копий щелкните стрелку вниз рядом с нужной резервной копией и выберите **Проверить все версии** или **Проверить последнюю версию**.

Как проверить определенную версию резервной копии или всю резервную копию в автономной версии Кибер Бэкап Старт (загрузочный носитель):

1. На вкладке **Восстановление** найдите резервную копию, содержащую версию, которую необходимо проверить. Если резервной копии нет в списке, нажмите кнопку **Поиск резервной копии** и укажите путь к резервной копии вручную. Кибер Бэкап Старт добавит эту резервную копию в список.
2. Щелкните правой кнопкой мыши резервную копию или нужную версию и выберите **Проверить архив**. Откроется **Мастер проверки**.
3. Нажмите кнопку **Приступить**.

Резервное копирование в разные хранилища

Версии резервной копии можно сохранять в разные хранилища, изменяя их в параметрах резервного копирования. Например, после сохранения первоначальной полной резервной копии на внешний жесткий диск USB можно выбрать в параметрах резервного копирования флеш-накопитель USB в качестве места сохранения резервной копии.

Последующие инкрементные или дифференциальные резервные копии будут записываться на флеш-накопитель USB.

Примечание

В зоне безопасности Киберпротект и на FTP-серверах может располагаться только вся резервная копия.

Разделение резервных копий на лету

Если свободного пространства на целевом диске недостаточно для завершения текущей операции резервного копирования, программа отобразит предупреждение.

Чтобы завершить резервное копирование, выполните одно из следующих действий.

- Освободите пространство на диске и нажмите кнопку **Повторить**.
- Нажмите кнопку **Обзор** и выберите другое устройство хранения.
- Нажмите **Форматировать**, чтобы стереть все данные на диске, и продолжите резервное копирование.

Если версии резервной копии хранятся в разных хранилищах, может потребоваться указать их при восстановлении.

Добавление существующей резервной копии в список

Возможно, у вас есть резервные копии, созданные в предыдущей версии Кибер Бэкап Старт или скопированные с другого компьютера. При каждом запуске Кибер Бэкап Старт сканирует компьютер на наличие таких резервных копий и автоматически добавляет их в список.

Если у вас есть резервные копии, которые отсутствуют в списке, их можно добавить вручную.

Как добавить резервные копии вручную:

1. В разделе **Резервное копирование** внизу списка резервных копий щелкните стрелку и выберите **Добавить существующую резервную копию**. Откроется окно, в котором можно просмотреть резервные копии на компьютере.
2. Выберите версию резервной копии (TIBX-файл) и нажмите кнопку **Добавить**.

   Вся резервная копия будет добавлена в список.

Очистка резервных копий, версий и реплик

Для удаления ненужных резервных копий и их версий используйте средства программы Кибер Бэкап Старт.

Кибер Бэкап Старт хранит сведения о резервных копиях в базе метаданных. Поэтому при удалении

ненужных файлов резервных копий в проводнике Windows сведения об этих резервных копиях не удаляются из базы данных. Это приведет к ошибкам, когда программа попытается выполнить операции с резервными копиями, которых больше не существует.

Удаление всей резервной копии вместе с репликой

В разделе **Резервные копии** щелкните стрелку вниз рядом с нужной резервной копией и выберите **Удалить**.

В зависимости от типа резервной копии, эта команда либо удаляет резервную копию полностью, либо позволяет сделать выбор между двумя альтернативами: удалить резервную копию полностью (со всеми файлами) или только удалить ее из списка. При удалении резервной копии из отображаемого списка файлы резервной копии остаются на своем месте, и вы можете добавить резервную копию в список позже. Имейте в виду, что после полного удаления резервной копии восстановить ее будет невозможно.

При удалении резервной копии вместе с ней автоматически удаляется реплика. Невозможно удалить локальную резервную копию, но сохранить ее реплику. Однако можно удалить только реплику и сохранить локальную резервную копию.

Удаление всей реплики резервной копии

Реплику можно удалить вместе с исходной резервной копией или отдельно. Чтобы удалить ее вместе с резервной копией, удалите резервную копию описанным выше способом.

Чтобы удалить реплику без удаления резервной копии, в разделе **Резервные копии** щелкните стрелку вниз рядом с нужной резервной копией и выберите **Удалить только реплику**.

Автоматическая очистка версий резервных копий

1. Перейдите в раздел **Резервное копирование**.
2. Выберите в списке резервную копию, для которой следует очистить версии реплики, и нажмите кнопку **Параметры**.
3. На вкладке **Схема** выберите **Пользовательская схема**, выберите метод резервного копирования, затем щелкните **Включить автоматическую очистку**.
4. Настройте правила очистки для резервной копии.

   Дополнительные сведения см. в разделе *Пользовательские схемы*.

Примечание

После очистки некоторые вспомогательные файлы могут остаться в хранилище. Не удаляйте их!

Автоматическая очистка версий реплики

1. Перейдите в раздел **Резервное копирование**.
2. Выберите в списке резервную копию, для которой следует очистить версии реплики, и нажмите кнопку **Параметры**.
3. На вкладке **Дополнительно** откройте раздел **Репликация в Кибер Облако**.
   - Используйте параметр **Хранить не более … последних версий реплики**, чтобы указать значение, ограничивающее максимальное количество версий реплики в хранилище.
   - Установите флажок **Удалять версии, если время хранения более ...** и введите значение, ограничивающее максимальный возраст старых версий. Храниться будут только самые последние версии, а все остальные — удаляться автоматически.

Удаление версий резервных копий вручную

Чтобы удалить ненужные версии резервных копий, используйте средства, встроенные в приложение. Если удалить файлы версий не через Кибер Бэкап Старт, а, например, через проводник, то это приведет к ошибкам при операциях с резервными копиями.

Версии резервных копий в зоне безопасности Киберпротект нельзя удалить вручную.

Как очистить определенные версии резервной копии

1. Запустите Кибер Бэкап Старт.
2. В разделе **Резервная копия** щелкните стрелку вниз рядом с нужной резервной копией и выберите **Очистить версии**.

   Откроется окно **Очистка версий резервных копий**.
3. Выберите нужные версии и нажмите **Удалить**.
4. Нажмите кнопку **Удалить** в окне подтверждения.

Подождите завершения операции очистки. После очистки некоторые вспомогательные файлы могут остаться в хранилище. Не удаляйте их.

Очистка версий с зависимыми версиями

При выборе версии резервной копии для удаления необходимо учитывать, что у нее могут быть зависимые версии. В этом случае зависимые версии будут также выбраны для удаления, поскольку восстановить данные из таких версий станет невозможно.

- **Если выбрана полная версия**, программа также выберет все зависимые инкрементные и

дифференциальные версии вплоть до следующей полной версии. Другими словами, будет удалена вся цепочка версий резервной копии.

- **Если выбрана инкрементная версия**, программа также выберет все зависимые инкрементные версии в этой цепочке версий.

См. также

- *Полные, инкрементные и дифференциальные резервные копии*.
- *Удаление данных из Кибер Облака*.

Удаление данных из Кибер Облака

Поскольку свободное пространство в Кибер Облаке ограничено, необходимо своевременно удалять устаревшие или ненужные данные. Очистку можно выполнить в программе Кибер Бэкап Старт.

Удаление целой резервной копии

Наиболее радикальный способ — удаление всей резервной копии из Кибер Облака. При удалении резервной копии все ее данные полностью стираются. Удаленные данные восстановить нельзя.

Чтобы удалить всю резервную копию, щелкните стрелку вниз рядом с нужной резервной копией и выберите **Удалить**. Резервная копия будет удалена вместе со всеми версиями, настройками и расписанием.

Удаление версий резервной копии в облаке

1. Щелкните стрелку вниз рядом с резервной копией, версии которой нужно удалить, и выберите **Очистить версии**.

   Откроется список версий резервной копии.

2. Выберите версии для удаления и нажмите **Удалить**.

Примечание

Для обновления квоты в Кибер Облаке может потребоваться до одного дня.

Удаление версий реплики резервной копии в облаке

1. В разделе **Резервные копии** найдите локальную резервную копию с репликацией в облако, щелкните стрелку вниз и выберите **Очистить версии**.

   Откроется диалоговое окно «Очистка версий резервных копии».

2. В разделе **Удалить версии из** выберите **Кибер Облако**.

   Откроется список версий реплики резервной копии.

3. Выберите версии реплики для удаления и нажмите **Удалить**.

4. В диалоговом окне подтверждения нажмите кнопку **Удалить**.

Примечание

Для обновления квоты в Кибер Облаке может потребоваться до одного дня.

Восстановление данных

Восстановление дисков и разделов

Восстановление системы после аварии

Если компьютер или сервер не загружается, сначала следует попытаться найти причину с помощью советов из раздела *Попытка определения причины сбоя*. Если отказ вызван повреждением операционной системы, используйте резервную копию для восстановления системы. Выполните подготовительные действия, как описано в разделе *Подготовка к восстановлению*, и приступайте к восстановлению системы.

Попытка определения причины сбоя

Аварийный сбой системы может быть вызван двумя основными причинами:

- **Сбой оборудования**

  В этом случае будет лучше, если восстановительные работы проведет сервисный центр. Однако можно выполнить некоторые стандартные тесты. Проверьте кабели, разъемы, питание внешних устройств и т. д. Затем перезагрузите компьютер. Если это аппаратная проблема, процедура самотестирования при включении питания (POST) сообщит вам о сбое.

  Если POST не обнаружит отказов оборудования, войдите в систему BIOS и проверьте, распознает ли она системный жесткий диск. Чтобы войти в систему BIOS, нажмите нужное сочетание клавиш (`Del`, `F1`, `Ctrl+Alt+Esc`, `Ctrl+Esc` или другое в зависимости от типа BIOS) во время выполнения процедуры POST. Как правило, требуемое сочетание клавиш отображается сразу после включения компьютера. Нажав эти клавиши, вы оказываетесь в меню настройки. Перейдите в утилиту автоматического определения жестких дисков, которая обычно находится в разделе «Стандартная настройка CMOS» или «Расширенная настройка CMOS». Если утилита не обнаруживает системный диск, это означает отказ системного диска; диск необходимо заменить.

- **Повреждение операционной системы (не удается запустить Windows)**

  Если процедура POST правильно обнаружила системный жесткий диск, причиной аварийного сбоя может быть вирус, вредоносная программа или повреждение системного файла, необходимого для загрузки. В этом случае необходимо восстановить систему с резервной копии системного диска или системного раздела. Дополнительные сведения см. в разделе *Восстановление системы*.

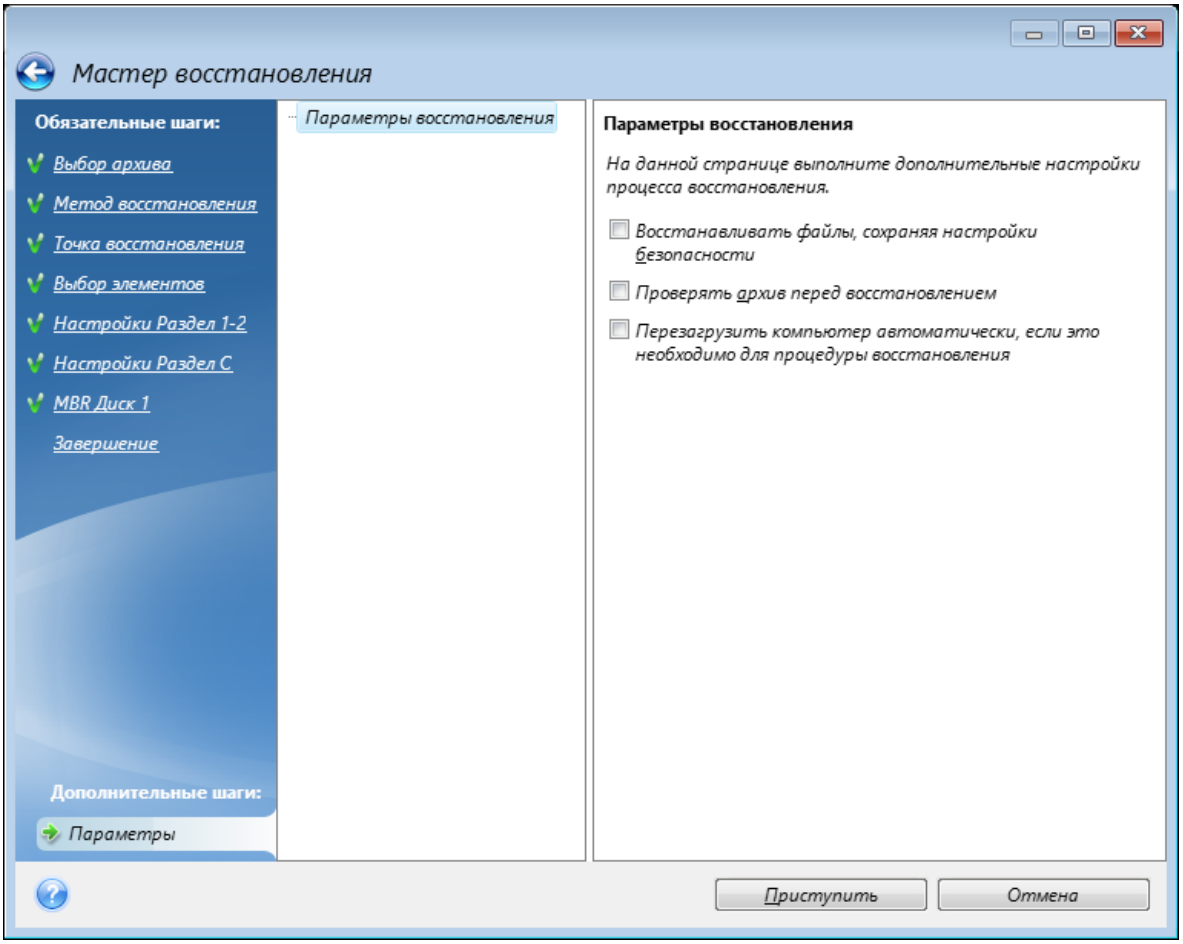
Подготовка к восстановлению

Рекомендуется выполнить следующие действия перед восстановлением:

- Просканируйте компьютер на вирусы, если есть подозрение, что сбой системы произошел из-за вирусной атаки или вредоносной программы.
- С помощью загрузочного носителя попробуйте выполнить тестовое восстановление на запасной жесткий диск (при его наличии).
- Проверьте резервную копию, используя загрузочный носитель. Резервная копия, которая может быть прочитана в ОС Windows, **не всегда может быть читаема в среде Linux**.

  При работе с загрузочного носителя существует два способа проверить резервную копию:

  - Чтобы проверить резервную копию вручную, на вкладке **Восстановление** щелкните правой кнопкой резервную копию и выберите **Проверить архив**.
  - Чтобы автоматически проверить резервную копию перед восстановлением, на шаге **Параметры мастера восстановления** установите флажок **Проверять архив перед восстановлением**.



- Назначайте всем разделам на жестких дисках уникальные имена (метки). Это облегчит поиск

диска, содержащего резервные копии.

При использовании загрузочного носителя присвоенные программой буквы дисков могут отличаться от букв тех же дисков в Windows. Например, диск D: при работе с загрузочного носителя может соответствовать диску E: в Windows.

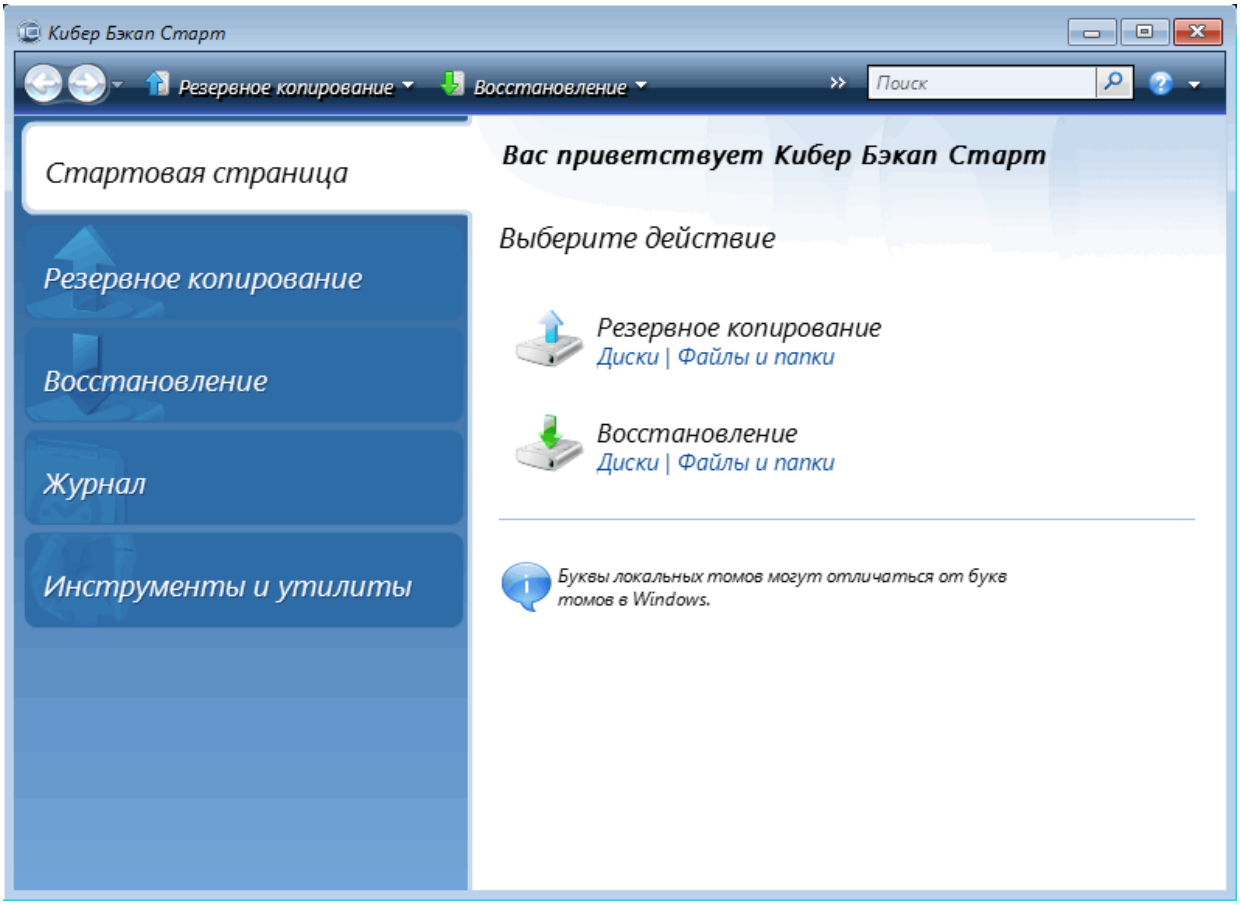
Восстановление системы на тот же диск

Перед началом работы рекомендуется выполнить процедуры, описанные в разделе *Подготовка к восстановлению*.

Как восстановить систему:

1. Если восстанавливаемая резервная копия находится на внешнем диске, подключите этот диск к компьютеру и убедитесь, что диск включен.
2. Измените порядок загрузки в BIOS так, чтобы сделать загрузочный носитель (CD, DVD или флеш-накопитель USB) первым устройством загрузки. См. раздел *Настройка порядка загрузки в BIOS или UEFI BIOS*.

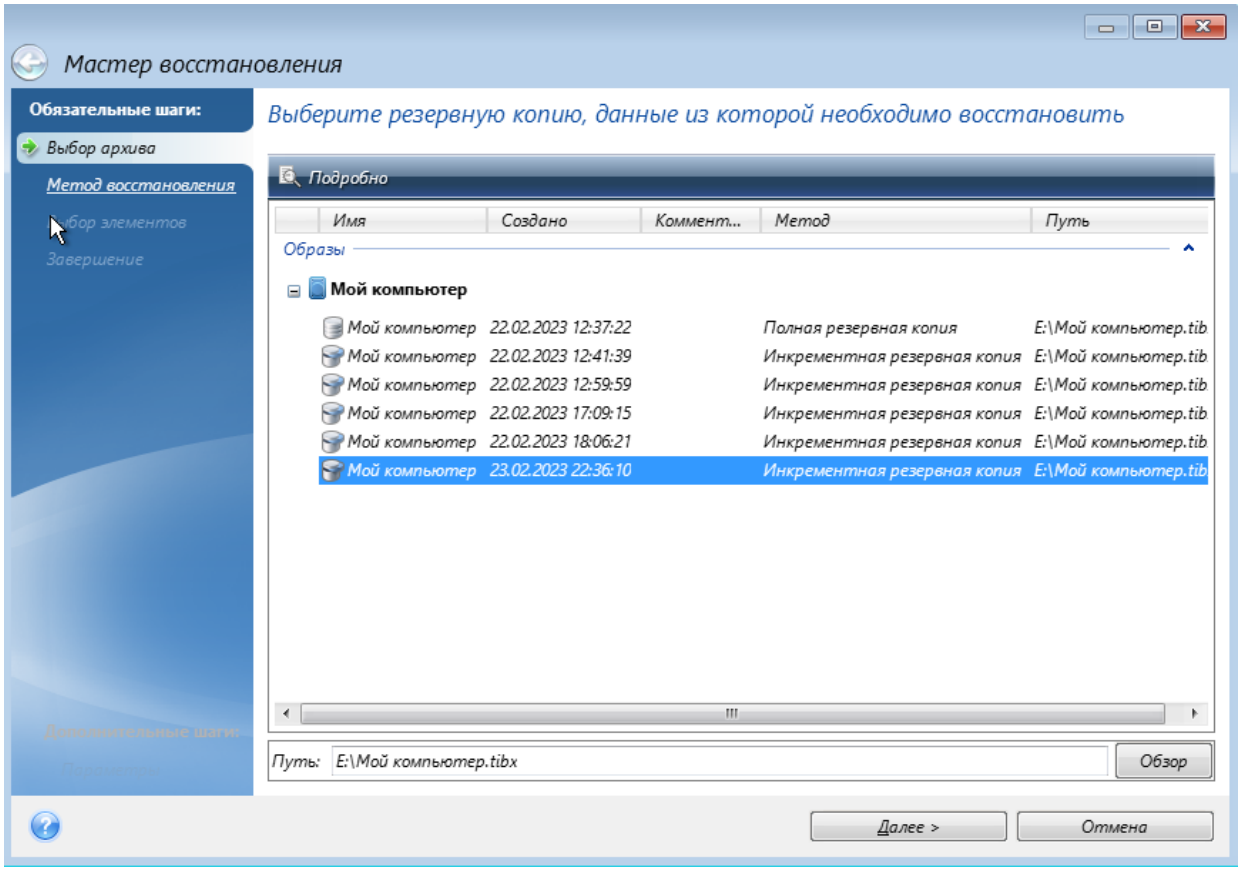
   Если вы используете компьютер UEFI, обратите внимание на режим загрузки носителя в UEFI BIOS. Рекомендуется использовать режим загрузки, соответствующий типу операционной системы в резервной копии. Если резервная копия содержит систему BIOS, загрузите носитель в режиме BIOS; если систему UEFI, то убедитесь, что установлен режим UEFI.
3. Выполните загрузку, используя загрузочный носитель.
4. На **главном экране** выберите **Диски** под заголовком **Восстановление**.



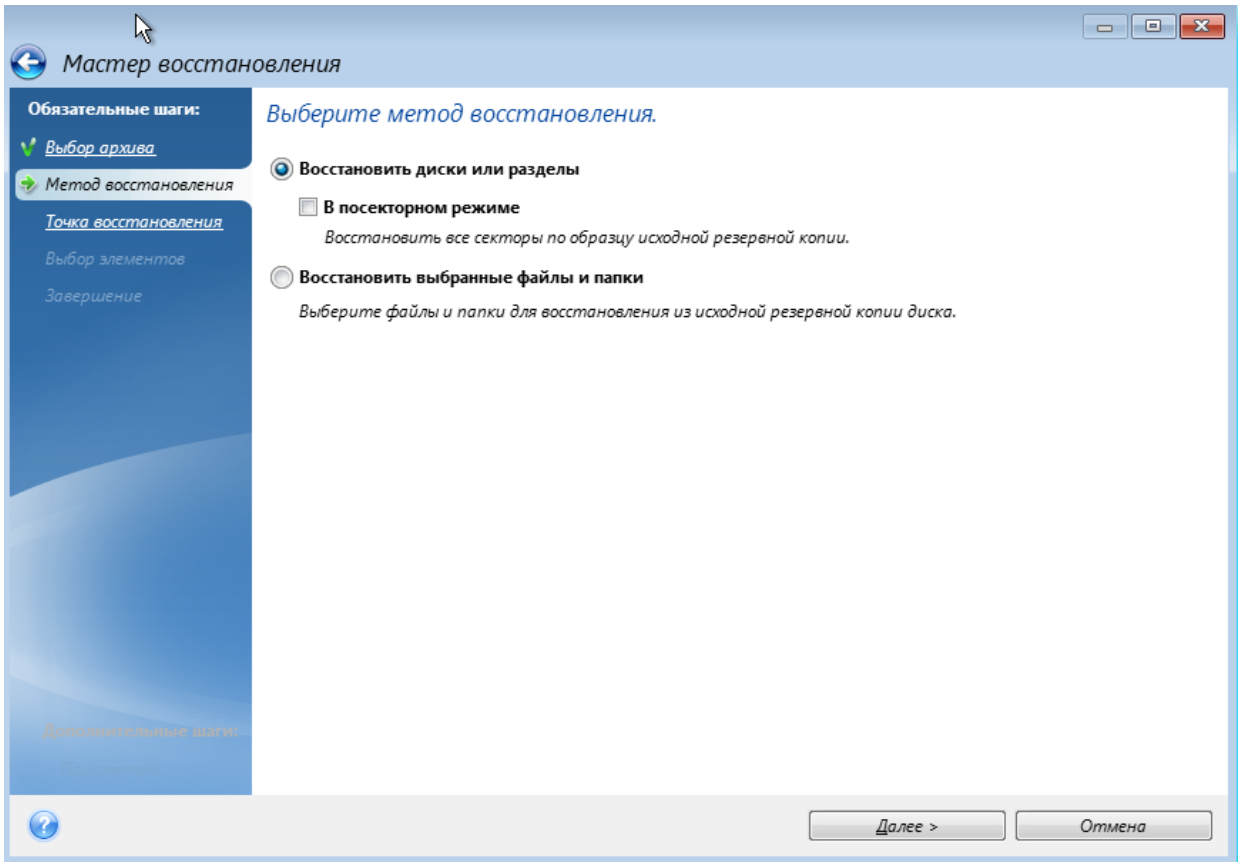
5. На шаге **Выбор архива** выберите резервную копию системного диска или раздела, которая будет использоваться для восстановления.

   Если резервная копия не отображается, нажмите кнопку **Обзор** и укажите путь к резервной копии вручную.

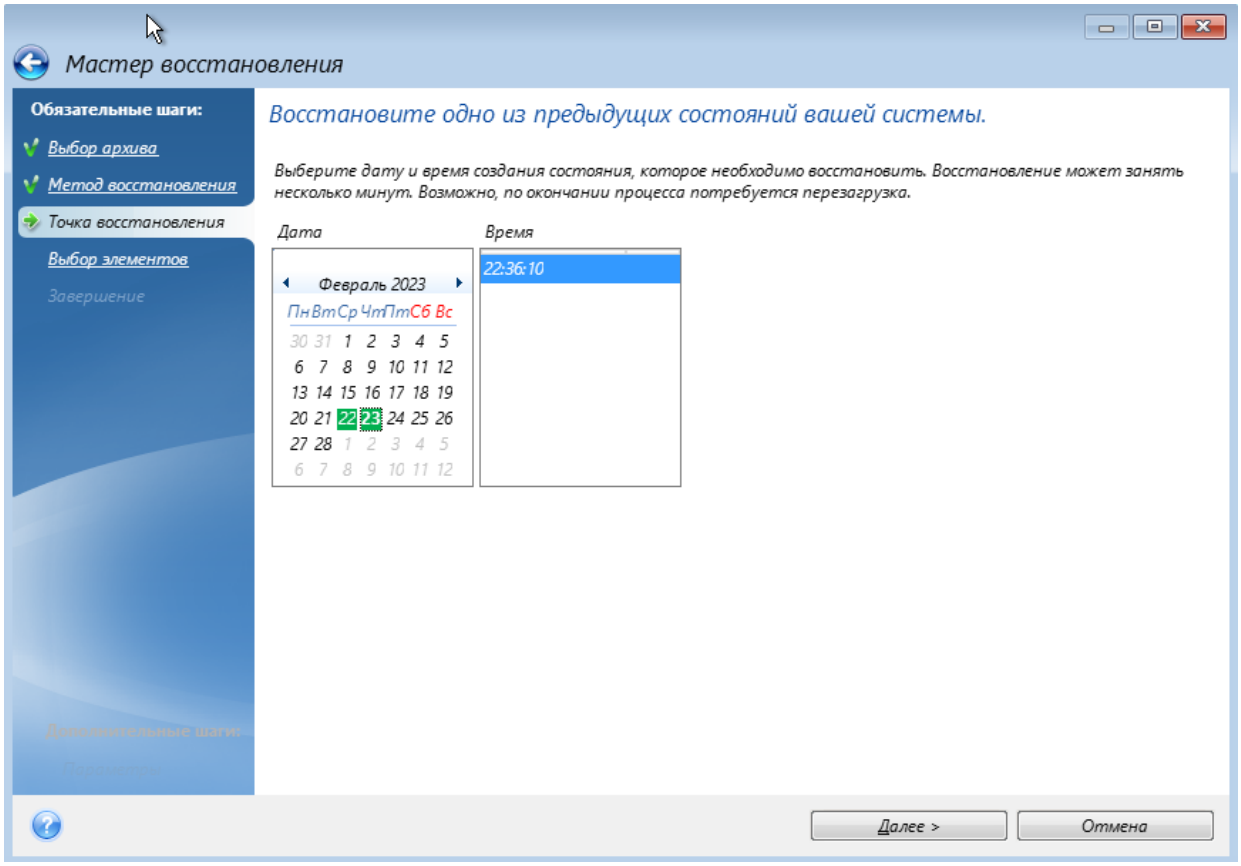
> **Примечание**
>
> Если резервная копия расположена на USB-накопителе и этот накопитель не распознается правильно, проверьте версию порта USB. Если это USB 3.0 или USB 3.1, попробуйте подключить накопитель к порту USB 2.0.



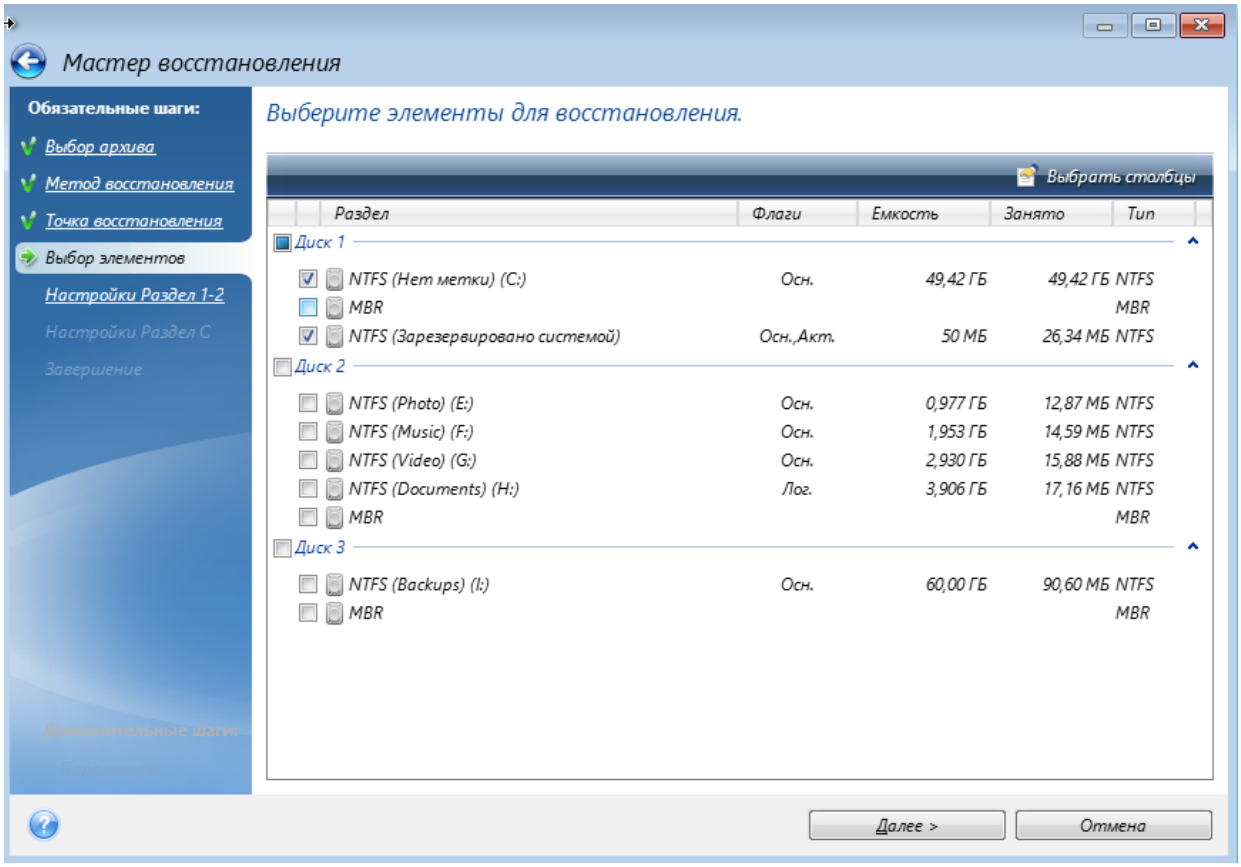
6. На шаге **Метод восстановления** выберите **Восстановить диски или разделы**.



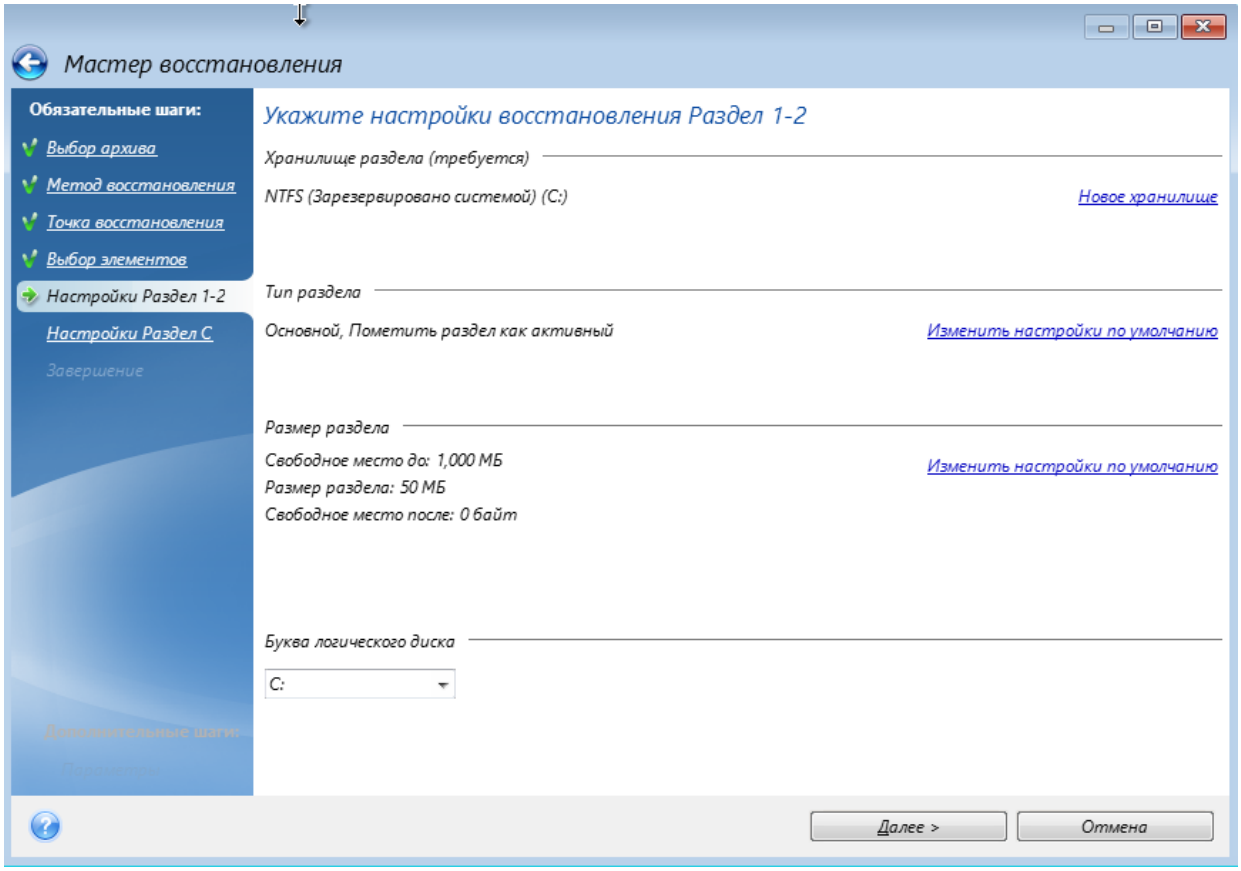
7. На шаге **Точка восстановления** выберите дату и время, на которые следует восстановить систему.

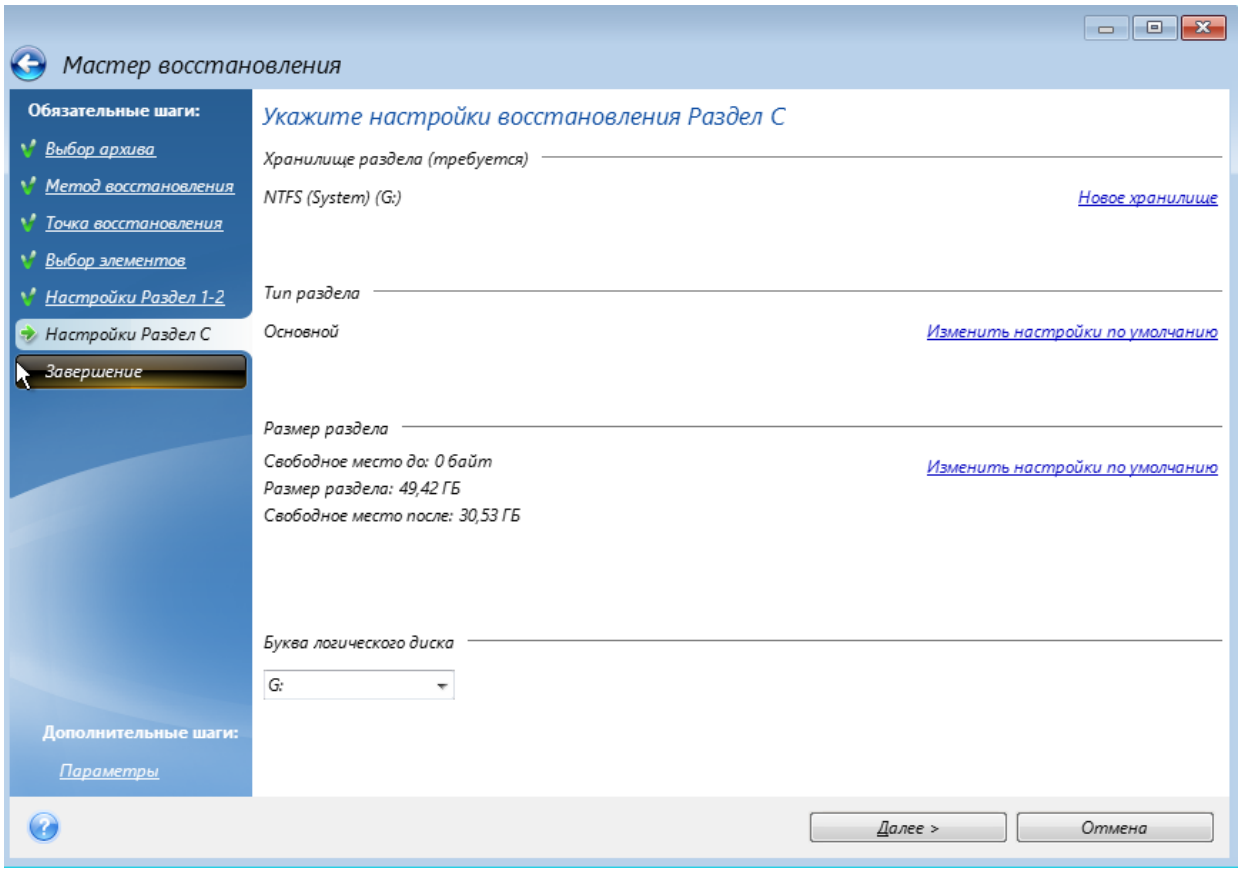


8. На шаге **Выбор элементов** выберите системный раздел (обычно диск C). Если буква диска, назначенная системному разделу, иная, отметьте галочкой необходимый раздел в столбце **Флаги**. Системный раздел должен иметь флаги **Осн.**, **Акт.**. Если есть раздел «Зарезервировано системой», выберите его тоже.



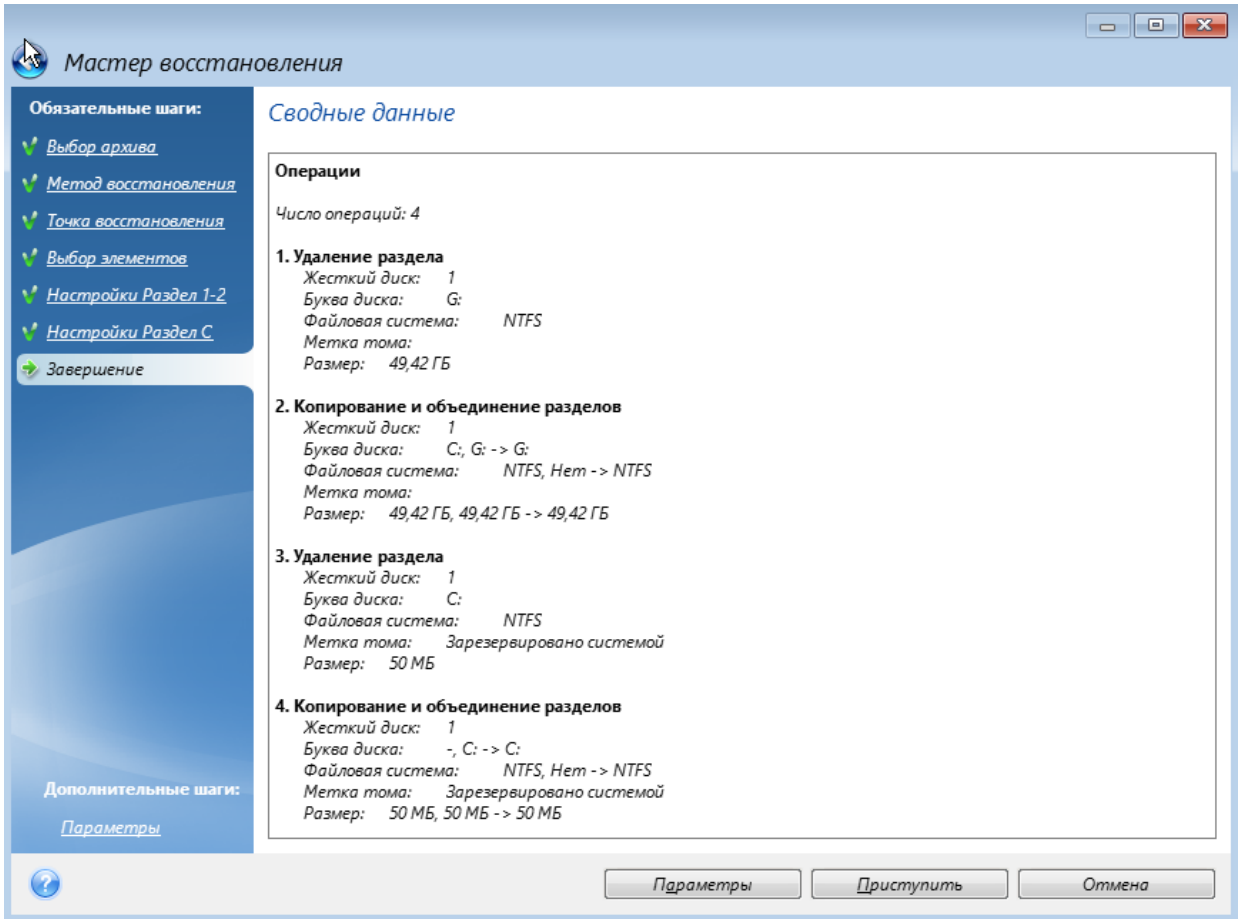
9. На шаге **Настройки Раздел C** (или другая буква системного раздела) проверьте правильность настроек по умолчанию и нажмите **Далее**. Или измените настройки, прежде чем нажимать кнопку **Далее**. Изменение настроек потребуется для восстановления на новый жесткий диск другой емкости.





10. Внимательно прочитайте перечень операций на последнем шаге **Завершение**. Если размер

восстанавливаемого раздела не был изменен, то обратите внимание, что размеры разделов в значениях **Удаление раздела** и **Копирование и объединение разделов** должны совпадать. Ознакомившись с перечнем операций, нажмите кнопку **Приступить**.



11. После завершения операции выйдите из автономной версии Кибер Бэкап Старт, извлеките загрузочный носитель и загрузите компьютер с восстановленного системного раздела. Когда вы убедитесь, что ОС Windows восстановлена до нужного состояния, восстановите исходный порядок загрузки.

Восстановление системы на новый диск при работе с загрузочного носителя

Перед началом работы рекомендуется выполнить процедуры, описанные в разделе *Подготовка к восстановлению*. Форматировать новый диск не нужно, так как это будет сделано в процессе восстановления.

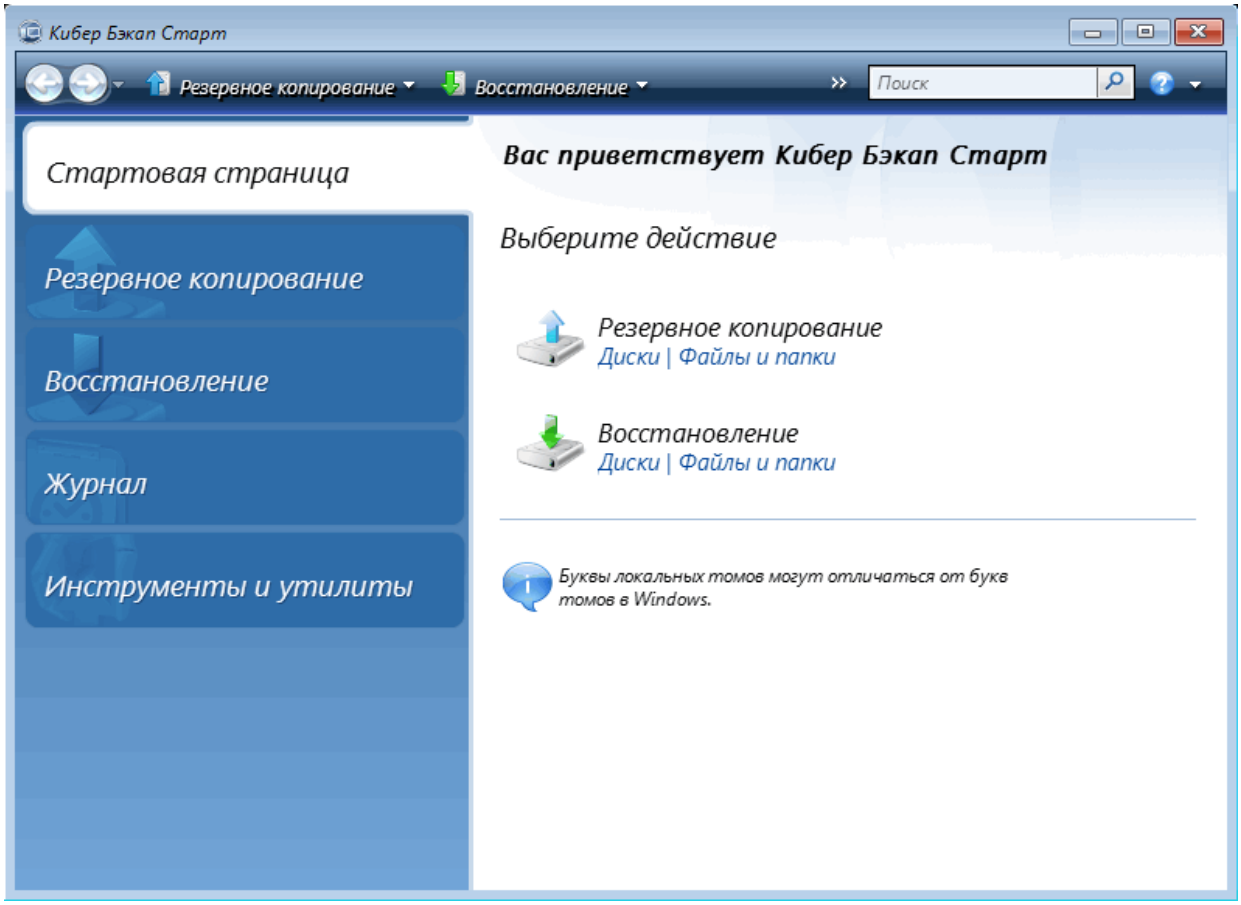
Примечание

Рекомендуется, чтобы старый и новый диски работали в одном режиме контроллера (например, IDE или AHCI). Иначе компьютер может не загружаться с нового жесткого диска.

