КИБЕРПРОТЕКТ

Кибер Бэкап Облачный 21.06

РУКОВОДСТВО АДМИНИСТРАТОРА КОМПАНИИ

Редакция: 21.06.2022

Содержание

Заявление об авторских правах

Все права защищены.

Все остальные упоминаемые товарные знаки могут быть зарегистрированными товарными знаками соответствующих владельцев.

Распространение существенно измененных версий данного руководства запрещено без явного разрешения владельца авторских прав.

Распространение настоящих или переработанных материалов, входящих в данное руководство, в виде печатного издания (книги) запрещено без письменного разрешения их владельца.

ДОКУМЕНТАЦИЯ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». НЕ СУЩЕСТВУЕТ НИКАКИХ ЯВНО ВЫРАЖЕННЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ОБЯЗАТЕЛЬСТВ, ПОДТВЕРЖДЕНИЙ ИЛИ ГАРАНТИЙ, В ТОМ ЧИСЛЕ И СВЯЗАННЫХ С ТОВАРНОСТЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ ПРИГОДНОСТЬЮ ЕГО ДЛЯ ИСПОЛЬЗОВАНИЯ В ОПРЕДЕЛЕННЫХ ЦЕЛЯХ, НАСКОЛЬКО ТАКАЯ ОГРАНИЧЕННОСТЬ ОТВЕТСТВЕННОСТИ ДОПУСКАЕТСЯ ЗАКОНОМ.

1 О документе

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

2 О портале управления

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

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

2.1 Учетные записи и отделы

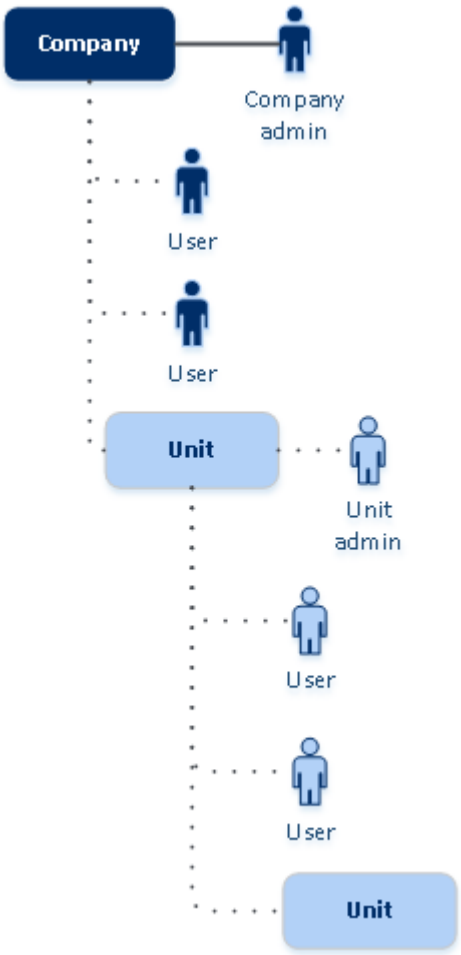
Учетные записи бывают двух типов: администраторы и пользователи.

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

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

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

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



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

Операция	Пользователи	Администраторы
Создать отделы	Нет	Да
Создание учетных записей	Нет	Да
Загрузить и установить программное обеспечение	Да	Да
Использовать службы	Да	Да
Создание отчетов об использовании сервиса	Нет	Да

2.2 Управление квотами

Квоты позволяют установить ограничения на использование службы для клиента.

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

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

2.2.1 Просмотр квот для вашей организации

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

Квоты резервного копирования

Можно указать квоту облачного хранилища данных, квоту локального резервного копирования и максимальное количество машин/устройств/веб-сайтов, которые может защитить пользователь. Доступны указанные ниже квоты.

Квоты для устройств

- **Рабочие станции**
- **Серверы**
- **Виртуальные машины**
- **Мобильные устройства**
- **Серверы веб-хостинга**
- **Веб-сайты**

Машина/устройство/веб-сайт считаются защищенными, если к ним применен как минимум один план защиты. Мобильное устройство становится защищенным после первого резервного копирования.

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

Квоты для источников облачных данных

- **Рабочие места Microsoft 365**

  Эта квота применяется поставщиком услуг для всей компании. Компании можно предоставить разрешение на защиту **почтовых ящиков** и (или) файлов **OneDrive**. Администраторы компании могут просматривать квоты и данные об их использовании на портале управления.

  Примечание
  Общие папки используют лицензии из квоты резервного копирования для рабочих мест Microsoft 365.

- **Microsoft 365 Teams**

  Эта квота применяется поставщиком услуг для всей компании. Эта квота активирует или отключает возможность защитить Microsoft 365 Teams и задать максимальное количество рабочих групп, которые можно защитить. Для защиты одной рабочей группы (независимо от

количества участников или каналов в ней) требуется одна квота. Администраторы компании могут просматривать квоты и данные об их использовании на портале управления.

