КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 26.03

Информационная безопасность в частном облаке

Редакция: 20.04.2026

Содержание

Заявление об авторских правах

1 Введение

В данном руководстве приведены рекомендации по обеспечению информационной безопасности продукта Кибер Бэкап Облачный при развёртывании в частном облаке.

2 Установка

Рекомендуется устанавливать все обновления Кибер Бэкапа Облачного, так как они могут включать важные исправления и улучшения безопасности.

2.1 Рекомендации по способам установки

Рекомендуемые способы установки Кибер Бэкапа Облачного приведены в документе Развёртывание частного облака.

Агенты Кибер Бэкапа Облачного можно установить следующими способами:

- **Офлайн-установка** (рекомендуемый способ)

  Понадобится загрузить установщик, который затем установит агенты. При использовани этого способа программы установки агентов можно разместить на сетевом диске. Описание порядка установки агентов приведено в Руководстве пользователя.
- **Веб-установка**

  Понадобится загрузить веб-установщик, который затем загрузит основную программу установки из интернета и сохранит её в качестве временного файла (этот файл будет удалён сразу после установки). В течение всей установки необходим доступ в интернет. Описание порядка установки агентов приведено в Руководстве пользователя.
- **Автоматическая установка**

  Данный способ позволяет выполнить установку агентов на машинах с ОС Windows в автоматическом режиме при использовании установщика Windows (программы msiexec) или с помощью групповой политики в домене Active Directory (описание порядка автоматической установки агентов приведено в Руководстве пользователя).

Примечание

Перед установкой агентов требуется выполнить подготовительные операции, в том числе проверить и настроить порты, необходимые для работы компонентов Кибер Бэкапа Облачного (подробнее см. в Руководстве пользователя).

2.1.1 Добавление сертификата в цепочку доверия агента

После установки агента в его цепочку доверия необходимо добавить самоподписанный сертификат, который использовался при развёртывании Кибер Бэкапа Облачного. Для этого потребуется внести соответствующие данные в файл cert_bundle.pem, который находится по следующему адресу:

- в ОС Windows: C:\ProgramData\Acronis\CurlCaCertificates;
- в ОС Linux: /var/lib/Acronis/CurlCaCertificates.

Примечание
Инструкции по добавлению сертификата в цепочку доверия агента относятся к агентам версии 25.11 и выше.

2.2 Рекомендации по регистрации агента

Машина с установленным агентом может быть зарегистрирована в Кибер Бэкапе Облачном как автоматически при установке агента на машину (подробнее см. в Руководстве пользователя), так и вручную с использованием интерфейса командной строки. При этом такие параметры, как адрес службы Кибер Бэкап Облачный, в которой должна быть зарегистрирована машина с агентом, и данные учётной записи, используемой для регистрации, указываются в процессе регистрации (в настройках автоматической регистрации, в параметрах маркера или в тексте используемой команды для регистрации вручную).

Регистрация машины с установленным агентом с использованием интерфейса командной строки может быть выполнена двумя способами:

- **С помощью маркера регистрации** (рекомендуемый способ)

  Маркер регистрации представляет собой уникальную последовательность из 12 цифро-буквенных символов (например, 7A85-70B2-445F). Его можно создать для пользователя и затем указать при развёртывании агента или виртуального устройства, не указывая и не сохраняя при этом имя учётной записи и пароль соответствующего пользователя.

  Маркер обладает ограниченным сроком действия (от 1 минуты до 12 месяцев), который задаётся при его создании. По истечении данного срока маркер автоматически удаляется. При необходимости можно создать несколько маркеров с разным сроком действия.

  Примечание
  - Рекомендуется назначать наименьший допустимый срок действия маркеров регистрации.
  - При удалении пользователя маркер регистрации, выпущенный на его имя, перестаёт действовать, даже если срок его действия не истёк.

