КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 24.03

Руководство администратора партнера

Редакция: 24.04.2024

Содержание

Заявление об авторских правах

1 О документе

Этот документ предназначен для администраторов партнера, которые хотят использовать Кибер Бэкап Облачный для предоставления служб своим клиентам.

В этом документе описана установка и управление службами, которые доступны в Кибер Бэкап Облачный, с использованием портала управления.

2 О программе Кибер Бэкап Облачный

Кибер Бэкап Облачный – это облачная платформа, которая позволяет поставщикам услуг, торговым посредникам и дистрибьюторам предоставлять услуги по защите данных своим партнерам и пользователям.

Службы предоставляются на уровне партнеров, уровне компании-клиента и уровне конечного пользователя.

Управление службами доступно посредством веб-приложений, которые называются **консолями службы**. Управление тенантом и учетной записью пользователя доступно через веб-приложение, которое называется **порталом управления**.

Портал управления позволяет администраторам выполнять следующие действия:

- отслеживать использование служб и получать доступ к консолям службы;
- управлять тенантами;
- управлять учетными записями пользователей;
- настраивать службы и квоты для тенантов;
- управлять хранилищем данных;
- управлять фирменным оформлением;
- создавать отчеты об использовании служб.

2.1 Управление функциональными пакетами и квотами

В этом разделе затронуты следующие темы:

- Что представляют собой службы и функциональные пакеты?
- Как включить или отключить функциональные пакеты?
- Что представляют собой Advanced Protection?
- Что подразумевается под выпусками и подвыпусками?
- Что представляют сбой «мягкие» и «жесткие» квоты?
- Когда можно превысить «жесткую» квоту?
- Что такое преобразование квоты резервного копирования?
- Каким образом доступность функционального пакета влияет на доступность установщика в консоли службы?

2.1.1 Службы и функциональные пакеты

2.1.1.1 Службы

Облачная служба – это набор функций, размещенных в Киберпротект, на площадке партнера или в частном облаке клиента. Как правило, службы оплачиваются по мере использования.

2.1.1.2 Элементы предложения

Функциональный пакет – это набор функций служб, сгруппированных по определенному типу рабочих нагрузок и функциональности. При включении того или иного функционального пакета вы выбираете рабочие нагрузки для защиты, указываете количество рабочих нагрузок для защиты (посредством квот) и уровень защиты, который будет доступен для ваших партнеров, клиентов и их конечных пользователей (посредством включения или отключения дополнительных пакетов защиты).

Данные об использовании функций собираются со служб и отображаются в функциональных пакетах, которые используются в отчетах.

2.1.1.3 Выпуски

В выпусках на одну рабочую нагрузку можно включить один функциональный пакет.

Выпуски можно использовать для настройки служб, доступных для тенантов. Для каждого тенанта Клиент можно выбрать только один выпуск. Поэтому для применения разных функций службы необходимо создать несколько тенантов для пользователя.

Чтобы ограничить использование служб в функциональном пакете, можно определить квоты для данного функционального пакета. См. раздел "Мягкие и жесткие квоты" (стр. 7).

2.1.2 Мягкие и жесткие квоты

Квоты позволяют установить ограничения на использование службы для тенанта. Чтобы задать квоты, выберите тенант на вкладке **Клиенты**, затем откройте вкладку службы и щелкните **Изменить**.

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 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 службы.

Квота с указанным значением "unlimited" считается **мягкой**.

Пример

Мягкая квота. Для количества рабочих станций вы установили квоту, равную 20. Когда количество защищенных рабочих станций клиента достигнет 20, он получит соответствующее уведомление по электронной почте, но служба Кибер Бэкап останется доступной 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, служба будет отключена.

2.1.2.1 Уровни, на которых можно задать квоты

Уровни, на которых можно задать квоты, перечислены в таблице ниже.

Тенант/пользователь	Мягкая квота (только квота)	Жесткая квота (квота и превышение)
Партнер	да	нет
Папка	да	нет
Клиент	да	да
Отдел	нет	нет
Пользователь	да	да

Мягкие квоты можно задать на уровне партнера и папки. На уровне отдела квоты не задаются. Жесткие квоты можно задать на уровне клиента и пользователя.

Общий объем жестких квот, который задан на уровне пользователя, не может превышать соответствующий объем жесткой квоты для клиента.

2.1.2.2 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 устройств

- **Рабочие станции**
- **Серверы**
- **Виртуальные машины**

Машина или сервер считаются защищенными, если к ним применен 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**

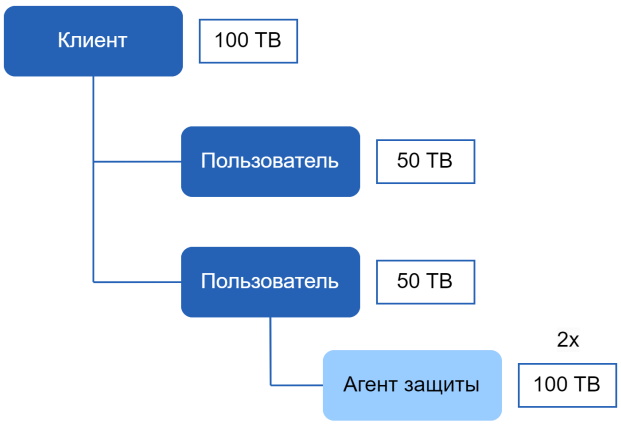
  Квота **Локальное резервное копирование** ограничивает общий размер локальных резервных копий, созданных с использованием облачной инфраструктуры. Для этой квоты нельзя задать превышение.
- **Облачные ресурсы**

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

Превышение жесткой квоты для хранилища резервных копий

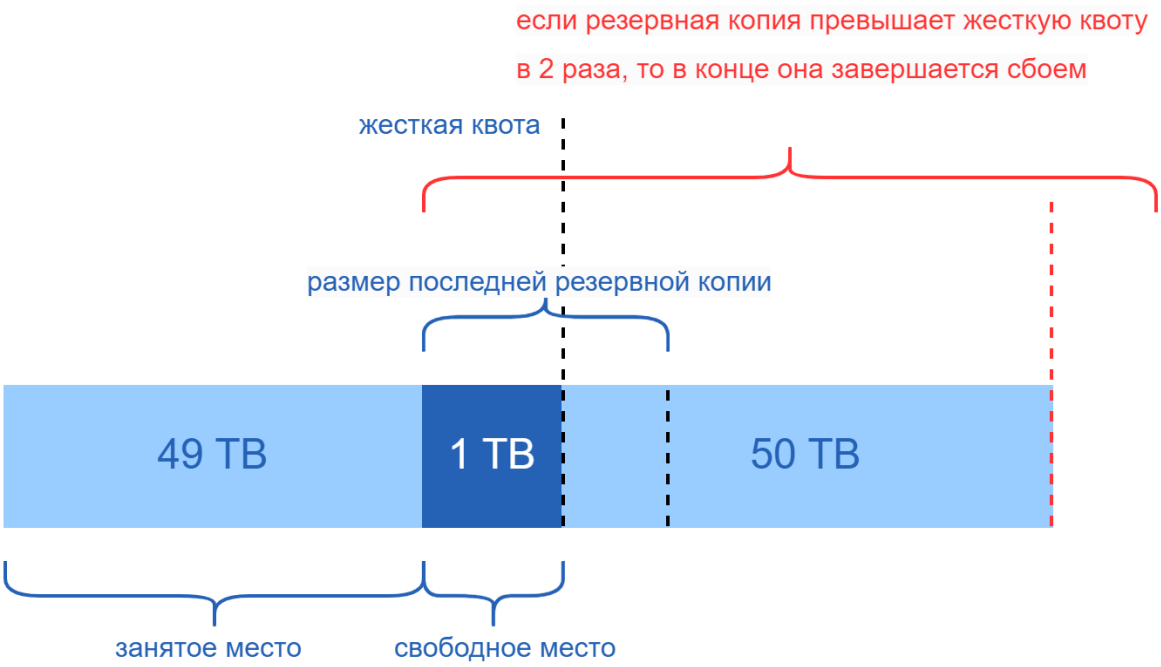
Для хранилища резервных копий жесткую квоту можно превысить в два раза от определенной жесткой квоты. Сертификат агента защиты имеет техническую квоту двойного объема, которая позволяет агенту превышать жесткую квоту тенанта, когда она еще не достигнута во время выполнения резервного копирования. Если квота тенанта превышена, невозможно будет создать следующую резервную копию. Если при создании резервной копии достигнуто удвоенное значение квоты (в сертификате), процесс резервного копирования завершится сбоем.

Пример: Вы задали для тенанта жесткую квоту облачного хранения данных, равную 100 ТБ. Это означает, что общая сумма жестких квот, выделенных тенантам пользователь, не может превышать 100 ТБ. Вы решили разделить жесткую квоту между двумя пользователями поровну. Это означает, что с технической точки зрения агент каждого пользователя имеет 100 ТБ технической квоты. Но это не означает, что агент может создавать резервные копии машин до достижения 100 ТБ. Если жесткая квота почти достигнута на момент запуска создания резервной копии, то резервная копия будет создана, если ее размер позволит уложиться в удвоенную жесткую квоту.



На представленной ниже схеме пользователь имеет 1 ТБ бесплатного места, но размер резервной копии больше (например, 3 ТБ). В этом случае резервная копия будет успешно создана, даже если жесткая квота на место в облачном хранилище данных будет превышена на 2 ТБ. Если

создаваемая резервная копия имеет размер 53 ТБ, то ее создание запустится, но завершится сбоем по достижении ограничения на место в облачном хранилище данных (100 ТБ).



Трансформация квоты резервного копирования

В целом, эта тема посвящена процедурам получения квоты резервного копирования и назначения функциональных пакетов соответствующим типам ресурсов: система сравнивает доступные функциональные пакеты с типом ресурса, а затем получает квоту для подходящего функционального пакета.

Кроме того, есть возможность назначить другую квоту функционального пакета, даже если в точности не соответствует типу ресурса. Этот процесс называется **трансформация квоты резервного копирования**. При отсутствии соответствующего функционального пакета система пытается найти более дорогостоящую подходящую квоту для типа ресурса (автоматическая трансформация квоты резервного копирования). Если ничего подходящего не найдено, можно вручную назначить квоту службы типу ресурса в консоли службы.

