КИБЕРПРОТЕКТ

# КИБЕР
# Бэкап Облачный

Версия 26.03

Руководство администратора компании

Редакция: 20.04.2026

# Содержание

# Заявление об авторских правах

# 1 О документе

Этот документ предназначен для администраторов клиента, которые планируют использовать облачный портал управления для создания учетных записей пользователя, отделов и квот и управления ими, а также для настройки и контроля доступа к ним, мониторинга использования и операций в облачной организации.

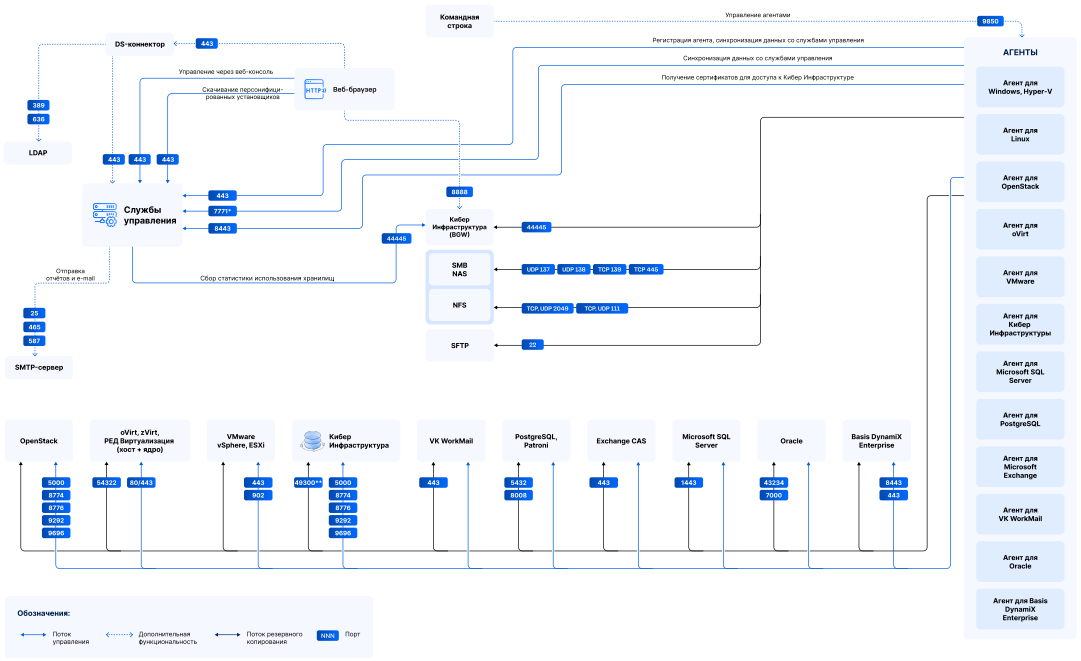
# 2 О портале управления

Портал управления – это веб-интерфейс облачной платформы, на котором предоставляются службы защиты данных.

Хотя для каждой службы есть свой веб-интерфейс (консоль службы), портал управления позволяет администраторам контролировать использование служб, создавать учетные записи пользователей и отделов, формировать отчеты и выполнять другие действия.

## 2.1 Схема взаимодействия компонентов

Взаимодействие основных компонентов продукта показано на схеме.




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<br>Агенты<br>DS-коннектор | TCP | Веб-консоль сервера управления и шлюз API-запросов.<br>Регистрация компонентов.<br>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<br>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<br>UDP | Загрузка и выгрузка резервных копий. |
| | Входящее | 2049 | Агенты | TCP<br>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.

## 2.2 Учетные записи и отделы

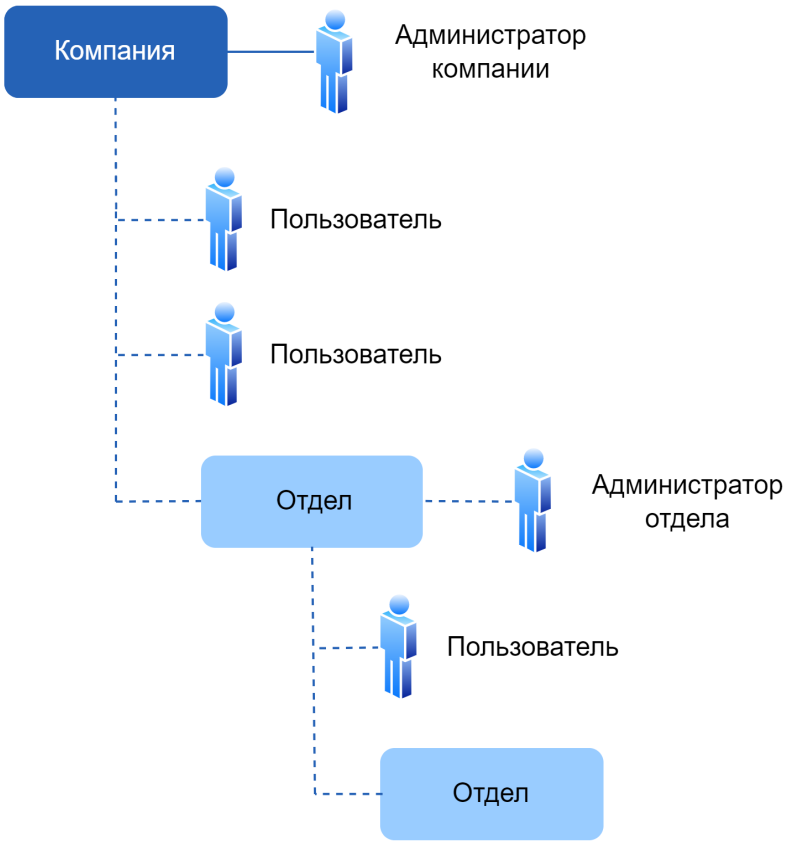
Учетные записи бывают двух типов: администраторы и пользователи.

- **Администраторы** имеют доступ к порталу управления. Они имеют роль администратора во всех службах.
- **Пользователи** не имеют доступа к порталу управления. Их доступ к службам и их роли определяются администратором.

Администраторы могут создавать отделы, которые обычно соответствуют отделам или подразделениям организации. Каждая учетная запись существует на уровне компании или в отделе.

Администратор может управлять отделами, учетными записями администраторов и пользователей на своем уровне иерархии или на уровнях ниже.

На указанной ниже диаграмме показаны три уровня иерархии – компания и два отдела. Дополнительные отделы и учетные записи показаны пунктирной линией.




В таблице ниже приведены операции, которые могут выполнять администраторы и пользователи.

| Операция | Пользователи | Администраторы |
|---|---|---|
| Создание отделов | Нет | Да |
| Создание учетных записей | Нет | Да |
| Загрузка и установка программного обеспечения | Да | Да |
| Использование службы | Да | Да |
| Создание отчетов об использовании сервиса | Нет | Да |

## 2.3 Управление квотами

**Квоты** позволяют установить ограничения на использование службы для тенанта.

На портале управления можно просмотреть квоты на использование службы, выделенные поставщиком услуг для вашей организации. Управление этими квотами для вас недоступно.

Однако вы можете управлять квотами в отношении службы для своих пользователей.

## 2.3.1 Просмотр квот для вашей организации

На портале управления выберите **Обзор** > **Использование**. На открывшейся панели мониторинга показаны квоты, выделенные для вашей организации. Квоты для каждой службы указаны на отдельной вкладке.

### 2.3.1.1 Квоты резервного копирования

Можно указать квоту облачного хранилища данных, квоту локального резервного копирования и максимальное количество машин или серверов, которые может защитить пользователь. Доступны указанные ниже квоты.

#### Квоты для рабочих нагрузок

- **Рабочие станции**;
- **Экземпляры СУБД**;
- **Почтовые ящики**;
- **Серверы**;
- **Виртуальные машины**;
- **Kubernetes (кластеры)**;
- **Серверы веб-хостинга**.

Машина или сервер считаются защищёнными, если к ним применён как минимум один план защиты.

При превышении максимально допустимого количества устройств пользователь не может применить план защиты к дополнительным устройствам.

#### Квоты для хранилища данных

- **Локальное резервное копирование**

  Квота **Локальное резервное копирование** ограничивает общий размер локальных резервных копий, созданных с использованием облачной инфраструктуры. Для этой квоты нельзя задать превышение.
- **Облачные ресурсы**

  Квота **Облачные ресурсы** состоит из квоты для хранилища резервных копий. Квота хранения данных ограничивает общий размер резервных копий, размещённых в облачном хранилище данных. При выходе за пределы значения превышения квоты хранения резервной копии резервное копирование не выполняется.

## 2.3.2 Определение квот для пользователей

**Квоты** позволяют установить ограничения на использование службы для пользователя. Чтобы задать квоты для пользователя, выберите его на вкладке **Пользователи**, затем щелкните значок

карандаша в разделе **Квоты**.

При превышении квоты на адрес электронной почты пользователя отправляется оповещение. Если превышение квоты не задано, квота считается **мягкой**. Это значит, что ограничения по использованию службы Кибер Бэкап Облачный не применяются.

Если для квоты указано превышение, она считается **жесткой**. **Превышение** позволяет пользователю превысить квоту на указанное значение. При превышении, большем максимального, налагаются ограничения на использование соответствующей службы.

Квота с указанным значением "Без ограничений" считается **мягкой**.

**Пример**

**Мягкая квота**. Для количества рабочих станций вы установили квоту, равную 20. Когда количество защищенных рабочих станций пользователя достигнет 20, он получит соответствующее уведомление по электронной почте, но сервис Кибер Бэкап Облачный останется доступным для него.

**Жесткая квота**. Для количества рабочих станций вы установили квоту со значением 20 и превышение со значением 5. Когда количество защищенных рабочих станций пользователя достигнет 20, он получит уведомление по электронной почте; когда же оно достигнет 25, сервис Кибер Бэкап Облачный будет отключен.

### 2.3.2.1 Квоты резервного копирования

Можно указать квоту хранилища резервных копий и максимальное количество машин или серверов, которые может защитить пользователь. Доступны указанные ниже квоты.

#### Квоты для рабочих нагрузок

- **Рабочие станции**;
- **Экземпляры СУБД**;
- **Почтовые ящики**;
- **Серверы**;
- **Виртуальные машины**;
- **Kubernetes (кластеры)**;
- **Серверы веб-хостинга**.

Машина или сервер считаются защищёнными, если к ним применён как минимум один план защиты.

При превышении максимально допустимого количества устройств пользователь не сможет применить план защиты к дополнительным устройствам.

### Квота для хранилища данных

- **Локальное резервное копирование**

  Квота **Локальное резервное копирование** ограничивает общий размер локальных резервных копий, созданных с использованием облачной инфраструктуры. Для этой квоты нельзя задать превышение.
- **Хранилище резервных копий**

  Квота хранения данных ограничивает общий размер резервных копий, размещённых в облачном хранилище данных. При превышении этой квоты резервное копирование не выполняется.

## 2.4 Поддерживаемые веб-браузеры

Веб-интерфейс платформы резервного копирования поддерживает перечисленные ниже браузеры:

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

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

# 3 Пошаговые инструкции

Приведенные ниже пошаговые инструкции помогут выполнить основные операции на портале управления. В них описано, как:

- Активировать учетную запись администратора
- Получение доступа к порталу управления и службам
- Создание отдела
- Создание учетной записи пользователя

## 3.1 Активация учетной записи администратора

Подписавшись на услугу, вы получите сообщение электронной почты с указанной ниже информацией.

- **Ссылка для активации учетной записи**. Щелкните эту ссылку и задайте пароль для учетной записи администратора. Убедитесь, что пароль содержит не менее восьми символов. Запомните имя для входа, которое отображается на странице активации учетной записи.
- **Ссылка на страницу входа**. При этом потребуется указать имя для входа и пароль из предыдущего шага.

## 3.2 Доступ к порталу управления и службам

1. Перейдите на страницу входа на консоль.
2. Введите имя пользователя и щелкните **Далее**.
3. Введите пароль и щелкните **Далее**.
4. Выполните одно из следующих действий:
   - Чтобы войти на портал управления, щелкните **Портал управления**.
   - Чтобы войти в службу, щелкните имя службы.

Время ожидания для портала управления составляет 24 часа для активных сеансов и 1 час для неактивных сеансов.

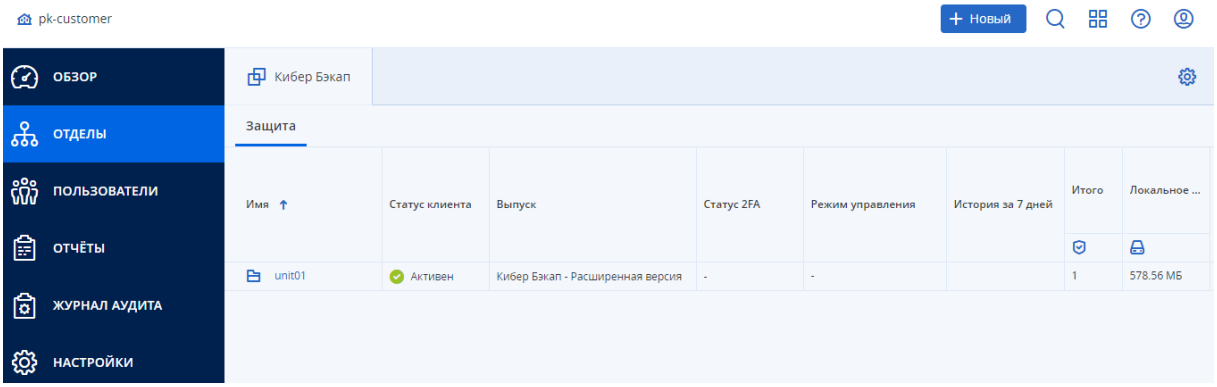
### 3.2.1 Переключение между порталом управления и консолями служб

Для переключения между порталом управления и консолями служб щелкните значок  в верхнем правом углу и выберите пункт **Портал управления** или службу, к которой необходимо перейти.

## 3.3 Навигация на портале управления

Используя портал управления, в каждый данный момент времени вы работаете в компании или в отделе. Это указано в верхнем левом углу.

По умолчанию выбран самый верхний уровень иерархии, который доступен вам. Щелкните имя отдела, чтобы развернуть иерархию. Чтобы вернуться назад на более верхний уровень, щелкните имя в верхнем левом углу.




Во всех частях пользовательского интерфейса будут отображаться только та компания или отдел, в которых вы работаете в данный момент. Пример:

- Кнопка **Создать** позволяет создать отдел или учетную запись пользователя только в этой компании или в этом отделе.
- На вкладке **Отделы** отображаются только те отделы, которые являются непосредственно дочерними для этой компании или отдела.
- На вкладке **Пользователи** отображаются только те учетные записи пользователей, которые существуют в компании или отделе.

## 3.4 Создание отдела

Пропустите этот шаг, если не хотите упорядочивать учетные записи пользователей в отделы.

Если вы планируете создать отделы позже, имейте в виду, что существующие учетные записи невозможно переместить между отделами или между компанией и отделами. Сначала необходимо создать отдел, а затем заполнить его учетными записями.

***Порядок создания отдела***

1. Войдите на портал управления.
2. Перейдите к отделу, в котором необходимо создать новый отдел.
3. В верхнем правом углу последовательно выберите пункты **Новый** > **Отдел.**
4. В поле **Имя** укажите имя нового отдела.

5. [Дополнительно] В поле **Язык** выберите язык по умолчанию для уведомлений, отчетов и программного обеспечения, который будет использоваться в этом отделе.
6. Выполните одно из следующих действий:
   - Чтобы создать администратора отдела, следуйте шагам, описанным в разделе "Создание учетной записи пользователя", начиная с шага 4.

     Администратор отдела может управлять отделами, учетными записями администраторов и пользователей на своем уровне иерархии и на уровнях ниже.
   - Чтобы создать отдел без администратора, щелкните **Готово**. Администраторов и пользователей можно добавить в отдел позже.

Новый созданный отдел появится на вкладке **Отделы**.

Чтобы изменить настройки отдела или указать контактную информацию, выберите отдел на вкладке **Клиенты**, а затем щелкните значок карандаша в том разделе, который нужно изменить.

## 3.5 Создание учетной записи пользователя

Пропустите этот шаг, если не нужно создавать дополнительные учетные записи пользователей.

Возможно, необходимо будет добавить дополнительные учетные записи в следующих случаях:

- Учетные записи администратора компании: чтобы делиться обязанностями по управлению с другими пользователями.
- Учетные записи администратора отдела: для делегирования управления другим пользователям, для которых права доступа будут ограничены рамками соответствующих отделов.
- Учетные записи пользователя: чтобы включить для пользователей только доступ к поднабору служб.

***Порядок создания учетной записи пользователя***

1. Войдите на портал управления.
2. Перейдите к отделу, в котором необходимо создать новую учетную запись пользователя.
3. В верхнем правом углу последовательно выберите пункты **Новый** > **Пользователь**.
4. Укажите приведенную ниже информацию для учетной записи:
   - **Имя для входа**

     **Внимание**
     У каждой учетной записи должно быть уникальное имя входа.

   - **Адрес электронной почты**
   - Необязательно: **Имя**
   - Необязательно: **Фамилия**
   - В поле **Язык** выберите язык, который будет использоваться для уведомлений, отчетов и программного обеспечения для этой учетной записи.

5. Выберите службы, к которым пользователь будет иметь доступ, и роли в каждой службе.
   - Установите флажок **Администратор компании**, чтобы пользователь имел доступ к порталу управления и роль администратора во всех службах.
   - Установите флажок **Портал управления**, чтобы у пользователя был доступ к порталу управления. Выберите роль для службы (подробнее см. в разделе Роли пользователя, доступные для каждой службы).
   - Установите флажок **Защита**, чтобы пользователь мог выполнять настройку резервного копирования и восстановления, а также управлять резервными копиями. Выберите роль для службы (подробнее см. в разделе Роли пользователя, доступные для каждой службы).

     В разделах "Обзор" и "Использование" эта служба называется **Кибер Бэкап**.