Как восстановить систему на новый диск:

1. Установите новый жесткий диск на то же место в компьютере при помощи того же кабеля и разъема, которые использовались для исходного диска. Если это невозможно, установите новый диск в то место, где он будет использоваться.
2. Если восстанавливаемая резервная копия находится на внешнем диске, подключите этот диск к компьютеру и убедитесь, что диск включен.
3. Измените порядок загрузки в BIOS так, чтобы сделать загрузочный носитель (CD, DVD или флеш-накопитель USB) первым устройством загрузки. См. раздел *Настройка порядка загрузки в BIOS или UEFI BIOS*.

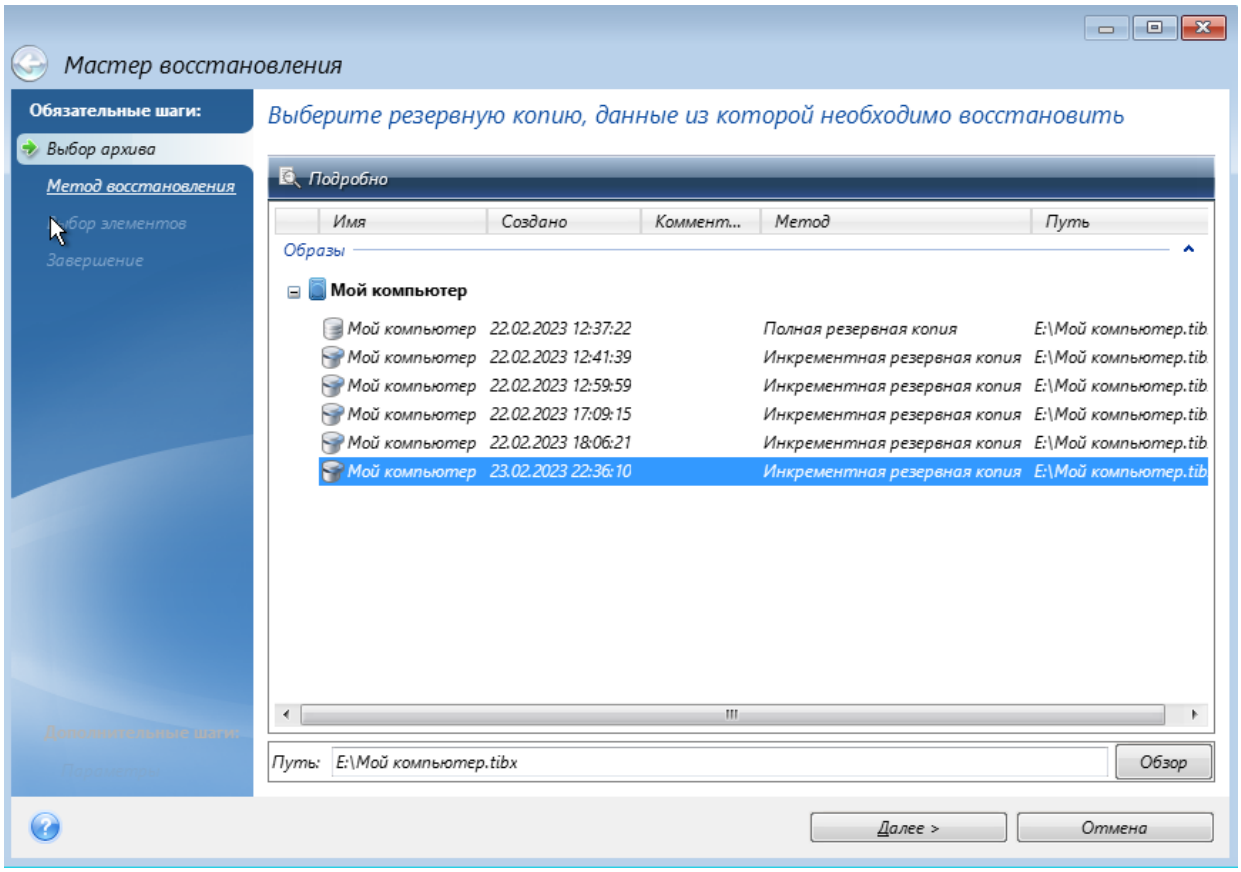
   Если вы используете компьютер UEFI, обратите внимание на режим загрузки носителя в UEFI BIOS. Рекомендуется использовать режим загрузки, соответствующий типу операционной системы в резервной копии. Если резервная копия содержит систему BIOS, загрузите носитель в режиме BIOS; если систему UEFI, то убедитесь, что установлен режим UEFI.
4. Выполните загрузку, используя загрузочный носитель.
5. На **главном экране** выберите **Диски** под заголовком **Восстановление**.



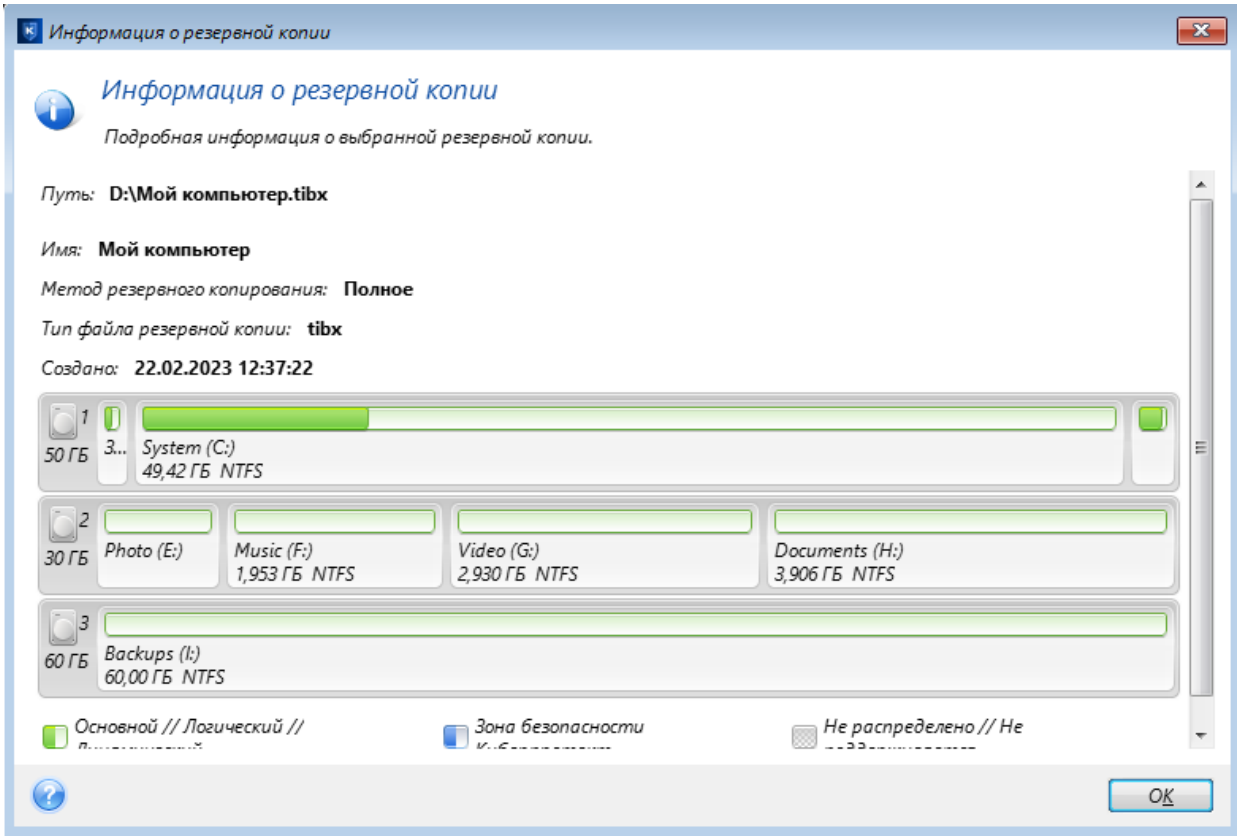
6. На шаге **Выбор архива** выберите резервную копию системного диска или раздела, которая будет

использоваться для восстановления. Если резервная копия не отображается, нажмите кнопку **Обзор** и укажите путь к резервной копии вручную.

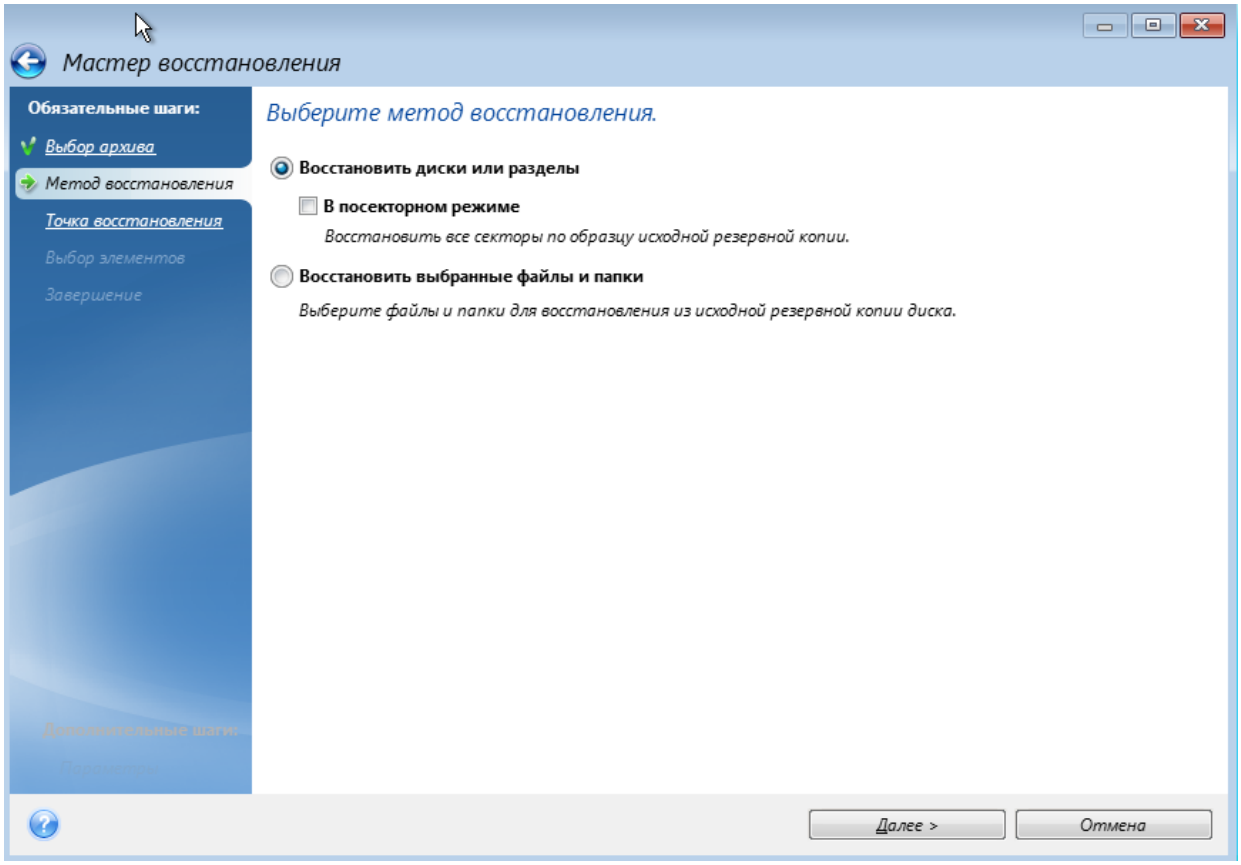
> **Примечание**
>
> Если резервная копия расположена на USB-накопителе и этот накопитель не распознается правильно, проверьте версию порта USB. Если это USB 3.0 или USB 3.1, попробуйте подключить накопитель к порту USB 2.0.



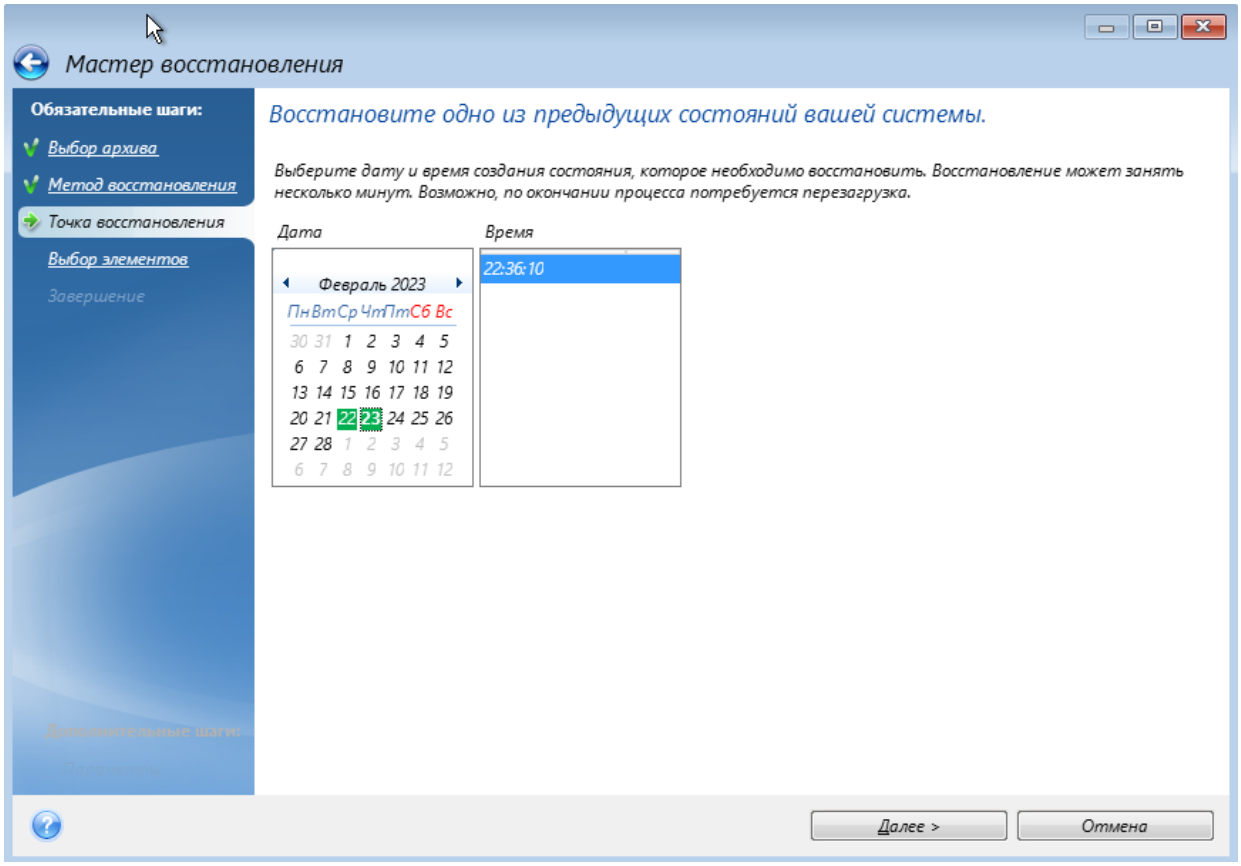
7. Если на диске есть скрытый раздел (например раздел «Зарезервировано системой» или раздел, созданный производителем компьютера), нажмите кнопку **Подробно** на панели инструментов мастера. Запомните расположение и размер скрытого раздела, так как эти параметры должны быть такими же на новом диске.



8. На шаге **Метод восстановления** выберите **Восстановить диски или разделы**.

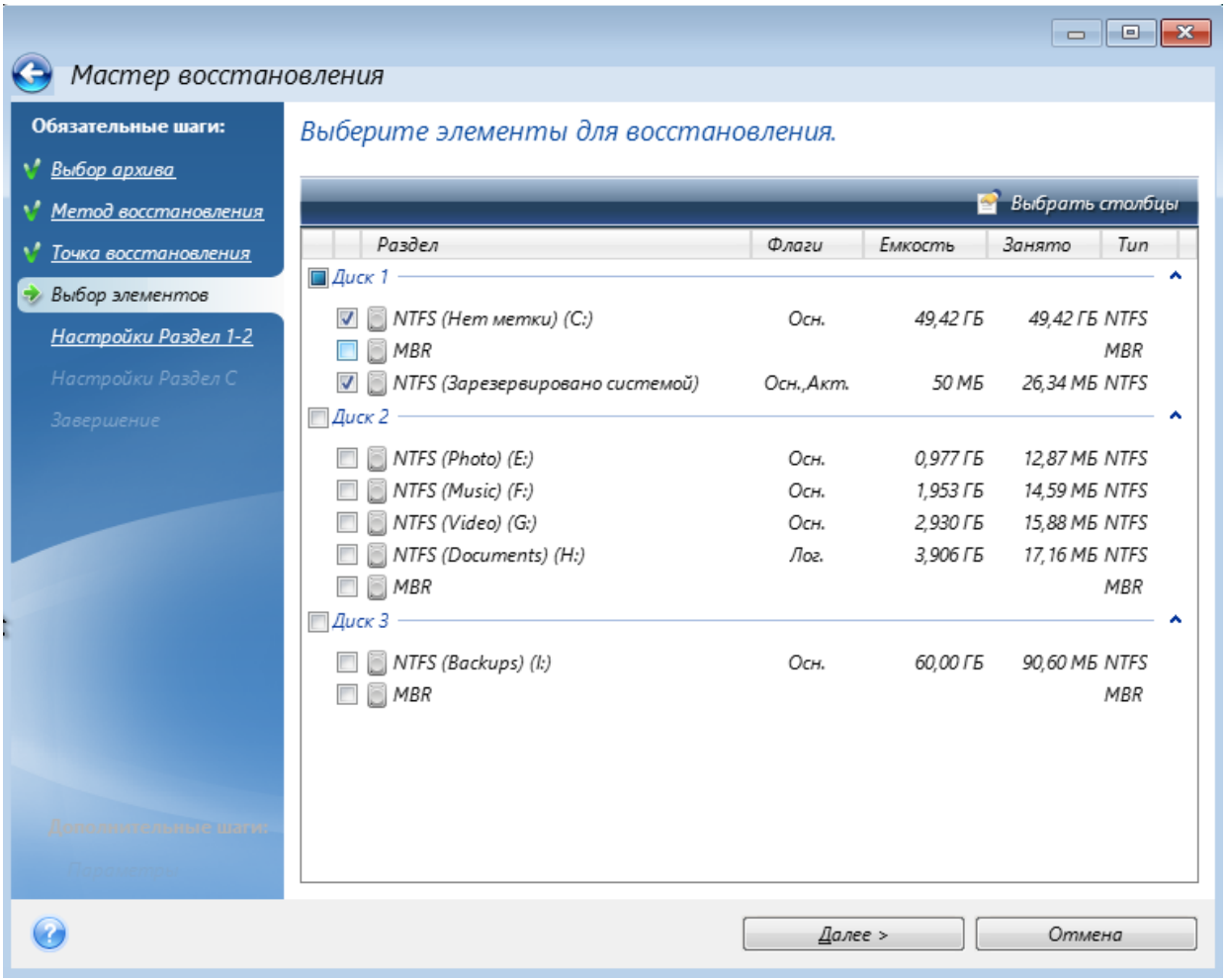


9. На шаге **Точка восстановления** выберите дату и время, на которые следует восстановить систему.



10. На шаге **Выбор элементов** установите флажки напротив нужных разделов.

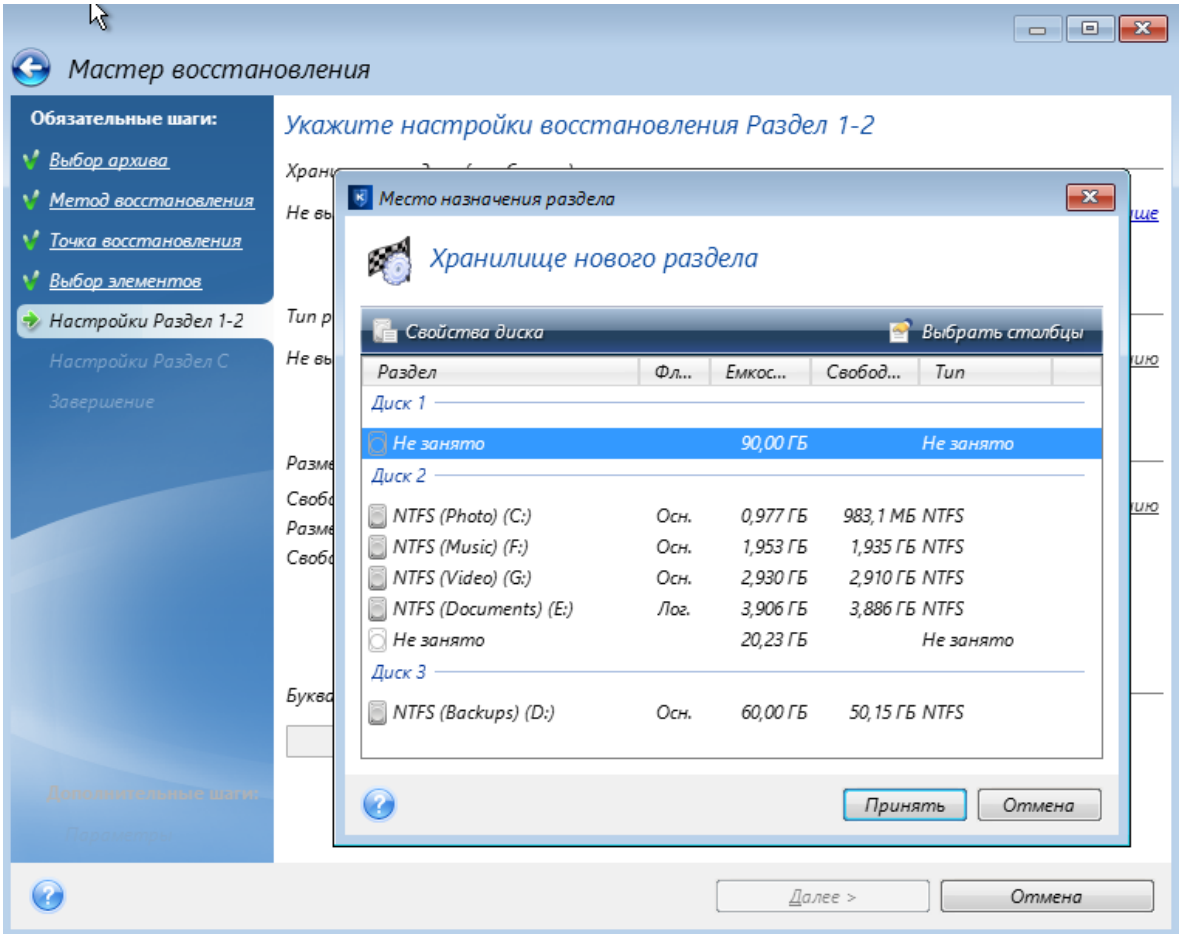
    Если выбран целый диск, то MBR и дорожка 0 этого диска также будут восстановлены.



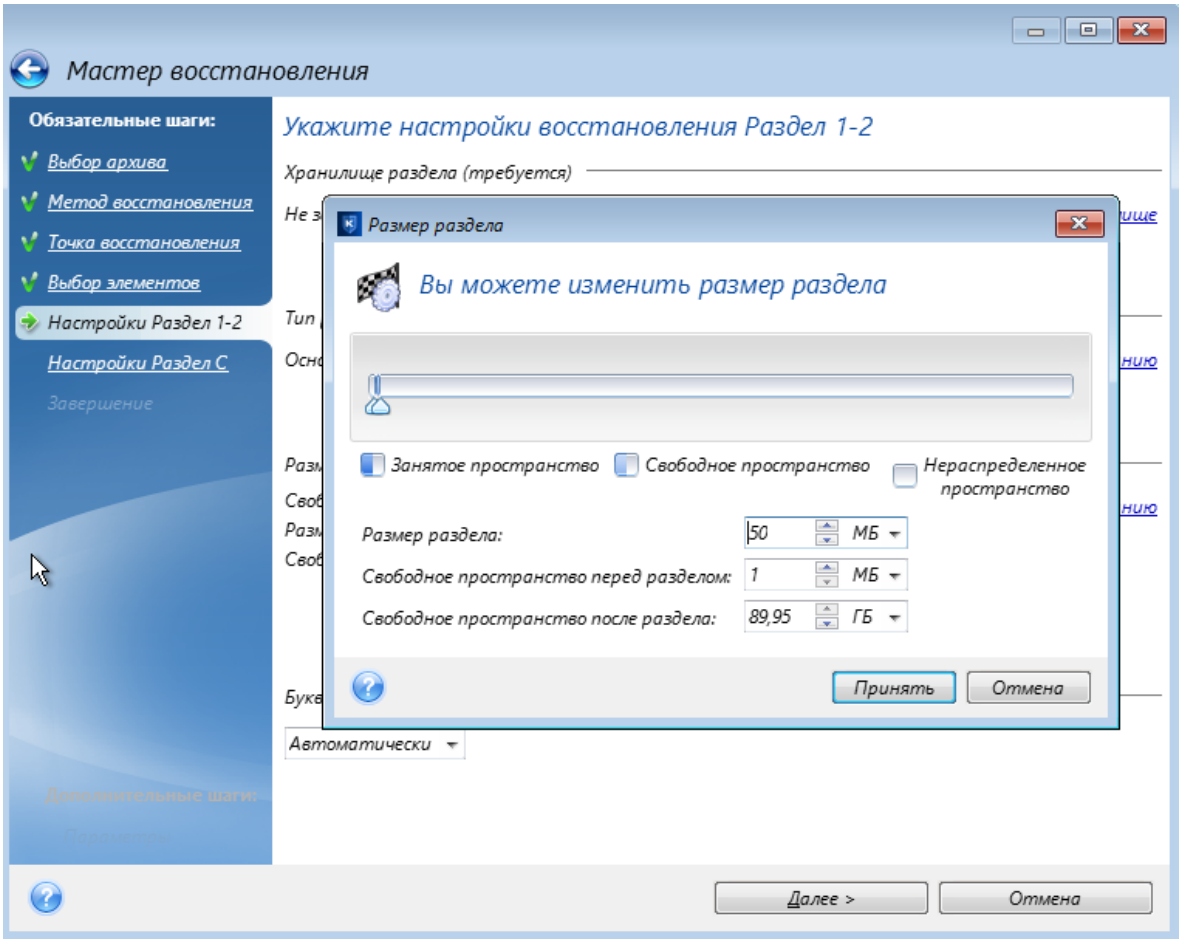
После выбора разделов появятся соответствующие шаги **Настройки раздела**. Данные шаги начинаются с разделов, которым не присвоены буквы дисков (обычно скрытые разделы относятся к этой категории). Затем разделы указываются в восходящем порядке букв дисков, присвоенных разделам. Этот порядок нельзя изменить. Порядок отображения разделов в программе не обязательно совпадает с физическим порядком расположения разделов на жестком диске.

11. На шаге настроек скрытого раздела (обычно «Настройки раздела 1-1») укажите следующие параметры.

    - **Хранилище** — щелкните **Новое хранилище**, выберите новый диск по присвоенному имени или емкости и нажмите кнопку **Принять**.

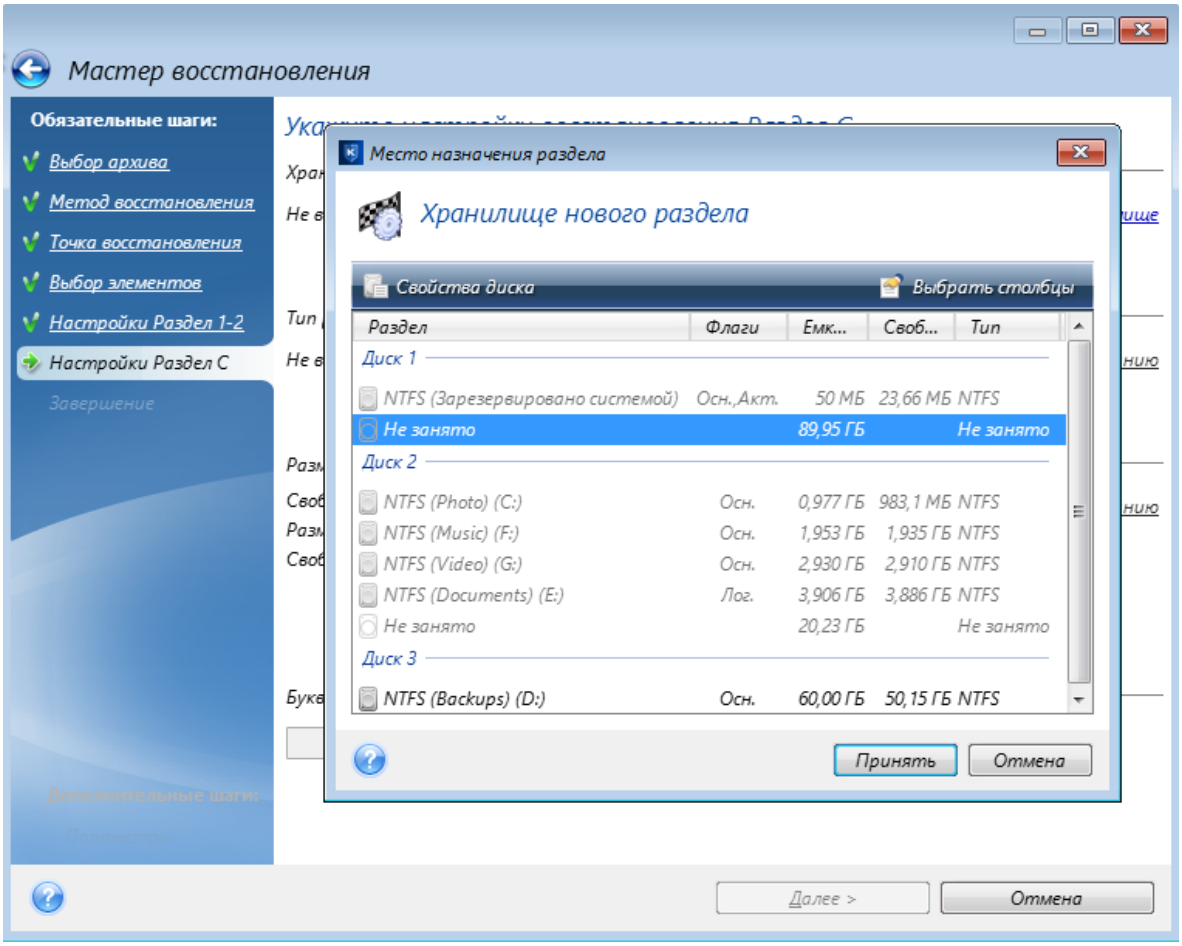


- **Тип** — проверьте тип раздела и измените его при необходимости. Убедитесь, что раздел «Зарезервировано системой» (если есть) является основным и помечен как активный.
- **Размер раздела** — в области «Размер раздела» щелкните **Изменить настройки по умолчанию**. По умолчанию раздел будет занимать весь новый диск. Введите правильное значение в поле «Размер раздела» (это значение показывается на шаге **Выбор элементов**). При необходимости перетащите раздел в расположение, которое было показано в окне «Информация о резервной копии». Нажмите кнопку **Принять**.



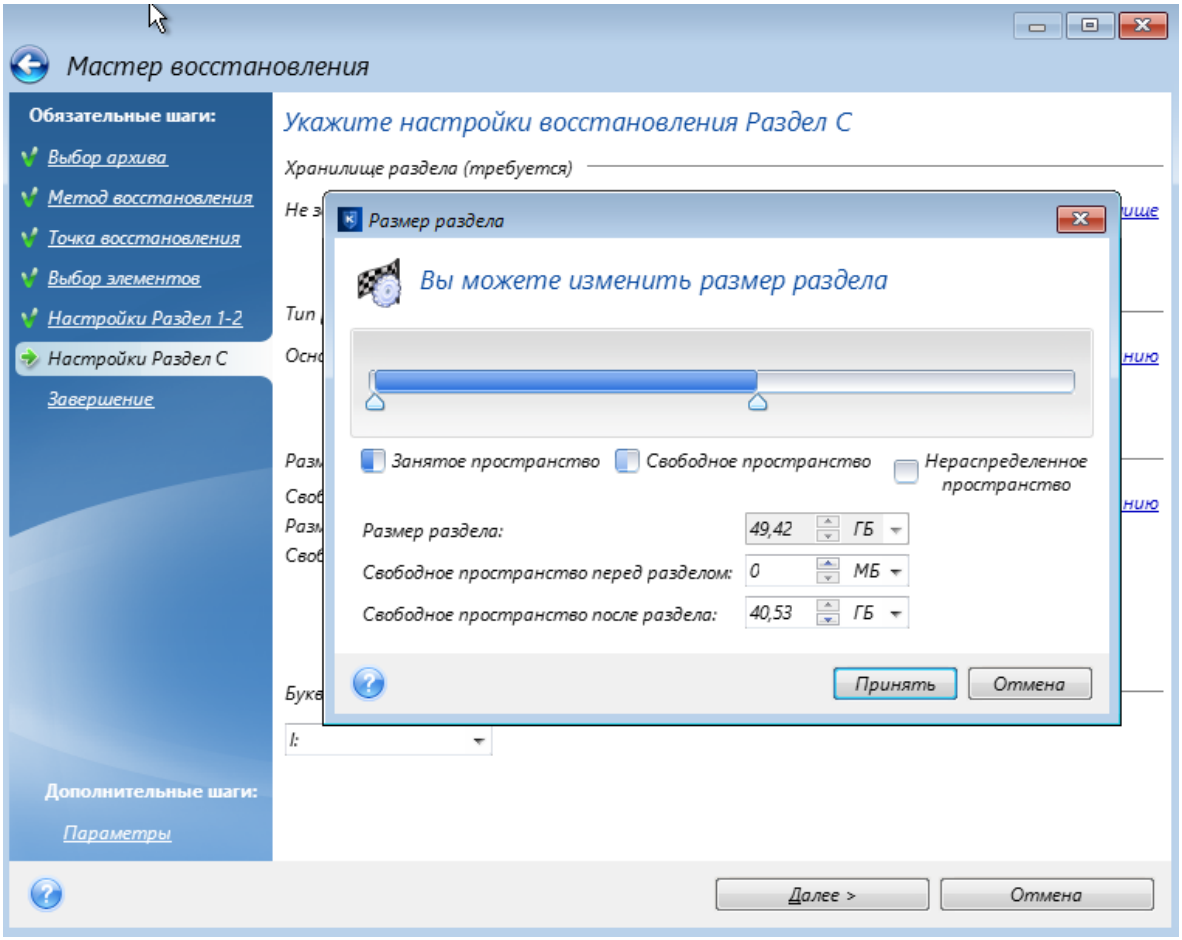
12. На шаге **Настройки раздела С** укажите настройки для второго раздела, который в данном случае является системным.

    a. Нажмите кнопку **Новое хранилище** и выберите нераспределенное пространство на целевом диске, где будет восстановлен раздел.

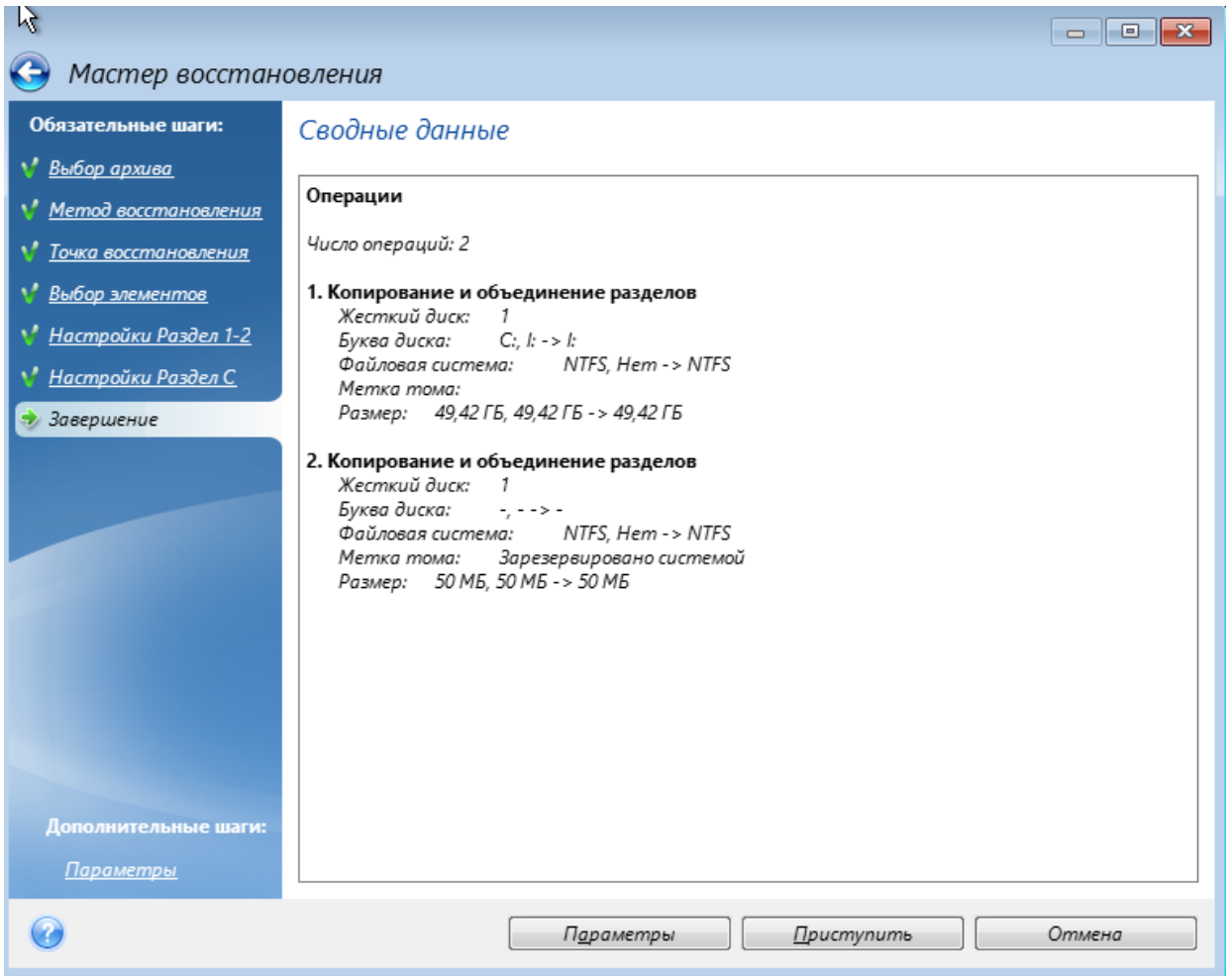


b. При необходимости измените тип раздела. Системный раздел должен быть основным.

c. Укажите размер раздела, который по умолчанию равен его исходному размеру. Обычно после раздела не бывает свободного пространства, поэтому все нераспределенное пространство следует выделить второму разделу. Нажмите кнопку **Принять**, а затем **Далее**.



13. На шаге **Завершение** внимательно прочтите перечень операций, подлежащих выполнению, а затем нажмите кнопку **Приступить**.



После завершения восстановления

Перед загрузкой компьютера отключите старый диск (если он подключен). Если во время загрузки Windows обнаружит и новый, и старый диск, это приведет к ошибке загрузки системы. Если система переносится со старого диска на новый большей емкости, до первой загрузки системы старый диск должен быть отключен.

Извлеките загрузочный носитель и загрузите Windows на компьютере. Возможно, система отобразит сообщение об обнаружении нового устройства (жесткого диска) и о перезагрузке Windows. Убедитесь, что система работает нормально, и восстановите первоначальный порядок загрузки.

Восстановление дисков и разделов

Можно восстанавливать диски из резервных копий, расположенных в локальном или сетевом хранилище либо в Кибер Облаке.

Примечание

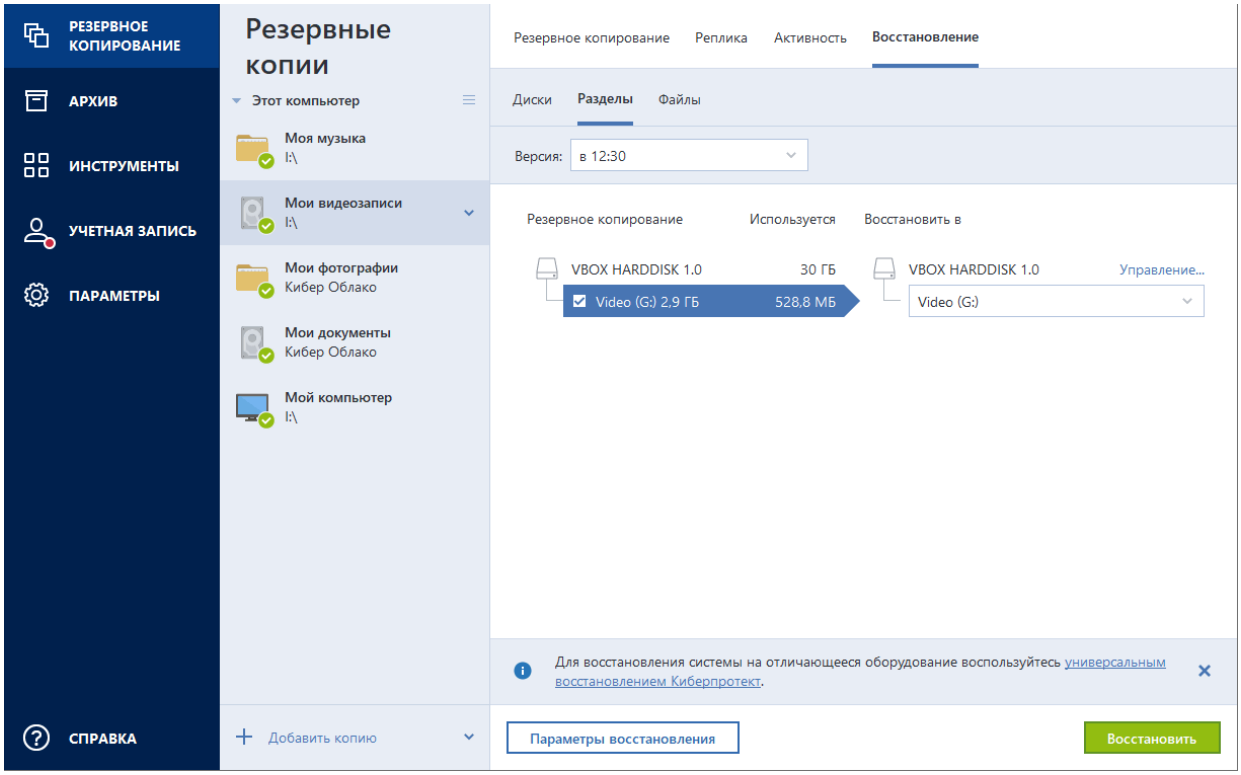
В зависимости от скорости подключения к Интернету восстановление диска из Кибер Облака может занять длительное время.

Ограничения:

- Содержимое резервных копий с файловой системой ExFAT не отображается в Проводнике Windows и в Кибер Бэкап Старт.
- При работе с резервными копиями с файловой системой ExFAT диски ExFAT блокируются в Проводнике. При попытке открыть их отображается сообщение ”Отказано в доступе”.

Как восстановить разделы или диски:

1. Запустите Кибер Бэкап Старт.
2. Для восстановления данных из Кибер Облака должен быть выполнен вход в учетную запись Киберпротект.
3. В разделе **Резервные копии** выберите резервную копию, содержащую разделы или диски, которые требуется восстановить, откройте вкладку **Восстановление**.
4. В списке **Версия** выберите нужную версию по дате и времени создания резервной копии.



5. Выберите вкладку **Диски** для восстановления дисков или вкладку **Разделы** для восстановления отдельных разделов. Выберите объекты, которые необходимо восстановить.

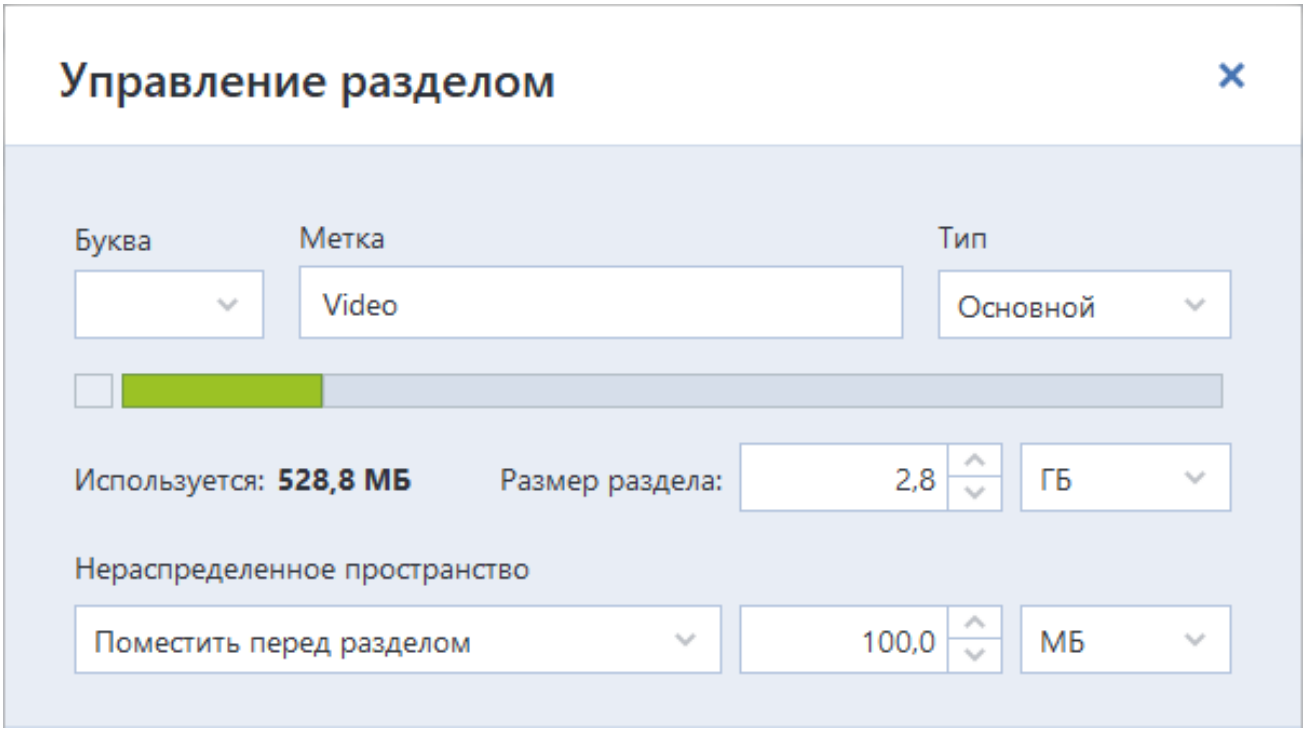
6. В поле пути восстановления под именем раздела выберите целевой раздел. Неподходящие разделы помечаются красной рамкой. Все данные на целевом разделе будут потеряны, так как будут заменены восстановленными данными и файловой системой.

> **Примечание**
>
> Для восстановления на исходный раздел на нем должно быть не менее 5% свободного пространства. Иначе кнопка **Восстановить** будет недоступна.

7. [Необязательно] Чтобы задать дополнительные параметры для процесса восстановления диска, щелкните **Параметры восстановления**.
8. Закончив выбор, нажмите кнопку **Восстановить**, чтобы начать восстановление.

Свойства раздела

При восстановлении разделов на базовый диск можно изменить свойства этих разделов. Чтобы открыть окно **Управление разделом**, щелкните **Управление** рядом с выбранным целевым разделом.



Можно изменить следующие свойства раздела:

- **Буква**
- **Метка**
- **Тип**

Раздел можно сделать основным, основным активным или логическим.