Пример

Вы планируете создать резервную копию виртуальной машины (рабочая станция, на основе агента).

Сначала система проверит, есть ли выделенная квота **Виртуальные машины**. Если эта квота не будет найдена, система автоматически попытается получить квоту **Рабочие станции**. Если не удастся найти и эту квоту, другая квота не будет автоматически получена. Если в достаточном объеме есть более дорогая квота, чем квота **Виртуальные машины**, и она применима к виртуальной машине, можно войти на консоль службы и назначить квоту **Серверы** вручную.

2.1.3 Доступные установщики агента в зависимости от функциональных пакетов

Установщики агента, которые доступны в разделе **Добавить устройства** в консоли службы, зависят от разрешенных функциональных пакетов. В приведенной ниже таблице перечислены установщики агента и указана их доступность в консоли службы в зависимости от активированных функциональных пакетов.

Активированный функциональный пакет Установщик агента	Серверы	Рабочие станции	Виртуальные машины
Рабочие станции: агент для Windows		+	+
Рабочие станции: агент для Mac OS		+	+
Серверы: агент для Windows	+		+
Серверы: агент для Linux	+		+
Агент для Hyper-V			+
Агент для VMware			+
Агент для SQL	+		+
Агент для Exchange	+		+
Агент для Active Directory	+		+
Полный установщик для Windows	+	+	+

2.2 Учетные записи пользователя и тенанты

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.

Каждая учетная запись принадлежит тенанту. Тенант – это составная часть ресурсов портала управления (например, учетные записи пользователей и дочерние тенанты) и предложений службы (включенные службы и элементы предложения в них), которая относится к тому или иному партнеру или клиенту. Иерархия тенантов должна соответствовать отношениям "клиент-поставщик" между пользователями и поставщиками услуг.

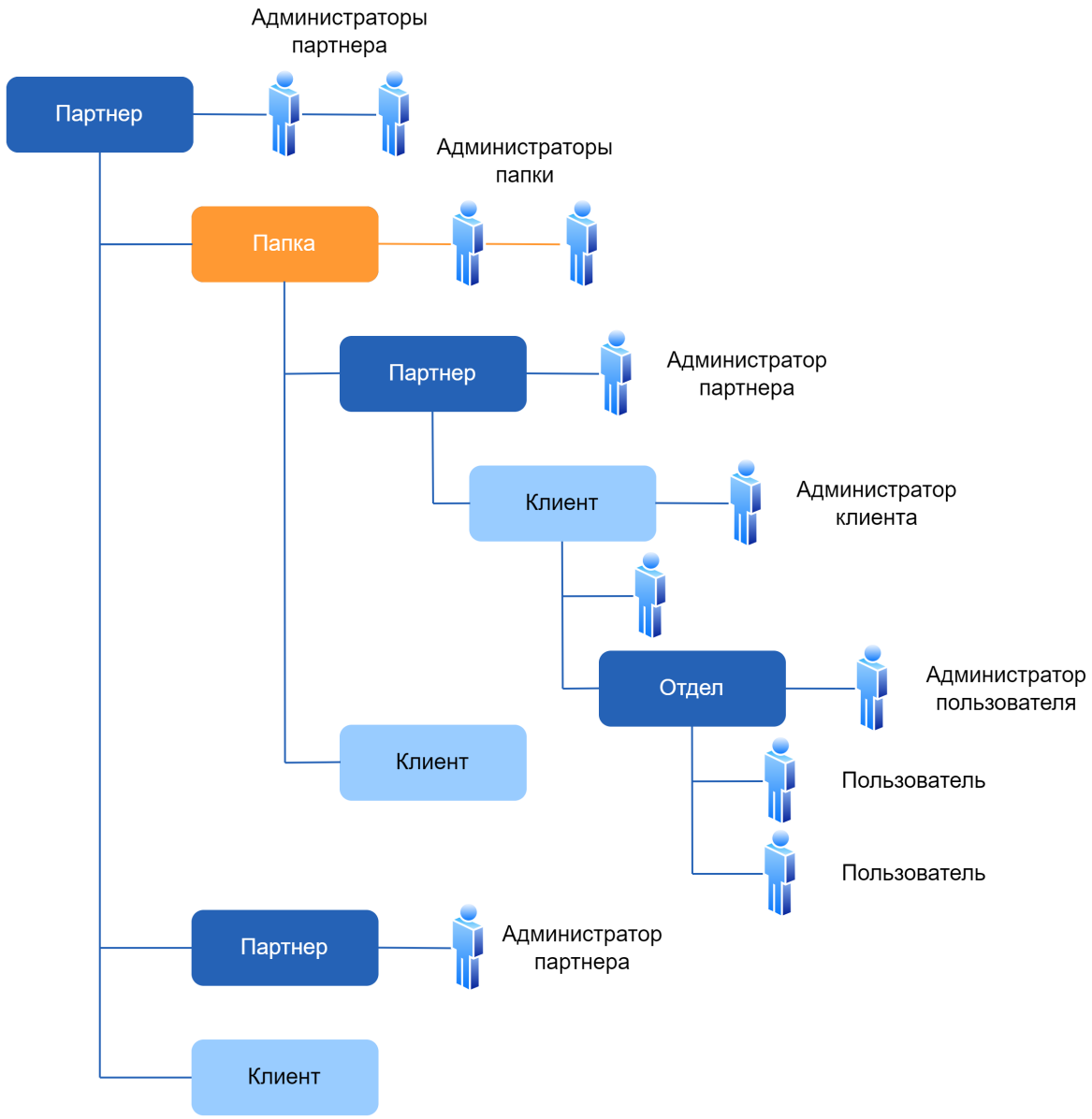
- Тип тенанта **Партнер** обычно соответствует поставщикам услуг, которые являются торговыми посредниками по продаже услуг.

- Тип тенанта **Папка** – это дополнительный тенант, который обычно используется администраторами партнера для группирования партнеров и пользователей с целью настройки отдельных предложений и (или) другого фирменного оформления.
- Тип тенанта **Клиент** обычно относится к организациям, которые используют службы.
- Тип тенанта **Отдел** обычно относится к отделам или подразделениям в организации.

Администратор может создавать тенанты, учетные записи администратора и пользователя (а также управлять ими) на своем уровне иерархии или на уровнях ниже.

Администратор родительского тенанта типа **Партнер** может действовать как администратор нижнего уровня в тенантах типа **Клиент** или **Партнер** с режимом управления **Под управлением поставщика услуг**. Поэтому администратор на уровне партнера может, например, управлять учетными записями пользователей и службами или получать доступ к резервным копиям и другим ресурсам в дочернем тенанте. Однако администратор более низкого уровня может ограничить доступ к своим клиентам для администраторов более высокого уровня.

На указанной ниже диаграмме показан образец иерархии тенантов – партнер, папка, клиент и отдел.



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

Операция	Пользователи	Администраторы тенантов Клиент и Отдел	Администраторы тенантов Партнер и Папка
Создание тенантов	Нет	Да	Да
Создание учетных записей	Нет	Да	Да
Загрузка и установка программного обеспечения	Да	Да	Нет*
Управление службами	Да	Да	Да
Создание отчетов об	Нет	Да	Да

использовании служб			
Настройка фирменного оформления	Нет	Нет	Да

*Администратор Партнера, которому необходимо выполнить эти операции, может создать администратора Клиента или учетную запись пользователя для себя.

2.3 Поддерживаемые веб-браузеры

Веб-интерфейс платформы резервного копирования поддерживает перечисленные ниже браузеры:

- Google Chrome 29 или более поздней версии
- Mozilla Firefox 23 или более поздней версии
- Opera 16 или более поздней версии
- Windows Internet Explorer 11 или более поздней версии
- Microsoft Edge 25 или более поздней версии
- В операционных системах macOS и iOS выполняется Safari 8 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 Использование портала управления

Приведенные ниже пошаговые инструкции помогут выполнить основные операции на портале управления.

3.1 Активация учетной записи администратора

После подписания партнерского соглашения вы получите сообщение электронной почты со следующей 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

1. Перейдите на страницу входа в службу.
   Адрес страницы входа был указан в электронном письме со сведениями об активации.
2. Введите имя пользователя и щелкните **Далее**.
3. Введите пароль и щелкните **Далее**.

   Примечание
   Для защиты Киберпротект Кибер Бэкап Облачный от атак методом подбора портал заблокирует вас после 10 неудавшихся попыток входа. Период блокировки составляет 5 минут. Количество неудавшихся попыток входа сбрасывается через 15 минут.

4. Используйте меню справа для перехода к порталу управления.

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

Некоторые службы предоставляют возможность перейти на портал управления с консоли службы.

3.3 Навигация на портале управления

Используя портал управления, в каждый данный момент времени вы работаете в рамках одного тенанта. Это указано в верхнем левом углу.

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

Во всех части пользовательского интерфейса будет отображаться только тот клиент, в котором вы работаете в данный момент. Пример:

- На вкладке **Клиенты** отображаются только тенанты, дочерние для тенанта, в котором вы работаете в настоящий момент.
- На вкладке **Пользователи** отображаются только учетные записи пользователей в тенанте, в котором вы работаете в настоящий момент.
- Кнопка **Создать** позволяет создать тенант или новую учетную запись пользователя только в том тенанте, в котором вы работаете в настоящий момент.

3.4 Доступ к службам

3.4.1 Вкладка «Обзор»

В разделе **Обзор** gt; **Использование** предоставлен обзор использования служб. В нем также можно получить доступ к службам в тенанте, в котором вы работаете.

Порядок управления службой для клиента на вкладке «Обзор»

1. Найдите тенант, для которого необходимо выполнить управление службой, затем щелкните **Обзор** gt; **Использование**.

   Обратите внимание, что одними службами можно управлять на уровне тенанта партнера и тенанта пользователя, а другими – только на уровне тенанта пользователя.
2. Щелкните имя службы, для которой нужно выполнить операции управления, затем щелкните **Управление службой** или **Настроить службу**.

   Информацию об использовании служб см. в руководствах пользователей, которые доступны на консолях служб.

