КИБЕРПРОТЕКТ

КИБЕР Протего

Версия 10.2

Руководство пользователя веб-консоли

Редакция: 27.03.2024

Заявление об авторских правах

Содержание

1 О веб-консоли

Веб-консоль Cyber Protego – это кроссплатформенное аналитическое решение, которое позволяет строить статистические отчёты на основе данных Management Server.

2 Установка и удаление

Веб-консоль можно установить на следующие 64-битные операционные системы:

- Альт Сервер 10.x с версией ядра 5.10.82-std-def и новее,
- Windows Server 2012 и новее.

Для работы веб-консоли требуется установленная СУБД Microsoft SQL Server 2012 и новее, PostgreSQL / Postgres Pro Standard 11 и новее или Jatoba 4.5 и новее.

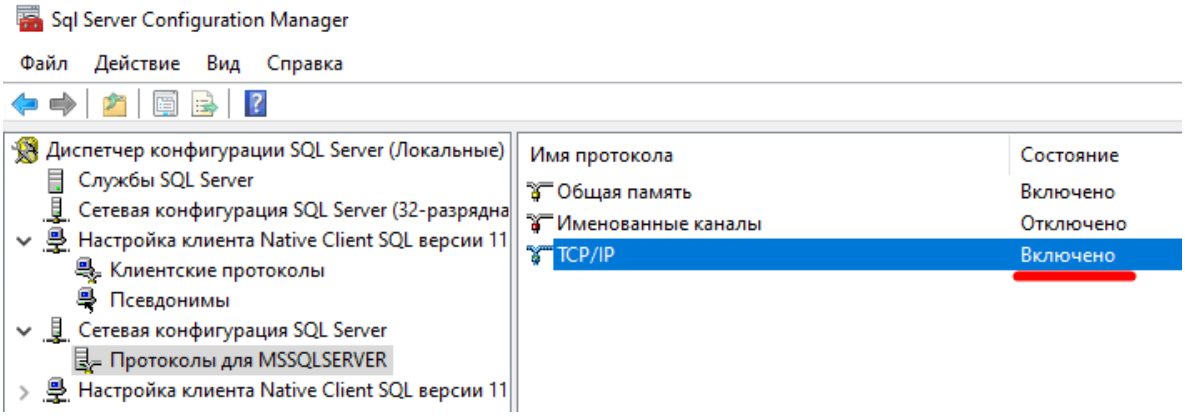
Процедуры установки и удаления веб-консоли описаны в следующих разделах.

2.1 Требования к Microsoft SQL Server

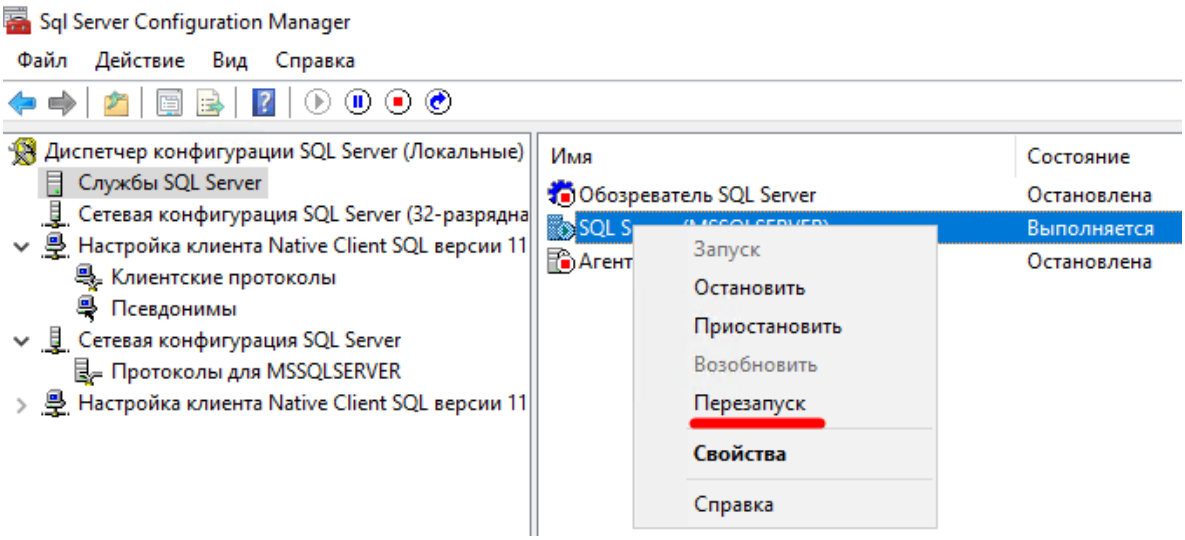
Для использования с веб-консолью СУБД Microsoft SQL Server должна удовлетворять этим требованиям:

- Используется протокол TCP/IP.

  Чтобы включить данный параметр, в консоли **Sql Server Configuration Manager** перейдите на экран **Сетевая конфигурация SQL Server** > **Протоколы для MSSQLSERVER** и измените состояние параметра **TCP/IP** на **Включено**.



  Затем перейдите на экран **Службы SQL Server** и перезапустите службу **SQL Server**.



- Есть поддержка TLS 1.2.

  В версиях 2016 и новее поддержка TLS 1.2 есть по умолчанию. Для более ранних версий необходимо установить обновление. См. Поддержка TLS 1.2 для Microsoft SQL Server.

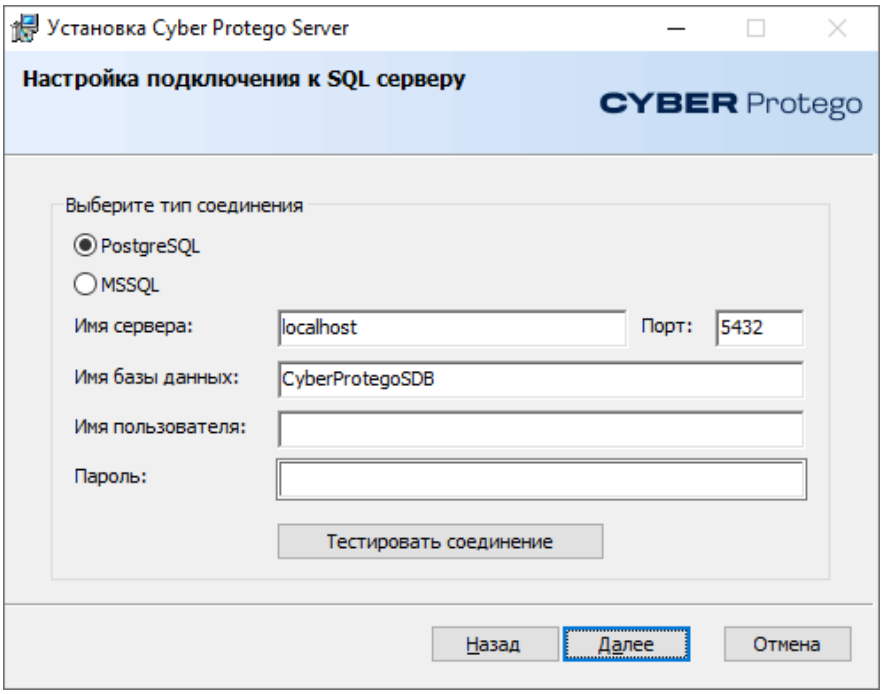
2.2 Установка на Windows

В дистрибутив для Windows входит программа установки CyberProtegoServerInstaller.exe.

Установка выполняется пользователем с привилегиями администратора.

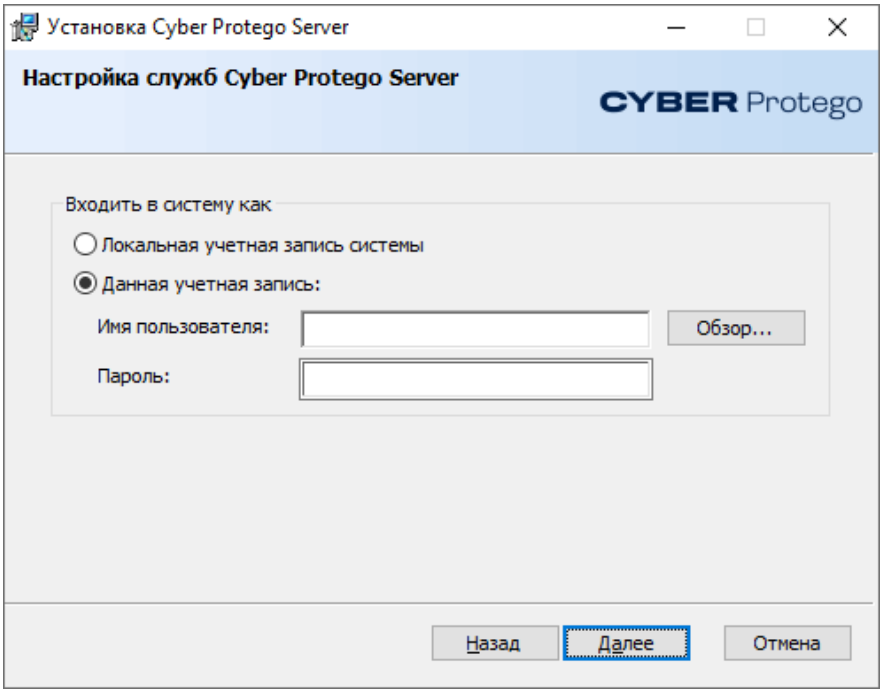
Чтобы установить веб-консоль, выполните следующие действия:

1. Запустите программу установки.
2. На экране приветствия нажмите **Далее**.
3. Примите лицензионное соглашение и нажмите **Далее**.
4. Укажите папку установки и нажмите **Далее**.
5. Укажите параметры служебной БД для размещения данных веб-консоли.



При необходимости проверьте подключение к серверу служебной БД, нажав **Тестировать соединение**. Нажмите **Далее**.

6. Укажите учетную запись, от имени которой будут запущены службы веб-консоли. Данной учетной записи будет дана привилегия **Вход в качестве службы**. Нажмите **Далее**.



7. На экране **Все готово к установке** нажмите **Установить**.
8. Нажмите **Готово**, чтобы выйти из программы установки.

Программа выполнит установку, создаст сертификаты и служебную БД, а также настроит и запустит NGINX.

После установки необходимо указать БД, по данным которой будут строиться отчёты. Выполните шаги из раздела "База данных Management Server" (стр. 35).

Чтобы обновить веб-консоль, также запустите программу установки. При этом вы сможете изменить данные для подключения к БД веб-консоли.

2.3 Установка на Linux

В дистрибутив для Linux входят RPM-пакет cpanalytics-<версия>.x86_64.rpm и скрипт установки start_setup_cpanalytics.sh.

Установка выполняется пользователем с привилегиями sudo.

Чтобы установить веб-консоль, выполните следующие действия:

1. Запустите скрипт установки:

   ```
   $ sudo ./start_setup_cpanalytics.sh
   ```

2. Укажите тип служебной БД для размещения данных веб-консоли: "MSSQL" или "PostgreSQL". Второй вариант также необходимо выбирать для Jatoba.

   ```
   Enter database dialect (MSSQL or PostgreSQL):
   ```

3. Укажите имя сервера служебной БД. Это может быть IP-адрес или имя хоста.

   ```
   Enter database server name:
   ```

4. Укажите порт сервера служебной БД. Нажав **Enter**, можно оставить порт по умолчанию.

   ```
   Enter port [default for PostgreSQL: 5432]:
   ```

5. Укажите имя служебной БД для веб-консоли. Нажав **Enter**, можно оставить порт по умолчанию.

   ```
   Enter database name [default: CyberProtegoSDB]:
   ```

6. Укажите имя пользователя служебной БД:

   ```
   Enter user name:
   ```

7. Укажите пароль пользователя служебной БД:

   ```
   Enter password:
   ```

8. При необходимости проверьте подключение к серверу служебной БД, нажав "Y". Если этого не требуется, нажмите "N".

   ```
   Check connection? (Y/N):
   ```

Скрипт установит необходимые пакеты, проверит подключение к серверу служебной БД (если указано), создаст сертификаты и служебную БД, а также настроит и запустит NGINX.

После установки необходимо указать БД, по данным которой будут строиться отчёты. Выполните шаги из раздела "База данных Management Server" (стр. 35).

Чтобы обновить веб-консоль, также запустите скрипт установки. При этом вы сможете изменить данные для подключения к БД веб-консоли.

2.4 Удаление

Удаление из ОС Windows

Чтобы удалить веб-консоль из ОС Windows, откройте **Панель управления** > **Программы и компоненты**, дважды щелкните **Cyber Protego Server** и выберите **Да** в диалоге удаления.

Будут удалены файлы веб-консоли, остановлены и удалены её службы.

Примечание
Служебная БД не будет удалена.

Удаление из ОС Linux

Чтобы удалить веб-консоль из ОС Linux, выполните следующую команду с привилегиями sudo:

```
$ sudo rpm -e cpanalytics
```

Будет удален RPM-пакет cpanalytics, остановлена и удалена служба cpanalyticsd. Кроме того, будут удалены файлы из директории /opt/cyberprotect/cpserver.

Примечание
Служебная БД не будет удалена.

3 Вход в веб-консоль

Чтобы войти в веб-консоль, перейдите по имени или адресу ее хоста, укажите логин и пароль в соответствующих полях и нажмите **Войти**. Используется протокол HTTPS.