  С помощью одного и того же маркера, срок действия которого ещё не истёк, можно зарегистрировать любое количество агентов и виртуальных устройств. Использование маркеров регистрации для иных целей не предусмотрено. Инструкции по созданию и удалению маркеров регистрации приведены в Руководстве пользователя.

  Для регистрации машины с помощью регистрационного маркера на защищаемой машине выполните следующую команду в интерфейсе командной строки:

  - в ОС Windows:

    ```
    "%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud -a https://<адрес службы> --token <маркер регистрации>
    ```

  - в ОС Linux:

```
sudo /usr/lib/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a <адрес службы>
--token <маркер регистрации>
```

Где:

- <адрес службы> – адрес службы Кибер Бэкап Облачный, в которой должна быть зарегистрирована машина с агентом;
- <маркер регистрации> – маркер регистрации.

- **По имени пользователя и паролю**

  Для регистрации машины с помощью имени пользователя и пароля на защищаемой машине выполните следующую команду в интерфейсе командной строки:

  - в ОС Windows:

    ```
    "%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud -a
    https://<адрес службы> -u <имя пользователя> -p "<пароль пользователя>"
    ```

  - в ОС Linux:

    ```
    sudo /usr/lib/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a <адрес службы>
    -u <имя пользователя> -p '<пароль пользователя>'
    ```

  Где:

  - <адрес службы> – адрес службы Кибер Бэкап Облачный, в которой должна быть зарегистрирована машина с агентом;
  - <имя пользователя> – имя пользователя, под чьей учётной записью регистрируется машина с агентом;
  - <пароль пользователя> – пароль пользователя, под чьей учётной записью регистрируется машина с агентом.

Предупреждение

Не рекомендуется вводить данные учётной записи, в том числе пароль, в открытом виде.

При регистрации машины с агентом с помощью данных учётной записи рекомендуется выполнить дополнительные шаги:

- подготовьте TXT-файл с аргументами для команды регистрации;
- по завершении регистрации машины с агентом поменяйте пароль учётной записи, использованной для регистрации (подробнее о порядке сброса пароля см. в Руководстве пользователя).

Ниже приведён шаблон файла с аргументами для команды регистрации:

```
-o
register
-t
cloud
-a
<адрес службы>
```

```
-u
<имя пользователя>
-b
-p
<пароль пользователя в формате base64>
```

Где:

- <адрес службы> – адрес службы Кибер Бэкап Облачный, в которой должна быть зарегистрирована машина с агентом;
- <имя пользователя> – имя пользователя, под чьей учётной записью регистрируется машина с агентом;
- <пароль пользователя> – пароль пользователя в формате base64, под чьей учётной записью регистрируется машина с агентом.

Далее выполните команду в интерфейсе командной строки:

- в ОС Windows:

  ```
  "%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -f <путь к файлу с аргументами>
  ```

- в ОС Linux:

  ```
  sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -f <путь к файлу с аргументами>
  ```