- **Размер**

  Чтобы изменить размер раздела, перетащите его правую границу мышью на горизонтальной полосе в окне. Чтобы задать определенный размер раздела, введите нужное число в поле **Размер раздела**. Также можно выбрать расположение нераспределенного пространства — до или после раздела.

Интерфейс UEFI

С помощью Кибер Бэкап Старт также можно преобразовывать системы **BIOS** в **UEFI**.

Что такое UEFI?

Интерфейс UEFI является спецификацией, которая обеспечивает взаимодействие программ за счет определения стандартного синтаксиса для загрузочных служб и служб времени выполнения. Дополнительные сведения о UEFI см. на сайте https://www.uefi.org.

Почему UEFI?

- **Совместимость с BIOS** — системы на основе UEFI по-прежнему могут загружать операционные системы на основе BIOS за счет модуля поддержки совместимости CSM.
- **Загрузка с больших дисков** — системы на основе UEFI поддерживают структуру разделов GPT, которая может работать с дисками, содержащими более 2^32 секторов.
- **Независимая архитектура ЦП** — UEFI работает одинаково для всех типов архитектуры процессоров.
- **Независимые драйверы ЦП** — спецификация UEFI включает байтовый код EFI (EBC) и позволяет создавать образы EBC (драйверы), которые работают на любой системе.
- **Гибкая среда до загрузки операционной системы** — системы на основе UEFI могут загружаться на любом оборудовании.
- **Модульная конструкция** — UEFI позволяет обновлять один компонент, не оказывая влияния на другие.

Примечание

Поскольку интерфейс UEFI является новой технологией, не все системы могут работать с ней. Обратитесь к разработчику оборудования, чтобы выяснить, поддерживает ли используемый компьютер технологию UEFI.

Как включить UEFI в BIOS?

Ниже приводится описание включения и отключения UEFI в BIOS.

1. Войдите в программу настройки BIOS, нажав клавишу, упомянутую в сообщении на экране во время загрузки. Обычно это клавиша `Del` или `F2`.
2. Вызовите меню **Boot Options** (Параметры загрузки).
3. Откройте элемент **UEFI Booting** (Загрузка UEFI) и выберите пункт **Enable** (Включить) (или **Disable** (Отключить), если необходимо **отключить** UEFI в системе).
4. Перейдите к пункту **Save & Exit Setup** (Сохранить и выйти из программы настройки) и нажмите клавишу `Enter` для сохранения изменений и загрузки системы.

Если для включения UEFI требуется помощь, обратитесь к производителю оборудования.

Как перенести исходную систему на жесткий диск большего размера?

Кибер Бэкап Старт позволяет перенести или восстановить систему из ранее созданного архива на жесткий диск, содержащий более 2^32 секторов (2 ТБ для дисков со стандартным размером логического сектора 512 байт или 16 ТБ для дисков с размером логического сектора 4 КБ (4096 байт)).

Это можно сделать с помощью загрузочного носителя Киберпротект или посредством загрузки операционной системы на основе UEFI, в которой установлена программа Кибер Бэкап Старт.

Как перенести систему с помощью носителя Киберпротект:

1. Загрузите систему с загрузочного носителя Киберпротект.
2. Выберите в меню загрузки Кибер Бэкап Старт (полная версия), чтобы продолжить загрузку с носителя.
3. Запустите необходимый мастер (**Восстановление** или **Клонирование**) и следуйте инструкциям.

Как перенести систему в операционной системе на основе UEFI:

1. Загрузите операционную систему Windows, поддерживающую UEFI.
2. Запустите Кибер Бэкап Старт, перейдите на вкладку **Резервное копирование и восстановление**, щелкните **Восстановить** на панели инструментов и следуйте инструкциям.

Структуры разделов

Структура разделов определяет, как операционная система организует разделы на жестком диске.

- **MBR (основная загрузочная запись)** — загрузочный сектор размером 512 байт, который является первым сектором жесткого диска и используется для размещения таблицы основных разделов

диска.

MBR является стандартной схемой секционирования и используется на большинстве жестких дисков. Основным ограничением MBR является то, что эта схема не поддерживает жесткие диски размером более 2 ТБ, то есть не подходит для современных больших жестких дисков, и дисковое пространство свыше 2 ТБ остается недоступным для пользователей.

- **GPT (схема разделов GUID)** — это новый стандарт для структуры разделов жестких дисков.

  GPT поддерживает диски и разделы размером до 9,4 ЗБ (9,4 x 10^21 байт).

Таблица 1. Целевой диск больше 2 ТБ

В таблице ниже отображены возможные варианты миграции содержимого исходного диска на жесткий диск большого размера (свыше 2 ТБ).

Если исходный диск является MBR-диском, необходимо выбрать, оставить ли его MBR-диском или преобразовать в GPT с помощью Кибер Бэкап Старт.

Каждый из вариантов обладает своими преимуществами и ограничениями в зависимости от параметров системы. В основном это касается загружаемости с целевого диска и способности использовать все пространство на больших дисках.

	Моя система загружается с помощью BIOS (Windows или загрузочный носитель)	Моя система загружается с помощью UEFI (Windows или загрузочный носитель)
Мой исходный диск является диском MBR, а ОС не поддерживает UEFI	Стилем разделов после клонирования останется MBR, в клонированной операционной системе будет установлен драйвер Киберпротект Bus. Кроме того, невозможно будет использовать дисковое пространство за пределами 2 ТБ, поскольку MBR не поддерживает жесткие диски размером более 2 ТБ. Чтобы использовать все дисковое пространство, необходимо изменить стиль разделов на GPT или перезапустить Кибер Бэкап Старт после завершения операции и с помощью диспетчера дисков расширенной емкости Киберпротект сделать дисковое пространство сверх 2 ТБ видимым для мастера добавления новых дисков.	Выберите один из требуемых методов миграции: • **Копировать исходный раздел без изменений** Стилем разделов останется MBR, но по завершении операции операционная система не загрузится из UEFI. В клонированной операционной системе будет установлен драйвер Киберпротект Bus. Кроме того, невозможно будет использовать дисковое пространство за пределами 2 ТБ, поскольку MBR не поддерживает жесткие диски размером более 2 ТБ. Чтобы использовать все дисковое пространство, необходимо изменить стиль разделов на GPT или перезапустить Кибер Бэкап Старт после завершения операции и с помощью диспетчера дисков расширенной емкости Киберпротект сделать дисковое пространство сверх 2 ТБ видимым для мастера добавления новых дисков. • **Преобразовать стиль разделов в GPT** Целевой раздел будет преобразован в стиль GPT. Он может использоваться в качестве несистемного диска, так как ваша операционная система не поддерживает UEFI. Все пространство диска будет доступно.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

	Моя система загружается с помощью BIOS (Windows или загрузочный носитель)	**Моя система загружается с помощью UEFI (Windows или загрузочный носитель)**
Мой исходный диск является MBR-диском, а ОС поддерживает UEFI	Стилем разделов после миграции останется MBR. В клонированной операционной системе будет установлен драйвер Киберпротект Bus. Использовать дисковое пространство за пределами 2 ТБ будет невозможно, поскольку MBR не поддерживает жесткие диски размером более 2 ТБ. Чтобы использовать все дисковое пространство, необходимо изменить стиль разделов на GPT или перезапустить Кибер Бэкап Старт после завершения операции и с помощью диспетчера дисков расширенной емкости Киберпротект сделать дисковое пространство сверх 2 ТБ видимым для мастера добавления новых дисков.	Стиль разделов целевого диска будет автоматически преобразован в GPT. Этот диск может использоваться для загрузки в UEFI. Кроме того, все пространство диска будет доступно.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

	Моя система загружается с помощью BIOS (Windows или загрузочный носитель)	**Моя система загружается с помощью UEFI (Windows или загрузочный носитель)**
Мой исходный диск является диском MBR, а ОС отличается от Windows или отсутствует	Выберите один из требуемых методов миграции: • **Копировать исходный раздел без изменений** Стилем разделов останется MBR, но использовать дисковое пространство за пределами 2 ТБ будет невозможно, поскольку MBR не поддерживает жесткие диски размером более 2 ТБ. Чтобы использовать все дисковое пространство, необходимо изменить стиль разделов на GPT или перезапустить Кибер Бэкап Старт после завершения операции и с помощью диспетчера дисков расширенной емкости Киберпротект сделать дисковое пространство сверх 2 ТБ видимым для мастера добавления новых дисков. • **Преобразовать стиль разделов в GPT** По завершении операции стиль разделов будет преобразован в GPT. Целевой диск нельзя будет использовать для загрузки, поскольку на исходном диске не установлена ОС Windows. Все пространство диска будет доступно.	Выберите один из требуемых методов миграции: • **Копировать исходный раздел без изменений** Стилем разделов останется MBR, но использовать дисковое пространство за пределами 2 ТБ будет невозможно, поскольку MBR не поддерживает жесткие диски размером более 2 ТБ. Чтобы использовать все дисковое пространство, необходимо изменить стиль разделов на GPT или перезапустить Кибер Бэкап Старт после завершения операции и с помощью диспетчера дисков расширенной емкости Киберпротект сделать дисковое пространство сверх 2 ТБ видимым для мастера добавления новых дисков. • **Преобразовать стиль разделов в GPT** Целевой раздел будет преобразован в стиль GPT. Целевой диск нельзя будет использовать для загрузки, поскольку на исходном диске не установлена ОС Windows. Кроме того, все пространство диска будет доступно.
Мой исходный диск является GPT-диском, а ОС поддерживает UEFI	Стилем разделов после миграции останется GPT. По завершении операции системе не удастся загрузиться из BIOS, так как ваша операционная система не поддерживает загрузку из GPT с помощью BIOS. Все пространство диска будет доступно.	Операция не повлияет ни на структуру разделов, ни на загружаемость диска: стилем разделов останется GPT, целевой диск будет загрузочным в UEFI. Все пространство диска будет доступно.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

	Моя система загружается с помощью BIOS (Windows или загрузочный носитель)	**Моя система загружается с помощью UEFI (Windows или загрузочный носитель)**
Мой исходный диск является GPT-диском, а ОС отличается от Windows или отсутствует	Операция не повлияет ни на структуру разделов, ни на загружаемость диска: стилем разделов останется GPT, целевой диск не будет загрузочным. Все пространство диска будет доступно.	Операция не повлияет ни на структуру разделов, ни на загружаемость диска: стилем разделов останется GPT, целевой диск не будет загрузочным в UEFI. Все пространство диска будет доступно.

Таблица 2. Целевой диск меньше 2 ТБ

В таблице ниже отображены возможные варианты миграции содержимого исходного диска на жесткий диск размером менее 2 ТБ.

Если исходный диск является MBR-диском, необходимо выбрать, оставить ли его MBR-диском или преобразовать в GPT с помощью Кибер Бэкап Старт.

Каждый из вариантов обладает своими преимуществами и ограничениями в зависимости от параметров системы. В основном это касается загружаемости целевого диска.

	Моя система загружается с помощью BIOS (Windows или загрузочный носитель)	**Моя система загружается с помощью UEFI (Windows или загрузочный носитель)**
Мой исходный диск является диском MBR, а ОС не поддерживает UEFI	Операция не повлияет ни на структуру разделов, ни на загружаемость диска: стилем разделов останется MBR, целевой диск будет загрузочным в BIOS. Все пространство диска будет доступно.	После завершения операции стилем разделов останется MBR, однако операционная система не сможет загрузиться из UEFI, поскольку ОС не обладает такой поддержкой.
Мой исходный диск является MBR-диском, а ОС поддерживает UEFI	Операция не повлияет ни на структуру разделов, ни на загружаемость диска: стилем разделов останется MBR, целевой диск будет загрузочным в BIOS. Все пространство диска будет доступно.	Целевой раздел будет преобразован в стиль GPT, который позволит целевому диску загружаться в UEFI. Все пространство диска будет доступно.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

	Моя система загружается с помощью BIOS (Windows или загрузочный носитель)	**Моя система загружается с помощью UEFI (Windows или загрузочный носитель)**
Мой исходный диск является диском MBR, а ОС отличается от Windows или отсутствует	Выберите один из требуемых методов миграции: • **Копировать исходный раздел без изменений** Стилем разделов останется MBR. Целевой диск не будет загрузочным, поскольку в системе не обнаружена ОС Windows. • **Преобразовать стиль разделов в GPT** Целевой диск будет преобразован в стиль GPT и использован в качестве несистемного диска, поскольку операционная система не поддерживает загрузку с GPT из-под BIOS.	Выберите один из требуемых методов миграции: • **Копировать исходный раздел без изменений** Стилем разделов останется MBR. Целевой диск не будет загрузочным, поскольку в системе не обнаружена ОС Windows. • **Преобразовать стиль разделов в GPT** Целевой раздел будет преобразован в стиль GPT и использован в качестве несистемного диска, поскольку в системе не обнаружено операционной системы Windows.
Мой исходный диск является GPT-диском, а ОС поддерживает UEFI	После завершения операции стилем раздела останется GPT, система не сможет загрузиться из-под BIOS, поскольку операционная система не поддерживает загрузку с GPT из-под BIOS.	После завершения операции стилем раздела останется GPT, операционная система сможет загружаться из UEFI.
Мой исходный диск является GPT-диском, а ОС отличается от Windows или отсутствует	После завершения операции стилем раздела останется GPT, система не сможет загрузиться из-под BIOS, поскольку операционная система не поддерживает загрузку с GPT из-под BIOS.	После завершения операции стилем раздела останется GPT, система не сможет загрузиться, поскольку в системе не обнаружено операционной системы Windows.

Способ миграции

Кибер Бэкап Старт позволяет выбрать структуру разделов для целевого диска после завершения операции восстановления.

- **MBR (основной загрузочный сектор)** — загрузочный сектор размером 512 байт, который является первым сектором жесткого диска и используется для размещения таблицы основных разделов диска.
- **GPT (таблица разделов GUID)** — это стандарт структуры таблицы разделов для жестких дисков. GPT поддерживает диски и разделы размером до 9,4 ЗБ (9,4 x 10^21 байт).

С помощью этого мастера можно преобразовать структуру разделов во время восстановления или восстановить разделы «один в один» без изменения структуры.

- **Копировать разделы без изменений** — выберите этот вариант для миграции системы один в один, без изменения структуры разделов. Обратите внимание, что в этом случае дисковое пространство за пределами 2 ТБ будет недоступно. Чтобы распределить дисковое пространство за пределами 2 ТБ, можно использовать диспетчер дисков расширенной емкости Киберпротект.
- **Копировать разделы и использовать диск как несистемный в стиле GPT** — выберите этот вариант, чтобы преобразовать раздел в структуру GPT.

С помощью Кибер Бэкап Старт также можно преобразовывать системы **BIOS** в **UEFI**.

Система загружается с помощью BIOS, MBR, UEFI не поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI не поддерживается.
- **Размер целевого диска**: меньше 2 ТБ.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью BIOS.
- **Стиль разделов**: MBR.
- **Операционная система**: Windows, загрузка в UEFI не поддерживается.
- **Размер диска**: доступно все дисковое пространство.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система, загружаемая с помощью BIOS, MBR, поддержка UEFI

На этом этапе мастера необходимо выбрать целевой жесткий диск.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI поддерживается.

- **Размер целевого диска**: меньше 2 ТБ.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью BIOS.
- **Стиль разделов**: MBR.
- **Операционная система**: Windows, загрузка в UEFI поддерживается.
- **Размер диска**: доступно все дисковое пространство.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью BIOS, MBR, без Windows

Кибер Бэкап Старт позволяет выбрать структуру разделов для целевого диска после завершения операции.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: отличается от Windows или отсутствует.
- **Размер целевого диска**: меньше 2 ТБ.

При этих параметрах системы можно выбрать один из следующих вариантов:

1. **Копировать разделы без изменений**

   На целевом диске можно оставить стиль разделов MBR.

   Целевой диск после миграции:

   - **Система**: загружается с помощью BIOS.
   - **Стиль разделов**: MBR.
   - **Операционная система**: отличается от Windows или отсутствует.
   - **Размер диска**: доступно все дисковое пространство.

2. **Копировать разделы и использовать диск как несистемный в стиле GPT**

   Стиль разделов можно преобразовать в GPT.

   Целевой диск после миграции:

   - **Система**: не загружается в BIOS.

- **Стиль разделов**: GPT.
- **Операционная система**: отличается от Windows или отсутствует.
- **Размер диска**: доступно все дисковое пространство.

⚠ Предупреждение

После миграции целевой диск можно использовать только как несистемный. Этот параметр недоступен при работе Кибер Бэкап Старт в операционной системе Windows XP x32.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью BIOS, GPT, UEFI поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: GPT.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI поддерживается.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: не загружается в BIOS.
- **Стиль разделов**: GPT.
- **Операционная система**: Windows, загрузка в UEFI поддерживается.
- **Размер диска**: доступно все дисковое пространство.

⚠ Предупреждение

После миграции операционная система не сможет загружаться с целевого диска в BIOS. Чтобы загрузиться с целевого диска после миграции, необходимо включить в системе UEFI-загрузку (см. раздел *Интерфейс UEFI*), а затем перезапустить операцию.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью BIOS, GPT, без Windows

На этом этапе мастера необходимо выбрать целевой жесткий диск.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: GPT.
- **Операционная система на исходном диске**: отличается от Windows или отсутствует.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью BIOS.
- **Стиль разделов**: GPT.
- **Операционная система**: отличается от Windows или отсутствует.
- **Размер диска**: доступно все дисковое пространство.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью UEFI, MBR, UEFI не поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI не поддерживается.
- **Размер целевого диска**: меньше 2 ТБ.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: не загружается в UEFI.
- **Стиль разделов**: MBR.
- **Операционная система**: Windows, загрузка в UEFI не поддерживается.
- **Размер диска**: доступно все дисковое пространство.

⚠ Предупреждение

Операционная система может не загрузиться в UEFI с целевого диска.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью UEFI, MBR, UEFI поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI поддерживается.

При миграции системы на выбранный диск со следующими характеристиками:

После миграции стиль разделов целевого диска будет преобразован в GPT, и с него можно будет загрузиться.

Целевой диск после миграции:

- **Система**: загружается с помощью UEFI.
- **Стиль разделов**: GPT.
- **Операционная система**: Windows, загрузка в UEFI поддерживается.
- **Размер диска**: доступно все дисковое пространство.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система на основе UEFI, MBR, Windows отсутствует

Кибер Бэкап Старт позволяет выбрать структуру разделов для целевого диска после завершения операции.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: отличается от Windows или отсутствует.
- **Размер целевого диска**: меньше 2 ТБ.

При этих параметрах системы можно выбрать один из следующих вариантов:

1. **Копировать разделы без изменений**

   На целевом диске можно оставить стиль разделов MBR.

Целевой диск после миграции:

- **Система**: загружается с помощью UEFI.
- **Стиль разделов**: MBR.
- **Операционная система**: отличается от Windows или отсутствует.
- **Размер диска**: доступно все дисковое пространство.

2. **Копировать разделы и использовать диск как несистемный в стиле GPT**

   Стиль разделов можно преобразовать в GPT.

   Целевой диск после миграции:

   - **Система**: не загружается в UEFI.
   - **Стиль разделов**: GPT.
   - **Операционная система**: отличается от Windows или отсутствует.
   - **Размер диска**: доступно все дисковое пространство.

> ⚠ **Предупреждение**
>
> После миграции целевой диск можно использовать только как несистемный.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью UEFI, GPT, UEFI поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI
- **Исходный стиль разделов**: GPT
- **Операционная система:** Windows, загрузка в UEFI поддерживается

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью UEFI
- **Стиль разделов**: GPT
- **Размер диска**: доступно все дисковое пространство

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система, загружаемая с помощью UEFI, GPT, без Windows

На этом этапе мастера необходимо выбрать целевой жесткий диск.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI
- **Исходный стиль разделов**: GPT
- **Операционная система**: отличается от Windows или отсутствует

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью UEFI
- **Стиль разделов**: GPT
- **Размер диска**: доступно все дисковое пространствos

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Восстановление динамических и GPT-дисков и томов

Восстановление динамических томов

Динамические тома можно восстановить в следующие расположения на локальных жестких дисках:

- **Динамический том**

> **Примечание**
>
> Изменение размера динамических томов вручную в процессе восстановления на динамические диски не поддерживается. Если во время восстановления необходимо изменить размер динамического тома, то его следует восстанавливать на базовый диск.

  - **Исходное расположение (на тот же самый динамический том)**

    Тип целевого тома не меняется.

  - **Другой динамический диск или том**

    Тип целевого тома не меняется. Например, при восстановлении динамического чередующегося тома на динамический составной целевой том остается составным.

  - **Нераспределенное пространство динамической группы**

    Тип восстановленного тома будет соответствовать типу в резервной копии.

- **Основной том или диск**

  Целевой том остается базовым.

- **Восстановление на «голое железо»**

  При восстановлении динамических томов на «голое железо» — на новый неотформатированный диск — восстановленные тома становятся базовыми. Если необходимо, чтобы восстановленные тома остались динамическими, целевые диски должны быть подготовлены как динамические (отформатированы и иметь созданные разделы). Это можно сделать при помощи сторонних утилит, например при помощи оснастки управления дисками Windows.

Восстановление основных томов и дисков

- при восстановлении базового тома на нераспределенное пространство динамической группы восстановленный том становится динамическим;
- при восстановлении базового диска на динамический диск динамической группы, состоящей из двух дисков, восстановленный диск остается базовым; динамический диск, на который производится восстановление, становится «отсутствующим», а составной/чередующийся динамический том на втором диске становится «ошибочным».

Стиль разделов после восстановления

Стиль разделов целевого диска зависит от того, поддерживает ли компьютер интерфейс UEFI, и от того, как загружена система — через BIOS или UEFI. См. следующую таблицу.

	Моя система загружается с помощью BIOS (Windows или загрузочный носитель)	**Моя система загружается с помощью UEFI (Windows или загрузочный носитель)**
Мой исходный диск является диском MBR, а ОС не поддерживает UEFI	Операция не повлияет ни на структуру разделов, ни на загружаемость диска: стилем разделов останется MBR, целевой диск будет загрузочным в BIOS.	После завершения операции стилем разделов станет GPT, однако операционная система не сможет загрузиться из UEFI, поскольку не обладает такой поддержкой.
Мой исходный диск является MBR-диском, а ОС поддерживает UEFI	Операция не повлияет ни на структуру разделов, ни на загружаемость диска: стилем разделов останется MBR, целевой диск будет загрузочным в BIOS.	Целевой раздел будет преобразован в стиль GPT, который позволит целевому диску загружаться в UEFI. См. *Пример восстановления в систему UEFI*.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

	Моя система загружается с помощью BIOS (Windows или загрузочный носитель)	**Моя система загружается с помощью UEFI (Windows или загрузочный носитель)**
Мой исходный диск является GPT-диском, а ОС поддерживает UEFI	После завершения операции стилем раздела останется GPT, система не сможет загрузиться из-под BIOS, поскольку операционная система не поддерживает загрузку с GPT из-под BIOS.	После завершения операции стилем раздела останется GPT, операционная система сможет загружаться из UEFI.

Пример восстановления в систему UEFI

Ниже приведен пример переноса системы со следующими условиями.

- Исходный диск является диском MBR, а ОС поддерживает UEFI.
- Целевая система загружается с помощью UEFI.
- Старый и новый диски работают в одном режиме контроллера (например, IDE или AHCI).

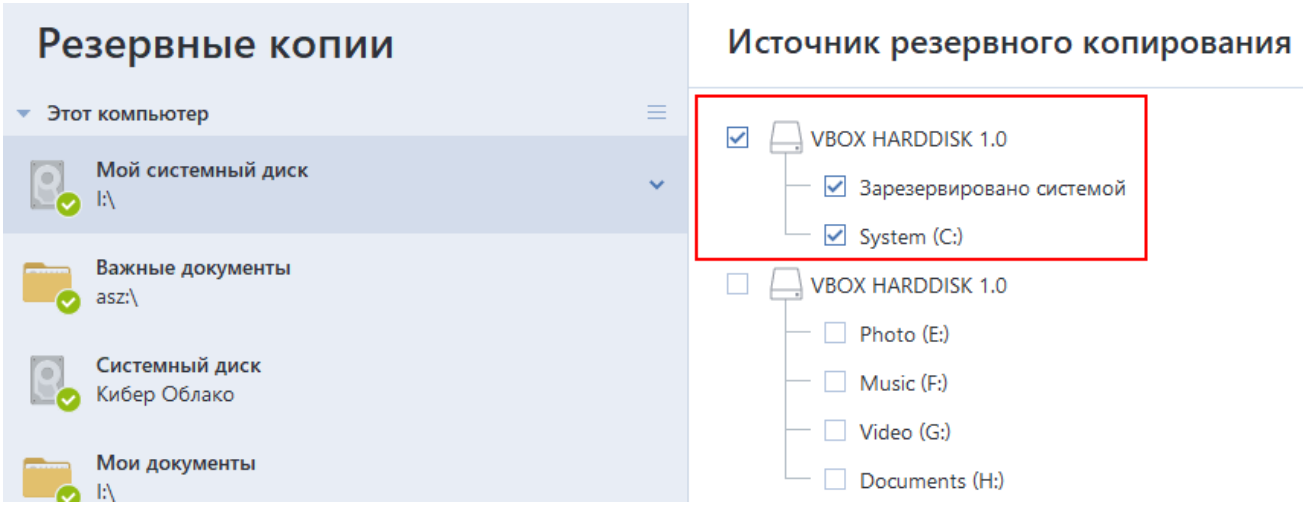
Перед началом процедуры убедитесь, что у вас имеется следующее:

- **Загрузочный носитель.**

  Дополнительные сведения см. в разделе *Как создать загрузочный носитель*.

- **Резервная копия системного диска, созданная в режиме диска.**

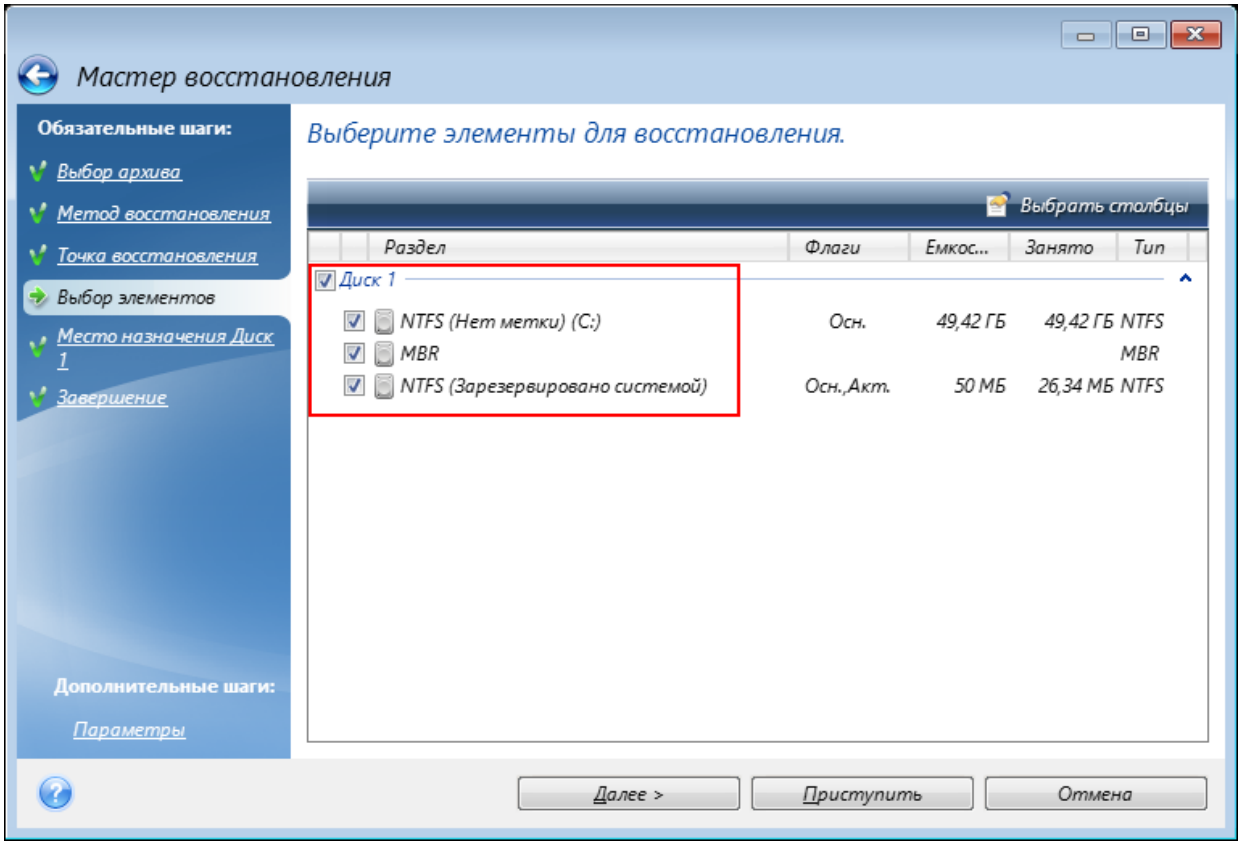
  Для создания такой резервной копии переключитесь в режим диска и выберите жесткий диск, на котором находится системный раздел. Дополнительные сведения см. в разделе *Резервное копирование дисков и разделов*.



Как перенести систему с MBR-диска на компьютер, загружаемый с помощью UEFI:

1. Выполните загрузку в режиме UEFI, используя загрузочный носитель, и выберите Кибер Бэкап Старт.
2. Запустите мастер восстановления и следуйте инструкциям в разделе *Восстановление системы*.
3. На шаге **Выбор элементов** установите флажок напротив имени диска, чтобы выбрать весь системный диск.

   В примере ниже необходимо установить флажок **Диск 1**.



4. На шаге **Завершение** нажмите кнопку **Приступить**.

По завершении операции целевой диск будет преобразован в стиль GPT, что позволит ему загружаться в UEFI.

После восстановления убедитесь, что загружаете компьютер в режиме UEFI. Может потребоваться изменить режим загрузки системного диска в пользовательском интерфейсе диспетчера загрузки UEFI.

Настройка порядка загрузки в BIOS или UEFI BIOS

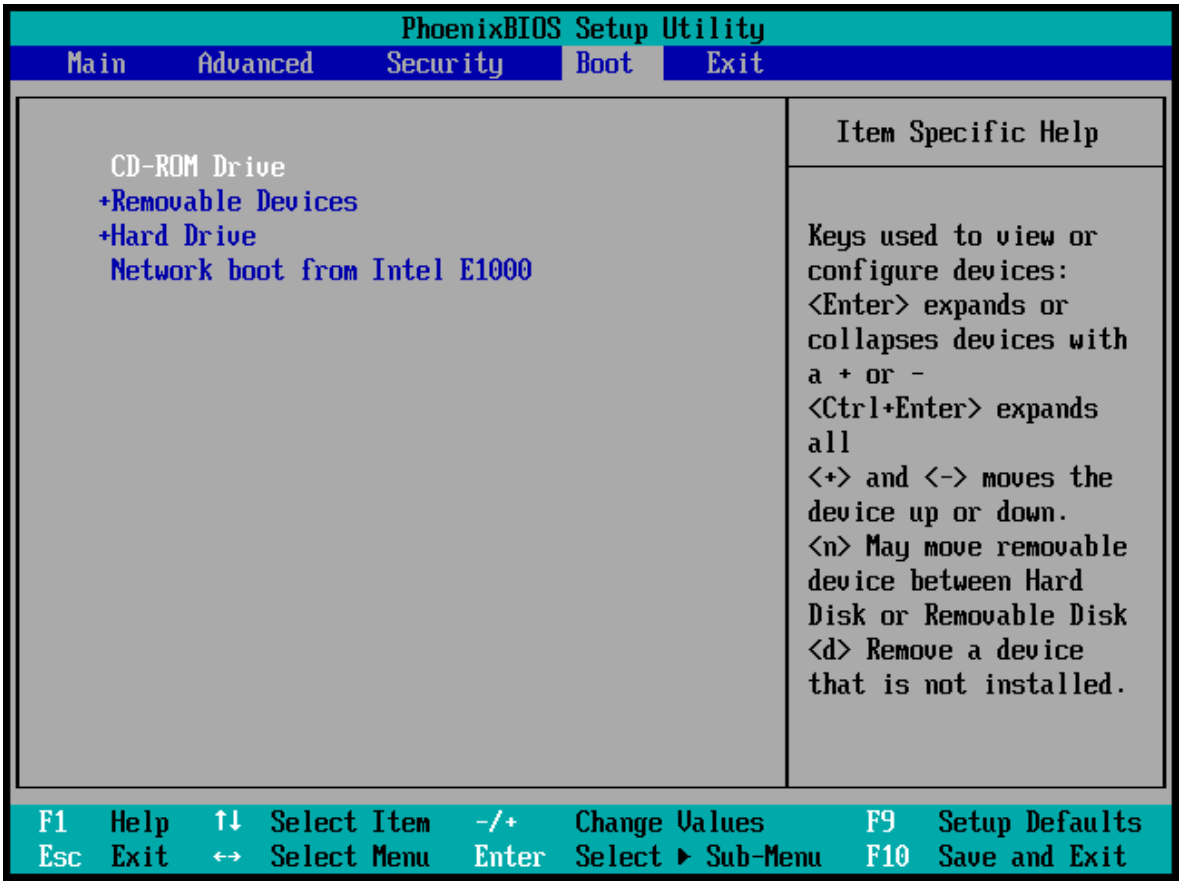
Чтобы загрузить компьютер, используя загрузочный носитель, необходимо установить такой порядок загрузки, чтобы этот носитель был первым загрузочным устройством. Порядок загрузки меняется в BIOS или UEFI BIOS в зависимости от микропрограммного интерфейса компьютера. Процедура очень похожа в обоих случаях.

Как выполнить загрузку, используя загрузочный носитель:

1. Если в качестве загрузочного носителя используется флеш-накопитель или внешний диск USB, подсоедините его к порту USB.
2. Включите компьютер. Во время самотестирования при включении питания (POST) отобразится сочетание клавиш, которое необходимо нажать, чтобы войти в BIOS или UEFI BIOS.
3. Нажмите это сочетание клавиш (например, `Del`, `F1`, `Ctrl+Alt+Esc`, `Ctrl+Esc`). Откроется утилита настройки BIOS или UEFI BIOS. Обратите внимание, что утилиты могут различаться по внешнему виду, набору пунктов, именам и т. д.

   > **Примечание**
   >
   > На некоторых системных платах есть так называемое меню загрузки, которое можно открыть, нажав определенную клавишу или сочетание клавиш, например **F12**. Меню загрузки позволяет выбрать устройство для загрузки из списка загрузочных устройств, не изменяя настройки BIOS или UEFI BIOS.

4. Если в качестве загрузочного носителя используется CD или DVD-диск, вставьте его в дисковод.
5. Сделайте загрузочный носитель (CD, DVD или USB-накопитель) первым загрузочным устройством.
   1. Перейдите к параметру порядка загрузки с помощью клавиш со стрелками.
   2. Расположите курсор на устройстве с загрузочным носителем и сделайте его первым элементом в списке. Обычно изменить порядок можно с помощью клавиш со знаками «плюс» и «минус».



6. Выйдите из BIOS или UEFI BIOS и сохраните внесенные изменения. Компьютер загрузится, используя загрузочный носитель.

Примечание

Если загрузиться с первого устройства не удастся, компьютер попытается загрузиться со второго устройства в списке, и так далее.

Восстановление дисков из Кибер Облака

Восстановление диска из Кибер Облака очень похоже на восстановление с обычного жесткого диска.

- Если вы можете запустить Windows и Кибер Бэкап Старт, см. раздел *Восстановление разделов и дисков*.
- Если Windows не запускается, см. раздел *Восстановление системы из Кибер Облака*.

Принцип работы

Компьютер должен быть подключен к Интернету посредством Ethernet-кабеля или через Wi-Fi. Кибер Бэкап Старт поддерживает несколько протоколов безопасности беспроводных сетей, включая WPA-Personal, WPA2-Personal и WPA2-Enterprise.

Восстановление в исходное расположение

При восстановлении диска в исходное расположение Кибер Бэкап Старт не загружает все дисковое пространство на компьютер. Программа выполняет сканирование диска на предмет изменений данных и восстанавливает только те файлы, которые отличаются от файлов в резервной копии. Эта технология значительно сокращает объем данных, загружаемых для восстановления диска.

Восстановление в новое расположение

Восстановление диска в другое расположение или на нераспределенное пространство аналогично восстановлению из локального хранилища. Единственным различием является метод записи данных. Кибер Бэкап Старт загружает и записывает данные не непрерывно, а отдельными блоками. Эта технология повышает скорость восстановления и надежность всего процесса.

Если восстановление было прервано

Поскольку восстановление дисков из Кибер Облака требует подключения к Интернету и обычно занимает длительное время, вероятность прерывания процесса выше, чем при восстановлении с обычного жесткого диска.

Возможные причины прерывания восстановления:

- Потеряно подключение к Интернету.
- Потеряно подключение к Кибер Облаку.
- Восстановление отменено пользователем намеренно или случайно.
- Перебой подачи электроэнергии.

Если восстановление не было завершено из-за проблемы с подключением, Кибер Бэкап Старт автоматически пытается заново подключиться к Кибер Облаку и возобновить процесс восстановления. В этом случае рекомендуется проверить параметры подключения к Интернету. Если все автоматические попытки закончились неудачей, запустите восстановление заново вручную, когда подключение восстановится.

В остальных случаях запустите восстановление вручную и убедитесь, что процесс завершен.

Независимо от причины прерывания Кибер Бэкап Старт не запускает восстановление с самого начала.

Процесс возобновляется, и загружаются только те данные, которые не были восстановлены.

Восстановление системы из Кибер Облака

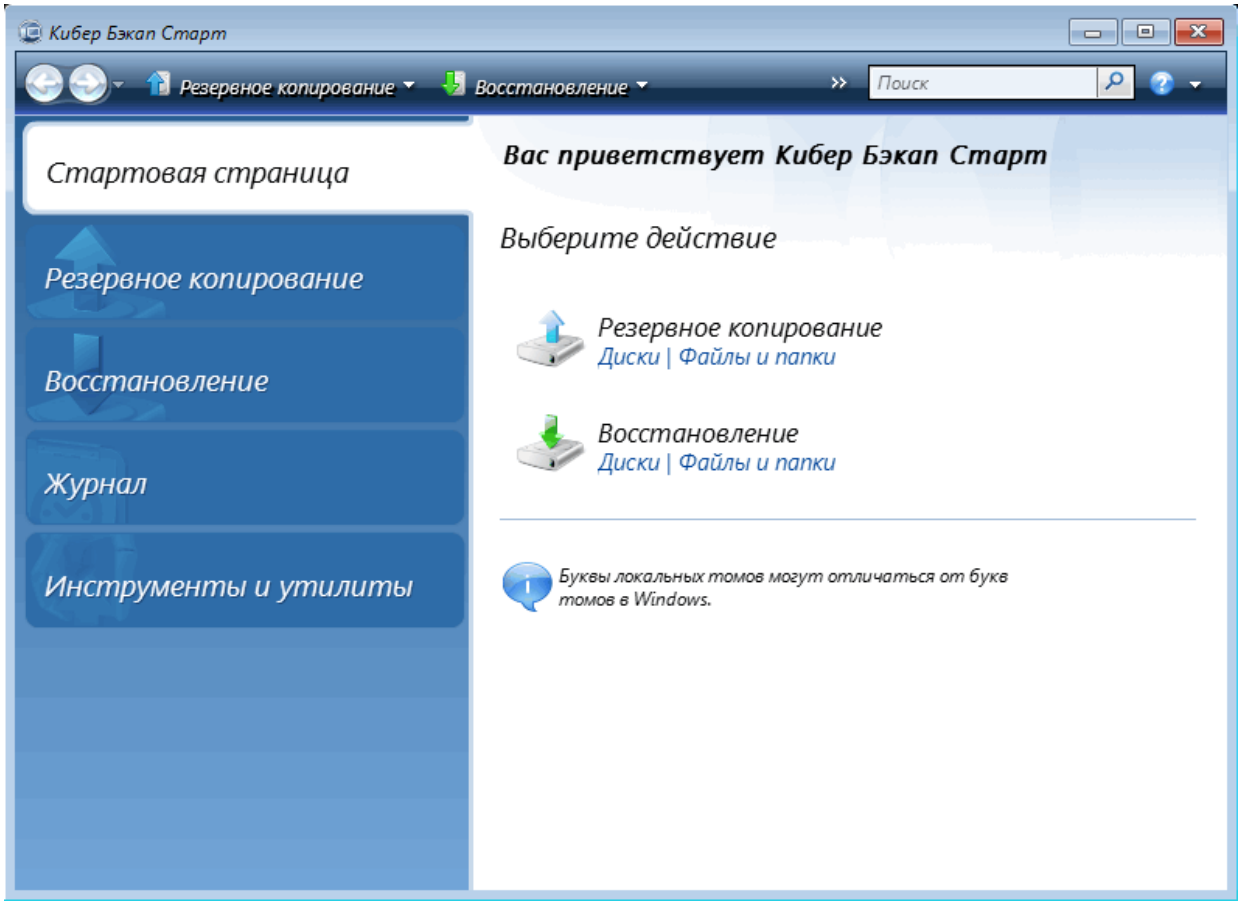
> **Примечание**
>
> В зависимости от скорости подключения к Интернету восстановление диска из Кибер Облака может занять длительное время.

Перед началом работы рекомендуется выполнить процедуры, описанные в разделе *Подготовка к восстановлению*. Если система восстанавливается на новый диск, то форматировать его не нужно, так как это будет сделано в процессе восстановления.

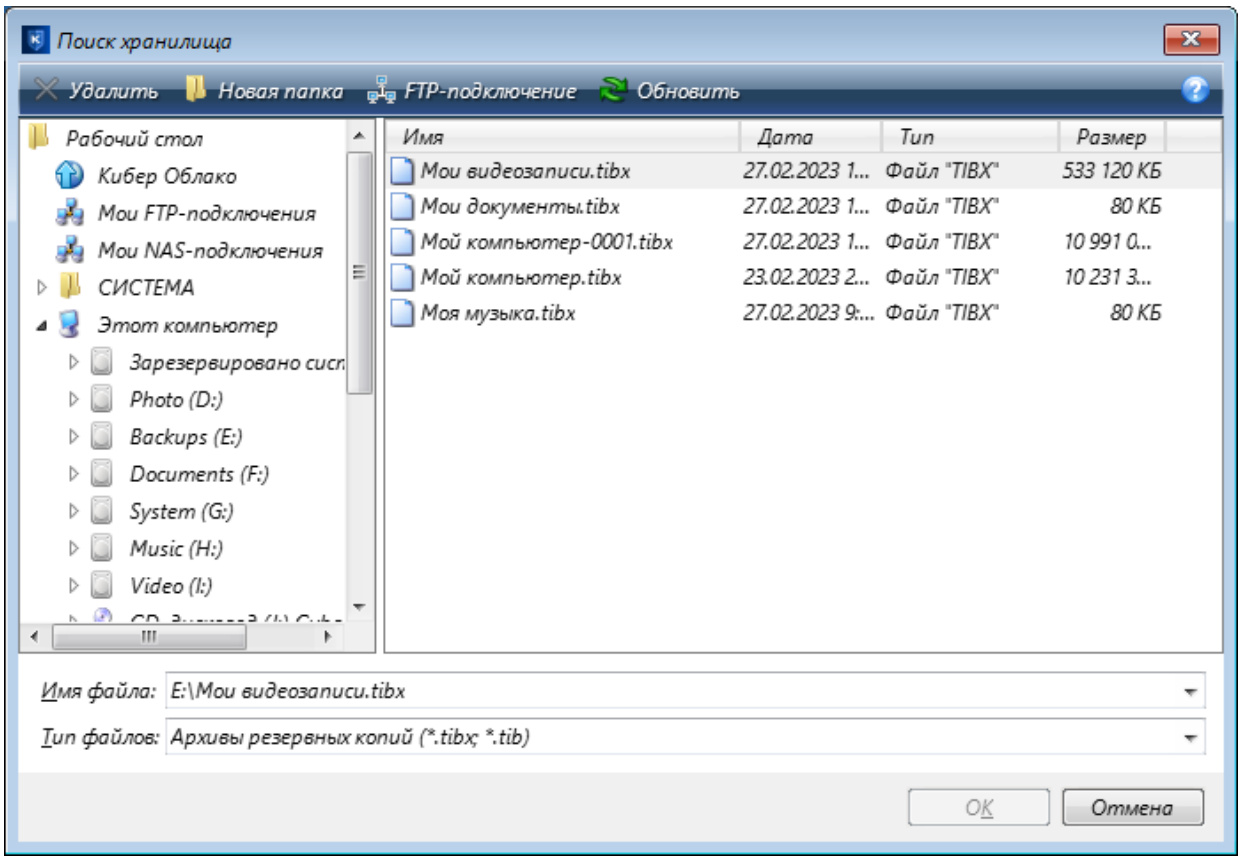
Перед запуском процедуры убедитесь, что компьютер подключен к Интернету посредством Ethernet-кабеля или через Wi-Fi.

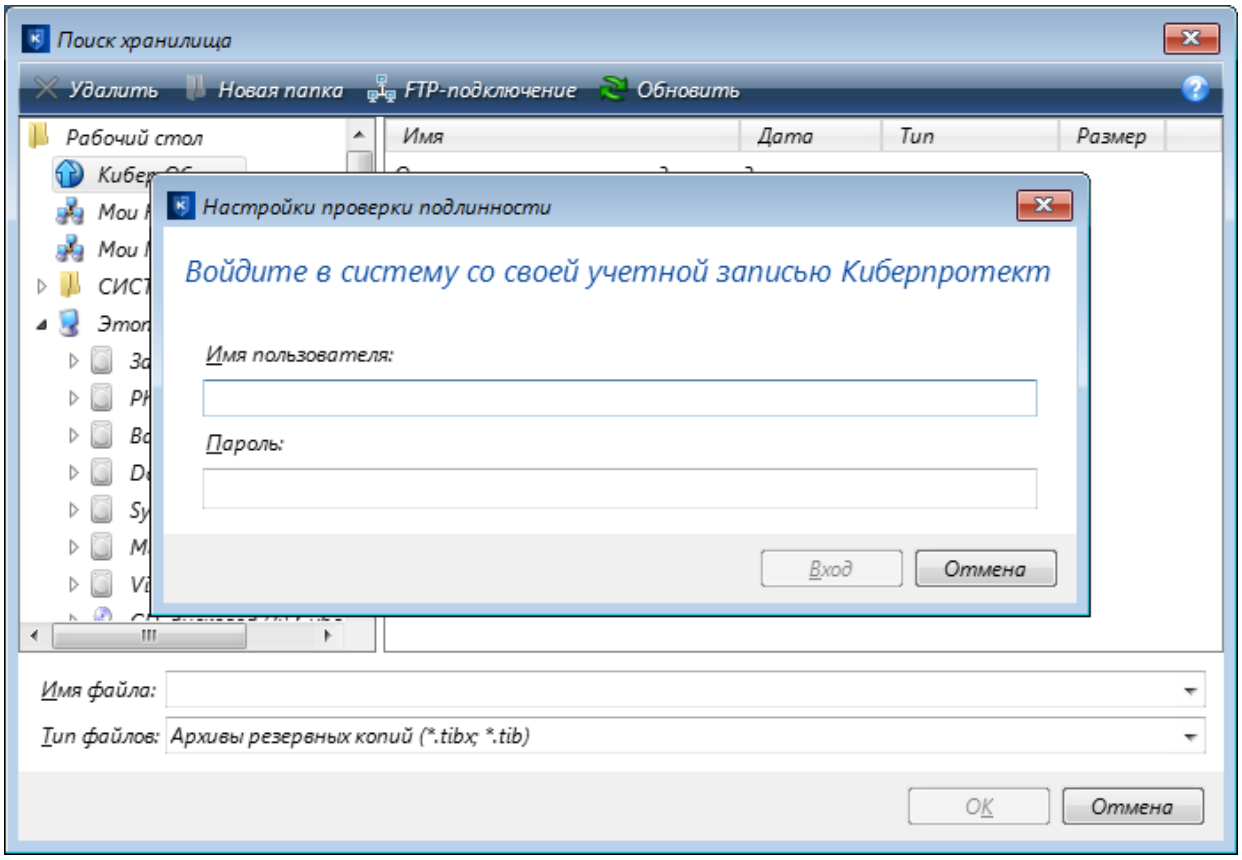
Как восстановить системный диск из Кибер Облака:

1. Измените порядок загрузки в BIOS так, чтобы сделать загрузочный носитель (CD, DVD или флеш-накопитель USB) первым устройством загрузки. См. раздел *Настройка порядка загрузки в BIOS*.
2. Выполните загрузку с загрузочного носителя и выберите Кибер Бэкап Старт.
3. На **главном экране** выберите **Диски** под заголовком **Восстановление**.