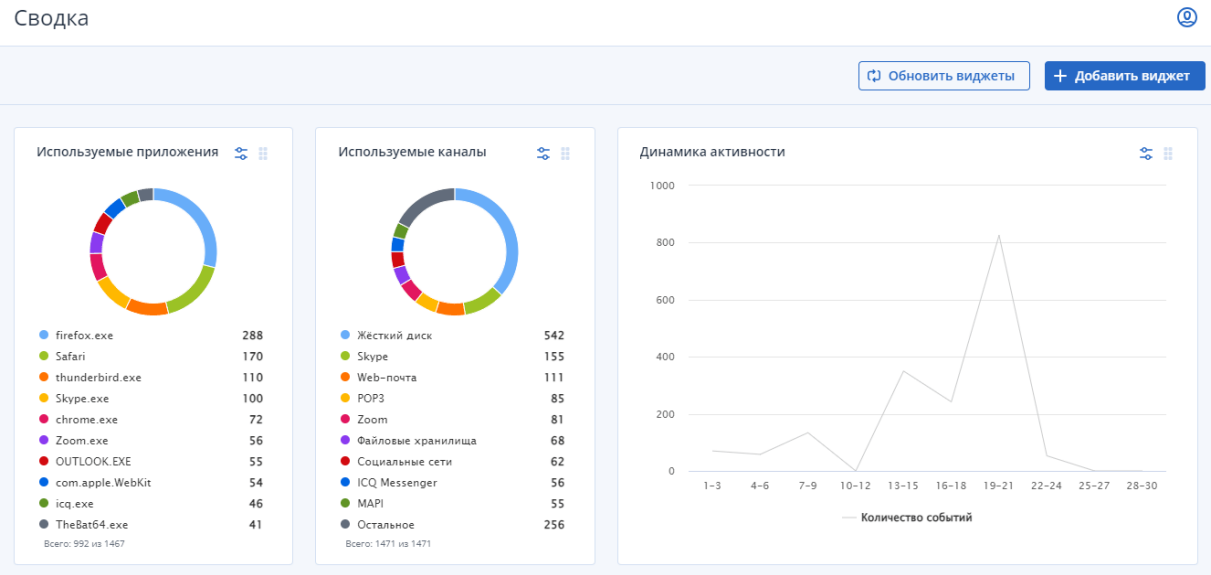
По умолчанию создан пользователь с логином "admin" и паролем "Cp*123456".

При необходимости можно изменить порт веб-консоли (см. "Изменение порта веб-консоли" (стр. 38)) и сертификаты (см. "Установка пользовательских сертификатов" (стр. 39)).

4 Сводка

В данном разделе представлены настраиваемые виджеты, которые вместе составляют сводку по подключенной базе данных Management Server. Набор виджетов может быть уникален для каждого пользователя.

Работать с этим разделом могут только пользователи с соответствующим правом доступа (см. "Роли" (стр. 33)).



Примечание
События, полученные с сервера Кибер Файлов, при построении виджетов не учитываются.

Доступны следующие виджеты:

- **Динамика активности** – количество событий за выбранный интервал времени. Показывает динамику активности пользователей в системе.
- **Используемые приложения** – самые часто используемые приложения. Показывает долю каждого приложения в общем объеме событий.
- **Используемые каналы** – самые часто используемые каналы передачи данных. Показывает распределение событий по каналам.
- **Используемые устройства** – самые часто используемые устройства. Показывает долю каждого устройства в общем объеме событий.
- **Используемые протоколы** – самые часто используемые протоколы. Показывает долю каждого протокола в общем объеме событий.
- **Количество активных пользователей** – количество активных пользователей за выбранный интервал времени. Показывает количество пользователей в журналах по дням.
- **Нарушители контентной политики** – пользователи, нарушающие контентные политики.
- **Применяемые контентные правила** – самые часто применяемые контентно-зависимые правила.

- **Передаваемые форматы файлов** – самые часто передаваемые форматы файлов за выбранный интервал времени. Показывает долю каждого типа файлов в общем объеме событий.

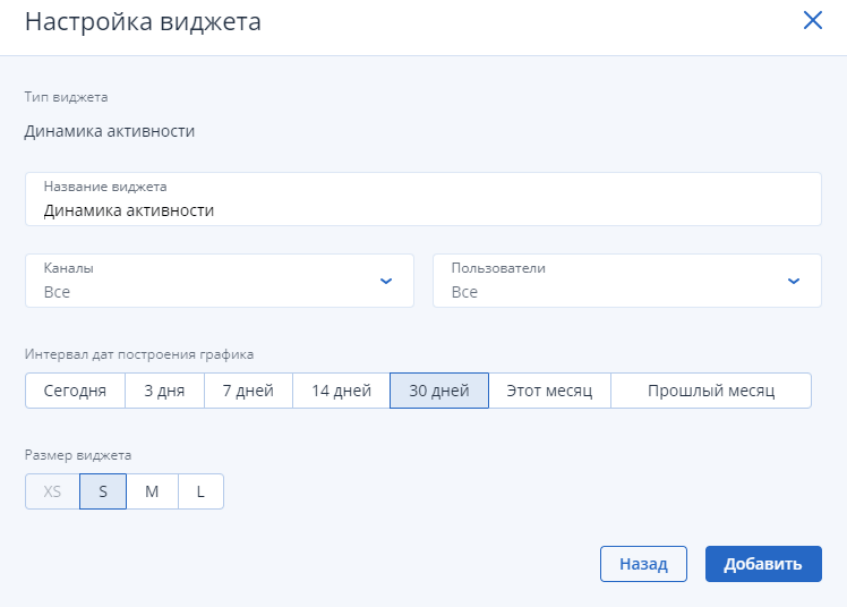
4.1 Управление виджетами

Пользователи могут добавлять, изменять и удалять виджеты в сводке.

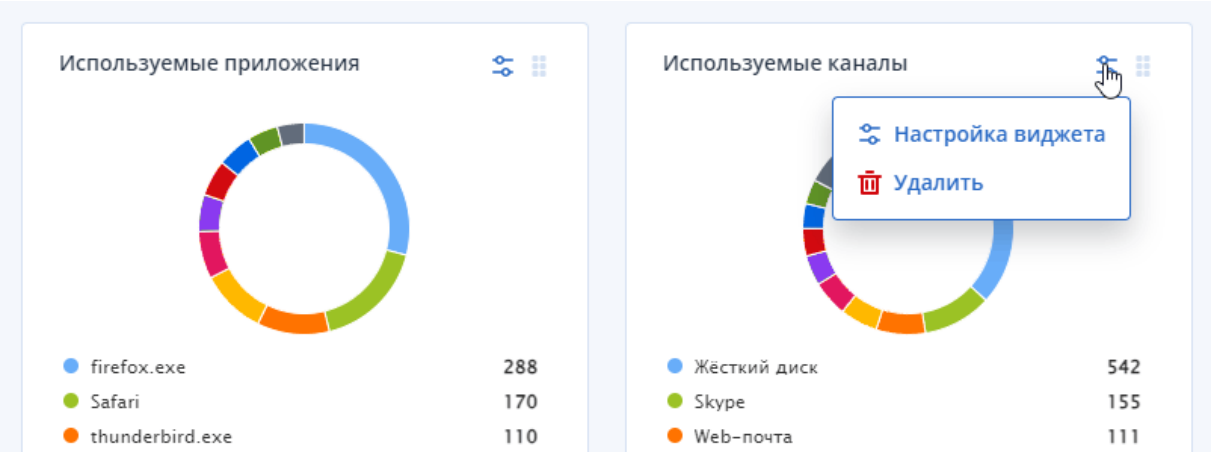
Чтобы создать виджет, щелкните **+ Добавить виджет** справа сверху. В появившемся окне выберите тип виджета. В следующем окне укажите его параметры. Нужно задать **Название виджета**, **Каналы**, **Пользователи**, **Интервал дат построения графика**, размер и количество отображаемых данных. При этом если для отображения выбрать **Топ 10**, в виджете появятся первые десять элементов с наибольшими значениями. Если выбрать **Все данные**, будут отображены первые девять элементов с наибольшими значениями и на десятом месте – элемент **Остальное** с обобщенной информацией по всем остальным значениям.

Указав параметры, нажмите **Добавить**. Виджет появится в конце сводки.

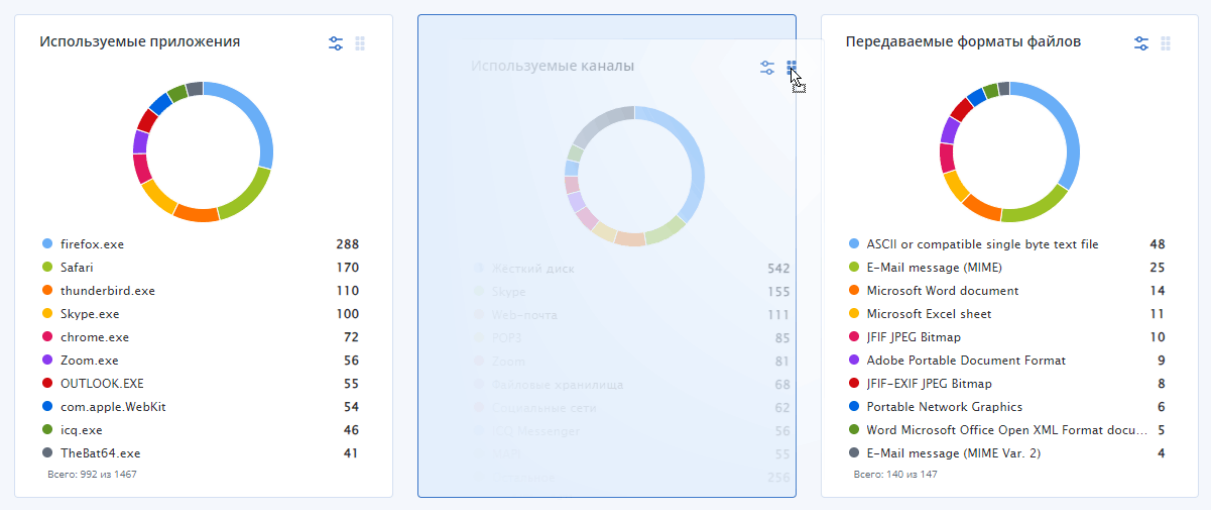
Примечание
Названия виджетов в сводке должны быть уникальны.



Чтобы изменить или удалить виджет, щелкните значок в правом верхнем углу, затем выберите нужное действие из контекстного меню.

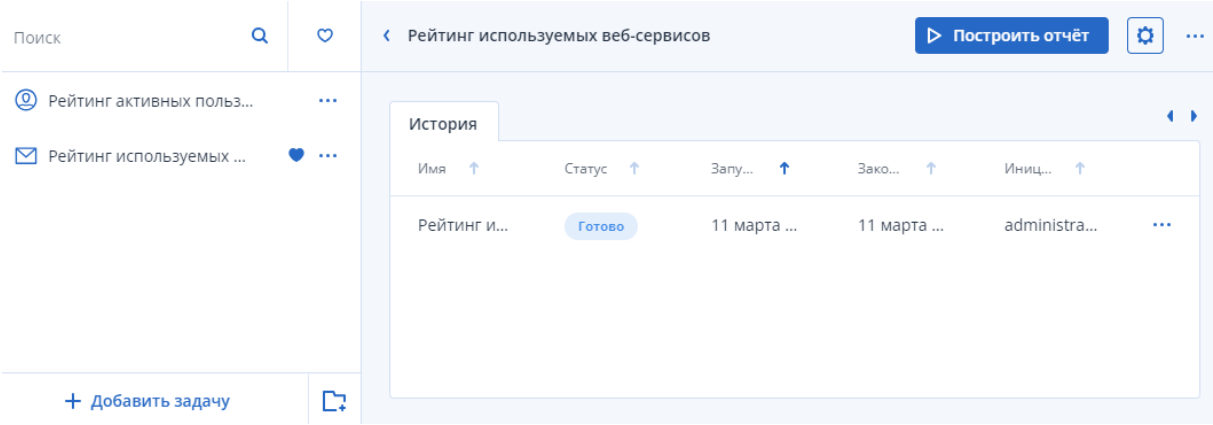


Чтобы переместить виджет, щелкните и удерживайте значок в правом верхнем углу и перетащите его на нужное место. Остальные виджеты подстроятся под новую раскладку.



5 Отчёты

Для анализа того, как сотрудники вашей компании используют те или иные устройства или сетевые протоколы, можно строить отчёты на основе данных БД Management Server.

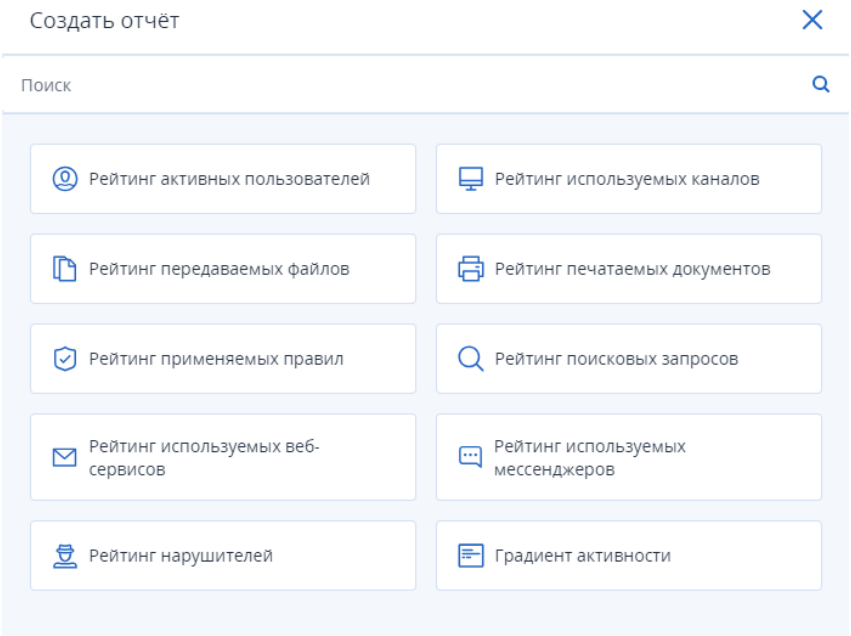


Примечание
События, полученные с сервера Кибер Файлов, при построении отчетов не учитываются.