- **Microsoft 365 SharePoint Online**

  Эта квота применяется поставщиком услуг для всей компании. Эта квота активирует или отключает возможность защитить сайты SharePoint Online и задает максимальное количество коллекций сайтов и сайтов группы, для которых можно включить защиту.

  Администраторы компании могут просматривать квоту на портале управления. Кроме того, в отчетах об использовании они могут просматривать сведения о квоте вместе с объемом хранилища, занятого резервными копиями SharePoint Online.

- **Рабочие места Google Workspace**

  Эта квота применяется поставщиком услуг для всей компании. Компании можно предоставить разрешение на защиту почтовых ящиков **Gmail** (включая календари и контакты) и (или) хранилища **Google Диск**. Администраторы компании могут просматривать квоты и данные об их использовании на портале управления.

- **Общий диск Google Workspace**

  Эта квота применяется поставщиком услуг для всей компании. Эта квота активирует или отключает возможность защитить общие диски Google Workspace. Если эта квота включена, можно включить защиту для любого количества общих дисков. Администраторы компании не могут просматривать данную квоту на портале управления, но могут просматривать объем хранилища, занятого резервными копиями общего диска в отчетах об использовании.

  Резервное копирование общих дисков Google Workspace доступно только клиентам, которые имеют как минимум одну дополнительную квоту для рабочих мест Google Workspace. Эта квота не используется, а только проверяется.

Рабочее место Microsoft 365 считается защищенным, если к почтовому ящику или OneDrive пользователя применен как минимум один план защиты. Рабочее место Google Workspace считается защищенным, если к почтовому ящику или хранилищу Google Диск пользователя применен как минимум один план защиты.

При превышении максимально допустимого количества рабочих мест администратор компании не может применить план защиты к дополнительным рабочим местам.

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 коты для хранилища резервных копий и квот для аварийного восстановления. Квота хранения данных ограничивает общий размер резервных копий, размещенных в облачном хранилище данных. При выходе за пределы значения превышения квоты хранения резервной копии резервное копирование не выполняется.

2.2.2 Определение квот для пользователей

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

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

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

Пример

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

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

Квоты резервного копирования

Можно указать квоту хранилища резервных копий и максимальное количество машин/устройств/веб-сайтов, которые может защитить пользователь. Доступны указанные ниже квоты.

Квоты для устройств

- **Рабочие станции**
- **Серверы**
- **Виртуальные машины**
- **Веб-сайты**

Машина/устройство/веб-сайт считаются защищенными, если к ним применен как минимум один план защиты.

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

Квота для хранилища данных

- **Хранилище резервных копий**

Квота хранения данных ограничивает общий размер резервных копий, размещенных в облачном хранилище данных. При выходе за пределы значения превышения квоты хранения резервной копии резервное копирование не выполняется.

2.3 Поддерживаемые веб-браузеры

Веб-интерфейс сервиса резервного копирования поддерживает перечисленные ниже браузеры:

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

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

3 Пошаговые инструкции

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

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

3.1 Активация учетной записи администратора

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

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

3.2 Доступ к порталу управления и службам

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

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

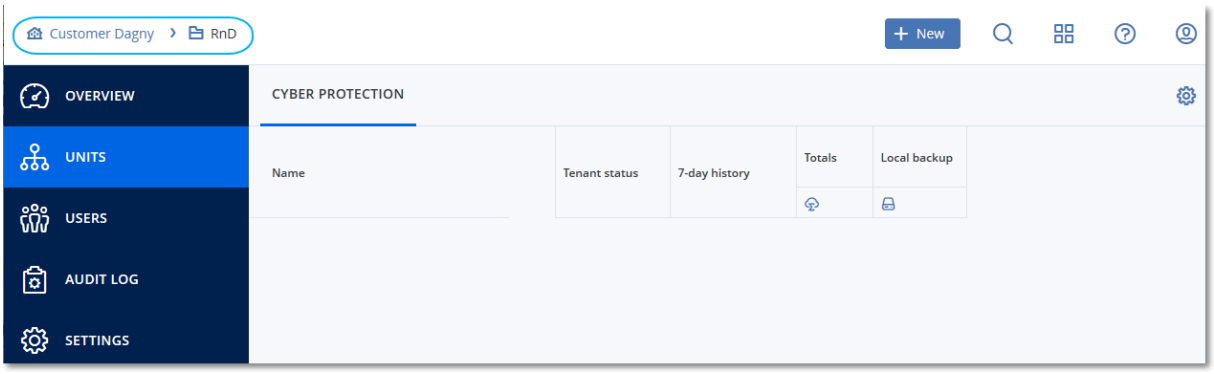
3.2.1 Переключение между порталом управления и консолями служб

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

3.3 Навигация на портале управления

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

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



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

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

3.4 Создание отдела

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

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

Порядок создания отдела

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

5. [Дополнительно] В поле **Язык** измените язык по умолчанию для уведомлений, отчетов и программного обеспечения, который будет использоваться в этом отделе.
6. Выполните одно из следующих действий:
   - Чтобы создать администратора отдела, нажмите кнопку **Далее**, а затем следуйте шагам, описанным в разделе "Создание учетной записи пользователя", начиная с шага 4.
   - Чтобы создать отдел без администратора, щелкните **Сохранить и закрыть**. Администраторов и пользователей можно добавить в отдел позже.

