КИБЕРПРОТЕКТ

# КИБЕР Протего

Версия 11.1

Руководство пользователя
веб-консоли

Редакция: 25.06.2026

# Оглавление

# О веб-консоли

Веб-консоль Cyber Protego — это кроссплатформенное аналитическое решение, которое позволяет выполнять следующие действия:

- Строить отчёты по данным аудита, теневого копирования и контроля рабочего времени.
- Управлять списком событий: просматривать, фильтровать, сортировать, экспортировать, комментировать и удалять события, назначать им статусы рассмотрения, а также просматривать и скачивать их теневые копии.
- Гибко настраивать сводку событий с помощью динамических виджетов.
- Исследовать статистику сетевой коммуникации пользователей с помощью графов связей.
- Управлять агентами для Linux.
- Просматривать, фильтровать, скачивать и удалять записи мониторинга активности пользователей (запись клавиатурного ввода, запись экранов, список запущенных процессов на момент записи), полученные от агентов для ОС Windows и Linux.

# Установка и удаление

## Требования к системе

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

- Альт Рабочая станция 10.x—11.1,
- Astra Linux SE 1.7.5—1.8.5 в редакциях Орел и Воронеж,
- РЕД ОС 7.3.4—8.0.2,
- CentOS Stream 9 и 10,
- Windows Server 2012 и новее.

Компьютер, на который устанавливается веб-консоль, должен иметь:

- процессор Intel Core i5 с 4 ядрами или более мощный,
- минимум 4 ГБ ОЗУ.

Для работы веб-консоли должна быть установлена одна из следующих СУБД: Microsoft SQL Server 2016 и новее, PostgreSQL / Postgres Pro Standard 13 и новее, Jatoba 4.5 и новее, Tantor SE 15 и новее.

Кроме того, для доступа к веб-консоли на машине, где она расположена, должны быть открыты и свободны следующие порты:

- 9137 — для взаимодействия с агентами.
- 80, 443 – для доступа к веб-консоли. Если эти порты по умолчанию заняты, можно выбрать другие (см. *Изменение порта веб-консоли*).
- 444, 8081 — для взаимодействия компонентов веб-консоли (должны быть открыты локально).

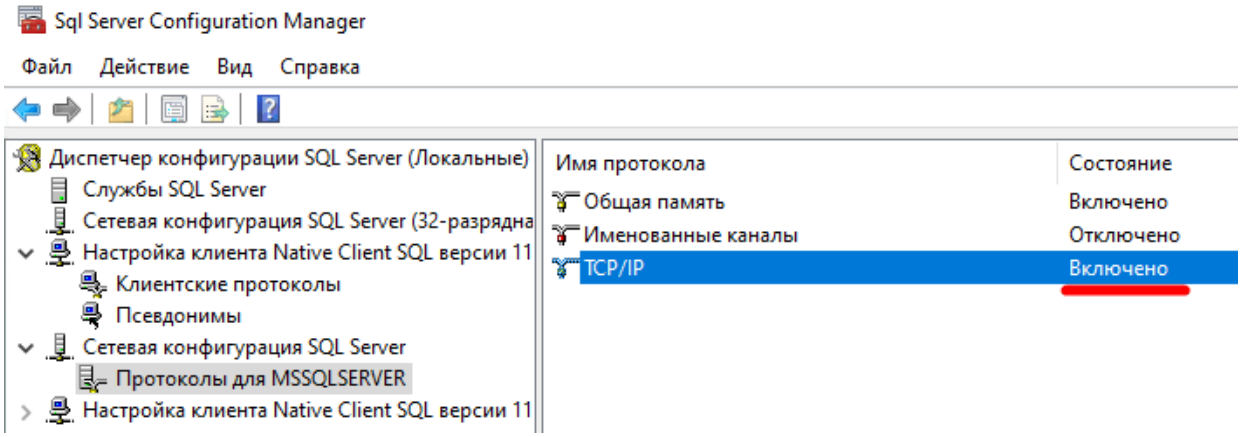
Кроме того, должны быть открыты порты для взаимодействия с СУБД (по умолчанию 5432 для PostgreSQL, Postgres Pro, Jatoba и Tantor, 1433 для Microsoft SQL Server) и для взаимодействия со службами каталогов по протоколам LDAP и LDAPS (по умолчанию 389 и 636, соответственно).

## Требования к Microsoft SQL Server

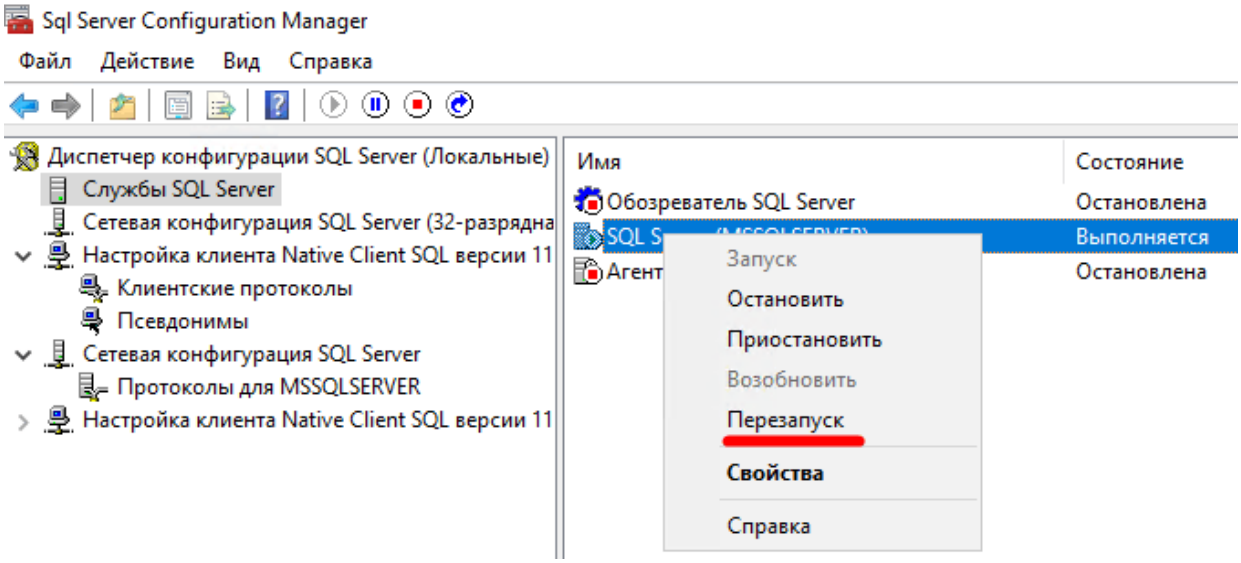
Для использования с веб-консолью СУБД Microsoft SQL Server должна удовлетворять этим требованиям:

- 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`**.




- Запущена служба SQL Server Browser.

  Подробнее настройка этой службы описана в документации Microsoft.

> **Примечание**
>
> Если данная служба остановлена, указывать именованный экземпляр не требуется.

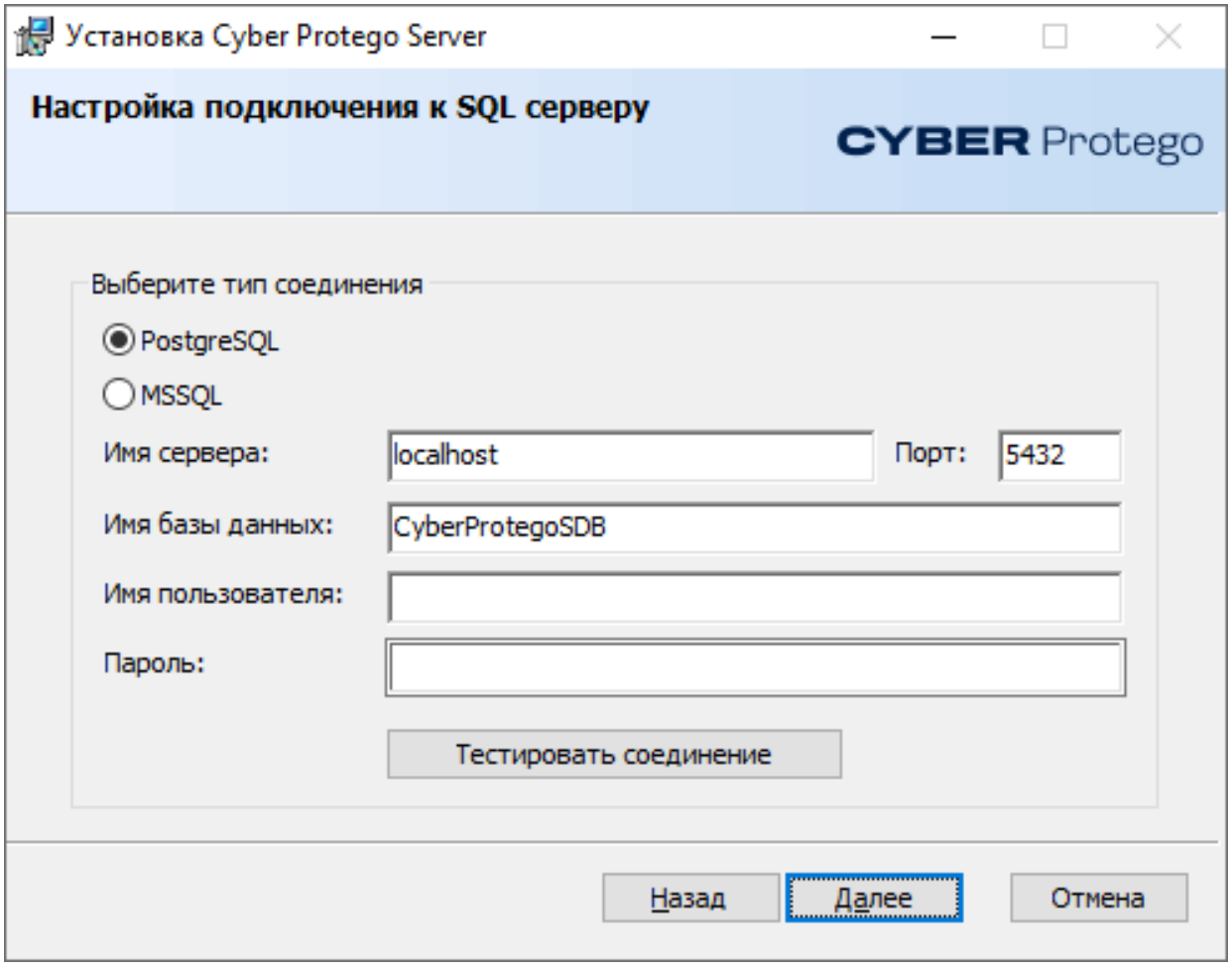
# Установка на Windows

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 автоматически созданной служебной БД для размещения данных веб-консоли.



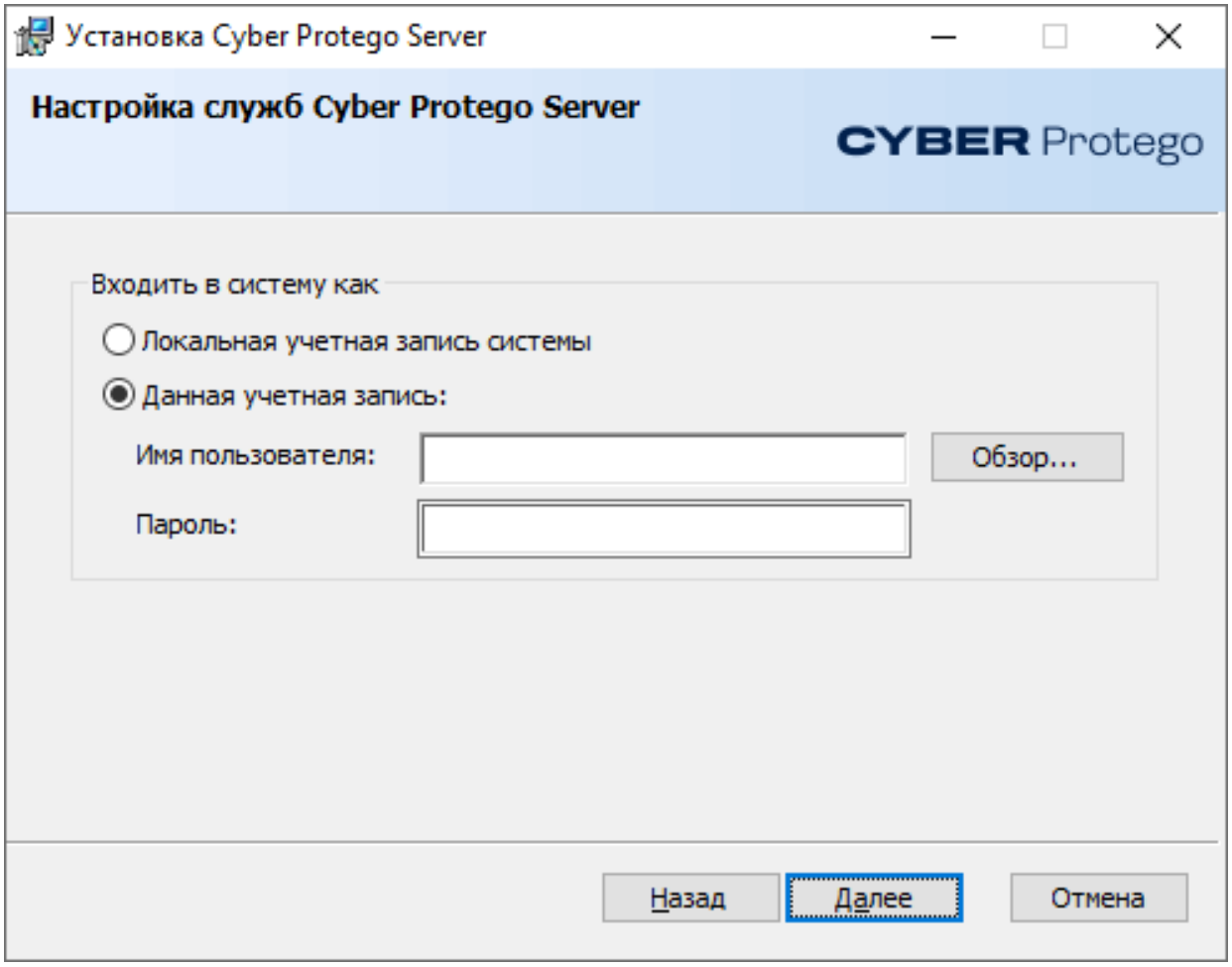

При использовании СУБД PostgreSQL (а также Postgres Pro, Jatoba или Tantor) должна существовать БД по умолчанию ”postgres”.

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

**Важно**

Служебная БД не является *базой данных событий*.

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 событий*.

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

После обновления веб-консоли необходимо обновить базу данных событий. Для этого в разделе

**НАСТРОЙКИ** → **База данных** заново укажите пароль к этой БД, сохраните изменения и подтвердите её обновление.

# Установка на Linux

В дистрибутив для Linux входят пакеты RPM и DEB для поддерживаемых ОС, а также скрипт установки **`start_CyberProtegoServerInstaller.sh`**.

Установка выполняется пользователем с привилегиями sudo.

Чтобы установить веб-консоль, выполните следующие действия:

1. Запустите скрипт установки:

   ```
   $ sudo ./start_CyberProtegoServerInstaller.sh
   ```

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

   ```
   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 автоматически созданной служебной БД для веб-консоли. Нажав `Enter`, можно оставить базу данных по умолчанию.

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

   При использовании СУБД PostgreSQL (а также Postgres Pro, Jatoba или Tantor) должна существовать БД по умолчанию ”postgres”.

   > **Важно**
   >
   > Служебная БД не является *базой данных событий*.

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.

> **Примечание**
>
> В Astra Linux необходимо предоставить служебному пользователю **_apt** права на доступ к каталогу с установочным пакетом и его родительским каталогам. Иначе при установке появится предупреждение. Установка при этом завершится успешно.

После установки необходимо указать БД, по данным которой будут строиться отчёты. Выполните шаги из раздела *База данных событий*.

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

После обновления веб-консоли необходимо обновить базу данных событий. Для этого в разделе **НАСТРОЙКИ** → **База данных** заново укажите пароль к этой БД, сохраните изменения и подтвердите её обновление.

# Настройка взаимодействия с агентами для Linux

Чтобы обеспечить взаимодействие между веб-консолью и агентами для Linux, необходимо разместить на них набор сертификатов и ключей. Можно использовать имеющийся у вас набор или создать тестовый (см. далее).

> **Примечание**
>
> В промышленных развёртываниях рекомендуется использовать сертификаты и ключи, выданные доверенным центром сертификации.

## Создание набора самоподписанных сертификатов и ключей

Чтобы создать тестовый набор сертификатов и ключей, выполните следующие действия:

1. Создайте временный каталог. Например:

```
$ mkdir /tmp/protego
```

2. Создайте во временном каталоге файл скрипта:

```
$ sudo touch /tmp/protego/gen_crt.sh
```

3. Внесите в файл скрипта следующий текст (с учетом особенностей вашей инфраструктуры):

```
# !/bin/bash

# Create dir
mkdir -p ~/certs
cd ~/certs

# Create file config
cat <<EOF > domains.ext
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
EOF

# Generate CA key and cert
openssl genrsa -out server_ca.key 2048
openssl req -new -x509 -nodes -days 365 -key server_ca.key -out server_ca.crt -subj "/C=RU/
↪ST=MOSCOW/L=MOSCOW/O=CyberProtect LLC/OU=RnD/CN=testSrvCA"

# Generate server key
openssl req -newkey rsa:2048 -nodes -keyout server.key -out server.req -subj "/C=RU/
↪ST=MOSCOW/L=MOSCOW/O=CyberProtect LLC/OU=RnD/CN=testSrv"
openssl x509 -req -in server.req -days 365 -CA server_ca.crt -CAkey server_ca.key -set_
↪serial 01 -out server.crt -extfile domains.ext

# Generate client key and cert
openssl req -newkey rsa:2048 -nodes -keyout client.key -out client.req -subj "/C=RU/
↪ST=MOSCOW/L=MOSCOW/O=CyberProtect LLC/OU=RnD/CN=testClient"
openssl x509 -req -in client.req -days 365 -CA server_ca.crt -CAkey server_ca.key -set_
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
↪serial 01 -out client.crt -extfile domains.ext
```

Имена ключей и сертификатов должны удовлетворять следующим правилам:

- При создании ключа клиента `client.key` поле `CN` должно заканчиваться словом ”Client” или ”Agent”. Например:

```
openssl req -newkey rsa:2048 -nodes -keyout client.key -out client.req -subj ”/C=RU/
↪ST=MOSCOW/L=MOSCOW/O=CyberProtect LLC/OU=RnD/CN=testClient”
```

- При создании ключа сервера `server.key` поле `CN` не должно заканчиваться словом ”Client” или ”Agent”. Например:

```
openssl req -newkey rsa:2048 -nodes -keyout server.key -out server.req -subj ”/C=RU/
↪ST=MOSCOW/L=MOSCOW/O=CyberProtect LLC/OU=RnD/CN=testSrv”
```

4. Перейдите в созданный каталог, сделайте скрипт исполняемым и запустите его:

```
$ cd /tmp/protego
$ sudo chmod +x ./gen_crt.sh
$ ./gen_crt.sh
```

В результате выполнения скрипта в домашней директории пользователя будет создан каталог `certs` с набором самоподписанных сертификатов и ключей. Например, для пользователя `administrator` будут созданы следующие файлы:

```
/home/administrator/certs/client.crt # Сертификат клиента
/home/administrator/certs/client.key # Закрытый ключ для сертификата клиента
/home/administrator/certs/client.req
/home/administrator/certs/domains.ext
/home/administrator/certs/server.crt # Сертификат сервера
/home/administrator/certs/server.key # Закрытый ключ для сертификата сервера
/home/administrator/certs/server.req
/home/administrator/certs/server_ca.crt # Сертификат центра сертификации
/home/administrator/certs/server_ca.key
```

Все следующие действия описаны на примере данного набора.

## Настройка веб-консоли для работы с набором сертификатов и ключей

Чтобы настроить веб-консоль для работы с набором сертификатов и ключей, выполните следующие действия:

1. Скопируйте в директорию веб-консоли `/opt/cyberprotect/cpserver/backend/ssl/` (ОС Linux) или `C:\Program Files\Cyber Protego Server\backend` (ОС Windows) следующие файлы: `server.crt`, `server.key`, `server_ca.crt`, `client.crt`, `client.key`.

   Пример для ОС Linux:

   ```
   $ sudo cp ~/certs/{server.crt,server.key,server_ca.crt,client.crt,client.key} /opt/
   ↪cyberprotect/cpserver/backend/ssl/
   ```

2. В конфигурационном файле `/opt/cyberprotect/cpserver/CPServerBackend.yml` (ОС Linux) или `C:\Program Files\Cyber Protego Server\backend\CPServerBackend.yml` (ОС Windows), в разделах `server` -> `management` и `client` включите использование TLS и укажите пути к скопированным файлам.

   **Пример для ОС Linux**

   ```
   server:
     <...>
     management:
       <...>
       tls:
         enabled: true
         cert: /opt/cyberprotect/cpserver/backend/ssl/server.crt
         key: /opt/cyberprotect/cpserver/backend/ssl/server.key
         caCert: /opt/cyberprotect/cpserver/backend/ssl/server_ca.crt
       agent_cert:
         cert: /opt/cyberprotect/cpserver/backend/ssl/client.crt
         key: /opt/cyberprotect/cpserver/backend/ssl/client.key
   client:
     <...>
     tls:
       enabled: true
       cert: /opt/cyberprotect/cpserver/backend/ssl/server.crt
       key: /opt/cyberprotect/cpserver/backend/ssl/server.key
       caCert: /opt/cyberprotect/cpserver/backend/ssl/server_ca.crt
   ```

#### Пример для ОС Windows

```
server:
  <...>
  management:
    <...>
    tls:
      enabled: true
      cert: C:\Program Files\Cyber Protego Server\backend\server.crt
      key: C:\Program Files\Cyber Protego Server\backend\server.key
      caCert: C:\Program Files\Cyber Protego Server\backend\server_ca.crt
client:
  <...>
  tls:
    enabled: true
    cert: C:\Program Files\Cyber Protego Server\backend\server.crt
    key: C:\Program Files\Cyber Protego Server\backend\server.key
    caCert: C:\Program Files\Cyber Protego Server\backend\server_ca.crt
```

3. Перезапустите службу **`CPServerBackend`**:

#### Linux

```
$ sudo systemctl restart CPServerBackend
```

#### Windows

```
> net stop CPServerBackend && net start CPServerBackend
```

## Настройка агентов для работы с набором сертификатов и ключей

Этот шаг можно пропустить, если используется веб-консоль на ОС Linux, для который выполнены все настройки, указанные ранее в этом разделе. В таком случае сертификаты будут размещены на агентах автоматически при выполнении задач установки.

Если в папке `/opt/cyberprotect/cpserver/backend/ssl/` нет ключа и сертификата клиента, при выполнении задач установки агенты будут установлены, но не настроены. В этом случае потребуется настроить взаимодействие с ними вручную.

Чтобы настроить агенты для работы с набором сертификатов и ключей, выполните следующие действия для каждого агента:

1. Скопируйте в директорию агента `/opt/cyberprotect/protego/bin/` следующие файлы: `client.crt`, `client.key`, `server_ca.crt`. Например:

```
$ sudo cp ~/certs/{client.key,client.crt,server_ca.crt} /opt/cyberprotect/protego/bin/
```

2. От имени пользователя root укажите владельца скопированных файлов и задайте права доступа к ним:

```
$ su
$ cd /opt/cyberprotect/protego/bin/
$ chown cyberprotect:cyberprotect *.crt *.key
$ chmod 0400 *.crt *.key
```

3. Перезапустите службу **`protegod`**:

```
$ sudo systemctl restart protegod
```

# 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:

### Для RPM-пакета