   В противном случае пользователь будет иметь роли, которые заданы в выбранных службах.
6. Нажмите кнопку **Создать**.

Созданная учетная запись пользователя появится на вкладке **Пользователи**.

Чтобы изменить настройки пользователя или указать настройки уведомления и квот для пользователя, выберите его на вкладке **Пользователи**, а затем щелкните значок карандаша в том разделе, который нужно изменить.

***Порядок сброса пароля пользователя***

1. На портале управления откройте раздел **Пользователи**.
2. Выберите пользователя, для которого необходимо сбросить пароль, щёлкните значок многоточия  > **Сбросить пароль**.
3. Подтвердите свое действие, щёлкнув **Сбросить**.

После этого пользователь может завершить процесс сброса пароля, следуя инструкциям в полученном электронном письме.

# 3.6 Роли пользователя, доступные для каждой службы

Один пользователь может иметь несколько ролей. При этом для каждой службы он может иметь только одну роль.

Для каждой службы можно определить роль, которая будет назначаться пользователю.

| Сервис | Роль | Описание |
|---|---|---|
| Недоступно | Администратор компании | Эта роль предоставляет права администратора для всех служб.<br><br>Эта роль позволяет получить доступ к корпоративному списку разрешений. |
| Портал управления | Администратор | Эта роль предоставляет доступ к порталу управления, на котором администратор может управлять пользователями во всей организации. |

| | | |
|---|---|---|
| | Администратор с доступом только для чтения | Эта роль предоставляет доступ только для чтения ко всем объектам на портале управления. Такие пользователи могут получить доступ к данным других пользователей организации в режиме "только чтение". |
| Защита | Администратор | Эта роль позволяет настраивать службу Кибер Бэкап и управлять ею для ваших пользователей. |
| | Администратор с доступом только для чтения | Эта роль предоставляет доступ только для чтения ко всем объектам службы Кибер Бэкап. Такие пользователи могут получить доступ к данным других пользователей организации в режиме "только чтение". |
| | Пользователь | Эта роль позволяет использовать службу Кибер Бэкап, но не предоставляет в отношении нее права администратора. Такие пользователи не могут получить доступ к данным других пользователей организации. |

### 3.6.1 Роль администратора с доступом только для чтения

Учетная запись с этой ролью по отношению к веб-консоли Кибер Бэкап Облачный имеет доступ «Только для чтения» и может выполнять следующие действия:

- Собирать диагностические данные (например, системные отчеты).
- Просматривать точки восстановления резервной копии без доступа к содержимому резервной копии и файлам, папкам и электронным письмам.

Администратор с доступом «Только для чтения» не может выполнять следующие действия:

- Запускать или останавливать любые задания.

  Например, администратор с доступом «Только для чтения» не может запускать восстановление и останавливать запущенное резервное копирование.
- Получать доступ к файловой системе на машине-источнике или целевой машине.

  Например, администратор с доступом «Только для чтения» не может просматривать файлы, папки или электронные письма на машине, для которой создана резервная копия.
- Менять любые настройки.

  Например, администратор с доступом «Только для чтения» не может создать план защиты и изменить любую из его настроек.
- Создавать, обновлять или удалять любые данные.

  Например, администратор с доступом «Только для чтения» не может удалять резервные копии.

Все объекты интерфейса пользователя, которые недоступны для администратора с доступом «Только для чтения», скрыты, за исключением настроек по умолчанию для плана защиты. Эти настройки отображаются, но кнопка **Сохранить** неактивна.

Все изменения, которые связаны с учетными записями и ролями, отображаются на вкладке **Действия** с указанной ниже информацией:

- Что изменено,
- Кем внесены изменения,
- Дата и время внесения изменений.

## 3.7 Изменение настроек уведомлений для пользователя

Чтобы изменить настройки уведомлений для пользователя, выберите пользователя на вкладке **Пользователи**, затем щелкните значок карандаша в разделе **Настройки**. Доступны следующие настройки уведомлений:

- **Оповещения о превышении квоты** (включено по умолчанию)
  Оповещения о превышенных квотах.
- **Запланированные отчеты использования**
  Описанные ниже отчеты об использовании, которые отправляются в первый день каждого месяца.
- **Уведомления о сбое**, **Уведомления с предупреждениями** и **Успешные уведомления** (отключено по умолчанию)
  Уведомления о результатах выполнения планов защиты.
- **Ежедневные краткие сведения об активных оповещениях** (включено по умолчанию)
  Ежедневные краткие сведения генерируются на основе списка активных оповещений в консоли службы в момент генерации кратких сведений. Краткие сведения генерируются и отправляются ежедневно в 10:00 и 23:59 (по времени UTC). Время генерации и отправки кратких сведений зависит от рабочей нагрузки центра обработки данных. Если по состоянию на тот момент времени не было никаких активных оповещений, то в кратких сведениях содержится сообщение о том, что все в порядке. В кратких сведениях нет информации о прошлых оповещениях, которые больше не активны. Например, если пользователь отменил оповещение об ошибке резервного копирования или резервное копирование перезапускается и выполняется успешно до формирования кратких сведений, данное оповещение удаляется и не включается в содержимое кратких сведений.

Все уведомления отправляются на адрес электронной почты пользователя.

### 3.7.1 Уведомления, полученные ролью пользователя

Уведомления, которые Кибер Бэкап Облачный отправляет в зависимости от роли пользователя.

| Тип оповещения\роль пользователя | Пользователь | Администратор клиента |
|---|---|---|
| Уведомления для собственных устройств | Да | Да |
| Уведомления для всех устройств в организации | Недоступно | Да |

## 3.8 Отключение и включение учетной записи пользователя

Возможно, необходимо будет отключить учетную запись пользователя, чтобы временно ограничить его доступ к облачной платформе.

***Порядок отключения учетной записи пользователя***

1. На портале управления откройте раздел **Пользователи**.
2. Выберите учетную запись пользователя для отключения, щелкните значок многоточия  > **Отключить**.
3. Подтвердите свое действие, щелкнув **Отключить**.

После этого пользователь не сможет использовать облачную платформу или получать уведомления.

Чтобы включить отключенную учетную запись пользователя, выберите его в списке пользователей, затем щелкните значок многоточия  > **Включить**.

## 3.9 Удаление учётной записи пользователя

Возможно, необходимо будет окончательно удалить учётную запись пользователя, чтобы освободить используемые им ресурсы (например, лицензию). Статистика использования будет обновлена в течение одного дня после удаления. Для учётных записей с большим объёмом данных это может занять больше времени.

Перед удалением учётной записи пользователя её необходимо отключить. Инструкции о том, как это сделать, см. в разделе Отключение и включение учётной записи пользователя.

**Внимание**
Удаление учётной записи пользователя необратимо.

***Порядок удаления учётной записи пользователя***

1. На портале управления откройте раздел **Пользователи**.
2. Выберите отключенную учётную запись пользователя, а затем щёлкните значок многоточия  > **Удалить**.
3. Чтобы подтвердить действие, введите учётные данные и щёлкните **Удалить**.

В результате:

- Учётная запись пользователя будет удалена.
- Все данные этой учётной записи пользователя будут удалены.
- Для всех машин, связанных с этой учётной записью пользователя, будет отменена регистрация.
- Все уведомления, настроенные для этой учётной записи, будут отключены.
- Все планы защиты будут отозваны со всех машин, связанных с этим пользователем.

## 3.10 Передача прав владения учетной записи пользователя

Возможно, необходимо будет передать права владения учетной записи пользователя, если нужно сохранить доступ к данным пользователя с ограниченным доступом.

**Внимание**
Содержимое удаленной учетной записи будет невозможно назначить заново.

***Порядок передачи прав владения учетной записи пользователя***

1. На портале управления откройте раздел **Пользователи**.
2. Выберите учетную запись пользователя, для которой необходимо передать права владения, и щелкните значок карандаша в разделе **Общие сведения**.
3. Замените существующий адрес электронной почты адресом будущего владельца учетной записи, а затем щелкните **Готово**.
4. Для подтверждения действия щелкните **Да**.
5. Новый владелец учетной записи должен подтвердить адрес электронной почты, следуя отправленным инструкциям.
6. Выберите учетную запись пользователя, для которой необходимо передать права владения и щелкните значок многоточия  > **Сбросить пароль**.
7. Подтвердите свое действие, щелкнув **Сбросить**.
8. Новый владелец учетной записи должен сбросить пароль, следуя отправленным инструкциям на его электронную почту.

После этого новый владелец сможет получить доступ к своей ученой записи.

## 3.11 Настройки двухфакторной проверки подлинности

**Двухфакторная проверка подлинности (2FA)** – это тип многофакторной проверки подлинности, обеспечивающий идентификацию пользователей с помощью комбинации двух факторов из следующих трех:

- PIN-кода или пароля, которые известны только пользователю.
- Токена, которым владеет только пользователь.

- Биометрических данных, которые присущи только пользователю.

Двухфакторная проверка подлинности обеспечивает дополнительную защиту от несанкционированного доступа к учетной записи.

Платформа поддерживает проверку подлинности с использованием алгоритма генерации одноразового пароля на основе времени **TOTP (Time-based One-Time Password)**. Если в системе включена проверка подлинности с использованием TOTP, для доступа к системе пользователи кроме обычного пароля должны ввести одноразовый код TOTP. Иными словами, сначала пользователь вводит пароль (первый фактор), а затем – код TOTP (второй фактор). Код TOTP генерируется в приложении проверки подлинности на устройстве второго фактора на основе текущего значения таймера и секретного ключа (QR-код или буквенно-цифровой код), предоставленных платформой.

## 3.11.1 Принципы работы

1. Двухфакторная проверка подлинности включается на уровне организации.
2. Все пользователи в организации должны установить приложение проверки подлинности на устройствах второго фактора. Такими устройствами могут быть мобильные телефоны, ноутбуки, настольные или планшетные ПК. Это приложение будет использоваться для генерации одноразовых кодов TOTP. Рекомендуемые генераторы кодов:
   - Google Authenticator

     Версия для iOS

     Версия для Android
   - Microsoft Authenticator

     Версия для iOS

     Версия для Android

   **Внимание**
   Необходимо убедиться, что время на устройстве с приложением проверки подлинности установлено правильно и соответствует фактическому.
3. Пользователи организации должны выйти из системы и заново войти в нее.
4. После ввода учетных данных пользователям будет предложено настроить двухфакторную проверку подлинности для своих учетных записей.
5. Им необходимо будет отсканировать QR-код в приложении проверки подлинности. Если возникнут проблемы со сканированием QR-кода, пользователи могут вручную ввести в приложение проверки подлинности секретный ключ TOTP, который отображается под QR-кодом.

**Внимание**
Настоятельно рекомендуется сохранить QR-код или секретный ключ TOTP. Для этого можно распечатать QR-код, записать секретный ключ TOTP или воспользоваться приложением, которое поддерживает резервное копирование кодов в облако. При утрате устройства второго фактора секретный ключ TOTP позволит сбросить настройки двухфакторной проверки подлинности.

6. В приложении проверки подлинности генерируется одноразовый код TOTP. Он генерируется заново каждые 30 секунд.
7. После ввода пароля пользователям необходимо ввести код TOTP на экране «Настройки двухфакторной проверки подлинности».
8. В результате выполнения этих процедур будет активирована двухфакторная проверка подлинности для пользователей.

С этого момента при входе в систему после ввода учетных данных у пользователей будет запрашиваться одноразовый код TOTP, сгенерированный в приложении проверки подлинности. При входе в систему пользователи могут пометить используемый браузер как доверенный. После этого при последующих входах в систему с этого браузера код TOTP не будет запрашиваться.

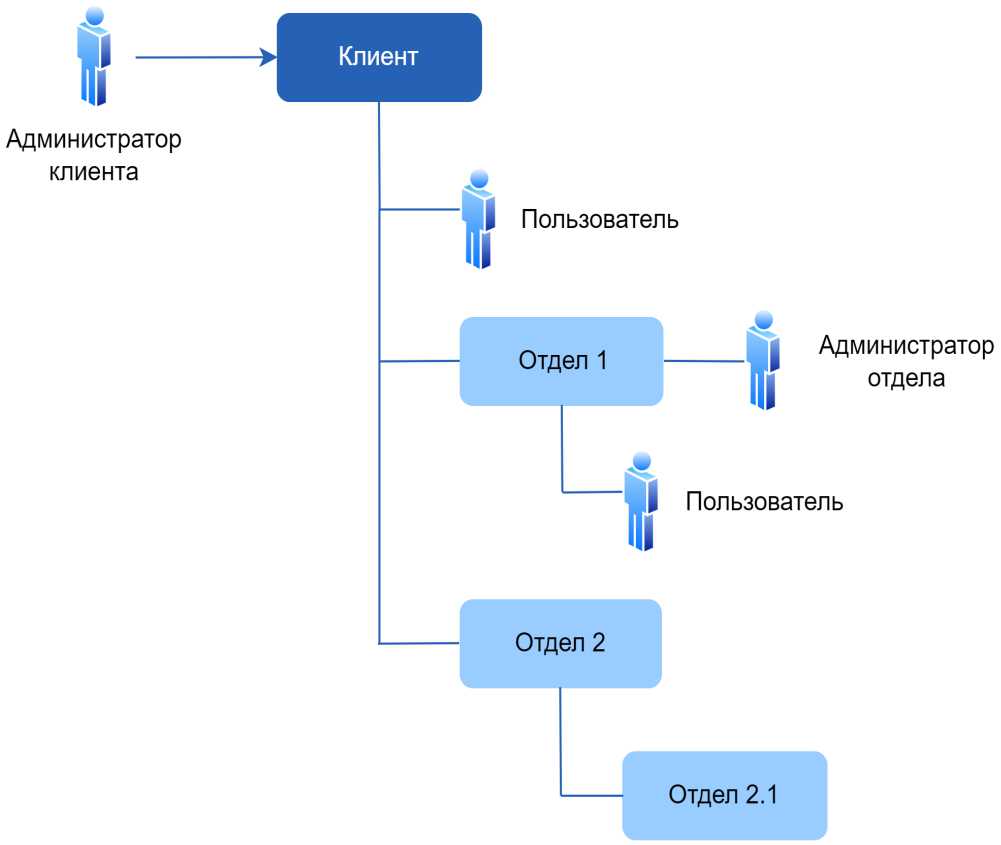
## 3.11.2 Распространение настроек двухфакторной проверки подлинности на уровне тенанта

Двухфакторная проверка подлинности задается на уровне **организации**. Настроить двухфакторную проверку подлинности можно только для собственной организации.

Настройки двухфакторной проверки подлинности распространяются по уровням тенанта следующим образом:

- Отделы автоматически наследуют настройки двухфакторной проверки подлинности от организации их клиента.

**Распространение настроек двухфакторной проверки подлинности с уровня тенанта Клиент**




**Примечание**

1. Невозможно настроить двухфакторную проверку подлинности на уровне отдела.
2. Можно настраивать параметры двухфакторной проверки подлинности для пользователей дочерних организаций (отделов).

## 3.11.3 Настройка двухфакторной проверки подлинности для вашего тенанта

### 3.11.3.1 Порядок включения двухфакторной проверки подлинности для вашего тенанта

1. На портале управления выберите **Настройки** > **Безопасность**.
2. С помощью ползунка включите двухфакторную проверку подлинности. Для подтверждения действия щелкните **Включить**.

Индикатор выполнения показывает количество пользователей, которые настроили двухфакторную проверку подлинности для своих учетных записей. В результате двухфакторная

проверка подлинности будет включена для вашей организации. Теперь все пользователи организации должны настроить двухфакторную проверку подлинности в своих учетных записях. После этого при входе пользователей в систему кроме учетных данных у них будет запрашиваться код TOTP.

На вкладке **Пользователи** появится столбец **Статус 2FA**. Данные этого столбца позволяют узнать, какие пользователи настроили двухфакторную проверку подлинности для своих учетных записей.

### 3.11.3.2 Порядок отключения двухфакторной проверки подлинности для вашего тенанта

1. На портале управления выберите **Настройки** > **Безопасность**.
2. С помощью ползунка отключите двухфакторную проверку подлинности. Для подтверждения действия щелкните **Отключить**.
3. (Если хотя бы один пользователь настроил двухфакторную проверку подлинности в организации.) Введите код TOTP из приложения проверки подлинности на мобильном устройстве.

Двухфакторная проверка подлинности для вашей организации будет отключена, будут удалены все секретные коды, а также информация о доверенных браузерах. Всем пользователям для входа в систему понадобятся только имя входа и пароль. На вкладке **Пользователи** будет скрыт столбец **Статус 2FA**.

## 3.11.4 Управление двухфакторной проверкой подлинности для пользователей

На портале управления на вкладке **Пользователи** можно отслеживать настройки двухфакторной проверки подлинности для всех пользователей и сбрасывать их.

### 3.11.4.1 Мониторинг

На портале управления на вкладке **Пользователи** можно просмотреть список всех пользователей в организации. В столбце **Статус 2FA** указано, настроена ли двухфакторная проверка подлинности для пользователя.

### 3.11.4.2 Порядок сброса двухфакторной проверки подлинности для пользователя

1. На портале управления на вкладке **Пользователи** найдите пользователя, для которого необходимо изменить настройки, а затем щелкните значок многоточия .
2. Щелкните **Сбросить двухфакторную проверку подлинности**.
3. Введите код TOTP, сгенерированный в приложении проверки подлинности на устройстве второго фактора, а затем щелкните **Сбросить**.

После этого пользователь сможет снова настроить двухфакторную проверку подлинности.

### 3.11.4.3 Порядок сброса доверенных браузеров для пользователя

1. На портале управления на вкладке **Пользователи** найдите пользователя, для которого необходимо изменить настройки, а затем щелкните значок многоточия  .
2. Щелкните **Сбросить все доверенные браузеры**.
3. Введите код TOTP, сгенерированный в приложении проверки подлинности на устройстве второго фактора, а затем щелкните **Сбросить**.

После сброса всех доверенных браузеров для пользователя при следующем входе ему необходимо будет указать код TOTP.

Пользователи могут сбрасывать информацию обо всех доверенных браузерах и параметры двухфакторной проверки подлинности самостоятельно. Это можно сделать при входе в систему, нажав соответствующую ссылку и введя код TOTP для подтверждения операции.