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

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

3.5 Создание учетной записи пользователя

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

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

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

Порядок создания учетной записи пользователя

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

     Внимание
     У каждой учетной записи должно быть уникальное имя входа.

   - **Электронная почта**
   - Необязательно:**Имя**
   - Необязательно: **Фамилия**
   - В поле **Язык** измените язык, который по умолчанию используется для уведомлений, отчетов и программного обеспечения для этой учетной записи.
5. Выберите службы, к которым пользователь будет иметь доступ и роли в каждой службе.

- Если установлен флажок **Администратор компании**, пользователь будет иметь доступ к порталу управления и роль администратора во всех службах.
- Если установлен флажок **Администратор отдела**, у пользователя будет доступ к порталу управления. При этом, в зависимости от службы, пользователь может иметь или не иметь роль администратора службы.
- В противном случае пользователь будет иметь роли, которые выбраны в выбранных службах.

6. Нажмите кнопку **Создать**.

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

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

Порядок сброса пароля пользователя

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

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

3.6 Роли пользователя, доступные для каждой службы

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

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

Сервис	Роль	Описание
Недоступно	Администратор компании	Эта роль предоставляет права администратора для всех служб. Эта роль позволяет получить доступ к корпоративному списку разрешений. Если для данной компании включена функция "Аварийное восстановление" службы Кибер Бэкап Облачный, эта роль также предоставляет доступ к функциональности аварийного восстановления.
Портал управления	Администратор	Эта роль предоставляет доступ к порталу управления, на котором администратор может управлять пользователями во всей организации.
	Администратор с	Эта роль предоставляет доступ только для чтения ко всем объектам

	доступом только для чтения	на портале управления. Такие пользователи могут получить доступ к данным других пользователей организации в режиме "только чтение".
Кибер Бэкап Облачный	Администратор	Эта роль позволяет настраивать службу Кибер Бэкап Облачный и управлять ею для ваших пользователей. Эта роль требуется для настройки функции "Аварийное восстановление" и корпоративного списка разрешений и управления ими.
	Администратор с доступом только для чтения	Эта роль предоставляет доступ только для чтения ко всем объектам службы Кибер Бэкап Облачный. Такие пользователи могут получить доступ к данным других пользователей организации в режиме "только чтение". Администратор с доступом только для чтения не может настраивать функцию "Аварийное восстановление" или корпоративный список разрешений и управлять ими.
	Пользователь	Эта роль позволяет использовать сервис Кибер Бэкап Облачный, но не предоставляет в отношении нее права администратора. Такие пользователи не могут получить доступ к данным других пользователей организации.

3.6.1 Роль администратора с доступом только для чтения

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

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

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

- Запускать или останавливать любые задания.

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

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

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

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

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

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

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

3.7 Изменение настроек уведомлений для пользователя

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

- **Оповещения о превышении квоты** (включено по умолчанию)
  Оповещения о превышенных квотах.
- **Запланированные отчеты использования**
  Описанные ниже отчеты об использовании, которые отправляются в первый день каждого месяца.
- **Уведомления о сбое**, **Уведомления с предупреждениями** и **Успешные уведомления** (отключено по умолчанию)
  Уведомления о результатах выполнения планов защиты и результатах операций аварийного восстановления 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 кратких сведений зависит от рабочей нагрузки центра обработки данных. Если по состоянию на тот момент времени не было никаких активных оповещений, то в кратких сведениях содержится сообщение о том, что все в порядке. В кратких сведениях нет информации о прошлых оповещениях, которые больше не активны. Например, если пользователь отменил оповещение об ошибке резервного копирования или резервное копирование перезапускается и выполняется успешно до формирования кратких сведений, данное оповещение удаляется и не включается в содержимое кратких сведений.
- **Уведомления функции "Контроль устройств"** (выключено по умолчанию)
  Уведомления о попытках использовать периферийные устройства и порты, доступ к которым ограничен в соответствии с планами защиты с включенным модулем контроля устройств.

Все уведомления отправляются на адрес электронной почты пользователя.

3.7.1 Уведомления, полученные ролью пользователя

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

Тип оповещения\роль пользователя	Пользователь	Администратор клиента
Уведомления для собственных устройств	Да	Да
Уведомления для всех устройств в организации	Недоступно	Да
Уведомления для Microsoft 365 и других облачных резервных копий	Недоступно	Да

3.8 Отключение и включение учетной записи пользователя

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

Порядок отключения учетной записи пользователя

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

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

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

3.9 Удаление учетной записи пользователя

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

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

Внимание
Удаление учетной записи пользователя необратимо.