```
$ sudo rpm -e cyber-protego-server
```

### Для DEB-пакета

```
$ sudo apt-get remove cyber-protego-server
```

Будет удален пакет **cyber-protego-server**, остановлена и удалена служба **CPServerBackend**. Кроме того, будут удалены файлы из директории `/opt/cyberprotect/cpserver`.

> **Примечание**
>
> Служебная БД не будет удалена.

# Вход в веб-консоль

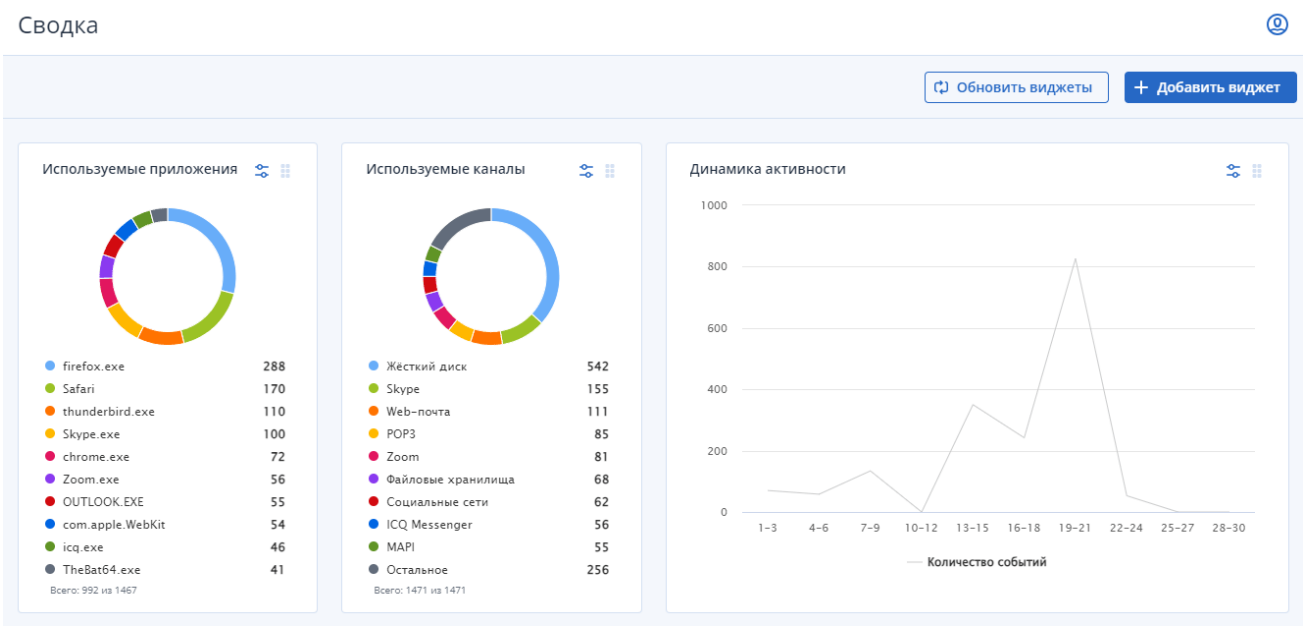
Чтобы войти в веб-консоль, перейдите по имени или адресу ее хоста, укажите логин и пароль в соответствующих полях и нажмите **Войти**. Используется протокол HTTPS.

По умолчанию создан пользователь с логином ”admin” и паролем ”Ср*123456”.

# Сводка

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

Работать с этим разделом могут только пользователи с соответствующим правом доступа (см. *Роли*).




**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.

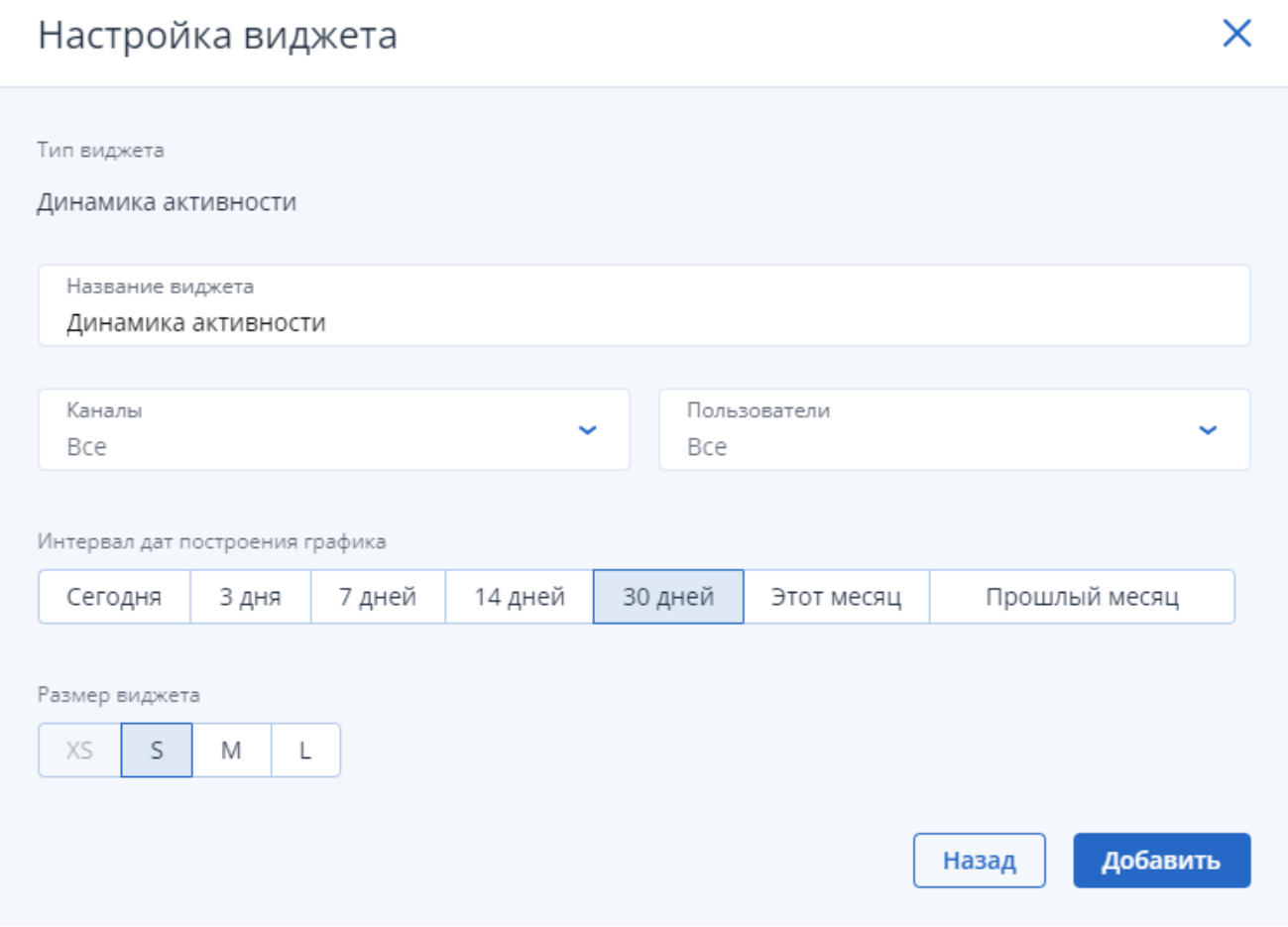
## Управление виджетами

Пользователи могут добавлять, изменять и удалять виджеты в сводке.

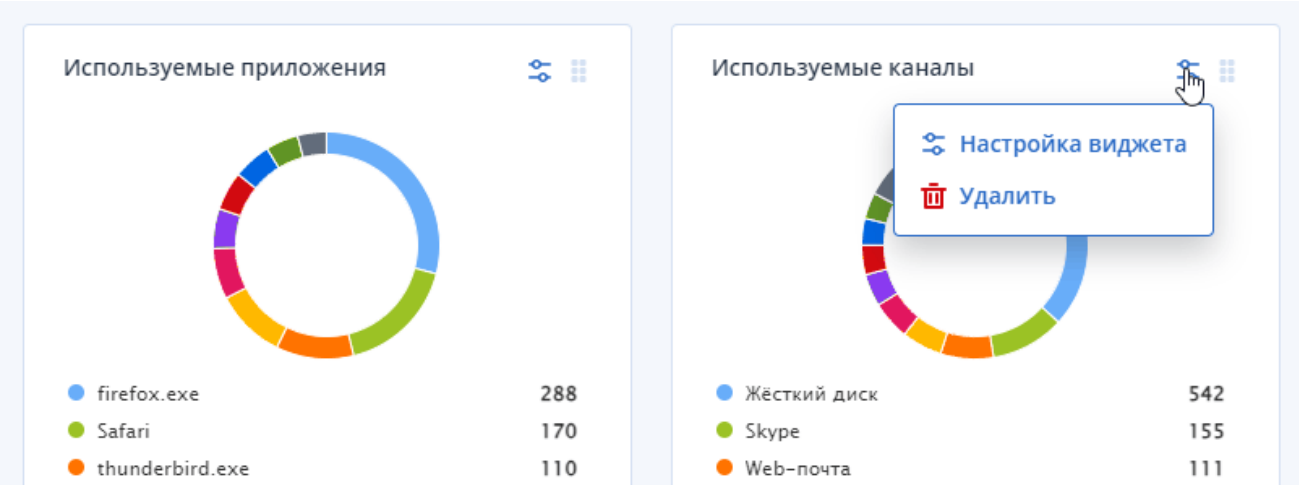
Чтобы создать виджет, щелкните **+ Добавить виджет** справа сверху. В появившемся окне выберите тип виджета. В следующем окне укажите его параметры. Нужно задать **Название виджета**, **Каналы**, **Пользователи**, **Интервал дат построения графика**, размер и количество отображаемых данных. При этом 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.

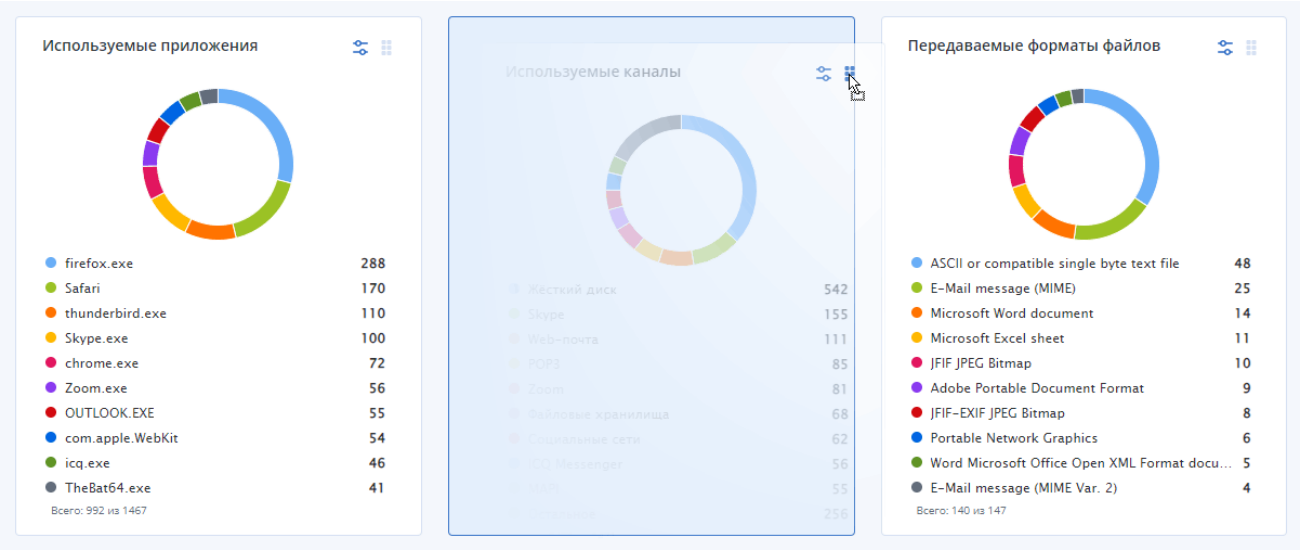
> **Примечание**
>
> Названия виджетов в сводке должны быть уникальны.




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



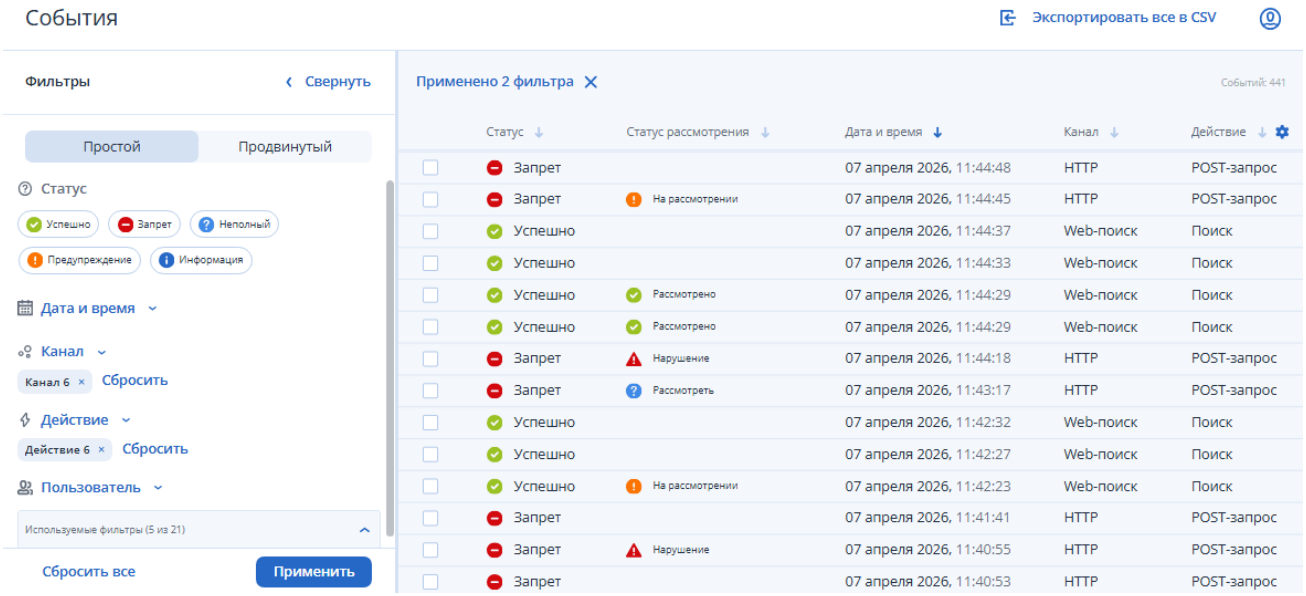

Чтобы переместить виджет, щелкните и удерживайте значок в правом верхнем углу и перетащите его на нужное место. Остальные виджеты подстроятся под новую раскладку.


Используемые приложения
firefox.exe 288
Safari 170
thunderbird.exe 110
Skype.exe 100
chrome.exe 72
Zoom.exe 56
OUTLOOK.EXE 55
com.apple.WebKit 54
icq.exe 46
TheBat64.exe 41
Всего: 992 из 1467
Используемые каналы
Передаваемые форматы файлов
ASCII or compatible single byte text file 48
E-Mail message (MIME) 25
Microsoft Word document 14
Microsoft Excel sheet 11
JFIF JPEG Bitmap 10
Adobe Portable Document Format 9
JFIF-EXIF JPEG Bitmap 8
Portable Network Graphics 6
Word Microsoft Office Open XML Format docu... 5
E-Mail message (MIME Var. 2) 4
Всего: 140 из 147

# Журналы

## События

В разделе **ЖУРНАЛЫ** → **События** можно просматривать, экспортировать и удалять события из подключённой базы данных, связанные с использованием устройств и сетевых протоколов сотрудниками вашей компании. Здесь же можно просматривать, скачивать и удалять теневые копии событий. Доступ к этому разделу имеют пользователи с правом просмотра событий (см. *Права для журналов*).




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 возникновения события.
- **Действие** — действие пользователя.

- **Теневая копия** — наличие теневой копии у события.
- **Канал** — тип протокола или устройства.
- **Пользователь** — имя пользователя, связанного с событием.
- **Компьютер** — имя или IP-адрес компьютера, на котором произошло событие.
- **Имя** — имя объекта (файла, USB-устройства и т. п.), связанного с событием.
- **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

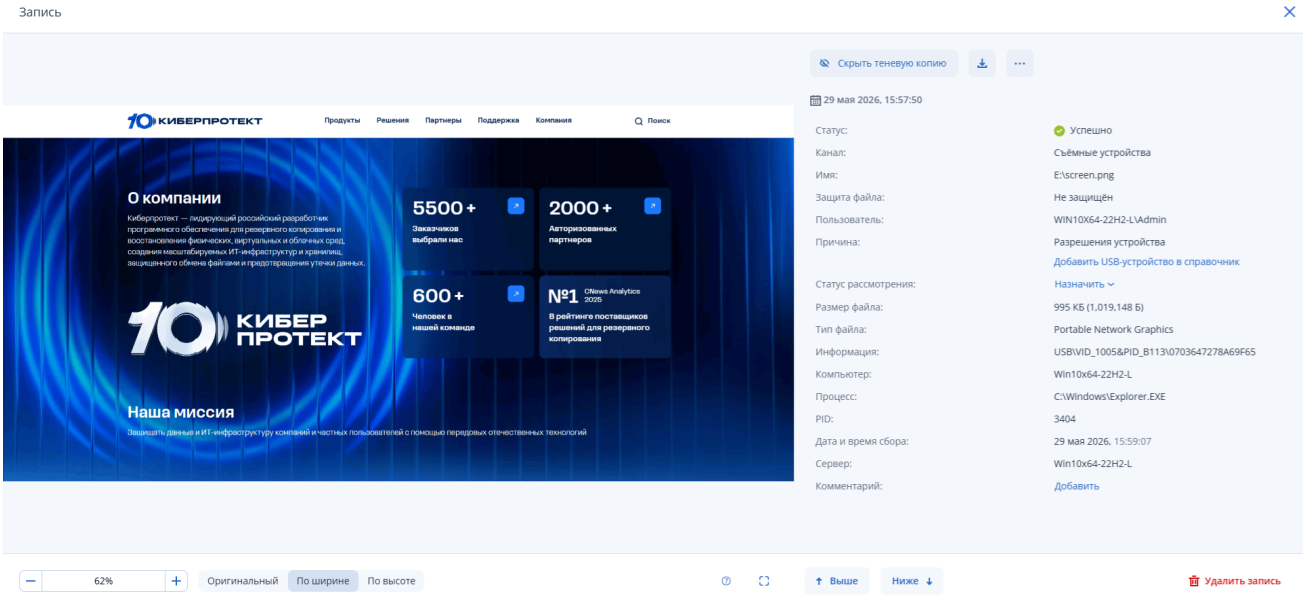
  Поле могут изменять только пользователи с правом на изменение событий (см. *Роли*).
- **Комментарий** — дополнительная информация о событии, заполняемая пользователем (не более 2000 символов). Указать комментарий можно только в окне сведений о событии, нажав **Добавить**. Изменить комментарий можно там же, нажав **Изменить**. Это поле отображается только в продвинутых фильтрах. Его нет в общем списке событий и простых фильтрах. Поле могут изменять только пользователи с правом на изменение событий (см. *Роли*).
- **Сервер** — имя сервера управления, получившего событие.
- **Серверный источник** — IP-адрес или имя клиента API, с которого получено событие.
- **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 управления.

- **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. В окне сведений также можно просмотреть, скачать или удалить теневую копию события. Переходить между записями можно с помощью кнопок **Выше** и **Ниже**.

Просматривать можно не защищённые паролем файлы следующих форматов:

- текстового (.txt);
- PDF (.pdf);
- изображений (.png, .jpg / .jpeg, .bmp);
- видео (.mp4).




Чтобы экспортировать события, удовлетворяющие текущему фильтру, нажмите **Экспортировать все в CSV** вверху справа. Чтобы экспортировать только события, отмеченые флажками, нажмите **Экспортировать в CSV** над их списком. По завершении экспорта внизу справа появится уведомление со ссылкой на итоговый файл в формате CSV (разделители — запятые).

Чтобы удалить событие, откройте сведения о нём и внизу нажмите **Удалить запись**. Чтобы удалить сразу несколько событий, отметьте их флажками в столбце слева и нажмите **Удалить** над списком событий.

Чтобы настроить автоматическую очистку журнала, щёлкните выпадающее меню **Очистить журнал** в

правом верхнем углу и выберите **Настроить автоматическое удаление старых данных**. В открывшемся разделе **Конфигурация** задайте параметры автоматической очистки журнала.

Чтобы очистить журнал вручную, щёлкните выпадающее меню **Очистить журнал** в правом верхнем углу и выберите **Удалить старые данные сейчас**. В появившемся диалоге укажите возраст записей, которые нужно удалить. Чтобы удалить все данные в журнале, укажите возраст записей, равный 0 лет, 0 месяцев и 0 дней.

Удаление записей выполняется в фоновом режиме. При запуске этой процедуры появляется уведомление.

## Продвинутые фильтры

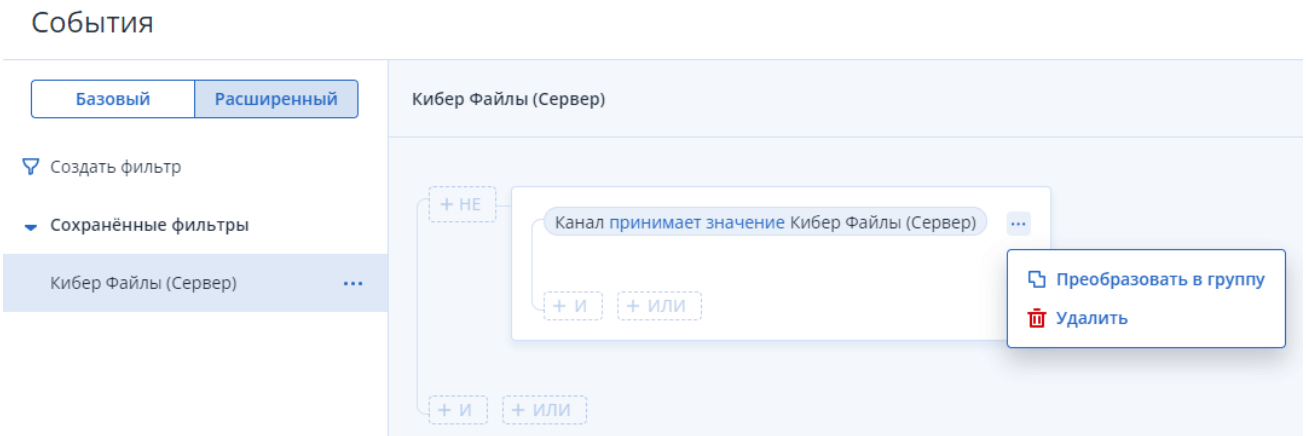
Продвинутые фильтры являются дополнением к простым фильтрам и позволяют создавать логические конструкции с использование операторов ”И”, ”ИЛИ”, ”НЕ”.

Выполнение сложных продвинутых фильтров может занимать долгое время. При необходимости можно увеличить время ожидания ответа сервера, как описано в разделе *Изменение времени ожидания ответа сервера*.

Продвинутые 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 продвинутых фильтров не ограничен.



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

Чтобы создать продвинутый фильтр, перейдите в раздел **События**, щелкните **Продвинутый** 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.

# Активность пользователей

В разделе **ЖУРНАЛЫ** → **Активность пользователей** можно просматривать, фильтровать, скачивать и удалять записи мониторинга активности пользователей (запись клавиатурного ввода, запись экранов, список запущенных процессов на момент записи), полученные от агентов для ОС Windows и Linux.

Журнал формируется на основе информации из базы данных событий (см. *База данных событий*).

Доступ к этому разделу имеют пользователи с правом просмотра активности пользователей (см. *Права для журналов*).

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

- **Тип** — тип записи: **Запись клавиатуры**, **Запись экрана**, **Запись клавиатуры и экрана**. Список процессов дополняет записи каждого типа.
- **Пользователь** — имя пользователя, чья активность записана.
- **Дата и время** — дата и время начала записи.
- **Продолжительность** — промежуток времени (часы, минуты и секунды), в течение которого выполнялась запись.
- **Правило** — список правил, активировавших начало записи.
- **Причина** — список критериев запуска правил, активировавших начало записи. Критерии перечисляются для каждого правила отдельно.
- **Компьютер** — имя или IP-адрес компьютера, на котором выполнена запись.
- **Дата и время сбора** — дата и время, когда запись была получена сервером управления.

- **Сервер** — имя сервера управления, получившего запись.

Чтобы просмотреть все сведения о записи, нажмите на неё в списке. В окне сведений можно выполнить следующие действия:

- Просмотреть запись экрана, нажав **Показать запись экрана**.

  Откроется окно видеоплеера, которым можно управлять с помощью мыши и горячих клавиш. Список клавиш управления можно посмотреть, нажав значок вопроса справа под видео.

- Скачать или удалить запись экрана, нажав значок многоточия справа от кнопки **Показать запись экрана** / **Скрыть запись экрана** и выбрав нужное действие из выпадающего меню.

- Скачать или удалить событие, нажав соответствующие кнопки справа вверху или внизу.

- Перейдя на вкладку **Запись клавиатуры**, просмотреть список клавиш, включая специальные, которые были нажаты пользователем за время события.

- Перейдя на вкладку **Процессы**, просмотреть список процессов, включая скрытые, которые были запущены на машине пользователя за время события.

- Перейти к предыдущей или следующей записи в списке с помощью кнопок **Выше** и **Ниже**.

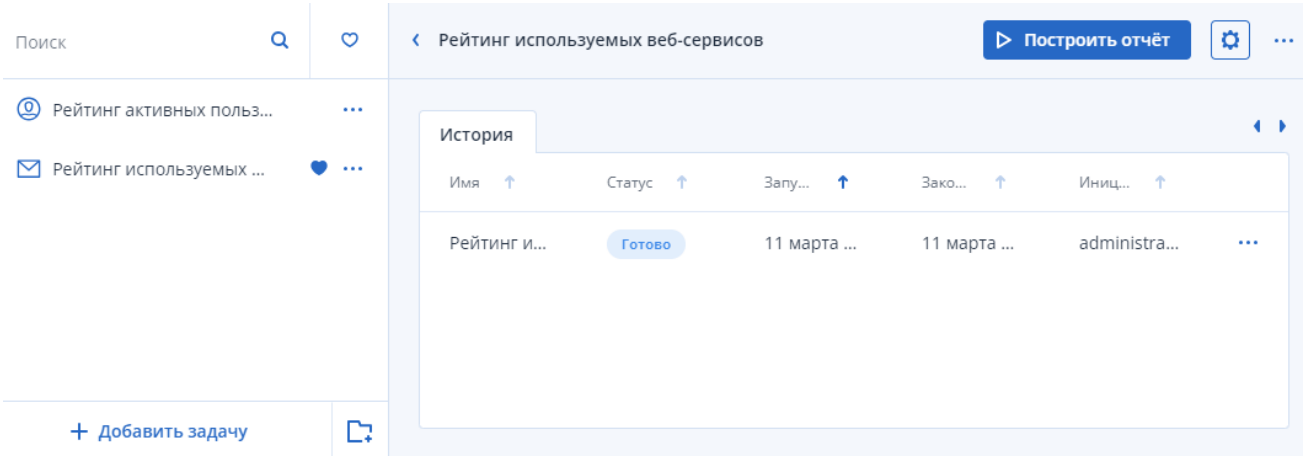
Чтобы настроить автоматическую очистку журнала, щёлкните выпадающее меню **Очистить журнал** в правом верхнем углу и выберите **Настроить автоматическое удаление старых данных**. В открывшемся разделе **Конфигурация** задайте параметры автоматической очистки журнала.

Чтобы очистить журнал вручную, щёлкните выпадающее меню **Очистить журнал** в правом верхнем углу и выберите **Удалить старые данные сейчас**. В появившемся диалоге укажите возраст записей, которые нужно удалить. Чтобы удалить все данные в журнале, укажите возраст записей, равный 0 лет, 0 месяцев и 0 дней.

Удаление записей выполняется в фоновом режиме. При запуске этой процедуры появляется уведомление.

# Отчёты

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



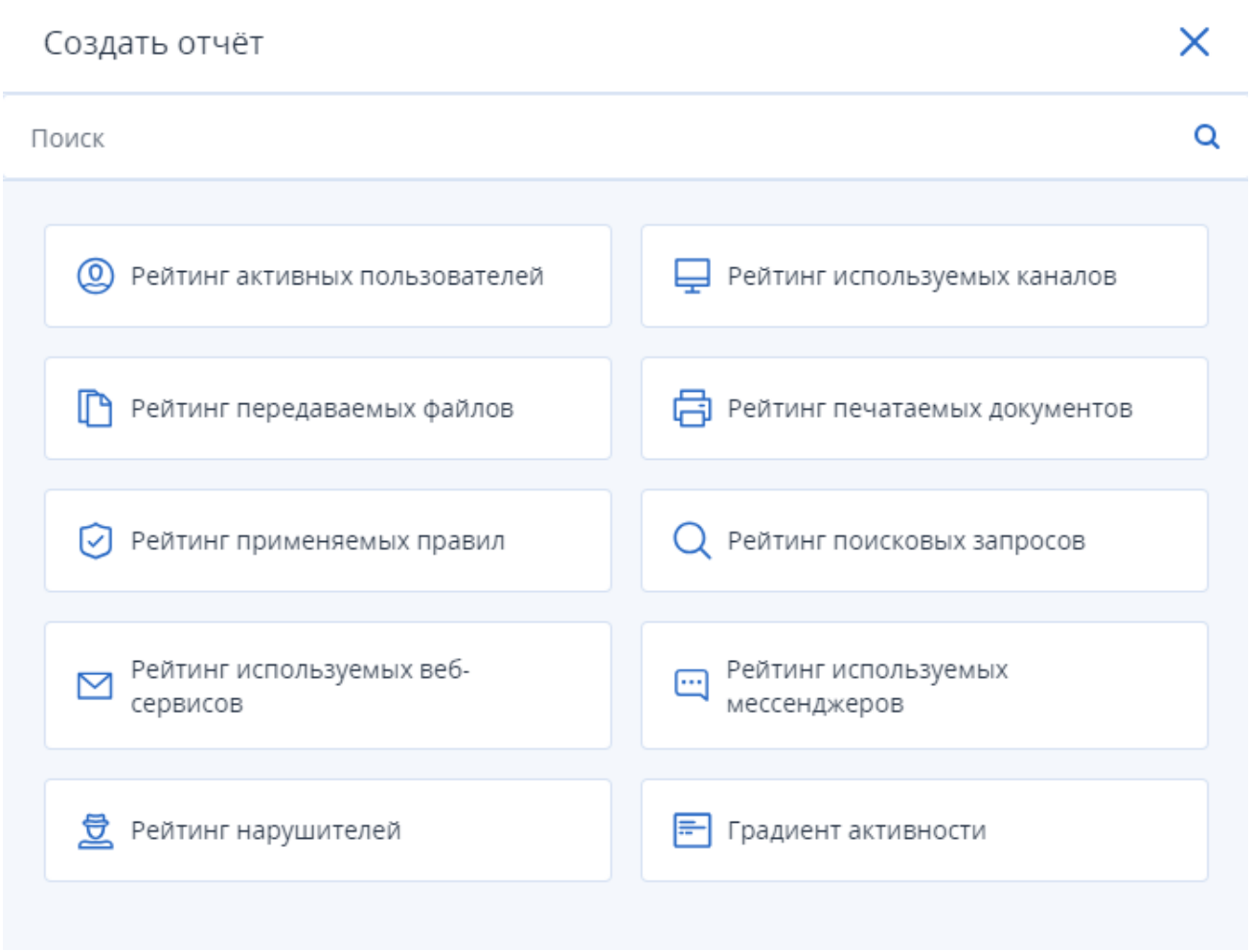

**Примечание**

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.

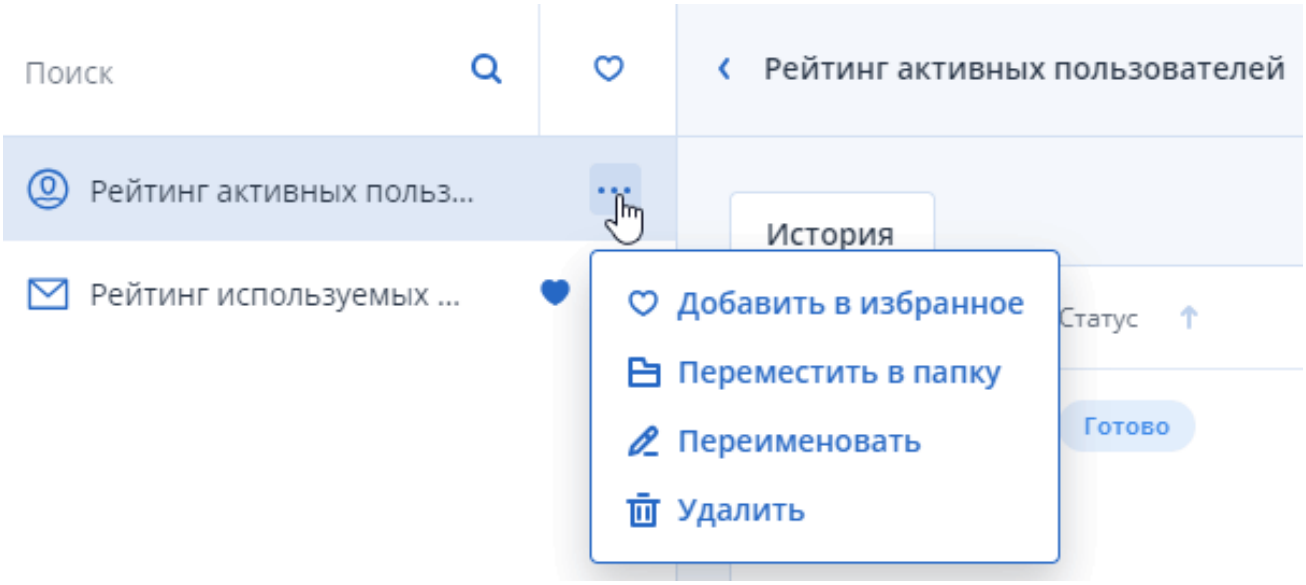
В дальнейшем отчёт можно перестраивать, запуская задачу вручную кнопкой **Построить отчёт** и выбирая диапазон дат.

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.

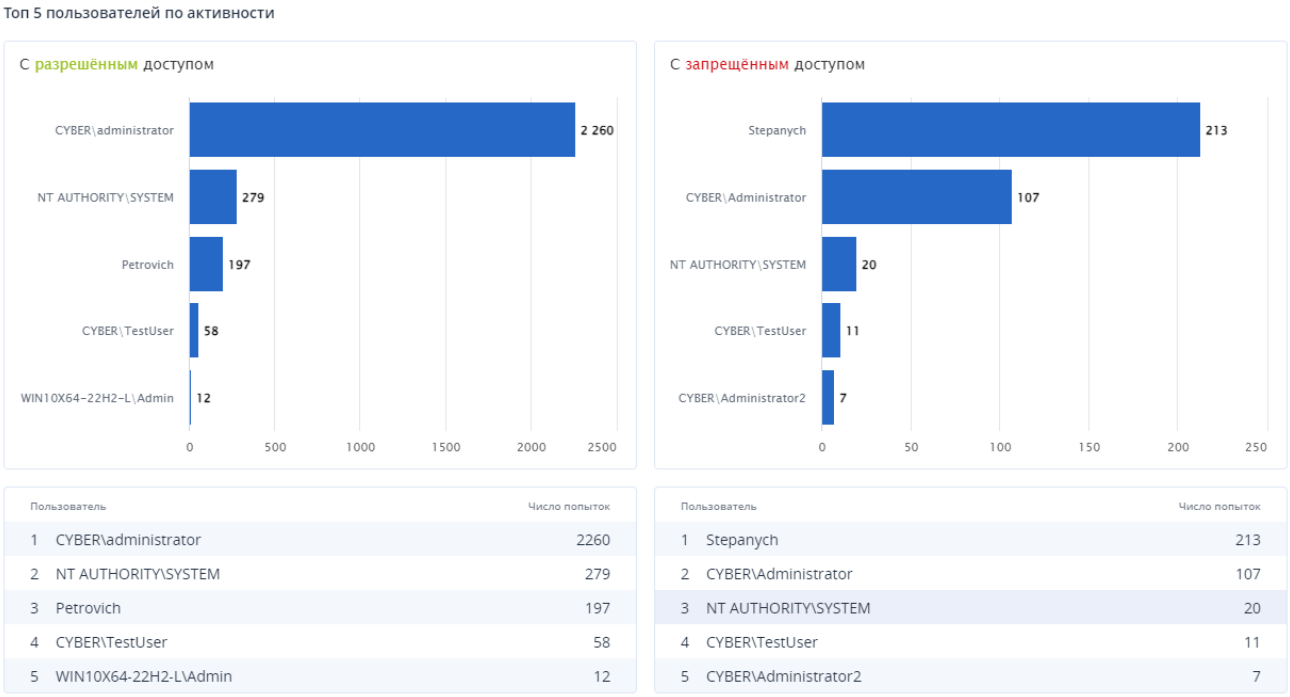



Чтобы перенести задачу в папку, откройте контекстное меню, нажав многоточие справа от ее имени в списке, и выберите **Переместить в папку**. В появившемся окне выберите папку и нажмите **Переместить**.

# Базовые

## Рейтинг активных пользователей

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

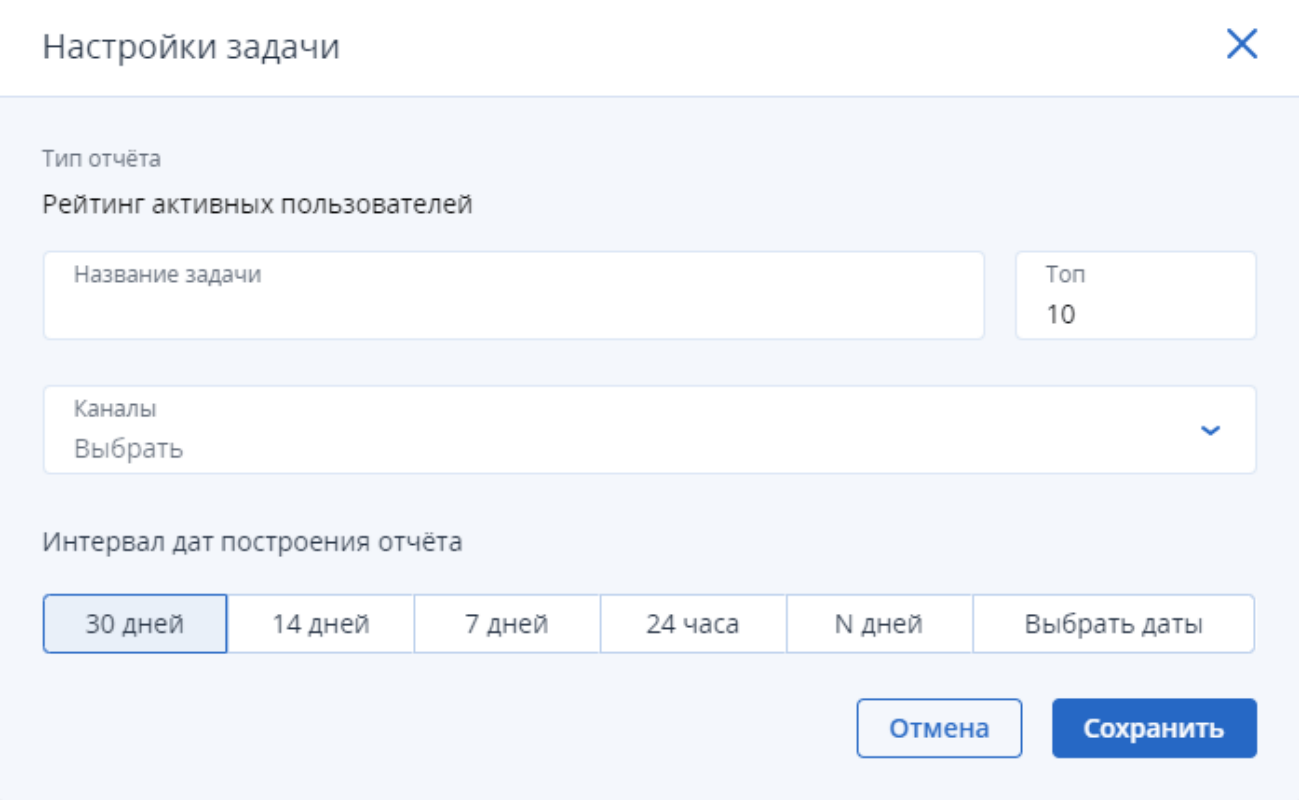



| | Пользователь | Число попыток |
|---|---|---|
| 1 | CYBER\administrator | 2260 |
| 2 | NT AUTHORITY\SYSTEM | 279 |
| 3 | Petrovich | 197 |
| 4 | CYBER\TestUser | 58 |
| 5 | WIN10X64-22H2-L\Admin | 12 |

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

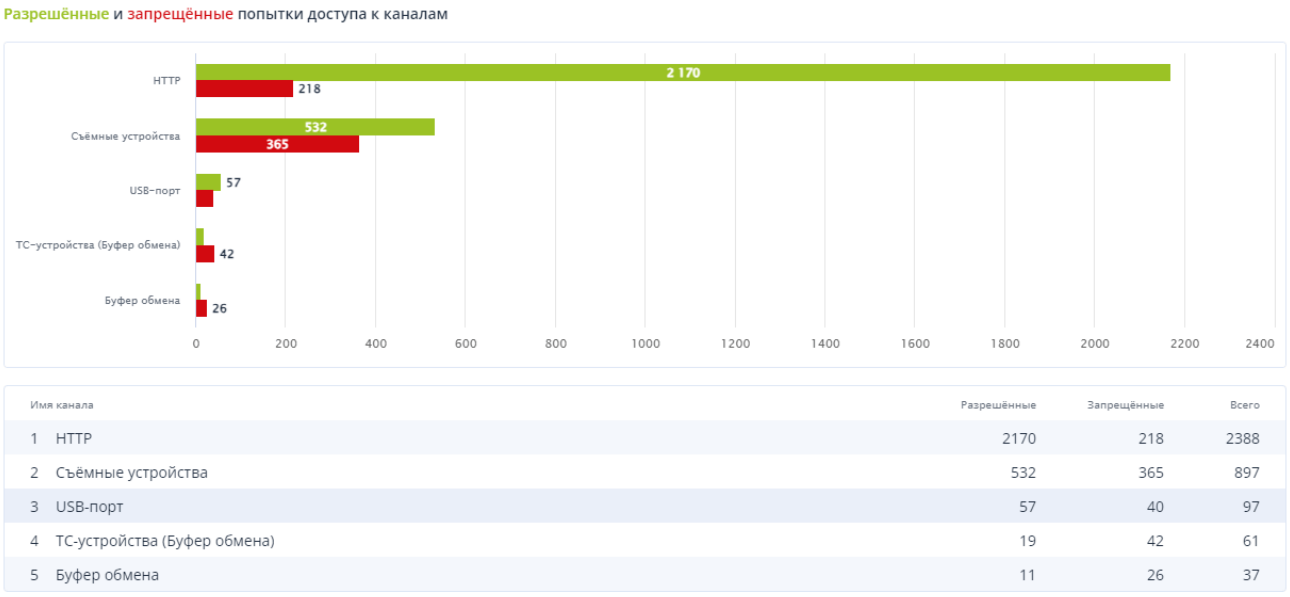
При создании задачи построения этого отчёта укажите следующие параметры:

- 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, 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, TrueConf, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.
- Интервал дат построения отчёта.




## Рейтинг используемых каналов

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

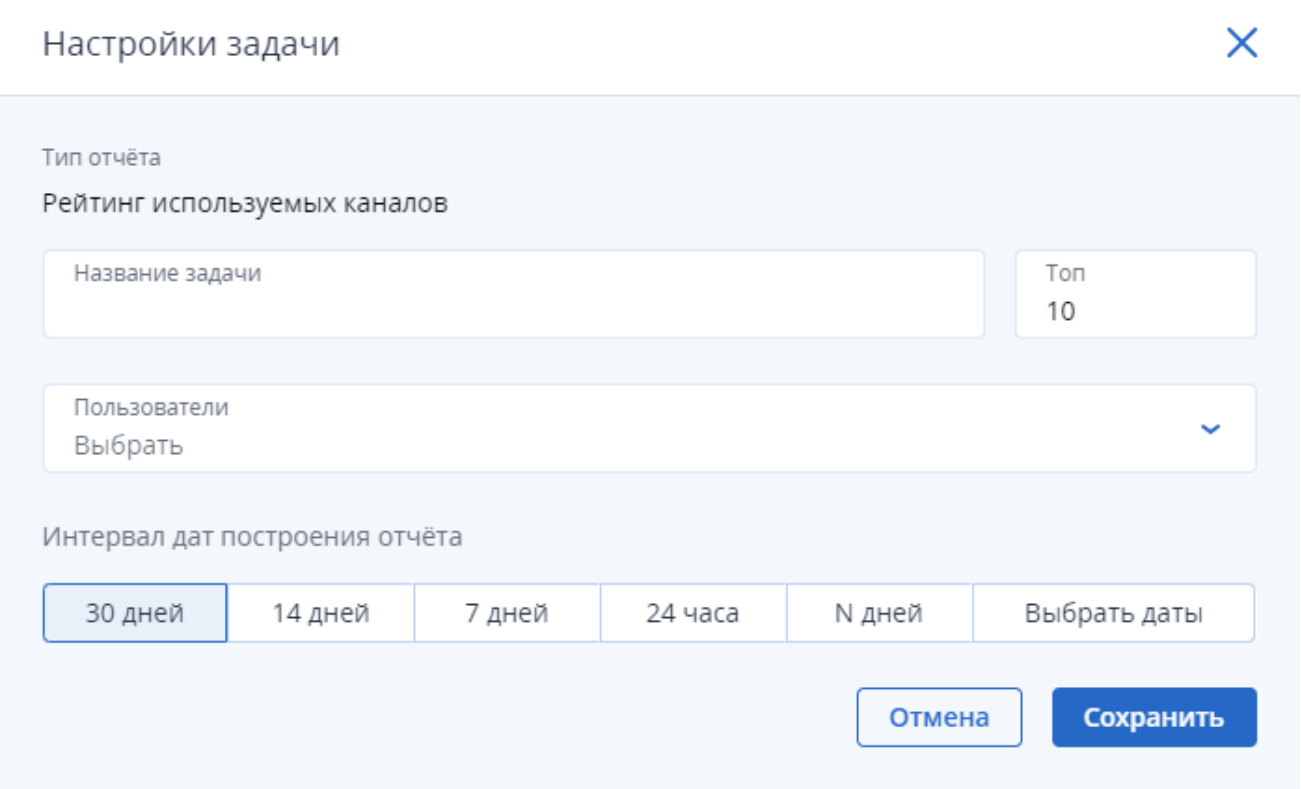



| Имя канала | Разрешённые | Запрещённые | Всего |
|---|---|---|---|
| 1 HTTP | 2170 | 218 | 2388 |
| 2 Съёмные устройства | 532 | 365 | 897 |
| 3 USB-порт | 57 | 40 | 97 |
| 4 TC-устройства (Буфер обмена) | 19 | 42 | 61 |
| 5 Буфер обмена | 11 | 26 | 37 |

При создании задачи построения этого отчёта укажите следующие параметры:

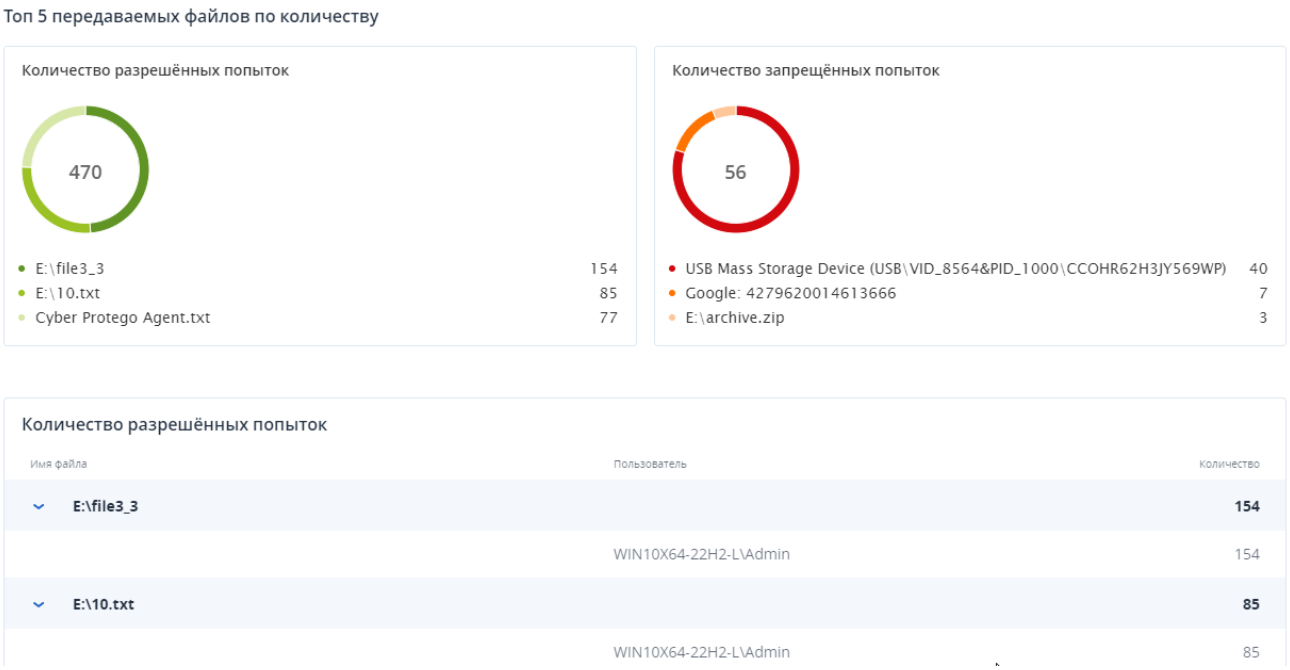
- Название задачи в соответствующем поле.

- В поле **Топ** — количество каналов, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** — сотрудников, использующих различные каналы.
- Интервал дат построения отчёта.