Управлять отчётами можно в разделе **ОТЧЁТЫ**:

- создавать, настраивать, запускать и удалять задачи построения отчётов, добавлять их в избранное, а также переносить между папками;
- создавать, переименовывать и удалять папки;
- фильтровать отчёты и папки по именам.

Чтобы создать задачу построения отчёта, нажмите **Добавить задачу** внизу экрана. В появившемся окне выберите тип отчёта.



В появившемся окне **Настройки задачи** выберите параметры отчёта. Параметры зависят от типа отчёта и описаны далее в соответствующих разделах. Указав параметры, нажмите **Создать и построить**.

Будет создана и запущена задача построения отчёта. Время, необходимое для построения отчёта, зависит от количества обрабатываемых данных. Статус задачи будет отображен в списке **История**. Пока отчёт не построен, в нем отображается, что данные отсутствуют.

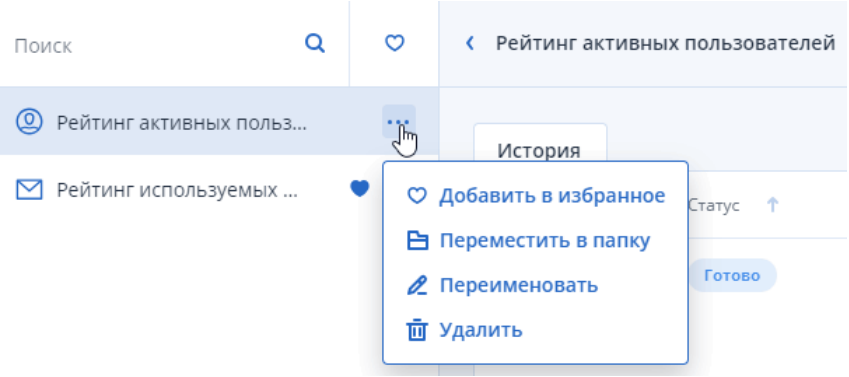
В дальнейшем отчёт можно перестраивать, запуская задачу вручную кнопкой **Построить отчёт** и выбирая диапазон дат.

Задачи построения отчётов перечислены в списке слева. При выборе задачи справа в списке **История** появляется список отчётов с указанием даты и времени запуска задачи. Чтобы открыть отчёт, выберите его в списке.

Чтобы изменить параметры задачи, выберите отчёт в списке слева и нажмите значок шестеренки справа. После сохранения параметров задача не будет запущена автоматически.

Задачи построения отчётов и папки можно фильтровать по именам. Для этого начните набирать любую часть имени в строке поиска над списком. Шаблоны поиска (wildcards) не поддерживаются.

Чтобы добавить задачу в избранное, откройте контекстное меню, нажав многоточие справа от ее имени в списке, и выберите **Добавить в избранное**. У названия задачи появится соответствующий значок. Быстро отфильтровать избранные задачи можно, нажав на значок избранного справа от строки поиска.

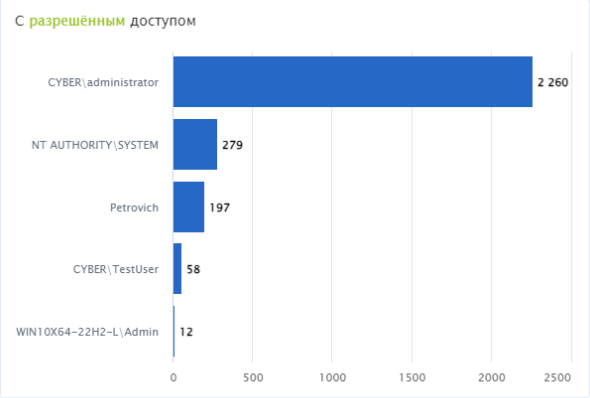


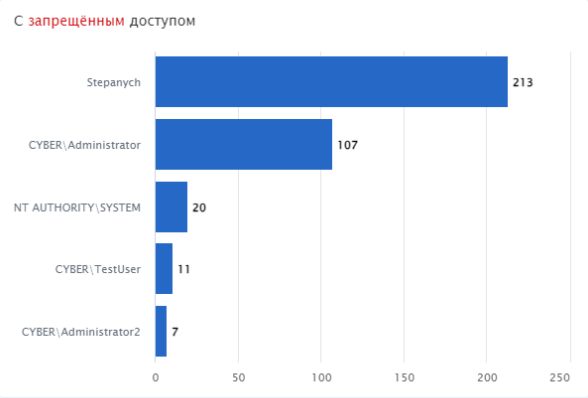
Чтобы перенести задачу в папку, откройте контекстное меню, нажав многоточие справа от ее имени в списке, и выберите **Переместить в папку**. В появившемся окне выберите папку и нажмите **Переместить**.

5.1 Рейтинг активных пользователей

Этот отчёт показывает наиболее активных пользователей, отсортированных по количеству разрешенных и запрещенных попыток доступа к устройствам и протоколам.

Топ 5 пользователей по активности



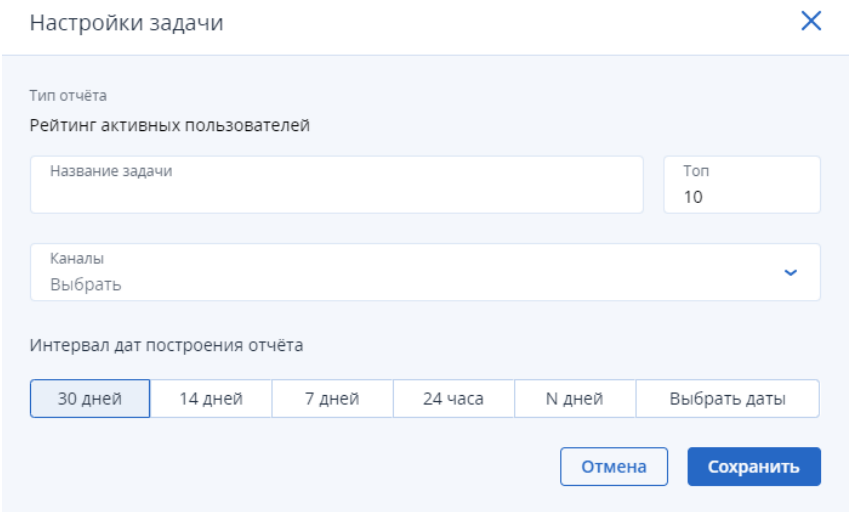


	Пользователь	Число попыток
1	CYBER\administrator	2260
2	NT AUTHORITY\SYSTEM	279
3	Petrovich	197
4	CYBER\TestUser	58
5	WIN10X64-22H2-L\Admin	12

	Пользователь	Число попыток
1	Stepanych	213
2	CYBER\Administrator	107
3	NT AUTHORITY\SYSTEM	20
4	CYBER\TestUser	11
5	CYBER\Administrator2	7

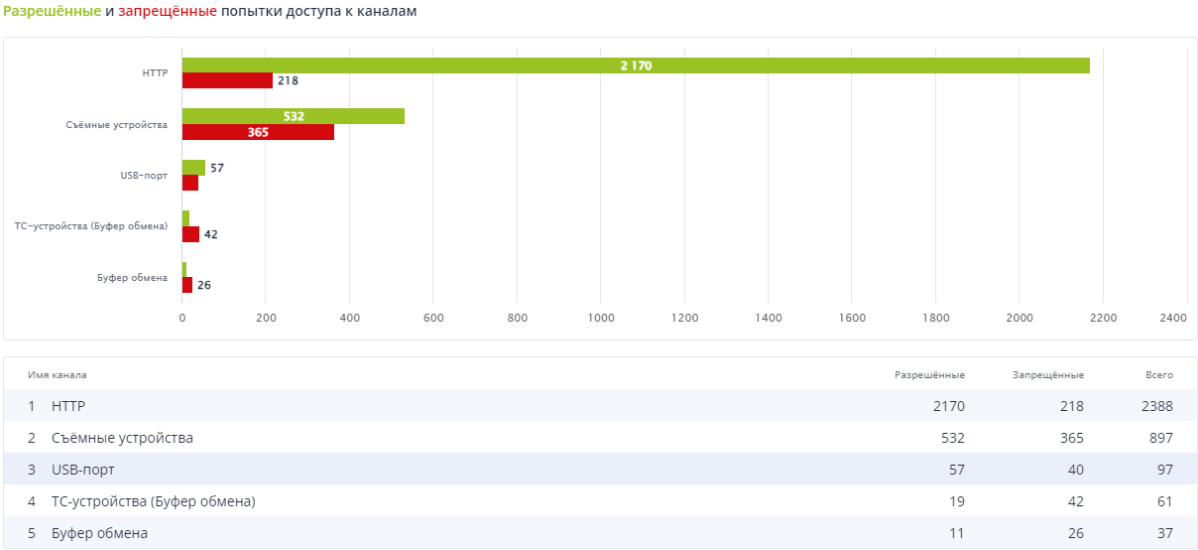
При создании задачи построения этого отчёта укажите следующие параметры:

- Название задачи в соответствующем поле.
- В поле **Топ** – количество пользователей, отображаемое на диаграммах и в списках отчёта.
- В списке **Каналы** – типы протоколов и устройств, к которым пользователи пытались получить доступ. Отслеживаемые каналы перечислены ниже.
  - Устройства: Bluetooth, буфер обмена, FireWire-порт, гибкий диск, жесткий диск, ИК-порт, iPhone-устройства, МТР, оптический привод, параллельный порт, последовательный порт, принтер, съемные устройства, ленточные накопители, ТС-устройства, USB-порт, Wi-Fi.
  - Протоколы: поиск работы, файловые хранилища, Кибер Файлы, FTP, HTTP, IBM Notes, ICQ Messenger, IMAP, IRC, Jabber, Mail.ru Агент, MAPI, POP3, SFTP, Skype, SMB, SMTP, социальные сети, TamTam, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.
- Интервал дат построения отчёта.



5.2 Рейтинг используемых каналов

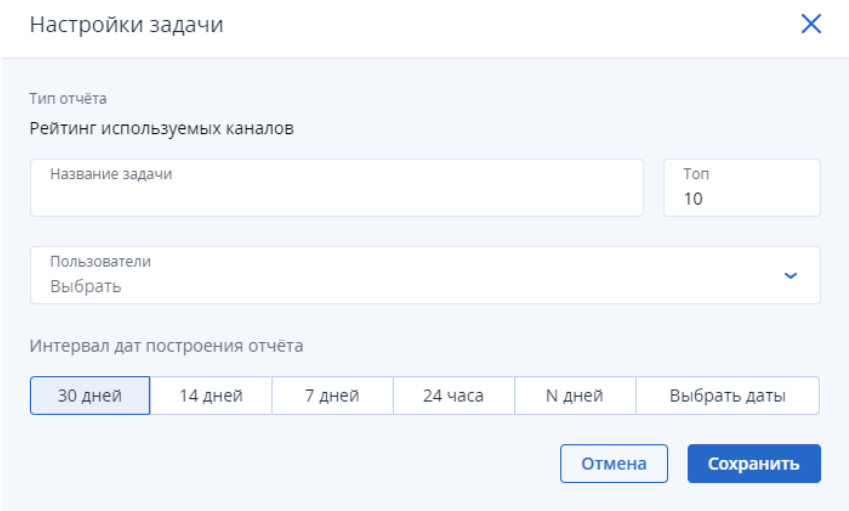
Этот отчёт показывает наиболее используемые каналы, отсортированные по количеству разрешенных и запрещенных попыток доступа к ним.



	Имя канала	Разрешённые	Запрещённые	Всего
1	HTTP	2170	218	2388
2	Съёмные устройства	532	365	897
3	USB-порт	57	40	97
4	ТС-устройства (Буфер обмена)	19	42	61
5	Буфер обмена	11	26	37

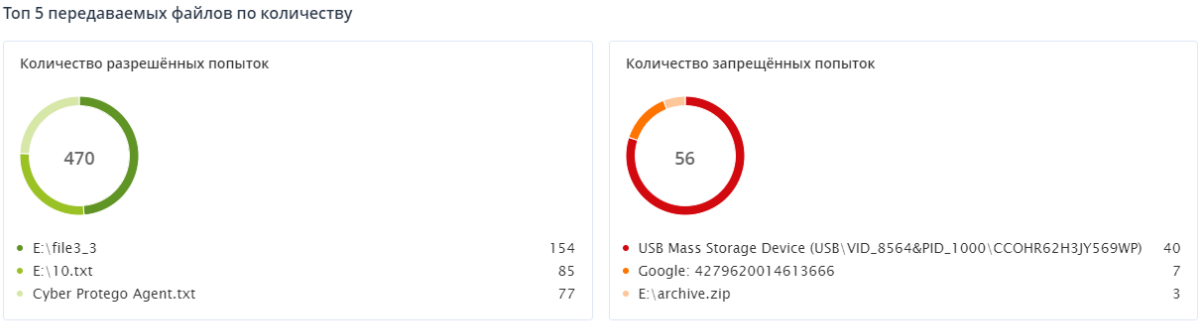
При создании задачи построения этого отчёта укажите следующие параметры:

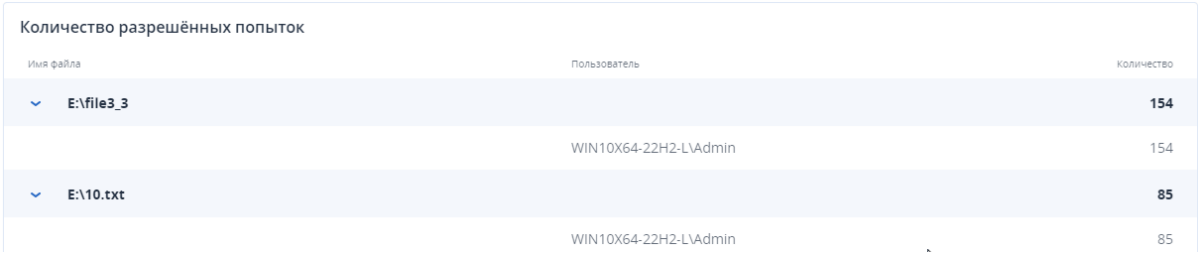
- Название задачи в соответствующем поле.
- В поле **Топ** – количество каналов, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** – пользователей, инициирующих использование каналов.
- Интервал дат построения отчёта.



