КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 26.03

Руководство администратора партнёра

Редакция: 20.04.2026

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.

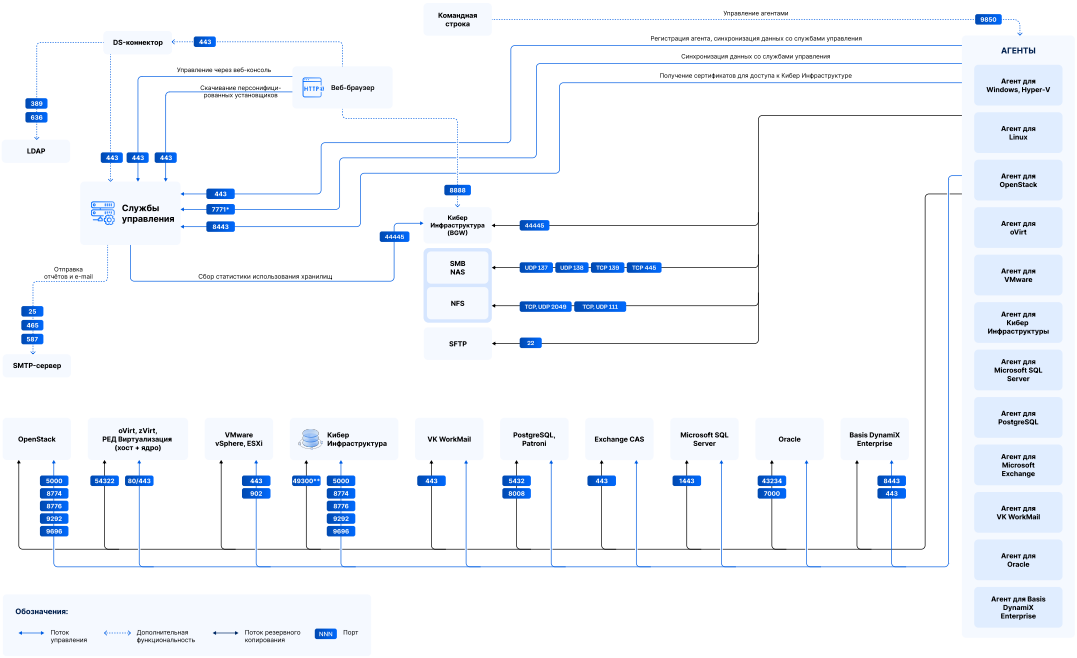
Управление службами доступно посредством веб-приложений, которые называются **консолями службы**. Управление тенантом и учетной записью пользователя доступно через веб-приложение, которое называется **порталом управления**.

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 Схема взаимодействия компонентов

Взаимодействие основных компонентов продукта показано на схеме.



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

Службы управления

Компонент	Тип	Порт	Источник подключения	Протокол	Описание
Службы управления					
	Входящее	443	Веб-консоль Агенты DS-коннектор	TCP	Веб-консоль сервера управления и шлюз API-запросов. Регистрация компонентов. Обмен информацией с агентами.
	Входящее	8443	Агенты	TCP	Получение сертификатов для доступа к Кибер Инфраструктуре.
	Входящее	7771*	Агенты	TCP	Шлюз ZeroMQ для подключения и обмена информацией с агентами. Основной трафик от агентов.
Агент для Windows/Hyper-V					
	Входящее	9850	Запросы через интерфейс командной строки	TCP	Работа с интерфейсом командной строки.
Агент для Linux					
	Входящее	9850	Запросы через интерфейс командной строки	TCP	Работа с интерфейсом командной строки.
Агент для виртуальных машин (VMware, oVirt)					
	Входящее	9850	Запросы через интерфейс командной строки	TCP	Работа с интерфейсом командной строки.
DS-коннектор					
	Входящее	443	Веб-консоль	TCP	Форма входа через LDAP.

Хранилища

Компонент	Тип	Порт	Источник	Протокол	Описание

			подключения		
Кибер Инфраструктура (BGW)					
	Входящее	8888	Веб-браузер администратора	TCP	Веб-консоль управления.
	Входящее	44445	Агенты Сервер управления	TCP	Загрузка и выгрузка резервных копий.
Сетевая папка SMB/NAS					
	Входящее	139	Агенты	TCP	Загрузка и выгрузка резервных копий.
	Входящее	445	Агенты	TCP	Загрузка и выгрузка резервных копий.
	Входящее	137	Агенты	UDP	Загрузка и выгрузка резервных копий.
	Входящее	138	Агенты	UDP	Загрузка и выгрузка резервных копий.
Сетевая папка NFS					
	Входящее	111	Агенты	TCP UDP	Загрузка и выгрузка резервных копий.
	Входящее	2049	Агенты	TCP UDP	Загрузка и выгрузка резервных копий.
Сетевая папка SFTP					
	Входящее	22	Агенты	TCP	Загрузка и выгрузка резервных копий.

Виртуализация

Компонент	Тип	Порт	Источник подключения	Протокол	Описание
VMware vSphere и ESXi					
	Входящее	902	Агент для VMware	TCP	Управляющие команды от агента.
	Входящее	443	Агент для VMware	TCP	Управляющие команды от агента.
oVirt, zVirt Engine, РЕД Виртуализация (хост)					
	Входящее	54322	Агент для oVirt	TCP	Передача агенту данных с

					дисков ВМ при включенном CBT. Передача ядру гипервизора образа виртуального устройства.
oVirt, zVirt Engine, РЕД Виртуализация (ядро)					
	Входящее	80	Агент для oVirt	TCP	Управляющие команды от агента.
	Входящее	443	Агент для oVirt	TCP	Управляющие команды от агента.
OpenStack					
	Входящее	5000	Агент для OpenStack	TCP	Управляющие команды от агента.
	Входящее	8774	Агент для OpenStack	TCP	Управляющие команды от агента.
	Входящее	8776	Агент для OpenStack	TCP	Управляющие команды от агента.
	Входящее	9292	Агент для OpenStack	TCP	Управляющие команды от агента.
	Входящее	9696	Агент для OpenStack	TCP	Управляющие команды от агента.
Кибер Инфраструктура					
	Входящее	5000	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	8774	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	8776	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	9292	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	9696	Агент для Кибер Инфраструктуры	TCP	Управляющие команды от агента.
	Входящее	49300**	Агент для Кибер Инфраструктуры	TCP	Передача данных с дисков виртуальной машины.
Basis DynamiX Enterprise					

	Входящее	443	Агент для Basis DynamiX Enterprise	TCP	Управляющие команды от агента.
	Входящее	8443	Агент для Basis DynamiX Enterprise	TCP	Управляющие команды от агента.

Приложения

Компонент	Тип	Порт	Источник подключения	Протокол	Описание
Microsoft Exchange CAS					
	Входящее	443	Агенты для Microsoft Exchange (почтовые ящики)	TCP	Загрузка и выгрузка содержимого почтовых ящиков.
PostgreSQL и Patroni					
	Входящее	5432	Агент для PostgreSQL	TCP	Выгрузка содержимого экземпляра БД.
	Входящее	8008	Агент для PostgreSQL	TCP	API службы управления кластером PostgreSQL.
Почта VK WorkMail					
	Входящее	443	Агент для VK WorkMail	TCP	Загрузка и выгрузка содержимого почтовых ящиков и хранилища Диск VK WorkSpace.
Microsoft SQL Server					
	Входящее	1443	Агент для Microsoft SQL Server	TCP	Работа с Windows Cluster API (для AAG) или через ODBC.
Oracle					
	Входящее	43234	Агент для Oracle	TCP	Работа с Oracle Restore Tool.
	Входящее	7000	Агент для Oracle	TCP	Работа с RMAN.