Порядок удаления учетной записи пользователя

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

В результате:

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

3.10 Передача прав владения учетной записи пользователя

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

Внимание
Содержимое удаленной учетной записи будет невозможно назначить заново.

Порядок передачи прав владения учетной записи пользователя

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

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

3.11 Настройки двухфакторной проверки подлинности

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

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

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

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

3.11.1 Принципы работы

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

     Версия для iOS (https://itunes.apple.com/sg/app/google-authenticator/id388497605?mt=8)

     Версия для Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_SG)
   - Microsoft Authenticator

     Версия для iOS (https://app.adjust.com/n094ls?campaign=appstore_ios&fallback=https://itunes.apple.com/app/microsoft-authenticator/id983156458)

     Версия для Android (https://app.adjust.com/n094ls?campaign=appstore_android&fallback=https://play.google.com/store/apps/details?id=com.azure.authenticator)

Внимание
Необходимо убедиться, что время на устройстве с приложением проверки подлинности установлено правильно и соответствует фактическому.

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

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

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

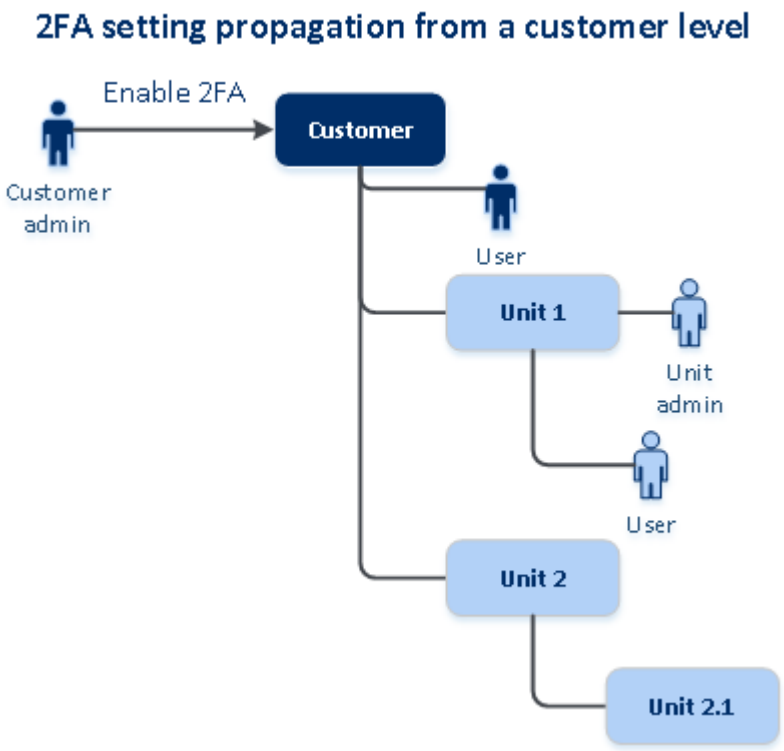
С этого момента при входе в систему после ввода учетных данных у пользователей будет запрашиваться одноразовый код TOTP, сгенерированный в приложении проверки подлинности. При входе в систему пользователи могут пометить используемый браузер как доверенный. После этого при последующих входах в систему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

3.11.2 Распространение настроек двухфакторной проверки подлинности на уровни клиента

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

Настройки двухфакторной проверки подлинности распространяются по уровням клиента следующим образом:

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



Примечание

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

3.11.3 Настройка двухфакторной проверки подлинности для вашего клиента

Порядок включения двухфакторной проверки подлинности для вашего клиента

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.

Порядок отключения двухфакторной проверки подлинности для вашего клиента

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

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

3.11.4 Управление двухфакторной проверкой подлинности для пользователей

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

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.

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.

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.

Порядок отключения двухфакторной проверки подлинности для пользователя

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

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

1. На портале управления на вкладке **Пользователи** найдите пользователя, для которого необходимо изменить настройки, а затем щелкните значок многоточия.
2. Щелкните **Отметить как сервисную учетную запись**. В результате пользователь получит особый статус двухфакторной проверки подлинности, который называется **Учетная запись службы**.
3. [Если у клиента 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.

Порядок включения двухфакторной проверки подлинности для пользователя

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

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

3.11.5 Сброс двухфакторной проверки подлинности при утрате устройства второго фактора

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

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

3.11.6 Защита от атак методом перебора

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

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

Параметры защиты от таких атак предварительно заданы на платформе.