3.4.2 Вкладка «Клиенты»

На вкладке **Клиенты** отображаются дочерние тенанты, в которых вы работаете. На ней также можно получить доступ к службам в этих тенантах.

Порядок управления службой для клиента на вкладке «Клиенты»

1. Выполните одно из следующих действий:
   - Откройте вкладку **Клиенты**, выберите тенант, для которого необходимо выполнить операции управления службой, щелкните имя или значок искомой службы и щелкните **Управление службой** или **Настроить службу**.
   - Откройте вкладку **Клиенты**, щелкните значок многоточия рядом с именем тенанта, для которого необходимо выполнить операции управления службой, щелкните **Управление службой**, затем выберите искомую службу.

   Обратите внимание, что одними службами можно управлять на уровне тенанта партнера и тенанта пользователя, а другими – только на уровне тенанта пользователя.

   Информацию об использовании служб см. в руководствах пользователей, которые доступны на консолях служб.

3.5 Создание и настройка тенантов

В Кибер Бэкап Облачный доступны указанные ниже тенанты:

- Клиент **Партнер** обычно создается для каждого партнера, который подписывает партнерское соглашение.
- Клиент **Папка** обычно создается для группировки партнеров и пользователей с целью настройки отдельных предложений и (или) другого фирменного оформления.
- Клиент **Пользователь** обычно создается для каждой организации, которая регистрируется в службе.
- Для распространения службы на новую организацию в клиенте пользователя создается новый клиент **Отдел**.

Конкретные этапы по созданию и настройке тенанта зависят от создаваемого тенанта, но в общем процесс состоит из следующих этапов:

1. Создайте тенант.
2. Выберите службы для данного тенанта.
3. Настройте функциональные пакеты для тенанта.

3.5.1 Создание тенанта

1. Войдите на портал управления.
2. Найдите тенант, в котором необходимо создать новый тенант.
3. В верхнем правом углу щелкните **Создать**, а затем выберите щелчком мыши один из указанных ниже пунктов, в зависимости от типа тенанта, который необходимо создать:
   - Клиент **Партнер** обычно создается для каждого партнера, который подписывает партнерское соглашение.
   - Клиент **Папка** обычно создается для группировки партнеров и пользователей с целью настройки отдельных предложений и (или) другого фирменного оформления.
   - Клиент **Пользователь** обычно создается для каждой организации, которая регистрируется в службе.
   - Для распространения службы на новую организацию в клиенте пользователя создается новый клиент **Отдел**.

   Набор доступных вариантов зависит от типа родительского тенанта.
4. В поле **Имя** укажите название нового клиента.
5. [Только при создании тенанта клиента] В поле **Режим** укажите, как именно (в пробном или рабочем режиме) тенант будет использовать службы. В ежемесячные отчеты об использовании не включаются данные для тенантов, работающих в пробном режиме.

Внимание
При переходе с пробного режима на рабочий в течение месяца в отчет будут включены данные об использовании службы за весь месяц. По этой причине мы рекомендуем перевести режим в первый день месяца. Пробный режим автоматически переводится в рабочий режим после того, как тенант использует его в течение одного полного месяца.

6. В разделе **Режим управления** выберите один из следующих режимов для управления доступом к клиенту:
   - **Самообслуживание**: в этом режиме для администраторов родительского тенанта ограничен доступ к этому тенанту – они могут только изменять свойства тенанта, но не могут получить доступ к объектам внутри (тенанты, пользователи, службы, резервные копии и другие ресурсы) и управлять ими.
   - **Под управлением поставщика услуг**: в этом режиме тенанту, который используется для администраторов родительского тенанта, предоставляется полный доступ – изменение свойств, управление тенантами, пользователями, службами, доступ к резервным копиям и другим ресурсам.

   Только администратор тенанта, созданного вами, сможет изменить режим управления с используемого режима **Самообслуживание**. Для этого администратору созданного тенанта нужно выбрать **Настройки** > **Безопасность** и установить переключатель **Доступ для службы поддержки**.

   Чтобы просмотреть выбранный режим управления для дочерних тенантов, откройте **Клиенты**.
7. В разделе **Безопасность** включите или отключите двухфакторную проверку подлинности для тенанта.
   Если она включена, всем пользователям этого тенанта необходимо будет настроить двухфакторную аутентификацию для своих учетных записей, чтобы повысить уровень безопасности доступа. Пользователи должны установить приложение проверки подлинности на своих устройствах второго фактора и использовать одноразовый сгенерированный код TOTP вместе с обычными учетными данными для входа на консоль. Дополнительную информацию см. в разделе "Настройка двухфакторной проверки подлинности". Чтобы просмотреть статус двухфакторной проверки подлинности для ваших клиентов, откройте раздел **Клиенты**.
8. [Только при создании тенанта пользователя в режиме «Улучшенная безопасность»] В разделе **Безопасность** установите флажок **Улучшенная безопасность**.
   В этом режиме разрешено создавать только зашифрованные резервные копии. На защищенном устройстве нужно задать пароль шифрования. В противном случае создание резервных копий завершится сбоем. Все операции, которые требуют пароль шифрования для облачной службы, недоступны.

   Внимание
   После создания тенанта невозможно отключить режим «Улучшенная безопасность».
9. В разделе **Создать администратора** введите имя входа и электронную почту для учетной записи администратора.

Язык можно не выбирать. В этом случае по умолчанию будет использоваться английский язык.

Примечание
Если для параметра **Режим управления** задано значение **Самообслуживание**, то для тенанта пользователя и тенанта партнера необходимо создать администратора.

10. В поле **Язык** измените язык по умолчанию для уведомлений, отчетов и программного обеспечения, который будет использоваться в тенанте.
11. Выполните одно из следующих действий:
    - Чтобы завершить создание тенанта, щелкните **Сохранить и закрыть**. В этом случае все функциональные пакеты будут включены для тенанта с неограниченной квотой.
    - Чтобы настроить функциональные пакеты для тенанта, щелкните **Далее**. См. раздел "Настройка функциональных пакетов для тенанта" (стр. 20).

3.5.2 Режим улучшенной безопасности

Режим улучшенной безопасности предназначен для клиентов с повышенными требованиями к безопасности. Этот режим требует обязательного шифрования для всех резервных копий и позволяет использовать только локально установленные пароли шифрования.

В режиме улучшенной безопасности все резервные копии, созданные в тенанте клиента и его отделах, автоматически шифруются с помощью алгоритма AES и 256-разрядного ключа. Пользователи могут устанавливать пароли шифрования только на защищаемых устройствах и не могут устанавливать их в планах защиты.

Внимание
Администратор партнера может включить режим улучшенной безопасности только при создании нового тенанта клиента и не может отключить этот режим позже. Включение режима повышенной безопасности для уже существующих тенантов невозможно.

3.5.2.1 Ограничения

- Режим улучшенной безопасности совместим только с агентами версии 15.0.26390 или более поздней.
- Режим улучшенной безопасности недоступен для устройств под управлением Red Hat Enterprise Linux 4.x или 5.x и их производных.
- Облачные службы не могут получить доступ к паролям шифрования. Из-за этого ограничения некоторые функции недоступны для тенантов в режиме улучшенной безопасности.

3.5.2.2 Неподдерживаемые функции

Следующие функции недоступны для тенантов в режиме улучшенной безопасности:

- Восстановление через консоль Кибер Бэкап
- Просмотр резервных копий на уровне файлов через консоль Кибер Бэкап

- Резервное копирование из облака в облако
- Резервное копирование приложений
- Сканирование резервных копий на наличие вредоносных программ
- Безопасное восстановление
- Автоматическое создание корпоративных белых списков
- Карта защиты данных
- Отчеты и панели мониторинга, связанные с недоступными функциями

3.5.3 Настройка функциональных пакетов для тенанта

При создании нового тенанта включаются все функциональные пакеты. Можно выбрать функциональные пакеты, которые будут доступны пользователям в тенанте, и его дочерних тенантах, а также задать квоты для них.

Эта процедура неприменима к тенанту отдела.

Порядок настройки функциональных пакетов для тенанта

1. В разделе **Настроить службы** диалогового окна создания/изменения тенанта на каждой вкладке службы снимите флажки для функциональных пакетов, которые необходимо отключить.
   Функциональность, которая соответствует отключенным функциональным пакетам, будет недоступна для пользователей в тенанте и его дочерних тенантах.
2. Выберите хранилища данных, которые будут доступны для нового тенанта. Хранилища данных группируются по расположениям. Их можно выбрать из списка расположений и хранилищ данных, которые доступны для тенанта.
   - При создании тенанта партнера/папки можно выбрать несколько расположений и хранилищ данных для каждой службы.
   - При создании тенанта пользователя необходимо выбрать одно расположение, после чего выбрать одно хранилище данных на каждую службу в этом расположении. Хранилища данных, назначенные тенанту, можно изменить позже, но только в том случае, если их использование составляет 0 ГБ, т. е. до того, как клиент начнет их использовать, или после того, как клиент удалит все резервные копии из этого хранилища. Информация об использовании пространства хранилища данных не обновляется в реальном времени. Информация обновится по истечении периода времени до 24 часов.

   Дополнительную информацию о хранилищах данных см. в разделе Управление расположениями и хранилищами данных.
3. Чтобы указать квоту для элемента, щелкните ссылку **Без ограничений** рядом с функциональным пакетом.
   Это «мягкие» квоты. При превышении любого из этих значений администраторам тенанта и администраторам родительского тенанта отправляется уведомление по электронной почте. Ограничения на использование служб не применяются. Для тенанта партнера использование

функционального пакета может превысить квоту по той причине, что ее превышение невозможно задать при создании тенанта партнера.

4. [Только при создании тенанта пользователя] Укажите превышения квоты.
   Превышение позволяет тенанту пользователя превысить квоты на указанное значение. При выходе за пределы значения превышения применяются ограничения на использование соответствующей службы.
5. Щелкните **Сохранить и закрыть**.

Новый созданный тенант появляется на вкладке **Клиенты** консоли управления.

Чтобы внести изменения в настройки тенанта или сменить администратора, выберите тенант на вкладке **Клиенты**, а затем щелкните значок карандаша в том разделе, который нужно изменить.

3.6 Отключение и включение тенанта

Иногда требуется временно отключить тенант. Например, если у него возникла задолженность по услугам.