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

** Используются динамические порты из диапазона 49300–65635.

2.2 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?

2.2.1 Службы и функциональные пакеты

2.2.1.1 Службы

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

2.2.1.2 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.

2.2.1.3 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. 12).

2.2.2 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 "Без ограничений" 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.

2.2.2.1 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. Жесткие квоты можно задать на уровне клиента и пользователя. Отделы наследуют квоты от клиентов.

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

2.2.2.2 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 рабочих нагрузок

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

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

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

Квоты для хранилища данных

- **Локальное резервное копирование**

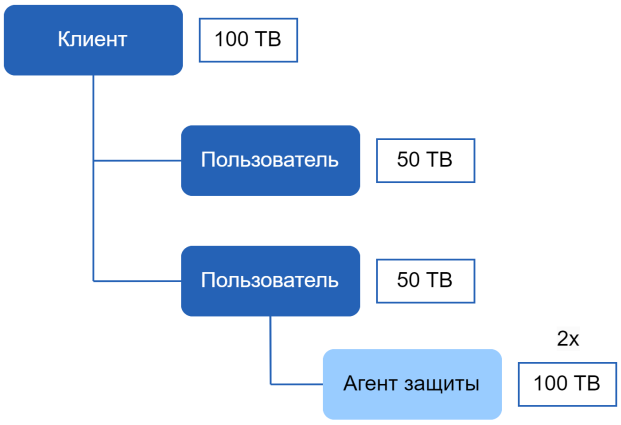
  Квота **Локальное резервное копирование** ограничивает общий размер локальных резервных копий, созданных с использованием облачной инфраструктуры. Для этой квоты нельзя задать превышение.
- **Облачные ресурсы**

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

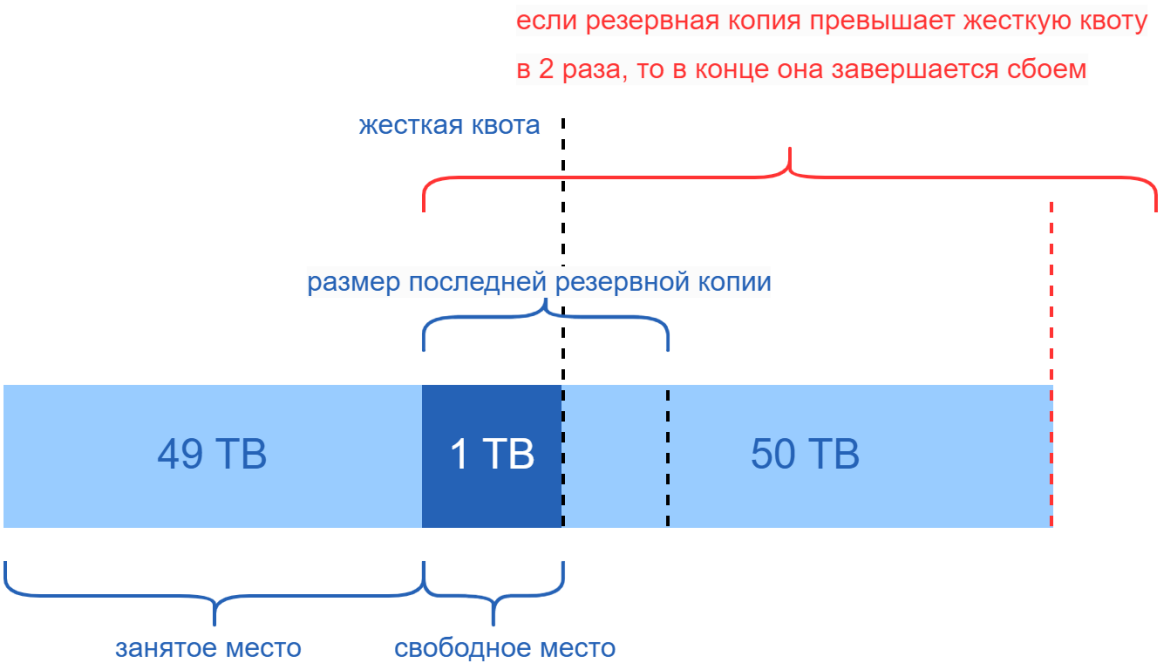
Превышение жесткой квоты для хранилища резервных копий

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.

2.2.3 Доступные рабочие нагрузки в зависимости от функциональных пакетов

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

Рабочая нагрузка	Активированный функциональный пакет				
	Серверы	Рабочие станции	Виртуальные машины	Почтовые ящики	Экземпляры СУБД
Несколько устройств					
Только в ОС Windows		+			
Рабочие станции					
Windows		+			
Серверы					

Windows	+				
Linux	+				
Хосты виртуализации					
VMware ESXi			+		
Cyber Infrastructure			+		
Hyper-V			+		
KVM			+		
Red Hat Virtualization (oVirt)			+		
Citrix XenServer			+		
Nutanix AHV			+		
Oracle VM			+		
OpenStack (VK Cloud)			+		
Приложения					
Microsoft SQL Server	+		+		
PostgreSQL	+		+		+
Кластер PostgreSQL Patroni	+		+		+
VK WorkMail				+	
Microsoft Exchange Server	+		+		
Microsoft Active Directory	+		+		
База данных Oracle	+		+		

2.3 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.