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

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

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

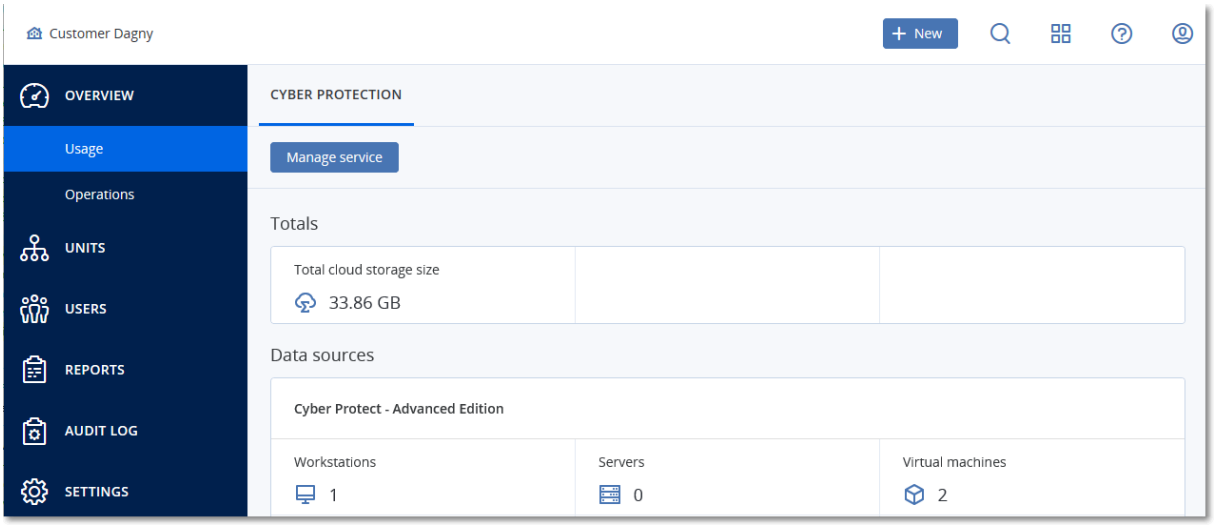
Попытки ввода кода TOTP регистрируются для каждого пользователя, а не для устройства. Это означает, что, если пользователь попытается ввести код TOTP с других устройств, он все равно будет заблокирован.

4 Мониторинг

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

4.1 Использование

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



4.2 Операции

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

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

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

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

Порядок изменения расположения виджетов на панели мониторинга

Перетащите виджеты, щелкнув их имена.

Порядок изменения виджета

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

Порядок добавления виджета

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

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

Порядок удаления виджета

Щелкните значок X рядом с именем виджета.

4.2.1 Статус защиты

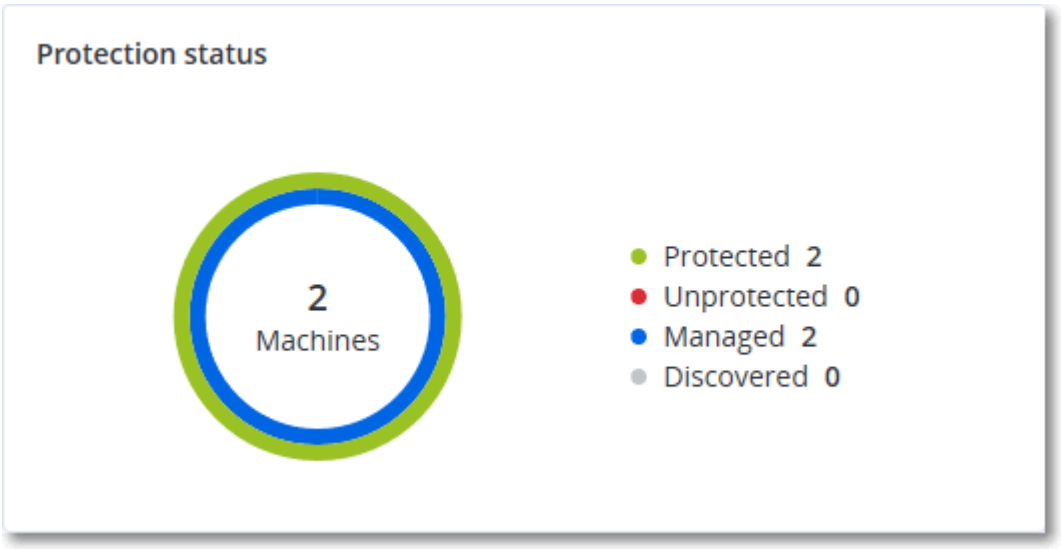
Статус защиты

В этом виджете показано текущее состояние защиты для всех машин.

Машина может быть в одном из следующих состояний:

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

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



Обнаруженные машины

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

Discovered machines

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

4.2.2 Сведения о сканировании резервной копии

В этом виджете показана подробная информация об обнаруженных угрозах в резервных копиях.