Порядок отключения тенанта

1. На портале управления перейдите в раздел **Клиенты**.
2. Выберите тенант, который необходимо отключить, и щелкните значок многоточия gt; **Отключить**.
3. Подтвердите свое действие, щелкнув **Отключить**.

В результате:

- Тенант и все его дочерние тенанты будут отключены, и все их службы будут приостановлены.
- При этом арендатору и его субарендаторам будут по-прежнему выставляться счета, поскольку их данные будут храниться в Кибер Бэкап Облачный.
- Все клиенты API в клиенте и его субклиентах будут отключены, и все интеграции, использующие эти клиенты, прекратят работу.

Чтобы включить арендатора, выберите его в списке клиентов, затем щелкните значок многоточия > **Включить**.

3.7 Удаление тенанта

Допустим, вы решили удалить тенант, чтобы освободить используемые им ресурсы. Статистика использования будет обновлена в течение одного дня после удаления. Для крупных тенантов это может занять больше времени.

Перед удалением тенанта его необходимо отключить. Инструкцию об удалении тенанта см. в разделе Включение и отключение тенанта.

Внимание
Удаление тенанта необратимо.

Порядок удаления тенанта

1. На портале управления перейдите в раздел **Клиенты**.
2. Выберите тенант, щелкните значок многоточия > **Удалить**.
3. Чтобы подтвердить действие, введите учетные данные и щелкните **Удалить**.

В результате:

- Тенант и его дочерние тенанты будут удалены.
- Все службы, которые были включены в тенанте и его дочерних тенантах, будут остановлены.
- Все пользователи в тенанте и его дочерних тенантах будут удалены.
- Будет отменена регистрация всех машин в тенанте и его дочерних тенантах.
- Все данные, относящиеся к службе, например, резервные копии и синхронизированные файлы, в тенанте и его дочерних тенантах будут удалены.
- Все клиенты API в тенанте и его дочерних тенантах будут удалены, все интеграции, использующие эти тенанты, прекратят работу.

3.8 Создание учетной записи пользователя

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

- Учетные записи администратора партнера/папки: чтобы делиться обязанностями по управлению службами с другими пользователями.
- Учетные записи администратора пользователи/отдела: для делегирования управления службами другим пользователям, для которых права доступа будут жестко ограничены рамками соответствующего пользователя/отдела.
- Учетные записи в тенантах пользователя или отдела: чтобы включить для пользователей только доступ к поднабору служб.

Имейте в виду, что существующие учетные записи невозможно переместить между тенантами. Сначала необходимо создать тенант, а затем заполнить его учетными записями.

Порядок создания учетной записи пользователя

1. Войдите на портал управления.
2. Найдите тенант, в котором необходимо создать учетную запись пользователя.
3. В верхнем правом углу последовательно выберите пункты **Создать** > Пользователь.
4. Укажите приведенные ниже контактные данные для учетной записи:

- **Имя для входа**

  Внимание
  У каждой учетной записи должно быть уникальное имя входа.

- **Электронная почта**
- Необязательно:**Имя**
- Необязательно: **Фамилия**
- В поле **Язык** измените язык, который по умолчанию используется для уведомлений, отчетов и программного обеспечения для этой учетной записи.

5. [Недоступно при создании учетной записи в тенанте партнера/папки] Выберите службы, к которым пользователь будет иметь доступ и роли в каждой службе.

   Доступные службы зависят от служб, включенных для тенанта, в котором создана учетная запись пользователя.

   - Если установить флажок **Администратор компании**, пользователь будет иметь доступ к порталу управления и роль администратора во всех службах, которые в данный момент включены для данного тенанта. Пользователь также будет иметь роль администратора во всех службах, которые будут включены для тенанта в будущем.
   - Если установлен флажок **Администратор отдела**, у пользователя будет доступ к порталу управления. При этом, в зависимости от службы, пользователь может иметь или не иметь роль администратора.
   - В противном случае пользователь будет иметь роли, которые выбраны 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 (недоступно для администраторов партнера/папки) для пользователя, выберите его на вкладке **Пользователи**, а затем щелкните значок карандаша в том разделе, который нужно изменить.

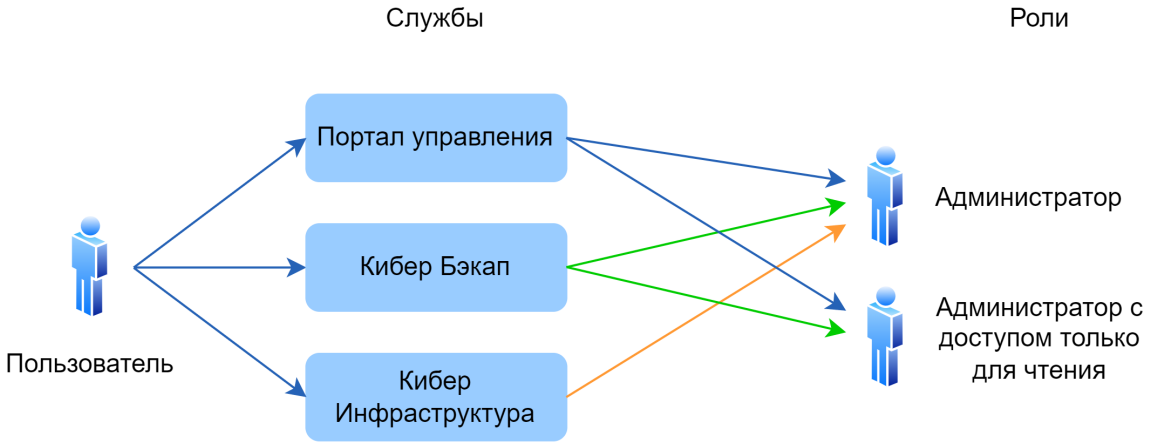
Порядок сброса пароля пользователя

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

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

3.9 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.

Служба	Роль	Описание
Недоступно	Администратор компании	Эта роль предоставляет права администратора для всех служб. Эта роль позволяет получить доступ к корпоративному белому списку.
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".
Кибер Бэкап	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".
Кибер Инфраструктура	Администратор	Эта роль позволяет настраивать службу Кибер Инфраструктура и управлять ею для ваших пользователей.

3.9.1 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

3.10 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 для каждого устройства.
- **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 отчета зависит от рабочей нагрузки центра обработки данных. Если по состоянию на тот момент времени не было никаких активных оповещений, краткие сведения не отправляются. 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.
- **Уведомления функции "Контроль устройств"** (выключено по умолчанию)

  Уведомления о попытках использовать периферийные устройства и порты, доступ к которым ограничен в соответствии с планами защиты с включенным модулем контроля устройств.

Все уведомления отправляются на адрес электронной почты пользователя.

3.10.1 Уведомления, полученные ролью пользователя

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

Тип оповещения\Роль пользователя	Пользователь	Администраторы компании и отдела	Администратор партнера и папки
Уведомления для собственных устройств	Да	Да	недоступно*
Уведомления для всех устройств дочерних тенантов	Недоступно	Да	Да

* Администраторы партнера не могут регистрировать собственные устройства, но могут создавать собственные учетные записи администратора клиента и использовать их для добавления собственных устройств. См. раздел Учетные записи пользователя и тенанты.

3.11 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**.

3.12 Удаление учетной записи пользователя

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

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

Внимание
Удаление учетной записи пользователя необратимо.

Порядок удаления учетной записи пользователя

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

В результате:

- Учетная запись пользователя будет удалена.
- Все данные этой учетной записи пользователя будут удалены.
- Для всех машин, связанных с этой учетной записью пользователя, будет отменена регистрация.

3.13 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.

3.14 Настройки двухфакторной проверки подлинности

Двухфакторная проверка подлинности (2FA) – это тип многофакторной проверки подлинности, обеспечивающий идентификацию пользователей с помощью комбинации двух различных факторов.

- Фактор знания, что-то, что пользователь знает (PIN-код или пароль)
- Фактор владения, что-то, что пользователь имеет (токен)
- Фактор свойства, что-то, что является частью пользователя (биометрика)

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.

3.14.1 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.

3.14.2 Распространение настроек двухфакторной проверки подлинности на уровне тенанта

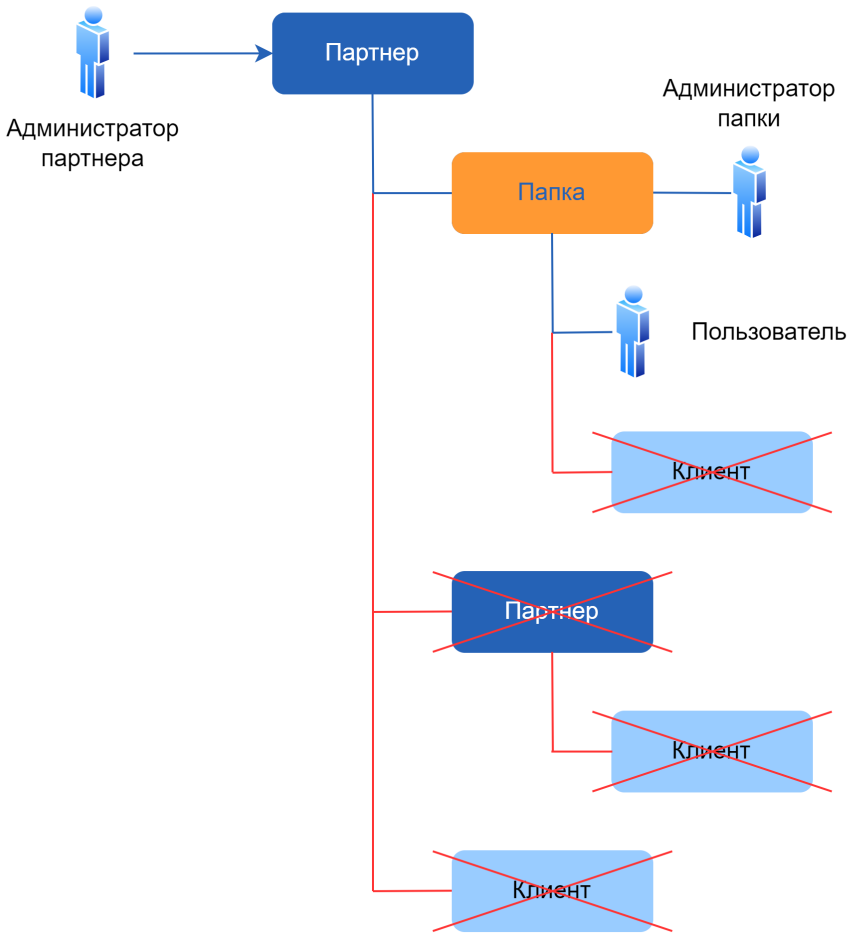
Двухфакторная проверка подлинности задается на уровне **организации**. Можно включить или отключить двухфакторную проверку подлинности.