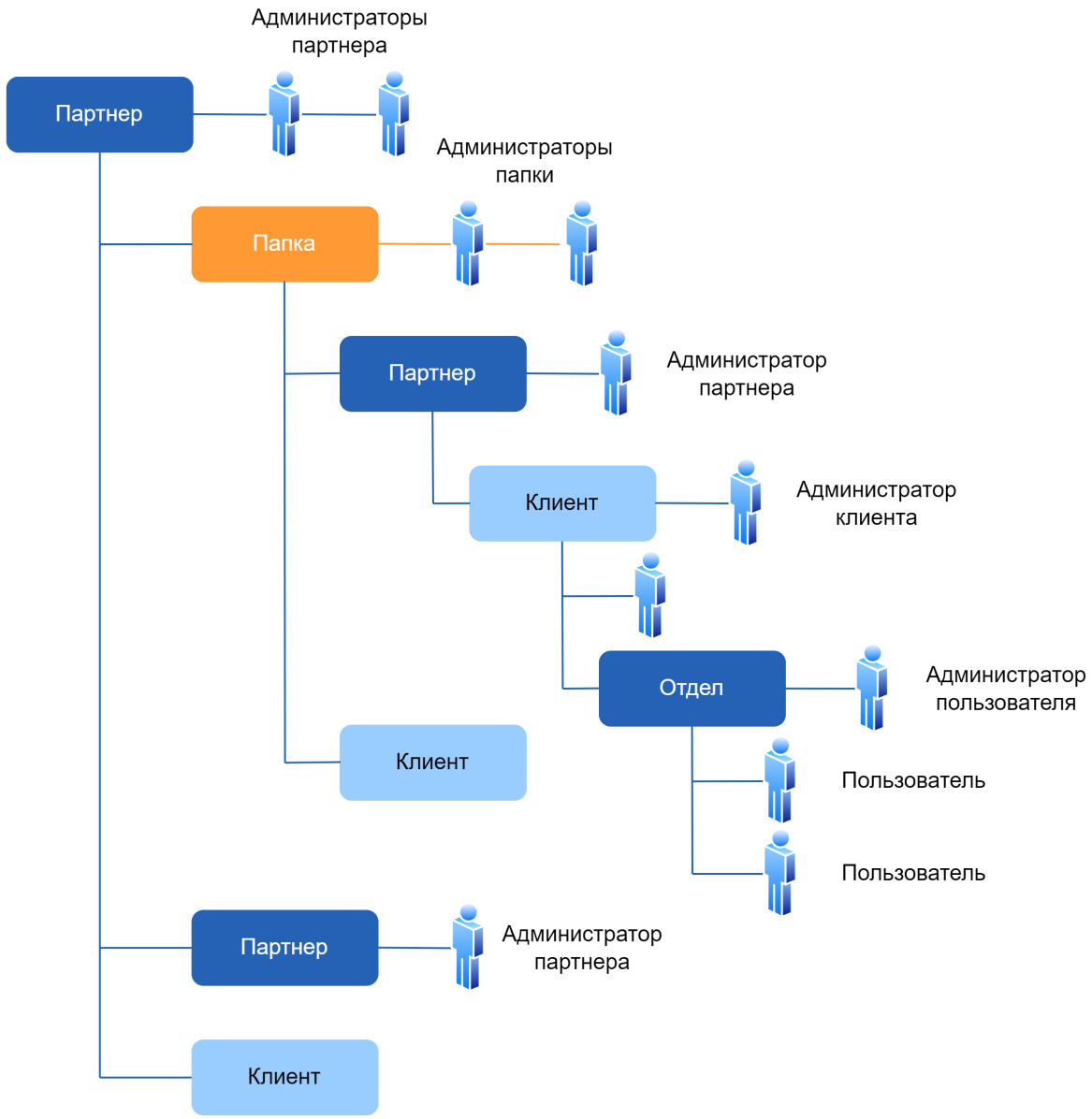
Каждая учетная запись принадлежит тенанту. Тенант – это составная часть ресурсов портала управления (например, учетные записи пользователей и дочерние тенанты) и предложений службы (включенные службы и элементы предложения в них), которая относится к тому или иному партнеру или клиенту. Иерархия тенантов 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.

2.4 Поддерживаемые веб-браузеры

Веб-интерфейс платформы резервного копирования поддерживает перечисленные ниже браузеры:

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

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

3 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 частях 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** > **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** > **Использование**.
   Обратите внимание, что одними службами можно управлять на уровне тенанта партнера и тенанта клиента, а другими – только на уровне тенанта клиента.
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 клиента, а другими – только на уровне тенанта клиента.
   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

Для создания тенанта выполните следующие действия:

1. Войдите на портал управления.
2. Выберите тенант, в котором необходимо создать новый тенант.
3. В верхнем правом углу нажмите кнопку **Новый** и выберите тип тенанта в выпадающем списке (подробнее о тенантах см. в разделе "Учетные записи пользователя и тенанты" (стр. 16)).

   Примечание
   Набор доступных вариантов зависит от типа родительского тенанта.

4. В поле **Имя** укажите название нового тенанта.
5. [Только при создании тенанта типа **Клиент**] В выпадающем списке **Режим** выберите режим использования тенантом служб (пробный или рабочий). В ежемесячные отчёты об использовании не включаются данные для тенантов, работающих в пробном режиме.

   Внимание
   При переходе с пробного режима на рабочий в течение месяца в отчёт будут включены данные об использовании службы за весь месяц. По этой причине рекомендуется 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 выпадающем списке **Язык** выберите язык уведомлений, отчётов и служб для данного тенанта.
7. [Только при создании тенанта типа **Партнёр** или **Клиент**] В разделе **Режим управления** выберите один из следующих режимов для управления доступом к тенанту:
   - **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 (тенантам, пользователям, службам, резервным копиям и другим ресурсам) 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**.
8. [Только при создании тенанта типа **Партнёр** или **Клиент**] В разделе **Безопасность** поставьте флажок, если требуетс двухфакторная проверка подлинности для тенанта.

   Если она включена, всем пользователям этого тенанта необходимо будет настроить двухфакторную аутентификацию для своих учётных 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 учётными данными для входа в консоль. Дополнительную информацию см. в разделе Настройка двухфакторной проверки подлинности. Чтобы просмотреть статус двухфакторной проверки подлинности для ваших клиентов, откройте раздел **Клиенты**.
9. [Только при создании тенанта типа **Клиент** в режиме "Улучшенная безопасность"] В разделе **Безопасность** установите флажок **Улучшенная безопасность**.

   В этом режиме разрешено создавать только зашифрованные резервные копии. На защищённом 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".

   Подробнее о режиме "Улучшенная безопасность" см. в разделе "Режим улучшенной безопасности" (стр. 24).
10. [Только при создании тенанта типа **Партнёр** или **Клиент**] В блоке **Завершить сеансы работы неактивных пользователей** укажите временной период бездействия пользователя (в минутах), по истечении которого его сессия будет автоматически завершена как на портале управления, так и в консоли службы. Диапазон доступных значений – от 5 до 999.

Данный параметр наследуется дочерними тенантами, если их администраторы не установили собственное значение. Индивидуальная настройка в дочернем тенанте имеет приоритет над родительской и сохраняется при изменении параметра на верхнем уровне. При сбросе настроек в дочернем тенанте применяется значение, наследуемое из родительского тенанта. Подробнее о сбросе или настройке периода бездействия пользователя см. в разделе "Настройка периода бездействия пользователя" (стр. 78).

11. [Только при создании тенанта типа **Партнёр** или **Клиент**] В блоке **Число неуспешных попыток входа** укажите число попыток входа, при превышении которого учётная запись будет заблокирована, а также укажите временной период этой блокировки в минутах.
12. В разделе **Создать администратора** укажите данные администратора:
    - **Имя для входа**: имя, которое будет использоваться администратором для входа.
    - **Адрес электронной почты**: адрес электронной почты администратора.
    - [Необязательно] **Фамилия**.
    - [Необязательно] **Имя**.
    - **Язык**: выберите значение из выпадающего списка.
13. Выполните одно из следующих действий:
    - Чтобы завершить создание тенанта, щёлкните **Сохранить и закрыть**. В этом случае все функциональные пакеты будут включены для тенанта с неограниченной квотой.
    - Чтобы выбрать службы и настроить функциональные пакеты для тенанта, щёлкните **Далее**. Описание настроек приведено в разделе "Выбор служб и настройка функциональных пакетов для тенанта" (стр. 25).

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.
- Отчеты и панели мониторинга, связанные с недоступными функциями.

3.5.3 Выбор служб и настройка функциональных пакетов для тенанта

3.5.3.1 Выбор служб

В блоке **Выберите службы** выполните следующие действия:

1. Выберите службы, которые будут включены для тенанта, переведя соответствующие переключатели в положение **Включено**.

   Примечание
   Набор доступных вариантов зависит от типа тенанта.

2. [Если выбрана служба **Кибер Бэкап**] Установите флажок **Защита** и выберите режимы выставления счетов и устаревшие выпуски.