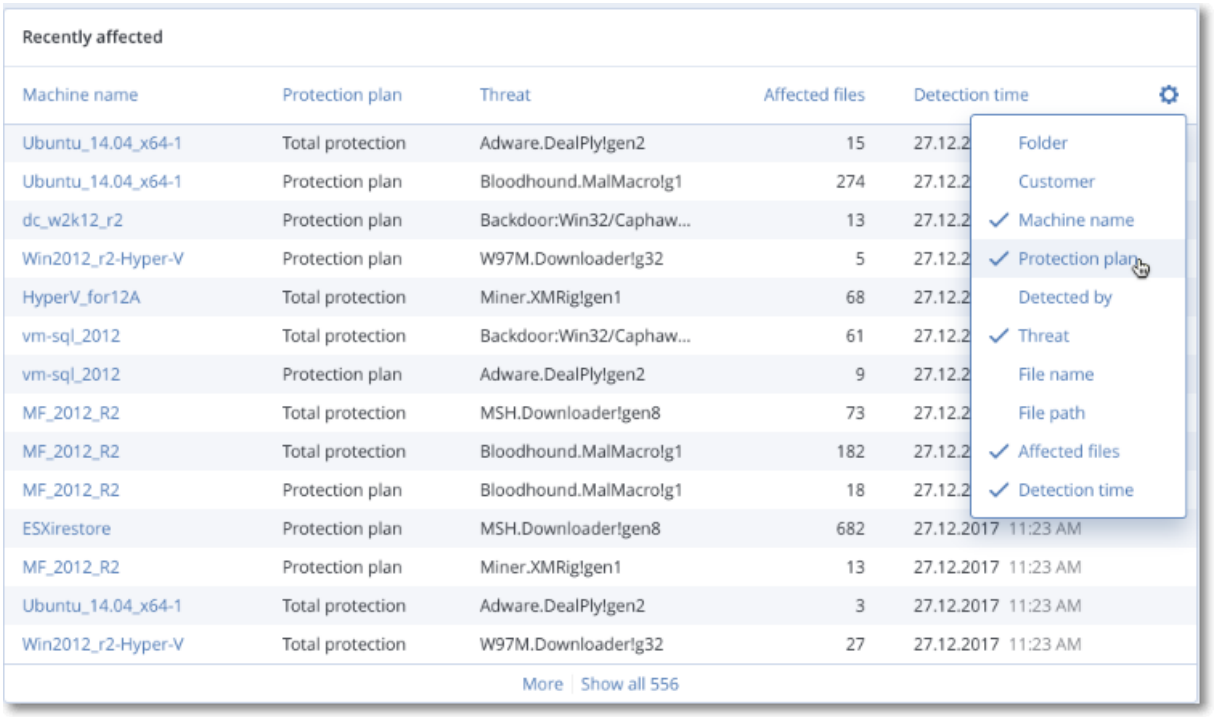
Backup scanning details (threats)

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

4.2.3 Последние затронутые

В этом виджете показана подробная информация о машинах, которые были инфицированы недавно. В частности, показана информация об обнаруженных угрозах и количество инфицированных файлов.



4.2.4 Заблокированные URL-адреса

В виджете отображается статистическая информация о заблокированных URL-адресах по категориям. Дополнительную информацию о фильтрации и категоризации URL-адресов см. руководстве пользователя по Cyber Protection.

5 Отчеты

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

Примечание
Эта функциональность недоступна в редакции Standard сервиса Кибер Бэкап Облачный.

5.1 Использование

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

5.1.1 Тип отчета

Можно выбрать один из указанных ниже типов отчета:

- **Текущее использование**
  В отчете содержатся показатели текущего использования службы.
- **Сводка за период**
  В отчете содержатся показатели использования службы за конец указанного периода и разница между показателями в начале и в конце указанного периода.
- **Ежедневно за период**
  В отчете содержатся показатели использования службы и данные об их изменении за каждый день указанного периода.

5.1.2 Область отчета

Можно выбрать область отчета из указанных ниже значений:

- **Непосредственные пользователи и партнеры**
  В отчете будут содержаться показатели использования службы только для непосредственных дочерних отделов компании или отдела, в котором вы работаете.
- **Все пользователи и партнеры**
  В отчете будут содержаться показатели текущего использования службы для всех дочерних отделов компании или отдела, в котором вы работаете.
- **Все клиенты, партнеры и пользователи**
  В отчете будут содержаться показатели текущего использования службы для всех дочерних отделов компании или отдела, в котором вы работаете, а также для всех пользователей в отделах.

5.1.3 Запланированные отчеты

Запланированный отчет охватывает показатели использования службы за последний полный календарный месяц. Данные отчеты формируются в 23:59:59 (по времени UTC) в первый день месяца и отправляются во второй день месяца. Они отправляются всем администраторам

компании или отдела, которые в пользовательских параметрах установили флажок **Запланированные отчеты использования**.

Порядок включения или отключения запланированного отчета

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

5.1.4 Пользовательские отчеты

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

Порядок формирования пользовательского отчета

1. Войдите на портал управления.
2. Выберите отдел, для которого необходимо создать отчет.
3. Щелкните **Отчеты** > **Использование**.
4. Щелкните **Настраиваемый**.
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**.