### 3.11.4.4 Порядок отключения двухфакторной проверки подлинности для пользователя

Вам может понадобиться отключить двухфакторную проверку подлинности для отдельного пользователя, не отключая ее для всех остальных. Такая необходимость может возникнуть, если данный пользователь используется для доступа к API.

**Внимание**
Не переводите обычных пользователей в категорию "Сервисная учётная запись" с тем, чтобы отключить двухфакторную проверку подлинности. В противном случае у пользователей могут возникнуть проблемы при входе в систему.

1. На портале управления на вкладке **Пользователи** найдите пользователя, для которого необходимо изменить настройки, а затем щелкните значок многоточия  .
2. Щелкните **Отметить как сервисную учетную запись**. В результате пользователь получит особый статус двухфакторной проверки подлинности, который называется **Учетная запись службы**.
3. [Если у тенанта есть хотя бы один пользователь, который настроил двухфакторную проверку подлинности] Для подтверждения отключения введите код TOTP, сгенерированный в приложении проверки подлинности на устройстве второго фактора.

### 3.11.4.5 Порядок включения двухфакторной проверки подлинности для пользователя

Вам может понадобиться включить двухфакторную проверку подлинности для пользователя, для которого она была отключена ранее.

1. На портале управления на вкладке **Пользователи** найдите пользователя, для которого необходимо изменить настройки, а затем щелкните значок многоточия  .
2. Щелкните **Отметить как обычную учетную запись**. В результате пользователю необходимо будет настроить двухфакторную проверку подлинности или указывать код TOTP при входе в систему.

## 3.11.5 Сброс двухфакторной проверки подлинности при утрате устройства второго фактора

Для сброса доступа к учетной записи при утрате устройства второго фактора можно применить один из описанных ниже подходов.

- Восстановите секретный ключ TOTP (QR-код или буквенно-цифровой код) с резервной копии. На другом устройстве второго фактора добавьте сохраненный секретный ключ TOTP в приложение проверки подлинности, установленное на этом устройстве.
- Обратитесь к администратору с просьбой сбросить настройки двухфакторной проверки подлинности для вашей учетной записи.

## 3.11.6 Защита от атак методом перебора

В ходе атаки методом перебора злоумышленник пытается получить доступ к системе, многократно отправляя пароли в надежде подобрать верную последовательность.

Защита от атак методом перебора основана на cookie-файлах устройства.

Параметры защиты от таких атак предварительно заданы на платформе.

| Параметр | Ввод пароля | Ввод кода TOTP |
|---|---|---|
| Максимальное число попыток | 10 | 5 |
| Период ограничения числа попыток (после которого ограничение сбрасывается) | 15 мин (900 с) | 15 мин (900 с) |
| Применение блокировки | Максимальное число попыток + 1 (11-я попытка) | Максимальное число попыток |
| Период блокировки | 5 мин (300 с) | 5 мин (300 с) |

Если вы включили двухфакторную проверку подлинности, cookie-файл устройства выдается клиенту (браузеру) только после удачной проверки подлинности с использованием двух факторов (пароль и код TOTP).

Если используется доверенный браузер, cookie-файл устройства выдается после удачной проверки подлинности с использованием одного фактора (пароля).

Попытки ввода кода TOTP регистрируются для каждого пользователя, а не для устройства. Это означает, что, если пользователь попытается ввести код TOTP с других устройств, он все равно будет заблокирован.

## 3.12 Настройка доступа для пользователей домена

При наличии службы каталогов и домена можно предоставить доступ к порталу управления и консолям служб пользователям этого домена. Поддерживаются следующие службы каталогов: Active Directory, Samba DC и основанная на ней РЕД АДМ, FreeIPA и основанная на ней ALD Pro.

Для настройки доступа необходимо выполнить следующие шаги:

1. Установить и настроить LDAP-коннектор. (см. раздел "Добавление домена" (стр. 30)).

   Посредством LDAP-коннектора Кибер Бэкап Облачный получает из службы каталогов список пользователей/групп домена, а также сведения о них: идентификатор пользователя/группы в домене, имя пользователя для входа (login name), имя пользователя/группы для отображения (display name), адрес электронной почты пользователя, состояние пользователя в домене (включен/отключен).
2. Выбрать пользователей/группы домена и указать их роли в Кибер Бэкап Облачный (см. раздел "Добавление пользователей и групп домена" (стр. 41)).

   При выборе пользователя/группы домена и указании роли в LDAP-коннекторе создается правило синхронизации, состоящее из идентификатора пользователя/группы в домене и идентификатора указанной роли.
3. Выполнить синхронизацию со службой каталогов вручную или дождаться выполнения автоматической синхронизации (см. раздел "Управление доменом" (стр. 45)).

   При синхронизации Кибер Бэкап Облачный через LDAP-коннектор получает сведения о пользователях/группах, указанных в правилах синхронизации, создает выбранных пользователей и назначает им указанные роли (для каждого пользователя, входящего в выбранную группу домена, в Кибер Бэкап Облачный создается отдельный пользователь и ему назначается роль, указанная для группы).

   При последующих запусках синхронизации статус пользователя в Кибер Бэкап Облачный устанавливается в соответствии со статусом пользователя в домене. Например, если пользователь был отключен в домене, то пользователь в Кибер Бэкап Облачный также будет отключен. Если пользователь удален из домена, то при синхронизации соответствующий пользователь в Кибер Бэкап Облачный будет отключен.

После выполнения этих шагов пользователи домена смогут входить в веб-интерфейс Кибер Бэкап Облачный со своими доменными учетными данными и выполнять операции согласно назначенным им ролям.

### 3.12.1 Добавление домена

Добавьте домен с пользователями и группами пользователей, которым планируется предоставлять доступ к порталу управления и службам. Для добавления домена необходимо последовательно выполнить инструкции, приведенные в подразделах ниже.

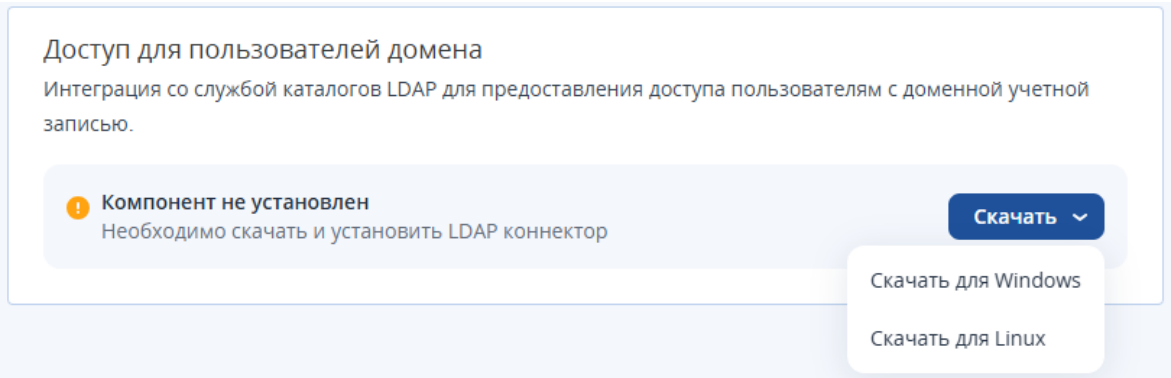
## 3.12.1.1 Установка, регистрация и удаление LDAP-коннектора

### Установка LDAP-коннектора

LDAP-коннектор может быть установлен как из общего дистрибутива Кибер Бэкапа Облачного при установке агента резервного копирования (подробнее см. в Руководстве пользователя), так и из отдельного дистрибутива для LDAP-коннектора.

Для установки LDAP-коннектора из отдельного дистрибутива выполните следующие шаги:

1. На портале управления перейдите в раздел **Настройки** > **Управление доступом**.
2. Нажмите **Скачать** и выберите установщик для используемой операционной системы, щёлкнув **Скачать для Windows** или **Скачать для Linux**. В результате файл установщика LDAP-коннектора будет сохранён на текущей машине.




3. Разместите установщик LDAP-коннектора на сервере под управлением ОС Linux или ОС Windows, с которого есть доступ по сети к порталу управления и службе каталогов и на котором не установлено никаких агентов.
4. Запустите установщик LDAP-коннектора.
5. Укажите учётные данные администратора тенанта, для которого выполняется установка.
6. Дождитесь окончания процесса установки.

### Регистрация машины с LDAP-коннектором

Машина с LDAP-коннектором может быть зарегистрирована в Кибер Бэкапе Облачном одним из следующих способов:

- автоматически при установке LDAP-коннектора;
- вручную с использованием интерфейса командной строки.

Регистрация машины с установленным LDAP-коннектором с использованием интерфейса командной строки может быть выполнена двумя способами:

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

  Для регистрации машины с помощью маркера регистрации на машине с LDAP-коннектором выполните следующую команду в интерфейсе командной строки:

- в ОС Windows:

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

- в ОС Linux:

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

В этих командах:

- <адрес службы> — адрес службы Кибер Бэкапа Облачного, в которой должна быть зарегистрирована машина с LDAP-коннектором;
- <маркер регистрации> — маркер регистрации.

- **По имени пользователя и паролю**

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

  - в ОС Windows:

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

  - в ОС Linux:

    ```
    sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s ldap -t cloud -a <адрес службы> -u <имя пользователя> -p <пароль пользователя>
    ```

  В этих командах:

  - <адрес службы> — адрес службы Кибер Бэкапа Облачного, в которой должна быть зарегистрирована машина с LDAP-коннектором;
  - <имя пользователя> — имя пользователя, под чьей учётной записью регистрируется машина с LDAP-коннектором;
  - <пароль пользователя> — пароль пользователя, под чьей учётной записью регистрируется машина с LDAP-коннектором.

Подробнее о регистрации машин вручную см. в Руководстве пользователя.

## Удаление LDAP-коннектора

### В ОС Windows

Для удаления LDAP-коннектора на машине с ОС Windows выполните следующие шаги:

1. Войдите в ОС с использованием данных учётной записи с правами администратора.
2. Откройте **Панель управления** и выберите **Программы и компоненты** > **LDAP Connector** > **Удалить**.

3. [Необязательно] В открывшемся окне программы удаления установите флажок **Удалить журналы и параметры конфигурации**.
4. Щёлкните **Удалить**.

### В ОС Linux

Для удаления LDAP-коннектора на машине с ОС Linux выполните следующие шаги:

1. От имени привилегированного пользователя выполните команду:
   - /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall (если LDAP-коннектор был установлен из общего дистрибутива Кибер Бэкапа Облачного);
   - /usr/lib/Acronis/LDAPConnectorFeature/uninstall/uninstall (если LDAP-коннектор был установлен из отдельного дистрибутива для LDAP-коннектора).
2. [Необязательно] В открывшемся окне программы удаления установите флажок **Очистить все следы продукта (удалить журналы продукта и параметры конфигурации)**.
3. Подтвердите операцию.

## 3.12.1.2 Настройка доступа к сервису аутентификации доменных пользователей

Настройте доступ к сервису аутентификации доменных пользователей по протоколу HTTPS (использование протокола HTTP допускается только для отладочных целей).

Сервис аутентификации входит в состав LDAP-коннектора. Он предоставляет форму ввода пароля доменной учётной записи и обеспечивает аутентификацию в службе каталогов. При указании имени доменной учётной записи на странице входа происходит перенаправление веб-браузера пользователя на страницу с формой.

### Настройка доступа по протоколу HTTPS через обратный прокси-сервер

Для настройки доступа к сервису аутентификации по протоколу HTTPS выполните следующие шаги:

1. Установите обратный прокси-сервер (например, nginx) на ту же машину, что и LDAP-коннектор, и настройте проксирование так, чтобы он принимал запросы по адресу https://<DNS_имя_прокси_сервера> и передавал их по адресу http://<IP_адрес_сервера_с_LDAP_коннектором>:9001 (9001 — порт сервиса аутентификации по умолчанию).

   При необходимости для установки LDAP-коннектора можно использовать отдельную машину. В этом случае необходимо настроить защищённое соединение между сервисом аутентификации доменных пользователей и прокси-сервером.

**Внимание**

Использование незащищённого соединения может привести к перехвату сетевого трафика, включая данные службы каталогов Active Directory и ключи аутентификации. Для защиты конфиденциальной информации необходимо обеспечить использование протокола TLS на всех участках взаимодействия компонентов системы, а также SSL-сертификата, выпущенного доверенным удостоверяющим центром.

Для получения сведений об установке и настройке прокси-сервера обратитесь к документации используемой ОС и официальной документации прокси-сервера.

Пример конфигурации nginx для обратного проксирования

```
server {
    listen 443 ssl http2 default_server;
    listen [::]:443 ssl http2 default_server;
    server_name _;

    # SSL-сертификаты (замените пути)
    ssl_certificate /etc/ssl/certs/certificate.crt;
    ssl_certificate_key /etc/ssl/private/certificate-key.key;

    # Настройки SSL (рекомендуемые параметры)
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384';
    ssl_prefer_server_ciphers on;
    ssl_session_cache shared:SSL:10m;
    ssl_session_timeout 10m;
    ssl_session_tickets off;
    ssl_stapling on;
    ssl_stapling_verify on;

    # Проксирование всего трафика
    location / {
        proxy_pass http://localhost:9001;  # Основное проксирование
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_cache_bypass $http_upgrade;
    }

    # Отключение журналирования для favicon.ico и robots.txt
    location = /favicon.ico { access_log off; log_not_found off; }
    location = /robots.txt  { access_log off; log_not_found off; }
}
```

2. Настройте преобразование DNS-имени прокси-сервера в его IP-адрес, чтобы клиентские устройства могли подключаться к прокси-серверу по DNS-имени.
3. На прокси-сервере установите SSL-сертификат, который заверен доверенным удостоверяющим центром и в котором указано DNS-имя прокси-сервера.
4. На сервере с LDAP-коннектором в конфигурационном файле /opt/acronis/etc/auth-connector/auth-connector.yaml (для ОС Linux) или C:\ProgramData\Acronis\Agent\etc\auth-connector\auth-connector.yaml (для ОС Windows) замените значение переменной host с http://localhost:9001 на https://<DNS_имя_прокси_сервера>.

   **Примечание**
   Рекомендуется ограничить доступ к сервису аутентификации, указав IP-адрес 127.0.0.1 (localhost) для переменной http.host.

   Например:

   ```
   <...>
   http:
    port: 9001
    host: 127.0.0.1
    <...>

   host: https://auth.company.ru

   swagger: true
   <...>
   ```

5. После сохранения изменений в файле перезапустите службу aakore:

   ```
   systemctl restart aakore
   ```

## Настройка доступа по протоколу HTTP

**Внимание**
Использование протокола HTTP и самоподписанных SSL-сертификатов возможно только на этапе отладки в тестовом окружении. Для обеспечения безопасности передаваемых данных в рабочей среде требуется настройка HTTPS с сертификатом, выпущенным доверенным удостоверяющим центром.

Для настройки доступа к сервису аутентификации по протоколу HTTP выполните следующие шаги:

1. На сервере с LDAP-коннектором в конфигурационном файле /opt/acronis/etc/auth-connector/auth-connector.yaml (для ОС Linux) или C:\ProgramData\Acronis\Agent\etc\auth-connector\auth-connector.yaml (для ОС Windows) замените значение переменной host с http://localhost:9001 на http://<IP_адрес_сервера_с_LDAP_коннектором>:9001. Например:

```
<...>
http:
  port: 9001
  host: 0.0.0.0
  <...>

host: http://192.168.10.20:9001

swagger: true
<...>
```

2. После сохранения изменений в файле перезапустите службу aakore:

```
systemctl restart aakore
```

### 3.12.1.3 Добавление SSL-сертификата корневого удостоверяющего центра

**Внимание**
Использование самоподписанных SSL-сертификатов возможно только на этапе отладки в тестовом окружении. Для обеспечения безопасности передаваемых данных в рабочей среде требуется настройка HTTPS с сертификатом, выпущенным доверенным удостоверяющим центром.

Добавьте SSL-сертификат корневого удостоверяющего центра (УЦ), которым заверен SSL-сертификат службы каталогов, в хранилище сертификатов доверенных УЦ сервера с LDAP-коннектором.

1. Подготовьте файл сертификата корневого УЦ.

   **Пример для Samba DC**

   a. Войдите на сервер, который настроен в качестве контроллера домена.
   b. Получите путь к файлу сертификата, просмотрев значение параметра tls cafile в конфигурационном файле smb.conf.
   c. Скопируйте файл сертификата на сервер, на котором установлен LDAP-коннектор.

   **Пример для FreeIPA**

   a. Войдите на сервер, который настроен в качестве контроллера домена.
   b. Скопируйте файл сертификата /etc/ipa/ca.crt на сервер, на котором установлен LDAP-коннектор.

   **Пример для Active Directory**

   a. Войдите на сервер, на котором установлены службы сертификатов Active Directory (AD CS), и откройте оснастку certsrv.msc.
   b. Щёлкните правой кнопкой мыши по имени УЦ и выберите пункт меню **Свойства**.
   c. Перейдите на вкладку **Общие** и нажмите **Просмотреть сертификат**.

d. В открывшемся окне перейдите на вкладку **Состав** и нажмите **Копировать в файл**. Запустится мастер экспорта сертификата.

e. Выберите **Формат X.509 (.CER)** и экспортируйте сертификат.

f. Скопируйте файл сертификата на сервер, на котором установлен LDAP-коннектор.

2. Добавьте сертификат корневого УЦ в хранилище сертификатов сервера, на котором установлен LDAP-коннектор.

**Пример для Astra Linux 1.7 (SE) / 2.12 (CE)**

a. Убедитесь, что сертификат сохранён в формате PEM. Преобразуйте его в этот формат при необходимости.

b. В папке /usr/share/ca-certificates создайте папку my-company и скопируйте в нее файл сертификата:

```
sudo mkdir -p /usr/share/ca-certificates/my-company
sudo cp /home/my-user/ca.crt /usr/share/ca-certificates/my-company/
```

c. Обновите конфигурацию хранилища сертификатов, добавив путь к файлу сертификата относительно папки /usr/share/ca-certificates:

```
echo "my-company/ca.crt" | sudo tee -a /etc/ca-certificates.conf
```

d. Обновите хранилище сертификатов, выполнив команду:

```
sudo update-ca-certificates
```

При успешном выполнении команды появится строка 1 added, 0 removed.

