Документация iBatyr Monitor

Выпуск 5.6

авг. 12, 2025

Оглавление

Глава 1

Введение

Возможности продукта

iBatyr Monitor – это программный комплекс для мониторинга рабочего времени сотрудников. Руководители компаний, сотрудники службы безопасности и администраторы сетей, использующие iBatyr Monitor , могут отслеживать практически все подозрительные события, происходящие на компьютерах предприятия, как в реальном времени, так и в ретроспективе. С помощью нашего программного комплекса Вы сможете реально оценить эффективность работы Ваших сотрудников, и узнать, на что они тратят рабочее время. Также это отличный инструмент для выявления инсайдеров и обнаружения утечки конфиденциальных данных.

- полный мониторинг сетевого трафика (в том числе шифрованного), корпоративной электронной и вебпочты (с вложениями), интернет мессенджеров, посещения веб-сайтов;
- мониторинг работы с файлами (файловая система, буфер обмена, копирование файлов на внешние носители, сетевые диски, анализ данных в архивах);
- мониторинг активности сотрудников на рабочем месте;
- мониторинг печати документов;
- удаленное подключение к рабочему столу;
- блокировка сайтов, запуска приложений и подключения USB-устройств;

- доступ к административной панели из любой точки мира, где есть интернет, через веб-интерфейс;
- мощная система многомерного анализа действий пользователя на основе технологии OLAP;
- детектор аномалий поведения пользователей;
- система оповещения о нарушении политик безопасности предприятия;
- гибкая система настройки сбора информации;
- разграничение прав доступа к накопленной информации по группам и пользователям;
- наглядное отображение полученных данных в табличном виде, в виде графиков и диаграмм.

Архитектура

iBatyr Monitor является клиент-серверным приложением и состоит из двух основных частей: Сервер и Агенты.

Сервер

Серверная часть предназначена для сбора, хранения, анализа и отображения собранной от агентов информации. Устанавливается на машину под управлением ОС Ubuntu Server.

Сервер использует для базы данных:

- PostgreSQL – основное хранение,
- *ClickHouse* – вспомогательное, может отсутствовать.

Доступ к данным и управление мониторингом осуществляется через веб-интерфейс (веб-консоль), работа с которым возможна с любого компьютера при подключения к серверу через интернет или локальную сеть. Для загрузки веб-интерфейса рекомендуем использовать современный браузер Chrome или Firefox.

Агенты

Агент представляет собой службу, запущенную на рабочей станции. Он собирает и передаёт на сервер информацию о событиях на компьютере и действиях сотрудника. Работа агента происходит в скрытом режиме незаметно для пользователя. Данные накапливаются в локальной базе, а после передачи на Сервер автоматически удаляются. Если нет связи с сервером, то сбор продолжается, но по достижении лимита на максимальный размер локальной базы Агент начинает циклично перезаписывать информацию, затирая самые старые данные.

Установка агента для ОС семейства Windows производится локально на рабочем месте сотрудника или по сети с помощью средств удаленной установки.

Установка Linux-агента выполняется путём запуска инсталлятора с правами root.

Установка агента для macOS производится с компьютера, на котором будет работать mac-агент или с помощью удалённого рабочего стола.

Данные передаются по шифрованному каналу (openSSL) пакетами, максимальный размер и интервал отправки которых задаются в настройках. При установке можно установить адреса и порты основного и альтернативного серверов. Если основной сервер недоступен, Агент будет передавать данные на альтернативный адрес. Таким образом можно обеспечить связь с сервером при выходе за рамки локальной сети предприятия (ноутбуки мобильных сотрудников).

План установки

Чтобы установить iBatyr Monitor воспользуйтесь *инструкцией по установке*.

Основные этапы установки:

1. Ознакомьтесь с *системными требованиями*.

2. Выберите подходящий *способ установки сервера*.
3. Настройте исключения антивируса.
4. *Установите агенты мониторинга*.
5. Настройте *конфигурации* и *исключения для антивирусов*.

При возникновении вопросов специалисты *технической поддержки* проконсультируют вас и при необходимости подключатся к вашему серверу для помощи и настройки. *Инструкция для удаленного подключения*.

Работа с программой

После установки и настройки проверьте, что события приходят на сервер.

В *Линзе событий* веб-консоли должны появиться события, которые агент отправляет на сервер. Если событий нет, проверьте аппаратные межсетевые экраны, программные шлюзы-файрволлы и другие устройства, которые могут блокировать трафик от агента к серверу.

Если события с компьютеров пользователей пришли на сервер, изучите полученные данные:

- *Стандартные типы отчётов*
- *Типовые сценарии поиска информации*
- *Что нового в версии 5.6*

Глава 2

Быстрый старт

Добро пожаловать в iBatyr Monitor ! В этом разделе вы найдете основные шаги для запуска и настройки системы.

2.1 План работы

1. *Установка сервера iBatyr Monitor*
2. *Настройка сети*
3. *Первый вход в веб-консоль и активация*
4. *Установка агентов iBatyr Monitor Enteprise*
5. *Настройка мониторинга агентов под пользовательскую архитектуру ПО*
6. *Первые шаги в работе с данными*
7. *Настройка уведомлений и отчетов*
8. *Основные настройки доступа к административной панели iBatyr Monitor*

2.2 Установка сервера

Перед установкой сервера iBatyr Monitor убедитесь, что ваше оборудование соответствует *Системным требованиям*.

Примечание: Для установки сервера используйте *одну из инструкций по установке*.

2.2.1 Настройка сети

После установки сервера настройте сетевое взаимодействие.

Сервер использует порт **443** для безопасного соединения через протокол HTTPS. Для смены портов сервера обратитесь к инструкции *Смена стандартного порта*.

Настройки сети зависят от расположения агента и сервера в сети:

- *одна подсеть*: дополнительная настройка не нужна;
- *разные подсети*: убедитесь, что *сетевые шлюзы не блокируют указанные в системных требованиях порты*;
- *разные сети с передачей данных через интернет*: *подключите агент к серверу из внешней сети*.

Для проверки доступности сервера откройте в браузере на ПК с агентом веб-консоль по адресу **https://внешний_ip:443**.

Вы можете установить агенты через VPN. Принципы настройки для VPN такие же, как и для локальных сетей.

2.3 Первый вход

Внимание: Если вы работаете в закрытом контуре, перед входом получите тестовый ключ. Для этого отравьте запрос на почту *sales@ibatyr.kz*.

После установки сервера войдите в веб-интерфейс:

1. Зайдите в Linux-консоль и авторизуйтесь с помощью указанных при установке учетных данных.

   Если вы забыли пароль, установите новый:

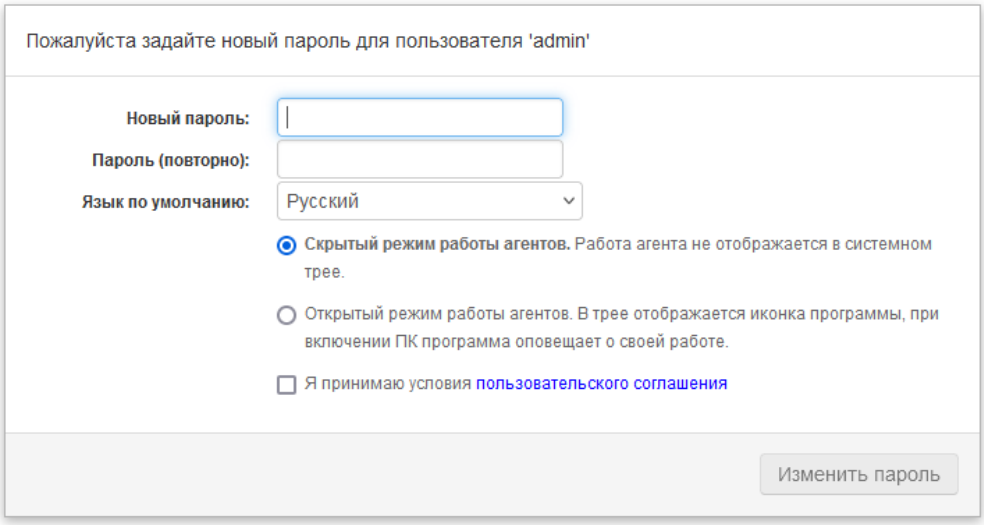
   ```
   sudo ibatyr passwd NEW_PASSWORD
   ```

2. В терминале введите команду для вывода IP-адреса:

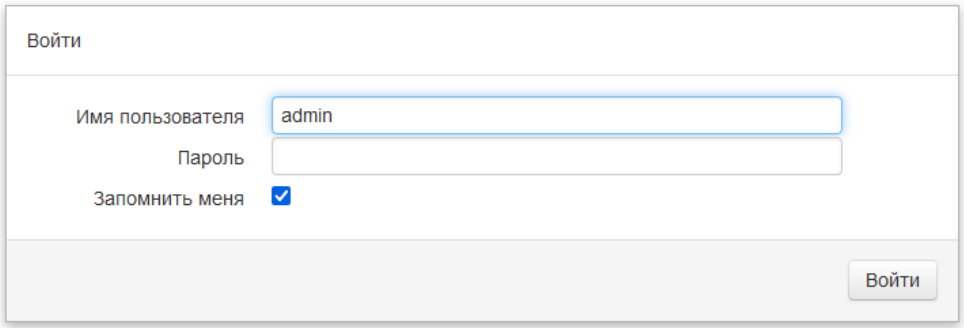
   ```
   ip a
   ```

3. Откройте браузер и введите в адресной строке IP-адрес из строки **inet**.

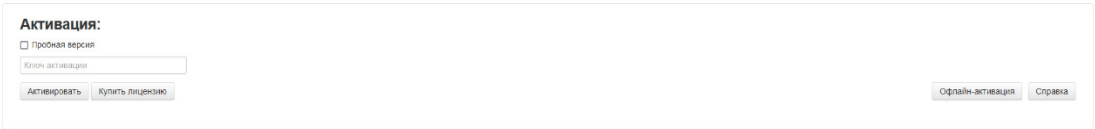
4. Откроется окно для создания пароля веб-консоли.



5. Задайте пароль для пользователя веб-консоли *admin*. Пароль должен содержать латинские буквы и цифры. Все требования к паролю перечислены в статье *Пароль веб-консоли*. Сохраните пароль в безопасном месте.
6. Выберите режим работы агентов и нажмите **Изменить пароль**.
7. В окне входа введите *admin* и только что созданный пароль, нажмите **Войти**.



Откроется окно активации.



2.4 Активация

В окне активации:

1. Введите регистрационный ключ в поле **Ключ активации**.
2. Если у вас пробная версия, поставьте флажок **Пробная версия** и введите регистрационный e-mail.
3. Нажмите **Активировать**.

После активации откроется веб-интерфейс сервера iBatyr Monitor.

Примечание: Если вы используете браузер Chrome с включенной темной темой в **chrome://flags/** → **forced_dark**, выберите для веб-интерфейса **Светлую** или **Классическую** тему в разделе **Меню** (**Admin**) → **Тема**.

2.5 Установка агентов

В веб-консоли iBatyr Monitor перейдите в раздел **Панель управления** → **Компьютеры** и нажмите **Скачать агент**. Выберите версию агента, подходящую для вашей системы.

Предупреждение: Перед установкой агентов *добавьте исключения в антивирус*. Если этого не сделать, антивирус заблокирует подключение агента и на сервер iBatyr Monitor не будут поступать данные.

Для установки агента следуйте одной из инструкций в разделе *Установка агентов*.

Перед установкой сервера iBatyr Monitor убедитесь, что ваше оборудование соответствует *Системным требованиям*.

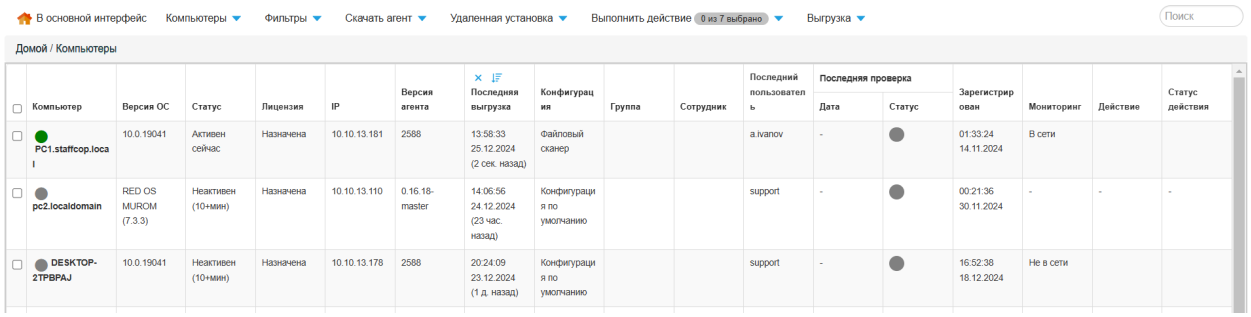
2.5.1 Настройка мониторинга агентов

После установки агент автоматически регистрируется на сервере iBatyr Monitor , если есть свободные лицензии.

Чтобы проверить успешную регистрацию агента:

1. Откройте веб-консоль.
2. Перейдите в меню **Панель управления** → **Компьютеры**.
3. В списке агентов появится новый агент. Имя агента будет автоматически считано с имени ПК, на котором он установлен. Регистрация агента может занять до 5 минут.

Пример списка агентов:



2.5.2 Присвоение конфигурации

После регистрации агенту присваивается **Конфигурация по умолчанию**. Агент использует эту конфигурацию, чтобы отслеживать события на рабочей станции пользователя.

Конфигурация по умолчанию позволяет:

- учитывать рабочее время по активности работы в приложениях и сайтах;
- фиксировать нажатия клавиш (кейлоггер);
- собирать информацию по авторизации пользователей;
- делать снимок экрана каждые 5 минут.

Конфигурацию можно изменить.

2.5.3 Как изменить конфигурацию

Конфигурация по умолчанию оптимальна по производительности. Если вы хотите мониторить все действия пользователей, назначьте агентам конфигурацию **Полный контроль**:

1. В меню **Панель управления** → **Конфигурация компьютеров** в списке конфигураций выберите **Полный контроль**.
2. Откройте секцию **Назначение агентов**.
3. Назначьте выбранным агентам конфигурацию.
4. Сохраните изменения.

Новые настройки применятся в течение 3—5 минут.

Примечание: Подробнее об изменении конфигурации читайте в статье *Как сменить конфигурацию*.

2.6 Первые шаги в работе с данными

Примечание: Перед началом работы с веб-интерфейсом ознакомьтесь *с основными элементами веб-интерфейса*.

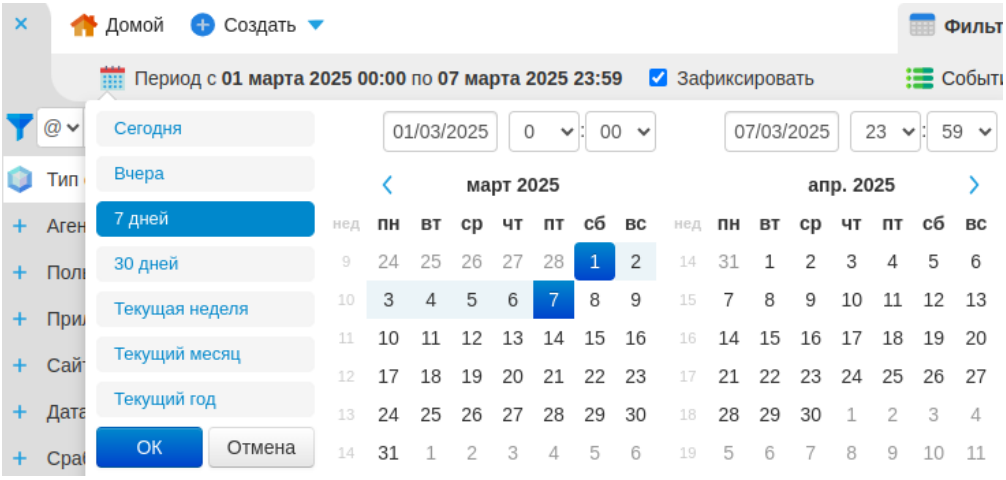
Для работы с полученными от агентов данными используются вкладки *Конструктор* и *Политики*.

Основной принцип работы заключается в настройке фильтров с помощью флажков в **Конструкторе**.

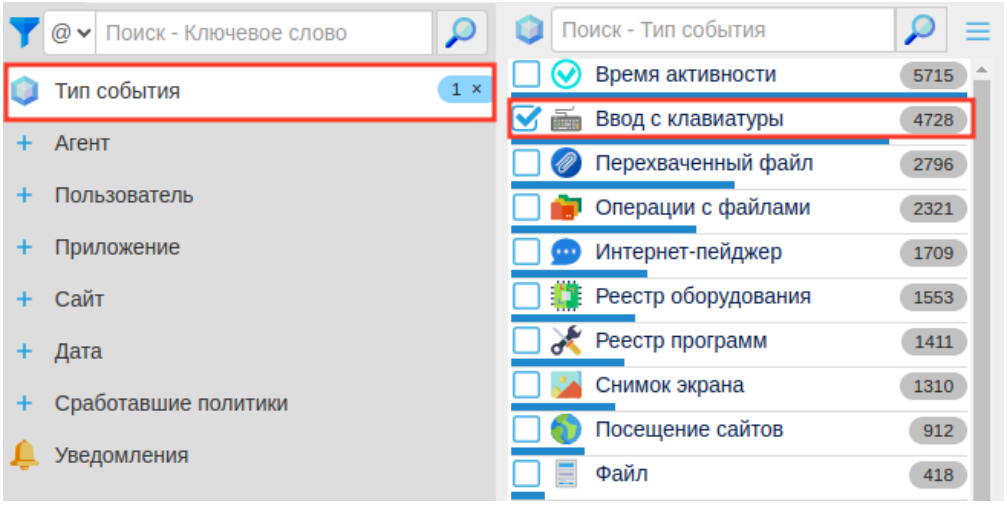
Конструктор содержит основные измерения по категориям: событие, пользователь, компьютер, сеть и так далее. Заданный набор параметров фильтрации можно сохранить с помощью панели фильтров. Подробнее — в статье *Навигационная панель фильтров*.

Пример работы:

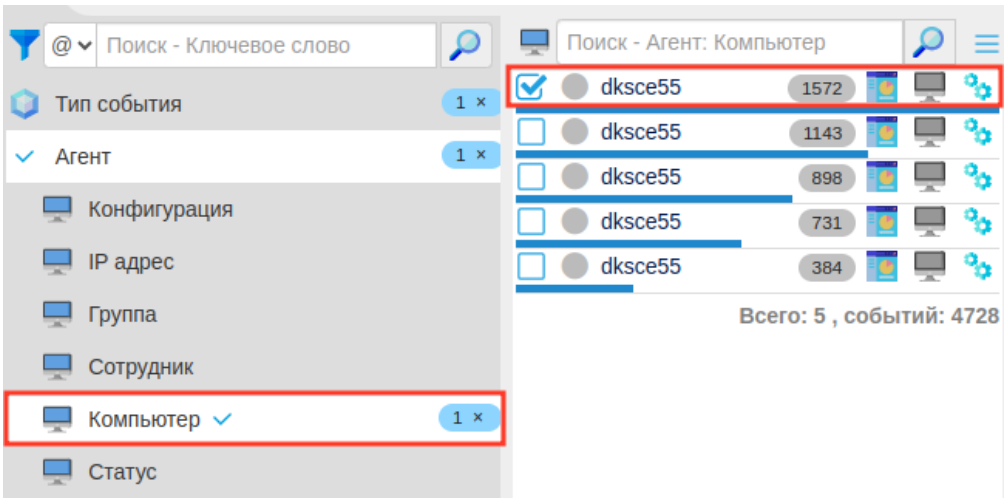
1. Выберите в датапикере диапазон событий — **7 дней**.



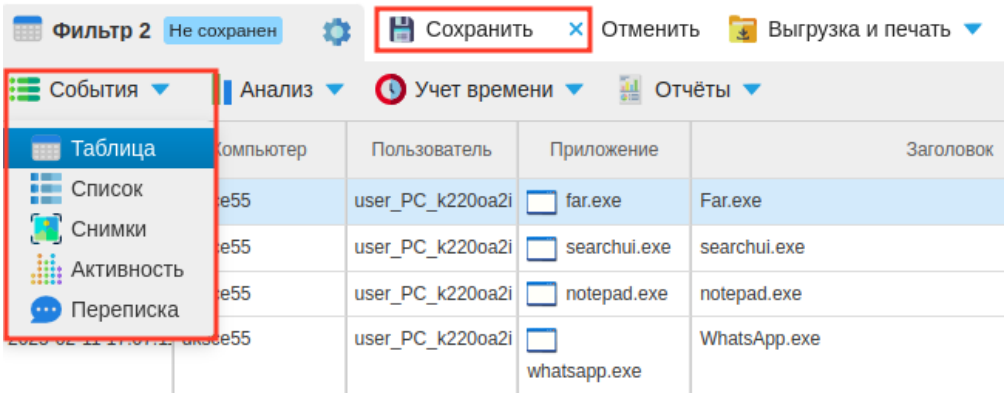
2. В **Конструкторе** выберите измерение **Тип события**.
3. В списке значений в соседней колонке выберите тип **Ввод с клавиатуры**.



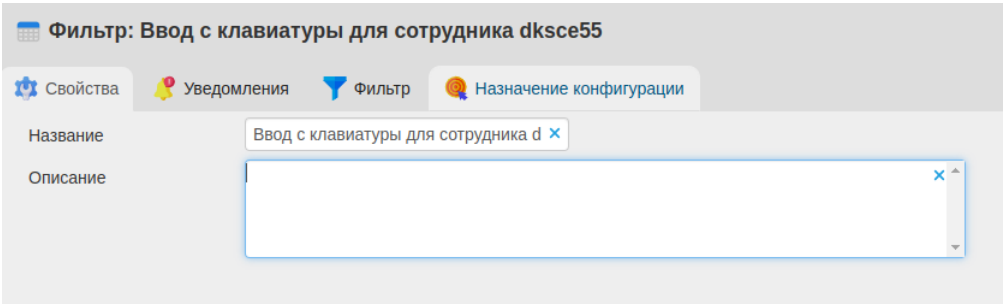
4. В **Конструкторе** выберите измерение **Агент**, а в списке значений — компьютер агента.



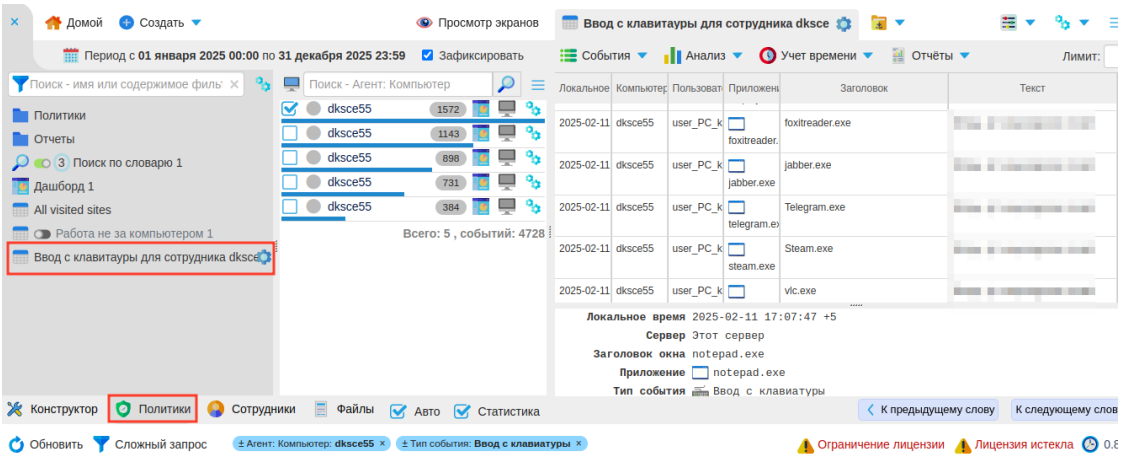
5. *В Линзе* нажмите на **События** и выберите **Таблица**.
6. На верхней панели нажмите **Сохранить**. Откроется модульное окно.



7. Задайте имя фильтру в модульном окне.



8. Перейдите во вкладку **Политики** и выберите только что созданный фильтр. В результате внизу страницы отобразятся параметры фильтрации **Агент** и **Ввод с клавиатуры**. В таблице событий останутся только события **Ввод с клавиатуры** для выбранного агента.



2.7 Отчеты и уведомления

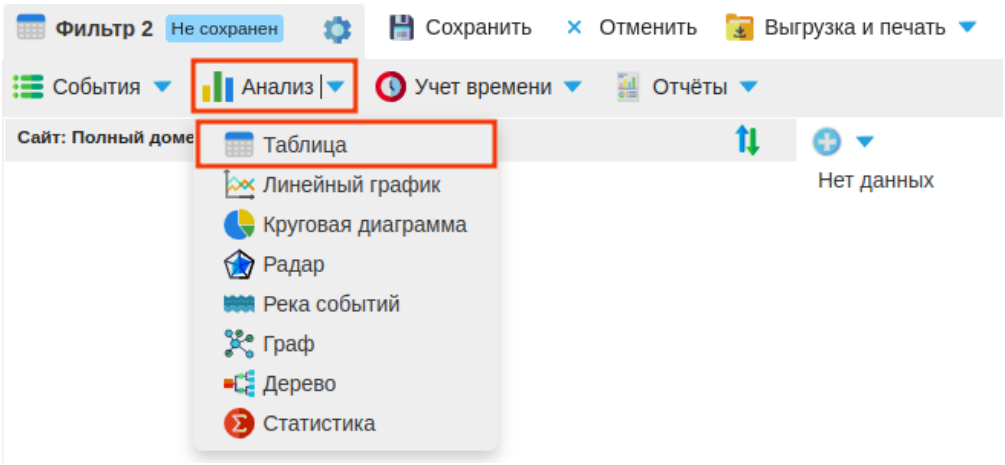
В меню Конструктора представлено два режима просмотра:

- информации — для пунктов меню **События**;
- отчетов — остальных пунктов, которые представляют собой шаблоны отчетов.

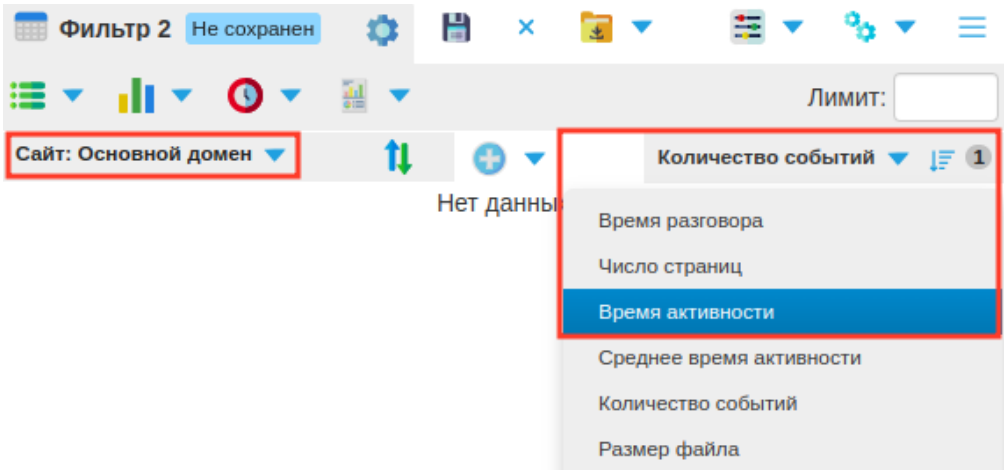
2.7.1 Примеры работы с данными

Чтобы выгрузить таблицы по посещению сайтов:

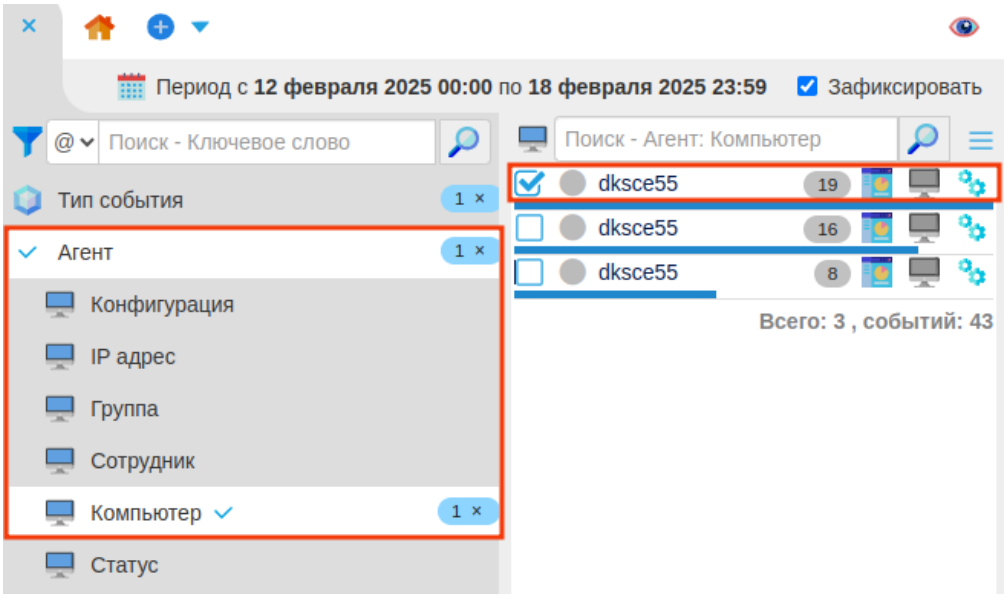
1. Перейдите на вкладку **Конструктор** и в меню **Линзы** нажмите **Анализ**.
2. Выберите **Таблица**.



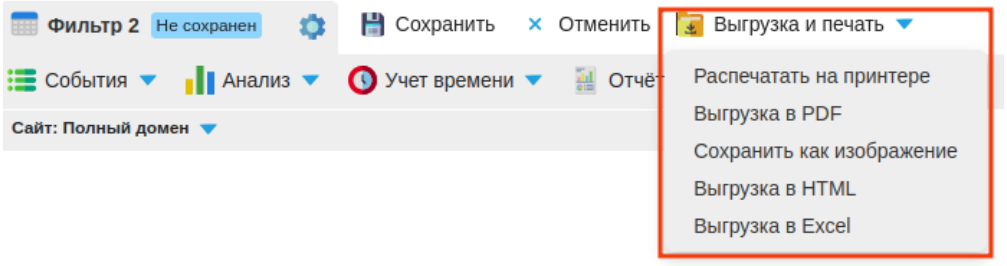
3. В группировке по измерению измените **Агент: Компьютер** на **Сайт: Основной домен**.
4. В параметре **Мера** выберите **Время активности**.



5. В **Конструкторе** выберите измерение **Агент**, а в списке значений — ПК агента.



6. Нажмите **Выгрузка и печать** в меню **Линзы** и выберите формат файла для скачивания, начнется скачивание.



Вы можете настроить отправку отчетов на почту:

1. В меню **Линзы** нажмите **Сохранить**, откроется модульное окно фильтра.
2. Задайте название фильтра, например *Отправка недельного отчета по активности*.
3. Перейдите на вкладку **Уведомления** и выберите **Активировать уведомления**.

4. Укажите, в каком виде хотите получать отчёты:

- при выборе пункта **Новые отчеты** будут приходить в формате HTML при каждом срабатывании фильтра;
- при выборе одного из периодов *Ежедневно/Еженедельно/Ежемесячно* отчёты будут приходить в почту в PDF-вложении.

После сохранения фильтра на ваш e-mail придет тестовый отчет с примененными фильтрами.

Примечание: Для отправки отчетов *настройте параметры почты*.

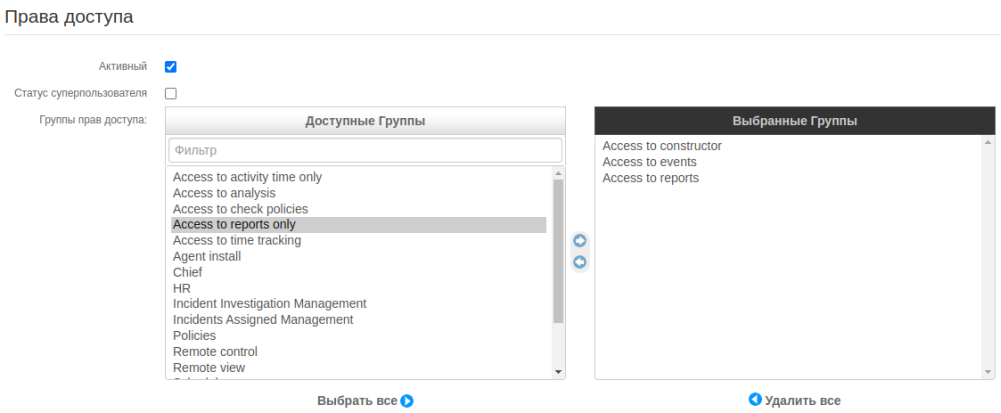
2.8 Настройка администраторов веб-консоли

В меню **Админ** создайте учетную запись и задайте права. Подробнее — в статье *Администраторы*.

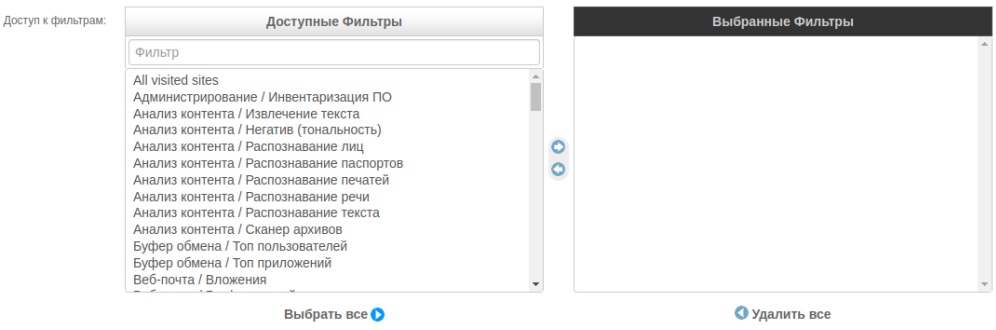
Например: вы хотите скрыть меню **Админ**, ограничить просмотр пользователей и сделать доступным все фильтры и отчеты.

Выполните:

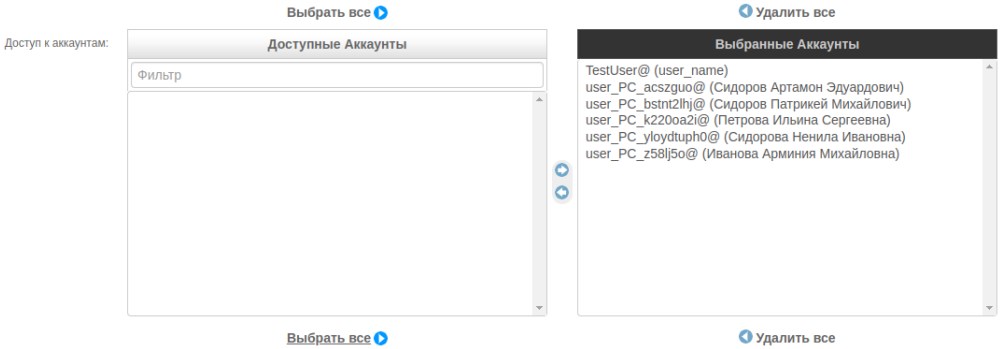
1. В меню **Панель управления** выберите **Администраторы**.
2. С помощью кнопки **Добавить** внизу страницы добавьте новую учетную запись.
3. В новой учетной записи задайте права:
   - в **Группах** дважды нажмите на **Access to events**, **Access to constructor**, **Access to reports**, чтобы переместить их в колонку **Выбранные группы**:



   - в **Фильтрах по умолчанию** все фильтры и отчеты доступны для работы:



- в **Аккаунтах** переведите пользователей из колонки **Доступные** в колонку **Выбранные** с помощью кнопки **Выбрать все**. Администратор будет видеть только этих пользователей:



4. Сохраните изменения.

Глава 3

Руководство администратора

3.1 Системные требования

Внимание: Соблюдайте требования для стабильной работы сервера, баз данных и компонентов системы. Невыполнение требований может вызвать нестабильную работу системы.

3.1.1 Сервер и базы данных

- *Требования к серверу*
- *Требования к базе данных*
  - *Диск для основной БД и сервера приложений*
  - *Диск для хранения файлов*
  - *Диск для хранения файлов видеозаписи*
  - *База данных ClickHouse*
  - *Рекомендации к администрированию БД*
- *Выбор конфигурации сервера*

Внимание: Соблюдайте требования для стабильной работы сервера, баз данных и компонентов системы. Невыполнение требований может вызвать нестабильную работу системы.

Требования к серверу

Мощность процессора, объем оперативной памяти и дисков зависит от количества агентов.

Операционная система

Сервер iBatyr Monitor поддерживают:

- Ubuntu Server 18.04;
- Ubuntu Server 20.04;
- Ubuntu Server 22.04;

Предупреждение: При обновлении операционной системы сервера из-за особенностей работы PostgreSQL обязательна *реиндексации баз данных*.

Оперативная память и процессор

Требования для архитектуры **x86/x64** с учетом количества агентов:

Агентов	RAM	CPU
10	4	2
50	16	4
100	32	8
200	48	10
500	64	10
1000	96	14

Оптимизация производительности

Начиная с версии 4.9 в iBatyr Monitor добавлен новый механизм загрузки данных (ETL), который значительно снижает нагрузку на процессор и позволяет эффективнее использовать дисковую подсистему.

Не рекомендуется устанавливать на сервер дополнительные ресурсоемкие сервисы и приложения, кроме следующих:

- Grafana — сервис анализа метрик нагрузки, который устанавливается командами сервиса приложений вместе с предустановленными метриками и сборщиками метрик.
- Zabbix — сторонее решение для анализа метрик нагрузки.
- Антивирусное ПО, в исключения которого необходимо *добавить* сервисы iBatyr Monitor и его директории *postgresql* и *ibatyr*.

Требования к базе данных

iBatyr Monitor поддерживает:

- Postgresql 11 и 15;

- ClickHouse*.

Примечание: *ClickHouse* — дополнительная база данных для улучшения скорости формирования отчетности. При установке iBatyr Monitor предоставляется актуальная версия ClickHouse.

Используйте **SSD** для хранения баз данных. **SSD** обеспечивают быстрый доступ к БД за счет высокой скорости записи-чтения. Файлы не требуют скорости, поэтому их можно хранить на **HDD**.

Примечание: Если вы используете 10–50 рабочих станций, нет необходимости разделять базу данных и файловое хранилище из-за небольшого объема данных.

Диск для основной БД и сервера приложений

Для оптимальной работы подсистемы хранения данных:

- используйте твердотельные накопители **NVMe** со скоростью не менее 1500 МБ/с,
- обеспечьте **IOPS** не менее 5000 операций ввода-вывода в секунду.

Внимание: Размещение БД на медленных дисках увеличивает риск нестабильной работы системы.

При средних настройках каждый пользователь генерирует около 350 МБ событий в месяц.

Буфер спуллера данных */var/lib/ibatyr/etl* рекомендуется размещать на быстром диске.

Рекомендации для базы данных приведены ниже.

Агентов	Месяц хранения	3 месяца хранения	12 месяцев хранения
10	34 GB (БД и ФХ)	101 GB (БД и ФХ)	402 GB (БД и ФХ)
50	170 GB (БД и ФХ)	502 GB (БД и ФХ)	2 TB (БД и ФХ)
100	35 GB	103 GB	411 GB
200	69 GB	206 GB	821 GB
500	171 GB	513 GB	2 TB
1000	342 GB	1,13 TB	4,1 TB

Диск для хранения файлов

При средних настройках сбора данных один пользователь генерирует около 4 ГБ файлов в месяц.

Объемы данных приведены для включенных политик безопасности:

- съемка экрана каждые 5 мин;
- смена фокуса на экране Full HD — 5 мин;
- перехват переписки в мессенджерах и почте.

Дополнительный перерасчет требуется при записи видео экрана, , аудио и пакетных снимков.

Агентов	Месяц хранения	3 месяца хранения	12 месяцев хранения
10	34 GB (БД и ФХ)	101 GB (БД и ФХ)	402 GB (БД и ФХ)
50	170 GB (БД и ФХ)	502 GB (БД и ФХ)	2 TB (БД и ФХ)
100	300 GB	900 GB	3,6 TB
200	600 GB	1,8 TB	7,2 TB
500	1,5 TB	4,5 TB	18 TB
1000	4 TB	12 TB	36 TB

Диск для хранения файлов видеозаписи

Требования приведены для записи одного экрана Full HD в течении восьмичасового рабочего дня. При других условиях измените объёмы.

Агентов	Месяц хранения	3 месяца хранения
10	350 GB	1050 GB
50	1750 GB	5,2 TB
100	3,5 TB	10,5 TB
200	7 TB	21 TB
500	17,5 TB	52,5 TB
1000	35 TB	105 TB

Примечание: Суммарное значение IOPS должно быть не ниже 5000 операций.

База данных ClickHouse

Вспомогательная база данных, которая предназначена для улучшения скорости загрузки данных в веб-консоли сервера. Получает данные из основной базы данных.

Используйте ClickHouse, если у вас:

- более 100 пользователей,
- срок хранения данных более 3-х месяцев.

Объем БД рассчитывается в соотношении 40–50% от объемов данных основной базы данных.

Агентов	RAM	Месяц хранения	3 месяца хранения	12 месяцев хранения
100	10 GB	18 GB	54 GB	216 GB
200	12 GB	36 GB	108 GB	432 GB
500	14 GB	90 GB	270 GB	1080 GB
1000	16 GB	180 GB	540 GB	2160 GB

Примечание: Для хранения данных в ClickHouse требуется диск NVMe со скоростью чтения-записи 1500 МБ/с и суммарное значение IOPS не ниже 5000 операций.

Рекомендации к администрированию БД

При превышении 1 ТБ базы данных:

1. **Разделите данные на горячее и холодное хранение**. Перенесите часть данных в холодное хранилище с защищенным доступом через адрес сервера. Веб-консоль сервера будет отображать только выбранную базу.
2. **Делайте бэкап базы данных еженедельно**. Сервер записывает данные в файловое хранилище, при создании бэкапа рекомендуется делать копию файлов в файловом хранилище.
3. **Выполняйте автоочистку**. Применяйте к базе данных VACUUM и ANALYZE каждые 2–3 месяца.

Выбор конфигурации сервера

Ссылки на профильные ресурсы для подбора серверного оборудования:

- https://servermall.ru/
- https://forpro.ru/

3.1.2 Сеть

Для корректной работы сервиса iBatyr Monitor настройте открытые порты и учитывайте ширину канала передачи данных между устройствами.

Порты системы

Предупреждение: Откройте **80** порт, иначе активация сервера будет невозможна ни в онлайн-, ни в офлайн-режиме.

Порт	Назначение
TCP:80	Начальная настройка и активация, установка обновлений. Не требуется для работы.
TCP:443	Доступ к серверу, передача данных от агентов, модуль удалённого управления, установка обновлений. Можно изменить на уникальный для компании порт.
TCP:22	SSH-доступ к серверу. Используется для технических работ.
TCP:445 **UDP:137** **UDP:138** **UDP:139**	Работа утилиты удалённой установки, обновления, удаления агента. Должны быть открыты на стороне рабочей станции.
TCP:445	Используется для удаленной установки агента со стороны сервера. Должна быть открыта на рабочей станции с установленным агентом.
TCP:9090	Передает данные на сервер распознавания. Порт открывается на сервер распознавания.

Требования к каналу передачи

Ширина канала должна быть рассчитана с учётом объёма передаваемых данных. При использовании мониторинга рабочего стола, файлового сканера, трансляции видео с рабочего стола и рекомендуется не менее **1** ГБ/с.

При основных настройках один агент генерирует около 100—200 Кбайт/с.

Нагрузка от агента на сетевой трафик возрастает:

- при включении файлового сканера, снимков экрана, видеозаписи с экрана и ,
- удаленном подключении к рабочему столу или онлайн-записи экрана — на 2 МБ/сек.

3.1.3 Терминальный сервер

Терминальный сервер оптимизирует ресурсы организации и позволяет централизованно управлять рабочими местами.
Вычислительная нагрузка переносится на отдельный сервер, а пользователи подключаются к нему через простые устройства или тонкие клиенты.

Внимание: Соблюдайте требования для стабильной работы сервера, баз данных и компонентов системы. Невыполнение требований может вызвать нестабильную работу системы.

Программное обеспечение

Операционная система:

- Windows Server 2008;
- Windows Server 2008 R2;
- Windows Server 2012 R2;
- Windows Server 2016;
- Windows Server 2019;
- Windows Server 2022.

Примечание: Для работы агента должна быть запущена **Служба терминалов** (**TermService**) и *настроены исключения антивируса.*

Оборудование

Требования к оборудованию зависят от конфигурации и количества пользователей.

Примечание: Терминальные сессии не требуют много процессорного времени. Рекомендуется выделять по одному ядру на 6–8 сессий. Windows Server сама по себе требует около 2 ГБ RAM, а один пользователь во время терминальной сессии — примерно 700 МБ.

Ниже перечислены требования для конфигурации с полным контролем без *пакетных снимков экрана*, *записи видео экрана* и *сканирования*.

tabularytabulary

	Количество пользователей на ТС
	10
	50
	100
	200
	500

Включение модулей *Пакет снимков экрана* и *Запись видео экрана* потребует дополнительной оперативной памяти:

- 200 МБ на контролируемого пользователя для записи пакетных снимков экрана.
- 1000 МБ на контролируемого пользователя для записи офлайн-видео.

Использование этих модулей не рекомендуется на АРМ с требованиями ниже указанных. Расчет приведен с использованием офлайн-видеозаписи по каждому пользователю.

tabularytabulary

	Количество пользователей на ТС
	10
	50
	100
	200
	500

Сканирование не требует постоянных дополнительных мощностей — процесс выполняется разово. Рекомендуется использовать его при отсутствии пользовательской активности.

Дисковая подсистема

Во время работы сервера происходит множество операций чтения-записи в секунду (IOPS). Правильный выбор жестких дисков обеспечивает быстродействие серверов.

Если использовать терминальный сервер как рабочую среду для работы с тонкими клиентами, дисковая нагрузка на сервер значительно возрастет. Например, при 30 пользователях на терминальном сервере с использованием RAID 1 и дисками SATA 3 Гбит/с диски вроде WD Velociraptor не обеспечивают комфортную работу с почтой и активном серфинге в интернете.

Примечание: Для терминальных серверов используйте **SSD**- или **SAS**-диски.

Используйте *аппаратный дисковый контроллер* со своей энергонезависимой памятью вместо программного. Современные серверы имеют хорошие встроенные контроллеры, например HP SmartArray

и DELL PERC. Однако некорректно использовать «набортные» решения при серьёзной нагрузке, когда требуется максимальная производительность.

Сеть

Агент генерирует 100–200 Кбит/с сетевого трафика, а при включении опций *Запись видео* и *Удаленное управление* — до 2 Мбит/с на каждого пользователя.

Пользователи

Для мониторинга учетных записей отдельных пользователей *настройте агент на терминальном сервере*.

3.1.4 Сервер распознавания

Внимание: Соблюдайте требования для стабильной работы сервера, баз данных и компонентов системы. Невыполнение требований может вызвать нестабильную работу системы.

Системные требования для *сервера графического распознавания*:

Рекомендуемые системные требования	Описание
Операционная система	• Ubuntu 18.04; • Ubuntu 20.04; • Ubuntu 22.04;
Дополнительное программное обеспечение	• Python 3.7; • Python 3.7-venv; • libpoppler-cpp0v5 poppler-utils libsm6 tesseract-ocr.
Процессор	Intel или AMD с поддержкой AVX инструкций. Количество потоков/ядер зависит от числа пользователей. Одно ядро способно обработать до 28 800 изображений за сутки. В среднем пользователь генерирует около 2000 изображений в день.
Размер диска	до 100 ГБ.
Диск	NVME со скоростью чтения-записи не менее 1500 МБ/сек.
IOPS	не менее 5000 операций ввода-вывода в секунду.
Оперативная память	Используется для распознавания в зависимости от размера и сложности файла. Рекомендуется рассчитывать до 80 МБ на графическое изображение или снимок экрана, до 300 МБ.

Ниже приведены требования к процессору и оперативной памяти для обработки всех данных за сутки, включая тяжелые файлы:

Агентов	Среднее количество изображений	CPU	RAM
10	20 000	2	4 GB
50	100 000	6	6 GB
100	200 000	9	6 GB
200	400 000	16	8 GB
500	1 000 000	37	16 GB
1000	2 000 000	72	24 GB

Расчет количества потоков/ядер и объёма оперативной памяти

Ниже представлены расчеты для определения системных требований.

Примечание: Включенная опция *Снимки экрана по смене фокуса окна* при выключенной *Делать скриншоты только при смене процесса* генерирует огромное количество скриншотов.

Как правило, у пользователя генерируется от 1500 до 2000 скриншотов в день, в зависимости от его активности и количества мониторов. Одно ядро в день может обработать до 28800 скриншотов.

Расчёт производится для 300 ПК при включенном модуле *Снимки экрана*.

Таким образом, количество скриншотов в день:

```
2000 * 300 = 600 000 скриншотов
```

Итоговое количество скриншотов делим на количество изображений, обрабатываемых одним ядром:

```
600 000 / 28 800  21 потоков/ядер
```

Расчёт объёма оперативной памяти

В среднем для обработки изображения требуется около 80 МБ на ядро. Для расчёта объёма оперативной памяти, умножим количество ядер/потоков на объём памяти для одного ядра и одного потока:

```
21*80 = 1680 МБ
```

Параллельно работают конвертеры изображений и сама операционная система сервера. В зависимости от получаемых данных они требуют от 1 до 4 ГБ RAM.

Таким образом, для оптимального функционирования системы под большой нагрузкой, используйте на сервере от 8 ГБ оперативной памяти.

3.1.5 Модуль Видеоконтроль

Особенности модуля *Видеоконтроль*:

- требователен к месту на жёстком диске;
- работает только при наличии связи с сервером;
- объём дискового пространства для записи напрямую зависит от количества мониторов на рабочих местах пользователей.

Один месяц работы модуля **Видеоконтроль** для мониторов с разным разрешением:

tabularytabulary

N	1024x768	1980x1080
1	9,3 GB	34,6 GB
50	465 GB	1,73 TB
100	930 GB	3,46 TB
200	1,86 TB	6,92 TB

Учитывайте **Пропускную способность канала**:

- агент генерирует 100–200 Kbps сетевого трафика,
- при включении опций **Запись видео** и **Удаленное управление** — до 2 МБ/с на терминальных серверах от одного пользователя.

3.1.6 Рабочая станция

Общие требования

Параметр	**Значение**
RAM	до **2** ГБ
Пропускная способность	**200** Kbps
• При включении опций: – *Запись видео*, – *Удаленное управление*.	до **2** Mbps

Windows-агент

Поддерживается работа 32- и 64-битных систем:

- Windows 7,
- Windows 8,
- Windows 8.1,
- Windows 10,
- Windows 11.

Примечание: Начиная с версии 5.3 поддержка агента для Windows XP прекращена. Последняя рабочая версия агента для Windows XP — 2531.

Дополнительное ПО

tabularytabulary

ПО
Windows 7
Windows 10

Требования к оборудованию

Работа Windows-агента требует на АРМ:

- CPU от **2** ядер,
- RAM от **2** GB,
- предпочтительно **SSD**-диск.

Остальные требования зависят от конфигурации.

tabularytabulary

Конфигурация
Полный контроль
Офлайн-запись видео экрана
Пакетные снимки экрана
Сканирование файлов

Терминальный сервер

Требования к терминальному серверу перечислены *в инструкции*.

Установка

Для установки агента на Windows *выберите способ установки и следуйте инструкции*.

macOS-агент

Агент поддерживает:

- macOS 10.15 (Catalina),
- macOS 11.x (BigSur),
- macOS 12.x (Monterey),
- macOS 13.x (Ventura),
- macOS 14.x (Sonoma).

Примечание: Поддержка работы агентов на macOS 10.13 High Sierra и macOS 10.14 Mojave прекращена. Агент запустится на машинах под управлением версий 10.13 (High Sierra) и 10.14 (Mojave), но его функционал будет ограничен.

Дополнительное ПО

Дополнительные пакеты не требуются.

Требования к оборудованию

Работа macOS-агента требует на АРМ:

- CPU от **2** ядер,
- RAM от **4** GB.

Дополнительного расширения мощностей CPU и RAM не требуется, если агент работает на конфигурации без высокопроизводительных компонентов.

tabularytabulary

	Конфигурация
Полный контроль	
Сканирование файлов	

Агент не требует дополнительной оперативной памяти.
Учитывайте использование других ресурсоемких программных продуктов.

Установка

Для установки агента на macOS *следуйте инструкции*.

Linux-агент

Агент поддерживает:

- CentOS,
- Ubuntu,
- Debian,
- Astra Linux,
- РЕД ОС,
- Arch Linux,
- Rosa Linux,
- ALT Linux.

Примечание: Поддерживается только графическая система X Windows System, версия 11 (X11). Протокол Wayland не поддерживается.

Дополнительное ПО

tabularytabulary

Требование	Комментарий
glibc	от *2.23* и выше.
Ядро	от *4.15* и выше.
Архитектуры	*i686*, *x86_64*, *arm64*.

Примечание: Запуск агента на более низких версиях возможен, но не гарантируется. При несовместимости отдельных подсистем агента с ОС функционал агента сократится без потери общей работоспособности. Для решения проблем совместимости обратитесь в службу технической поддержки.

Требования к оборудованию

Работа Linux-агента требует на APM:

- CPU от **2** ядер,
- RAM от **4** GB.

Дополнительного расширения процессорных мощностей CPU не требуется, если агент работает на конфигурации без высокопроизводительных компонентов.

tabularytabulary

Конфигурация
Полный контроль
Сканирование файлов

Агент не требует дополнительной оперативной памяти.
Учитывайте использование других ресурсоемких программных продуктов.

Терминальный сервер

Linux-агент не поддерживает терминальный сервер.

Установка

Для установки агента на Linux *следуйте инструкции*.

3.2 Установка серверной части

Перед началом установки:

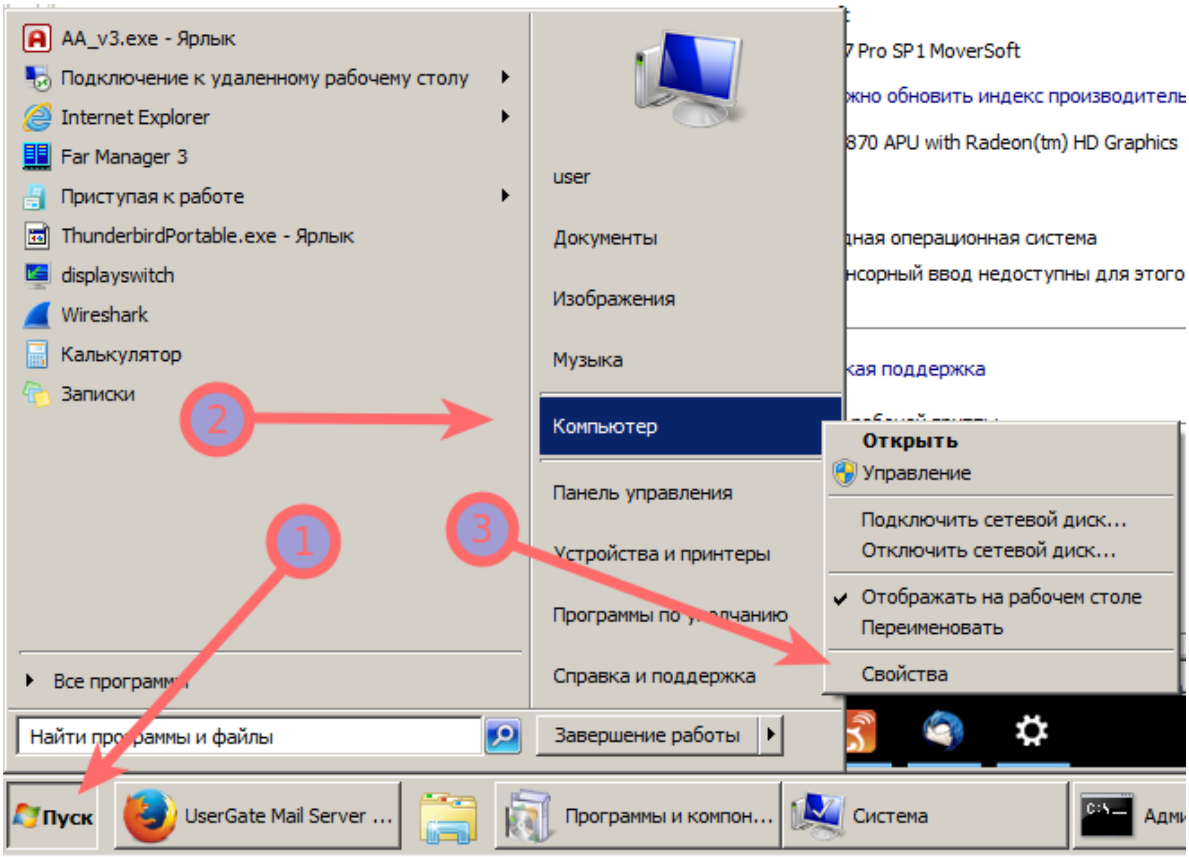
- определитесь с количеством контролируемых компьютеров;
- подберите серверное оборудование;
- выберите тип установки.

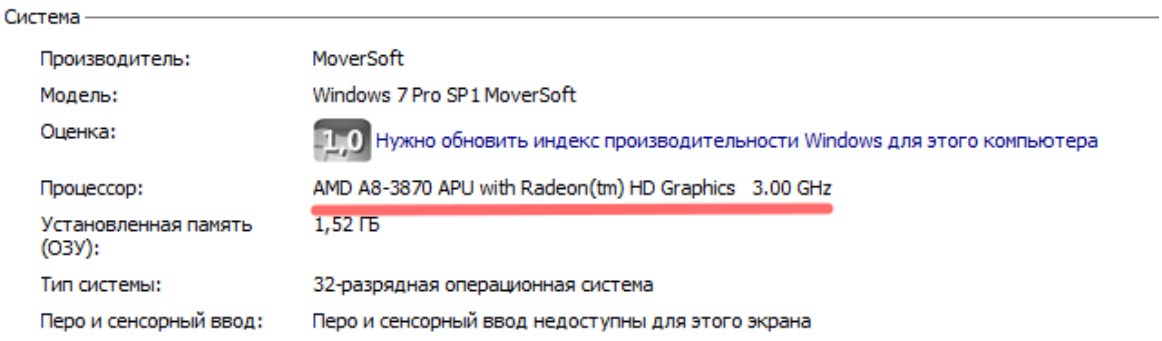
3.2.1 Включение виртуализации

Если при запуске виртуализатора Hyper-V, VmWare или VirtualBox возникают проблемы с работой виртуальной машины в 64-х битном режиме, то нужно включить виртуализацию в BIOS вашего процессора.

Ниже представлены основные советы как это сделать:

1. Определите тип вашего процессора.





В данном примере это процессор - **AMD A8-3870**.

Затем нужно открыть один из соответствующих сайтов от Intel или AMD, и поискать на сайте спецификацию вашего процессора.

INTEL - https://ark.intel.com/#@Processors.

AMD - http://support.amd.com/en-us/kb-articles/Pages/GPU120AMDRVICPUsHyperVWin8.aspx

Иногда нужно использовать поиск yandex\google, потому, что AMD не публикует сама эти списки и спецификации.

2. Если по спецификации на сайте производителя процессора виртуализация - поддерживается, то надо проверить, что она включена в BIOS вашего компьютера.
3. Включить виртуализацию в BIOS:

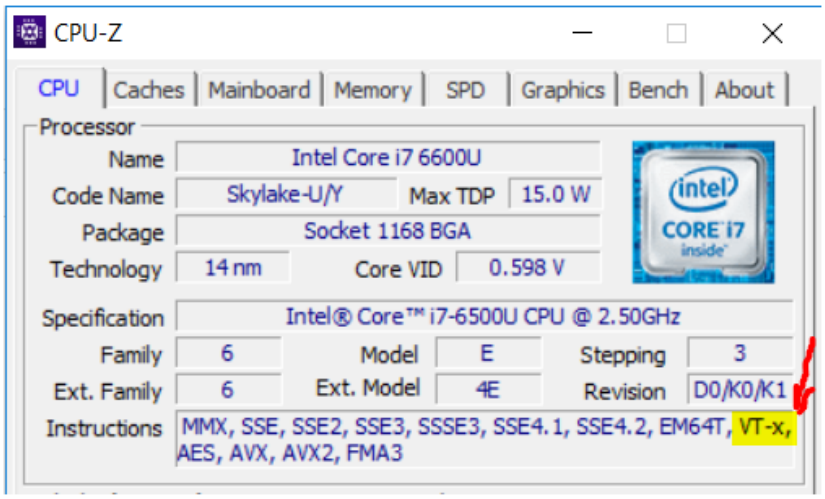
– Пример, того, как включить виртуализацию на HP Elite 8200, Core i7 2600:

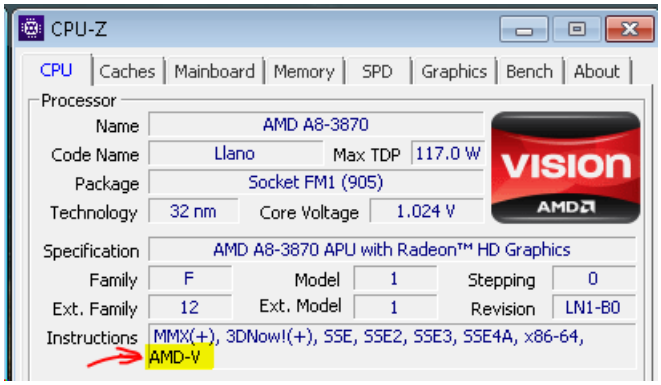
Пример как можно включить виртуализацию на HP Compaq 8200 или подобном ПК:

- Включите ваш ПК.
- Нажмите F10 чтобы войти в BIOS.
- На вкладке Безопасность → Системная безопасность (Security - System Security)
- Включите опцию - «Enable Virtualization Technology (VTx) and Virtualization Technology Directed I/O (VTd)».
- Сохраните изменения и перезагрузите ПК.

4. Если найти опции для включения виртуализации в BIOS - не представляется возможным, то стоит попробовать обратиться к поисковой системе и ввести в поиск что-то подобное.

5. Так же в определении флагов виртуализации у процессора - вам может помочь программа CPU-Z. Её нужно запустить и посмотреть внизу окна флаги поддерживаемые вашим процессором, для процессоров **Intel** - это должен быть флаг **VT-x**, для процессоров **AMD** - **AMD-V**.





Если эти флаги у вас присутствуют, то виртуализация с большой вероятностью уже включена в системе, или её можно задействовать через BIOS.

3.2.2 Установка на компьютер

Установка iBatyr Monitor на виртуальную машину удобна, но имеет ряд минусов: снижается производительность системы, виртуальная ОС зависит от реально установленной и т. д.

Чтобы избежать этого, установите серверную часть iBatyr Monitor на физическое оборудование:

1. Установите на машину сервер:
   - скачайте последний доступный образ:

     Ubuntu Server 18.04
     Ubuntu Server 20.04
     Ubuntu Server 22.04

   - установите Ubuntu Server:

     18.04
     20.04
     22.04

– не устанавливайте дополнительное ПО после завершения установки.

2. Установите iBatyr Monitor с помощью скрипта.

Примечание: Для установки ПО сервер должен быть подключен к интернету.

3.2.3 Установка в Hyper-V

Предупреждение: Не устанавливайте на один компьютер несколько сред виртуализации, в частности VirtualBox и Hyper-V.

Предварительная проверка

Перед началом установки:

1. Подготовьте установочный образ iBatyr Monitor :

– Ubuntu 18.04, PostgreSQL 11,

– Ubuntu 22.04, PostgreSQL 15.

2. Установите на машину систему виртуализации Hyper-V.
3. Включите в BIOS *поддержку виртуализации*. Если эта опция отключена, виртуальная система будет работать только в 32-разрядном режиме, а для работы iBatyr Monitor требуется поддержка 64-битных систем.

После запуска виртуальная машина захватывает курсор мыши и клавиатуру. Они станут недоступны для реальной системы — курсор будет двигаться только в пределах окна виртуальной машины. Чтобы вернуться к реальной системе, нажмите правый Ctrl.

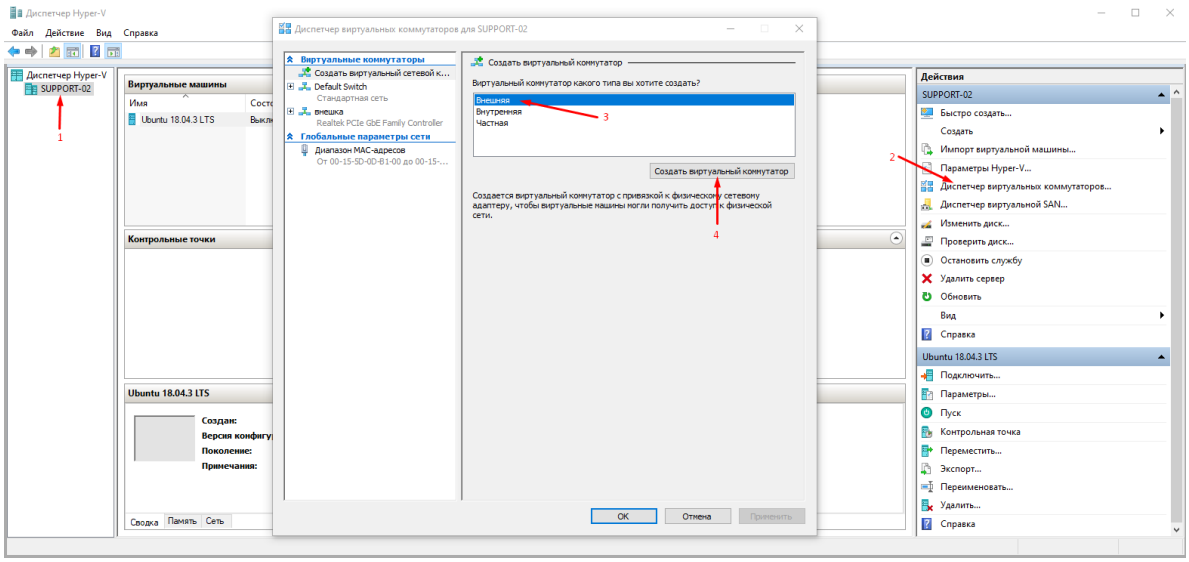
Создание виртуальной машины

Предварительная настройка

Запустите **Диспетчер Hyper-V**. Затем выберите машину, для которой хотите настроить сетевые параметры.

Настройте сетевые параметры:

1. Выберите **Диспетчер виртуальных коммутаторов**.
2. В открывшемся окне выберите тип коммутатора **Внешняя**.
3. Нажмите **Создать виртуальный коммутатор**.
4. Нажмите **OK**, в следующем окне — **Да**.

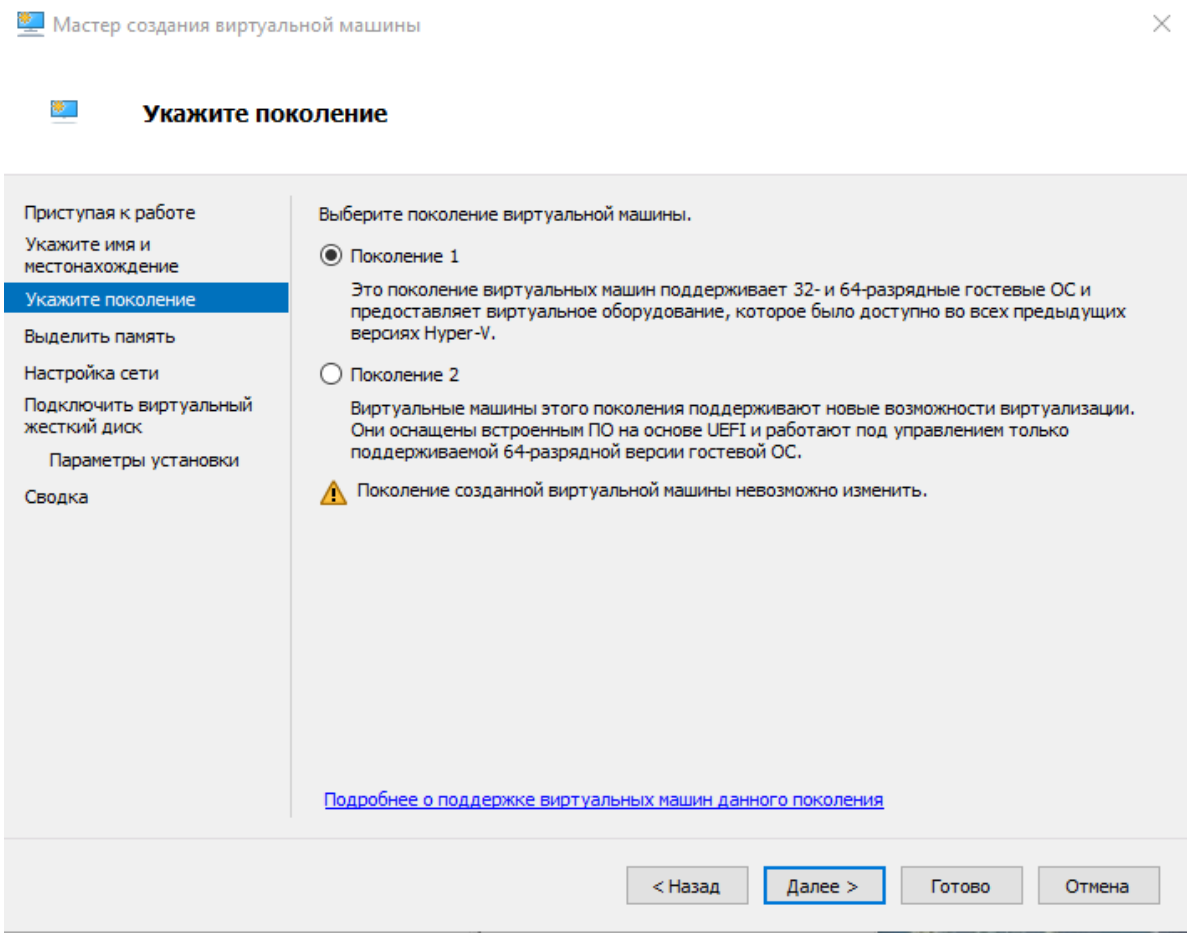


После настройки сетевых параметров перейдите к созданию виртуальной машины.

Новая виртуальная машина

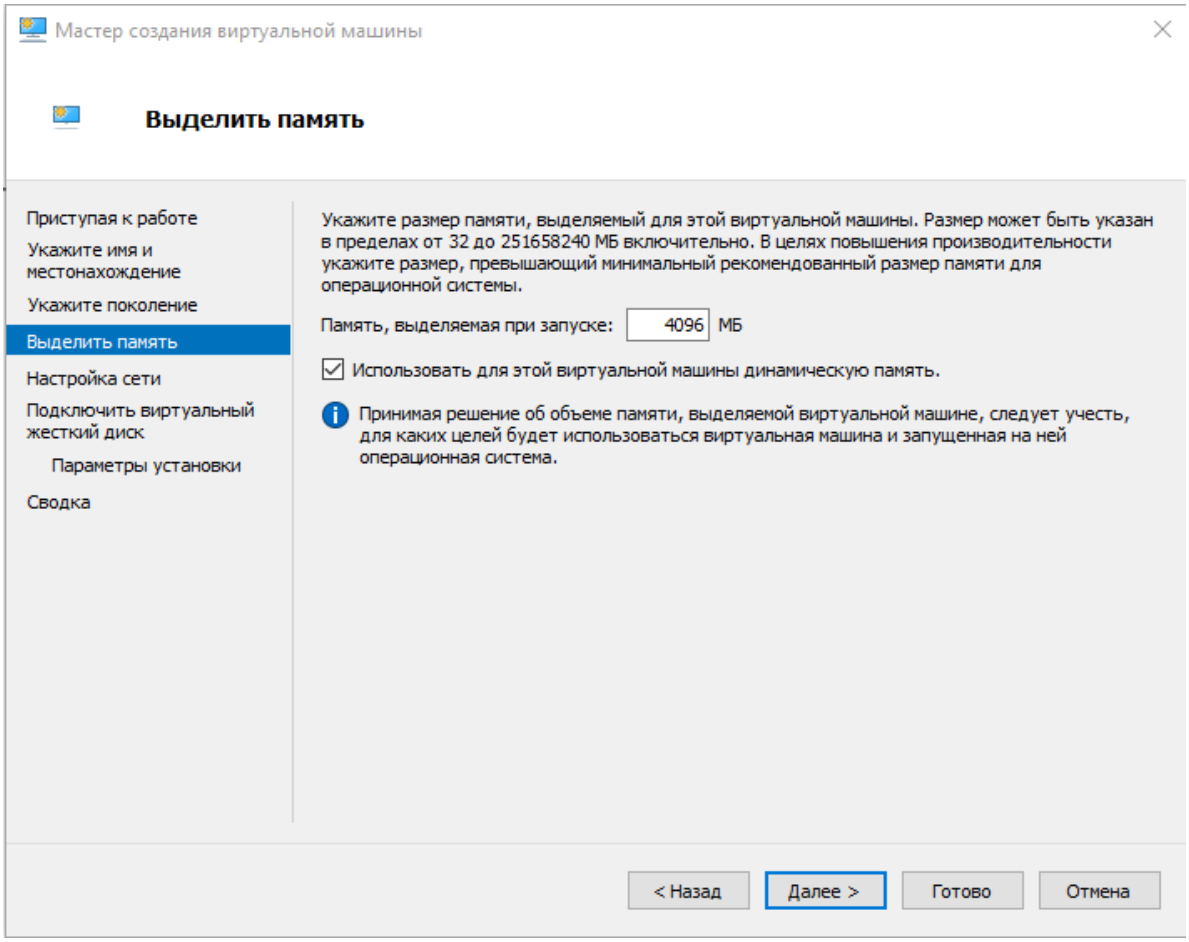
В рабочем окне **Диспетчера Hyper-V** нажмите **Создать** м выберите **Виртуальная машина...**. Следуйте указаниям мастера создания виртуальной машины.

- В окне выбора поколений виртуальной машины выберите поколение в зависимости от версии Ubuntu:
- Ubuntu 18.04 — **Поколение 1**,
- Ubuntu 20.04, 22.04 — **Поколение 2**.

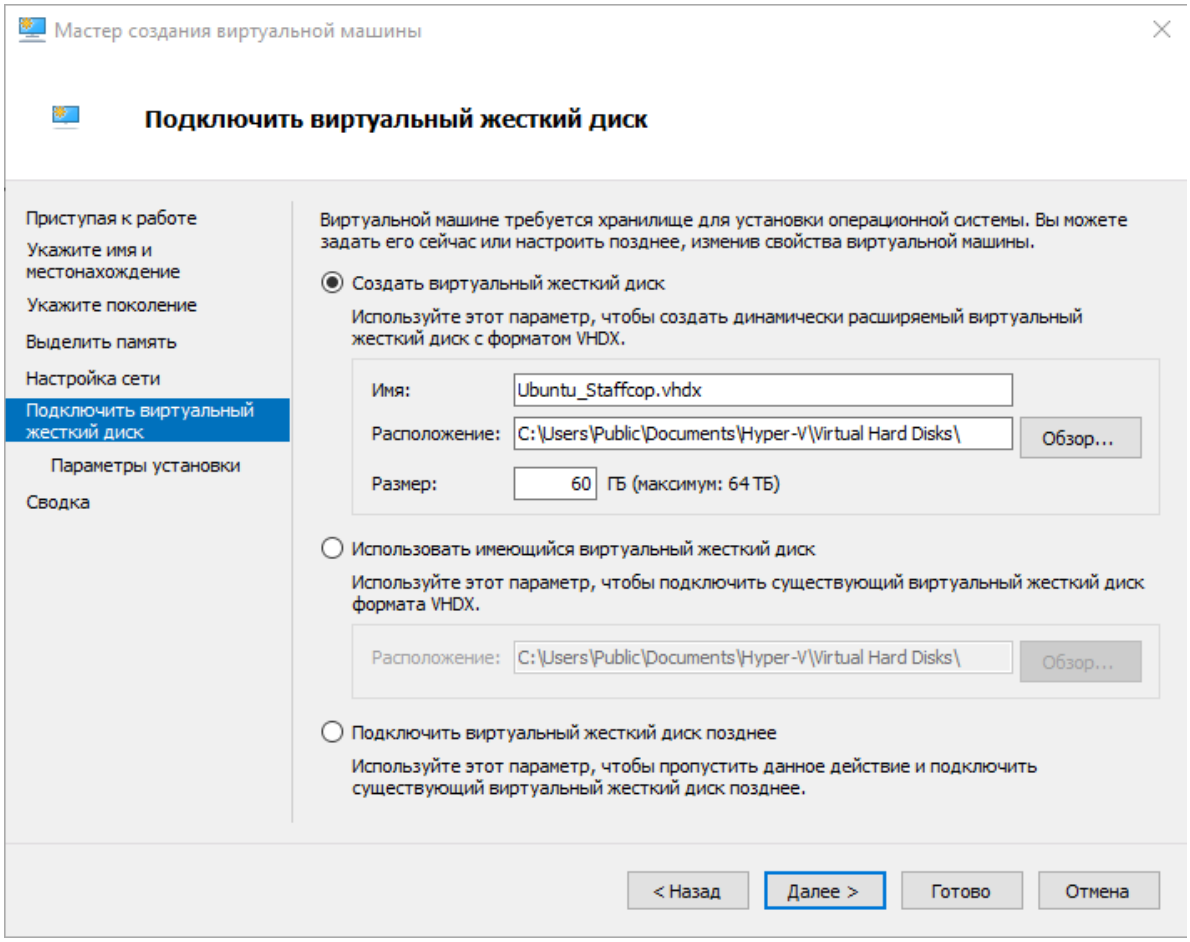


– Выделите виртуальной машине память. Системные требования указаны в разделе *Сервер и базы данных*.

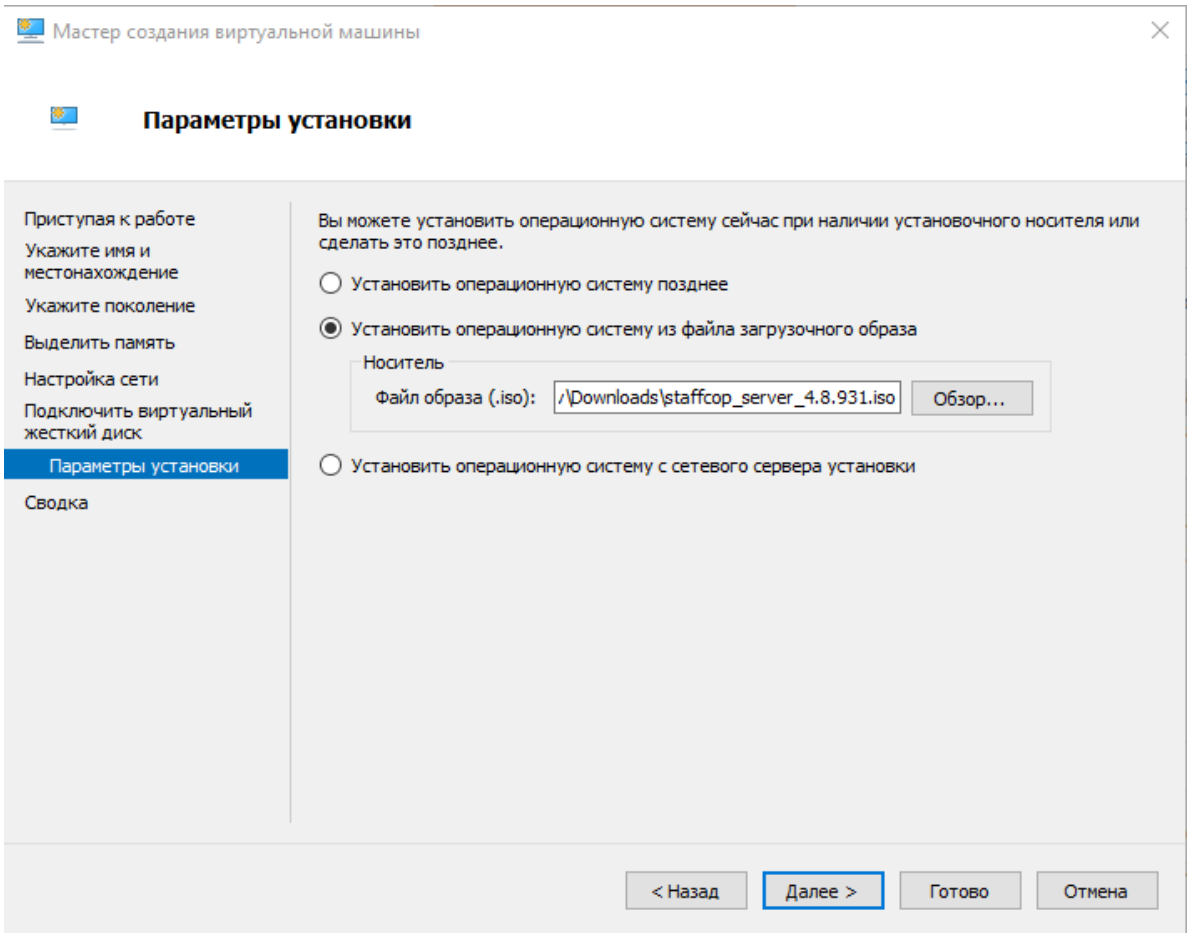
Примечание: Выделение более 50% основной памяти для виртуальной машины может привести к снижению производительности основной операционной системы.



– Укажите имя, расположение и объем виртуального жесткого диска. Рекомендуемый минимальный объем — 60 ГБ.



– На этапе установки операционной системы укажите **Установить операционную систему из файла загрузочного образа** и выберите ISO-образ iBatyr Monitor .



После завершения установки запустите виртуальную машину и продолжите настройку в разделе *Установка из ISO-образа*.

Примечание: Для организации SSH-подключения к виртуальной машине используйте авторизацию по ключам и нестандартный порт, чтобы снизить риск несанкционированного доступа к серверу.

3.2.4 Установка в VMWare

Для начала установки понадобятся:

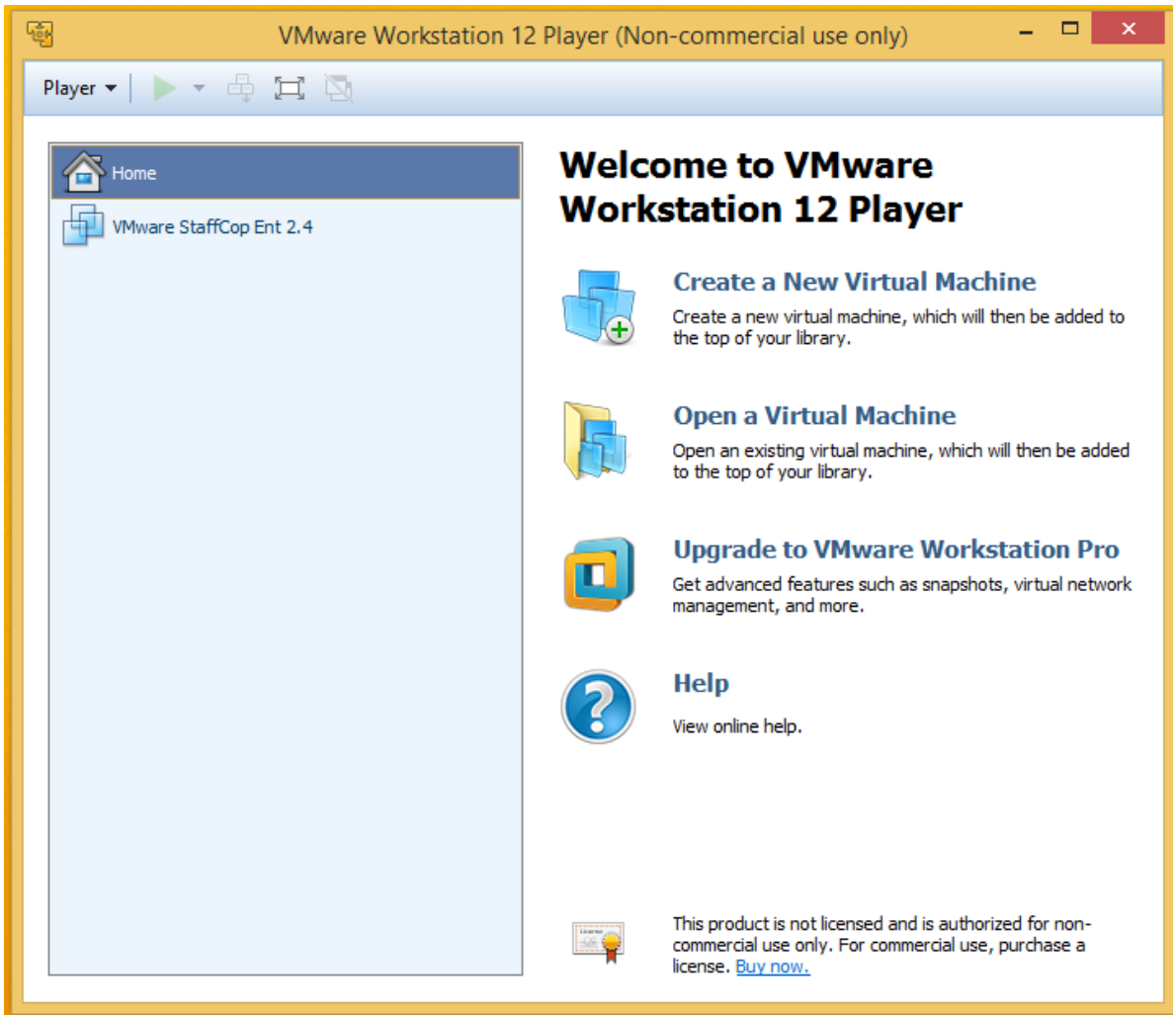
- установочный образ iBatyr Monitor :
  - Ubuntu 18.04, PostgreSQL 11,
  - Ubuntu 22.04, PostgreSQL 15;
- установленная Vmware Workstation Player;
- *процессор, поддерживающий виртуализацию*: если опция отключена в BIOS, то любая система виртуализации сможет создавать лишь 32-разрядные машины, для работы iBatyr Monitor необходима поддержка 64-х разрядных систем.

Примечание: Виртуальная машина может производить автозахват клавиатуры и мыши. При

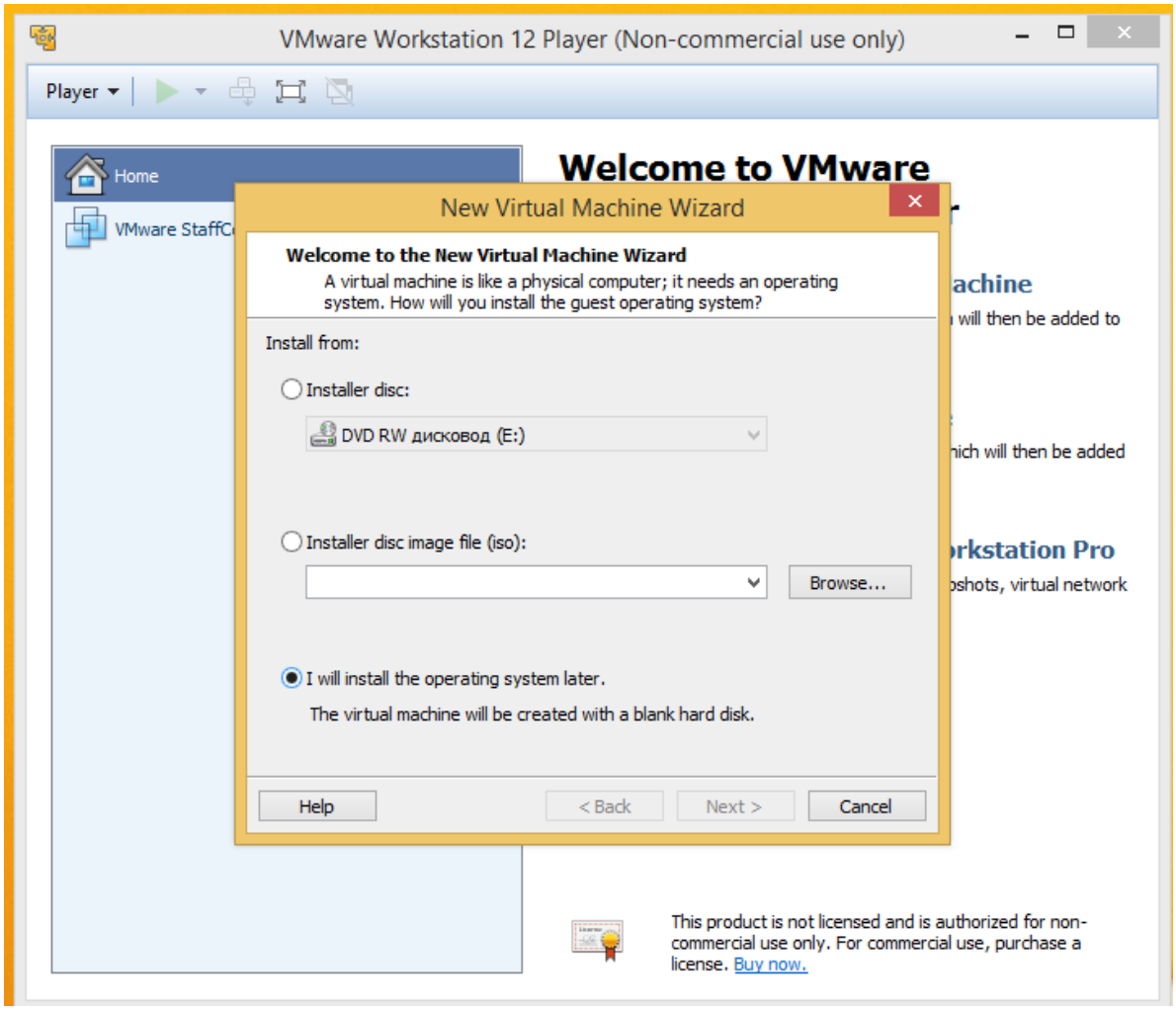
этом для текущей операционной системы они временно будут недоступны. Переключение между виртуальной машиной и реальной как правило производится нажатием клавиш Ctrl+Alt.

Создание виртуальной машины

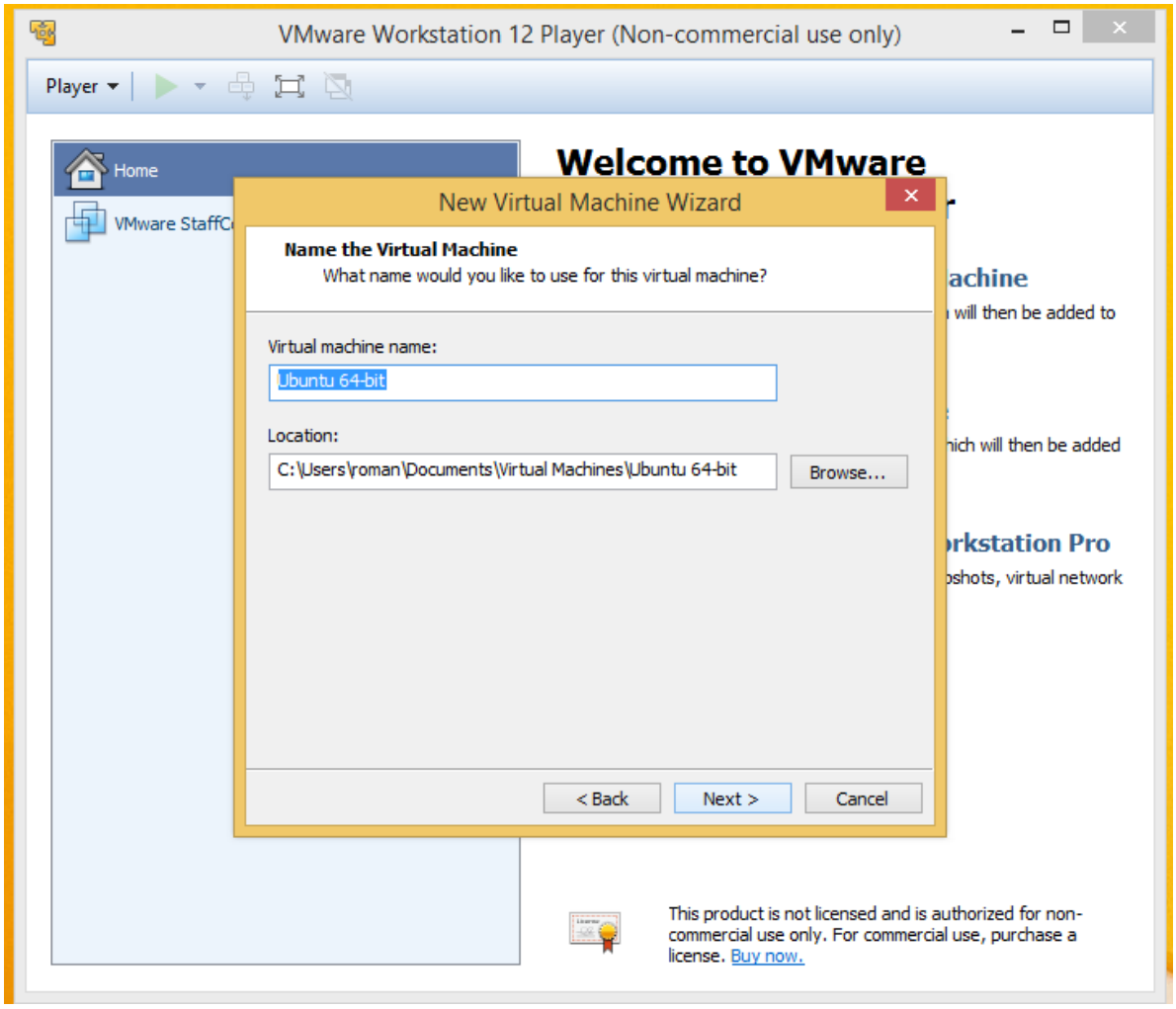
1. Запустите Vmware и в стартовом окне выберите пункт **Create a New Virtual Machine**.



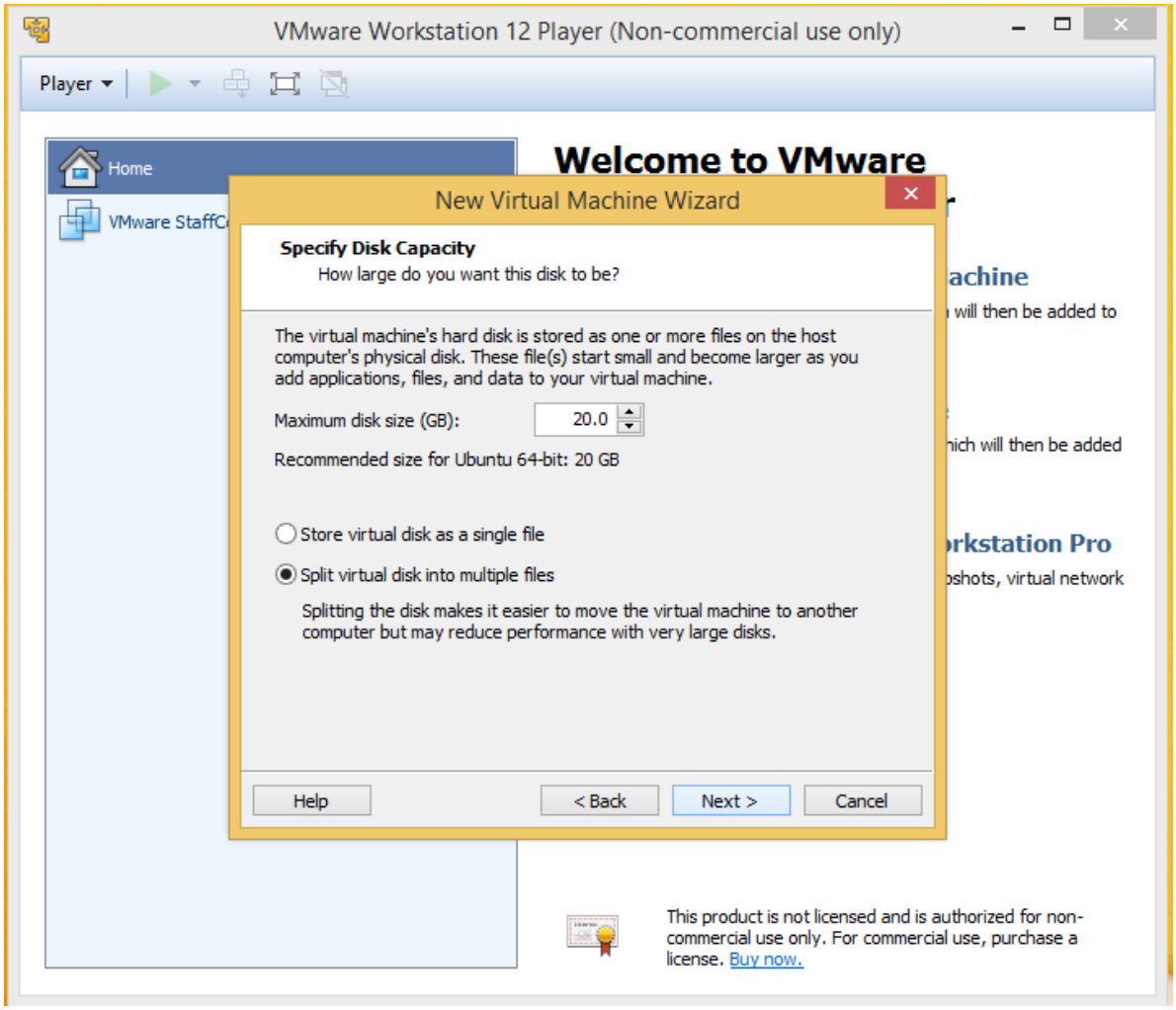
2. Выберете пункт **I will install the operating system later**: некоторые версии VMware при выборе ISO-образа запускают быструю установку без службы iBatyr Monitor.



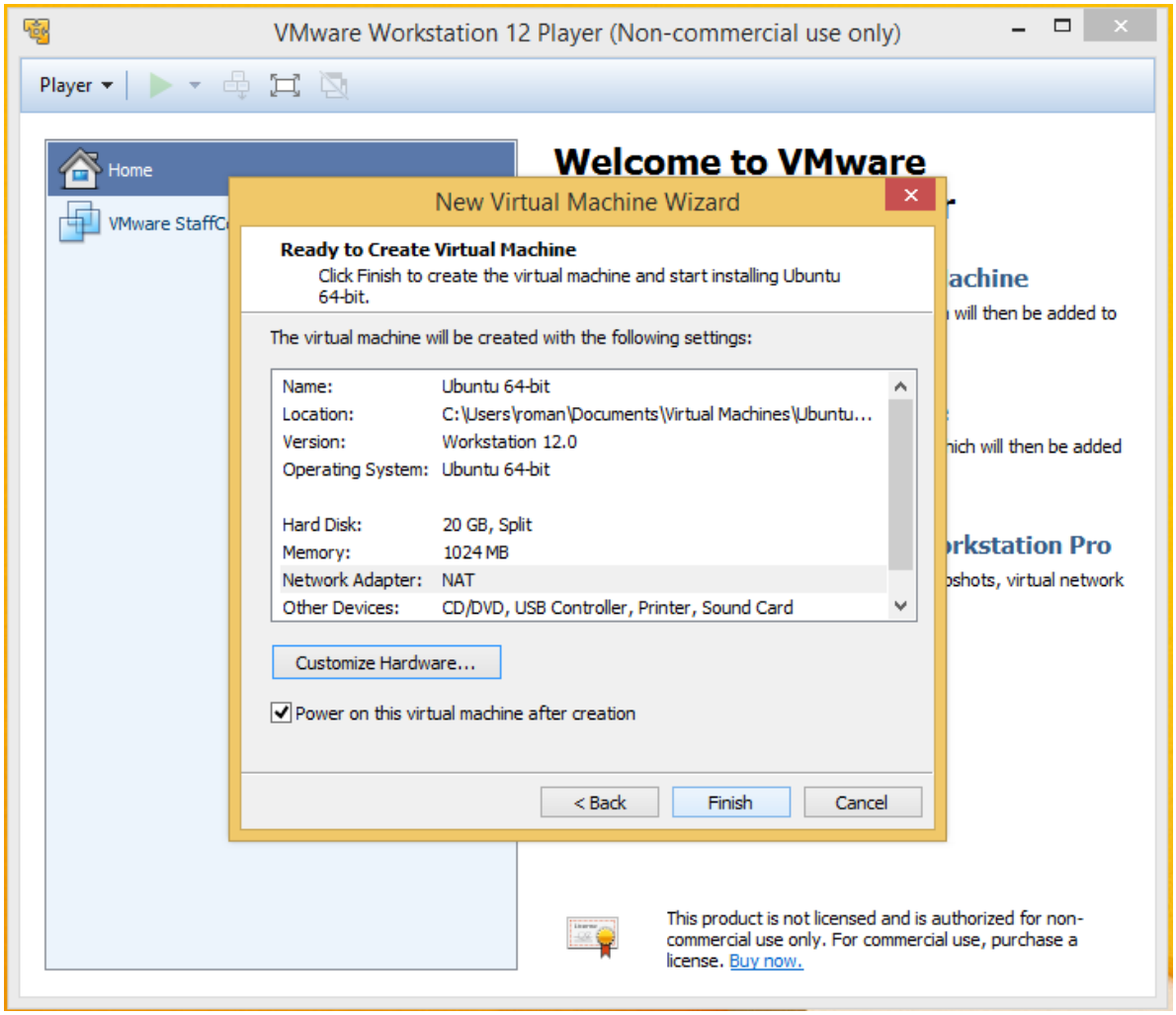
3. Укажите название новой виртуальной машины и место ее расположения.



4. Выберете размер и тип жёсткого диска.



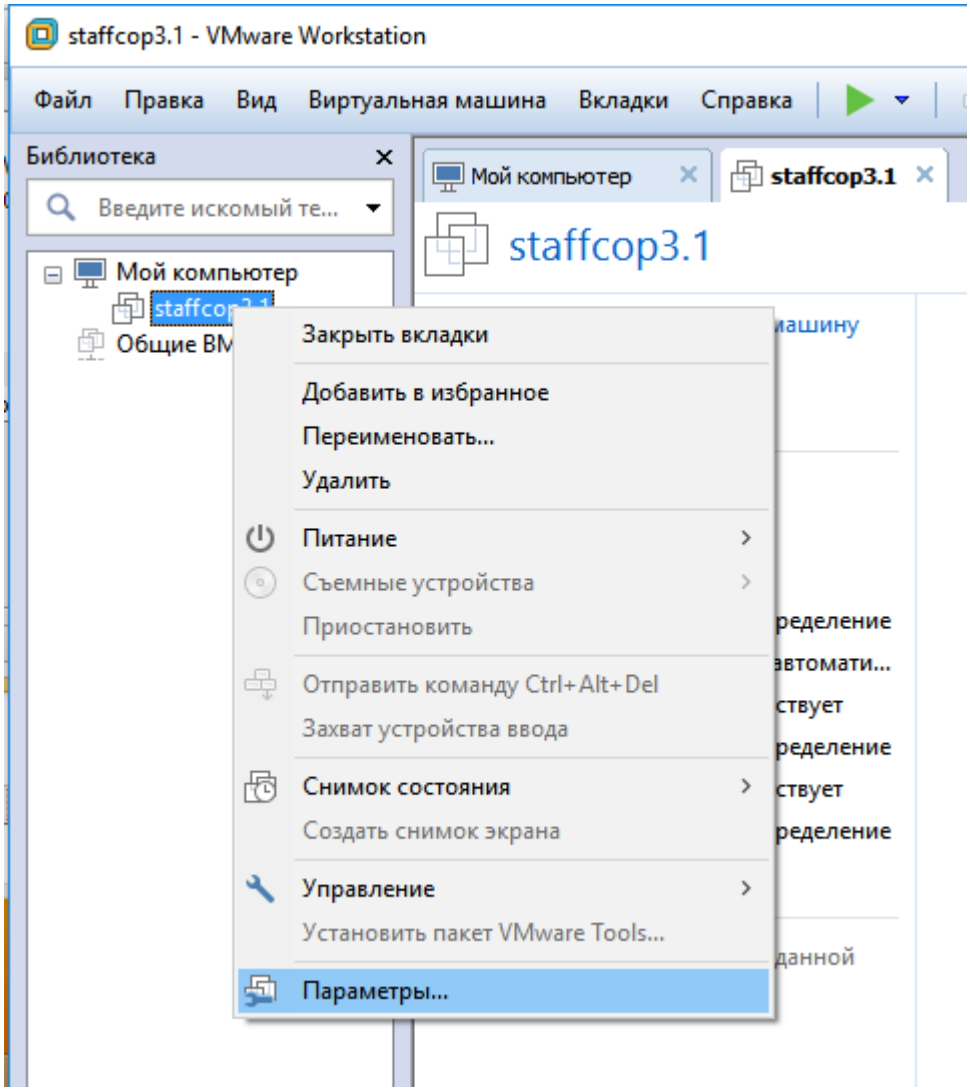
5. Укажите прочие параметры виртуальной машины.

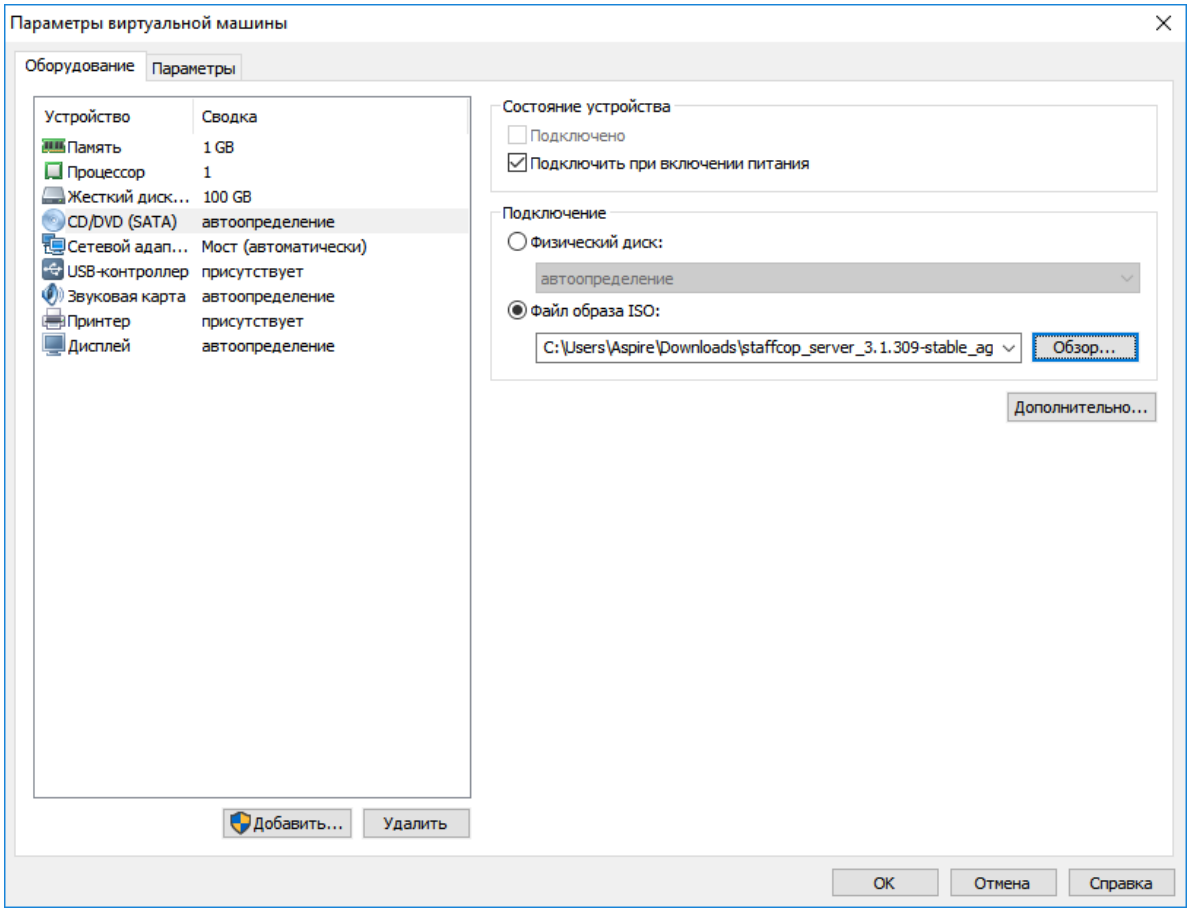


6. Нажмите **Finish**.

Готово! Виртуальная машина создана.

Далее вызовите контекстное меню и в разделе **Параметры** выберите ISO-образ для установки.


staffcop3.1 - VMware Workstation
Файл
Правка
Вид
Виртуальная машина
Вкладки
Справка
Библиотека
Введите искомый те...
Мой компьютер
Общие ВМ
Мой компьютер
staffcop3.1
staffcop3.1
Закрыть вкладки
Добавить в избранное
Переименовать...
Удалить
Питание
Съемные устройства
Приостановить
Отправить команду Ctrl+Alt+Del
Захват устройства ввода
Снимок состояния
Создать снимок экрана
Управление
Установить пакет VMware Tools...
Параметры...



После этого следуйте инструкциям в разделе «*Установка из ISO-образа*».

Примечание: Для организации SSH-подключения к виртуальной машине используйте авторизацию по ключам и нестандартный порт, чтобы снизить риск несанкционированного доступа к серверу.

3.2.5 Установка в Virtualbox

Предупреждение:

Не устанавливайте на один компьютер несколько сред виртуализации, например Virtualbox и Hyper-V.

Не рекомендуется использовать VirtualBox для установки сервера с нагрузкой более 5–7 агентов или глубиной хранения данных более 3–4 месяцев.

Предварительная проверка

Для начала установки понадобятся:

- установочный образ iBatyr Monitor :
  - Ubuntu 18.04, PostgreSQL 11,
  - Ubuntu 22.04, PostgreSQL 15;
- установленная система виртуализации Virtualbox;
- *процессор, поддерживающий виртуализацию*: если опция отключена в BIOS, то любая система виртуализации сможет создавать лишь 32-разрядные машины, для работы iBatyr Monitor необходима поддержка 64-х разрядных систем.

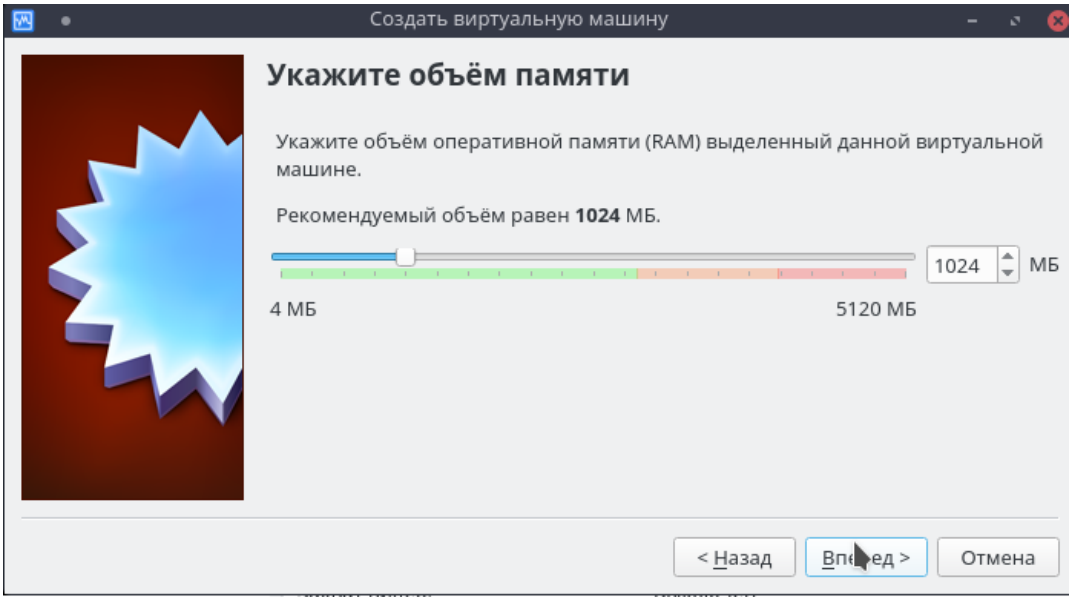
После запуска виртуальная машина может захватывать курсор мыши и клавиатуру. При этом они будут недоступны для реальной системы — мышь будет перемещаться в пределах окна виртуальной системы. Переключиться между виртуальной машиной и реальной можно нажатием правого Ctrl.

Создание новой виртуальной машины

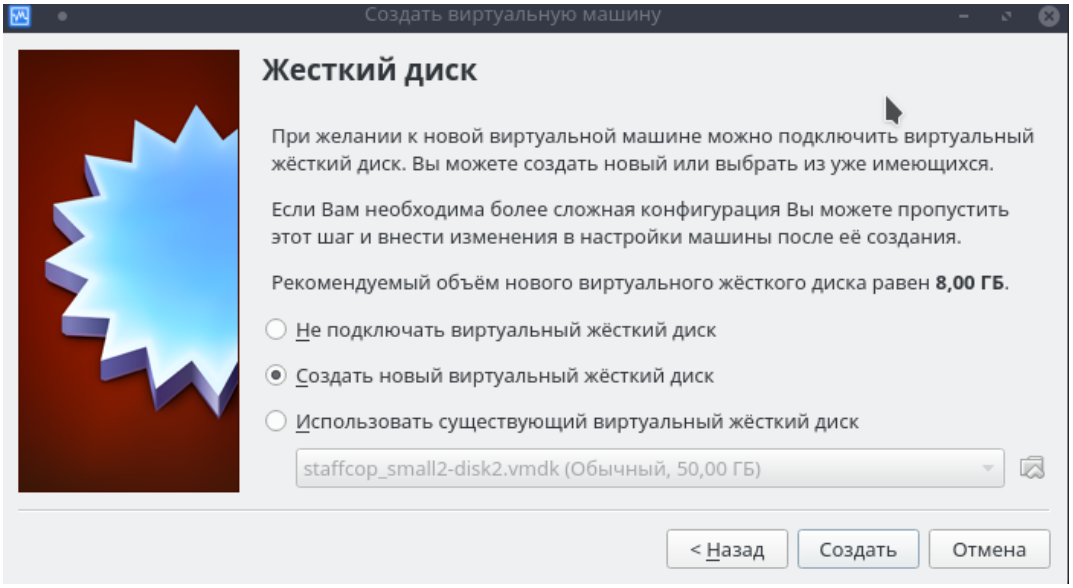
1. Запустите Virtualbox.
2. Нажмите **Создать** в главном рабочем окне и укажите:

- имя — на ваш выбор;
- тип — Linux;
- версия — Ubuntu 18.04, 20.04, 22.04.

3. Выделите виртуальной ОС память:
   - основные системные требования к памяти указаны в разделе «*Сервер и базы данных*»;
   - если выделить виртуальной ОС более 50% выделенной памяти, производительность основной ОС может заметно упасть;
   - более 75% из основной памяти нельзя выделить, используя графический интерфейс — это можно сделать только через командную строку.



4. Создайте новый виртуальный жёсткий диск.



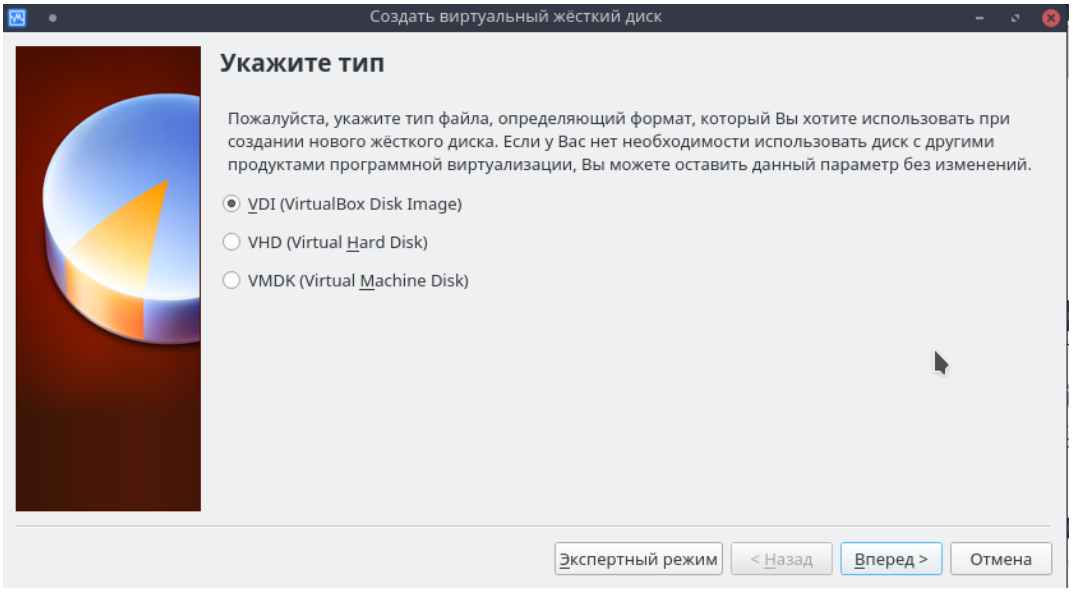
5. Выберите тип жесткого диска.

   При тестирования сервера используйте формат дисков VDI, чтобы увеличить скорость работы.

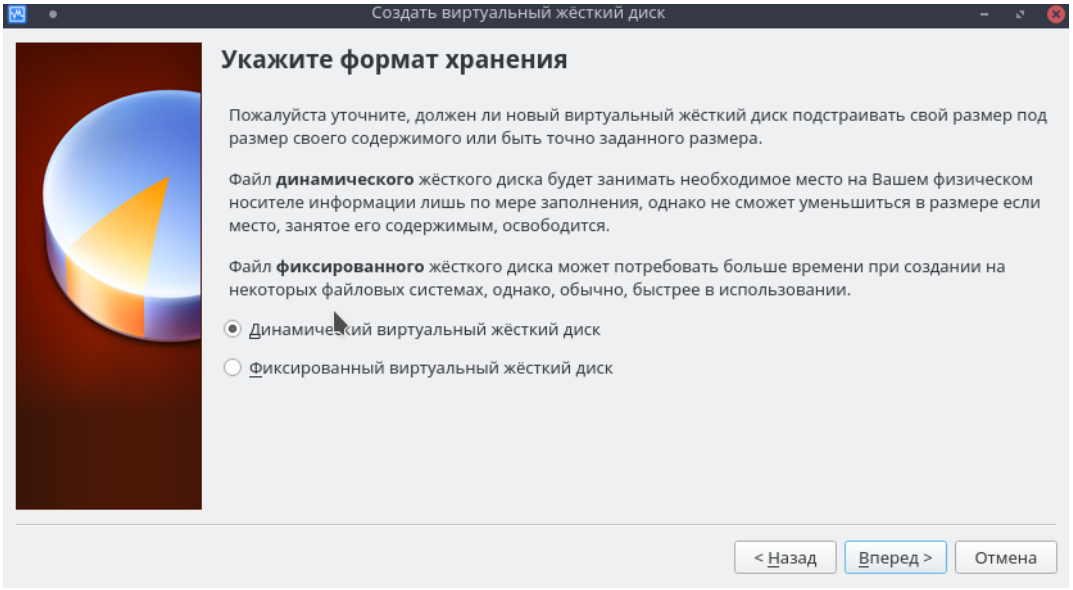
   Для постоянного использования и переноса сервера на другие платформы виртуализации выберите:

   – VHD для Hyper-V,

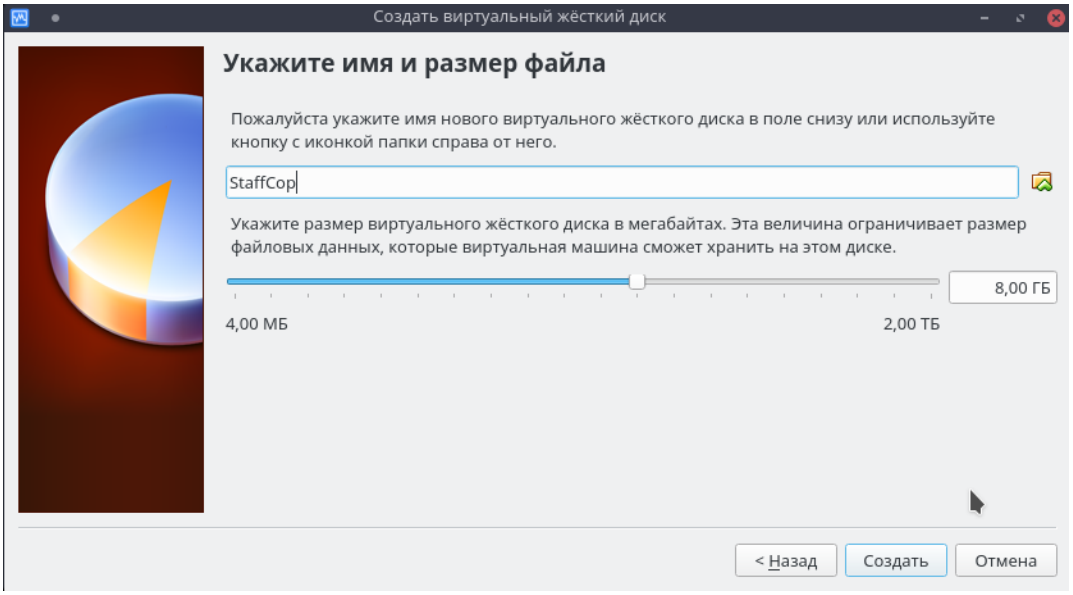
   – VMDK для VMWare.



6. Выберите формат виртуального жесткого диска: динамический или фиксированный.



7. Укажите имя диска и его размер. Не создавайте диск со значениями по умолчанию — их не хватит для полноценной работы iBatyr Monitor . Минимальный рекомендуемый объём жёсткого диска — 50 ГБ.



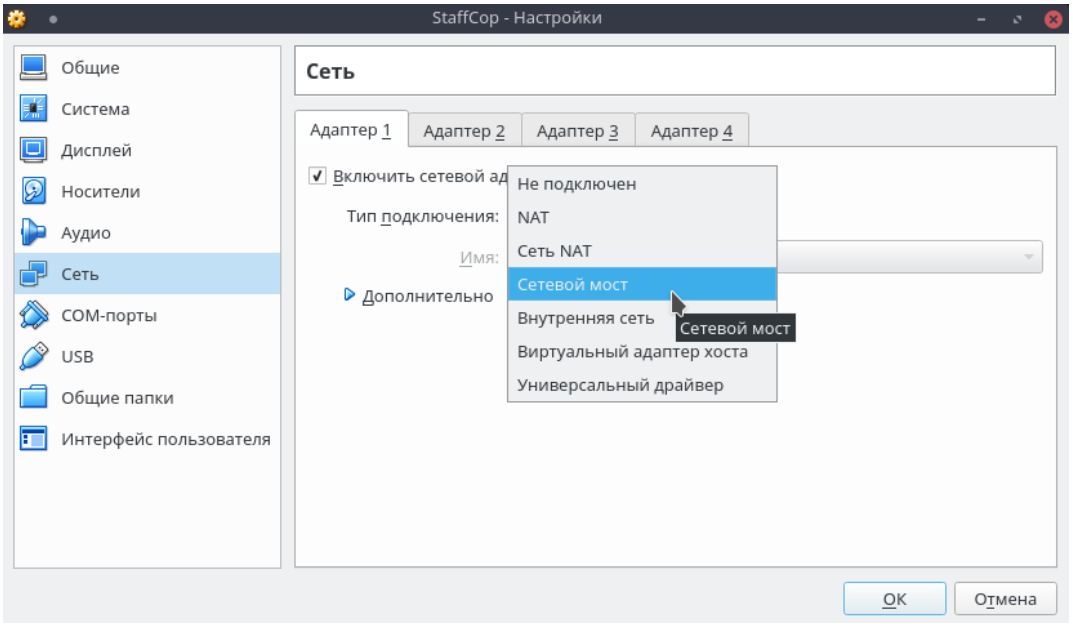
8. Нажмите **Создать**.

Исходная конфигурация создана!

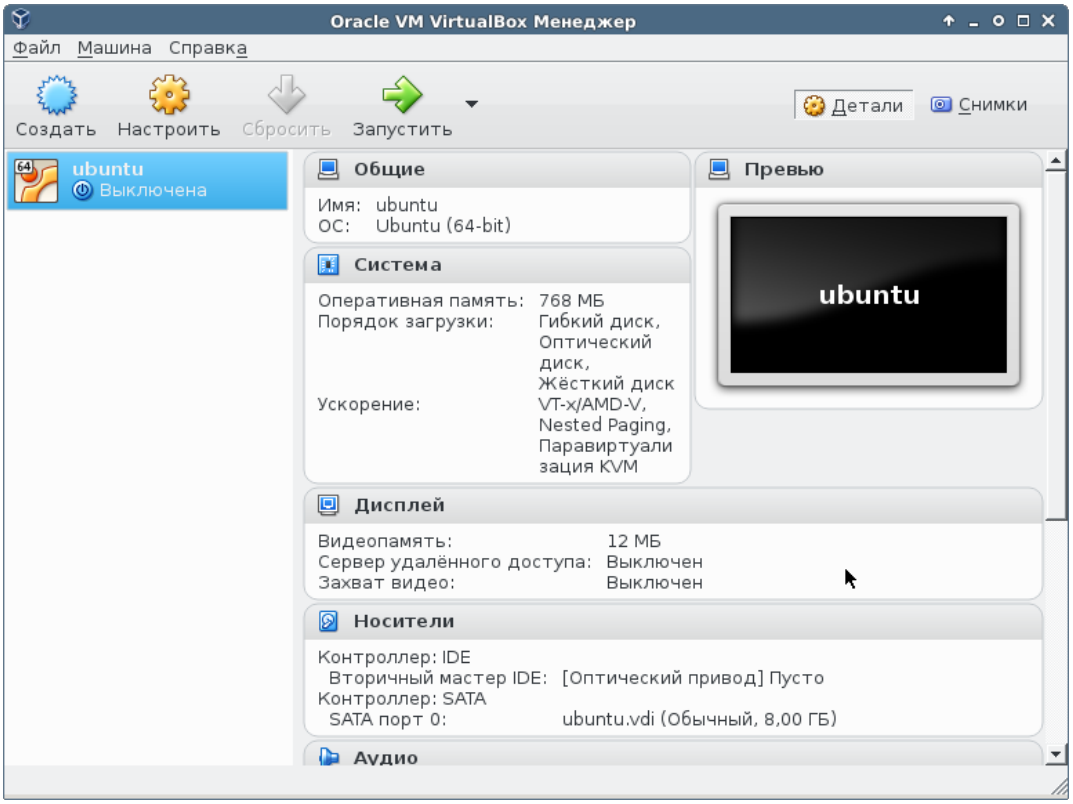
Примечание: Чтобы настроить автоматический запуск виртуальной машины после перезагрузки физического сервера, прочитайте инструкцию *Автоматический запуск виртуальной машины iBatyr Monitor в VirtualBox*.

Завершите настройку виртуальной машины и запустите установку iBatyr Monitor:

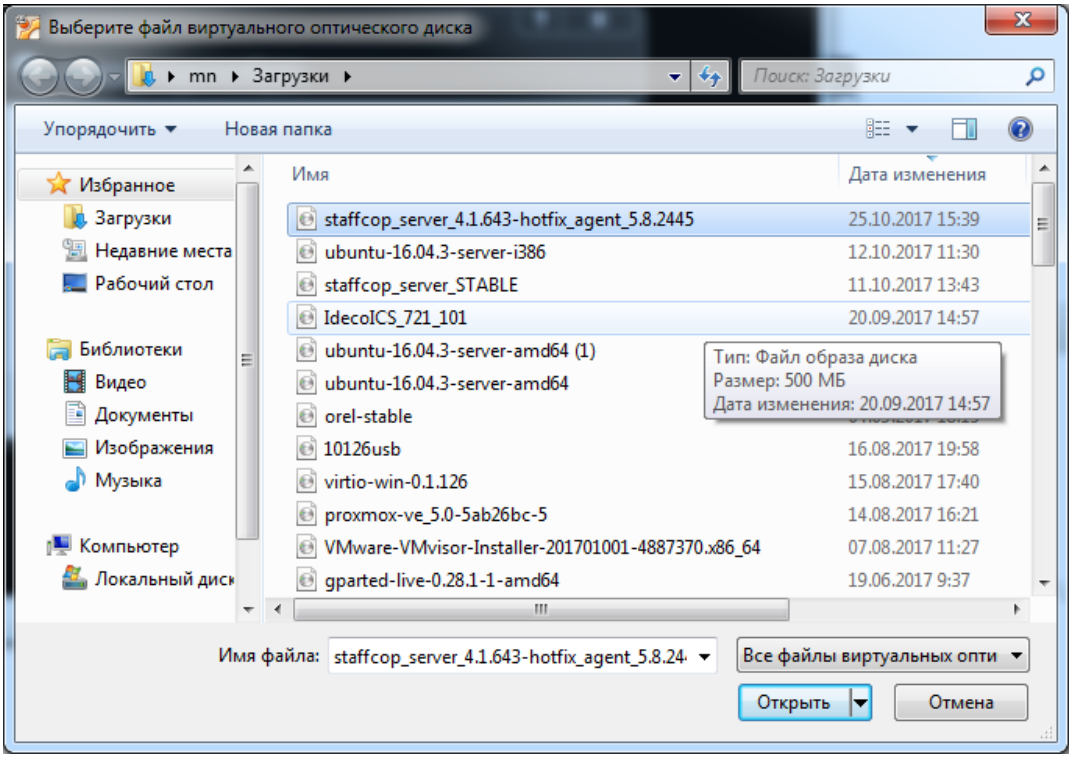
1. В разделе **Сеть** замените тип подключения **NAT** на **Сетевой мост**.



2. Нажмите **Запустить**.



3. Выберите загрузочный образ и нажмите **Открыть**.



После этого перейдите к инструкции в статье *установщик ОС*.

Примечание: Для организации SSH-подключения к виртуальной машине, используйте авторизацию по ключам и нестандартный порт, чтобы снизить риск несанкционированного доступа к серверу.

3.2.6 Установка из ISO-образа

Установка сервера iBatyr Monitor — это инсталляция операционной системы Ubuntu Server из ISO-образа, в который входят:

- пакет программы iBatyr Monitor ;
- Ubuntu 18.04;
- PostgreSQL 11;
- Nginx.

Дополнительно поставляется ISO-образ с Ubuntu 22.04 и PostgreSQL 15.

Процесс идентичен стандартной установке Ubuntu на физический или виртуальный сервер.

Подготовка

Скачайте последний стабильный ISO-образ:

- Ubuntu 18.04, PostgreSQL 11
- Ubuntu 22.04, PostgreSQL 15

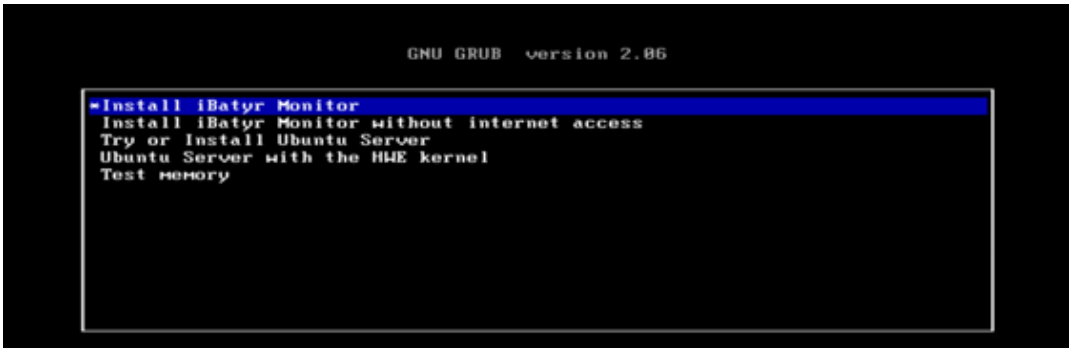
Если вы используете виртуальную машину:

- убедитесь, что *процессор поддерживает флаги виртуализации*,
- включите виртуализацию в BIOS вашего компьютера.

Перед установкой из ISO-образа на виртуальную машину установите среду виртуализации: *VirtualBox* или *VMWare*.

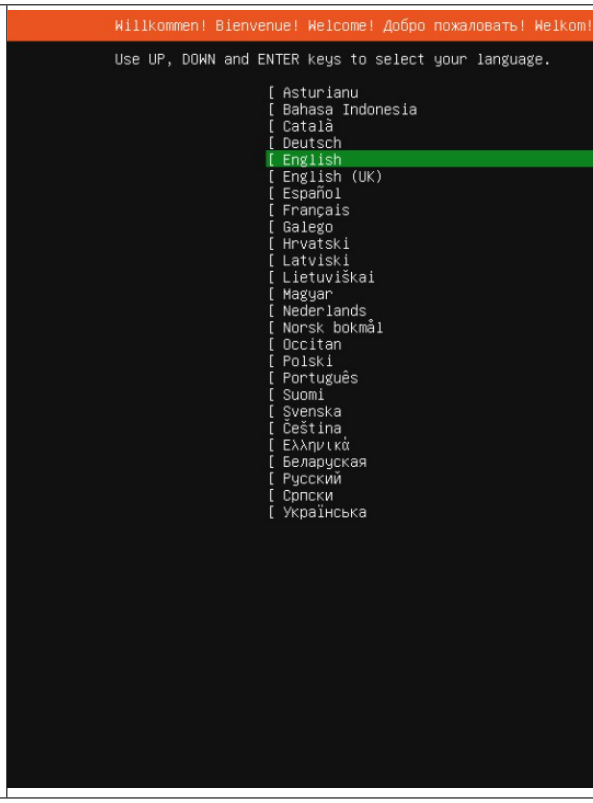
Установка

1. Загрузитесь с ISO-образа.
2. В загрузочном меню выберите один из вариантов установки:
   - **Install iBatyr Monitor Server** — предназначен для установки с доступом к интернету. Включает файл параметров cloud-init, который указывает на загрузку пакетов из внешних репозиториев. Этот метод позволяет получить актуальные версии всех зависимостей с исправлениями багов и уязвимостей.
   - **Install iBatyr Monitor Server without internet access** — используется в изолированной среде без доступа в интернет. В этом случае файл cloud-init предписывает установку пакетов из каталога server/extras/ внутри в ISO-образа.

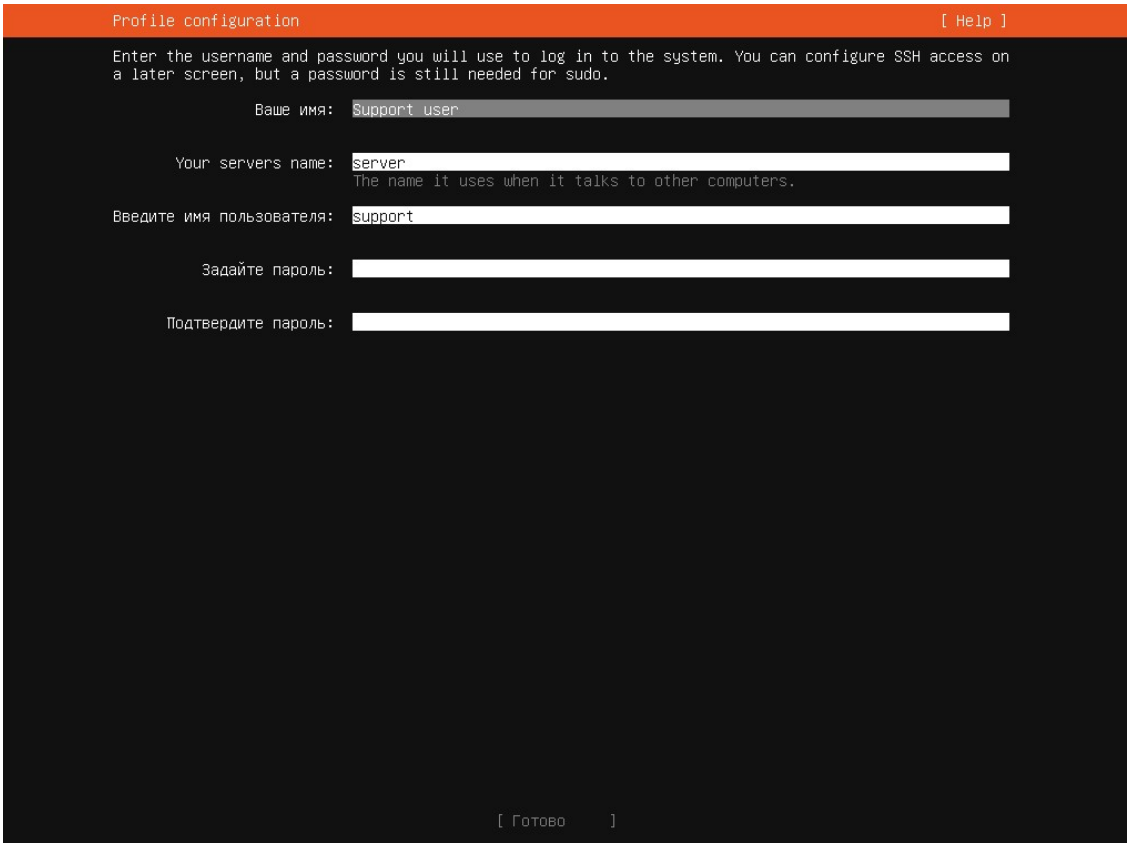


3. Выберите язык интерфейса и раскладку клавиатуры.

tabularytabulary



4. Задайте имя сервера и создайте пользователя.

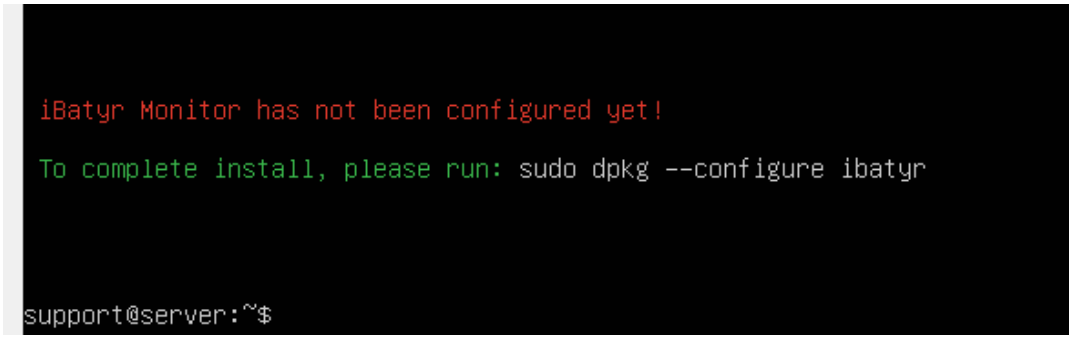


5. Дождитесь завершения установки и автоматической перезагрузки операционной системы.
6. После перезагрузки ОС iBatyr Monitor Server будет установлен, но не настроен.

   Для финальной настройки выполните команду:

   ```
   sudo dpkg --configure ibatyr
   ```

   До выполнения этой команды останется не настроенным, а при каждом входе в систему будет отображаться напоминание:

7. После настройки переходите к этапу *Завершение установки*.

Безопасность

Не подключайте сервер к внешней сети через SSH.

Если SSH-доступ необходим — используйте:

- аутентификацию по SSH-ключам,
- нестандартный порт для подключения.

3.2.7 Установка на Linux-систему

Особенности установки:

- iBatyr Monitor-сервер работает **только на Ubuntu Server 18.04, 20.04, 22.04** другие версии и Linux-системы не поддерживаются;
- скрипты установки предназначены для работы на чистой Ubuntu — в систему не должны быть установлены никакие дополнительные приложения или зависимости;
- сервер для работы iBatyr Monitor должен соответствовать *рекомендуемым системным требованиям*.

Предупреждение: Для стабильной работы iBatyr Monitor не устанавливайте на сервер никаких других приложений.

Чтобы установить последнюю версию iBatyr Monitor , скачайте и запустите скрипт-установщик:

```
sudo wget -O - http://dist.ibatyr.kz/ibatyr5.4/ibatyr.gpg | sudo apt-key add -
sudo echo "deb http://dist.ibatyr.kz/ibatyr5.4 ibatyr5.4 non-free" | sudo tee /etc/
↪apt/sources.list.d/ibatyr.list
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install ibatyr
ibatyr postgresql install
ibatyr init
```

После завершения работы скрипта, проверьте правильность установки сервера iBatyr Monitor командой:

```
sudo ibatyr info
```

Если установка прошла успешно, вывод будет примерно таким:

```
Version: 5.06.2-3.1
Branch: stable5.06
Repository: deb http://distr.ibatyr.kz/stable5.06 stable5.06 non-free
Locale: ru_RU
CPU: 4
Memory (Mb): 7937
Workers: 38
ETL: True
ICAP: False
Pipeline: False
HyperScan: True
RustSrv: False
Current IP: 10.0.194.155
Database IP: localhost
Current Databases:
    - default
```

Единственный вопрос, на который вам придется ответить в процессе установки — ваше географическое расположение. Эта информация нужна для указания корректного часового пояса сервера.

Далее следуйте инструкциям в разделе *Завершение установки*.

Примечание: Избегайте SSH-доступа к вашему серверу из внешней сети. Если организовать SSH-доступ необходимо, используйте аутентификацию по ключам и нестандартный порт для подключения.

3.2.8 Завершение установки

Смена пароля в Linux

После завершения установки запустите виртуальную машину и введите логин и пароль, указанные при установке.

Чтобы изменить уже созданный пароль введите команду

```
passwd
```

и дважды введите новый пароль.

Примечание: Начиная с версии 5.0, в iBatyr Monitor добавлено *средство оценки надежности паролей*, которое включено по умолчанию. Чтобы не забыть созданный сложный пароль воспользуйтесь программой-хранителем паролей. Например: http://keepass.info/ .

Обновление системы

Перед началом работы с сервером, обновите установленную систему. Это может занять несколько минут. Введите команду:

```
sudo apt-get update && sudo apt-get upgrade
```

После обновления очистите систему от старых пакетов:

```
sudo apt-get autoclean && sudo apt-get autoremove
```

IP-адрес сервера

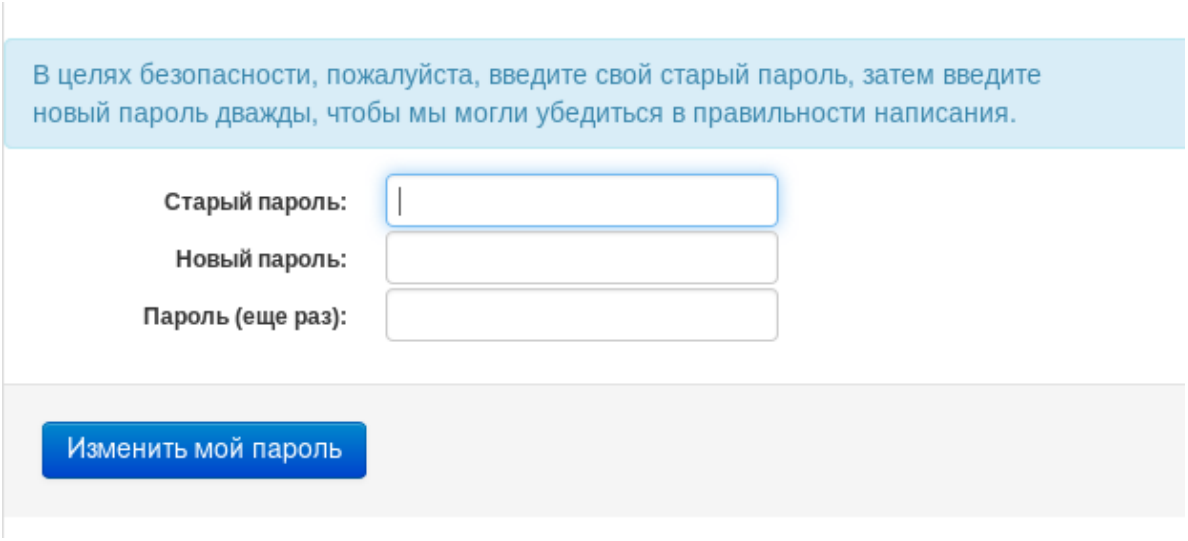
Чтобы узнать IP-адрес установленного сервера воспользуйтесь командой

```
ip a | grep -v inet6 | grep -i inet
```

Вход в веб-интерфейс

Предупреждение: Для работы с веб-интерфейсом системы, используйте браузеры Google Chrome, Mozilla Firefox, Safari, MS Edge, Yandex-браузер. Разрешение монитора должно быть не менее 1920×1080 (Full HD).

Введите полученный IP-адрес в адресную строку браузера.



Обратите внимание, что для веб-интерфейса используется отдельная пара логин-пароль, не совпадающая с логином и паролем от установленного сервера.

Для входа в веб-интерфейс используйте логин **admin**. Пароль задаётся при первом входе в систему.

Активация лицензионного ключа

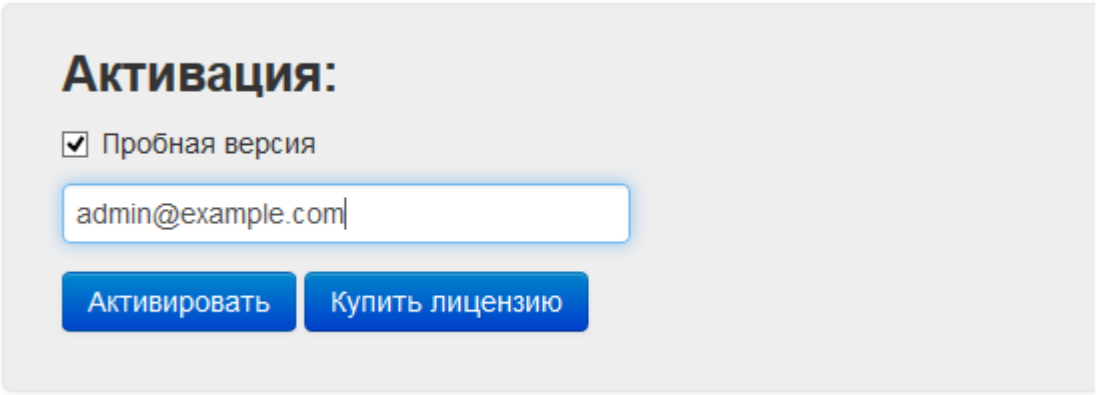
Пробная версия

При первом входе в панель администратора есть возможность активировать пробную версию на 5 агентов со сроком 15 дней.

Чтобы активировать пробную версию:

1. Установите флаг на **Пробная версия**.
2. Введите регистрационный email.
3. Нажмите **Активировать**.

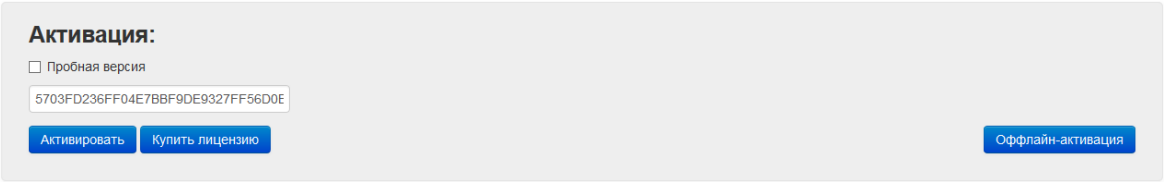
Если сервер имеет доступ в интернет, то пройдет онлайн активация, появится зеленая полоса и в течении минуты откроется панель администратора iBatyr Monitor .



Онлайн активация по ключу

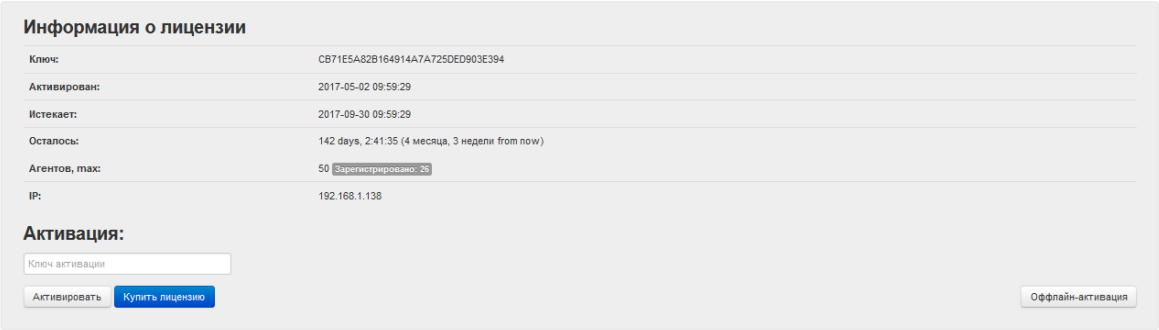
Для активации вставьте в поле **Ключ активации** ключ и нажмите **Активировать**.

Если сервер подключен к интернету, то пройдет онлайн активация и автоматически в течении минуты откроется панель администратора iBatyr Monitor .

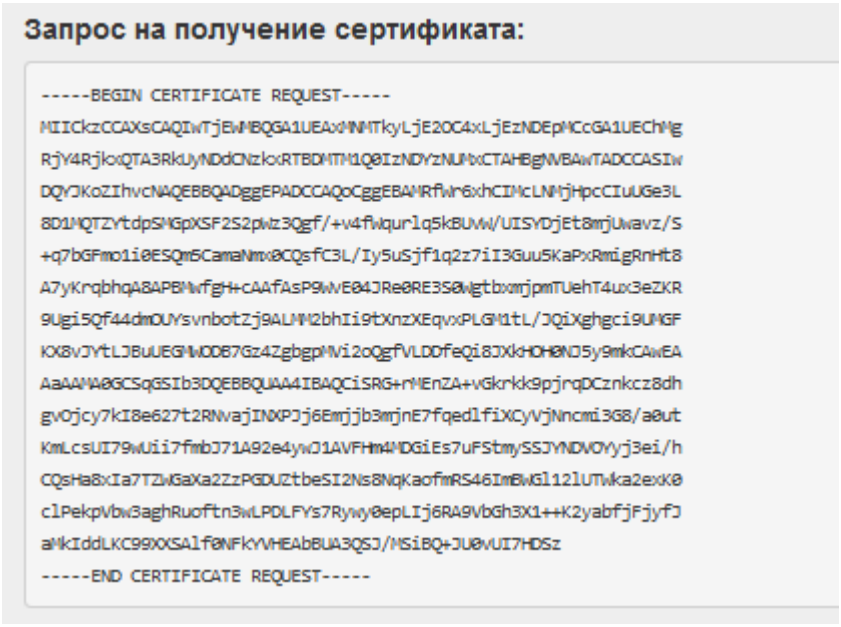


Оффлайн активация

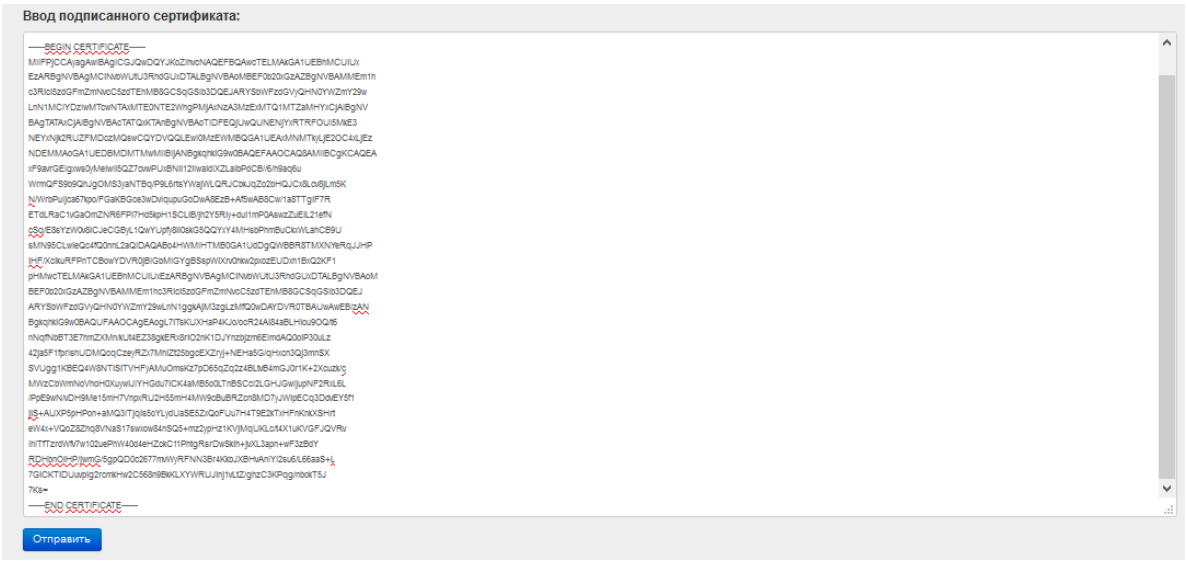
Для оффлайн активации вставьте ключ в поле **Ключ активации** и нажмите **Оффлайн-активация**.



После этого программа пришлёт запрос сертификата. Скопируйте этот запрос и отправьте менеджеру iBatyr Monitor Enteprise.



В ответ менеджер пришлёт ответный запрос. Вставьте его в поле **Ввод подписанного сертификата** и нажмите **Отправить**. После этого в течение минуты автоматически откроется панель администратора iBatyr Monitor .



Далее, можно переходить к *установке агентов*.

3.2.9 Горизонтальное масштабирование

Содержание

- *Системные требования*
- *Предварительная настройка*
  - *Подготовка мастер-сервера*
- *Развёртывание кластера*
  - *Настройка конфигурации*
  - *Сборка кластера*
- *Начало работы*
  - *Синхронизация политик*
- *Как добавить или убрать ноду в кластер iBatyr Monitor*
  - *Добавить ноду*
  - *Удалить ноду*

Начиная с версии 5.2 в iBatyr Monitor доступен компонент Горизонтальное масштабирование, который позволяет создавать кластер из нескольких отдельных серверов iBatyr Monitor.

Преимущества:

- **объединение настроек политик**: настройки политик для всех серверов iBatyr Monitor в кластере централизованы;
- **единая веб-консоль**: информация со всех АРМ кластера отображается в одной веб-консоли;
- **объединённые отчёты**: получение отчетов по всем пользователям кластера;

– **доступ ко всем узлам**: всем администраторам системы имеют доступ ко всем узлам кластера.

Системные требования

Мастер-сервер — это центральный сервер для управления кластером. Он предоставляет инструменты для мониторинга, анализа и управления данными, которые поступают с подчиненных серверов кластера.

Для корректной работы убедитесь:

– что мастер-сервер соответствует общим требованиям к серверу,

– у вас достаточно места на диске: при создании кластера в обязательном порядке автоматически устанавливаются ClickHouse и PostgreSQL.

Подробнее о требованиях — в статье Сервер и базы данных.

Внимание: Функционал кластера оптимизирован для новых установок. Интеграция работающего сервера с данными возможна, но не рекомендуется при большом объеме данных. При миграции такого сервера потребуется выполнение ресурсоемких операций неприемлемой длительности, прерывание которых может привести к потере целостности данных. Для оценки возможности интерграции обратитесь *в техническую поддержку*.

Предварительная настройка

Перед развёртыванием кластера:

1. Проверьте версию серверов iBatyr Monitor, которые будут включены в кластер:

```
sudo ibatyr info
```

   Во время сборки кластера разные версии автоматически обновятся до последней версии, указанной в конфигурации.

2. Обновите ПО на всех серверах, которые будут входить в кластер:

```
sudo apt update
sudo apt upgrade
```

Подготовка мастер-сервера

1. Установите пакеты:

   Сервер с доступом к сети

   1. Добавьте в список репозиториев системы репозитории iBatyr Monitor:

```
wget -O - https://distr.ibatyr.kz/stable5.06/ibatyr.gpg | sudo apt-key add -
echo "deb https://distr.ibatyr.kz/stable5.06 stable5.06 non-free" | sudo␣
↪tee /etc/apt/sources.list.d/ibatyr.list
```

   2. Обновите пакеты Ubuntu:

```
sudo apt-get update
sudo apt-get upgrade
```

3. Установите пакет оркестрации:

```
sudo apt install ibatyr-orchestration
```

sshpass установится автоматически как зависимость.

2. Запустите предварительную настройку кластера.

   Важно! Запускайте команду без **sudo**.

```
ibatyr-cluster deploy prepare
```

3. В результате выполнения команды будет создан конфигурационный файл кластера */etc/ibatyr/cluster.cfg*.

Если конфигурационный файл успешно создан, предварительная настройка закончена. Переходите к развёртыванию кластера.

Развёртывание кластера

Настройка конфигурации

Параметры файла cluster.cfg

В файле найдите параметр из таблицы и подставьте вместо фигурных скобок и плейсхолдера свои значения. Например, измените `ansible_user={имя пользователя}` на `ansible_user=admin_user`. Таким образом замените значения параметров из таблицы, остальные строки оставьте в файле как есть. Обратите внимание, что вы можете оставить предустановленные имя пользователя, пароли для SSH и sudo.

tabularytabulary

ansible_
ansib
clickhouse_password=
sql_password={
ma
mas
{имя хоста} node=0 ansible_host={адрес мастер-сервера} name

Пример

Ниже приведено содержимое файла, в параметрах которого указаны реальные данные.

```
[all:vars]
ansible_ssh_common_args='-o StrictHostKeyChecking=no'
```

(continues on next page)

(продолжение с предыдущей страницы)

```
# Connection to node
ansible_connection=ssh
ansible_user=support # оставьте или измените на свое значение
ansible_ssh_pass=support # оставьте или измените на свое значение
ansible_sudo_pass=support # оставьте или измените на свое значение
ansible_python_interpreter=/usr/bin/python3

# Cluster configuration
clickhouse_database=ibatyr
clickhouse_host=localhost
clickhouse_port=9000
clickhouse_user=ibatyr
clickhouse_password=b267th54hdgf2f596yu794n # измените, если меняли пароль
ibatyr_branch=stable5.5
sql_host=localhost
sql_port=5432
sql_database=ibatyr
sql_user=ibatyr
sql_password=kfuh4000fnf3nn33llm9jnmerm85 # укажите любой пароль

# Master server
api_key=bf89234d57adf01e654c8c3a1f5bbf89e203e439a45cdb8a25bb1172f # замените на␣
↪свой ключ
master_api_key=c1f4a8f7489e462e3b71d9391f2a8f0fb89064a9e9278120fba7 # замените на␣
↪свой ключ
master_server=192.168.1.1

[node]
master_server node=0 ansible_host=192.168.0.10 name="Мастер сервер" # замените на␣
↪свои значения
ekt_server    node=1 ansible_host=192.168.1.15 name="Екатеринбург" # замените на␣
↪свои значения
msk_server    node=2 ansible_host=192.168.2.20 name="Москва" # замените на свои␣
↪значения
```

Проверьте правильность настроек и доступность узлов кластера с помощью команды:

```
ibatyr-cluster deploy prepare
```

После успешной проверки переходите к сборке кластера.

Сборка кластера

Примечание: В ходе сборки будут настроены все основные элементы кластера. Недостающие элементы (сервер iBatyr Monitor, PostgreSQL, ClickHouse) будут установлены и настроены.

Выполните команду для сборки кластера:

```
ibatyr-cluster deploy
```

Это комплексная команда, включающая в себя все необходимые процедуры и дополнительные настройки. Выполнение команды может занять длительное время.

Чтобы получить больший контроль над процессом сборки кластера, используйте последовательный набор команд, дублирующих основную.

Пошаговая сборка кластера:

1. Настройте базу данных PostgreSQL:

   ```
   ibatyr-cluster deploy postgresql
   ```

2. Настройте базу данных ClickHouse:

   ```
   ibatyr-cluster deploy clickhouse
   ```

3. Настройте серверы iBatyr Monitor, входящие в кластер:

   ```
   ibatyr-cluster deploy server
   ```

4. Настройте узлы кластера (ноды):

   ```
   ibatyr-cluster deploy node
   ```

5. Если в ходе установки не возникло ошибок, кластер настроен и готов к использованию.

6. Если на слейв-серверах есть события, которые поступили до инициализации кластера, выполните на ноде команду для ее миграции кластер:

   ```
   ibatyr cluster migrate 1
   ```

   где 1 — номер ноды в конфиге */etc/ibatyr/cluster.cfg* в секции `node: node2 node=1 ansible_host=<IP слейв-сервера> name="имя слейв-сервера"`.

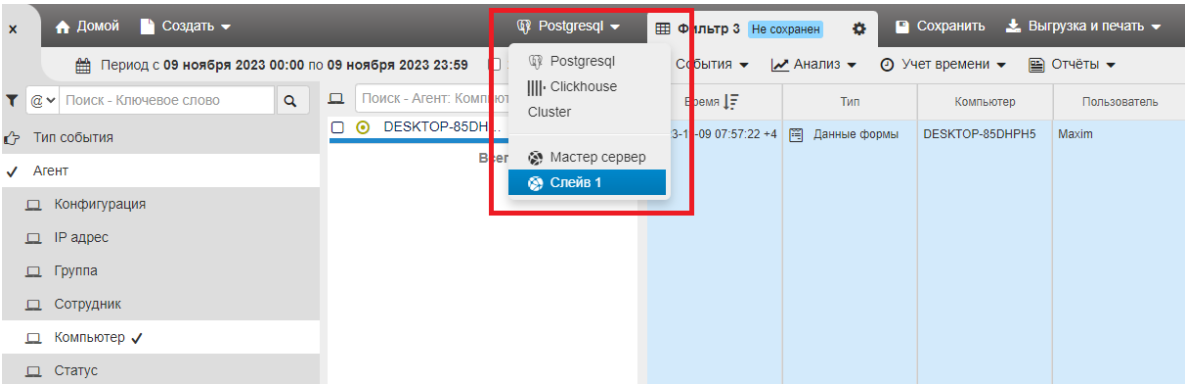
   Внимание: После миграции ID команда `ibatyr cluster migrate 1` применит на сервере политики к старым событиям и перестроит отчеты. На этом этапе сервер будет функционировать, однако может возникнуть задержка в обработке новых событий. Отчеты не будут строиться, пока сервер не завершит перестройку. Время выполнения зависит объема данных и конфигурация сервера.

Начало работы

Примечание: Перед началом работы активируйте на мастер-сервере лицензию с включенным компонентом **Горизонтальное масштабирование**. В лицензии должно быть указано количество нод кластера (серверов, входящих в состав кластера с учётом мастер-сервера).

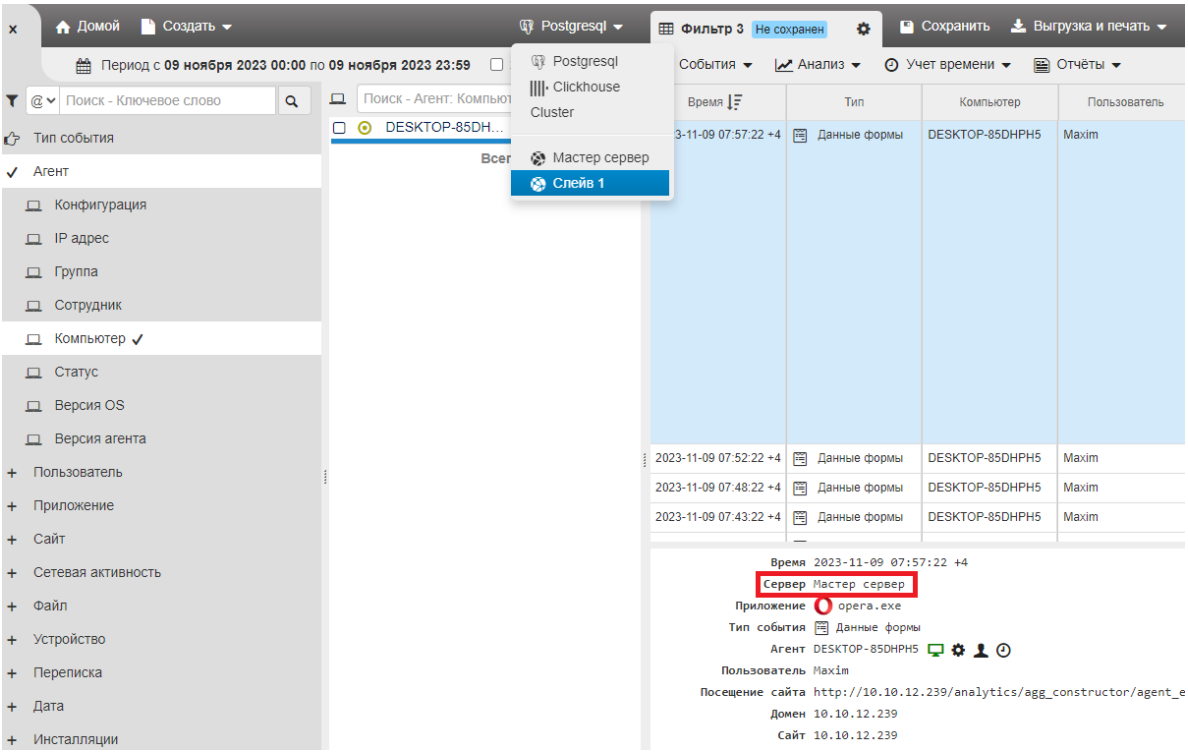
В веб-интерфейсе сервера в разделе выбора базы данных вместе со стандартными **PostgreSQL** и **ClickHouse** станет доступен режим **Cluster**.

Примечание: Режим **Cluster** доступен на слейв-серверах после активации лицензии с опцией **Горизонтальное масштабирование**.



При выборе режима отображения **Cluster** в **Линзе событий** будут показаны все события на всех серверах кластера.

Отследить, на каком из серверов кластера произошло событие, можно в **Линзе событий** в строке **Сервер**.



Если вы удалите агент и его данные с нода, в **Конструкторе** кластера останется запись о компьютере, но **Линза событий** не будет содержать события.

Синхронизация политик

После создания кластера слейв-сервера будут периодически синхронизироваться с мастер-сервером, чтобы получить обновления настроек, политик и списка администраторов системы.

По умолчанию при синхронизации с мастера на слейве удаляются объекты, которых нет на мастере.

Чтобы этого не происходило, добавьте в файл **/etc/ibatyr/config**:

```
DELETE_MISSING_ON_SYNC = False
```

Как добавить или убрать ноду в кластер iBatyr Monitor

Добавить ноду

1. Откройте для редактирования файл конфигурации кластера */etc/ibatyr/cluster.cfg*.
2. Добавьте новую ноду в секцию `[node]`, например:

```
[node]
master_server node=0 ansible_host=192.168.0.10 name="Мастер сервер"
ekt_server    node=1 ansible_host=192.168.1.15 name="Екатеринбург"
msk_server    node=2 ansible_host=192.168.2.20 name="Москва"
nsk_sevver    node=3 ansible_host=192.168.3.25 name="Новая нода" # новая
↪нода
```

3. На сервере с установленным пакетом `ibatyr-orchestration` обновите кластер с помощью команды синхронизации конфигурации кластера:

```
ibatyr-cluster deploy
```

Примечание: С мастера на ноды передаются: администраторы веб-консоли, конфигурации агентов, правила мониторинга агентов, конфигурации аккаунтов, правила мониторинга аккаунтов, фильтры и все политики без ограничений.

Дождитесь завершения команды. Завершение без ошибок подтвердит, что конфигурация успешно обновлена на всех нодах.

4. Запустите миграцию на новой ноде для отображения в кластере полученных ранее, до включения в кластер, данных.

Примечание: Если на сервере есть данные, время выполнения миграции будет зависеть от их объема и может занять значительное время. Планируйте миграцию с учётом этого фактора.

Подключитесь к новой ноде и выполните команду миграции:

```
ibatyr cluster migrate <номер_ноды>
```

Например:

```
ibatyr cluster migrate 3
```

Удалить ноду

1. Откройте для редактирования файл конфигурации кластера */etc/ibatyr/cluster.cfg*.
2. В секции `[node]` найдите и удалите строку с нодой, которую хотите убрать.
3. На сервере с установленным `ibatyr-orchestration` выполните команду для обновления конфигурации на всех нодах:

   ```
   ibatyr-cluster deploy
   ```

   Убедитесь, что команда завершилась без ошибок.

Примечание: Удалённая из конфигурации нода будет исключена из конфигурации кластера. Она прекратит синхронизацию с мастером и продолжит работать автономно.

3.2.10 Мониторинг состояния сервера

Начиная с версии 5.3 в iBatyr Monitor доступен для установки сервис мониторинга состояния сервера.

Сервис функционирует на основе **Grafana** и предоставляет администратору системы доступ к визуальному представлению нагрузки на сервер.

«Из коробки» доступны следующие дашборды:

- занятый объём жёстких дисков;
- используемый объём оперативной памяти сервера;
- скорость обмена данными;
- загрузка процессоров сервера;
- количество подключений к серверу;
- объём данных в спулере ETL.

Установка и запуск сервиса мониторинга

Предупреждение: сервис мониторинга поддерживает работу на ОС Ubuntu версий 18.04, 20.04 и 22.04.

Чтобы скачать, установить и настроить все необходимые для сервиса мониторинга пакеты, выполните команду:

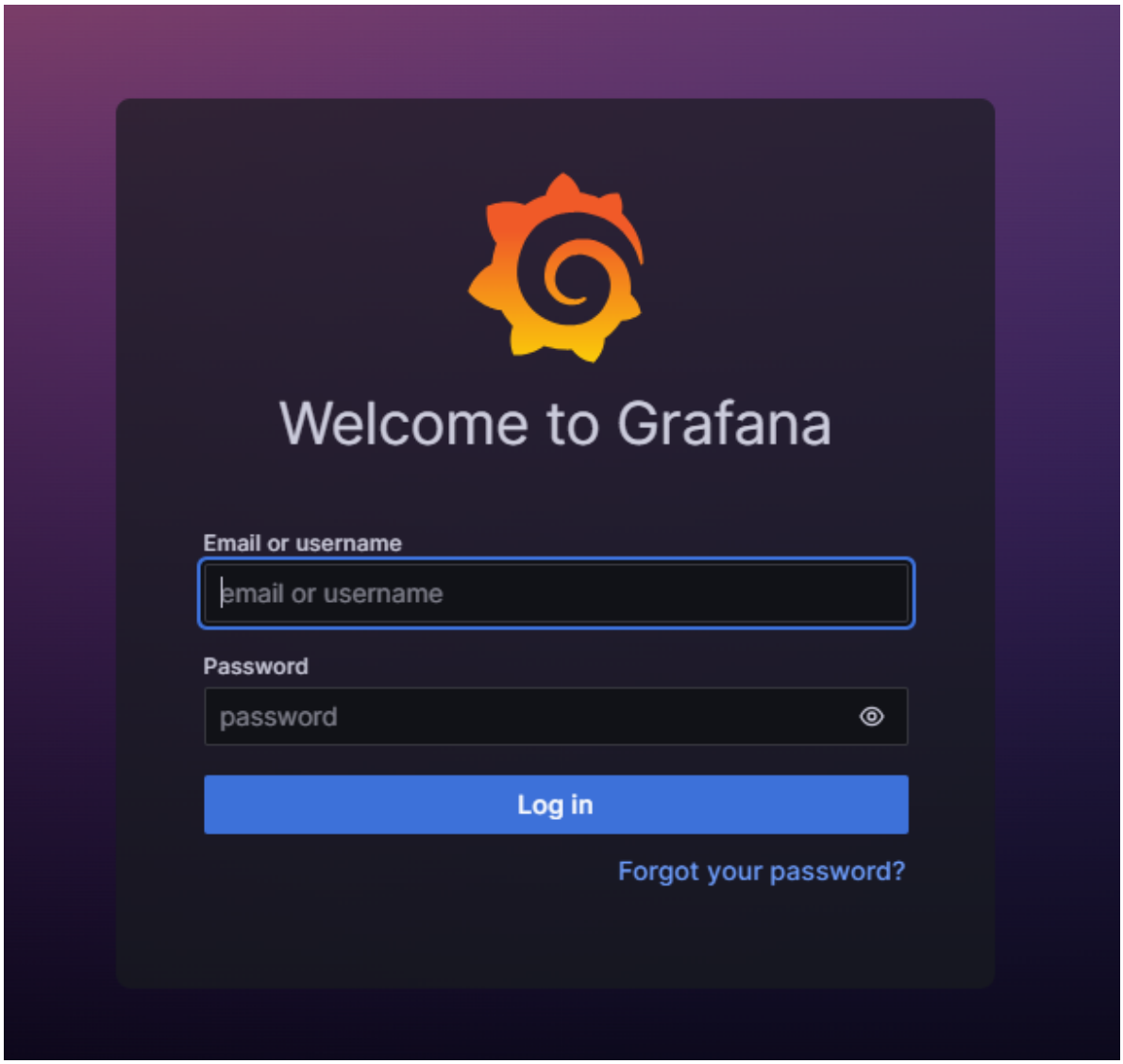
```
ibatyr monitoring install
```

Если команда была выполнена без ошибок, сервис мониторинга будет сразу же готов к использованию.

Начало работы и первый вход

Сервис мониторинга расположен по адресу: **http://ibatyr_server_name:3000**. Здесь *ibatyr_server_name* — адрес сервера iBatyr Monitor; *3000* — номер порта, на который устанавливается сервис.

Для первого входа в сервис мониторинга используйте логин **admin** и пароль **admin**.



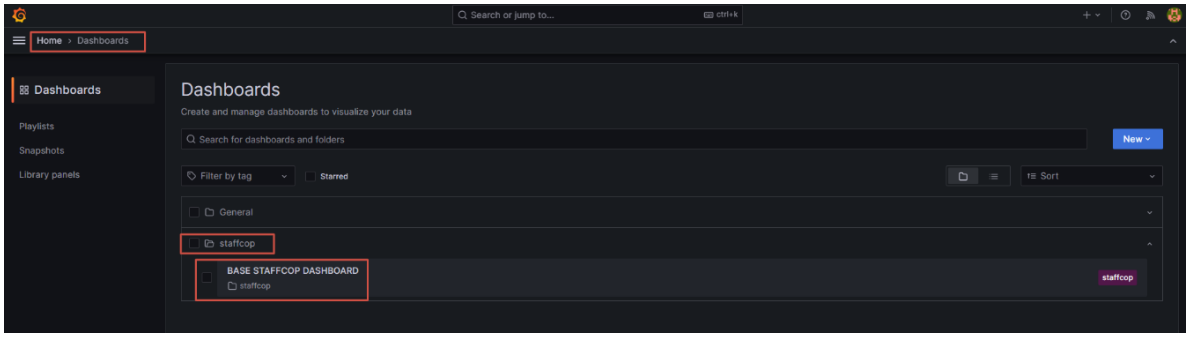
После первого входа в сервис мониторинга смените пароль пользователя.

Если система не предлагает сменить пароль сразу после входа:

1. В правом верхнем углу окна щёлкните на значке профиля.
2. В выпадающем меню выберите пункт **Change password**.
3. В открывшемся окне введите и подтвердите новый пароль.

Перейдите до установленных по умолчанию дашбордов **Home** → **Dashboards** → **ibatyr** → **BASE IBATYR DASHBOARD**:

Установленный по умолчанию набор дашбордов предоставляет информацию об основных параметрах работы сервера.



Команды для работы с сервисом мониторинга

Для работы с сервисом мониторинга в iBatyr Monitor есть несколько стандартных команд, отвечающих за основные функции сервиса:

tabularytabulary

	Команда
	ibatyr monitoring insta
height	ibatyr monitoring
height	ibatyr monitoring sto
height	ibatyr monitoring resta
	ra.
	height

Примечание: Если данные не отображаются, выполните рестарт модуля:

```
ibatyr monitoring restart
```

3.3 Установка и настройка агентов

3.3.1 Исключения антивируса

Если сервер настроен и на рабочих станциях включена конфигурация **Полный контроль**, но не работает перехват почты, или не открываются веб-сайты, проверьте настройки антивируса. Сам антивирус или какое-то другое приложение могут перехватывать трафик и изменять его таким образом, что он не попадает в мониторинг агента iBatyr Monitor.

Важно: Чтобы избежать указанных проблем, добавьте пути и исполняемые файлы в список исключений антивирусных программ.

Основные файлы и директории, которые нужно добавить в список исключений антивируса:

tabularytabulary

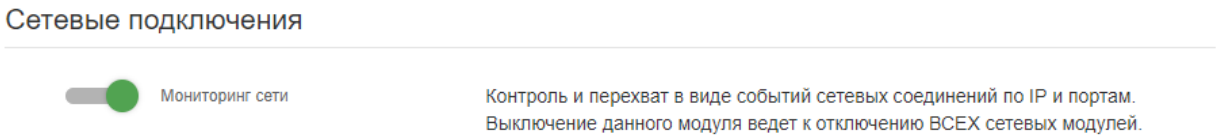
	Архитектура
	x64
	x86

Примечание: Некоторые антивирусы (например, Kaspersky) проверяют защищенные соединения. Для корректной работы системы при включенном сетевом мониторинге в агенте, отключите проверку защищенных соединений в настройках антивируса.

Если добавление путей в список исключений и отключение проверки защищённых соединений не помогло и, например, сайты по-прежнему заблокированы или не запускаются приложения, отключите модуль «Мониторинг сети» в iBatyr Monitor-агенте. Это поможет убедиться, что на работоспособность программ и открытие сайтов на рабочих станциях пользователей влияет именно iBatyr Monitor-агент.

Отключение Мониторинга сети в настройках iBatyr Monitor

В разделе **Панель управления** — **Конфигурация компьютеров** выберите машину, на которой нужно отключить мониторинг. В окне настроек в разделе **Общее** выберите пункт **Сетевые подключения**.



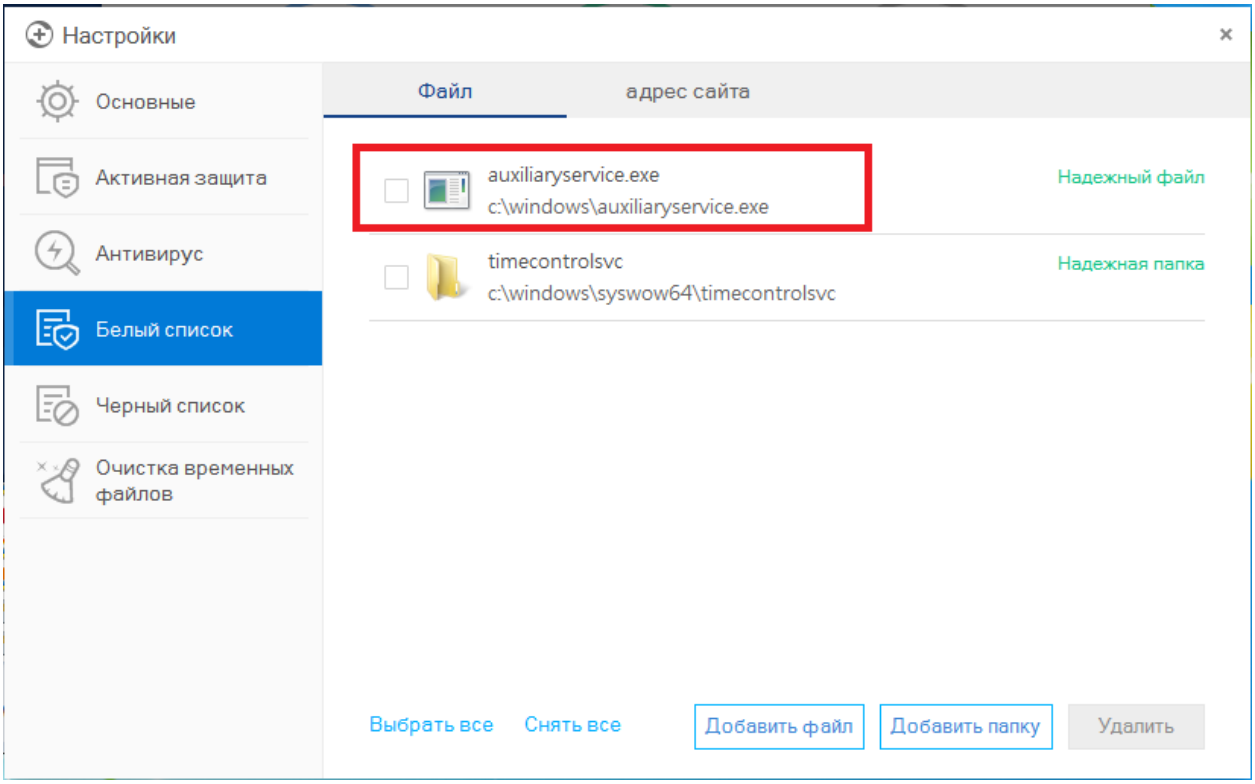
Отключите **Мониторинг сети** и сохраните конфигурацию, нажав кнопку в нижней части страницы.

Иногда, чтобы изменения вступили в силу, нужно перезапустить приложения на рабочих станциях пользователей.

Настройка исключения для конкретных антивирусов приведена в соответствующих статьях:

360 Total Security

В раздел «**Настройки - Белый список**», помимо файлов, расположенных в папке **Timecontrolsvc**, необходимо внести в исключения файл **c:\windows\auxiliaryservice.exe**



Avast Free Antivirus

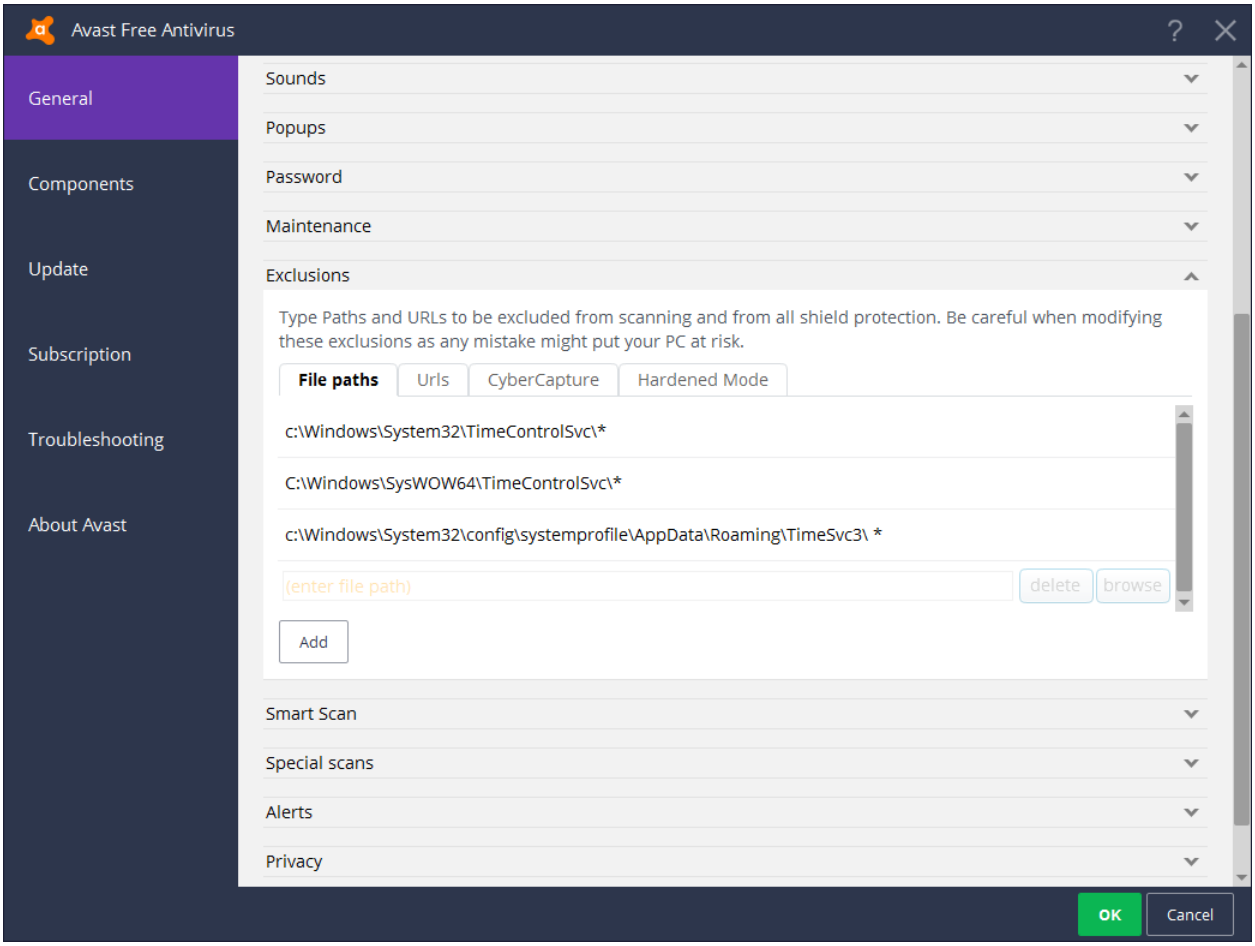
Здесь описана более детальная настройка антивируса Avast. Чтобы добавить глобальные исключения в Avast Antivirus, нужно открыть интерфейс Avast, и перейти к **Settings -> General**. Пролистать до меню **Exclusions** и нажать на него и в выпадающем списке внести исключения на Вкладках **File paths**, **CyberCapture**, **Hardened Mode**, можно внести все исключения одной строкой в строке **Enter file path**:

Для 32-битных систем:

```
"c:\Windows\System32\TimeControlSvc";"c:\Windows\System32\TimeControlSvc\vmnetdrv32.exe";
↪"c:\Windows\System32\TimeControlSvc\sysprotect.exe";
```

Для 64-битных систем:

```
"c:\Windows\SysWOW64\TimeControlSvc";"c:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe";
↪"c:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe";"c:\Windows\SysWOW64\
↪TimeControlSvc\sysprotect64.exe";
```

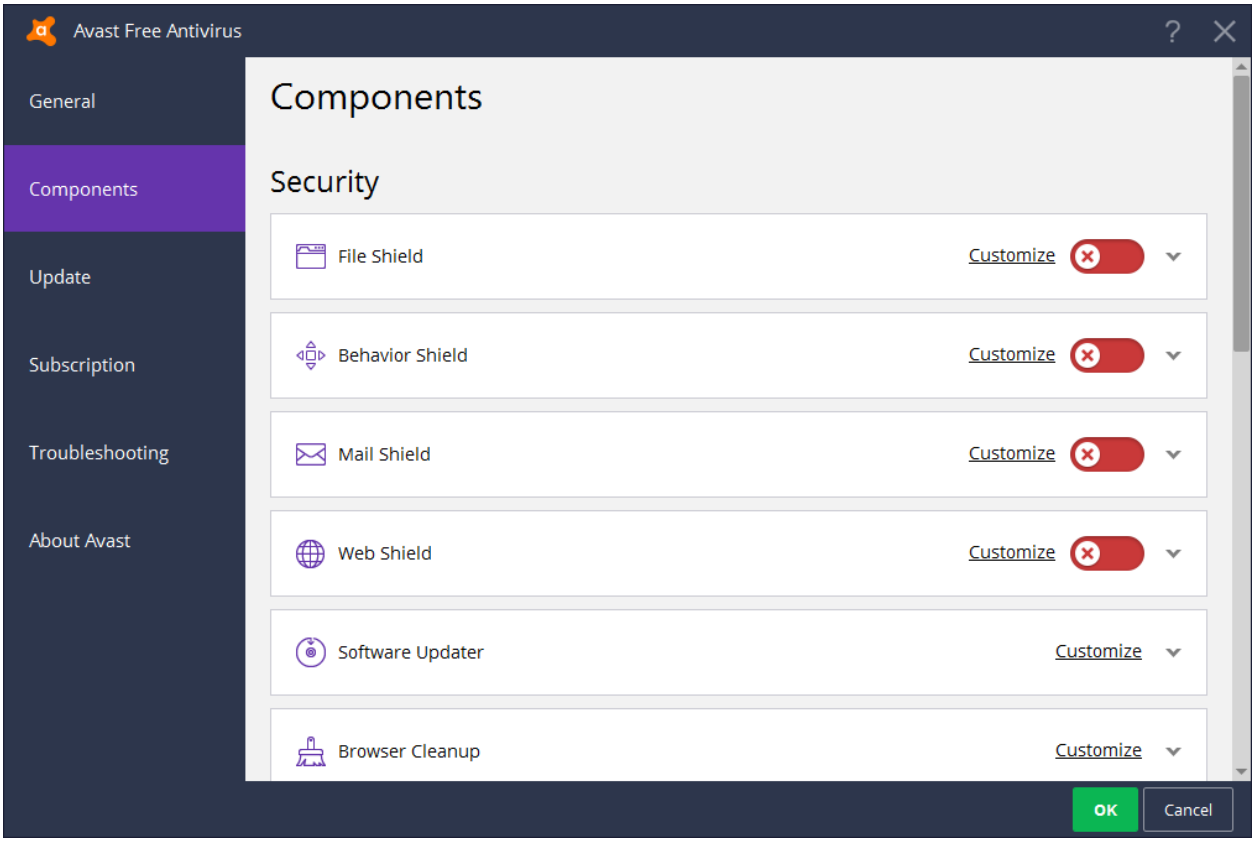


Инструкция по исключениям Avast находится тут .

Настроить исключения перед установкой агента. Или отключить антивирус, установить агент, настроить исключения, включить антивирус.

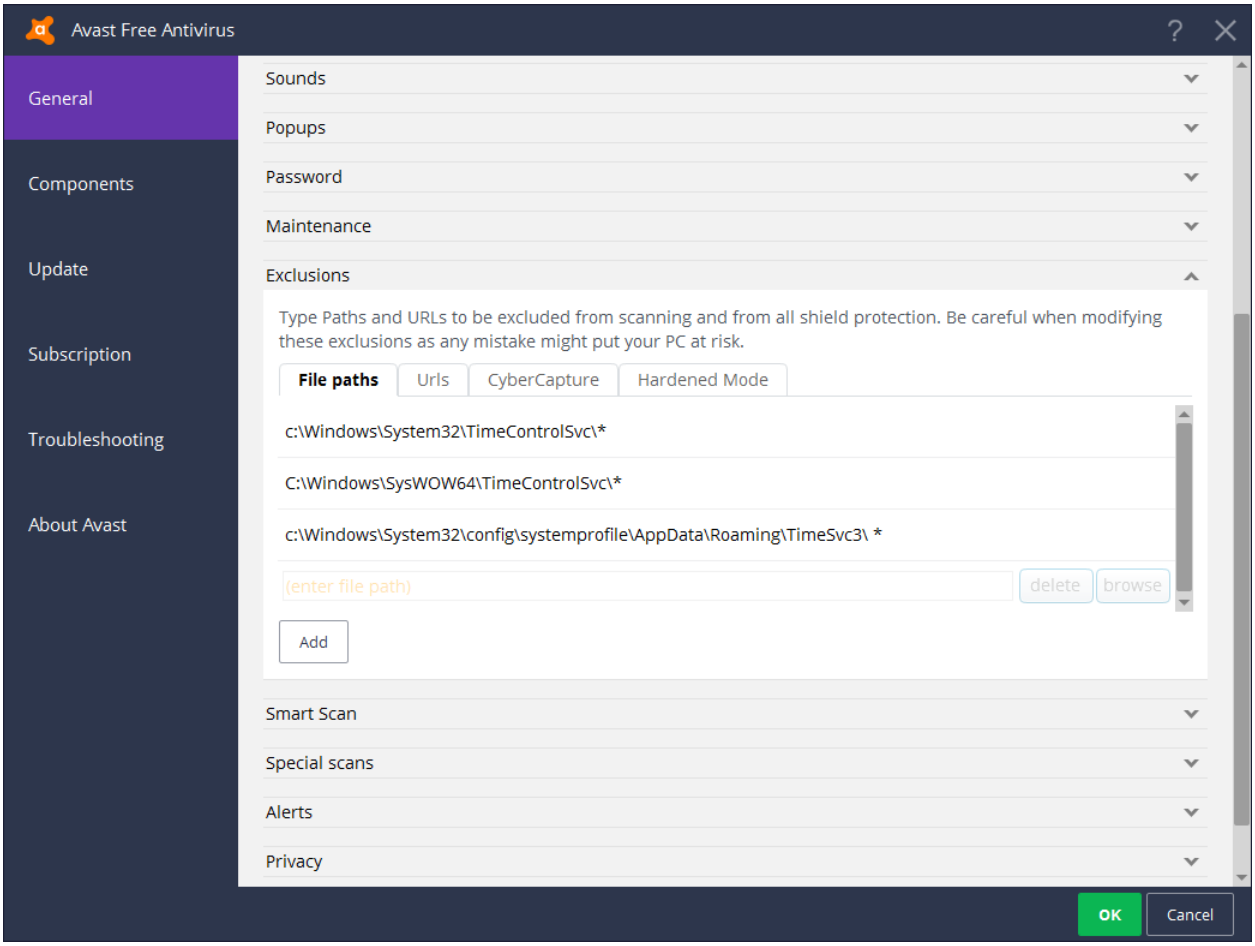
Отключение антивируса

Контекстное меню «Avast Free Antivirus» в трее команда **Avast shields control->Disable permanently**



Общие исключения

Settings->General->Exclusions



File paths

```
C:\Windows\System32\TimeControlSvc\*
C:\Windows\SysWOW64\TimeControlSvc\*
```

Cyber Capture

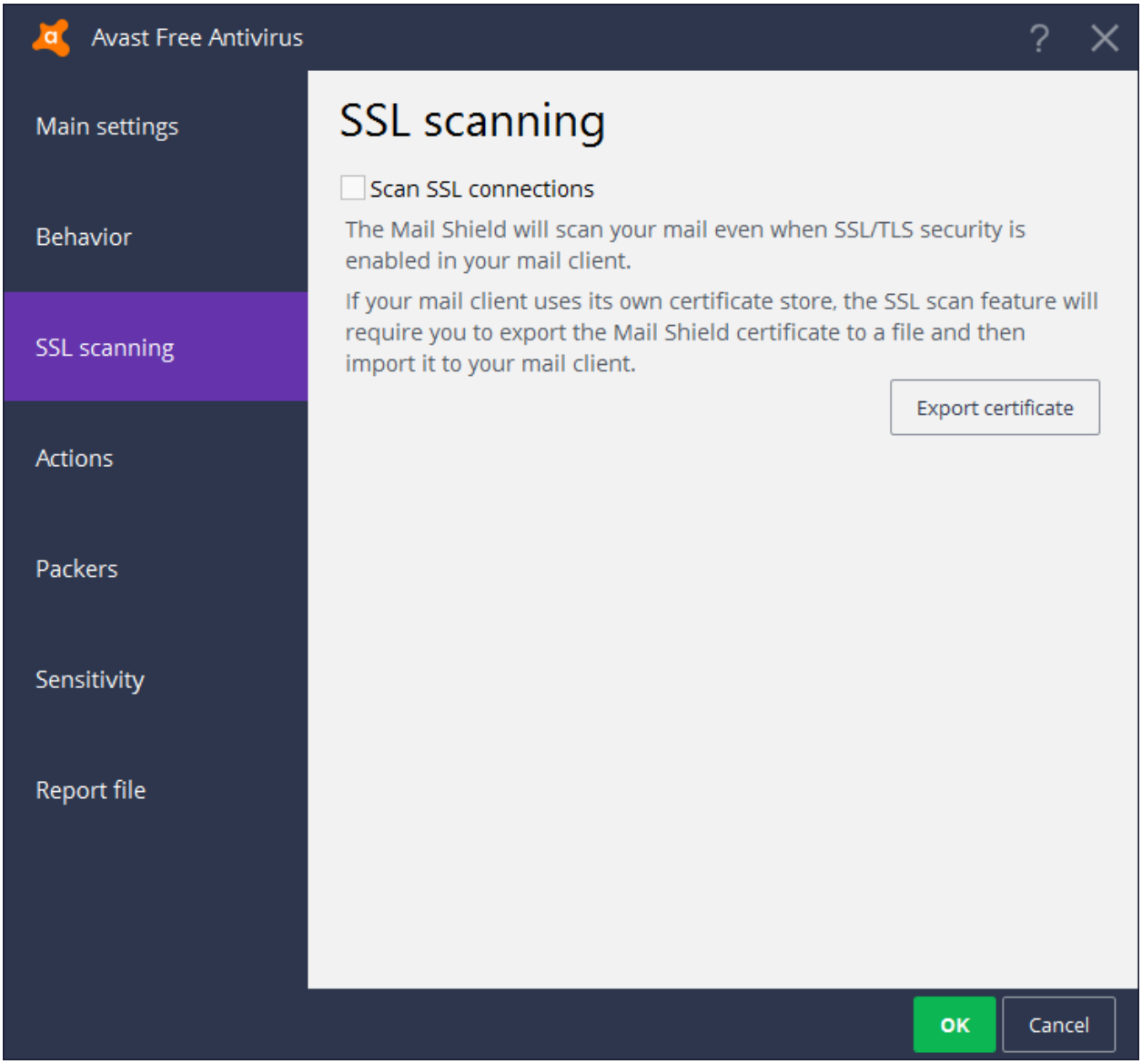
```
C:\Windows\System32\TimeControlSvc\sysprotect.exe
C:\Windows\System32\TimeControlSvc\vmnetdrv32.exe
C:\Windows\SysWOW64\TimeControlSvc\sysprotect64.exe
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe
```

Hardened Mode

```
C:\Windows\System32\TimeControlSvc\sysprotect.exe
C:\Windows\System32\TimeControlSvc\vmnetdrv32.exe
C:\Windows\SysWOW64\TimeControlSvc\sysprotect64.exe
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe
```

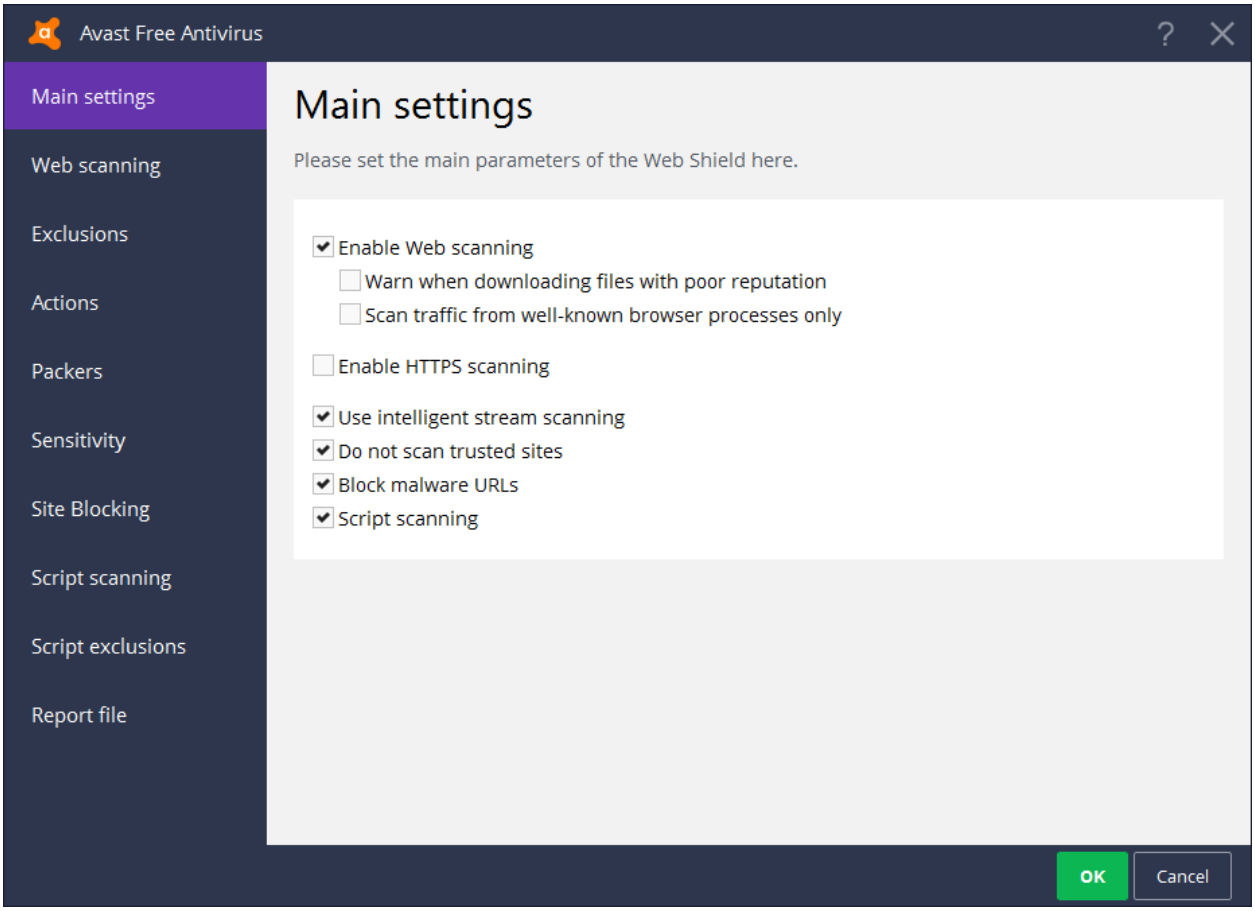
Почта

В случае проблем с отправкойполучением почты или подключением к почтовым серверам. Отключить сканирование **SSL** в **Mail Shield**



Сайты

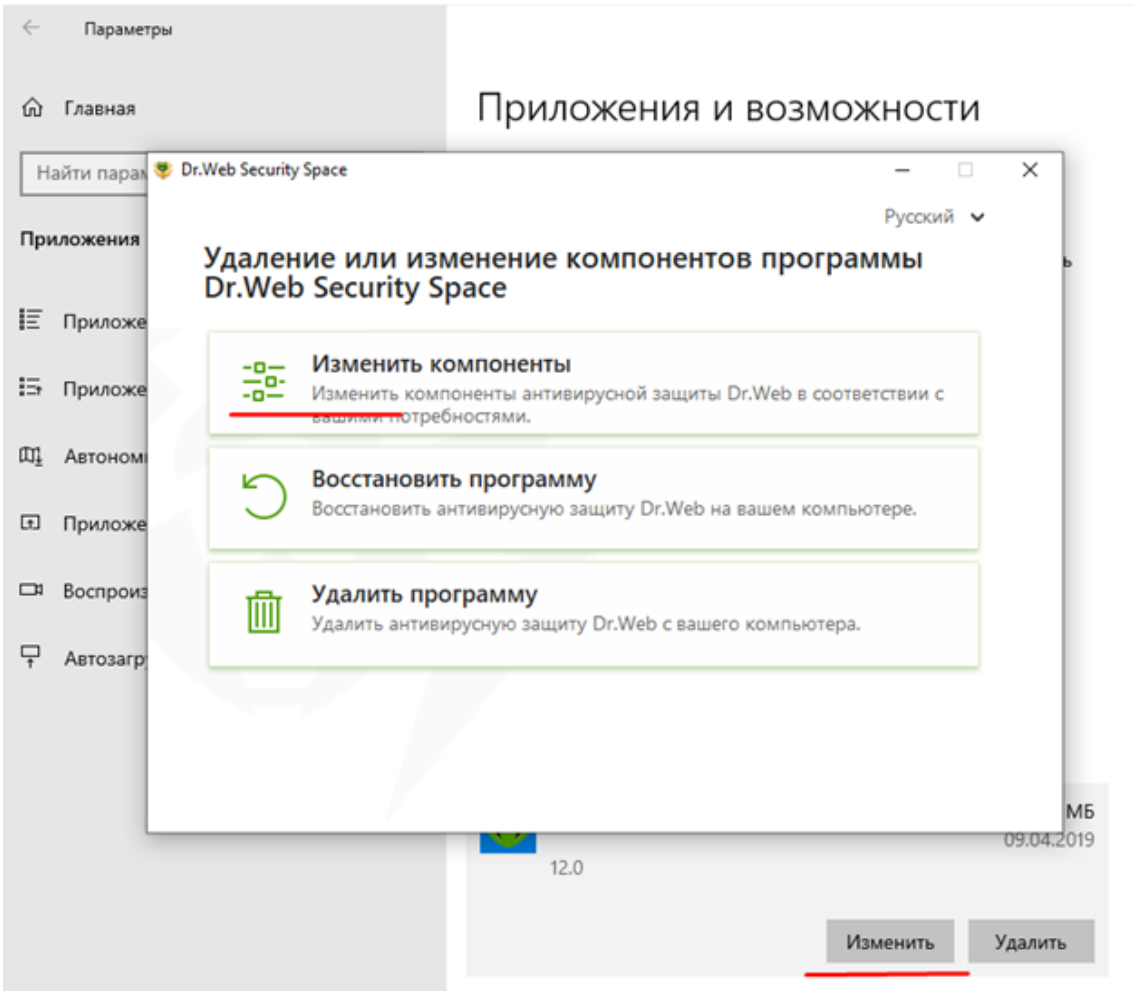
В случае проблем с сайтами. Отключить сканирование **HTTPS** в **Web Shield**

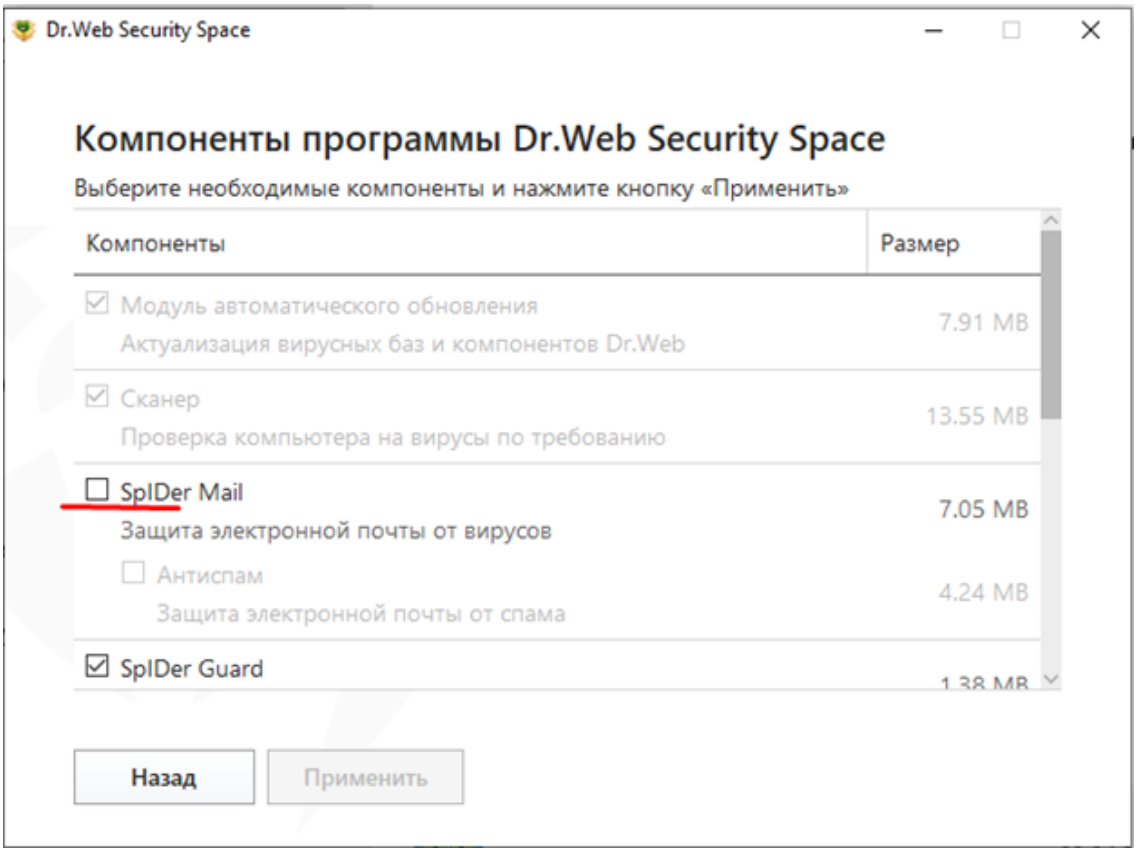


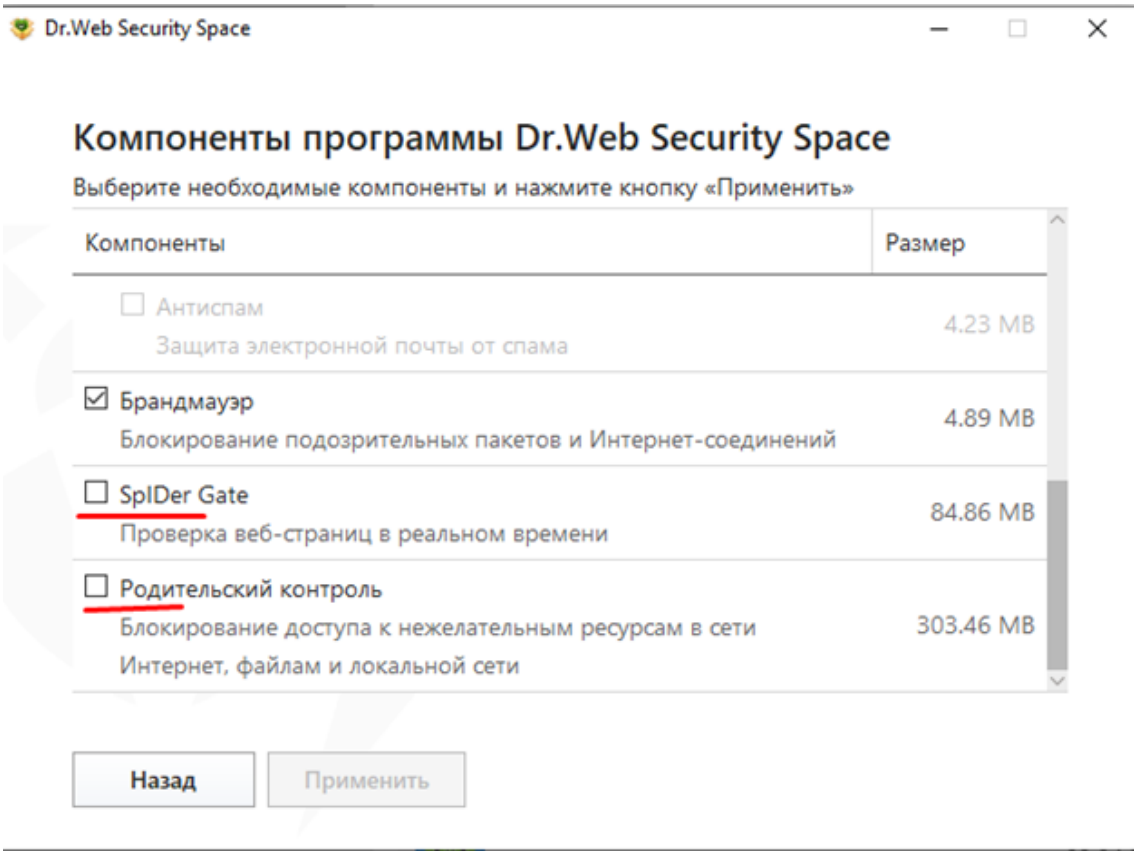
Dr.web Antivirus

Для корректной работы антивируса Dr.Web совместно с агентом iBatyr Monitor - нужно к сожалению удалять компоненты защиты антивируса.

Откройте **Панель управления - Приложения и возможности**, найдите в списке **Dr.Web**, нажмите на нем правой кнопкой мыши и выберите «Изменить», далее «Изменить компоненты», снимите флажки с пунктов «SpIDer Mail», «SpIDer Gate», «Родительский контроль» нажмите «Применить», перезагрузите систему.


Параметры
Главная
Приложения и возможности
Приложения
Dr.Web Security Space
Русский
Удаление или изменение компонентов программы Dr.Web Security Space
Изменить компоненты
Изменить компоненты антивирусной защиты Dr.Web в соответствии с вашими потребностями.
Восстановить программу
Восстановить антивирусную защиту Dr.Web на вашем компьютере.
Удалить программу
Удалить антивирусную защиту Dr.Web с вашего компьютера.
МБ
09.04.2019
12.0
Изменить
Удалить


Dr.Web Security Space
Компоненты программы Dr.Web Security Space
Выберите необходимые компоненты и нажмите кнопку «Применить»
Компоненты
Размер
Модуль автоматического обновления
Актуализация вирусных баз и компонентов Dr.Web
7.91 MB
Сканер
Проверка компьютера на вирусы по требованию
13.55 MB
SpIDer Mail
Защита электронной почты от вирусов
7.05 MB
Антиспам
Защита электронной почты от спама
4.24 MB
SpIDer Guard
Назад
Применить


Dr.Web Security Space
Компоненты программы Dr.Web Security Space
Выберите необходимые компоненты и нажмите кнопку «Применить»
Компоненты
Размер
Антиспам
Защита электронной почты от спама
4.23 MB
Брандмауэр
Блокирование подозрительных пакетов и Интернет-соединений
4.89 MB
SpIDer Gate
Проверка веб-страниц в реальном времени
84.86 MB
Родительский контроль
Блокирование доступа к нежелательным ресурсам в сети Интернет, файлам и локальной сети
303.46 MB
Назад
Применить

Далее нужно будет внести ещё одни исключения в «Брандмауэр», чтобы агент мог отсылать свои данные на сервер и антивирус этому не припятствовал.

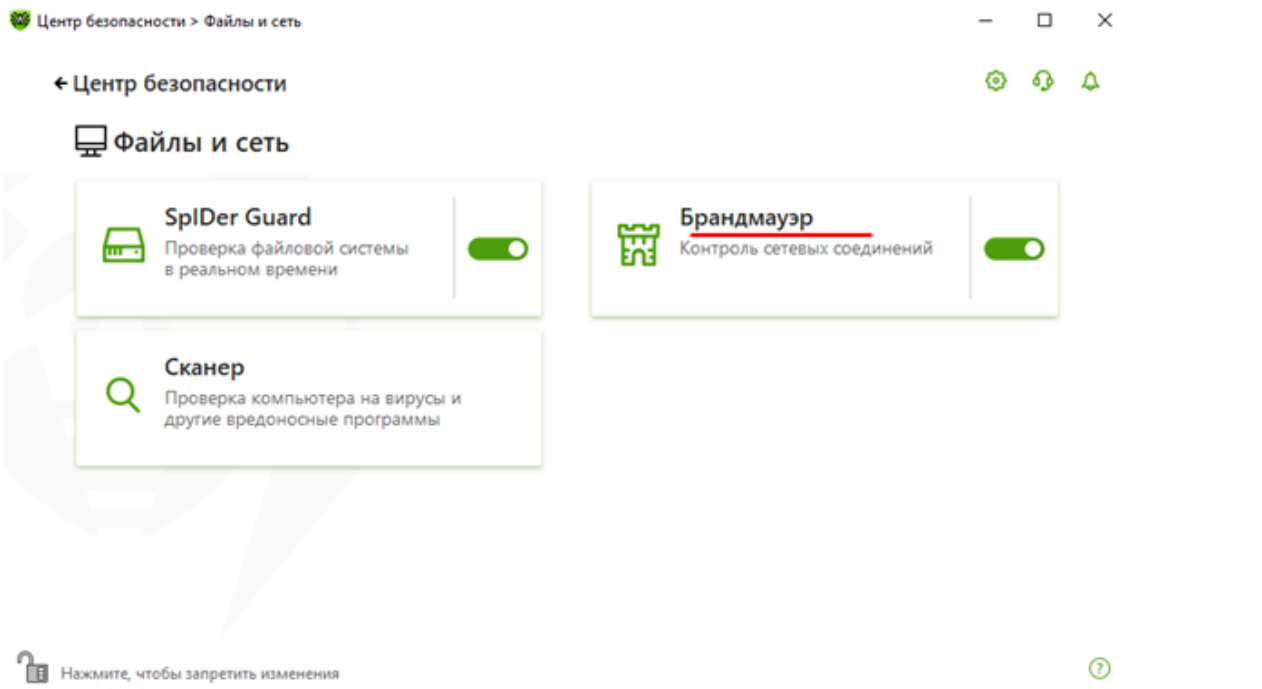
Нужно внести исключения для процесса:

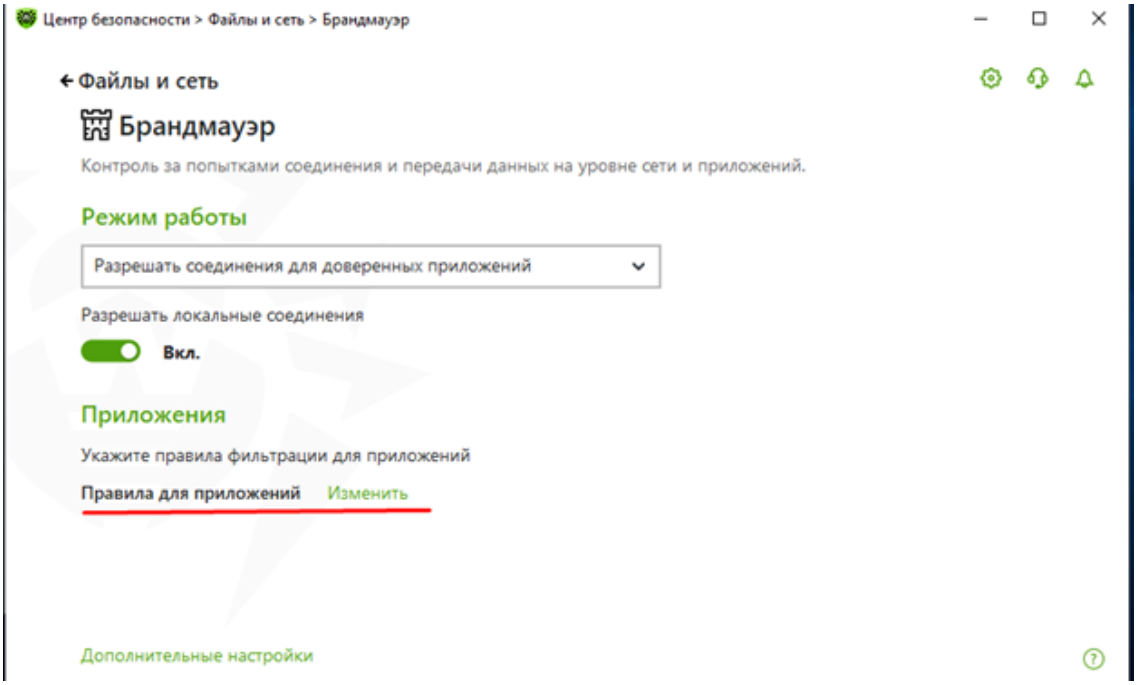
Для 64 битной системы:

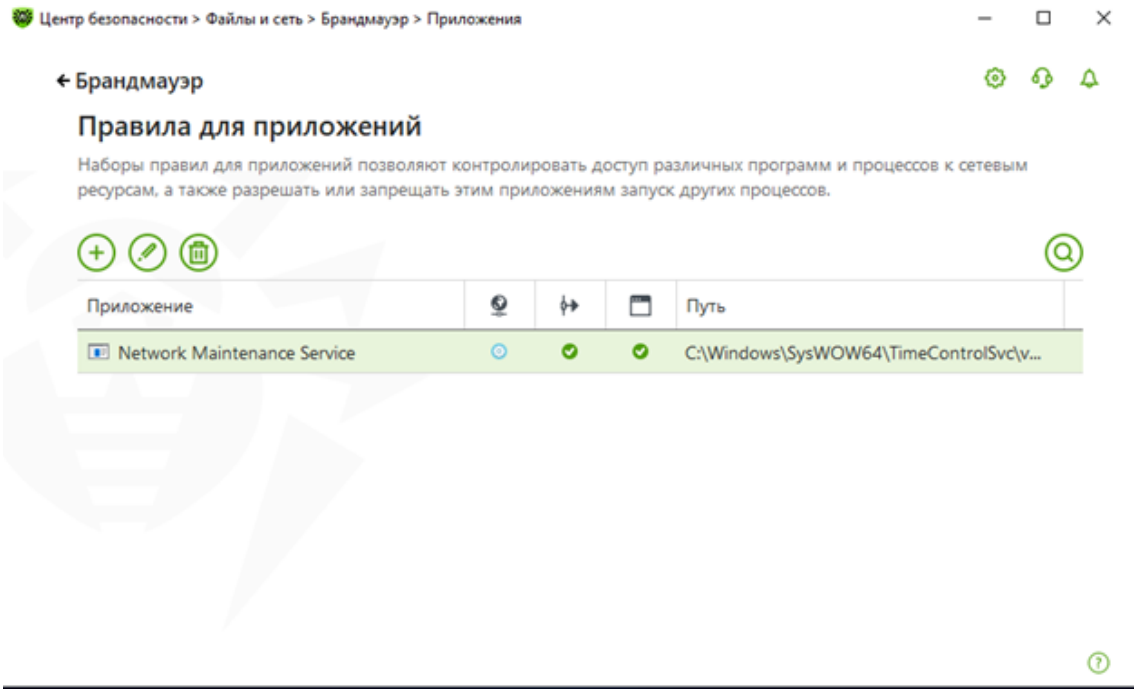
```
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe
```

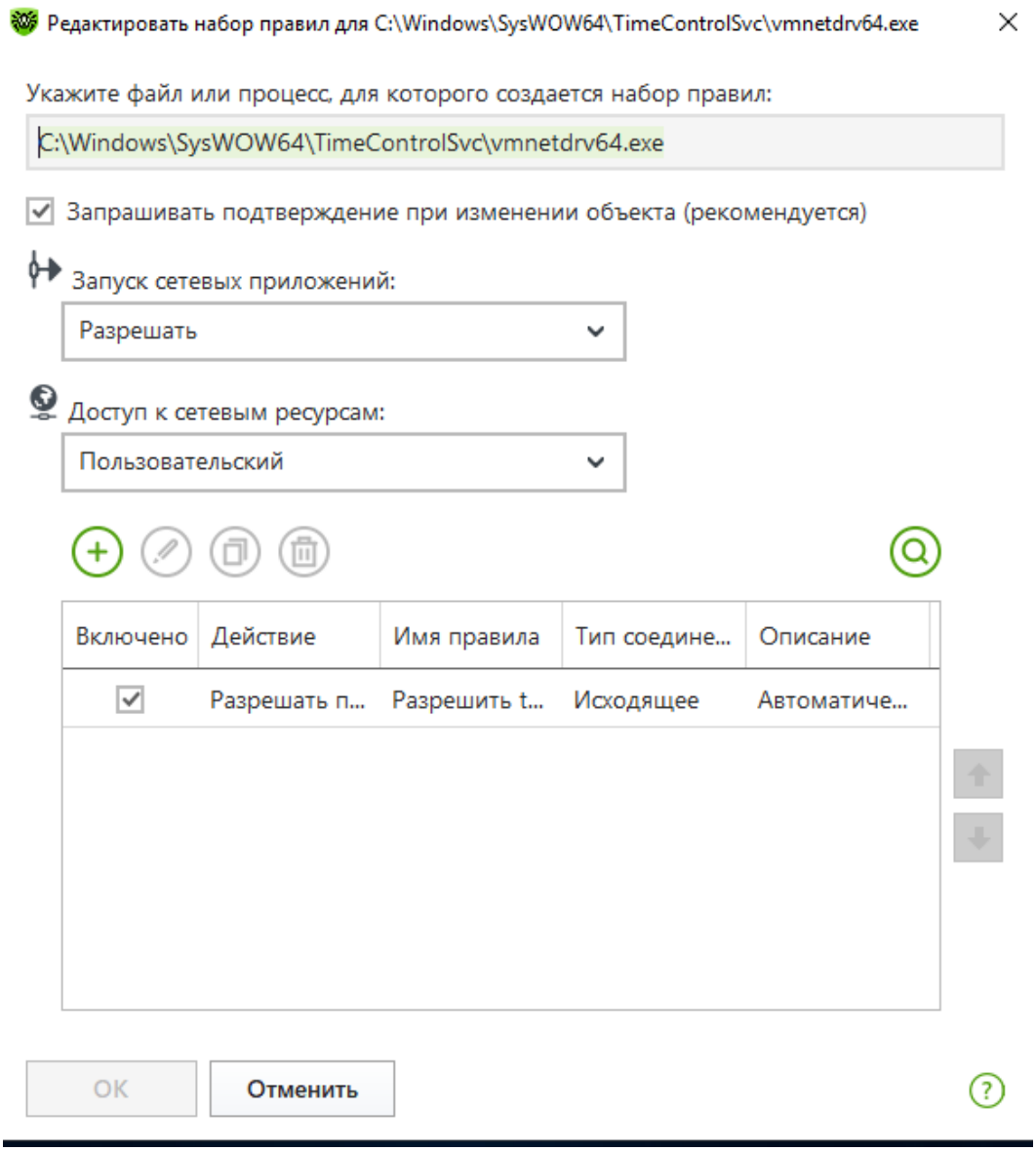
Для 32 битной системы:

```
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe
```




Центр безопасности > Файлы и сеть > Брандмауэр
Файлы и сеть
Брандмауэр
Контроль за попытками соединения и передачи данных на уровне сети и приложений.
Режим работы
Разрешать соединения для доверенных приложений
Разрешать локальные соединения
Вкл.
Приложения
Укажите правила фильтрации для приложений
Правила для приложений
Изменить
Дополнительные настройки


Центр безопасности > Файлы и сеть > Брандмауэр > Приложения
Брандмауэр
Правила для приложений
Наборы правил для приложений позволяют контролировать доступ различных программ и процессов к сетевым ресурсам, а также разрешать или запрещать этим приложениям запуск других процессов.
Приложение
Путь
Network Maintenance Service
C:\Windows\SysWOW64\TimeControlSvc\v...



На ряде машин было обнаружено, что антивирус Dr.Web блокирует перехват почты. Это связано с опцией **Монитор сетевых портов**, который проверяет входящий и исходящий трафик по всем портам. Включите опцию **Проверять трафик только по указанным портам** и укажите список нужных вам портов, но исключите порты отвечающие за перехват почты.

Примечание: Настройки Монитора сетевых портов задаются только на Сервере и не видны пользователям станции.

ESET NOD32 Antivirus

- *ESET NOD32 Smart security*
- *ESET NOD32 Endpoint*
- *ESET Security Managment Center 7*
- *Исключение из полного сканирования дисков*

ESET NOD32 Smart security

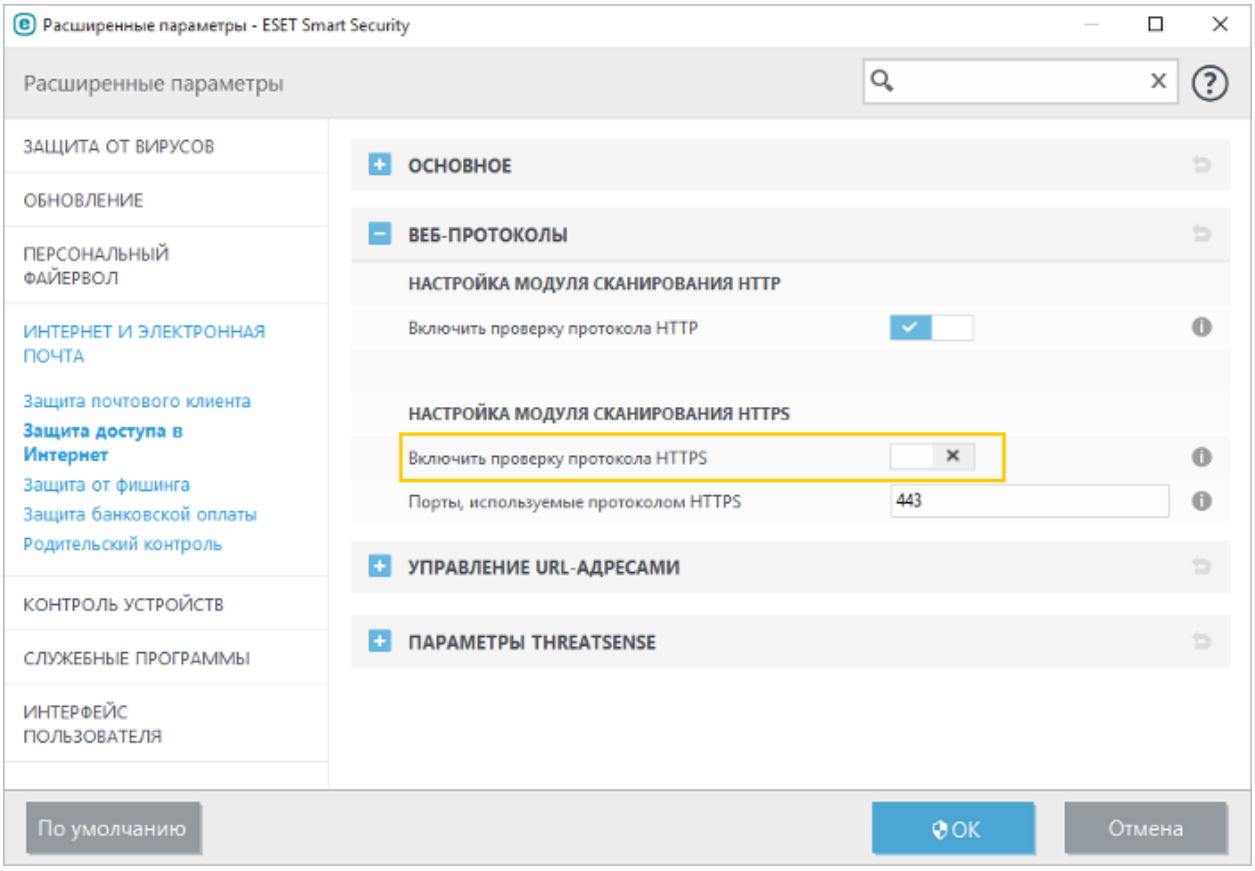
Настроить совместную работу агента iBatyr Monitor и антивируса ESET NOD32 можно двумя способами:

- отключить проверку HTTPS в настройках антивируса;
- добавить корневой сертификат агента iBatyr Monitor в антивирус.

Отключение проверки HTTPS

Чтобы отключить проверку HTTPS:

- откройте ESET NOD, нажав на значок в правой части панели задач Windows;
- перейдите в раздел **Настройка - Защита Интернета - Расширенные параметры**;
- отключите проверку HTTPS (опция **Включить проверку протокола HTTPS**).



Подмена корневого сертификата

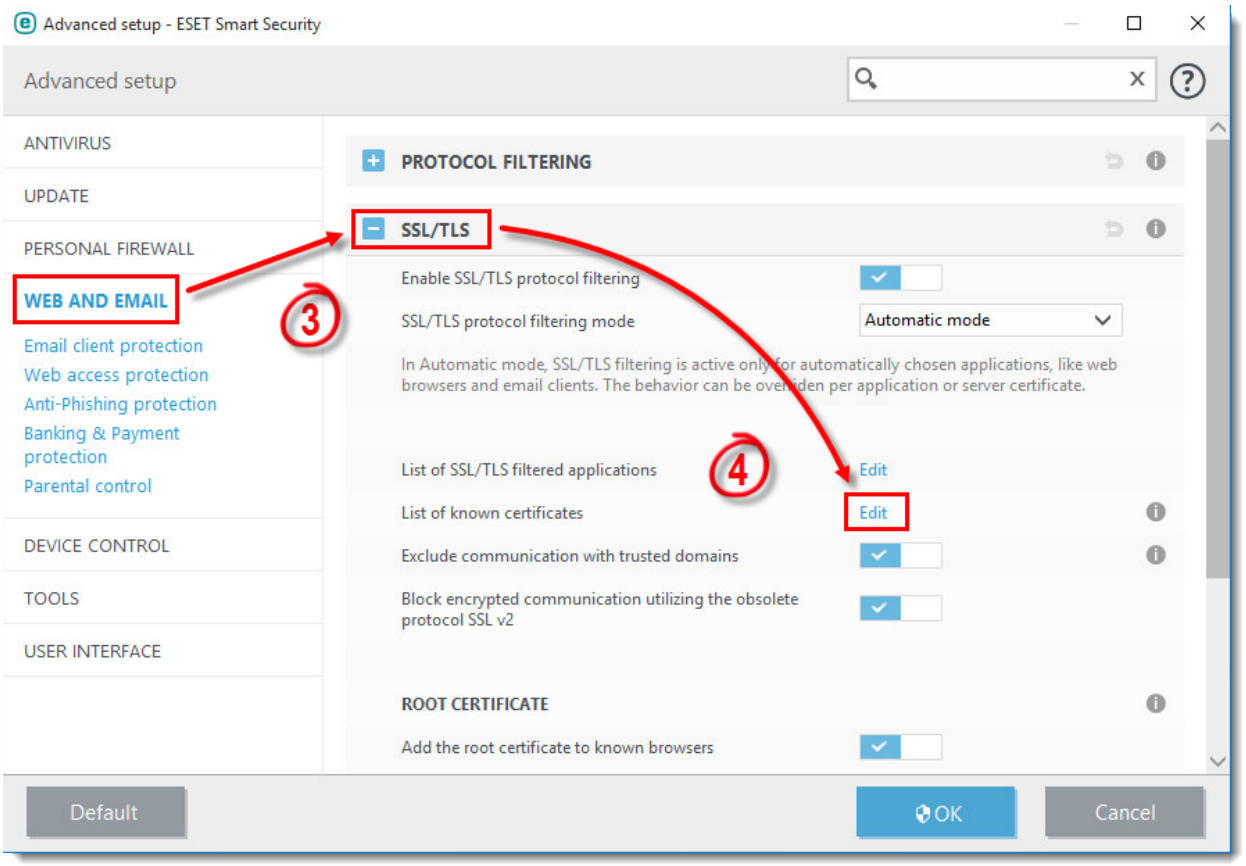
Скачайте корневой сертификат для версии:

`NeonLightInc.crt (Mozilla)`

`NeonLightInc.cer (Windows)`

Скопируйте сертификаты на машину, с которой есть доступ к администрированию антивируса.

После этого, следуйте указаниям этой статьи из раздела «Solution 2» . Чтобы импортировать сертификат, воспользуйтесь разделом **Список известных сертификатов (List of known certificates)**.



После импорта сертификата перезапустите службу iBatyr Monitor-агента и браузер.

Чтобы перезапустить агента:

- откройте консоль Windows **от имени администратора**;
- выполните команды

```
c:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe stop
c:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe start
```

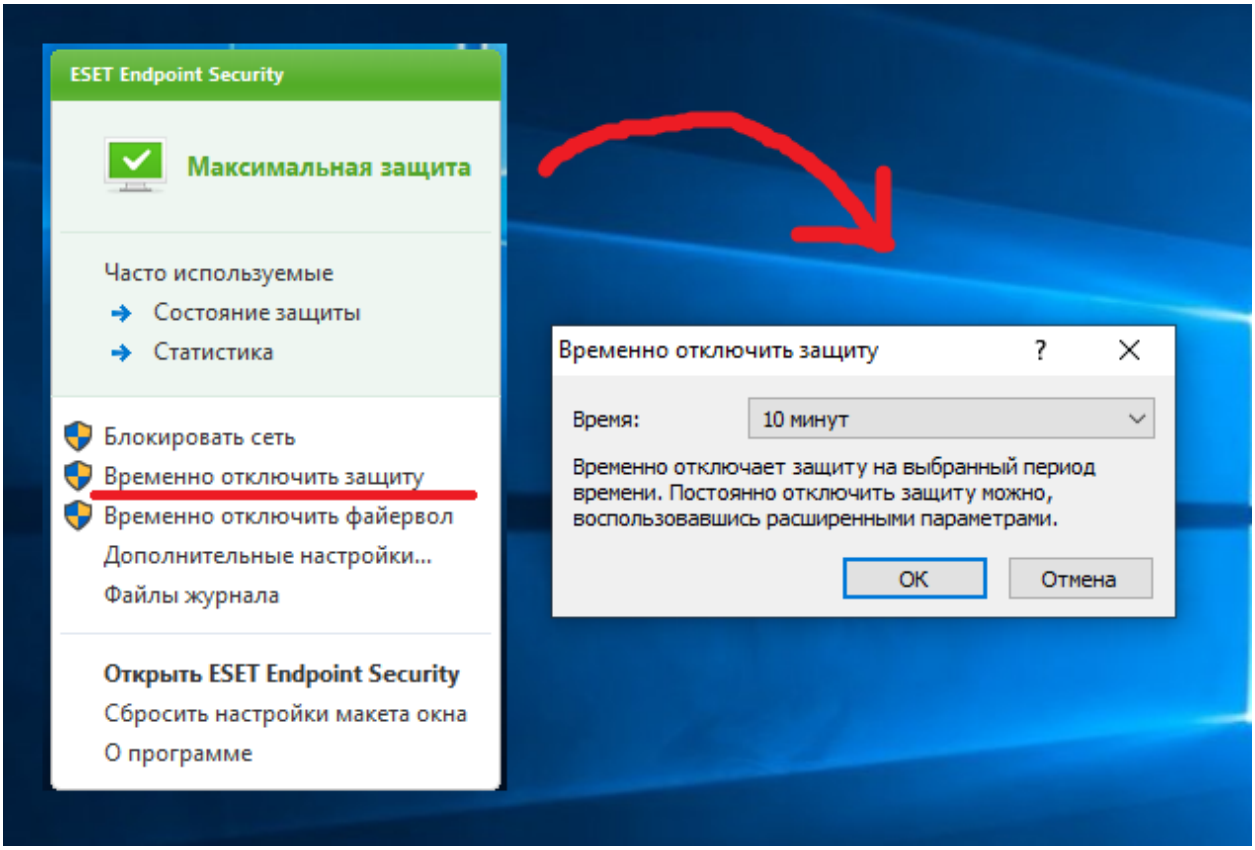
Готово! Сертификаты заменены и можно проверять работу сайтов в браузере.

Примечание: В зависимости от версии программы пути к нужной настройке могут различаться.

ESET NOD32 Endpoint

Примечание: Настройки для всех версий антивируса аналогичны.

Перед установкой агента на рабочую станцию, отключите антивирус:



Добавьте исключения антивируса:

- в трее нажмите правой кнопкой мыши на значок антивируса;
- в открывшемся контекстном меню выберите пункт **Открыть ESET Endpoint Security**;
- в открывшемся окне нажмите кнопку **F5**;
- в окне **Дополнительные настройки** в разделе **Компьютер - Защита от вирусов и шпионских программ - Исключения**, добавьте в список следующие файлы:

```
C:\Windows\agent.msi
C:\windows\auxiliaryservice.exe
C:\Windows\Winexesvc.exe
C:\windows\installer\*
C:\Windows\System32\TimeControlSvc\vmnetdrv32.exe
C:\Windows\System32\TimeControlSvc\sysprotect.exe
C:\Windows\System32\TimeControlSvc\*.*
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe
```

(continues on next page)

(продолжение с предыдущей страницы)

```
C:\Windows\SysWOW64\TimeControlSvc\sysprotect64.exe
C:\Windows\SysWOW64\TimeControlSvc\*.*
```

Добавьте исключения из обнаружения:

1. Перейдите в раздел **Настройка - Дополнительные настройки - Модуль обнаружения - Исключения - Исключения из обнаружения**.
2. Добавьте в список исключения файлы:

```
Win32/KeyLogger.ibatyr.E
Win32/KeyLogger.ibatyr.D
Win32/KeyLogger.ibatyr.F
Win64/KeyLogger.ibatyr.E
Win64/KeyLogger.ibatyr.D
Win64/KeyLogger.ibatyr.F
```

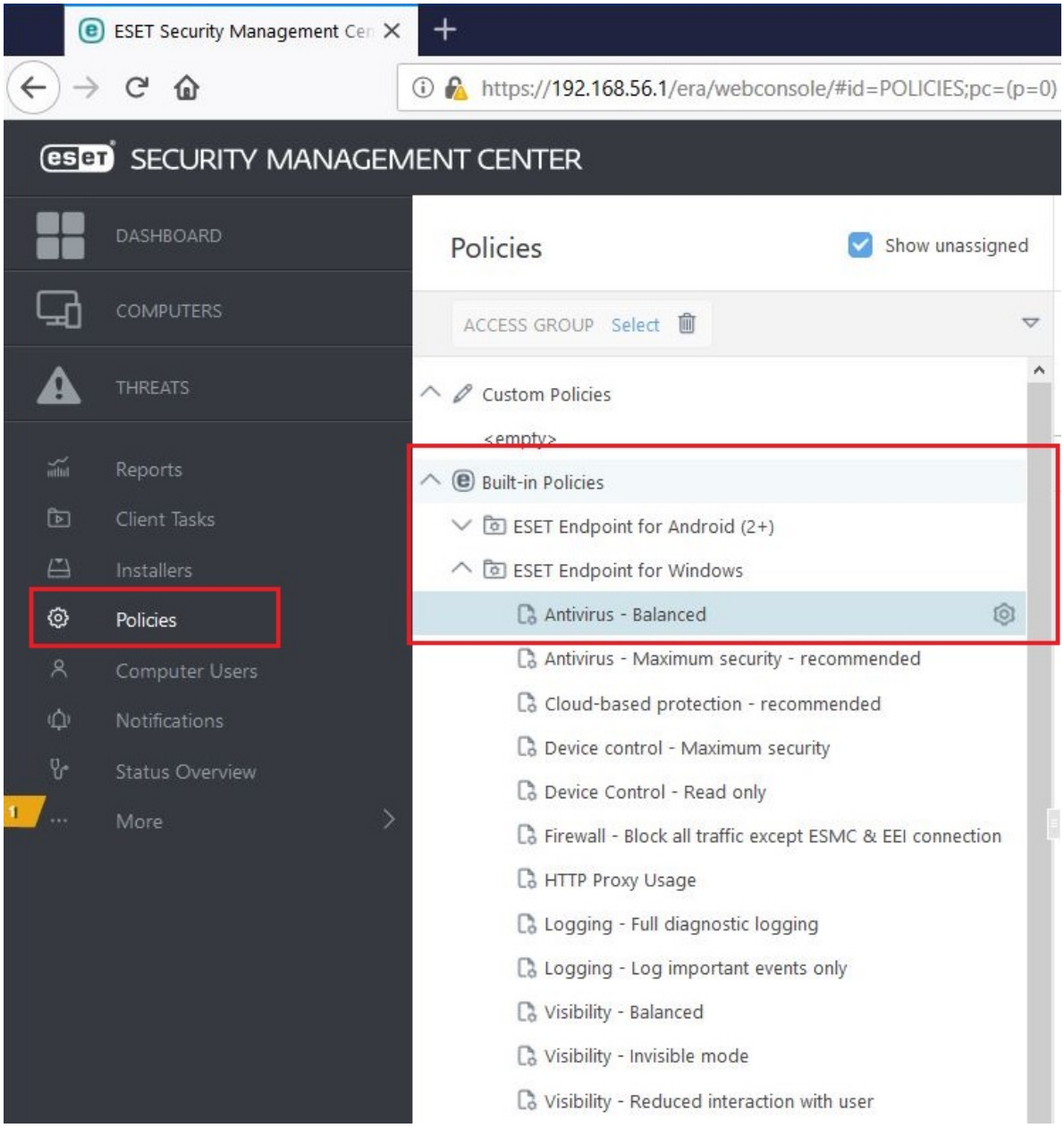
Примечание: Если на терминальном серевер с агентом и установленным ESET Endpoint Security пропадает сеть через несколько минут работы, отключите в ESET модуль **Контроль доступа в Интернет**.

ESET Security Managment Center 7

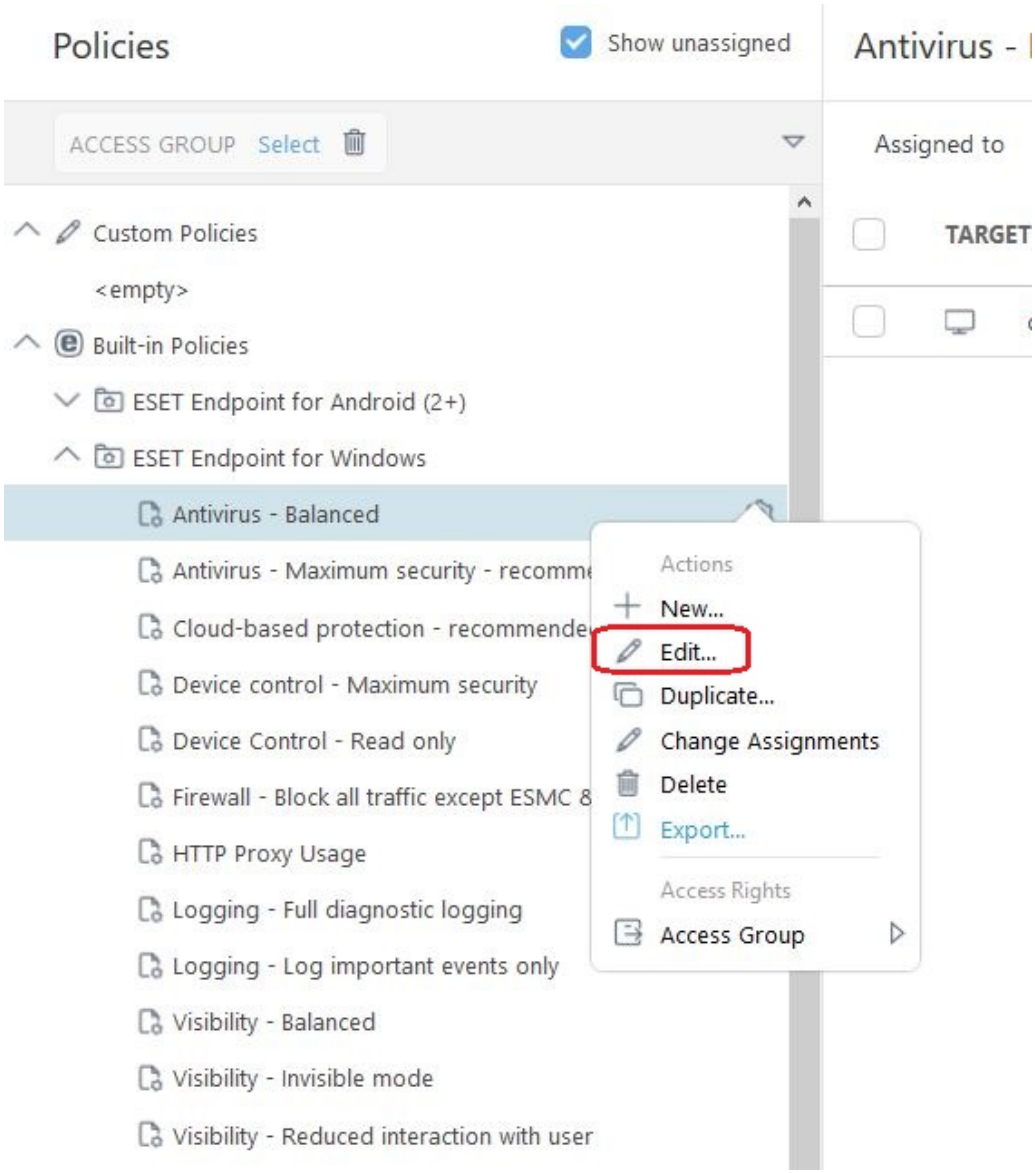
Предупреждение: Если установка агента была произведена до внесения исключений в антивирус, переустановите агент, чтобы все его модули работали корректно.

Чтобы настроить исключения в политике по умолчанию:

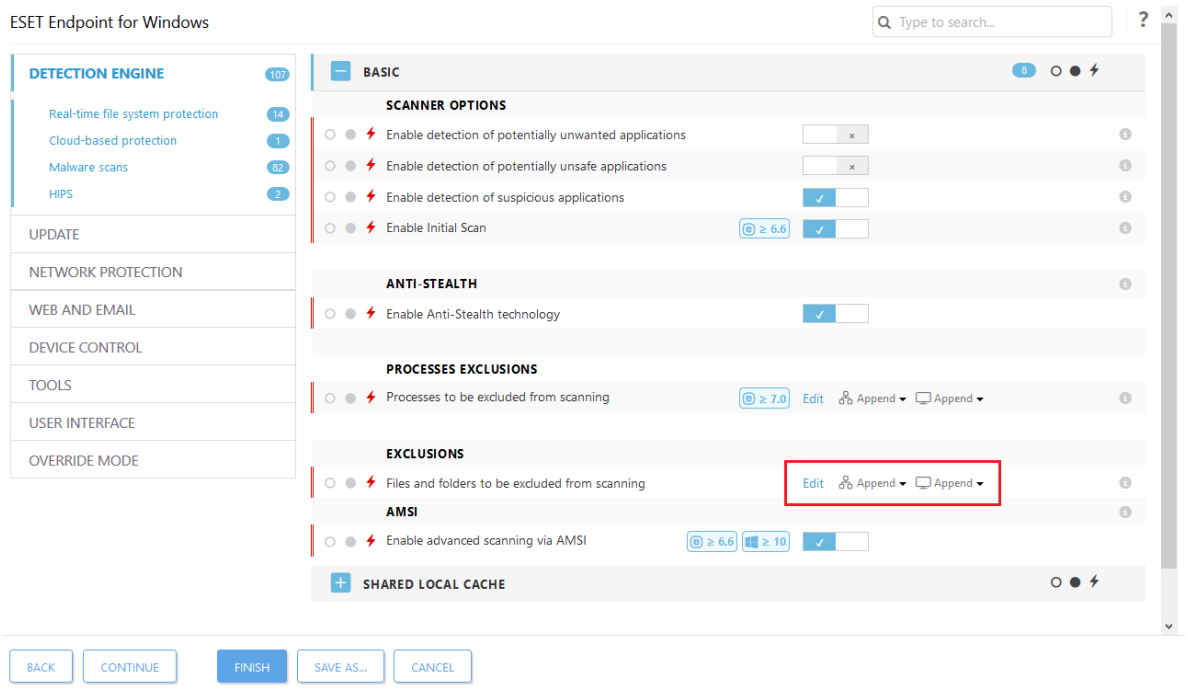
- войдите в консоль управления **ESET Security Managment Center**;
- на вкладке **Polices - ESET Endpoint for Windows** выберите политику **Antivirus - Balanced**;



- нажмите на шестерёнку и выберите **Edit**;



- в разделе **SETTINGS - DETECTION ENGINE - BASIC** выберите секцию **EXCLUSIONS**;
- нажмите **Edit**;



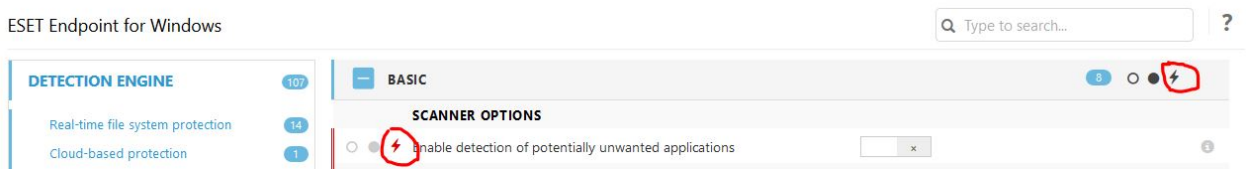
- в открывшемся окне добавьте в список исключений следующие пути и файлы:

```
C:\Windows\agent.msi
C:\windows\auxiliaryservice.exe
C:\Windows\Winexesvc.exe
C:\windows\installer\*
C:\Windows\System32\TimeControlSvc\vmnetdrv32.exe
C:\Windows\System32\TimeControlSvc\sysprotect.exe
C:\Windows\System32\TimeControlSvc\*.*
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe
C:\Windows\SysWOW64\TimeControlSvc\sysprotect64.exe
C:\Windows\SysWOW64\TimeControlSvc\*.*
```

Добавление этих путей позволит агенту работать на рабочей станции пользователя без удаления антивирусом.

Примечание: Работа исключений была проверена на ESET Endpoint версии 7.0.2100.46.55.0.2272, и ESET Security Management Center Version 7.0 (7.0.577.0). Для других версий ESET Endpoint Antivirus\ESET Managment Center исключения могут вести себя иначе. В случае возникновения проблем в работе исключений, свяжитесь с технической поддержкой.

Чтобы политика точно сработала, нажмите значок молнии в строке с названием редактируемого модуля.



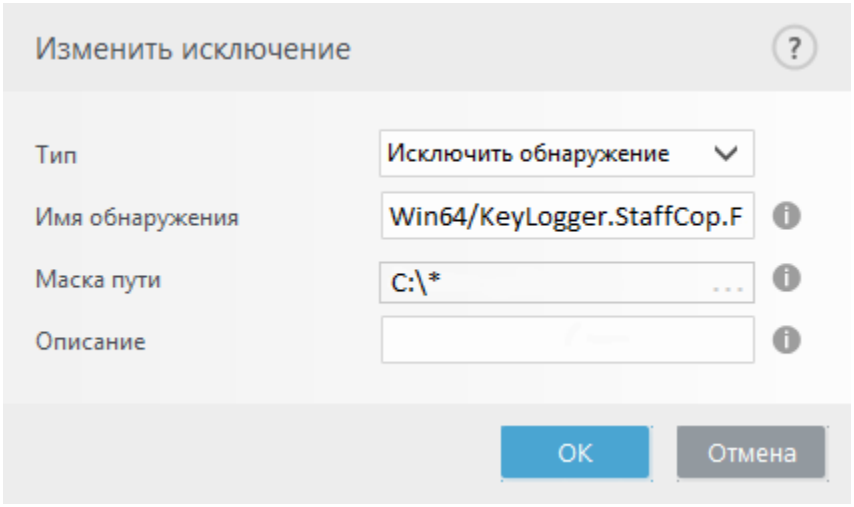
- нажмите кнопку **FINISH**.

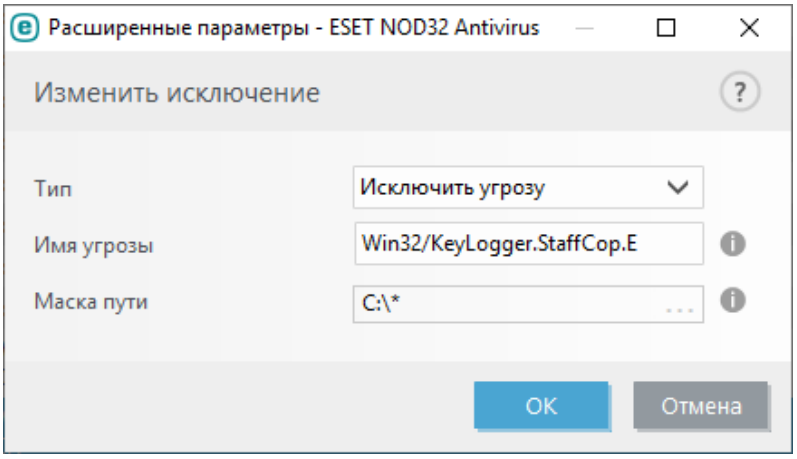
Политика **ESET Endpoint for Windows** будет применена сразу же на всех ПК, для которых указана. По умолчанию она распространяется на все ПК с Windows-системами.

Примечание: Если после внесения исключений, агент по-прежнему удаляется, убедитесь, что исключения действительно применились на рабочих станциях пользователей. Для этого в настройках антивируса проверьте текущие исключения для модуля файлового мониторинга и общую страницу со списком исключений.

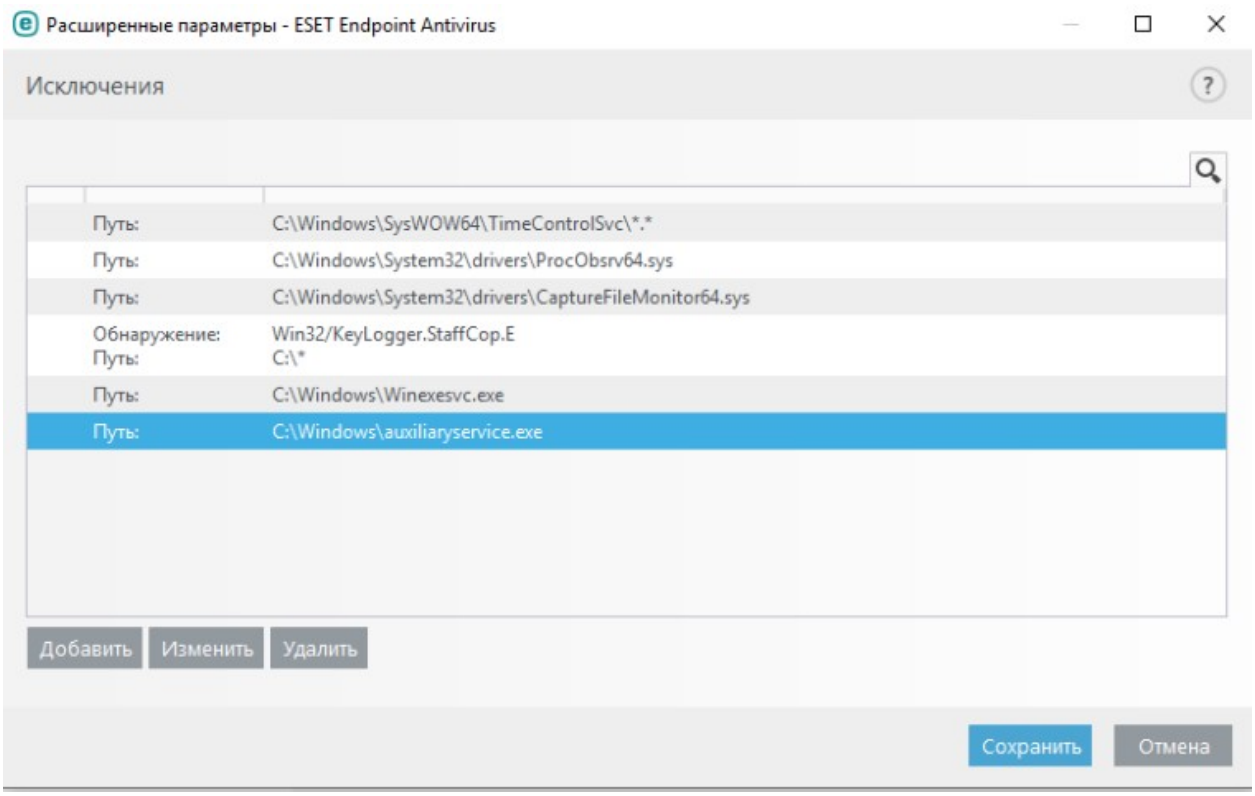
Чтобы не вносить в список исключений папку **C:\windows\installer**, можно внести исключения по угрозе или обнаружению (в зависимости от версии антивируса):

```
Win32/KeyLogger.ibatyr.E
Win32/KeyLogger.ibatyr.D
Win32/KeyLogger.ibatyr.F
Win64/KeyLogger.ibatyr.E
Win64/KeyLogger.ibatyr.D
Win64/KeyLogger.ibatyr.F
```





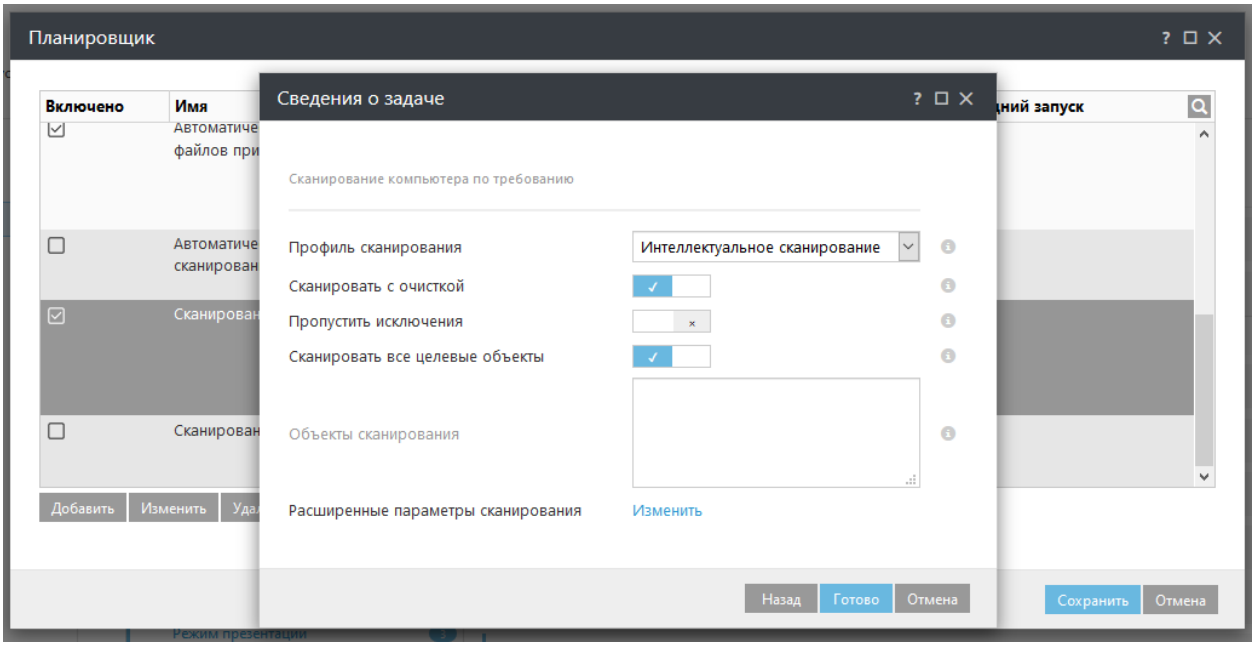
В итоге, список исключений должен будет выглядеть так:



Примечание: Это исключение работает только для антивируса версии 7.x и старше! В Качестве «Маски пути» - нужно указать диск **C:***

Исключение из полного сканирования дисков

В последних версиях антивируса ESET при запланированной проверке могут быть обнаружены и удалены бинарные файлы агента iBatyr Monitor. Чтобы этого избежать в настройках запланированного сканирования отключите опцию **Пропустить исключения**:



Kaspersky Antivirus

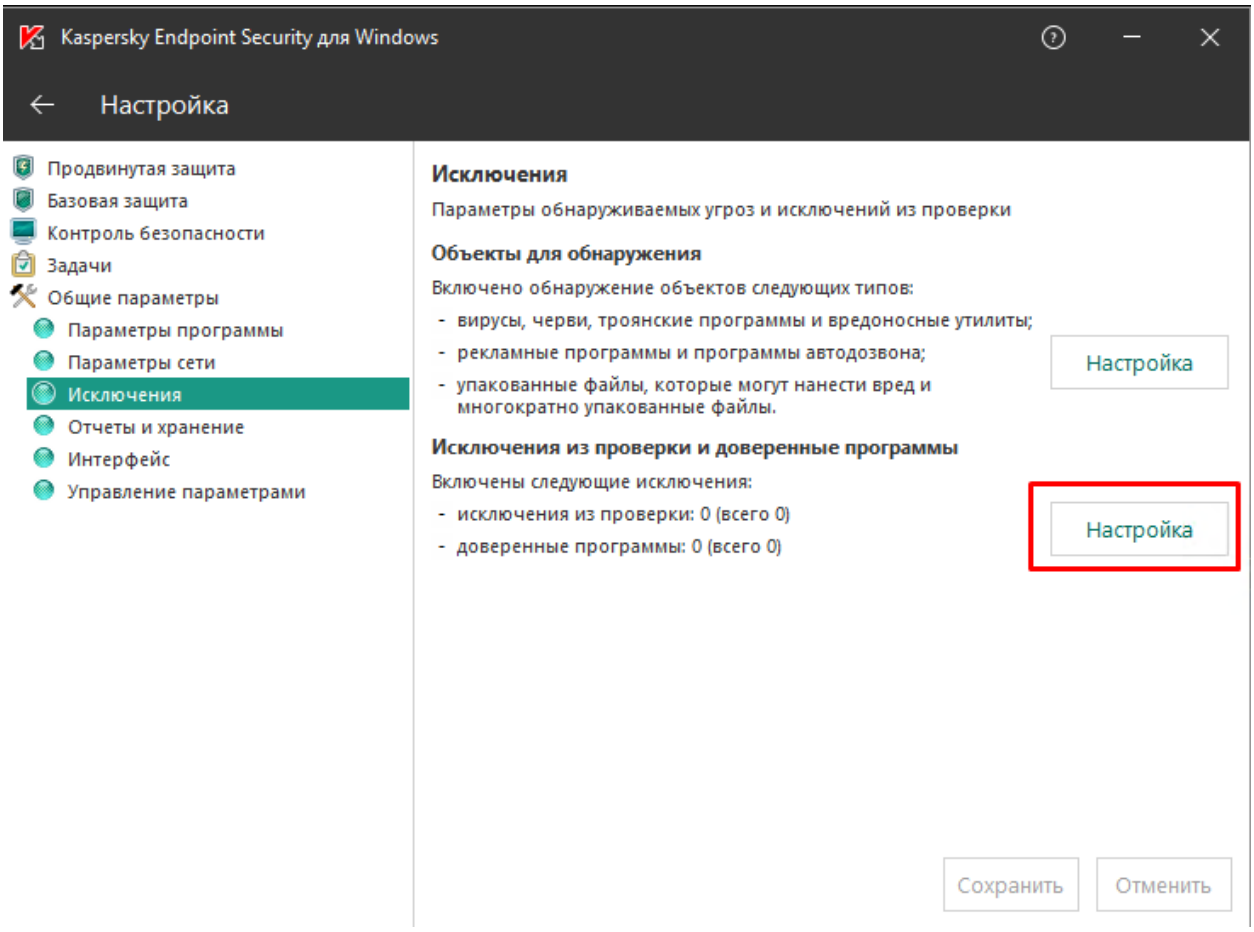
- *Kaspersky Endpoint Security 11*
- *Kaspersky Small Office Security*
- *Kaspersky Security Center*
- *Kaspersky Security for Virtualization 5.1*

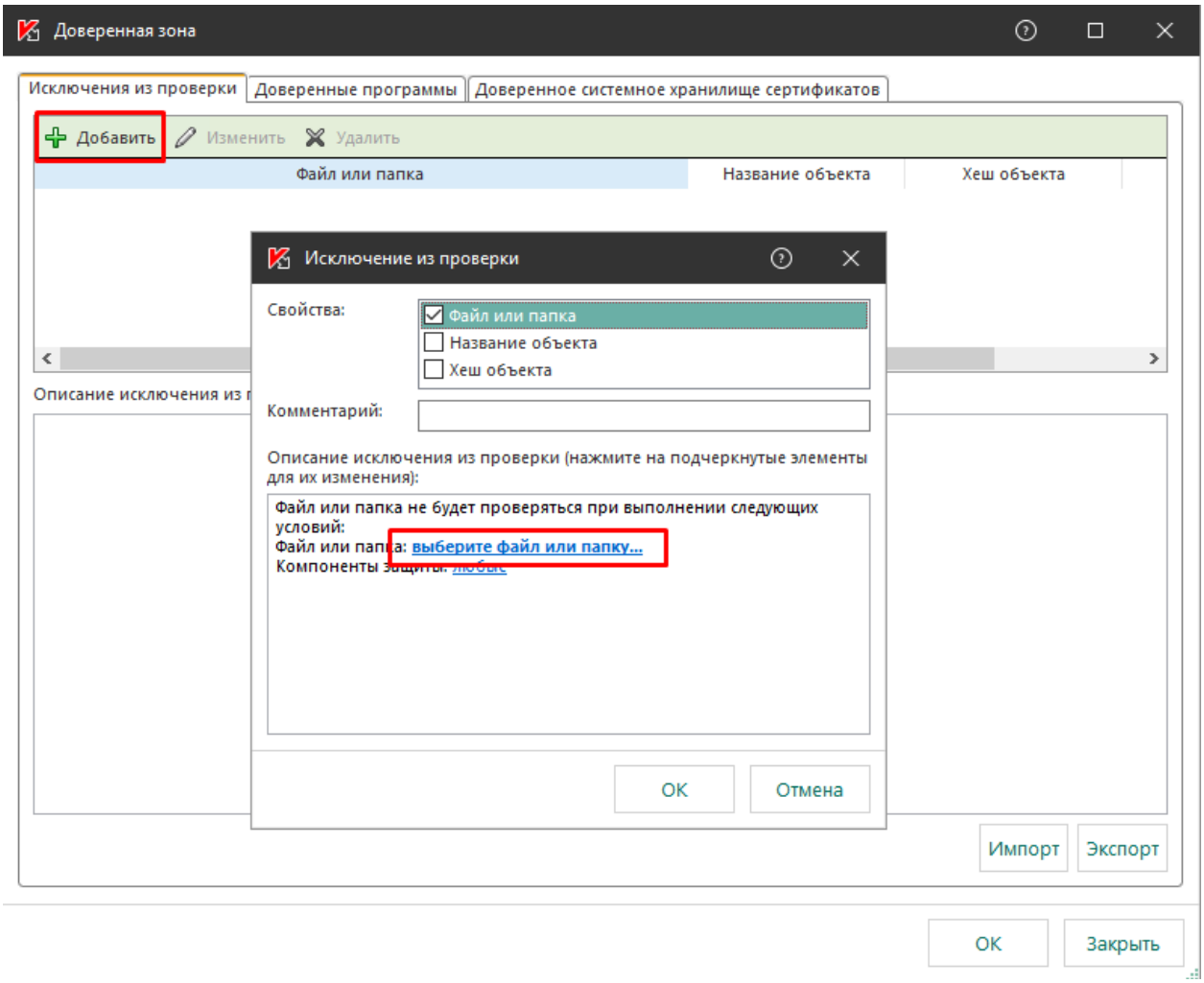
Примечание: Способ настройки в разных версиях антивирусного ПО может отличаться от указанного в документации.