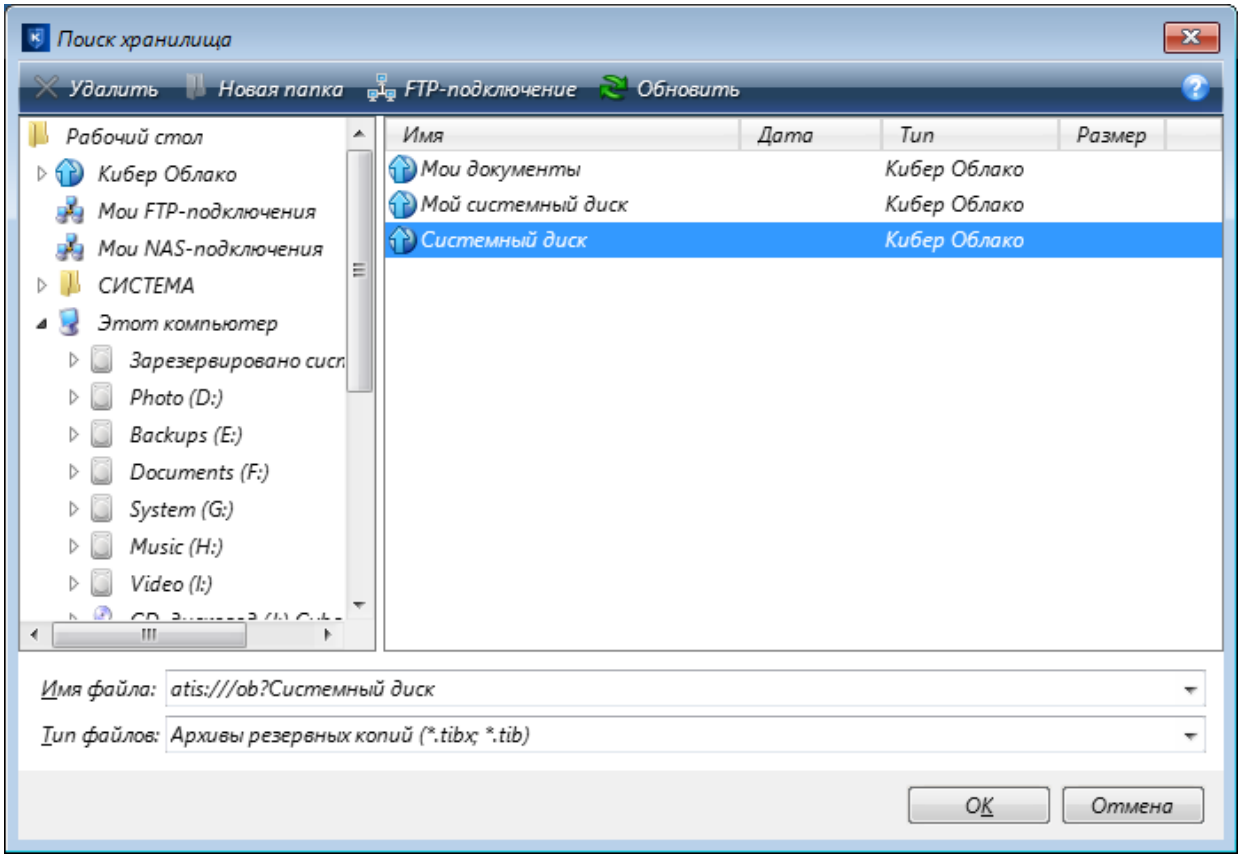


4. Чтобы добавить резервную копию системного диска или раздела из онлайн-хранилища в список доступных резервных копий, нажмите кнопку **Обзор**.
5. В открывшемся окне выберите в дереве каталогов Кибер Облако и введите данные своей учетной записи Киберпротект.

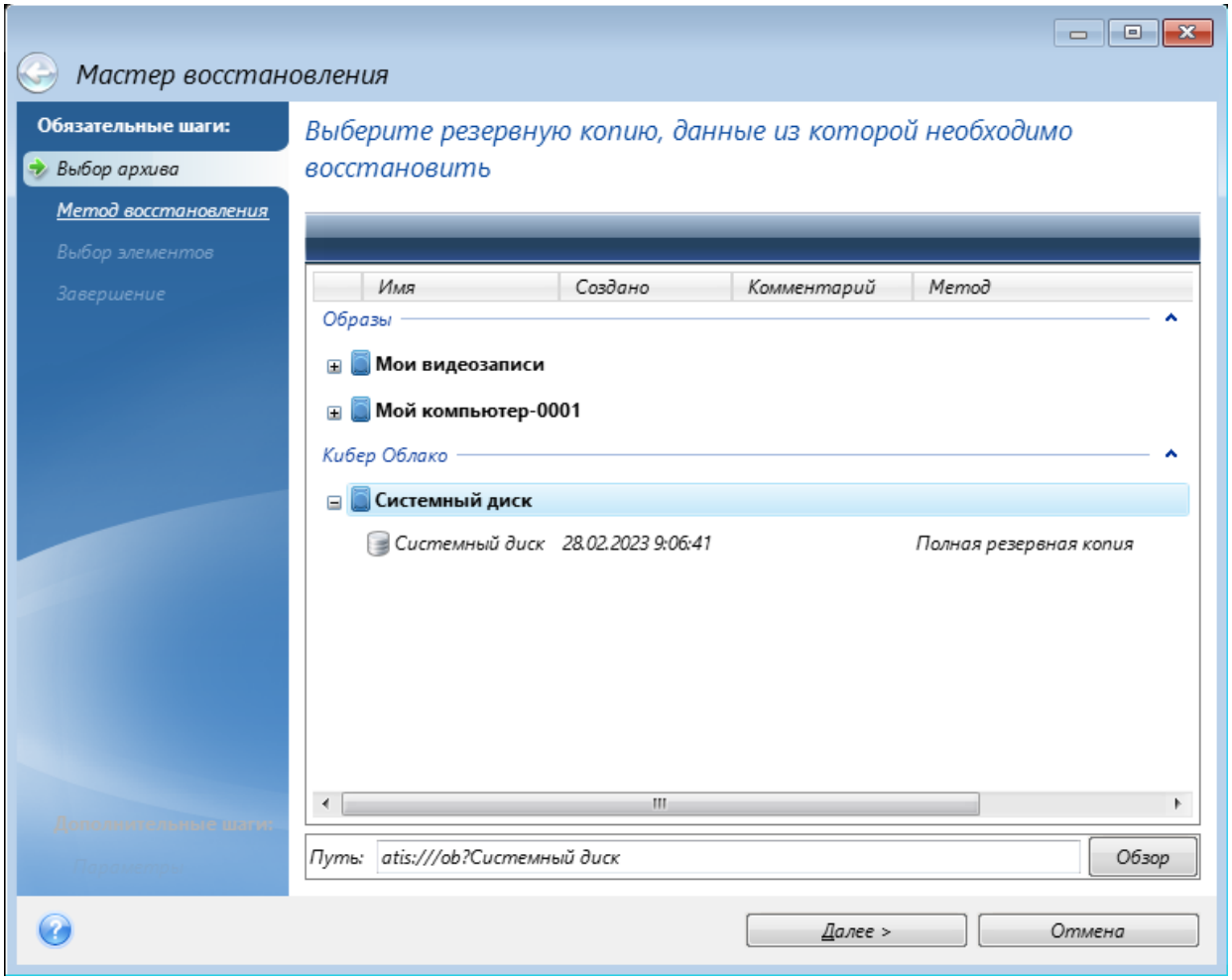




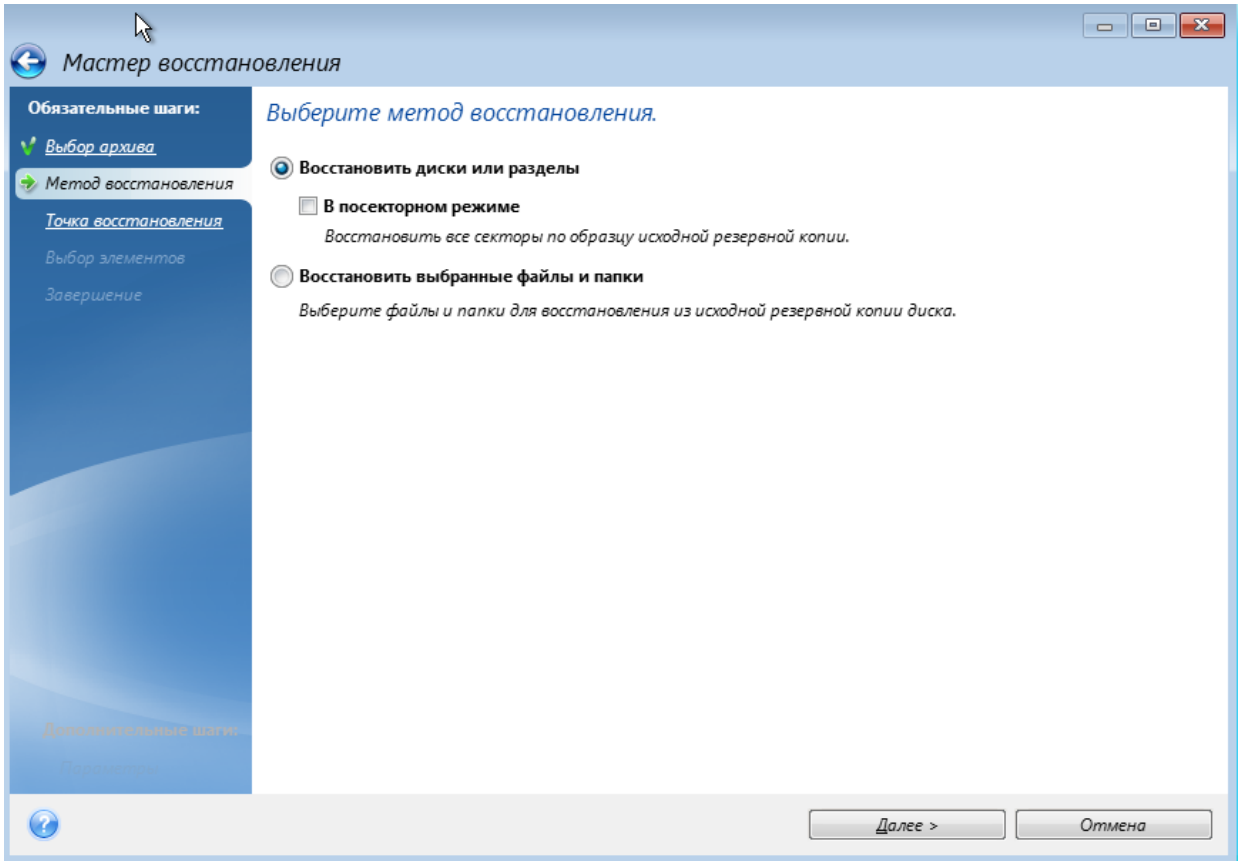
6. Выберите резервную копию для восстановления и нажмите кнопку **ОК**.



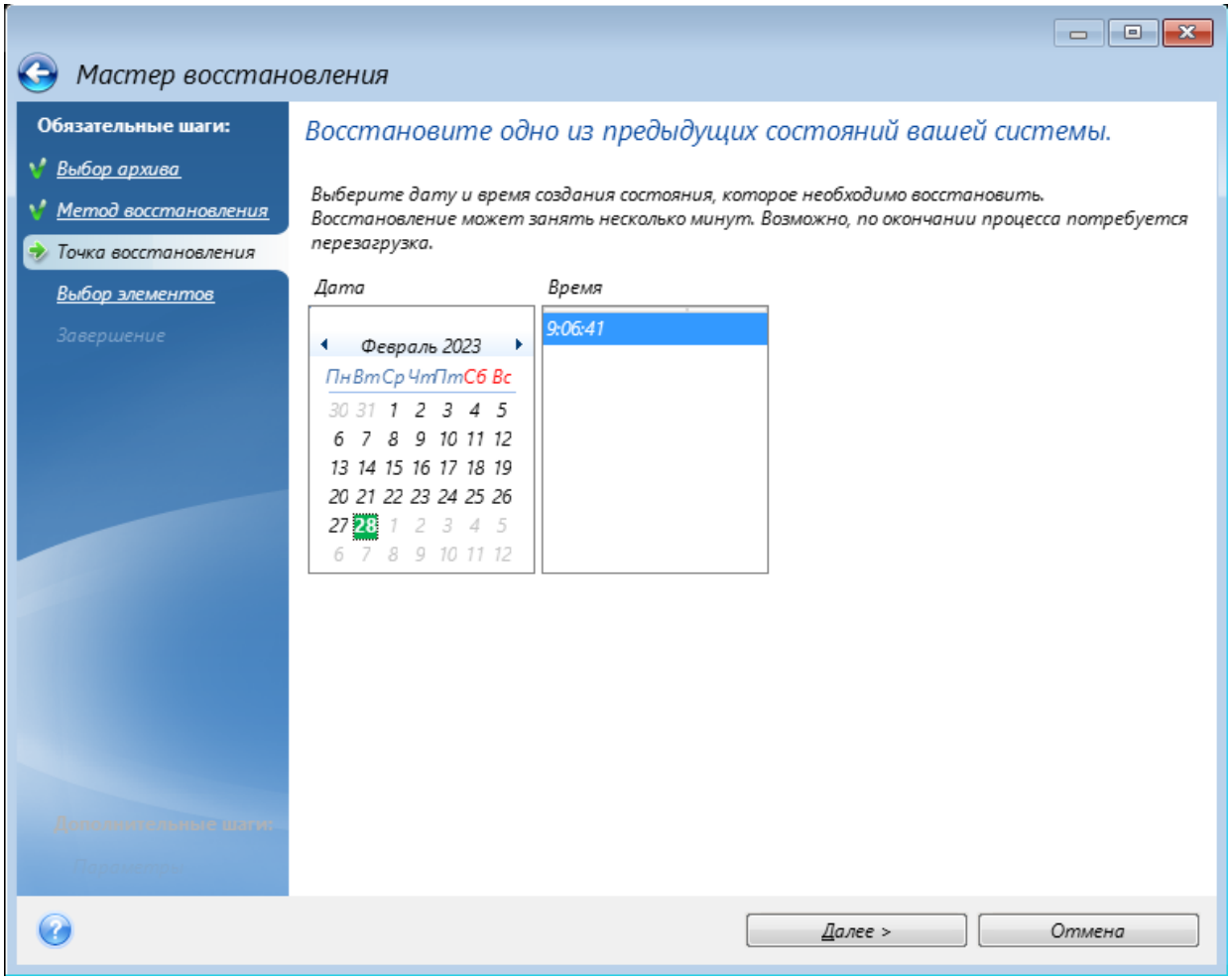
7. На шаге **Выбор архива** выберите резервную копию в онлайн-хранилище и нажмите кнопку **Далее**.



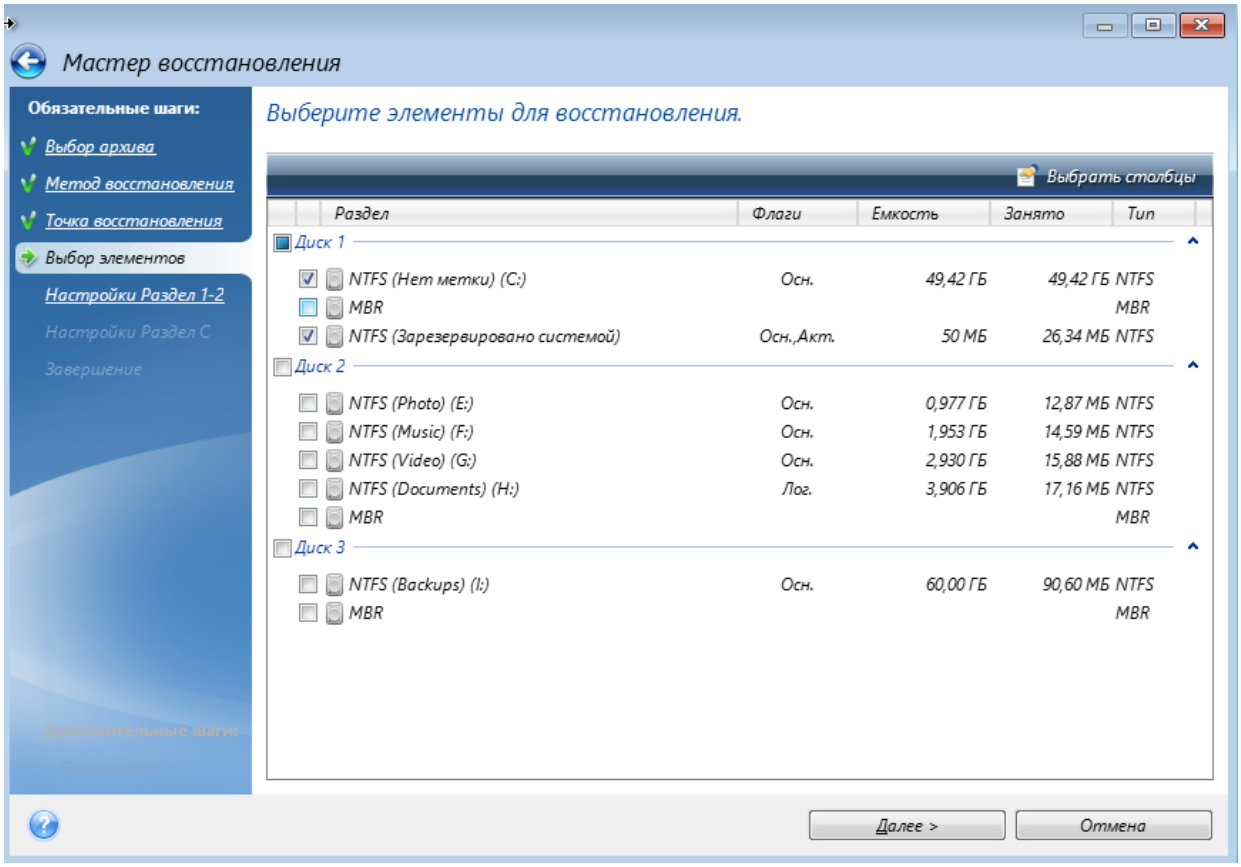
8. На шаге **Метод восстановления** выберите **Восстановить диски или разделы**.



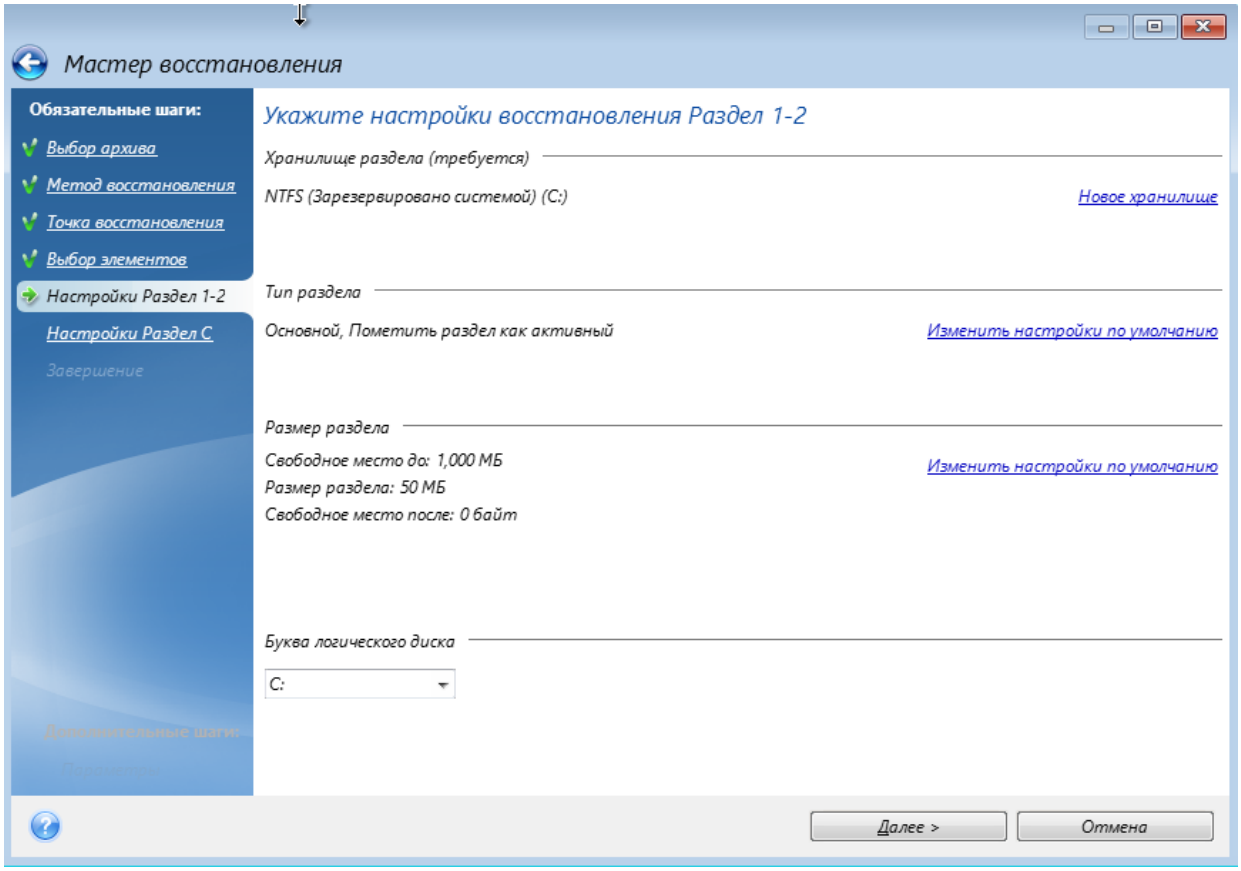
9. На шаге **Точка восстановления** выберите дату и время, на которые следует восстановить систему.

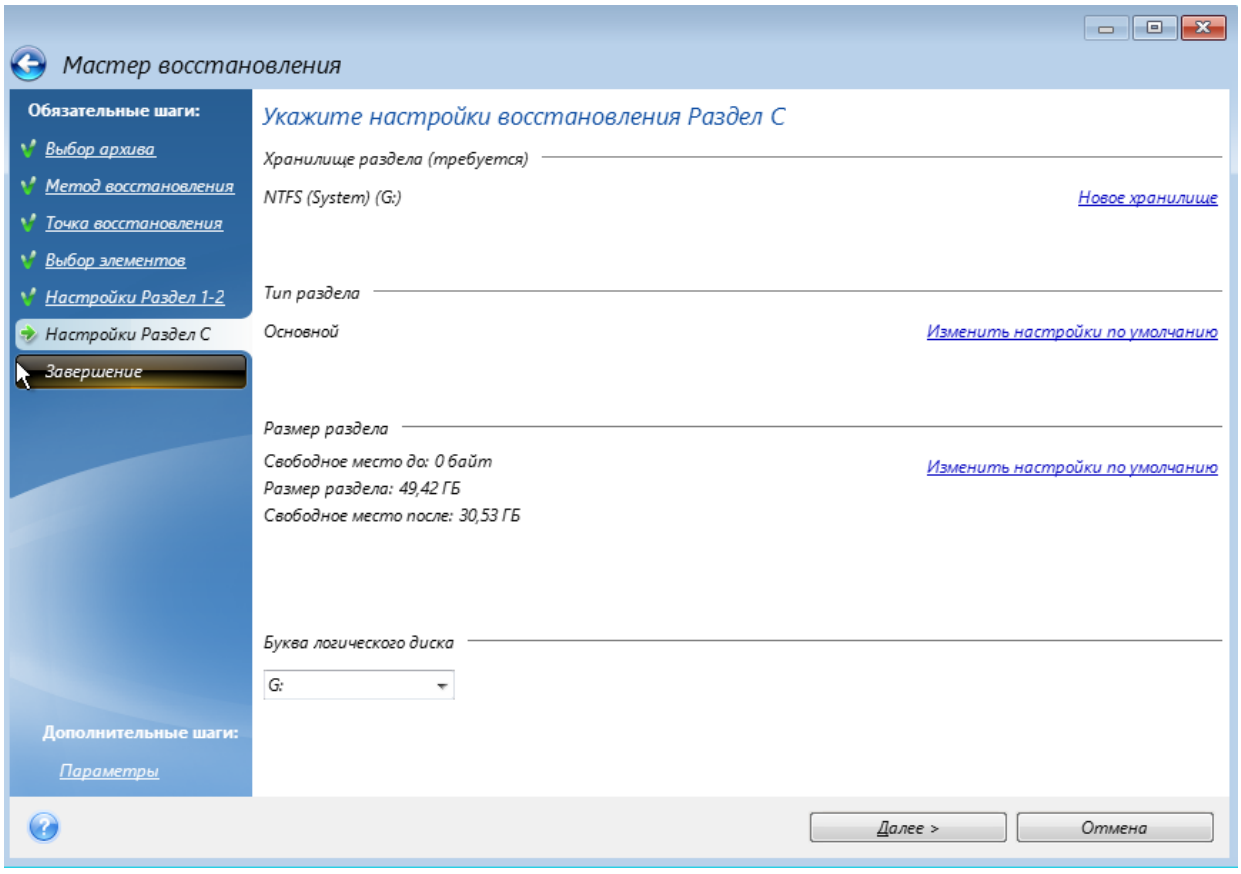


10. На шаге **Выбор элементов** выберите системный раздел (обычно C) и раздел «Зарезервировано системой» (если есть). Эти разделы также можно отличить по флагам **Pri** и **Act**.



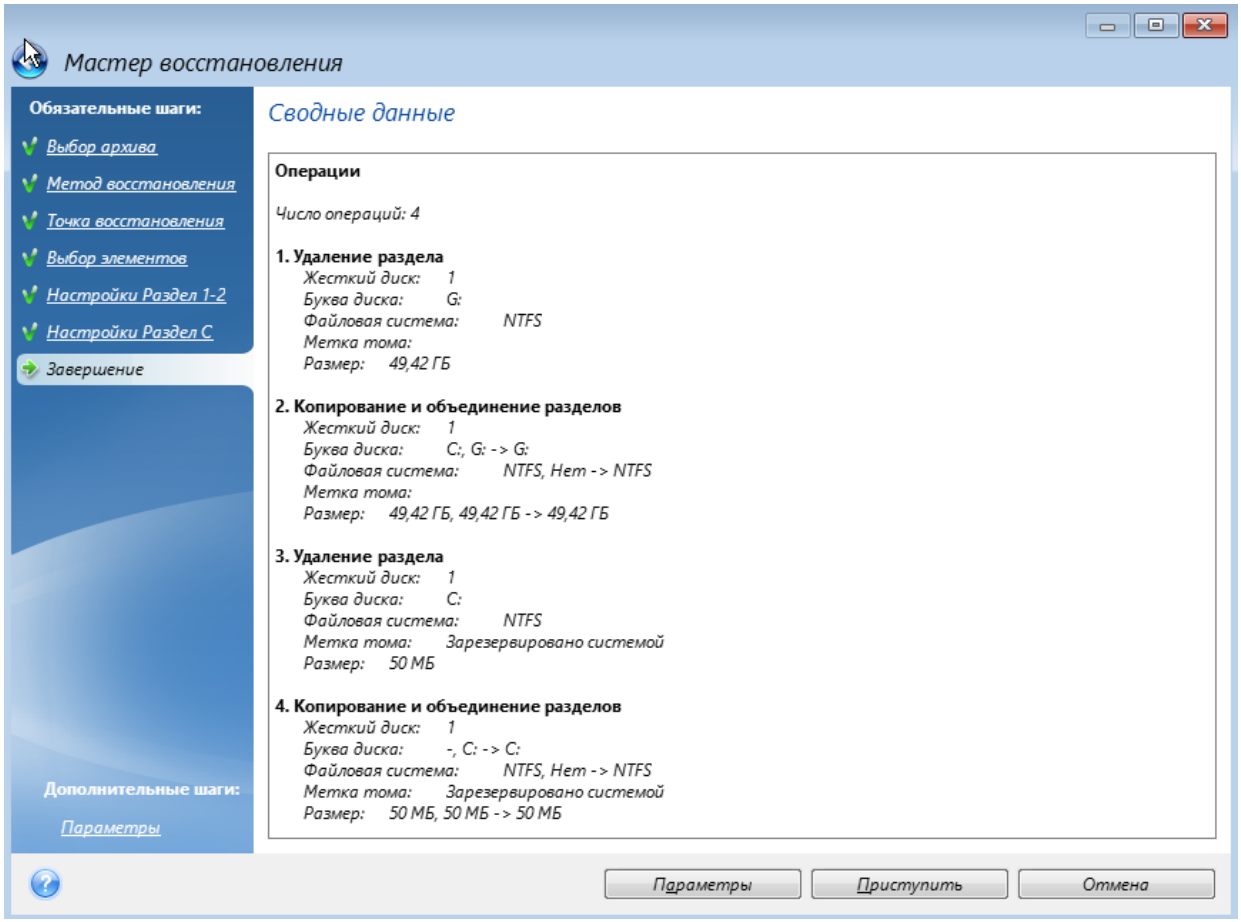
11. На шаге **Настройки раздела С** (или другая буква системного раздела) измените настройки, если это необходимо. Например, изменение настроек требуется при восстановлении на новый жесткий диск другой емкости.





12. Внимательно прочитайте перечень операций на последнем шаге **Завершение**. Если размер

восстанавливаемого раздела не был изменен, то обратите внимание, что размеры разделов в значениях **Удаление раздела** и **Копирование и объединение разделов** должны совпадать. Нажмите кнопку **Приступить**.



13. После завершения восстановления выйдите из автономной версии Кибер Бэкап Старт и извлеките загрузочный носитель. Загрузите компьютер с восстановленного системного раздела. Убедившись, что ОС Windows восстановлена до нужного состояния, *восстановите исходный порядок загрузки*.

Восстановление файлов и папок

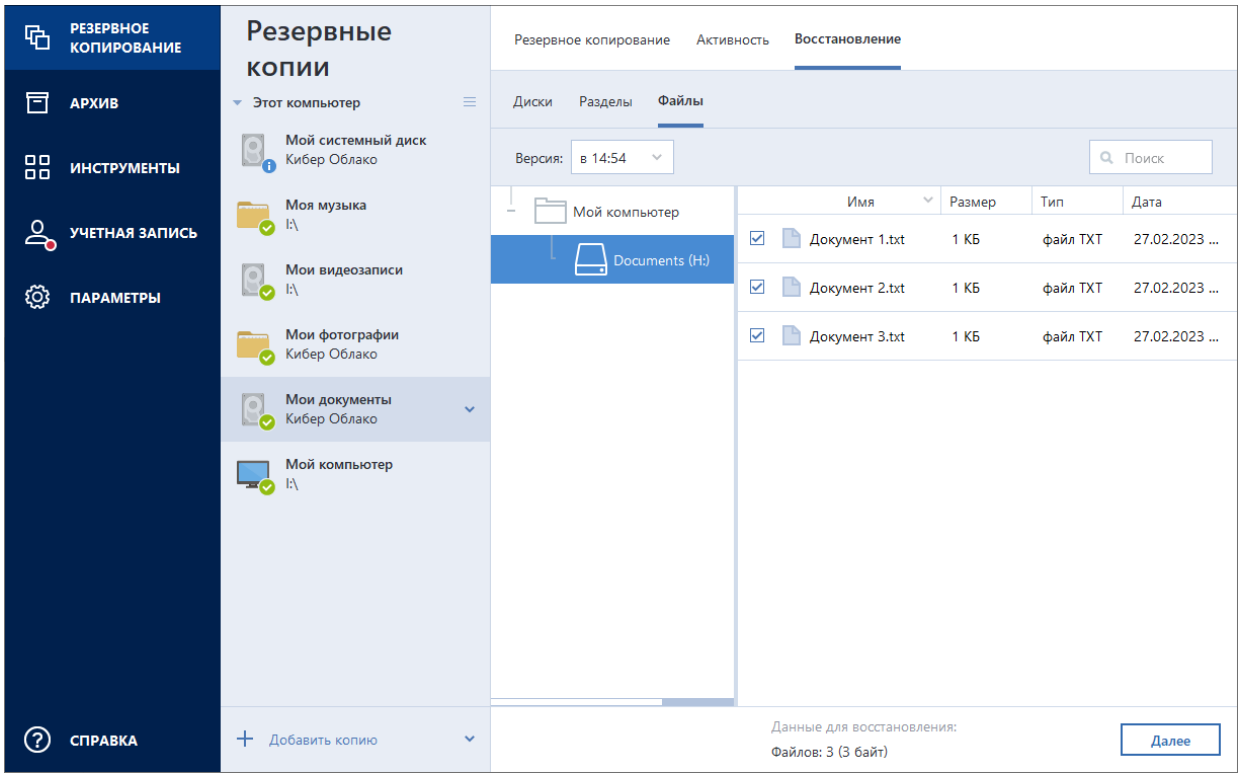
Резервные копии файлов и папок можно просматривать и восстанавливать в программе Кибер Бэкап Старт, проводнике Windows или в Кибер Облаке. Файлы и папки можно восстанавливать из резервных копий на уровне файлов или дисков.

Как восстановить данные в Кибер Бэкап Старт:

1. На боковой панели нажмите **Резервное копирование**.
2. Выберите из списка резервную копию, содержащую файлы и папки, которые необходимо восстановить, и откройте вкладку **Восстановление**.
3. [Необязательно] На панели инструментов в раскрывающемся списке **Версия** выберите нужную

дату и время резервной копии. По умолчанию восстанавливается последняя резервная копия.

4. Выберите вкладку **Файлы**.
5. Установите флажки для файлов и папок, которые следует восстановить, и нажмите **Далее**.



6. [Необязательно] По умолчанию данные будут восстановлены в исходное расположение. Чтобы изменить его, нажмите кнопку **Обзор** на панели инструментов и укажите нужное место назначения.
7. [Необязательно] Задайте параметры восстановления (приоритет процесса восстановления, параметры безопасности файлов и т. д.). Для этого щелкните **Параметры восстановления**. Параметры, заданные здесь, относятся только к текущей операции восстановления.
8. Чтобы начать восстановление, нажмите кнопку **Восстановить**.

   Чтобы остановить восстановление, нажмите кнопку **Остановить**. Помните, что даже прерванное восстановление может вызвать изменения в целевой папке.

Как восстановить данные в проводнике Windows:

1. Дважды щелкните соответствующий TIBX-файл, а затем перейдите к файлу или папке, которые нужно восстановить.
2. Скопируйте этот файл или папку на жесткий диск.

Примечание

Скопированные файлы теряют атрибут «Сжатый» и «Зашифрованный». Если нужно сохранить эти атрибуты, рекомендуется восстановить резервную копию.

Как восстановить данные в Кибер Облаке:

1. В списке ПК, для которых создавались резервные копии, выберите нужный ПК.
2. В списке резервных копий выберите облачную резервную копию, содержащую файлы или папки, которые необходимо восстановить.
3. В списке файлов и папок выберите элементы, которые следует восстановить.
4. Чтобы начать восстановление, нажмите **Загрузить** на правой боковой панели. Выбранные данные будут скопированы в папку загрузки по умолчанию.

Примечание

Если выбрано несколько файлов и папок, они будут помещены в ZIP-архив.

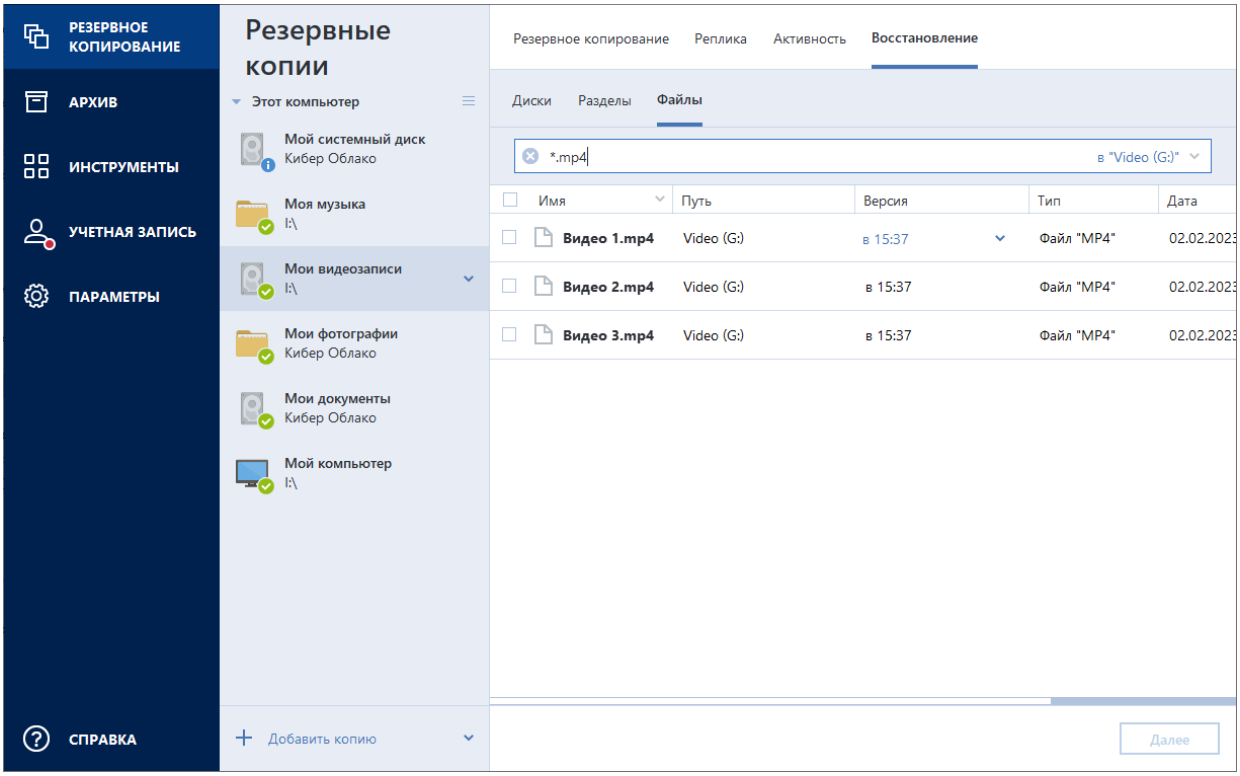
Поиск в содержимом резервных копий

При восстановлении данных можно выполнить поиск конкретных файлов и папок в выбранной резервной копии.

Как искать файлы и папки:

1. Запустите восстановление данных, как указано в разделе *Восстановление дисков и разделов* или *Восстановление файлов и папок*.
2. При выборе файлов и папок для восстановления введите имя файла или папки в поле **Поиск**. Программа отобразит результаты поиска.

   Можно также использовать стандартные подстановочные знаки Windows: * и ?. Например, чтобы найти все файлы с расширением .exe, введите `*.exe`. Чтобы найти все EXE-файлы, имена которых состоят из пяти символов и начинаются с my, введите `my???.exe`.



3. По умолчанию Кибер Бэкап Старт выполняет поиск в папке, выбранной на предыдущем шаге. Для поиска во всей резервной копии щелкните стрелку вниз и выберите **по всей резервной копии**.

   Для возврата к предыдущему шагу удалите текст поиска и щелкните значок с крестиком.

4. После завершения поиска выберите файлы, которые необходимо восстановить, и нажмите кнопку **Далее**.

> **Примечание**
>
> Обращайте внимание на столбец «Версия». Файлы и папки, принадлежащие к разным версиям резервной копии, не могут восстанавливаться одновременно.

Параметры восстановления

Можно настроить параметры для процессов восстановления диска/раздела и файлов. После установки приложения всем параметрам присваиваются значения по умолчанию. Параметры можно изменить как для текущей операции восстановления, так и для всех последующих. Установите флажок **Сохранить по умолчанию**, чтобы применить измененные параметры ко всем последующим операциям восстановления.

Параметры восстановления дисков и файлов полностью независимы друг от друга, и задать их необходимо отдельно.

Чтобы вернуть все измененные параметры в исходные значения, которые были заданы после установки продукта, нажмите кнопку **Исходные настройки**.

Режим восстановления диска

Расположение: **Параметры восстановления** → **Дополнительно** → **Режим восстановления диска**

Этот параметр позволяет выбрать режим восстановления диска для резервных копий дисков.

- **Восстановить посекторно** — установите этот флажок, если требуется восстановить используемые и неиспользуемые сектора дисков и разделов. Посекторное восстановление возможно только для резервных копий, созданных в посекторном режиме.

Команды до и после восстановления

Расположение: **Параметры восстановления** → **Дополнительно** → **Pre/Post-команды**

Укажите команды или пакетные файлы, которые будут автоматически выполняться до и после процесса восстановления.

Например, может потребоваться запустить или остановить определенные процессы Windows или проверить данные на вирус перед запуском восстановления.

Как указать команды (пакетные файлы):

- В поле **Pre-команда** выберите команду, которая будет выполняться перед запуском восстановления. Чтобы создать новую команду или выбрать пакетный файл, нажмите кнопку **Изменить**.
- В поле **Post-команда** выберите команду, которая будет выполняться после завершения восстановления. Чтобы создать новую команду или выбрать пакетный файл, нажмите кнопку **Изменить**.

Не пытайтесь выполнить интерактивные команды, т. е. команды, требующие вмешательства пользователя (например, «pause»). Они не поддерживаются.

Редактирование пользовательских команд, выполняемых при восстановлении

Укажите пользовательские команды, которые будут выполнены перед процедурой восстановления или после нее:

- В поле **Команда** введите команду или выберите ее из списка. Чтобы выбрать пакетный файл, нажмите кнопку **...**.
- В поле **Рабочая папка** введите путь для выполнения команды или выберите его из списка использованных путей.

- В поле **Аргументы** введите или выберите из списка аргументы исполняемой команды.

Снятие флажка у параметра **Не выполнять операции до завершения исполнения команды**, установленного по умолчанию для команд, выполняемых перед резервным копированием, позволит процессу восстановления протекать одновременно с выполнением пользовательских команд.

Параметр **При возникновении ошибки отменить выполнение операции** (включен по умолчанию) прервет процедуру при возникновении каких-либо ошибок, произошедших во время выполнения команды.

Чтобы проверить созданную команду, нажмите кнопку **Тест команды**.

Параметры проверки

Расположение: **Параметры восстановления** → **Дополнительно** → **Проверка**

- **Проверять резервную копию перед восстановлением** — включите этот параметр, чтобы выполнить проверку целостности резервной копии перед восстановлением.
- **Проверять файловую систему после восстановления** — включите этот параметр, чтобы проверить целостность файловой системы на восстановленном разделе.

> **Примечание**
>
> - Проверить можно только файловые системы FAT16/32 и NTFS.
> - Файловая система не будет проверена, если при восстановлении требуется перезагрузка, например, при восстановлении системного раздела в исходное место.

Перезагрузка компьютера

Расположение: **Параметры восстановления** → **Дополнительно** → **Перезагрузка компьютера**

Если необходимо, чтобы компьютер перезагружался автоматически, когда это требуется для восстановления, установите флажок **При необходимости автоматически перезагружать компьютер во время восстановления**. Это может потребоваться, если восстанавливаемый раздел заблокирован операционной системой.

Параметры восстановления файлов

Расположение: **Параметры восстановления** → **Дополнительно** → **Параметры восстановления файлов**

Задайте следующие параметры восстановления файлов:

- **Восстанавливать файлы, сохраняя настройки безопасности** — если настройки безопасности файлов были сохранены при резервном копировании (см. *Параметры безопасности файлов для*

создаваемой резервной копии) , вы можете выбрать восстановить файлы вместе с настройками или позволить файлам унаследовать настройки безопасности папки, в которую они будут восстановлены. Данный параметр действует только при восстановлении файлов из резервных копий файлов и папок.

- **Устанавливать текущую дату для восстановленных файлов** — выберите, восстанавливать дату и время файла из резервной копии или присваивать текущее значение даты и времени. По умолчанию восстановленным файлам будут присвоены дата и время из резервной копии.

Параметры перезаписи файлов

Расположение: **Параметры восстановления** → **Дополнительно** → **Параметры перезаписи файлов**

Укажите, что должна делать программа при обнаружении в целевой папке файлов с именами, совпадающими с именами файлов из резервной копии.

> **Примечание**
>
> Этот вариант доступен только при восстановлении файлов и папок (при восстановлении дисков и разделов он недоступен).

Установите флажок **Заменять существующие файлы**, чтобы файлы на жестком диске перезаписывались файлами из резервной копии.

В разделе **Не заменять** установите флажок **Более новые файлы и папки**, чтобы запретить перезапись новых файлов и папок.

Производительность операций восстановления

Расположение: **Параметры восстановления** → **Дополнительно** → **Производительность**

Можно настроить следующие параметры.

Приоритет операции

Изменение приоритета операции резервного копирования или восстановления может ускорить или замедлить процесс (в зависимости от того, был ли приоритет повышен или понижен), но также существенно влияет на производительность других выполняющихся программ. Приоритет каждого протекающего в системе процесса определяет долю выделяемых этому процессу системных ресурсов и процессорного времени. Понижение приоритета операции освободит часть ресурсов для других выполняемых компьютером задач. Повышение приоритета резервного копирования или восстановления, напротив, может ускорить процесс за счет отбора ресурсов у параллельных задач.

Насколько будет выражен этот эффект, зависит от общей загрузки процессора и других факторов.

Приоритеты операции:

- **Низкий** (выбран по умолчанию) — процесс резервного копирования или восстановления будет выполняться медленнее, но скорость работы других программ будет выше.
- **Обычный** — процесс резервного копирования или восстановления будет выполняться наравне с другими процессами системы.
- **Высокий** — процесс резервного копирования или восстановления будет происходить быстрее за счет уменьшения производительности других программ. Учтите, что при выборе этого варианта Кибер Бэкап Старт может использовать 100% ресурсов компьютера.

Уведомления при восстановлении

Расположение: **Параметры восстановления** → **Уведомления**

Иногда резервное копирование или восстановление может длиться час или более. Кибер Бэкап Старт может уведомлять о завершении операции по электронной почте. Также возможна отправка дубликатов сообщений, выдаваемых в процессе работы программы, и полного журнала операции после ее завершения.

По умолчанию отправка любых уведомлений отключена.

> **Примечание**
>
> Сообщение не будет показано, если в настройках **Обработка ошибок** установлен флажок **Не показывать сообщения и диалоговые окна во время выполнения операции**.

Уведомление по электронной почте

1. Выберите флажок **Отправлять по электронной почте уведомления о состоянии операции**.
2. Настройте параметры электронной почты:
   - Введите адрес электронной почты в поле **Кому**. Можно ввести несколько адресов, разделенных точкой с запятой.
   - Укажите сервер исходящей почты (SMTP) в поле **Настройки сервера**.
   - Укажите порт сервера исходящей почты. По умолчанию используется порт 25.
   - При необходимости установите флажок **Проверка подлинности SMTP** и введите имя пользователя и пароль в соответствующие поля.

3. Чтобы проверить правильность настроек, нажмите кнопку **Отправить тестовое сообщение**.

Если не удается отправить тестовое сообщение:

1. Щелкните **Расширенные настройки**.
2. Настройте дополнительные параметры электронной почты:
    - Введите адрес электронной почты отправителя в поле **От**. Если вы не знаете, какой адрес указывать, наберите любой адрес в стандартном формате, например *aaa@bbb.com*.
    - При необходимости измените тему сообщения в поле **Тема**.
    - Установите флажок **Логин для сервера входящей почты**.
    - Укажите сервер входящей почты (POP3) в поле **Сервер POP3**.
    - Укажите порт сервера входящей почты. По умолчанию используется порт 110.
3. Снова нажмите кнопку **Отправить тестовое сообщение**.

Дополнительные параметры уведомления:

- Чтобы отправлять уведомления о завершении процесса, установите флажок **Отправлять уведомления об успешном завершении операции**.
- Чтобы отправлять уведомления в случае сбоя процесса, установите флажок **Отправлять уведомления при возникновении ошибки операции**.
- Чтобы отправлять уведомления с сообщениями об операции, установите флажок **Оповещать о необходимости вмешательства пользователя**.
- Чтобы отправлять уведомления с полным журналом операций, установите флажок **Присоединять к уведомлению полный журнал**.