**Пример для РЕД ОС**

a. Убедитесь, что сертификат сохранён в формате PEM. Преобразуйте его в этот формат при необходимости.

b. Скопируйте файл сертификата в папку /etc/pki/ca-trust/source/anchors:

```
sudo cp /home/my-user/ca.crt /etc/pki/ca-trust/source/anchors/
```

c. Обновите хранилище сертификатов, выполнив команду:

```
sudo update-ca-trust
```

d. Проверьте, что сертификат добавлен в хранилище:

```
trust list | grep -A5 "My Root CA"
```

**Пример для ALT Linux**

a. Убедитесь, что сертификат сохранён в формате PEM. Преобразуйте его в этот формат при необходимости.

b. Скопируйте файл сертификата в папку /usr/local/share/ca-certificates:

```
sudo cp /home/my-user/ca.crt /usr/local/share/ca-certificates/
```

c. Обновите хранилище сертификатов, выполнив команду:

```
sudo update-ca-certificates
```

При успешном выполнении команды появится строка 1 added, 0 removed.

**Пример для Windows**

a. Нажмите клавиши Win+R, введите certlm.msc и нажмите Enter. Откроется оснастка **Сертификаты — локальный компьютер**.

b. В дереве слева последовательно выберите **Доверенные корневые центры сертификации** > **Сертификаты**.

c. Щёлкните правой кнопкой мыши на папке **Сертификаты** и последовательно выберите пункты меню **Все задачи** > **Импорт**. Запустится **Мастер импорта сертификатов**.

d. Нажмите **Далее** для продолжения.

e. Укажите путь к файлу сертификата и нажмите **Далее**.

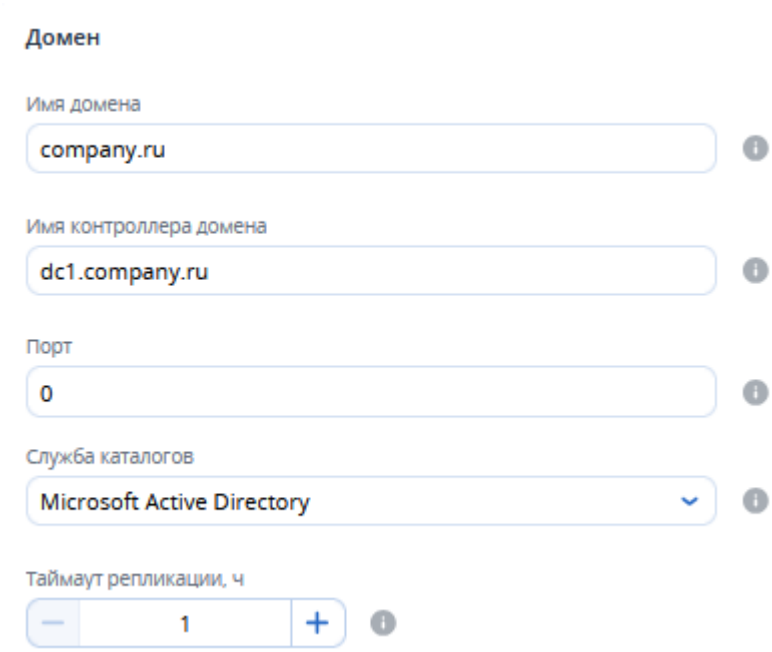
f. Убедитесь, что выбран вариант **Поместить все сертификаты в следующее хранилище** и что в поле **Хранилище сертификатов** указано значение **Доверенные корневые центры сертификации**, затем нажмите **Далее**.

g. Нажмите **Готово** для завершения импорта. Сертификат появится в списке.

### 3.12.1.4 Настройка подключения к службе каталогов домена

Настройте подключение к службе каталогов домена, выполнив следующие шаги:

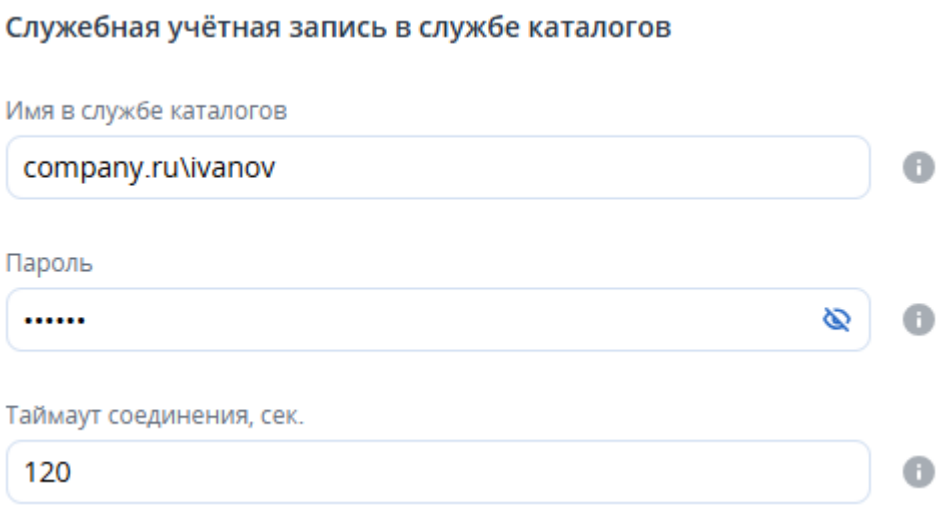
1. На портале управления перейдите в раздел **Настройки** > **Управление доступом**.
2. В области **Доступ для пользователей домена** щёлкните **Настроить**. В результате откроется форма ввода параметров домена, служебной учётной записи в службе каталогов и сервиса аутентификации.
3. В области **Домен** укажите следующие параметры:
   - **Имя домена**. Введите полное имя домена (FQDN), например: company.ru.
   - **Имя контроллера домена**. Укажите полное DNS-имя или IP-адрес сервера, на котором работает контроллер домена, например: dc1.company.ru или 192.168.1.10.
   - **Порт**. Укажите порт подключения к службе каталогов. Для обычного подключения порт по умолчанию — 389. Для подключения, защищённого посредством протокола SSL, порт по умолчанию — 636. Если указать значение 0, то будет автоматически использован порт по умолчанию в зависимости от типа подключения.
   - **Служба каталогов**. В выпадающем списке выберите **Active Directory**, **FreeIPA** или **Samba DC**. Для ALD Pro выберите **FreeIPA**, для РЕД АДМ — **Samba DC**.
   - [Необязательно] **Таймаут репликации, ч**. Укажите временной промежуток (в часах), служащий периодом выполнения репликации (синхронизации) данных из службы каталогов. Максимальное значение и значение по умолчанию — 24.




4. В области **Служебная учётная запись в службе каталогов** укажите следующие параметры:
   - **Имя в службе каталогов**. Введите имя учётной записи пользователя (с учётом регистра) для подключения к службе каталогов:
     - для FreeIPA или ALD Pro укажите имя в DN-формате, например: uid=ivanivanov,cn=users,cn=accounts,dc=company,dc=ru;
     - для Active Directory, РЕД АДМ или Samba DC укажите имя в формате COMPANYRU\ivanivanov или ivanivanov@company.ru, где COMPANYRU – NetBIOS-имя домена службы каталогов, company.ru – полное DNS-имя домена службы каталогов, ivanivanov – имя учётной записи пользователя домена службы каталогов.

     **Примечание**
     Пользователь должен обладать правами на чтение объектов каталога и их свойств.

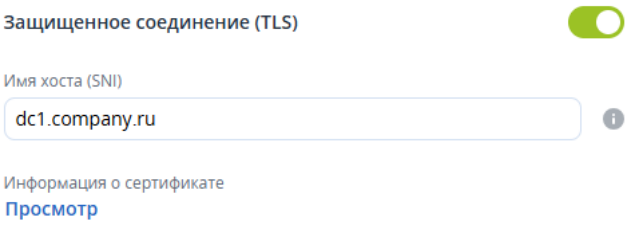
   - **Пароль**. Введите пароль от учётной записи для подключения к службе каталогов.
   - [Необязательно] **Таймаут соединения, с**. Введите значение промежутка времени в секундах, в течение которого будет выполняться попытка подключения. Максимальное значение – 600, значение по умолчанию – 120.




5. В области **Защищённое соединение (TLS)** укажите следующие параметры:
   - **Защищённое соединение (TLS)**. Переведите переключатель в положение **Включено**, если необходимо использовать защищённое подключение к домену (для этого также потребуется настроить SSL-сертификат).

     **Внимание**
     Использование незащищённого соединения может привести к перехвату сетевого трафика, включая данные службы каталогов Active Directory и ключи аутентификации. Для защиты конфиденциальной информации необходимо обеспечить использование протокола TLS на всех участках взаимодействия компонентов системы, а также SSL-сертификата, выпущенного доверенным удостоверяющим центром.

   - [Если включено защищённое соединение (TLS)] **Имя хоста (SNI)**. Введите имя машины, указанное в сертификате, с которым осуществляется TLS-соединение.
     Для просмотра информации о сертификате щёлкните **Просмотр**.

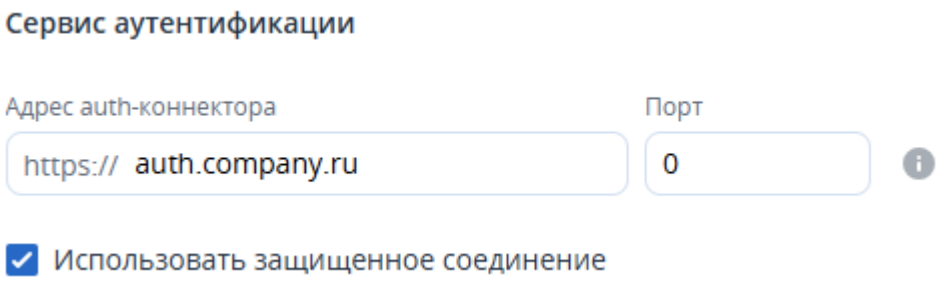



6. В области **Сервис аутентификации** укажите следующие параметры:
   - **Адрес auth-коннектора**. Укажите полное DNS-имя или IP-адрес машины, на которой работает сервис аутентификации, например: auth.company.ru или 192.168.10.11.
   - **Порт**. Укажите порт подключения к сервису аутентификации. Для обычного подключения с использованием протокола HTTP порт по умолчанию – 80. Для подключения с использованием протокола HTTPS порт по умолчанию – 443. Если указать значение 0, то будет автоматически использован порт по умолчанию в зависимости от типа подключения.

**Внимание**
Использование протокола HTTP и самоподписанных SSL-сертификатов возможно только на этапе отладки в тестовом окружении. Для обеспечения безопасности передаваемых данных в рабочей среде требуется настройка HTTPS с сертификатом, выпущенным доверенным удостоверяющим центром.

- **Использовать защищённое соединение**. Установите этот флажок, если необходимо использовать защищённое соединение с сервисом аутентификации.

**Внимание**
Использование незащищённого соединения может привести к перехвату сетевого трафика, включая данные службы каталогов Active Directory и ключи аутентификации. Для защиты конфиденциальной информации необходимо обеспечить использование протокола TLS на всех участках взаимодействия компонентов системы, а также SSL-сертификата, выпущенного доверенным удостоверяющим центром.




7. По окончании ввода данных нажмите **Сохранить**.

После настройки подключения к службе каталогов можно добавлять пользователей и группы домена и назначать им роли (см. раздел "Добавление пользователей и групп домена" (стр. 41)).

## 3.12.2 Добавление пользователей и групп домена

Для добавления пользователя или группы домена выполните следующие действия:

1. Войдите на портал управления.
2. Перейдите к отделу, для которого необходимо добавить пользователей/группы из домена.

**Примечание**
Домен должен быть заранее добавлен к этому отделу или вышестоящему тенанту (см. раздел "Добавление домена" (стр. 30)).

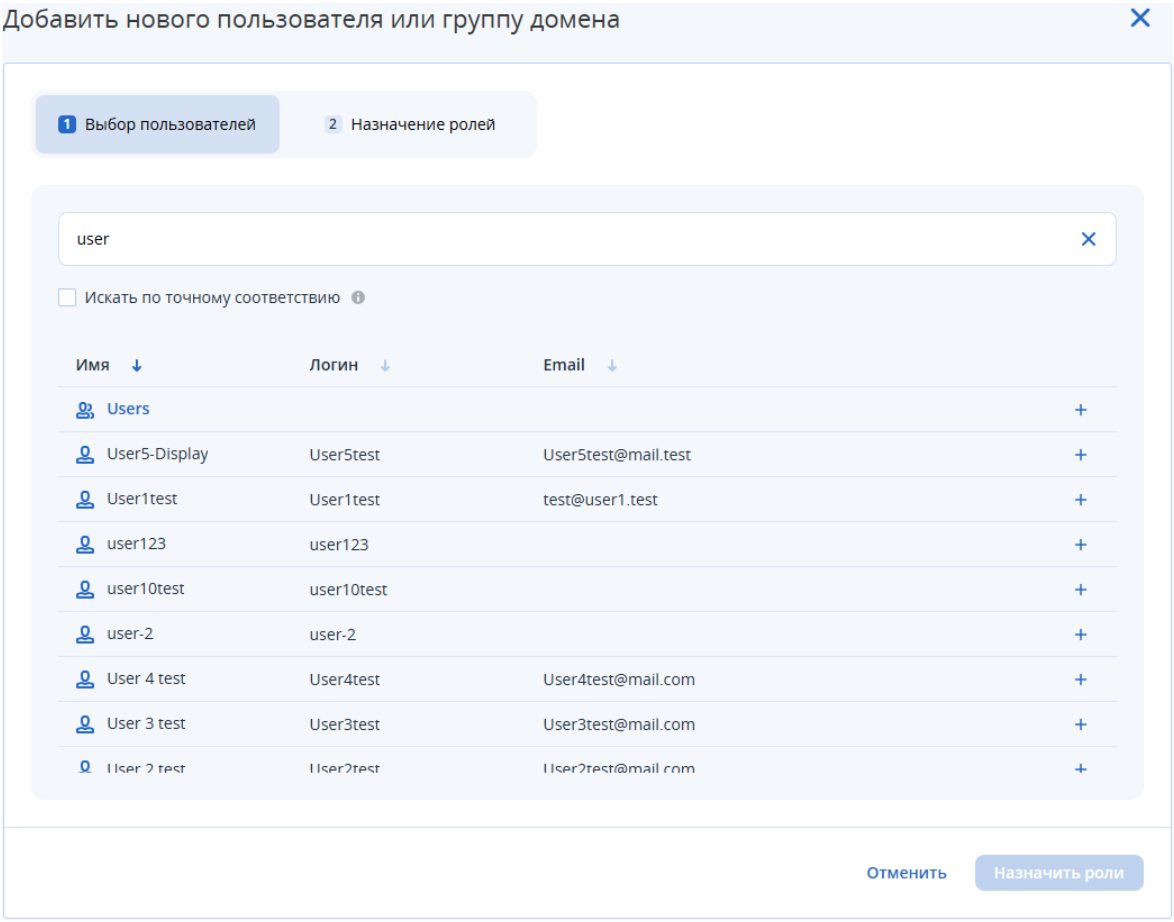
3. В верхнем правом углу окна программы щёлкните **Новый** > **Пользователь домена**. В результате откроется окно **Добавить нового пользователя или группу домена**.
4. Выполните поиск пользователей или групп домена, введя текст в строку поиска. Отображаемые результаты будут соответствовать введённой комбинации символов. При

необходимости установите флажок **Искать по точному соответствию**.

Для сортировки отображаемых данных в колонках **Имя**, **Логин**, **Email** щёлкните значок стрелки в соответствующей колонке.

В строке пользователя домена отображается значок , в строке группы домена – значок .

Для просмотра состава группы домена щёлкните его имя.




5. Выберите пользователей и группы домена, щёлкнув значок . В результате выбранные пользователи и группы домена будут отображены в списке **Выбрано для добавления** в правой области окна. При необходимости пользователей и группы домена можно удалить из этого списка.

**Примечание**

Из больших доменов (более 10 000 пользователей) или из доменов с группами высокого уровня вложенности (третьего уровня и выше) рекомендуется добавлять пользователей по одному или в составе группы, в которую входят все необходимые пользователи.

6. Щёлкните **Назначить роли**.
7. Выберите службы, к которым пользователям будет предоставлен доступ, и их роли в каждой службе.
   - Установите флажок **Администратор компании**, чтобы пользователь имел доступ к порталу управления и роль администратора во всех службах.

- Установите флажок **Портал управления**, чтобы у пользователя был доступ к порталу управления. Выберите роль для службы (подробнее см. в разделе Роли пользователя, доступные для каждой службы).
- Установите флажок **Защита**, чтобы пользователь мог выполнять настройку резервного копирования и восстановления, а также управлять резервными копиями. Выберите роль для службы (подробнее см. в разделе Роли пользователя, доступные для каждой службы).

В противном случае пользователь будет иметь роли, которые заданы в выбранных службах.

8. Нажмите **Добавить выбранных пользователей**.
9. Выполните синхронизацию вручную (см. раздел "Запуск синхронизации данных домена вручную" (стр. 46)) или дождитесь выполнения автоматической синхронизации. После завершения синхронизации добавленные пользователи домена появятся на вкладке **Пользователи**.