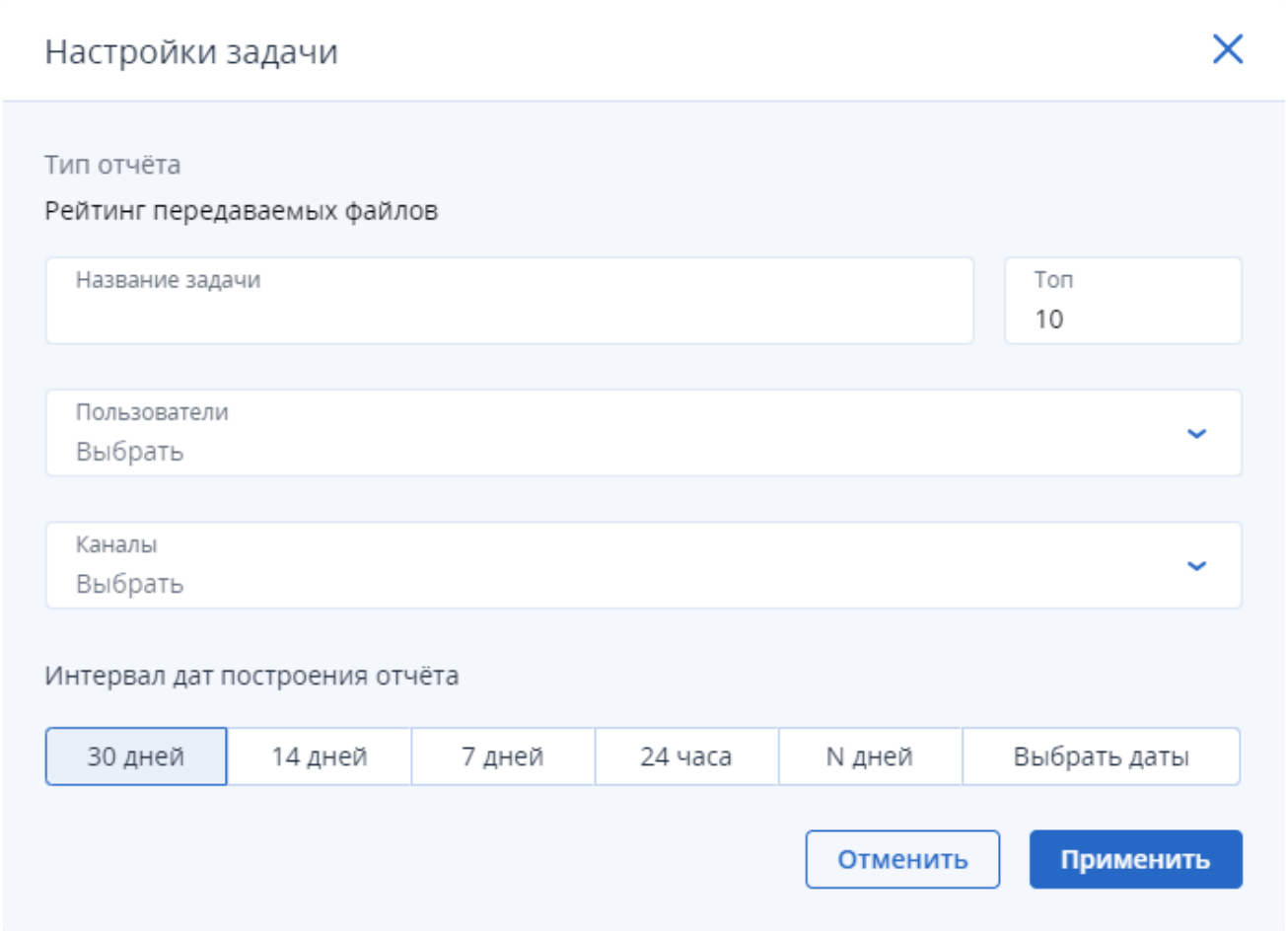

## Рейтинг передаваемых файлов

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



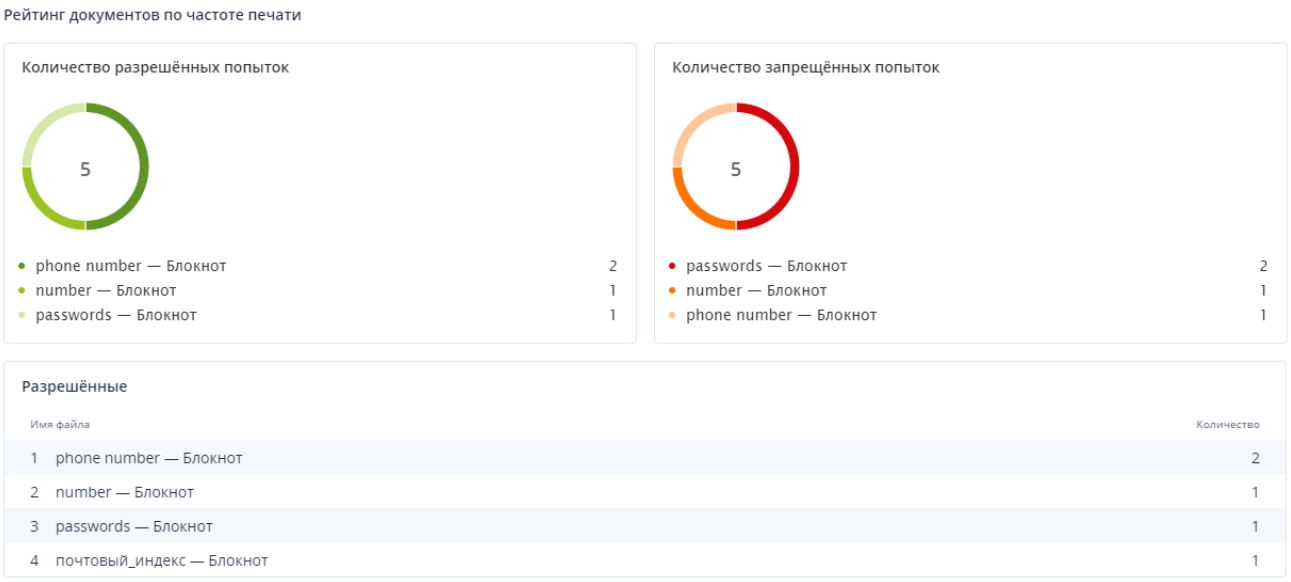

При создании задачи построения этого отчёта укажите следующие параметры:

- 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, TrueConf, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.
- Интервал дат построения отчёта.



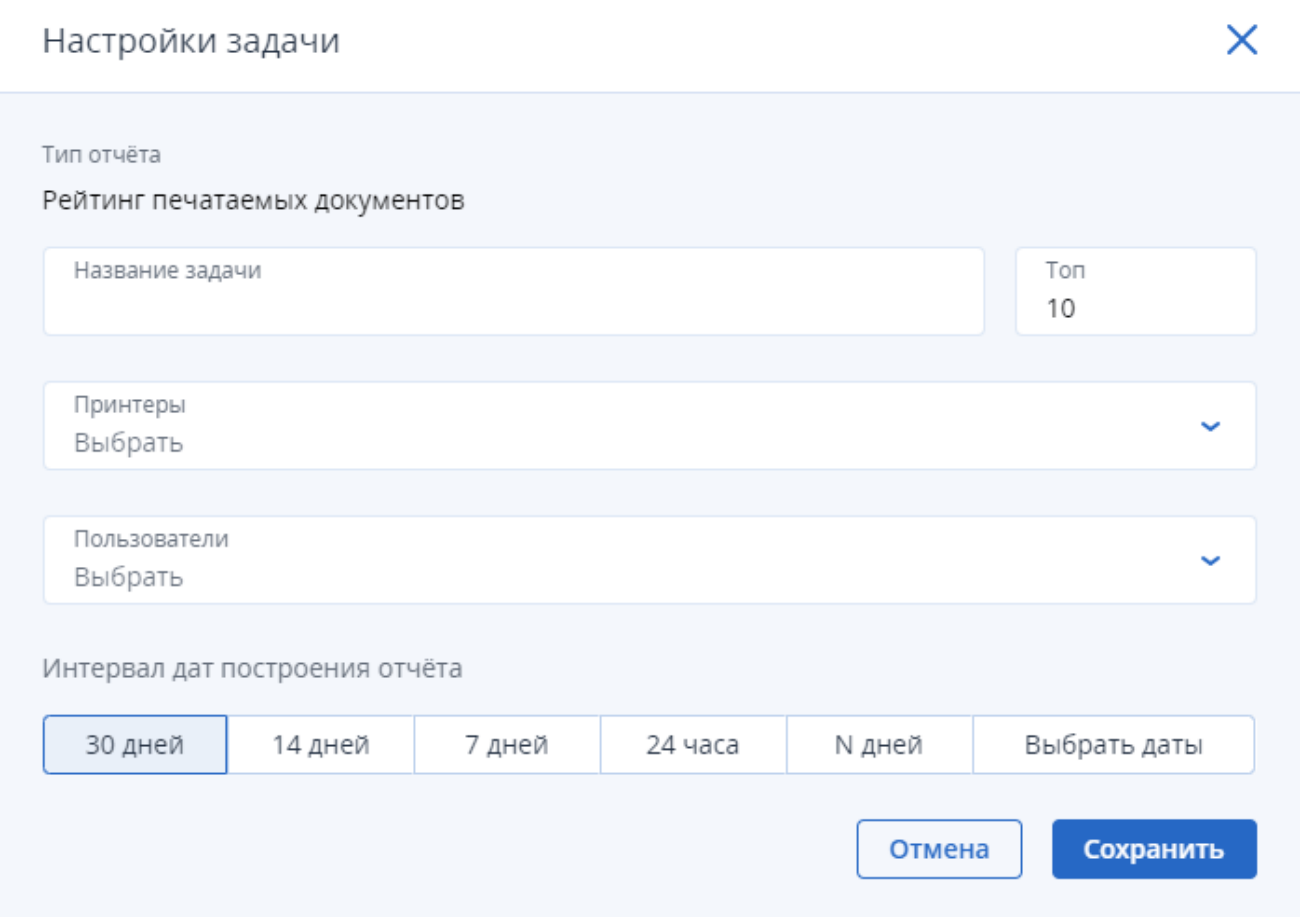

## Рейтинг печатаемых документов

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:

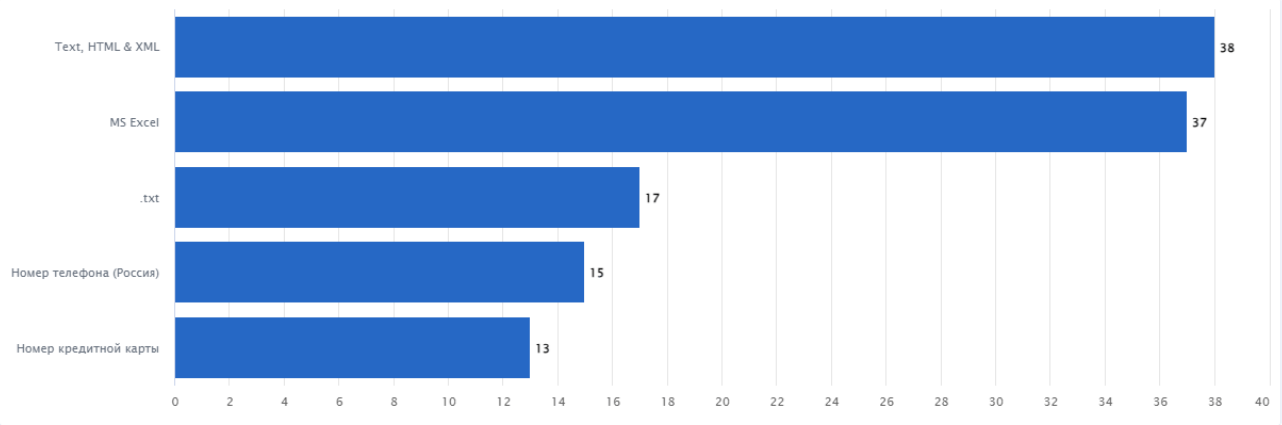
- Название задачи в соответствующем поле.
- В поле **Топ** — количество документов, отображаемое на диаграммах и в списках отчёта.
- В списке **Принтеры** — принтеры, используемые для печати.
- В списке **Пользователи** — пользователей, инициирующих печать.
- Интервал дат построения отчёта.




## Рейтинг применяемых правил

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

Применяемые правила

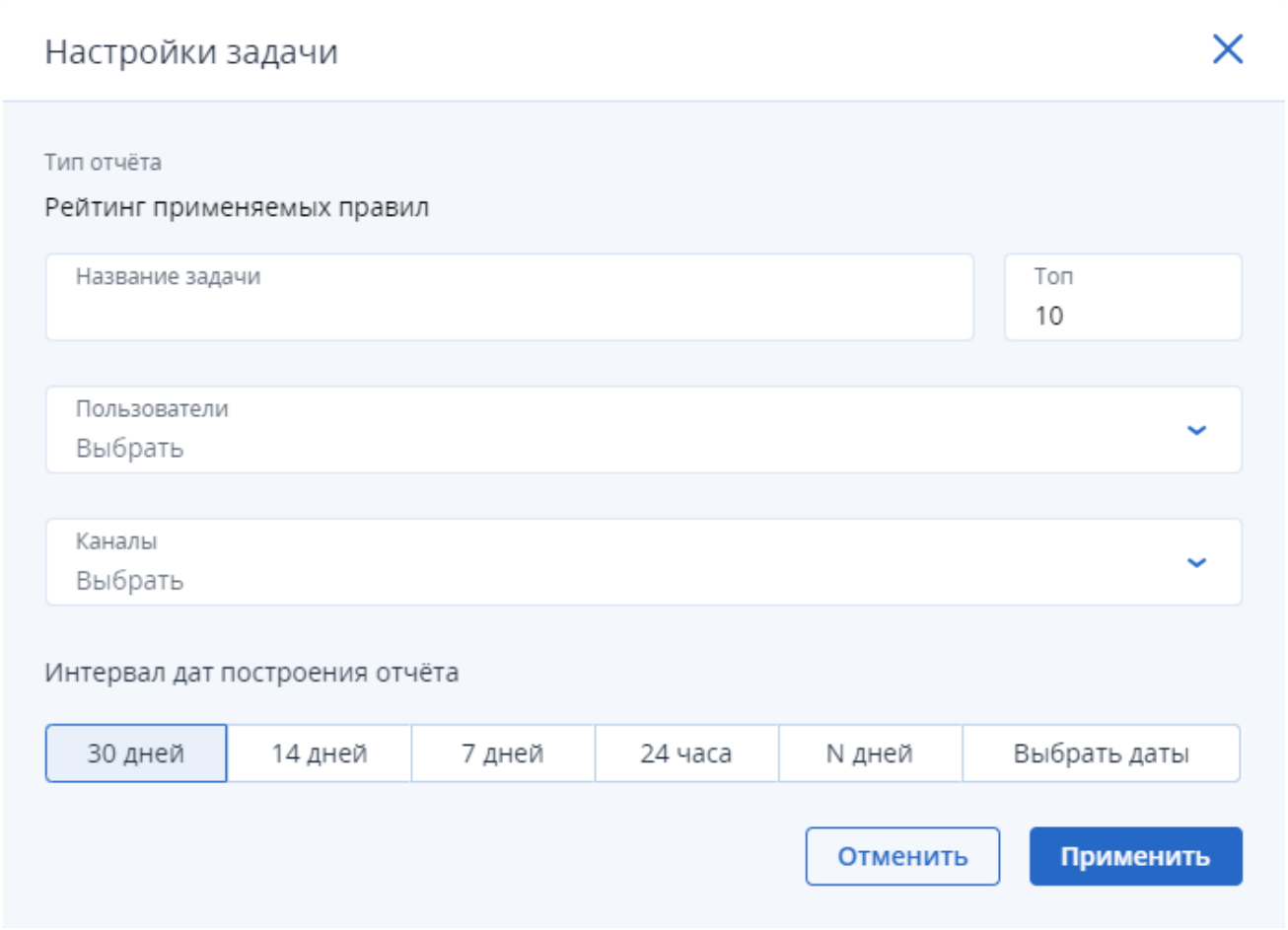



| Применяемое правило | | Частота применения |
|---|---|---|
| 1 | Text, HTML & XML | 38 |
| 2 | MS Excel | 37 |
| 3 | .txt | 17 |
| 4 | Номер телефона (Россия) | 15 |
| 5 | Номер кредитной карты | 13 |

Щёлкнув столбец на диаграмме или строку в таблице под диаграммой, можно перейти в журнал событий, отфильтрованный по указанному правилу с помощью временного фильтра. При необходимости такой фильтр можно сохранить как постоянный, нажав **Редактировать временный фильтр** и назначив ему имя.

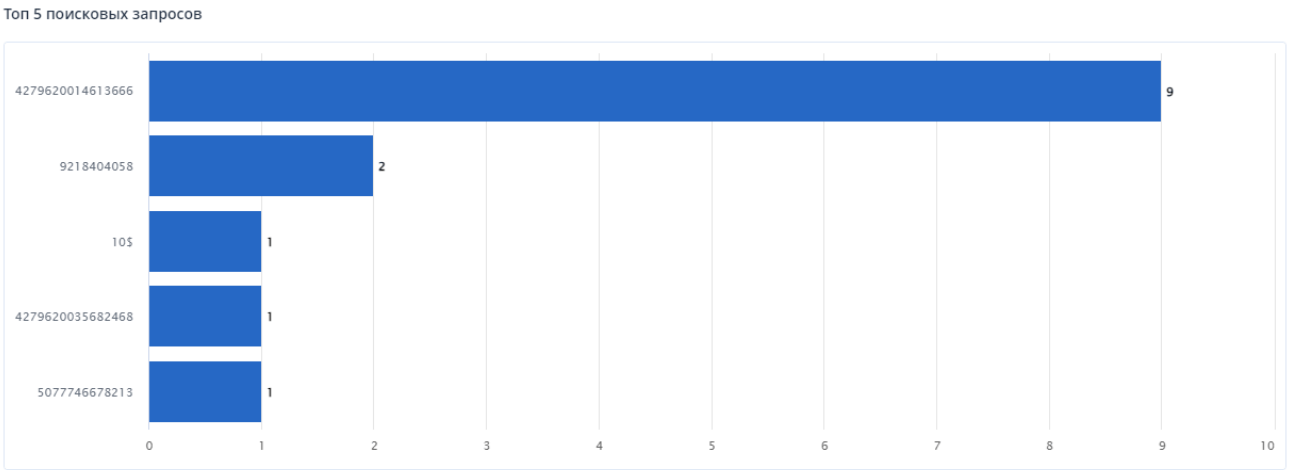
При создании задачи построения этого отчёта укажите следующие параметры:

- 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, 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, TrueConf, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.
- Интервал дат построения отчёта.




## Рейтинг поисковых запросов

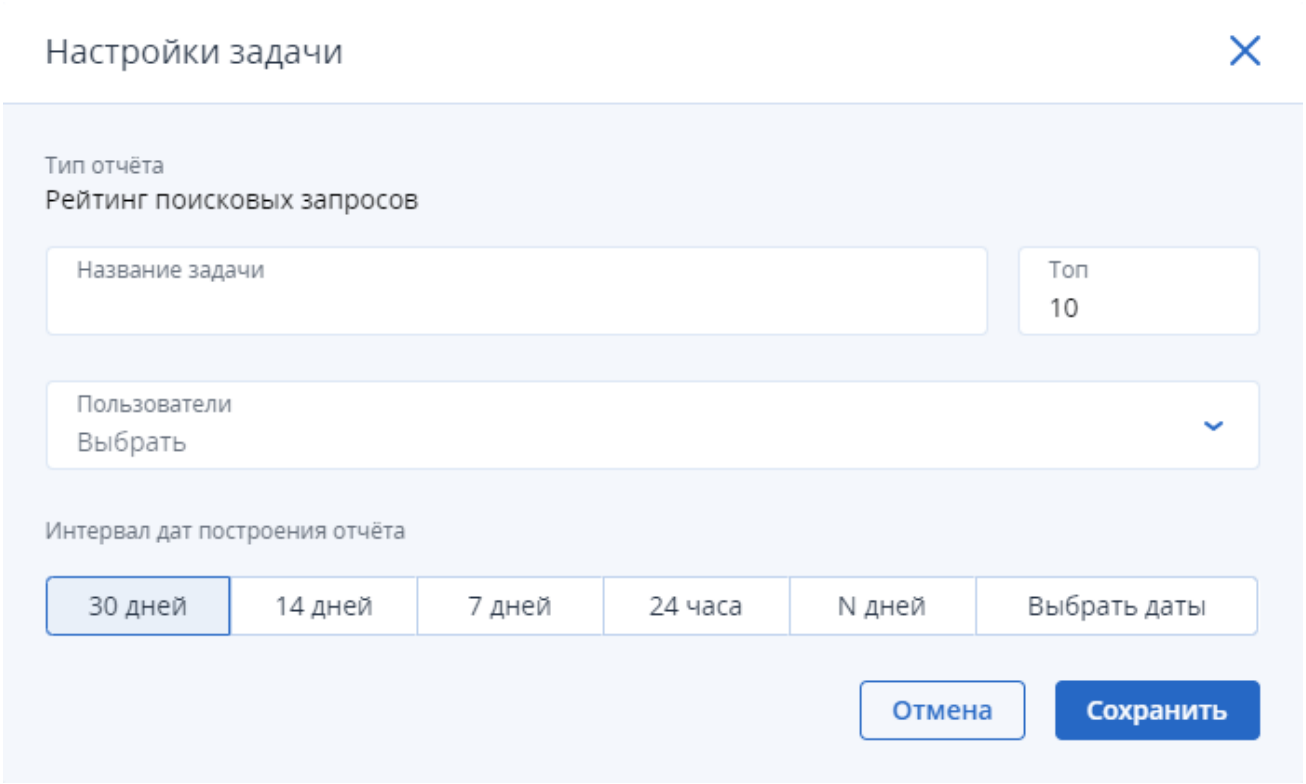
Этот отчёт показывает наиболее частые поисковые запросы, отсортированные по количеству.




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

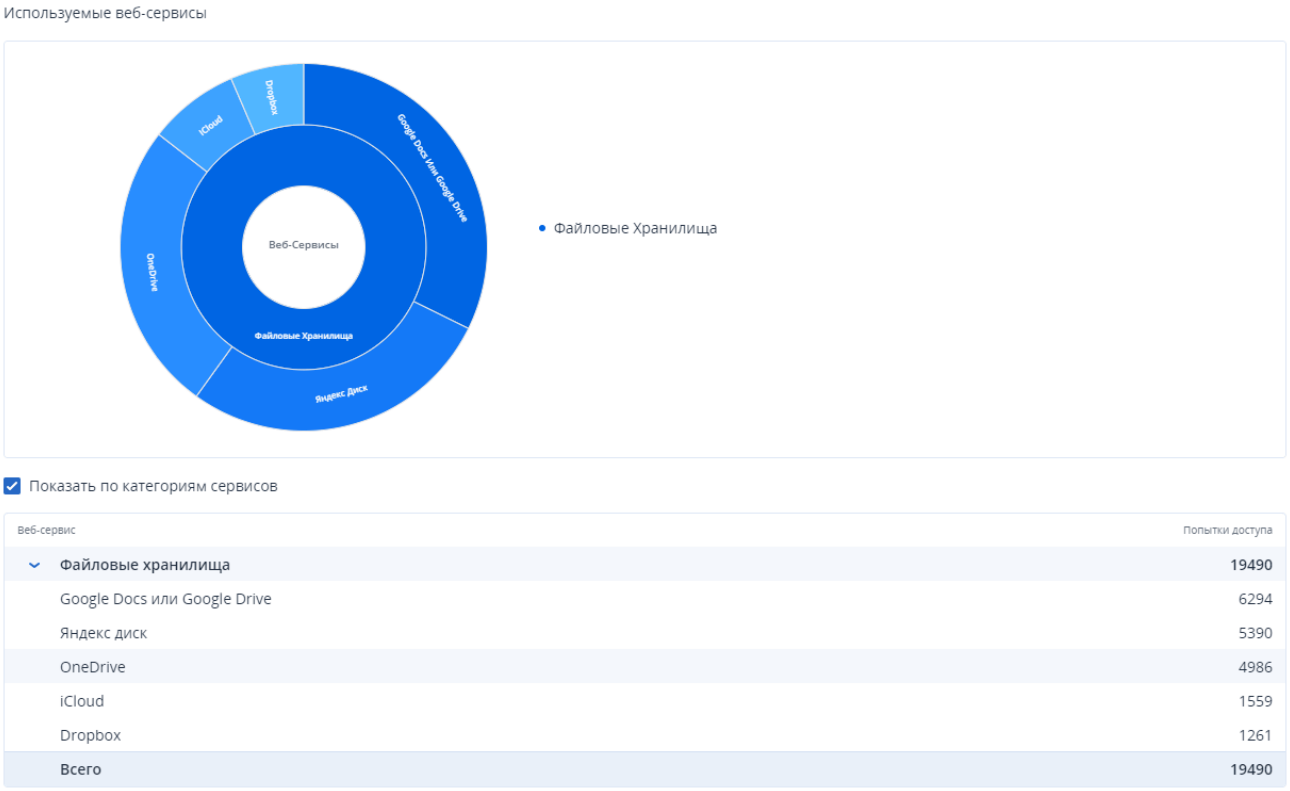
При создании задачи построения этого отчёта укажите следующие параметры:

- 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.




## Рейтинг используемых веб-сервисов

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




Щёлкнув сектор на диаграмме или строку в таблице под диаграммой, можно перейти в журнал событий, отфильтрованный по указанному веб-сервису с помощью временного фильтра. При необходимости такой фильтр можно сохранить как постоянный, нажав **Редактировать временный фильтр** и назначив ему имя.

При создании задачи построения этого отчёта укажите следующие параметры:

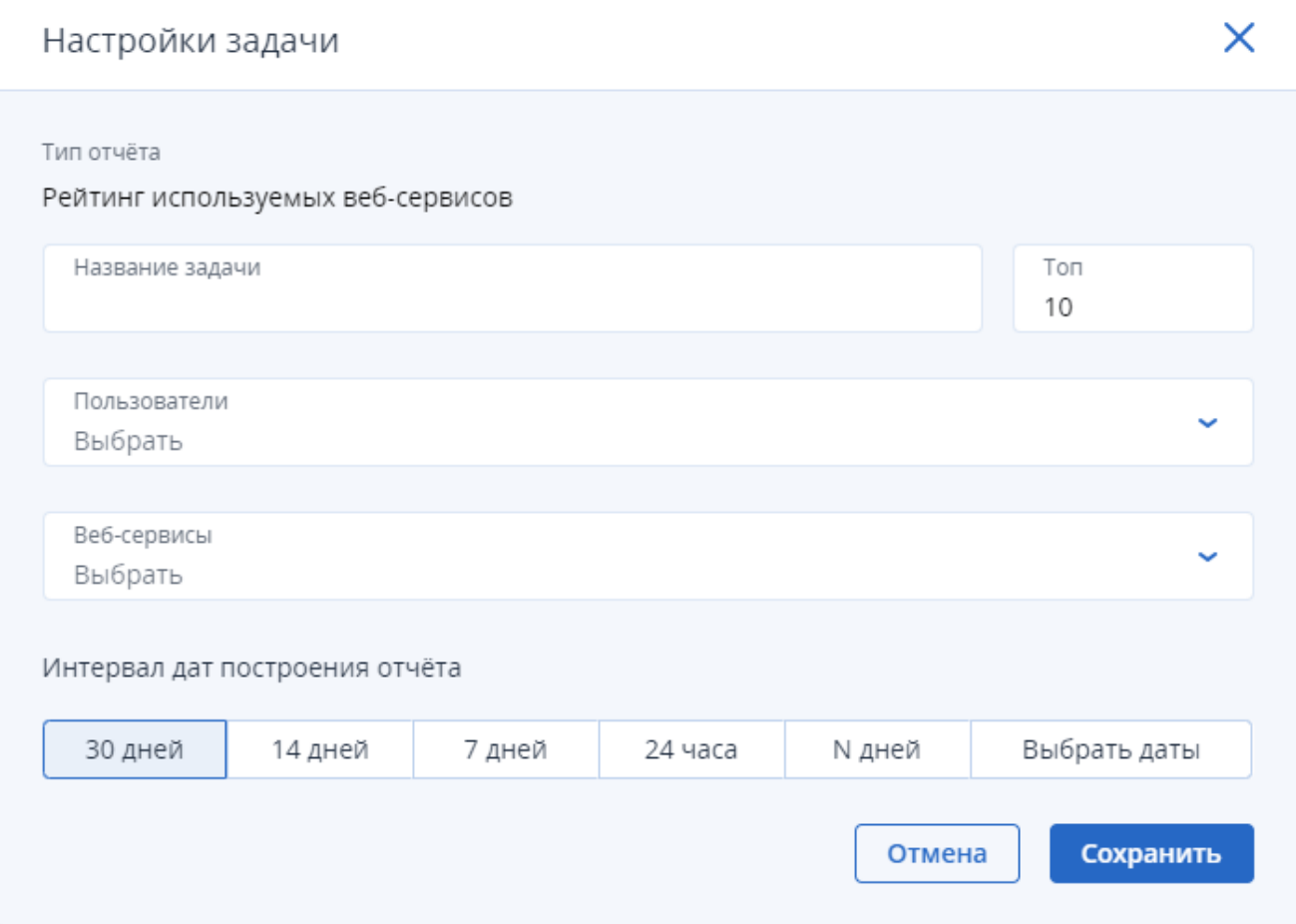
- Название задачи в соответствующем поле.
- В поле **Топ** — количество веб-сервисов, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** — пользователей, использующих веб-сервисы.
- В списке **Веб-сервисы** — типы файловых хранилищ, социальных сетей и почтовых сервисов. Отслеживаемые 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, VK WorkDisk.
  - Социальные сети: Disqus, Facebook[1], Google+, Instagram[1], LinkedIn, LiveInternet.ru, LiveJournal, MeinVZ.de, Myspace, Odnoklassniki.ru, Pinterest, StudiVZ.de, Tumblr, Twitter, Vkontakte,

[1] Деятельность социальных сетей Instagram и Facebook, принадлежащих компании Meta Platforms Inc., признана экстремистской и запрещена на территории России.

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, VK WorkMail, Zimbra.

- Интервал дат построения отчёта.

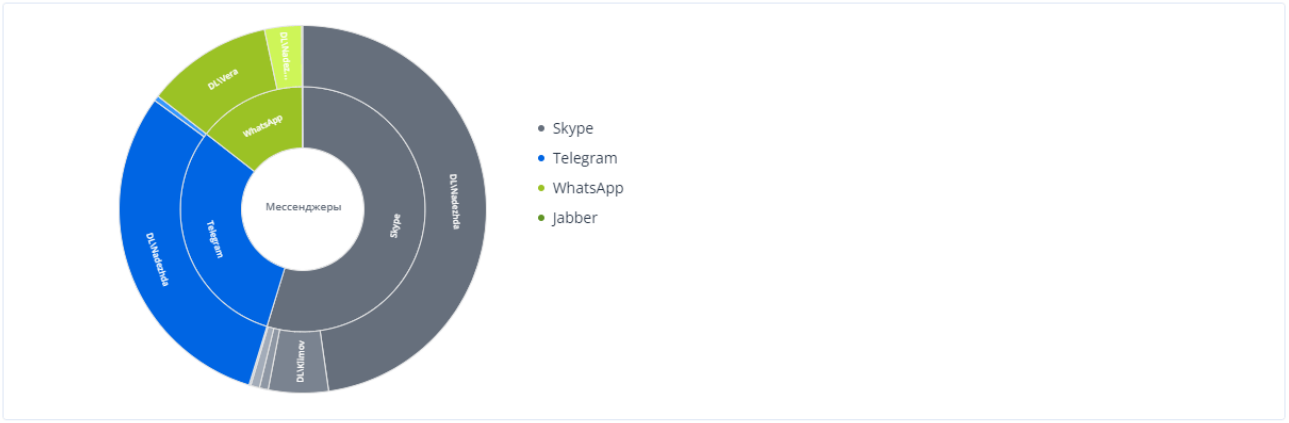



Нажимая на типы сервисов на круговой диаграмме отчёта, можно переключаться на диаграммы использования данного типа сервисов. Кроме того, можно группировать сервисы в списке по категориям.

## 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, TrueConf, Telegram, Viber, WhatsApp, Zoom.

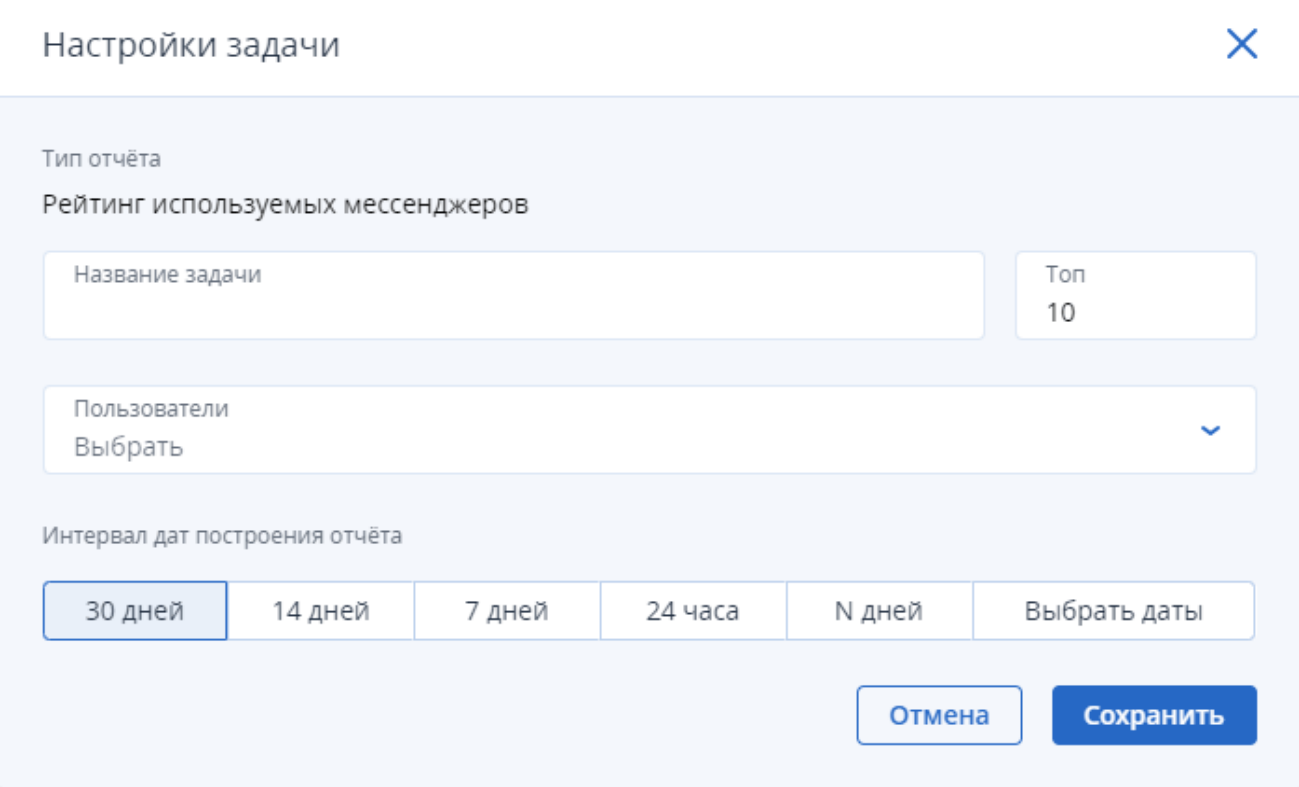
Топ используемых мессенджеров и пользователей в них




| Мессенджер | Пользователь | Попытки доступа |
|---|---|---|
| 1. Skype | | 1410 |
| | DL\nadezhda | 1230 |
| | DL\klimov | 136 |
| | DL\oleg.z | 20 |
| | DL\vera | 20 |
| | NT AUTHORITY\система | 4 |

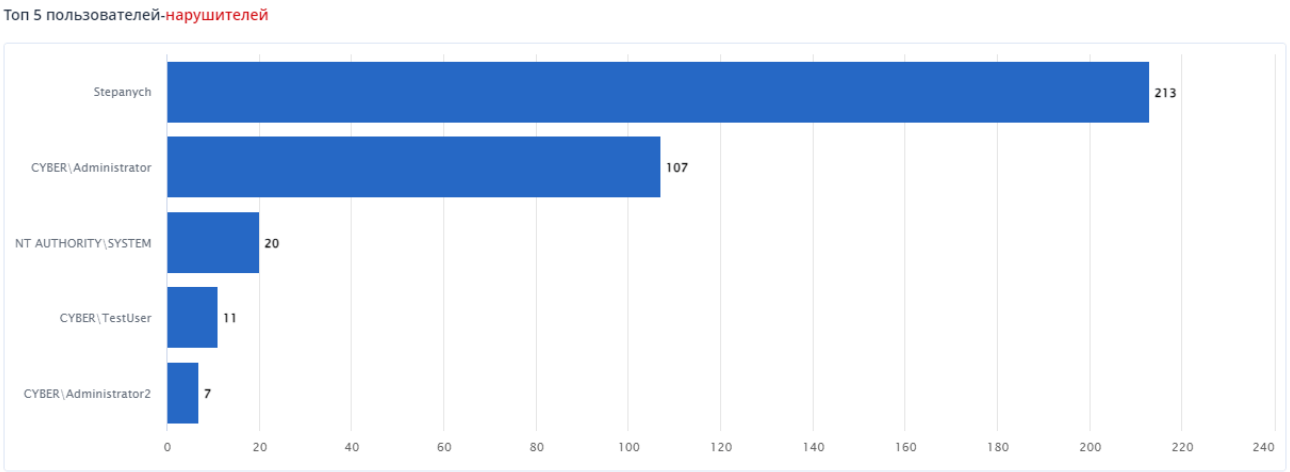
При создании задачи построения этого отчёта укажите следующие параметры:

- Название задачи в соответствующем поле.
- В поле **Топ** — количество мессенджеров, отображаемое на диаграммах и в списках отчёта.
- В списке **Пользователи** — сотрудников, которые использовали мессенджеры.
- Интервал дат построения отчёта.




## Рейтинг нарушителей

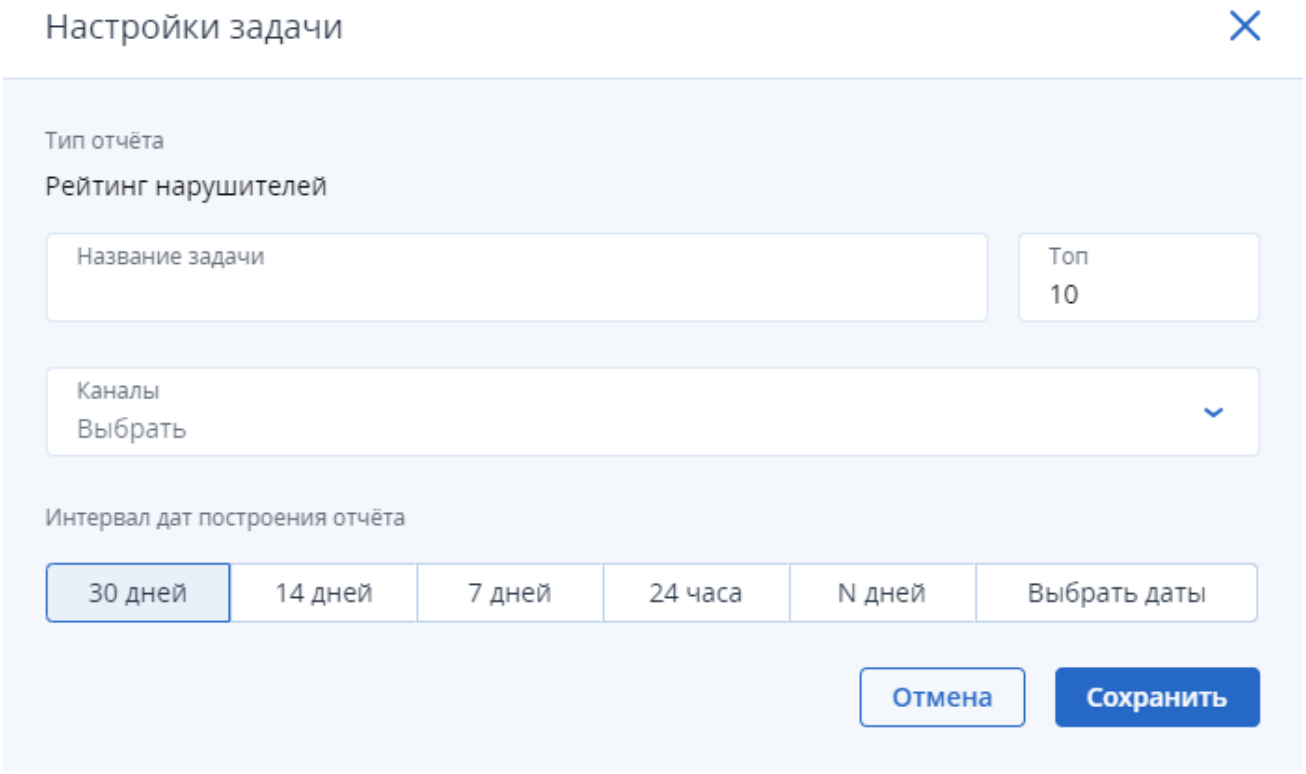
Этот отчёт показывает нарушителей, которым чаще всего был запрещен доступ, отсортированных по количеству запрещенных попыток доступа к устройствам и протоколам.




Щёлкнув столбец на диаграмме или строку в таблице под диаграммой, можно перейти в журнал событий, отфильтрованный по указанному пользователю с помощью временного фильтра. При необходимости такой фильтр можно сохранить как постоянный, нажав **Редактировать временный фильтр** и назначив ему имя.

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, TrueConf, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.
- Интервал дат построения отчёта.

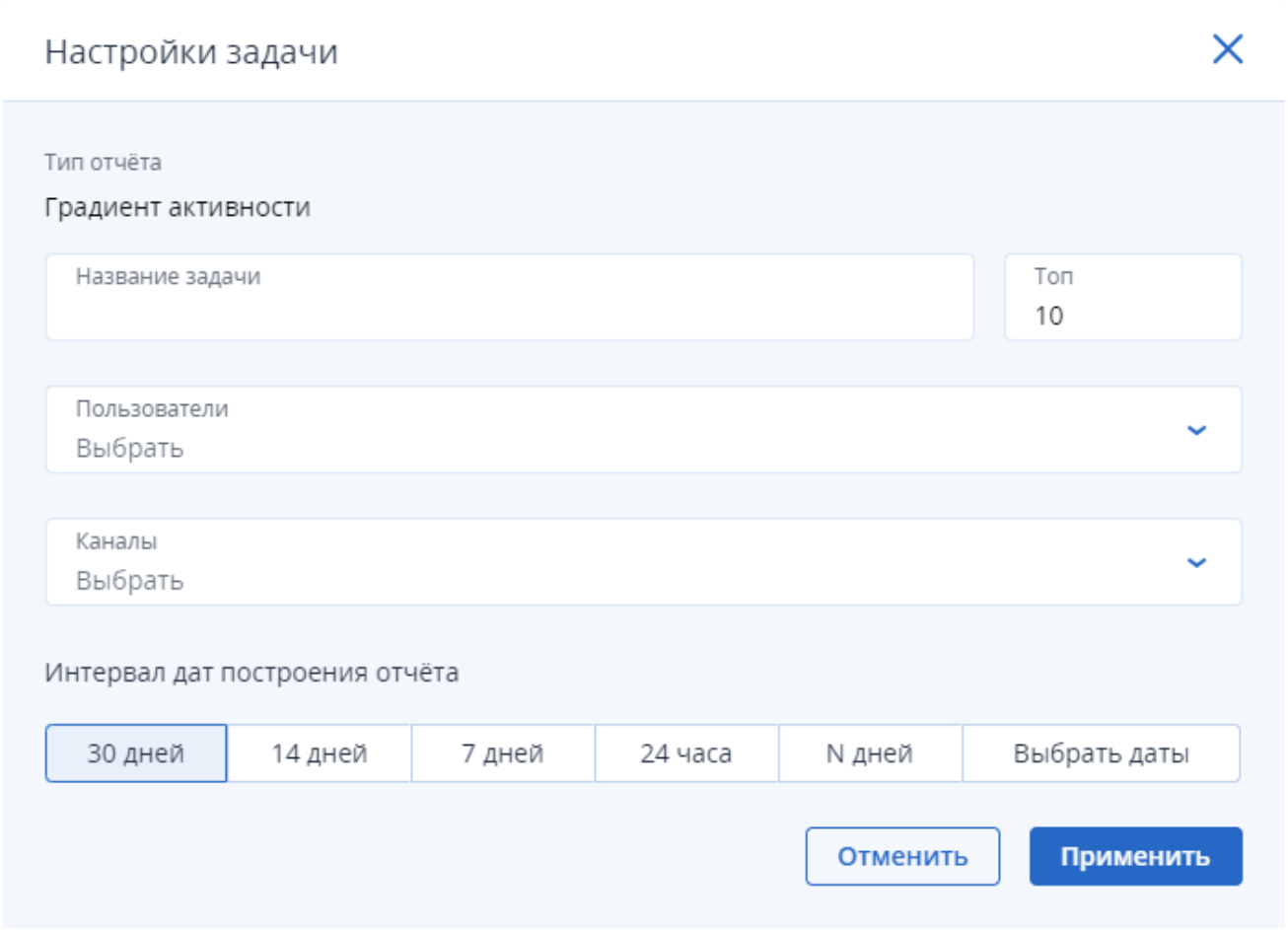



## Градиент активности

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, 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, TrueConf, Telegram, Telnet, торрент, Viber, Web-почта, Web-поиск, WhatsApp, Zoom.
- Интервал дат построения отчёта.




# Контроль рабочего времени

## Активность сотрудников

Этот отчёт показывает периоды активности сотрудников в рабочие и выходные дни, продолжительность рабочего дня, сведения о начале и окончании рабочего дня, используемые процессы (с детализацией), а также самых активных и неактивных сотрудников.

При создании задачи построения этого отчёта укажите следующие параметры:

- Название задачи в соответствующем поле.
- Папку в выпадающем списке **Выберите папку**.
- В списке **Пользователи** — сотрудников, по которым необходимо построить отчёт.
- Интервал дат построения отчёта.

## Топ процессов

Этот отчёт показывает наиболее используемые приложения (процессы) и время их использования.

При создании задачи построения этого отчёта укажите следующие параметры:

- Название задачи в соответствующем поле.
- Папку в выпадающем списке **Выберите папку**.
- В списке **Пользователи** — сотрудников, по которым необходимо построить отчёт.
- Интервал дат построения отчёта.

## Продолжительность рабочего времени

Этот отчёт показывает среднюю продолжительность рабочего дня, среднюю продолжительность рабочего времени за период и значения начала и окончания рабочего дня.

При создании задачи построения этого отчёта укажите следующие параметры:

- Название задачи в соответствующем поле.
- Папку в выпадающем списке **Выберите папку**.
- В списке **Пользователи** — сотрудников, по которым необходимо построить отчёт.
- Интервал дат построения отчёта.

# Граф связей

Графы связей позволяют исследовать сетевые коммуникации пользователей, представляя их в интерактивном графическом виде. Графы строятся на основе данных журнала событий.

Граф состоит из узлов и линий связей. Узлами представлены участники коммуникаций — объекты службы каталогов, такие как домен, подразделение (OU) или пользователь. Линиями обозначены связи или соединения между узлами. Толщина линии связи между узлами отражает общее число коммуникаций между ними. Чем толще линия, тем больше коммуникаций было между узлами.

При наведении указателя мыши на линию появляется всплывающее окно с информацией о связи между узлами, которые она соединяет. Информация включает следующие сведения: канал коммуникации, направление коммуникации (входящая/исходящая), общий объем переданных данных, размер переданных файлов, а также число коммуникаций на канал.

Графы являются иерархическими структурами. Узлы верхнего уровня обозначают домены организации. Все такие узлы выделены цветом. Щелчок на значке плюса (+) под узлом верхнего уровня раскрывает узлы уровнем ниже — пользователей данного домена. Все узлы нижнего уровня выделены тем же цветом, что и их родительский узел. Щелчок на значке плюса (+) под узлом уровня пользователя раскрывает информацию о его идентификаторах (адресах электронной почты, идентификаторах социальных сетей и сервисов мгновенных сообщений) и данные о соединениях с другими пользователями. Чтобы свернуть раскрытый узел, щёлкните на значке минуса (-).

При наведении указателя мыши на узел пользователя выводится всплывающее окно с информацией о данном пользователе. Эта информация включает имя пользователя в формате ”DOMAINUserName” (например, ”DLkatya”), имена используемых им компьютеров, а также его идентификаторы (адреса электронной почты, идентификаторы социальных сетей и сервисов мгновенных сообщений).

Пользователи в графах связей разделяются на внутренних и внешних. Внутренние пользователи находятся внутри корпоративной сети и являются участниками домена организации. Внешние пользователи находятся вне корпоративной сети и не являются участниками домена организации. Внешние пользователи определяются по адресам электронной почты или идентификаторам социальных сетей и сервисов мгновенных сообщений.

Графы связей доступны при использовании всех СУБД, поддерживаемых веб-консолью.

Управлять графами можно в разделе **ГРАФ СВЯЗЕЙ**:

- создавать, настраивать, запускать и удалять задачи построения графов, добавлять их в избранное, а также переносить между папками;
- создавать, переименовывать и удалять папки;

- фильтровать графы и папки по именам.

Чтобы создать задачу построения графа, нажмите **Добавить задачу** внизу экрана.

В появившемся окне укажите параметры графа:

- Папку в выпадающем списке **Выберите папку**.
- Название задачи в соответствующем поле.
- В списке **Пользователи** — внутренних пользователей, которых необходимо отобразить на графе или скрыть из него.
- В списке **Каналы** — типы протоколов, которые необходимо отобразить на графе или скрыть из него.
- В поле **Контакты** — идентификаторы пользователей (адреса электронной почты, идентификаторы социальных сетей и сервисов мгновенных сообщений), которые необходимо отобразить на графе.
- В поле **Исключение внешних контактов** — идентификаторы внешних пользователей, которые необходимо скрыть на графе.
- Интервал дат построения отчёта.

Указав параметры, сохраните изменения.

Будет создана и запущена задача построения графа. Время, необходимое для его построения, зависит от количества обрабатываемых данных. Статус задачи будет отображен в списке **История**.

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

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

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

Задачи построения графов 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 напротив её имени в списке или сверху справа, 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 напротив её имени в списке или сверху справа, и выберите **Переместить в папку**. В появившемся окне выберите папку и

нажмите **Переместить**.

Чтобы переименовать или удалить задачу, откройте контекстное меню, нажав многоточие напротив её имени в списке или сверху справа, и выберите соответствующее действие в списке.

# Досье пользователей

В разделе **Досье пользователей** можно отслеживать компьютерную активность пользователей с помощью удобного графического представления статистики их действий на компьютере.