   Варианты режима выставления счетов:

   - **На рабочую нагрузку**: предоставляет киберзащиту, мониторинг, управление, резервное копирование и аварийное восстановление, которое удовлетворяет большинству потребностей пользователей. Счета выставляются в соответствии с количеством защищённых рабочих нагрузок. Счета за использованное облачное хранилище данных выставляются отдельно.
   - **На гигабайт**: предоставляет киберзащиту, мониторинг, управление, резервное копирование и аварийное восстановление, которое удовлетворяет большинству потребностей пользователей. Счета выставляются в соответствии с используемым облачным и локальным хранилищем данных.

   Варианты устаревших выпусков:

- **Кибер Протект Версия (все функции, на рабочую нагрузку)**;
- **Кибер Бэкап Версия (все функции, на гигабайт)**;
- **Кибер Протект – Стандартная версия**;
- **Кибер Протект – Расширенная версия**;
- **Кибер Протект – Версия Disaster Recovery**;
- **Кибер Бэкап – Стандартная версия**;
- **Кибер Бэкап – Расширенная версия**;
- **Кибер Бэкап – Версия Disaster Recovery**.

Для тенанта типа **Клиент** можно выбрать только один из вариантов выставления счетов, либо один из вариантов устаревших выпусков.

3. [Если выбран режим выставления счетов **На рабочую нагрузку** или **На гигабайт**] Установите флажки для добавления расширенных возможностей, если необходимо:
   - **Advanced Backup**: активирует возможность резервного копирования Microsoft SQL в кластере, данных Microsoft Exchange в кластере, Oracle DB, SAP HANA;
   - **Advanced Management**: активирует возможности управления функциями Кибер Бэкап и их мониторинг для рабочих нагрузок, что позволяет обеспечить управление группами и централизованное управление планами защиты.
4. Выполните одно из следующих действий:
   - Чтобы завершить настройку, щёлкните **Сохранить и закрыть**. В этом случае все функциональные пакеты будут включены для тенанта с неограниченной квотой.
   - Чтобы выбрать функциональные пакеты и настроить их квоты, щёлкните **Далее**.

3.5.3.2 Настройка функциональных пакетов

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 типа **Партнёр** или **Папка** можно выбрать несколько расположений и хранилищ данных для каждой службы.

- При создании тенанта **Клиент** необходимо выбрать одно расположение, после чего выбрать одно хранилище данных в этом расположении для службы **Кибер Бэкап**. 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" (стр. 42).
3. Чтобы указать квоту для элемента, щёлкните 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 типа **Партнёр** использование функционального пакета может превысить квоту по той причине, что её превышение невозможно задать при создании тенанта типа **Партнёр**.
4. [Только при создании тенанта типа **Клиент**] Укажите превышения квоты.

   Превышение позволяет тенанту типа **Клиент** превысить квоты на указанное значение. При выходе за пределы значения превышения применяются ограничения на использование соответствующей службы.
5. Щёлкните **Сохранить и закрыть**.

Созданный тенант появляется на вкладке **Клиенты** портала управления.

Чтобы внести изменения в настройки тенанта или сменить администратора, выберите тенант на вкладке **Клиенты**, а затем щёлкните 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 > **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 учётной записи пользователя

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

- Учётные записи администратора партнёра/папки: чтобы делиться обязанностями по управлению службами с другими пользователями.

- Учётные записи администратора пользователи/отдела: для делегирования управления службами другим пользователям, для которых права доступа будут жёстко ограничены рамками соответствующего пользователя/отдела.
- Учётные записи в тенантах пользователя или отдела: чтобы включить для пользователей только доступ к поднабору служб.

Примечание
Существующие учётные записи невозможно переместить между тенантами. Сначала необходимо создать тенант, а затем заполнить его учётными записями.

Порядок создания учётной записи пользователя

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

     Внимание
     У каждой учётной записи должно быть уникальное имя входа.

   - **Электронная почта**
   - [Необязательно] **Имя**
   - [Необязательно] **Фамилия**
   - В поле **Язык** измените язык, который по умолчанию используется для уведомлений, отчётов и веб-интерфейса программного обеспечения для этой учётной записи.
5. Выберите службы, к которым пользователь будет иметь доступ, и роли в каждой службе.
   Доступные службы зависят от служб, включённых для тенанта, в котором создана учётная запись пользователя.
   - Установите флажок **Администратор компании**, чтобы пользователь имел доступ к порталу управления и роль администратора во всех службах.
   - Установите флажок **Портал управления**, чтобы у пользователя был доступ к порталу управления. Выберите роль для службы (подробнее см. в разделе Роли пользователя, доступные для каждой службы).
   - Установите флажок **Защита**, чтобы пользователь мог выполнять настройку резервного копирования и восстановления, а также управлять резервными копиями. Выберите роль для службы (подробнее см. в разделе Роли пользователя, доступные для каждой службы).
6. Нажмите кнопку **Создать**.

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

Чтобы изменить настройки пользователя или указать настройки уведомления и квот (недоступно для администраторов партнёра/папки) для пользователя, выберите его на вкладке **Пользователи**, а затем щёлкните значок карандаша в том разделе, который нужно изменить.

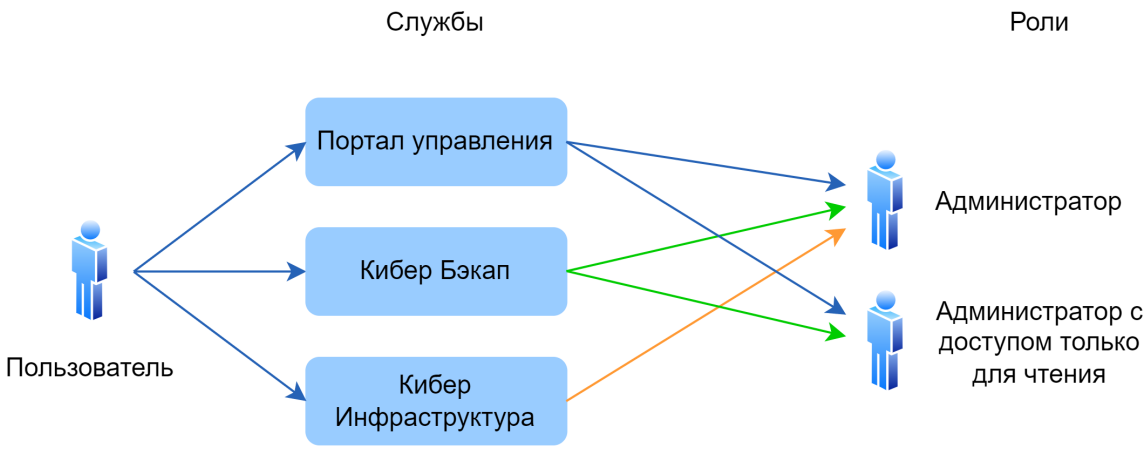
Порядок сброса пароля пользователя

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

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

3.9 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	Эта роль предоставляет доступ только для чтения ко всем объектам на портале управления. Такие пользователи могут

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

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 учётной записи пользователя

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

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

Внимание
Удаление учётной записи пользователя необратимо.

Порядок удаления учётной записи пользователя

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

В результате:

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

3.13 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 факторов из следующих трех:

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

- Биометрических данных, которые присущи только пользователю.