## 3.12.3 Действия с добавленными доменными пользователями

Доступны следующие действия с добавленными доменными пользователями:

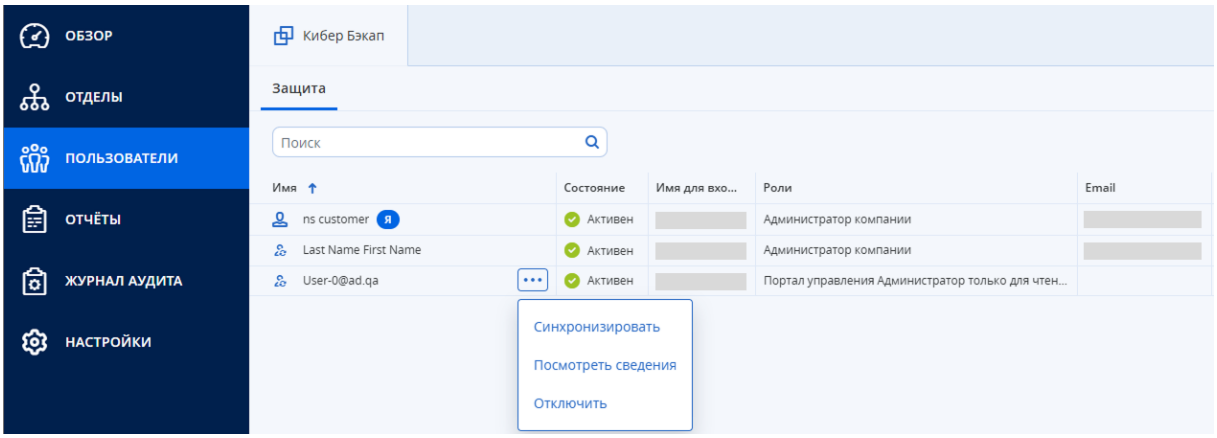
- синхронизация данных с доменом;
- просмотр сведений;
- изменение данных пользователя;
- отключение и включение учётной записи (подробнее см. в разделе "Отключение и включение учетной записи пользователя" (стр. 22));
- удаление пользователя (подробнее см. в разделе "Удаление учётной записи пользователя" (стр. 22)).

### 3.12.3.1 Синхронизация данных с доменом

Чтобы синхронизировать данные с доменом, выполните следующие действия:

1. На портале управления перейдите в раздел **Пользователи**.
2. Выберите пользователя и щёлкните значок многоточия.
3. В появившемся меню выберите **Синхронизировать**.

В результате выполненных действий данные будут синхронизированы с доменом.




## 3.12.3.2 Просмотр сведений

Для просмотра сведений о пользователе выполните следующие действия:

1. На портале управления перейдите в раздел **Пользователи**.
2. Выберите пользователя и щёлкните значок многоточия.
3. В появившемся меню выберите **Посмотреть сведения**.

В результате выполненных действий в правой области окна будут отображены сведения о пользователе:

- **Общие сведения**;
- **Службы и роли**;
- **Настройик**;
- **Квоты**.

При необходимости в эти даннные можно внести изменения.

## 3.12.3.3 Изменение данных пользователя

Для изменения данных пользователя выполните следующие действия:

1. На портале управления перейдите в раздел **Пользователи**.
2. Выберите пользователя и щёлкните значок многоточия.
3. В появившемся меню выберите **Посмотреть сведения**.
4. Щёлкните значок карадаша в разделе, который нужно изменить:
   - [При изменении блока **Общие сведения**] Выберите язык и введите комментарий при необходимости, для сохранения изменений щёлкните **Готово**.
   - [При изменении блока **Службы и роли**] Установите флажки для служб и выберите роли пользователя для этих служб, для сохранения изменений щёлкните **Готово**.

     При запросе данных администратора введите их и подтвердите изменения.

- [При изменении блока **Настройки**] Установите флажки для необходимых уведомлений и щёлкните **Готово** (подробнее см. раздел "Изменение настроек уведомлений для пользователя" (стр. 21)).
- [При изменении блока **Квоты**] Щёлкните на значение квоты и введите новое значение (подробнее о квотах см. в разделе "Управление квотами" (стр. 12)).

В результате выполненных действий данные будут изменены.

## 3.12.4 Управление доменом

Возможности управления добавленным доменом включают в себя:

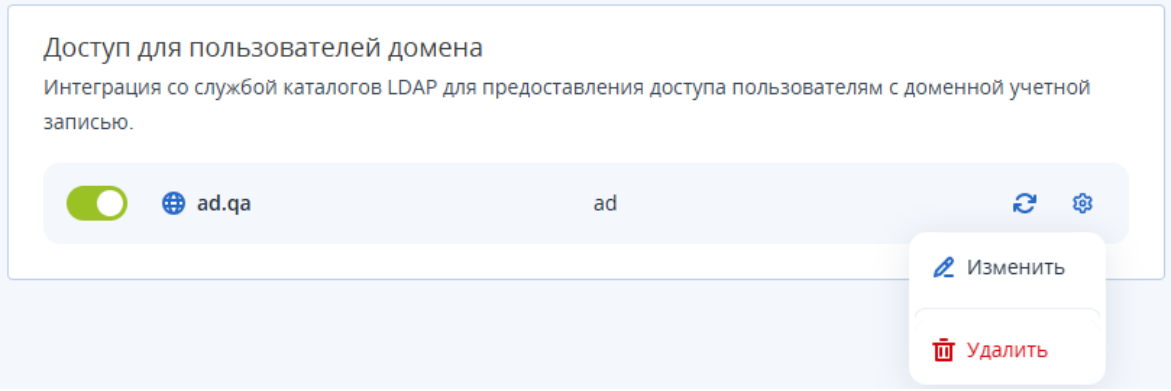
- изменение параметров подключения к службе каталогов;
- запуск синхронизации данных вручную;
- отключение и включение доступа для пользователей домена;
- удаление домена.

Подробные инструкции приведены в соответствующих разделах.

### 3.12.4.1 Изменение параметров подключения к службе каталогов домена

Для изменения параметров подключения к службе каталогов домена выполните следующие действия:

1. На портале управления перейдите в раздел **Настройки** > **Управление доступом**.
2. Щёлкните значок шестерёнки рядом с доменом, для которого необходимо изменить параметры подключения, далее щёлкните **Изменить** в появившемся меню.




**Примечание**
Изменение имени домена или типа службы каталогов возможно только с помощью удаления домена и его повторного добавления с новыми значениями параметров. Кроме того, потребуется повторное добавление пользователей/групп из домена, так как все текущие пользователи домена будут отключены при его удалении.

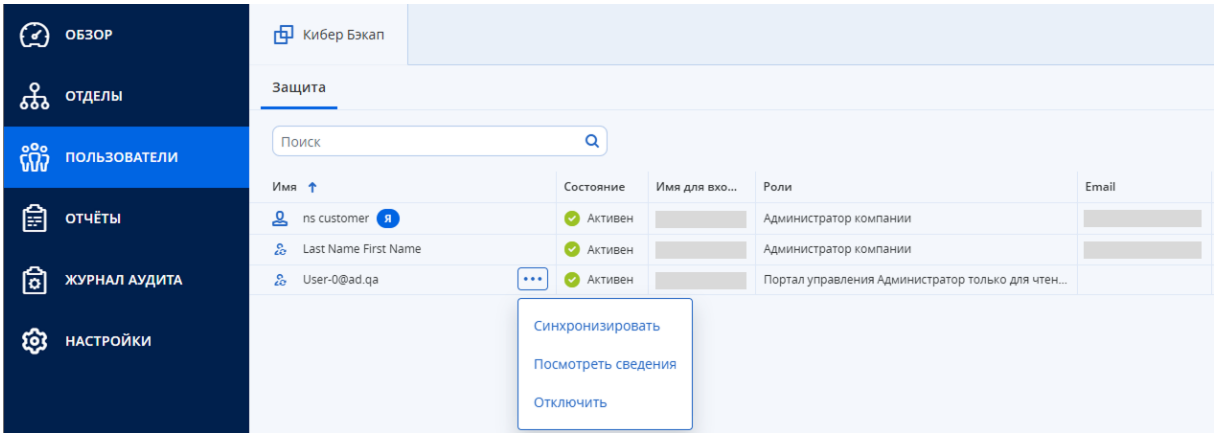
3. Измените значения требуемых параметров (подробнее см. в разделе "Настройка подключения к службе каталогов домена" (стр. 38)).
4. Нажмите **Сохранить**. В результате параметры будут изменены, а в нижнем правом углу окна программы появится подтверждающее сообщение **Настройки домена изменены**.

## 3.12.4.2 Запуск синхронизации данных домена вручную

Для запуска синхронизации данных домена вручную выполните следующие действия:

1. На портале управления перейдите в раздел **Настройки** > **Управление доступом**.
2. Щёлкните значок  в области домена, для которого необходимо выполнить синхронизацию. В результате синхронизация данных будет запущена, в а нижнем углу появится подтверждающее сообщение.

Синхронизацию данных домена также можно запустить в разделе **Пользователи**, щёлкнув в строке пользователя значок многоточия и выбрав **Синхронизировать** в появившемся меню.




## 3.12.4.3 Отключение и включение доступа для пользователей домена

### Отключение доступа для пользователей домена

Для отключения доступа пользователей домена выполните следующие действия:

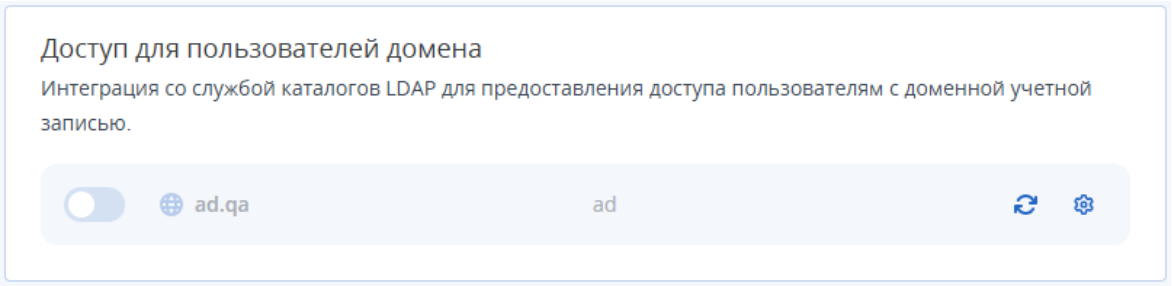
1. На портале управления перейдите в раздел **Настройки** > **Управление доступом**.
2. Выберите домен, для пользователей которого необходимо отключить доступ, и переведите его переключатель в положение **Отключено**.
3. Подтвердите отключение, щёлкнув **Отключить** в открывшемся окне.

   В результате выполненных действий доступ для пользователей домена будет отключён, а в нижнем правом углу окна программы появится подтверждающее сообщение.

### Включение доступа для пользователей домена

Для возобновления доступа пользователей ранее отключенного домена выполните следующие действия:

1. На портале управления перейдите в раздел **Настройки** > **Управление доступом**.
2. Выберите домен, для пользователей которого необходимо включить доступ. Пример домена, для пользователей которого доступ отключён, приведён на рисунке.




3. Переведите переключатель в области домена в положение **Включено**.

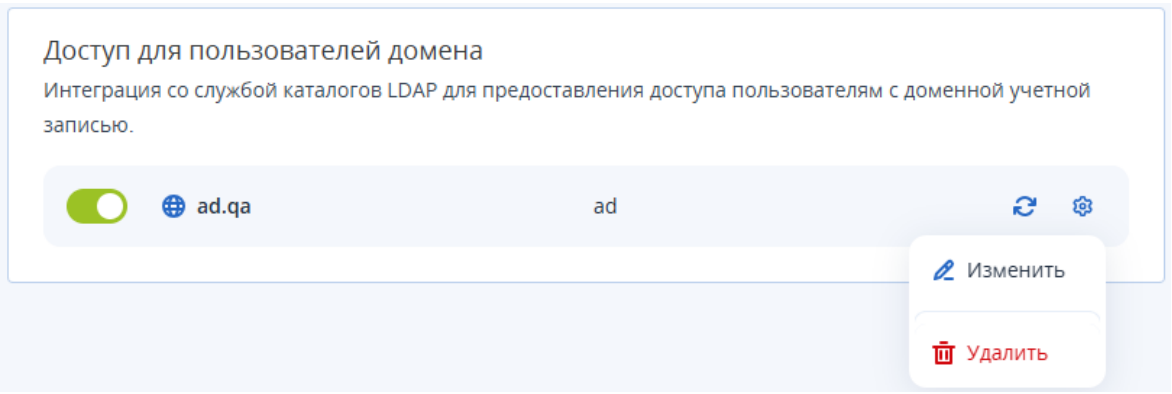
   В результате выполненных действий доступ для пользователей домена будет возобновлён.

### 3.12.4.4 Удаление домена

**Предупреждение**
Удаление домена из тенанта ведёт к отключению в нём всех пользователей, добавленных из этого домена. Доступ к объектам СРК отключенного пользователя сохраняется для администратора тенанта до момента удаления этого пользователя (см. раздел "Удаление учётной записи пользователя" (стр. 22)).

Для удаления домена выполните следующие действия:

1. На портале управления перейдите в раздел **Настройки** > **Управление доступом**.
2. Щёлкните значок шестерёнки рядом с доменом, который необходимо удалить, и выберите **Удалить** в появившемся меню.



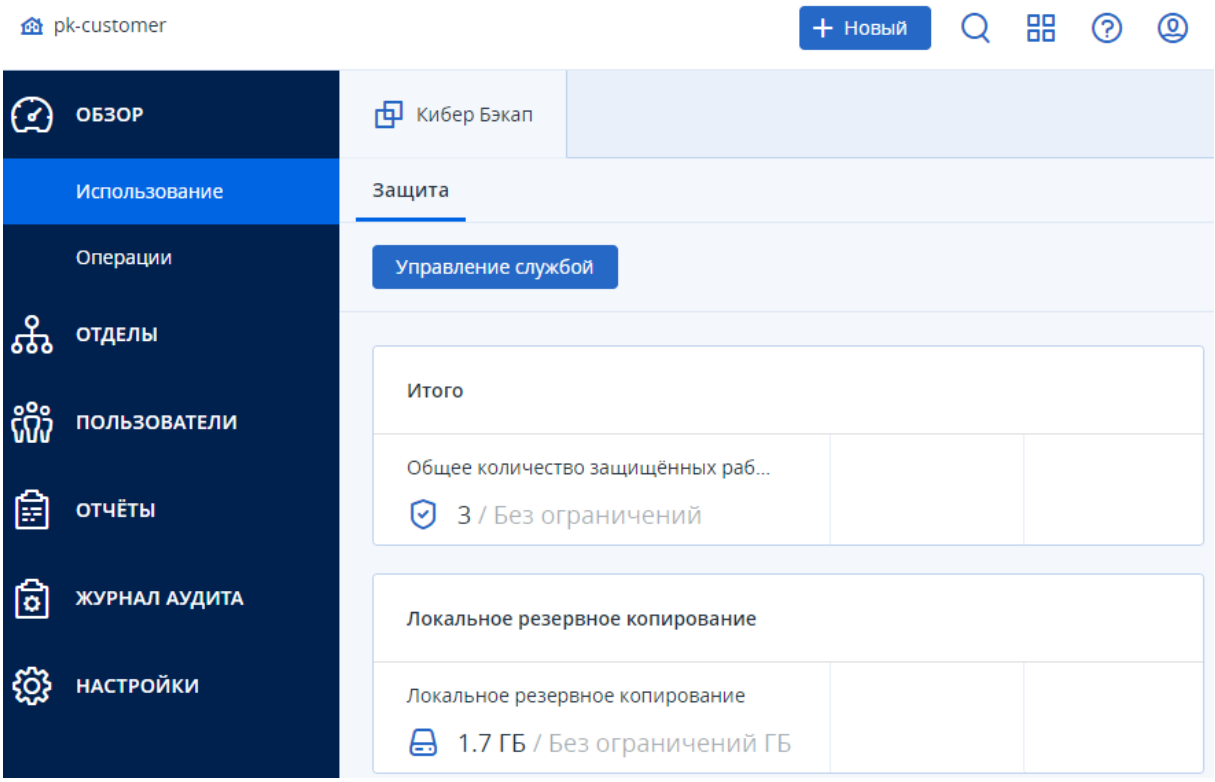

3. Нажмите **Удалить** в окне подтверждения.

# 4 Мониторинг

Чтобы получить информацию об использовании служб и операциях, щелкните **Обзор**.

## 4.1 Использование

На вкладке **Использование** предоставлен обзор использования служб (включая квоты). На ней также можно получить доступ к консолям служб.




## 4.2 Операции

Панель мониторинга **Операции** доступна только для администраторов компании при работе на уровне компании.

На панели мониторинга **Операции** есть несколько настраиваемых виджетов, которые позволяют выполнить обзор операций, относящихся к сервису Кибер Бэкап Облачный. Виджеты для других служб будут доступны в следующих выпусках.

Виджеты обновляются каждые две минуты. У виджетов есть активные элементы, на которые можно нажать для анализа возникших неполадок, их диагностики и устранения. Вы можете загрузить текущее состояние панели мониторинга или отправить его по электронной почте в файле формата .pdf и (или) .xlsx.

Вы можете выбирать из целого ряда виджетов, представленных в виде таблиц, круговых диаграмм, линейчатых диаграмм, списков и карт дерева. Можно добавить несколько виджетов одного типа с разными фильтрами.

***Порядок изменения расположения виджетов на панели мониторинга***

Перетащите виджеты, щелкнув их имена.

***Порядок изменения виджета***

Щелкните значок карандаша рядом с именем виджета. Изменение виджета позволяет переименовать его, изменить диапазон времени и задать фильтры.

***Порядок добавления виджета***

Щелкните **Добавить виджет** и выполните одно из следующих действий:

- Щелкните виджет, который необходимо добавить. Виджет будет добавлен с настройками по умолчанию.
- Чтобы изменить виджет перед его добавлением, щелкните значок карандаша, когда виджет выбран. После изменения виджета щелкните **Готово**.

***Порядок удаления виджета***

Щелкните значок X рядом с именем виджета.