- Для собственной организации.
- Для дочернего тенанта (только если у дочернего тенанта включен параметр **Доступ с целью поддержки**).

Настройки двухфакторной проверки подлинности распространяются по уровням тенанта следующим образом:

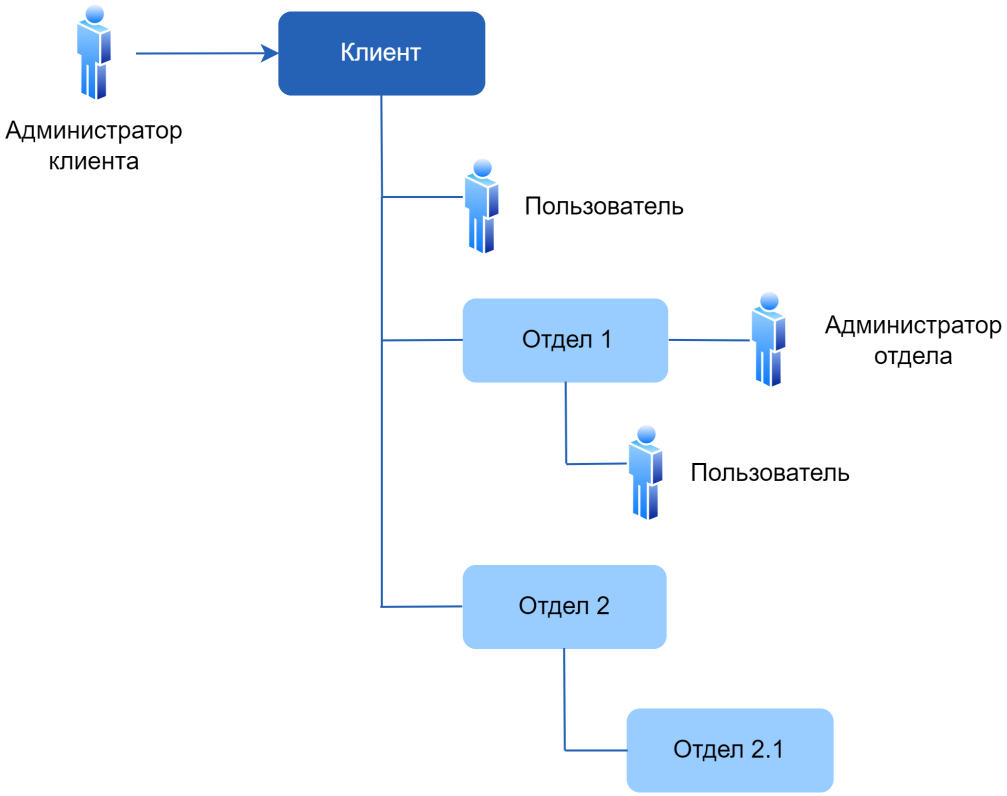
- Папки автоматически наследуют настройки двухфакторной проверки подлинности от организации партнера. На приведенной ниже схеме красными линиями обозначены направления, в которых распространение настроек двухфакторной проверки подлинности невозможно.

Распространение настроек двухфакторной проверки подлинности с уровня тенанта Партнер



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

Распространение настроек двухфакторной проверки подлинности с уровня тенанта Клиент



Примечание

1. Можно включить или выключить двухфакторную проверку подлинности для дочерней организации только в том случае, если у нее включен параметр **Доступ с целью поддержки**.
2. Можно изменять параметры двухфакторной проверки подлинности для дочерней организации только в том случае, если у нее включен параметр **Доступ с целью поддержки**.
3. Невозможно настроить двухфакторную проверку подлинности на уровне папки или отдела.
4. Настройки двухфакторной проверки подлинности можно сконфигурировать, даже если для родительской организации соответствующая настройка не включена.

3.14.3 Настройка двухфакторной проверки подлинности для вашего тенанта

3.14.3.1 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.

3.14.3.2 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**.

3.14.4 Управление двухфакторной проверкой подлинности для пользователей

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

3.14.4.1 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.

3.14.4.2 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.

3.14.4.3 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.

3.14.4.4 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 пользователей услуги 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.

3.14.4.5 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.

3.14.5 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.

3.14.6 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.

3.15 Управление расположениями и хранилищами данных

В разделе **Настройки** > **Расположения** отображаются облачные хранилища данных, которые можно использовать для предоставления службы **Кибер Бэкап** вашим партнерам и клиентам.

3.15.1 Расположения

Расположение – это контейнер, который позволяет удобно группировать облачные хранилища данных. Оно может иметь разные формы в зависимости от вашего выбора – от определенного центра обработки данных до географического расположения компонентов инфраструктуры.

Можно создать любое количество расположений и заполнить их хранилищами резервных копий. Расположение может содержать несколько облачных хранилищ данных.

Информацию об операциях с хранилищами данных см. в разделе «Управление хранилищем данных».

3.15.1.1 Выбор расположений и хранилищ данных для партнеров и клиентов

При создании тенанта партнера/папки для каждой службы в этом тенанте можно выбрать несколько расположений и хранилищ данных, которые будут доступны.

При создании тенанта клиента необходимо выбрать одно расположение, после чего выбрать одно хранилище данных на каждую службу в этом расположении. Хранилища данных, назначенные клиенту, можно изменить позже, но только в том случае, если их использование составляет 0 ГБ, т. е. до того, как клиент начнет их использовать, или после того, как клиент удалит все резервные копии из этого хранилища.

Информация о хранилищах данных, назначенных тенанту клиента, отображается на панели данных тенанта, когда тенант выбран на панели **Клиенты**. Информация об использовании пространства хранилища данных не обновляется в реальном времени. Информация обновится по истечении периода времени до 24 часов.

3.15.1.2 Операции с расположениями

Чтобы создать новое расположение, щелкните **Добавить расположение** и укажите его имя.

Чтобы переместить хранилище данных в другое расположение, выберите хранилище данных, в поле **Расположение** щелкните значок карандаша и выберите целевое расположение.

Чтобы переименовать расположение, щелкните значок многоточия рядом с именем расположения, выберите пункт **Переименовать** и укажите имя нового расположения.

Чтобы удалить расположение, щелкните значок многоточия рядом с именем расположения, выберите пункт **Удалить** и подтвердите свое решение. Удалить можно только пустые расположения.

3.15.2 Управление хранилищем данных

3.15.2.1 Добавление новых хранилищ данных

- Служба **Кибер Бэкап**:
  - По умолчанию хранилища резервных копий расположены в центрах обработки данных Киберпротект.
  - Если функциональный пакет **Хранилище резервных копий, которым владеет партнер** включен для тенанта партнера администратором более высокого уровня, администраторы партнера могут организовать хранилище данных в центре обработки данных партнера, используя программу Кибер Инфраструктура. Чтобы узнать, как организовать хранилище резервных копий в собственном центре обработки данных, откройте раздел **Расположения** и выберите пункт **Добавить хранилище резервных копий**.

  Примечание
  Невозможно проверить резервные копии в хранилищах объектов в общедоступных облаках, которые используются центрами обработки данных Киберпротект.
  Проверку можно выполнить для резервных копий в хранилищах объектов в общедоступных облаках, которые используются партнерами Киберпротект. Однако не рекомендуется ее включать, поскольку операции проверки повышают объем исходящего трафика от этих хранилищ объектов в общедоступном облаке. Это может привести к существенным затратам.

- За информацией о добавлении хранилищ данных, которые будут использоваться другими службами, обратитесь в службу технической поддержки Киберпротект по ссылке https://www.cyberprotect.ru/support.

3.15.2.2 Удаление хранилищ данных

Хранилища данных, добавленные вами или дочерними тенантами, можно удалить.

Если хранилище данных назначено какому-либо тенанту пользователя, то перед удалением хранилища данных необходимо отключить службу, которая использует его для всех тенантов пользователя.

Порядок удаления хранилища данных

1. Войдите на портал управления.
2. Найдите тенант, в который было добавлено хранилище данных.
3. Последовательно выберите пункты **Настройки** > **Расположения**.
4. Выберите хранилище данных, которое необходимо удалить.

5. На панели свойств хранилища данных щелкните значок многоточия и выберите пункт **Удалить хранилище**.
6. Подтвердите операцию.

3.16 Настройка фирменного оформления

В разделе **Настройки** > **Фирменное оформление** администраторы партнера могут настроить пользовательский интерфейс портала управления и службы **Кибер Бэкап**, чтобы удалить любую связь с Киберпротект или партнерами более высокого уровня.

Фирменное оформление можно настроить на уровнях партнера и папки. Фирменное оформление (там, где оно настроено) будет применяться ко всем прямым и непрямым дочерним партнерам/папкам и пользователям клиента.

Возможность настройки фирменного оформления для всех служб будет доступна в будущих выпусках. Некоторые службы обеспечивают отдельную возможность фирменного оформления. Дополнительную информацию см. в руководствах пользователей, которые доступны на консолях служб.

3.16.1 Элементы фирменного оформления

3.16.1.1 Вид

- **Имя службы**. Это имя используется во всех сообщениях электронной почты, которые отправляются порталом управления и облачными службами (сообщения активации учетной записи, сообщения электронной почты со служебными уведомлениями), на экране **приветствия** после первого входа, а также в качестве имени вкладки браузера портала управления.
- **Логотип**. Этот логотип отображается на портале управления и в службах. Щелкните логотип, чтобы передать файл изображения.
- **Цветовая схема**. Цветовая схема определяет комбинацию цветов, которая используется для всех элементов пользовательского интерфейса. Щелкните схему, а затем выберите одну из предварительно установленных схем, которая наилучшим образом соответствует вашим потребностям.