5.3 Рейтинг передаваемых файлов

Этот отчёт показывает наиболее часто передаваемые файлы, отсортированные по количеству разрешенных и запрещенных попыток передачи, а также размеру.

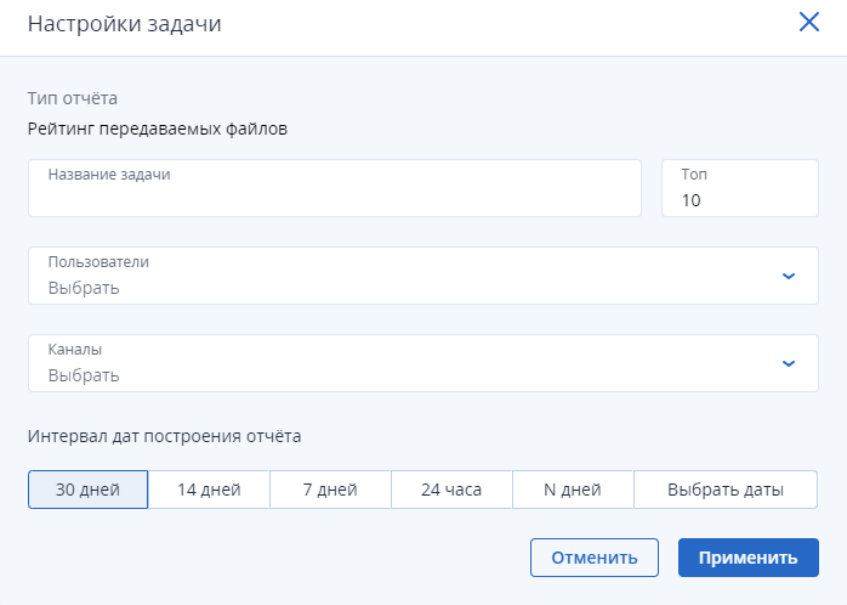




При создании задачи построения этого отчёта укажите следующие параметры:

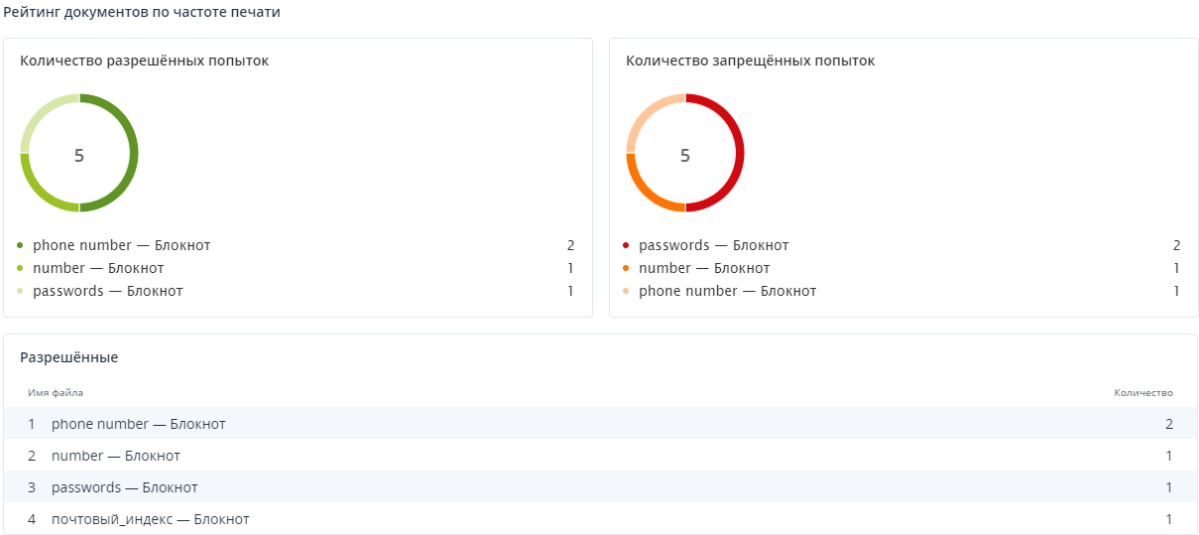
- Название задачи в соответствующем поле.
- В поле **Топ** – количество файлов, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** – пользователей, инициирующих передачу файлов.
- В списке **Каналы** – типы протоколов и устройств, используемых при передаче файлов. Отслеживаемые каналы перечислены ниже.
  - Устройства: Bluetooth, буфер обмена, FireWire-порт, гибкий диск, жесткий диск, ИК-порт, iPhone-устройства, MTP, оптический привод, параллельный порт, последовательный порт,

принтер, съемные устройства, ленточные накопители, ТС-устройства, USB-порт, Wi-Fi.
  - Протоколы: поиск работы, файловые хранилища, Кибер Файлы, FTP, HTTP, IBM Notes, ICQ Messenger, IMAP, IRC, Jabber, Mail.ru Агент, MAPI, POP3, SFTP, Skype, SMB, SMTP, социальные сети, TamTam, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.
- Интервал дат построения отчёта.



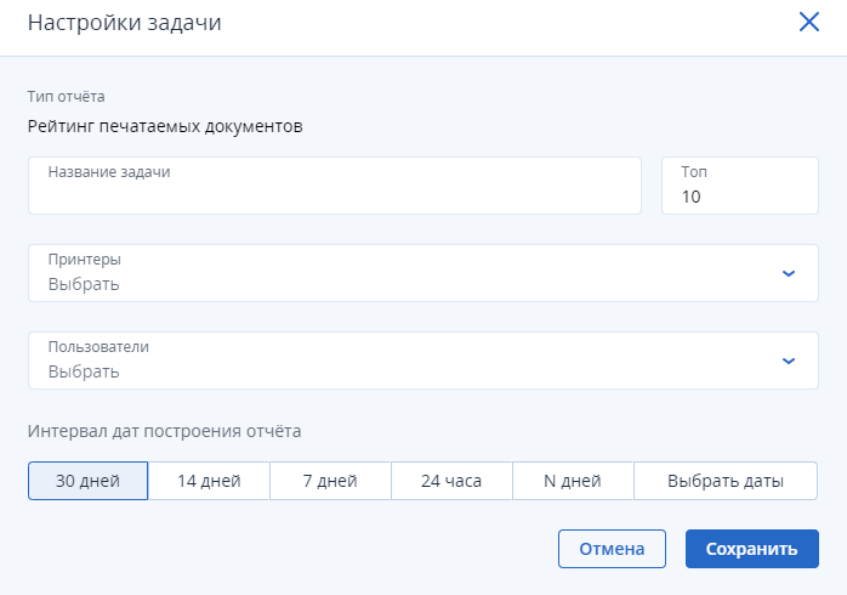
5.4 Рейтинг печатаемых документов

Этот отчёт показывает наиболее печатаемые документы, отсортированные по количеству разрешенных и запрещенных попыток, а также по объему печати.



При создании задачи построения этого отчёта укажите следующие параметры:

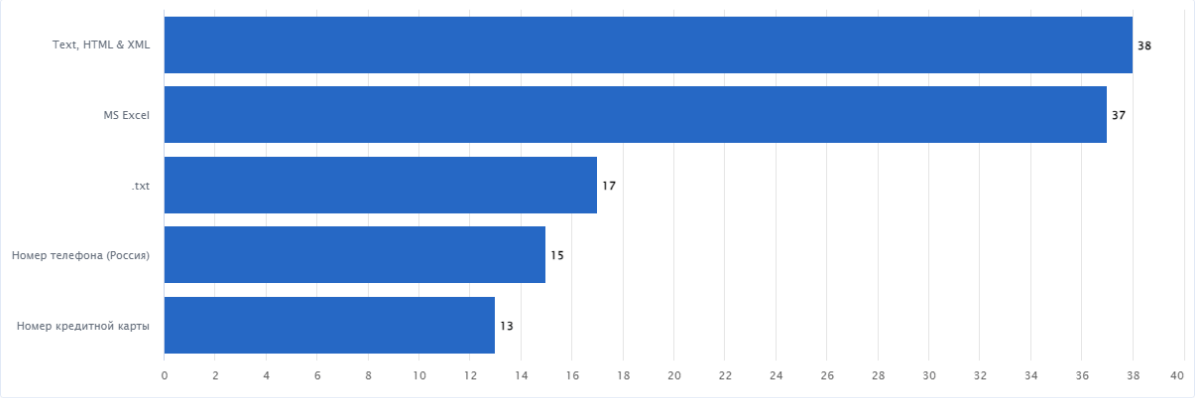
- Название задачи в соответствующем поле.
- В поле **Топ** – количество документов, отображаемое на диаграммах и в списках отчёта.
- В списке **Принтеры** – принтеры, используемые для печати.
- В списке **Пользователи** – пользователей, инициирующих печать.
- Интервал дат построения отчёта.



5.5 Рейтинг применяемых правил

Этот отчёт показывает наиболее часто применяемые контентно-зависимые правила, отсортированные по частоте применения.

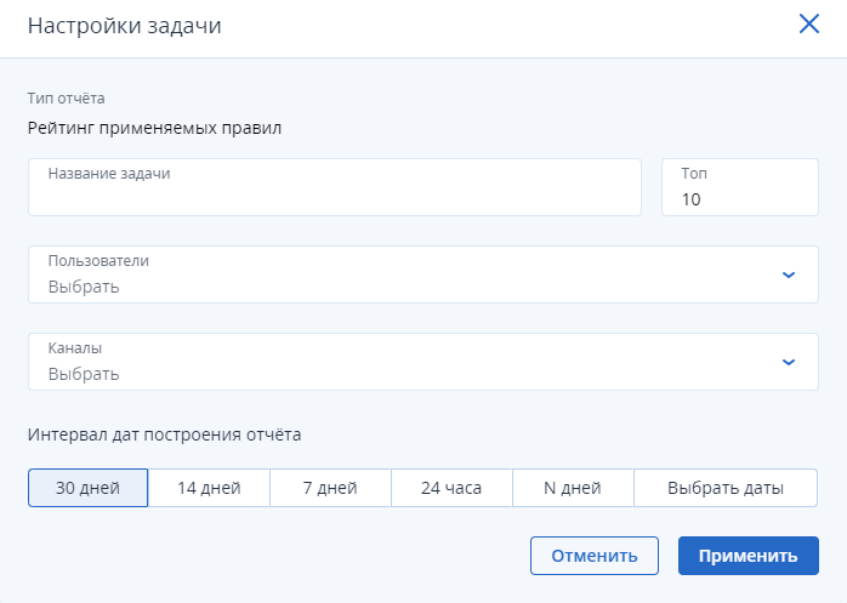
Применяемые правила



	Применяемое правило	Частота применения
1	Text, HTML & XML	38
2	MS Excel	37
3	.txt	17
4	Номер телефона (Россия)	15
5	Номер кредитной карты	13

При создании задачи построения этого отчёта укажите следующие параметры:

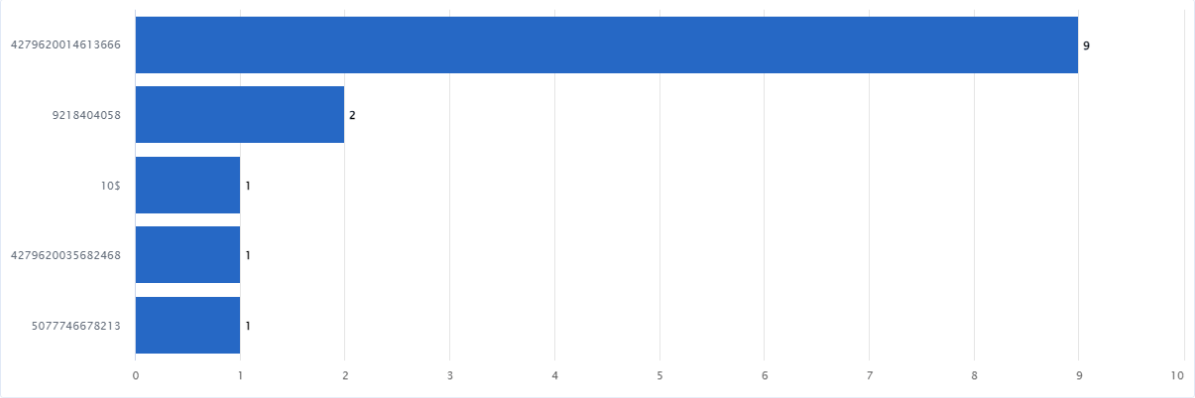
- Название задачи в соответствующем поле.
- В поле **Топ** – количество правил, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** – пользователей, для которых сработали правила.
- В списке **Каналы** – типы протоколов и устройств, для которых сработали правила. Отслеживаемые каналы перечислены ниже.
  - Устройства: Bluetooth, буфер обмена, FireWire-порт, гибкий диск, жесткий диск, ИК-порт, iPhone-устройства, MTP, оптический привод, параллельный порт, последовательный порт, принтер, съемные устройства, ленточные накопители, TC-устройства, USB-порт, Wi-Fi.
  - Протоколы: поиск работы, файловые хранилища, Кибер Файлы, FTP, HTTP, IBM Notes, ICQ Messenger, IMAP, IRC, Jabber, Mail.ru Агент, MAPI, POP3, SFTP, Skype, SMB, SMTP, социальные сети, TamTam, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.
- Интервал дат построения отчёта.