## 4.2.1 Список доступных виджетов

- **Действия**. Показывает результаты действий за последние семь дней.
- **Список действий**. Показывает результаты действий, выполненных за указанный период времени.
- **5 последних оповещений**. Показывает 5 последних оповещений определенного типа.
- **Сводка по истории активных оповещений**. Показывает общее количество всех оповещений за указанный период времени.
- **Сводка по активным оповещениям**. Показывает общее количество активных оповещений по типам.
- **Журнал оповещений**. Показывает оповещения за указанный период времени.
- **Подробная информация об активных оповещениях**. Показывает активные оповещения.
- **Устройства**. Показывает подробную информацию о зарегистрированных устройствах.
- **Состояние резервного копирования**. Показывает устройства и примененные к ним планы резервного копирования.
- **Без защиты**. Показывает устройства без плана резервного копирования.
- **Статус защиты**. Показывает текущий статус защиты для машин.
- **Обнаруженные машины**. Показывает обнаруженные машины в течение указанного периода времени.

- **Сводные данные о хранилищах**. Показывает подробную информацию о хранилищах резервных копий.

# 5 Отчеты

Чтобы получить доступ к отчетам об использовании служб и операциях, щелкните **Отчеты**.

## 5.1 Использование

В отчетах об использовании предоставлены исторические данные об использовании служб. Отчеты об использовании доступны в обоих форматах CSV и HTML.

### 5.1.1 Тип отчета

Можно выбрать один из указанных ниже типов отчета:

- **Текущее использование**

  В отчете содержатся показатели текущего использования службы.
- **Итог за период**

  В отчете содержатся показатели использования службы за указанный период и разница между показателями в начале и в конце указанного периода.
- **Ежедневно в течение периода**

  В отчете содержатся показатели использования службы и данные об их изменении за каждый день указанного периода.

### 5.1.2 Уровень детализации

Можно выбрать детализацию отчета из указанных ниже значений:

- **Непосредственные клиенты и партнеры**

  В отчете будут содержаться показатели использования службы только для непосредственных дочерних отделов компании или отдела, в котором вы работаете.
- **Все клиенты и партнеры**

  В отчете будут содержаться показатели текущего использования службы для всех дочерних отделов компании или отдела, в котором вы работаете.
- **Все клиенты и партнеры (включая подробную информацию о пользователях)**

  В отчете будут содержаться показатели текущего использования службы для всех дочерних отделов компании или отдела, в котором вы работаете, а также для всех пользователей в отделах.

### 5.1.3 Запланированные отчеты

Запланированный отчет охватывает показатели использования службы за последний полный календарный месяц. Данные отчеты формируются в 23:59:59 (по времени UTC) в первый день месяца и отправляются во второй день месяца. Они отправляются всем администраторам компании или отдела, которые в пользовательских параметрах установили флажок **Запланированные отчеты использования**.

***Порядок включения или отключения запланированного отчета***

1. Войдите на портал управления.
2. Убедитесь, что вы работаете в компании самого верхнего уровня, которая вам доступна.
3. Щелкните **Отчеты** > **Использование**.
4. Нажмите кнопку **По плану**.
5. Установите или снимите флажок **Отправлять ежемесячный сводный отчет**.
6. В разделе **Уровень детализации** выберите область отчета, как описано выше.

### 5.1.4 Пользовательские отчеты

Пользовательский отчет формируется по требованию. Его невозможно запланировать. Отчет отправляется на ваш адрес электронной почты.

***Порядок формирования пользовательского отчета***

1. Войдите на портал управления.
2. Выберите отдел, для которого необходимо создать отчет.
3. Щелкните **Отчеты** > **Использование**.
4. Щелкните **По требованию**.
5. В разделе **Тип** выберите тип отчета, как описано выше.
6. [Недоступно для отчета типа **Текущее использование**] В поле **Период** выберите период отчета:
   - **Текущий календарный месяц**
   - **Предыдущий календарный месяц**
   - **Пользовательская**. Укажите начальную и конечную дату.
7. В разделе **Уровень детализации** выберите область отчета, как описано выше.
8. Чтобы создать отчет, нажмите кнопку **Сформировать и отправить**.

### 5.1.5 Отчеты об использовании

В отчете об использовании сервиса Кибер Бэкап Облачный содержатся следующие данные о компании или отделе:

- Размер резервных копий по отделам, пользователям и типам устройств.
- Количество защищенных устройств по отделам, пользователям и типам устройств.
- Общий размер резервных копий.

**Примечание**
Если сервис Кибер Бэкап Облачный не может обнаружить тип устройства, такое устройство отображается в отчете как **тип не установлен**.

# 5.2 Операции

Отчеты **Операции** доступны только для администраторов компании при работе на уровне компании.

Отчет об операциях может включать в себя любой набор виджетов **панели** мониторинга операций. Во всех виджетах отображается сводная информация для всей компании. Во всех виджетах показаны параметры для одного диапазона времени. Этот диапазон можно изменить в настройках отчета.

Для просмотра отчета щелкните его имя.

Можно скачать отчет об операциях или отправить его по электронной почте в формат Excel (XLSX) или PDF.

Чтобы получить доступ к операциям в отчете, щелкните значок многоточия в строке отчета. Такие же операции доступны из отчета.

Вы можете использовать предварительно созданные отчеты или создать пользовательский отчет.

Ниже перечислены отчеты по умолчанию

| Имя отчета | Описание |
|---|---|
| Ежедневные задания | Показывает сводную информацию о действиях, выполненных за указанный период времени |
| Еженедельные действия | Показывает сводную информацию о действиях, выполненных за указанный период времени |
| Обнаруженные машины | Показывает все найденные машины в сети организации |
| Оповещения | Показывает оповещения, выполненные за указанный период времени |
| Пользовательская | Пользовательский отчет формируется по требованию |
| Сводка | Показывает сводную информацию об устройствах, защищенных за указанный период времени |

### 5.2.0.1 Добавление отчета

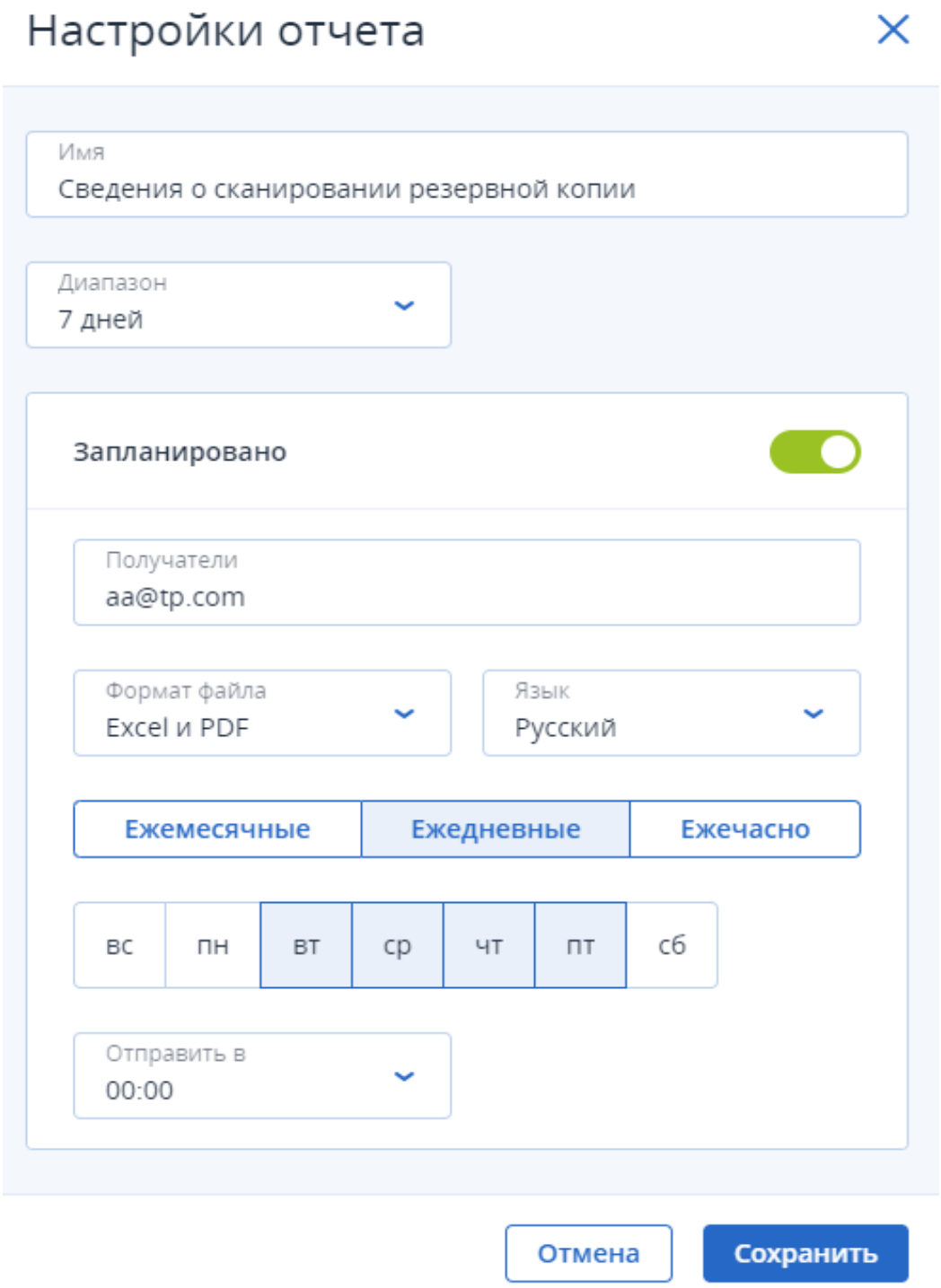
1. Щелкните **Добавить отчет**.
2. Выполните одно из следующих действий:
   - Чтобы добавить предопределенный отчет, щелкните имя отчета.
   - Чтобы добавить настраиваемый отчет, щелкните **Пользовательская**. Выберите имя отчета (по умолчанию назначаются имена типа **Пользовательская (1)**) и добавьте виджеты в отчет.

3. [Необязательно] Для изменения положения виджетов перетащите их.
4. [Необязательно] Измените отчет, как описано ниже.

#### 5.2.0.2 Изменение отчета

Чтобы изменить отчет, щелкните его имя и выберите пункт **Настройки**. При изменении отчета можно выполнить следующие действия:

- Переименовать отчет.
- Изменить диапазон времени для всех виджетов, включенных в отчет.
- Запланировать отправку отчета по электронной почте в форматах PDF и (или) Excel.




### 5.2.0.3 Планирование отчета

1. Щелкните имя отчета и выберите **Настройки**.
2. Включите переключатель **Запланировано**.
3. Укажите адреса электронной почты получателей.
4. Выберите формат отчета: PDF, Excel или оба.

5. Выберите дни, время и интервал отправки отчета.
6. Щелкните **Сохранить**.

### 5.2.0.4 Экспорт и импорт структуры отчета

Вы можете экспортировать и импортировать структуру отчета (набор виджетов и настроек отчета) в файл .json.

Чтобы экспортировать структуру отчета, щелкните имя отчета, щелкните значок многоточия в правом верхнем углу и выберите пункт **Экспорт**.

Для импорта структуры отчета щёлкните **Добавить отчет** и выберите пункт **Импорт**.

### 5.2.0.5 Скачивание отчета

Чтобы скачать отчет, щелкните **Скачать** и выберите необходимые форматы:

- Excel и PDF
- Excel
- PDF

**Примечание**
Для виджетов на основе таблиц можно скачать не более 1000 строк (для обоих форматов).

### 5.2.0.6 Дамп данных отчета

Дамп данных отчета в файле CSV можно отправить по электронной почте. Дамп содержит все данные отчета (без фильтрации) за определенный промежуток времени. В отчетах CSV метки времени указаны в формате UTC. В отчетах Excel и PDF метки времени указаны в текущем часовом поясе системы.

ПО динамически генерирует дамп данных. При указании большого промежутка времени данное действие может долго выполняться.

***Дамп данных отчета***

1. Щелкните имя отчета.
2. Щелкните значок многоточия в правом верхнем углу, а затем щелкните **Данные дампа**.
3. Укажите адреса электронной почты получателей.
4. В **Диапазон времени** укажите диапазон времени.
   Необработанные исторические данные хранятся постоянно, но могут действовать определенные ограничения для конечных форматов экспорта.
5. Щелкните **Отправить**.

## 5.3 Сводка руководства

В сводке руководства предоставлен обзор состояния защиты для среды вашей организации и защищенных устройств за указанный диапазон времени.

Сводка руководства включает в себя настраиваемые разделы с динамическими виджетами, которые отображают основные метрики работы.

Список доступных виджетов:

- **Обзор рабочих нагрузок**
  - **Устройства**. Показывает подробную информацию о зарегистрированных устройствах.
  - **Без защиты**. Показывает устройства без плана резервного копирования.
  - **Статус защиты**. Показывает текущий статус защиты для машин.
  - **Обнаруженные машины**. Показывает обнаруженные машины в течение указанного периода времени.
  - **Статус защиты рабочих нагрузок**. Показывает защищенные и незащищенные рабочие нагрузки по типу.
- **Резервная копия**
  - **Состояние резервного копирования**. Показывает устройства и примененные к ним планы резервного копирования.
  - **Сводные данные о хранилищах**. Показывает подробную информацию о хранилищах резервных копий.
  - **Рабочие нагрузки с резервной копией**. Показывает общее количество рабочих нагрузок с резервными копиями и без них.
  - **Использование хранилища резервных копий**. Показывает диаграмму использования хранилища данных для облачных и локальных хранилищ резервных копий.
- **Оповещения**
  - **5 последних оповещений**. Показывает 5 последних оповещений определенного типа.
  - **Сводка по истории активных оповещений**. Показывает общее количество всех оповещений за указанный период времени.
  - **Сводка по активным оповещениям**. Показывает общее количество активных оповещений по типам.
  - **Журнал оповещений**. Показывает оповещения за указанный период времени.
  - **Подробная информация об активных оповещениях**. Показывает активные оповещения.
- **Действия**
  - **Действия**. Показывает результаты действий за последние семь дней.
  - **Список действий**. Показывает результаты действий, выполненных за указанный период времени.

Настройка сводки руководства включает в себя следующие возможности:

- Добавление и удаление разделов.
- Изменение порядка разделов.
- Переименование разделов.
- Перенос виджетов из одного раздела в другой.
- Изменение порядка виджетов в каждом разделе.
- Добавление или удаление виджетов.
- Настройка виджетов.

Можно создавать сводные отчеты в формате PDF и Excel и отправлять их заинтересованным лицам или владельцам вашей организации.

### 5.3.1 Создание сводки руководства

Чтобы создать сводку руководства:

1. На портале управления откройте раздел **Отчеты** > **Сводка руководства**.
2. Нажмите **Создать сводку руководства**.
3. В поле **Имя отчета** введите имя сводного отчета.
4. Выберите получателей отчета.
   - Чтобы отправить отчет всем контактным лицам и пользователям, выберите **Отправить всем контактным лицам и пользователям**.
   - Чтобы отправить отчет отдельным контактным лицам и пользователям, выполните следующие действия:
     a. Снимите флажок **Отправить всем контактным лицам и пользователям**.
     b. Щелкните **Выбрать контактные лица**.
     c. Выберите нужных контактных лиц и пользователей. Чтобы найти нужное контактное лицо, воспользуйтесь поиском.
     d. Щелкните **Выбрать**.
5. Выберите диапазон сводного отчета: **30 дней** или **Этот месяц**.
6. Выберите формат файла: **PDF**, **Excel** или **Excel и PDF**.
7. Настройте параметры планирования.
   - Чтобы задать дату и время отправки отчета получателям, выполните следующие действия:
     a. Включите параметр **Запланировано**.
     b. Щелкните поле **День месяца**, снимите флажок **Последний день** и щелкните дату, которую необходимо установить.
     c. В поле **Время** введите время в часах.
     d. Нажмите кнопку **Применить**.
   - Чтобы создать отчет, не отправляя его получателям, отключите параметр **Запланировано**.
8. Нажмите кнопку **Сохранить**.

## 5.3.2 Настройка сводки руководства

***Порядок добавления раздела***

1. Щелкните **Добавить элемент** > **Добавить раздел**.
2. В окне **Добавить раздел** укажите имя раздела или используйте имя раздела по умолчанию.
3. Щелкните **Добавить в отчет**.

***Порядок переименования раздела***

1. В разделе, который необходимо переименовать, щелкните **Изменить**.
2. В окне **Изменить раздел** введите новое имя.
3. Нажмите кнопку **Сохранить**.

***Порядок удаления раздела***

1. В разделе, который необходимо удалить, щелкните **Удалить раздел**.
2. В окне подтверждения **Удалить раздел** щелкните **Удалить**.

***Порядок добавления виджета с настройками по умолчанию в раздел***

1. В разделе, куда необходимо добавить виджет, щелкните **Добавить виджет**.
2. В окне **Добавить виджет** щелкните виджет для добавления.

***Порядок добавления настраиваемого виджета в раздел***

1. В разделе, куда необходимо добавить виджет, щелкните **Добавить виджет**.
2. В окне **Добавить виджет** найдите виджет для добавления и щелкните **Настроить**.
3. Настройте поля по своему усмотрению.
4. Щелкните **Добавить виджет**.

***Порядок добавления виджета с настройками по умолчанию в отчет***

1. Щелкните **Добавить элемент** > **Добавить виджет**.
2. В окне **Добавить виджет** щелкните виджет для добавления.

***Порядок добавления настраиваемого виджета в отчет***

1. Щелкните **Добавить виджет**.
2. В окне **Добавить виджет** найдите виджет для добавления и щелкните **Настроить**.
3. Настройте поля по своему усмотрению.
4. Щелкните **Добавить виджет**.

***Порядок сброса настроек виджета по умолчанию***

1. В виджете, который необходимо настроить, щелкните **Изменить**.
2. Щелкните **Сбросить**.
3. Нажмите кнопку **Готово**.

***Порядок настройки виджета***

1. В виджете, который необходимо настроить, щелкните **Изменить**.
2. Измените поля по своему усмотрению.
3. Нажмите кнопку **Готово**.

### 5.3.3 Отправка сводки руководства

Сводку руководства можно отправить по запросу. В этом случае настройки **Запланировано** не принимаются во внимание и отчет отправляется незамедлительно. При отправке отчета система использует значения "Получатели", "Диапазон" и "Формат файла", которые указаны в разделе **Настройки**.