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

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

3.14.1 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

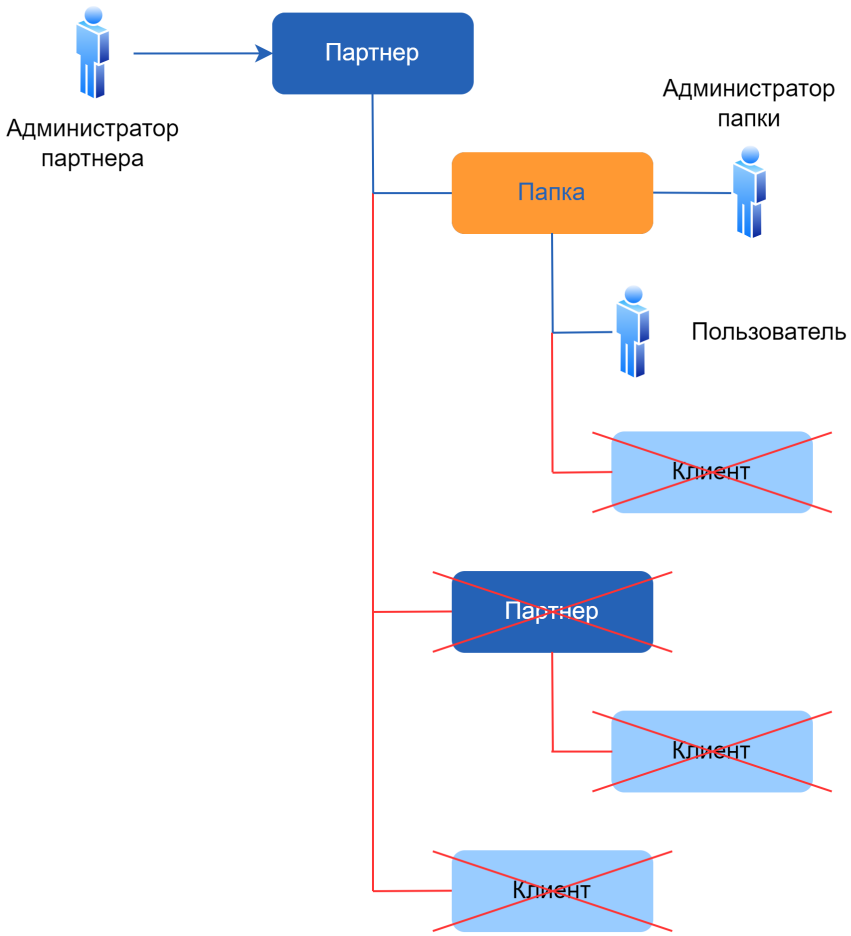
Двухфакторная проверка подлинности задается на уровне **организации**. Можно включить или отключить двухфакторную проверку подлинности.

- 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:

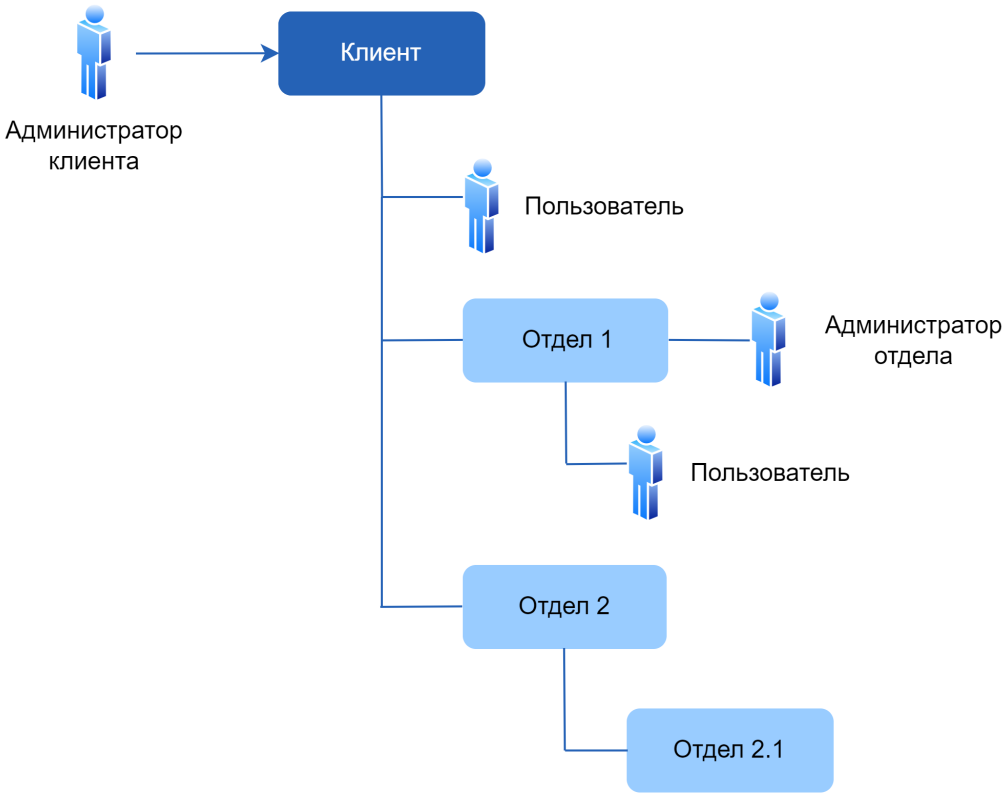
- Папки автоматически наследуют настройки двухфакторной проверки подлинности от организации партнера. На приведенной ниже схеме красными линиями обозначены направления, в которых распространение настроек двухфакторной проверки подлинности невозможно.

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

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

3.14.4.5 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.

3.15.2.2 Удаление хранилищ данных

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

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

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 и Linux) и Кибер Бэкап Облачный Monitor (для Windows 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 Дополнительные продажи

Дополнительные продажи – это способ пригласить клиентов приобрести дополнительные функции.

Возможно, вы захотите предложить своим клиентам, которые используют стандартную функциональность Кибер Бэкап, выпуски с усовершенствованными функциональными возможностями.

Можно включить или отключить возможность продажи дополнительных функциональных пакетов для каждого клиента. По умолчанию эта возможность включена. Для ваших клиентов дополнительная функциональность станет доступной только после ее покупки. Эта дополнительная функциональность помечена метками, которые показывают имя или значки расширенного пакета.

Порядок настройки ссылки на покупку

Можно настроить ссылку для кнопки **Включить**, которая будет перенаправлять ваших клиентов на ваш веб-сайт для покупки расширенных служб.

1. На портале управления откройте раздел **Настройки** > **Фирменное оформление**.
2. В разделе **Дополнительные продажи** измените значение строки **URL-адрес покупки**.

Примечание
Фирменное оформление можно настроить на уровнях партнера и папки. Фирменное оформление будет применяться ко всем прямым и непрямым дочерним партнерам/папкам и пользователям клиента.

Теперь, если клиент нажмет кнопку **Включить** в диалоговом окне продажи дополнительных пакетов, он будет перенаправлен на указанный URL-адрес.