Kaspersky Endpoint Security 11

Чтобы отключить проверку защищенных соединений и добавить исключения из списка исключений, внесите следующие изменения в настройки Kaspersky Endpoint Security 11:

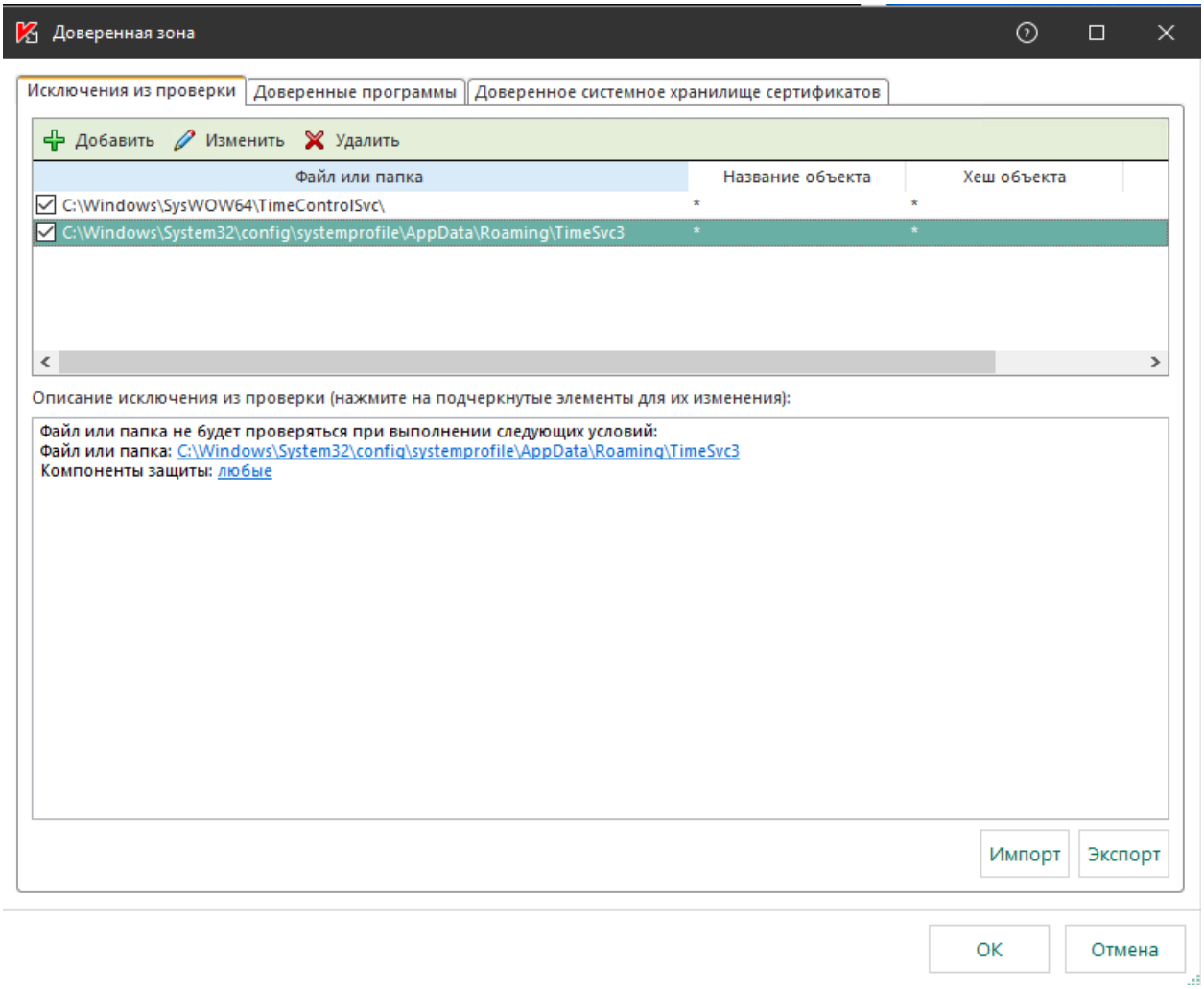
Исключения из проверки





Пути:

```
C:\Windows\SysWOW64\TimeControlSvc\
C:\Windows\system32\config\systemprofile\AppData\Roaming\TimeSVC3
C:\Windows\System32\TimeControlSvc\
C:\Windows\System32\TimeControlSvc\vmnetdrv32.exe
C:\Windows\System32\TimeControlSvc\sysprotect.exe
```

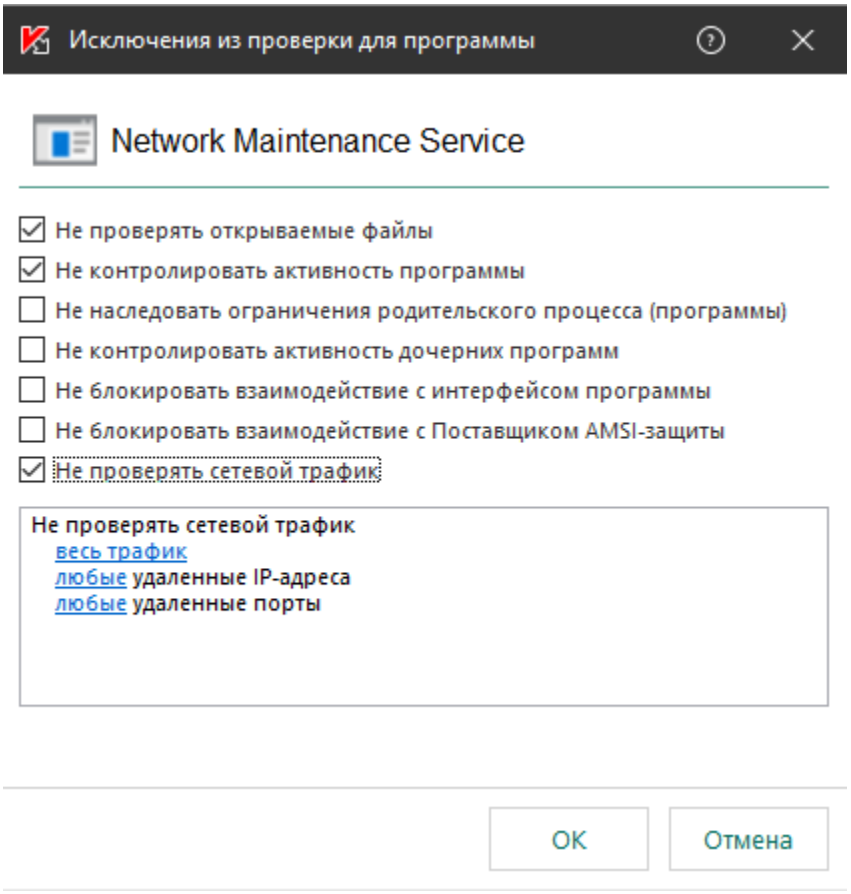


Доверенные программы

Укажите следующие программы:

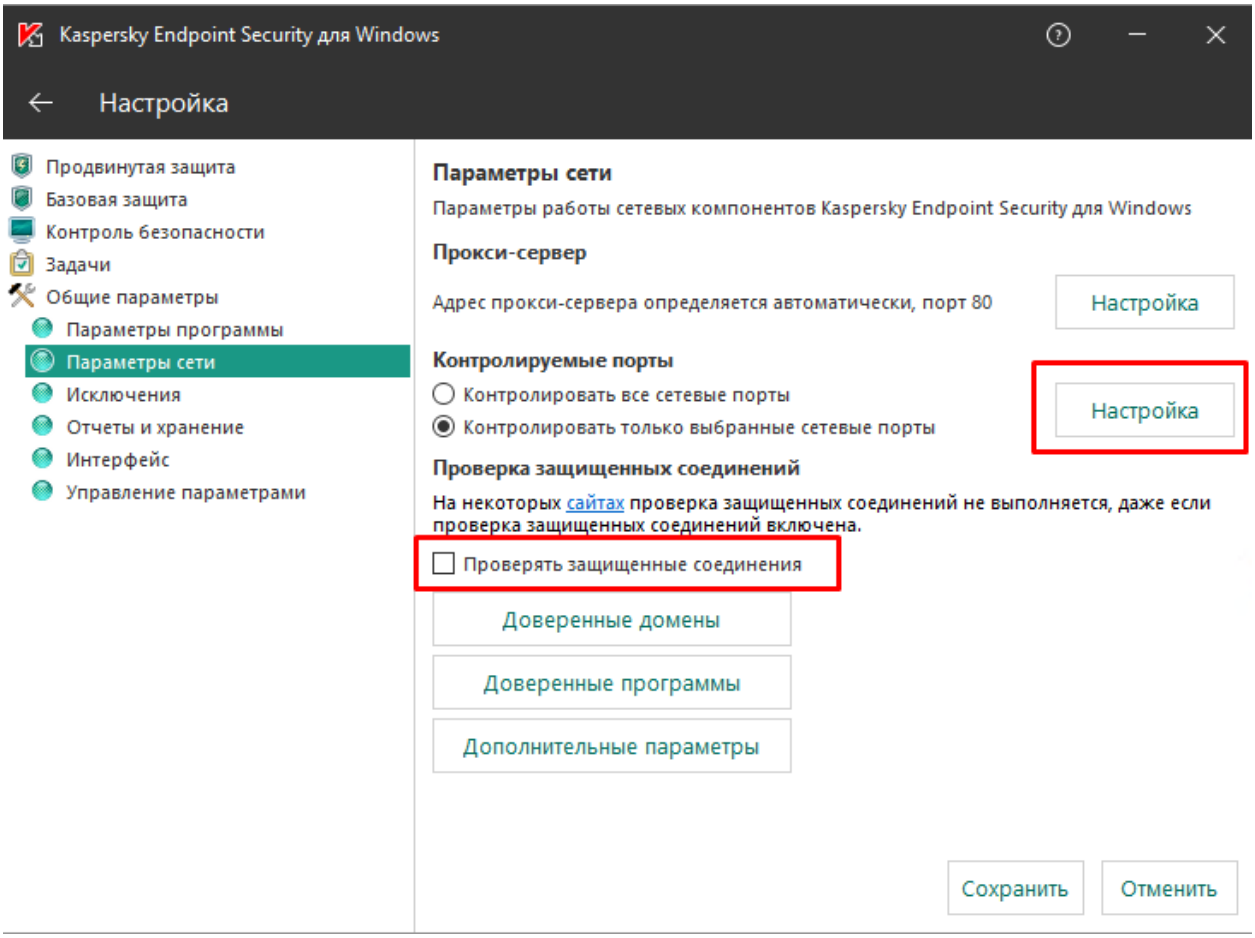
```
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe
C:\Windows\System32\TimeControlSvc\vmnetdrv32.exe
```

Выберите следующие параметры для доверенных программ:

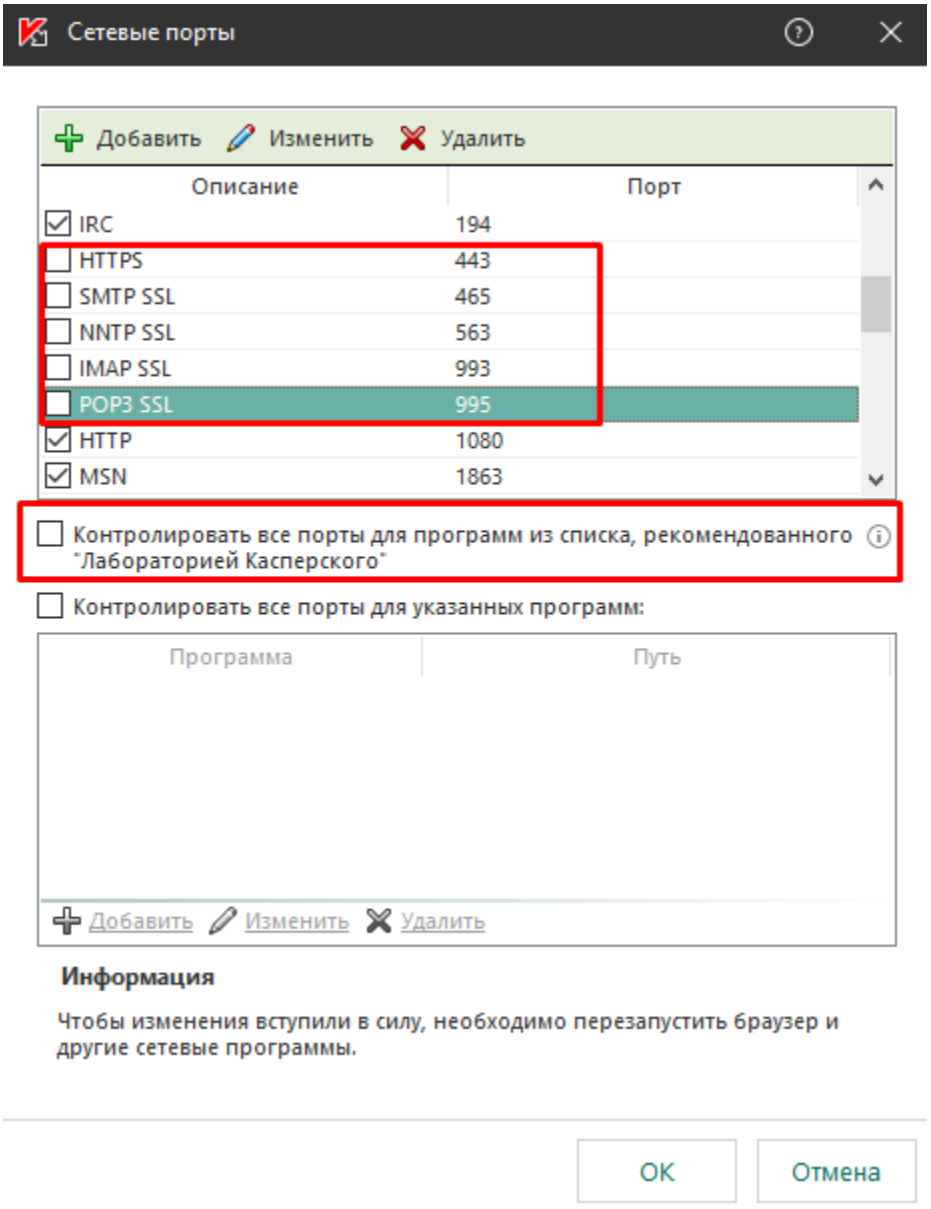


Настройки SSL

Перейдите в «Параметры сети»



Отключите проверку следующих портов:

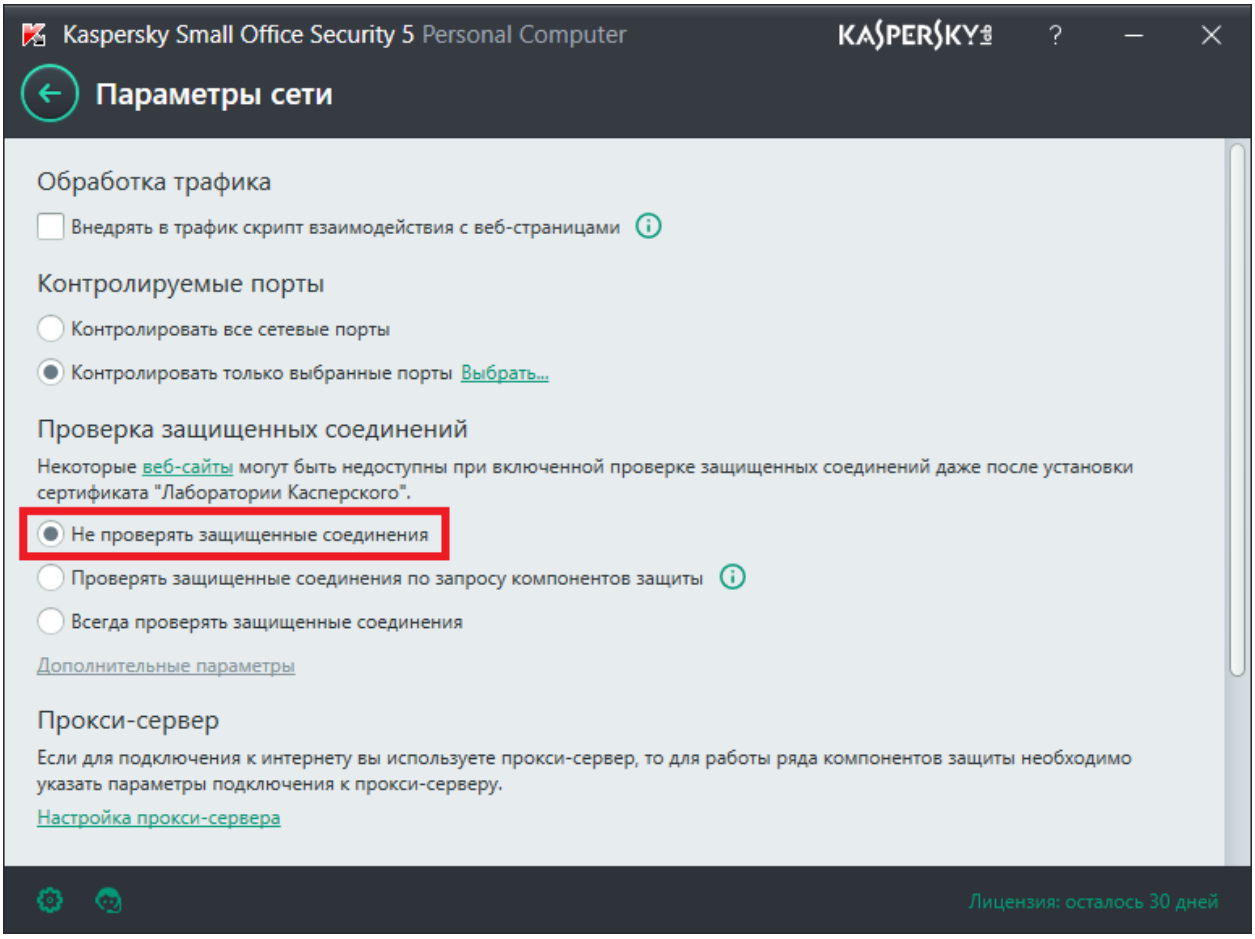


Разрешение на запись аудио

1. В разделе «Настройки» в пункте «Защита/Предотвращение вторжений» выберите «Управление программами».
2. В контекстном меню группы «Слабые ограничения» выберите «Подробности и правила».
3. В открывшемся окне в разделе «Права» выберите пункт «Доступ к устройствам записи звука» и установите ему значение «Разрешить».
4. Перезагрузите ПК или перезапустите Агент.

Kaspersky Small Office Security

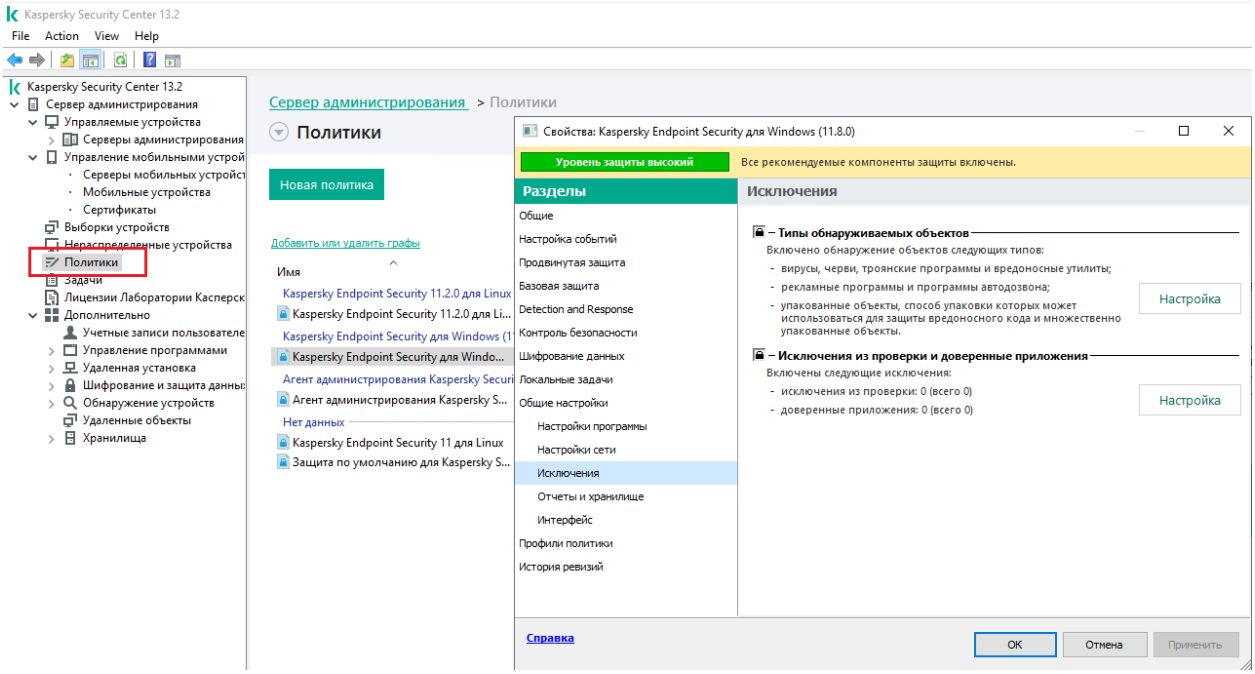
В Kaspersky Small Office Security это делается с помощью пункта меню **Настройки - Дополнительно - Сеть:**



Примечание: В зависимости от версии программы пути к нужной настройке могут различаться.

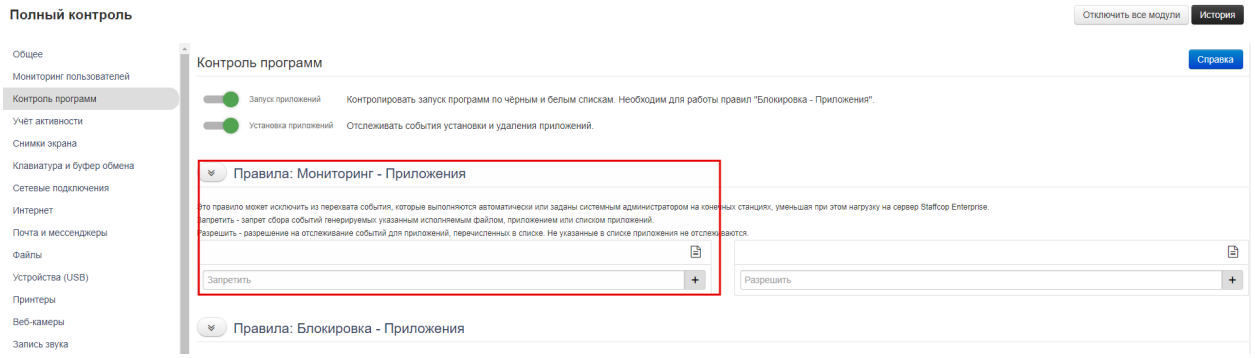
Kaspersky Security Center

В Kaspersky Security Center необходимо выбрать политику, которая у вас назначена на компьютеры и произвести настройки согласно описанию выше о «Kaspersky Endpoint Security 11».



Kaspersky Security for Virtualization 5.1

Для операционных систем на Linux и установленном Kaspersky Security for Virtualization 5.1, необходимо внести исключения в конфигурацию агента:

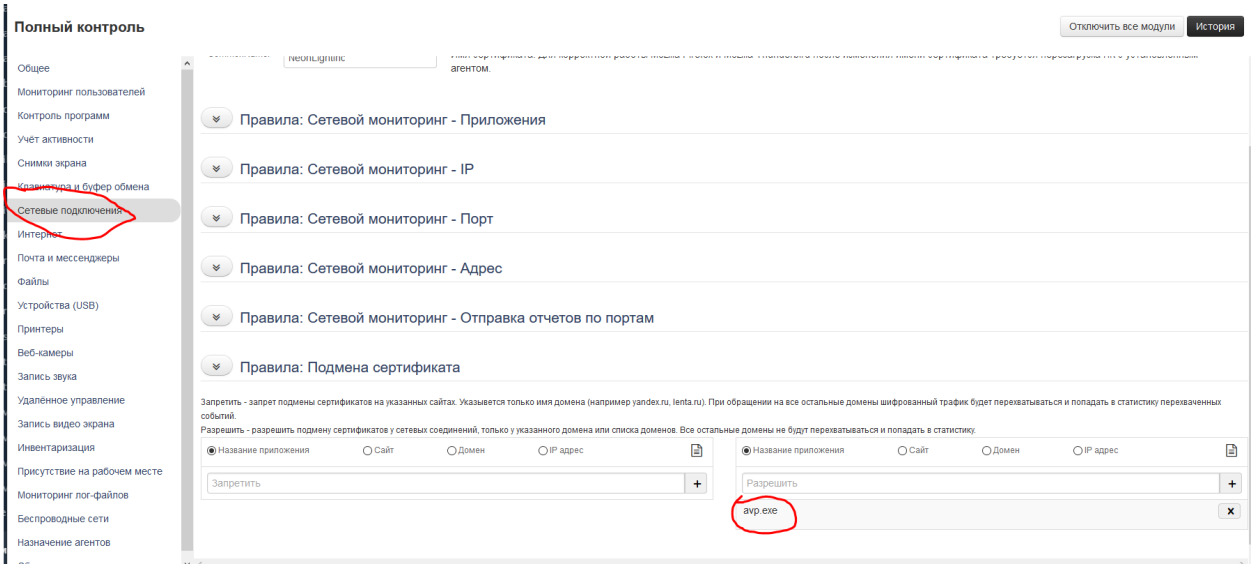


Исключения:

```
/var/opt/kaspersky/*
/usr/local/sbin/lightagent
/usr/lib/systemd/system/lightagent.service
/usr/bin/kaspersky/*
/sys/fs/cgroup/systemd/system.slice/lightagent.service
/run/kaspersky/*
/opt/kaspersky/*
/etc/systemd/system/multi-user.target.wants/lightagent.service
/etc/systemd/system/graphical.target.wants/lightagent.service
/etc/opt/kaspersky/*
```

Примечание: Для корректного перехвата почты рекомендуется включить подмену сертификата в

процессе avp.exe

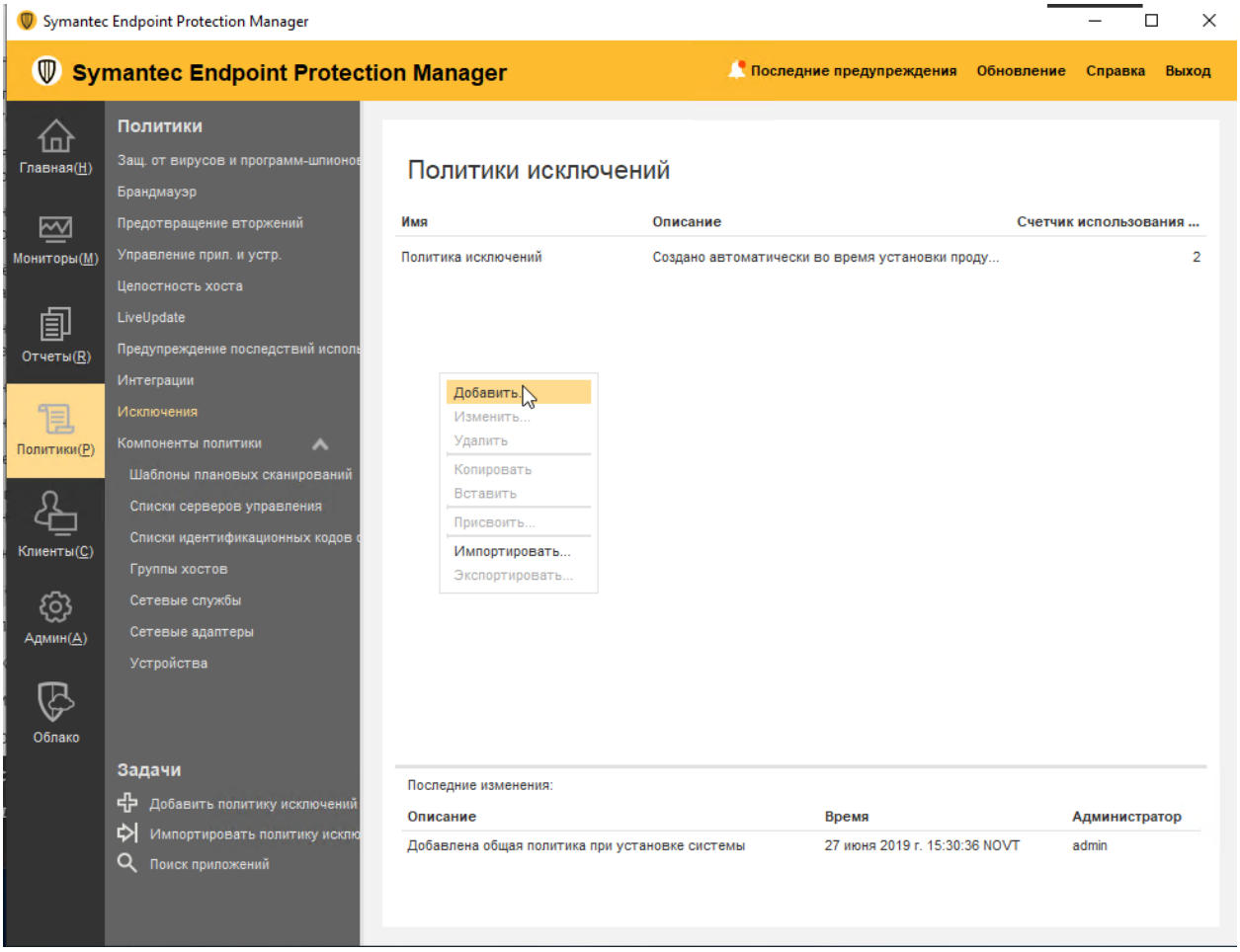


Symantec Endpoint Protection

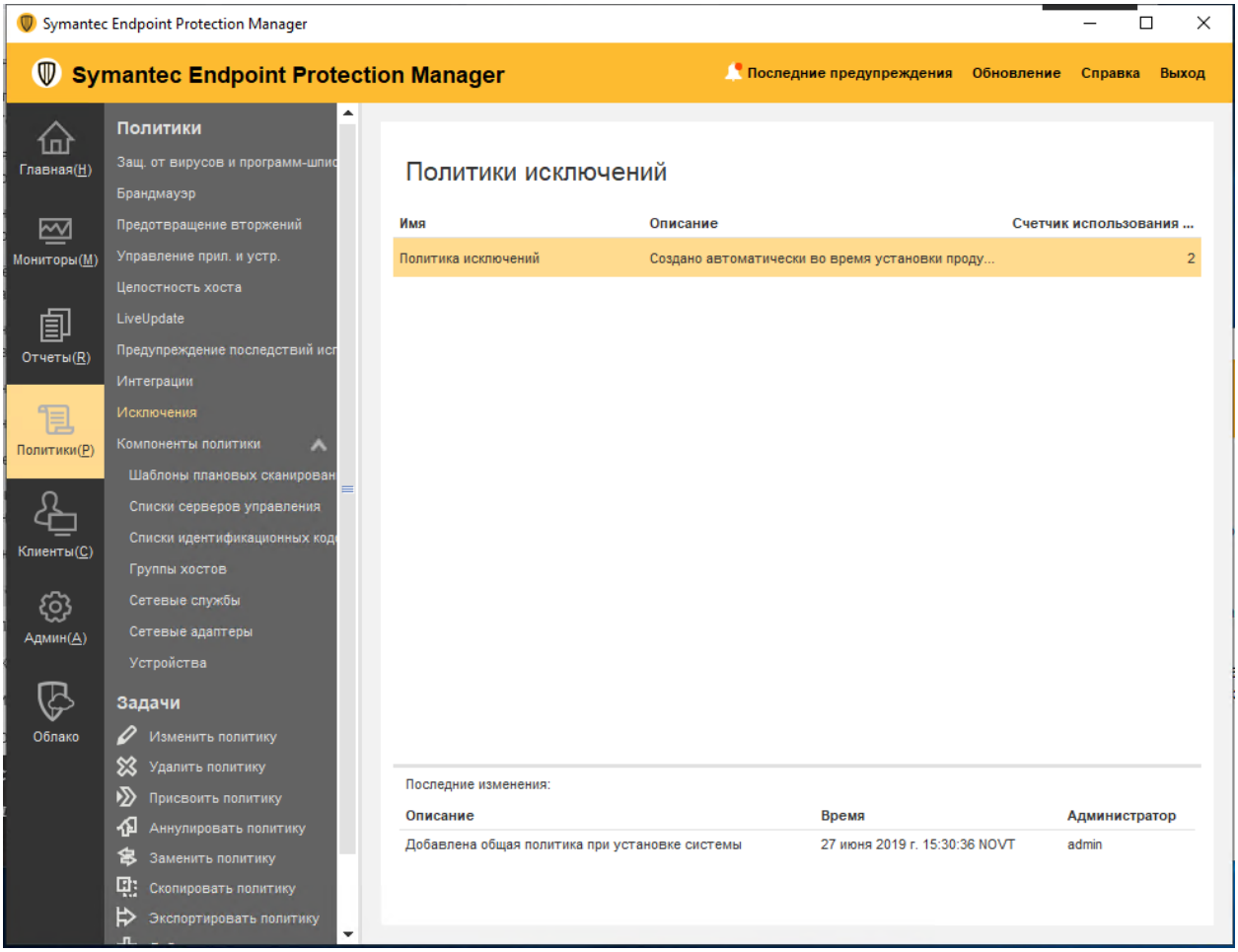
Предупреждение: При удаленной установке требуется отключить антивирус на ПК, на который планируется установить агент.

Откройте консоль управления Endpoint Protection manager

Перейдите в Политики - Исключения

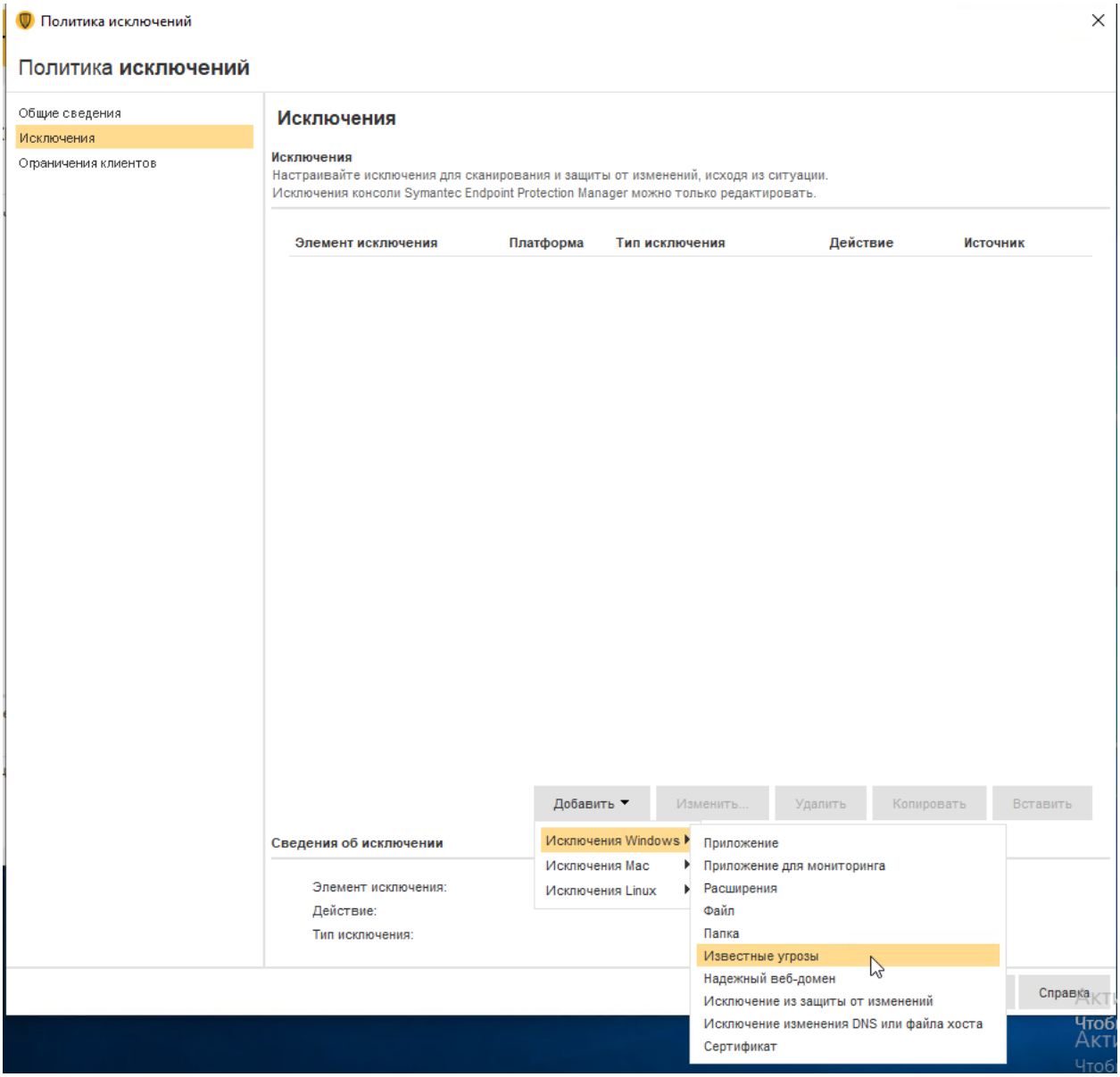


Добавьте новую политику:

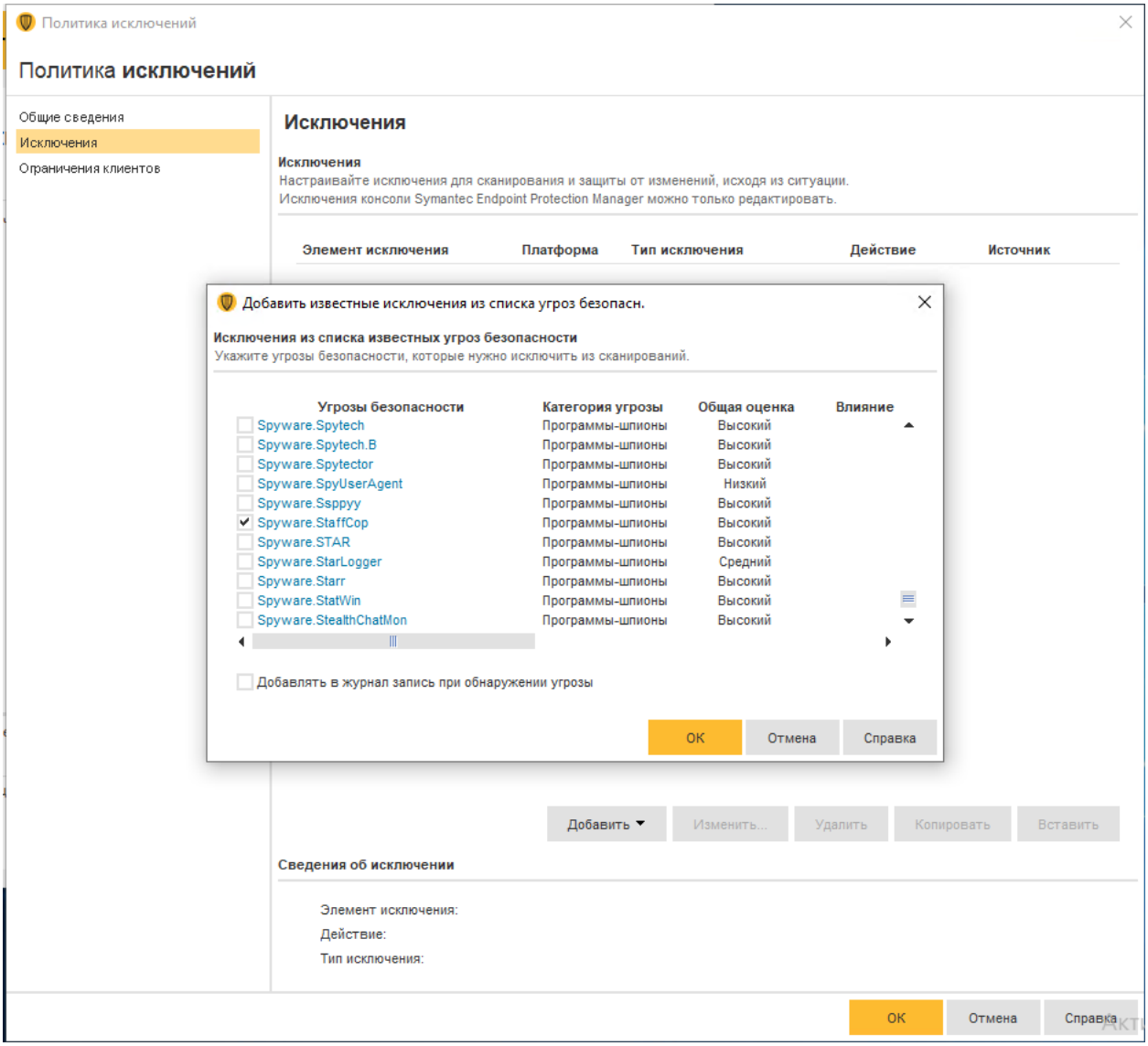


Внесите iBatyr Monitor в исключения:

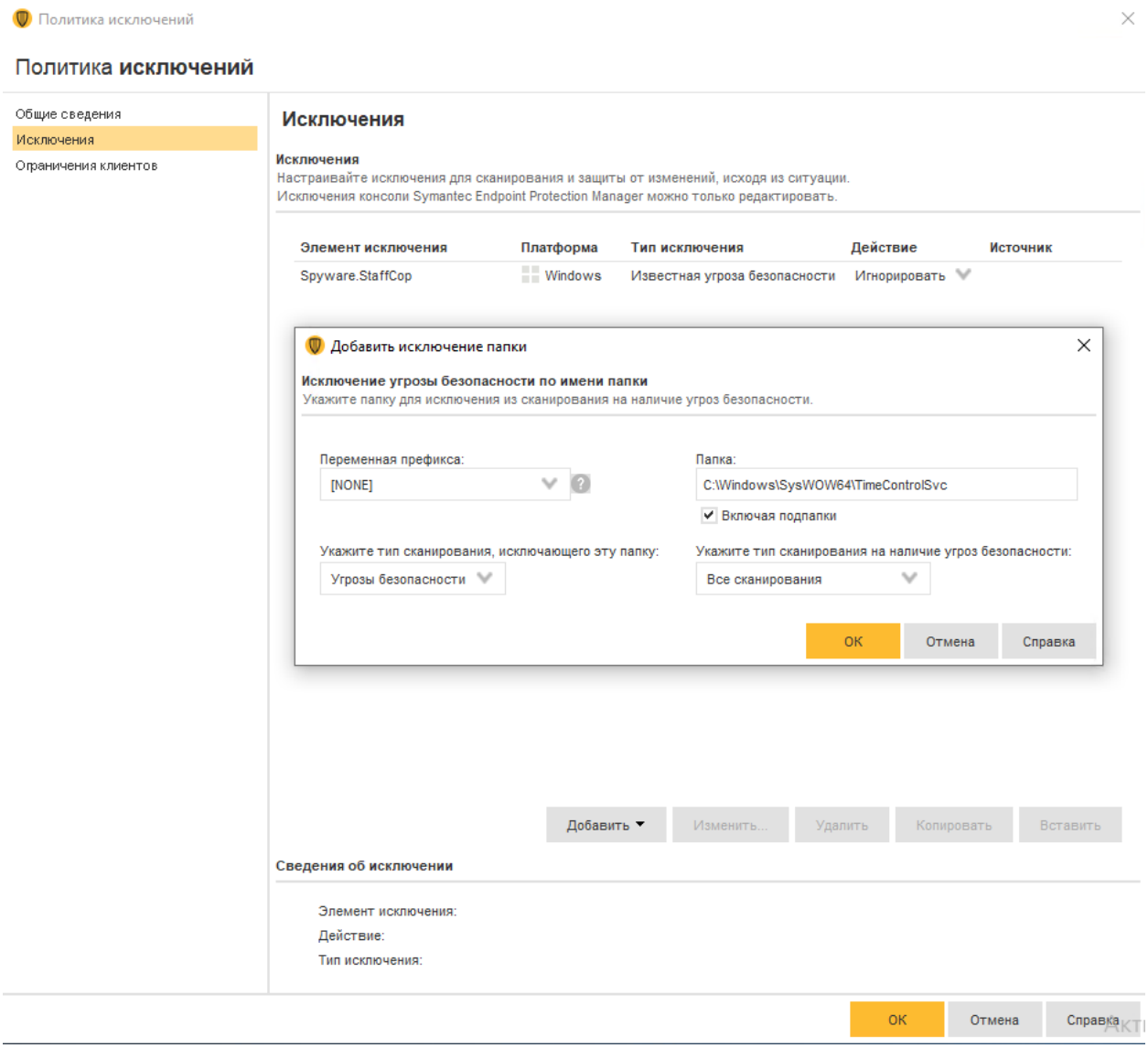
Добавить - Исключения Windows - Известные угрозы



Программа откроет все известные им угрозы. Они отсортированы по алфавиту, нужно опуститься до Spyware.iBatyr Monitor

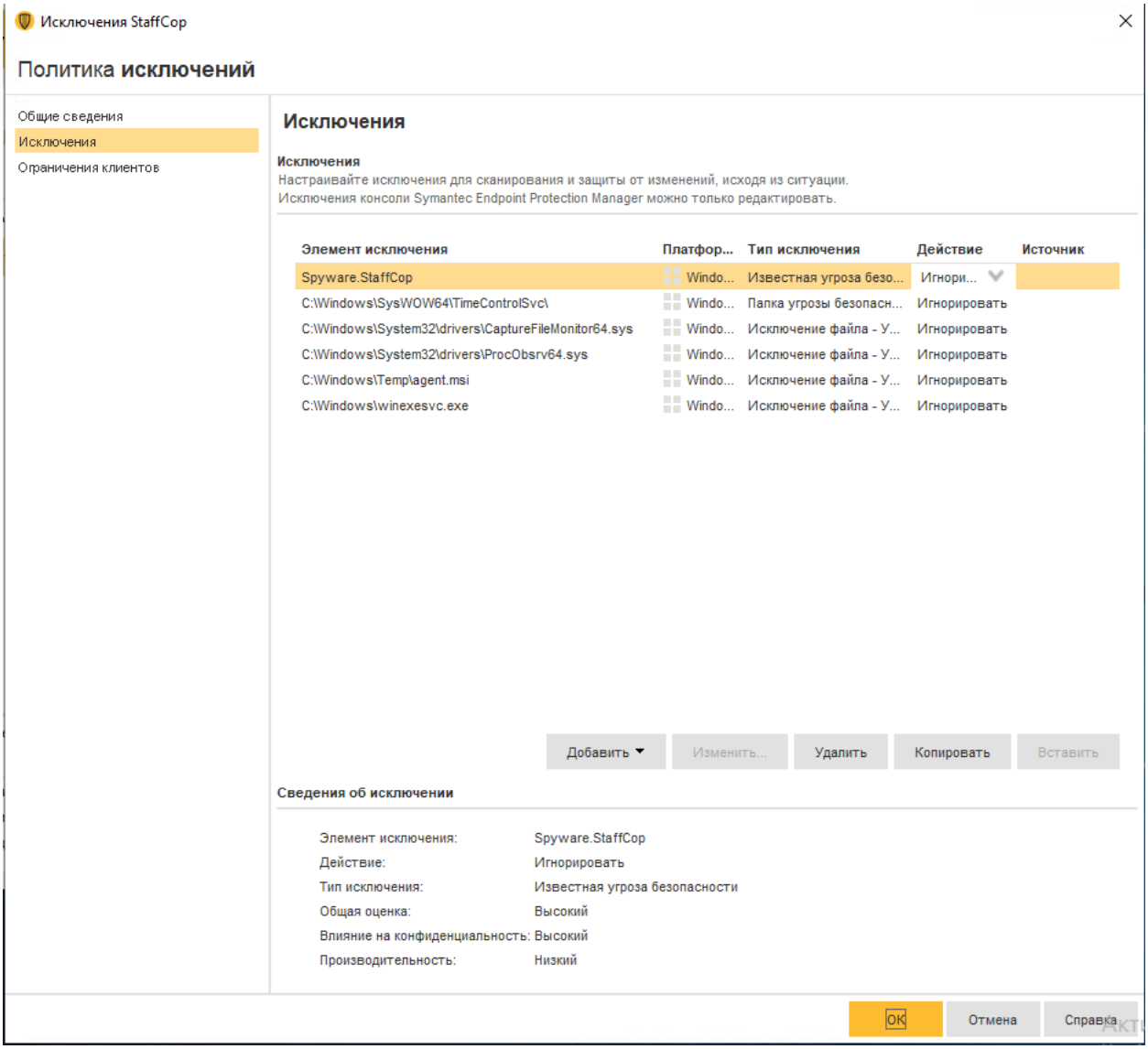


Дополнительно необходимо следующим образом внести исключения для файлов и директорий агента:

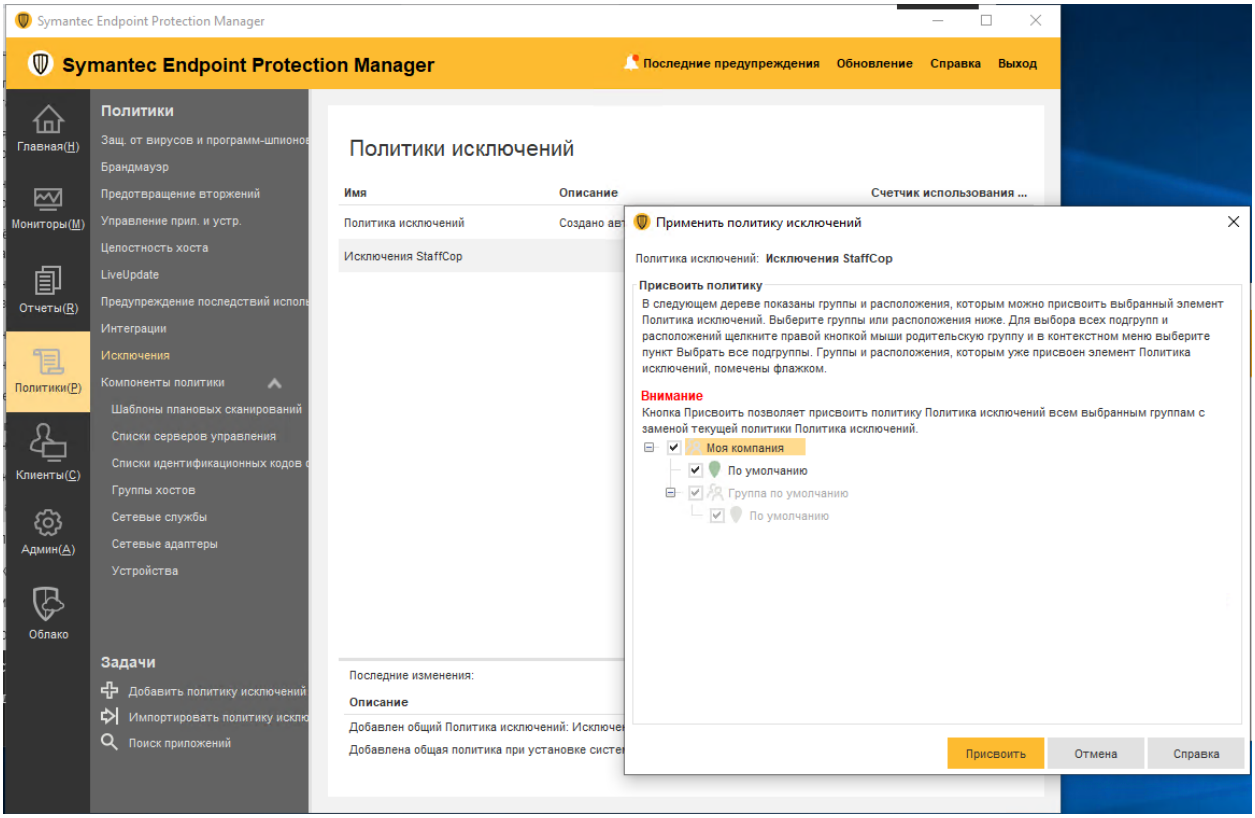


Укажите следующие файлы и папки:

```
c:\Windows\System32\TimeControlSvc\
c:\Windows\Syswow64\TimeControlSvc\
c:\Windows\System32\Drivers\CaptureFileMonitor.sys
c:\Windows\System32\Drivers\ProcObsrv.sys
c:\Windows\agent.msi
c:\Windows\Winexesvc.exe
```



Примените политику на те ПК, которые нужны.



Windows Defender

В последних обновлениях Windows Defender при скачивании или установке можно увидеть надпись: **Найдена программа-шантажист**. Для установки внесите установочный файл агента в исключения.

Примечание: На данный момент проблема наблюдается на агентах версии 2539, 2537 и ниже.

Кроме этого, внесите исключения для основных файлов агента, указанных *в Исключениях антивируса*.

Defender может обнаружить еще одну угрозу — PUA:Win32/WinExecSvc threat description — Microsoft Security Intelligence.

Добавьте ее в исключения командой:

```
powershell -inputformat none -outputformat none -NonInteractive -Command WMIC /
↪NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add␣
↪ThreatIDDefaultAction_Ids=268775 ThreatIDDefaultAction_Actions=6
```

Не отслеживаются файловые операции

Windows Defender в обновлении 1.293.1336.0 начал блокировать работу модуля iBatyr Monitor по контролю над файловыми операциями. Для того чтобы узнать, заблокировал ли Windows Defender файловый драйвер, проверьте наичие файлв:

```
C:\Windows\System32\drivers\CaptureFileMonitor.sys
```

Если файла нет – выполните указанные в этой статье действия.

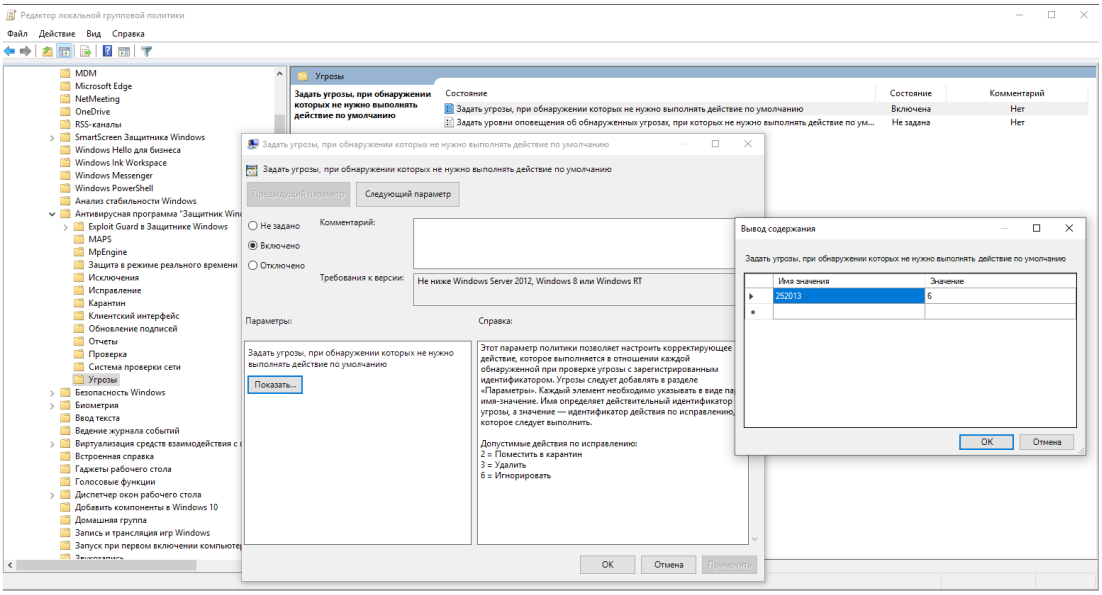
Внесение исключений

Через CMD:

```
WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add␣
↪ThreatIDDefaultAction_Ids=252013 ThreatIDDefaultAction_Actions=6
```

Исключения через политики

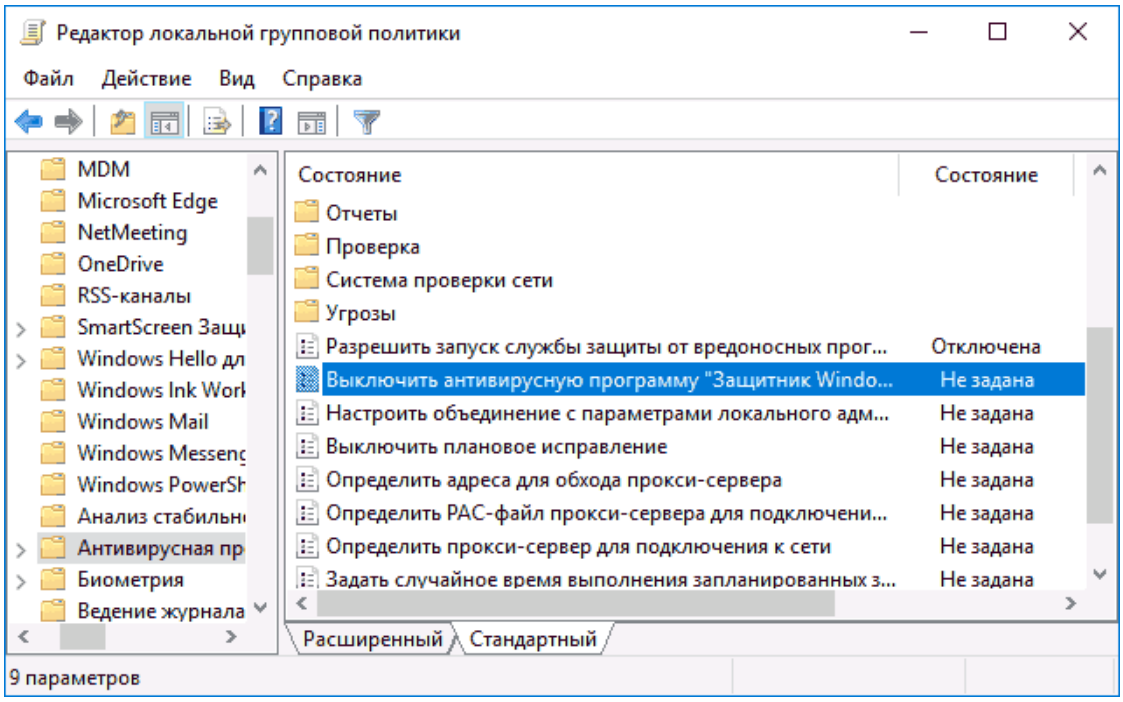
1. Нажмите клавиши Win+R на клавиатуре и введите gpedit.msc.
2. В открывшемся редакторе локальной групповой политики перейдите к разделу **Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Антивирусная программа Защитник Windows**.



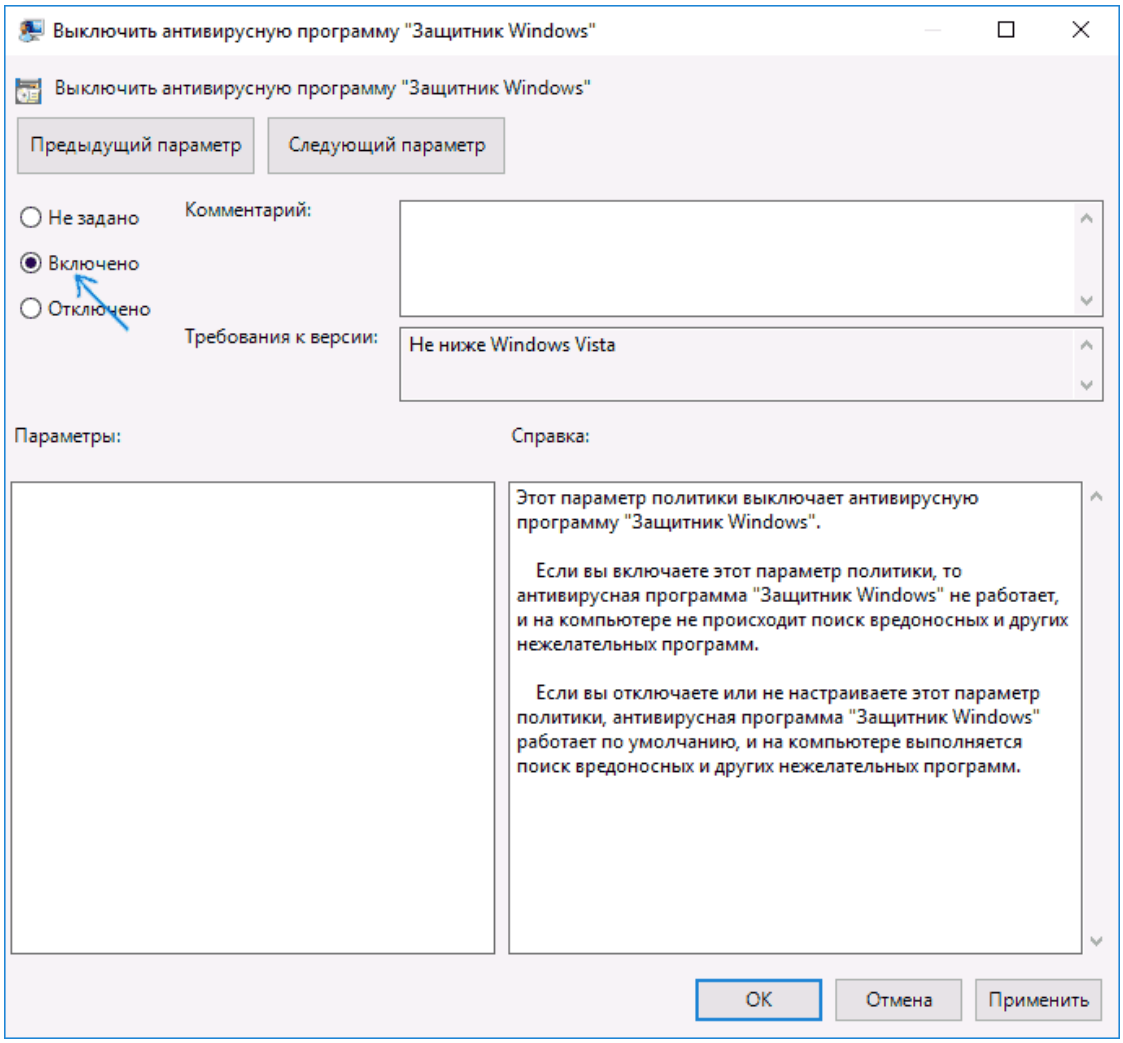
Отключение Windows Defender

Если версия агента выше 5.8.2495, исключения вносятся автоматически при установке агента. Однако загрузка агента может быть недоступна, поэтому отключите защитник или внесите исключения, как было рекомендовано ранее.

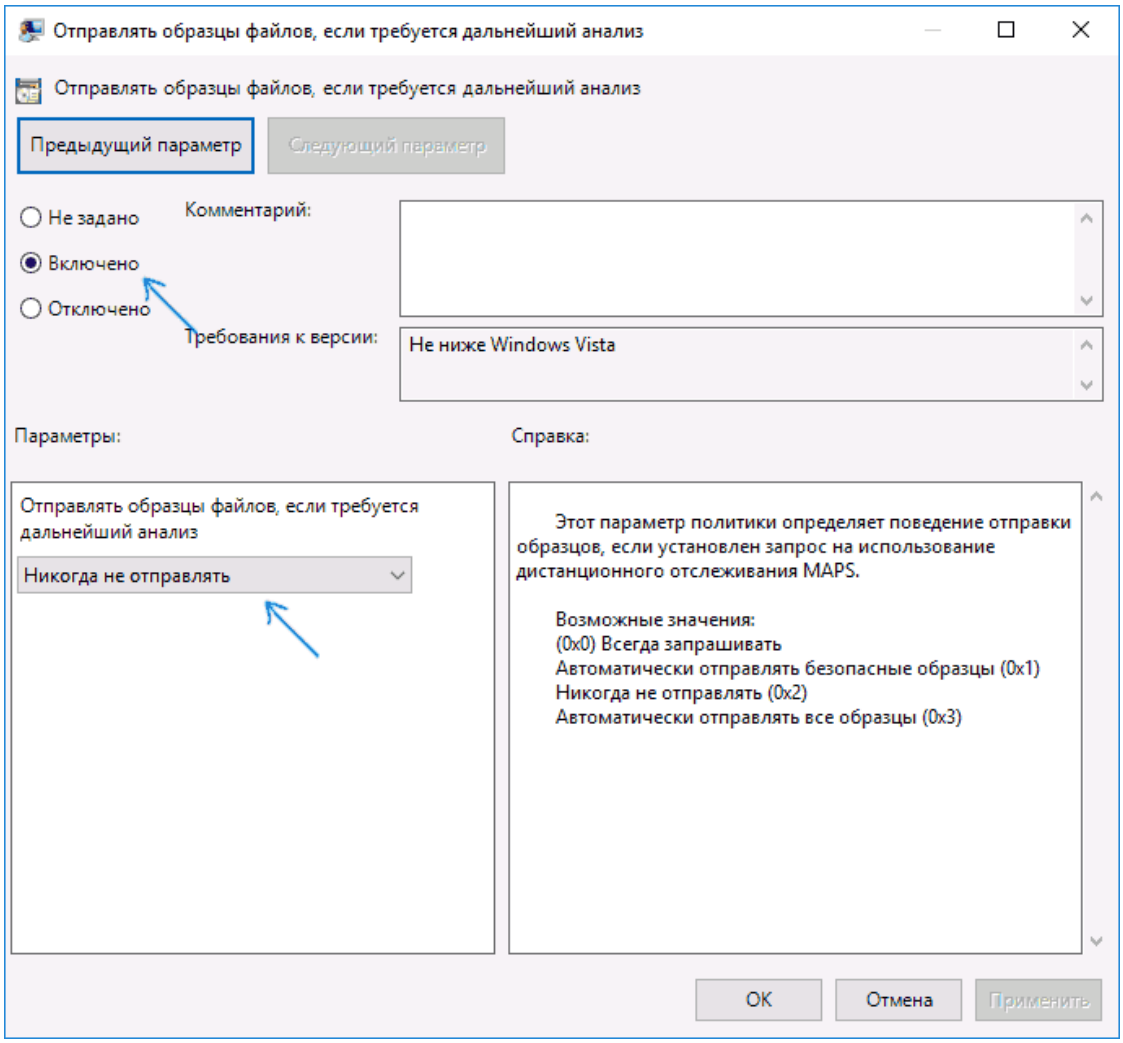
1. Нажмите клавиши Win+R на клавиатуре и введите gpedit.msc
2. В открывшемся редакторе локальной групповой политики перейдите к разделу **Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Антивирусная программа Защитник Windows**.



3. Дважды нажмите параметр **Выключить антивирусную программу Защитник Windows** и выберите **Включено**:



4. Отключите параметры **Разрешить запуск службы защиты от вредоносных программ** и **Разрешить постоянную работу службы защиты от вредоносных программ**.
5. Зайдите в подраздел **Защита в режиме реального времени**, установите параметр **Выключить защиту в реальном времени** в значение **Включено**.
6. Отключите параметр **Проверять все загруженные файлы и вложения**.
7. В подразделе **MAPS** отключите все параметры, кроме **Отправлять образцы файлов**.
8. Включите **Отправлять образцы файлов, если требуется дальнейший анализ**, а внизу слева (в том же окне настройки политики) задайте **Никогда не отправлять**.



Примечание: В случае если Windows Defender уже обновился и удалил файлы агента, вам сначала внесите исключения, а затем *переустановите агент*.

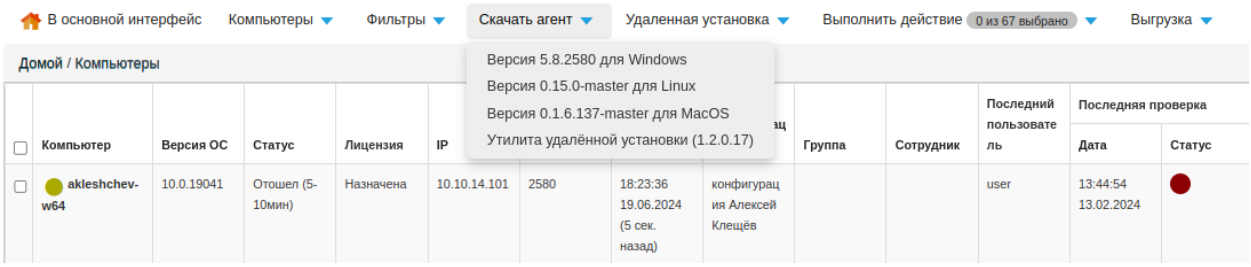
Примечание: Способ настройки в разных версиях антивирусного ПО может отличаться от указанного в документации.

3.3.2 Агент для Windows

Локальная установка

Скачать агент

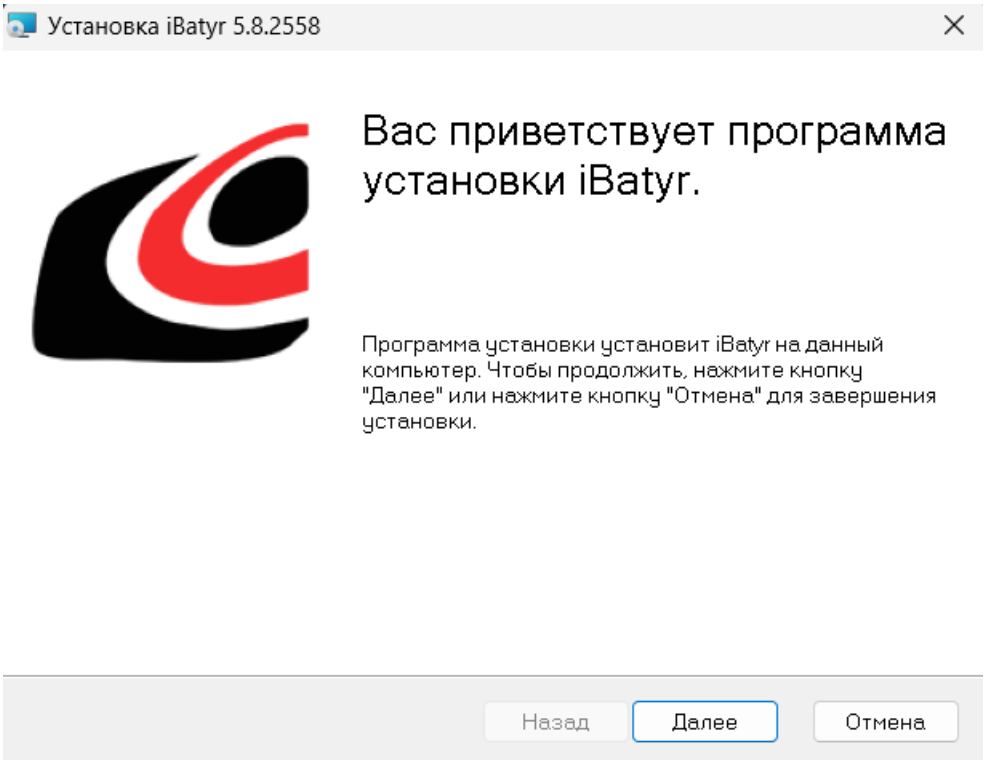
Чтобы скачать программу-установщик агента, в веб-интерфейсе сервера iBatyr Monitor перейдите в раздел **Панель управления** → **Компьютеры**. В выпадающем меню **Скачать агент** выберите **Версия для Windows**.



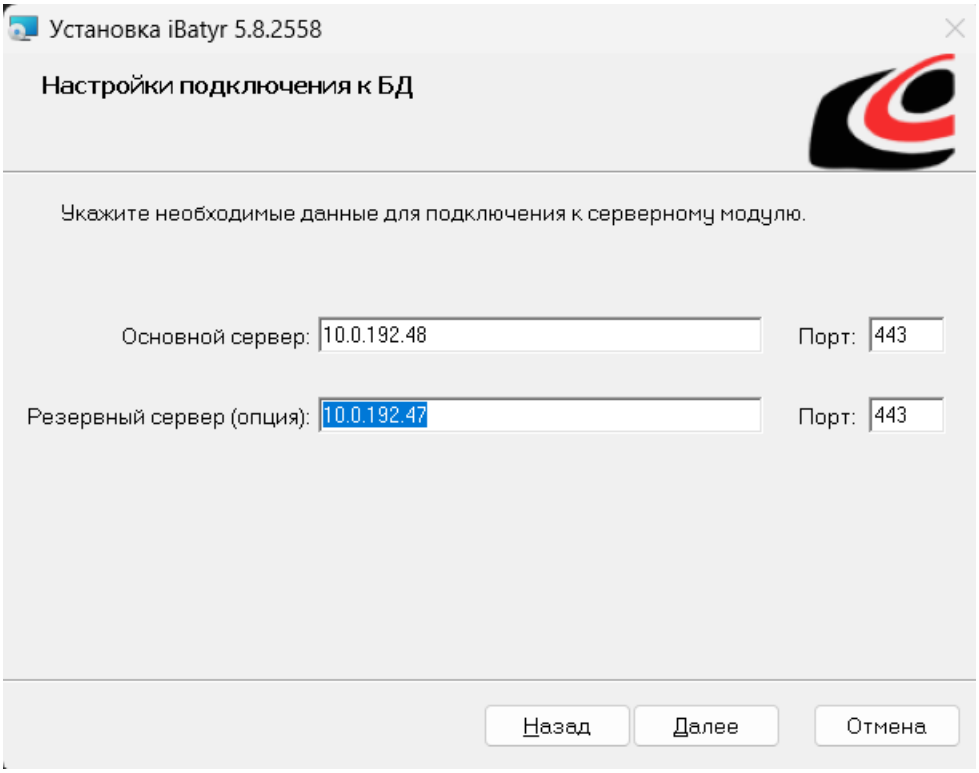
Установка Windows-агента

Примечание: Если вы хотите изменить HWID агента, обратитесь к статье *Настройка HWID*. По умолчанию установится HWID на основе уникальных аппаратных данных компьютера.

Запустите установщик агента **agent-[IP _сервера].msi**. Следуйте указаниям мастера установки.



В окне **Настройки подключения к БД** укажите основной и резервный IP-адреса сервера iBatyr Monitor, к которому будет подключаться агент.



Подтвердите правильность указанных данных и нажмите кнопку **Установить**.

После завершения установки нажмите **Готово** и перезагрузите компьютер для корректной работы агента.

Готово! Агент iBatyr Monitor установлен на компьютер и готов к использованию.

Открытие сетевой шары для установки

Примечание: Если у вас сеть с Active Directory, то лучше сразу попробовать *запустить удалённую установку агента* с правами администратора домена, пропустив шаг настройки сетевых доступов для ресурса ADMIN$.

Если в вашей компании используется централизованное управление политиками антивируса, то перед настройкой рабочих станций пользователей для внедрения iBatyr Monitor агента, стоит произвести *централизованное изменение политик антивируса*.

Оговоримся, что сетевые параметры в сетевой карте не менялись, т. е. никакие галочки в сетевых параметрах не снимались.

Локальная политика безопасности компьютера — не менялась.

Брандмауэр Windows не выключался.

Чтобы удалённый инсталлятор заработал, нам нужно выполнить следующие действия на стороне клиентской машины:

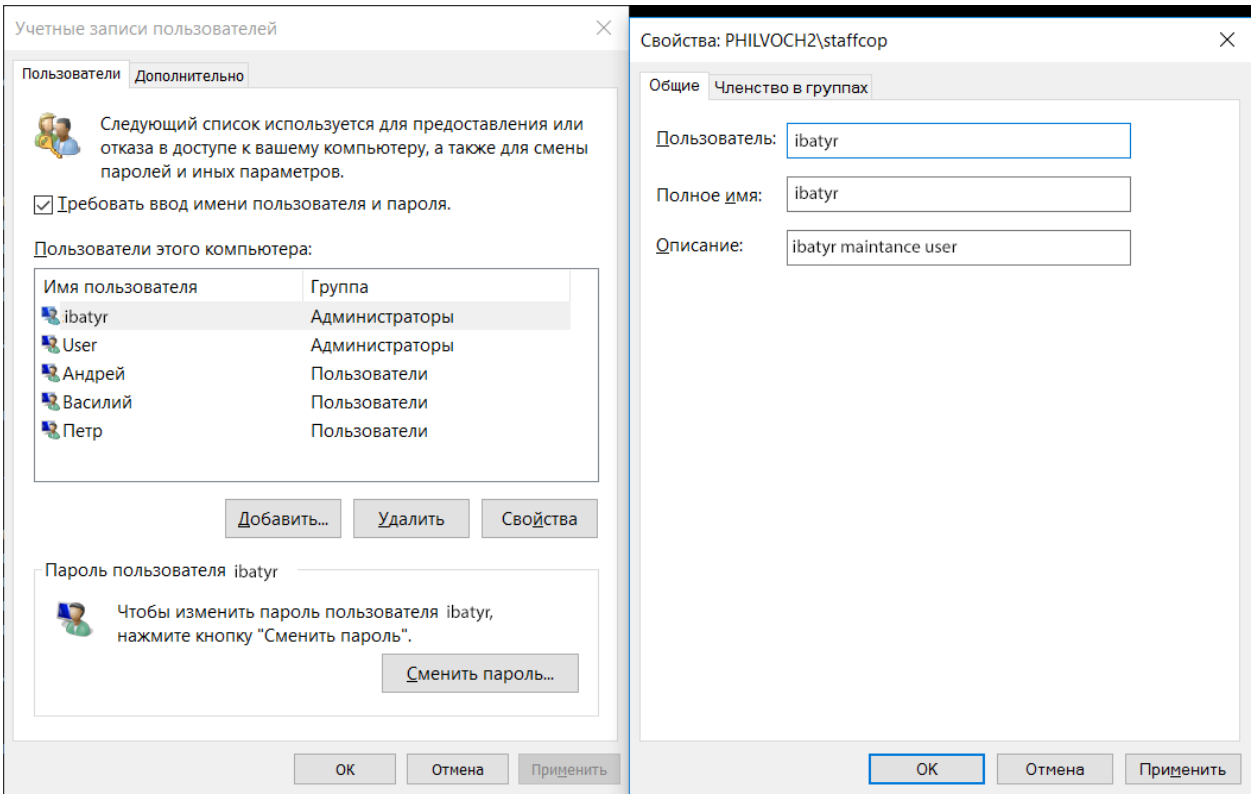
- добавить пользователя через **control userpasswords2**;
- расшарить диск C: по сети через проводник Windows;

- выполнить команду, для внесения изменений в реестр и тем самым разрешив пользователю выполнять команды по сети:

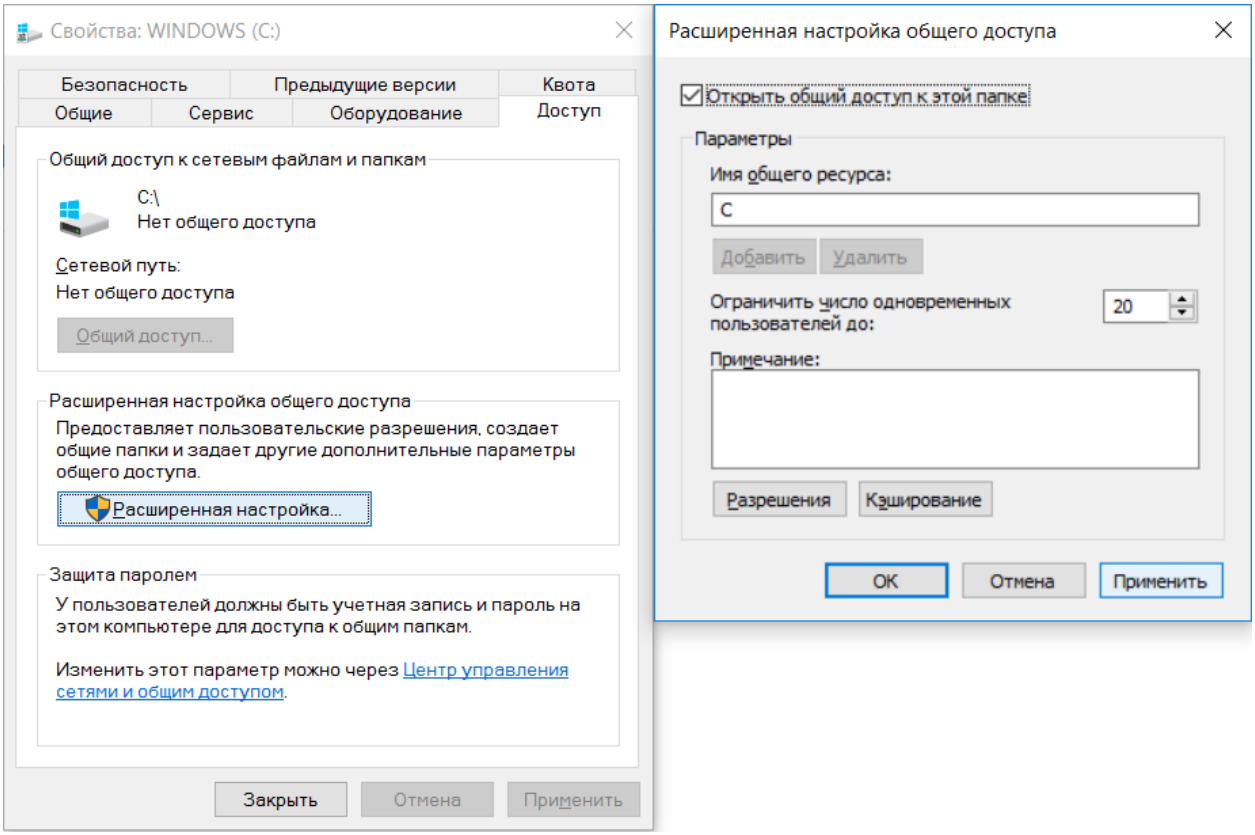
```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v␣
↪LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

1. Входим на компьютер пользователя и запускаем командную строку: **Пуск** → **Программы** → **Служебные Windows** → **cmd**, кликаем правой кнопкой на **cmd** и выбираем пункт — **Запустить от имени администратора** и вводим команду **control userpasswords2** и в открывшемся диалоговом окне/мастере добавляем локального пользователя, например, с именем **ibatyr** и паролем **2wsxCDE#**, роль в системе на второй вкладке **Членство в группах** пользователю выставляем группу **Администратор**.

Командную строку не закрываем, т. к. она нам ещё понадобится.



2. Чтобы расшарить доступ к жесткому диску по сети для нашего пользователя, открываем **Мой компьютер** и кликаем правой кнопкой на диске **C:**, на вкладке **Доступ** нажимаем кнопку **Расширенная настройка** и разрешаем доступ, нажав кнопку **Применить**.



3. Чтобы наш пользователь смог работать с удалённым доступом по сети, нужно в локальной политике безопасности разрешить эти действия, для этого введём через реестр команду на добавление параметров в системный реестр компьютера.

Переключаемся на открытую с правами администратора командную строку и вводим команду:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v␣
↪LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Согласимся с вносимыми изменениями.

На этом этап подготовки компьютера к удалённой установке iBatyr Monitor агента завершён.

Теперь, если в удалённом инсталляторе повторить поиск компьютеров в сети и указать логин и пароль указанный выше, этот компьютер должен появиться в списке тех, кому можно установить агента.

Примечание: Проверка проводилась на Windows10 x64, Windows 7 x64, Windows 8.1 x64 с установленными обновлениями в системе. Возможно, для корректной работы инсталлятора потребуется перезагрузка рабочей станции пользователя.

Тихая установка (без интерфейса)

«Тихая» установка (без интерфейса пользователя) выполняется при помощи утилит SysInternals Suite.

Скачать утилиты SysInternals Suite.

Для начала установки понадобятся:

- пользователь с правами локального администратора или с правами на установку ПО;
- IPv4-адрес компьютера или его имя, на который нужно установить агента;
- адрес и порт сервера iBatyr Monitor;
- включенная *«админская шара»*;
- настроенные *исключения антивирусов*.

В статье будут использованы следующие значения:

Чтобы установить агент на целевую машину:

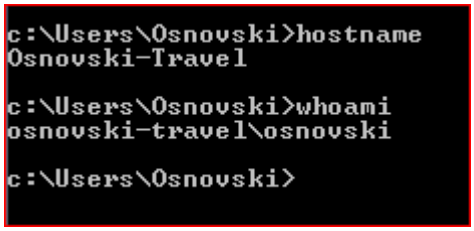
1. В веб-интерфейсе iBatyr Monitor в разделе **Панель управления** → **Компьютеры** → **Скачать агент** → **Версия для Windows** скачайте агент.
2. Переименуйте файл агента в **agent.msi** — именно такое имя добавляется в исключения антивируса.
3. Скопируйте файл агента в папку **C:\Windows** через «админскую шару».
4. Запустите командную строку и перейдите в папку, в которую были скачаны утилиты SysInternals Suite:

```
cd \Portable\PSTools
```

5. Запустите командный процессор на компьютере *osnovski-travel*:

```
psexec -i \\osnovski-travel -u osnovski-travel\osnovski -h cmd.exe
```

6. Введите пароль пользователя.
7. С помощью команд **hosthame** и **whoami** проверьте, что находитесь на целевой машине и вошли под целевым пользователем



8. Запустите установку агента.

Примечание: Если вы хотите изменить HWID агента, обратитесь к статье *Настройка HWID*. По умолчанию установится HWID на основе уникальных аппаратных данных компьютера.

```
msiexec.exe /norestart /l*vx install.log /qn /i "C:\Windows\agent.msi" GATE_
↪URL="ibatyr_server" GATE_URL2="ibatyr_server_reserve" GATE_PORT=port GATE_
↪PORT2=port2 ALLUSERS=1 REBOOT=ReallySuppress
```

В данном случае:

- **C:Windowsagent.msi** — путь к установщику агента; можно указать любой путь, включая сетевой, но необходимо будет добавить его в исключения антивируса;
- **GATE_URL=»ibatyr_server»** — IP-адрес сервера iBatyr Monitor; вместо IP-адреса можно указать имя компьютера;
- **GATE_URL2=»ibatyr_server_reserve»** — резервный IP-адрес сервера iBatyr Monitor; вместо IP-адреса можно указать имя компьютера;
- **GATE_PORT=port** — номер порта сервера iBatyr Monitor; 443 по умолчанию.
- **GATE_PORT2=port2** — номер порта резервного сервера iBatyr Monitor.

Примечание: Если имя установщика агента привести к виду **agent[ip_address#port].msi**, где вместо **ip_address#port** указать IP-адреса и порт сервера iBatyr Monitor, то в команде установки можно опустить параметры «GATE_URL», «GATE_PORT», «GATE_URL2», «GATE_PORT2».

Если после нажатия **Enter** не были выданы сообщения об ошибках, установка агента прошла успешно.

Готово! Агент iBatyr Monitor установлен на вашем компьютере и готов к использованию. Дождитесь, когда он отобразится в веб-интерфейсе сервера.

Журнал установки *install.log* находится в директории, из которой запущена команда установки. Например, если текущий путь *C:|Users|ibatyr*, журнал доступен по пути *C:|Users|ibatyr|install.log*.

При переустановке агента, возможно, понадобится дополнительно указать опцию **REINSTALL=ALL**.

Тихое удаление агента описано в разделе *Удаление агента*.

Автоустановка из исполняемого архива

При необходимости создания исполняемого файла для автоматической установки агента на рабочей станции, обратитесь в службу технической поддержки: **support@ibatyr.kz** .

Пример сценария для WinRar:

```
;Расположенный ниже комментарий содержит команды SFX-сценария

Setup=msiexec.exe /norestart /qn /i "agent_ru.msi" GATE_URL="2.2.2.2" GATE_PORT=443␣
↪ALLUSERS=1 REBOOT=ReallySuppress
TempMode
Silent=1
Overwrite=1
Delete=agent_ru.msi
```

Удалённая установка через инсталлятор агента

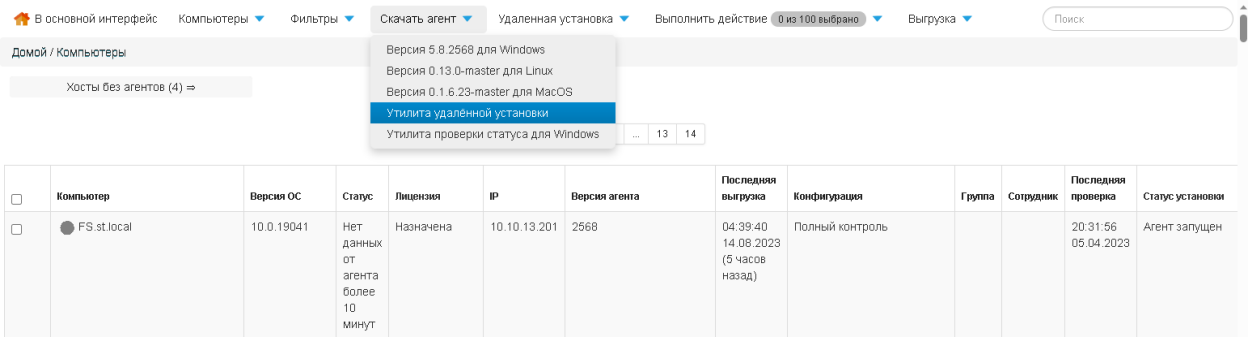
Предупреждение: Удаленная установка используется только для агентов версии 5.8.2498 или выше.

Подходит для установки агента в рабочей группе Windows или в Active Directory. Чтобы установить агенты на рабочие станции:

- *проверьте системные требования для агентов*;
- скачайте агента;
- подготовьте рабочие станции для установки агента;
- добавьте имена ПК пользователей в список на установку агента iBatyr Monitor;
- убедитесь в корректности установки агентов на рабочие станции пользователей.

Скачать агент

В веб-интерфейсе сервера iBatyr Monitor в разделе **Панель управления** → **Компьютеры** нажмите кнопку **Скачать агент**. В выпадающем меню выберите пункт **Утилита удалённой установки**:



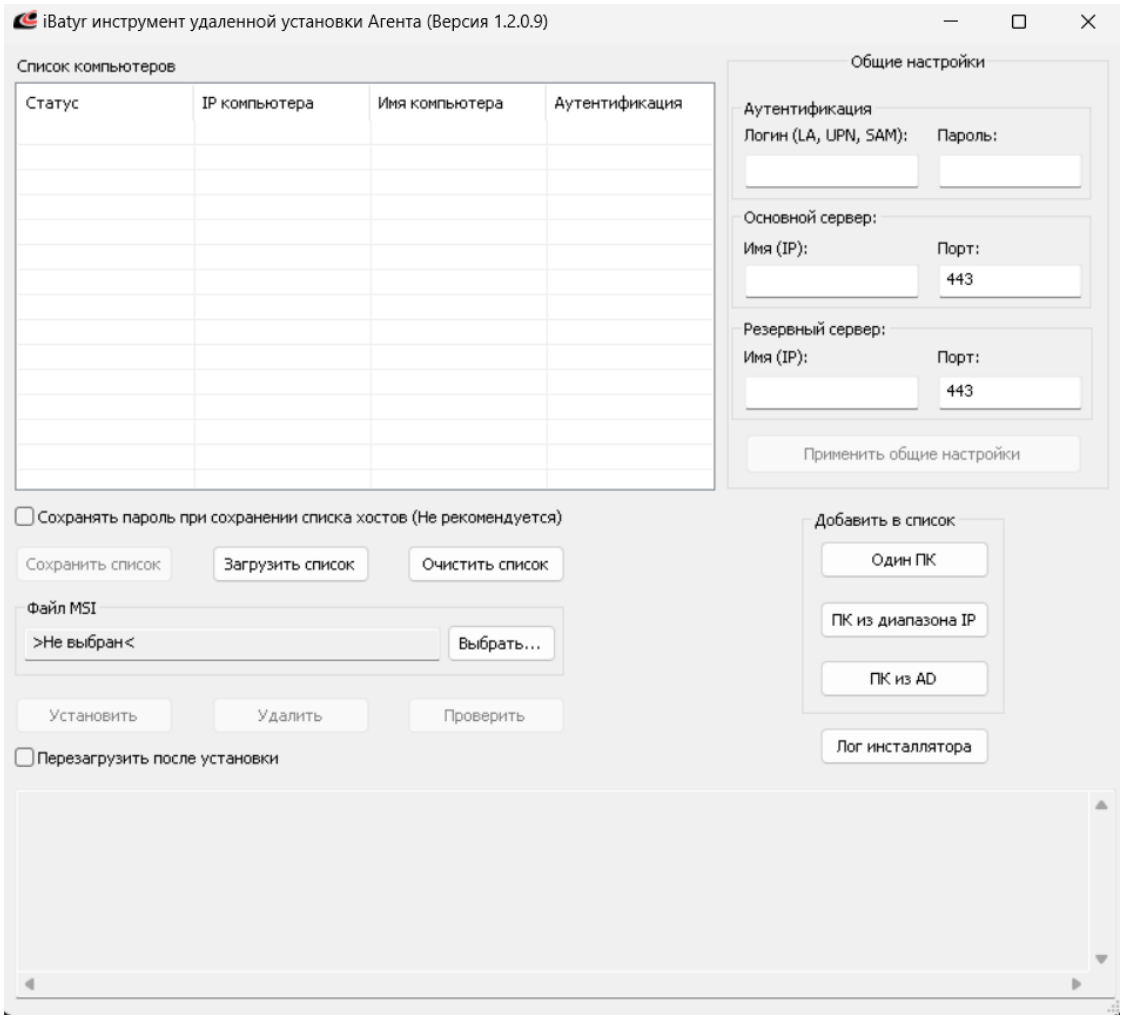
В окне выбора вариантов выберите **Скачать также дистрибутив агента и bat файл для запуска утилиты удаленной установки**.

Предупреждение: Некоторые антивирусы — например, ESET — могут блокировать запуск утилиты. Чтобы этого не произошло, добавьте исполняемый файл «**InstallerUI-ru.exe**» в *список исключений антивируса*.

Порядок работы с утилитой удалённой установки

Примечание: Если вы хотите изменить HWID агента, обратитесь к статье *Настройка HWID*. По умолчанию установится HWID на основе уникальных аппаратных данных компьютера.

1. Запустите утилиту.



2. В разделе **Аутентификация** введите данные для авторизации на удалённых ПК.
3. Добавьте MSI-пакет для установки агента (для проверки сертификата MSI-пакета понадобится доступ в интернет).
4. Добавьте в **Список компьютеров** ПК из вашей сети.
5. Выберите из **Списка компьютеров** нужные ПК.
6. Укажите действия с агентами на ПК (**Установить**, **Удалить**, **Обновить**, **Проверить**).
7. Проверьте работу агентов.
8. Сохраните текущий список ПК для дальнейшего переиспользования.

Подготовка рабочих станций для установки агента

Чтобы подготовить рабочие станции к установке агента:

- проверьте наличие прав администратора на них;
- порты 137,138,139 и 445 на рабочей станции не должны быть заблокированы;
- проверьте наличие *доступа к сетевому ресурсу ADMIN$*;
- внесите агент *в список исключений антивируса*.

Добавить имена компьютеров в список установки агента iBatyr Monitor

Запустите .bat-файл для утилиты удаленной установки **InstallerUI-ru.bat** и следуйте подсказкам установщика.

При добавлении ПК к списку допустимы следующие форматы ввода логина:

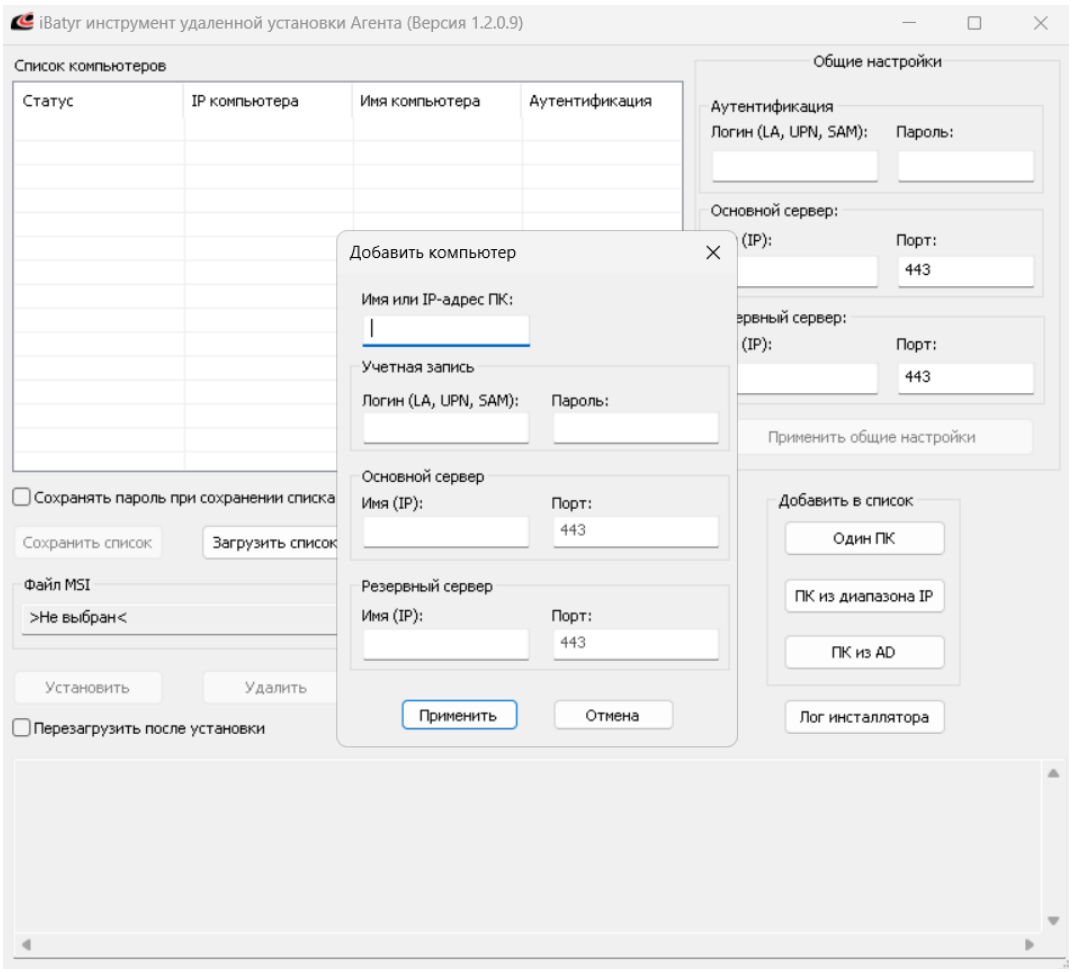
- LA (Local Account) — для подключения к ПК без домена, имя в формате *username*;
- UPN (AD User Principle Name) — подключение внутри домена, имя в формате *username@domain*;
- SAM (AD SamAccountName) — подключение внутри домена, имя в формате *domain/username*.

Введённые данные будут наследоваться при добавлении новых ПК вручную.

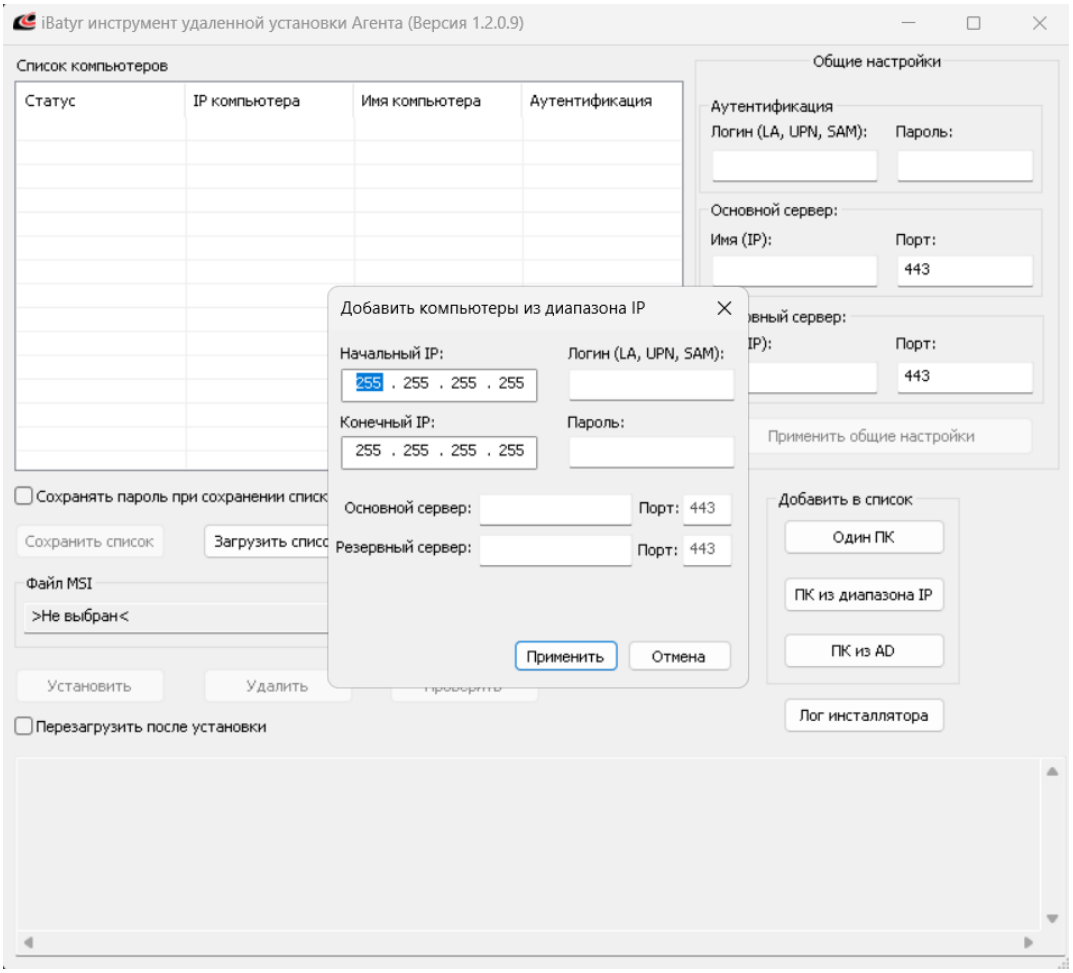
Примечание: В разделе «ПК из AD» используются только форматы UPN и SAM. Отличия между форматами UPN и SAM описаны в документации основных атрибутов Active Directory.

Варианты добавления компьютеров к списку установки:

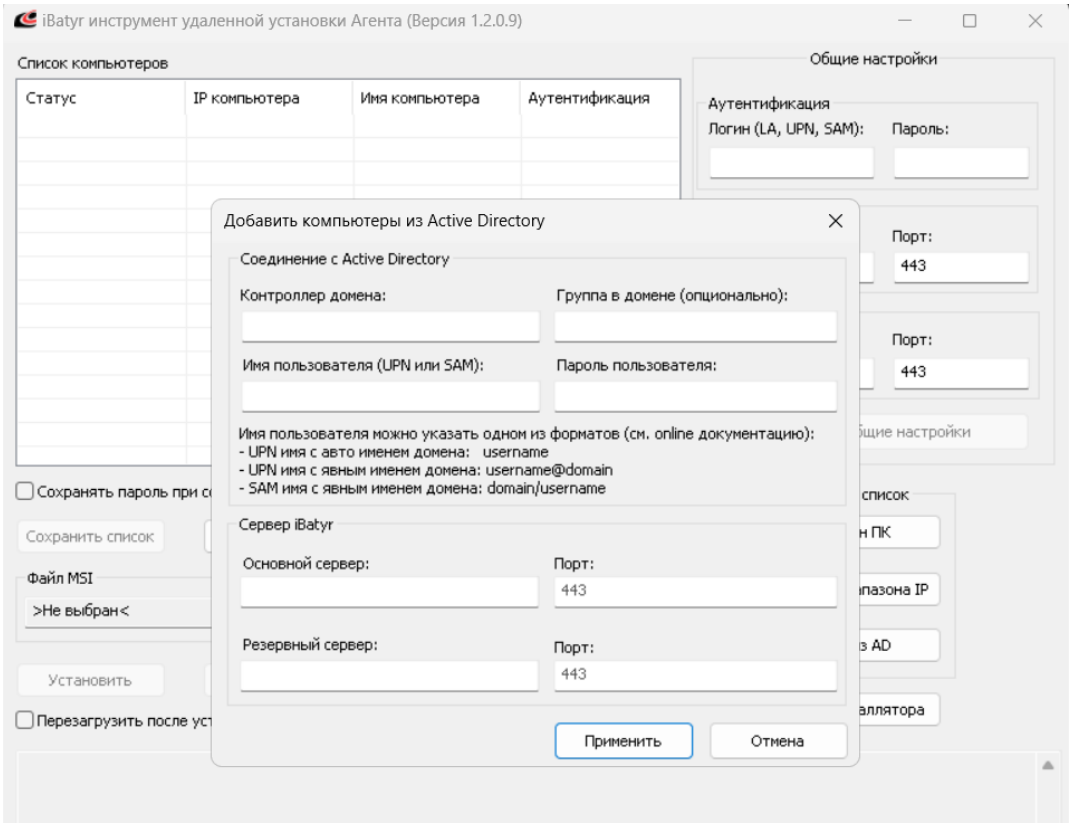
- **Один ПК**. Добавить имена или IP-адреса компьютеров вручную. Нажмите кнопку и заполните обязательные поля.



- **ПК из диапазона IP**. Нажмите кнопку, выберите начало и конец диапазона IP-адресов для сканирования и заполните обязательные поля.


iBatyr инструмент удаленной установки Агента (Версия 1.2.0.9)
Список компьютеров
Статус
IP компьютера
Имя компьютера
Аутентификация
Общие настройки
Аутентификация
Логин (LA, UPN, SAM):
Пароль:
Основной сервер:
Имя (IP):
Порт:
443
Применить общие настройки
Добавить компьютеры из диапазона IP
Начальный IP:
255 . 255 . 255 . 255
Конечный IP:
255 . 255 . 255 . 255
Логин (LA, UPN, SAM):
Пароль:
Основной сервер:
Порт: 443
Резервный сервер:
Порт: 443
Применить
Отмена
Сохранять пароль при сохранении списк
Сохранить список
Загрузить списо
Файл MSI
>Не выбран<
Установить
Удалить
Перезагрузить после установки
Добавить в список
Один ПК
ПК из диапазона IP
ПК из AD
Лог инсталлятора

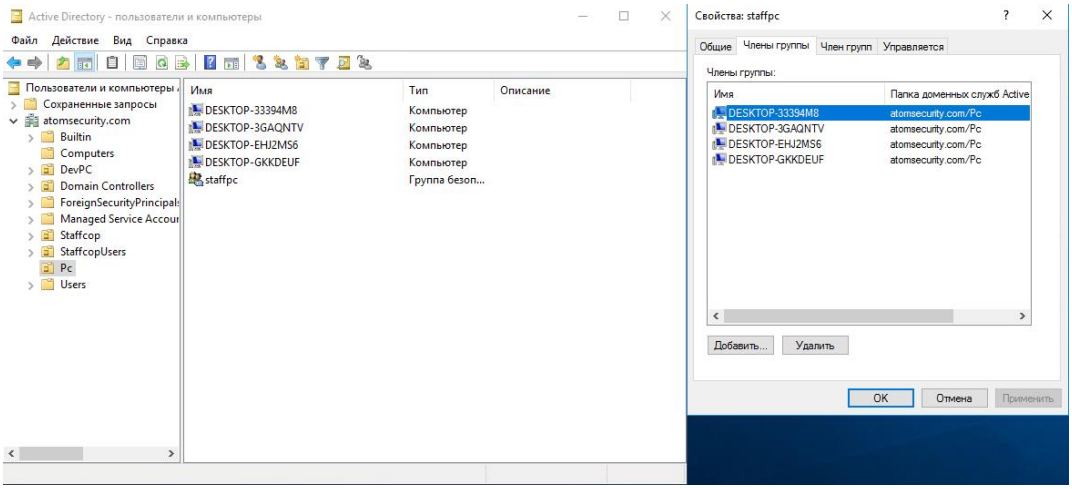
- ПК из AD.



Для использования этого способа настройте AD:

– создайте отдельную группу компьютеров в AD;

– внесите выбранные компьютеры в созданную группу.



В приведённом выше примере в удалённом установщике группа, в которую входят пользователи, называется **ibatyr_safety_group**. Именно это название нужно указать в форме добавления новых ПК в список на установку.

Примечание: Если не указать имя группы, то установщик попытается отыскать все возможные имена ПК в указанном AD по имени группы «Domain computers». Если список возвращаемых имён ПК пуст, попробуйте указать корректную группу в AD и

повторите попытку подключения к AD.

- **Загрузить список**. Позволяет добавить имена ПК из заранее подготовленного списка. Нажмите **Загрузить список** и в открывшемся окне выберите файл формата *.txt* . Файл со списком можно создать вручную или воспользоваться ранее сохранённым списком из утилиты установки.

  Правила оформления списка компьютеров:

  – имена (IP-адреса) компьютеров расположены в столбик;

  – одно имя (IP-адрес) — одна строка;

  – знаки препинания в качестве разделителей не используются.

Нажмите **OK** и выбранные имена компьютеров появятся в списке на установку агента.

Выберите, кому из найденных пользователей установить агент iBatyr Monitor.

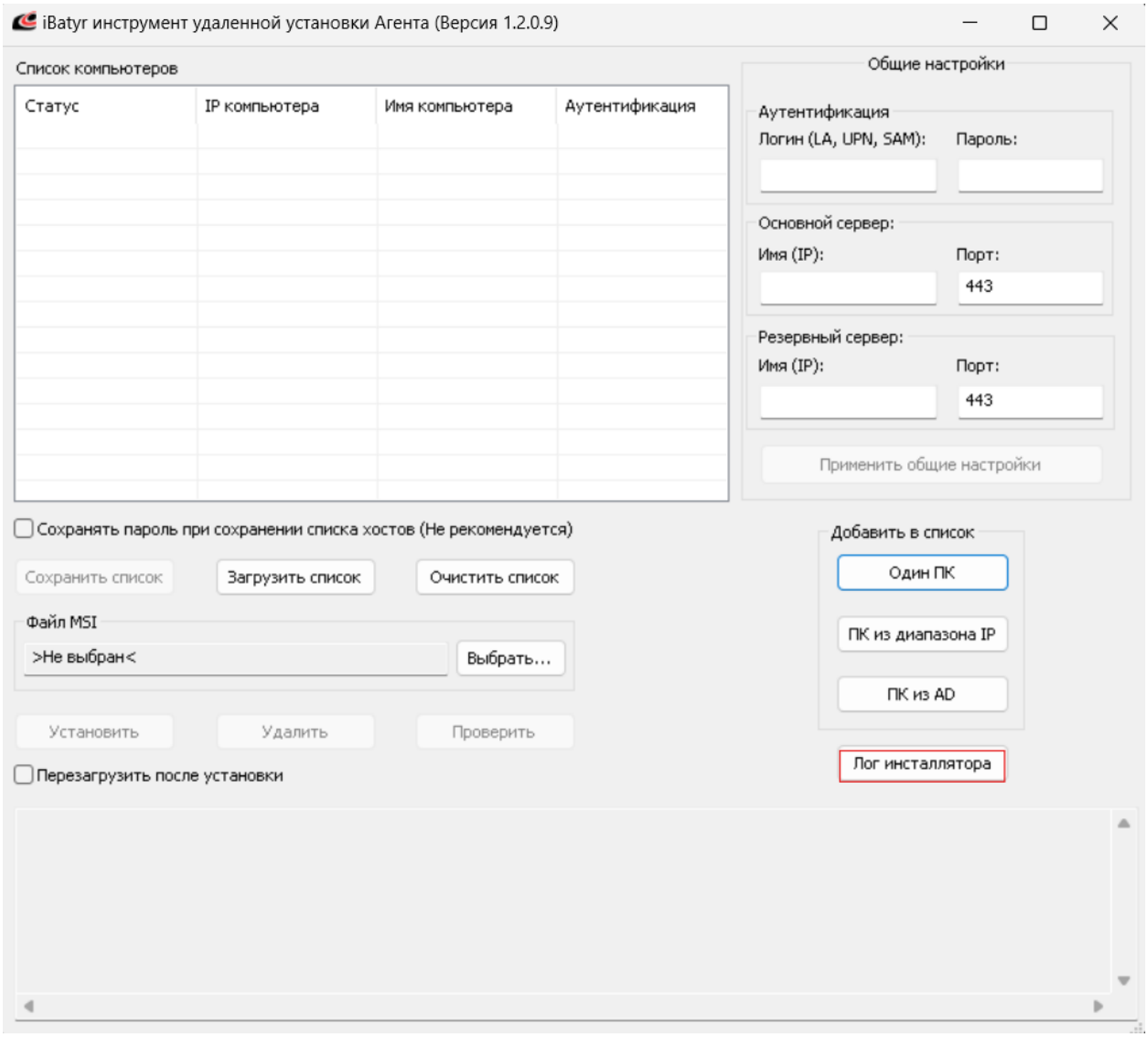
Примечание: Чёрные, красные и серые индикаторы статуса напротив имени машины означают, что агента не удастся установить/удалить на этой рабочей станции.

Нажмите **Установить** и начнётся установка агентов на выбранные компьютеры.

После завершения установки агенты обновят свои статусы и начнут присылать информацию на сервер iBatyr Monitor .

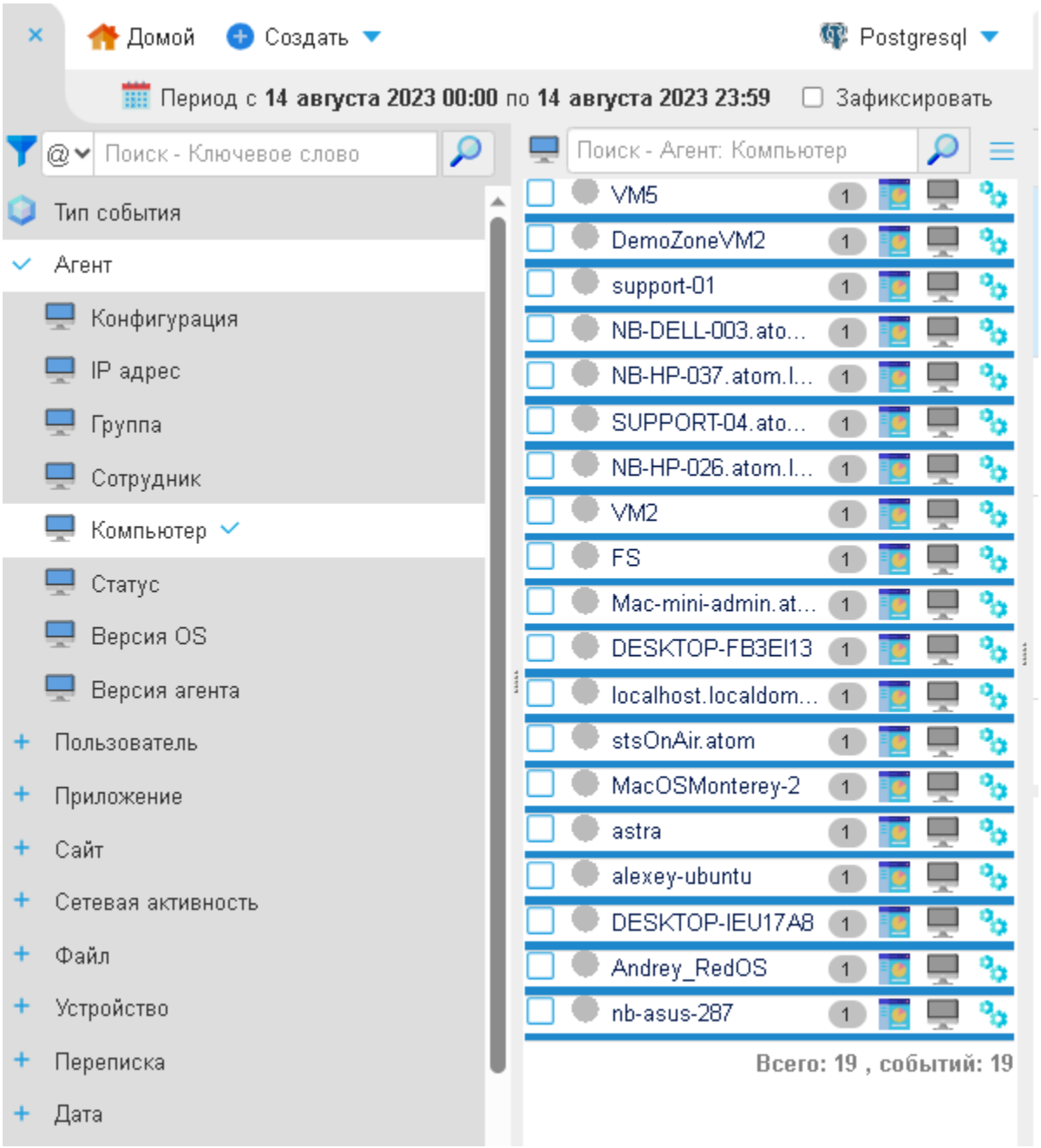
После завершения установки, сохраните список просканированных компьютеров в отдельный файл кнопкой **Сохранить список**. Это будет удобно для дальнейшей работы с агентами.

Чтобы получить лог установки, выберите нужные ПК в списке и нажмите **Лог инсталлятора**.



Проверка правильности установки агентов

После обновления страницы веб-администратора iBatyr Monitor в интерфейсе должны появиться полученные от агентов данные.



Дистанционное удаление

Первый способ

Удалить агент с одного или нескольких ПК можно с помощью утилиты удалённой установки:

- загрузите список установки, который был использован ранее или просканируйте сеть на наличие ПК;
- выберите из списка компьютеры, с которых нужно удалить агентов;
- нажмите **Удалить**.

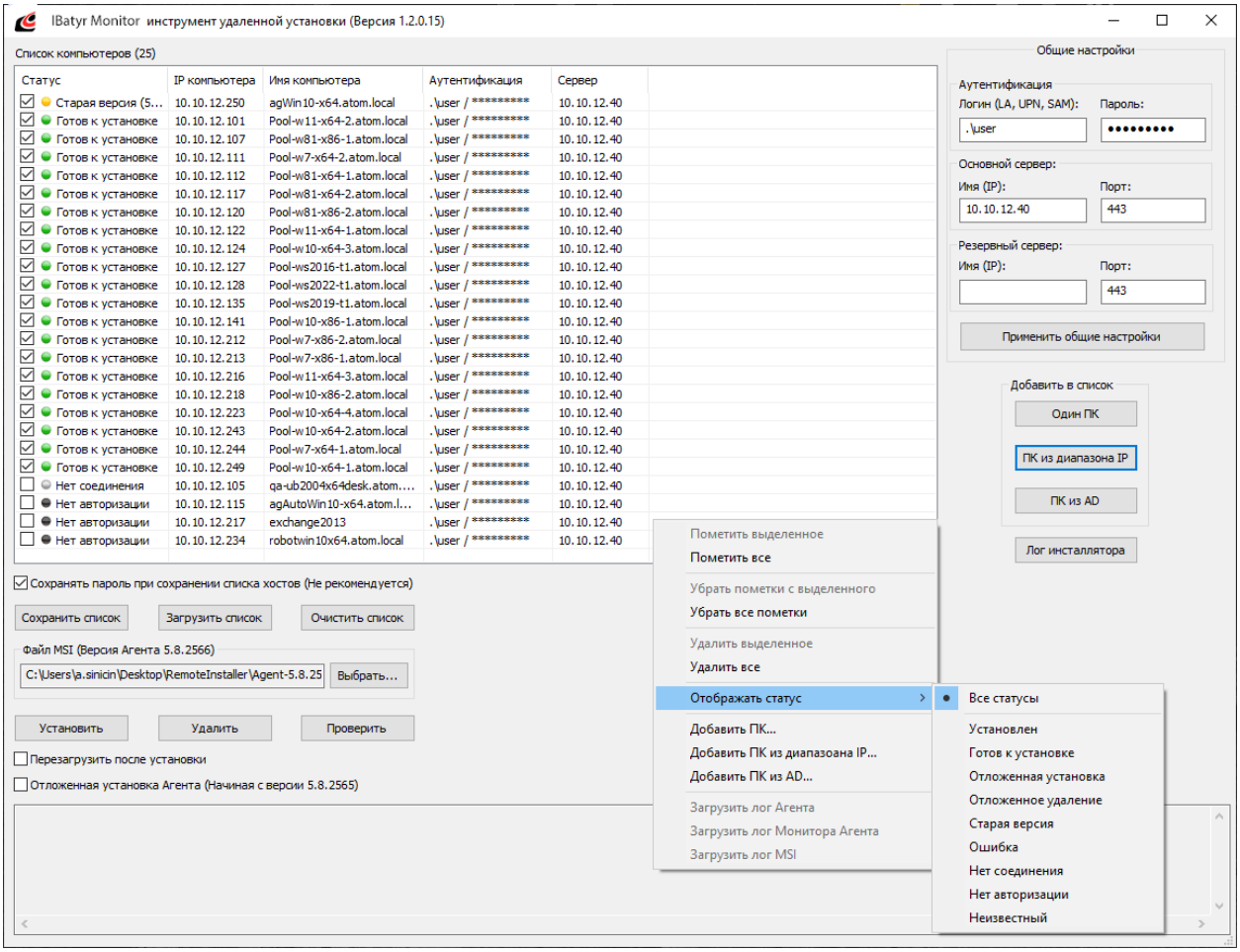
Через некоторое время после завершения удаления, можно просканировать сеть снова, чтобы убедиться, что агенты на выбранных станциях удалены. Значок напротив рабочей станции будет «зелёным», т. е. система свободна от агента.

Второй способ

Удалить агента можно из меню администрирования: *Админ* → *Панель управления* → *Выбрать необходимые ПК* → *Вызов деинсталяции*.

Статус агента

Утилита удалённой установки позволяет отслеживать статусы агентов на машинах в сети и фильтровать список машин по статусам.



Оставшиеся вопросы

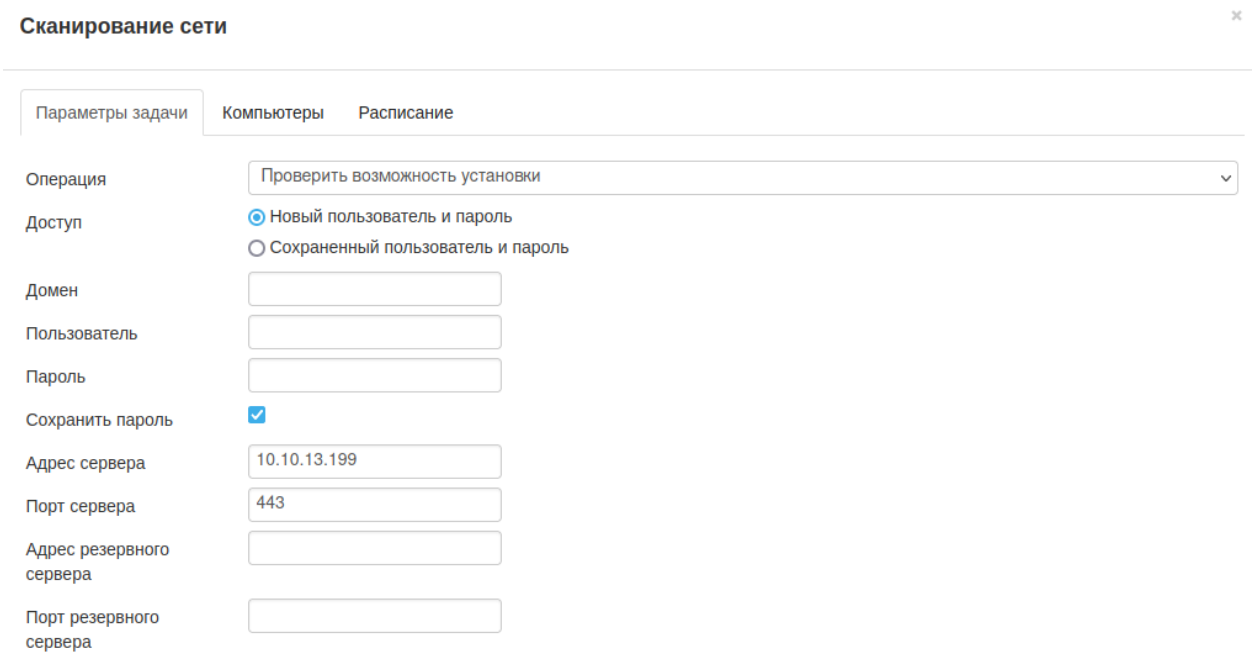
По всем возникшим в ходе работы вопросам обращайтесь в *отдел технической поддержки пользователей*.

Установка через веб-интерфейс

Установка агентов доступна через веб-интерфейс. Для этого перейдите в **Панель управления** → **Компьютеры**. Меню **Удаленная установка**

Установка в локальной сети

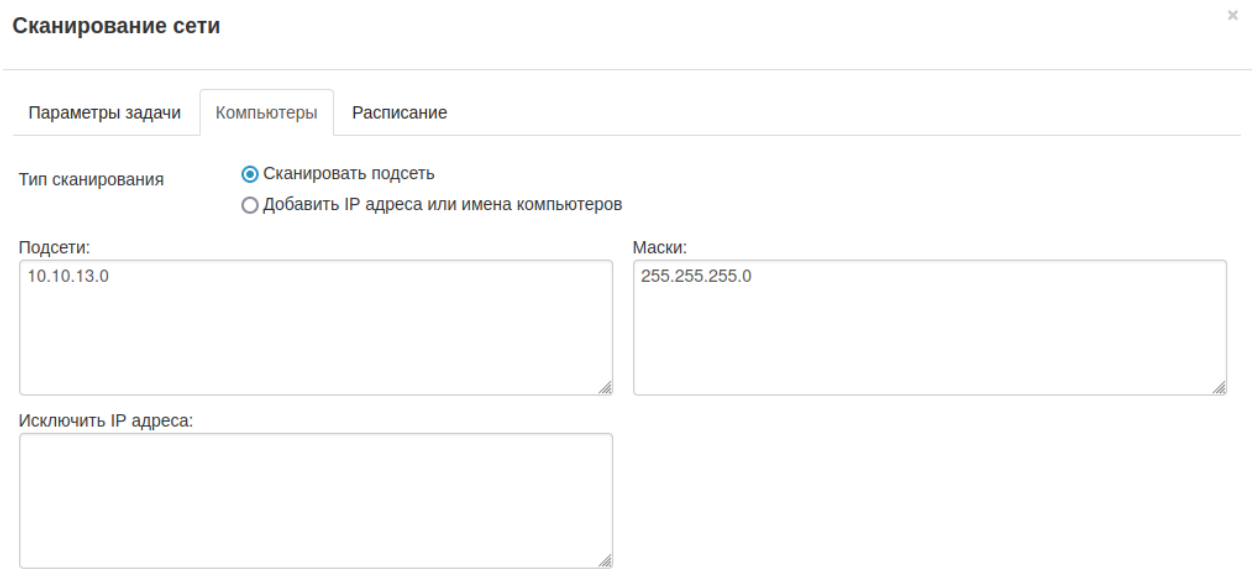
Во вкладке **Параметры задачи** находятся следующие опции:



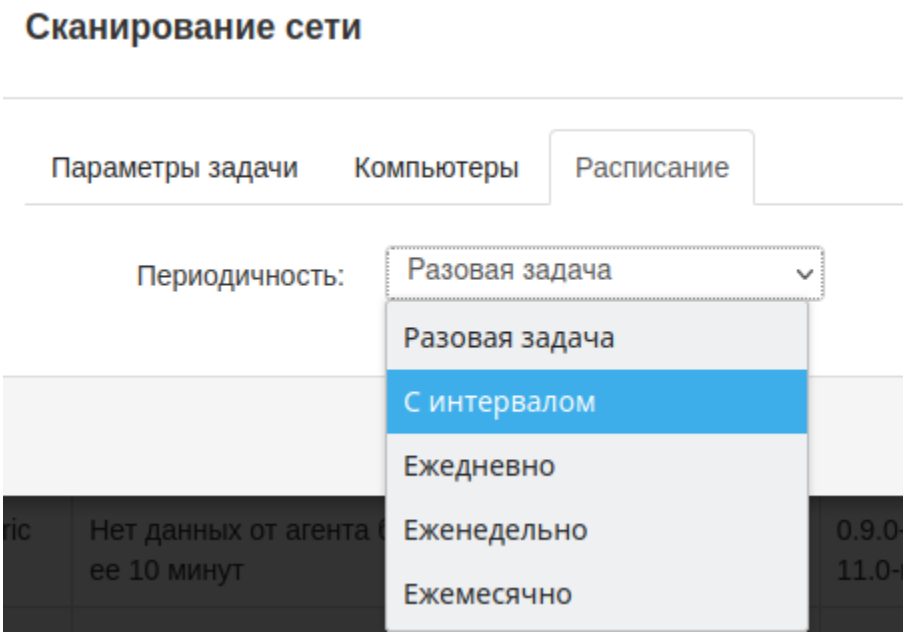
- **Операция** — позволяет установить, переустановить, удалить агента или проверить возможность установки в просканированном диапазоне сети.
- **Доступ** — позволяет выбрать существующий логин и пароль из хранилища паролей.
- **Домен** — заполняется, если используется доменная учетная запись.
- **Пользователь** — логин пользователя.
- **Пароль** — пароль пользователя.
- **Сохранить пароль** — сохраняет логин и пароль в хранилище паролей.
- **Адрес сервера** — адрес сервера iBatyr Monitor.
- **Порт сервера** — порт сервера iBatyr Monitor. По умолчанию 443.
- **Адрес резервного сервера** — адрес резервного сервера iBatyr Monitor.
- **Порт резервного сервера** — порт резервного сервера iBatyr Monitor.

Примечание: Учетная запись должна обладать правами администратора на машине, на которой устанавливается агент.

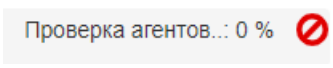
Во вкладке **Компьютеры** имеются возможность указать подсети, IP-адреса или имена компьютеров для сканирования.



Во вкладке **Расписание** есть возможность выбрать периодичность запуска сканирования сети.



После запуска сканирования сети появится окно статуса сканирования и установки:



Возможные ошибки

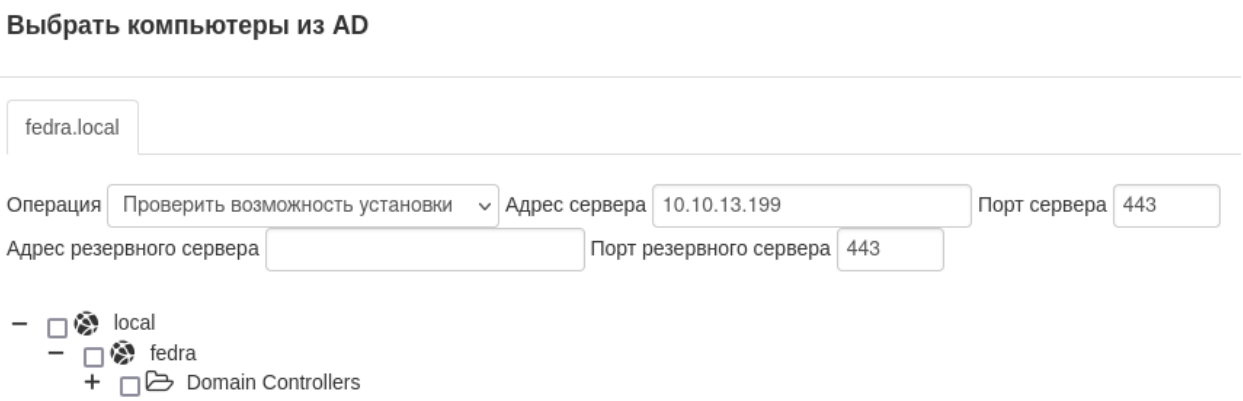
Если вы сталкиваетесь с ошибками «ERROR: No memory» или «Необходима ручная настройка», то выполните в cmd на машине с агентом:

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters /t␣
↪REG_DWORD /v Size /d 00000003 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory␣
↪Management" /t REG_DWORD /v LargeSystemCache /d 00000001 /f
net stop browser
net stop lanmanserver
net start lanmanserver
net start browser
```

Установка в Active Directory

Примечание: для возможности установки компьютеров в Active Directory, необходимо заполнить *Настройки AD* и проверить подключение.

После настроенного подключения к Active Directory, вам откроется интерфейс установки:



Укажите адрес и порт сервера, выберите ПК для установки и операцию с агентом. Нажмите кнопку **OK**.

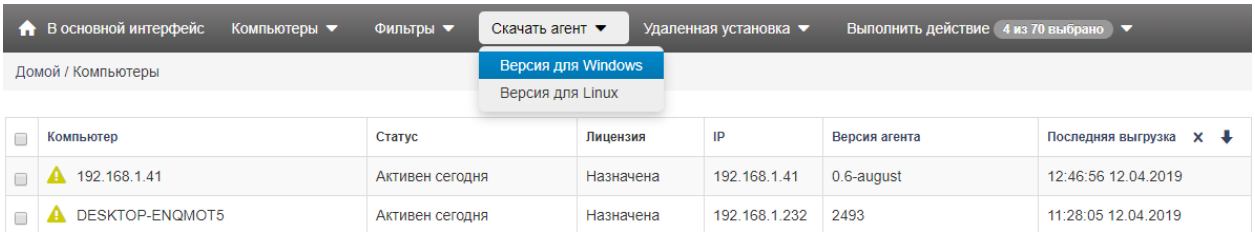
Установка через Active Directory

- *Установка агента через групповую политику AD*
- *Обновление агента через групповую политику*
- *Удаление агента через групповую политику*

Установка агента через групповую политику AD

Скачайте установочный файл агента с веб-интерфейса iBatyr Monitor:

Панель управления — Компьютеры

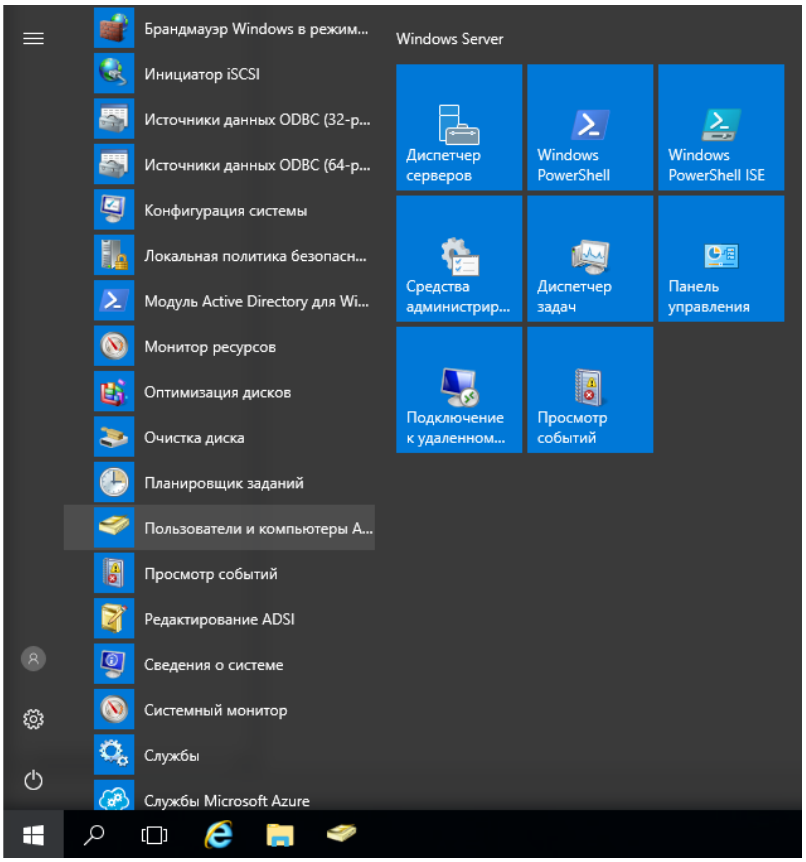


Скопируйте на контроллер домена дистрибутив агента скачанный с сервера **agent_ru-5.8.2465-[192.168.1.134].msi**.

Примечание: Если вы хотите изменить HWID агента, обратитесь к статье *Настройка HWID*. По умолчанию установится HWID на основе уникальных аппаратных данных компьютера.

Поместите этот файл в каталог **C:\sc** на своем компьютере и откройте доступ по сети, чтобы у вас открылось \ **имя_контроллера_домена****sc$**

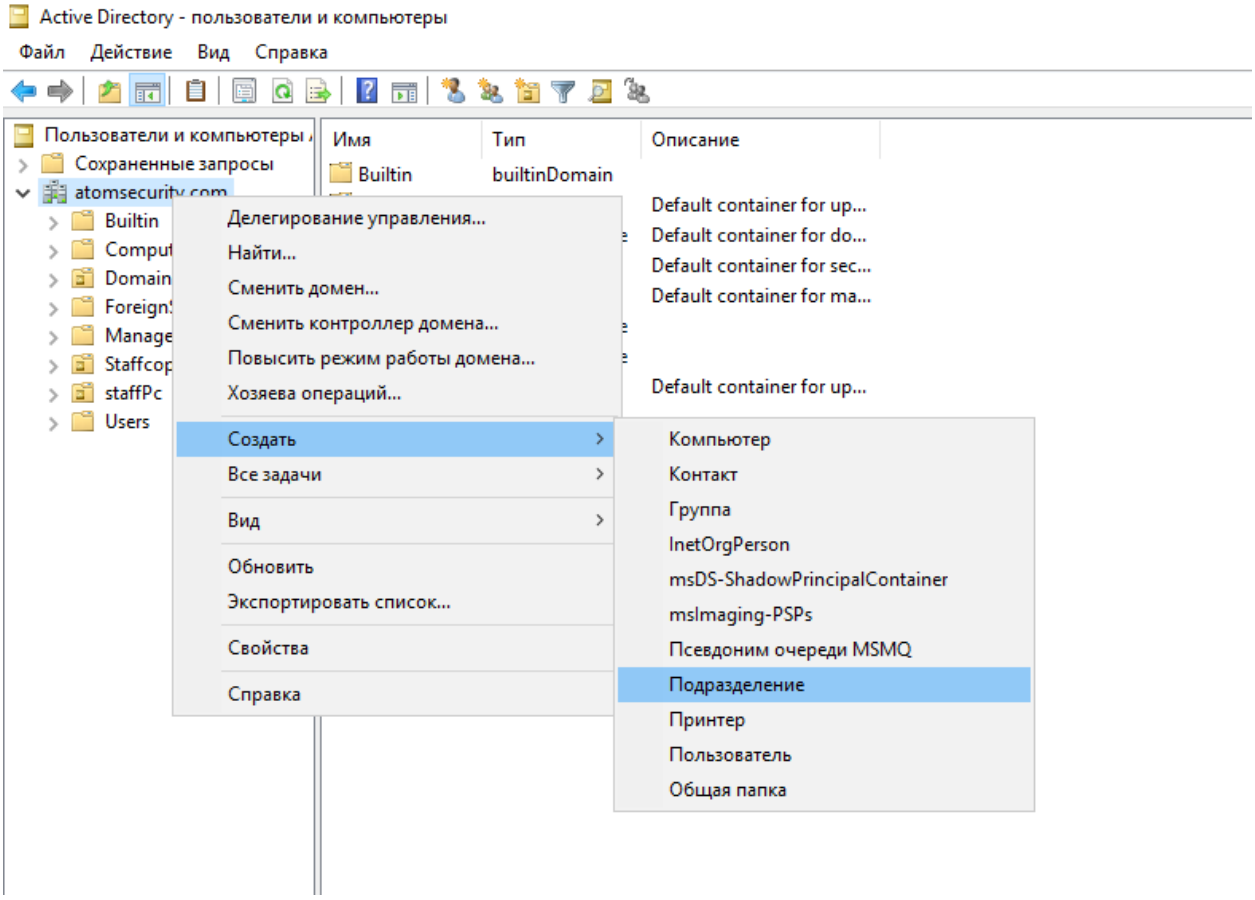
В Панели управления (или в меню «Пуск» для Windows 2003/2008) выберите **Администрирование — Active Directory — Пользователи и компьютеры**.



В домене, включающем компьютеры, на которые предполагается установка агентов, создайте новое **Подразделение** (**Организационное подразделение** для Windows 2000) с именем, например, **iBatyr Monitor**.

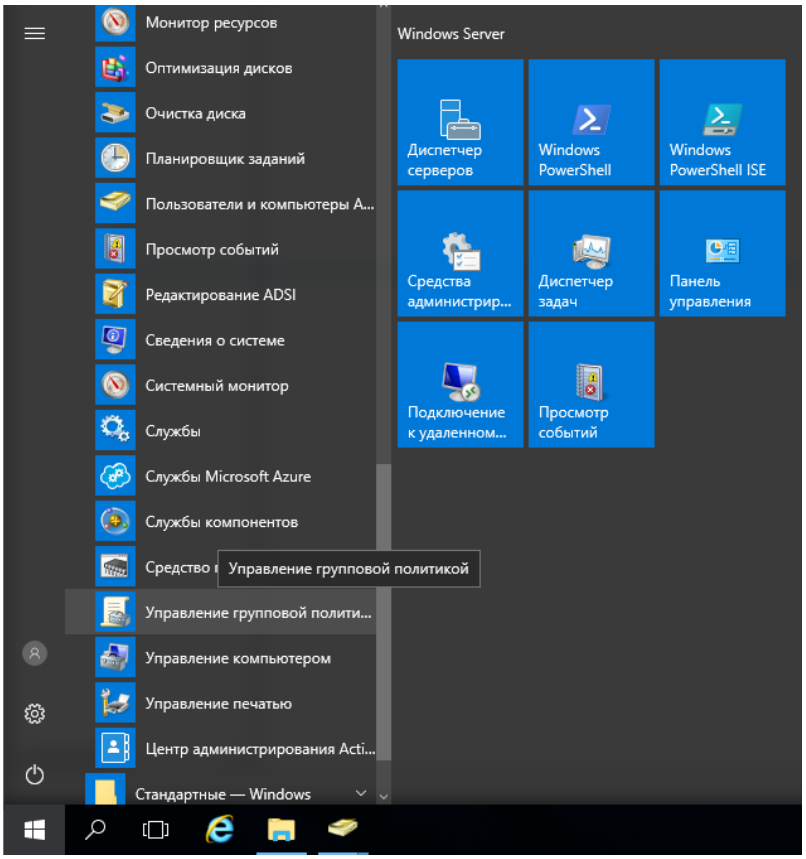
Для этого в контекстном меню домена выберите **Создать** — **Подразделение**. В открывшемся окне введите название нового подразделения и нажмите **OK**.

Включите в созданное подразделение компьютеры, на которые предполагается устанавливать агент.



Откройте окно редактирования групповых политик.

Для этого нажмите **Пуск/Администрирование/Управление групповой политикой**.

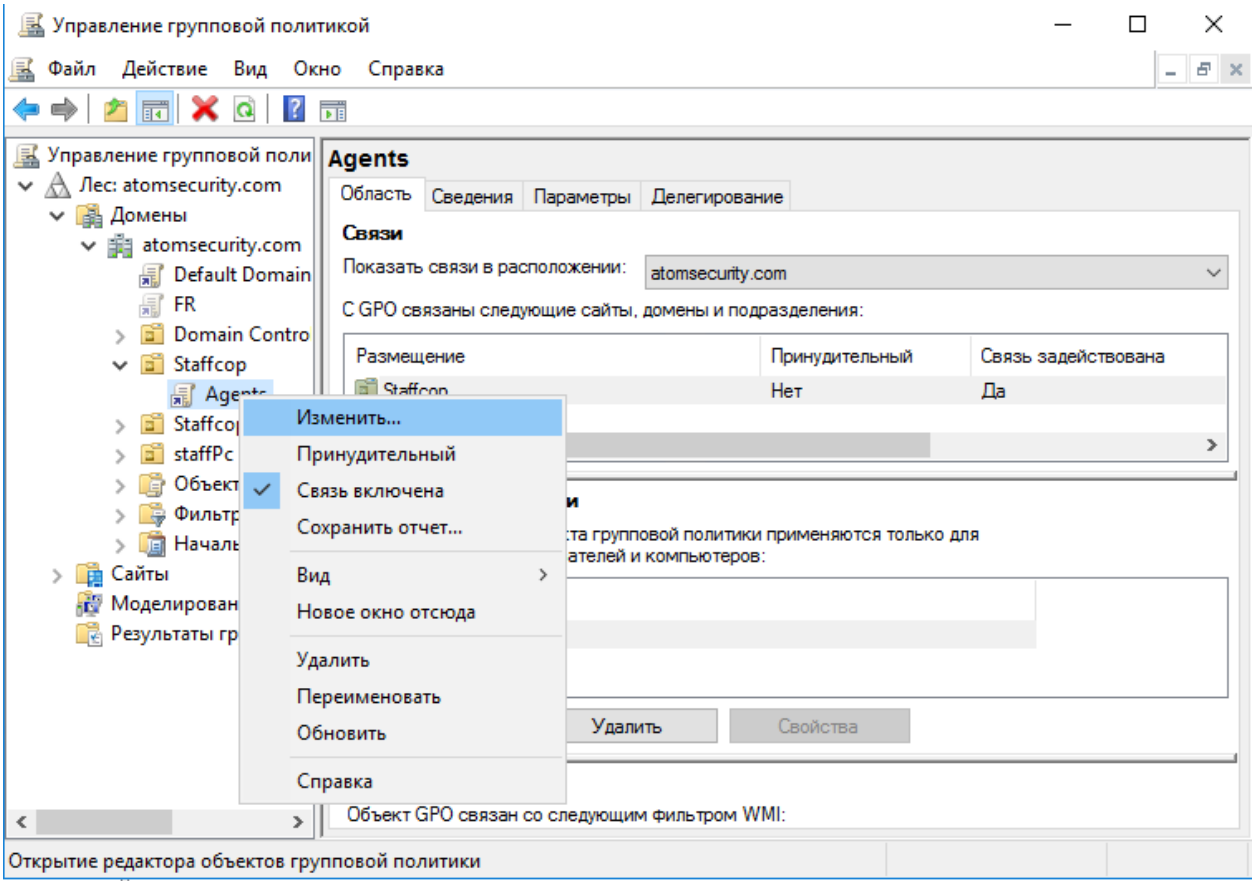


Для созданного подразделения **iBatyr Monitor** задайте групповую политику.

Для этого в контекстном меню созданного подразделения **iBatyr Monitor** выберите пункт **Создать объект GPO в этом домене и связать его...**

В открывшемся окне задайте название нового объекта групповой политики и нажмите на кнопку **OK**.
.. image:: img/active_install_5.png

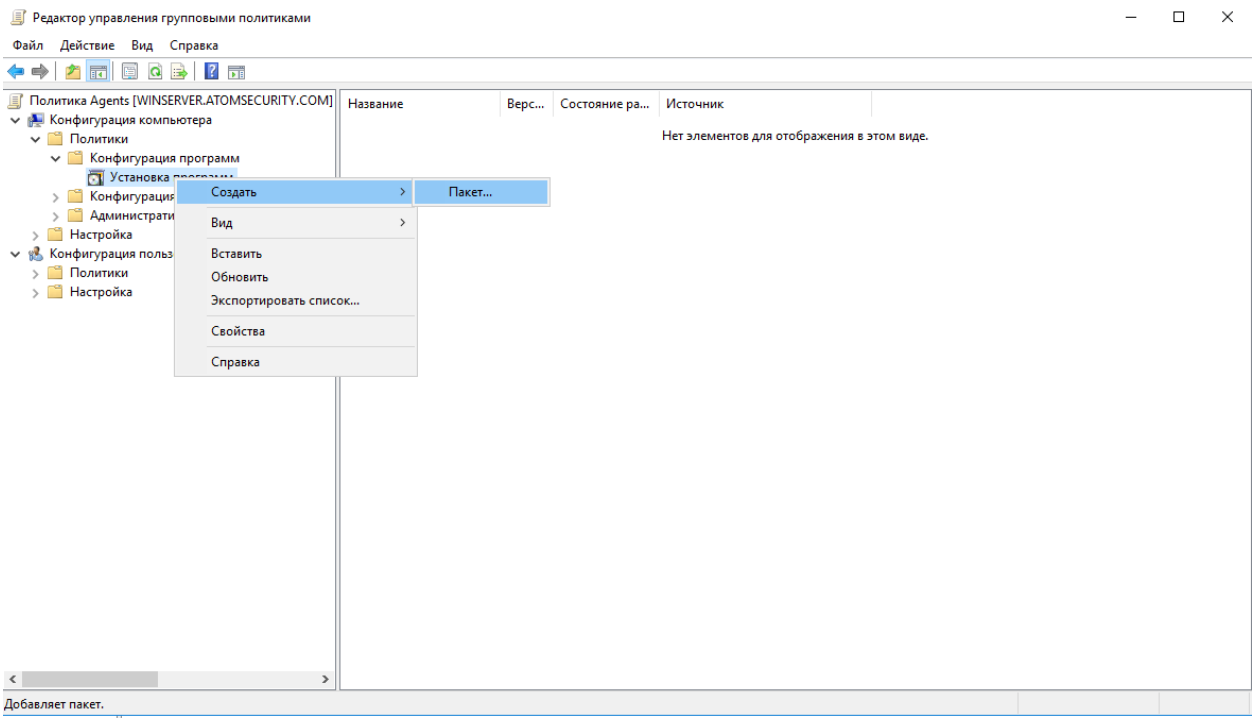
В контекстном меню созданной новой групповой политики выберите пункт **Изменить...**



В открывшемся окне **Редактор управления групповыми политиками** внесите настройки для групповой политики, созданной ранее.

Для этого выберите элемент **Конфигурация компьютера/Политики/Конфигурация программ/Установка программ**.

В контекстном меню элемента **Установка программ** выберите пункт **Создать/Пакет**.



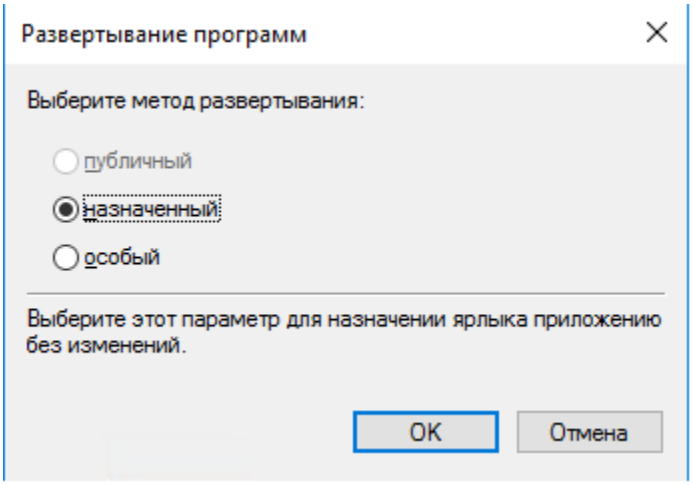
Далее задайте установочный пакет агента.

Для этого укажите адрес сетевого разделяемого ресурса.

Путь к каталогу с пакетом следует указывать в формате сетевых адресов:

\ **имя_контроллера_домена****sc****agent_ru-5.8.2465-[192.168.1.134].msi**.

Откроется окно Развертывание программ. Выберите опцию **Назначенные**. Нажмите **OK**.



Агент будет установлен на выбранные компьютеры при ближайшей регистрации их в домене.

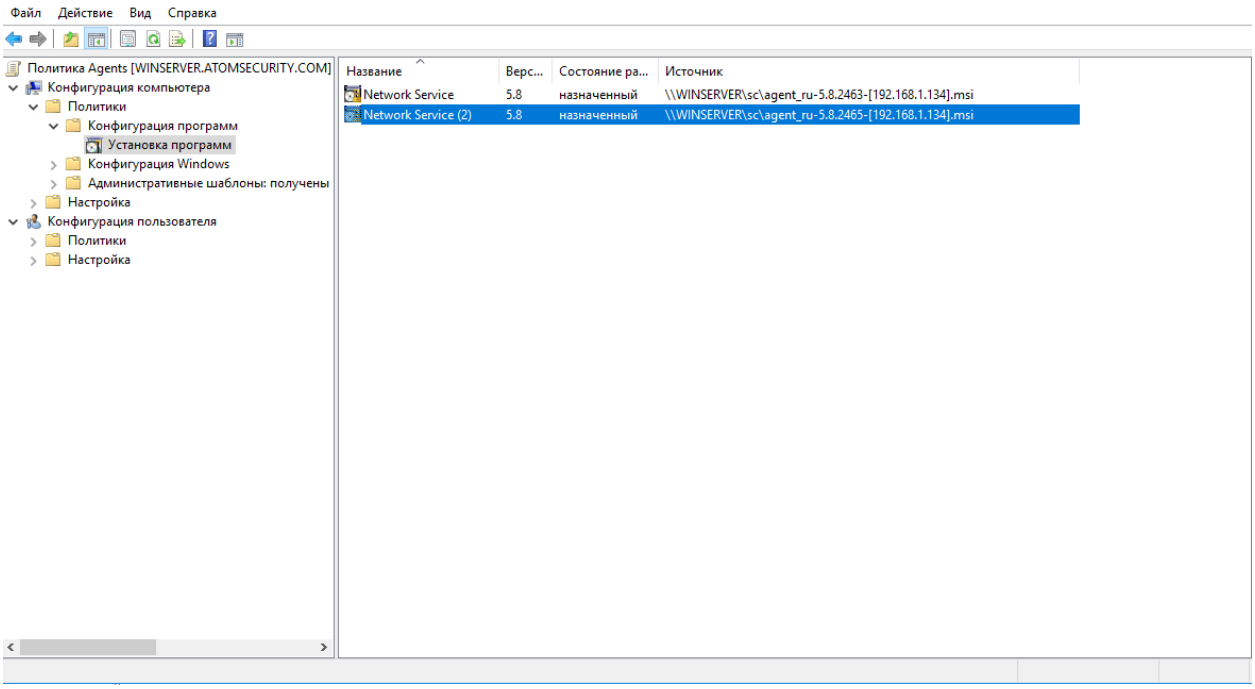
Возможно принудительное применение групповых политик, нужно в командной строке Windows вызвать принудительное обновление групповой политики:

```
gpupdate /force
```

И согласиться на перезагрузку компьютера.

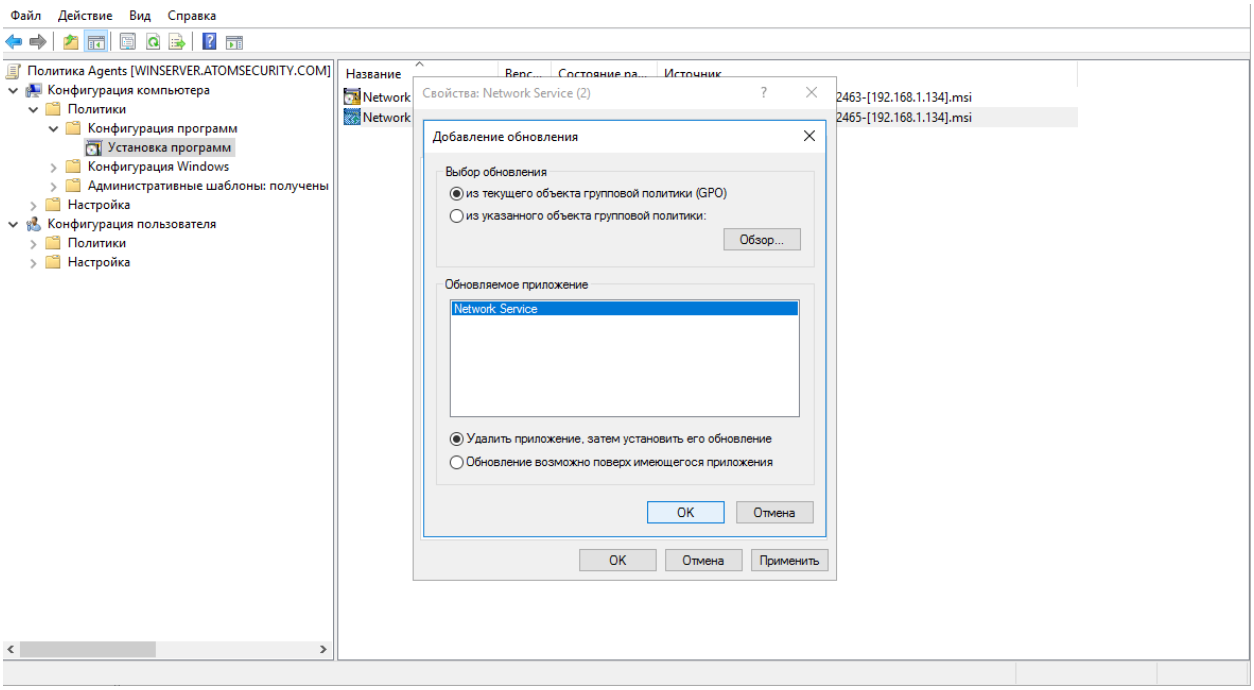
Обновление агента через групповую политику

Аналогично установке агента добавьте дистрибутив агента, на который вам необходимо обновиться, в данное окно:

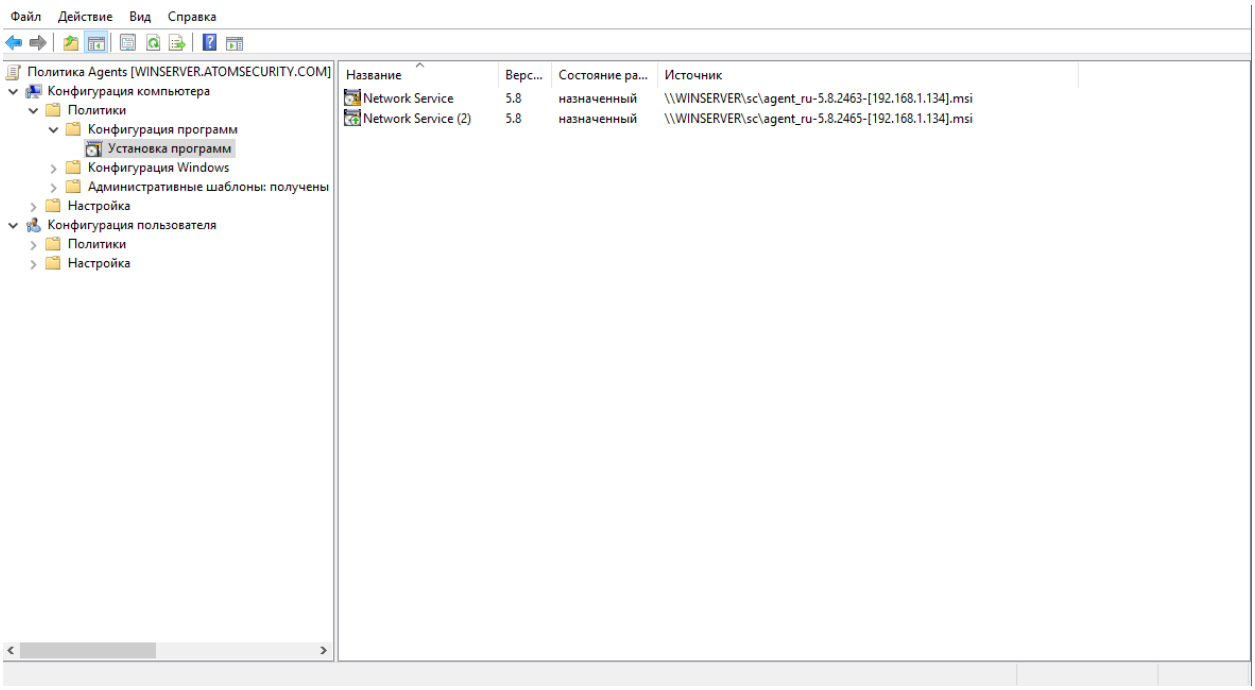


Теперь открываем свойства новой версии агента и переходим на вкладку **Обновления**, нажимаем **Добавить** для выбора приложения, обновляемого данным пакетом.

Выбираем более старую версию агента в открывшемся окне (если новая версия в той же групповой политике, то из текущего GPO, если в другой, то выбираем через кнопку «Обзор»). Ниже можно выбрать удалять предыдущую версию или устанавливать приложение поверх старой версии. Рекомендуется удалять предыдущую версию, дабы не тянуть проблемы из старых версий в новые.



После этого в GPO старые пакеты отображаются с замком, а новые с зеленой стрелкой.



Примечание: Если вы установили агенты через групповые политики, то обновлять агентов нужно только при помощи групповых политик.

Удаление агента через групповую политику

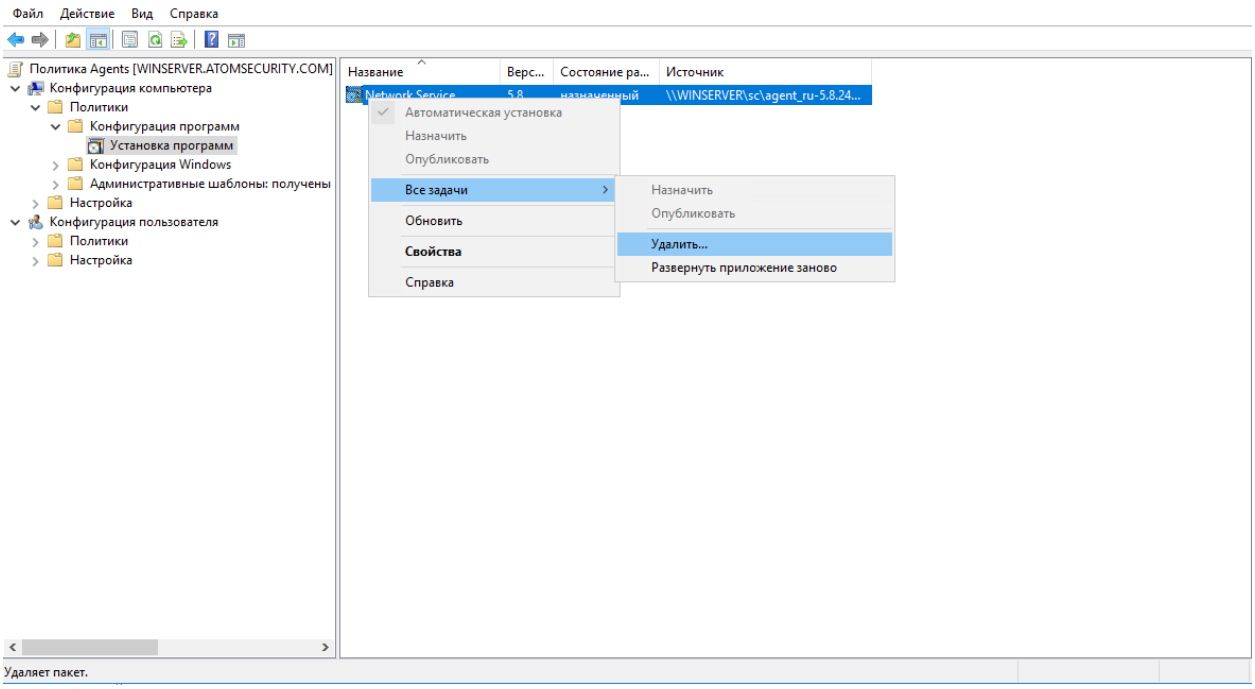
Для удаления агента iBatyr Monitor со станций пользователей запустите оснастку управления групповыми политиками, найдите политику, в которой вы настраивали установку агента iBatyr Monitor.

Нажать на политику правой кнопкой и в выпадающем окне выбрать **Изменить** и в секции:

Конфигурация компьютера — Политики — Конфигурация программ — Установка программ

Удалите ранее добавленного агента, в назаначеных на установку на рабочие станции пользователей агента iBatyr Monitor.

Назначенный пакет для установки может называться в списке как «Network Service».



Затем надо закрыть все окна групповой политики и на стороне клиента перезагрузить машину или вызвать в командной строке принудительное обновление политик:

```
gpupdate /force
```

И согласиться на перезагрузку рабочей станции пользователя.

Удаление агента

Локальное удаление

Запустите с правами администратора установочный файл **agent_ru.msi** и выберете пункт **Удалить установку**.

Примечание: Для удаления приложения желательно запускать тот же установочный файл, которым вы производили установку.

Дистанционное удаление

Аналогично установке агентов через утилиту удалённой установки, можно вызвать массовое или единичное удаление агентов.

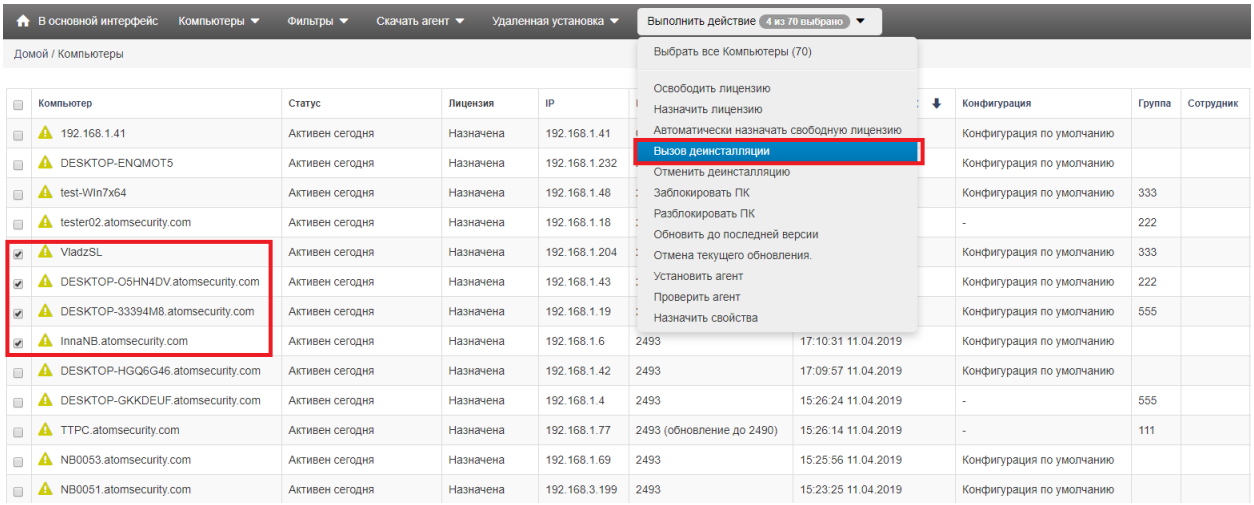
Для этого необходимо загрузить список установки, который был использован ранее либо просканировать вашу сеть снова.

В списке компьютеров выбрать те компьютеры, которым необходимо будет удалить агентов и нажать кнопку **Удалить**.

Через некоторое время после завершения удаления, можно просканировать сеть снова, чтобы убедиться, что агенты на выбранных станциях будут удалены и значок напротив рабочей станции будет «зелёным», т. е. система будет освобождена от агента.

Удаление через веб-интерфейс

Для удаления агентов через веб-интерфейс перейдите в меню **Панель управления**. Выберите ПК, с которых вы хотите удалить агентов, и выберите **Выполнить действие** → **Вызов деинсталляции**. После перезагрузки компьютера агент удалится.



Тихое удаление

Нужно производить в командной строке:

Пуск → **Программы** → **Стандартные** → **Коммандная строка**, кликнуть правой кнопкой, выбрать пункт **Запустить от имени администратора** и ввести эту строку:

```
msiexec.exe /uninstall C:\windows\agent.msi /qn /norestart REBOOT=ReallySuppress
```

При этом установочный файл агента **agent.msi** должен находиться в папке **C:\windows**

Настройка HWID

Агент использует Уникальный идентификатор диска (**HWID**) для регистрации на сервере и взаимодействия с сервисом мониторинга.

С версии iBatyr Monitor 5.5 для Windows-агентов с версии 5.8.2583 добавлены новые параметры, которые позволяют:

- выбирать тип HWID, который будет использоваться при установке;
- удалять текущий HWID из реестра и устанавливать новый.

Примечание: Параметры **HWID** опциональны. По умолчанию установится HWID на основе уникальных аппаратных данных компьютера.

Передача параметров происходит двумя способами:

- *через управление командой msiexec в командной строке* — используйте этот способ при *Тихой установке* и установки из *Active Directory*;
- *изменение названия MSI-файла* — используйте при установке через *Утилиту удаленной установки* и *Локальную установку*.

Параметры HWID

- `hwid` — значение HWID, которое зависит от выбранного типа: HWID, HWID-FQDN или FQDN.
- `use_fqdn` — тип HWID, который может принимать следующие значения:
  - `0` (или отсутствие параметра) — **HWID** – идентификатор на основе уникальных аппаратных данных компьютера в формате GUID, например: 076ee660-54b6-49c3-baaf-b0f8bb81f9e1. Сохраняется в реестре, не изменяется при смене имени или настроек сети. При удалении генерируется повторно.
  - `1` — **HWID-FQDN** – использует полное доменное имя компьютера (FQDN) в нижнем регистре. Сохраняется в реестре и не меняется. При удалении из реестра генерируется повторно.
  - `2` — **FQDN** – полное доменное имя компьютера (FQDN), не сохраняется и не читается из реестра. Это значение генерируется при каждом запуске агента. При удалении из реестра заново не создается.

Примечание: Тип и значение HWID хранятся в ветке реестра: HKEY_LOCAL_MACHINESYSTEMSCHWID.

Передача параметров через команду msiexec

Для команды установки агента `msiexec` добавлены два новых параметра:

- **DROPHWID**:
  - `DROPHWID=1` — удаляет текущий HWID и генерирует новое значение.
  - `DROPHWID=0` — не удаляет текущий идентификатор.

  При некорректном значении тип HWID не изменится, а в логе инсталлятора появится сообщение.

- **HWIDMODE**:
  - `HWIDMODE=HWID`, `HWIDMODE=HWIDFQDN`, `HWIDMODE=FQDN` — задает тип HWID. При некорректном значении в логе будет сообщение об ошибке.

Пример команды, которая удалит текущий HWID и установит HWID-FQDN:

```
msiexec.exe /norestart /l*vx install.log /qn /i "C:\Windows\agent.msi" GATE_URL="ibatyr_
↪server" GATE_URL2="ibatyr_server_reserve" GATE_PORT=port GATE_PORT2=port2 ALLUSERS=1␣
↪REBOOT=ReallySuppress DROPHWID=1 HWIDMODE=HWIDFQDN
```

Примечание: Если параметры указаны и в названии MSI-файла, и в командной строке, приоритет будет у параметров командной строки.

Передача параметров при отложенной установке

Новые параметры можно применять при отложенной установке.

Пример команды, которая сбросит HWID и применит параметр HWID-FQDN после перезагрузки системы:

```
msiexec.exe /i "Agent.msi" /qn /l*vx "install.log" GATE_URL="main.server.url" ALLUSERS=1␣
↪REBOOT=ReallySuppress REINSTALLMODE=amus DROPHWID=1 HWIDMODE=HWIDFQDN AGENT_FORCE_
↪REBOOT=delayed
```

Передача параметров через название MSI-файла

Утилита удаленной установки версии 1.2.0.18 и выше поддерживает передачу параметров HWID через название MSI-файла.

Перед запуском утилиты добавьте в название файла подстроки:

- `drophwid` — удаляет текущий HWID из реестра и генерирует новое значение;
- `hwidmode=hwid`, `hwidmode=hwidfqdn` или `hwidmode=fqdn` — указывает тип HWID.

Правила указания параметров:

- параметры можно указывать в любом порядке и в любом регистре;
- один или оба параметра могут отсутствовать;
- если параметр не указан или указан некорректно, тип идентификатора не изменится, а в логе инсталлятора появится сообщение о некорректном значении;
- сервер берет параметры HWID из названия файла, но игнорирует URL серверов в имени MSI-файла — они берутся из настроек утилиты.

Пример названия файла, которое заменит старый HWID на HWID-FQDN:

```
Agent[main.server.url{reserve.server.url}]-drophwid-hwidmode=hwidfqdn.msi
```

где знак «минус» (-) — разделительный символ.

Предупреждение: Не используйте переименованный MSI-файл для операции Repair, если у него тот же Product Code. Операция завершится с ошибкой, потому что Windows Installer не сможет найти правильный установочный файл по исходному имени.

Repair (Восстановление) — это функция Windows Installer, которая позволяет восстановить или исправить установленную программу, если она работает некорректно или какие-то файлы были удалены или повреждены.

ProductCode — уникальный идентификатор (GUID) для каждого MSI-пакета, который использует Windows Installer для распознавания и управления установленными программами. Позволяет системе отличать одну версию программы от другой, особенно при обновлении, восстановлении или удалении. Если у разных MSI-пакетов один и тот же ProductCode, Windows считает их одной и той же программой.

3.3.3 Агент для macOS

Возможности macOS-агента

- *Обзор функций*
- *Описание функций*
  - *Перехват файлов через браузер*
  - *Учет активности на сайтах*
  - *Блокировка компьютеров*
  - *Контроль USB*
  - *Перехват документов на печать*

Обзор функций

Кастомизация	Изменение имени и иконки сборки *через техподдержку*.
Установка	Установка и обновление: • универсальный инсталлятор для Intel, M1 и M2, • обновление агента с сервера, • задание резервного сервера.
Мониторинг пользователей	Контроль аутентификации сотрудников: • логирование удаленного и локального входа/выхода из системы, • логирование блокировки и снятия блокировки сессии, • черно-белые списки для исключения пользователей из мониторинга.
Контроль программ	Контроль и блокировка запуска приложений по черно-белому списку.
Учет активности	Контроль пользовательской активности пользователя: • учет активного времени в приложении, • *учет активности на сайтах через сетевой перехват*, • *учет активности через перехват истории браузеров*.
Снимки экрана	Создание скриншотов: • с заданным интервалом времени, • по переключению окна или смене его заголовка, • сжатие для экономии места.
Клавиатура и буфер обмена	Перехват информации: • *ввод с клавиатуры (кейлоггер)*, • системные клавиши, • текст, изображения и файлы из буфера.
Интернет	Анализ данных сетевой активности: • перехват запросов в поисковиках, • запись посещений сайтов.
Почта и мессенджеры	*Контроль переписок и загрузок* на основе: • активности пользователя; • снимков экрана; • кейлоггера. Перехват переписки: • мессенджеры: WhatsApp, Telegram, Skype, MS Teams, VK Teams, Bitrix 24; • веб-почта и почтовые приложения: Яндекс Почта, VK Mail, Google Mail, Outlook и др.
Файлы	Перехват файловых операций: • пользователя, • фоновых процессов приложений. Контроль файлов: • теневые копии файлов при копировании на

Описание функций

Перехват файлов через браузер

Начиная с версии iBatyr Monitor 5.3 для macOS-агентов доступен перехват загрузок файлов в браузере.

Чтобы активировать перехват:

1. В разделе **Панель управления** → **Конфигурации компьютеров** выберите конфигурацию.
2. В разделе конфигурации **Файлы** активируйте опцию **Файловая активность** и задайте **Размер файла для теневого копирования**.
3. В разделе конфигурации **Интернет** активируйте опцию **История браузеров**.
4. Готово!

После активации:

- если браузер был установлен раньше агента, требуется перезагрузка для начала перехвата загрузок;
- если браузер установлен позже агента, агент создаст теневые копии *всех* файлов из истории загрузок браузера.

Примечание: Агент перехватывает файлы только из истории загрузок. Файлы могут быть скачаны пользователем в обход загрузки, в этом случае агент не делает теневую копию.

Учет активности на сайтах

Агент позволяет отслеживать посещения сайтов и поисковые запросы.

Посещение сайтов

С версии 5.5 учет активности на сайтах возможен через перехват сетевых подключений.

Чтобы включить мониторинг посещения сайтов:

1. Перейдите **Панель управления** → **Конфигурации компьютеров** и выберите конфигурацию.
2. В боковом меню выберите **Интернет** и включите **Веб-трафик**.

После этого агент будет отправлять событие **Посещение сайтов** с данными:

- имя пользователя,
- время активности,
- название браузера,
- адрес сайта, включая URL, Домен, Полный домен.

Чтобы посмотреть посещения сайтов в отчете по активности:

1. В **Конструкторе** выберите **Тип события** → **Время активности**.
2. В верхней панели в левой части экрана установите временной период.
3. В правой части экрана нажмите **Отчет** → **Подробный отчет по активности**.

4. В **Линзе событий** появится отчет со списком событий **Посещение сайтов**.

Поисковые запросы

Поисковые запросы фиксируются через историю браузеров.

Агент отслеживает активность пользователя в браузерах:

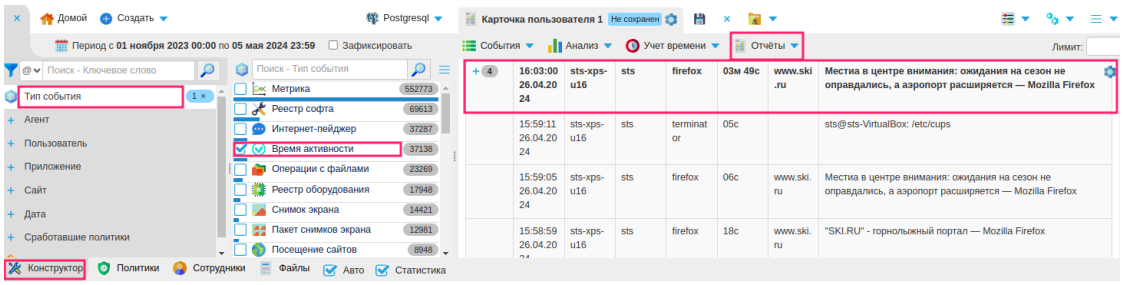
- Safari,
- Google Chrome,
- Яндекс.Браузер,
- Mozilla Firefox,
- Opera,
- Vivaldi.

Чтобы отслеживать поисковые запросы:

1. Перейдите **Панель управления** → **Конфигурации компьютеров** и выберите конфигурацию.
2. В боковом меню выберите **Учет активности** и включите **Активность приложений** для учета активности в приложениях.
3. В разделе **Интернет** включите **Историю браузера** для перехвата адресов сайтов.

Чтобы составить отчет на основе поисковых запросов в истории браузеров:

1. В **Конструкторе** выберите **Тип события** → **Время активности**.
2. В верхней панели в левой части экрана установите временной период.
3. В правой части экрана нажмите **Отчет** → **Подробный отчет по активности**.
4. В **Линзе событий** появится отчет со списком событий **Время активности**. Найдите в нем события посещения сайтов.



В результате создается событие **Время активности**, которое содержит:

- имя пользователя,
- время активности,
- название браузера,
- адрес сайта, включая URL, Домен, Полный домен.

Контроль почты и месседжеров

Контроль почты и мессенджеров возможен благодаря снимкам экрана, кейлоггеру и учету активности. Эти инструменты обеспечивают комплексный мониторинг.

Чтобы включить контроль:

1. Перейдите **Панель управления** → **Конфигурации компьютеров** и выберите конфигурацию.
2. Выберите в боковой панели **Снимки экрана**.
   - *Настройте снимки экрана.*
3. Выберите в боковой панели **Клавиатура и буфер обмена**.
   - *Настройте кейлоггер.*
4. Выберите в боковой панели **Учет активности**.
   - *Настройте учет активности.*

После настройки в *Линзе событий* появятся события. Проведите комплексный анализ событий:

- *Время активности* — проанализируйте время активности в почте и мессенджерах. Найдите другие события пользователя, которые происходили в это же время.
- *Снимок* — просмотрите снимки экрана, чтобы увидеть активные приложения, открытые окна и необычные действия пользователей.
- *Кейлоггер* — изучите записи кейлоггера, чтобы найти все текстовые данные, которые ввел пользователь. Обратите внимание на сообщения в почтовых клиентах и мессенджерах.

Таким образом вы сможете выявить несанкционированные действия пользователя в почтовых приложениях и мессенджерах.

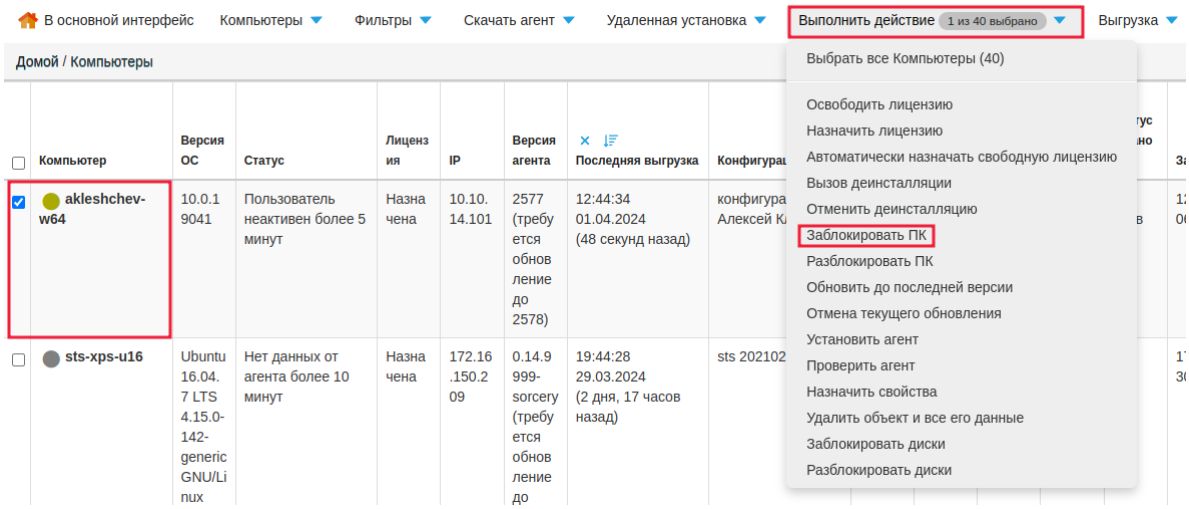
Блокировка компьютеров

Добавлено с версии 5.4

Функция позволяет заблокировать текущего пользователя. При активной блокировке автоматически отклоняет попытки входа.

Чтобы активировать блокировку:

1. Перейдите **Панель управления** → **Компьютеры**.
2. Поставьте флажок напротив компьютера для блокировки.
3. Выберите во вкладке **Выполнить действие** опцию **Заблокировать ПК**.



4. Готово!

После активации блокировки пользователь выйдет из системы, а на экране компьютера отобразится окно входа.

Чтобы отключить блокировку:

1. В **Панели управления** → **Компьютеры** поставьте флажок напротив заблокированного компьютера.
2. Перейдите в **Выполнить действия**.
3. Нажмите **Разблокировать ПК**.

Контроль USB

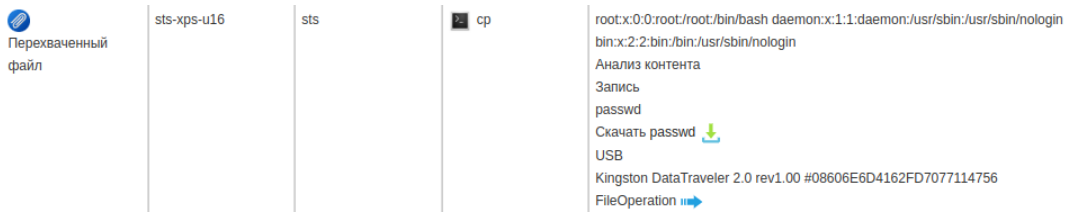
С версии 5.4 iBatyr Monitor позволяет контролировать устройства USB.

Если функция включена, то при использовании USB-устройств агент создает события:

- *Внешние диски* — при включении/отключении USB-устройства;

- **Операции с файлами** — при изменении, копировании, удалении и других операциях с файлами на USB-устройствах;

- **Перехваченный файл** — при копировании файлов на USB-устройство;

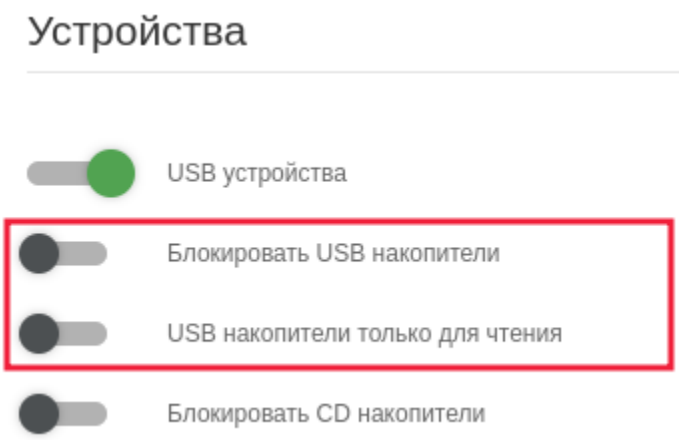


Примечание: Для теневого копирования перехваченного файла включите *Теневое копирование* в **Конфигурации компьютера** → **Файлы**.

Чтобы включить контроль USB:

1. Перейдите **Админ** → **Конфигурации компьютеров**.
2. Выберите **Устройства**.
3. Сдвиньте переключатель **USB устройства**.

Для блокировки всех USB-устройств или доступа только для чтения активируйте соответствующие переключатели:

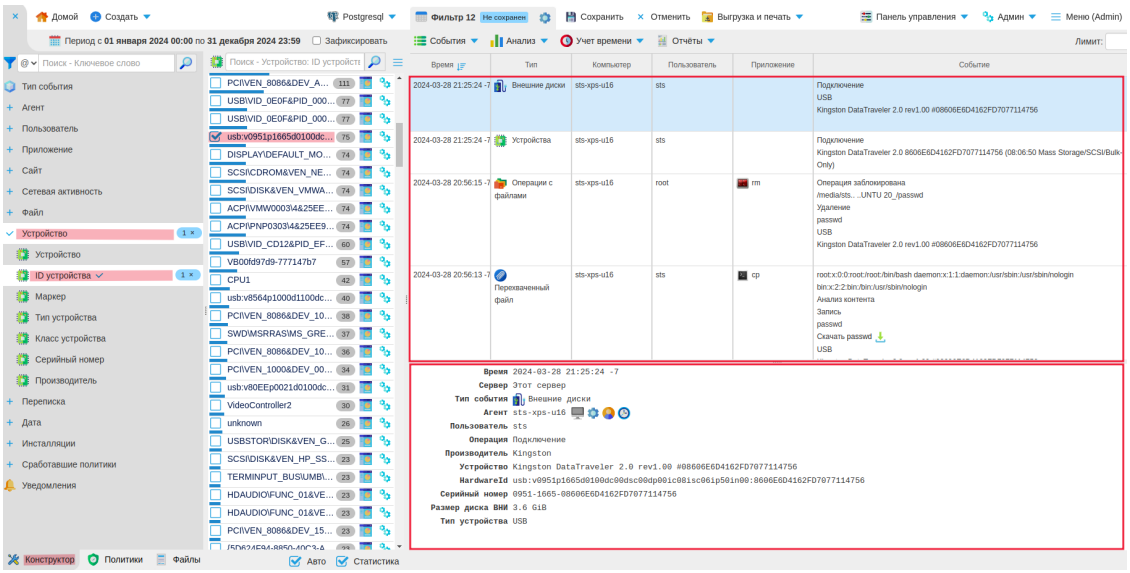


Управление блокировкой накопителей происходит на основе *черных и белых списков*.

Примечание: По черно-белым спискам блокируются только USB-накопители.

Чтобы посмотреть связанное с устройством событие:

1. Выберите в **Конструкторе событий** измерение **Устройство**.
2. Выберите **ID-устройства**
3. Выберите устройство для отображения событий.



Перехват документов на печать

С версии 5.5 агент перехватывает документы, отправленные на печать.

Примечание: Перехват печати доступен только для CUPS (Common Unix Printing System) – стандартной системы печати в macOS.

Чтобы включить перехват документов на печать:

1. Перейдите **Админ** → **Конфигурации компьютеров**.
2. Выберите в боковой панели **Файлы** и активируйте **Теневое копирование**.
3. Выберите **Принтеры** и активируйте **Печать на принтере**.

После этого в момент перехвата агент создает два события: **Перехваченный файл** и **Печать документа**.

Событие **Печать документа** содержит измерения:

- агент,
- пользователь,
- приложение,
- файл,
- количество страниц,
- содержимое.

Событие **Перехваченный файл** содержит:

- информацию о печати,
- теневую копию документа,
- копию файла с распечатанной информацией,
- снимок экрана в момент печати.

Установка macOS-агента

- *Установка*
- *Установка агента из pkg-дистрибутива*
  - *Установка через MDM*
- *Удаление*

Перед установкой ознакомьтесь *с требованиями к рабочей станции*.

Установка

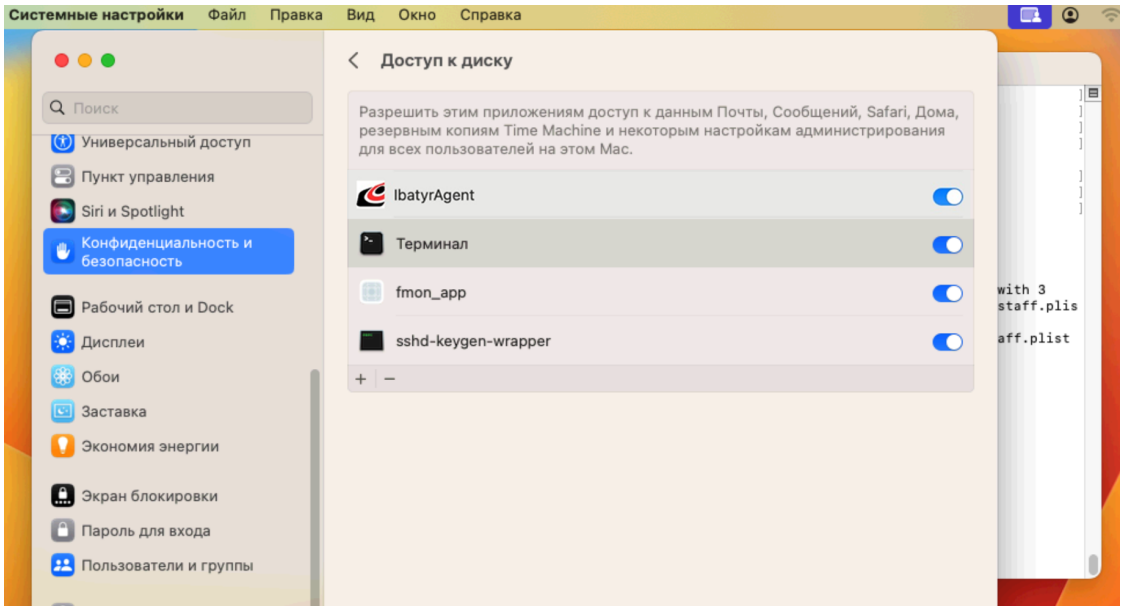
1. Скачайте агент:

- через веб-интерфейс сервера,
- по ссылке.

2. Выдайте разрешение на доступ к жёсткому диску для запуска скрипта-установщика.

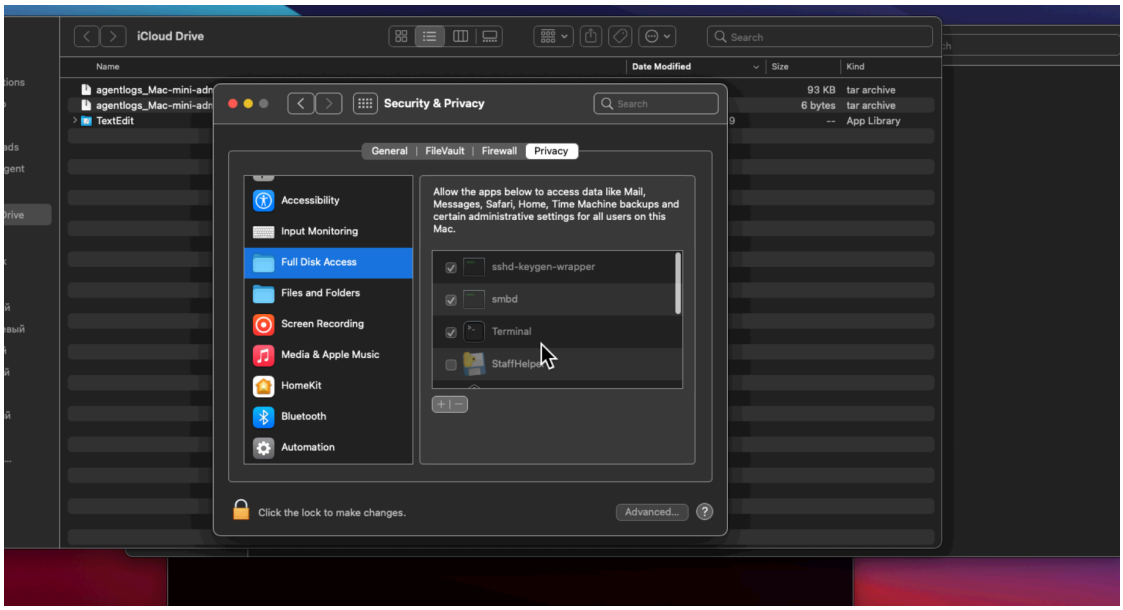
Ventura

Для .ibatyrAgent, Терминала, fmon_app, sshd-keygen-wrapper:



Monterey

Для .ibatyrAgent, Терминала, smbd:



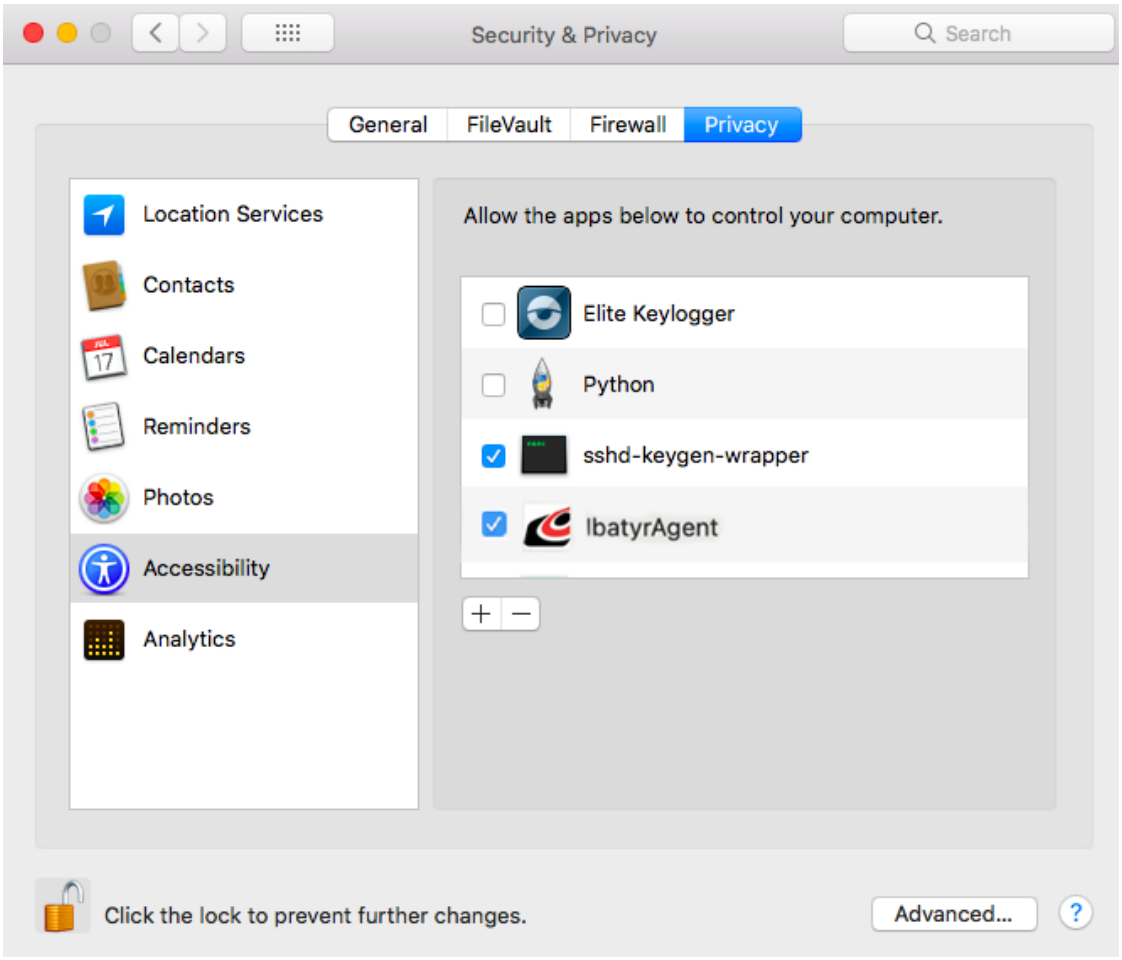
3. Разместите установочный файл на машине, действия которой будут отслеживаться.

   Для этого в терминале из папки с агентом выполните команду:

```
sudo bash ./agent-macos.sh 10.0.0.1
```

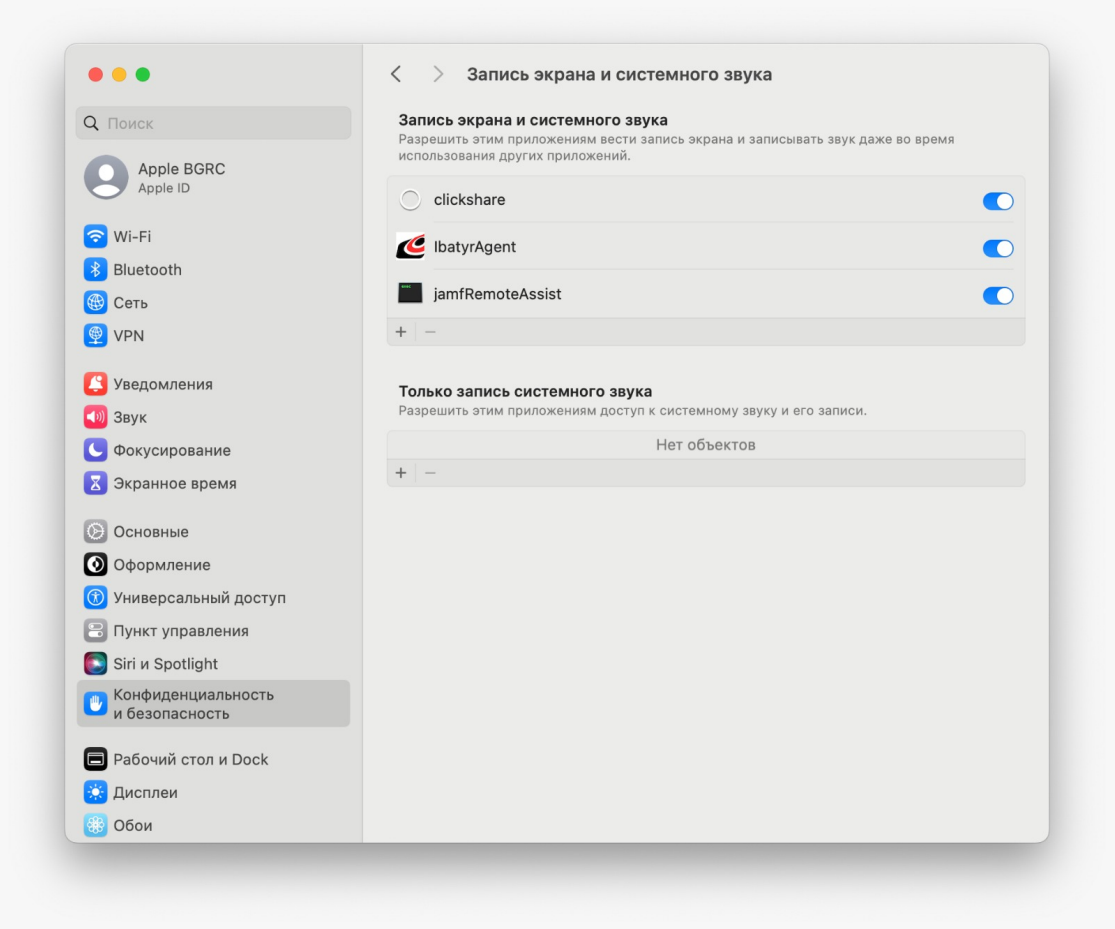
   Вместо **10.0.0.1** укажите IP-адрес своего сервера iBatyr Monitor.

   В появившемся окне «ibatyrAgent нуждается в accessibility» выдайте права агенту:



4. Предоставьте разрешение **Terminal** для установки агента:

В некоторых версиях macOS необходимо выдать права на **Запись экрана**:



5. Для контроля *файловых операций* разрешите доступ к диску для приложения */Library/Application Support/.AtomSec/fmon_app*.

Установка агента из pkg-дистрибутива

1. Скачайте pkg-дистрибутив

Примечание: Если в имени дистрибутива не указан адрес сервера iBatyr Monitor, на который будут отправляться данные, укажите его.

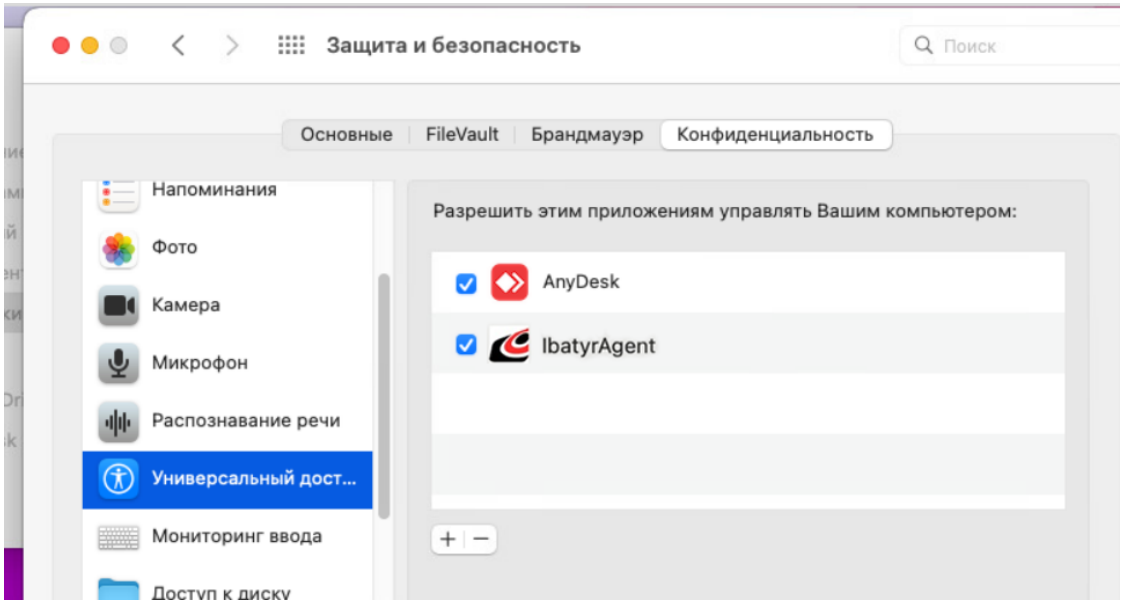
Приведите имя файла к виду **agent-macos[server_address].pkg**. Здесь вместо **server_address** укажите IP-адрес своего сервера iBatyr Monitor.

---

2. Запустите файл.

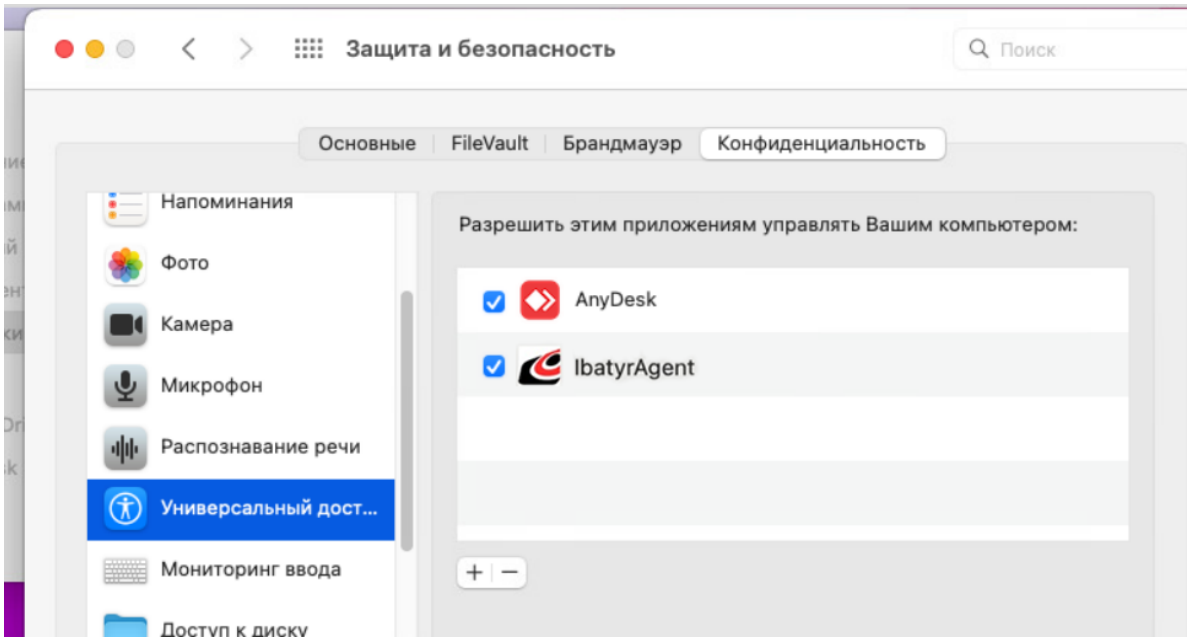
3. Выполняйте указания мастера установки.
4. При запросе введите логин и пароль администратора системы.
5. Предоставьте системе все необходимые разрешения.

Примечание: Для контроля *файловых операций* разрешите доступ к диску для приложения */Library/Application Support/.AtomSec/fmon_app*.



После завершения установки:

- проверьте на всех вкладках, что предоставлены все необходимые разрешения:



- в веб-интерфейсе сервера iBatyr Monitor в **Алертах** и в разделе **Панель управления** — **Компьютеры** появится информация об установленном агенте.

Установка через MDM

При установке агента через стандартный MDM Apple изменить настройки pkg-пакета напрямую или через название файла нельзя. Чтобы передать параметры, добавьте postinstall-скрипт в манифест установки.

Пример команд для настройки агента:

```
# Путь к исполняемому файлу агента
EXE="/Library/Application Support/.AtomSec/StaffAgent.app/Contents/MacOS/StaffAgent"

# Переустановка компонентов агента:
# демоны, plist-файлы, PAM-модуль, служебные файлы
"$EXE" reinit

# Указание основного сервера
"$EXE" set_server <host> <port>

# Добавление резервного сервера
"$EXE" add_servers <host> <port>

# Перезапуск служб агента
"$EXE" restart
```

Дополнительные команды:

```
# Путь к исполняемому файлу агента
EXE="/Library/Application Support/.AtomSec/StaffAgent.app/Contents/MacOS/StaffAgent"

# Полное удаление агента
"$EXE" uninstall

# Управление PAM-модулем (отвечает за блокировку входа в систему)
"$EXE" install_pam        # Установить PAM-модуль
"$EXE" uninstall_pam      # Удалить PAM-модуль
"$EXE" remove_pam         # Альтернативная команда для удаления PAM-модуля

# Управление службами агента
"$EXE" start              # Запустить службы агента
"$EXE" stop               # Остановить службы агента
```

Справка по всем доступным командам:

```
"/Library/Application Support/.AtomSec/StaffAgent.app/Contents/MacOS/StaffAgent" help
```

Удаление

Чтобы удалить агент, выполните команду:

```
bash ./agent-macos.sh uninstall
```

См.также:

Проблема пустых скриншотов после удаления агента.

Логи агента

```
cat /Library/Caches/com.atomsec.ibatyr/ibatyr.log
cat /Library/Caches/com.atomsec.ibatyr/staff_filemon.log
cat /tmp/ibatyr.err.log
cat /var/log/system.log | grep com.atomsec.ibatyr
```

Задание резервного сервера

macOS-агенту можно задать один или несколько резервных серверов для передачи событий или обновления самого агента.

Задать резервные серверы можно двумя способами:

1. Через терминал:

   ```
   sudo /Library/Application\ Support/.AtomSec/StaffAgent.app/Contents/MacOS/
   ↪StaffAgent add_servers 1.1.1.1 555 https://2.2.2.2:888
   ```

   Здесь приведён пример добавления двух резервных серверов: 1.1.1.1 с портом связи 555 и 2.2.2.2 с портом 888.

   После добавления новых серверов перезапустите агент, чтобы обновлённая конфигурация вступила в силу:

   ```
   sudo /Library/Application\ Support/.AtomSec/StaffAgent.app/Contents/MacOS/
   ↪StaffAgent restart
   ```

2. Вручную в конфигурационном файле:

   2.1 Откройте конфигурационный файл **/Library/Caches/com.atomsec.ibatyr/config**.

   2.2 Добавьте адрес нового сервера и порт для подключения к нему в формате:

   ```
   server2 = 1.1.1.1
   port2 = 555
   ```

При недоступности основного сервера агент автоматически переключится на резервный. Если недоступен первый резервный сервер, агент переключится на следующий, указанный в списке.

Чтобы изменить сервер для передачи данных от агента, используйте команду:

```
sudo /Library/Application\ Support/.AtomSec/StaffAgent.app/Contents/MacOS/StaffAgent set_
↪server 1.1.1.1 555
```

Создание резервного сервера

macOS-агенту можно задать один или несколько резервных серверов для передачи событий или обновления самого агента.

При недоступности основного сервера агент автоматически переключится на резервный. В случае, если недоступен первый резервный сервер, агент переключится на следующий, указанный в списке.

Задать резервные серверы можно двумя способами:

1. Через терминал:

```
sudo /Library/Application\ Support/.AtomSec/StaffAgent.app/Contents/MacOS/
↪StaffAgent add_servers 1.1.1.1 555 https://2.2.2.2:888
```

   Здесь приведён пример добавления двух резервных серверов: 1.1.1.1 с портом связи 555 и 2.2.2.2 с портом 888.

   После добавления новых серверов перезапустите агент, чтобы обновлённая конфигурация вступила в силу:

```
sudo /Library/Application\ Support/.AtomSec/StaffAgent.app/Contents/MacOS/
↪StaffAgent restart
```

2. Вручную в конфигурационном файле:

   2.1 Откройте конфигурационный файл */Library/Caches/com.atomsec.ibatyr/config*.

   2.2 Добавьте адрес нового сервера и порт для подключения к нему в формате:

```
server2 = 1.1.1.1
port2 = 555
```

Чтобы указать в качестве основного ранее добавленный сервер 1.1.1.1 с портом связи 555, используйте команду:

```
sudo /Library/Application\ Support/.AtomSec/StaffAgent.app/Contents/MacOS/StaffAgent 1.1.
↪1.1 555 restart
```

Командная строка

Путь к папке

Перед выполнением убедитесь, что вы находитесь в папке агента или используйте в команде путь к папке:

```
sudo /Library/Application\ Support/.AtomSec/StaffAgent.app/Contents/MacOS/StaffAgent␣
↪[команда]
```

Команды

Запуск

```
sudo start
```

Проверка текущего состояния работы агента

```
sudo status
```

Остановка агента

```
sudo stop
```

Вывод запросов, которые обрабатывает агент

```
sudo prof
```

Создание архива с логами

```
sudo zip
```

Перезапуск агента

```
sudo restart
```

Просмотр логов

```
sudo log
```

Последние 10 строк логов

```
sudo tail
```

Удаление агента

```
sudo uninstall
```

Добавление резервного сервера

```
sudo add_servers 1.1.1.1 555
```

Указание сервера для передачи данных

```
sudo set_server 1.1.1.1 555
```

3.3.4 Агент для Linux

Установка агента

- *Возможности Linux-агента*
- *Установка*
- *Дополнительный адрес сервера*
- *Обновление*
- *Удаление*

Возможности Linux-агента

Linux-агент поддерживает:

- управление агентом через конфигурацию в веб-консоли iBatyr Monitor;
- создание скриншотов:
  - с заданным интервалом времени;
  - в зависимости от активности пользователя (по переключению окна или смене заголовка окна);
  - *по заданным условиям*;
- изменение формата и степени сжатия скриншотов;
- атрибуты приложений - имена окон и иконки;
- учёт времени работы в приложениях;
- кейлоггер (X11 и низкоуровневый);
- учёт подключения USB-устройств;
- возможность блокировки USB-устройств (создание белых и чёрных списков);
- события локального или удалённого входа и выхода из системы (включая ssh подключения);
- запись истории ввода команд shell (bash, zsh);

- перехват печати на принтере (CUPS);
- удаленное управление;
- запись видео рабочего стола;
- запись истории и времени посещений сайтов в Firefox, Chrome и Vivaldi;
- отслеживание содержимого буфера обмена;
- функции управления агентом в командной строке;
- отслежвание системных логов и управление правилами мониторинга через конфиг агента;
- с подключенных микрофонов;
- модуль перехвата снимков с ;
- файловые операции: определение действий с файлами, поддержка правил мониторинга (черный и белый списки контроля);
- создание теневых копий файлов при перехвате файловых операций;
- возможность блокировки сайтов;
- перехват shell-сессий в виде текста или gif-файла;
- поддержка SNAP-пакетов браузеров;
- каналы перехвата:
  - почтовые клиенты Thunderbird, Akonadi, Evolution, Geary, Р7-Офис.Органайзер;
  - Telegram (десктоп-приложение);
  - VK mail (чаты и файлы);
  - VK Teams (чаты и файлы);
  - bitrix (чаты и файлы в веб- и десктоп-приложении);
  - Nextcloud и Owncloud (скачиваемые и загружаемые файлы);
  - One Drive (скачиваемые и загружаемые файлы);
  - Yandex Disk (скачиваемые и загружаемые файлы);
- DLP-модуль;
- файловый сканер;
- поддержка STARTTLS;
- сетевой перехват:
  - исходящих сессий tcp и ssl/tls;
  - отправки почты SMTP;
  - почты IMAP;
  - почты POP3;
  - POST-запросы.
- отслеживание портов, в том числе нестандартных;
- настройка правил по мониторингу портов;

- пакет распространения для менеджера пакетов Portage в Gentoo.

Установка

Предупреждение: Для полноценной работы агента отключите SELinux.

1. Скачайте скрипт для установки агента: в разделе **Панель управления** → **Компьютеры** → **Скачать агент** выберите версию для Linux. При скачивании, к имени скрипта автоматически добавится IP-адрес машины, на которую он скачивается (как правило, адрес сервера).
2. Скопируйте скрипт на целевую машину:

```
wget http://10.10.0.1/agent-install-[10.10.0.1].sh
```

   Здесь **10.10.0.1** - пример IP-адреса сервера.

3. Запустите установщик:

```
sudo bash /path/to/agent-install-[10.10.0.1].sh 10.10.0.1
```

   Здесь **/path/to/agent-install-[10.10.0.1].sh** — полный путь к скрипту и его имя; **10.10.0.1** — IP-адрес сервера iBatyr Monitor, куда будет передавать данные устанавливаемый агент.

Примечание: По умолчанию, для связи агента с сервером используется порт **443**. Его можно не указывать в команде установки агента. Если порт связи агента с севером *был изменён*, укажите его в команде установки агента:

```
sudo bash /path/to/agent-install-[10.10.0.1].sh 10.10.0.1 new_port
```

Здесь **new_port** — новый номер порта.

После установки агента, перезагрузите машину.

Дополнительный адрес сервера

Начиная с версии агента *0.8.0-master* для передачи событий можно указать один или несколько дополнительных серверов, которые будут использоваться, если основной сервер окажется недоступен.

Чтобы указать дополнительный сервер:

1. Откройте файл scela

```
sudo nano /etc/scelarc
```

2. Добавьте адрес и порт резервного сервера после строки **server**:

```
server2 = 192.168.0.3
port2 = 4334
```

Если не указать номер порта, по умолчанию будет использован **443**.

Обновление

Начиная с версии *0.7.46*, Linux-агент поддерживает функцию обновления до новой версии по команде с сервера.

Чтобы обновить агент:

1. В разделе **Панель управления** → **Компьютеры** выберите нужный компьютер.
2. В пункте меню **Выполнить действие** выберите **Обновить до последней версии**.

Агент обновится до последней, находящейся на сервере, версии.

Удаление

Удалить агента можно несколькими способами:

- на машине, на которой он установлен, выполнить команду:

```
sudo /usr/share/ibatyr/agent uninstall
```

- на машине, на которой он установлен, обратиться к установщику:

```
sudo bash agent-install.sh uninstall
```

- в веб-интерфейсе сервера iBatyr Monitor в разделе **Панель управления** → **Компьютеры**.

Настройка агента

Перехват печати

Для перехвата печати:

1. Перейдите **Панель управления** → **Конфигурации компьютеров** → *ваша конфигурация*.
2. В боковом меню перейдите в раздел **Файлы** и включите **Теневое копирование**.
3. Перейдите в раздел **Принтеры** и включите **Печать на принтерах**.
4. Перейдите в **Назначение агентов** и добавьте компьютер, на котором агент будем перехватывать печать.

Опция **Автоматически настраивать все принтеры на печать через спулер** позволяет перехватывать задания на печать по имени файла. Для полноценной работы этой опции установите **libmagic** — библиотеку для определения Content-Type файлов:

```
sudo apt-get install libmagic-dev
```

После установки библиотеки перезагрузите ПК.

Сетевой перехват почты IMAP4/SMTP

Чтобы настроить перехват почты:

1. В разделе **Панель управления** → **Конфигурации компьютеров** выберите машину, на которой хотите включить перехват.
2. В открывшемся окне с настройками в разделе **Сетевые подключения** включите опцию **Мониторинг сети**.
3. В разделе **Почта и мессенджеры** выберите **Электронная почта**.

Примечание: Для версий агента *0.11.0-master* и выше, добавлена поддержка совместной работы с AppArmor. Для версий ниже *0.11.0-master* отключите AppArmor на рабочей станции с агентом:

```
sudo systemctl disable apparmor
```

Для перехвата вложений, дополнительно включите **Файлы** → **Теневое копирование** и укажите размер файлов в окне **Выполнять теневые копии для файлов не более:**.

Перехват писем в локальных клиентах

Отслеживание почты и перехват вложений доступны для Thunderbird, Evolution, Geary и клиентов, завязанных на фреймворке Akonadi (Kmail, Gmail. . .). Для клиентов на Akonadi имя приложения для события указано как Akonadi.

Для перехвата почты и вложений:

1. В разделе **Панель управления** → **Конфигурации компьютеров** выберите конфигурацию целевой машины.
2. В пункте **Почта и мессенджеры** включите опцию **Электронная почта MAPI**.
3. В пункте **Файлы** включите опции **Файловая активность** и **Теневое копирование**.
4. В окне **Выполнять теневые копии для файлов не более** укажите максимальный размер файла для теневого копирования.

Файловая активность

Для отслеживания файловых операций и создания теневых копий файлов включите соответствующие правила в конфигурации компьютера в *разделе Файлы*.

Примечание: В ОС Linux копирование и перемещение файлов – разные процессы. Для правильного мониторинга файловых операций нужно отслеживать все процессы: создание копии, запись данных, удаление оригинала. По этой причине Linux-агент при фиксации файловых операций создает два события:

---

tabularytabulary

	Операция	События
	Копирование	Копирование, Запись
	Перемещение	Копирование, Перемещение

Перехват портов

Начиная с версии 5.6 агент iBatyr Monitor поддерживает перехват данных через любые порты, включая нестандартные. Функциональность позволяет мониторить сетевой трафик, даже если стандартные порты заблокированы.

Данные передаются на сервер в виде события **Сеть**.

Пример: антивирус блокирует стандартные порты 80 и 443, что не позволяет агенту мониторить трафик. В таких случаях можно настроить прокси-сервер. Прокси будет перенаправлять трафик через нестандартный порт — например, 3128. Агент продолжит мониторинг трафика, несмотря на блокировку стандартных портов.

Чтобы агент мониторил порт 3128:

1. Перейдите **Панель управления** → **Конфигурации компьютеров** и выберите конфигурацию агента.
2. В модуле **Мониторинг сетей** включите **Сетевые подключения**.
3. В разделе **Порты**:

- в поле **Разрешить** укажите порт **3128** для перехвата;
- поле **Запретить** оставьте без изменений.

4. Нажмите **Сохранить**.

После сохранения настроек агент начнёт перехватывать трафик в соответствии с заданным условием.

Команды для работы

Ниже приведены основные команды для управления агентом через терминал.

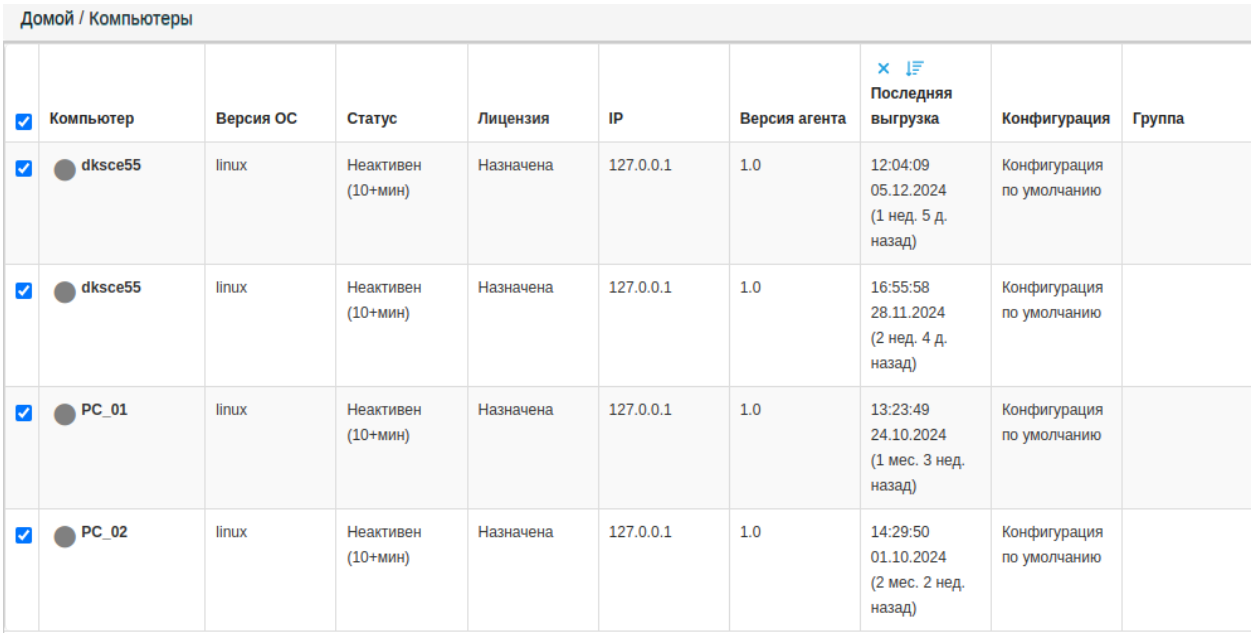
3.3.5 Обновление агентов

Примечание: С версии агента 5.8.2569 изменилась схема установки агента. При обновлении более ранних версий сначала удалите агент и сервис мониторинга, иначе обновление будет невозможно. После этого перезагрузите компьютер и установите агент любым способом.

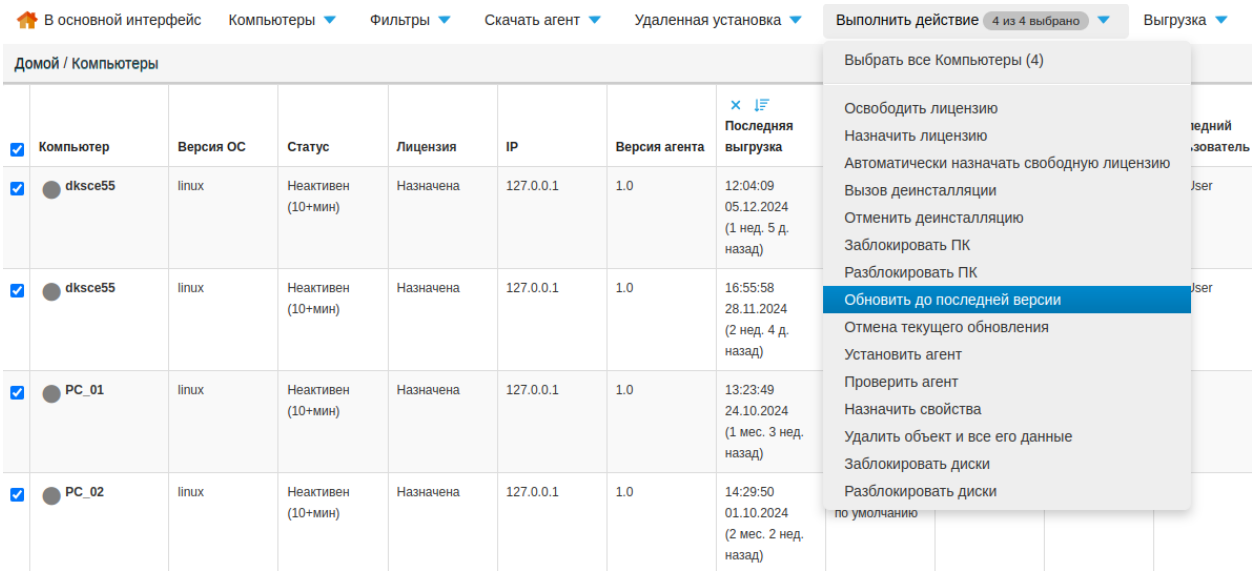
Обновление через веб-интерфейс

Чтобы обновить агенты через веб-интерфейс:

1. В раздел **Панель управления** → **Компьютеры** выберите машины.



2. В меню **Выполнить действие** выберите пункт **Обновить до последней версии**.



После запуска обновления статус в столбце **Действие** будет изменён на **Обновление агента**, а в столбце **Статус действия** будет отображаться процесс обновления.

Примечание: Если по какой-то причине в процессе обновления произойдёт ошибка, повторная попытка обновить агент произойдёт автоматически.

В случае повторения ошибки обновления в столбце появится соответствующий статус.

Обновление через сервис удаленной установки агентов

Для обновления определённых агентов или обновления агентов без перезагрузки используйте *удалённую установку агентов*.

Агенты старых версий будут подсвечены желтым цветом.

После установки обязательно перезагрузите компьютер с установленным агентом.

Предупреждение: Если перезагрузка сразу после установки невозможна, во время установки выберите опцию **Отложенная установка**. В этом случае будет создана задача в планировщике задач, которая выполнит установку агента при следующей перезагрузке компьютера.

Обновление агентов через групповые политики

Обновление всех агентов в домене с помощью групповых политик описано *в статье*.

Предупреждение: Если вы устанавливали агенты через групповые политики, производите обновление только через групповые политики.

3.3.6 Логи агента

С версии 5.6 агент автоматически собирает логи с рабочих станций и передает их на сервер по запросу администратора.

Автоматическая система логирования:

- позволяет получать данные без удаленного подключения к рабочей станции или изменения конфигурации;
- предотвращает случайное отключение сбора логов.

Сбор логов происходит локально на компьютерах в постоянном режиме. Чтобы загрузить логи на сервер:

1. Перейдите **Панель управления** → **Компьютеры**.
2. Выберите все или отдельные компьютеры для сбора логов.
3. Перейдите в меню **Выполнить действие**.
4. Нажмите **Загрузить логи**.

Агент передаст все собранные логи в событии **Системный лог**. Объем данных зависит от количества записей, сделанных до запроса.

Примечание: Если компьютер был недоступен в момент запроса, логи передаются при следующем подключении к сети.

Агенты всех операционных систем передают основные логи:

- работы агента,
- конфигурации агента,

- предыдущей конфигурации агента,
- системных сведений,
- проверки антивируса.

В **Windows-агента** реализованы дополнительные журналы, которые предоставляют информацию о диагностике, сетевой активности, системных службах, действиях пользователей и запущенных процессах. Расширенные логи позволяют выявлять проблемные настройки и возможные конфликты с другим ПО.

Локальный лог агента

Может потребоваться в случае нетипичного поведения агента на компьютере. Место расположения логов для версии агента **2555** и ниже:

64-разрядная система

C:\Windows\SysWOW64\TimeControlSvc\Debug_Agent.log

32-разрядная система

C:\Windows\System32\TimeControlSvc\Debug_Agent.log

Начиная с версии агента **2557** месторасположение логов изменено:

64-разрядная система

C:\Windows\SysWOW64\TimeControlSvc\Logs\Debug_Agent.log

32-разрядная система

C:\Windows\System32\TimeControlSvc\Logs/Debug_Agent.log

Логи удалённого установщика для Windows

Находятся в папке на компьютере, с которого производится установка:

```
C:\Users\Ваш_пользователь\AppData\Local\Temp\Debug_InstallerUI.log
```

На удаленном ПК:

```
C:\Windows\Debug_AuxibatyrSvc.Log
```

Логи конфигурации

Лог конфигурации расположен по адресу:

```
C:\Windows\System32\config\systemprofile\AppData\Roaming\TimeSvc3\cfg.log
```

Логи Linux-агента

Можно получить такой командой:

```
sudo /usr/share/ibatyr/agent zip
```

Логи в виде живого просмотра:

```
sudo /usr/share/ibatyr/agent tail
```

Вывод логов на экран консоли:

```
sudo /usr/share/ibatyr/agent log
```

Логи macOS агента

Логи агента расположены по следующему пути:

```
/Library/Caches/com.atomsec.ibatyr/ibatyr.log
/tmp/ibatyr.err.log
```

Заменить и расширить пути на маски

```
/Library/Caches/com.atomsec.ibatyr/ibatyr.conf
/Library/Caches/com.atomsec.ibatyr/staff_filemon.log*
/Library/Caches/com.atomsec.ibatyr/subtleties.txt
/Library/Caches/com.atomsec.ibatyr/ibatyr.log*
/tmp/ibatyr*.log
```

Пример команды для сбора логов:

```
(sudo tar -Pczf - /Library/Caches/com.atomsec.ibatyr/ibatyr.conf /Library/Caches/com.
↪atomsec.ibatyr/ibatyr*.log* /tmp/ibatyr*.log /Library/Caches/com.atomsec.ibatyr/
↪subtleties.txt) > macos-logs-$(date +"%d-%m-%Y").tar
```

3.3.7 Подключение агента к серверу iBatyr Monitor из внешней сети

В ходе работы регулярно возникают ситуации, когда подконтрольный компьютер оказывается вне локальной сети организации (командировка сотрудника, больничный лист, удалённая работа и т. д.). В этих случаях необходимо настроить агент iBatyr Monitor таким образом, чтобы он продолжал передавать данные на сервер.

Настроить агент на передачу данных из внешней сети можно двумя способами:

- настроить передачу данных через VPN-соединение;
- создать NAT-правило на маршрузтизаторе.

Подключение через VPN-соединение

Для подключения агента к серверу iBatyr Monitor через VPN-соединение, понадобится сервер или маршрутизатор с фиксированным внешним IP-адресом.

1. Установите на выбранный сервер VPN-сервер / Запустите VPN-сервер на маршрутизаторе.
2. Установите на компьютер, который будет работать вне локальной сети, VPN-клиент.
3. Настройте соединение клиента и сервера.
4. Настройте автоматический запуск VPN-клиента при старте операционной системы.

Готово! Никаких дополнительных настроек агента не требуется. При выбраном типе подключения, агент будет передавать данные серверу по VPN-каналу.

Примечание: Для установки и настройки VPN-сервера, обратитесь к своему сетевому или системному администратору.

Настройка NAT-правила на маршрутизаторе

1. На маршрутизаторе, который используется для выхода в сеть, создайте NAT-правило для внешнего источника. Обратитесь для этого к своему сетевому или системному администратору.

   Вид правила:

   ```
   [внешний IP-адрес]:[порт] => [локальный IP-адрес сервера iBatyr Monitor]:443
   ```

   здесь **внешний IP-адрес** — статический IP-адрес, предоставленный провайдером, **порт** в данном случае указывайте не стандартный (например 44344).

2. Настройте агенты на компьютерах, которые будут работать вне сети. Для этого при установке агента укажите внешний адрес и порт маршрутизатора в качестве параметров резервного сервера.

   Если агенты уже установлены:

   Windows-агент

   1. Создайте скрипт

      ```
      set var2=XXX.XXX.XXX.XXX:port
      REG ADD HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\
      ↪TimeSvc3\ServiceConfiguration /v Url2 /t REG_EXPAND_SZ /d
      ↪%var2% /f
      C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe stop
      C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe start
      ```

      здесь **XXX.XXX.XXX.XXX:port** — выбранные внешний IP-адрес и порт маршрутизатора.

   2. Запустите скрипт от имени администратора.

Примечание: То же самое можно сделать вручную, изменив значение переменной **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TimeSvc3\ServiceConfiguration\url2**

Укажите в значении переменной IP-адрес и порт маршрутизатора в виде **XXX.XXX.XXX.XXX:port**.

Linux-агент

Настройка Linux-агента описана в разделе Дополнительный адрес сервера.

При задании дополнительного адреса сервера, Linux-агент сам будет определять, находится агент во внутренней или во внешней сети и в зависимости от этого будет выбирать канал передачи данных серверу.

3.4 Сервер распознавания графических объектов

- *Описание и возможности*
- *Установка сервера*
- `Настройка на стороне сервера iBatyr Monitor `_
- *Настройка модуля Анализ контента*
- *Политики распознавания контента*
  - *Анализ контента*
    - *Распознавание текста*
    - ``_
    - *Распознавание печатей*
    - *Распознавание лиц*
- *Логи*
  - *Сервер распознавания*
  - *Сервер iBatyr Monitor*

3.4.1 Описание и возможности

Сервер распознавания устанавливается на отдельную от сервера iBatyr Monitor (виртуальную) машину. В состав сервера входит несколько движков, которые извлекают данные и обнаруживают графические сущности в документах.

Возможности сервера распознавания:

- обнаружение печатей на изображениях по заданному образцу: скан-копии, скриншоты, фотографии документов с оттиском печати;
- распознавание лиц и создание оповещений по результатам распознавания;
- распознавание больших объёмов текста, в том числе текста с любых изображений (скан-копии, скриншоты, фотографии) или из файлов-контейнеров (например, формата pdf или в zip);
- работа с наиболее популярными форматами хранения изображений: png, jpeg, jpg, jpe, pdf.

3.4.2 Установка сервера

Для работы анализатора графических объектов установите дополнительные пакеты:

```
sudo apt update && sudo apt upgrade
sudo apt install software-properties-common

# установите python3.7
sudo add-apt-repository ppa:deadsnakes/ppa
sudo apt install python3.7
sudo apt install python3.7-venv

# установите оставшиеся пакеты
sudo apt install -y libpoppler-cpp0v5 poppler-utils libsm6 tesseract-ocr
```

Добавьте репозиторий iBatyr Monitor в список репозиториев системы и установите сервер распознавания при помощи *apt*:

```
wget -O - https://distr.ibatyr.kz/stable5.06/ibatyr.gpg | sudo apt-key add -
echo "deb https://distr.ibatyr.kz/stable5.06 stable5.06 non-free" | sudo tee /etc/apt/
↪sources.list.d/ibatyr.list
sudo apt update
sudo apt install ibatyr-cpservice
```

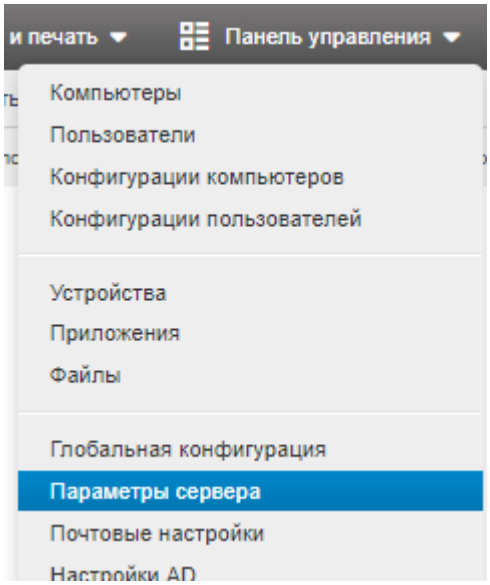
Общий размер пакета около 850 МБ — при низкой скорости доступа в Интернет скачивание может занять длительное время.

На этом установка программного обеспечения завершена.

3.4.3 Настройка на стороне сервера iBatyr Monitor

Перед настройкой модуля **Анализ контента** включите доступ к API сервера в параметрах сервера iBatyr Monitor :

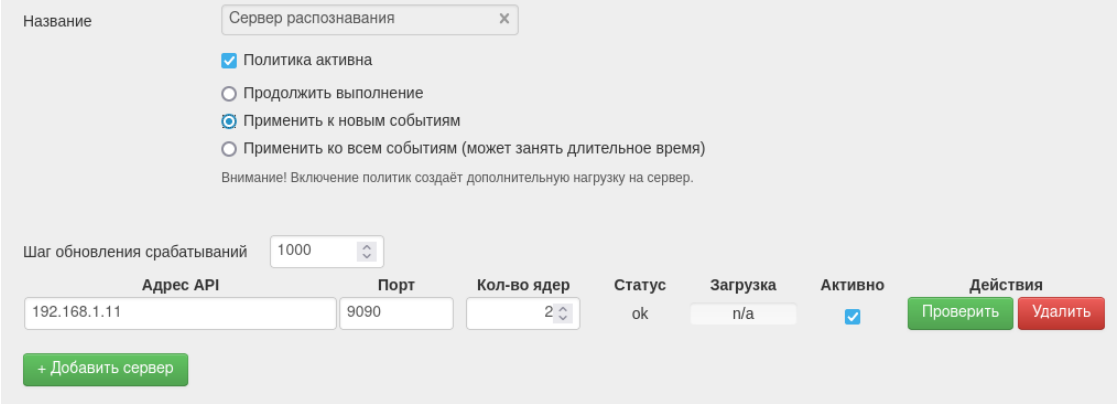
1. Зайдите в основном интерфейсе в **Панель управления** → **Параметры сервера**:



2. Выберите **Доступ к API разрешён**.
3. Поставьте флажок в чекбоксе **Значение** и нажмите **Сохранить**. Значение параметра **Доступ к API разрешён** изменится на **Да**.
4. Во вкладке **Политики** перейдите в **Политики** → **Системные политики** → **Сервер распознавания**.
5. Добавьте в поля данные машины, на которой установлен сервер распознавания:

- **Шаг обновления срабатываний** — количество событий, которое обрабатывает сервер распознавания за один раз. Чем меньше это число, тем чаще будет происходить обновление. Оптимальное значение параметра — **10 000**. Если строка пустая, значение также принимается равным 10 000. Не устанавливайте значения меньше **10 000**, чтобы не увеличивать нагрузку на сервер.
- **Адрес API** — доменное имя или IP-адрес сервера распознавания.
- **Порт** — порт доступа к серверу распознавания. По умолчанию — 9090.
- **Кол-во ядер** — должно соответствовать числу ядер сервера модуля.
- **Статус** — наличие связи с сервером.
- **Загрузка** — нагрузка на сервер распознавания.
- **Активно** — включение/выключение сервера распознавания.

6. Поставьте галочку **Политика активна** и сохраните изменения.



3.4.4 Настройка модуля Анализ контента

Подключитесь к серверу распознавания по SSH. Откройте конфигурационный файл сервера в текстовом редакторе:

```
sudo nano /etc/ibatyr/cpservice-config
```

И укажите параметры:

```
PORT = 9090
SERVER_ADDR = 'http://192.168.1.x'
SECRET = 'xxxxxxxxxxxxxxx'
```

Здесь **PORT** — порт доступа к серверу.
SERVER_ADDR — адрес сервера iBatyr Monitor .

SECRET — значение **ключа API**, указанное в **Параметрах сервера** (см. выше).

Сохраните изменения и перезапустите сервер командой:

```
sudo service ibatyr-cpservice restart
```

Готово! Сервер настроен.

3.4.5 Политики распознавания контента

Настраиваются на сервере iBatyr Monitor в веб-интерфейсе.

Время на обработку изображений:

tabularytabulary

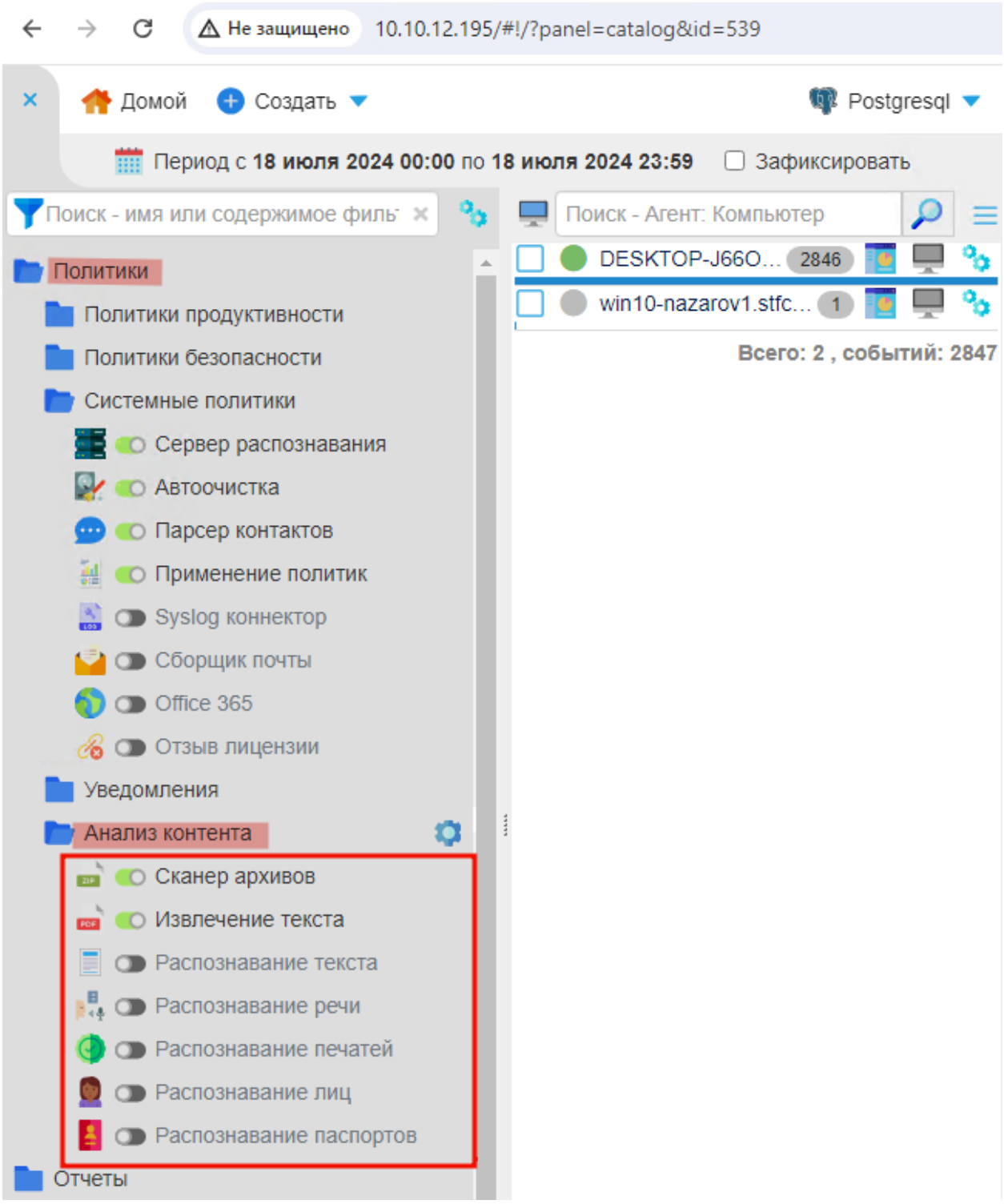
	Форм
	full HD изображ
	изображение печати, паспорта, картинк
	р

Анализ контента

В разделе **Фильтры** перейдите во вкладку **Политики**, далее в папке **Политики** выберите **Анализ контента**.

Сервер распознает:

- текст,
- речь,
- печати,
- лица,

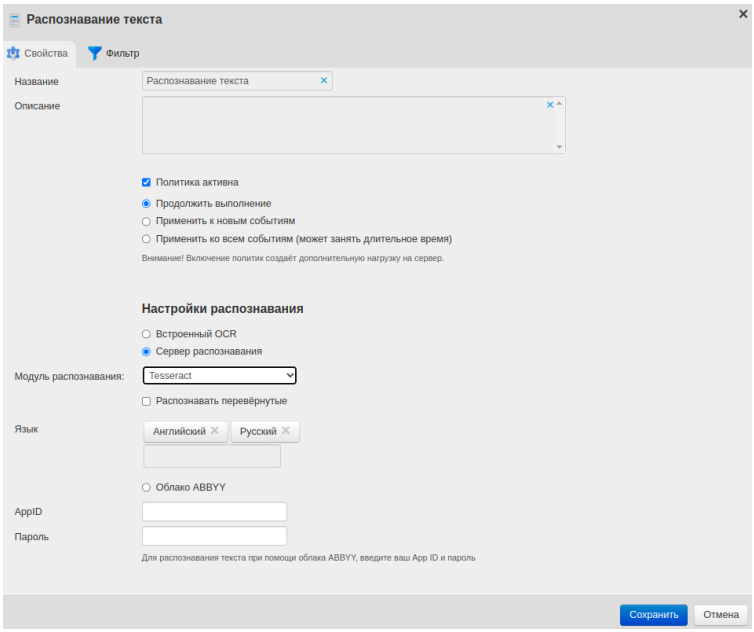


Кроме этого, в **Анализе контента** доступны опции:

- **Извлечение текста** — сохраняет текстовое содержимое из события *Перехаченный файл*.
- **Сканер архивов** — создает событие *Перехваченный файл* из файлов перехваченного архива.

Распознавание текста

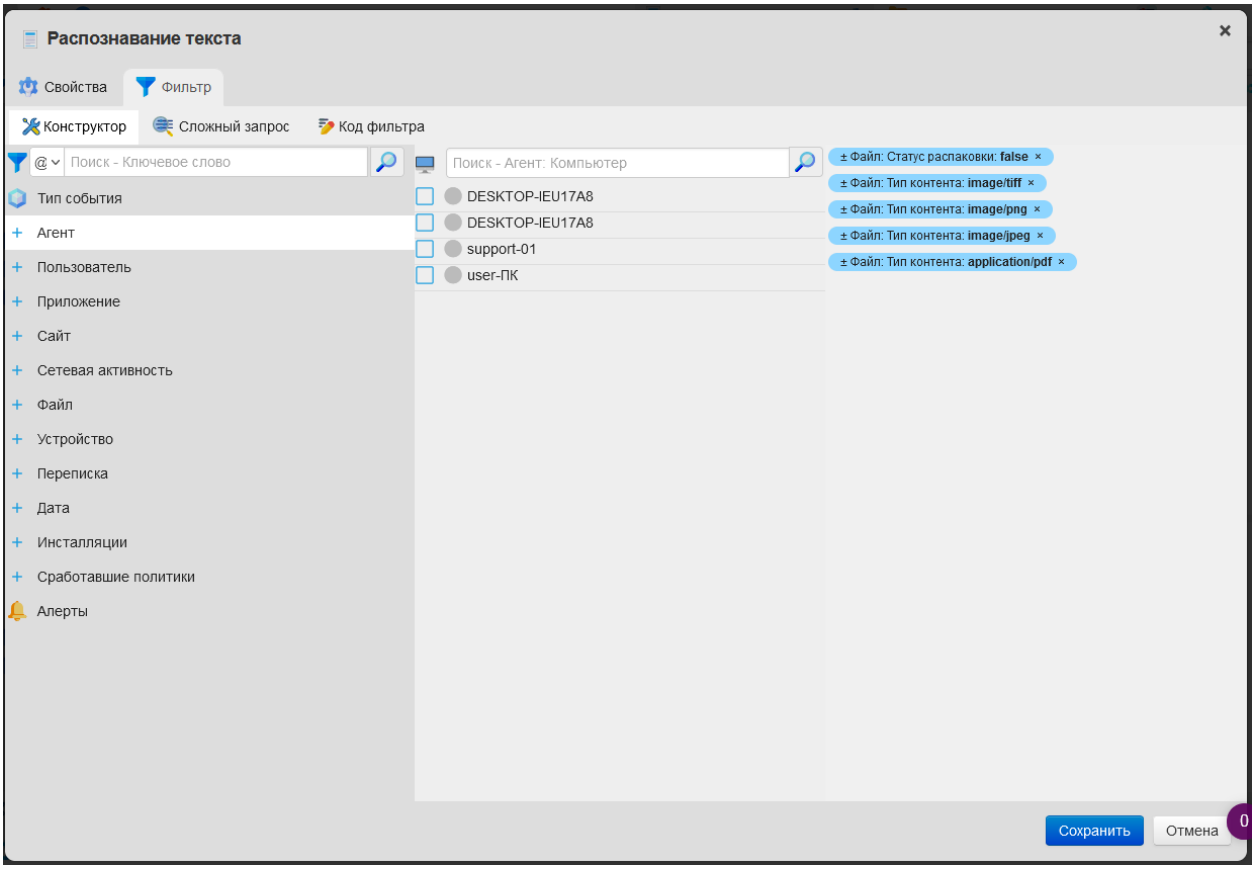
Позволяет распознавать текст на изображениях.



Вкладка **Свойства** содержит настройки распознавания текста:

- **Встроенный OCR / Сервер распознавания** — выбор инструмента распознавания. Кроме сервера распознавания, вы можете использовать встроенный OCR. Подробнее — в статье *Настройка модуля OCR*.
- **Модуль распознавания** — движок для распознавания.
  - *Tesseract*. Бесплатная библиотека для базового OCR, простая и гибкая.
  - *Content AI ABBYY*. Платный движок, требует дополнительных настроек на сервере и платной лицензии с компонентом OCR. Обеспечивает высокую точность, лучше распознает перевернутые изображения.
- **Распознавать перевёрнутые** — распознавание текста на перевёрнутых изображениях. Опция расширяет возможности, но нагружает сервер распознавания.
- **Язык** — языки для распознавания: русский, английский.
- **Облако ABBYY** — если у вас есть аккаунт на облачном сервисе ABBYY, вы можете его подключить. Просто введите свой логин и пароль.

Во вкладке **Фильтр** можно настроить фильтр для политики распознавания текста.



Настроенный по умолчанию фильтр выглядит так:

```
 agent_attachedfile@mime:mime=application/pdf
 agent_attachedfile@mime:mime=image/jpeg
 agent_attachedfile@mime:mime=image/png
 agent_attachedfile@mime:mime=image/tiff
 agent_attachedfile@extracted:extracted=false
 agent_eventtype@default:agent_eventtype=0#Intercepted file

{
 "operator": "AND",
 "rules": []
}
```

Переводит аудиозаписи в текст. Подробнее — в статье :ref:` <speech_to_text>`.

Распознавание печатей

Примечание: На данный момент поддерживается поиск только круглых печатей.

Сервер распознаваний находит изображения печати по заданным образцам в документах формата jpg, jpe, jpeg, png и pdf.

Примечание: На данный момент политику можно создать только одну политику для одной печати. Если у вас несколько печатей, обратитесь *в техподдержку*.

Для работы политики понадобятся образцы печатей — фрагменты изображений, на котором содержится печать. Окружающий текст и подписи не являются помехами для распознавания. Чтобы повысить качество распознавания используйте несколько образцов печати.

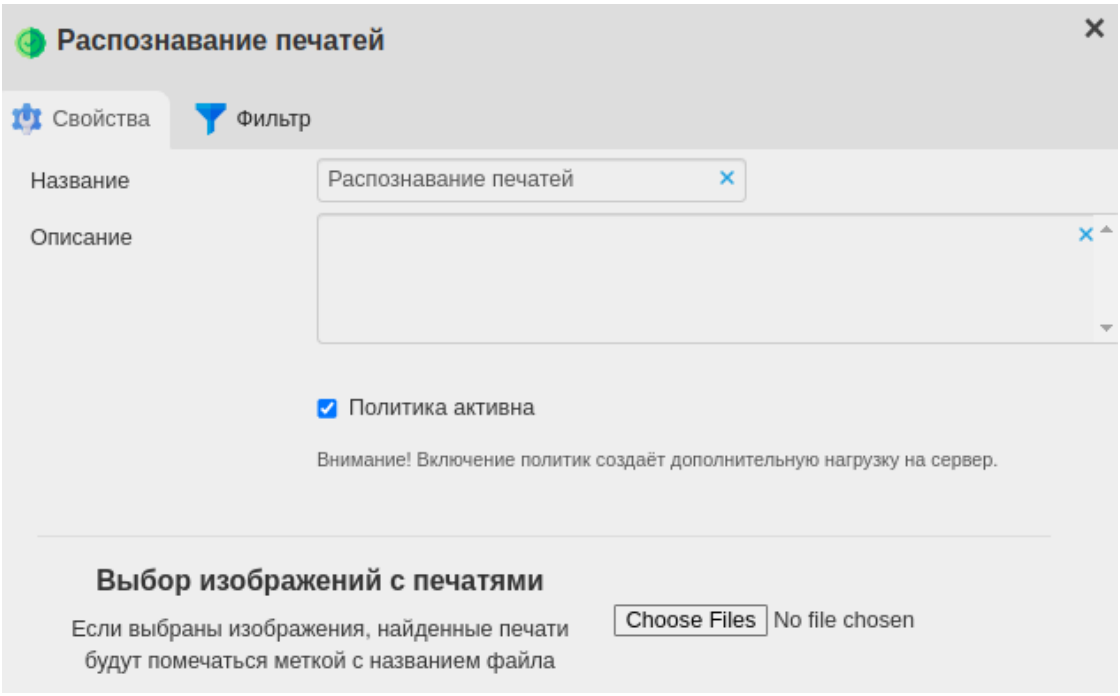
Что важно для таких образцов:

- размер изображения — 400x400px;
- разная степень нажатия при печати;
- небольшие различия между образцами;
- отсутствие бракованных оттисков;
- расположение печатей под разными углами.

Чтобы создать политику распознавания для печати:

1. Перейдите во вкладке **Политики** в папку **Политики** → **Анализ контента**.
2. Сдвиньте переключатель **Распознавание печатей** вправо.
3. Загрузите образец печати через кнопку выбора файла в **Выбор изображений с печатями**; дождитесь, пока у распознанных печатей в столбце **Статус** появится галочка.
4. Задайте фильтр для политики. Например:
   - **Типы контента** — pdf, jpg, png;
   - **Типы события** — перехваченные файлы/скриншоты.

   Примечание: Политика не работает с пустыми фильтрами. Не пропускайте этот шаг.
5. Установите галочку **Политика активна** для активации политики. Найденные факты будет доступны в разделе **Сработавшие политики**.



Ложные срабатывания

Для любой политики распознавания образов существует вероятность ложного срабатывания. Чаще всего такое происходит с печатями, имеющими определённое сходство. Чтобы снизить количество ложных срабатываний, откройте конфигурационный файл сервера iBatyr Monitor:

```
sudo nano /usr/share/ibatyr/settings.py
```

и измените значения параметра **STAMP_RECOGNITION_THRESHOLD** в сторону уменьшения.

Ложные срабатывания возможны, когда компания или организация имеют похожие печати, отличающиеся названием отдела или кодом подразделения. В этом случае обратитесь в нашу техническую поддержку.

Распознавание лиц

Сервер распознавания содержит функцию распознавания лиц на снимках веб-камер. Результат распознавания фиксируется в виде соответствующего уведомления: *Нет лица*, *Свое лицо*, *Неизвестное лицо*, *Несколько лиц*. Своё и неизвестное лица определяются по заранее назначенным в веб-консоли снимкам их владельцев.

Чтобы включить распознавание лиц:

1. Перейдите во вкладку **Политики**, далее — в папку **Политики** → **Анализ контента**.
2. Сдвиньте переключатель **Распознавание лиц** вправо.
3. Поставьте галочку **Политика активна**.
4. Перейдите во вкладку **Фильтр**, нажмите **Тип события** и поставьте флажок напротив *Снимок с *.
5. Нажмите + **Файл**, выберите **Тип контента** и поставьте флажки *image/jpg* и *image/png*.

После поступления первых результатов распознавания установите для каждого аккаунта соответствие изображения пользователю:

1. Выберите снимок с подходящим освещением и ракурсом анфас (лицом к камере) в таблице событий.
2. Нажмите на фотографию, откроется диалоговое окно.
3. Если лицо соответствует аккаунту, ответьте **Да** на вопрос **Распознавание лиц: Данное лицо принадлежит пользователю N**.

Примечание: При ответе **Нет** ранее установленное соответствие будет сброшено. Используйте кнопку **Закрыть**, если случайно открыли это окно или решили ничего не менять.

Изменения в результате установки соответствия будут применяться только к новым событиям. Проверьте, что лица на изображениях соответствуют владельцам компьютеров.

Алерты в **Конструкторе** для распознавания лиц:

tabularytabulary

Алерт	
Нет лица	
Своё лицо	
Неизвестное лицо	
Несколько лиц	
Нет снимка	

Ложные срабатывания

К ложным срабатываниям или полному отсутствию распознавания могут привести поворот головы, несоответствующий ракурс лица, закрытая, например рукой, часть лица. Повлиять на результат распознавания можно, уменьшив параметр **FACE_DETECT_THRESHOLD** в **/usr/share/ibatyr/settings.py**:

```
FACE_DETECT_THRESHOLD = 0.5
```

Примечание: При необходимости параметр можно уменьшать до 0.4, но следует учитывать, что чем меньше значение, тем меньше распознаваний.

Распознавание иных изображений, кроме снимков веб-камер

Чтобы распознать лица не только на снимках веб-камер, в фильтре политики **Распознавание лиц** выберите подходящие критерии. В */usr/share/ibatyr/settings.py* добавьте запись:

```
FACES_TYPES = ( "WebcamSnapshot", "Screenshot", "InterceptedFile")
```

и перезапустите iBatyr Monitor:

```
sudo service ibatyr restart
```

Дополнительные особенности функции распознавания лиц:

- Присутствует проверка на «заглушенные камеры» — заклеенные камеры, сбитая резкость и т. д. В срабатывания так же могут попадать трудно различимые для компьютерного зрения изображения, темнота и подобное. Если в алерте *Нет снимка* часто происходят нежелательные срабатывания, обратитесь в техническую поддержку.
- Площадь лица для корректного распознавания должна составлять не менее 2,5 % от площади изображения.
- При распознавании нескольких лиц их размеры не должны отличаться друг от друга более, чем в два раза. Это исключит срабатывание на случайно попавшие в поле зрения камеры лица вдалеке.
- Лица не должны пересекаться. Центр меньшего лица не должен лежать внутри рамки большего, в противном случае меньшее лицо игнорируется.
- Одно и то же лицо из базы не может распознаться на изображении более одного раза. Избыточные срабатывания игнорируются.
- Алгоритм распознавания лиц — HOG.

3.4.6 Логи

Сервер распознавания

Лог расположен по адресу: */var/log/ibatyr-cpservice.log*.

Запрос и его опции:

```
2020-09-10 12:19:39,065 [DEBUG] cp_server:112 Request for 2020_09_10/
↪ae4cd000abaecdaf46eec3d3ac90750d327e688a.jpe : text_extraction face_detection
```

Где *text_ extraction face_ detection* — опциональные параметры, извлечение текста и распознавание лиц.

Результат обработки:

```
2020-09-10 12:24:20,125 [DEBUG] cp_server:127 Response for 2020_09_10/
↪9ade404783b02bff8741ed1632ffbf63d883c64e.jpe done in 0:01:04.814513: "document_class":␣
↪undetected, "face": {'size': {'width': 640, 'height': 480}, 'bounds': [{'top': 306,
↪'right': 381, 'bottom': 476, 'left': 211}], 'vectors': '...'}, "extracted_text": "
```

В команде указан тип документа, сэмплы результата обработки лиц и извлечения текста, время затраченное на обработку.

Сервер iBatyr Monitor

Лог расположен по адресу */var/log/ibatyr/content_processing.log*.

Сообщение об ошибке *[ERROR] content_processing:420 API error: [Errno28] No space left on device* указывает, что серверу недостаточно RAM-диска. Ошибка возникает при работе с большими файлами или большом количестве ядер на сервере. Чтобы ее исправить, увеличьте размер дисковой памяти.

Для увеличения памяти добавьте в */etc/ibatyr/cpservice-config* строку:

```
RAMDISK_SIZE = '5G'
```

Примечание: Рекомендуемое значение для RAMDISK_SIZE можно рассчитать следующим образом: умножьте максимальный размер файла на обработку на количество ядер сервера. По умолчанию используется **500** МБ.

3.5 Обновление серверной части

3.5.1 Обновление iBatyr Monitor-сервера до версии 5.6

Подготовка

В ходе обновления сервер запросит ключ для версии 5.6. Если у вас его нет или есть ключ от более ранней версии, обратитесь в Отдел продаж: sales@ibatyr.kz. При обращении укажите информацию о ключе, который у вас есть.

Предупреждение: Не обновляйте сервер, если у вас нет лицензионного ключа от версии 5.6. Новую версию нельзя будет запустить без ключа, а откат на предыдущую приведет к утрате данных.

Обновление может занять длительное время. Чтобы ускорить процесс обновления, уменьшите размер базы данных .

Для обновления сервер iBatyr Monitor должен быть подключен к сети интернет.

Обновление

Чтобы обновить версию iBatyr Monitor-сервера:

1. Подключитесь к серверу по SSH.
2. Проверьте установленную версию Ubuntu:

```
lsb_release -a
```

Примечание: iBatyr Monitor поддерживает Ubuntu Server версий 18.04, 20.04, 22.04. Если вы планируете обновить версию, ознакомьтесь *с инструкцией по реиндексации базы данных*, иначе могут возникнуть ошибки на сервере.

3. Скачайте и запустите скрипт обновления:

```
wget -O - https://distr.ibatyr.kz/stable5.06/ibatyr.gpg | sudo apt-key add -
echo "deb https://distr.ibatyr.kz/stable5.06 stable5.06 non-free" | sudo tee /
↪etc/apt/sources.list.d/ibatyr.list
sudo apt-get update
sudo apt-get upgrade
```

Скрипт выполнит:

- проверку системных требований;
- запрос на создание резервной копии БД;
- скачивание необходимых пакетов;
- обновление всей системы и iBatyr Monitor .

При обновлении система запросит пароль для базы данных ClickHouse, который используется для дополнительной безопасности. Укажите пароль, только если он действительно нужен. В противном случае оставьте поле пустым.

Действия после обновления

Обновите агенты по инструкции *Обновление агентов*.

Возможные проблемы

Если после обновления не приходят события от пользователей:

1. Перейдите в раздел **Панель управления** → **Пользователи**.
2. Выберите всех пользователей и в выпадающем меню **Освободите лицензию**.
3. Снова выберите всех пользователей.
4. В выпадающем меню выберите **Назначить лицензию**.

3.5.2 Обязательные действия при обновлении операционной системы

Обновление операционной системы сервера требует реиндексации баз данных PostgreSQL.

Причина: из-за особенностей работы PostgreSQL при обновлении ОС меняется версия системной библиотеки **glibc**, отвечающая за настройки сортировки Collation в PostgreSQL. Это может привести к появлению дубликатов значений на уникальных индексах. Дубли нарушают целостность данных и могут вызвать ошибки в работе сервера — например, зависание спуллера из-за накопления сообщений о дублях в логах.

Решение: при обновлении ОС обновите Collation для PostgreSQL 15 и проведите реиндексацию базы данных для всех версий PostgreSQL.

Порядок действий про обновлении ОС:

1. Остановите iBatyr Monitor.

```
sudo ibatyr stop
sudo systemctl disable ibatyr
```

2. Обновите операционную систему в соответствии с вашим процессом.
3. Только для PostgreSQL 15: обновите настройки сортировки Collation.

```
echo "ALTER DATABASE postgres REFRESH COLLATION VERSION;" | sudo -u postgres␣
↪psql -d postgres
echo "ALTER DATABASE template1 REFRESH COLLATION VERSION;" | sudo -u postgres␣
↪psql -d template1
echo "ALTER DATABASE ibatyr REFRESH COLLATION VERSION;" | sudo -u postgres␣
↪psql -d ibatyr
```

4. Для всех версий PostgreSQL: реиндексируйте БД.

```
echo "REINDEX (VERBOSE) DATABASE postgres" | sudo -u postgres psql -d postgres
echo "REINDEX (VERBOSE) DATABASE template1" | sudo -u postgres psql -d␣
↪template1
echo "REINDEX (VERBOSE) DATABASE ibatyr" | sudo -u postgres psql -d ibatyr
```

5. Запустите iBatyr Monitor.

```
sudo systemctl enable ibatyr
sudo ibatyr start
```

6. Готово!

3.6 Обслуживание базы данных

3.6.1 Встроенная база данных ClickHouse

В iBatyr Monitor есть возможность включения базы данных ClickHouse.

Включение ClickHouse позволяет создать гибридный режим работы iBatyr Monitor : часто используемые данные хранятся в ClickHouse, остальные данные — в PostgreSQL.

На практике этот гибридный режим позволяет повысить производительность даже на базах данных с сотнями миллионов записей. На пилотном проекте скорость работы с реальными данными увеличилась до 50 раз.

Дополнительно для работы ClickHouse требуется:

- место на жестком диске — порядка 50% от размера базы данных Postgresql;
- оперативная память, потребление которой зависит от объёма базы данных и от нагрузки.

См.также:

Требования к базе данных ClickHouse.

Включение базы данных ClickHouse

По умолчанию iBatyr Monitor работает с базой данных PostgreSQL. Для включения ClickHouse и работы в гибридном режиме, выполните команду:

```
sudo ibatyr clickhouse-install
```

Примечание: При установке, система запросит пароль для базы данных ClickHouse. Оставьте его пустым.

Чтобы установить пароль или настроить ClickHouse для работы на другом сервере, обратитесь в *службу технической поддержки*.

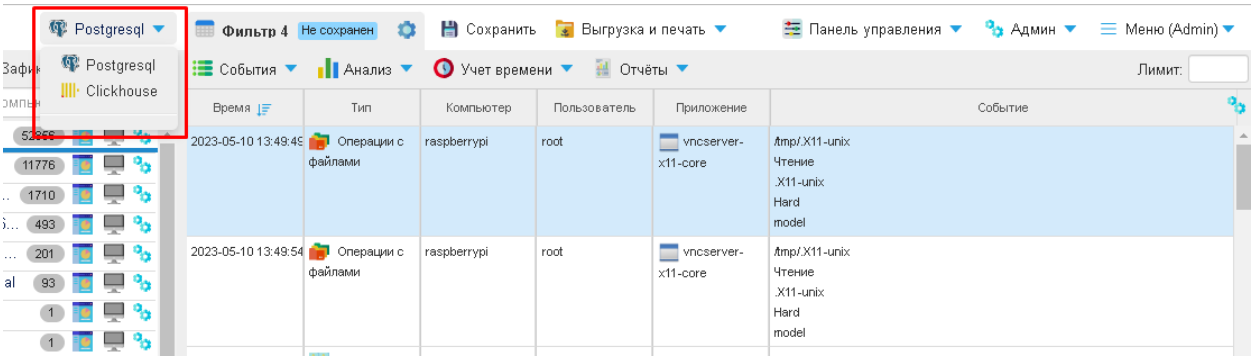
Скрипт установки скачает ClickHouse и установит в систему. После установки будет запущен процесс миграции необходимых данных из Postgresql в ClickHouse.

После установки ClickHouse и запуска iBatyr Monitor в гибридном режиме, данные в конструкторе и часть событий будут появляться с задержкой в 5—10 минут от реального времени. При этом общее быстродействие системы повысится. Особенно это будет заметно, если сервер iBatyr Monitor расположен на HDD-дисках.

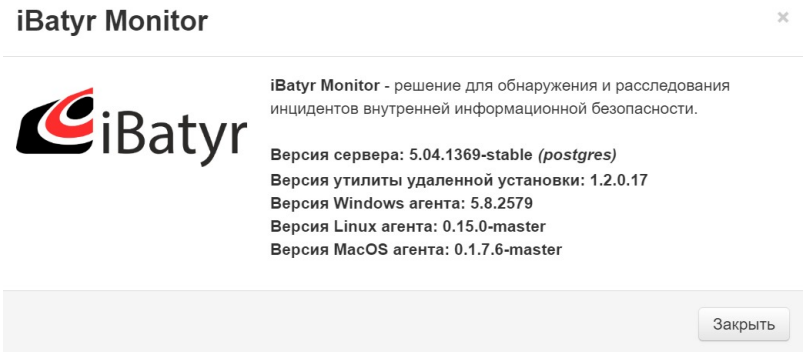
Процесс миграции на большой базе данных может занять некоторое время. Чтобы проследить за прогрессом миграции, откройте раздел **Администрирование** → **Статус сервера**. На этой странице будет отображаться название политики и количество событий, которые ещё не были обработаны этой политикой.

Обработка политик по умолчанию запускается раз в 5 минут. Страница автоматически обновляется, как только количество событий, которые должны быть мигрированы в ClickHouse, приблизится к нулю. Для работы с новой базой данных можно использовать веб-интерфейс.

После завершения миграции появится дополнительное меню переключения режима работы базы данных в веб-интерфейсе:



Также в **Меню** → **О программе** можно заметить, что текущая база данных сменилась с Postgresql на ClickHouse.



Примечание: На больших базах данных (от 10 ГБ) процесс миграции в гибридный режим работы может занимать до нескольких часов объективного времени. В ходе миграции в веб-интерфейсе администратора могут не отображаться события и отчёты.

Настройка SSL для ClickHouse

Чтобы настроить безопасное подключение к базе данных ClickHouse:

1. Настройте ClickHouse для использования OpenSSL.
2. На сервере iBatyr Monitor откройте конфигурационный файл **/etc/ibatyr/config/**.
3. В блоке **CLICKHOUSE** = укажите IP-адрес сервера и порт для подключения в следующем виде:

```
CLICKHOUSE = {
    'URL': 'clickhouses://ip-address:port/ibatyr'
}
```

Если не указать номер порта для подключения, то будет использован порт **9440** — порт для безопасного подключения по умолчанию.

Примечание: Обратите внимание, что в блоке **CLICKHOUSE** = для безопасного подключения необходимо указывать схему **clickhouses**. Схема **clickhouse** используется для незащищённого подключения.

Отключение базы ClickHouse

Чтобы отключить гибридный режим работы базы данных iBatyr Monitor , остановите службу Cliskhouse:

```
sudo service clickhouse-server stop && sudo service ibatyr restart
```

Чтобы полностью удалить базу данных из системы, удалите пакет ClickHouse:

```
sudo service clickhouse-server stop && sudo apt-get -y purge clickhouse-server && sudo␣
↪service ibatyr restart
```

При отстутствии связи с базой данных ClickHouse, iBatyr Monitor будет работать с PostgreSQL.

Выделение большего объема памяти для ClickHouse

Для выделения дополнительного объёма памяти базе данных откройте файл **/etc/clickhouse-server/users.xml** и в строке

```
<max_memory_usage>10000000000</max_memory_usage>
```

укажите в байтах размер памяти, который необходимо выделить для ClickHouse.

После увеличения размера базы данных перезагрузите сервисы ibatyr:

```
sudo service clickhouse-server restart
sudo ibatyr restart
```

Оценка занимаемых ресурсов базой данных ClickHouse

Чтобы определить, сколько места занято базой данных, выполните запрос:

```
sudo du -sm /var/lib/clickhouse/
```

Выданная цифра будет означать размер базы данных ClickHouse в мегабайтах.

Чтобы определить, сколько новая база данных занимает в оперативной памяти, выполните команду:

```
sudo ps -aux | grep -i clickhouse-server | awk '{print $5}'
```

Расширенные команды для управления ClickHouse в iBatyr Monitor

3.6.2 Создание архивной базы данных

В случае ухудшения работы сервера iBatyr Monitor из-за большого объёма накопленных данных, можно разделить текущую базу данных на две: актуальную и архивную. В актуальной можно оставить данные за текущий календарный год, а в архивную поместить данные за всё предыдущее время работы.

Примечание: Начиная с версии 5.6 скрипт поддерживает создание архивной БД для основной БД, расположенной на другом хосте. См. параметр `[DATABASE HOST]` в п. 6 инструкции.

Итогом выполнения всех операций данной инструкции станут:

- две базы данных:
  - архивная, в которой будут содержаться данные с года xxxx до прошлого года включительно;
  - текущая, в которой будут храниться данные за текущий год;
- возможность выбора базы данных для просмотра.

Предупреждение: Перед созданием архивной базы данных сделайте бэкап БД. Резервное копирование гарантирует восстановление данных при потере.

Предупреждение: Перед архивированием БД закройте старые инциденты или *отключите защиту инцидентов*. Если защита от удаления включена и есть открытые инциденты за текущий год, связанные с этими инцидентами шарды из архивной БД не удалятся.

Создать архив данных можно двумя способами:

1. **Скриптом**.
2. **Командами**.

Примечание: Скрипт ускоряет работу, но находится на стадии тестирования и доработки. По всем вопросам обращайтесь в поддержку за последней информацией.

Организация архива с помощью скрипта

Подготовка к архивации

1. Убедитесь, что на вашем диске есть около 150% свободного места от размера текущей базы данных.

Примечание: При недостатке доступного пространства воспользуйтесь скриптом *compact* из п.4 инструкции в соседней вкладке.

---

2. Если вы используете ClickHouse, создайте в нём базу данных ClickHouse по инструкции из раздела **Создание архивной базы данных** в соседней вкладке.
3. Создайте папку для архива с правами доступа для PostgreSQL. Желательно сделать это на отдельном носителе:

```
sudo mkdir /mnt/separate_disk/<archive_name>
sudo chmod 700 /mnt/separate_disk/<archive_name>
sudo chown postgres:postgres /mnt/separate_disk/<archive_name>
```

где `<archive_name>` – имя архивной базы данных.

Примечание: Используйте для папок и баз данных простые имена, основанные на датах архивов. Например, *archive_2022*.

---

4. Создайте папку *archives*, если она отсутствует:

```
sudo mkdir /var/lib/ibatyr/archives
```

5. Создайте символическую ссылку на новую папку:

```
cd /var/lib/ibatyr/archives
sudo ln -s /mnt/separate_disk/<archive_name> <archive_name>
```

6. Создайте новое табличное пространство и скопируйте в него базу данных:

```
bash /usr/share/ibatyr/bin/db/experimental/copy_db_to_tablespace <ARCHIVE NAME>
↪ [DATABASE HOST] [--remote]
```

где:

`<ARCHIVE NAME>` — имя новой архивной базы данных;

`[DATABASE HOST]` — укажите этот параметр, только если база данных находится *на другом хосте*.

`[--remote]`— флаг, который указывает на необходимость удаленного подключения к БД.

Примечание: Скрипт экспериментальный и требует внимания оператора. По окончанию работы будет предложено создать архивную БД Clickhouse. Этот процесс выполняется долго, но уже не требует внимания. Копирование базы 13 ГБ занимает 39 минут, копирование базы 3,3 ТБ занимает 4 часа.