***Порядок отправки сводки руководства***

1. На портале управления откройте раздел **Отчеты** > **Сводка руководства**.
2. Щелкните название сводки, которую необходимо отправить.
3. Нажмите **Отправить сейчас**.

## 5.4 Часовые пояса в отчете

Часовые пояса, используемые в отчетах, зависят от типа отчета. В представленной ниже таблице приведена информация для справки.

| Расположение и тип отчета | Часовой пояс, используемый в отчете |
|---|---|
| Портал управления > Обзор > Операции (виджеты) | Время создания отчета указано в часовом поясе машины, в которой запущен браузер. |
| Портал управления > Обзор > Операции (экспортирован в PDF или xslx) | • Метка времени экспортированного отчета находится в часовом поясе машины, которая использовалась для экспорта отчета.<br>• Для действий, которые отображаются в отчете, указано время в часовом поясе UTC. |
| Портал управления > Отчеты > Использование > По плану | • Отчет создается в 23:59:59 (по времени UTC) в первый день месяца.<br>• Отчет отправляется во второй день месяца. |
| Портал управления > Отчеты > Использование > По требованию | Для отчета и даты его создания используется часовой пояс UTC. |

| | |
|---|---|
| Портал управления > Отчеты > Операции (виджеты) | • Время создания отчета указано в часовом поясе машины, в которой запущен браузер.<br>• Для действий, которые отображаются в отчете, указано время в часовом поясе UTC. |
| Портал управления > Отчеты > Операции (экспортирован в PDF или xslx) | • Метка времени экспортированного отчета находится в часовом поясе машины, которая использовалась для экспорта отчета.<br>• Для действий, которые отображаются в отчете, указано время в часовом поясе UTC. |
| Портал управления > Отчеты > Операции (запланированная доставка) | • Время доставки отчета указано в часовом поясе UTC.<br>• Для действий, которые отображаются в отчете, указано время в часовом поясе UTC. |
| Портал управления > Пользователи > Имя пользователя > Ежедневные краткие сведения об активных оповещениях | • Этот отчет отправляется один раз в промежуток между 10:00 и 23:59 UTC. Время отправки отчета зависит от рабочей нагрузки центра обработки данных.<br>• Для действий, которые отображаются в отчете, указано время в часовом поясе UTC. |

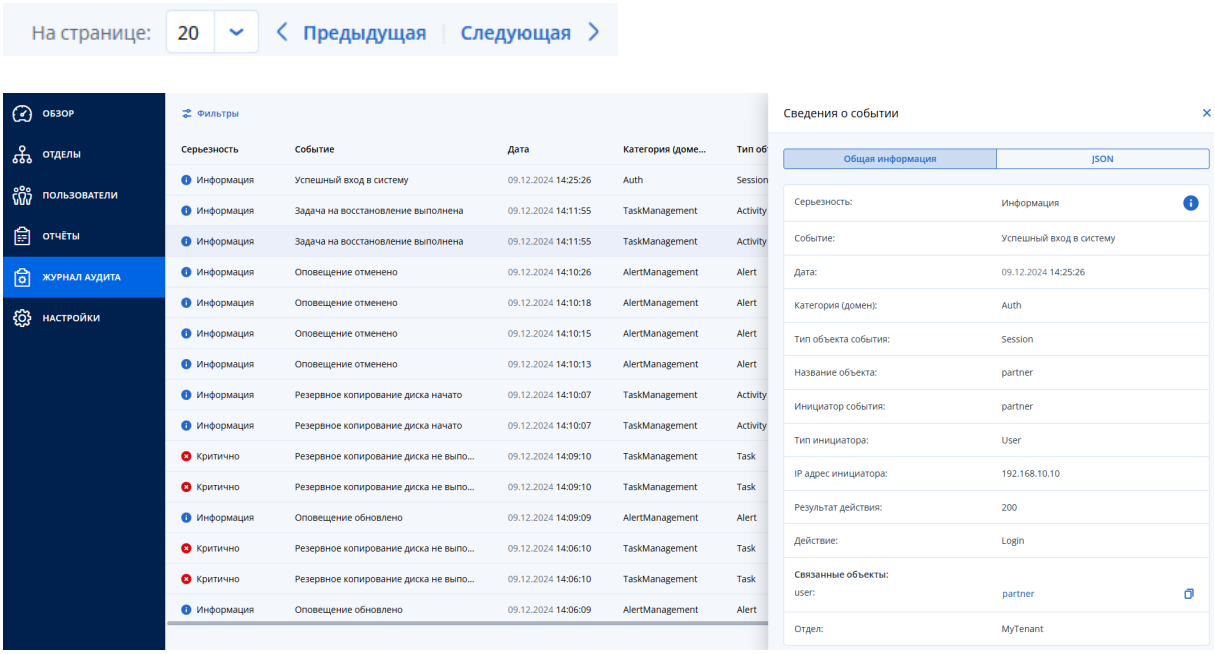
# 6 Журнал аудита

Журнал аудита содержит сведения о событиях, произошедших вследствие действий пользователей или работы системных компонентов. В журнале отображаются события тенанта, в котором вы работаете в настоящий момент, а также его дочерних тенантов.

Чтобы просмотреть список событий, перейдите в раздел **Журнал аудита**. События отображаются постранично с сортировкой по дате и времени в обратном порядке (от более новых к более старым). Для переключения между страницами используйте кнопки **< Предыдущая** и **Следующая >** внизу справа. Для просмотра сведений о событии щелкните по нему в списке.

**Примечание**

Переключение на следующую страницу не выполняется, если текущей страницей является последняя страница. Переключение на предыдущую страницу не выполняется, если текущей страницей является первая страница и с момента ее отображения не произошло новых событий.




На вкладке **Общая информация** будут отображены сведения о выбранном событии. При необходимости на вкладке **JSON** можно просмотреть подробные сведения о событии в формате JSON.

Срок хранения записи в журнале – 1 год. Записи, срок хранения которых истек, удаляются автоматически.

## 6.1 Основной поиск событий

Чтобы найти события с помощью основного поиска, выполните следующие действия:

1. Щелкните **Фильтры** над списком событий и перейдите на вкладку **Основной**.
2. Укажите от одного до нескольких критериев поиска:
   - название тенанта,
   - серьезность события (можно выбрать от одного до нескольких значений в выпадающем списке, в котором приведены все возможные значения),
   - период времени (можно выбрать один из предопределенных периодов или вручную указать его начало и окончание),
   - тип объекта события (можно выбрать от одного до нескольких значений в выпадающем списке, в котором приведены все возможные значения),
   - объект события,
   - инициатор события,
   - тип инициатора события (можно выбрать от одного до нескольких значений в выпадающем списке, в котором приведены все возможные значения),
   - IP-адрес инициатора события.
3. Нажмите **Применить** для отображения результатов.

## 6.2 Расширенный поиск событий

Чтобы найти события с помощью расширенного поиска, выполните следующие действия:

1. Щелкните **Фильтры** над списком событий и перейдите на вкладку **Расширенный**.
2. Введите поисковый запрос. Параметры и операторы, которые можно использовать в запросе, приведены в таблицах ниже.
3. Нажмите **Применить** для отображения результатов.

Кроме параметров и операторов можно использовать круглые скобки для группировки условий поиска, например:

```
(status = '204' OR status = '200') AND action = 'Login'
```

Параметры расширенного поиска

| Параметр | Описание | Примеры |
|---|---|---|
| uuid | Идентификатор события. Идентификатор можно узнать, просмотрев JSON-представление события. | • uuid = '0193c41a-6f13-7aa4-8448-2cad89f23385' |
| tenant_name | Название тенанта. | • tenant_name = 'MyTenant' |
| src_ip | IP-адрес и порт инициатора события. | • src_ip LIKE '192.168.10.10%' |
| level | Уровень важности события. Возможные значения: | • level = 'warning' |

| Параметр | Описание | Примеры |
|---|---|---|
| | • info – информация;<br>• warning – предупреждение;<br>• critical – критично;<br>• error – ошибка. | |
| obj_name | Имя объекта события. | • obj_name = 'WIN2019X64-5\\Administrator' |
| obj_domain | Категория (область) события. Возможные значения можно узнать, просмотрев JSON-представления событий. | • obj_domain = 'TaskManagement' |
| obj_type | Название типа объекта события. Возможные значения можно узнать, просмотрев JSON-представления событий. | • obj_type = 'Task' |
| obj_subtype | Название подтипа объекта события. Возможные значения можно узнать, просмотрев JSON-представления событий. | • obj_subtype = 'Backup::Disks' |
| action | Название действия. Возможные значения можно узнать, просмотрев JSON-представления событий. | • action IN ('Login', 'Logout') |
| status | Результат действия. | • status = '200' |
| principal_type | Название типа инициатора события. Возможные значения:<br>• User – инициатором события является пользователь;<br>• ServiceAccount – инициатором события является системный компонент. | • principal_type = 'User' |
| principal_name | Имя инициатора события. | • principal_name LIKE '%admin%' |
| event.timestamp | Дата и время события.<br>Операторы поиска **<**, **>**, **=**, **!=**, **IN**, **NOT IN** и **LIKE** не поддерживаются. | • event.timestamp <= '2024-11-30 12:00:00Z'<br>• event.timestamp >= '2024-11-30 12:00:00Z' |

Операторы расширенного поиска

| Оператор | Описание | Примеры |
|---|---|---|
| <параметр> = <значение> | Оператор сравнения "равно". | • level = 'warning' |
| <параметр> != <значение> | Оператор сравнения "не равно". | • level != 'info' |
| <параметр> < | Оператор сравнения "меньше". | • status < '400' |

| Оператор | Описание | Примеры |
|---|---|---|
| <значение> | | |
| <параметр> > <значение> | Оператор сравнения "больше". | • status > '200' |
| <параметр> <= <значение> | Оператор сравнения "меньше или равно". | • event.timestamp <= '2024-11-30 12:00:00Z' |
| <параметр> >= <значение> | Оператор сравнения "больше или равно". | • event.timestamp >= '2024-11-30 12:00:00Z' |
| <выражение> AND <выражение> | Логический оператор "И". | • src_ip LIKE '192.168.10.10%' AND level = 'info' |
| <выражение> OR <выражение> | Логический оператор "ИЛИ". | • level = 'critical' OR level = 'warning' |
| <параметр> IN (<значение 1>, ..., <значение n>) | Проверяет, присутствует ли значение параметра в заданном наборе значений. | • level IN ('critical', 'warning') |
| <параметр> NOT IN (<значение 1>, ..., <значение n>) | Проверяет, отсутствует ли значение параметра в заданном наборе значений. | • level NOT IN ('critical', 'warning') |
| <параметр> LIKE <шаблон значения> | Проверяет, соответствует ли значение параметра указанному шаблону (регистр символов не учитывается). В шаблоне можно использовать знак процента (**%**), который подменяет любую, в том числе и пустую, последовательность символов. | • principal_name LIKE '%admin%' |

## 6.3 Использование сохраненных поисковых запросов

Чтобы сохранить поисковый запрос, нажмите **Сохранить как шаблон**, введите имя и при необходимости описание запроса и нажмите **Сохранить**.

Сохраненный запрос можно выполнить, выбрав его в поле **Шаблон фильтрации** и нажав **Применить**. Для удаления сохраненного запроса щелкните значок корзины рядом с его именем и нажмите **Удалить** в окне подтверждения удаления.

# 6.4 Отправка записей журнала аудита на Syslog-сервер

По умолчанию журнал аудита хранится в базе данных сервиса Кибер Бэкап Облачный, однако для централизованного хранения и обработки можно настроить отправку записей журнала аудита на удаленный Syslog-сервер. Для отправки записей может использоваться протокол TCP, UDP или TLS.

## 6.4.1 Предварительные требования для протокола TLS

Если для отправки записей планируется использовать протокол TLS, то перед настройкой должны быть выполнены следующие требования:

- Для сервиса Кибер Бэкап Облачный подготовлены сертификат и закрытый ключ. Сертификат заверен корневым или промежуточным удостоверяющим центром (УЦ).
- Для Syslog-сервера подготовлены сертификат и закрытый ключ. Сертификат заверен корневым УЦ. В поле сертификата IPAddress указан IP-адрес Syslog-сервера, или в поле DNSname указано его DNS-имя.
- Сертификат и закрытый ключ Syslog-сервера загружены на Syslog-сервер и указаны в его настройках.
- Файл цепочки сертификатов для проверки сертификата сервиса Кибер Бэкап Облачный загружен на Syslog-сервер и указан в его настройках.
- Подготовлен сертификат УЦ, которым был заверен сертификат Syslog-сервера.

Подробные сведения о подготовке сертификатов и настройке Syslog-сервера см. в документации используемого в вашем окружении Syslog-сервера.

## 6.4.2 Настройка отправки записей на Syslog-сервер

Для настройки выполните следующие действия:

1. Перейдите в раздел **Настройки** > **Параметры Syslog** и переведите переключатель **Передавать журнал аудита на Syslog сервер** в состояние "вкл".
2. Укажите параметры подключения к Syslog-серверу:
   - **Адрес удаленного сервера**. IP-адрес или DNS-имя Syslog-сервера.
   - **Порт**. Порт Syslog-сервера.
   - **Протокол**. Протокол для подключения к Syslog-серверу. Можно указать **TCP**, **UDP** или **TLS**.
   - **Формат сообщения**. Формат, в котором будут отправляться сообщения. Можно указать **CEF (RFC 3164)** или **Syslog**.
   - [Только для протокола TLS] **TLS Certificate**. Сертификат сервиса Кибер Бэкап Облачный в формате PEM. Этот сертификат будет использоваться Syslog-сервером для проверки подлинности сервиса Кибер Бэкап Облачный.
   - [Только для протокола TLS] **TLS Key**. Закрытый ключ сертификата сервера управления Кибер Бэкап Облачный. Ключ должен быть указан в формате PEM.

- [Только для протокола TLS] **TLS CA Certificate**. Сертификат удостоверяющего центра (УЦ), которым заверен сертификат Syslog-сервера. Сертификат УЦ должен быть указан в формате PEM. Этот сертификат будет использоваться сервисом Кибер Бэкап Облачный при проверке подлинности Syslog-сервера.

3. Нажмите **Отправить тестовое сообщение** и убедитесь, что сообщение получено Syslog-сервером.

   **Примечание**
   При использовании протокола UDP сообщение об ошибке отправки будет показано только в том случае, когда хост, на котором установлен Syslog-сервер, недоступен.

4. Нажмите **Сохранить**.

После настройки запись о каждом новом событии будет сохраняться в журнал аудита, а также отправляться на указанный Syslog-сервер.

## 6.5 Регистрируемые события

В журнале аудита Кибер Бэкап Облачный фиксируются события следующих категорий:

- оповещения;
- действия с планами защиты;
- действия с устройствами и их группами;
- аутентификация и авторизация;
- действия с тенантами;
- резервное копирование;
- лицензирование;
- регистрация агентов.

Более подробная информация о записываемых в журнал событиях приведена в таблицах ниже.

### 6.5.1 События оповещений

| Событие | Серьёзность | Название объекта | Тип объекта события | Инициатор события | Результат действия |
|---|---|---|---|---|---|
| Оповещение создано (Alert created) | Информация (info) | Имя ресурса | Alert | - | 200 |
| Оповещение обновлено (Alert updated) | Информация (info) | Имя ресурса | Alert | - | 200 |
| Оповещение отменено (Alert reset)* | Информация (info) | Имя ресурса | Alert | Имя пользователя | 204 |

* При использовании массового действия с оповещениями, например, **Очистить всё**, для каждого оповещения будет создана отдельная запись в журнале аудита.