5.1.5 Отчеты об использовании

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

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

- Цена по отделам, пользователям и типам устройств.
- Общий размер резервных копий.
- Общее количество защищенных устройств.
- Общая стоимость.

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

5.2 Операции

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

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

Для просмотра отчета щелкните его имя.

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

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

Вы можете использовать предварительно созданные отчеты или создать пользовательский отчет.

Ниже перечислены отчеты по умолчанию

Имя отчета	Описание
Оповещения	Показывает оповещения, выполненные за указанный период времени.
Сведения о сканировании резервной копии	Показывает подробную информацию об угрозах, выявленных в резервных копиях.
Ежедневные задания	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Обнаруженные угрозы	Показывает сведения о машинах, на которых выявлены проблемы: количество заблокированных угроз, а также количество машин без уязвимостей и с уязвимостями.
Обнаруженные машины	Показывает все найденные машины в сети организации.
Сводные данные	Показывает сводную информацию об устройствах, защищенных за

	указанный период времени.
Еженедельные действия	Показывает сводную информацию о действиях, выполненных за указанный период времени.

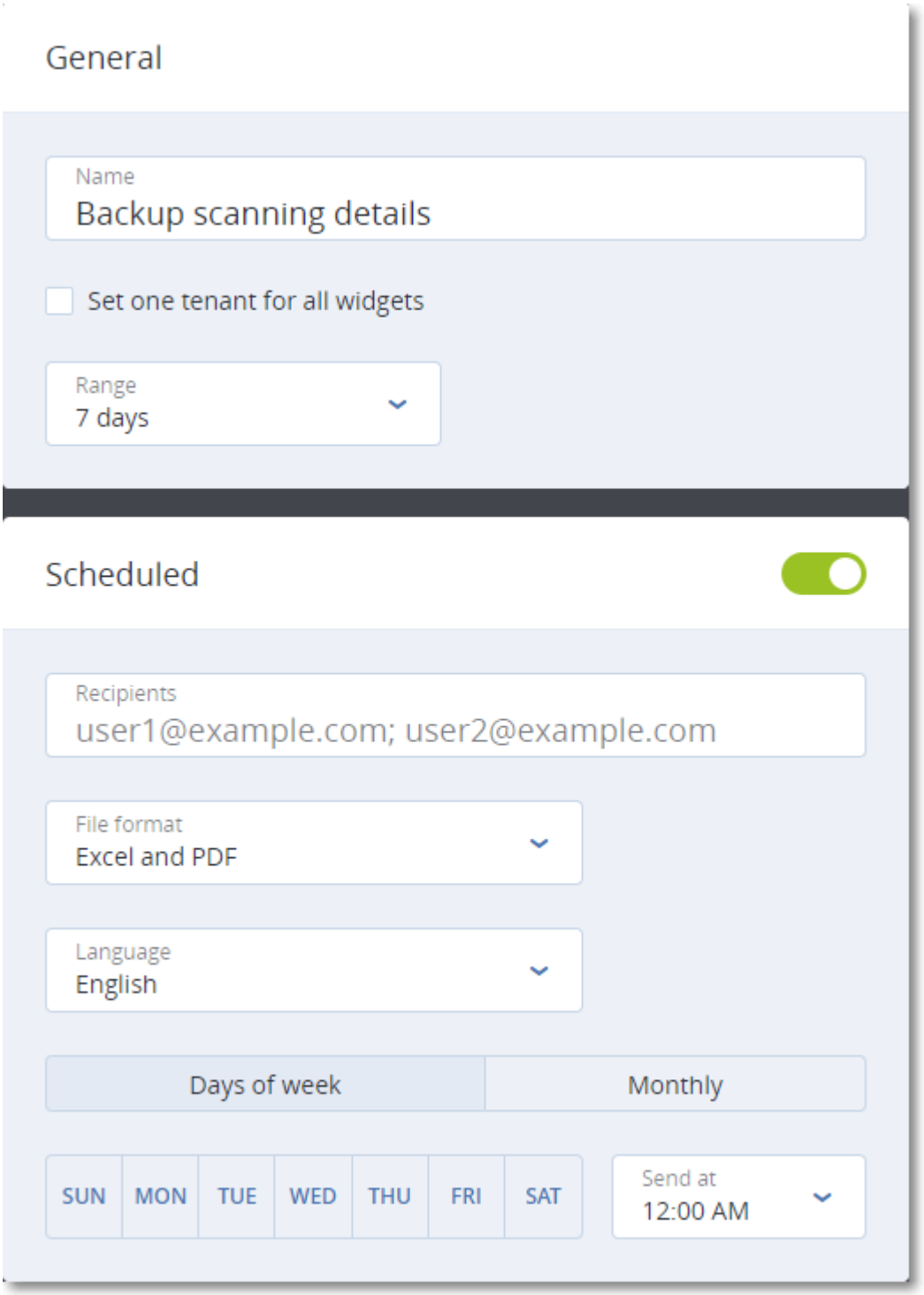
Добавление отчета

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

Изменение отчета

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

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



Планирование отчета

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

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

Экспорт и импорт структуры отчета

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

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

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

Дамп данных отчета

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

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

Дамп данных отчета

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

5.3 Часовые пояса в отчете

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

Расположение и тип отчета	Часовой пояс, используемый в отчете
Портал управления > Обзор > Операции (виджеты)	Время создания отчета указано в часовом поясе машины, в которой запущен браузер.
Портал управления > Обзор > Операции (экспортирован в PDF или xslx)	• Метка времени экспортированного отчета находится в часовом поясе машины, которая использовалась для экспорта отчета. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Отчеты > Использование > Запланированные отчеты	• Отчет создается в 23:59:59 (по времени UTC) в первый день месяца. • Отчет отправляется во второй день месяца.
Портал управления > Отчеты > Использование > Пользовательские отчеты	Для отчета и даты его создания используется часовой пояс UTC.
Портал управления > Отчеты > Операции (виджеты)	• Время создания отчета указано в часовом поясе машины, в которой запущен браузер. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Отчеты > Операции (экспортирован в PDF или xslx)	• Метка времени экспортированного отчета находится в часовом поясе машины, которая использовалась для экспорта отчета. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Отчеты > Операции (запланированная доставка)	• Время доставки отчета указано в часовом поясе UTC. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Пользователи > Ежедневные краткие сведения об активных оповещениях	• Этот отчет отправляется один раз в промежуток между 10:00 и 23:59 UTC. Время отправки отчета зависит от рабочей нагрузки центра обработки данных. • Для действий, которые отображаются в отчете, указано время в часовом поясе UTC.
Портал управления > Пользователи > Уведомления о статусе Cyber	• Этот отчет отправляется, когда действие завершено.

Protection	**Примечание** В зависимости от рабочей нагрузки в центре обработки данных некоторые отчеты могут отправляться с задержкой. • Для действий в отчете указано время в часовом поясе UTC.

6 Журнал аудита

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