  Примечание
  Чтобы просмотреть, как будет выглядеть интерфейс для дочерних тенантов, щелкните **Предварительно просмотреть схему в новой вкладке**. Фирменное оформление не будет применяться до тех пор, пока не щелкнуть кнопку **Готово** на странице **Выбрать цветовую схему**.

- **Наш агент Кибер Бэкап Облачный под вашим брендом**. Этот параметр позволяет определить для всех дочерних партнеров и клиентов, будет ли агент Кибер Бэкап Облачный (для Windows, macOS и Linux) и Кибер Бэкап Облачный Monitor (для Windows, macOS и Linux) предоставляться под брендом Киберпротект или под вашим брендом. Если включить этот параметр, то агент и

индикатор в области уведомлений будут предоставляться под нашим брендом. Этот параметр влияет на имена и логотипы, используемые в установщике и Кибер Бэкап Облачный Monitor.

3.16.1.2 Документация и поддержка

- **URL-адрес домашней страницы**. Эта страница открывается, когда пользователь щелкает имя компании на панели **О программе**.
- **URL-адрес поддержки**. Эта страница открывается, когда пользователь переходит по ссылке **Обратиться за поддержкой** на панели О программе или в сообщении электронной почты, отправленном порталом управления.
- **Телефон службы поддержки**. Этот номер телефона показан на панели **О программе**.
- **URL-адрес базы знаний**. Эта страница открывается, когда пользователь переходит по ссылке **База знаний** в сообщении об ошибке.
- **Руководство администратора портала управления**. Эта страница открывается, если пользователь щелкает значок вопроса в верхнем правом углу пользовательского интерфейса портала управления, а затем последовательно выбирает пункты **О программе** > Руководство администратора.
- **Справка администратора портала управления**. Эта страница открывается, если пользователь щелкает значок вопроса в верхнем правом углу пользовательского интерфейса портала управления, а затем щелкает **Справка**.

3.16.1.3 Настройки юридических документов

- **URL лицензионного соглашения с конечным пользователем**. Эта страница открывается, когда пользователь после входа переходит по ссылке **Лицензионное соглашение** на панели **О программе** или экране **приветствия**.
- **URL-адрес условий использования платформы**. Эта страница открывается, когда администратор партнера после входа переходит по ссылке **Условия использования платформы** на панели **О программе** или экране **приветствия**.
- **URL-адрес заявления о конфиденциальности**. Эта страница открывается, когда пользователь после входа переходит по ссылке **Заявление о конфиденциальности** на экране **приветствия**.

Внимание
Чтобы документ не появлялся на экране приветствия, не вводите URL-адрес для него.

3.16.1.4 Настройки сервера электронной почты

Можно указать настраиваемый почтовый сервер, который будет использоваться для отправки уведомлений электронной почты с портала управления и служб. Чтобы указать настраиваемый сервер электронной почты, щелкните **Настраиваемый**, затем укажите следующие настройки:

- В поле **От** введите имя, которое будет отображаться в поле **От** уведомлений электронной почты.
- В поле **SMTP** введите имя сервера исходящей почты (SMTP).
- В поле **Порт** введите порт сервера исходящей почты. По умолчанию это порт 25.

- В поле **Шифрование** укажите, следует ли использовать шифрование SSL или TLS. Выберите **Нет**, чтобы отключить шифрование.
- В поле **Имя пользователя** и **Пароль** укажите учетные данные учетной записи, которая будет использоваться для отправки сообщений.

3.16.2 Настройка фирменного оформления

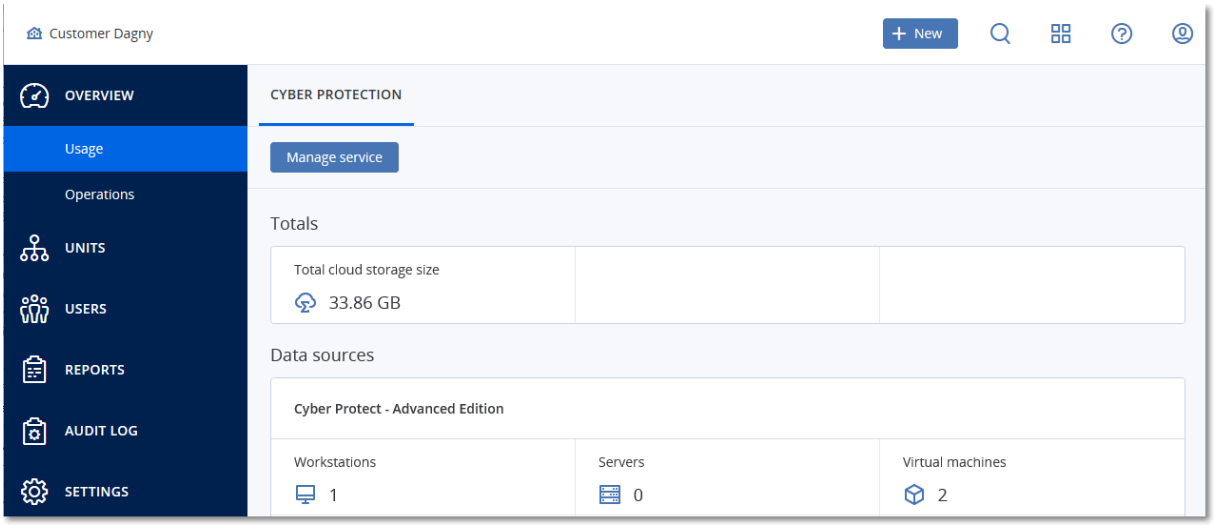
1. Войдите на портал управления.
2. Найдите тенант, в котором необходимо настроить форменное оформление.
3. Щелкните **Настройки** > **Фирменное оформление**.
4. Щелкните **Включить фирменное оформление**.
5. Выполните одно из следующих действий:
   - Настройте описанные выше элементы фирменного оформления.
   - Щелкните **Ребрендинг**, чтобы очистить все элементы фирменного оформления, за исключением следующих: **Имя службы**, **URL лицензионного соглашения с конечным пользователем**, **Руководство администратора портала управления**, **Справка администратора портала управления** и **Настройки сервера электронной почты**.
   - Щелкните **Восстановить настройки по умолчанию**, чтобы сбросить все элементы фирменного оформления к их значениям по умолчанию.

3.17 Мониторинг

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

3.17.1 Использование

На вкладке **Использование** предоставлен обзор использования служб. На ней также можно получить доступ к службам в тенанте, в которым вы работаете.



3.17.2 Операции

На панели мониторинга **Операции** есть несколько настраиваемых виджетов, которые позволяют выполнить обзор операций, относящихся к службе **Кибер Бэкап**.

По умолчанию данные отображаются для тенанта, в котором вы работаете. Можно изменить отображаемый тенант по отдельности для каждого виджета, отредактировав его. Также отображается сводная информация о прямых дочерних тенантах пользователя выбранного тенанта, включая тенанты расположенные в папках. На панели мониторинга *не* отображается информация о дочерних партнерах и их дочерних тенантах. Однако если преобразовать дочерний тенант партнера в тенант папки, информация о дочерних пользователях этого тенанта появится на панели мониторинга родительского тенанта.

Виджеты обновляются каждые две минуты. У виджетов есть активные элементы, на которые можно нажать для анализа возникших неполадок, их диагностики и устранения. Можно загрузить текущее состояние панели мониторинга в виде файла формата .pdf и (или) .xlsx либо же отправить эти данные по электронной почте на любой адрес, включая внешних получателей.

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 для разных тенантов или 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 период времени, выбрать тенант, для которого отображаются данные, 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 шестерни, когда виджет выбран. После изменения виджета щелкните **Готово**.

Порядок удаления виджета

Щелкните значок X рядом с именем виджета.

3.17.2.1 Статус защиты

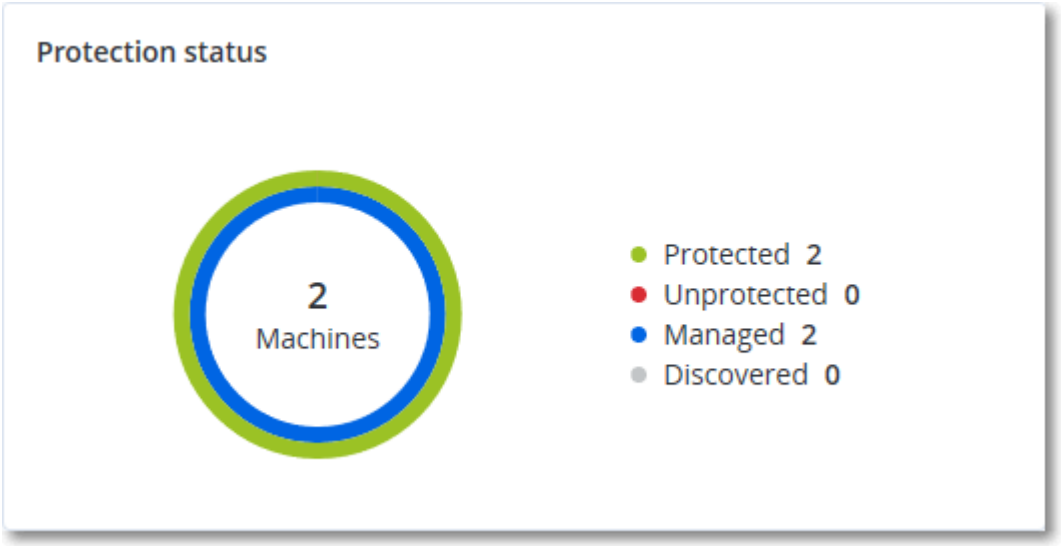
Статус защиты

В этом виджете показано текущее состояние защиты для всех машин.

Машина может быть в одном из следующих состояний:

- **Защищенные**: машины, для которых применен план защиты.
- **Незащищенные**: машины, для которых не применен план защиты. Под ними подразумеваются как обнаруженные, так и управляемые машины без примененного плана защиты.
- **Управляемое**: машины с установленным агентом защиты.
- **Обнаружено**: машины без установленного агента защиты.

Если щелкнуть состояние машины, для получения более подробной информации откроется список машин, которые имеют данное состояние.