Удаление устаревших данных

1. Запустите скрипт, который удаляет из основной базы данных *шарды (месяцы)*, предшествующие текущему году:

```
bash /usr/share/ibatyr/bin/db/experimental/drop_shards -d <MAIN DB NAME> [-n␣
↪100 (default 3)] [-o ASC (default)] -md true
```

где:

`-d` указывает на базу данных, из которой нужно удалить данные;

`-n` определяет количество шардов, значение по умолчанию — 3;

`-o` указывает порядок удаления шардов. `ASC` применяет порядок по возрастанию от самых старых данных до начала текущего года (значение по умолчанию);

`-md` при указании `true` отмечает указанную в параметре `-d` базу данных как основную, что влияет на получение списка шардов для удаления (по умолчанию false);

Пример: чтобы стереть данные за два предыдущих года, укажите `-n 24 -md true`. Порядок `ASC` применяется автоматически.

2. Удалите шарды текущего года из архивной базы данных:

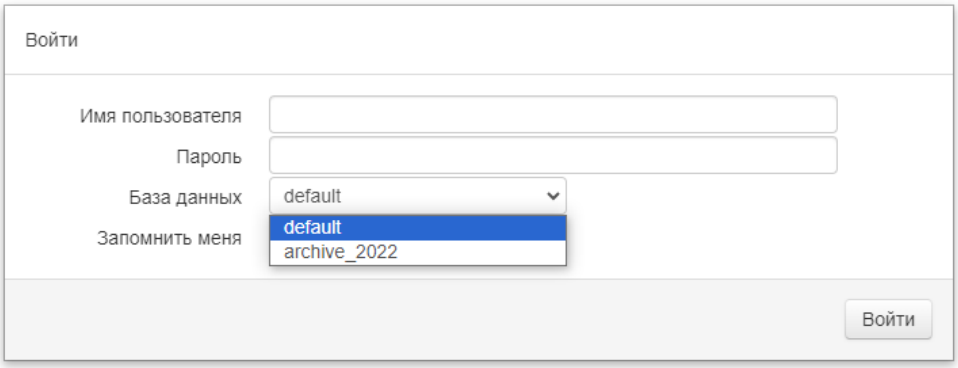
```
bash /usr/share/ibatyr/bin/db/experimental/drop_shards -d <ARCHIVE NAME> [-n␣
↪100 (default 3)] -o DESC
```

где `-o DESC` означает, что вы удаляете данные в порядке убывания с последнего по первый месяц текущего года. Например, чтобы удалить все шарды текущего года, укажите `-n 12 -o DESC`.

3. Удалите данные из PostgreSQL и ClickHouse архивной и основной БД:

```
./bin/db/experimental/cleanup_archive_data
```

Готово! При входе в iBatyr Monitor вы увидите новый архив в списке баз данных:



Организация архива с помощью команд

Подготовка к архивации

1. Убедитесь, что на диске (отдельном диске) есть достаточное количество свободного места — около 150% от текущей базы данных.

Примечание: Рекомендуем хранить архивную базу данных на отдельном диске. Это упростит работу с ней и ускорит работу с основной базой.

---

2. Остановите сервисы iBatyr Monitor:

```
sudo service ibatyr stop
sudo service nginx stop
```

3. Проверьте, что сервисы остановились. Для этого выполните:

```
ibatyr top
ibatyr ps

Ни одна из этих команд не должна выводить список процессов.
```

4. Если есть сомнения в доступном количестве свободного места:

   4.1 Откройте файл скрипта *compact*, являющегося частью iBatyr Monitor:

   ```
   sudo nano /usr/share/ibatyr/bin/compact
   ```

   4.2 В открывшемся файле раскомментируйте строки `echo "Vacuum database"` и `sudo -u postgres psql ibatyr -c "vacuum full"`. Итоговый файл будет иметь следующий вид:

   ```
   #!/bin/bash
   # USE compact
   # HELP Cleanup unreffered dimensions and vacuum database
   ibatyr stop
   echo "Cleanup dimensions"
   cat sql/cleanup_dimensions.sql | bin/sql
   echo "Vacuum database"
   sudo -u postgres psql ibatyr -c "vacuum full"
   ibatyr start
   echo "Cleanup done"
   bin/info
   ```

   4.3 Сохраните изменения.

   4.4 После завершения очистки базы запустите:

   ```
   ibatyr compact
   ```

   Примечание: Эта команда существенно уменьшит объём памяти, который занимает база данных.

Создание архивной базы данных

Примечание: Если вы не используете ClickHouse, то переходите к пункту **Создание новой базы данных**.

Чтобы не потерять данные в ClickHouse, выполните следующие действия:

1. Зайдите в ClickHouse:

   ```
   ibatyr clickhouse
   ```

2. Переименуйте текущую базу данных:

   ```
   RENAME DATABASE ibatyr TO archive_2022;

   Здесь *archive_2022* - имя архивной базы данных.
   ```

3. Создайте новую основную базу данных в ClickHouse:

   ```
   ibatyr clickhouse reinit
   ```

После этого переходите к созданию новой базы данных.

Создание новой базы данных

Примечание: Для удобства работы в качестве имени новой базы и TABLESPACE используйте простые имена, основанные на датах архивов. Например: `archive_2022`.

1. Создайте папку с правами доступа для PostgreSQL. Желательно сделать это на отдельном носителе:

```
sudo mkdir /mnt/separate_disk/archive_2022
sudo chmod 700 /mnt/separate_disk/archive_2022
sudo chown postgres:postgres /mnt/separate_disk/archive_2022
```

2. Создайте папку *archives*, если она отсутствует:

```
sudo mkdir /var/lib/ibatyr/archives
```

3. Создайте символическую ссылку на новую папку:

```
cd /var/lib/ibatyr/archives
sudo ln -s /mnt/separate_disk/archive_2022 archive_2022
```

4. Создайте TABLESPACE. Для этого войдите в консоль управления PostgreSQL:

```
sudo -u postgres psql
```

   и выполните команду:

```
CREATE TABLESPACE archive_2022 LOCATION '/var/lib/ibatyr/archives/archive_2022
↪';
```

5. Скопируйте текущую базу в архивную:

```
CREATE DATABASE archive_2022 TEMPLATE ibatyr TABLESPACE archive_2022;
```

6. Удалите шарды из таблицы до текущего года. Чтобы открыть список шардов, выйдите из PostgreSQL:

```
\q
```

   Откройте список:

```
ibatyr shard list
```

   Вернитесь в PostgreSQL:

```
sudo -u postgres psql -d ibatyr
```

   или

```
ibatyr sql
```

   Удалите шарды, подставив название в *<название таблицы>*:

```
drop table <название таблицы>;
```

7. Теперь текущая база полностью скопирована в архивную. Удалите из текущей базы iBatyr Monitor всё, что было перенесено в архив:

```
delete from agent_event where local_time < '2023-01-01 00:00:00'; # в нашем␣
↪случае оставляем только 2023-й год
# Очистите измерения
delete from agent_web where id not in (select distinct web_data_id from agent_
↪event where web_data_id IS NOT NULL);
delete from agent_time where id not in (select distinct time_id from agent_
↪event where time_id IS NOT NULL);
delete from agent_account where id not in (select distinct account_id from␣
↪agent_event where account_id IS NOT NULL);
delete from agent_appinstallation where id not in (select distinct app_
↪installation_id from agent_event where app_installation_id IS NOT NULL);
delete from agent_application where id not in (select distinct application_id␣
↪from agent_event where application_id IS NOT NULL);
delete from agent_networkconnection where id not in (select distinct net_data_
↪id from agent_event where net_data_id IS NOT NULL);
delete from agent_dialog where id not in (select distinct dialog_id from agent_
↪event where dialog_id IS NOT NULL);
delete from agent_device where id not in (select distinct device_id from agent_
↪event where device_id IS NOT NULL);
delete from agent_attachedfile where not exists (select 1 from agent_event␣
↪where agent_event.attached_file_id=agent_attachedfile.id) and agent_
↪attachedfile.category is null;
delete from agent_filepath where not exists (select 1 from agent_event where␣
↪agent_event.file_path_id = agent_filepath.id);
delete from analytics_session where local_time < '2023-01-01 00:00:00';
delete from analytics_filter_events where not exists (select 1 from agent_
↪event where agent_event.id=analytics_filter_events.event_id);

# Выйдите из PostgreSQL
\q

# Завершите сессии в iBatyr Monitor
ibatyr reset_extended_sessions
```

8. Вернитесь в PostgreSQL с помощью одной из команд:

```
sudo -u postgres psql -d ibatyr
```

или

```
ibatyr sql
```

9. Оптимизируйте работу базы (процедура может занять много времени):

```
ANALYZE;
```

10. Добавьте архивную базу данных в конфигурационный файл *etc/ibatyr/config* в секцию `DATABASES`:

```
DATABASES = {
'default': {
'ENGINE': 'django.db.backends.postgresql_psycopg2',
'NAME': 'ibatyr',
'USER': 'ibatyr',
```

(continues on next page)

(продолжение с предыдущей страницы)

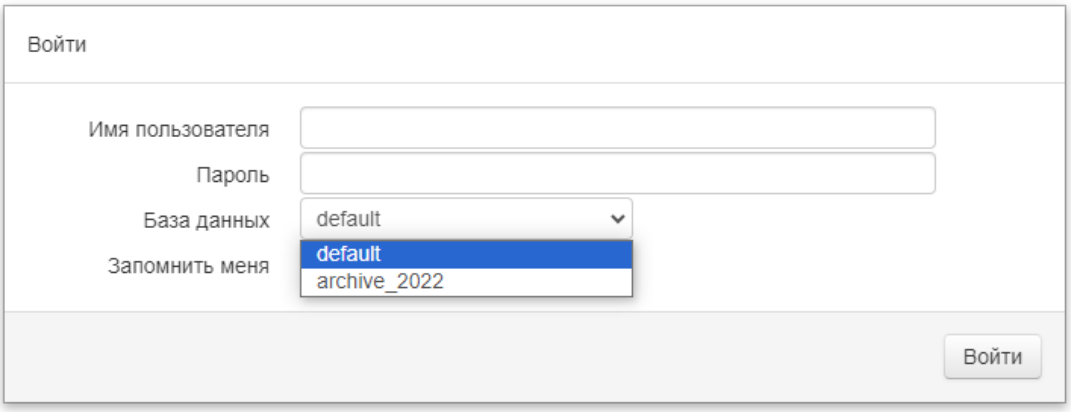
```
'PASSWORD': 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx',
'HOST': '',
'PORT': '',
},
'archive_2022': {
'ENGINE': 'django.db.backends.postgresql_psycopg2',
'NAME': 'archive_2022',
'USER': 'ibatyr',
'PASSWORD': 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx', # пароль такой же, как у␣
↪базы данных default
'HOST': '',
'PORT': '',
   }
 }
```

Готово! Теперь можно проверять, что перенос прошёл успешно.

Для этого запустите сервер iBatyr Monitor:

```
ibatyr start
```

Откройте веб-интерфейс сервера. Если всё прошло успешно, в форме входа можно будет выбрать базу данных.



Окончательное оформление архивной базы данных

После проверки доступности обеих баз, закончите оформление архивной базы данных. Для этого:

1. Остановите сервисы iBatyr Monitor:

```
sudo service ibatyr stop
sudo service nginx stop
```

2. Проверьте, что сервисы остановились. Для этого выполните:

```
ibatyr top
ibatyr ps
```

Ни одна из этих команд не должна выводить список процессов.

3. Очистите архивную базу данных PostgreSQL от лишних данных:

```
ibatyr sql
ibatyr=>\c archive_2022

Вы подключены к базе данных "archive_2022" как пользователь "ibatyr".
archive_2022=>
```

Предупреждение: Перед выполнением следующей операции ещё раз проверьте, что подключены к архивной базе!

4. Удалите все шарды текущего года с помощью команды:

```
drop table <название таблицы>;
```

5. Удалите данные:

```
delete from agent_event where local_time >= '2023-01-01 00:00:00'; # Убираем␣
↪2023-й год
# Очищаем измерения
delete from agent_web where id not in (select distinct web_data_id from agent_
↪event where web_data_id IS NOT NULL);
delete from agent_time where id not in (select distinct time_id from agent_
↪event where time_id IS NOT NULL);
delete from agent_account where id not in (select distinct account_id from␣
↪agent_event where account_id IS NOT NULL);
delete from agent_appinstallation where id not in (select distinct app_
↪installation_id from agent_event where app_installation_id IS NOT NULL);
delete from agent_application where id not in (select distinct application_id␣
↪from agent_event where application_id IS NOT NULL);
delete from agent_networkconnection where id not in (select distinct net_data_
↪id from agent_event where net_data_id IS NOT NULL);
delete from agent_dialog where id not in (select distinct dialog_id from agent_
↪event where dialog_id IS NOT NULL);
delete from agent_device where id not in (select distinct device_id from agent_
↪event where device_id IS NOT NULL);
delete from agent_attachedfile where not exists (select 1 from agent_event␣
↪where agent_event.attached_file_id=agent_attachedfile.id) and agent_
↪attachedfile.category is null;
delete from agent_filepath where not exists (select 1 from agent_event where␣
↪agent_event.file_path_id = agent_filepath.id);
delete from analytics_session where local_time >= '2023-01-01 00:00:00';
delete from analytics_session_extended where local_time >= '2023-01-01 00:00:00
↪';
delete from analytics_filter_events where not exists (select 1 from agent_
↪event where agent_event.id=analytics_filter_events.event_id);
```

6. Оптимизируйте работу базы (процедура может занять много времени):

```
ANALYZE;
```

7. Заполните данными архив ClickHouse:

```
OVERRIDE_DBNAME=archive_2022 ibatyr clickhouse reinit
OVERRIDE_DBNAME=archive_2022 ibatyr clickhouse pump
```

Готово! Можно запускать сервис iBatyr Monitor и проверять работу архивной базы данных.

Итоги работы

Итогом правильного выполнения всех операций станут:

- основная и архивная базы данных, доступные для выбора при входе в веб-интерфейс;
- возможность работы ClickHouse со всеми базами данных;
- в основной базе данных будут выполняться политики, в архивной — нет.

3.6.3 Как уменьшить рост базы данных Postgresql автоматически?

Примечание: Данные настройки в версии 4.4 и выше добавляются автоматически.

Если у вас база данных слишком быстро растёт, то можно попробовать сдержать её рост агрессивными параметрами «автовакума». Автовакум это такой встроенный процесс для поддержания структуры базы данных в упорядоченном виде.

Шаги для достижения цели:

- Нужно открыть консоль linux на сервере с установленным iBatyr Monitor Server
- Открыть на редактирование файл настроек postgresql (9.5 - ваша версия postgresql):

```
sudo nano /etc/postgresql/9.5/main/postgresql.conf
```

- В конце файла вставить строки:

```
autovacuum = on # Enable autovacuum subprocess? 'on'
log_autovacuum_min_duration = 0 # -1 disables, 0 logs all actions and
autovacuum_max_workers = 5 # max number of autovacuum subprocesses
autovacuum_naptime = 1min # time between autovacuum runs
autovacuum_vacuum_threshold = 300 # min number of row updates before
autovacuum_analyze_threshold = 200 # min number of row updates before
autovacuum_vacuum_scale_factor = 0.01 # fraction of table size before vacuum
autovacuum_analyze_scale_factor = 0.005 # fraction of table size before analyze
```

- Сохранить файл, нажав **Ctrl** + **x** и нажав **y**
- Перезапустить postgresql

```
sudo service postgresql restart
```

После этого база данных будет расти понятными и умеренными темпами, и будет более предсказуема в размерах.

3.6.4 Локальная база данных агента

Windows- и Linux-агент при отсутствии соединения с сервером сохраняют данные в локальной базе. Накопленные данные из локальной базы передаются на сервер после установления связи.

При достижении максимального размера локальной базы и отсутствии связи с сервером новые данные заменят самые старые.

Размер базы

По умолчанию размер локальной базы данных равен 1 ГБ.

Размер можно изменить:

1. Перейдите в **Панель управления** → **Конфигурации компьютеров** → *ваша конфигурация* → **Сбор данных**.
2. Укажите размер в поле **Локальная база данных агента**. Максимальный размер — 50 ГБ.

Сжатие данных

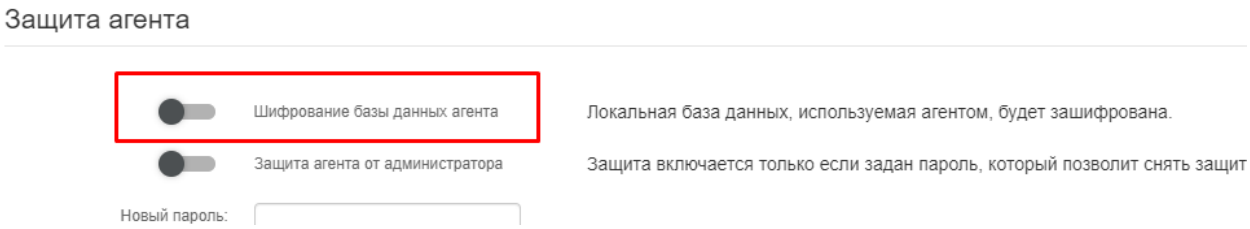
Для более эффективного использования дискового пространства и уменьшения объема передаваемой информации на сервер можно включить сжатие данных.

Чтобы активировать сжатие:

1. Перейдите в **Панель управления** → **Конфигурации компьютеров** → *ваша конфигурация* → **Сбор данных**.
2. Передвиньте бегунок **Сжимать данные при хранении и передаче**.

Шифрование

Для дополнительной защиты включите шифрование локальной базы данных в **Конфигурации компьютеров** → *ваша конфигурация* → **Защита агента**.



Примечание: После включения шифрования агент шифрует данные, а затем сохраняет их в локальной базе. После этого данные передаются в зашифрованном виде на сервер. Нельзя прочитать зашифрованные данные на агенте, потому что только у сервера есть ключ для расшифровки.

Переключение на резервный сервер

Если указан резервный сервер, а связь с основным потеряна, агент попытается передать зашифрованные данные из локальной базы на резервный.

Однако резервный сервер использует другой ключ, поэтому не может расшифровать данные. В результате при попытке передачи возникает ошибка.

После нескольких безуспешных попыток отправки:

- данные в локальной базе удаляются безвозвратно,
- агент переключается на резервный сервер,
- начинает собирать новые данные,
- шифрует их уже под ключ резервного сервера и отправляет на него.

Таким образом, работа продолжается, но ранее собранные данные теряются.

3.6.5 Бэкап базы данных

Подготовка

1. Убедитесь, что на жёстком диске достаточно свободного места:

```
df -h
```

2. Проверьте, что установлена и запущена работоспособная версия PostgreSQL:

```
sudo service postgresql status
```

3. Остановите службы сервера, иначе резервное копирование может занять длительное время:

```
sudo ibatyr stop
```

4. Проверьте, что службы остановлены:

```
sudo ibatyr top
sudo ibatyr ps
```

Проведение бэкапа

Выполните команду:

```
sudo ibatyr backup_db
```

Ваш бэкап будет размещен в папке **/var/lib/ibatyr/ibatyr_backup**.

Для переноса на другой компьютер скопируйте эту папку по сети или на переносной носитель.

Восстановление бэкапа

Примечание: Восстановление базы данных должно выполняться в той же версии iBatyr Monitor, в которой был создан бэкап. В противном случае не гарантируется работоспособность системы.

Для восстановления бэкапа выполните команду:

```
sudo ibatyr restore_db
```

Если файл бэкапа находится не в **/var/lib/ibatyr/ibatyr_backup**, путь к нему нужно указать явно, например:

```
sudo ibatyr restore_db /home/support/backup
```

Примечание: Путь к папке должен быть указан полностью!

Исходные коды скриптов:

- скрипт инсталлятора — **bp_install.sh**:

```
#!/bin/bash -e
cd ~
wget -O ~/backup_db http://dist.ibatyr.kz/utils/script/backup/backup_db
cp ~/backup_db /usr/share/ibatyr/bin/
chmod +x /usr/share/ibatyr/bin/backup_db

wget -O ~/restore_db http://dist.ibatyr.kz/utils/script/backup/restore_db \
cp ~/restore_db /usr/share/ibatyr/bin/restore_db \
chmod +x /usr/share/ibatyr/bin/restore_db
```

- скрипт создания бэкапа — **backup_db.sh**:

```
echo "Backup iBatyr Monitor"

if ! [ -f /bin/tar ]; then
echo "No app tar. Please install 'sudo apt-get install tar'"
exit 3
fi

if ! [ -f /usr/bin/pg_dump ]; then
echo "No app pg_dump. Exit"
exit 3
fi
#---------------------------
bname=${DBNAME}-db.dump
sname=${DBNAME}-setting.tar
cname=${DBNAME}-sert.tar
default_folder="ibatyr_backup"
default_path="/var/lib/ibatyr"
#---------------------------
```

(continues on next page)

(продолжение с предыдущей страницы)

```
function backup_path_dialog() {
    echo -e "\e[32mПуть для размещения резервной копии базы: '${default_
↪path}'(Y/N)?:\e[0m"
    read var1
    case $var1 in
            Y|y)
            path=${default_path}
            ;;
            N|n)
            request_backup_path
            ;;
            *)
            error
            backup_path_dialog
            ;;
    esac
}

function request_backup_path() {
    echo -e "\e[32mЗадайте путь для размещения резервной копии базы:\e[0m"
    read path
}

function error() {
    echo 'не могу распознать ответ'
    echo 'введите Y или N'
}

if [ $1 ] ;  then
        path=$1
else
    backup_path_dialog
fi

#free space from hdd?
TREE_ROOT=$(df --output=avail $path | sed 1d)

echo "Свободное место в папке '${path}': ${TREE_ROOT}"

DBPATH=$(echo $(su - postgres -c "psql -t -U postgres $DBHOST_OPTION
↪$DBPORT_OPTION -d $DBNAME -c \"show data_directory;\""))
SIZE_DB=`du -sk $DBPATH | cut -f1`

if [[ "$TREE_ROOT" -gt "$SIZE_DB" ]]; then
echo -e "\e[32mСоздаем резервную копию базы...\e[0m"
else
echo -e "\e[31mНехватает свободного места для создания резервной копии базы\
↪e[0m"
exit 1
fi

if ! [ -f /usr/bin/realpath ]; then
```

(continues on next page)

(продолжение с предыдущей страницы)

```
echo "Warning. No app realpath. Please install 'sudo apt-get install␣
↪realpath'"
else
path=$(realpath $path)
fi

path=${path}/${default_folder}
echo "Backup path $path"

#Create backup path
echo "Create backup path"
mkdir -p $path
chmod 777 -R $path

if ! [ -d  "$path" ] ; then
        echo "directory does not exist. exit"
        exit 1
fi
echo "Remove old backup files"
rm $path/* || true

#File name
full_path=${path}/${bname}
sfull_path=${path}/${sname}
cfull_path=${path}/${cname}

echo "Backup path $full_path"
echo "Setting path $sfull_path"
echo "CA path $cfull_path"
echo "-----------------------------------------"
echo "Backup config"
tar --absolute-names --create --verbose --file $sfull_path /etc/ibatyr

echo "Backup CA"
tar --absolute-names --create --verbose --file $cfull_path /var/lib/ibatyr/
↪CA

echo "Backup DB"
sudo -u postgres pg_dump --host=$DBHOST_OPTION $DBPORT_OPTION --verbose --
↪compress=7 --clean --create --blobs --format=c --file=$full_path --dbname=
↪$DBNAME

echo "-----------------------------------------"
echo "Backup path"

if ! [ -f $full_path ]; then
echo 'No file db. Error'
exit 1
else
echo "File DB: $(du -h $full_path)"
fi
```

(continues on next page)

(продолжение с предыдущей страницы)

```
if ! [ -f $sfull_path ]; then
echo 'No file setting. Error'
exit 1
else
echo "File seting: $(du -h $sfull_path)"
fi

if ! [ -f $sfull_path ]; then
echo 'No file CA. Error'
exit 1
else
echo "File CA: $(du -h $sfull_path)"
fi
echo "-----------------------------------------"
echo "Finish Backup iBatyr Monitor"
```

- скрипт восстановления базы данных — **restore_db.sh**:

```
bname=${DBNAME}-db.dump
sname=${DBNAME}-setting.tar
cname=${DBNAME}-sert.tar
def_folder="ibatyr_backup"
def_path="/var/lib/ibatyr/${def_folder}"

if [ $1 ] ;  then
    path=$1
else
    path=${def_path}
fi

path=$(realpath $path)

full_path=${path}/${bname}
cfull_path=${path}/${cname}

if ! [ -f $full_path ]; then
        echo "No db backup at $full_path"
else
        echo "Restore DB ${DBNAME} from $full_path"
        ibatyr stop
        service postgresql restart
        echo "sudo -u postgres pg_restore  --host=$DBHOST_OPTION --port=
↪$DBPORT_OPTION  --verbose --clean --create  --format=c $full_path -d␣
↪postgres"
        sudo -u postgres pg_restore --host=$DBHOST_OPTION --port=$DBPORT_
↪OPTION  --verbose --clean --create  --format=c $full_path -d postgres
        ibatyr init
        echo "Done!"
fi

if ! [ -f $cfull_path ]; then
        echo "No license backup at $cfull_path"
```

(continues on next page)

(продолжение с предыдущей страницы)

```
else
        echo "Restore license"
        rm /var/lib/ibatyr/CA/*
        tar --absolute-names --extract --verbose --file $cfull_path
        chown -R ibatyr:ibatyr /var/lib/ibatyr/CA/
        chmod 775 -R /var/lib/ibatyr/CA/
        ibatyr restart
fi
```

3.6.6 Выгрузка событий из базы данных

Выгрузка событий кейлоггера:

Иногда возникают вопросы, как можно выгрузить из базы данных собранную информацию.

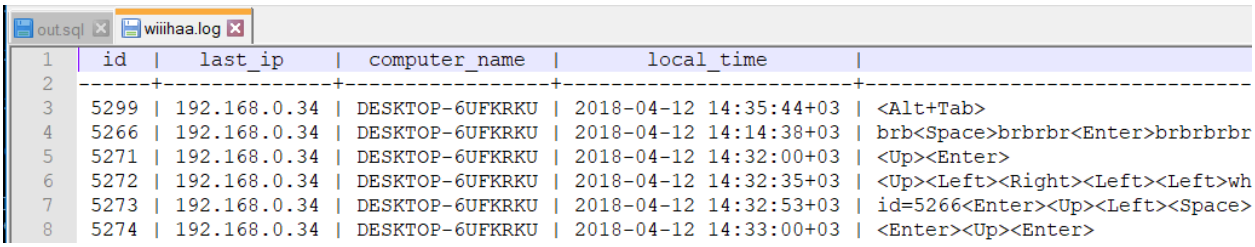
На примере конкретного вопроса, разберём что мы можем выгрузить из базы данных PostgreSQL, которая используется в iBatyr Monitor .

Задача: Выгрузить все события модуля нажатий клавиш, чтобы было время события, IP-адрес машины и название рабочей станции и событие ввода с клавиатуры.

Решение: Ниже приведен пример скрипта, который делает эту операцию и вывод помещает в файл - «out.log». Команду нужно вводить в Linux-консоли.

```
echo "select agent_event.id,agent_agent.last_ip,agent_agent.computer_name,agent_event.
↪local_time,agent_event.text_data from agent_event INNER JOIN agent_agent on agent_
↪event.agent_id = agent_agent.id where event_type_id=1;" | ibatyr sql > out.log
```

И мы увидим такой вывод в текстовом файле:



Этот файл можно будет скачать с сервера из домашней папки пользователя - через Filezilla или Winscp, введя логин и пароль от консоли Linux (По умолчанию логин и пароль **support\support**).

Выгрузка событий по скриншотам:

Вывести все события снимков с экрана:

```
echo "select agent_event.id,agent_agent.last_ip,agent_agent.computer_name,agent_event.
↪local_time,agent_event.window_title from agent_event INNER JOIN agent_agent on agent_
↪event.agent_id = agent_agent.id where event_type_id=4;" | ibatyr sql > out.log
```

Вывести все события снимков экрана, от рабочей станции с именем **«DESKTOP-6UFKRKU»**:

```
echo "select agent_event.id,agent_agent.last_ip,agent_agent.computer_name,agent_event.
↪local_time,agent_event.window_title from agent_event INNER JOIN agent_agent on agent_
↪event.agent_id = agent_agent.id where event_type_id=4 and agent_agent.computer_name=
↪'DESKTOP-6UFKRKU';" | ibatyr sql > out.log
```

3.6.7 Перенос базы на другой жёсткий диск

Внимание: Жёсткий диск / раздел должен существовать в системе и быть подключен физически.

Внимание: Нельзя использовать одну и ту же точку монтирования для файлов и БД.

Если на диске есть необходимые разделы, переходим к п.2.

При отсутствии разделов — размечаем диск *любой программой разметки*, например так:

```
sudo cfdisk /dev/sdX
```

и создаём на нём файловую систему командой:

```
sudo mkfs.ext4 /dev/sdX
```

где `X` — завершение имени диска.

1. Останавливаем сервисы командами:

```
sudo service postgresql stop
sudo ibatyr stop
```

2. Редактируем файл /etc/fstab:

```
sudo nano -w /etc/fstab
```

Прописываем в него строку:

```
/dev/sdX  /var/lib/postgresql/ ext4 rw,noatime 0 2
```

где `/dev/sdX` — ваш жёсткий диск; `/var/lib/postgresql/` — каталог, в котором отобразится содержимое диска; `ext4` — тип файловой системы (если вы используете другую фс jfs/xfs/reiser и т. д., эта опция меняется), `rw` — разрешение на чтение-запись на диск. Также можно прописать диск по `UUID`. Узнать `UUID` диска можно с помощью команды:

```
sudo blkid
```

В этом случае первая часть записи примет вид `UUID=`, где в кавычки нужно вписать результат вывода вышеуказанной команды.

Предупреждение: Разделы с GPT-форматированием можно примонтировать только по UUID-диска!

3. Создаём папку для резервного копирования и перемещаем в неё данные из каталога базы данных:

```
mkdir /home/user/rezerv && sudo mv /var/lib/postgresql/* /home/user/rezerv
```

где `user` — это домашний каталог пользователя. Скорее всего, у вас он отличается. Узнать домашний каталог пользователя можно командой:

```
env | grep -E "home|HOME"
```

Результатом выдачи данной команды будет домашний каталог пользователя, от имени которого эта команда выполнена.

4. Проверяем корректность монтирования командой:

```
sudo mount -a
```

Эта команда монтирует диск, который уже прописан в **fstab**, но еще не примонтирован.

Если мы что-то вписали неверно либо ошиблись, то мы увидим ошибки монтирования и, соответственно, получим возможность исправить допущенную ошибку. Проверяем корректность монтирования диска командой типа:

```
df -h
```

Также можно проверить, что данный раздел доступен на запись. Например, создадим текстовый файл и проверим его наличие командами:

```
touch /var/lib/postgresql/15/main/test_write.txt && ls -l /var/lib/postgresql/15/main/
```

Либо просто выполнив команду `mount` без параметров: её результатом станет вывод всех монтированных систем; наше новое устройство должно быть монтировано `rw`.

Если используете PostgreSQL 11, здесь и далее укажите правильную версию в пути — например, `/var/lib/postgresql/11/main/`

5. Копируем всё на жёсткий диск:

```
sudo cp -R  /home/user/rezerv/* /var/lib/postgresql/
```

В случае если вы перемещали данные в другой каталог, произведите изменения в соответствии с реальным расположением файлов.

6. Меняем владельца на postgres:

```
sudo chown -R postgres:postgres /var/lib/postgresql/15/main
```

7. Выставляем ему права доступа на 700:

```
sudo chmod -R 700 /var/lib/postgresql/15/main
```

8. Запускаем сервисы PostgreSQL, iBatyr Monitor и Nginx :

```
sudo service postgresql start
sudo ibatyr start
```

Выполняем команду:

```
sudo ibatyr sql
```

в появившемся приглашении пишем `analyze`; ждём.

Ошибки типа `ПРЕДУПРЕЖДЕНИЕ: pg_shdescription пропускается - только суперпользователь может анализировать этот объект` некритичны, т. к. говорят о том, что команда, запущенная с данными правами, не смогла проанализировать служебные таблицы БД. Это и не требуется.

9. Заходим в веб-интерфейс, проверяем, что всё работает, все отчёты видны и т. д. Если всё в порядке, можно удалять резервные файлы:

```
rm -R /home/user/rezerv
```

Используйте `rm` с осторожностью, чтобы не потерять данные.

3.6.8 Перенос базы данных на выделенный сервер

Если вы хотите разместить базу данных отдельно от службы iBatyr Monitor и веб-интерфейса, подготовьте сервер БД и подключите к нему сервер iBatyr Monitor.

Работы на сервере БД

Установите ПО

1. Установите чистый Ubuntu Server версии 20 или 22.
2. Обновите пакеты в системе:

```
sudo apt update && sudo apt upgrade
```

3. Установите пакеты для установки БД:

```
sudo apt install dirmngr ca-certificates software-properties-common apt-
↪transport-https lsb-release curl -y
```

4. Добавьте ключи к репозиторию PostgreSQL:

```
curl -fSsL https://www.postgresql.org/media/keys/ACCC4CF8.asc | gpg --dearmor␣
↪| sudo tee /usr/share/keyrings/postgresql.gpg > /dev/null
```

5. Добавьте репозиторий:

```
echo deb [arch=amd64,arm64,ppc64el signed-by=/usr/share/keyrings/postgresql.
↪gpg] http://apt.postgresql.org/pub/repos/apt/ $(lsb_release -cs)-pgdg main |␣
↪sudo tee /etc/apt/sources.list.d/postgresql.list
```

6. Обновите списки репозиториев в пакетном менеджере:

```
sudo apt update
```

7. Установите PostgreSQL 15:

```
sudo apt install postgresql-client-15 postgresql-15 -y
```

Создайте пользователя

1. Найдите пароль на сервере iBatyr Monitor с помощью команды:

```
cat /etc/ibatyr/config | grep PASSWORD
```

2. Скопируйте пароль. Он будет в кавычках, например:

```
'PASSWORD': '05ce255df14c33081437373161396b77',
```

3. Вставьте пароль в команду вместо `пароль` и выполните ее на сервере БД:

```
sudo -u postgres psql -c "create user ibatyr with password 'пароль';"
```

Пример:

```
sudo -u postgres psql -c "create user ibatyr with password
↪'05ce255df14c33081437373161396b77';"
```

Измените конфигурацию

1. Откройте файл конфигурации */etc/postgresql/15/main/postgresql.conf* для редактирования.

В примере используется Vim, но подойдет любой редактор:

```
sudo vim /etc/postgresql/15/main/postgresql.conf
```

Найдите строку:

```
#listen_addresses = 'localhost,00.00.00.000'                # what IP address(es)␣
↪to listen on;
```

Уберите в строке символ # в начале строки и добавьте IP, по которому iBatyr Monitor будет обращаться на сервер БД.

Примечание: Важно указать именно IP-адрес сервера базы данных. Этот адрес определяет интерфейс, через который сервер принимает запросы. Он не связан с IP-адресом, с которого приходят запросы.

Сохраните изменения и выйдите из редактора.

2. Откройте файл */etc/postgresql/15/main/pg_hba.conf* для редактирования:

```
sudo vim /etc/postgresql/15/main/pg_hba.conf
```

В конец файла добавьте:

```
host    all             all             {ip сервера iBatyr Monitor}/{маска}    ␣
↪    md5
```

Например, если `00.00.00.000` – IP-адрес сервера iBatyr Monitor и 32 – маска подсети:

```
host    all             all             00.00.00.000/32         md5
```

3. Перезагрузите PostgreSQL для применения изменений:

```
sudo systemctl restart postgresql
```

Работы на сервере iBatyr Monitor

Перенесите базу данных

Примечание: Если на сервере нет данных, пропустите этот шаг и перейдите к разделу *Создайте базу данных*.

---

1. Выключите сервер iBatyr Monitor:

```
ibatyr stop
```

2. Создайте бэкап командой:

```
ibatyr backup_db
```

3. Перенесите резервную копию из каталога */var/lib/ibatyr/ibatyr_backup/ibatyr-db.dump* на сервер базы данных.

4. Запустите восстановление БД на удаленном сервере:

```
sudo -u postgres pg_restore --verbose --clean --create --format=c {путь до␣
↪файла бекапа} -d postgres
```

Например:

```
sudo -u postgres pg_restore --verbose --clean --create --format=c /home/ibatyr-
↪db.dump -d postgres
```

Создайте базу данных

1. На сервере БД подключитесь к PostgreSQL:

```
sudo -u postgres psql
```

2. Создайте базу данных:

```
CREATE DATABASE ibatyr WITH OWNER = ibatyr ENCODING = 'UTF8' LC_COLLATE = 'ru_RU.UTF-8'␣
↪LC_CTYPE = 'ru_RU.UTF-8' TEMPLATE = template0;
```

3. Выберите созданную базу и создайте необходимые расширения:

```
\c ibatyr
CREATE EXTENSION pg_trgm;
CREATE EXTENSION ltree;
CREATE EXTENSION cube;
CREATE EXTENSION dblink;
CREATE EXTENSION pgcrypto;
```

4. Скопируйте все файлы из директории */usr/share/ibatyr/data/ispell/* на сервере iBatyr Monitor в директорию */usr/share/postgresql/15/tsearch_data/*.

   Например, с помощью команды `scp`:

   ```
   scp -r /usr/share/ibatyr/data/ispell/* user@10.10.10.2:/usr/share/postgresql/
   ↪15/tsearch_data/
   ```

   где `user@10.10.10.1`– имя пользователя и ip-адрес сервера iBatyr Monitor, а `user@10.10.10.2` – имя пользователя и адрес сервера с базой данных.

5. Инициализируйте БД на сервере iBatyr Monitor:

   ```
   ibatyr init
   ```

6. Готово! База данных перенесена на выделенный сервер.

Подключите базу данных

1. Выключите сервер iBatyr Monitor:

   ```
   ibatyr stop
   ```

2. Откройте файл конфигурации iBatyr Monitor */etc/ibatyr/config*:

   ```
   sudo vim /etc/ibatyr/config
   ```

   Найдите блок:

   ```
   DATABASES = {
      'default': {
          'ENGINE': 'django.db.backends.postgresql_psycopg2',
          'NAME': 'ibatyr',
          'USER': 'ibatyr',
          'PASSWORD': '05ce255df14c33081437373161396b77',
          'HOST': '',
          'PORT': '',
      }
   }
   ```

   Укажите в HOST и PORT адрес и порт удаленного сервера PostgreSQL, например:

   ```
   DATABASES = {
      'default': {
          'ENGINE': 'django.db.backends.postgresql_psycopg2',
          'NAME': 'ibatyr',
          'USER': 'ibatyr',
          'PASSWORD': '05ce255df14c33081437373161396b77',
          'HOST': '10.10.13.243',
          'PORT': '5432',
      }
   }
   ```

3. Отключите автоматический запуск БД на сервере iBatyr Monitor:

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. Проверьте подключение к БД:

```
ibatyr sql
```

Если нет ошибок и вы видите приглашение от PostgreSQL (`ibatyr=>`), подключение прошло успешно.

Выйдите из приглашения:

```
\q
```

5. Инициализируйте БД:

```
ibatyr init
```

6. Готово! База данных перенесена на выделенный сервер.

3.6.9 Настройка еженедельной очистки базы данных

Автоматическая логическая очистка производится с помощью планировщика задач **Cron**. Последующая физическая очистка и оптимизация дискового пространства запускается вручную через скрипт iBatyr Monitor **compact**.

Примечание: На диске должно быть не менее 15% от объема базы, подробнее — в статье *Ручная очистка диска*.

Логическая очистка

1. Откройте планировщик задач в терминале iBatyr Monitor и запустите **Cron**:

```
sudo crontab -e
```

2. Добавьте строки, чтобы выполнить очистку базы данных. Например, чтобы удалять данные из базы за год каждое 1 число месяца в 23:00.

Примечание: Файлы и события не восстанавливаются, поэтому тщательно проверяйте временной диапазон для удаления перед началом работы. При возникновении вопросов обратитесь *в техническую поддержку*.

```
00 23 1 * * && sudo ibatyr shard cleanup 12 >> /srv/cleanupdb.log 2>&1
```

Команда удаляет шарды в PostgreSQL, партиции в ClickHouse и привязанные к ним файлы. Записывает лог работы в файл /**srv/cleanupdb.log**.

См.также:

Подробнее о шардировании

Оптимизация очищенной базы

Чтобы физически освободить дисковое пространство после очистки базы:

1. Откройте файл скрипта **compact**:

```
sudo nano /usr/share/ibatyr/bin/compact
```

2. В файле раскомментируйте строки **echo «Vacuum database»** и **sudo -u postgres psql ibatyr -c «vacuum full»**, вот так:

```
#!/bin/bash
# USE compact
# HELP Cleanup unreffered dimensions and vaccum database
ibatyr stop
echo "Cleanup dimensions"
cat sql/cleanup_dimensions.sql| bin/sql
echo "Vacuum database"
sudo -u postgres psql ibatyr -c "vacuum full"
ibatyr start
echo "Cleanup done"
bin/info
```

Примечание: При обновлении сервера все скрипты перезаписываются, поэтому внесённые в них изменения исчезают. После следующего обновления сервера повторите настройку.

---

3. Сохраните изменения.
4. После завершения очистки базы запустите скрипт:

```
ibatyr compact
```

Примечание: Оптимизация базы данных может занимать длительное время. Запускайте её в нерабочие или выходные дни.

3.6.10 Шардирование

Начиная с версии iBatyr Monitor 4.7 шардирование поддерживается из коробки.

Принцип работы

Шардирование — принцип проектирования базы данных, при котором логически независимые строки таблицы базы данных хранятся раздельно, заранее сгруппированные в секции. Эти секции, в свою очередь, размещаются на разных, физически и логически независимых серверах базы данных. При этом один физический узел кластера может содержать несколько серверов баз данных.

В iBatyr Monitor шардирование работает следующим образом:

1. Создаётся несколько таблиц, разбитых по месяцам с 1 числа, таблица на следующий месяц и дефолтная таблица (agent_event_default).
2. Таблица текущего месяца заполняется по мере поступления событий.

```
public | agent_event_2019_09_01                | таблица |
public | agent_event_2019_11_01                | таблица |
public | agent_event_2019_12_01                | таблица |
public | agent_event_2020_01_01                | таблица |
public | agent_event_2020_02_01                | таблица |
public | agent_event_2020_03_01                | таблица |
public | agent_event_2020_04_01                | таблица |
public | agent_event_2020_05_01                | таблица |
public | agent_event_2020_06_01                | таблица |
public | agent_event_2020_07_01                | таблица |
public | agent_event_2020_08_01                | таблица |
public | agent_event_2020_09_01                | таблица |
public | agent_event_2020_10_01                | таблица |
public | agent_event_2020_11_01                | таблица |
public | agent_event_default                   | таблица |
```

Примечание: **agent_event_default** — таблица в которую попадают события, не попавшие ни в одну из созданных таблиц. Например, если на агенте выставлено неверное время (месяц, год).

Если **agent_event_default** увеличилась до большого размера, значит где-то возникла проблема или что-то работает некорректно.

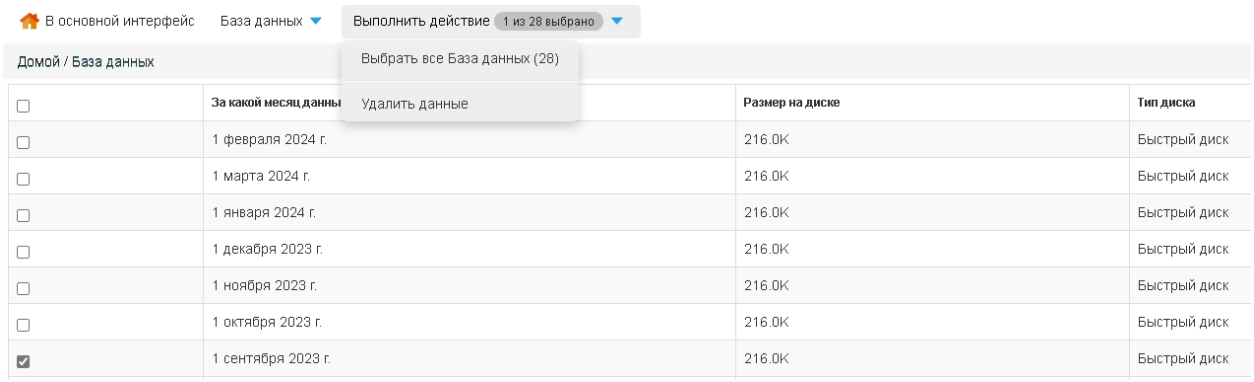
Полезные команды

Список команд, с помощью которых можно произвести диагностику или посмотреть информацию.

Удаление шарда через веб-интерфейс

Примечание: При удалении шарда, будут удалены все файлы, привязанные к указанной таблице.

Удалить шарды в PostgreSQL и ClickHouse можно из веб-интерфейса сервера iBatyr Monitor. Для этого в разделе **Панель управления** — **Базы данных** выберите интересующую вас базу и в выпадающем меню **Выполнить действие** выберите **Удалить данные**.



3.6.11 ETL (Extract, Transform, Load)

Начиная с версии 4.9 в iBatyr Monitor реализован новый механизм загрузки данных(ETL), который позволяет существенно снизить нагрузку на процессор и дисковую подсистему, а также ускорить работу системы.

Примечание: С версии 4.9 работает из коробки, то есть включен по умолчанию при новой установке. Если вы обновили систему с версии 4.8 и ниже, то модуль будет выключен.

Что такое ETL (извлечение, преобразование, загрузка)?

ETL подразумевают миграцию данных из одного приложения/базы данных в аналитическую базу данных. ETL выполняет три шага для передачи данных из базы данных A в базу данных B. Это:

- Извлечение (Extract)
- Преобразование (Transform)
- Загрузка (Load)

Извлечение

Функция извлечения включает в себя процесс чтения данных в базе данных. Этот этап также включает сбор и извлечение данных. В зависимости от типа системы извлечение может происходить несколькими различными способами. Оно может заключаться в извлечении данных в виде плоского файла или просто получения его из API. Это зависит от риска взаимодействия с системой приложений, требований к срокам и ряда других технических ограничений.

Преобразование

Эта функция отвечает за преобразование извлеченных данных в надлежащий формат для анализа и хранения. Такой процесс включает в себя изменение извлеченных данных из их старой структуры в более денормализованный формат. Этот шаг зависит от конечной базы данных. Например, хранилища данных имеют очень специфический шаблон проектирования, который требует изменения данных и реализации медленно меняющихся измерений.

Загрузка

Функция загрузки выполняет процесс записи преобразованных данных в новое приложение /базу данных. Это может занять несколько шагов, так как каждый этап может увеличивать данные по-разному. Стандартная настройка - иметь сырые, промежуточные и производственные базы данных. Существуют и другие конфигурации в зависимости от потребностей проекта.

Как включить ETL после обновления?

Вначале вам необходимо посмотреть *системные требования для нового модуля*. Новый модуль потребляет меньше процессора, но требуется больше оперативной памяти.

Внимание: При миграции будет выполняться множество преобразований в БД. В связи с этим имеется вероятность, что миграция может пройти не успешно. *Обязательно делайте бэкап*. Также рекомендую позвонить в техподдержку и обсудить вопрос миграции.

Если ваш сервер соответствует требованиям, то запускаете команду миграции:

```
screen -S etl
ibatyr migrate etl
```

Скрипт спросит про создание бэкапа. **Обязательно сделайте его, иначе есть возможность потерять данные**.

Дальше начнется процесс миграции, который может занять длительное время.

Если в ходе миграции будут обнаружены ошибки, то система напишет, что необходимо восстановить БД.

3.6.12 Миграция PostgreSQL 11 на PostgreSQL 15

Миграция PostgreSQL 11 на PostgreSQL 15 производится с помощью скрипта *postgresql-upgrade*.
После запуска скрипт:

1. Устанавливает PostgreSQL 15.
2. Переносит данные из текущего кластера.
3. Удаляет PostgreSQL 11 в случае успешного переноса данных.

Миграция данных производится с помощью утилиты *pg_upgrade* от PostgresPRO, входящей в состав скрипта.

См.также:

Документация утилиты pg_upgrade

Предупреждение: *Без резервного копирования* вы рискуете потерять данные.

Системные требования

Операционная система:

- Ubuntu 18.04 LTS,
- Ubuntu 20.04 LTS,
- Ubuntu 22.04 LTS.

База данных:

- Предустановленная PostgreSQL 11.

Примечание: Скрипт производит миграцию путём переназначения файлов данных, дополнительное место не требуется.

Условия миграции

Скрипт сработает при соблюдении условий:

Подготовка

Архивные базы данных

Для переноса архивной базы данных откройте скрипт *postgresql-upgrade* для редактирования:

```
sudo nano /usr/share/ibatyr/bin/postgresql-upgrade
```

Измените переменную ARCHIVED_DATABASES:

- при переносе одной архивной БД:

```
ARCHIVED_DATABASES="archive2023"
```

- при переносе нескольких архивных БД :

```
ARCHIVED_DATABASES="archive_2021 archive_2022 archive_2023"
```

Резервное копирование

Перед запуском скрипта выполните резервное копирование БД с помощью команды:

```
ibatyr backup_db
```

Предупреждение: Без резеврного копирования перед миграцией вы рискуете потерять данные из-за ошибок обновления.

Запуск скрипта

1. Запустите в терминале скрипт командой:

   ```
   sudo ibatyr postgresql upgrade
   ```

   Скрипт автоматически проверит совместимость старого и нового кластеров PostgreSQL с помощью утилиты *pg_ upgrade*.

2. После успешной проверки скрипт запросит подтверждение перед обновлением PostgreSQL:

   ```
   *** WARNING! You are really want to run Postgres upgrade script (type 'yes')?
   ```

   Введите *yes*, чтобы начать миграцию кластера PostgreSQL 11 на версию 15.

Завершение миграции

Установка завершена

Скрипт удалит PostgreSQL 11 и предложит перезапустить iBatyr Monitor командой:

```
ibatyr init
```

Время перезапуска зависит от объема базы.

Ошибки при установке

Перейдите в журнал действий *pg_ upgrade* для просмотра логов:

```
cd /var/lib/postgresql/15/main/pg_upgrade_output.d
```

При возникновении вопросов обратитесь *в техподдержку*.

3.6.13 Ошибка invalid tablespace location при миграции на PostgreSQL 15

Проблема

При миграции на PostgreSQL 15 возникает ошибка неправильного расположения архивной базы данных:

```
ERROR: invalid tablespace location: /var/lib/postgresql/11/archive_2023 (name=archive_
↪2023, owner=postgres)
```

Причина

Симлинк на архивные БД создан по устаревшей инструкции и находится в путях старого кластера */var/lib/postgresql/11/*.

Выясните расположение БД:

1. Запустите SQL:

   ```
   ibaytr sql
   ```

2. В psql-консоли выполните запрос в SQL:

   ```
   SELECT spcname AS "Name", pg_catalog.pg_get_userbyid(spcowner) AS "Owner", pg_
   ↪catalog.pg_tablespace_location(oid) AS "Location" FROM pg_catalog.pg_tablespace␣
   ↪ORDER BY 1;
   ```

   Пример вывода:

   ```
    Name          |  Owner   |              Location
   --------------+----------+-------------------------------------
    archive_2023 | postgres | /var/lib/postgresql/11/archive_2023
    pg_default   | postgres |
    pg_global    | postgres |
    (3 строки)

    ibatyrr=>
   ```

База данных *archive_2023* находится в старом кластере */var/lib/postgresql/11/*.

Решение

Пересоздайте симлинк на смонтированный том.

1. Остановите PostgreSQL:

```
sudo systemctl stop postgresql@11-main
```

2. Узнайте имя текущего симлинка на архивную БД, в нашем случае — *archive_2023*:

```
sudo ls -l /var/lib/postgresql/11/main/pg_tblspc
total 0
lrwxrwxrwx 1 postgres postgres 35 июн  3 22:18 24939407 -> /var/lib/postgresql/11/
↪archive_2023
```

3. Удалите симлинк:

```
sudo rm /var/lib/postgresql/11/main/pg_tblspc/24939407
```

4. Проверьте, что всё удалилось:

```
sudo ls -l /var/lib/postgresql/11/main/pg_tblspc
```

5. Создайте новый симлинк:

```
sudo ln -sf /mnt/archive_2023/ /var/lib/postgresql/11/main/pg_tblspc/24939407
```

6. Убедитесь, что симлинк создан и ведет к нужному каталогу:

```
sudo ls -l /var/lib/postgresql/11/main/pg_tblspc
total 0
lrwxrwxrwx 1 root root 18 июл  1 18:41 24939407 -> /mnt/archive_2023/
```

7. Возобновите работу PostgreSQL:

```
sudo systemctl start postgresql@11-main
```

8. Вновь войдите в консоль psql и проверьте все тейблспейсы:

```
ibatyr sql

ibatyr sql
psql (11.20 (Ubuntu 11.20-1.pgdg18.04+1))
```

9. Получите справку:

```
help
```

Пример вывода:

```
ibatyr=> SELECT spcname AS "Name", pg_catalog.pg_get_userbyid(spcowner) AS "Owner",␣
↪pg_catalog.pg_tablespace_location(oid) AS "Location" FROM pg_catalog.pg_
↪tablespace ORDER BY 1;
```

(continues on next page)

(продолжение с предыдущей страницы)

```
     Name     |  Owner   |      Location
--------------+----------+--------------------
 archive_2023 | postgres | /mnt/archive_2023/
 pg_default   | postgres |
 pg_global    | postgres |
(3 строки)

ibatyr=>
```

Теперь БД расположена в правильном каталоге — */mnt/archive_ 2023/*.

3.6.14 Инкрементальные бэкапы PostgreSQL в pgBackRest

Инкрементальные бэкапы PostgreSQL в pgBackRest — метод резервного копирования, который позволяет сохранять только измененные данные с момента последнего полного или инкрементального бэкапа. Помогает экономить место на диске и уменьшает время выполнения резервного копирования.

Ссылки на ресурсы:

- Репозиторий утилиты pgBackRest
- Сайт pgBackRest
- Документация утилиты

Вы можете установить pgBackRest с помощью *команд* или *скрипта*.

Установка pgBackRest

Выберите один из способов установки:

- через репозиторий,
- из исходников.

Установка из репозитория

```
sudo apt install pgbackrest postgresql-client
```

Установка из исходников

В Astra Linux нет пакета для установки pgBackRest, поэтому соберите его из исходников.

Примечание: На успешный результат влияет точная установка времени. Рекомендуем ознакомиться с официальной документацией Astra Linux.

---

1. Сначала убедитесь, что у вас установлен Perl:

   ```
   apt list perl
   ```

2. Установите пакеты.

В официальной документации по сборке указаны пакеты:

```
meson gcc libpq-dev libssl-dev libxml2 libxml2-dev pkg-config liblz4-dev␣
↪libzstd-dev libbz2-dev libz-dev libyaml-dev libssh2 libssh2-1-dev postgresql-
↪client
```

Убедитесь, что все пакеты есть в репозитории Astra Linux:

```
for pkg in meson gcc libpq-dev libssl-dev libxml2 libxml2-dev pkg-config␣
↪liblz4-dev libzstd-dev libbz2-dev libz-dev libyaml-dev libssh2 libssh2-1-dev␣
↪postgresql-client; do apt-cache show "$pkg" > /dev/null 2>&1 && echo "$pkg:␣
↪найден" || echo "$pkg: не найден"; done
```

Вывод:

```
meson: найден
gcc: найден
libpq-dev: найден
libssl-dev: найден
libxml2: найден
libxml2-dev: найден
pkg-config: найден
liblz4-dev: найден
libzstd-dev: найден
libbz2-dev: найден
libz-dev: найден
libyaml-dev: найден
libssh2: не найден
libssh2-1-dev: найден
postgresql-client: найден
```

В ненайденном пакете *libssh2* есть уязвимость. Описание на сайте ФСТЭК .

По всей видимости, пакет исправлен и сменил название на *libssh2-1*:

```
provisor@astr-sce54:~$ sudo apt search libssh
Сортировка… Готово
Полнотекстовый поиск… Готово
libssh-4/stable 0.9.7-0+deblllul amd64
  tiny C SSH library (OpenSSL flavor)

libssh-dev/stable 0.9.7-0+deblllul amd64
  tiny C SSH library - Development files (OpenSSL flavor)

libssh-doc/stable 0.9.7-0+deblllul all
  tiny C SSH library - Documentation files

libssh-gcrypt-4/stable,now 0.9.7-0+deblllul amd64 [установлен, автоматически]
  tiny C SSH library (gcrypt flavor)

libssh-gcrypt-dev/stable 0.9.7-0+deblllul amd64
  tiny C SSH library - Development files (gcrypt flavor)

libssh2-1/stable,now 1.11.0-2 amd64 [установлен, автоматически]
  SSH2 client-side library

libssh2-1-dev/stable 1.11.0-2 amd64
  SSH2 client-side library (development headers)

php-ssh2/stable 1.1.2+0.13-4 amd64
  Bindings for the libssh2 library
```

Соберите pgBackRest без *libssh2*, потому что он уже установлен:

```
sudo apt install meson gcc libpq-dev libssl-dev libxml2 libxml2-dev pkg-config␣
↪liblz4-dev libzstd-dev libbz2-dev libz-dev libyaml-dev libssh2-1-dev␣
↪postgresql-client
```

Сборка pgBackRest

Используйте для сборки систему сборки Meson и Ninja.

1. Соберите версию, которая используется в репозиториях Ubuntu:

```
sudo mkdir /build && cd /build
sudo wget https://github.com/pgbackrest/pgbackrest/archive/refs/tags/release/2.
↪53.tar.gz
sudo tar -xvf 2.53.tar.gz
sudo meson setup /build/pgbackrest /build/pgbackrest-release-2.53/
sudo ninja -C /build/pgbackrest
```

Пример вывода при успешной сборке и компиляции:

```
provisor@iBatyr Monitor-54:/build$ sudo meson setup /build/pgbackrest /build/
↪pgbackrest-release-2.53/
The Meson build system
Version: 0.53.2
Source dir: /build/pgbackrest-release-2.53
Build dir: /build/pgbackrest
Build type: native build
WARNING: Unknown options: "unity_size"
```

(continues on next page)

(продолжение с предыдущей страницы)

```
Project name: pgbackrest
Project version: 2.53
C compiler for the host machine: cc (gcc 9.4.0 "cc (Ubuntu 9.4.0-1ubuntu1~20.
↪04.2) 9.4.0")
C linker for the host machine: cc ld.bfd 2.34
Host machine cpu family: x86_64
Host machine cpu: x86_64
Compiler for C supports arguments -Wconversion: YES
Compiler for C supports arguments -Wduplicated-cond: YES
Compiler for C supports arguments -Wduplicated-branches: YES
Compiler for C supports arguments -Wformat-nonliteral: YES
Compiler for C supports arguments -Wformat=2: YES
Compiler for C supports arguments -Wformat-signedness: YES
Compiler for C supports arguments -Wpointer-arith: YES
Compiler for C supports arguments -Wstrict-prototypes: YES
Compiler for C supports arguments -Wvla: YES
Compiler for C supports arguments -Wwrite-strings: YES
Compiler for C supports arguments -Wno-clobbered -Wclobbered: YES
Compiler for C supports arguments -Wno-missing-field-initializers -Wmissing-
↪field-initializers: YES
Compiler for C supports arguments -Wno-implicit-fallthrough -Wimplicit-
↪fallthrough: YES
Compiler for C supports arguments -funroll-loops: YES
Compiler for C supports arguments -ftree-vectorize: YES
Program python3 found: YES (/usr/bin/python3)
Compiler for C supports arguments -fmacro-prefix-map=../pgbackrest-release-2.
↪53/src/=: YES
Compiler for C supports arguments -fmacro-prefix-map=../pgbackrest-release-2.
↪53/test/src/=test/: YES
Library backtrace found: YES
Library bz2 found: YES
Found pkg-config: /usr/bin/pkg-config (0.29.1)
Run-time dependency liblz4 found: YES 1.9.2
Run-time dependency openssl found: YES 1.1.1f
Run-time dependency libpq found: YES 16.4
Run-time dependency libxml-2.0 found: YES 2.9.10
Run-time dependency yaml-0.1 found: YES 0.2.2
Run-time dependency zlib found: YES 1.2.11
Run-time dependency libssh2 found: YES 1.8.0
Run-time dependency libzstd found: YES 1.4.4
Configuring build.auto.h using configuration
Configuring build.auto.h using configuration
Configuring build.auto.h using configuration
Build targets in project: 10

Found ninja-1.10.0 at /usr/bin/ninja

provisor@iBatyr Monitor-54:/build$ sudo ninja -C /build/pgbackrest
ninja: Entering directory `/build/pgbackrest'
[250/250] Linking target src/pgbackrest.
```

2. Перенесите полученый бинарный файл:

```
sudo cp /build/pgbackrest/src/pgbackrest /usr/bin/
sudo chmod 755 /usr/bin/pgbackrest
```

3. Создайте директории для конфигурационных файлов и логов:

```
sudo mkdir -p -m 770 /var/log/pgbackrest && sudo chown postgres:postgres /var/
↪log/pgbackrest && sudo mkdir -p /etc/pgbackrest && sudo mkdir -p /etc/
↪pgbackrest/conf.d && sudo touch /etc/pgbackrest/pgbackrest.conf && sudo␣
↪chmod 640 /etc/pgbackrest/pgbackrest.conf && sudo chown postgres:postgres /
↪etc/pgbackrest/pgbackrest.conf
```

4. Создайте директории для репозитория бекапов.

Предупреждение: Директории указаны для примера. Вы можете указать свои директории, либо примонтировать к указанным директориям накопители для резервных копий.

```
sudo mkdir -p /var/lib/pgbackrest
sudo chmod 750 /var/lib/pgbackrest
sudo chown postgres:postgres /var/lib/pgbackrest
```

Проверка установки

Проверьте установку:

```
sudo -u postgres pgbackrest
```

Вывод:

```
pgBackRest 2.53 - General help

Usage:
pgbackrest [options] [command]

Commands:
annotate Add or modify backup annotation.
archive-get Get a WAL segment from the archive.
archive-push Push a WAL segment to the archive.
backup Backup a database cluster.
check Check the configuration.
expire Expire backups that exceed retention.
help Get help.
info Retrieve information about backups.
repo-get Get a file from a repository.
repo-ls List files in a repository.
restore Restore a database cluster.
server pgBackRest server.
server-ping Ping pgBackRest server.
stanza-create Create the required stanza data.
stanza-delete Delete a stanza.
```

(continues on next page)

(продолжение с предыдущей страницы)

```
stanza-upgrade Upgrade a stanza.
start Allow pgBackRest processes to run.
stop Stop pgBackRest processes from running.
verify Verify contents of the repository.
version Get version.

Use 'pgbackrest help [command]' for more information.
```

Если ошибок нет, pgBackRest установлен корректно.

Настройка pgBackRest

Отредактируйте конфигурационный файл */etc/pgbackrest/pgbackrest.conf* в удобном для вас редакторе.

Предупреждение: Будьте внимательны при редактировании файла. Версии PostgreSQL могут отличаться.

```
[demo]
pg1-path=/var/lib/postgresql/15/main

[global]
repo1-path=/var/lib/pgbackrest
repo1-retention-full=2

[global:archive-push]
compress-level=3
```

Настройка PostgreSQL

1. Добавьте строки в конец файла */etc/postgresql/15/main/postgresql.conf*. Крайне рекомендуется добавить комментарий, чтобы в будущем было понятно, зачем были внесены эти изменения.

   ```
   #2.09.2024 settings for incremental backup. System administrator Ivanov I.
   archive_command = 'pgbackrest --stanza=demo archive-push %p'
   archive_mode = on
   max_wal_senders = 3
   wal_level = replica
   ```

2. Перезапустите PostgreSQL:

   ```
   sudo systemctl restart postgresql
   ```

3. Убедитесь, что PostgreSQL запустился после внесения изменений в конфигурационный файл:

   ```
   sudo systemctl status postgresql
   ```

   Корректный вывод:

```
provisor@astr-sce54:/build$ sudo systemctl status postgresql
 postgresql.service - PostgreSQL RDBMS
Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor␣
↪preset: enabled)
Active: active (exited) since Mon 2024-09-02 17:15:48 +07; 9s ago
Process: 3903 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
Main PID: 3903 (code=exited, status=0/SUCCESS)
    CPU: 7ms

сен 02 17:15:48 astr-sce54 systemd[1]: Starting PostgreSQL RDBMS...
сен 02 17:15:48 astr-sce54 systemd[1]: Started PostgreSQL RDBMS.
```

Запуск пакета pgBackRest для кластера

1. Используйте команду для запуска:

```
sudo -u postgres pgbackrest --stanza=your_stanza_name --log-level-console=info␣
↪stanza-create
```

Примечание: `stanza` — конфигурация кластера баз данных PostgreSQL, которая определяет месторасположение кластера. способ создания резервной копии, параметры архивирования и т. д. Большинство серверов БД имеют только один кластер базы данных PostgreSQL и, следовательно, один *stanza*. В то же время, серверы резервного копирования могут иметь отдельную конфигурацию `stanza` для каждого кластера баз данных, который они обслуживают.

В приведенной команде используется `your_stanza_name` в качестве имени для конфигурации `stanza`.

Не называйте `stanza` именем основного кластера. Более подходящее название описывает базы данных, которые входят в кластер. Поскольку имя `stanza` используется для первичной и всех реплик, более уместно выбрать имя, которое описывает фактическую функцию кластера. Например `app` или `dw` вместо имени локального кластера вроде `main` или `prod`.

Вывод:

```
sudo -u postgres pgbackrest --stanza=demo --log-level-console=info stanza-
↪create
2024-05-28 13:20:12.820 P00 INFO: stanza-create command begin 2.51: --exec-
↪id=40337-0602407f --log-level-console=info --pg1-path=/var/lib/postgresql/15/
↪main --repo1-path=/var/lib/pgbackrest --stanza=demo
2024-05-28 13:20:13.626 P00 INFO: stanza-create for stanza 'demo' on repo1
2024-05-28 13:20:13.633 P00 INFO: stanza-create command end: completed␣
↪successfully (814ms)
```

2. Проверьте созданный репозиторий:

```
sudo -u postgres pgbackrest --stanza=demo --log-level-console=info check
```

Вывод:

```
sudo -u postgres pgbackrest --stanza=demo --log-level-console=info check 2024-
↪05-28 13:24:03.434 P00 INFO: check command begin 2.51: --exec-id=40938-
↪d6c55df1 --log-level-console=info --pg1-path=/var/lib/postgresql/15/main --
↪repo1-path=/var/lib/pgbackrest --stanza=demo 2024-05-28 13:24:04.041 P00␣
↪INFO: check repo1 configuration (primary) 2024-05-28 13:24:04.443 P00 INFO:␣
↪check repo1 archive for WAL (primary) 2024-05-28 13:24:04.443 P00 INFO: WAL␣
↪segment 000000010000000300000000B9 successfully archived to '/var/lib/
↪pgbackrest/archive/demo/15-1/0000000100000003/000000010000000300000000B9-
↪f099b13a5bce53307041b204c4 edd5215e2402b0.gz' on repo1 2024-05-28 13:24:04.
↪444 P00 INFO: check command end: completed successfully (1011ms)
```

Создание бэкапа

Инкрементное резервное копирование должно основываться на полной резервной копии. Поскольку полной резервной копии не существует, нужно ее сделать. На время создания бекапа отстановите прием данных от агента.

Предупреждение: Перед бекапом крайне важно завершить работу iBatyr Monitor и убедиться, что все процессы остановлены. Дело в том, даже после запрета приема данных от агентов через Iptables или через остановку Nginx внутри могут продолжаться процессы ETL, которые изменят состояние БД.

1. Остановите передачу данных на сервер iBatyr Monitor:

   ```
   ibatyr stop
   ```

2. Сделайте полный бэкап — это первая полная копия всех данных, которая служит основой для будущих инкрементальных резервных копий:

   ```
   sudo -u postgres pgbackrest --stanza=demo --type=full backup
   ```

3. Создайте инкрементальный бэкап — резервное копирование только тех изменений, которые произошли с момента последнего полного бэкапа:

   ```
   sudo -u postgres pgbackrest --stanza=demo--type=incr backup
   ```

Дополнительные выводы

pgBackRest поддерживает расширенный вывод при создании резервных копий, что позволяет получить более детальную информацию о процессе. В предыдущих примерах не был указан дополнительный вывод, но его можно добавить для более информативного мониторинга.

Используйте параметр `--log-level-console` для управления уровнем детализации вывода в консоль.

Основные уровни логирования, которые вы можете использовать:

- `error`: показывает только ошибки.
- `warn`: показывает предупреждения и ошибки.
- `info`: показывает информационные сообщения, предупреждения и ошибки.

- `detail`: показывает детализированные сообщения, информационные сообщения, предупреждения и ошибки.
- `debug`: показывает отладочные сообщения, детализированные сообщения, информационные сообщения, предупреждения и ошибки.
- `trace`: показывает трассировочные сообщения, отладочные сообщения, детализированные сообщения, информационные сообщения, предупреждения и ошибки.

Примеры уровней логирования

Если вы хотите создать резервную копию с расширенным выводом, рекомендуется использовать уровень `detail` или `debug`.

Уровень `detail`

```
sudo pgbackrest --stanza=your_stanza_name --log-level-console=detail backup
```

Уровень `debug`

Для большей детализации используйте `debug`:

```
sudo pgbackrest --stanza=your_stanza_name --log-level-console=debug backup
```

Уровень `trace`

Используйте `trace` для максимального уровня детализации:

```
sudo pgbackrest --stanza=your_stanza_name --log-level-console=trace backup
```

Настройка уровня логирования в конфигурационном файле

Вместо выполнения команды можете задать уровень логирования в конфигурационном файле *pgbackrest.conf*. Например:

```
[global]
log-level-console=detail
```

Просмотр бэкапа

Для просмотра бэкапа выполните:

```
sudo -u postgres pgbackrest info
```

Вывод:

```
sudo -u postgres pgbackrest info
stanza: demo
status: ok
cipher: none

db (current)
wal archive min/max (15): 000000010000000300000088/0000000100000003000000BD

full backup: 20240528-132503F
timestamp start/stop: 2024-05-28 13:25:03+07 / 2024-05-28 13:25:39+07
wal start/stop: 000000010000000300000088 / 000000010000000300000088
database size: 98.9MB, database backup size: 98.9MB
repo1: backup set size: 16.8MB, backup size: 16.8MB

incr backup: 20240528-132503F_20240528-133032I
timestamp start/stop: 2024-05-28 13:30:32+07 / 2024-05-28 13:30:40+07
wal start/stop: 0000000100000003000000BD / 0000000100000003000000BD
database size: 99.0MB, database backup size: 16.1MB
repo1: backup set size: 16.8MB, backup size: 4.2MB
backup reference list: 20240528-132503F
```

Восстановление из инкрементального бекапа

1. Восстановите из БД из последнего бэкапа.

   Посмотрите, какие кластеры есть и какие у них имена:

   ```
   pg_lsclusters
   ```

   Остановите кластер:

   ```
   sudo pg_ctlcluster 15 main stop
   ```

   На всякий случай проверьте, что кластер остановлен:

   ```
   pg_lsclusters
   ```


   Приступите к восстановлению. Для начала посмотрите, какие копии есть:

   ```
   sudo -u postgres pgbackrest info
   ```

   Вывод:

   ```
   stanza: demo
       status: ok
       cipher: none

       db (current)
           wal archive min/max (15): 000000010000000300000088/
   ```

(continues on next page)

(продолжение с предыдущей страницы)

```
↪000000010000000300000C2

       full backup: 20240528-132503F
           timestamp start/stop: 2024-05-28 13:25:03+07 / 2024-05-28␣
↪13:25:39+07
           wal start/stop: 000000010000000300000BB / 000000010000000300000BB
           database size: 98.9MB, database backup size: 98.9MB
           repo1: backup set size: 16.8MB, backup size: 16.8MB

       incr backup: 20240528-132503F_20240528-133032I
           timestamp start/stop: 2024-05-28 13:30:32+07 / 2024-05-28␣
↪13:30:40+07
           wal start/stop: 000000010000000300000BD / 000000010000000300000BD
           database size: 99.0MB, database backup size: 16.1MB
           repo1: backup set size: 16.8MB, backup size: 4.2MB
           backup reference list: 20240528-132503F

       incr backup: 20240528-132503F_20240528-143603I
           timestamp start/stop: 2024-05-28 14:36:03+07 / 2024-05-28␣
↪14:36:11+07
           wal start/stop: 000000010000000300000BF / 000000010000000300000BF
           database size: 99.0MB, database backup size: 16.5MB
           repo1: backup set size: 16.8MB, backup size: 4.2MB
           backup reference list: 20240528-132503F, 20240528-132503F_20240528-
↪133032I

       incr backup: 20240528-132503F_20240528-152508I
           timestamp start/stop: 2024-05-28 15:25:08+07 / 2024-05-28␣
↪15:26:51+07
           wal start/stop: 000000010000000300000C2 / 000000010000000300000C2
           database size: 114.8MB, database backup size: 77.8MB
           repo1: backup set size: 21.3MB, backup size: 17.8MB
           backup reference list: 20240528-132503F, 20240528-132503F_20240528-
↪133032I, 20240528-132503F_20240528-143603I
```

Восстановите БД из последнего полного бекапа:

```
sudo -u postgres pgbackrest --stanza=demo --log-level-console=info --delta␣
↪restore
```

Восстановитесь к инкрементальному бэкапу. Обратите внимание, что пути могут отличаться.

```
ibatyr stop
sudo systemctl stop postgresql
rm -rf /var/lib/postgresql/11/main/*
sudo -u postgres pgbackrest --stanza=ibatyr --log-level-console=info restore --
↪set=20240929-132900F_20240929-134211I --type=time "--target=2024-09-29␣
↪13:42:11+03"
```

Бэкап восстановлен, `pg_wal` «перемотана» до даты нужного инкрементального бэкапа. БД доступна только в режиме чтения.

Проверка бэкапа

1. Зайдите в PostgreSQL и выполните:

```
sudo systemctl start postgresql
sudo -u postgres psql
select pg_wal_replay_resume();
```

2. Запустите кластер:

```
sudo pg_ctlcluster 15 main start
```

3. Убедитесь, что кластер запущен:

```
pg_lsclusters
```

4. Запустите iBatyr Monitor:

```
sudo ibatyr start
```

5. Посмотрите информацию о восстановлении в логах:

```
sudo -u postgres cat /var/lib/postgresql/15/demo/postgresql.auto.conf
cat: /var/lib/postgresql/15/demo/postgresql.auto.conf: No such file or␣
↪directory
sudo -u postgres cat /var/lib/postgresql/15/main/postgresql.auto.conf
# Do not edit this file manually!
# It will be overwritten by the ALTER SYSTEM command.

# Recovery settings generated by pgBackRest restore on 2024-05-28 15:50:57
restore_command = 'pgbackrest --stanza=demo archive-get %f "%p"'
recovery_target_time = '2024-05-28 15:26:51+07'
recovery_target_action = 'promote'
```

Скрипт для автоматизации

Альтернативно вы можете использовать скрипт.

1. Сохраните скрип в тестовом файле на вашем сервере. Назовите файл *backup-and-restore.sh*.

```
#! /bin/bash

RED="\e[31m"
GREEN="\e[32m"
NORM="\e[0m"

# Определение системного языка
USELANG=0
if [ $(echo ${LANG/_/-} | grep -Ei "\\b(ru|RU)\\b") ]; then USELANG=1; fi

# Определение функции echo с поддержкой вывода на нескольких языках
function echo2(){
if [ $USELANG == 1 ]; then
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    echo -e $1; #Show Russian
else
    echo -e $2; #Show English
fi
}

#you root?
UID_ROOT=0
if [ "$UID" -ne "$UID_ROOT" ]; then
echo2 "${RED}Эта операция может быть выполнена только пользователем root${NORM}
↪" "${RED}This operation can only be performed by the root user${NORM}"
exit 1
fi

if [ -e /etc/pgbackrest.conf ]; then
DB=$(grep pg1-path /etc/pgbackrest.conf | sed -e 's/pg1-path=\/var\/lib\///g')
elif [ -e /etc/pgbackrest/pgbackrest.conf ]; then
DB=$(grep pg1-path /etc/pgbackrest/pgbackrest.conf | sed -e 's/pg1-path=\/var\/
↪lib\///g')
else
echo2 "${RED}pgbackrest не установлен, либо не настроен.${NORM}" "${RED}
↪pgbackrest not installed or misconfigured.${NORM}"
exit 1
fi

STANZA=$(grep stanza /etc/$DB/postgresql.conf | sed -e 's/^.*=//g' -e 's/ .*//g
↪')
BACKUPS=$(sudo -u postgres pgbackrest info | grep 'backup:' | sed -e 's/^.
↪*backup: //g')
COUNT=$(sudo -u postgres pgbackrest info | grep -c 'backup:')

echo2 "${GREEN}Количество точек восстановления: $COUNT${NORM}" "${GREEN}Number␣
↪of recovery points: $COUNT${NORM}"

function error() {
    echo2 "Не могу распознать ответ '$var1'" "Can't recognize the answer '$var1
↪'"
    echo2 "Введите Y или N" "Enter Y or N"
}

function todo_dialog(){
    echo2 "${RED}Создать новую точку восстановления? y/n${NORM}" "${RED}Create␣
↪a new recovery point? y/n${NORM}"
    read var1
    case $var1 in
        Y)
        backup_dialog
        ;;
        y)
        backup_dialog
        ;;
        N)
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        restore_dialog
        ;;
        n)
        restore_dialog
        ;;
        *)
        error
        todo_dialog
        ;;
    esac
}

function backup_dialog(){
    if [ $COUNT >0 ]; then
    echo2 "${RED}Создать новый инкрементальный бэкап?. y/n${NORM}" "${RED}
↪Create an incremental backup?. y/n${NORM}"
    echo2 "${RED}(Нет = создать новый полный бэкап.)${NORM}" "${RED}(No =␣
↪create a new full backup.)${NORM}"
    read var1
    case $var1 in
        Y)
        TYPE=incr
        backup
        ;;
        y)
        TYPE=incr
        backup
        ;;
        N)
        TYPE=full
        backup
        ;;
        n)
        TYPE=full
        backup
        ;;
        *)
        error
        backup_dialog
        ;;
    esac
    else
    echo2 "${GREEN}Не найдено ни одной точки восстановления. Будет создан␣
↪полный бэкап.${NORM}" "${GREEN}No recovery points found. A full backup will␣
↪be created.${NORM}"
    TYPE=full
    backup
    fi
}

function backup(){
    echo2 "${RED}Создание точки восстановления: $TYPE backup${NORM}" "${RED}
```

(continues on next page)

(продолжение с предыдущей страницы)

```
↪Creating recovery point: $TYPE backup${NORM}"
    ibatyr stop
    echo "select max(id) from agent_event;select count(*) from agent_event;" |␣
↪ibatyr sql
    sudo -u postgres pgbackrest --stanza=$STANZA --type=$TYPE backup
    ibatyr start
}

function restore_dialog(){
    if [ $COUNT >0 ]; then
    echo2 "${RED}Восстановить БД из бэкапа? y/n${NORM}" "${RED}Restore DB from␣
↪a backup? y/n${NORM}"
    read var1
    case $var1 in
        Y)
        restore_prepare
        ;;
        y)
        restore_prepare
        ;;
        N)
        exit 0
        ;;
        n)
        exit 0
        ;;
        *)
        error
        restore_dialog
        ;;
    esac
    else
    echo2 "${RED}Не найдено ни одной точки восстановления.${NORM}" "${RED}No␣
↪recovery points found.${NORM}"
    todo_dialog
    fi
}

function select_restorepoint(){
    sudo -u postgres pgbackrest info
    echo2 "${RED}Нажмите кнопку от [ 1 ] до [ $COUNT ] для выбора точки␣
↪восстановления.${NORM}" "${RED}Press button from [ 1 ] to [ $COUNT ] to␣
↪select a recovery point.${NORM}"
    echo2 "${RED}Или любую другую кнопку для выхода из режима восстановления...
↪${NORM}" "${RED}Or any other button to exit recovery process...${NORM}"
    read var1
    if ((var1 >= 1 && var1 <= COUNT)); then
        SELECTPOINT=$(sudo -u postgres pgbackrest info | grep -m$var1 'backup:
↪' | tail -n1 | sed -e 's/^.*backup: //g')
        SELECTTARGET=$(sudo -u postgres pgbackrest info | grep -m$var1
↪'timestamp start/stop:' | tail -n1 | sed -e 's/^.*stop: //g' -e 's/ \/.*//g')
    else
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        exit 0
    fi
}

function restore_prepare(){
    if [ -e /etc/pgbackrest.conf ]; then
    DBNAME=$(grep pg1-path /etc/pgbackrest.conf | sed -e 's/.*\///g')
    DBVER=$(grep pg1-path /etc/pgbackrest.conf | sed -e 's/.*\/1/1/g' -e 's/\/.
↪*//g')
    else
    DBNAME=$(grep pg1-path /etc/pgbackrest/pgbackrest.conf | sed -e 's/.*\///g
↪')
    DBVER=$(grep pg1-path /etc/pgbackrest/pgbackrest.conf | sed -e 's/.*\/1/1/g
↪' -e 's/\/.*//g')
    fi
    select_restorepoint
    echo2 "${RED}Выбранная точка [ $SELECTPOINT ] [ $SELECTTARGET ]. Начать␣
↪восстановление? y/n${NORM}" "${RED}Selected point [ $SELECTPOINT ] [
↪$SELECTTARGET ]. Proceed recovery? y/n${NORM}"
    read var1
    case $var1 in
        Y)
        restore
        ;;
        y)
        restore
        ;;
        N)
        select_restorepoint
        ;;
        n)
        select_restorepoint
        ;;
        *)
        error
        select_restorepoint
        ;;
    esac
}

function restore(){
    ibatyr stop
    pg_ctlcluster $DBVER $DBNAME stop
    if [ $(pg_lsclusters | grep -c down) != 0 ]; then
    systemctl stop postgresql
    sudo -u postgres rm -rf /var/lib/$DB/*
    sudo -u postgres pgbackrest --stanza=$STANZA --log-level-console=info␣
↪restore --set=$SELECTPOINT --type=time "--target=$SELECTTARGET"
    systemctl start postgresql
    echo "select pg_wal_replay_resume();" | sudo -u postgres psql
    pg_ctlcluster $DBVER $DBNAME start
    if [ $(pg_lsclusters | grep -c online) != 0 ]; then
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        echo "select max(id) from agent_event;select count(*) from agent_event;
↪" | ibatyr sql
        ibatyr start
        echo2 "${GREEN}БД успешно восстановлена.${NORM}" "${GREEN}DB recovered␣
↪successfully.${NORM}"
    else
        echo2 "${RED}Возникла непредвиденная ошибка во время восстановления БД.
↪${NORM}" "${RED}An unexpected error occured during DB recovery.${NORM}"
        pg_lsclusters
        exit 1
    fi
    else
    pg_lsclusters
    echo2 "${RED}ОШИБКА. Кластер не остановлен. Восстановление в данный момент␣
↪невозможно.${NORM}" "${RED}ERROR. Cluster is not stopped. Recovery is not␣
↪possible at the moment.${NORM}"
    echo2 "Попробуйте перезапустить скрипт позже." "Try restarting the script␣
↪later."
    exit 1
    fi
}

todo_dialog
exit 0
```

2. Сделайте скрипт исполняемым:

```
chmod +x backup-and-restore.sh
```

3. Запустите скрипт:

```
sudo ./backup-and-restore.sh
```

4. Следуйте инструкциям на экране.

3.6.15 Автоматическое определение версии локальной базы данных

После выполнения команды `ibatyr init` автоматически заполняется файл конфигурации базы данных */etc/ibatyr/db_profile*.

Определение настроек происходит для баз данных:

- PostgreSQL 11,
- PostgreSQL 15,

Например, для PostgreSQL 15 он имеет вид:

```
PSQL_VERSION=15
PSQL_BIN_DIR=/usr/lib/postgresql/15/bin
```

(continues on next page)

(продолжение с предыдущей страницы)

```
PSQL_LIB_DIR=/usr/lib/postgresql/15/lib
PSQL_SHARE_DIR=/usr/share/postgresql/15
PSQL_CONF_PATH=/etc/postgresql/15/main/postgresql.conf
PSQL_DATA_DIR=/var/lib/postgresql/15/main
PSQL_HBA_PATH=/etc/postgresql/15/main/pg_hba.conf
PSQL_TSEARCH_DIR=/usr/share/postgresql/15/tsearch_data
PSQL_HYPERSCAN=hyperscan.so.15
PSQL_SERVICE=postgresql
```

Изменение файла

При изменении локальной базы или версии базы рекомендуем сделать копию файла *db_profile*, чтобы сохранить старые настройки. Добавьте в название версию базы данных и сделайте бэкап. Затем удалите исходный файл вручную, потому что он не удаляется автоматически.

После изменения файла перезапустите сервер:

```
ibatyr restart
```

При выполнении команды `ibatyr init` система создаст новый файл *db_profile* с актуальными настройками.

Удаленная база данных

Если при переносе БД на удаленный хостинг стандартные пути не меняются, файл *db_profile* можно оставить без изменений.

Если база другая — например, версия PostgreSQL отличается, — укажите в файле *db_profile* правильные настройки вручную. Это связано с тем, что при работе с удаленным сервером система не может автоматически определить все пути и настройки, как это происходит для локальной базы данных.

После внесения изменений в файл перезапустите сервер:

```
ibatyr restart
```

Стандартные настройки баз данных

Используйте эти настройки при изменении файла *db_profile*.

Примечание: Важно указать правильную версию Hyperscan, потому что она зависит от версии вашей базы данных.

PostgreSQL 11

```
PSQL_VERSION=11
PSQL_BIN_DIR=/usr/lib/postgresql/11/bin
PSQL_LIB_DIR=/usr/lib/postgresql/11/lib
PSQL_SHARE_DIR=/usr/share/postgresql/11
PSQL_CONF_PATH=/etc/postgresql/11/main/postgresql.conf
PSQL_DATA_DIR=/var/lib/postgresql/11/main
PSQL_HBA_PATH=/etc/postgresql/11/main/pg_hba.conf
PSQL_TSEARCH_DIR=/usr/share/postgresql/11/tsearch_data
PSQL_HYPERSCAN=hyperscan.so.11
PSQL_SERVICE=postgresql
```

3.7 Администрирование сервера

3.7.1 Командная строка iBatyr Monitor

Многие операции, связанные с администрированием, имеют удобную и лаконичную систему команд, выполняемых из командной строки.

Вывод доступных команд

```
sudo ibatyr help [command|django]
```

Выберите *django* для вывода команд из командной строки Django.

Активация ключа через командную строку

```
sudo ibatyr activate [ключ]
```

Добавление правил мониторинга в глобальную конфигурацию

```
sudo ibatyr acl <RULE> <VALUE>
```

Подробный список правил представлен *здесь*

Бэкап базы данных и настроек

```
sudo ibatyr backup_db [PATH_TO_BACKUP]
```

По умолчанию бэкап сохраняется в **/var/lib/ibatyr/ibatyr_backup**.

Восстановление базы данных из бэкапа

Примечание: Восстановление базы данных должно выполняться в той же версии iBatyr Monitor, в которой был создан бэкап. В противном случае не гарантируется работоспособность системы.

```
sudo ibatyr restore_db [PATH_TO_BACKUP]
```

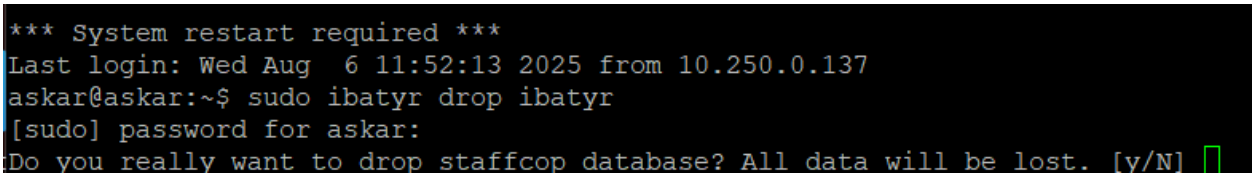
По умолчанию обращается по адресу **/var/lib/ibatyr/ibatyr_backup**.

Удаление базы данных

Предупреждение: Команда удаляет всю базу данных.

```
sudo ibatyr drop ibatyr
```

Если вы уверены в своих действиях, подтвердите удаление с помощью клавиши **y** в ответ на вопрос сервера.



После удаления сервер восстановит настройки сервера с помощью команды *sudo ibatyr init*.

Удаление всех файлов и скриншотов старше, чем значение DAYS

```
sudo ibatyr cleandata <DAYS>
```

Удаление из базы данных всех файлов и событий кроме последних DAYS

```
sudo ibatyr cleanup <DAYS>
```

Примечание: Чтобы механизм очистки отработал быстро и легко, необходимо свободное дисковое пространство (не менее 15% от размера текущей базы данных).

Эта команда удалит только записи, но физически не освободит место на жёстком диске. Процесс очистки жёсткого диска *описан в отдельной инструкции*.

Управление ClickHouse

```
sudo ibatyr clickhouse [install|init|reinit|pump|test|start|stop|restart]
```

Установка и активация базы данных clickhouse

```
sudo ibatyr clickhouse install
```

Апгрейд базы данных ClickHouse до стабильной версии

```
ibatyr upgrade clickhouse
```

Ставит последнюю известную стабильную версию ClickHouse. Иногда избавляет от проблем нестабильных версий ClickHouse, обычно более новых.

Загрузка данных из PostgreSQL в ClickHouse

```
sudo ibatyr clickhouse pump
```

Примечание: Эта команда не должна выполняться просто так! Запускайте только если знаете, что делаете!

Тестирование системы выгрузки из PostgreSQL в ClickHouse нужно для диагностики

```
sudo ibatyr clickhouse test
```

Перезапись всех данных ClickHouse

```
sudo ibatyr clickhouse reinit
```

Перезапуск сервера ClickHouse

```
sudo ibatyr clickhouse restart
```

Запуск сервера ClickHouse

```
sudo ibatyr clickhouse start
```

Остановка сервера ClickHouse

```
sudo ibatyr clickhouse stop
```

Тест отправки данных от клиента до сервера и вывод конфигурации агента.

```
sudo ibatyr client [SERVER]
```

Копирование базы данных и файлов с удаленного до локального сервера (PostgreSQL)

```
sudo ibatyr clone <SSH-USER>@<REMOTE-HOST> [ssh options]
```

Очистка незанятого места и дефрагментация базы данных

```
sudo ibatyr compact
```

Удаление всех данных по выбранному измерению

```
sudo ibatyr delete [--type agent|account|event] [--days N] [--keep-files] [--compact]
↪<NAME>

--type        Удаление данных по агенту, имени пользователя или типу событий
--days N      Оставить данные за N дней
--compact     Дефрагментация базы данных
--keep-files  Оставить файлы
--keep-events Оставить события
--use-id      Удаление данных по id (значения можно найти в БД)

Доступный список event для команды:

DiskDrive          | Внешние диски
FileOperation      | Операции с файлами
SystemLog          | Системный лог
UserActivity       | Алерт
WebcamSnapshot     | Снимок с
MicRecording       |
DevInventory       | Реестр оборудования
AppInventory       | Реестр софта
WebSearch          | Поисковый запрос
DesktopVideo       | Видео рабочего стола
FormData           | Данные формы
WLan               | Беспроводное подключение
InterceptedFile    | Перехваченный файл
Keyboard           | Ввод с клавиатуры
Run                | Запуск приложения
Exit               | Завершение приложения
Screenshot         | Снимок экрана
NetworkConnection  | Сеть
AppInstallation    | Установка ПО
Web                | Посещение сайтов
Im                 | Интернет-пейджер
Mail               | Почта
```

(continues on next page)

(продолжение с предыдущей страницы)

```
FTP             | FTP
PrintDoc        | Печать документов
UserLogon       | Вход/выход из системы
Clipboard       | Буфер обмена
Device          | Устройства
Stat            | Время активности
File            | Файловый сканер
```

Примечание: Эта команда чувствительна к регистру имени компьютера, будьте пожалуйста внимательны!

Управление специальными разрешениями администраторов

```
Usage: ibatyr special [options] list | grant <user> <permission|all> | revoke <user>
↪<permission|all>

Special permission management

Avaiable permissions:
 can_access_terminal        Имеет доступ к WEB-терминалу
 can_delete_shard           Может удалять данные из БД (помесячно)
 can_delete_event           Может удалять отдельные события
 can_delete_agent           Может удалять компьютеры и пользователей
 can_mass_delete            Может массово удалять события и файлы
 can_add_task               Может добавлять задания в планировщике
 can_delete_global_config   Может удалять правила из Глобальной конфигурации
 can_reset_settings         Может сбросить предустановленные настройки до изначального␣
↪состояния
 all                        Все разрешения

Options:
--password            Параметр позволяет задать дополнительный пароль, который будет␣
↪запрошен перед исполнением операции в веб-консоли.
```

Дать разрешение:

```
ibatyr special grant [USER] [PERMISSION]
```

Отозвать разрешение:

```
ibatyr special revoke [USER] [PERMISSION]
```

Посмотреть разрешения:

```
ibatyr special list
```

Восстановление дерева фильтров

```
sudo ibatyr rebuild_mptt
```

Выполните команду, если у вас наблюдаются ошибки при открытии веб-интерфейса в консоли JS

Экспорт фильтров и конфигураций

```
sudo ibatyr export FILE_TO_EXPORT.json
```

Экспорт производится в файл **FILE_TO_EXPORT.json**. Указывайте полный путь до файла.

Импорт фильтров и конфигураций

```
sudo ibatyr import FILE_TO_IMPORT.json
```

При выполнении команды указывайте полный путь до файла.

Текущие фильтры будут сохранены.

Вывод информации о сервере и занятом месте на диске

```
sudo ibatyr info
```

Инициализация или восстановление настроек сервера

```
sudo ibatyr init
```

Установка агента с сервера iBatyr Monitor

```
sudo ibatyr install [options] ip-address

--domain=DOMAIN        | Домен
--user=USER            | Имя пользователя
--password=PASSWORD    | Пароль
--server=SERVER_HOST   | IP-адрес сервера ibatyr
--port=SERVER_PORT     | Порт сервера ibatyr
--dry-run              | Проверка возможности установки
--reinstall            | Переустановка агента
--traceback            | Вывод trace ошибок
--uninstall            | Удаление агента
--language=LANGUAGE    | Выбор языка (en, ru)
--log                  | Показать лог установки
--version              | Вывод версии программы
```

Где, ip-address - это IP-адрес того ПК на котором вы хотите установить агента. В качестве адреса ПК - может выступать и имя рабочей станции, в этом случае у вас должен быть корректно настроен DNS-сервер в параметрах сетевых подключений системы.

Запуск mule в высоком приоритете

```
sudo ibatyr mule <MULE_NAME>
```

Распознавание текста в изображениях или pdf

```
sudo ibatyr ocr <image or pdf file>
```

Вывод статистики по ящику

```
ibatyr grab --server=<server> --login=<login> --password=<password>
```

Установка нового пароля для пользователя

```
sudo ibatyr passwd NEW_PASSWORD
```

Вывод текущих SQL-запросов и план выполнения

```
sudo ibatyr prof
```

Удаление пользователей и агентов, которые не имеют событий

```
sudo ibatyr prune
```

Вывод процессов ibatyr

```
sudo ibatyr ps
```

Перестройка отчетов за N месяцев

```
sudo ibatyr rebuild_sessions MONTHS
```

Сброс к настройкам сервера по умолчанию

```
sudo ibatyr reinit [full]
```

Предупреждение: Сброс настроек на сервере исключит сервер из кластера. При сбросе на мастер-сервере будет разрушена связь в кластере.

Параметр `[full]` удаляет все пользовательские фильтры.

Перезапуск сервиса ibatyr

```
sudo ibatyr restart
```

Создание суперпользователя в веб-интерфейсе

```
sudo ibatyr createsuperuser
```

Объединение событий агентов или аккаунтов с идентичными именами

```
ibatyr sane                                 | объединяются агенты и аккаунты
ibatyr sane agents                          | объединяются только агенты
ibatyr sane accounts                        | объединяются только аккаунты
ibatyr sane -l <количество дублей>          | позволяет обрабатывать только часть дублей␣
↪за запуск - например, 500 из 3000
ibatyr sane --limit <количество дублей>     | идентично ibatyr sane -l
ibatyr sane --help                          | вызов справки
```

Проверка индексов, включая первичные ключи и шардированные таблицы

```
ibatyr check
```

Управление шардированием

```
sudo ibatyr shard [init|install|list|ddl|index|copy|drop]
```

Создание шарда для текущего месяца

```
sudo ibatyr shard init
```

Включение функционала шардирования базы данных

```
sudo ibatyr shard install
```

Предупреждение: Необратимая операция! Команда работает в PostgreSQL версии 11 и выше, требуется 50% дискового пространства.

Вывод списка текущих шардов

```
sudo ibatyr shard list
```

Удаление части шардированной базы данных

```
sudo ibatyr shard drop agent_event_2021_01_01
```

Удалить часть БД, которая накопилась за январь 2021 года

Доступ к SQL-консоли iBatyr Monitor

```
sudo ibatyr sql
```

Добавление, удаление и отображение динамических полей в модели куба

```
ibatyr dynamic [options]
```

Примечание: Для вывода краткой справки по этой команде, напишите просто **ibatyr dynamic**

Создание и обновление профиля пользователя из AD

```
ibatyr ad_sync - синхронизация всех аккаунтов
ibatyr ad_sync --exists - синхронизация только существующего аккаунта
ibatyr ad_sync --user USER_NAME@DOMAIN - синхронизация конкретного пользователя
```

Примечание: Использует настройки AD указанные в Web-интерфейсе

Синхронизация по указанному домену

```
sudo ibatyr ad_sync --domain DOMAIN.local
```

Статистика синхронизации

```
sudo ibatyr ad_sync --stats
```

Присвоение конфигурации для пользователя или агента

```
ibatyr config --[user|agent] <AgentName|UserName>
↪<ComputerConfigurationName|UserConfigurationName>
```

Примечание: Если название конфигурации состоит из нескольких слов, тогда следует использовать кавычки: "Computer Config".

Включение на сервере нового механизма присвоения конфигурации

Начиная с версии 5.4 доступен новый механизм назначения конфигурации агенту. Он необязателен для использования, но может повысить скорость взаимодействия агента и сервера.

```
ibatyr enable rustsrv
```

Примечание: Механизм меняет *процесс присвоения конфигурации агентам из группы Active Directory*.

Запуск сервиса iBatyr

```
sudo ibatyr start
```

Остановка сервиса iBatyr

```
sudo ibatyr stop
```

Вывод топовых процессов iBatyr

```
sudo ibatyr top
```

Удаление всех данных

```
sudo ibatyr truncate
```

Обновление до последней версии

```
sudo ibatyr upgrade
```

Обновление PostgreSQL до версии 15

```
sudo ibatyr postgresql upgrade
```

Дополнительные возможности веб-интерфейса

Чтобы включить Linux-консоль на сервере и опцию удаления данных от агентов нужно выполнить команду:

```
sudo ibatyr special grant <user> <permission|all>
```

Чтобы выключить Linux-консоль на сервере, и опцию удаления данных от агентов нужно выполнить команду:

```
sudo ibatyr special revoke <user> <permission|all>
```

Примечание: По умолчанию эти меню отключены в веб-интерфейсе.

3.7.2 Работа с лицензиями

Основные особенности работы с лицензиями:

- данные о действиях пользователя за компьютером передаются на сервер, только если лицензия назначена и на пользователя, и на компьютер;
- если лицензия назначена только на компьютер, то с него на сервер передаются только данные инвентаризации и файлового сканера;
- лицензии для пользователей и компьютеров учитываются независимо друг от друга - при покупке N лицензий, для назначения на компьютеры и на пользователей доступно по N свободных лицензий.

После *установки сервера* и *агентов* iBatyr Monitor, получения данных о *компьютерах* и *пользователях*, можно переходить к распределению лицензий.

Распределение лицензий

При работе с лицензиями доступны:

- автоназначение лицензии;
- назначение лицензии вручную;
- освобождение от лицензии.

Все доступные для назначения лицензии хранятся в пуле свободных лицензий, из которого они вручную или автоматически назначаются Пользователям или Компьютерам. «Освобождённые» лицензии попадают в этот же пул.

Работать с лицензиями можно как через веб-интерфейс сервера iBatyr Monitor, так и через командную строку, подключившись к серверу по SSH.

Автоматическое распределение лицензий

Примечание: Для компьютеров включено по умолчанию. Чтобы отключить, в разделе **Панель управления - Настройки сервера** уберите галочку **Автоматически назначать лицензию новым агентам**.

Новые компьютеры получают лицензию из пула свободных лицензий. Если свободной лицензии на данный момент нет, компьютер ставится в очередь и получает первую освободившуюся лицензию.

Новые пользователи:

- добавленные агентами, автоматически получают лицензию из пула свободных;
- добавленные путём синхронизации с Active Directory, получают статус **Ожидает данные**. Лицензии таким пользователям будут назначены автоматически, как только от них поступят данные.

Ручное управление лицензиями

В разделах меню **Панель управления – Компьютеры** и **Панель управления – Пользователи** доступны операции с лицензиями для конкретных Компьютеров и Пользователей или для их групп.

Выберите Компьютеры или Пользователей и в выпадающем меню **Выполнить действие** выберите операцию с лицензией:

- Освободить лицензию
- Назначить лицензию
- Автоматически назначать лицензию

При выборе действия **Освободить лицензию**, лицензия снимается с выбранного Пользователя или Компьютера и помещается в пул свободных лицензий. Подробнее о политике отзыва лицензии можно прочитать в статье *Системные фильтры* в разделе Системные политики.

Командная строка

Команды для работы с лицензиями:

tabularytabulary

Команда
ibatyr drm info
ibatyr drm resync
ibatyr drm clear [agent|account]
ibatyr drm limit [agent|account]
ibatyr drm count [agent|account]
ibatyr drm allocate [agent|account] guid
ibatyr drm release [agent|account] guid
ibatyr drm disable [agent|account] guid
ibatyr drm enable [agent|account] guid

3.7.3 Настройка HTTPS для веб-интерфейса

Чтобы защитить веб-интерфейс iBatyr Monitor, рекомендуется использовать безопасное соединение HTTPS.
Его настройка займет несколько минут, но значительно повысит безопасность системы.

1. Откройте терминал: **Админ** → **Консоль администратора**.
2. Войдите в консоль с помощью логина и пароля, который вы указали *при установке сервера*. Если вы забыли пароль, восстановите его *по инструкции*.
3. Выполните команду:

```
ibatyr enable https
```

Вернитесь в веб-интерфейс и дважды кликните на адресную строку. Если в начале адреса появился *https://*, соединение защищено.

3.7.4 VirtualBox - командная строка

В VirtualBox не все параметры могут быть изменены из графического интерфейса. Часть меняется с помощью командной строки. Меняем размер жёсткого диска

Жёсткий диск виртуальной машины как правило находится в директориях **~/VirtualBox** далее имя виртуальной машины или **~/.VirtualBox/HardDisks**

Примечание: Изменение размера диска возможно, только для диска в формате VDI. Диски импортируемые из OVA-образа, не могут быть расширены этой командой!

Изменяем размер жесткого диска

Изменяется размер командой:

```
VBoxManage modifyhd Your_disk.vdi -resize size_in_Mb
```

Путь к диску придётся указывать полностью. В текущей 5 версии VirtualBox (командный сервис **VBoxManage**) команда **modifyhd** заменена на **modifymedium**.

Более подробнее. Например, если вы хотите установить размер диска в 12000 Мегабайт (12 Гб) то выполните:

```
VBoxManage modifyhd natty.vdi -resize 12000
```

Меняем объем оперативной памяти

Переходим в каталог **C\:ProgramFiles\Oracle\Virtualbox** и выполняем команду:

```
VBoxManage modifyvm «machine_name» -memory 4000
```

Размер оперативной памяти указывается в мегабайтах, позволяет задать виртуальной машине памяти больше, чем есть на реальной машине.

Примечание: После выставления памяти больше, чем доступно на хостовой машине, вы не сможете редактировать свойства машины чз. графический интерфейс. !!

Меняем имя ОС

Имя ОС меняется командой типа:

```
VboxManage modifyvm «имя_машины_до» -name NEW_NAME
```

Кавычки в новом имени машины - не обязательны.

Конвертация образа VMWare vmdk в VirtualBox vdi

Руководство взято с сайта - https://vmblog.ru/konvertaciya-obraza-vmware-vmdk-v-virtualbox-vdi/

В этой статье описано, как сконвертировать образ виртуальной машины в формате VMWare (файл **vmdk**) в формат Oracle VirtualBox (**vdi** — VirtualBox Disk Image). Данная методика поможет вам без лишних сложностей запустить виртуальную машину, созданную в среде VMWare на компьютере с установленным VirtualBox.

Нам понадобится десктопная среда виртуализации — Oracle VirtualBox. Скачайте дистрибутив и установите VirtualBox. Скопируйте vmdk файлы виртуальной машины на локальный диск и запустите командную строку с правами администратора и перейдите в каталог с VirtualBox:

```
cd c: \Program Files\Oracle\VirtualBox\
```

Теперь запустим встроенную утилиты VBoxManage с параметром **clonehd** для создании копии файла данных виртуальной машины и преобразования его из формата VMDK в VDI.

Примечание: Примечание. Перед началом конвертации нужно удалить снапшоты виртуальной машины и убедится, что диск не используется запущенными виртуальными машинами.

```
VBoxManage clonehd --format VDI D:\clonation\PROJECT.virtual.vmdk D:\Virtual.vdi
```

Теперь в VirtualBox можно создать новую виртуальную машину и подключить к ней полученный vdi диск. Сконвертированный диск будет лежать в корне папки **D:**

3.7.5 Квадратики вместо кириллицы (русских букв) в серверной консоли

Иногда в консоли Linux вместо кириллицы можно увидеть «квадратики».

Это мешает читать сообщения системы, если установлена кириллическая локаль (Русская локаль).

Данная проблема типовая для Ubuntu, решение тут.

Проблему можно решить выполнив эту команды:

```
sudo -i
echo 'FRAMEBUFFER=Y' >> /etc/initramfs-tools/initramfs.conf
sudo update-initramfs -u
sudo dpkg-reconfigure console-setup
sudo init 6
```

Второй вариант настройки консоли - руссифицировать её

Для этого нужно будет скачать пакет локализации для системы и прописать корректную локаль в настройках системы по умолчанию.

```
sudo apt-get install console-cyrillic
```

Редактируем файл конфигурации консоли

```
sudo nano /etc/default/console-setup
```

Меняем следующие переменные:

```
CODESET="CyrSlav"
FONTFACE="VGA"
FONTSIZE="16"
```

Сохраняем файл Применяем сделанные изменения:

```
setupcon -v
```

Последнее изменение, прописать русскую локаль в системе в файле /etc/default/locale

```
sudo nano /etc/default/locale
```

Вписываем туда вместо того, что там указано:

```
LANG="ru_RU.UTF-8"
```

Сохраняем файл, и выходим и входим в систему или перезагружаем ПК

3.7.6 Добавление правил в конфигурацию из командной строки

Правила в конфигурацию компьютеров можно добавлять:

- через *веб-интерфейс сервера iBatyr Monitor*;
- с помощью командной строки.

Чтобы добавить правило в конфигурацию через командную строку, используйте команду:

```
ibatyr acl 'правило' 'значение' 'конфигурация1 | конфигурация2 |...'
```

Чтобы удалить правило из конфигурации:

```
ibatyr acl 'правило' 'значение' 'конфигурация1 | конфигурация2 |...' --drop
```

При добавлении правил в конфигурацию важно помнить:

- если в команде добавления или удаления правила не указать название конфигурации, то правило будет добавлено или удалено в *глобальную конфигурацию*;
- значения величин, в которых есть пробелы, должны указываться в кавычках.

Примеры команд

Добавить в глобальную конфигурацию правило, запрещающее подмену сертификата для сайта **kontur.ru**:

```
ibatyr acl 'PROXY_SSL_APP_EXCLUDE' 'kontur.ru'
```

Удалить из конфигураций *TD* и *Конфигурация по умолчанию* правило, блокирующее USB-устройство с Device ID **USBVID_16&PID_B18030131**:

```
ibatyr acl 'USB_EXCLUDE' 'USB\VID_16&PID_B18\030131' 'TD|Конфигурация по умолчанию' --
↪drop
```

Доступные правила

Правило	Раздел
APP_RUN_EXCLUDE	*Контроль программ - Правила: Мониторинг - Приложения*
APP_RUN_INCLUDE	*Контроль программ - Правила: Мониторинг - Приложения*
APP_RUN_BLACKLIST	*Контроль программ - Правила: Блокировка - Приложения*
APP_RUN_WHITELIST	*Контроль программ - Правила: Блокировка - Приложения*
FILE_PATH_EXCLUDE	*Файлы - Правила: Файловый мониторинг - Пути и маски*
FILE_PATH_INCLUDE	*Файлы - Правила: Файловый мониторинг - Пути и маски*
FILE_APP_EXCLUDE	*Файлы - Правила: Файловый мониторинг - Приложения*
FILE_APP_INCLUDE	*Файлы - Правила: Файловый мониторинг - Приложения*
FILE_APP_READ_EXCLUDE	*Файлы - Правила: Файловый мониторинг - Приложения - Чтение*
FILE_APP_READ_INCLUDE	*Файлы - Правила: Файловый мониторинг - Приложения - Чтение*
SPECIAL_DOC_LIST	*Файлы - Правила: Файлы - Особый контроль*
PROXY_APP_EXCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Приложения*
PROXY_APP_INCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Приложения*
PROXY_IP_EXCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - IP*

continues on next page

Таблица 1 – продолжение с предыдущей страницы

PROXY_IP_INCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - IP*
PROXY_PORT_EXCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Порт*
PROXY_PORT_INCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Порт*
PROXY_URL_EXCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Адрес*
PROXY_URL_INCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Адрес*
PROXY_SSL_APP_EXCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Подмена серт*
PROXY_SSL_APP_INCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Подмена серт*
REPORT_NET_PORT_EXCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Отправка от*
REPORT_NET_PORT_INCLUDE	*Сетевые подключения - Правила: Сетевой мониторинг - Отправка от*
USB_EXCLUDE	*Устройства - Правила: Блокировка - USB*
USB_INCLUDE	*Устройства - Правила: Блокировка - USB*
USB_CLASS_EXCLUDE	*Устройства - Правила: Блокировка - USB-класс*
USB_CLASS_INCLUDE	*Устройства - Правила: Блокировка - USB-класс*
WEB_SITES_BLACKLIST	*Интернет - Правила: Блокировка - Сайты*
WEB_SITES_WHITELIST	*Интернет - Правила: Блокировка - Сайты*
WEB_CONTENTTYPE_EXCLUDE	*Интернет - Правила: Веб мониторинг - Отправка отчетов по типу к*
WEB_CONTENTTYPE_INCLUDE	*Интернет - Правила: Веб мониторинг - Отправка отчетов по типу к*
SPECIAL_APP_LIST	*Снимки экрана - Правила: Особый контроль*
KBD_APP_EXCLUDE	*Клавиатура и буфер обмена - Правила: Перехват клавиатуры - Прило*
KBD_APP_INCLUDE	*Клавиатура и буфер обмена - Правила: Перехват клавиатуры - Прило*
ACCOUNT_BLACKLIST	*Мониторинг пользователей - Правила: Мониторинг пользователей*
ACCOUNT_WHITELIST	*Мониторинг пользователей - Правила: Мониторинг пользователей*
WATCH_FILES	*Мониторинг Linux - Правила: Мониторинг лог-файлов*

Добавление меток к устройствам

Утилита **acl** позволяет не только создавать правила для конфигураций компьютеров, но и работать с метками USB-устройств.

Для работы с метками с командами **USB_EXCLUDE**, **USB_INCLUDE**, **USB_CLASS_EXCLUDE** и **USB_CLASS_INCLUDE** используется параметр **--add_label=**, добавляющий значение метки указанному устройству.

Синтаксис команды при работе с метками:

```
ibatyr acl USB_EXCLUDE device_id my_config --add_label=my_label
```

Данная команда заполняет правило **Устройства - Правила: Блокировка-USB - Запретить** значением **device_id** в конфигурации **my_config**, и в разделе **Панель управления - Устройства** добавляет метку **my_label** к устройству с тем же **device_id**.

Примечание: Если устройства с указанным **device_id** нет в списке, оно будет создано.

3.7.7 Смена часового пояса и времени на сервере

Смена часового пояса

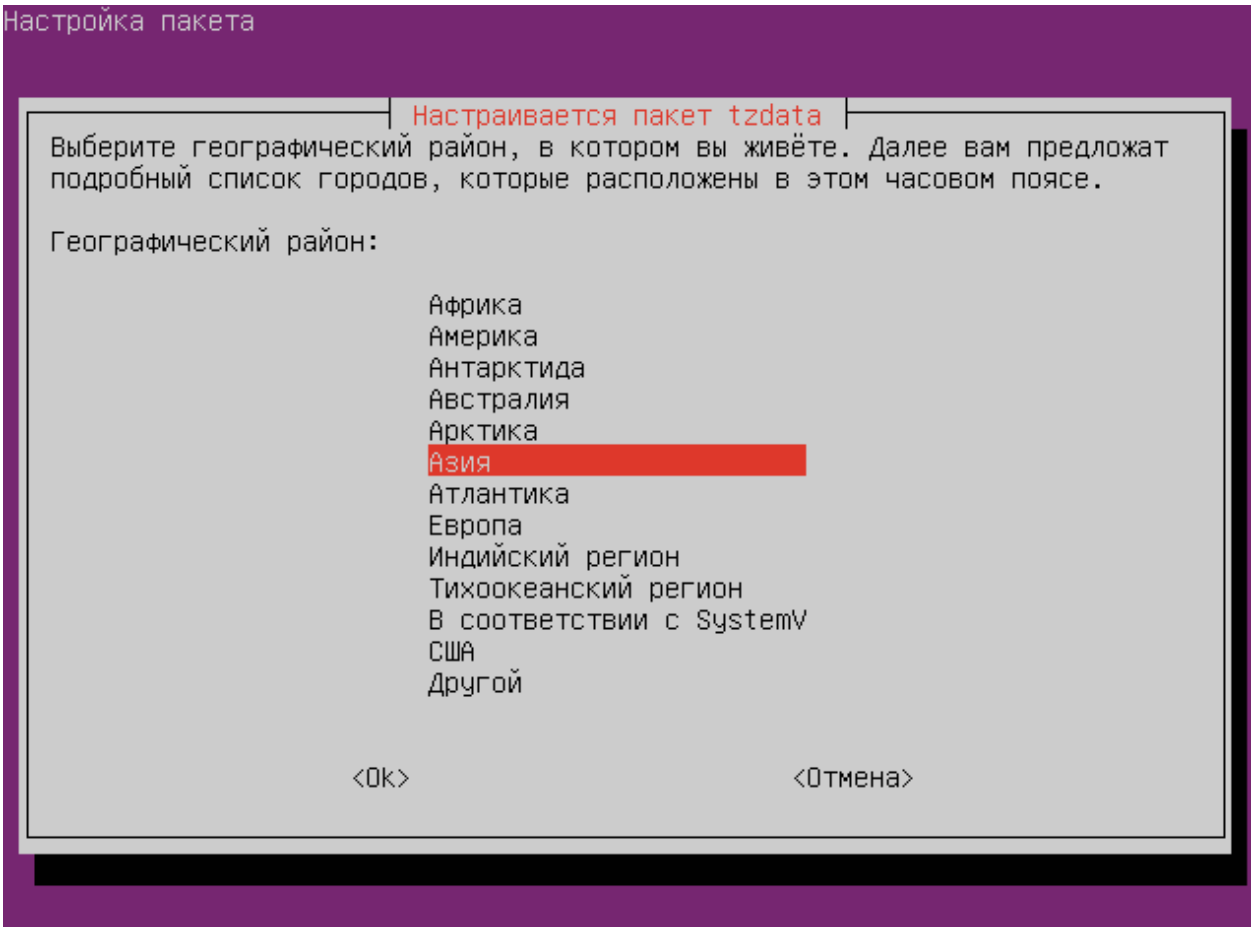
В большинстве случаев на сервере и наблюдаемых компьютерах должно быть выставлено одно время и один часовой пояс.

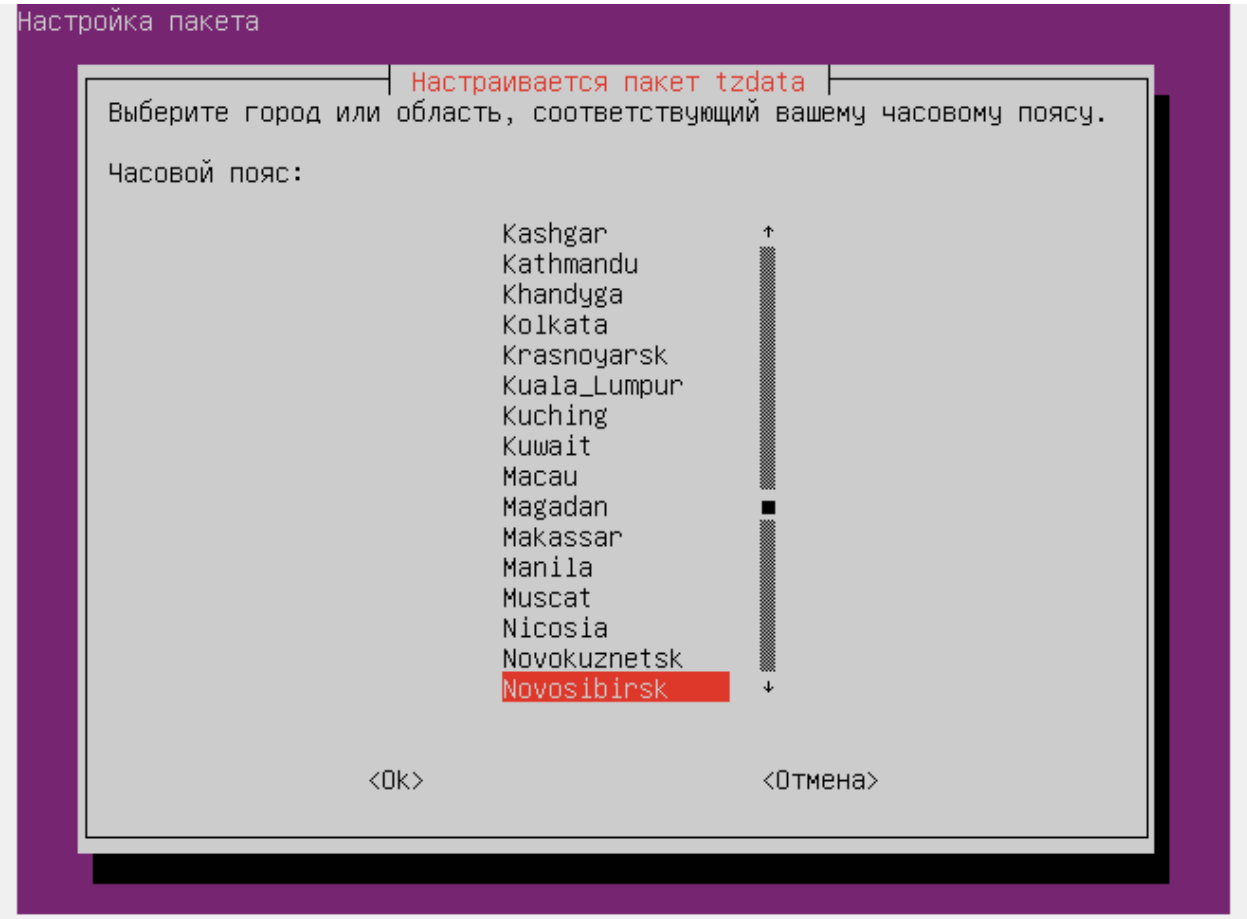
Установка времени и часового пояса производится в момент инсталляции операционной системы.

В случае, если вам нужно сменить часовой пояс на уже работающей системе:

```
sudo dpkg-reconfigure tzdata
```

Далее последовательно выбираем свой регион и город.





Смена времени

Чтобы установить текущее время, нужно воспользоваться командой:

```
sudo date +%T -s "11:14:00"
```

Чтобы установить текущую дату выполняем:

```
sudo date +%Y%m%d -s "20120418"
```

Примечание: Обратите внимание - время и часовой пояс - разные вещи.

Измените цифры на своё значение времени.

ДеньМесяцЧасМинутаГод, где каждому значению выделено двузначное число, и только году - четырёхзначное.

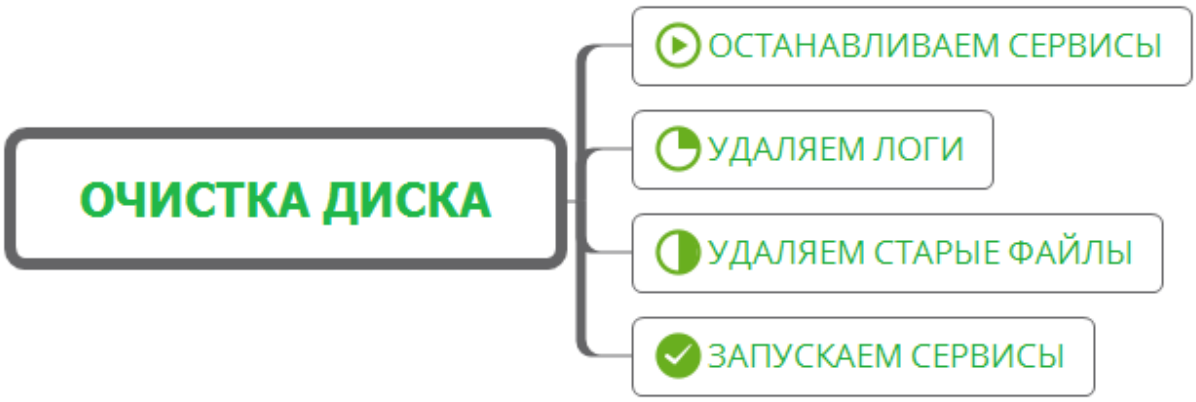
Автоматическая синхронизация времени

Можно воспользоваться автоматической синхронизацией времени при помощи NTPD и руководства для демона синхронизации времени для Ubuntu Server.

3.7.8 Ручная очистка диска

Каким бы большим не был жёсткий диск, место на нём конечно, и если заранее не принять мер, рано или поздно оно закончится. Самое страшное, что может произойти после этого - это невозможность работы системы или потеря самых старых данных сохранённых в системе.

Примечание: Для предотвращения данной ситуации заранее планируйте необходимый объем жёсткого диска, исходя из количества клиентских машин, того, что конкретно на них собирается и сроков хранения данных.



В административной панели можно выставить настройки *автоочистки*.

Также можно провести очистку диска вручную. Для этого:

1. Остановите сервер ibatyr командой:

```
sudo service ibatyr stop
```

2. Проверьте доступное место на диске:

```
df -h
```

3. Удалите записи в логах

```
sudo rm /var/log/*gz
```

4. Удалите старые базы iBatyr Monitor:

   4.1 Откройте файл скрипта **compact**, являющегося частью iBatyr Monitor:

   ```
   sudo nano /usr/share/ibatyr/bin/compact
   ```

   4.2 В открывшемся файле раскомментируйте строки **echo «Vacuum database»** и **sudo -u postgres psql ibatyr -c «vacuum full»**. Итоговый файл будет иметь следующий вид:

```
#!/bin/bash
# USE compact
# HELP Cleanup unreffered dimensions and vaccum database
ibatyr stop
echo "Cleanup dimensions"
cat sql/cleanup_dimensions.sql| bin/sql
echo "Vacuum database"
sudo -u postgres psql ibatyr -c "vacuum full"
ibatyr start
echo "Cleanup done"
bin/info
```

4.3 Сохраните изменения.

4.4 Очистите старые записи в базе:

```
sudo ibatyr cleanup X
```

здесь X - это число дней, данные за которые нужно оставить.

4.5 Запустите скрипт:

```
ibatyr compact
```

Примечание: Оптимальным запасом для обеспечения производительной работы механизма очистки базы будет наличие свободного места на диске (15% от размера текущей базы).

В случае, если диск забит «под завязку», возможны проблемы с удалением. В этом случае есть обходной способ, позволяющий очистить диск.

```
sudo tune2fs -m 0 /dev/sdX
```

Эта команда позволяет освободить зарезервированную для системных нужд часть диска. После этого нужно выполнить описанную выше последовательность действий по очистке. Далее нужно вернуть суперпользователю его резерв дискового пространства. Для этого следует выполнить следующую команду:

```
sudo tune2fs -m 5 /dev/sdX
```

Если эта команда не будет выполнена, то при неправильных настройках есть вероятность занятия всего жёсткого диска, включая 5% суперпользователя.

Примечание: Обязательно возвращайте 5% резерв, 5% резерва это общепринятая стандартная практика.

После очистки диска нужно вновь запустить ibatyr командой

```
sudo service ibatyr start
```

3.7.9 Системный раздел: копирование

Иногда возникает необходимость в резервном копировании не только данных, но и самой операционной системы.

Копирование операционной системы имеет смысл делать в том случае, если вы доставляли некие дополнительные программы, имеете много особых настроек и т.д.

Это можно сделать несколькими способами, самый простой из которых - копирование всего раздела целиком.

Например, использовав команду **dd**.

```
sudo dd if=/dev/sdXY bs=1M conv=noerror | gzip -c> /folder/folder/part.dd.gz
```

Получившийся файл - это побайтная копия вашего раздела, включая не только файлы, но тип файловой системы.

Из этого видно, что если система и данные, например, база ibatyr и скрины, находятся на одном разделе, этот способ вам **не** подходит.

Конечно же, как любую копию, его нужно хранить на другом устройстве.

3.7.10 Смена IP-адреса сервера iBatyr Monitor

Автоматическая смена IP-адреса на Ubuntu

Примечание: Автоматический способ гарантирует сохранение текущего адреса без изменений. Текущий динамический IP-адрес будет становлен в качестве статического.

Для смены адреса выполните:

```
wget docs.ibatyr.kz/dynamic-to-static-ip.sh
sudo bash dynamic-to-static-ip.sh
```

Если вы хотите сразу задать определенный адрес серверу, введите этот адрес через пробел после имени скрипта, например так:

```
sudo bash dynamic-to-static-ip.sh 192.168.1.132
```

Ручная смена IP-адреса на Ubuntu

Предупреждение: Актуально только для версии 4.7 и выше

В Ubuntu для установки статического IP-адреса сервера используется утилита Netplan.

1. Установите Netplan

```
apt install netplan
```

Все настройки Netplan выполняются только от имени пользователя **root**. Для этого войдите в режим **root** с помощью команды `sudo su -` и введите пароль обычного пользователя:

```
sudo su
```

2. Отключите Cloud-init

После установки Netplan отключите Cloud-init.

Примечание: Cloud-init — это инструмент для настройки серверов на стадии запуска. На серверах со статическими IP-адресами Cloud-init может сбрасывать заданные вручную настройки сети. Чтобы сохранить настройки сети неизменными, отключите для Cloud-init управление сетью.

Создайте файл:

```
sudo nano /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg
```

Добавьте в файл строку, которая отключает управление сетью для Cloud-Init:

```
network: {config: disabled}
```

Чтобы настройки сети не перезаписывались, удалите конфигурационный файл, который Cloud-init создает для Netplan:

```
sudo rm -f /etc/netplan/50-cloud-init.yaml
```

После этого можно создавать свою конфигурацию.

3. Создайте конфигурацию

Определите, в каком файле содержится текущая конфигурация. Для этого посмотрите содержимое папки **/etc/netplan** с помощью команды `ls`:

```
ls /etc/netplan
```

В этом примере конфигурация лежит в файле **01-netcfg.yaml**. Запустите редактор Nano с параметром – именем этого файла:

```
nano /etc/netplan/01-netcfg.yaml
```

Откроется окно редактора.

Добавьте в файл сниппет:

Ubuntu 18.04, 20.04

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.124.200/24]
      gateway4: 192.168.124.1
    nameservers:
        addresses: [192.168.124.1, 8.8.8.8, 8.8.4.4]
```

Ubuntu 22.04

В Ubuntu 22.04 формат конфигурации немного изменился. Вместо устаревшего `gateway4` задайте маршрут через ключ `via`.

```
network:
 version: 2
 renderer: networkd
ethernets:
  eth0:
    dhcp4: no
    dhcp6: no
    addresses: [192.168.124.200/24]
    routes:
       to: 0.0.0.0/0
       via: 192.168.124.1
```

(continues on next page)

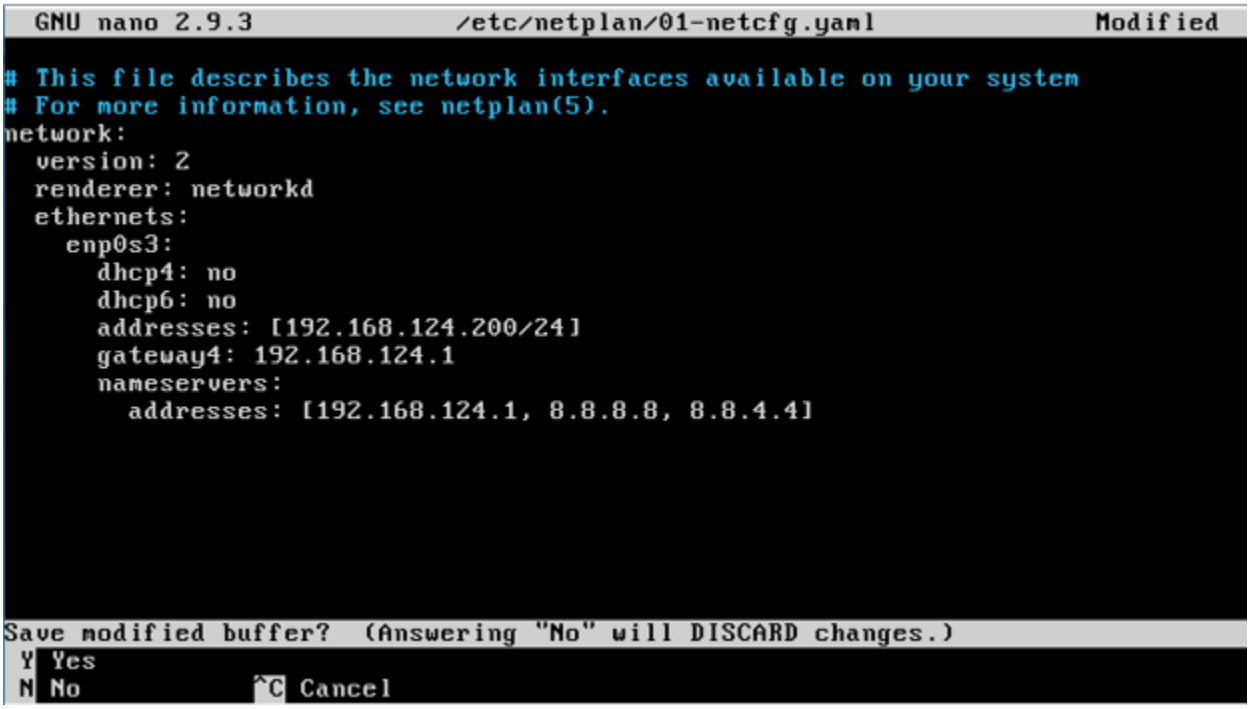
(продолжение с предыдущей страницы)

```
    nameservers:
      addresses: [192.168.124.1, 8.8.8.8, 8.8.4.4]
```

где:

- адрес `192.168.124.200` в первой строке `addresses` замените на адрес вашего сервера;
- маска `/24` соответствует `255.255.255.0`. Если она совпадает с вашей маской, ничего не меняйте. В противном случае, замените на свою;
- адрес `192.168.124.1` в строке `gateway4` или `via` — на адрес своего шлюза;
- значения адресов DNS-серверов во второй строке `addresses` — на значения адресов своих DNS-серверов;
- в конце текста должна быть как минимум одна пустая строка.

После внесения изменений выйдите из режима редактирования с помощью клавиш Ctrl+X. Редактор запросит сохранение изменённого файла:



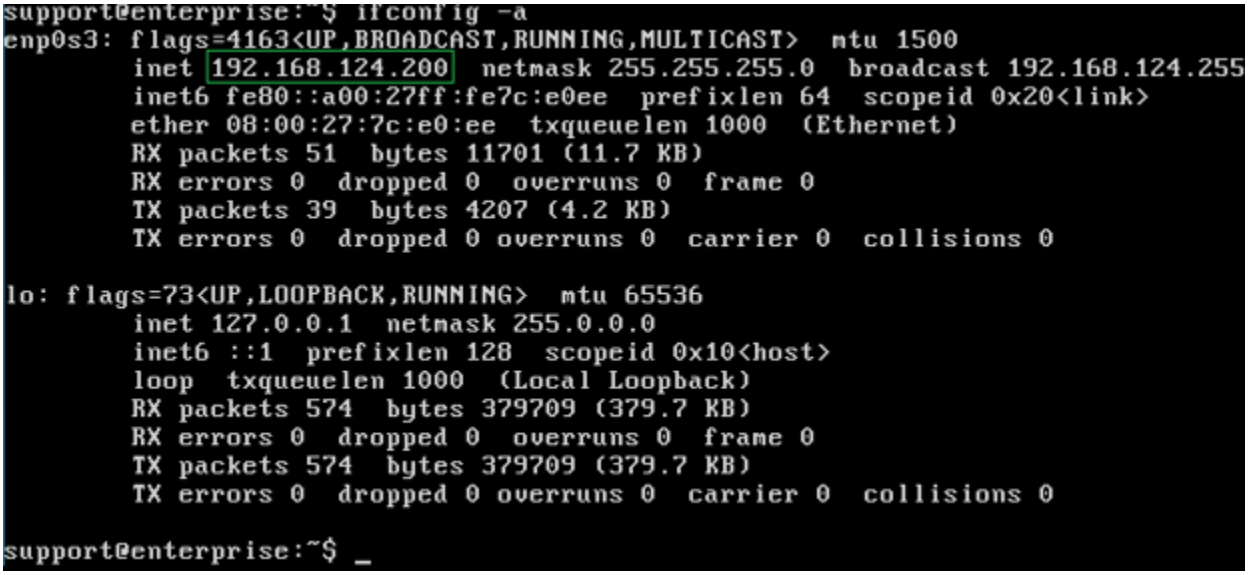
Ответьте нажатием клавиши **Y** (yes). Редактор предложит имя файла для сохранения. Нажмите **Enter**, чтобы согласиться.

Примените конфигурацию:

```
netplan apply
```

Если вывод без ошибок — все выполнено верно. Для гарантии перезагрузитесь с помощью команды `reboot` и проверьте получение IP-адреса:

```
ifconfig -a
```



3.7.11 Смена стандартного порта 443

По умолчанию для связи сервера с агентом используется порт 443. Чтобы назначить новый - укажите его номер в настройках агента и сервера.

Изменение порта в настройках сервера

Чтобы изменить номер порта:

1. Откройте конфигурационный файл веб-сервера:

```
sudo nano /etc/nginx/sites-available/ssl.ibatyr
```

2. Измените номер порта в строке *listen*: вместо указанного по умолчанию 443 укажите свой.
3. Перезапустите ibatyr и nginx:

```
sudo service ibatyr restart; sudo service nginx restart
```

Изменение порта в настройках агента

Изменить порт в настройках агента можно:

- при переустановке агента (новая версия агента должна быть не ниже установленной);
- без переустановки, с помощью записи в реестре:

```
ADD HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TimeSvc3\ServiceConfiguration
```

Дополнительный порт для управления работой сервера

Если возникает потребность в назначении дополнительного порта для управления работой сервера:

1. Создайте копию уже имеющегося конфигурационного файла:

```
sudo cp /etc/nginx/sites-available/ssl.ibatyr /etc/nginx/sites-available/ssl.ibatyr2
```

2. Откройте новый конфигурационный файл:

```
sudo nano /etc/nginx/sites-available/ssl.ibatyr2
```

3. Закомментируйте первые две строки конфигурационного файла:

```
# client_max_body_size
# large_client_header_buffers
```

4. В строке *listen* укажите новый номер порта.
5. Создайте символьную ссылку на новый конфигурационный файл:

```
sudo ln -s /etc/nginx/sites-available/ssl.ibatyr2 /etc/nginx/sites-enabled
```

6. Перезапустите ibatyr и nginx:

```
sudo service ibatyr restart; sudo service nginx restart
```

После этого сервер будет прослушивать указанные порты.

3.7.12 Сменить заголовок страницы

Если вы не хотите, чтобы при сканировании сети или попытке входа на страницу отображался заголовок iBatyr Monitor, то нужно отредактировать файл:

```
sudo nano /etc/ibatyr/config
```

дописав в конец файла строку:

```
BRAND_TITLE='Title_instead_of_iBatyr Monitor'
```

После файл нужно сохранить, и рестартовать сервисы nginx и ibatyr.

```
sudo service ibatyr restart
sudo service nginx restart
```

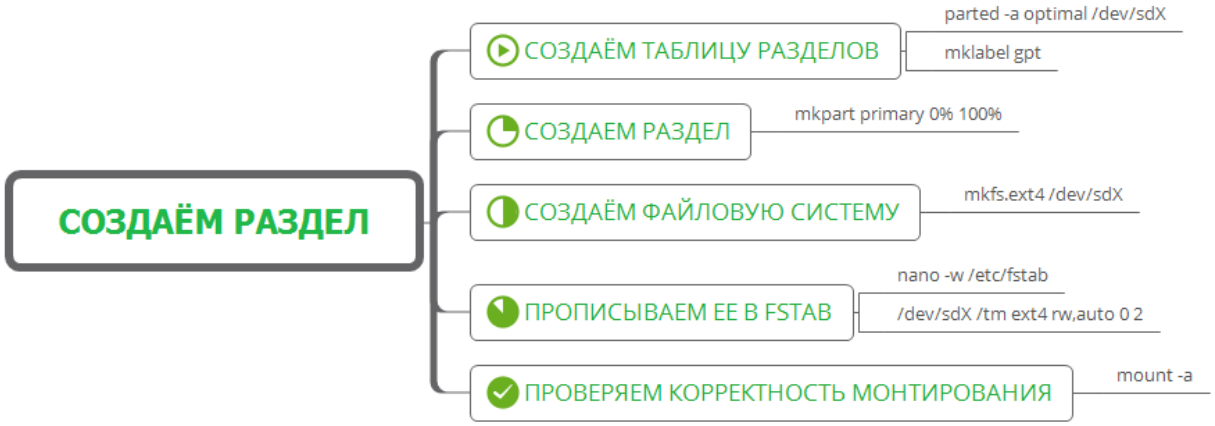
3.7.13 Создание/изменение разделов

Создание разделов мы рассмотрим на примере работы с реальными разделами под управлением ОС Linux. В случае с виртуальной системой, установленной под виртуальной машиной типа Virtualbox, все действия и команды будут идентичны.

Общие понятия

- Программы разметки - программы для разметки жесткого диска.
- Точка монтирования - это папка, в которой будет видно содержимое устройства, например, жёсткого диска.
- Устройство - любое устройство, жёсткий ли диск, флешка ли, CD-диск или что-то другое видится в linux в виде файла. Обычно это отображается в стиле /dev/sda.
- Таблица разделов - в таблице разделов хранится информация о типе раздела и его расположении на жёстком диске.
- Файловая система - данные о файловой системе раздела.

Принципиальная схема действий



Предупреждение: Будьте внимательны при следующих операциях. Они необратимо удаляют информацию с диска. Если вы ошибётесь, и выберете не тот жёсткий диск, вы потеряете накопленные там данные.

Примечание: Если вам удобнее работать с графическим интерфейсом, вы можете скачать Live-CD Gparted, загрузиться с него, и разбить диск так, как вам нужно.

1. Выбираем устройство (жёсткий диск) который будем размечать командой:

```
sudo parted -a optimal /dev/sdX
```

Попадаем в интерфейс командной строки программы.

2. Создаём таблицу разделов командой типа

```
mklabel gpt
```

Примечание: т.к. мы уже находимся в текстовом интерфейсе команды parted, запущенной с правами суперпользователя, вводить sudo не нужно.

---

3. Создаём раздел командой

```
mkpart primary 0% 100%
```

Это означает, что мы создаём один раздел, который займёт весь диск, от начала до конца, и является первичным. Если вам нужно, чтобы раздел занимал часть диска, вы можете изменить начало либо завершение раздела.

4. Создаём файловую систему

Для ОС linux существует несколько типов файловых систем, по умолчанию используется ext4. Если вы не имеете чёткого представления о том, в чём состоят сильные и слабые стороны каждой файловой системы, то оптимальным выбором будет использование ext4. Создаётся она командой

```
sudo mkfs.ext4 /dev/sdX1
```

5. Прописываем устройство в **/etc/fstab** , чтобы оно монтировалось автоматически при каждой загрузке.

Строка будет иметь примерно такой вид:

```
/dev/sdX1 /folder ext4 rw,auto 0 2
```

6. Проверяем корректность монтирования командой

```
sudo mount -a
```

Эта команда монтирует все устройства, прописанные в **/etc/fstab**, но не монтированные.

Увеличиваем размер без отмонтирования диска

Предупреждение: Помните - любые операции с разделами потенциально опасны, и ставят под угрозу целостность ваших данных на изменяемом разделе.

Данная операция возможна только на Ubuntu 18 и выше. Проверить версию вы можете следующей командой:

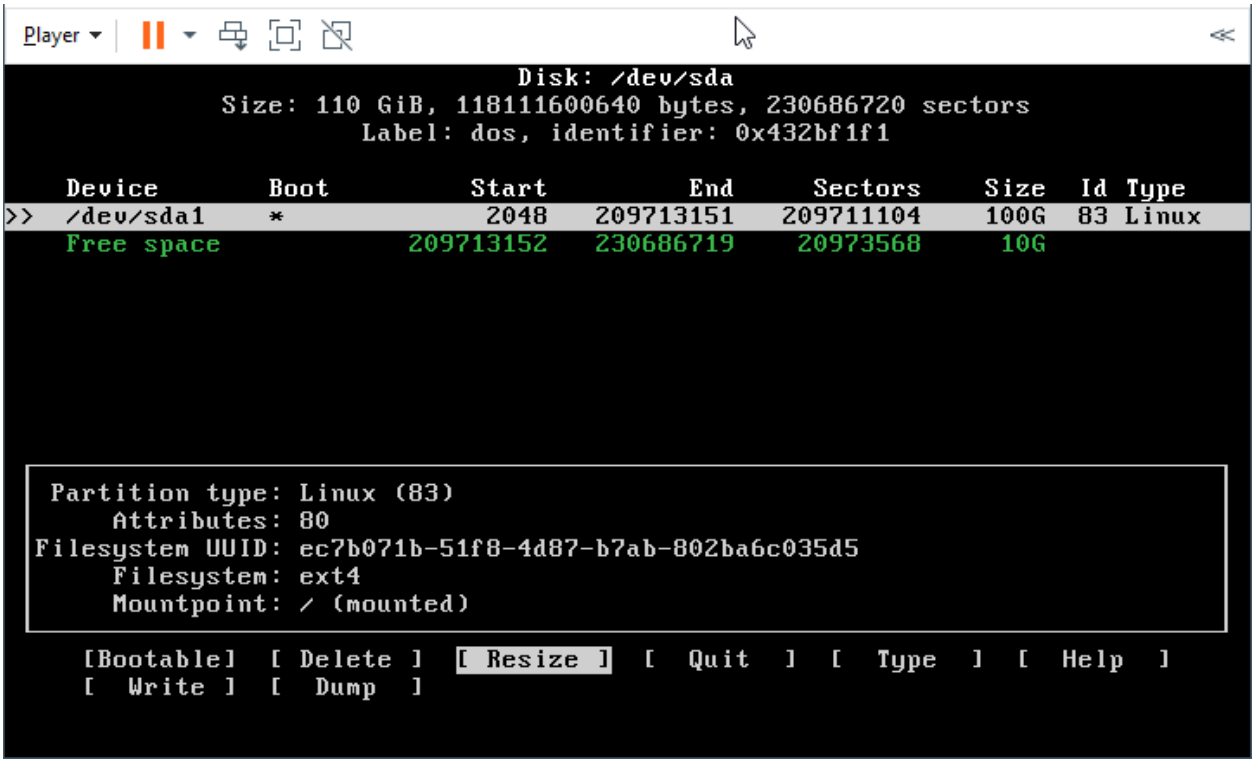
```
lsb_release -a
```

1. Если версия Ubuntu 18 и выше, то продолжаем. Вначале необходимо выключить сервисы:

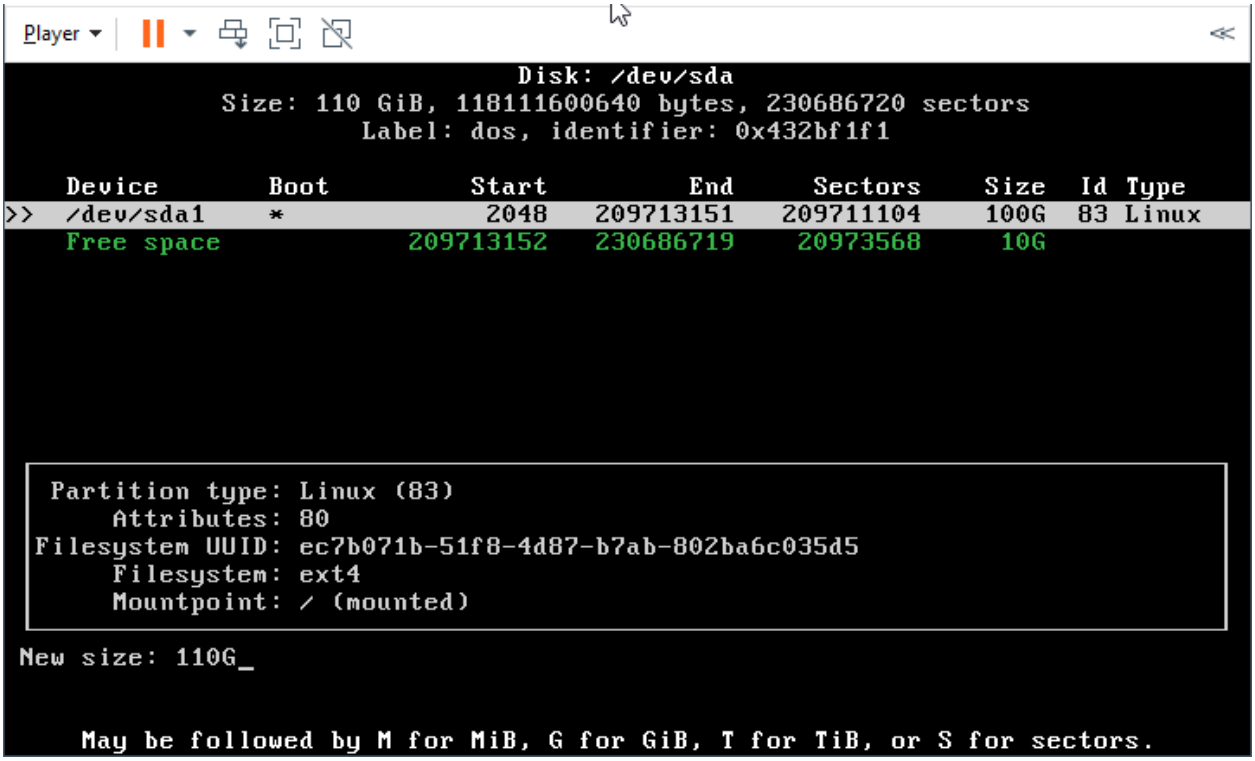
```
ibatyr stop
systemctl stop postgresql
```

2. Запускаем cfdisk и выбираем Resize

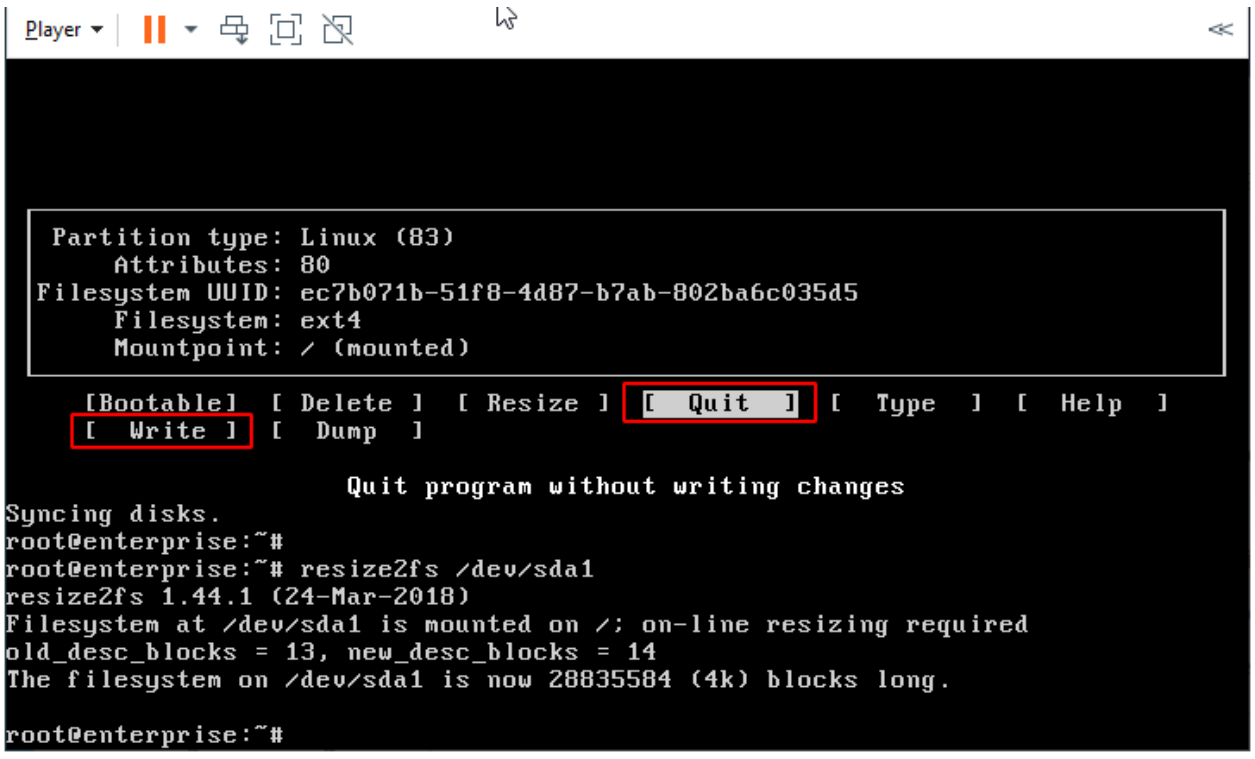
```
sudo cfdisk
```



3. Соглашаемся с новым размером



4. Записываем изменения (Write) и выходим из cfdisk



5. Перечитываем таблицу разделов и расширяем файловую систему

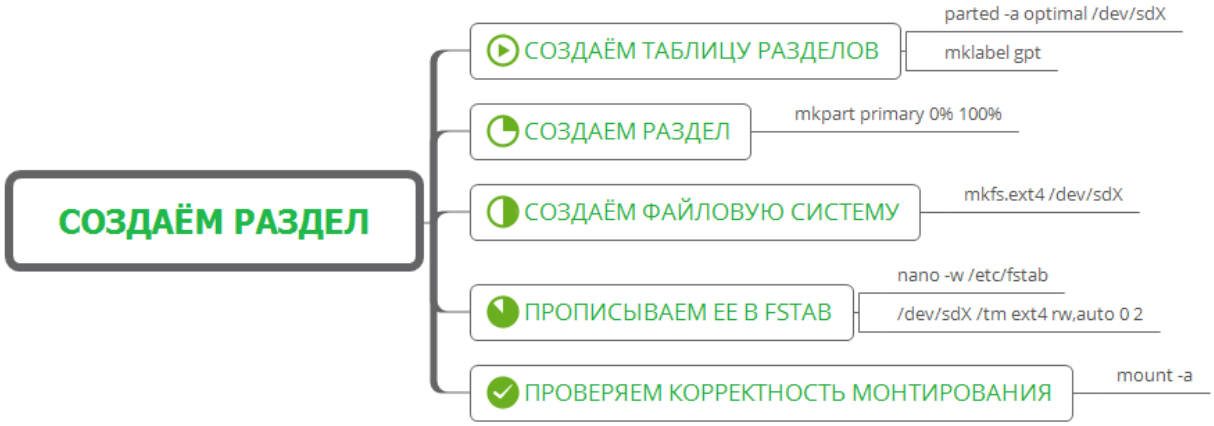
```
partprobe
resize2fs /dev/sdX1
```

6. Включаем сервисы

```
systemctl start postgresql
ibatyr start
```

Увеличиваем размер диска

Предупреждение: Помните - любые операции с разделами потенциально опасны, и ставят под угрозу целостность ваших данных на изменяемом разделе.



Иногда необходимо изменить размер диска. Проделать можно это следующим образом:

1. Выключаем сервисы:

```
ibatyr stop
systemctl stop postgresql
```

2. Отмонтируем изменяемый раздел.

Внимание: Не работает для загрузночого раздела. Рекомендуем использовать другие способы «**live-cd**» или «**gparted**». Рекомендуем скачать по ссылке выше и загрузиться с диска.

```
umount /dev/sdX1.
```

3. Далее запускаем parted и изменяем размер раздела.

```
sudo parted /dev/sdX1
resizepart №part 100%
```

Эта команда растянет раздел на весь свободный остаток диска, при условии, что тот имеется.

4. Диск увеличен, однако если мы не выполним следующий шаг, то для нашей системы будет недоступно новое место. Выходим из **parted** и выполняем команду:

```
sudo resize2fs /dev/sdX1
```

5. После изменения раздела полезно выполнить его проверку:

```
sudo fsck.ext4 -f /dev/sdX1
```

Предупреждение: Не запускайте **fsck** на примонтированном разделе! Это грозит потерей данных.

6. Включаем сервисы

```
systemctl start postgresql
ibatyr start
```

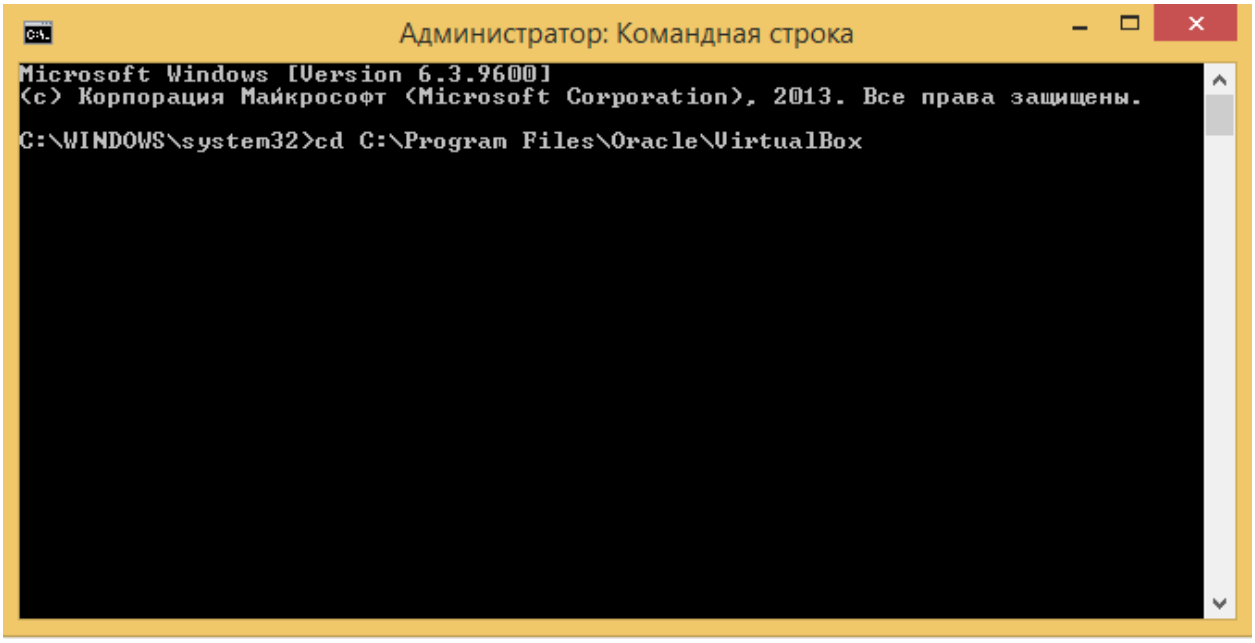
Также для изменения размера раздела вы можете загрузиться с **livecd** или **gparted**, и получить графический интерфейс для работы с вашими разделами.

Ссылка на gparted: https://gparted.org/download.php

3.7.14 Увеличение размера диска на сервере для VirtualBox

- В командной строке с правами администратора(cmd) перейти в папку **C:\Program Files\Oracle\VirtualBox**

```
cd C:\Program files\Oracle\VirtualBox
```



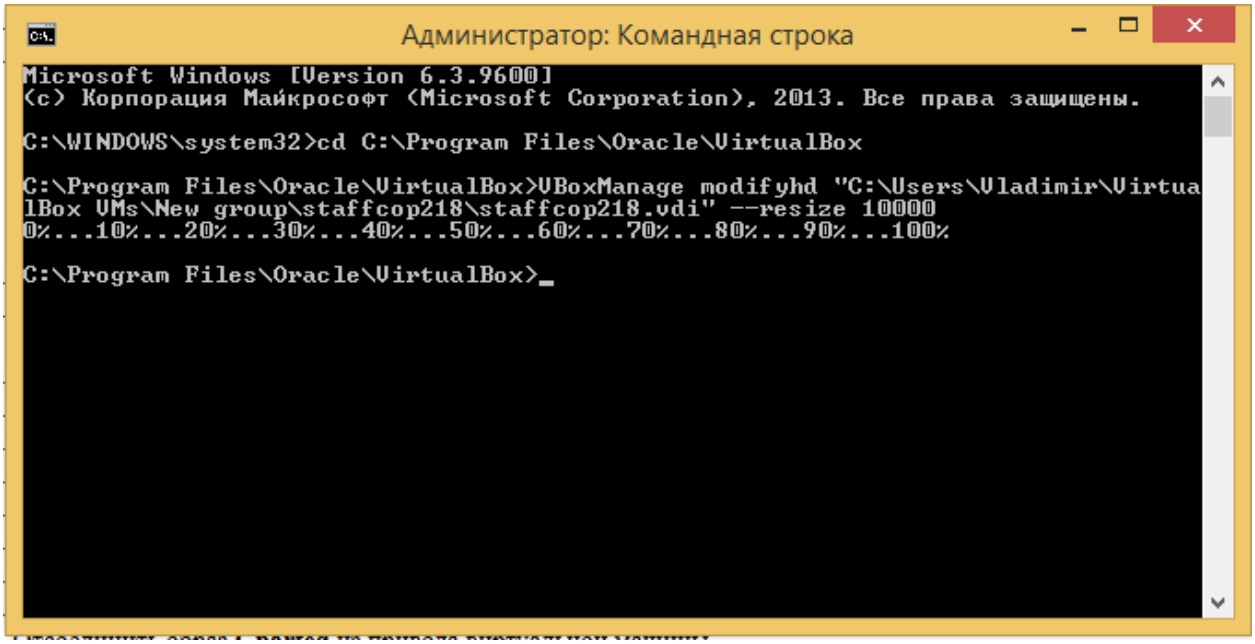
- Выполнить команду:

```
VBoxManage modifyhd «C:\Users\NameUser\VirtualBox VMs\iBatyr Monitor\iBatyr Monitor.vdi»␣
↪--resize X
```

Где X – количество Мб до которого нужно увеличить место диска

Примечание: Путь до диска посмотреть в VirtualBox в машине Настройка → Носители и выделив

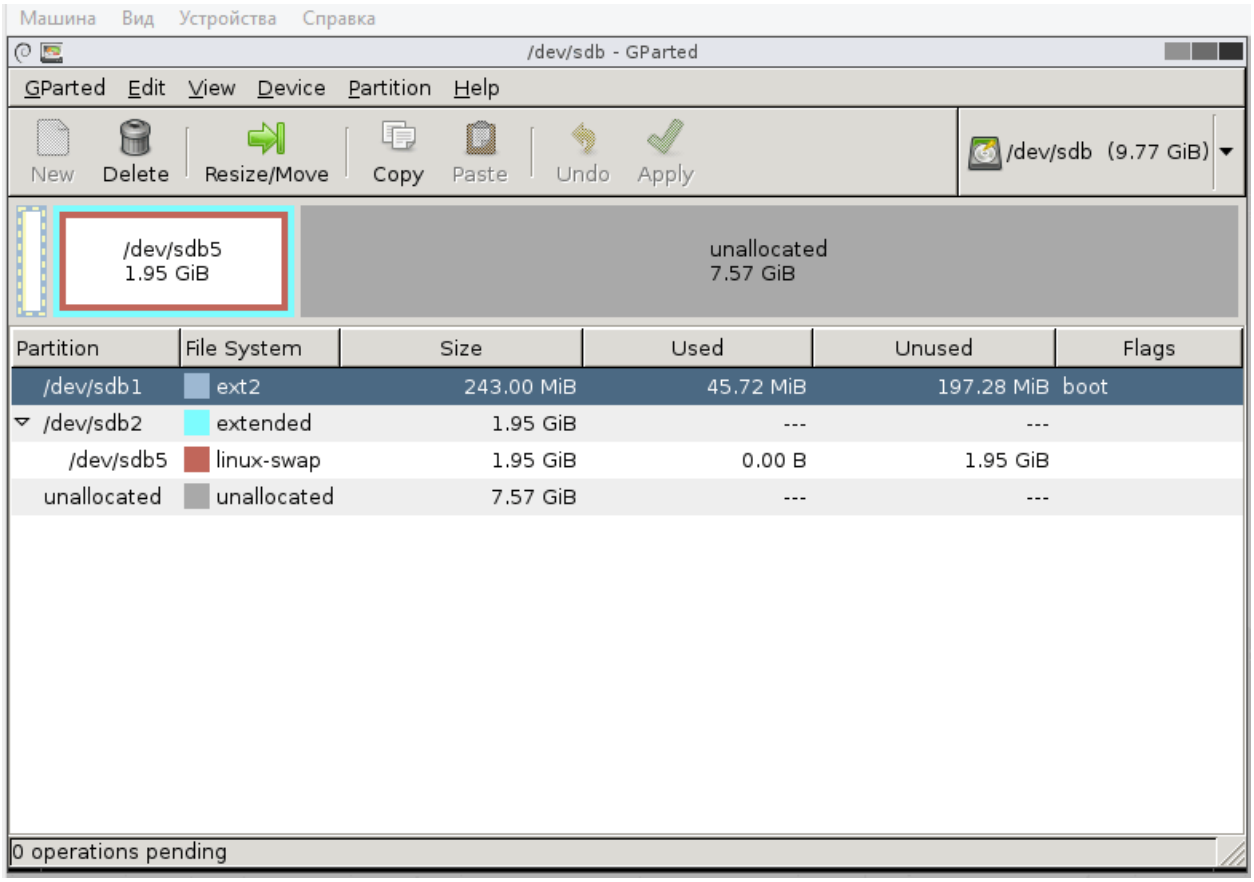
абсолютный пусть диска .vdi. Размер диска задается в МБ



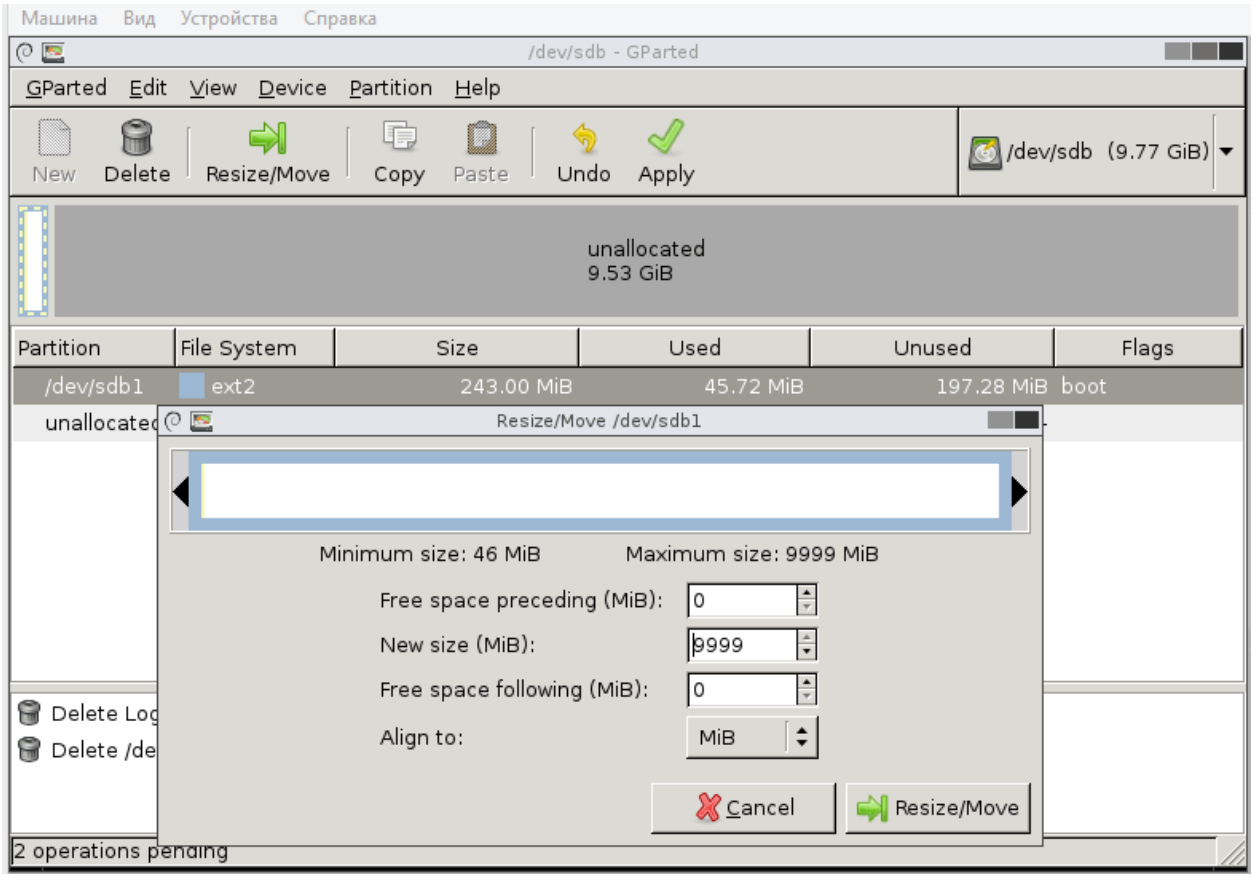
- Скачать образ Gparted, смотри сноску про **Gparted** в конце статьи.
- Выключить виртуальную машину с сервером и перейти в **Настройка** → **Носители** → **Контроллер**: IDE, далее нажать **Добавить привод оптических дисков**, затем подключить скачанный образ **Gparted** и, перейдя на него, выбрать **Первичный мастер IDE**
- Запустить виртуальную машину и произвести вход в операционную среду с **Gparted**

Примечание: Если ранее не работали с подобными программами, то рекомендуем сделать бэкап и сохранить на другом диске//сервере.

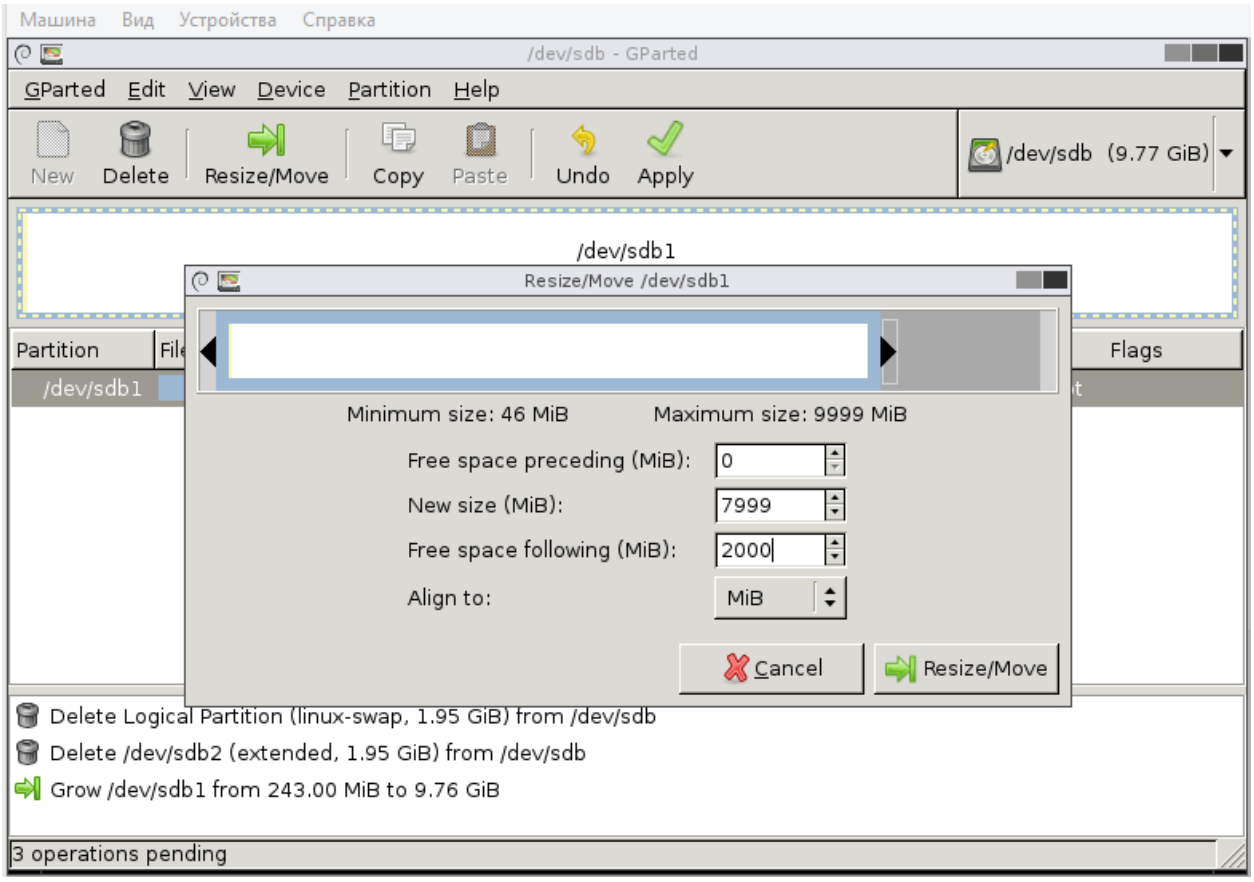
- В программе **Gparted** выбрать диск виртуальной машины сервера (например: **/dev/sdb1**)



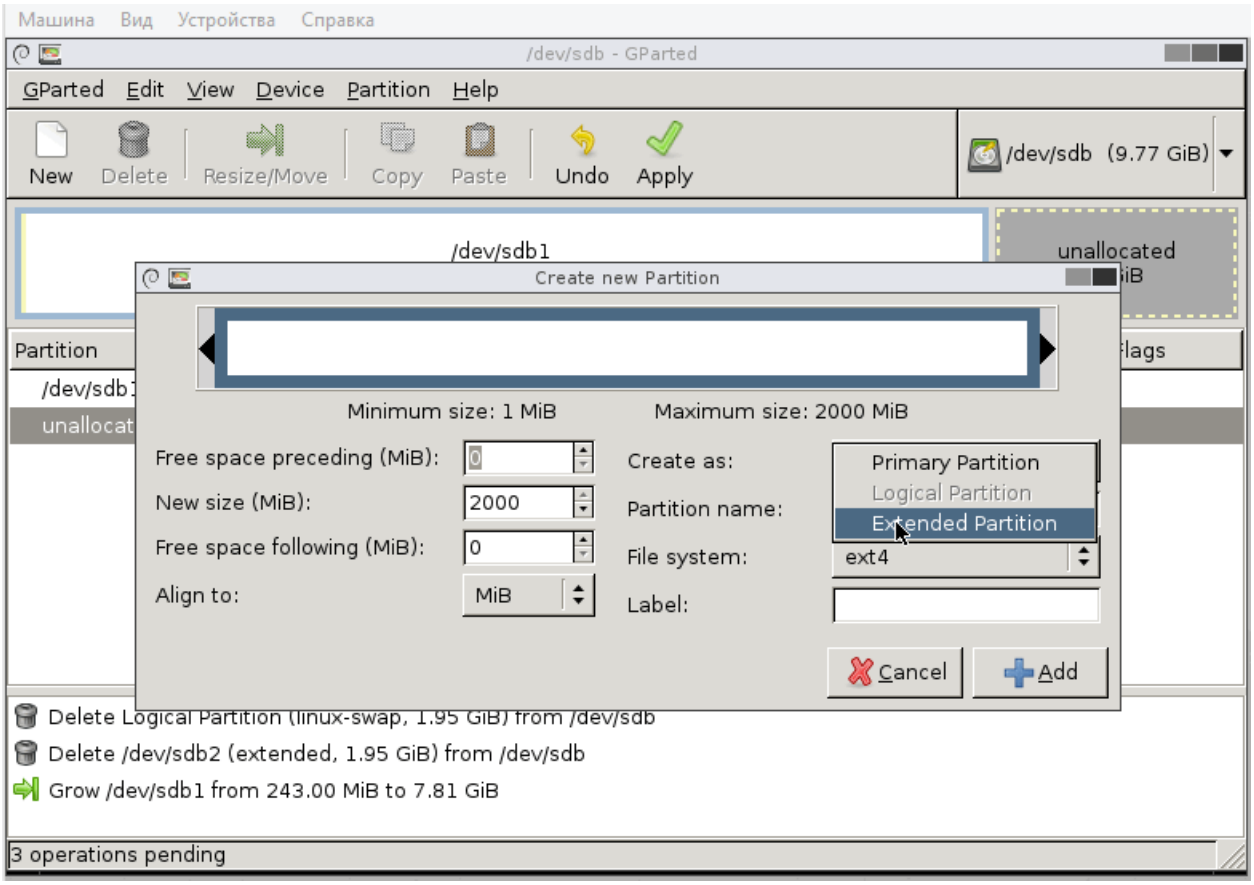
- Удалить разделы **linux-swap** и **extended**
- Увеличить **ext4** до максимума и нажать **Apply**



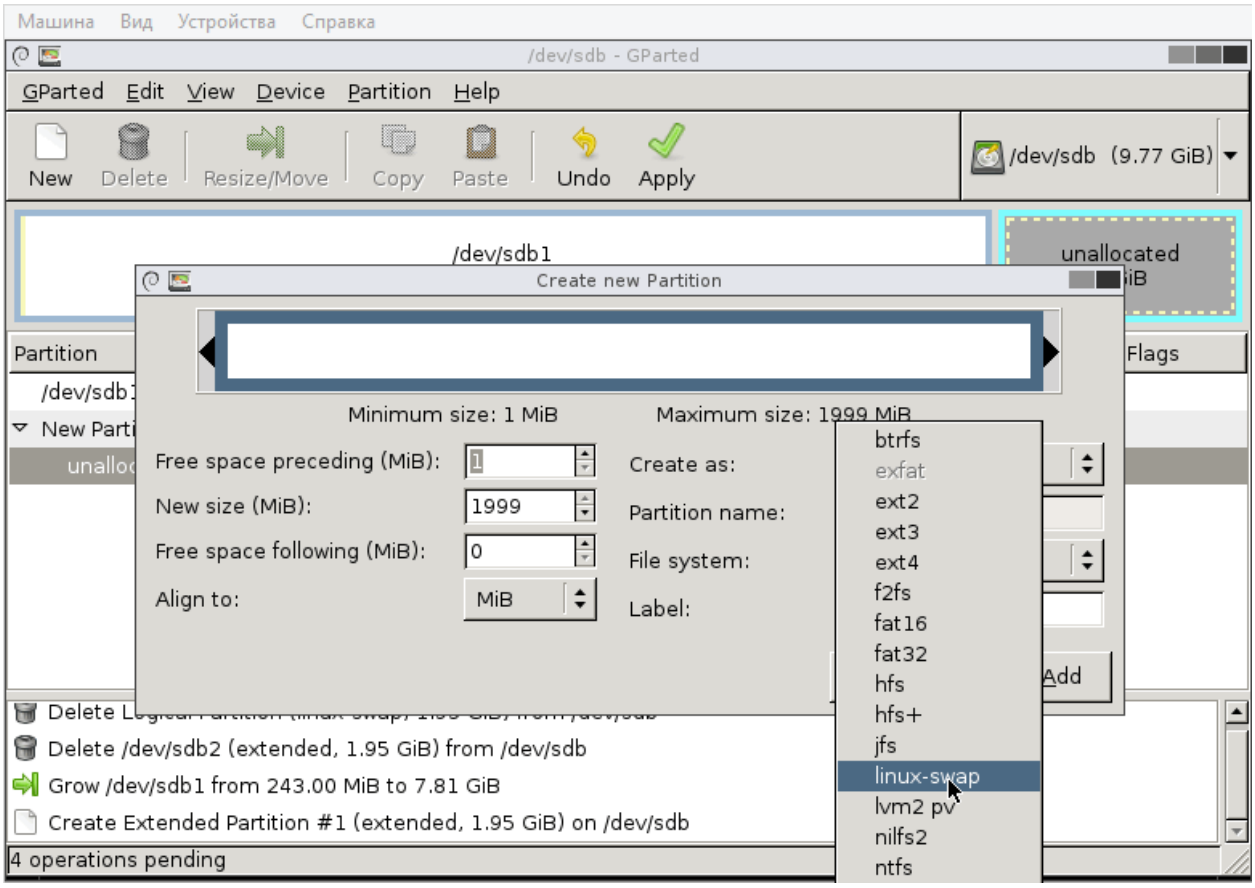
- Изменить размер **ext4**, забрав у него место примерно 2000 МБ



- Создать из свободного с 2000 Мб раздела через контекстное меню **Extended/Расширенный**



- И создать раздел с файловой системой/file system : **linux-swap**



- Нажать **Apply** и выйти из **Gparted**
- Запустить виртуальную машину ibatyr и убедиться, что размер диска увеличен командой: **df –h**
- Проверить сохранность всех данных и настроек сети.

Примечание: Для виртуальных машин **Hyper-V** и **VMware** размер диска увеличивается средствами программ в настройках, а увеличение размера логического раздела производится по аналогии в **Gparted**

Примечание: Все права на продукт Gparted принадлежат сообществу gparted, ссылка на ISO-образ дана локальная, т.к. ресурс **sourceforge**, очень часто бывает недоступен.

3.7.15 Удалённый доступ

Иногда технической поддержке нужен удаленный доступ к рабочему столу для консультации или технических работ.

Для удаленного подключения к рабочим станциям используйте:

- Контур.Доступ — предпочтительный вариант для организации удалённого доступа. Скачать последнюю версию программы можно с официального сайта по прямой ссылке: konturvncids.exe.
- **AnyDesk** — последняя версия программы доступна для скачивания на сайте разработчика.

Будьте готовы к тому, что потребуется подключение по SSH и пользователь с правами администратора.

3.7.16 Проверка контрольных сумм

Начиная сверсии 5.6 доступен инструмент сверки контрольных сумм системных файлов с эталонными значениями, которые были зафиксированы при установке или обновлении.

Сверка контрольных сумм помогает проверить целостность файлов сервера и агентов. Инструмент выявляет изменения, внесённые вручную или вредоносным ПО.

Проверка доступна на:

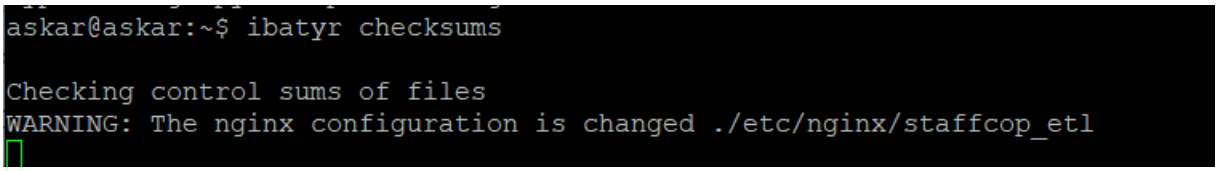
- сервере iBatyr Monitor,
- Windows-агенте версии 5.8.2591 и выше,
- Linux-агенте любой версии.

Сервер

Для проверки контрольных сумм на сервере запустите команду:

```
ibatyr checksums
```

Если файлы подверглись изменениям, команда выведет предупреждение, например:



Агенты

Сверка контрольных сумм на Windows- и Linux-агентах происходит с помощью *скрипта проверки контрольных сумм.*

Примечание: Для получения скрипта *уточните версию агента* и *обратитесь в техническую поддержку*.

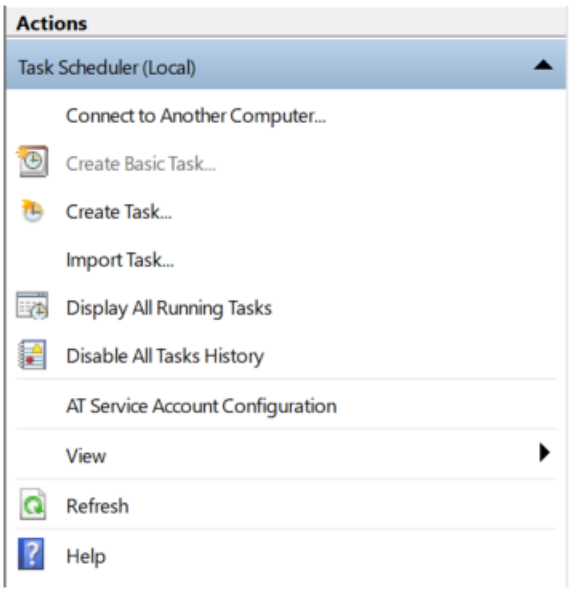
3.7.17 Автоматический запуск виртуальной машины iBatyr Monitor в VirtualBox

После установки серверной части iBatyr Monitor , часто возникает вопрос автоматического запуска этой виртуальной машины при перезагрузке физического сервера.

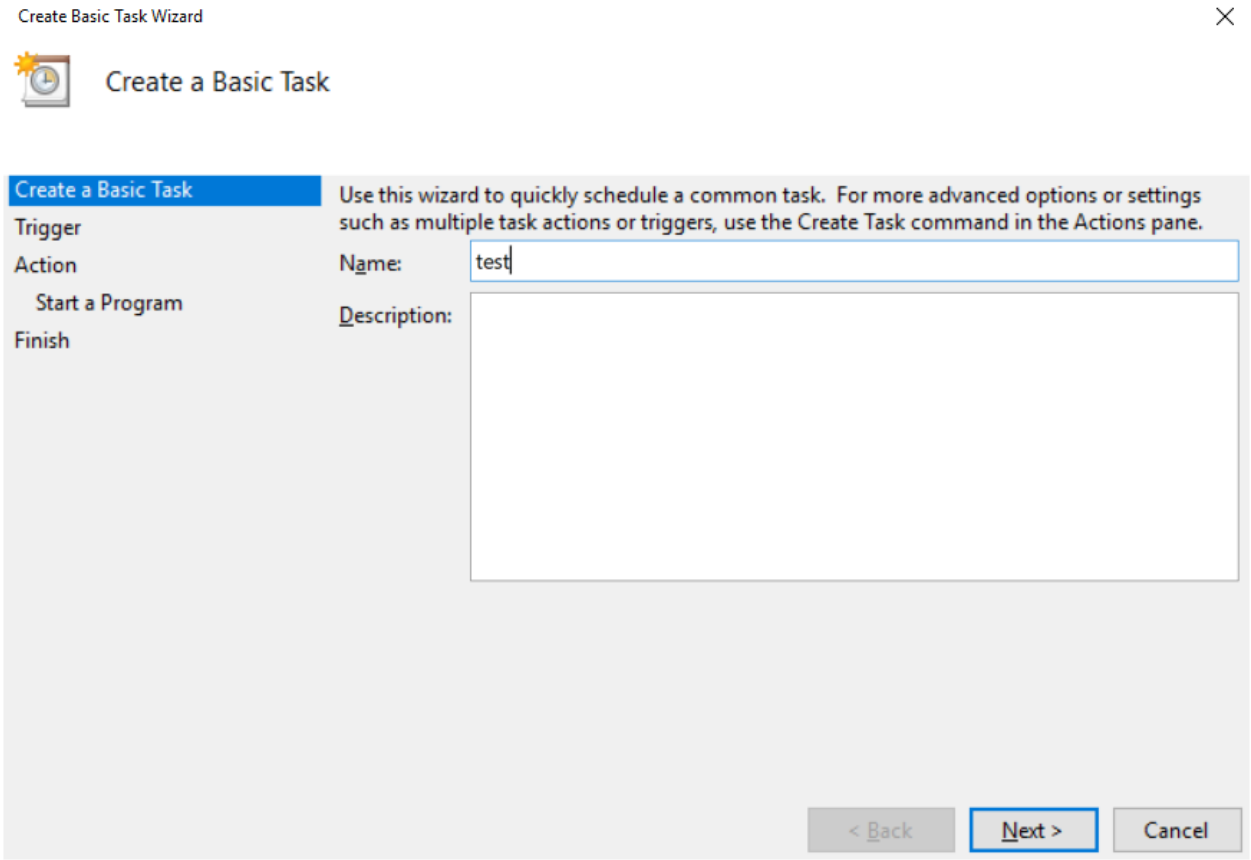
Этот вопрос достаточно легко и надежно решается через встроенный в планировщик Windows функционал.

Шаги для достижения цели автоматического запуска виртуальной машины:

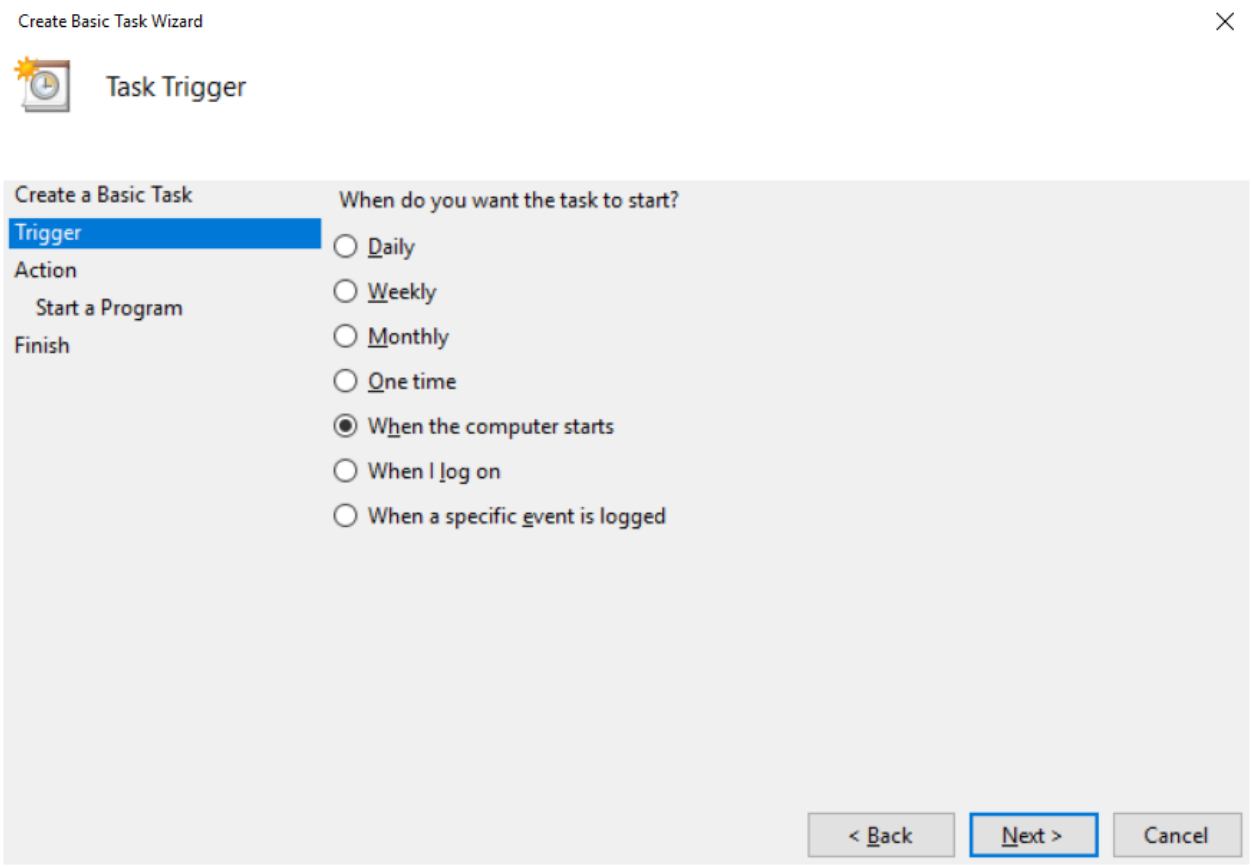
- Открыть планировщик Windows - **Пуск - выполнить - Taskschd.msc** или в строке поиска Windows сразу вписать - **Taskschd.msc**
- Нажать на кнопку «Create basic task..»



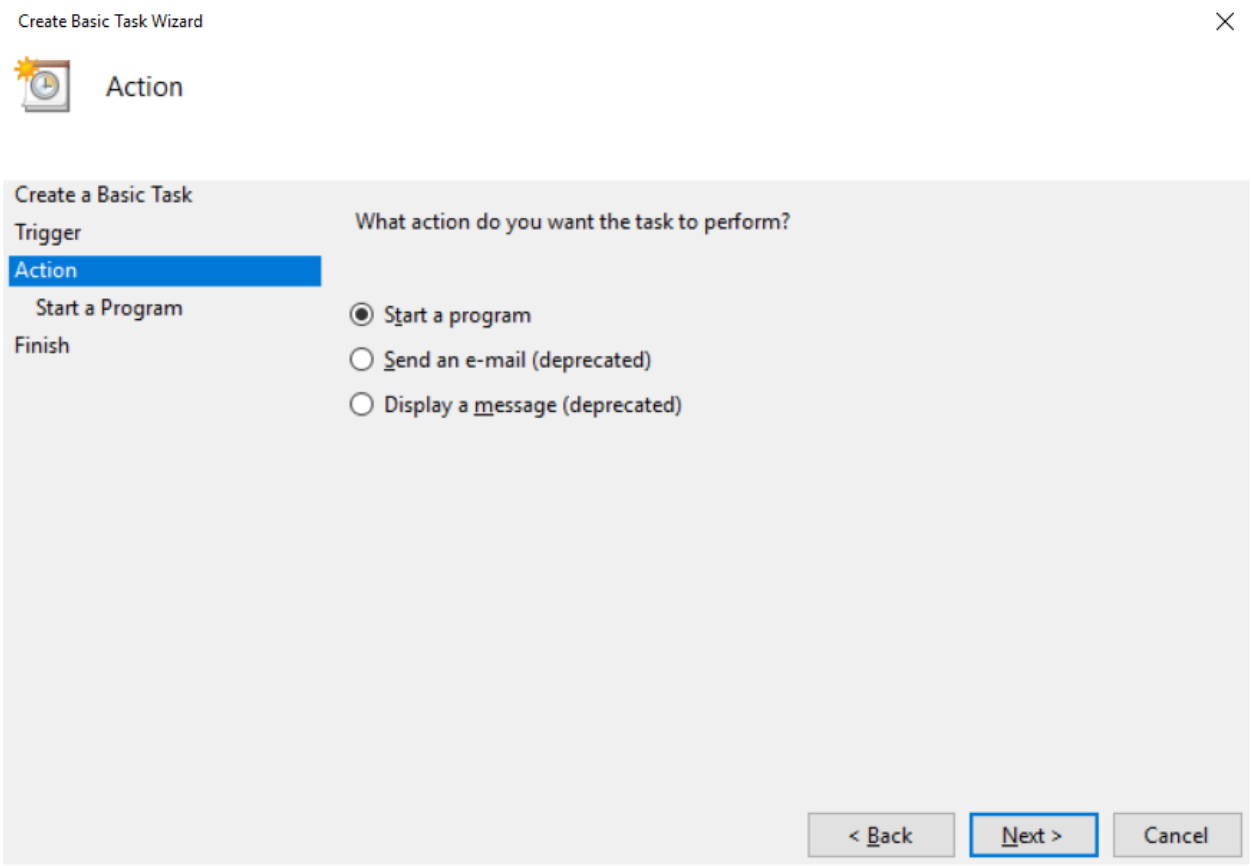
- Указать имя нашего задания, например **test** или **iBatyr**



- Выбрать в в какой период или при каком событии будет выполняться задание, выбираем - **When the computer starts**



- Действие - запустить программу - **Start a programm**

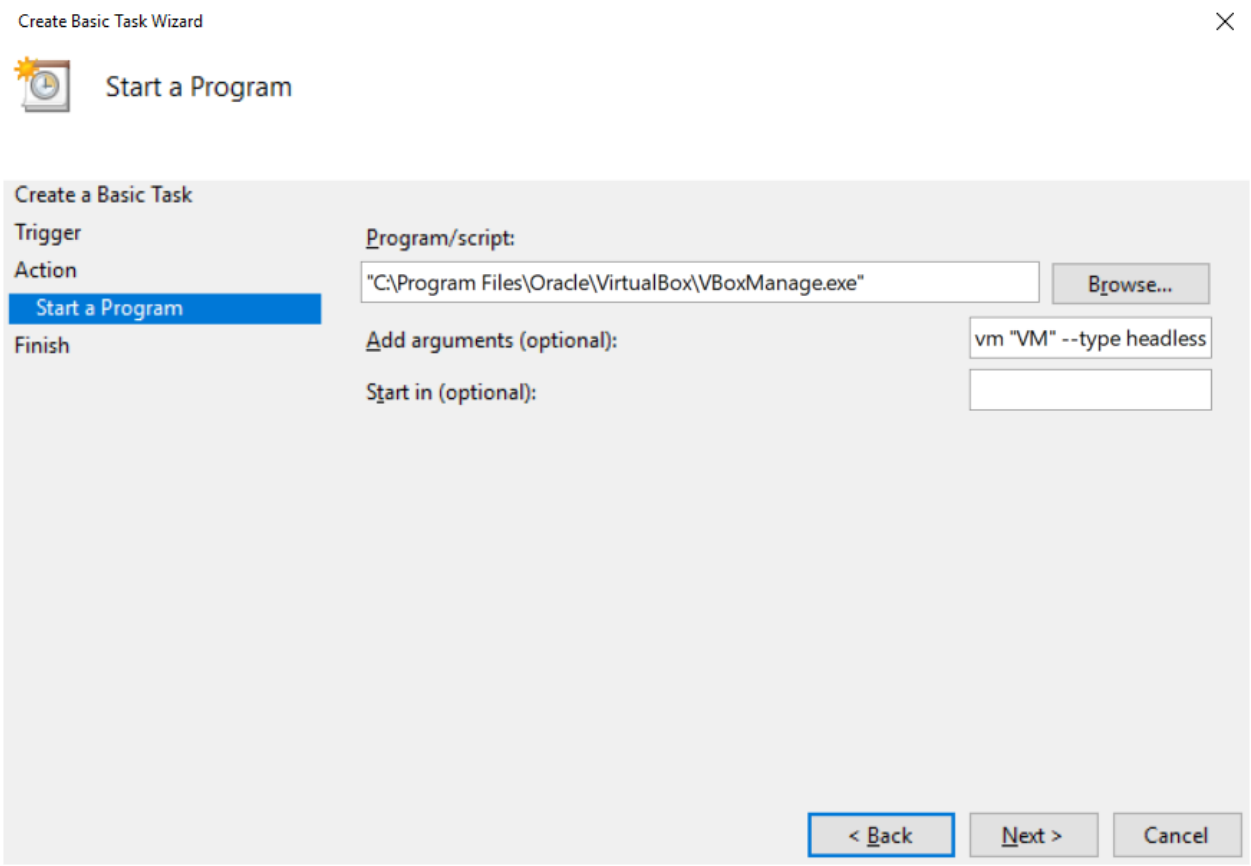


- И указываем параметры запуска программы, в качестве исполняемого файла, указываем

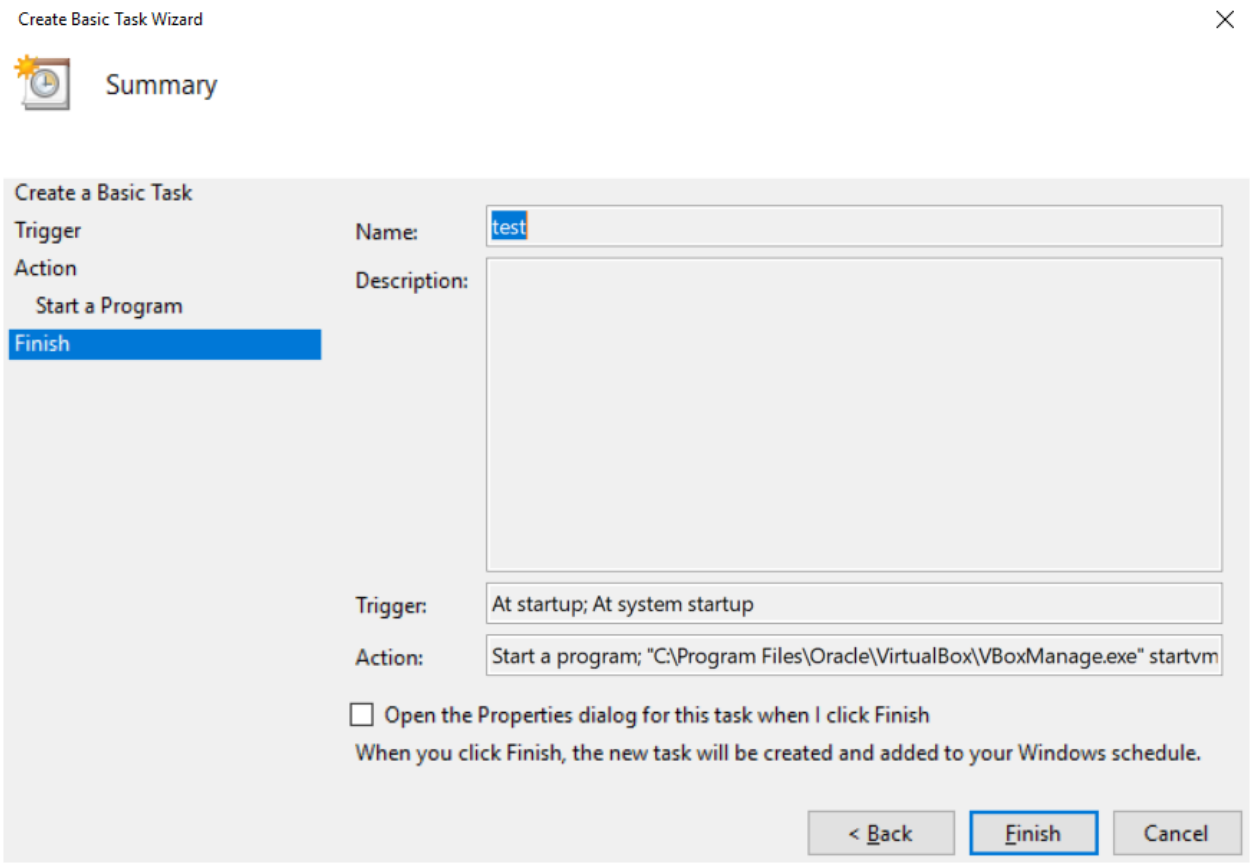
```
C:\Program Files\Oracle\VirtualBox\VBoxManage.exe
```

И дополнительно указываем агументы командной строки

```
startvm ibatyr --type headless
```



- Нажимаем кнопку **Finish**



После этого у нас при перезагрузках системы будет выполняться автоматический запуск виртуальной машины с именем «VM».

3.7.18 Собственный сертификат для пользовательского интерфейса (UI)

URI пользовательского интерфейса и URI для обращения агентов должны быть разными. При этом они могут указывать на один IP адрес.

Чтобы привязать SSL-сертификат к URI пользовательского интерфейса:

1. Получите SSL-сертификат. Это можно сделать различными способами.

Примечание: Обратите внимание, что при генерации ключей (например при помощи *certificate authority windows*), могут появиться лишние записи, что приведёт к ошибкам в работе nginx. Общий вид сертификатов:

```
* для сертификата.key:

  -----BEGIN RSA PRIVATE KEY-----
  ...
  -----END RSA PRIVATE KEY-----

* для сертификата .crt:

  -----BEGIN CERTIFICATE-----
```

(continues on next page)

(продолжение с предыдущей страницы)

```
...
-----END CERTIFICATE-----
```

2. Разместите приватный ключ и сертификат на сервере в папке **/var/lib/ibatyr/CA**.
3. Создайте копию конфигурационного файла **/etc/nginx/sites-available/ssl.ibatyr**

```
cp /etc/nginx/sites-available/ssl.ibatyr /etc/nginx/sites-available/ssl.
↪ibatyrui
```

4. Отредактируйте конфигурационный файл:

```
sudo nano /etc/nginx/sites-available/ssl.ibatyr
```

Приведите следующие поля к указанному виду:

tabularytabulary

Поле
location
server_name

5. Отредактируйте созданный конфигурационный файл:

```
sudo nano /etc/nginx/sites-available/ssl.ibatyrui
```

Приведите следующие поля к указанному виду:

tabularytabulary

Поле
server_name
ssl_certificate
ssl_certificate_key
ssl_client_certificate
ssl_verify_depth
ssl_verify_client

Примечание: Чтобы вести раздельные логи для UI и агента, укажите пути к логам UI в полях **access_log** и **error_log**.

6. Создайте символьную ссылку на новый конфигурационный файл:

```
ln -s /etc/nginx/sites-available/ssl.ibatyrui /etc/nginx/sites-enabled
```

7. Проверьте правильность новой конфигурации nginx:

```
sudo nginx -t
```

8. Примените новую конфигурацию:

```
systemctl reload nginx
```

Единый конфигурационный файл

Для удобства работы, новые настройки можно добавить в уже существующий конфигурационный файл.

Для этого:

1. Откройте конфигурационный файл:

```
sudo nano /etc/nginx/sites-available/ssl.ibatyr
```

2. Приведите его к виду:

```
client_max_body_size 10G;
large_client_header_buffers 16 65536;

server
{
    server_name ui.iBatyr Monitor.local;
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    ssl on;
    ssl_certificate /var/lib/ibatyr/CA/server_UI.crt;
    ssl_certificate_key /var/lib/ibatyr/CA/server_UI.key;
    ssl_client_certificate /var/lib/ibatyr/CA/client_UI.crt;
    ssl_verify_depth 1;
    ssl_verify_client off;

    access_log /var/log/ibatyr/https.access.log;
    error_log /var/log/ibatyr/https.error.log;

    client_body_timeout 3600s;
    client_header_timeout 3600s;

    location /
    {
            include /etc/nginx/uwsgi_params_ibatyr;
            uwsgi_pass unix:/var/lib/ibatyr/ui_wsgi.sock;
    }
    include /etc/nginx/ibatyr_*;
}

server
{
    server_name agent.iBatyr Monitor.local;
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    ssl on;
    ssl_certificate /var/lib/ibatyr/CA/server.crt;
    ssl_certificate_key /var/lib/ibatyr/CA/server.key;
    ssl_client_certificate /var/lib/ibatyr/CA/client.crt;
    ssl_verify_depth 2;
    ssl_verify_client optional;
```

(continues on next page)

(продолжение с предыдущей страницы)

```
    ssl_session_timeout 1d;
    ssl_session_tickets off;
    ssl_stapling on;
    ssl_protocols TLSv1.3 TLSv1.2;
    ssl_ecdh_curve secp384r1;
    ssl_prefer_server_ciphers on;
    ssl_ciphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-
↪RSA-AES256-GCM-SHA384;

    access_log /var/log/ibatyr/https.access.log;
    error_log /var/log/ibatyr/https.error.log;

    client_body_timeout 3600s;
    client_header_timeout 3600s;

    location ~^/agent/$
    {
            include /etc/nginx/uwsgi_params_ibatyr;
            uwsgi_pass unix:/var/lib/ibatyr/ui_wsgi.sock;
    }

    include /etc/nginx/ibatyr_*;
}
```

3. Проверьте правильность новой конфигурации nginx:

```
sudo nginx -t
```

4. Примените новую конфигурацию:

```
systemctl reload nginx
```

3.7.19 Ручное обновление агентов средствами сервера

1. Необходимо создать конфиг с именем AGENT_UPDATE.
2. Перенести всех агентов, которых надо обновить в AGENT_UPDATE.
3. На сервере, в терминале, необхоидмо выполнить команду, в которой надо только обновить NEEDED_VERSION.

```
echo "UPDATE agent_config SET agent_build_number=NEEDED_VERSION where id=(select id from␣
↪agent_config where name_ru='AGENT_UPDATE' or name_en='AGENT_UPDATE')" |ibatyr sql;
```

3.7.20 Отключение модулей

Если в вашей компании существует какие-то юридические документы согласно которым вы не можете осуществлять сбор данных по определенным событиям, то возможно отключить модули, отвечающие за эти типы событий.

Список модулей:

```
AccountModule, ApplicationModule, ActivityModule, ScreenshotModule,␣
↪KeyboardClipboardModule,
NetworkProxyModule, InternetModule, CommunicationModule, FileModule, DeviceModule,
PrintingModule, WebCamModule, MicModule, RemoteAdminModule, DesktopVideoModule,
InventoryModule, WorkplacePresenceModule, LinuxModule, WLanModule, DlpModule,␣
↪FileScanModule.
```

Например, в компании нельзя осуществлять и делать снимки с веб-камер АРМ. Для отключения данных модулей необходимо проделать следующие действия:

1. Открыть в любом текстовом редакторе файл **/etc/ibatyr/config**
2. Найти нужные нам модули из списка выше и добавить их в конец файла в формате DISABLE_MODULES=[„name“]

```
DISABLE_MODULES=['MicModule', 'WebCamModule']
```

3.7.21 SystemD

Начиная с версии 16.04, в Ubuntu сменилась система инициализации. Иногда это ведет к появлению 502 ошибки, потому что сервис iBatyr Monitor не стартует автоматически. Для решения этой проблемы нужно явно разрешить запуск данного юнита. sudo systemctl enable ibatyr

Другие команды для юнитов: Незамедлительно запустить юнит:

```
systemctl start unit
```

Незамедлительно остановить юнит:

```
systemctl stop unit
```

Перезапустить юнит:

```
systemctl restart unit
```

Запросить у юнита перезагрузку его настроек:

```
systemctl reload unit
```

Показать статус юнита, а также запущен он или нет:

```
systemctl status unit
```

Проверить, включен ли юнит в автозапуск при загрузке системы:

```
systemctl is-enabled unit
```

Включить юнит в автозапуск при загрузке системы:

```
systemctl enable unit
```

Убрать юнит из автозапуска при загрузке системы:

```
systemctl disable unit
```

Маскировать юнит, чтобы сделать невозможным его запуск:

```
systemctl mask unit
```

Снять маску юнита:

```
systemctl unmask unit
```

Показать страницу справочного руководства, связанного с юнитом (необходима поддержка этой функции в указанном файле юнита):

```
systemctl help unit
```

Перезагрузить systemd для поиска новых или измененных юнитов:

```
systemctl daemon-reload
```

все логи с момента последний загрузки

```
journalctl -b
```

фильтруем по дате.

```
$ journalctl ---since yesterday
$ journalctl --since 09:00 --until now
$ journalctl --since 10:00 --until "1 hour ago"
```

фильтруем по службам

```
journalctl -u nginx.service
```

по службам за период времени.

journalctl -u nginx.service –since yesterday

```
journalctl -u nginx.service -u php-fpm.service -since today
```

по ID

```
journalctl _PID=381
```

по ID

```
journalctl _UID=33
```

кто есть в логах

```
journalctl -F _UID
```

все фильтры

```
man systemd.journal-fields
```

смотрим по пути

```
journalctl /usr/bin/docker
```

что там у ядра

```
journalctl -k
```

по уровню ошибок

```
journalctl -k
```

ошибки такие:

- 0 — **EMERG** (система неработоспособна);
- 1 — **ALERT** (требуется немедленное вмешательство);
- 2 — **CRIT** (критическое состояние);
- 3 — **ERR** (ошибка);
- 4 — **WARNING** (предупреждение);
- 5 — **NOTICE** (всё нормально, но следует обратить внимание);
- 6 — **INFO** (информационное сообщение);
- 7 — **DEBUG** (отложенная печать).

вывод без less

```
journalctl --no-pager
```

форматы логов.

```
journalctl  -u nginx.service -o json
```

вот такие

- **cat** — только сообщения из логов без служебных полей;
- **export** — бинарный формат, подходит для экспорта или резервного копирования логов;
- **short** — формат вывода syslog;
- **short-iso** — формат вывода syslog с метками времени в формате ISO 8601;
- **short-monotonic** — формат вывода syslog с метками монотонного времени (monotonic timestamp);
- **short-precise** — формат вывода syslog с метками точного времени (время событий указывается с точностью до микросекунд);
- **verbose** — максимально подробный формат представления данных (включает даже те поля, которые в других форматах не отображаются).

недавние

```
journalctl -n
```

реал тайм

```
journalctl -f
```

сколько логов?

```
journalctl --disk-usage
```

ужать логи до

```
sudo journalctl --vacuum-size=1G
```

ужать логи по времени

```
sudo journalctl --vacuum-time=1years
```

то же в конф файле

```
/etc/systemd/journald.conf, which contain next parameters:
```

- **SystemMaxUse** = максимальный объём, который логи могут занимать на диске;
- **SystemKeepFree** = объём свободного места, которое должно оставаться на диске после сохранения логов;
- **SystemMaxFileSize** = объём файла лога, по достижении которого он должен быть удален с диска;
- **RuntimeMaxUse** = максимальный объём, который логи могут занимать в файловой системе /**run**;
- **RuntimeKeepFree** = объём свободного места, которое должно оставаться в файловой системе /**run** после сохранения логов;
- **RuntimeMaxFileSize** = объём файла лога, по достижении которого он должен быть удален из файловой системы /**run**.

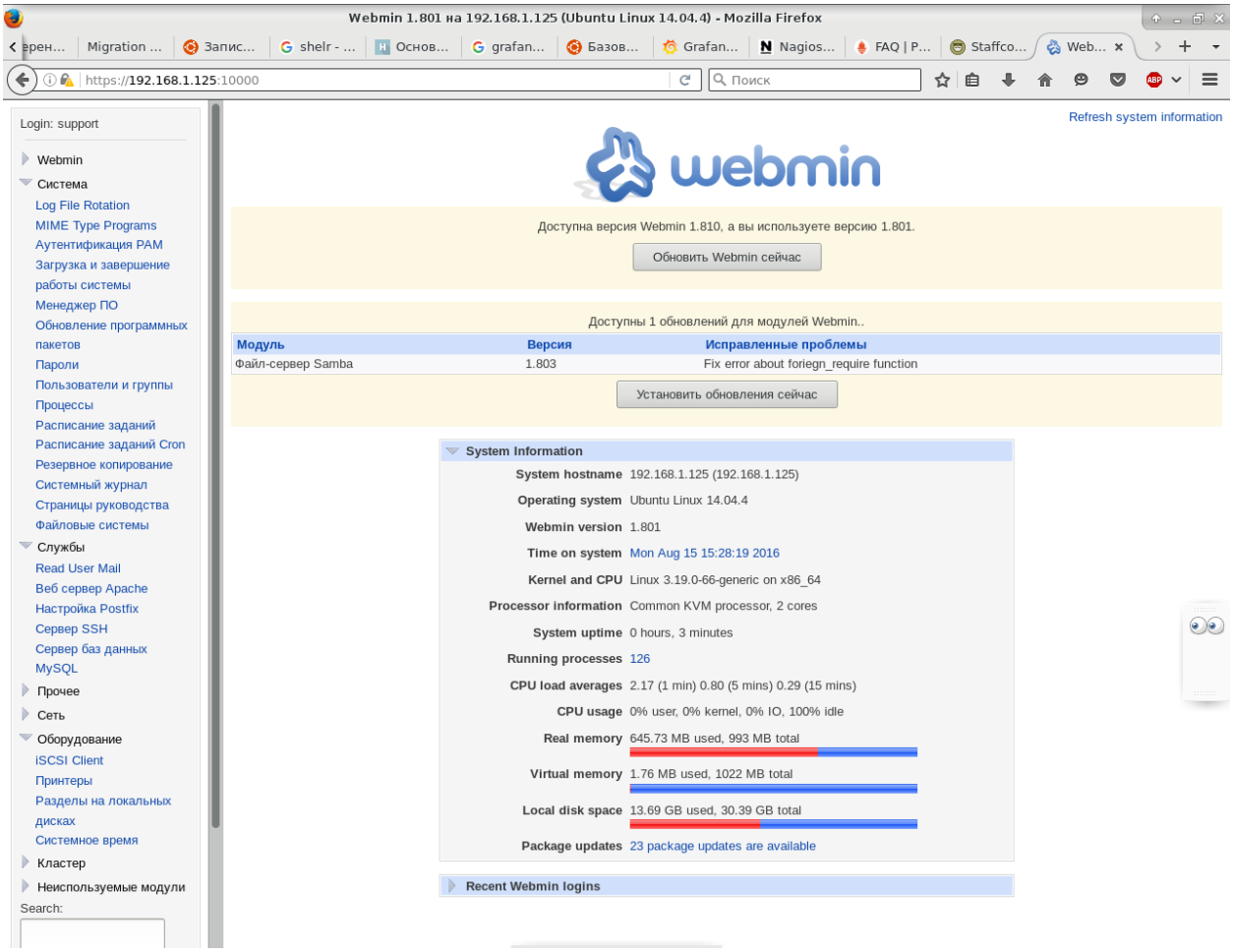
Централизованное хранение логов

```
systemd-journal-remote --url https://some.host:19531/
```

3.7.22 Webmin

Webmin — веб-интерфейс для администрирования серверов под управлением Unix-систем. Это удобная графическая оболочка, которая позволяет управлять сервером без командной строки через браузер.

Подробное описание Webmin представлено на .



3.7.23 Установка

Добавьте репозиторий в список, который использует APT для установки на вашем сервере:

```
curl -o setup-repos.sh https://raw.githubusercontent.com/webmin/webmin/master/setup-
↪repos.sh

sh setup-repos.sh
```

Обновите список репозиториев:

```
sudo apt update
```

Установите Webmin:

```
apt-get install webmin --install-recommends
```

Если на сервере установлен стандартный фаервол UFW, добавьте порт **10000** в список исключений:

```
sudo ufw allow 10000
```

Чтобы получить доступ к веб-интерфейсу, откройте в браузере *https://ip_адрес_сервера_ibatyr:10000*.

Для входа используйте логин и пароль терминала сервера.

3.7.24 Восстановление пароля

В случае утери пароля его можно восстановить несколькими способами, в зависимости от того, какой именно пароль был утерян - от операционной системы сервера (Linux) или от веб-консоли администратора.

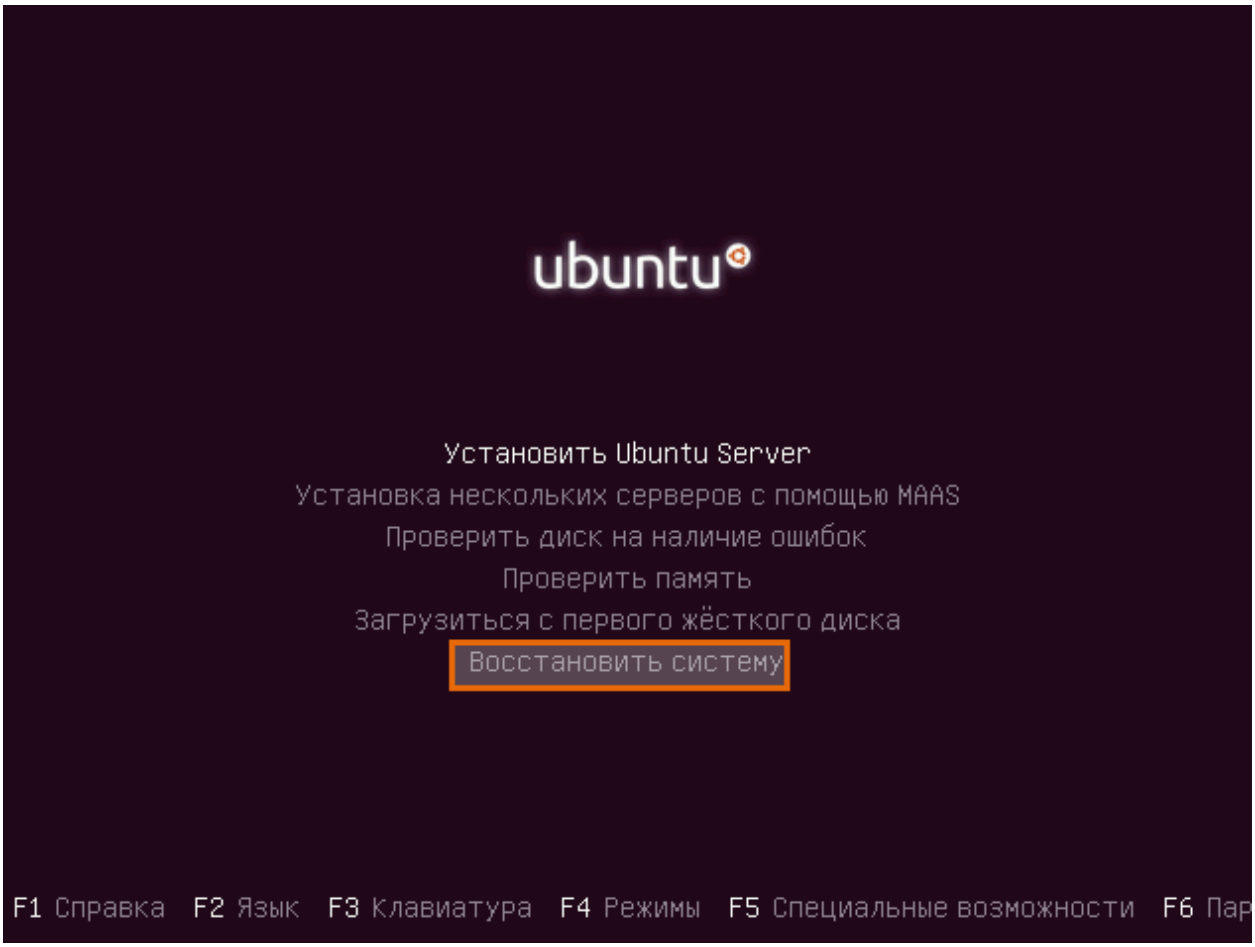
Пароль от Linux

Восстановить пароль от операционной системы можно двумя способами:

- с использованием загрузочного диска;
- через BIOS.

Первый способ

Загрузитесь с установочного образа, который использовали для первоначальной установки системы и выберите «восстановить систему».



Следуйте указаниям установщика пока не попадете в консоль. В консоли выполните команду

```
sudo passwd user_name
```

и задайте новый пароль.

Имя пользователя можно узнать с помощью команды

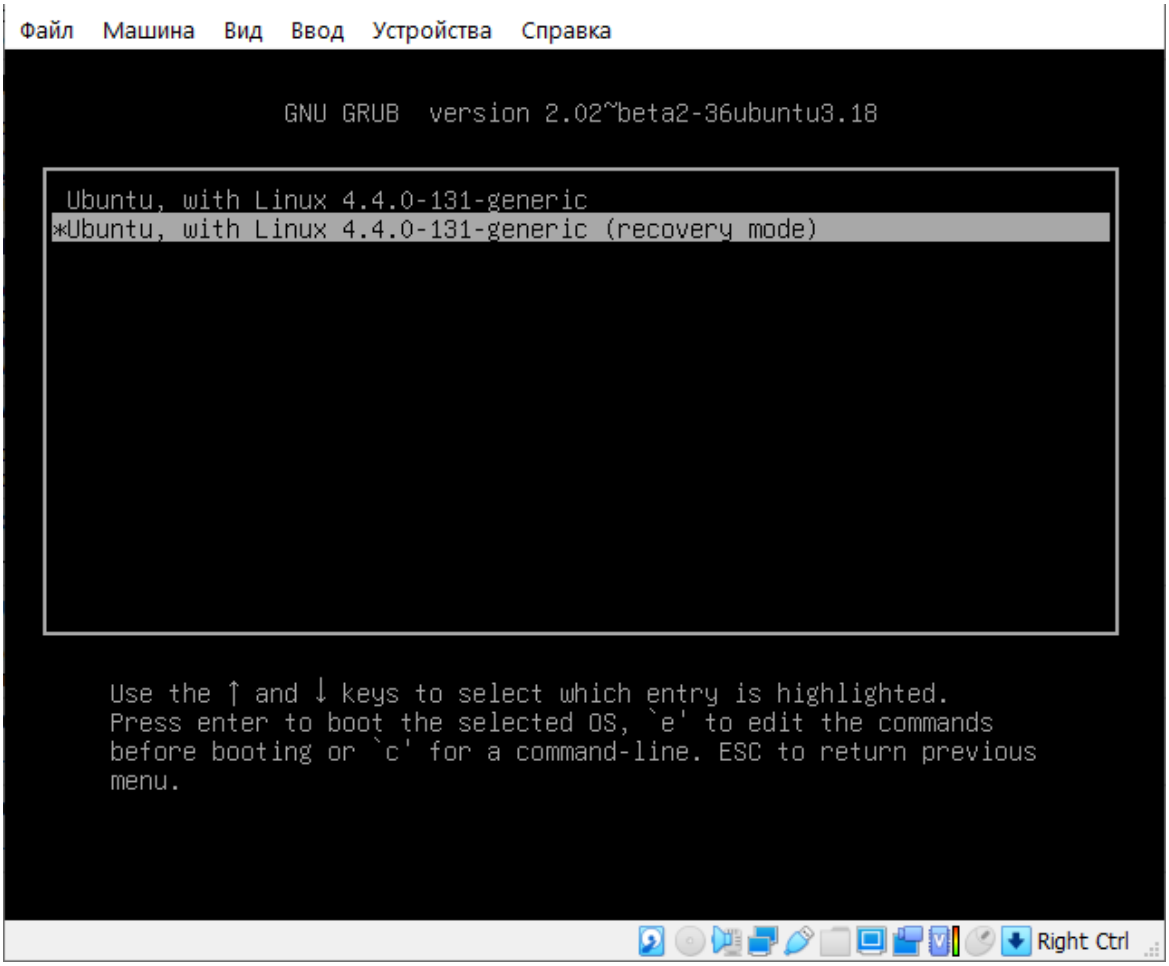
```
cat /etc/passwd
```

Результат работы команды будет примерно таким:

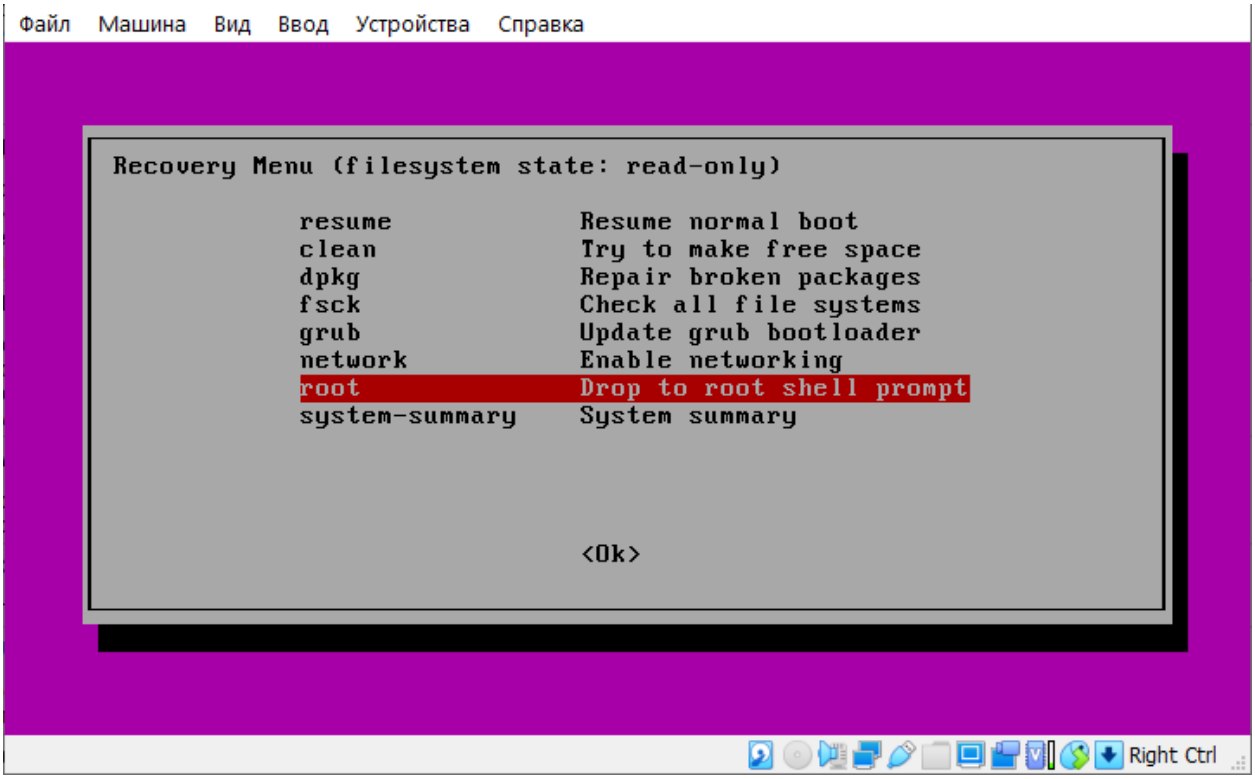
Ваш пользователь - с id 1000 и более и расположен в самой нижней строчке.

Второй способ

Чтобы попасть в BIOS системы или виртуальной машины нажмите **Shift** сразу после загрузки. В открывшемся окне выберите «Recovery Mode» и подождите пока появится меню выбора вариантов:



Выберите «root»:



Из root-консоли выполните следующие действия:

1. Примонтируйте файловую систему в режиме записи.

```
mount -o remount,rw /
```

2. Смените пароль пользователю **support**.

```
passwd support
```

3. Перезагрузите машину.

```
reboot
```

Восстановление пароля от веб-интерфейса

Чтобы восстановить или изменить пароль от веб-интерфейса введите в консоли команду

```
sudo ibatyr passwd NEWPASSWORD
```

где NEWPASSWORD - новый пароль от суперпользователя веб-консоли **admin**.

3.7.25 Импорт и экспорт настроек и конфигураций сервера

Предупреждение: Для успешного импорта версии серверов должны совпадать.

Чтобы создать резервную копию всех пользовательских конфигураций на сервере, используйте команду:

```
sudo ibatyr dumpdata agent.Config --indent 4 > config.json
```

где

- *–ident 4* — задаёт четыре пробела для отступа на каждом уровне вложенности для удобства чтения;
- *config.json* — файл JSON, в котором сохранится резервная копия.

Для полной выгрузки всех фильтров, конфигураций и пользователей используйте команду:

```
sudo ibatyr dumpdata --indent=4 -n analytics.filter analytics.backupfilter analytics.
↪corpusprocessfilter analytics.sessionprocessfilter analytics.extractextprocessfilter␣
↪analytics.dimensioncardfilter auth.user agent.config agent.acl agent.accountacl agent.
↪accountconfig > backup.json
```

Экспорт вместе с фильтрами:

Примечание: Убедитесь, что путь до файла указан полностью.

```
ibatyr export [filename].json
```

Импорт вместе с фильтрами:

Примечание: Убедитесь, что путь до файла указан полностью.

```
ibatyr import [filename].json
```

3.7.26 Удалённое копирование

Перенос файлов с//на удалённых серверов можно выполнять так:

```
sudo scp -rpC -c blowfish source/. user@server:/folder
```

где:

- r - рекурсивное копирование (для каталогов),
- p - сохранение времени создания файла,
- C - сжатие файлов (неактуально при передаче сжатых компрессором файлов),
- c - наиболее быстрый протокол шифрования.

В случае наличия особых потребностей при копировании воспользуйтесь справкой по команде scp.

```
man scp
```

Также можно запускать удалённое копирование с третьего сервера между двумя другими.

Для копирования вам потребуется знание пароля удалённого пользователя либо наличие его ключа (в зависимости от схемы авторизации) и наличие у этого пользователя прав на запись в папку назначения.

Если вы производите копирование из под системного аккаунта - **root**, то нужно после переноса файлов проверить, что целевой пользователь (в т.ч. системный) имеет право на доступ к папкам и право на запись.

Например, выполнив команду:

```
ls -l /folder/subfolder
```

Если нужно - смените владельца командой

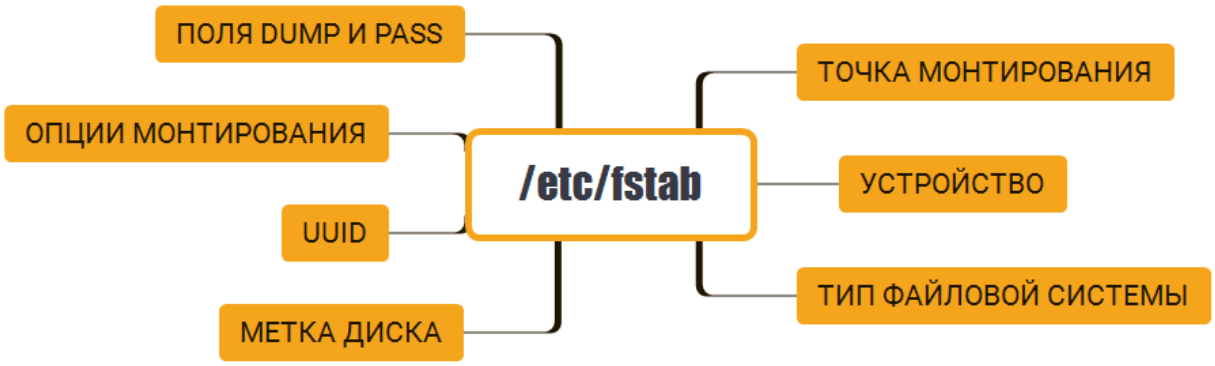
```
sudo chmod -R user:user /folder/subfolder
```

Либо при помощи **rsync**:

```
rsync -avh /path/to/files user@server:/new_path
```

3.7.27 Монтирование дисков

Данная статья предназначена для тех, кто по необходимости или из интереса хочет разобраться в работе команды mount чуть глубже. Для начала введем общие понятия, которые применяются в работе с **mount**.



tabularytabulary

	filesystem	dir	type
	Ваше устройство	Точка монтирования	тип ФС
	/dev/sda3	/home	xfs

Эта запись означает, что устройство **/dev/sda3** будет смонтировано в каталог **/home**, а монтироваться будет автоматически, для чтения и записи.

Тип файловой системы **-XFS**, резервных копий делаться не будет, а проверка целостности фс будет осуществляться при каждом монтировании.

Такого же результата мы могли добиться при вводе следующей команды вручную:

```
mount -t xfs /dev/sda3 /home
```

Примечание: Итого **fstab** может рассматриваться как автоматизация обязательных монтирований.

Более того, указывать тип ФС не обязательно, если это только не есть некая экзотическая файловая система. Структура каталогов в linux является древовидной, с корнем в / Каждый новый носитель информации, будь то жёсткий диск, dvd диск, usb флэшка или сетевой ресурс подключается посредством монтирования, и его файловая структура отображается в определённой папке.

Монтирование может быть проведено вручную, командой:

```
mount
```

Либо автоматически, для этого нужный диск/устройство должно быть прописано в конфигурационном файле **/etc/fstab**

Файл **/etc/fstab** состоит из колонок, разделителями между которыми являются символы табуляции (клавиша TAB).

В общем виде там имеется 6 полей:

- **Устройство**, по пути (/dev/sda /dev/hda /dev/sr0 /dev/sdb1 и т.п.) либо по т.н. уникальному идентификатору - UUID.

UUID генерируется утилитами mkfs. при создании файловой системы. Утилита **blkid** - показывает **UUIDs** устройств и разделов: В этом случае поле имеет вид **UUID=«550e8400-e29b-41d4-a716-446655440000**

- **Точка монтирования** - это папка, в которой будет видна файловая система подключаемого устройства.

- Тип файловой системы - Чаще всего вам придётся иметь дело с фс **ext4**, т.к. это файловая система по умолчанию для большинства дистрибутивов Linux, а также с **ntfs** и **vfat** - двумя файловыми системами от компании Microsoft.
- **Опции** - Включает в себя дополнительные опции, как то: rw - чтение-запись, ro - только чтение. Подробнее можно посмотреть здесь или тут.
- **Dump** - Используется утилитой dump для определения того, нужно ли создать резервную копию данных в файловой системе. Возможные значения: 0 или 1. Если указано число 1, dump создаст резервную копию. У большинства пользователей утилита dump не установлена, поэтому им следует указывать 0 в этом поле.
- **Проверка диска** - Используется программой **fsck** для определения того, нужно ли проверять целостность файловой системы. Возможные значения: 0, 1 или 2. Значение 1 следует указывать только для корневой файловой системы (с точкой монтирования /); для остальных ФС, которые вы хотите проверять, используйте значение 2, которое имеет менее высокий приоритет.Обратите внимание, что в случае btrfs следует всегда указывать 0, даже если эта файловая система используется в качестве корневой. Файловые системы, для которых в поле указано значение 0, не будут проверяться **fsck**.

3.7.28 Обновление системы

Разработчики Ubuntu регулярно выпускают обновления отдельных программ, повышающие безопасность, и исправляющие мелкие ошибки. Рекомендуется регулярно производить обновление системы. Это делается при помощи двух последовательно вводимых команд, для удобства объединённых в одну:

```
sudo apt-get update && sudo apt-get upgrade -y
```

Примечание: Для выполнения этого действия вам требуется выполнять его от пользователя, имеющего доступ к привилегиям root, и знать его пароль.

В случае с импортом из ova это пользователь support. Обновление может занять некоторое время, тем большее, чем больше времени прошло с момента создания ova образа либо последнего обновления. В среднем на обновление уходит несколько минут. Также для обновления требуется доступ в интернет.

После завершения обновления можно выполнить команды

```
sudo apt-get autoclean
```

С их помощью мы можем удалить неиспользуемые пакеты, если они имеются, и почистить архив пакетов.

Обновление iBatyr Monitor

Процесс обновления iBatyr Monitor *описан в этом разделе базы знаний.*

3.7.29 Оптимизация

Базы данных

Чтобы определить оптимальные настройки для конфигурации и нагрузки, используйте калькулятор конфигурации PostgreSQL. Если на сервере БД работают iBatyr Monitor и другие сервисы, учитывайте потребляемые ими ресурсы.

Программная часть

Не рекомендуем использовать VirtualBox, если сеть насчитывает более 10 агентов. Используйте серверный вариант ОС, например Ubuntu 20.04 Server.

Дисковая подсистема

В опции монтирования используйте **noatime**, чтобы не фиксировать запись последнего доступа к файлам:

```
/dev/sdX /your_point/mount ext4 rw,noatime 0 2
```

Устанавливайте iBatyr Monitor на отдельный диск, чтобы избежать возможных проблем с производительностью.

При установке агента на своем сервере (например, на Windows или в Hyper-V) *отключите файловый мониторинг*. В противном случае агент будет отслеживать все многочисленные события на сервере.

Если у вас более сотни агентов, перенесите:

- iBatyr Monitor на отдельный диск;
- базы данных на отдельный SSD-диск;
- файловое хранилище на отдельный диск, предпочтительно SSD.

3.7.30 Ошибка прав доступа к сертификату

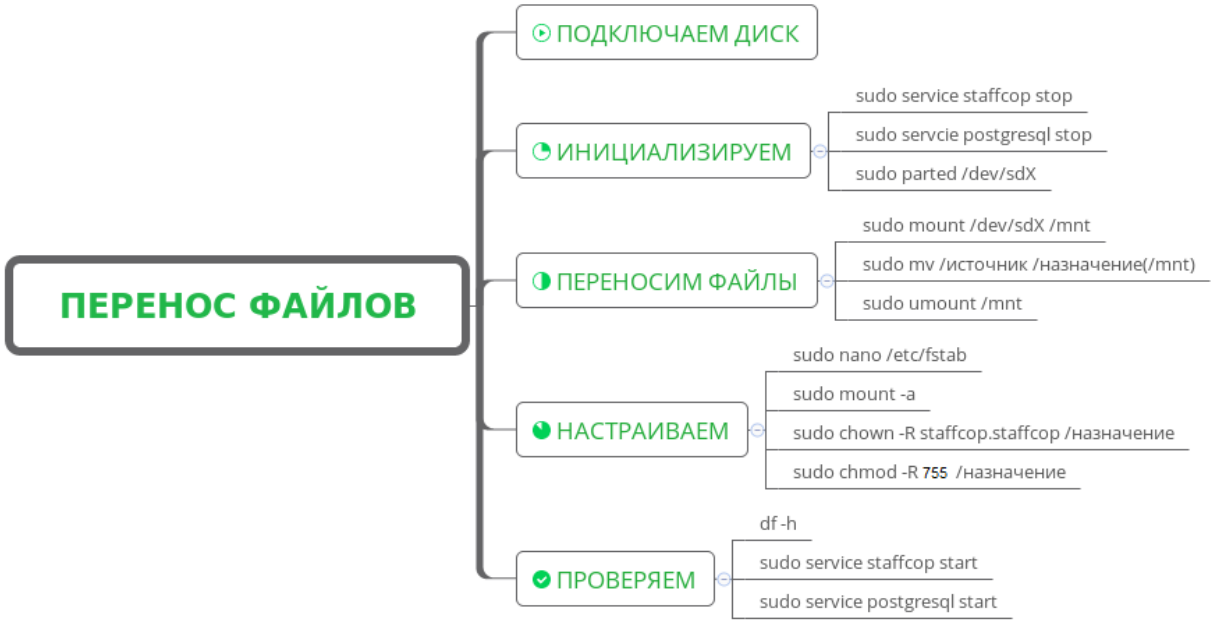
Если вы обнаружили где-то записи про ошибки доступа к сертификатам, то выполните эти действия:

```
sudo chown postgres /etc/ssl/private/ssl-cert-snakeoil.key
sudo chown postgres /etc/ssl/certs/ssl-cert-snakeoil.pem
sudo chmod 600 /etc/ssl/private/ssl-cert-snakeoil.key
sudo chmod 600 /etc/ssl/certs/ssl-cert-snakeoil.pem
```

Также нужно проверить это при ошибке доступа к 5432 сокету.

3.7.31 Перенос файлов и скриншотов

iBatyr Monitor отдельно хранит метаданные (базы данных) и перехваченные файлы. При больших объемах данных это позволяет хранить базы данных и файлы на разных жестких дисках. Например, базы данных держать на быстрых SSD-накопителях, а файлы - на отдельном объемном raid-массиве или сетевом хранилище.



Примечание: Ниже приведена инструкция для работы с диском **sdb1**. Имя вашего жёсткого диска может отличаться.

raid-массивы и NAS монтируются аналогично.

Чтобы перенести файлы и скриншоты:

1. Остановите сервисы

```
sudo service ibatyr stop
sudo service postgresql stop
sudo service nginx stop
```

2. Смонтируйте новый диск

Если ваш диск еще не отформатирован, то *воспользуйтесь инструкцией по созданию и добавлению разделов*.

```
sudo mount /dev/sdb1 /mnt
```

Внимание: Нельзя использовать одну и ту же точку монтирования для файлов и баз данных. База данных не должна храниться в **/var/lib/ibatyr/upload/**.

3. Переместите содержимое папки

Переместите **/var/lib/ibatyr/upload** на новый диск.

```
sudo mv /var/lib/ibatyr/upload/* /mnt
```

4. Размонтируйте диск

```
sudo umount /mnt
```

5. Откройте файл **/etc/fstab**

```
sudo nano -u /etc/fstab
```

6. Добавьте новый диск - новая строка в открытом файле **/etc/fstab**:

```
/dev/sdb1 /var/lib/ibatyr/upload ext4  rw,noatime  0 2
```

Подробнее о монтировании дисков можно *прочитать в статье*.

Проверьте корректность монтирования:

```
sudo mount -a
```

7. Выдайте права доступа:

```
sudo chown -R ibatyr:ibatyr /var/lib/ibatyr/upload
sudo chmod -R 755 /var/lib/ibatyr/upload
```

7. Запустите сервисы

```
sudo service postgresql start
sudo service ibatyr start
sudo service nginx start
```

3.7.32 Увеличиваем коннекты к базе данных

1. Открываем файл конфигурации командой

```
sudo nano /etc/postgresql/11/main/postgresql.conf
```

2. Нажимаем **Ctrl+W**, вводим **max_conn** нажимаем Enter
3. Меняем значение со **100** на значение **300**
4. нажимаем **Ctrl+O** для сохранения, потом **Ctrl+X** для выхода.
5. Перезапускаем Postgresql командой:

```
sudo service postgresql restart
```

3.7.33 Узнаём IP

Для того чтобы узнать ваш IP, есть несколько команд.

```
ifconfig -a
```

выдаст вам все используемые сетевые интерфейсы.