Архивирование данных

Что такое архивирование данных

Функция архивирования данных позволяет перенести большие и редко используемые файлы в Кибер Облако, на устройство NAS, внешний жесткий диск или флеш-накопитель USB. При каждом запуске она анализирует данные в выбранной папке и предлагает загрузить найденные файлы в Кибер Облако или перенести в локальное хранилище. Можно выбрать файлы и папки, которые необходимо архивировать. После отправки в архив локальные копии этих файлов удаляются. Ссылки на файлы хранятся в специальном месте, которое называется Cyber Drive. Вы можете обратиться к этому архиву, как к обычной папке в проводнике Windows. Если дважды щелкнуть ссылку файла, файл откроется, как если бы он хранился в локальной папке. Если файл архивирован в Кибер Облако, сначала он будет снова загружен на компьютер. Доступ к файлам и управление ими также можно выполнять непосредственно в Кибер Облаке.

Основные характеристики архивирования данных

- **Экономия места в хранилище данных**

  Как правило, больше всего места на современных жестких дисках большой емкости занимают такие данные пользователей, как фотографии и документы, а не операционная система и приложения. Поскольку большая часть этих данных используется лишь изредка, нет необходимости хранить их на локальных дисках. Архивирование данных позволяет освободить место для хранения часто используемых файлов.

- **Облачное архивирование и локальное архивирование**

  Можно выбрать тип хранилища для своего архива: Кибер Облако или локальное устройство, такое как внутренний жесткий диск, внешний жесткий диск, устройство NAS или флеш-накопитель USB. Каждый раз, когда в качестве места назначения выбирается Кибер Облако, выбранные данные сохраняются в одном и том же облачном архиве. Локальные архивы не зависят друг от друга и могут иметь разные имена, местоположение, параметры защиты паролем и т. д., хотя в качестве места хранения можно выбрать уже существующий архив, а не создавать новый. Количество локальных архивов не ограничено.

- **Простой доступ к облачному архиву с любого устройства**

  Доступ к архивным файлам в Кибер Облаке возможен через Кибер Бэкап Старт и веб-интерфейс Кибер Облака с любого устройства под управлением Windows, macOS, iOS и Android, включая планшеты и смартфоны.

- **Защита данных в облачном архиве**

  Хранящиеся в Кибер Облаке данные защищены от повреждений и аварий. Например, если локальный жесткий диск вашего компьютера выйдет из строя, можно будет загрузить на новый диск файлы из облака. Кроме того, данные хранятся в защищенном виде. Поэтому доступ к вашим данным имеете только вы.

Что исключается из архивов

Чтобы уменьшить размер архивов и исключить возможность повреждения системы, Кибер Бэкап Старт по умолчанию исключает из архивов следующие данные:

- `pagefile.sys`
- `swapfile.sys`
- Папка `Temp`
- Папка `System Volume Information`
- Корзина
- Временные данные веб-браузера:
  - Временные файлы Интернета
  - Кэш
- Файлы TIB и TIBX
- Файлы .tib.metadata и .tibx.metadata
- TMP-файлы
- Файлы с расширением .~

Полный список файлов см. в статье Базы знаний: https://kb.cyberprotect.ru/articles/199.

Чем архивирование в облако отличается от резервного копирования в онлайн-хранилище

Архивирование данных в Кибер Облако похоже на резервное копирование в онлайн-хранилище, но есть ряд отличий.

	Резервное копирование в онлайн-хранилище	**Архивирование в облако**
Назначение функции	Защита данных на случай повреждения операционной системы, жестких дисков или отдельных файлов.	Освобождение места на локальном устройстве хранения и перемещение данных в Кибер Облако.
Защита данных	• Полная защита всех имеющихся в компьютере данных, особенно операционной системы. • Защита часто используемых файлов.	Защита редко используемых и старых файлов. Как правило, это личные документы, фотографии и прочие подобные файлы.
Выбор исходных данных	Выбор вручную	Выбор автоматически найденных файлов вручную.
Обработка исходных данных	Исходные данные остаются на своем первоначальном месте.	Исходные данные удаляются из их первоначального места. Такая защита гарантирует, что ваши данные не попадут в чужие руки, если кто-то украдет ваш компьютер или жесткий диск.
Частота изменения данных	Данные, подлежащие резервному копированию, изменяются часто. У резервной копии обычно много версий, которые время от времени обновляются.	Данные, подлежащие архивированию, изменяются редко. У файлов нет версий.

Удаление дубликатов

Перед архивированием данных вы можете найти и удалить файлы-дубликаты, чтобы уменьшить размер архива.

Выполните следующие шаги:

1. Чтобы найти дубликаты, перейдите в раздел **Архив** и нажмите **Анализ домашней папки** внизу справа.

   По завершении анализа на экране появится список дубликатов, а также их оригиналов.

2. Выберите дубликаты (или оригиналы) для удаления.

   Одиночные файлы можно выделить вручную. Чтобы выбрать сразу все дубликаты, нажмите

Выделить дубликаты.

3. Чтобы удалить выбранные файлы, нажмите **Удалить**.

> **Важно**
>
> Файлы будут удалены окончательно, без перемещения в Корзину.

Создание архивов

Архивирование данных позволяет освободить место на устройстве хранения данных путем переноса старых или редко используемых файлов в Кибер Облако или локальное хранилище. Дополнительные сведения см. в разделе *Что такое архивирование данных*.

Как выполнить архивирование данных:

1. Запустите Кибер Бэкап Старт и перейдите в раздел **Архив**.
2. [Необязательно] Чтобы ознакомиться с основами архивирования данных, посмотрите слайды «Начало работы».
3. Выберите один из следующих вариантов.
   - Чтобы выполнить анализ файлов в папке пользователя Windows по умолчанию (обычно это папка `C:\Users\<имя_пользователя>`), щелкните **Анализ домашней папки**.
   - Чтобы выполнить анализ файлов в другой папке, щелкните стрелку «вниз», щелкните **Выбрать другую папку**, а затем выберите нужную папку.

   Кибер Бэкап Старт выполнит анализ файлов на компьютере. Этот процесс может занять несколько минут.
4. Слева выберите категорию данных. Затем справа выберите файлы и папки, которые необходимо архивировать.

   При выборе найденных файлов можно их отсортировать, например, по размеру или возрасту (дате последнего изменения). Для сортировки файлов щелкните заголовок нужного столбца.
5. Нажмите **Выбор хранилища**, а затем выберите Кибер Облако или локальное хранилище для архивных файлов.
6. [Необязательно] Выберите **Параметры**, чтобы задать параметры архива. Дополнительные сведения см. в разделе *Параметры архивирования данных*.
7. Нажмите кнопку **Архивировать**.

8. Подтвердите, что хотите перенести файлы в архив и автоматически удалить их со своего компьютера.

Параметры архивирования данных

Для защиты архивных данных от несанкционированного доступа можно защитить архив с помощью пароля с высокой степенью защиты.

> **Примечание**
>
> Нельзя задать или изменить параметр защиты архива паролем для уже существующего архива.

Защита архива паролем:

1. При настройке первого процесса архивирования щелкните **Параметры**.
2. Установите флажок **Защитить архив паролем с использованием высокой степени защиты**.
3. Введите пароль для архива в соответствующее поле. Рекомендуется использовать сложный пароль длиной более семи символов, содержащий как буквы (прописные и строчные), так и цифры.

   > **Примечание**
   >
   > Извлечь пароль невозможно. Запомните пароль, указанный вами для защиты архива.

Кибер Бэкап Старт запрашивает пароль при каждой попытке изменения архива. Для доступа к архиву необходимо ввести правильный пароль.

Доступ к архивным файлам

После успешного архивирования файлов доступ к ним можно получить следующими способами.

- **Проводник Windows**

  Откройте проводник Windows и выберите **Cyber Drive** в разделе **Избранное**.

  С файлами можно работать в режиме «только чтение». Чтобы изменить файл, сначала скопируйте его в другую папку.

- **Кибер Облако** (только для облачного архива)

  Откройте веб-интерфейс Кибер Облака одним из следующих способов.

  - Запустите Кибер Бэкап Старт, щелкните **Архив** и выберите **Просмотреть в веб-браузере**.

- Войдите в свою учетную запись Киберпротект и перейдите в раздел **Резервные копии**.

Клонирование и перенос диска

В ходе этой операции выполняется копирование всего содержимого одного диска на другой диск. Например, это может быть необходимо, если требуется перенести операционную систему, приложения и данные на новый диск большей емкости. Это можно сделать двумя способами.

- *Использовать утилиту клонирования диска*.
- *Создать резервную копию старого диска, а затем восстановить ее на новый диск*.

Утилита клонирования дисков

Используйте утилиту клонирования дисков для создания клона операционной системы на другом жестком диске путем копирования разделов.

Перед началом операции:

- Если необходимо клонировать систему на жесткий диск большей емкости, рекомендуется сразу установить целевой (новый) диск в место планируемого использования, а исходный диск — в другое место, например во внешний USB-корпус. Это особенно важно для ноутбуков.

  Примечание

  - Рекомендуется, чтобы старый и новый диски работали в одном режиме контроллера (например, IDE или AHCI). Иначе компьютер может не загружаться с нового жесткого диска.
  - Если клонировать диск с Windows на внешний жесткий диск USB, загрузка с него может быть невозможна. Рекомендуется выполнить клонирование на внутренний твердотельный накопитель или жесткий диск.

- Утилита клонирования диска не поддерживает мультизагрузочные системы.
- Программа отмечает поврежденные разделы красным кружком с белым крестом внутри в левом верхнем углу. Перед началом клонирования необходимо проверить такие диски соответствующими средствами операционной системы для выявления и устранения ошибок.
- Настоятельно рекомендуется создать резервную копию целого исходного диска в качестве меры предосторожности. Это может сохранить данные в случае, если что-либо произойдет с исходным жестким диском во время клонирования. Сведения о том, как создать такую резервную копию, см. в разделе *Резервное копирование разделов и дисков*. После создания резервной копии не

забудьте выполнить ее проверку.

Мастер клонирования дисков

Перед началом работы рекомендуем прочитать общие сведения об *утилите клонирования диска*. Если вы используете компьютер UEFI, то при запуске клонирования с загрузочного носителя обратите внимание на режим загрузки носителя в UEFI BIOS. Рекомендуется использовать режим загрузки, соответствующий типу операционной системы в резервной копии. Если резервная копия содержит систему BIOS, загрузите носитель в режиме BIOS; если систему UEFI, то убедитесь, что установлен режим UEFI.

Как клонировать диск:

1. Запустите Кибер Бэкап Старт.
2. На боковой панели щелкните **Инструменты** и выберите **Клонирование диска**.
3. На шаге **Режим клонирования** выберите режим переноса.
   - **Автоматически** — рекомендуется в большинстве случаев.
   - **Вручную** — ручной режим предоставляет большую гибкость при передаче данных. Ручной режим используется, если необходимо изменить структуру разделов на диске.

   Примечание

   Если программа обнаружит на компьютере два диска, один из которых содержит разделы, а другой — нет, она автоматически распознает диск с разделами как исходный, а диск без разделов как целевой. В этом случае следующие шаги будут пропущены и откроется экран **Сводные данные**.

4. На шаге **Исходный диск** выберите диск, который необходимо клонировать.

   Примечание

   Кибер Бэкап Старт не поддерживает клонирование динамических дисков.

5. На шаге **Целевой диск** выберите диск, на который будут перенесены клонированные данные.

   Если выбранный целевой диск содержит разделы, необходимо будет подтвердить их удаление. Обратите внимание, что фактическое уничтожение данных будет произведено только после нажатия кнопки **Приступить** на последнем шаге мастера.

Примечание

Если на одном из дисков разделы отсутствуют, программа сама определит, что данный диск является целевым, и текущий шаг будет пропущен.

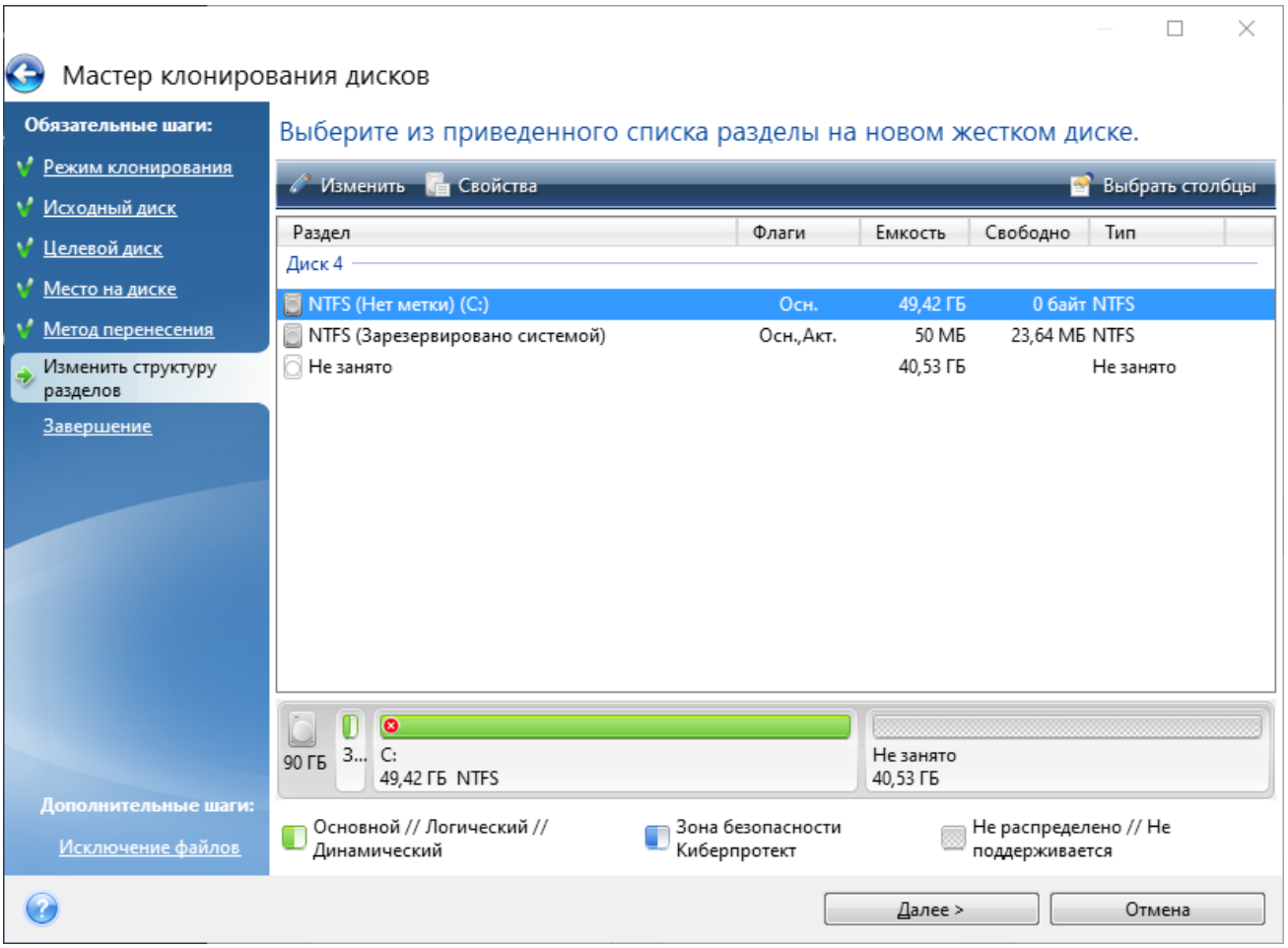
6. [Этот шаг доступен, только если на исходном диске установлена ОС.] На шаге **Место на диске** выберите, как будет использоваться клонированный диск.
   - **Для замены диска на этой машине** будут скопированы данные системного диска, клонированный диск будет загрузочным. Используйте этот клонированный диск для замены системного диска новым на этом ПК.
   - **Для использования на другой машине** будут скопированы данные системного диска, клонированный диск будет загрузочным. Используйте этот клонированный диск для переноса всех данных на другой ПК на загрузочном диске.
   - **Для использования в качестве диска с данными** будут скопированы данные на диске. Используйте этот клонированный диск в качестве незагрузочного диска данных.
7. [Этот шаг доступен только в ручном режиме клонирования.] На шаге **Метод перенесения** выберите способ перемещения данных.
   - **Один в один** — для каждого раздела старого диска на новом диске будет создан раздел того же типа и размера, с той же файловой системой и меткой тома. Неиспользованное место станет нераспределенным.
   - **Пропорционально** — место на новом диске пропорционально распределяется между переносимыми разделами старого диска.
   - **Вручную** — пользователь самостоятельно указывает новый размер и другие параметры.
8. [Этот шаг доступен только в ручном режиме клонирования.] На шаге **Изменить структуру разделов** можно изменить параметры разделов, которые будут созданы на целевом диске. Дополнительные сведения см. в разделе *Создание разделов вручную*.
9. [Необязательно] На шаге **Исключение файлов** можно указать файлы и папки, которые не следует клонировать. Дополнительные сведения см. в разделе *Исключение элементов из клонирования*.
10. На шаге **Завершение** убедитесь, что настроенные параметры соответствуют вашим целям, и нажмите кнопку **Приступить**.

Если операция клонирования будет по какой-то причине остановлена, потребуется заново настроить и запустить процедуру. Данные не будут потеряны, так как во время клонирования Кибер Бэкап Старт не изменяет исходный диск и хранящиеся на нем данные.

По умолчанию Кибер Бэкап Старт выключает компьютер после завершения процесса клонирования. Это позволит извлечь один из жестких дисков.

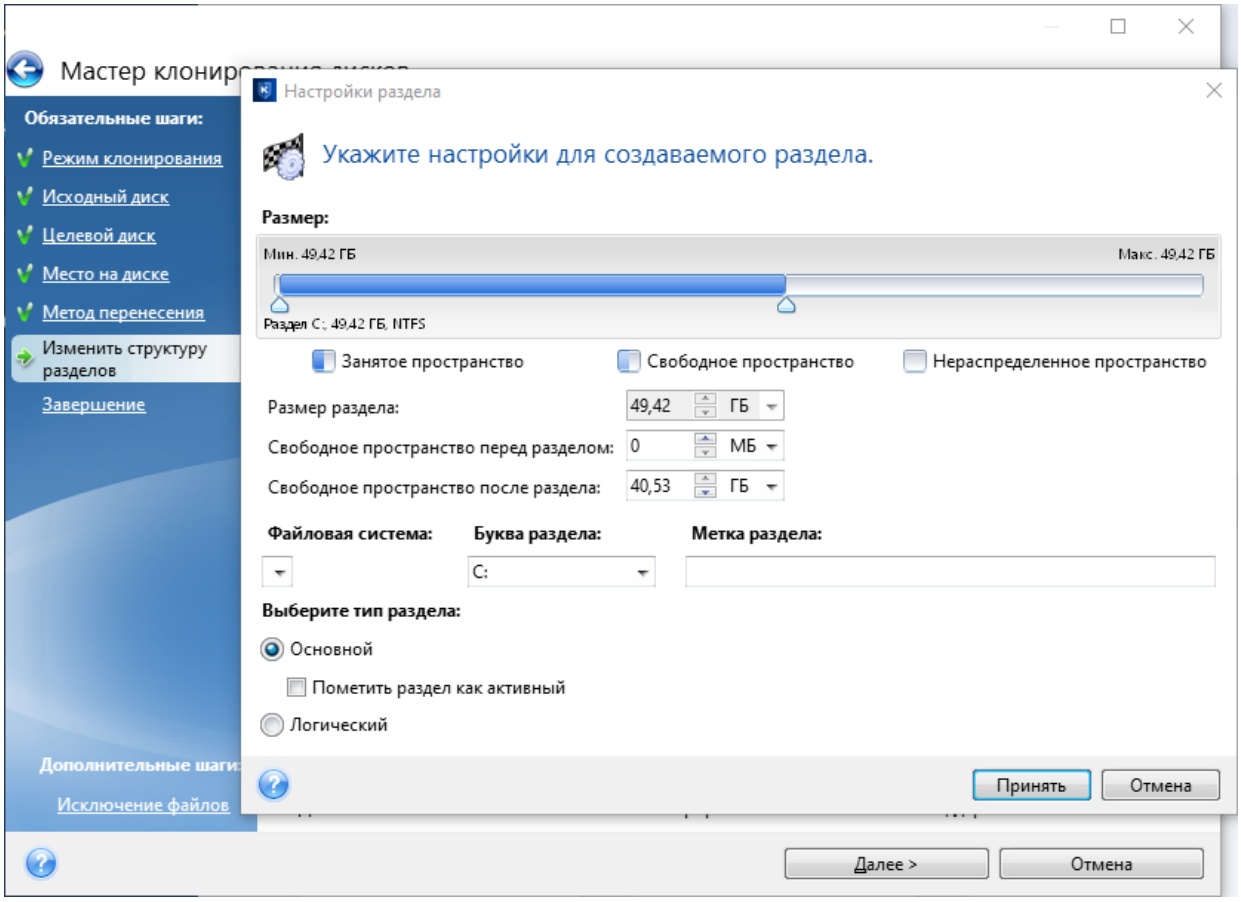
Создание разделов вручную

Ручной способ переноса позволяет изменить размеры любого раздела на новом диске. По умолчанию программа изменяет размер разделов пропорционально.



Как изменить раздел:

1. Выберите раздел, затем нажмите кнопку **Изменить**. При этом откроется окно параметров раздела.



2. Укажите следующие настройки для раздела:

   - Размер и положение
   - Файловая система
   - Тип раздела (доступно только для MBR-дисков)
   - Буква и метка раздела

   Дополнительные сведения см. в разделе *Настройки раздела*.

3. Нажмите кнопку **Принять**.

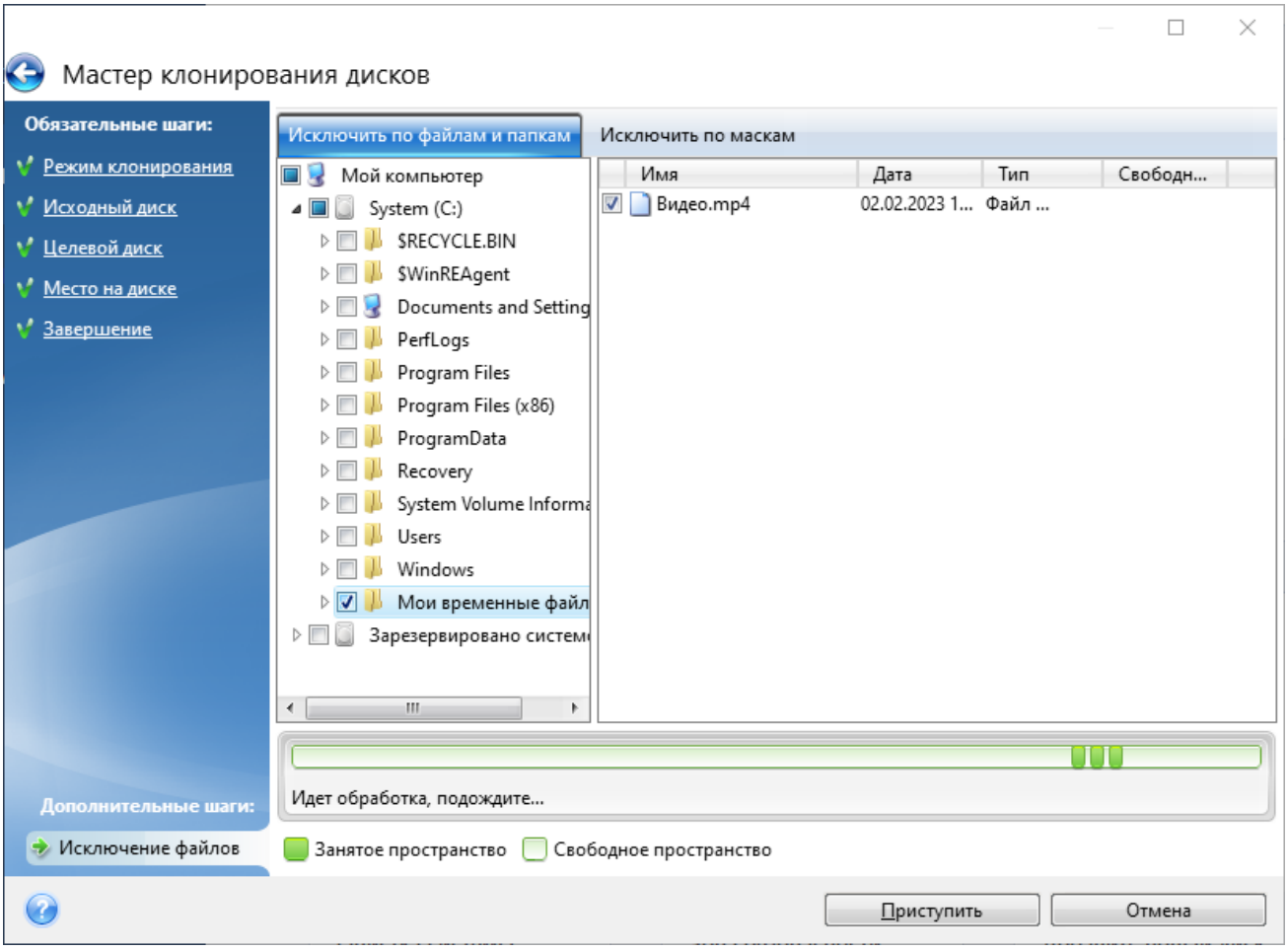
Предупреждение

Если нажать любой из предыдущих шагов мастера на боковой панели в этом окне, будут сброшены все изменения размера и расположения, так что их придется задать заново.

Исключение элементов из клонирования

Чтобы не выполнять клонирование определенных файлов с исходного диска (например, когда размер целевого диска меньше исходного), можно исключить их на шаге **Исключение файлов**.

> **Примечание**
>
> При клонировании системного раздела не рекомендуется исключать скрытые и системные файлы.



Существует два способа исключить файлы и папки:

- **Исключить по файлам и папкам** — на этой вкладке можно выбрать определенные папки и файлы из дерева папок.
- **Исключить по маскам** — на этой вкладке можно исключить группу файлов по маске либо отдельный файл, указав имя или путь.

  Чтобы добавить критерий исключения, щелкните **Добавить**, введите имя файла, путь или маску и нажмите кнопку **ОК**. Количество добавляемых файлов и масок не ограничено.

Примеры критериев исключения:

- Можно ввести имя файла полностью:
  - `file.ext` — все файлы с данным именем и расширением будут исключены из клонирования.
  - `C:\file.ext` — файл `file.ext` на диске C: будет исключен.
- Можно ввести подстановочные знаки (* и ?):
  - `*.ext` — все файлы с расширением EXT будут исключены.
  - `??name.ext` — все файлы с расширением EXT, имеющие шесть букв в имени (которое начинается с любых двух символов (??) и заканчивается на *name*), будут исключены.
- Можно ввести путь к папке:
  - `C:\изображения` — папка с изображениями на диске C: будет исключена.

Изменить или удалить критерии исключения можно с помощью соответствующих кнопок на правой панели.

Способ миграции

Кибер Бэкап Старт позволяет выбрать структуру разделов для целевого диска после завершения операции клонирования.

- **MBR (основной загрузочный сектор)** — загрузочный сектор размером 512 байт, который является первым сектором жесткого диска и используется для размещения таблицы основных разделов диска.
- **GPT (таблица разделов GUID)** — это стандарт структуры таблицы разделов для жестких дисков. GPT поддерживает диски и разделы размером до 9,4 ЗБ (9,4 x 10^21 байт).

С помощью этого мастера можно преобразовать структуру разделов во время операции клонирования или клонировать разделы «один в один» без изменения структуры.

- **Копировать разделы без изменений** — выберите этот вариант для миграции системы один в один, без изменения структуры разделов. Обратите внимание, что в этом случае дисковое пространство за пределами 2 ТБ будет недоступно. Чтобы распределить дисковое пространство за пределами 2 ТБ, можно использовать диспетчер дисков расширенной емкости Киберпротект.
- **Копировать разделы и использовать диск как несистемный в стиле GPT** — выберите этот вариант, чтобы преобразовать раздел в структуру GPT.

С помощью Кибер Бэкап Старт также можно преобразовывать системы **BIOS** в **UEFI**. Дополнительные сведения см. в разделе *Интерфейс UEFI*.

Система загружается с помощью BIOS, MBR, UEFI не поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI не поддерживается.
- **Размер целевого диска**: меньше 2 ТБ.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью BIOS.
- **Стиль разделов**: MBR.
- **Операционная система**: Windows, загрузка в UEFI не поддерживается.
- **Размер диска**: доступно все дисковое пространство.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система, загружаемая с помощью BIOS, MBR, поддержка UEFI

На этом этапе мастера необходимо выбрать целевой жесткий диск.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI поддерживается.
- **Размер целевого диска**: меньше 2 ТБ.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью BIOS.
- **Стиль разделов**: MBR.
- **Операционная система**: Windows, загрузка в UEFI поддерживается.
- **Размер диска**: доступно все дисковое пространство.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью BIOS, MBR, без Windows

Кибер Бэкап Старт позволяет выбрать структуру разделов для целевого диска после завершения операции.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: отличается от Windows или отсутствует.
- **Размер целевого диска**: меньше 2 ТБ.

При этих параметрах системы можно выбрать один из следующих вариантов:

1. **Копировать разделы без изменений**

   На целевом диске можно оставить стиль разделов MBR.

   Целевой диск после миграции:

   - **Система**: загружается с помощью BIOS.
   - **Стиль разделов**: MBR.
   - **Операционная система**: отличается от Windows или отсутствует.
   - **Размер диска**: доступно все дисковое пространство.

2. **Копировать разделы и использовать диск как несистемный в стиле GPT**

   Стиль разделов можно преобразовать в GPT.

   Целевой диск после миграции:

   - **Система**: не загружается в BIOS.
   - **Стиль разделов**: GPT.
   - **Операционная система**: отличается от Windows или отсутствует.
   - **Размер диска**: доступно все дисковое пространство.

⚠ Предупреждение

После миграции целевой диск можно использовать только как несистемный. Этот параметр недоступен при работе Кибер Бэкап Старт в операционной системе Windows XP x32.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью BIOS, GPT, UEFI поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: GPT.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI поддерживается.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: не загружается в BIOS.
- **Стиль разделов**: GPT.
- **Операционная система**: Windows, загрузка в UEFI поддерживается.
- **Размер диска**: доступно все дисковое пространство.

> **Предупреждение**
>
> После миграции операционная система не сможет загружаться с целевого диска в BIOS. Чтобы загрузиться с целевого диска после миграции, необходимо включить в системе UEFI-загрузку (см. раздел *Интерфейс UEFI*), а затем перезапустить операцию.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью BIOS, GPT, без Windows

На этом этапе мастера необходимо выбрать целевой жесткий диск.

Текущие характеристики системы:

- **Система**: загружается с помощью BIOS.
- **Исходный стиль разделов**: GPT.
- **Операционная система на исходном диске**: отличается от Windows или отсутствует.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью BIOS.
- **Стиль разделов**: GPT.
- **Операционная система**: отличается от Windows или отсутствует.

- **Размер диска**: доступно все дисковое пространство.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью UEFI, MBR, UEFI не поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI не поддерживается.
- **Размер целевого диска**: меньше 2 ТБ.

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: не загружается в UEFI.
- **Стиль разделов**: MBR.
- **Операционная система**: Windows, загрузка в UEFI не поддерживается.
- **Размер диска**: доступно все дисковое пространство.

Предупреждение

Операционная система может не загрузиться в UEFI с целевого диска.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью UEFI, MBR, UEFI поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: Windows, загрузка в UEFI поддерживается.

При миграции системы на выбранный диск со следующими характеристиками:

После миграции стиль разделов целевого диска будет преобразован в GPT, и с него можно будет загрузиться.

Целевой диск после миграции:

- **Система**: загружается с помощью UEFI.
- **Стиль разделов**: GPT.
- **Операционная система**: Windows, загрузка в UEFI поддерживается.
- **Размер диска**: доступно все дисковое пространство.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система на основе UEFI, MBR, Windows отсутствует

Кибер Бэкап Старт позволяет выбрать структуру разделов для целевого диска после завершения операции.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI.
- **Исходный стиль разделов**: MBR.
- **Операционная система на исходном диске**: отличается от Windows или отсутствует.
- **Размер целевого диска**: меньше 2 ТБ.

При этих параметрах системы можно выбрать один из следующих вариантов:

1. **Копировать разделы без изменений**

   На целевом диске можно оставить стиль разделов MBR.

   Целевой диск после миграции:

   - **Система**: загружается с помощью UEFI.
   - **Стиль разделов**: MBR.
   - **Операционная система**: отличается от Windows или отсутствует.
   - **Размер диска**: доступно все дисковое пространство.

2. **Копировать разделы и использовать диск как несистемный в стиле GPT**

   Стиль разделов можно преобразовать в GPT.

   Целевой диск после миграции:

   - **Система**: не загружается в UEFI.
   - **Стиль разделов**: GPT.

- **Операционная система**: отличается от Windows или отсутствует.
- **Размер диска**: доступно все дисковое пространство.

> **Предупреждение**
>
> После миграции целевой диск можно использовать только как несистемный.

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система загружается с помощью UEFI, GPT, UEFI поддерживается

На этом этапе мастера необходимо выбрать целевой жесткий диск.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI
- **Исходный стиль разделов**: GPT
- **Операционная система:** Windows, загрузка в UEFI поддерживается

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью UEFI
- **Стиль разделов**: GPT
- **Размер диска**: доступно все дисковое пространство

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Система, загружаемая с помощью UEFI, GPT, без Windows

На этом этапе мастера необходимо выбрать целевой жесткий диск.

В настоящее время ваша система имеет следующие характеристики:

- **Система**: загружается с помощью UEFI
- **Исходный стиль разделов**: GPT
- **Операционная система**: отличается от Windows или отсутствует

При миграции системы на выбранный диск со следующими характеристиками:

- **Система**: загружается с помощью UEFI
- **Стиль разделов**: GPT

- **Размер диска**: доступно все дисковое пространство

Дополнительные сведения о процедуре миграции см. в разделе *Способ миграции*.

Перенос системы с жесткого диска на твердотельный накопитель

Прежде всего убедитесь, что Кибер Бэкап Старт распознает новый твердотельный накопитель как в Windows, так и в среде компонента загрузочного носителя. При возникновении проблем см. раздел *Что делать, если Кибер Бэкап Старт не распознает твердотельный накопитель*.

Размер твердотельного накопителя

Так как твердотельные накопители обычно имеют меньшую емкость, чем жесткие диски, занятое пространство на вашем жестком диске может превышать размер имеющегося твердотельного накопителя. В таком случае перенос невозможен.

Чтобы уменьшить объем данных на системном диске, попробуйте выполнить следующие действия.

- Переместите файлы данных со старого жесткого диска в другое расположение, например на другой жесткий диск (внутренний или внешний).
- Создайте ZIP-архивы файлов данных (например, ваших документов, фотографий, аудиофайлов и т. д.), после чего удалите исходные файлы.
- Очистите жесткий диск с помощью утилиты Windows «Очистка диска».

Обратите внимание, что для стабильной работы Windows требуется несколько гигабайт свободного пространства в системном разделе.

Какой способ переноса выбрать

Если системный диск состоит из одного раздела (не считая скрытого раздела «Зарезервировано системой»), можно попробовать выполнить перенос на твердотельный накопитель с помощью средства клонирования. Дополнительные сведения см. в разделе *Клонирование жесткого диска*.

Однако в большинстве случаев рекомендуется использовать резервное копирование и восстановление. Этот метод обеспечивает большую гибкость и контроль над переносом. См. раздел *Перенос системы на твердотельный накопитель методом резервного копирования и восстановления*.

Что делать, если Кибер Бэкап Старт не распознает твердотельный накопитель

Иногда Кибер Бэкап Старт может не распознавать твердотельный накопитель.

В таком случае проверьте, распознается ли твердотельный накопитель в BIOS.

Если BIOS вашего компьютера не показывает твердотельный накопитель, проверьте, что кабель питания и кабели данных правильно подключены. Можно также попробовать обновить драйверы BIOS и SATA. Если это не поможет, свяжитесь со службой поддержки производителя твердотельного накопителя.

Если BIOS компьютера показывает твердотельный накопитель:

1. В поле «Поиск» или «Запустить» (в зависимости от операционной системы) введите **cmd** и нажмите клавишу `Enter`.
2. В командной строке введите:

   ```
   diskpart
   list disk
   ```

   На экране появятся диски, подключенные к компьютеру. Выясните номер диска для твердотельного накопителя. В качестве отправной точки используйте размер диска.
3. Для выбора диска выполните следующую команду:

   ```
   select disk N
   ```

   Здесь N — номер диска вашего твердотельного накопителя.
4. Чтобы удалить всю информацию с твердотельного накопителя и заменить запись MBR на стандартную, выполните команду:

   ```
   clean
   exit
   exit
   ```

Запустите Кибер Бэкап Старт и проверьте, обнаруживает ли программа твердотельный накопитель. Если твердотельный накопитель обнаруживается, используйте инструмент добавления новых дисков, чтобы создать на диске один раздел, занимающий все дисковое пространство. Создавая раздел, проверьте, что свободное пространство перед разделом составляет 1 МБ. Дополнительные сведения см. в разделе *Добавление нового жесткого диска*.

Как проверить, распознает ли загрузочный носитель твердотельный накопитель:

1. Выполните загрузку, используя загрузочный носитель.
2. Выберите в главном меню **Инструменты и утилиты** → **Добавить новый диск**, и на экране **Выбор диска** появятся сведения обо всех жестких дисках в системе. Используйте это, чтобы проверить, обнаруживается ли твердотельный накопитель в среде восстановления.
3. Если твердотельный накопитель отображается на экране, просто нажмите кнопку **Отмена**.

Если загрузочный носитель не распознает твердотельный накопитель, а режим контроллера твердотельных накопителей — AHCI, можно попробовать изменить режим на IDE (или ATA в некоторых брендах BIOS) и посмотреть, решит ли это проблему.

> **Предупреждение**
>
> Внимание! Не запускайте Windows после изменения режима: это может вызвать серьезные системные проблемы. Прежде чем запускать Windows, вернитесь в режим AHCI.

Если после изменения режима загрузочный носитель обнаруживает твердотельный накопитель, можно использовать следующую процедуру для восстановления или клонирования с загрузочного носителя.

1. Выключите компьютер.
2. Загрузите BIOS, измените режим с AHCI на IDE (или ATA в некоторых брендах BIOS).
3. Выполните загрузку, используя загрузочный носитель.
4. Восстановите или клонируйте диск.
5. Загрузите BIOS и вернитесь из режима IDE в режим AHCI.
6. Запустите Windows.

Что делать, если вышеуказанные действия не помогают

Можно попробовать создать носитель на основе WinPE. Это может обеспечить необходимые драйверы. Дополнительные сведения см. в разделе *Как создать загрузочный носитель*.

Перенос системы на твердотельный накопитель методом резервного копирования и восстановления

Следующую процедуру можно использовать во всех поддерживаемых операционных системах. Сначала рассмотрим простой случай: системный диск состоит из одного раздела. Обратите внимание, что на системном диске может быть скрытый раздел «Зарезервировано системой».

Рекомендуется перенести систему на пустой твердотельный накопитель, который не содержит разделов

(т. е. дисковое пространство не распределено). Если твердотельный накопитель новый и еще не использовался, разделов на нем нет.

Как перенести систему на твердотельный накопитель:

1. Запустите Кибер Бэкап Старт.
2. Если загрузочный носитель отсутствует, создайте его. Для этого в разделе **Инструменты** щелкните **Создать загрузочный носитель** и следуйте инструкциям на экране.
3. Создайте резервную копию всего системного диска (в режиме резервного копирования диска) на жестком диске, отличном от системного и от твердотельного накопителя.
4. Выключите компьютер и отсоедините системный жесткий диск.
5. Подключите твердотельный накопитель к слоту, где был подключен жесткий диск.

   Примечание

   Некоторые марки твердотельных накопителей может потребоваться вставить в слот PCI Express.

6. Выполните загрузку, используя загрузочный носитель.
7. Выполните проверку резервной копии, чтобы убедиться, что она пригодна для восстановления. Для этого щелкните **Восстановление** на панели слева и выберите резервную копию. Щелкните правой кнопкой мыши, выберите в контекстном меню пункт **Проверить архив** и нажмите кнопку **Приступить**.
8. После завершения проверки щелкните резервную копию правой кнопкой мыши и выберите пункт **Восстановить** в контекстном меню.
9. На шаге **Метод восстановления** выберите **Восстановить диски или разделы** и нажмите кнопку **Далее**.
10. На шаге **Точка восстановления** выберите дату и время, на которые следует восстановить систему.
11. Выберите системный диск на шаге **Выбор элементов**.
12. На шаге **Место назначения** выберите твердотельный накопитель в качестве нового расположения системного диска, а затем нажмите кнопку **Далее**.
13. На следующем шаге нажмите кнопку **Приступить**, чтобы запустить восстановление.
14. После завершения восстановления выйдите из автономной версии Кибер Бэкап Старт.
15. Попробуйте загрузить компьютер с твердотельного накопителя и убедитесь, что Windows и приложения работают правильно.

Если на системном жестком диске имеется скрытый раздел для восстановления или диагностики, как это часто бывает на ноутбуках, процедура будет отличаться. Как правило, требуется изменить размер разделов вручную во время восстановления на твердотельный накопитель. Инструкции см. в разделе *Восстановление диска, содержащего скрытый раздел*.

Инструменты

Инструменты защиты:

- *Восстановление при загрузке*
- *Мастер создания загрузочных носителей*
- *Зона безопасности*

Клонирование диска:

- *Утилита клонирования дисков*

Безопасность и конфиденциальность:

- *Очистка диска*
- *Очистка системы*

Управление дисками:

- *Добавление нового жесткого диска*

Мастер создания загрузочных носителей

Мастер создания загрузочных носителей позволяет сделать загрузочным флеш-накопитель USB, внешний диск или чистый диск CD/DVD. Если Windows не запускается, используйте загрузочный носитель, чтобы запустить автономную версию Кибер Бэкап Старт и восстановить компьютер.

Предусмотрена возможность создавать загрузочные носители нескольких типов:

- **Загрузочный носитель**

  Этот тип рекомендуется для большинства пользователей.

- **Носитель на основе WinPE с компонентом Подключаемый модуль**

  Драйверы Windows, входящие в среду предустановки, обеспечивают лучшую совместимость Кибер Бэкап Старт с аппаратной частью компьютера.

  Рекомендуется создать носитель этого типа, если не удается загрузить компьютер, используя загрузочный носитель.

  Для использования этого варианта должен быть установлен комплект средств для развертывания и оценки Windows (ADK). Он компонент требуется для создания носителей на основе WinPE 4.0,

WinPE 5.0 и WinPE 10.0.

- **Носитель на основе WinRE с компонентом Подключаемый модуль**

  Этот тип загрузочного носителя аналогичен носителям на основе WinPE, но имеет одно важное преимущество — отсутствие необходимости загружать Windows ADK с веб-сайта Майкрософт. Среда восстановления Windows (WinRE) уже входит в Windows Vista и более поздние версии Windows. Кибер Бэкап Старт использует эти системные файлы для создания носителя на основе WinRE. Как и в случае с носителем на основе WinPE, можно добавить нужные драйверы для лучшей совместимости с оборудованием. Однако носитель на основе WinRE можно использовать только на компьютере, на котором он был создан, или на компьютере с такой же операционной системой.

Примечания:

- Рекомендуется создавать новый загрузочный носитель после каждого обновления Кибер Бэкап Старт.
- Если используется не оптический носитель, он должен иметь файловую систему FAT16 или FAT32.
- Мастер создания загрузочных носителей поддерживает только x64 WinPE 3.0, WinPE 4.0, WinPE 5.0 и WinPE 10.0.
- На компьютере должно быть:
  - для WinPE 3.0 не менее 256 МБ ОЗУ;
  - для WinPE 4.0 не менее 512 МБ ОЗУ;
  - для WinPE 5.0 не менее 1 ГБ ОЗУ;
  - для WinPE 10.0 не менее 512 МБ ОЗУ.
- При загрузке с загрузочного носителя невозможно выполнять резервное копирование на диски или разделы с файловыми системами Ext2/Ext3/Ext4, ReiserFS и Linux SWAP.
- При загрузке с загрузочного носителя и использовании автономной версии Кибер Бэкап Старт невозможно восстановить файлы и папки, зашифрованные с помощью функции шифрования, имеющейся в Windows XP и более поздних операционных системах. Дополнительные сведения см. в разделе *Параметры безопасности файлов при резервном копировании*. Однако можно восстанавливать резервные копии, защищенные паролем с помощью функции защиты паролем Кибер Бэкап Старт.
- Если вы создаете загрузочный носитель на диске, где уже есть Пакет для восстановления, то Мастер создания загрузочных носителей попытается перезаписать и обновить только скрытый раздел с загрузочным носителем, не форматируя всего диска.

Как создать загрузочный носитель

1. Подключите флеш-накопитель USB или внешний жесткий диск / твердотельный накопитель, либо вставьте чистый диск CD/DVD.
2. Запустите Кибер Бэкап Старт.
3. В разделе **Инструменты** выберите **Мастер создания загрузочных носителей**.
4. Выберите метод создания.
   - **Простой** — это самый удобный вариант. Кибер Бэкап Старт выберет оптимальный тип носителя для вашего компьютера.
   - **Дополнительный** — этот вариант позволяет выбрать тип носителя. Таким образом можно создать загрузочный носитель не только для этого компьютера, но и для компьютера под управлением другой версии Windows. Дополнительные сведения см. в разделе *Мастер создания загрузочных носителей*.

     Если выбран носитель на основе WinRE или WinPE, сделайте следующее.
     - Выберите тип архитектуры носителя — 32- или 64-разрядный. Обратите внимание, что 32-разрядный загрузочный носитель будет работать только на 32-разрядных компьютерах, а 64-разрядный носитель совместим как с 32-, так и с 64-разрядными компьютерами.
     - Укажите набор средств для создания загрузочного носителя. Если выбран пакет Windows ADK, который не установлен на компьютере, потребуется загрузить его с веб-сайта Майкрософт, а затем установить необходимые компоненты: средства развертывания и среду предустановки Windows (Windows PE).

       Если на компьютере уже есть файлы WinPE, которые хранятся не в папке по умолчанию, просто укажите их расположение и Подключаемый модуль будет добавлен в существующий образ WinPE.
     - Для лучшей совместимости с оборудованием можно выбрать драйверы, которые будут добавлены на носитель.
5. Выберите место назначения для загрузочного носителя:
   - **CD;**
   - **DVD;**
   - **внешний диск;**
   - **флеш-накопитель USB.**

     Если накопитель имеет неподдерживаемую файловую систему, Кибер Бэкап Старт предложит

переформатировать его в FAT.

> **Предупреждение**
>
> При форматировании все данные на диске будут удалены без возможности восстановления.

- **Файл ISO-образа**

  Потребуется указать имя ISO-файла и целевую папку.

  После создания ISO-файла его можно записать на CD/DVD.

- **Файл WIM-образа** (доступно только для носителей на основе WinPE)

  Кибер Бэкап Старт добавит Подключаемый модуль в WIM-файл из пакета Windows ADK. Потребуется указать имя нового WIM-файла и целевую папку.

  Чтобы создать загрузочный носитель с помощью WIM-файла, сначала необходимо преобразовать его в ISO-файл. Дополнительные сведения см. в разделе *Создание ISO-файла из WIM-файла*.

> **Примечание**
>
> Если Мастер создания загрузочных носителей обнаружит на этом диске ранее созданный Пакет для восстановления, то попытается перезаписать и обновить только скрытый раздел с загрузочным носителем, не форматируя всего диска.

6. Нажмите кнопку **Приступить**.

Загрузочный носитель: параметры запуска

Здесь можно задать параметры запуска компонента загрузочный носитель, чтобы настроить параметры загрузки носителя для лучшей совместимости с отличающимся оборудованием. Доступны несколько параметров (nousb, nomouse, noapic и т. д.). Данные параметры предназначены для опытных пользователей. Если при тестировании загрузки с помощью загрузочного носителя возникают любые проблемы совместимости оборудования, рекомендуется связаться со службой технической поддержки Киберпротект.

Как добавить параметры запуска:

1. Введите команду в поле **Параметры запуска**. Можно ввести несколько команд, разделенных пробелами.

2. Для продолжения нажмите кнопку **Далее**.