5.6 Рейтинг поисковых запросов

Этот отчёт показывает наиболее частые поисковые запросы, отсортированные по количеству.

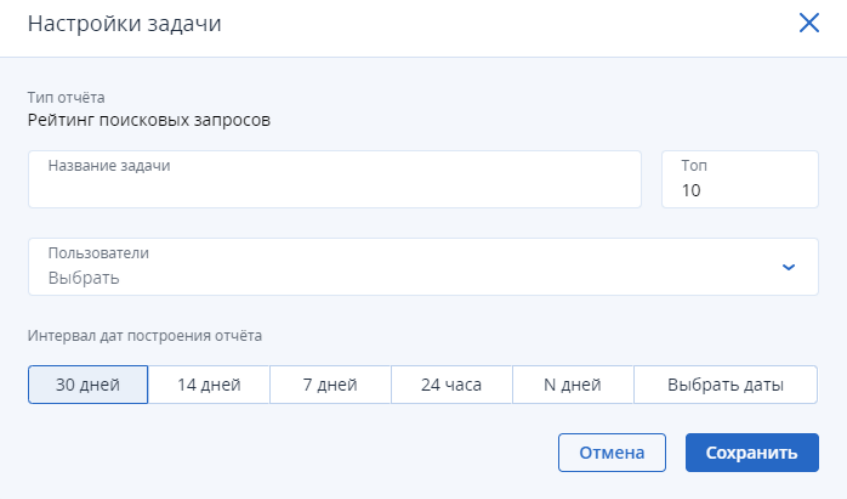
Топ 5 поисковых запросов



	Поисковый запрос	Число запросов
1	4279620014613666	9
2	9218404058	2
3	10$	1
4	4279620035682468	1
5	5077746678213	1

При создании задачи построения этого отчёта укажите следующие параметры:

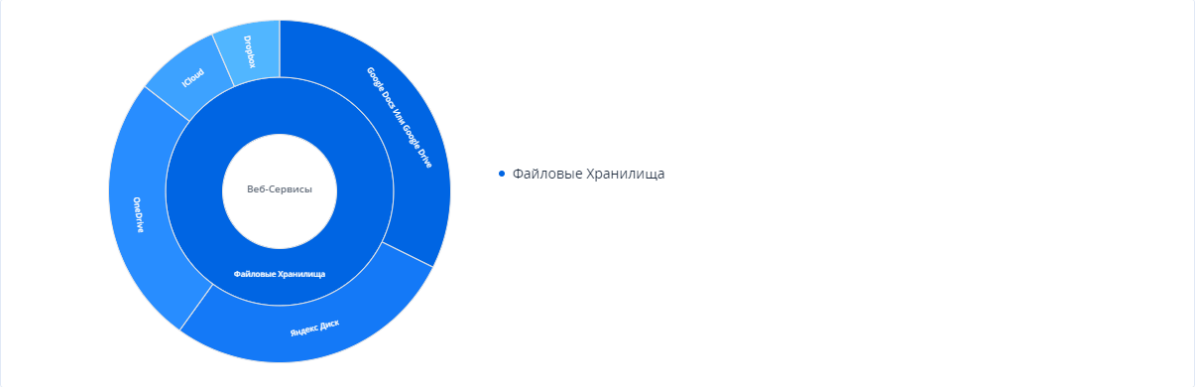
- Название задачи в соответствующем поле.
- В поле **Топ** – количество поисковых запросов, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** – пользователей, инициирующих поиск.
- Интервал дат построения отчёта.



5.7 Рейтинг используемых веб-сервисов

Этот отчёт показывает наиболее часто используемые веб-сервисы, отсортированные по частоте использования.

Используемые веб-сервисы

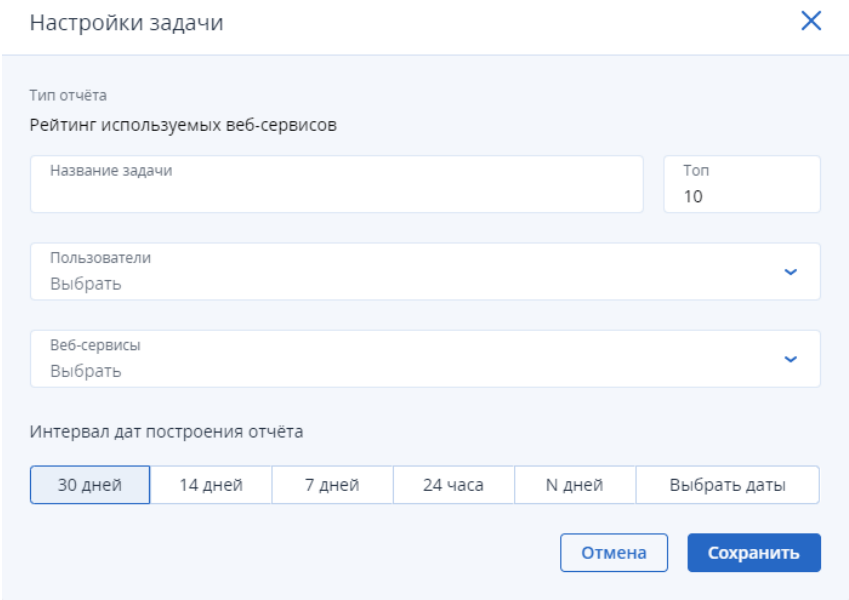


Показать по категориям сервисов

Веб-сервис	Попытки доступа
Файловые хранилища	**19490**
Google Docs или Google Drive	6294
Яндекс диск	5390
OneDrive	4986
iCloud	1559
Dropbox	1261
Всего	**19490**

При создании задачи построения этого отчёта укажите следующие параметры:

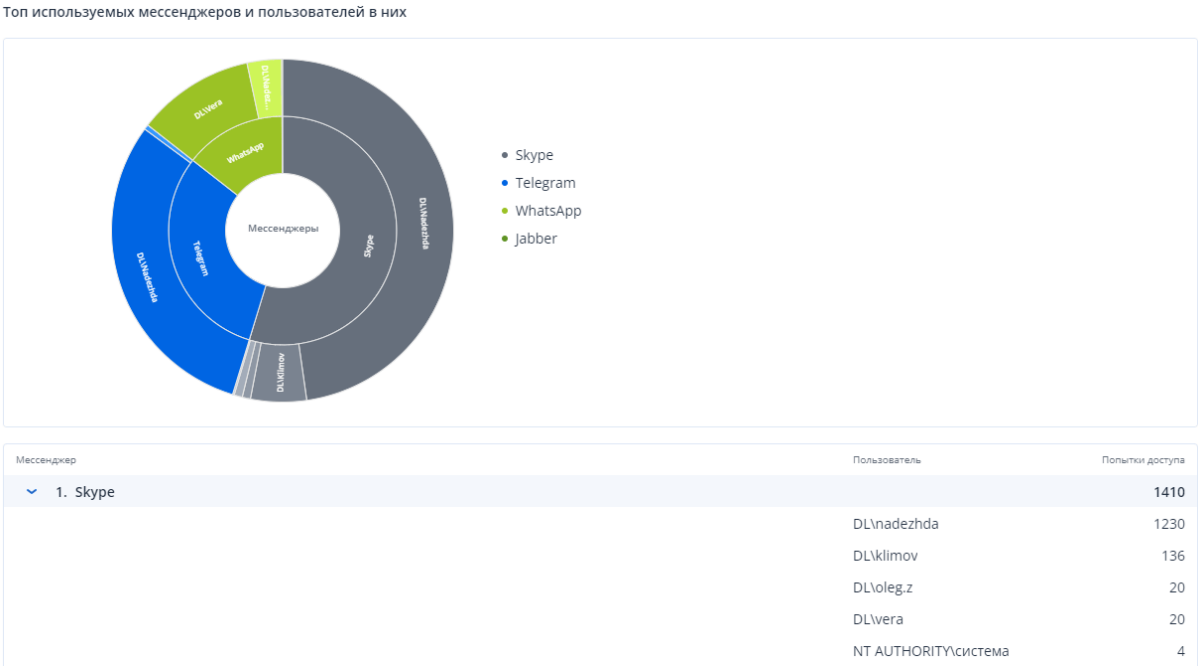
- Название задачи в соответствующем поле.
- В поле **Топ** – количество веб-сервисов, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** – пользователей, использующие веб-сервисы.
- В списке **Веб-сервисы** – типы файловых хранилищ, социальных сетей и почтовых сервисов. Отслеживаемые веб-сервисы перечислены ниже.
  - Файловые хранилища: 4shared, Amazon S3, AnonFile, Box, dmca.gripe, Dropbox, DropMeFiles, Easyupload.io, Files.fm, freenet.de, GitHub, GMX, Gofile.io, Google Docs / Google Drive, iCloud, IDrive, MagentaCLOUD, MediaFire, MEGA, OneDrive, Sendspace, transfer.sh, TransFiles.ru, Uploadfiles.io, Web.de, WeTransfer, Облако Mail.ru, Яндекс.Диск.
  - Социальные сети: Disqus, Facebook, Google+, Instagram, LinkedIn, LiveInternet.ru, LiveJournal, MeinVZ.de, Myspace, Odnoklassniki.ru, Pinterest, StudiVZ.de, Tumblr, Twitter, Vkontakte, XING.com.
  - Почтовые сервисы: ABV Mail, AOL Mail, freenet.de, Gmail, GMX Mail, Hotmail (Outlook.com), iCloud, Mail.ru, NAVER, OWA, Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail, Mailion, Zimbra.
- Интервал дат построения отчёта.



Нажимая на типы сервисов на круговой диаграмме отчёта, можно переключаться на диаграммы использования данного типа сервисов. Кроме того, можно группировать сервисы в списке по категориям.

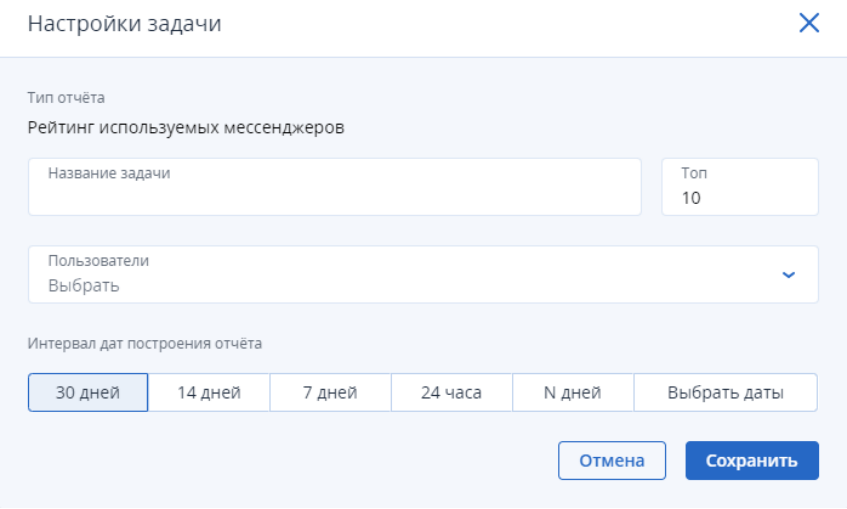
5.8 Рейтинг используемых мессенджеров

Этот отчёт показывает наиболее используемые мессенджеры, отсортированные по частоте использования. Отслеживаются данные мессенджеры: ICQ Messenger, IRC, Jabber, Mail.ru Агент, Skype, TamTam, Telegram, Viber, WhatsApp, Zoom.



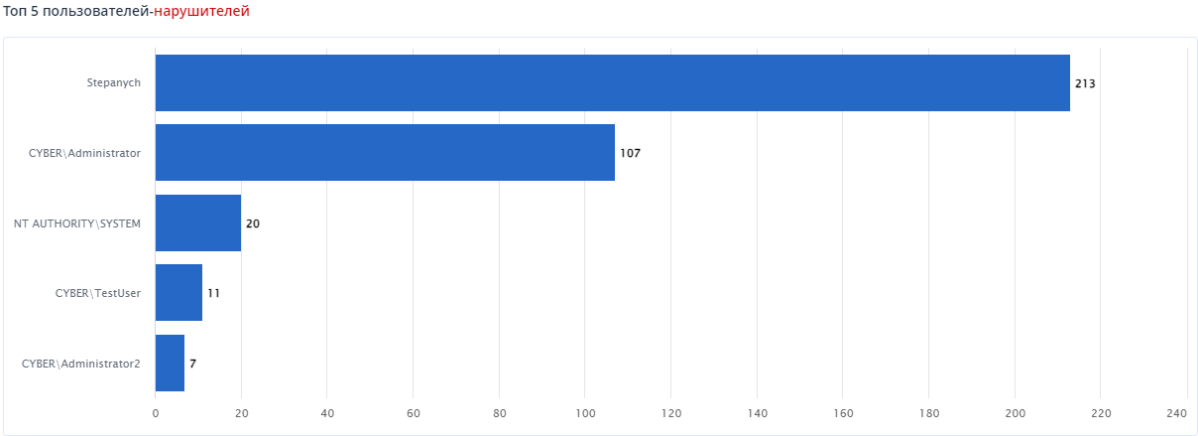
При создании задачи построения этого отчёта укажите следующие параметры:

- Название задачи в соответствующем поле.
- В поле **Топ** – количество мессенджеров, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** – пользователей, инициирующих беседы и передачу файлов в мессенджерах.
- Интервал дат построения отчёта.