Обнаруженные машины

В этом виджете показан список машин, обнаруженных за указанный период времени.

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

3.18 Отчеты

Чтобы создать отчеты об использовании служб и операциях, щелкните **Отчеты**.

3.18.1 Использование

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

3.18.1.1 Тип отчета

Можно выбрать один из указанных ниже типов отчета:

- **Текущее использование**

  В отчете содержатся показатели текущего использования службы.

  Показатели использования рассчитываются в рамках каждого расчетного периода каждого дочернего тенанта. Если включенные в отчет тенанты имеют другие расчетные периоды, показатели использования родительского тенанта могут отличаться от суммы показателей использования дочерних тенантов.
- **Текущее распределение использования**

  Этот отчет доступен только для тенантов партнера, которые управляются внешней системой распределения. Этот отчет полезен, когда периоды выставления счетов дочерних тенантов не совпадают с аналогичными периодами родительского тенанта. В отчете содержатся показатели использования службы для дочерних тенантов, рассчитанные за текущий период выставления счетов родительского тенанта. Использование родительского тенанта гарантированно равно сумме использований всех дочерних тенантов.
- **Сводка за период**

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

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

3.18.1.2 Область отчета

Можно выбрать область отчета из указанных ниже значений:

- **Непосредственные пользователи и партнеры**

  В отчете будут содержаться показатели использования службы только для непосредственных дочерних тенантов тенанта, в котором вы работаете.
- **Все пользователи и партнеры**

  В отчете будут содержаться показатели использования службы для всех дочерних тенантов того тенанта, в котором вы работаете.
- **Все клиенты, партнеры и пользователи**

В отчете будут содержаться показатели использования службы для всех дочерних тенантов того тенанта, в котором вы работаете, а также для всех пользователей в тенантах.

3.18.1.3 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 вашего тенанта, 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 тенанте самого верхнего уровня, который вам доступен.
3. Щелкните **Отчеты** > **Использование**.
4. Нажмите кнопку **Запланированные**.
5. Установите или снимите флажок **Отправлять ежемесячный сводный отчет**.
6. В разделе **Уровень детализации** выберите область отчета, как описано выше.

3.18.1.4 Настраиваемые отчеты

Отчет этого типа создается по требованию. Его рассылку нельзя запланировать. Отчет отправляется на ваш адрес электронной почты.

Порядок формирования настраиваемого отчета

1. Войдите на портал управления.
2. Выберите тенант, для которого необходимо создать отчет.
3. Щелкните **Отчеты** > **Использование**.
4. Откройте вкладку **Пользовательские**.
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**
   - **Пользовательские**
7. [Недоступно для отчета типа **Текущее использование**] Чтобы указать настраиваемый период создания отчетности, выберите начальную и конечную дату. В противном случае пропустите этот шаг.
8. В разделе **Уровень детализации** выберите область отчета, как описано выше.
9. Чтобы создать отчет, нажмите кнопку **Сформировать и отправить**.

3.18.2 Операции

Отчет об операциях может включать в себя любой набор виджетов **панели** мониторинга операций. По умолчанию во всех виджетах показана итоговая информация для тенанта, в которых вы работаете. Это можно изменить по отдельности для каждого виджета или для всех виджетов в настройках отчета. Во всех виджетах показаны параметры для одного диапазона времени. Этот диапазон можно изменить в настройках отчета.

Вы можете использовать отчеты по умолчанию или создать собственный отчет.

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

Ниже перечислены отчеты по умолчанию

Имя отчета	Описание
Оповещения	Показывает оповещения, выполненные за указанный период времени.
Ежедневные задания	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Обнаруженные машины	Показывает все найденные машины в сети организации.
Сводные данные	Показывает сводную информацию об устройствах, защищенных за указанный период времени.
Еженедельные действия	Показывает сводную информацию о действиях, выполненных за указанный период времени.

Для просмотра отчета щелкните его имя.

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

Добавление отчета

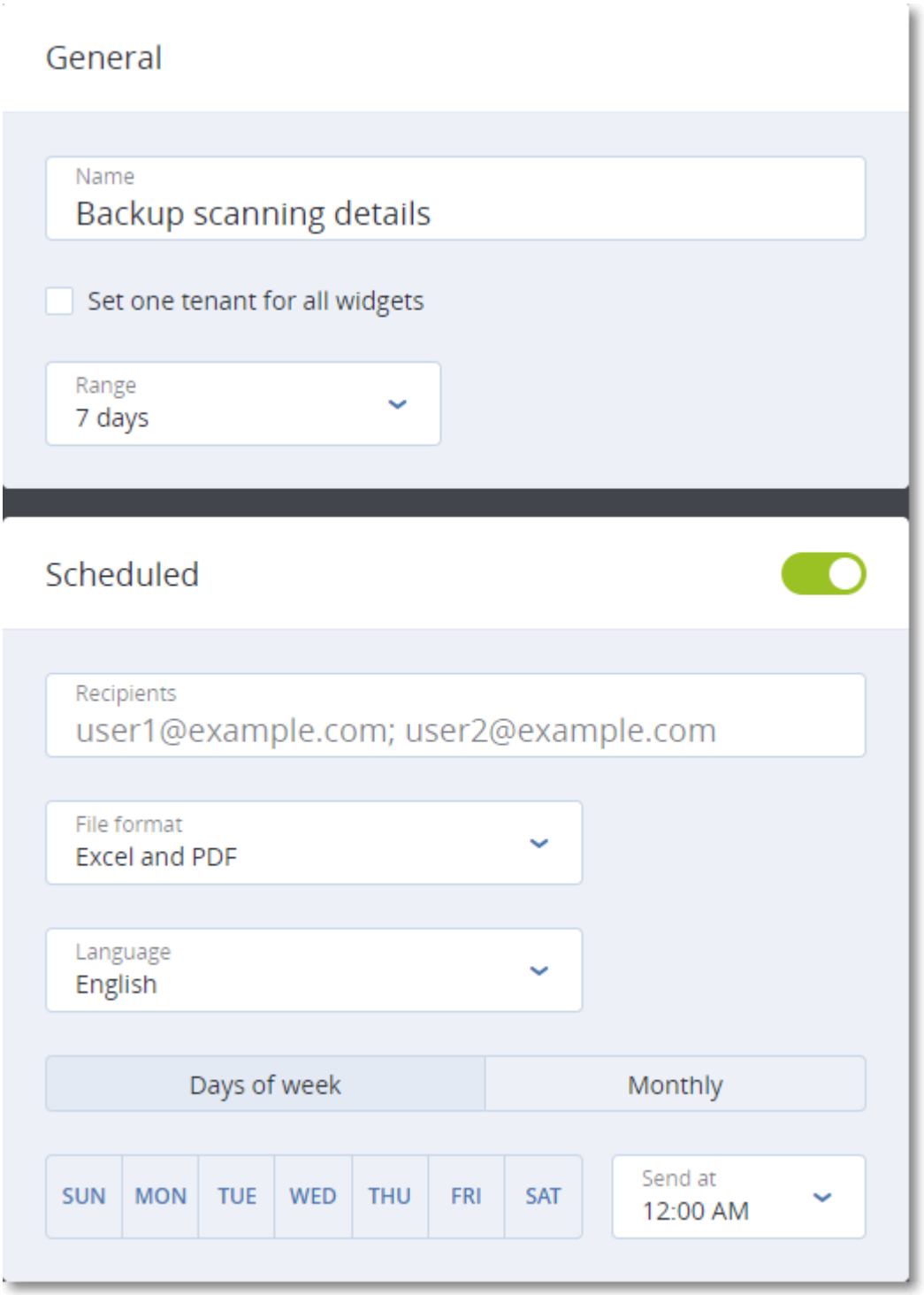
1. Щелкните **Добавить отчет**.
2. Выполните одно из следующих действий:
   - Чтобы добавить предопределенный отчет, щелкните его имя.
   - Чтобы добавить настраиваемый отчет, щелкните **Настраиваемый**, выберите имя отчета (по умолчанию назначаются имена типа **Custom(1)**) и добавьте виджеты в отчет.
3. [Необязательно] Для изменения положения виджетов перетащите их.
4. [Необязательно] Измените отчет, как описано ниже.

Изменение настроек отчета

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

- Переименовать отчет.
- Изменить отображаемого клиента для всех виджетов, включенных в отчет.

  При наличии дочерних клиентов для вас будет доступен параметр **Задать одного клиента для всех виджетов**. Этот параметр позволит фильтровать данные по выбранному клиенту во всех виджетах для данного отчета. Если этот параметр не выбран, то виджеты будут показывать данные для всех дочерних клиентов вашего текущего клиента.
- Изменить диапазон времени для всех виджетов, включенных в отчет.
- Запланировать отправку отчета по электронной почте в форматах PDF и (или) Excel.



Планирование отчета

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

5. Выберите дни и время отправки отчета.
6. Щелкните **Сохранить** в верхнем правом углу.

Экспорт и импорт структуры отчета

Вы можете экспортировать и импортировать структуру отчета (набор виджетов и настроек отчета) в файл .json. Это может быть полезно при копировании структуры отчета из одного клиента в другой.

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

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

Скачивание отчета

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

- Excel и PDF
- Excel
- PDF

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. Метки времени в CSV-отчетах указаны в формате UTC, а в отчетах Excel и PDF — в часовом поясе текущей системы.

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

Дамп данных отчета

1. Щелкните имя отчета.
2. Нажмите значок в виде вертикального эллипса в правом верхнем углу и затем нажмите **Дамп данных**.
3. Укажите адреса электронной почты получателей.
4. В **Диапазон времени** укажите диапазон времени.
5. Щелкните **Отправить**.

3.18.3 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. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Отчеты > Использование > Запланированные отчеты	• Отчет создается в 23:59:59 (по времени UTC) в первый день месяца. • Отчет отправляется во второй день месяца.
Портал управления > Отчеты > Использование > Пользовательские отчеты	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. • 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. • 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. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Пользователи > 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. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Пользователи > Уведомления о статусе Cyber Protection	• Этот отчет отправляется, когда действие завершено. **Примечание** В зависимости от рабочей нагрузки в центре обработки данных некоторые отчеты могут отправляться с задержкой. • Для действий в отчете указано время в часовом поясе UTC.