## 6.5.2 События действий с планами защиты

| Событие | Серьёзность | Название объекта | Тип объекта события | Инициатор события | Результат действия |
|---|---|---|---|---|---|
| План защиты создан (Backup plan created) | Информация (info) | Имя плана | Policy | Имя пользователя | 20x |
| План защиты обновлён (Backup plan updated) | Информация (info) | Имя плана | Policy | Имя пользователя | 20x |
| План защиты удалён (Backup plan deleted) | Информация (info) | Имя плана | Policy | Имя пользователя | 204 |
| Статус установки плана (Plan deployment state) | Информация (info) | Имя плана | Policy | - | 200 |
| Политика применена к устройству (Policy applied to workload) | Информация (info) | Имя плана | PolicyApplication | Имя пользователя | 20x |

## 6.5.3 События действий с устройствами и их группами

| Событие | Серьёзность | Название объекта | Тип объекта события | Инициатор события | Результат действия |
|---|---|---|---|---|---|
| Устройство создано (Workload created) | Информация (info) | Имя ресурса | Workload | - | 200 |
| Устройство обновлено (Workload updated) | Информация (info) | Имя ресурса | Workload | - | 200 |
| Устройство удалено (Workload deleted) | Информация (info) | Имя ресурса | Workload | - | 200 |

| | | | | | |
|---|---|---|---|---|---|
| Группа устройств создана (Workload group created) | Информация (info) | Имя группы | GroupMembership | Имя пользователя | 201 |
| Участники добавлены в статическую группу устройств (Workload static group member added) | Информация (info) | Имя группы | GroupMembership | - | 200 |
| Участники добавлены в динамическую группу устройств (Workload dynamic group member added) | Информация (info) | Имя группы | GroupMembership | - | 200 |
| Участники удалены из статической группы устройств (Workload static group member removed) | Информация (info) | Имя группы | GroupMembership | - | 200 |
| Участники удалены из динамической группы устройств (Workload dynamic group member removed) | Информация (info) | Имя группы | GroupMembership | - | 200 |
| Группа устройств удалена (Workload group deleted) | Информация (info) | Имя группы | GroupMembership | Имя пользователя | 200 |

## 6.5.4 События аутентификации и авторизации

| Событие | Серьёзность | Название объекта | Тип объекта события | Инициатор события | Результат действия |
|---|---|---|---|---|---|
| Успешный вход | Информация | Имя | Session | Имя | 200 |

| | | | | | |
|---|---|---|---|---|---|
| в систему (Logged in) | (info) | пользователя | | пользователя | |
| Превышено число попыток войти в систему (Exceeded the number of login attempts) | Критично (critical) | Имя пользователя | Session | Имя пользователя | 429 |
| Успешный выход из системы (Logged out) | Информация (info) | Имя пользователя | Session | Имя пользователя | 200 |
| Документ был подписан (Legal document signed) | Информация (info) | - | LegalDocument | Имя пользователя | 200 |
| Токен доступа выписан (Access token issued) | Информация (info) | - | Token | - | 200 |

## 6.5.5 События действий с тенантами

| Событие | Серьёзность | Название объекта | Тип объекта события | Инициатор события | Результат действия |
|---|---|---|---|---|---|
| Тенант создан (Tenant created) | Информация (info) | Имя созданного тенанта | Tenant | Имя пользователя | 200 |
| Тенант обновлён (Tenant updated) | Информация (info) | Имя обновлённого тенанта | Tenant | • Имя пользователя (при обновлении имени тенанта любого типа, при включении тенанта, а также при любом обновлении тенанта типа **Клиент**);<br>• '-' (при | 200 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | обновлении родительского тенанта, кроме его имени). | |
| Тенант отключён (Tenant disabled) | Предупреждение (warning) | Имя обновлённого тенанта | Tenant | Имя пользователя | 200 |
| Тенант удалён (Tenant deleted) | Предупреждение (warning) | Имя удалённого тенанта | Tenant | Имя пользователя | 200 |
| Изменение привилегий пользователя (User privileges updated) | Информация (info) | - | UserPrivileges | Имя пользователя, совершившего действие | 200 |
| Учётная запись пользователя создана (User created) | Информация (info) | Имя пользователя | User | Имя пользователя | 200 |
| Учётная запись пользователя обновлена (User updated) | Информация (info) | Имя (логин) обновлённого пользователя | User | Имя пользователя | 200 |
| Учётная запись пользователя отключена (User disabled) | Предупреждение (warning) | Имя обновлённого пользователя | User | Имя пользователя | 200 |
| Учётная запись пользователя включена (User enabled) | Предупреждение (warning) | Имя изменённого пользователя | User | Имя пользователя, совершившего действие | 200 |
| Пароль сброшен (User reset) | Предупреждение (warning) | Имя обновлённого пользователя | User | Имя пользователя | 200 |
| Учётная запись | Критично (critical) | Имя пользователя | User | Имя пользователя | 200 |

| | | | | | |
|---|---|---|---|---|---|
| пользователя удалена (User deleted) | | | | | |
| Служебная учётная запись создана (Account created)<br><br>**Примечание**<br>При работе с API-клиентами. | Информация (info) | Имя API-клиента | ServiceAccount | Имя пользователя | 200 |
| Служебная учётная запись обновлена (Account updated)<br><br>**Примечание**<br>При работе с API-клиентами. | Информация (info) | Имя API-клиента | ServiceAccount | Имя пользователя | 200 |
| Служебная учётная запись удалена (Account deleted)<br><br>**Примечание**<br>При работе с API-клиентами. | Информация (info) | Имя API-клиента | ServiceAccount | Имя пользователя | 200 |
| Секрет служебной учётной записи сброшен (Account secret reset) | Информация (info) | Имя API-клиента | ServiceAccount | Имя пользователя | 200 |

| | | | | | |
|---|---|---|---|---|---|
| **Примечание**<br>При работе с API-клиентами. | | | | | |
| Юридический документ добавлен (Legal document created) | Информация (info) | Версия документа (например, Version 2024-04-03) | LegalDocument | Имя пользователя | 200 |
| Юридический документ опубликован (Legal document published) | Информация (info) | Версия документа (например, Version 2024-04-03) | LegalDocument | Имя пользователя | 200 |
| Юридический документ удалён (Legal document deleted) | Информация (info) | Версия документа (например, Version 2024-04-03) | LegalDocument | Имя пользователя | 200 |
| Документ был подписан (Legal document signed) | Информация (info) | Версия документа (например, Version 2024-04-03) | LegalDocument | Имя пользователя | 200 |
| Служба добавлена для тенанта (Service added for tenant) | Информация (info) | Cyber Infrastructure | Application | Имя пользователя | 200 |
| Служба удалена для тенанта (Service removed from tenant) | Информация (info) | Cyber Infrastructure | Application | Имя пользователя | 200 |
| Служба добавлена для тенанта (Service added | Информация (info) | Cyber Protection | Application | Имя пользователя | 200 |

| | | | | | |
|---|---|---|---|---|---|
| for tenant) | | | | | |
| Служба удалена для тенанта (Service removed from tenant) | Информация (info) | Cyber Protection | Application | Имя пользователя | 200 |

## 6.5.6 События резервного копирования

| Событие | Серьёзность | Название объекта | Тип объекта события | Инициатор события | Результат действия |
|---|---|---|---|---|---|
| Резервное копирование помещено в очередь (Backup queued) | Информация (info) | Имя ресурса | Task | • Имя пользователя (если тип инициатора **User**)<br>• '-' (если тип инициатора **ServiceAccount**) | 200 |
| Резервное копирование назначено агенту (Backup assigned to agent) | Информация (info) | Имя ресурса | Task | • Имя пользователя (если тип инициатора **User**)<br>• '-' (если тип инициатора **ServiceAccount**) | 200 |
| Ошибка при назначении резервного копирования агенту (Error assigning backup to agent) | Критично (critical)* | Имя ресурса | Task | • Имя пользователя (если тип инициатора **User**)<br>• '-' (если тип инициатора **ServiceAccount**) | 500 |
| Резервное копирование начато (Backup started) | Информация (info) | Имя ресурса | Task | • Имя пользователя (если тип инициатора **User**)<br>• '-' (если тип | 200 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | инициатора **ServiceAccount**) | |
| Резервное копирование выполнено (Backup completed) | Информация (info) | Имя ресурса | Task | • Имя пользователя (если тип инициатора **User**)<br>• '-' (если тип инициатора **ServiceAccount**) | 200 |
| Резервное копирование завершилось с предупреждением (Backup finished with warning) | Предупреждение (warning)* | Имя ресурса | Task | • Имя пользователя (если тип инициатора **User**)<br>• '-' (если тип инициатора **ServiceAccount**) | 200 |
| Резервное копирование завершилось с ошибкой (Backup failed) | Критично (critical)* | Имя ресурса | Task | • Имя пользователя (если тип инициатора **User**)<br>• '-' (если тип инициатора **ServiceAccount**) | 500 |
| Задача на восстановление создана (Recovery task created) | Информация (info) | Имя ресурса | Activity | Имя пользователя | 200 |
| Задача на восстановление запущена (Recovery task started) | Информация (info) | Имя ресурса | Activity | Имя пользователя | 200 |
| Задача на восстановление выполнена (Recovery task completed) | Информация (info) | Имя ресурса | Activity | Имя пользователя | 200 |

* Серьёзность зависит от кода задачи: если она завершена с кодом **warning**, то Серьёзность – **предупреждение** (**warning**); если с кодом **error**, то Серьёзность – **критично** (**critical**).

## 6.5.7 События лицензирования

| Событие | Серьёзность | Название объекта | Тип объекта события | Инициатор события | Результат действия |
|---|---|---|---|---|---|
| Лицензия для тенанта включена (Tenant license enabled) | Информация (info) | pw_pack... или pg_ pack... | OfferingItemCount | Имя тенанта | 200 |
| Лицензия для тенанта включена (Tenant license enabled) | Информация (info) | local_ storage | OfferingItemCount | Имя тенанта | 200 |
| Успешное выключение лицензии для тенанта (Tenant license disabled) | Предупреждение (warning) | pw_pack... или pg_ pack... | OfferingItemCount | Имя пользователя | 200 |
| Квота для тенанта установлена (Tenant quota set) | Информация (info) | pw_base... или pg_ base... | TenantQuota | Имя тенанта | 200 |

## 6.5.8 События регистрации агентов

| Событие | Серьёзность | Название объекта | Тип объекта события | Инициатор события | Результат действия |
|---|---|---|---|---|---|
| Регистрация агента завершена (Agent registered) | Информация (info) | Имя агента (имя хоста) | Agent | - | 200 |
| Регистрация агента отозвана (Agent unregistered) | Информация (info) | Имя агента (имя хоста) | Agent | - | 200 |

| | | | | | |
|---|---|---|---|---|---|
| **Примечание**<br>При удалении агента с помощью интерфейса командной строки. | | | | | |
| Регистрация агента отозвана (Agent unregistered)<br><br>**Примечание**<br>При удалении агента с помощью консоли службы. | Информация (info) | Имя агента (имя хоста) | Agent | Имя пользователя, инициировавшего удаление | 200 |

# 7 Дополнительные сценарии использования

## 7.1 Ограничение доступа к веб-интерфейсу

Можно ограничить доступ к веб-интерфейсу, указав список IP-адресов, с которых пользователям будет разрешено выполнять вход.

Это ограничение также действует для доступа к порталу управления через API.

Это ограничение применяется только на том уровне, на котором оно задано. Это *не* применяется к участникам дочерних отделов.

***Порядок ограничения доступа к веб-интерфейсу***

1. Войдите на портал управления.
2. Найдите отдел, в котором необходимо ограничить доступ.
3. Щелкните **Настройки** > **Безопасность**.
4. Установите флажок **Контроль входа в систему**.
5. В поле **Разрешенные IP-адреса** укажите разрешенные IP-адреса.
   Можно ввести любые из указанных ниже параметров, используя в качестве разделителя точку с запятой:
   - IP-адреса, например 192.0.2.0;
   - Диапазоны IP-адресов, например 192.0.2.0-192.0.2.255;
   - Подсети, например 192.0.2.0/24.
6. Нажмите кнопку **Сохранить**.

## 7.2 Ограничение доступа к вашей компании

Администраторы компании могут ограничить доступ к компании для администратора более высокого уровня.

Если доступ к компании ограничен, администраторы более высокого уровня могут только менять свойства компании. Они вообще не видят учетные записи и дочерние отделы.

***Порядок ограничения доступа к компании***

1. Войдите на портал управления.
2. Щелкните **Настройки** > **Безопасность**.
3. Отключите параметр **Доступ для службы поддержки**.
4. Нажмите кнопку **Сохранить**.

## 7.3 Настройка числа неуспешных попыток входа

По умолчанию Кибер Бэкап Облачный имеет ограничение на количество неуспешных попыток входа в 10 попыток за 15 минут. При превышении данного ограничения вход на портал управления для учетной записи пользователя блокируется на 15 минут.

Чтобы изменить значение настройки:

1. Войдите на портал управления.
2. Найдите отдел, в котором необходимо изменить значение настройки.
3. Нажмите **Настройки** > **Безопасность**.
4. В разделе **Число неуспешных попыток входа** установите значения:
   - В поле **Число неуспешных попыток входа** укажите количество неудачных попыток входа до блокировки. Возможные значения: от 1 до 10.
   - В поле **Период блокировки учетной записи** укажите время блокировки учетной записи пользователя в минутах. Возможные значения: от 1 до 60.
5. Нажмите **Сохранить**.

Новое значение настройки применяется ко всем пользователям этого тенанта и его дочерних тенантов.

## 7.4 Настройка периода бездействия пользователя

Настройка определяет временной период бездействия пользователя (в минутах), по истечении которого его сессия будет автоматически завершена как на портале управления, так и в консоли службы. Диапазон доступных значений – от 5 до 999. Значение по умолчанию – 15.

Данный параметр наследуется дочерними тенантами, если их администраторы не установили собственное значение. Индивидуальная настройка в дочернем тенанте имеет приоритет над родительской и сохраняется при изменении параметра на верхнем уровне. При сбросе настроек в дочернем тенанте применяется значение, наследуемое из родительского тенанта.

### 7.4.1 Изменение настройки периода бездействия пользователя

Чтобы изменить настройку периода бездействия пользователя, выполните следующие шаги:

1. Войдите на портал управления.
2. Выберите тенант, для которого нужно изменить настройки.
3. Щёлкните **Настройки** > **Безопасность**.
4. В блоке **Завершить сеансы работы неактивных пользователей** укажите новое значение периода бездействия пользователя.
5. Для применения настроек нажмите **Сохранить**.

В результате выполненных действий значение периода бездействия пользователя будет изменено. Настройка будет применена к пользователям данного тенанта, а также будет наследоваться его дочерними тенантами (если их администраторы не установили собственное значение).

### 7.4.2 Сброс настройки периода бездействия пользователя

Чтобы сбросить настройку периода бездействия пользователя, выполните следующие шаги:

1. Войдите на портал управления.
2. Выберите тенант, для которого нужно изменить настройки.
3. Щёлкните **Настройки** > **Безопасность**.
4. В блоке **Завершить сеансы работы неактивных пользователей** нажмите **Сбросить**.

В результате выполненных действий параметр примет значение, унаследованное от родительского тенанта (если оно задано), в противном случае – значение по умолчанию. Это значение также будет наследоваться дочерними тенантами (если их администраторы не установили собственное).

## 7.5 Управление клиентами API

Сторонние системы можно интегрировать с Кибер Бэкап Облачный, используя программные интерфейсы (API). Доступ к этим API включён через клиенты API – это часть инфраструктуры авторизации OAuth 2.0 на платформе.

### 7.5.1 Что такое клиент API?

Клиент API – это специальная учётная запись платформы, представляющая стороннюю систему, для которой нужна идентификация и авторизация для доступа к данным через API платформы и её служб.

Клиент API имеет доступ только к тенанту, для которого администратор создал его, а также к его дочерним тенантам.

При создании клиенту API назначается роль **Администратор компании**. Эту роль невозможно изменить впоследствии. Изменение ролей учётной записи администратора или её отключение не влияет на клиент API.

Учётные данные клиента API состоят из уникального идентификатора и значения секрета. Учётные данные не имеют срока действия и не могут использоваться для входа на портал управления или в консоль службы. Значение секрета можно сбросить.

Для клиента API можно включить двухфакторную аутентификацию.

## 7.5.2 Типовая процедура интеграции

1. Администратор создаёт клиент API в тенанте, которым будет управлять сторонняя система.
2. Администратор включает поток учётных данных клиента OAuth 2.0 в сторонней системе.

   Согласно этому потоку, перед доступом к тенанту и его службам через API система сначала должна отправить учётные данные созданного клиента на платформу, используя API авторизации. Платформа создаёт и отправляет обратно маркер безопасности – уникальную криптографически защищённую строку, которая назначается только данному клиенту. После этого система должна добавить этот маркер во все запросы API.

   Маркер безопасности устраняет необходимость передачи учётных данных клиента с запросами API. Для обеспечения дополнительной безопасности срок действия маркера истекает через два часа. По истечении этого времени просроченный маркер даёт сбой, после чего системе необходимо запросить новый маркер с платформы.

## 7.5.3 Создание клиента API

1. Войдите на портал управления.
2. Щелкните **Настройки** > **Клиенты API** > **Создать клиент API**.
3. Введите имя клиента API.
4. Нажмите кнопку **Далее**.

   Клиент API создается со статусом **Активный** по умолчанию.
5. Скопируйте и сохраните идентификатор и секрет клиента и URL-адрес центра обработки данных. Они понадобятся при включении потока учетных данных клиента OAuth 2.0 в сторонней системе.

   **Внимание**
   По причинам безопасности ключ отображается только один раз. Он не подлежит восстановлению при утрате. Его можно только сбросить.
6. Нажмите кнопку **Готово**.

## 7.5.4 Сброс значения секрета клиента API

1. Войдите на портал управления.
2. Щелкните **Настройки** > **Клиенты API**.
3. Найдите нужный клиент в списке.
4. Щелкните , а затем щелкните **Сбросить секрет**.
5. Подтвердите свое решение, щелкнув **Далее**.

   Будет создано новое значение секрета. Идентификатор клиента и URL-адрес центра обработки данных не меняются.

Для всех маркеров безопасности, назначенных этому клиенту, немедленно завершится срок действия, а запросы API с этими маркерами завершатся сбоем.

6. Скопируйте и сохраните новое значение секрета клиента.

**Внимание**
По причинам безопасности ключ отображается только один раз. Оно не подлежит восстановлению при утрате. Его можно только сбросить.

7. Нажмите кнопку **Готово**.

## 7.5.5 Отключение клиента API

1. Войдите на портал управления.
2. Щелкните **Настройки** > **Клиенты API**.
3. Найдите нужный клиент в списке.
4. Щелкните , а затем щелкните **Отключить**.
5. Подтвердите операцию.

   Статус клиента изменится на **Отключен**.

   Не удастся выполнить запросы API с маркерами безопасности, которые назначены этому клиенту, но маркеры не станут просроченными сразу же после этого. Отключение клиента не влияет на срок действия маркеров.

   Клиент можно заново включить в любое время.

## 7.5.6 Включение отключенного клиента API

1. Войдите на портал управления.
2. Щелкните **Настройки** > **Клиенты API**.
3. Найдите нужный клиент в списке.
4. Щелкните , а затем щелкните **Включить**.

   Статус клиента изменится на **Активный**.

   Запросы API с маркерами безопасности, которые назначены этому клиенту, будут успешно выполнены, если срок действия этих маркеров еще не истек.

## 7.5.7 Удаление клиента API

1. Войдите на портал управления.
2. Щелкните **Настройки** > **Клиенты API**.
3. Найдите нужный клиент в списке.
4. Щелкните , а затем щелкните **Удалить**.

5. Подтвердите операцию.

   Для всех маркеров безопасности, назначенных этому клиенту, немедленно завершится срок действия, а запросы API с этими маркерами завершатся сбоем.

   **Внимание**
   Восстановить удаленный клиент невозможно.

## 7.6 Обновление агентов

Чтобы настроить автоматическое обновление агентов, выполните следующие действия:

1. Войдите на портал управления.
2. Перейдите в **Настройки** > **Обновление агентов**.
3. В разделе **Канал обновления** укажите версию, до которой следует обновлять агенты.
4. Установите флажок **Обновлять агенты автоматически**.
5. Установите флажок **Окно обслуживания** и укажите дни и время для автоматического обновления агентов.
6. Нажмите кнопку **Сохранить**.

# Указатель

## О



## П