Для загрузки ядра Linux в специальных режимах можно использовать следующие параметры:

- **acpi=off** — Отключает ACPI, что используется в некоторых конфигурациях оборудования.
- **noapic** — Отключает APIC (расширенный программируемый контроллер прерываний), что используется в некоторых конфигурациях оборудования.
- **nousb** — Отключает загрузку модулей USB.
- **nousb2** — Отключает поддержку USB 2.0. При использовании этого параметра устройства с интерфейсом USB 1.1 будут работать. Параметр позволяет использовать некоторые USB-накопители в режиме USB 1.1, если они не работают в режиме USB 2.0.
- **quiet** — Этот параметр включен по умолчанию, и при загрузке сообщения не выводятся. Удаление параметра приведет к тому, что сообщения будут отображаться при загрузке ядра Linux и перед запуском программы будет предложено войти в командную оболочку.
- **nodma** — Отключает режим прямого доступа к памяти (DMA) для всех IDE-дисков. Предотвращает «зависание» ядра на некоторых машинах.
- **nofw** — Отключает поддержку интерфейса FireWire (IEEE1394).
- **nopcmcia** — Отключает обнаружение устройств стандарта PCMCIA.
- **nomouse** — Отключает поддержку мыши.
- **[имя модуля]=off** — Отключает загрузку модуля (например, **sata_sis=off**).
- **pci=bios** — Принудительно заставляет использовать PCI BIOS вместо прямого доступа к устройству. Например, этот параметр может использоваться, если в машине применен нестандартный хост-мост PCI.
- **pci=nobios** — Запрещает использование BIOS PCI; разрешены только методы прямого доступа к устройствам. Например, этот параметр может использоваться, если при загрузке происходит сбой системы, вероятно вызванный BIOS.
- **pci=biosirq** — Использует вызовы BIOS PCI для получения таблицы маршрутизации прерываний. Известно, что эти вызовы работают с ошибками на некоторых машинах и их использование приводит к зависанию машины, но на других компьютерах это является единственной возможностью получения таблицы маршрутизации прерываний. Попробуйте использовать этот параметр, если ядро не может назначить IRQ или обнаружить вторичные шины PCI на системной плате.
- **vga=ask** — Получает список видеорежимов, поддерживаемых вашей видеокартой, и позволяет выбрать видеорежим, наиболее подходящий для видеокарты и монитора. Попробуйте

использовать этот параметр, если видеорежим, выбранный по умолчанию, не совместим с оборудованием.

Добавление драйверов в существующий WIM-образ

Иногда базовый диск WinPE с компонентом Подключаемый модуль не содержит драйверов для определенного оборудования, например контроллеров запоминающих устройств. Самый простой способ добавить их — выбрать расширенный режим в программе *Мастер создания загрузочных носителей* и указать нужные драйверы. Можно добавить драйверы в существующий WIM-образ вручную перед созданием ISO-файла с компонентом Подключаемый модуль.

> **⚠ Предупреждение**
>
> Внимание! Можно добавлять только драйверы с расширением файла INF.

Следующая процедура основана на статье MSDN, доступной по адресу https://technet.microsoft.com/en-us/library/dd799244(WS.10).aspx.

Как создать пользовательский образ Windows PE:

1. Если у вас нет WIM-файла с компонентом Подключаемый модуль, запустите Мастер создания загрузочных носителей и создайте такой файл, выбрав **WIM-файл** в качестве места назначения для носителя на основе WinPE. Дополнительные сведения см. в разделе *Как создать загрузочный носитель*.
2. В меню **Пуск** выберите **Windows Kits**, затем **Windows ADK**, щелкните правой кнопкой мыши пункт **Среда средств развертывания и работы с образами** и выберите **Запуск от имени администратора**.
3. Запустите сценарий `Copype.cmd`, чтобы создать папку с файлами Windows PE. Например, введите в командной строке:

   ```
   copype amd64 C:\winpe_x64
   ```

4. Скопируйте свой WIM-файл, например, в папку `C:\winpe_x64\`. По умолчанию файл называется `CyberBootablePEMedia.wim`.
5. Подключите базовый образ в локальную папку с помощью утилиты DISM. Для этого введите:

   ```
   Dism /Mount-Wim /WimFile:C:\winpe_x64\CyberBootablePEMedia.wim /index:1 /MountDir:C:\winpe_
   ↪x64\mount
   ```

6. Добавьте драйвер оборудования с помощью команды DISM с параметром `Add-Driver`. Например, чтобы добавить драйвер `Mydriver.inf`, расположенный в папке `C:\drivers\`, введите:

```
Dism /image:C:\winpe_x64\mount /Add-Driver /driver:C:\drivers\mydriver.inf
```

7. Повторите предыдущий шаг для каждого драйвера, который необходимо добавить.
8. Подтвердите изменения с помощью команды DISM:

```
Dism /Unmount-Wim /MountDir:C:\winpe_x64\mount /Commit
```

9. Создайте PE-образ (ISO-файл) из получившегося WIM-файла. Дополнительные сведения см. в разделе *Создание ISO-файла из WIM-файла*.

Создание ISO-файла из WIM-файла

Чтобы создать загрузочный носитель посредством WIM-файла, сначала необходимо преобразовать его в ISO-файл.

Как создать PE-образ (ISO-файл) из полученного WIM-файла:

1. В меню **Пуск** выберите **Windows Kits**, затем **Windows ADK**, щелкните правой кнопкой мыши пункт **Среда средств развертывания и работы с образами** и выберите **Запуск от имени администратора**.
2. Запустите сценарий `Copype.cmd`, чтобы создать папку с файлами Windows PE. Например, введите в командной строке:

```
copype amd64 C:\winpe_x64
```

3. Замените стандартный файл boot.wim в папке Windows PE созданным WIM-файлом (например, CyberBootablePEMedia.wim). Если файл CyberBootablePEMedia.wim расположен на диске C:, то:

   Для WinPE 3.0 введите:

```
copy c:\CyberBootablePEMedia.wim c:\winpe_x64\ISO\sources\boot.wim
```

   Для WinPE 4.0, WinPE 5.0 или WinPE 10.0 введите:

```
copy ”c:\CyberBootablePEMedia.wim” c:\winpe_x64\media\sources\boot.wim
```

4. Используйте инструмент `Oscdimg`. Чтобы создать ISO-файл, введите:

```
oscdimg -n –bc:\winpe_x64\etfsboot.com c:\winpe_x64\ISO c:\winpe_x64\winpe_x64.iso
```

   Либо, чтобы сделать носитель загрузочным на компьютерах BIOS и UEFI, введите:

```
oscdimg -m -o -u2 -udfver102 -bootdata:2#p0,e,bc:\winpe_x64\fwfiles\etfsboot.com#pEF,e,bc:\
↪winpe_x64\fwfiles\efisys.bin c:\winpe_x64\media c:\winpe_x64\winpe_x64.iso
```

5. Записав ISO-образ на компакт-диск с помощью сторонней программы, вы получите загрузочный диск Windows PE с программой Кибер Бэкап Старт.

Проверка загрузочного носителя на возможность использования в случае необходимости

Чтобы обеспечить максимальную вероятность восстановления компьютера, следует проверить, сможет ли этот компьютер загрузиться с загрузочного носителя. Кроме того, необходимо проверить, распознает ли загрузочный носитель все устройства вашего компьютера, такие как жесткие диски, мышь, клавиатура и сетевой адаптер.

Если вы приобрели коробочную версию продукта, в которую входит загрузочный компакт-диск, и не обновляли Кибер Бэкап Старт, то можно протестировать этот компакт-диск. В противном случае создайте новый загрузочный носитель. Дополнительные сведения см. в разделе *Как создать загрузочный носитель*.

Тестирование загрузочного носителя:

Примечание

Если для хранения резервных копий используются внешние диски, необходимо подсоединить их перед загрузкой с загрузочного компакт-диска. В противном случае программа их может не обнаружить.

1. Настройте компьютер так, чтобы разрешить загрузку с загрузочного носителя. Затем сделайте устройство с загрузочным носителем (дисковод CD-ROM/DVD-ROM или USB-накопитель) первым загрузочным устройством. Дополнительные сведения см. в разделе *Настройка порядка загрузки в BIOS*.
2. Если имеется загрузочный компакт-диск, нажмите любую клавишу, чтобы запустить загрузку с компакт-диска, как только появится сообщение «Press any key to boot from CD» (Нажмите любую клавишу для загрузки с компакт-диска). Если не нажать клавишу в течение пяти секунд, необходимо будет перезагрузить компьютер.
3. После появления меню загрузки выберите Кибер Бэкап Старт.

Примечание

- Если не работает беспроводная мышь, попробуйте заменить ее проводной. Та же рекомендация касается и клавиатуры.
- Если запасной мыши или клавиатуры нет, обратитесь в службу поддержки Киберпротект. Они сформируют специальный загрузочный компакт-диск, на котором будут содержаться драйверы ваших моделей мыши и клавиатуры. Помните, что поиск нужных драйверов и создание специального загрузочного компакт-диска могут занять некоторое время. Более того, для некоторых моделей это будет вообще невозможно.

4. После запуска программы рекомендуется попробовать восстановить некоторые файлы из резервной копии. Пробное восстановление позволит убедиться, что загрузочный компакт-диск можно использовать для восстановления. Кроме того, так можно проверить, обнаруживает ли программа все жесткие диски в системе.

Примечание

Если у вас имеется запасной жесткий диск, настоятельно рекомендуется опробовать испытательное восстановление вашего системного раздела на этот жесткий диск.

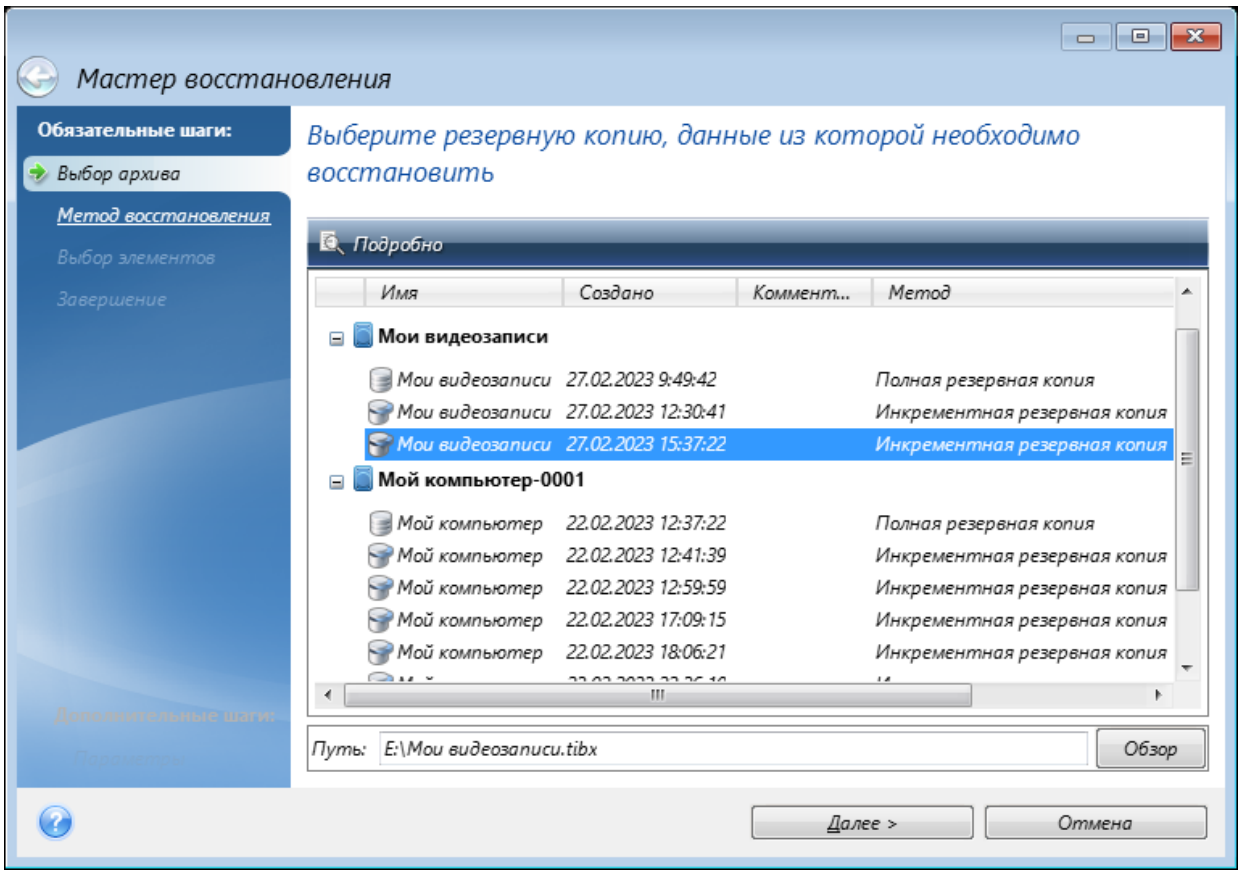
Как выполнить пробное восстановление, а также проверить диски и сетевой адаптер:

1. При наличии резервных копий файлов запустите мастер восстановления, щелкнув **Восстановление** → **Восстановление файлов** на панели инструментов.

Примечание

При наличии резервной копии только дисков и разделов мастер восстановления также запустится, и процедура восстановления будет аналогичной. В этом случае необходимо выбрать пункт **Восстановить выбранные файлы и папки** на шаге **Метод восстановления**.

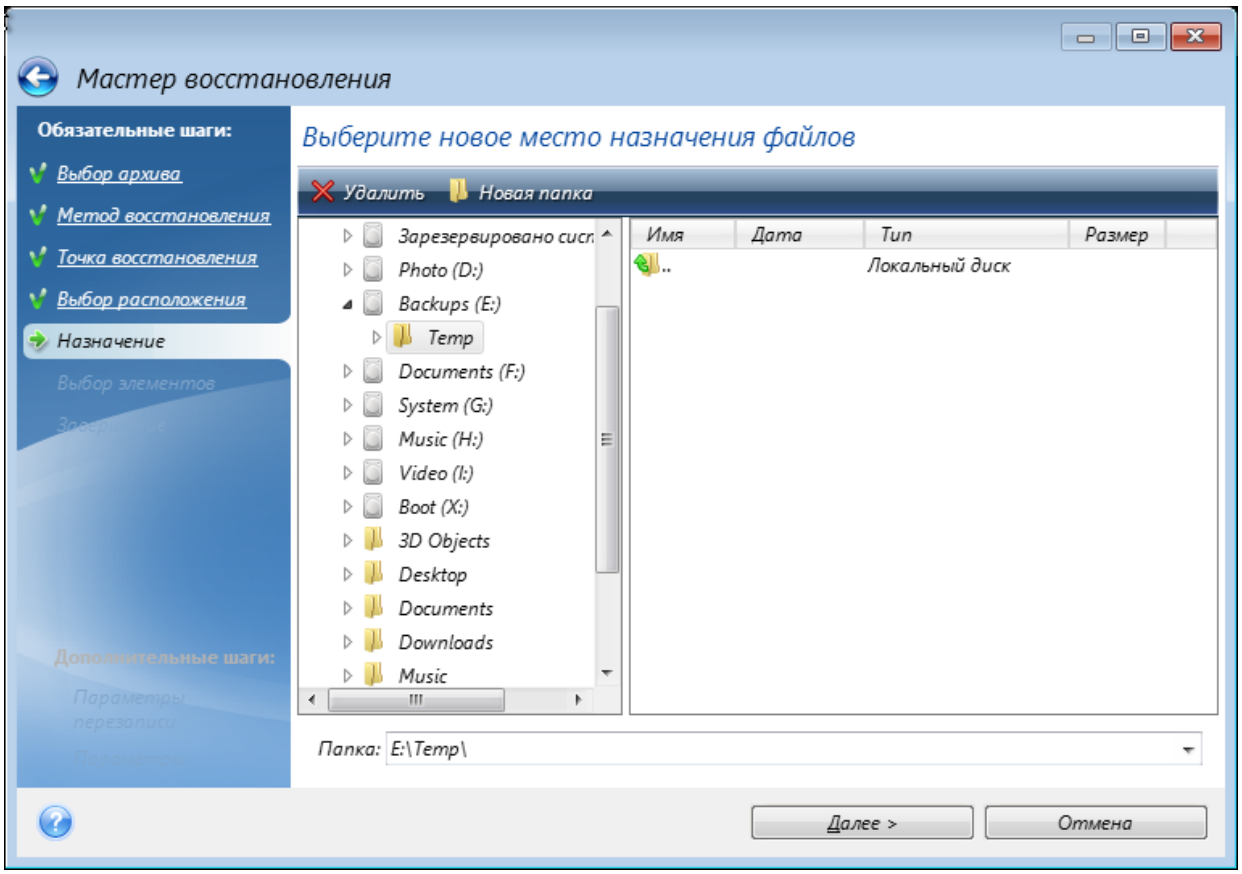
2. Выберите резервную копию на шаге **Выбор архива**, а затем нажмите кнопку **Далее**.



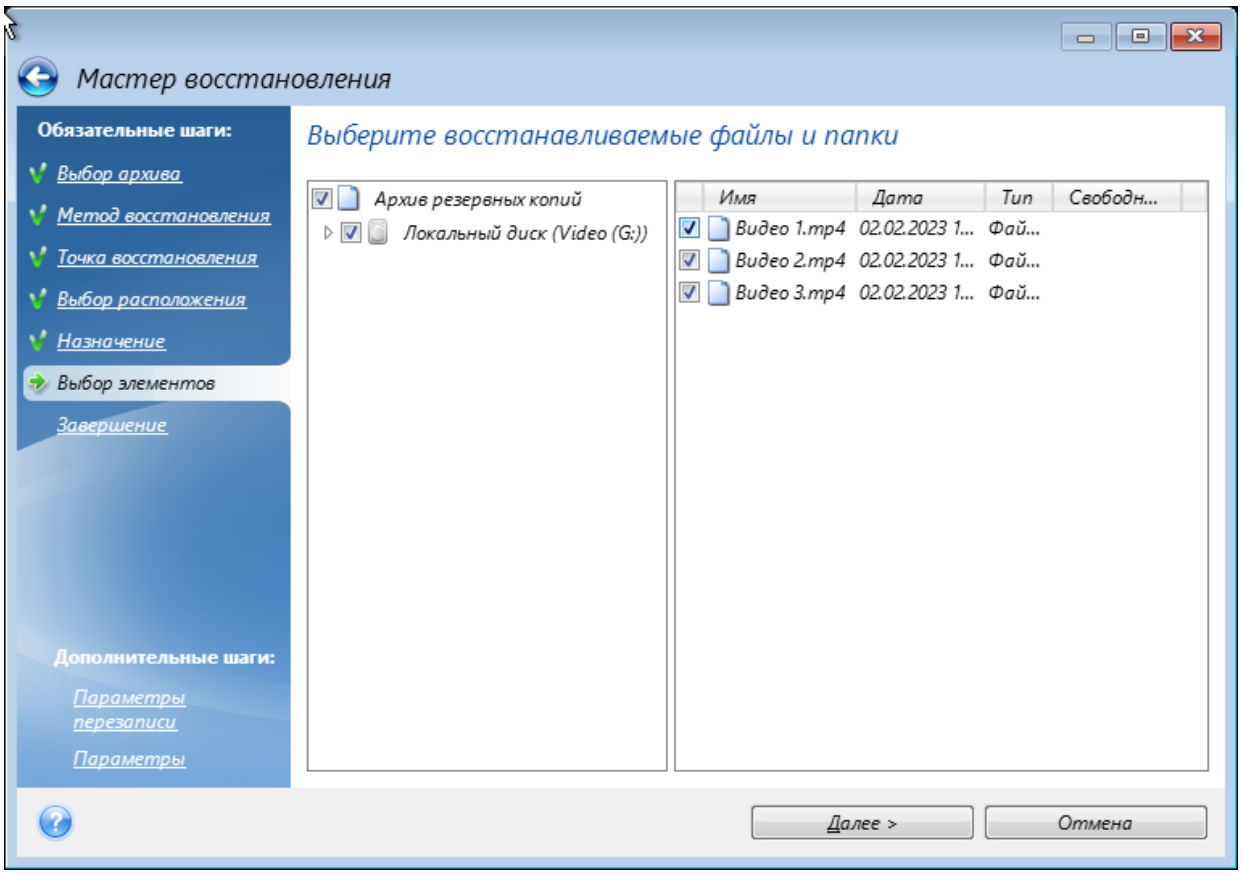
3. На шаге **Точка восстановления** выберите дату и время, на которые следует восстановить файлы и папки из резервной копии.
4. При восстановлении файлов с помощью загрузочного компакт-диска можно выбрать только новое хранилище для восстанавливаемых файлов. Поэтому просто нажмите кнопку **Далее** на шаге **Выбор расположения**.
5. На шаге **Назначение** убедитесь, что все имеющиеся накопители отображаются в папке **Этот компьютер**.

Примечание

- Если резервные копии хранятся в сети, проверьте наличие доступа к этой сети.
- Если в сети не обнаружен ни один компьютер, но значок **Соседние компьютеры** отображается в папке **Этот компьютер**, укажите параметры сети вручную. Для этого откройте окно через меню **Параметры сети** → **Сетевые адаптеры**.
- Если значок **Соседние компьютеры** недоступен в разделе **Этот компьютер**, проблема может быть в сетевой карте или драйвере карты, находящемся на загрузочном носителе Кибер Бэкап Старт.



6. Выберите место сохранения файлов, а затем нажмите кнопку **Далее**.
7. На шаге **Выбор элементов** выберите несколько файлов для восстановления, установив напротив них флажки, и нажмите кнопку **Далее**.



8. На шаге **Завершение** нажмите кнопку **Приступить**, чтобы начать восстановление.
9. После завершения восстановления выйдите из автономной версии Кибер Бэкап Старт.

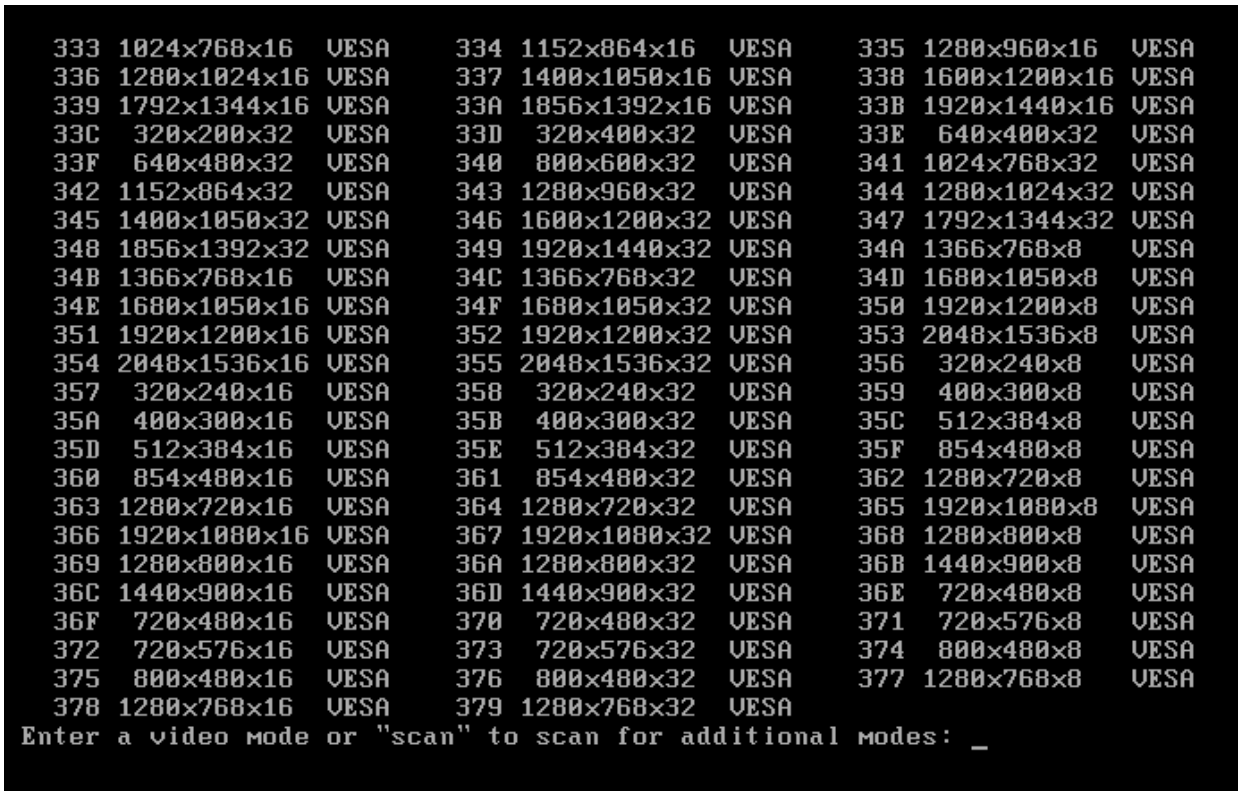
Теперь можно с определенной степенью уверенности сказать, что в случае необходимости загрузочный компакт-диск вам поможет.

Выбор видеорежима при загрузке с загрузочного носителя

При загрузке с загрузочного носителя оптимальный видеорежим выбирается автоматически, в зависимости от спецификаций видеокарты и монитора. Однако иногда программа может выбрать неверный видеорежим, который не подойдет имеющемуся оборудованию. В этом случае можно выбрать подходящий видеорежим следующим образом.

1. Запустите загрузку с загрузочного носителя. После появления меню загрузки наведите курсор мыши на Кибер Бэкап Старт и нажмите клавишу `F11`.
2. При появлении командной строки введите `vga=ask` и нажмите кнопку **ОК**.
3. Выберите в меню загрузки Кибер Бэкап Старт, чтобы продолжить загрузку с загрузочного носителя. Чтобы увидеть доступные видеорежимы, нажмите клавишу Enter при появлении соответствующего сообщения.

4. Выберите наиболее подходящий видеорежим для монитора и введите его номер в командную строку. Например, ввод номера 338 позволит выбрать видеорежим 1600x1200x16 (см. рис. ниже).



5. Подождите, пока Кибер Бэкап Старт не запустится, и убедитесь, что вам подходит изображение экрана приветствия на мониторе.

Для проверки другого видеорежима закройте Кибер Бэкап Старт и повторите вышеуказанную процедуру.

После того как найден оптимальный видеорежим для имеющегося оборудования, можно создать новый загрузочный носитель, который будет выбирать видеорежим автоматически.

Для этого запустите Мастер создания загрузочных носителей, выберите необходимые компоненты носителя и введите в командную строку номер режима с префиксом 0x (0x338 в нашем примере) на шаге параметров запуска загрузочного носителя, а затем создайте носитель обычным способом.

Восстановление при загрузке

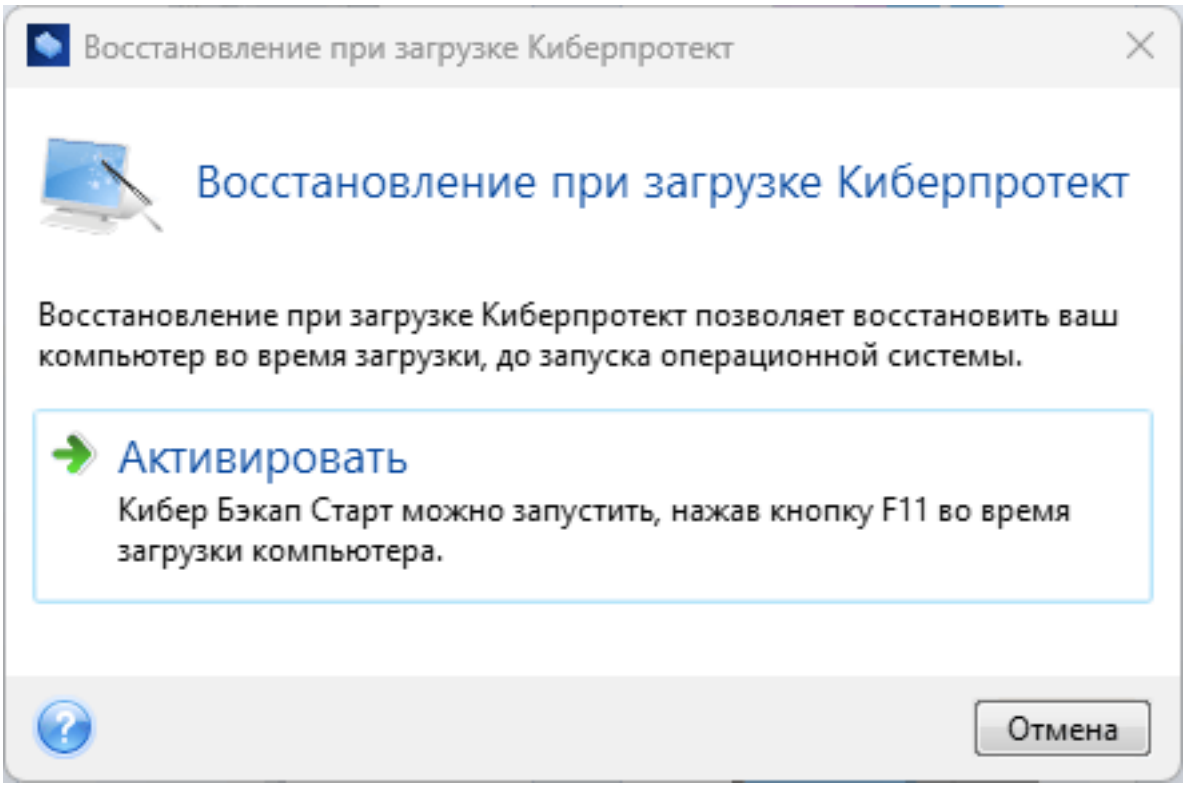
Восстановление при загрузке позволяет запустить Кибер Бэкап Старт без загрузки операционной системы. Благодаря этой функции, Кибер Бэкап Старт можно использовать для восстановления поврежденных разделов даже в том случае, если операционная система не загружается. В отличие от загрузки со съемного носителя Киберпротект для запуска Кибер Бэкап Старт не требуется отдельный носитель или подключение к сети.

Примечание

Восстановление при загрузке нельзя использовать на планшетах под управлением Windows.

Как активировать восстановление при загрузке:

1. Запустите Кибер Бэкап Старт.
2. В разделе **Инструменты** щелкните **Восстановление при загрузке**.
3. В открывшемся окне щелкните **Активировать**.



В случае сбоя включите компьютер и при появлении сообщения «Press F11 for Cyberprotect Startup Recovery Manager» нажмите клавишу F11. Запустится автономная версия Кибер Бэкап Старт, незначительно отличающаяся от полной версии программы.

Как деактивировать восстановление при загрузке:

1. Запустите Кибер Бэкап Старт.
2. В разделе **Инструменты** щелкните **Восстановление при загрузке**.
3. В открывшемся окне щелкните **Деактивировать**.

Дополнительная информация

Буквы дисков в автономной версии Кибер Бэкап Старт иногда могут отличаться от идентификации дисков в Windows. Например, диск D: в автономной версии Кибер Бэкап Старт может соответствовать диску E: в Windows. Метки дисков и информация о размерах разделов, файловых системах, емкости дисков, производителях и номерах моделей поможет правильно идентифицировать диски и разделы.

Влияет ли восстановление при загрузке на другие загрузчики?

При активации функция восстановления при загрузке перезаписывает основную загрузочную запись (MBR), внося в нее собственный загрузочный код. Если на компьютере установлены диспетчеры загрузки сторонних производителей, после активации восстановления при загрузке необходимо будет заново их активировать. Для загрузчиков Linux (например, LiLo и GRUB) можно выбрать их установку в корневой (или загрузочный) раздел Linux вместо MBR перед активацией восстановления при загрузке.

Механизм загрузки UEFI отличается от BIOS. Любой загрузчик ОС или другая загрузочная программа имеет собственную переменную загрузки, которая определяет путь к соответствующему загрузчику. Все загрузчики хранятся в специальном системном разделе EFI. Когда восстановление при загрузке активируется в системе, загружаемой с помощью UEFI, функция изменяет последовательность загрузки, прописывая собственную переменную. Эта переменная добавляется в список, не изменяя существующие переменные. Поскольку все загрузчики независимы и не влияют друг на друга, нет необходимости что-либо изменять до или после активации восстановления при загрузке.

Экспериментальный режим

При включении Экспериментального режима компьютер переходит в режим, в котором можно выполнять любые потенциально опасные операции, не беспокоясь о том, что они могут привести к повреждению операционной системы, программ или данных. При выключении Экспериментального режима вы решаете, применить ли сделанные изменения или же их отменить.

Когда полезен Экспериментальный режим

Рекомендуется включить Экспериментальный режим перед следующими действиями:

- Изменение любых системных настроек, когда вы не уверены в том, как это может повлиять на работу компьютера.
- Установка обновлений системы, драйверов и т. д.
- Установка незнакомых приложений.
- Открытие почтовых вложений от неизвестных отправителей.
- Посещение веб-сайтов, которые могут содержать потенциально опасный контент.

Примечание

Помните, что если вы в Экспериментальном режиме загружали сообщения электронной почты с POP-сервера, создавали новые файлы или редактировали существующие документы, а затем выбрали отмену изменений, то эти файлы, изменения в документах и сообщения электронной почты перестанут существовать. В таких случаях сохраняйте новые файлы и измененные документы, например, на флэш-накопитель USB, а перед отменой изменений извлеките его.

Как Экспериментальный режим работает после перезагрузки компьютера

Экспериментальный режим может работать неограниченное время, так как не выключается в случае перезагрузки компьютера.

Если во время работы в данном режиме произошла перезагрузка компьютера, при последующей загрузке ОС появится диалоговое окно с двумя вариантами для выбора: остановить работу в этом режиме и отменить изменения или продолжить работу в этом режиме. Это позволит отменить изменения, вызвавшие сбой в работе системы. С другой стороны, если перезагрузить компьютер, например, после установки какого-либо приложения, работа может быть продолжена в Экспериментальном режиме после запуска ОС Windows.

При каждой «теплой» перезагрузке компьютера в этом режиме к служебным данным Экспериментального режима в хранилище, выбранном для сохранения виртуальных изменений, добавляется до 500 МБ.

Ограничения использования Экспериментального режима

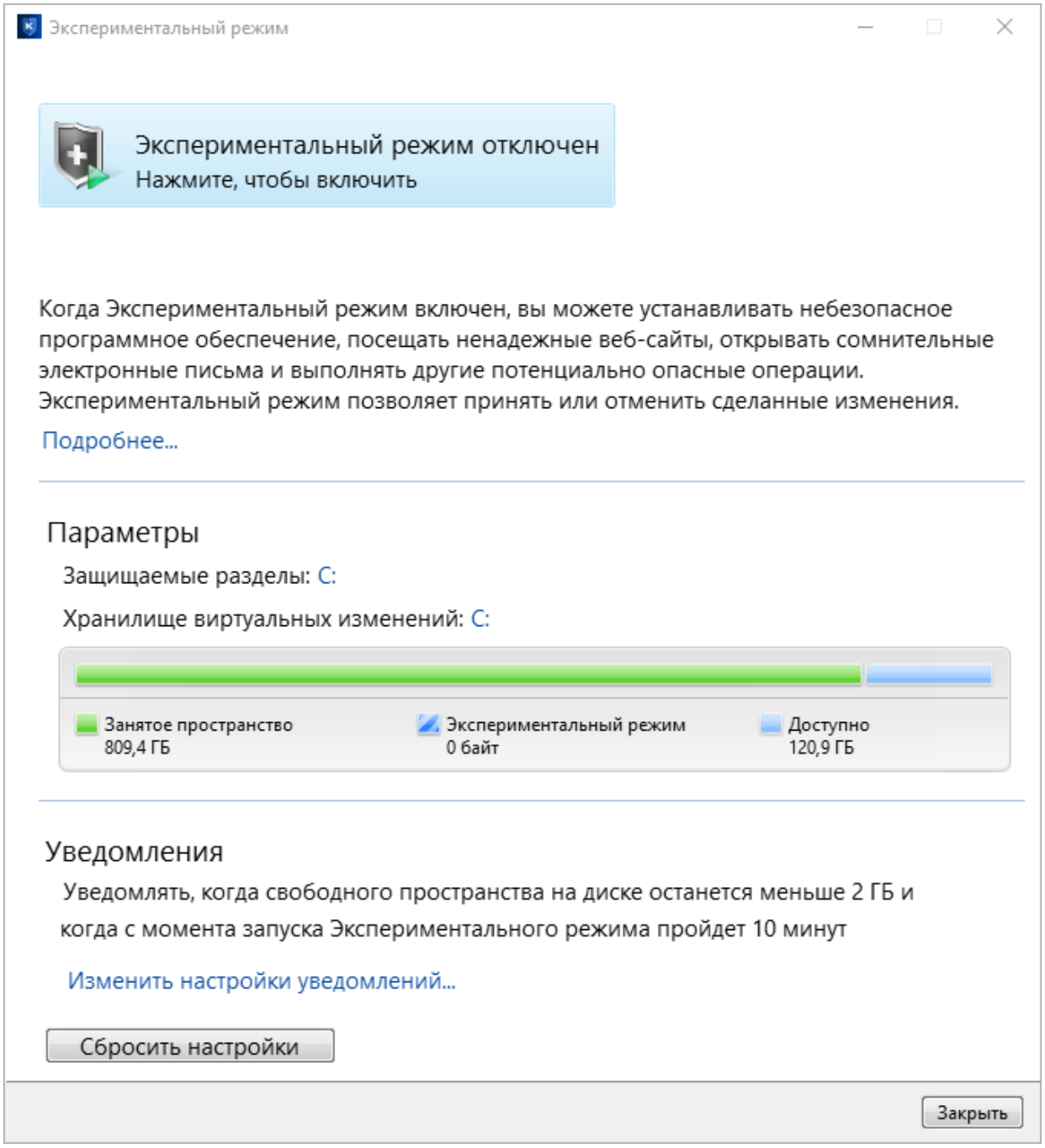
- Экспериментальный режим не может использоваться с включенной изоляцией ядра Windows.
- Необходимо помнить о том, что в Экспериментальном режиме программа может интенсивно использовать свободное дисковое пространство даже во время простоя компьютера. Причиной этого являются действия, выполняемые в фоновом режиме, такие как индексирование и дефрагментация файлов.
- При работе в Экспериментальном режиме наблюдается некоторое снижение быстродействия системы. Кроме того, процесс применения изменений может занять много времени, особенно если данный режим был включен несколько дней подряд.
- В Экспериментальном режиме не отслеживаются изменения в разделах диска, поэтому нельзя использовать этот режим для виртуальных операций с разделами, таких как изменение их схемы или размера. Кроме того, нельзя одновременно использовать Экспериментальный режим и системные утилиты дефрагментации диска или проверки диска из-за риска повредить файловую систему без возможности восстановления, а также помешать операционной системе загружаться с

этого диска.

- При работе в Экспериментальном режиме невозможно использовать ранее активированную функцию восстановления при загрузке. Перезагрузка компьютера в этом режиме позволит снова использовать восстановление при загрузке.
- Экспериментальный режим и непрерывное резервное копирование не могут работать одновременно. Запуск Экспериментального режима приостанавливает непрерывное резервное копирование. Непрерывное резервное копирование будет возобновлено после остановки данного режима.
- После запуска Экспериментального режима невозможно использовать ранее активированную функцию гибернации для экономии электроэнергии.
- Экспериментальный режим не может использоваться для защиты динамических дисков.
- Экспериментальный режим не работает, если какой-либо раздел в системе зашифрован с помощью BitLocker.
- Экспериментальный режим не может защитить зону безопасности Киберпротект или использовать ее в качестве хранилища для виртуальных изменений.

Использование Экспериментального режима

1. Запустите Кибер Бэкап Старт.
2. В разделе **Инструменты** щелкните **Экспериментальный режим**.
3. При необходимости настройте параметры Экспериментального режима. Дополнительные сведения см. в разделе *Параметры и уведомления Экспериментального режима*.
4. Чтобы включить Экспериментальный режим, щелкните значок **Экспериментальный режим**. Программа будет отслеживать все изменения, сделанные в ОС, и временно запоминать все изменения на выбранном диске.

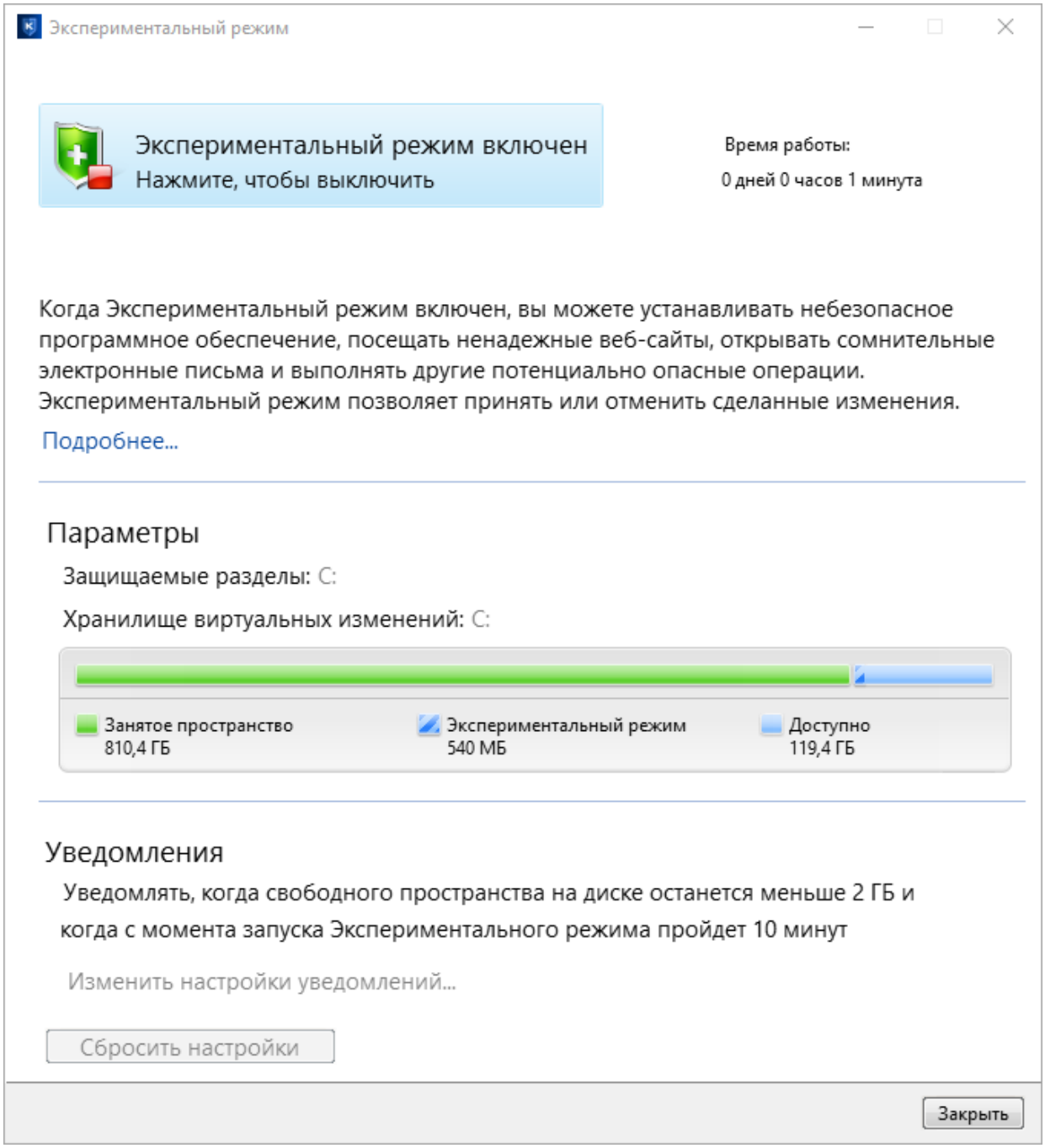


5. Сделайте все изменения, которые вы хотели проверить.

Примечание

Когда в хранилище, выбранном для сохранения виртуальных изменений, остается минимум пространства для того, чтобы применить изменения, программа выдает запрос на применение или отмену изменений. Если оповещение будет проигнорировано, программа автоматически перезапустит систему при заполнении диска, отменив изменения.

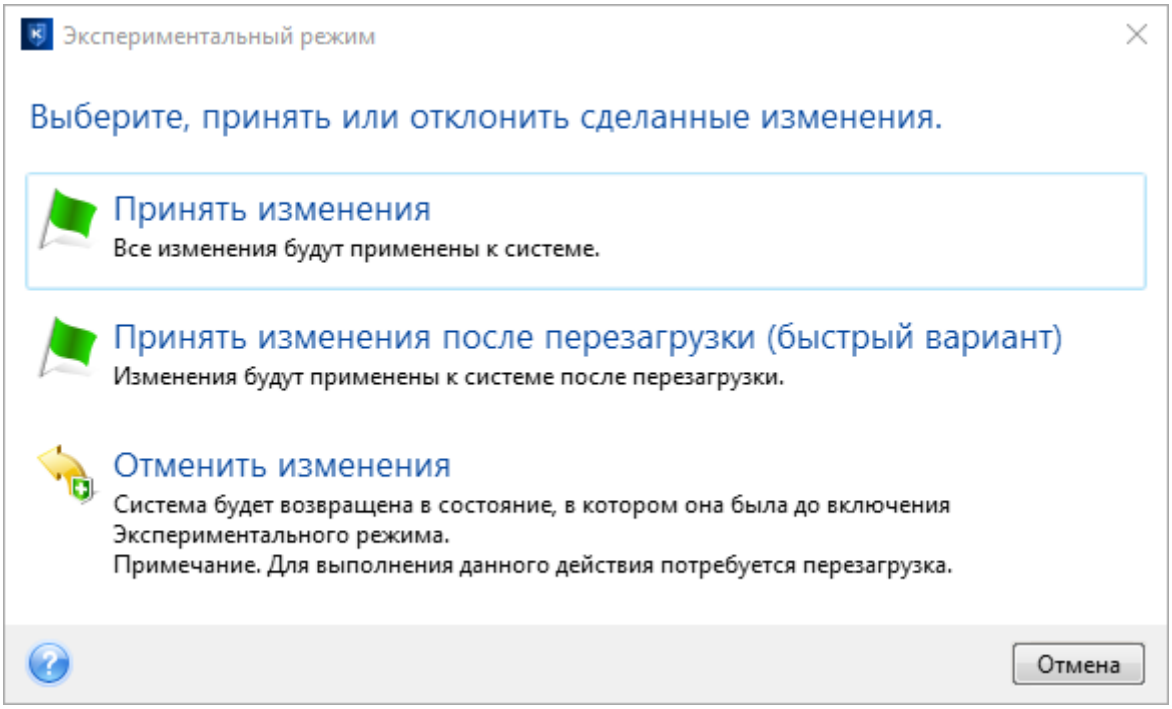
6. Чтобы выключить Экспериментальный режим, щелкните значок **Экспериментальный режим** в окне **Экспериментальный режим**.



7. Выберите один из вариантов:

   - Выберите **Принять изменения**, если необходимо сохранить изменения, сделанные в системе.
   - Выберите **Принять изменения после перезагрузки**, чтобы ускорить процесс сохранения изменений в системе. При выборе данного параметра Экспериментальный режим перезагрузит компьютер и применит изменения после перезагрузки.
   - Выберите **Отменить изменения**, если нужно вернуть систему в состояние, предшествующее

запуску Экспериментального режима. При выборе этого параметра отображается всплывающее окно со следующими вариантами: **Перезагрузить компьютер и отменить изменения** и **Не выполнять перезагрузку**. Если выбрать вариант **Не выполнять перезагрузку**, функция Экспериментальный режим останется включенной, а изменения не будут отменены.



Примечание

Если выбрать вариант **Отменить изменения** и перезагрузить компьютер, на котором установлено несколько операционных систем, будет невозможно запустить другие операционные системы, кроме той, в которой работает Экспериментальный режим. Вторая перезагрузка восстановит исходную запись MBR и позволит загружать остальные операционные системы.

Параметры и уведомления Экспериментального режима

Параметры Экспериментального режима можно изменить в окне **Экспериментальный режим**. Чтобы восстановить значения параметров по умолчанию, нажмите кнопку **Сбросить настройки**.

Защищаемые разделы

По умолчанию в Экспериментальном режиме защищен системный раздел (диск C), но можно выбрать для защиты любые другие разделы в системе.

Чтобы изменить этот параметр:

1. Щелкните букву раздела рядом с именем параметра. Откроется окно **Выбор раздела**.

2. Выберите разделы, которые необходимо защитить, и нажмите кнопку **ОК**.

Хранилище виртуальных изменений

По умолчанию Экспериментальный режим сохраняет информацию на свободное пространство диска C.

Чтобы изменить этот параметр:

1. Щелкните букву раздела рядом с именем параметра. Откроется окно **Хранилище виртуальных изменений**.
2. Выберите раздел, который необходимо использовать в качестве хранилища виртуальных изменений, и нажмите кнопку **ОК**.

> **Примечание**
>
> Невозможно выбрать раздел, защищаемый Экспериментальным режимом, в качестве хранилища виртуальных изменений. Также невозможно сохранять виртуальные изменения на внешнем жестком диске.