3.16.1.5 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

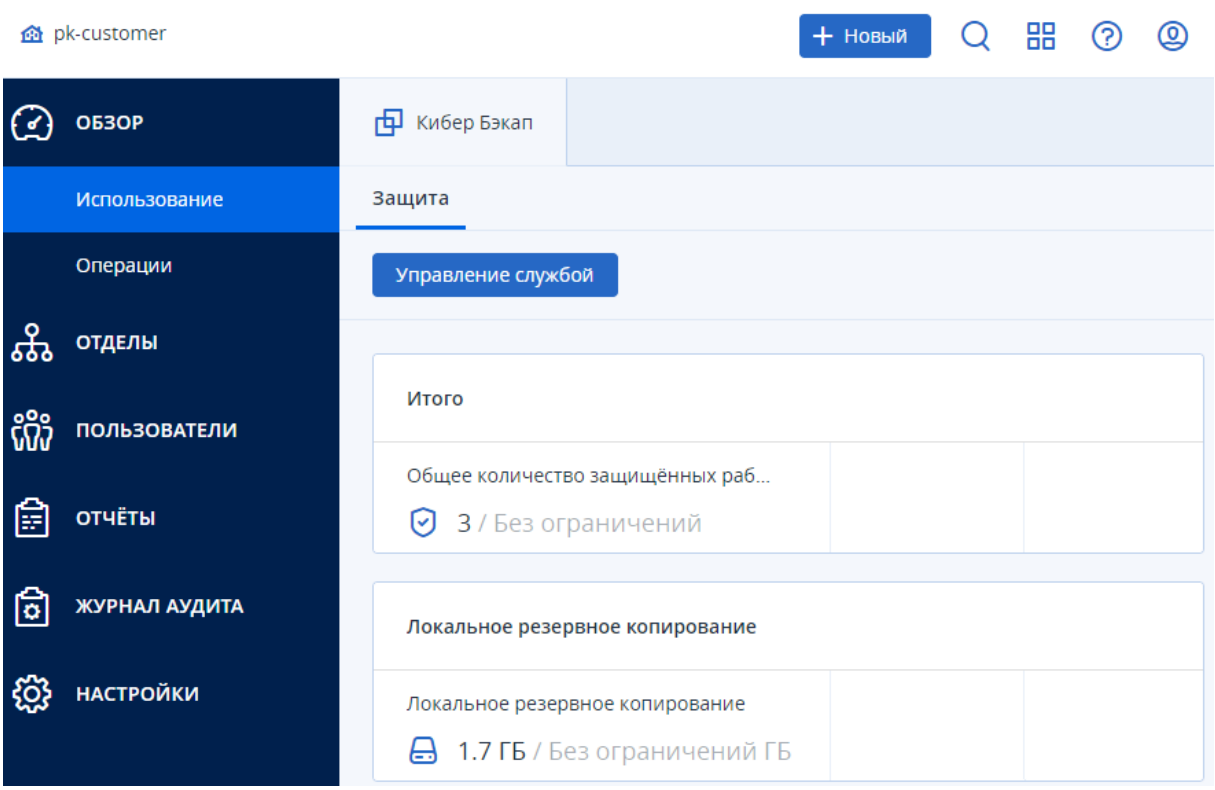
1. Войдите на портал управления.
2. Найдите тенант, в котором необходимо настроить форменное оформление.
3. Щелкните **Настройки** > **Фирменное оформление**.
4. Щелкните **Включить фирменное оформление**.
5. Выполните одно из следующих действий:
   - Настройте описанные выше элементы фирменного оформления.
   - 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, нажмите **Настроить**, когда виджет выбран. После изменения виджета щелкните **Добавить виджет**.

Порядок удаления виджета

Щелкните значок X рядом с именем виджета.

Список доступных виджетов

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

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.
- **Итог за период**

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

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

3.18.1.2 Уровень детализации

Можно выбрать область отчета из указанных ниже значений:

- **Непосредственные клиенты и партнеры**

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

  В отчете будут содержаться показатели использования службы для всех дочерних тенантов того тенанта, в котором вы работаете.
- **Все клиенты и партнеры (включая подробную информацию о пользователях)**

  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 **По плану**.
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 **По требованию**.
5. В разделе **Тип** выберите тип отчета, как описано выше.
6. [Недоступно для отчета типа **Текущее использование**] В поле **Период** выберите период отчета:
   - **Текущий календарный месяц**
   - **Предыдущий календарный месяц**
   - **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
Ежедневные задания	Показывает сводную информацию о действиях, выполненных за указанный период времени
Еженедельные действия	Показывает сводную информацию о действиях, выполненных за указанный период времени
Обнаруженные машины	Показывает все найденные машины в сети организации
Оповещения	Показывает оповещения, выполненные за указанный период времени
Пользовательская	Пользовательский отчет формируется по требованию
Сводка	Показывает сводную информацию об устройствах, защищенных за указанный период времени

Для просмотра отчета щелкните его имя.

Добавление отчета

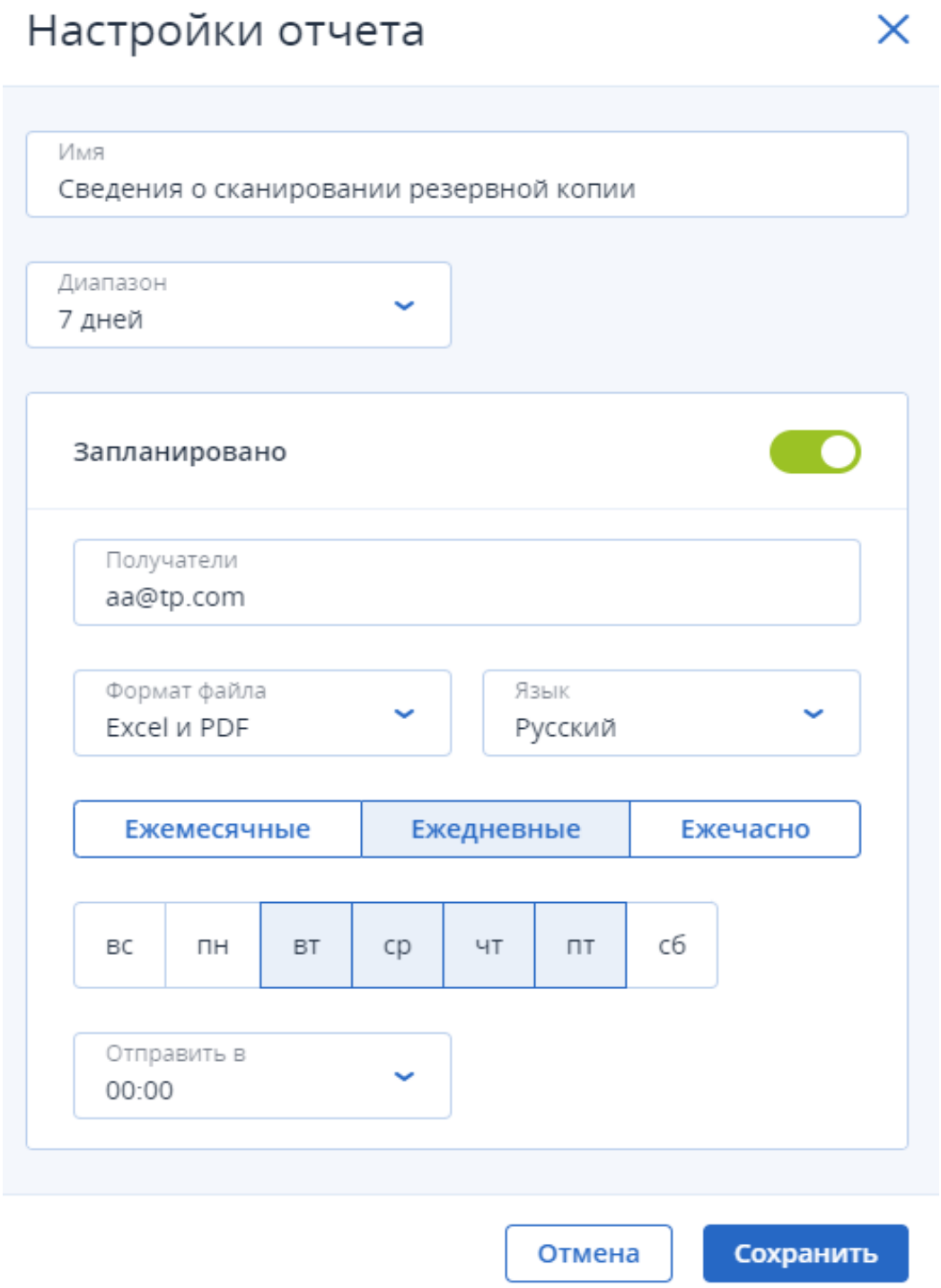
1. Щелкните **Добавить отчет**.
2. Выполните одно из следующих действий:
   - Чтобы добавить предопределенный отчет, щелкните его имя.
   - Чтобы добавить настраиваемый отчет, щелкните **Пользовательская**, выберите имя отчета (по умолчанию назначаются имена типа **Пользовательская (1)**) и добавьте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