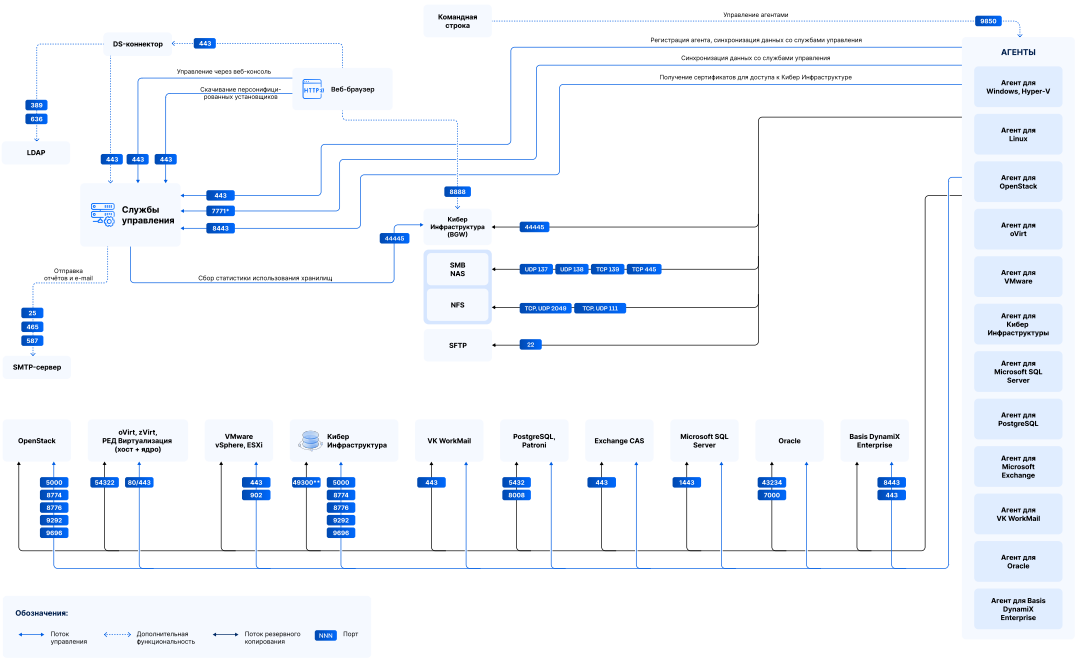
Где:

- <путь к файлу с аргументами> – путь к файлу в формате TXT, содержащему аргументы для команды.

Подробнее о регистрации машин с агентами вручную см. в Руководстве пользователя.

3 Сетевое окружение

Взаимодействие основных компонентов Кибер Бэкапа Облачного показано на схеме.



В целях безопасности рекомендуется закрыть все порты, кроме перечисленных ниже.

В таблицах перечислены порты, необходимые для внешнего подключения к компонентам продукта.

Службы управления

Компонент	Тип	Порт	Источник подключения	Протокол	Описание
Службы управления					
	Входящее	443	Веб-консоль Агенты DS-коннектор	TCP	Веб-консоль сервера управления и шлюз API-запросов. Регистрация компонентов. Обмен информацией с агентами.
	Входящее	8443	Агенты	TCP	Получение сертификатов для доступа к Кибер Инфраструктуре.
	Входящее	7771*	Агенты	TCP	Шлюз ZeroMQ для подключения и обмена информацией с агентами. Основной трафик от

					агентов.
Агент для Windows/Hyper-V					
	Входящее	9850	Запросы через интерфейс командной строки	TCP	Работа с интерфейсом командной строки.
Агент для Linux					
	Входящее	9850	Запросы через интерфейс командной строки	TCP	Работа с интерфейсом командной строки.
Агент для виртуальных машин (VMware, oVirt)					
	Входящее	9850	Запросы через интерфейс командной строки	TCP	Работа с интерфейсом командной строки.
DS-коннектор					
	Входящее	443	Веб-консоль	TCP	Форма входа через LDAP.

Хранилища

Компонент	Тип	Порт	Источник подключения	Протокол	Описание
Кибер Инфраструктура (BGW)					
	Входящее	8888	Веб-браузер администратора	TCP	Веб-консоль управления.
	Входящее	44445	Агенты Сервер управления	TCP	Загрузка и выгрузка резервных копий.
Сетевая папка SMB/NAS					
	Входящее	139	Агенты	TCP	Загрузка и выгрузка резервных копий.
	Входящее	445	Агенты	TCP	Загрузка и выгрузка резервных копий.
	Входящее	137	Агенты	UDP	Загрузка и выгрузка резервных копий.
	Входящее	138	Агенты	UDP	Загрузка и выгрузка резервных копий.
Сетевая папка NFS					
	Входящее	111	Агенты	TCP	Загрузка и выгрузка

				UDP	резервных копий.
	Входящее	2049	Агенты	TCP UDP	Загрузка и выгрузка резервных копий.
Сетевая папка SFTP					
	Входящее	22	Агенты	TCP	Загрузка и выгрузка резервных копий.