```
ifconfig | grep inet | grep -v inet6 | grep -v 127.0.0.1 | cut -d: -f2 | awk '{printf $1
↪"\n"}'
```

уменьшит вывод команды, сделав его более информативным.

Если вам попалась система без встроенной команды ifconfig (да, такое тоже возможно)

то попробуйте:

```
ip links list
```

для вывода интерфейсов и

```
ip addr show | grep inet
```

для вывода IP.

3.7.34 Фавикон

Если вы хотите сменить значок во вкладке, замените этот файл на свой -

```
/usr/share/ibatyr/static/favicon.ico
```

3.7.35 Пароль от веб-консоли

При первом входе в веб-консоль, программа попросит задать пароль для администратора.

Надёжность пароля

Для проверки силы пароля iBatyr Monitor использует open-scource утилиту **zxcvbn**.

Основные преимущества **zxcvbn** по сравнению со стандартными политиками, следящими за силой пароля:

- **безопасность**: в отличие от стандартных политик **zxcvbn** не пропускает слабые пароли, удовлетворяющие стандартным критериям (P@ssword1);
- **гибкость**: **zxcvbn** проверяет наличие необычных слов в пароле, расстояние между клавишами и углы поворота при наборе пароля, что позволяет использовать различные стили при создании паролей;
- **удобство**: интерфейс взаимодействия с **zxcvbn** прост и не содержит ничего лишнего.

Уровни надёжности пароля

При задании пароля, проверяется уровень его надёжности. Поле ввода нового пароля подсвечивается соответствующим цветом:

tabularytabulary

Уровень	Описание	Цвет
0	Очень слабый	Красный
1	Слабый	Жёлтый
2	Средний	Оливковый
3	Хороший	Зелёный
4	Отличный	Зелёный

Задать минимально допустимый уровень надёжности можно в файле **/usr/share/ibatyr/settings.py** в строке **MIN_PASSWORD_SCORE** =. По умолчанию задан уровень **2**.

Защита от подбора пароля к веб-консоли

Для активации защиты используйте команду

```
ibatyr enable fail2ban
```

После выполнения команды запустится диалог, в котором нужно будет указать:

- число ошибочных вводов пароля;
- время, за которое отслеживаются ошибочные вводы;
- время, на которое блокируется IP-адрес, с которого производились ошибочные вводы.

Чтобы отключить защиту используйте команду

```
ibatyr disable fail2ban
```

Восстановление пароля

Для восстановления или изменения пароля от веб-интерфейса введите в консоли команду

```
sudo ibatyr passwd NEWPASSWD
```

где NEWPASSWD - новый пароль суперпользователя веб-консоли **admin**.

3.8 iBatyr Monitor API

Данный документ описывает структуры данных и программный интерфейс приложения iBatyr Monitor .

Предупреждение: REST API доступно, начиная с версии iBatyr Monitor 4.4.

Содержание:

3.8.1 Модель данных

Система iBatyr Monitor построена на базе технологии OLAP.

OLAP-структура, созданная из рабочих данных, называется OLAP-куб. Куб создаётся из соединения таблиц с применением схемы звезды.

В центре схемы звезды находится таблица фактов, которая содержит ключевые факты, по которым делаются запросы.

Множественные таблицы с измерениями присоединены к таблице фактов. Эти таблицы показывают, как могут анализироваться агрегированные реляционные данные.

Таблица фактов

Основной таблицей является таблица фактов **agent_event**, содержащая внешние ключи на таблицы измерений

tabularytabulary

Колонка	Тип
id	integer
event_type_id	integer
agent_id	integer
account_id	integer
time_id	integer
application_id	integer
web_data_id	integer
net_data_id	integer
file_operation_id	integer
file_path_id	integer
attached_file_id	integer
dialog_id	integer
app_installation_id	integer
device_id	integer
feedback_id	integer
call_duration	integer
activity_time	bigint
idle_time	bigint
time_registered	timestamp with time zone
local_time	timestamp with time zone
window_title	text
text_data	text
parent_id	integer
children_count	integer
filters_data	text

Измерение Агент

Измерение **Агент** содержится в таблице **agent_agent**.

Колонка	Назначение
computer_name	Компьютер
last_report	Статус
last_ip	IP адрес
agent_version	Версия агента
os	Версия OS
id	ID
guid	HWID
label	Группа

Измерение Пользователь

Измерение **Пользователь** содержится в таблице **agent_account**.

Колонка	Назначение
id	ID
guid	SID
user_name	Пользователь
full_name	Полное имя
office	Отдел
company	Организация
post	Должность
phone	Телефон
mail	Почта
comment	Комментарий
user_domain	Домен
last_report_time	Последний выход на связь
last_activity_time	Последняя активность пользователя

Измерение Приложение

Измерение **Приложение** содержится в таблице **agent_application**.

Колонка	Назначение
app_name	Название
exe_path	Полный путь
app_description	Описание
window_title	Заголовок окна

Измерение Сайт

Измерение **Сайт** содержится в таблице **agent_web**.

Колонка	Назначение
site	Сайт
domain	Домен
url	URL
protocol	Протокол
mime	Тип контента

Измерение Сетевая активность

Измерение **Сетевая активность** содержится в таблице **agent_networkconnection**.

Колонка	Назначение
remote_address	IP адрес
remote_port	Сетевой порт

Измерение Файл

Измерение **Файл** содержится в таблице **agent_attachedfile**.

Колонка	Назначение
file_name	Имя файла
file_ext	Расширение
file_path	Путь
mime	Тип контента
data	Url
drive_type	Тип диска
sha1	Хеш файла
guid	GUID
id	Ид
extracted	Статус распаковки
file_operation	Операция

Измерение Устройство

Измерение **Устройство** содержится в таблице **agent_device**.

Колонка	Назначение
manufacturer	Тип устройства
description	Устройство
hwid	ID устройства
drive_type	Тип диска
device_class	Класс устройства

Измерение Переписка

Измерение **Переписка** содержится в таблице **agent_dialog**.

Колонка	Назначение
sender	Отправитель
contact	Получатель
recipients	Все получатели
sender_domain	Домен отправителя
domain	Домен получателя
direction	Направление
dialog_type	Канал общения
message_format	Формат сообщения
members	Чаты

Измерение Дата

Измерение **Дата** содержится в таблице **agent_time**.

Колонка	Назначение
year	Год
month	Месяц
day	День
hour	Час
quarter	Четверть часа
minute	Минута
weekday	День недели
time_zone	Часовой пояс

Измерение Инсталляции

Измерение **Инсталляции** содержится в таблице **agent_appinstallation**.

Колонка	Назначение
install_event	Операция
product_name	Продукт
publisher	Поставщик
version	Версия

Измерение Сработавшие политики

Измерение **Сработавшие политики** содержится в таблице **analytics_filter**.

Колонка	Назначение
name	Название
category	Категория
syscat	Сист. категория

3.8.2 Database API

iBatyr Monitor использует реляционную базу данных PostgreSQL.

Прямое подключение к базе данных – наиболее эффективный способ извлечения данных.

Настройка удаленного подключения

Шаг 1. Разрешите подключение к PostgreSQL с внешних IP

1. Найдите файл *postgresql.conf* в папке */etc/postgresql/[ВЕРСИЯ]/main/* и откройте его для редактирования.
2. Измените параметр:

```
listen_addresses = 'localhost,00.00.00.000'             # what IP address(es)␣
↪to listen on
```

   Убедитесь, что перед этой строкой нет символа комментария #.

   Замените 00.00.00.00 на имя вашего сервера, на котором установлена база данных.

3. В этой же директории найдите файл *pg_hba.conf* и добавьте строку:

```
host    ibatyr        ibatyr        00.00.00.00/32          md5
```

   где:

4. Перезапустите PostgreSQL командой:

```
service postgresql restart
```

Шаг 2. Получите пароль для подключения к БД

Откройте файл */etc/ibatyr/config* и найдите пароль:

```
DATABASES = {
    'default': {
         'NAME': 'ibatyr',
        'USER': 'ibatyr',
         'PASSWORD': 'password',
         'HOST': '',
         'PORT': '',
     }
 }
```

Шаг 3. Подключитесь с другого ПК

Используйте клиент для проверки подключения, например pgAdmin.

1. В pgAdmin нажмите **Новое подключение** и заполните поля:

   Остальные поля стоят по умолчанию.

2. Нажимите **OK**. Если всё заработало – удалённое подключение к PostgreSQL настроено.

Выгрузка данных

Для выгрузки всех данных в денормализованном виде (факты и измерения) используйте SQL-запрос:

```
SELECT
DATE("local_time"),
COALESCE(agent_event.id, 0) AS "agent_event.id",
COALESCE(agent_event.activity_time, 0) AS "agent_event.activity_time",
COALESCE(agent_event.idle_time, 0) AS "agent_event.idle_time",
COALESCE(agent_event.call_duration, 0) AS "agent_event.call_duration",
replace(replace(array(select filter_id from analytics_filter_events where event_id=agent_
↪event.id)::text, '{', '['), '}', ']') AS "agent_event.filters",
COALESCE(agent_time.id, 0) AS "agent_time.id",
COALESCE(agent_time.year, 0) AS "agent_time.year",
COALESCE(agent_time.month, 0) AS "agent_time.month",
COALESCE(agent_time.day, 0) AS "agent_time.day",
COALESCE(agent_time.hour, 0) AS "agent_time.hour",
COALESCE(agent_time.quarter, 0) AS "agent_time.quarter",
COALESCE(agent_time.minute, 0) AS "agent_time.minute",
COALESCE(agent_time.weekday, 0) AS "agent_time.weekday",
COALESCE(agent_time.time_zone::text, '') AS "agent_time.time_zone",
COALESCE(agent_eventtype.id, 0) AS "agent_eventtype.id",
COALESCE(agent_eventtype.description_ru::text, '') AS "agent_eventtype.description_ru",
COALESCE(agent_eventtype.description_en::text, '') AS "agent_eventtype.description_en",
COALESCE(agent_eventtype.name::text, '') AS "agent_eventtype.name",
COALESCE(agent_agent.id, 0) AS "agent_agent.id",
COALESCE(agent_agent.guid::text, '') AS "agent_agent.guid",
COALESCE(agent_agent.computer_name::text, '') AS "agent_agent.computer_name",
COALESCE(agent_agent.last_ip::text, '') AS "agent_agent.last_ip",
COALESCE(agent_agent.agent_version::text, '') AS "agent_agent.agent_version",
COALESCE(agent_agent.os::text, '') AS "agent_agent.os",
COALESCE(agent_agent.last_report_time::text, '') AS "agent_agent.last_report_time",
COALESCE(agent_agent.last_activity_time::text, '') AS "agent_agent.last_activity_time",
COALESCE(agent_agent.label::text, '') AS "agent_agent.label",
COALESCE(agent_agent.last_report::text, '') AS "agent_agent.last_report",
COALESCE(agent_account.id, 0) AS "agent_account.id",
COALESCE(agent_account.guid::text, '') AS "agent_account.guid",
COALESCE(agent_account.user_name::text, '') AS "agent_account.user_name",
COALESCE(agent_account.last_report_time::text, '') AS "agent_account.last_report_time",
COALESCE(agent_account.last_activity_time::text, '') AS "agent_account.last_activity_time
↪",
COALESCE(agent_account.full_name::text, '') AS "agent_account.full_name",
COALESCE(agent_account.office::text, '') AS "agent_account.office",
COALESCE(agent_account.company::text, '') AS "agent_account.company",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
COALESCE(agent_account.post::text, '') AS "agent_account.post",
COALESCE(agent_account.phone::text, '') AS "agent_account.phone",
COALESCE(agent_account.mail::text, '') AS "agent_account.mail",
COALESCE(agent_account.comment::text, '') AS "agent_account.comment",
COALESCE(agent_account.user_domain::text, '') AS "agent_account.user_domain",
COALESCE(agent_application.id, 0) AS "agent_application.id",
COALESCE(agent_application.app_name::text, '') AS "agent_application.app_name",
COALESCE(agent_application.exe_path::text, '') AS "agent_application.exe_path",
COALESCE(agent_application.app_description::text, '') AS "agent_application.app_
↪description",
COALESCE(agent_event.window_title::text, '') AS "agent_event.window_title",
COALESCE(agent_application.icon::text, '') AS "agent_application.icon",
COALESCE(agent_web.site::text, '') AS "agent_web.site",
COALESCE(agent_web.domain::text, '') AS "agent_web.domain",
COALESCE(agent_web.url::text, '') AS "agent_web.url",
COALESCE(agent_web.id, 0) AS "agent_web.id",
COALESCE(agent_web.protocol::text, '') AS "agent_web.protocol",
COALESCE(agent_web.mime::text, '') AS "agent_web.mime",
COALESCE(agent_networkconnection.id, 0) AS "agent_networkconnection.id",
COALESCE(agent_networkconnection.remote_address::text, '') AS "agent_networkconnection.
↪remote_address",
COALESCE(agent_networkconnection.remote_port::text, '') AS "agent_networkconnection.
↪remote_port",
COALESCE(agent_filepath.name::text, '') AS "agent_filepath.name",
COALESCE(agent_filepath.ext::text, '') AS "agent_filepath.ext",
COALESCE(agent_filepath.path::text, '') AS "agent_filepath.path",
COALESCE(agent_attachedfile.mime::text, '') AS "agent_attachedfile.mime",
COALESCE(agent_attachedfile.data::text, '') AS "agent_attachedfile.data",
COALESCE(agent_device.drive_type::text, '') AS "agent_device.drive_type",
COALESCE(agent_attachedfile.sha1::text, '') AS "agent_attachedfile.sha1",
COALESCE(agent_attachedfile.guid::text, '') AS "agent_attachedfile.guid",
COALESCE(agent_attachedfile.id, 0) AS "agent_attachedfile.id",
COALESCE(agent_attachedfile.extracted::text, '') AS "agent_attachedfile.extracted",
COALESCE(agent_fileoperationtype.description_en::text, '') AS "agent_fileoperationtype.
↪description_en",
COALESCE(agent_fileoperationtype.description_ru::text, '') AS "agent_fileoperationtype.
↪description_ru",
COALESCE(agent_device.manufacturer::text, '') AS "agent_device.manufacturer",
COALESCE(agent_device.description::text, '') AS "agent_device.description",
COALESCE(agent_device.hwid::text, '') AS "agent_device.hwid",
COALESCE(agent_device.device_class::text, '') AS "agent_device.device_class",
COALESCE(agent_dialog.sender::text, '') AS "agent_dialog.sender",
COALESCE(agent_dialog.recipients::text, '') AS "agent_dialog.recipients",
COALESCE(agent_dialog.sender_domain::text, '') AS "agent_dialog.sender_domain",
COALESCE(agent_dialog.direction::text, '') AS "agent_dialog.direction",
COALESCE(agent_dialog.dialog_type::text, '') AS "agent_dialog.dialog_type",
COALESCE(agent_dialog.message_format::text, '') AS "agent_dialog.message_format",
COALESCE(agent_dialog.members::text, '') AS "agent_dialog.members",
COALESCE(agent_appinstallation.install_event::text, '') AS "agent_appinstallation.
↪install_event",
COALESCE(agent_appinstallation.product_name::text, '') AS "agent_appinstallation.product_
↪name",
```

(continues on next page)

(продолжение с предыдущей страницы)

```
COALESCE(agent_appinstallation.publisher::text, '') AS "agent_appinstallation.publisher",
COALESCE(agent_appinstallation.version::text, '') AS "agent_appinstallation.version",
COALESCE(agent_event.text_data::text, '') AS "agent_event.text_data",
COALESCE(agent_feedbacktype.id, 0) AS "agent_feedbacktype.id",
COALESCE(agent_feedbacktype.description_ru::text, '') AS "agent_feedbacktype.description_
↪ru",
COALESCE(agent_feedbacktype.description_en::text, '') AS "agent_feedbacktype.description_
↪en",
COALESCE(agent_feedbacktype.name::text, '') AS "agent_feedbacktype.name",
COALESCE(agent_event.logon_event::text, '') AS "agent_event.logon_event",
DATE_TRUNC('second', agent_event.local_time::TIMESTAMP WITHOUT TIME ZONE) AS "agent_
↪event.local_time",
COALESCE(agent_event.time_registered::text, '') AS "agent_event.time_registered",
COALESCE(agent_event.parent_id::text, '') AS "agent_event.parent_id",
COALESCE(agent_event.children_count::text, '') AS "agent_event.children_count"

FROM agent_event
LEFT JOIN agent_feedbacktype ON agent_feedbacktype.id = agent_event.feedback_id
LEFT JOIN agent_dialog ON agent_dialog.id = agent_event.dialog_id
LEFT JOIN agent_time ON agent_time.id = agent_event.time_id
LEFT JOIN agent_application ON agent_application.id = agent_event.application_id
LEFT JOIN agent_filepath ON agent_filepath.id = agent_event.file_path_id
LEFT JOIN agent_eventtype ON agent_eventtype.id = agent_event.event_type_id
LEFT JOIN agent_agent ON agent_agent.id = agent_event.agent_id
LEFT JOIN agent_web ON agent_web.id = agent_event.web_data_id
LEFT JOIN agent_fileoperationtype ON agent_fileoperationtype.id = agent_event.file_
↪operation_id
LEFT JOIN agent_attachedfile ON agent_attachedfile.id = agent_event.attached_file_id
LEFT JOIN agent_appinstallation ON agent_appinstallation.id = agent_event.app_
↪installation_id
LEFT JOIN agent_networkconnection ON agent_networkconnection.id = agent_event.net_data_id
LEFT JOIN agent_device ON agent_device.id = agent_event.device_id
LEFT JOIN agent_account ON agent_account.id = agent_event.account_id
```

3.8.3 REST API

Аутентификация

Для возможности выполнять запросы к REST API, в меню **Админ -> Параметры сервера** необходимо включить опцию **Доступ к API разрешен**.

Аутентификация запросов к API происходит через передачу ключа, указанного в опции **Ключ API**. Вы можете указать собственное значение этого параметра.

Ключ API передается в **GET** параметре запроса **secret**, например:

```
https://[HOST]/analytics/model/?secret=password
```

Модель куба

Обработчик: /**analytics**/**model**/

Пример запроса:

```
https://[HOST]/analytics/model/?secret=3a7e...418418e
```

Возвращает модель данных OLAP куба. С описанием формата можно ознакомиться здесь

Модель куба описана в разделе *Модель данных*

Фильтры и политики

Возвращает все сохраненные фильтры и политики в виде иерархии объектов.

Обработчик: /**analytics**/**filter**/**list**/

Пример запроса:

```
https://[HOST]/analytics/filter/list/?secret=3a7e...418418e
```

Пример возвращаемого значения:

```
[
  {
        "id": 1,
        "content_type": "filter",
        "name": "Название фильтра",
        "facts_count": 0,
        "measure": "record_count",
        "dimension": "agent_time@ymdh:hour",
        "category": "neutral",
        "listType": "table",
        "do_scan": false,
        "reporting_schedule_type": "",
        "drilldown": [ "agent_agent@computer_name:computer_name", ... ],
        "notify": false,
        "emails": "",
        "orderDim": "agent_account@office:office",
        "url": "/analytics/report/aggregate/index/",
        "report_if_filter_data_exists": false,
        "tab": "filter",
        "mode": "explore",
        "order": "record_count",
        "orderDir": "desc",
        "filters": [
          {
                "predicates": [],
                "dimension": "agent_account@office:office",
                "value": "",
                "label": ""
          },
          ...
        ],
```

(continues on next page)

(продолжение с предыдущей страницы)

```
        "children": [...]
  },
...
]
```

Параметры запросов к OLAP кубу

Обработчики указанные ниже могут принимать параметры фильтрации. Все параметры являются необязательными.

Название	Описание
backend	Предпочтительный поставщик данных (postgresql, clickhouse, hybrid)
limit	Размер страницы (количество возвращаемых строк)
page	Номер страницы
time_from	Начало периода времени
time_to	Окончание периода времени
order	Атрибут для сортировки
dir	Порядок сортировки (asc, desc)
dim	Измерения для фильтрации. Данный параметр может присутствовать несколько раз.
filter	Значение измерений для фильтрации. Порядок и количество должно соответствовать параметрам dim

Факты

Обработчик: /**analytics**/**facts**/**agent_event**/

Пример запроса:

```
https://[HOST]/analytics/facts/agent_event/?backend=postgresql&dim=agent_
↪eventtype@default:agent_eventtype&dir=desc&filter=1&limit=50&order=local_time&page=0&
↪time_from=2018-09-04T00:00:00.000&time_to=2018-09-04T23:59:59.999&secret=3a7e...418418e
```

Пример возвращаемого значения:

```
{
  "object_list": [
        {
          "agent_device.description": null,
          "analytics_filter.id": null,
          "agent_attachedfile.file_ext": null,
          "agent_dialog.sender": null,
          "agent_agent.last_report": "Активен вчера",
          "agent_agent.os": "6.2.9200",
          "agent_eventtype.name": "Screenshot",
          "agent_web.url": null,
          "time_registered": "2018-09-02T12:00:09.286822+00:00",
          "agent_account.guid": "S-1-5-21-1174184718-2834874228-2720016071-1001",
          "agent_web.id": null,
          "agent_feedbacktype.description": null,
```

(continues on next page)

(продолжение с предыдущей страницы)


```
          "agent_agent.last_activity_time": "2018-09-02T11:59:04.523638+00:00",
          "parent_id": null,
          "agent_attachedfile.mime": "image/jpeg",
          "agent_appinstallation.publisher": null,
          "agent_networkconnection.id": null,
          "agent_account.office": "",
          "agent_networkconnection.remote_address": null,
          "agent_attachedfile.id": 1755,
          "agent_attachedfile.extracted": false,
          "agent_appinstallation.version": null,
          "agent_agent.label": "",
          "agent_device.drive_type": null,
          "agent_web.domain": null,
          "agent_application.id": 271,
          "agent_time.weekday": 6,
          "agent_web.protocol": null,
          "agent_web.site": null,
          "agent_account.id": 322,
          "agent_agent.guid": "HWIDVB94bea50c-4604cbd0",
          "agent_web.mime": null,
          "agent_attachedfile.file_name": null,
          "agent_dialog.dialog_type": null,
          "agent_account.user_domain": "WORKGROUP",
          "agent_time.day": 2,
          "agent_time.id": 564,
          "text_data": "",
          "agent_application.app_icon_id": 1723,
          "agent_account.last_report_time": "2018-09-02T12:00:09.255085+00:00",
          "agent_account.comment": "",
          "agent_application.window_title": "{E:\\opt\\tor-browser_en-US\\Browser\\
↪Downloads\\MS Office 2013 Portable (2017) 7z SFX} - Far 3.0.5225 x64",
          "agent_agent.last_report_time": "2018-09-02T12:00:09.255085+00:00",
          "agent_device.hwid": null,
          "agent_account.mail": "",
          "agent_account.company": "",
          "agent_eventtype.description": "Снимок экрана",
          "agent_eventtype.id": 4,
          "agent_dialog.direction": null,
          "agent_attachedfile.file_exist": true,
          "agent_attachedfile.file_path": null,
          "agent_time.month": 9,
          "agent_account.user_name": "ermakus",
          "agent_time.year": 2018,
          "agent_agent.last_ip": "192.168.0.111",
          "window_title": "{E:\\opt\\tor-browser_en-US\\Browser\\Downloads\\MS Office␣
↪2013 Portable (2017) 7z SFX} - Far 3.0.5225 x64",
          "%(140392777775632 id)s": 19354,
          "agent_appinstallation.product_name": null,
          "analytics_filter.syscat": null,
          "agent_attachedfile.guid": "0fec5042-9665-edbd-d490-657eb442d401",
          "agent_time.hour": 15,
          "agent_feedbacktype.id": null,
```


(continues on next page)

(продолжение с предыдущей страницы)


```
          "children_count": 0,
          "agent_dialog.contact": null,
          "agent_attachedfile.data": "filedata/by_date/2018_09_02/
↪ac5df7124c4bad5d0e07a277ad4563af0abca928.jpe",
          "agent_account.post": "",
          "agent_feedbacktype.name": null,
          "agent_dialog.recipients": null,
          "agent_networkconnection.remote_port": null,
          "agent_dialog.domain": null,
          "agent_dialog.message_format": null,
          "agent_device.manufacturer": null,
          "agent_agent.agent_version": "2465",
          "agent_time.minute": 0,
          "idle_time": 0,
          "agent_agent.computer_name": "DESKTOP-E308NV5",
          "agent_application.app_description": "File and archive manager",
          "agent_account.last_activity_time": "2018-09-02T11:59:04.523638+00:00",
          "id": 19354,
          "agent_account.full_name": "",
          "agent_agent.id": 2526,
          "activity_time": 0,
          "agent_device.device_class": null,
          "agent_time.quarter": 60,
          "filters_data": null,
          "agent_account.phone": "",
          "agent_dialog.sender_domain": null,
          "agent_attachedfile.sha1": "ac5df7124c4bad5d0e07a277ad4563af0abca928",
          "agent_attachedfile.file_operation": null,
          "analytics_filter.name": null,
          "logon_event": "",
          "agent_time.time_zone": "UTC+3",
          "agent_dialog.members": null,
          "call_duration": null,
          "analytics_filter.category": null,
          "agent_application.exe_path": "C:\\PROGRAM FILES\\FAR MANAGER\\FAR.EXE",
          "agent_application.app_name": "far.exe",
          "local_time": "2018-09-02T19:00:08+07:00",
          "agent_attachedfile.drive_type": null,
          "agent_appinstallation.install_event": null
        },
        ...
]}
```

Агрегация

Обработчик: **/analytics/aggregate/agent_event/**

Таблица 2: Параметры

Название	Описание
drill	Измерения для drilldown, может присутствовать несколько раз

Пример запроса:

```
https://[HOST]/analytics/aggregate/agent_event/?backend=postgresql&drill=agent_
↪agent@computer_name:computer_name&time_from=2018-09-04T00:00:00.000&time_to=2018-09-
↪04T23:59:59.999&secret=3a7e...418418e
```

Пример возвращаемого значения:


```
{
  "cells": [
        {
          "record_count": 292,
          "call_duration_sum": 0,
          "agent_agent.computer_name": "DESKTOP-E308NV5",
          "agent_agent.last_activity_time": "2018-09-02T11:59:04.523638+00:00",
          "activity_time_sum": 27158538723,
          "agent_agent.guid": "HWIDVB94bea50c-4604cbd0",
          "agent_agent.id": 2526,
          "local_time_max": "2018-09-02T12:00:08+00:00",
          "idle_time_sum": 16101090000,
          "local_time_min": "2018-09-02T10:43:52+00:00",
          "agent_agent.last_report_time": "2018-09-02T12:00:09.255085+00:00"
        }
  ],
  "cell": [
        {
          "hierarchy": "computer_name",
          "path": [
                "2526",
                "HWIDVB94bea50c-4604cbd0",
                "DESKTOP-E308NV5"
          ],
          "type": "point",
          "dimension": "agent_agent",
          "level_depth": 3
        },
        {
          "from": [
                "2018-08-29T00:00:00+07:00"
          ],
          "level_depth": 1,
          "hierarchy": null,
          "to": [
                "2018-09-04T23:59:59.999000+07:00"
```


(continues on next page)

(продолжение с предыдущей страницы)

```
          ],
          "type": "range",
          "dimension": "local_time"
        }
  ],
  "levels": {
        "agent_agent": [
          "id",
          "guid",
          "computer_name"
        ]
  },
  "remainder": {}
}
```

Можно сразу получать агрегированные данные, например для УРВ. Использует куб analytics_session, факты в кубе agent_event:

Обработчик: /**analytics**/**aggregate**/**analytics_session**/

Таблица 3: Параметры

Название	Описание
drill	Измерения для drilldown, может присутствовать несколько раз

Пример запроса:

```
http://[HOST]/analytics/aggregate/analytics_session/?drill=agent_time@ymd:day,
↪drill=agent_account@full_name:full_name
```

Значения измерений

Обработчик: /**analytics**/**values**/**agent_event**/

Таблица 4: Параметры

Название	Описание
drill	Название измерения

Пример запроса:

```
https://[HOST]/analytics/values/agent_event/?backend=postgresql&drill=agent_
↪agent@computer_name:computer_name&time_from=2018-09-04T00:00:00.000&time_to=2018-09-
↪04T23:59:59.999&secret=3a7e...418418e
```

Пример возвращаемого значения:

```
{
  "cells": [
        {
```

(continues on next page)

(продолжение с предыдущей страницы)

```
          "agent_agent.last_report_time": "2018-09-02T12:00:09.255085+00:00",
          "agent_agent.guid": "HWIDVB94bea50c-4604cbd0",
          "agent_agent.id": 2526,
          "agent_agent.computer_name": "DESKTOP-E308NV5",
          "agent_agent.last_activity_time": "2018-09-02T11:59:04.523638+00:00"
        },
        ...
  ]
}
```

3.8.4 Интеграция со сторонними сервисами

iBatyr Monitor предоставляет интерфейс для загрузки в систему данных от сторонних приложений.

Добавлять события из сторонних приложений в систему можно при помощи API. Для этого включите опцию *Доступ к API разрешен*.

Для передачи событий *рекомендуем использовать HTTPS*.

Список параметров (POST или GET, рекомендуем POST):

tabularytabulary

Параметр	
secret	
local_time	
event_type_id	
computer_name	
user_name	
exe_path	
window_title	
text_data	
sender	
recipients	
file1.txt file2.txt	

Возвращаемые значения:

- ID события (код 200);
- неверный ключ или API отключено (код 403);
- трасса ошибки (код 500)

Пример использования

curl

-F «secret=vi123p8rzgqwerdjioea0987kikgj9p2d4casdf804fqmaucq1y1neeg3n4hleg» -F «local_time=2023-11-14 14:00:00.00Z» -F «event_type_id=8» -F «computer_name=user1-pc» -F «user_name=user 1» -F «exe_path=c:test/app.exe» -F «window_title=Заголовок или название чата» -F «text_data=Текст подмножество HTML» -F «sender=test» -F «recipients=test2,test3» -F «file1.sh=@api/test_api.sh» -F «file2.sh=@api/test_api.sh» http://localhost/api/event/

Глава 4

Руководство пользователя

4.1 Конфигурация компьютеров

Для настройки конфигураций:

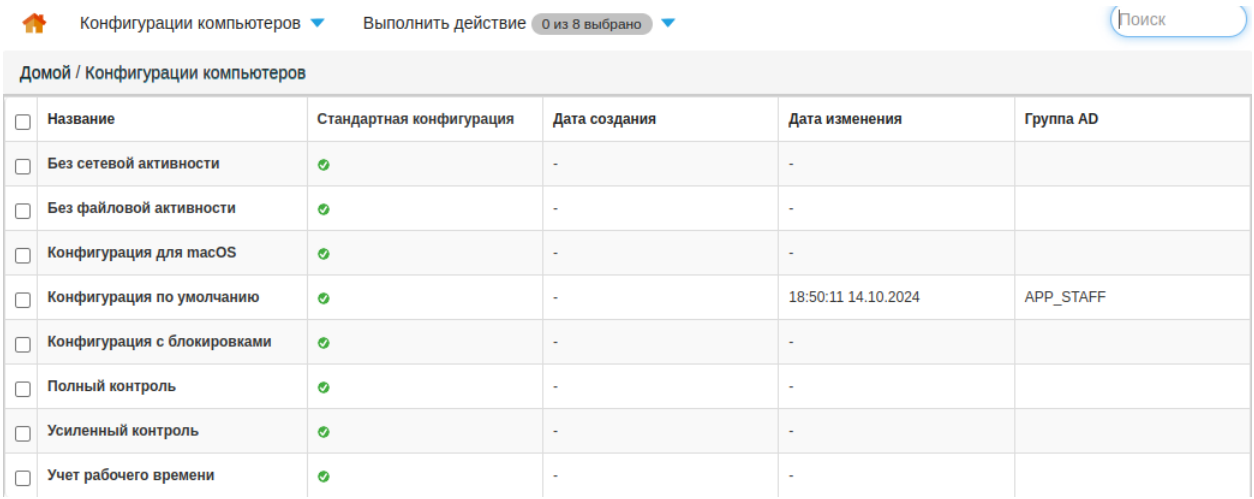
1. Перейдите в **Панель управления** → **Конфигурации компьютеров**.
2. Выберите конфигурацию.
3. Выберите в списке модуль и переключите его в положение «включено».

Конфигурация выполняет несколько функций:

- включение и отключение модулей мониторинга;
- настройка агентов;
- добавление **Правил мониторинга** — гибких настроек перехвата и блокировки, благодаря которым возможна тонкая настройка агентов для оптимального решения задач.

При первом подключении к агентам применяется **Конфигурация по умолчанию**, но каждому агенту можно присовить уникальную конфигурацию.

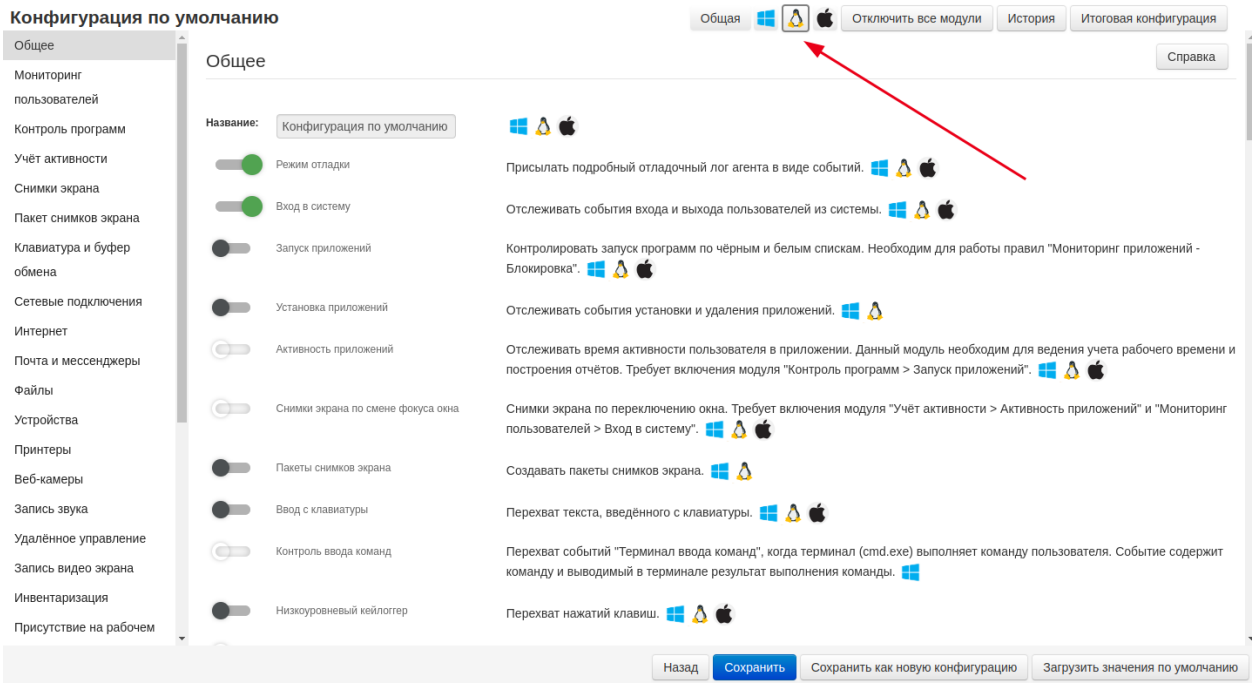
Для редактирования конфигурации нажмите на соответствующее название конфигурации.



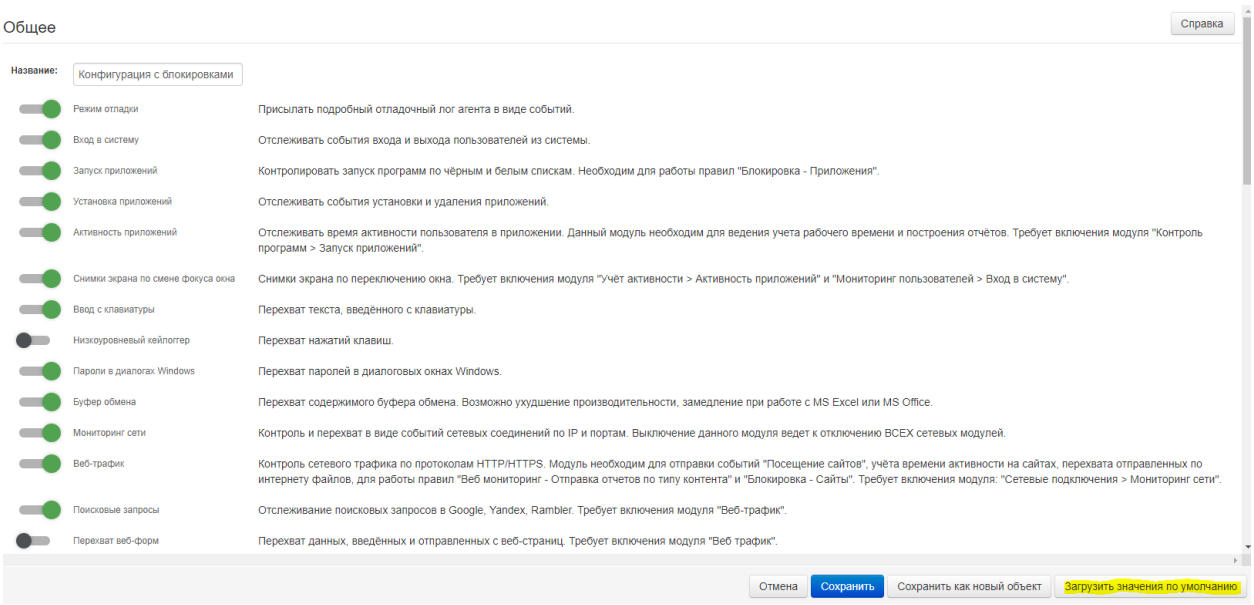
Название	Стандартная конфигурация	Дата создания	Дата изменения	Группа AD
Без сетевой активности	✓	-	-	
Без файловой активности	✓	-	-	
Конфигурация для macOS	✓	-	-	
Конфигурация по умолчанию	✓	-	18:50:11 14.10.2024	APP_STAFF
Конфигурация с блокировками	✓	-	-	
Полный контроль	✓	-	-	
Усиленный контроль	✓	-	-	
Учет рабочего времени	✓	-	-	

На странице конфигурации представлен список доступных модулей для всех операционных систем. В разных операционных системах доступны разные модули.

Чтобы отфильтровать модули по операционной системе, выберите значок соответствующей ОС в верхнем правом углу. У активных модулей будет отображаться переключатель, позволяющий их включать или отключать.



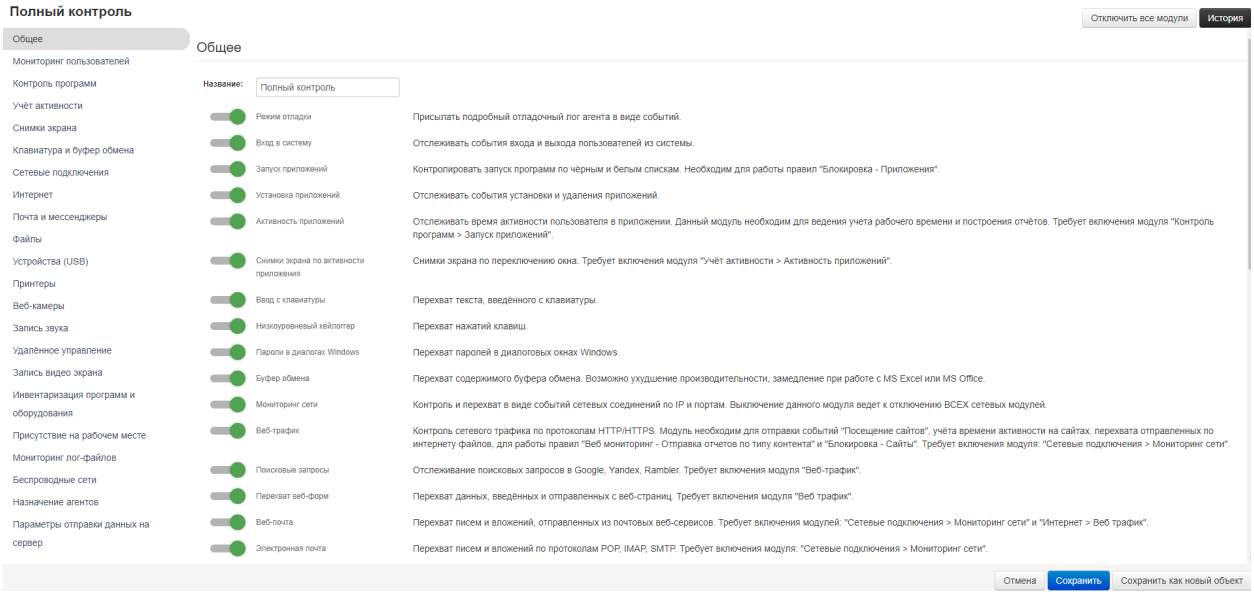
Примечание: В предустановленных политиках конфигурации компьютеров, таких как **Полный контроль**, **Усиленный контроль**, **Учет рабочего времени** и прочие, предусмотрен сброс до первоначальных настроек. Для этого нужно нажать кнопку **Загрузить значения по умолчанию**.



Предупреждение: Внимание! При заполнении правил мониторинга заполняйте только один тип правил: **Запретить** или **Разрешить**. Если заполнены оба типа правил, будет учитываться приоритет правил **Запретить**, а правила **Разрешить** применяться не будут.

Основные модули:

4.1.1 Общее

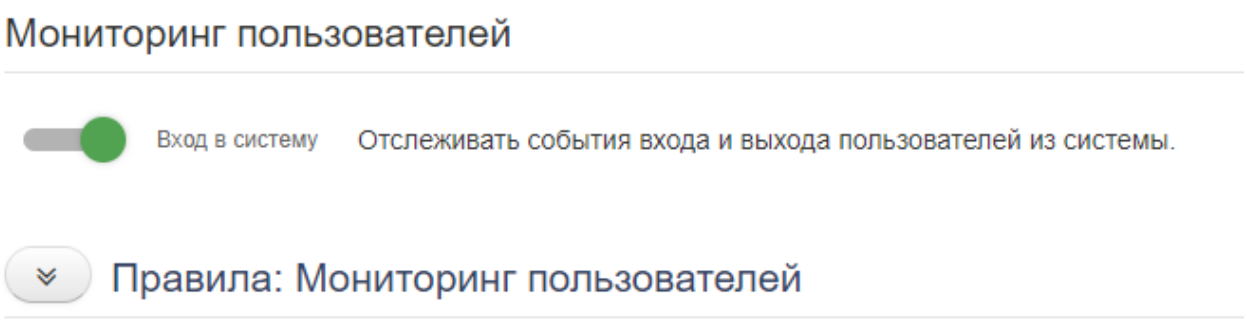


Вкладка **Общее** позволяет увидеть все включенные модули и задать название конфигурации. Также, только в этой вкладке находится модуль **Режим отладки** - включение этого модуля принуждает агент отправлять на сервер подробный отладочный лог, который необходим для выяснения причин

возникновения нештатных ситуаций на агенте. Для настройки правил требуется перейти в настройки конкретного модуля.

Примечание: Обратите внимание, кнопка «Сохранить как новый объект», расположенная рядом с кнопкой «Сохранить», позволяет копировать политику из существующей.

4.1.2 Мониторинг пользователей



- **Вход в систему** — модуль отслеживает вход/выход пользователей.

Правила: Мониторинг пользователей

Задает черно-белые списки для пользователей.

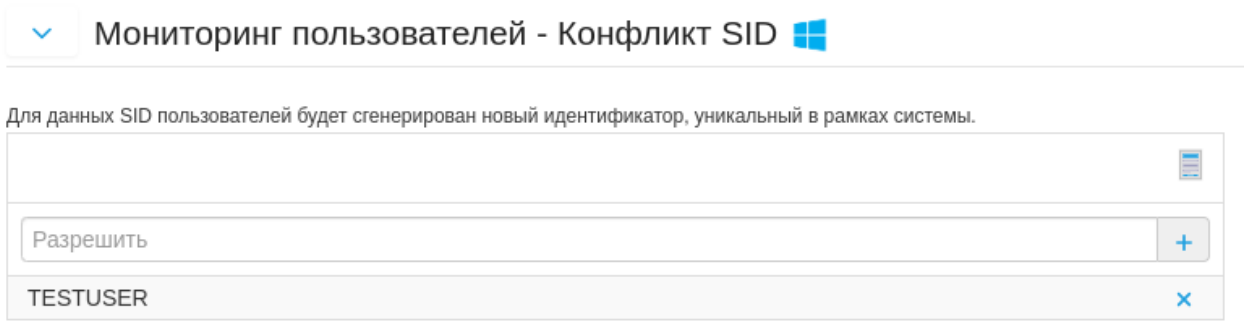
Запретить — запрет сбора событий указанных в списке пользователей.

Разрешить — разрешение сбора событий для указанных в списке пользователей. Все остальные события со всех остальных пользователей собираться не будут.

Правила: Мониторинг пользователей — Конфликт SID

Конфликт SID возникает, когда два пользователя получают одинаковый уникальный идентификатор (SID).

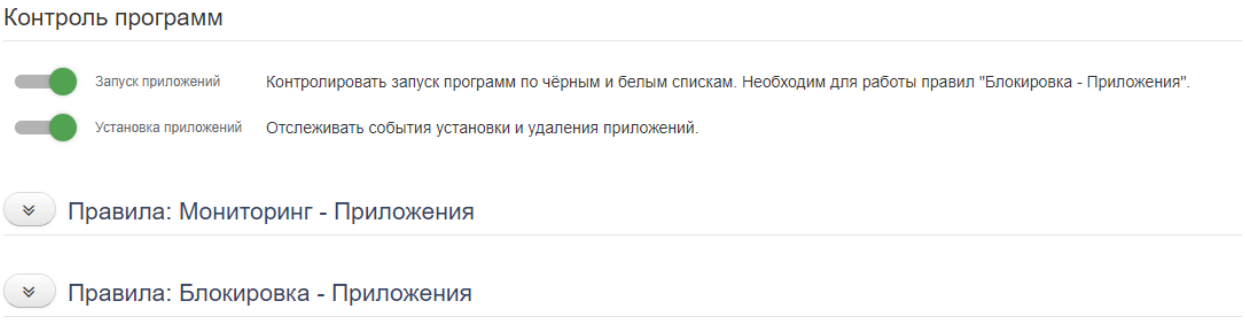
Используйте правило, чтобы задать пользователям новый идентификатор.



См.также:

Подробнее в статье *Идентификация пользователей на клонированных системах*.

4.1.3 Контроль программ



- **Запуск приложений** - модуль отслеживает запуск приложений.
- **Установка приложений** - модуль отслеживает установку/удаление приложений.

Запуск приложений

По умолчанию **события запуска/завершения приложений** не фиксируются в БД. Для включения данного типа события необходимо проделать следующие действия:

1. Зайти под root и включить данный тип событий:

```
sudo su
echo "APP_RUN_EVENTS=True" >> /etc/ibatyr/config
```

2. Перезагрузить ibatyr:

```
ibatyr restart
```

Теперь события будут обрабатываться сервером.

Правила: Мониторинг - Приложения

Это правило может исключить из перехвата события, которые выполняются автоматически или заданы системных администратором на конечных станциях, уменьшая при этом нагрузку на сервер iBatyr Monitor .

Запретить - запрет сбора событий генерируемого указанным исполняемым файлом, приложением или списка приложений.

Разрешить - разрешение на отслеживание событий для приложений, перечисленных в списке. Не указанные в списке приложения не отслеживаются.

Правила: Блокировка - Приложения

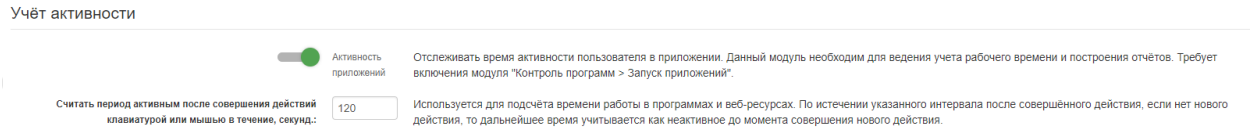
Блокировать - блокировать запуск приложений по имени. Не внесённые в список приложения не блокируются.

Разрешить - список разрешенных приложений по имени.

Примечание: При добавлении разрешенных приложений учитывайте, что все приложения, не внесенные в разрешенный список, блокируются! Это может привести к неработоспособности операционной системы.

Осторожно: Для корректной работы системы при внесении изменений в список разрешенных программ обязательно должны быть указаны системные процессы.

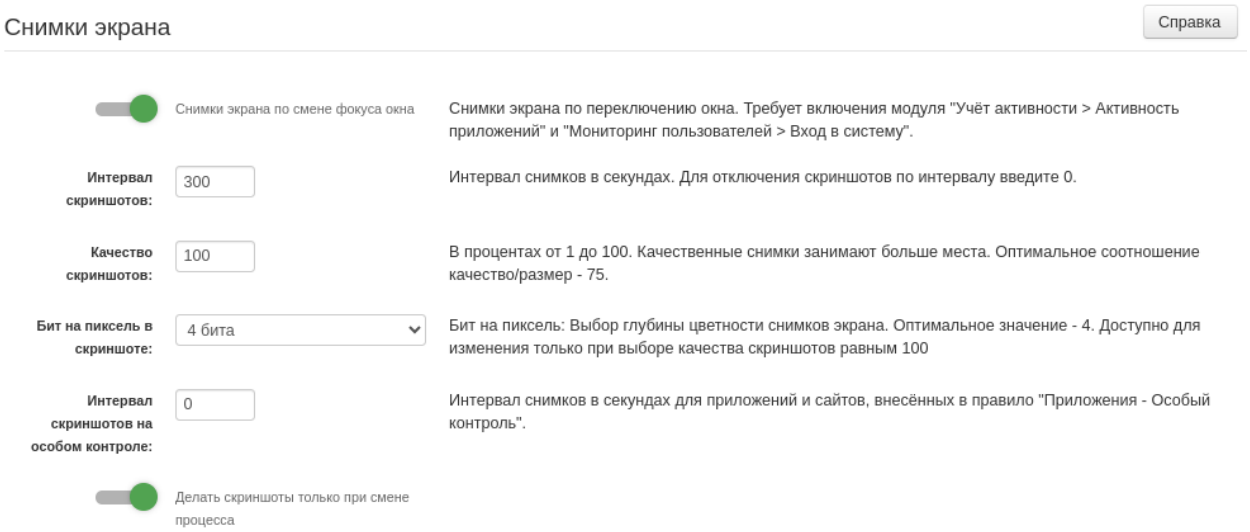
4.1.4 Учёт активности



- **Активность приложений** — модуль отслеживает общее время работы приложений, время активности пользователя в приложении, время неактивности пользователя в приложении. Работа этого модуля необходима для построения отчетов по учету рабочего времени, отчетов продуктивности и др.
- **Считать период активным после совершения действий клавиатурой или мышью в течение, секунд** — интервал, после которого, если не совершалось никаких действий, время будет считаться неактивным, до совершения новых действий.

Примечание: Активное время будет считаться только в том случае, если данное приложение является активным окном. Если окно свернуть, активность по данному приложению или сайту прекратится.

4.1.5 Снимки экрана



Настройте параметры снимков экрана:

- **Снимки экрана по фокусу окна** — фиксируют состояние экрана в момент активации определенного окна или приложения — к примеру, сочетанием клавиш Alt+Tab.
- **Интервал создания скриншотов** — создает скриншоты через указанное в секундах время. Чтобы отключить функционал, введите значение равное **0**.

> **Предупреждение:** Снимки в этом режиме могут делаться с высокой частотой, поэтому заранее *рассчитайте объем дисков для хранения скриншотов*.

- **Качество скриншотов** — снижает качество скриншотов для экономии места на жестком диске сервера. Оптимальное значение: **75**.
- **Бит на писксель** — задает глубину цвета скриншота. Чем ниже значение битности, тем меньше места занимают скриншоты. Оптимальное значение для скриншотов: **4**.
  - **1** — чёрно-белые скриншоты,
  - **4**, **8** — неполноцветные скриншоты,
  - **16**, **24**, **32** — полноцветные скриншоты.

> **Внимание:** Настройка цветности снимков доступна только на Windows-агенте.

- **Интервал создания скриншотов на особом контроле** — задает интервал времени снимков приложений, которые внесены в правило *Особый контроль* текущей конфигурации.
- **Делать скриншоты только при смене процесса** — создает скриншоты только при переключении процессов — к примеру, переходе из Word в Excel.

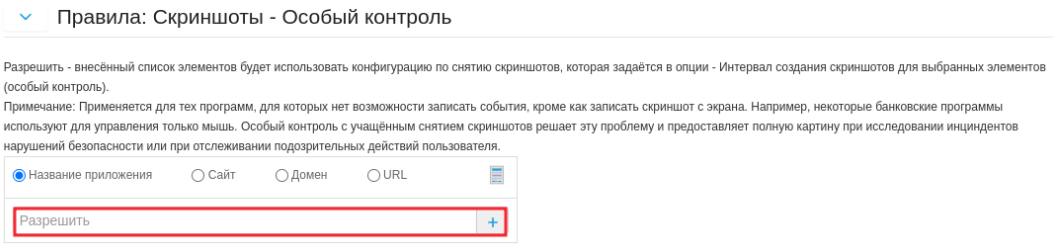
Примечание: Скриншоты при смене:

Правила: Особый контроль

Правило позволяет создавать скриншоты для определенных программ или сайтов с заданной периодичностью независимо от того, активно ли окно приложения или нет. Это особенно полезно для приложений, в которых скриншоты — единственный способ отследить действия пользователя. Например, некоторые банковские программы используют для управления только мышь.

Чтобы поставить приложение или сайт под особый контроль:

1. Откройте вкладку **Правила: Особый контроль**.
2. Введите название приложения, адрес сайта, домен, URL в поле **Разрешить**.
3. Добавьте приложение в список.



4. Вернитесь в настройки снимков и задайте частоту в параметре **Интервал создания скриншотов на особом контроле**.

См.также:

Как работают чёрные и белые списки

4.1.6 Пакет снимков экрана

Модуль **Пакет снимков с экрана** создаёт серию скриншотов рабочего стола с заданным интервалом и качеством снимков. Технология их создания и хранения позволяет значительно экономить ресурсы машины, в частности дисковое пространство.

Примечание: Реализовано для Windows- и Linux-агентов.

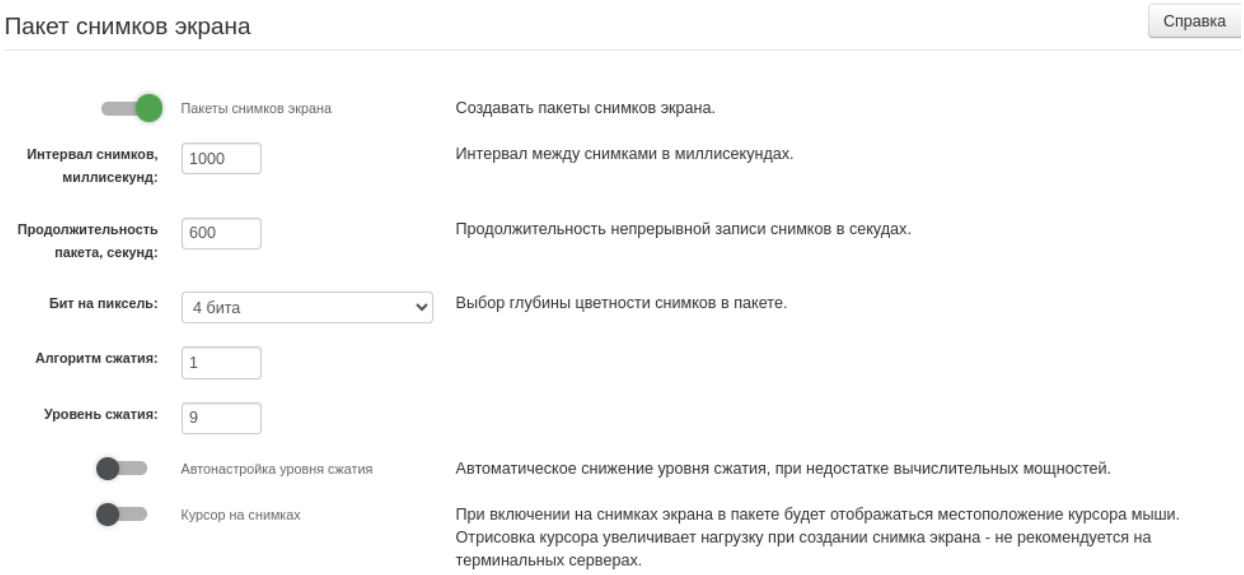
Пакет снимков экрана можно воспроизвести как видео с помощью встроенного плеера.

См.также:

Подробнее о работе с пакетами снимков экрана.

Особенности работы модуля:

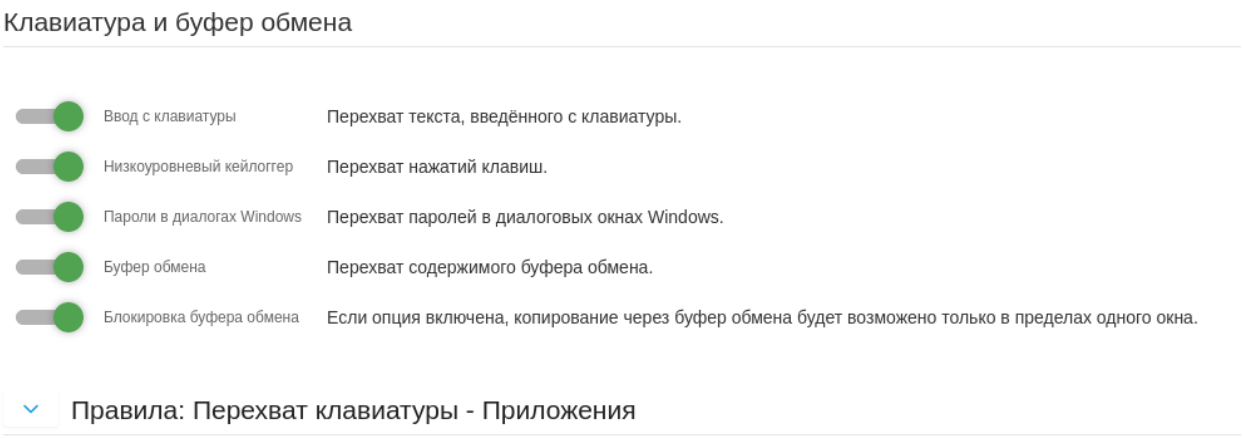
- модуль начинает свою работу сразу после сохранения изменений в конфигурации компьютера;
- событие **Пакет снимков экрана** приходит на сервер, как только начинает создаваться пакет;
- файл к событию **Пакет снимков экрана** прикладывается после его получения сервером;
- если во время отправки пакета скриншотов, связь с сервером была потеряна, отправка продолжится сразу после восстановления связи.



Описание опций модуля **Пакет снимков с экрана**:

Опция	**Описание**
Пакеты снимков экрана	Включает пакетную запись скриншотов.
Интервал снимков, миллисекунд	Позволяет выбрать временной интервал между снимками.
Продолжительность пакета, секунд	Продолжительность непрерывной записи пакета. Оптимальная продолжительность пакета — 10 минут (600 секунд).
Бит на пиксель	Позволяет выбрать цветность создаваемых скриншотов. Поддерживаемые значения: • **2**, **4**, **8** — оттенки серого, • **24**, **32** — полноцветные скриншоты. Чем ниже значение битности, тем меньше места занимают скриншоты. При этом качество самих скриншотов также снижается.
Алгоритм сжатия	Выбор алгоритма для сжатия скриншотов. Допустимые значения: • **0** — быстрый алгоритм, оптимизированный для слабых ПК, • **1** — эффективный алгоритм сжатия (используется по умолчанию).
Уровень сжатия	Степень сжатия снятых скриншотов. Допустимые значения: от **0** до **9**. Чем выше уровень сжатия, тем само сжатие лучше, но тем выше нагрузка на ПК.
Автонастройка уровня сжатия	Опция, позволяющая настроить оптимальное соотношение параметров **Алгоритм сжатия** и **Уровень сжатия** с учётом производительности АРМ. **Уровень сжатия** при автонастройке не опускается ниже **3**.

4.1.7 Клавиатура и буфер обмена



- **Ввод с клавиатуры** — модуль перехвата ввода с клавиатуры (кейлоггер). Для macOS работает в обход Безопасного ввода, как низкоуровневый кейлоггер.
- **Низкоуровневый кейлоггер** — модуль, который перехватывает любые нажатия клавиш, в том числе функциональные и служебные кнопки, кнопки управления курсором, горячие клавиши. Обходит Защищенный рабочий стол в Windows и механизмы защиты в Linux. Позволяет перехватывать пароли при входе в Windows.
- **Пароли в диалогах Windows** — модуль для перехвата паролей.

Примечание: Для получения событий необходимо также включить модули **Ввод с клавиатуры** и **Перехват паролей в диалогах Windows**.

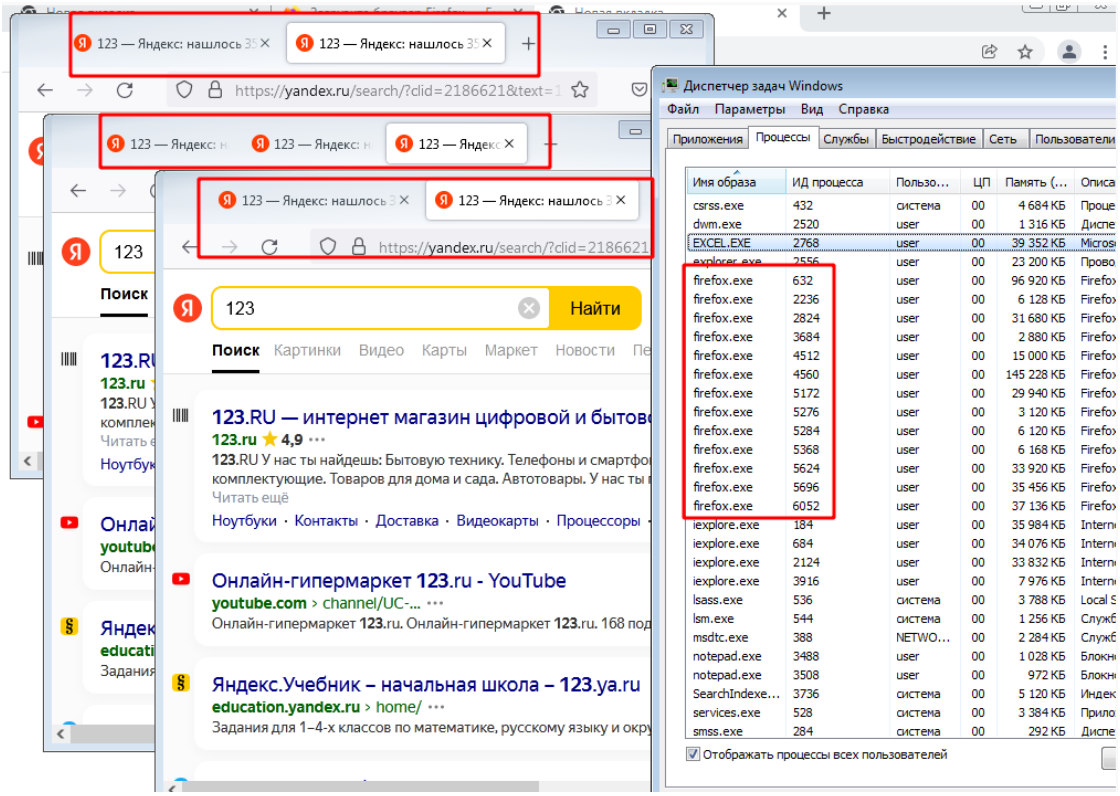
- **Буфер обмена** — модуль перехвата текста из буфера обмена.

  Чтобы модуль перехватывал скриншоты, которые создает пользователь с помощью клавиши Print Screen, включите в модуле **Файлы** опцию *Теневое копирование*.

Примечание: В редких случаях этот модуль может конфликтовать с приложениями MS Office. Если у пользователей наблюдаются просадки производительности при работе в MS Office, попробуйте отключить этот модуль.

- **Блокировка буфера обмена** — блокирует копирование текста или изображений через буфер обмена в пределах приложения. Блокировка работает по PID, то есть если у окон один и тот же PID (браузер, офис и другие), то работа с буфером в рамках этих окон возможна. Данный модуль работает только на Windows начиная с версии агента 2552.

Примечание: Хотя большинство известных браузеров имеет несколько процессов с разными PID, но у всех есть основной процесс, поэтому модуль **Блокировка буфера обмена** работает корректно.



Правила: Перехват клавиатуры — Приложения

Запретить — запрет отслеживания при помощью кейлоггера ввода с клавиатуры для указанного списка приложений. Остальные приложения отслеживаются с помощью кейлоггера.

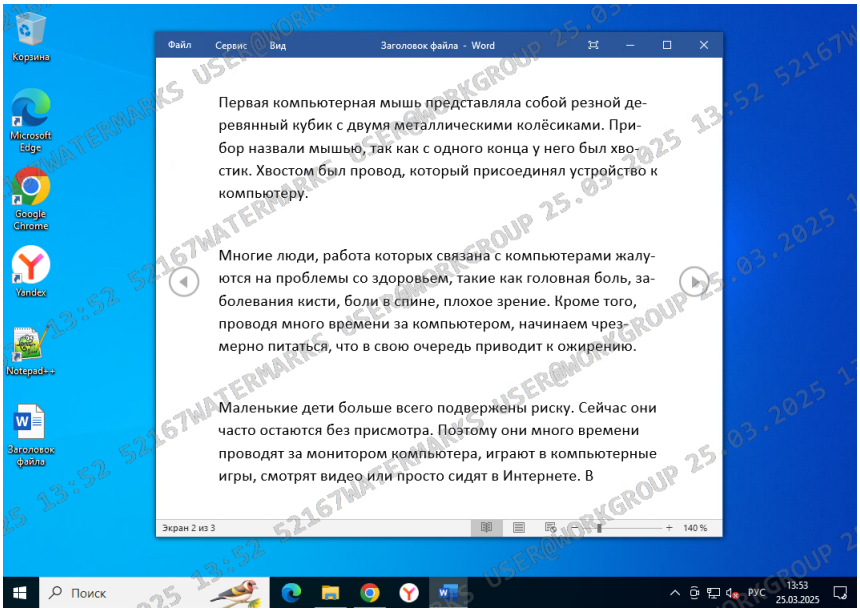
Разрешить — разрешение отслеживания ввода с клавиатуры через кейлоггер только от указанного списка приложений. Ввод с клавиатуры от остальных приложений не отслеживается.

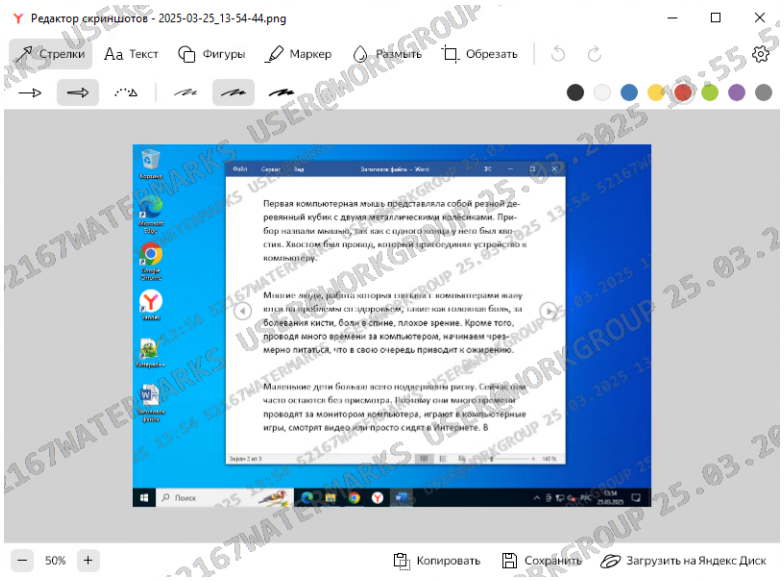
4.1.8 Водяные знаки

Водяные знаки защищают данные от утечек, если кто-то решит сфотографировать экран или сделать скриншот. Они автоматически выводятся на весь экран при запуске указанных в настройках приложений или сайтов. Знаки остаются на экране, даже если пользователь свернул окно приложения.

На водяном знаке отображаются имя компьютера, логин пользователя и локальное время.

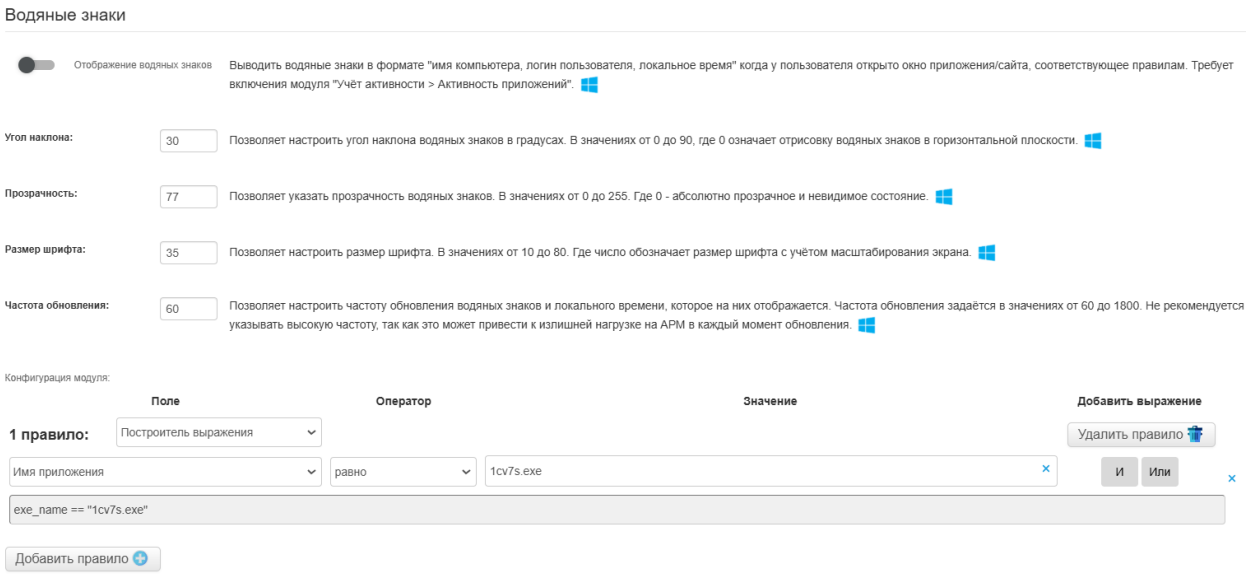
Водяные знаки высвечиваются и на скриншотах.


Файл Сервис Вид
Заголовок файла - Word
Первая компьютерная мышь представляла собой резной деревянный кубик с двумя металлическими колёсиками. Прибор назвали мышью, так как с одного конца у него был хвостик. Хвостом был провод, который присоединял устройство к компьютеру.
Многие люди, работа которых связана с компьютерами жалуются на проблемы со здоровьем, такие как головная боль, заболевания кисти, боли в спине, плохое зрение. Кроме того, проводя много времени за компьютером, начинаем чрезмерно питаться, что в свою очередь приводит к ожирению.
Маленькие дети больше всего подвержены риску. Сейчас они часто остаются без присмотра. Поэтому они много времени проводят за монитором компьютера, играют в компьютерные игры, смотрят видео или просто сидят в Интернете. В
Экран 2 из 3
140 %
Поиск
РУС
13:53
25.03.2025


Редактор скриншотов - 2025-03-25_13-54-44.png
Стрелки
Текст
Фигуры
Маркер
Размыть
Обрезать
50%
Копировать
Сохранить
Загрузить на Яндекс Диск

Раздел настройки

Перейдите в **Панель управления** → **Конфигурации компьютеров** → *ваша конфигурация* и в боковом меню выберите **Водяные знаки**. Откроется окно настроек:



Отображение водяных знаков — включает вывод водяных знаков в формате *Имя компьютера, Логин пользователя, Локальное время*.

Угол наклона — угол наклона водяных знаков в градусах от 0 до 90, где 0 означает отрисовку водяных знаков в горизонтальной плоскости.

Прозрачность — прозрачность от 0 до 255, где 0 — невидимое состояние.

Размер шрифта — размер шрифта от 10 до 80, где число обозначает размер шрифта с учётом масштабирования экрана.

Частота обновления — частота обновления локального времени на водяном знаке от 60 до 1800 секунд.

> **Предупреждение:** Не указывайте высокую частоту обновления — это может привести к дополнительной нагрузке на компьютеры сотрудников.

Настройка водяных знаков

Перед началом работы убедитесь, что в конфигурации включён параметр **Активность приложений**. Без этого нельзя наложить водяные знаки на окно приложений.

1. Перейдите **Панель управления** → **Конфигурации компьютеров** → *ваша конфигурация*.
2. Перейдите в раздел **Учёт активности** и убедитесь, что включена опция *Активность приложений*.

После этого включите и настройте водяные знаки:

1. Выберите в боковом меню **Водяные знаки**.
2. Активируйте **Отображение водяных знаков**.

3. При необходимости настройте отображение водяных знаков в полях **Угол наклона**, **Прозрачность**, **Размер шрифта** и **Частота обновления**.

Активации отображения в окне настроек недостаточно, чтобы знаки отображались на экране. Для этого нужно создать правило в разделе **Конфигурация модуля**.

Как добавить водяные знаки для приложений и сайтов

После настройки знаков добавьте в разделе **Конфигурация модуля** сайты или приложения для вывода водяного знака.

Настроим правило для вывода водяных знаков на примере приложения *1С:Предприятие 8*:

1. Нажмите **Добавить правило**.
2. Выберите переменную в столбце **Поле**. В нашем случае мы работаем с приложением, поэтому выбираем **Имя приложения**.

   Доступные опции:

   tabularytabulary

Поле
Имя приложения
Описание приложения
Заголовок окна
Полный домен

3. Выберите **Логический оператор** и укажите **Значение**. Например, **Имя приложения** — **равно** — *1cv8s.exe*.

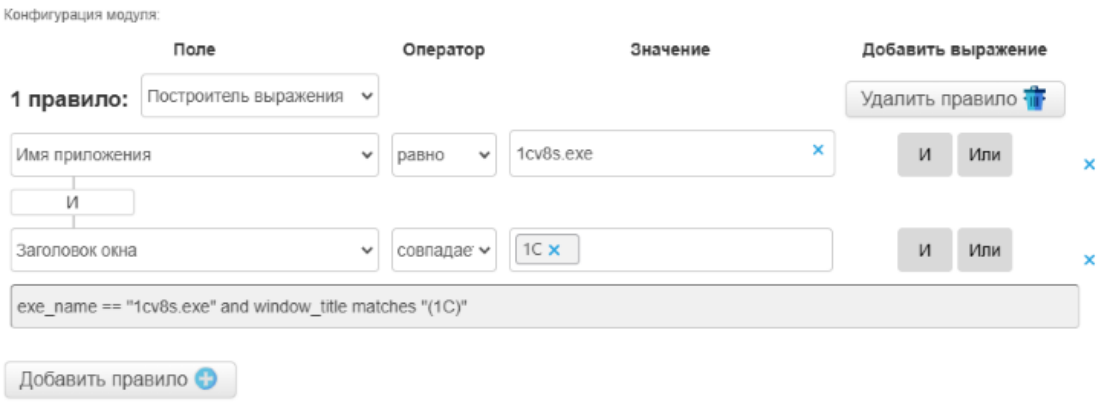
   Вы можете выбрать операторы для своих задач:

   tabularytabulary

Логический оператор	
равно	**Значение** полностью
не равно	**Значение** полностью н
совпадает	**Поле** подходит под *регулярн*
не совпадает	**Поле** не подходит под *регулярно*
содержится в	**Поле** содержится в списке.
не содержится в	**Поле** не содержится в списке.

4. При необходимости добавьте дополнительные условия с помощью операторов **И** / **ИЛИ**. Например, нажмите **И** и добавьте правило **Заголовок окна** — **совпадает** — *1С*.

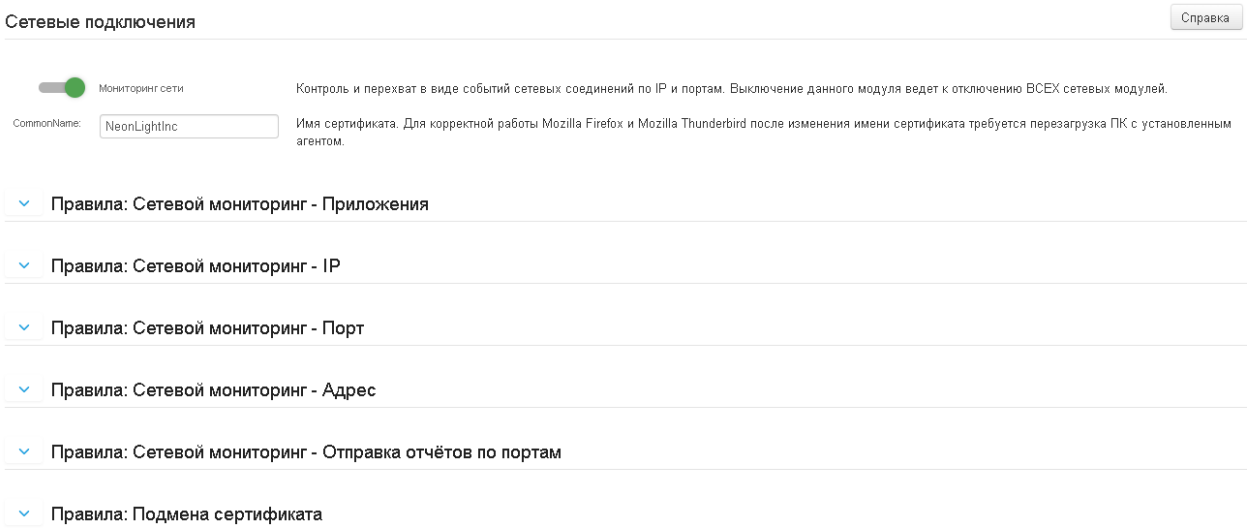
   На этом шаге настройки имеют вид:



5. Нажмите **Сохранить** и подождите 3–5 минут, чтобы изменения вступили в силу.

В результате водяные знаки будут отображаться на экране пользователя, если открыто приложение *1С:Предприятие 8*.

4.1.9 Сетевые подключения



Мониторинг сети — модуль для перехвата фактов соединений в сети по IP и портам.

CommonName — имя сертификата, которое будет использоваться при подмене. Оставьте его указанным по умолчанию или задайте своё для удобства.

Примечание: После смены имени сертификата, перезагрузите машины, на которых установлены Mozilla Firefox и Thunderbird.

Правила: Сетевой мониторинг — Приложения

Запретить — сетевые обращения указанных приложений не отслеживаются. Все остальные сетевые операции любого приложения в системе будут записаны.

Разрешить — отслеживается только сетевая активность указанных приложений.

Правила: Сетевой мониторинг — IP

Запретить — сетевая активность любых приложений на указанные IP-адреса не отслеживается.

Разрешить — отслеживается сетевая активность только для указанных IP-адресов.

Примечание: Пример написания диапазона IP-адресов: **192.168.0.1-192.168.10.254**.

Правила: Сетевой мониторинг — Порт

Запретить — не отслеживаются события для определённого порта в сетевом трафике от всех приложений.

Разрешить — отслеживаются только события для определённого порта в трафике.

Примечание: В разделе **Панель управления** — **Глобальная конфигурация** уже существуют правила для отслеживания сетевого трафика по определённым портам. Указанные здесь правила будут переопределять правила из глобальной конфигурации.

Правила: Сетевой мониторинг — Адрес

Запретить — запрещает отслеживание сетевых операций для указанного адреса списка сайтов.

Разрешить — разрешает отслеживание сетевой активности только для указанного адреса сайта или списка адресов сайтов.

Примечание:

При создании маски для правила можно использовать спецсимвол «*» для замены набора символов. Символ «?» спецсимволом не является.

Пример: выражение **example.com* в строке **Запретить** создаст правило, по которому не будет отслеживаться трафик на все поддомены домена *example.com*.

Чтобы агент не перехватывал в WhatsApp служебные dat-файлы и BLOB-объекты, запретите два адреса:

- https://graph.whatsapp.net,
- https://dit.whatsapp.net.

См.также:

Как работают чёрные и белые списки

Правила: Сетевой мониторинг — Отправка отчетов по портам

Запретить — запрещает отслеживание сетевых операций для указанного списка портов.

Разрешить — отслеживает сетевые операции только для указанного списка портов.

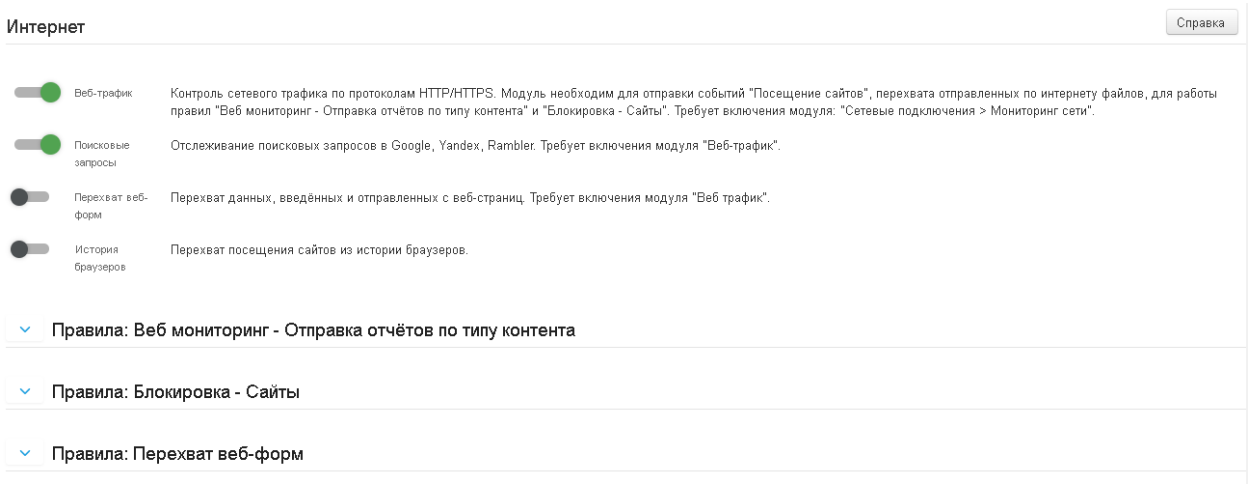
Правила: Подмена сертификата

Запретить — запрещает подмену сертификатов на указанных сайтах. В данном поле указывается только имя домена, не IP-адрес. При обращении на все остальные домены, шифрованный трафик будет перехватываться и попадать в статистику перехваченных событий.

Разрешить — разрешает подмену сертификатов у сетевых соединений, только для указанного списка доменов. Все остальные домены не будут перехватываться и попадать в статистику.

Внимание: Если у вас используются сертификаты для IP-адресов, внесите их в **Правила: Сетевой мониторинг — IP**. После этого проверка защищенного соединения проводиться не будет.

4.1.10 Интернет



- **Веб трафик** — модуль перехвата сетевого трафика по протоколам HTTP/HTTPS. Агент перехватывает и фиксирует всю сетевую активность приложений, в том числе по зашифрованным каналам (SSL/TLS). Данный модуль необходим для перехвата истории посещения веб-страниц и для построения отчетов по учету рабочего времени.
- **Поисковые запросы** — модуль отслеживания запросов в поисковых системах (Rambler, Google, Yandex).
- **Перехват веб-форм** — модуль перехвата post-запросов с веб-страниц в браузере. Используется для перехвата паролей веб-ресурсов при помощи политики безопасности «Перехват паролей в браузерах».

Примечание: Для просмотра событий, связанных с перехватом паролей веб-ресурсов, необходимо перейти в **Сработавшие политики – Перехват паролей в браузерах**.

- **История браузеров** — модуль перехвата посещения сайтов из истории браузеров. Используется для Linux-агентов.

Правила: Веб мониторинг — Отправка отчетов по типу контента

Запретить — запрещает сбор данных по выбранным типам контента.

Разрешить — разрешает сбор данных только по выбранным типам контента.

Правила: Блокировка — Сайты

Блокировать — блокирует сайты доменному имени (vk.com, youtube.com, . . .).

Разрешить — сайты, разрешенные для посещения (hh.ru, example.com, . . .). Все остальные сайты будут запрещены.

Для запрета и разрешения доступа к сайтам по протоколам *http* и *https* есть возможность гибкой настройки:

- Если явно указать в разрешающих правилах адрес **https://vk.com**, доступ к нему будет разрешён только по протоколу *https*. Адрес **http://vk.com** будет заблокирован.
- Если в разрешающем правиле указать **vk.com**, то к **vk.com** будет разрешен доступ по обоим протоколам (*http* и *https*).

См.также:

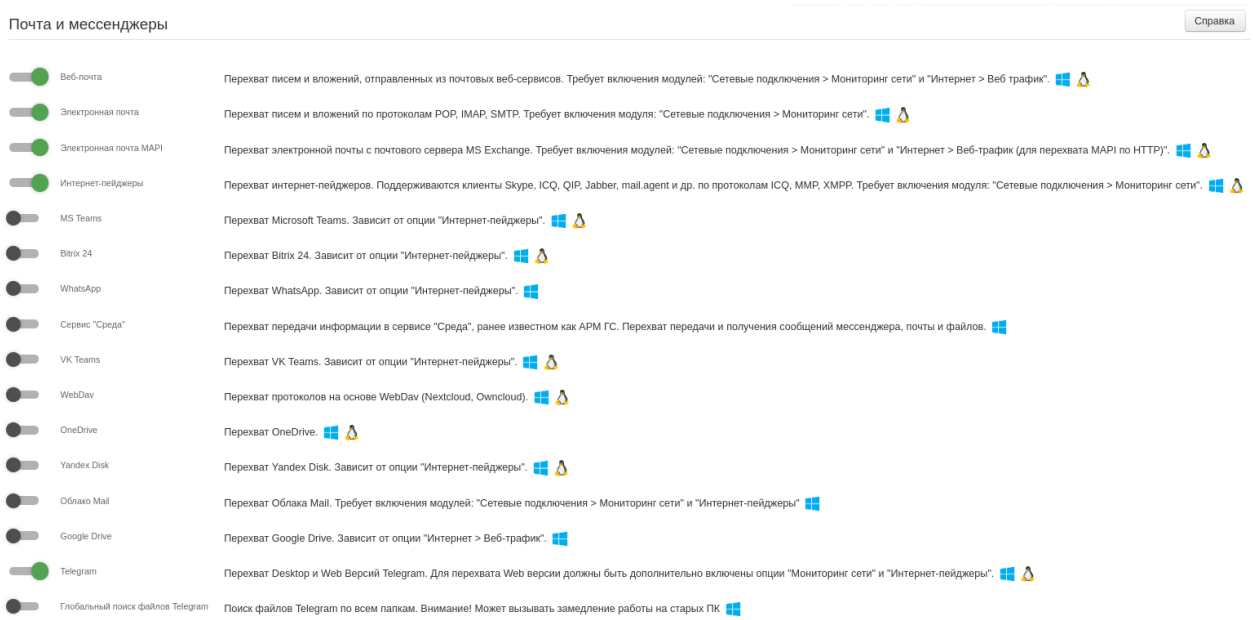
Как работают чёрные и белые списки

Правила: Перехват веб-форм

Запретить — запрещает сбор данных веб-форм с указанных сайтов или URL.

Разрешить — разрешает сбор данных веб-форм только с указанных сайтов или URL.

4.1.11 Почта и мессенджеры



Некторые интернет-пейджеры вынесены в отдельные опции, поскольку при их включении создаётся дополнительный процесс в системе.

Примечание: Файлы и текстовые сообщения из мессенджера Express перехватываются без включения/выключения. После интеграции через ICAP они появятся на сервере в типах событий **Интернет-пейджер** и **Перехваченные файлы** соответственно.

Примечание: Для перехвата файлов включите **Теневое копирование** в разделе конфигурации *Файлы*.

Описание модулей

tabularytabulary

Модуль
Веб-почта
Электронная почта
Электронная почта MAPI
Перехват сервиса «Среда»
Интернет-пейджеры
MS Teams
Bitrix 24
WhatsApp
VK Teams
WebDav
OneDrive
Яндекс.Диск
Mail.ru
Google Drive
Telegram
Глобальный поиск файлов Telegram

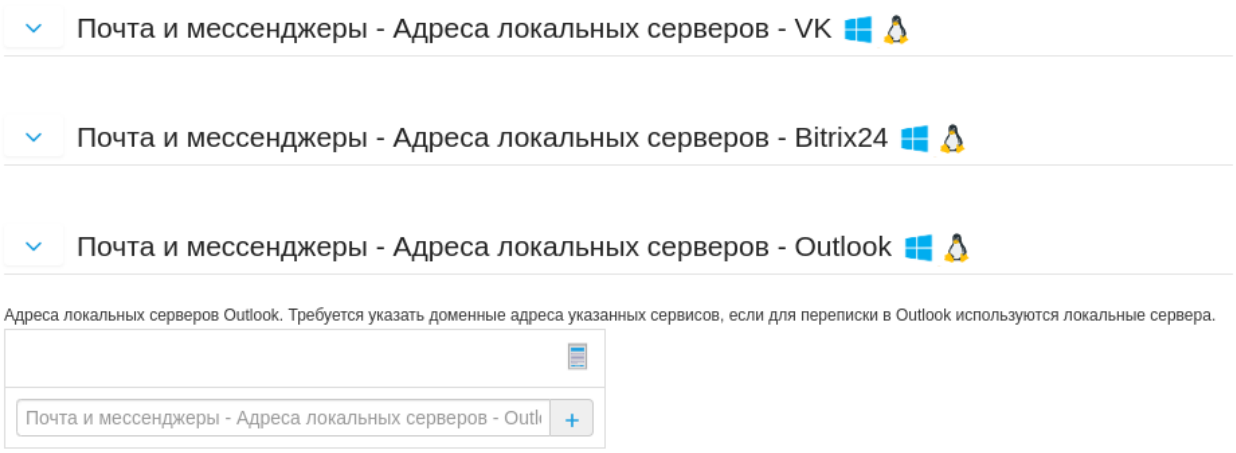
Поддержка локальных адресов

Начиная с версии 5.6 в конфигурацию агента добавлена поддержка локальных адресов для сервисов:

- VK Teams,
- VK Mail,
- Outlook,
- Bitrix24.

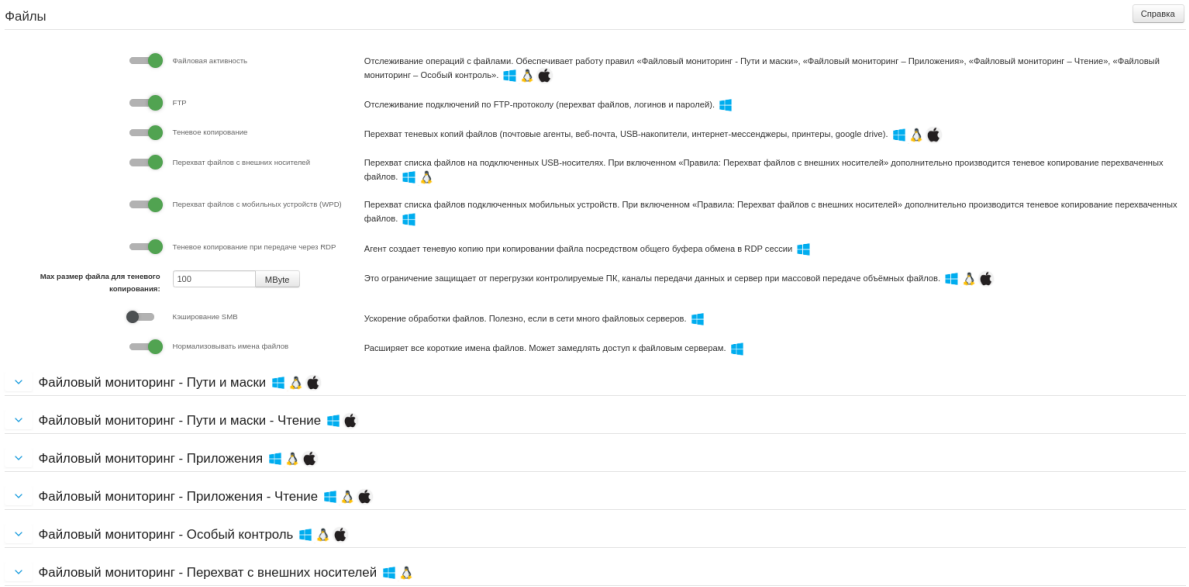
Теперь администратор может вручную указывать нестандартные доменные имена локальных серверов этих сервисов в поле **Почта и мессенджеры — Адреса локальных серверов**.

[1] WhatsApp не перехватывает служебные dat-файлы и BLOB-объекты, если они добавлены в исключения в конфигурации. Подробнее — в разделе **Правила: Сетевой мониторинг — Адрес** *статьи Сетевые подключения*.



В результате агент будет перехватывать переписку в соотвествии с возможностями перехвата, которые описаны в разделе *Описание модулей*.

4.1.12 Файлы



Файловая активность — отслеживает основные операции с файлами (чтение, запись, удаление и др.).

Примечание: Неправильная настройка данного модуля может привести к снижению производительности на рабочих станциях пользователей. Если нет задачи контроля за файловой активностью, отключите этот модуль, чтобы снизить нагрузку.

FTP — отслеживание подключений по FTP-протоколу: перехват логинов, паролей, скачиваемых и загружаемых файлов.

Теневое копирование — перехват теневых копий файлов. Поддерживает перехват файлов, отправленных:

- по электронной почте через почтовые агенты и веб-почту;

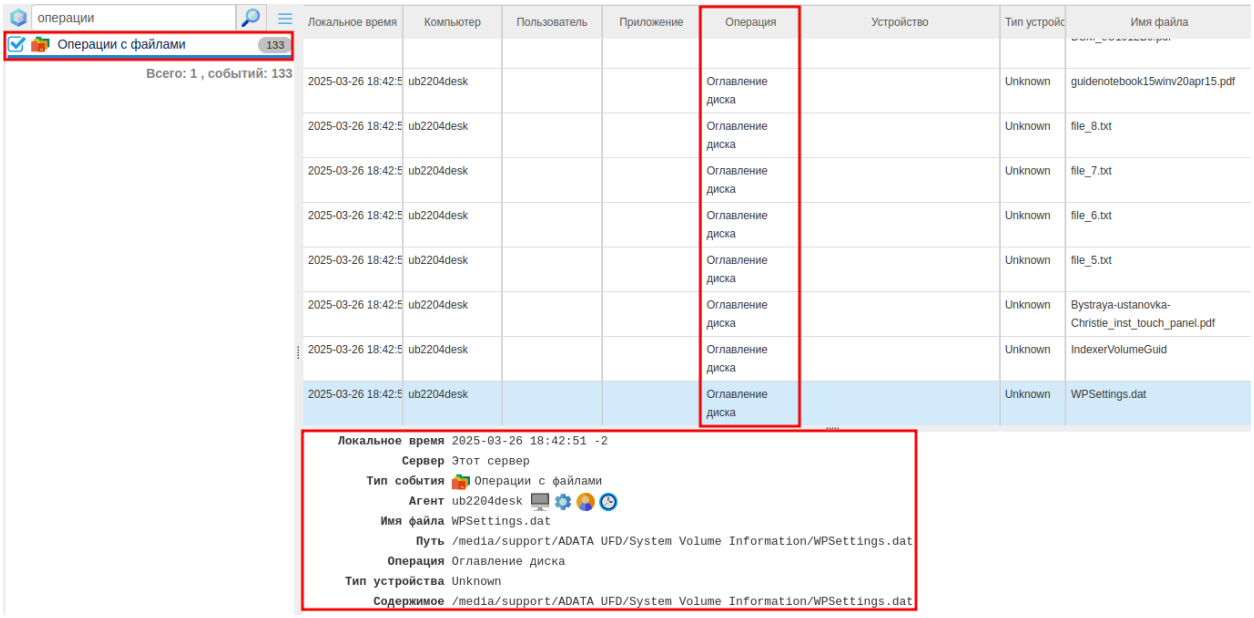
- на USB-накопители;
- через интернет-мессенджеры: QIP, ICQ, Skype, Агент Mail.ru и др.;
- на принтер;
- через браузер на Google Drive.

Примечание: Для Linux-систем теневое копирование файлов на USB-накопителях возможно только по адресам, указанным в **Правила: Файловый мониторинг — Пути и маски**.

Перехват файлов с внешних носителей — перехват списка файлов, которые находятся на USB-накопителе в момент подключения. Перехват доступен для **Windows-** и **Linux-**агентов.

Агент перехватывает файлы с расширениями: .png, .mp4, .xls, .txt, .docx, .doc, .jpg, .jpeg, .pdf.

Для каждого файла агент создает отдельное событие **Операция с файлом** с типом операции **Оглавление диска**. Событие содержит имя файла и его расположение на ВНИ.



Чтобы агент создавал копии файлов и передавал их на сервер, включите *Теневое копирование* и *задайте правила перехвата*.

Перехват файлов с мобильных устройств (WPD) — перехват списка файлов с подключенных мобильных устройств. При включенном **Правила: Перехват файлов с внешних носителей** дополнительно производится теневое копирование файлов.

Теневое копирование при передаче через RDP — создание теневых копий при копировании файлов через общий буфер обмена при подключении к удаленному рабочему столу через RDP-протокол.

Примечание: Включите опцию **Буфер обмена** в параметрах RDP-подключения для работы общего буфера обмена. Он позволяет копировать файлы между локальным и удаленным компьютером.

Предупреждение: Для работы модуля включите **Буфер обмена** в разделе *Клавиатура и буфер обмена*. Без него агент не будет контролировать общий буфер обмена и создавать теневые копии файлов при копировании.

Поведение при различных сценариях:

Сценарий	Результат
1. *ПК без агента* подключился через RDP к *ПК с агентом*. 2. Пользователь скопировал файл на *любом из ПК*.	Агент создаёт теневую копию файла.
1. *ПК с агентом* подключился через RDP к *ПК без агента*. 2. Пользователь скопировал файл на *ПК с агентом*.	Агент создаёт теневую копию файла.
1. *ПК с агентом* подключился через RDP к *ПК без агента*. 2. Пользователь скопировал файл на *ПК без агента*.	Агент не создаёт теневую копию файла.
1. *ПК с агентом* подключился через RDP к другому *ПК с агентом*. 2. Пользователь скопировал файл на *любом из ПК*.	Агент создаёт теневую копию файла.

Теневая копия создаётся как при копировании файла с компьютера на удалённый рабочий стол, так и в обратном направлении — с удалённого рабочего стола на компьютер под наблюдением агента.

Примечание: Для создания теневой копии размер файла не должен превышать значение в поле **Max размер файла для теневого копирования**.

Max размер файла для теневого копирования — максимальный размер файла для теневого копирования. Это ограничение защищает от перегрузки контролируемые ПК, каналы передачи данных и сервер в случае массовой передачи объемных файлов.

Кэширование SMB — ускорение обработки файлов. Полезно, если в вашей сети используется много файловых серверов.

Нормализовывать имена файлов — расширяет все короткие имена файлов. Может замедлять доступ к файловым серверам.

Правила: Файловый мониторинг — Пути и маски

Запретить — отключает отслеживание файловых операций по указанным путям.

Разрешить — отслеживает файловые операции только по указанным путям. Вся остальная файловая активность не отслеживается.

При указании путей мониторинга поддерживаются спецсимволы:

- звёздочка «*» — любое количество символов до или после указанной строки;
- вопросительный знак «?» — указание одного любого символа строки.

Файловый мониторинг на Linux-агентах

Чтобы включить файловый мониторинг на Linux-агенте, включите переключатель **Файловая активность** и добавьте пути для слежения в раздел **Правила: Файловый мониторинг — Пути и маски**.

Примечание: Если оставить пустыми строки **Разрешить** и **Запретить**, файловая активность не будет отслеживаться.

Примечание: Копирование файлов на Linux-агенте фиксируется только при перемещении по указанным путям. Если путь не включён в список, операция копирования не отслеживается.

Примеры указания путей:

tabularytabulary

Путь	Описание
/	Все директории на машине.
~/	Домашние директории пользователей.
~**user**/	Домашняя директория пользователя user.
/**media**/	Операции с CD- и USB-устройствами.
/**mnt**/	Операции с примонтированными USB-устройствами.
~/**.***	Операции в системных папках (*/home/user/.cahce/* и др.)

Правила: Файловый мониторинг — Пути и маски — Чтение

Запретить — отключает отслеживание операций *чтения* по указанным путям.

Разрешить — отслеживает операции *чтения* только по указанным в фильтре путям. Вся остальная файловая активность по любым путям не отслеживается.

Примечание: Это правило влияет на работу модуля «Файловая активность»: если в строке **Запретить** в конце пути или маски установлена «*****», то по этому пути не будут отслеживаться операции чтения файлов и в Линзе не будут отображаться никакие файловые операции, поскольку первая операция при работе с файлами всегда *Чтение*.

Правила: Файловый мониторинг — Приложения

Запретить — список исполняемых файлов, чьи операции с файлами не отслеживаются.

Разрешить — список исполняемых файлов, для которых нужно отслеживать файловые операции.

Правила: Файловый мониторинг — Приложения — Чтение

Запретить — запрещает отслеживать файловые операции *чтения* указанными исполняемыми файлами.

Разрешить — разрешает отслеживать файловые операции *чтения* только указанными исполняемыми файлами.

Правила: Файлы — Особый контроль

Разрешить — создает теневую копию для выбранных файлов при всех файловых операциях, кроме удаления.

Для Linux-систем теневое копирование файлов работает только внутри путей, указанных в **Правила: Файловый мониторинг — Пути и маски** и при включенном **Теневом копировании**. Теневые копии записываются в конструктор отчётов в соответствующую операцию в типе событий — **Файл — Операция**.

Примечание: При активном использовании, например, имени папки, может сформироваться очень много теневых копий файлов.

Правила: Перехват файлов с внешних носителей

Разрешить — маски для перехвата файлов с внешних накопителей.

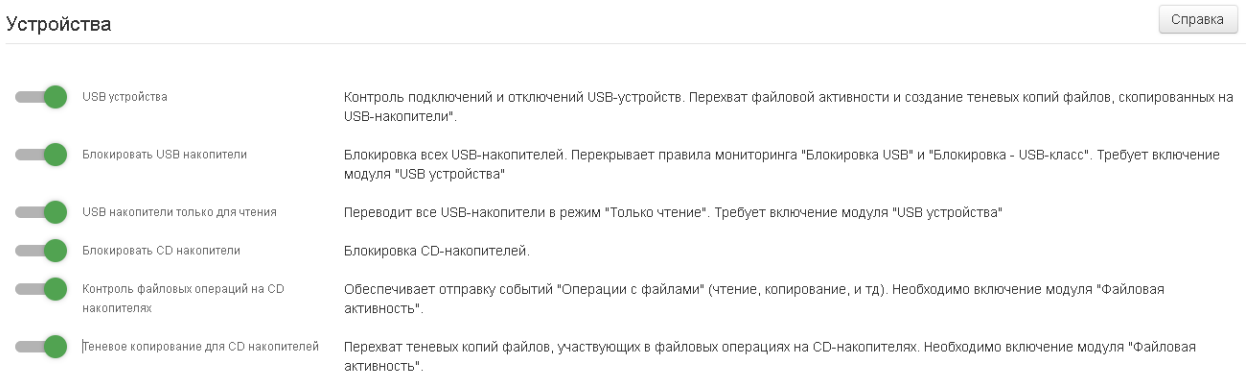
Поддерживаемый формат записей:

- ***.docx** — перехват файлов с указанным расширением;
- **name.*** — перехват файлов с заданным именем;
- ***.*** — перехват всех файлов с носителя.

Предупреждение: Правило ***.*** может вызвать большую нагрузку на сервер.

4.1.13 Устройства

Раздел **Устройства** позволяет настраивать контроль за подключаемыми устройствами: USB-накопителями и приводами CD/DVD-ROM.



Описание опций в разделе **Устройства**:

Опция	**Описание**
USB устройства	Основной управляющий модуль. Отвечает за фиксацию всех событий, относящихся к USB-устройствам (перехват операций, теневые копии. . .).
Блокировать USB накопители	Блокирует все подключаемые USB-носители (класса DiskDrive).
USB накопители только для чтения	Запрещает изменение файлов на USB-носителях.
Блокировать CD накопители	Блокирует все подключенные CD/DVD-диски.
Контроль файловых операций на CD накопителях	Включает отправку событий «Операции с файлами»: • чтение файлов с диска; • копирование файлов с диска; • запись файлов на диск, если диск форматирован как USB-накопитель. Требует включения опции «Файловая активность».
Теневое копирование для CD накопителей	Создание теневых копий файлов, участвующих в файловых операциях. Требует включения опции «Файловая активность».

Правила

Создание чёрного и белого списка USB-устройств описанио в статье *Контроль USB-устройств*.

Предупреждение: Будьте осторожны с правилом **Разрешить**!

«Device ID» или классы, не указанные в правиле, будут заблокированы. Это может сказаться даже на работе клавиатур и мышей.

Правила: Блокировка - USB

При добавлении «Device ID» в правило, указывайте его полным.

Блокировать - блокирует все «Device ID» в списке.

Разрешить - блокирует все «Device ID», кроме указаных в списке.

Правила: Блокировка - USB-класс

Блокировать - блокирует USB-устройства по классам. Значения берутся из списка «Устройства - Класс устройства».

Разрешить - разрешает использование USB-устройств по классам. Значения берутся из списка «Устройства - Класс устройства».

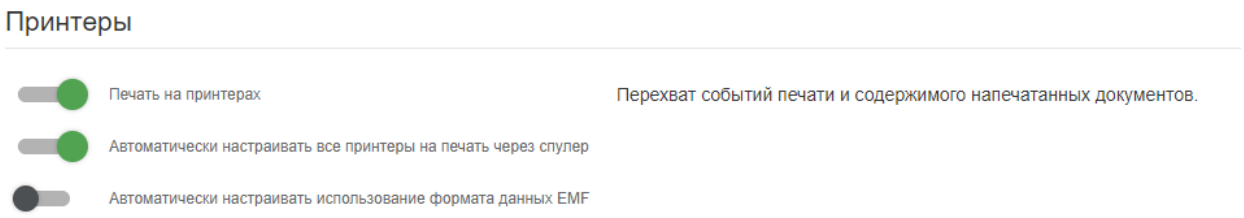
Правила: Блокировка - USB группы

Блокировать - блокирует USB-устройства по группам. Значения берутся из списка «Устройства - Маркер».

Разрешить - разрешает использование USB-устройств по группам. Значения берутся из списка «Устройства - Маркер».

Примечание: По умолчанию, маркер не назначен ни на одно устройство.

4.1.14 Принтеры



Настройка конфигурации

Печать на принтерах - модуль перехвата документов, отправленных на печать.

Включение данного модуля, при соблюдении *условий*, позволяет перехватывать:

- теневую копию документа, отправленного на печать;
- файл спулера, который формирует принтер перед печатью;
- скриншот рабочего стола в момент отправки документа на печать.

Автоматически настраивать все принтеры на печать через спулер - модуль автоматически настраивает принтеры на печать через спулер. При включенном параметре конфигурации «Файлы» - «Теневое копирование» и успешной настройки принтеров на печать через спулер, в событие печати будет добавлен архив с образом документа отправленного на принтер. Этот образ можно скачать и *просмотреть* с помощью веб-интерфейса или специальных программ в зависимости от формата образа.

Автоматически настраивать использование формата данных EMF - модуль автоматически переводит «Обработчик печати» в формат NT EMF 1.008. Эта настройка поможет при просмотре файла спулера сторонними приложениями.

Примечание: Автоматическая настройка включает печать через спулер, что для некоторых моделей принтеров приводит к невозможности печати, поэтому перед включением данного параметра необходимо проверить все используемые у вас модели принтеров на совместимость со спулером Windows.

Примечание: При выключении перехвата печати или остановке Агента параметр принтера «Сохранять документы после печати» отключается. Также при выключении перехвата или остановке Агента восстанавливается формат образа документа, на тот который был установлен до вмешательства Модуля. Остальные атрибуты не восстанавливаются до прежних значений, т.к. считается, что они всегда подходят пользователям и не нарушают процесс печати.

Примечание: Текущая реализация перехвата содержимого распечатываемых документов требует сохранения документов в спулере без их последующего удаления операционной системой. Это может привести к накоплению большого количества заданий печати в диспетчере печати и расходованию дискового пространства на ПК, где установлен Агент. Поэтому Агент автоматически и как можно быстрее удаляет успешно выполненные задания печати после их обработки, что в свою очередь приводит к удалению операционной системой соответствующих файлов в каталоге спулера. Эта информация может быть важна для тех, кто использует настройку принтера сохранять документы после печати в своих целях, отличных от задачи перехвата печати Агентом.

Описание необходимых условий для полноценного перехвата документов

1. Для перехвата скриншотов рабочего стола, при отправке документа на печать, необходимо включение модуля «Снимки экрана по смене фокуса окна» в разделе конфигурации «Снимки экрана».
2. Для перехвата необходимо выполнить автоматическую или ручную настройку принтеров. То есть, в свойствах принтера - «Дополнительно» должны быть включены следующие модули:

- «Использовать очередь печати»
- «Начинать печать после помещения в очередь всего задания»
- «Сохранять документы после печати»
- «Включить дополнительные возможности»

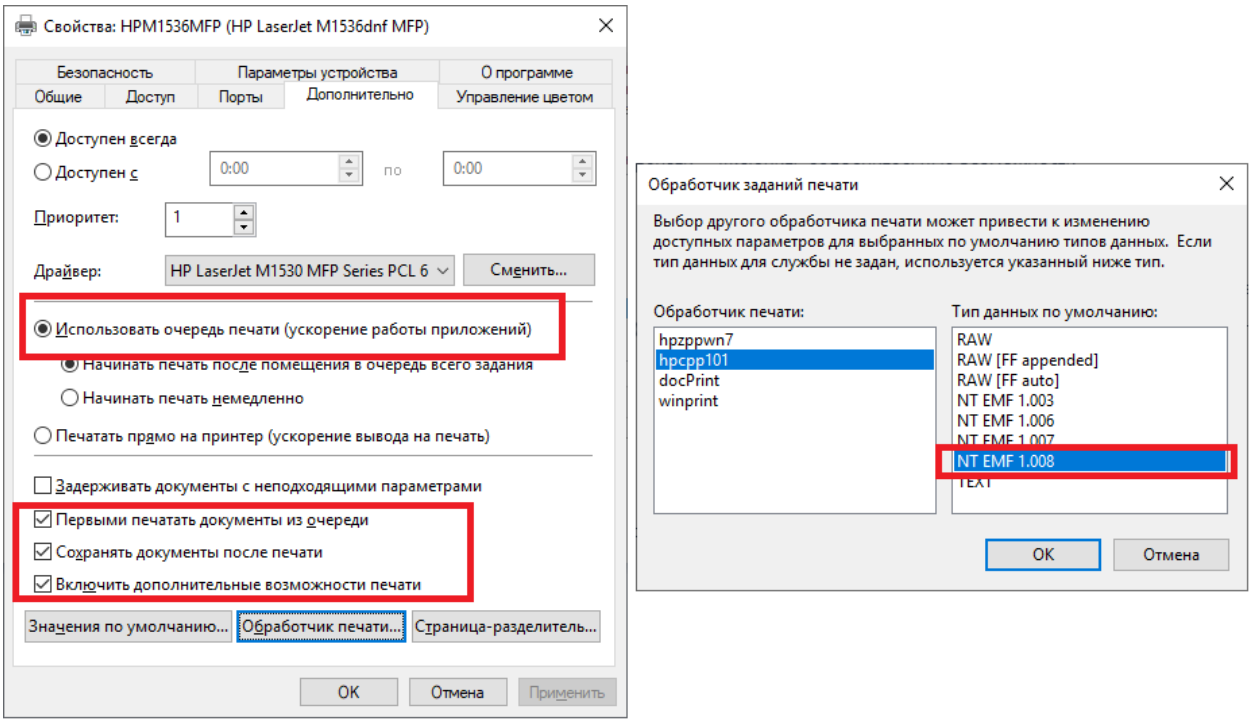
3. Для перехвата теневых копий документов необходимо включение модулей «Файловая активность» и «Теневое копирование» в конфигурации в разделе «Файлы» и должны быть выполнены необходимые настройки принтера.

Поиск оригинального файла, который был распечатан имеет следующие недостатки:

- Находит файл, который содержит документ не полностью соответствующий реально распечатанному, например, потому что пользователь его изменил и изменения не сохранил перед распечаткой.
- Не найдёт файл, если был создан новый документ и он не был ещё сохранен либо если файл с документом был удалён или перемещён в течении 30-60 секунд после печати.
- Не найдёт файл, если имя задания печати не содержит имя файла.
- Не найдёт файл, если печатающая программа не входит в заранее составленный список наблюдаемых процессов (winword.exe, excel.exe, wordpad.exe, notepad.exe, notepad++.exe, AcroRd32.exe, TOTALCMD64.EXE, TOTALCMD.EXE, SumatraPDF.exe, mspaint.exe, soffice.bin, FoxitReader.EXE, STDUViewerApp.exe, WinDjView.exe, acad.exe, SLDWORKS.exe).

Ручная настройка принтеров для перехвата событий печати

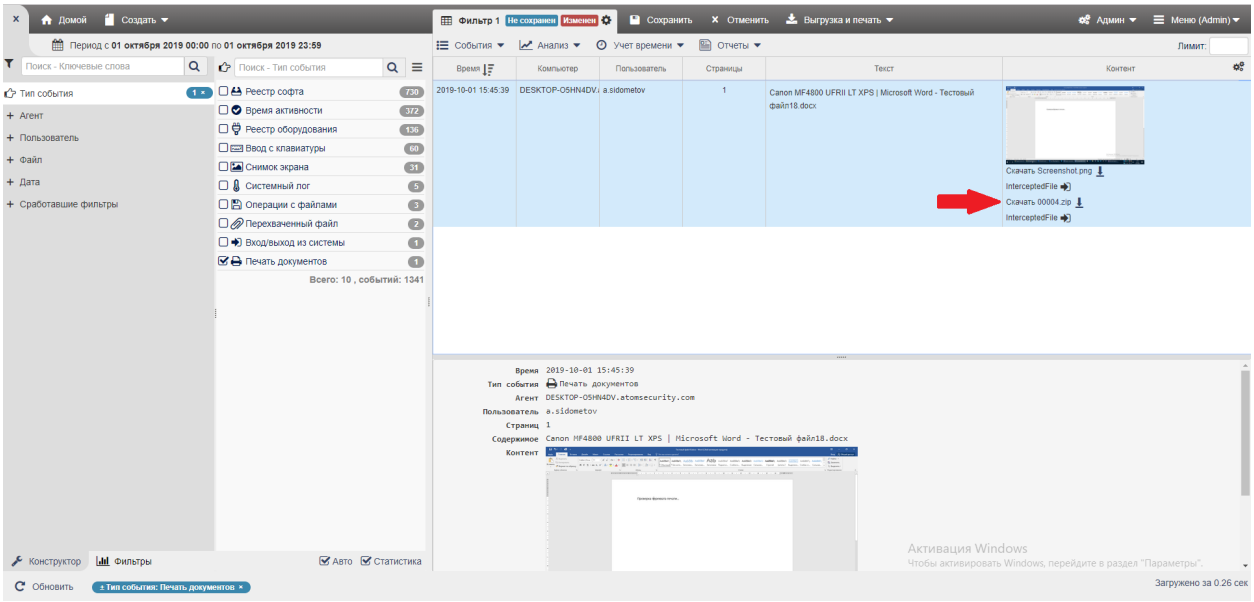
Если принтер является сетевым и у ПК с агентом нет возможности выполнить автоматическую настройку, вы можете выполнить настройку вручную. Для этого перейдите в свойства принтера и выполните следующие настройки:



Остальные параметры на закладке «Дополнительно» могут быть настроены согласно усмотрению администратора ПК.

Просмотр образа распечатанного документа

Образ распечатанного документа включается в Событие печати как zip-архив с именем в виде числа.



Этот архив содержит 2 файла, образ хранится в файле с расширением spl. Образы распечатываемых документов имеют формат который зависит от драйвера принтера, поэтому для их просмотра нужны соответствующие программы.

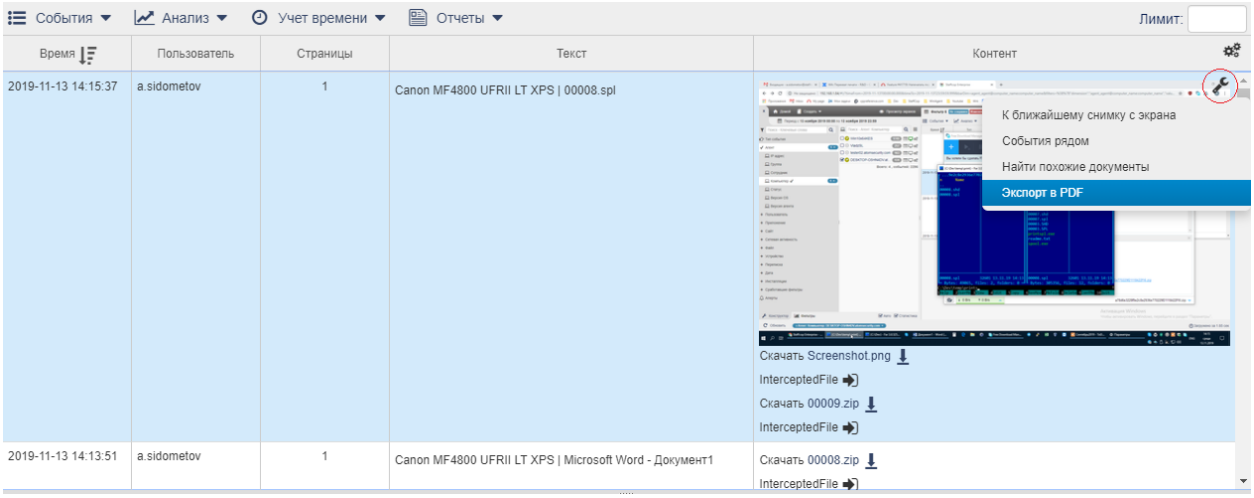
Принтеры с XPS-драйверами

Для принтеров с XPS-драйверами (в своём названии эти драйверы как правило имеют аббревиатуру XPS) образы документов формируются в формате XPS и их можно просматривать в веб-интерфейсе или с помощью программы «Средство просмотра XPS».

Примечание: для сетевых принтеров ОС Windows не использует формат XPS для файлов spl, даже если установлен драйвер XPS. Для таких перехваченных spl-файлов необходимо воспользоваться другими программами или *повторно распечатать*.

Просмотр в веб-интерфейсе Сервера

Начиная с версии Сервера 4.6. для просмотра перехваченного образа можно воспользоваться дополнительным меню контента (иконка в виде гаечного ключа в верхнем правом углу при наведении на ячейку с контентом), выбрав пункт «Экспорт в PDF».



Если архив в Событии печати содержит spl-файл в формате XPS или PSL, то в новой вкладе браузера откроется PDF-файл содержащий точную копию образа распечатанного документа. В случае отсутствия архива или spl-файла, или если архив содержит файл не в поддерживаемом формате, в нём будет выведена страница, описывающая данную проблему и рекомендации по её устранению.

Просмотр в программе «Средство просмотра XPS»

Для этого необходимо скачать архив включённый в событие печати, разархивировать из него файл с расширением spl и открыть этот файл в программе «Средство просмотра XPS».

Чтобы это было проще сделать, можно после разархивирования изменить расширение spl на расширение xps. Если «Средство просмотра XPS» (XPS Viewer) не установлено в вашей системе, то есть несколько вариантов решения:

- Откройте командную строку от имени администратора и выполните в ней команду установки «Средство просмотра XPS»:

```
dism /Online /Add-Capability /CapabilityName:XPS.Viewer~~~~0.0.1.0
```

- Программа «Средство просмотра XPS» входит в состав ОС Windows 8.1 и ОС Windows 7 .
- Microsoft рекомендует установить .NET Framework 3.0 или выше, в состав которого входит эта утилита.
- Можно воспользоваться бесплатной программой STDU Viewer, которая совместима с Microsoft Windows 2000/XP/2003/Vista/7/10.

Принтеры с не XPS-драйверами

К сожалению, для просмотра всех остальных форматов образов, наша компания не может предложить универсального средства, но вот несколько ссылок на бесплатные программы:

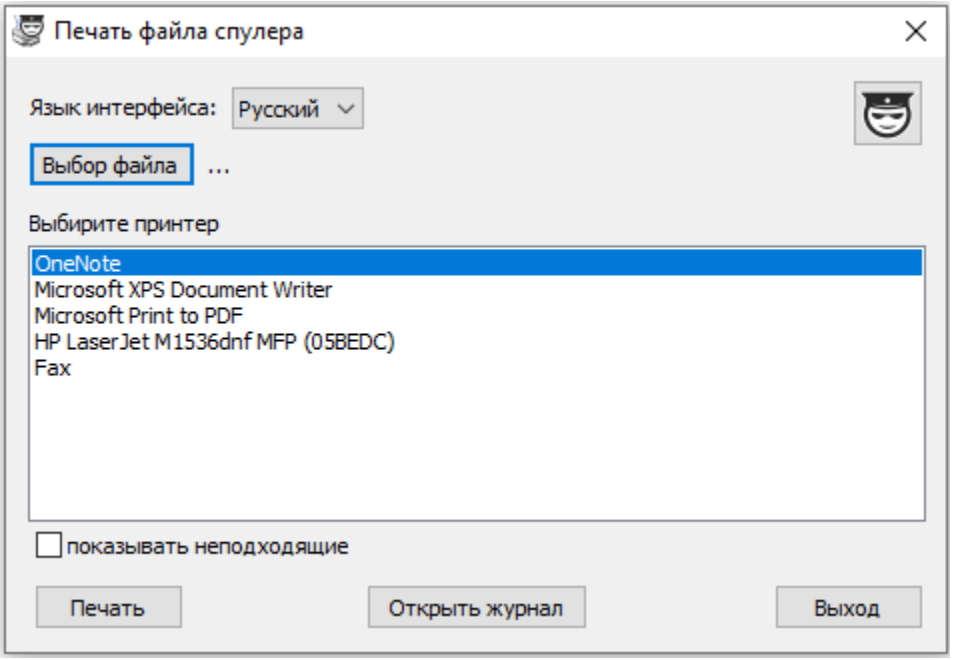
- O&K Printer Viewer
- SPLViewer
- Ghostscript, GhostPCL, GhostXPS and GhostPDL

Повторная печать документа при помощи файла спулера

В случае, если вы попытались просмотреть распечатанный документ в веб-интерфейсе и получили ошибку:

Преобразование перехваченного образа в pdf невозможно, т.к. для принтера используется драйвер не поддерживающий формат XPS или PCL.

Скачайте архив с файлами спулера и утилиту для печати документов reprint.exe, ссылка на программу будет доступна в открывшейся странице браузера.



Выберите архив спулера кнопкой «Выбор файла» или перенесите его мышкой в окно программы.

Программа предложит вам распечатать документ на принтере, который имеет аналогичный оригинальному принтеру драйвер. Также вы можете скачать лог, в котором отображается информация о файлах спулера и предполагаемых драйверах. Основываясь на этой информации вы можете поставить галочку «Показывать неподходящие» и выбрать принтер, который имеет подходящий, на ваш взгляд, драйвер печати.

Предупреждение: Печать на неподходящих принтерах может привести к невозможности печати, расходу бумаги и даже поломке принтера. Будьте аккуратны, если вы планируете запустить печать на неподходящем принтере.

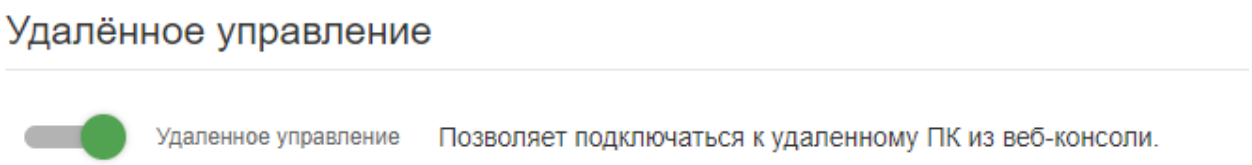
Известные проблемы

Предупреждение: Если на компьютере отключена служба «Диспетчер печати», то перехват печати работать не будет, а в логе появятся ошибки EnumPrinters() failed, error: [1722, Сервер RPC недоступен]. Для решения этой проблемы включите службу «Диспетчер печати» и перезапустите агента.

Примечание: Принтеры, которые раздаются по сети с других компьютеров, используют спулер только на том компьютере, к которому подключены непосредственно. Поэтому, перехватить содержимое печати на ПК, которые отправляют документ на печать на такой сетевой принтер не получится. Если раздающий компьютер имеет операционную систему Windows, то надо установить на него Агента, включить перехват печати и настроить свойства принтеров автоматически через Агента или вручную.

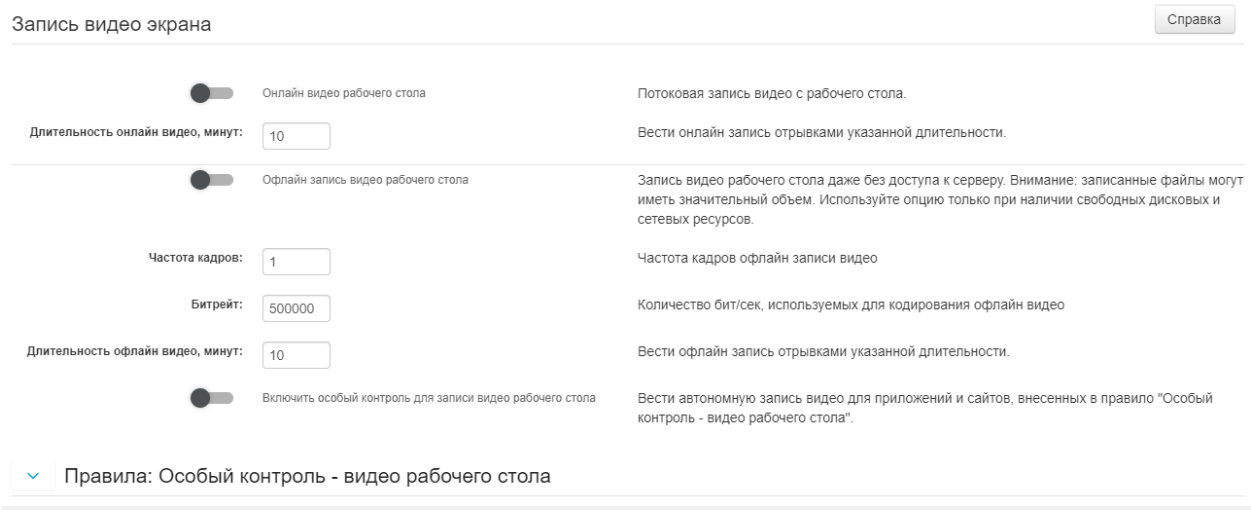
Примечание: Операционная система Windows может ограничивать количество копий в заданиях печати числом 9999. Некоторые драйверы принтеров не предполагают использование копий, например принтер «Microsoft XPS Document Writer», для таких принтеров количество копий всегда будет равно 1. Также вам следует учитывать тот факт, что общее число страниц в событии печати при превышении примерно 32 миллионов преобразуется в число 1, так как такое количество для одного документа расценивается как сбой.

4.1.15 Удалённое управление



- **Удаленное управление** - модуль, позволяющий администратору удаленно подключаться к агенту.

4.1.16 Запись видео экрана



Записывает видео рабочего стола можно в онлайн- и офлайн-режимах работы.

Опции для записи видео рабочего стола онлайн

Онлайн-режим требует постоянной связи агента с сервером, но менее требователен к ресурсам рабочей станции.
Запись делает сервер через удаленное подключение.

tabularytabulary

Опция
Видео рабочего стола
Длительность видео

Примечание: При онлайн-записи двух и более экранов с разными разрешениями качество видео может быть снижено.

Длительность записанного видео

При записи видео рабочего стола в **онлайн-режиме** сохраняются только кадры, на которых происходят изменения на экране — например, когда пользователь двигает мышкой или набирает текст. Кадры без изменений не записываются. Таким образом уменьшается размер видеофайла для экономии места на сервере.

Отключение пропуска кадров рекомендуется в случаях, когда нужна точная синхронизация таймлайна с событиями, корректное отображение периодов бездействия или стабильное воспроизведение всей записи.

Чтобы отключить пропуск кадров:

1. Откройте конфигурационный файл **/etc/ibatyr/config**.
2. Добавьте строку:

```
VNC_CONVERTER_SKIP_FRAMES = False
```

3. Перезапустите сервер:

```
ibatyr restart
```

После этого система будет сохранять все кадры, даже если на экране ничего не происходит. Фактическая длительность видеофайла будет соответствовать длительности сеанса, указанной в поле **Длительность видео**.

Опции для записи видео рабочего стола офлайн

В этом режиме агент записывает на жёсткий диск рабочей станции видео указанного качества и продолжительности. Передача видео на сервер происходит по мере накопленния данных, после чего данные удаляются с жесткого диска.

Примечание: Офлайн-режим подразумевает отсутствие связи с сервером iBatyr Monitor и не зависит от интернет-соединения.

Пример использования. Онлайн-запись можно включить при работах на сервере. Агент будет записывать экран рабочего стола как с интернет-соединением, так и без него. При восстановлении связи с сервером агент отправит запись на сервер.

tabularytabulary

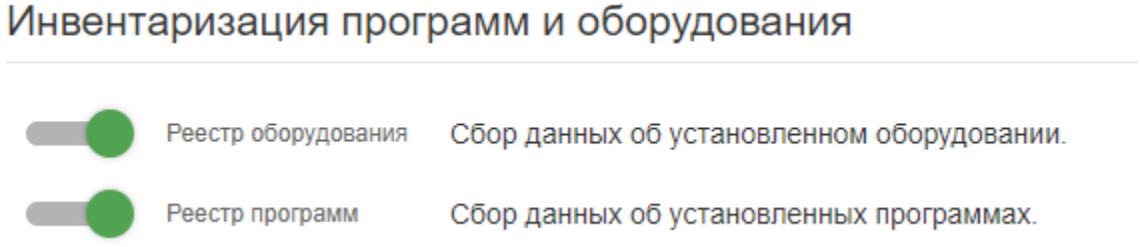
	Опция
	Офлайн-запись видео рабочего стола
	Битрейт
	Частота кадров
	Длительность офлайн видео
	Включить особый контроль для записи видео рабочего стола

В разделе **Правила: Особый контроль — видео рабочего стола** укажите приложения и сайты, для которых будет вестись запись экрана.

См.также:

Как работают чёрные и белые списки

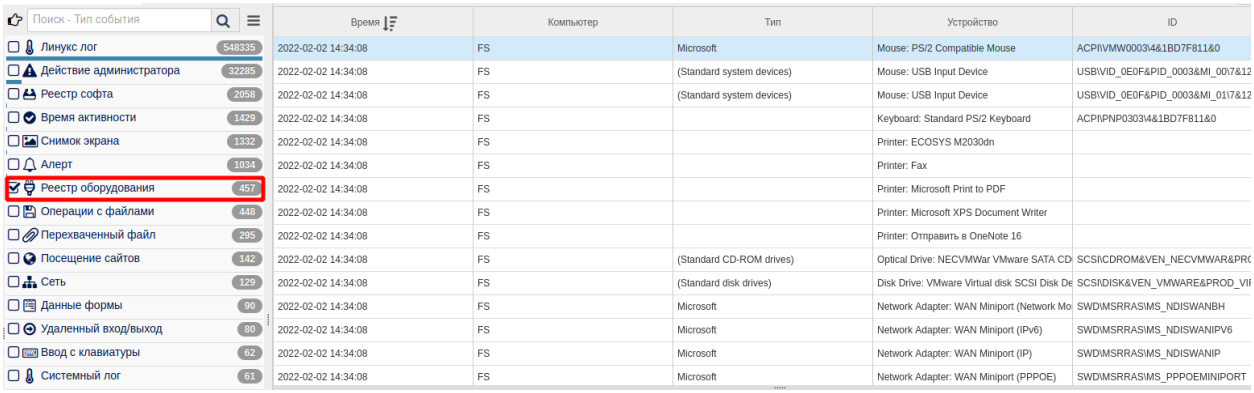
4.1.17 Инвентаризация программ и оборудования

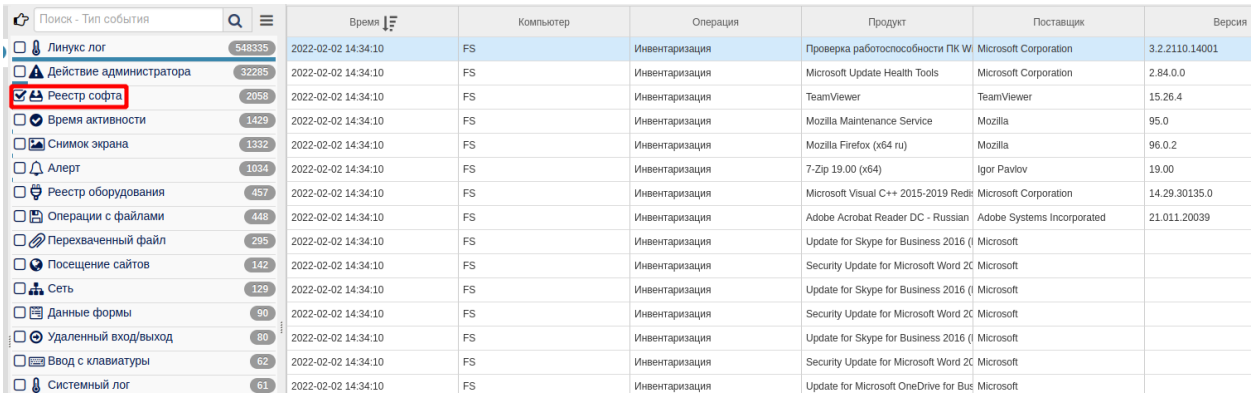


- **Реестр оборудования** — модуль, собирающий информацию по конфигурации компьютерного оборудования пользователя.

- **Реестр программ** — модуль, который собирает информацию о программном обеспечении, установленном на операционной системе пользователей.

События инвентаризации можно посмотреть выбрав в конструкторе **Реестр оборудования** или **Реестр программ**:

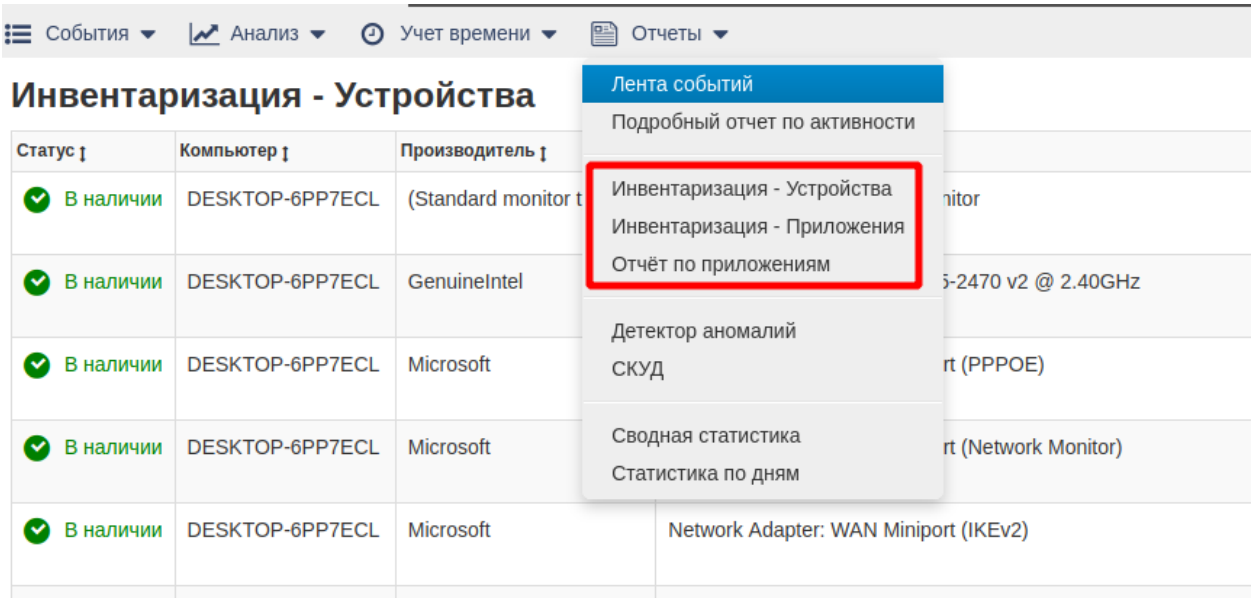




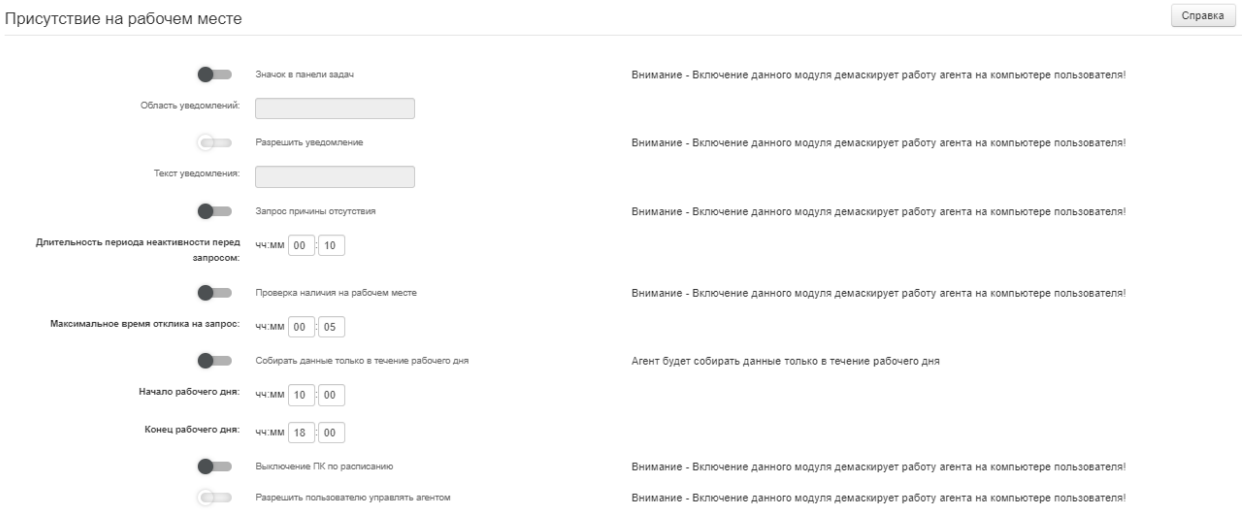
На основе полученных данных формируются три отчета:

- Инвентаризация — Устройства;
- Инвентаризация — Приложения;
- Отчет по приложениям.

Нажмите на вкладку **Отчеты**, чтобы их посмотреть:



4.1.18 Присутствие на рабочем месте



Выключение ПК по расписанию - выключает ПК пользователей во время, указанное в параметре «Конец рабочего дня». Пользователю будет предложено продолжить рабочий день с указанием причины продолжения или выключить ПК.

Значок в панели задач - модуль добавляет иконку агента в трей. Визуально отображает, что агент запущен на данном ПК.

Примечание: Данная опция не работает, если в разделе «Параметры сервера» в параметре «Видимый режим работы агента» указано «нет».

Область уведомлений - текст в заголовке окна уведомления.

Разрешить уведомление - включение или выключение окна с уведомлением.

Текст уведомления - текст в окне уведомления агента.

Запрос причины отсутствия - модуль предназначен для проверки присутствия пользователя на рабочем месте. Запускается по истечении времени неактивности, заданного в окне.

Длительность периода неактивности перед запросом - интервал времени, после которого будет выдано окно с запросом причины отсутствия активности на ПК пользователя.

Проверка наличия на рабочем месте - на рабочем столе пользователя всплывает окошко с математическим примером, который ему будет предложено решить.

Максимальное время отклика на запрос - за какой интервал времени пользователь должен отреагировать на запрос об отсутствии на рабочем месте.

Предупреждение: Включение всех выше описанных модулей демаскирует агента.

Собирать данные только в течение рабочего дня - данная опция позволяет отключать мониторинг ПК на основе заданного расписания работы сотрудников. До начала рабочего дня и после его окончания - события собираться не будут. Эта политика позволяет в автоматическом режиме решить вопрос с приватностью персональных данных на ПК в нерабочее время. Актуально включать если для работы на ПК - сотрудник использует свой личный ноутбук или персональный компьютер.

Пример работы модулей

Модуль «Запрос причины отсутствия»

При включенном модуле «Запрос причины отсутствия», если пользователь неактивен согласно времени указанному в **Длительность периода неактивности перед запросом**, то на рабочем столе пользователя всплывает окно:

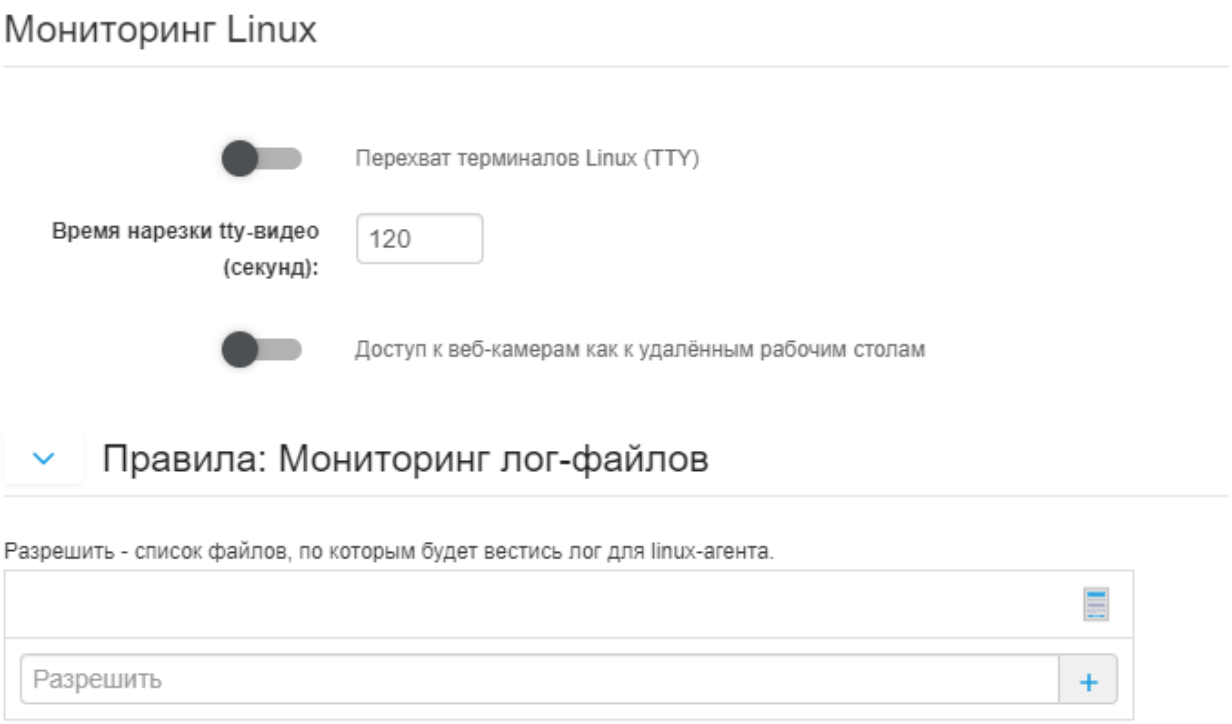
«На компьютере отсутствует активность с ЧЧ-ММ. Пожалуйста, укажите причину отсутствия» - где «ЧЧ-ММ», время последней пользовательской активности.

Пользователь в этом окошке может объяснить, почему его не было на рабочем месте. По нажатию кнопки **OK**, событие передастся на сервер, где его можно будет наблюдать в Тип событий: Контроль пользователей. Если пользователь ничего не напишет, а просто нажмет **OK** или закроет окошко, на сервер передастся событие без текста, но с указанием длительности неактивности пользователя.

Модуль «Проверка наличия на рабочем месте»

Если пользователь неактивен согласно времени указанному в **Длительность периода неактивности перед запросом**, то на рабочем столе пользователя всплывает окошко с математическим примером, который ему будет предложено решить. При вводе пользователем правильного ответа окно закрывается, и на сервер уходит событие вида **ДА**, в случае неправильного ответа окно закрывается, и на сервер уходит событие типа **ОШИБКА**. Если пользователь не ввел никаких данных, по истечении интервала, указанного в поле **Максимальное время отклика на запрос**, то окно исчезнет и на сервер передастся событие типа **НЕТ**.

4.1.19 Мониторинг Linux



Перехват терминалов Linux (TTY) – включает перехват терминалов, используемых в Linux в формате gif.

Время нарезки tty-видео (секунд) – возможность задать длительность нарезки записанного видео.

Правила: Мониторинг лог-файлов

В этом разделе указываются полные пути до файлов, которые нужно контролировать постоянно. Например:

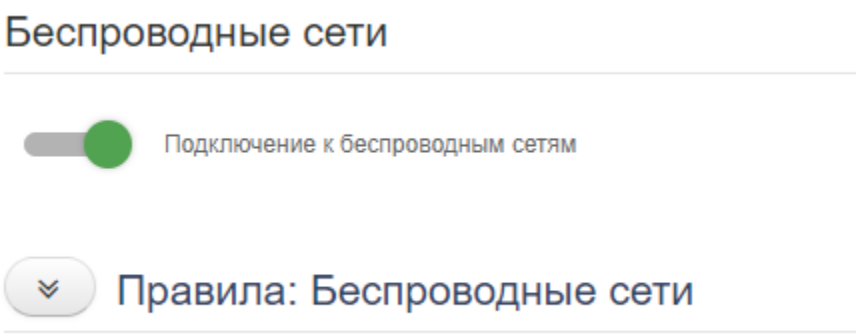
- **/var/log/syslog**
- **/var/log/auth.log**
- **/var/log/ibatyr/ibatyr.log**

Примечание: Если в Правиле не указаны файлы, то отслеживается **/usr/share/ibatyr/syslog.txt**. Чтобы исключить его из мониторинга, укажите путь к файлу, который необходимо отслеживать.

Чтобы полностью выключить мониторинг файлов при включенном модуле, укажите путь к несуществующему файлу.

События от изменений указанных файлов будут построчно передаваться на сервер и отображаться в типе события *Терминал linux* .

4.1.20 Беспроводные сети



- **Подключение к беспроводным сетям -** модуль для контроля подключений и к беспроводным сетям.

Правила: Беспроводные сети

Блокировать - блокировка подключений ко всем наименованиям сетей, указанных в списке.

Разрешить - блокировка всех подключений за исключением тех, что указаны в данном списке.

4.1.21 Метки и блокировка доступа

Модуль **Метки и блокировка доступа** позволяет блокировать доступ к файлам по заданным параметрам.

> **Внимание:** Не включайте этот модуль, если не собираетесь блокировать файлы по содержимому.
>
> Включение модуля может привести к замедлению работы с файлами на рабочих станциях.

Для файлов, указанных в разделе **Файлы** → **Правила: Файловый мониторинг** → **Пути и маски** и **Правила: Файловый мониторинг** → **Пути и маски** → **Чтение**, не будут отображаться уведомления о блокировке.

См.также:

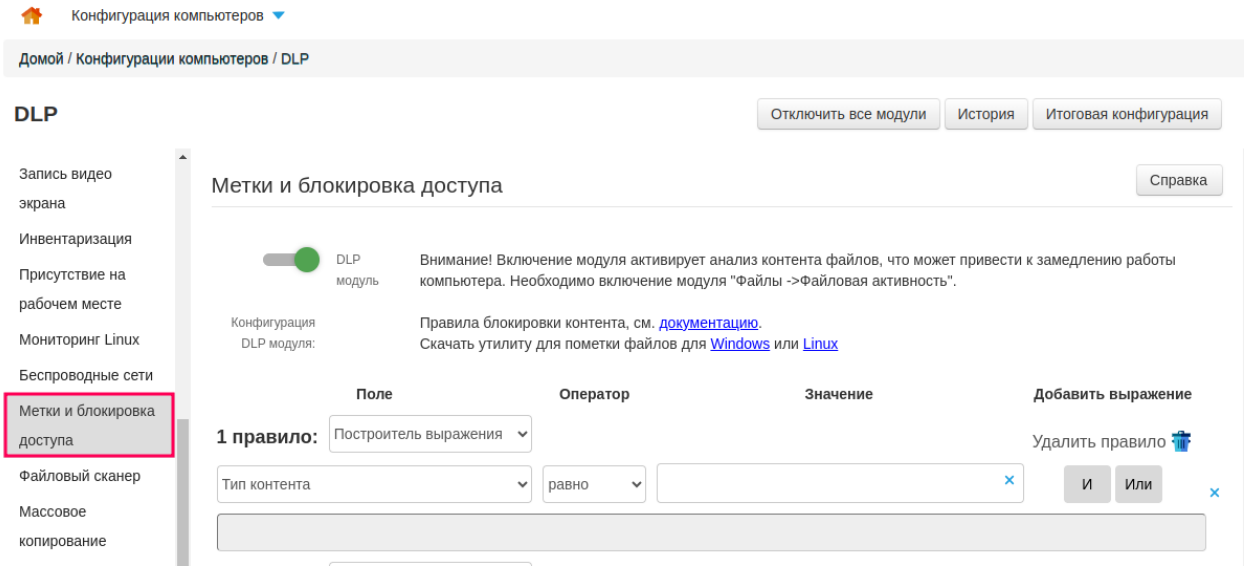
Метки также можно настроить *в Краулере*.

Настройка конфигурации модуля

Создание и настройка правил блокировки доступа происходит в основном веб-интерфейсе iBatyr Monitor.

Перейдите **Панель управления** → **Конфигурации компьютеров**, найдите в списке **DLP** и поставьте галочку.

Нажмите на **DLP** и выберите в боковом меню **Метки и блокировки доступа**.



Чтобы создать правило:

1. В строке **Поле** выберите атрибут правила — признак, по которому правило будет работать.

   Примечание: В конфигурации Linux-агента блокировка устройств типов Hard, USB, CD, Network, Removable возможна только по одному признаку — **Диск-источник**. Такое поведение определяется архитектурными особенностями операционной системы Linux.

   Доступные атрибуты:

Атрибут	Описание
Имя компьютера	Запрет для определенного устройства.
Имя пользователя	Запрет для определенного пользователя.
Домен пользователя	Запрет для пользователей домена.
Имя приложения	Запрет на действия с файлом в приложении.
Имя файла	Ограничения на действия с файлом по названию. Если имя изменится, доступ будет открыт. Для **Windows-агента** имя файла должно быть указано с расширением: *your-file.pdf*, иначе правило не сработает. Это связано с тем, что в Windows имя файла включает и основную часть, и расширение. Чтобы правило сработало без указания расширения, используйте оператор **содержит**.
Путь файла	Ограничения для файлов, расположенным по указанному пути. Даже при изменении имени доступ будет ограничен.
Расширение файла	Ограничение операций по расширению файла: .docx, .xls и т. д. Если пользователь изменит расширение, доступ будет открыт.
Тип контента	Ограничение доступа к определенному формату контента. Сохраняется даже при изменении расширения файла.
Признак наличия метки	Блокировка по любой *метке* файла.
Значение метки	Блокировка по *метке* с определенным значением.
Контент	Блокировка по содержанию.
Тип файловой операции	Запрет на все или отдельные операции с файлом.
Диск-Источник	Запрет переноса файлов с источника на съемный носитель.
Диск-Приёмник	Запрет переноса файлов с носителя.

2. В строке **Оператор** выберите логический оператор.

   Доступные логические операторы:

   tabularytabulary

Оператор	Сокращение	
не равно	!	
равно	==	
совпадает		Регул
содержится		Нах
не содержится		От
или	or	
и	and	

3. В поле **Значение** укажите значение выбранного атрибута (имя файла, имя компьютера. . .). Все значения регистронезависимы.

   Особенности атрибутов:

   - для атрибута **Тип контента** расширение файла определяется на основе его содержимого и может отличаться от указанного в пути;
   - по атрибуту **Контент** можно блокировать только файлы MS Office и *.txt*;
   - при создании правил с атрибутом **Контент** используйте логический оператор *совпадает*.

Особенности работы модуля

Неверная настройка правил блокировки может нарушить работу некоторых приложений.

Например, блокировка zip-архивов можно нарушить работу *MS Excel*, поскольку кэш *Excel* хранится в формате zip-архива. Чтобы этого избежать, правила блокировки zip-архивов должны быть следующими:

- mime == «application/zip» and not exe_name matches «(7zfm.exe|excel.exe)»
- mime == «application/zip» and exe_name != «7zfm.exe» or exe_name != «excel.exe»

Больше примеров работы модуля блокировки приведено в *отдельной статье*.

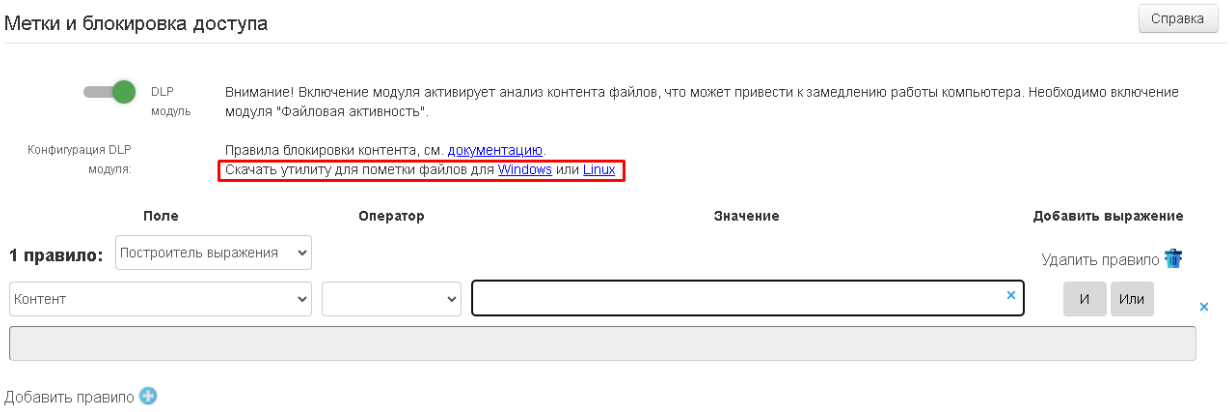
Цифровые метки

Помимо правил блокировки, модуль поддерживает работу с цифровыми метками файлов. Такие метки позволяют отслеживать файлы даже при изменении их имени или содержимого.

Модуль **Метки и блокировка доступа** поддерживает работу с файлами в формате:

- Microsoft Office Word Document (.docx)
- Microsoft Office Excel Workbook (.xlsx)
- Microsoft Office PowerPoint Presentation (.pptx)
- Open Office Text Documen (.odt)
- Open Office Spreadsheet (.ods)
- Open Office Presentation (.odp)

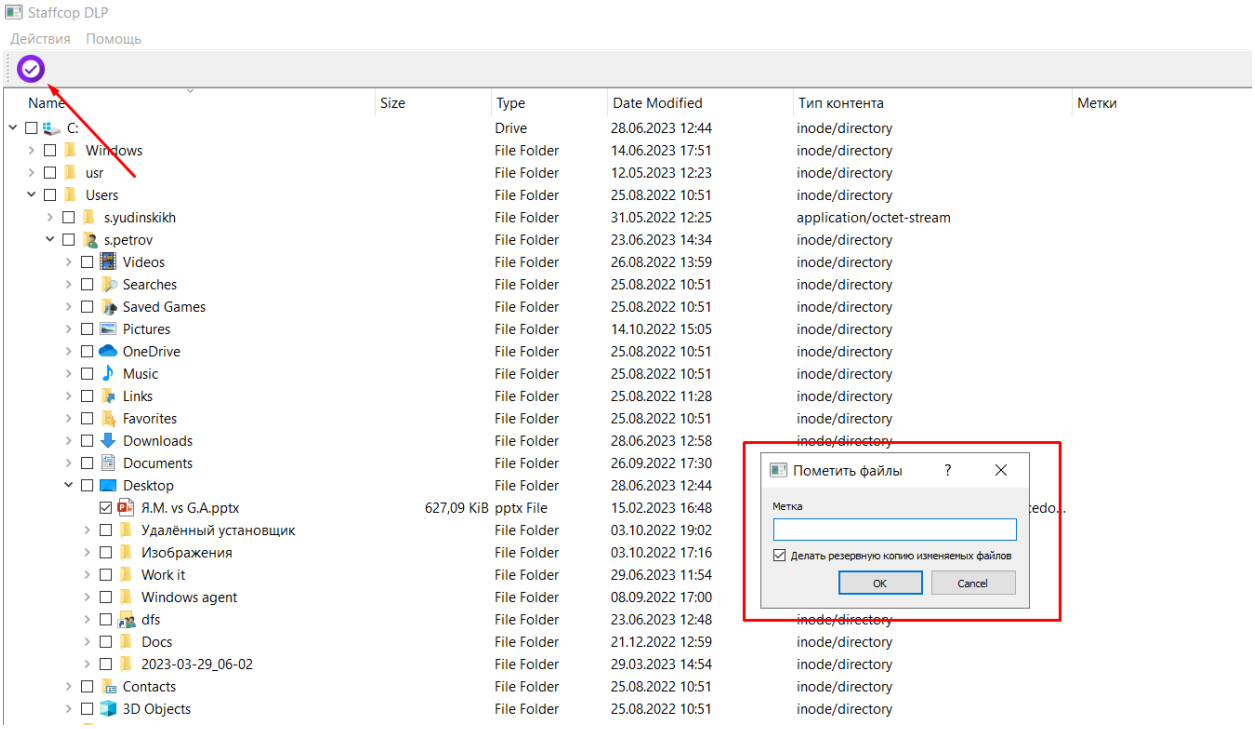
Поставить цифровую метку можно при помощи утилиты **tagger** для Windows и Linux. Скачать утилиту можно в окне модуля.



Утилита для Windows

Чтобы поставить цифровую метку на файл:

1. Скачайте и установите утилиту **tagger** в **Метки и блокировка доступа** → **Конфигурация DLP модуля**.
2. После завершения установки запустите программу от имени администратора.
3. Выберите необходимые файлы и нажмите значок **Пометить файлы**.
4. В открывшемся окне создания метки, введите текст метки.



5. Готово! Цифровая метка поставлена.

Теперь можно настраивать *отслеживание перемещений этих файлов внутри периметра безопасности*.

Утилита для Linux

Чтобы поставить цифровую метку на файл:

1. Скачайте утилиту **tagger** в **Метки и блокировка доступа** → **Конфигурация DLP модуля**.
2. Сделайте файл скрипта исполняемым:

```
chmod +x /path/to/tagger
```

   Здесь **/path/to/** — полный путь до скачанного скрипта.

3. Установите метку на выбранный файл:

```
./tagger tag -v mark_name path/to/file_name
```

Здесь **mark_name** — текст метки; **path/to/file_name** — путь к файлу, который необходимо пометить (в том числе — сетевой путь).

4. Готово! Цифровая метка поставлена. Теперь можно настраивать *отслеживание перемещений этих файлов внутри периметра безопасности*.

Список команд и флагов утилиты **tagger**:

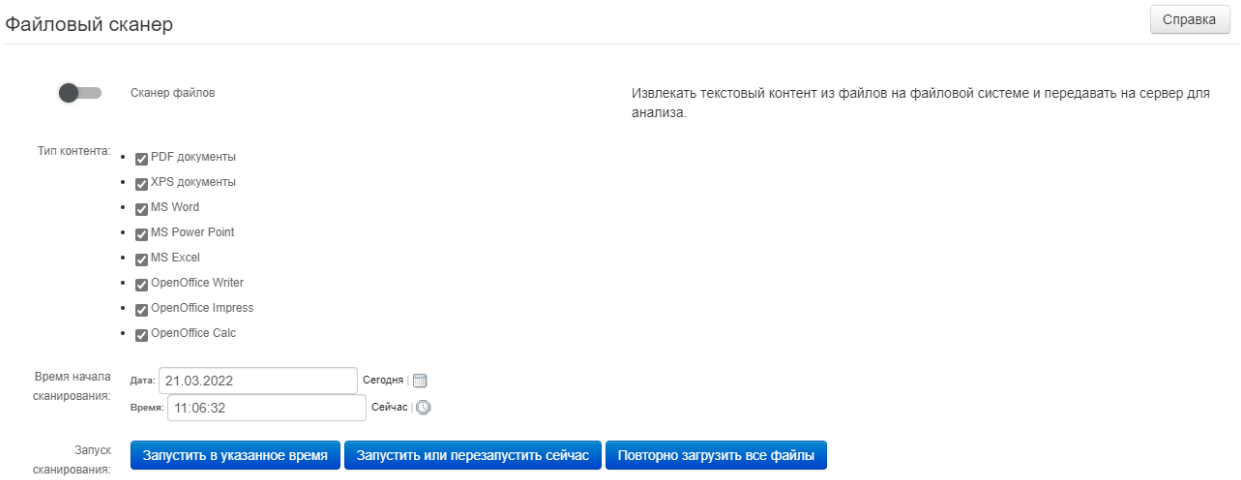
tabularytabulary

Команда / флаг
-H
-V
help
info
rule
simularity
tag

4.1.22 Файловый сканер

Файловый сканер — модуль для поиска контента определенного типа на ПК с установленным агентом. Типы контента представлены в разделе **Конфигурация компьютеров** → **Файловый сканер**.

Внимание: **Файловый сканер** недоступен в конфигурации компьютеров, если активирован *Краулер*.



Примечание: Включение модуля может привести к замедлению работы с файлами на рабочих станциях. Проводите сканирование файлов в нерабочее время.

Для запуска сканирования выберите одну из опций:

- **Запустить в указанное время** — запустить сканирование по расписанию. Время запуска сканирования указывается в поле **Время начала сканирования**.

  Важно: Если вы присвоили агенту конфигурацию с активным **Файловым сканером**, а время

сканирования уже прошло, сканирование начнется сразу после присвоения конфигурации.

- **Запустить или перезапустить сейчас** — запустить или перезапустить сканирование сразу после получения агентом конфигурации.
- **Повторно загрузить все файлы** — заново выполнить полное сканирование.

Отсканированные файлы доступны в событиях *Файл*.

Правила: Файловый сканер — Пути и маски

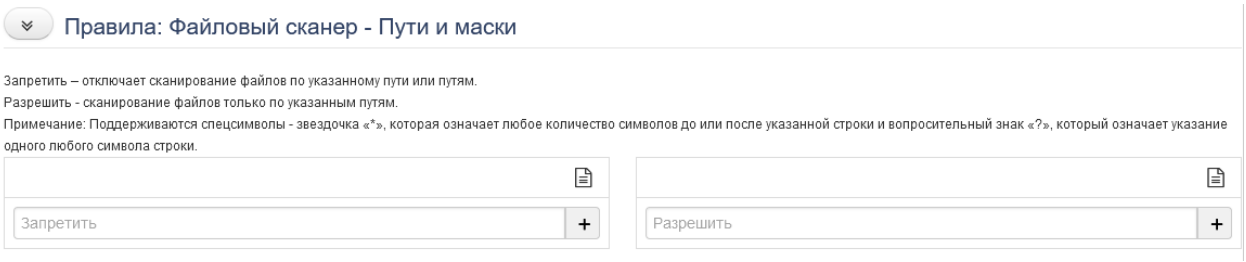
Позволяет добавлять исключения для оптимизации поиска.

Файлы или пути, указанные в строке **Запретить**, не будут сканироваться.

Если указать файлы или пути в строке **Разрешить**, то поиск будет проводиться только по ним.

Примечание: При указании путей и масок поддерживаются спецсимволы:

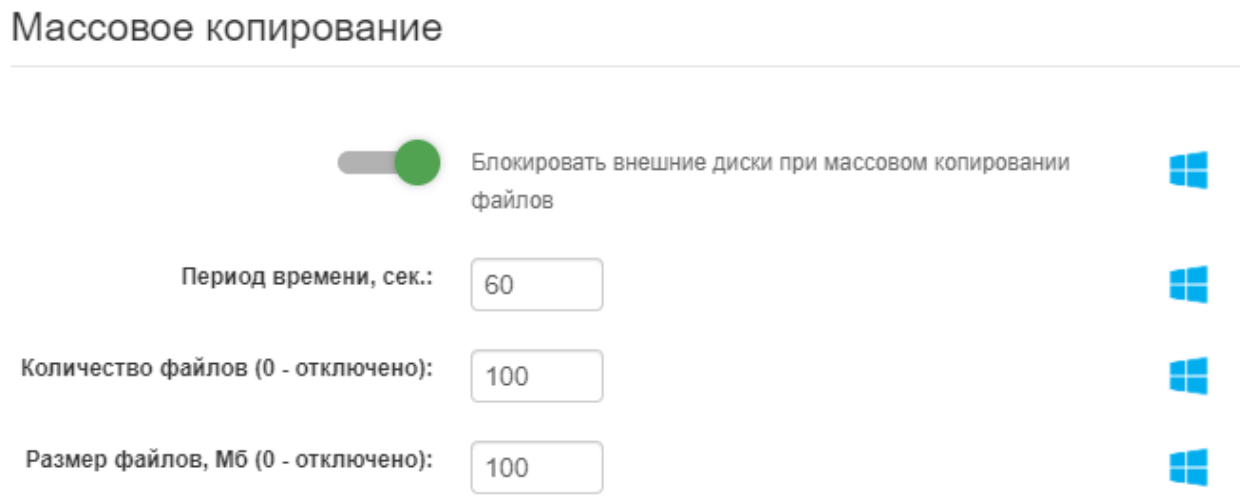
- «*» — любое количество символов до или после указанной строки;
- «?» — один любой символ строки.



4.1.23 Массовое копирование

Раздел конфигурации **Массовое копирование** позволяет настроить блокировку доступа ко всем съемным устройствам (Removable Devices) при копировании определенного объема и количества файлов.

Примечание: Функциональность доступна только для Windows-агента.

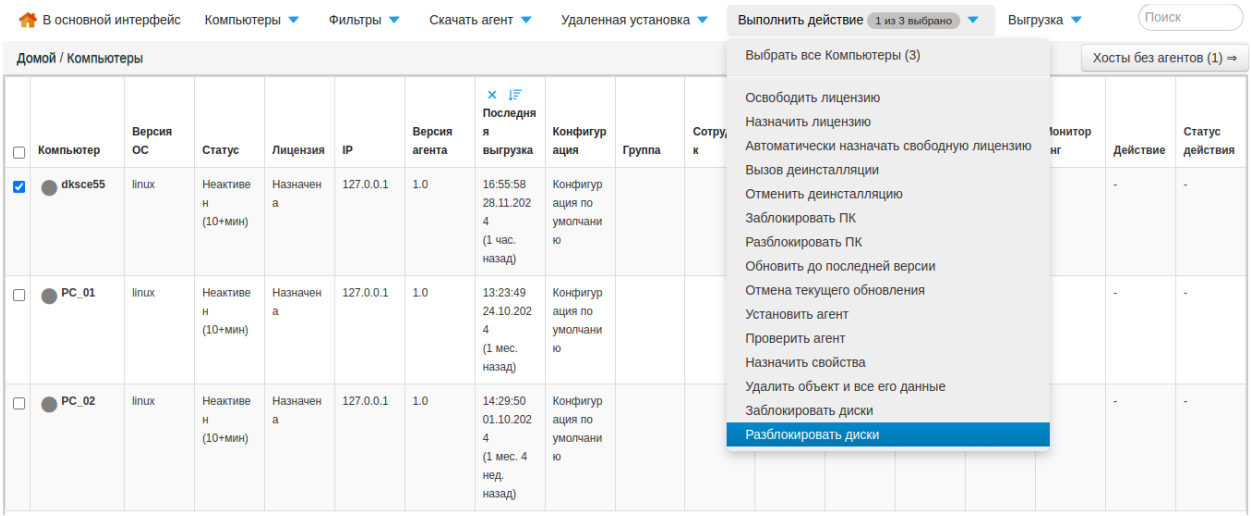


- **Блокировать внешние диски при массовом копировании файлов** — включить или отключить блокировку внешних дисков при массовом копировании файлов.

Примечание: Для работы опции включите в конфигурации *Файлы* → *Файловая активность* и *Устройства* → *USB устройства*.

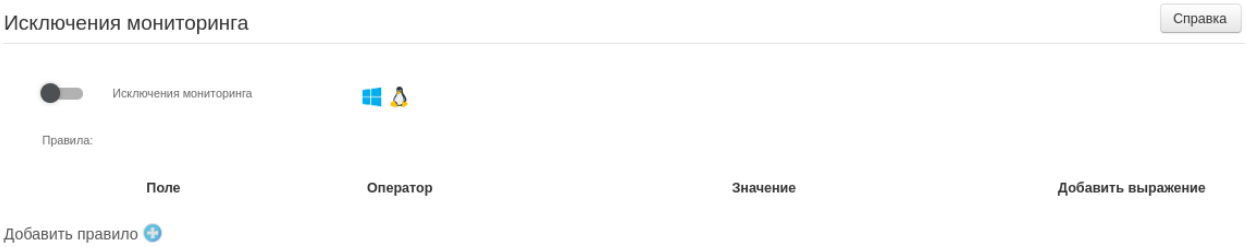
- **Период времени** — если за указанный в секундах промежуток пользователь скопирует файлы, и их количество и размер достигнут указанных в настройках значений, USB-устройство будет заблокировано.
- **Количество файлов** — число файлов, при копировании которых произойдет блокировка USB-устройства.
- **Размер файлов** — общий объем файлов в мегабайтах, при копировании которых устройство будет заблокировано.

Для разблокировки устройств на компьютере перейдите в **Панель управления** → **Компьютеры**. Далее выберите компьютер и нажмите **Выполнить действия** → **Разблокировать диски**.



4.1.24 Исключения мониторинга

Раздел конфигурации **Исключения мониторинга** позволяет исключать из мониторинга определённые события, происходящие на подконтрольных машинах.



Исключения мониторинга доступны для Windows- и Linux-агентов.

Windows-агент позволяет исключить события:

- **Перехваченные файлы**;
- **Снимки экрана**;
- **Пакеты снимков экрана**;
- **Видеозапись**;
- **Буфер обмена** — исключает перехват содержимого буфера по измерениям:
  - Имя пользователя,
  - Домен пользователя,
  - Имя компьютера,
  - Имя приложения,
  - Описание приложения.

Linux-агент позволяет исключить события:

- **Перехваченные файлы** — отключает перехват файлов с флешки или в локальной сети. Недоступно для теневых копий отправленных в облака файлов, вложений почты и мессенджеров.
- **Снимки экрана**.

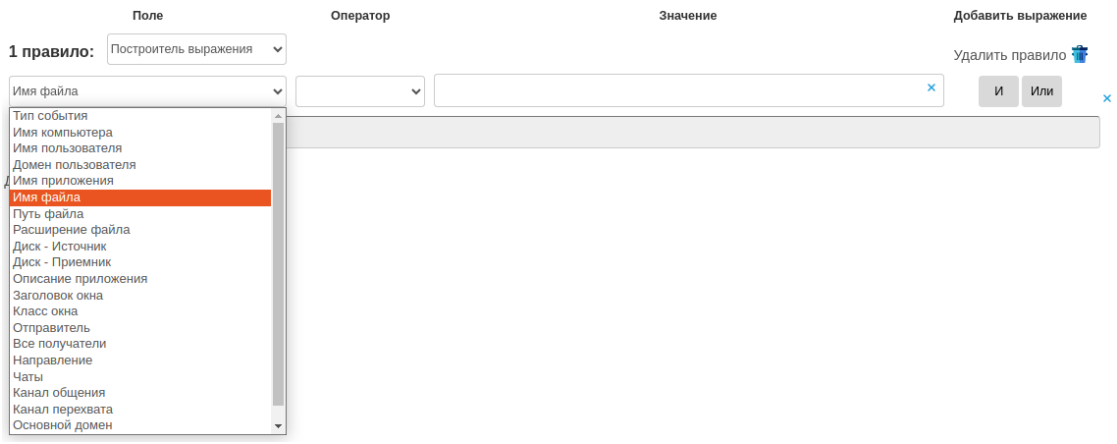
Исключение события из мониторинга

Активируйте исключения мониторинга:

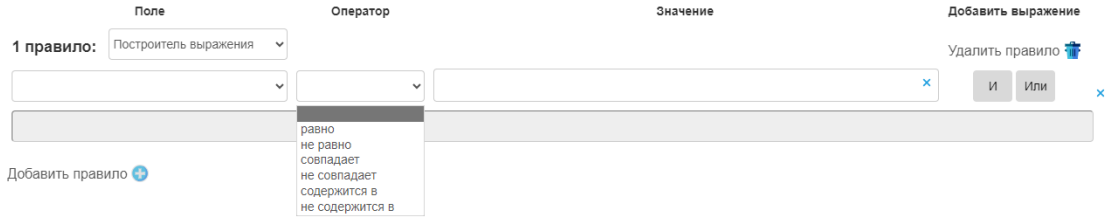
1. В веб-интерфейсе сервера iBatyr Monitor перейдите в раздел **Панель управления** → **Конфигурации компьютеров**.
2. Выберите конфигурацию.
3. Перейдите в раздел **Исключения мониторинга**.
4. Активируйте опцию **Исключения мониторинга**.
5. Перейдите к созданию правила для исключения событий.

Создайте правило исключения событий:

1. Нажмите **Добавить правило**.
2. Выберите значение в столбце **Поле**.



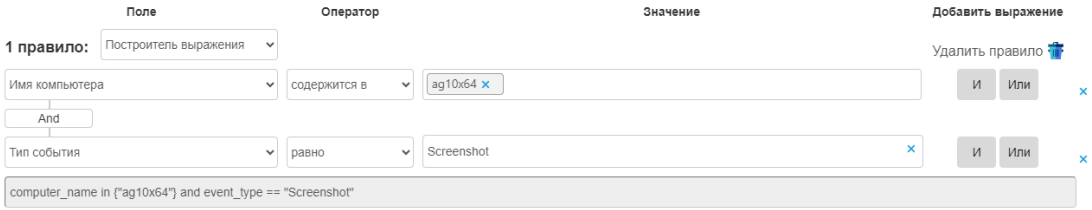
3. Выберите **Логический оператор** и укажите **Значение**.



4. При необходимости добавьте условие с помощью оператора **И** / **ИЛИ**.
5. Сохраните правило.
6. Готово!

Пример

Правило для запрета мониторинга скриншотов на компьютере *ag10x64*:



Настройка исключений для перехваченных файлов

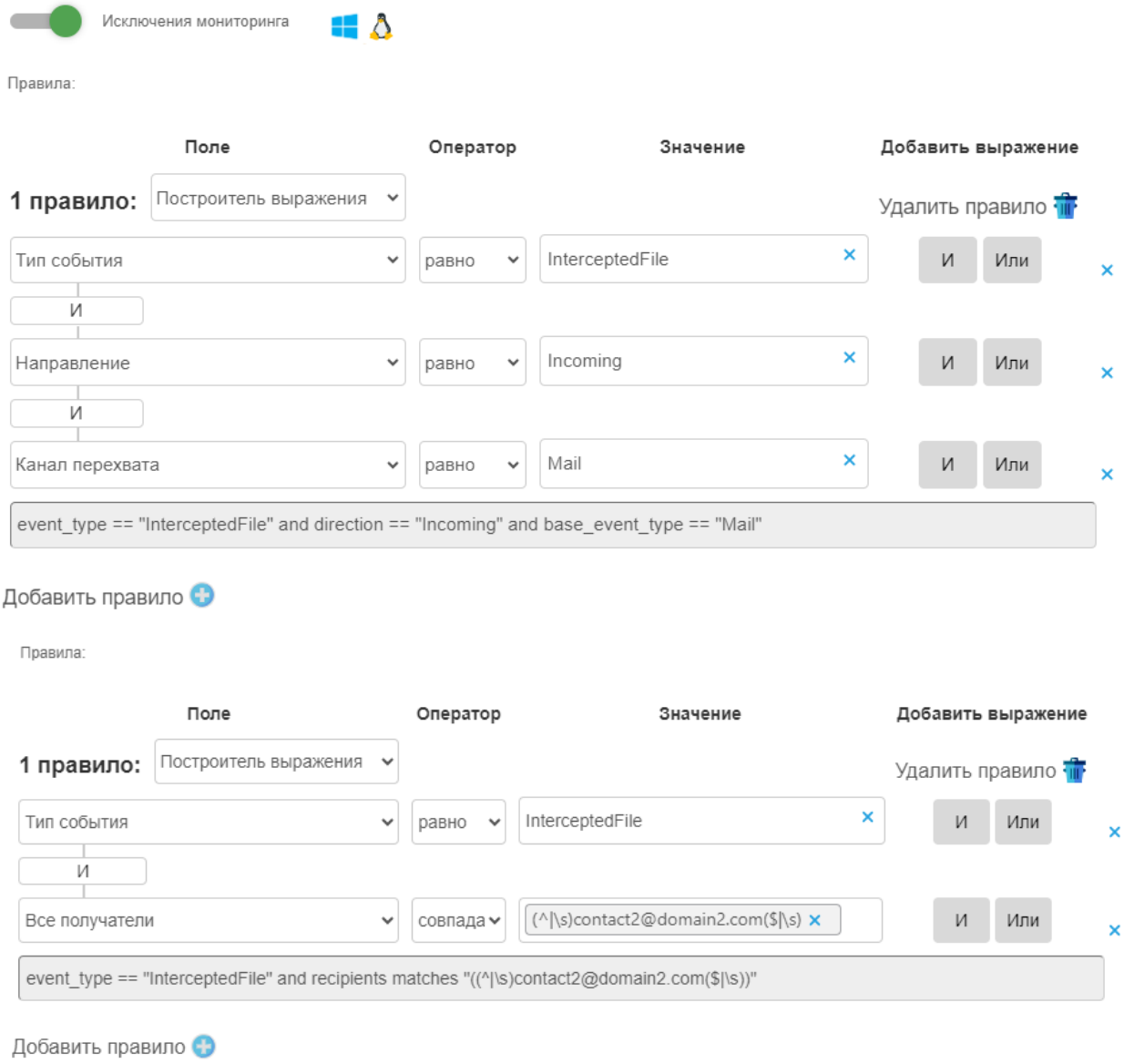
Если во время переписки агенты собирают чрезмерное количество вложенных файлов, исключите перехват файлов с помощью правил **Исключения мониторинга**.

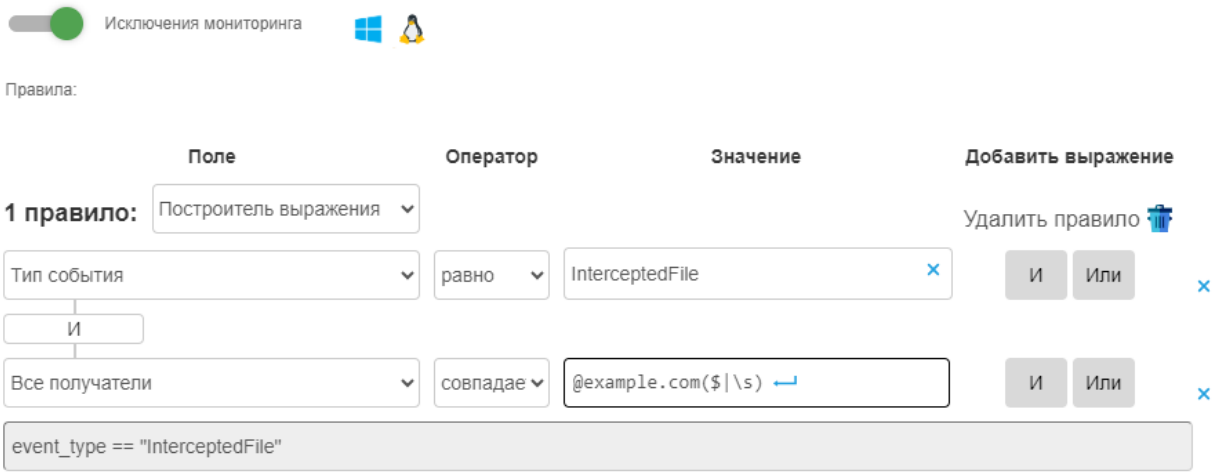
Вы можете выбрать, через какие каналы система не будет перехватывать файлы:

- веб-почта;
- мессенджеры;
- почта по протоколам: IMAP, POP3, SMTP;
- черновики почтовых сообщений;

- теневые копии файлов, *загруженные или выгруженные в облачное хранилище*;
- отправленные на печать документы;
- данные форм.

Примеры правил исключения





Примечание: Для исключения конкретных пользователей или домена для измерений **Все получатели** и **Чаты** используйте оператор **совпадает** с использованием *регулярного выражения*. Для удобства работы с регулярными выражениями измените режим **Построитель выражения** на **Редактировать выражение**.

Настройка исключений для Видео рабочего стола и Пакетов снимков экрана

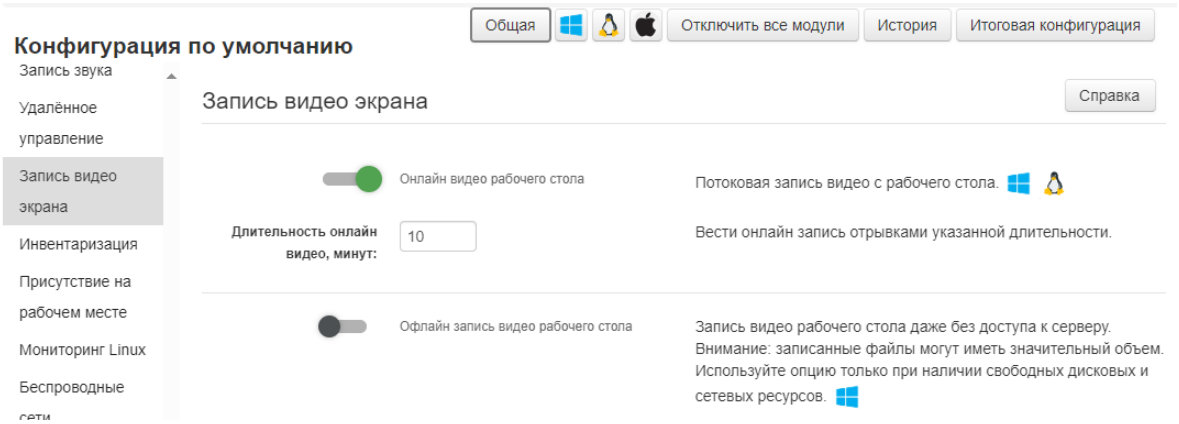
Предупреждение: Исключения мониторинга для событий **Видео рабочего стола** и **Пакеты снимков экрана** влияют на работу других модулей и требует дополнительной настройки.

Онлайн-видео рабочего стола

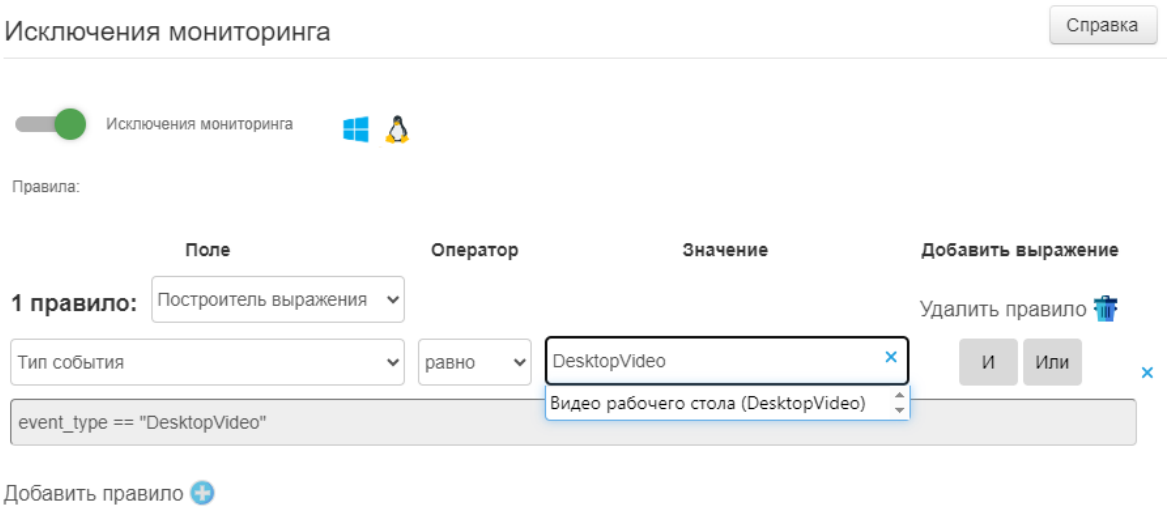
Онлайн-видео рабочего стола и **Удаленное управление** используют один и тот же модуль.

Удаленное управление прервется, если в текущей конфигурации:

- в разделе **Запись видео экрана** включена опция **Онлайн-видео рабочего стола**:



- в **Исключении мониторинга** настроено правило **Тип события — равно — Видео рабочего стола**:



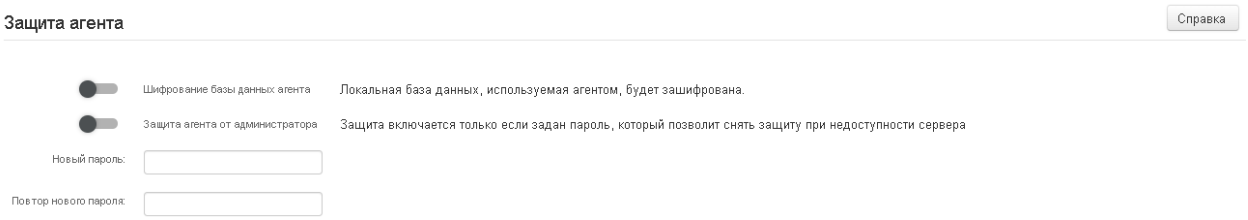
Примечание: Исключения мониторинга для событий **Офлайн-записи видео рабочего стола** и **Пакетов снимков экрана** на **Удаленное подключение** не влияют.

Офлайн-запись видео рабочего стола и Пакеты снимков экрана

Для исключения записи офлайн-видео и пакетов снимков экрана по измерениям **Имя приложения** и **Заголовок окна** используйте операторы **равно**, **содержит** и **совпадает**.

Предупреждение: Операторы **не равно**, **не содержит** и **не соответствует** для измерений **Имя приложения** и **Заголовок окна** могут привести к полному отключению записи видео и пакетов снимков экрана, если начало записи выпадает на приложение или окно вне указанного списка.

4.1.25 Защита агента



Шифрование базы данных агента включает шифрование локальной базы данных, собираемой на стороне агента.

Защита агента от администратора позволяет установить пароль для защиты от удаления исполняемых файлов и процессов iBatyr Monitor, а также связанных веток реестра. В этом случае удалить агент с компьютера будет нельзя, даже если пользователь имеет права администратора.

Защита от удаления будет включена только если задан пароль - этот пароль позволит снять защиту локально при недоступности сервера.

При включенной опции **Защита агента от администратора**, нельзя удалить, переустановить или обновить агент. Для удаления, переустановки или обновления агента, отключите защиту агента в конфигурации компьютера.

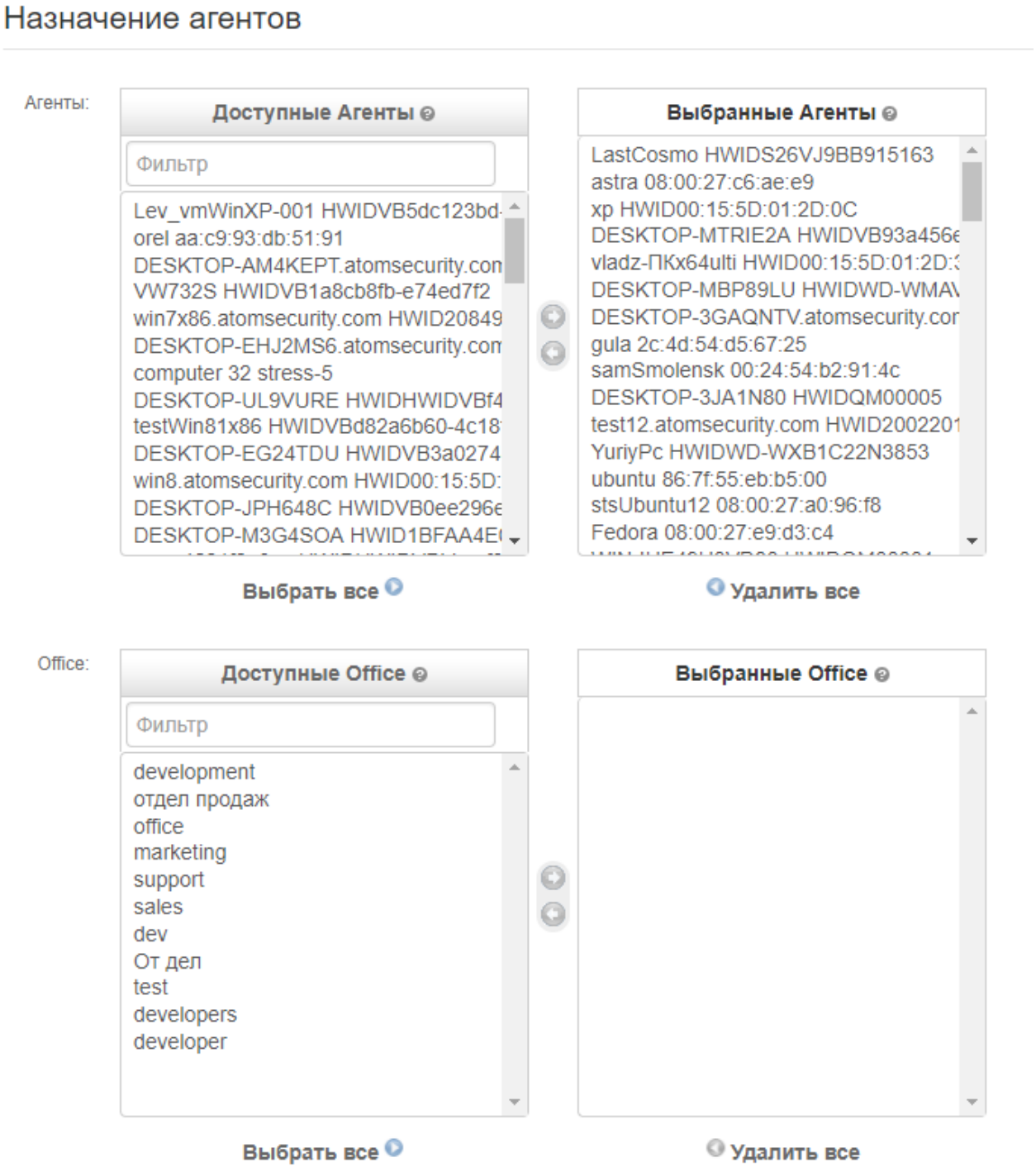
Чтобы снять защиту локально используйте команду:

```
vmnetdrv64.exe unprotect PASSWORD
```

Примечание: Из-за особенностей ввода спецсимволов в командной строке, для корректного чтения символов ^ & " ' | \ < > перед ними необходимо дополнительно указывать символ ^.

Таким образом, пароль, состоящий только из спецсимволов ~!@#$%^&*()_+{}[]:;"'|\<,>.?/`, при вводе в командной строке, должен выглядеть так: ~!@#$%^^^&*()_+{}[]:;^"^'^|^\^<,^>.?/`.

4.1.26 Назначение агентов



Интерфейс позволяет назначать или снимать конфигурацию для выбранных пользователей или отделов.

Назначение конфигурации группе из Active Directory

Примечание: Перед назначением конфигурации *подключите Active Directory*.

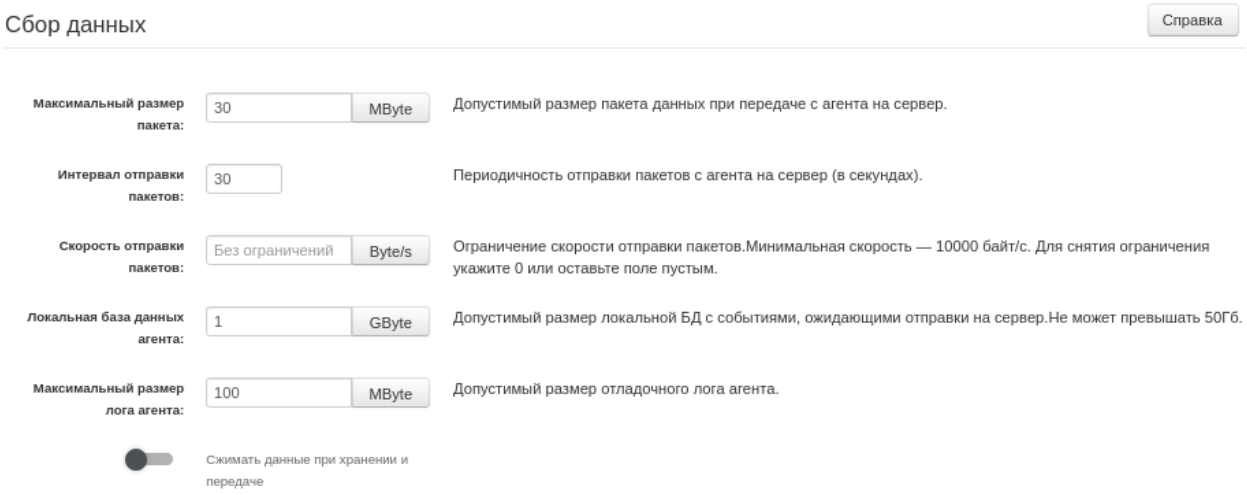
Чтобы назначить конфигурацию группе:

1. Укажите в поле **Группа AD** название группы из Active Directory.
2. Нажмите **Сохранить**.

С версии 5.4 для улучшения скорости обработки данных от агента вы можете включить механизм назначения конфигурации.
Более подробно назначение конфигурации группе AD описано *в инструкции*.

4.1.27 Сбор данных

Основные настройки отправки отчетов от агентов на сервер представлены в разделе **Сбор данных**. Изменяя параметры раздела, можно регулировать нагрузку на сеть и сервер.



Агент отсылает данные на сервер небольшими шифрованными пакетами, распределенными по времени. Это позволяет избежать лишней нагрузки на сеть.

Размер пакета и интервал отправки определяются полями **Максимальный размер пакета** и **Интервал отправки пакетов**.

Примечание: Для выбора единиц измерения используйте кнопки в конце строки.

Скорость отправки

Чтобы снизить нагрузку на канал связи агента с сервером, измените скорость передачи данных.

Для этого в поле **Скорость отправки пакетов** укажите необходимое значение. Минимальное допустимое значение скорости передачи данных — 10 Кб/с. Любое меньшее значение будет округлено до 10 Кб/с.

Чтобы снять ограничение на скорость передачи данных, оставьте поле **Скорость отправки пакетов** пустым или введите **0**.

Информацию о скорости передачи данных также можно получить, выполнив на машине с Linux-агентом команду:

```
sudo /usr/share/ibatyr/agent info
```

В выводе команды скорость передачи данных — значение параметра **rate**:

```
...
Config: every 15s report 100M rate 100K ...
```

В этой строке указаны интервал передачи данных и размер пакета данных.

Примечание: Если в выводе команды указано **rate 0b**, это значит, что ограничение на скорость передачи не задано и используется весь доступный канал.

Локальная база данных

Агенты собирают события, отправляют их на сервер и, после подтверждения сервером, очищают локальную базу данных.

См.также:

Локальная база данных агента.

Максимальный размер лога агента

При включенном *Режиме отладки* агент пишет служебный лог.

Лог отправляется на сервер при:

- рестарте компьютера;
- рестарте агента;
- обновлении конфигурации агента.

Размер отладочного лога можно ограничить в поле **Максимальный размер лога агента**.

Сжатие данных

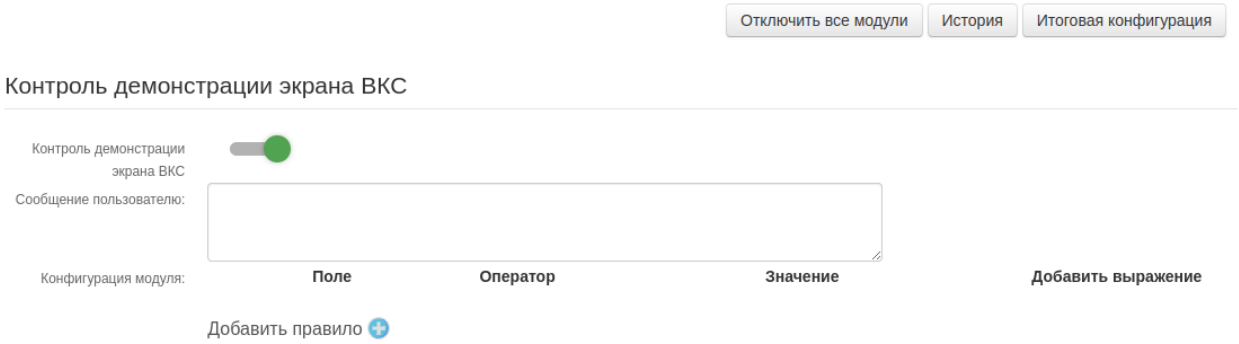
Включите опцию **Сжимать данные при хранении и передаче**, чтобы сжимать события и файлы при записи в локальную базу данных агента. Это снизит объем локальной базы данных агента и передаваемых данных на сервер.

> **Внимание:** Сжатие данных может увеличить нагрузку на аппаратные ресурсы агента.

4.1.28 Видеоконференцсвязь (ВКС)

Добавлено в версии iBatyr Monitor 5.4 для Windows-агента.

Контроль ВКС отслеживает демонстрацию экрана во время видеоконференции. При демонстрации запрещенного файла или приложения модуль прерывает демонстрацию и отправляет уведомление в iBatyr Monitor.



Реализовано для платформ:

- Контур.Толк,
- Яндекс.Телемост,
- МТС Линк,
- SberJazz (веб, десктоп),
- Zoom.

Чтобы включить контроль демонстрации:

1. Перейдите в **Панель управления** → **Конфигурации компьютеров**.
2. Выберите конфигурацию.
3. Выберите в списке **Контроль ВКС** и переключите его в положение «включено».

Правила

Время участия в ВКС

Добавлено в версии 5.5.

Функционал **Время участия в ВКС** предназначен для отслеживания времени участия пользователя в звонках по видеоконференцсвязи.

Агент отслеживает активность в сервисах видеосвязи:

- K-talk,
- Яндекс-телемост,
- МТС-линк,
- Jazz.Sber,
- Zoom.

Примечание: Поддерживается только веб-версии перечисленных сервисов.

Когда пользователь подключается к ВКС, агент создает событие **Время участия в ВКС**. События создаются длительностью до минуты. Например, при длительности конференции пять минут будет создано пять событий.

Чтобы включить отслеживание времени участия в ВКС:

1. Убедитесь, что в вашей конфигурации включен **Мониторинг сетевой активности**.
2. В **Контроле ВКС** передвиньте выключатель **Время участия в ВКС** в активное положение.

После включения агент будет отправлять на сервер событие **Время участия в ВКС**, которое содержит информацию:

- локальное время;
- длительность участия в ВКС;
- имя пользователя;
- компьютер;
- приложение — например, Zoom или K-talk;
- URL сервиса — например, https://example.ktalk.ru.

Сообщение пользователю

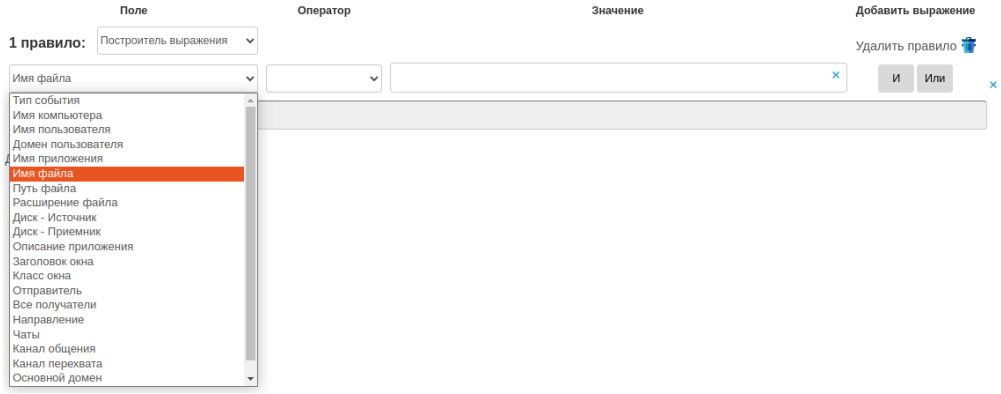
Здесь вы можете написать уведомление, которое получит пользователь при прерывании демонстрации экрана.

Максимальная длина: **200** символов.

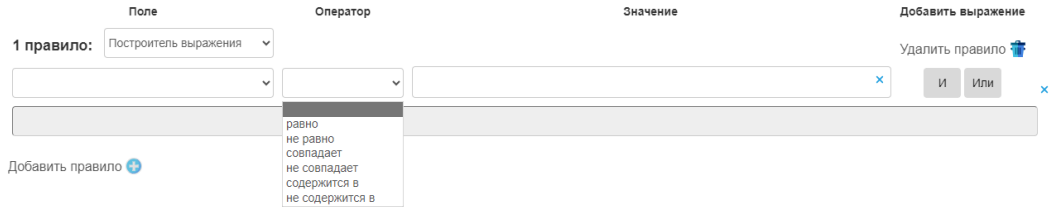
Конфигурация модуля

В этом разделе задайте условия срабатывания функции:

1. Нажмите **Добавить правило** +.
2. Выберите в **Поле** параметр, который будет включать срабатывание:



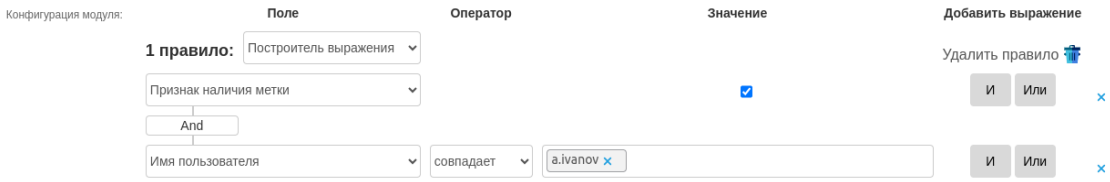
3. Выберите логический **Оператор** и укажите **Значение**:



4. При необходимости добавьте новую строку к правилу с помощью оператора **И** / **ИЛИ** или кнопки **Добавить правило** +.
5. Сохраните правило.

Пример

Блокировка демонстрации файла для пользователя по метке:



Уведомления

Во время демонстрации экрана агент каждую минуту отправляет на сервер уведомление, которое содержит информациию:

- об агенте,
- пользователе,
- времени демонстрации.

При прерывании демонстрации агент также отправляет уведомление.

Примечание: Чтобы узнать, что показывал пользователь во время демонстрации, включите любой модуль, который захватывает экран: *Пакеты снимков экрана*, *Снимки экрана*, *Видеозапись*. После этого от уведомления о демонстрации можно будет перейти к изображениям экрана из ближаших событий.

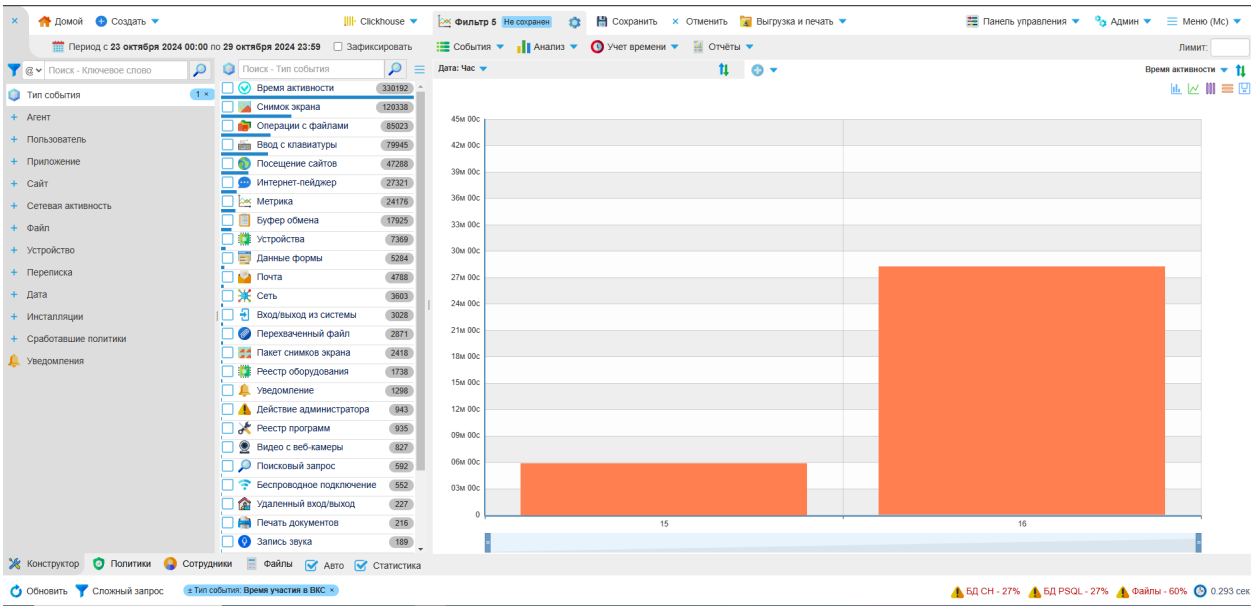
Все уведомления доступны в основном интерфейсе во вкладке **Конструктор** → **Уведомления**.

Отчеты

Время участия в ВКС не относится к управлению рабочим временем (УРВ), поэтому обработка данных происходит отдельно от других метрик рабочего времени. Отчеты строятся на основе события **Время участия в ВКС** по длительности сессии.

Чтобы построить отчет:

1. Выбрите тип события **Время участия в ВКС**.
2. В правой части экрана выберите в верхнем меню **Анализ**.
3. Выберите формат визуального анализа — например, линейный график.
4. Выберите меру анализа — **Время активности**.
5. Выберите измерения для построения отчета — например, **дата: час суток**.
6. Нажмите **Отсортировать**.



4.1.29 Перехват командной строки

С версии 5.5 доступен перехват командной строки, в том числе связанные с выполнением команд от имени других пользователей или повышением привилегий.

Включение перехвата

По умолчанию перехват командной строки отключен.

Чтобы включить перехват:

1. Перейдите **Панель управления** → **Конфигурации компьютера** → *ваша конфигурация* → **Клавиатура и буфер обмена**.
2. Активируйте выключатели **Контроль ввода команд**.
3. Сохраните изменения.

Просмотр событий

После включения перехвата агент создаёт событие **Терминал ввода команд**:

- при выполнении команды,
- запуске скрипта в командной строке.

Чтобы посмотреть события:

1. Выберите во вкладке **Конструктор** тип события **Терминал ввода команд**.
2. Опционально. Выберите агента, пользователя, приложение для фильтрации событий.
3. Готово. События отобразятся в правой части экрана в **Линзе событий**.

В событии записываются:

- команда;

- результат выполнения команды;
- имя компьютера;
- пользователь;
- приложение;
- локальное время.

Команда отображается в поле **Событие**.

Пример: перехват команды от имени другого пользователя

Пользователь может запустить команду от имени другого пользователя с помощью:

- **PsExec** — утилиты из Sysinternals для удаленного запуска команд с правами другой учётной записи,
- **runas** — встроенной команды Windows для запуска программ с правами другой учётной записи.

Агент перехватит обе команды и создаст событие о запуске команды с указанием имени пользователя, который инициировал выполнение. Для **PsExec** будет указано имя исполняемого файла `psexec.exe`, для **runas** — отображена встроенная команда `runas`.

4.1.30 Защита файлов инцидентов от удаления

Система автоматически защищает от удаления события и файлы, связанные с открытыми инцидентами. Функциональность позволяет сохранить данные, которые могут понадобиться для расследований.

Примечание: Система защищает от удаления только данные открытых инцидентов. Данные закрытых инцидентов можно удалить.

Если администратор попытается удалить такое событие или файл, появится сообщение: «Событие связано с инцидентом N XXXX, удаление невозможно. Удалите инцидент или отключите защиту в настройках».

Как включить защиту

По умолчанию защита от удаления выключена.

Чтобы включить защиту:

1. Откройте файл *config*:

```
sudo nano /etc/ibatyr/config
```

2. Добавьте в конец файла строку и сохраните изменения:

```
PROTECT_EVENTS_WITH_INCIDENTS = True
```

3. Перезапустите сервер:

```
ibatyr restart
```

От каких действий защищает

Защита блокирует удаление событий и файлов в случаях:

- удаление месячного шарда в базе данных;
- ручное удаление события в веб-консоли;
- автоочистка событий по политике;
- автоочистка файлов по политике;
- удалении объекта и всех данных компьютера и пользователя;
- удаление событий и файлов командой `ibatyr cleandata`;
- удаление событий и файлов командой `ibatyr cleanup`.

Как удалить файл или событие

Чтобы удалить событие или файл:

- закройте инцидент,
- удалите инцидент,
- отключите защиту через файл *config*.

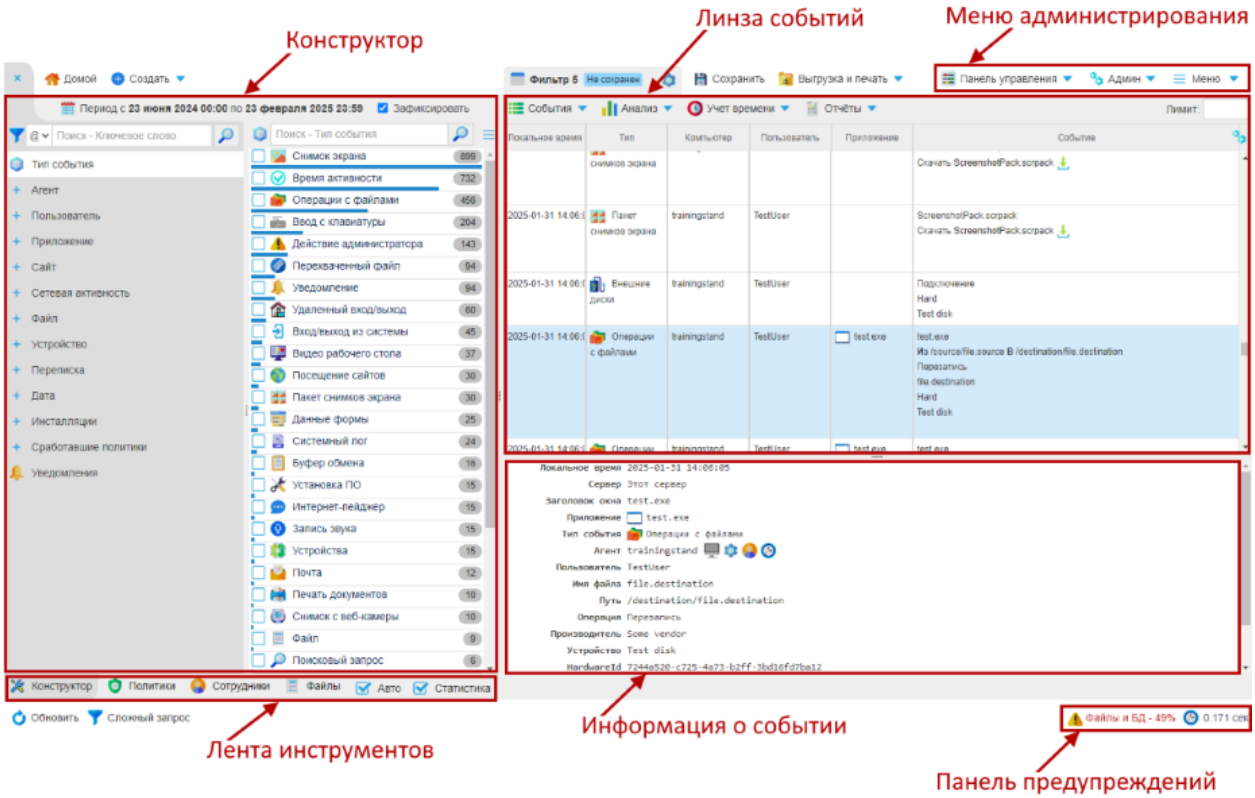
4.2 Интерфейс веб-консоли

4.2.1 Обзор

Содержание

- *Обзор*
  - *Домой*
  - *Создать*
  - *Линза событий*
  - *Лента инструментов*
  - *Меню администрирования*
  - *Панель предупреждений*
  - *Выгрузка и печать*

Главный интерфейс позволяет просматривать, фильтровать и анализировать события, поступающие на сервер iBatyr Monitor. Интерфейс состоит из нескольких областей: **Линза событий**, **Информация о событии**, **Лента инструментов**, **Конструктор**, **Меню администрирования** и **Панель предупреждений**.



Иконки и цвет кнопок отличаются в зависимости от выбранной темы интерфейса. Если размер экрана не позволяет уместить элементы интерфейса, подписи кнопок будут скрыты.

Домой

Кнопка **Домой** расположена в левом верхнем углу экрана. Используйте ее, чтобы перейти на главную страницу.

На некоторых страницах кнопка возврата называется **В основной интерфейс**.

Обратите внимание, что при клике на кнопки происходит сброс всех условий фильтрации. Чтобы обновить события в **Линзе** без потери условий, нажмите кнопку **Обновить** в нижнем левом углу.

Совет: Если новые события не отображаются в веб-интерфейсе, проверьте период в **Датапикере** и условия фильтрации. Нажмите кнопку **Домой** для сброса фильтров и установки текущей даты.

Создать

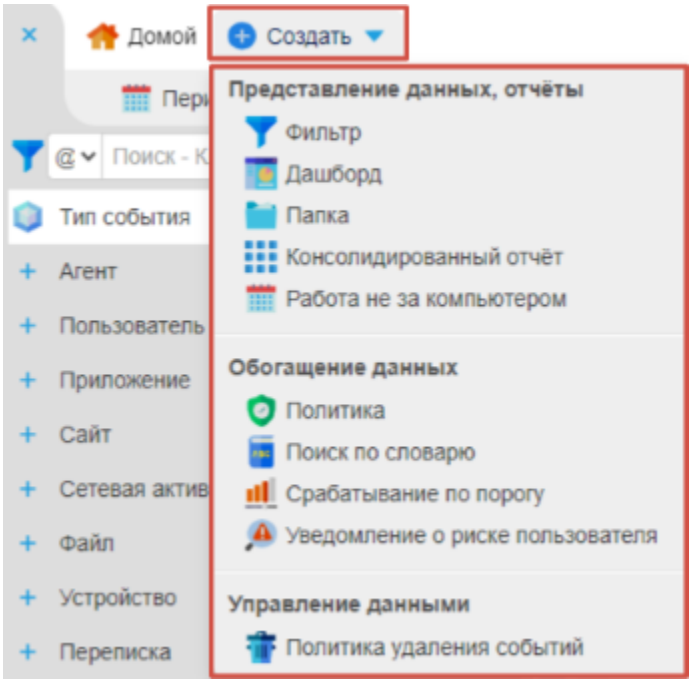
Меню **Создать** позволяет добавить новый инструмент фильтрации. Инструменты фильтрации служат для управления событиями. К ним относятся **Фильтры**, **Дашборды**, **Политики**, **Поиск по словарю** и пр.

См.также:

Подробнее об инструментах фильтрации

Например, чтобы создать фильтр:

1. Нажмите на **Создать** и выберите инструмент **Фильтр**. Откроется окно настройки инструмента.
2. Заполните настройки инструмента.
3. Нажмите **Сохранить**. Инструмент появится во вкладке **Политики**.



Линза событий

Входящие события отображаются в **Линзе событий**, которая располагается в правой части интерфейса.

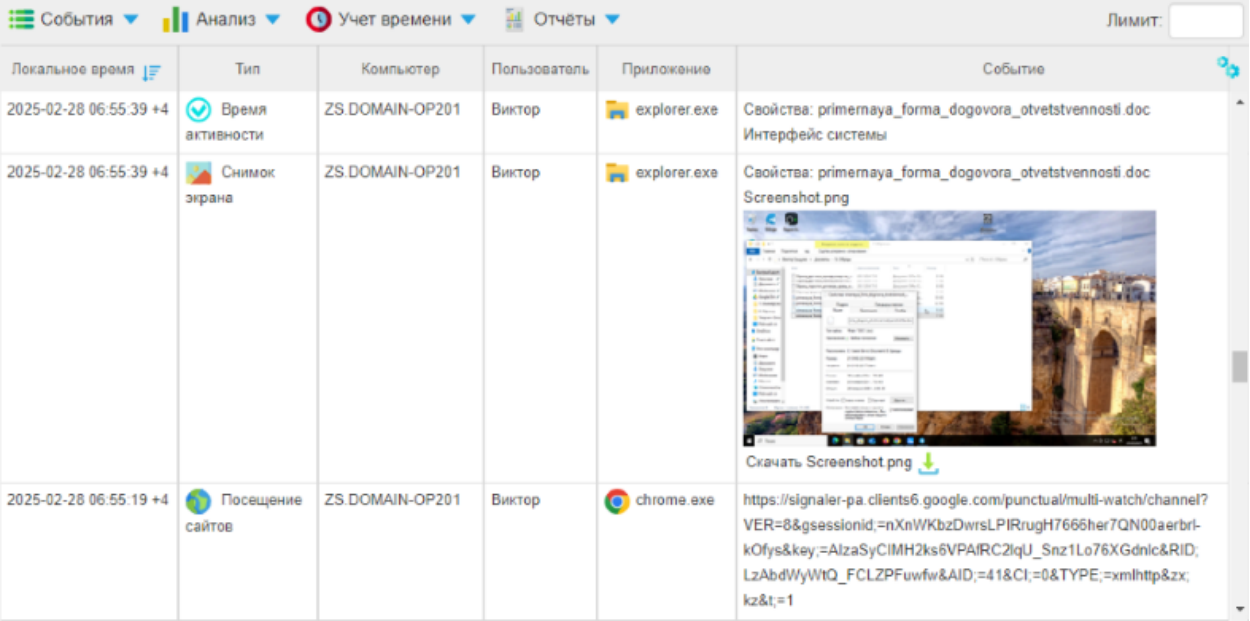
В линзе доступны:

- события, перехваченные агентом на компьютерах сотрудников;
- системные события.

См.также:

Подробнее о работе с данными в Линзе событий

По умолчанию данные в линзе отображаются в виде **Таблицы событий**:

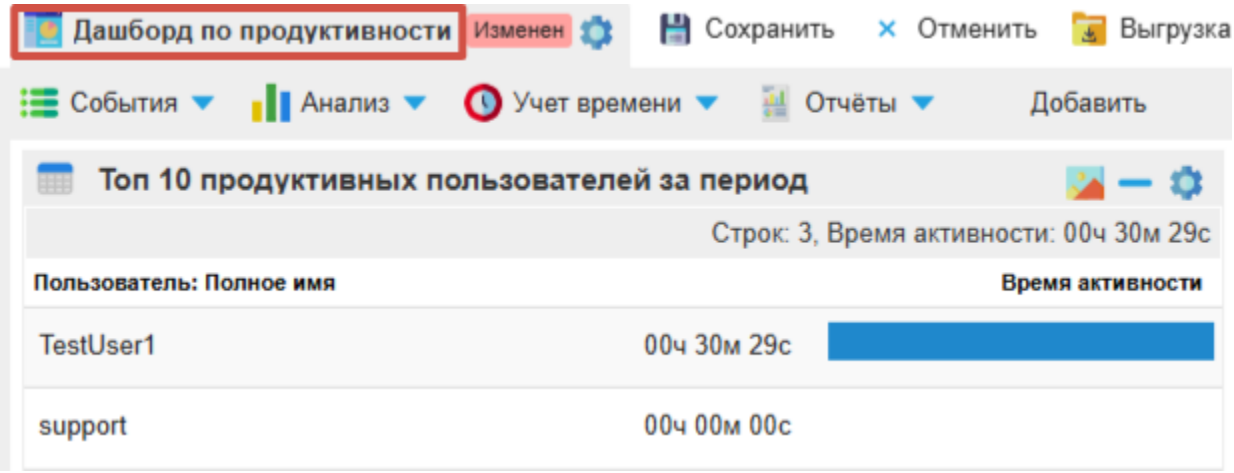


Нажмите на иконку шестеренок в правом верхнем углу **Линзы событий**, чтобы *добавить или удалить колонки в Таблице событий*.

Вы можете изменить формат отображения данных через несколько меню: **События**, **Анализ**, **Учет времени** и **Отчеты**. В зависимости от выбора данные будут отображаться в виде графиков, диаграмм или отчетов.

Текущий инструмент

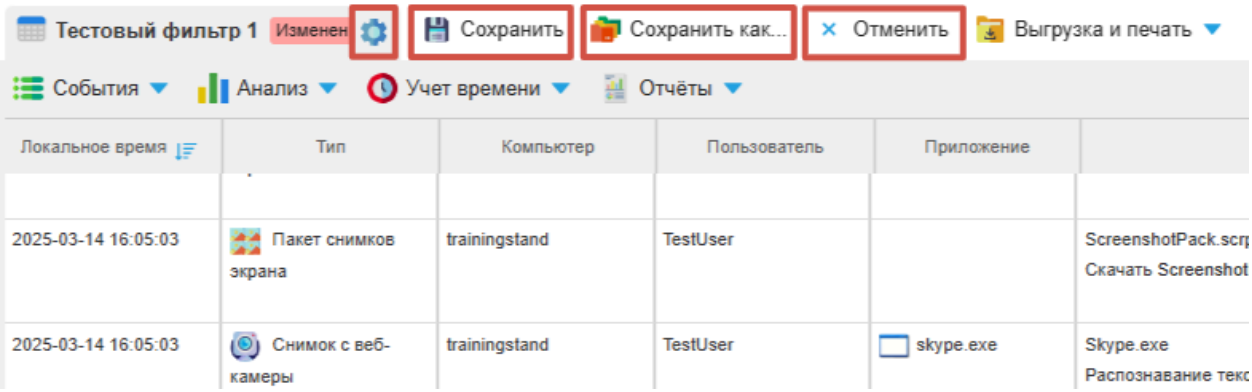
Над **Линзой событий** отображается название текущего инструмента. Например, если выбрать во вкладке **Политики** → **Отчеты** → **Дашборд по продуктивности**, над **Линзой** отобразится **Дашборд по продуктивности**, а в самой **Линзе** откроется дашборд графиков продуктивности.



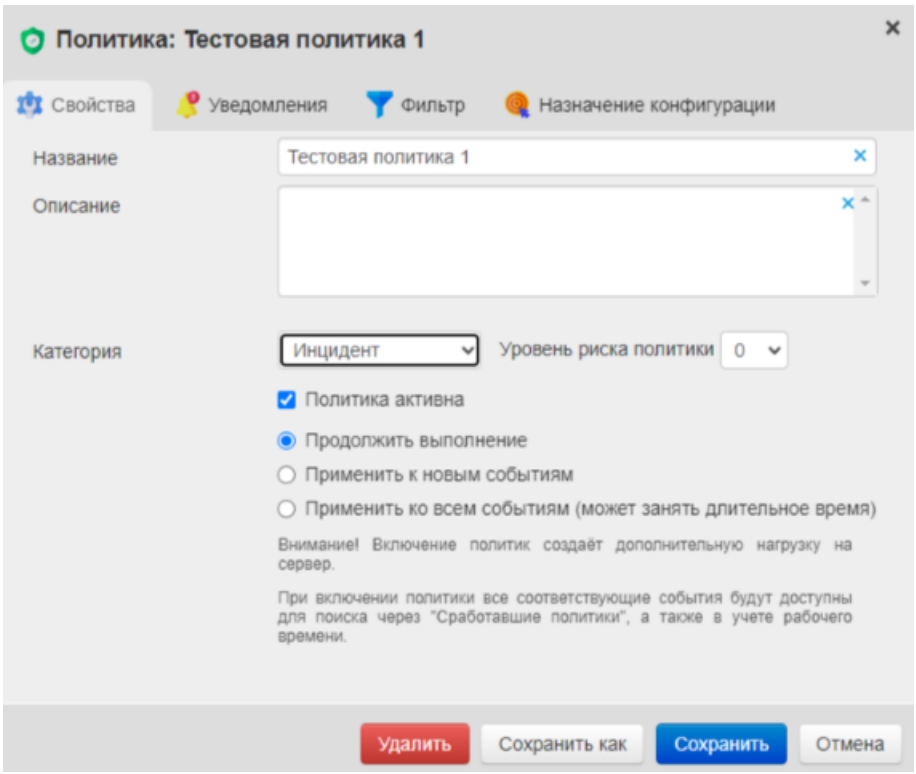
Если изменить инструмент в **Конструкторе**, например, добавить условия фильтрации, справа от названия появятся статус **Изменен** и кнопки:

- **Сохранить** — открывает окно сохранения инструмента,
- **Сохранить как** — сохраняет копию текущего инструмента с внесенными изменениями,

- **Отменить** — сбрасывает имя фильтра и условия фильтрации.

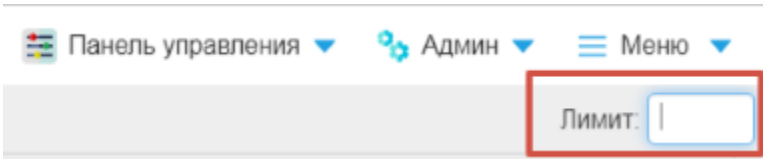


Справа от имени текущего инструмента располагается иконка шестеренки , нажатие на которую открывает *Окно настройки*:



Лимит

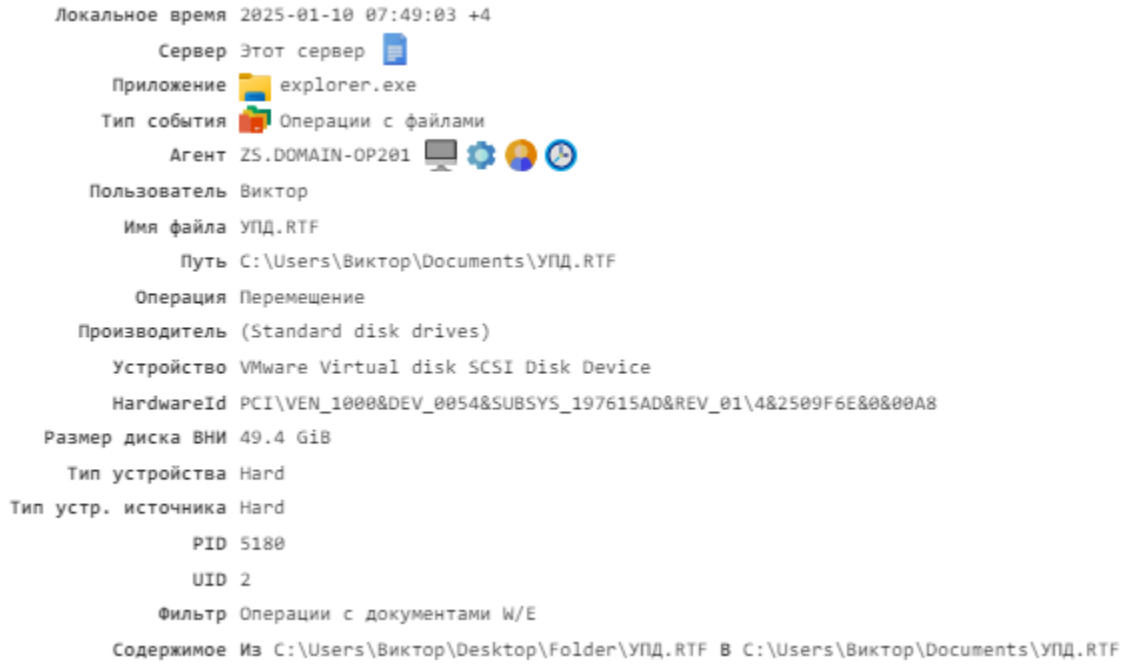
В **Линзе событий** отображаются все события, которые соответствуют условиям фильтрации. При большом количестве данных загрузка таблицы может занять длительное время. Укажите в поле **Лимит** количество событий для показа в **Линзе событий**, чтобы ускорить загрузку.



Информация о событии

Информация о событии находится в нижней правой части экрана под **Линзой событий**.

Нажмите на событие в **Линзе**, чтобы в **Информации о событии** отобразились все данные события. В этом поле указаны компьютер, пользователь, время, тип события, индивидуальные поля каждого типа.

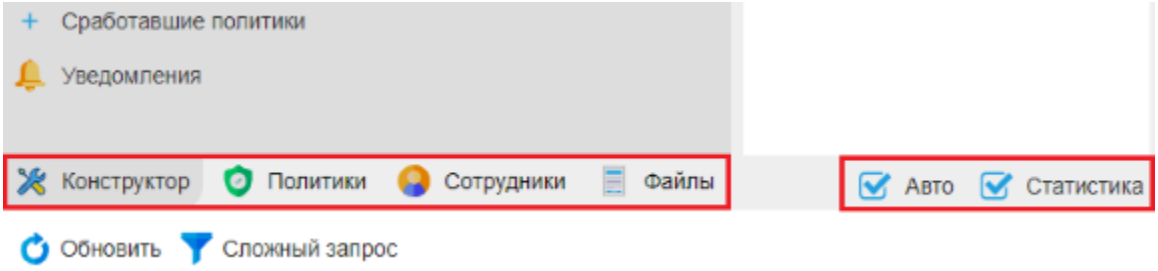


См.также:

Подробнее о типах событий

Лента инструментов

Лента инструментов располагается под **Конструктором**. Включает вкладки **Конструктор**, **Политики**, **Файлы**, **Сотрудники**, флаги **Авто** и **Статистика**.



Флаги:

- **Статистика**, чтобы выводить **Значения измерений** вне зависимости от наличия событий.
- **Авто** — автоматическое обновление данных в **Конструкторе** и **Линзе событий**.

Кнопка **Обновить** — позволяет обновить события в **Конструкторе** и **Линзе событий**. При этом будут сохранены условия фильтрации в отличие от обновления с помощью кнопки **Домой** или **В**

основной интерфейс.

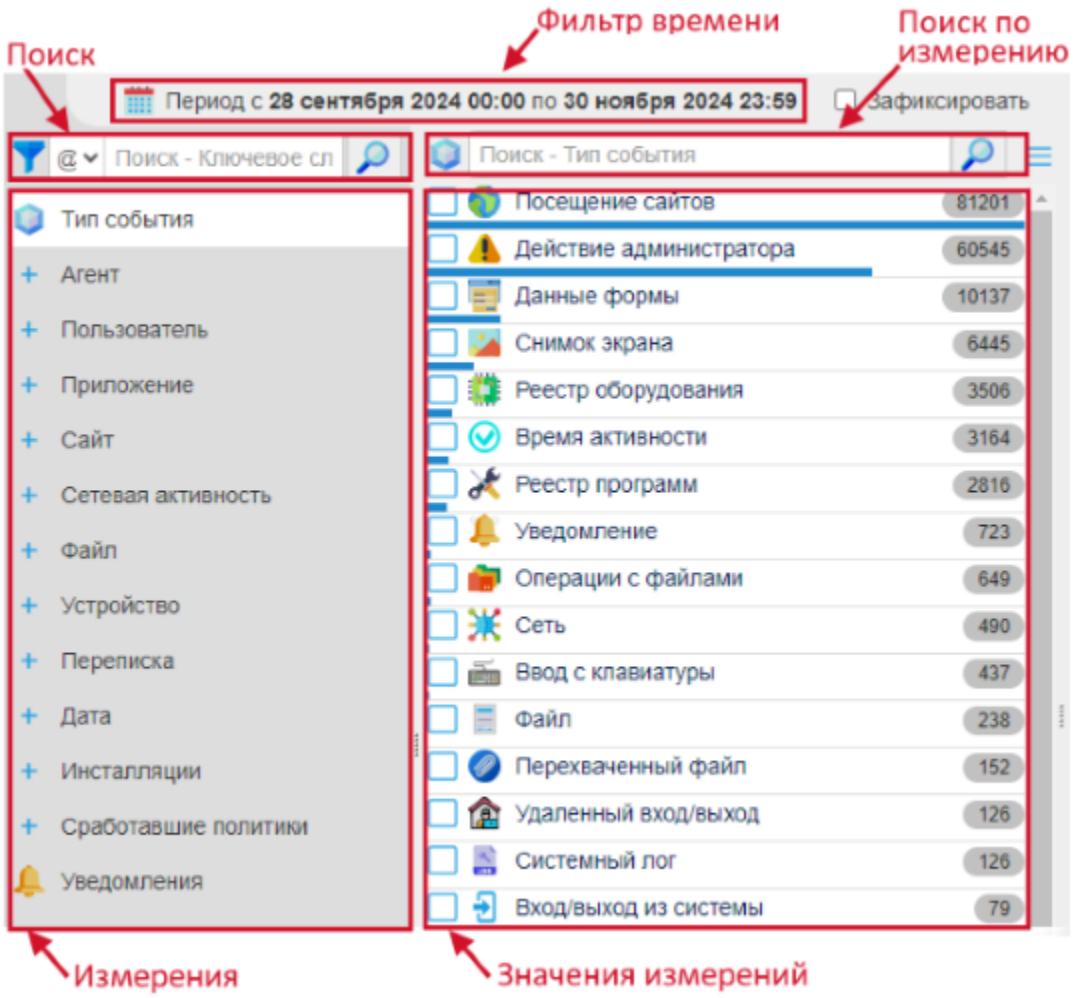
Конструктор

Конструктор — основной инструмент для фильтрации данных. С его помощью можно настроить фильтрацию по времени и условиям. Например, посмотреть, что делал пользователь *TestUser* на прошлой неделю.

Примечание: **Конструктор** доступен на главной странице и в *Окне настройки*.

В **Конструкторе** доступны функции:

- **Фильтр времени (Датапикер)** — выбор временного диапазона для отображения данных, например, месяц или год. Нажмите на **Датапикер**, выберите диапазон дат и нажмите **Enter** или **OK**.
- **Измерения** — список измерений для фильтрации данных: **Типы событий**, **Пользователи**, **Сайты**, **Устройства** и др. Например, нажмите на измерение **Сайт** и выберите параметры: **URL**, **Протокол**, **Полный домен**, **Тип контента**, **Основной домен**. Справа от измерений появится список значений этого измерения.
- **Значения измерений** — список значений для выбранного измерения. Например, при выборе **Приложение** отобразятся названия всех запущенных программ. Если выбрать конрентное значение — например, *ms word.exe* — в линзе отобразятся только события приложения MS Word.
- **Поиск** — поле для поиска по тексту, фразе или регулярному выражению.
- **Поиск по измерению** — поиск значений внутри выбранного измерения.



См.также:

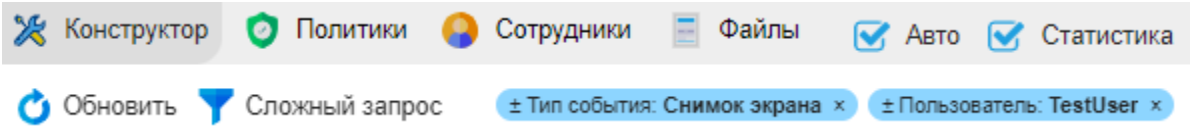
Подробнее о работе с Конструктором

Как отфильтровать данные в Конструкторе

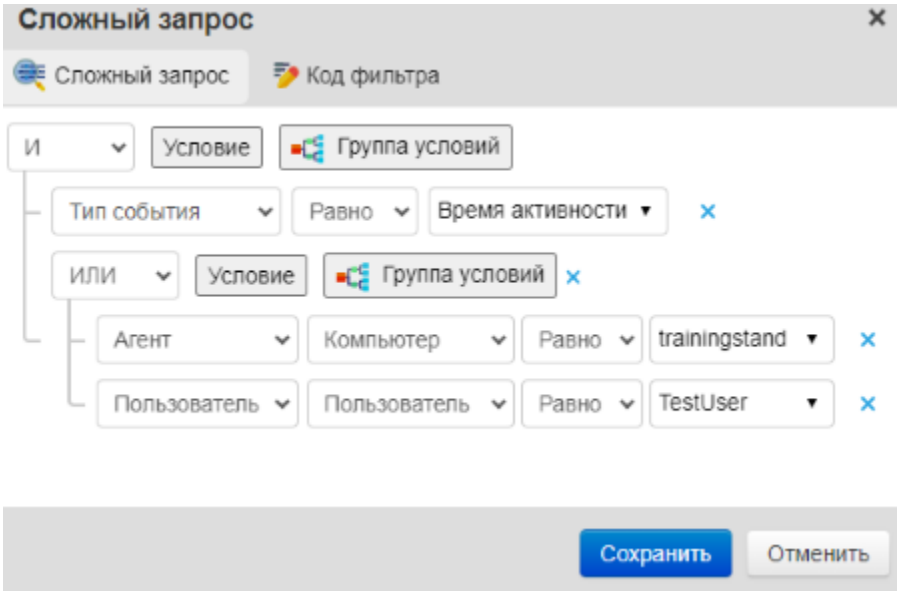
Пример: отфильтровать снимки экрана пользователя *TestUser* за текущую неделю.

1. В **Фильтре времени (Датапикер)** выберите **7 дней** и нажмите **Enter** или **OK**.
2. Выберите измерение **Пользователь**, укажите значение *TestUser*.
3. Выберите измерение **Тип события**, укажите значение **Снимок экрана**.

В линзе отобразятся события **Снимок экрана** для *TestUser* за неделю, а в левом нижнем углу экрана появятся условия фильтрации:



Кнопка **Сложный запрос** в нижнем левом углу экрана открывает окно, в котором можно задать сложные условия фильтрации с помощью логических выражений *И*, *ИЛИ*.



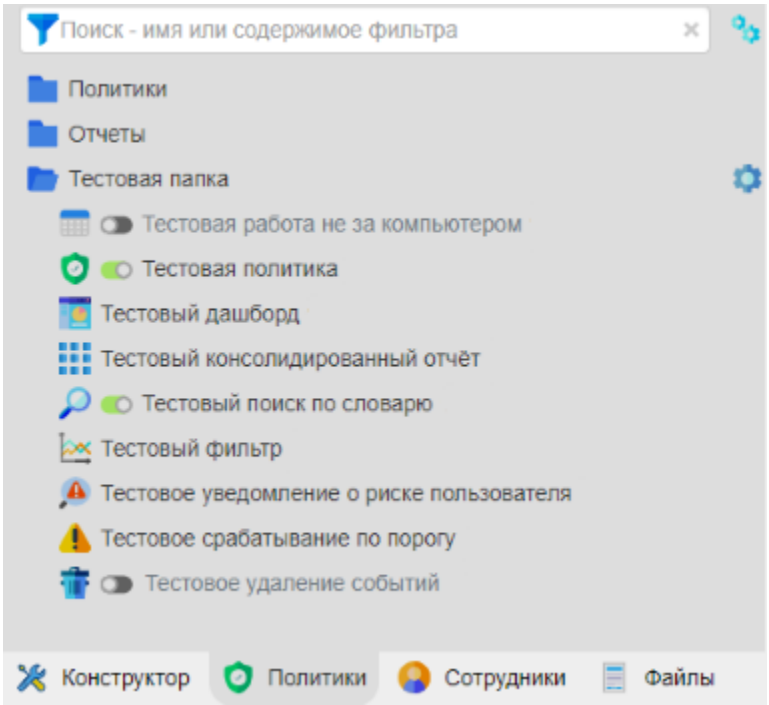
См.также:

Подробнее о работе со Сложным фильтром

Политики

Во вкладке **Политики** собраны встроенные и пользовательские *инструменты фильтрации данных*: **Фильтры**, **Политики**, **Дашборды** и т. д.

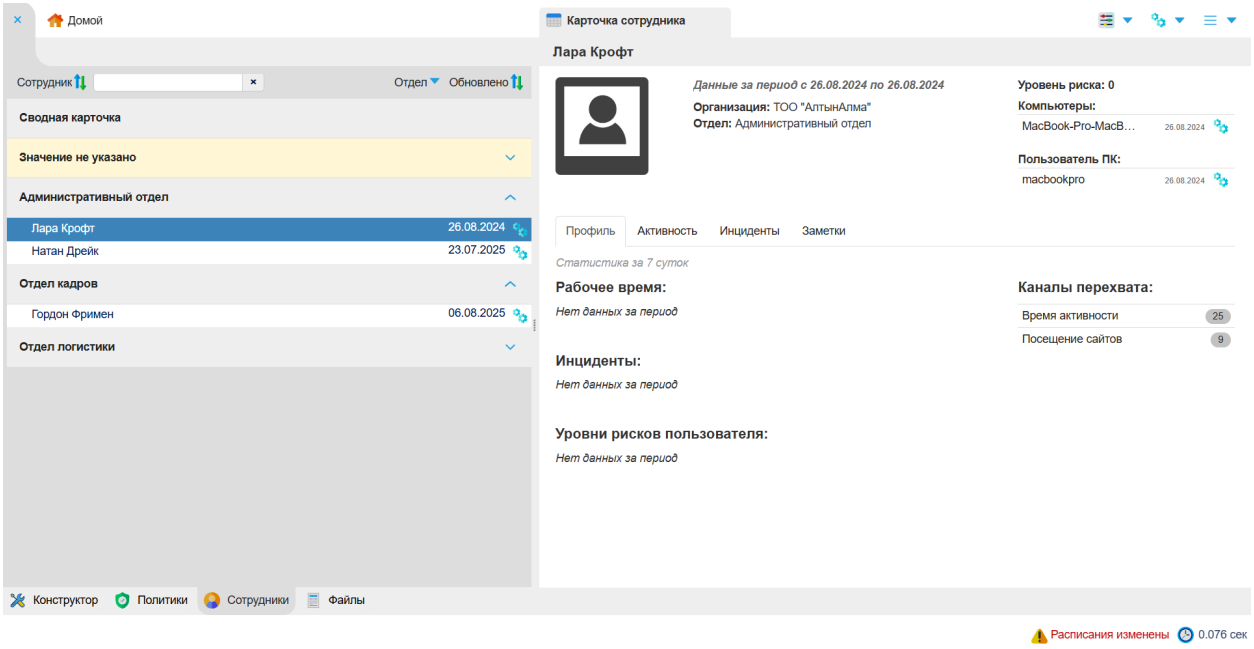
Нажмите на инструмент, чтобы увидеть его содержимое в **Линзе событий**.



Сотрудники

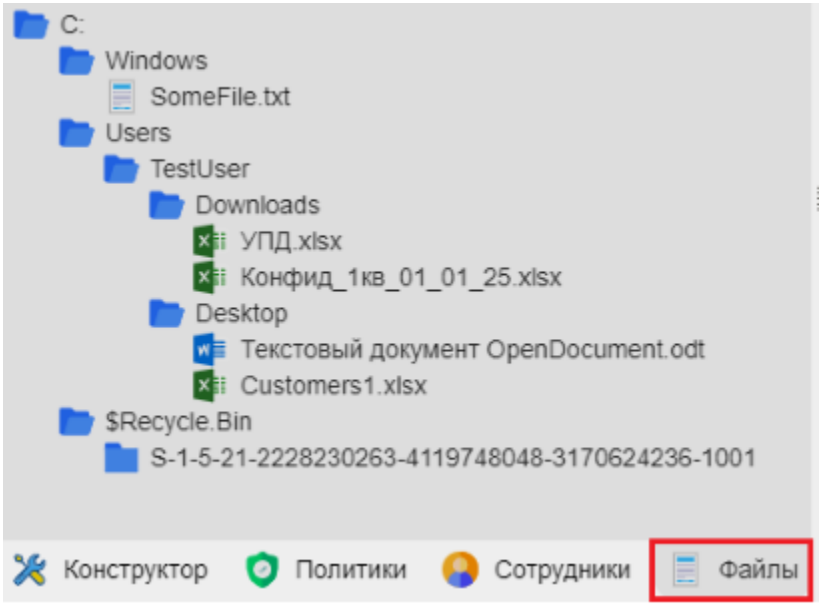
Во вкладке **Сотрудники** представлены **Карточки сотрудников** — дашборды с полной информацией о зарегистрированных в системе iBatyr Monitor пользователях.

Предупреждение: Чтобы вкладка отображалась, активируйте *Карточки сотрудника*.



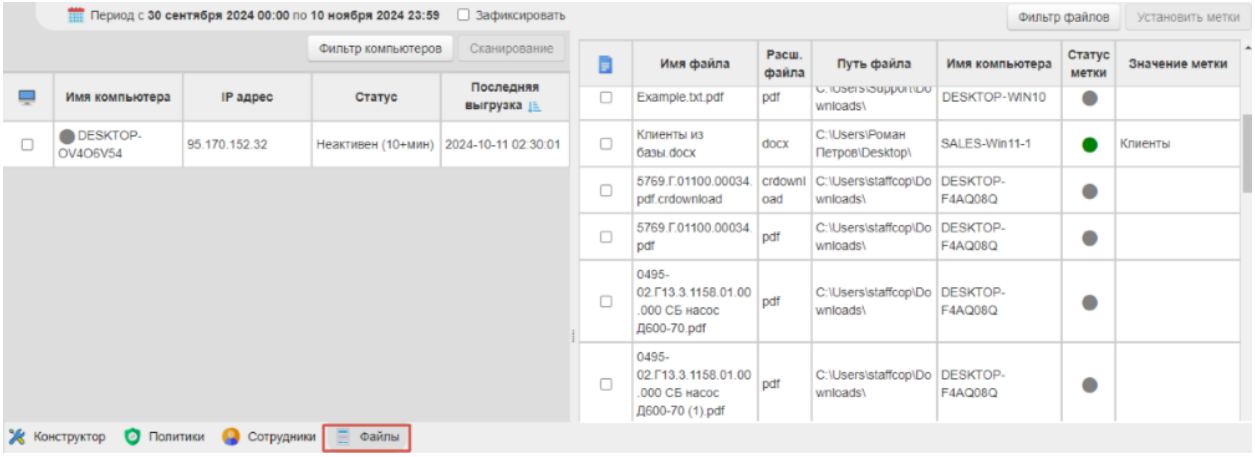
Файлы

Раздел **Файлы** отображает структуру файлов, полученных при сканировании компьютеров сотрудников.



Предупреждение: Для перехвата файлов включите *Файловый мониторинг* или *Файловый сканер*.

В этом разделе доступен функционал Централизованного сканирования и установки меток.



Меню администрирования

Меню администрирования располагается в правом верхнем углу экрана. Предназначено для детальной настройки работы сервера и *конфигураций агентов*.

Включает в себя разделы:

- *Панель управления*;
- *Админ*;
- *Меню*.

Панель предупреждений

Панель предупреждений — находится в правом нижнем углу, отображает предупреждения о состоянии системы и лицензии.

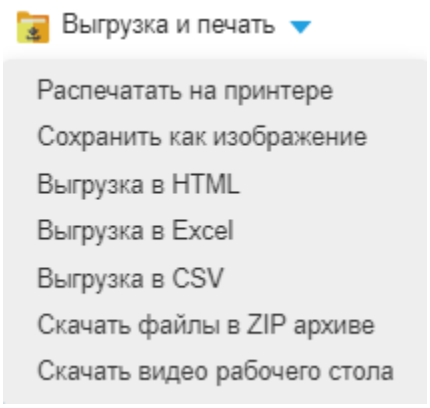
См.также:

Настройте предупреждения о состоянии базы данных и файлового хранилища в системной политике *Автоочистка*.

Время загрузки событий — находится в правом нижнем углу, отображает в секундах скорость загрузки **Линзы событий**.

Выгрузка и печать

Раздел **Выгрузка и печать** расположен в верхней левой части веб-интерфейса. Позволяет экспортировать отфильтрованные события в различных форматах.



Предупреждение: Опции в меню **Выгрузка и печать** отличаются для разных форм отображения данных — таблицы, дашборда, линейной диаграммы и т. д.

- **Распечатать на принтере** — открывает стандартное окно печати браузера;

  Подсказка: Чтобы выгрузить данные в формате **PDF**, нажмите **Распечатать на принтере** и выберите **Принтер** → **Сохранить как PDF** → **Сохранить**.

- **Сохранить как изображение** — экспортирует данные из линзы событий в формате PNG;
- **Выгрузка в HTML** — сохраняет данные в формате HTML;
- **Выгрузка в Excel** — экспортирует таблицу в формате XLSX;
- **Выгрузка в CSV** — сохраняет данные в формате CSV;
- **Скачать файлы в ZIP архиве** — загружает значения из таблицы в ZIP-архив с изображениями в формате PNG;
- **Скачать видео рабочего стола** — выгружает все события типа **Видео рабочего стола** за выбранный период в единый MKV-файл.

  Примечание: Выгрузка видео рабочего стола может занять длительное время, в зависимости от объема данных. В файле сохранятся только загруженные в **Линзу событий** видео.

4.2.2 Панель управления

Панель управления — основной инструмент администрирования программы iBatyr Monitor , который позволяет устанавливать агенты, настраивать конфигурации, настраивать параметры сервера и интегрированных учетных записей.

Компьютеры

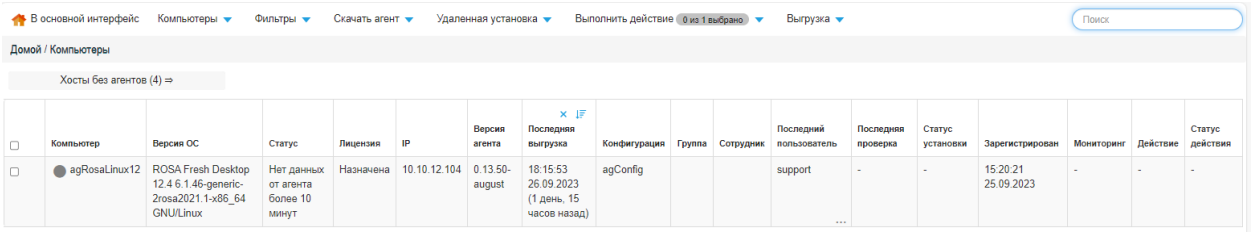
В разделе **Панель управления** → **Компьютеры** представлены компьютеры, на которых:

- установлен агент;
- был установлен агент;
- проверялась возможность установки агента.

Информация с агентов начинает передаваться на сервер и отображаться в web-интерфейсе сразу после добавления агента.

Информация о компьютерах

Вся доступная информация о компьютерах представлена в таблице:



Столбец **Статус** содержит общую информацию о состоянии агента и статусе передачи данных.

В столбце **Лицензия** указан статус лицензии для всех компьютеров в списке:

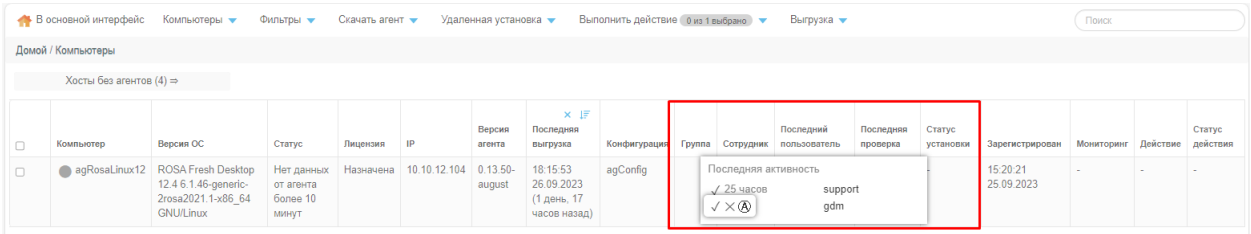
tabularytabulary

	Статус
	Назначена
	Отозвана
	Автоматически

В столбце **Конфигурация** указано название *конфигурации, назначенной данному компьютеру*.

Столбец **Последний пользователь** позволяет:

- посмотреть список пользователей, которые последними пользовались компьютером;
- время, когда пользователи подключались;
- управлять назначением лицензий для данных пользователей.



Столбец **Последняя проверка** показывает дату последней диагностики состояния компьютера и агента.

В столбце **Статус установки** отображается результат проверки. Эти статусы предоставляют информацию о текущем состоянии установки.

tabularytabulary

Статус
Неизвестная ошибка *Серый*
Хост не отвечает *Красный*
Хост недоступен *Красный*
Соединение отвергнуто *Красный*
Соединение сброшено *Красный*
Неверный пароль *Красный*
Пароль устарел *Красный*
Ограниченная учетная запись *Красный*
Нет прав *Красный*
Ресурс ADMIN$ недоступен *Красный*
Ошибка SMB *Красный*
Протокол не поддерживается *Красный*
Имя ресурса не найдено *Красный*
Требуется ручная настройка *Красный*
Требуется перезагрузка *Желтый*
Сбой доверительных отношений *Красный*
Агент запущен *Зеленый*
Агент установлен *Зеленый*
Агент поврежден *Красный*
Агент удален *Серый*
– *Серый*

В столбце **Мониторинг** приведена информация о состоянии агента на компьютере:

tabularytabulary

Статус
В сети
Не в сети
Был сегодня
Мониторинг отключен
-

Столбцы **Действие** и **Статус действия** позволяют следить за процедурами обновления или удаления агента с машины.

Меню управления разделом Компьютеры

Меню управления состоит из разделов:

- **В основной интерфейс**. Быстрый переход в основное меню работы с iBatyr Monitor.
- **Компьютеры**. Переход между разделами меню **Панели управления**.
- **Фильтры**. Сортировка агентов по выбранному параметру:
  - Сканирование;
  - Статус;

  - Статус установки;
  - Лицензия;
  - Зарегистрирован;
  - Статус агента;
  - Группа;
  - Конфигурация;
  - Версия ОС.
- **Скачать агент**. Загрузка установщика агента для выбранной операционной системы:
  - Windows;
  - Linux;
  - macOS;
  - Утилита удаленной установки для Windows;
- **Удаленная установка**. Удалённая работа с агентом через веб-интерфейс.

  Доступные опции:
  - установка в локальной сети;
  - установка в Active Directory.

  Подробнее о вариантах установки можно прочитать в статье *Установка агентов*
- **Выполнить действия**. Выбор действий с компьютерами, на которые установлен агент.

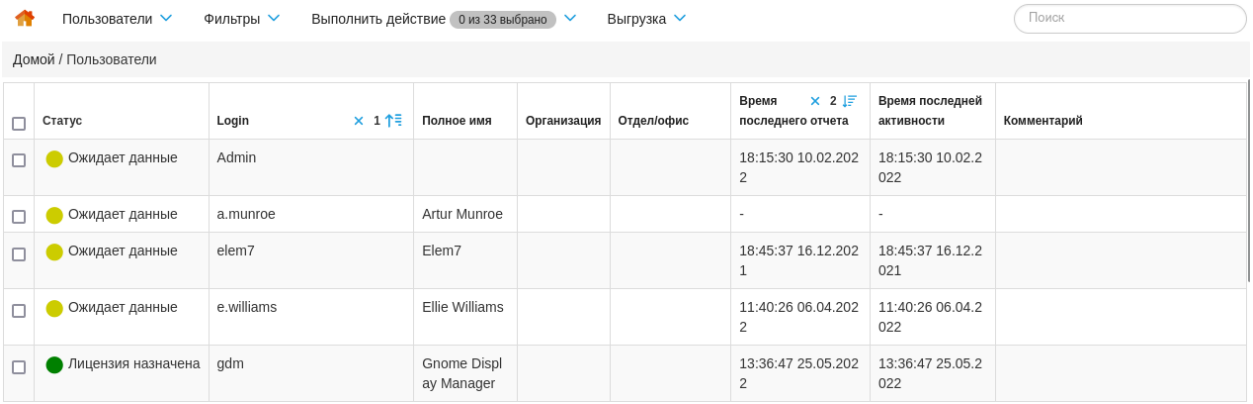
  Доступные варианты:

Примечание: В случае возникновения ошибок при обновлении или удалении агентов, сервис автоматически предпримет повторную попытку обновления/удаления. Если ошибка повторится, в столбце **Статус действия** появится сообщение **Критическая ошибка**. На такие машины необходимо обратить внимание администратору сети.

- **Выгрузка**. Выгружает данные по компьютерам с возможностью выбора полей в формате csv.

Пользователи

В этом разделе представлена информация из Active Directory о пользователях компьютеров, на которых установлены агенты.



Статус	Login	Полное имя	Организация	Отдел/офис	Время последнего отчета	Время последней активности	Комментарий
Ожидает данные	Admin				18:15:30 10.02.2022	18:15:30 10.02.2022	
Ожидает данные	a.munroe	Artur Munroe			-	-	
Ожидает данные	elem7	Elem7			18:45:37 16.12.2021	18:45:37 16.12.2021	
Ожидает данные	e.williams	Ellie Williams			11:40:26 06.04.2022	11:40:26 06.04.2022	
Лицензия назначена	gdm	Gnome Display Manager			13:36:47 25.05.2022	13:36:47 25.05.2022	

Для удобства работы значения полей **Login**, **Полное имя**, **Организация**, **Отдел/офис** и **Комментарий** можно изменить.

Статус

В поле **Статус** представлена информация о лицензии для данного пользователя:

Способы синхронизации сервера iBatyr Monitor с Active Directory:

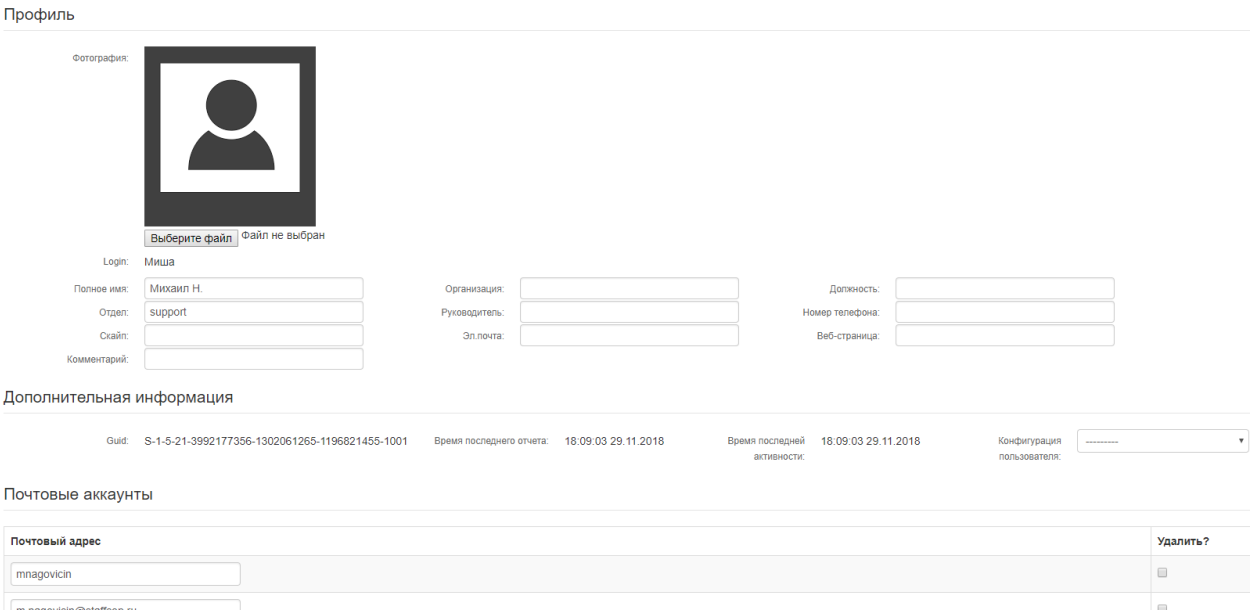
- в разделе «Панель управления - Настройки Active Directory» нажать кнопку «Выполнить синхронизацию»;
- в консоли управления сервером выполнить команду:

```
ibatyr ad_sync
```

Если пользователь был уволен или по каким-то другим причинам был отключен в Active Directory, с его учётной записи снимается лицензия. Информация об этом добавляется в раздел «Администрирование -> Последние действия».

Карточка пользователя

Данные о пользователе представлены в Карточке пользователя. Чтобы открыть её, нажмите на логин пользователя или на статус его учетной записи.



Данные в карточке пользователя можно:

- заполнить вручную;
- внести данные в учетную запись Windows;
- заполнить профиль в Active Directory.

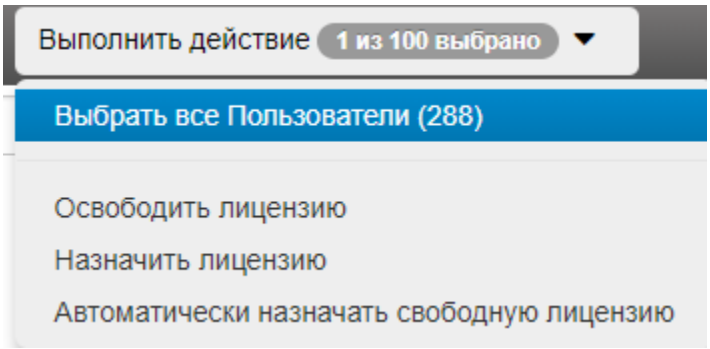
Добавление новых пользователей к системе происходит автоматически при регистрации агента на сервере. Вручную добавлять пользователей не нужно. Для регистрации и идентификации агентов используется SID.

Примечание: Если в карточке пользователя в почтовые аккаунты добавить логин скайпа, то события скайпа подвяжутся к пользователю.

Начиная с версии 5.0, в iBatyr Monitor появился элемент **Выгрузка**. Он позволяет выгружать данные по пользователям с возможностью выбора полей в формате csv.

Распределение лицензий

Освобождать и назначать лицензии можно как для отдельных, так и для групп пользователей. Для этого выберите одну или несколько учетных записей и в выпадающем списке **Действие** выберите нужное. Пользователи, которым освободили лицензию, не будут попадать в систему мониторинга.

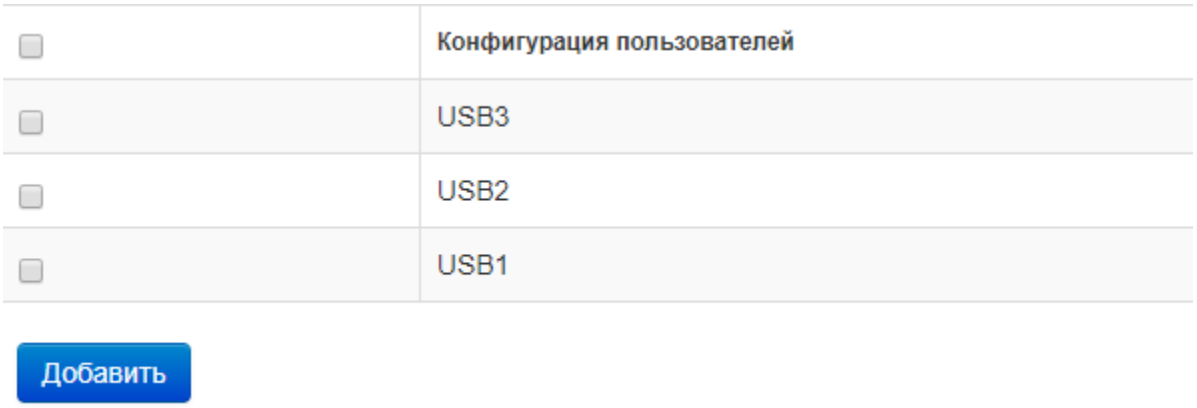


Конфигурация пользователей

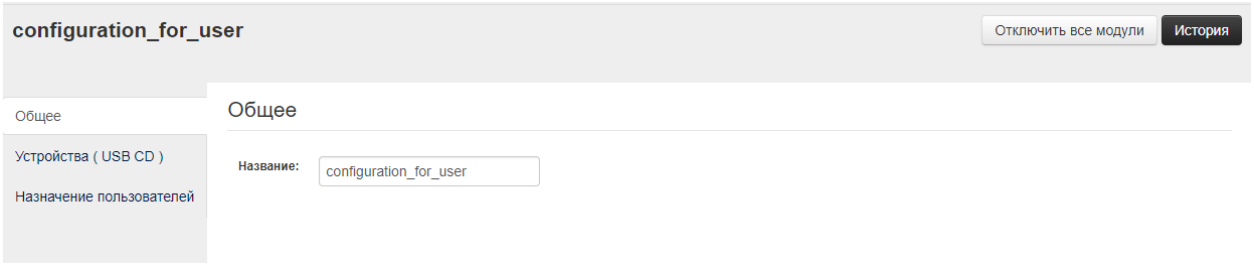
Конфигурация пользователей, как и конфигурация агентов, служит для включения/отключения модулей мониторинга по пользователям. На текущий момент, конфигурация пользователей используется для настроек конфигурации устройств USB.

Каждому пользователю можно присвоить уникальную конфигурацию.

Для редактирования конфигурации нажмите на соответствующее название конфигурации, либо добавьте новую.



Общее



Название - здесь задается название новой конфигурации или отображается имя существующей конфигурации.

Устройства USB, CD

Примечание: Для работы данных модулей, в конфигурации агента должны быть включены модули «Файловая активность» и «USB-устройства».

- **Блокировать USB накопители** - включение данного модуля блокирует подключение всех USB-накопителей.
- **USB накопители только для чтения** - включение данного модуля запретит изменять файлы на USB накопителях.

Правила: Блокировка - USB:

- **Блокировать** - блокировка всех «Device ID» указанных в списке.
- **Разрешить** - блокировка всех «Device ID» за исключением тех, что указаны в данном списке.

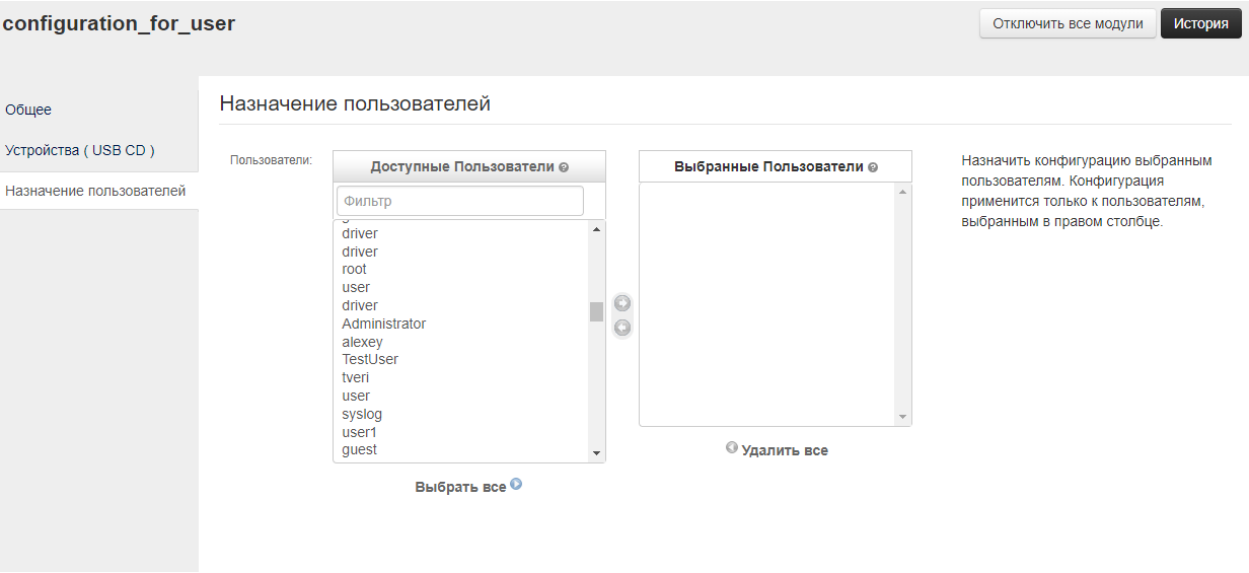
Если вам необходимо настроить белый список устройств или список заблокированных устройств, рекомендуем ознакомиться со статьей *Контроль USB-устройств*. Правила для пользователей работают идентично.

Примечание: Включение модулей в конфигурации пользователя имеет наивысший приоритет. Если в конфигурации агентов есть правила для USB-устройств, конфигурация пользователя их перекроет.

Примечание: Необходимо указывать полный «Device ID» устройства.

Предупреждение: Только для Linux агента: если не внести «Device ID» клавиатур и мышей в список разрешенных, то у вас перестанут работать все USB-устройства, кроме тех что введены в этот список, будьте осторожны с этим видом блокировок на Linux.

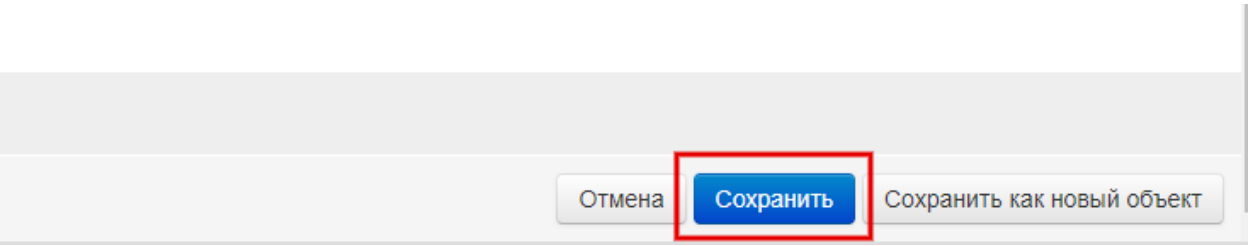
Назначение пользователей



Интерфейс позволяет назначать или снимать конфигурацию для выбранных пользователей.

Сохранение конфигурации

Для сохранения конфигурации пользователя нажмите на кнопку «Сохранить».



Устройства

Содержит список устройств со следующими полями:

- ID устройства
- Описание
- Производитель
- Тип устройства
- Класс устройства
- Метка

Примечание: Возможно установить метку для устройств, которая в основном используется при формировании отчета СКУД.

Приложения

Содержит список приложений используемых на компьютерах, где установлен агент со следующими полями:

- Имя приложения
- Описание приложения
- Исполняемый путь

Примечание: Возможно сменить описание приложения нажав на имя продукта.

Файлы — Поиск похожих

Метод триграмм измеряет, насколько две строки похожи, сравнивая их подстроки длиной 3 символа. Например, у слов *буклет*: {*бук*, *укл*, *кле*, *лет*} и *билет*: {*бил*, *иле*, *лет*} только одна общая триграмма. Чем больше у слов общих триграмм, тем выше коэффициент схожести.

Начиная с версии 4.5 добавлен новый поисковый механизм — поиск похожих по содержимому документов.
Функция определяет схожесть алфавитно-цифровых строк в документе с образцом на основе триграмм.
Для удобства работы с функцией была добавлена новая функциональность в веб-консоль iBatyr Monitor.

Поиск по образцу

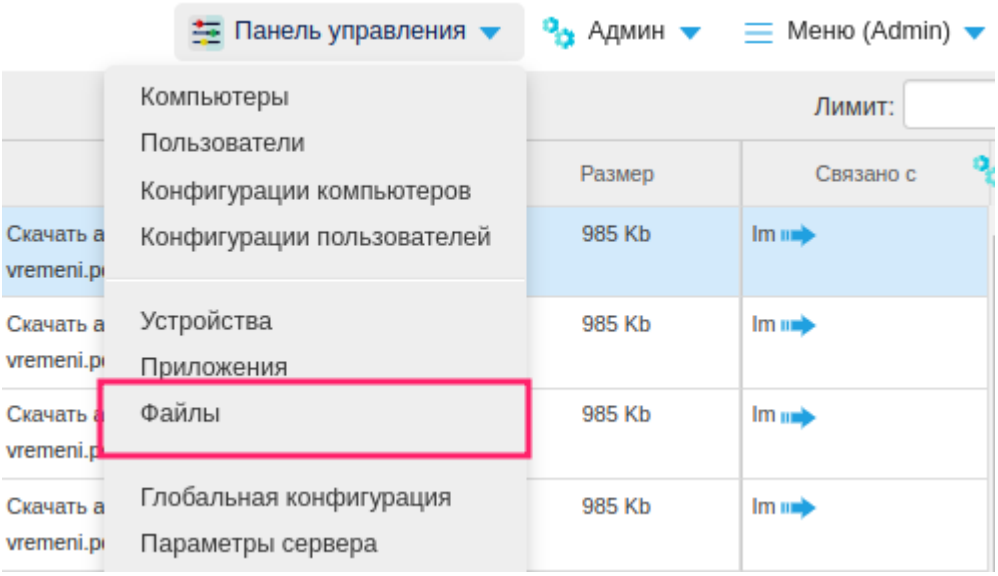
Загрузите образцы для поиска похожих документов.

Доступные форматы для образцов:

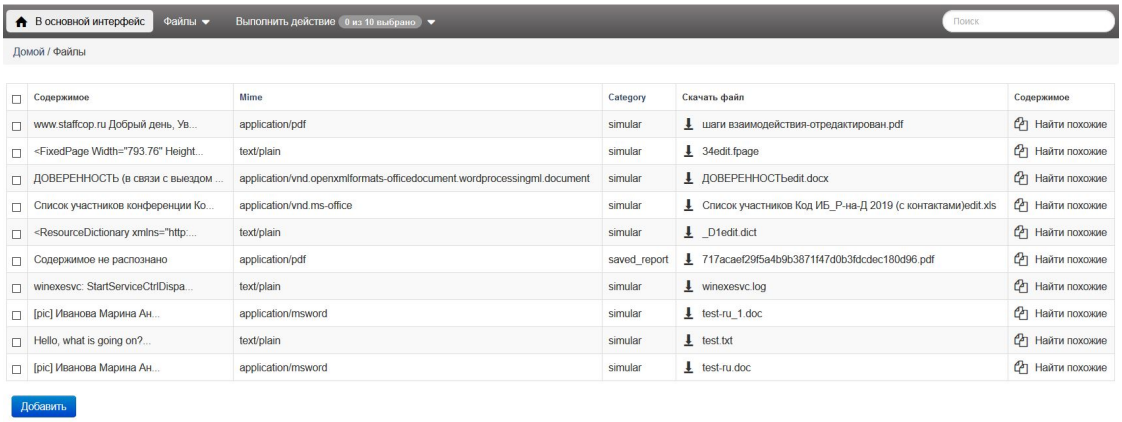
- TEXT — обычные текстовые документы,
- XLS/XLSX — форматы хранения электронных таблиц,
- ODT/DOC/DOCX — распространённые форматы хранения текстовых файлов,
- XPS — файлы печати Windows,
- PDF — распространённый формат для электронного обмена документами.

Чтобы загрузить образец и найти похожие документы:

1. Перейдите **Панель управления** → **Файлы**:



2. Нажмите кнопку **Добавить** и загрузите образец.
3. Напротив загруженного документа нажмите кнопку **Найти похожие**.



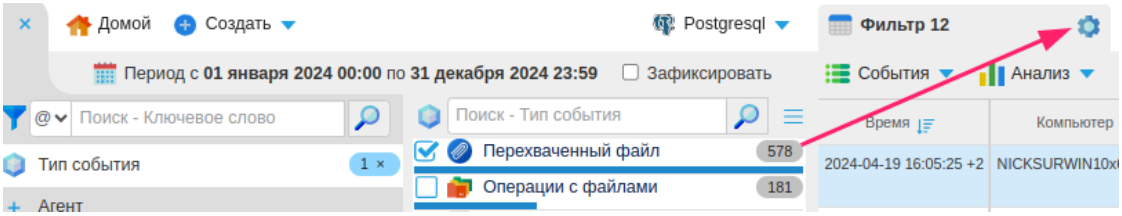
После этого вы будете перенаправлены в **Конструктор** с применением фильтра по поиску похожего документа.

Примечание: Обратите внимание, что поиск похожего документа может не дать результатов, если в **Конструкторе** выбран короткий период времени. Рекомендуем выбрать период от месяца.

Поиск по перехваченным файлам

Найдите документы, похожие на перехваченный файл.

1. Выберите в **Конструкторе** тип события **Перехваченный файл**.
2. Нажмите на значок фильтра в верхнем меню.

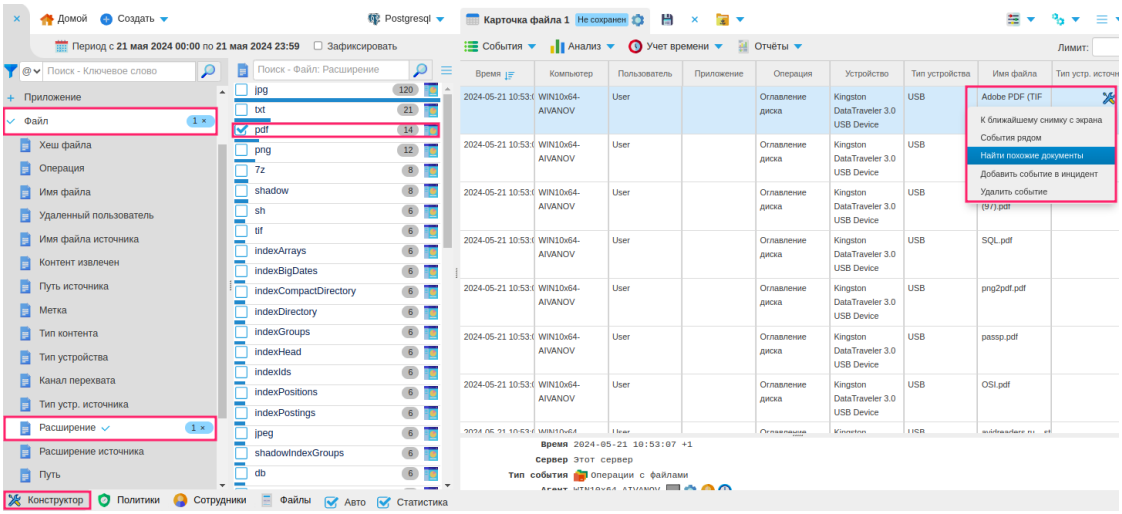


3. В открывшемся окне перейдите во вкладку **Фильтр**.
4. Выберите **Файл** → **Расширение** и укажите расширение, например *pdf*.

Примечание: Опция доступна только для документов. Ее нельзя применить к изображениям, архивам и служебным файлам.

---

5. Наведите курсор на событие и нажмите значок инструментов.
6. Выберите в меню **Найти похожие документы**.



В результате в **Линзе событий** отобразятся документы, которые имеют совпадения по полю **Содержимое** перехваченного файла.

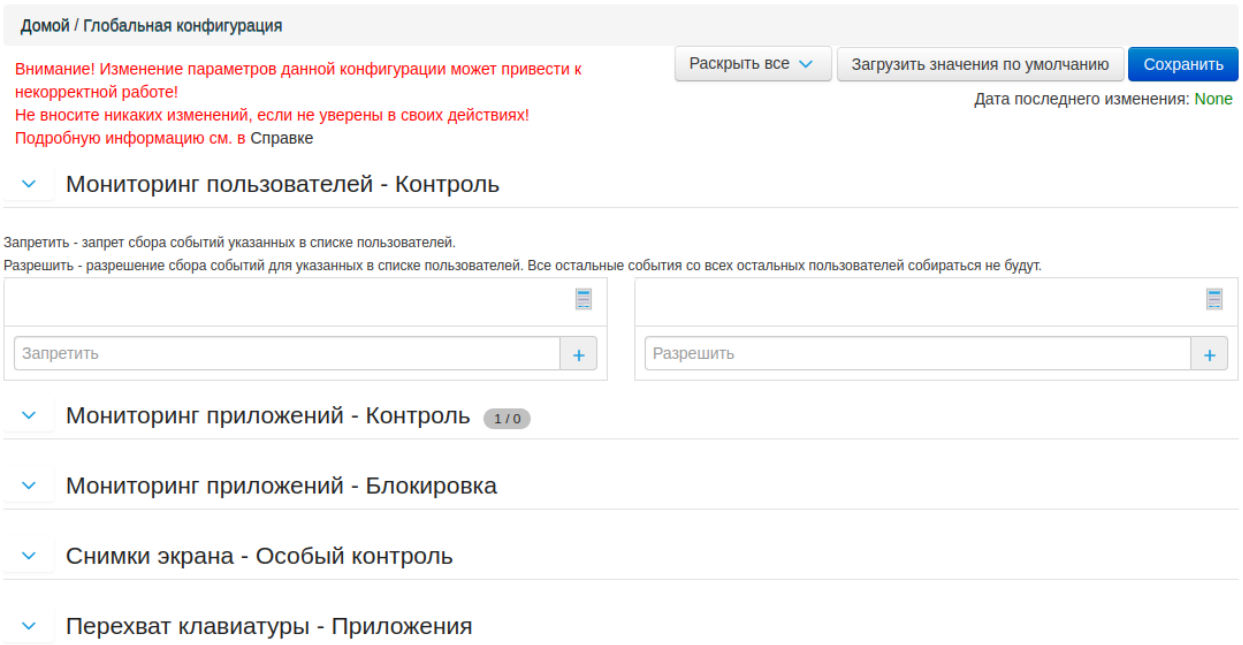
Глобальная конфигурация

Глобальная конфигурация – интерфейс для настройки правил для модулей мониторинга для всех пользователей, независимо от назначенной им конфигурации.

Удаление и изменение правил глобальной конфигурации не рекомендуется и может привести к неработоспособности вашей системы. Настройки глобальной конфигурации накладываются на правила мониторинга конфигурации агентов.

Администратор должен иметь *разрешение на редактирование глобальной конфигурации*.

Для редактирования конфигурации нажмите на название правила конфигурации.



Форма редактирования идентична форме настроек **Правил мониторинга** в *конфигурации*, она предназначена для добавления новых типов правил и их значений.

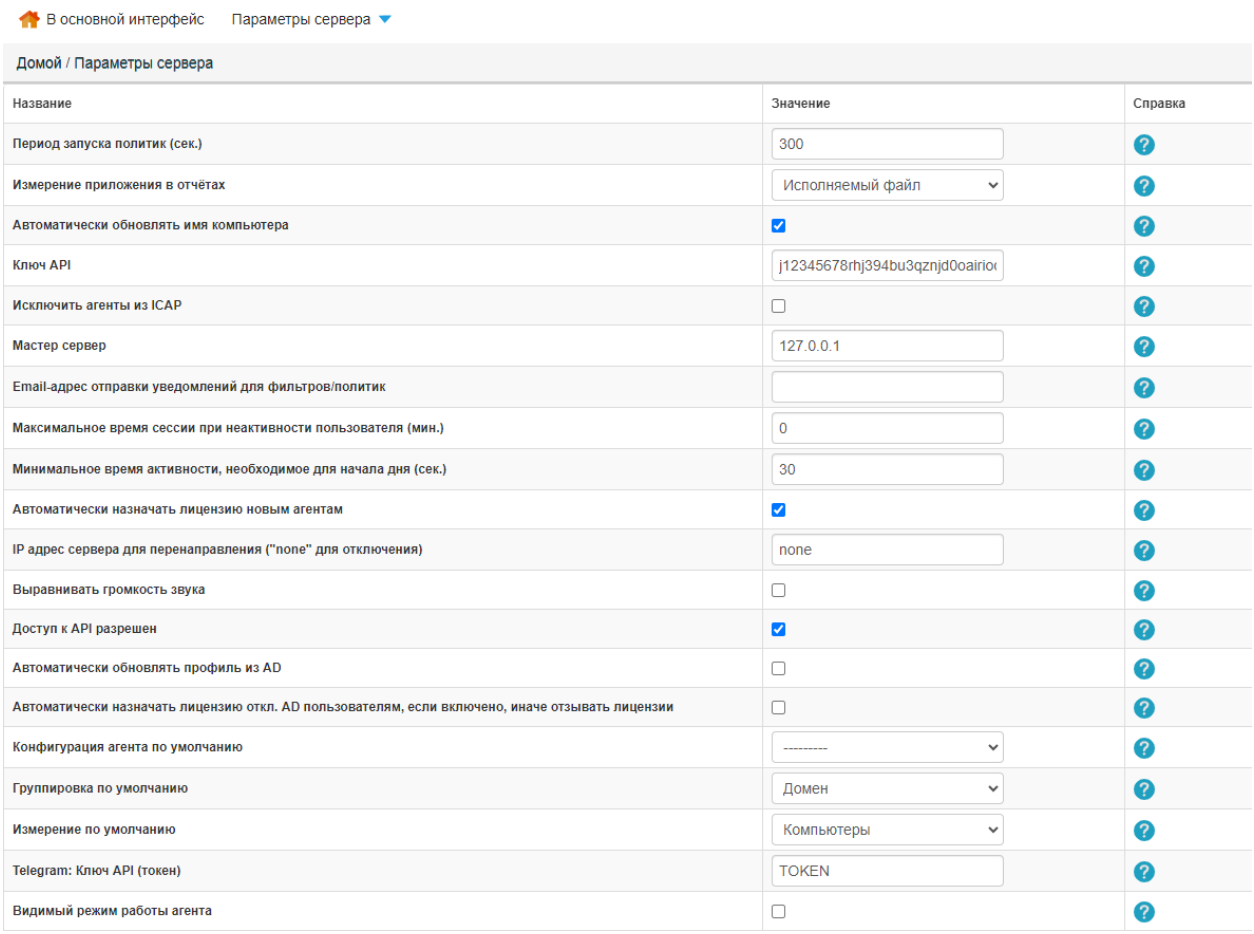
Разрешить – позволяет разрешить сбор данных/подключение только по выбранным значениям, остальное блокируется.

Запретить – запрещает собирать данные/блокирует устройства из списка, разрешая сбор данных/подключение всем остальным.

Чтобы правила мониторинга глобальной конфигурации вступили в силу, нажмите кнопку **Сохранить**.

Параметры сервера

Параметры сервера — интерфейс, предназначенный для изменения базовых настроек веб-консоли. Чтобы перейти в настройки, кликните на название настройки или перейдите **Панель управления** → **Параметры сервера**.



Исключить агенты из ICAP — исключает агенты из перехвата трафика на ICAP-сервере.

Записывать просмотр скриншотов в действия администратора — записывает просмотр скриншотов в действия администратора.

Период запуска политик (сек.) — период обработки событий настроенными политиками. Уменьшение параметра повысит нагрузку на сервер.

Параметры расчета риска пользователя: количество дней — задаёт количество дней, в течение которых будут учитываться события пользователя для расчета уровня риска. Доступны значения от 0 до 84, по умолчанию — 14 дней.

Примечание: Для доступа к опции активируйте *Уровень риска*.

Автоматически обновлять имя компьютера — параметр обновляет имя ПК при изменении. Не используйте параметр, если вы используете свои имена в веб-интерфейсе.

Ключ API — в параметре указывается API мастер-сервера.

Мастер сервер — адрес сервера, который используется как master-сервер при синхронизации политик, конфигураций и пользователей.

Email-адрес отправки уведомлений для фильтров/политик — почта для отправки уведомлений для фильтров/политик.

Максимальное время сессии при неактивности пользователя (мин.) — через указанный промежуток времени при неактивной сессии произойдет автоматическое разлогинивание.

Минимальное время активности, необходимое для начала дня (сек.) — события, короче указанного значения до начала дня, игнорируются. Сделано для исключения случайных событий — например, кто-то случайно пошевелил мышь.

Параметры расчета риска пользователя: максимальное значение риска за день — определяет максимальное количество баллов риска, которые могут быть учтены за один день. Доступны значения от 0 до 10 000, по умолчанию — 100.

Примечание: Для доступа к опции активируйте *Уровень риска*.

Автоматически назначать лицензию новым агентам — параметр позволяет отключить автоматическое назначение лицензий новым агентам.

IP-адрес сервера для перенаправления(«none» для отключения) — укажите IP-адрес и порт нового сервера, на который необходимо перевести всех агентов. Порт указывается после двоеточия, например 10.10.11.22:3333. Агенты будут перезапущены и направлены на новый сервер.

Выравнивать громкость звука — при включении параметра выравнивается громкость звука для новых записей.

Доступ к API разрешен — переведите параметр в положение **Да**, если вы хотите разрешить доступ к master-серверу по API для синхронизации.

Автоматически обновлять профиль из AD — при синхронизации профиля пользователя с карточкой AD параметр будет автоматически загружать изменения из AD. Не требует настройки Active Directory — данные отправит агент.

Автоматически назначать лицензию откл. AD пользователям, если включено, иначе отзывать лицензии — автоматически назначает лицензию отключенным в AD пользователям, если выключено — отзывает и не назначает лицензию, даже если пользователь снова активирован.

Конфигурация агента по умолчанию — позволяет выбрать конфигурацию для автоматического назначения новым агентам.

Группировка по умолчанию — отображает группировку для пользователей по заданному значению в опции **Назначение агентов** в конфигурации компьютеров.

Измерение по умолчанию — измерение для отображения в отчетах и при входе в веб-консоль по умолчанию.

- *Компьютеры*,
- *Пользователи*,
- *Пользователи, Полное имя*.

Примечание: Если выбрать опцию *Пользователи, Полное имя*, Конструктор будет по умолчанию открываться на пользователях, а в отчете **Учет рабочего времени** будут отображаться пользователи.

Telegram: Ключ API (токен) — введите ключ бота, который будет отправлять уведомления для пользователей в Telegram.

Видимый режим работы агента — при включении модуля в панели задач отобразится иконка iBatyr Monitor. При первом запуске сервера и при изменении конфигурации появится оповещение «Компьютер находится под наблюдением». Настроить заголовок и текст оповещения можно в конфигурации компьютера в разделе Присутствие на рабочем месте.

Ключ API мастер-сервера — ключ API, который используется на slave-серверах, если использовать данный сервер в качестве master-сервера.

Словарям искать в заголовке окна — при включении модуля поиск по словарям будет автоматически искать ключевые слова в заголовках окон.

Режим slave-сервера — включение параметра переводит сервер в режим работы slave-сервера. После этого сервер копирует политики master-сервера и собирает события без повторной настройки.

Email-адрес для отправки системных уведомлений — почта для отправки системных уведомлений.

Добавлять просмотры отчетов и построение выборок в журнал — параметр позволяет увидеть информацию о построении выбранных отчетов и запросов к БД. Чтобы ознакомиться с информацией, перейдите **Админ** → **Последние действия**.

Распознавание голоса — преобразование записанного звука в текст. Позволяет использовать распознавание в конфигурации агентов по умолчанию.

Статистика включена по умолчанию — параметр включает **Статистику событий** в конструкторе. При отключении параметра по умолчанию будут выводиться все доступные типы событий вне зависимости, есть ли по ним данные или нет.

Формат времени отчетов — позволяет выбрать формат построения отчетов.

Отображать пустые значения — в меню **Анализ** позволяет скрыть события, которые имеют тип **Значение не указано**.

Максимальное количество фактов в уведомлении фильтров — ограничение работает только для отчетов из фильтров при отправке уведомлений в pdf-формате.

Язык по умолчанию — язык веб-интерфейса по умолчанию. Параметр учитывается при отправке уведомлений.

Ширина канала для приема отчетов (байт/сек, 0 — без лимита) — задает максимальную ширину канала для записи онлайн-видео. Для отключения укажите 0.

Ширина канала для записи онлайн видео (байт/сек, 0 — без лимита) — задает максимальную ширину канала для записи онлайн-видео. Для отключения укажите 0.

Примечание: Оба параметра ширины канала работают только для нового механизма присвоения конфигурации. См. **Включение на сервере нового механизма присвоения конфигурации** *в статье Командная строка iBatyr Monitor*.

Полнотекстовый поиск словарей по умолчанию — использование полнотекстового индекса вместо like для поиска словарей, что значительно увеличивает скорость. Но из-за того, что словари рассчитаны на поиск подстрок, могут быть ложные срабатывания и пропуски подсветки.

Измерение приложения в отчетах — измерение для отображения в комбинированном отчете.

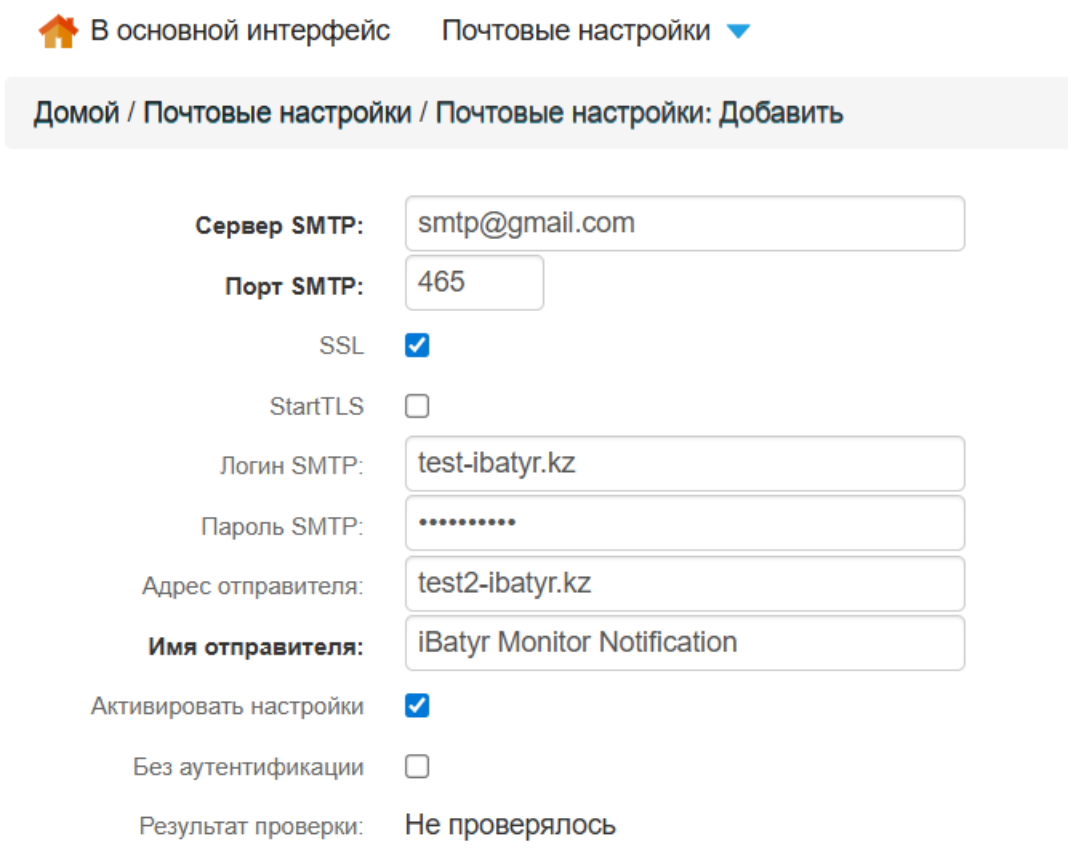
- исполняемый файл,
- описание приложения.

Домен или адрес сервера — имя домена, по которому доступна веб-консоль. Измените параметр при изменении IP-адреса сервера или доменного адреса. Значение должно совпадать с действующим IP или доменным именем сервера iBatyr Monitor. Также этот параметр влияет на IP-адрес сервера, который будет подставляться в ссылках при рассылках уведомлений администраторам системы.

Состояние флажка Запомнить меня на странице логина — выбор флажка **Запомнить меня** при входе в систему.

Почтовые настройки

Почтовые настройки - интерфейс для настройки параметров отправки почты, которая используется для отправки отчетов и уведомлений по настроенным фильтрам. Для перехода в настройки нажмите на название сервера SMTP или добавьте новую учетную запись кнопкой «Добавить».



Введите значения в соответствии со своей почтовой учетной записью.

Например, для учетной записи gmail.com, настройки сервера SMTP будут как на скриншоте выше.

Логин SMTP - Логин от вашей учетной записи **Пароль SMTP** - пароль от вашей учетной записи

Примечание: Для gmail необходимо включить двухфакторную авторизацию и создать пароль приложения. Полученный пароль приложения указать в качестве SMTP пароля.

Почтовая учетная запись должна существовать, быть заранее настроена и работоспособна.

Адрес отправителя (Sender Address) - адрес, который будет указываться в полученных сообщениях в «SMTP MAIL FROM». Используется для случаев когда поле «Login» не содержит корректного адреса электронной почты.

Примечание: Если поле «Адрес отправителя» оставить пустым, то в поле «SMTP MAIL FROM»

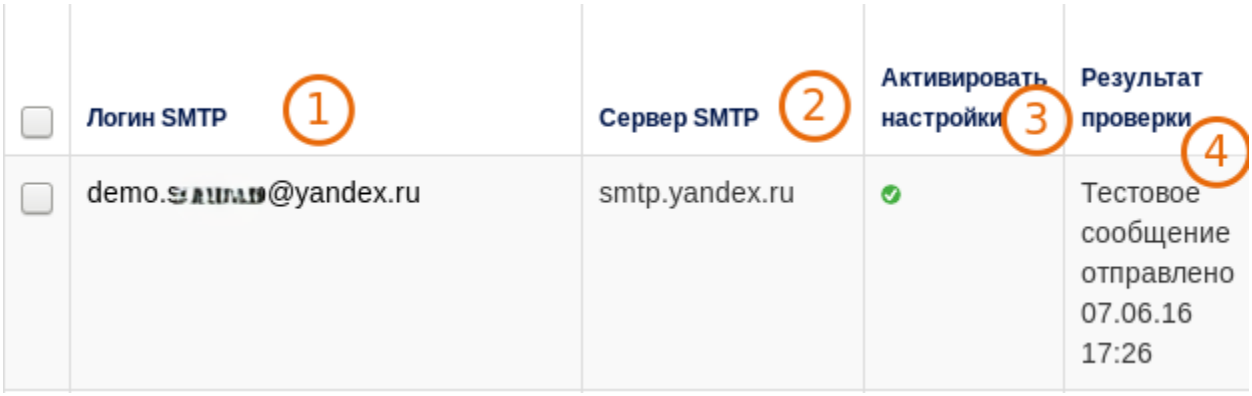
будет подставляться переменная из поля «Логин».

Имя отправителя - имя, от которого придет письмо.

Активировать настройки - обязательный параметр, включающий работоспособность модуля и отправку с данной учетной записи.

Без аутентификации - настройка используется, если на вашем почтовом сервере не используется аутентификация.

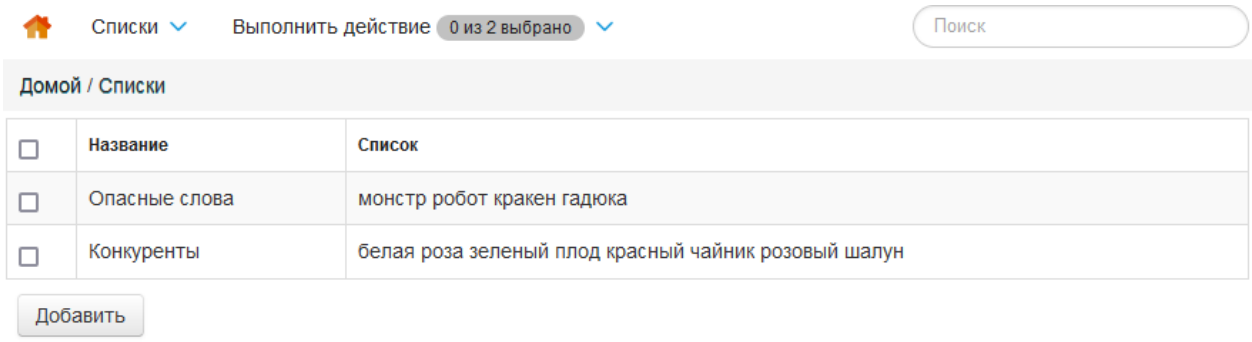
После сохранения почтовой учётной записи можно проверить ее работоспособность нажатием кнопки «Отправить тестовое письмо» на email, указанный в поле «Введите email».



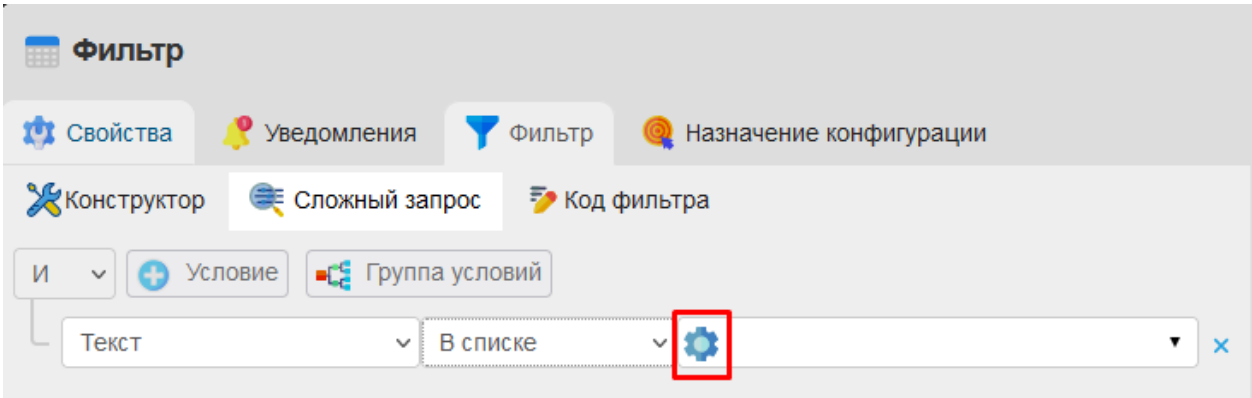
Для удаления учетной записи нажмите на кнопку «Удалить» в настройках учетной записи.

Списки

Данный функционнал позволяет добавить список с набором определенных значений/слов/словосочетаний, которые дальше можно использовать при работе с сложным запросом в фильтрах или политиках.



Список можно также добавить через сложный запрос в фильтрах или политиках нажав на шестеренку.



Примеры использования списков:

Можно создать отедельные списки, которые хотите использовать в разных фильтрах, чтобы не вносить их каждый раз. Например:

- почтовые домены для контроля / исключения контроля