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, время и интервал отправки отчета.
6. Щелкните **Сохранить**.

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 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 многоточия в правом верхнем углу и затем нажмите **Данные дампа**.
3. Укажите адреса электронной почты получателей.
4. В **Диапазон времени** укажите диапазон времени.
5. Щелкните **Отправить**.

3.18.3 Сводка руководства

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

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

Список доступных виджетов:

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

Настройка сводки руководства включает в себя следующие возможности:

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

- Изменение порядка виджетов в каждом разделе.
- Добавление или удаление виджетов.
- Настройка виджетов.

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

3.18.3.1 Создание сводки руководства

Чтобы создать сводку руководства:

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

3.18.3.2 Настройка сводки руководства

Порядок добавления раздела

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

Порядок переименования раздела

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

Порядок удаления раздела

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

Порядок добавления виджета с настройками по умолчанию в раздел

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

Порядок добавления настраиваемого виджета в раздел

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

Порядок добавления виджета с настройками по умолчанию в отчет

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

Порядок добавления настраиваемого виджета в отчет

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

Порядок сброса настроек виджета по умолчанию

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

Порядок настройки виджета

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

3.18.3.3 Отправка сводки руководства

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

Порядок отправки сводки руководства

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

3.18.4 Часовые пояса в отчете

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

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

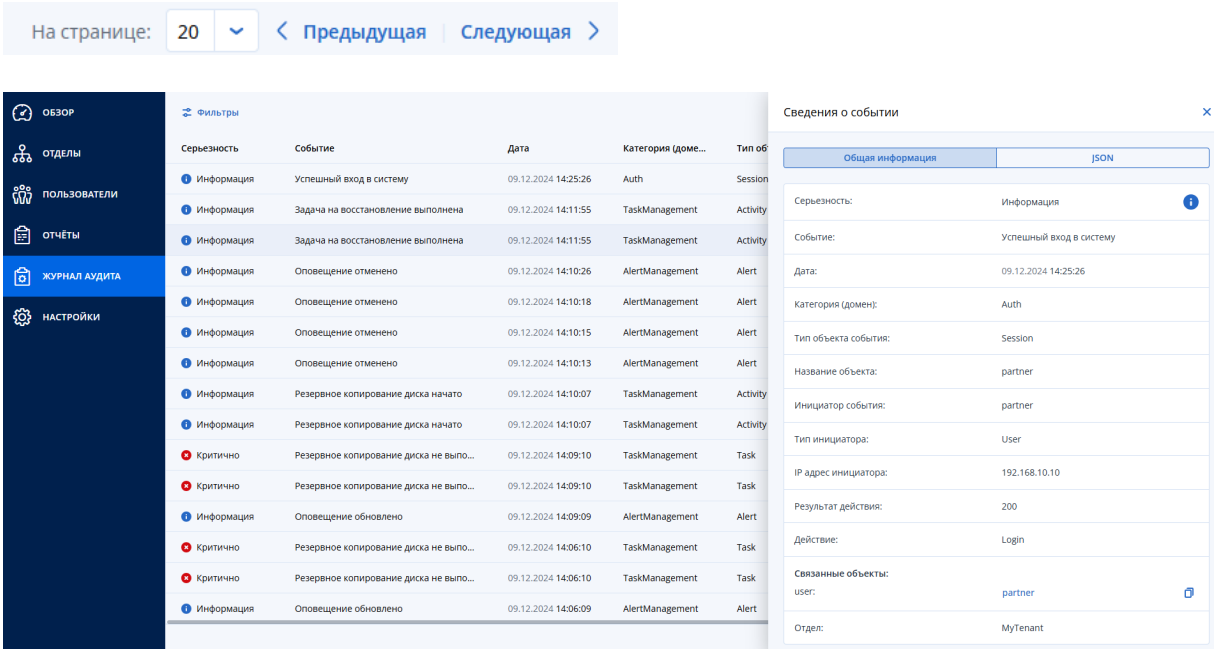
	экспорта отчета. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Отчеты > Операции (запланированная доставка)	• Время доставки отчета указано в часовом поясе UTC. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Пользователи > Имя пользователя > Ежедневные краткие сведения об активных оповещениях	• Этот отчет отправляется один раз в промежуток между 10:00 и 23:59 UTC. Время отправки отчета зависит от рабочей нагрузки центра обработки данных. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.

3.19 Журнал аудита

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

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

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



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

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

3.19.1 Основной поиск событий

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

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

3.19.2 Расширенный поиск событий

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

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

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

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

Параметры расширенного поиска

Параметр	Описание	Примеры
uuid	Идентификатор события. Идентификатор можно узнать, просмотрев JSON-представление события.	• uuid = '0193c41a-6f13-7aa4-8448-2cad89f23385'
tenant_name	Название тенанта.	• tenant_name = 'MyTenant'
src_ip	IP-адрес и порт инициатора события.	• src_ip LIKE '192.168.10.10%'
level	Уровень важности события. Возможные значения: • info – информация; • warning – предупреждение; • critical – критично; • error – ошибка.	• level = 'warning'
obj_name	Имя объекта события.	• obj_name = 'WIN2019X64-5\\Administrator'
obj_domain	Категория (область) события. Возможные значения можно узнать, просмотрев JSON-представления событий.	• obj_domain = 'TaskManagement'
obj_type	Название типа объекта события. Возможные значения можно узнать, просмотрев JSON-представления событий.	• obj_type = 'Task'
obj_subtype	Название подтипа объекта события. Возможные значения можно узнать, просмотрев JSON-представления событий.	• obj_subtype = 'Backup::Disks'
action	Название действия. Возможные значения можно узнать, просмотрев JSON-представления событий.	• action IN ('Login', 'Logout')
status	Результат действия.	• status = '200'
principal_type	Название типа инициатора события. Возможные значения: • User – инициатором события является пользователь; • ServiceAccount – инициатором события является системный компонент.	• principal_type = 'User'
principal_name	Имя инициатора события.	• principal_name LIKE '%admin%'
event.timestamp	Дата и время события. Операторы поиска **<**, **>**, **=**, **!=**, **IN**, **NOT IN** и **LIKE** не поддерживаются.	• event.timestamp <= '2024-11-30 12:00:00Z' • event.timestamp >= '2024-11-30 12:00:00Z'