Доступ к этому разделу имеют пользователи с правом просмотра списка пользователей в группах и досье пользователей, а также с правом изменения периода построения досье (см. *Права для досье пользователей*).

Досье строятся на основе данных из журнала событий, то есть только для пользователей, чья активность зафиксирована в этом журнале.

В досье учитывается информация за последние 2 месяца. При этом можно просматривать досье за более короткие временные интервалы:

- **Сегодня**,
- **Вчера**,
- **Эта календарная неделя**,
- **Прошлая календарная неделя**,
- **Последние 7 дней**,
- **Этот календарный месяц**,
- **Прошлый календарный месяц**,
- **Последние 30 дней**,
- **Последние 14 дней**.

Если в журнале событий есть данные об активности в сетевых каналах (например, отправка почты и общение в мессенджерах), то в досье также отображаются идентификаторы используемых сервисов, например, адреса электронной почты и имена учетных записей в мессенджерах (в графе связей такие идентификаторы называются контактами).

Информация о пользователе размещена на двух вкладках: **Общее** и **Статистика**.

На вкладке **Общее** отображается основная информация о пользователе:

- Учетная запись в формате `domain\user`.
- Группа (см. далее).
- Информация из службы каталогов (если настроена интеграция). Например, имя в формате ”Имя

Фамилия”, фотография (при наличии), корпоративный адрес электронной почты, название отдела, имя руководителя, доменные группы и пр.

- Индикатор лояльности (нормальности) — показатель того, насколько выбранный пользователь выделяется из остальных в группе. Например, если число совершенных им запрещённых действий выше среднего по группе, индикатор покажет низкую лояльность. Состояние этого индикатора также отображается в общем списке пользователей в виде смайла, что позволяет обнаруживать таких пользователей без просмотра сведений о каждом.
- История действий пользователя — количество разрешенных и запрещённых действий при использовании устройств и протоколов (а также средние показатели по группе) за выбранный интервал.
- Топ сработавших контентно-зависимых правил — аналог виджета **Применяемые контентные правила** и отчета **Рейтинг применяемых правил** с фильтром по выбранному пользователю.

На вкладке **Статистика** отображается краткая информация о пользователе и набор статистических данных:

- Краткая информация о пользователе (сокращенный аналог вкладки **Общее**):
  - Учетная запись;
  - Группа;
  - Некоторая информация из службы каталогов (если настроена интеграция), например, имя, фотография, корпоративный адрес электронной почты, номер телефона.
- Отчеты в формате графиков:
  - Попытки доступа к устройствам;
  - Попытки доступа к протоколам;
  - Топ разрешенных входящих файлов;
  - Топ запрещенных входящих файлов;
  - Топ разрешенных исходящих файлов;
  - Топ запрещенных исходящих файлов;
  - Топ разрешенных к печати файлов;
  - Топ запрещенных к печати файлов.

## Группы пользователей

Для расчета индикатора лояльности (нормальности) и вычисления его средних показателей пользователей необходимо объединять в группы.

По умолчанию есть неудаляемая и неизменяемая группа **Все**, в которую включаются все пользователи с досье. Данные пользователя, выбранного в этой группе, сравниваются со средними показателями по всем пользователям. Из группы **Все** пользователей удалять нельзя.

В дополнение можно создавать, переименовывать и расформировывать (удалять) другие группы. При этом одного и того же пользователя можно добавить сразу в несколько групп (или удалить из нескольких групп). Индикатор лояльности и средние показатели пользователя рассчитываются, исходя из того, в какой группе он выбран.

# Управление

В данном разделе можно создавать и распространять политики на агенты Cyber Protego для Linux, а также управлять списком компьютеров, контролируемых данными агентами.

## Политики

В данном разделе можно создавать и распространять политики на агенты Cyber Protego для Linux.

В каждой политике задаётся список настроек для агентов Cyber Protego, а также список компьютеров, для которых эта политика будет действовать. Одну и ту же политику можно применить к одиночным компьютерам, их динамическим группам (по информации из службы каталогов при настроенной интеграции), а также папкам (объединениям одиночных компьютеров и/или динамических групп). И, наоборот, к одному компьютеру можно применить ряд политик. При этом если к одному компьютеру применено множество политик, они объединяются в единую итоговую политику.

Значение настроек в итоговой политике зависит от приоритета используемых политик. Если в используемых политиках заданы разные значения для одних и тех же настроек, в итоговой политике будут применены настройки более приоритетной политики. Приоритет политик указывается числом. Чем оно больше, тем выше приоритет.

Политику по умолчанию нельзя переименовать, остановить или удалить. Кроме того, нельзя изменить её приоритет (”0” — низший).

### Создание политик

При создании новой политики необходимо указать:

- Имя.
- Приоритет. Можно выбрать минимальный (”1” — выше приоритета политики по умолчанию) или высший. Впоследствии приоритет можно изменить, нажав кнопку **Управлять приоритетами** на основном экране раздела.
- Состояние после создания — с помощью флажка **Активировать политику сейчас**.

Также можно задать необязательное описание.

#### Редактирование политик

Чтобы начать редактирование политики, щёлкните по ней в списке.

При редактировании политики доступны следующие разделы: **Общие сведения о политике** и **Настройки политики**.

В разделе **Общие сведения о политике** указывается список компьютеров, на которые она распространяется, их число. В этом разделе над политикой можно выполнить следующие действия:

- изменить имя и описание,
- запустить и остановить,
- клонировать,
- сбросить настройки в исходное состояние,
- удалить.

В разделе **Настройки политики** указываются настройки, которые будут применены к агентам Cyber Protego на контролируемых компьютерах.

При этом в веб-консоли доступны следующие профили:

- **При нахождении во внутренней сети** — соответствует основному профилю центральной консоли управления.
- **Вне внутренней сети** — соответствует офлайн-профилю центральной консоли управления.

# Управление агентами для ОС Linux

В данном разделе описаны настройки политик, доступные для агентов Cyber Protego для ОС Linux.

## Настройки агента

#### Конфигурация

На этом экране можно задать следующие параметры:

- **Серверы управления** — имя хоста или IP-адрес сервера управления, на который агенты Cyber Protego будут отправлять данные своих журналов.
- **Способ определения нахождения во внутренней сети** — настройки автономного режима. Эти параметры описаны в руководстве пользователя классического сервера управления.
- **Отображать значок в системной области** — отображать в системной области значок, щёлкнув который можно узнать версию агента и просмотреть историю уведомлений или сообщений.

Если значок выключен, но включены уведомления или сообщения, они все равно будут отображаться.

### Аудит и теневое копирование

На этом экране можно задать следующие параметры:

- **Локальная квота** — предельный размер дискового пространства, которое агент сможет использовать для локального хранения данных теневого копирования до их передачи на сервер управления (по умолчанию 100 ГБ, минимум 10 ГБ). Необходимо также указать действия агента в случае превышения квоты:
  - **Разрешить передачу данных, записывать новые события вместо старых** (выбран по умолчанию) — агент не будет блокировать каналы передачи данных (пользовательские настройки продолжат работать), но ранее полученные теневые копии будут автоматически заменяться новыми, начиная с самых старых.
  - **Разрешить передачу данных, не записывать новые события вместо старых** — агент не будет блокировать каналы передачи данных (пользовательские настройки продолжат работать) и не будет создавать новые теневые копии. Ранее полученные теневые копии будут храниться до их передачи на сервер управления, или пока администратор не удалит их вручную из директории агента.
  - **Запретить передачу данных** — агент будет блокировать каналы передачи данных (временно переопределять пользовательские настройки) и не будет создавать новые теневые копии. Ранее полученные теневые копии будут храниться до их передачи на сервер управления, или пока администратор не удалит их вручную из директории агента. Блокировка продлится до тех пор, пока не появится свободное место для новых теневых копий.
- **Записывать события об изменении политики** — включить протоколирование изменений в настройках агента.

### Алерты

На этом экране можно задать следующие параметры:

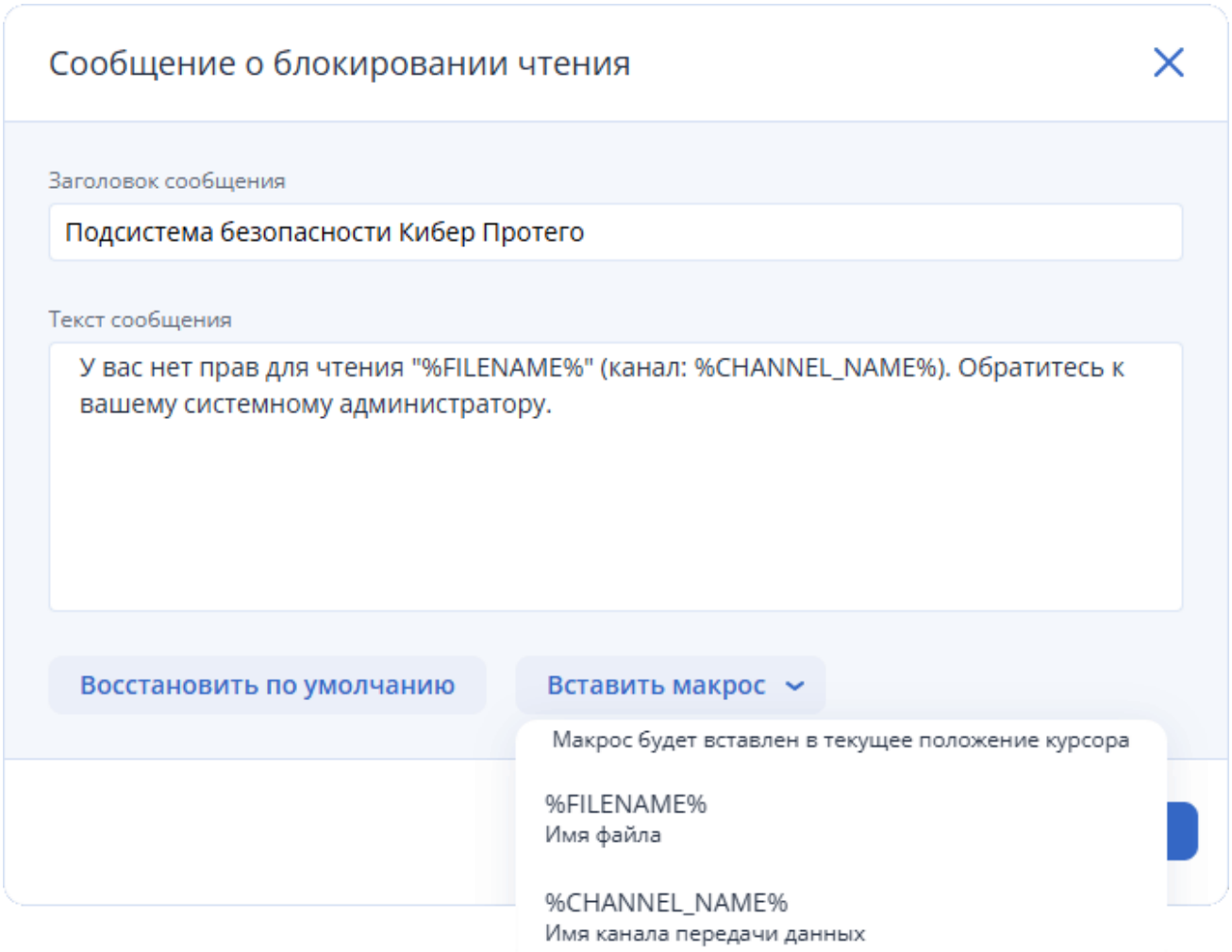
- **Настройки отправки алертов**:
  - SMTP (описание параметров см. в руководстве пользователя классического сервера управления).
  - Syslog (описание параметров см. в руководстве пользователя классического сервера управления). Не поддерживается параметр **Порог**. Алерты, отправляемые по данному каналу, не объединяются.

- **События для отправки административных алертов**:
  - **Изменение политик агента** — см. описание алерта **Оповещать при изменении политик агента** в руководстве пользователя классического сервера управления.
  - **Превышение локальной квоты** — см. описание алерта **Оповещать при превышении локальной квоты** в руководстве пользователя классического сервера управления.
  - **Изменение настроек алертов** — см. описание алерта **Оповещать при изменении настроек алертов** в руководстве пользователя классического сервера управления.
  - **Возникновение ошибок агента** — информирует об ошибках, которые могут возникнуть в агенте для Linux и повлиять на его поведение (например, ошибка инициализации драйвера).

### Сообщения

На этом экране можно задать сообщения, отправляемые пользователям при попытках совершить действия, запрещённые текущей политикой.

Чтобы задать сообщение, щёлкните **Задано** для выбранного типа сообщения. Появится окно, в котором можно будет задать заголовок и текст сообщения. Например:




В сообщениях можно использовать макросы, доступные в выпадающем списке **Вставить макрос**:

Можно задать следующие основные типы сообщений:

- О блокировании чтения (аналогичная настройка агентов для Windows).

  Доступные макросы:

  - %FILENAME% — имя файла. В ряде случаев подставленное имя файла может содержать в себе также и путь к нему.
  - %CHANNEL_NAME% — название канала передачи данных.

- О блокировании записи (аналогичная настройка агентов для Windows).

  Доступные макросы:

  - %FILENAME% — имя файла. В ряде случаев подставленное имя файла может содержать в себе также и путь к нему.
  - %CHANNEL_NAME% — название канала передачи данных.

- О блокировании USB-устройства (аналогичная настройка агентов для Windows).

  Доступные макросы:

  - %DEVICE% — имя устройства (полученное от операционной системы).
  - %CHANNEL_NAME% — название канала передачи данных.

Можно задать следующие контентно-зависимые типы сообщений:

- О блокировании чтения (аналогичная настройка агентов для Windows).

  Доступные макросы:

  - %FILENAME% — имя файла. В ряде случаев подставленное имя файла может содержать в себе также и путь к нему.
  - %CHANNEL_NAME% — название канала передачи данных.
  - %REASON% — причина блокирования доступа. Подставляется название сработавшего контентного правила и сопутствующая информация.
- О блокировании записи (аналогичная настройка агентов для Windows).

  Доступные макросы:

  - %FILENAME% — имя файла. В ряде случаев подставленное имя файла может содержать в себе также и путь к нему.