Виртуализация

Компонент	Тип	Порт	Источник подключения	Протокол	Описание
VMware vSphere и ESXi					
	Входящее	902	Агент для VMware	TCP	Управляющие команды от агента.
	Входящее	443	Агент для VMware	TCP	Управляющие команды от агента.
oVirt, zVirt Engine, РЕД Виртуализация (хост)					
	Входящее	54322	Агент для oVirt	TCP	Передача агенту данных с дисков ВМ при включенном CBT. Передача ядру гипервизора образа виртуального устройства.
oVirt, zVirt Engine, РЕД Виртуализация (ядро)					
	Входящее	80	Агент для oVirt	TCP	Управляющие команды от агента.
	Входящее	443	Агент для oVirt	TCP	Управляющие команды от агента.
OpenStack					
	Входящее	5000	Агент для OpenStack	TCP	Управляющие команды от агента.
	Входящее	8774	Агент для OpenStack	TCP	Управляющие команды от агента.
	Входящее	8776	Агент для OpenStack	TCP	Управляющие команды от агента.
	Входящее	9292	Агент для OpenStack	TCP	Управляющие команды от агента.

	Входящее	9696	Агент для OpenStack	TCP	Управляющие команды от агента.
Кибер Инфраструктура					
	Входящее	5000	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	8774	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	8776	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	9292	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	9696	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	49300**	Агент для Кибер Инфраструктуры	TCP	Передача данных с дисков виртуальной машины.
Basis DynamiX Enterprise					
	Входящее	443	Агент для Basis DynamiX Enterprise	TCP	Управляющие команды от агента.
	Входящее	8443	Агент для Basis DynamiX Enterprise	TCP	Управляющие команды от агента.

Приложения

Компонент	Тип	Порт	Источник подключения	Протокол	Описание
Microsoft Exchange CAS					
	Входящее	443	Агенты для Microsoft Exchange (почтовые ящики)	TCP	Загрузка и выгрузка содержимого почтовых ящиков.
PostgreSQL и Patroni					
	Входящее	5432	Агент для PostgreSQL	TCP	Выгрузка содержимого экземпляра БД.
	Входящее	8008	Агент для PostgreSQL	TCP	API службы управления кластером PostgreSQL.

Почта VK WorkMail					
	Входящее	443	Агент для VK WorkMail	TCP	Загрузка и выгрузка содержимого почтовых ящиков и хранилища Диск VK WorkSpace.
Microsoft SQL Server					
	Входящее	1443	Агент для Microsoft SQL Server	TCP	Работа с Windows Cluster API (для AAG) или через ODBC.
Oracle					
	Входящее	43234	Агент для Oracle	TCP	Работа с Oracle Restore Tool.
	Входящее	7000	Агент для Oracle	TCP	Работа с RMAN.

* Используются порты из диапазона 7771–7780. Количество открытых портов зависит от количества используемых виртуальных машин со службами управления, для каждой из них должен быть открыт свой порт из указанного диапазона. В минимальной конфигурации используется две виртуальные машины со службами управления, для них должны быть открыты порты 7771 и 7772.

** Используются динамические порты из диапазона 49300–65635.

4 Операции

4.1 Защита резервных копий

Рекомендуется защищать резервные копии паролем. В этом случае для просмотра или восстановления резервной копии потребуется ввести пароль. Защита резервных копий паролем не оказывает влияния на производительность продукта.

Внимание
Если пароль утерян, восстановить защищённые резервные копии будет невозможно.

4.2 Рекомендуемые места хранения резервных копий

По таблице ниже можно выбрать места хранения резервных копий в соответствии с принятой моделью угроз.