Уведомления

Чтобы изменить параметры уведомлений по умолчанию, щелкните **Изменить настройки уведомлений**. Откроется окно **Настройки**.

- **Остаток свободного дискового пространства** — если свободного пространства в хранилище виртуальных изменений остается меньше указанного значения, программа уведомляет об этом.
- **Время работы Экспериментального режима** — программа выдаст уведомление, если Экспериментальный режим работает дольше указанного вами периода.

Примеры использования Экспериментального режима

Функция Экспериментальный режим может оказаться полезной при различных обстоятельствах, например в следующих случаях.

Пробное использование программ

Иногда может быть полезно включить Экспериментальный режим перед установкой новой программы. Например, его рекомендуется включить, когда вы хотите выполнить следующие действия:

- Выбрать антивирусное ПО.

  Иногда установка антивирусного ПО нарушает работоспособность некоторых программ, они даже могут перестать запускаться. Вы можете протестировать пробную версию антивирусной

программы. Если возникли какие-либо проблемы, отмените изменения в системе и попробуйте использовать антивирусную программу другого разработчика.

- Установить пробную версию программы.

  Известно, что компонент «Установка и удаление программ» панели управления Windows не дает гарантии полного удаления приложений. Если вам не понравилась установленная программа, отмените изменения в системе. В этом случае вы можете быть уверены, что функция Экспериментальный режим удалит все следы программы.

- Установить подозрительное ПО.

  Если вы не доверяете разработчику программы, которую собираетесь установить, или если источник программы неизвестен, включите Экспериментальный режим перед установкой. Если возникнут какие-либо проблемы, отмените изменения, произведенные в Экспериментальном режиме.

Восстановление файлов

Пользователь удалил несколько файлов и затем очистил корзину. Потом вспомнил, что удаленные файлы содержали важную информацию, и теперь собирается восстановить удаленные файлы с использованием соответствующего программного обеспечения. Однако иногда, пытаясь восстановить удаленные файлы, можно совершить ошибку, которая еще более уменьшит шансы восстановления удаленных файлов.

Выполните следующие действия:

- Включите Экспериментальный режим.
- Запустите утилиту восстановления удаленных файлов.

После того как утилита закончит сканирование диска и найдет удаленные файлы или папки, она покажет обнаруженные удаленные файлы и предложит их восстановить. Всегда имеется вероятность того, что будет выбран неверный файл и во время его восстановления утилита «затрет» именно тот файл, который необходимо восстановить. Если бы не Экспериментальный режим, эту ошибку было бы невозможно исправить и файл был бы потерян безвозвратно.

Но теперь можно просто отменить изменения, произведенные в Экспериментальном режиме, и сделать еще одну попытку восстановить файлы после того, как данный режим снова будет включен. Такие попытки можно повторять до тех пор, пока файлы не будут восстановлены или пока не будет ясно, что сделано все возможное для их восстановления.

Защита личных сведений в сети

Предположим, необходимо скрыть историю посещения веб-страниц. Для облегчения навигации по веб-страницам операционная система сохраняет следующую конфиденциальную информацию: файлы cookie, история поиска, история посещения веб-страниц и т. д. Данная информация не удаляется полностью при удалении временных файлов Интернета и файлов cookie при помощи инструментов браузера. Специальные программы-шпионы могут иметь доступ к этой информации.

Включите Экспериментальный режим и спокойно просматривайте любые веб-страницы. После этого отмените изменения, произведенные в Экспериментальном режиме, чтобы удалить все следы ваших действий.

Зона безопасности Киберпротект

Зона безопасности Киберпротект — это специальный защищенный раздел, который можно создать на компьютере для хранения резервных копий. Зона безопасности Киберпротект имеет файловую систему FAT32.

После создания Зона безопасности Киберпротект отображается в разделе **Устройства и диски** в проводнике. По зоне безопасности Киберпротект можно перемещаться как по обычному разделу.

Если Зона безопасности Киберпротект защищена паролем, то для выполнения любых операций, кроме просмотра сведений о версии, требуется ввести пароль.

Очистка зоны безопасности Киберпротект

Если в зоне безопасности Киберпротект недостаточно места для новой резервной копии:

- Отмените операцию резервного копирования, увеличьте размер зоны безопасности Киберпротект и снова запустите резервное копирование.
- Отмените операцию резервного копирования, вручную удалите некоторые резервные копии из зоны безопасности Киберпротект и снова запустите резервное копирование.
- Подтвердите, что следует автоматически удалять самую старую резервную копию того же типа (на уровне файлов или дисков) со всеми последующими инкрементными и дифференциальными версиями. Если после этого места все еще недостаточно, Кибер Бэкап Старт запрашивает подтверждение и удаляет следующую полную резервную копию. Процедура повторяется, пока в зоне безопасности не будет достаточно свободного места для новой резервной копии. Если после удаления всех предыдущих резервных копий места по-прежнему не хватает, резервное копирование отменяется.

Чтобы предотвратить переполнение зоны:

1. Выберите запланированную резервную копию.
2. Нажмите **Параметры**.
3. На вкладке **Дополнительно** разверните раздел **Обработка ошибок**.
4. Установите флажок **При недостатке места в Зоне безопасности удалять самую старую резервную копию**.
5. Нажмите кнопку **ОК**.

Дополнительные сведения см. в разделе *Обработка ошибок*.

Создание и изменение зоны безопасности Киберпротект

1. В разделе **Инструменты** щелкните **Зона безопасности**.

   Откроется мастер управления зоной безопасности Киберпротект.

2. Выполните одно из следующих действий.

   - Чтобы создать зону безопасности Киберпротект, укажите ее *расположение* и *размер*.
   - Для изменения зоны безопасности Киберпротект выберите одно из следующих действий.
     - *Увеличить или уменьшить размер*
     - *Удалить*
     - *Изменить пароль*

   После этого следуйте инструкциям мастера.

3. На шаге **Завершение** нажмите кнопку **Приступить**.

Примечание

Эта операция может потребовать перезапуска компьютера.

Расположение зоны безопасности Киберпротект

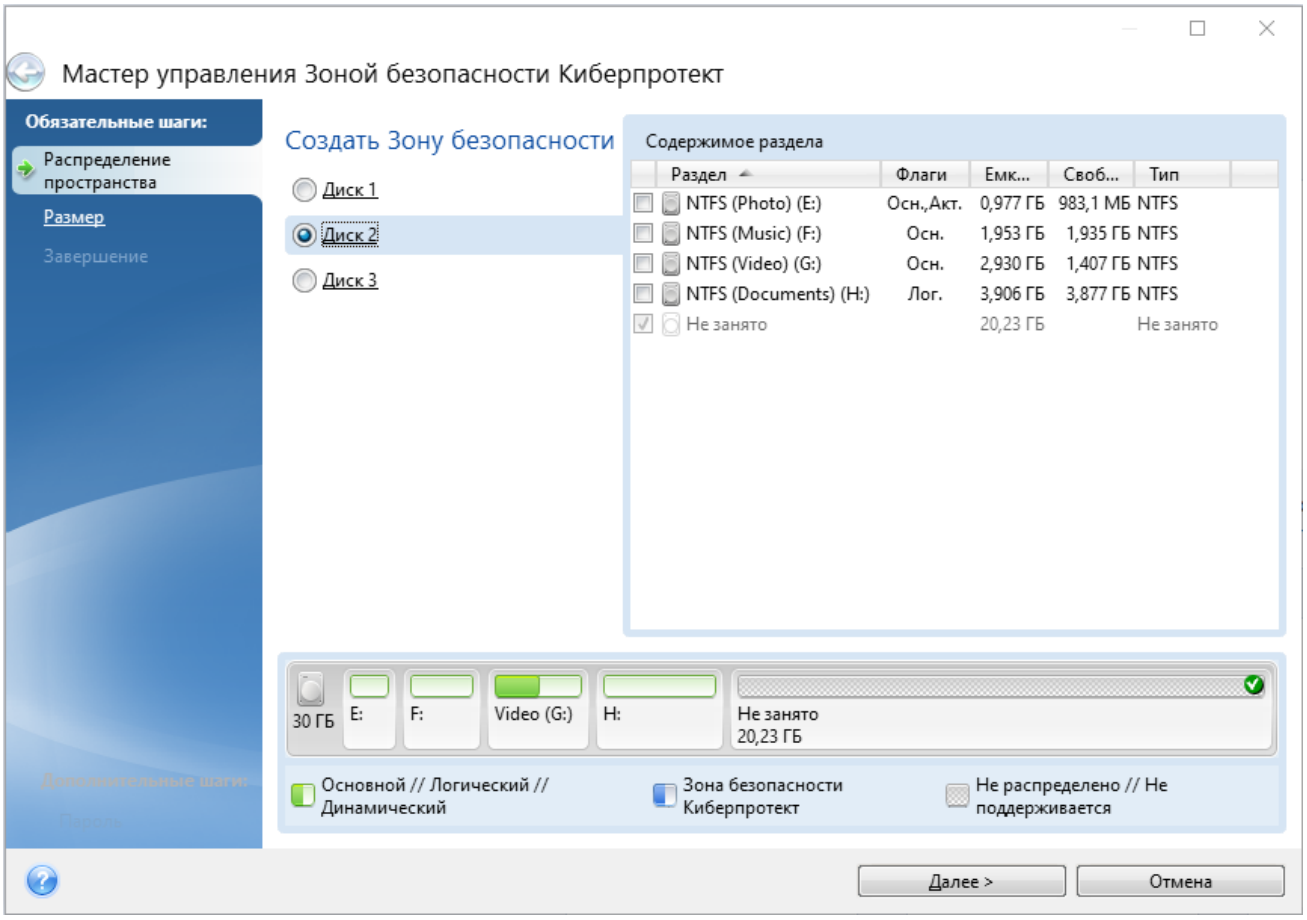
Как задать расположение зоны безопасности Киберпротект:

1. Выберите жесткий диск, на котором будет создана Зона безопасности Киберпротект.
2. Выберите один или несколько разделов, нераспределенное или свободное пространство которых будет использоваться. При необходимости размеры этих разделов будут уменьшены, чтобы освободить место для зоны безопасности Киберпротект.

Примечание

Зону безопасности Киберпротект нельзя создать на динамических дисках или томах.

3. Нажмите кнопку **Далее**.

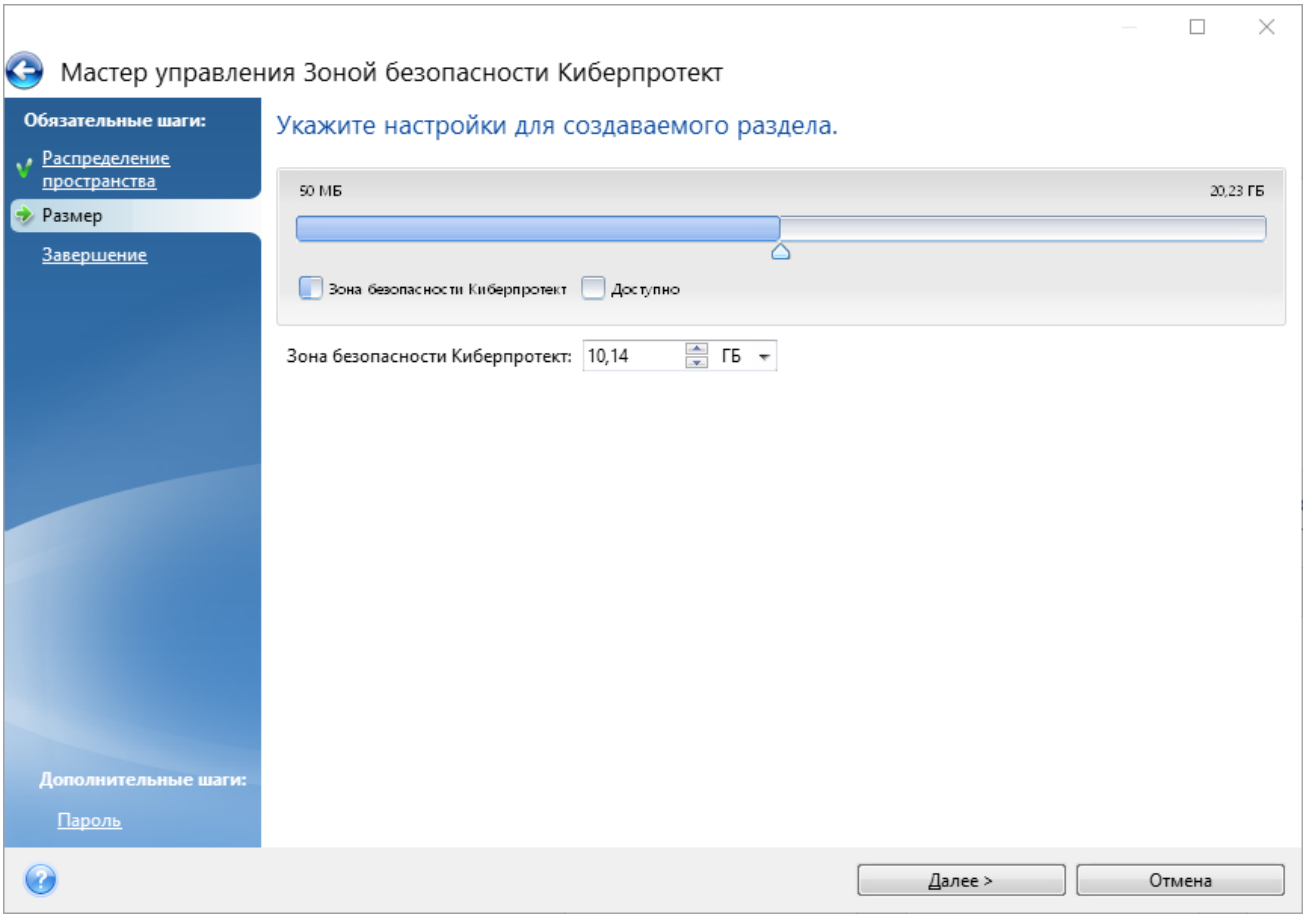


Как увеличить или уменьшить размер зоны безопасности Киберпротект:

1. Выберите разделы, пространство которых будет использовано для увеличения размера зоны безопасности Киберпротект или к которым будет добавлено свободное пространство после уменьшения размера зоны безопасности Киберпротект. Также можно выбрать и разделы с нераспределенным пространством.
2. Нажмите кнопку **Далее**.

Размер зоны безопасности Киберпротект

Чтобы задать размер зоны безопасности Киберпротект, передвиньте ползунок в нужное положение или введите точное значение.



Минимальный размер зоны составляет около 50 МБ, в зависимости от геометрии жесткого диска. Максимальный размер равен сумме незанятого пространства на диске и свободного пространства во всех разделах, выбранных на предыдущем шаге.

При создании зоны безопасности Киберпротект в первую очередь используется нераспределенное пространство. Если нераспределенного пространства недостаточно для размещения зоны требуемого размера, размер выбранных разделов будет уменьшен. Изменение размера разделов может потребовать перезагрузки компьютера.

Если при уменьшении размера зоны безопасности Киберпротект на жестком диске есть нераспределенное пространство, оно распределяется между выбранными разделами вместе с пространством, которое освободилось в результате уменьшения размера зоны безопасности. Таким образом, на диске не останется нераспределенного пространства.

Предупреждение

При уменьшении системного раздела до минимального размера операционная система может перестать загружаться.

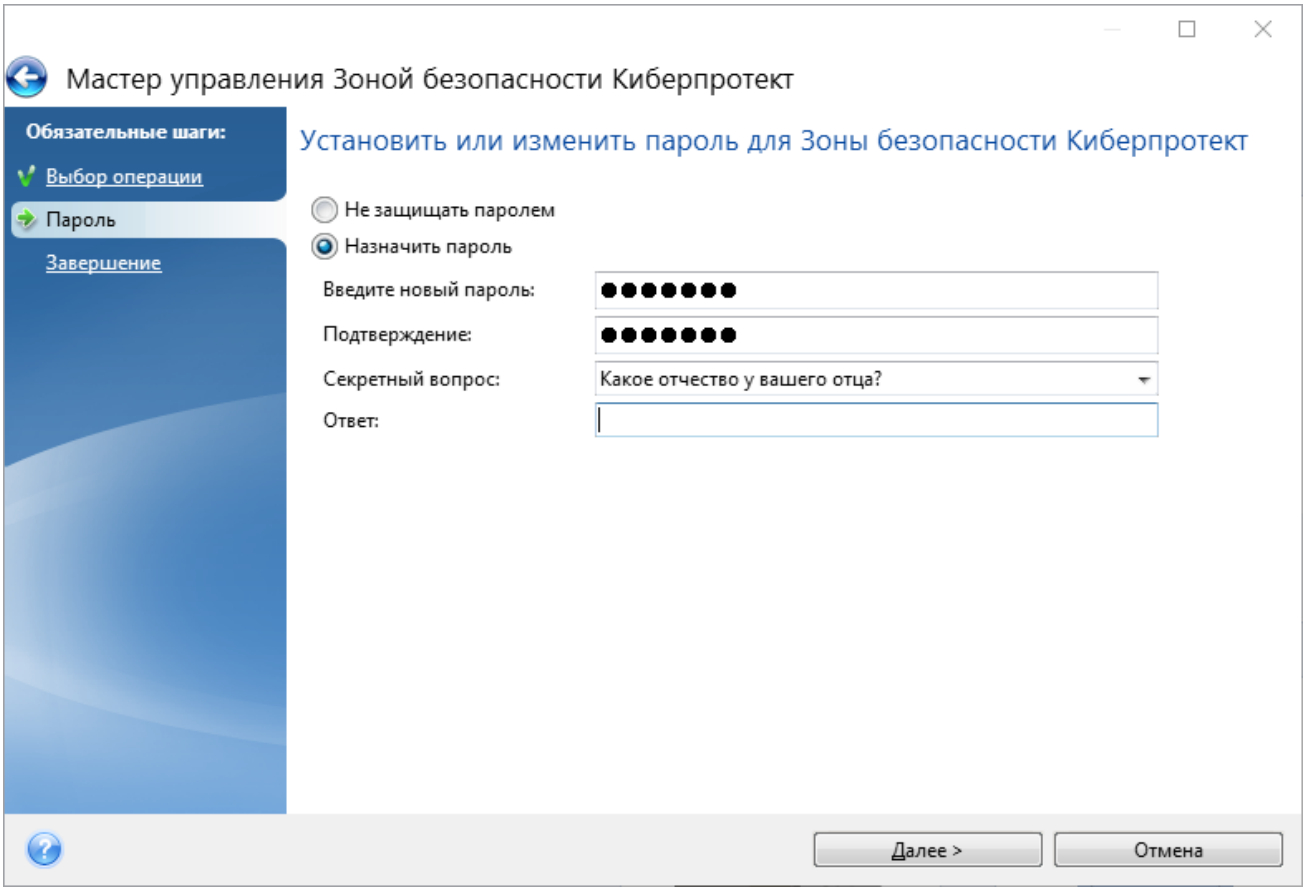
Защита зоны безопасности Киберпротект

Чтобы ограничить доступ к зоне безопасности Киберпротект, можно установить пароль.

Ввод пароля необходим при любых операциях с зоной безопасности Киберпротект, таких как резервное копирование и восстановление данных, подключение резервных копий или проверка архивов, хранящихся в зоне безопасности, изменение размера и удаление зоны безопасности.

Как установить пароль для зоны безопасности Киберпротект:

1. Выберите **Назначить пароль**.
2. Введите пароль в поле **Введите новый пароль**.
3. Повторите ввод пароля в поле **Подтверждение**.
4. [Необязательно] Выберите секретный вопрос, который будет использован для восстановления пароля в случае его утери. Выберите секретный вопрос из списка и введите ответ на него.
5. Для продолжения нажмите кнопку **Далее**.



Примечание

Обновление или восстановление Кибер Бэкап Старт не повлияет на настройки пароля. Однако, если программу удалить, оставив зону безопасности Киберпротект на диске, а потом установить снова, то пароль для зоны безопасности будет сброшен.

Удаление зоны безопасности Киберпротект

Предупреждение

При удалении зоны безопасности Киберпротект будут автоматически удалены все хранящиеся в ней резервные копии.

Укажите разделы, к которым будет добавлено пространство, освободившееся в результате удаления зоны безопасности Киберпротект. Если выбрано несколько разделов, свободное место будет распределено пропорционально размеру разделов.

Также можно выбрать удаление зоны безопасности Киберпротект во время удаления программы.

Добавление нового жесткого диска

При недостатке места для хранения данных можно либо заменить старый жесткий диск новым диском большей емкости, либо добавить новый диск только для хранения данных, оставив систему на старом диске.

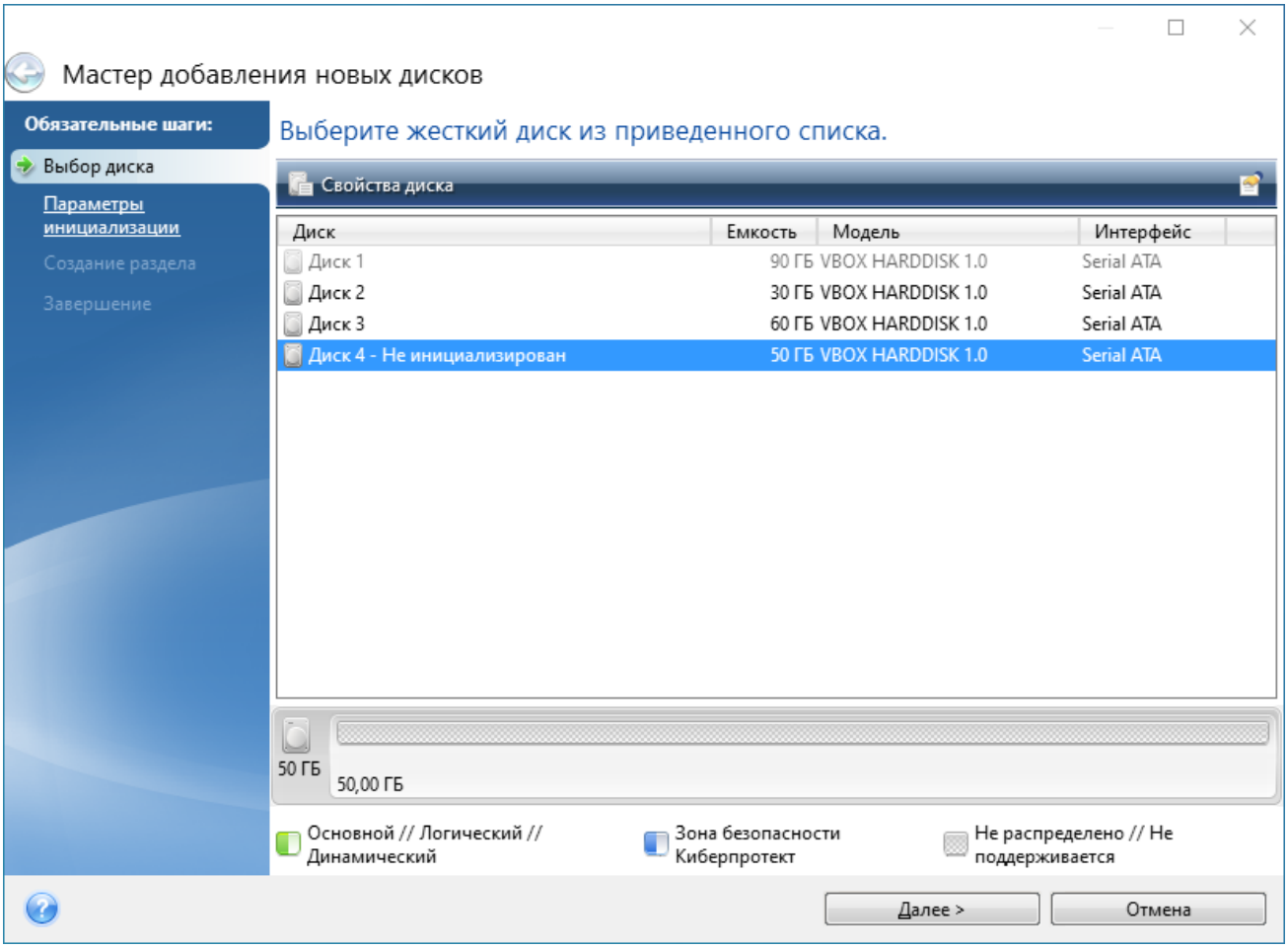
Как добавить новый жесткий диск:

1. Выключите компьютер и установите новый диск.
2. Включите компьютер.
3. Запустите Кибер Бэкап Старт.
4. В разделе **Инструменты** щелкните **Добавить новый диск**.
5. Следуйте инструкциям мастера.
6. На шаге **Завершение** убедитесь, что настроенная структура разделов соответствует вашим целям, и нажмите кнопку **Приступить**.

Выбор жесткого диска

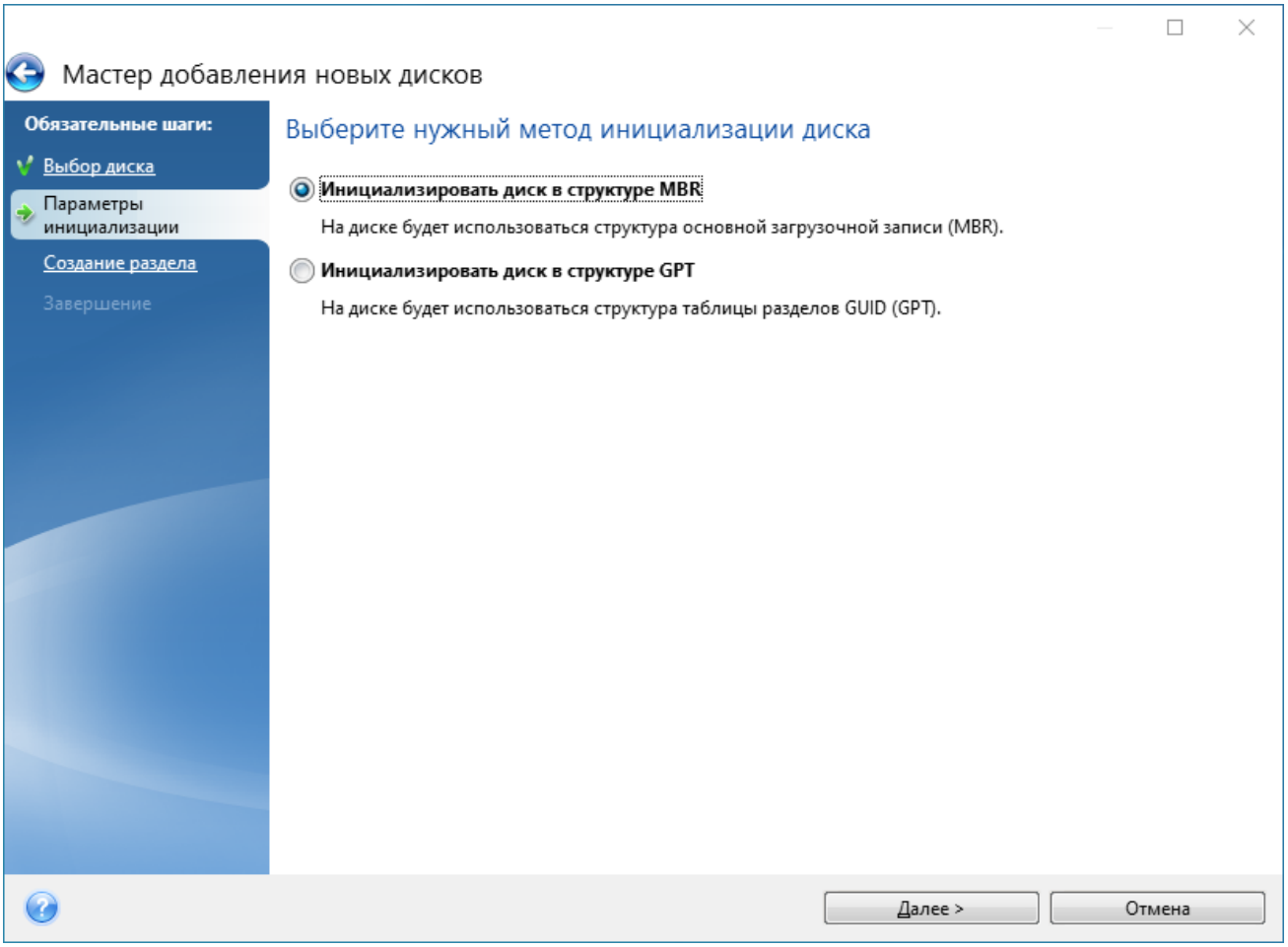
Выберите диск, который был добавлен в компьютер. Если было добавлено несколько дисков, выберите нужный и нажмите **Далее**. Остальные диски можно выбрать позднее, перезапустив мастер добавления новых дисков.

> **Примечание**
>
> Если на новом диске есть разделы, Кибер Бэкап Старт выдаст предупреждение о том, что эти разделы будут удалены.



Выбор метода инициализации

Кибер Бэкап Старт поддерживает стили разделов MBR и GPT. Новая таблица разделов GUID (GPT) имеет ряд преимуществ перед старым методом организации разделов MBR. Если операционная система поддерживает GPT-диски, можно выбрать новый диск для инициализации в качестве GPT-диска.



- Чтобы добавить GPT-диск, нажмите **Инициализировать диск в структуре GPT**.
- Чтобы добавить MBR-диск, нажмите **Инициализировать диск в структуре MBR**.

Выбрав метод инициализации, нажмите кнопку **Далее**.

Создание разделов

Чтобы использовать пространство жесткого диска, необходимо создать на нем разделы. Создание разделов — это разделение пространства жесткого диска на логические части. Каждый раздел может функционировать как отдельный диск с назначенной буквой, собственной файловой системой и т. д.

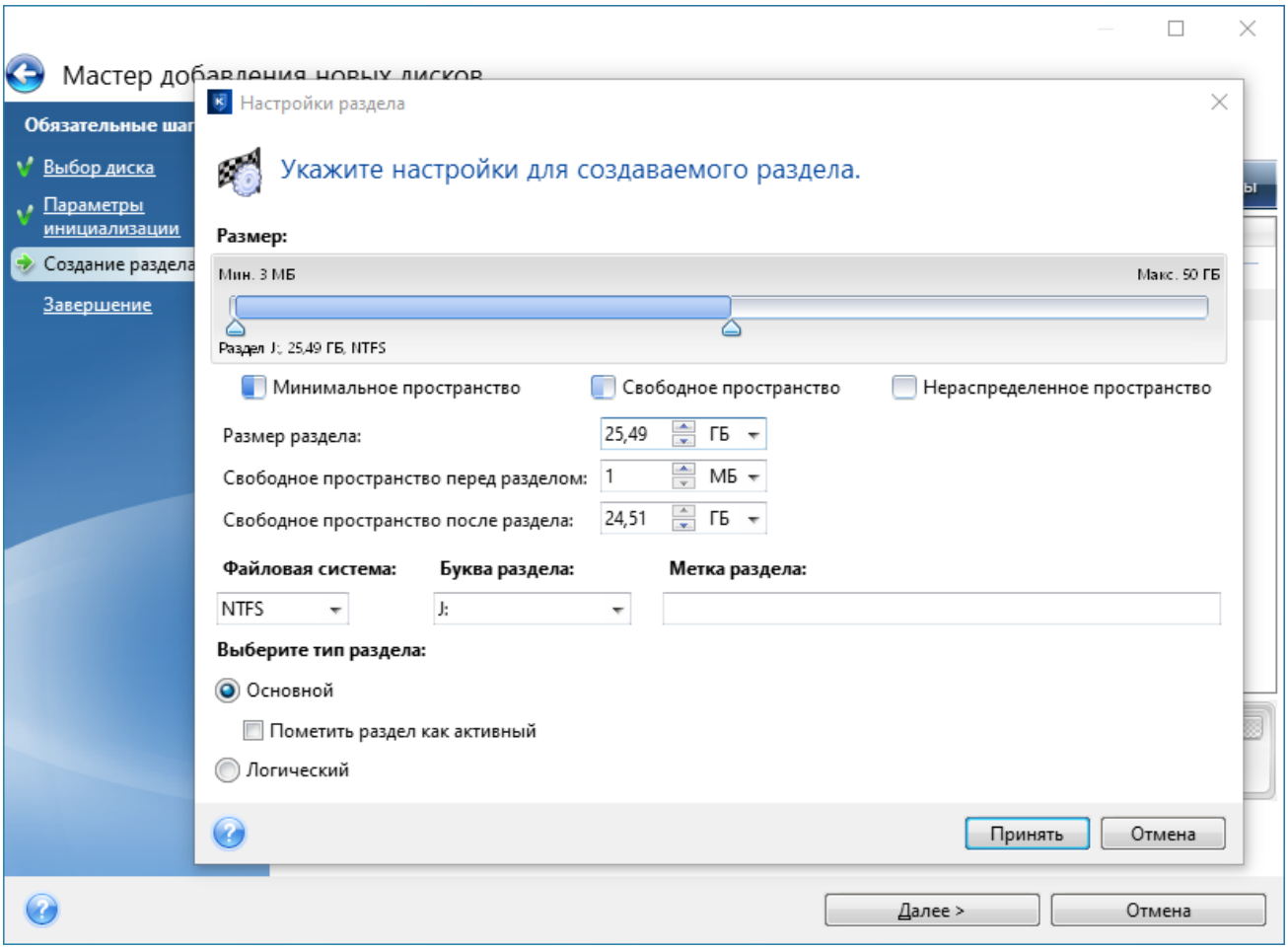
Как создать новый раздел:

1. На шаге мастера **Создание раздела** выберите нераспределенное пространство и щелкните **Создать новый раздел**.
2. Укажите следующие настройки для создаваемого раздела:
    - Размер и положение
    - Файловая система

- Тип раздела (доступно только для MBR-дисков)
- Буква и метка раздела

Дополнительные сведения см. в разделе *Настройки раздела*.

3. Нажмите кнопку **Принять**.



Настройки раздела

Размер

Чтобы изменить размер раздела, выполните одно из следующих действий:

- Наведите указатель мыши на границу раздела. Когда указатель превратится в двунаправленную стрелку, перетащите его, чтобы увеличить или уменьшить размер раздела.
- Введите нужное значение в поле **Размер раздела**.

Чтобы изменить расположение раздела, выполните одно из следующих действий:

- Перетащите раздел в новое положение.
- Введите нужный размер в поле **Свободное пространство перед разделом** или **Свободное**

пространство после раздела.

> **Примечание**
>
> При создании разделов программа может зарезервировать некоторый объем нераспределенного пространства для системных нужд перед создаваемыми разделами.

Файловая система

Оставьте раздел неформатированным или выберите одну из следующих файловых систем:

- NTFS — основная файловая система Windows NT, Windows 2000, Windows XP и более поздних версий операционной системы. Укажите тип используемой операционной системы. Windows 95/98/Me и DOS не имеют доступа к разделам NTFS.
- FAT 32 — улучшенная 32-битная версия файловой системы FAT поддерживает тома размером до 2 ТБ.
- FAT 16 — собственная файловая система DOS. распознается большинством операционных систем. Однако если диск имеет объем более 4 ГБ, его нельзя отформатировать в FAT 16.
- Ext2 — основная файловая система ОС Linux. Достаточно быстрая, но не является журналируемой файловой системой.
- Ext3 — журналируемая файловая система Linux, официально введенная начиная с RedHat Linux версии 7.2. Linux Ext3 обратно совместима с Linux Ext2. Ext3 имеет несколько режимов журналирования, а также широкую кросс-платформенную совместимость с 32- и 64-битными архитектурами.
- Ext4 — новая файловая система ОС Linux. В нее внесены усовершенствования по сравнению с ext3. Она полностью обратно совместима с ext2 и ext 3. Однако ext3 только частично совместима с ext4.
- ReiserFS — журналируемая файловая система Linux, которая Как правило, она надежнее и быстрее Ext2. Выберите ее для разделов данных в Linux.
- Linux Swap — раздел подкачки ОС Linux. Выберите данный параметр, если необходимо увеличить размер области подкачки, используемой Linux.

Буква раздела

Выберите букву, которая будет присвоена разделу. Если выбран параметр **Автоматически**, программа присвоит первую неиспользуемую букву в алфавитном порядке.

Метка раздела

Метка представляет собой имя, которое присваивается разделу для дальнейшего быстрого распознавания. Например, System — раздел с операционной системой, Data — раздел с данными и т. д. Метка раздела является необязательным атрибутом.

Тип раздела (только для MBR-дисков)

Тип нового раздела можно назначить основным или логическим.

- **Основной** — выберите данный тип, если с него планируется производить загрузку. В противном случае рекомендуется создать новый раздел в виде логического диска. Можно создать только четыре основных раздела на диске или три основных раздела и один расширенный.

  > **Примечание**
  >
  > При наличии нескольких основных разделов только один из них будет активным в определенный момент времени, остальные будут скрыты и их нельзя будет увидеть средствами ОС.

  - **Пометить раздел как активный** — установите этот флажок, если на данный раздел планируется установить операционную систему.
- **Логический** — выберите данный тип, если не требуется устанавливать и запускать операционную систему с данного раздела. Логический диск является частью физического диска, последний содержит разделы, распределенные как независимые единицы и функционирующие как отдельные диски.

Средства обеспечения безопасности и конфиденциальности

Очистка диска

Утилита Очистка диска позволяет уничтожить все данные на выбранных жестких дисках и разделах без возможности восстановления. Для уничтожения можно использовать один из готовых алгоритмов или создать собственный. Дополнительные сведения см. в разделе *Выбор алгоритма*.

Зачем это нужно?

Если вы просто форматируете старый жесткий диск, прежде чем его выбросить, информация не удаляется безвозвратно и все еще может быть восстановлена. Таким образом ваша информация может попасть не в те руки. Чтобы этого не произошло, рекомендуется использовать утилиту Очистка диска, когда вы:

- заменяете старый жесткий диск новым и не планируете больше использовать старый диск;
- отдаете старый жесткий диск родственнику или знакомому;
- продаете старый жесткий диск.

Использование утилиты Очистка диска

Как уничтожить данные на диске без возможности восстановления:

1. Запустите Кибер Бэкап Старт, перейдите в раздел **Инструменты** и щелкните **Очистка диска**. Откроется мастер Очистка диска.
2. На шаге **Выбор источника** выберите диски и разделы, которые требуется очистить. Дополнительные сведения см. в разделе *Выбор источника*.
3. На шаге **Выбор алгоритма** выберите алгоритм, который следует использовать для уничтожения данных. Дополнительные сведения см. в разделе *Выбор алгоритма*.
4. [Необязательно] Можно создать свой собственный алгоритм. Дополнительные сведения см. в разделе *Создание пользовательского алгоритма*.
5. [Необязательно] На шаге **Заключительные действия** выберите, что делать с разделами и диском после уничтожения данных. Дополнительные сведения см. в разделе *Заключительные действия*.
6. На шаге **Завершение** убедитесь, что параметры настроены правильно. Для запуска процесса установите флажок **Удалить выбранные разделы без возможности восстановления** и нажмите кнопку **Приступить**.

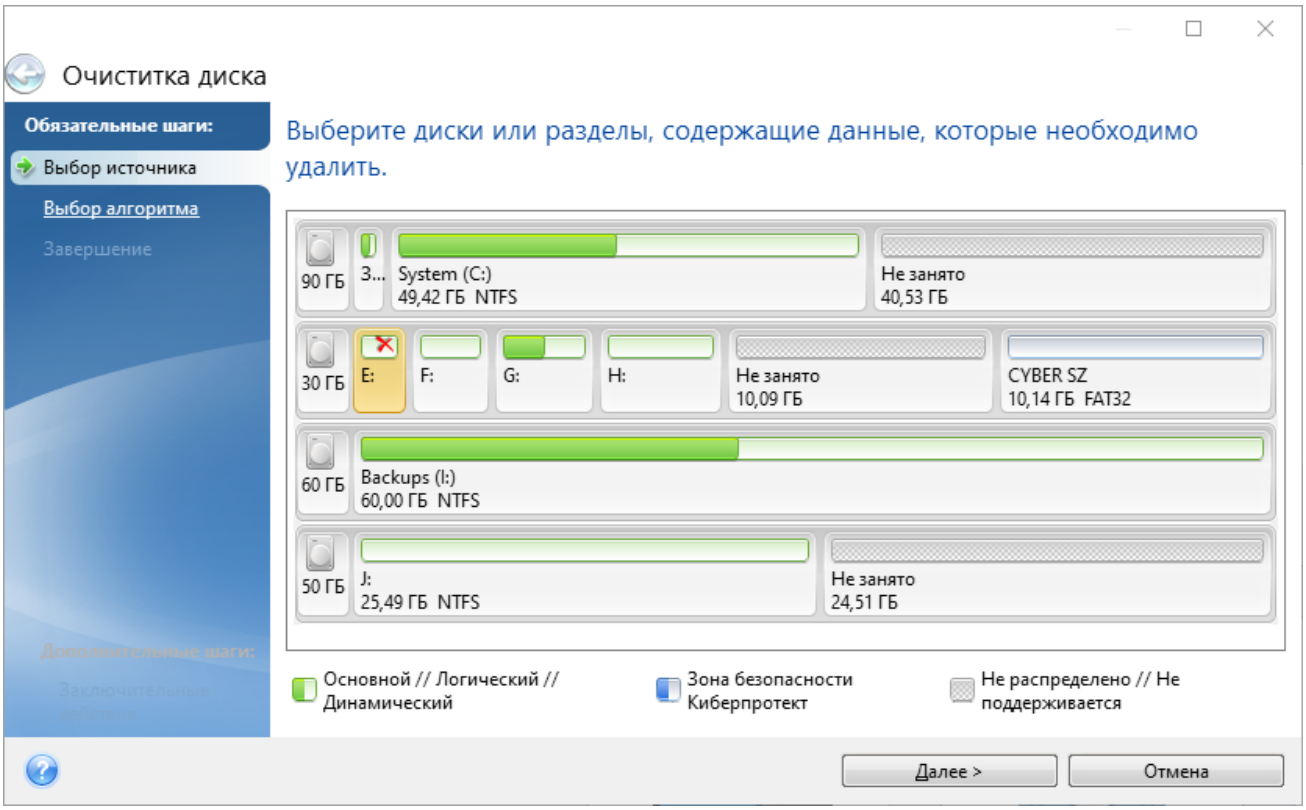
⚠ Предупреждение

Учтите, что процесс уничтожения данных может занять несколько часов, в зависимости от общего размера выбранных разделов и от выбранного алгоритма.

Выбор источника

На шаге **Выбор источника** выберите разделы и диски, на которых необходимо уничтожить данные.

- Для выбора раздела щелкните соответствующий прямоугольник. Красная метка ( ) означает, что раздел выбран.
- Чтобы выбрать весь жесткий диск, щелкните значок диска ( ).



Примечание

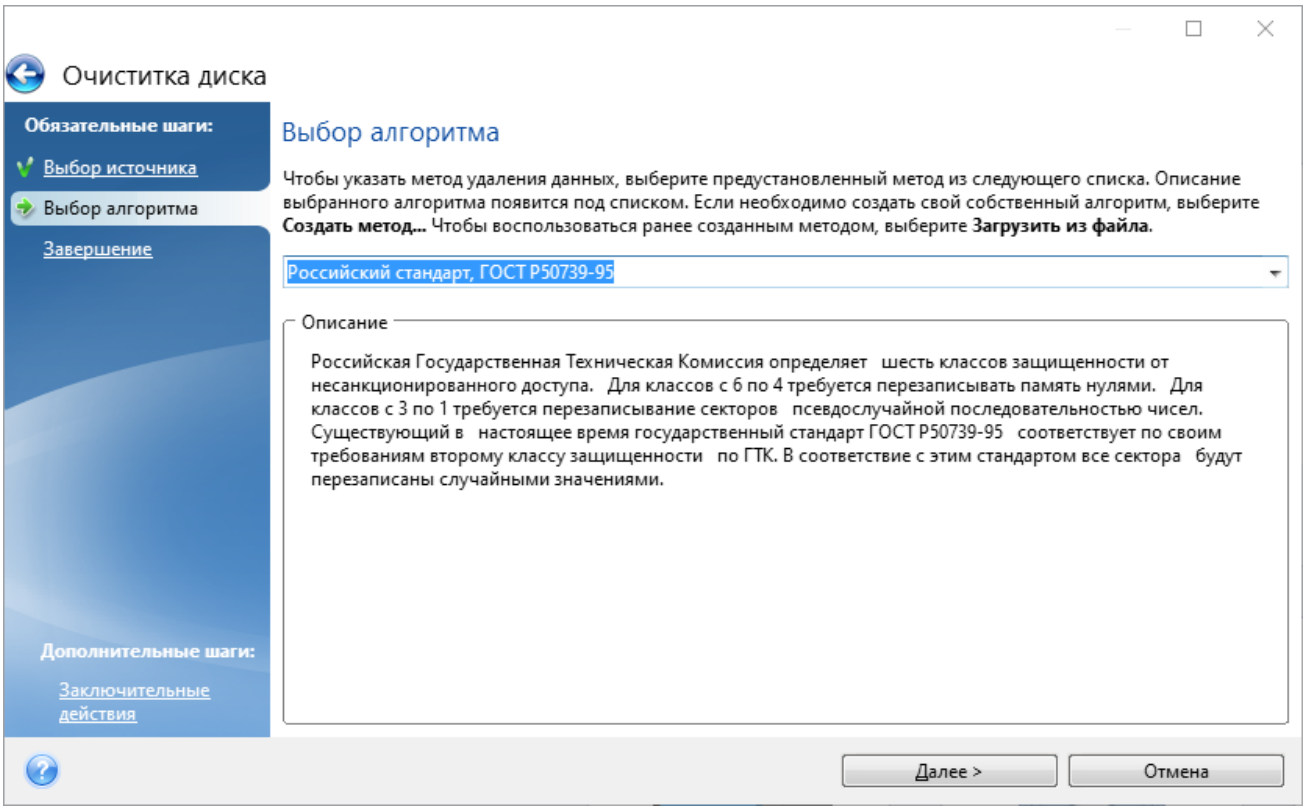
Очистка диска не очищает разделы на динамических и GPT-дисках, поэтому они не будут отображаться.

Выбор алгоритма

На шаге **Выбор алгоритма** выполните одно из следующих действий:

- Чтобы использовать готовый алгоритм, выберите нужный. Дополнительные сведения см. в разделе *Методы очистки жесткого диска*.
- [Только для опытных пользователей] Чтобы создать собственный алгоритм, выберите **Создать метод**. Затем продолжите создание на шаге **Определение алгоритма**. После этого можно будет сохранить созданный алгоритм в файл с расширением ALG.

- Чтобы использовать сохраненный ранее пользовательский алгоритм, выберите **Загрузить из файла** и укажите файл, содержащий нужный алгоритм.



Методы очистки жесткого диска

Информация, удаленная с жесткого диска ненадежными методами (например, простым удалением в Windows), может быть легко восстановлена. При наличии специализированного оборудования возможно восстановление даже многократно перезаписанной информации.

Как известно, данные на жестком диске хранятся в двоичной форме — в виде последовательности 1 и 0 (единиц и нулей), которые представлены различным образом намагниченными участками поверхности диска. Единица, записанная на жесткий диск, будет прочитана контроллером жесткого диска как 1, а записанный нуль будет прочитан как 0. Однако если поверх нуля будет записана единица, то результат будет условно равен 0,95, и наоборот, если поверх единицы будет записана единица, результат будет равен 1,05. Для контроллера эти различия несущественны. Но, используя специальную аппаратуру, легко прочитать, какую последовательность единиц и нулей содержала «нижележащая» запись.

Методы уничтожения информации

Подробное изложение теории гарантированного уничтожения информации можно найти, например, в статье Питера Гутмана (Peter Gutmann). См. Secure Deletion of Data from Magnetic and Solid-State Memory (Безопасное удаление данных с магнитных и твердотельных накопителей) по адресу http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

№	Алгоритм (метод записи)	Количе-ство проходов	Запись
1.	Американский: DoD 5220.22-M	4	1 проход — случайно выбранные символы в каждый байт каждого сектора; 2 — дополнительные к записанным на первом проходе; 3 — снова случайно выбранные символы; 4 — верификация записей.
2.	Американский: NAVSO P-5239-26 (RLL)	4	1 проход — 0x01 во все сектора, 2 — 0x27FFFFFF, 3 — случайные последовательности символов, 4 — верификация.
3.	Американский: NAVSO P-5239-26 (MFM)	4	1 проход — 0x01 во все сектора, 2 — 0x7FFFFFFF, 3 — случайные последовательности символов, 4 — верификация.
4.	Немецкий: VSITR	7	Проходы1–6 — чередующаяся последовательность из 0x00 и 0xFF; проход 7 — 0xAA; т. е. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
5.	Российский: ГОСТ Р50739-95	1	Запись логических нулей (чисел вида 0x00) в каждый байт каждого сектора для систем с шестого по четвертый класс защиты. Запись случайно выбранных чисел в каждый байт каждого сектора для систем с третьего по первый класс защиты.
6.	Метод П. Гутмана	35	Метод Питера Гутмана очень сложен и основан на его теории об очистке данных с жесткого диска (см. Secure Deletion of Data from Magnetic and Solid-State Memory (Безопасное удаление информации с магнитных и полупроводниковых источников хранения данных)).
7.	Метод Б. Шнайера	7	В своей книге «Прикладная криптография» Брюс Шнайер предложил метод, состоящий из 7 проходов перезаписи. 1 проход — запись логических единиц (0xFF), 2 — нулей (0x00), 3–7 — случайно выбранных чисел.
8.	Быстрый	1	Запись логических нулей (чисел вида 0x00) во все очищаемые сектора.