5.9 Рейтинг нарушителей

Этот отчёт показывает нарушителей, которым чаще всего был запрещен доступ, отсортированных по количеству запрещенных попыток доступа к устройствам и протоколам.

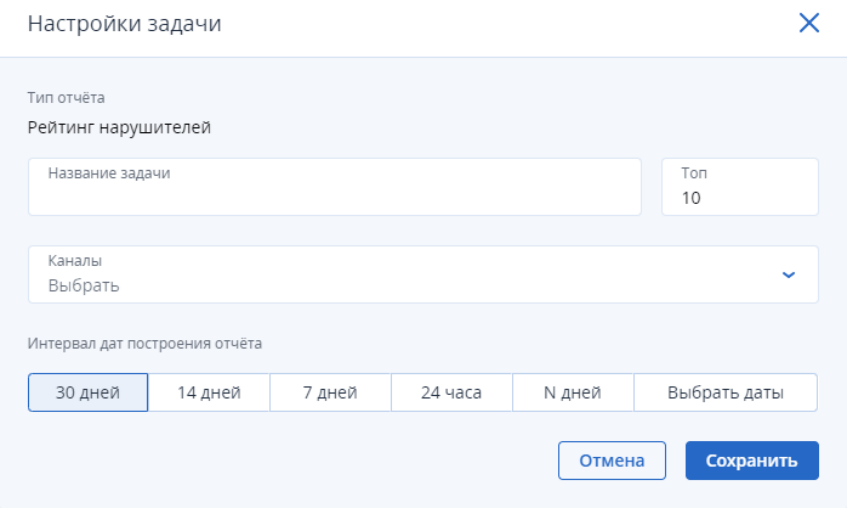


При создании задачи построения этого отчёта укажите следующие параметры:

- Название задачи в соответствующем поле.
- В поле **Топ** – количество пользователей, отображаемое на диаграммах и в списках отчёта.
- В списке **Каналы** – типы протоколов и устройств, к которым был запрещен доступ. Отслеживаемые каналы перечислены ниже.

- Устройства: Bluetooth, буфер обмена, FireWire-порт, гибкий диск, жесткий диск, ИК-порт, iPhone-устройства, MTP, оптический привод, параллельный порт, последовательный порт, принтер, съемные устройства, ленточные накопители, ТС-устройства, USB-порт, Wi-Fi.
- Протоколы: поиск работы, файловые хранилища, Кибер Файлы, FTP, HTTP, IBM Notes, ICQ Messenger, IMAP, IRC, Jabber, Mail.ru Агент, MAPI, POP3, SFTP, Skype, SMB, SMTP, социальные сети, TamTam, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.

- Интервал дат построения отчёта.



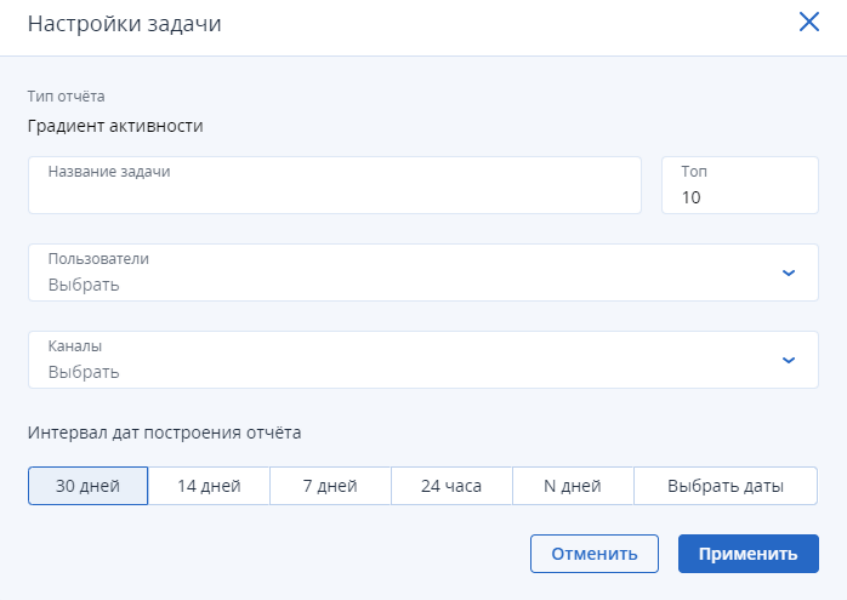
5.10 Градиент активности

Этот отчёт показывает тепловую карту каналов для выбранных пользователей.

При создании задачи построения этого отчёта укажите следующие параметры:

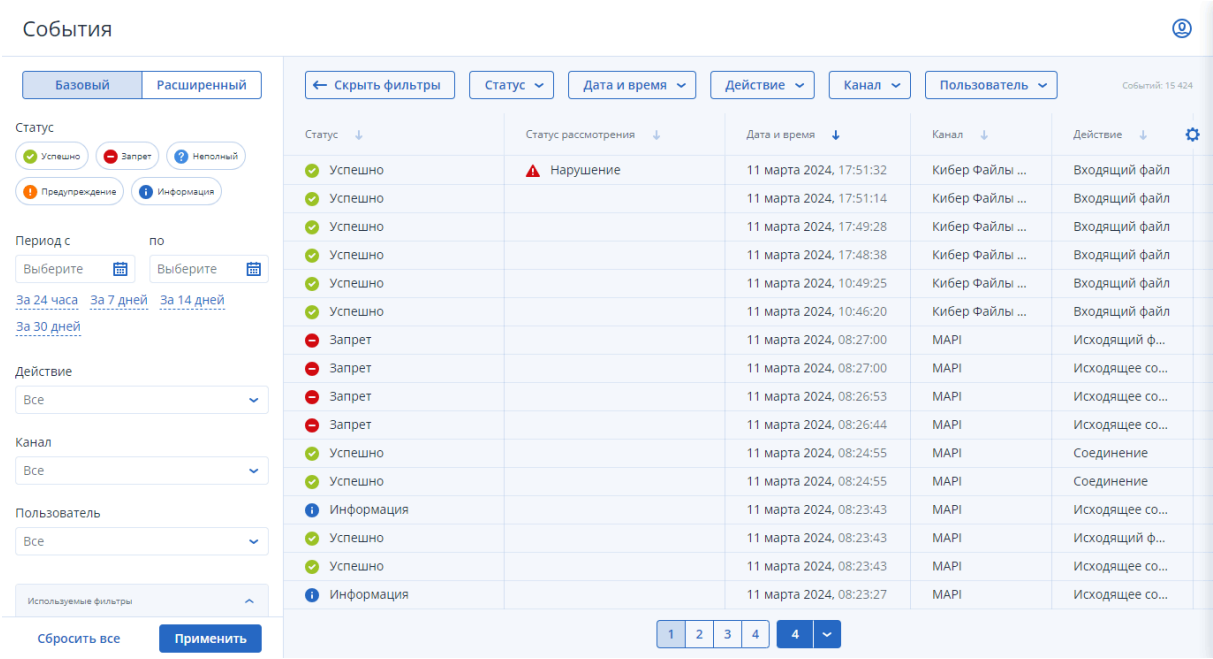
- Название задачи в соответствующем поле.
- В поле **Топ** – количество пользователей, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** – пользователей, добавляемых на тепловую карту.

- В списке **Каналы** – типы протоколов и устройств, добавляемых на тепловую карту. Отслеживаемые каналы перечислены ниже.
  - Устройства: Bluetooth, буфер обмена, FireWire-порт, гибкий диск, жесткий диск, ИК-порт, iPhone-устройства, MTP, оптический привод, параллельный порт, последовательный порт, принтер, съемные устройства, ленточные накопители, TC-устройства, USB-порт, Wi-Fi.
  - Протоколы: поиск работы, файловые хранилища, Кибер Файлы, FTP, HTTP, IBM Notes, ICQ Messenger, IMAP, IRC, Jabber, Mail.ru Агент, MAPI, POP3, SFTP, Skype, SMB, SMTP, социальные сети, TamTam, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.
- Интервал дат построения отчёта.



6 События

В веб-консоли, в разделе **События** можно просматривать события из БД Management Server, связанные с использованием устройств и сетевых протоколов сотрудниками вашей компании. Доступ к этому разделу имеют пользователи с правом просмотра событий (см. "Роли" (стр. 33)).



По умолчанию выводятся все события, однако их можно фильтровать. Изначально отображается базовый набор фильтров. Полный список можно вывести, нажав **Используемые фильтры** внизу экрана:

- **Статус** – состояние записи:
  - **Успешно** – операция была разрешена;
  - **Запрет** – операция была запрещена;
  - **Неполный** – возможно, теневая копия создана не полностью;
  - **Предупреждение** – сообщение о возможных осложнениях или ошибках;
  - **Информация** – событие обнаружения контента.
- **Дата и время** – дата и время, когда событие было получено агентом Cyber Protego.
- **Действие** – действие пользователя.
- **Канал** – тип протокола или устройства.
- **Пользователь** – имя пользователя, связанное с событием.
- **Компьютер** – имена или IP–адреса компьютеров, на которых произошли события.
- **Имя** – имена объектов (файлов, USB–устройств и т. п.), связанных с событиями.
- **Защита файла** – состояние защиты файла.
- **Причина** – причина наступления события.

- **Процесс** – путь к исполняемому файлу приложения. В некоторых случаях вместо полного пути может быть показано только имя процесса.
- **Статус рассмотрения** – статус рассмотрения события. Поле может принимать одно из этих значений:
  - Не заполнено (пустая строка)
  - Рассмотреть
  - На рассмотрении
  - Рассмотрено
  - Нарушение

  Поле могут изменять только пользователи с правом на изменение событий (см. "Роли" (стр. 33)).
- **Комментарий** – дополнительная информация о событии, заполняемая пользователем (не более 2000 символов). Указать комментарий можно только в окне сведений о событии, нажав **Добавить**. Изменить комментарий можно там же, нажав **Редактировать**. Это поле отображается только в расширенных фильтрах. Его нет в общем списке событий и базовых фильтрах. Поле могут изменять только пользователи с правом на изменение событий (см. "Роли" (стр. 33)).
- **Сервер** – имя сервера Cyber Protego Management Server, получившего событие от Cyber Protego Agent.
- **Серверный источник** – IP-адрес или имя сервера Кибер Файлов, с которого получены события.
- **Размер файла** – размер данных.
- **Тип файла** – настоящий тип файла (определяется по сигнатурам независимо от расширения файла).
- **Информация** – прочая относящаяся к устройству или протоколу информация о событии, такая как флаги доступа, имя устройства или протокола, ID и описание USB–устройства и т. п.
- **Дата и время сбора** – дата и время, когда событие было получено сервером Cyber Protego Management Server от Cyber Protego Agent.
- **Сервер консолидации** – имя сервера, который последним получил данное событие при консолидации журналов.
- **Дата и время консолидации** – дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов.
- **PID** – Идентификатор процесса, связанного с событием.

Чтобы просмотреть все сведения о событии, нажмите на него в списке.

6.1 Расширенные фильтры

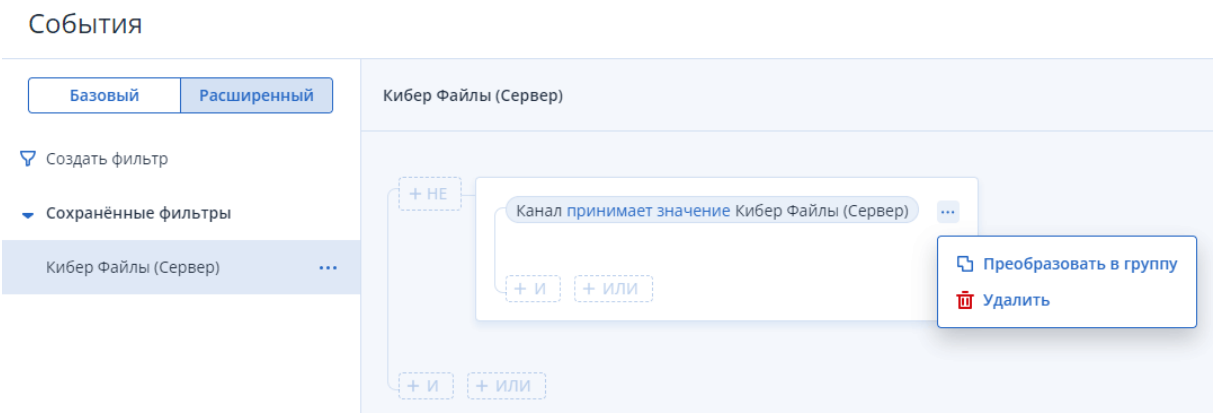
Расширенные фильтры являются дополнением к базовым фильтрам и позволяют создавать логические конструкции с использование операторов "И", "ИЛИ", "НЕ".