В журнал аудита в хронологическом порядке заносятся следующие события:

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

В журнале отображаются события во всей организации или в подразделении, в котором вы работаете в настоящий момент, а также его дочерних подразделениях. Чтобы посмотреть более подробные сведения о событии, щелкните по нему.

Журнал ежедневно очищается. События удаляются через 180 дней.

6.1 Поля журнала аудита

Для каждого события в журнале отображаются указанные ниже данные.

- **Событие**
  Краткое описание события. Пример: **Клиент создан**, **Клиент удален**, **Пользователь создан**, **Пользователь удален**, **Квота достигнута**.
- **Серьезность**
  Принимает перечисленные ниже значения.
  - **Ошибка**
    Обозначает ошибку.
  - **Предупреждение**
    Обозначает действие с потенциально отрицательным эффектом. Пример: **Клиент удален**, **Пользователь удален**, **Квота достигнута**.
  - **Уведомление**
    Обозначает событие, которое может требовать внимания. Пример: **Клиент обновлен**, **Пользователь обновлен**.
  - **Информация**
    Нейтральное изменение или действие информационного характера. Пример: **Клиент создан**, **Пользователь создан**, **Квота обновлена**.
- **Дата**
  Дата и время события.
- **Имя объекта**
  Объект, с которым была выполнена операция. Например для события **Пользователь обновлен** объектом является пользователь, свойства которого были изменены. Для событий, связанных с квотами, объектом является квота.
- **Клиент**

Название отдела, к которому относится объект. Например для события **Пользователь обновлен** клиентом является отдел, в котором расположен пользователь. Для события **Квота достигнута** клиентом является пользователь, для которого достигнута данная квота.

- **Инициатор**

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

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

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

  IP-адрес машины, с которой инициировано событие.

6.2 Фильтрация и поиск

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

7 Дополнительные примеры

7.1 Ограничение доступа к веб-интерфейсу

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

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

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

Порядок ограничения доступа к веб-интерфейсу

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

7.2 Ограничение доступа к вашей компании

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

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

Порядок ограничения доступа к компании

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

7.3 Управление клиентами API

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

7.3.1 Что такое клиент API?

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

Клиент имеет доступ только к пользователю, для которого администратор создал его, а также к его субклиентам.

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

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

Для клиента можно включить двухфакторную аутентификацию.

7.3.2 Типичная процедура интеграции

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

7.3.3 Создание клиента API

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

4. Нажмите кнопку **Далее**.

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

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

7.3.4 Сброс значения секрета клиента API

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

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

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

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

7.3.5 Отключение клиента API

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

   Статус клиента изменится на **Отключен**.

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

Клиент можно заново включить в любое время.

7.3.6 Включение отключенного клиента API

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

   Статус клиента изменится на **Активный**.

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

7.3.7 Удаление клиента API

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

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

Внимание
Восстановить удаленного клиента невозможно.

Указатель

Ф

Ч

Э