Место хранения	Протоколы безопасности	Возможность изоляции тенантов
Облачное хранилище	TLS, сертификат клиент-сервер	Да
Локальное хранилище	-	Нет
Сетевая папка	SMB/CIFS	Нет
NFS-папка	-	Нет
Зона безопасности	-	Нет

4.3 Назначение администраторов

Ограничивайте число администраторов с полным доступом к Кибер Бэкапу Облачному.

4.4 Создание структуры организации

Кибер Бэкап Облачный позволяет создать иерархическую структуру организации. Иерархия в такой структуре обеспечивается за счёт использования различных типов тенантов: **Партнёр**, **Папка**, **Клиент**, **Отдел** (подробнее о типах тенантов см. в Руководстве администратора партнёра).

Учётные записи администраторов и пользователей относятся к какому-либо тенанту. Администратор родительского тенанта может создавать дочерние тенанты и учётные записи администраторов и пользователей (и управлять ими) на своем уровне иерархии, а также в дочерних тенантах. Администратор также может иметь доступ к резервным копиям и другим ресурсам своего и дочерних тенантов, но при этом администратор дочернего тенанта может ограничить доступ к своим дочерним тенантам для администраторов более высокого уровня (подробнее см. в Руководстве администратора партнёра).

Таким образом, каждая учётная запись позволит видеть только те резервные копии и ресурсы, к которым у неё есть право доступа.

5 Практические рекомендации

В этом разделе приведены практические рекомендации по безопасному развёртыванию, настройке и поддержке вашего окружения после интеграции с Кибер Бэкапом Облачным. Они помогут сервис-провайдерам, партнёрам и клиентам повысить безопасность резервного копирования, конечных точек, автоматизации и управления доступом.

5.1 Пользовательский доступ

- Регулярно проверяйте списки учётных записей и API-клиентов всех тенантов и субтенантов Кибер Бэкапа Облачного. Удаляйте или отключайте неиспользуемые или временные учётные записи.
- Используйте ролевую модель управления доступом (RBAC).
- Включите многофакторную аутентификацию (MFA/2FA) для всех тенантов и пользователей.
- Разрешите тенантам доступ только с фиксированного диапазона IP-адресов. Таким образом, администрировать продукт смогут только сотрудники компании, использующие офисную сеть или корпоративный VPN.

5.2 Подключение устройств

- Используйте регистрационные токены.
- Сокращайте сроки действия токенов до минимума.

5.3 Автоматизация

- При использовании открытого API используйте API-клиенты. При этом станет возможна аутентификация без необходимости ввода 2FA-токенов и вы сможете более точно настроить привилегии интерактивного доступа и автоматизации.
- Для автоматизации отправки отчётов используйте служебную учётную запись с правами только на чтение.

5.4 Защита резервных копий

Включайте защиту резервных копий паролем.

5.5 Защита агентов резервного копирования

- Включите функцию «Самозащита».
- Регулярно обновляйте компоненты продукта для устранения уязвимостей.
- Настройте автоматическое обновление агентов.

- Настройте многоуровневую защиту с помощью фильтров электронной почты и систем обнаружения сетевых вторжений.

5.6 Обновления продукта

- Создавайте резервные копии машин с агентами перед установкой обновлений. Описание создания резервной копии и восстановления из неё см. в Руководстве пользователя.
- Сокращайте сроки хранения резервных копий и удаляйте ненужные резервные копии.

5.7 Отчеты и оповещения о событиях

- Отслеживайте в журналах аудита попытки несанкционированного доступа или необычные события.
- Настройте оповещения об аномальных явлениях при работе с резервными копиями.
- Используйте планы мониторинга.
- Настройте автоматические ответные действия.
- Настройте создание и отправку еженедельных отчётов о безопасности сотрудникам.
- После инцидентов сохраняйте системные журналы. Сообщайте об инцидентах ответственным лицам.

5.8 Обучение пользователей

- Пользователям нужно уметь узнавать попытки фишинга.
- Пользователи не должны скачивать данные из недостоверных источников.
- Пользователи должны сообщать о подозрительных случаях ответственным лицам.

Указатель