3.19 Журнал аудита

Чтобы посмотреть журнал аудита, щелкните пункт **Журнал аудита**.

В журнал аудита в хронологическом порядке заносятся следующие события:

- операции, выполняемые пользователями на портале управления;
- системные сообщения о достижении и использовании квот.

В журнале отображаются события тенанта, в котором вы работаете в настоящий момент, а также его дочерних тенантов. Чтобы посмотреть более подробные сведения о событии, щелкните по нему.

Журналы аудита хранятся в центре обработки данных Киберпротект; на их доступность не влияют проблемы на машинах конечных пользователей.

Журнал ежедневно очищается. События удаляются через 180 дней.

3.19.1 Поля журнала аудита

Для каждого события в журнале отображаются указанные ниже данные.

- **Событие**

  Краткое описание события. Пример: **Тенант создан**, **Тенант удален**, **Пользователь создан**, **Пользователь удален**, **Квота достигнута**.
- **Серьезность**

  Принимает перечисленные ниже значения.
  - **Ошибка**

    Обозначает ошибку.
  - **Предупреждение**

    Обозначает действие с потенциально отрицательным эффектом. Пример: **Тенант удален**, **Пользователь удален**, **Квота достигнута**.
  - **Уведомление**

    Обозначает событие, которое может требовать внимания. Пример: **Тенант обновлен**, **Пользователь обновлен**.
  - **Информация**

    Нейтральное изменение или действие информационного характера. Пример: **Тенант создан**, **Пользователь создан**, **Квота обновлена**.
- **Дата**

  Дата и время события.
- **Имя объекта**

  Объект, с которым была выполнена операция. Например для события **Пользователь обновлен** объектом является пользователь, свойства которого были изменены. Для событий, связанных с квотами, объектом является квота.

- **Тенант**

  Название тенанта, к которому относится объект.
- **Инициатор**

  Имя пользователя, инициировавшего событие. Для системных сообщений и событий, инициируемых администраторами верхнего уровня, в качестве инициатора отображается **Система**.
- **Тенант инициатора**

  Название тенанта, к которому относится инициатор. В случае системных сообщений и событий, инициируемых администраторами верхнего уровня, это поле остается пустым.
- **Метод**

  Показывает, было ли событие инициировано через веб-интерфейс или через API.
- **IP-адрес**

  IP-адрес машины, с которой инициировано событие.

3.19.2 Фильтрация и поиск

События можно фильтровать по описанию, серьезности и дате. Кроме того, можно искать события по объектам, тенантам, инициаторам и отделам инициаторов.

4 Дополнительные сценарии использования

4.1 Перемещение тенанта в другой тенант

Портал управления позволяет перемещать тенант из одного родительского тенанта в другой родительский тенант. Это может быть полезно при переносе пользователя с одного партнера в другой или в случае, если нужно перенести некоторые из тенантов в новый тенант папки, который создан для упорядочивания.

4.1.1 Ограничения

- Тенант партнера/папки можно переместить только в тенант партнера/папки.
- Тенант клиента можно переместить только в тенант партнера/папки.
- Тенант отдела невозможно переместить.
- Тенант можно переместить, только если целевой родительский тенант имеет такой же или больший набор услуг и элементов предложения, как и исходный родительский тенант.
- Тенанты можно перенести только в пределах иерархии одного партнера. Перемещение тенантов между иерархиями учетной записи партнера не поддерживается.
- При перемещении тенанта пользователя все хранилища данных, назначенные тенанту пользователя в исходном родительском тенанте, должны существовать в целевом родительском тенанте. Это необходимо, поскольку данные, связанные с обслуживанием пользователей, невозможно переместить с одного хранилища данных в другое.

4.1.2 Перемещение тенанта

1. Войдите на портал управления.
2. На вкладке **Клиенты** выберите целевой тенант, в который необходимо переместить тенант.
3. На панели свойств тенанта щелкните вертикальный значок многоточия, затем щелкните **Показать ИД**.
4. Скопируйте текстовую строку в поле **Внутренний идентификатор**, затем щелкните **Отмена**.
5. На вкладке **Клиенты** выберите тенант, который необходимо переместить.
6. На панели свойств тенанта щелкните значок в виде вертикального эллипса, затем щелкните **Переместить**.
7. Вставьте внутренний идентификатор целевого тенанта, затем щелкните **Переместить**.

4.2 Преобразование тенанта партнера в тенант папки и наоборот

На портале управления можно преобразовать тенант партнера в тенант папки.

Это может быть полезно в тех случаях, когда тенант партнера использовался для группировки, а теперь необходимо организовать инфраструктуру тенанта должным образом. Это также полезно для того, чтобы иметь на операционной панели мониторинга сводную информацию о тенанте.

Можно также преобразовать тенант папки в тенант партнера.

Примечание
Преобразование – это безопасная операция, которая не влияет на пользователей в тенанте и какие-либо данные, относящиеся к службе.

Порядок преобразования тенанта

1. Войдите на портал управления.
2. На вкладке **Клиенты** выберите тенант, которого необходимо преобразовать.
3. Выполните одно из следующих действий:
   - Щелкните значок многоточия рядом с именем тенанта.
   - Выберите тенант, затем щелкните значок многоточия на панели свойств тенанта.
4. Щелкните **Преобразовать в папку** или **Преобразовать в партнера**.
5. Подтвердите операцию.

4.3 Ограничение доступа к веб-интерфейсу

Администраторы могут ограничить доступ к веб-интерфейсу, указав список IP-адресов, с которых пользователям тенанта 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 пользователям дочерних тенантов.

Порядок ограничения доступа к веб-интерфейсу

1. Войдите на портал управления.
2. Найдите тенант, в котором необходимо ограничить доступ.
3. Щелкните **Настройки** > **Безопасность**.
4. Включите переключатель **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**.

4.4 Ограничение доступа к тенанту

Администраторы на уровне пользователя и более высоком уровне могут ограничить доступ к своим тенантам для администраторов более высокого уровня.

Если доступ к тенанту ограничен, администраторы родительского тенанта могут только изменять свойства тенанта. Они вообще не видят учетные записи и дочерних тенантов.

Порядок действия для предотвращения доступа администраторов более высокого уровня к тенанту

1. Войдите на портал управления.
2. Последовательно выберите пункты **Настройки** > **Безопасность**.
3. Деактивируйте переключатель **Доступ для службы поддержки**.

После этого администраторы родительских тенантов будут иметь ограниченный доступ к вашему тенанту. Они смогут только изменять свойства, но не смогут получить доступ к объектам внутри тенанта (дочерние тенанты, пользователи, службы, резервные копии и другие ресурсы) и управлять ими.

Если включен переключатель **Доступ для службы поддержки**, администраторы родительских тенантов будут иметь полный доступ к вашему тенанту. Они смогут выполнять следующие действия: изменять свойства; управлять тенантами, пользователями и службами; получать доступ к резервным копиям и другим ресурсам.

4.5 Интеграция с системами сторонних производителей

Поставщик услуг может интегрировать Кибер Бэкап Облачный со сторонними системами следующим образом:

- Настройка расширения платформы в этой системе.

  На странице **Интеграция** портала управления перечислены расширения, доступные для самых широко используемых системам автоматизации профессиональных услуг (Professional Services Automations, PSA) и удаленного мониторинга и управления (Remote Monitoring and Management, RMM).

  Это рекомендуемый способ интеграции платформы.
- Путем создания клиента API для системы и включения системы для доступа к прикладным программным интерфейсам (API) платформы и ее служб. Клиенты API – это часть инфраструктуры авторизации OAuth 2.0 на платформе. Дополнительную информацию о OAuth 2.0 см. по ссылке https://tools.ietf.org/html/rfc6749.

  Это низкоуровневый способ интеграции платформы, который требует навыков программирования. Его рекомендуется использовать, если для системы нет расширения платформы или систему необходимо настроить для тех случаев управления платформой и ее службами, которые не предусмотрены доступным расширением.

4.5.1 Настройка расширения Кибер Бэкап Облачный

1. Войдите на портал управления.
2. Щелкните **Настройки** > **Интеграция**.
3. Щелкните имя сторонней системы, интеграцию с которой необходимо включить.
4. Следуйте инструкциям на экране.

Дополнительная информация об интеграции со сторонними системами доступна в разделе "Справочник по интеграции" на веб-сайте Киберпротект.

4.5.2 Управление клиентами API

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

4.5.2.1 Что такое клиент API?

Клиент API – это специальная учетная запись платформы, представляющая стороннюю систему, для которой нужна авторизация и авторизация для доступа к данным в интерфейсах API платформы и ее служб.

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

При создании клиента он наследует роли службы учетной записи администратора. Эти роли невозможно изменить впоследствии. Изменение ролей учетной записи администратора или ее отключение не влияет на клиент.

Учетные данные клиента состоят из уникального идентификатора (ИД) и значения секрета. Учетные данные не имеют срока действия и не могут использоваться для входа на портал управления или на консоль службы. Значение секрета можно сбросить.

Для клиента можно включить двухфакторную аутентификацию.

4.5.2.2 Типичная процедура интеграции

1. Администратор создает клиент API в тенанте, которым будет управлять сторонняя система.
2. Администратор включает поток учетных данных клиента OAuth 2.0 в сторонней системе. Согласно этому потоку, перед доступом к тенанту и его службам через API система сначала должна отправить учетные данные созданного клиента на платформу, используя API авторизации. Платформа создает и отправляет обратно токен безопасности – уникальную криптографически защищенную строку, которая назначается только данному клиенту. После этого система должна добавить этот токен во все запросы API.

Токен безопасности устраняет необходимость передачи учетных данных клиента с запросами API. Для обеспечения дополнительной безопасности срок действия токена истекает через два часа. По истечении этого времени просроченный токен дает сбой, после чего системе необходимо запросить новый токен с платформы.

4.5.2.3 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. Оно не подлежит восстановлению при утрате. Его можно только сбросить.

6. Нажмите кнопку **Готово**.

4.5.2.4 Сброс значения секрета клиента API

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

4.5.2.5 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.

4.5.2.6 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.

4.5.2.7 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 удаленного клиента невозможно.

Указатель

О

П

Р

С

Т

У

Ф

Ч

Э