Создание пользовательских алгоритмов

Определение алгоритма:

На шаге **Определение алгоритма** отображается шаблон будущего алгоритма.

В таблице имеются следующие условные обозначения:

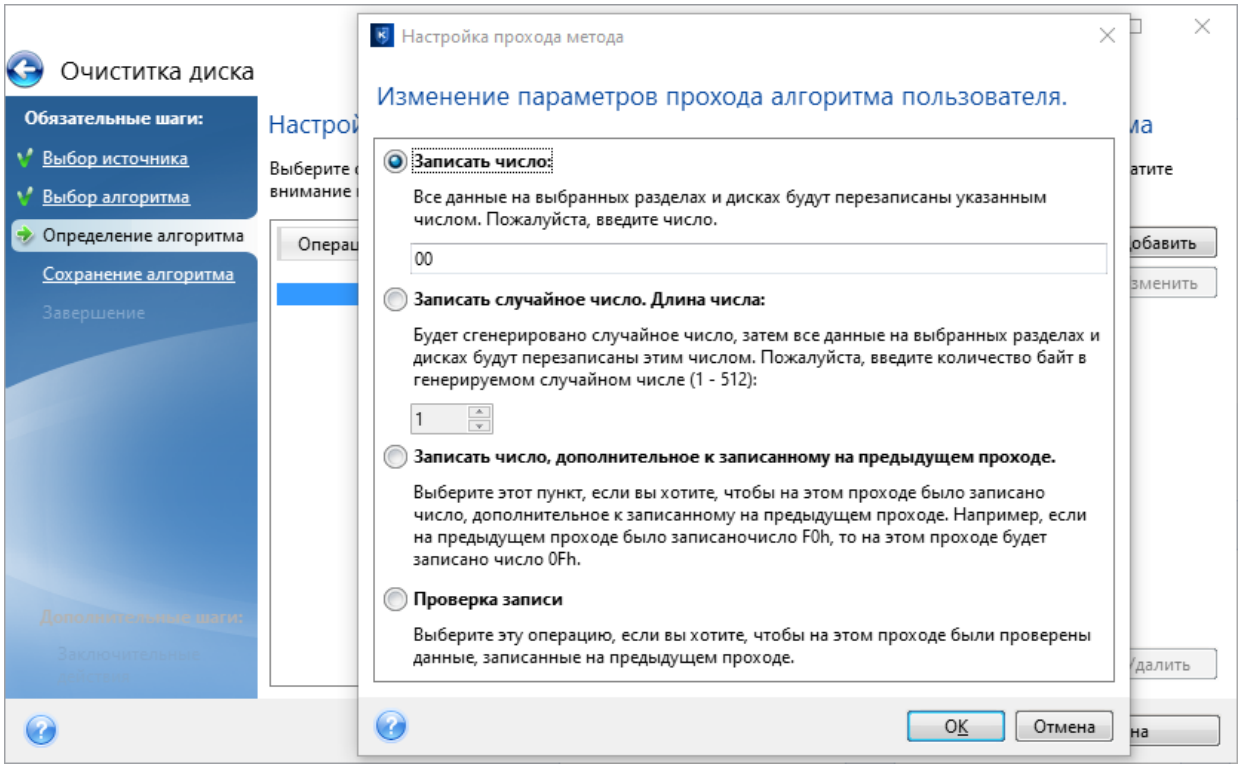
- В первом столбце указан тип операции (запись символа на диск и проверка записанного).

- Во втором столбце содержится записываемый на диск набор чисел.

Каждая строка определяет операцию, которая будет выполнена во время прохода. Чтобы создать собственный алгоритм, добавьте в таблицу столько строк, сколько сочтете нужным для надежного уничтожения данных.

Как добавить новый проход:

1. Нажмите кнопку **Добавить**. Откроется окно настройки прохода.



2. Выберите один из вариантов:

   - **Записать число**

     Введите шестнадцатеричное число, то есть число вида 0x00, 0xAA или 0xCD и т. д. В данном случае приведены числа длиной 1 байт, но они могут иметь длину до 512 байт. Кроме таких чисел можно ввести для записи случайное шестнадцатеричное число любой длины (до 512 байт, 512 байт — длина области данных сектора).

     > **Примечание**
     >
     > Если бинарное значение представлено последовательностью 10001010 (0x8A), то дополнительное бинарное значение будет представлено последовательностью 01110101 (0x75).

- **Записать случайное число**

  Укажите длину случайного числа в байтах.

- **Записать число, дополнительное к записанному на предыдущем проходе**

  Кибер Бэкап Старт добавит дополнительное значение к записанному на диск во время предыдущего прохода.

- **Проверка записи**

  Кибер Бэкап Старт проверит значения, записанные на диск во время предыдущего прохода.

3. Нажмите кнопку **ОК**.

Как изменить существующий проход:

1. Выберите соответствующую строку и щелкните **Изменить**.

   Откроется окно настройки прохода.

   > **Примечание**
   >
   > При выборе нескольких строк новые настройки будут применены ко всем выбранным проходам.

2. Измените настройки и нажмите кнопку **ОК**.

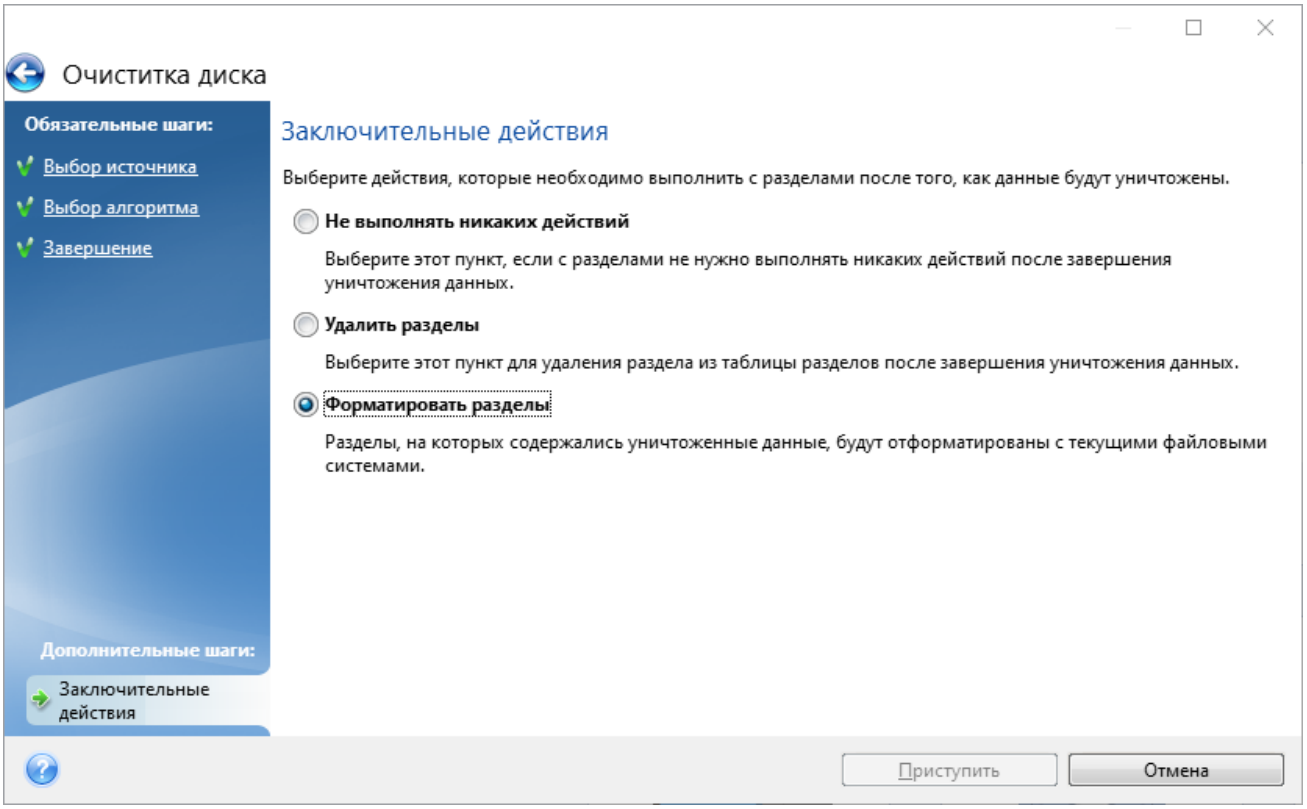
Сохранение алгоритма в файл:

1. На шаге **Сохранение алгоритма** выберите **Сохранить в файл** и нажмите кнопку **Далее**.
2. В открывшемся окне укажите имя и расположение файла и нажмите кнопку **ОК**.

Заключительные действия

В окне **Заключительные действия** выберите действия, проводимые с разделами, которые выбраны для уничтожения данных. Очистка диска предоставляет три варианта.

- **Не выполнять никаких действий** — просто удалить данные с помощью алгоритма, выбранного ниже.
- **Удалить разделы** — удалить данные и разделы.
- **Форматировать разделы** — удалить данные и отформатировать разделы (используется по умолчанию).



Очистка системы

Мастер очистки системы позволяет гарантированно удалять все следы работы на компьютере, включая имена пользователей, пароли и другие личные сведения.

Мастер может выполнять следующие операции:

- надежно уничтожать данные в **Корзине Windows**;
- удалять **временные файлы** из соответствующих папок Windows;
- очищать **свободное пространство на жестком диске** от любых следов хранившейся там прежде информации;
- удалять следы использования **поиска файлов и компьютеров** на подключенных дисках и компьютерах в локальной сети;
- очищать список **недавно использовавшихся документов**;
- очищать список **запускавшихся программ Windows**;
- очищать список истории **открытых или сохраненных файлов**;
- очищать список сетевых ресурсов, к которым подключался пользователь, используя **системные учетные данные**;
- очищать **папку запускавшихся приложений Windows**, где Windows хранит сведения о недавно

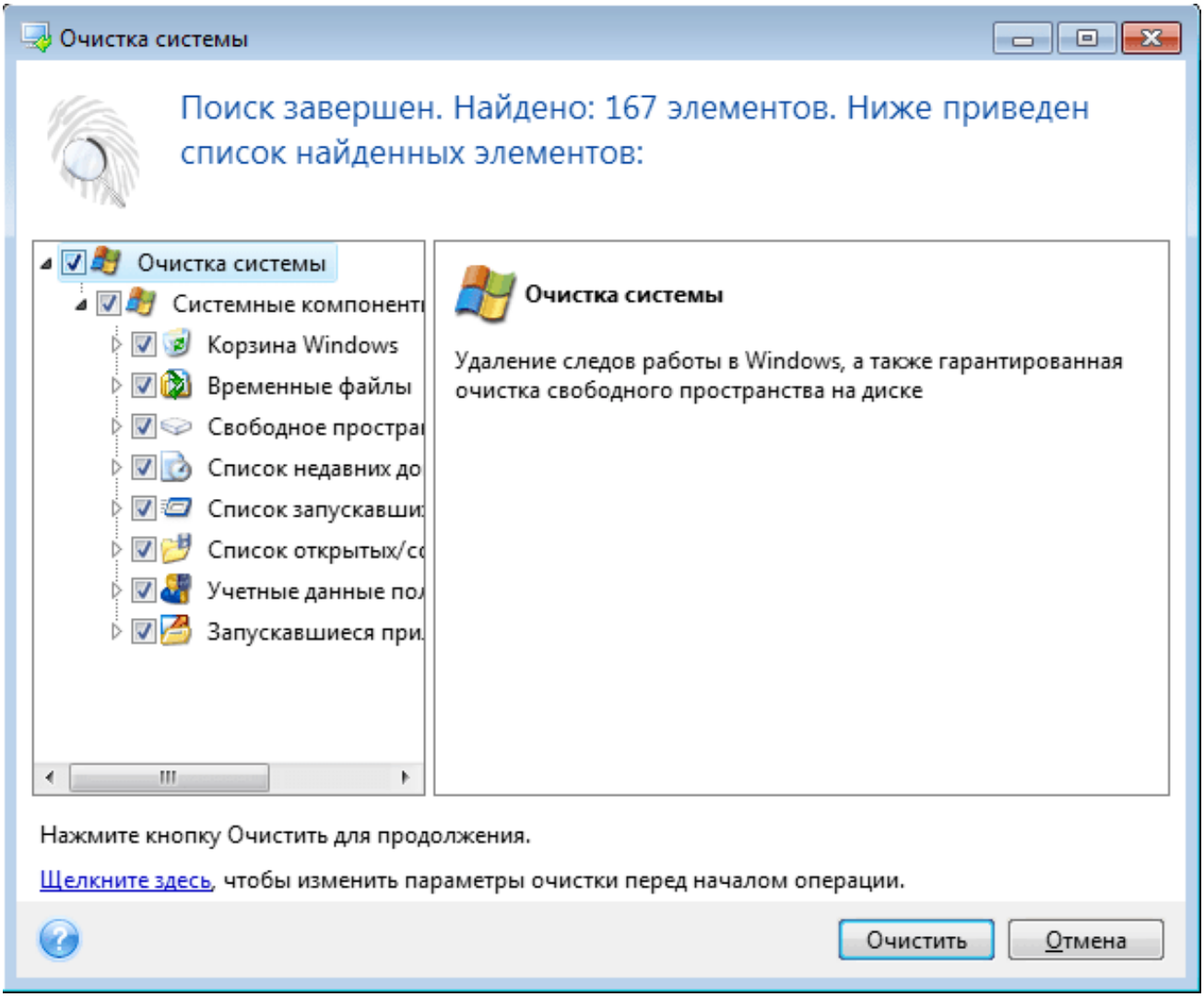
запускавшихся и выполнявшихся программах.

Примечание

- ОС Windows не хранит сведений о проведенных операциях поиска компьютеров и файлов. Более того, сведения об открытых или сохраненных файлах хранятся в реестре по-другому, поэтому мастер отображает эти сведения тоже по-другому.
- Windows хранит пароли до окончания сеанса, поэтому очистка списка сетевых учетных данных пользователей не вступит в силу, пока текущий сеанс Windows не завершится путем выхода пользователя из системы или перезагрузки компьютера.

Для запуска мастера очистки системы откройте Кибер Бэкап Старт, перейдите в раздел **Инструменты** и щелкните **Очистка системы**.

После запуска мастер начинает искать следы любых действий пользователей, которые сохранились в Windows. После завершения поиска его результаты будут доступны в верхней части окна мастера.



Просмотрите результаты поиска и вручную выберите те, которые необходимо удалить.

Нажмите текстовую гиперссылку **Щелкните здесь**, чтобы изменить настройки очистки перед тем как продолжить.

Нажмите кнопку **Очистить**, чтобы запустить удаление найденных элементов.

Настройки очистки

В этом окне можно изменить настройки очистки для каждого компонента системы. Некоторые из этих параметров применимы ко всем компонентам.

Как изменить настройки очистки для компонента:

- Разверните элемент **Системные компоненты** в дереве и выберите компонент, настройки очистки которого необходимо изменить. Чтобы включить или отключить сканирование компонента мастером очистки, установите или снимите флажок **Включено**.

  При необходимости разверните компонент и настройте метод уничтожения данных, файлы для

очистки, очистку строк поиска в реестре, использованных для поиска компьютеров в локальной сети, и т. д. Для этого щелкните треугольник рядом с компонентом, выберите вариант из списка и произведите настройки.

- Настроив нужные параметры компонентов, нажмите кнопку **ОК**, чтобы сохранить изменения. Эти настройки будут использоваться по умолчанию при следующем запуске мастера очистки.

Если настройки очистки уже изменялись прежде, всегда можно вернуться к параметрам по умолчанию, нажав кнопку **Восстановить настройки по умолчанию**.

Системные компоненты:

- Корзина Windows
- Временные файлы
- Свободное пространство жесткого диска
- Строка поиска компьютеров
- Строка поиска файлов
- Список недавних документов
- Список запускавшихся программ
- Список открытых или сохраненных файлов
- Учетные данные пользователя
- Запускавшиеся приложения

Параметры очистки по умолчанию

Чтобы просмотреть параметры очистки, установленные по умолчанию, используйте ссылку **Щелкните, чтобы изменить данный параметр** на странице параметра **Метод удаления данных**.

Как изменить параметры очистки по умолчанию:

1. Выберите в дереве компонент настроек очистки, который необходимо изменить.
2. После настройки параметров нажмите кнопку **ОК**, чтобы сохранить изменения.

Если настройки очистки уже изменялись прежде, всегда можно вернуться к параметрам по умолчанию, нажав кнопку **Восстановить настройки по умолчанию**.

Общие

По умолчанию диалоговое окно итогов отображается после завершения каждой операции очистки (при выбранном параметре **Показывать отчет**). Если отображать это окно не требуется, снимите соответствующий флажок.

Параметры очистки

При очистке системы используются самые популярные методы уничтожения данных. Выберите метод уничтожения данных, который будет использоваться по умолчанию для всех других компонентов.

Дополнительные сведения о методах уничтожения данных см. в разделе *Методы очистки жесткого диска*.

Отдельные параметры очистки

Можно настроить следующие параметры очистки.

- Метод удаления данных
- Параметры по умолчанию
- Файлы
- Свободное пространство на диске
- Компьютеры
- Команды
- Фильтр сетевого окружения

Метод удаления данных

При очистке системы используются самые популярные методы уничтожения данных. Выберите желаемый метод уничтожения данных.

- **Использовать общий метод** — при выборе этого параметра программа будет использовать метод по умолчанию (исходная настройка — быстрый метод).

  Если необходимо выбрать для использования по умолчанию другой метод уничтожения данных, щелкните соответствующую ссылку.

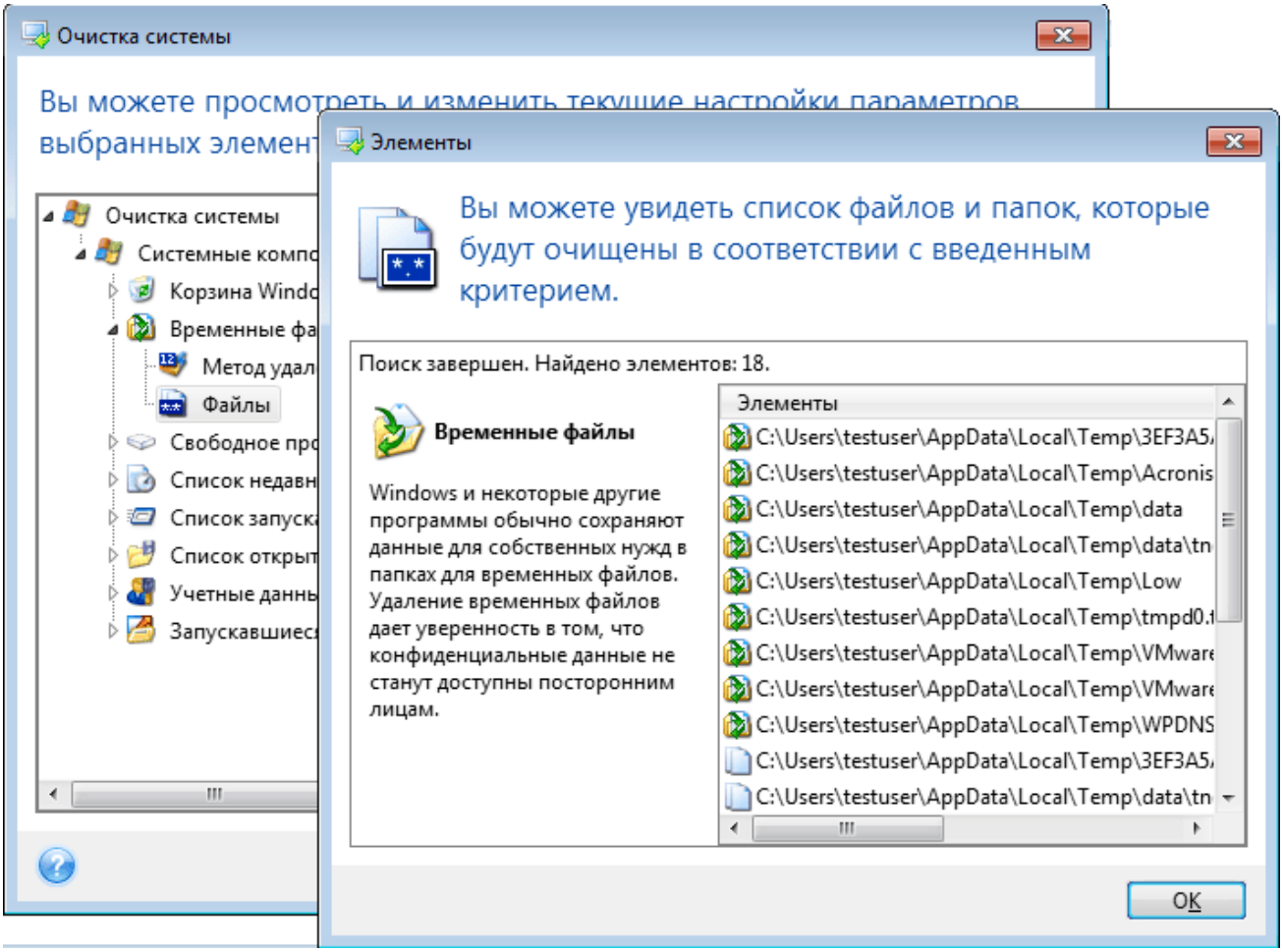
- При выборе пункта **Использовать общий метод для данного компонента** будет использован один из имеющихся методов уничтожения данных. Выберите необходимый метод уничтожения данных из раскрывающегося списка.

Дополнительные сведения о методах уничтожения данных см. в разделе *Методы очистки жесткого*

диска.

Файлы

Параметр «Файлы» служит для задания имен файлов, удаляемых мастером очистки системы, и может использоваться со строкой поиска.



При выполнении поиска в ОС Windows в строке поиска можно ввести полное имя файла или его часть. Строка поиска может состоять из любых буквенно-цифровых символов, включая запятую и подстановочные знаки Windows, и содержать, например, следующие значения:

- `*.*` — удаляются все файлы с любыми именами и расширениями;
- `*.doc` — удаляются файлы с определенным расширением, в данном случае файлы документов Майкрософт;
- `read*.*` — удаляются все файлы с любым расширением, имена которых начинаются с ”read”;
- `read?.*` — удаляются все файлы с именами из пяти букв и любыми расширениями, если имена файлов начинаются с ”read”; пятая буква может быть любой.

  Последняя строка поиска, например, приведет к удалению файлов `read1.txt`, `ready.doc`, но

оставит файл `readyness.txt`, так как длина его имени (без расширения) слишком велика.

Можно ввести несколько различных строк поиска, разделив их точкой с запятой, например:

`*.bak;*.tmp;*.~~~` (без пробелов между строками поиска).

При этом будут удаляться все файлы, имена которых соответствуют хотя бы одной из введенных строк.

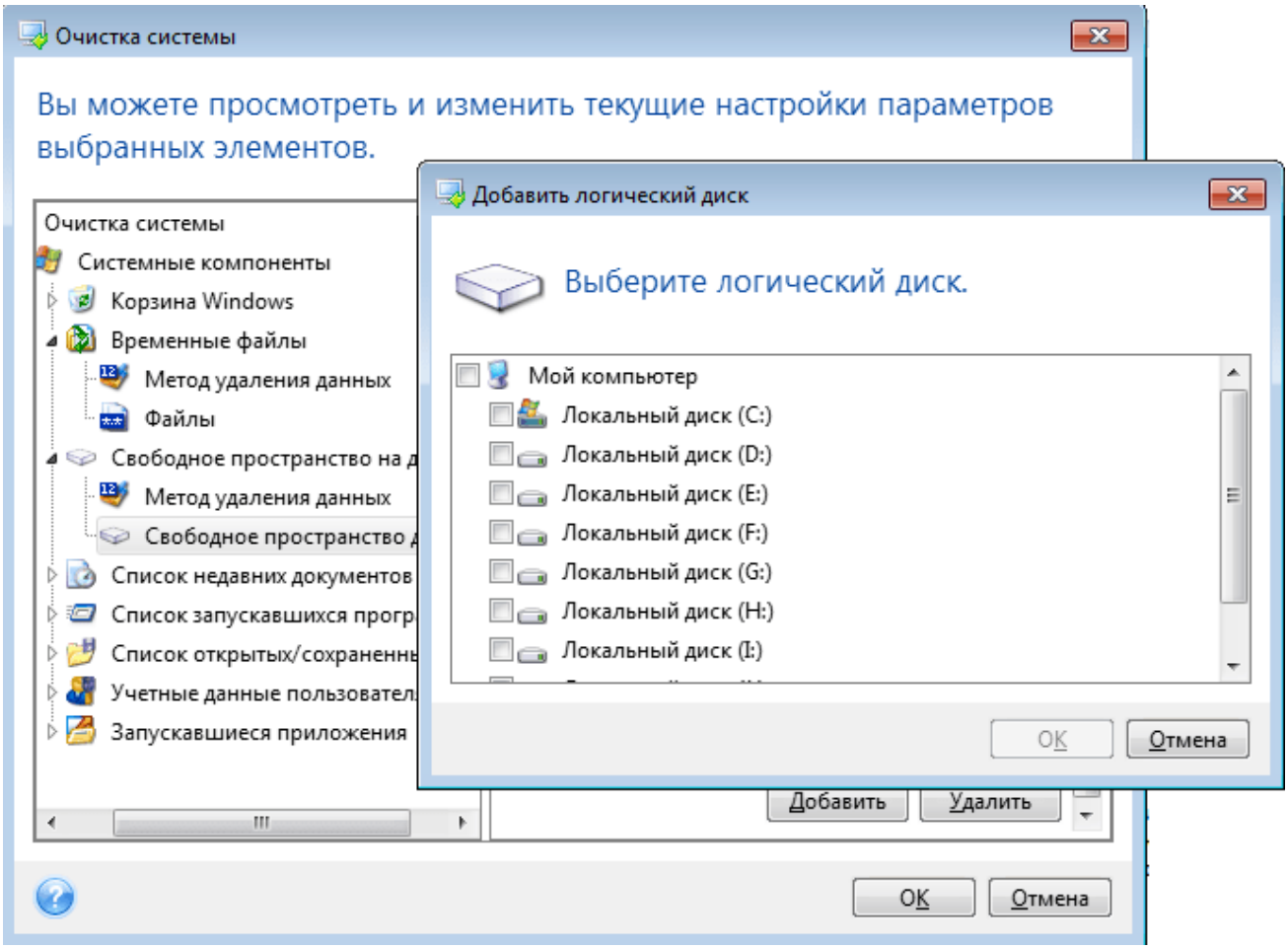
После ввода значений параметра **Файлы** можно просмотреть файлы, которые соответствуют введенным строкам поиска. Для этого нажмите кнопку **Показать файлы**. Откроется окно с именами найденных файлов. Эти файлы будут удалены.

Свободное пространство на диске

Здесь можно вручную указать, на каких физических или логических дисках следует освободить дисковое пространство. По умолчанию функция очистки системы освобождает пространство на всех доступных физических и логических дисках.

Чтобы изменить настройки данного параметра, нажмите кнопку **Удалить** для удаления из списка дисков, очистка свободного пространства на которых не требуется.

Если затем потребуется добавить в данный список удаленные диски, нажмите кнопку **Добавить**.



Компьютеры

Параметр **Компьютеры** предназначен для настройки удаляемых из реестра строк поиска компьютеров в локальной сети. Строки поиска сохраняют информацию о том, что интересовало пользователя в сети. Поэтому для сохранения конфиденциальности они должны быть удалены.

Настройка параметра **Компьютеры** сходна с настройкой параметра **Файлы**. Это строка, которая может содержать любое количество полных или частичных имен компьютера, разделенных точкой с запятой. При удалении строк поиска компьютеров используется сравнение этих строк со значением параметра **Компьютеры** в соответствии с правилами ОС Windows.

Если необходимо просто удалить все строки поиска компьютеров в локальной сети (чаще всего только это и необходимо), просто оставьте значение, принятое по умолчанию для этого параметра. Чтобы восстановить настройки по умолчанию:

- выберите компонент **Строка поиска компьютеров**;
- убедитесь, что установлен флажок **Включить**;
- выберите параметр **Компьютеры**; убедитесь, что текстовое поле пустое.

В результате из реестра будут удалены все строки поиска компьютеров.

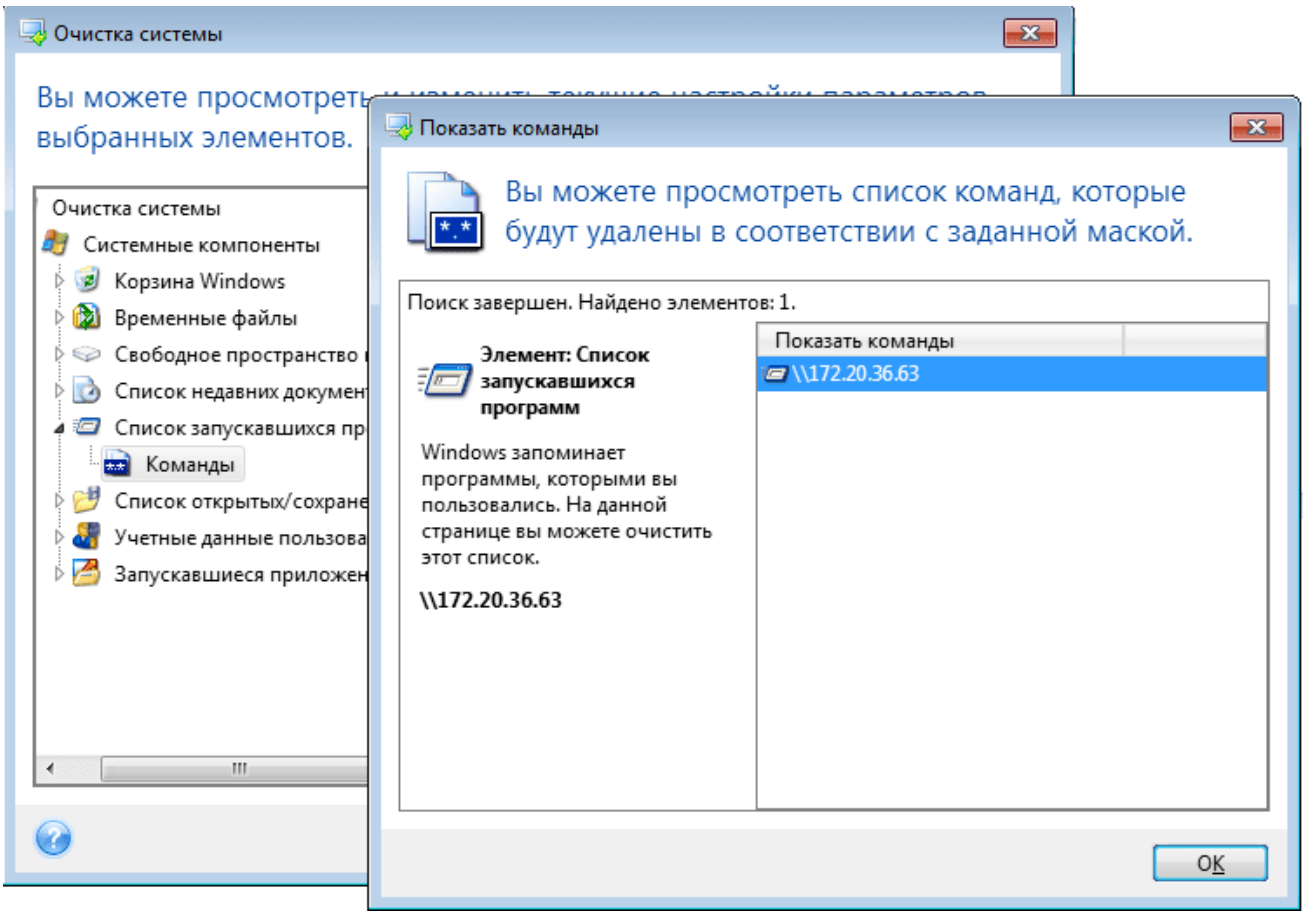
Введя значение параметра **Компьютеры**, можно просмотреть строки поиска, сохраненные в реестре и найденные мастером очистки системы. Для этого нажмите кнопку **Показать компьютеры**. Откроется окно с именами компьютеров, соответствующими параметрам поиска. Данные элементы будут удалены.

Настройка команд

В данном пункте можно выбрать команды, которые подлежат удалению при очистке **Списка запускавшихся программ**.

Данный шаблон может содержать имена любых команд или их части, введенные через точку с запятой, например: `\*help; cmd; reg\*`.

При этом из списка удаляются те команды, названия которых соответствуют хотя бы одному из введенных имен или содержат часть этих введенных имен.



Фильтр сетевого окружения

Здесь можно ввести (через точку с запятой) любые имена хостов или IP-адреса сетевого окружения, серверов, FTP-серверов, общих сетевых папок и других ресурсов, к которым осуществлялось подключение с введением сетевых учетных данных (имени пользователя и пароля). При вводе имен узлов и IP-адресов можно использовать подстановочные символы * и ?.

Нажмите **Показать сетевое окружение**, чтобы просмотреть список сетевых ресурсов, при посещении которых использовались учетные данные, которые необходимо удалить.

Просмотр

После завершения сканирования его результаты будут доступны в верхней части окна мастера. По умолчанию все системные компоненты сканируются для очистки. Если необходимо указать, какие из системных компонентов требуется сканировать, а какие нет, измените параметры очистки, установленные по умолчанию.

Просмотрите результаты поиска и вручную выберите те элементы, которые необходимо удалить, или отмените выбор тех, которые необходимо оставить. Чтобы помочь сделать правильный выбор, все компоненты сопровождаются кратким описанием. Просто выберите имя компонента, и его описание

отобразится в правой части окна.

Как выбрать или отменить выбор компонента:

- Разверните элемент **Системные компоненты** в дереве «Очистка системы» и убедитесь, что компонент, который требуется очистить, выбран. Если не требуется очищать компонент, просто снимите с него флажок.
- При необходимости произведите более детальный выбор, развернув компонент и выбрав или отменив выбор содержащихся в нем элементов.

Указав компоненты для очистки, нажмите кнопку **Очистить**, чтобы продолжить.

Примечание

ОС Windows не хранит сведений о проведенных операциях поиска компьютеров и файлов. Более того, сведения об открытых или сохраненных файлах хранятся в реестре по-разному, поэтому мастер отображает эти сведения тоже по-разному.

Состояние операции очистки

В данном окне показывается текущее состояние операции.

Ход выполнения выбранной операции показывается в виде индикатора выполнения.

Иногда выполнение операции может занять длительное время. В этом случае установите флажок **Выключить компьютер после завершения**. После завершения операции Кибер Бэкап Старт выключит компьютер.

Подключение резервной копии

Подключение резервных копий в качестве виртуальных дисков позволяет обращаться к ним как к физическим дискам. Можно подключить локальные резервные копии, которые содержат разделы или целые диски, а затем выбрать разделы для подключения. После подключения:

- В системе появляется новый диск для каждого подключенного раздела.
- Содержимое резервной копии можно просматривать в режиме «только чтение» с помощью проводника Windows и других диспетчеров файлов.

Примечание

- Операции, описанные в этом разделе, поддерживаются только для файловых систем FAT и

NTFS.

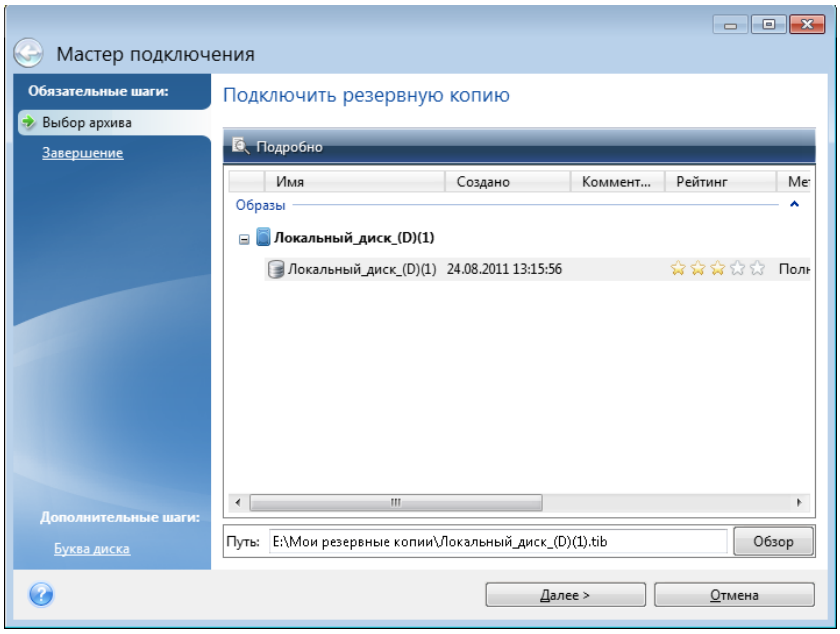
- Резервную копию диска подключить нельзя, если она хранится на FTP-сервере.

Как подключить резервную копию

1. В проводнике Windows щелкните правой кнопкой мыши файл резервной копии, который необходимо подключить, и в контекстном меню выберите **Cyber Backup Start → Подключить**.

   Откроется мастер подключения.

2. Выберите резервную копию для подключения по дате и времени создания. Таким образом, можно проанализировать состояние данных на определенный момент времени.



3. [Необязательно] На шаге **Буква диска** в раскрывающемся списке **Назначить букву** выберите букву, которая будет присвоена виртуальному диску. Если нет необходимости подключать раздел, выберите в списке вариант **Не назначать** или снимите флажок рядом с названием раздела.

4. Нажмите кнопку **Приступить**.

5. После подключения резервной копии откроется окно проводника Windows, в котором будет показано её содержимое.

Отключение резервной копии

После выполнения необходимых операций подключенную резервную копию (виртуальный диск) рекомендуется отключить, так как поддержка виртуального диска отнимает значительную часть системных ресурсов.

Чтобы отключить резервную копию, выполните одно из следующих действий:

- В проводнике Windows в меню **Этот компьютер** щелкните значок диска правой кнопкой мыши и в контекстном меню выберите **Cyber Backup Start** → **Отключить**.
- Перезагрузите или выключите компьютер.

Работа с VHD(X)-файлами

Резервные копии Киберпротект (TIBX-файлы) дисков и разделов можно преобразовать в виртуальные жесткие диски (VHD(X)-файлы).

Использование VHD(X)-файлов

- Можно загрузить компьютер из преобразованного VHD(X)-файла, чтобы проверить целостность резервной копии и возможность восстановления работоспособной ОС.
- Преобразованный VHD(X)-файл можно сохранить на случай аварийной ситуации. Например, если компьютер не запускается, а вам необходимо работать на нем прямо сейчас, можно загрузить его из VHD(X)-файла.
- Преобразованный VHD(X)-файл можно запустить в качестве виртуальной машины.

Ограничения и дополнительная информация

- Резервную копию файлов нельзя преобразовать в VHD(X)-файл.
- Чтобы выполнить загрузку из преобразованного VHD(X)-файла, он должен содержать:
  - Системный раздел этого компьютера. Загрузить другие компьютеры с помощью этого же VHD(X)-файла нельзя.
  - Поддерживаемую ОС Windows.
- Любые изменения, сделанные в загруженном или подключенном VHD(X)-файле, сохраняются в нем. Если загрузить компьютер из VHD(X)-файла, а затем изменить данные, резервное копирование которых не выполнялось, эти изменения повлияют на вашу систему.
- Автономные версии Кибер Бэкап Старт на загрузочном носителе не поддерживают операции преобразования.
- Кибер Бэкап Старт не может преобразовывать TIBX-файлы, содержащие динамические тома, изначально находившиеся на более чем одном диске (чередующемся или составном из двух или более дисков).

Преобразование резервных копий, созданных в ПО Киберпротект

Пользователи Windows могут преобразовать резервные копии системных разделов из формата TIBX в формат VHD(X), чтобы использовать преобразованные файлы для загрузки операционной системы. Либо им может потребоваться возможность подключать резервные копии без использования Кибер Бэкап Старт.

Как преобразовать резервную копию диска Киберпротект (TIBX-файл) в резервную копию Windows (VHD(X)-файл):

1. Запустите Кибер Бэкап Старт.
2. Перейдите в раздел **Резервное копирование**.
3. В списке резервных копий щелкните стрелку вниз рядом с нужной резервной копией и выберите **Преобразовать в VHD**.

   Если резервная копия защищена паролем, Кибер Бэкап Старт предложит его ввести. Учтите, что получившийся VHD(X)-файл потеряет защиту паролем.
4. Выберите версию резервной копии, которую нужно преобразовать.

   Преобразование инкрементной резервной копии требует наличия всех предыдущих инкрементных резервных копий и исходной полной резервной копии. Преобразование дифференциальной резервной копии требует наличия исходной полной резервной копии. Результатом преобразования всегда является полная резервная копия.
5. Укажите путь к создаваемому файлу.

   Файл можно сохранить в любом локальном хранилище, поддерживаемом Кибер Бэкап Старт (кроме зоны безопасности Киберпротект). Кроме того, его можно сохранить на сетевой ресурс SMB.
6. [Необязательно] Пока идет преобразование резервной копии, можно установить флажок **Запустить виртуальную машину после завершения**. Если флажок установлен, Кибер Бэкап Старт перезагрузит компьютер и запустит виртуальную машину Hyper-V с помощью созданного VHD(X)-файла.

Если TIBX-файл, выбранный для преобразования, содержит разделы, например, из двух физических жестких дисков, программа создаст два VHD(X)-файла, соответствующие этим физическим дискам.

Импорт и экспорт параметров резервного копирования

Кибер Бэкап Старт позволяет импортировать и экспортировать параметры резервных копий. Это удобно, когда необходимо перенести параметры на новый ПК после установки на нем Кибер Бэкап Старт. Сохраненные параметры также могут быть полезны при переходе на новую версию Кибер Бэкап Старт.

Такой перенос значительно упростит настройку параметров резервного копирования на новом ПК.

Достаточно экспортировать параметры, а затем импортировать их на другой ПК. Параметры экспортируются в виде файлов сценариев.

Содержимое параметров может различаться в зависимости от типа резервной копии. В случае «классических» резервных копий дисков и файлов параметры содержат следующие элементы:

- список элементов для резервного копирования;
- параметры резервного копирования;
- хранилище резервных копий;
- расписание;
- схема резервного копирования;
- правила автоматической очистки;
- правила присвоения имен версиям резервной копии.

Примечание

Импортировать параметры резервного копирования в онлайн-хранилище с одного компьютера на другой невозможно.

Как экспортировать параметры резервного копирования:

1. Запустите Кибер Бэкап Старт.
2. На боковой панели выберите **Параметры** → **Перенос параметров резервного копирования**, щелкните **Сохранить параметры в файл** и выберите расположение, в котором следует сохранить файлы сценариев с параметрами.

Как импортировать параметры резервного копирования:

1. Запустите Кибер Бэкап Старт на другом компьютере.
2. На боковой панели выберите **Параметры** → **Перенос параметров резервного копирования**, щелкните **Импортировать параметры из файла** и укажите путь к файлам сценариев с параметрами.

После импорта параметров на новом компьютере некоторые из них, возможно, потребуется изменить. Например, список элементов для резервного копирования, место назначения резервных копий и т. д.

Если необходимо скопировать некоторые резервные копии на другой компьютер, рекомендуется экспортировать и их параметры. Тогда функции копируемых резервных копий будут сохранены.

Устранение неисправностей

Создание отчетов о системе

При обращении в службу поддержки Киберпротект для устранения проблемы обычно требуются сведения о системе. Создание системного отчета вручную — трудоемкий процесс, занимающий много времени.

Утилита **Создать системный отчет** создает системный отчет со всей необходимой технической информацией и сохраняет эту информацию в файле. Прикрепите созданный файл к описанию имеющейся проблемы и отправьте его в службу поддержки. В этом случае проблема может быть решена проще и быстрее.

Для создания системного отчета выполните одно из следующих действий:

- На боковой панели нажмите **Справка** и выберите **Создать системный отчет**.
- Нажмите сочетание клавиш `CTRL+F7`. Это сочетание клавиш можно использовать, даже если Кибер Бэкап Старт выполняет любую другую операцию.
- Если используется ОС Windows 11, щелкните **Все приложения** → **Cyberprotect** → **System Report**.
- Если используется ОС Windows 10, в меню **Пуск** щелкните **Cyberprotect** → **System Report**.

После создания отчета:

- Чтобы сохранить созданный системный отчет, щелкните **Сохранить** и в открывшемся окне укажите расположение для созданного файла.
- Чтобы выйти из главного окна программы без сохранения отчета, нажмите кнопку **Отмена**.

Чтобы создать системный отчет, когда компьютер не загружается, поместите этот инструмент на загрузочный носитель в виде отдельного компонента. После загрузки с помощью загрузочного носителя можно создать отчет, не запуская Кибер Бэкап Старт. Просто подключите флеш-накопитель USB и щелкните по значку **Cyberprotect System Report**. Созданный отчет будет сохранен на флеш-накопитель USB.

Как поместить утилиту создания системных отчетов на загрузочный носитель:

1. Установите флажок **Системный отчет** на странице **Выбор содержимого загрузочного носителя** в программе **Мастер создания загрузочных носителей**.
2. Для продолжения нажмите кнопку **Далее**.

Создание системного отчета с помощью командной строки:

1. Запустите утилиту командной строки Windows (**cmd.exe**) от имени администратора.
2. Смените текущий каталог на папку установки Кибер Бэкап Старт. Для этого введите следующее:

   ```
   cd C:\Program Files (x86)\Cyberprotect\CyberBackupPersonal
   ```

3. Чтобы создать системный отчет, введите:

   ```
   SystemReport
   ```

   Файл `SystemReport.zip` будет создан в текущей папке.

   Чтобы назвать файл отчета другим именем, введите его на месте параметра <имя файла>:

   ```
   SystemReport.exe /filename:<file name>
   ```

Как создать системный отчет в среде загрузочного носителя:

1. Если загрузочный носитель отсутствует, создайте его. Дополнительные сведения см. в разделе *Мастер создания загрузочных носителей*.
2. Измените порядок загрузки в BIOS так, чтобы сделать устройство с загрузочным носителем (CD-диск или флеш-накопитель USB) первым устройством загрузки. Дополнительные сведения см. в разделе *Настройка порядка загрузки в BIOS*.
3. Выполните загрузку, используя загрузочный носитель, и выберите Кибер Бэкап Старт.

   Примечание

   Вместо нажатия на название продукта можно вставить флеш-накопитель USB и щелкнуть **Cyberprotect System Report**. В этом случае программа создает отчет и автоматически сохраняет его на флеш-накопитель.

4. Щелкните стрелку рядом со значком справки () и выберите **Создать системный отчет**.
5. Когда отчет будет создан, нажмите кнопку **Сохранить** и в открывшемся окне выберите расположение для созданного файла.

   Программа архивирует отчет в ZIP-файл.

Сбор аварийных дампов

Поскольку сбой Кибер Бэкап Старт или Windows может быть вызван различными причинами, каждый случай необходимо рассматривать отдельно. Службе поддержки пользователей Киберпротект будет полезна следующая информация.

При критической ошибке Кибер Бэкап Старт предоставьте следующие сведения:

1. Описание точной последовательности действий, выполненных перед возникновением проблемы.
2. Аварийный дамп.

Если Кибер Бэкап Старт вызывает критическую ошибку Windows:

1. Описание точной последовательности действий, выполненных перед возникновением проблемы.
2. Дамп-файл Windows.

Если Кибер Бэкап Старт не отвечает:

1. Описание точной последовательности действий, выполненных перед возникновением проблемы.
2. Пользовательский дамп процесса.
3. Журнал программы Procmon.

Если вы не можете получить доступ к этим сведениям, обратитесь в службу поддержки пользователей Киберпротект за помощью.

Эти сведения ускорят поиск решения.