  - %CHANNEL_NAME% — название канала передачи данных.
  - %REASON% — причина блокирования доступа. Подставляется название сработавшего контентного правила и сопутствующая информация.

## Устройства

### Права доступа

На этом экране можно задать права доступа к поддерживаемым типам устройств:

- съёмные устройства,
- USB-устройства,
- принтеры,
- ТС-устройства (буфер обмена по протоколу Microsoft Remote Desktop Protocol (RDP) при использовании сервера Xrdp; подключённые диски (локальные, сетевые, съёмные); перенаправленные USB-устройства при использовании технологии USB over IP).

> **Примечание**
>
> Контроль ТС-устройств доступен только в ОС Astra Linux.

Основные права доступа описаны в руководстве пользователя классического сервера управления. Нажав **Другое**, можно уточнить права доступа разных пользователей к выбранному типу устройств.

Для съёмных устройств и USB-устройств можно задать разрешения на чтение и запись.

Для принтеров можно задать разрешения на печать.

Для ТС-устройств можно задать следующие разрешения:

- **Чтение с подключённого диска** — Разрешает чтение данных с подключённых дисков в терминальной сессии.
- **Запись на подключённый диск** — Разрешает запись данных на подключённые диски в терминальной сессии, а также переименование и удаление данных.
- **Доступ к USB-устройствам** — Разрешает взаимодействие с перенаправленными в терминальную сессию USB-устройствами.
- **Буфер обмена — входящий текст** — Разрешает вставку текстовых данных из буфера обмена в окно терминальной сессии.
- **Буфер обмена — исходящий текст** — Разрешает вставку текстовых данных из буфера обмена окна терминальной сессии.
- **Буфер обмена — входящие файлы** — Разрешает вставку файлов из буфера обмена в окно терминальной сессии.
- **Буфер обмена — исходящие файлы** — Разрешает вставку файлов из буфера обмена окна терминальной сессии.

> **Примечание**
>
> Не поддерживается контроль по времени.

### Аудит, теневое копирование и алерты

На этом экране можно задать правила аудита и теневого копирования, а также включить алерты для поддерживаемых типов устройств:

- съёмные устройства,
- USB-устройства,

- принтеры,
- ТС-устройства (буфер обмена по протоколу Microsoft Remote Desktop Protocol (RDP) при использовании сервера Xrdp; подключённые диски (локальные, сетевые, съёмные); перенаправленные USB-устройства при использовании технологии USB over IP).

> **Примечание**
>
> Контроль ТС-устройств доступен только в ОС Astra Linux.

Основные параметры описаны в руководстве пользователя классического сервера управления: аудит, теневое копирование, алерты. Нажав **Задано**, можно уточнить правила для разных пользователей и выбранного типа устройств.

Для съёмных устройств можно задать следующие правила:

- Аудит: чтение, запись
- Теневое копирование: запись
- Алерты: чтение, запись

Для USB-устройств можно задать следующие правила:

- Аудит: чтение, запись
- Алерты: чтение, запись

Для принтеров можно задать следующие правила:

- Аудит: печать
- Теневое копирование: печать
- Алерты: печать

Для ТС-устройств можно задать следующие правила:

- Аудит:
  - **Буфер обмена — входящие данные** — Протоколирование всех попыток вставки различных типов данных (текстовых и файлов) из буфера обмена в окно терминальной сессии.
  - **Буфер обмена — исходящие данные** — Протоколирование всех попыток вставки различных типов данных (текстовых и файлов) из буфера обмена окна терминальной сессии.
  - **Чтение с подключённого диска** — Протоколирование всех попыток чтения данных с подключённых дисков в терминальной сессии.

    - **Запись на подключённый диск** — Протоколирование всех попыток записи данных на подключённые диски в терминальной сессии, а также всех попыток переименования и удаления данных.
    - **Доступ к USB-устройствам** — Протоколирование всех попыток взаимодействия с перенаправленными в терминальную сессию USB-устройствами.
- Теневое копирование:
    - **Буфер обмена — входящие данные** — Включается теневое копирование различных типов данных (текстовых и файлов), скопированных из буфера обмена в окно терминальной сессии.
    - **Буфер обмена — исходящие данные** — Включается теневое копирование различных типов данных (текстовых и файлов), скопированных в буфер обмена из окна терминальной сессии.
    - **Чтение с подключённого диска** — Теневое копирование всех данных, читаемых с подключённых дисков в терминальной сессии.
    - **Запись на подключённый диск** — Теневое копирование всех данных, записываемых на подключённые диски в терминальной сессии.
- Алерты:
    - **Буфер обмена — входящие данные** — Отправка тревожных оповещений обо всех попытках вставки различных типов данных (текстовых и файлов) из буфера обмена в окно терминальной сессии.
    - **Буфер обмена — исходящие данные** — Отправка тревожных оповещений обо всех попытках вставки различных типов данных (текстовых и файлов) из буфера обмена окна терминальной сессии.
    - **Чтение с подключённого диска** — Отправка тревожных оповещений о всех попытках чтения данных с подключённых дисков в терминальной сессии.
    - **Запись на подключённый диск** — Отправка тревожных оповещений о всех попытках записи данных на подключённые диски в терминальной сессии, а также о всех попытках переименования и удаления данных.
    - **Доступ к USB-устройствам** — Отправка тревожных оповещений о всех попытках взаимодействия с перенаправленными в терминальную сессию USB-устройствами.

**Примечание**

Не поддерживается контроль по времени.

### Белый список USB-устройств

Реализация белого списка USB-устройств в агенте для Linux совпадает с его реализацией в агенте для Windows (см. руководство пользователя классического сервера управления) за исключением следующих особенностей:

- Данные настройки распространяются на обычные USB-устройства, а также USB-устройства, перенаправленные в терминальную сессию.
- Поддерживается только параметр **Контролировать как тип** (см. руководство пользователя классического сервера управления). При этом выбранный вариант **Полный доступ** соответствует снятому флажку **Контролировать как тип** в агенте для Windows.

### Белый список принтеров

На этом экране можно задать список принтеров, для которых будет отключен контроль доступа, аудит и теневое копирование на уровне класса устройств ”принтер”.

Если принтер одновременно является USB-устройством, для него по-прежнему будет выполняться проверка разрешений на уровне USB-устройств (см. схему в руководстве пользователя классического сервера управления). Отключить контроль USB-принтера на уровне USB-устройств можно в белом списке USB-устройств.

Если аудит и теневое копирование включены на уровне ”принтер”, при печати на принтеры из белого списка в журнале аудита рядом с именами принтеров будет указано, что они не контролируются. Кроме того, при печати на такие принтеры не будут создаваться теневые копии.

### Контентные правила

На данном экране можно создавать контентные правила (контентно-зависимые правила в классическом сервере управления). Для агента для Linux есть следующие ограничения:

- Поддерживаются следующие виды триггеров (контентных групп в классическом сервере управления):
  - **Регулярное выражение** (см. Группы шаблонов в руководстве пользователя классического сервера управления).
  - **Свойства документа** (см. Свойства документа в руководстве пользователя классического сервера управления).
  - **Составной** (см. Составные группы в руководстве пользователя классического сервера управления).
- Для триггеров типа **регулярное выражение** поддерживаются только следующие параметры: **Имя**,

**Описание**, **Регулярное выражение**, **Условие**, **Учитывать регистр**, **Считать идентичные совпадения за одно**.

- Для триггеров типа **свойства документа** поддерживаются только следующие параметры: **Имя**, **Описание**, **Размер (включая элементы выпадающего списка и соответствующие текстовые поля)**.
- Для триггеров типа **составной** поддерживается весь функционал. В их состав могут входить другие поддерживаемые триггеры, включая составные.
- Контентные правила могут быть применены только к типу устройств **ТС-устройства** (только буфер обмена по протоколу Microsoft Remote Desktop Protocol (RDP) при использовании сервера Xrdp).

> **Примечание**
>
> Контроль ТС-устройств доступен только в ОС Astra Linux.

  - **Буфер обмена — входящий текст** — Разрешает вставку текстовых данных из буфера обмена в окно терминальной сессии.
  - **Буфер обмена — исходящий текст** — Разрешает вставку текстовых данных из буфера обмена окна терминальной сессии.

#### Дополнительные настройки

На этом экране можно задать параметры ограничения доступа, дополняющие настройки на экране **Права доступа**:

- **Управление доступом к типам устройств при запрете доступа к портам USB** — контроль и протоколирование доступа к выбранным типам устройств (см. руководство пользователя классического сервера управления).
- **Другое** — контроль и протоколирование доступа к выбранным типам устройств (см. руководство пользователя классического сервера управления).

Данные настройки распространяются на обычные USB-устройства, а также USB-устройства, перенаправленные в терминальную сессию.

## Мониторинг активности пользователей

Для ОС Astra Linux Cyber Protego предоставляет возможность мониторинга действий пользователей с помощью видеозаписи экранов, записи нажатий клавиш на клавиатуре, а также сбора информации о процессах и приложениях, которые работали во время записи. Это позволяет существенно расширить доказательную базу при расследовании инцидентов информационной безопасности и помогает

выявлять подозрительное поведение пользователей и злоупотребления привилегиями доступа или политиками защиты данных, что в результате снижает риск утечки данных.

После отправки политик с настройками мониторинга на агенты для Linux, агенты начинают вести запись событий. Полученные данные передаются на сервер, где их можно просмотреть в журнале активности пользователей (см. *Активность пользователей*).

Для работы с настройками мониторинга активности необходимо включить права **Просмотр** и **Изменение** в разделе **НАСТРОЙКИ → Роли → Управление → Политики / Мониторинг активности пользователей** (см. *Права для управления компонентами политик, справочниками и служебными событиями*).

### Параметры

На данном экране можно выбрать параметры мониторинга активности пользователей:

- **Черно-белое изображение** — определяет цветовой режим видеозаписей с экрана: черно-белые, если параметр включен, и цветные, если выключен. Черно-белые видеозаписи занимают меньше места.
- **Запись до события** — определяет, какой отрезок времени до наступления события необходимо включать в запись. Таким образом можно зафиксировать действия пользователя, предшествующие событию, и сам момент нарушения, что упрощает расследование инцидентов.

  В настройках параметра можно выбрать время до события или указать его вручную (до 300 секунд). Чтобы отключить параметр, установите значение, равное 0 секунд, или переведите его в положение **Выкл**.

  Запись до события не учитывается при вычислении продолжительности записи для завершения по параметру **Принудительно прекращать запись через <число> сек.**

  Этот параметр работает, только если для текущего пользователя (или группы) заданы правила мониторинга активности.
- **Приостановить запись при неактивности** — позволяет приостанавливать запись при отсутствии активности пользователя, сокращая объем данных мониторинга.