Выполнение сложных расширенных фильтров может занимать долгое время. При необходимости можно увеличить время ожидания ответа сервера, как описано в разделе "Изменение времени ожидания ответа сервера" (стр. 44).

Расширенные фильтры составляются из логических блоков (условий). Каждый блок состоит из 3 элементов:

- **Поле** – любое из поддерживаемых полей в журнале событий, а также поле **Комментарий**.
- **Условие** – условие, зависящее от типа поля (текстовое, числовое, дата). Например, **Пустое**, **Не пустое**, **Содержит**, **Не содержит**, **Ранее чем**, **Позднее чем** и т. д.
- **Значение** – конкретное значение, зависящее от условия. Например, **Запрет** для поля **Статус**, **HTTP** для поля **Канал**, **Archive.zip** для поля **Имя** и т. д.

Отдельные блоки условий можно объединять в группы. Уровень вложенности расширенных фильтров не ограничен.



Просмотреть расширенные фильтры можно во вкладке **Расширенный**, в списке **Сохраненные фильтры**. Нажав на фильтр в списке, можно просмотреть его условия. Чтобы применить выбранный фильтр, нажмите **Применить** внизу экрана.

Чтобы создать расширенный фильтр, перейдите в раздел **События**, щелкните **Расширенный** в левой части окна, затем щелкните **Создать фильтр**. В появившемся окне создайте хотя бы один логический блок, указав поля, условия и значения. Чтобы преобразовать блок в группу, нажмите многоточие справа вверху блока и выберите **Преобразовать в группу**. Созданный фильтр можно применить без сохранения, нажав **Применить**, или же сохранить и применить соответствующей кнопкой внизу экрана.

Изменить выбранный сохраненный фильтр можно, нажав на одно из его условий. Очистить условия фильтра можно одноименной кнопкой внизу экрана. Чтобы переименовать или удалить фильтр, щелкните многоточие справа от его имени в списке и выберите соответствующее действие.

7 Настройки

7.1 Пользователи

Управлять пользователями можно в разделе **НАСТРОЙКИ** > **Пользователи**:

- создавать и удалять пользователей, просматривать и редактировать их данные, а также переносить их между папками;
- создавать, переименовывать и удалять папки;
- фильтровать пользователей и папки по именам.

Чтобы создать пользователя, перейдите на экран **НАСТРОЙКИ** > **Пользователи** и нажмите **Добавить пользователя** внизу экрана. В появившихся полях укажите данные пользователя и нажмите **Сохранить**.

Обязательно указать:

- **Логин**. Подходят символы, допустимые в адресах электронной почты. Допустимая длина: 4-320 символов.
- **Пароль**. Должен содержать большие и маленькие буквы, специальные символы и цифры. Допустимая длина: 8-320 символов.
- **Имя**. Допустимы буквы латиницы и кириллицы, а так же знак дефиса. Допустимая длина: 1-320 символов.
- **Роль**. Необходимо выбрать из списка. При этом можно добавить новую роль, нажав **Добавить роль**. Права выбранной роли будут отображены ниже.

Дополнительно можно указать:

- **Папку**. Пользователь сразу будет создан в указанной папке.
- **Фамилию**. Допустимы буквы латиницы и кириллицы, а так же знак дефиса. Допустимая длина: 1-320 символов.
- **Отчество**. Допустимы буквы латиницы и кириллицы, а так же знак дефиса. Допустимая длина: 1-320 символов.
- **Телефон**. Допустимая длина: 2-30 символов.
- **Email**. Подходят символы, допустимые в адресах электронной почты. Допустимая длина: 3-320 символов.

После создания новый пользователь появится в списке. Просмотреть его данные можно, выбрав его.

Пользователей и папки можно фильтровать по именам. Для этого начните набирать любую часть имени в строке поиска над списком. Шаблоны поиска (wildcards) не поддерживаются.

Чтобы перенести пользователя в папку, откройте контекстное меню, нажав многоточие справа от его имени в списке, и выберите **Переместить в папку**. В появившемся окне выберите папку и нажмите **Переместить**.

Чтобы изменить данные пользователя, выберите его в списке и нажмите **Редактировать** справа, над его данными. Изменив данные, нажмите **Сохранить**.

Чтобы удалить пользователя, откройте контекстное меню, нажав многоточие справа от его имени в списке, и выберите **Удалить**. В появившемся окне подтвердите действие, нажав **Удалить**.

Внимание
В системе должен быть хотя бы один пользователь с ролью, которая обеспечивает полный доступ к разделу настроек.

7.2 Роли

Роли определяют возможные действия пользователей в системе. Управлять ролями можно в разделе **НАСТРОЙКИ** > **Роли**:

- создавать и удалять роли, просматривать и редактировать их данные, а также переносить их между папками;
- создавать, переименовывать и удалять папки;
- фильтровать роли и папки по именам.

Чтобы создать роль, перейдите на экран **НАСТРОЙКИ** > **Роли** и нажмите **Добавить роль** внизу экрана. В появившихся полях укажите название роли, папку (необязательно), отметьте обеспечиваемые ей права и нажмите **Сохранить**. Можно выбирать целые наборы прав (все, только просмотр, никаких) с помощью меню **Выбрать права** справа.

Права просмотра данных включаются автоматически при включении прав изменения этих данных. И, наоборот, права изменения данных отключаются автоматически при отключении права просмотра этих данных.

Для настроек системы доступны следующие права:

- Параметры базы данных:
  - **Просмотр параметров**. Активные действия недоступны.
  - **Назначение параметров**. Задание параметров базы данных, тестирование соединения.
- Роли:
  - **Просмотр роли**. Просмотр прав, назначенных ролям.
  - **Изменение роли**. Изменение данных ролей.
  - **Изменение списка**. Создание, переименование, удаление папок.
  - **Создание роли**. Изменение всех параметров роли при ее создании.
  - **Удаление роли**. Удаление ролей.
- Пользователи:
  - **Просмотр пользователя**. Просмотр данных пользователей.
  - **Изменение пользователя**. Изменение данных пользователей, включая пароли.

- **Изменение списка**. Создание, переименование, удаление папок.
- **Создание пользователя**. Изменение всех параметров пользователя при его создании.
- **Удаление пользователя**. Удаление пользователей.
- **Назначение роли**. Назначение ролей пользователям.

- Клиенты API:
  - **Просмотр параметров**. Просмотр списка клиентов API.
  - **Изменение параметров**. Управление клиентами API.

Для отчётов доступны следующие права:

- **Создание задачи отчёта**. Создание задач генерации отчётов, указание параметров задач.
- **Изменение задачи отчёта**. Редактирование задач генерации отчётов.
- **Запуск задачи отчёта**. Ручной запуск задач генерации отчётов. Указание интервала выборки событий при запуске задач.
- **Просмотр задачи отчёта**. Просмотр параметров задач генерации отчётов.
- **Удаление задачи отчёта**. Удаление задач генерации отчётов.
- **Просмотр отчёта**. Просмотр сгенерированных отчётов.
- **Удаление отчёта**. Удаление сгенерированных отчётов.
- **Изменение списка**. Создание, переименование, удаление папок.

Для событий доступны следующие права:

- **Просмотр событий**. Доступ к разделу событий.
- **Изменение событий**. Изменение статусов рассмотрения событий, а также создание и редактирование комментариев к событиям.

Для сводки доступны следующие права:

- **Доступ**. Просмотр и настройка виджетов.

После создания новая роль появится в списке. Просмотреть ее данные можно, выбрав ее.

Роли и папки можно фильтровать по именам. Для этого начните набирать любую часть имени в строке поиска над списком. Шаблоны поиска (wildcards) не поддерживаются.

Чтобы перенести роль в папку, откройте контекстное меню, нажав многоточие справа от ее имени в списке, и выберите **Переместить в папку**. В появившемся окне выберите папку и нажмите **Переместить**.

Чтобы изменить данные роли, выберите ее в списке и нажмите **Редактировать** справа, над ее данными. Изменив данные, нажмите **Сохранить**.

Чтобы удалить роль, откройте контекстное меню, нажав многоточие справа от ее имени в списке, и выберите **Удалить**. В появившемся окне подтвердите действие, нажав **Удалить**. Удалять можно только роли, которые не назначены пользователям.

Внимание
В системе должен быть хотя бы один пользователь с ролью, которая обеспечивает полный доступ к разделу настроек.

7.3 Папки

Для удобства отчёты, пользователей и роли можно группировать по папкам.

Примечание
Папки в папки помещать нельзя.

Чтобы создать папку, нажмите значок **Создать папку** под списком отчётов, пользователей или ролей. В появившемся окне укажите имя папки и нажмите **Создать**. Новая папка появится в списке.

Нажав на имя папки, можно увидеть отчеты, пользователей или роли в ней.

Чтобы переименовать папку, откройте контекстное меню, нажав многоточие справа от ее имени в списке, и выберите **Переименовать**. Укажите новое имя папки в появившемся окне и нажмите **Переименовать**.

Чтобы удалить папку, откройте контекстное меню, нажав многоточие справа от ее имени в списке, и выберите **Удалить**. В появившемся окне подтвердите действие, нажав **Удалить**.

При удалении папки будут удалены все помещенные в нее отчеты, пользователи или роли. При этом, ни одна роль в удаляемой папке не должна быть назначена пользователям.

Внимание
В системе должен быть хотя бы один пользователь с ролью, которая обеспечивает полный доступ к разделу настроек.

7.4 База данных Management Server

Чтобы подключиться к базе данных Management Server для построения отчётов и отображения событий, необходимо указать ее параметры в окне **НАСТРОЙКИ** > **База данных**:

- тип подключения,
- имя базы данных,
- имя сервера,
- порт,
- имя пользователя,
- пароль.

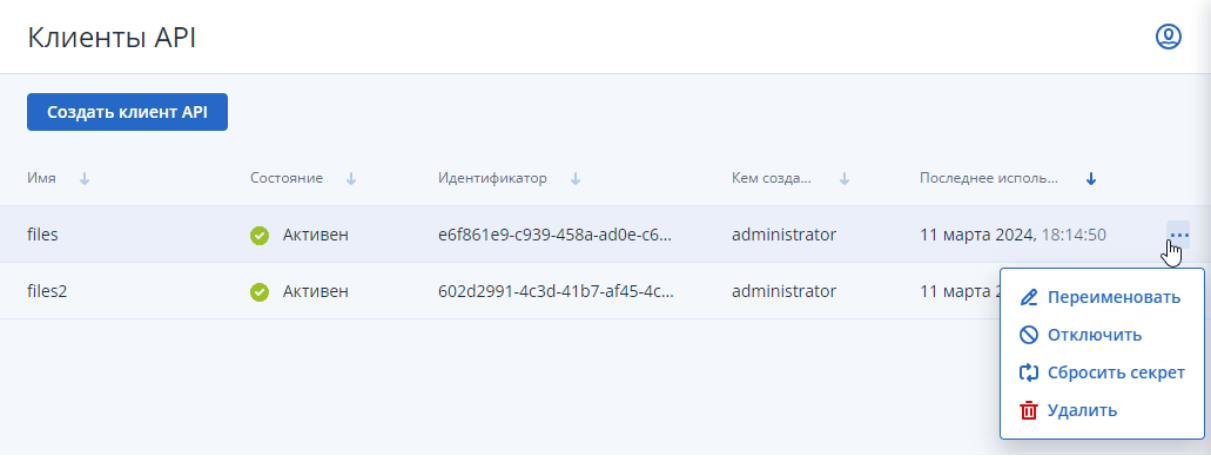
Указав параметры, нажмите **Применить**. Чтобы проверить соединение с БД, нажмите **Тестировать соединение**.

7.5 Клиенты API

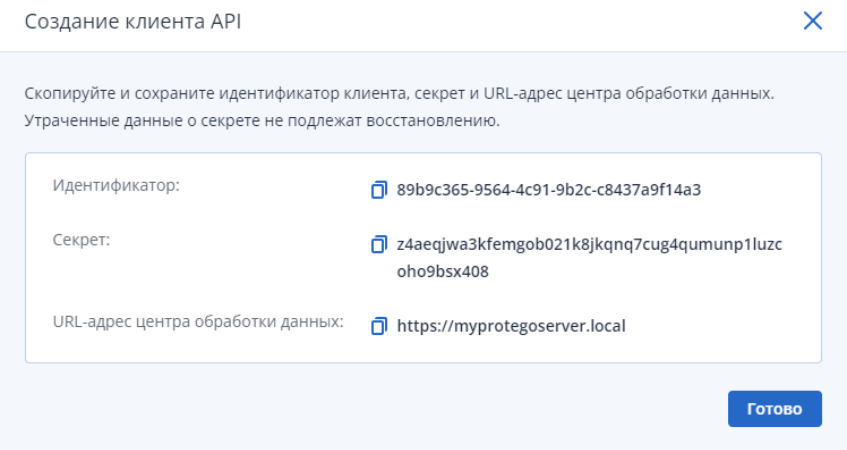
Создавать клиентов для интеграции со сторонним ПО можно в окне **НАСТРОЙКИ** > **Клиенты API**.

Примечание

В данной версии в качестве клиентов поддерживаются только серверы Кибер Файлов.



Создать клиент можно, щелкнув одноименную кнопку. В появившемся окне понадобится указать название клиента и нажать **Далее**. В следующем окне появится информация, которую нужно указать на стороне клиентского ПО (например, Кибер Файлах) для настройки интеграции: идентификатор, секрет и URL-адрес центра обработки данных.