Операторы расширенного поиска

Оператор	Описание	Примеры
<параметр> = <значение>	Оператор сравнения "равно".	• level = 'warning'
<параметр> != <значение>	Оператор сравнения "не равно".	• level != 'info'
<параметр> < <значение>	Оператор сравнения "меньше".	• status < '400'
<параметр> > <значение>	Оператор сравнения "больше".	• status > '200'
<параметр> <= <значение>	Оператор сравнения "меньше или равно".	• event.timestamp <= '2024-11-30 12:00:00Z'
<параметр> >= <значение>	Оператор сравнения "больше или равно".	• event.timestamp >= '2024-11-30 12:00:00Z'
<выражение> AND <выражение>	Логический оператор "И".	• src_ip LIKE '192.168.10.10%' AND level = 'info'
<выражение> OR <выражение>	Логический оператор "ИЛИ".	• level = 'critical' OR level = 'warning'
<параметр> IN (<значение 1>, ..., <значение n>)	Проверяет, присутствует ли значение параметра в заданном наборе значений.	• level IN ('critical', 'warning')
<параметр> NOT IN (<значение 1>, ..., <значение n>)	Проверяет, отсутствует ли значение параметра в заданном наборе значений.	• level NOT IN ('critical', 'warning')
<параметр> LIKE <шаблон значения>	Проверяет, соответствует ли значение параметра указанному шаблону (регистр символов не учитывается). В шаблоне можно использовать знак процента (**%**), который подменяет любую, в том числе и пустую, последовательность символов.	• principal_name LIKE '%admin%'

3.19.3 Использование сохраненных поисковых запросов

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

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

3.19.4 Отправка записей журнала аудита на Syslog-сервер

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

3.19.4.1 Предварительные требования для протокола TLS

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

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

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

3.19.4.2 Настройка отправки записей на Syslog-сервер

Для настройки выполните следующие действия:

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

подлинности сервиса Кибер Бэкап Облачный.

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

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

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

4. Нажмите **Сохранить**.

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

3.19.5 Регистрируемые события

В журнале аудита Кибер Бэкап Облачный фиксируются события следующих категорий:

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

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

3.19.5.1 События оповещений

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Оповещение создано (Alert created)	Информация (info)	Имя ресурса	Alert	-	200
Оповещение обновлено (Alert	Информация (info)	Имя ресурса	Alert	-	200

updated)					
Оповещение отменено (Alert reset)*	Информация (info)	Имя ресурса	Alert	Имя пользователя	204

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

3.19.5.2 События действий с планами защиты

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

3.19.5.3 События действий с устройствами и их группами

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

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

3.19.5.4 События аутентификации и авторизации

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

3.19.5.5 События действий с тенантами

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Тенант создан (Tenant created)	Информация (info)	Имя созданного тенанта	Tenant	Имя пользователя	200
Тенант обновлён (Tenant updated)	Информация (info)	Имя обновлённого тенанта	Tenant	• Имя пользователя (при обновлении имени тенанта любого типа, при включении тенанта, а	200

				также при любом обновлении тенанта типа **Клиент**); • '-' (при обновлении родительского тенанта, кроме его имени).	
Тенант отключён (Tenant disabled)	Предупреждение (warning)	Имя обновлённого тенанта	Tenant	Имя пользователя	200
Тенант удалён (Tenant deleted)	Предупреждение (warning)	Имя удалённого тенанта	Tenant	Имя пользователя	200
Изменение привилегий пользователя (User privileges updated)	Информация (info)	-	UserPrivileges	Имя пользователя, совершившего действие	200
Учётная запись пользователя создана (User created)	Информация (info)	Имя пользователя	User	Имя пользователя	200
Учётная запись пользователя обновлена (User updated)	Информация (info)	Имя (логин) обновлённого пользователя	User	Имя пользователя	200
Учётная запись пользователя отключена (User disabled)	Предупреждение (warning)	Имя обновлённого пользователя	User	Имя пользователя	200
Учётная запись пользователя включена (User enabled)	Предупреждение (warning)	Имя изменённого пользователя	User	Имя пользователя, совершившего действие	200

Пароль сброшен (User reset)	Предупреждение (warning)	Имя обновлённого пользователя	User	Имя пользователя	200
Учётная запись пользователя удалена (User deleted)	Критично (critical)	Имя пользователя	User	Имя пользователя	200
Служебная учётная запись создана (Account created) **Примечание** При работе с API-клиентами.	Информация (info)	Имя API-клиента	ServiceAccount	Имя пользователя	200
Служебная учётная запись обновлена (Account updated) **Примечание** При работе с API-клиентами.	Информация (info)	Имя API-клиента	ServiceAccount	Имя пользователя	200
Служебная учётная запись удалена (Account deleted) **Примечание** При работе с API-клиентами.	Информация (info)	Имя API-клиента	ServiceAccount	Имя пользователя	200
Секрет служебной	Информация (info)	Имя API-клиента	ServiceAccount	Имя пользователя	200

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

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

3.19.5.6 События резервного копирования

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

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

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

3.19.5.7 События лицензирования

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

3.19.5.8 События регистрации агентов

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

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

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 клиента все хранилища данных, назначенные тенанту клиента 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 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 многоточия , 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. 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 Настройка периода бездействия пользователя

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

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

4.5.1 Изменение настройки периода бездействия пользователя

Чтобы изменить настройку периода бездействия пользователя, выполните следующие шаги:

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

периода бездействия пользователя.

5. Для применения настроек нажмите **Сохранить**.

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

4.5.2 Сброс настройки периода бездействия пользователя

Чтобы сбросить настройку периода бездействия пользователя, выполните следующие шаги:

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

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

4.6 Настройка числа неуспешных попыток входа

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

Администратор может изменить значение настройки для своего тенанта и дочерних тенантов.

Чтобы изменить значение настройки:

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

4.7 Интеграция с системами сторонних производителей

Поставщик услуг может интегрировать Кибер Бэкап Облачный со сторонними системами 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.

Этот способ интеграции платформы требует навыков программирования.

4.7.1 Управление клиентами API

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

4.7.1.1 Что такое клиент API?

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

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

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

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

Для клиента API можно включить двухфакторную аутентификацию.

4.7.1.2 Типовая процедура интеграции

1. Администратор создаёт клиент API в тенанте, которым будет управлять сторонняя система.
2. Администратор включает поток учётных данных клиента OAuth 2.0 в сторонней системе.
   Согласно этому потоку, перед доступом к тенанту и его службам через API система сначала должна отправить учётные данные созданного клиента на платформу, используя API авторизации. Платформа создаёт и отправляет обратно маркер безопасности – уникальную криптографически защищённую строку, которая назначается только данному клиенту. После этого система должна добавить этот маркер во все запросы API.
   Маркер безопасности устраняет необходимость передачи учётных данных клиента с запросами API. Для обеспечения дополнительной безопасности срок действия маркера истекает через два часа. По истечении этого времени просроченный маркер даёт сбой, после чего системе необходимо запросить новый маркер с платформы.

4.7.1.3 Создание клиента API

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

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

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

4.7.1.4 Сброс значения секрета клиента API

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

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

   Для всех маркеров безопасности, назначенных этому клиенту, немедленно завершится срок действия, а запросы API с этими маркерами завершатся сбоем.
6. Скопируйте и сохраните новое значение секрета клиента.

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

4.7.1.5 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.

4.7.1.6 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.

4.7.1.7 Удаление клиента API

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

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

   Внимание

   Восстановить удаленный клиент невозможно.

Указатель

О

П

Ч

Э