  Когда параметр включен, запись приостанавливается, если пользователь в течение указанного времени не нажимает клавиши на клавиатуре, не перемещает мышь и не нажимает на её клавиши. Запись возобновляется при нажатии любой клавиши или перемещении мыши. Когда параметр отключен, запись продолжается даже при отсутствии активности пользователя.

  Параметр устанавливает максимально допустимое время отсутствия активности пользователя. Чтобы включить его, в настройках параметра установите значение от 3 секунд. Чтобы отключить параметр, установите значение, равное 0 секунд.

- **Разрешение видеозаписи** — позволяет задать выходное разрешение для видеозаписи экрана. Чтобы создать видеозапись в разрешении экрана пользователя, в настройках параметра выберите **Базовое**.

  При записи сохраняется соотношение сторон записываемого экрана. По этой причине высота или ширина видеозаписи может отличаться от указанной в настройках. Как правило, ширина совпадает с указанной, а высота вычисляется так, чтобы сохранить исходное соотношение сторон.

- **Несколько мониторов** — позволяет указать, как вести запись с компьютеров с несколькими мониторами. Можно вести запись только с основного монитора или со всех сразу (в единую запись или отдельную для каждого монитора).

### Правила

В данном разделе можно добавлять правила, а также просматривать, редактировать, клонировать, запускать, останавливать и удалять существующие правила.

Для каждого правила можно задать следующие параметры:

- **Имя правила**.
- **Описание правила** — дополнительная информация о правиле.
- **Группы и пользователи** — список групп и пользователей, для которых будет работать данное правило.
- **Объект записи** — ввод с клавиатуры, экран, ввод с клавиатуры и экран.
- **Принудительно прекращать запись через** — если флажок установлен, запись начнется при выполнении условия начала записи и прекратится через указанное количество секунд. Если условие начала записи все еще будет выполняться, запись начнется снова, если только не включен следующий параметр.
- **Возобновлять запись, если состояние не изменилось** (отображается, если включен предыдущий флажок) — если флажок установлен, запись возобновится после принудительного прекращения, если условие начала записи еще выполняется. Например, если запись началась при запуске определенного процесса и принудительно прекратилась после указанного времени, она возобновится, если процесс еще запущен.
- **Интервал между снимками экрана** — частота снимков экрана в видеозаписи. Этот параметр помогает избежать добавления в запись одинаковых снимков экрана.
- **Составление правила для начала записи** — логический конструктор для составления условия срабатывания правила из критериев (см. далее).

Правила для начала записи можно комбинировать из следующих критериев:

- **Пользователь вошел в систему** (обязательный) — контролируемый пользователь вошел в систему локально или удаленно с помощью служб терминалов или удаленного рабочего стола, пройдя проверку подлинности. Может использоваться самостоятельно.
- **Сработавшее контентное правило** — контролируемый пользователь попытался отправить или получить данные, соответствующие контентно-зависимому правилу с указанным именем. Значение этого параметра можно задавать с помощью условий **содержит**, **начинается с**, **заканчивается на** и **принимает значение**.
- **Сработавшее правило белого списка USB-устройств** — контролируемый пользователь попытался получить доступ к входящему в белый список USB-устройству с указанным описанием. Значение этого параметра можно задавать с помощью условий **содержит**, **начинается с**, **заканчивается на** и **принимает значение**.
- **Доступ на чтение запрещен** — попытка контролируемого пользователя получить данные была заблокирована из-за отказа в доступе к одному из указанных устройств/протоколов или в соответствии с указанными настройками безопасности. Применимы следующие каналы:
  - USB-порт,
  - Съёмные устройства,
  - TC-устройства (USB-устройства),
  - TC-устройства (Буфер обмена),
  - TC-устройства (Подключённые диски).
- **Доступ на запись запрещен** — попытка контролируемого пользователя отправить данные была заблокирована из-за отказа в доступе к одному из указанных устройств/протоколов или в соответствии с указанными настройками безопасности. Применимы следующие каналы:
  - USB-порт,
  - Съёмные устройства,
  - TC-устройства (Буфер обмена),
  - TC-устройства (Подключённые диски),
  - Принтер.
- **Ethernet-подключение существует** — к компьютеру подключен сетевой кабель.
- **Процесс существует** — контролируемый пользователь запустил на компьютере указанный процесс. Значение этого параметра можно задавать с помощью условий **содержит**, **начинается с** и **заканчивается на**.

- **Окно находится в фокусе** — открытое контролируемым пользователем окно с указанным заголовком активно и может получать ввод с клавиатуры и мыши. Значение этого параметра можно задавать с помощью условий **содержит**, **начинается с** и **заканчивается на**.

# Компьютеры

В данном разделе можно управлять списком компьютеров, контролируемых агентами Cyber Protego для Linux.

Список компьютеров может состоять из следующих сущностей: одиночных компьютеров, их динамических групп (по информации из службы каталогов при настроенной интеграции), а также папок (объединений одиночных компьютеров и/или динамических групп).

В этом разделе можно менять сущности, назначать или отключать им политики, синхронизировать назначенные политики, а также просматривать политики, назначенные выбранной сущности.

Доступно два вида отображения списка:

- **Структура** — древовидное представление, в котором отображена вложенность сущностей, причем они могут быть представлены в списке несколько раз. Например, одиночный компьютер может быть представлен как на верхнем уровне, так и в составе группы или папки. Группа также может быть представлена как на верхнем уровне, так и в составе папки. Папки могут быть представлены только на верхнем уровне. Одну папку нельзя поместить в другую.
- **Плоский список** — представление, на котором отображены все контролируемые компьютеры независимо от уровня вложенности.

Помимо имён сущностей в списке также отображается сводная информация:

- список проблем (например, нехватка лицензий или недоступность компьютера),
- версия агента,
- список примененных политик (в порядке уменьшения приоритета).

Щёлкнув сущность в списке, можно просмотреть все назначенные ей политики. В режиме просмотра доступны следующие разделы:

- Общие сведения о папке, группе или компьютере (в зависимости от типа выбранной сущности).

  В этом разделе отображается краткая информация о сущности и перечисляются применённые к ней политики. При этом указаны как явно назначенные, так и унаследованные политики (например, если сущность входит в папку, которой назначены политики).

  В этом разделе можно назначать и отключать политики, а также синхронизировать их вне расписания.

- Сумма политик, применённых к папке, группе или компьютеру (в зависимости от типа выбранной сущности).

  Папкам, группам и компьютерам может быть назначено сразу несколько политик. В них могут быть заданы разные значения одних и тех же параметров (например, в одной политике доступ к съемным устройствам может быть разрешен, в другой — запрещен, а в третьей — не определен). С учётом приоритета политик и их настроек формируется итоговая политика (сумма политик), которая применяется к папкам, группам и компьютерам.

  В сумме политик можно только просматривать итоговые значения параметров и политики, из которых они получены. Поменять значения можно, перейдя в соответствующую политику.

# Управление агентами

Если веб-консоль установлена на ОС Linux, в разделе **УПРАВЛЕНИЕ** → **Управление агентами** можно управлять агентами для Linux на удаленных компьютерах: устанавливать, обновлять и удалять.

Требования:

- На целевой системе должен быть установлен и запущен SSH-сервер (обычно из пакета `openssh-server`) с поддержкой SFTP и парольной аутентификацией.
- Должно быть *настроено взаимодействие с агентами для Linux*.

Для выполнения каждого из перечисленных действий необходимо создать соответствующую задачу. Для удобства задачи можно размещать в папках, создаваемых в этом же разделе.

## Создание задач

Чтобы создать задачу, нажмите **Добавить задачу** в списке задач слева. В окне **Добавление задачи** заполните следующие поля:

- **Имя** — имя задачи.
- **Описание** (необязательно) — описание задачи.
- Переключатель **Задача активна сразу после добавления** — включает или отключает задачу при создании. Если активной задаче назначено расписание, она будет выполняться по нему автоматически. По умолчанию включен.
- **Операционная система** — операционная система удаленного компьютера. Поддерживаются только машины с ОС Linux.
- **Действие** — тип задачи:
  - **Установка и обновление** — позволяет установить и обновить агенты на указанных

компьютерах. Если агента на компьютере нет, он будет установлен.

- **Обновление** — позволяет обновить агенты до актуальной версии на указанных компьютерах. Если агента на компьютере нет, он не будет установлен.
- **Удаление** — позволяет удалить агенты с указанных компьютеров.

Для действий **Установка и обновление** и **Обновление** доступен флажок **Обновить список пакетов перед выполнением задачи**. Если он включен, перед установкой или обновлением агентов на целевых системах будет обновлён список пакетов (локальный кэш репозиториев). При этом, если задача затрагивает большое число агентов, важно соблюдать рекомендации, приведённые далее.

- **Подключение к ПК** — сведения для подключения к указанным компьютерам:
  - **Имя пользователя** — имя пользователя, от имени которого необходимо подключиться к компьютерам и выполнить выбранные действия. Должен обладать привилегиями sudo.
  - **Пароль** — пароль пользователя.
  - **Порт** — номер TCP-порта для подключения. По умолчанию указан порт 22.

Заполнив поля, нажмите **Добавить**. Задача появится в списке.

После создания задачи необходимо указать для неё список компьютеров, групп или папок, для которых она будет выполняться. Кроме того, можно назначить ей расписание.

Чтобы перейти на экран задачи, щёлкните её в списке.

На экране задачи можно указать для неё компьютеры и группы, изменить её параметры или отдельно действие, назначить ей расписание, переключить её активность для автоматического выполнения по расписанию, а также запустить задачу вручную.

Чтобы запустить задачу вручную нажмите **Выполнить** на экране задачи. Кроме того, задачу можно запустить или удалить, нажав в списке задач значок многоточия у имени задачи и выбрав соответствующее действие.

### Рекомендации по обновлению списка пакетов

Если в задаче включён флажок **Обновить список пакетов перед выполнением задачи**, на каждой целевой системе перед установкой или обновлением агента будет обновлён список пакетов с помощью соответствующих команд. Например, `apt-get update` (Альт Рабочая станция), `apt update` (Astra Linux), `dnf makecache` (РЕД ОС).

Для корректного распределения нагрузки при массовой установке или обновлении важно соблюдать следующие рекомендации:

1. Уменьшите число одновременно обрабатываемых целевых систем. Это снизит единомоментную

нагрузку при отправке запросов к репозиториям в окружениях с нестабильным сетевым соединением или с большим парком компьютеров.

Для этого уменьшите значение параметра `maxParallelInstallWorkers` вплоть до 3—5 в конфигурационном файле `/opt/cyberprotect/cpserver/CPServerBackend.yml`:

1. Остановите службу CPServerBackend командой `systemctl stop CPServerBackend`.
2. Измените значение параметра `maxParallelInstallWorkers`, например:

```
server:
<...>
    management:
        <...>
        maxParallelInstallWorkers: 5
```

3. Запустите службу CPServerBackend командой `systemctl start CPServerBackend`.

2. Используйте локальные зеркала репозиториев. Это позволит не зависеть от внешних репозиториев и ускорит массовую установку или обновление агентов.

   Шаги по настройке локальных репозиториев приведены в документации для соответствующих ОС. Например: Альт Рабочая станция, Astra Linux, РЕД ОС.

## Добавление компьютеров в задачи

Чтобы указать задаче компьютеры, для которых она будет выполняться, на экране задачи нажмите **Добавить компьютеры и группы**. Если настроена интеграция со *службой каталогов*, в открывшемся окне **Добавление компьютеров и групп** на соответствующих вкладках можно будет выбрать группы компьютеров в домене и компьютеры в домене. Кроме того, на вкладке **Компьютеры по имени или IP-адресу** можно будет указать отдельные компьютеры по их имени или IP-адресу. Имена и IP-адреса можно указать вручную или загрузить из файла.

Выбрав компьютеры и их группы, нажмите **Добавить**.

## Назначение расписания задачам

Чтобы назначить задаче расписание, на экране задачи нажмите **Добавить** в блоке **Расписание** справа. В открывшемся окне **Расписание выполнения задачи** нажмите **+ Расписание** и выберите необходимые параметры:

- каждый час: в любой день, в рабочий день, в выходные;
- каждый день: любой, рабочий, выходной;
- каждую неделю: любую, первую, вторую, третью, четвертую, последнюю;

- каждый месяц: в указанное число или нужный день недели.

Задаче можно одновременно назначить ряд условий, которые вместе составят расписание её выполнения.

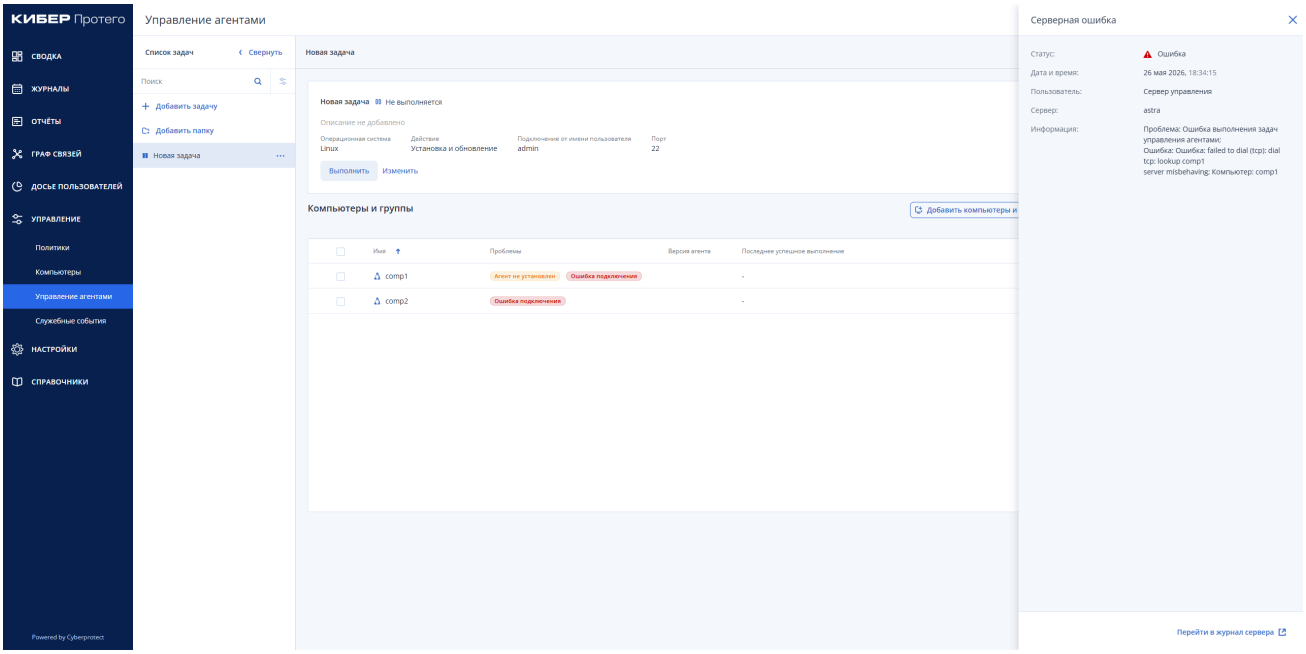
Чтобы изменить расписание задачи, на экране задачи в блоке справа нажмите **Изменить**. В открывшемся окне **Расписание выполнения задачи** щёлкните нужное условие расписания и отредактируйте его или нажмите значок корзины справа от условия, чтобы его удалить.

Задачи без расписания можно запускать только вручную.

## Просмотр информации об ошибках

Для получения информации об ошибках, возникающих при выполнении задач, можно щёлкнуть тип ошибки в столбце **Проблемы**. Справа появится боковая панель с подробностями об ошибке.

Кроме того, для просмотра других событий можно перейти в журнал сервера, отфильтрованный по имени компьютера, на котором возникла ошибка. Для этого на боковой панели щёлкните **Перейти в журнал сервера**.




# Служебные события

В разделе **УПРАВЛЕНИЕ → Служебные события** можно просматривать, фильтровать и удалять записи журнала служебных событий. Этот журнал дает представление о состоянии и работе агентов, например, записи о запуске и остановке агентов, об изменении настроек (прав доступа, аудита, теневого копирования, алертов, белых списков, контентных правил и пр.), о переполнении квоты, восстановлении поврежденных файлов и так далее.

Журнал формируется на основе информации из базы данных событий (см. *База данных событий*).

Доступ к этому разделу имеют пользователи с правом просмотра служебных событий (см. *Права для управления компонентами политик, справочниками и служебными событиями*).

По умолчанию выводятся все события, однако их можно фильтровать с помощью базового набора фильтров. Полный список можно вывести, нажав **Используемые фильтры** внизу экрана:

- **Статус** — состояние записи:
  - Успешно — операция выполнена успешно;
  - Предупреждение — сообщение о возможных осложнениях или ошибках.
- **Компьютер** — имя или IP-адрес компьютера, на котором произошло событие.
- **Дата и время** — дата и время возникновения события.
- **Источник** — источник события.
- **Действие** — выполненное действие или зафиксированное событие.
- **Имя** — дополнительная информация о событии.
- **Информация** — прочая информация, относящаяся к событию.
- **Причина** — причина наступления события.
- **Пользователь** — имя пользователя, связанного с событием.
- **Процесс** — путь к исполняемому файлу приложения, связанного с событием.
- **Дата и время сбора** — дата и время, когда событие было получено сервером управления.
- **Сервер** — имя сервера управления, получившего событие.
- **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.

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

Чтобы удалить событие, откройте сведения о нём и внизу нажмите **Удалить событие**. Чтобы удалить сразу несколько событий, отметьте их флажками в столбце слева и нажмите **Удалить** над списком событий.

Чтобы настроить автоматическую очистку журнала, щёлкните выпадающее меню **Очистить журнал** в правом верхнем углу и выберите **Настроить автоматическое удаление старых данных**. В открывшемся разделе **Конфигурация** задайте параметры автоматической очистки журнала.

Чтобы очистить журнал вручную, щёлкните выпадающее меню **Очистить журнал** в правом верхнем углу и выберите **Удалить старые данные сейчас**. В появившемся диалоге укажите возраст записей, которые нужно удалить. Чтобы удалить все данные в журнале, укажите возраст записей, равный 0 лет, 0 месяцев и 0 дней.

Удаление записей выполняется в фоновом режиме. При запуске этой процедуры появляется уведомление.

# Настройки

## 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**.

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

## 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.

После создания новая роль появится в списке. Выбрав роль, можно просмотреть её данные.

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 **Изменить** 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 роль**. В появившемся окне подтвердите действие, нажав **Удалить**. Удалять можно только роли, которые не назначены пользователям.

**Важно**

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

## Права для сводки

Для сводки доступны следующие права:

- **Доступ** — просмотр и настройка виджетов.

## Права для журналов

Для журналов доступны следующие права:

- События:
  - **Просмотр** — доступ к разделу событий, экспорт событий.
  - **Изменение** — изменение статусов рассмотрения событий, создание и редактирование комментариев к событиям.
  - **Доступ к теневым копиям** — просмотр, скачивание и удаление теневых копий событий.
  - **Удаление** — удаление событий и их теневых копий.

  Для удаления теневых копий событий необходимы права **Доступ к теневым копиям** и **Удаление**.
- Активность пользователей:
  - **Просмотр** — доступ к журналу активности пользователей, а также просмотр, фильтрация и скачивание записей.
  - **Удаление** — удаление записей экрана из событий и удаление событий целиком.

## Права для отчётов

Для отчётов доступны следующие права:

- Задачи:
  - **Создание** — создание задач генерации отчётов, указание параметров задач.
  - **Просмотр** — просмотр параметров задач генерации отчётов.
  - **Редактирование** — редактирование задач генерации отчётов.
  - **Изменение списка** — создание, переименование, удаление папок.
  - **Запуск** — ручной запуск задач генерации отчётов. Указание интервала выборки событий при запуске задач.
  - **Удаление** — удаление задач генерации отчётов.
- Базовые отчёты:
  - **Просмотр** — просмотр сгенерированных отчётов.
  - **Удаление** — удаление сгенерированных отчётов.
- Отчеты КРВ:
  - **Просмотр** — просмотр сгенерированных отчётов контроля рабочего времени.
  - **Удаление** — удаление сгенерированных отчётов контроля рабочего времени.

## Права для графов связей

Для графов связей доступны следующие права:

- **Просмотр** — просмотр содержимого графов связей.
- **Удаление** — переименование и удаление графов связей.
- Задачи:
  - **Создание** — создание задач генерации графов связей, указание параметров задач.
  - **Просмотр** — просмотр параметров задач генерации графов связей.
  - **Редактирование** — редактирование задач генерации графов связей.
  - **Изменение списка** — создание, переименование и удаление папок; перемещение задач в папки.
  - **Запуск** — ручной запуск задач генерации графов связей, указание интервала выборки событий при запуске задачи.

- **Удаление** — удаление задач генерации графов связей.

## Права для досье пользователей

Доступны следующие права:

- **Просмотр** — просмотр списка и досье пользователей, изменение периода построения отчётов.
- **Изменение** — редактирование, удаление, создание групп, добавление пользователей в группы и удаление пользователей из групп.

## Права для управления компонентами политик, справочниками и служебными событиями

Доступны следующие права:

- Политики / Список политик:
  - **Просмотр** — доступ к списку политик.
  - **Изменение** — редактирование настроек политик.
- Политики / Настройки агента:
  - **Просмотр** — доступ к разделу настроек агента.
  - **Изменение** — редактирование настроек агента.
- Политики / Имя, компьютеры, группы (список), Управление / Компьютеры (список), Управление агентами / Имя, компьютеры, группы (список):
  - **Просмотр** — доступ к соответствующим подразделам.
  - **Изменение** — редактирование настроек в соответствующих подразделах.
- Политики / Права доступа, Справочники / Библиотека контентных триггеров:
  - **Просмотр** — доступ к соответствующим подразделам.
  - **Изменение** — редактирование настроек в соответствующих подразделах.
- Политики / Мониторинг активности пользователей:
  - **Просмотр** — доступ к подразделу мониторинга активности пользователей.
  - **Изменение** — редактирование настроек в подразделе мониторинга активности пользователей.
- Управление агентами:

        - **Просмотр** — доступ к разделу, к просмотру списка задач и папок, к просмотру задач.
        - **Изменение** — редактирование задач.
        - **Изменение списка** — редактирование списка задач и папок (создание, переименование и удаление папок, а также перемещение задач в папки и из них).
        - **Запуск** — запуск выполнения задач.
        - **Удаление** — удаление задач.
    - Служебные события:
        - **Просмотр** — доступ к разделу, просмотр и фильтрация записей.
        - **Удаление** — удаление записей из журнала служебных событий.

## Права для настроек системы

Для настроек системы доступны следующие права:

- Пользователи:
    - **Создание** — изменение всех параметров пользователя при его создании.
    - **Просмотр** — просмотр данных пользователей.
    - **Изменение** — изменение данных пользователей, включая пароли.
    - **Изменение списка** — создание, переименование, удаление папок.
    - **Назначение роли** — назначение ролей пользователям.
    - **Удаление** — удаление пользователей.
- Роли:
    - **Создание** — изменение всех параметров роли при ее создании.
    - **Просмотр** — просмотр прав, назначенных ролям.
    - **Изменение** — изменение данных ролей.
    - **Изменение списка** — создание, переименование, удаление папок.
    - **Удаление** — удаление ролей.
- Параметры базы данных:
    - **Просмотр** — активные действия недоступны.
    - **Изменение** — задание параметров базы данных, тестирование соединения.

- Параметры клиента API:
  - **Просмотр** — просмотр списка клиентов API.
  - **Изменение** — управление клиентами API.
- Параметры службы каталогов:
  - **Просмотр** — просмотр настроек служб каталогов.
  - **Изменение** — изменение настроек служб каталогов, удаление добавленных каталогов.
- Параметры конфигурации:
  - **Просмотр** — просмотр настроек хранилища.
  - **Изменение** — изменение настроек хранилища.
- Лицензирование:
  - **Просмотр** — просмотр списка загруженных лицензий.
  - **Изменение** — загрузка, скачивание и удаление лицензий.
- Журнал сервера:
  - **Просмотр** — доступ к журналу, просмотр и фильтрация записей.
  - **Удаление** — удаление записей из журнала.

# 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.

**Важно**

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

## База данных событий

Чтобы подключиться к базе данных событий 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**.

Если базы данных с этими параметрами не существует, вам будет предложено создать её автоматически.

Базу данных событий необходимо обновлять после обновления веб-консоли. Для этого в данном разделе заново укажите пароль к БД, сохраните изменения и подтвердите её обновление.

**Примечание**

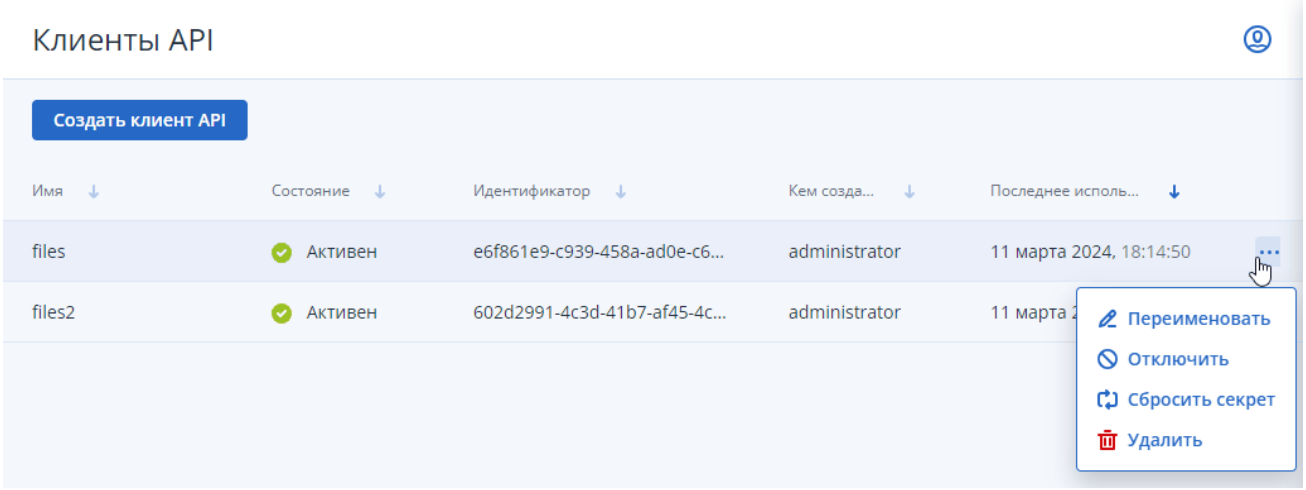
База данных событий — не служебная база данных, указываемая при установке (также см. *Замена служебной базы данных*). Это отдельная БД, параметры которой можно задать только на данном экране.

# Клиенты API

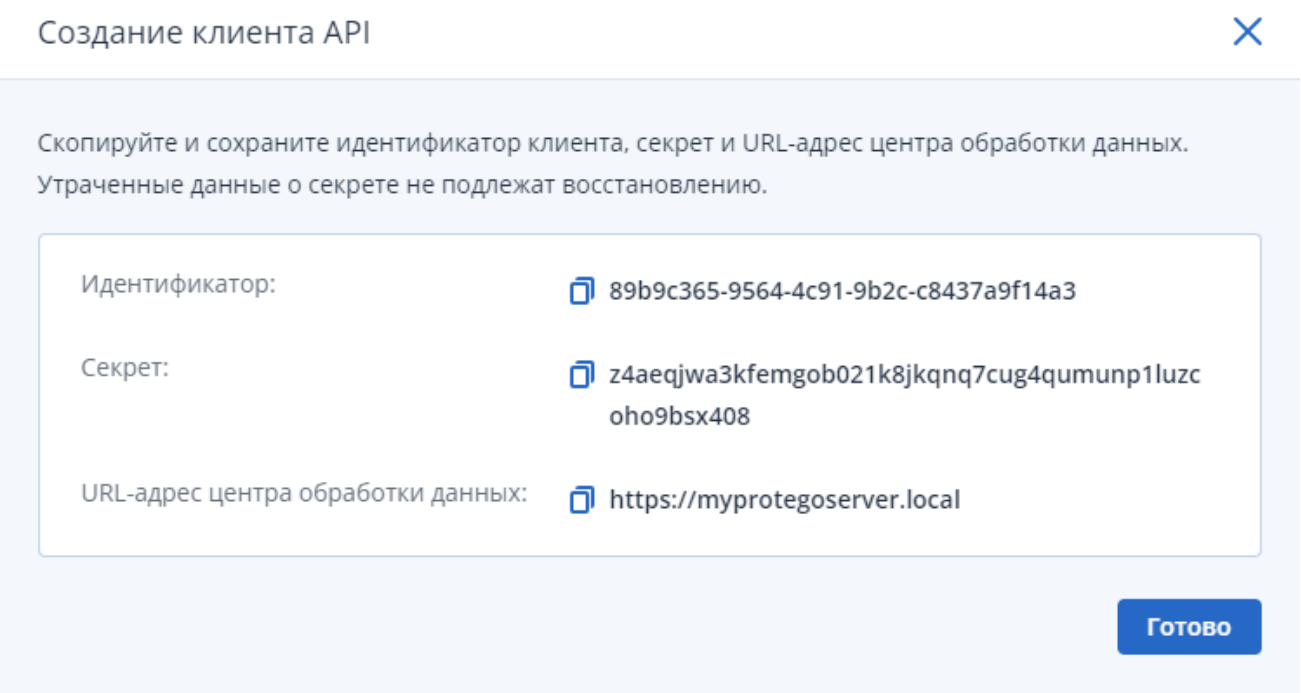
Создавать клиентов для интеграции со сторонним ПО можно в окне **НАСТРОЙКИ** → **Клиенты API**.

Поддерживаются следующие клиенты:

- Кибер Файлы — решение для безопасного доступа, синхронизации и совместного использования файлов организации.
- Microolap EtherSensor — решение для анализа сетевого трафика в режиме реального времени, которое распознает такие объекты пользовательских и системных коммуникаций, как сообщения, файлы и сетевые события.




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 для настройки интеграции: идентификатор, секрет и URL-адрес центра обработки данных.

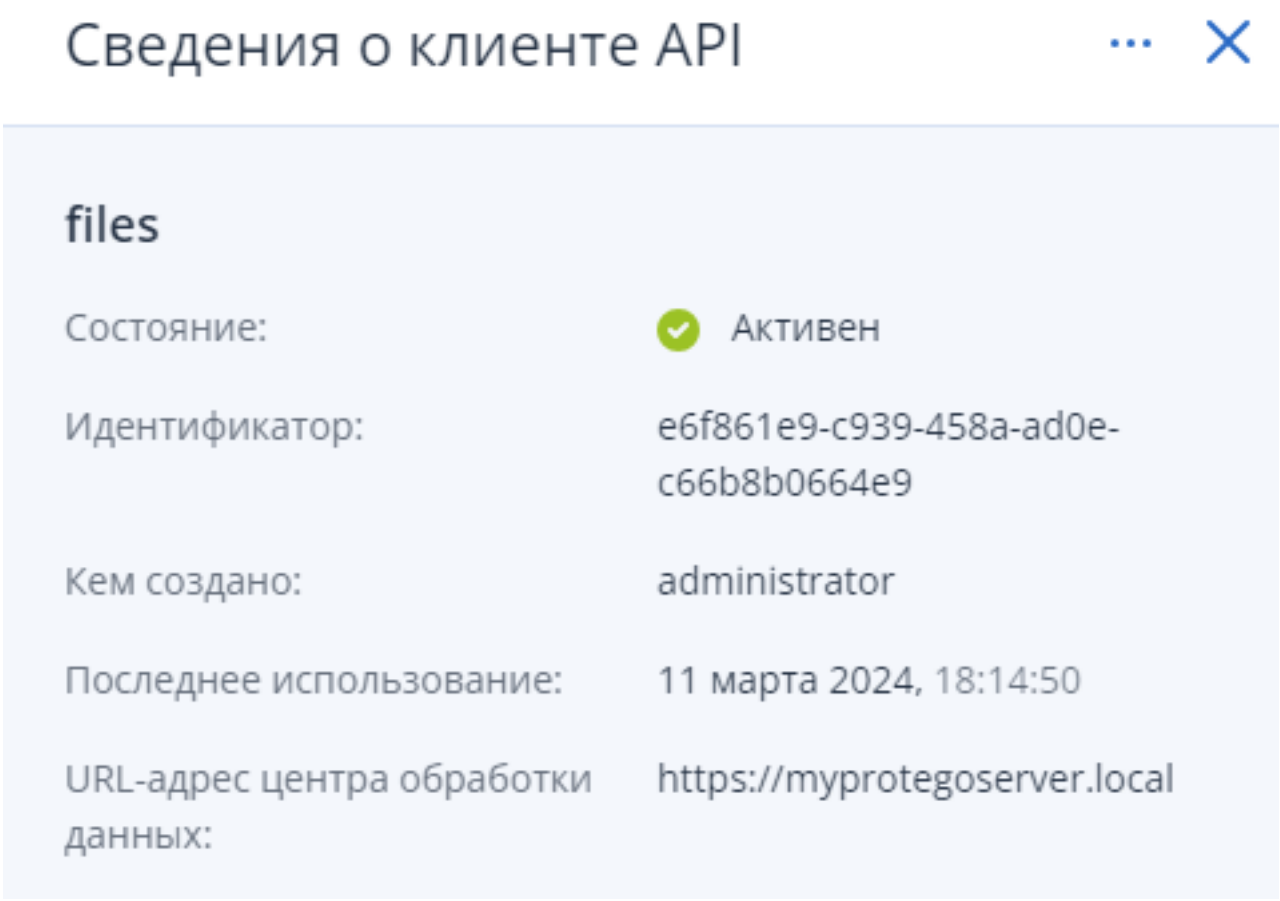



Скопируйте и сохраните идентификатор клиента, секрет и URL-адрес центра обработки данных.

**Важно**

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.

## Службы каталогов

На данном экране можно указать параметры службы каталогов. Это необходимо для получения списка доменных пользователей и групп, компьютеров и подразделений (Organizational Unit, OU) для взаимодействия с ними в разделе **Управление**.

Можно указать следующие параметры:

- **Тип службы каталогов** — Active Directory, Samba DC, Эллес, РЕД АДМ. Можно одновременно использовать несколько служб каждого из поддерживаемых типов.
- **Имя сервера** — доменное имя или IP-адрес сервера, на котором работает служба каталогов.
- **Порт** — порт, по которому доступна служба каталогов.
- **Базовый DN** — начальная точка для просмотра дерева каталога.
- **Имя пользователя** и **Пароль** — имя и пароль пользователя для подключения к службе каталогов.

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

Включить использование SSL можно с помощью одноимённого флажка.

# Конфигурация

## Хранилище

На данной странице можно указать путь хранения данных и настроить автоматическое удаление старых данных: записей в журнале событий, теневых копий, записей активности пользователей, видеозаписей, записей контроля рабочего времени, записей в журналах служебных событий и сервера. Доступ к хранилищу по указанному пути осуществляется под той же учетной записью, из-под которой запущена служба веб-консоли.

Данные хранятся в обезличенном виде (аналогично реализации на сервере управления). Удалить полученные данные можно вручную или автоматически.

Чтобы включить автоматическое удаление старых данных, нажмите **Изменить**, отметьте необходимые флажки и укажите период в годах, месяцах и днях, через который их следует удалить. Наименьший возраст данных для удаления равен одному дню.

### Способы указания путей хранения данных

Чтобы изменить путь, нажмите **Изменить**, затем нажмите на поле **Путь хранения данных**, укажите новый путь и нажмите **Сохранить**. Например: `\\storageserver\shadowcopiesstorage\`.

Поддерживаются локальные пути в форматах Windows и Linux. Кроме того, для хранилищ на ОС Windows можно указывать UNC-пути. Чтобы указать путь к сетевому хранилищу на ОС Linux, необходимо подмонтировать его локально и указать локальный путь. Также можно указывать абсолютные и относительные пути. Относительные пути указываются от расположения исполняемого файла веб-консоли:

#### Windows

Относительно директории `C:\Program Files\Cyber Protego Server\backend`.

#### Linux

Относительно директории `/opt/cyberprotect/cpserver/`.

При установке веб-консоли на Windows пути можно указывать и в формате Linux (через обычные косые черты). При этом если на Linux использовать формат Windows, в директории исполняемого файла будет создана поддиректория с указанным именем, то есть с точкой и обратной косой чертой в названии.

По умолчанию используются следующие пути:

#### Windows