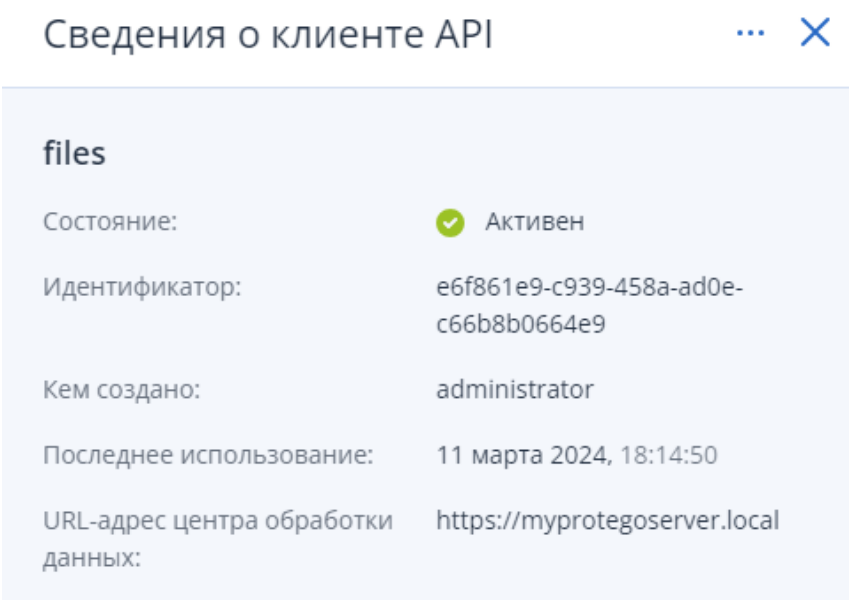


Скопируйте и сохраните идентификатор клиента, секрет и URL-адрес центра обработки данных.

Внимание

Секрет отображается только в окне создания клиента или сброса секрета. Закрыв это окно, посмотреть секрет еще раз не удастся. При утрате секрета его можно лишь сбросить и создать новый.

Чтобы посмотреть сведения о клиенте API, щелкните его в списке. Откроется окно сведений о данном клиенте.



Чтобы переименовать, отключить, удалить клиент или сбросить его секрет, щелкните значок многоточия справа в строке клиента или в окне сведений о нем.

8 Расширенные настройки

8.1 Изменение порта веб-консоли

По умолчанию веб-консоль доступна на стандартном для протокола HTTPS порте 443. При необходимости порт можно изменить, как описано далее.

Внимание
Не используйте порт 444.

Изменение порта на ОС Windows

1. Остановите службы CPServer-backend и CPServer-proxy:

```
> net stop CPServer-backend
> net stop CPServer-proxy
```

2. Измените значение порта в конфигурационном файле C:\Program Files\Cyber Protego Server\proxy\conf\cpserver_proxy.conf:
   a. Закомментируйте строку 3:

```
# listen 80;
```

   b. Укажите порт в строках 5 и 11:

```
listen <порт> ssl http2;
```

```
return 301 https://$host:<порт>$request_uri;
```

   В итоге конфигурационный файл может выглядеть так:

```
server {
 # FOR SWITCHING TO NON-DEFAULT PORT: COMMENT NEXT LINE
 # listen 80;
 # FOR SWITCHING TO NON-DEFAULT PORT: CHANGE PORT TO REQUIRED IN THE NEXT
LINE
 listen <порт> ssl http2;
 server_name cpanalytics;

 # Redirect for http
 if ($scheme = 'http') {
 # FOR SWITCHING TO NON-DEFAULT PORT: CHANGE PORT TO REQUIRED IN THE NEXT
LINE
   return 301 https://$host:<порт>$request_uri;
 }
<...>
```

3. Запустите остановленные ранее службы:

```
> net start CPServer-backend
> net start CPServer-proxy
```

Изменение порта на ОС Linux

1. Остановите службу nginx:

```
# systemctl stop nginx
```

2. Измените значение порта в конфигурационном файле /etc/nginx/sites-available.d/cp_analytics_proxy.conf:
   a. Закомментируйте строку 3:

   ```
   # listen 80;
   ```

   b. Укажите порт в строках 5 и 11:

   ```
   listen <порт> ssl http2;
   ```

   ```
   return 301 https://$host:<порт>$request_uri;
   ```

   В итоге конфигурационный файл может выглядеть так:

```
server {
  # FOR SWITCHING TO NON-DEFAULT PORT: COMMENT NEXT LINE
  # listen 80;
  # FOR SWITCHING TO NON-DEFAULT PORT: CHANGE PORT TO REQUIRED IN THE NEXT
LINE
  listen <порт> ssl http2;
  server_name cpanalytics;

  # Redirect for http
  if ($scheme = 'http') {
  # FOR SWITCHING TO NON-DEFAULT PORT: CHANGE PORT TO REQUIRED IN THE NEXT
LINE
    return 301 https://$host:<порт>$request_uri;
  }
<...>
```

3. Запустите остановленную ранее службу:

```
# sudo systemctl start nginx
```

8.2 Установка пользовательских сертификатов

Веб-консоль поставляется и устанавливается с двумя самоподписанными (самозаверяющими) сертификатами:

- Для подключения к веб-интерфейсу.
- Для подключения к API (необходимо, в частности, для передачи событий на сервер Кибер Протего с сервера Кибер Файлов).

Любой из этих сертификатов при необходимости можно заменить на пользовательский. При этом понадобится соответствующий сертификату закрытый (приватный) ключ.

8.2.1 Установка сертификатов в ОС Windows

Чтобы установить пользовательский сертификат для подключения к веб-интерфейсу, выполните следующие действия:

1. Остановите службу CPServer-proxy:

```
> net stop CPServer-proxy
```

2. Поместите новый сертификат и соответствующий закрытый ключ в папку C:\Program Files\Cyber Protego Server\proxy.
3. Укажите имена файлов сертификата и закрытого ключа в файле C:\Program Files\Cyber Protego Server\proxy\conf\cpserver_proxy.conf. Например, для сертификата customcert.crt и ключа customkey.key укажите:

```
# Configuration for SSL/TLS certificates
ssl_certificate ../customcert.crt;
ssl_certificate_key ../customkey.key;
```

4. Запустите остановленную ранее службу:

```
> net start CPServer-proxy
```

Чтобы установить пользовательский сертификат для подключения к API, выполните следующие действия:

1. Остановите службу CPServer-backend:

```
> net stop CPServer-backend
```

2. Поместите новый сертификат и соответствующий закрытый ключ в папку C:\Program Files\Cyber Protego Server\backend.
3. Укажите имена файлов сертификата и закрытого ключа в файле C:\Program Files\Cyber Protego Server\backend\cpanalytics.yml. Например, для сертификата customcert.crt и ключа customkey.key укажите:

```
tls:
enabled: true
cert: customcert.crt
key: customkey.key
```

4. Запустите остановленную ранее службу:

```
> net start CPServer-backend
```

8.2.2 Установка сертификатов в ОС Linux

Чтобы установить пользовательский сертификат для подключения к веб-интерфейсу, выполните следующие действия:

1. Остановите службу nginx:

```
# systemctl stop nginx
```

2. Поместите новый сертификат и соответствующий закрытый ключ в директорию /etc/nginx/ssl.
3. Укажите имена файлов сертификата и закрытого ключа в файле /etc/nginx/sites-available.d/cp_analytics_proxy.conf. Например, для сертификата customcert.crt и ключа customkey.key укажите:

```
# Configuration for SSL/TLS certificates
ssl_certificate /etc/nginx/ssl/customcert.crt;
ssl_certificate_key /etc/nginx/ssl/customkey.key;
```

4. Запустите остановленную ранее службу:

```
# systemctl start nginx
```

Чтобы установить пользовательский сертификат для подключения к API, выполните следующие действия:

1. Остановите службу cpanalyticsd:

```
# systemctl stop cpanalyticsd
```

2. Поместите новый сертификат и соответствующий закрытый ключ в директорию /opt/cyberprotect/cpserver/backend/ssl.
3. Укажите имена файлов сертификата и закрытого ключа в файле /opt/cyberprotect/cpserver/config.yml. Например, для сертификата customcert.crt и ключа customkey.key укажите:

```
tls:
enabled: true
cert: /opt/cyberprotect/cpserver/backend/ssl/customcert.crt
key: /opt/cyberprotect/cpserver/backend/ssl/customkey.key
```

4. Запустите остановленную ранее службу:

```
# systemctl start cpanalyticsd
```

8.3 Замена служебной базы данных

Веб-консоль хранит сведения об авторизации, пользователях, ролях, правах и т. д. в служебной базе данных, которая автоматически создается при установке продукта. При необходимости эту БД можно заменить, выполнив следующие шаги (принимается, что продукт установлен в директории по умолчанию).

1. Остановите службу веб-консоли.

   В ОС Windows выполните команду:

   ```
   > net stop CPServer-backend
   ```

   В ОС Linux выполните команду:

   ```
   # systemctl stop cpanalyticsd
   ```

2. Отредактируйте конфигурационный файл.

   В ОС Windows: C:\Program Files\Cyber Protego Server\backend\cpanalytics.yml.

   В ОС Linux: /opt/cyberprotect/cpserver/config.yml.

   В файле укажите диалект базы данных: mssql или postgres. Второй вариант также необходимо выбирать для Jatoba. Например:

   ```
   db:
     dialect: mssql
   ```

   Также укажите следующие параметры:

   - **host** – IP-адрес или имя хоста, на котором работает сервер БД.
   - **port** – порт сервера БД; игнорируется при указании именованного экземпляра (named instance) для диалекта mssql.
   - **user** – имя пользователя БД.
   - **password** – пароль пользователя БД.
   - **database** – имя служебной БД; если такой базы данных не существует, она будет создана.
   - **sslMode** (только для диалекта postgres) – режим SSL-соединения; возможные значения: disable, require, verify-ca, verify-full.

   Например:

   ```
   db:
     dialect: mssql
     mssql:
       host: 10.10.10.10
       port: 1433
       user: sa
       password: strong_password
       database: NewCyberProtegoSDB
   ```

или

```
db:
  dialect: postgres
  <...>
  postgres:
    host: 10.10.10.10
    port: 5432
    user: postgres
    password: strong_password
    database: NewCyberProtegoSDB
    sslMode: disable
```

3. Если необходимо, примените к новой БД требуемую схему. Изначально она применяется к БД автоматически при установке веб-консоли. При смене базы данных, к новой БД также необходимо применить требуемую схему, если ранее этого не выполнялось.

   В случае, если к новой БД актуальная схема уже была применена (например, БД меняется на одну из использованных ранее), то применять схему еще раз не требуется, и этот шаг можно пропустить.

   Примечание
   Если на момент применения схемы БД еще не существует, она будет создана автоматически.

   Чтобы применить схему к БД в ОС Windows, выполните следующую команду из папки C:\Program Files\Cyber Protego Server\backend:

   ```
   > cpanalytics.exe migrate-db --config="cpanalytics.yml"
   ```

   Чтобы применить схему к БД в ОС Linux, выполните следующую команду из директории /opt/cyberprotect/cpserver/backend/:

   ```
   # ./cpanalyticsd migrate-db --config='../config.yml'
   ```

   Пример вывода в случае успешного выполнения команды:

   ```
   migration/mssql/20230210959000_init_report_tasks
   migration/mssql/20230210959000_init_roles
   migration/mssql/20230210959000_init_users
   migration/mssql/20230210959000_init_public
   ```

4. Запустите остановленную ранее службу.

   В ОС Windows выполните команду:

   ```
   > net start CPServer-backend
   ```

   В ОС Linux выполните команду:

   ```
   # systemctl start cpanalyticsd
   ```

8.4 Изменение времени ожидания ответа сервера

По умолчанию время ожидания ответа сервера составляет 10 минут. При необходимости его можно увеличить, выполнив следующие шаги.

Примечание
Максимально допустимое время ожидания – 3 часа.

8.4.1 Изменение времени ожидания в ОС Windows

1. Остановите службы CPServer-backend и CPServer-proxy:

```
> net stop CPServer-backend
> net stop CPServer-proxy
```

2. В конфигурационном файле C:\Program Files\Cyber Protego Server\backend\cpanalytics.yml укажите необходимое время ожидания в формате "<минуты>m" или "<часы>h". Например, "15m":

```
server:
  <...>
  timeouts:
    write: 15m
```

3. В конфигурационном файле C:\Program Files\Cyber Protego Server\proxy\conf\cpserver_proxy.conf укажите необходимое время ожидания в секундах. Например, "900":

```
location /api/ {
  proxy_read_timeout 900;
  <...>
}
```

4. Запустите остановленные ранее службы:

```
> net start CPServer-backend
> net start CPServer-proxy
```

8.4.2 Изменение времени ожидания в ОС Linux

1. Остановите службы cpanalyticsd и nginx:

```
# systemctl stop cpanalyticsd
# systemctl stop nginx
```

2. В конфигурационном файле /opt/cyberprotect/cpserver/config.yml укажите необходимое время ожидания в формате "<минуты>m" или "<часы>h". Например, "15m":

```
db:
  <...>
  connMaxLifeTime: 15m
```

3. В конфигурационном файле /etc/nginx/sites-available.d/cp_analytics_proxy.conf укажите необходимое время ожидания в секундах. Например, "900":

```
location /api/ {
  proxy_read_timeout 900;
  <...>
}
```

4. Запустите остановленные ранее службы:

```
# systemctl start cpanalyticsd
# systemctl start nginx
```

Указатель