```
C:\Program Files\Cyber Protego Server\backend\shadow
```

#### Linux

```
/opt/cyberprotect/cpserver/shadow/
```

# Лицензирование

В данном разделе можно загружать, просматривать, скачивать и удалять лицензии, которые необходимы для полноценной работы веб-консоли в качестве управляющего сервера.

Поддерживаются следующие типы лицензий:

- Device Control Linux (обязательная),
- Content Control Linux (дополнительная),
- TS Control Linux (дополнительная),
- User Activity Monitor Linux (дополнительная).

Тип загруженных лицензий определяет, какие настройки будут доступны при создании политик для агентов Cyber Protego. Без лицензии Device Control Linux остальные лицензии недействительны. Количество загруженных лицензий определяет число контролируемых агентов.

Применение лицензий для Windows также поддерживается, но только для использования аналитических возможностей веб-консоли.

## Область действия лицензии Device Control Linux

- Доступ к разделу **Управление**.
- Изменение следующих настроек в политиках для Linux и распространение таких политик на агенты для Linux:
  - Настройки агента.
  - Доступ к разделу **Устройства**. Для ТС-устройств также понадобится лицензия TS Control Linux. Для контентных правил для устройств и справочника **Библиотека контентных триггеров** также понадобится лицензия Content Control Linux.
- Доступ к справочнику **USB-устройства**.

- Сбор данных с агентов для Linux.

Подробнее о данном типе лицензии см. в Руководстве пользователя в разделах О типах лицензий Cyber Protego и Лицензирование Web Control и Content Control.

## Область действия лицензии Content Control Linux

- Изменение настроек политик для Linux: все поддерживаемые типы контентных правил для устройств (регулярные выражения, свойства документа, составные). Для ТС-устройств также понадобится лицензия TS Control Linux.
- Доступ к справочнику **Библиотека контентных триггеров**.

Подробнее о данном типе лицензии см. в Руководстве пользователя в разделах О типах лицензий Cyber Protego и Лицензирование Web Control и Content Control.

## Область действия лицензии TS Control Linux

Изменение настроек политик для Linux: взаимодействие с ТС-устройствами в разделах **Права доступа**, **Аудит, теневое копирование и алерты**, **Контентные правила**. Для доступа к разделу **Контентные правила** также понадобится лицензия Content Control Linux.

## Область действия лицензии User Activity Monitor Linux

Изменение настроек мониторинга активности пользователей.

## Использование лицензий

Лицензии используются (расходуются) при распространении политик и сборе данных с агентов. Один агент для Linux использует одну лицензию Device Control Linux для получения политик и передачи данных на сервер. При этом если агент запущен на терминальном сервере, он лицензируется по максимальному числу одновременных пользовательских сеансов удаленного рабочего стола по протоколу xrdp. Например, для 30 сеансов понадобится 30 лицензий для отправки настроек на агент и сбора с него данных.

Если лицензий меньше, чем агентов, часть агентов не сможет получать настройки от сервера и передавать данные на сервер. В списке компьютеров у таких агентов появится соответствующая отметка.

Использованные (израсходованные) лицензии освобождаются через 6 часов с момента последнего взаимодействия между лицензированным агентом и веб-консолью. Информация о максимальном числе зафиксированных на терминальном сервере одновременных пользовательских xrdp-сессий хранится в течение недели.

### Пробный период

В течение 30 дней с момента установки веб-консоль можно полноценно использовать для управления пятью агентами для Linux. После этого, если не добавить лицензию, станет недоступен функционал разделов **Управление** и **Справочники**, агенты не смогут получать новые политики и передавать данные на сервер.

# Журнал сервера

В разделе **НАСТРОЙКИ** → **Журнал сервера** можно просматривать, фильтровать и удалять записи журнала сервера. Этот журнал дает представление о состоянии сервера и фиксирует действия администраторов, например, создание задач построения отчетов, редактирование политик, удаление записей в журналах, применение лицензий, обновление используемой базы данных и пр.

Информация для журнала берется из служебной базы данных.

Доступ к этому разделу имеют пользователи с правом просмотра журнала сервера (см. *Права для настроек системы*).

По умолчанию выводятся все события, однако их можно фильтровать с помощью базового набора фильтров. Полный список можно вывести, нажав **Используемые фильтры** внизу экрана:

- **Статус** — тип записи:
  - **Информация** — штатное событие;
  - **Предупреждение** — событие, требующее внимания;
  - **Ошибка** — сбой в работе системы.
- **Дата и время** — дата и время возникновения события.
- **Событие** — краткое описание события.
- **Информация** — дополнительная информация о событии.
- **Пользователь** — идентификатор и полное имя пользователя веб-консоли, вызвавшего появление события (для служебных событий используется специальное имя ”Сервер управления”).
- **Сервер** — имя сервера, на котором произошло событие.
- **Компьютер** — имя или IP-адрес компьютера, на котором произошла ошибка при выполнении задач управления агентами. Доступен только при переходе в журнал сервера из задач управления агентами.

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

Чтобы настроить автоматическую очистку журнала, щёлкните выпадающее меню **Очистить журнал** в правом верхнем углу и выберите **Настроить автоматическое удаление старых данных**. В открывшемся разделе **Конфигурация** задайте параметры автоматической очистки журнала.

Чтобы очистить журнал вручную, щёлкните выпадающее меню **Очистить журнал** в правом верхнем углу и выберите **Удалить старые данные сейчас**. В появившемся диалоге укажите возраст записей, которые нужно удалить. Чтобы удалить все данные в журнале, укажите возраст записей, равный 0 лет, 0 месяцев и 0 дней.

Удаление записей выполняется в фоновом режиме. При запуске этой процедуры появляется уведомление.

# Расширенные настройки

## Изменение порта веб-консоли

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

**Важно**

Не используйте порт 444.

1. Остановите службы:

   **Windows**

   ```
   > net stop CPServerBackend
   > net stop CPServerProxy
   ```

   **Linux**

   ```
   # systemctl stop nginx
   ```

2. Измените значение порта в конфигурационном файле:

   **Windows**

   `C:\Program Files\Cyber Protego Server\proxy\conf\CPServerProxy.conf`

   **Linux**

   `/etc/nginx/sites-available.d/CPServerProxy.conf`

   1. Закомментируйте строку 3.
   2. Укажите порт в строках 5 и 11.

   В итоге конфигурационный файл может выглядеть так:

```
1 server {
2   # FOR SWITCHING TO NON-DEFAULT PORT: COMMENT NEXT LINE
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

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

  # 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:

#### Windows

```
> net start CPServerBackend
> net start CPServerProxy
```

#### Linux

```
# sudo systemctl start nginx
```

# Создание и 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 получения событий от клиентов API).

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

## Установка сертификатов в ОС Windows

Чтобы установить пользовательские сертификаты, выполните следующие действия:

1. Остановите службы:

```
> net stop CPServerBackend
> net stop CPServerProxy
> net stop CPServerFrontend
```

2. Поместите новый сертификат для подключения к веб-интерфейсу и соответствующий закрытый ключ в папку `C:\Program Files\Cyber Protego Server\proxy`.
3. Укажите имена файлов сертификата для подключения к веб-интерфейсу и соответствующего закрытого ключа в файле `C:\Program Files\Cyber Protego Server\proxy\conf\CPServerProxy.conf`. Например, для сертификата `customwebcert.crt` и ключа `customwebkey.key` укажите:

```
# Configuration for SSL/TLS certificates
ssl_certificate ../customwebcert.crt;
ssl_certificate_key ../customwebkey.key;
```

4. Поместите новый сертификат для подключения к API и соответствующий закрытый ключ в папку `C:\Program Files\Cyber Protego Server\backend`.
5. Укажите имена файлов сертификата для подключения к API и соответствующего закрытого ключа в файле `C:\Program Files\Cyber Protego Server\backend\CPServerBackend.yml`. Например, для сертификата `customapicert.crt` и ключа `customapikey.key` укажите:

```
tls:
enabled: true
cert: customapicert.crt
key: customapikey.key
```

6. Запустите остановленные ранее службы:

```
> net start CPServerBackend
> net start CPServerProxy
> net start CPServerFrontend
```

## Установка сертификатов в ОС Linux

Чтобы установить пользовательские сертификаты для подключения к веб-интерфейсу, выполните следующие действия:

1. Остановите службы:

```
# systemctl stop CPServerBackend
# systemctl stop nginx
```

2. Поместите новый сертификат для подключения к веб-интерфейсу и соответствующий закрытый ключ в директорию `/etc/nginx/ssl`.
3. Укажите имена файлов сертификата для подключения к веб-интерфейсу и соответствующего закрытого ключа в файле `/etc/nginx/sites-available.d/CPServerProxy.conf`. Например, для сертификата `customwebcert.crt` и ключа `customwebkey.key` укажите:

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

4. Поместите новый сертификат для подключения к API и соответствующий закрытый ключ в директорию `/opt/cyberprotect/cpserver/backend/ssl`.
5. Укажите имена файлов сертификата для подключения к API и соответствующего закрытого ключа в файле `/opt/cyberprotect/cpserver/CPServerBackend.yml`. Например, для сертификата `customapicert.crt` и ключа `customapikey.key` укажите:

```
tls:
enabled: true
cert: /opt/cyberprotect/cpserver/backend/ssl/customapicert.crt
key: /opt/cyberprotect/cpserver/backend/ssl/customapikey.key
```

6. Запустите остановленные ранее службы:

```
# systemctl start CPServerBackend
# systemctl start nginx
```

# Управление служебной базой 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 подключение к этой БД можно перенастроить. Также можно заменить саму БД.

## Перенастройка подключения к служебной базе данных

Настройки подключения к служебной БД можно изменить с помощью следующей команды:

### Windows

```
CPServerBackend.exe change-db <параметры...>
```

### Linux

```
./CPServerBackend change-db <параметры...>
```

Параметры:

- `--obfuscate-password` — обфусцировать пароль в конфигурационном файле. Если параметр пропустить, пароль будет указан в явном виде.
- `--db-name {<имя_БД>}` — имя служебной БД (по умолчанию `postgres`).
- `--dialect {<postgres|mssql>}` — диалект базы данных (по умолчанию `postgres`).
- `--host {<хост>}` — IP-адрес или имя хоста, на котором работает сервер БД (по умолчанию `localhost`).
- `--port {<порт>}` — порт сервера БД; игнорируется при указании именованного экземпляра (named instance) для диалекта mssql (по умолчанию `5432`).
- `--ssl-mode {<режим_SSL>}` (только для диалекта postgres) — режим SSL-соединения; возможные значения: `disable`, `require`, `verify-ca`, `verify-full` (по умолчанию `disable`).
- `--user {<пользователь>}` — имя пользователя БД (по умолчанию `postgres`).
- `--config {<конфигурационный_файл>}` — путь к конфигурационному файлу БД (по умолчанию `config.yml`).

Для пропущенных параметров подставляются значения по умолчанию.

Пароль для подключения к БД запрашивается при каждом вызове команды. При этом его можно обфусцировать в конфигурационном файле, не меняя остальных параметров подключения. Используйте следующую команду:

#### Windows

```
CPServerBackend.exe obfuscate-password --config <конфигурационный_файл> [--read-from-file]
```

#### Linux

```
./CPServerBackend obfuscate-password --config <конфигурационный_файл> [--read-from-file]
```

Если задан параметр `--read-from-file`, пароль будет взят из конфигурационного файла. Если параметр не задан, будет запрошен новый пароль.

## Замена служебной базы данных

При необходимости служебную БД можно заменить, выполнив следующие шаги (принимается, что продукт установлен в директории по умолчанию).

1. Остановите службу веб-консоли.

   #### Windows

   ```
   > net stop CPServerBackend
   ```

   #### Linux

   ```
   # systemctl stop CPServerBackend
   ```

2. Отредактируйте конфигурационный файл.

   #### Windows

   `C:\Program Files\Cyber Protego Server\backend\CPServerBackend.yml`

   #### Linux

   `/opt/cyberprotect/cpserver/CPServerBackend.yml`

   В файле укажите диалект базы данных: `mssql` или `postgres`. Второй вариант также необходимо выбирать для Jatoba/Tantor. 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, выполните следующую команду:

#### Windows

Из директории `C:\Program Files\Cyber Protego Server\backend`

```
> CPServerBackend.exe migrate-db --config=”CPServerBackend.yml”
```

#### Linux

Из директории `/opt/cyberprotect/cpserver/backend`

```
# ./CPServerBackend migrate-db --config='../CPServerBackend.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:

#### Windows

```
> net start CPServerBackend
```

#### Linux

```
# systemctl start CPServerBackend
```

# 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.

1. Остановите службы:

   **Windows**

   ```
   > net stop CPServerBackend
   > net stop CPServerProxy
   ```

   **Linux**

   ```
   # systemctl stop CPServerBackend
   # systemctl stop nginx
   ```

2. Укажите необходимое время ожидания в формате `{<минуты>}m` или `{<часы>}h`. Например, ”15m”.

   **Windows**

   В конфигурационном файле `C:\Program Files\Cyber Protego Server\backend\CPServerBackend.yml`

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

   **Linux**

   В конфигурационном файле `/opt/cyberprotect/cpserver/CPServerBackend.yml`

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

3. Укажите необходимое время ожидания в секундах. Например, ”900”.

#### Windows

В конфигурационном файле `C:\Program Files\Cyber Protego Server\proxy\conf\CPServerProxy.conf`

#### Linux

В конфигурационном файле `/etc/nginx/sites-available.d/CPServerProxy.conf`

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

4. Запустите остановленные ранее службы:

#### Windows

```
> net start CPServerBackend
> net start CPServerProxy
```

#### Linux

```
# systemctl start CPServerBackend
# systemctl start nginx
```

## Восстановление учетной записи администратора с полными правами

При необходимости можно восстановить в веб-консоли учетную запись администратора, которая имеет максимальные права в разделе **Настройки**. Это можно сделать командой **`reset-admin`**, которая имеет следующий синтаксис:

#### Windows

```
> CPServerBackend.exe reset-admin [--password <новый пароль>] [--login <логин>] [--role <роль>] --
↪config <путь к CPServerBackend.yml>
```

### Linux

```
# ./CPServerBackend reset-admin [--password <новый пароль>] [--login <логин>] [--role <роль>] --
↪config <путь к CPServerBackend.yml>
```

Можно задать следующие параметры:

- `{<новый пароль>}` — новый пароль для указанного логина. Если параметр не указан, используется значение по умолчанию ”Cp*123456”.
- `{<логин>}` — логин, для которого задается новый пароль и роль. Если параметр не указан, используется значение по умолчанию ”admin”.
- `{<роль>}` — роль, которая будет создана или обновлена с максимальными правами в разделе **Настройки** и назначена указанному логину. Если параметр не указан и указанного логина не существует, используется значение по умолчанию ”admin_role”.
- `{<путь к CPServerBackend.yml>}` — путь к конфигурационному файлу `CPServerBackend.yml`.

Например, чтобы в ОС Windows задать пользователю ”admin” пароль ”Qazxsw123!” и роль ”admin_role” с максимальными правами в разделе **Настройки**, из директории `C:\Program Files\Cyber Protego Server\backend` выполните:

```
> CPServerBackend.exe reset-admin --password Qazxsw123! --login admin --role admin_role --config¬
↪CPServerBackend.yml
```

Чтобы задать то же самое в ОС Linux, из директории `/opt/cyberprotect/cpserver/backend/` выполните:

```
# ./CPServerBackend reset-admin --password Qazxsw123! --login admin --role admin_role --config ../
↪CPServerBackend.yml
```

При этом:

- Если пользователь с заданным логином существует, его пароль будет изменён на новый.
- Если пользователя с заданным логином не существует, он будет создан с новым паролем.
- Если заданная роль существует, ей будут даны максимальные права в разделе **Настройки**, и она будет назначена пользователю.

> **Важно**
>
> Если эта роль уже назначена другим пользователям, они также получат максимальные права в разделе **Настройки**.

- Если заданной роли не существует, она будет создана с максимальными правами в разделе **Настройки** и назначена пользователю.
- Если пользователь существует, но роль не задана, максимальные права в разделе **Настройки** будут даны текущей роли пользователя.
- Если пользователя не существует и роль не задана, созданному пользователю будет назначена роль по умолчанию ”admin_role”, которой будут даны максимальные права в разделе **Настройки**. Если этой роли не существует, она будет создана с данными правами.

> **Важно**
>
> Если эта роль уже назначена другим пользователям, они также получат максимальные права в разделе **Настройки**.

- Если пользователь с указанным логином уже зашел в веб-консоль на момент выполнения команды, ему необходимо будет выйти из неё и зайти заново, чтобы применить изменения в правах.

# Справочники

В данном разделе можно создавать, структурировать и хранить данные, которые можно использовать при создании политик.

## Библиотека контентных триггеров

Данный справочник позволяет управлять контентными триггерами, которые необходимы при работе с контентными правилами.

В данном справочнике можно просматривать, фильтровать и сортировать, а также создавать, изменять и удалять триггеры. Кроме того, здесь можно оценивать частоту использования триггеров в составных триггерах или контентных правилах.

> **Примечание**
>
> Используемые триггеры удалить нельзя.

Чтобы добавить триггер, щёлкните **Добавить**, на открывшемся экране укажите параметры триггера и щёлкните **Сохранить**.

Доступны следующие типы триггеров: **регулярное выражение**, **свойства документа** и **составной**.

### Триггеры регулярных выражений

Триггеры регулярных выражений позволяют контролировать содержимое передаваемых данных с помощью регулярных выражений Perl.

Для таких триггеров можно указать следующие параметры:

- **Имя** — имя триггера.
- **Описание** — описание триггера.
- **Регулярное выражение** — регулярное выражение Perl для поиска совпадений. Подробнее см. в руководствах Perl regular expressions quick start и Perl regular expressions tutorial.
- **Условие** — условие для определения совпадения с регулярным выражением:
  - **Меньше или равно** — число совпадений должно быть меньше заданного значения или равно ему.

    - **Равно** — число совпадений должно быть равно заданному значению.
    - **Больше или равно** — число совпадений должно быть больше заданного значения или равно ему.
    - **Между** — число совпадений должно находиться в заданном диапазоне значений.
    - **Точное совпадение** — весь проверяемый текст должен совпадать с регулярным выражением.
- **Значение** — число, заданное для проверки условия (для условия **Между** — диапазон).
- **Учитывать регистр** — различать строчные и прописные буквы при поиске совпадений.
- **Считать идентичные совпадения за одно** — объединять повторяющиеся совпадения в один результат.

## Триггеры свойств документа

Триггеры свойств документа предназначены для контроля передаваемых данных на основе их свойств.

Для таких триггеров можно указать следующие параметры:

- **Имя** — имя триггера.
- **Описание** — описание триггера.
- **Размер** — размер файла в байтах, килобайтах, мегабайтах или гигабайтах. Можно выбрать один из следующих вариантов:
    - **Не указан** — Не учитывать размер.
    - **Равен** — размер файла должен быть равен заданному значению.
    - **Меньше чем** — размер файла не должен превышать заданного значения.
    - **Больше чем** — размер файла должен превышать заданное значение.
    - **Между** — размер файла должен находиться в заданном диапазоне значений.

## Составные триггеры

Составные триггеры позволяют компоновать уже имеющиеся триггеры, включая составные, а также их группы с помощью логических операторов:

- НЕ — логическое отрицание одного из триггеров или одной из групп триггеров,
- И — необходимо срабатывание обоих триггеров или обеих групп триггеров,
- ИЛИ — необходимо срабатывание хотя бы одного из триггеров или одной из групп триггеров.

Для таких триггеров можно указать следующие параметры:

- **Имя** — имя триггера.
- **Описание** — описание триггера.
- **Составление триггера** — конструктор для совмещения триггеров с помощью логических операторов.
- **Результат** — итоговый триггер.

# USB-устройства

Данный справочник позволяет управлять списком USB-устройств, которые используются при создании правил белого списка USB-устройств в политиках.

В справочнике можно просматривать, фильтровать и сортировать, а также добавлять, переименовывать и удалять USB-устройства. Кроме того, здесь можно оценивать частоту использования USB-устройств в правилах белого списка USB-устройств.

> **Примечание**
>
> Используемые USB-устройства удалить нельзя.

USB-устройства можно добавлять как модели и как уникальные устройства:

- **Модель устройства** описывает все устройства одной и той же модели. Каждое устройство определяется по комбинации идентификатора производителя (VID) и продукта (PID).
- **Уникальное устройство** описывает одно конкретное устройство. Каждое устройство определяется по комбинации идентификатора производителя (VID), продукта (PID) и серийного номера. Если устройство не имеет серийного номера, его нельзя добавить как уникальное.

Устройство можно добавить двумя способами: вручную или из текстовых файлов с расширением .txt. При этом для каждого устройства необходимо задать имя и указать идентификатор.

Идентификатор обязательно должен содержать VID и PID устройства в формате Windows или Linux (см. далее) и пройти проверку на количество символов и их значение. Указывать серийный номер необязательно. Если он не указан, устройство будет добавлено как модель.

При загрузке списка USB-устройств из текстовых файлов каждое устройство должно быть описано на отдельной строке в формате ”имя идентификатор”. При этом имя и идентификатор должны быть разделены хотя бы одним пробелом или символом табуляции.

При добавлении устройств любым способом идентификаторы будут приведены к формату Windows.

Примеры идентификаторов в формате Windows:

- `USB\VID_1005&PID_B113` — Будет добавлена модель устройства (VID = 1005, PID = B113).
- `USB\VID_1005&PID_B113\0703647278A69F65` — Будет добавлено уникальное устройство (VID = 1005, PID = B113, серийный номер = 0703647278A69F65).

Примеры идентификаторов в формате Linux:

- `1005:B113` — Будет добавлена модель устройства (VID = 1005, PID = B113). При загрузке значение будет преобразовано в `USB\VID_1005&PID_B113`.
- `1005:B113:0703647278A69F65` — Будет добавлено уникальное устройство (VID = 1005, PID = B113, серийный номер = 0703647278A69F65). При загрузке значение будет преобразовано в `USB\VID_1005&PID_B113\0703647278A69F65`.
- `usb:v1005pB113d0100dc00dsc00dp00ic08isc06ip50in00` — Будет добавлена модель устройства (VID = 1005, PID = B113, остальное не учитывается). При загрузке значение будет преобразовано в `USB\VID_1005&PID_B113`.