```
ibatyr.kz
gmail.com
list.ru
```

- компьютеры / пользователи

```
user21
miras.k
askar
```

- адресаты для исключения доступа к чувствительной информации в системе при настройке ролей пользователе

Схема работы операторов «В списке/Не в списке»:

При использовании операторов *«В списке/Не в списке»* на текущий момент для 4 измерений используются операторы сравнения **«^» - Содержит**, **«!^» - Не содержит**:

- Приложение -> Заголовок окна (agent_application -> window_title)
- Текст (text_data)
- Переписка -> Все получатели (agent_dialog -> recipients)
- Переписка -> Чаты (agent_dialog -> members)

Для всех остальных измерений используются операторы сравнения **«=» - Равно**, **«!» - Не равно**.

Настройки Active Directory

- *Подключение к Active Directory*
- *Расписание*
- *Группы пользователей с доступом к iBatyr Monitor*
- *Как назначить конфигурацию группе AD*

Раздел **Панель управления – Настройки Active Directory** позволяет:

- задать параметры авторизации на контроллере домена,

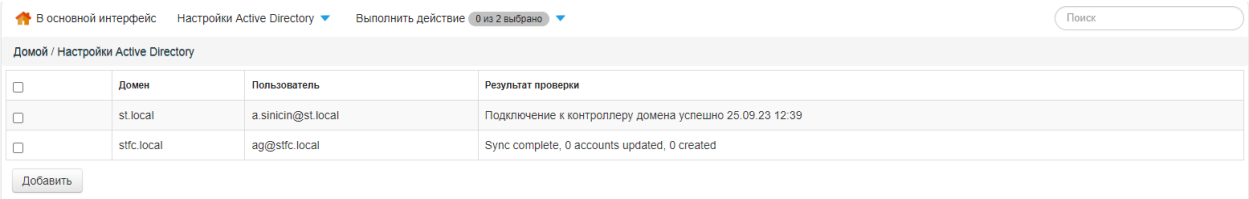
- создать группы пользователей AD, которые смогут входить в веб-интерфейс iBatyr Monitor с помощью своих учетных записей из AD.

На основе авторизационных данных на контроллере домена можно:

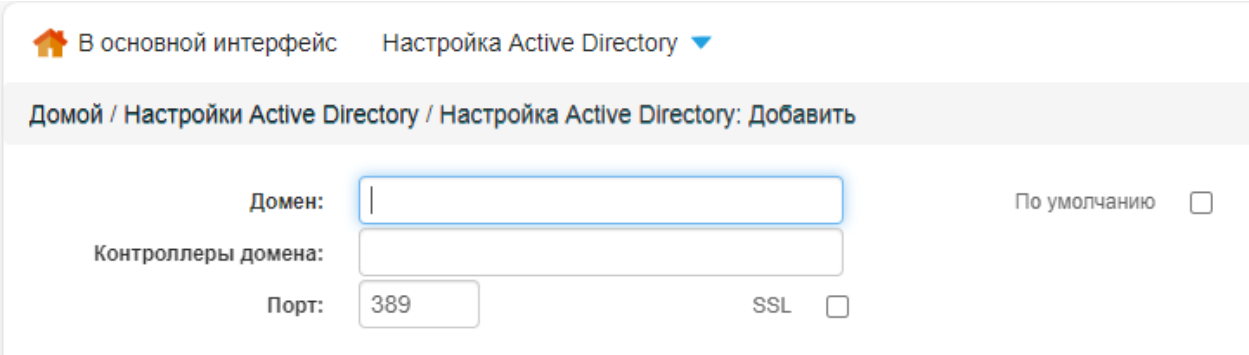
- назначать конфигурации для агентов групп пользователей,
- разрешать доступ к веб-интерфейсу iBatyr Monitor .

Подключение к Active Directory

Чтобы настроить подключение к AD, в разделе **Панель управления** → **Настройки Active Directory** выберите один из доменов или создайте новое подключение с помощью **Добавить**.

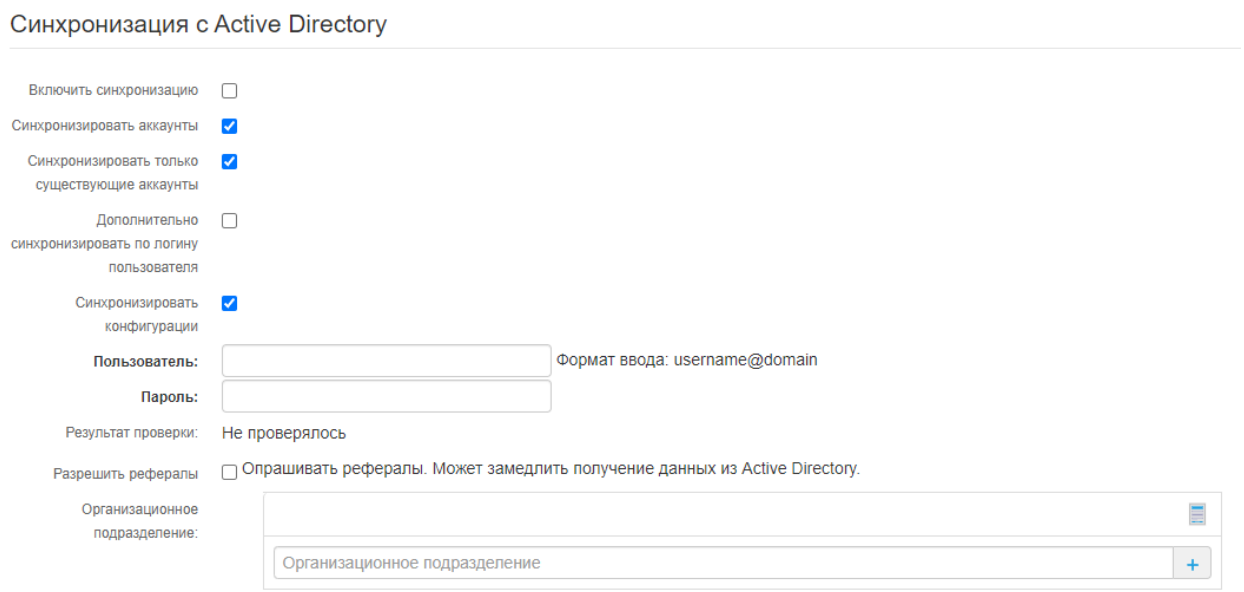


В открывшемся окне задайте основные настройки для подключения.



- **Домен** – имя домена;
- **Контроллеры домена** – IP-адрес или FQDN контроллера домена, если контроллеров домена больше одного, укажите их через запятую;
- **Порт** – порт подключения (389 без использования SSL, 636 – с использованием);
- **SSL** – включает подключение по SSL-протоколу.

В секции **Синхронизация профилей Active Directory** заполните все поля и выберите опции.



- **Включить синхронизацию** — включает синхронизацию с контроллером домена;
- **Синхронизировать аккаунты** — синхронизирует все аккаунты из AD;

> **Предупреждение:** Не используйте одновременно параметры **Включить синхронизацию аккаунтов** и *Автоматически обновлять профиль из AD*. Если включены оба, информация в профиле пользователя может стать некорректной, так как **Автоматически обновлять профиль из AD** получает данные от агента, а **Включить синхронизацию аккаунтов** — из Active Directory

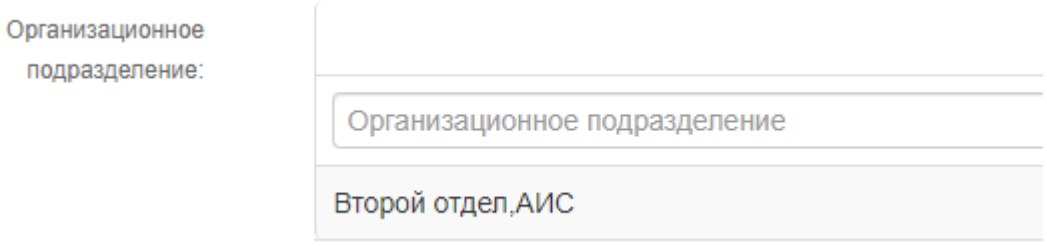
- **Синхронизировать только существующие аккаунты** — синхронизирует данные учетных записей согласно списку **Пользователи** на сервере iBatyr Monitor. Опция не работает, если не включено **Синхронизировать аккаунты**;
- **Дополнительно синхронизировать по логину пользователя** — синхронизирует пользователей по логину из Active Directory, если в ходе синхронизации выявлены аккаунты без SID в поле **GUID**. Включите опцию, если в домене есть пользователи ОС Linux. У таких пользователей в поле **GUID** указаны логины, потому что в Linux отсутствует SID пользователя;

> **Предупреждение:** Если есть аккаунты с одинаковыми логинами, данные пользователей могут некорректно перезаписаться, даже если они находятся на разных поддоменах и имеют разные суффиксы — например, test.user@1example.ru и test.user@2example.ru.

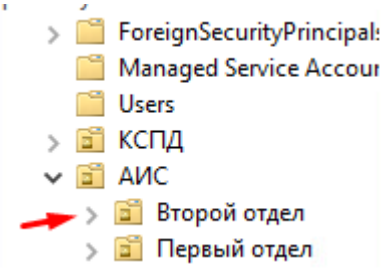
- **Синхронизировать конфигурации** — позволяет назначать конфигурации компьютерам в соответствии с группами в Active Directory;
- **Пользователь** — логин для авторизации на контроллере домена;
- **Пароль** — пароль для авторизации на контроллере домена;
- **Разрешить рефералы** — позволяет опрашивать все контроллеры домена для получения информации о запрошенной учетной записи. Может замедлить получение данных из AD;
- **Организационное подразделение** — подразделение, для которого будет произведена синхронизация.

Особенности работы с настройкой **Организационное подразделение**:

- формат ввода – название подразделения в нижнем регистре с разделителем в виде запятой без пробелов: *organizational,unit*;
- максимальная длина – 255 символов;
- синхронизация проводится только для уже существующих в подразделении аккаунтов, потому что опция **Синхронизировать только существующие аккаунты** учитывает **Организационное подразделение**;
- вложенная папка создается с помощью перечислений названий папок через запятую, начиная с вложенной, например: *Левый,КСПД*.



Результат:



Организационное подразделение игнорируется:

- при пустом поле;
- при авторизации пользователя в iBatyr Monitor – поиск пользователя ведётся по всей AD;
- при назначении **Конфигурации компьютера** из AD;
- *при установке из AD* – поиск ведётся по всей AD.

Расписание

Секция **Расписание** позволяет выбрать периодичность синхронизации:

- Разовая задача,
- С интервалом,
- Ежедневно,
- Еженедельно,
- Ежемесячно.

Включение механизма назначения конфигурации

Начиная с версии 5.4 на сервере доступен новый механизм назначения конфигурации на агентов. Механизм не является обязательным для работы системы, но улучшает скорость взаимодействия агентов и сервера.

Механизм включается командой:

```
ibatyr enable rustsrv
```

Включение механизма меняет способ назначения конфигурации:

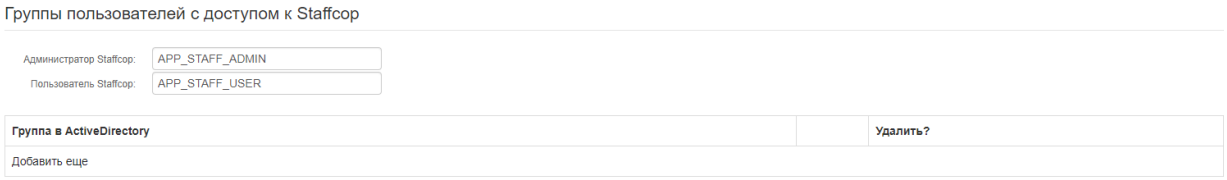
- на агента: просто включите механизм командой и назначьте конфигурацию,
- группу AD: включите механизм и синхронизируйте аккаунты в разделе *Синхронизация профилей Active Directory*, а затем назначьте конфигурацию.

См.также:

Как назначить конфигурацию группе AD

Группы пользователей с доступом к iBatyr Monitor

Начиная с версии 5.2 в iBatyr Monitor можно управлять правами доступа пользователей на основе групп из AD. Помимо предустановленных групп с заданными правами доступа, можно добавить любые другие группы пользователей из AD и назначить им права.



Предустановленные группы пользователей:

- **Администратор iBatyr Monitor: APP_STAFF_ADMIN** – группа в AD, пользователи которой будут получать административный доступ к веб-интерфейсу iBatyr Monitor .
- **Пользователь iBatyr Monitor: APP_STAFF_USER** – группа в AD, пользователи которой будут получать пользовательский доступ к веб-интерфейсу iBatyr Monitor .

Создание новых групп пользователей

Начиная с версии 5.2 можно назначать права неединичным пользователям, а на основе групп из AD. Для этого:

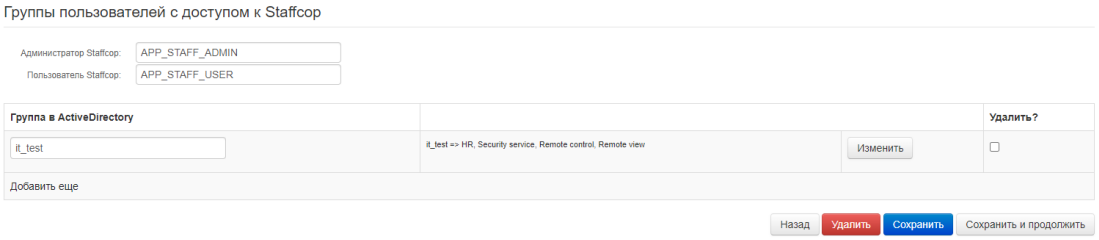
1. Объедините нужных пользователей в группу в AD.

   Примечание: Не используйте запятую в имени группы, так как это может вызвать проблемы с фильтрацией и настройкой прав доступа.

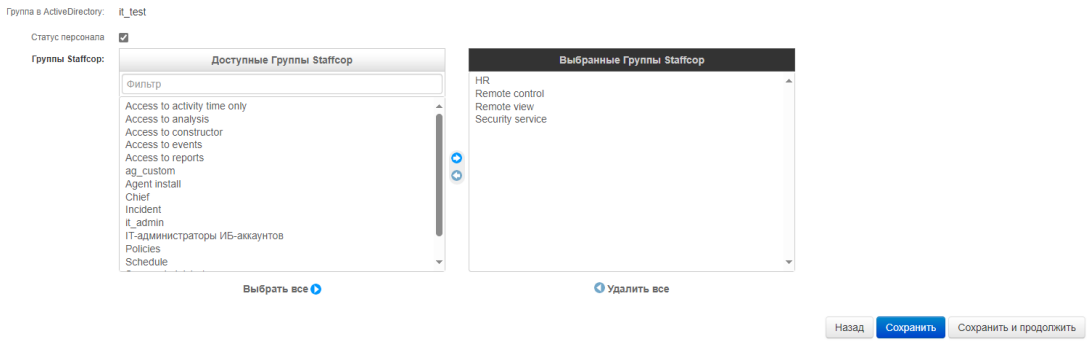
   ---

2. В веб-интерфейсе iBatyr Monitor в разделе **Панель управления** → **Настройки Active Directory** откройте раздел для редактирования или создайте новый.

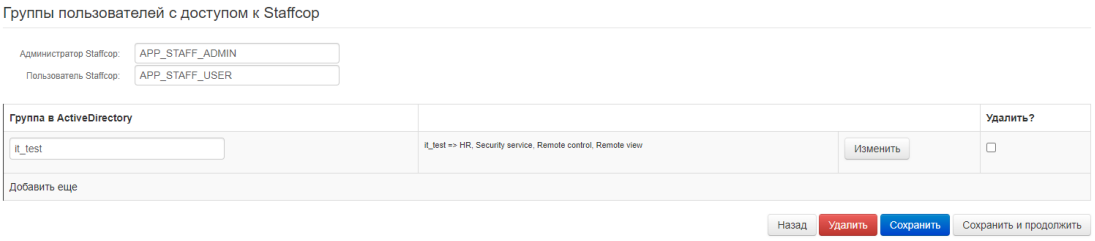
3. В секции **Группы пользователей с доступом к iBatyr Monitor** нажмите кнопку **Добавить ещё**.



4. Укажите имя группы в AD, для которой хотите настроить права доступа.
5. Нажмите **Сохранить**.
6. В открывшемся окне выберите необходимые *группы прав iBatyr Monitor*.



7. После сохранения изменений настроенные права групп будут видны в разделе **Настройки Active Directory**.



Как назначить конфигурацию группе AD

Назначение конфигурации группе в AD позволяет одновременно присваивать конфигурацию множеству пользователей.

Шаг 1. **Создайте группу в AD**:

1. Откройте консоль управления **Пользователями и Компьютерами**.
2. В группе **Computers** (**Компьютеры**) создайте группу, например *ibatyr_full_control*.
3. Добавьте в группу компьютеры для назначения конфигурации.

Шаг 2. **Назначьте конфигурацию на сервере iBatyr Monitor**:

1. Перейдите **Панель управления** → **Настройки Active Directory**.
2. Выберите домен и заполните данные в разделе *Подключение к Active Directory*.

Совет: Для улучшения скорости обработки данных агентов на сервере вы можете включить *механизм назначения конфигурации агенту на сервере*. Перед включением механизма убедитесь, что в разделе *Синхронизация профилей Active Directory* синхронизированы аккаунты.

4. Перейдите в **Панель управления** → **Конфигурация компьютеров** и выберите конфигурацию.
5. Перейдите в раздел **Назначение агентов** и введите в поле **Группы AD** название группы, в нашем случае – *ibatyr_full_control*.
6. Сохраните конфигурацию.
7. В разделе **Админ** → **Глобальная конфигурация** нажмите **Сохранить**.

После синхронизации конфигурация **Усиленный контроль** будет назначена всем рабочим станциям из группы *ibatyr_full_control*. Синхронизация сервера и AD произойдет *по расписанию*.

Запланированные и выполняемые задачи

Запланированные задачи

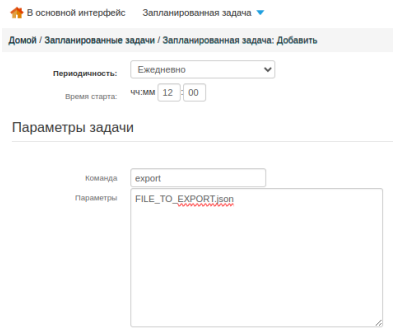
Раздел **Запланированные задачи** позволяет создавать задачи для выполнения *команд iBatyr Monitor*.

При создании задачи можно выбрать:

- команду выполнения,
- параметры команды,
- частоту выполнения.

Чтобы добавить задачу:

1. Перейдите **Панель управления** → **Запланированные задачи**.
2. Нажмите на кнопку **Добавить**.
3. Заполните поля согласно правилам:



4. Перезагрузите сервер, чтобы добавить задачи в расписание:

```
service ibatyr restart
```

Результаты выполнения команд представлены в логах сервера **/var/log/ibatyr/process.log**.

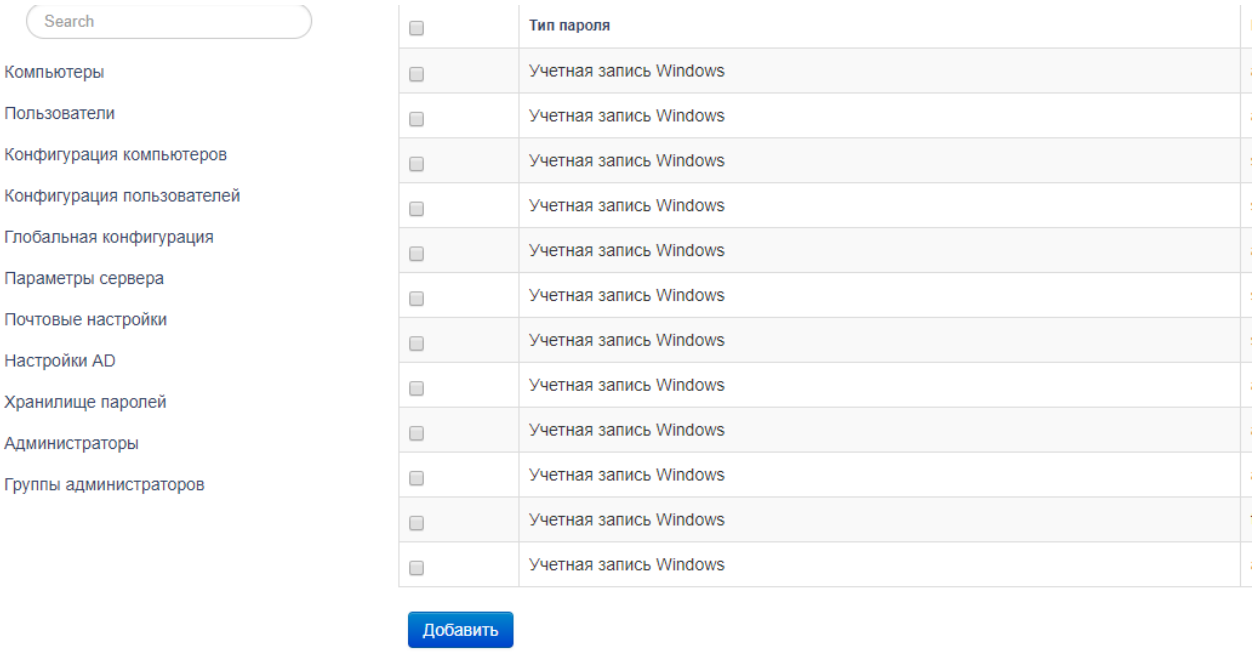
Выполняемые задачи

Здесь отображается список задач, которые были добавлены в **Запланированные**.

По умолчанию в **Выполняемые задачи** добавлены команды:

- *usercard –find-new-only –userstat* — поиск новых карточек сотрудников каждые полчаса,
- *usercard –reinit –userstat** — сбор статистики по карточкам каждую ночь в 01:10.

Хранилище паролей

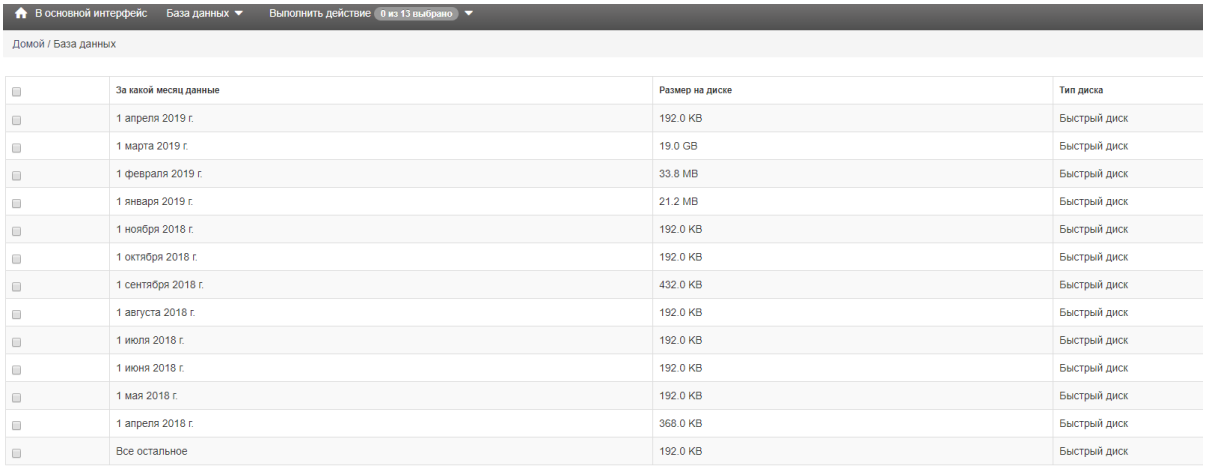


Хранилище паролей служит для сохранения и редактирования паролей, использующихся при установке через веб-интерфейс.

- **Название** - название сохраненного пароля.
- **Пользователь** - имя учетной записи.
- **Пароль** - пароль учетной записи.
- **Тип пароля** - тип пароля учетной записи, по умолчанию - учетная запись Windows.

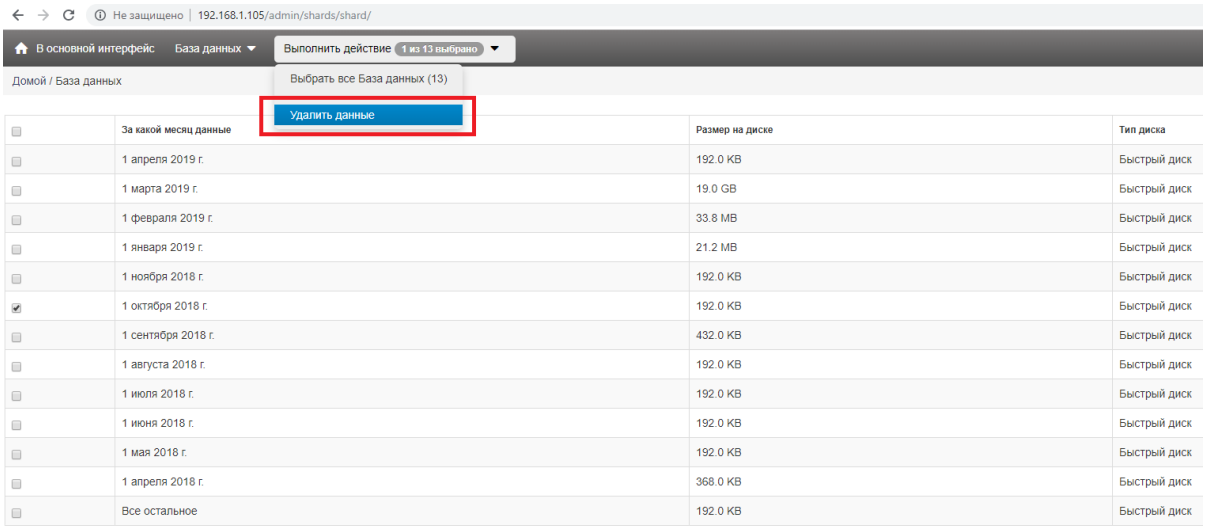
Базы данных

Интерфейс визуально отображает разбиение базы данных по месяцам (шардирование).



	За какой месяц данные	Размер на диске	Тип диска
	1 апреля 2019 г.	192.0 KB	Быстрый диск
	1 марта 2019 г.	19.0 GB	Быстрый диск
	1 февраля 2019 г.	33.8 MB	Быстрый диск
	1 января 2019 г.	21.2 MB	Быстрый диск
	1 ноября 2018 г.	192.0 KB	Быстрый диск
	1 октября 2018 г.	192.0 KB	Быстрый диск
	1 сентября 2018 г.	432.0 KB	Быстрый диск
	1 августа 2018 г.	192.0 KB	Быстрый диск
	1 июля 2018 г.	192.0 KB	Быстрый диск
	1 июня 2018 г.	192.0 KB	Быстрый диск
	1 мая 2018 г.	192.0 KB	Быстрый диск
	1 апреля 2018 г.	368.0 KB	Быстрый диск
	Все остальное	192.0 KB	Быстрый диск

Есть возможность удалить данные за выбранный месяц.



	За какой месяц данные	Размер на диске	Тип диска
	1 апреля 2019 г.	192.0 KB	Быстрый диск
	1 марта 2019 г.	19.0 GB	Быстрый диск
	1 февраля 2019 г.	33.8 MB	Быстрый диск
	1 января 2019 г.	21.2 MB	Быстрый диск
	1 ноября 2018 г.	192.0 KB	Быстрый диск
☑	1 октября 2018 г.	192.0 KB	Быстрый диск
	1 сентября 2018 г.	432.0 KB	Быстрый диск
	1 августа 2018 г.	192.0 KB	Быстрый диск
	1 июля 2018 г.	192.0 KB	Быстрый диск
	1 июня 2018 г.	192.0 KB	Быстрый диск
	1 мая 2018 г.	192.0 KB	Быстрый диск
	1 апреля 2018 г.	368.0 KB	Быстрый диск
	Все остальное	192.0 KB	Быстрый диск

Примечание: Для отображения данного списка у вас должно быть включено *шардирование*

Администраторы

В разделе **Администраторы** представлены учётные записи пользователей веб-консоли. Указаны их имена, признаки активности и наличия прав суперпользователя, а также приведены даты регистрации и последнего визита.

Добавить новую учётную запись можно кнопкой **Добавить**.

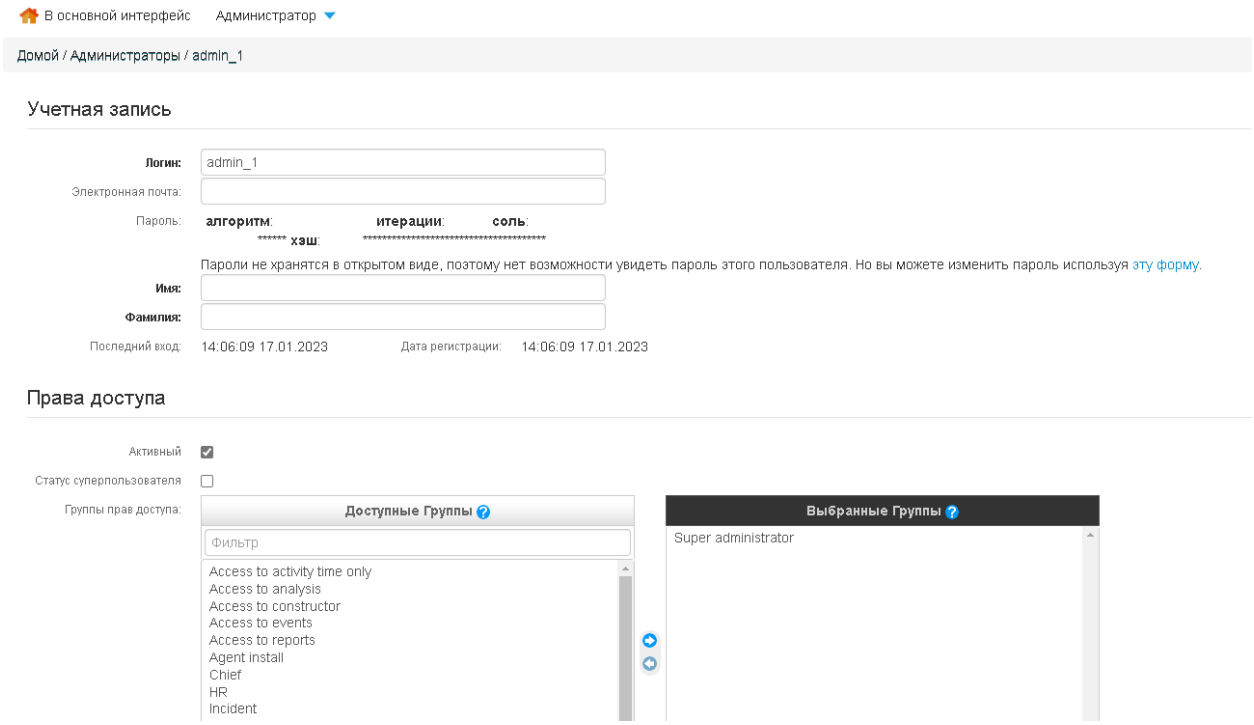
Чтобы удалить учётную запись, активируйте чекбокс возле неё и в выпадающем меню **Выполнить действие** выберите **Удалить**.

Каждой учетной записи можно назначить свою роль и соответствующие права доступа (кроме тех, которые были созданы автоматически при авторизации через Active Directory). В системе есть несколько предустановленных ролей и возможность добавить свои роли с произвольными правами.

Чтобы перейти в форму редактирования учётной записи, выберите запись в столбце **Имя пользователя**.

Редактирование учётной записи

Форма редактирования учётной записи содержит разделы **Учётная запись** и **Права доступа**.



Учетная запись

В разделе **Учётная запись** доступны для редактирования следующие параметры:

tabularytabulary

Поле
Логин
Электронная почта
Имя и **Фамилия**

Пароли в iBatyr Monitor хранятся в зашифрованном виде и не могут быть представлены в явном. В разделе **Учётная запись** представлены параметры шифрования для пароля и приведена ссылка для его изменения.

В этом же разделе представлены дата последнего входа и дата регистрации пользователя - поля **Последний вход** и **Дата регистрации** соответственно.

Права доступа

Раздел **Права доступа** позволяет назначать пользователю статусы, присваивать роли и открывать доступ к определённым фильтрам, отчётам и аккаунтам.

Статусы пользователя представлены двумя опциями:

- **Активный** - служит для отключения пользователя вместо его удаления; в остальных случаях эта опция должна быть включена для корректной работы учётной записи;
- **Статус суперпользователя** предоставляет пользователю все права без явного их назначения.

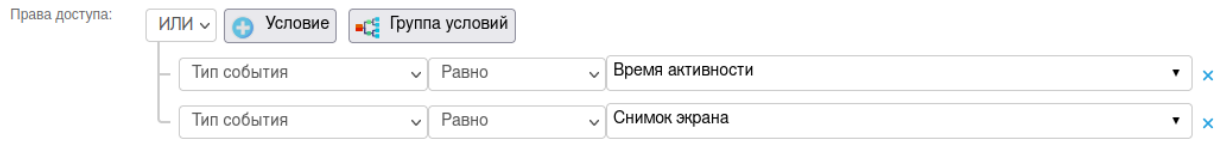
В разделе **Группы прав доступа** пользователя можно добавить в одну или несколько групп, для которых заранее настроены права и доступы:

Группа	К чему открывает доступ
Access to activity time only	Только просмотр событий «время активности» и некоторых отчетов. Остальные типы событий будут недоступны.
Access to analysis	Доступ к отчетам в меню «Анализ».
Access to constructor	Доступ к конструктору, в том числе и при изменении фильтра. Добавьте эту роль пользователю, чтобы открыть ему доступ к Конструктору.
Access to events	Доступ к линзе событий и представлению событий в виде списка, таблицы и т.д. Добавьте эту роль пользователю, чтобы открыть ему доступ к Событиям.
Access to reports	Разрешает просматривать отчеты (скрывает и открывает меню **Отчеты** в представлении).
Agent install	Пункты меню **Панель управления** и редактирование компьютеров, в том числе - конфигураций.
Chief	Все события и отчеты, **Конструктор**. Доступ в административную часть закрыт.
HR	Только отчеты и статистические данные. К событиям и в административную часть доступа нет.
Policies	Редактирование политик.
Remote view	Подключение к удаленному рабочему столу пользователя только для просмотра.
Remote control	Подключение к удаленному рабочему столу пользователя для просмотра и перехвата управления.
Schedule	Отчеты «Учет времени», меню «Администрирование - Рабочее расписание», «Календарь».
Security service	«Панель управления»: • Пользователи; • Компьютеры; • Конфигурация компьютеров; • Конфигурация пользователей; • Приложения; • Файлы. «Администрирование»: • Настройки расписания; • Настройки календаря. Ограничен доступ к функционалу «Анализа» и «Отчётов», доступ к событиям, меню «Создать» и, частично, к «Анализу» через «Карточку пользователя».
System administrator	Только «УРВ-отчёты». «Панель управления»: • Запланированные задачи; • База данных; • Хранилище паролей. «Администрирование»: • Консоль терминала; • Завершить все сеансы работы. Нет доступа к собранной информации и произошедшим событиям.
Super administrator	«Панель управления»: • Запланированные задачи; • База данных; • Хранилище паролей; • Администраторы; • Группы администраторов.

В разделах **Доступ к фильтрам**, **Доступ к аккаунтам** и **Доступ к компьютерам** можно выбрать фильтры, политики, отчеты, аккаунты и компьютеры, которые будут доступны для учетной записи.

Примечание: Если ни одного ограничивающего отчета не выбрано, для просмотра доступны все возможные отчеты.

В разделе **Права доступа** можно настроить доступ к событиям по определённым правилам. Для этого используется инструмент, аналогичный сложному запросу в свойствах фильтра.

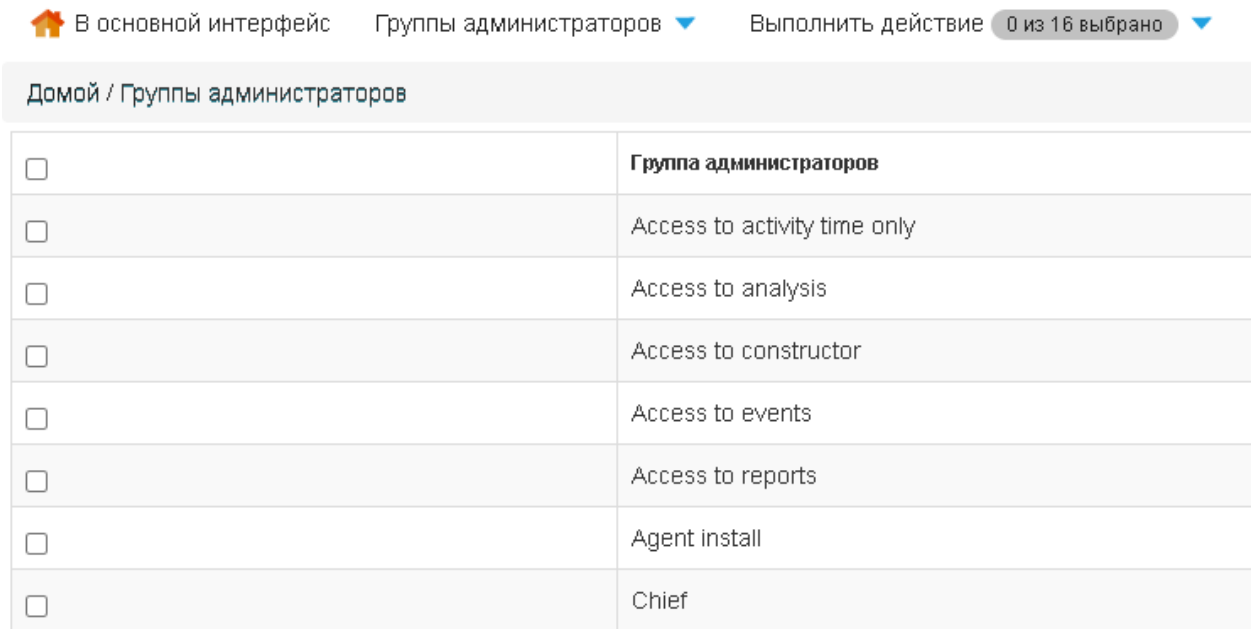


Для учётных записей, созданных через Active Directory, важно учитывать следующие особенности:

- учётная запись пользователя домена имеет доступ только к событиям по имени своей учётной записи;
- учётная запись администратора домена имеет полный доступ к веб-интерфейсу сервера iBatyr Monitor наравне с пользователем «admin».

Группы администраторов

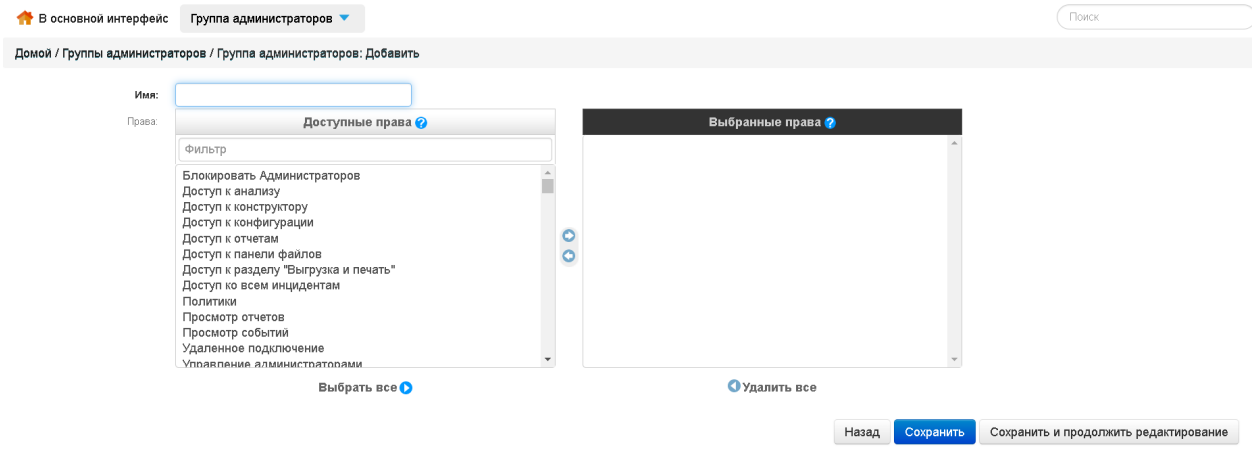
Раздел предназначен для создания, редактирования и удаления групп администраторов.



Создание группы администраторов

Чтобы создать новую группу, нажмите кнопку **Добавить** под списком групп администраторов.

В открывшемся окне задайте имя новой группы и выберите права для неё из приведённого списка.

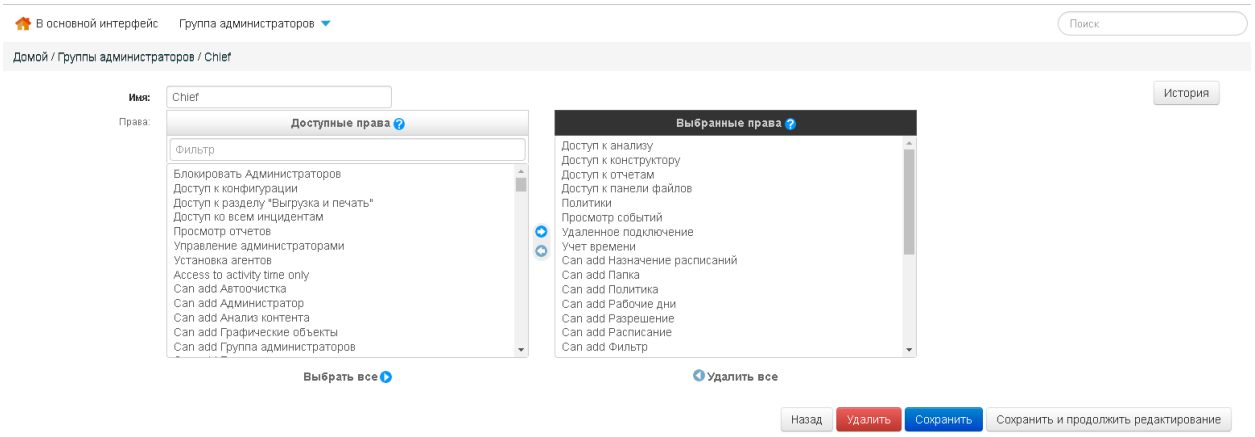


Редактирование группы

Чтобы отредактировать группу администраторов, выберите её название из списка.

В окне редактирования можно изменить название группы, просмотреть текущие права, добавить новые или удалить существующие.

Вы можете добавить новое разрешение или ограничить доступ с помощью конструктора Права доступа.

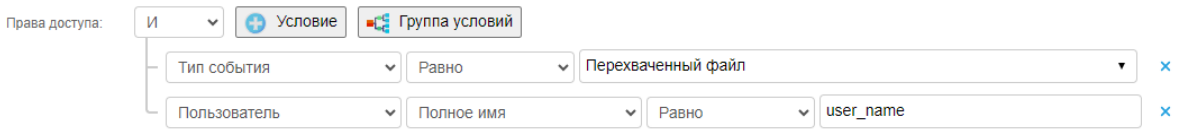


Пример: ограничение права доступа для группы

Воспользуйтесь **Правами доступа** для настройки доступа к событиям у всей группы, а не для каждого администратора в отдельности.

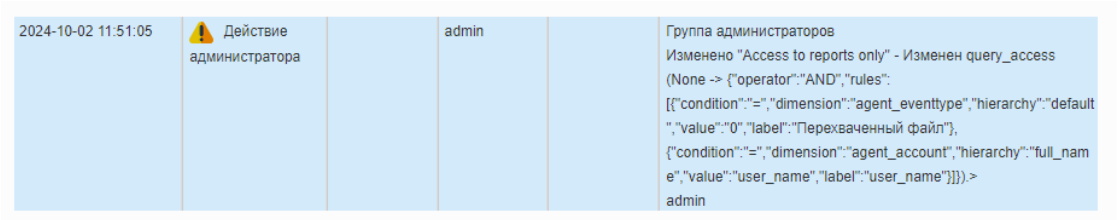
Чтобы ограничить доступ группы к событиям **Перехваченный файл** для пользователя *user_name*, в конструкторе **Права доступа**:

1. Нажмите +**Условие**.
2. Установите значения: **Тип событий** — **Равно** — **Перехваченный файл**.
3. Выберите логический оператор **И**.
4. Добавьте новое условие: **Пользователь** — **Полное имя** — **Равно** — *user_name*.



После сохранения настройки администраторы группы будут видеть только события типа **Перехваченный файл** для пользователя *user_name*.

Все изменения прав доступа группы администраторов отображаются в **Действиях администратора**.



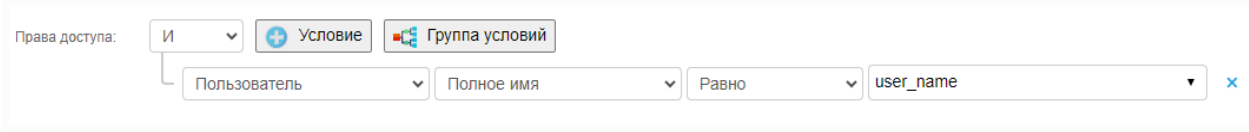
Пересечение прав доступа

Пересечение прав — это ситуация, когда учитываются как личные права администратора, так и права групп, к которым он принадлежит. Возможны несколько вариантов пересечения прав.

Администратор имеет личные права и права группы

Если у администратора есть свои права и права группы, они комбинируются через логический оператор **И**. Сервер предоставляет доступ только при выполнении всех условий одновременно.

Условия: администратор имеет доступ к событиям пользователя *user_name*:



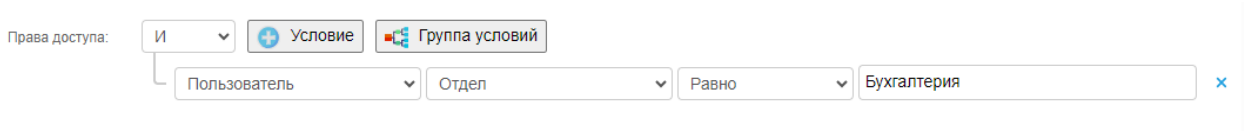
Кроме этого, он состоит в группе, которая видит только события типа **Снимок экрана**.

Результат: администратор видит только снимки экрана *user_name*.

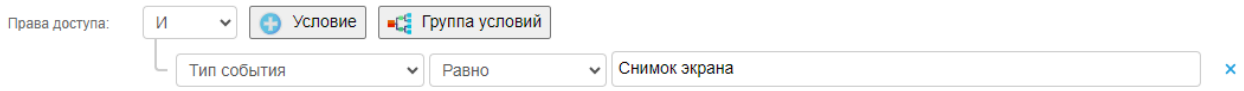
Администратор состоит в нескольких группах

Если администратор входит в несколько групп, права комбинируются через логическое **ИЛИ**. Сервер предоставляет доступ, если выполняется хотя бы одно из условий.

Условия: администратор состоит в *Группе 1* с доступом к событиям отдела *Бухгалтерия*:



Также он относится к в *Группе 2* с доступом к событиям типа **Снимок экрана**:



Результат: администратор видит события пользователей из отдела Бухгалтерия и события типа Снимок экрана для всех пользователей.

Удаление группы

Удалить выбранную группу можно двумя способами:

1. В списке групп чекбоксом выберите название группы и в меню **Выполнить действие** нажмите **Удалить выбранные Группы администраторов**.
2. В окне редактирования группы нажмите кнопку **Удалить**.

4.2.3 Карточка сотрудника

- *Активация карточки сотрудника*
- *Интерфейс карточки сотрудника*
- *Сводная карточка сотрудников*
- *Консольные команды*

Карточка сотрудника — раздел веб-интерфейса, в котором собрана вся информация о сотрудниках, зарегистрированных в системе iBatyr Monitor.

Карточка сотрудника позволяет:

- ускорить процесс сбора данных о сотруднике;
- улучшить анализ продуктивности сотрудника;
- обнаружить аномалии в работе сотрудника;
- ускорить процесс расследования инцидентов, в которых сотрудник выступает фигурантом;
- облегчить настройку системы в зависимости от действий конкретного пользователя.

Активация карточки сотрудника

По умолчанию функциональность карточки сотрудника не активирована. Чтобы карточка сотрудника стала доступна в веб-интерфейсе:

1. Откройте конфигурационный файл сервера **/etc/ibatyr/config**.
2. Добавьте в **config** параметр **ENABLE_USERCARD = True**.
3. Сохраните изменения.
4. Перезапустите сервер командой:

```
ibatyr restart
```

5. Добавьте карточку в **Запланированные задачи**:

```
ibatyr migrate usercard
```

После этого к ней можно будет применять *команды* для обновления и сбора статистики.

6. Заполните карточку данными сотрудника:

```
ibatyr usercard --reinit --userstat
```

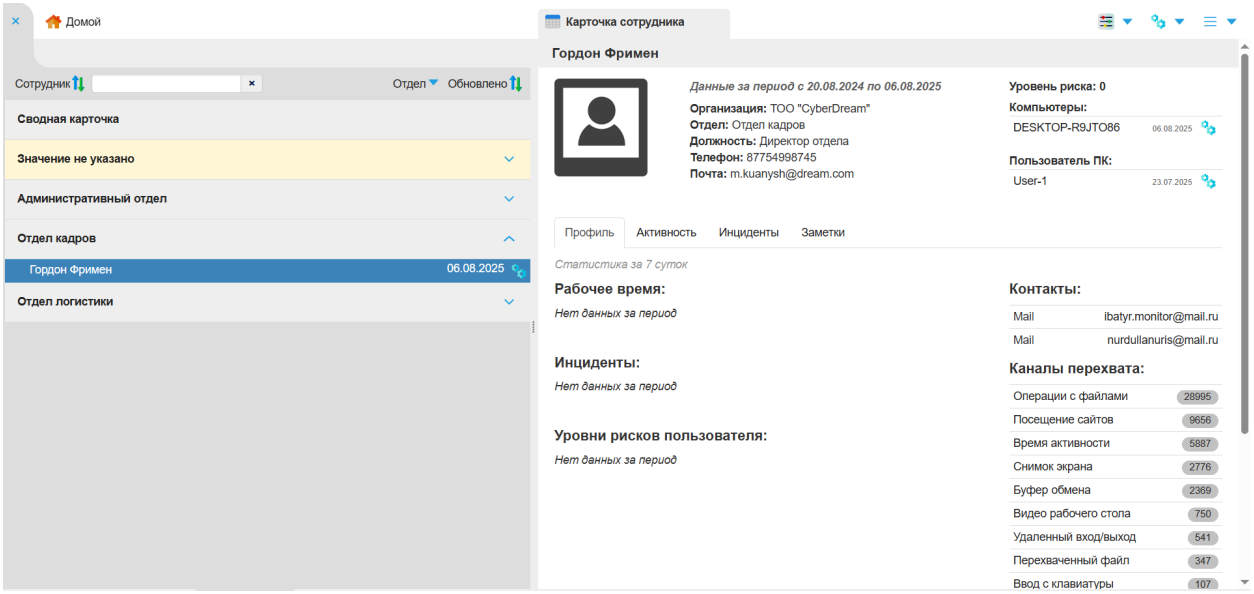
Команда *ibatyr usercard –reinit –userstat* не обновляет *сводную карточку*, для этого добавьте ключ *–summary*:

```
ibatyr usercard --reinit --userstat --summary
```

Интерфейс карточки сотрудника

После активации карточки сотрудника в Конструкторе появится новая вкладка **Сотрудники**.

Карточки подтянутся автоматически при следующем обновлении, которое по умолчанию *производится каждые полчаса согласно Запланированным задачам*.

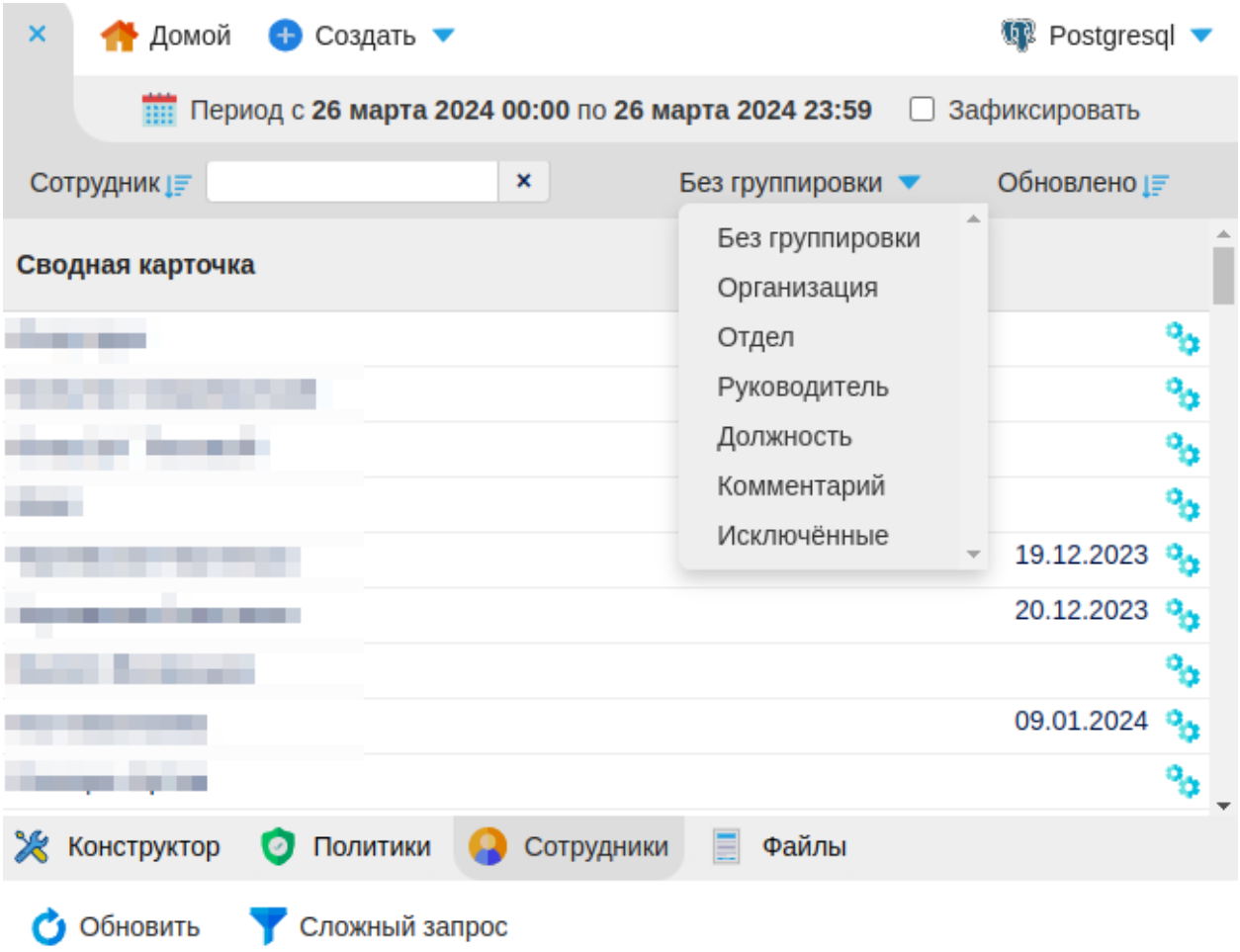


Список сотрудников

При переходе на вкладку **Сотрудники** в левой части экрана появится *сводная карточка* и список карточек сотрудников.

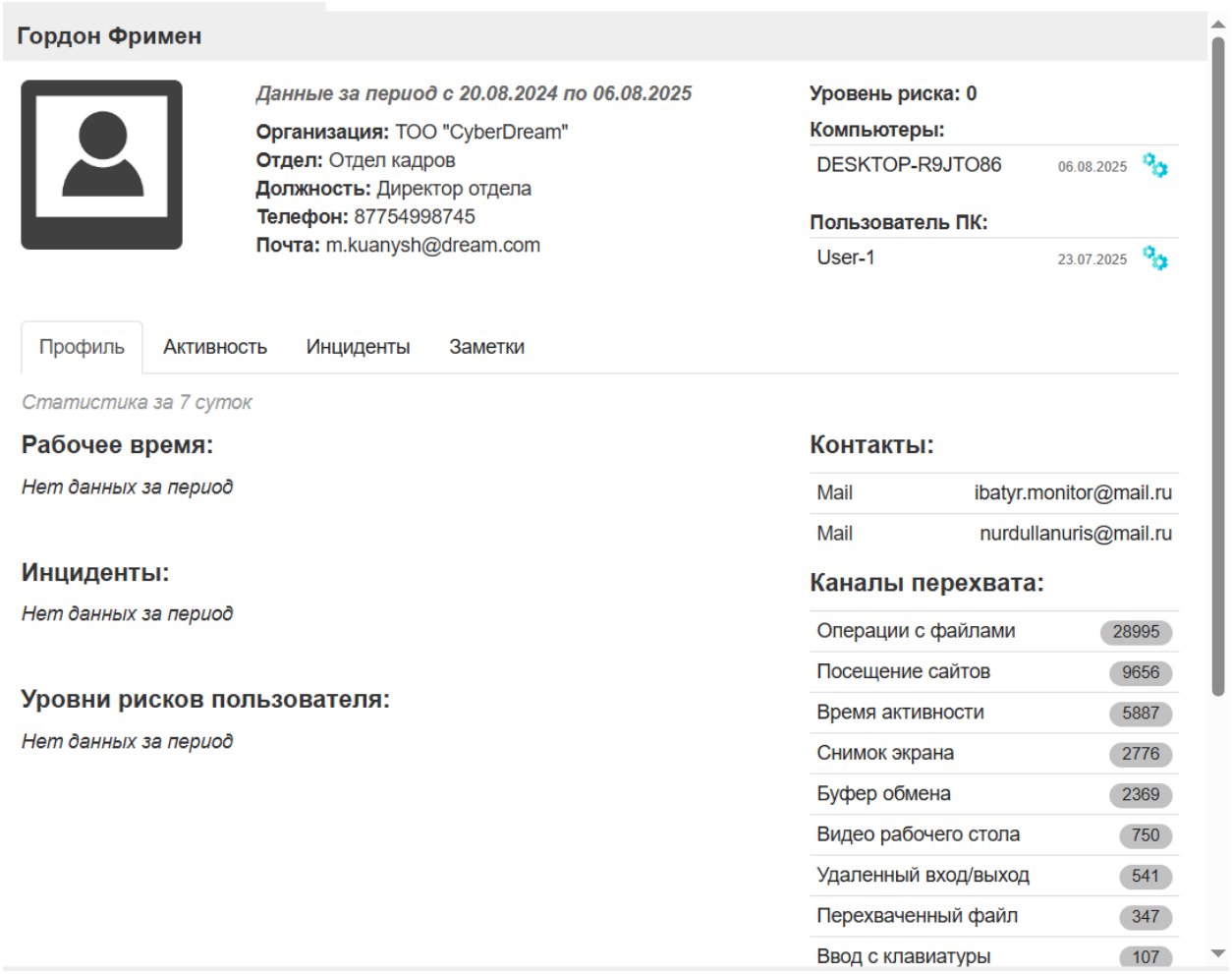
Группировку карточек можно настроить:

- по организации;
- отделу;
- руководителю;
- должности сотрудника;
- указанному комментарию в карточке;
- удаленным карточкам с помощью группы **Исключенные**.



Карточка сотрудника

Кликните на имя сотрудника, чтобы открыть карточку.



В карточке сотрудника представлены:

- данные о сотруднике из Active Directory (имя, подразделение, руководитель, почта);
- компьютеры, к которым привязан сотрудник;
- данные о последней активности сотрудника;
- события, зарегистрированные iBatyr Monitor;
- информация об активности сотрудника;
- инциденты, в которых сотрудник выступает фигурантом.

Примечание: Данные представлены за последний календарный год.

Чтобы удалить карточку:

1. Нажмите на шестеренку рядом с именем сотрудника.
2. Нажмите **Удалить**.

Чтобы восстановить карточку:

1. Нажмите на список **Без группировки**.
2. Выберите **Исключенные**.
3. Нажмите на шестеренку рядом с именем сотрудника.
4. Нажмите **Восстановить**.

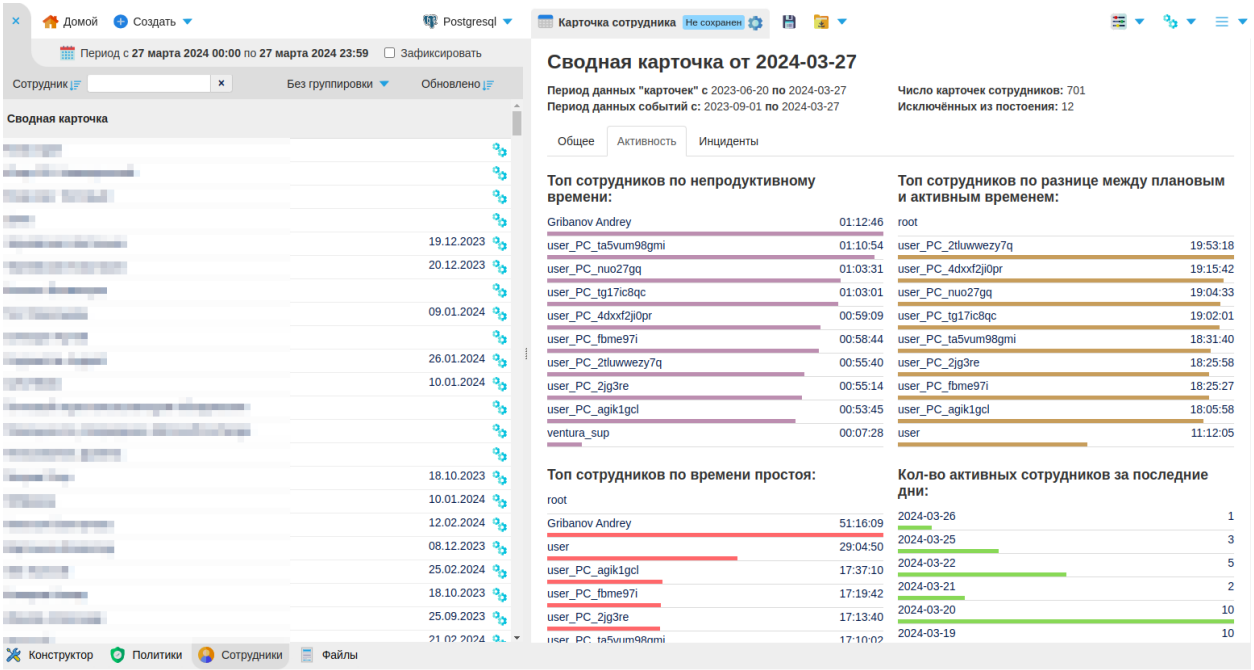
Сводная карточка сотрудников

Добавлено в версии 5.4.

Сводная карточка автоматически собирает данные о деятельности сотрудников и инцидентах за месяц в виде компактных отчетов без предварительной настройки фильтров. Вам достаточно открыть карточку, чтобы получить быстрый доступ к обзорной информации.

Примечание: Удалить сводную карточку нельзя.

Карточка находится на верху списка во вкладке **Сотрудники**:



В шапке карточки расположена информация:

- **Период данных карточек** — временной интервал записи событий в карточке;
- **Период данных событий** — временной интервал записи событий в системе;
- **Число карточек сотрудников** — количество карточек;
- **Исключённых из построения** — количество зарегистрированных пользователей без карточек.

Отчеты расположены во вкладках:

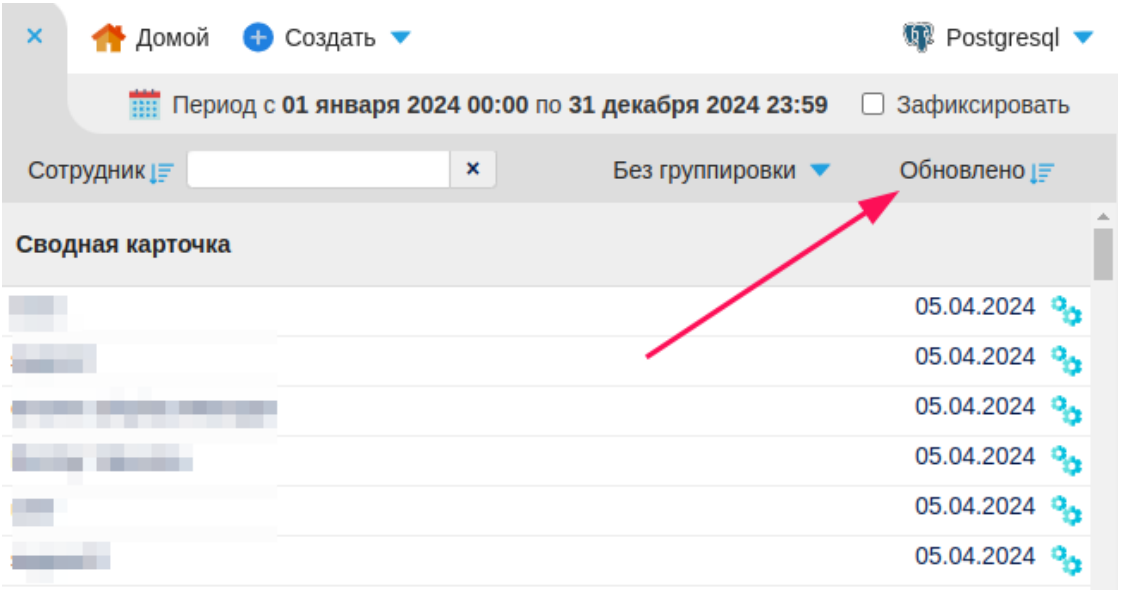
Управление карточками

Добавлено в версии 5.4.

Данные в сводной карточке и в карточках сотрудников можно обновить.

Чтобы обновить карточки:

1. Нажмите на кнопку **Обновить** в панели над списком карточек:



2. Готово! В карточки подтянутся последние данные по сотудникам.

Примечание: Если администратор удалил политику после обновления карточки, название политики изменится на *unknown*.

В сводной карточке возможен переход к деталям:

- клик на ФИО сотрудника открывает карточку сотрудника;
- клик на события позволяет просмотреть в конструкторе события, отфильтрованные по данным из сводной карточки.

Консольные команды

Для работы с карточками сотрудников из консоли сервера используется команда:

```
ibatyr usercard --[parameter] 'user_name'
```

Здесь **parameter** — один из параметров команды; **user_name** — имя пользователя, для которого была создана карточка.

Параметры команды **usercard**:

tabularytabulary

Параметр
userstat
reinit
find-new-only
period
userstat-only

Основные особенности команды **usercard**:

- параметр **user_name** не является обязательным — без указания имени конкретного пользователя команда будет выполнена для всех карточек сотрудников;
- статистика по рабочему времени и инцидентам собирается за последние 7 дней вне зависимости от значения, указанного в параметре **period**;
- по умолчанию в *Запланированные задачи* добавлены команды:

```
usercard --find-new-only --userstat (каждые полчаса)
usercard --reinit --userstat (каждую ночь в 01:10)
```

Примеры использования команд

Добавить в карточку пользователя **Иванов Иван** статистику за последний месяц:

```
ibatyr usercard --userstat --period=`1 month` 'Эммануель Макрон'
```

Создать заново все карточки сотрудников и собрать по ним статистику:

```
ibatyr usercard --reinit --userstat
```

4.2.4 Менеджер ВНИ

Содержание

- *Менеджер ВНИ*
  - *Активация менеджера ВНИ*
  - *Работа с менеджером ВНИ*
    - *Общие настройки*
    - *Настройка прав для отдельного ВНИ*
    - *Настройка групп ВНИ*
  - *Уведомление для администратора*
  - *Теневые копии*

Менеджер внешних носителей информации (**ВНИ**) — подключаемый компонент, который позволяет комплексно управлять парком съёмных носителей информации.

Менеджер ВНИ позволяет:

- управлять правами доступа к отдельным ВНИ;
- задавать режим доступа к ВНИ по умолчанию;
- выдавать права на доступ к ВНИ отдельным пользователям.

Активация менеджера ВНИ

Компонент **Менеджер ВНИ** активируется через платный или тестовый ключ. Активируйте сервер ключом, который включает в себя компонент **Менеджер ВНИ**. После этого менеджер ВНИ станет доступен на сервере. Доступ к носителям информации регулируют заданные в Менеджере ВНИ права.

Примечание: По умолчанию для всех незарегистрированных устройств настроены права на чтение и запись.

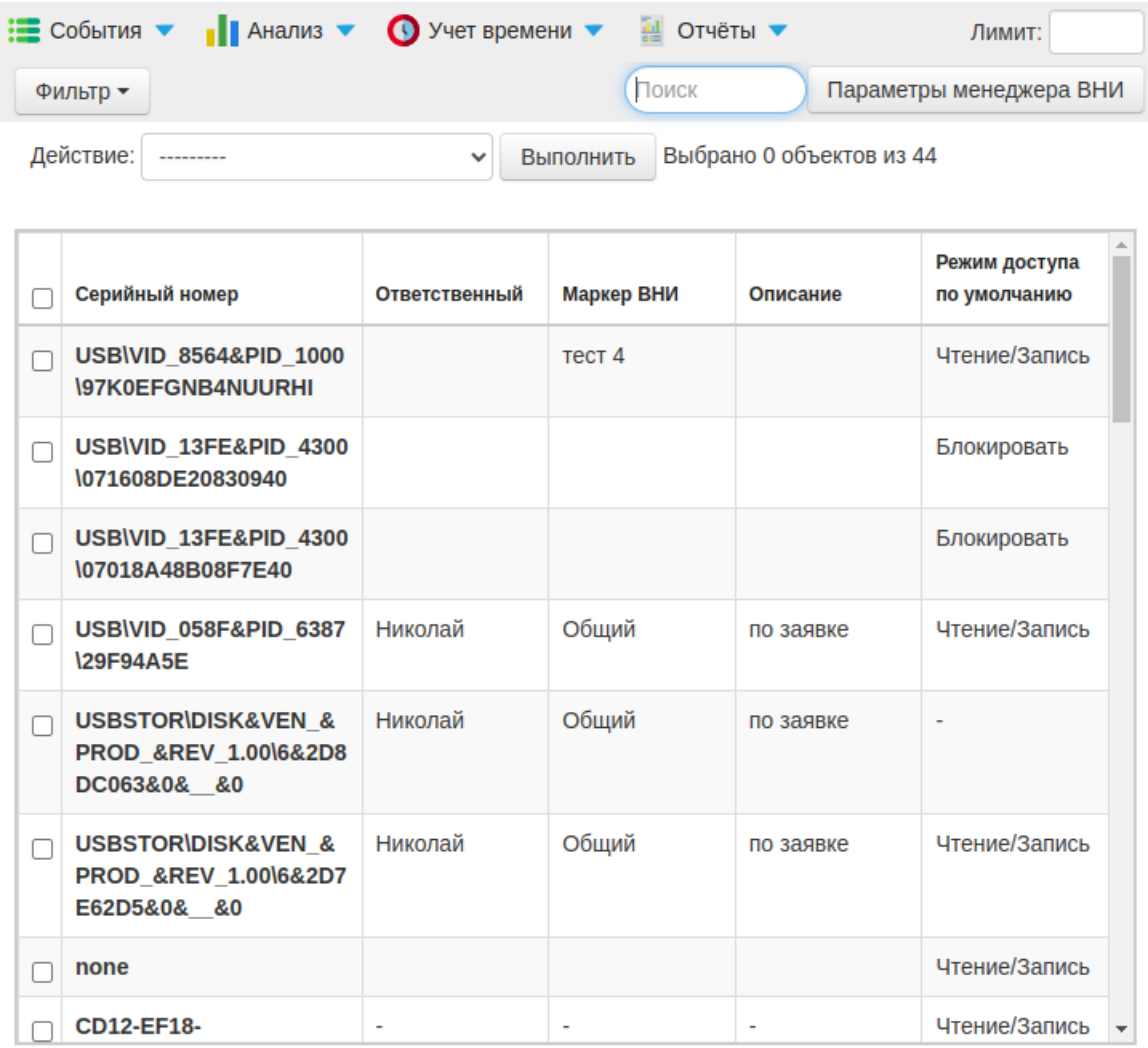
После активации и настройки агент будет передавать на сервер события:

- Внешние диски,
- Файловые операции,
- Перехваченные файлы,
- Устройства.

Работа с менеджером ВНИ

Чтобы открыть менеджер ВНИ, в разделе **Администрирование** выберите пункт **Менеджер ВНИ**.

Откроется список всех зарегистрированных в системе iBatyr Monitor ВНИ.



Для каждого ВНИ указаны:

- **Серийный номер** — уникальный идентификатор;
  - агент сохраняет идентификатор в нижнем регистре в событиях **Внешние диски**, **Файловые операции**, **Перехваченный файл**;
  - если у ВНИ нет идентификатора, агент передает значение *none*.
- **Ответственный** — отвечающий за устройство сотрудник;
- **Маркер ВНИ** — тег для группировки ВНИ, например «Аналитика» или «Отдел продаж»;
- **Описание** — дополнительная информация об устройстве;
- **Режим доступа по умолчанию** — начальные права доступа для устройства, например **Только для чтения**.

Общие настройки

Для общей настройки нажмите в правом верхнем углу **Параметры менеджера ВНИ**.

Уведомления для пользователя

Примечание: Уведомления доступны только для Linux-агента.

В разделе **Сообщение пользователю о блокировании** добавьте сообщения для пользователя в поля:

- **Попытка записи в режиме Только чтение** — сообщение при попытке записи на ВНИ в режиме **Только чтение**.
  - В текущей реализации из-за особенностей архитектуры Linux пользователь получает это сообщение при подключении устройства в режиме **Только чтение**. При попытке записи пользователь увидит системное сообщение о недопустимой файловой операции.
- **Полная блокировка устройства** — пользователь увидит это сообщение при блокировке устройства.

Агент отправляет уведомление раз в минуту, чтобы избежать чрезмерного количества уведомлений. Если в течение минуты после первого уведомления пользователь снова попытается записать файл, новое уведомление не появится.

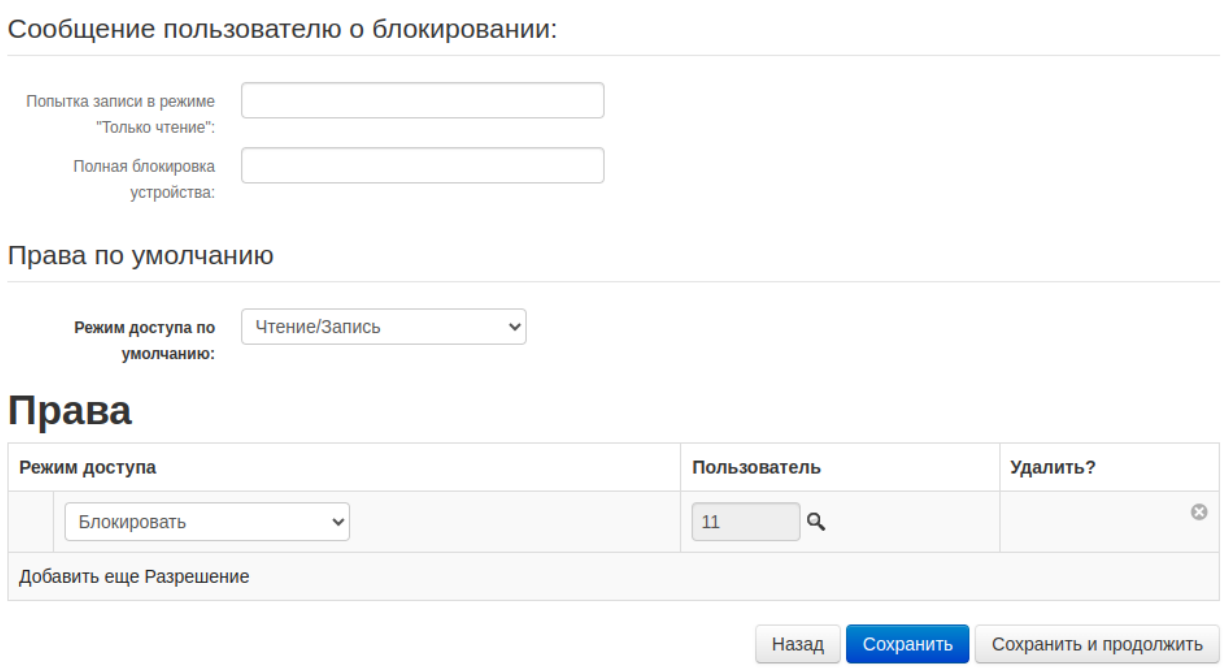
Права по умолчанию ко всем ВНИ

Настройте общие права в разделах:

- **Права по умолчанию** — ко всем устройствам,
- **Права** — ко всем устройствам для конкретного пользователя.

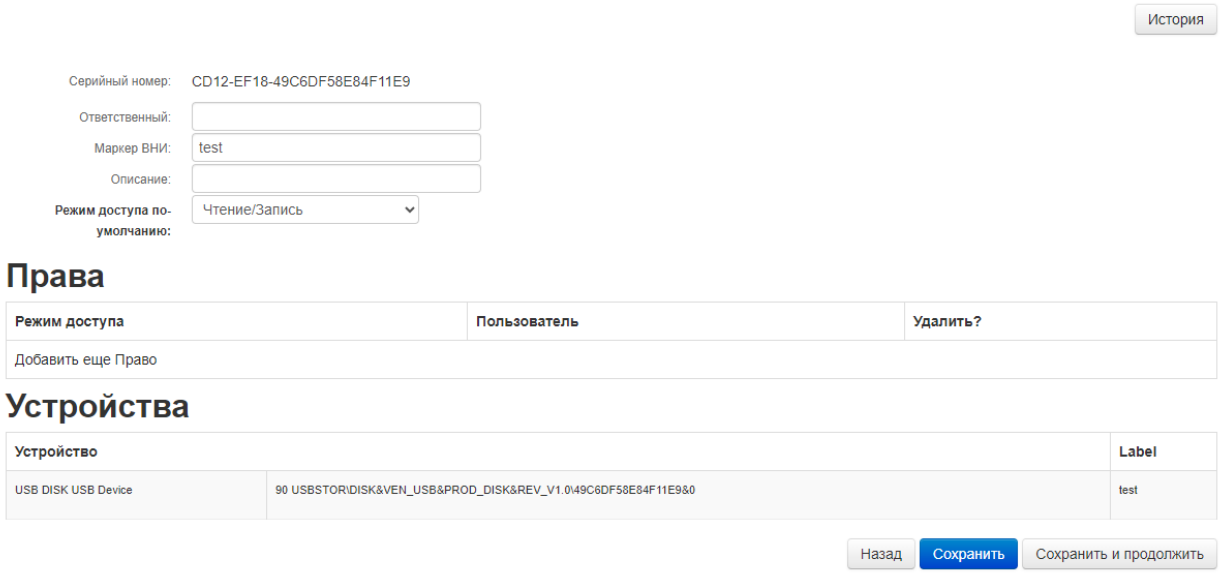
Для настройки выберите в списке право:

- Чтение/запись,
- Блокировать,
- Только чтение.



Настройка прав для отдельного ВНИ

Для настройки доступа выберите ВНИ из списка.



Заполните поля:

- **Ответственный** — сотрудник, отвечающий за ВНИ;
- **Маркер ВНИ** — признак для группировки ВНИ при создании отчётов;
- **Описание** — детальное описание конкретного ВНИ;
- **Режим доступа по умолчанию** — права доступа к ВНИ по умолчанию.

Права пользователя

В разделе **Права** укажите права доступа к ВНИ для конкретного пользователя.

Например, по умолчанию для ВНИ можно установить режим **Только чтение**, а в разделе **Права** разрешить **Чтение/Запись** для администраторов.

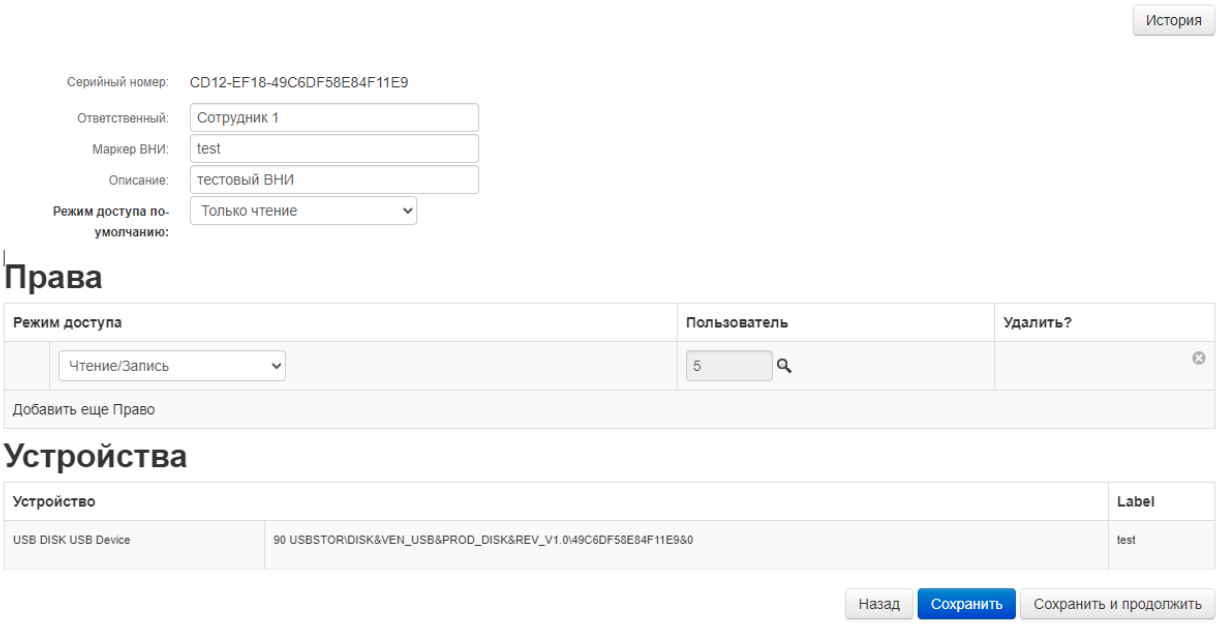
Устройства

При подключении одного и того же ВНИ к разным компьютерам ему могут быть присвоены разные идентификационные номера. В разделе **Устройства** приведены все идентификационные номера выбранного ВНИ.

Пример настройки прав

Чтобы открыть ВНИ **Только для чтения** для всех пользователей и разрешить **Чтение и запись** одному из них:

1. Перейдите в раздел **Администрирование** → **Менеджер ВНИ**.
2. В открывшемся окне выберите ВНИ.
3. В окне настроек в строке **Режим доступа по умолчанию** установите **Только чтение**.
4. В разделе **Права** выберите **Добавить еще Право**.
5. Укажите **Чтение/Запись**.
6. Выберите пользователя, для которого будет актуально разрешение.
7. Сохраните настройки.



Настройка групп ВНИ

Чтобы настроить группу ВНИ:

1. Выберите ВНИ из списка.
2. В строке **Действия** выберите **Задать измерения**.
3. В открывшемся окне укажите параметры: **Ответственный**, **Маркер ВНИ** , **Описание** .
4. Сохраните изменения.
5. Укажите идентичные настройки для остальных устройств группы.

Уведомление для администратора

Примечание: Уведемление для администратора работает только на Linux-агентах.

Агент автоматически отправляет уведомления на сервер при блокировке устройства. Уведомления содержат информацию:

- о времени блокировки,
- пользователе,
- агенте,
- уникальном номере ВНИ.

Уведомление при записи дополнительно содержит информацию о файле, который пользователь пытался записать.

Чтобы посмотреть уведомления:

1. Во вкладке **Конструктор** выберите **Уведомления**.
2. Выберите в списке уведомления **Заблокировано подключение ВНИ**.
3. Уведомления отобразятся в таблице в правой части экрана.

Теневые копии

Windows- и Linux-агенты создают теневые копии при копировании или перемещении файлов:

- на АРМ,
- другой ВНИ,
- сетевую шару.

Примечание: Чтобы агент отправлял теневые копии на сервер, у вас должны быть активированы файловая активность, теневое копирование и контроль USB-устройств.

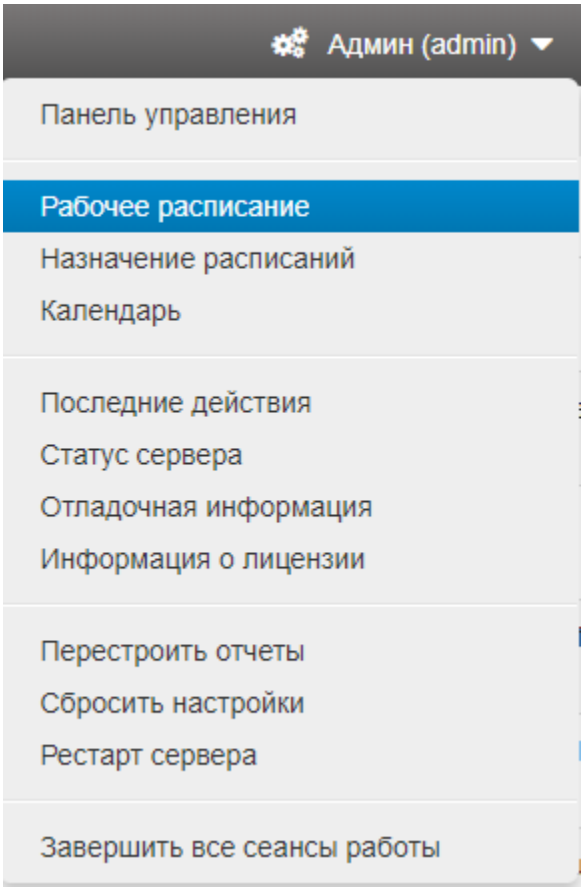
Вместе с теневой копией агент передает на сервер:

- путь директории файла на ВНИ;
- информацию о ВНИ;
- путь директории файла на новом устройстве;

- информацию о новом устройстве.

Теневая копия сохраняется в событии **Перехваченный файл**.

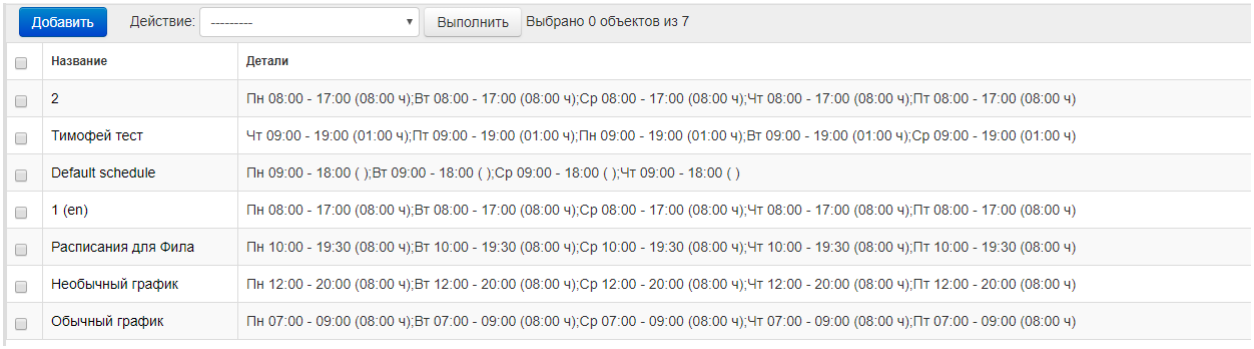
4.2.5 Рабочее расписание



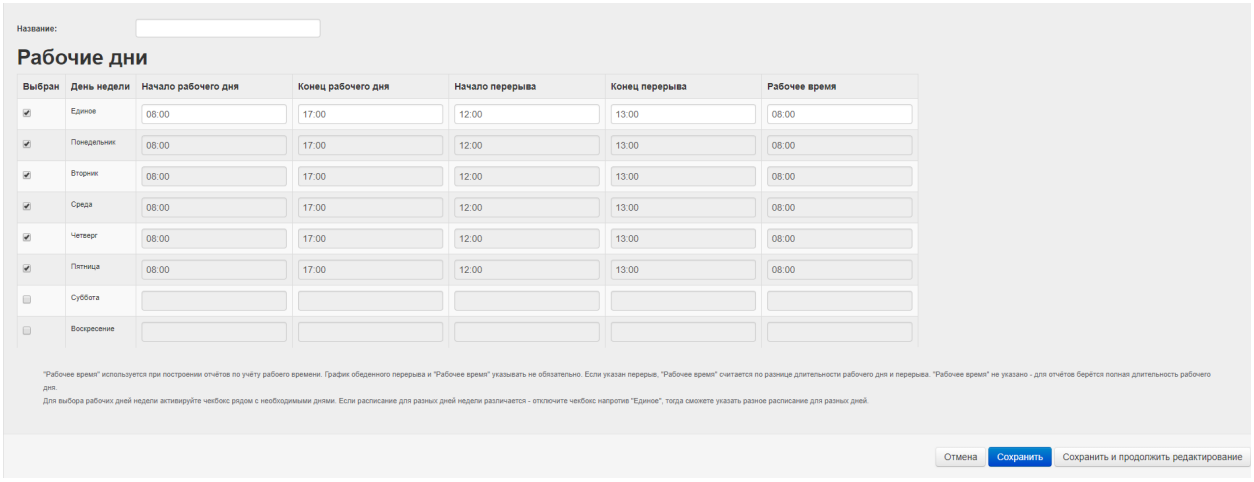
Рабочее расписание предназначено для того, чтобы задавать расписание рабочей недели. Заданное расписание будет использоваться при построении отчетов «Учет рабочего времени», «Отчет по опозданиям», «Сводный отчет» и др. Можно создать несколько вариантов расписания для рабочей недели. Например, при работе в несколько смен есть необходимость в создании рабочего расписания для каждой смены.

Добавление нового расписания

Для того чтобы добавить расписание, нажмите на кнопку **Добавить**.



Перед вами откроется страница с интерфейсом создания рабочего расписания.

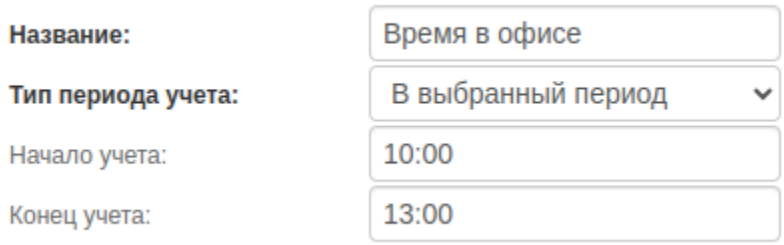


Название — название рабочего расписания.

Тип периода учета — позволяет выбрать формат ведения отчета «Учет рабочего времени»:

- с начала и конца суток;
- только рабочее расписание;
- в выбранный период.

Если вы устанавливаете отслеживание в выбранный период, укажите в полях «Начало учёта» и «Конец учёта» время в формате ЧЧ:ММ. Активность будет учитываться только в указанном временном интервале.



Единое расписание — установка единого расписания на всю неделю с понедельника по пятницу. Если расписание в разные дни недели будет отличаться, то для редактирования определенных дней, необходимо снять чекбокс слева от «Единого расписания».

Начало рабочего дня — время, с которого начинается рабочий день.

Конец рабочего дня — время окончания рабочего дня. Время окончания рабочего дня не должно быть раньше начала рабочего дня.

Начало перерыва — начало обеденного перерыва. В это время, при построении отчетов «Учета рабочего времени», игнорируется любая активность, то есть данное время не будет учитываться при подсчете продуктивности, общего времени активности и др.

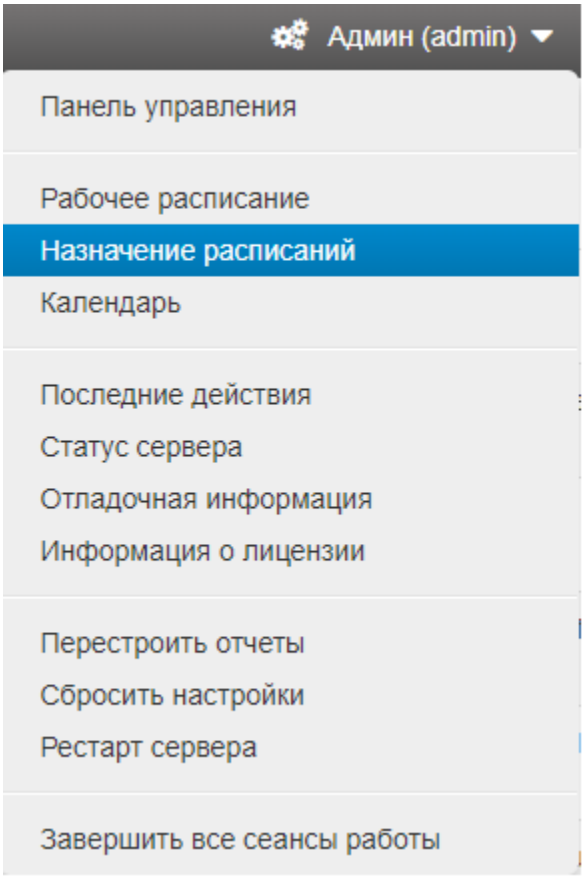
Конец перерыва — конец обеденного перерыва. После окончания перерыва возобновляется подсчет продуктивности. Перерыв должен попадать во время рабочего дня.

Рабочее время — время используется для построения ряда дисциплинарных отчётов, где сравнивается фактическое время с планируемым. По умолчанию, если поле «Рабочее время» не заполнено, в качестве такового берётся длительность рабочего дня за вычетом перерыва (если есть). Плановое время не должно превышать длительность рабочего дня.

Для сохранения рабочего расписания нажмите кнопку **Сохранить**. Для отмены внесенных изменений нажмите кнопку **Отмена**.

Для удаления созданного расписания зайдите в расписание и нажмите кнопку **Удалить**.

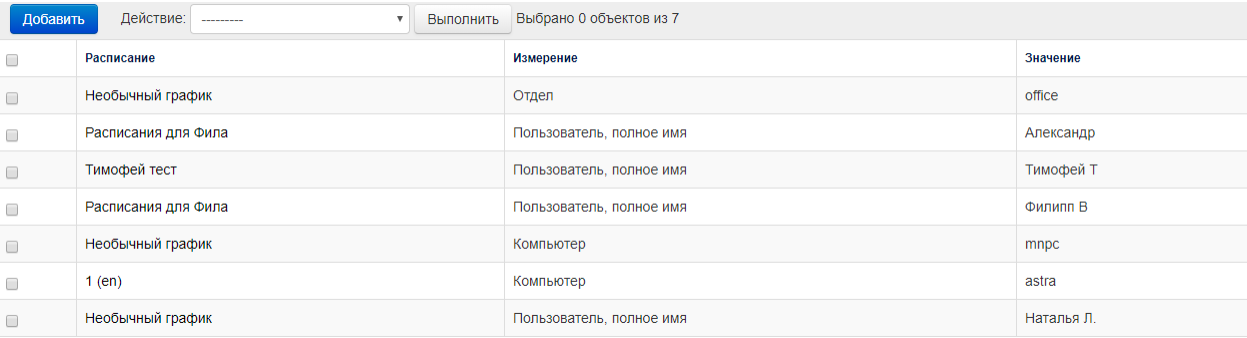
4.2.6 Назначение расписаний



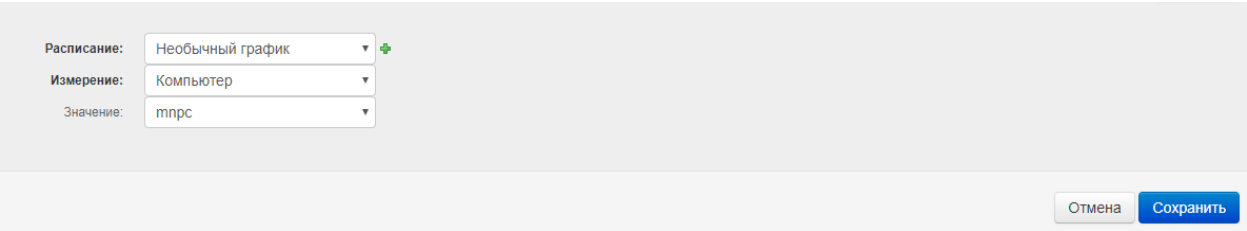
Назначение расписаний позволяет задавать рабочее расписание для разных групп пользователей. Например, можно назначить расписание по компьютеру, отделу или метке агента.

Назначение рабочего расписания

Нажмите на расписание, которое вы хотите назначить:



Откроется интерфейс назначения рабочего расписания.



Расписание – выбор расписания. Для создания нового расписания нажмите на знак +.

Измерение – выбор измерения, по которому будут выбираться пользователи для установки расписания.

- *Компьютер* – по имени компьютера;
- *Группа* – по группе пользователей;
- *Отдел* – по отделу;
- *Пользователь* – пользователю ПК;
- *Пользователь, полное имя* – по имени пользователя из доменного имени;
- *Организация* – по организации.

Значение – выбор пользователей или групп пользователей по выбранному измерению.

Для сохранения назначенного расписания нажмите **Сохранить**. Для отмены внесенных изменений нажмите **Отмена**.

Перекрестное раписание

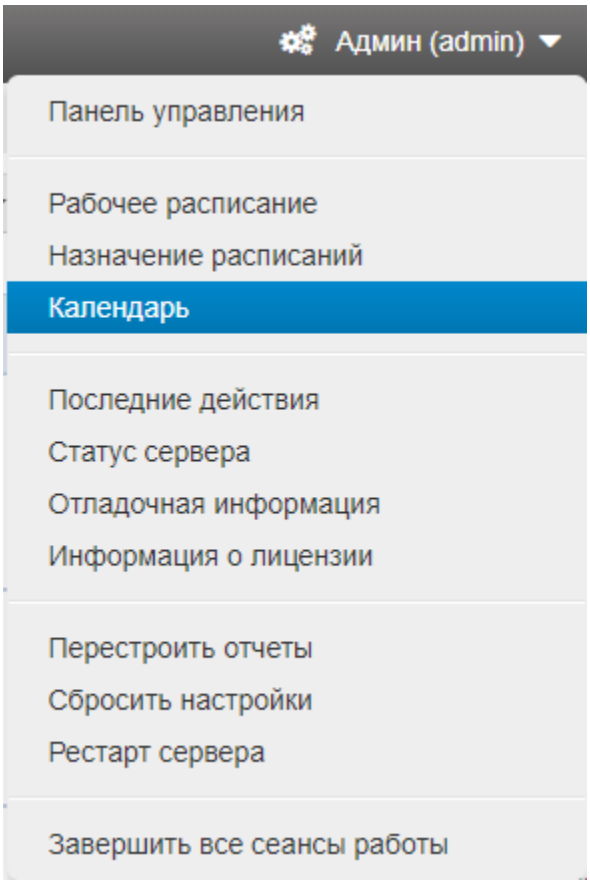
Перекрестное расписание возникает, когда одно и то же измерение встречается в нескольких расписаниях. В таких случаях в отчетах будет указано расписание, основанное на измерении с более высоким приоритетом.

Измерения в порядке уменьшения приоритета:

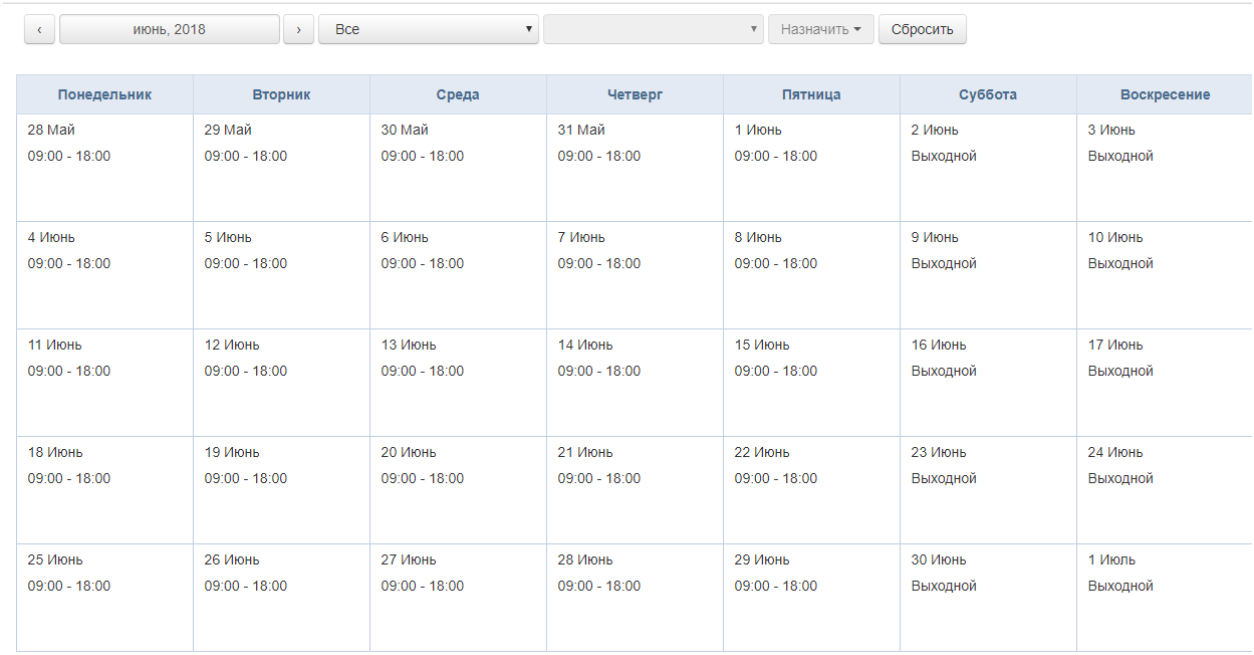
- *Компьютер*;
- *Группа*;
- *Пользователь*;
- *Пользователь, полное имя*;
- *Отдел*;
- *Организация*.

Например, если пользователь присутствует в расписании по отделу и имени пользователя, в отчетах будет указано расписание по имени пользователя.

4.2.7 Календарь



Календарь предназначен для построения точного рабочего графика с учётом праздников, отпусков, отгулов, больничных и сокращённых дней. По умолчанию в производственном календаре используются рабочие дни, указанные в недельном «Расписании».



Изменения доступны в трех вариантах:

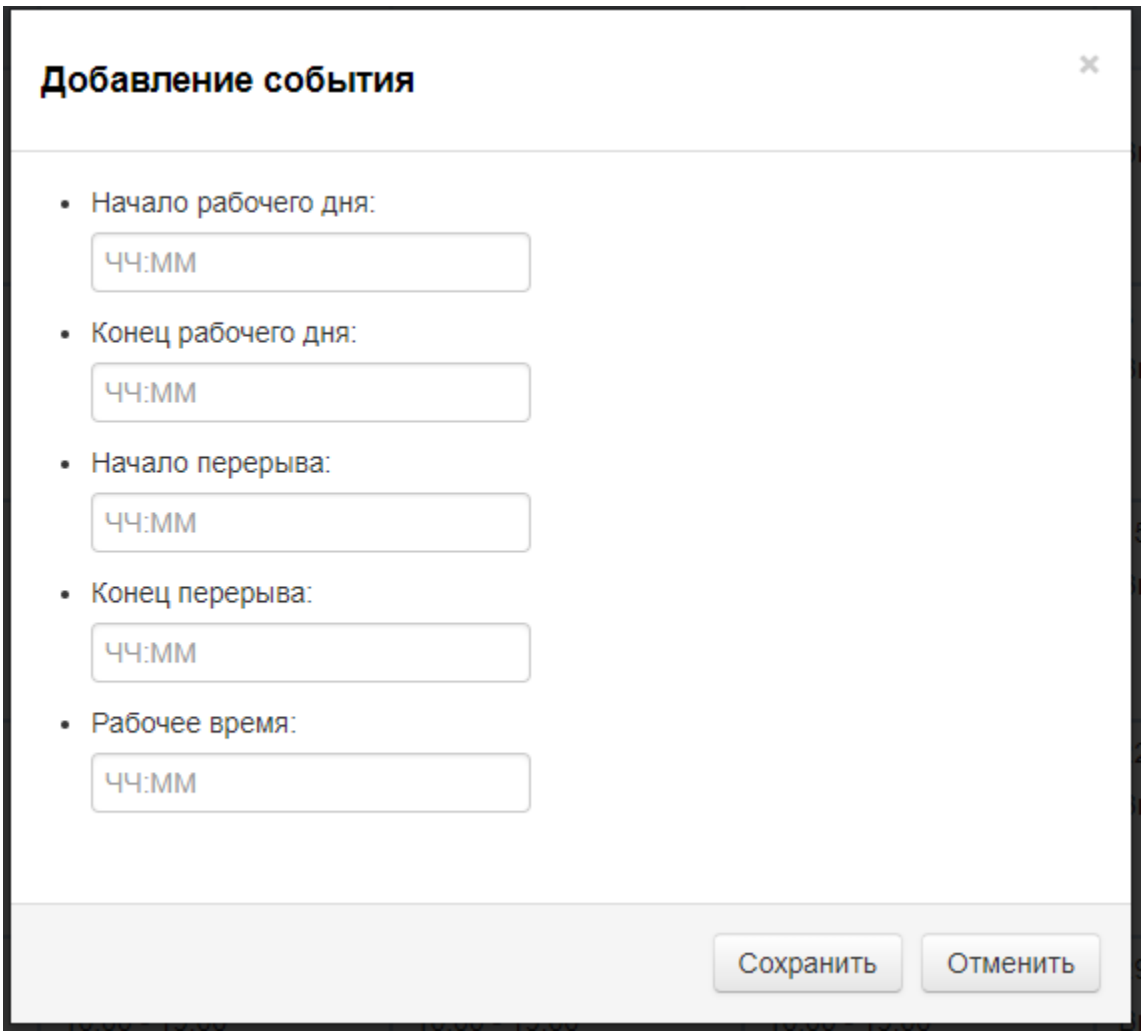
- Все - вносит изменения в рабочее время для всех пользователей.
- Отдел - вносит изменения в расписание для выбранного отдела.
- Пользователь - вносит изменения для каждого пользователя отдельно.

Для всех и для отделов можно назначить «Рабочие часы» и «Праздник».

Для пользователя можно дополнительно назначить «Больничный», «Отгул» или «Отпуск».

Назначение рабочего времени

Выберите дни, в которые необходимо внести изменения, выберите пользователей и нажмите кнопку назначить рабочее время



Начало рабочего дня - время, с которого начинается рабочий день.

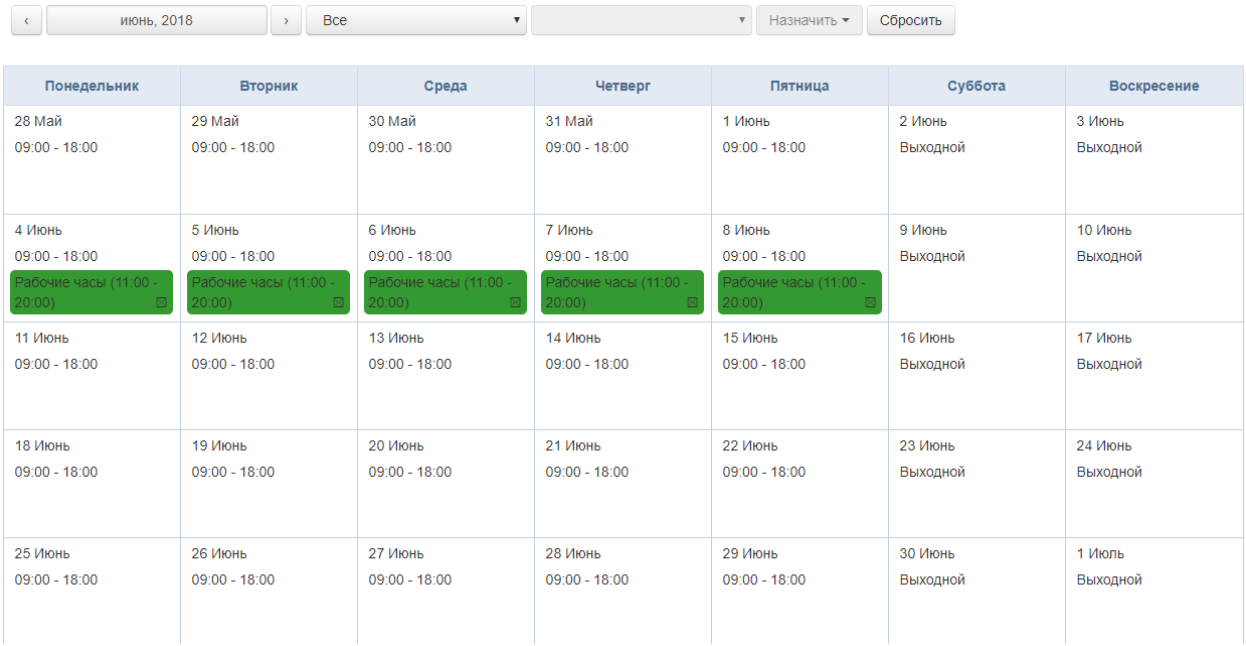
Конец рабочего дня - время окончания рабочего дня. Время окончания рабочего дня не должно быть раньше начала рабочего дня.

Начало перерыва - начало обеденного перерыва. В это время, при построении отчетов «Учета рабочего времени», игнорируется любая активность, то есть данное время не будет учитываться при подсчете продуктивности, общего времени активности и др.

Конец перерыва - конец обеденного перерыва. После окончания перерыва возобновляется подсчет продуктивности. Перерыв должен попадать во время рабочего дня.

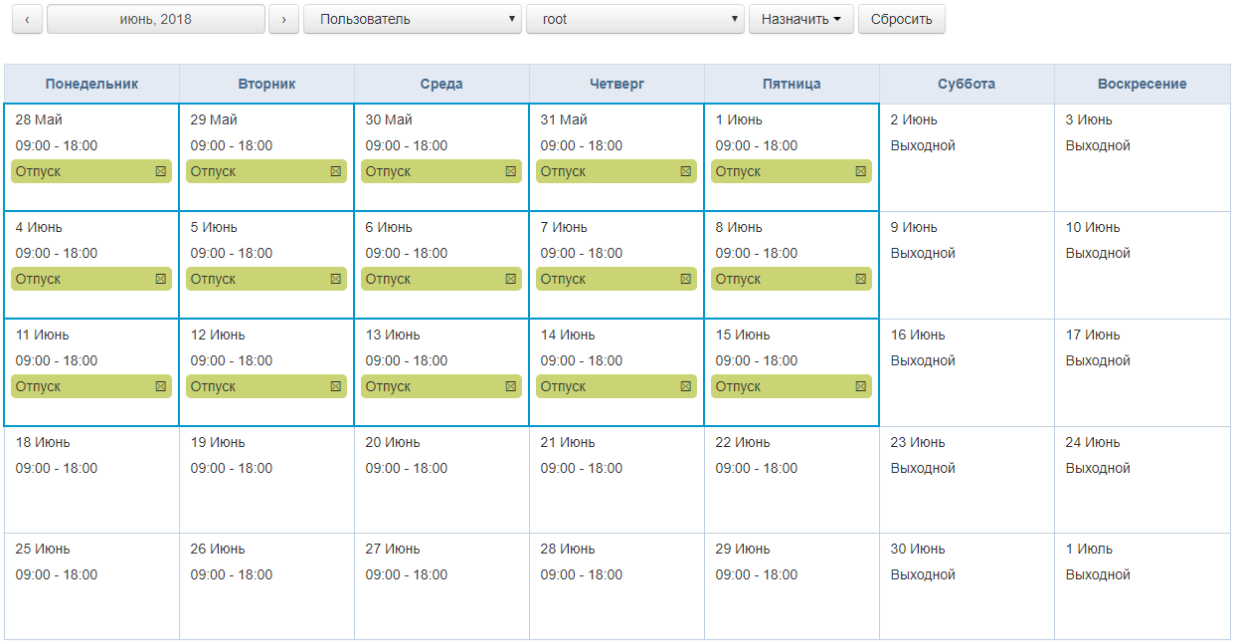
Рабочее время - время используется для построения дисциплинарных отчётов, где сравнивается фактическое время с планируемым. По умолчанию, если поле «Рабочее время» не заполнено, в качестве такового берётся длительность рабочего дня за вычетом перерыва (если есть). Плановое время не должно превышать длительность рабочего дня.

Для применения расписания, нажмите кнопку «Сохранить». В результате у выбранных пользователей будет изменено рабочее время в выбранные дни.



Назначение праздников, больничных и отпусков

Выберите дни, в которые необходимо внести изменения, выберите пользователей и нажмите кнопку назначить отпуск, праздник, отгул или больничный.



В результате, в выбранные дни, для отчета «Учет рабочего времени, пользовательские активности (опоздания, сверхурочные и др.) подсчитываться не будут.

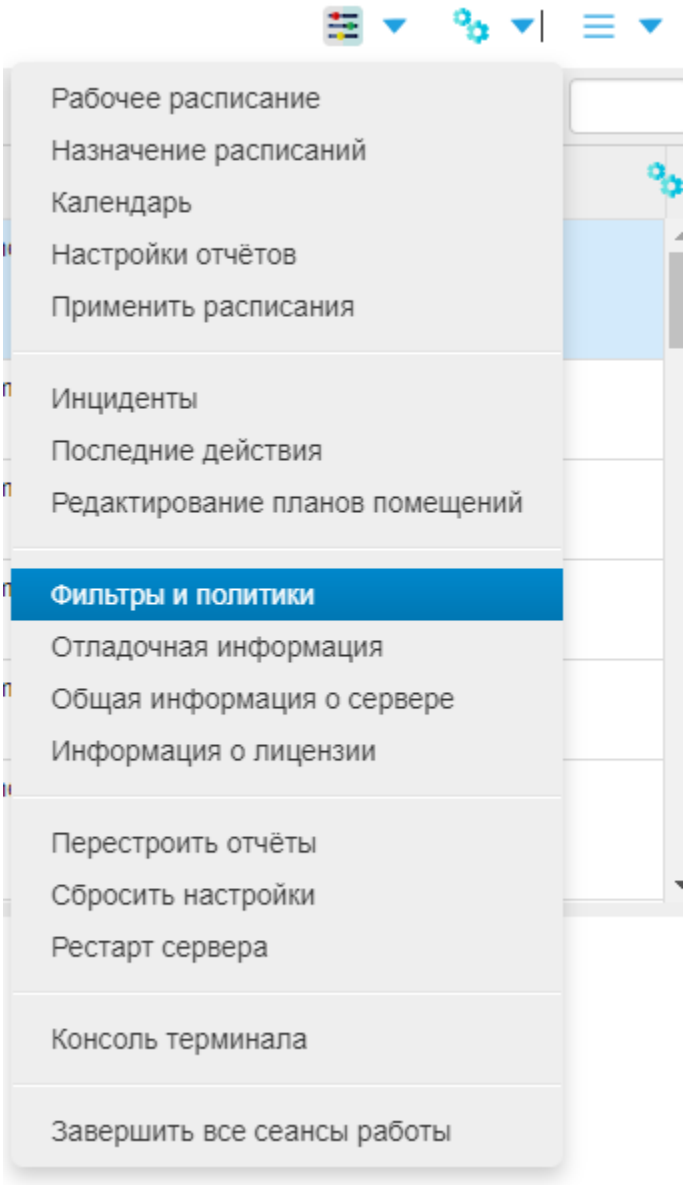
Сбросить расписание

Чтобы отменить назначенные события:

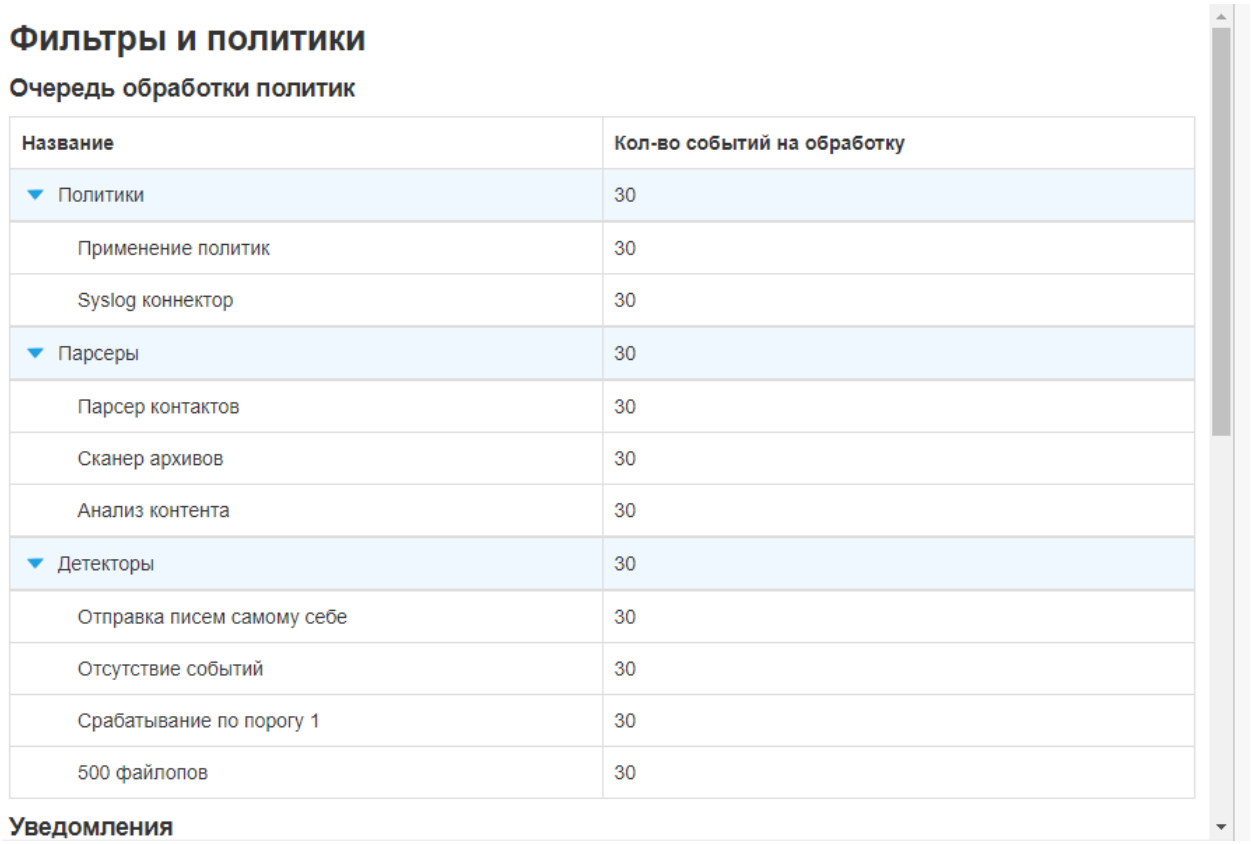
- выберите пользователя;
- в расписании пользователя выберите дни, для которых нужно отменить события;
- нажмите кнопку **Сбросить**.

4.2.8 Фильтры и политики

Чтобы посмотреть информацию об очереди обработки политик на сервере, перейдите в раздел **Админ - Фильтры и политики**.



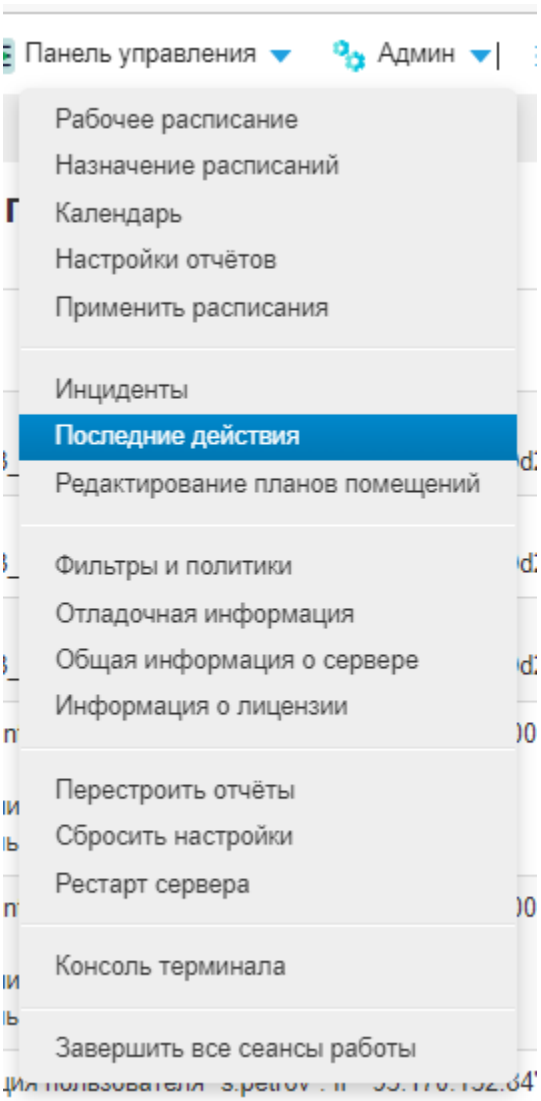
В открывшейся таблице указаны названия политик и парсеров и количество событий в очереди на обработку.



4.2.9 Последние действия

В разделе **Последние действия** представлена информация обо всех действиях администраторов веб-консоли iBatyr Monitor.

Начиная с версии 5.2-1039, в iBatyr Monitor-сервер появилась возможность отслеживать действия администраторов в меню **Создать** (создание/изменение/удаление политик, фильтров, отчётов, дашбордов и т.д.).


Панель управления
Админ
Рабочее расписание
Назначение расписаний
Календарь
Настройки отчётов
Применить расписания
Инциденты
Последние действия
Редактирование планов помещений
Фильтры и политики
Отладочная информация
Общая информация о сервере
Информация о лицензии
Перестроить отчёты
Сбросить настройки
Рестарт сервера
Консоль терминала
Завершить все сеансы работы

Последние действия

Имя пользователя	Время	Объект	Название объекта	Действие
admin	13:11:21 21.06.2018	Настройки AD	192.168.1.197	Ни одно поле не изменено.
admin	12:33:00 21.06.2018	Настройки AD	192.168.1.197	Ни одно поле не изменено.
admin	12:29:02 21.06.2018	Конфигурация	Конфигурация по умолчанию	Изменен screenshot_making_period,user_timeout,schedule_timeout,schedule_start и schedule_finish.
admin	12:24:07 21.06.2018	Конфигурация	Конфигурация по умолчанию	Изменен disable_network_web,disable_webmail,disable_network_mail,disable_network_im,disable_network_ftp,user_time
admin	12:22:11 21.06.2018	Настройки AD	192.168.1.197	Ни одно поле не изменено.
admin	12:12:59 21.06.2018	Настройки AD	192.168.1.197	Ни одно поле не изменено.
admin	12:12:55 21.06.2018	Настройки AD	192.168.1.197	Ни одно поле не изменено.
admin	12:12:53 21.06.2018	Настройки AD	192.168.1.197	Объект создан
admin	11:01:37 21.06.2018	Расписание	Default schedule	Изменены work_time для Рабочие дни "ScheduleRecord object". Изменены work_time для Рабочие дни "ScheduleRec
admin	06:03:44 21.06.2018	Конфигурация	vladz webmail	Изменен disable_filespy_shadow_copying,user_timeout,schedule_timeout,schedule_start,schedule_finish и agents.
admin	06:03:13 21.06.2018	Конфигурация	vladz webmail	Объект создан

Имя пользователя - имя учетной записи администратора, который производил изменения.

Время - время внесения изменений.

Объект - объект, в который были внесены изменения.

Название объекта - параметр объекта, в который были внесены изменения.

Действие - что конкретно было изменено.

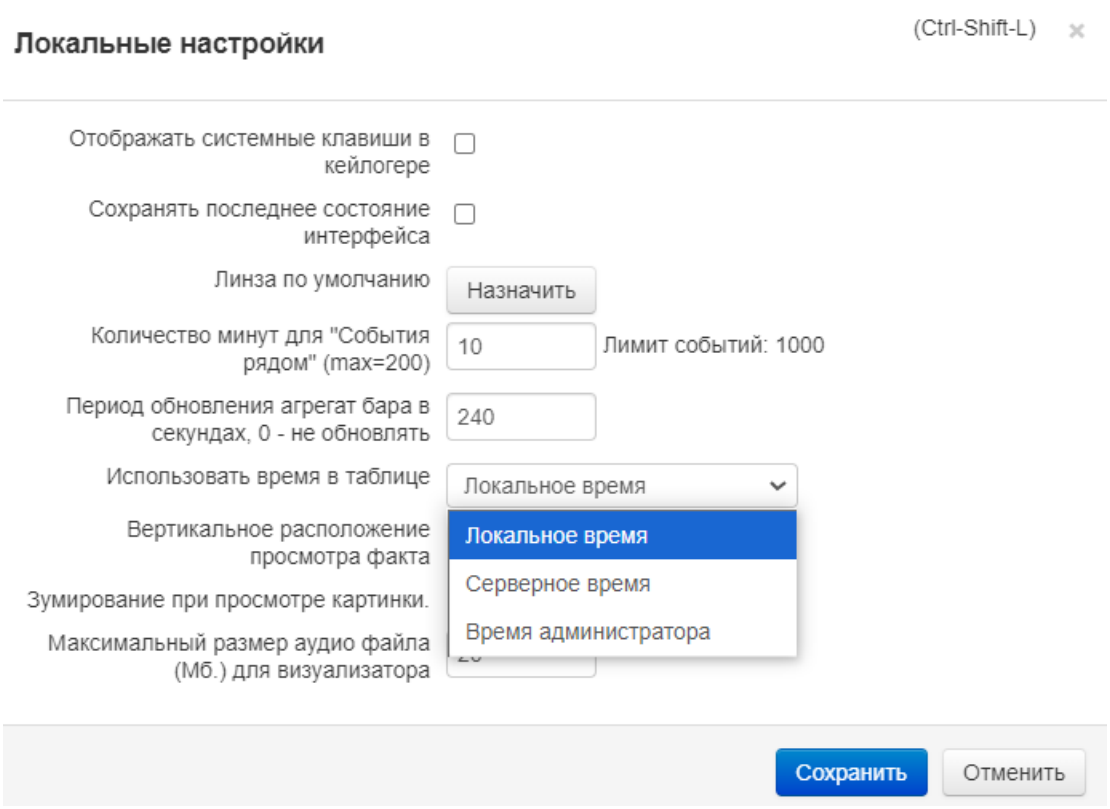
Например, запись

admin	12:04:13 04.08.2023	Конфигурация компьютеров	Конфигурация по умолчанию	Изменен disable_cd_files_control (True -> False), disable_file_activity (True -> False), disable_usb_devices (True -> False).

означает, что 4 августа в 12:04 пользователь с именем admin внёс изменения в конфигурацию компьютеров по умолчанию. Были отключены контроль файлов на CD-накопителях, отключен мониторинг файловой активности и отключен контроль USB-устройств.

4.2.10 Локальные настройки

В разделе **Меню** – **Локальные настройки** представлены настройки веб-интерфейса, позволяющие настроить удобное отображение событий в Линзе.



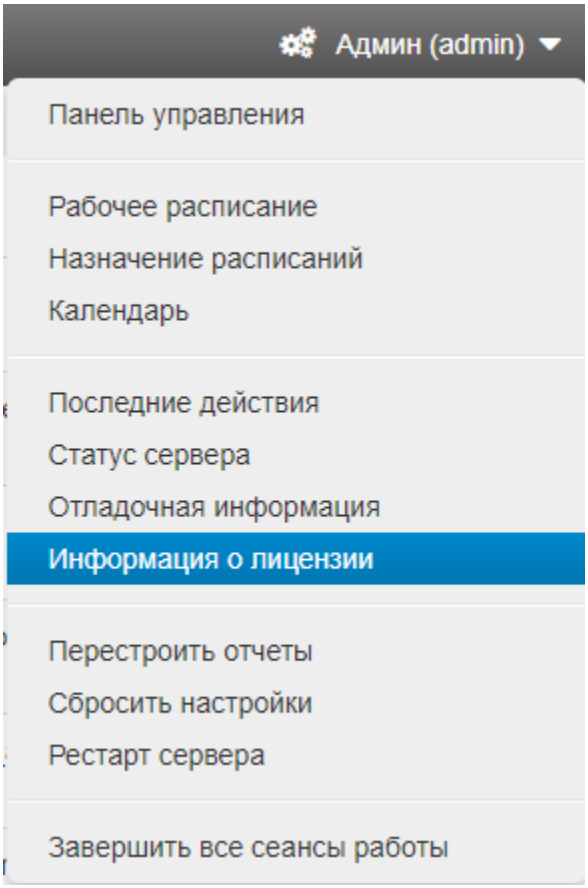
Примечание: Локальные настройки не влияют на выгрузку отчетов.

Описание пунктов меню **Локальные настройки**:

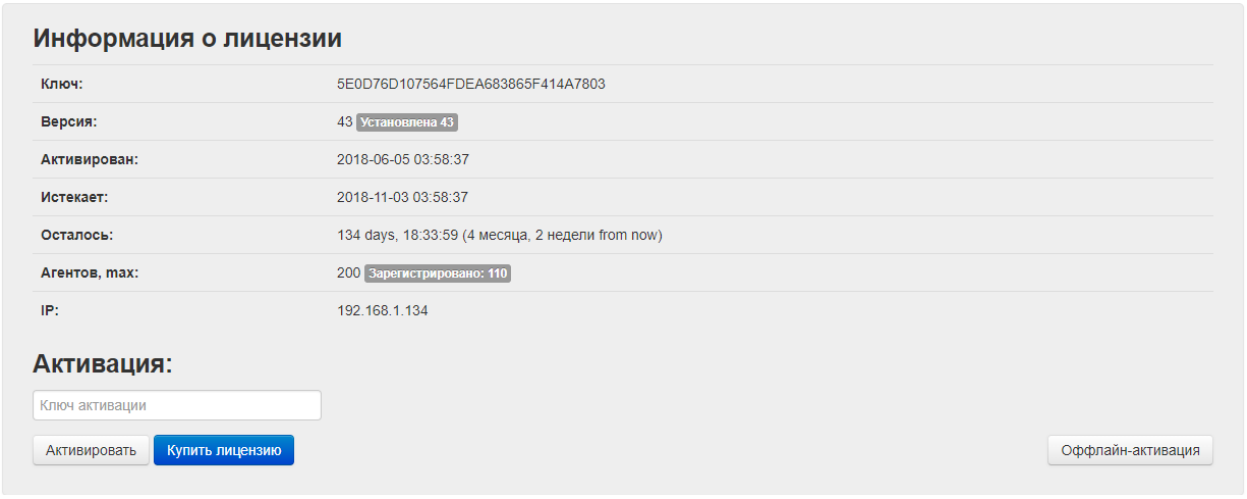
tabularytabulary

Пункт меню
Отображать системные клавиши в кейлоггере
Сохранять последнее состояние интерфейса
Линза по умолчанию
Количество минут для «События рядом» (max=200)
Период обновления агрегат бара в секундах, 0 - не обновлять
Использовать время в таблице
Вертикальное расположение просмотра факта
Зуммирование при просмотре картинки
Максимальный размер аудиофайла (Mb) для визуализатора

4.2.11 Информация о лицензии



Информация о лицензии позволяет посмотреть информацию о лицензии, сроке её активации и истечения, количестве компьютеров, которые могут подключаться к серверу и количество подключенных компьютеров.

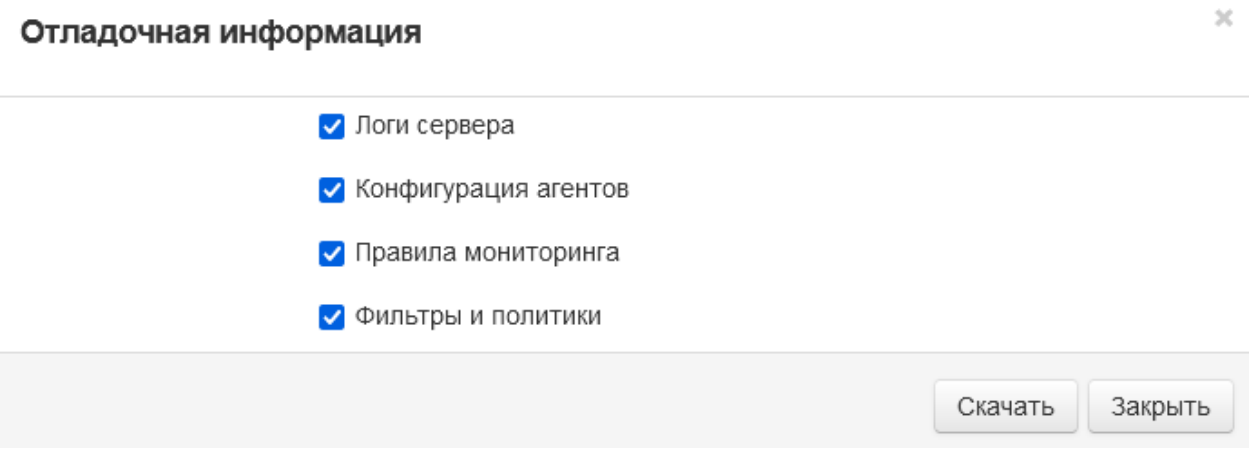


Здесь же можно ввести новый ключ, и пройти активацию снова, например, при переходе с временной лицензии на постоянную.

4.2.12 Отладочная информация

Отладочная информация позволяет выгружать логи системы iBatyr Monitor.

Для этого откройте в меню **Админ - Отладочная информация** и отметьте чекбоксами системные логи, которые требуется выгрузить, затем нажать кнопку «Скачать».

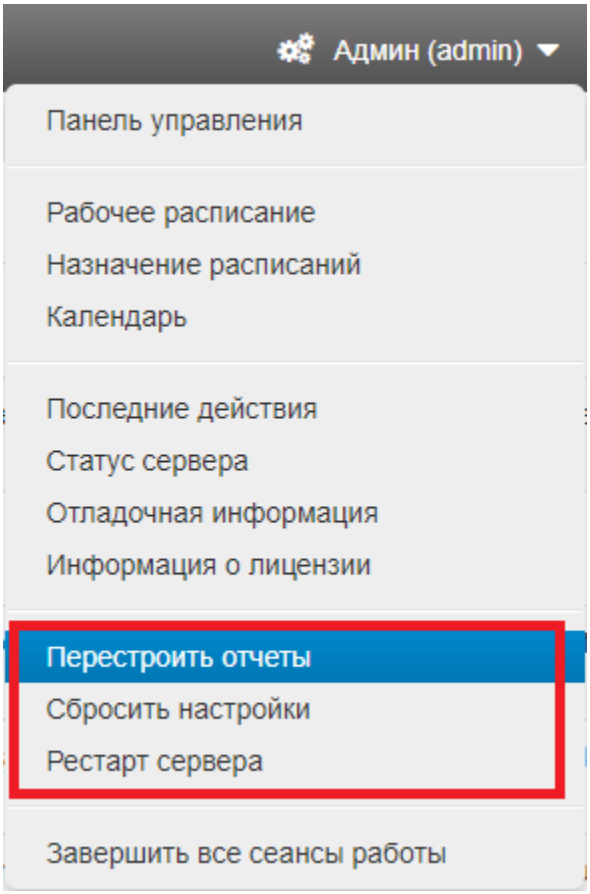


4.2.13 Общая информация о сервере

В разделе **Администрирование** / **Общая информация о сервере** представлены результаты выполнения базовых системных команд:

- **date** - текущая дата и время на сервере;
- **top -b -n 1 | head -n 20** - список выполняемых процессов и уровень нагрузки на сервер;
- **df -h** - сведения о дисковом пространстве сервера;
- **ping ya.ru -c 1 | grep -i ya** - проверка связи сервера с внешней сетью;
- **cat /etc/apt/sources.list** - список репозиториев системы;
- **cat /etc/apt/sources.list.s/ibatyr.list** - репозиторий iBatyr Monitor;
- **ibatyr info –without-disk-usage** - общие сведения об установленной версии iBatyr Monitor;
- **tail /var/log/ibatyr/ibatyr.log** - последние строки общего лога iBatyr Monitor;
- **tail /var/log/ibatyr/process.log** - последние строки лога процессов iBatyr Monitor.

4.2.14 Выполнить команду



Перестроить отчеты - команда запускает пересчёт всех отчетов.

Примечание: Процедура может занять длительное время!

Сбросить настройки - команда удаляет все пользовательские настройки, возвращая сервер к первоначальным настройкам.

Рестарт сервера - команда перезапускает все службы, связанные со ibatyr непосредственно из веб-интерфейса.

4.2.15 Окно настроек

Содержание

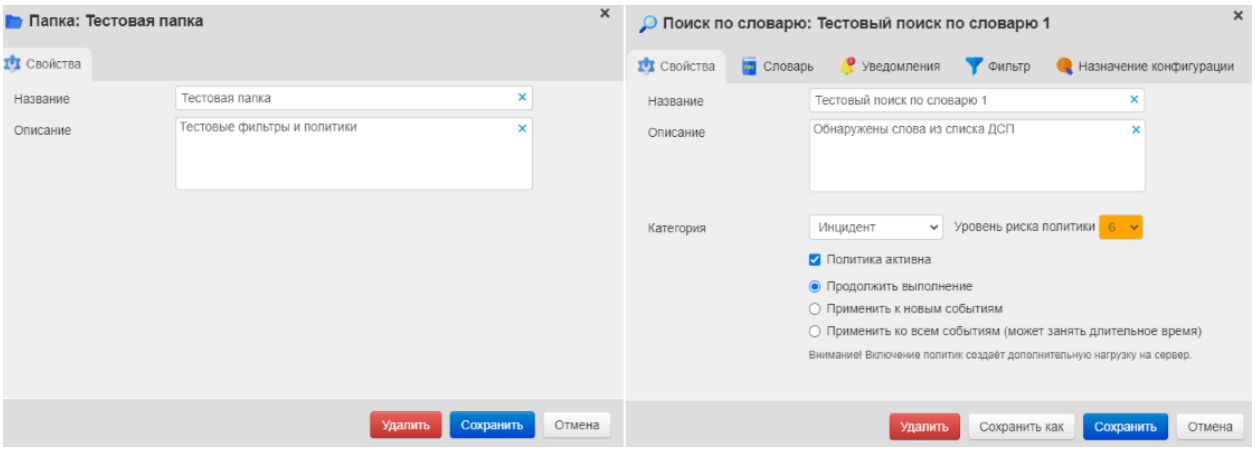
- *Окно настроек*
  - *Панель управления*
  - *Вкладки*

В **окне настроек** можно создать или отредактировать *инструменты фильтрации*.

Чтобы открыть окно настроек инструмента:

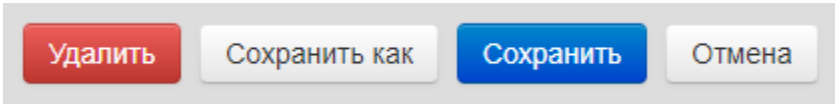
1. На главной странице веб-интерфейса перейдите во вкладку **Политики**.
2. Нажмите на название инструмента. Справа от названия появится иконка шестеренки .
3. Нажмите на иконку шестеренки — откроется **окно настроек** с заголовком *Тип инструмента: Имя инструмента*.

В зависимости от типа инструмента в окне доступны различные свойства и вкладки. Например, для инструмента **Папка** доступна только вкладка **Свойства**, а для инструмента **Поиск по словарю** доступны вкладки **Свойства**, **Словарь**, **Уведомления**, **Фильтр**, **Назначение конфигурации**.



Панель управления

Внизу окна настроек располагаются кнопки, которые позволяют управлять инструментом.



Удалить — удаляет инструмент фильтрации данных.

Сохранить как — позволяет создать инструмент на основе текущего.

Сохранить — сохраняет изменения или создает новый инструмент.

Отмена — сбрасывает несохраненные изменения.

Вкладки

Наверху окна располагаются вкладки параметров инструмента.

Свойства

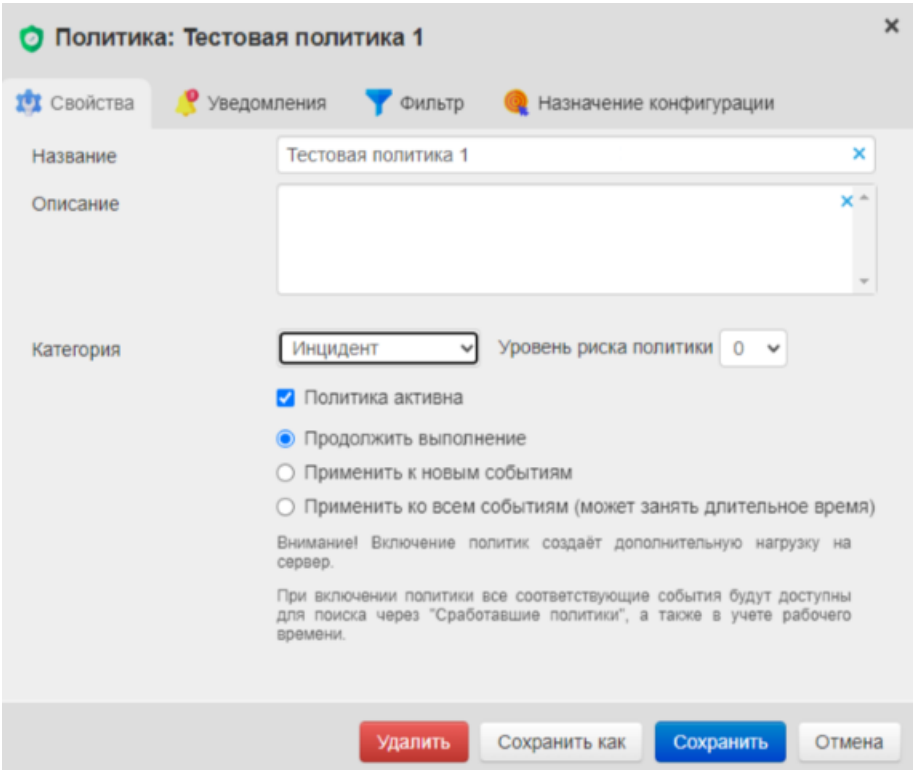
В этой вкладке можно задать параметры:

- **Название** и **Описание** инструмента.
- **Категория** — определяет продуктивность и безопасность события. Если событие подходит под условия фильтрации, политика назначит ему **Категорию** и отметит соответствующим цветом в отчете *Учет времени*.

  См.также:

  Подробнее о категориях продуктивности

  Этот параметр доступен для инструментов **Работа не за компьютером**, **Политика** и **Поиск по словарю**.
- **Политика активна** — активирует политики **Политика удаления событий**, **Политика** и **Поиск по словарю**. Без этого флага политики не будут работать.



  При активации выберите вариант работы:

  - **Продолжить выполнение** — инструмент продолжит обработку событий. Опция включена по умолчанию, если политика уже активна.
  - **Применить к новым событиям** — инструмент будет обрабатывать только события, которые поступили после активации. Старые события инструмент обрабатывать не будет.
  - **Применить ко всем событиям (может занять длительное время)** — инструмент обработает события за весь период работы системы и продолжит обработку поступающих событий.

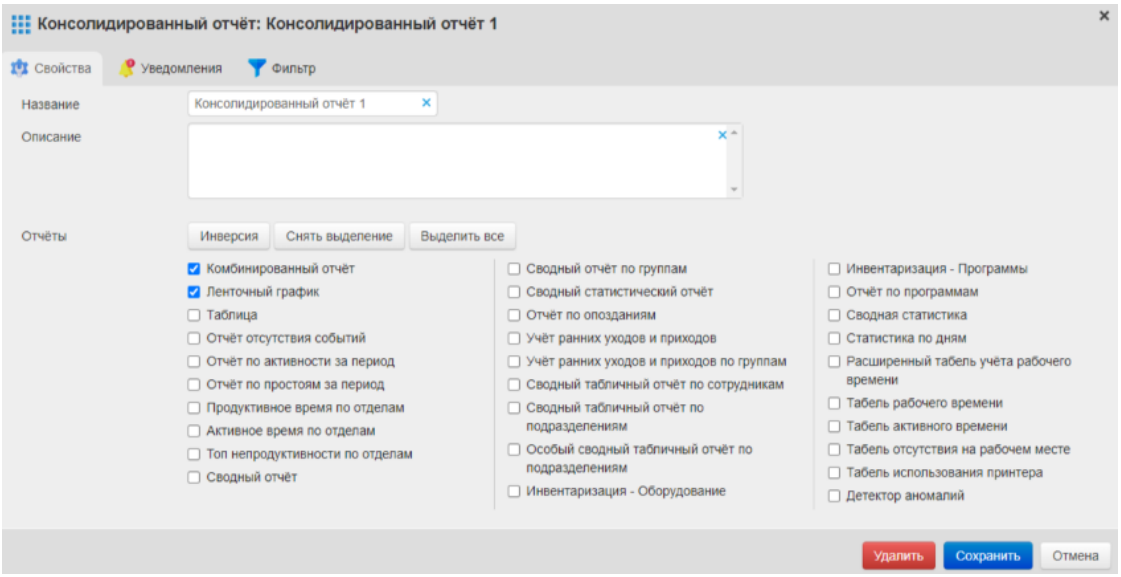
> **Предупреждение:** Опция перестраивает отчеты за весь период работы системы. При большой базе данных лучше запускать её в нерабочее время. Альтернативный вариант — *команда ibatyr rebuild_sessions*. Она позволяет перестроить отчеты за указанное количество месяцев.

- **Уровень риска** — параметр, который определяет *уровень риска события категории Инцидент*.

  Есть только у инструментов **Работа не за компьютером**, **Политика** и **Поиск по словарю**.

Важно: *Активируйте Уровень риска*, чтобы параметр появился в свойствах.

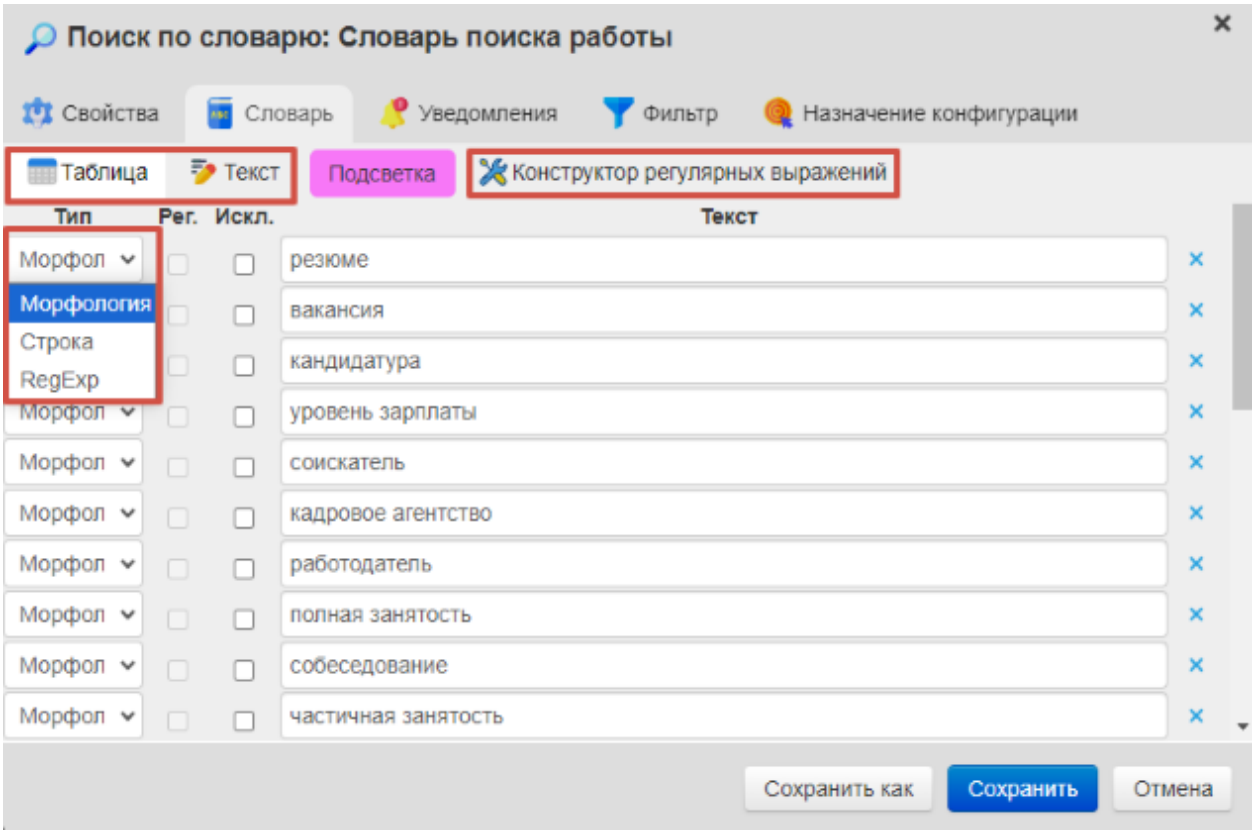
- **Отчеты** — список отчетов, которые могут входить *в Консолидированный отчет*.



Поиск по словарю

Примечание: Вкладка доступна только для инструментов *Поиск по словарю*.

В этой вкладке можно настроить *мониторинг ключевых слов*.

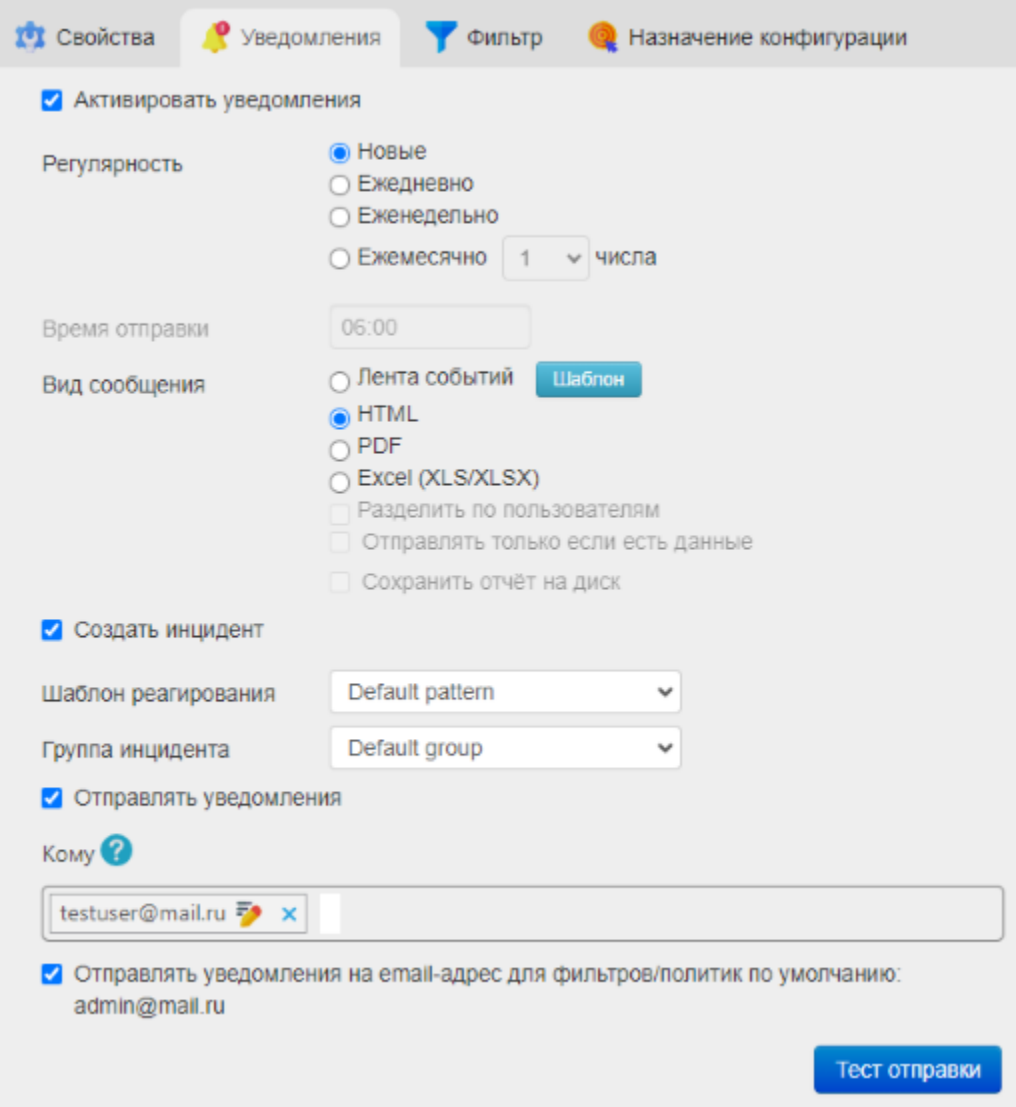


Уведомления

Примечание: Для рассылки сообщений *настройте почту*.

Настройки уведомлений доступны для инструментов:

- Фильтр,
- Дашборд,
- Консолидированный отчет,
- Политика,
- Поиск по словарю,
- Срабатывание по порогу.



Уведомления содержат список связанных с инструментом событий.

Активировать уведомления — отправка уведомлений.

Регулярность — периодичность отправки отчетов.

Время отправки — время отправки отчета.

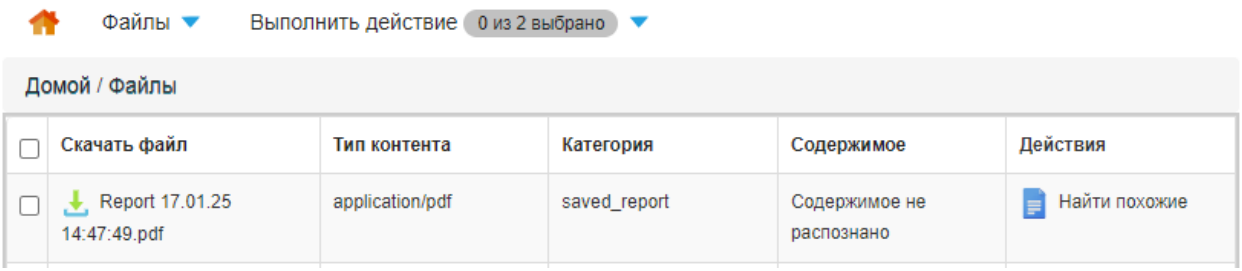
В разделе **Вид сообщения** можно выбрать формат документа для выгрузки:

- Лента событий — представляет события в виде таблицы,
- HTML,
- PDF,
- Excel (XLS/XLSX).

Разделить по пользователям — разбивает отчет по отдельным пользователям.

Отправлять только если есть данные — отправляет отчеты, только если есть данные.

Сохранить отчет на диск — сохраняет отчет в формате PDF в разделе **Панель управления** — **Файлы**.



Создать инцидент — создает инцидент *в консоли инцидентов*.

См.также:

Подробнее об инцидентах

- **Шаблон реагирования** — выбор *шаблона реагирования*.
- **Группа инцидента** — назначение *группы для инцидента*.
- **Отправлять уведомления** — отключения рассылки при создании инцидента.
- Выбор адресата:
  - **Кому** — поле для ввода адресов электронной почты или тега Telegram-бота для получения рассылки.

  См.также:

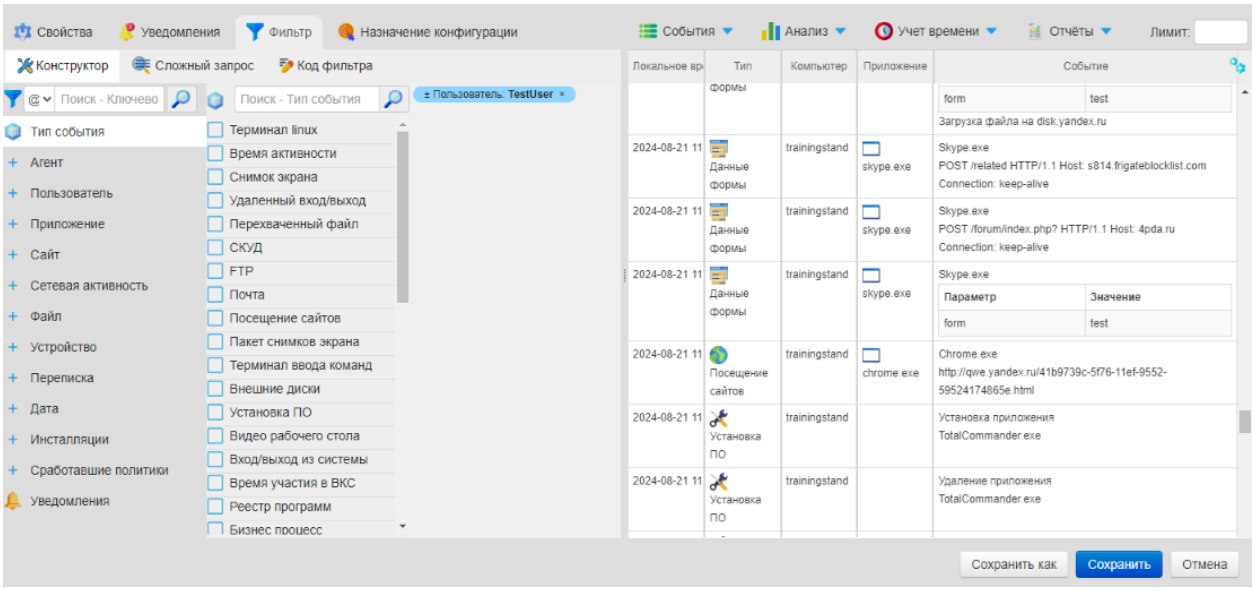
  Подробнее о настройке *уведомлений на электронную почту и в Telegram*.

  - **Отправлять уведомления на email-адрес для фильтров/политик по умолчанию** — отправка рассылки на общий адрес.

    Общий адрес можно задать в разделе **Панель управления** → **Параметры сервера** в параметре сервера **Email-адрес отправки уведомлений для фильтров/политик**.

Фильтр

В этой вкладке располагается **Конструктор**. Он позволяет задавать параметры фильтрации данных и просматривать события.

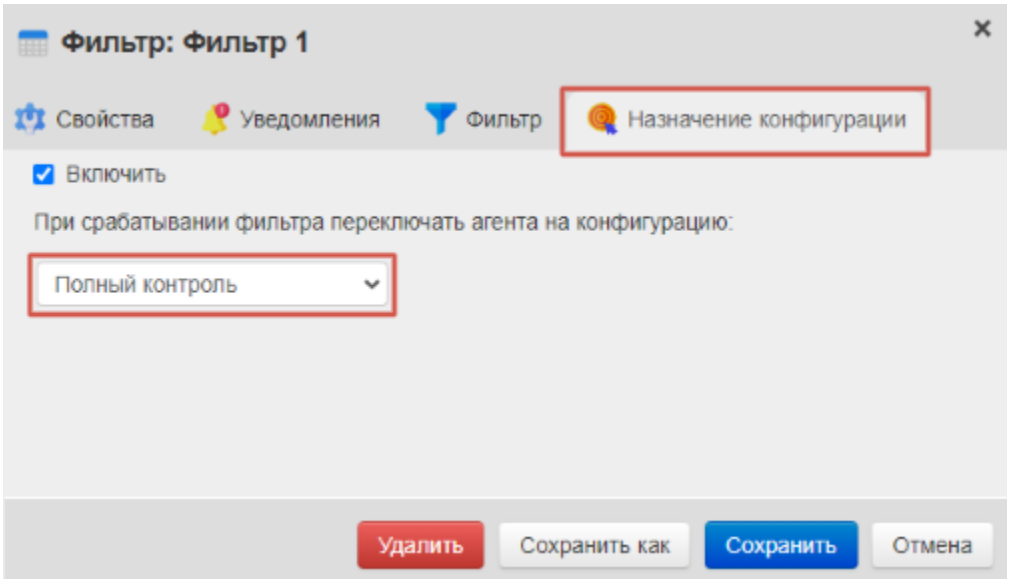


См.также:

Подробнее о работе с Конструктором

Назначение конфигурации

При поступлении событий, которые подходят под условия фильтрации, позволяет переключать *конфигурацию агента*.



Пример: настроить смену **Конфигурация по умолчанию** на **Полный контроль** после запуска пользователем *TestUser* программы удалённого подключения. Агент будет перехватывать все события: снимки с , запись видео с экрана, аудиозапись и другие.

1. Создайте политику и во вкладке **Фильтр** укажите условия:

- **Приложение** — **Название** — *anydesk.exe*,
- **Приложение** — **Название** — *mstsc.exe*,

- **Пользователь** — *TestUser*.

2. Во вкладке **Назначение конфигурации** активируйте опцию **Включить**.
3. В поле **При срабатывании фильтра переключать агента на конфигурацию** выберите **Полный контроль**.
4. Нажмите **Сохранить**.

Результат: при срабатывании политики конфигурация изменится на **Полный контроль**, которая дает полную информацию о действиях пользователя.

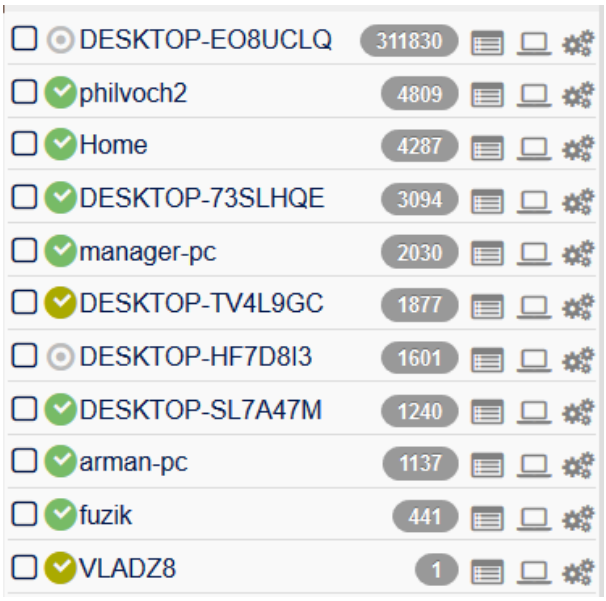
Важно: Смена конфигурации произойдет после того, как агент получит новую конфигурацию с сервера. Получение конфигурации занимает от одной до пяти минут в зависимости от сетевой инфраструктуры.

Если вы хотите настроить блокировку, то выберите **Конфигурацию с блокировками** в поле **При срабатывании фильтра переключать агента на конфигурацию**. В результате система будет блокировать:

- подключение USB-накопителей,
- доступ к файлам с метками,
- посещение сайтов,
- запуск приложений.

4.2.16 Описание статусов агентов

Описание основных статусов, которые могут быть напротив имён агентов:



.

- агент передавал данные об активности пользователя в течении последних 5 минут.

- агент последний раз передавал данные от 5 до 10 минут назад.

- новых данных от агента не было уже 10 и более минут, и, с большой долей вероятности, пользователя за рабочим местом уже нет, или его компьютер выключен.

Примечание: Обратите внимание, что при работе с веб-консолью, если вы оставите страницу больше чем на 10 минут без действия, то на измерении «Агенты», все агенты станут «серыми». Чтобы обновить статус по агентам и увидеть текущие статусы, нужно нажать кнопку «Обновить» в левой части окна.

4.2.17 Поиск — ключевые слова

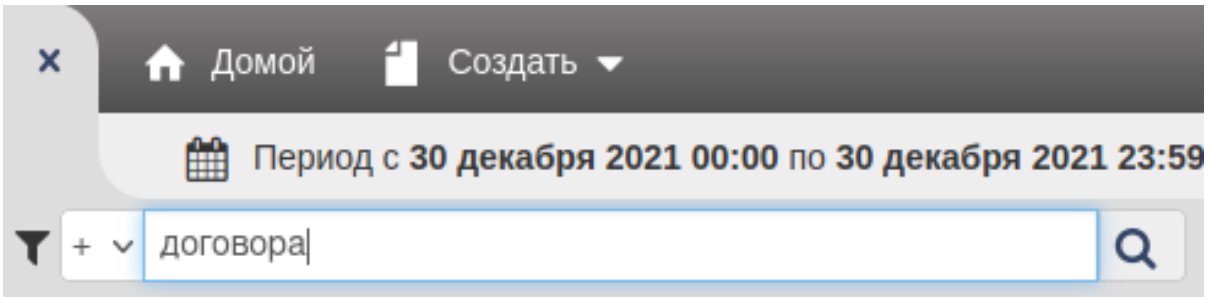
Все заголовки окон, названия документов, буфер обмена, содержимое перехваченных файлов и др. попадает в текстовую базу iBatyr Monitor .

После индексации событий в базе данных возможен полнотекстовый поиск этой информации.

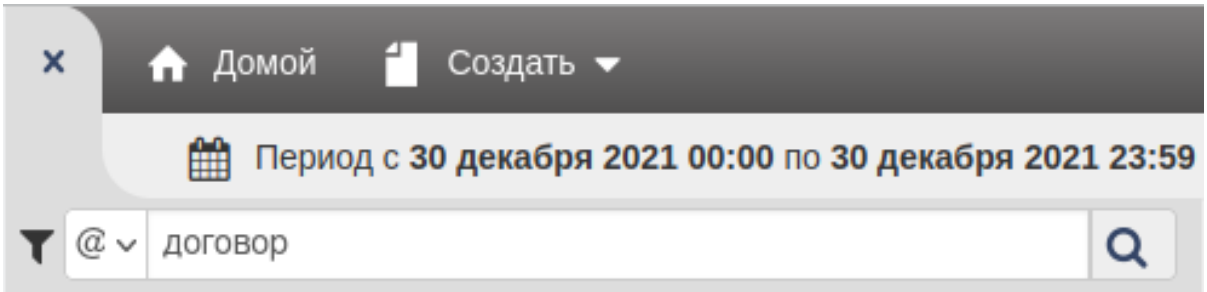
Вам доступны следующие варианты поиска:

- \+ - по подстроке;
- **@** - по ключевым словам (**Установлен по умолчанию**);
- **~** - по регулярным выражениям.

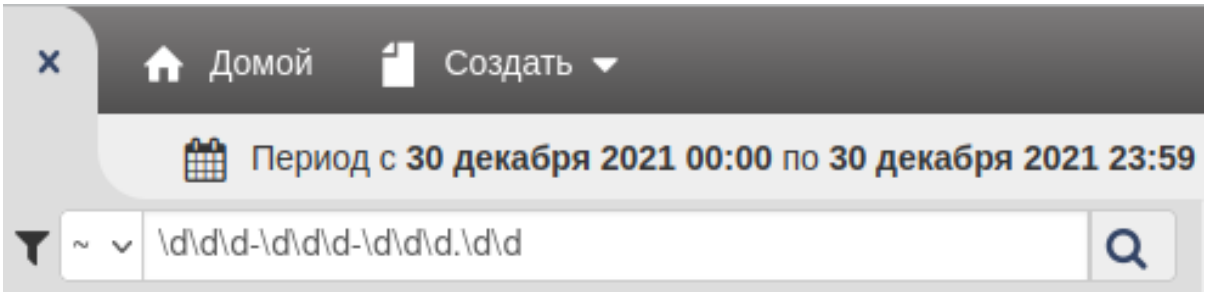
- Поиск **по подстроке** осуществляется после ввода в строку поиска интересуемого вас слова *(точное совпадение)*, например, **«договора»**.



- Поиск **по ключевым словам** осуществляется после ввода в строку поиска интересуемого вас слова *(с учетом морфологии)*, например, **«договор»**.



- Поиск **по регулярному выражению** нужно начинать с символа тильды «~», например, чтобы найти СНИЛС по формату «xxx-xxx-xxx xx», нужно ввести такую строку для поиска информации по регулярному выражению **«~\d\d\d\-\d\d\d\-\d\d\d.\d\d»**:



Примечание: Формат регулярных выражений используемый в iBatyr Monitor - PCRE.

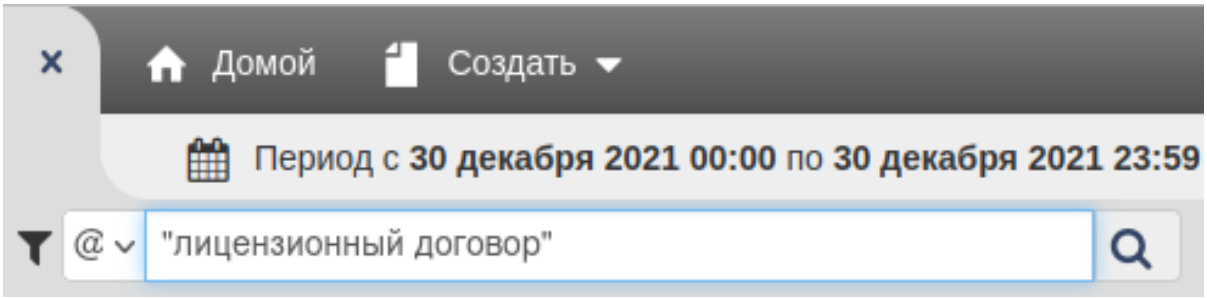
Отличный сайт для проверки Регулярных выражений - https://regex101.com/

Отличный сайт по введению в регулярные выражения - http://www.pcre.ru/docs/perl/text/intro/

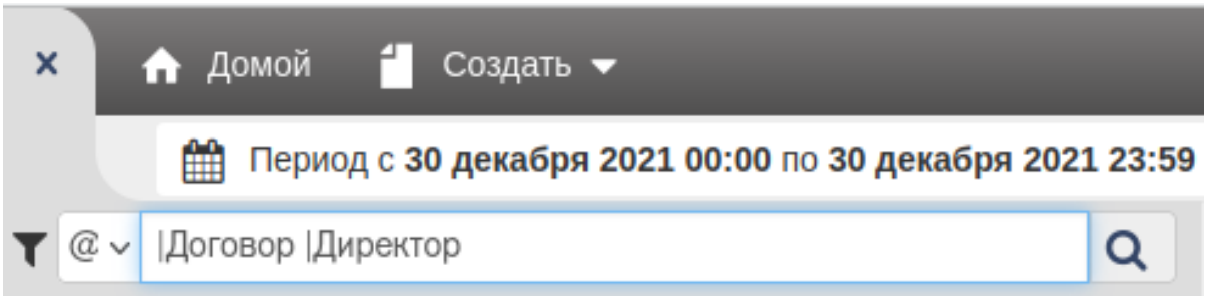
Примеры работы с поиском:

- по нескольким словам;
- по объединению слов;
- по точным фразам;
- по стоп-словам.

- Поиск **по нескольким словам** нужно заключать в кавычки, например, **«лицензионный договор»**:



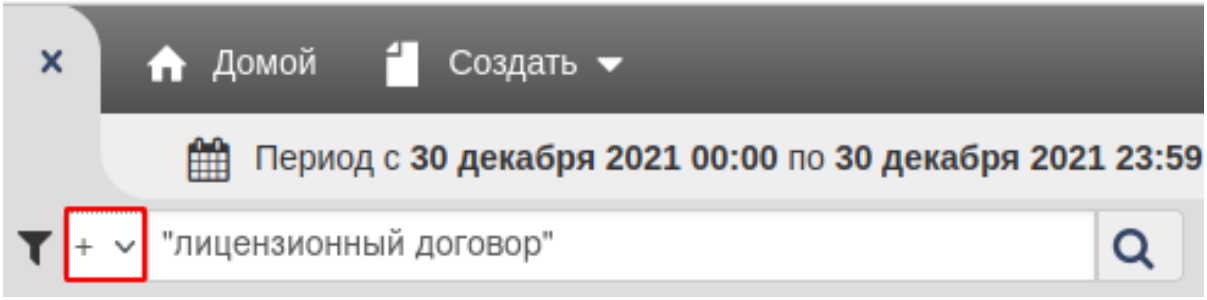
- Поиск **по объединению слов (ИЛИ)**. На данный момент, если в поиск ввести несколько слов, будет выводиться их пересечение **(И)**. Для того чтобы осуществить поиск по объединению **(ИЛИ)**, нужно вводить знак | перед каждым словом. Например, если нам нужно найти Договор ИЛИ Директор, нужно вводить в поиск:



Соответственно, поиск отобразит все события, в которых есть слово Договор ИЛИ Директор.

Примечание: Вводить знак | нужно перед каждым словом. Если ввести Договор Директор, будет выводиться пересечение слов Директор **И** Договор.

- Поиск **по точным фразам** нужно заключать в кавычки и выбрать символ «+», например, точный поиск фразы **«лицензионный договор»**:



- Поиск **стоп-слов**. Например, такие слова как **и**, **про**, **нас**, **хоть** и др. являются стоп-словами и при поиске ключевых слов они не учитываются. Для того чтобы осуществить поиск по таким словам, нужно указывать «+» перед ними, например +**и**, +**про**, +**нас**, +**хоть**

4.2.18 Удаленный рабочий стол

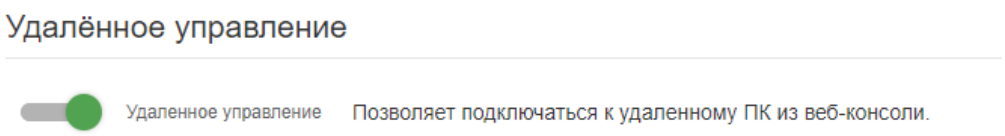
Вы можете подключиться к удаленному рабочему столу двумя способами:

- **iBatyr Monitor** — подходит для подключения ко всем компьютерам. Предоставляет базовые возможности удалённого подключения. Не поддерживает выполнение административных действий. Подходит для мониторинга и лёгкой технической поддержки.
- Контур.Доступ — доступен для компьютеров в периметре **Контура.Доступ**. Встроен в веб-интерфейс с 5.6 версии iBatyr Monitor. Предоставляет возможность выполнять любые действия администратора, Доступен только для Windows- и Linux-агентов, потому что Контур.Доступ реализован только для этих операционных систем.

Подготовка

Перед подключением убедитесь, что в вашей конфигурации включено **Удаленное управление**:

1. Перейдите **Панель управления** → **Конфигурация компьютеров** → *ваша конфигурация*.
2. Выберите в боковой панели **Удаленное управление**.
3. Активируйте модуль:



После этого удаленный рабочий стол **iBatyr Monitor** готов к работе.

Контур.Доступ требует дополнительной активации на сервере.

Активация удаленного стола Контур.Доступ

Выполните шаги:

1. Откройте файл конфигурации **/etc/ibatyr/config** и добавьте строку:

```
KONTUR_DOSTUP_URL = 'https://dostup.kontur.ru'
```

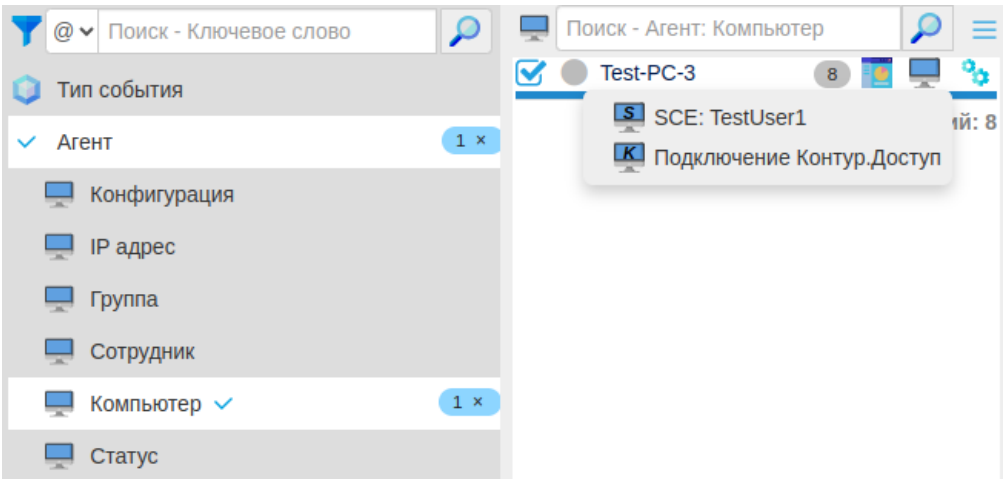
2. Перезагрузите сервер:

```
sudo ibatyr restart
```

Как подключиться

Чтобы подключиться к рабочей станции через удаленный рабочий стол:

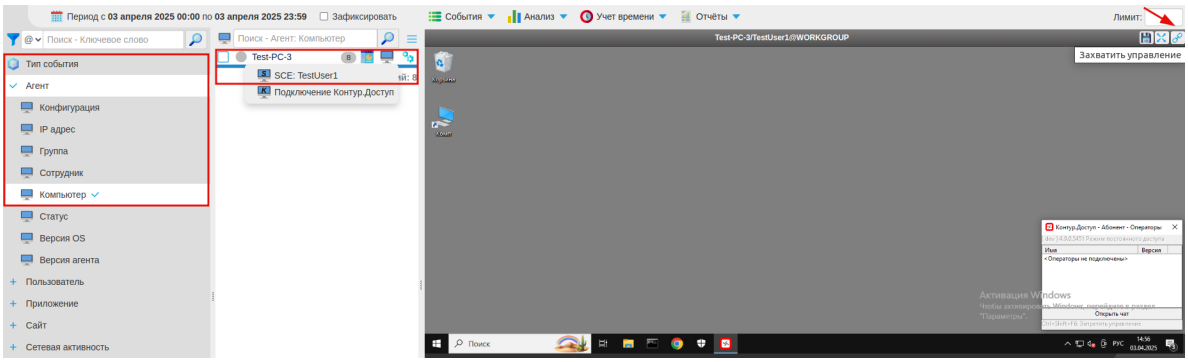
1. В панели измерений выберите **Агенты** → **Компьютер**.
2. В появившемся списке агентов найдите нужный компьютер.
3. Нажмите на значок монитора рядом с именем агента. Отобразится меню с опциями **iBatyr Monitor** и **Контур.Доступ**.



Выберите ваш вариант подключения.

iBatyr Monitor

1. При выборе **iBatyr Monitor** отобразится список активных пользователей компьютера.
2. Нажмите на пользователя для просмотра удаленного рабочего стола. В правой части экрана появится окно удаленного рабочего стола.
3. Для управления компьютером нажмите кнопку **Захватить управление** в правом верхнем углу окна подключения.



Пользователь заметит подключение по окну в нижнем правом углу стола.

Чтобы выйти, повторно нажмите кнопку **Захватить управление**.

Контур.Доступ

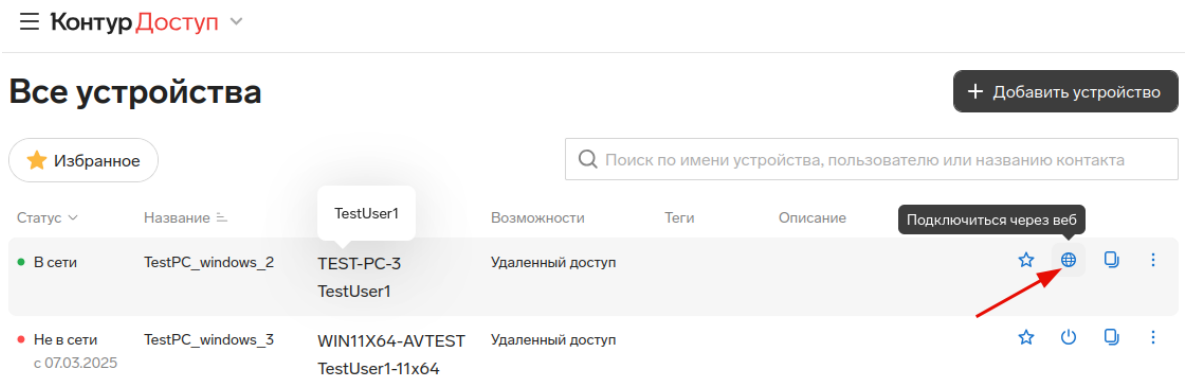
При выборе этого подключения удаленный рабочий стол откроется сразу, если компьютер есть в списке Контур.Доступа. Чтобы компьютер появился в списке, настройте абонента по инструкции на сайте Контура.

Примечание: Пользователь заметит ваше присутствие по окну в нижнем правом углу.

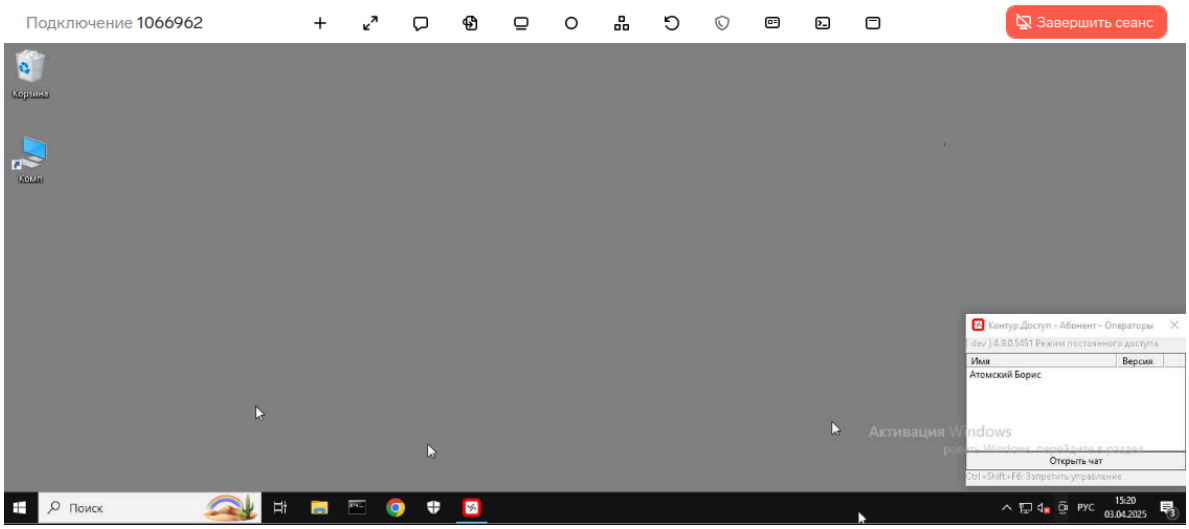
Некоторые браузеры блокируют всплывающее окно удалённого рабочего стола, поэтому во время подключения открывается сайт dostup.kontur.ru. Чтобы удаленный стол открывался сразу во всплывающем окне, разрешите всплывающие окна для dostup.kontur.ru или отключите блокировку всплывающих окон на время подключения.

Как подключиться вручную, если открылся сайт dostup.kontur.ru:

1. В списке компьютеров нажмите значок подключения рядом с нужным пользователем.

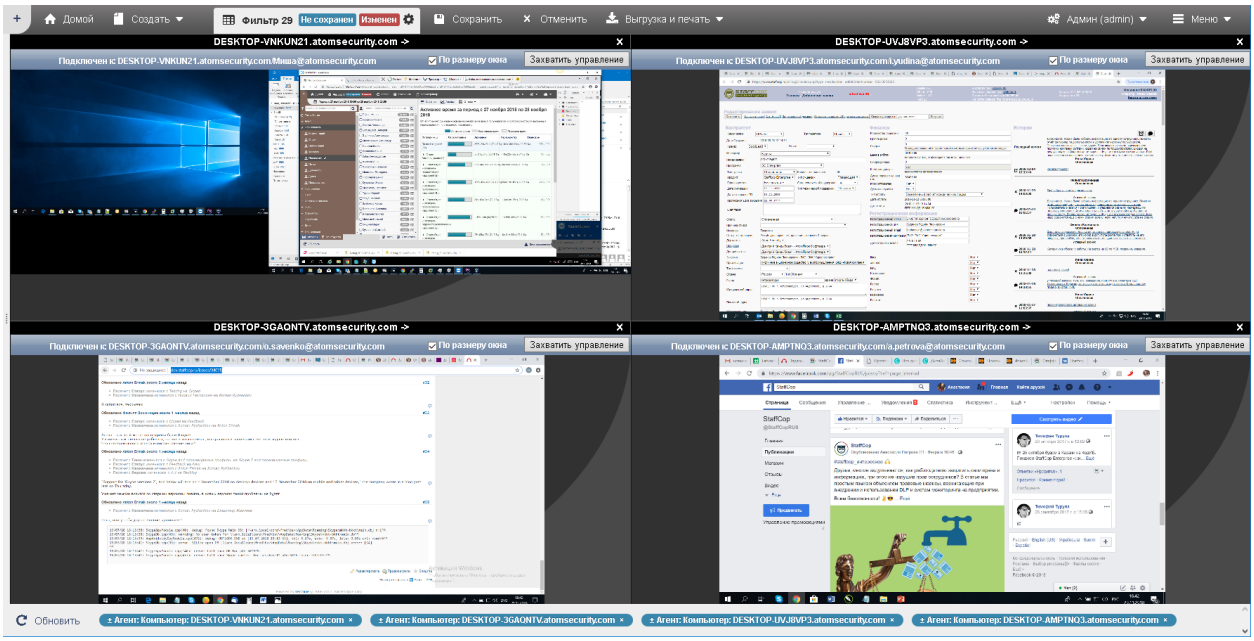


2. Откроется рабочий стол:

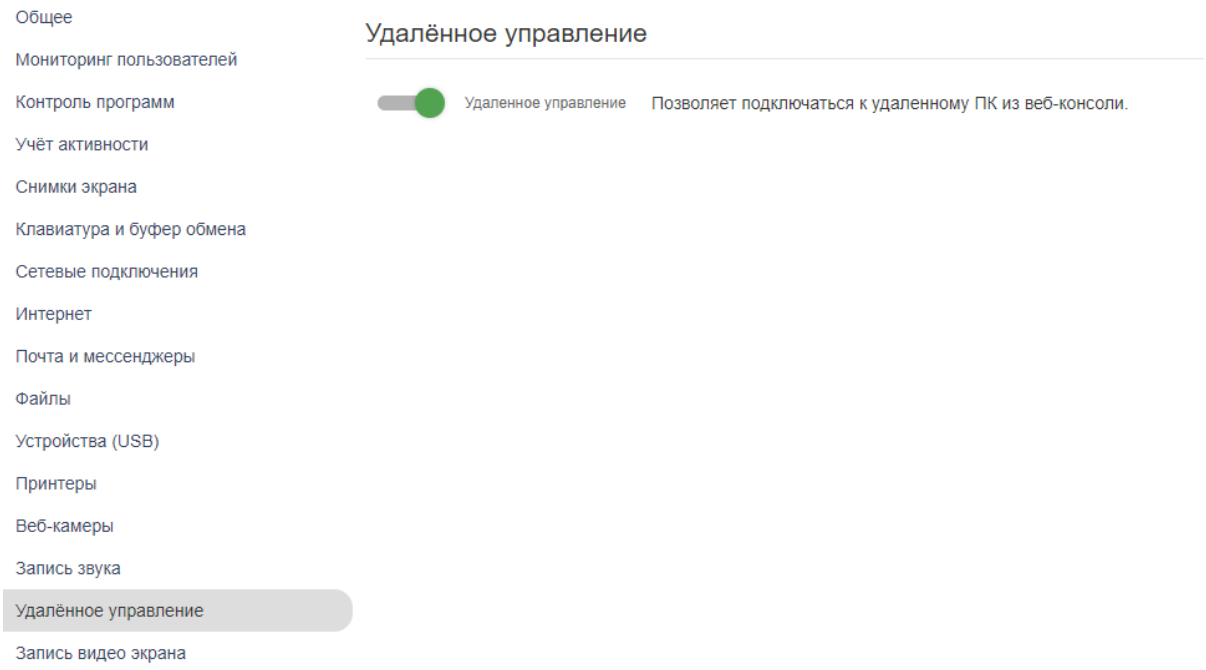


4.2.19 Квадратор

Квадратор - это модуль, который позволяет включить наблюдение сразу за несколькими удаленными рабочими столами.



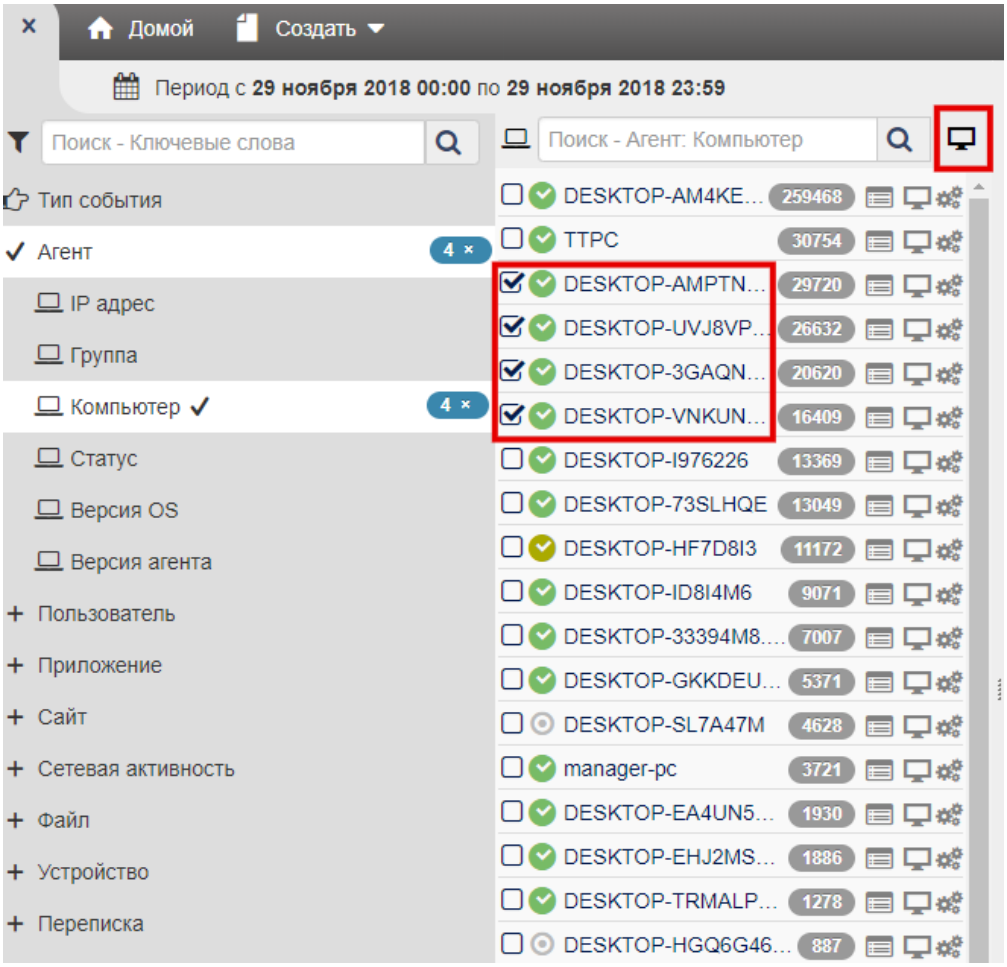
Для работы данного модуля в вашей конфигурации должно быть включено **Удалённое управление**.



Включение: В панели измерений выбрать Агент → Компьютер.

В конструкторе появится список Агентов, выберите необходимые для просмотра агенты (максимум 16).

Нажмите на значок монитора над списком агентов, чтобы подключиться к выбранным компьютерам.



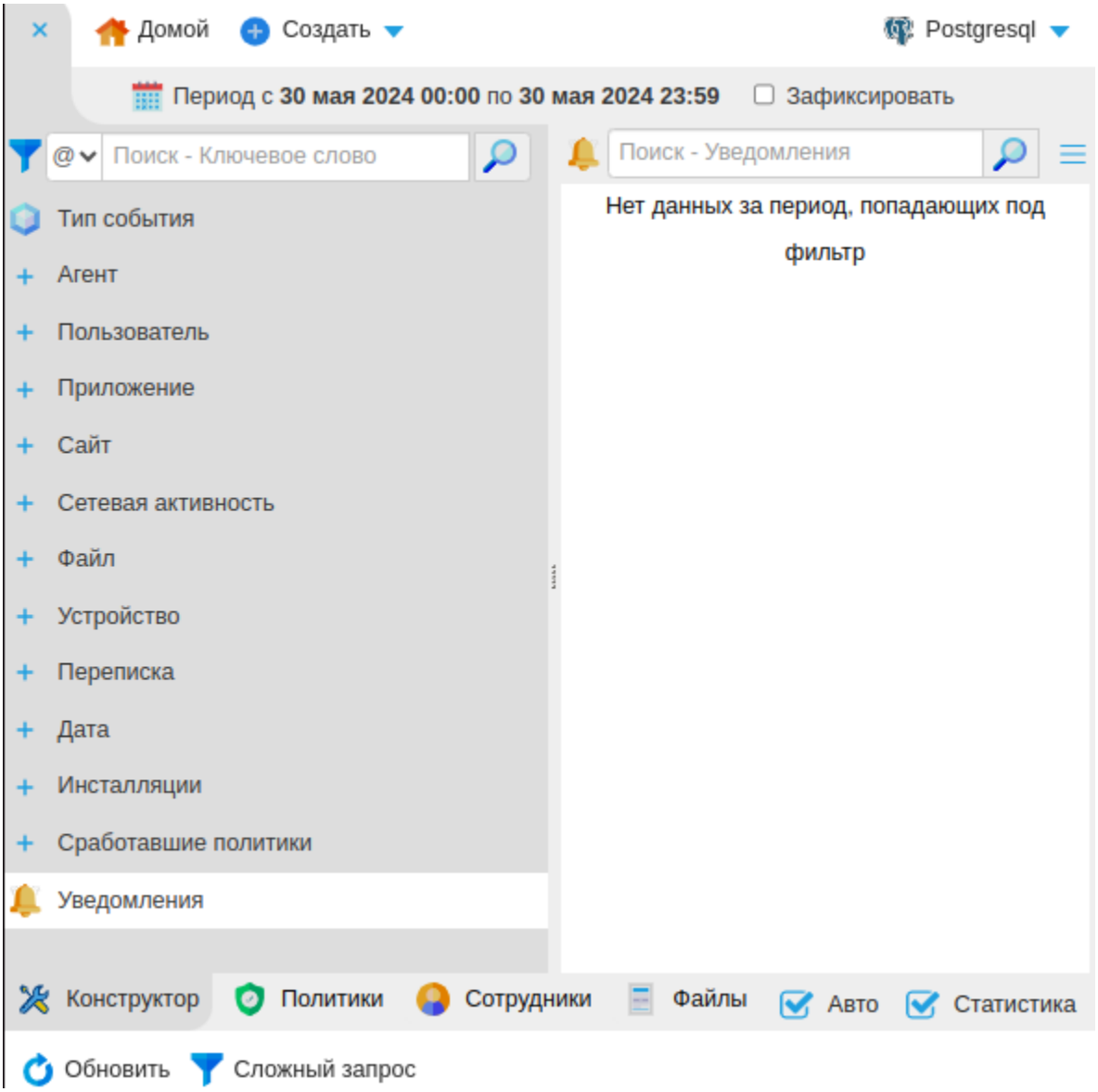
После успешного подключения, в окне должны отобразиться рабочие столы пользователей.

Ненужные окна можно закрыть, рабочая область автоматически будет подстраиваться под количество подключенных компьютеров

Для управления подключенными компьютерами нужно нажать на кнопку «Захватить управление» в правом верхнем углу окна подключения, при этом, если пользователь находится за рабочим местом, то он сможет это заметить.

4.2.20 Уведомления

Уведомления — оповещения, появляющиеся при срабатывании определённых политик. Сработавшие уведомления можно посмотреть на вкладке **Конструктор — уведомления**.



Примечание: Срабатывание уведомления можно *отправлять на почту как обычный фильтр или политику*.

Уведомления и критерии их появления

tabularytabulary

Уведомлени
СНИЛ
Операция заблокирован
Изменение оборудовани
Долгая неактивность агент
Причина отсутстви
Свое лиц
Отсутствие на рабочем мест
Нет снимк
Несколько ли
Паспор
Штам
Удаленное подключени
Присутствие подтвержден
Опоздание пользовател
Новый аген
Присутствие подтверждено с ошибко
Неизвестное лиц
Постороннее лиц
Выгрузка данных клиентом после длительного перерыв
Нет лиц

Особенности работы уведомлений:

- при включении уведомления, все события для всех пользователей проверяются по его политике, и на основе срабатываний генерируются соответствующие уведомления;
- если уведомление выключили, накопленные по нему данные сбрасываются и при новом включении уведомления, пользователи и события сканируются заново;
- если уведомление сработало, при следующем срабатывании политики оно не сработает, если состояние проверяемого объекта не изменилось;
- уведомления по опозданиям сбрасывают счётчик срабатывания один раз в сутки в 00:00, т. к. должны оповещать один раз в день.

4.3 Работа с данными

4.3.1 Конструктор

Работа в Конструкторе

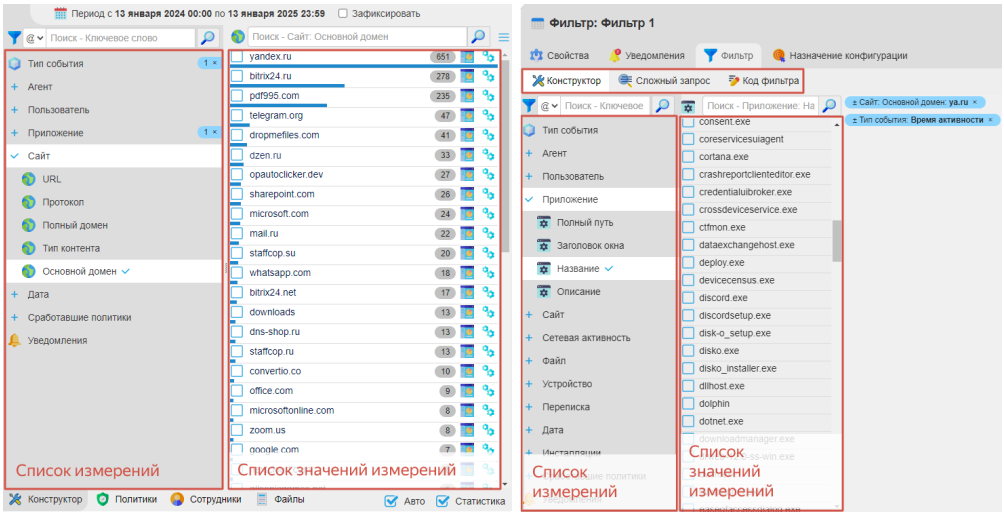
Содержание

- *Работа в Конструкторе*
  - *Как использовать конструктор*
  - *Поиск — Ключевое слово*

- *Датапикер*
- *Измерения*
- *Значения измерений*
- *Сложный запрос*
- *Код фильтра*

Конструктор запросов — основной инструмент для отображения и фильтрации данных в веб-интерфейсе iBatyr Monitor.

Конструктор располагается на главной странице и *на странице фильтра*:



Основные элементы конструктора:

- **Фильтр времени** (**Датапикер**) — выбор временного диапазона для отображения данных, например месяц или год.
- **Поиск** — поле для поиска по тексту, фразе или регулярному выражению.
- **Измерения** — список измерений для фильтрации данных: **Типы событий**, **Пользователи**, **Устройства** и др.
- **Значения измерений** — список значений для выбранного измерения. Например, список всех пользователей для измерения **Пользователь**.
- **Поиск по измерению** — поиск значений внутри выбранного измерения.

Конструктор на странице фильтра содержит две дополнительные кнопки:

- **Сложный запрос** — окно для фильтрации данных с помощью логических выражений **И**, **ИЛИ**.
- **Код фильтра** — текстовый редактор для изменения параметров фильтра или передачи кода фильтра в службу поддержки.

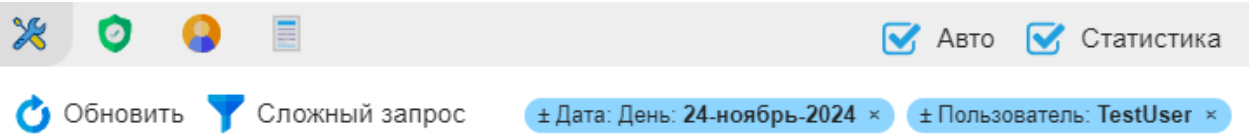
Как использовать конструктор

В соответствии с выбранным измерением меняется содержимое панели конструктора.

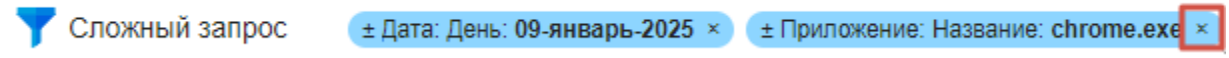
Пример: Вывести события пользователя *TestUser* за 24 ноября.

1. Выберите измерение **Пользователь** → **Пользователь** в **Списке измерений**.
2. Выделите значение *TestUser* в **Списке значений измерений**.
3. Выберите измерение **Дата — По дням** в **Списке измерений**.
4. Выделите значение *24-ноябрь-2024* в **Списке значений измерений**.

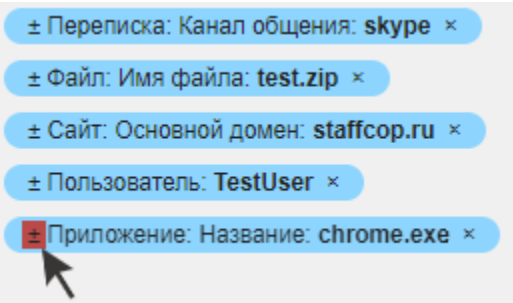
Условия фильтрации отображаются в левом нижнем углу страницы.

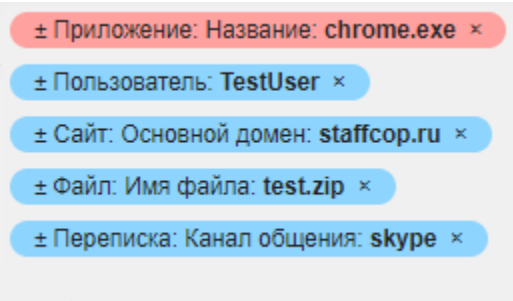


Нажмите **x** на условии, чтобы полностью удалить его.



Нажмите на ±, чтобы исключить только значение. Например, нажмите на ± возле значения *chrome.exe*, чтобы исключить события из приложения *Google Chrome*.

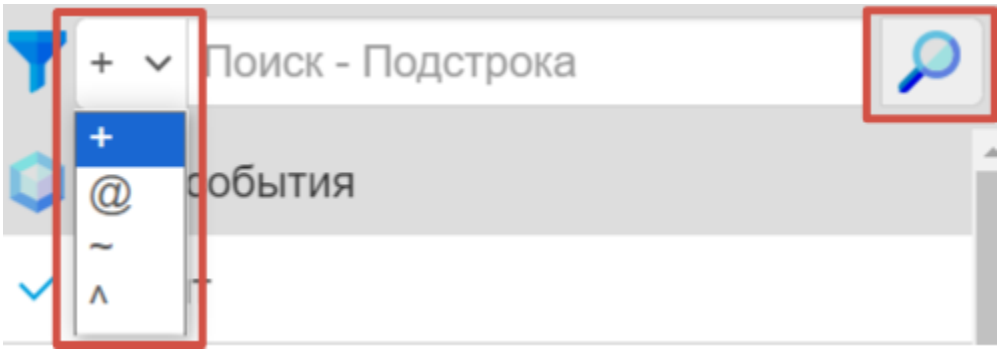




Поиск — Ключевое слово

Поле **Поиск — Ключевое слово** позволяет искать данные по ключевому слову, подстроке или регулярному выражению.

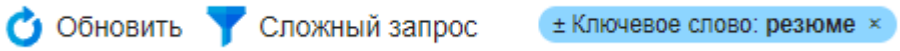
Для выбора условия нажмите на выпадающее меню рядом с полем поиска:



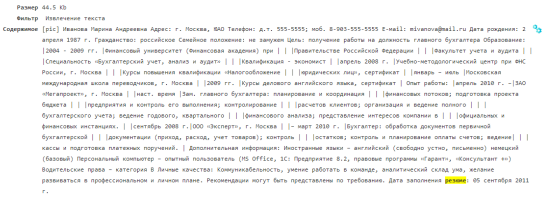
- **@** — ключевое слово;
- **+** — подстрока;
- **~** — *регулярное выражение* без учета регистра;
- **^** — *регулярное выражение* с учетом регистра.

Пример. Найти события по ключевому слову *резюме*.

1. Слева от поля **Поиск — Ключевое слово** выберите опцию **@**.
2. В поле **Поиск — Ключевое слово** введите *резюме* и нажмите кнопку поиска. После этого в нижнем левом углу появится условие поиска, а в **Линзе событий** отобразятся события, которые содержат *резюме*.



3. Нажмите на событие в **Линзе**, чтобы посмотреть информацию по нему. Ключевое слово будет выделено желтым цветом.



См.также:

Подробнее об условиях поиска

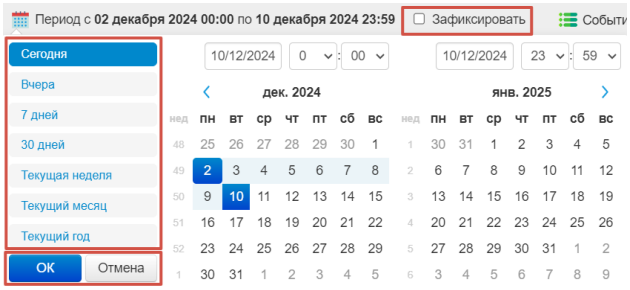
Датапикер

Датапикер позволяет отфильтровать события по времени. Чтобы его открыть, нажмите на строку **Период с** в верхней панели слева.

Установить время можно тремя способами:

- выделите дни на календаре;
- укажите даты начала и конца периода в поле ввода;
- выберите подходящую опцию слева от календаря.

После выбора даты поставьте галочку **Зафиксировать**. Благодаря этому фильтр времени не сбросится при обновлении страницы через кнопки **Домой** и **Обновить** или клавишу **F5**.

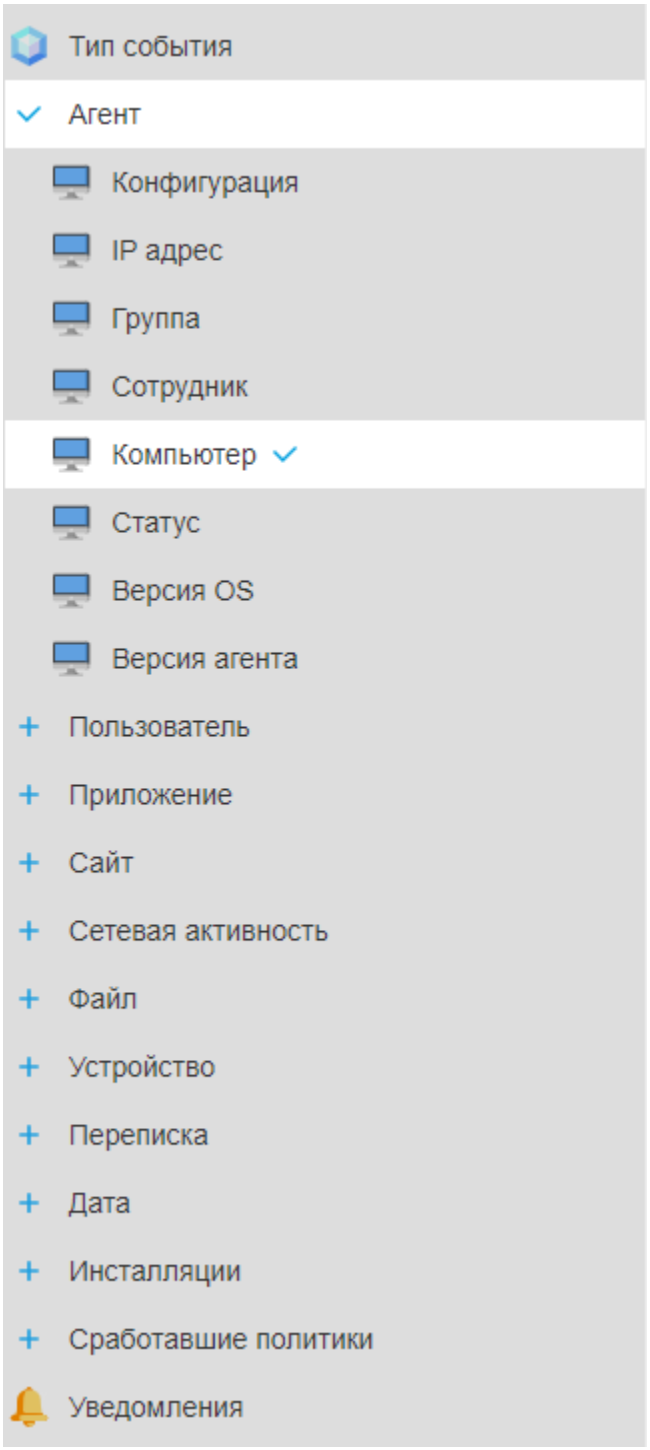


Измерения

Фиксированный список категорий измерений, который отображается в левой части окна. При выборе измерения конструктор покажет события мониторинга только для этого измерения.

См.также:

Подробное описание измерений.



Вы можете выбрать сразу несколько измерений.

Пример. Показать события **** для пользователя *TestUser*.

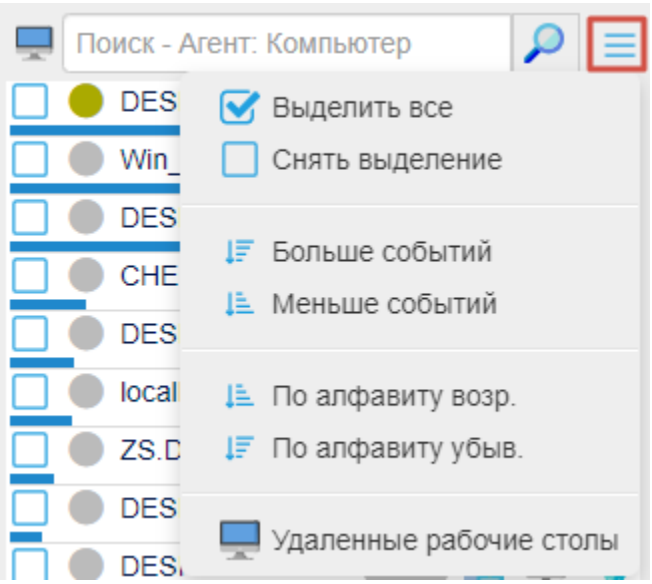
1. Нажмите на **Тип события**.
2. Выберите в соседней колонке значений событие ****.
3. В списке измерений нажмите **Пользователь** и выберите пользователя *TestUser* из списка значений.

Значения измерений

Позволяет отфильтровать события по конкретным значениям выбранного измерения. Например, при выборе измерения **Компьютер** появится список всех компьютеров. Выберите компьютер, чтобы в **Линзе** отобразились релевантные события.

Примечание: При создании или редактировании фильтра установленные в **Датапикере** даты не учитываются, поэтому в окне фильтра конструктор покажет данные за все время.

Для управления списком нажмите три горизонтальных линии в правом углу:



Добавление правил мониторинга из конструктора

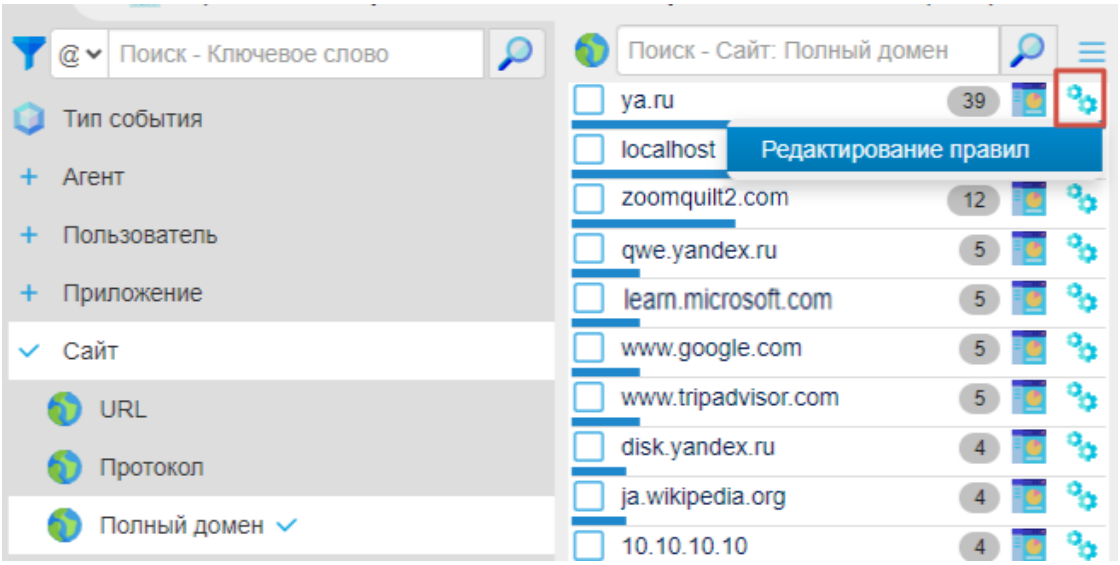
В **Конструкторе** вы можете добавить правило мониторинга *в конфигурацию компьютера*.

Доступно добавление правил для следующих измерений:

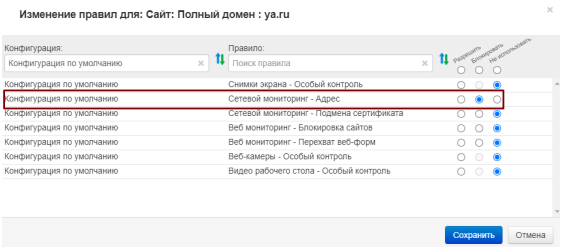
- Пользователь — Пользователь,
- Приложение — Название,
- Сайт — Полный домен,
- Сайт — URL,
- Сайт — Основной домен,
- Сайт — Тип контента,
- Сетевая активность — IP-адрес,
- Сетевая активность — Сетевой порт,
- Файл — Путь файла,
- Устройство — ID-устройства,
- Устройство — Класс устройства.

Пример. Пользователи регулярно посещают сайт *ya.ru*, поэтому нет необходимости в отслеживании активности на сайте. Нужно добавить запрет на отслеживание в **Конфигурацию по умолчанию**.

1. На главной странице веб-интерфейса в **Списке измерений** выберите **Сайт — Полный домен**.
2. В **Списке значений измерений** найдите значение *ya.ru*.
3. Нажмите на иконку шестеренок рядом со значением и выберите **Редактирование правил**. Откроется окно добавления правил в конфигурацию.

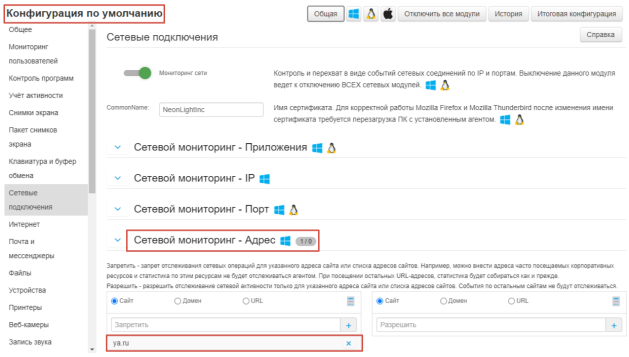


4. Выберите **Конфигурацию по умолчанию** и выберите **Блокировать** для поля **Сетевой мониторинг — Адрес**.



5. Нажмите **Сохранить**.

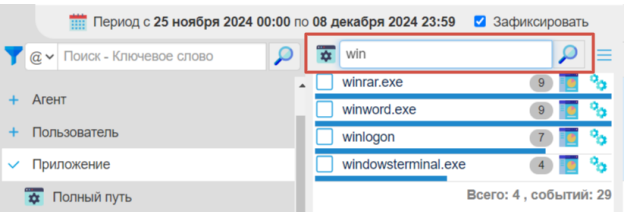
В результате для **Конфигурации по умолчанию** в разделе **Сетевой мониторинг — Адрес** добавлен запрет отслеживания событий с *ya.ru*.



Поиск по измерению

Поле ввода **Поиск — Измерение** позволяет найти значение измерения в конструкторе.

Пример. За сутки пользователи открыли более ста приложений, вы хотите найти события *winword.exe*. Выберите в списке измерений **Приложения** → **Название** и введите в поиске *win*.



Сложный запрос

Дополнительная кнопка в конструкторе на странице фильтра. Используйте сложный запрос для группировки нескольких простых условий через логические операторы.

Когда вы указываете условия фильтрации в **Конструкторе**, между измерениями стоит **И** — например, тип события **И** имя пользователя. В **Сложном запросе**, кроме **И**, доступен оператор **ИЛИ**.

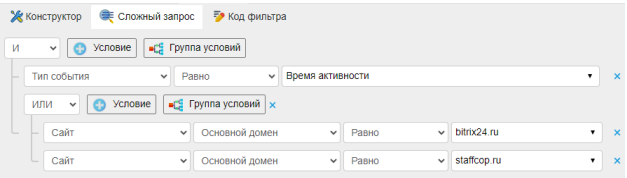
Используйте логические операторы:

- **И**: чтобы оба условия должны быть выполнены;
- **ИЛИ**: если достаточно одного выполненного условия.

Сложный запрос удобнее для настройки фильтра *политик*, потому что для их фильтрации используются более комплексные условия.

Пример. Нужно создать политику, которая отслеживает посещение корпоративных сайтов.

1. Нажмите + **Создать** — **Политика**. Откроется окно создания политики.
2. Укажите название *Рабочие ресурсы* и нажмите **Политика активна**.
3. Перейдите на вкладку **Фильтр** — **Сложный запрос**.
4. Нажмите + **Условие** и выберите **Тип событий** — **Равно** — **Время активности**.
5. Выберите оператор **И** и нажмите **Группа условий**.
6. Нажмите + **Условие** и выберите **Сайт** — **Основной домен** — **Равно** — *ibatyr.kz*.
7. Выберите оператор **ИЛИ** и нажмите + **Условие**.
8. Нажмите + **Условие** и выберите **Сайт** — **Основной домен** — **Равно** — *bitrix24.ru*.



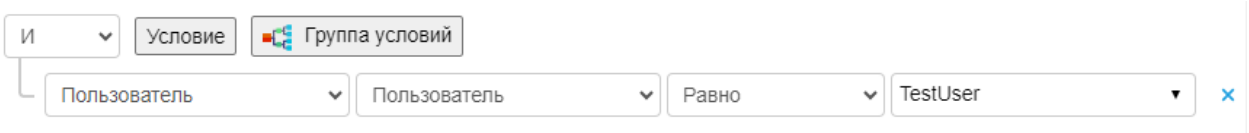
Условные операторы сложного запроса

Сложные запросы позволяют фильтровать события, комбинируя операторы сравнения. Эти операторы помогают задать условия, по которым данные будут включаться или исключаться из выборки.

Равно / Не равно

Равно выводит события, значения которых строго равны значению в условии.

Вывести события пользователя *TestUser*:



Не равно исключает события с указанным значением.

Отобразить письма, отправленные на любой домен, кроме *company_ domain.ru*:

Содержит / Не содержит

Содержит выводит события, если их значение включает указанную подстроку.

Вывести события с файлами, в названии которых содержится подстрока *УПД*, например *УПД 2.xls*, *УПД.rtf*, *Обновленный упд2_ 0.pdf*:

Не содержит исключает события, содержащие указанную подстроку.

Отфильтровать файлы, в названии которых нет слова *screenshot*:

В списке / Не в списке

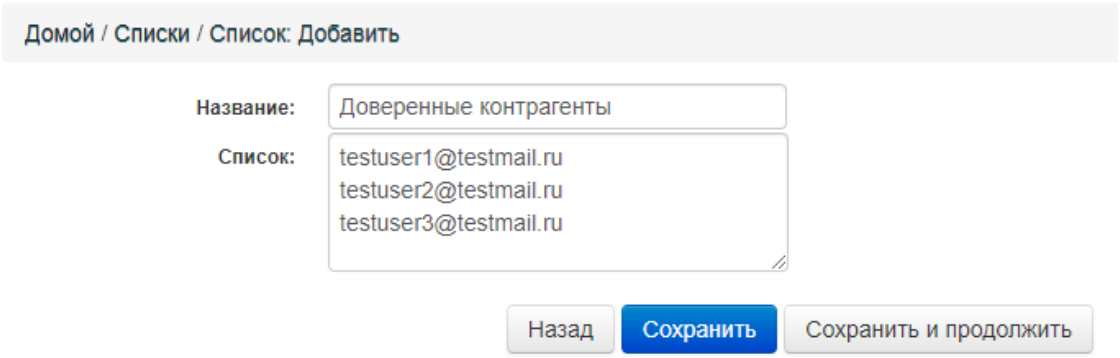
В списке выводит события, значения которых входят в список значений.

См.также:

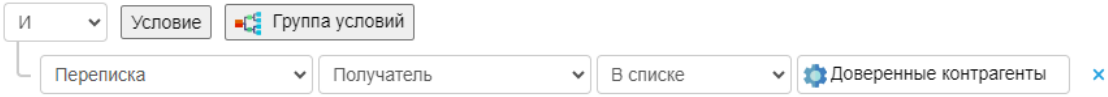
Подробнее о создании и редактировании списков

Чтобы найти письма, отправленные на адреса *testuser1@testmail.ru*, *testuser2@testmail.ru* или *testuser3@testmail.ru* из списка *Доверенные контрагенты*:

1. Создайте список *Доверенные контрагенты* и добавьте в него значения.



2. Добавьте условие:



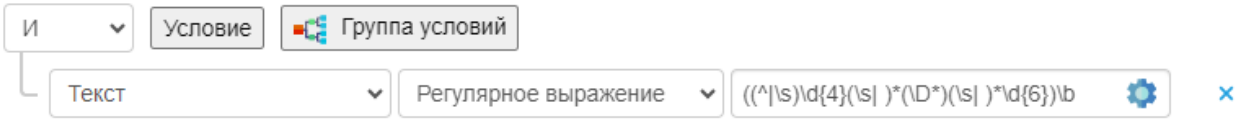
Не в списке исключает события со значениями из списка.

Вывести события с устройствами, которые не входят в список *Доверенные USB-накопители*:

Регулярное выражение

Выводит события, значения которых соответствуют *шаблону регулярного выражения*.

Найти события, содержащие номер паспорта *4321 567890*:



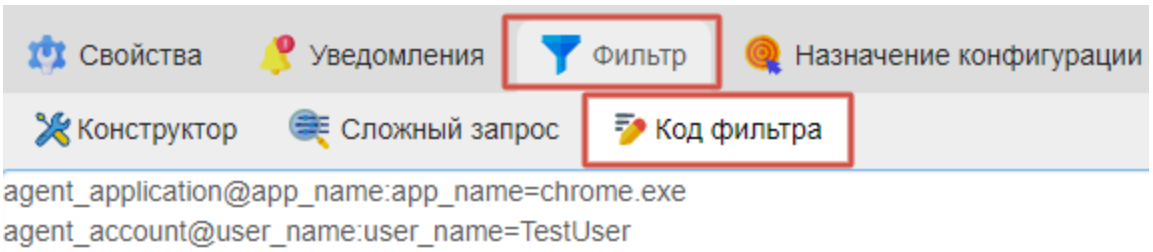
См.также:

Подробнее о работе с регулярными выражениями

Код фильтра

Код фильтра отображает условия фильтрации, которые были заданы через **Конструктор** или **Сложный фильтр**.

Предупреждение: Вы можете проверить значения параметров в **Коде фильтра**, но не используйте его для полноценной настройки. При возникновении вопросов или ошибок во время работы с фильтром, скопируйте код и передайте его *в службу технической поддержки*.



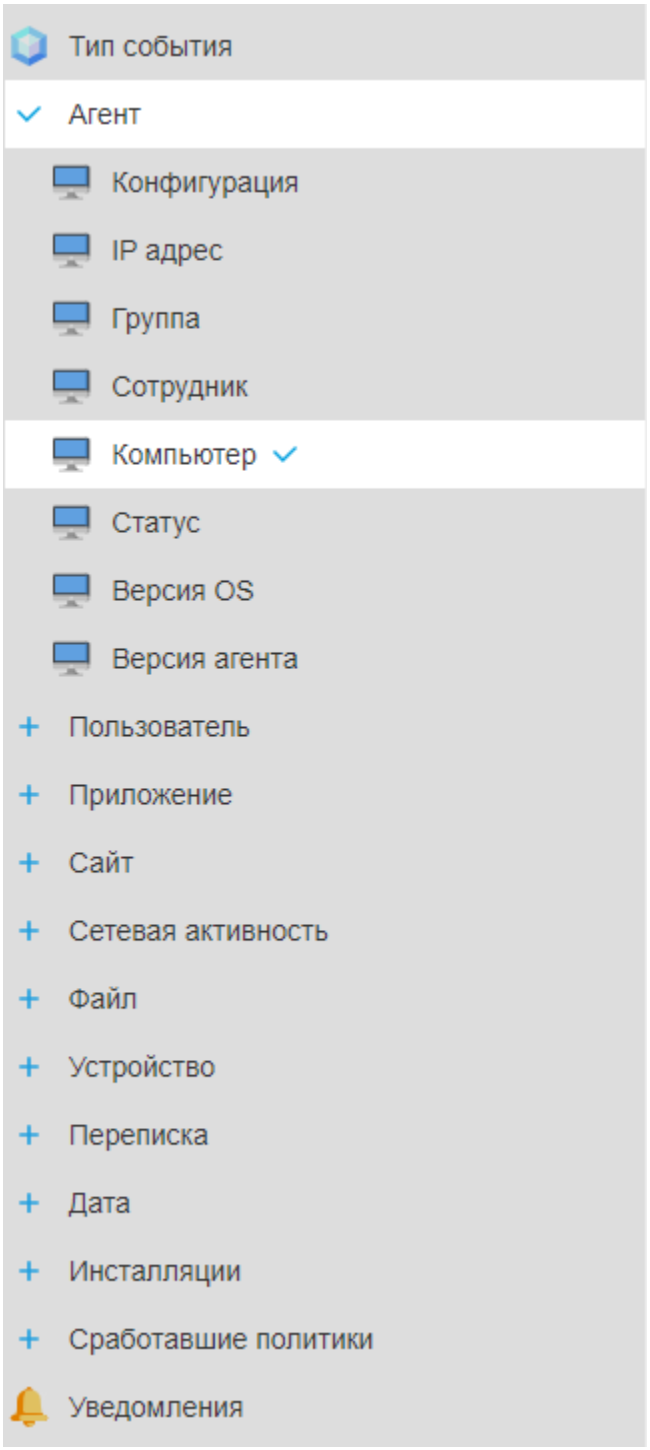
Список измерений

Содержание

- *Список измерений*
  - *Тип события*
  - *Агент*
  - *Пользователь*
  - *Приложения*
  - *Сайт*
  - *Сетевая активность*
  - *Файл*
  - *Устройство*
  - *Переписка*
  - *Дата*
  - *Инсталляции*
  - *Сработавшие политики*
  - *Уведомления*

Список измерений — основной инструмент фильтрации данных. Измерения относятся к категории: типу события, агенту, пользователю и так далее. При выборе одной или нескольких категорий и измерений в **Линзе** отображаются соответствующие события.

Список располагается в левой части **Конструктора**:

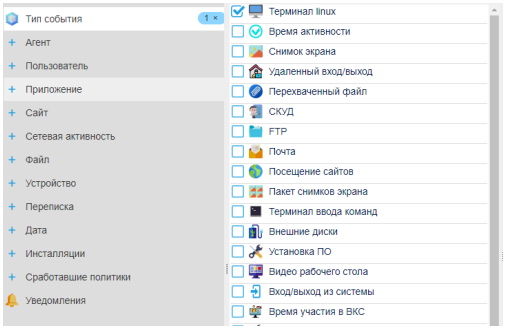

Тип события
Агент
Конфигурация
IP адрес
Группа
Сотрудник
Компьютер
Статус
Версия OS
Версия агента
Пользователь
Приложение
Сайт
Сетевая активность
Файл
Устройство
Переписка
Дата
Инсталляции
Сработавшие политики
Уведомления

Тип события

Категория, которая позволяет фильтровать данные по **Типу событий**.

Агенты перехватывают события разных типов в зависимости от модулей, активированных *в конфигурации*. Список типов события соответствует основным модулям мониторинга: **Ввод с клавиатуры**, **Посещение сайтов** и др.

Чтобы события определенного типа отразились в **Линзе**, выберите сначала **Тип события** в конструкторе, а затем тип события в списке значений:

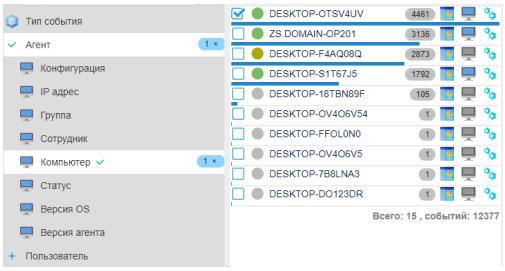


См.также:

Подробнее о Типах событий

Агент

Категория отображает список компьютеров, на которых установлен агент. При выборе измерения **Конструкторе** отображаются имена компьютеров:



Чтобы посмотреть события от установленных на компьютерах агентов, выберите агент в списке.

Измерения для фильтрации агентов:

- **Конфигурация** — присвоенная агенту конфигурация;
- **IP адрес** — IP-адрес агента;
- **Группа** — группа, к которой относится агент. Поле заполняется вручную в разделе **Панель управления** → **Компьютеры**;
- **Сотрудник** — сотрудники, которые работают за компьютером. Поле заполняется вручную в разделе **Панель управления** → **Компьютеры**;
- **Компьютер** — имя ПК, на котором установлен агент;

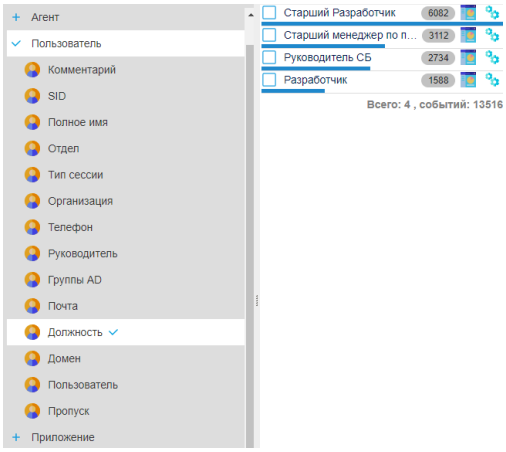
Примечание: Чтобы имя компьютера обновлялось автоматически, активируйте параметр **Автоматически обновлять имя компьютера** в **Панель управления** → **Параметры сервера**.

- **Статус** — статус активности компьютера;
- **Версия OS** — версия операционной системы компьютера;
- **Версия агента** — версия агента.

Примечание: Нумерация версий агентов различается: у Windows-агента версии могут быть, например, *2588* или *2570*, а у Linux-агента — *0.16.18-master*.

Пользователь

Отображает в **Конструкторе** список учетных записей, зарегистрированных на компьютерах с установленным агентом.



Связанные с пользователями события можно посмотреть в **Таблице событий**. Для этого выберите пользователя в списке значений.

Примечание: Чтобы значения измерений автоматически обновлялись, *настройте синхронизацию с Active Directory*.

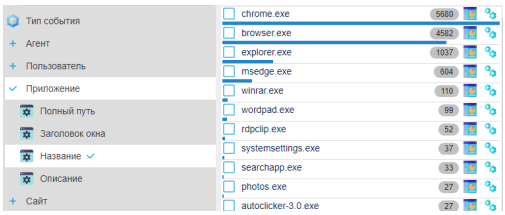
Состоит из измерений:

- **Комментарий** — комментарий к учетной записи;
- **SID** — уникальный идентификатор учетной записи;
- **Полное имя** — полное имя учетной записи;
- **Отдел** — отдел пользователя;
- **Тип сессии** — тип сессии для авторизации;
- **Организация** — организация, в которой работает пользователь;
- **Телефон** — телефон пользователя;

- **Руководитель** — руководитель пользователя;
- **Группы AD** — группы AD, в которых значится учетная запись;
- **Почта** — адрес электронной почты учетной записи;
- **Должность** — должность пользователя учетной записи;
- **Домен** — домен, в котором находится учетная запись;
- **Пользователь** — имя пользователя;
- **Пропуск** — номер пропуска учетной записи. Может использоваться *для интеграции со СКУД-системами*.

Приложения

Отображает в **Конструкторе** список приложений.

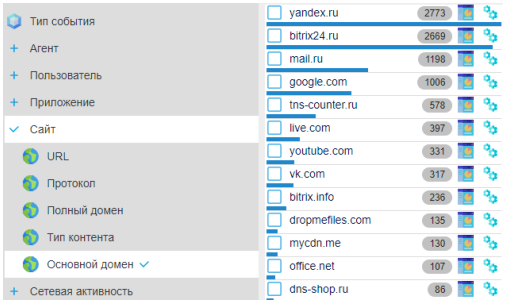


Измерения для фильтрации приложений:

- **Полный путь** — полный путь к исполняемому файлу;
- **Заголовок окна** — заголовок окна приложения;
- **Название** — название приложения;
- **Описание** — описание приложения.

Сайт

Отображает список сайтов по исполняемым файлам, заголовку окна, абсолютному пути или по названию программы.



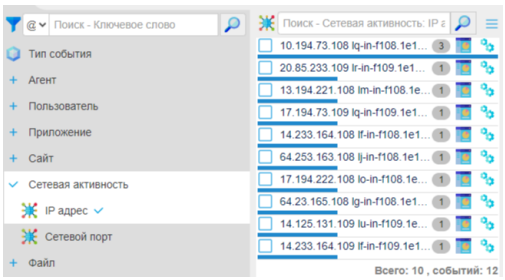
Состоит из измерений:

- **URL** — URL сайта;
- **Протокол** — протокол, по которому происходило подключение к сайту;
- **Полный домен** — полный домен сайта;

- **Тип контента** — тип контента, который был получен при подключении к сайту, например, *application* или *x-javascript*;
- **Основной домен** — основной домен сайта.

Сетевая активность

Категория измерений, которая отображает список характеристик сетевых соединений. Отображает соединения с различными IP и статистику использования портов за выбранный период.

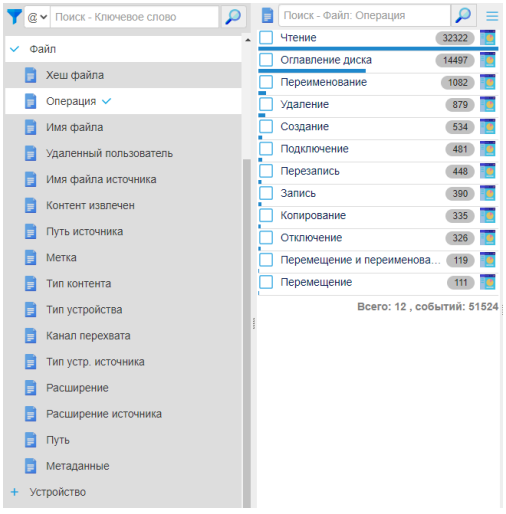


Состоит из измерений:

- **IP адрес** — подключенные к компьютеру IP-адреса;
- **Сетевой порт** — активные порты.

Файл

Категория измерений, которая отображает список файлов. Позволяет просмотреть информацию о перехваченных файлах.



Состоит из измерений:

- **Хеш файла** — уникальная строка для проверки целостности файла;
- **Операция** — файловая операция, например, копирование или удаление;
- **Имя файла** — имя файла;
- **Удаленный пользователь** — операция с файлом, выполненная удалённым пользователем;

- **Имя файла источника** — имя исходного файла;

  Примечание: При перемещении или копировании файла извлекается информация и о его источнике.

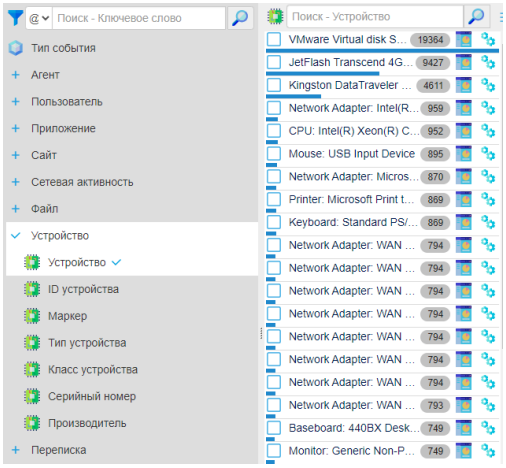
- **Контент извлечен** — указывает, был ли извлечен контент из события;
- **Путь источника** — путь к исходному файлу;
- **Метка** — установленная в файле метка;

  См.также:

  Для работы меток включите *DLP-модуль*.
- **Тип контента** — тип контента, файла, например, *text* или *html*, *application* или *x-javascript*;
- **Тип устройства** — тип устройства, на котором располагался файл;
- **Канал перехвата** — канал перехвата файла, например, *Буфер обмена* или *Печать документов*;
- **Тип устр. источника** — тип устройства, на котором располагался файл-источник;
- **Расширение** — расширение файла;
- **Расширение источника** — расширение исходного файла;
- **Путь** — путь к файлу;
- **Метаданные** — метаданные файла в формате JSON.

Устройство

Категория измерений, которая отображает список устройств по именам. Позволяет посмотреть устройства, которые были подключены к ПК за выбранный период.



Состоит из измерений:

- **Устройство** — имя устройства;
- **ID устройства** — ID устройства;
- **Маркер** — маркер устройства;
- **Тип устройства** — тип устройства;

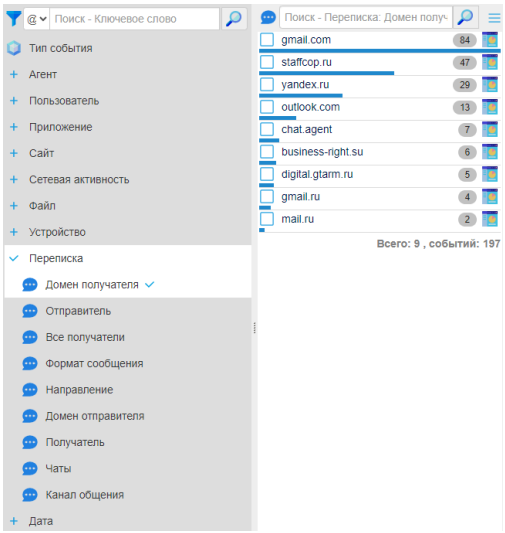
- **Класс устройства** — класс устройства;
- **Серийный номер** — уникальный номер устройства, который не меняется вне зависимости от ОС и способа подключения;

  См.также:

  Подробнее о Менеджере ВНИ
- **Производитель** — производитель устройства.

Переписка

Категория измерений, которая отображает участников диалогов в переписке по именам.

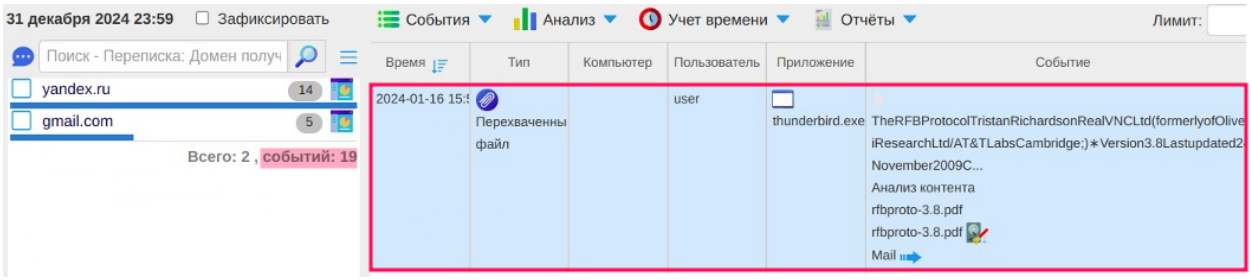


Состоит из измерений:

- **Домен получателя** — домен получателя;
- **Отправитель** — отправитель;
- **Все получатели** — все участники беседы;
- **Формат сообщения** — формат сообщения;
- **Направление** — направление сообщения: **Входящий** или **Исходящий**;
- **Домен отправителя** — домен отправителя;
- **Получатель** — получатель;
- **Чаты** — чаты;
- **Канал общения** — канал связи.

Важно: Количество событий **Переписки** в меню **Конструктора** соответствует количеству получателей и может отличаться от числа событий в **Линзе**.

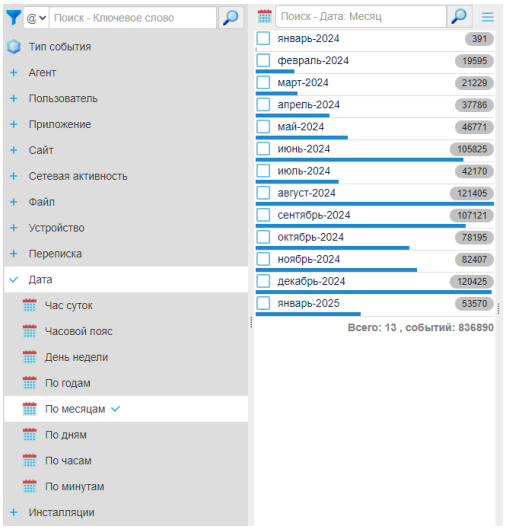
Например, на скриншоте в меню указано 19 событий, но в **Линзе** отображается только одно — **Перехваченный файл**. Количество событий различается, потому что в меню конструктора указаны все получатели файла, а в **Линзе** — событие как таковое.



Дата

Категория измерений, которая отображает события по конкретным датам или абстрактным временным параметрам, таким как месяц или год.

Позволяет выбирать данные за определённый промежуток времени, по часам, дням недели и т. д.



Состоит из измерений:

- **Час суток**,

Примечание: **Час суток** отображает события с группировкой по часам от 0 до 23. Выберите в **Датапикере** период 7 дней и добавьте в **Конструкторе** условие **Дата — Час суток** — *13*, чтобы посмотреть все события за неделю, которые происходили с 13:00 до 13:59.

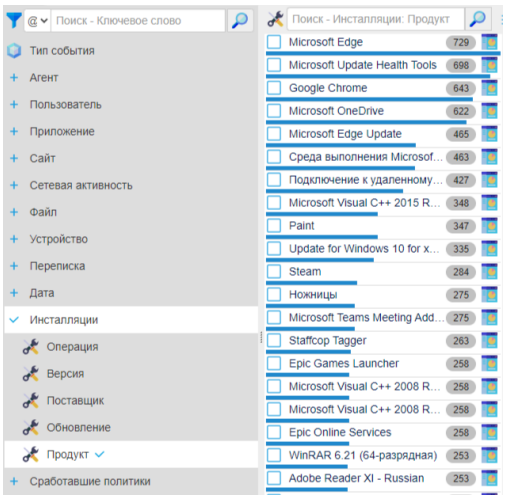
- **Часовой пояс**,
- **День недели**,
- **По годам**,
- **По месяцам**,
- **По дням**,
- **По часам**,

Примечание: **По часам** группирует данные по временным интервалам длительностью в час — например, *12-июля-2024 00:00 - 00:59* или *16-августа-2024 16:00 - 16:59*.

- **По минутам**.

Инсталляции

Отображение списка установленных или удаленных программ:

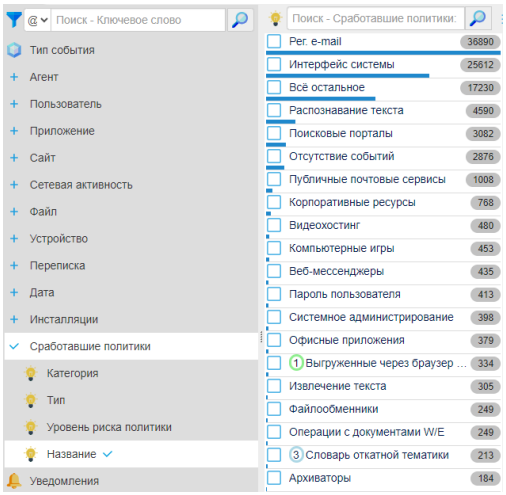


Состоит из измерений:

- **Операция** — операция, которая производилась над программой;
- **Версия** — версия программы;
- **Поставщик** — поставщик программы;
- **Обновление** — показывает обновления;
- **Продукт** — название программы.

Сработавшие политики

Категория измерений, которая отображает список сработавших политик. Позволяет делать выборку по типу сработавших политик и их продуктивности.



Состоит из измерений:

- **Категория** — категория продуктивности политики;

  См.также:

  Подробнее о категориях продуктивности политик

- **Тип** — тип политики;
- **Уровень риска политики** — категория продуктивности политики;

  См.также:

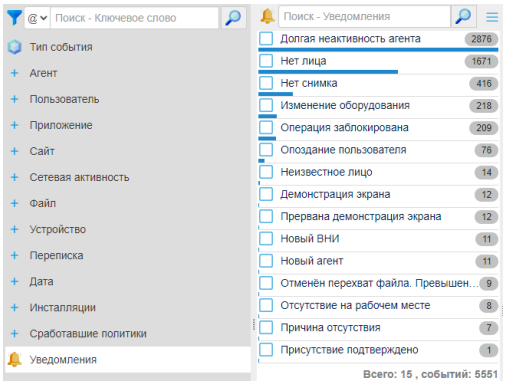
  Для просмотра уровня риска политики включите *Уровень риска*.

- **Название** — название политики.

Уведомления

Категория измерений, которая отображает оповещения от сервера или агента об уникальных событиях безопасности или контроля состоянии системы.

Например, оповещения об опоздании пользователей, длительной неактивности агента, удаленном подключении и пр.

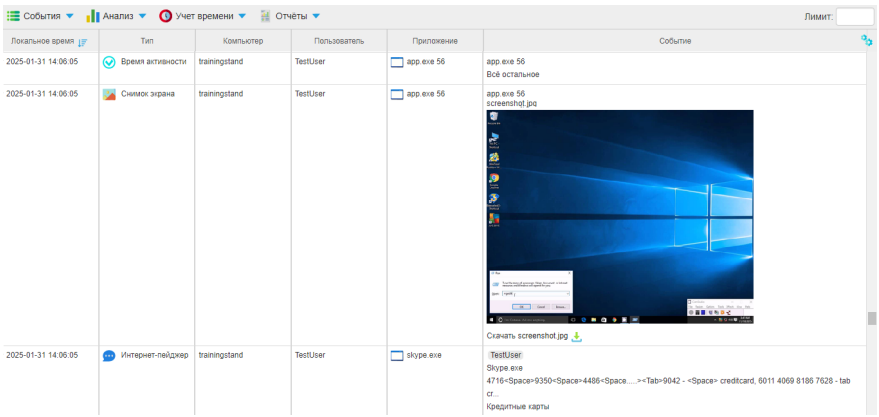


4.3.2 Линза событий

Содержание

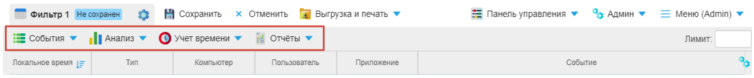
- *Линза событий*
  - *События*
    - *Таблица*
    - *Список*
    - *Снимки*
    - *Активность*
    - *Переписка*
  - *Анализ*
    - *Настройка отображения данных в Анализе*
    - *Представление данных в Анализе*
  - *Учет времени и Отчеты*

Линза событий — это область экрана, в которой отображаются события, графики или отчёты.

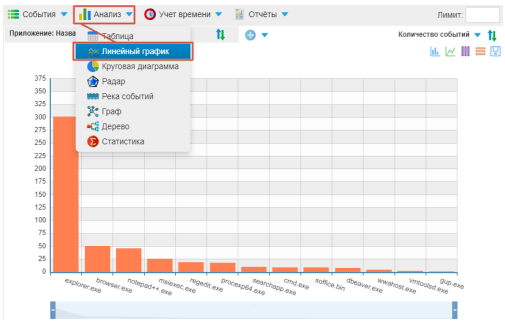


Для выбора отображения информации в **Линзе событий** используйте опции:

- **События** — просмотр событий;
- **Анализ** — отображение статистики;
- **Учет времени**, **Отчеты** — построение отчетов.



По умолчанию в Линзе отображаются событий в виде таблицы. При выборе другой опции интерфейс изменится. Например, выберите **Анализ** → **Линейный график** для отображения событий в виде графика.



При переходе на главную страницу в **Линзе событий** по умолчанию открывается новый **Фильтр 1** без условий фильтрации.

События

В разделе **События** представлена подробная информация о каждом событии. Информация доступна в нескольких режимах просмотра:

- Таблица,
- Список,
- Снимки,
- Активность,
- Переписка.

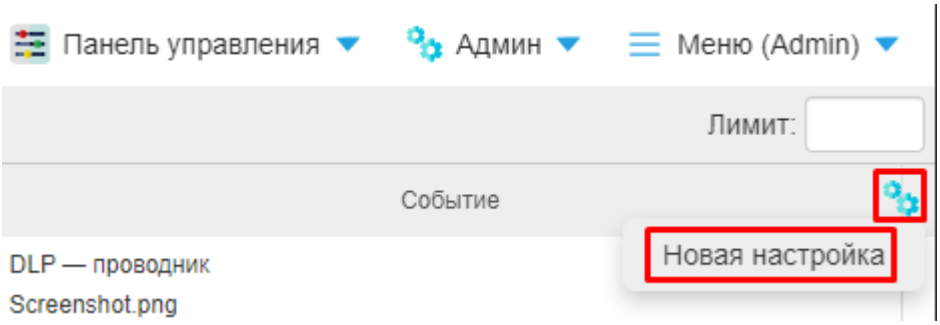
Таблица

Таблица — позволяет просматривать события в табличном формате. В колонках таблицы отображаются сведения о событии: Локальное время, Тип, Компьютер, Пользователь и другие.

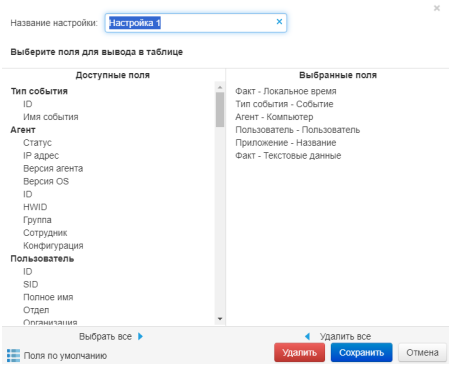
2025-08-06 17:40:59	Действие администратора		a.bakeyev		Администратор Успешная авторизация пользователя "a.bakeyev". IP "10.250.0.137", база данных "default". a.bakeyev
2025-08-06 16:24:11	Посещение сайтов	DESKTOP-R9JTO86	User-1	msedgewebview2.exe	https://deff.nelreports.net/api/report?cat=msn
2025-08-06 16:19:21	Действие администратора		a.bakeyev		Администратор Успешная авторизация пользователя "a.bakeyev". IP "10.250.0.137", база данных "default". a.bakeyev
2025-08-06 15:24:18	Посещение сайтов	DESKTOP-R9JTO86	User-1	msedgewebview2.exe	https://deff.nelreports.net/api/report?cat=msn
2025-08-06 14:47:50	Действие администратора		admin		Администратор Успешная авторизация пользователя "admin". IP "100.67.0.2", база данных "default". admin
2025-08-06 12:34:56	Действие администратора		admin		Расписание Изменено "asdsa" - Изменены для Рабочие дни "DaySchedule object". Изменены для

Чтобы добавить или убрать колонку в таблицу:

1. Нажмите на иконку с шестеренками в правом верхнем углу **Линзы событий**.
2. Выберите **Новая настройка**:



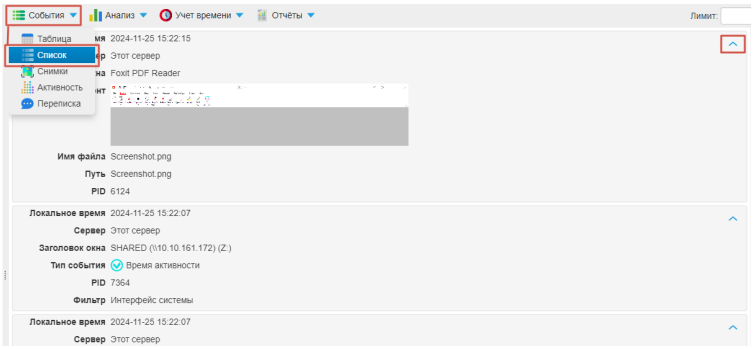
3. Нажмите на значение в разделе **Доступные поля**, чтобы добавить его в таблицу. Поле переместится в список **Выбранные поля**. Нажмите на поле в списке **Выбранные поля**, чтобы убрать его из таблицы.



4. При необходимости измените название настройки в поле **Название настройки**.
5. Нажмите на кнопку **Сохранить** в правом нижнем углу.

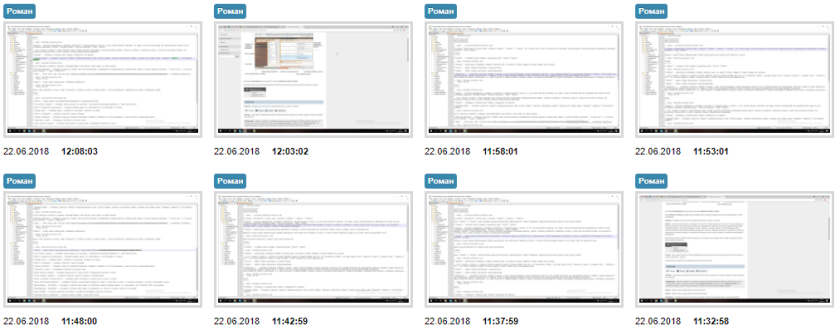
Список

Список — каждое событие отображается в отдельном блоке списка. Этот формат удобен для просмотра каждого события по отдельности.



Снимки

Снимки — события отображаются в виде карточек. Используйте этот формат для просмотра событий **Снимок экрана** и **Снимок с **.



Примечание: При выборе режима отображения **Снимки** условие **Тип события** в фильтре изменится на **Снимок экрана** и **Снимок с **.

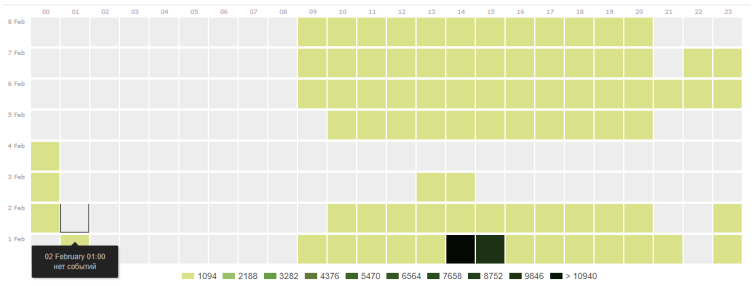
Активность

Активность — показывает количество событий по времени в виде тепловой диаграммы. Чем насыщеннее цвет, тем больше событий произошло в конкретный момент.

При изменении временного диапазона в **Датапикере** цвета могут меняться, потому что изменяется единица времени и вместе с ней количество событий.

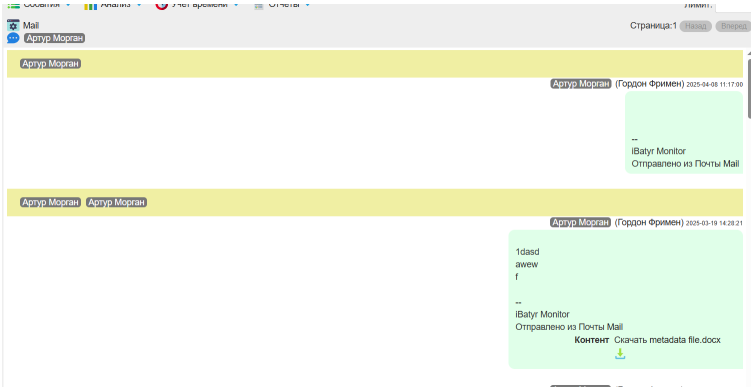
Например, при выборе одного дня единица времени равна минуте, в течение которой пользователь совершает до 10 событий. Если период увеличен до недели, единицей времени станет час, а количество событий возрастёт до 600. Цвет станет более насыщенным.

Кликните на карту активности, чтобы детализировать события за определённое время.



Переписка

Переписка — отображает события **Почта** и **Интернет-пейджер** в виде диалогов. Привязывается к учетным записям пользователей.



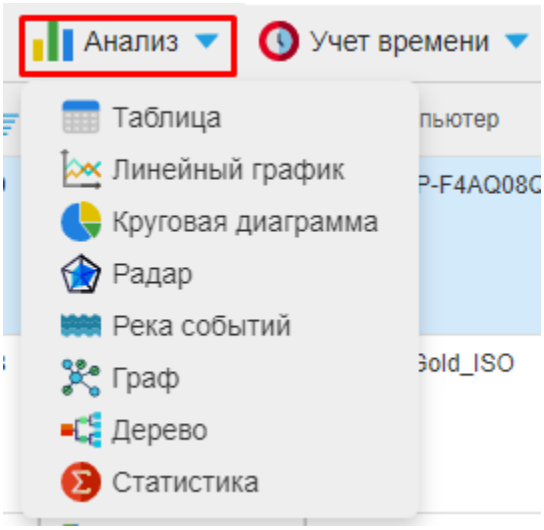
Примечание: При выборе режима отображения **Переписка** условие **Тип события** в фильтре изменится на **Почта** и **Интернет-пейджер**.

Анализ

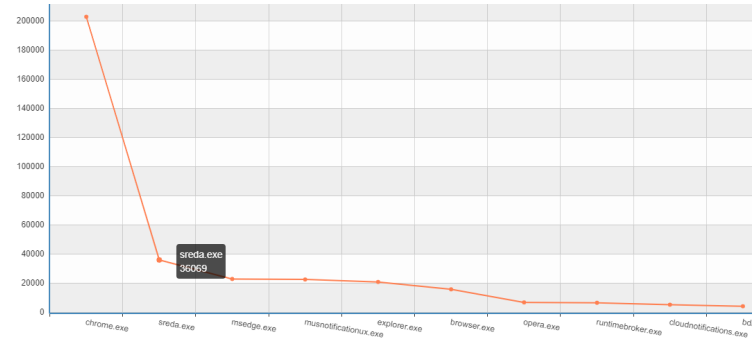
В меню **Анализ** представлены инструменты статистики и визуализации данных. Доступно несколько способов представления данных:

- Таблица,
- Линейный график,
- Круговая диаграмма,
- Радар,
- Река событий,
- Граф,
- Дерево,
- Статистика.

Предупреждение: Отображение данных зависит от выбора условий в **Конструкторе**. Если при анализе данные не отобразились, возможно, в выборке нет событий. Попробуйте изменить условия фильтрации в **Конструкторе**.

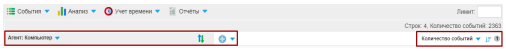


Все графики и диаграммы кликабельны. Например, нажмите на значение на **линейном графике**, чтобы перейти к событиям, на основе которых он построен.



Настройка отображения данных в Анализе

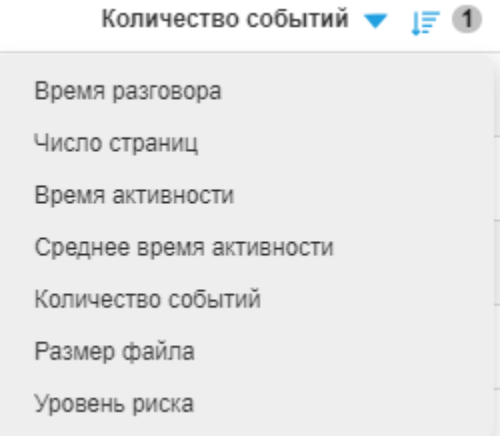
Настроить отображение данных можно с помощью параметров **Меры измерения** и **Группировка по измерениям**.



Мера измерения

Мера измерения — это количественный показатель, который позволяет более точно анализировать данные. С ее помощью можно сделать отчёты более детализированными. Например, строить графики не просто по количеству событий, а по их длительности или значимости.

Чтобы выбрать меру измерения, нажмите на **Количество событий** в правом углу линзы событий:



Пример. Чтобы узнать время активности событий:

1. Выберите в **Линзе событий** любой вид отображения в меню **Анализ**, например **Линейный график**.
2. В верхнем правом углу **Линзы** нажмите на **Количество событий**. Откроется список с доступными мерами измерения.
3. Выберите **Время активности**.

В результате **Линейный график** будет построен на основе времени активности, а не количества событий.

Доступные меры измерений:

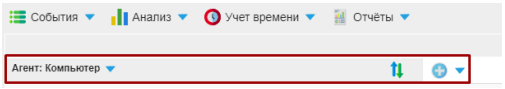
- **Всего** — количество значений измерения.
- **Время разговора** — общее время разговоров через SIP-телефонию. Вычисляется на основе событий **Интернет-пейджер** с форматом сообщения **Call**.
- **Число страниц** — общее число страниц. Вычисляется на основе событий **Печать документов** и **Перехваченный файл**.
- **Время активности** — общее время активности. Вычисляется на основе событий **Время активности**.
- **Среднее время активности** — общее значение среднего времени активности. Вычисляется на основе событий **Время активности**.
- **Количество событий** — общее количество событий.
- **Размер файла** — общий объем перехваченных файлов. Вычисляется на основе событий **Перехваченный файл** и **Файл**.
- **Уровень риска** — общий *Уровень риска*. Вычисляется на основе событий **Сработавшие политики**.

Нажмите на иконку справа от названия меры, чтобы изменить направление сортировки. Рядом с направлением сортировки цифрой указан **порядок сортировки** . Он определяет, какие данные сортируются в первую очередь. Например, сначала события сортируются по мере **Количество событий**, а потом уже по измерению **Агент** → **Компьютер**.

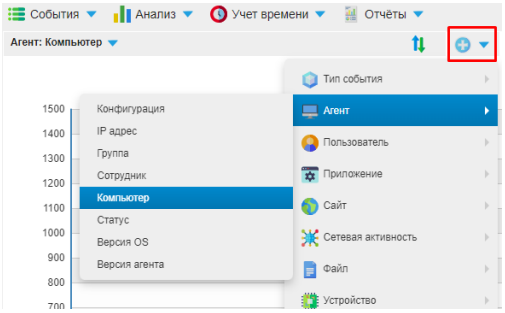
Группировка по измерению

Группировка по измерению — это выбор одного или нескольких измерений, на основе которых группируются события и строятся данные в режиме отображения **Анализ**.

По умолчанию группировка по измерению — **Агент: Компьютер**. Чтобы измерить группировку, нажмите на **Агент: Компьютер** в левом углу линзы событий и выберите нужное измерение.



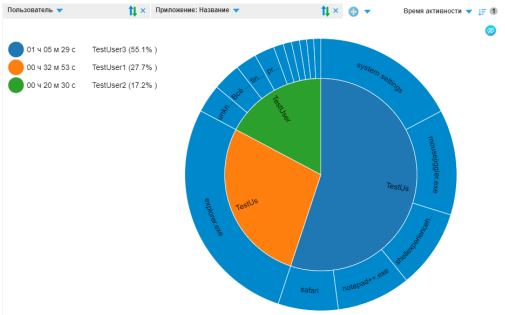
Можно добавлять группировку по нескольким измерениям. Чтобы добавить еще одну группировку по измерению, нажмите на + справа от названия измерения.



Пример. Чтобы увидеть количество событий в приложениях:

1. Выберите **Анализ** → **Круговая диаграмма** в **Линзе событий**.
2. В верхнем левом углу **Линзы** нажмите на **Агент: Компьютер**. Откроется список с доступными измерениями.
3. Выберите **Приложение** → **Название**.
4. Нажмите + справа от названия измерения. Откроется список с доступными измерениями.
5. Выберите **Пользователь** → **Пользователь**.

В результате **Круговая диаграмма** будет отображать количество событий в приложениях у каждого пользователя.



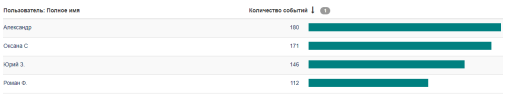
Нажмите на иконку справа от названия измерения, чтобы изменить направление сортировки.

Рядом с направлением сортировки цифрой указан **порядок сортировки** . Он определяет, какие данные сортируются в первую очередь. Например, сначала события сортируются по измерению **Агент** → **Компьютер**, а потом уже по измерению **Приложение** → **Название**.

Представление данных в Анализе

Таблица

Отображает данные по выбранным компьютерам и фильтрам в табличном виде. Таблица удобна для просмотра всей информации за определенное время.

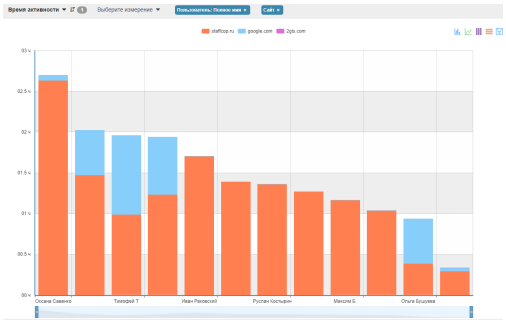


Линейный график

Отображает количество событий по измерениям в виде интерактивного графика.

Виды графиков:

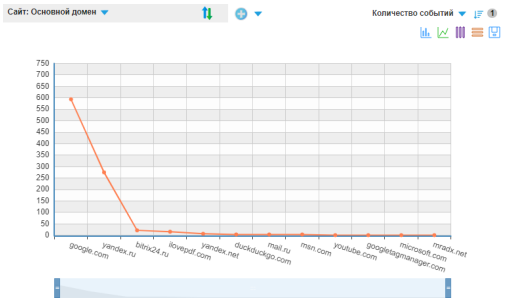
- Гистограмма,
- Линейный график,
- Без накопления,
- С накоплением.



Линейный график удобен для визуализации тенденций, изменений и сравнения событий во времени.

Пример. Чтобы сравнить активность пользователя на разных сайтах:

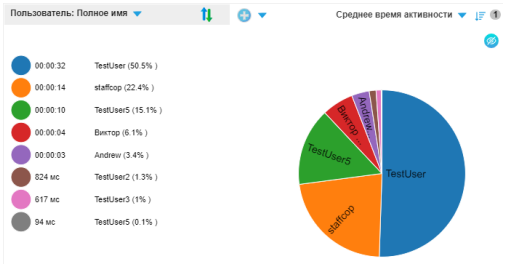
1. Выберите в **Конструкторе** пользователя, например, *TestUser*.
2. Перейдите в **Анализ** → **Линейный график**.
3. Укажите меру измерения **Количество событий**.
4. Укажите группировку по измерению **Сайт** → **Основной домен**.
5. Выберите наглядный вид графика, например, **Линейный график**.



Нажмите на иконку дискеты , чтобы сохранить график.

Круговая диаграмма

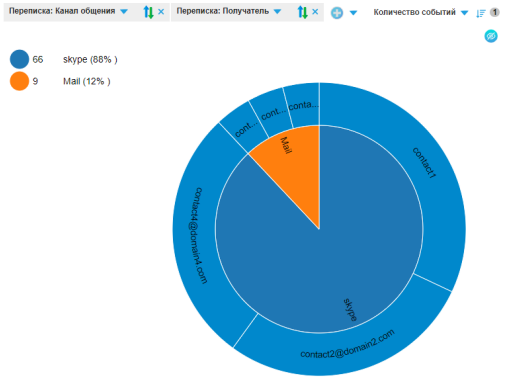
Отображает количество событий в виде круговой диаграммы. Круговая диаграмма подходит для визуализации долей или процентного соотношения категорий или значений.



Поддерживаются вложенные условия. Например, выберите в качестве первого условия приложение — *browser.exe*, а второго — **Сайты** → **Полный URL**.

Пример. Чтобы посмотреть долю переписки пользователя с разными адресатами:

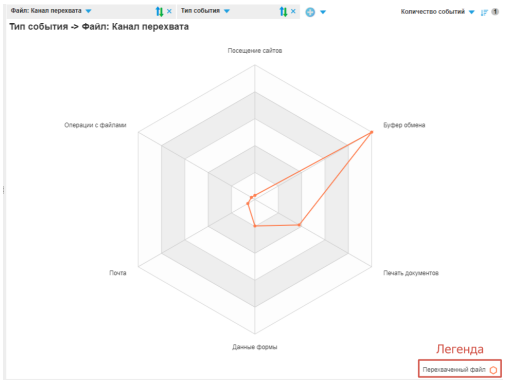
1. Выберите в **Конструкторе** пользователя, например, *TestUser*.
2. Перейдите в **Анализ** → **Круговая диаграмма**.
3. Укажите группировку по измерению **Канал общения** → **Основной домен**.
4. Нажмите + и добавьте группировку по измерению **Переписка** → **Получатель**.
5. Укажите в качестве меры **Количество событий**.



Радар

Отображает количество событий по измерениям в виде радара.

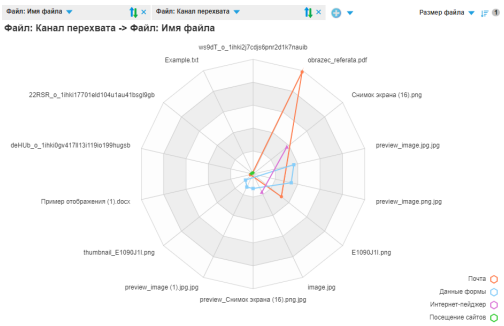
Примечание: **Радар** — диаграмма с двумя измерениями, на радиальных осях которой отображаются значения.



Поддерживаются вложенные фильтры.

Пример. Чтобы посмотреть перехваченные файлы большого размера:

1. Выберите в **Конструкторе** пользователя, например, *TestUser*.
2. Перейдите в **Анализ** → **Радар**.
3. Укажите группировку по измерению **Файл** → **Имя файла**.
4. Нажмите + и добавьте группировку по измерению **Файл** → **Канал перехвата**.
5. Укажите в качестве меры **Размер файла**.



Река событий

Визуализирует объём событий или других показателей по измерениям в выбранный период времени.

Диаграмма **Река событий** позволяет наглядно отслеживать последовательность событий, взаимосвязи и потоки действий во времени. Поддерживаются вложенные фильтры.

Пример. Чтобы проанализировать активность пользователей в приложениях в течение дня:

1. Выберите в **Конструкторе** пользователей, например, *TestUser1* и *TestUser2*.
2. Перейдите в **Анализ** → **Река событий**.

3. Укажите группировку по измерению **Пользователь** → **Пользователь**.
4. Нажмите + и добавьте группировку по измерению **Приложение** → **Название**.
5. В качестве меры измерения выберите **Время активности**.

Граф

Строит на основе событий граф в виде майндмапа.

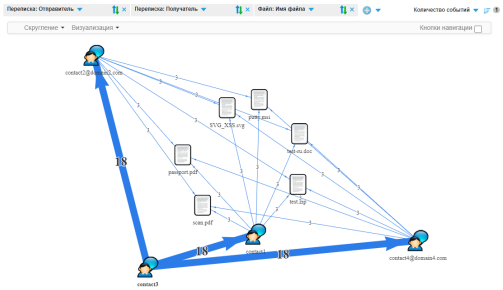
Для отображения графа доступны настройки **Скругление** и **Визуализация**.

Используйте граф для визуального представления связей между объектами.

Пример. Чтобы посмотреть переписку пользователя и отправленные файлы:

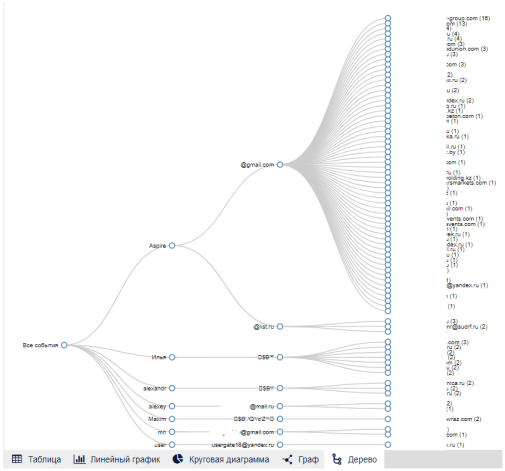
1. Выберите в **Конструкторе** пользователя, например, *TestUser*.
2. Перейдите в **Анализ** → **Граф**.
3. Укажите группировку по измерению **Переписка** → **Отправитель**.
4. Нажмите + и добавьте группировку по измерению **Переписка** → **Получатель**.
5. Нажмите + и добавьте группировку по измерению **Файл** → **Имя файла**.
6. Укажите в качестве меры **Количество событий**.

Граф покажет, кому пользователь отправлял сообщения:



Дерево

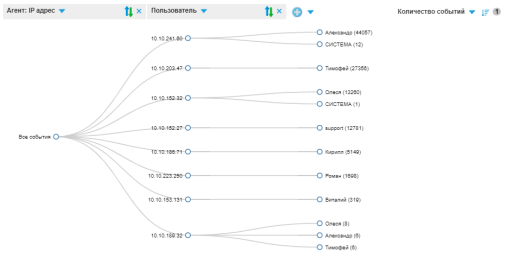
Строит дерево взаимосвязей на основе событий.



Дерево взаимосвязей удобно для представления иерархических структур данных, в которых каждый элемент имеет родителя.

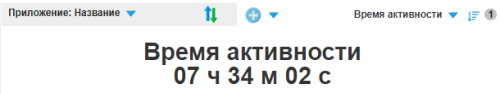
Пример. Чтобы узнать IP-адреса компьютеров, с которых подключались пользователи:

1. Перейдите в **Анализ** → **Дерево**.
2. Укажите в списке измерений **Агент** → **IP адрес**.
3. Нажмите + и добавьте измерение **Пользователь** → **Пользователь**.
4. Укажите в качестве меры **Количество событий**.



Статистика

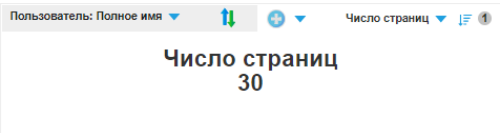
Суммирует события по *Мере измерения* с учетом условий фильтрации.



Используется для подсчета итоговых значений, например, количества событий, времени активности или числа страниц.

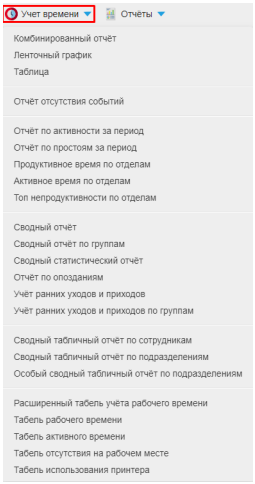
Пример. Чтобы увидеть, сколько листов распечатал пользователь:

1. Выберите в **Конструкторе** пользователя, например, *TestUser*.
2. Укажите **Тип события** → **Печать документов**.
3. Перейдите в **Анализ** → **Статистика**.
4. Укажите в качестве меры **Число страниц**.



Учет времени и Отчеты

Учет времени и **Отчеты** позволяют выводить проанализированную информацию по встроенным шаблонам. Используются для быстрого получения сводных данных об активности пользователей.



См.также:

Описание встроенных отчетов

4.3.3 Политики

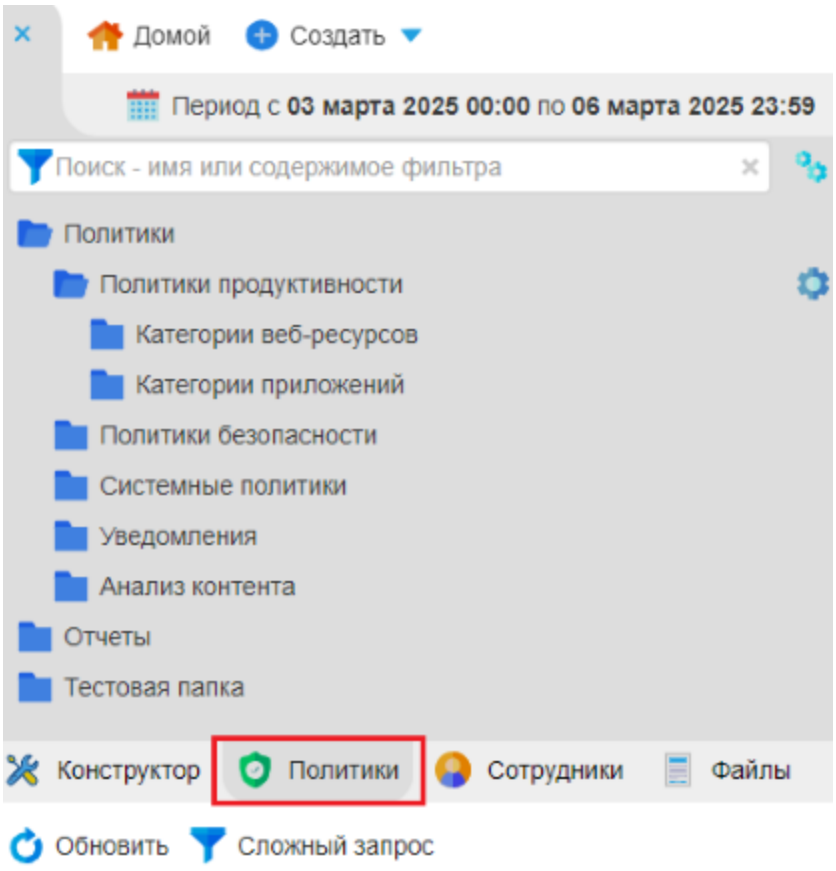
Содержание

- *Политики*
  - *Как работают политики*
  - *Как создать новую политику*
  - *Встроенные политики*

Политика — инструмент, который анализирует входящие события на продуктивность и потенциальные риски. Позволяет строить отчеты о рабочем времени и настраивать ответные действия: отправку уведомлений, смену конфигурации, блокировки.

В системе предусмотрены встроенные политики, но вы можете создать свои.

Все политики находятся во вкладке **Политики**.


Домой
Создать
Период с 03 марта 2025 00:00 по 06 марта 2025 23:59
Поиск - имя или содержимое фильтра
Политики
Политики продуктивности
Категории веб-ресурсов
Категории приложений
Политики безопасности
Системные политики
Уведомления
Анализ контента
Отчеты
Тестовая папка
Конструктор
Политики
Сотрудники
Файлы
Обновить
Сложный запрос

Как работают политики

События поступают на сервер, где их обрабатывают политики. Политика срабатывает, если событие соответствует ее условиям, и назначает ему *Категорию*.

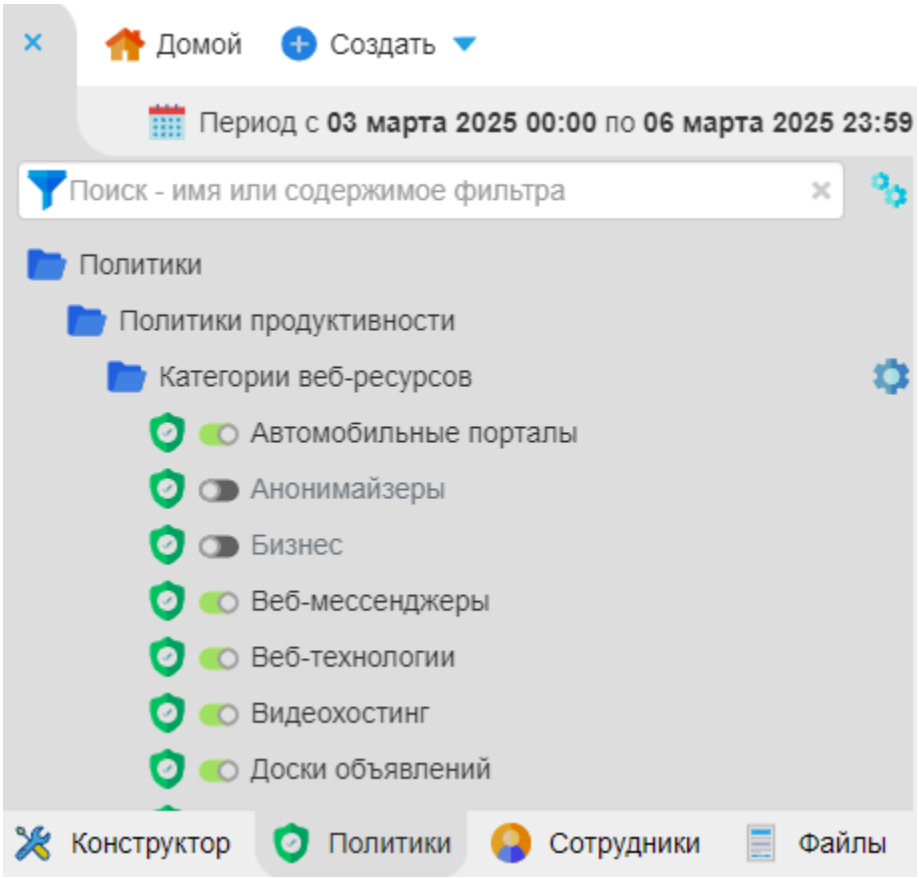
Пример. Пользователь *TestUser* зашел на сайт социальной сети. Политика **Социальные сети** присвоит этому событию категорию **Непродуктивно**. *В отчете учета рабочего времени* это время окрашено красным цветом и прибавлено к общему непродуктивному времени сотрудника.

Управление политиками

Активация

Политика работает только в активном состоянии.

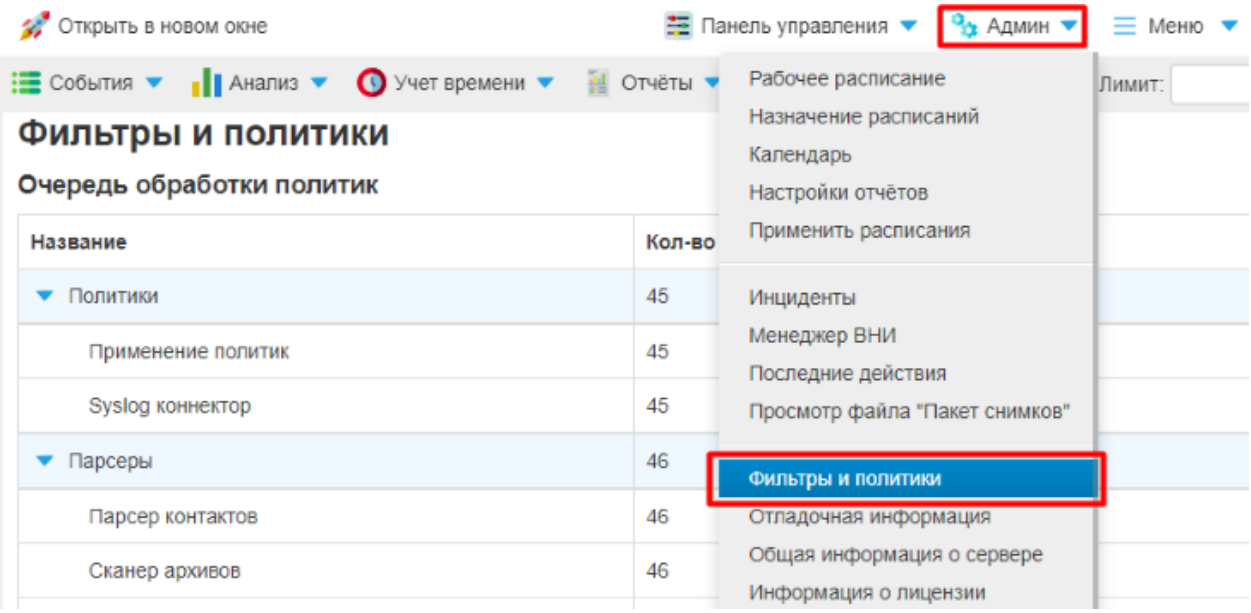
Чтобы включить политику, нажмите на нее и в окне настроек поставьте флаг **Политика активна** .



Периодичность

Активные политики обрабатывают входящие события с частотой, которая указана в значении *Параметры сервера → Период запуска политик (сек)*.

При большой нагрузке формируется очередь событий, которую можно отслеживать в разделе **Админ → Фильтры и политики**:



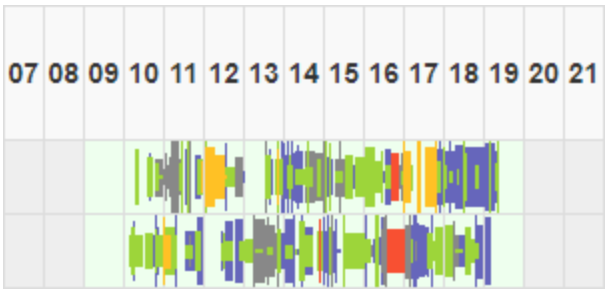
Категории событий

При срабатывании политик продуктивности и безопасности каждому событию присваивается одна из категорий:

- **Премиально** — важные задачи;
- **Продуктивно** — продуктивная деятельность;
- **Нейтрально** — нейтральная деятельность;
- **Непродуктивно** — непродуктивная деятельность;
- **Инциденты** — события, которые нарушают политику безопасности организации.

Примечание: В отчетах также отображается дополнительная категория **Все остальное**. В нее входят события, которые не соответствуют ни одной из категорий.

Категория указана *в настройках политики* .



Например, если сотрудник зашёл на сайт по поиску работы — сработает политика **Сайты по трудоустройству**, а время будет засчитано как непродуктивное. В отчетах учета рабочего времени время будет выделено красным цветом. Работа с корпоративными документами считается продуктивной активностью, выделяется зеленым.

Действие будет считаться опасным, если в окне настройках политики указана категория **Инцидент**. Например, обход мониторинга может расцениваться, как несанкционированное действие.

Примечание: Категория **Инцидент** не создает инцидент *в Консоли управления*. Она только отмечает событие в отчетах как потенциально опасное. Инциденты же позволяют расследовать небезопасное событие и *настраивать ответное поведение*.

Чтобы при срабатывании любой политики создавался инцидент, во вкладке **Уведомления** поставьте галочку **Создать инцидент**. Это позволит системе формировать инциденты независимо от назначенной категории.

На основе событий **Время активности** и их категории формируется отчет о рабочем дне пользователя и его продуктивности.

Начало		Окончание		Общее время		Дисциплина		Активность		Продуктивность		
факт	распис	факт	распис	факт	план	сверх	опозд	актив	неактив	прод	непрод	нейтр
8:21:53	9:00:00	17:41:21	18:00:00	9:20:28	8:00:00	10:59:28	0:00:00	7:42:50	1:38:38	2:19:25	0:00:00	0:08:28
10:08:14	9:00:00	19:10:40	20:00:00	9:02:26	8:00:00	1:02:26	1:08:14	6:40:18	2:22:08	2:43:01	0:01:38	0:13:59

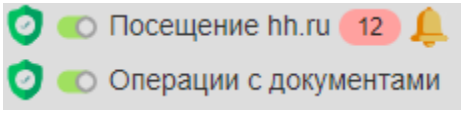
См.также:

Подробнее об учете рабочего времени

Сработавшие политики

Результат работы политик можно увидеть в **Конструктор** → **Сработавшие политики**.

Рядом с названием политики во вкладке **Политики** отображается количество связанных событий:



В зависимости от настроек политика может *отправлять уведомления* и *менять конфигурацию компьютера*.

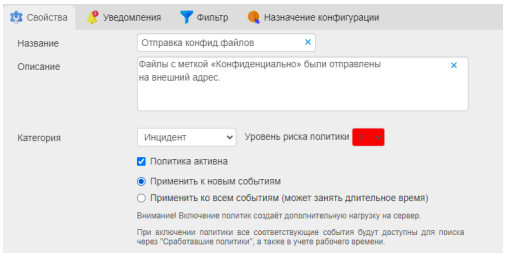
Как создать новую политику

Пример. Вы хотите, чтобы при отправке файлов с меткой *Конфиденциально* на внешние адреса политика отправляла уведомление администратору и *меняла конфигурацию компьютера* на **Полный контроль**.

См.также:

Подробнее о метках и блокировке доступа

1. Нажмите на + **Создать** → **Политика**. Откроется окно создания политики.



2. Укажите **Название** политики, например, *Отправка конфид. файлов*. При необходимости задайте **Описание** политики.
3. Выберите категорию **Инцидент** и укажите *Уровень риска*, если он доступен.
4. Включите флаг **Политика активна** и выберите вариант применения политики:
   - **Применить к новым событиям** — политика будет обрабатывать только те события, которые поступили после её активации. К старым событиям политика не будет применена.
   - **Применить ко всем событиям (может занять длительное время)** — политика применится ко всем событиям.

   > **Предупреждение:** **Применить ко всем событиям** запускает *Перестройку отчетов* за весь период работы системы. При работе с большой базой данных выполняйте процедуру в нерабочее время или используйте команду, которая перестраивает отчеты за указанное количество месяцев — `ibatyr rebuild_sessions N`, где N — количество месяцев.

5. Перейдите во вкладку **Уведомления** и поставьте флаг **Активировать уведомления**.

   См.также:

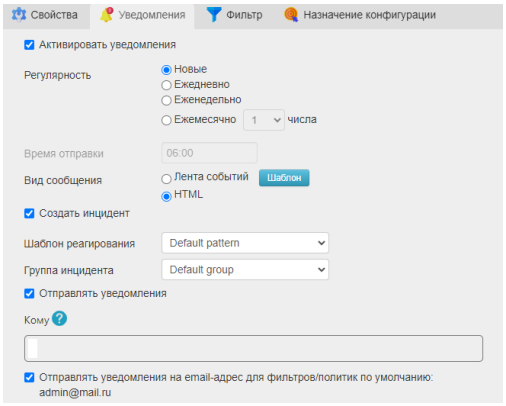
   Как настроить отправку уведомлений

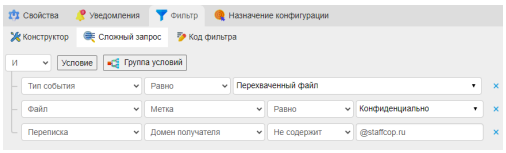
6. Поставьте флаг **Отправлять уведомления** и укажите адрес электронной почты в поле **Кому**.

   > **Предупреждение:** Для отправки почтовых уведомлений *заполните Почтовые настройки*.

7. Перейдите во вкладку **Фильтр** и переключитесь на **Сложный запрос**.

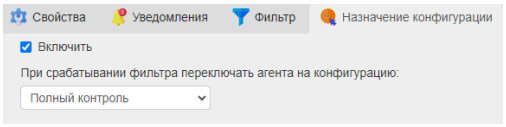
8. Нажмите + **Условие** и добавьте условия:





- **Тип события** — **Равно** — **Перехваченный файл**,
- **Файл** — **Метка** — **Равно** — *Конфиденциально*,
- **Переписка** — **Домен получателя** — **Не содержит** — *@ibatyr.kz*.

9. Перейдите во вкладку **Назначение конфигурации** и поставьте флаг **Включить**.



10. Выберите в поле **При срабатывании фильтра переключать агента на конфигурацию** значение **Полный контроль**.
11. Нажмите **Сохранить**.

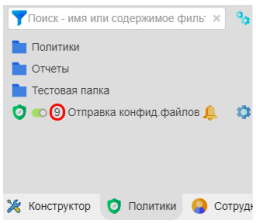
Отправка конфид. файлов появится во вкладке **Политики** и начнет обработку входящих событий. При срабатывании политики администратор получит уведомление на почту Компьютеру будет присвоена конфигурация **Полный контроль**, которая отслеживает все действия пользователя.

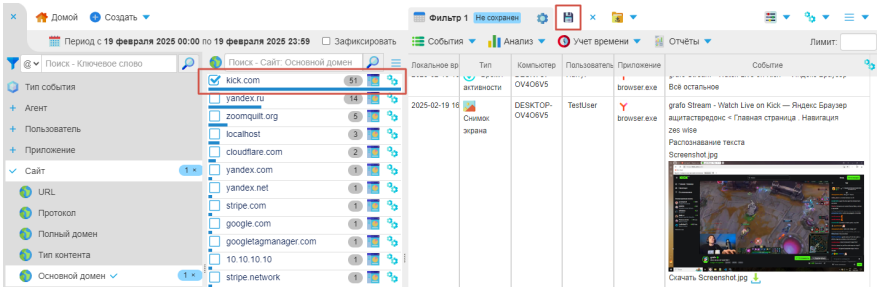
Создать политику через Конструктор

Конструктор позволяет создать политику на основе уже обнаруженного события. Это особенно удобно, когда вы видите непродуктивную активность и хотите учесть ее в отчете.

Пример. Представим ситуацию: вы заметили, что сотрудники слишком много времени проводят на стриминговой платформе, например, на *kick.com*. Давайте создадим политику, которая будет отмечать такие посещения как непродуктивные.

1. На главной странице в **Конструкторе** добавьте условие **Сайт** — **Основной домен** — *kick.com*. Отобразится выборка событий с сайта kick.com и появится кнопка **Сохранить** над **Линзой событий**.





2. Нажмите на кнопку **Сохранить** над **Линзой событий**. Откроется окно создания **Фильтра**.
3. В нижнем правом углу окна нажмите на кнопку **Сохранить как** → **Политику**. Откроется окно настроек **Политики**.
4. Укажите **Название** и выберите **Категория** → **Непродуктивно**.
5. Включите флаг **Политика активна** и выберите пункт **Применить ко всем событиям (может занять длительное время)**, чтобы учитывать и новые, и старые события как непродуктивные.
6. Вкладка **Фильтр** уже содержит все условия из **Конструктора**, но вы можете внесите дополнительные условия при необходимости.
7. Нажмите кнопку **Сохранить**.

Свойства политики

Откройте окно настроек политики, чтобы посмотреть как она работает или создать на ее основе новую. Чтобы не сломать работающий инструмент, рекомендуем не изменять предустановленные политики, а создавать на их основе новую политику с помощью кнопки **Сохранить как**.

1. Перейдите во вкладку **Политики**.
2. Нажмите на название политики. Рядом с названием политики появится иконка шестеренки .
3. Нажмите на иконку шестеренки . После этого откроется окно настроек политики.

Чтобы посмотреть условия фильтрации, перейдите во вкладку **Фильтр** → **Сложный запрос**. Например, у политики **Развлекательные сайты** в запросе перечислены нежелательные для посещения сайты.

См.также:

Подробнее об окне настроек

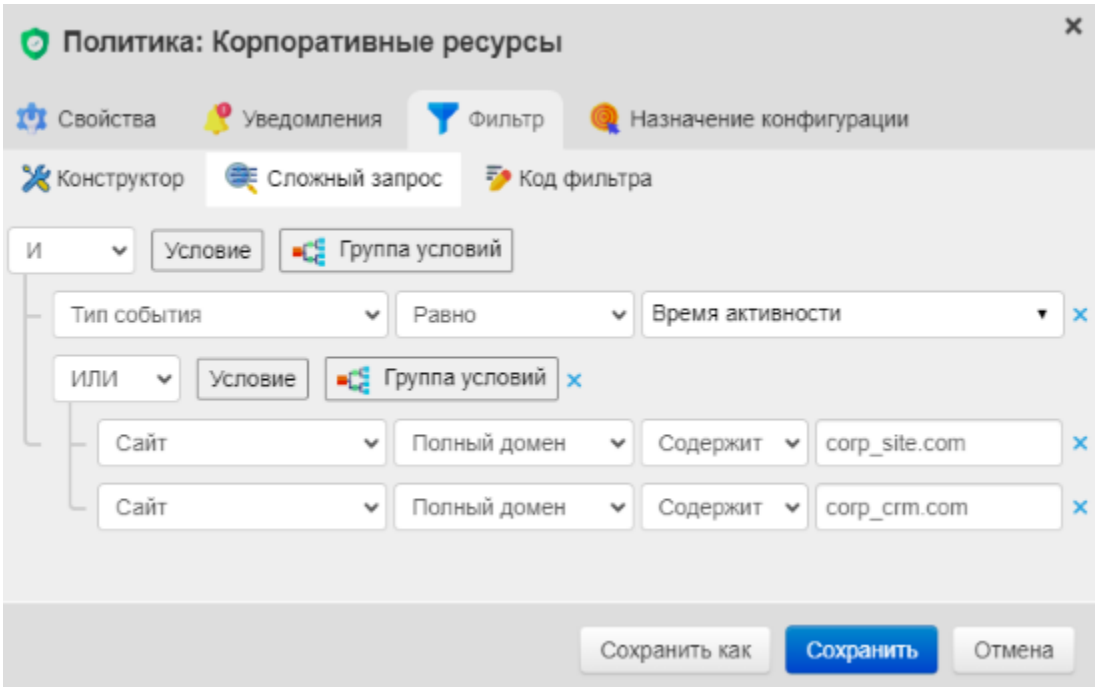
Встроенные политики

Встроенные политики — это набор готовых правил, которые отслеживают продуктивность сотрудников и обеспечивают безопасность компании.

Вы можете добавлять в папки встроенных политики новые политики и перемещать встроенные политики в другие папки.

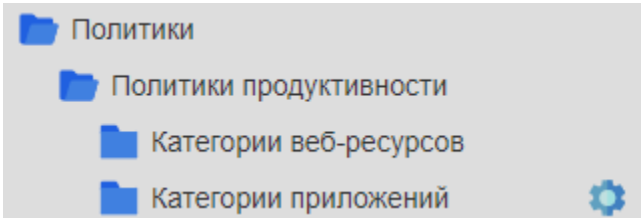
Политики делятся на несколько групп, которые описаны ниже. Список всех встроенных политик приведен в статье *Системные фильтры*.

Внесите в условия фильтрации встроенных политик сайты и приложения, которые нужно отслеживать в вашей компании. Например, в **Политики продуктивности** → **Категории веб-ресурсов** → **Корпоративные ресурсы** укажите ваши корпоративные ресурсы вместо значений *corp_ site.com* и *corp_ crm.com*:



Политики продуктивности

В разделе **Политики продуктивности** собраны политики, которые определяют продуктивность событий.



К ним относятся:

- **Категории веб-ресурсов** — отслеживают сайты: форумы, развлекательные сайты и так далее.

Например, политика **Видеохостинг** засчитывает время на *youtube.com* и *rutube.ru* как непродуктивное.

- **Категории сайтов** — отслеживают работу в приложениях.

Учет рабочего времени

На основе событий **Время активности** и их категории формируется *отчет о рабочем дне пользователя и его продуктивности*.

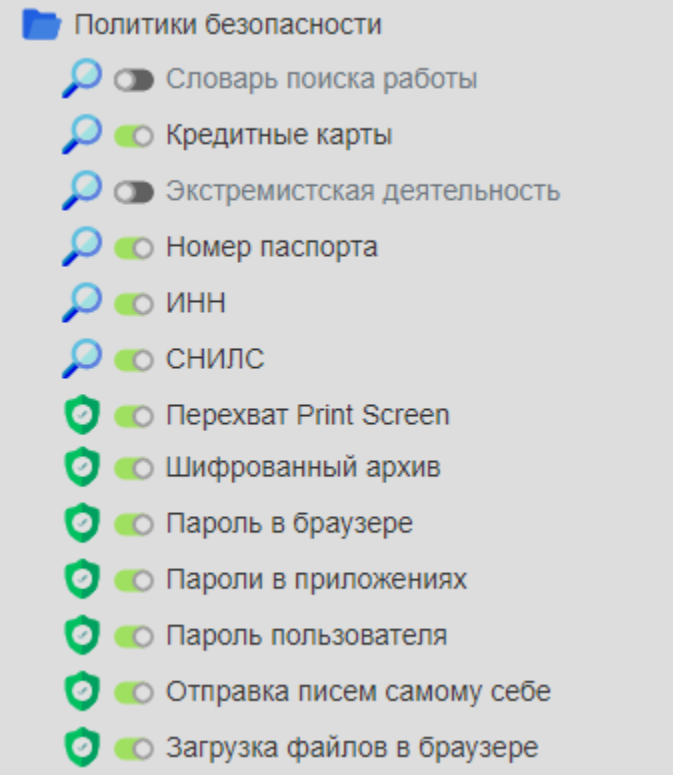
Начало		Окончание		Общее время		Дисциплина		Активность		Продуктивность		
факт	распис	факт	распис	факт	план	сверх	опозд	актив	неактив	прод	непрод	нейтр
8:21:53	9:00:00	17:41:21	18:00:00	9:20:28	8:00:00	10:59:28	0:00:00	7:42:50	1:38:38	2:19:25	0:00:00	0:08:28
10:08:14	9:00:00	19:10:40	20:00:00	9:02:26	8:00:00	1:02:26	1:08:14	6:40:18	2:22:08	2:43:01	0:01:38	0:13:59

См.также:

Подробнее об учете рабочего времени

Политики безопасности

Политики безопасности определяют безопасность событий.

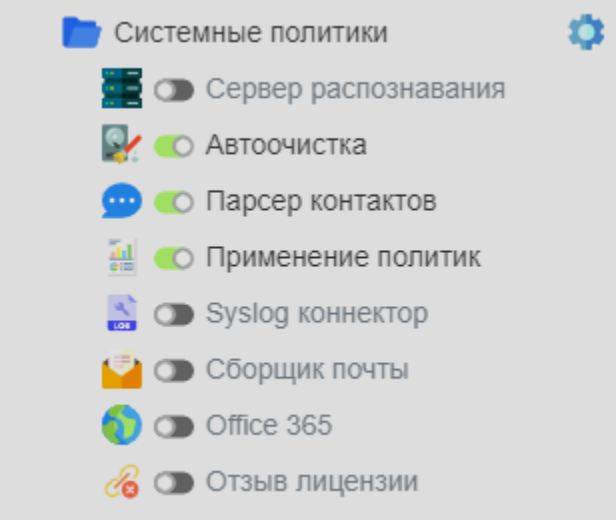


Например, политика безопасности **Кредитные карты** ищет в событиях номера кредитных карт с помощью *регулярного выражения*.

К политикам безопасности относятся политики по поиску слов в событиях — *Поиск по словарю*.

Системные политики

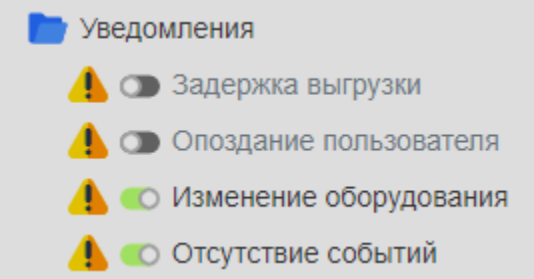
Системные политики — запускают служебные обработчики информации.



Например, *Автоочистка* отслеживает свободное место на диске сервера iBatyr Monitor. Если диск заполняется больше установленного процента, она автоматически удаляет или перемещает старые файлы.

Уведомления

В этом разделе находятся служебные обработчики, которые отправляют уведомление при различных сценариях.



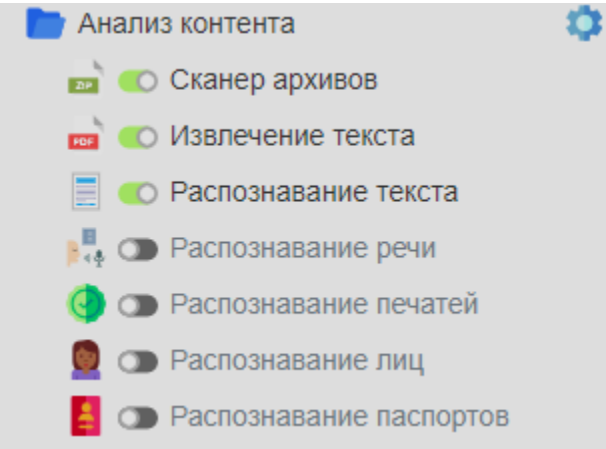
Например, **Отсутствие событий** следит за активностью компьютеров. Если какой-то компьютер перестает отправлять данные в течение заданного времени, система отправляет уведомление **Долгая неактивность агента**.

См.также:

Подробнее об уведомлениях

Анализ контента

К анализу контента относятся обработчики, которые отвечают за распознавание контента и анализ содержимого архивов.



Например, **Распознавание текста** распознает текст на изображениях с помощью *Сервера распознавания графических объектов*.

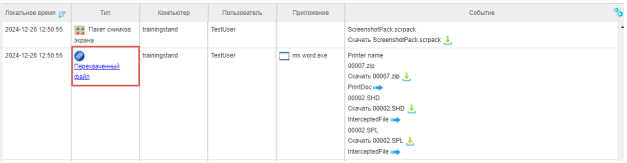
4.3.4 Навигация

Для навигации в веб-интерфейсе используйте описанные ниже инструментами.

Таблица событий

Чтобы добавить фильтр, кликните на значение в **Таблице событий**.

Например, чтобы отфильтровать события по типу **Перехваченный файл**, нажмите на **Перехваченный файл** в колонке **Тип**.

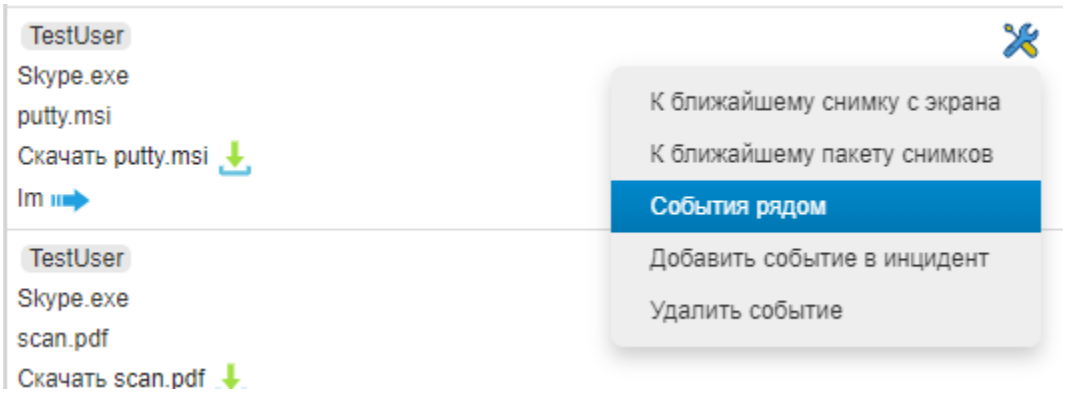


После этого в категорию **Тип события** будет добавлено новое измерение **Перехваченный файл**, а таблица отобразит все события **Перехваченный файл**. Таким образом вы можете добавить время, пользователя, компьютер и другие измерения.

Кроме того, вы можете использовать для фильтрации отдельные параметры события. Например, выберите источник перехвата **Clipboard** (буфер обмена), чтобы отобразить только связанные с ним события.

Меню взаимодействия с событием

Чтобы открыть **Меню взаимодействия с событием**, наведите курсор на событие и нажмите на иконку инструментов .



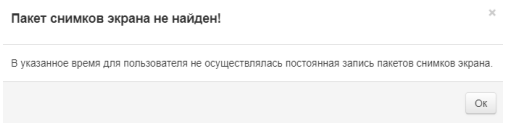
К ближайшему снимку экрана — нажмите, чтобы перейти к ближайшему *снимку экрана*.

> **Предупреждение:** Убедитесь, что в конфигурации включено *создание снимков экрана*.

К ближайшему пакету снимков — нажмите, чтобы перейти к ближайшему по времени снимку *из пакета снимков экрана*.

> **Предупреждение:** Убедитесь, что в конфигурации включено *создание снимков экрана*.

Если для указанного в датапикере временного промежутка нет пакета снимков экрана, система об этом уведомит.

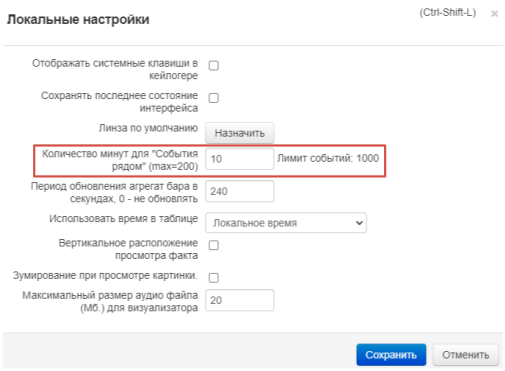


См.также:

Подробнее об анализе снимков экрана

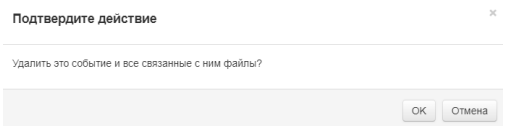
События рядом — нажмите, чтобы отобразить соседние события.

Изменить временной промежуток для поиска соседних событий можно в параметре **Количество минут для «События рядом»** *в Локальных настройках Меню*.



Добавить событие в инцидент — нажмите, чтобы добавить событие *в Инцидент*.

Удалить событие — удаляет событие из базы данных.

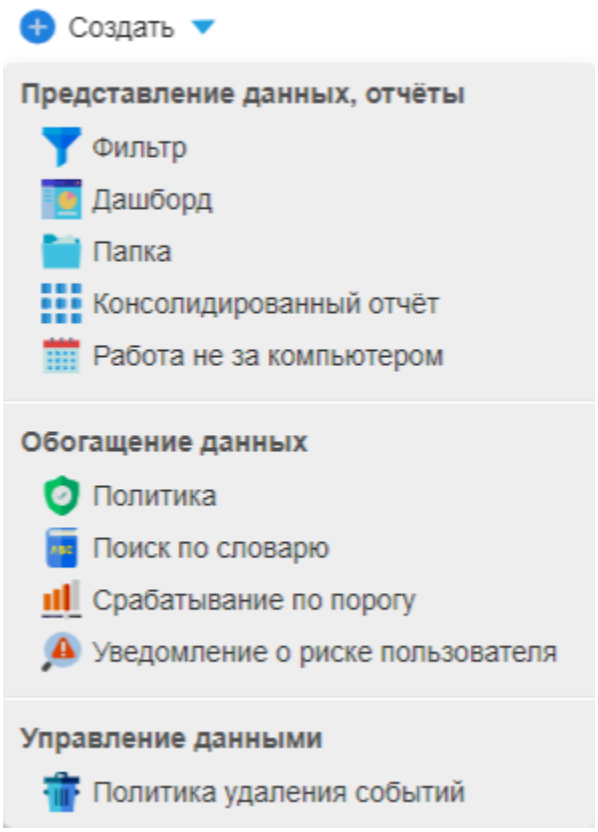


Осторожно: **Удалить событие** необратимо удаляет данные о событии из системы.

4.3.5 Инструменты фильтрации данных

Инструменты фильтрации данных — это набор механизмов для управления данными. Они позволяют отбирать, анализировать и визуализировать события по заданным измерениям, автоматизировать отчеты и ответные реакции.

В системе доступны встроенные инструменты фильтрации, но можно создать собственные для решения конкретных задач.

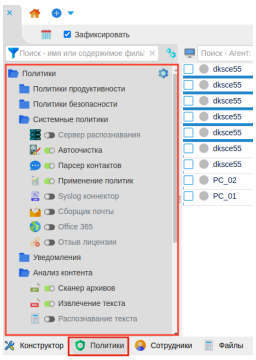


К инструментам фильтрации данных относятся **Фильтры**, **Политики**, **Поиск по словарю** и другие:

tabularytabulary

Представление данных	
Обогащение данных	дополнение данных, оценка уровня
Управление данн	

Все предустановленные и пользовательские инструменты фильтрации находятся на вкладке **Политики**.



Подробнее об инструментах фильтрации:

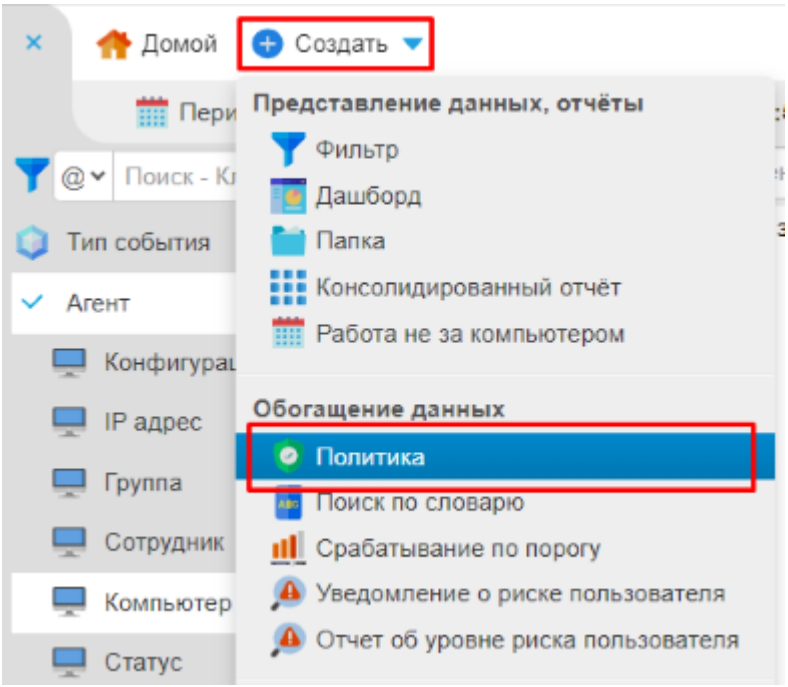
Как создать инструмент фильтрации

Инструмент фильтрации можно создать двумя способами: с помощью меню + **Создать** или через *Конструктор*.

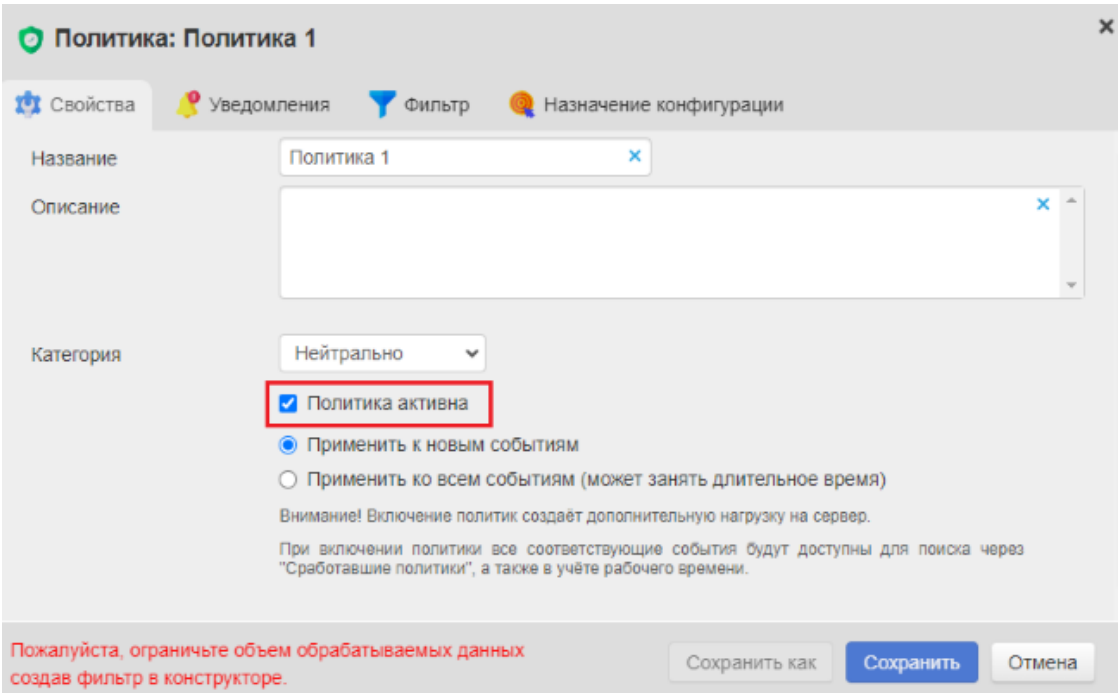
Пример: создать политику, которая срабатывает при установке приложений у пользователей из отдела прямых продаж.

Меню Сохранить

1. Нажмите кнопку + **Создать** и выберите опцию **Политика**.



Откроется модальное окно:

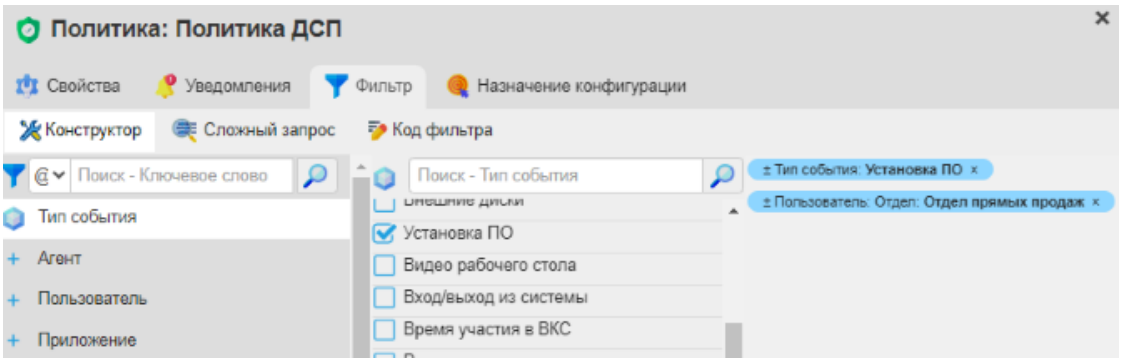


2. Во вкладке **Свойства** введите **Название** — например, для служебного пользования: *Политика ДСП* — и поставьте флаг **Политика активна**.

Примечание: Некоторые инструменты требуют активации с помощью флажка **Политика активна**, без нее они не смогут выполнять свои функции.

---

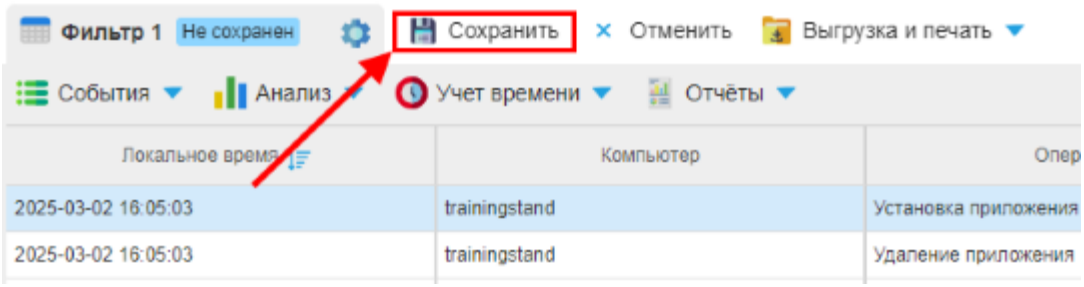
3. Во вкладке **Уведомления** при необходимости *настройте отправку уведомлений на почту*.
4. Во вкладке **Фильтр** добавьте условия **Пользователь** — **Отдел** — *Отдел прямых продаж* и **Тип события** — **Установка ПО**.



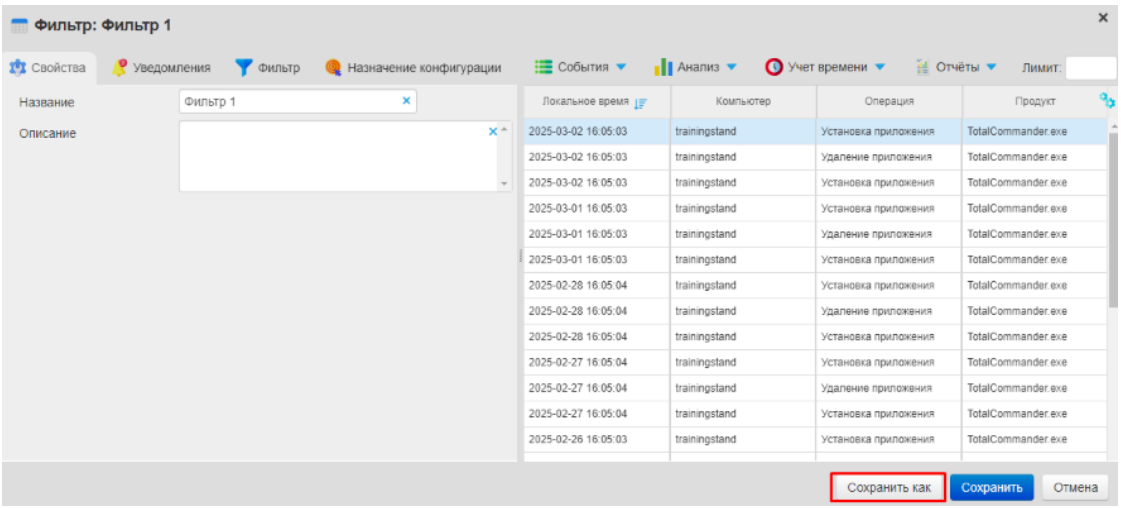
5. Нажмите кнопку **Сохранить**.

Конструктор

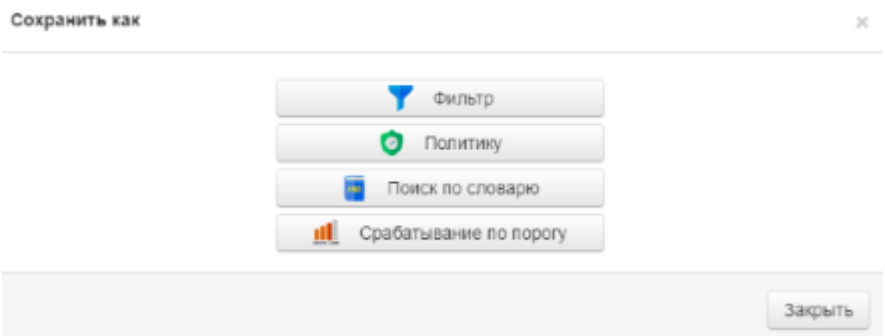
1. Укажите условия фильтрации в **Конструкторе** — например, **Пользователь** — **Отдел** — *Отдел прямых продаж* и **Тип события** — **Установка ПО**.
2. Нажмите **Сохранить** над **Линзой**.



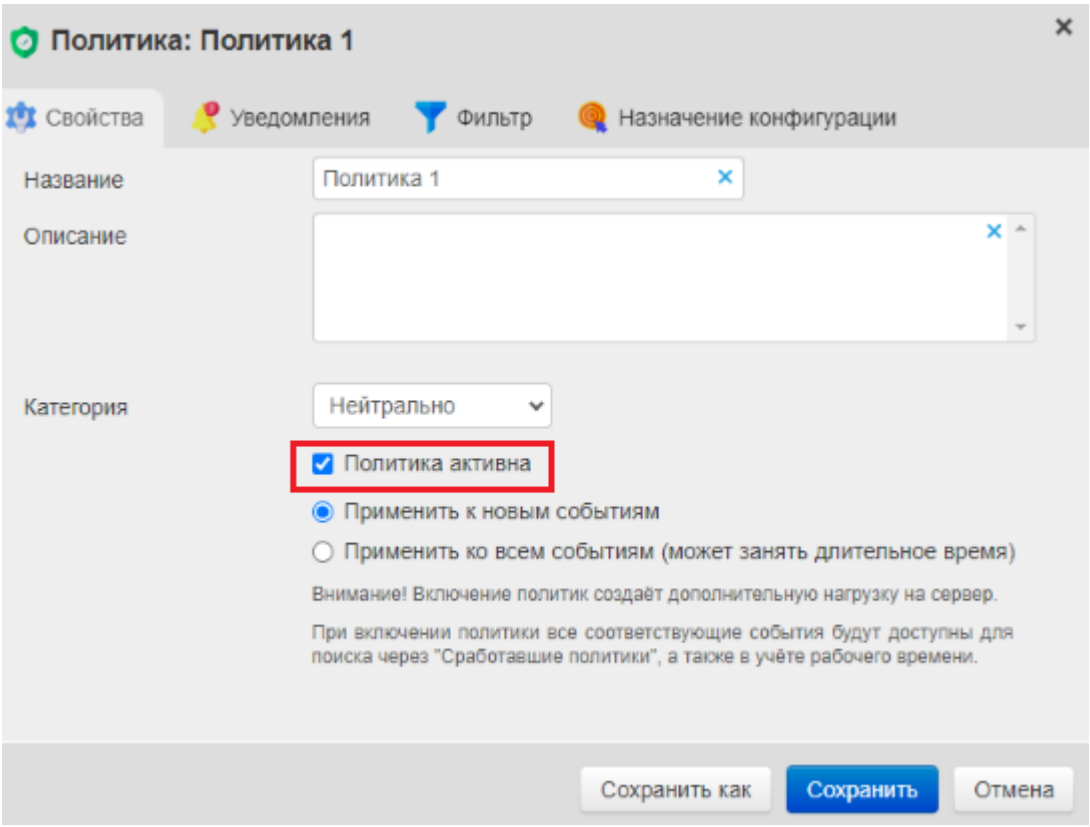
Откроется окно создания фильтра:



3. Нажмите **Сохранить как** и выберите **Политика**.



Откроется окно создания политики. Во вкладке **Фильтр** будут условия, которые вы установили в п.1.



4. Поставьте флаг **Политика активна**.

Примечание: Некоторые инструменты требуют активации с помощью флажка **Политика активна**, без нее они не смогут выполнять свои функции.

---

5. Во вкладке **Уведомления** *настройте отправку уведомлений на почту*.
6. Нажмите кнопку **Сохранить**.

Сохранить как

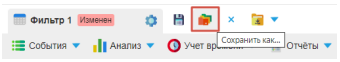
Сохранить как позволяет создать инструмент на основе текущего.

Возможны несколько вариантов использования.

Изменение инструмента. Используйте **Сохранить как**, если хотите изменить встроенный инструмент, чтобы случайно его не сломать.

Допустим, вы хотите изменить фильтр *ДСП*. Создайте копию, чтобы не нарушить его работоспособность:

1. Найдите фильтр во вкладке **Политики**.
2. Откройте фильтр и внесите изменения в **Конструкторе**. Например, добавьте условие **Пользователь** — *TestUser*.
3. Нажмите иконку папок над **Линзой событий**.



4. В открывшемся окне измените **Название**, например, *Фильтр ДСП копия*.
5. Нажмите **Сохранить как**.

В результате во вкладке **Политики** доступны два инструмента: исходный *Фильтр ДСП* и новый *Фильтр ДСП копия*.

Преобразование инструмента. Фильтры можно сохранять, как политики, и наоборот.

Например, вы нашли подозрительный сайт и создали фильтр для его отслеживания. Если потом выяснится, что сайт действительно опасный, можно не настраивать политику с нуля, а просто создать ее на основе готового фильтра. Для этого откройте **Фильтр**, внесите дополнительные настройки (например, смену конфигурации) и нажмите **Сохранить как** → **Политику**. Этот метод экономит время и сохраняет все настройки.

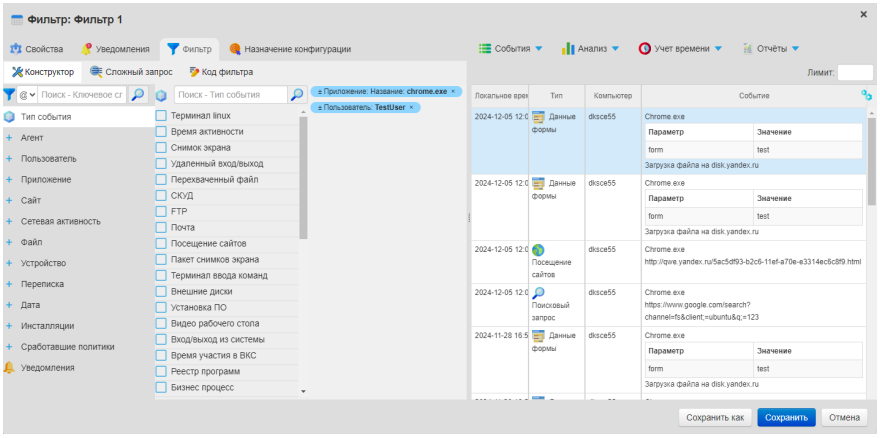
Представление данных, отчеты

Представление данных и отчеты — это инструменты для анализа и визуализации событий.

Фильтр

Фильтр — позволяет отображать события, которые соответствуют заданным условиям: типу события, имени пользователя, дате и другим.

При создании фильтра условия задаются в окне настроек с помощью **Конструктора** или **Сложного запроса**:



См.также:

Подробнее о Конструкторе и сложных запросах

Дополнительные вкладки:

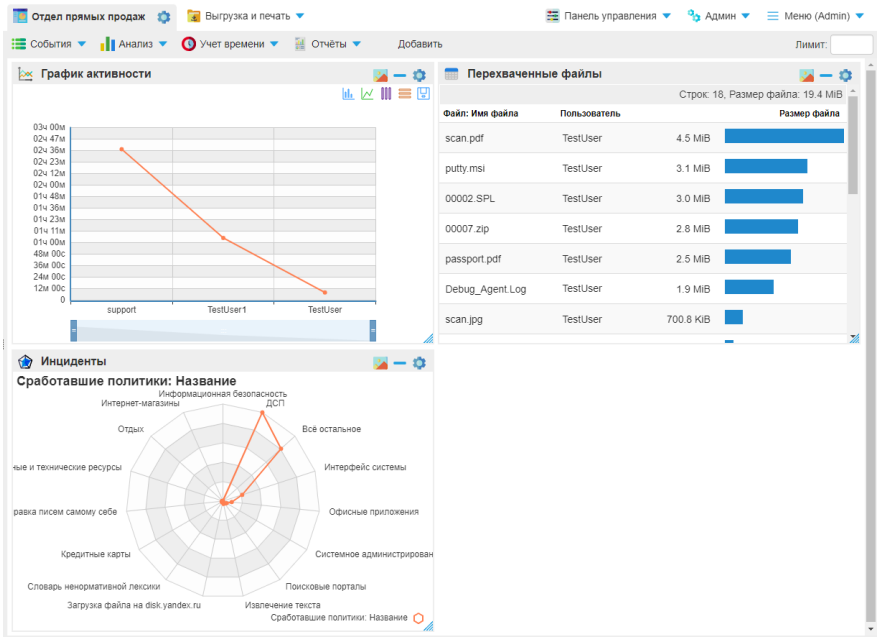
- *Уведомления*— настройка уведомлений, которые будут приходить на почту при срабатывания фильтра.
- *Назначение конфигурации* — настройка смены конфигурации компьютера. При обнаружении указанных в настройках событий система автоматически сменит конфигурацию.

См.также:

Больше о конфигурации компьютера

Дашборд

Дашборд — набор фильтров и отчетов, которые отображаются в одном окне.



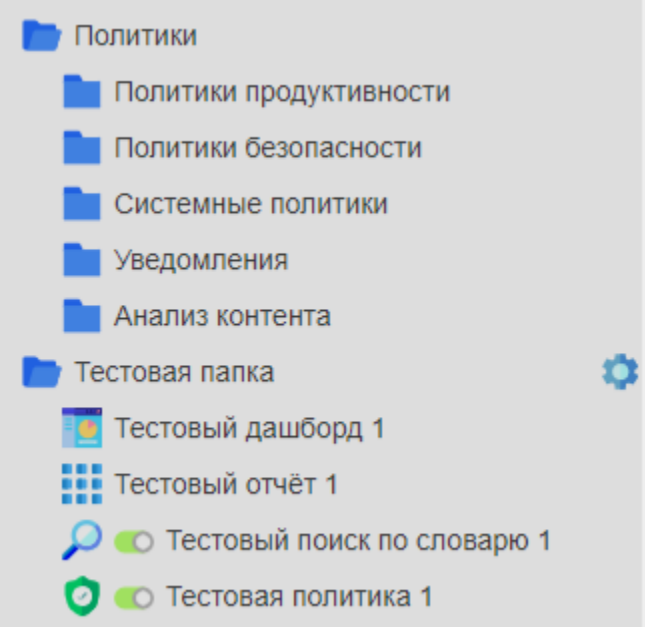
См.также:

Подробнее о работе с дашбордами

Помимо обычных дашбордов доступны дашборды по каждому измерению — *Карточки измерений*.

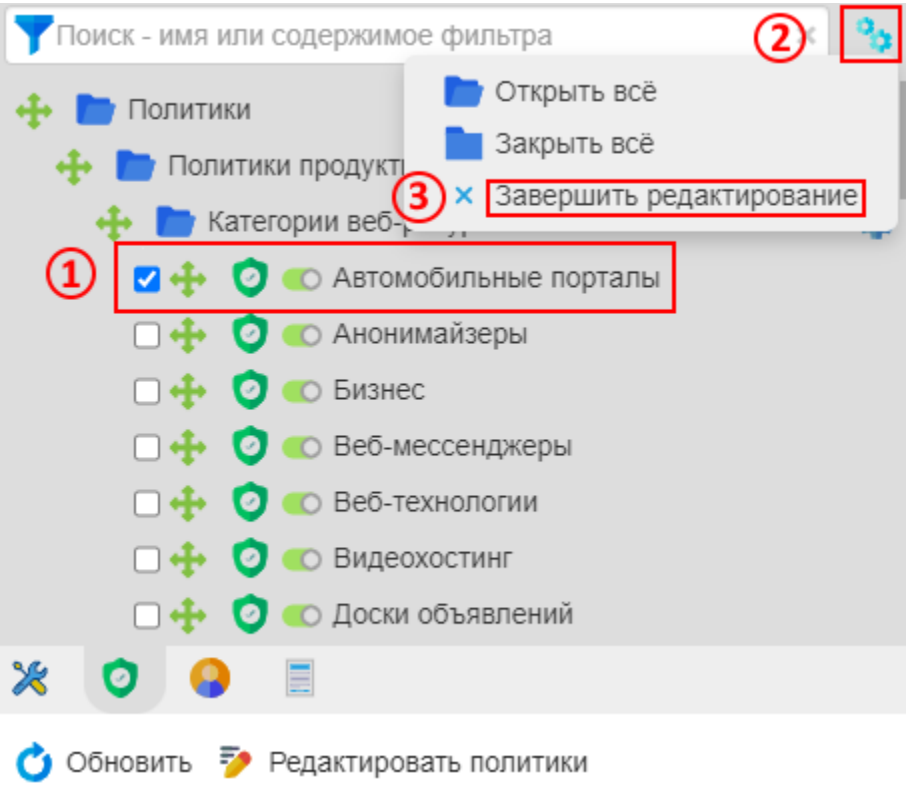
Папка

Создайте с помощью этого инструмента папку для систематизированного хранения инструментов фильтрации данных.



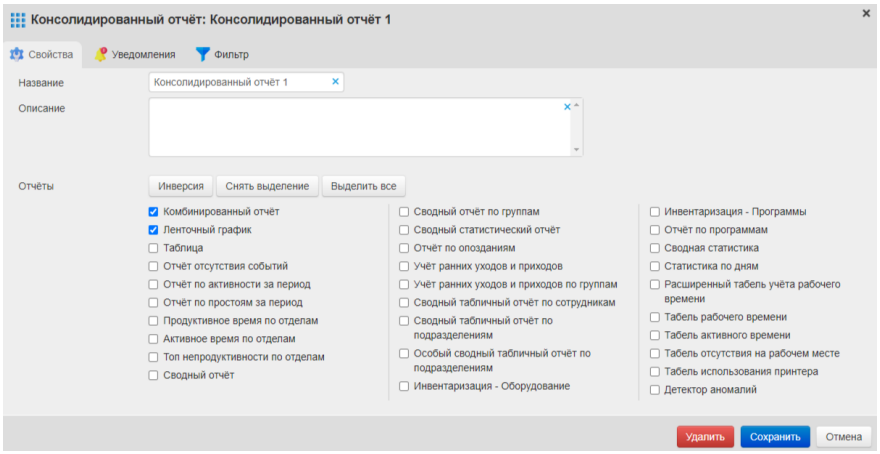
Чтобы переместить инструмент в папку:

1. Перейдите во вкладку **Политики**.
2. Нажмите иконку шестеренок рядом со строкой поиска и выберите **Редактировать**.
3. Зажмите и переместите инструмент.
4. По завершению нажмите иконку шестеренок и выберите **Завершить редактирование**.



Консолидированный отчет

Консолидированный отчет — набор отчетов о событиях за определённый период. Вы можете выбрать из списка все или отдельные отчеты для регулярной отправки на почту.



См.также:

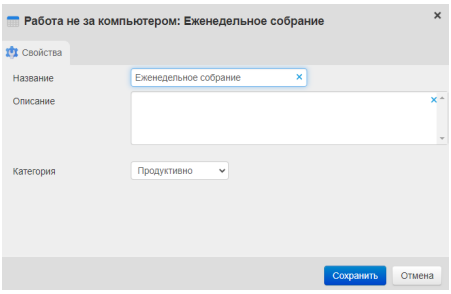
Подробнее о консолидированном отчете

Работа не за компьютером

Работа не за компьютером — это функция для учета работы не за компьютером. Например, у сотрудника *TestUser* есть регулярное очное собрание, которое должно учитываться как продуктивная деятельность.

Для этого сначала создайте новый инструмент:

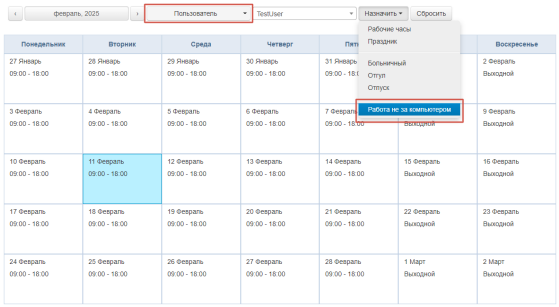
1. Нажмите + **Создать** → **Работа не за компьютером**.
2. В модальном окне укажите категорию продуктивности **Продуктивно** и название, например *Еженедельное собрание*.



3. Нажмите кнопку **Сохранить**. Новый инструмент появится на вкладке **Политики**.

После этого добавьте собрание в расписание:

1. Перейдите в **Админ** → **Календарь** и выделите дату собрания.
2. Нажмите на поле **Все**, выберите вариант **Пользователь** и укажите в свободном поле пользователя.

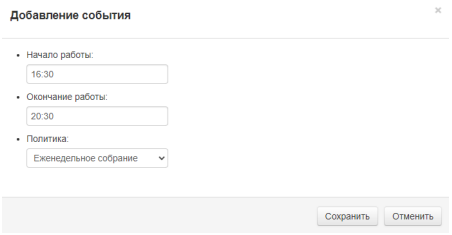


3. Выберите **Назначить** → **Работа не за компьютером**, чтобы открыть окно **Добавление события**.

Совет: Выделите дату в календаре, если меню **Назначить** недоступно для выбора.

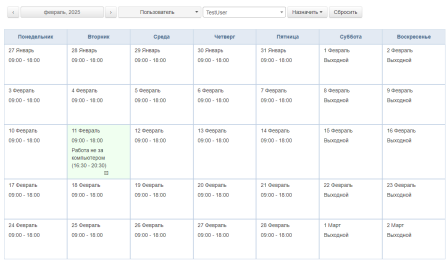
---

4. Укажите **Начало работы** и **Окончание работы** и выберите *Еженедельное собрание*.



5. Нажмите **Сохранить**. Новое событие отобразится в календаре, а в **Панели предупреждений** появится предупреждение **Расписания изменены**.

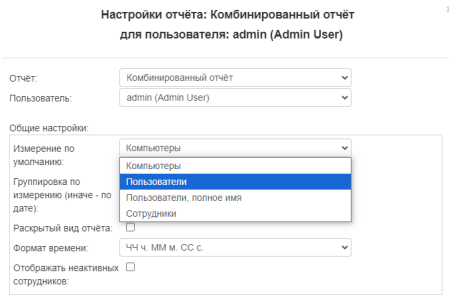
Подсказка: Нажмите крестик , чтобы удалить событие.



6. Выберите **Админ** → **Применить расписания** и дождитесь окончания применения расписаний.

Наконец, добавьте собрание в отчет:

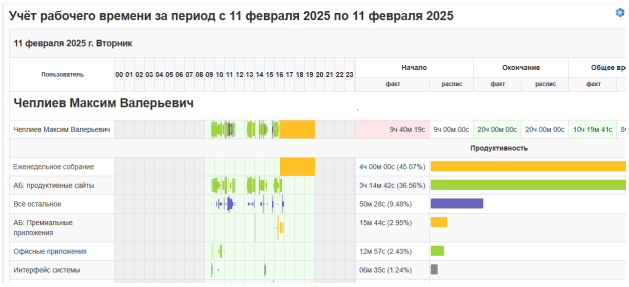
1. Нажмите кнопку **Домой** и выделите в **Датапикере** временной период, в который попадает дата еженедельного собрания.
2. Добавьте условие **Пользователь** — **Пользователь** — *TestUser*.
3. Выберите **Учет времени** → **Комбинированный отчет** и нажмите на шестеренку. Откроется окно **Настройки отчета**.



4. Укажите значение *Пользователи* или *Пользователи, полное имя* в поле **Измерение по умолчанию** и нажмите **Сохранить**.

Важно: **Работу не за компьютером** можно назначить только пользователю. Поэтому при построении отчетов на основе активности компьютеров она не будет отображаться.

В результате **Работа не за компьютером** отобразится в **Комбинированном отчете** и убдет учитываться в активности пользователя.



Обогащение данных

Инструменты **Обогащение данных** позволяют оценивать продуктивность и опасность событий. На основе этого можно настроить ответные действия системы: уведомления, смену конфигурации.

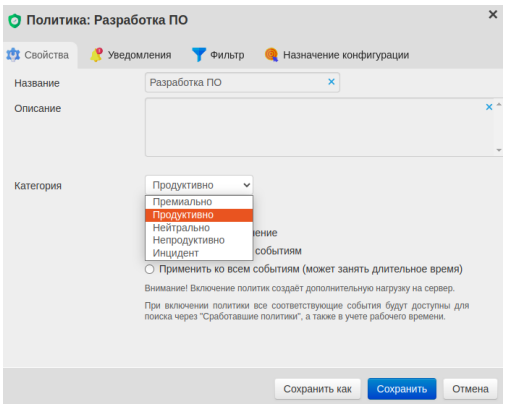
Политика

Политика — это набор правил, который помогает определить продуктивность сотрудников и уровень опасности их действий на рабочем месте.

Когда сотрудник работает за компьютером, его действия проверяются по заданным правилам. Если действие подходит под правило — политика присваивает ему категорию продуктивности рабочего времени: продуктивное, непродуктивное, нейтральное, премиальное.

Например, работа с корпоративными документами считается продуктивной активностью. Когда сотрудник заходит на сайт по поиску работы — сработает политика **Сайты по трудоустройству**, а время будет засчитано как непродуктивное. В отчетах учета рабочего времени оно выделено красным цветом.

Некоторые события могут попадать под категорию **Инцидент**. Это значит, что действие небезопасно. Например, обход мониторинга может расцениваться, как несанкционированное действие.



См.также:

Список встроенных политик

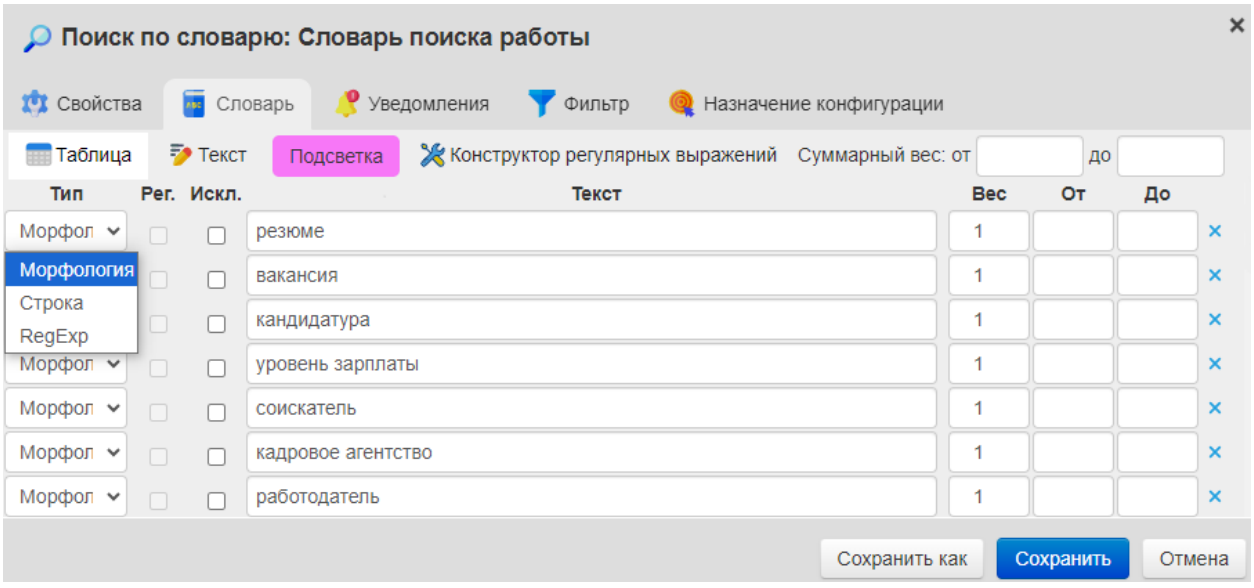
См.также:

Подробнее о политиках

Поиск по словарю

Поиск по словарю — отдельная политика для поиска указанного в настройках контента. Помогает находить персональные данные, служебную информацию и другие важные категории данных в текстовых полях. Поиск по словарю использует контекстный анализ, поддерживает морфологию и регулярные выражения, что делает его точным и эффективным инструментом.

Примечание: *Активируйте модуль Hyperscan* для увеличения производительности при поиске регулярных выражений, определения веса строк.



См.также:

Подробнее о настройке Поиска по словарю

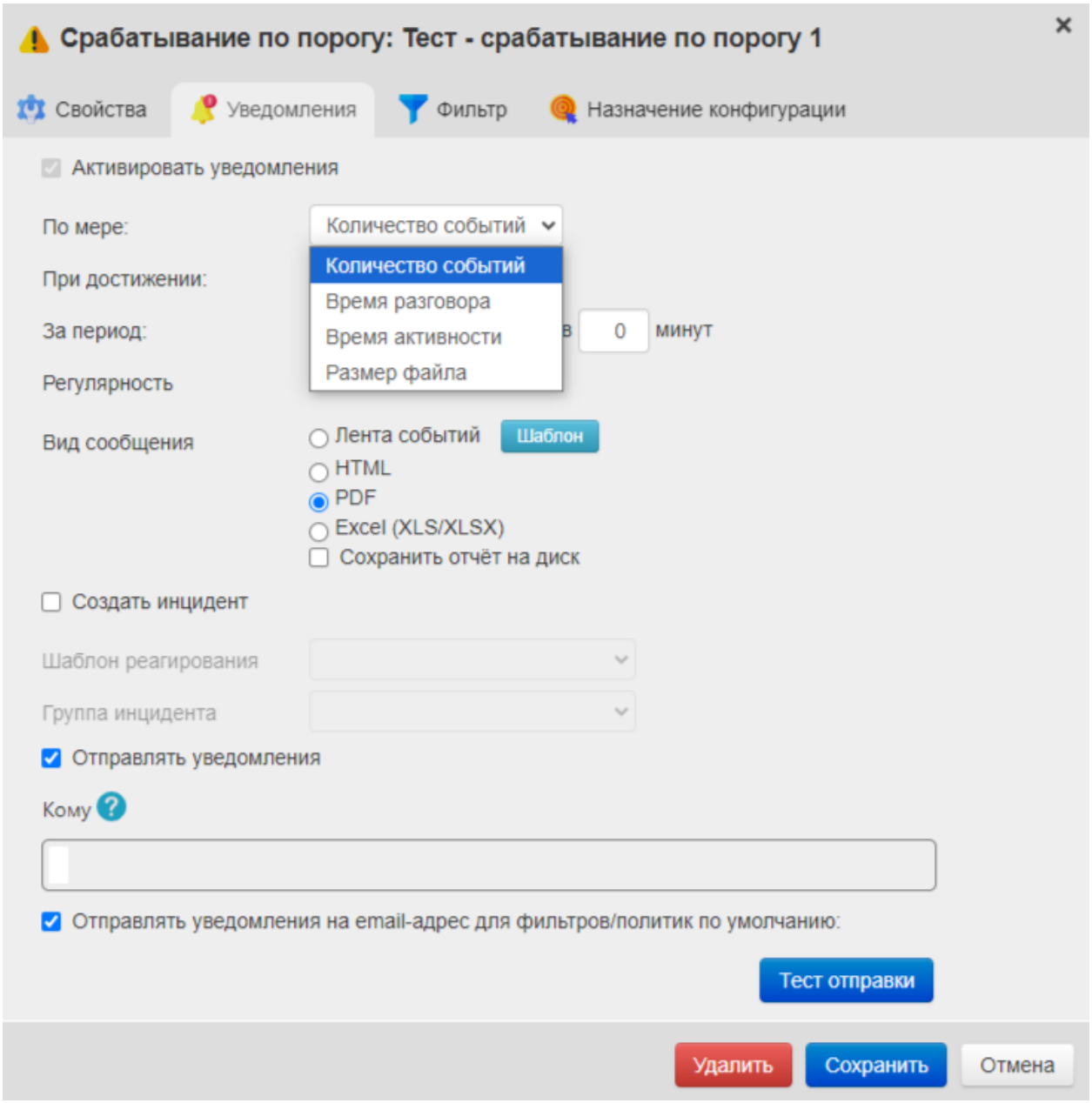
Срабатывание по порогу

Срабатывание по порогу — политика, которая отправляет уведомление при достижении установленного порога за определенное время.

Порог можно задать для измерений:

- Количество событий,
- Время разговора,
- Время активности,
- Размер файла.

Примечание: **Срабатывание по порогу** не обогащает данные, но анализирует поступающие события и отправляет уведомление, если условия срабатывания выполнены.



Пример настройки: допустим, уведомление должно приходить, если сотрудник распечатывает более 50 страниц за 5 минут.

1. Нажмите + **Создать** → **Срабатывание по порогу**.
2. В открывшемся окне заполните поля **Название** и **Описание**.
3. Во вкладке **Фильтр** выделите **Тип события** → **Печать документов**.
4. Во вкладке **Уведомления** укажите:

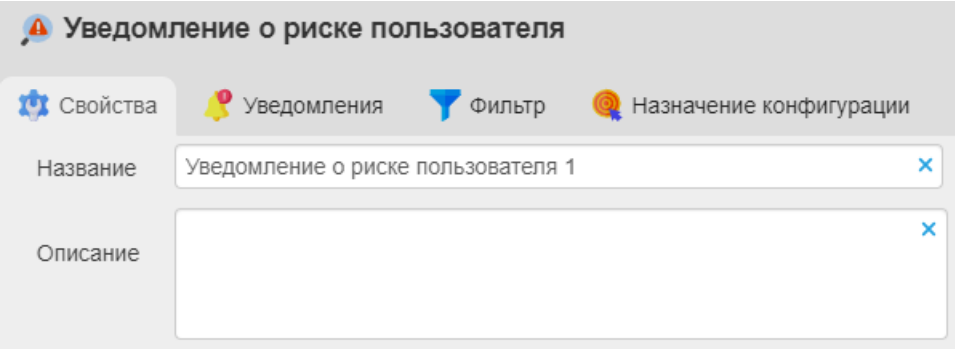
- **По мере** → **Количество событий**,
- **При достижении** → **50 событий**,
- **За период** → **0 дней 0 часов 5 минут**.

5. Активируйте **Отправлять уведомления** и укажите в поле **Кому** электронную почту.

6. Нажмите **Сохранить**.

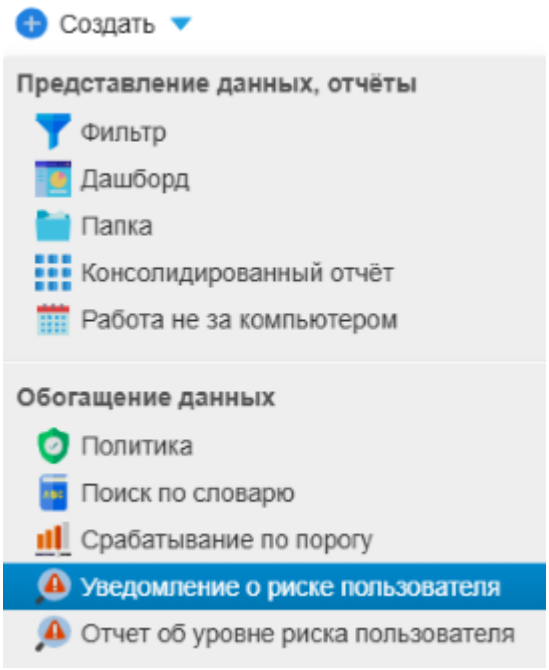
Уведомление о риске пользователя

Уведомление о риске пользователя — политика, которая отправляет уведомления, если зафиксирован повышенный *Уровень риска*.

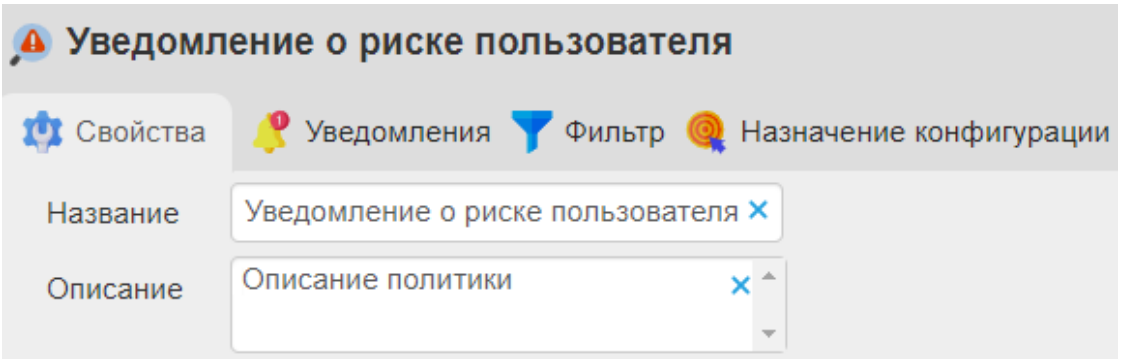


Чтобы создать уведомление, выполните следующие действия:

1. Нажмите + **Создать** и выберите **Уведомление о риске пользователя**.



2. Заполните поля **Название** и **Описание**.



3. Перейдите во вкладку **Уведомления**.

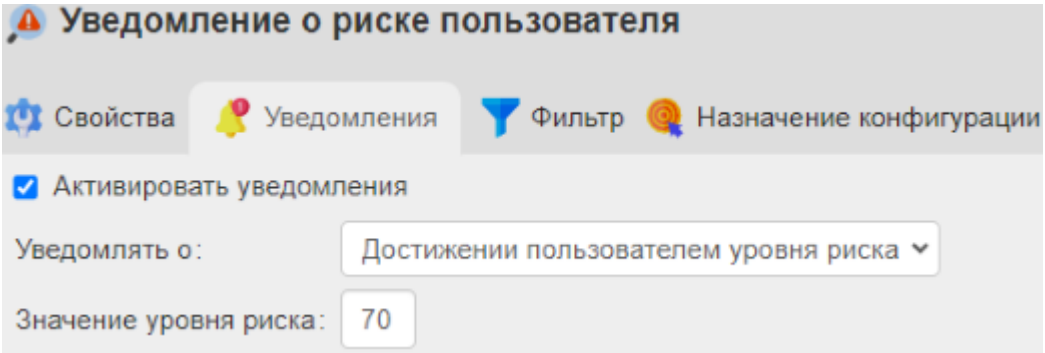
Вкладка Уведомления

1. Активируйте галочку **Активировать уведомления**.
2. Выберите условие уведомления в поле **Уведомлять о**:
   - **Достижении пользователем уровня риска** — при достижении определенного уровня риска создает событие **Высокий уровень риска пользователя**;
   - **Изменении уровня риска на указанное значение** — при изменении уровня риска на указанное значение создает событие **Увеличение уровня риска пользователя**.

Примечание: События **Высокий уровень риска пользователя** и **Увеличение уровня риска пользователя** доступны в **Конструкторе** → **Уведомления**.

---

3. Если вы выбрали опцию **Изменение уровня риска на указанное значение**, то укажите **период**, за который должно измениться значение риска. По умолчанию — 1 день.
4. Задайте **Значение уровня риска**. По умолчанию — 70.



5. Заполните опции из разделов **Регулярность**, чтобы получать *регулярную рассылку отчетов*:

- по пользователям с высоким уровнем риска,
- по пользователям с резким ростом уровня риска за период, который указан в разделе **Регулярность** .

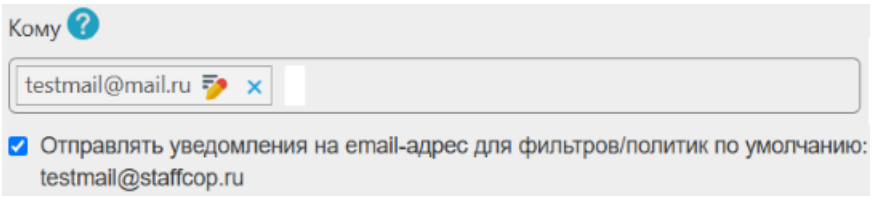
6. Если вы хотите, чтобы при срабатывании политики создавался инцидент, поставьте галочку **Инцидент** и укажите:
   - **Шаблон реагирования для инцидента** — шаблон действий для решения инцидента,

- **Группу инцидента** — группу, к которой может относиться инцидент, например, **Уровень риска**.

См.также:

Как *создать группу инцидентов*.

7. Укажите **Адрес получателя уведомления** или активируйте опцию **Отправлять уведомления на email-адрес для фильтров/политик по умолчанию**.

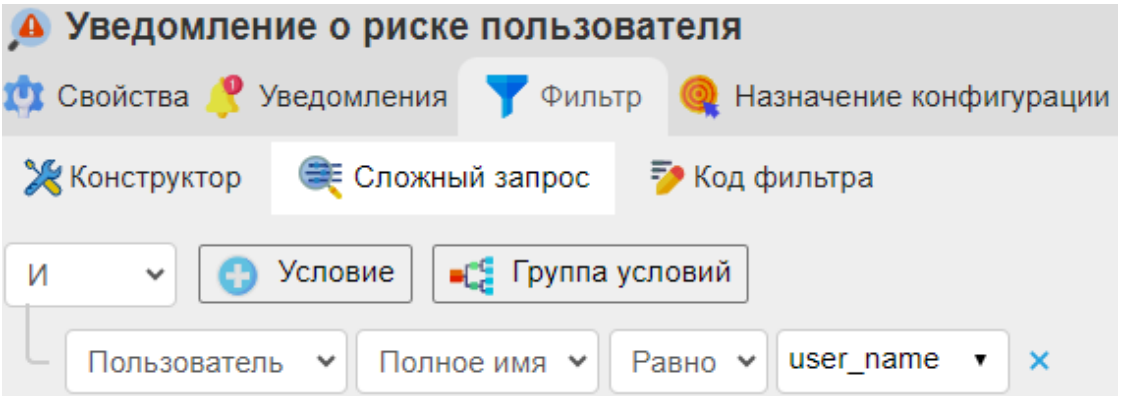


8. Перейдите во вкладку **Фильтр**.

Вкладка Фильтр

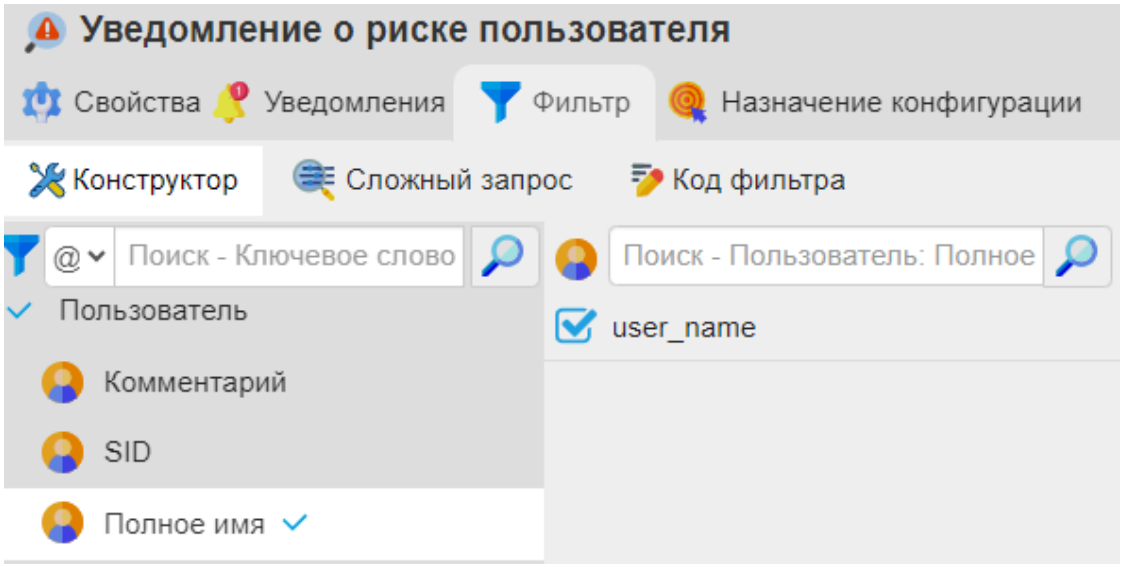
С помощью Сложного запроса

1. Выберите тип фильтра — **Сложный запрос**.
2. Нажмите + **Условие**.
3. Заполните поля: **Пользователь** — **Полное имя** — **Равно** — *имя пользователя*.



С помощью Конструктора

1. Выберите тип фильтра — **Конструктор**.
2. Выберите в левой боковой панели интересующих вас сотрудников. Для **Конструктора** доступны только измерения группы **Пользователь**.



Примечание: Если фильтр по пользователям не настроен, уведомления будут отправляться по риску всех пользователей.

Вкладка Назначение конфигурации

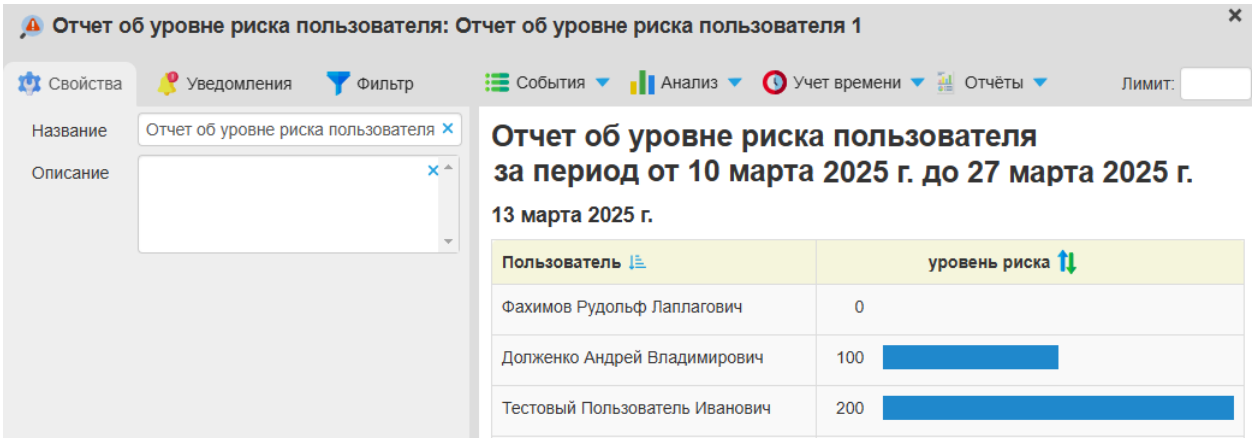
При необходимости вы можете включить изменение конфигурации при срабатывании политики. Это может быть полезно, если у пользователя зафиксирован резкий рост уровня риска, и нужно сменить конфигурацию на другую.

1. Поставьте галочку **Включить**.
2. Выберите в списки конфигурацию, которая включится при срабатывании политики. Например, вы можете активировать более строгий контроль через конфигурацию **Усиленный контроль**.

После настройки политики сервер отобразит в правой части экрана отчет, в котором указаны пользователи и уровень риска.

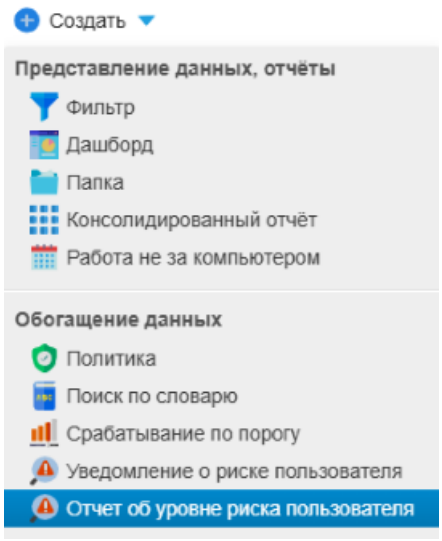
Отчет об уровне риска пользователя

Отчет об уровне риска пользователя — инструмент, который отображает пользователей, чей уровень риска больше или меньше заданного.

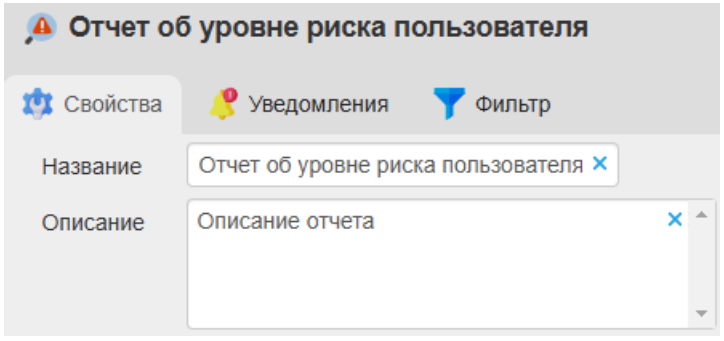


Чтобы создать отчет:

1. Нажмите + **Создать** и выберите **Отчет об уровне риске пользователя**.



2. Заполните поля **Название** и **Описание**.



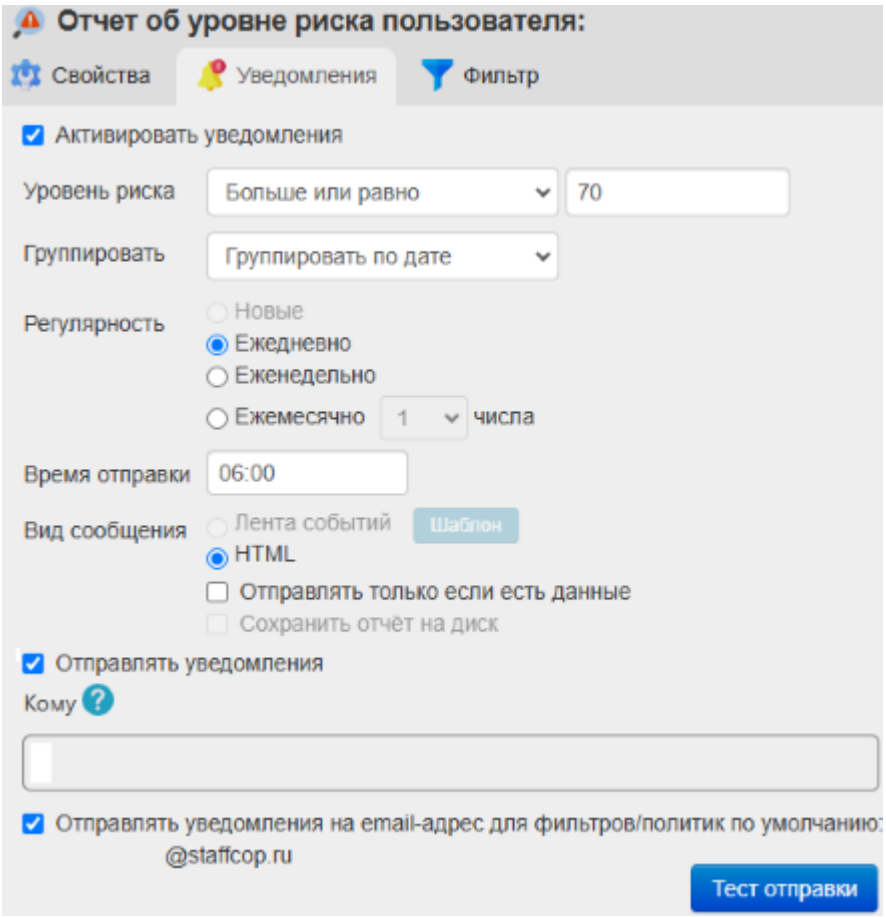
3. Перейдите во вкладку **Уведомления**.

Вкладка Уведомления

1. Активируйте галочку **Активировать уведомления**.
2. Укажите условие уведомления в поле **Уровень риска**:

- **Больше или равно** — отображать пользователей с уровнем риска больше или равным заданному в поле **Уровень риска**,
- **Меньше** — отображать пользователей с уровнем риска меньше заданного в поле **Уровень риска**.

3. Задайте значение уровня риска в поле слева от **Уровня риска**. По умолчанию — 70.
4. Выберите опцию в поле **Группировать**: **Группировать по дате** или **Группировать по пользователю**.
5. Заполните опции из разделов **Регулярность**, чтобы получать *регулярную рассылку отчетов*.



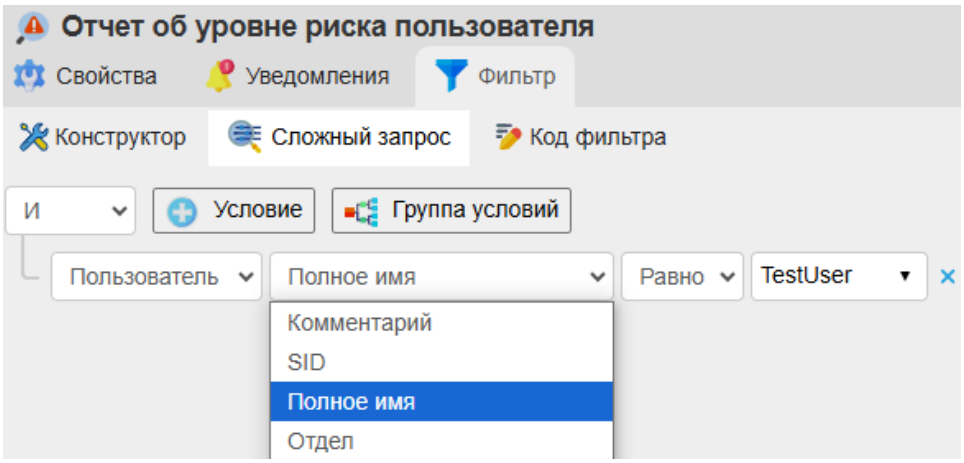
6. Укажите **Адрес получателя уведомления** или активируйте опцию **Отправлять уведомления на email-адрес для фильтров/политик по умолчанию**.
7. Перейдите во вкладку **Фильтр** и при необходимости выберите пользователей, по которым нужно формировать отчет.

Вкладка Фильтр

Примечание: Если фильтр по пользователям не настроен, отчет будет формироваться по риску всех пользователей.

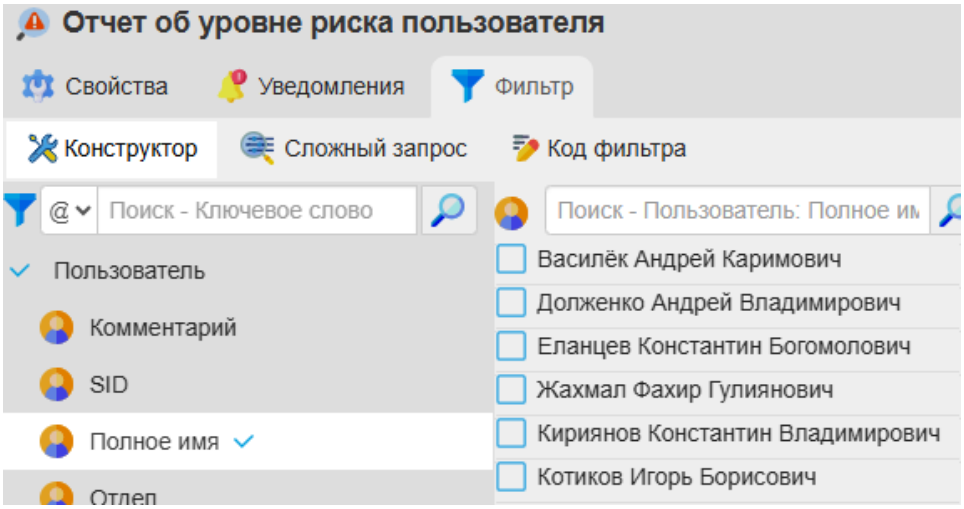
С помощью Сложного запроса

1. Выберите тип фильтра — **Сложный запрос**.
2. Нажмите + **Условие**.
3. Заполните поля: **Пользователь** — **Полное имя** — **Равно** — *имя пользователя*.

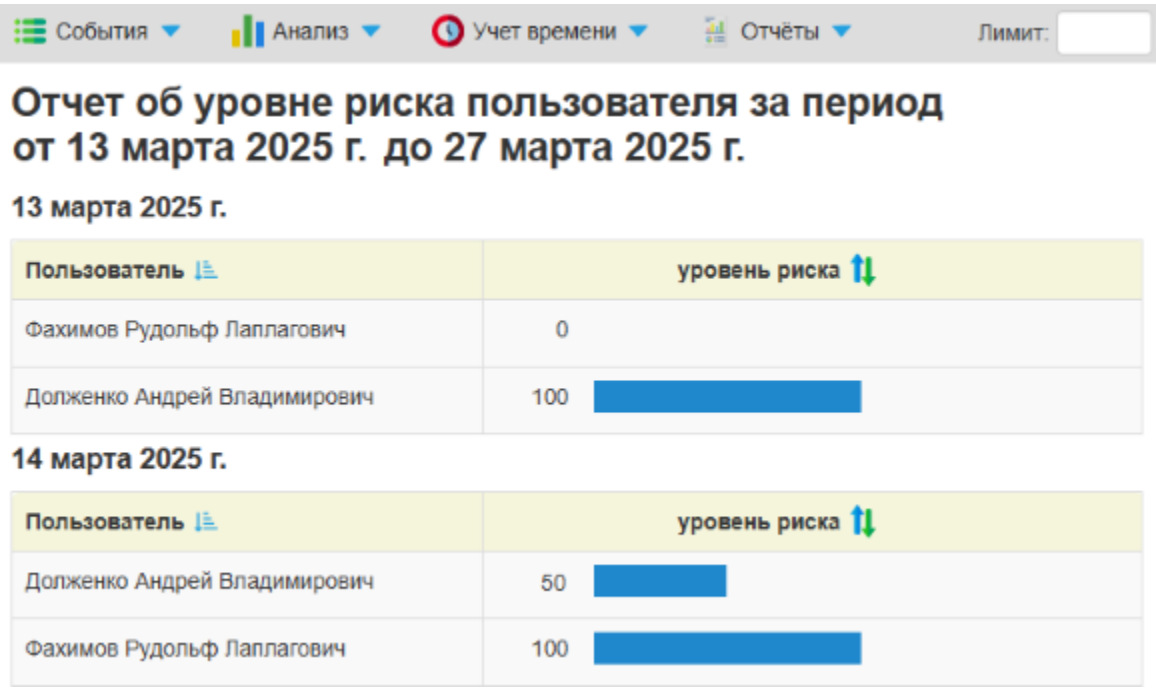


С помощью Конструктора

1. Выберите тип фильтра — **Конструктор**.
2. Выберите в левой боковой панели интересующих вас сотрудников.



После настройки инструмент появится на вкладке **Политики** — нажмите на него, чтобы отчет отобразился в **Линзе событий**.



Управление данными

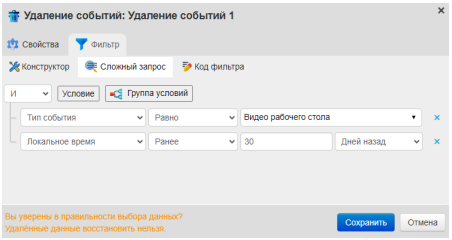
Политика удаления событий

Политика удаления событий — политика, которая удаляет события из базы данных в соответствии с заданными правилами.

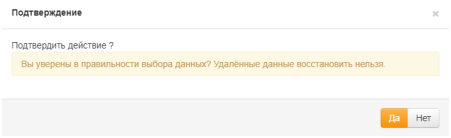
Важно: Чтобы создать **Политику удаления событий**, администратор должен иметь *расширенные права*.

Пример настройки: удаления событий **Видео рабочего стола** старше месяца:

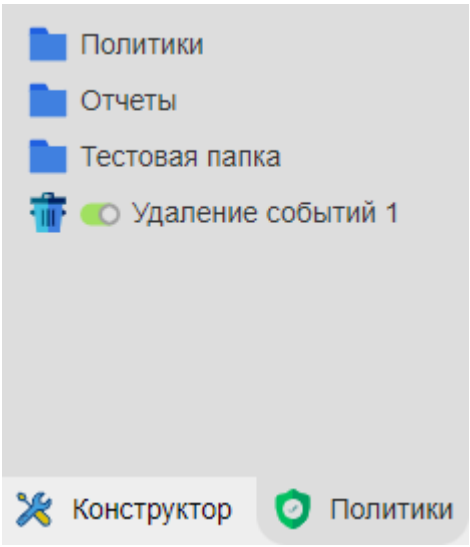
1. Нажмите + **Создать** → **Политика удаления событий**.
2. В открывшемся окне активируйте опцию **Политика активна**.
3. Во вкладке **Фильтр** → **Сложный запрос** выберите логический оператор **И**.
4. Нажмите + **Условие** и введите **Тип события** → **Видео рабочего стола**.
5. Нажмите + **Условие** и введите **Локальное время** — **Ранее** — *30* — **Дней назад**.



6. Нажмите **Сохранить**.
7. Нажмите **Да** в диалоговом окне, чтобы подтвердить удаление.



После сохранения **Политика удаления событий** появится на вкладке **Политики** и будет автоматически удалять видео рабочего стола, которым больше 30 дней. Чтобы отключить политику, переведите зеленый триггер в неактивное состояние.



4.3.6 Системные фильтры

При первом входе в веб-консоль после установки сервера, во вкладке **Фильтры** можно увидеть уже созданные фильтры, сконфигурированные в дерево фильтров. Данное дерево фильтров состоит из трёх основных разделов: **Эффективность**, **Безопасность** и **Политики**. Фильтры, содержащиеся в каждом из этих разделов, имеют свою значимость в отображении данных и настройках подсчетов отчетов по продуктивности (например, в **Учете рабочего времени**). Данные фильтры были созданы на основе среднестатистической востребованности среди пользователей DLP-систем по сбору пользовательских данных на ПК. Далее описаны предназначения каждого фильтра из дерева **Системных фильтров** по категориям.

Эффективность

Категория **Эффективность** содержит в себе готовые фильтры для отображения продуктивности сотрудников. Состоит из следующих подкатегорий:

Отчеты и табели:

tabularytabulary

Название фильтра
Активное время по отделам
Продуктивное время по отделам
Общий отчет по рабочему времени
Сводный отчет по продуктивности
Отчет по опозданиям
Статистика за период
Статистика по дням
Табель использования принтера
Табель учета рабочего времени

Продуктивность:

tabularytabulary

Название фильтра
Продуктивная деятельность
Непродуктивная деятельность

Безопасность

Категория **Безопасность** содержит фильтры для контроля утечки данных в переписке, ввода номеров банковских карт, копирования файлов на внешние носители и упоминания неприемлемых слов в деловом общении.

Подкатегории:

События:

tabularytabulary

Название фильтра
Снимки экрана
**Снимки с **
Интернет-пейджеры
Почта
Буфер обмена
Внешние накопители

Инциденты:

tabularytabulary

Название фильтра
Динамика нарушений
Нарушители
Нарушители по отделам
Нарушители по должностям
Нарушения

Политики

В свойствах Политики имеются настройки «Политика активна», «Применять политику к новым событиям» или «Применить политику ко всем событиям». «Политика активна» включает политику, «Применение ко всем событиям» запускает пересчет всех событий по данной политике.

Рассмотрим более детально подкатегории дерева фильтров Политики.

Политики продуктивности

tabularytabulary

Название фильтра
Категории приложений
Категории веб-ресурсов

Политики безопасности

tabularytabulary

Название фильтра
Кредитные карты
Словарь ненормативной лексики
Отправка писем самому себе
Скриншоты по PrtScr
Поиск iBatyr Monitor
Шифрованный архив
Пароль в браузерах

Системные политики

Детекторы

Детектор - сводный отчет, отображающий характеристики объекта или множества объектов и события с ними связанные в удобном, для данного типа, виде.

tabularytabulary

Название фильтра
Отсутствие событий
Изменение оборудования
Задержка выгрузки
Опоздание пользователя

Карточки измерений

Карточка измерения - сводный отчет, отображающий характеристики объекта или множества объектов и события с ними связанные в удобном, для данного типа, виде.

Данные фильтры позволяет детально настроить вывод карточек измерений.

tabularytabulary

Название фильтра
Карточка компьютера
Карточка пользователя
Карточка приложения
Карточка сайта
Карточка сетевой активности
Карточка файлов
Карточка устройства
Карточка диалога
Карточка инсталляций

4.3.7 Карточка измерения

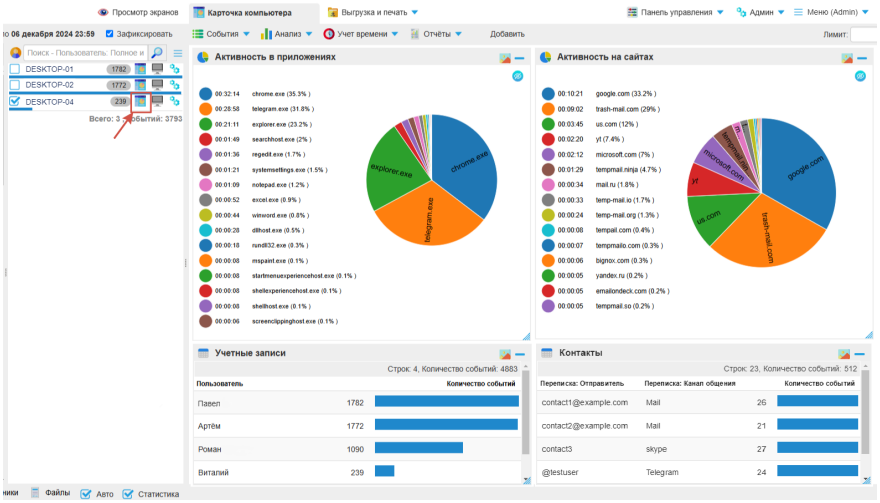
Карточка измерения — это дашборд, который показывает сводную информацию по выбранному объекту в виде набора готовых отчетов. Позволяет быстро анализировать данные по агентам, пользователям, приложениям, сайтам и другим объектам без ручной настройки фильтрации.

Карточки доступны для объектов:

- Агент,
- Пользователь,
- Приложение,
- Сайт,
- Сетевая активность,
- Файл,
- Устройство,
- Диалог,
- Инсталляции.

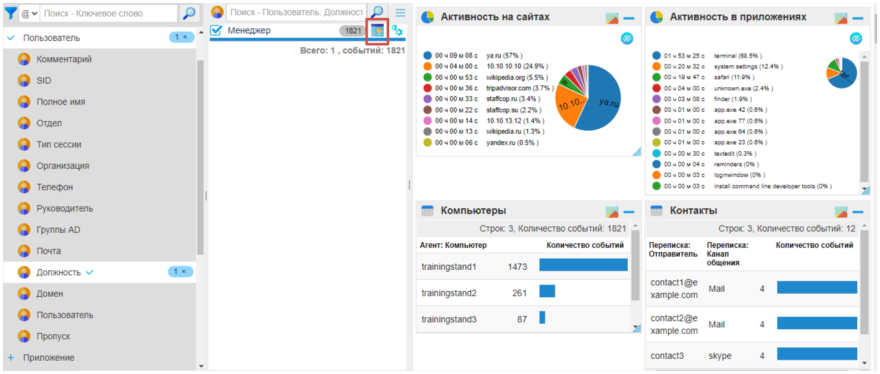
Раабота с карточкой

Чтобы открыть карточку, нажмите на иконку рядом с объектом в **Конструкторе** — например, возле имени компьютера. Карточка откроется в правой части экрана:



Карточка позволяет анализировать данные по разным параметрам объекта.

Например, в **Конструкторе** выберите **Пользователь** и добавьте измерение **Должность**. Выберите должность и нажмите на иконку рядом с ней. В отчете отобразятся данные всех пользователей, которые занимают эту должность.



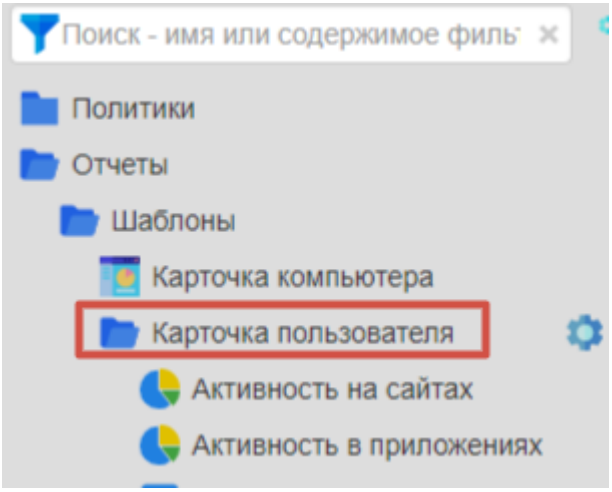
Как добавить отчет в карточку

Примечание: Не рекомендуется изменять вложенные отчеты в предустановленных **Карточках измерений**. Изменение параметров может привести к некорректным результатам. При необходимости вы можете добавить новый отчет в готовую **Карточку измерений** или создать новый **Дашборд**.

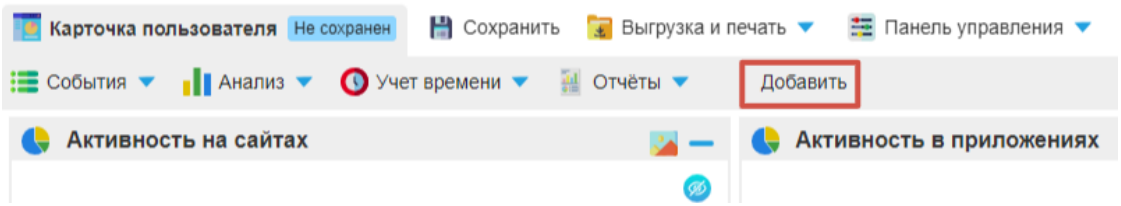
Шаблоны карточек находятся во вкладке **Политики** в разделе **Отчеты** → **Шаблоны**. Вы можете добавить новый отчет в шаблон карточки.

Например, чтобы добавить отчет **Табель отсутствия на рабочем месте** в **Карточку пользователя**:

1. Перейдите во вкладку **Политики** → **Отчеты** → **Шаблоны** и нажмите на **Карточку пользователя**.

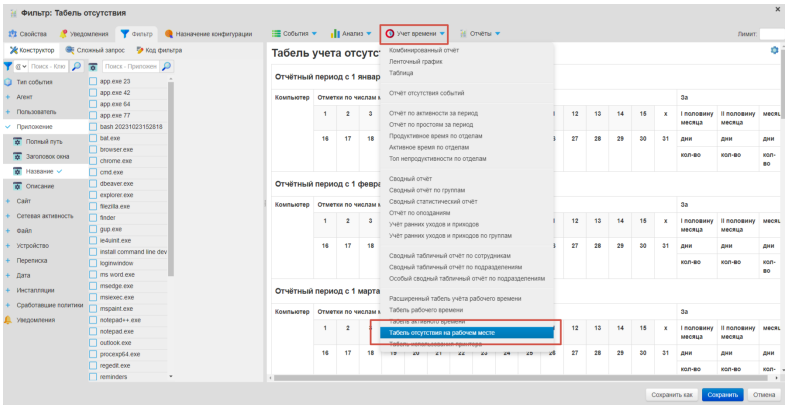


2. В **Линзе событий** нажмите кнопку **Добавить**.



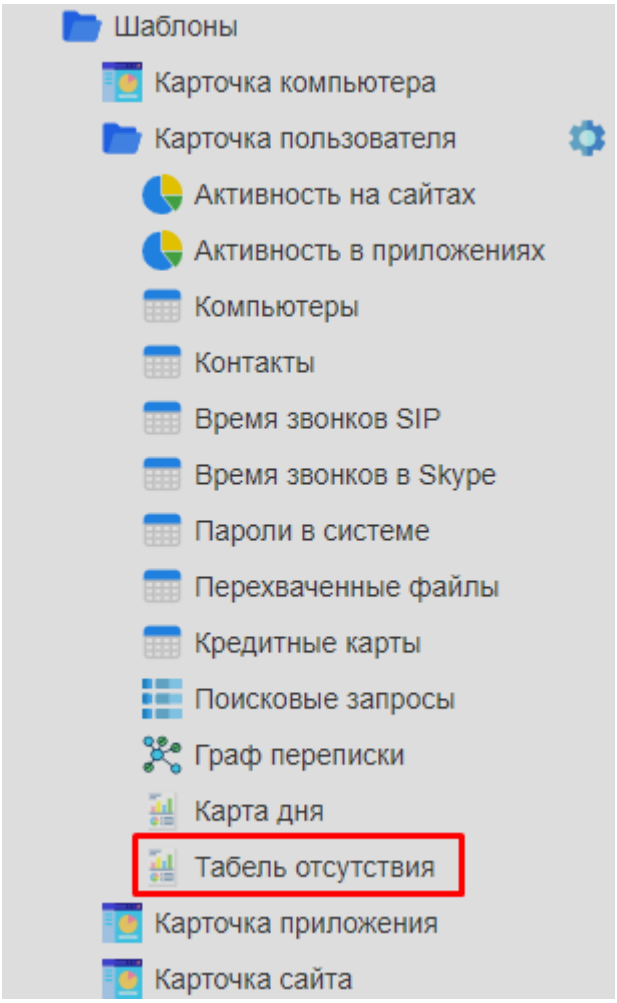
3. В окне **Свойства** введите название отчета, например *Табель отсутствия*.

4. Выберите **Учет времени** → **Табель отсутствия на рабочем месте**.

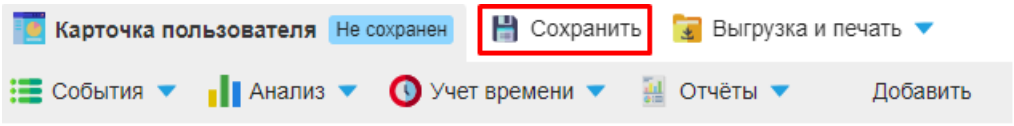


5. Нажмите **Сохранить**.

6. Убедитесь, что **Табель отсутствия** появился в **Карточке пользователя**.

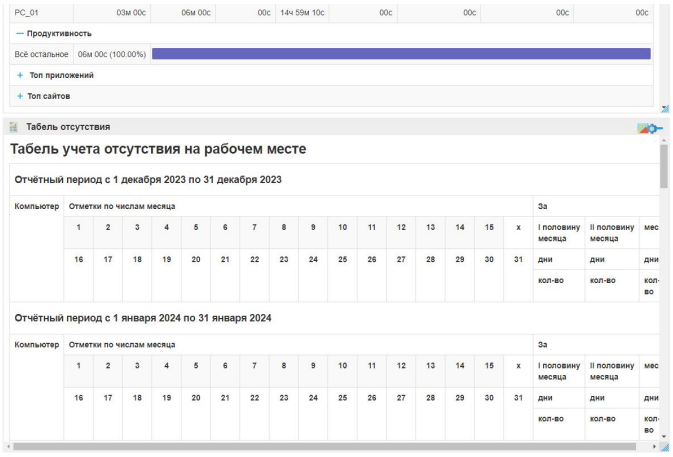


7. Нажмите на кнопку **Сохранить**.



> **Предупреждение:** После сохранения статус карточки **Не сохранен** изменится на **Сохранен**. Не обновляйте страницу до сохранения карточки, чтобы не потерять настройки.

8. Выберите в **Конструкторе** пользователя, например, *TestUser*.
9. В **Линзе событий** пролистайте дашборд вниз, чтобы увидеть новый отчет. При необходимости зажмите на отчете левую кнопку мыши и перенесите его в удобное для вас удобное место.

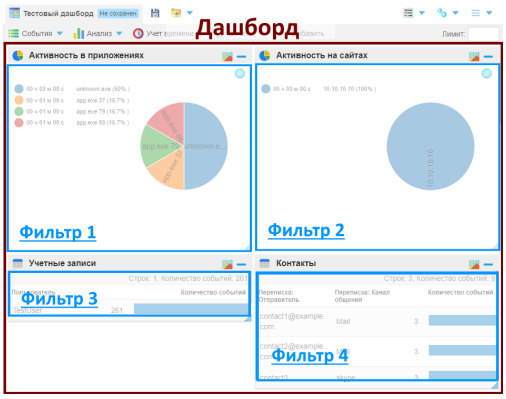


4.3.8 Дашборд

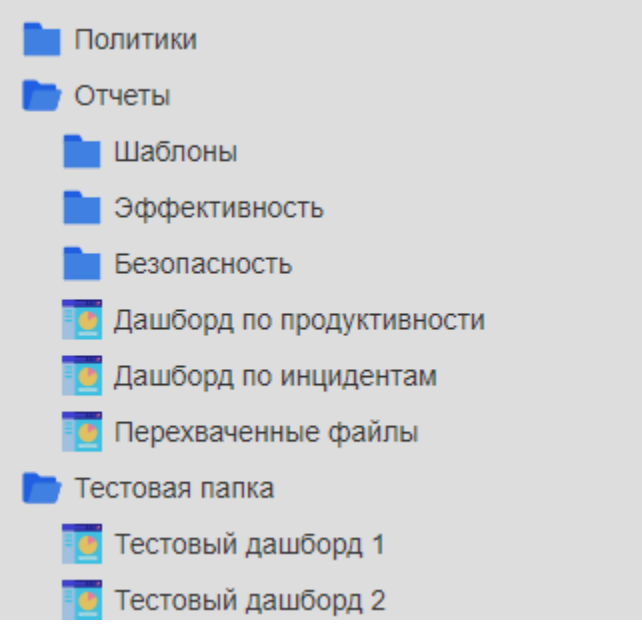
Дашборд — набор из нескольких фильтров и отчетов, которые отображаются в одном окне.

См.также:

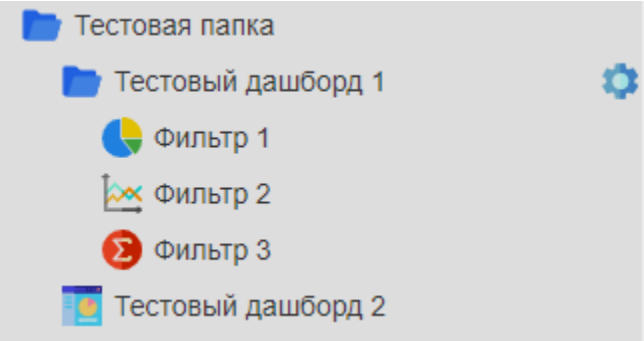
Подробнее о встроенных дашбордах — *Карточках измерений*.



Все готовые и созданные дашборды находятся на вкладке **Политики**.



Нажмите на дашборд, чтобы увидеть фильтры и отчеты, из которых он состоит.



Дашборды позволяют посмотреть различные отчеты и графики по отфильтрованной группе событий.

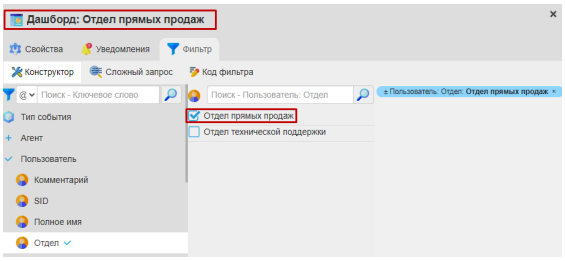
Как создать дашборд

Пример: Необходимо создать дашборд для анализа активности сотрудников *Отдела прямых продаж*.

В дашборде события будут отфильтрованы по пользователям из *Отдела прямых продаж*, а каждый вложенный отчет/фильтр будет отображать информацию по их активности, файлам и инцидентам.

1. На главной странице интерфейса нажмите + **Создать** → **Дашборд**.
2. В открывшемся окне введите **Название** дашборда — *Отдел прямых продаж*.
3. Добавьте условие **Пользователи** — **Отдел** — *Отдел прямых продаж* во вкладке **Фильтр**.

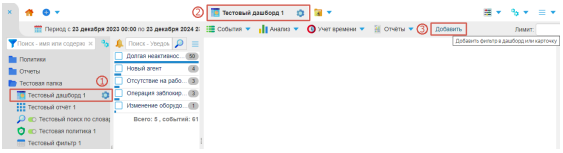
Важно: Условия фильтрации, которые были указаны для дашборда, применятся и ко всем вложенным фильтрам и отчетам внутри дашборда.



4. Нажмите **Сохранить**.

5. В главном интерфейсе на вкладке **Политики** откройте новый дашборд — над **Линзой событий** появится название дашборда.

6. Выберите **Добавить** над **Линзой событий** — откроется окно создания **Фильтра**.



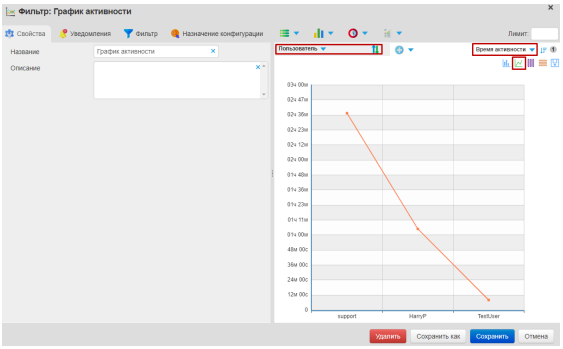
7. В открывшемся окне введите **Название** фильтра — *График активности*.

8. На вкладке **Фильтр** выберите формат отображения данных **Анализ** — *Линейный график*.

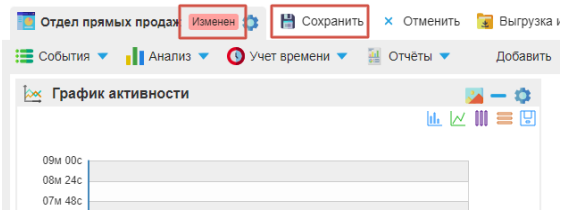
   См.также:

   Подробнее о работе в режиме *Анализ и группировке по измерению*.

9. Укажите *группировку по измерению* **Пользователь — Пользователь**, *меру* **Время активности** и вид **Линейный график** .



10. Нажмите **Сохранить** — после этого окно закроется и внутри дашборда появится область с новым фильтром.

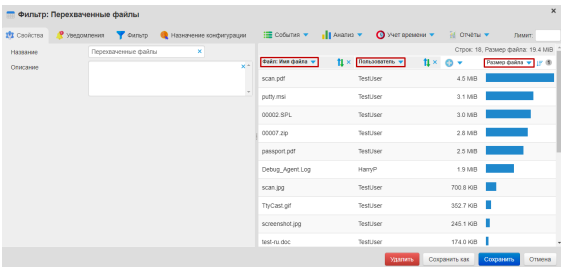


Примечание: Обратите внимание, что возле названия дашборда появилась метка **Изменен** — это значит, что в дашборд были внесены несохраненные изменения. Сохраните

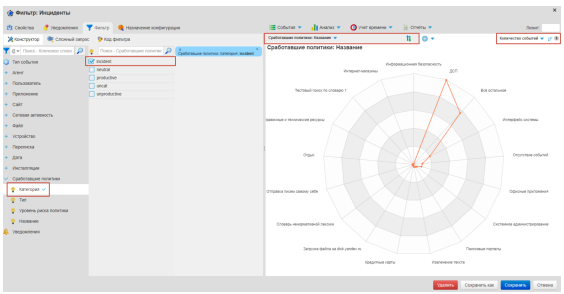
изменения , иначе при переключении на другой объект в **Линзе событий** все изменения будут сброшены.

---

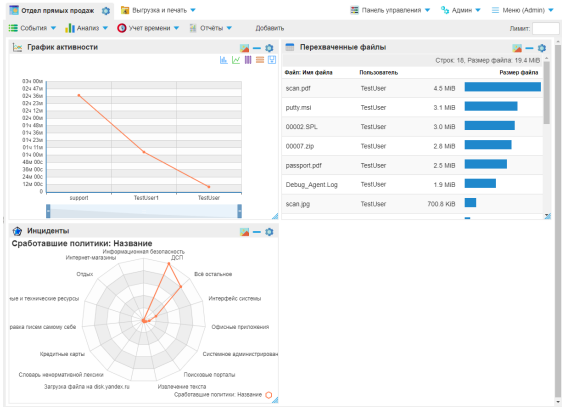
11. Нажмите **Добавить** над **Линзой событий**.
12. В открывшемся окне укажите *Перехваченные файлы* в поле **Название**.
13. На вкладке **Фильтр** выберите формат отображения данных **Анализ** — *Таблица*.
14. Укажите группировку по измерению **Файл** — **Имя файла** и меру **Размер файла**.
15. Нажмите на + и выберите группировку **Пользователь** — **Пользователь**.
16. Нажмите **Сохранить**.



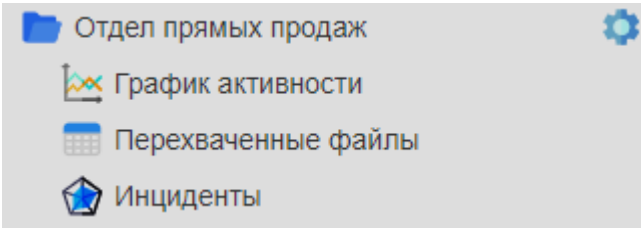
17. Нажмите **Добавить** над **Линзой событий**.
18. В открывшемся окне укажите *Перехваченные файлы* в поле **Название**.
19. На вкладке **Фильтр** выберите формат отображения данных **Анализ** — *Радар* и добавьте условие **Сработавшие политики** — **Категория** — *incident*.
20. Укажите группировку по измерению **Сработавшие политики** — **Название** и меру **Количество событий**.



21. Нажмите **Сохранить**.



22. Сохраните дашборд , после чего на вкладке **Политики** новые фильтры отобразятся внутри дашборда.



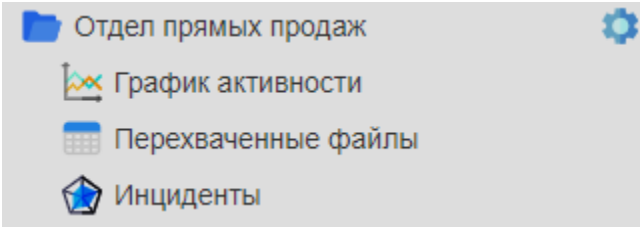
Работа с дашбордом

Фильтры внутри дашборда можно изменять, сворачивать, сохранять и перетаскивать.

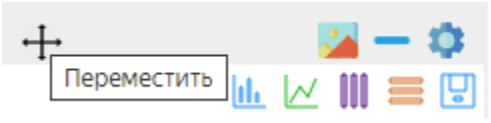
Нажмите на иконку изображения , чтобы **Сохранить фильтр как изображение**.

Нажмите на иконку черты , чтобы **Свернуть фильтр**.

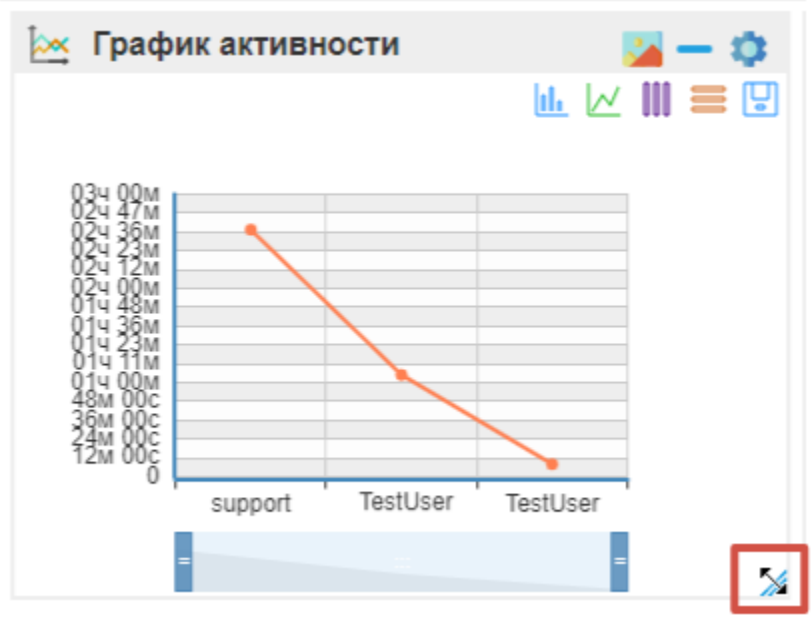
Нажмите на иконку шестеренки , чтобы открыть окно **Свойства фильтра**.



Наведите курсор на рамку фильтра, зажмите ЛКМ и потяните окно, чтобы его переместить.

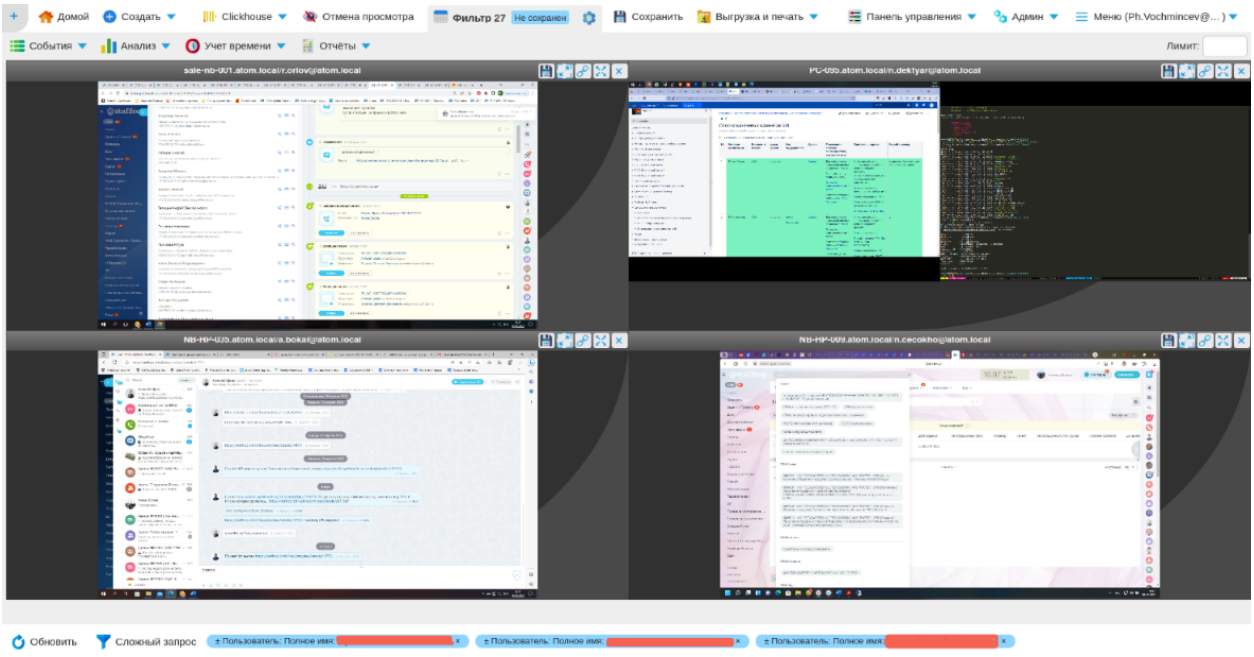


Зажмите край рамки фильтра и потяните, чтобы изменить размер фильтра.



4.3.9 Просмотр экранов

Просмотр экранов позволяет просматривать снимки или рабочие столы нескольких пользователей одновременно.



Важно: Вы можете одновременно просматривать не более 15 окон.

В режиме **Просмотр экранов** доступны:

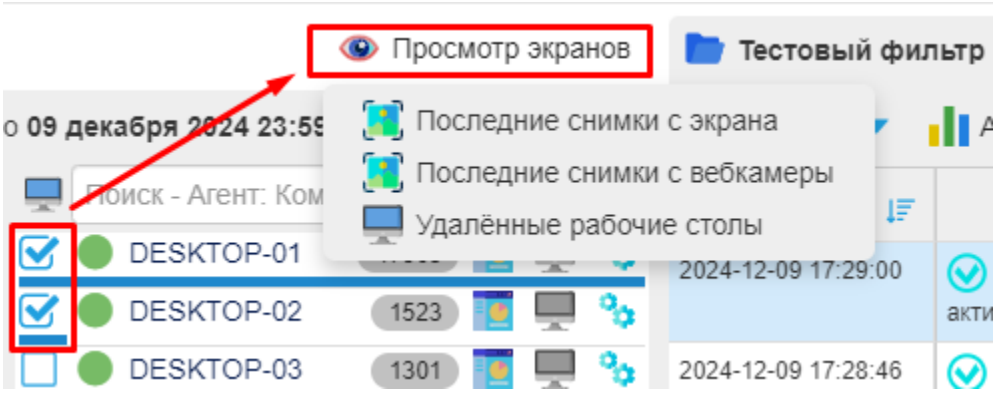
- **Последние снимки с экрана**,

- **Последние снимки с вебкамеры**,
- **Удаленные рабочие столы**.

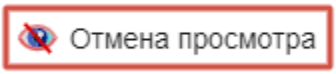
Примечание: Включите опции Снимки с и *Удаленное управление* в вашей конфигурации, чтобы просматривать **Последние снимки с вебкамеры** и **Удаленные рабочие столы**.

Для просмотра снимков или рабочих столов:

1. Выберите в **Конструкторе** компьютеры или пользователей, чьи экраны вы хотите просмотреть. Над **Конструктором** появится кнопка **Просмотр экранов**.
2. Нажмите на кнопку **Просмотр экранов**.
3. Выберите интересующую опцию — **Последние снимки с экрана**, **Последние снимки с вебкамеры** или **Удаленные рабочие столы**. После этого снимки или видео появятся в **Линзе событий**.



Нажмите **Отмена просмотра** чтобы выйти из режима просмотра экранов.

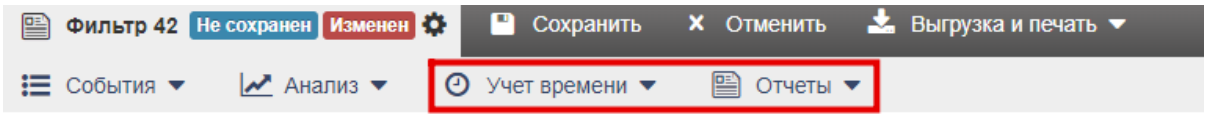


См.также:

Что делать, если *не работает удаленный рабочий стол*.

4.3.10 Отчеты

Предустановленные отчеты расположены в разделах **Учет времени** и **Отчеты**.



Учет времени

В разделе **Учёт времени** представлена информация о времени, проведённом сотрудниками на рабочем месте и о продуктивности их деятельности.

Информация о рабочем времени сотрудников может быть представлена в виде:

- комбинированного отчёта,
- ленточного графика,
- таблицы.

Информацию о деятельности сотрудников можно сортировать:

- по дате,
- по сотруднику.

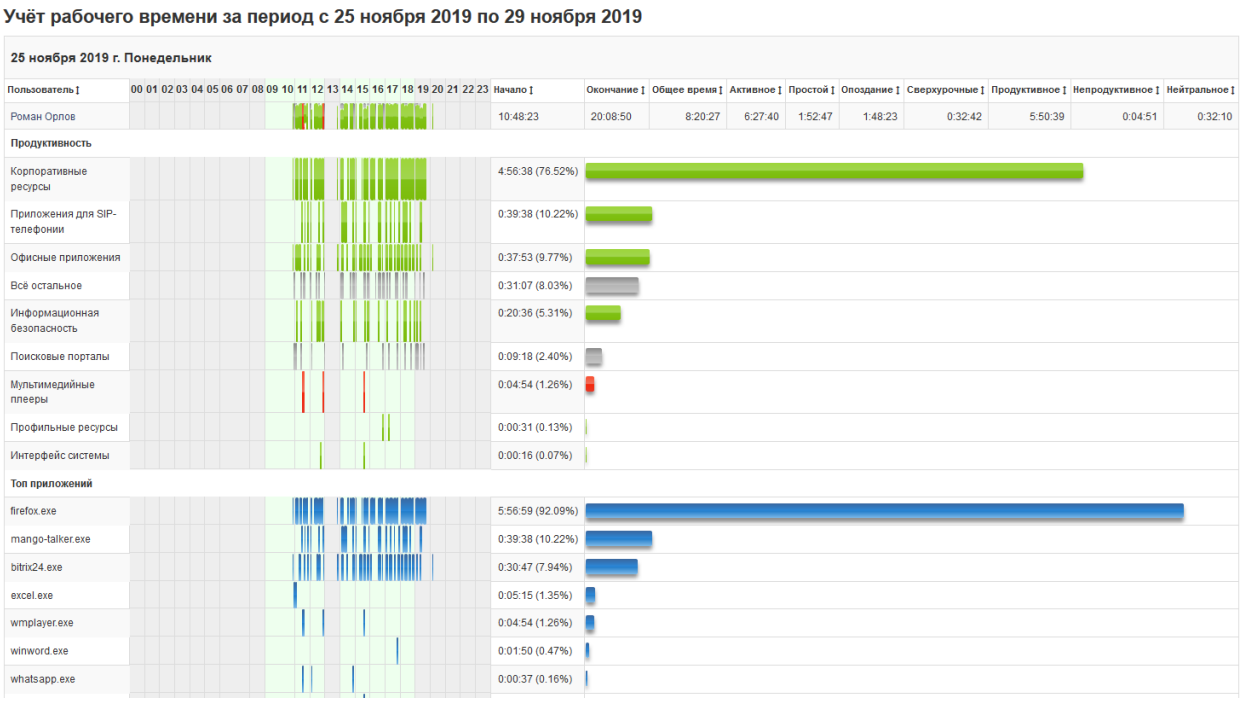
Чтобы выбрать вид представления информации в отчете:

1. В разделе **Администрирование** выберите пункт **Настройка отчётов**.
2. В открывшемся окне выберите тип отчёта: **Комбинированный отчет**, **Ленточный график** или **Таблица**.
3. Установите галочку в пункте **Группировка по измерению (иначе — по дате)**.

Варианты работы опции **Группировка по измерению (иначе — по дате)**:

Группировка по измерению (иначе — по дате)	**Вариант отображения**
вкл	***Сотрудник1*** *Дата1 Дата2 Дата3*
откл	***Дата1*** *Сотрудник1 Сотрудник2 Сотрудник3*

Учёт рабочего времени удобно использовать для быстрого анализа продуктивности сотрудников. Чтобы посмотреть детальный отчёт пользователя, нажмите на него левой кнопкой мыши.



В отчёте представлены подробности действий пользователя за компьютером:

- список сайтов и приложений, которые использовал и посещал пользователь;
- в какое время пользователь запускал те или иные сайты и приложения;
- общий временной вклад каждого приложения или сайта в рабочий день пользователя.

В отчёте деятельность сотрудника помечается цветовыми отметками продуктивности:

tabularytabulary

Цвет
Зелёный
Красный
Серый
Отсутствует

Продуктивность сотрудника определяется за пятиминутный интервал. При построении отчёта временная метка закрашивается от центра к краям. Если за один интервал времени произошло несколько событий разной продуктивности, то метка будет разделена по высоте на несколько цветов. Высота цветов пропорциональна времени деятельности.

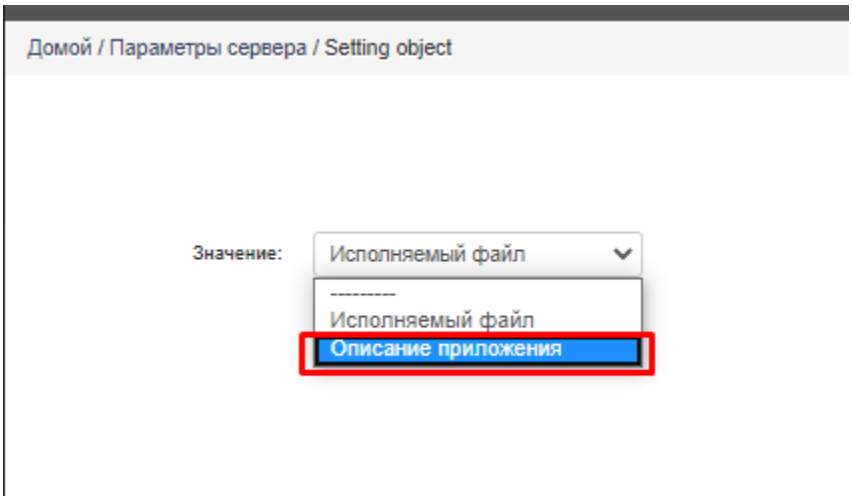
Пример: если за прошедшие 5 минут сотрудник 3 минуты смотрел видео и 2 минуты работал, то отметка будет разделена в отношении 3:2.

В дополнение к графической составляющей, в отчётах представлены:

- время начала и окончания рабочего дня;
- общее рабочее время;
- активное время;
- время простоя;
- опоздания;
- сверхурочные;

- категории продуктивности.

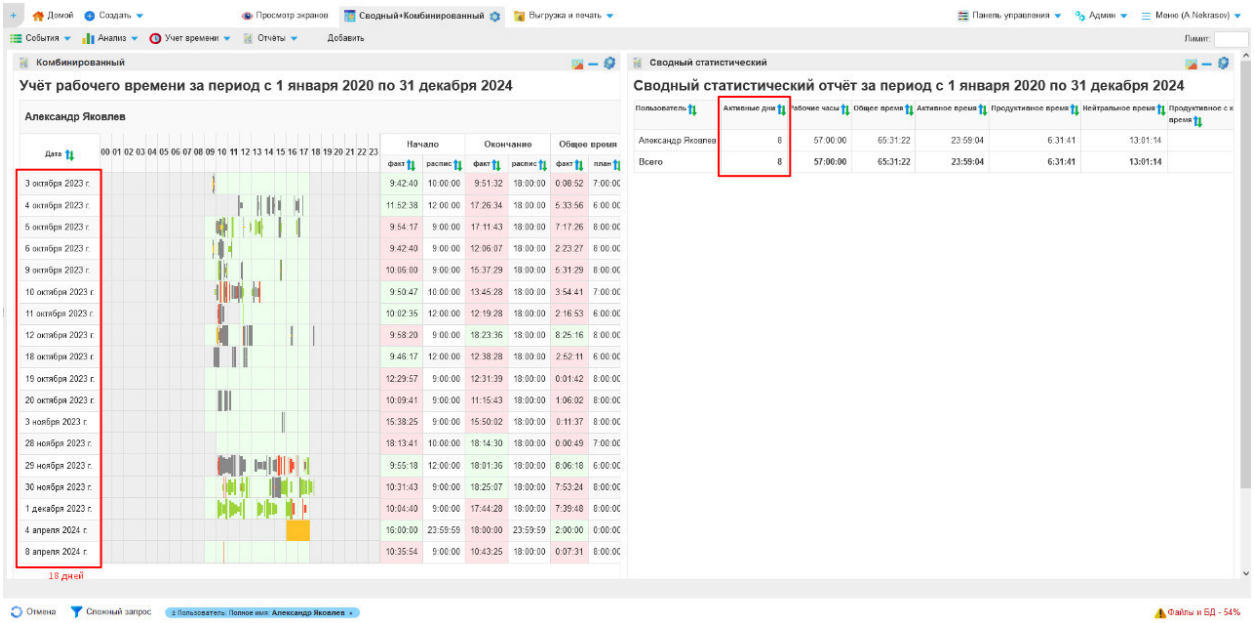
Примечание: В отчёте имена исполняемых файлов приложений можно заменить на описания приложений. Для этого в разделе **Панель управления** → **Параметры сервера** измените параметр **Измерение приложения в отчетах** на **Описание приложения**.



Определение активных дней в отчетах

День считается активным, если сотрудник работал больше одного часа.

Обратите внимание, что количество дней в **Комбинированном отчете** и **Сводном статистический отчете** может отличаться.



Оценка продуктивности

Продуктивность действий пользователя определяет набор входных фильтров. Эти фильтры анализируют информацию от рабочих станций и присваивают деятельности пользователя метки продуктивности.

Предустановленные фильтры уже содержат список наиболее популярных сайтов и приложений, которые отнесены к определённой категории деятельности. Предустановленные фильтры можно изменять, дополнять, удалять. Подробнее о работе с фильтрами читайте в статье Фильтры .

Изменение категории продуктивности

Для разных сотрудников внутри компании разные сайты и приложения могут иметь разную категорию продуктивности. Так, сервисы поиска работы могут считаться непродуктивными для рядового сотрудника, но продуктивными для отдела HR.

Чтобы изменить категорию продуктивности сайта или приложения, отредактируйте фильтр, в котором он содержится:

1. В нижней части веб-консоли в разделе **Фильтры** выберите вкладку **Политики**.
2. В разделе **Политики** → **Политики продуктивности** → **Категории приложений**/**Категории веб-ресурсов** выберите категорию.
3. Откройте редактирование выбранной категории.
4. На вкладке **Свойства** выберите категорию продуктивности.
5. Нажмите **Сохранить**.

Чтобы добавить к уже созданному фильтру приложение или сайт:

1. В нижней части веб-консоли в разделе **Фильтры** выберите вкладку **Политики**.
2. В разделе **Политики** → **Политики продуктивности** → **Категории приложений** / **Категории веб-ресурсов** выберите категорию.
3. В открывшемся окне перейдите на вкладку **Фильтр**.
4. На вкладках **Код фильтра** или **Конструктор** добавьте или удалите приложение (адрес сайта), соответствующее этой категории.
5. Нажмите **Сохранить**.

Добавление приложений или сайтов в политику из отчёта:

1. Наведите курсор на приложение или сайт и нажмите **Настроить политику**.
2. В открывшемся окне настроек политики выберите нужный фильтр в левой части экрана.

Чтобы удалить фильтр, нажмите на его название.

После завершения редактирования нажмите **Сохранить**.

Примечание: Новая категория продуктивности для выбранных сайтов или приложений будет отображаться только на новых данных. Данные, полученные до изменения категории продуктивности, останутся с прежней статистикой. Чтобы пересчитать продуктивность всех событий с учётом новой категории, в разделе **Администрирование** выберите пункт **Перестроить отчёты**. Это может занять значительное время, вплоть до нескольких суток.

Предустановленные отчёты

Отчёты в разделе **Учёт времени**.

tabularytabulary

Название отчёта
Отчёт по активности за период
Продуктивное время по отделам
Активное время по отделам
Топ непродуктивности по отделам
Сводный отчёт
Отчёт по опозданиям
Учёт ранних приходов и уходов
Табель рабочего времени
Табель активного времени
Табель отсутствия на рабочем месте
Табель использования принтера

Отчёты в разделе «Отчеты».

tabularytabulary

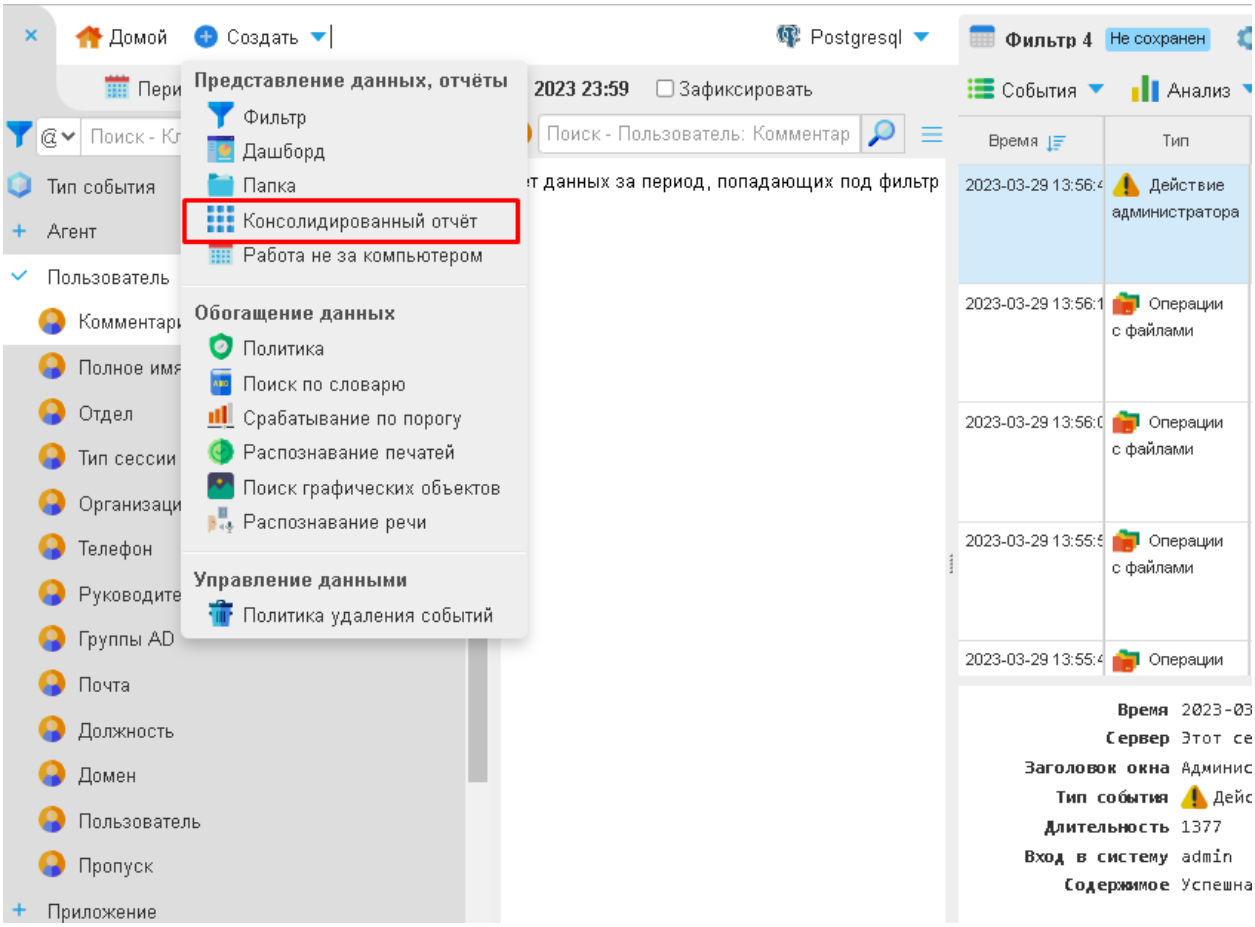
Название отчёта	
Сводная статистика	Ко
Статистика по дням	Количество принятых и с
Инвентаризация - устройства	
Инвентаризация - Приложения	
Лента событий	
Подробный отчёт по активности	
Детектор аномалий	
Ежедневные отчеты (zip-архивы)	

4.3.11 Консолидированный отчёт

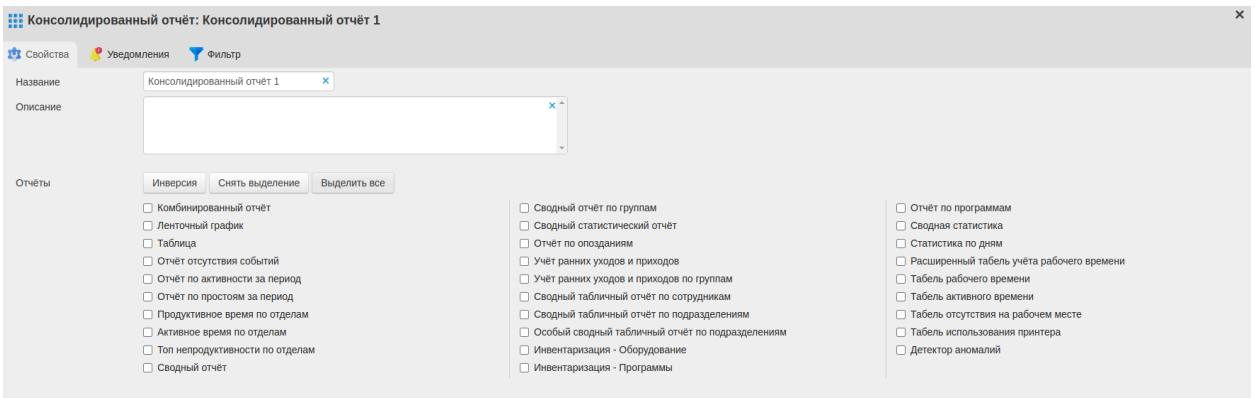
Содержит всю необходимую пользователю информацию за выбранный промежуток времени.

Создание и настройка

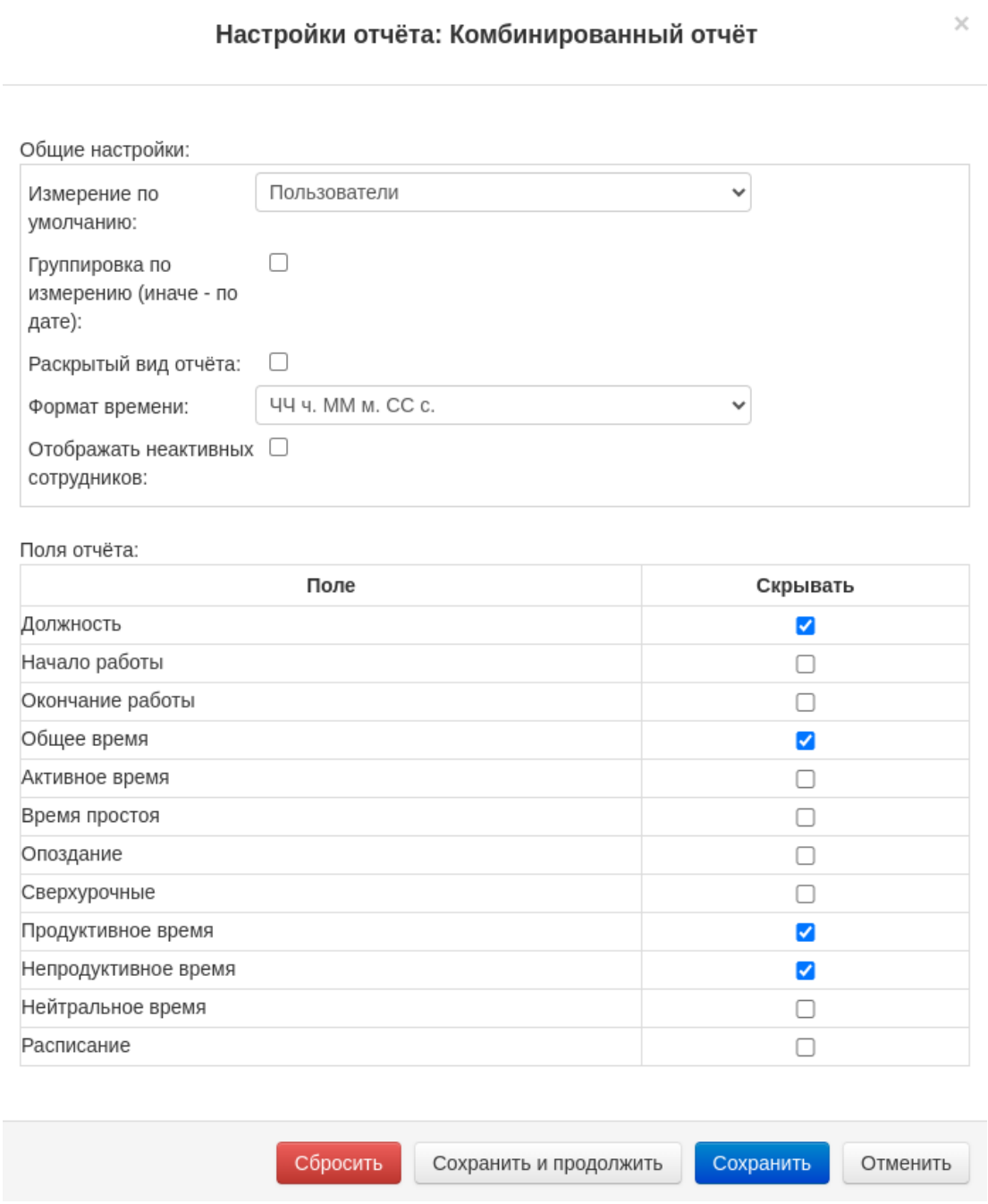
Чтобы создать новый консолидированный отчёт, в разделе **Создать** выберите **Консолидированный отчёт**.



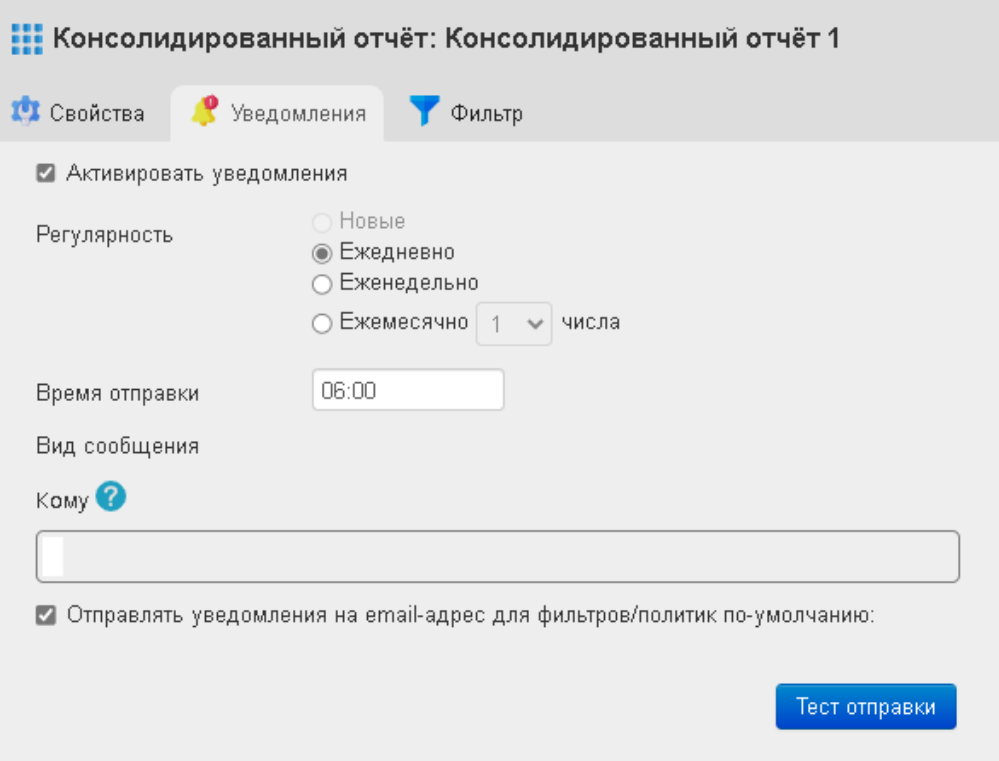
В открывшемся окне во вкладке **Свойства** выберите отчет.



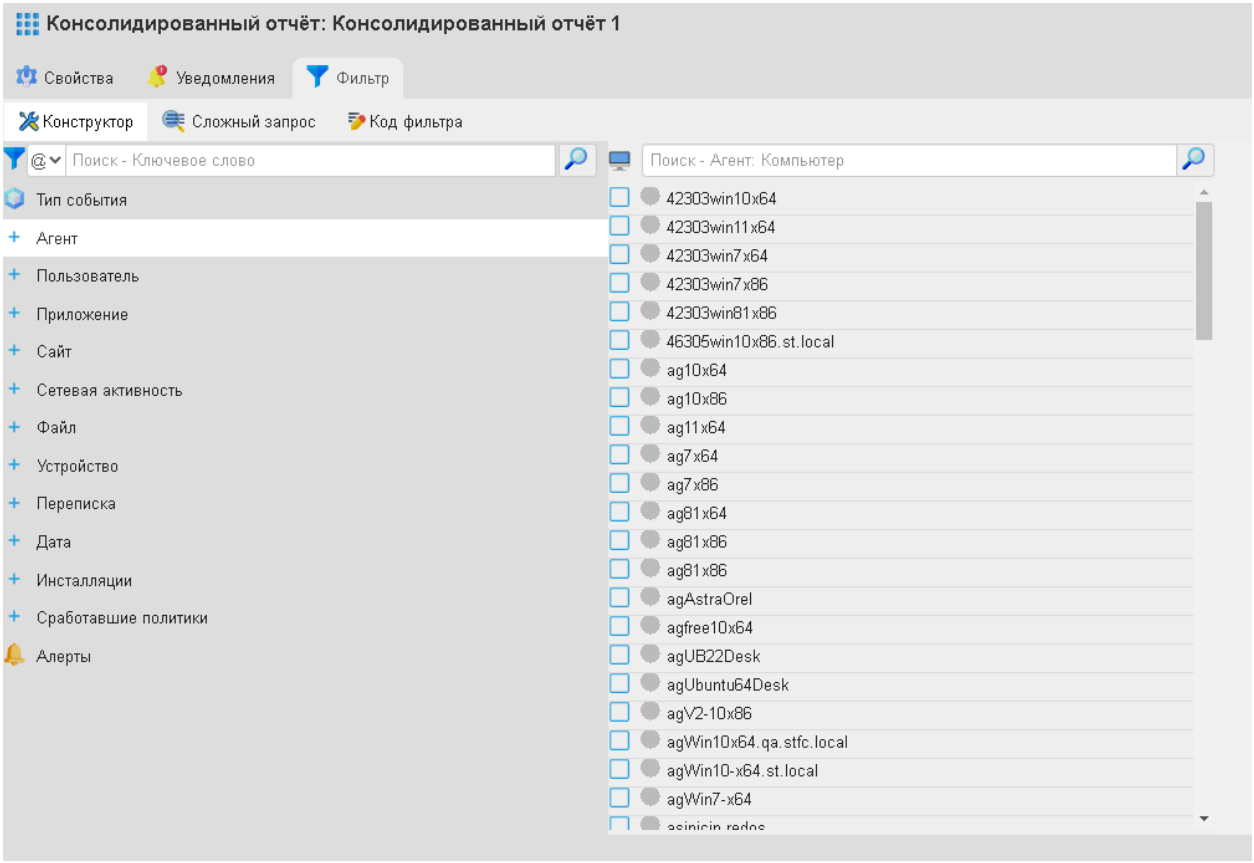
Откроется окно настройки отчета. Заполните **Общие настройки** и **Поля**. В отчете будет только указанная в полях информация. Например, отчет может содержать должность, общее время, продуктивное и непродуктивное время:



Во вкладке **Уведомления** поставьте флажок **Активировать уведомления** и задайте **Регулярность отправки**, а в поле **Кому** – адрес электронной почты, на который iBatyr Monitor будет отправлять отчёты.



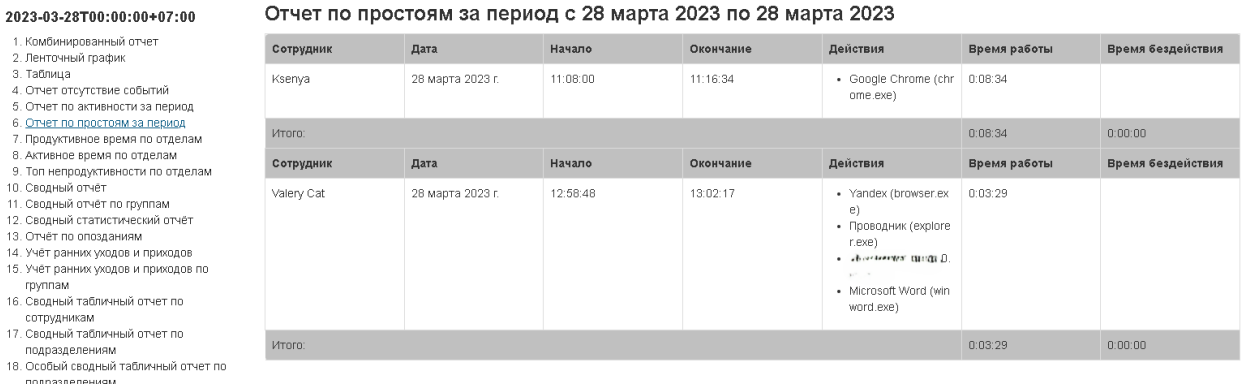
Во вкладке **Фильтр** в **Конструкторе** задайте точные параметры отчёта: конкретные агенты или пользователи, по которым будет формироваться отчёт и т. д.



Работа с отчётом

После получения отчёта по элеткронной почте:

1. Скачайте архив на компьютер.
2. Распакуйте его.
3. В папке с отчётом запустите файл **index.html**.
4. Выберите интересующие пункты.



2023-03-28T00:00:00+07:00

1. Комбинированный отчет
2. Ленточный график
3. Таблица
4. Отчет отсутствие событий
5. Отчет по активности за период
6. Отчет по простоям за период
7. Продуктивное время по отделам
8. Активное время по отделам
9. Топ непродуктивности по отделам
10. Сводный отчёт
11. Сводный отчёт по группам
12. Сводный статистический отчёт
13. Отчёт по опозданиям
14. Учёт ранних уходов и приходов
15. Учёт ранних уходов и приходов по группам
16. Сводный табличный отчет по сотрудникам
17. Сводный табличный отчет по подразделениям
18. Особый сводный табличный отчет по подразделениям

Отчет по простоям за период с 28 марта 2023 по 28 марта 2023

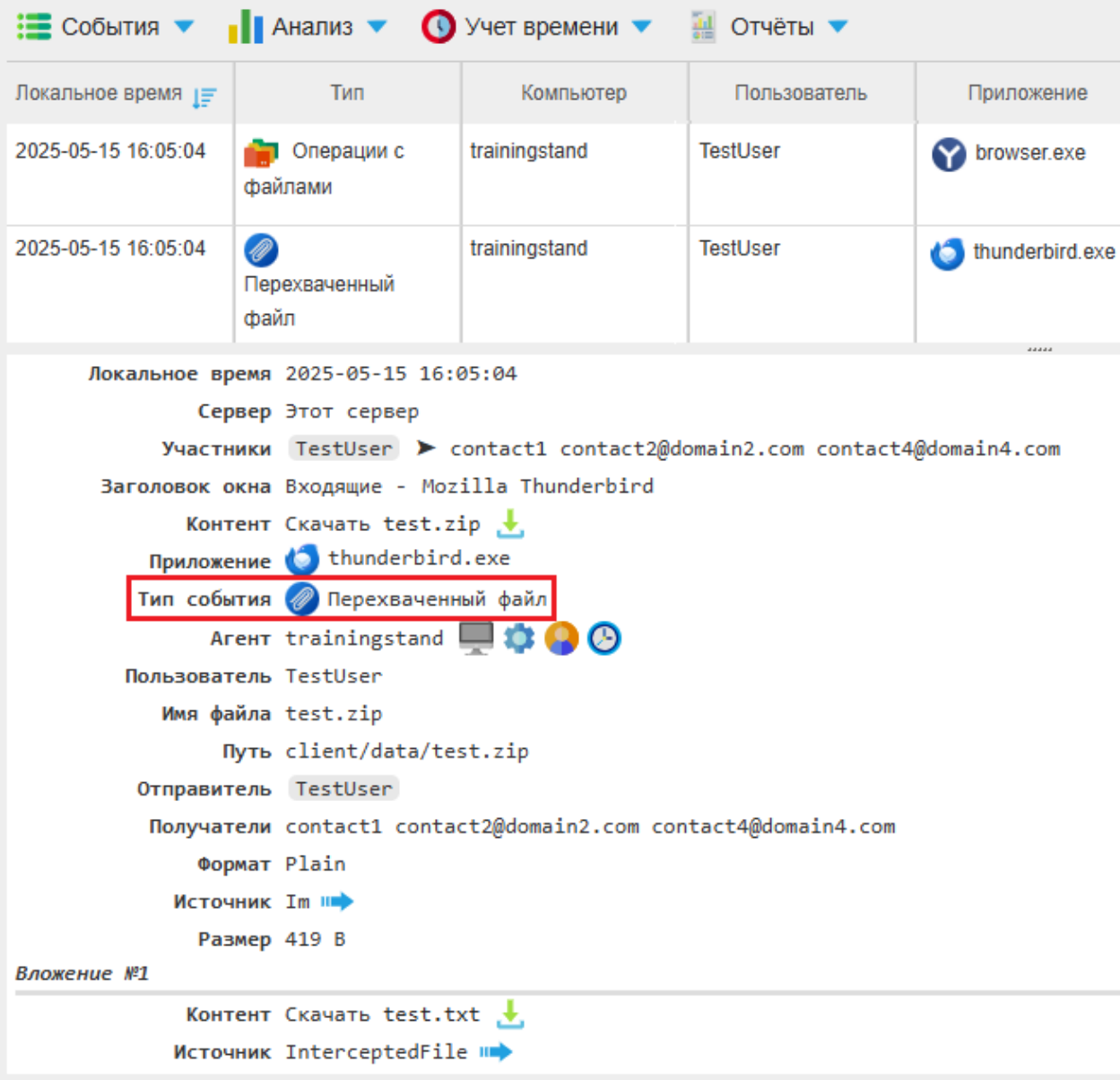
Сотрудник	Дата	Начало	Окончание	Действия	Время работы	Время бездействия
Ksenya	28 марта 2023 г.	11:08:00	11:16:34	• Google Chrome (chrome.exe)	0:08:34	
Итого:					0:08:34	0:00:00
Сотрудник	**Дата**	**Начало**	**Окончание**	**Действия**	**Время работы**	**Время бездействия**
Valery Cat	28 марта 2023 г.	12:58:48	13:02:17	• Yandex (browser.exe) • Проводник (explorer.exe) • [redacted] • Microsoft Word (winword.exe)	0:03:29	
Итого:					0:03:29	0:00:00

4.3.12 Типы событий

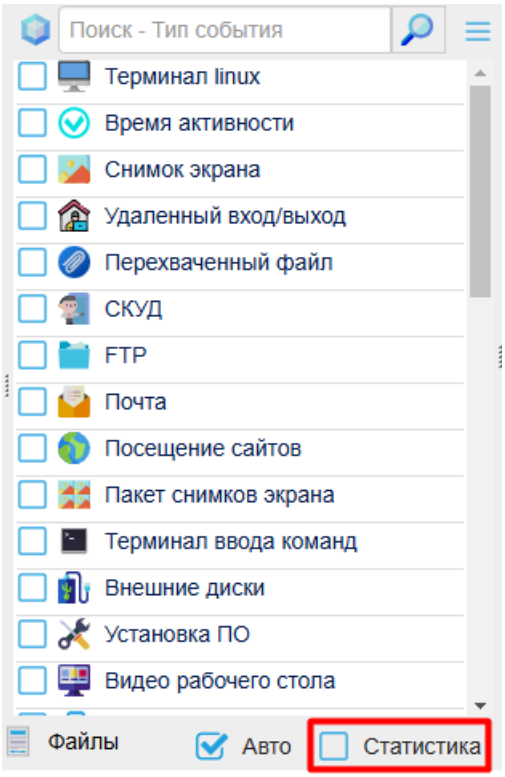
Содержание

- *Типы событий*
  - *Активность пользователя*
  - *Файлы*
  - *Записи и снимки активности*
  - *Интернет*
  - *Терминалы*
  - *Системные события*
  - *Отладочная информация*
  - *Оборудование, программное обеспечение и сеть*

У каждого события в iBatyr Monitor есть свой тип. Его можно узнать в **Линзе событий** и **Информации о событии**.



Для просмотра списка событий перейдите в **Конструктор** → **Типы событий** и отключите флаг **Статистика**.



Примечание: Чтобы система создавала события, включите соответствующий модуль или выполните другие действия для активации. Подробнее — ниже в описании событий.

Активность пользователя

Время активности

Период, в течение которого сотрудник взаимодействует с приложениями или веб-ресурсами. Система фиксирует активность при любых действиях мыши, клавиатуры или других устройств ввода.

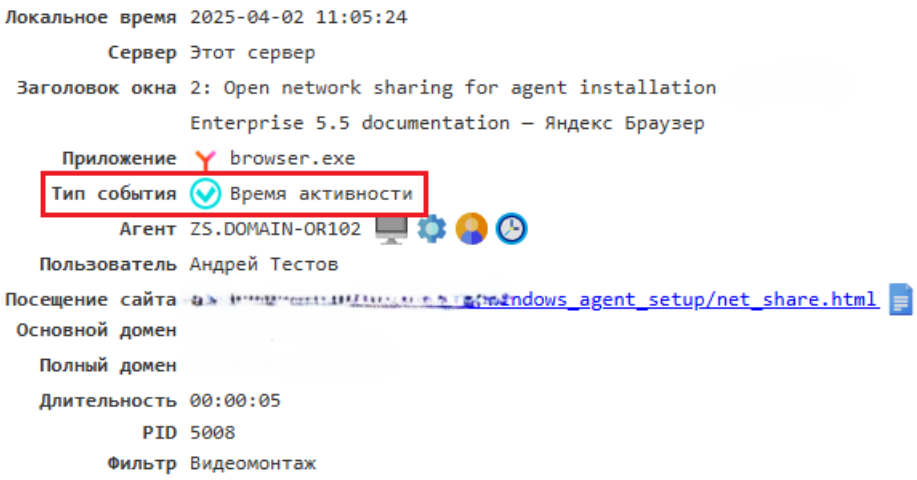
Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-02 11:05:29	Время активности	ZS.DOMAIN-OR102	Андрей Тестов	cmd.exe	Администратор: Командная строка - C:\Windows\SysWOW64\TimeControlSvc\uninstall.cmd
2025-04-02 11:05:24	Время активности	ZS.DOMAIN-OR102	Андрей Тестов	browser.exe	2: Open network sharing for agent installation — Staffcop Enterprise 5.5 documentation — Яндекс Браузер

См.также:

Как система расчитывает время активности

Для активации включите модули:

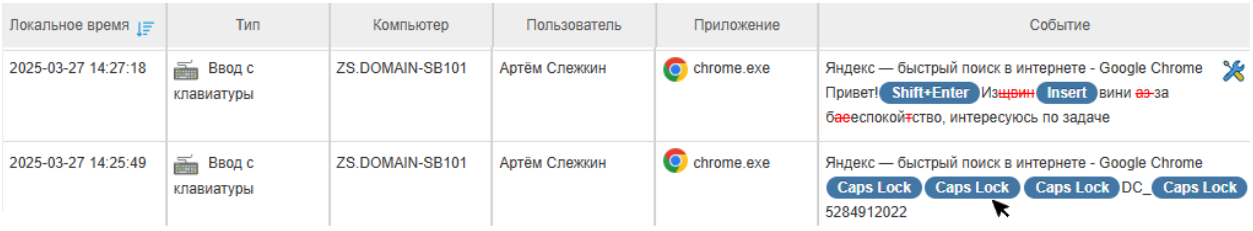
- *Контроль программ* → *Запуск приложений*,
- *Учет активности* → *Активность приложений*.



Ввод с клавиатуры

Отображает нажатия клавиш и их сочетаний в различных приложениях, перхватывает пароли при логине в Windows.

Наведите курсор на перехваченный текст, чтобы увидеть нажатые клавиши, например, Caps Lock или Alt. Если пользователь удалял напечатанное, удаленные символы будут зачеркнуты.



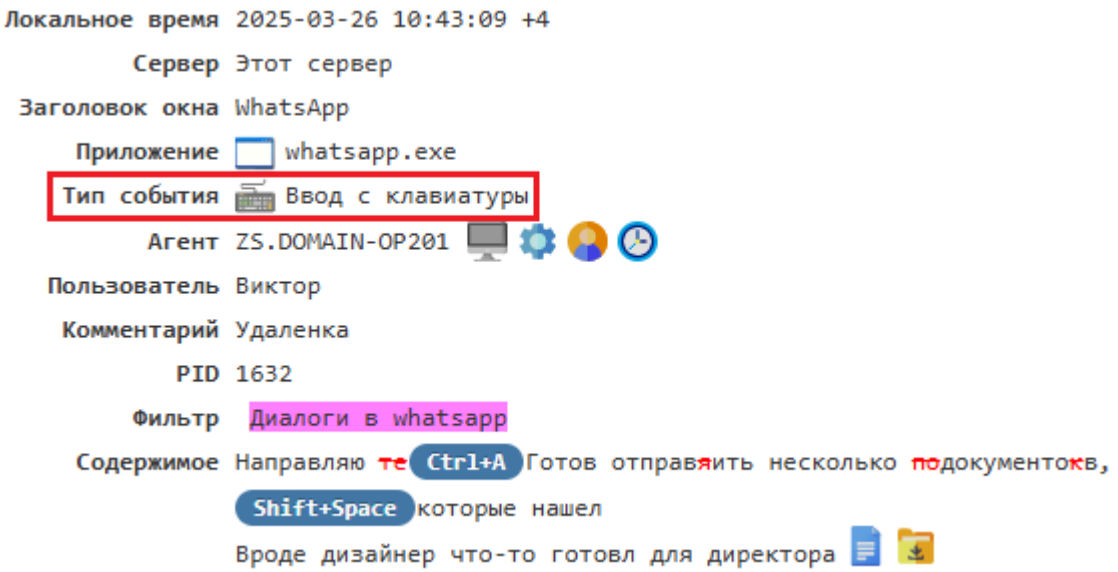
Примечание: Перехваченные пароли при логине в Windows можно посмотреть в **Сработавшие политики → Пароль пользователя**.

Для активации включите опции **Ввод с клавиатуры** и **Низкоуровневый кейлоггер** в модуле *Клавиатура и буфер обмена*.

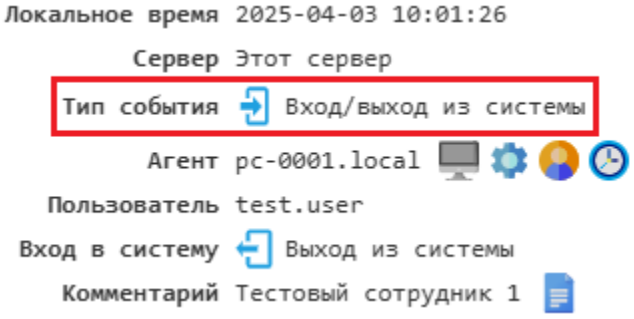
Вход/выход из системы

Перехват входа и выхода пользователей.

Для активации включите *Мониторинг пользователей → Вход в систему*.



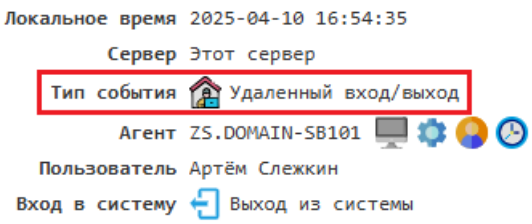
Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-03 10:01:26	Вход/выход из системы	pc-0001.local	test.user		Выход из системы
2025-04-04 10:03:43	Вход/выход из системы	pc-0001.local	test.user		Вход в систему
2025-04-09 15:25:45	Вход/выход из системы	pc-0001.local	test.user		Сессия заблокирована
2025-04-07 14:11:11	Вход/выход из системы	pc-0001.local	test.user		Сессия разблокирована



Удаленный вход/выход

Данные об удаленных входе и выходе в Windows.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-07 17:31:22	Удаленный вход/выход	ZS.DOMAIN-SB101	Артём Слежкин		Вход в систему
2025-04-07 10:48:19 +4	Удаленный вход/выход	ZS.DOMAIN-OP201	Виктор		Выход из системы
2025-04-07 10:40:02 +4	Удаленный вход/выход	ZS.DOMAIN-OP201	Виктор		Сессия разблокирована



Для активации включите *Мониторинг пользователей → Вход в систему*.

Запуск приложения

Информация о запуске приложений:

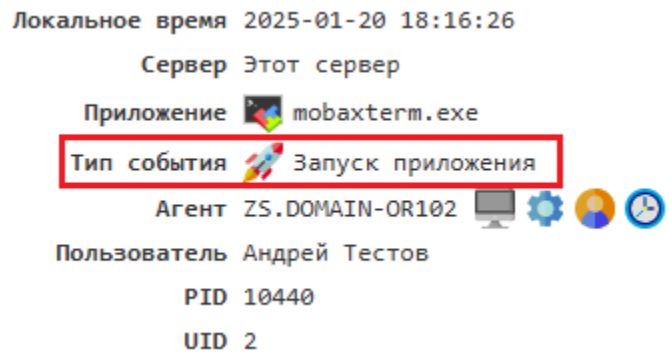
Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-01-20 18:16:28	Запуск приложения	ZS.DOMAIN-OR102	Андрей Тестов	xwin_mobax.exe	
2025-01-20 18:16:26	Запуск приложения	ZS.DOMAIN-OR102	Андрей Тестов	mobaxterm.exe	
2025-01-20 18:16:26	Запуск приложения	ZS.DOMAIN-OR102	Андрей Тестов	smartscreen.exe	

Для активации **Запуска приложений** *внесите изменения в /etc/ibatyr/config* и включите *Контроль программ → Запуск приложений*.

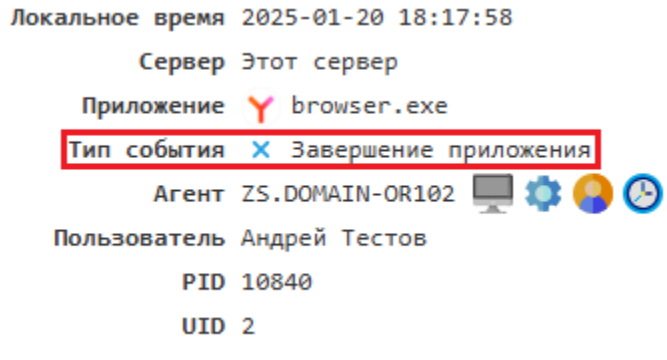
Завершение приложения

Информация о завершении работы приложения.

Для активации *внесите изменения в /etc/ibatyr/config* и включите *Контроль программ → Запуск приложений*.



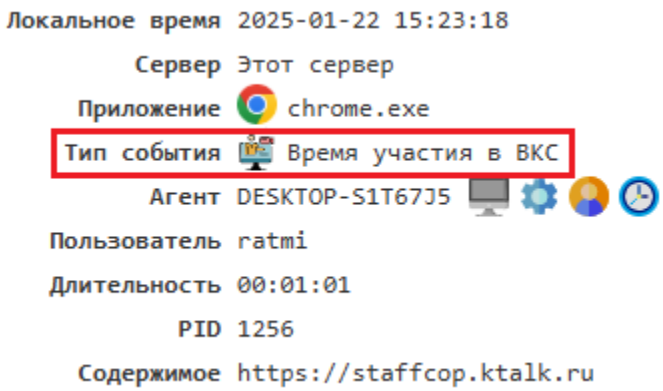
Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-01-20 18:17:58	Завершение приложения	ZS.DOMAIN-OR102	Андрей Тестов	browser.exe	
2025-01-20 18:17:48	Завершение приложения	ZS.DOMAIN-OR102	Андрей Тестов	steam.exe	
2025-01-20 18:17:48	Завершение приложения	ZS.DOMAIN-OR102	Андрей Тестов	steamwebhelper.exe	



Время участия в ВКС

Содержит время участия пользователя в видеоконференциях.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-01-22 11:26:19	Время участия в ВКС	ZS.DOMAIN-OP201	Виктор	chrome.exe	https://app.zoom.us
2025-01-22 15:26:18	Время участия в ВКС	DESKTOP-S1T67J5	ratmi	chrome.exe	



Для активации включите *Контроль ВКС — Контроль участия в ВКС*.

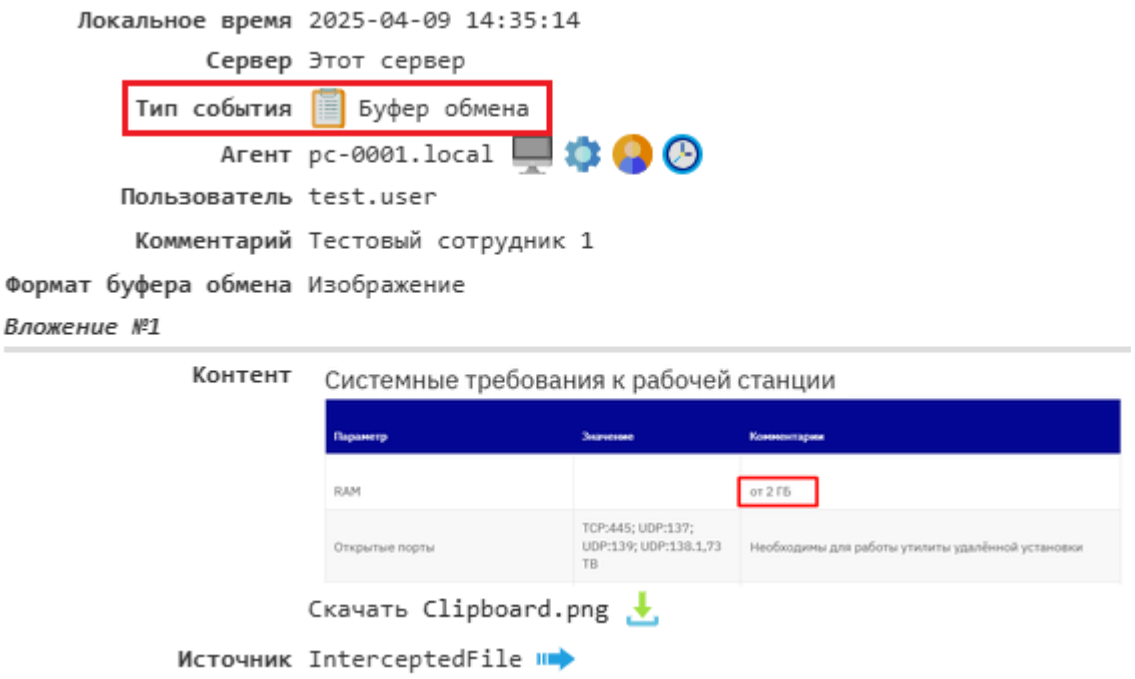
Буфер обмена

Скопированные текст и изображения из буфера обмена.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-09 14:35:46	Буфер обмена	pc-001.local	test.user	browser.exe	Рекомендуемые системные требования: Операционная система: Ubuntu 18.04 и выше. Процессор: Intel или AMD с поддержкой AVX инструк...
2025-04-09 14:35:18	Буфер обмена	pc-0001.local	test.user	browser.exe	https://www.staffcop.ru/enterprise/sistemnye-trebovaniya
2025-04-09 14:35:14	Буфер обмена	pc-0001.local	test.user		Clipboard.png Системные требования к рабочей станции Скачать Clipboard.png Clipboard

Для активации включите *Клавиатура и буфер обмена → Буфер обмена*.

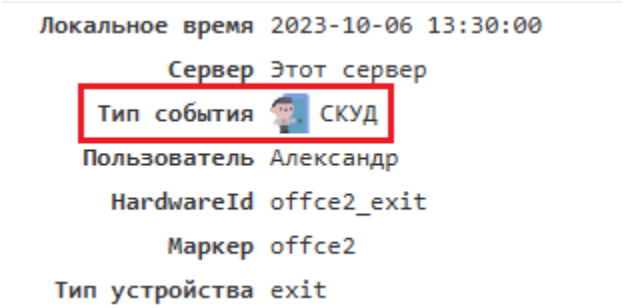
Чтобы перехватывать скриншоты, сделанные с помощью клавиши Print Screen, включите в модуле **Файлы** опцию *Теневое копирование*.



СКУД

Вывод событий из системы СКУД.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2023-10-06 13:30:00	СКУД		Александр		exit



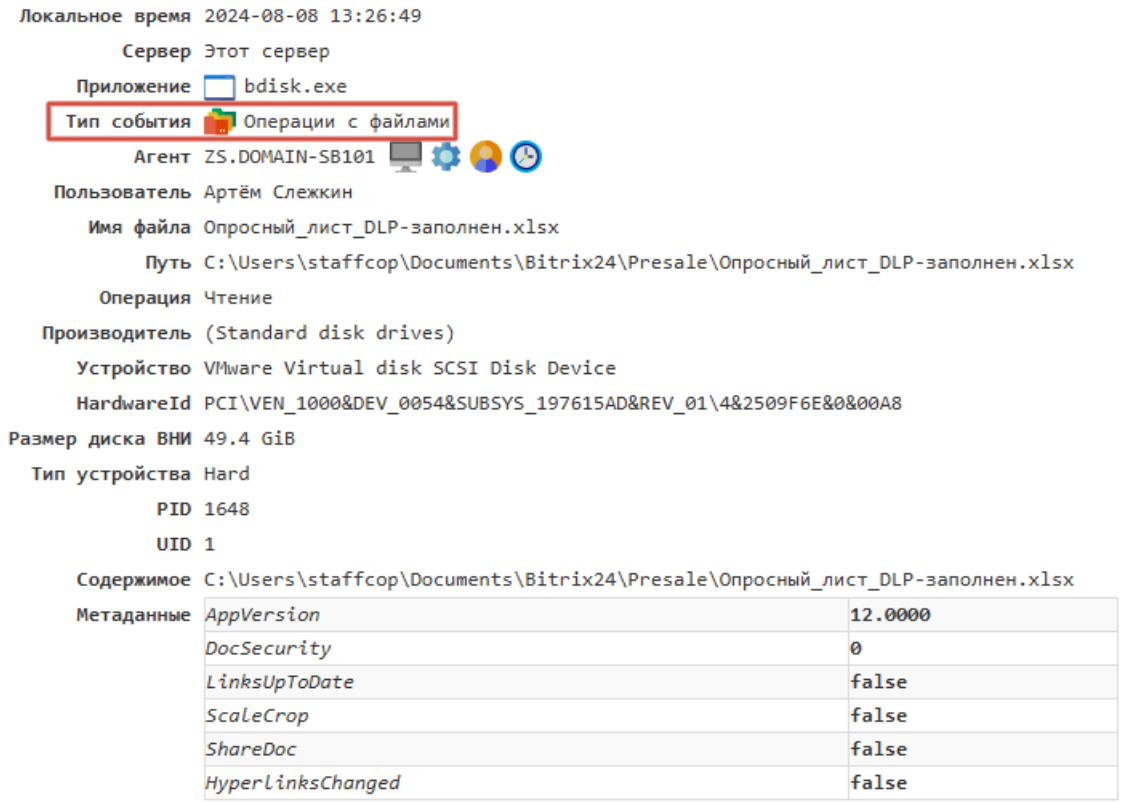
Для вывода событий **СКУД** импортируйте *данные из СКУД-системы*.

Файлы

Операции с файлами

Файловые операции, которые совершают приложения: файловые менеджеры, браузеры, другие ПО.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-01 12:05:54	Операции с файлами	ZS.DOMAIN-SB101	Артём Слежкин	installerui-ru.exe	C:\Users\staffcop\Do.. ..ebug_InstallerUI.log Запись Debug_InstallerUI.log Hard VMware Virtual disk SCSI Disk Device



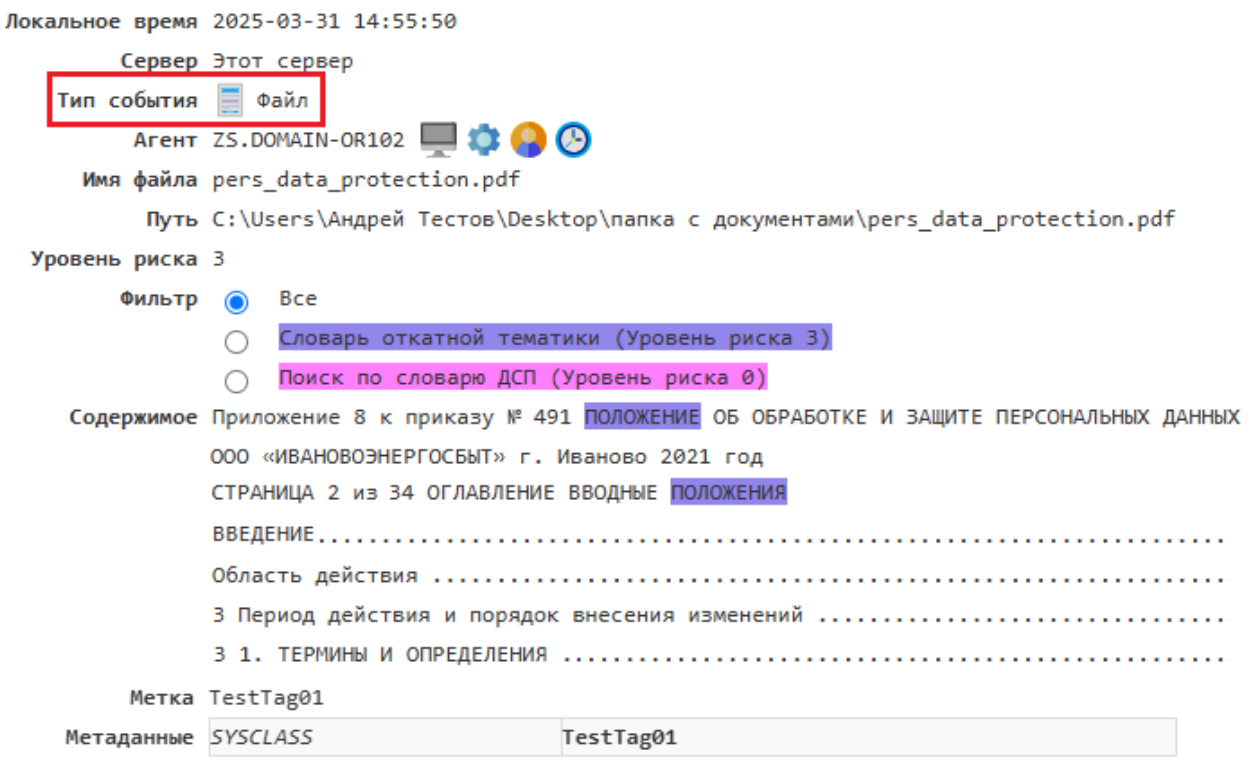
Для активации события включите *Файлы — Файловая активность*.

Файл

Файлы, которые были получены в результате работы **Файлового сканера** или **Краулера**.

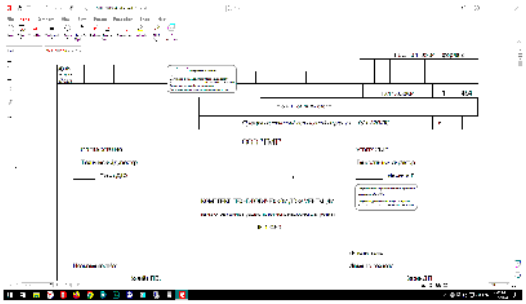
Для активации включите и настройте *Файловый сканер → Сканер файлов* или *Краулер*.

Локальное время	Тип	Компьютер	Пользователь	Путь	Событие
2025-04-04 05:30:5	Файл	ZS.DOMAIN-OP201		C:\Users\Виктор\AppData\Local\Google\DriveFS\116872384366191051705\content_cache\d5\	Федор Достоевский Хоть убей, следа не видно,Сбились мы, что делать нам?В поле бес нас водит, видно,Да кружит по сторонам.Сколько... Словарь откатной тематики 1010 Метка
2025-03-31 14:55:5	Файл	ZS.DOMAIN-OR102		C:\Users\Андрей Тестов\Desktop\папка с документами\Приказ.pdf	Приказ.pdf
2025-03-31 14:55:5	Файл	ZS.DOMAIN-OR102		C:\Users\Андрей Тестов\Desktop\папка с документами\паспорт.pdf	паспорт.pdf
2025-03-31 14:55:5	Файл	ZS.DOMAIN-OR102		C:\Users\Андрей Тестов\Desktop\папка с документами\pers_data_protection.pdf	Приложение 8 к приказу № 491 ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ Поиск по словарю ДСП pers_data_protection.pdf



Печать документов

Распечатанные документы.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2024-11-25 15:06:47	Печать документов	DESKTOP-OV4O6V5	Support	foxitpdfreader.exe	Microsoft Print to PDF Microsoft Print to PDF | 5769.Г.01100.00034.pdf 5769.г.01100.00034.pdf Скачать 5769.г.01100.00034.pdf PrintDoc 00002.zip Скачать 00002.zip PrintDoc Screenshot.png  Скачать Screenshot.png PrintDoc

Для активации включите *Принтеры → Печать на принтерах*.

Записи и снимки активности

Снимок экрана

Снимки экрана пользователя, которые сделал агент.

Примечание: Снимки экрана, которые сделал сам пользователь, хранятся в событиях *Буфер обмена*.

Активировать событие, настроить частоту и качество снимков можно в модуле *Снимки экрана*.

Пакеты снимков экрана

Набор снимков экрана пользователя, которые можно просматривать в слайд-шоу. Пакеты снимков занимают гораздо меньше места, чем отдельные снимки экрана или видео.

Примечание: *Подробнее о анализе пакетов снимков экрана*

Для создания пакетов снимков экрана включите и настройте *Пакеты снимков экрана*.

Локальное время 2024-11-25 15:06:47
Сервер Этот сервер
Заголовок окна Microsoft Print to PDF
Приложение foxitpdfreader.exe
Тип события Печать документов
Агент DESKTOP-OV4O6V5
Пользователь Support
Страниц 16
Содержимое Microsoft Print to PDF | 5769.Г.01100.00034.pdf

Вложение №1

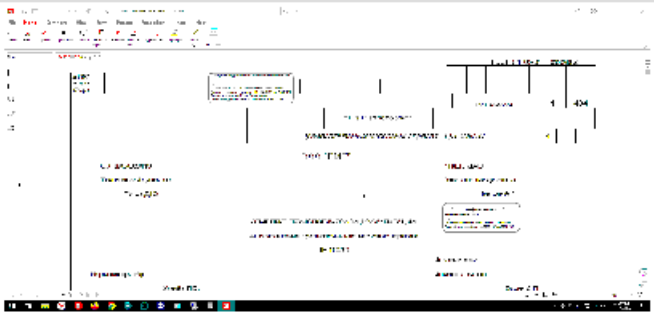
Контент Скачать 5769.г.01100.00034.pdf
Источник InterceptedFile

Вложение №2

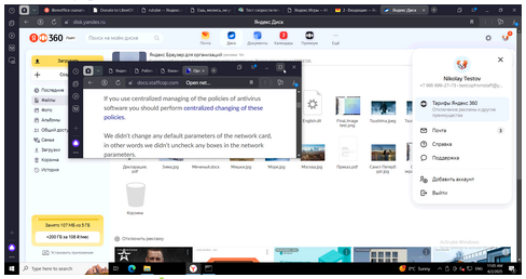
Контент Скачать 00002.zip
Источник InterceptedFile

Вложение №3

Контент



Скачать Screenshot.png
Источник InterceptedFile

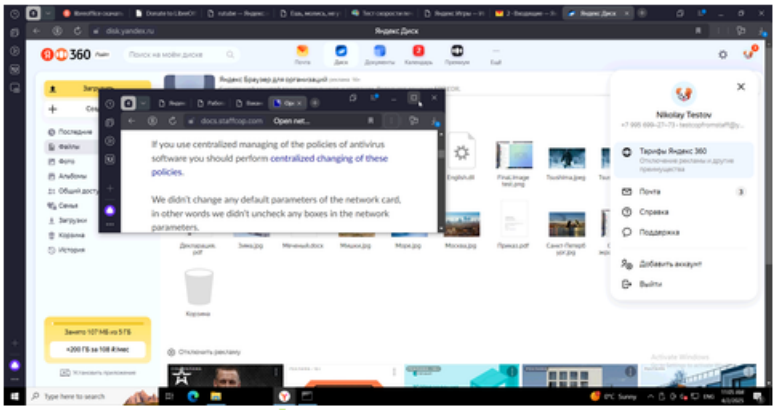
Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-02 11:05:24	Снимок экрана	ZS.DOMAIN-OR102	Андрей Тестов	browser.exe	2: Open network sharing for agent installation — Staffcop Enterprise 5.5 documentation — Яндекс Браузер Screenshot.png  Скачать Screenshot.png

Локальное время 2025-04-02 11:05:24

Сервер Этот сервер

Заголовок окна 2: Open network sharing for agent installation — Staffcop Enterprise 5.5 documentation — Яндекс Браузер

Контент



Скачать Screenshot.png

Приложение browser.exe

Тип события Снимок экрана

Агент ZS.DOMAIN-OR102

Пользователь Андрей Тестов

Имя файла Screenshot.png

Путь Screenshot.png

Посещение сайта https://docs.staffcop.com/windows_agent_setup/net_share.html

Основной домен staffcop.com

Полный домен docs.staffcop.com

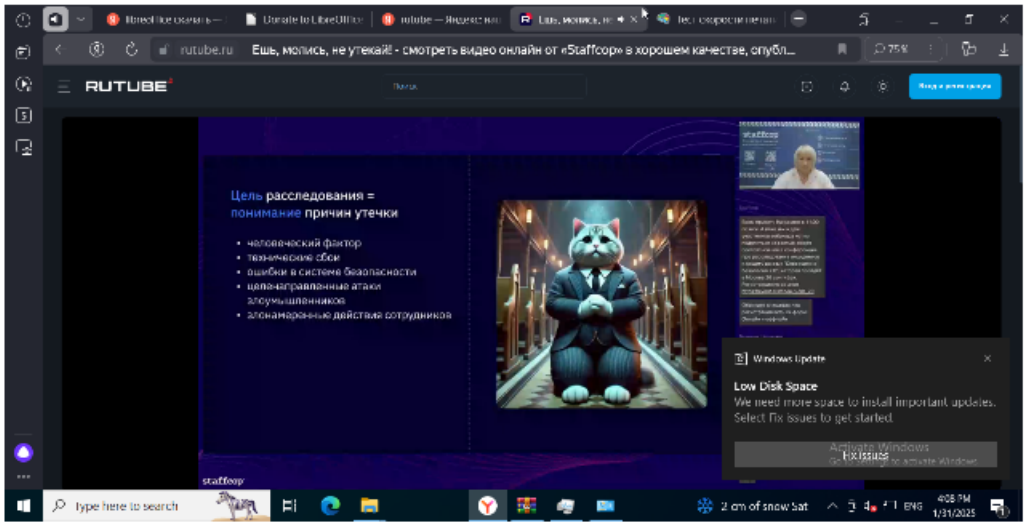
PID 5008

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-03-06 09:26:46 +4	Пакет снимков экрана	ZS.DOMAIN-OP201	Виктор		ScreenshotPack.scrpack Скачать ScreenshotPack.scrpack
2025-01-31 16:12:35	Пакет снимков экрана	ZS.DOMAIN-OR102	Андрей		ScreenshotPack.scrpack Скачать ScreenshotPack.scrpack

Локальное время 2025-01-31 16:08:34

Сервер Этот сервер

Контент



1.2 Mb x1 16:08:36 (3/120)

Тип события Пакет снимков экрана

Агент ZS.DOMAIN-OR102

Пользователь Андрей Тестов

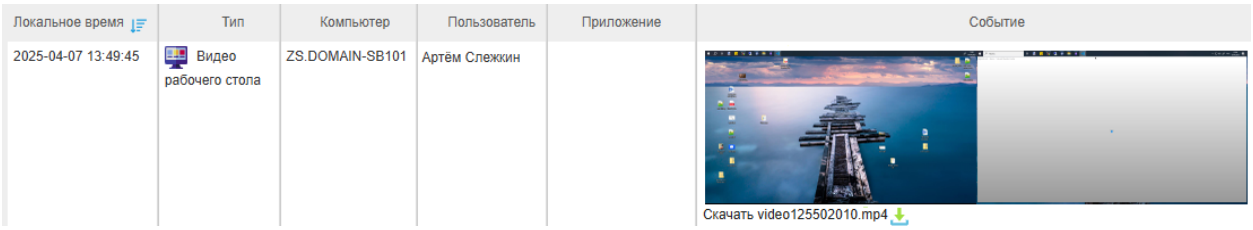
Имя файла ScreenshotPack.scrpack

Путь ScreenshotPack.scrpack

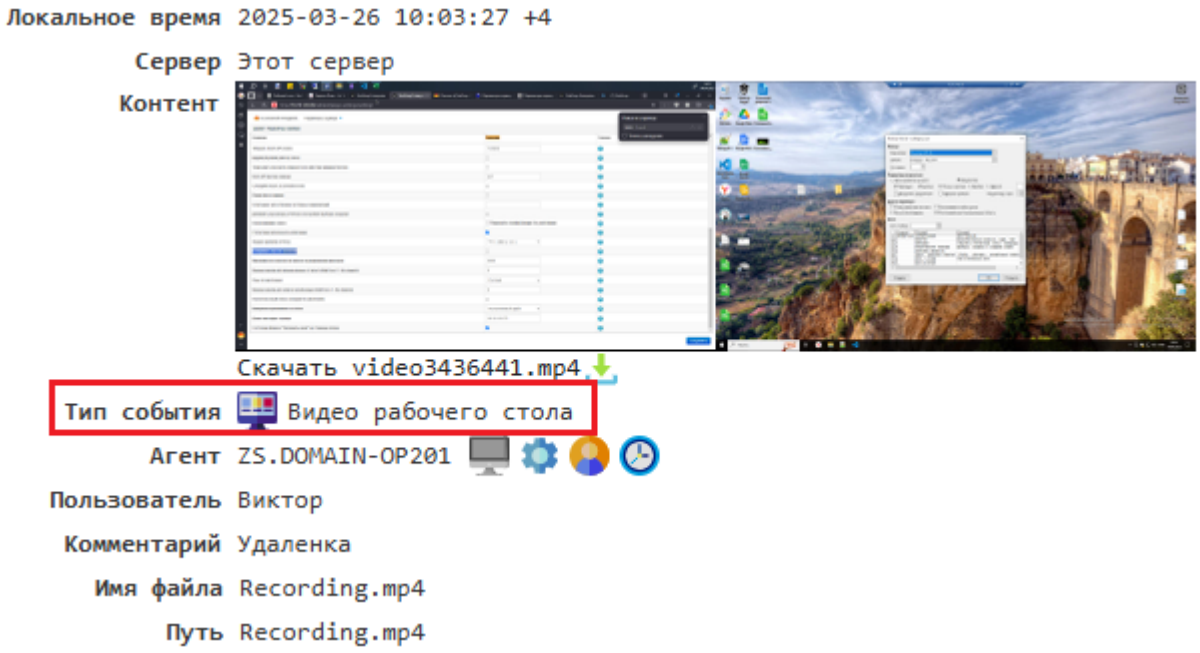
Длительность 00:02:00

Видео рабочего стола

Видеозапись экрана пользователя.



Примечание: Нажмите на превью видео, чтобы открыть проигрыватель и посмотреть запись.



Для записи видео на компьютерах пользователей включите **Онлайн видео рабочего стола** или **Офлайн запись видео рабочего стола** в разделе *Запись видео экрана*.

Интернет

Посещение сайтов

Сайты, которые посещал пользователь.

Примечание: Информация о посещении сайта хранится и в событиях другого типа, например, **Время активности** или **Снимок экрана**.

Для активации включите *Сетевые подключения — Мониторинг сети* и *Интернет — Веб-трафик*.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-03-13 11:50:28	Посещение сайтов	ZS.DOMAIN-OP201	Виктор	msedge.exe	https://web.whatsapp.com/ajax/whatsapp_error_reports/?device_level=unknown
2025-03-11 11:50:41	Посещение сайтов	ZS.DOMAIN-OR101	red	browser.exe	Лента новостей https://login.vk.com/?act=migrate_cookies&from;=aHR0cHM6Ly92ay5jb20vaW5kZXgucGhw&hash;=1741683031_94db2423ccc2ab392e072e4c8ef8ceb81fc6d4e7e7972300e68a9a24a63b5014&i;=5KzysU8PsGh_VC9c3Jqi8LIoMplyEVEk7stf584xRBIxuvP3sE4Ezfch-C-HQDj5yBTDiszXbeOFZvj-N2nefFlc68TUHeoe4mjrVqeUuCXADzAOkf6_BOEria8NXgZ8

Локальное время 2025-03-06 08:43:07 +4
Сервер Этот сервер
Приложение msedge.exe
Тип события Посещение сайтов
Агент ZS.DOMAIN-OP201
Пользователь Виктор
Посещение сайта https://crashlogs.whatsapp.net/wa_clb_data
Основной домен whatsapp.net
Полный домен crashlogs.whatsapp.net
Длительность 1 мс
Комментарий Удаленка
PID 7616
Содержимое https://crashlogs.whatsapp.net/wa_clb_data

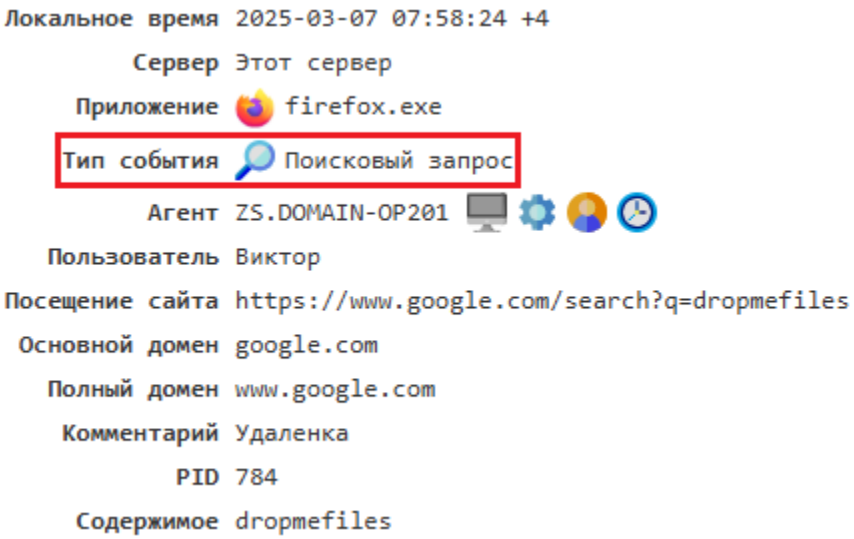
Вложение №1

Контент Скачать logs.txt
Источник InterceptedFile

Поисковый запрос

Поисковые запросы пользователей в популярных поисковиках.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-03-17 18:38:43	Поисковый запрос	ZS.DOMAIN-OR102	Андрей Тестов	browser.exe	смайлик клоуна
2025-03-13 11:50:30 +4	Поисковый запрос	ZS.DOMAIN-OP201	Виктор	msedge.exe	временные облачные хранилища на 24 час
2025-03-07 07:54:52 +4	Поисковый запрос	ZS.DOMAIN-OP201	Виктор	opera.exe	dropmefiles
2025-03-07 07:43:56 +4	Поисковый запрос	ZS.DOMAIN-OP201	Виктор	firefox.exe	dropbox
2025-03-07 07:17:48 +4	Поисковый запрос	ZS.DOMAIN-OP201	Виктор	chrome.exe	mediafire



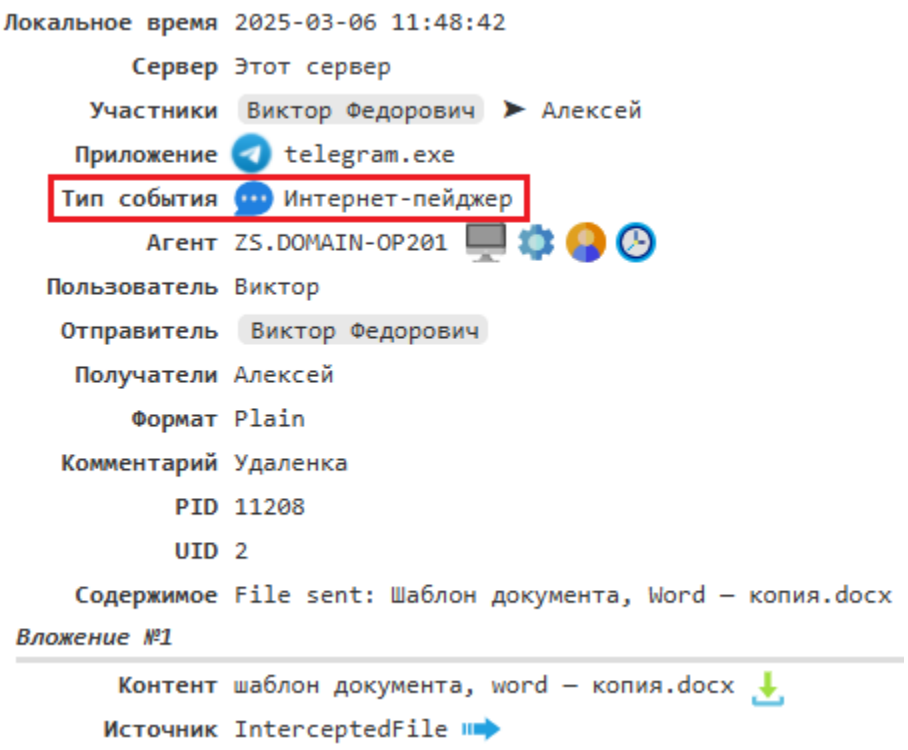
Для активации включите *Интернет* → *Поисковые запросы*.

Интернет-пейджер

Перехват событий в мессенджерах.

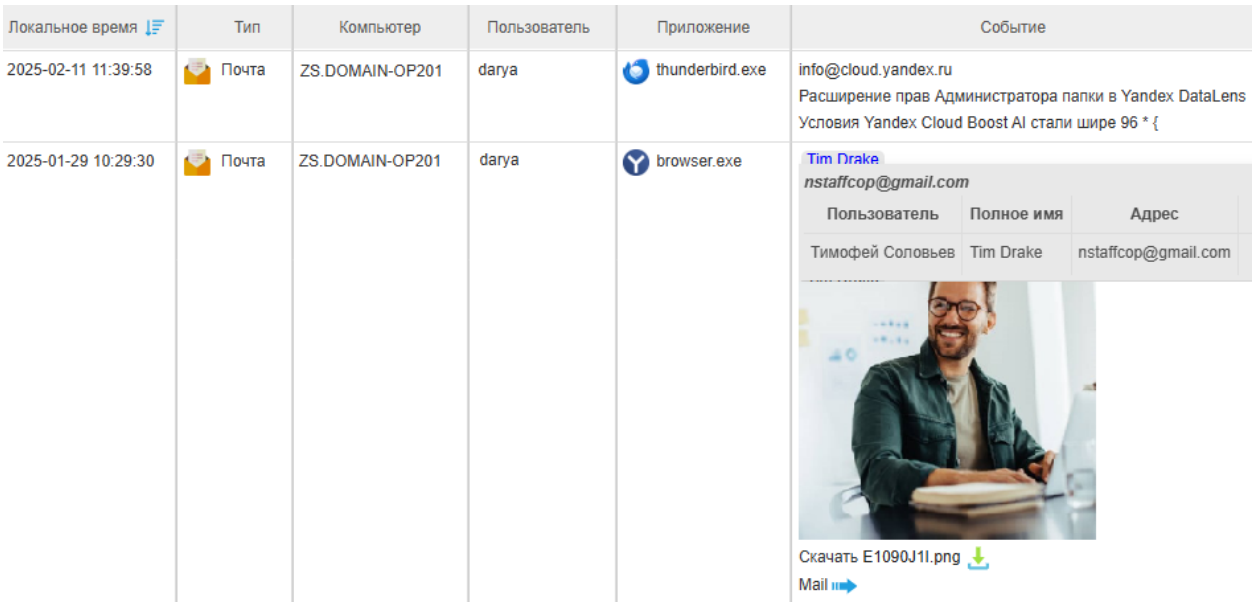
Для перехвата переписки включите *Сетевые подключения — Мониторинг сети* и *Почта и мессенджеры — Интернет-пейджеры*. Для перехвата Telegram или WhatsApp — *дополнительные опции перехвата*.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-03-06 09:04:08	Интернет-пейджер	ZS.DOMAIN-OP201	Виктор	chrome.exe	Виктор Федорович Шаблон документа, Word.docx
2025-03-04 10:48:14	Интернет-пейджер	ZS.DOMAIN-OP201	Виктор	telegram.exe	Я Мегафон Ну вы конечно и да, все как на подбор.
2025-02-20 09:22:26	Интернет-пейджер	ZS.DOMAIN-OP201	Виктор	telegram.exe	Виктор Федорович Peer chat with Артём File sent: 9fe24a04-5504-4d20-9a9f-81a2fa356e45.jpg
2025-02-20 09:22:05	Интернет-пейджер	ZS.DOMAIN-OP201	Виктор	telegram.exe	Виктор Федорович Peer chat with Артём File sent: pers_data_protection.pdf
2025-02-20 09:21:37	Интернет-пейджер	ZS.DOMAIN-OP201	Виктор	chrome.exe	Виктор Федорович 9fe24a04-5504-4d20-9a9f-81a2fa356e45.jpg



Почта

Почтовая переписка. События формируются при перехвате электронной почты или с помощью *Сборщика почты*.



Примечание: Наведите курсор на имя отправителя, чтобы увидеть данные из его *Карточки пользователя*.

Для перехвата почтовой переписки включите *Сетевые подключения — Мониторинг сети* и активируйте почтовые модули в разделе *Почта и мессенджеры*.

Данные формы

Данные форм, которые были перехвачены в браузере.

Примечание: Событие **Данные формы** перехватывает пароли в браузере. Перехваченные пароли можно посмотреть в **Сработавшие политики** → **Пароль в браузере**.

Для активации события включите опции **Веб-трафик** и **Перехват веб-форм** в разделе *Интернет*.

Инцидент K.ID

Информация о входе через Контур.ID.

Для активации входа через Контур.ID настройте *Отслеживание входа в Контур.ID*.

Локальное время 2025-02-28 06:57:07 +4
Сервер Этот сервер
Участники Виктор Федорович ➤ testmail.1996@mail.ru
Заголовок окна Проект - #61305
Приложение chrome.exe
Тип события Почта
Агент ZS.DOMAIN-OP201
Пользователь Виктор
Отправитель Виктор Федорович
Получатели testmail.1996@mail.ru
Формат Plain
Комментарий Удаленка
PID 2760
Фильтр ◉ Все
○ Рег. Номер телефона
○ Рег. e-mail
Содержимое Акционерное общество «Тестовая Организация» (АО «Тестовая Организация»)
Выберите формат адресата вверху текущего блока или напечатайте его самостоятельно

Ул. Тестовая, д. 11, Москва, 123456
Телефон (888) 123-44-55, факс (495) 123-45-67
E-mail: info@testorg.ru
ОКПО 64609789, ОГРН 9876543212345 65
ИНН 123456789, КПП 987654321
На № 61305 от 28.02.2025

Вложение №1

Контент Скачать Образец_договора_найма_жилого_помещения-_заключаемого_между_физическими_лицами . docx.docx
Источник InterceptedFile

Вложение №2

Контент Скачать Образец_договора_аренды_квартиры_с_мебелью_и_бытовой_техникой . docx.docx
Источник InterceptedFile

Локальное время	Тип	Компьютер	Приложение	Событие
2025-02-28 17:51:58	Данные формы	pc-001.local	browser.exe	

os_password	123456789Pass!
login	Войти
os_username	user.test
os_destination	/pages/viewpage.action?pageId=47585142&preview=/4292728/

Пароль в браузере

Локальное время 2025-02-28 14:51:20
Сервер Этот сервер
Приложение browser.exe
Тип события Данные формы
Агент pc-0001.local
Пользователь user.test
Посещение сайта https://test.wiki.local/dologin.action
Основной домен test.wiki
Полный домен test.wiki.local
Длительность 1 мс
Комментарий Тестовый сотрудник 1
PID 8552
Фильтр Пароль в браузере
Содержимое

os_password	123456789Pass!
login	Войти
os_username	user.test
os_destination	/index.action

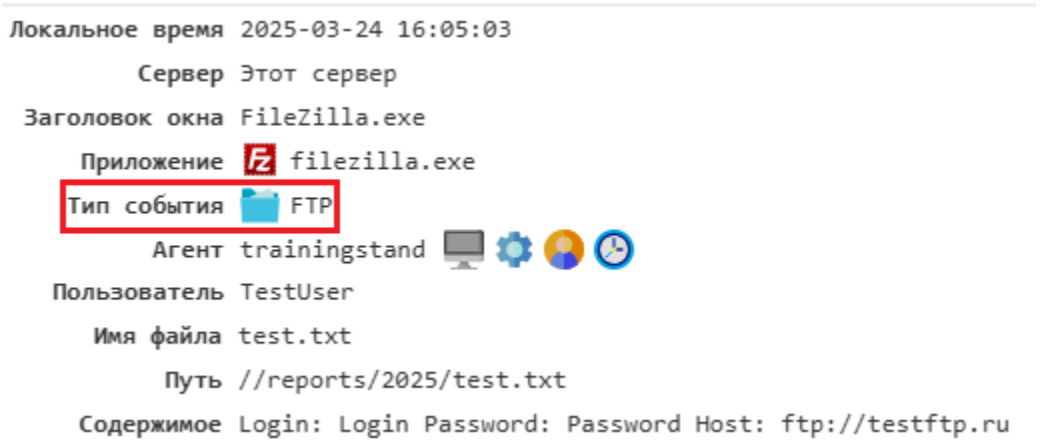
Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-03-02 17:25:46 +4	Инцидент K.ID	Kontur ID			Check2FAEvent Подтверждение второго фактора аутентификации, тип ресурса: SSH, тип FA: Push, Ip: 10.10.10.175, город: Екатеринбург
2025-03-02 17:25:35 +4	Инцидент K.ID	Kontur ID			EntryToResourceEvent Вход пользователя на ресурс, тип ресурса: SSH

Локальное время 2025-03-02 17:22:56 +4
Сервер Этот сервер
Заголовок окна Check2FAEvent
Тип события Инцидент K.ID
Агент Kontur ID
Содержимое Подтверждение второго фактора аутентификации, тип ресурса: SSH, тип FA: Push, Ip: 10.10.10.175, город: Екатеринбург

FTP

Информация о подключении к FTP-серверам.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-04 16:05:04	FTP	trainingstand	TestUser	filezilla.exe	FileZilla.exe Login: Login Password: Password Host: ftp://testftp.ru test.txt



Для активации включите *Файлы* → *FTP*.

Перехваченный файл

Теневые копии файлов, которые были перехвачены:

- при отправке по электронной почте через почтовые агенты и веб-почту;
- загрузке на USB-накопители;
- отправке через интернет-мессенджеры: QIP, ICQ, Skype, Агент Mail.ru и др.;
- печати на принтере;
- загрузке через браузер на Google Drive.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-03 13:24:30	Перехваченный файл	ZS.DOMAIN-SB101	Артём Слежкин	chrome.exe	Выгруженные через браузер файлы TsushimaGhost.jpeg Скачать TsushimaGhost.jpeg Web

Локальное время 2025-04-03 13:24:30
Сервер Этот сервер
Контент

Скачать TsushimaGhost.jpeg
Приложение chrome.exe
Тип события Перехваченный файл
Агент ZS.DOMAIN-SB101
Пользователь Артём
Имя файла TsushimaGhost.jpeg
Путь TsushimaGhost.jpeg
Уровень риска 1
Посещение сайта https://clients6.google.com/upload/drive/v2internal/batch?key=AIzaSyD_InbmS
Основной домен google.com
Полный домен clients6.google.com
Источник Web
Длительность 1 мс
PID 11980
Размер 126.1 Kb
Фильтр
- (•) Все
- ( ) Выгруженные через браузер файлы
- ( ) Утечка данных на облако GoogleDrive

Для перехвата файлов включите **Файловая активность**, **Теневое копирование** и другие опции в разделе *Файлы*.

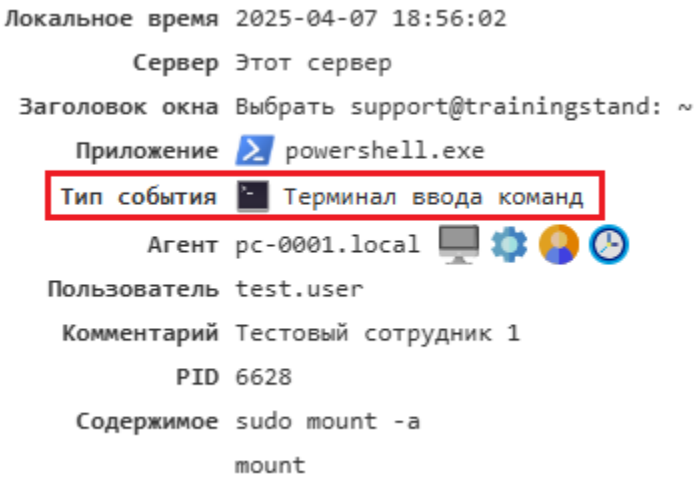
Терминалы

Терминал ввода команд

Данные ввода команд и результат выполнения в **CMD** и **PowerShell**.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2024-11-29 14:22:42	Терминал ввода команд	pc-0111.atom.local	test.user	cmd.exe	Командная строка C:\Users\test.user>ping 10.10.10.100 Обмен пакетами с 10.10.10.100 по с 32 байтами данных: Ответ от 10.10.10.100: число байт=32 время<1мс TTL=63 Ответ от 10.10.10.100: число байт=32 время<1мс TTL=63 Статистика Ping для 10.10.10.100: Пакетов: отправлено = 2, получено = 2, потеряно = 0 (0% потерь) Приблизительное время приема-передачи в мс: Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек Control-

Внимание: В Windows 11 вместо **CMD** и **Powershell** используется **Терминал Windows**, который iBatyr Monitor не перехватывает.

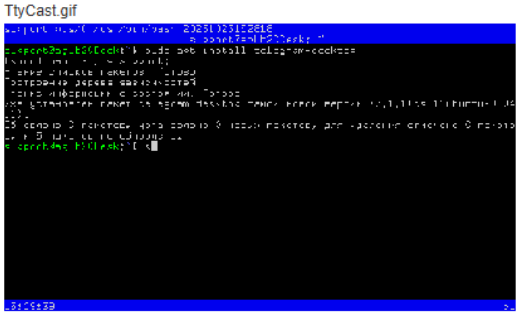


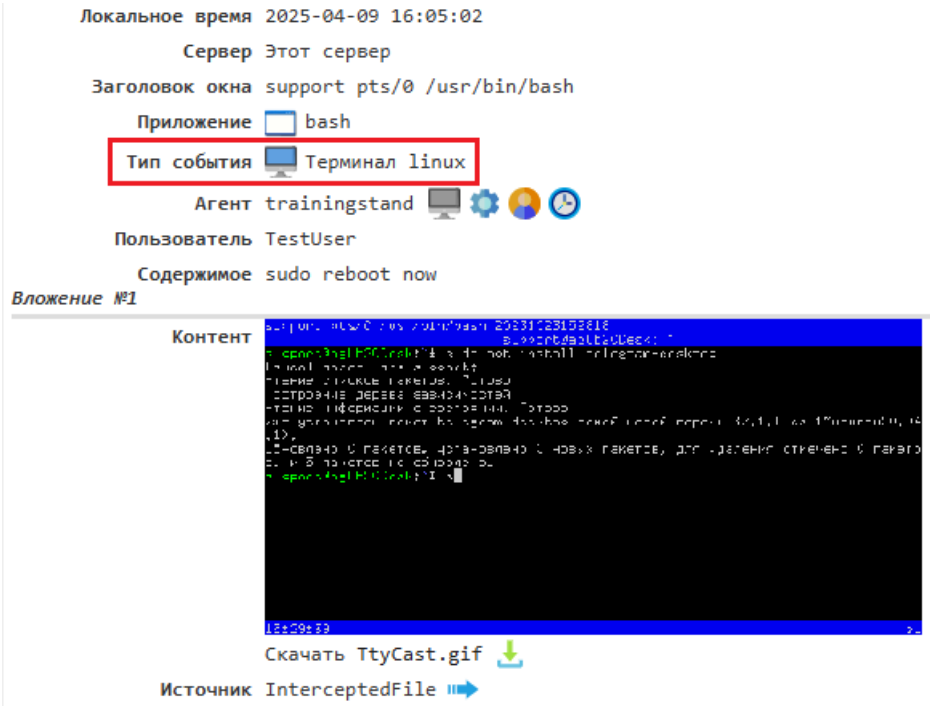
Для активации включите *Клавиатура и буфер обмена → Контроль ввода команд*.

Терминал Linux

Отображает данные, введенные в терминале в виде текста и gif:

Для активации включите *Мониторинг Linux → Перехват терминалов Linux (TTY)*.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-11 16:05:02	Терминал linux	trainingstand	TestUser	bash	support pts/0 /usr/bin/bash sudo reboot now TtyCast.gif  Скачать TtyCast.gif TTY



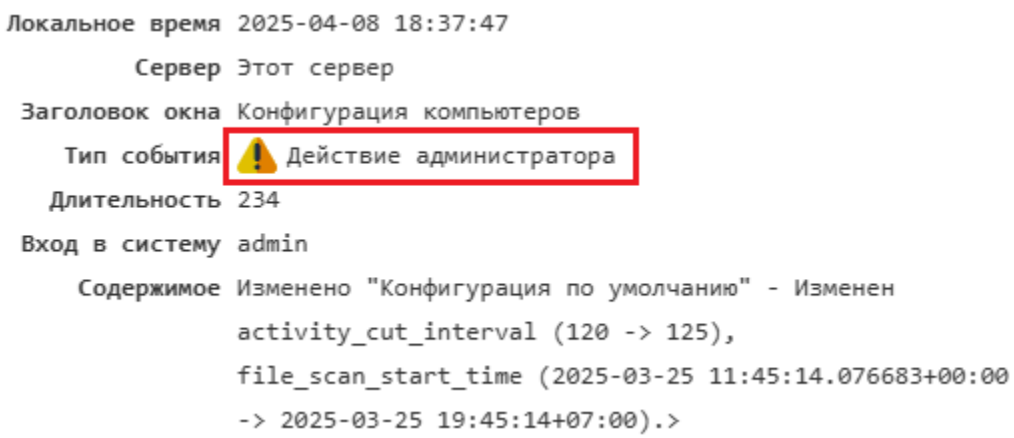
Системные события

Действие администратора

Действия администраторов в веб-интерфейсе iBatyr Monitor.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-08 18:13:45	Действие администратора		a.murzina		Администратор Изменено "a.murzina" - Выборка "agent_event" в конструкторе за период с 2025-01-01T00:00:00.000 по 2025-12-31T23:59:59.999 с фильтром: (значение не указано) по измерениям: Пользователь - Полное имя a.murzina
2025-04-08 18:13:42	Действие администратора		a.murzina		Администратор Изменено "a.murzina" - Скачивание файла filedata/by_date/2025_04_07/7efb1d11bc49471abaf2278aa27191975d0daede.bin a.murzina
2025-04-08 17:46:38	Действие администратора		a.dolgushin		Администратор Успешная авторизация пользователя "a.dolgushin". IP "95.170.152.84", база данных "default" a.dolgushin
2025-04-08 17:22:28	Действие администратора		m.litvinko		Фильтр Удалено "Объект #2709 "переписка" удален.." m.litvinko
2025-04-08 17:21:59	Действие администратора		n.suhoterin		Фильтр Добавлено "#2710 "Фильтр Интересный фильтр" типа analytics.filter". n.suhoterin

Примечание: Действия администраторов можно также посмотреть в *Админ → Последние действия*.



При необходимости включите в **Параметрах сервера**:

- для перехвата отчетов и построения выборок — *Добавлять просмотры отчетов и построение выборок в журнал*;
- перехвата скриншотов — *Записывать просмотр скриншотов в действия администратора*.

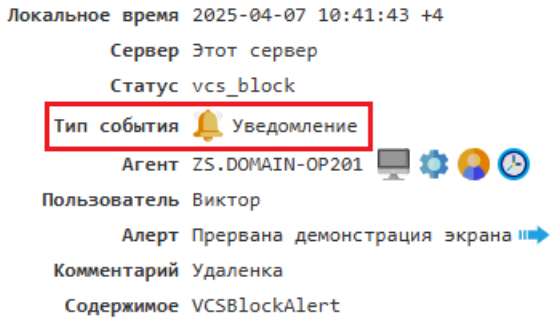
Уведомления

Сообщения о действиях, которые требуют внимания администратора.

См.также:

Подробнее об уведомлениях.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-11 18:25:29	Уведомление	DESKTOP-S1T67J5			Долгая неактивность агента Отсутствие событий
2025-04-11 14:06:13 +4	Уведомление	ZS.DOMAIN-OP201			Изменение оборудования +6/-2
2025-04-10 15:46:57	Уведомление	ZS.DOMAIN-SB101	Артём Слежкин		Опоздание пользователя Опоздание пользователя
2025-04-07 10:47:12 +4	Уведомление	ZS.DOMAIN-OP201	Виктор		Демонстрация экрана VCSScreenSharingAlert
2025-04-07 10:47:06 +4	Уведомление	ZS.DOMAIN-OP201	Виктор		Прервана демонстрация экрана VCSBlockAlert

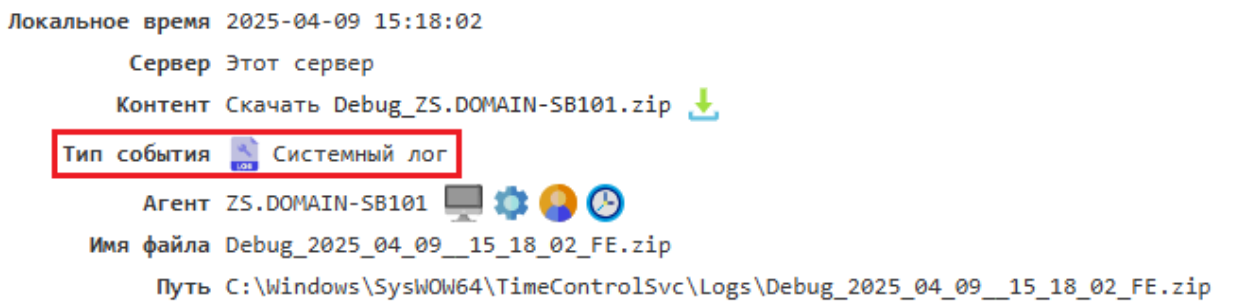


Отладочная информация

Системный лог

Архив отчетов о процессе работы агента, формируется автоматически. Необходим для отладки и передачи логов *в службу технической поддержки.*

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-04-09 15:18:02	Системный лог	ZS.DOMAIN-SB101			Debug_2025_04_09__15_18_02_FE.zip Скачать Debug_ZS.DOMAIN-SB101.zip
2025-04-09 09:49:33 +4	Системный лог	ZS.DOMAIN-OP201			Debug_2025_04_09__09_49_33_85.zip Скачать Debug_ZS.DOMAIN-OP201.zip
2025-04-09 13:49:30	Системный лог	Win_11_Gold_ISO			Debug_2025_04_09__13_49_29_FF.zip Скачать Debug_Win_11_Gold_ISO.zip



Линукс лог

Ввод и вывод в syslog, bash, других логах и командных оболочках Linux-агента.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-01-23 11:53:08	Линукс лог	ZS.DOMAIN-OR101	red	shell	ls
2025-01-23 11:52:46	Линукс лог	ZS.DOMAIN-OR101	red	shell	sudo fdisk -l
2025-01-20 16:13:20	Линукс лог	ZS.DOMAIN-OR101	red	shell	ping google.com
2025-01-20 16:13:03	Линукс лог	ZS.DOMAIN-OR101	red	shell	ps

Примечание: События **Линукс лог** не относятся к политике *Syslog коннектор*.

Для активации укажите список файлов в *Мониторинг Linux* → *Контроль лог-файлов*.

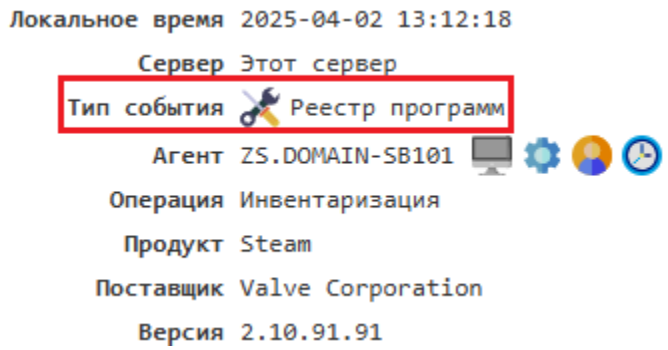
Оборудование, программное обеспечение и сеть

Реестр программ

Содержит информацию об установленном на ПК программном обеспечении. Система формирует событие при обновлении конфигурации и перезапуске агента.

Для активации включите *Инвентаризация* → *Реестр программ*.

Локальное время	Компьютер	Операция	Продукт	Поставщик	Версия
2025-04-02 13:12:18	ZS.DOMAIN-SB101	Инвентаризация	Telegram Desktop	Telegram FZ-LLC	5.8.2
2025-04-02 13:12:18	ZS.DOMAIN-SB101	Инвентаризация	Zoom	Zoom Video Communications, Inc.	5.17.11 (34827)



Реестр оборудования

Список всех устройств компьютера и их идентификаторов:

Локальное время	Компьютер	Тип	Устройство	ID
2025-04-02 13:12:17	ZS.DOMAIN-SB101	(Standard CD-ROM drives)	Optical Drive: NECVMWar VMware SATA CD00	SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7
2025-04-02 13:12:17	ZS.DOMAIN-SB101	(Standard disk drives)	Disk Drive: VMware Virtual disk SCSI Disk Device	SCSI\DISK&VEN_VMWARE&PROD_VIRTUAL_DISK\5&1EC51BF7&0&000000
2025-04-02 13:12:17	ZS.DOMAIN-SB101	Microsoft	Network Adapter: WAN Miniport (Network Monitor)	SWD\MSRRAS\MS_NDISWANBH

Для активации включите *Инвентаризация* → *Реестр оборудования*.

Сеть

IP-адреса и порты, через которые происходило подключение.

Для активации включите *Сетевые подключения* → *Мониторинг сети*.

Устройства

Список устройств, которые были подключены к компьютеру сотрудника.

Для активации включите и настройте *Устройства* → *USB устройства*.

Установка ПО

Записи об установке и удалении программ на компьютерах сотрудников.

Для активации включите и настройте *Контроль программ* → *Установка приложений*.

Локальное время 2025-04-02 13:12:17
Сервер Этот сервер
Тип события Реестр оборудования
Агент ZS.DOMAIN-SB101
Производитель Intel Corporation
Устройство Network Adapter: Intel(R) 82574L Gigabit Network Connection
HardwareId PCI\VEN_8086&DEV_10D3&SUBSYS_07D015AD&REV_00\005056FFFFAE25F600
Содержимое Network Adapter: Intel(R) 82574L Gigabit Network Connection

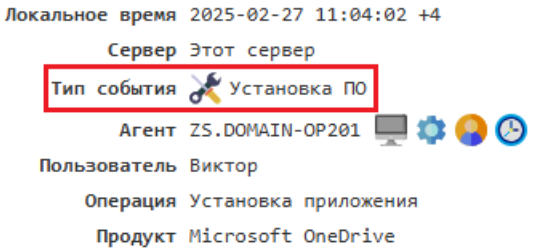
Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-02-28 11:49:53	Сеть	pc-0001.local	test.user	thunderbird.exe	11.22.33.444 mail-imap.stable.qloud-b.yandex.net:993

Локальное время 2025-02-20 14:05:28
Сервер Этот сервер
Приложение thunderbird.exe
Тип события Сеть
Агент pc-0001.local
Пользователь test.user
Сетевая активность 11.22.33.444 mail-imap.stable.qloud-b.yandex.net:993
Комментарий Тестовый сотрудник 1
PID 2892
UID 1

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-03-21 18:39:19	Устройства	ZS.DOMAIN-OR101	red		Подключение VMware, Inc. VMware Virtual USB Hub (09:00:00 Hub/Full speed (or root) hub)
2025-03-21 18:39:19	Устройства	ZS.DOMAIN-OR101	red		Подключение VMware Virtual USB Mouse (03:01:02 Human Interface Device/Boot Interface Subclass/Mouse)

Локальное время 2025-01-29 13:53:24
Сервер Этот сервер
Тип события Устройства
Агент DESKTOP-S1T67J5
Пользователь ratmi
Операция Отключение
Производитель Microsoft
Устройство Микрофон гарнитуры (Jabra EVOLVE 20 MS)
HardwareId SWD\MMDEVAPI\{0.0.1.00000000}.{17EC0ACD-6DB5-45E1-9D1F-7A7265FB9A49}

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-02-07 01:28:46	Установка ПО	DESKTOP-S1T67J5	ratmi		Удаление приложения Microsoft OneDrive
2025-02-06 12:22:26 +4	Установка ПО	ZS.DOMAIN-OP201	Виктор		Установка приложения Microsoft OneDrive
2025-01-31 16:12:26	Установка ПО	ZS.DOMAIN-OR102			Удаление приложения FileZilla Server 1.9.4
2025-01-30 12:09:10 +4	Установка ПО	ZS.DOMAIN-OP201	Виктор		Установка приложения Microsoft OneDrive
2025-01-30 12:09:09 +4	Установка ПО	ZS.DOMAIN-OP201	Виктор		Удаление приложения Microsoft OneDrive
2025-01-29 11:18:04 +4	Установка ПО	ZS.DOMAIN-OP201	Артём Слежкин		Установка приложения VK Teams

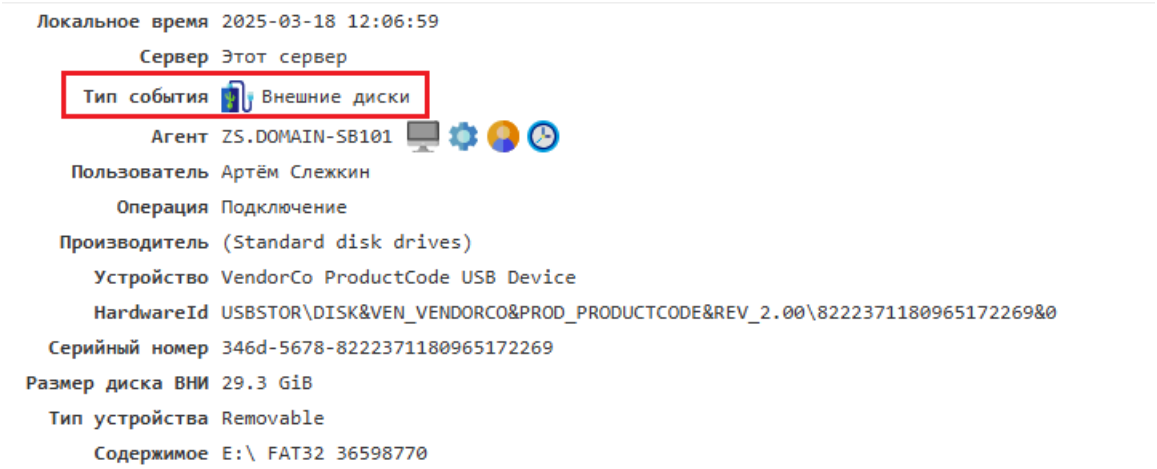


Внешние диски

Подключенные внешние накопители.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2025-03-18 19:03:21	Внешние диски	ZS.DOMAIN-SB101	Артём Слежкин		Подключение Removable VendorCo ProductCode USB Device
2025-03-18 12:06:59	Внешние диски	ZS.DOMAIN-SB101	Артём Слежкин		E:\ FAT32 36598770 Подключение Removable VendorCo ProductCode USB Device
2025-02-03 18:13:02	Внешние диски	DESKTOP-S1T67J5	ratmi		E:\ FAT 1871568006 Отключение Removable VendorCo ProductCode USB Device

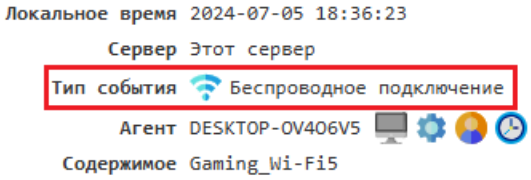
Для активации включите и настройте *Инвентаризация* → *Реестр оборудования*.



Беспроводные подключения

Данные о подключениях к беспроводным сетям.

Локальное время	Тип	Компьютер	Пользователь	Приложение	Событие
2024-07-08 20:10:54	Беспроводное подключение	DESKTOP-OV4O6V5			Gaming_Wi-Fi5
2024-07-07 14:00:07	Беспроводное подключение	DESKTOP-OV4O6V5			Mercury



Для создания событий о беспроводном подключении включите и настройте *Беспроводные сети* → *Подключение к беспроводным сетям*.

4.3.13 Уровень риска событий и пользователей

Содержание

- *Уровень риска событий и пользователей*
  - *Активация уровня риска*
  - *Настройка уровня риска*
  - *Управление уровнем риска событий*
    - *Отображение в Конструкторе событий*
    - *Фильтрация и настройка уведомлений*
  - *Управление уровнем риска пользователей*

- *Пример расчета риска пользователя*
- *Настройка уведомлений*
- *Отчет об уровне риске пользователя*
- *Отображение уровня риска сотрудника*

Начиная с версии 5.5 функциональность **Уровень риска** позволяет присвоить значимость событиям политик безопасности.

На основе этих данных вы можете оценить серьезность инцидентов и связанные с каждым сотрудником риски.

Активация уровня риска

Функциональность **Уровень риска** не активирована по умолчанию, потому что включение может привести к увеличению нагрузки на сервер.

Чтобы включить **Уровень риска**:

1. Откройте на сервере конфигурационный файл */etc/ibatyr/config* с помощью nano или в другом удобном для вас редакторе:

```
sudo nano /etc/ibatyr/config
```

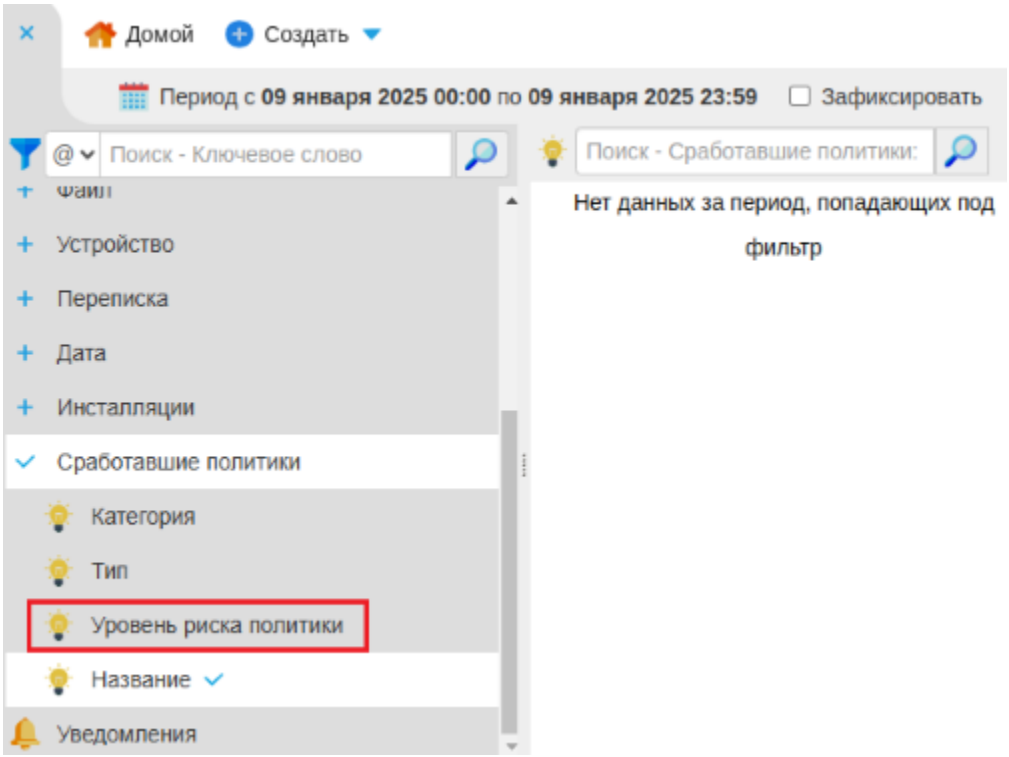
2. Добавьте в конце файла строку:

```
RISK_LEVEL_ENABLED = True
```

3. Сохраните изменения в файле.
4. Перезапустите iBatyr Monitor командой:

```
ibatyr restart
```

После активации функционал станет доступен в **Конструкторе** в **Сработавших политиках**.



Настройка уровня риска

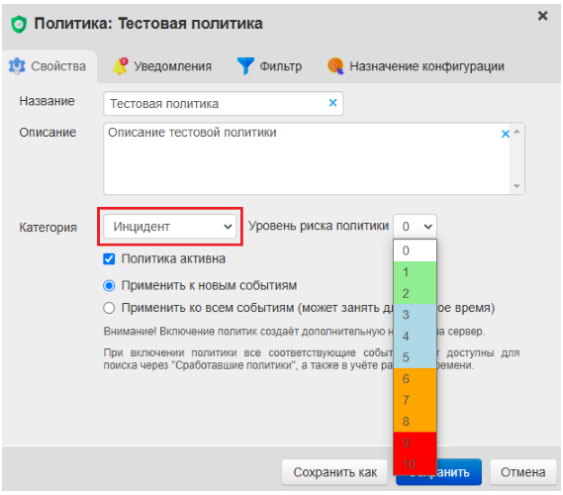
Вы можете присвоить уровень риска только *политикам* и *словарям*, которые относятся к категории **Инцидент**. Поэтому сначала присвойте политике категорию **Инцидент**, а после этого задайте уровень риска.

Примечание: Функциональность действует как для предустановленных, так и кастомных политик и словарей.

Примечание: Не рекомендуется устанавливать уровень риска для политик, которые обрабатывают большие группы событий — например, **Политики продуктивности**. Это может привести к увеличению уровня риска пользователя за счёт множества ложных срабатываний.

---

1. В окне **Политики** или **Поиска по словарю** перейдите во вкладку **Свойства**.
2. В поле **Категория** выберите **Инцидент**.
3. В поле **Уровень риска** укажите значение от 0 до 10.



Уровень риска выделяется цветом в зависимости от значения:

- **0**: белый,
- **1–2**: светло-зеленый,
- **3–5**: светло-синий,
- **6–8**: оранжевый,
- **9–10**: красный.

4. Готово! После настройки событию будет присваиваться уровень риска. *Уровень риска пользователей* присваивается на основе уровня риска сработавших для них событий.

Примечание: Если уровень риска не задан или категория политики изменена с **Инцидент** на другую, уровень риска сбрасывается до значения по умолчанию — 0.

Управление уровнем риска событий

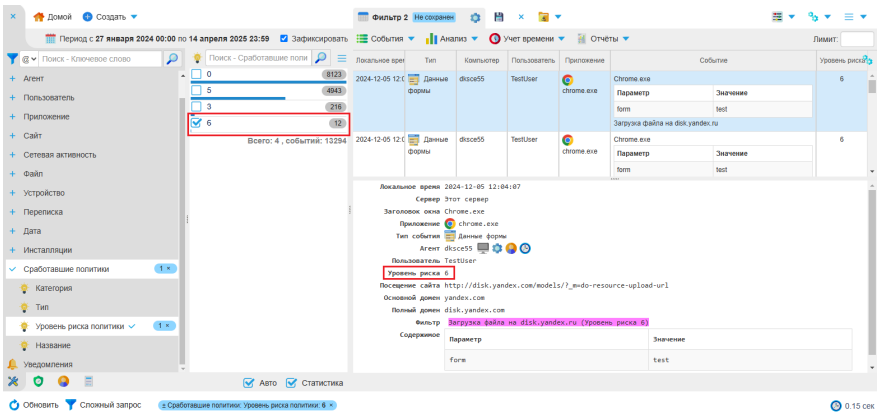
После назначения **Уровня риска политики** сервер при срабатывании политики присвоит событию уровень риска.

Отображение в Конструкторе событий

Чтобы посмотреть события, которым присвоен уровень риска:

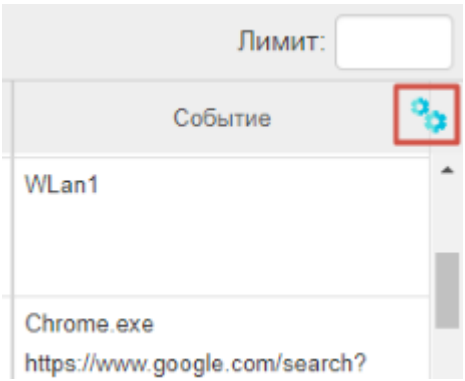
1. Перейдите в **Конструктор**.
2. В разделе **Сработавшие политики** выберите **Уровень риска политики**.
3. В **Конструкторе** появится список событий, сгруппированных по уровню риска сработавших политик. **Уровень риска события** отображается в **Таблице**.

Поставьте галочку в чекбоксе, чтобы группа событий отобразилась в **Линзе событий**. Уровень риска отдельного события отражен в **Информации о событии**.

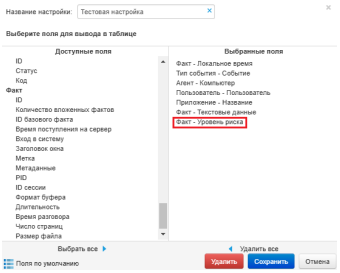


В **Линзе событий** столбец **Уровень риска** не отображается по умолчанию. Чтобы столбец появился в таблице:

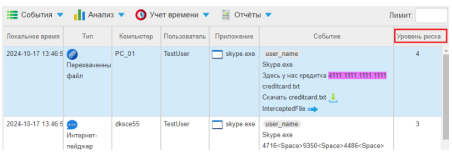
1. Нажмите на иконку с шестернями и выберите **Новая настройка**.



2. В разделе **Доступные поля** → **Факт** нажмите на строку **Уровень риска**. Строка переместится в **Выбранные поля**.



3. После сохранения настройки в таблице появится столбец:

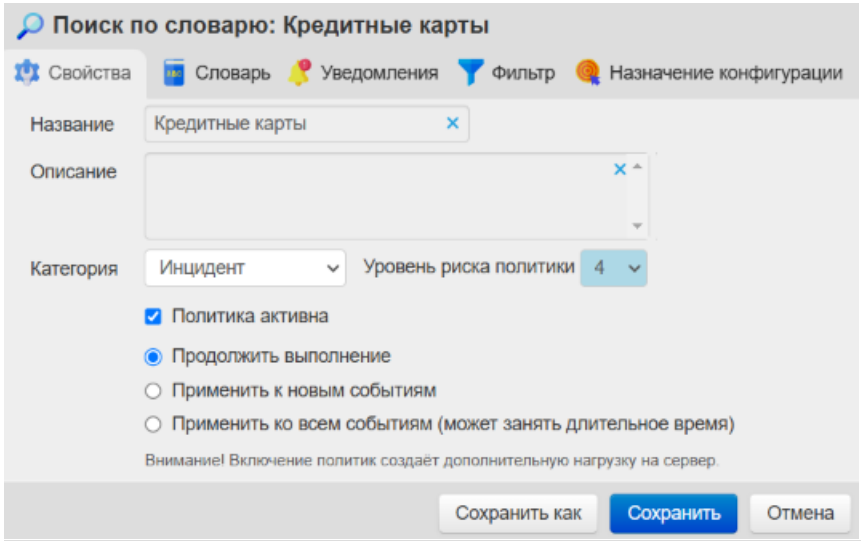


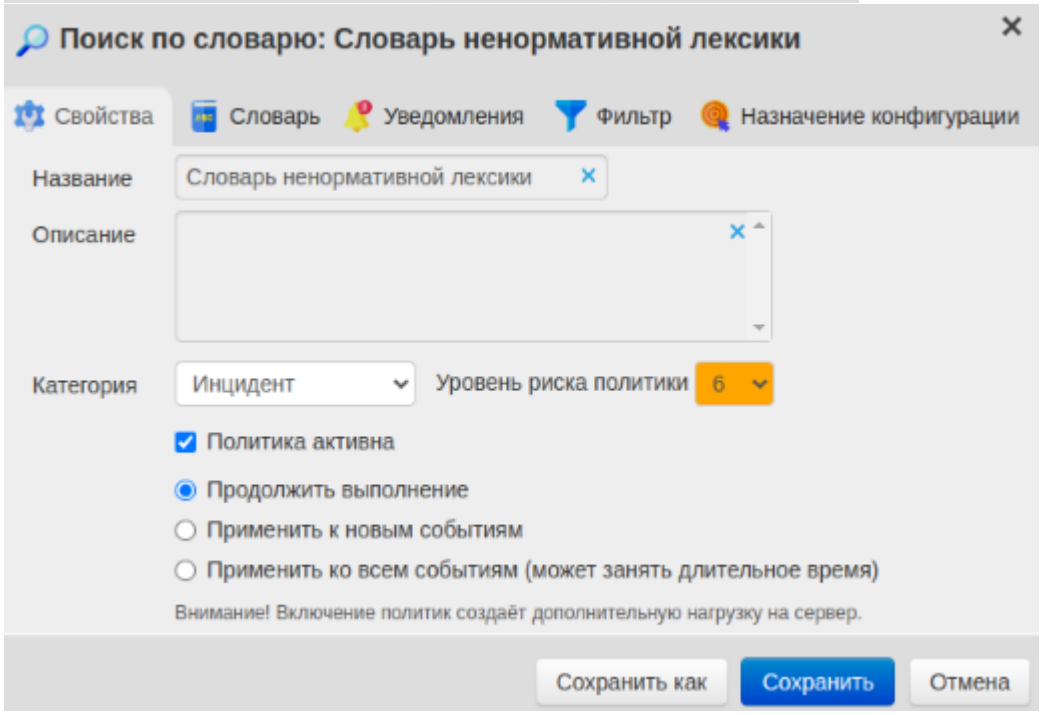
Увеличение уровня риска события

События могут совмещать в себе несколько сработавших политик. В этом случае общий уровень риска события — это сумма уровня рисков всех политик.

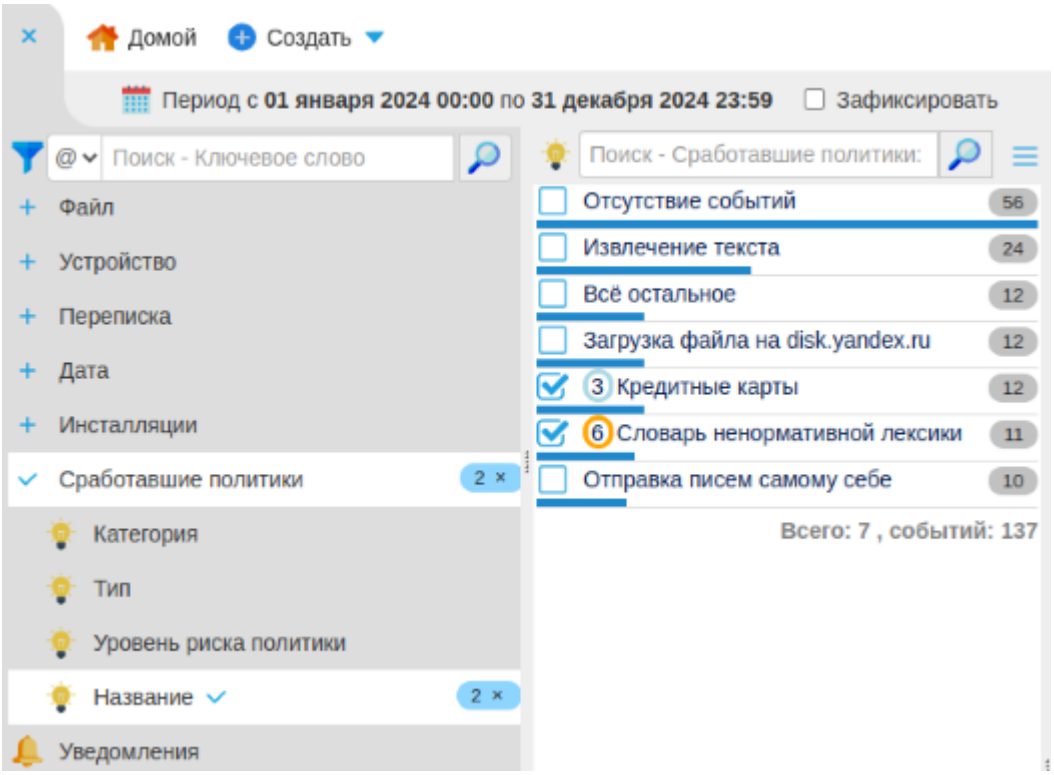
Пример

1. Установите значение **Уровня риска**. В этом примере для события **Кредитных карт** значение равно трем, а у **Словаря ненормативной лексики** — шести:

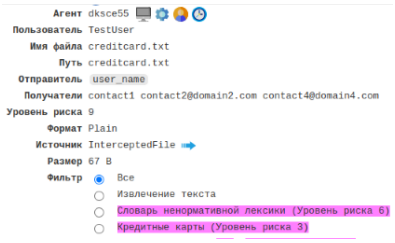




2. При появлении события перейдите в **Конструкторе** к измерению **Сработавшие политики**. В **Названии** выберите политики, рядом с которыми указано значение уровня риска.



3. Выберите событие. Например, **Перехваченный файл**. В нашем примере в тексте перехваченного файла есть и номер кредитной карты, и номер паспорта, поэтому в информации о событии уровень риска равен девяти. Это общая сумма для всех политик, которые сработали при передаче файла.



Примечание: Значения суммируются, но общее значение для отдельного события **не может превышать 20**. Ограничение позволяет более реалистично оценить общий риск без чрезмерного влияния отдельных высоких рисков на итоговую оценку.

Фильтрация и настройка уведомлений

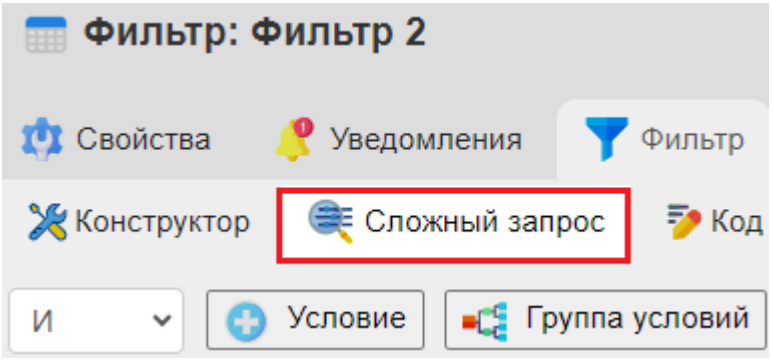
Используйте фильтр и сложный запрос для сортировки событий с определенным уровнем риска. Например, вы можете получить список событий с уровнем риска 10 для определенной подсети. Чтобы отфильтровать события по суммарному риску, используйте сложный запрос.

После настройки фильтрации в **Конструкторе событий** отобразятся только события, которые соответствуют заданным условиям.

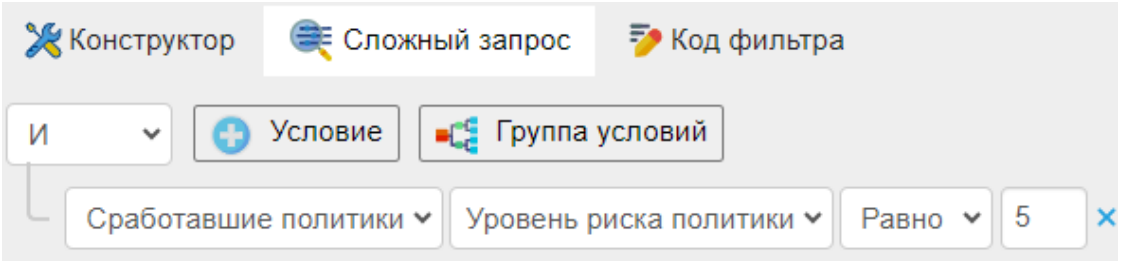
Фильтр событий на основе уровня риска сработавших политик

С помощью Сложного запроса

1. *Создайте или перейдите* в существующий фильтр.
2. Перейдите во вкладку **Фильтр** → **Сложный запрос**.



3. Нажмите на кнопку +**Условие**.
4. Выставите значение **Сработавшие политики — Уровень риска политики**.
5. Выберите логический оператор и введите значение уровня риска.

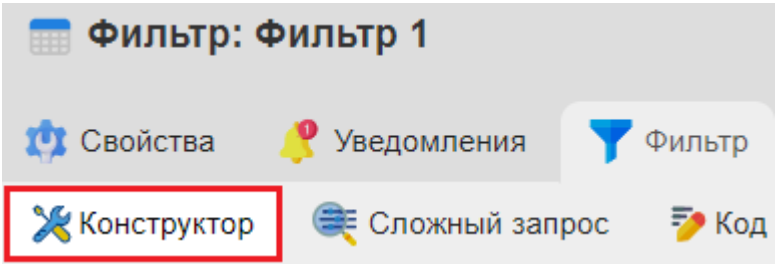


6. При необходимости добавьте другие условия и *настройте отправку уведомлений на почту* во вкладке **Уведомления**.
7. Сохраните фильтр.

Результат: в линзе отображаются события, на которые среагировала хотя бы одна политика с заданным в условии уровнем риска.

С помощью Конструктора

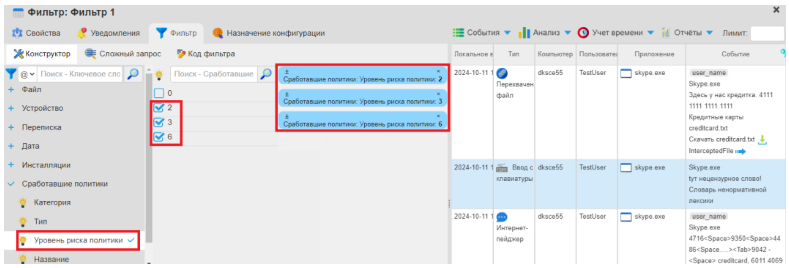
1. *Создайте или перейдите* в существующий фильтр.
2. Перейдите во вкладку **Фильтр** → **Конструктор**.



3. Выберите в левой боковой панели **Уровень риска политики** в разделе **Сработавшие политики**.

4. Выберите уровень риска.

Примечание: Количество значений для каждого уровня риска указывает на количество срабатываний политик с уровнем риска. Поэтому возможна ситуация, когда количество реакций с уровнем риска будет пять, а при выборе в конструкторе будет всего два события.



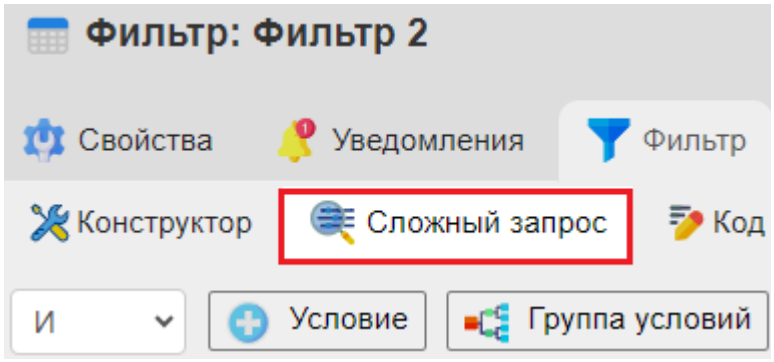
5. При необходимости добавьте другие условия и *настройте отправку уведомлений на почту* во вкладке **Уведомления**.
6. Сохраните фильтр.

Результат: в линзе отображаются события, на которые среагировала хотя бы одна политика с заданным в условии уровнем риска.

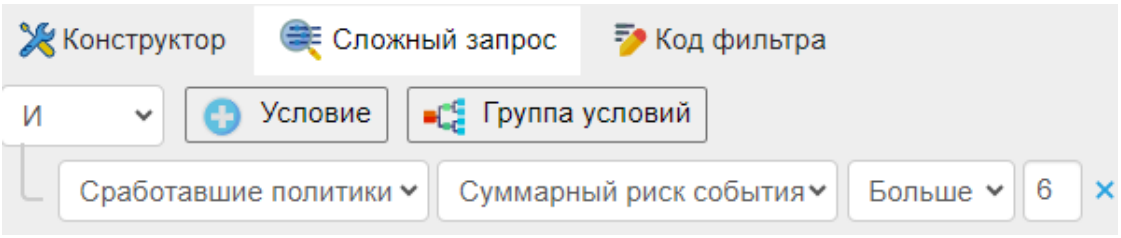
Фильтр событий по суммарному уровню риска

Используйте сложный запрос для фильтрации событий, чей уровень риска суммируется за счет всех сработавших политик:

1. *Создайте или перейдите* в существующий фильтр.
2. Перейдите во вкладку **Фильтр** → **Сложный запрос**.



3. Нажмите на кнопку + **Условие**.
4. Выставите значение **Сработавшие политики — Суммарный риск события**.
5. Выберите логический оператор и введите значение уровня риска.



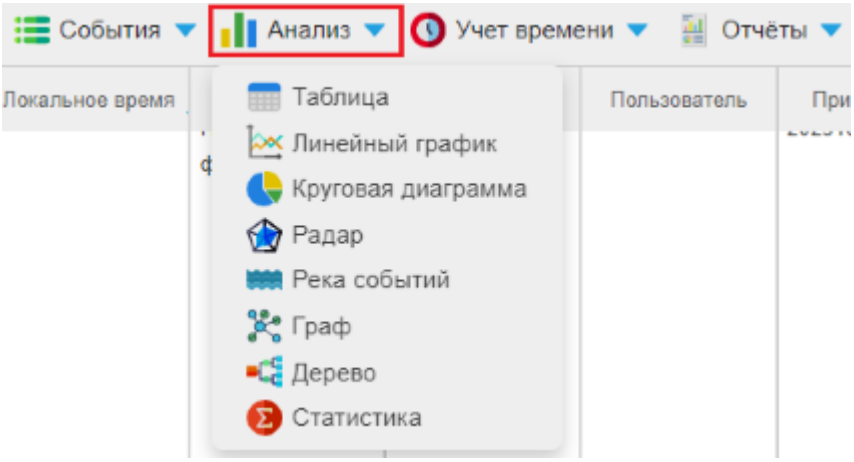
6. При необходимости добавьте другие условия и *настройте отправку уведомлений на почту* во вкладке **Уведомления**.
7. Сохраните фильтр.

Результат: в линзе отображаются события, чей суммарный уровень риска сработавших политик соответствует условию.

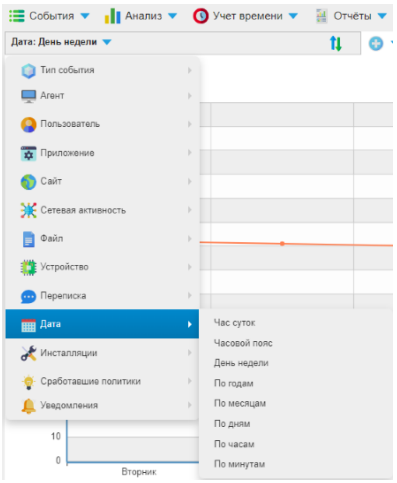
Отчеты

Для построения наглядных графиков и статистики используйте инструменты меню *Анализа* с указанием меры **Уровень риска**:

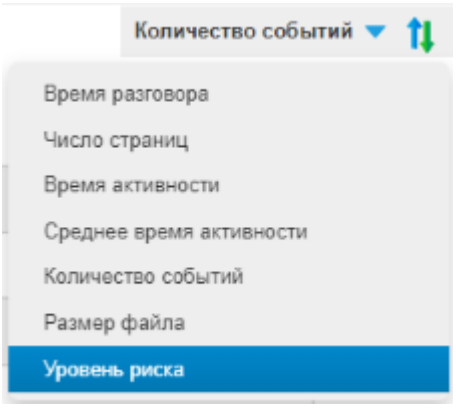
1. Выберите в меню **Анализ** способ отображения данных. В примере используется **Линейный график**:



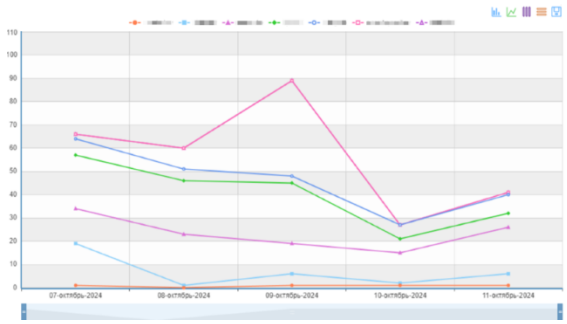
2. Выберите измерения данных, по которым нужно построить график, например **Дата — По дням**:



3. Установите в качестве меры **Уровень риска**:



4. Система автоматически сгенерирует график:



Управление уровнем риска пользователей

> **Предупреждение:** Чтобы видеть уровень риска пользователей, активируйте *Карточку сотрудника*.

Система оценивает **Уровень риска пользователя** на основе событий пользователя. Каждое событие с присвоенным уровнем риска увеличивает общий показатель. Чем больше таких событий — тем выше уровень риска пользователя.

- система суммирует риски событий за несколько дней — количество дней задаётся в **Параметрах сервера**;
- в пределах одного дня учитывается только максимальное значение риска, заданное в **Параметрах сервера** — чтобы избежать резких скачков риска за день;
- полученные данные отображаются *в сводной карточке и в карточках сотрудников*.

Чтобы задать параметры для оценки уровня риска пользователя:

1. Перейдите в **Панель управления** → **Параметры сервера** .
2. На странице **Параметры сервера** установите значения в двух параметрах:
   - **Параметры расчета риска пользователя: количество дней** – задаёт количество дней, в течение которых будут учитываться события пользователя для расчета уровня риска.
     - число от 0 до 84,
     - значение по умолчанию: 14 дней.
   - **Параметры расчета риска пользователя: максимальное значение риска за день** – определяет максимальное количество баллов риска, которые могут быть учтены за один день.
     - число от 0 до 10 000,
     - значение по умолчанию: 100.

   Оба параметры обязательны для заполнения.
3. Сохраните изменения.

Пример расчета риска пользователя

В **Параметрах сервера** указаны значения по умолчанию для **Параметров расчета риска пользователя**:

- уровень риска пользователя считается за последние 14 дней,
- при расчете уровень риска за день не превышает **максимальное значение риска за день** = 100.

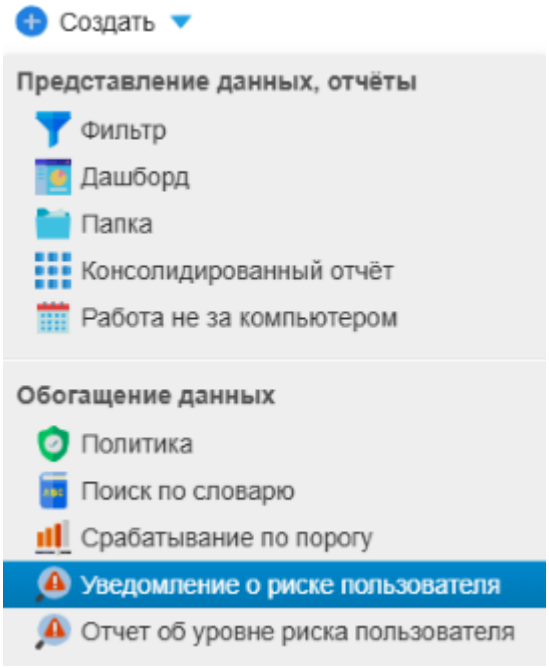
За период с 16 сентября по 14 октября система зафиксировала у пользователя:

tabularytabulary

Период	**События с уровнем риска > 0**
16.09 — 30.09	Нет
01.10	Зафиксированы события с суммарным уровнем риска = 90
02.10 — 13.10	Нет
14.10	Зафиксированы события с суммарным уровнем риска = 250
15.10	Нет

Настройка уведомлений

Чтобы создать уведомление, нажмите + **Создать** и выберите **Уведомление о риске пользователя**.

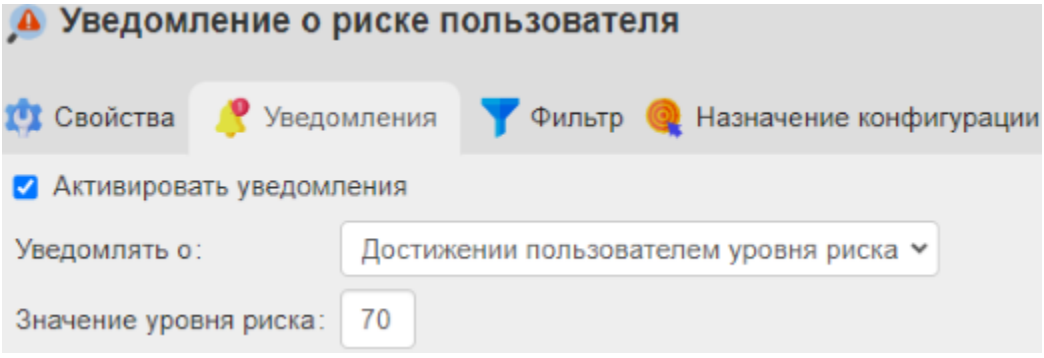


Настройте уведомления *по инструкции*. После настройки уведомления о уровня риска пользователя будут приходить на почту не чаще одного раза в сутки.

Обратите внимание, что сам рост уровня риска фиксируется в **Конструкторе** в измерении **Уведомления** в одном из событий при достижении порогового значения:

- **Высокий уровень риска пользователя**— событие срабатывает, когда уровень риска достигает заданного значения.
- **Увеличение уровня риска пользователя** — событие фиксируется, когда риск увеличивается на указанное значение.

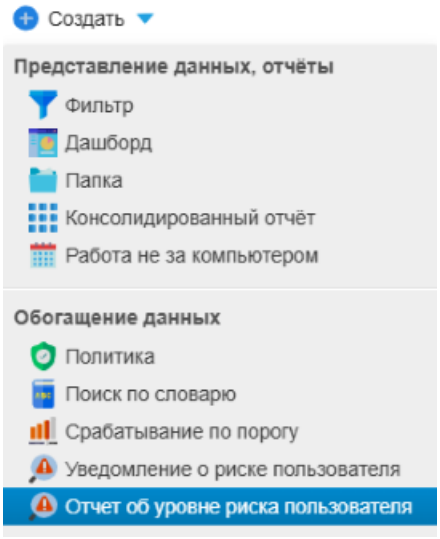
Для того, чтобы эти события создавались, выберите одно из них во вкладке **Уведомления** в поле **Уведомлять о** и задайте значение:



Отчет об уровне риске пользователя

Отчет об уровне риска пользователя — инструмент, который показывает, у каких пользователей уровень риска выше или ниже заданного значения.

Чтобы создать отчет, нажмите + **Создать** и выберите **Отчет об уровне риске пользователя**.



См.также:

Как создать и настроить *Отчет об уровне риска пользователя*.

Отчет отправляется на почту ежедневно/еженедельно/ежемесячно. В отчете доступна группировка данных по пользователям или дате. Используйте вкладку **Фильтр**, чтобы выбрать, по каким пользователям формировать отчет.

Отображение уровня риска сотрудника

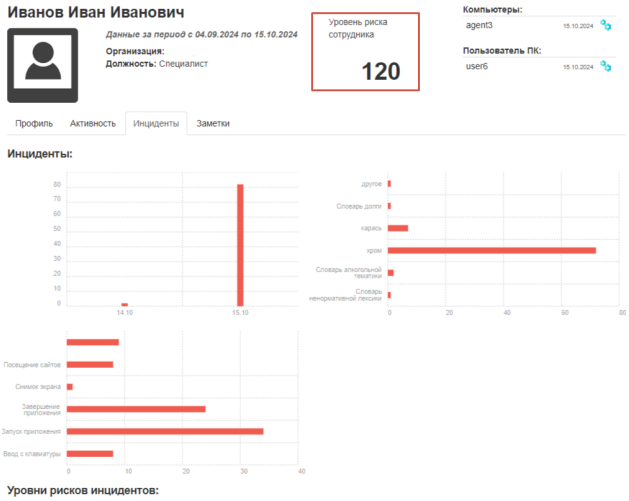
Уровень риска сотрудника отображается в **карточках сотрудников**. Карточки сотрудников находятся во вкладке **Сотрудники**.

Нажмите на пользователя, чтобы открыть карточку.

В карточке данные отображаются во вкладках:

- **Профиль** – отображает уровень риска сотрудника по дням за последние семь дней. График предоставляет визуализацию изменения уровня риска со временем.
- **Инциденты** – отображает сумму уровней риска событий сотрудника по дням за последние семь дней.

Внимание: Графики во вкладке **Профиль** напрямую зависят от **Параметров расчета риска пользователя** в **Параметрах сервера**.

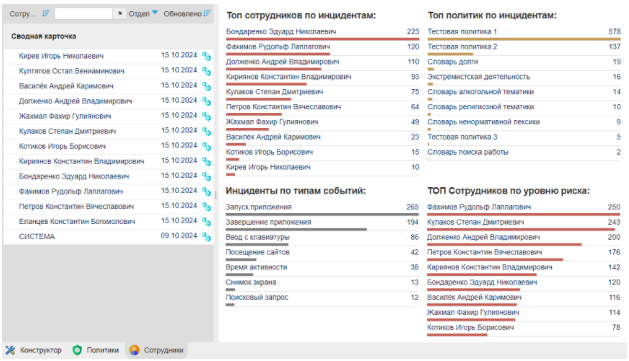


Примечание: Если у пользователя несколько учетных записей, то уровень риска суммируется.

Сводная карточка

В **Сводной карточке** отображается общая информация по уровням риска сотрудников.

В отчете **Топ сотрудников** по уровню риска представлены десять сотрудников с наибольшим уровнем риска:



4.3.14 Анализ пакетов снимков экрана

Содержание

- *Анализ пакетов снимков экрана*
  - *Просмотр записанных пакетов из события*
  - *Переход из события к ближайшему пакету снимков экрана*
  - *Просмотр на полном экране*
    - *Просмотр событий и активности*

        * *Поиск событий и активности*
    - *Просмотр scrpack-файлов пакетов снимков экрана*
        * *Просмотр в веб-интерфейсе*
        * *Просмотр в офлайн-проигрывателе*

Пакет снимков экрана — это набор изображений рабочего стола, которые агент делает на компьютере пользователя, собирает в сжатый пакет и отправляет на сервер.

Примечание: Для анализа пакетов снимков экрана включите в конфигурации сбор *пакетов снимков экрана*

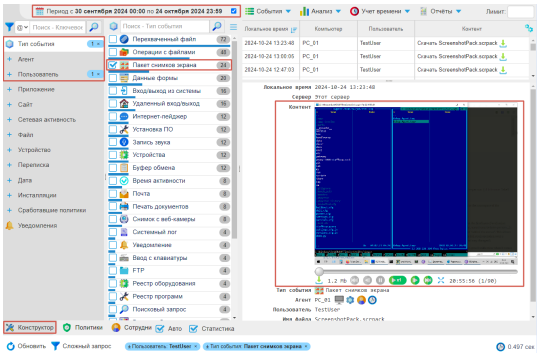
Снимки позволяют:

- постоянно отслеживать и сохранять активность пользователя на основе снимков рабочего стола,
- находить изображения рабочего стола на основе событий безопасности,
- анализировать действия пользователя на основе изображений, что упрощает мониторинг выполнения задач, выявление нарушений и оценку производительности.

Просмотр записанных пакетов из события

Чтобы просмотреть записанные пакеты снимков:

1. Перейдите в **Конструктор** на главной странице веб-интерфейса iBatyr Monitor.
2. В измерениях **Агент** или **Пользователь** выберите компьютер или пользователя, чьи снимки экрана хотите увидеть.
3. Выберите **Тип события** → **Пакет снимков экрана**.
4. В верхней панели конструктора установите временной период.
5. При необходимости добавьте другие условия фильтрации по измерениям.
6. В **Линзе событий** отобразится список всех пакетов снимков за указанный промежуток времени.
7. Выберите интересующее событие и воспользуйтесь плеером в разделе **Контент** для просмотра снимков экрана.



Чтобы *начать* или *остановить воспроизведение*, нажмите на любую часть скриншота.

Проигрыватель пакетов снимков экрана поддерживается в браузерах:

- Chrome,

- Mozilla,
- Opera,
- MS Edge,
- Yandex Browser.

На панели управления плеером указаны размер пакета, количество скриншотов и время создания каждого скриншота. При наведении на прогрессбар появляется время и порядковый номер скриншота в пакете. Нажмите на прогрессбар под сообщением, чтобы перейти к скриншоту:

Используйте кнопки на панели управления:

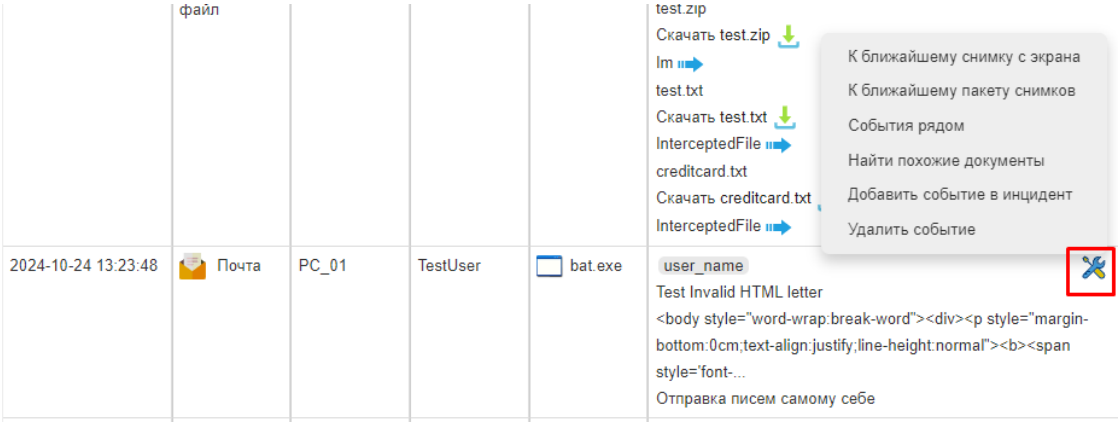
- для скачивания пакета скриншотов,
- перехода к первому или последнему скриншоту,
- перемотки скриншотов,
- изменения скорости воспроизведения,
- выхода в полноразмерный экран.

Переход из события к ближайшему пакету снимков экрана

С версии 5.5 вы можете переходить из события к ближайшему снимку экрана, чтобы увидеть, что именно делал пользователь в момент события.

Чтобы из события перейти к изображению в пакете снимков экрана:

1. Нажмите на иконку инструментов рядом с событием.
2. Выберите **К ближайшему пакету снимков**.



Сервер запустит проигрыватель пакетов снимков экрана для пакета:

- локальное время события входит в диапазон локального времени пакета,
- **имя компьютера** и **имя пользователя** события соответствуют **имени компьютера** и **имени пользователя** пакета.

Предупреждение: Если после клика на **К ближайшему пакету снимков** появляется предупреждение *В указанное время для пользователя не осуществлялась постоянная запись пакетов*

снимков экрана, сервер не нашёл снимков экрана за этот период. Проверьте в разделе конфигурации *Пакет снимков экрана* значение **Интервал снимков**. Возможно, частота снимков слишком низкая, поэтому на момент события не было записи.

Просмотр на полном экране

Для просмотра пакета снимков экрана в полноэкранном режиме:

- нажмите клавишу **F** — на англоязычную раскладку переключаться не нужно;
- нажмите кнопку развертывания во встроенном плеере:

В полноэкранном режиме доступно управление с клавиатуры:

tabularytabulary

Кнопка	
Пробел	Воспр
[или **]**	Изменение скор
, или **.**	П
← или →	П
↑ или ↓	Шаг назад или
PgUp или **PgDown**	Шаг назад или
Home или **End**	Перехо

Выйти из режима полного экрана:

- кнопка **F**;
- кнопка развертывания/свертывания на панели управления;
- кнопка **Esc**.

В полноэкранном режиме проигрывателя доступны данные:

1. **Имя компьютера** и **Имя пользователя**, у которых зафиксирован снимок экрана.

2. **Данные по активности** — данные времени активности:
   - название приложения,
   - адрес сайта, если приложение является браузером,
   - заголовок окна.

   Примечание: Сервер скрывает часть строки с метаданными, если она не помещается в окно проигрывателя. Чтобы посмотреть полностью, наведите на неё курсор более чем на две секунды.

   ---

3. **Таблица событий** — при клике на пиктограмму откроется **Таблица событий**.
4. **Таблица активности** — при клике на пиктограмму откроется **Таблица активности**.
5. **Плеер проигрывателя пакета снимков экрана**.

Примечание: Строка *Нет данных активности* в **Данных по активности** означает, что для изображения в пакете снимков экрана нет события **Время активности** или не указан пользователь.

Просмотр событий и активности

Для просмотра активности и событий нажмите в верхней правой части на пиктограммы **Таблицы событий** и **Таблицы активности**.

Во время воспроизведения в таблицах подсвечиваются записи, локальное время которых соответствует текущему снимку. При двойном ЛКМ по записи из **Таблицы активности** или **Таблицы событий** проигрыватель переходит к их отображению.

Нажмите на пиктограмму **Скрыть таблицу**, чтобы скрыть таблицу.

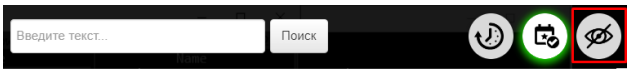
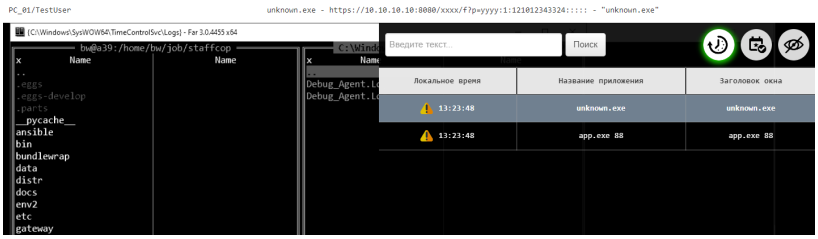


Таблица активности

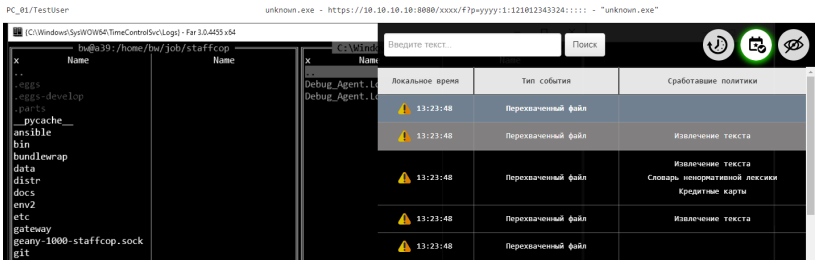
Таблица активности позволяет увидеть всю активность пользователя, которая входит в диапазон времени пакета снимков экрана.



Включает в себя **Локальное время**, **Название приложения** и **Заголовок окна**.

Таблица событий

Таблица событий позволяет увидеть события пользователя, которые входят в диапазон времени пакета снимков экрана.



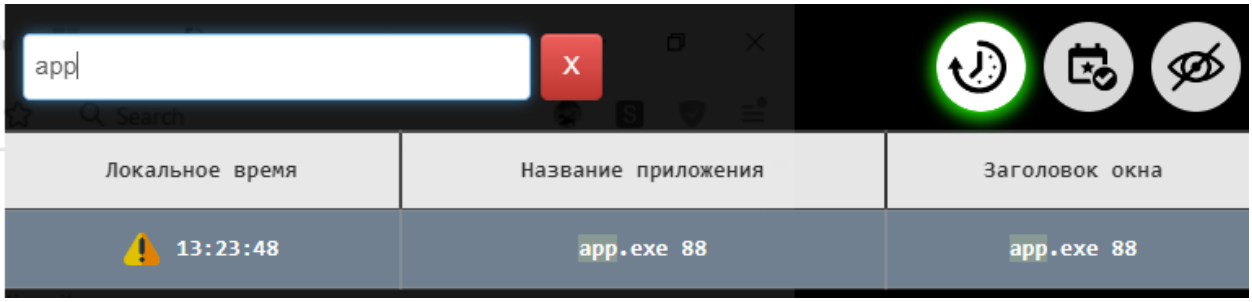
Включает в себя **Локальное время события**, **Тип события** и **Сработавшая политика**.

Недоступно для типов событий:

- Снимок экрана,
- Пакет снимков экрана,
- Видео рабочего стола,
- Время активности,
- Реестр софта,
- Реестр оборудования,
- Метрика,
- Системный лог.

Поиск событий и активности

В **Таблицах событий** и **Таблицах активности** доступен поиск по событиям из таблицы: введите в поисковую строку до 100 символов и нажмите **Найти**.



Для возвращения к исходному списку нажмите на крестик — **Сбросить результаты поиска**.

Просмотр scrpack-файлов пакетов снимков экрана

При скачивании пакет снимков экрана сохраняется в специальном формате *scrpack*, который не поддерживается стандартными приложениями для просмотра изображений.

Открыть scrpack-файл пакета снимков экрана можно:

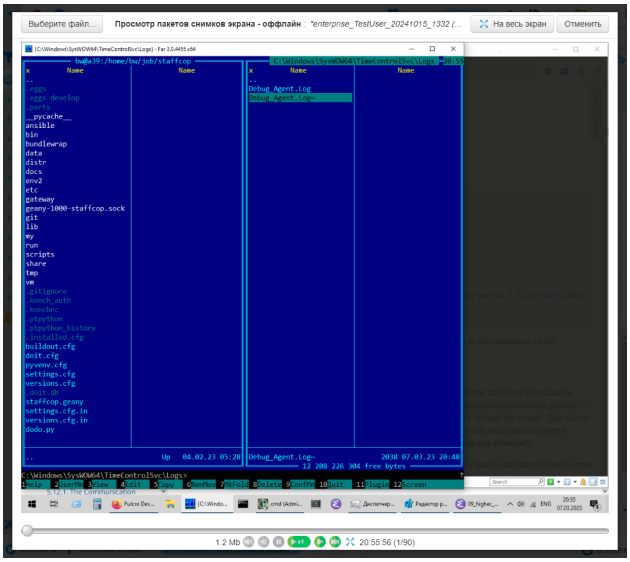
- в веб-интерфейсе,
- в офлайн-проигрывателе пакетов снимков экрана.

Офлайн-проигрыватель имеет функционал стандартного проигрывателя пакетов снимков экрана за исключением просмотра таблиц событий и активности.

Просмотр в веб-интерфейсе

Для просмотра scrpack-файла в веб-интерфейсе:

1. Нажмите **Админ** → **Просмотр файла «Пакет снимков»**.
2. В открывшемся окне нажмите **Выберите файл** и откройте нужный scrpack-файл.



Просмотр в офлайн-проигрывателе

Для просмотра scrpack-файлов установите офлайн-проигрыватель на свой компьютер.

Установка на Windows

1. Нажмите **Панель управления** → **Компьютеры**.
2. В разделе **Скачать агент** выберите **Проигрыватель пакетов снимков — Windows** и подтвердите загрузку файла.
3. Запустите exe-файл.

Примечание: Если при запуске exe-файла появилось системное предупреждение «Система Windows защитила ваш компьютер», нажмите **Подробнее** → **Выполнить в любом случае**.

4. После завершения установки откройте приложение **scrpack-player**.
5. В открывшемся окне нажмите **Выберите файл...** и откройте нужный scrpack-файл.

Установка на Linux

1. Перейдите **Панель управления** → **Компьютеры**.
2. В разделе **Скачать агент** выберите **Проигрыватель пакетов снимков — Linux** и подтвердите загрузку файла.
3. Запустите deb-пакет.
4. После завершения установки откройте приложение **scrpack-player**.
5. В открывшемся окне нажмите **Выберите файл...** и откройте нужный scrpack-файл.

Установка на macOS

1. Скачайте проигрыватель с дистрибутивного сервера.
2. Запустите загруженный файл.
3. После завершения установки откройте приложение **scrpack-player**.
4. В открывшемся окне нажмите **Выберите файл...** и откройте нужный scrpack-файл.

Решение проблемы с запуском

В macOS Sonoma и более ранних версиях файлы могут не запускаться, потому что для них установлен атрибут `quarantine`.

Атрибут `quarantine` — это метка macOS, которая помечает загруженные файлы и предупреждает о возможных рисках перед запуском файла.

Чтобы снять атрибут:

1. Откройте терминал **Launchpad** → **Другие** → **Терминал** или **Cmd** () + пробел и введите *терминал*.
2. Выполните команду:

```
xattr -d com.apple.quarantine <имя файла или архива>
```

После этого файл должен запускаться без ограничений.

4.4 Консоль управления инцидентами

4.4.1 Общее

- *Вход в консоль*
- *Список инцидентов*
- *Варианты просмотра*
- *Меню управления*

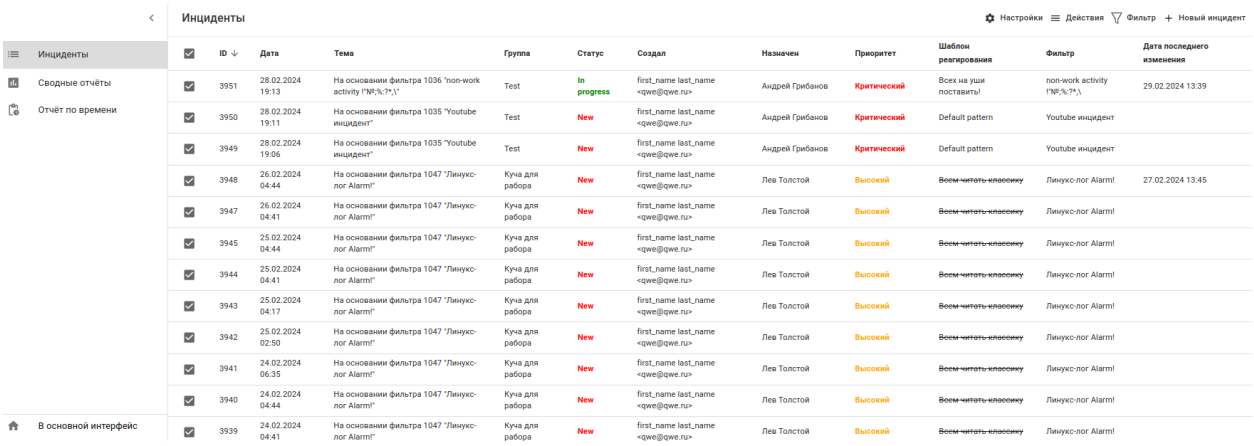
Для управления инцидентами используйте консоль инцидентов. После входа в консоль вы сможете выполнять операции с инцидентами и просматривать отчеты.

Вход в консоль

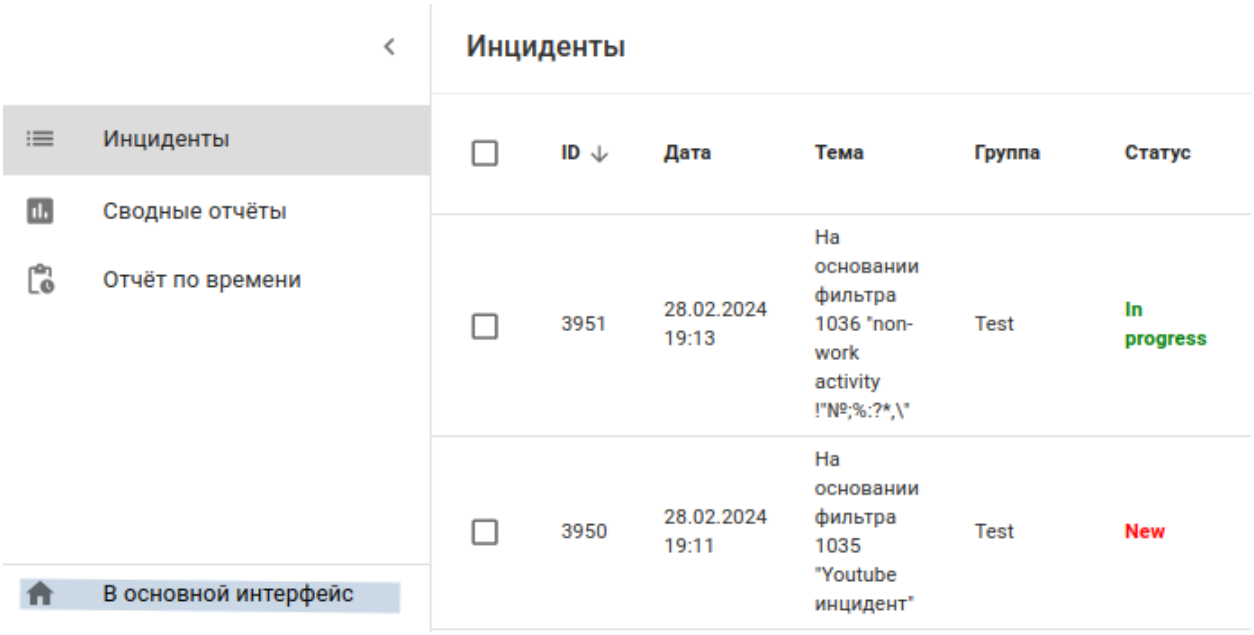
Для входа в консоль:

1. Перейдите в раздел **Адмнин**.
2. Выберите **Инциденты**.

В новой вкладке браузера откроется консоль управления инцидентами:



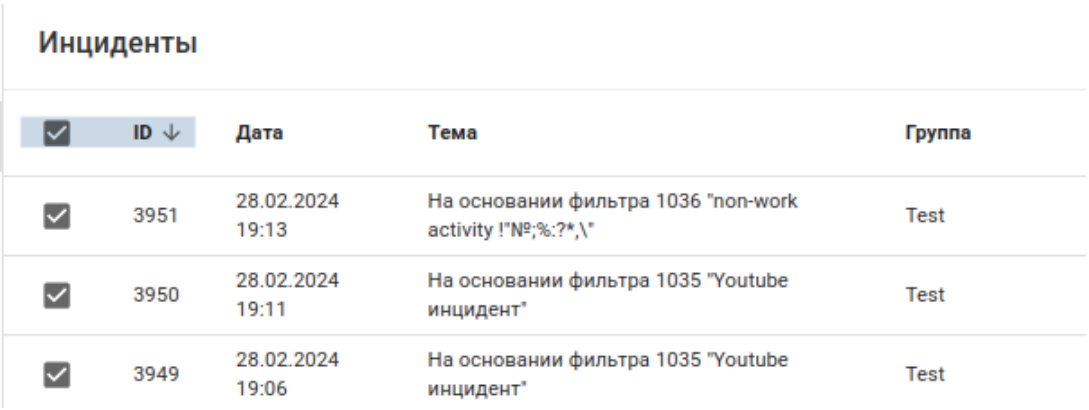
Для выхода из консоли нажмите **В основной интерфейс** в левом нижнем углу:



Список инцидентов

По умолчанию консоль открывается на странице **Инциденты**, на которой отображена таблица с данными всех инцидентов.

Напротив каждого инцидента расположен чекбокс, который позволяет совершать с выбранной группой инцидентов действие *через меню Действие*. Поставьте флажки, если вы хотите посмотреть, изменить или удалить инциденты.

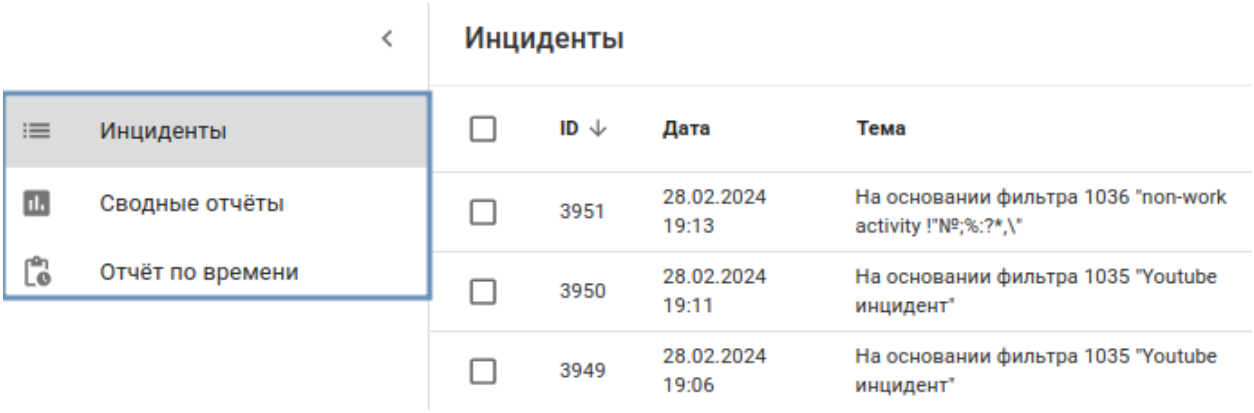


При клике на инцидент откроется *окно редактирования*. Чтобы открыть окно редактирования в новой вкладке, наведите курсор на конец строки инцидента и нажмите на появившуюся стрелку **Открыть в новом окне**.

Варианты просмотра

Варианты просмотра – это способы просмотра данных об инцидентах в системе.

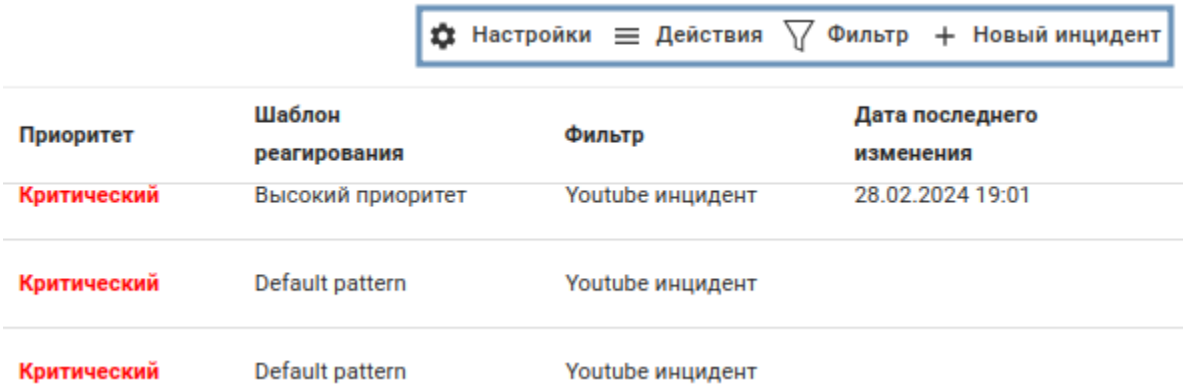
Варианты просмотра доступны в боковом меню:



- **Инциденты** – список всех инцидентов.
- *Сводный отчет* – общая статистика по инцидентам с возможностью использовать готовые отчеты и создавать новые.
- *Отчёт по времени* – список инцидентов в хронологическом порядке с указанием времени ожидания сервера, начала анализа и окончания обработки.

Меню управления

В правом верхнем углу страницы находится меню:

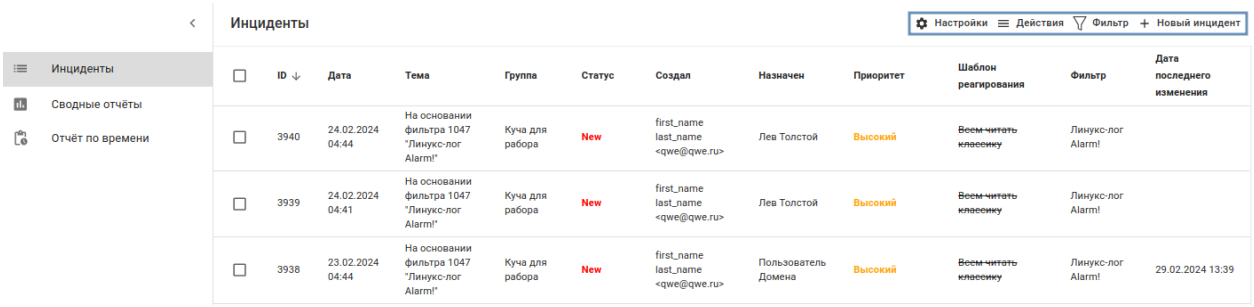


- *Настройки* – создание статусов, групп инцидентов, шаблонов реагирования.
- *Действия* – операции с инцидентами: экспорт, объединение и удаление инцидентов, изменение статуса и других атрибутов.
- *Фильтр* – поиск инцидентов в системе с помощью фильтров.
- *Новый инцидент* – создание нового инцидента вручную.

4.4.2 Меню управления

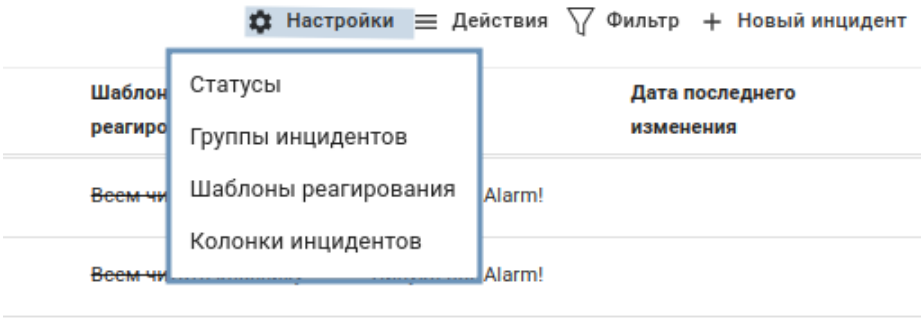
- *I. Настройки*
  - *Статус*
  - *Группы инцидентов*
  - *Шаблон реагирования*
  - *Дополнительные настройки*
    - *Удаление настройки*
- *II. Действия*
- *III. Фильтр*

Меню управления консолью инцидентов располагается в верхнем правом углу страницы.



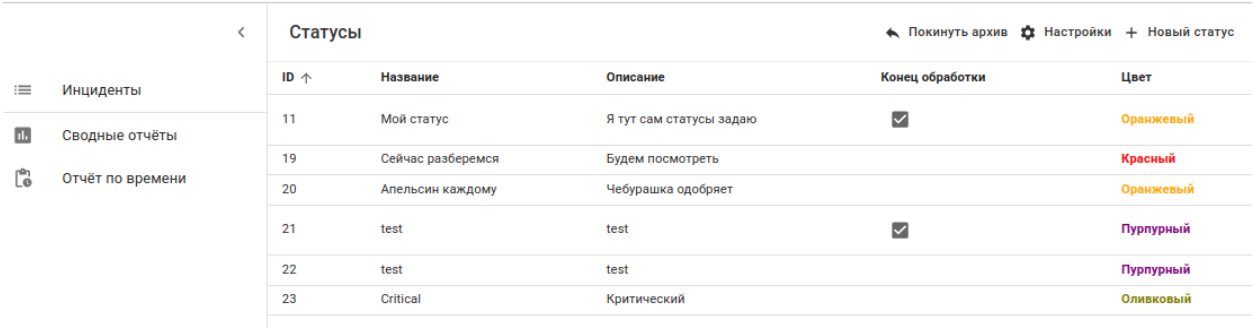
I. Настройки

В разделе **Настройки** вы можете скрыть лишние колонки из таблицы инцидентов; изменить или создать статусы, группы инцидентов и шаблоны реагирования.



Статус

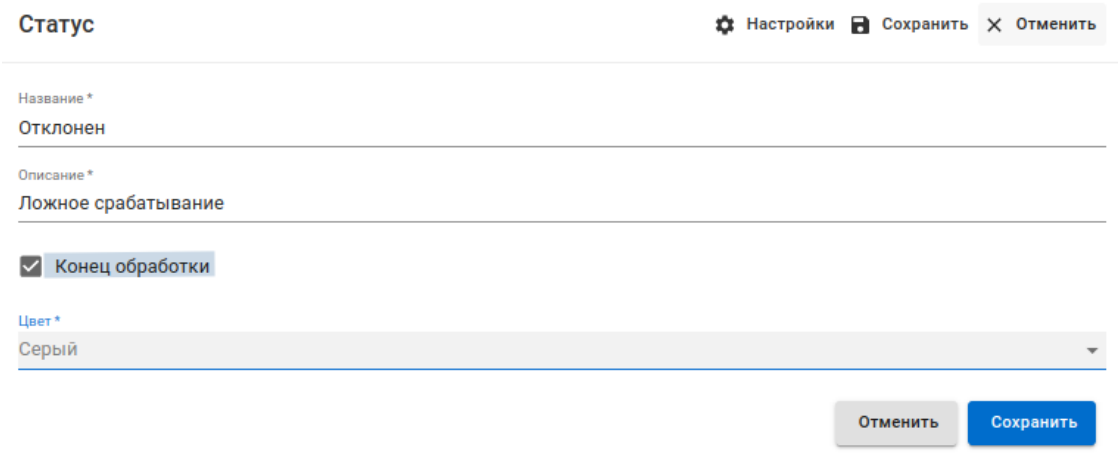
Используйте настройку для создания и редактирования статусов.



По умолчанию установлен только статус *New*. Вы можете его изменить. Для этого нажмите на статус и отредактируйте его, например измените *New* на *Новый*. После сохранения изменений обновленный статус появится в списке.

Чтобы создать остальные статусы вроде «В работе», «Закрыт», «Отклонен»:

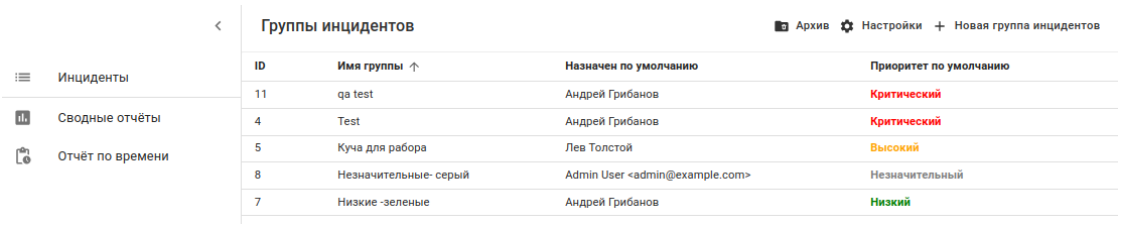
1. Нажмите + **Добавить статус**.
2. Заполните поля **Название** и **Описание**, выберите цвет.
   - Если статус указывает на завершение расследования инцидента, установите флажок в чекбоксе **Конец обработки**:



   Параметр **Конец обработки** поможет при создании отчетов по закрытым инцидентам. Например, можно создать статус *Отклонен* для ложных срабатываний и отметить его как **Конец обработки**. Такой подход позволит отслеживать все завершенные инциденты вне зависимости от результата расследования.
3. Сохраните изменения.

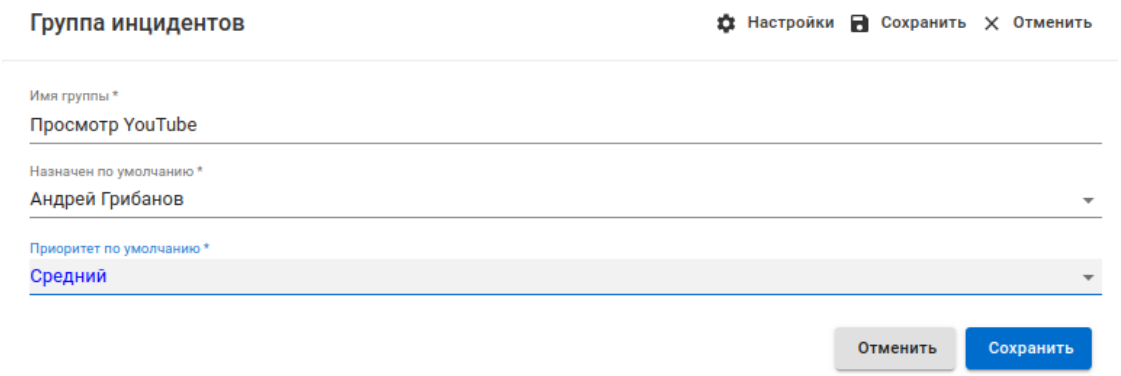
Группы инцидентов

Эта настройка позволяет создать группы инцидентов, например *Утечка информации* или *Нерегламентированный доступ*. По умолчанию инциденты входят в группу *Defaul group*.



Чтобы создать группу:

1. Нажмите на + **Добавить новую группу инцидентов**.
2. Заполните поля **Название**, **Назначен по умолчанию**, **Приоритет по умолчанию**.
   - В списке **Назначен по умолчанию** выберите администратора, который будет расследовать инцидент. Администраторы приведены в списке по указанным имени и фамилии.

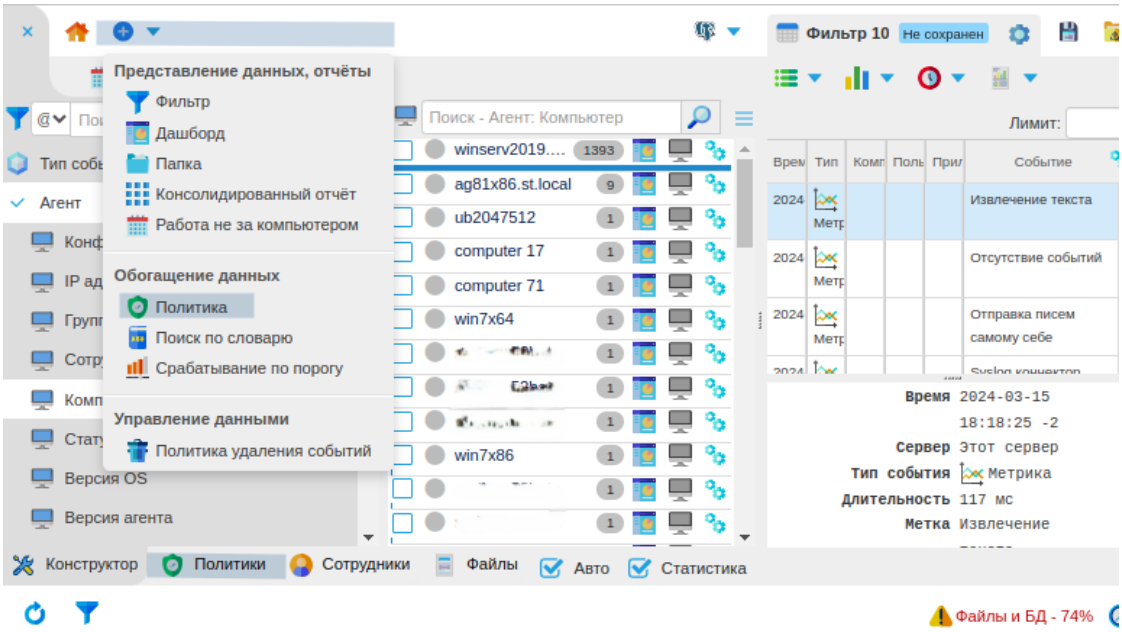


3. Сохраните изменения.

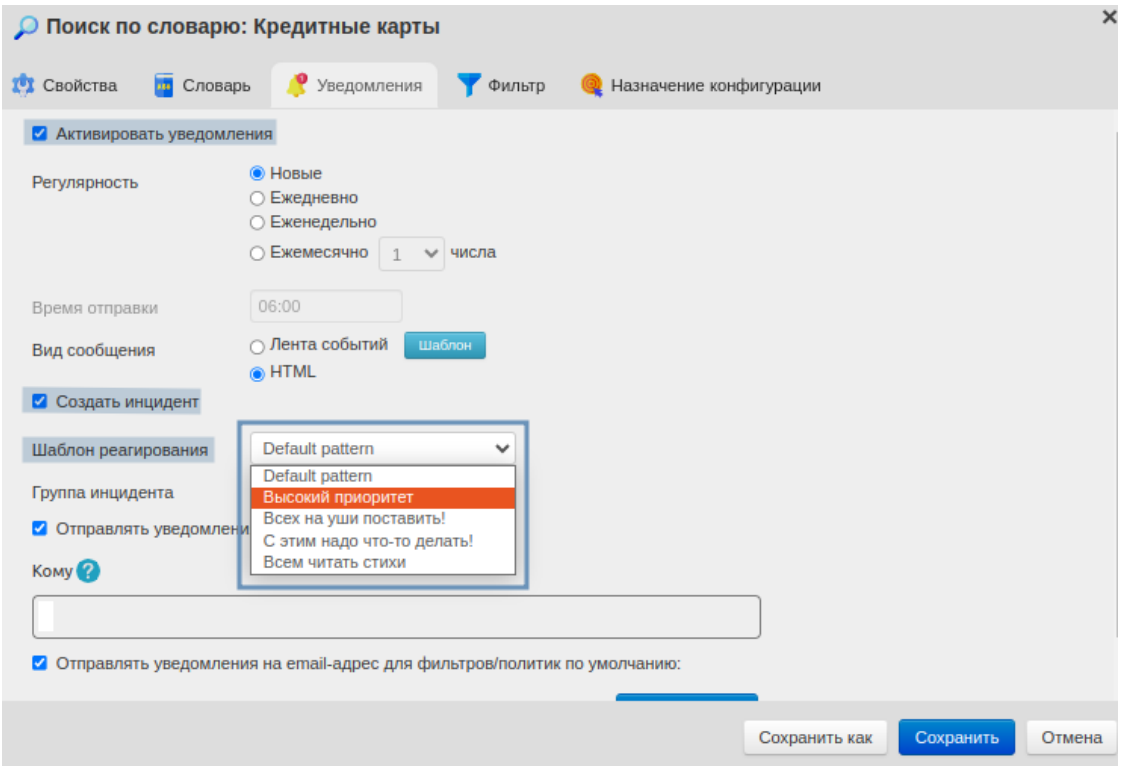
Группу можно отредактировать. Для этого нажмите на группу в списке и внесите изменения.

Чтобы изменить применить группу к политикам:

1. Верните в основной интерфейс.
2. Перейдите во вкладку **Политики** или создайте новую политику через + **Создать** → **Политика**.



3. Найдите политику и перейдите во вкладку **Уведомления**.
4. Убедитесь, что поставлены флажки **Активировать уведомления** и **Создать инцидент**.
5. Выберите группу в **Группе инцидентов**.

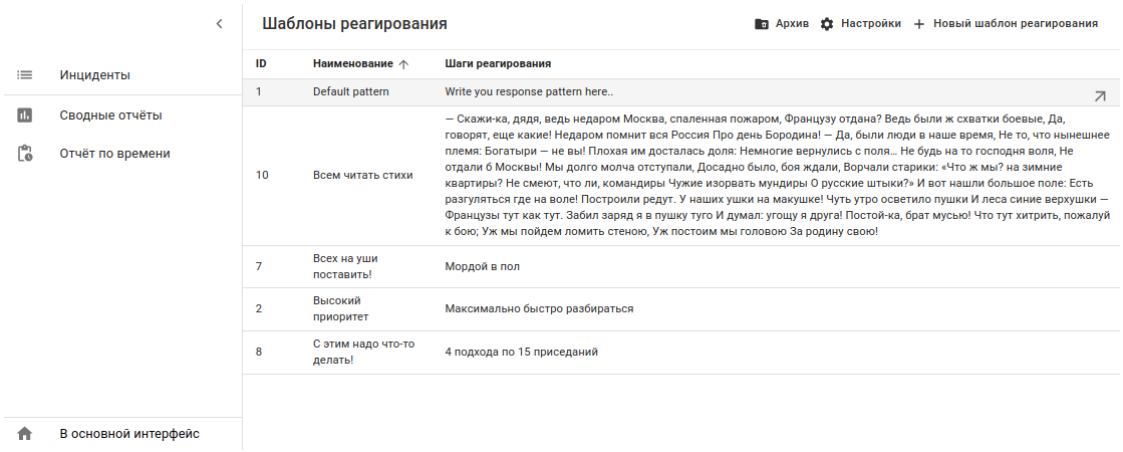


После этого в группу будут входить инциденты, которые автоматически регистрируются при реакции политики на действия пользователя.

Добавить или изменить группу для конкретного инцидента можно в консоли на странице *редактирования инцидента*.

Шаблон реагирования

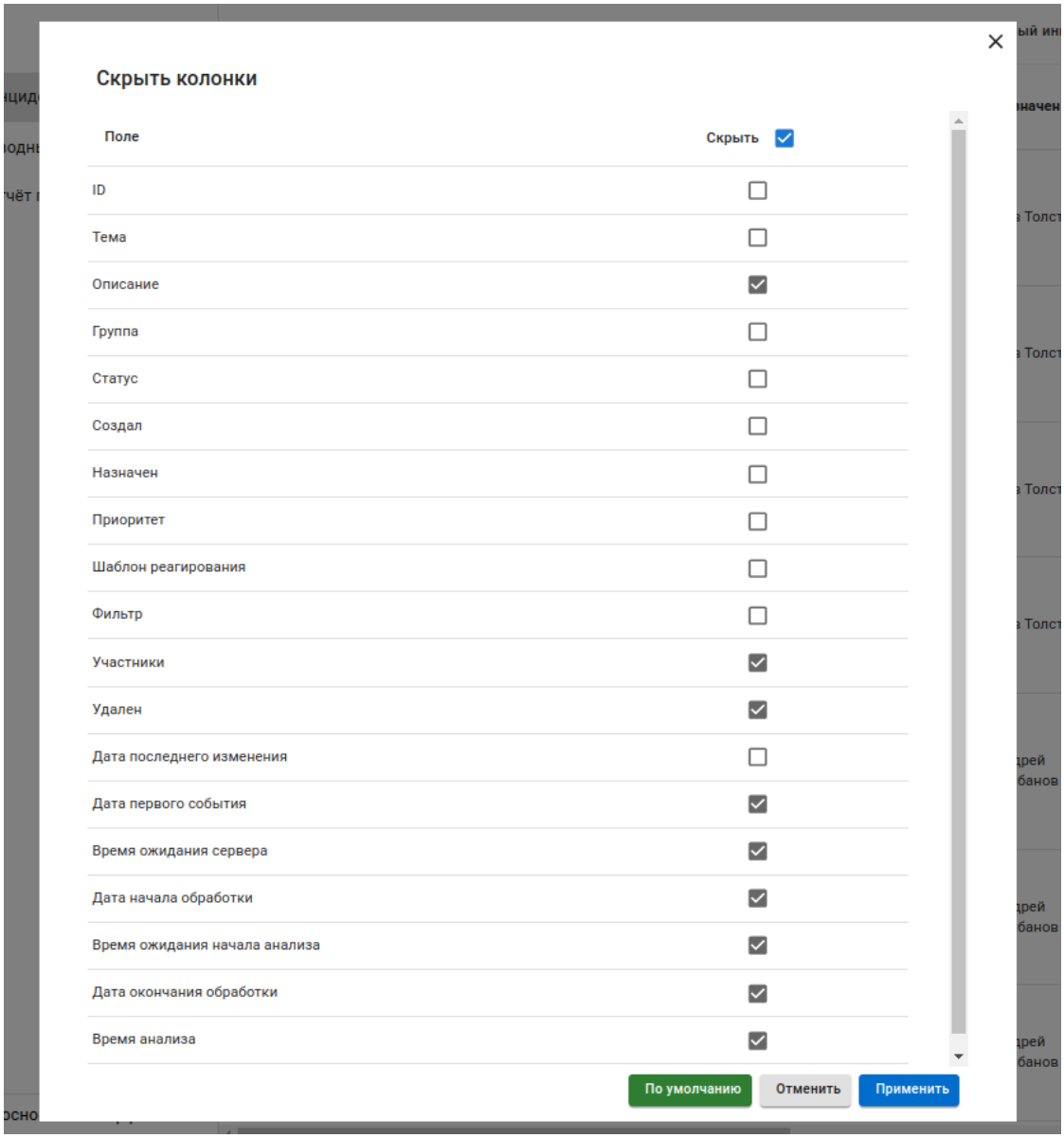
В шаблон можно добавить инструкции по решению проблемы в соответствии с регламентами вашей организации.



Изменить шаблон можно так же, как группу: на странице политики или инцидента.

Дополнительные настройки

В **Настройках** можно задать **Колонки инцидентов**. Выберите из списка только те колонки, которые вы хотите скрыть на странице **Инциденты**:



Удаление настройки

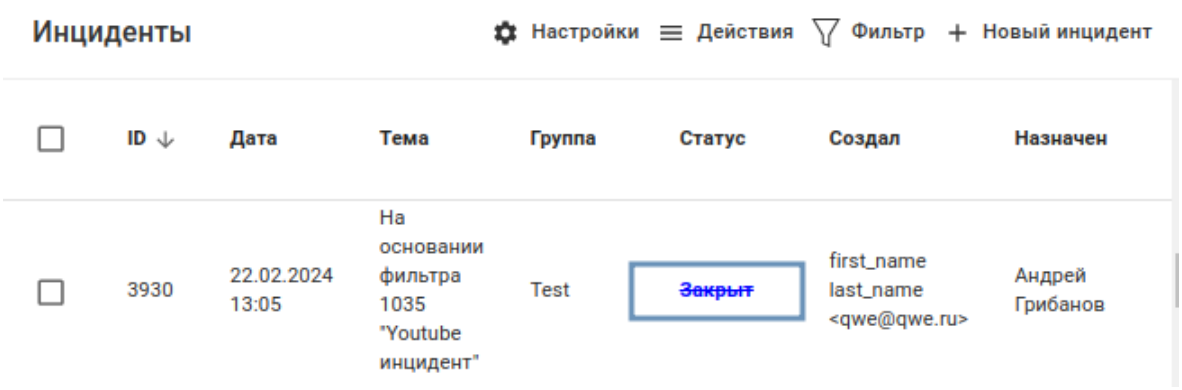
Чтобы удалить в настройке статус, шаблон или шаблон реагирования:

1. Откройте **Настройки**.
2. Выберите настройку и атрибут.
3. Нажмите **Удалить**.

Примечание: При удалении атрибут будет перенесен в **Архив**.

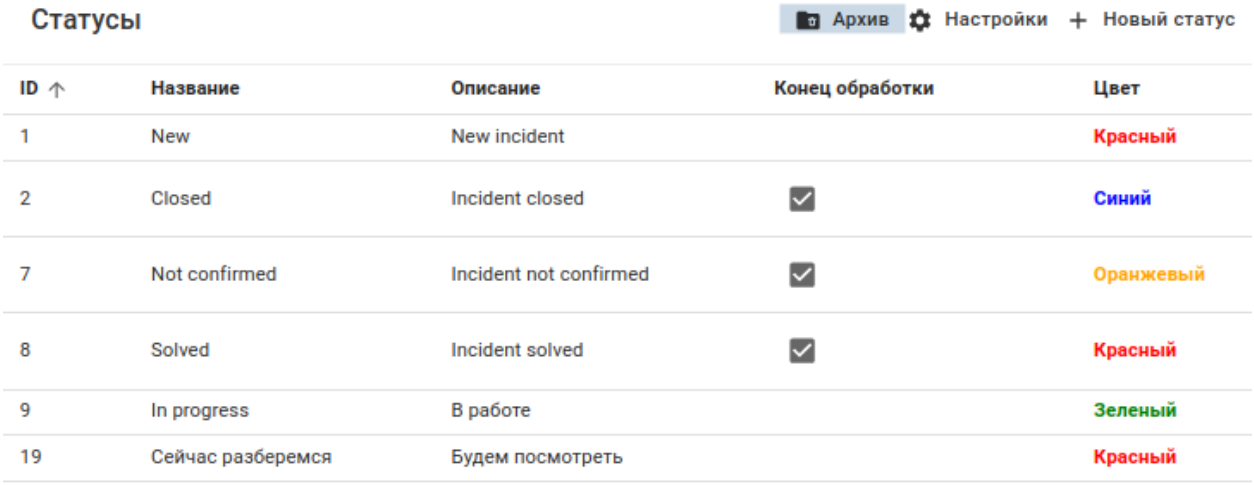
Например, удалите статус *Закрыт*: **Настройки** → **Статусы** → **Закрыт** → **Удалить**.

Если после удаления атрибут все еще отображается в списке, обновите страницу.



Архив

Архив находится на странице настройки в верхнем правом углу:



Чтобы восстановить атрибут:

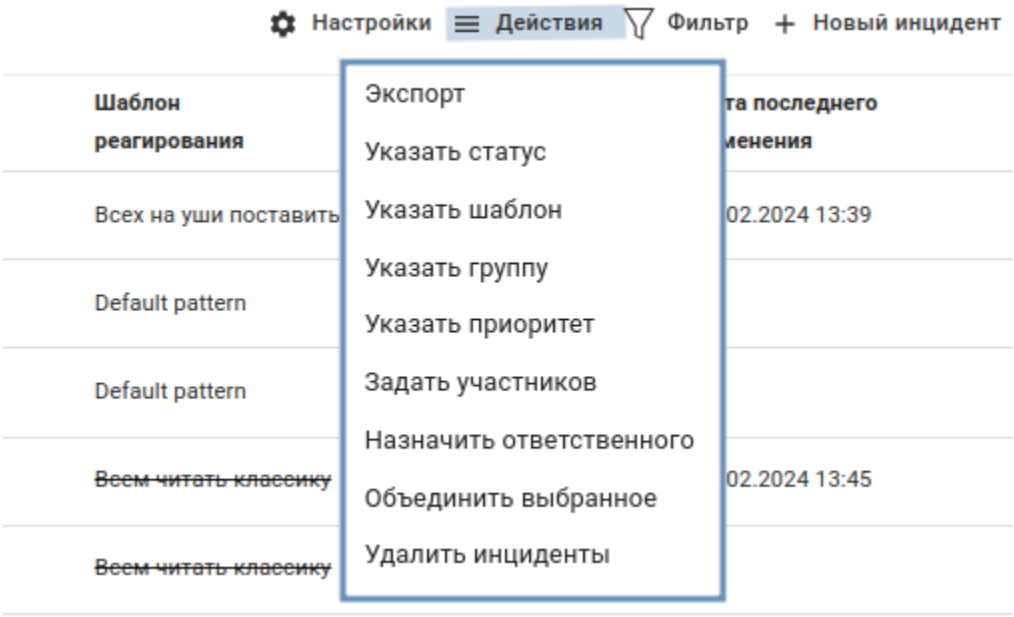
1. Откройте **Архив**.
2. Выберите атрибут.
3. Снимите флажок с чекбокса **Удален**:

Для удаления всех атрибутов из архива *используйте команды*.

II. Действия

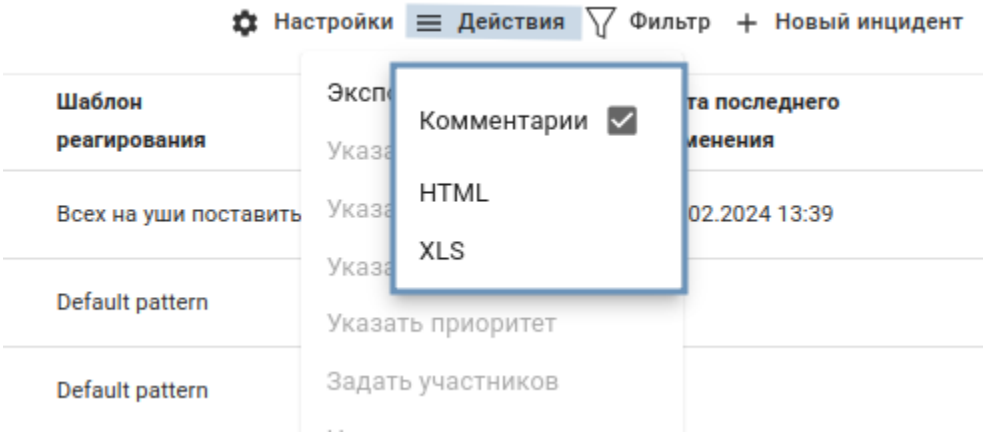
В разделе **Действия** доступны операции с инцидентами.

По умолчанию доступен только **Экспорт**. Для активации остальных действий поставьте флажок напротив отдельных инцидентов или колонки **ID** для выбора всех инцидентов. Действие будет применено только к выбранным инцидентам.



Экспорт

Экспорт создает файл со списком инцидентов без комментариев в форматах xls или html. При установке флажка **Комментарий** выгруженные инциденты будут содержать все комментарии.



При установке флажков напротив отдельных инцидентов в файл будут выгружены выбранные инциденты. Если вы примените *фильтр*, то экспортируются только отфильтрованные инциденты.

Указать: статус, шаблон, группу, приоритет

Эти опции изменяют соответствующие атрибуты у выбранных инцидентов.

Задать участников

Позволяет добавить участников инцидента.

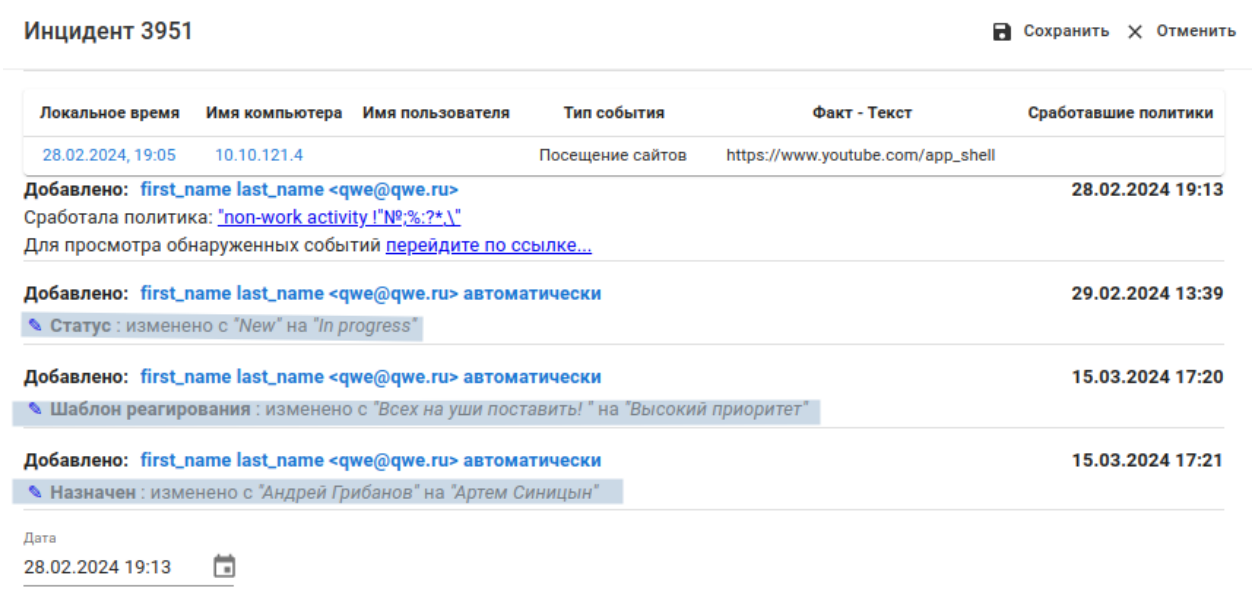
Примечание: Участник инцидента – это пользователь или группа пользователей, прямо или косвенно связанных с событием. По умолчанию указывается пользователь события, на основе которого был создан инцидент.

Администратор может *добавить в инцидент других участников*. Если у инцидента несколько участников, их имена указаны в поле **Участник** в алфавитном порядке.

Назначить ответственного

Опция позволяет выбрать администратора консоли для расследования инцидента.

Все изменения отображаются в истории изменений на странице инцидента.



Объединить инциденты

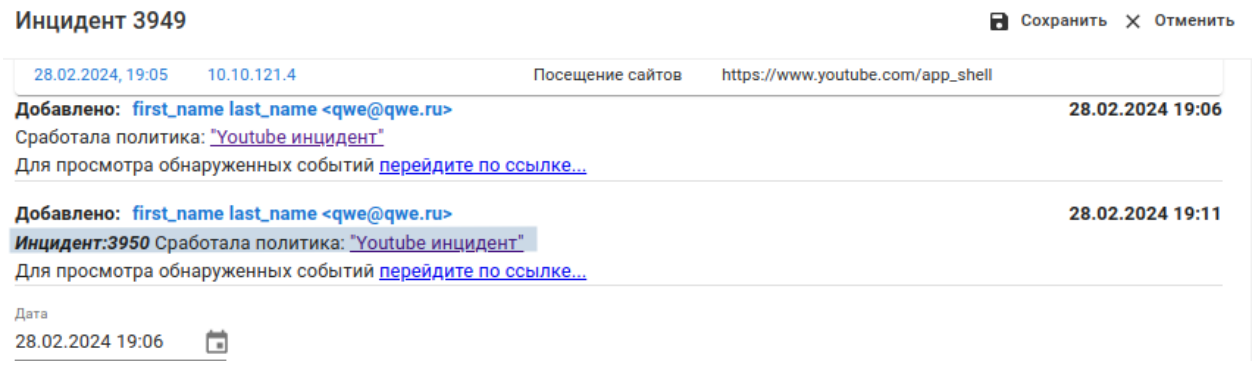
Объединяет два и более инцидента в один.

Чтобы объединить инциденты:

1. Поставьте галочки напротив инцидентов, которые хотите объединить.
2. Нажмите **Объединить инциденты**.

Вы можете объединить похожие инциденты. Например, загрузки файлов на облачных хранилища.

При объединении в списке останется самый первый инцидент, а более поздние отправятся в архив. Информация о более поздних инцидентах будет перенесена на страницу первого инцидента. На этом скриншоте информация об инциденте *3950* появилась на странице инцидента *3849*:



Удалить инциденты

Удаляет в архив выбранные инциденты.

См.также:

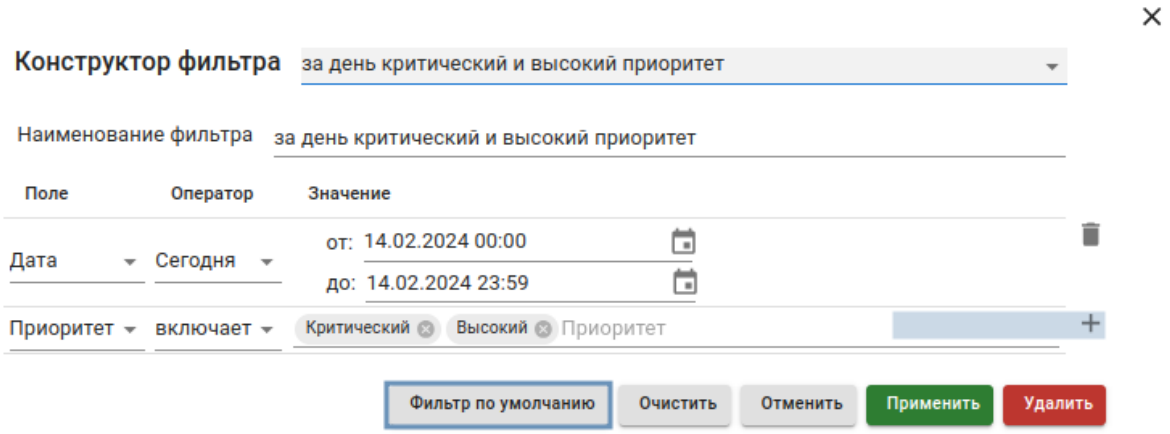
- *Навсегда удалить инциденты из архива*
- *Посмотреть удаленные инциденты*

III. Фильтр

В разделе **Фильтр** можно создать и сохранить фильтр для выборочного просмотра инцидентов.

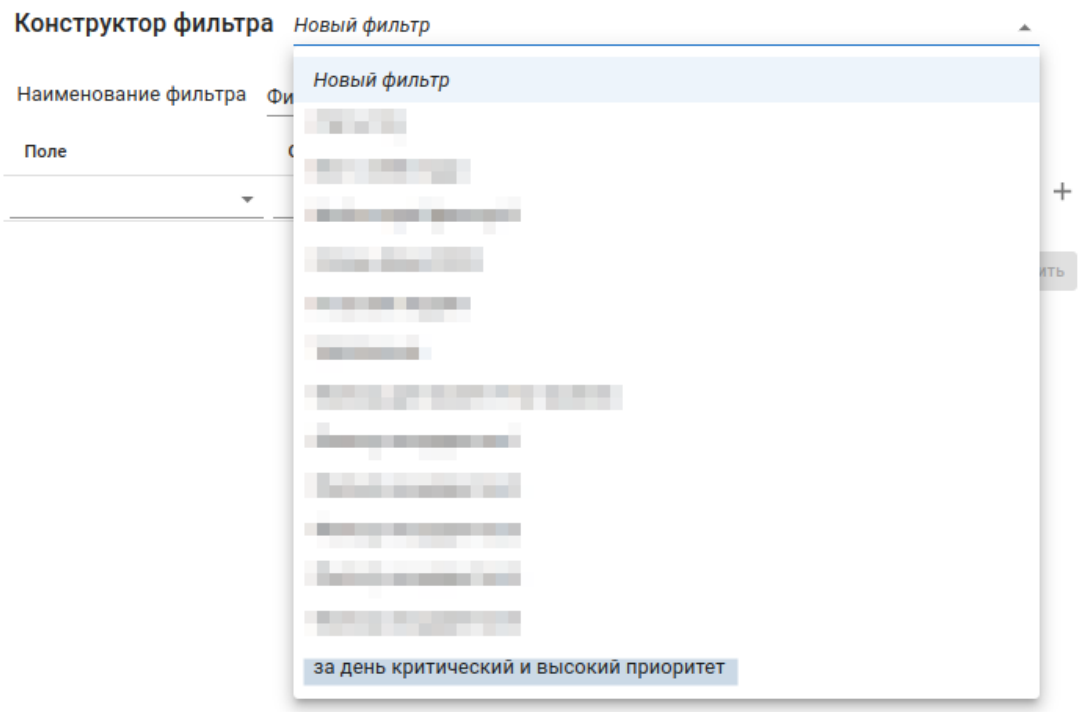
Чтобы создать фильтр:

1. Выберите **Новый фильтр** в **Конструкторе фильтра**.
2. Задайте название в поле **Наименование фильтра**.
3. Выберите атрибут для фильтрации в **Поле**, например **Приоритет**.
   - Добавить новый атрибут можно с помощью значка +.
   - При клике на кнопку **Фильтр по умолчанию** фильтр будет автоматически применяться к инцидентам, в том числе при повторном входе в консоль.



4. Нажмите **Сохранить**.
   - Для разового использования без сохранения нажмите **Применить**.

Чтобы применить сохраненный фильтр, выберите его из списка в **Конструкторе фильтров**:



Чтобы отменить действие фильтра:

1. Убедитесь, что в фильтре не стоит флажок **Фильтр по умолчанию**.
2. Перейдите из консоли в основной интерфейс.
3. Вернитесь обратно в консоль.

4.4.3 Работа с инцидентами

- *Новый инцидент*
  - *Создание инцидента из консоли*
  - *Автоматическое создание инцидента*
  - *Добавление инцидента из основного интерфейса*
- *Операции с инцидентами*
  - *Редактирование*
  - *Удаление*

Новый инцидент

Создать инцидент можно:

- вручную из консоли инцидентов;
- автоматически в результате срабатывания политики или фильтра;
- вручную из основного интерфейса.

Создание инцидента из консоли

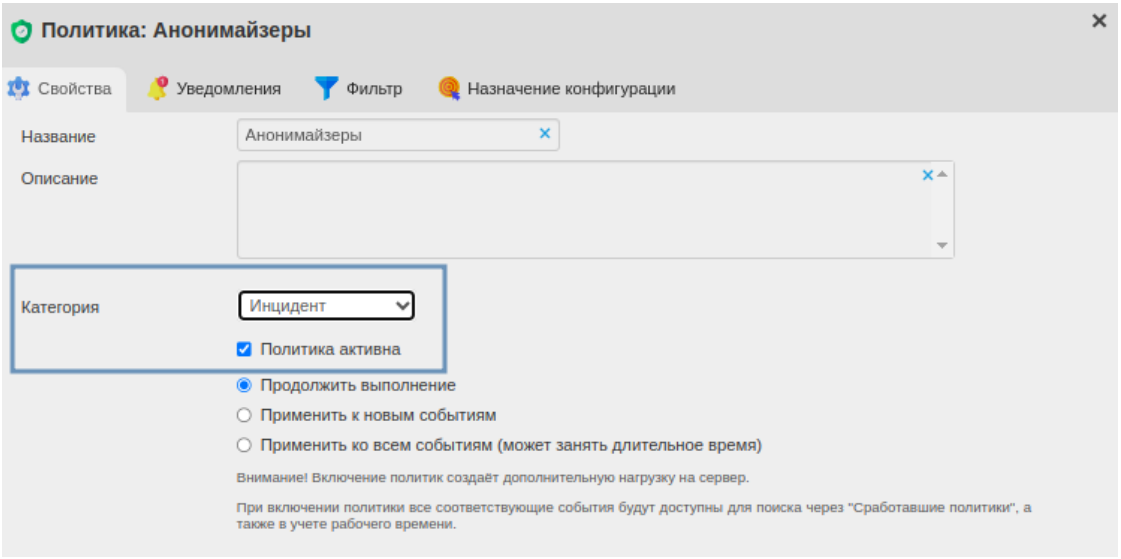
Чтобы создать инцидент из консоли, нажмите кнопку + **Создать инцидент** в верхнем правом углу. В открывшемся окне заполните все поля и нажмите **Сохранить**.

Автоматическое создание инцидента

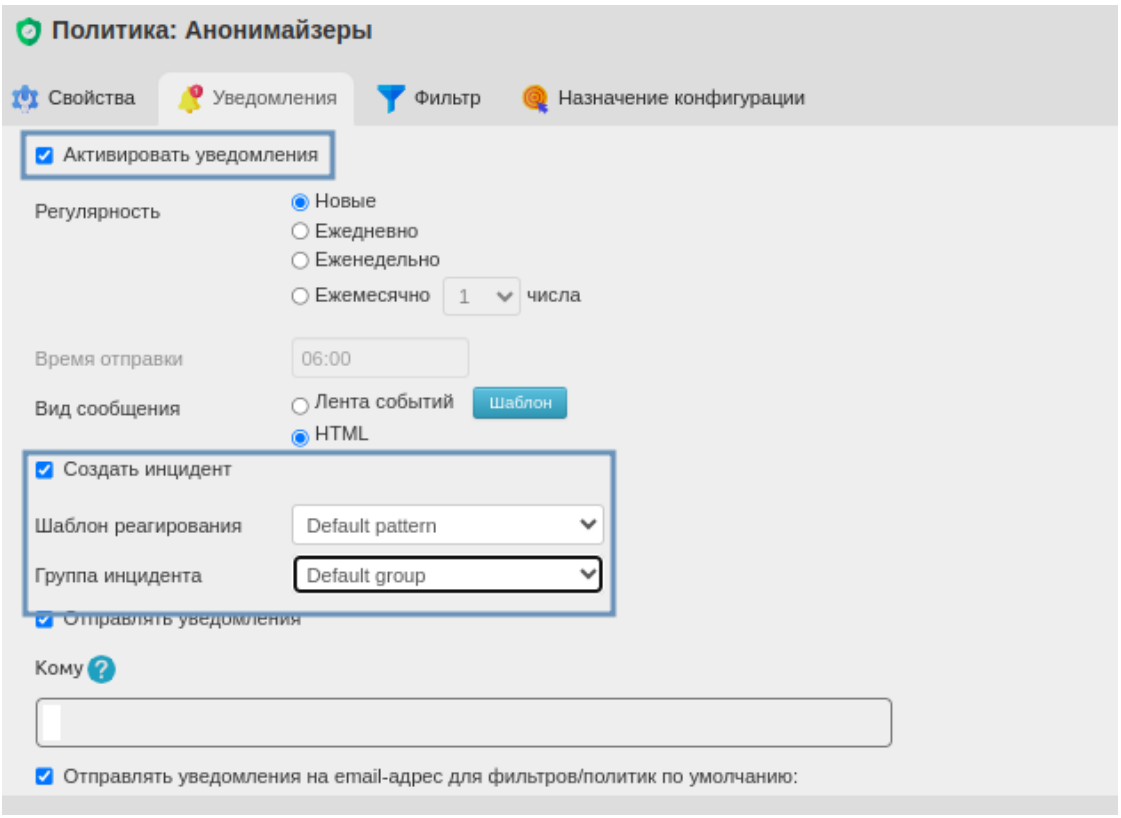
Инцидент может быть создан в результате срабатывания политики.

Чтобы добавить в политику инцидент:

1. В основном интерфейсе во вкладке **Политика** перейдите в папку *Политики*.
2. Выберите политику или *создайте новую*.
3. В окне политики во вкладке **Свойства** в поле **Категория** выберите **Инцидент**.
4. Включите опцию **Политика активна**.



5. Во вкладке **Уведомления** активируйте уведомления.
6. Укажите параметры реагирования на событие: шаблон реагирования и группу инцидентов.

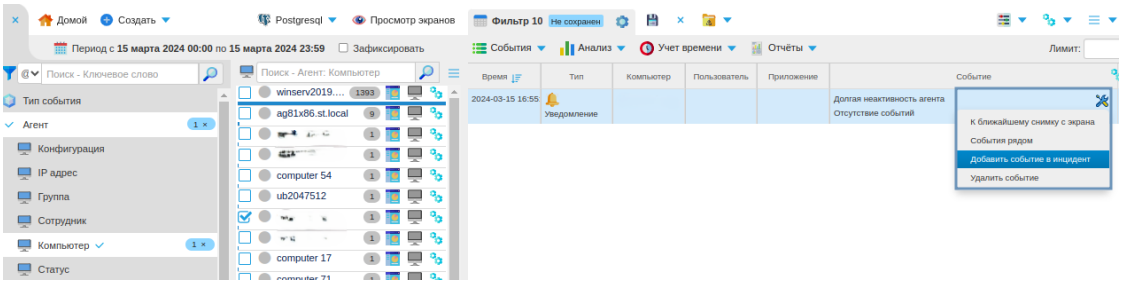


7. Сохраните политику.

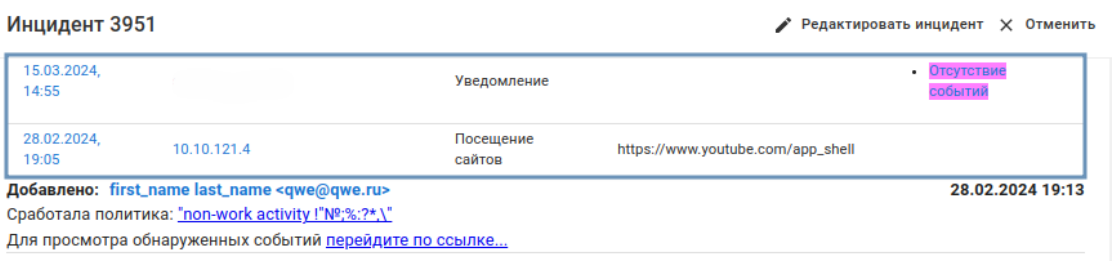
Добавление инцидента из основного интерфейса

Чтобы добавить инцидент или дополнить событием уже созданный:

1. В *Линзе событий* найдите событие.
2. Кликните на иконку ключа и в контекстном меню выберите пункт **Добавить событие в инцидент**.



3. Выберите инцидент или создайте новый в открывшемся окне. После этого откроется страница инцидента, на которой вы увидите добавленное событие:

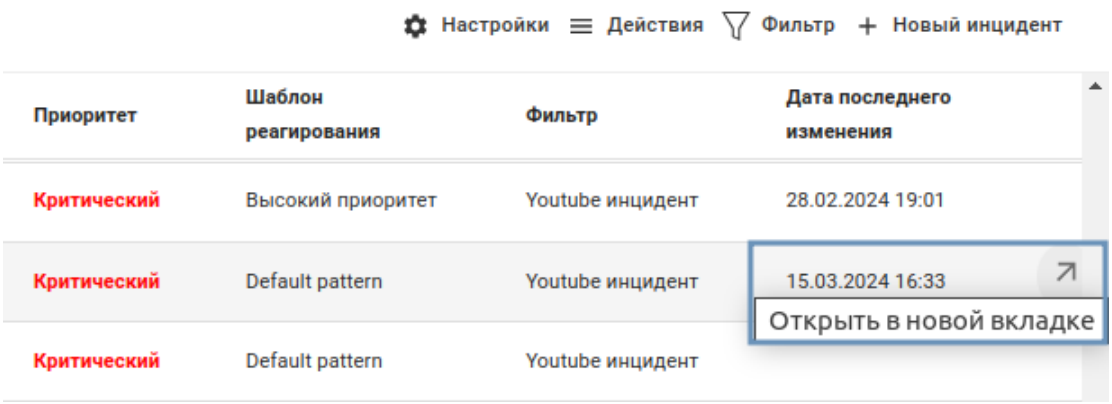


- При необходимости отредактируйте инцидент: измените статус, добавьте комментарии, участников, шаблон, группу и другие атрибуты.

Операции с инцидентами

При клике на инцидент открывается страница редактирования инцидента.

Чтобы открыть окно в новой вкладке, подведите курсор к последней колонке инцидента и нажмите на появившуюся стрелку:



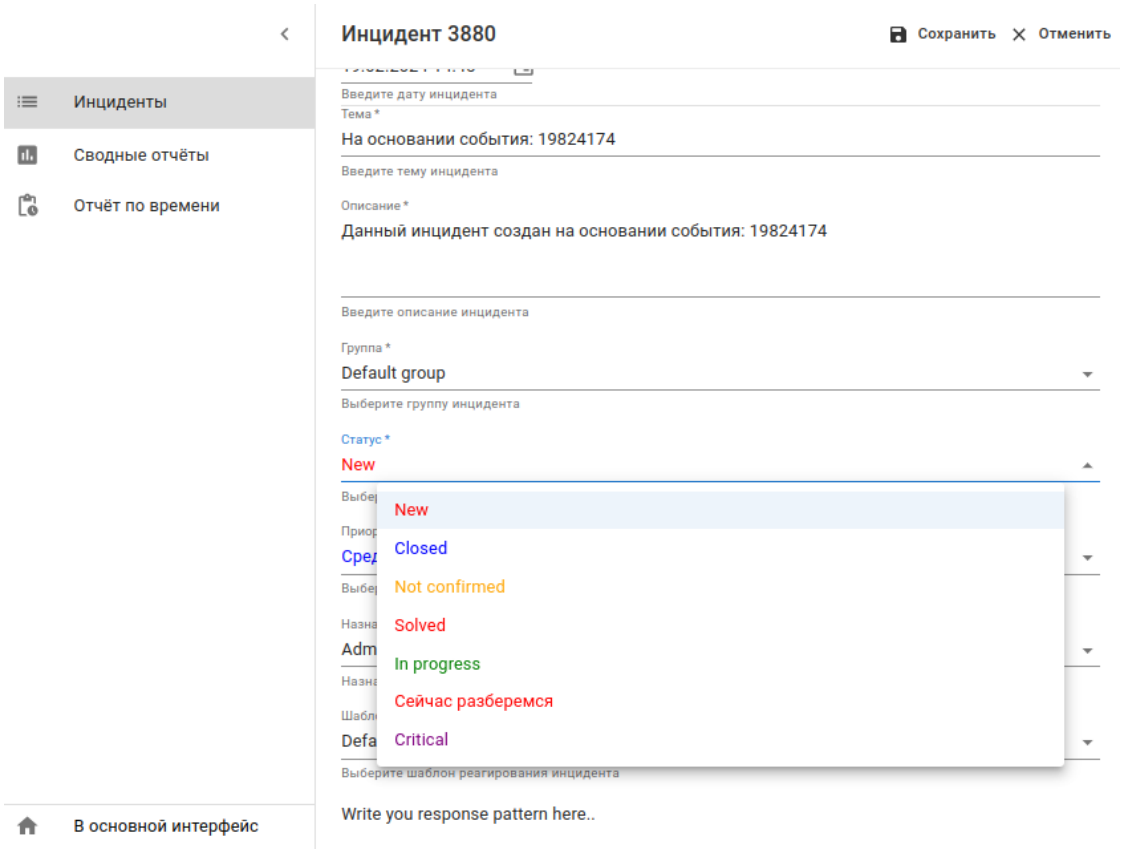
Редактирование

В окне редактирования инцидента вы можете изменять атрибуты инцидента:

- группу,
- шаблон реагирования,
- статус,
- участников,
- события,
- приоритет,
- ответственного,
- дату создания.

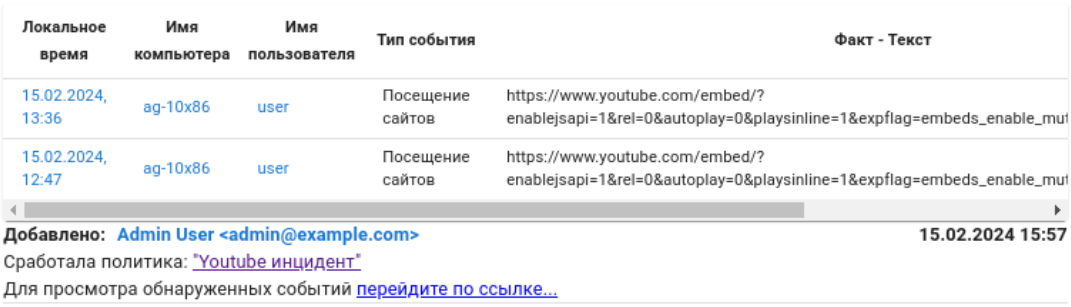
Чтобы изменить атрибут:

1. Кликните на поле атрибута.
2. Введите новые значения:



Кроме этого, у вас есть возможность:

- прикладывать файлы и оставлять комментарии;
- просматривать приложенные к инциденту скриншоты;
- посмотреть сработавшую политику и связанные с ней события за последние 12 часов:



- посмотреть группу событий в диапазоне +- 5 минут от события с помощью опции **Для просмотра обнаруженных событий перейдите по ссылке**:
- посмотреть историю изменений ответственных за индицент, атрибутов и статуса инцидента.

Удаление

При удалении инцидент перемещается в архив.

> **Внимание:** Восстановить инцидент из архива нельзя. Вы сможете просматривать инцидент, но не сможете изменить. Поэтому перед удалением убедитесь, что это действительно необходимо.

Чтобы удалить инцидент:

1. Выберите в боковом меню **Инциденты**.
2. Поставьте флажок напротив инцидентов, которые вы хотите удалить.
3. В правом верхнем меню выберите **Действия** → **Удалить инциденты** и подтвердите удаление.

Удалить инциденты из архива можно с помощью *команд*.

4.4.4 Отчеты

- *Сводный отчет*
  - *Новый отчет*
    - *Как задать параметры отчета*
  - *Экспорт*
  - *Удаление*
- *Отчет по времени*

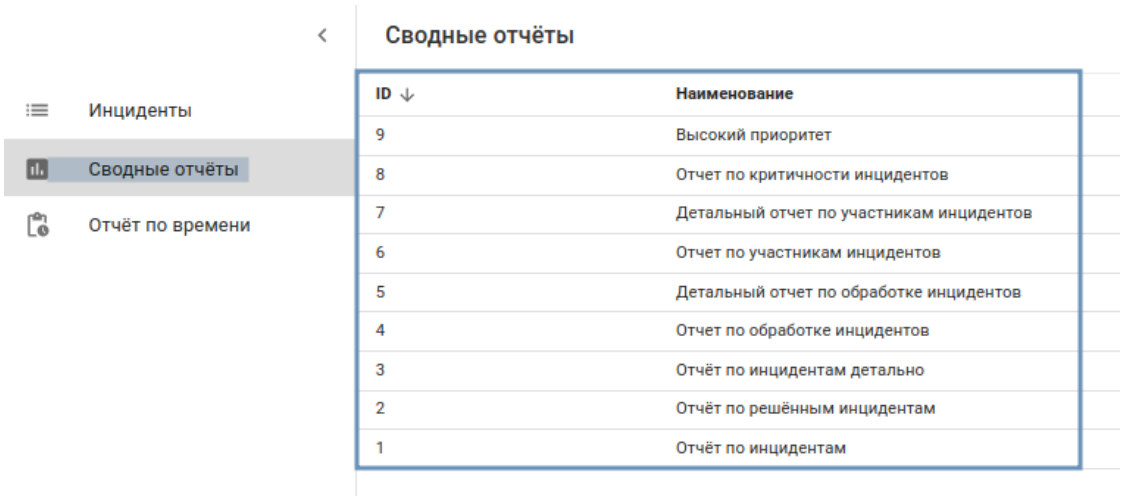
Отчеты позволяют получить информацию по инцидентам.

Выберите в левом боковом меню тип отчета:

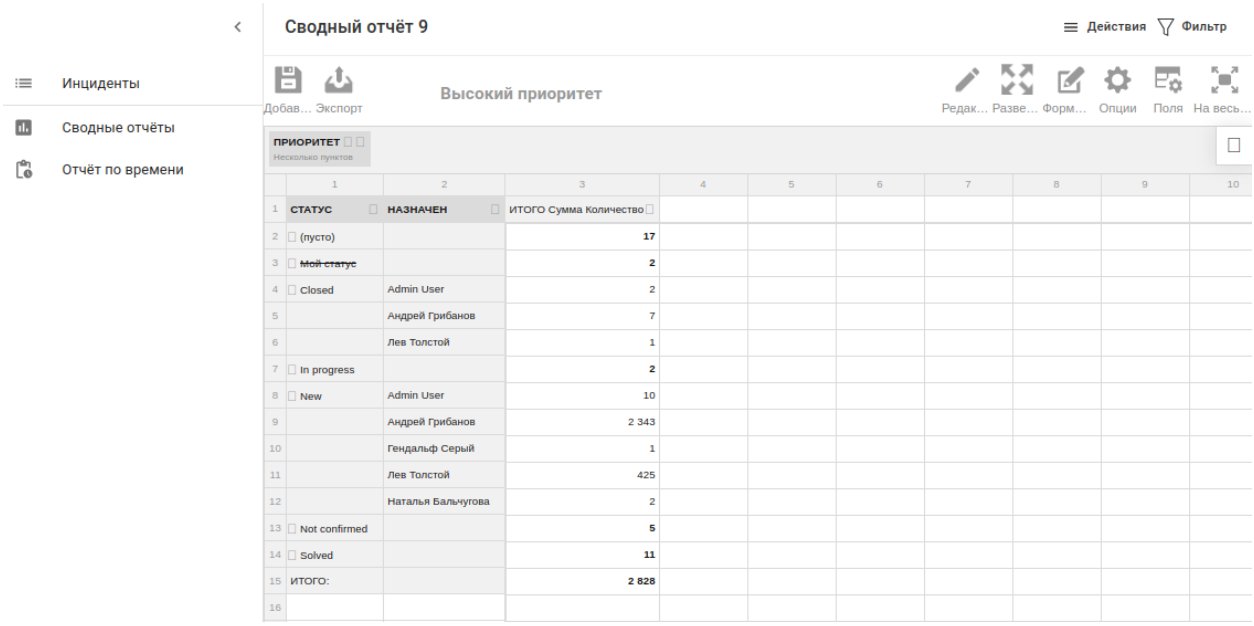
- **Сводные отчеты**,
- **Отчет по времени**.

Сводный отчет

После клика на **Сводные отчеты** вы увидите список предустановленных отчетов:



Нажмите на отчет, чтобы его открыть:

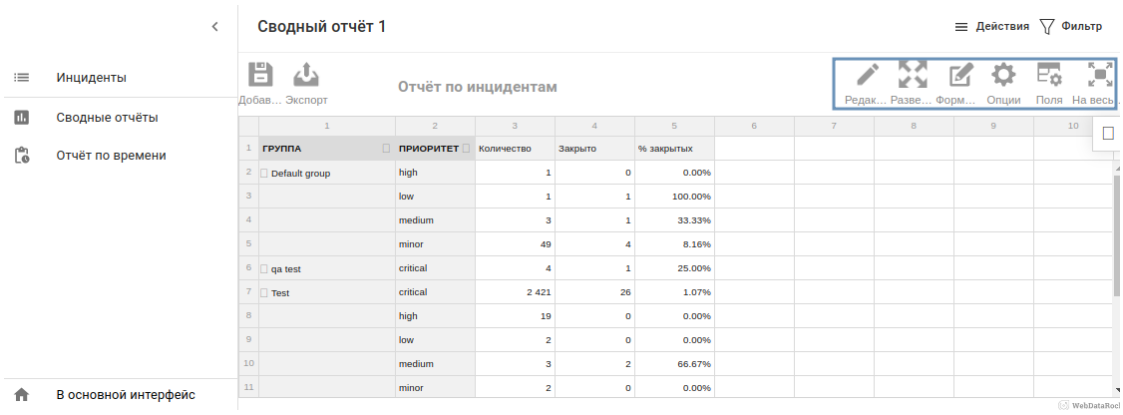


Примечание: Зачеркнутые ячейки означают, что атрибут был удален.

Новый отчет

Чтобы создать новый или отредактировать отчет:

1. В консоли инцидентов в разделе **Сводные отчеты** откройте готовый отчет или нажмите **Новый сводный отчет**.
2. В открывшемся окне задайте параметры нового отчета с помощью панели инструментов в верхнем правом углу:

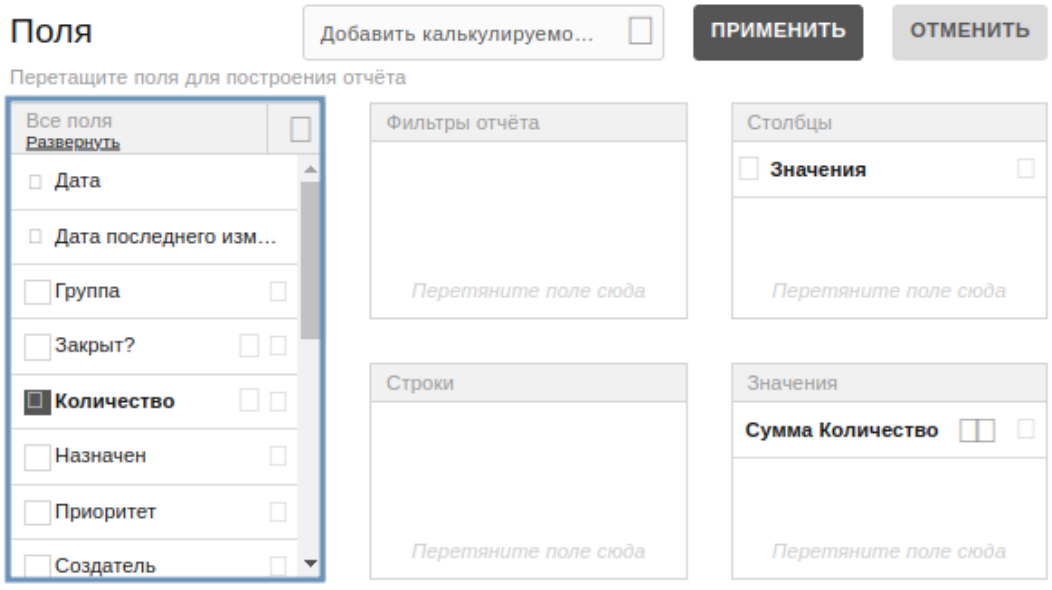


- **Редактировать**. Если вы владеете JSON, используйте этот инструмент для изменения полей отчета.
- **Свернуть**. Позволяет свернуть и развернуть часть полей для удобства просмотра.
- **Форматирование ячеек**. Задает формат ячеек.
- **Опции**. Позволяет добавить *Итог* и *Подытог*, изменить вид таблицы.
- **Поля**. Настройка полей таблицы.
- **На весь экран**. Просмотр таблицы на полном экране.

3. Сохраните изменения.

Как задать параметры отчета

1. На странице создания нового отчета кликните на иконку **Поля** в верхнем правом углу.
2. Посмотрите на раздел **Все поля** слева — это данные, которые могут быть включены в отчет.



3. Перетащите нужные поля в правую область, где есть разделы **Строки**, **Столбцы**, **Значения** и **Фильтры отчета**.

Распределите данные так:

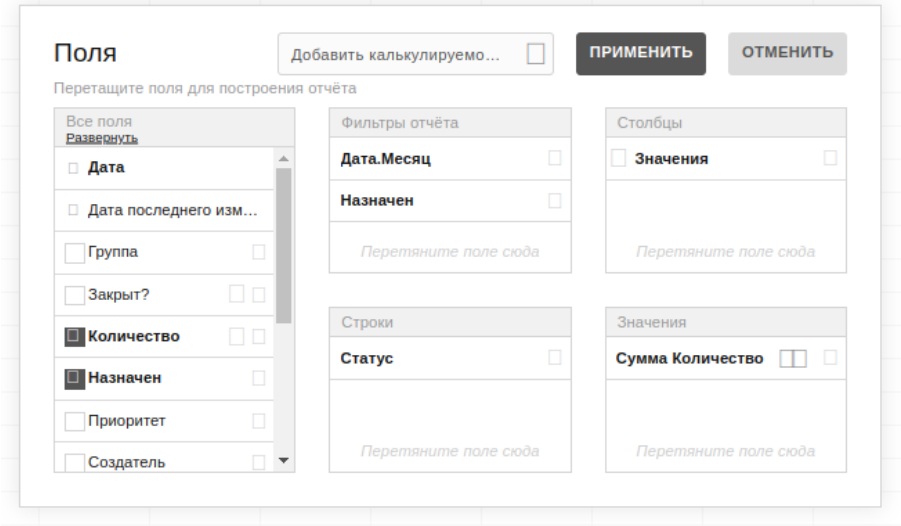
- **Фильтры отчета** — помогает выбрать данные, которые вы хотите увидеть в отчете, например, можно отфильтровать данные по дате или ответственному;
- **Строки** — задают название столбцов;
- **Столбцы** — задают значения;
- **Значение** — определяют формат значений, такие как сумма, количество, среднее.

4. Нажмите **Применить**.

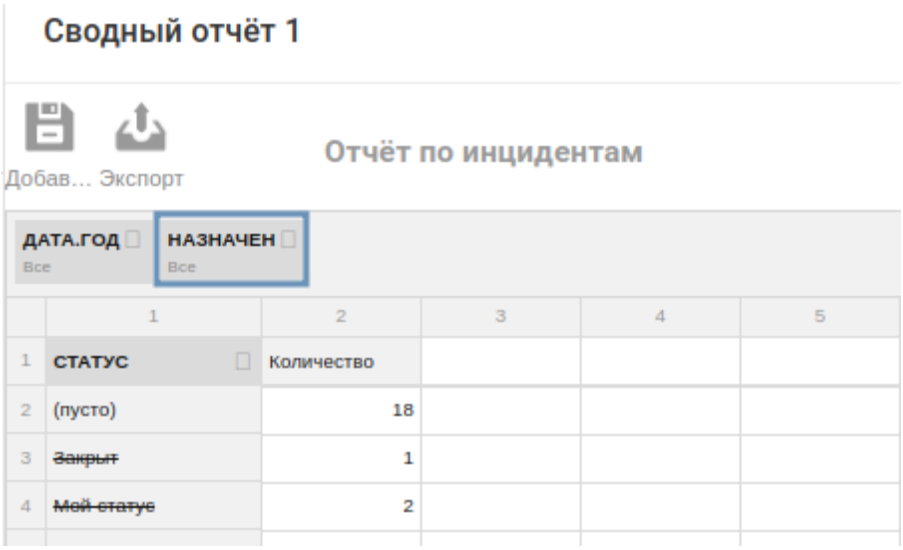
Пример

Количество задач администратора за месяц с распределением по приоритету и статусу.

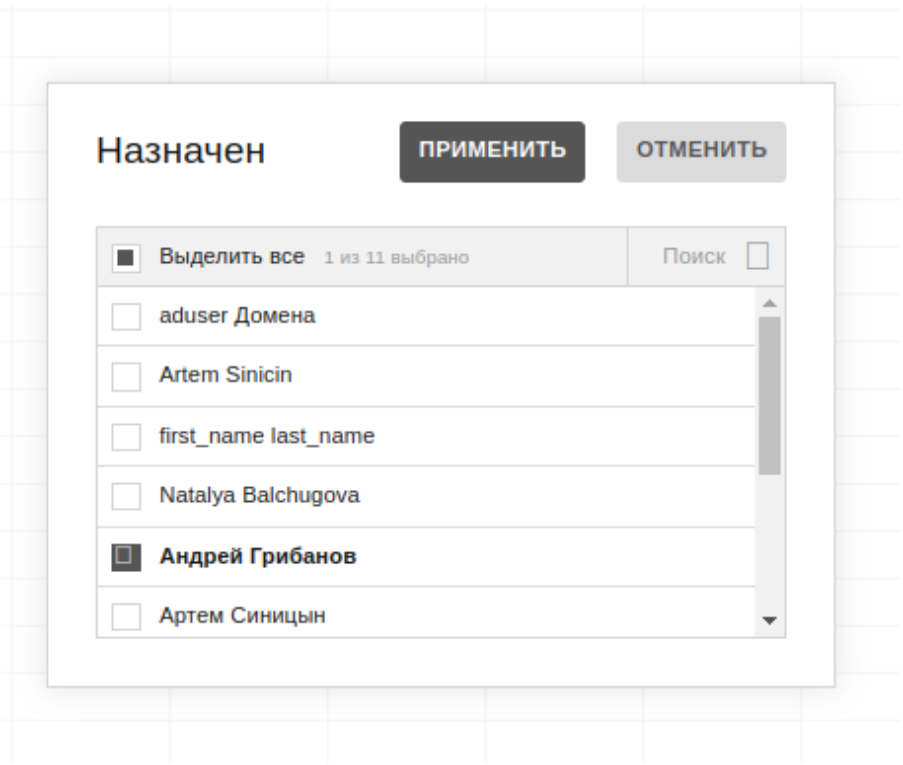
- добавьте в **Фильтры отчета** поля **Дата.Год** и **Назначен**;
- добавьте в **Строки** поле **Статус**;
- добавьте в **Значения** поле **Количество**;
- нажмите **Применить**:



- перейдите в шапке таблицы во вкладку **Назначен**:



- выберите администратора из списка:



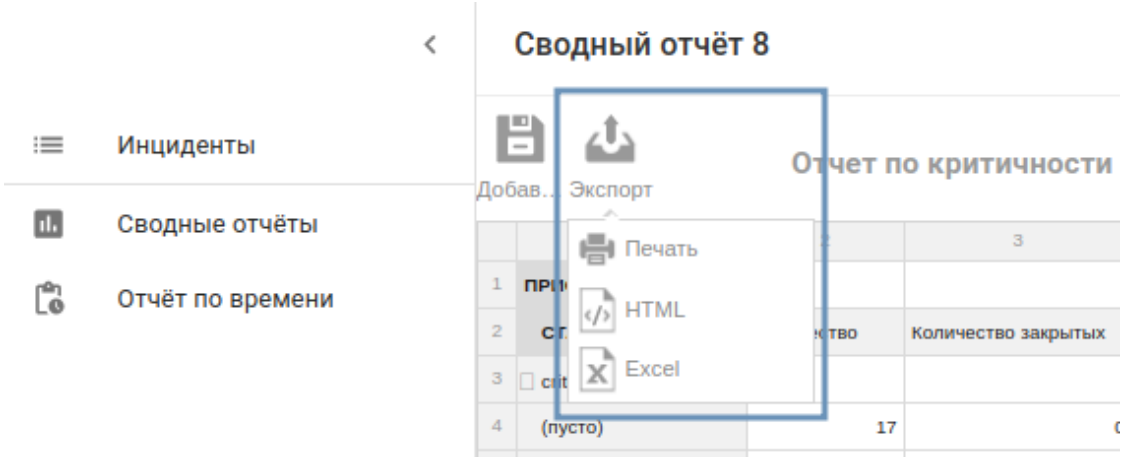
- таким же образом выберите месяц во вкладке **Год.Месяц**.

Готово! В таблице отобразится количество задач по статусам.

Экспорт

Чтобы выгрузить отчет:

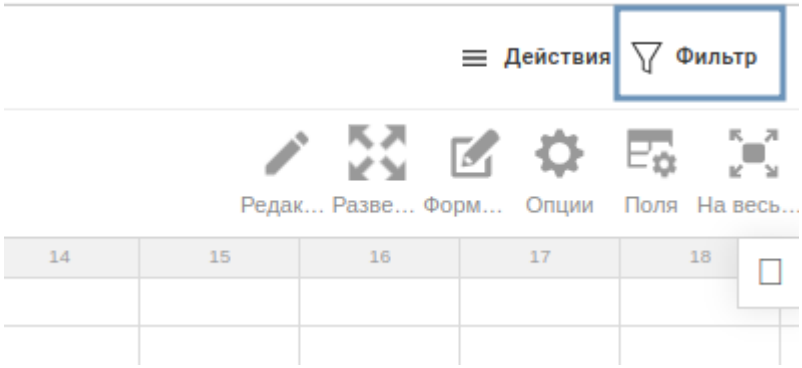
1. Нажмите кнопку **Экспорт** в окне просмотра отчета.
2. Выберите формат выгрузки: **Печать**, **HTML**, **Excel**.
   - **Печать** позволяет сохранить отчет в формате pdf.



Удаление

Удалить созданный отчет можно в окне редактирования:

1. Откройте отчет.
2. Нажмите кнопку **Фильтр** в правом верхнем углу.

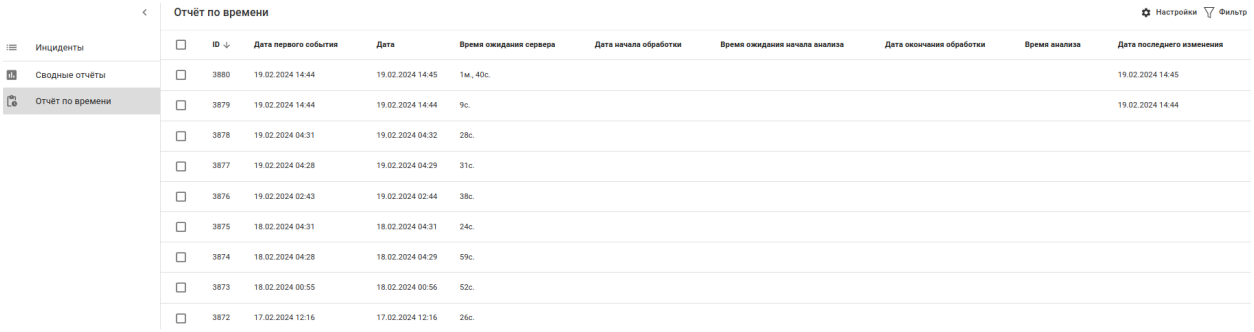


3. Нажмите кнопку **Удалить**.

Примечание: Предустановленные отчеты удалить нельзя.

Отчет по времени

Раздел **Отчет по времени** предоставляет информацию об инцидентах в хронологическом порядке:



Используйте отчет, чтобы узнать, сколько времени заняло расследование инцидента. Кроме этого, отчет показывает время между событием и созданием инцидента. Эти данные важны при большом объеме данных, когда система может отставать от сбора информации.

В таблице отчета указаны колонки:

- **дата первого события** – время первого события, которое привело к инциденту;
- **время создания инцидента** — время регистрации инцидента;
- **время обработки** — разница между временем события и временем создания инцидента;
- **время ожидания** — время с момента создания инцидента до его перехода из статуса **Новый** в другой;
- **в работе** — время, в течение которого инцидент находится в статусе **В работе**;
- **закрытие** — время перевода инцидента в статус **Конец обработки**;
- **время анализа** – разница времени между **В работе** и **Закрыто**.

Примечание: Если новый инцидент сразу переводится в статус **Закрыто**, время анализа указывается как 0.

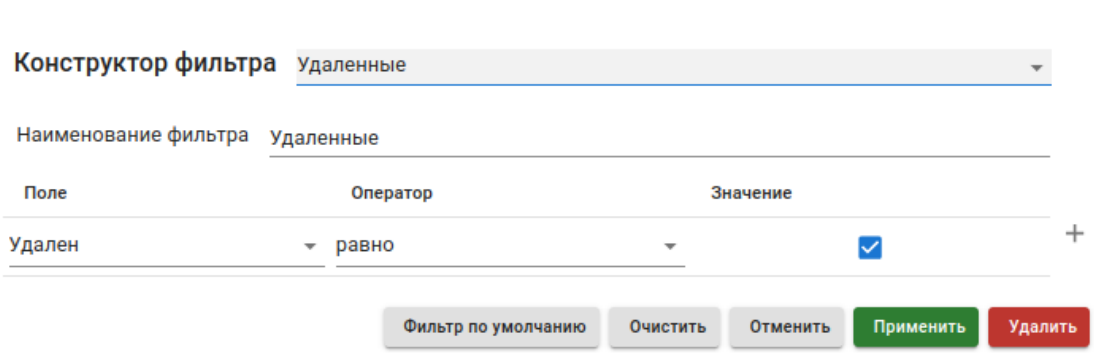
4.4.5 Архив

- *Просмотр инцидентов в архиве*
- *Удаление из архива*

Просмотр инцидентов в архиве

Посмотреть инциденты в архиве можно с помощью фильтра в консоли инцидентов.

1. Перейдите в меню в правом верхнем углу в **Фильтр**.
2. Создайте фильтр **Удаленные**:
   - выберите **Новый фильтр** в **Конструкторе фильтров**;
   - задайте название в поле **Наименование фильтра**;
   - выберите в **Поле** атрибут **Удален**.



3. Нажмите **Сохранить**.
4. Нажмите **Применить**.

После автоматической перезагрузки на странице отобразятся все удаленные инциденты.

Удаление из архива

Перейдите **Админ** → **Консоль терминала** и используйте команды для удаления информации из архива.

Удалить инциденты из архива консоли инцидентов:

```
ibatyr incident_clean incident
```

Вместе с инцидентами удалятся записи в таблице с инцидентами, комментарии, участники, связи с событиями.

Примечание: Система удаляет только атрибуты, которые не связаны ни с одним из инцидентов, включая инциденты в архиве. Если статус, шаблон или группа указаны в инцидентах, он не удалится.

Удалить статусы:

```
ibatyr incident_clean status
```

Удалить группы:

```
ibatyr incident_clean group
```

Удалить шаблоны:

```
ibatyr incident_clean responsepattern
```

Предупреждение: Нельзя удалить статус **New**, дефолтные группу и шаблон.

Очистить весь архив:

```
ibatyr incident_clean all
```

Примечание: При очистке всего архива выполняются все приведенные выше операции.

4.4.6 Контроль действий администратора

Права и группы доступа

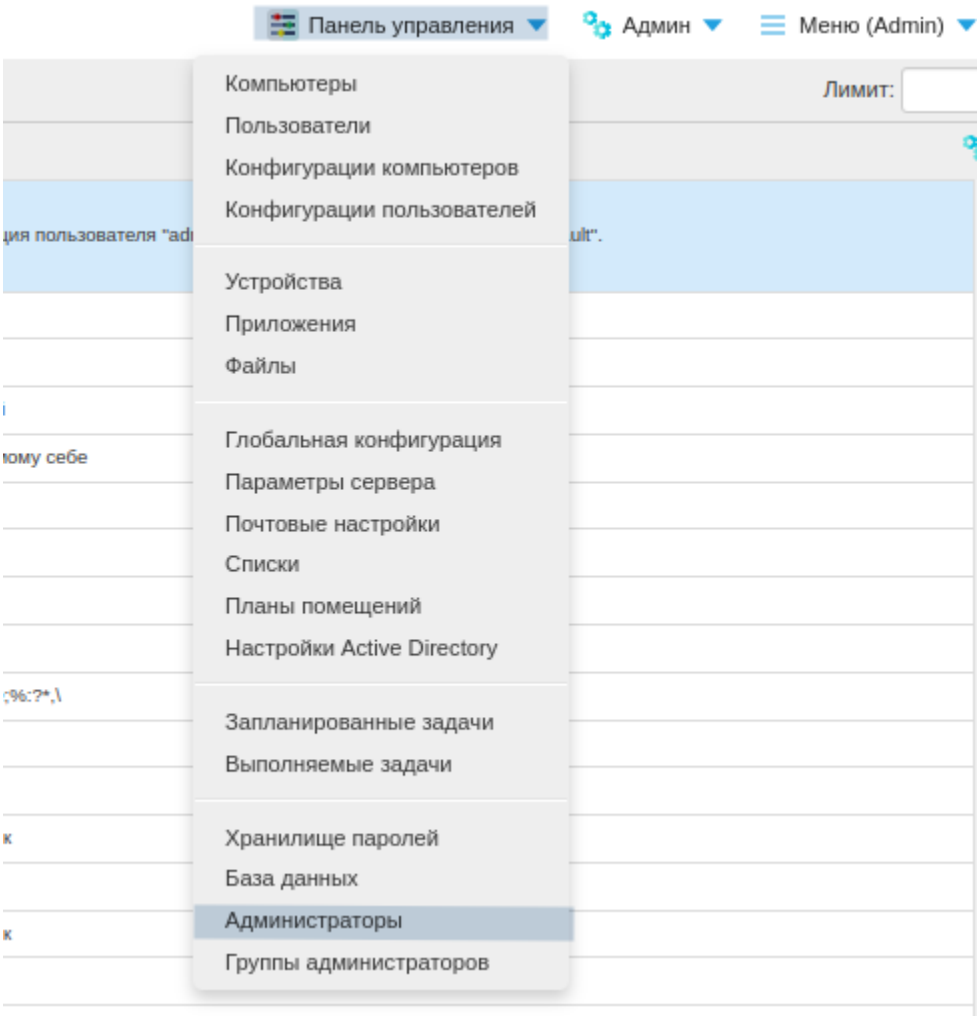
Доступ	Разрешено
Доступ к консоли	Просмотр своих инцидентов без редактирования и доступа к другим элементам системы.
Доступ ко всем инцидентам	Просмотр всех инцидентов и отчетов.
Создание	Создание инцидента без редактирования.
Редактирование	Редактирование и удаление созданного инцидента без возможности создать новый.
Доступ к настройкам	Управление статусами, шаблонами реагирования и группами инцидентов.
Доступ к фильтрам	Управление фильтрами списков инцидентов
Доступ к экспорту	Экспорт инцидентов или группы инцидентов.

По умолчанию права доступа собраны в две группы:

- **Incident Investigation Managment** — управление расследованием инцидентов для доступа:
  - к консоли,
  - всем инцидентам,
  - созданию инцидента,
  - редактированию инцидента,
  - настройкам,
  - управлению фильтрами.
- **Incident Assigned Managment** — управление назначенными инцидентами для доступа:
  - к консоли инцидентов,
  - редактированию,
  - экспорту.

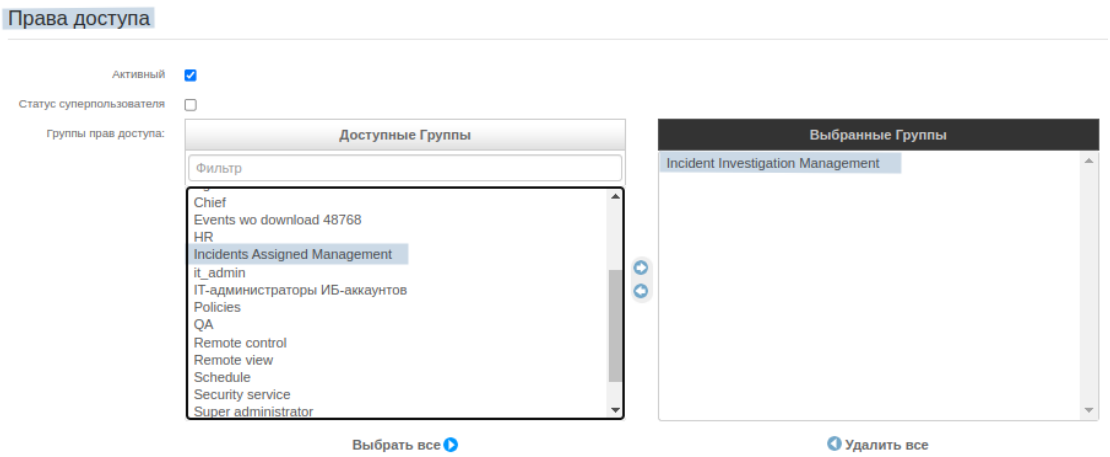
Вы можете создать новую группу под конкретные задачи.

Перейдите в основной интерфейс, далее — **Панель управления** → **Администраторы**.



Чтобы добавить администратора в группу доступа:

1. Выберите администратора из списка.
2. В окне **Доступные группы** дважды кликните группу доступа, чтобы переместить ее в окно **Выбранные группы**.
3. Сохраните изменения с помощью кнопки **Сохранить** внизу страницы.



Чтобы создать администратора и добавить его в группу доступа:

1. Нажмите на кнопку **Добавить** внизу страницы.
2. Добавьте в поля логин и пароль для входа.
3. Нажмите **Сохранить и продолжить**.
4. При необходимости заполните поля учетной записи.
5. В окне **Доступные группы** дважды кликните группу доступа, чтобы переместить ее в окно **Выбранные группы**.
6. Сохраните изменения с помощью кнопки **Сохранить** внизу страницы.

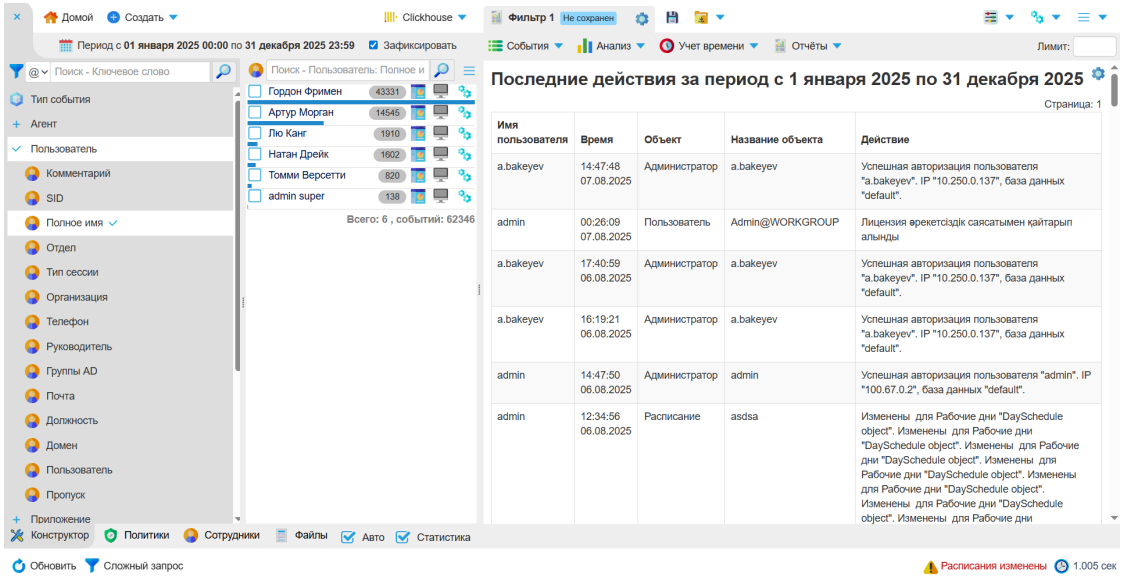
Готово! Теперь администратор имеет права, которые вы указали.

Регистрация действий администратора

На основе действий администратора создается запись в основном интерфейсе.

Перейдите в основной интерфейс, выберите **Панель управления** → **Последние действия**.

Откроется таблица с последними действиями администраторов системы:



Консоль управления инцидентами предназначена для обработки событий, которые администратор системы или офицер безопасности определил как **Инциденты** при создании **Фильтра** или **Политики**.

Консоль содержит список всех инцидентов и позволяет:

- создавать новые инциденты вручную;
- управлять созданными инцидентами;
- выделять основные группы инцидентов;
- создавать описания групп инцидентов;
- назначать ответственного за расследование инцидентов;
- задавать шаблоны реагирования на инцидент.

4.5 Типовые решения задач (Кейсы)

4.5.1 Установка и настройка Ideco UTM

Ideco UTM - широко распространённое программное решение для контроля сетевого трафика, одной из составных частей которого является прокси-сервер.

В этой статье будет описана настройка Ideco UTM и проверка его работы.

Настройка Ideco UTM для работы в связке с iBatyr Monitor будет описана в *отдельной статье*.

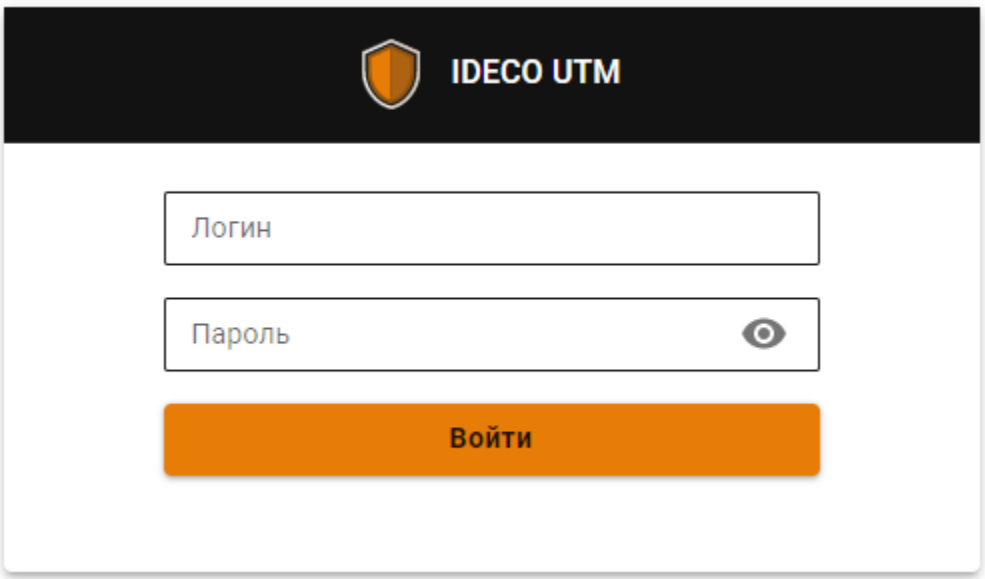
Начало работы

Установите Ideco UTM, используя официальную документацию разработчика.

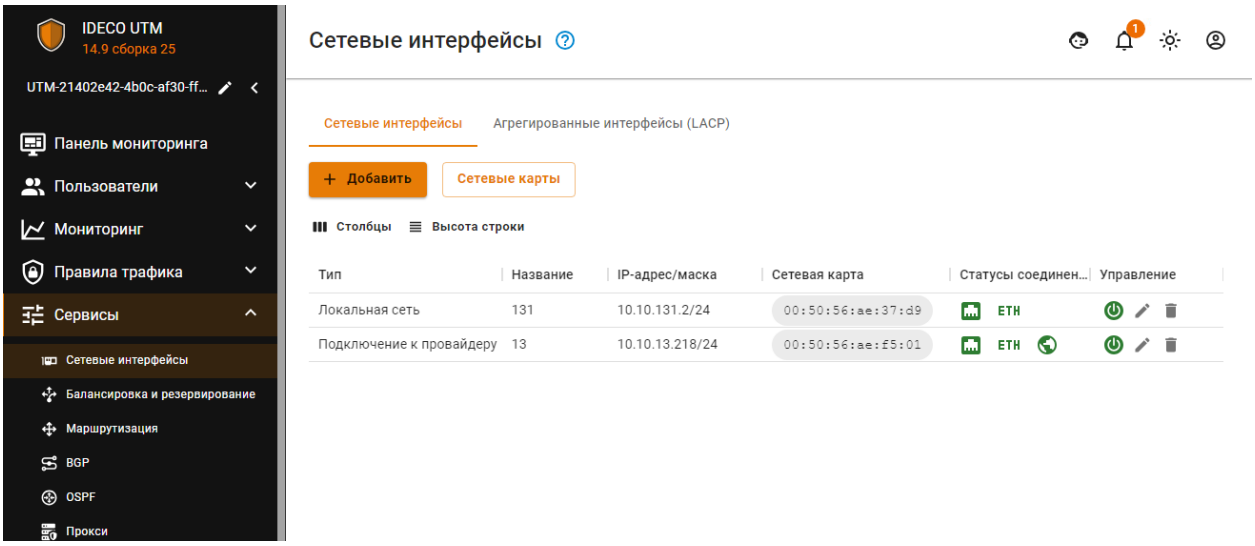
Настройка Ideco UTM

После завершения установки, в адресной строке браузера введите адрес сервера в формате **ip_address:8443**. Здесь **ip_address** - IP-адрес сервера, указанный при установке; **8443** - номер порта, который по умолчанию использует Ideco UTM.

В открывшемся окне авторизации укажите логин и пароль, заданные при установке.

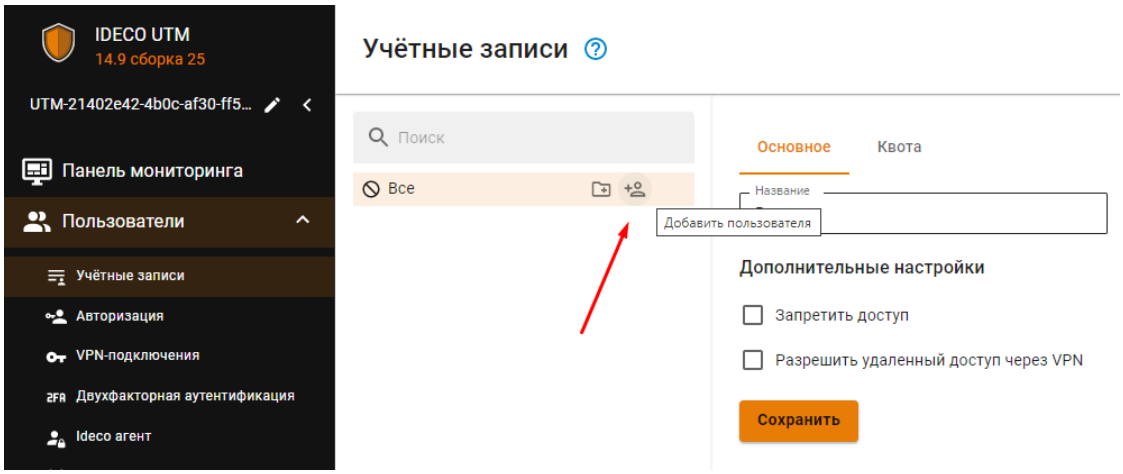


После успешной авторизации, проверьте указанные при установке сетевые интерфейсы. Для этого в разделе **Сервис - Сетевые интерфейсы** убедитесь, что сетевые интерфейсы активны: есть сигнал, назначен IP-адрес, установлено соединение с интернетом.

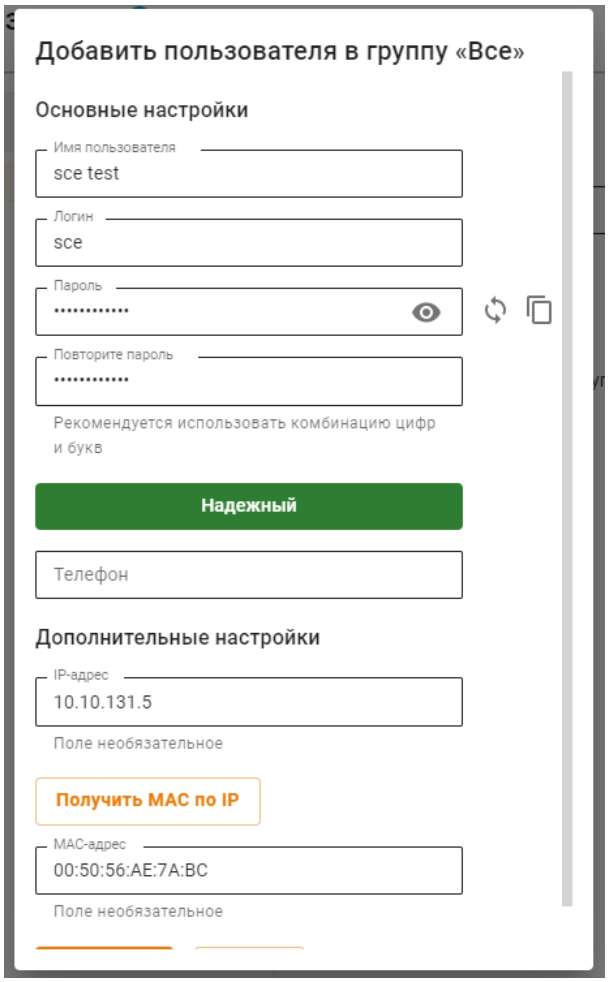


Ideco UTM блокирует соединение неавторизованных пользователей. Чтобы добавить новых пользователей:

1. В разделе **Пользователи - Учетные записи** добавьте новую запись.

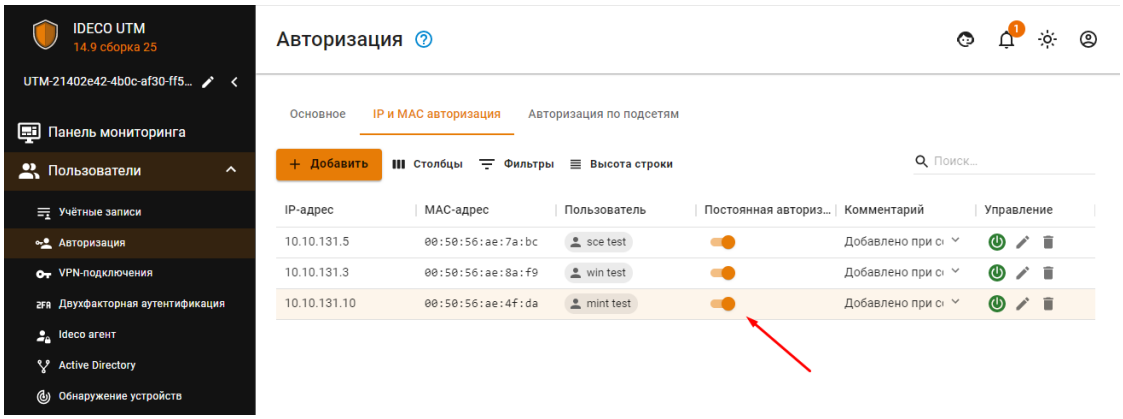


2. В открывшемся окне **Добавить пользователя в группу...** укажите IP-адрес машины нового пользователя или его логин и пароль.



3. Добавьте нужных пользователей сети.
4. В разделе **Пользователи - Авторизация** напротив имён пользователей включите переключатель **Постоянная авторизация**.

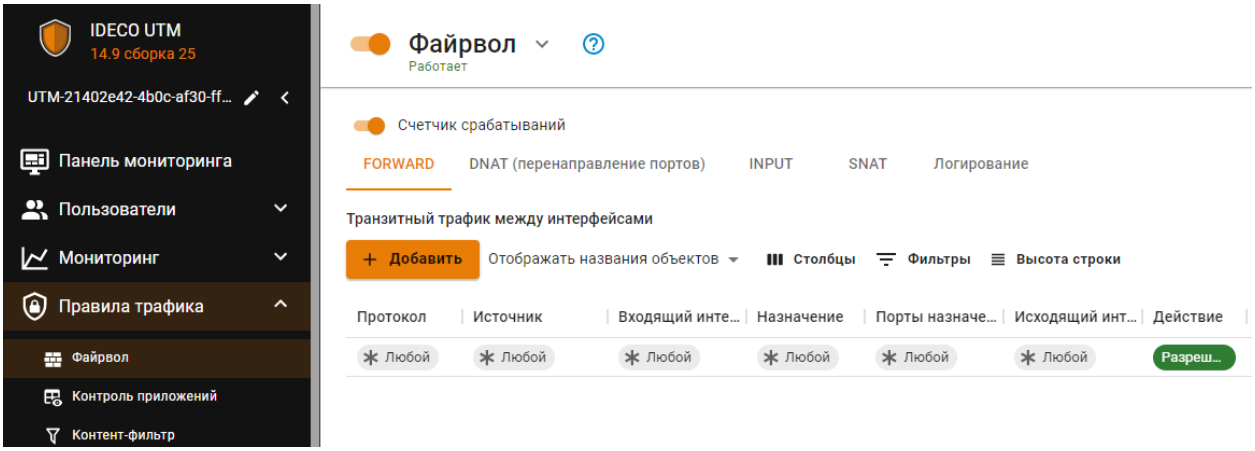
> **Примечание:** Если не включить опцию **Постоянная авторизация**, каждое сетевое действие такого пользователя потребует от него авторизации.



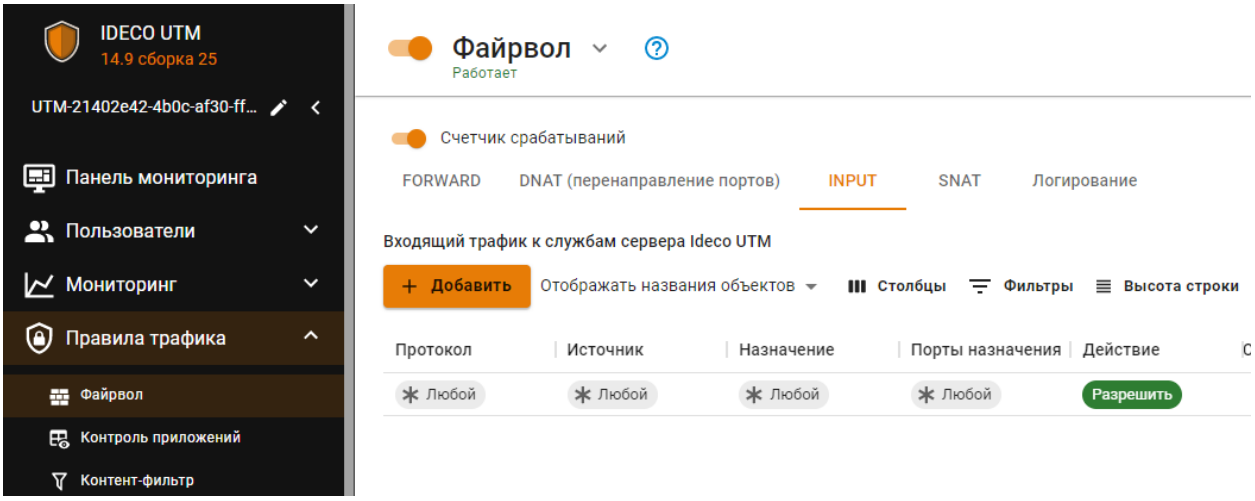
После добавления новых пользователей, в разделе **Сервис - DNS** укажите DNS-сервер сети.

Настройка файрвола

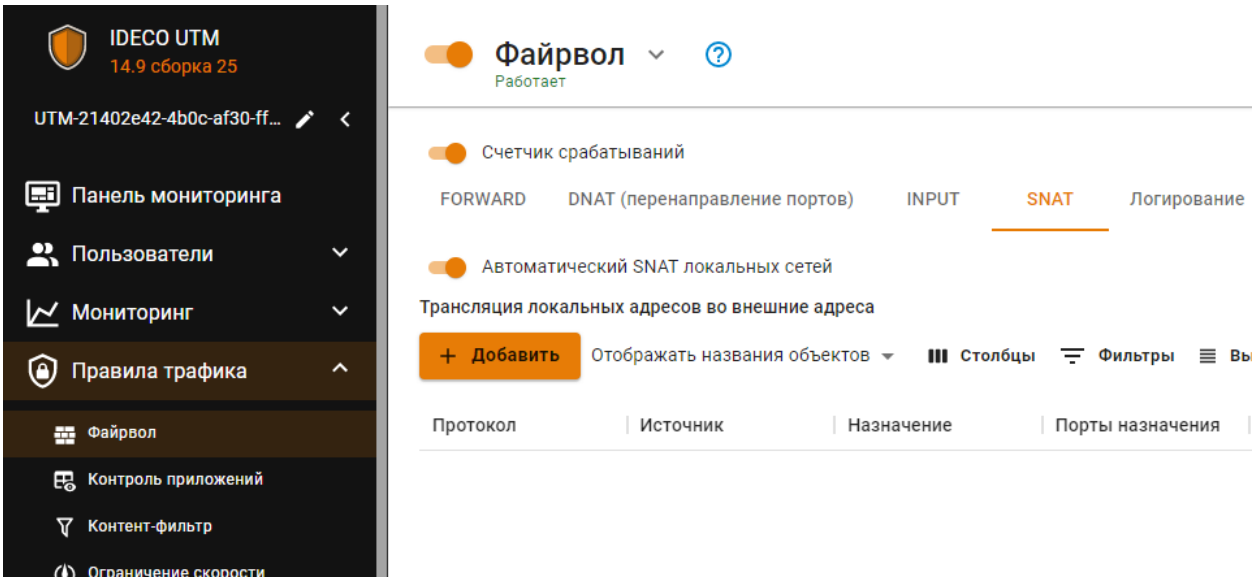
В разделе **Правила трафика - Файрвол** на вкладке **FORWARD** добавьте новое правило и разрешите любую передачу трафика



На вкладке **INPUT** добавьте новое правило. По умолчанию правило разрешает любой входящий трафик по любому интерфейсу.



На вкладке **SNAT** активируйте **Счетчик срабатываний** и **Автоматический SNAT локальных сетей**.



Готово! **Ideco UTM** настроен и работает. Чтобы проверить его работу, с любой из машин внутри сети откройте любой интернет-сайт.

После того, как Ideco UTM был установлен, настроен и проверен, можно переходить к его *настройке в качестве ICAP-сервера и к их совместной работе с сервером iBatyr Monitor* для дальнейшего мониторинга трафика.

4.5.2 Установка и настройка Squid Proxy

Squid Proxy — популярный и стабильный open-source прокси-сервер, отлично подходящий для решения широкого спектра задач.

В этой статье будет описана:

- установка Squid Proxy на подготовленную к работе Ubuntu 18.04;
- настройка использования самоподписных SSL-сертификатов;
- проверка функционирования Squid Proxy.

В дальнейшем будем использовать данный Squid Proxy для настройки перехвата трафика на ICAP-сервере.

Подготовка к установке

Перед началом установки Squid Proxy обновите пакеты системы и установите все доступные обновления:

```
apt update && apt upgrade && apt-get update && apt-get upgrade
```

После этого, добавьте в список репозиториев источник исходного кода Squid. Для этого в файл **/etc/apt/sources.list** добавьте строку **deb-src http://ru.archive.ubuntu.com/ubuntu/ focal main restricted**.

Установите необходимые для дальнейшей работы Squid утилиты:

```
apt-get install devscripts build-essential fakeroot libssl-dev libssl1.0-dev
```

Подготовка к установке завершена, теперь можно переходить непосредственно к процессу установки.

Установка Squid Proxy

Установите Squid Proxy из исходного кода. Для этого создайте папку, в которую будете устанавливать Squid, и сделайте её доступной для редактирования:

```
mkdir /usr/src/squid
chown _apt:root /usr/src/squid
cd /usr/src/squid
```

Теперь, установите необходимые для сборки Squid пакеты:

```
apt-get source squid
# Пакеты, необходимые для компиляции
apt-get build-dep squid
```

Добавьте поддержку SSL Bump и генерации сертификатов. Для этого в файл /usr/src/squid/squid3-3.5.27/debian/rules добавьте строки:

```
--with-gnutls \
--enable-ssl \
--enable-ssl-crtd \
--with-openssl \
```

В файл **/usr/src/squid/squid3-3.5.27/src/ssl/certificate_db.cc** добавьте строку **#include <unistd.h>**.

В итоге файл будет выглядеть примерно так:

```
#include "squid.h"
#include "ssl/certificate_db.h"

#include <unistd.h>
#include <cerrno>
#include <fstream>
#include <stdexcept>
#if HAVE_SYS_STAT_H
#include <sys/stat.h>
#endif
#if HAVE_SYS_FILE_H
#include <sys/file.h>
#endif
#if HAVE_FCNTL_H
#include <fcntl.h>
#endif
```

Удалите лишние форматы:

```
rm -r /usr/src/squid/squid3-3.5.27/debian/source
```

Подготовка к сборке завершена. Теперь переходите к сборке пакетов:

```
cd /usr/src/squid/squid3-3.5.27
apt install libssl1.0-dev
```

(continues on next page)

(продолжение с предыдущей страницы)

```
apt list --upgradable -a
dpkg-buildpackage -rfakeroot -d -us -uc -ui
debuild -d
```

Примечание: В процессе сборки возможно возникновение ошибок вида:

```
Now signing changes and any dsc files...
signfile dsc squid_4.10-1ubuntu1.dsc Andreas Hasenack <andreas@canonical.com>
gpg: directory '/root/.gnupg' created
gpg: keybox '/root/.gnupg/pubring.kbx' created
gpg: skipped "Andreas Hasenack <andreas@canonical.com>": No secret key
gpg: /tmp/debsign.YiTaKCMO/squid_4.10-1ubuntu1.dsc: clear-sign failed: No secret key
debsign: gpg error occurred! Aborting....
debuild: fatal error at line 1112:
running debsign failed
```

Это нормально, поскольку у нас нет закрытого ключа разработчика.

Установите собранные пакеты:

```
cd /usr/src/squid
dpkg -i squid_3.5.27-1ubuntu1_amd64.deb squid-common_3.5.27-1ubuntu1_all.deb squidclient_
↪3.5.27-1ubuntu1_amd64.deb

# Дополнительные зависимости
apt-get --fix-broken install

# Сохраните список установленных зависимостей
apt-mark hold squid squidclient squid-common
```

После установки Squid, проверьте его статус:

```
systemctl status squid
```

Прокси-сервер должен быть запущен.

Настройка использования SSL-сертификатов

Чтобы настроить использование прокси-сервером самоподписного SSL-сертификата:

1. Остановите Squid:

   ```
   systemctl stop squid
   ```

2. Создайте папку для хранения SSL-сертификатов и выдайте пользователю полные права на неё:

   ```
   mkdir /etc/squid/ssl
   chmod 700 /etc/squid/ssl
   ```

3. Сгенерируйте корневой сертификат, на основе которого будут подписываться сертификаты для сайтов:

```
openssl genrsa -out /etc/squid/ssl/squid.key
openssl req -new -key /etc/squid/ssl/squid.key -out /etc/squid/ssl/squid.csr
openssl x509 -req -days 999 -in /etc/squid/ssl/squid.csr -signkey /etc/squid/
↪ssl/squid.key -out /etc/squid/ssl/squid.pem
```

4. Сгенерируйте сертификат, который затем нужно будет добавить в бразуер:

```
openssl x509 -in /etc/squid/ssl/squid.pem -outform DER -out /etc/squid/ssl/
↪squid.der
```

5. Создайте базу данных для генерируемых сертификатов:

```
/usr/lib/squid3/ssl_crtd -c -s /var/spool/squid/ssl_db
```

6. Настройте конфигурацию Squid с использованием сгенерированных сертификатов. Для этого приведите конфигурационный файл **/etc/squid/squid.conf** к следующему виду:

7. Отключите включенную по умолчанию поддержку IPv6:

```
sysctl -w net.ipv6.conf.all.disable_ipv6=1
sysctl -w net.ipv6.conf.default.disable_ipv6=1
sysctl -w net.ipv6.conf.lo.disable_ipv6=1
```

8. Для поддержки IPv4, в любое место конфигурационного файла Squid добавьте строку **dns_v4_first on**.

9. Перезагрузите конфигурацию и запустите Squid:

```
squid -z
systemctl daemon-reload
systemctl restart squid
```

10. Добавьте самозаверяющийся сертификат в список доверенных:

```
apt-get install ca-certificates
cp /etc/squid/ssl/squid.pem /usr/local/share/ca-certificates/squid.crt
update-ca-certificates
dpkg-reconfigure ca-certificates
```

11. Перезапустите сервер.

Прокси-сервер установлен и настроен. Можно проверять его работоспособность внутри сети.

Проверка работы Squid

Чтобы проверить правильность настройки Squid Proxy, укажите его адрес в качестве адреса прокси в настройках машин внутри сети. Компьютеры из подсети должны получать доступ к сети.

Готово! Squid Proxy установлен, настроено использование SSL-сертификатов и данная конфигурация исправно работает.

4.5.3 Перехват трафика на ICAP-сервере

Введение

Примечание: ICAP-сервер – это компонент, который включается по отдельной лицензии в составе iBatyr Monitor .

Начиная с версии iBatyr Monitor 5.2 ICAP-сервер поддерживает перехват следующих событий:

- файлы в POST-запросах;
- посещение сайтов;
- данные веб-форм;
- чаты MS Teams;
- чаты Bitrix24.

Предварительная настройка

Для перехвата трафика на ICAP-сервере понадобятся:

- установленный и настроенный сервер iBatyr Monitor ;
- прокси-сервер или UTM, настроенный для работы в сети пользователя;
- ICAP-клиент, настроенный на прокси-сервере и передающий сведения на ICAP-сервер iBatyr Monitor.

Сервер iBatyr Monitor

Установка и подготовка к работе сервера iBatyr Monitor описаны в разделе *Руководство администратора*.

Прокси-сервер

Работа компонента перехвата трафика на ICAP-сервере не зависит от прокси-сервера, который используется в системе заказчика.

В статье будет описана настройка перехвата трафика в случае, когда в сети используется Ideco UTM или Squid Proxy. При этом использовать можно любой другой прокси-сервер.

В отдельных статьях описаны процессы установки и настройки *Ideco UTM* и *Squid Proxy*. Установка и настройка UserGate UTM подробно описаны в пользовательской документации.

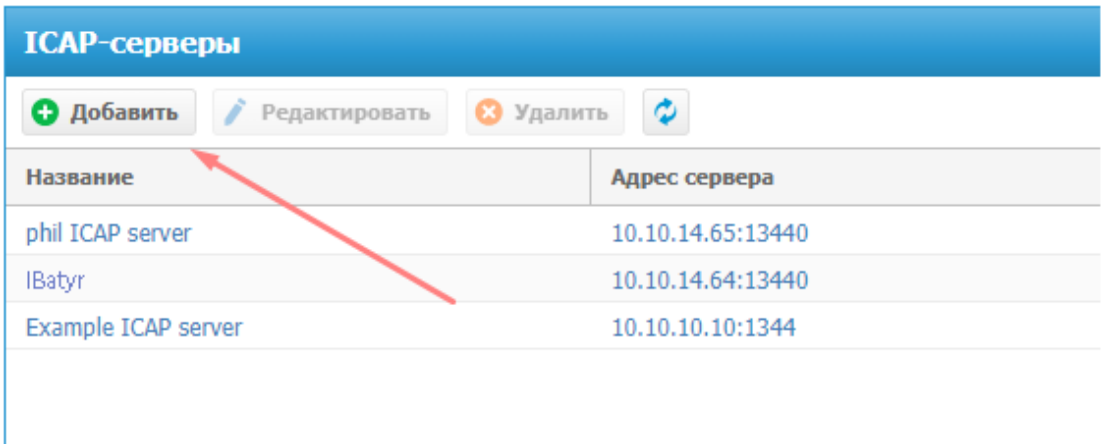
При возникновении проблем с настройками других прокси, обратитесь в нашу *службу технической поддержки*.

Настройка ICAP-клиента

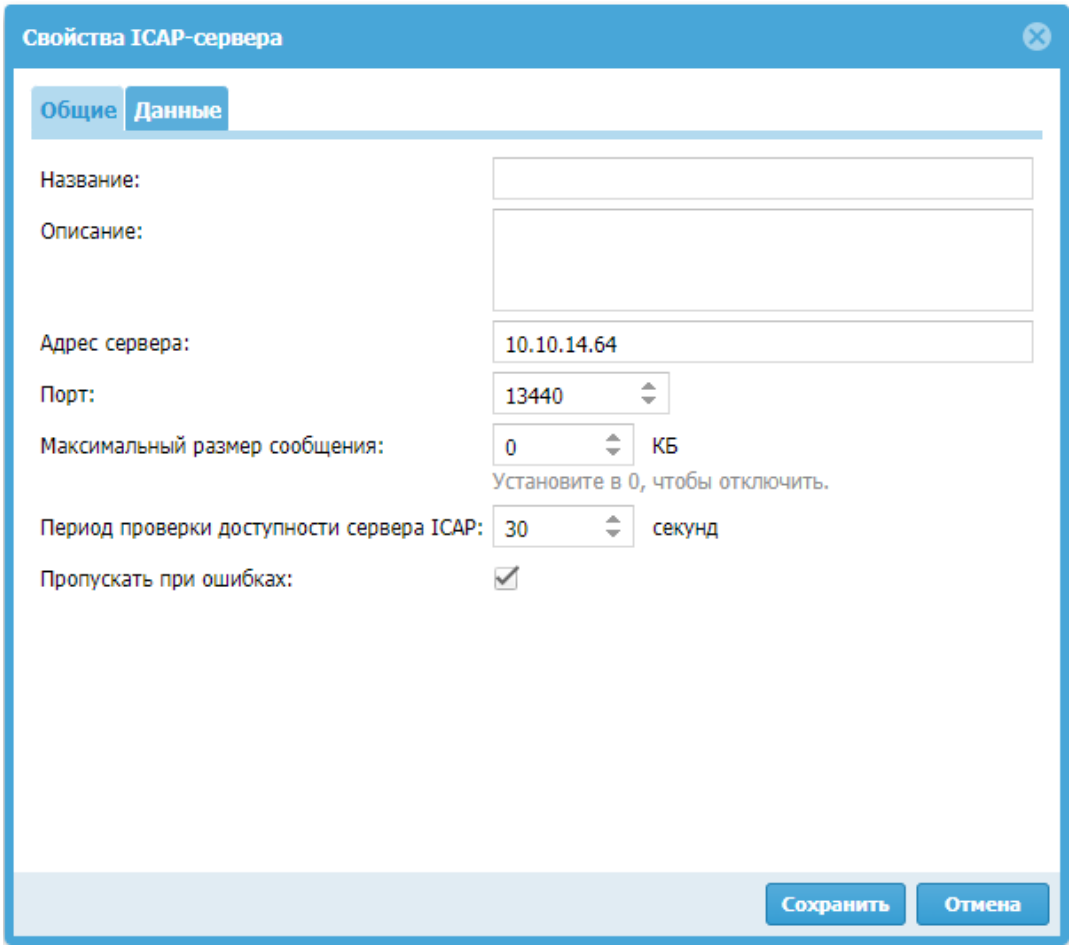
UserGate UTM

Чтобы настроить UserGate UTM в качестве ICAP-клиента

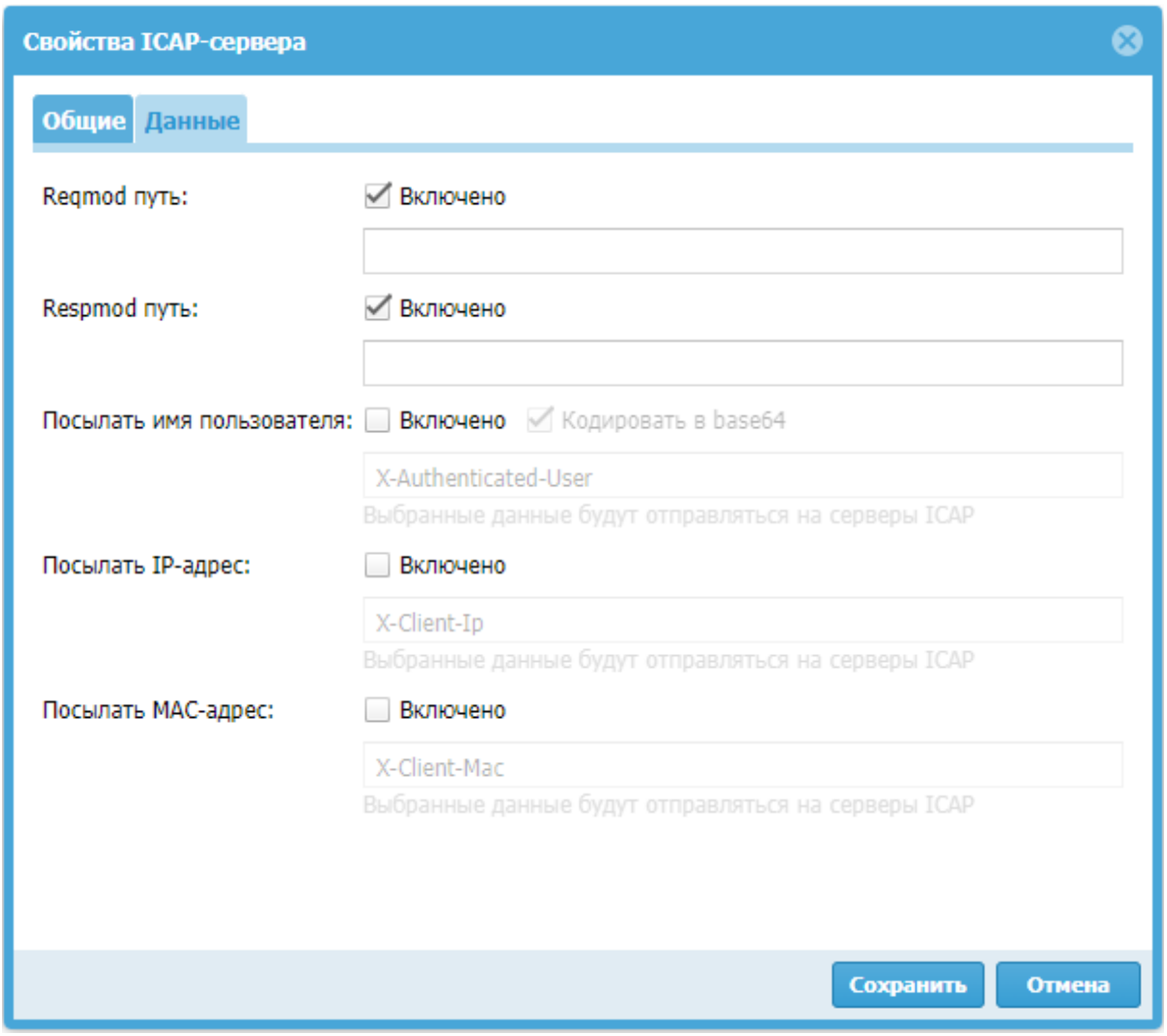
1. В веб-интерфейсе UserGate UTM в разделе **Политики безопасности** → **ICAP-серверы** добавьте новый сервер:



2. В открывшемся окне **Свойства ICAP-сервера** на вкладке **Общие** укажите:
   - в строке **Адрес сервера** — IP-адрес сервера iBatyr Monitor;
   - в строке **Порт** — номер порта (по умолчанию — **13440**);
   - активируйте опцию **Пропускать при ошибках**;
   - заполните значения в полях **Название**, **Описание**, **Максимальный размер пакета** и **Период проверки доступности...**.

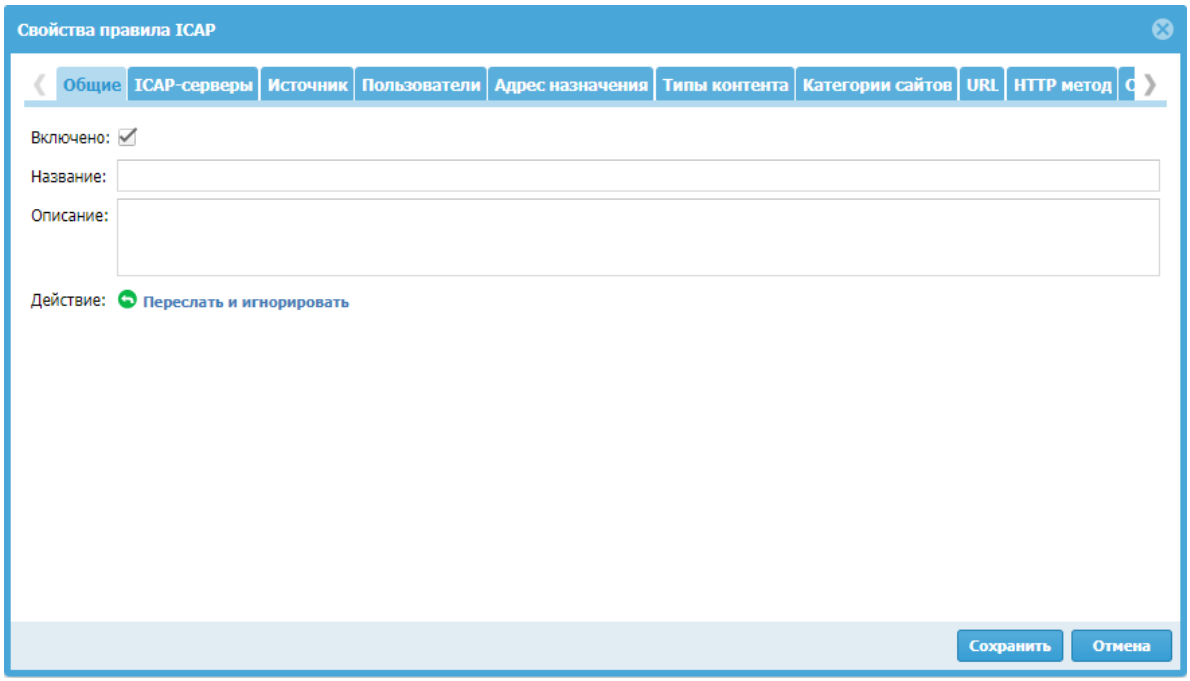


3. На вкладке **Данные** заполните поля **Reqmod путь** и **Respmod путь**. Полный путь имеет вид **icap://ip_address:13440/ibatyr**. Поскольку IP-адрес и номер порта указаны на вкладке **Общие**, в строках **Reqmod путь** и **Respmod путь** укажите только **/ibatyr**.

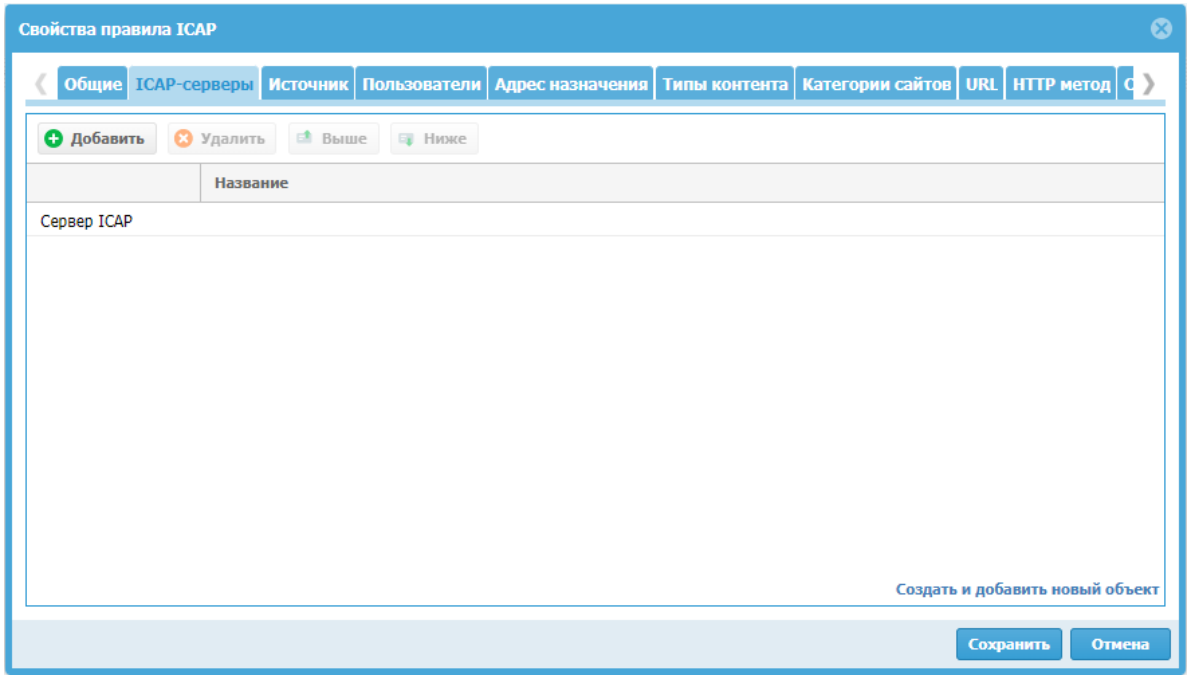


4. В разделе **Политик безопасности** → **ICAP-правила** создайте новое правило, по которому будет работать ICAP-сервер.

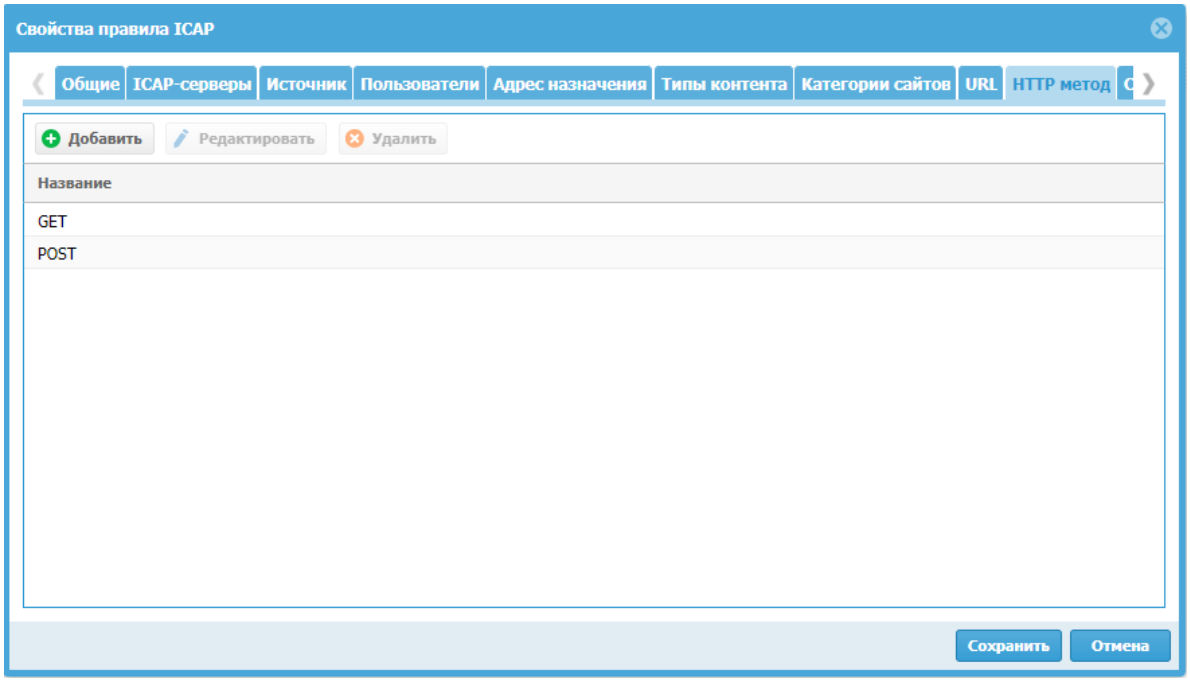
5. В окне создания нового правила на вкладке **Общие** укажите его название, описание и добавьте действие **Переслать и игнорировать**.



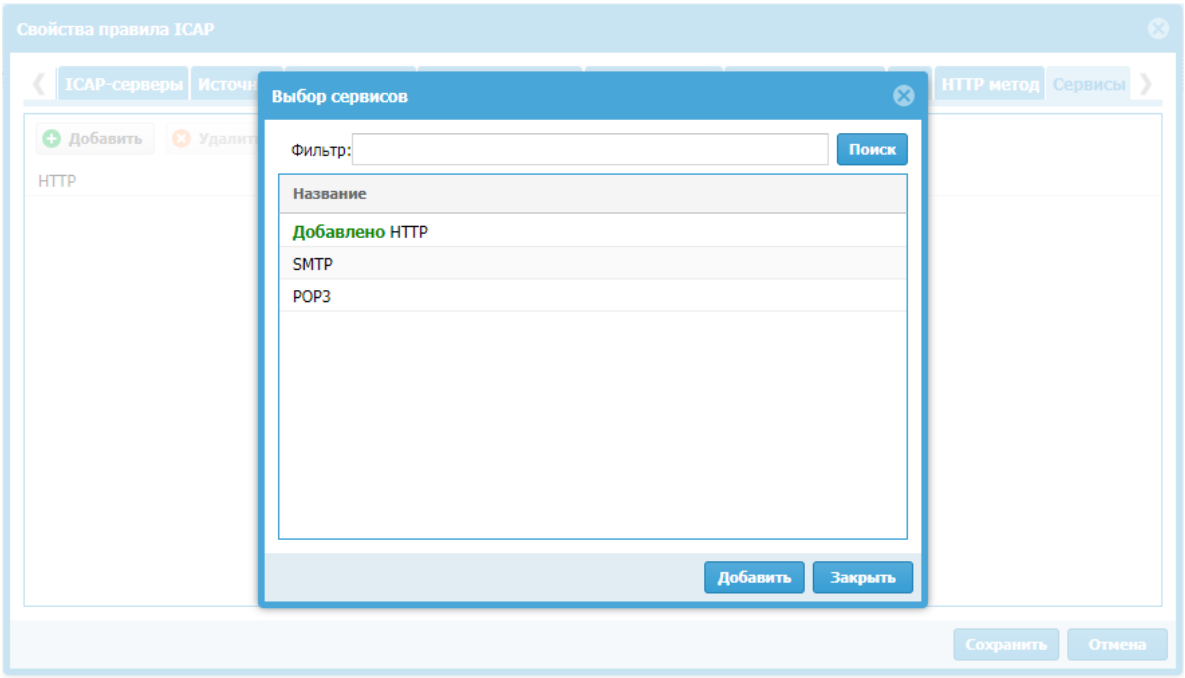
6. На вкладке **ICAP-серверы** выберите только что созданный ICAP-сервер.



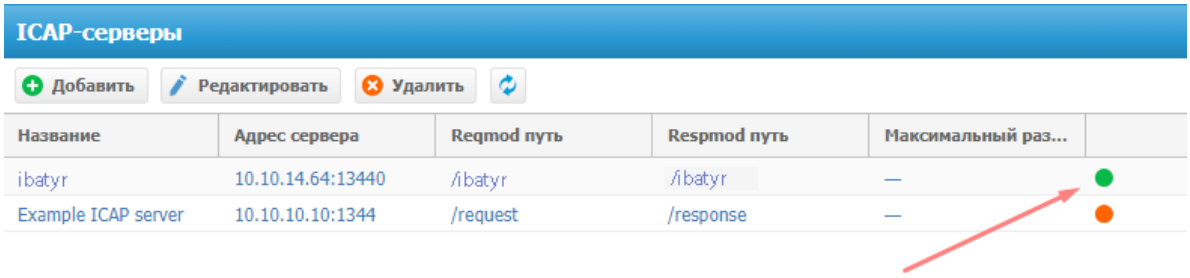
7. На вкладке **HTTP-метод** укажите методы **GET** и **POST**.



8. На вкладке **Сервисы** в окне выбора добавляемых сервисов выберите только протокол **HTTP**.



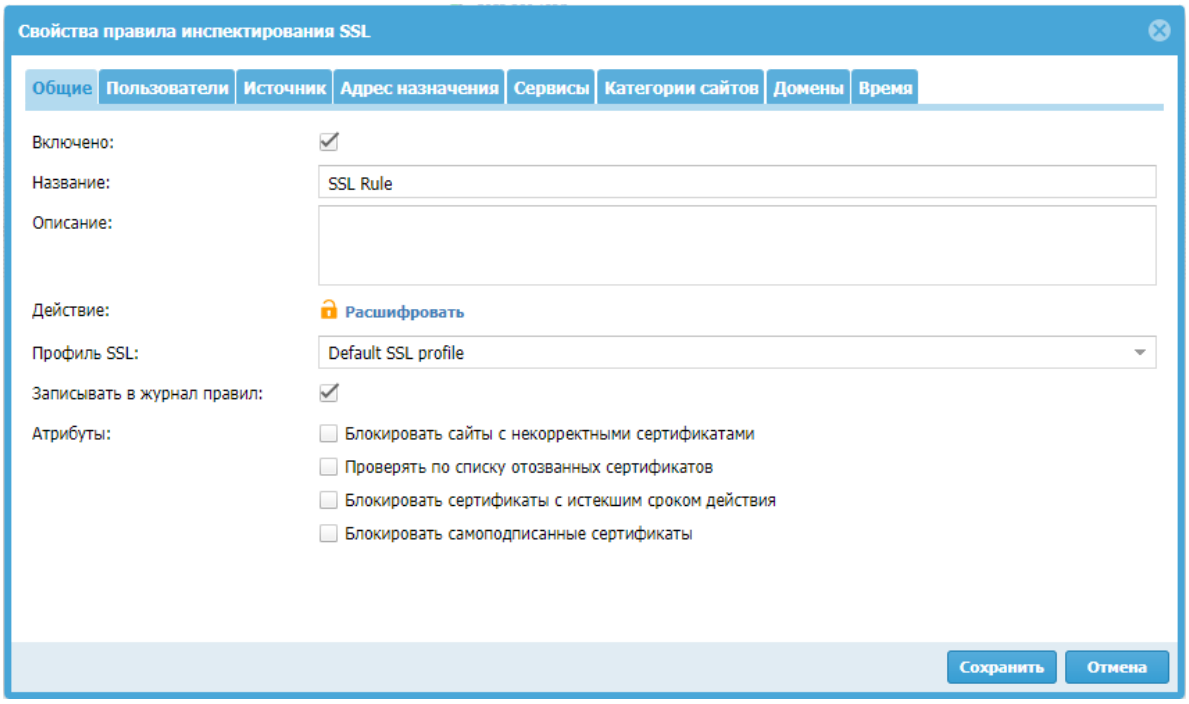
9. Сохраните созданное правило и в окне **ICAP-серверы** дождитесь зелёного значка установления связи с сервером.



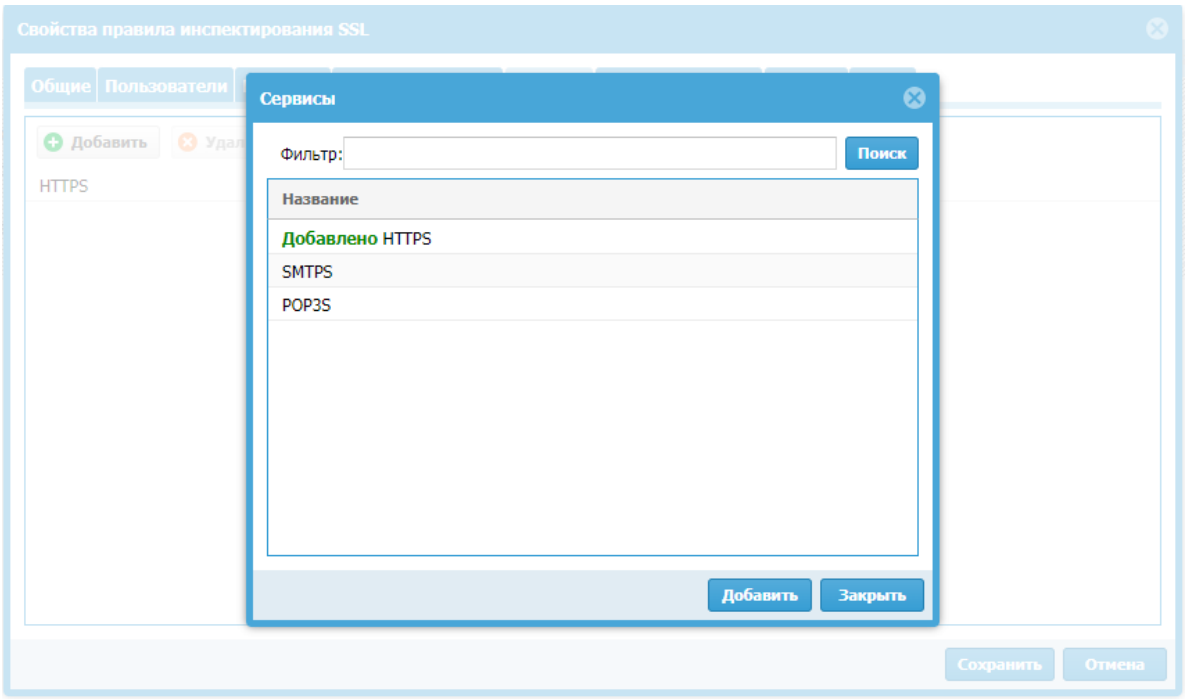
10. Готово! ICAP-сервер настроен и работает.

Теперь настройте правила расшифровки трафика на сервере:

1. В разделе **Политики безпасности** → **Инспектирование SSL** создайте новое правило:
   - в строке **Действие** укажите **Расшифровать**;
   - **Профиль SSL** оставьте без изменений;
   - включите **Запись в журнал правил** по желанию.

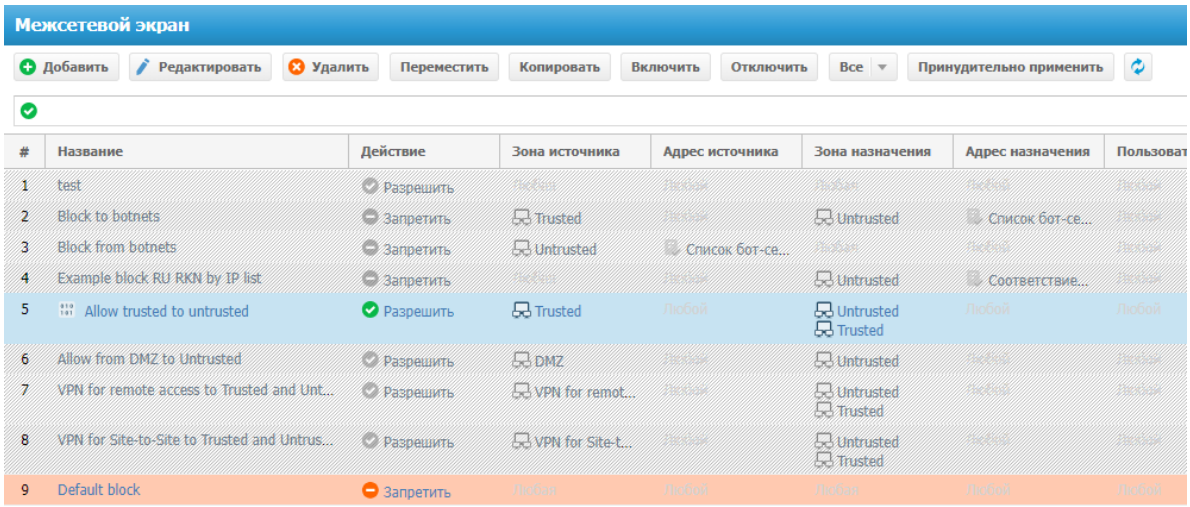


2. На вкладке **Сервисы** добавьте только **HTTPS**.

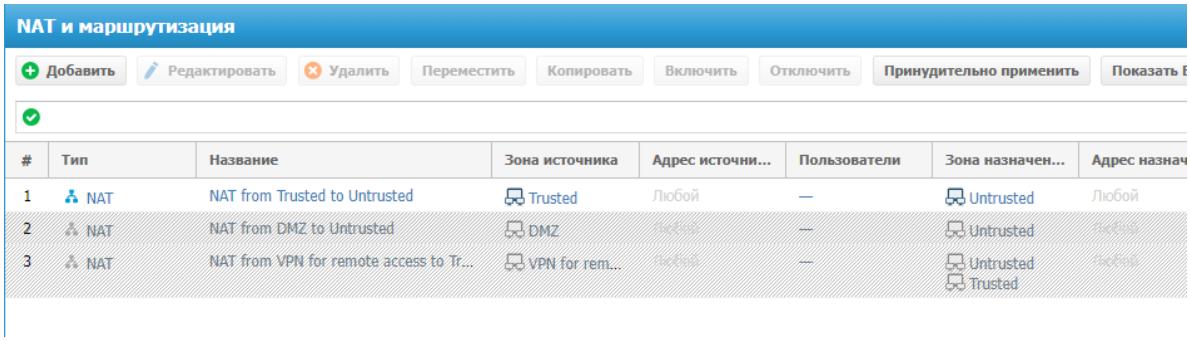


3. Настройте правила расшифровки трафика под свои требования согласно официальной документации UserGate UTM

4. В настройках межсетевого экрана разрешите трафик между локальной и внешней сетью. Также, если в локальной сети есть серверы с веб-интерфейсом (например, iBatyr Monitor) и пользователи, которые к нему подключаются, укажите в назначении саму локальную сеть.



5. Включите NAT из локальной сети во внешнюю для корректной работы прокси-сервера.



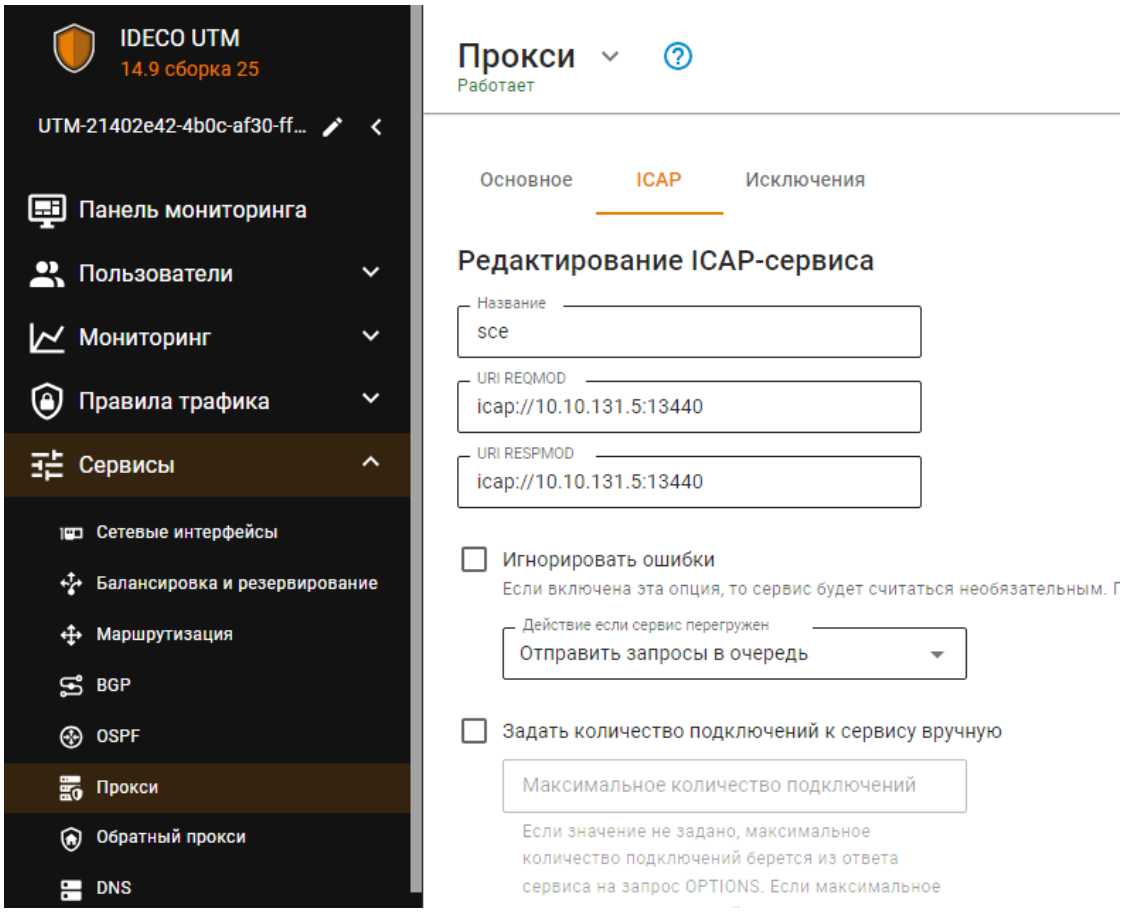
Готово! Настройка UserGate UTM завершена.

Ideco UTM

Настройте перенаправление трафика на ICAP-сервер iBatyr Monitor:

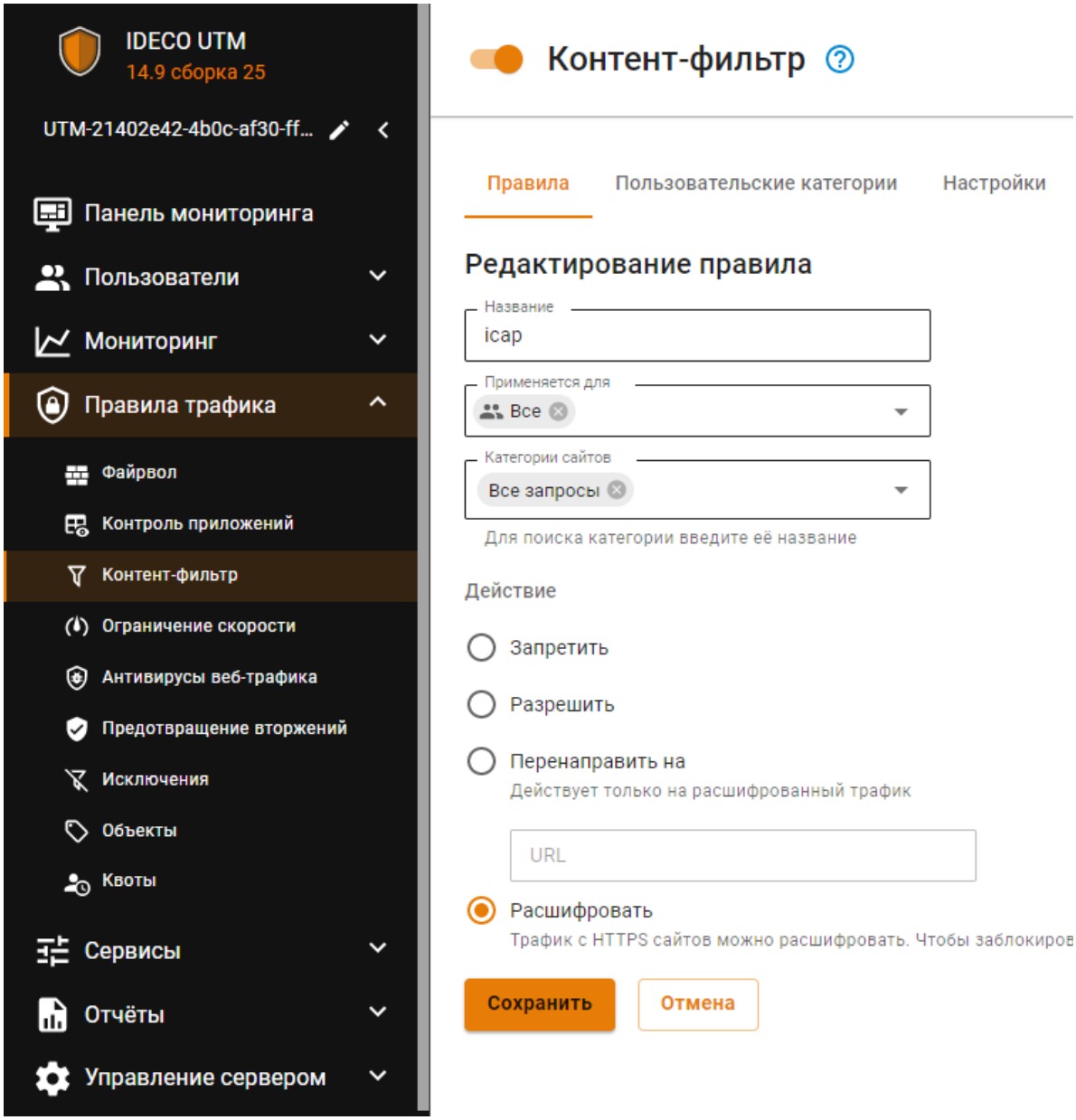
1. В разделе **Сервисы** → **Прокси** перейдите на вкладку **ICAP**. В строках **URI REQMOD** и **URI RESPMOD** укажите адрес ICAP-сервера iBatyr Monitor и порт для подключения. По умолчанию ICAP-сервер iBatyr Monitor использует для подключения порт **13440**. В общем виде запись адреса будет иметь вид:

```
icap://10.0.0.1:13440/ibatyr
```



2. Настройте перехват ICAP. В разделе **Правила трафика** → **Контент-фильтр** создайте правило фильтрации. Включите опцию **Расшифровать**. Это правило позволяет расшифровывать

трафик, идущий по HTTPS-соединению, всем встроенным в Ideco UTM компонентам и внешним ICAP-серверам.



3. Готово! Ideco UTM настроен и передаёт трафик на ICAP-сервер, предоставляемый iBatyr Monitor. Можно переходить к настройке работы самого iBatyr Monitor-сервера.

Squid Proxy

Для Squid Proxy версий 3.5 и выше, поддержка ICAP включена автоматически.

Для Squid Proxy версий ниже 3.5, при создании конфигурации пакетов в файл **/usr/src/squid/squid3-3.5.27/debian/rules** необходимо добавить строку **–enable-icap-client**.

Чтобы настроить на Squid Proxy подключение к ICAP серверу iBatyr Monitor, в конфигурационный файл **/etc/squid/squid.conf** внесите следующие изменения:

```
icap_enable on
icap_service_failure_limit -1
icap_preview_enable on
icap_preview_size 4096
adaptation_send_client_ip on
adaptation_send_username on

icap_service service_req reqmod_precache bypass=1 icap://ip_address:port/ibatyr
icap_service service_resp respmod_precache bypass=1 icap://ip_address:port/ibatyr

adaptation_access service_req allow all
adaptation_access service_resp allow all
```

Здесь **icap://ip_address:port/ibatyr** - IP-адрес и порт сервера iBatyr Monitor, на котором запущена ICAP-служба.

После этого перезагрузите конфигурацию и перезапустите сервис:

```
squid -z
systemctl daemon-reload
systemctl restart squid
```

Настройка прокси-сервера завершена.

Перехват ICAP

Чтобы настроить перехват на сервере iBatyr Monitor, обновите список доступных пакетов и установите дополнительную библиотеку:

```
sudo apt-get update
sudo apt-get install libatomic1
```

Запустите ICAP-службу сервера iBatyr Monitor и проверьте её на ошибки:

```
ibatyr enable-icap
ibatyr icap dev
```

Чтобы служба ICAP работала не только на IPv6, в конфигурационном файле **/etc/ibatyr/icap.conf** в строке **Port** укажите IP-адрес сервера:

```
Port ip_address:13440
```

Сохраните внесённые изменения и перезапустите службы строго в указанном порядке:

```
systemctl daemon-reload
ibatyr icap stop
ibatyr icap start
```

Проверить, что запуск перехвата прошёл успешно можно в логе событий. Для этого в консоли сервера iBatyr Monitor выполните команду:

```
sudo tail -n 10 /var/log/ibatyr/icap-access.log
```

Если перехват запущен и работает в штатном режиме, запись в логах будет примерно такой:

```
support@enterprise:~$ sudo tail -n 10 /var/log/staffcop/icap-access.log
15/Aug/2023:13:17:26 +0700, 10.10.14.65 10.10.14.66 REQMOD staffcop 204
15/Aug/2023:13:17:26 +0700, 10.10.14.65 10.10.14.66 REQMOD staffcop 204
15/Aug/2023:13:17:26 +0700, 10.10.14.65 10.10.14.66 REQMOD staffcop 204
15/Aug/2023:13:17:26 +0700, 10.10.14.65 10.10.14.66 RESPMOD staffcop 204
15/Aug/2023:13:17:26 +0700, 10.10.14.65 10.10.14.66 REQMOD staffcop 204
15/Aug/2023:13:17:29 +0700, 10.10.14.65 10.10.14.66 REQMOD staffcop 204
15/Aug/2023:13:17:30 +0700, 10.10.14.65 10.10.14.66 REQMOD staffcop 204
15/Aug/2023:13:17:30 +0700, 10.10.14.65 10.10.14.66 REQMOD staffcop 204
15/Aug/2023:13:17:33 +0700, 10.10.14.65 10.10.14.66 OPTIONS staffcop 200
15/Aug/2023:13:17:33 +0700, 10.10.14.65 10.10.14.66 OPTIONS staffcop 200
support@enterprise:~$
```

Готово! Трафик с ICAP-сервера перехватывается сервером iBatyr Monitor. Все события присваиваются приложению **ICAP**.

События ICAP

Изменено в версии 5.4.

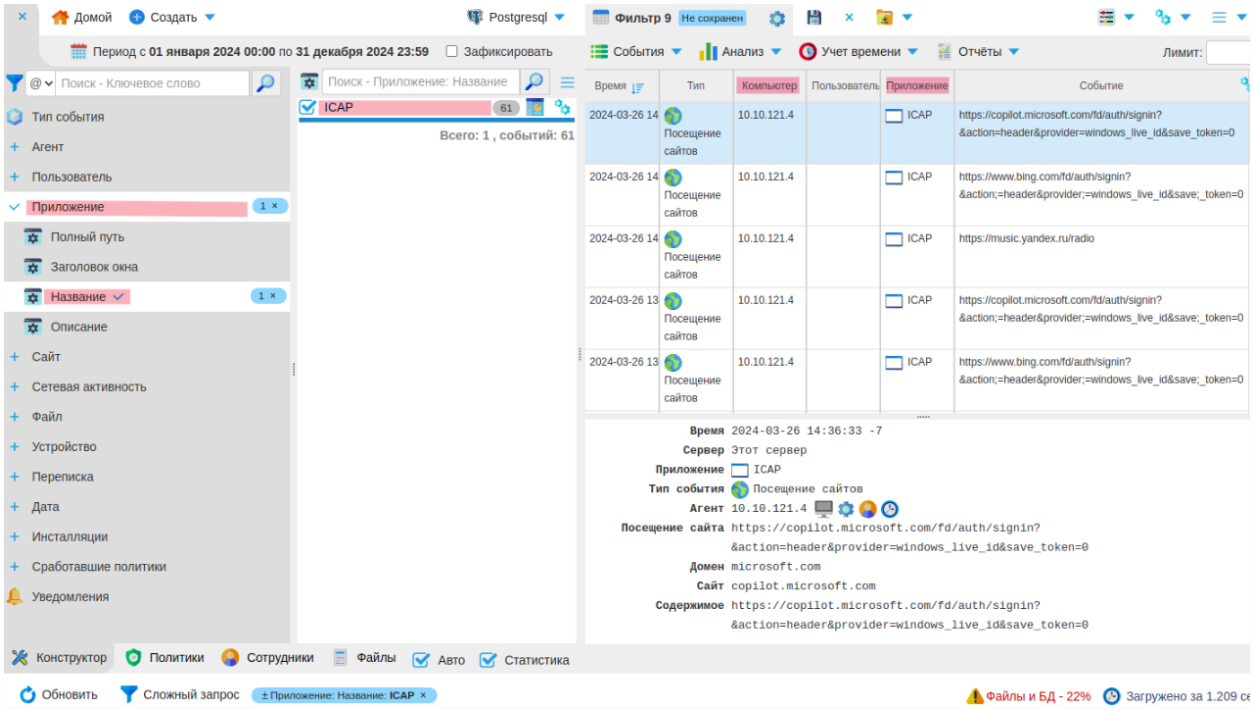
После запуска настройки ICAP-сервера, активации компонента ICAP и получения данных агент записывает события сетевого трафика организации.

Чтобы найти события ICAP:

1. Перейдите в **Конструктор событий**.
2. В **Приложении** выберите **Название**.
3. Введите в поле поиска *ICAP*.

События ICAP содержат в измерении **Компьютер** IP-адрес АРМ, с которого был получен или отправлен трафик.

До версии 5.4 в событиях ICAP-сервера в измерении **Компьютер** указывалось значение **ICAP**, а идентификации по компьютеру не было.



Как убрать дубликаты событий

При одновременном сетевом перехвате от агента и ICAP данные могут дублироваться. Вы можете отключить сетевой перехват на агентах или исключить агентов из ICAP.

Чтобы ICAP не дублировал события от агентов:

1. Перейдите **Панель управления** → **Параметры сервера**.
2. Выберите **Исключить агенты из ICAP**.
3. После переключении опции подождите минуту для обновления кэша или или перезапустите сервер:

```
ibatyr restart
```

После этого будут записаны только события агента.

Отключение ICAP-модуля

Чтобы отключить ICAP, выполните команды:

```
ibatyr disable-icap
ibatyr restart
```

4.5.4 Перехват мессенджера Express

Начиная с версии 5.2.1317, в iBatyr Monitor доступен перехват сообщений, отправленных через мессенджер Express.

Чтобы настроить перехват:

1. Установите и настройте мессенджер Express, согласно официальной инструкции разработчика.
2. Проверьте версию iBatyr Monitor (**Меню(User)** → **О программе** → **Версия сервера**). Она должна быть не ниже 5.2.1317.

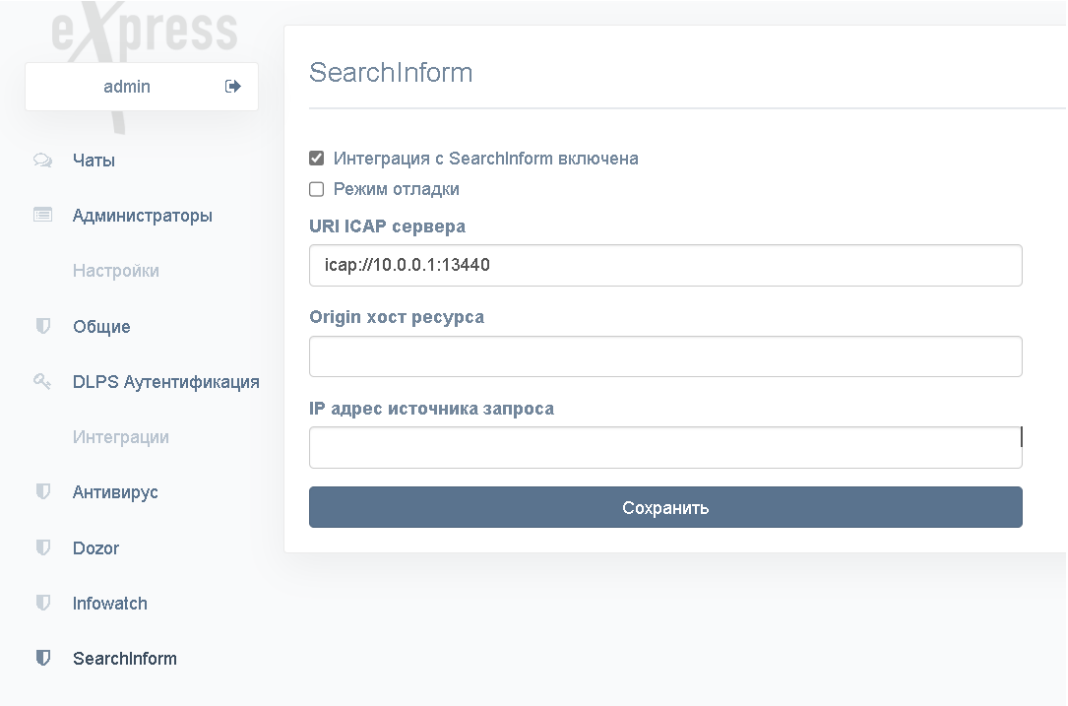
   При необходимости, *обновите сервер до последней доступной версии*.
3. На сервере iBatyr Monitor запустите сервис **ibatyr-icap.service**:

   Первый запуск сервиса

   ```
   ibatyr enable icap
   ```

   Если сервис был запущен, но остановлен

   ```
   ibatyr icap start
   ```
4. В адресной строке браузера укажите адрес *https://express_server/dlps/integrations/search_inform*. Здесь *express_server* — адрес развёрнутого сервера Express.



5. В окне настроек перехвата поставьте галочку в пункте **Включен**.
6. В полях URI ICAP сервера и Origin хост ресурса укажите *icap://ip_address_ibatyr:port_icap/ibatyr*.

   Здесь *ip_address_ibatyr* — IP-адрес сервера iBatyr Monitor; *port_icap* — номер порта для перехвата ICAP.

Примечание: Номер порта для перехвата ICAP указан в конфигурационном файле *etc/ibatyr/icap.conf* в разделе **TAG: Port** в строке **Port**.

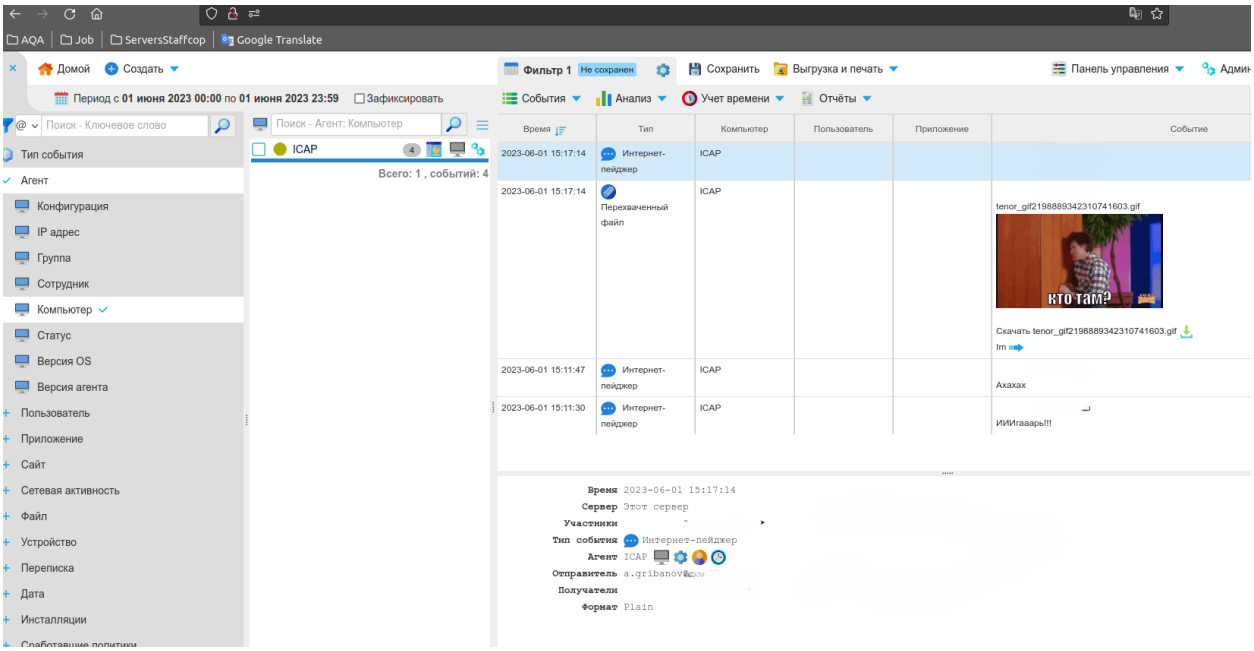
Значение в строке **Port** может иметь вид *0.0.0.0:13440*. В этом случае в качестве **port_icap** нужно будет указать *13440*.

Таким образом, для сервера iBatyr Monitor, расположенного по адресу 10.0.0.1, **URI ICAP сервера** имеет вид *icap://10.0.0.1:13440/ibatyr*.

7. В поле **IP адрес источника запроса** укажите IP-адрес сервера iBatyr Monitor с ICAP или название для отображения в веб-интерфейсе iBatyr Monitor. Например, *ICAP*.
8. Нажмите **Сохранить**, появится надпись **Настройки обновлены**.

Готово! Перехват Express настроен и запущен.

Чтобы проверить работу перехвата, залогинтесь в мессенджере и отправьте сообщение. В веб-интерфейсе сервера iBatyr Monitor можно будет увидеть событие перехвата.



4.5.5 Отслеживание входа в Контур.ID

Контур.ID — это система управления доступом, которая фиксирует все попытки входа в корпоративные приложения. Пользователи авторизуются через единый аккаунт, а система хранит логи входов.

iBatyr Monitor (iBatyr Monitor) позволяет анализировать неправомерный доступ к защищенной информации (ЗИ) на основе полученных от Контура.ID логов. Данные отображаются в интерфейсе iBatyr Monitor в виде событий **Инцидент К.ID**. На их основе можно расследовать инциденты по цепочкам событий после входа.

iBatyr Monitor получает данные от Контур.ID через API.

Как настроить интеграцию

1. Настройте API Контура.ID.
2. Включите интеграцию в конфигурации iBatyr Monitor.

Чтобы включить интеграцию, откройте файл **/etc/ibatyr/config** и добавьте в него параметры:

```
KONTUR_ID_ENABLED = True
KONTUR_ID_KEY = "90wh39h-1j49-l3ra-fq29-t336b127j3p"
KONTUR_ID_URL = "https://kid.kontur.ru/api/mfa/events"
KONTUR_ID_TIMEOUT_MIN = 5
KONTUR_ID_TIMEOUT_OFFSET_MIN = 0
```

где

tabularytabulary

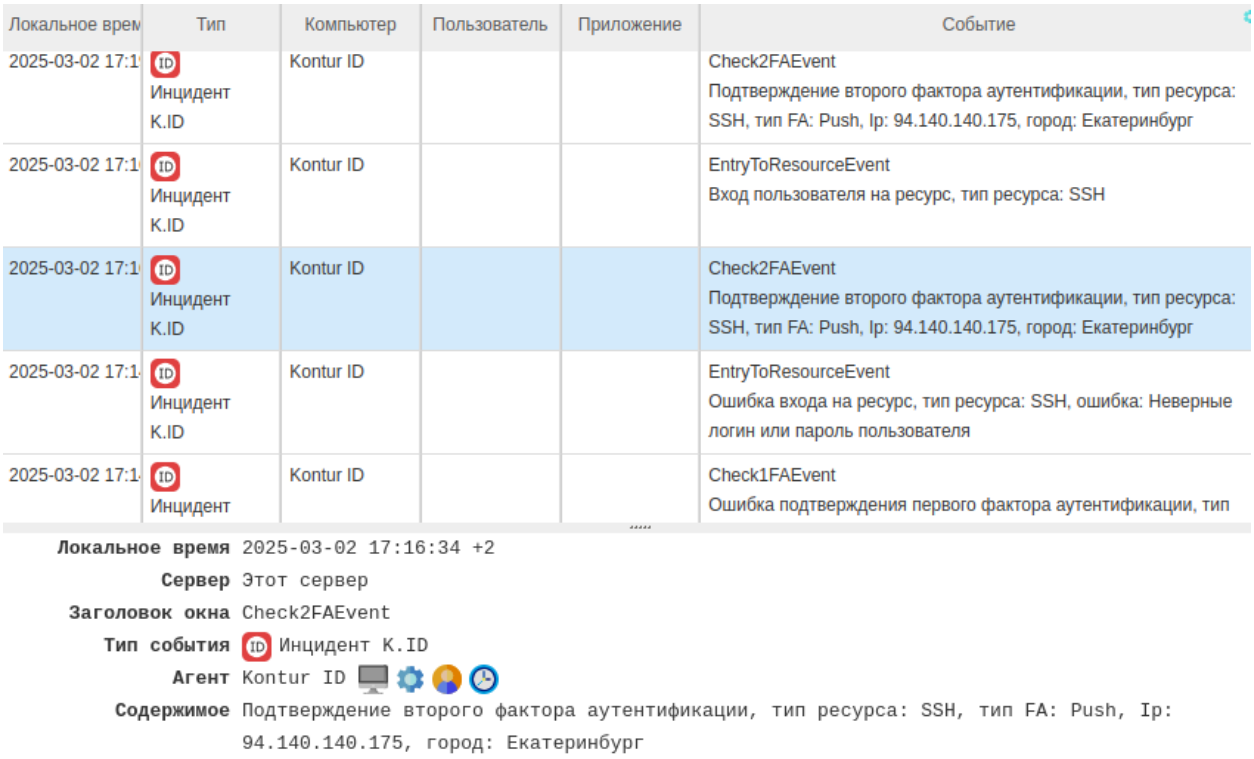
Параметр
KONTUR_ID_ENABLED = True
KONTUR_ID_KEY = "390wh39h-1j49-l3ra-fq29-t336b127j3pp"
KONTUR_ID_URL = "https://kid.kontur.ru/api/mfa/events"
KONTUR_ID_TIMEOUT_MIN = 5
KONTUR_ID_TIMEOUT_OFFSET_MIN = 0

После установки параметра `kontur_id` в значение `True` на сервер будут приходить события **Инцидент K.ID**.

Предупреждение: Не оставляйте параметры пустыми, иначе события не будут приходить на сервер. Значения в параметре `kontur_id_timeout_offset_min` не должны превышать 1440.

Нажмите на инцидент, чтобы внизу таблицы событий появились данные события:

[1] Помогает избежать потери событий, если предыдущий запрос к Контур.ID не сработал из-за задержки или сбоя. При каждом запросе агент запрашивает события за период, равный `kontur_id_timeout_min` + `kontur_id_timeout_offset_min`. Если запрос не сработает, в следующем запросе придет часть событий за указанное в параметре время. Например, при параметрах `kontur_id_timeout_min = 5` и `kontur_id_timeout_offset_min = 1` агент будет запрашивать данные за последние 6 минут.



Локальное врем	Тип	Компьютер	Пользователь	Приложение	Событие
2025-03-02 17:1	Инцидент K.ID	Kontur ID			Check2FAEvent Подтверждение второго фактора аутентификации, тип ресурса: SSH, тип FA: Push, Ip: 94.140.140.175, город: Екатеринбург
2025-03-02 17:1	Инцидент K.ID	Kontur ID			EntryToResourceEvent Вход пользователя на ресурс, тип ресурса: SSH
2025-03-02 17:1	Инцидент K.ID	Kontur ID			Check2FAEvent Подтверждение второго фактора аутентификации, тип ресурса: SSH, тип FA: Push, Ip: 94.140.140.175, город: Екатеринбург
2025-03-02 17:1	Инцидент K.ID	Kontur ID			EntryToResourceEvent Ошибка входа на ресурс, тип ресурса: SSH, ошибка: Неверные логин или пароль пользователя
2025-03-02 17:1	Инцидент	Kontur ID			Check1FAEvent Ошибка подтверждения первого фактора аутентификации, тип

Локальное время 2025-03-02 17:16:34 +2
Сервер Этот сервер
Заголовок окна Check2FAEvent
Тип события Инцидент K.ID
Агент Kontur ID
Содержимое Подтверждение второго фактора аутентификации, тип ресурса: SSH, тип FA: Push, Ip: 94.140.140.175, город: Екатеринбург

Событие Инцидент K.ID

Событие **Инцидент K.ID** содержит ключевые данные, которые помогают понять, что именно произошло, где и когда.

Как использовать данные для расследования

Используйте полученные данные для мониторинга подозрительной активности и расследования инцидентов. Ниже приведено несколько примеров.

Подбор пароля

Признаки: в событиях **Инцидент K.ID** появились многочисленные ошибки *Неверные логин или пароль* с одного IP-адреса с интервалом 1–2 секунды, это может быть brute-force атака.

Что делать: заблокируйте IP и проверьте, не было ли успешного входа.

Отключение двухфакторной аутентификации

Признаки: в логах появился заголовок окна *Skip2FAEvent*, а политика аутентификации не позволяет отключение двухфакторной аутентификации. Возможно, кто-то снял защиту.

Что делать: проверьте, кто изменил настройки. Если это несанкционированное действие, отключите учетную запись.

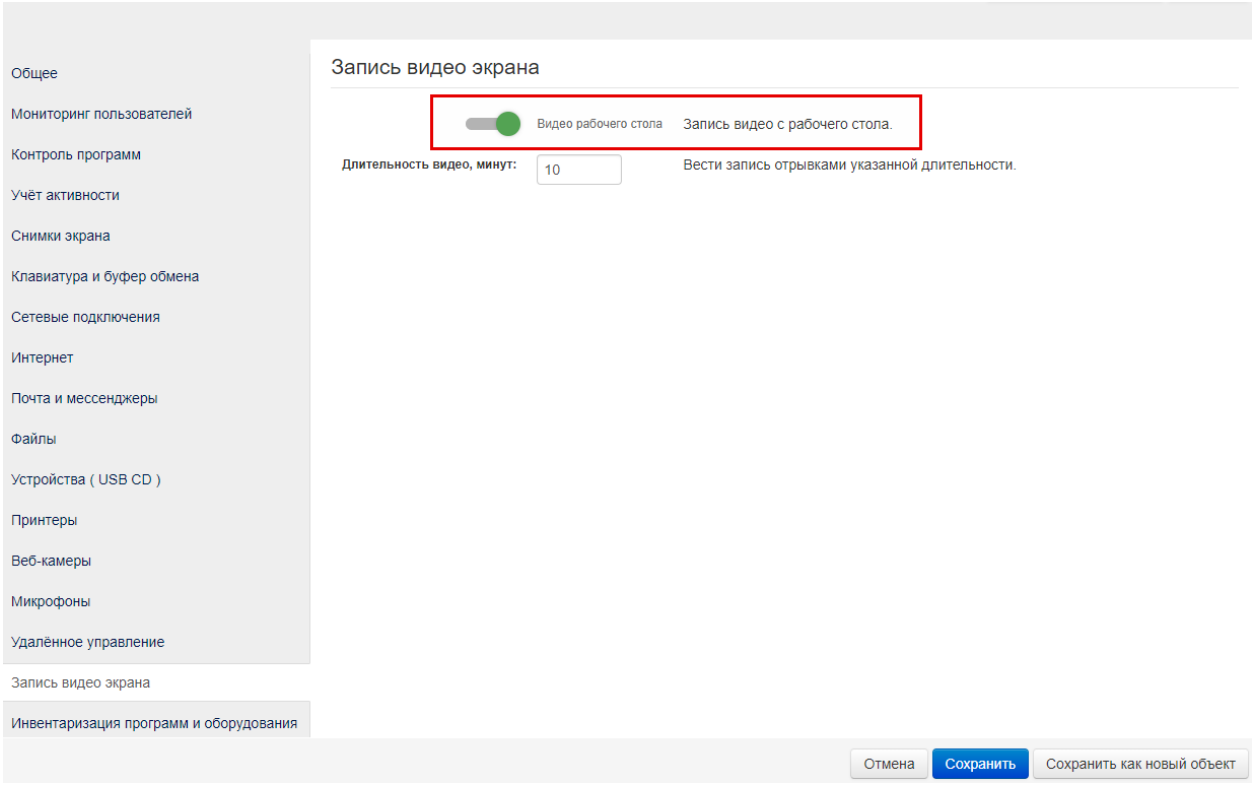
Вход в необычное время

Признаки: сотрудник, работающий с 9:00 до 18:00, зашел в систему в 03:30 с неизвестного IP. Логи *Check1FAEvent* и *Check2FAEvent* подтверждают успешную аутентификацию.

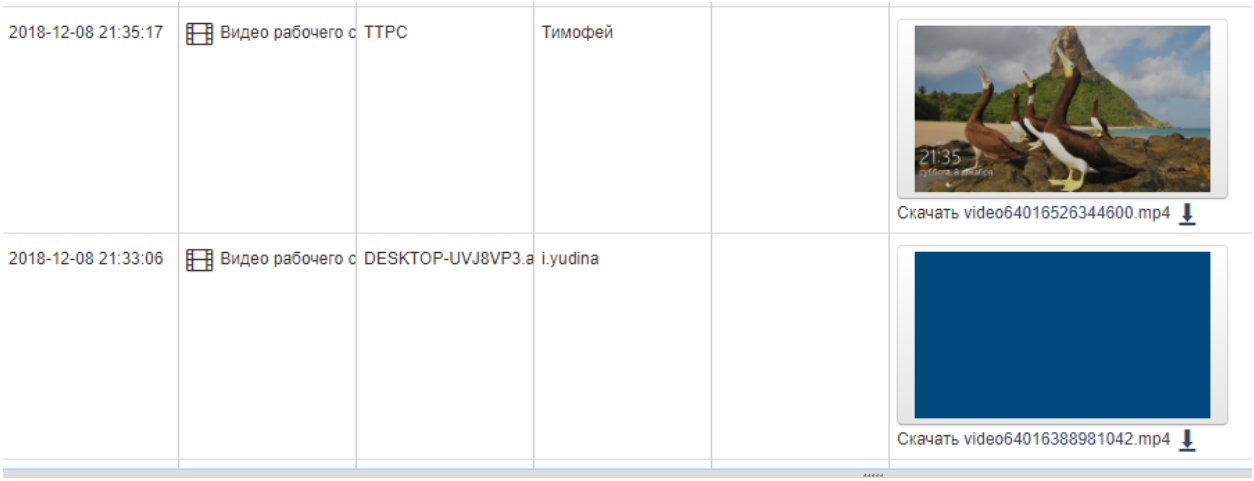
Что делать: начните расследование с проверки событий после входа, чтобы понять, какие действия выполнил пользователь.

4.5.6 Видеоконтроль и удаленное подключение к агенту

Для работы функции **Видеоконтроль**, т. е. записи видео рабочего стола пользователя, необходимо настроить конфигурацию как на скриншоте:

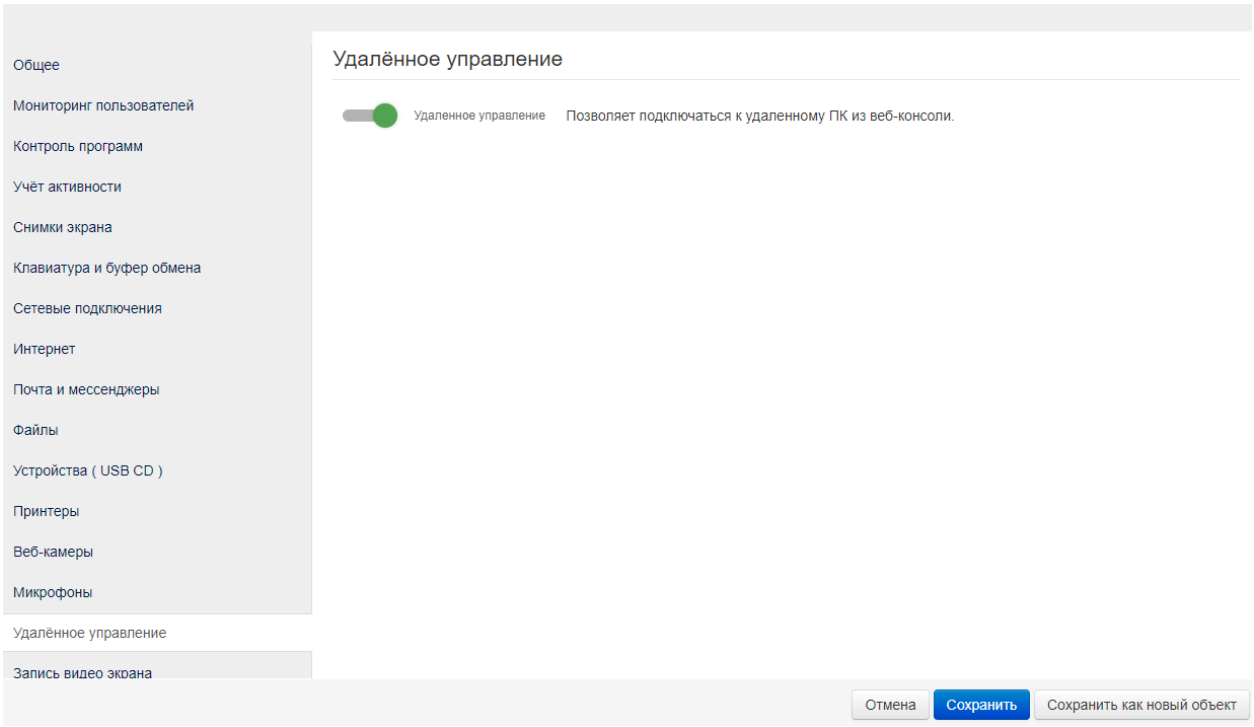


Записанные видео можно посмотреть, выбрав **Тип события** → **Видео рабочего стола** и нажать на иконку видео.



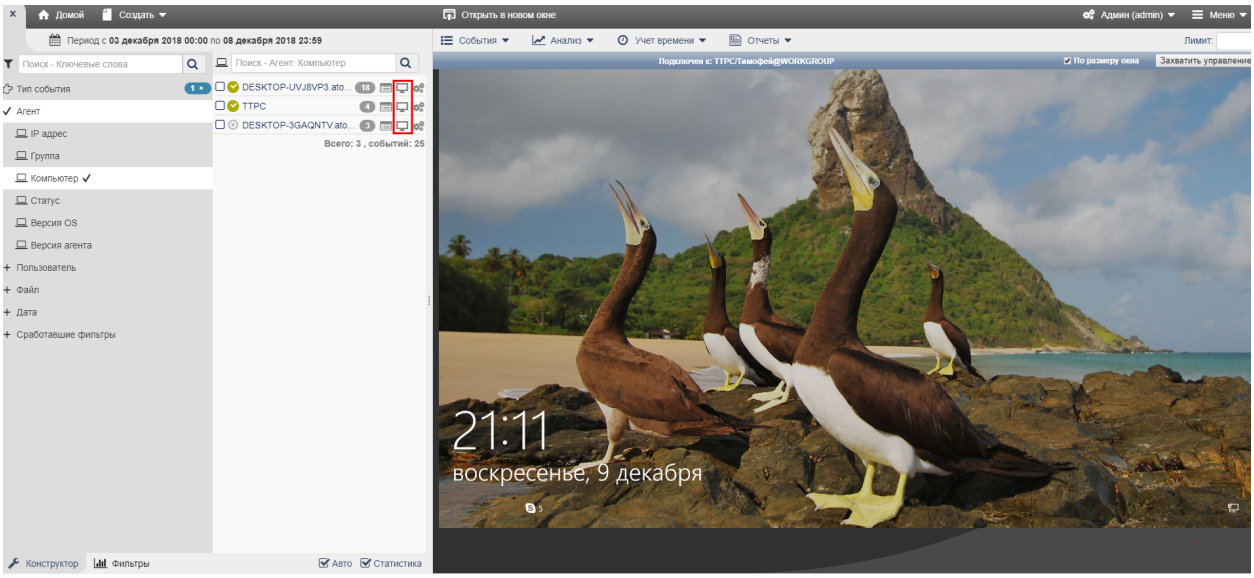
Также записанные видео можно скачать по ссылке под превью видео.

Удалённое подключение к рабочему столу настраивается следующим образом:

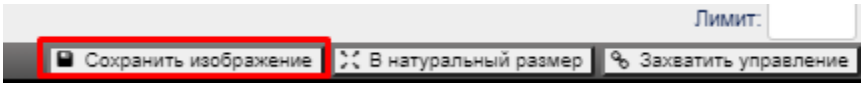


Удалённое подключение к любому агенту возможно через нажатие иконки **Удалённого подключения** на соответствующем агенте в веб-консоли.

Для перехвата управления клавиатуры и мыши на удаленной станции пользователя можно нажать кнопку **Захватить управление**. При этом вы сможете управлять компьютером с помощью своей мыши и клавиатуры, не теряя возможности управления системой удалённым пользователем.



Для того чтобы сделать скриншот рабочего стола, нажмите на кнопку **Сохранить изображение**:

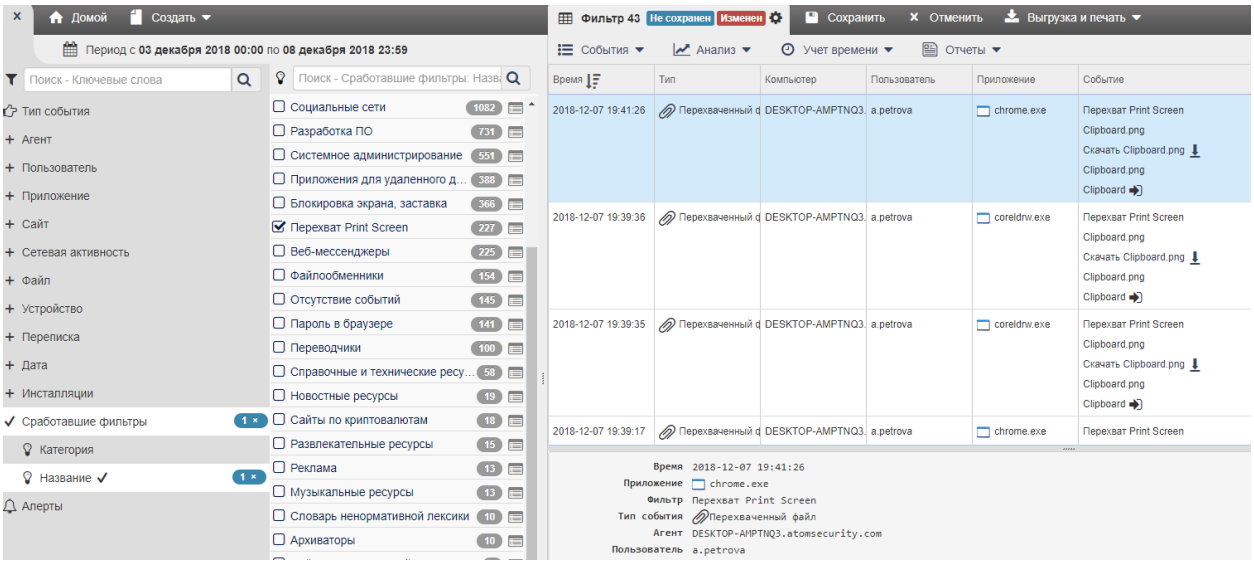


4.5.7 Как найти перехваченные скриншоты

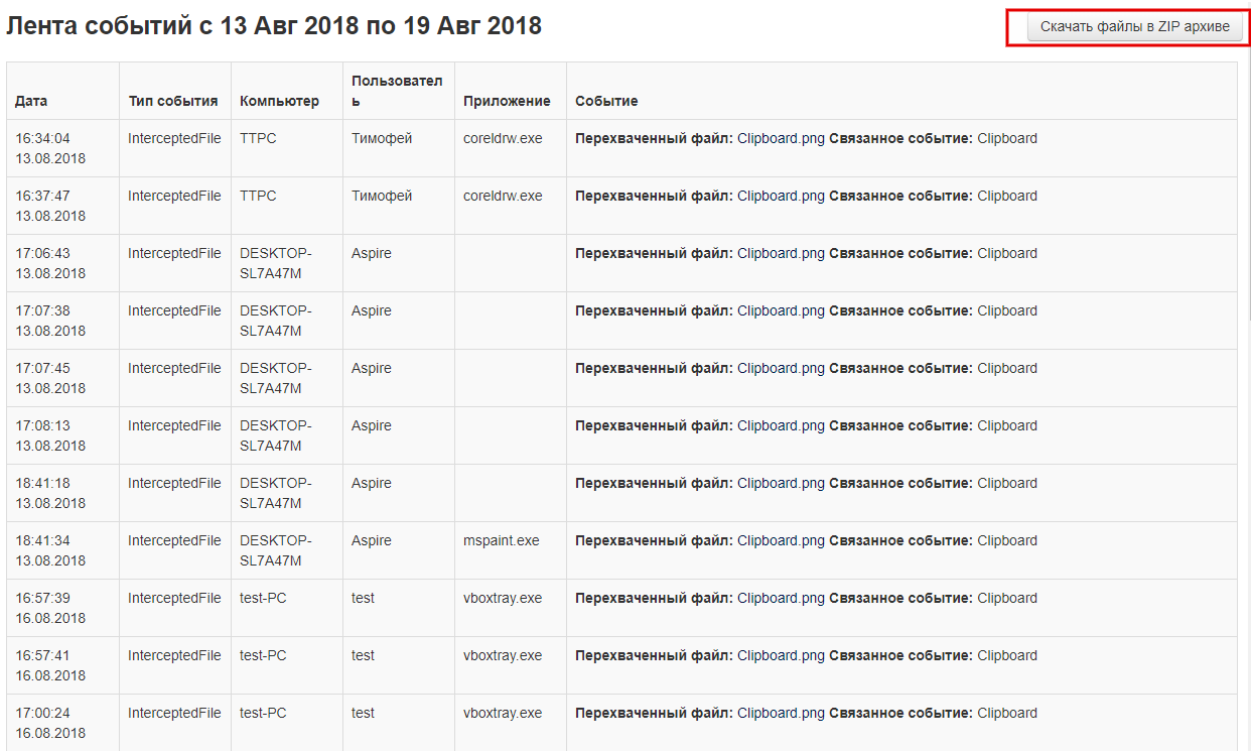
Чтобы найти все файлы, которые попали в буфер обмена после нажатия Print Screen:

1. Убедитесь, что в конфигурации компьютера в модуле **Клавиатура и буфер обмена** включен *Буфер обмена*.
2. Перейдите **Сработавшие политики** → **Название**.
3. Выберите в списке значений **Перехват Print Screen**.

После этого в **Линзу** будут приходить события **Перехват Print Screen**:



Если в меню **Отчеты** выбрать тип отчёта **Лента событий**, отобразятся все перехваченные снимки экрана. Чтобы скачать снимки, нажмите **Скачать файлы в ZIP-архиве**.

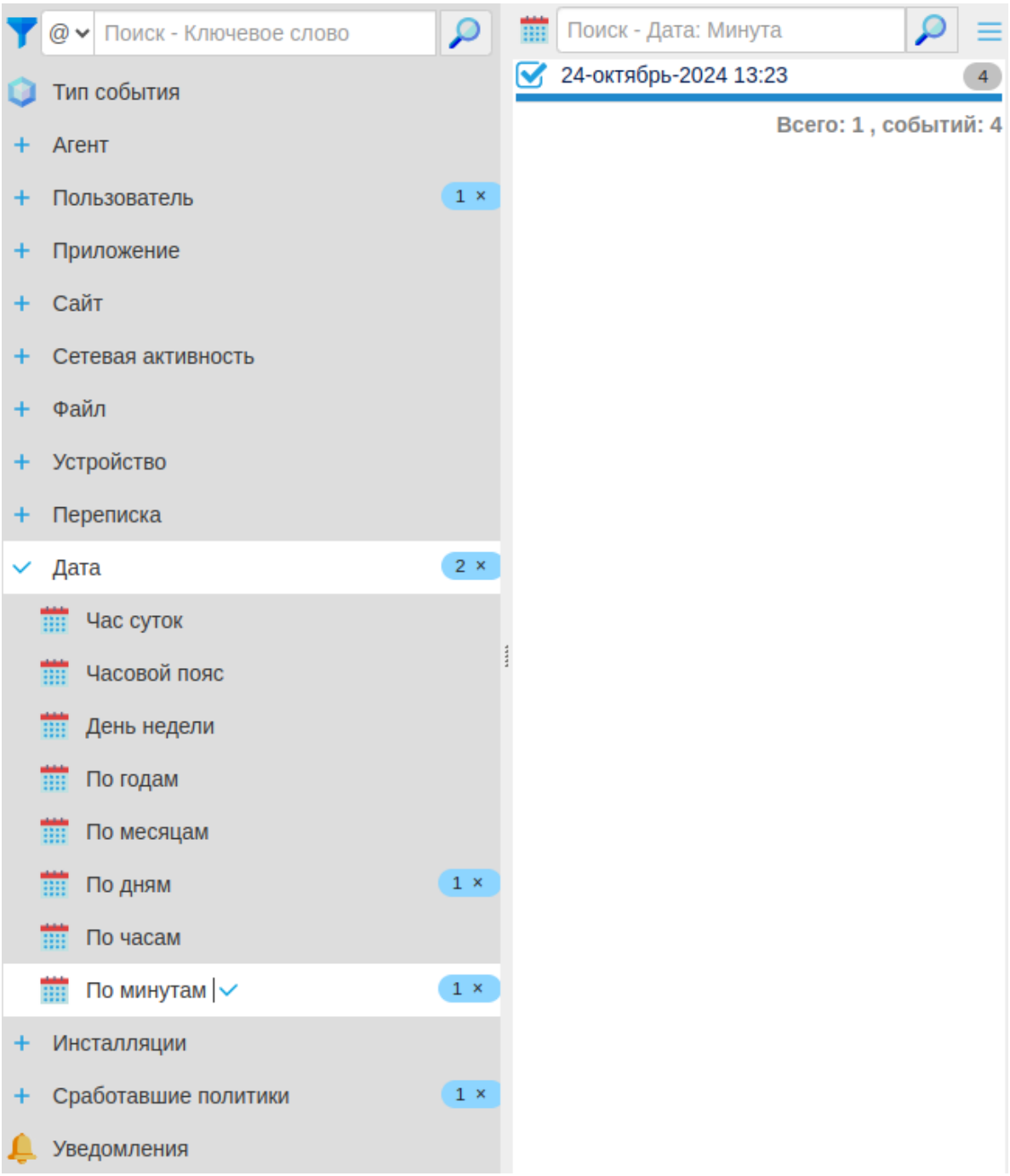


Дата	Тип события	Компьютер	Пользователь	Приложение	Событие
16:34:04 13.08.2018	InterceptedFile	TTPC	Тимофей	coreldrw.exe	**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
16:37:47 13.08.2018	InterceptedFile	TTPC	Тимофей	coreldrw.exe	**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
17:06:43 13.08.2018	InterceptedFile	DESKTOP-SL7A47M	Aspire		**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
17:07:38 13.08.2018	InterceptedFile	DESKTOP-SL7A47M	Aspire		**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
17:07:45 13.08.2018	InterceptedFile	DESKTOP-SL7A47M	Aspire		**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
17:08:13 13.08.2018	InterceptedFile	DESKTOP-SL7A47M	Aspire		**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
18:41:18 13.08.2018	InterceptedFile	DESKTOP-SL7A47M	Aspire		**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
18:41:34 13.08.2018	InterceptedFile	DESKTOP-SL7A47M	Aspire	mspaint.exe	**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
16:57:39 16.08.2018	InterceptedFile	test-PC	test	vboxtray.exe	**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
16:57:41 16.08.2018	InterceptedFile	test-PC	test	vboxtray.exe	**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard
17:00:24 16.08.2018	InterceptedFile	test-PC	test	vboxtray.exe	**Перехваченный файл:** Clipboard.png **Связанное событие:** Clipboard

Обычно в архиве не так много файлов, но иногда среди них можно найти опасные скриншоты, например печать с заверенной подписью руководителя организации. С помощью копипаст таких изабражений можно подписать несогласованные документы.

Чтобы понять, кто сделал скриншот:

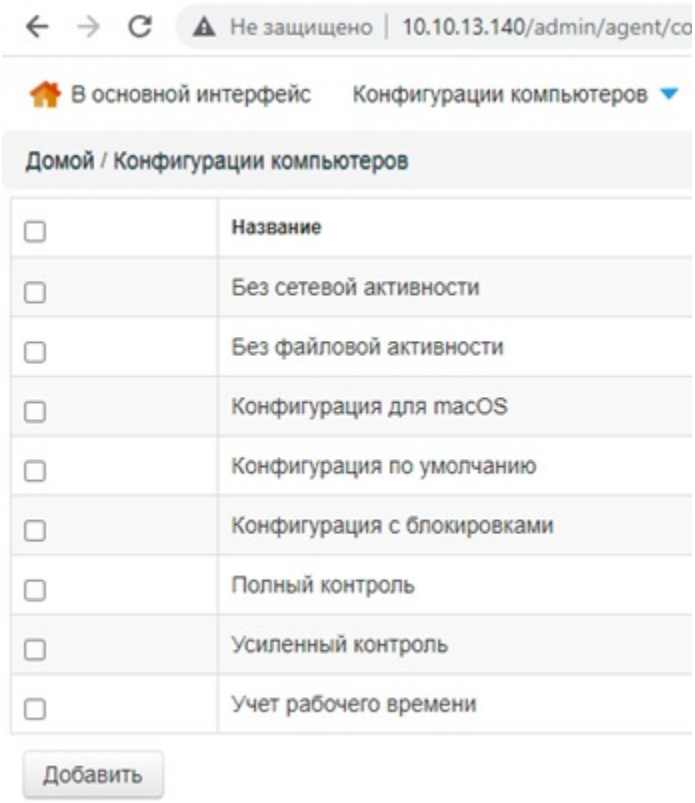
1. Установите измерения:
   - **Сработавшие политики** → **Название** → **Перехват Print Screen**;
   - **Пользователь**.
2. В измерении **Дата** выберите день и время создания скриншота.



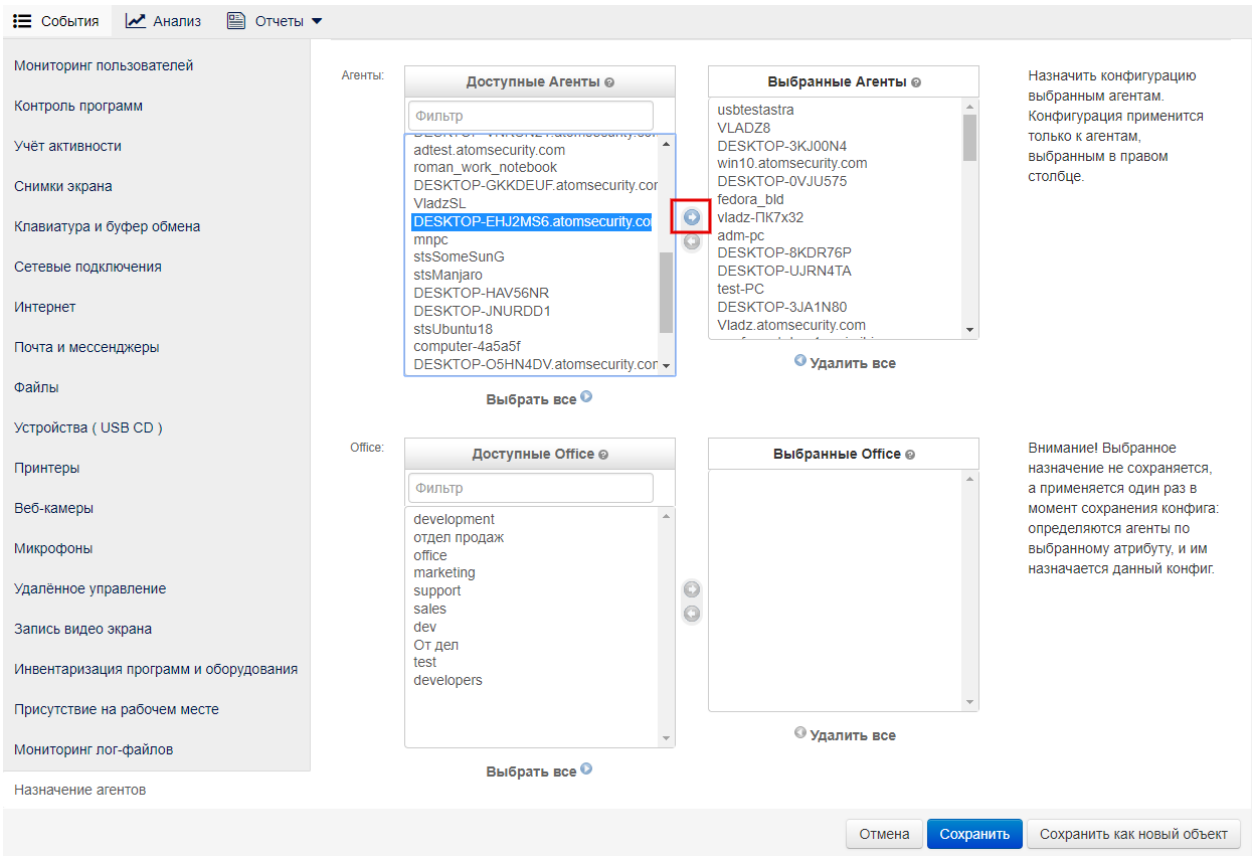
В **Линзе** появятся скриншоты, сделанные пользователями в указанное время.

4.5.8 Как сменить конфигурацию у компьютеров

Чтобы поменять конфигурацию у компьютеров, в разделе **Панель управления** → **Конфигурации компьютеров** выберите конфигурацию, которую хотите назначить.

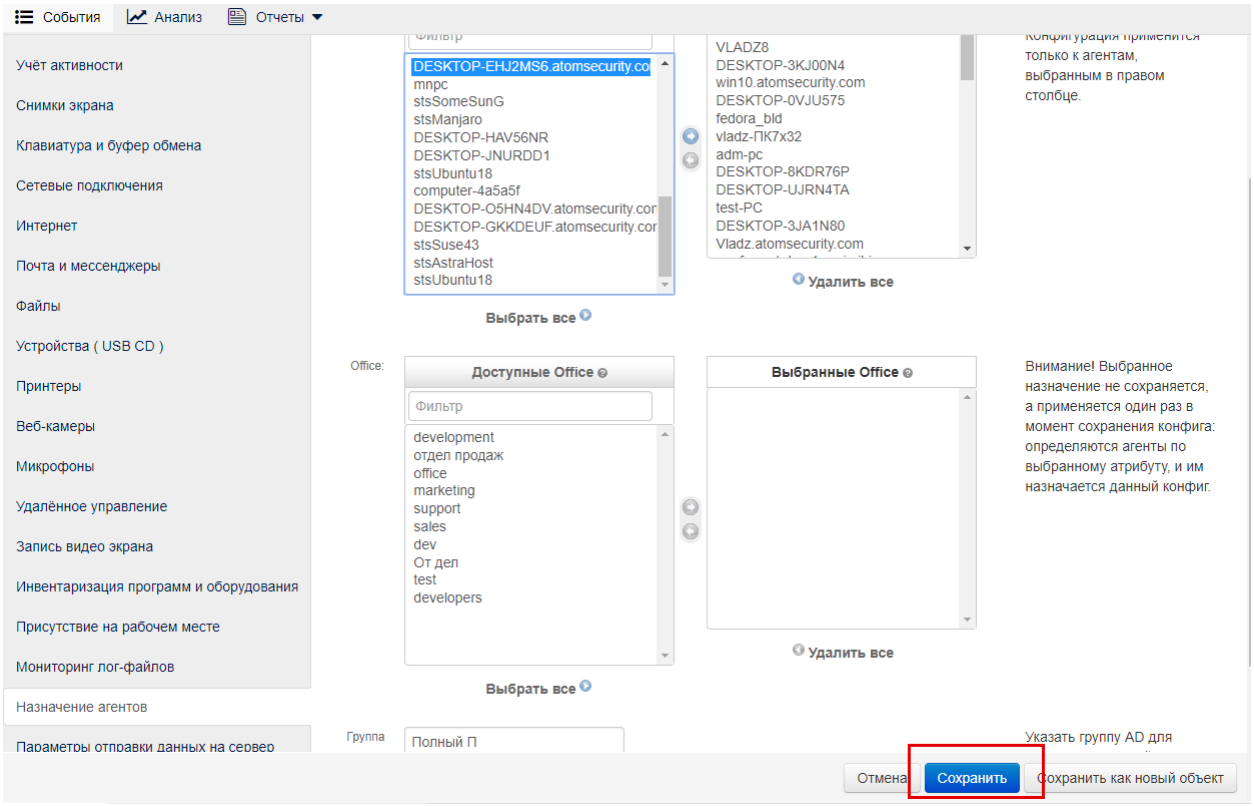


В настройках конфигурации перейдите в раздел **Назначение агентов**. Выберите машины, которым хотите назначить данную кофигурацию.



Примечание: Для добавления ПК из AD, убедитесь, что у вас настроено *подключение к AD*.

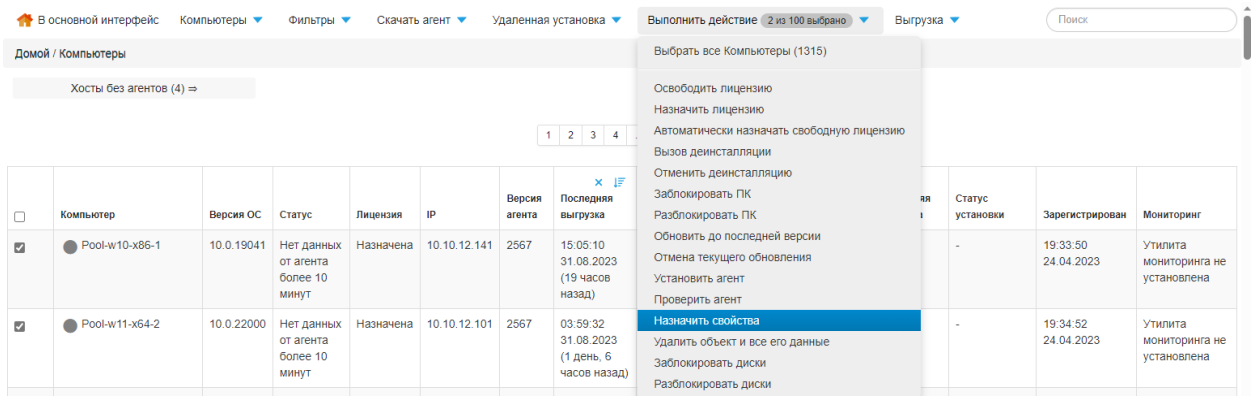
Нажмите кнопку **Сохранить**.



Массовая смена конфигураций у компьютеров

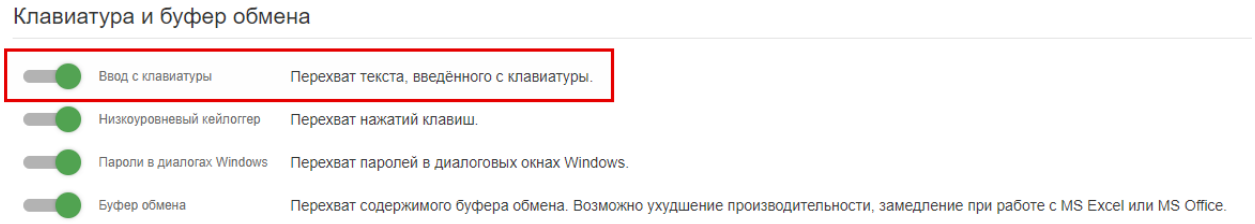
Чтобы изменить конфигурацию для множества новых агентов:

1. Зайдите в раздел **Панель управления** → **Компьютеры**.
2. Необходимые компьютеры.
3. В меню **Выполнить действие** выберите **Назначить свойства**.

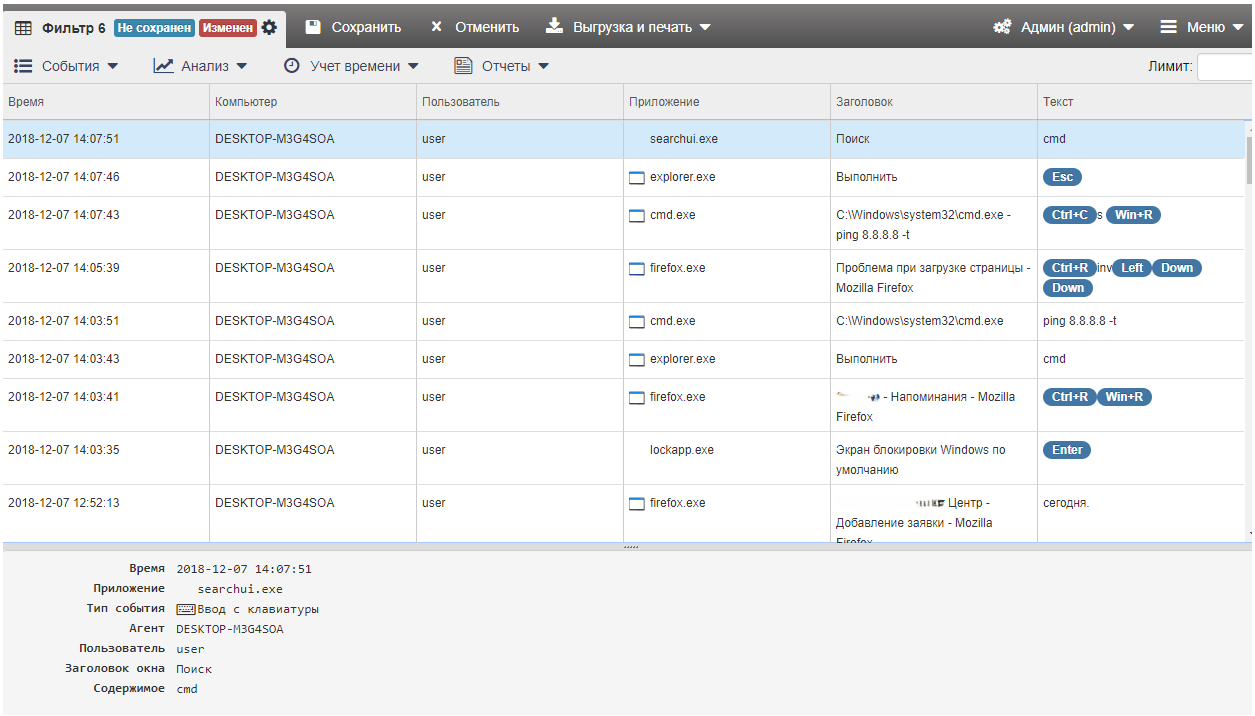


4.5.9 Кейлоггер

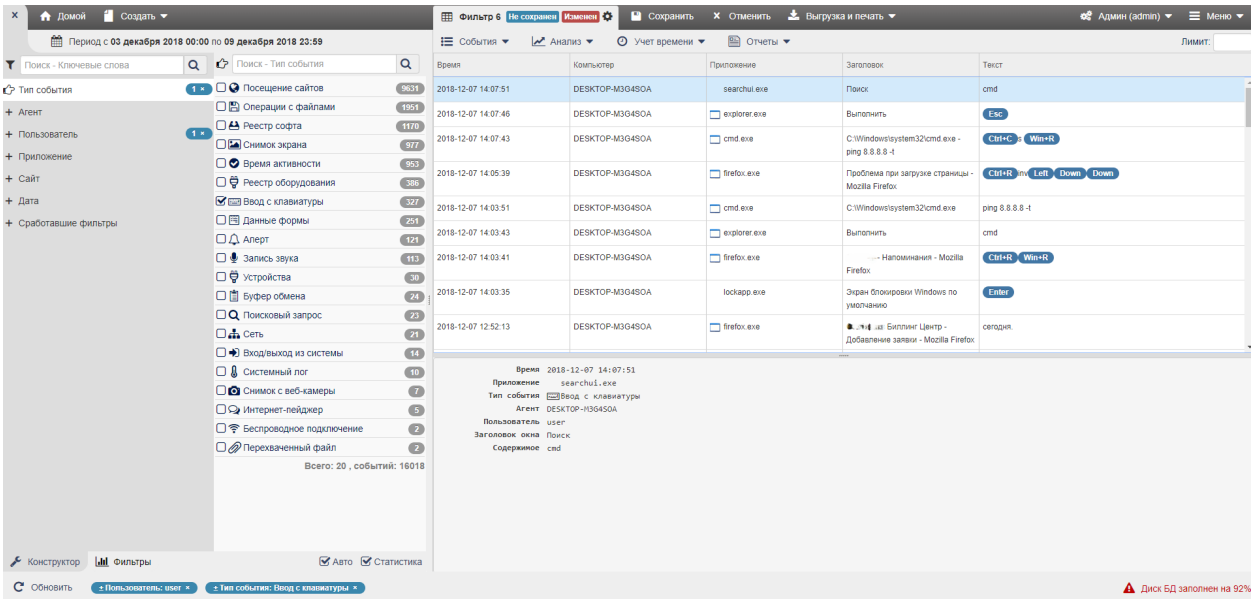
Чтобы убедиться, что нужный модуль перехвата включен, необходимо открыть конфигурацию агента и в разделе **Клавитура и буфер обмена** включить модуль **Ввод с клавиатуры**, далее **Сохранить**.



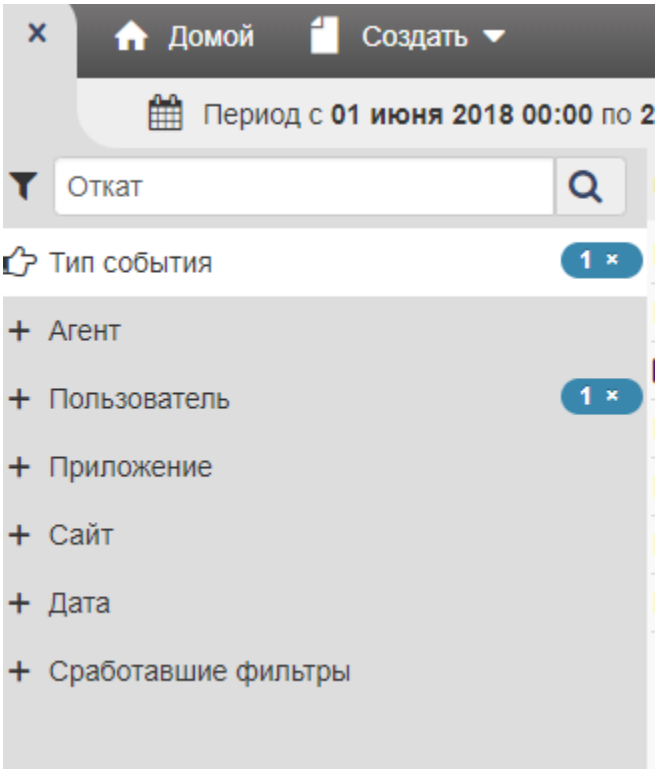
Через некоторое время агент получит и применит новую конфигурацию, после чего в **События** → **Таблица** можно будет увидеть факты перехвата, содержащие текст.



Чтобы отфильтровать факты по пользователю, необходимо нажать на имя пользователя в столбце **Пользователь**. После этого внизу добавится синий значок с критерием *Пользователь: user*.



Можно искать по ключевым словам в перехваченном тексте. Для этого вводим ключевое слово «**Откат**» в поле **Поиск/Ключевые слова**:

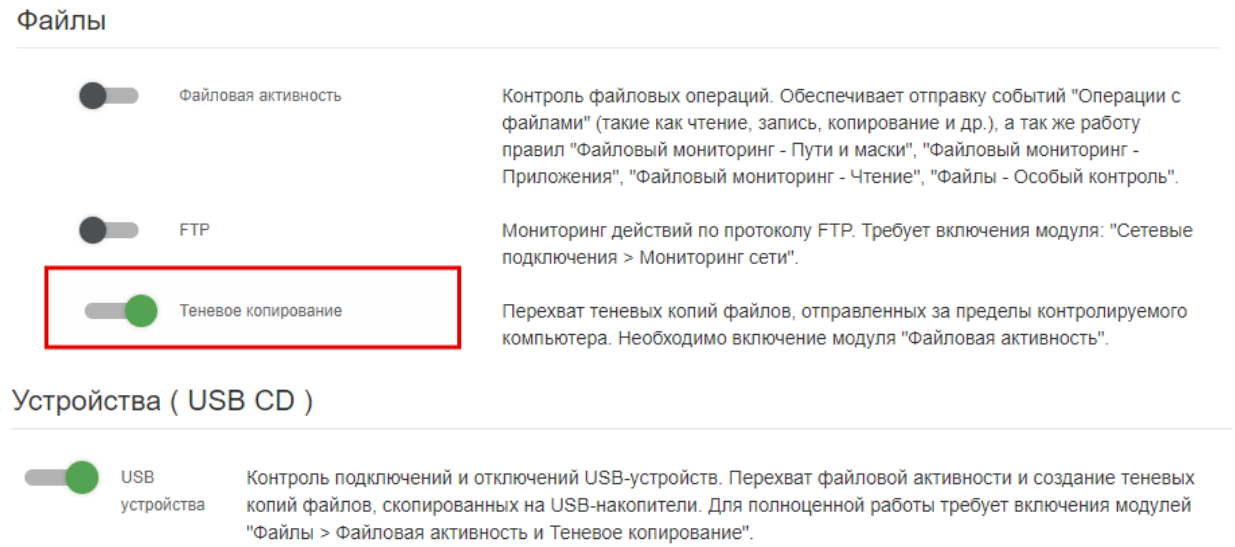


Жмём **Enter** и получаем отфильтрованные факты:

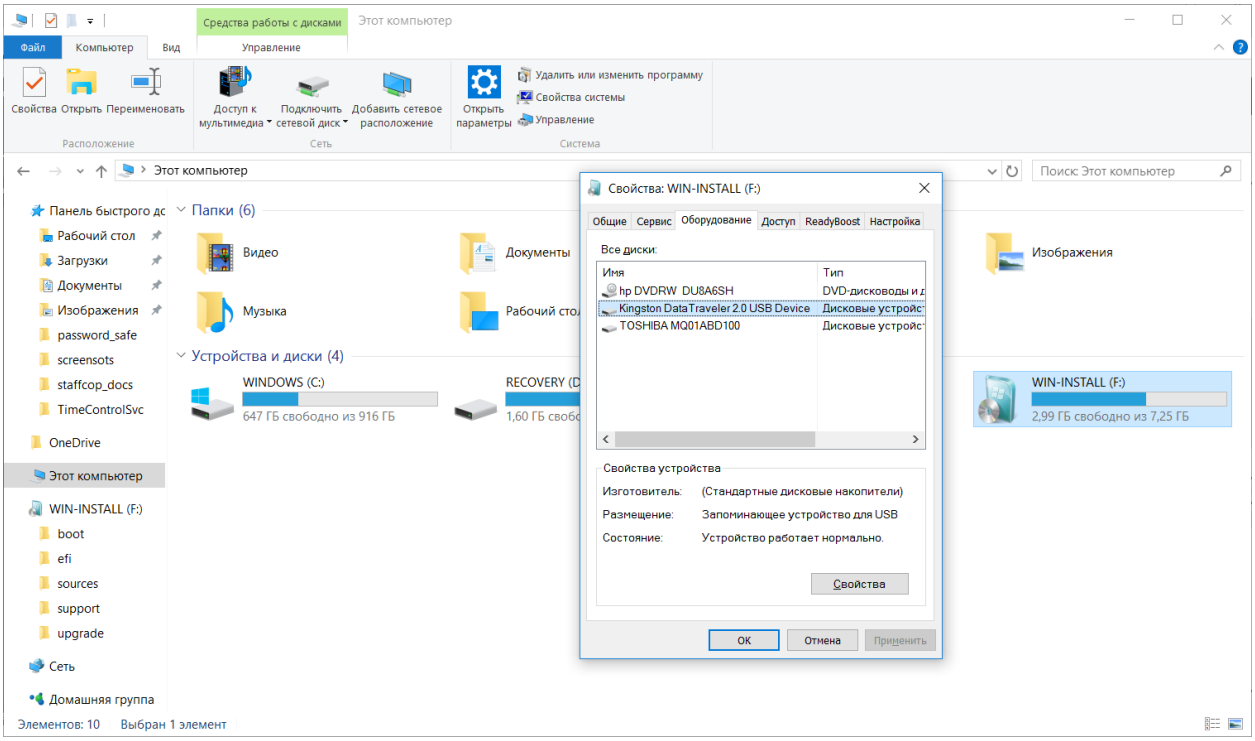
Время	Компьютер	Приложение	Заголовок	Текст
2018-11-20 17:47:44	DESKTOP-M3G4SOA	explorer.exe	Загрузки	проценты откаты Ctrl+C Ctrl+V
2018-11-20 17:47:27	DESKTOP-M3G4SOA	firefox.exe	Mozilla Firefox	ghjwtyns прор откаты Ctrl+W Win+D
2018-11-16 18:51:07	DESKTOP-M3G4SOA	notepad.exe	словарь_откатов — Блокнот	Ctrl+A Ctrl+C Alt+Tab
2018-11-16 18:50:28	DESKTOP-M3G4SOA	firefox.exe	- Mozilla Firefox	deСловарь откатов тест Tab
2018-10-03 17:23:40	DESKTOP-6UFKRKU	notepad.exe	откаты.txt - Notepad	Ctrl+V Ctrl+S
2018-10-03 17:23:31	DESKTOP-6UFKRKU	thunderbird.exe	Attach File(s)	щелфеоткаты
2018-06-01 21:07:34	DESKTOP-6UFKRKU	teamviewer.exe	K0777 - TeamViewer	откат

4.5.10 Контроль внешних дисков

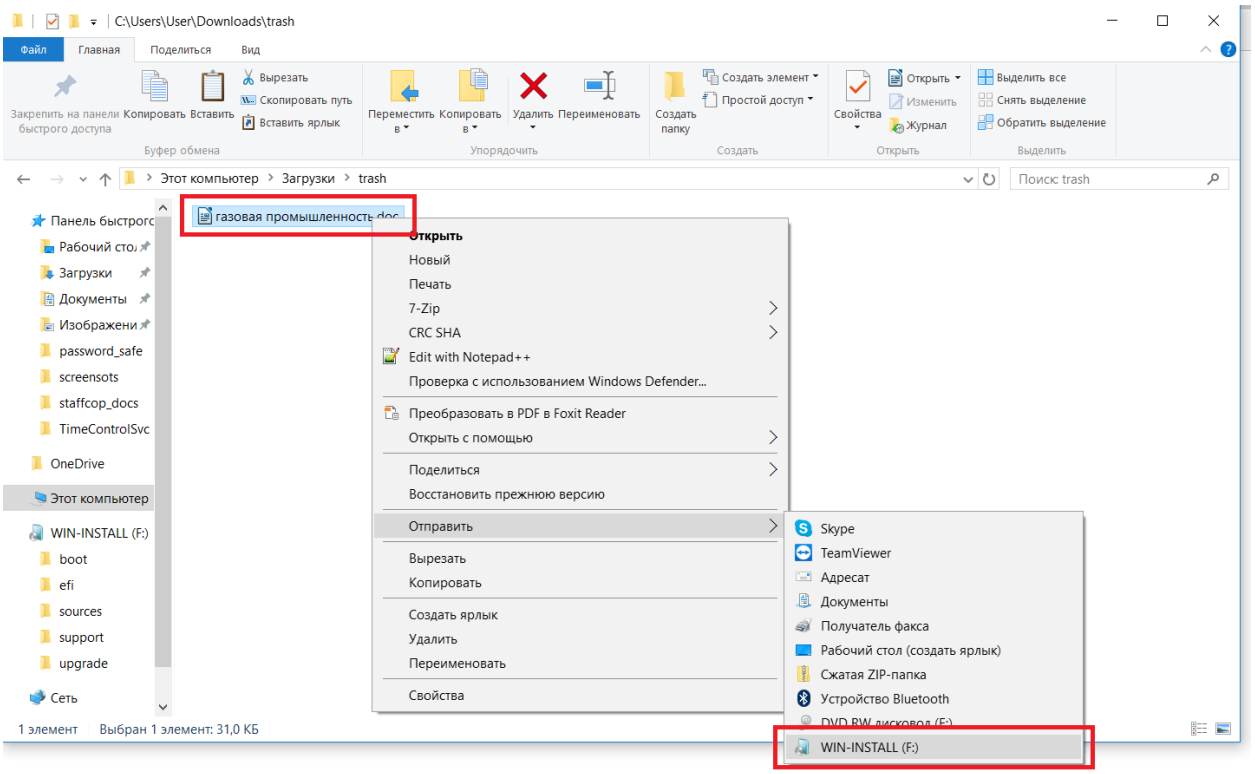
Убедитесь, что в конфигурации агента включены необходимые опции. Включите модули в меню **Устройства USB-CD → USB-Устройства** и **Файлы → Теневое копирование**. Если конфигурация изменилась, нажмите **Сохранить** и подождите несколько минут, пока она применится на контролируемых компьютерах.



Теперь подключите USB-диск (флешку) к одному из контролируемых компьютеров.



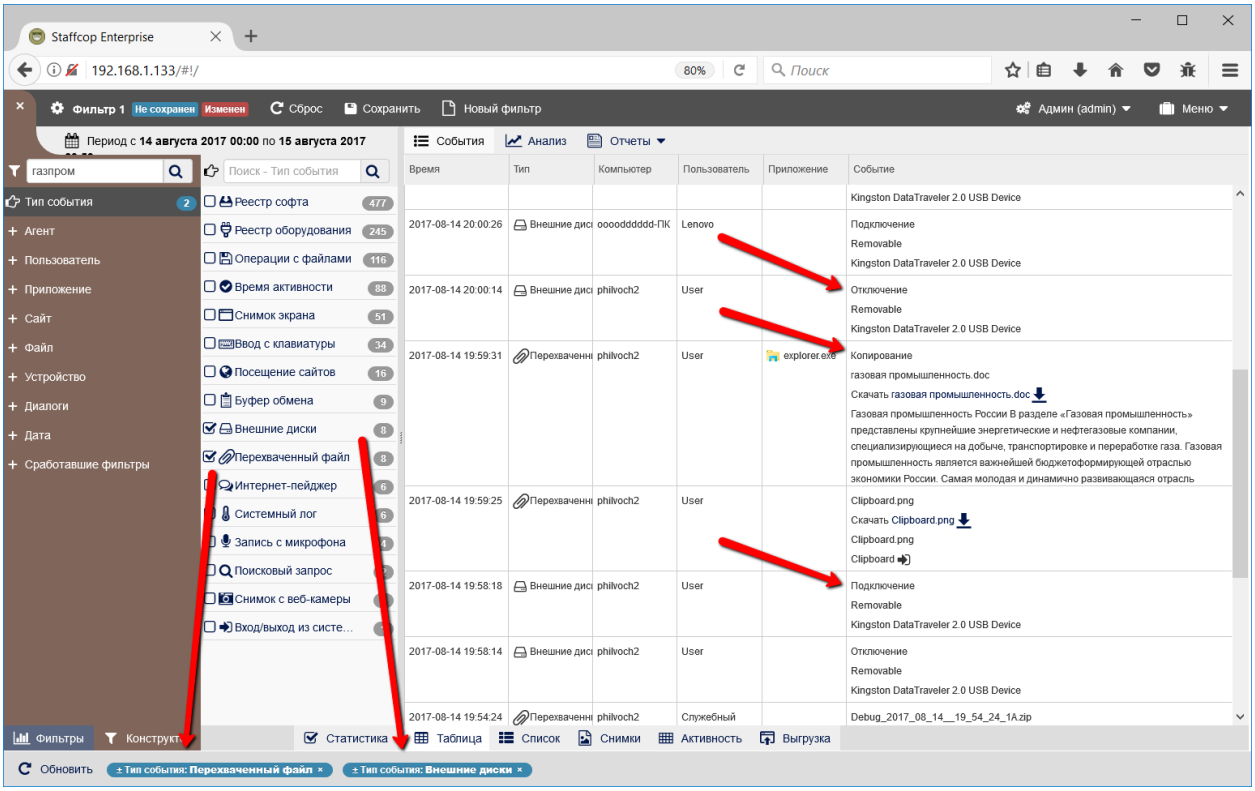
И скопируйте файл на подключенный носитель.



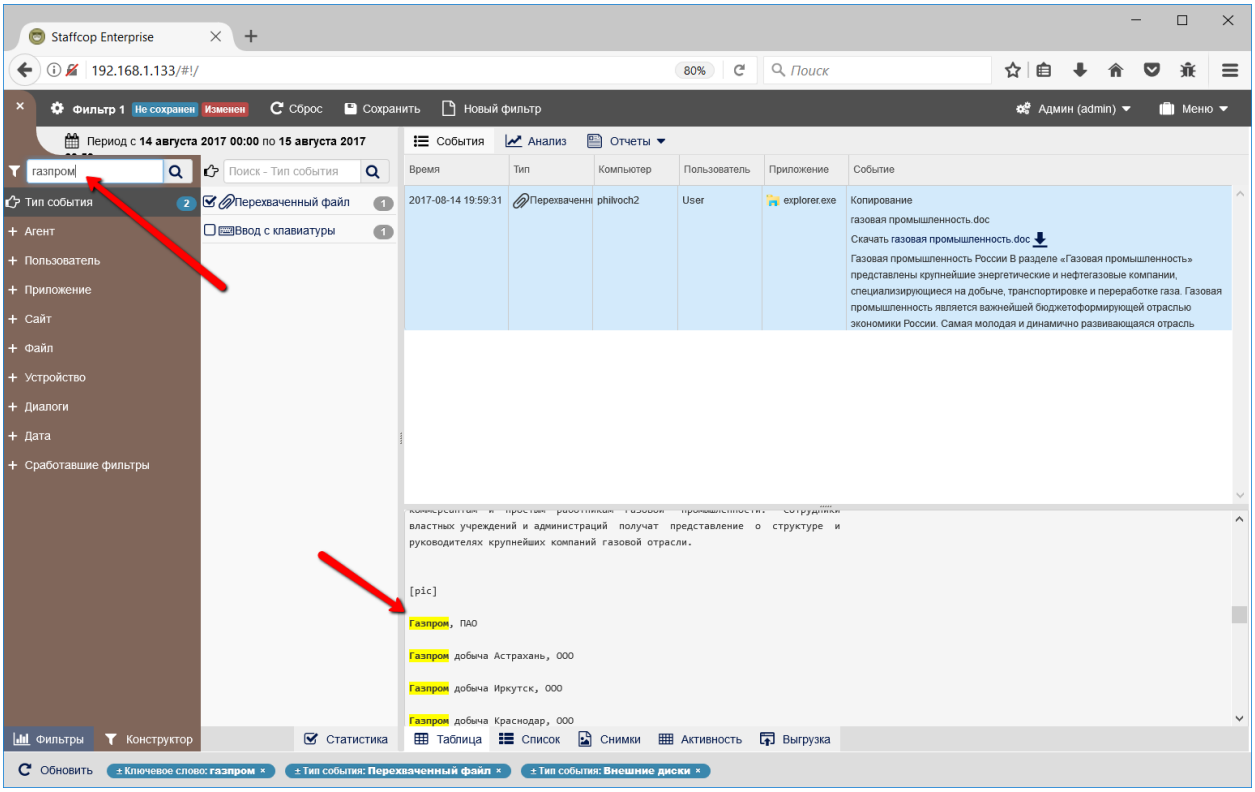
Извлеките USB-носитель.

В консоли iBatyr Monitor откройте основную страницу, вкладку **Тип события**. Выберите **Внешние диски** и **Перехваченные файлы**. В нижней панели появятся выбранные критерии, а в таблице —

результат перехвата: в 19:58:18. Пользователь *User* на машине *philvoch2* подключил съёмный диск *Kingston DataTraveler 2.0 USB Device* и скопировал на него файл с именем *Газовая промышленность*.

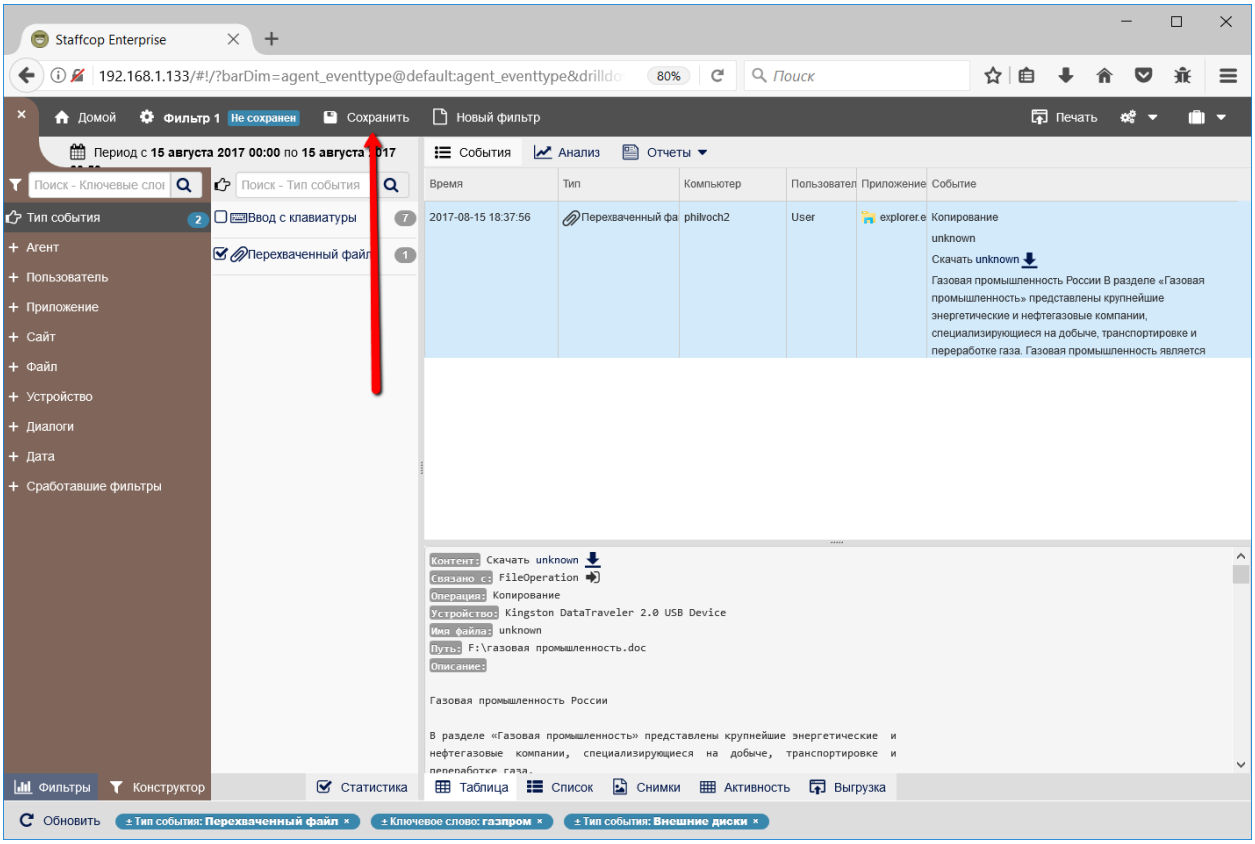


Вы можете выполнить поиск в содержимом перехваченного файла по важным словам. Например, введите ключевое слово *Газпром*. Вы увидите, что в перехваченном документе это слово нашлось.



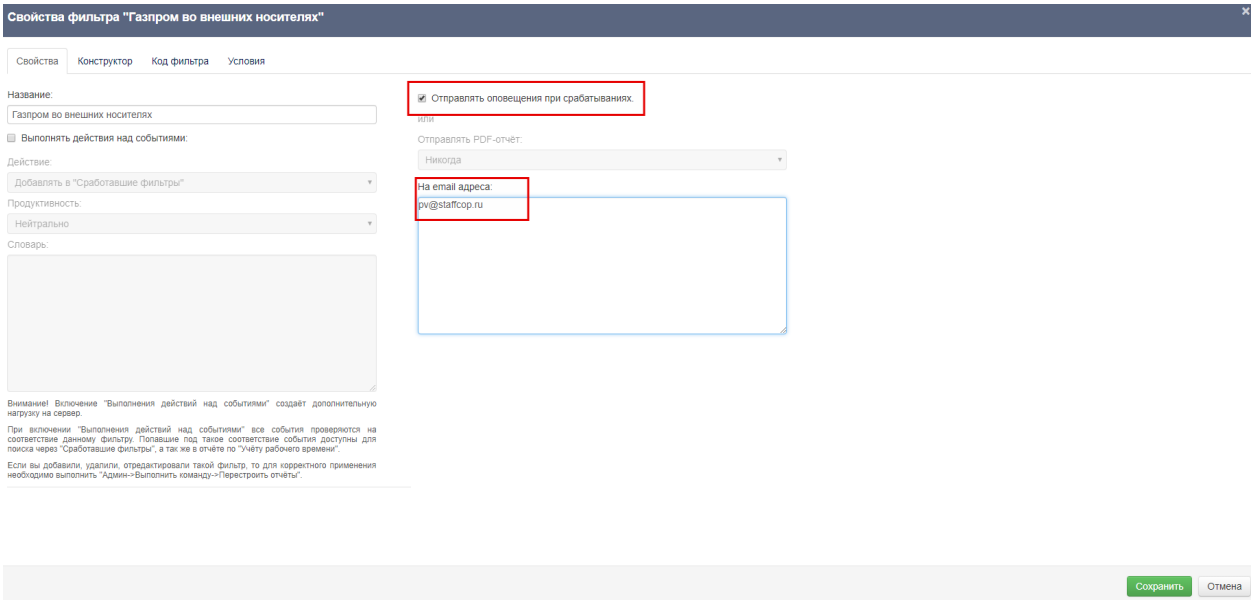
Далее вы можете сохранить выбранный фильтр и получать уведомления каждый раз, когда на каком-то из компьютеров под контролем агента iBatyr Monitor будет происходить событие копирования файла, в котором содержится слово *Газпром*.

Для этого кликните в верхней части окна на кнопку-ссылку **Сохранить** и укажите в параметрах фильтра *кому* присылать уведомление по сработавшему событию.



В данном случае письмо будет выслано адресату *pv@ibatyr.kz*.

После указания адресата для получения писем нажмите кнопку **Сохранить**.

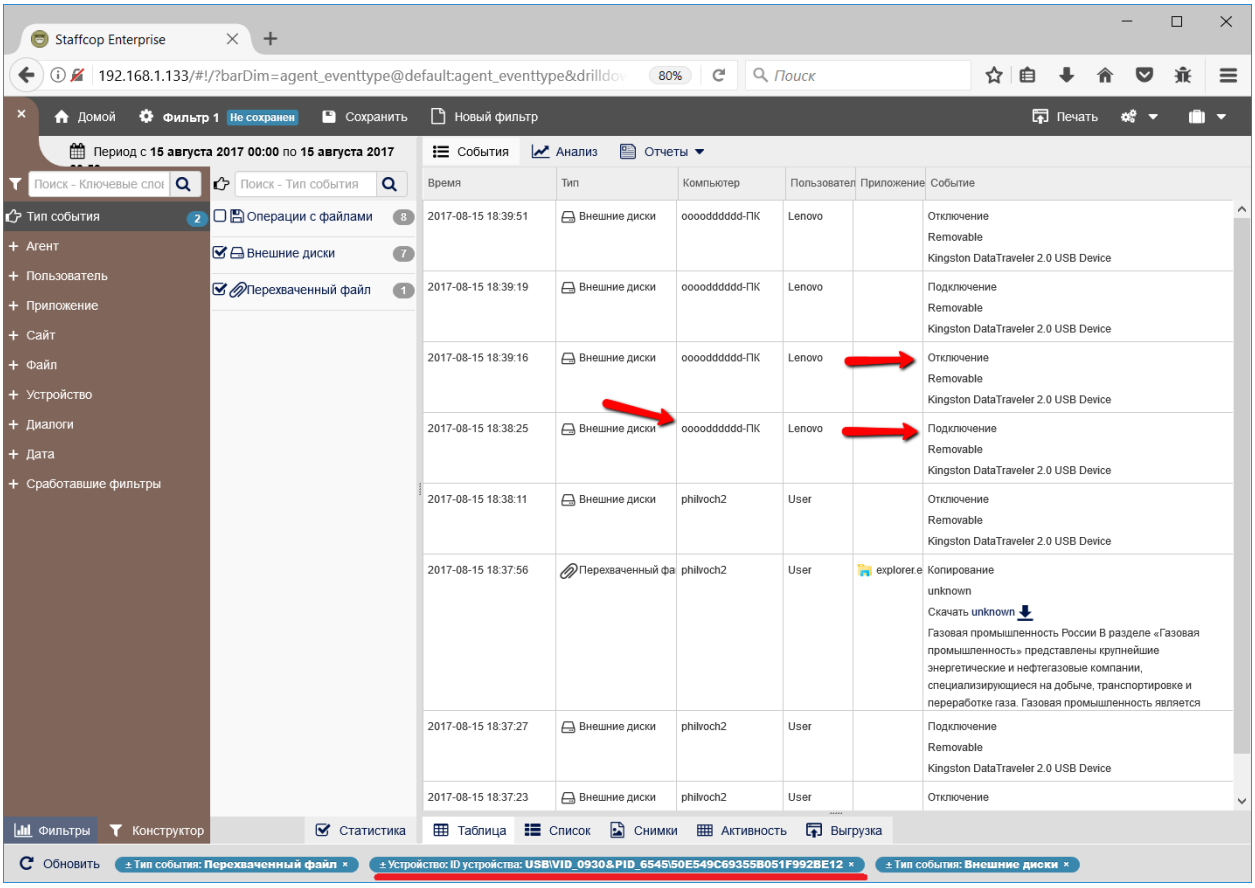


Также не стоит забывать, что перед тем, как письмо дойдёт до адресата, указанного в фильтре, необходимо настроить *почтовые параметры для рассылки писем*.

Если посмотреть на события, зафиксированные агентами на рабочих станциях, то очевидно, что та же самая флешка, с тем же уникальным номером, была подключена к другому компьютеру с именем

ooooddddddd-ПК и пользователем в системе Lenovo.

Скорей всего, эта флешка была передана другому сотруднику компании вместе со скопированными на неё файлами.



4.5.11 Мониторинг ключевых слов

- *Поиск с использованием предустановленного словаря*
- *Создание словаря для поиска вручную*
- *Вес строки*

При внедрении системы защиты данных логичным образом возникает вопрос поиска ключевых слов или терминов, которые необходимо контролировать во всех возможных каналах передачи данных.

В iBatyr Monitor для этой задачи используется **Поиск по словарю**.

Примечание: Начиная с версии iBatyr Monitor 5.3 для работы политик поиска по словарю используется модуль **Hyperscan**. Для работы модуля процессор должен поддерживать расширение **SSSE3** (не SSE3).

Чтобы активировать модуль **Hyperscan**, выполните:

```
ibatyr hyperscan enable
```

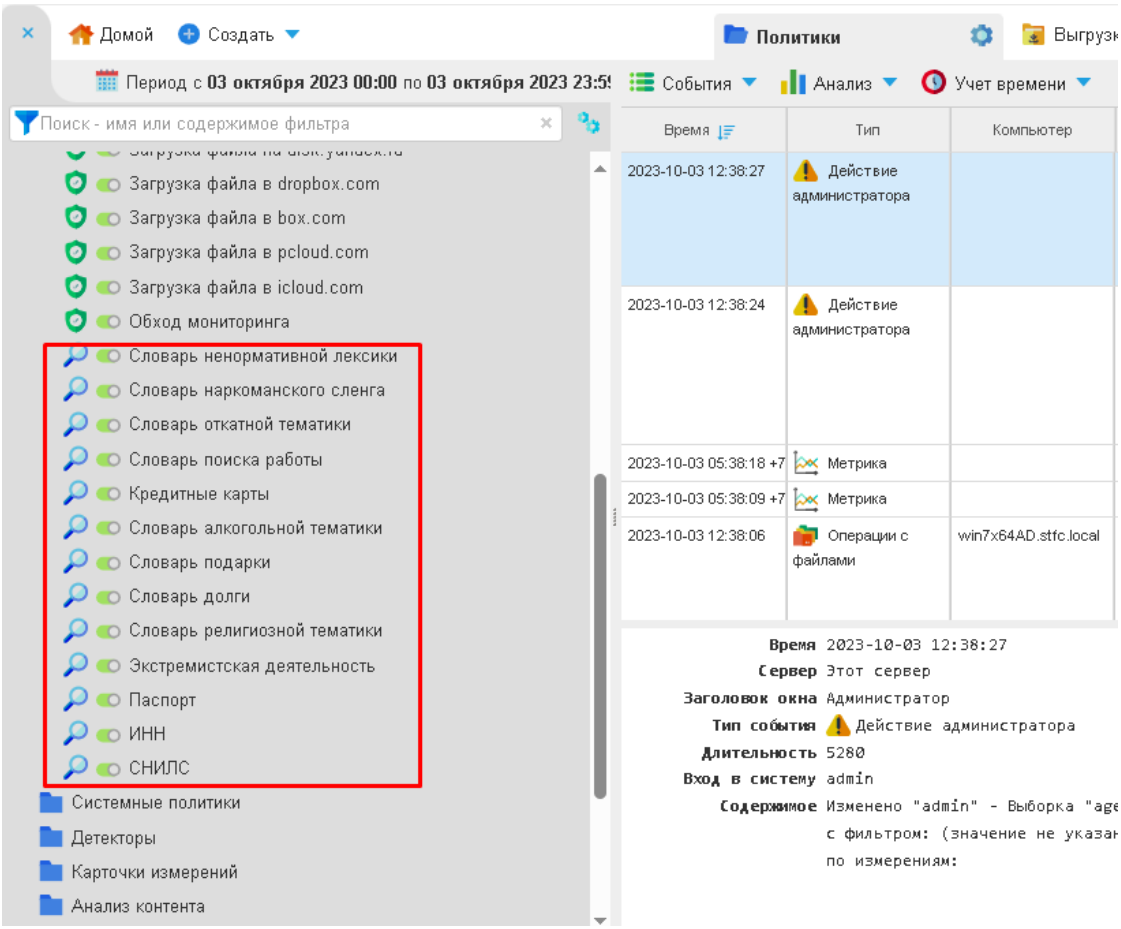
Поиск с использованием предустановленного словаря

В iBatyr Monitor доступен ряд предустановленных словарей по различным тематикам:

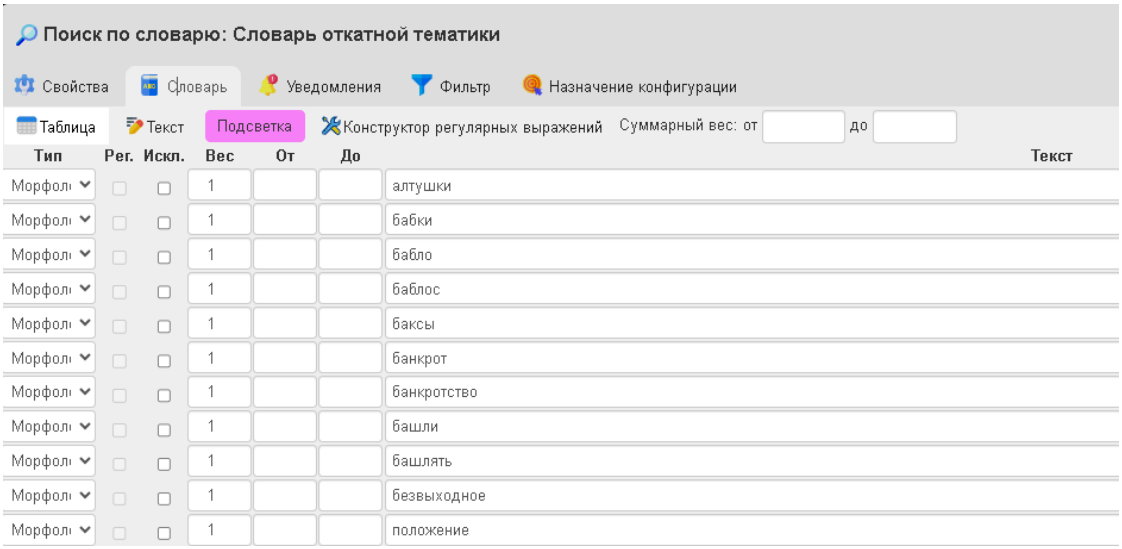
- словарь ненормативной лексики;
- словарь наркоманского сленга;
- словарь откатной тематики;
- словарь поиска работы;
- кредитные карты
- словарь алкогольной тематики;
- словарь подарки;
- словарь долги;
- словарь религиозной тематики;
- словарь экстремистской деятельности;
- паспорт;
- ИНН;
- СНИЛС.

Чтобы активировать предустановленную политику поиска по одному из словарей:

1. В веб-интерфейсе перейдите на вкладку **Политики**.
2. Перейдите в папку **Политики — Политики безопасности**.
3. Выберите одну из предустановленных политик поиска по словарю.



4. Настройте её свойства и задайте пороги срабатывания для различных слов.



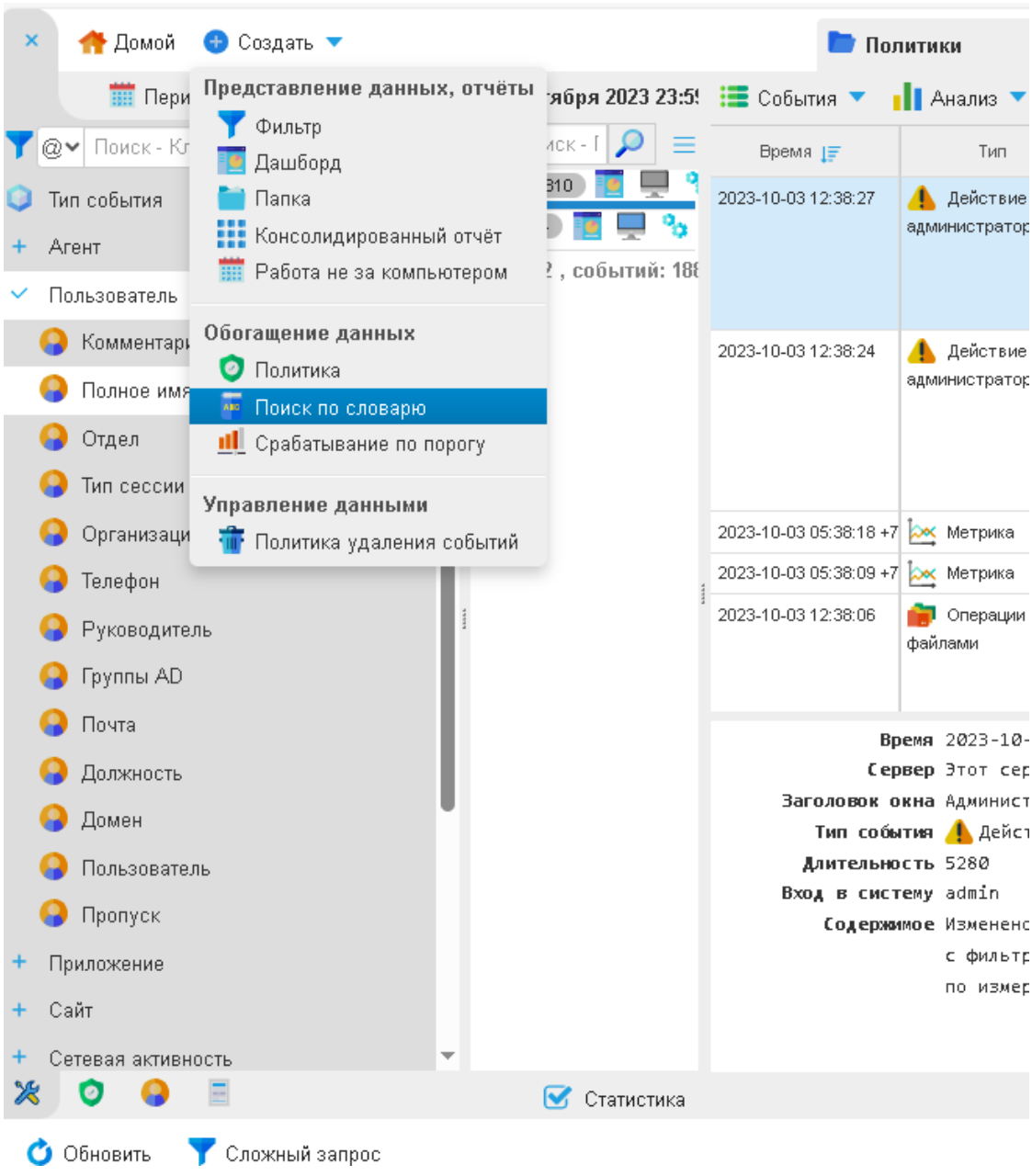
5. На вкладке **Свойства** включите опцию **Политика активна**.
6. **Сохраните** изменения.

Готово! Политика поиска по словарю создана и активна. Теперь все события, касающиеся срабатывания данной политики, будут отображаться в линзе событий.

Создание словаря для поиска вручную

Чтобы создать собственную политику поиска по словарю:

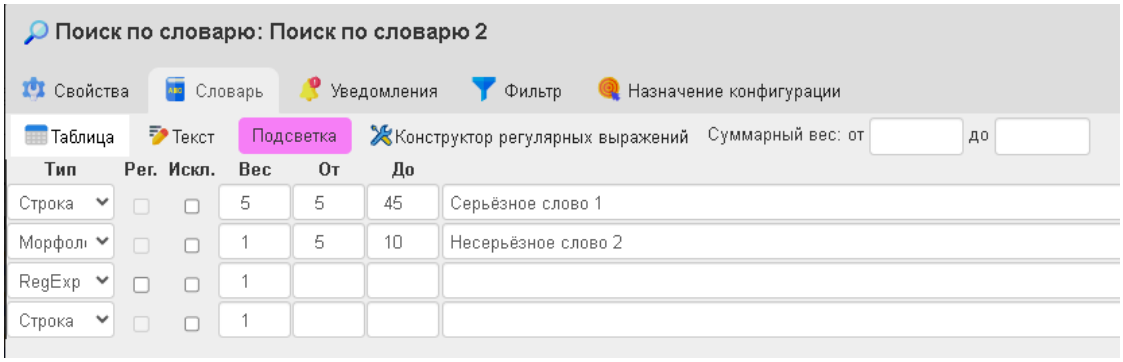
1. В веб-интерфейсе нажмите кнопку **Создать**.
2. Выберите пункт **Поиск по словарю**



3. В открывшемся окне настройки политики на вкладке **Свойства** включите опцию **Политика активна**.
4. На вкладке **Словарь** задайте список слов, которые хотите включить в свою политику поиска.
5. Задайте *вес строки* и его пороговые значения.
6. Выберите тип задаваемого выражения (**Строка**, **Поиск по морфологии**, **Регулярное выра-**

жение).

7. Укажите, будет ли строка регистрочувствительной или исключением.



8. Завершите настройку политики и сохраните её.

Готово! Политика поиска по пользовательскому словарю создана и активна. Теперь все события, касающиеся срабатывания данной политики, будут отображаться в линзе событий.

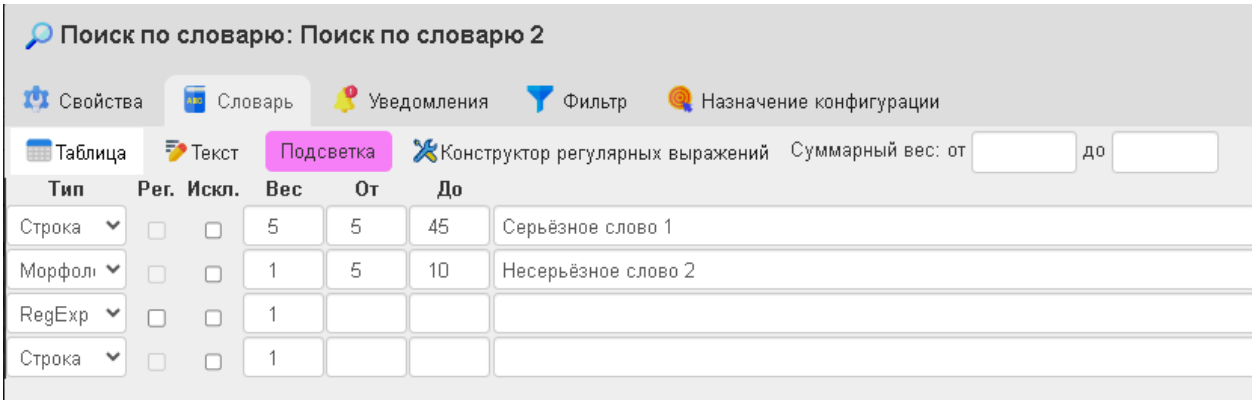
Вес строки

Начиная с версии 5.3, в iBatyr Monitor при создании политики **Поиск по словарю**, появилась возможность настраивать чувствительность политики.

Возможность срабатывания политики не на первое упоминание слова в событиях, а по достижении определённой «критической массы» реализована при помощи задания **веса** для каждой конкретной строки.

Примечание: Чтобы активировать возможность задавать вес строки, необходимо включить модуль **Hyperscan**.

При создании политики **Поиск по словарю** на вкладке **Словарь** можно настроить срабатывание политики на каждое конкретное слово или регулярное выражение.



Доступные для заполнения поля:

Поле	Описание
Тип	Позволяет выбрать один из трёх типов значений в строке: • строка — слово или строка для поиска; • морфология — строка для поиска по морфологии; • RegExp — регулярное выражение.
Рег.	Опция, включающая контроль регистра.
Искл.	Опция, позволяющая задавать исключения из поиска по словарю.
Вес	Значение веса указанной строки.
От и **До**	Пороговые значения веса для срабатывания политики.
Текст	Значение строки для поиска по словарю.

4.5.12 Регулярные выражения

Регулярные выражения - сильный инструмент для поиска строк, проверки их на соответствие какому-либо шаблону и другой подобной работы.

Особенности создания регулярных выражений:

- учитывается регистр символов в строке;
- необходимо экранировать спецсимволы **. ^ $ * + ? { } [ ]** \ | **( )** указанием перед ними обратного слэша \;

При создании политики **Поиск по словарю** можно воспользоваться **Конструктором регулярных выражений**, чтобы создать и проверить своё регулярное выражение.

Примечание: Обратите внимание, что спецсимвол границы слова **b** по-разному отрабатывает в PostgreSQL и ClickHouse:

- в PostgreSQL **b** заменятся на **y**, который срабатывает на начало и конец слова;
- в PostgreSQL **b** также работает после спецсимвола и с юникодом;
- в ClickHouse юникод не поддерживается, начало слова считается только после пробела, табуляции или начала строки.

Больше спецсимволов для регулярных выражений представлено на сайте для создания выражений https://regex101.com/

Примеры регулярных выражений

Поиск в тексте e-mail или логина AD

```
(\s|^|\n|\b)(\w|\.?|\-?)+@([A-zA-я0-9][-A-zA-я0-9]+\.)+[A-zA-я]{2,13}((\s|$|\n|\b))
```

Номерные знаки машин, расширенные и короткие

```
(A|B|E|K|M|H|O|P|C|T|У|X)(\s|\-)?\d{3}(A|B|E|K|M|H|O|P|C|T|У|X){2}(\s|\-)?\d{2,3}
(A|B|E|K|M|H|O|P|C|T|Y|X)(\s|\-)?\d{3}(A|B|E|K|M|H|O|P|C|T|Y|X){2}(\s|\-)?\d{2,3}
(A|B|E|K|M|H|O|P|C|T|Y|X){3}(\s|\-)?\d{3}(\s|\-)?\d{2,3} (\s|\n|\b|^\d)
```

Полис ОСАГО

```
(^|.*)(PPP|HHH|XXX|TTT|AAC|AAB|AAK|AAM)(-|\s)\d{10}\s
```

IP адрес

```
([0-9]{1,3}[\.]){3}[0-9]{1,3}
```

Найти **слово** в любом регистре

```
слово
```

Номер мобильного телефона

```
(8|\+7)?(\-|\s)?((9\d{9})|(\(?9\d{2}\)?)(((\-|\s)\d{2,4}){2,3}|(\s|-)\d{7}))
```

Номер стационарного телефона в формате 8-(код города)-номер_телефона (8-(123)-456-78-90)

```
(8|\+7)?(\-|\s)?((383\d{7})|(\(?383\)?)(((\-|\s)\d{2,4}){2,3}|(\s|-)\d{7})) - код 383
(8|\+7)?(\-|\s)?((495\d{7})|(\(?495\)?)(((\-|\s)\d{2,4}){2,3}|(\s|-)\d{7})) - код 495
(8|\+7)?(\-|\s)?((499\d{7})|(\(?499\)?)(((\-|\s)\d{2,4}){2,3}|(\s|-)\d{7})) - код 499
(8|\+7)?(\-|\s)?((812\d{7})|(\(?812\)?)(((\-|\s)\d{2,4}){2,3}|(\s|-)\d{7})) - код 812
```

4.5.13 Операции с файлами: Удаление/Перемещение/Переименование

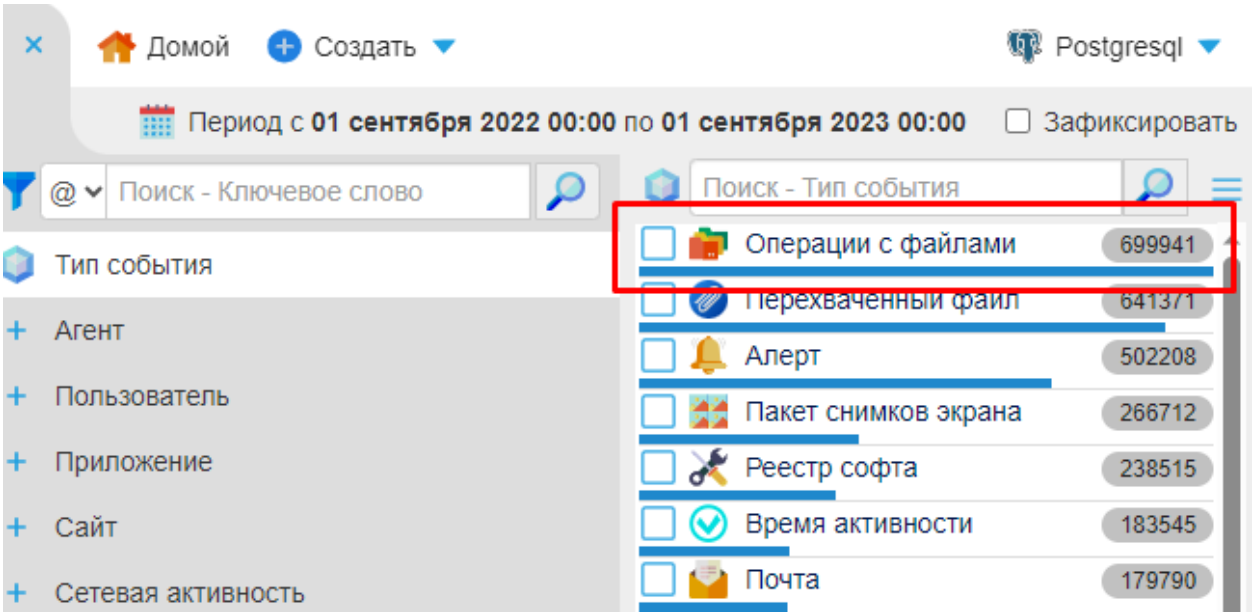
Агентская часть iBatyr Monitor обладает полным функционалом по отслеживанию и перехвату любых файловых операций, происходящих на рабочей станции пользователя или на терминальном сервере.

Решение о перехвате файлов принимается на основе правил, заданных в конфигурации агента.

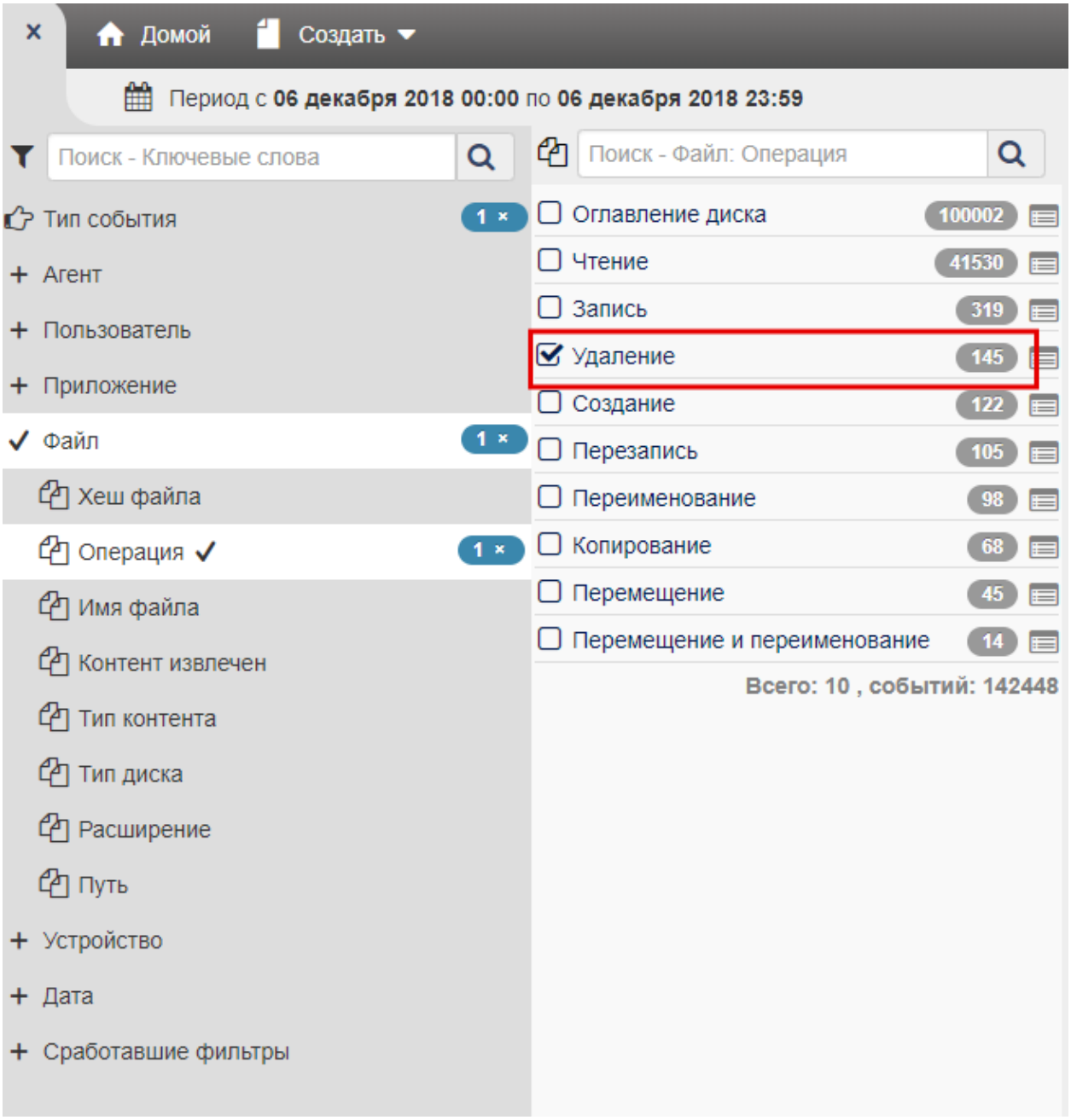
Конфигурация агента может быть общей или распространяемой только на определённые группы агентов\отдельные рабочие станции пользователей.

Наиболее частыми файловыми операциями, на которые нужно обращать внимание офицеру безопасности, это операции Удаления/Перемещения/Переименования файлов.

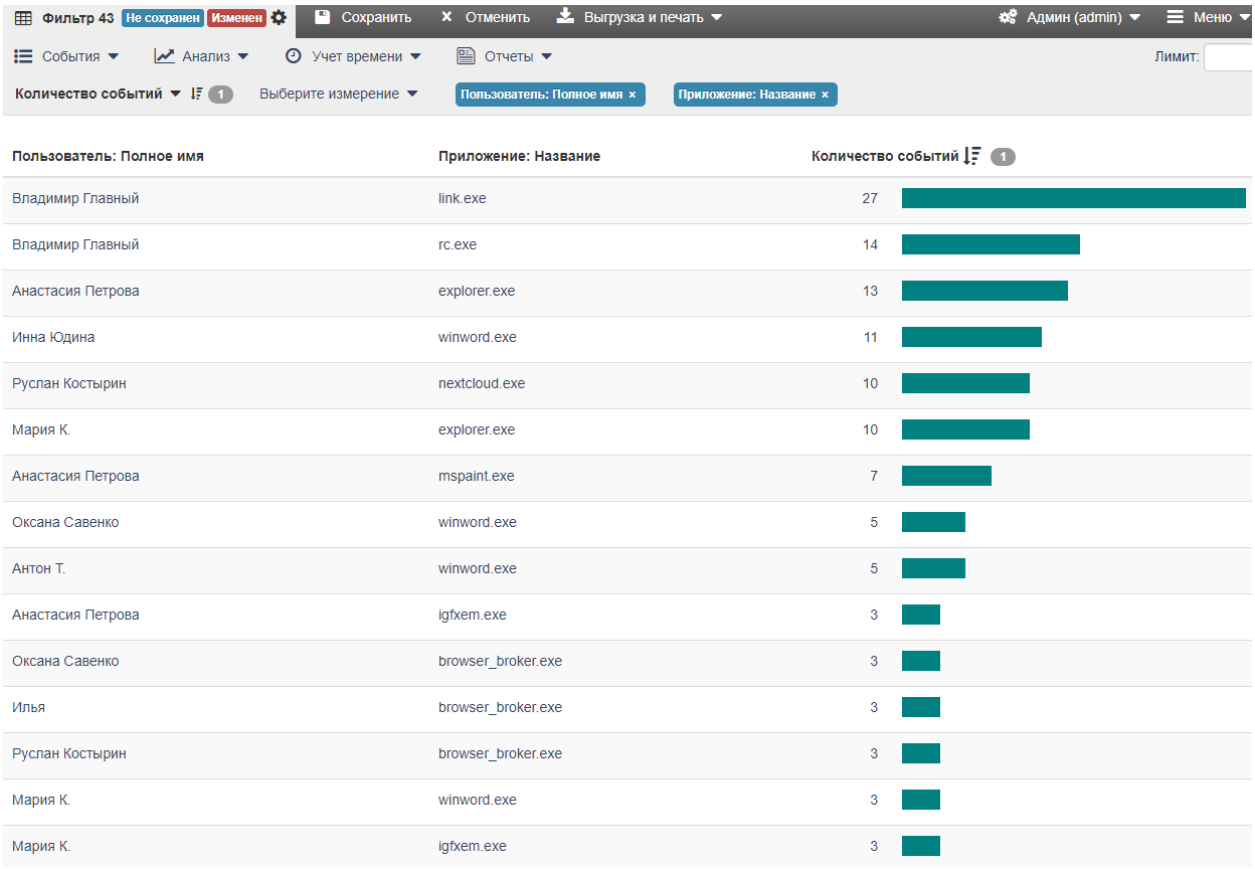
Все эти события можно отследить, нажав в меню администрирования в дереве событий «Операции с файлами».



Чтобы детализировать отчётность только по интересующим событиям, к примеру «Удаления», необходимо выбрать данную операцию. В результате этого получаем список всех операций с файлами, которые были удалены.



Существует возможность детализации информации при выборе «Анализ» в меню отображения. При этом необходимо в фильтре измерения добавить «Имя пользователя» и выбрать «Имя приложения».

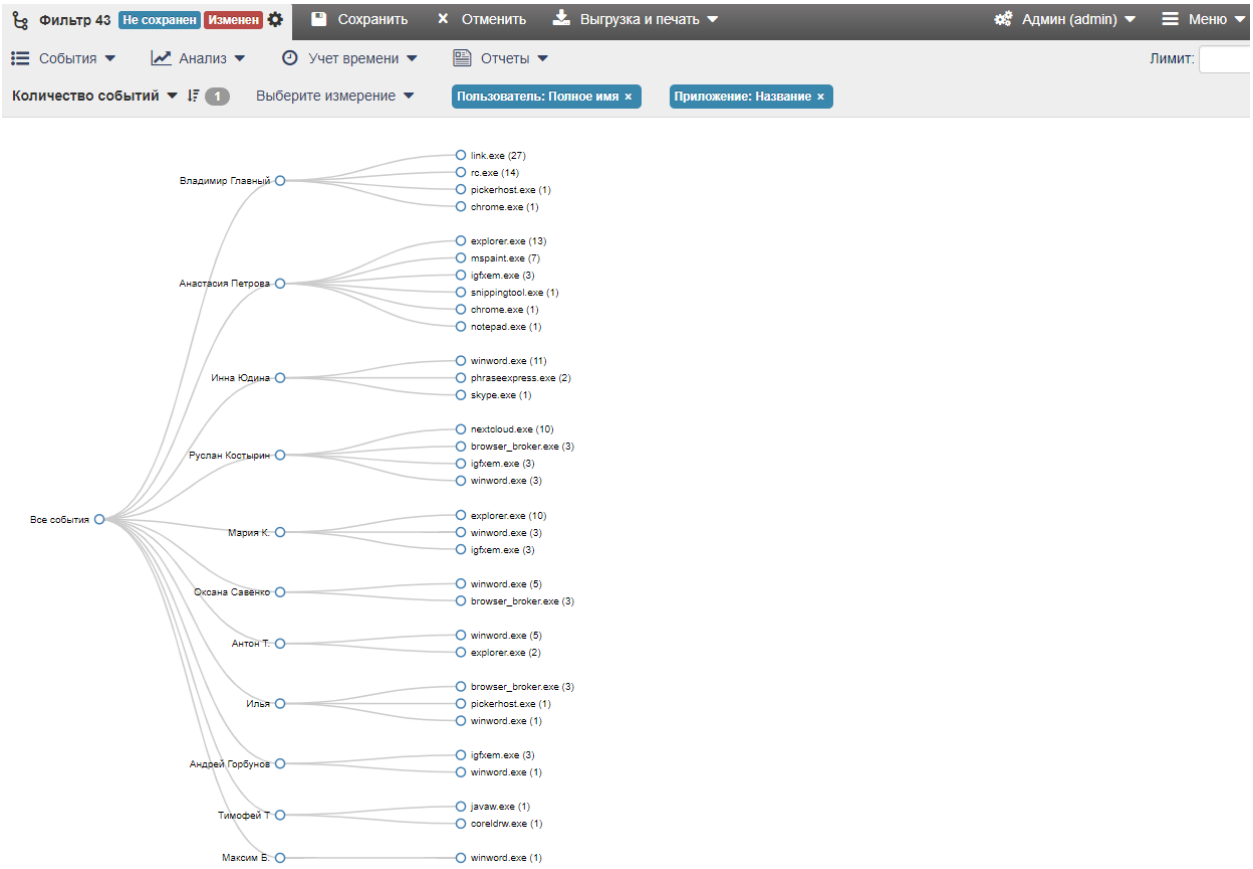


Пользователь: Полное имя	Приложение: Название	Количество событий 1
Владимир Главный	link.exe	27
Владимир Главный	rc.exe	14
Анастасия Петрова	explorer.exe	13
Инна Юдина	winword.exe	11
Руслан Костырин	nextcloud.exe	10
Мария К.	explorer.exe	10
Анастасия Петрова	mspaint.exe	7
Оксана Савенко	winword.exe	5
Антон Т.	winword.exe	5
Анастасия Петрова	igfxem.exe	3
Оксана Савенко	browser_broker.exe	3
Илья	browser_broker.exe	3
Руслан Костырин	browser_broker.exe	3
Мария К.	winword.exe	3
Мария К.	igfxem.exe	3

В нижней части окна можно представить эту информацию в графическом виде. Например, выбрать построение дерева по начальным фильтрам:

- файловые операции
- файловая операция удаления
- ветка дерева «Имя пользователя»
- подветка «Имя приложения»

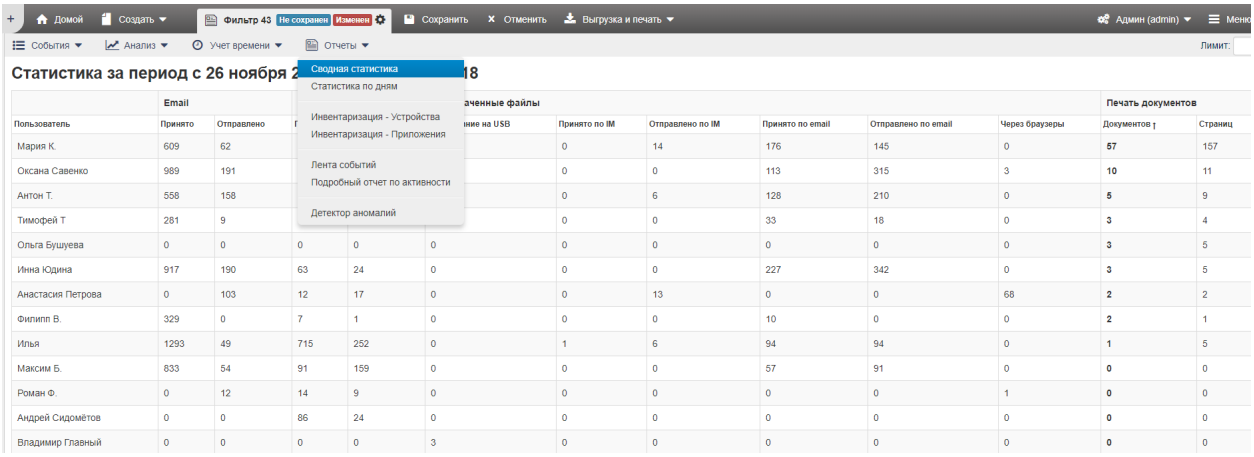
Вид отображения «Дерево» легко анализировать визуально, а также распечатать в формате PDF (нажав «Печать» в верхней части меню администрирования).



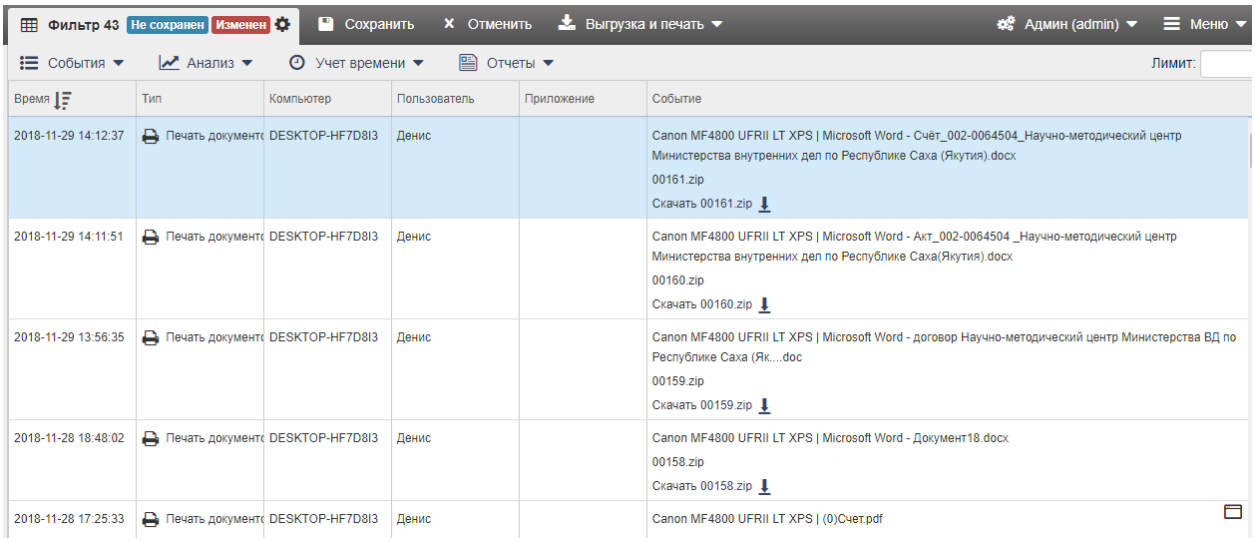
Затем нажать «Выгрузка и печать», получив всю ленту событий для выгрузки и анализа - позволит распечатать полученную информацию (например, в PDF) для детального анализа.

4.5.14 Печать документов

Для анализа документов в компании, выведенных на печать, существует специальный отчёт, располагающийся в меню консоли администратора - «Отчёты/Сводная статистика».

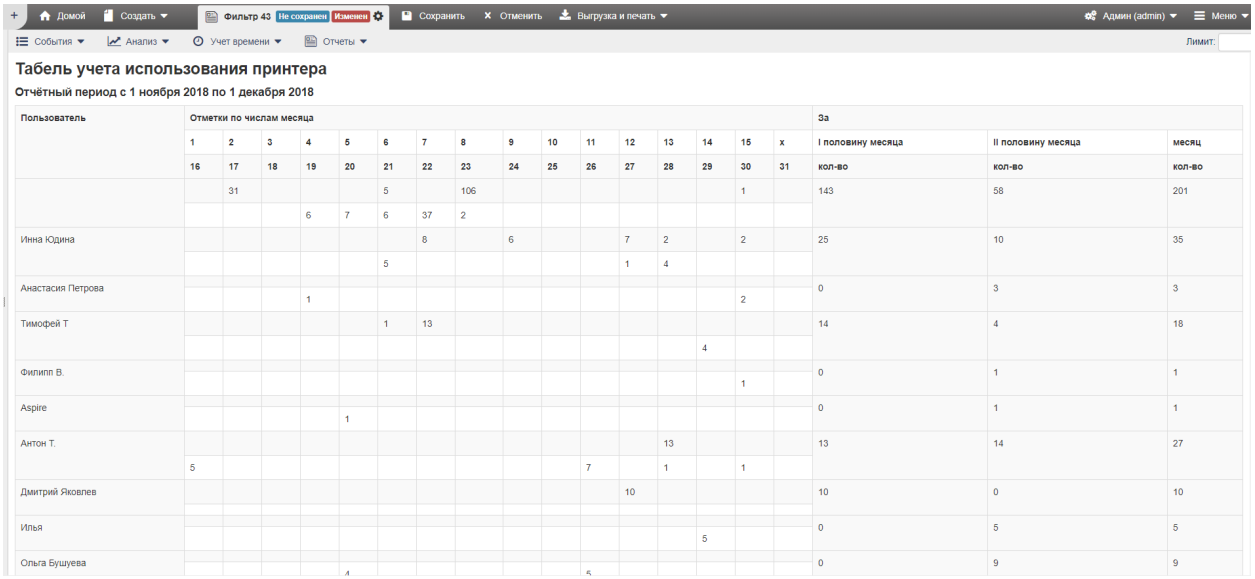


Из этого отчёта следует, что существует «самый печатающий» сотрудник компании. Возможна детализация по названию документов, их объему и количеству. Для этого необходимо выделить в фильтре интересующие документы:



Выделенный файл можно скачать, нажав на иконку скачивания файла.

Если этой информации недостаточно или нужен табель распечатанных документов за длительный период времени, существует дополнительный отчёт: «Табель использования принтера», который расположен в меню отчетов «Учет времени - Табель - Табель использования принтера».



4.5.15 Построение аналитической таблицы - «Список USB-устройств»

При блокировке USB-устройств часто требуется получить список **ID устройств**.

Такой список легко получить в аналитической таблице.

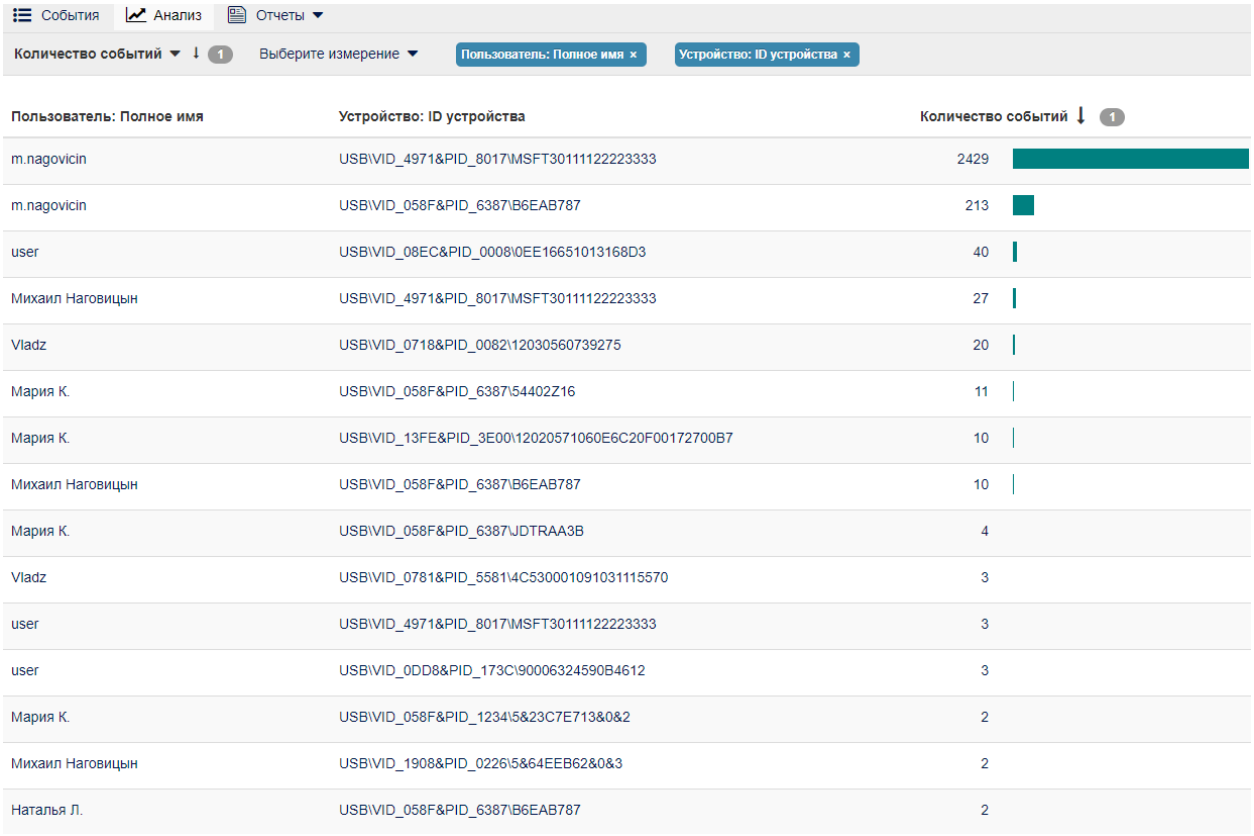
Для вывода списка всех используемых USB-устройств выполните следующие шаги:

- В меню Конструктора выбрать **Анализ - Таблица**
- В параметре «Выберите измерение» выставить значение **Устройство - ID устройства**
- В **Конструкторе** нужно выбрать **Файл - Тип диск - Removable** (можно также выбрать **USB**)

В итоге получим список USB устройств.

Чтобы выгрузить полученный список в файл, нужно нажать на верхней панели на кнопку - **Выгрузка и печать - Выгрузка в Excel**.

В выгруженном в Excel формате можно скопировать столбец **ID устройства** и применить их в конфигурации агента при создании белого списка USB-устройств *USB-контроль*.



Пользователь: Полное имя	Устройство: ID устройства	Количество событий ↓ 1
m.nagovicin	USB\VID_4971&PID_8017\MSFT30111122223333	2429
m.nagovicin	USB\VID_058F&PID_6387\B6EAB787	213
user	USB\VID_08EC&PID_0008\0EE16651013168D3	40
Михаил Наговицын	USB\VID_4971&PID_8017\MSFT30111122223333	27
Vladz	USB\VID_0718&PID_0082\12030560739275	20
Мария К.	USB\VID_058F&PID_6387\54402Z16	11
Мария К.	USB\VID_13FE&PID_3E00\12020571060E6C20F00172700B7	10
Михаил Наговицын	USB\VID_058F&PID_6387\B6EAB787	10
Мария К.	USB\VID_058F&PID_6387\JDTRAA3B	4
Vladz	USB\VID_0781&PID_5581\4C530001091031115570	3
user	USB\VID_4971&PID_8017\MSFT30111122223333	3
user	USB\VID_0DD8&PID_173C\90006324590B4612	3
Мария К.	USB\VID_058F&PID_1234\5&23C7E713&0&2	2
Михаил Наговицын	USB\VID_1908&PID_0226\5&64EEB62&0&3	2
Наталья Л.	USB\VID_058F&PID_6387\B6EAB787	2

4.5.16 Почтовый канал общения

iBatyr Monitor поддерживает полноценный перехват почтовых протоколов **POP3**, **IMAP**, **SMTP**, **MAPI** и их шифрованных аналогов.

Чтобы включить перехват почты и вложений:

1. В разделе **Панель управления ** → **Конфигурации компьютеров** откройте интересующую конфигурацию или создайте новую.
2. В настройках конфигурации в разделе **Сетевые подключения** активируйте опцию **Мониторинг сети**.
3. В разделе **Файлы** активируйте **Файловая активность**, **Теневое копирование** и задайте *максимальный размер файла для теневого копирования*.
4. В разделе **Почта и мессенджеры** активируйте опции **Веб-почта**, **Электронная почта** и **Электронная почта MAPI**.

iBatyr Monitor поддерживает перехват почтовых приложений (Outlook, The bat, Thunderbird...) и веб-сервисов (mail.ru, yandex.ru, google.com...).

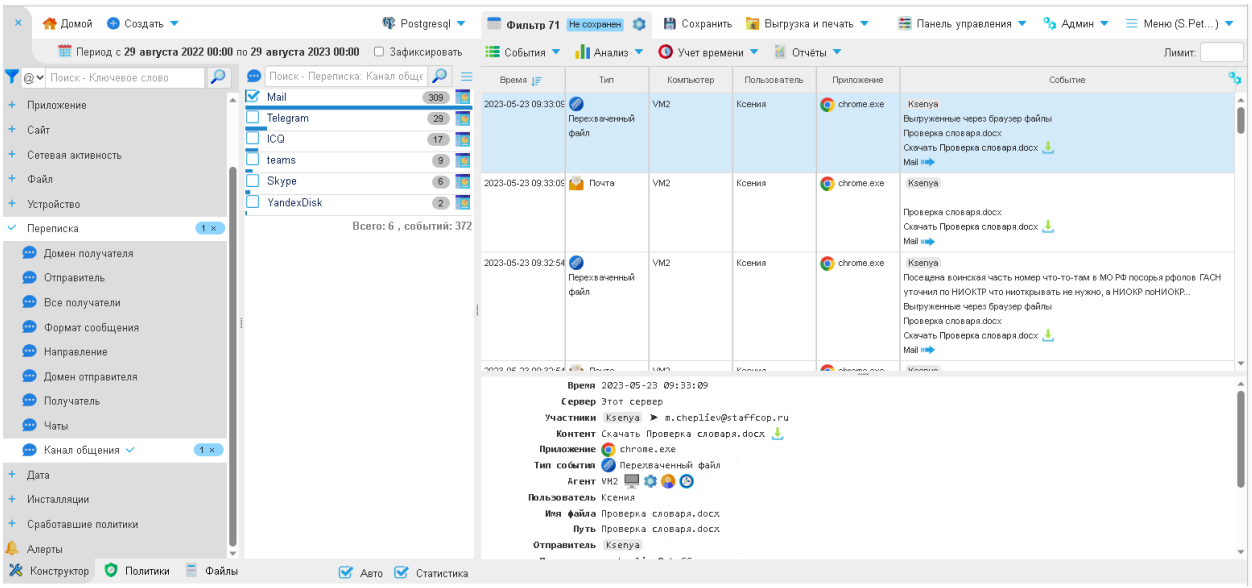
Как работает

Основные особенности перехвата почты:

- перехват писем и вложений осуществляется в фоновом режиме - незаметно для пользователя;
- при распознавании слов в перехваченных документах, они автоматически индексируются и заносятся в специальную таблицу на сервере;
- обработка распознанных документов по заданным словарям происходит в режиме реального времени - результат обработки сообщений и распознанных файлов можно увидеть сразу же в результатах работы соответствующих фильтров.

Как посмотреть перехваченную почту

1. В веб-интерфейсе в разделе **Конструктор** выберите **Пользователя**, для которого хотите просмотреть переписку.
2. Выберите опцию **Переписка**.
3. В открывшемся меню выберите параметры, по которым хотите отфильтровать события для выбранного пользователя.
4. Выбранные события будут показаны в Линзе событий.

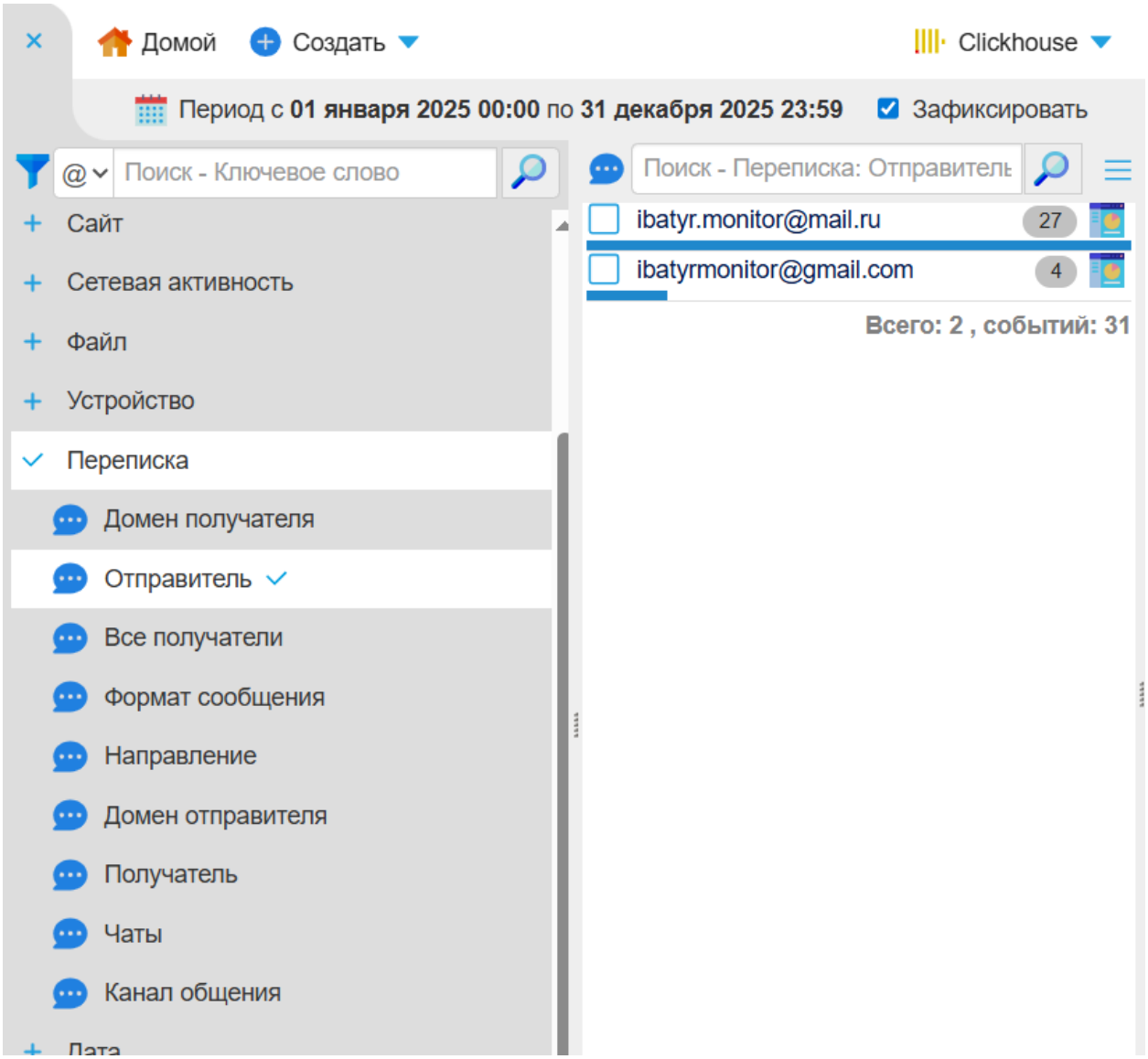


При анализе действий пользователя может выясниться, что этот пользователь использовал личную почту для пересылки служебных документов, что может быть интересно с точки зрения нарушения политики безопасности сети.

Чтобы посмотреть все почтовые ящики, которые использует один пользователь:

1. В веб-интерфейсе в разделе **Конструктор** выберите пользователя, для которого хотите просмотреть переписку.
2. Выберите опцию **Переписка**.
3. В измерении **Канал общения** выберите **Mail**.
4. **Направление** → **Исходящие**.

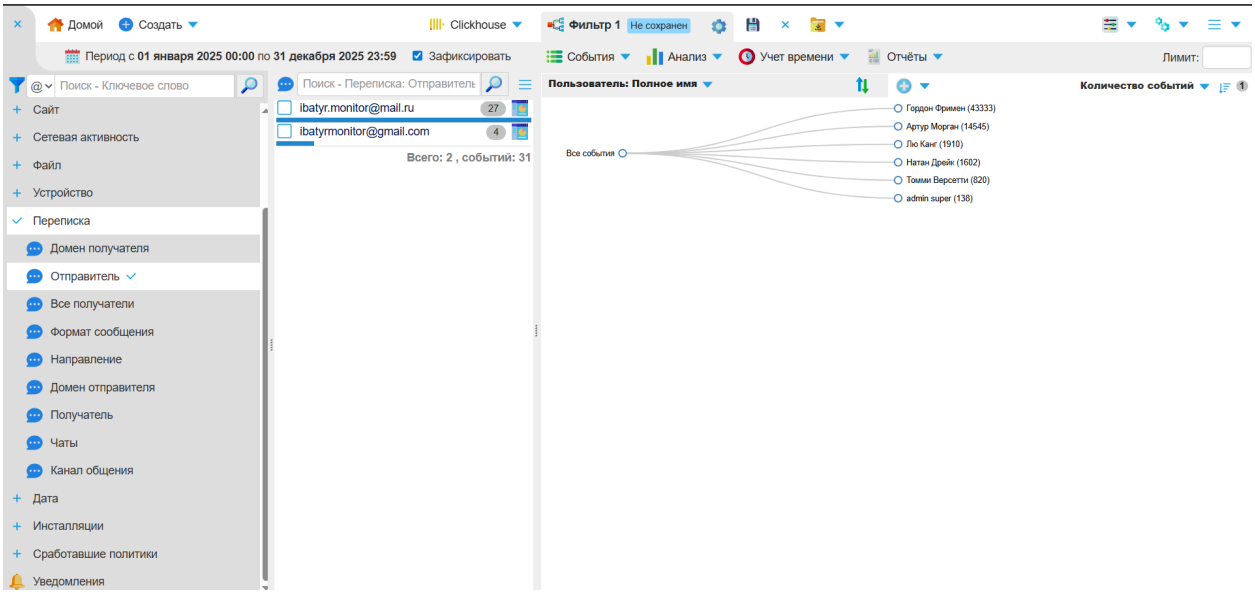
В этом измерении будут представлены почтовые ящики, привязанные к выбранному пользователю.



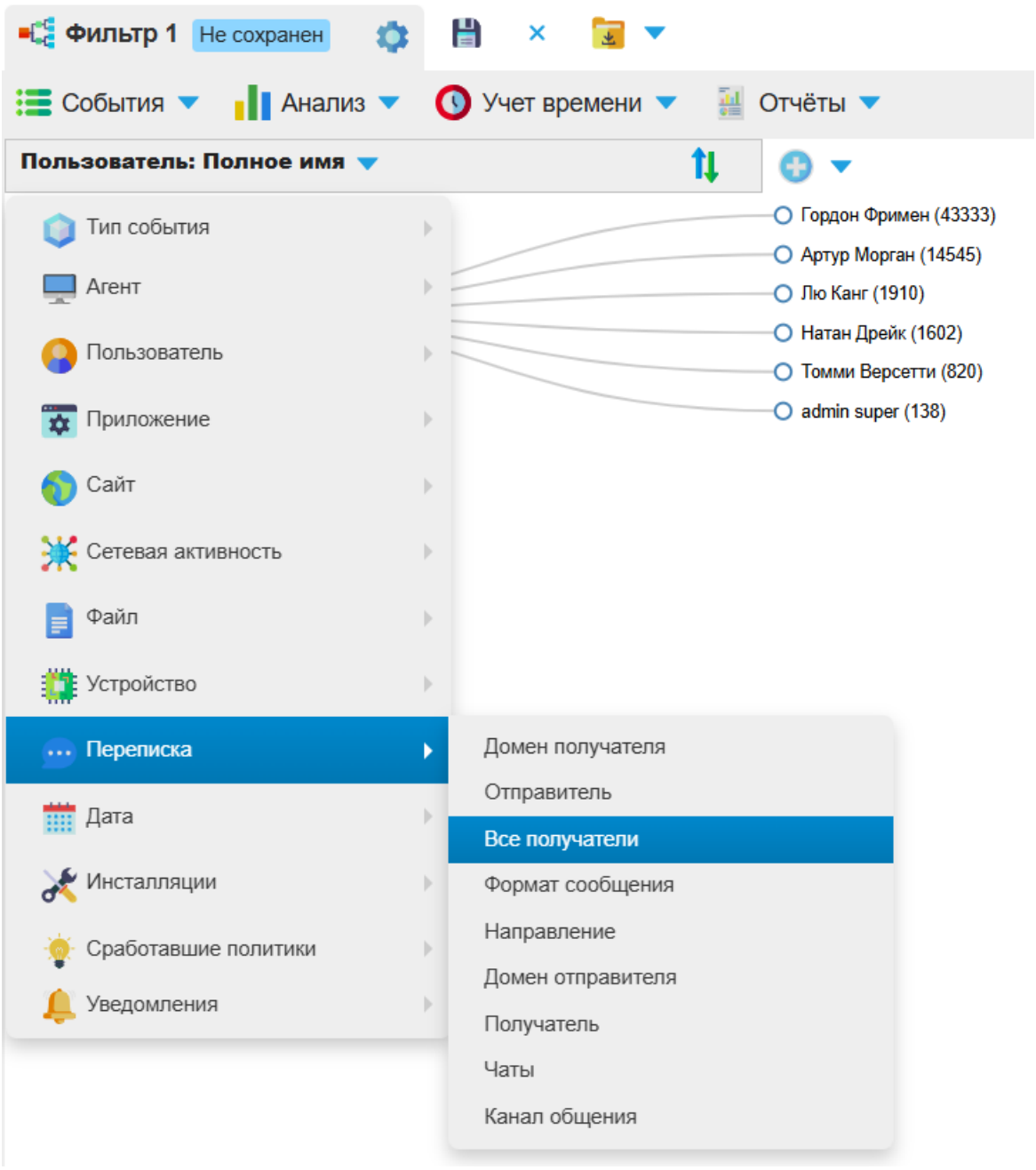
Чтобы посмотреть, пользуется ли кто-то из сотрудников не только корпоративной, но и личной почтой:

1. В веб-интерфейсе в разделе **Конструктор** выберите опцию **Переписка**.
2. В измерении **Канал общения** выберите **Mail**.
3. **Направление** → **Исходящие**.
4. В Линзе событий выберите **Анализ** → **Дерево**.
5. В открывшемся окне добавьте измерение **Переписка** → **Отправитель**.

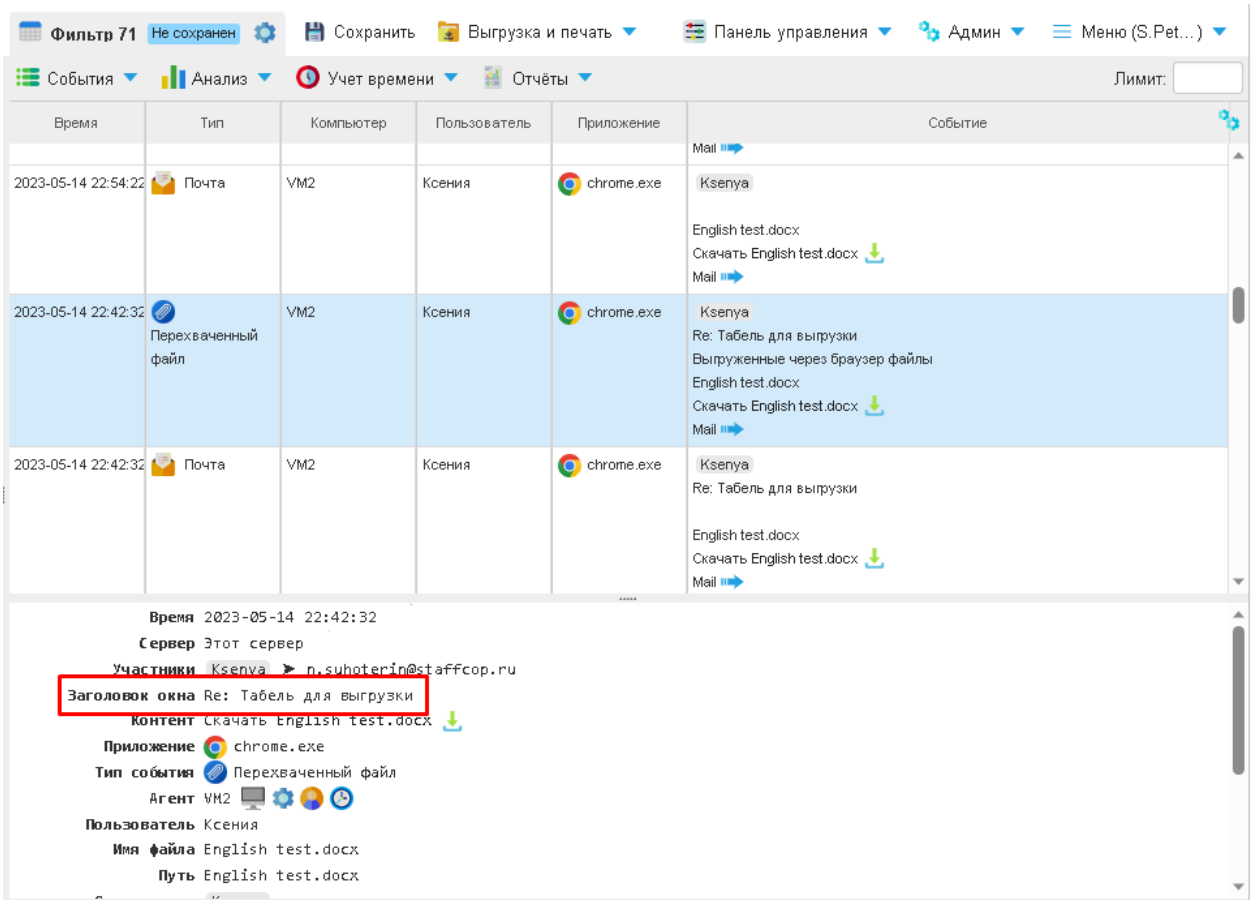
В построенном дереве можно будет увидеть пользователей сети и привязанные к их именам почтовые ящики.



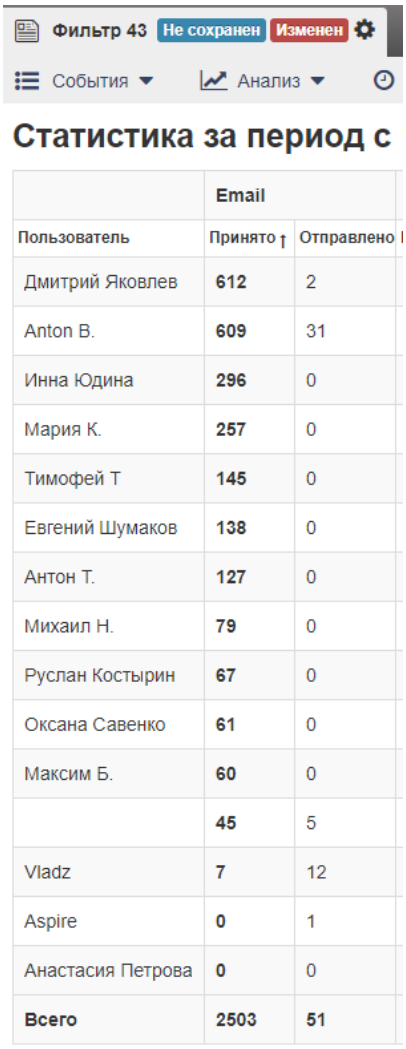
Если добавить измерение **Переписка-Все получатели**, можно будет отследить, с какой почты каким адресатам были отправлены письма.



Если в письме была указана тема, её можно прочитать в таблице событий в строке **Заголовок окна**.



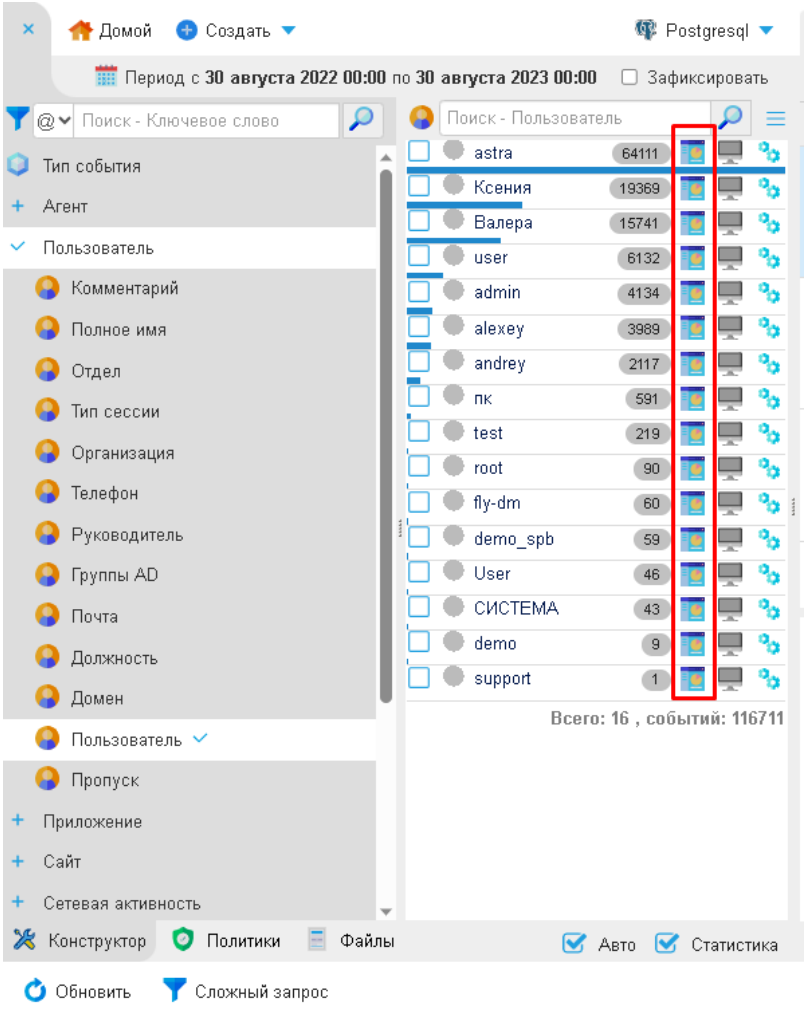
Количество принятых и отправленных писем за период можно посмотреть в разделе **Отчёты → Сводная статистика**.



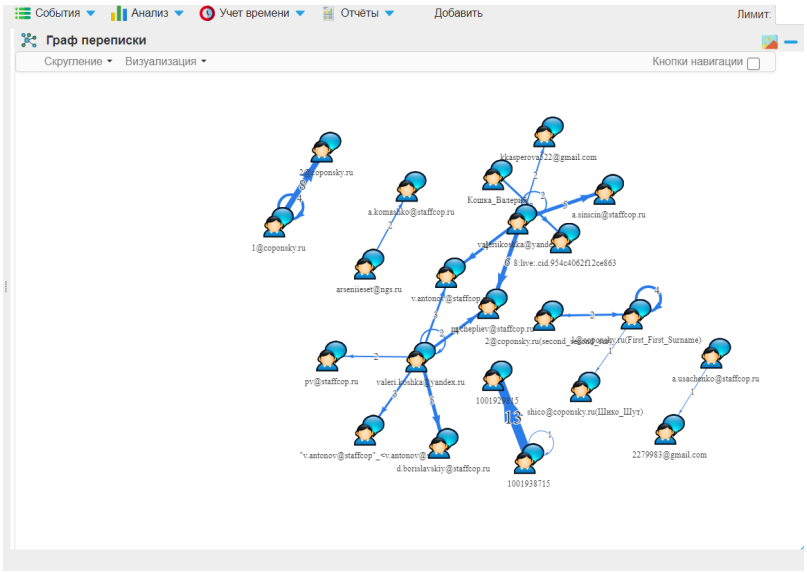
	Email	
Пользователь	Принято	Отправлено
Дмитрий Яковлев	**612**	2
Anton B.	**609**	31
Инна Юдина	**296**	0
Мария К.	**257**	0
Тимофей Т	**145**	0
Евгений Шумаков	**138**	0
Антон Т.	**127**	0
Михаил Н.	**79**	0
Руслан Костырин	**67**	0
Оксана Савенко	**61**	0
Максим Б.	**60**	0
	45	5
Vladz	**7**	12
Aspire	**0**	1
Анастасия Петрова	**0**	0
Всего	**2503**	**51**

Карточка пользователя

В веб-интерфейсе при выборе измерения **Пользователь** в списке доступных пользователей есть возможность открыть предварительно настроенный дашборд **Карточка пользователя**.



По умолчанию, в **Карточке пользователя** можно посмотреть не только список контактов выбранного пользователя, но и граф его переписки.



Настроить дашборд можно в разделе **Конструктор** → **Политики** → **Карточки измерений** →

Карточка пользователя.

4.5.17 Как отследить перемещения файла в сети

Представьте, что вам нужно отследить путь файла в корпоративной сети.

В iBatyr Monitor для этого предусмотрен специальный инструмент — **граф взаимосвязи событий**. Это визуальная схема, которая наглядно показывает весь путь файла: от создания до последней точки назначения.

Как построить граф

1. Выбираем файл.
2. Уточняем даты, отправителей, получателей и другие измерения.
3. Строим граф перемещений.

Пример: перемещения файла Миграция.docx

Допустим, кто-то получил доступ к чувствительному файлу *Миграция.docx*. Мы хотим выяснить, как это произошло.

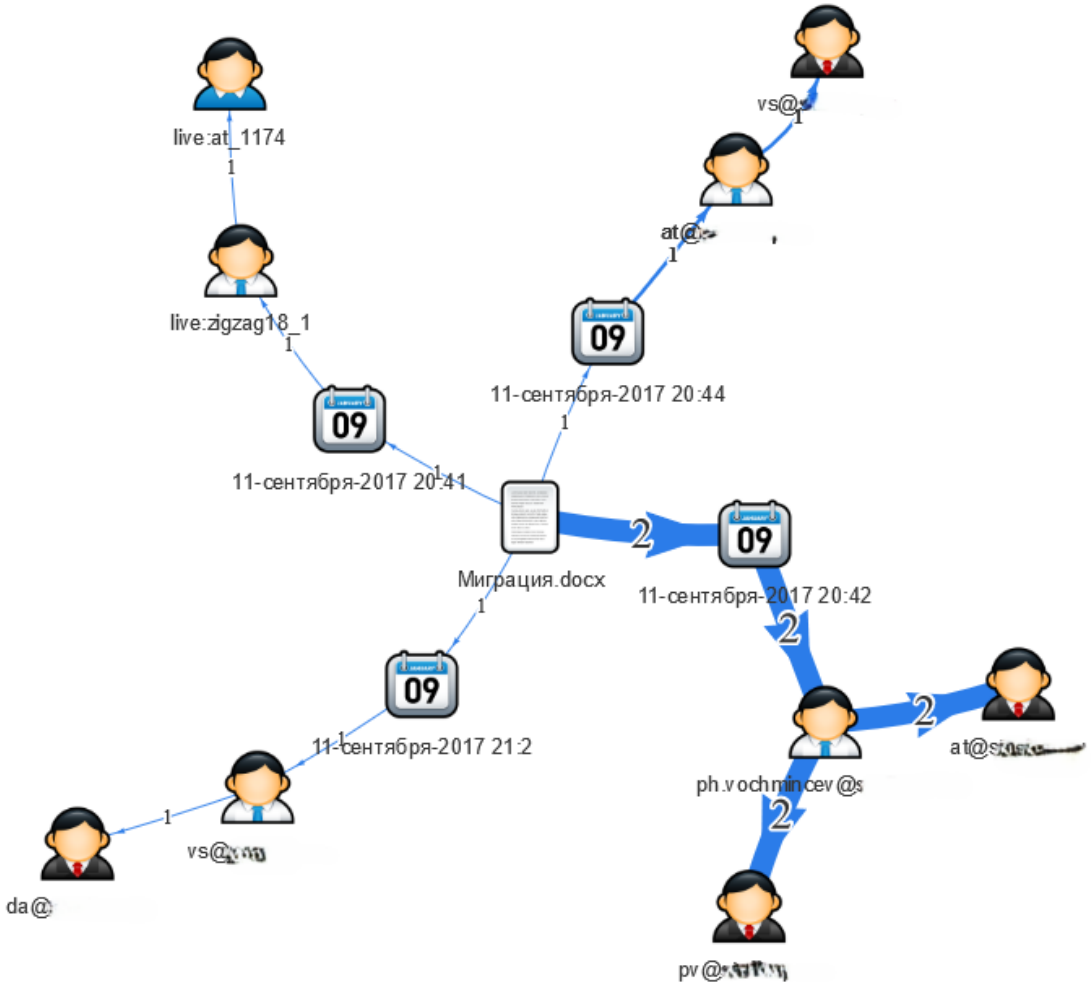
Сначала мы находим файл в **Конструкторе** через измерение **Файл** → **Имя файла**.

При выборе файла в **Линзе** отразятся связанные с файлом события. Например, файл связан с пятью событиями. Можно анализировать их по списку, но удобнее построить визуализировать путь на графе.

Чтобы построить граф:

1. В **Конструкторе** дополнительно к **Файл** → **Имя файла** выберите **Дата** → **Минуты**.
2. В измерении **Переписка** выберите **Отправители** и **Получатели**.
3. В верхнем меню выберите **Анализ** → **Граф**.

В результате получим примерно такой граф:



В центре графа расположен файл *Миграция.docx*. От него отходит время перемещения файла с отправителями и получателями:

- 20:41 — отправка через Skype от live:zigzag18_1 к live:at_1174;
- 20:42 — пересылка по почте от ph.vochmincev@ к at@ и pv@;
- 20:44 — at@ отправил письмо по почте с вложением файла *Миграция* получателю vs@;
- 21:20 — пересылка по почте от vs@ к da@.

Такой подход помогает увидеть последовательность действий, выявить нестандартные перемещения и установить источник доступа.

См.также:

Подробнее об анализе данных

4.5.18 Контроль USB-накопителей

USB-накопители в iBatyr Monitor можно полностью заблокировать, настроить для них частичный доступ (чёрный и белый списки) или открыть только для чтения. Для настройки доступа USB-накопителей необходим их ID.

ID USB-накопителя можно определить с помощью веб-консоли iBatyr Monitor или стандартными средствами операционной системы.

ID USB-накопителя в Windows-агентах

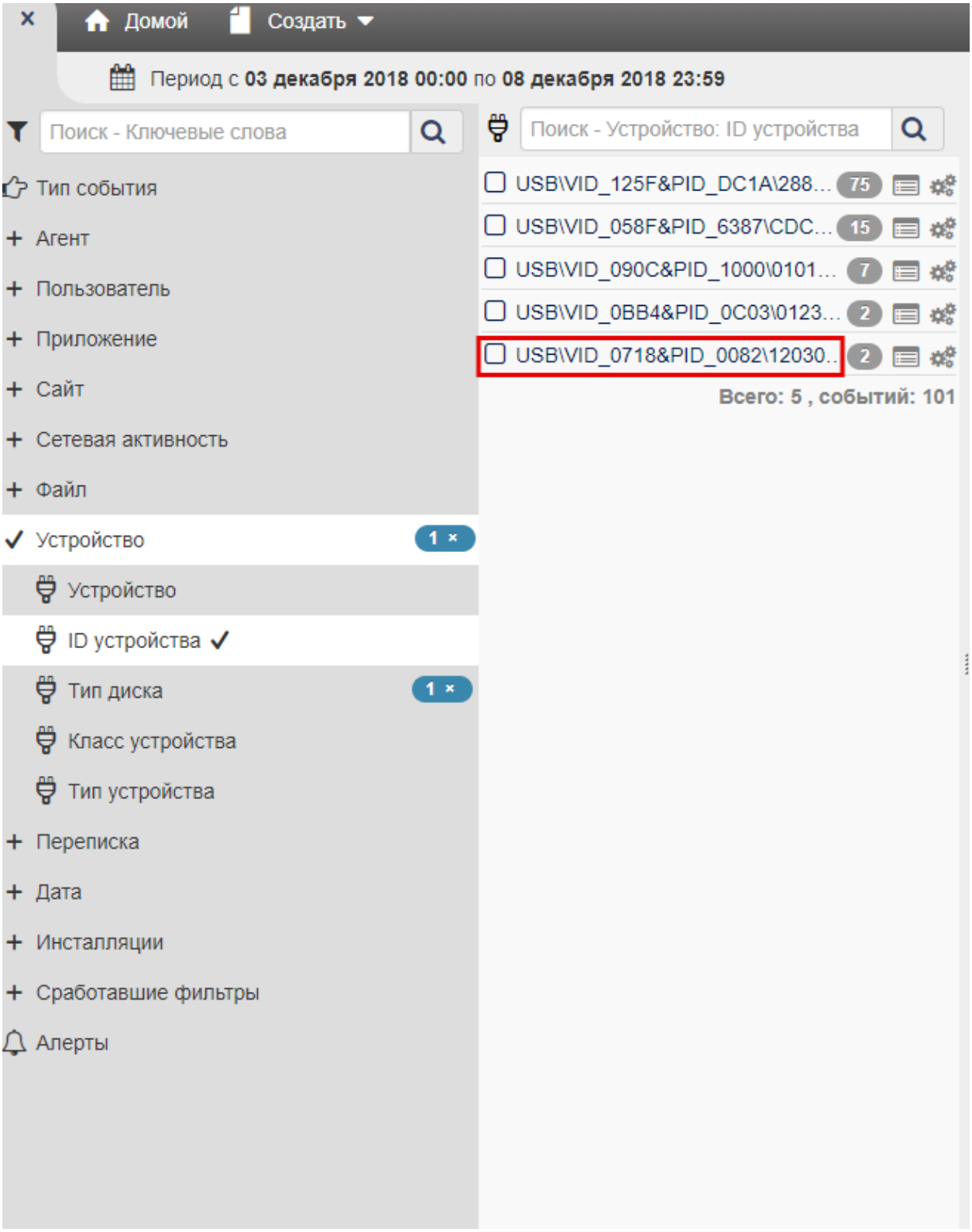
В списке ID USB-накопителей возможны ID, начинающиеся с **USB\...** или с **USBSTOR\...**.

Для блокировки USB-накопителей на Windows-агентах используйте ID, начинающийся на **USB\...**.

Определение ID средствами iBatyr Monitor

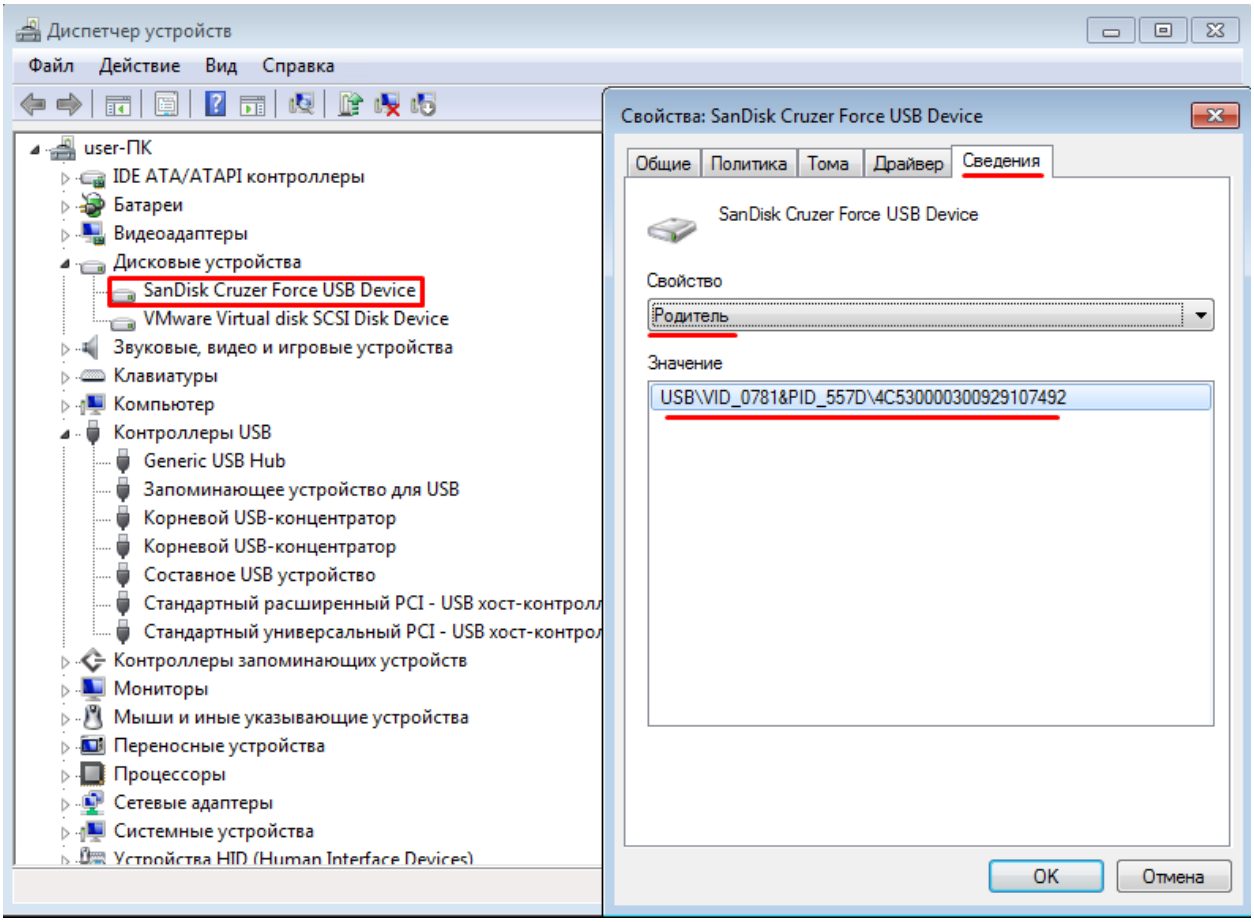
Чтобы получить ID подключенного USB-накопителя через веб-консоль iBatyr Monitor:

1. В Конструкторе выберите ПК, к которому подключен накопитель.
2. Выберите измерение **Устройства** → **Тип диска** → **Removable**.
3. В открывшемся окне в разделе **Устройства** выберите пункт **ID-устройства**.
4. В появившемся списке представлены устройства, подключенные к выбранному ПК. Найдите устройство, ID которого начинается с **USB\...**.


Домой
Создать
Период с 03 декабря 2018 00:00 по 08 декабря 2018 23:59
Поиск - Ключевые слова
Поиск - Устройство: ID устройства
Тип события
Агент
Пользователь
Приложение
Сайт
Сетевая активность
Файл
Устройство
1 ×
Устройство
ID устройства
Тип диска
1 ×
Класс устройства
Тип устройства
Переписка
Дата
Инсталляции
Сработавшие фильтры
Алерты
USB\VID_125F&PID_DC1A\288... 75
USB\VID_058F&PID_6387\CDC... 15
USB\VID_090C&PID_1000\0101... 7
USB\VID_0BB4&PID_0C03\0123... 2
USB\VID_0718&PID_0082\12030... 2
Всего: 5 , событий: 101

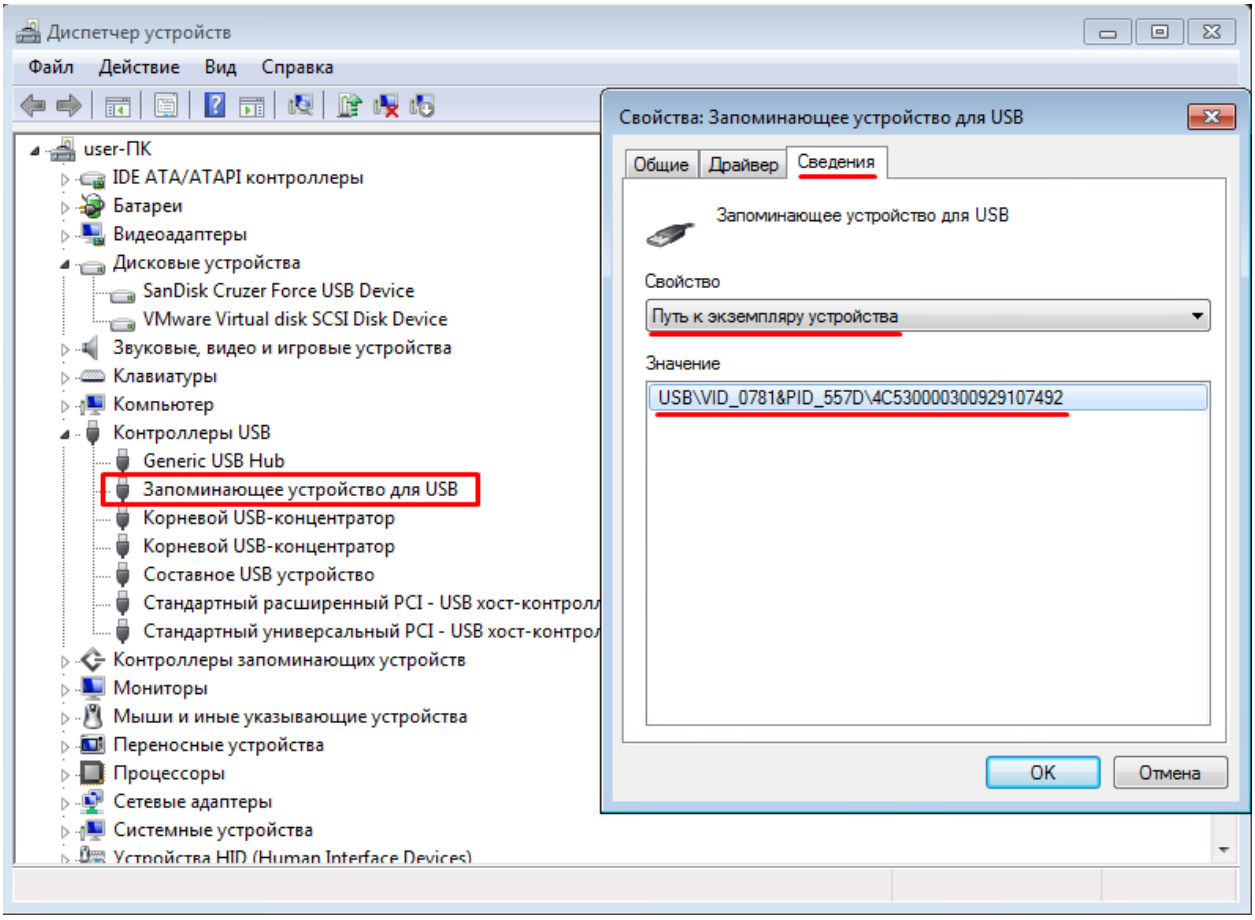
Определение ID стандартными средствами Windows

1. Запустите **Диспетчер устройств**.
2. В пункте **Дисковые устройства**, найдите подключенную флэшку и откройте **Свойства**.
3. На вкладке «Сведения» выберите свойство **Родитель**.
4. В окне **Значение** будет представлен ID флэшки (**HardwareId**).



Альтернативный вариант:

1. Запустите **Диспетчер устройств**.
2. В пункте **Контроллеры USB** найдите **Запоминающее устройство для USB** (название может отличаться).
3. Откройте окно **Свойства**.
4. На вкладке **Сведения** выберите свойство **«Путь к экземпляру устройства»**
5. Значение этого пункта → ID USB-устройства (**HardwareId**).

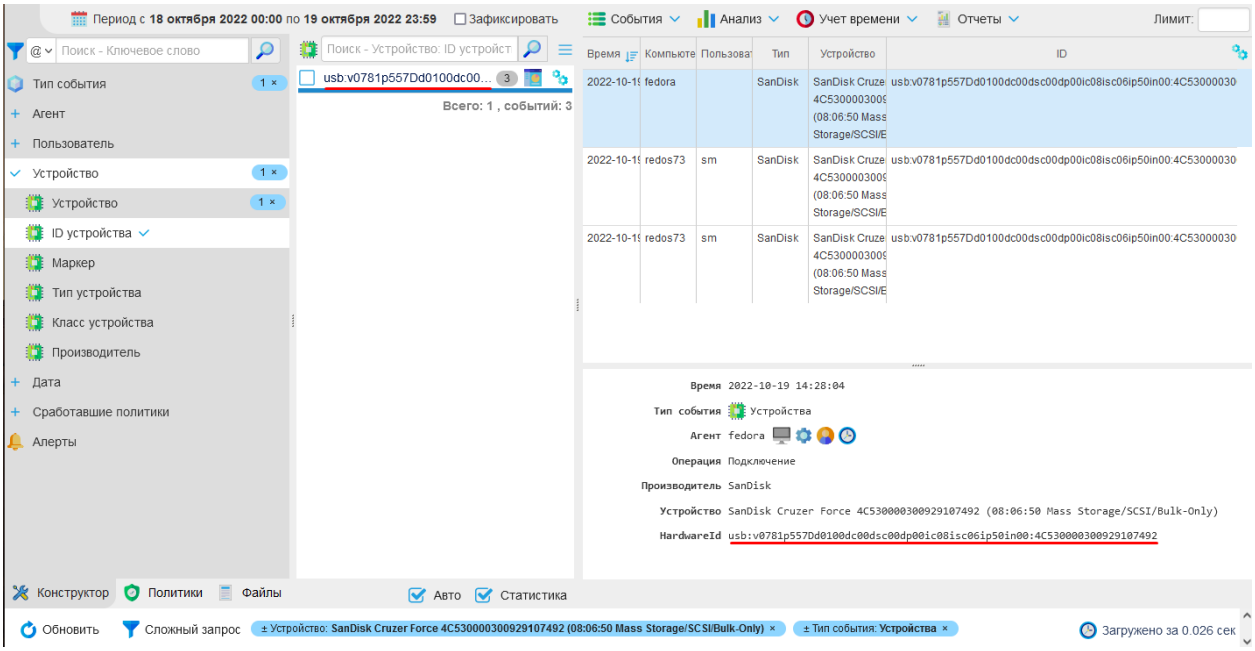


ID USB-накопителя в Linux-агентах

ID USB-накопителя для Linux-агентов передаётся в виде **modalias:serial**.

Определение ID средствами iBatyr Monitor

1. В конструкторе выберите ПК, к которому подключен USB-накопитель.
2. В измерении **Устройство** выберите **Устройство** и найдите флэшку по названию производителя.
3. В разделе **Устройства** → **ID-устройства** будут показаны ID всех устройств, которые подключены к выбранному ПК.
4. Выберите устройство с ID, начинающимся на *usb:*.



Определение ID средствами Linux

Чтобы получить *modalias* и *serial* подключенных устройств, используйте команды:

```
find /sys -name modalias -print0 | xargs -0 cat | sort -u

sudo lsusb -v
```

Также *modalias* и *serial* можно посмотреть в аналоге «Диспетчера устройств» для Linux. Все зависит от того какую оболочку вы используете.

Примечание: Дополнительную информацию о modalias можно прочитать в статье Modalias strings — a practical way to map «ibatyr» to hardware

---

Блокировка USB-накопителей

Полная блокировка

Заблокировать USB-накопители можно как для конкретного компьютера, так и для определёного пользователя. Для этого отредактируйте используемую конфигурацию компьютера (**Панель управления → Конфигурация компьютеров**) или создайте новую конфигурацию для конкретного пользователя (**Панель управления → Конфигурация пользователей → Новая**).

После этого перейдите в настройки **Устройства** и активируйте опцию **Блокировать USB-накопители**.

Частичная блокировка. Чёрный и белый списки

Чёрный список — список заблокированных устройств. При этом устройства, которых нет в чёрном списке, могут быть подключены к компьютеру.

Белый список — список устройств, которым разрешено подключение. При этом устройства, которых нет в списке, не могут быть подключены.

Чёрный список

Чтобы создать чёрный список, то есть заблокировать конкретные USB-накопители или классы USB-устройств:

1. Отключите опцию **Блокировать USB накопители**.
2. Отредактируйте пункт **Правила: Блокировка → USB** (**Правила: Блокировка USB-класс**): укажите ID или класс блокируемых устройств в поле **Блокировать**.

При вводе ID (класса) используется поиск по всем устройствам, которые подключались к агентам. Устройства можно найти и добавить из списка.

Внимание: «**Правила: Блокировка USB-класс**» не используется для Linux-агентов.

Также USB-накопители можно объединять в USB-группы. Для этого в разделе **Панель управления → Устройства** найдите нужные устройства и в поле **Маркер** укажите название группы. Теперь это название можно будет использовать в разделе **Правила: Блокировка → USB группы**.

Подробнее о классах и подклассах ОС Windows можно прочитать в статье Defined Class Codes .

Белый список

Предупреждение: Все устройства и классы устройств, не внесенные в белый список, будут заблокированы.

Чтобы разрешить подключение к компьютеру конкретных USB-накопителей:

1. Определите ID-устройств, которые вносите в белый список.
2. Выберите свою конфигурацию в разделе **Панель управления → Конфигурация компьютеров** или создайте новую в **Панель управления → Конфигурация пользователей** в зависимости от типа блокировки.
3. Перейдите в настройки **Устройства**.
4. Введите ID добавляемых устройств в поле **Разрешить**.

Важно!

Устройства, не добавленные в правило **Разрешить**, будут заблокированы. Обязательно создайте правило с указанием устройств, которые нельзя блокировать. Правило **Белых классов устройств**. Добавьте в это правило usb-hub, клавиатуры, мыши и т. д.

ID, которые нужно добавить в правило **Белых классов**:

- **usb:*ic09isc00*** — оставляет открытым usb-hub. Если не добавить этот ID, то заблокируются все устройства, подключенные через usb.
- **usb:*ic03isc*** — оставляет открытыми клавиатуры и мыши. Некоторые клавиатуры и мыши могут иметь другой *modalias*.

Примечание: У ноутбуков некоторые устройства считаются подключенными через USB: звуковая карта, bluetooth, веб-камера... Эти устройства также нужно добавить в правило **Белых классов устройств**. Для этого в строке **usb:*ic03isc*** вместо «**3**» укажите значение вашего устройства. Символ «*****» в данном случае означает любые символы в зависимости от места постановки.

Только чтение

Чтобы подключаемые USB-устройства переводились в режим **Только чтение**, отредактируйте используемую конфигурацию компьютера или создайте новую конфигурацию для пользователя.

В настройке **Устройства USB** включите опцию **USB накопители только для чтения**.

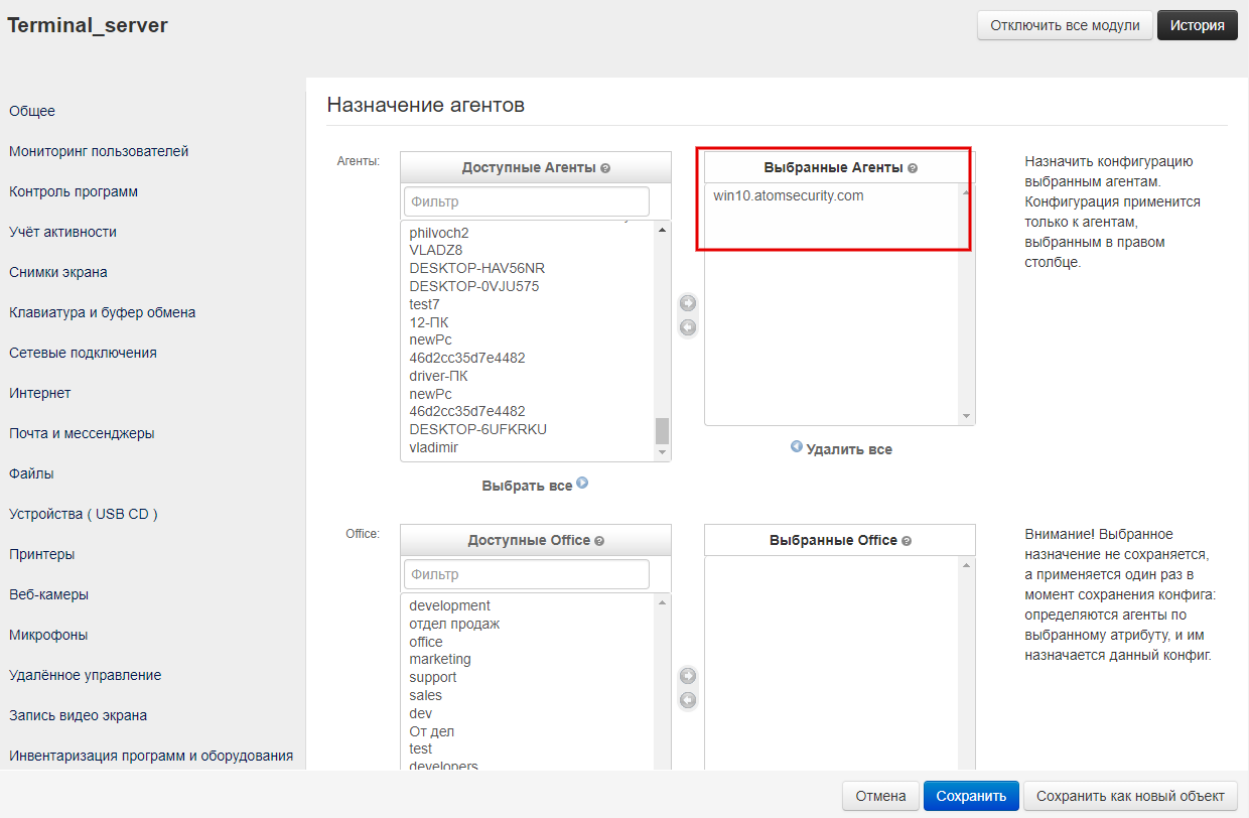
Внимание: Режим **Только чтение** не позволяет составить белый список устройств для полного доступа.

4.5.19 Настройка агента на терминальном сервере

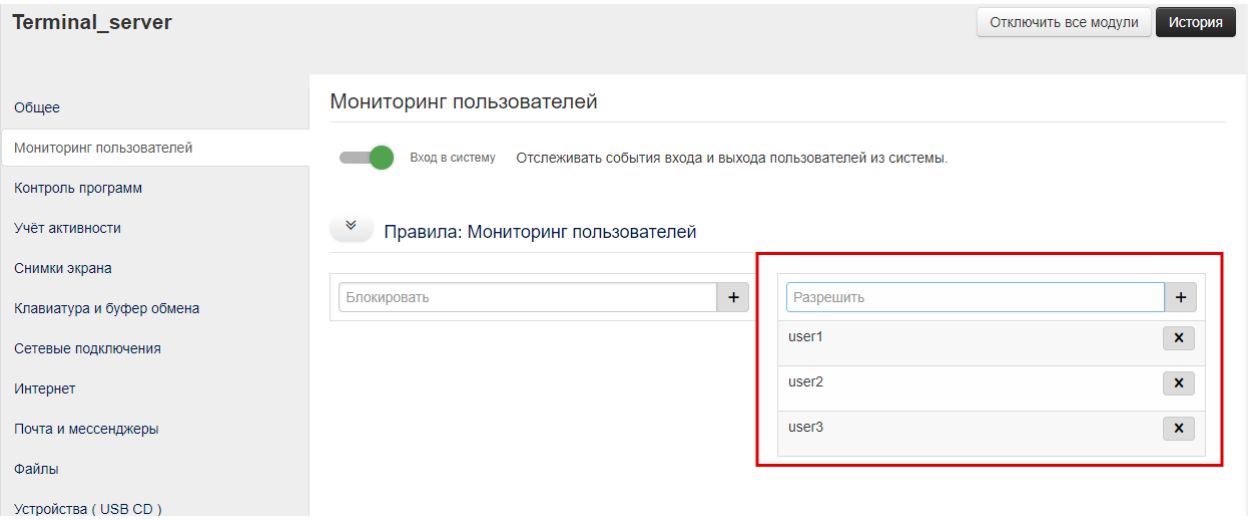
Иногда возникает необходимость в мониторинге пользователей на терминальных серверах. Зачастую есть потребность в мониторинге лишь некоторых определенных пользователей.

Установка агента производится способами, идентичными установке на обычный ПК. Способы описаны разделе *Установка агентов*.

После установки агента на терминальный сервер рекомендуется создать отдельную конфигурацию для терминального сервера, включить необходимые модули мониторинга и затем во вкладке **Назначение агентов** добавить в конфигурацию агента с сервера.



Для того, чтобы выбрать только определенных пользователей для мониторинга используйте **Правила: Мониторинг пользователей**.



При таких настройках будет вестись мониторинг только указанных пользователей, остальные пользователи под наблюдение попадать не будут.

Примечание: Количество пользователей на терминальном сервере лицензируется отдельно. За более подробной информацией обратитесь в отдел продаж по адресу sales@ibatyr.kz

---

4.5.20 Блокировка вложений в веб-почте

Возникла задача:

- Заблокировать отправку файлов в веб-почте популярных почтовых служб, yandex\mail\google\rambler.

Чтобы это сделать нужно добавить правило в Глобальной конфигурации - «Блокировка - Сайты», следюущий список URL-адресов:

```
api/v1/messages/attaches/add
mail.rambler.ru/upload
web-api/upload-attachment
mail.google.com/_/upload
```

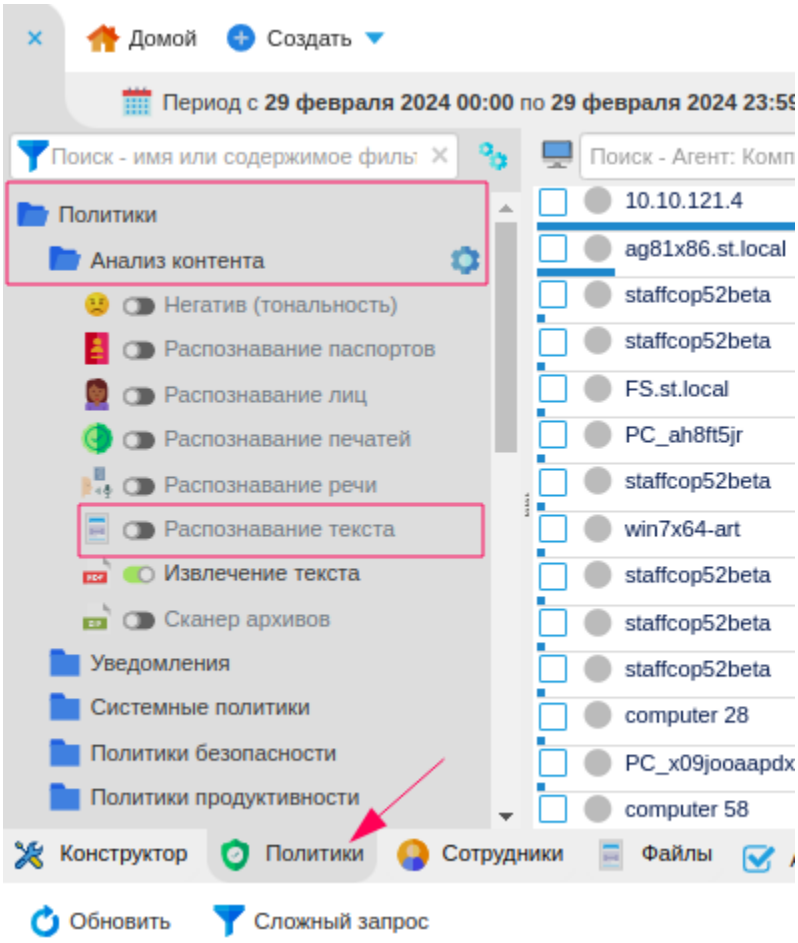
Это заблокирует возможность отправки файлов на популярные почтовые службы. По этому же примеру можно блокировать и другие службы обмена файлами и доменами, для предотвращения попыток выгрузки информации из локальной сети в сеть интернет.

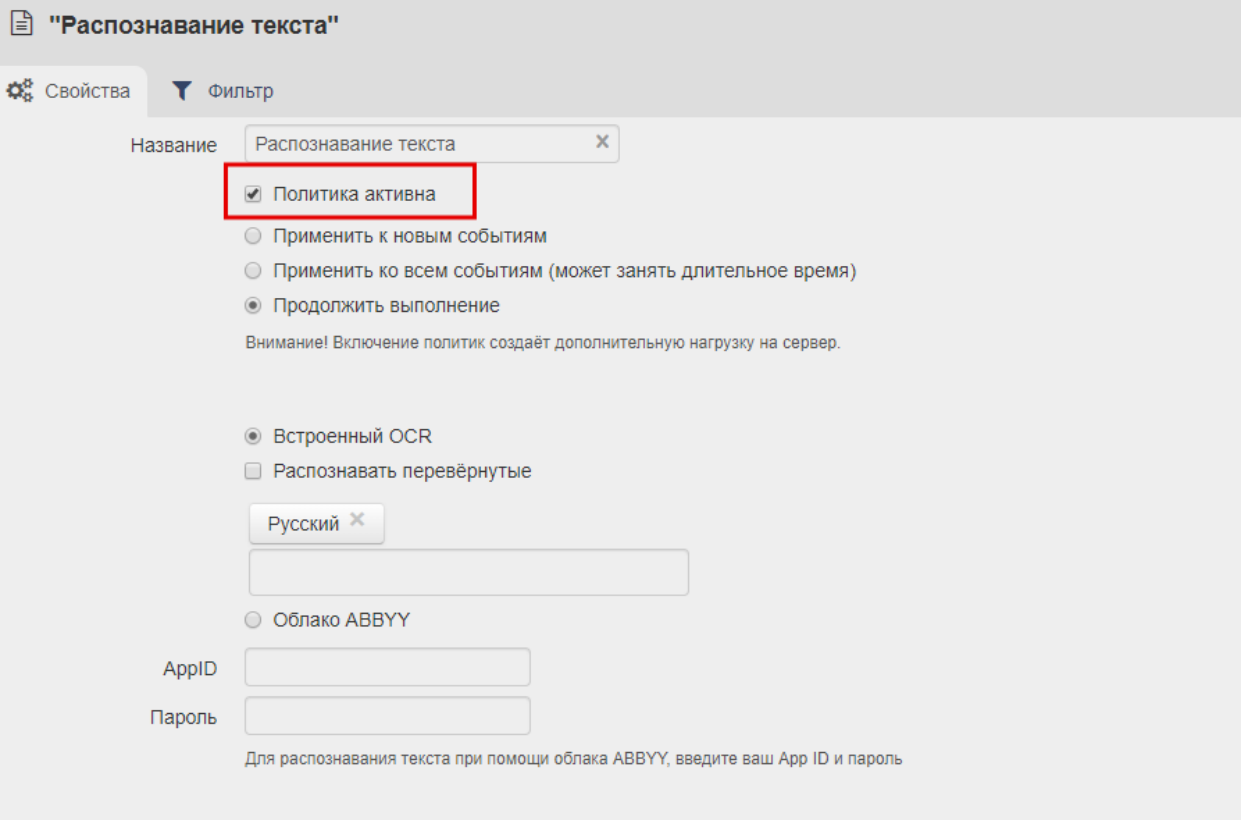
Примечание: Если вы не хотите блокировать отправку вложений для всех пользователей сразу, то эти исключения нужно вносить на странице настроек соответствующей конфигурации пользователей в разделе «Интернет - Правила: Блокировка - Сайты»

4.5.21 Настройка модуля OCR

Для активации распознавания текста на изображениях и документах включите политику **Распознавание текста**.

1. Перейдите во вкладку **Политики**.
2. Откройте папку **Политики**.
3. В папке **Анализ контента** активируйте движок **Распознавание текста**. Откроется окно настройки политики.
4. Установите флажок **Политика активна**.

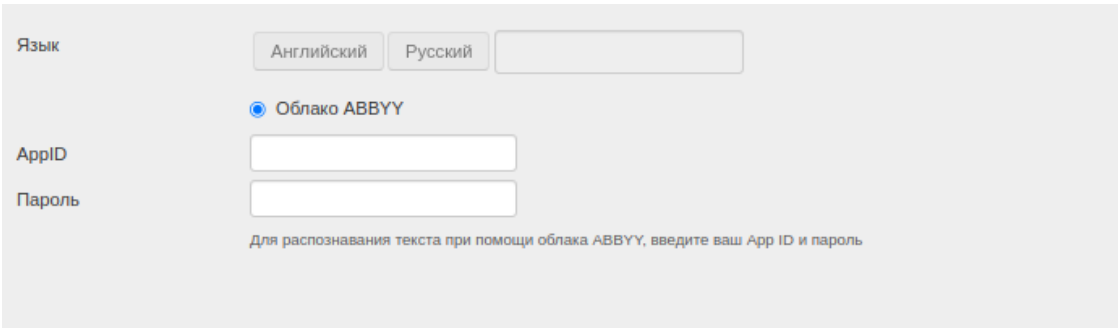

Домой
Создать
Период с 29 февраля 2024 00:00 по 29 февраля 2024 23:59
Поиск - имя или содержимое фильт
Поиск - Агент: Комп
Политики
Анализ контента
Негатив (тональность)
Распознавание паспортов
Распознавание лиц
Распознавание печатей
Распознавание речи
Распознавание текста
Извлечение текста
Сканер архивов
Уведомления
Системные политики
Политики безопасности
Политики продуктивности
10.10.121.4
ag81x86.st.local
staffcop52beta
staffcop52beta
FS.st.local
PC_ah8ft5jr
staffcop52beta
win7x64-art
staffcop52beta
staffcop52beta
staffcop52beta
computer 28
PC_x09jooaapdx
computer 58
Конструктор
Политики
Сотрудники
Файлы
Обновить
Сложный запрос



4. Выберите опции применения политики:
   - *Применить и продолжить* запустит распознавание событий, которые произойдут после планового запуска политик;
   - *Применить к новым событиям* запустит анализ новых событий;
   - *Применить ко всем событиям* перестроит сервер для анализа и старых, и новых событий.
5. Выберите сервер для обработки изображений:

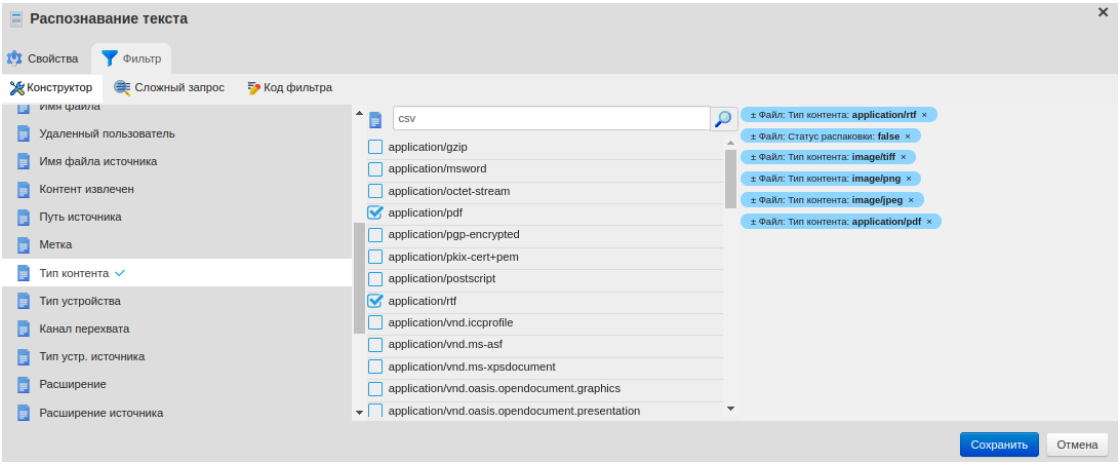
> *Облако ABBYY* и *Content AI ABBYY* — это два разных продукта компании ABBYY.
>
> *Облако ABBYY* — облачная платформа для доступа к сервисам ABBYY, в то время как *Content AI ABBYY* — часть продуктового портфеля ABBYY, ориентированная на использование ИИ для обработки текста и документов.

6. Подключите **Облако ABBYY**. Если у вас есть аккаунт в ABBYY для распознавания документов, вы можете его подключить. После этого для распознавания будут применяться алгоритмы ABBYY.



7. Настройте формат файлов для распознавания. По умолчанию включено распознавание *application/pdf*. Вы можете включить распознавание файлов в форматах *image/jpeg*, *image/png* или других типов документов, например снимков экрана.

   Перейдите во вкладку **Фильтры**, затем в **Файлы** → **Тип контента** и выберите в поле поиска формат файлов:

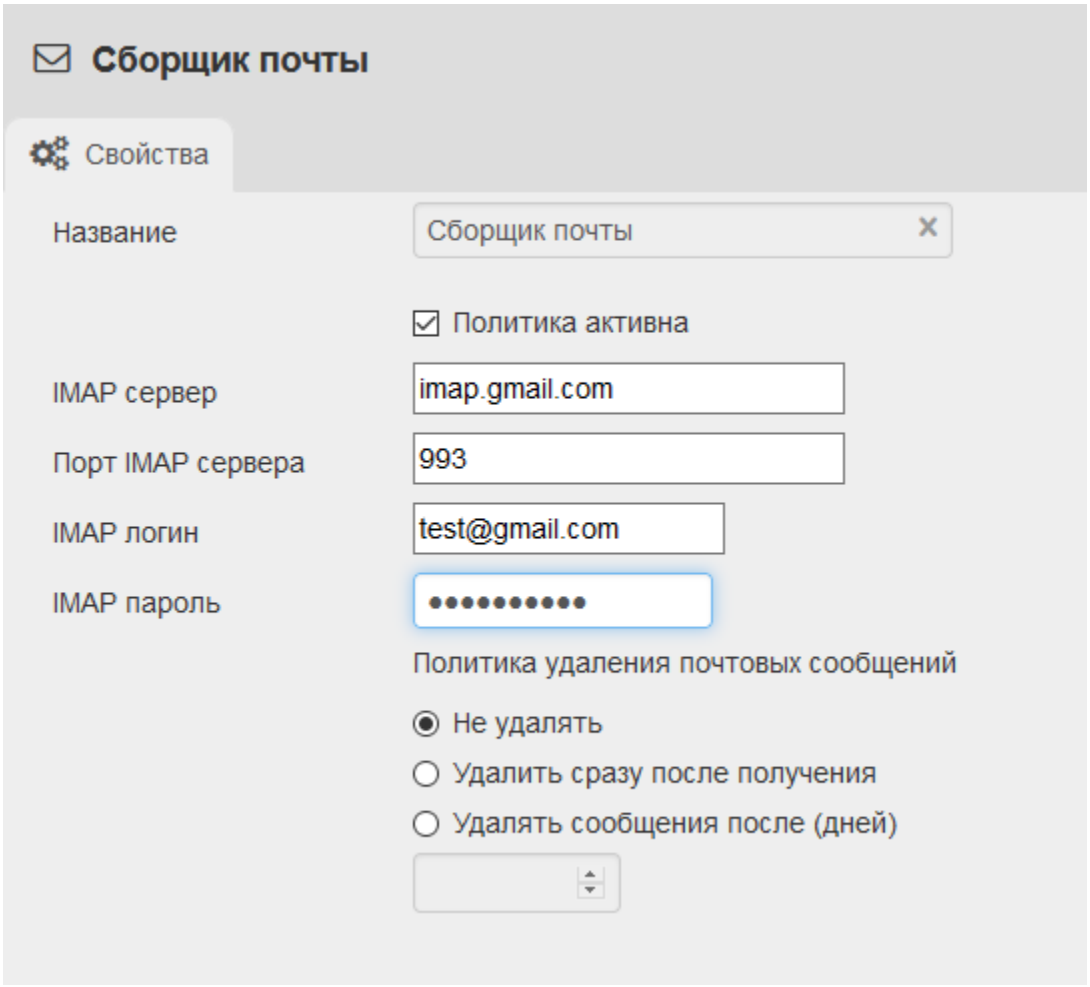


Примечание: При распознавании не перегружайте сервер. Распознавание изображения составляет около 15 с, ряд изображений в очереди снизит скорость обработки.

4.5.22 Перехват почты через IMAP сервер

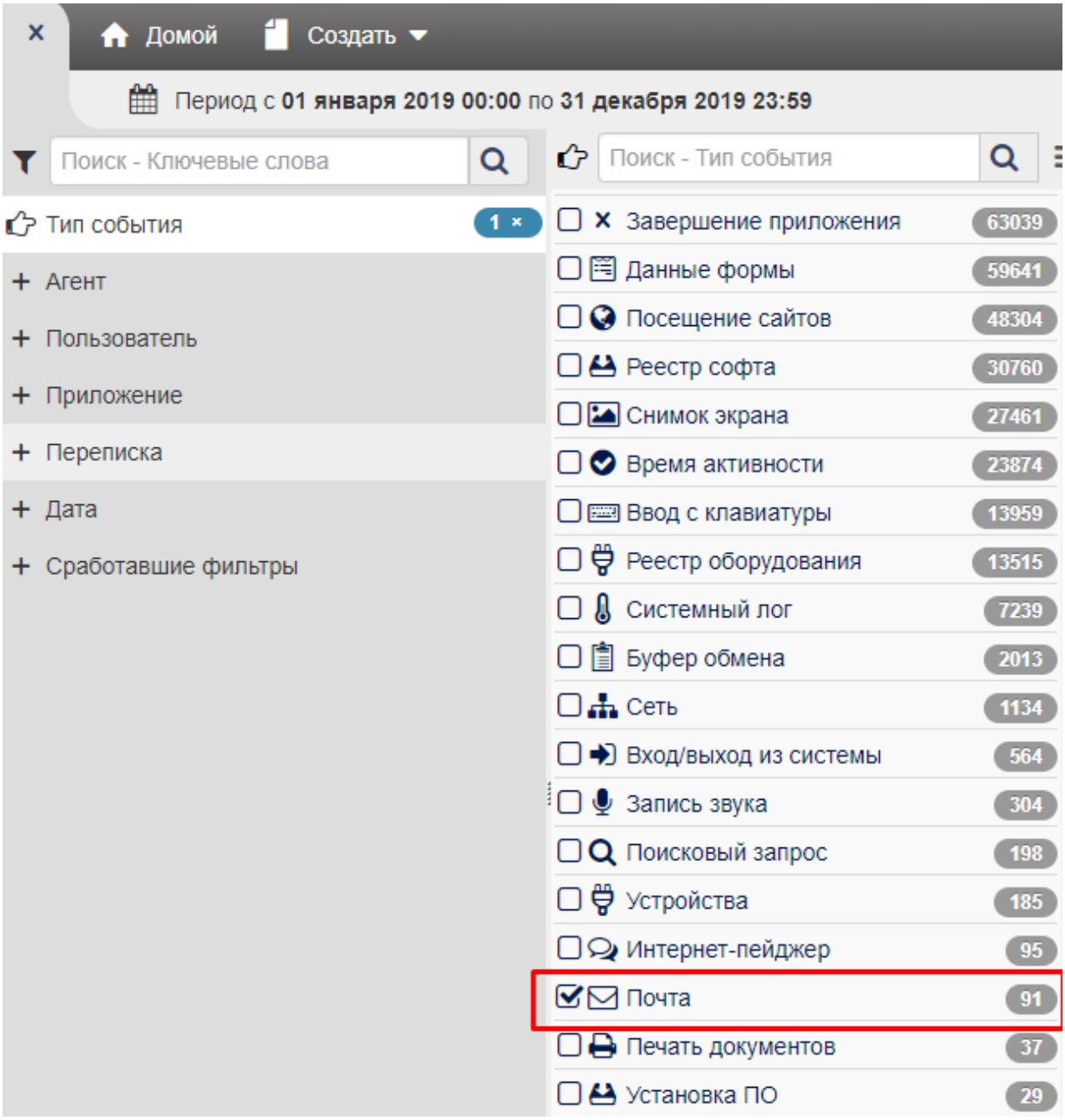
Настройка политики

Для включения политики перехвата почты перейдите в «Фильтры» - «Политики» - «Системные политики» - «Сборщик почты» и включите политику, добавив галочку «Политика активна» и заполните параметры вашего IMAP-сервера. Также можете настроить политику удаления почтовых сообщений.



Примечание: Перехватывается только почта из папки «Входящие»

После включения политики входящая почта будет перехватываться и попадать в тип события «Почта», без указания имени пользователя.

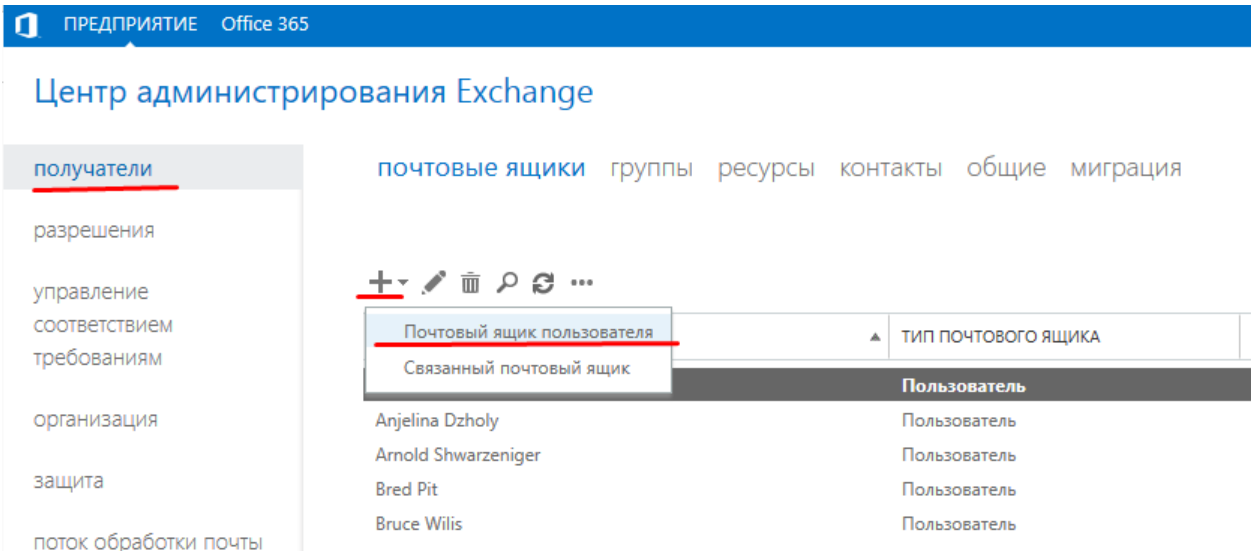


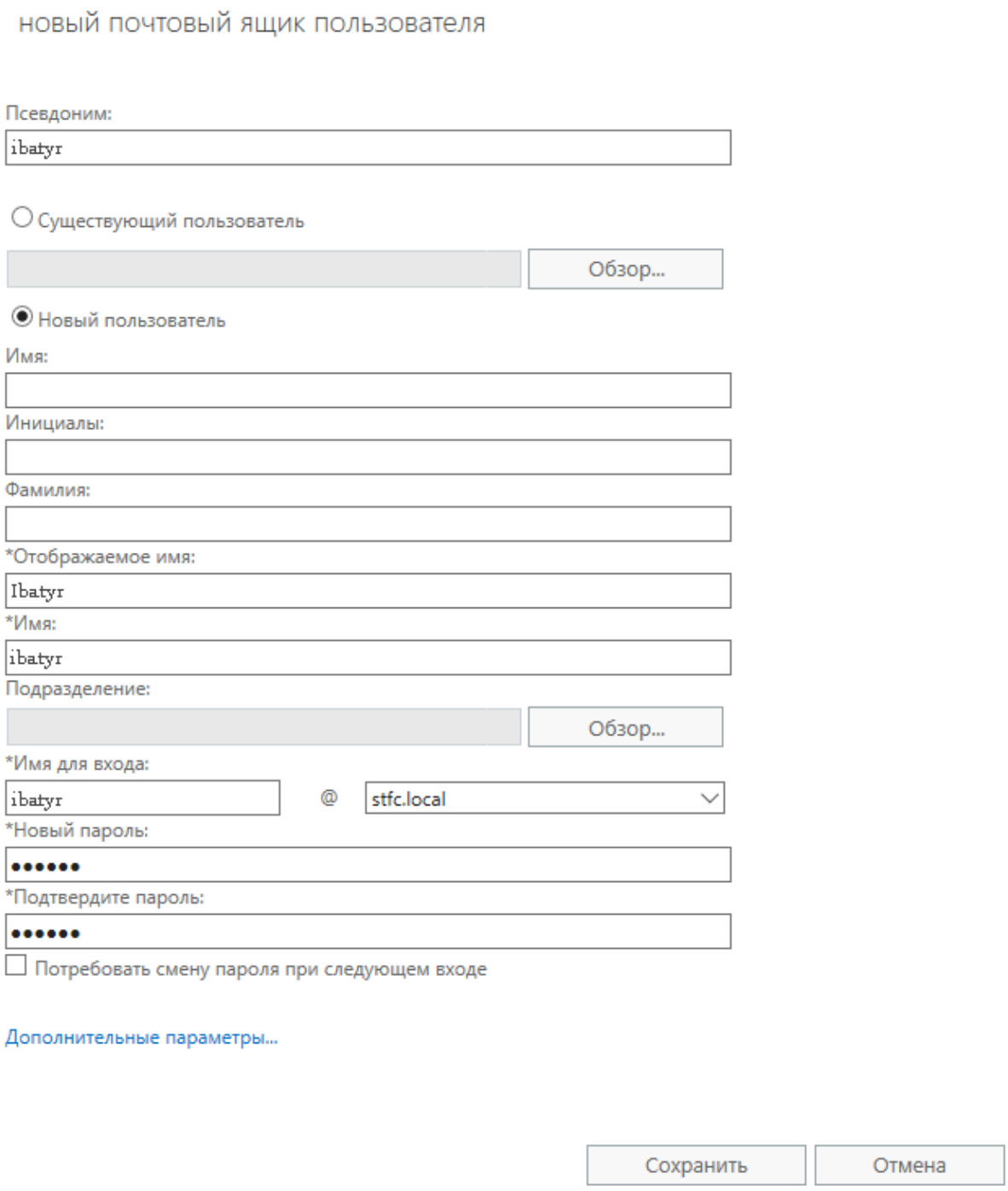
Работу перехвата можно проверить на сервере, выполнив команду

```
ibatyr grab --server=imap.gmail.com --login=test@gmail.com --password=XXXXX
```

Настройка сервера Exchange для работы перехвата

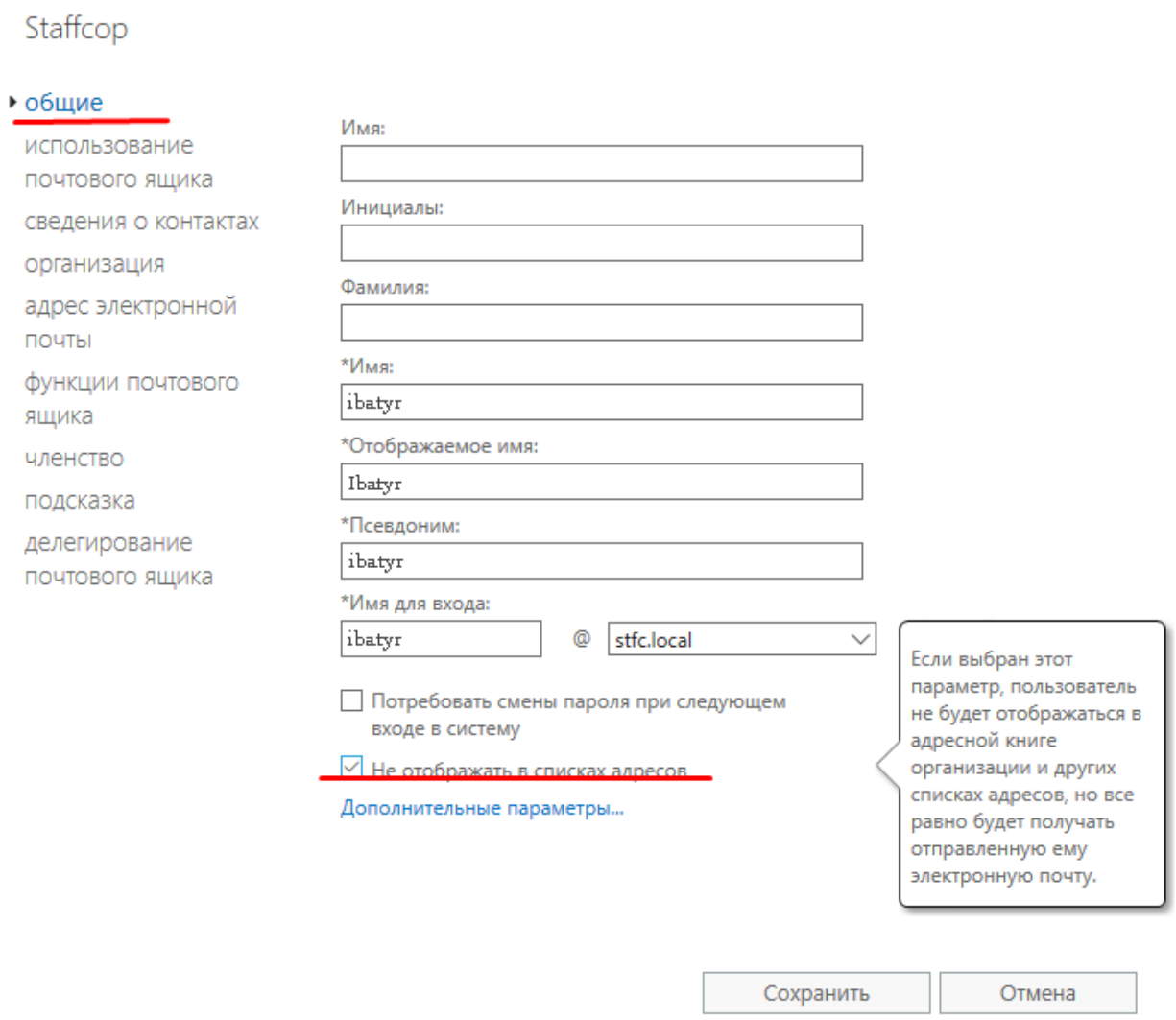
Создайте служебный почтовый ящик, откуда будет собираться информация.

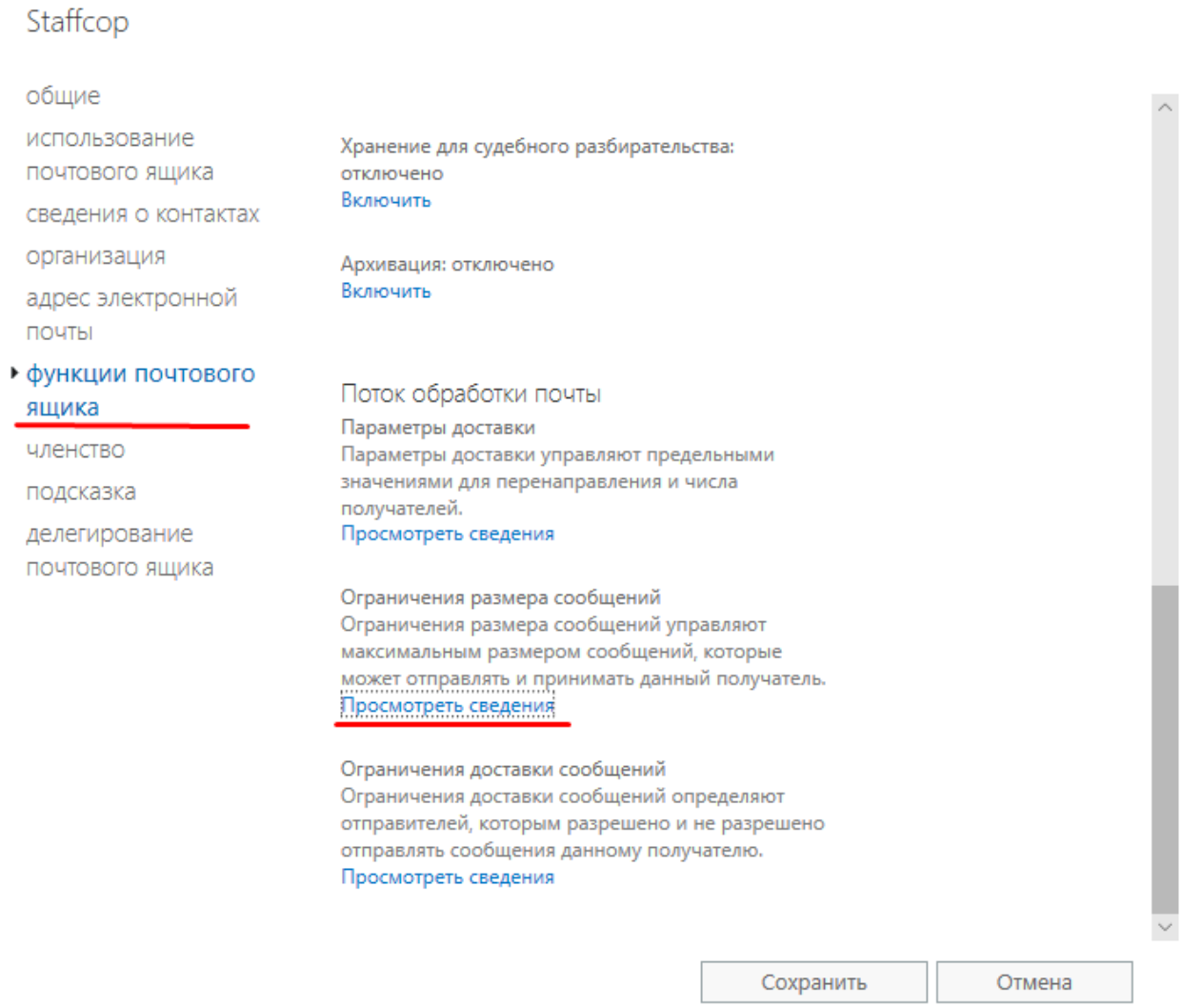


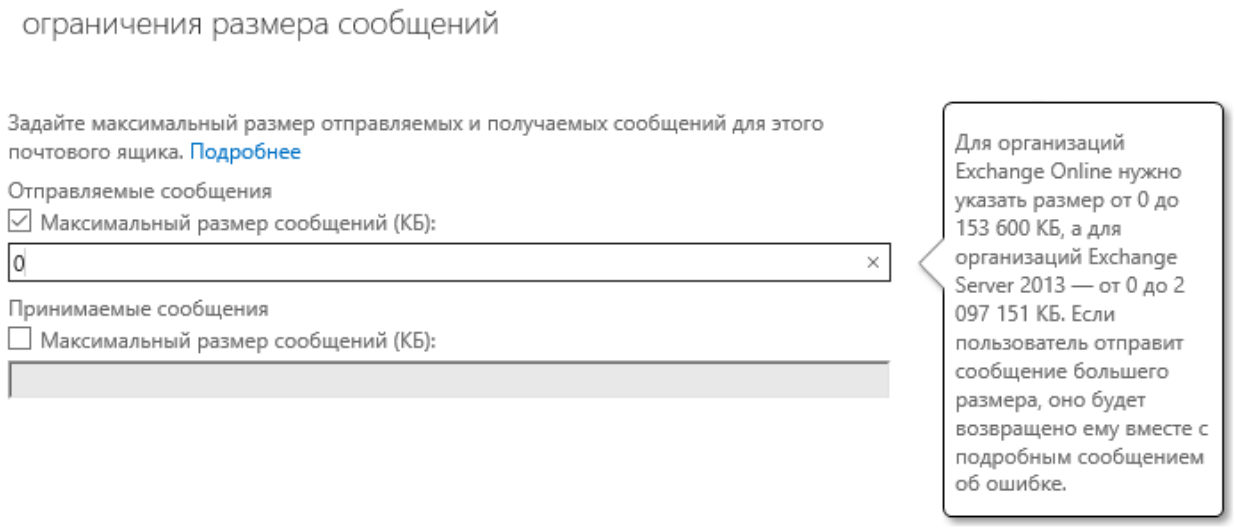


В созданном почтовом ящике нужно указать следующие значения:

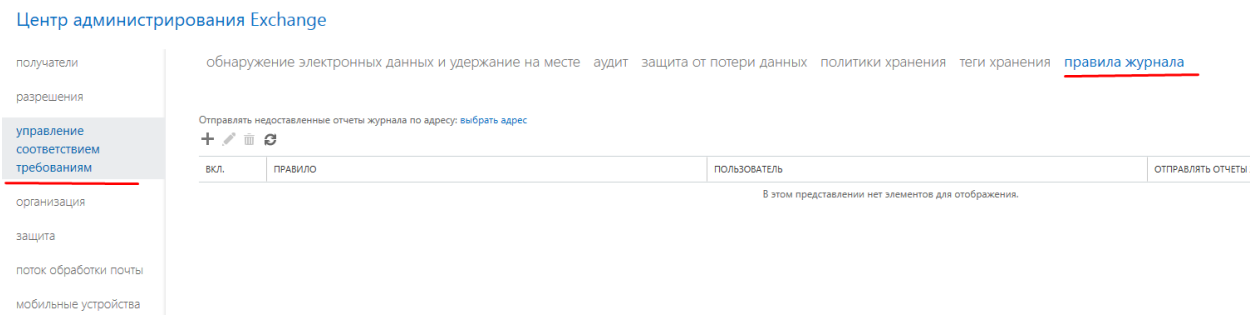
- Общие: Не отображать в списке адресов
- Функции почтового ящика: Ограничения размера сообщений
- Установите Максимальный размер сообщений 0 кб

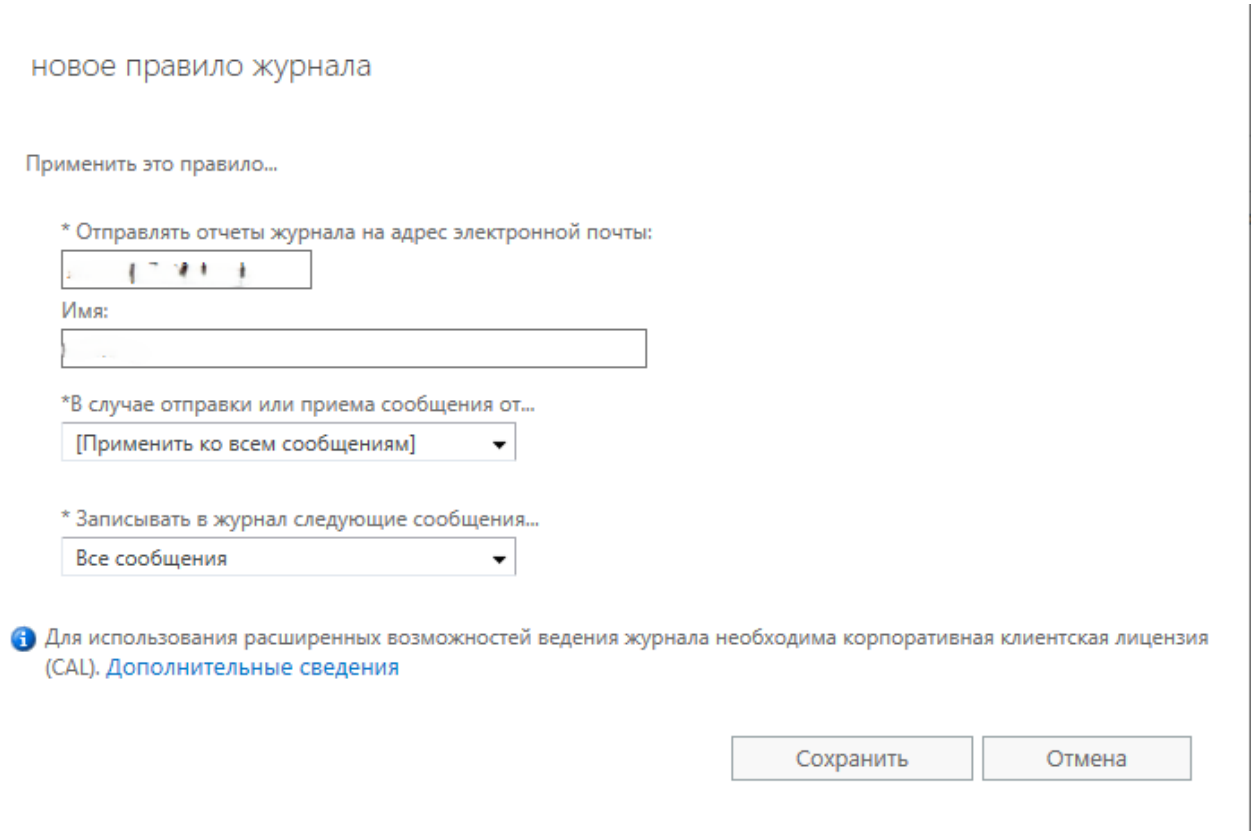

Staffcop
общие
использование почтового ящика
сведения о контактах
организация
адрес электронной почты
функции почтового ящика
членство
подсказка
делегирование почтового ящика
Имя:
Инициалы:
Фамилия:
*Имя:
ibatyr
*Отображаемое имя:
Ibatyr
*Псевдоним:
ibatyr
*Имя для входа:
ibatyr
@
stfc.local
Потребовать смены пароля при следующем входе в систему
Не отображать в списках адресов
Дополнительные параметры...
Если выбран этот параметр, пользователь не будет отображаться в адресной книге организации и других списках адресов, но все равно будет получать отправленную ему электронную почту.
Сохранить
Отмена


Staffcop
общие
использование почтового ящика
сведения о контактах
организация
адрес электронной почты
функции почтового ящика
членство
подсказка
делегирование почтового ящика
Хранение для судебного разбирательства: отключено
Включить
Архивация: отключено
Включить
Поток обработки почты
Параметры доставки
Параметры доставки управляют предельными значениями для перенаправления и числа получателей.
Просмотреть сведения
Ограничения размера сообщений
Ограничения размера сообщений управляют максимальным размером сообщений, которые может отправлять и принимать данный получатель.
Просмотреть сведения
Ограничения доставки сообщений
Ограничения доставки сообщений определяют отправителей, которым разрешено и не разрешено отправлять сообщения данному получателю.
Просмотреть сведения
Сохранить
Отмена

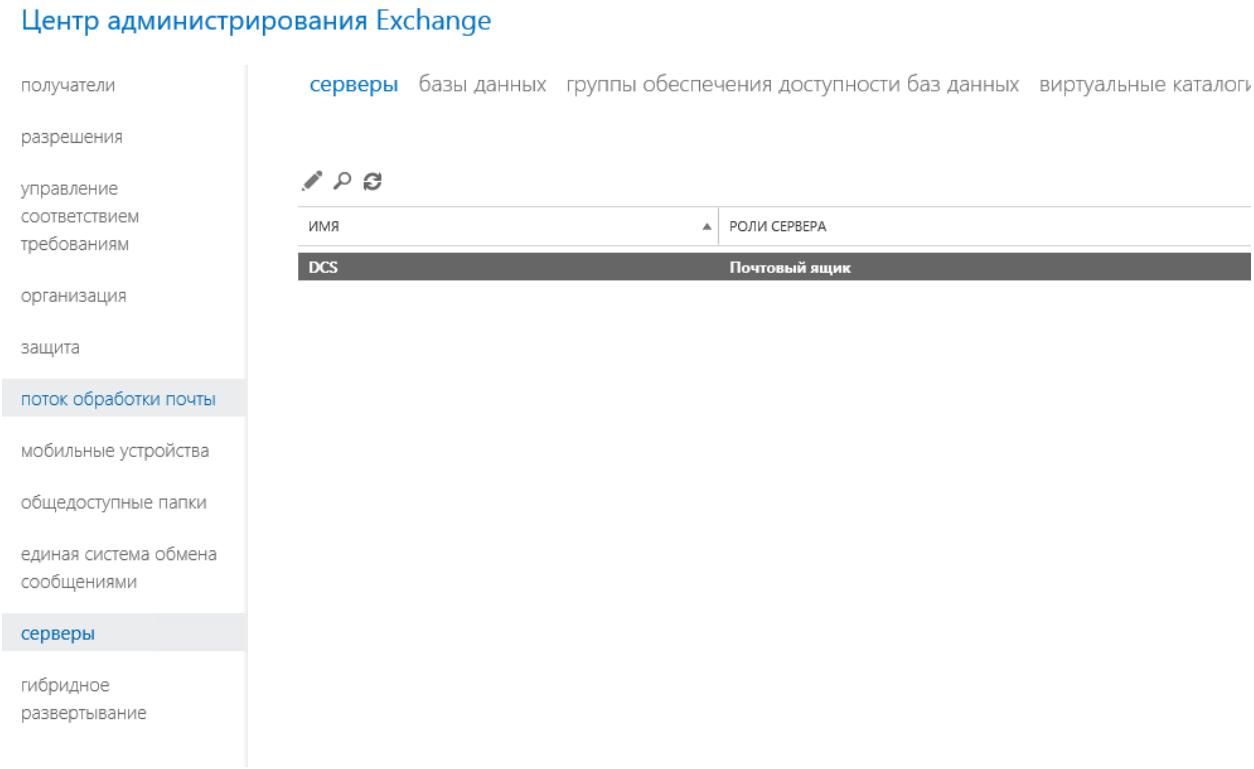


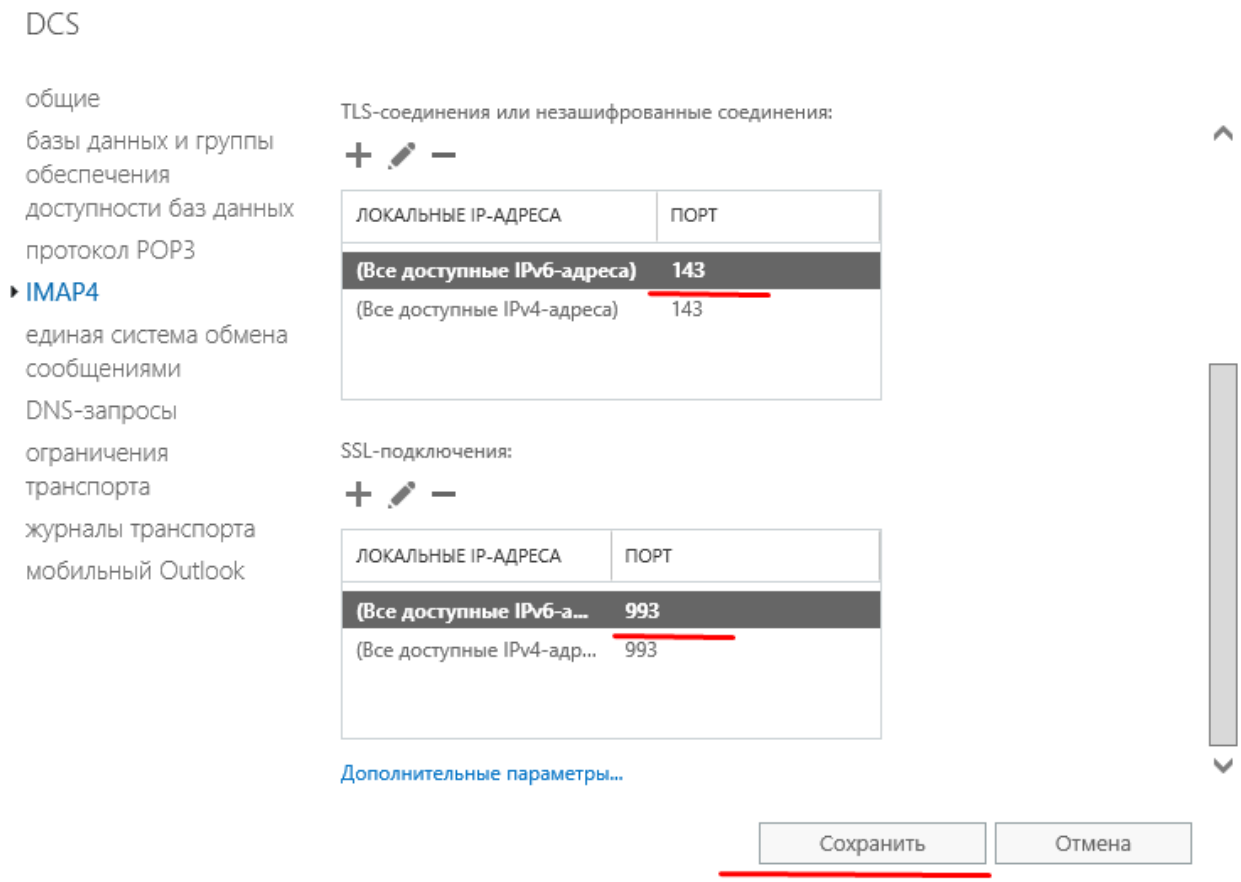
Настройте правила перехвата писем



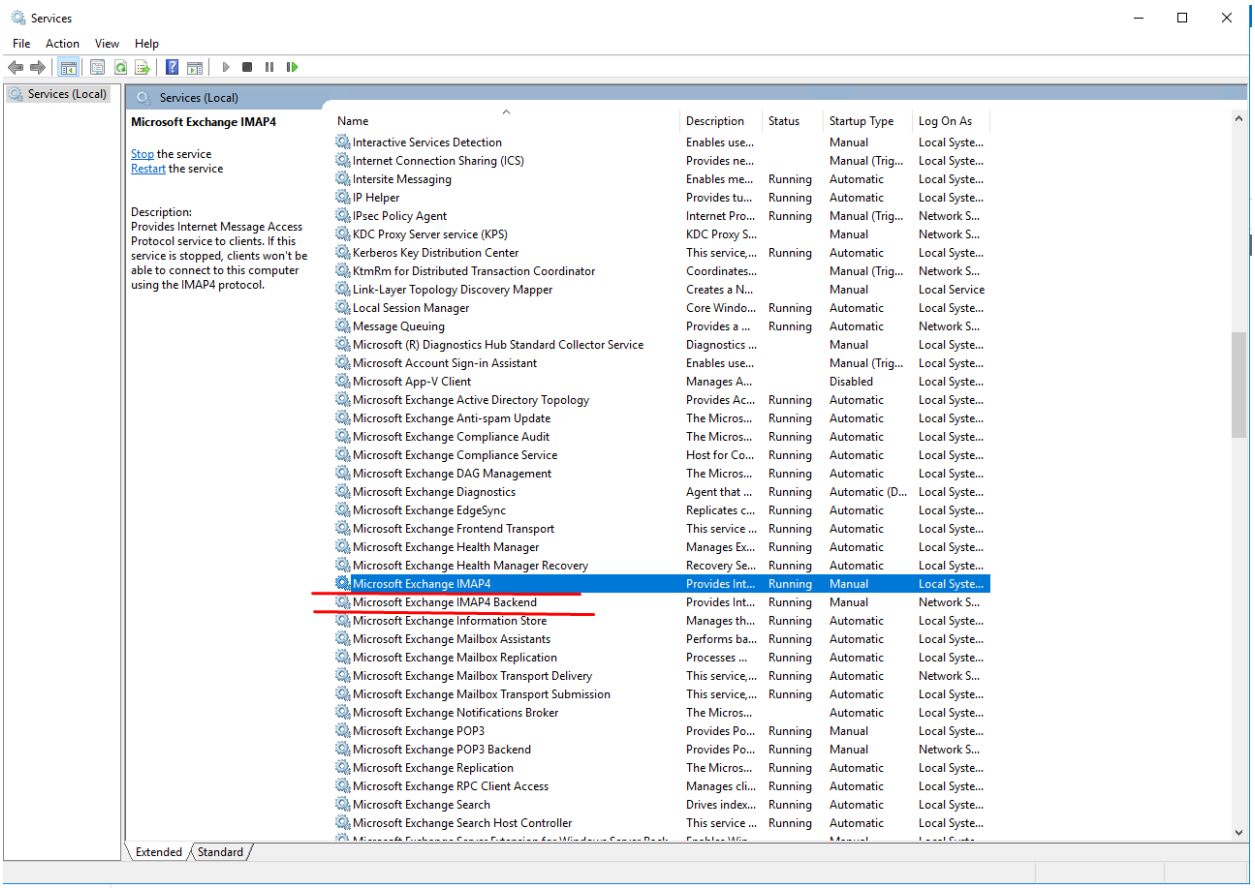


Не забудьте включить протокол IMAP в настройках Exchange



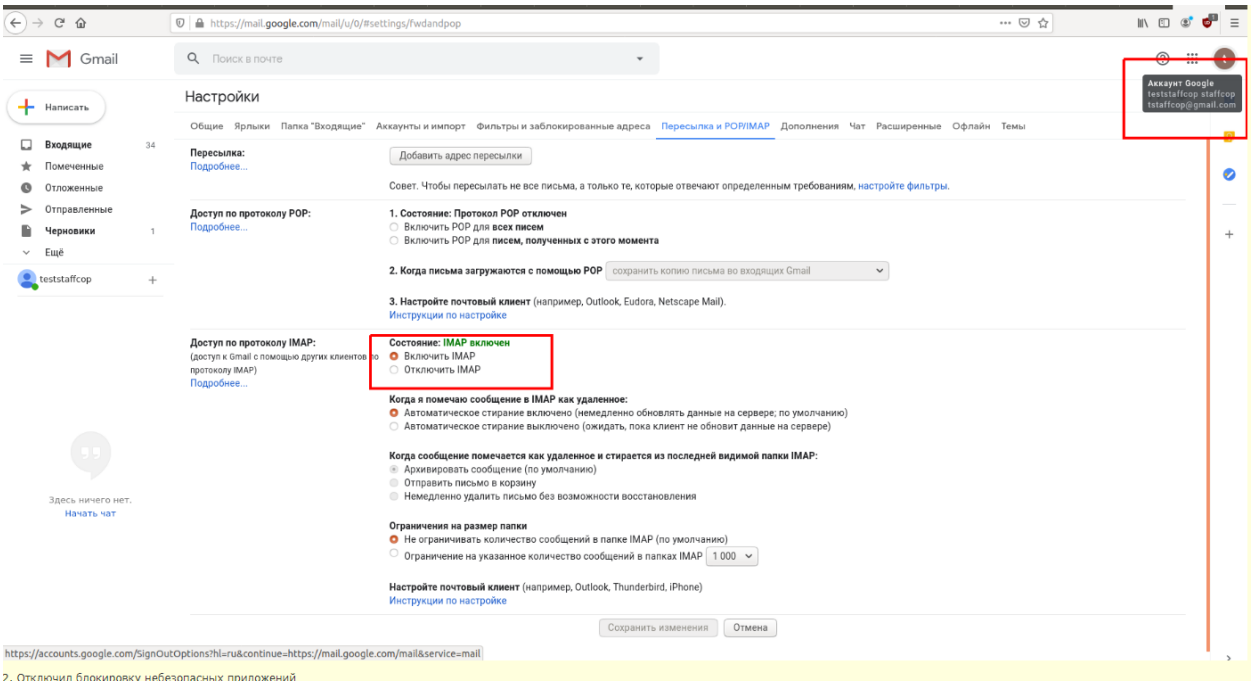


И запустить соответствующие службы

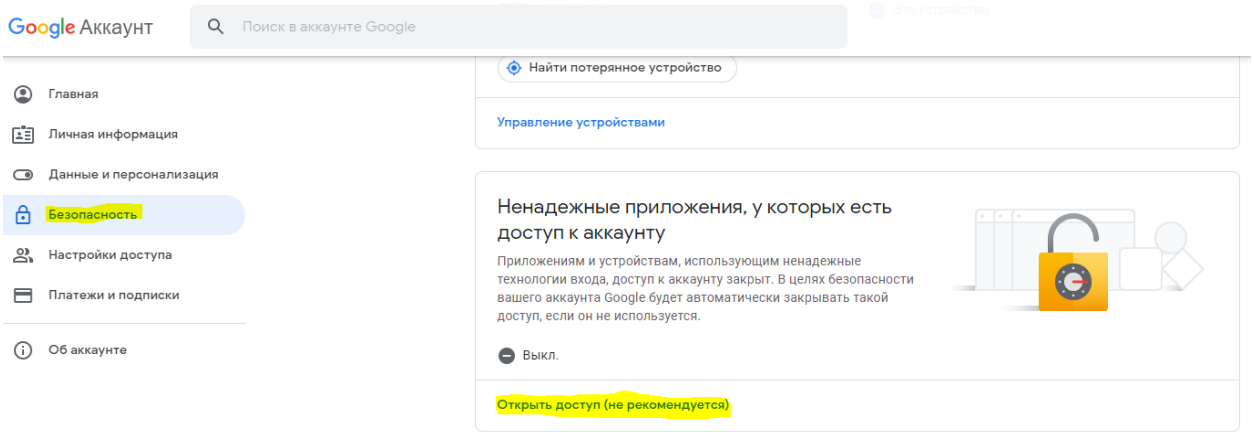


Настройка перехвата почты из почтового ящика Gmail

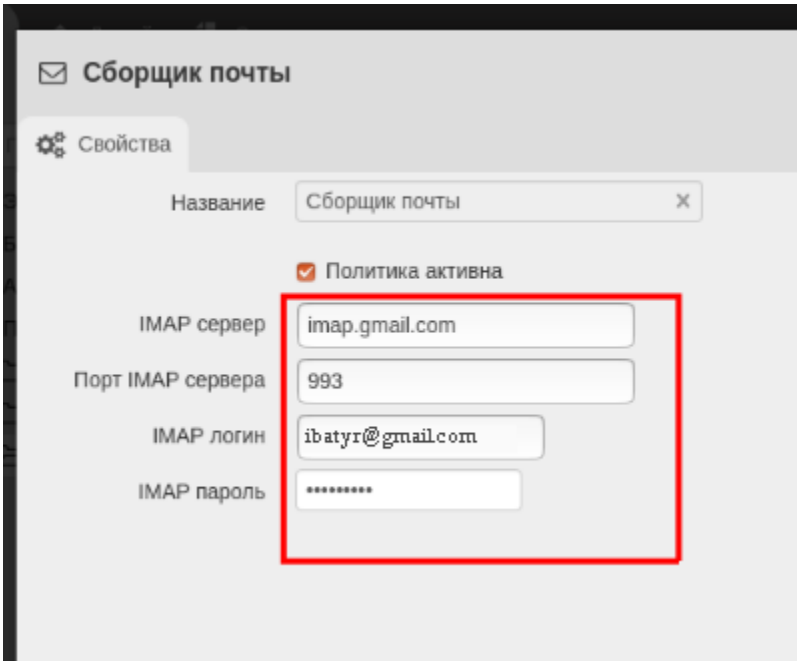
1. Необходимо включить поддержку Imap протокола в настройках почтового ящика



2. В настройках аккаунта Google требуется явно разрешить доступ сторонних сервисов, включением специальной настройкой безопасности для доступа в почтовый ящик



3. В настройках сборщика почты указать адрес сервера и учетные данные.



Настройка почтового ящика Zimbra на перехват почты:

В файле main.cf

/opt/zimbra/postfix/conf/main.cf

или на версии 8.8

/opt/zimbra/common/conf/main.cf

добавить строку

always_bcc = сервисный_ящик@домен.ru

Копия всей почты сыпется на **сервисный_ящик@домен.ru**, а потом уже iBatyr Monitor забирает её через через IMAP-граббер.

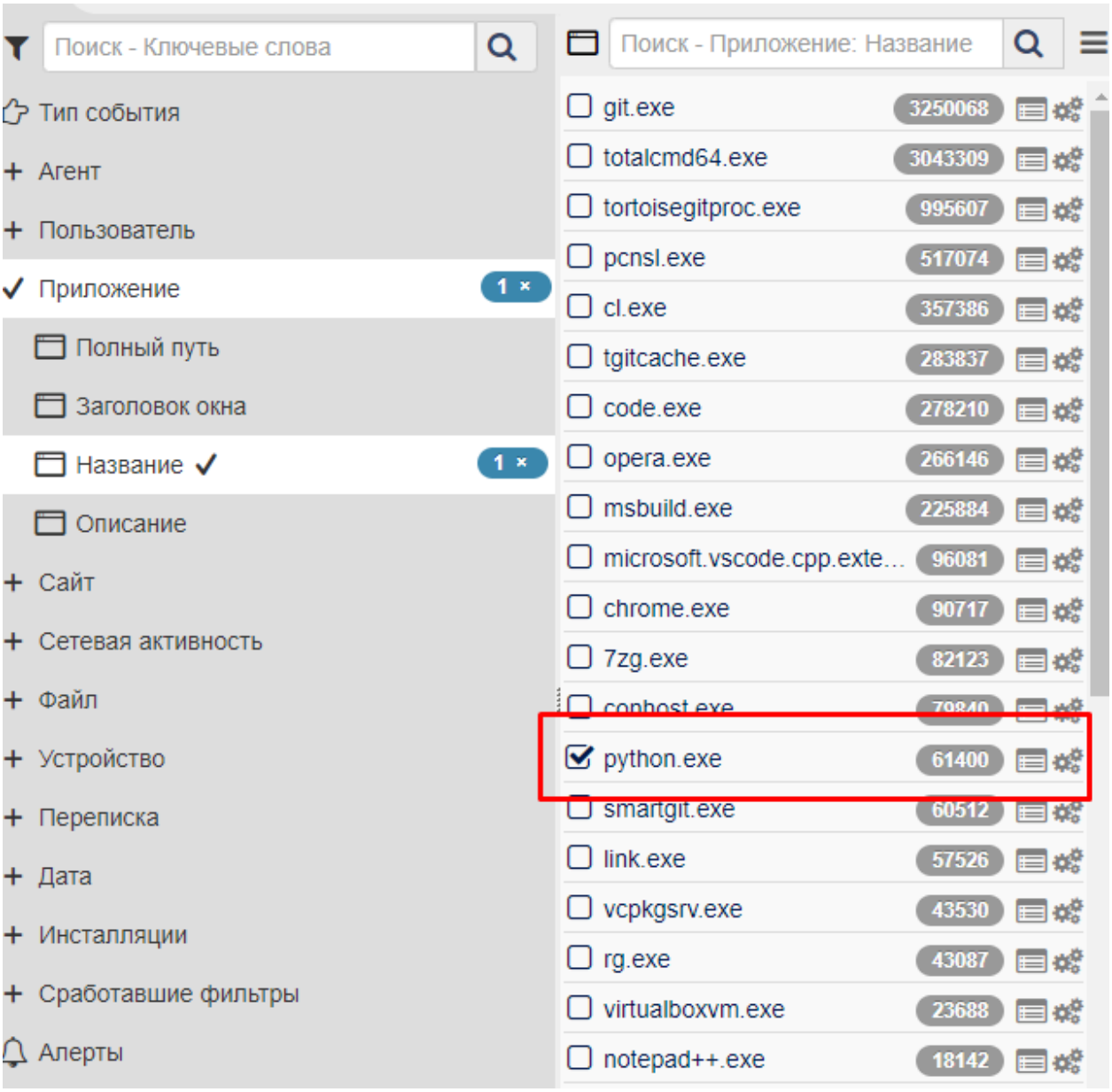
4.5.23 Отслеживание работы в «левых» проектах

При помощи модуля файловой активности можно отследить пользователей, которые используют рабочее время для участия в сторонних проектах. Отследить такое поведение можно в случае соблюдения нескольких правил:

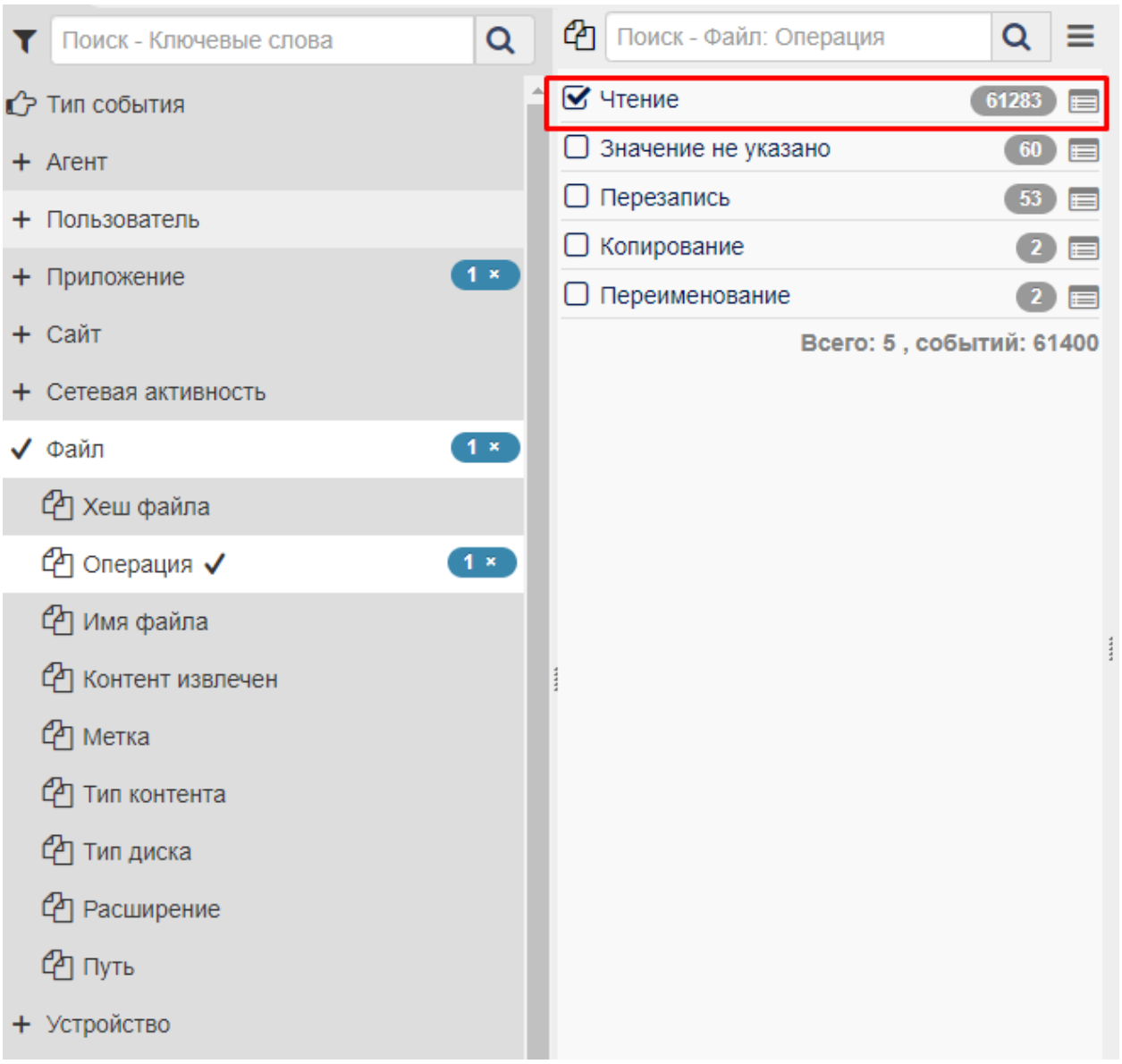
- Ваше рабочее пространство — проекты, находится в одной, четко определенной директории.
- Используется определенное программное обеспечение для работы всех сотрудников в проекте, например, AutoCAD.

При соблюдении этих правил можно построить фильтр, который выявит всю работу в выбранном приложении, которая происходила не в вашем рабочем пространстве. Например при открытии проектов с флешки.

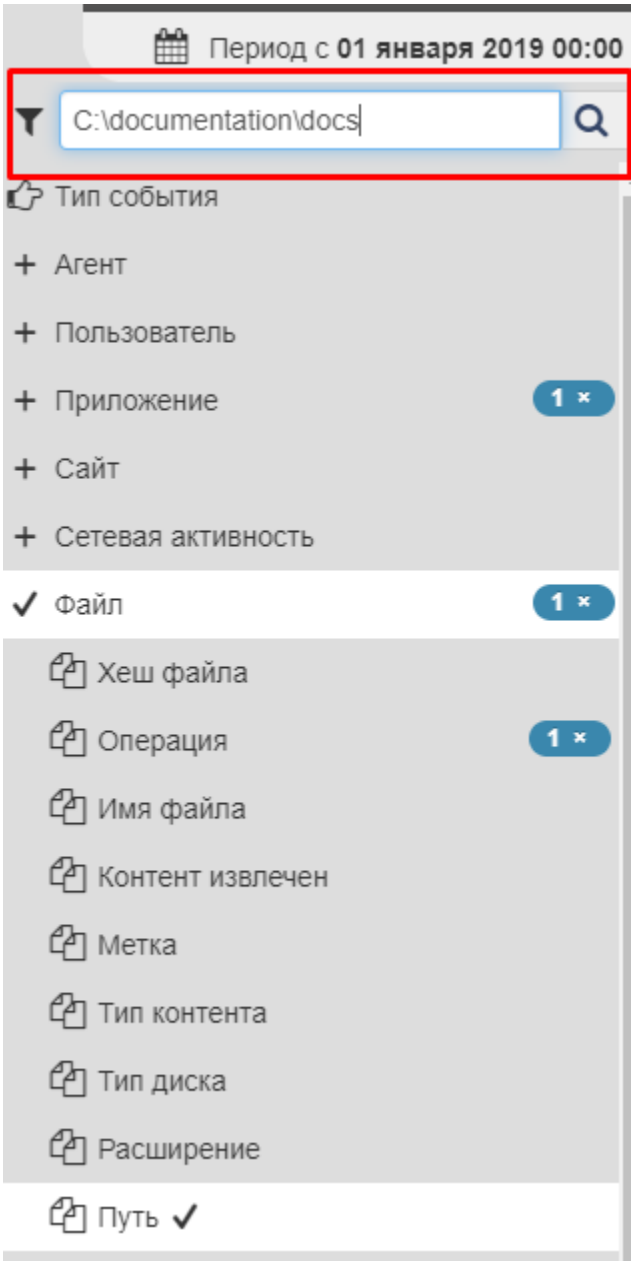
Для этого создайте новый фильтр. Укажите в качестве первого параметра имя приложения. В нашем примере это будет python.exe



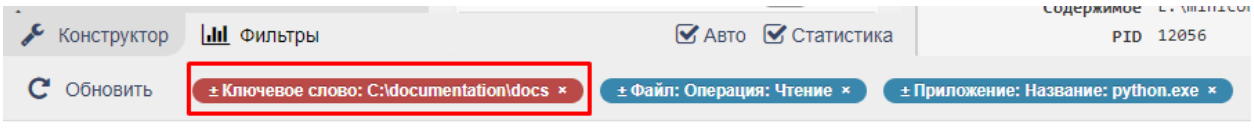
Затем перейдите в файловые операции и выберите операции чтения. При работе приложения с файлами проекта будет очень много файловых операций чтения.



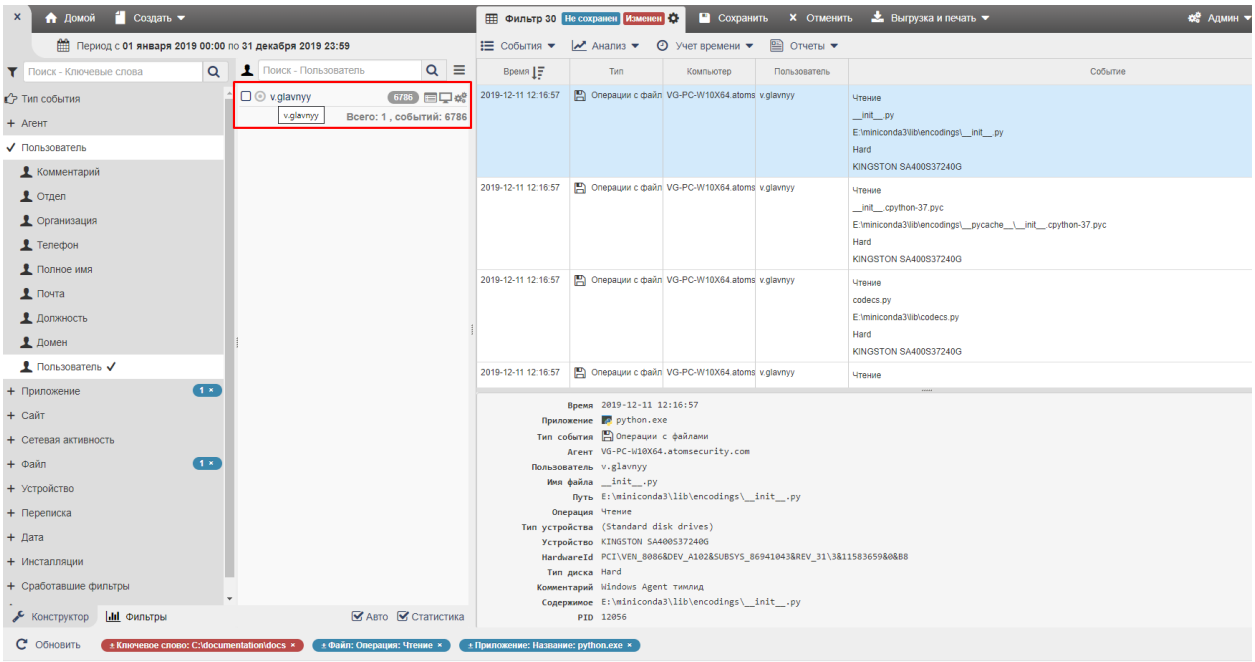
Теперь осталось только указать директорию, в которой лежат проекты в качестве ключевого слова.



И инвертировать поиск, оставив только файловые операции в директориях, отличных от нашей рабочей директории.



Таким образом можно выявить пользователей, файлы, с которыми они работают и расследовать инциденты в случае работы «на стороне».



4.5.24 Загрузка дополнительной информации о сотрудниках в динамические поля

Работа с динамическими полями

Добавляет новый атрибут в измерение (создает колонку в таблице постгресса и кликхауса, отображает ее измерениях и в формах админки): **ibatyr dynamic add [dimension] [attribute] [Русская метка] [Английская метка]**

```
ibatyr dynamic add agent_account physicalDeliveryOfficeName Комната Room
```

Удаляет атрибут из измерения, дропает колонки: **ibatyr dynamic delete [dimension] [attribute]**

```
ibatyr dynamic delete agent_account physicalDeliveryOfficeName
```

Отображает динамические атрибуты: **ibatyr dynamic list**

```
ibatyr dynamic list
{
   "agent_account": [
       {
           "name": "physicaldeliveryofficename",
           "label": {
               "ru": "Комната",
               "en": "Room"
           }
       }
   ]
}
```

Информация о динамических атрибутах хранится в файле /var/lib/ibatyr/dynamic.json

Имя атрибута АД должно совпадать с именем динамического атрибута. После синхронизации с AD данные заполняются.

Загрузка данных о сотрудниках через csv

Для загрузки данных используется команда **ibatyr update_models_from_csv**.

Позволяет обновить данные в модели, включая динамические поля из файла формата csv.

Естественно, что динамические поля должны быть добавлены к таблице.

Ключи командной строки:

- —search-key search_expr* — поле по которому будет произведен поиск записи для обновления и какое значение из строки csv-файла будет использовано для поиска.
- —map map_expr* — одна или несколько данных опций указывают какие поля и необходимо обновить и какие значения из строки csv-файла будут использованы для этого.
- —no-dry-run* — действительно обновить данные. По умолчанию обновление не происходит - только вывод протокола обновления на экран.
- —coding* — кодировка входного csv-файла
- —skip-header* — пропустить первую строку csv-файла (она может содержать заголовок). По умолчанию отключена.
- -v / —verbosity* — уровень логирования (0 - отключить)
- —delimiter* — разделитель колонок в csv-файле. По умолчанию „;“

Выражения в командной строке в опциях –search-key и –map

Выражение имеет вид: <имя_поля>=<столбцы в строке csv-файла через запятую>

Например: «*—search_expression mail=1*» — означает, что для поиска записей для обновления будет использовано поле mail, а значения будут браться из колонки первой строки csv-файла

«*—map office=1,2,3*» - означает, что если запись найдена, то для нее будет обновлено поле office, которое примет объединенное значение из колонок 1,2,3

Дополнительно можно указывать символ объединения: «*—map office=1,2,3:.*» — означает, что если запись найдена, то для нее будет обновлено поле office, которое примет объединенное через „.“ значение из колонок 1,2,3

Можно не перечислять все номера, а использовать диапазон. Последний номер не включается (как в Python) «*—map office=1-4:.*» — означает, что если запись найдена, то для нее будет обновлено поле office, которое примет объединенное через „.“ значение из колонок 1,2,3

И можно использовать комбинации номеров колонок и диапазонов «*—map office=1-4,10:.*» — означает, что если запись найдена, то для нее будет обновлено поле office, которое примет объединенное через „.“ значение из колонок 1,2,3,10

Пересечение и дублирование номеров колонок в выражениях допускается. В таком случае значение колонки будет просто продублировано, столько раз, сколько некоторый номер колонки встретился в выражении (включая диапазоны).

Вместо номера последней колонки можно использовать символ * - это верно и для диапазонов.

0-* — означает взять значения из всех колонок

Ограничения:

Пока можно обновлять только одну модель (таблицу) — Пользователи (*agent_account*)

Не все поля можно обновить — для *agent_ account* это:

- „comment“— Комментарий
- „skype“ — Номер / логин скайп
- „phone“ — Номер телефона
- „post“ — Должность
- „full_ name“ — Полное Имя
- „office“ — Отдел/офис
- „www“ — Веб-страница
- „company“ — Организация
- „manager“ — Руководитель
- „Все динамические поля, которые добавлены командой ibatyr dynamic add .... „

Не по всем полям можно производить поиск (не все поля можно указывать в –search-key) для *agent_ account* это:

- mail — email юзера
- user_ name — имя пользователя

Поиск записей происходит только по текстовым полям. С использованием выражения „like“ Это означает, что при поиске может быть найдено сразу несколько подходящих записей для обновления. Обновлены будут все!

Формат файла csv

Пример:

```
Сотрудник;Корпоративный email;Подразделение1;;;;;;;;
;;;;;;;;;;
Иванов Александр Петрович;a.ivanov@atloc.ru;Хозяйственное управление;;;;;;;;
Петров Антон Александрович;a.petrov@atloc.ru;Департамент страхования;;;;;;;;
Дихтярь Илья Сергеевич;i.dictyar@atloc.ru;Департамент клиентского обслуживания;;;;;;;;
;;;;;;;;;;
```

Загрузку на основе примера выше:

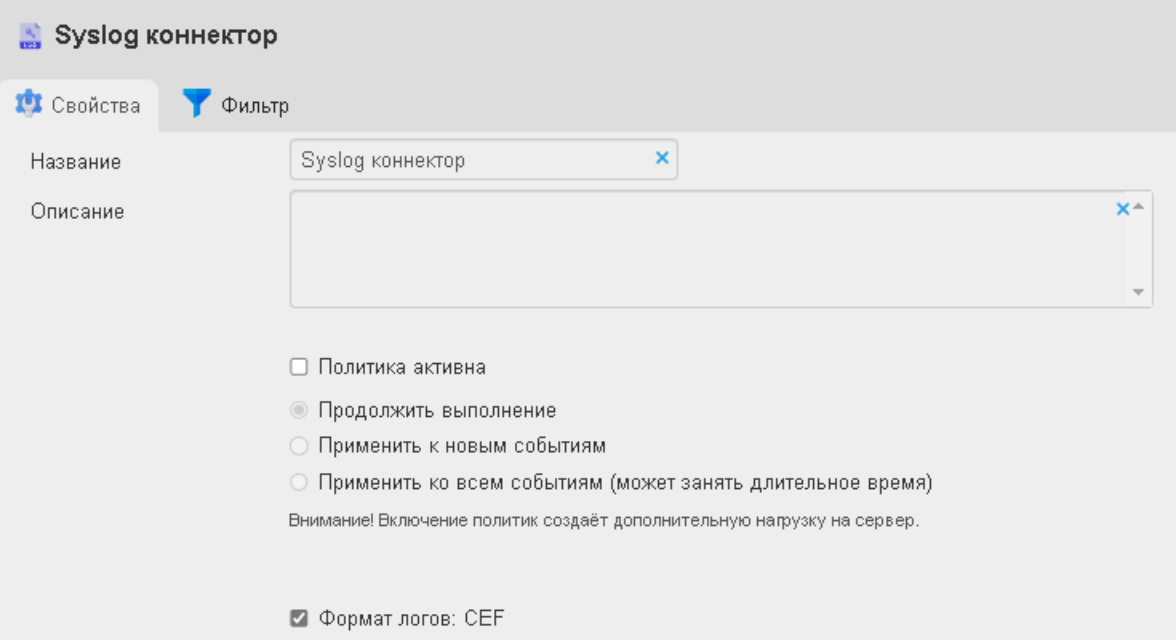
```
ibatyr update_models_from_csv путь_к_csv --search-key mail=1 --map англ_имя_кастомного_
↪поля_ Подразделение1=2 --no-dry-run
```

4.5.25 Syslog коннектор

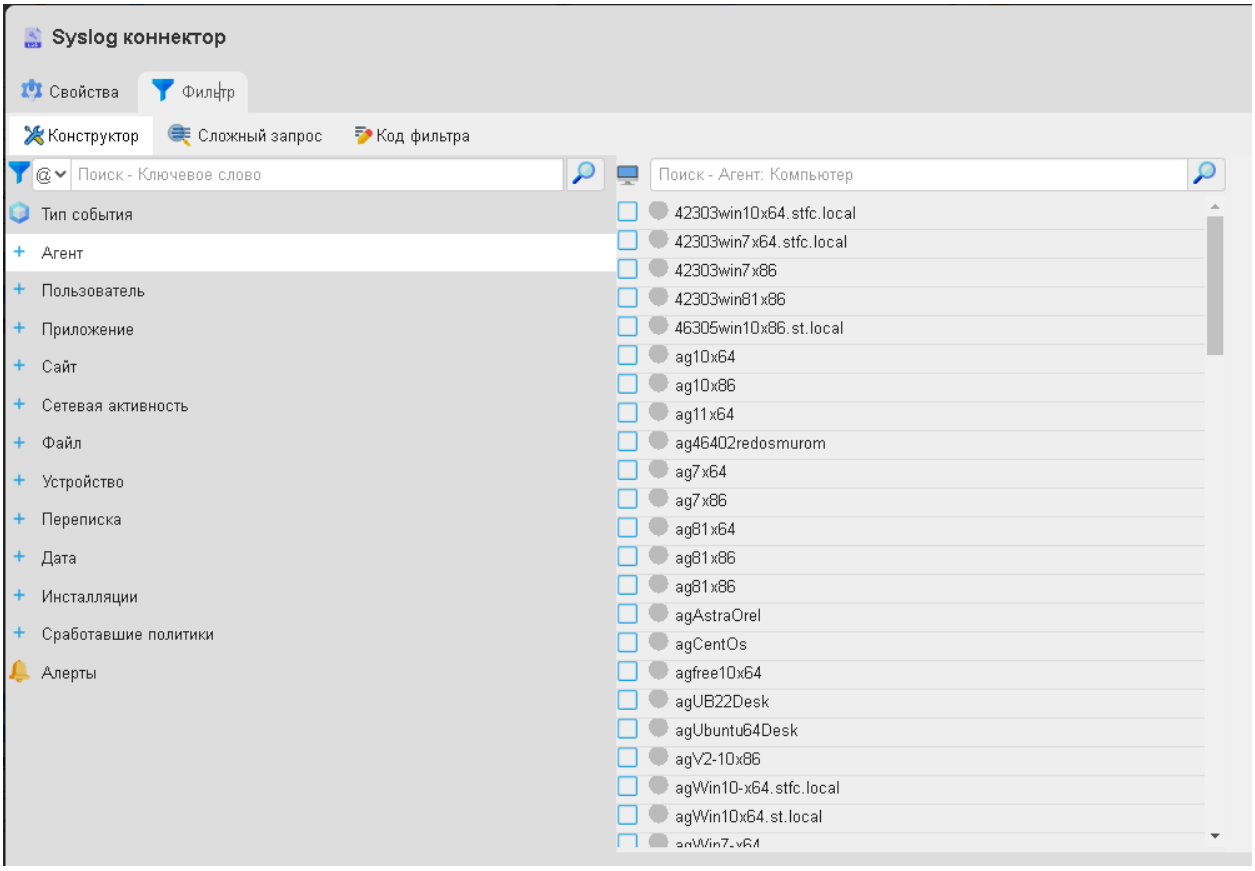
Syslog-коннектор – системная политика, позволяющая выводить информацию в системный журнал **/var/log/syslog**. Политика может быть полезна для выгрузки и интеграции с SIEM- или BI-системой для анализа накопленных в iBatyr Monitor данных.

Политика **Syslog коннектор** расположена в разделе **Политики** в папке **Политики – Системные политики**. По умолчанию политика выключена.

Чтобы включить политику **Syslog-коннектор**, зайдите в её свойства и установите галочку в разделе **Политика активна**.



На вкладке **Фильтр** настройте данные, которые будут передаваться в syslog-файл.



После этого один раз в 5 минут в файл **/var/log/syslog** будут помещаться события вида:

```
support@ubuntu:~$ grep -i ibatyr /var/log/syslog
```

(continues on next page)

(продолжение с предыдущей страницы)

```
Jan 29 12:53:44 ubuntu ibatyr: time="Jan 29 09:53:09" event="InterceptedFile" computer=
↪"NB0202" user="user" app="None" data="Clipboard.png"
Jan 29 12:57:52 ubuntu ibatyr: time="Jan 29 09:57:28" event="InterceptedFile" computer=
↪"NB0202" user="user" app="snippingtool.exe" data="Clipboard.png"
Jan 29 12:57:52 ubuntu ibatyr: time="Jan 29 09:57:26" event="InterceptedFile" computer=
↪"NB0202" user="user" app="snippingtool.exe" data="Clipboard.png"
Jan 29 12:59:38 ubuntu ibatyr: time="Jan 29 09:59:11" event="InterceptedFile" computer=
↪"NB0202" user="user" app="snippingtool.exe" data="Clipboard.png"
Jan 29 12:59:38 ubuntu ibatyr: time="Jan 29 09:59:10" event="InterceptedFile" computer=
↪"NB0202" user="user" app="snippingtool.exe" data="Clipboard.png"
Jan 29 12:59:38 ubuntu ibatyr: time="Jan 29 09:59:08" event="InterceptedFile" computer=
↪"NB0202" user="user" app="snippingtool.exe" data="Clipboard.png"
Jan 29 12:59:38 ubuntu ibatyr: time="Jan 29 09:59:06" event="InterceptedFile" computer=
↪"NB0202" user="user" app="snippingtool.exe" data="Clipboard.png"
Jan 29 12:59:38 ubuntu ibatyr: time="Jan 29 09:59:03" event="InterceptedFile" computer=
↪"NB0202" user="user" app="snippingtool.exe" data="Clipboard.png"
```

Появление таких событий означает, что политика **Syslog-коннектор** отработала нормально, и теперь эти данные можно *собирать с помощью SYSLOG-граббера от SIEM* или отправлять на удалённый rsyslog-сервер.

CEF-формат логов

Чтобы выгружать события в syslog-коннектор в формате CEF, на вкладке **Свойства** установите галочку в разделе **Формат логов: CEF**.

Данные загружаются в формате **CEF0**.

Примечание: Формат **CEF24** больше не поддерживается. Файлы будут загружаться в формате **CEF0**, даже если ранее вы указали другой формат в **etc/ibatyr/config**.

Формат **CEF0** использует пары ключ-значение для передачи информации о событиях. Эти пары определяют, какие данные и атрибуты включить в лог.

4.5.26 Организация совместной работы RuSIEM и iBatyr Monitor

Введение

RuSIEM – программный комплекс, представляющий собой SIEM-систему (Security Information and Event Management – информация о безопасности и управление событиями), предназначенную для сбора и анализа информации о событиях в информационной среде компании.

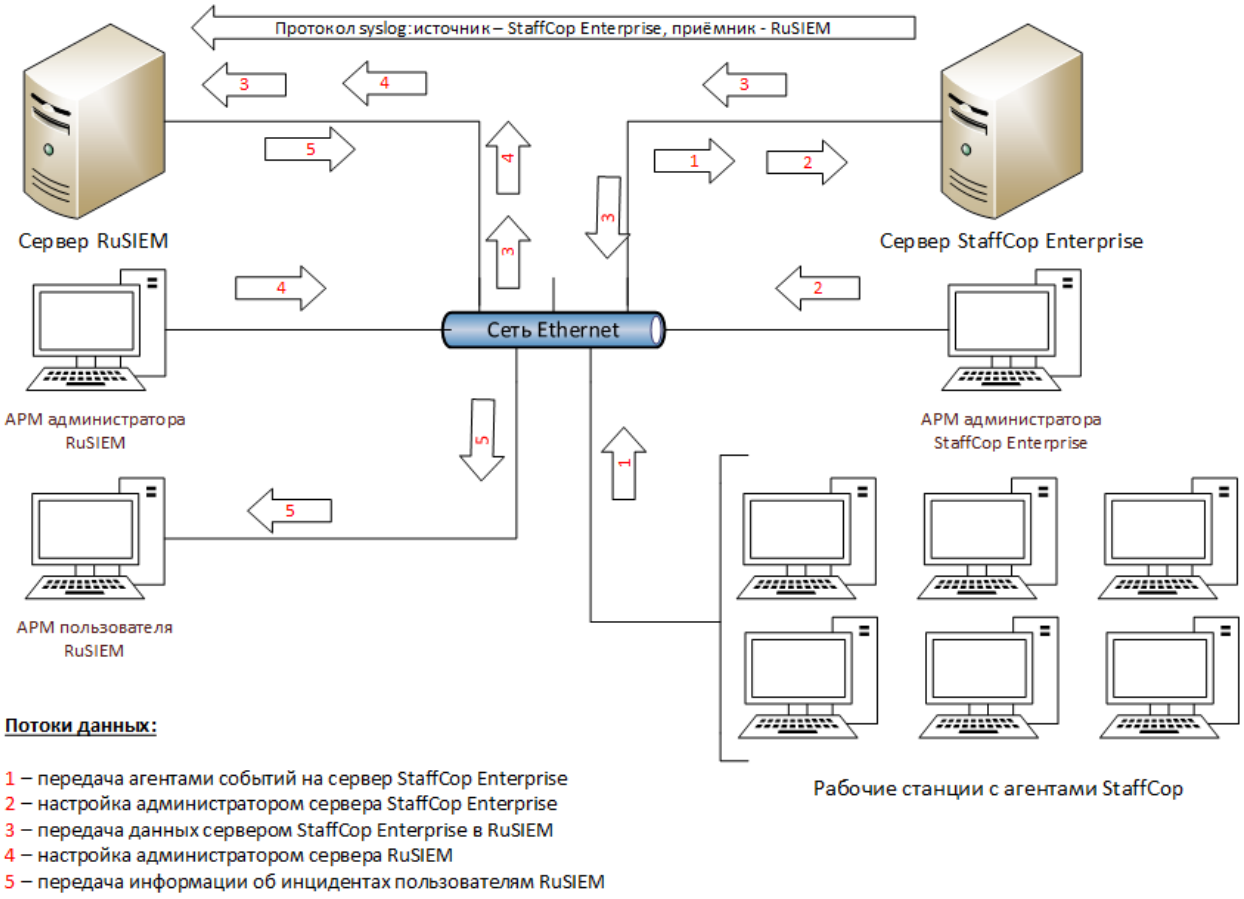
RuSIEM включает в себя различные модули – сбора и анализа информации, автоматического уведомления о событиях, которые классифицируются как инциденты, составления отчётов и т. д. Применение RuSIEM позволит автоматизировать комплексную обработку журналов различных программных комплексов, устройств безопасности и приложений и предоставить содержащиеся в них данные в виде наглядных отчётов, а также своевременно оповестить пользователей системы о произошедших событиях и инцидентах.

С помощью RuSIEM можно получить информацию об инцидентах, зарегистрированных в iBatyr Monitor и осуществить рассылку оповещений о них группам пользователей RuSIEM, но для этого

должно быть настроено взаимодействие (передача информации о событиях и инцидентах) между iBatyr Monitor и RuSIEM.

Схема организации передачи информации из iBatyr Monitor в RuSIEM

В самых общих чертах схема передачи информации из iBatyr Monitor в RuSIEM может быть представлена следующей схемой:



Сервер iBatyr Monitor по протоколу syslog передаёт информацию о событиях и инцидентах, собранных агентами iBatyr Monitor, на сервер RuSIEM, и пользователи RuSIEM получают уведомления об этих инцидентах в автоматическом режиме.

Администратор системы RuSIEM должен выполнить настройку сервера RuSIEM, администратор сервера iBatyr Monitor - настройку сервера iBatyr Monitor .

Настройка сервера iBatyr Monitor для передачи информации в RuSIEM

Предполагается, что сервер iBatyr Monitor уже развёрнут в системе, на нём созданы группы пользователей. Сервер функционирует в полном объёме, соответствующие политики для поиска инцидентов настроены. Рассмотрим на примере с следующими параметрами для подключения к серверу iBatyr Monitor :

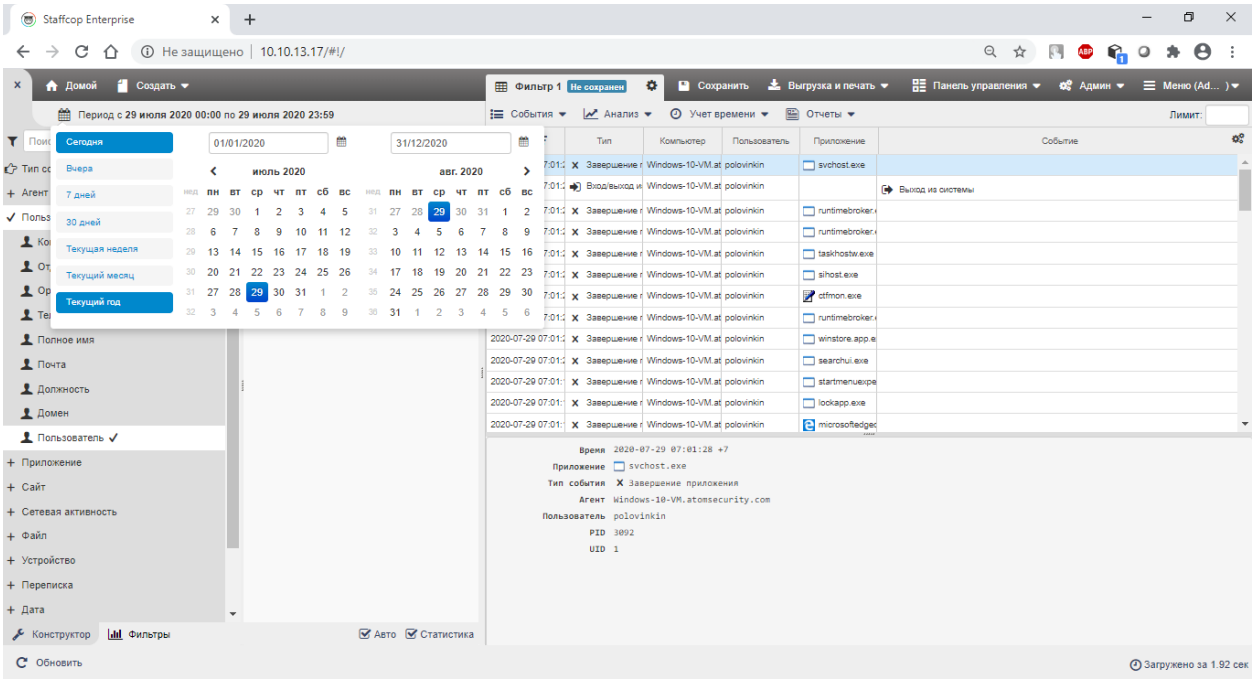
- IPv4-адрес для подключения по протоколу ssh – 10.10.13.17
- веб-интерфейс — http://10.10.13.17
- логины – support для подключения по протоколу ssh и admin для веб-интерфейса
- пароли – известны администратору
- порт, используемый для подключения к серверу RuSIEM – 5014

В начале необходимо включить системную политику *Syslog-коннектор*.

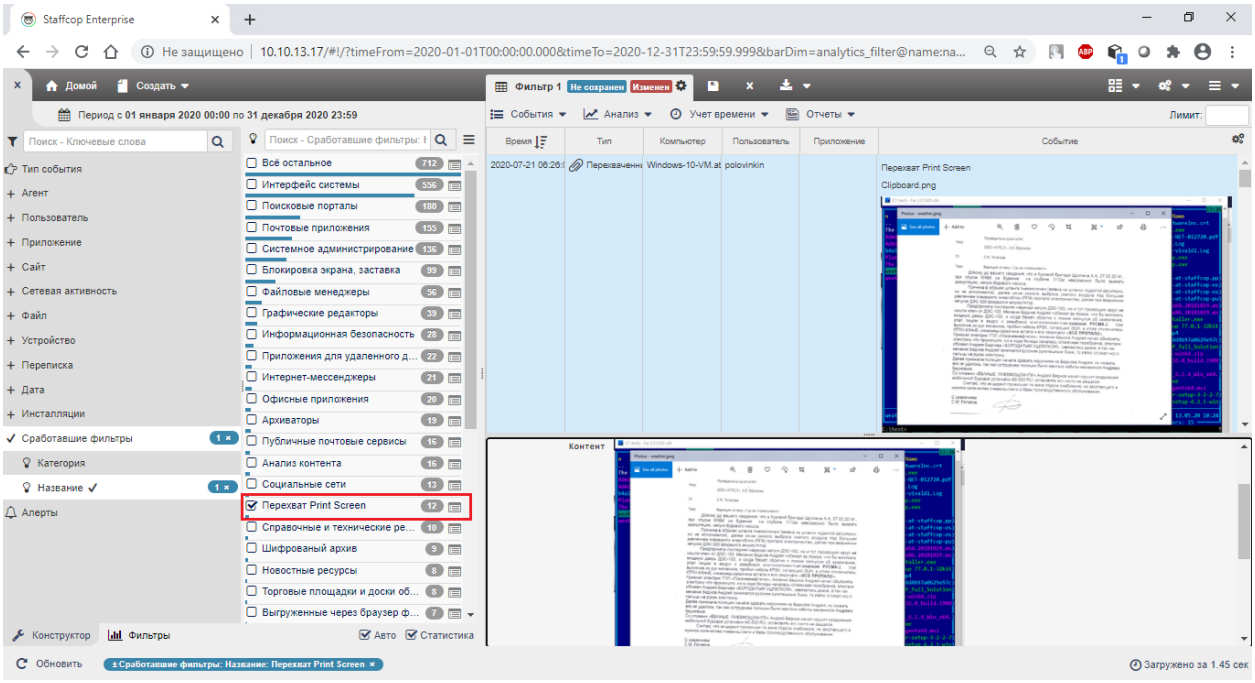
Для примера будем выполнять настройку сообщения об инциденте «Выполнение PrintScreen» - будем считать, что в организации выполнение PrintScreen (сохранение в буфер копии экрана для дальнейшего использования) считается инцидентом.

Зайдём в веб-интерфейс управления сервером iBatyr Monitor через браузер (рекомендуется использовать Google Chrrome), введём логин, пароль и нажмём кнопку «Войти». Откроется веб-интерфейс сервера iBatyr Monitor :

Далее убедимся, что события PrintScreen агентами iBatyr Monitor были зарегистрированы ранее (а значит, можно предполагать, что они будут и в будущем). Выберем период «Текущий год»:

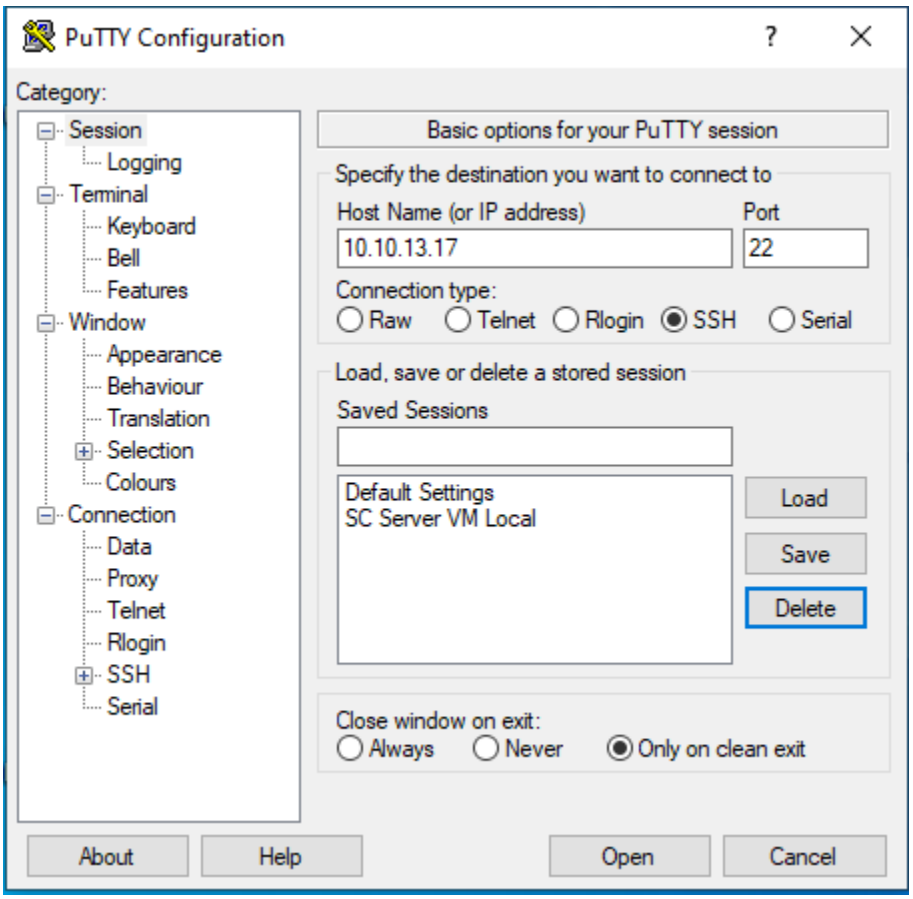


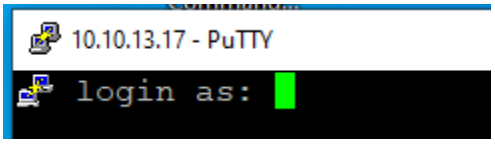
После отображения событий за год во вкладке «Конструктор» выберем измерение «Сработавшие политики», а в нём – фильтр по событиям «Перехват PrintScreen». Убеждаемся, что события были, для чего во вкладке «Конструктор» переместимся вниз, до ссылки «Сработавшие политики», и выберем фильтр «Перехват PrintScreen» (выделено красной рамкой):



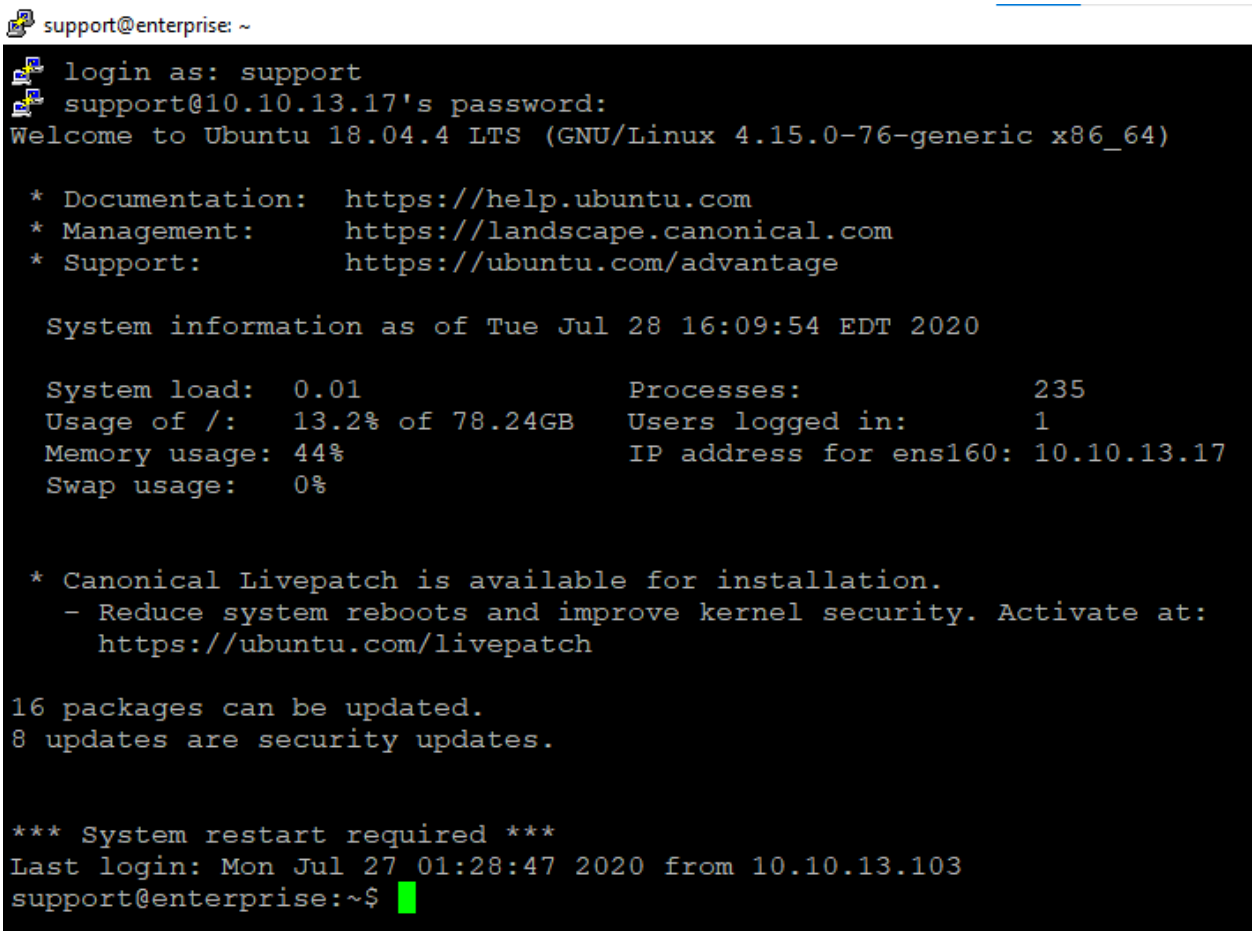
События действительно были, это видно в правой части окна браузера.

Теперь можно переходить к настройке сервера для передачи информации о событиях в RuSIEM. Подключимся к серверу по ssh-протоколу, например, с помощью приложения PuTTY (IPv4-адрес сервера, логин и пароль нам известны заранее, показаны только актуальные фрагменты скриншотов):



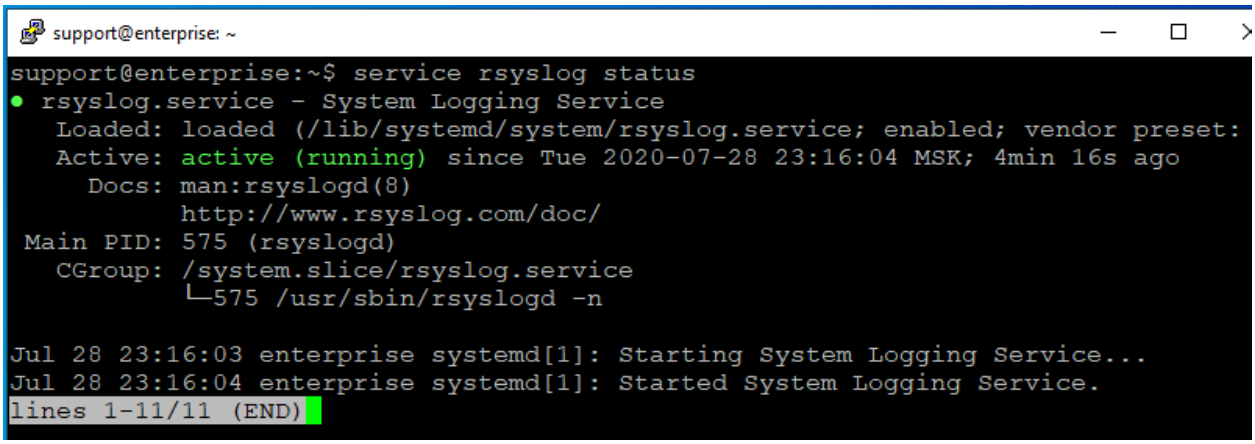


После ввода логина и пароля откроется интерфейс командной строки сервера iBatyr Monitor .



Передача информации на сервер RuSIEM выполняется сервисом rsyslog. Нужно убедиться, что сервис установлен и запущен (активен). Это делается с помощью команды:

```
service rsyslog status
```



Вывод может отличаться от показанного на скриншоте, главное, чтобы сервис был установлен и запущен: это отображено строкой «active: running» зелёного цвета в выводе результатов работы команды. Далее нажатием комбинации клавиш **Ctrl-C** сервер вернётся к приглашению командной строки. Если сообщения о работающем сервисе («active: running» зелёного цвета) в выводе команды нет (что является не нормальным – это системный сервис, и на сервере iBatyr Monitor Enterprise он должен работать

«из коробки»), попробуйте запустить сервис командой:

```
sudo service rsyslog start
```

После чего повторно запросить состояние сервиса. Если сервис так и не заработал, единственный выход – обратиться к Вашему системному администратору Linux.

Дальше с помощью редактора nano создадим конфигурационный файл /etc/rsyslog.d/50-siem.conf от имени суперпользователя (root). Делается это командой:

```
sudo nano /etc/rsyslog.d/50-siem.conf
```

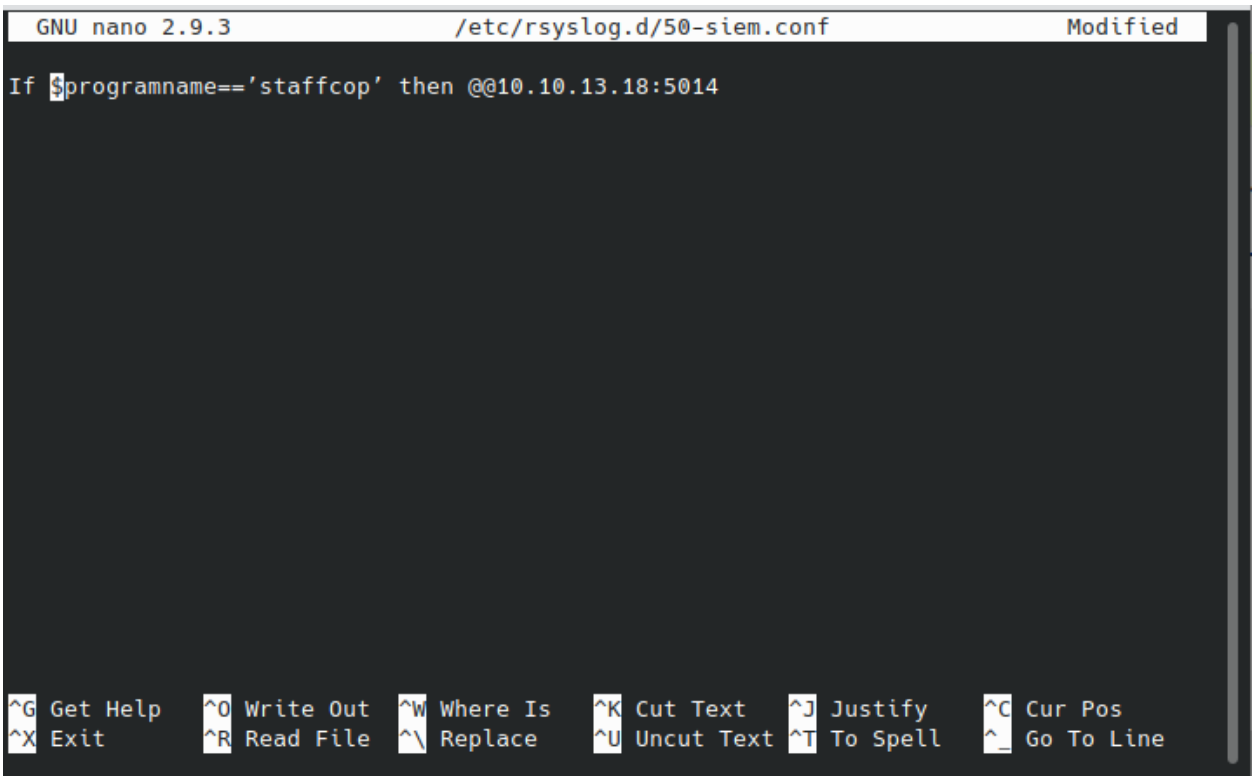
После ввода пароля пользователя support откроется окно редактора nano с пустым файлом (это покажет надпись «New File» над строками подсказки команд редактора). В этот файл нужно добавить две строки:

```
$RepeatedMsgReduction off
If $programname=='ibatyr' then @@10.10.13.18:5014
```

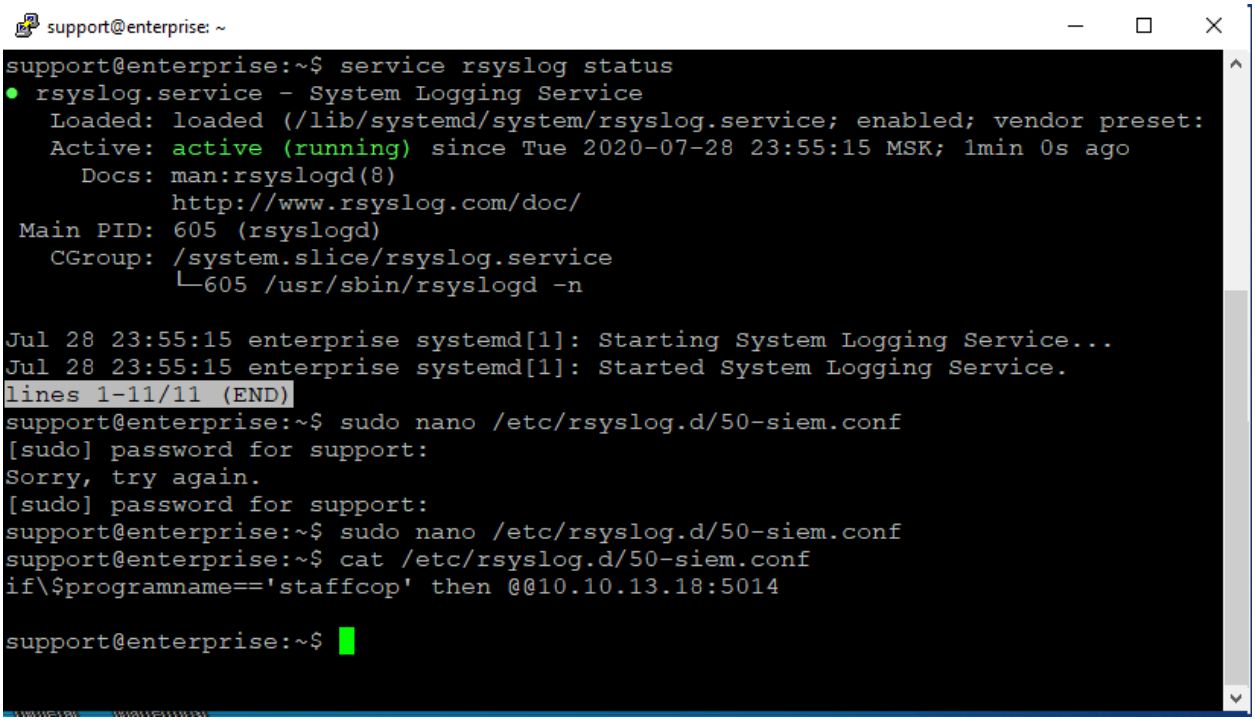
Если вы используете две или более RuSIEM системы, конфигурация со списком серверов должна быть построчной:

```
$RepeatedMsgReduction off
If $programname=='ibatyr' then @@10.10.10.19:518
If $programname=='ibatyr' then @@10.18.10.12:514
```

Адрес сервера указан для примера. Замените его на адрес Вашего RuSIEM-сервера и добавить пустую строку:



после чего нажать клавиши **Ctrl-X, Y** и **Enter**. Сервер выдаст приглашение командной строки. Командой **cat /etc/rsyslog.d/50-siem.conf** нужно убедиться, что файл содержит введённую строку:



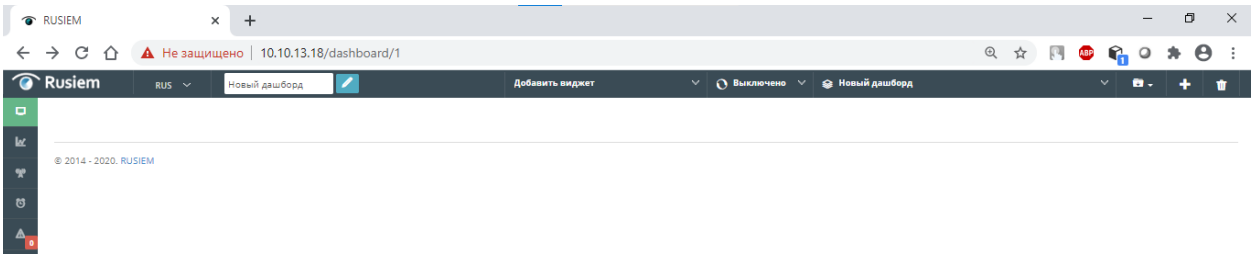
После этого необходимо перезапустить сервис rsyslog командой:

```
sudo service rsyslog restart
```

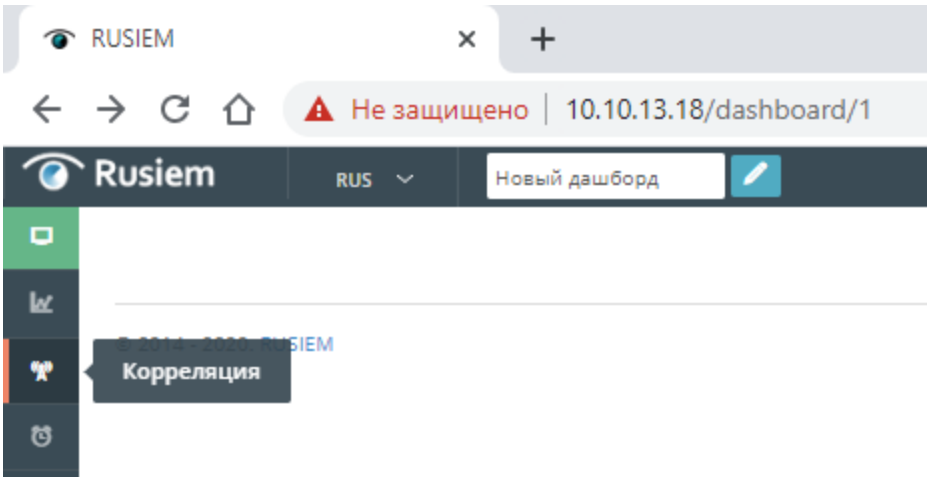
Если команда не выведет ничего и сервер выдаст приглашение командной строки, значит, всё настроено правильно и можно переходить к настройке сервера RuSIEM для приёма информации, передаваемой сервером iBatyr Monitor . Настройка сервера RuSIEM для получения информации с сервера iBatyr Monitor Предполагается, что сервер RuSIEM уже развёрнут в системе, на нём созданы группы пользователей. Сервер функционирует в полном объёме. Параметры для подключения к нему следующие:

- веб-интерфейс – https://10.10.13.18
- логин – admin
- пароль – известен администратору.

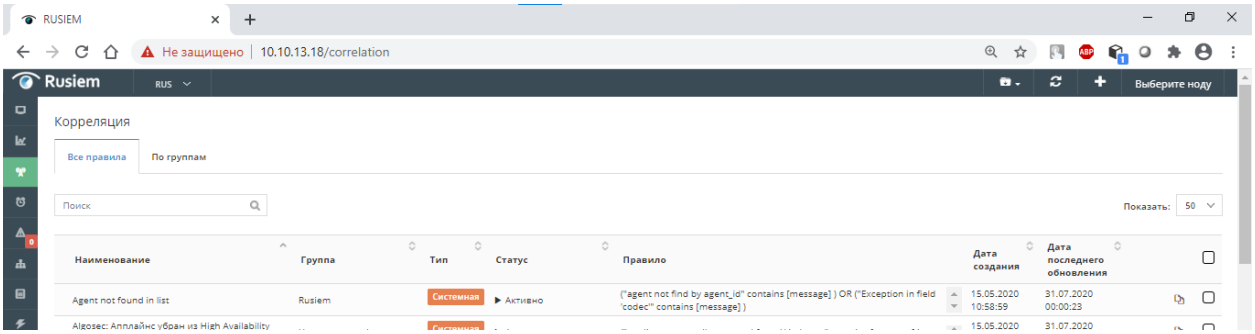
Настройка взаимодействия со iBatyr Monitor выполняется из веб-интерфейса RuSIEM. Подключимся к серверу RuSIEM с помощью браузера Google Chrome по протоколу https, будет отображено окно входа в систему. После ввода известных нам логина и пароля, и нажатия кнопки «Войти» откроется окно интерфейса программного комплекса RuSIEM (по умолчанию – открывается пустой рабочий стол, показана часть экрана):



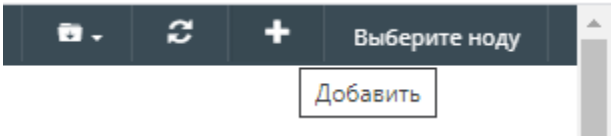
Настройка правил извещения об инцидентах, собранных программным комплексом iBatyr Monitor , производится в панели «Корреляция» (третья сверху кнопка в левой панели инструментов, если навести на неё курсор мыши – всплывёт подсказка, показана часть экрана):



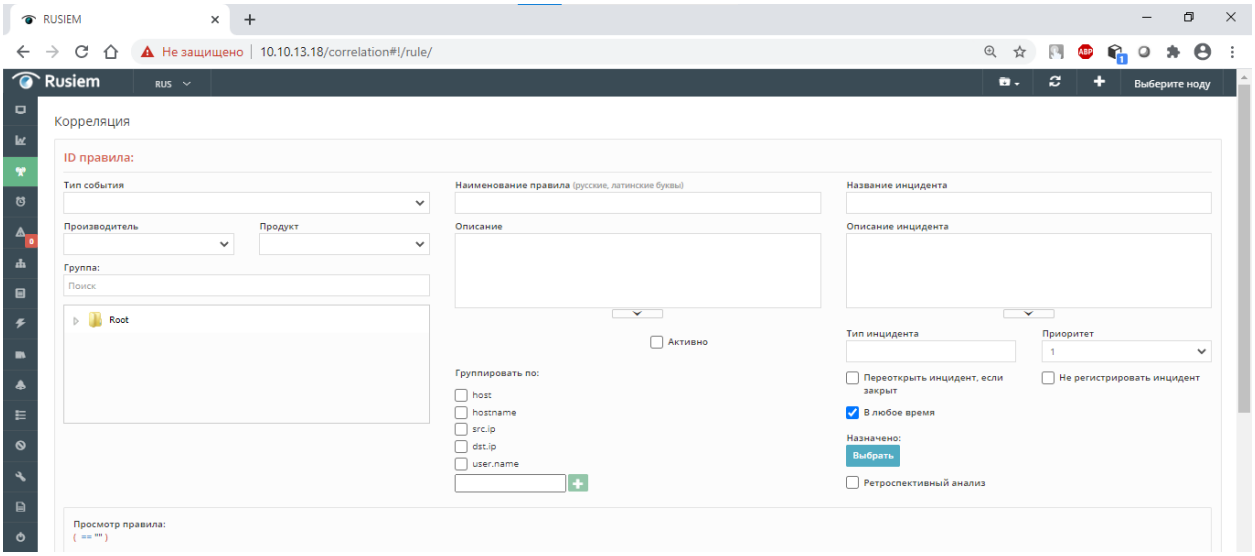
При нажатии на эту кнопку будет открыта панель правил корреляции и отображён список уже имеющихся корреляций (показана часть экрана):



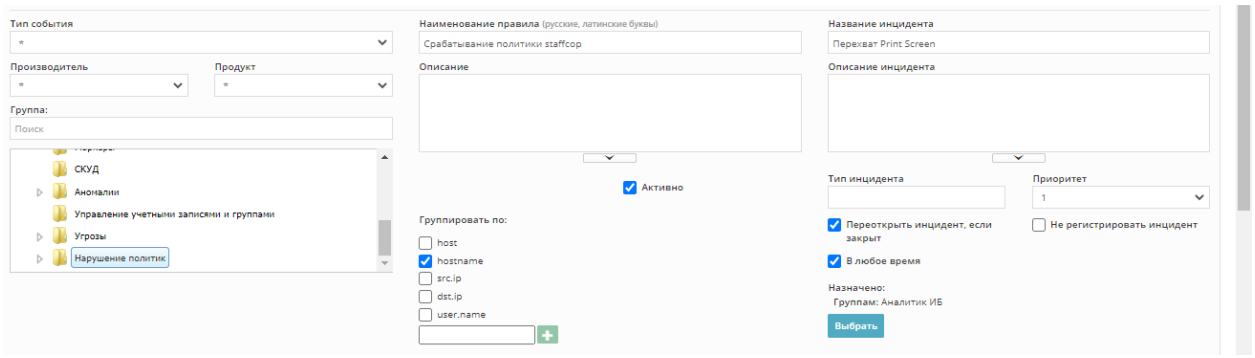
Нужно добавить новую корреляцию, соответствующую получению информации о событии «Выполнение операции «Print Screen», зафиксированной агентом iBatyr Monitor. Для этого нужно нажать кнопку добавления корреляции «+» в панели инструментов (слева от словосочетания «Выберите ноду»).



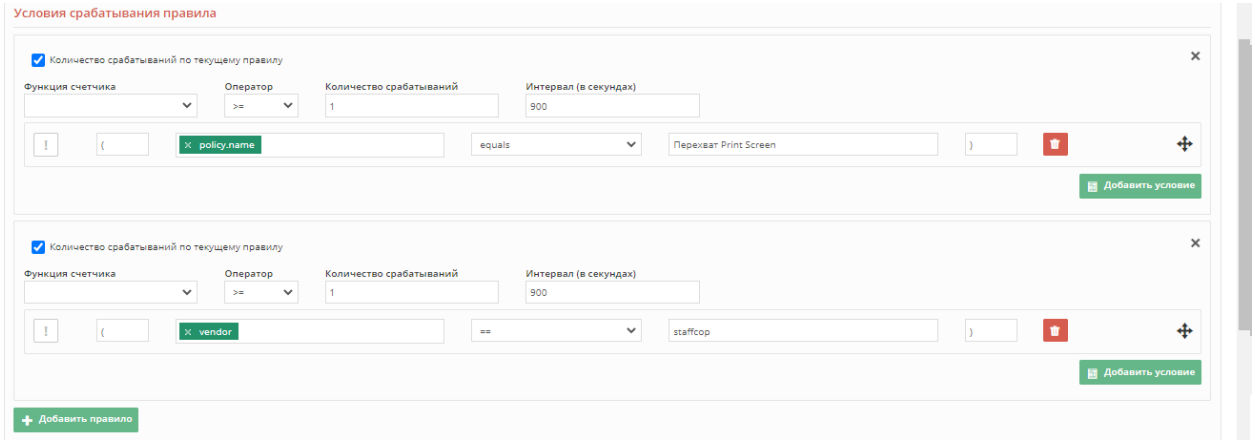
Откроется панель добавления новой корреляции (показана часть экрана):



Нужно заполнить поля в этом разделе следующим образом (показана часть экрана):

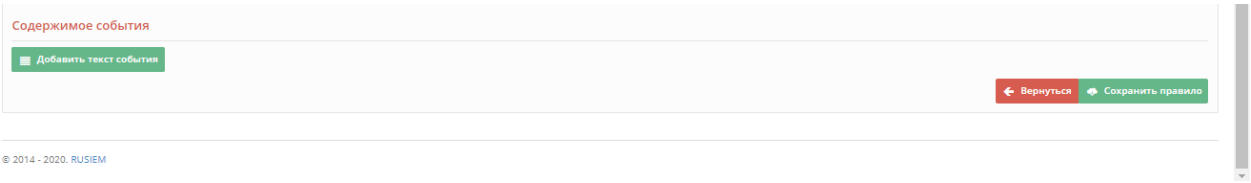


Далее нужно прокрутить панель создания правила корреляции вниз и сформировать правила срабатывания корреляции. Имя политики (поле policy.name) должно быть эквивалентно (equals) названию сработавшей политики в iBatyr Monitor («Перехват Print Screen»), а значение поля vendor равняться строке “ibatyr”. Поскольку в одном условии два значения задать нельзя, нужно будет задать два правила (показана часть экрана):

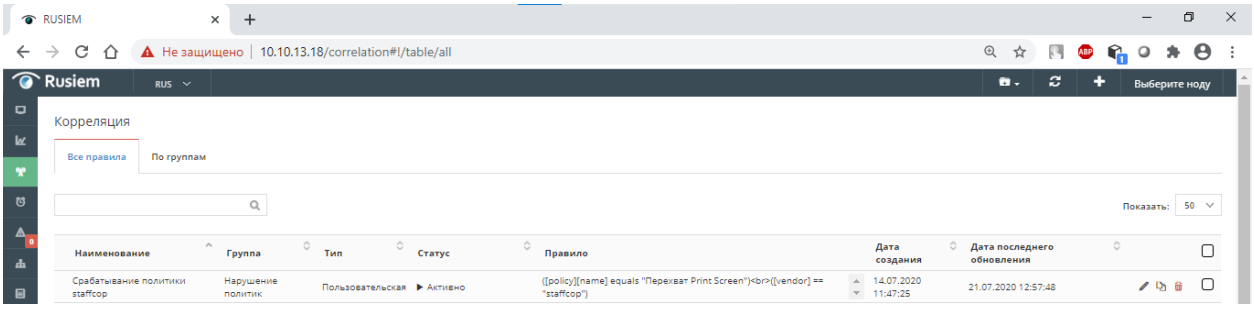


Можно также добавить одно или несколько дополнительных уведомлений о срабатывании правила (показана часть экрана):

И описать содержимое события (показана часть экрана):



После того, как правила созданы, нужно сохранить правило корреляции, нажав кнопку «Сохранить правило» (в самом низу панели, зелёного цвета, показана на предыдущей иллюстрации). В панели корреляций будет отображено правило, созданное нами (показана часть экрана):



Теперь у пользователей группы «Нарушение политик» будут создаваться инциденты каждый раз, когда будет срабатывать политика «Перехват Print Screen» в iBatyr Monitor .

4.5.27 Интеграция iBatyr Monitor с Komrad SIEM

KOMRAD SIEM — система для централизованного сбора событий информационной безопасности. Позволяет оперативно выявлять инциденты информационной безопасности и реагировать на них.

Чтобы настроить передачу событий из iBatyr Monitor в Komrad SIEM:

1. Установите и подготовьте к работе Komrad SIEM.
2. На сервере iBatyr Monitor активируйте политику *Syslog-коннектор*.
3. Внесите изменения в конфигурационный файл **/etc/rsyslog.conf**:

   3.1 Откройте конфигурационный файл:

   ```
   sudo nano /etc/rsyslog.conf
   ```

   3.2 В конец файла добавьте строку

   ```
   *.* action(type="omfwd" target="<1>" port="<2>" protocol="<3>" action.
   ↪resumeRetryCount="<4>" queue.type="<5>" queue.size="<6>")
   ```

   Здесь <**1**> — IP-адрес хоста с Syslog-коллектором, на который нужно посылать события; <**2**> — номер порта хоста с коллектором; <**3**> — протокол (tcp или udp); <**4**> — количество попыток передачи перед отбрасыванием сообщения (рекомендуем 100); <**5**> — тип очереди, которая будет использоваться (рекомендуем

LinkedList); <**6**> — максимальный размер очереди по количеству сообщений (рекомендуем **10000**).

4. Проверьте, что rsyslog запущен:

```
sudo systemctl status rsyslog
```

5. Выберите формат CEF0 для передачи логов. Для этого:

   5.1 Откройте конфигурационный файл: **/etc/ibatyr/config**.

   5.2 Добавьте строку **CEF_VERSION** = **'0'**.

   5.3 Если строка **CEF_VERSION** = уже существует, приведите её к вышеуказанному виду.

6. Проверьте поступление событий из iBatyr Monitor в Komrad.

4.5.28 Удаление данных по созданной политике или фильтру

Допустим, есть какая-то программа или что-то другое, что сгенерировало огромное количество событий или файлов, но эти данные для вас не несут пользы и требуется удалить их. Существует два способа удаления данных:

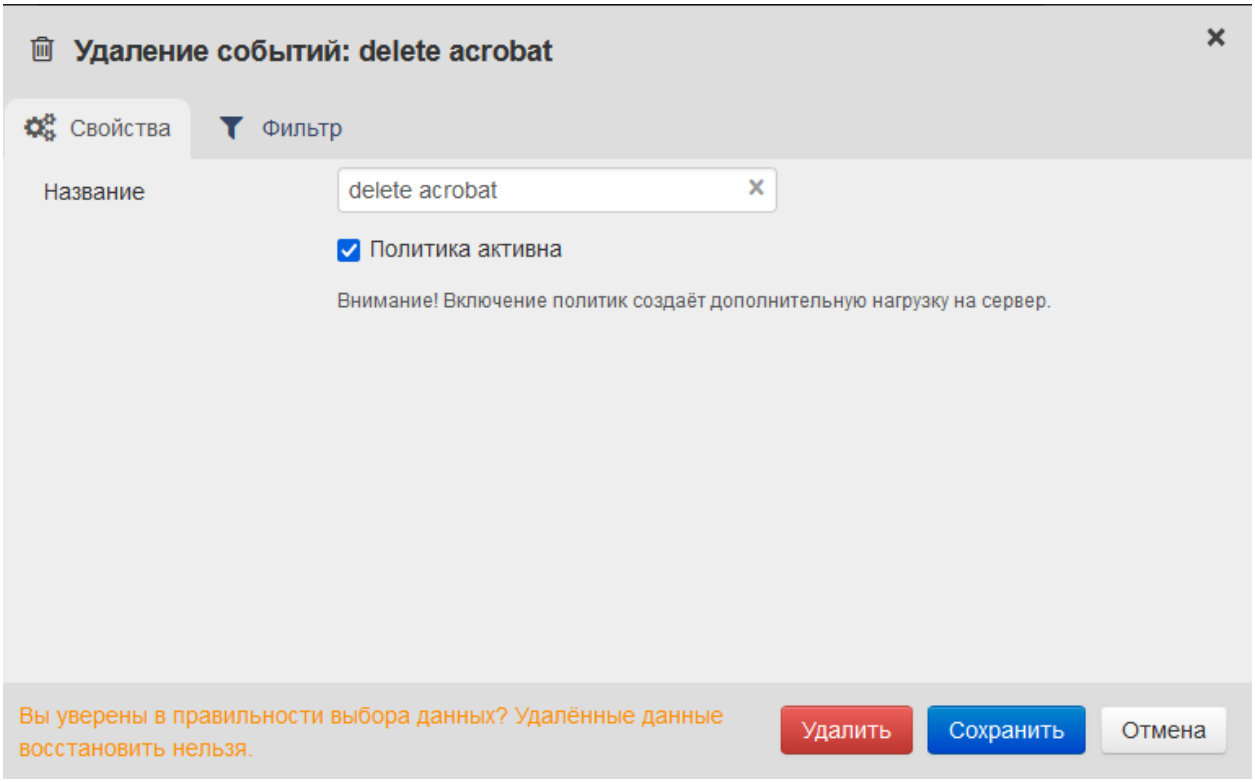
Политика удаления событий

С помощью данной политики возможно удалить события попадающие под критерии фильтра в заданном диапазоне времени (если указано). Удаление происходит не сразу, а в течение некоторого времени (зависит от кол-ва событий).

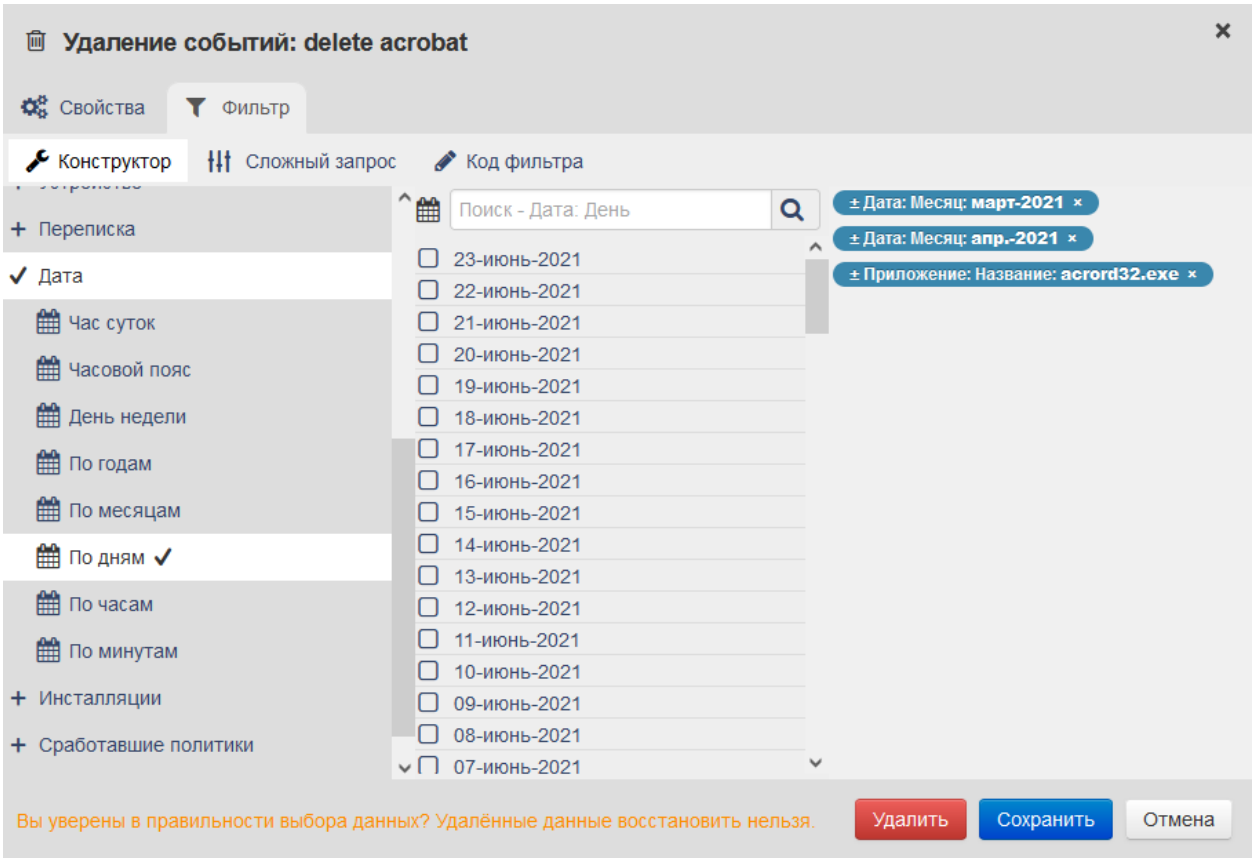
Примечание: Рекомендуем указывать период за который требуется удалить данные. В противном случае политика удалит все события включая новые. Удаляются события и связанные с ними файлы.

Пример работы

1. Создаем политику удаления событий и включаем ее нажав на «Политика активна».



2. Переходим во вкладку фильтр и выбираем нужные нам данные. В примере удаляем все событий для приложения acrord32.exe за апрель и май.



Удаления данных с использованием фильтра

Для удаления данных за определенный период используется команда:

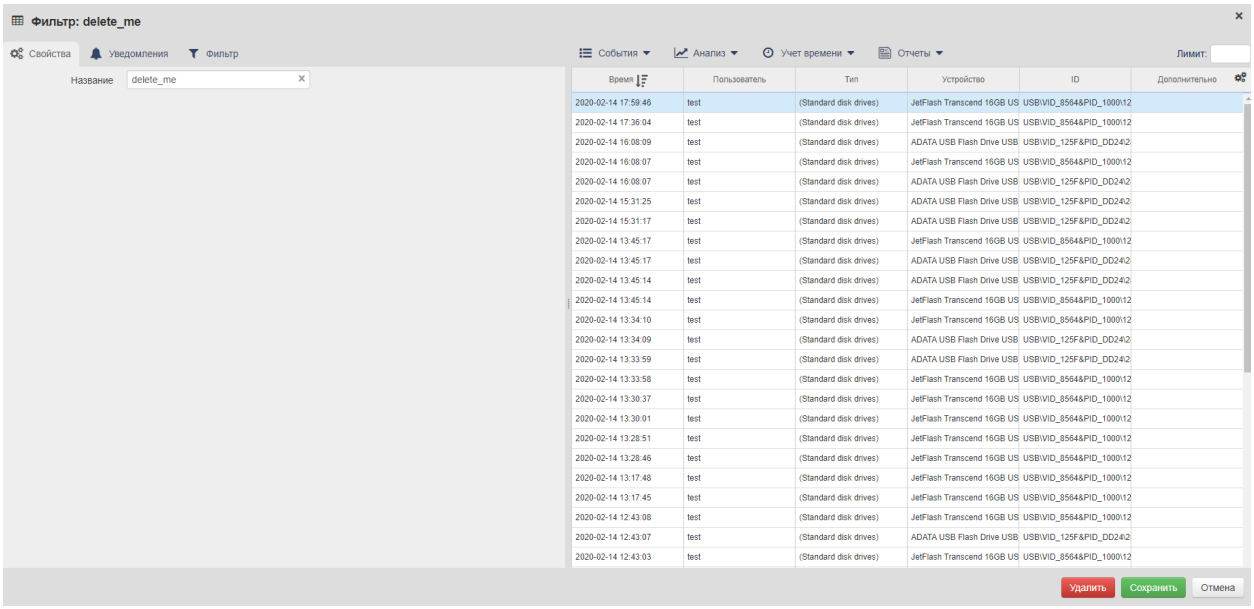
```
ibatyr delete-filter [--from=YYYY-MM-DD] [--to=YYYY-MM-DD] FILTER_NAME
```

Команда удаляет события попадающие под критерии фильтра «ИМЯ_ФИЛЬТРА» в заданном диапазоне времени (если указано).

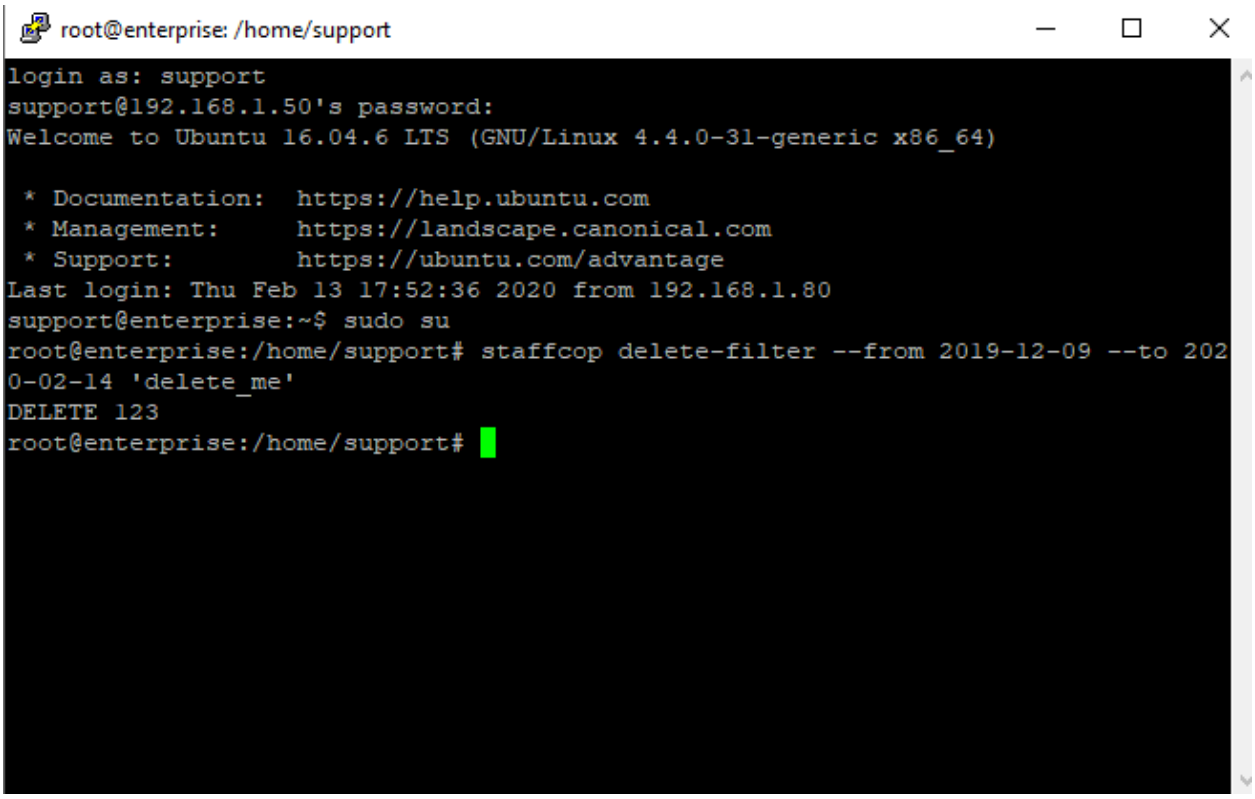
Примечание: Команда не сработает, если количество удаляемых событий больше 50000. В таком случае рекомендуется использовать политику удаления событий.

Пример работы

1. Создаем фильтр с данными для удаления



2. Удаляем все данные с 9 декабря по 13 февраля.

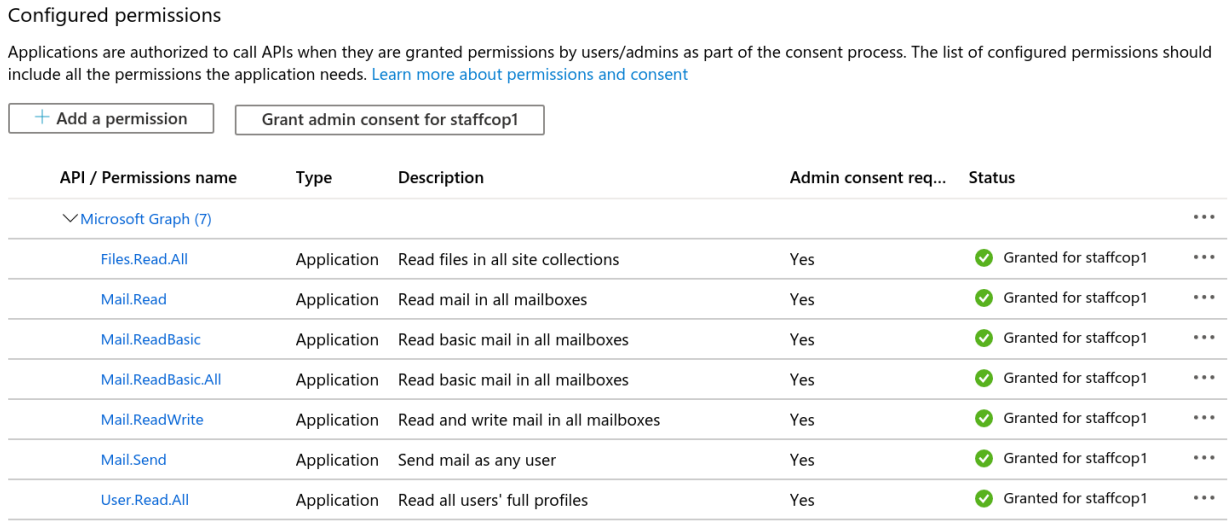


Было удалено 123 события из базы данных.

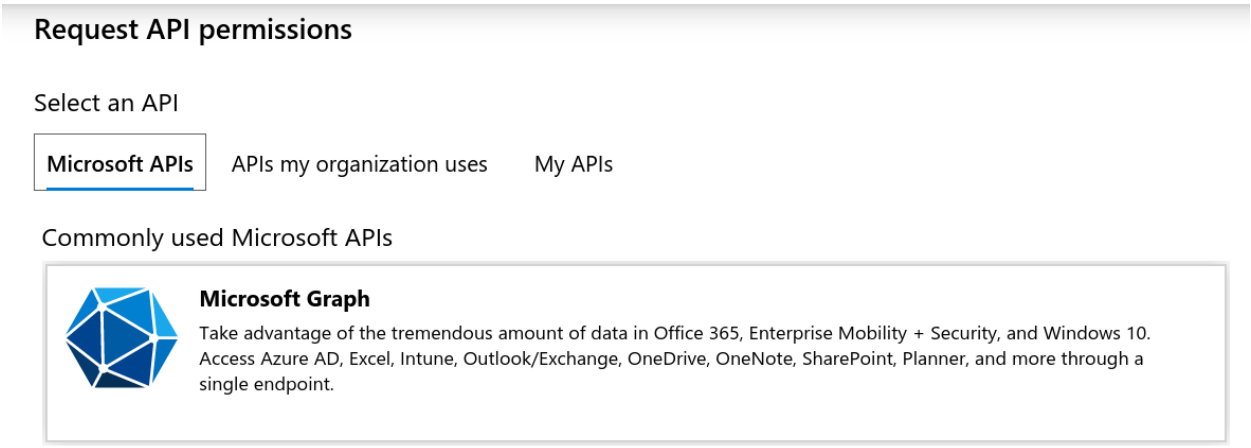
4.5.29 Настройка импорта писем и файлов из office 365

Предупреждение: Необходима PRO версия Office 365

1. В разделе App registrations создается новое приложение name = ibatyr, остальные пункты по умолчанию.
2. В настройках приложения в разделе API permissions добавляются следующие права доступа:



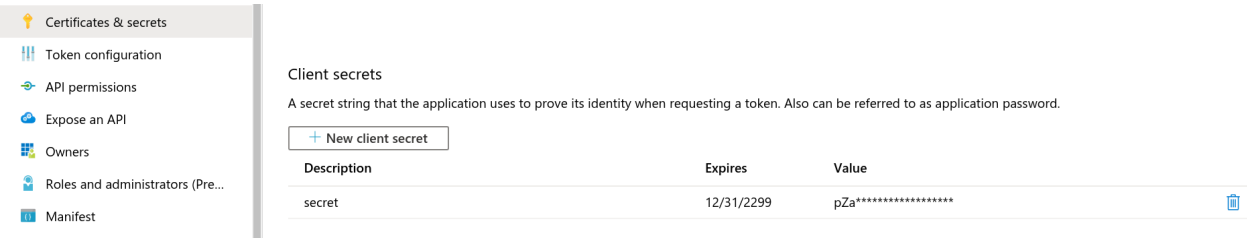
Права доступа добавляются из этого раздела:



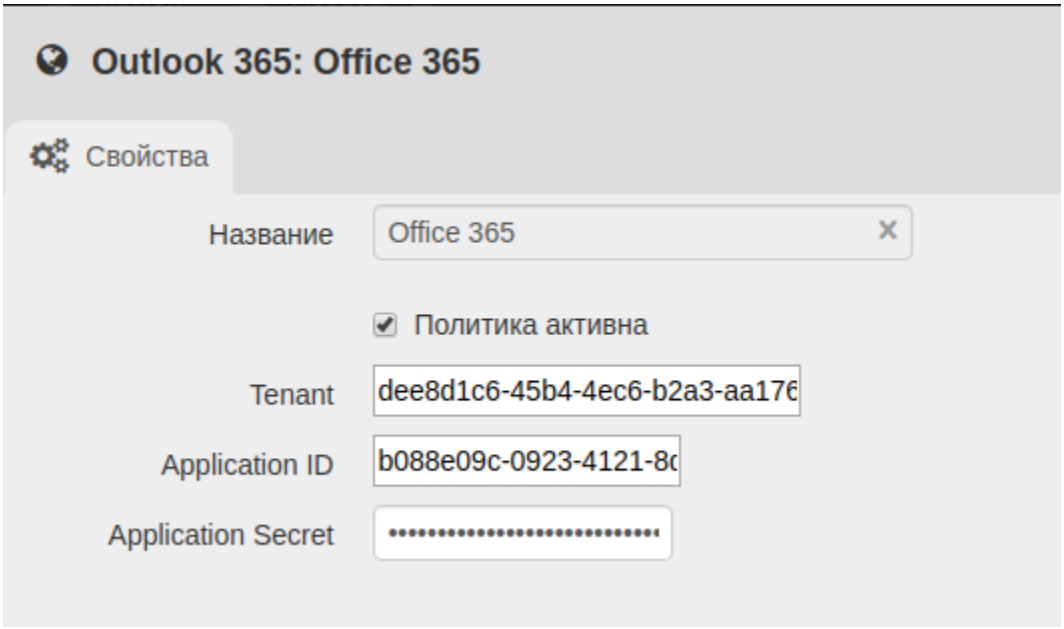
После добавления прав доступа обязательно следует добавить разрешение «Grant admin consent for . . . »

Примечание: Данная опция доступна только при работе под аккаунтом администратора AD

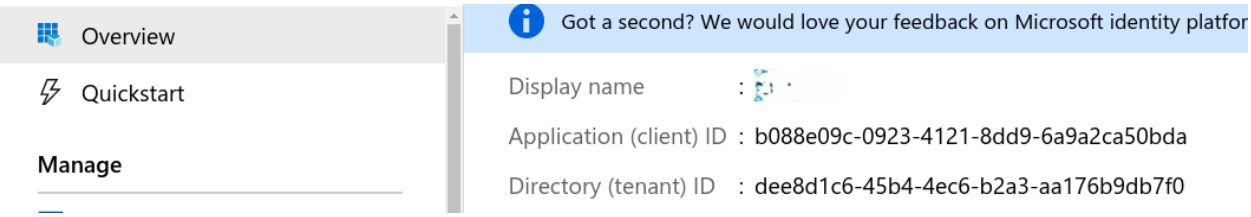
После этого необходимо создать ключ доступа приложения (secret)



Затем настройте политику iBatyr Monitor. **Фильтры** → **Политики** → **Системные политики** → **Office 365**.



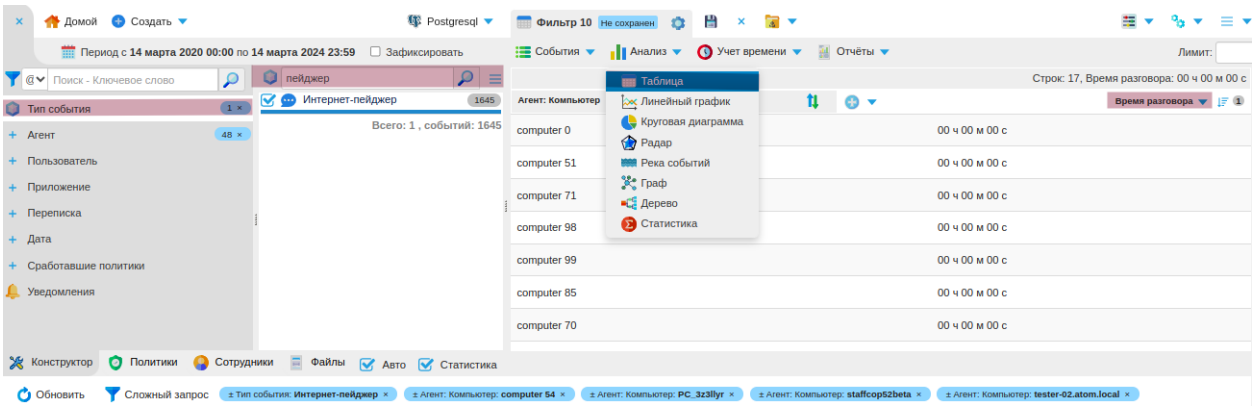
Tenant и Application ID берется отсюда:



После включения данной политики, сервер iBatyr Monitor начинает подтягивать все письма и файлы, созданные в облачной версии office 365

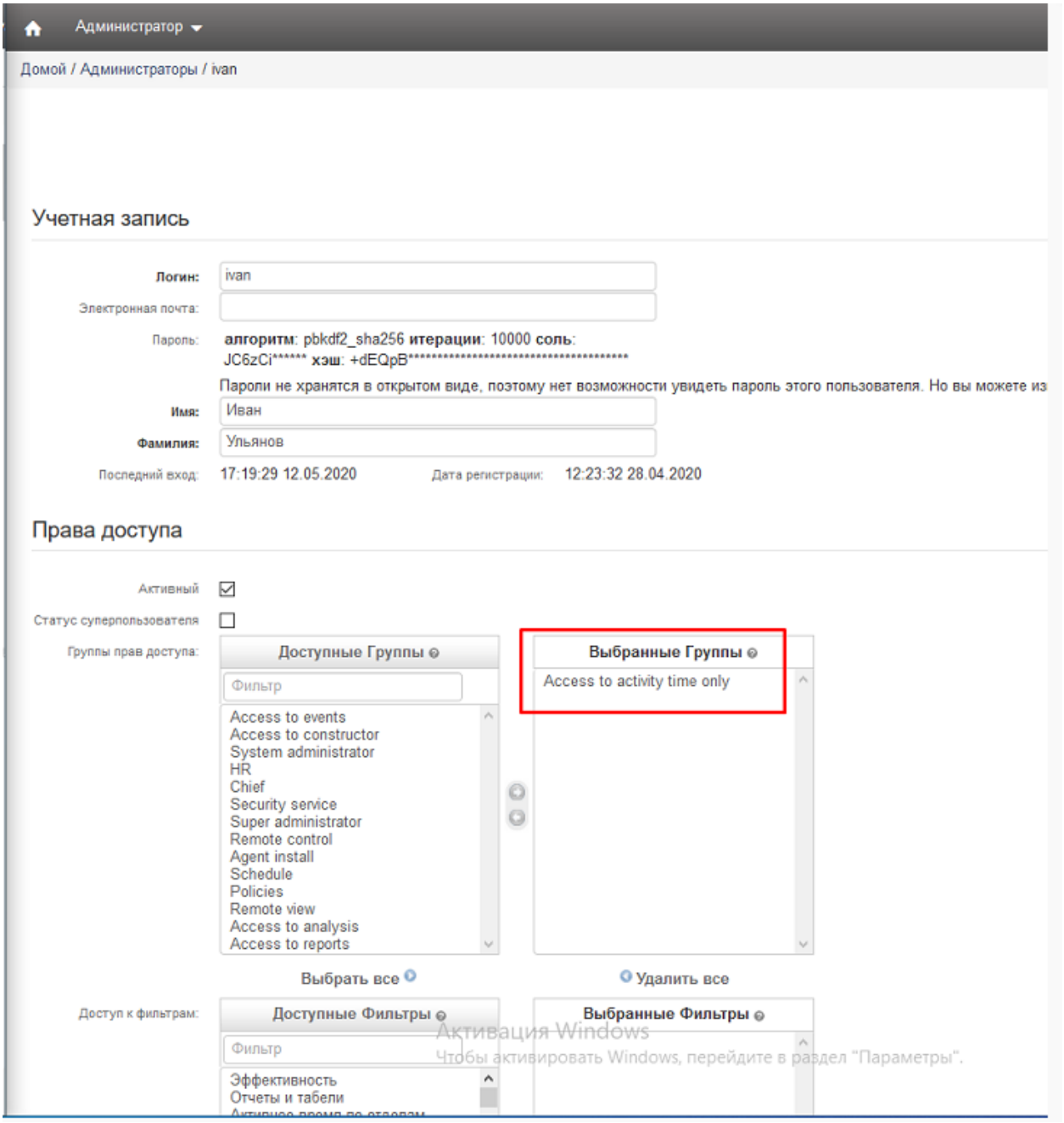
4.5.30 Построение отчета времени разговора в интернет-пейджере по сотрудникам

Для составления отчета выберите **Тип события** и найдите события типа **Интернет-пейджер**. Затем в **Конструкторе событий** в меню **Анализ** установите режим просмотра **Таблица** и выберите фильтрацию по времени разговора:

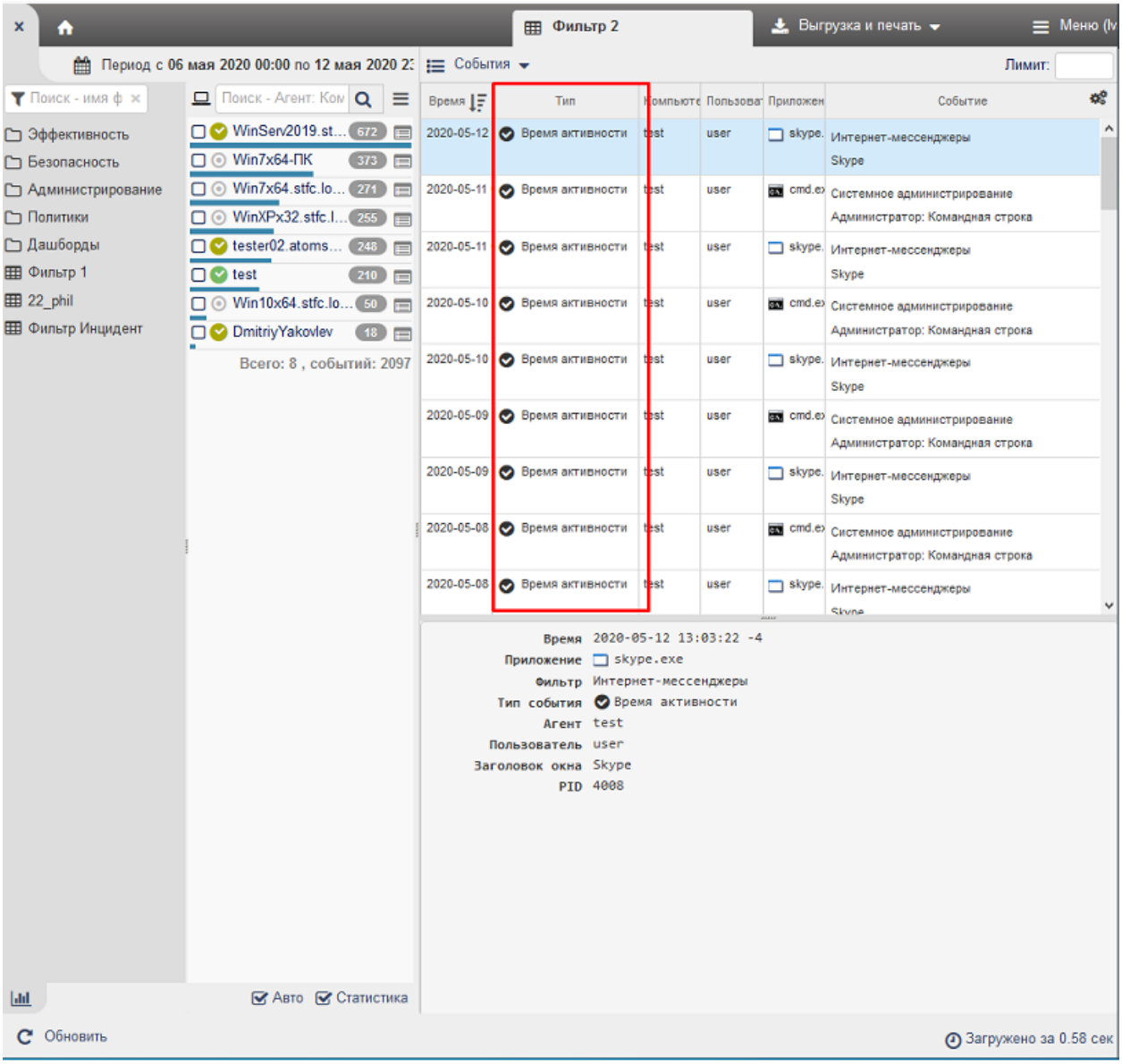


4.5.31 Настройка доступа только к событиям «время активности» и отчётам по УРВ.

Реализована специальная группа для раздачи прав доступа «Access to activity time only».



После раздачи добавления в указанную группу участник будет иметь доступ только к событиям «время активности» и отчётам по УРВ.



4.5.32 Кейсы по DLP модулю

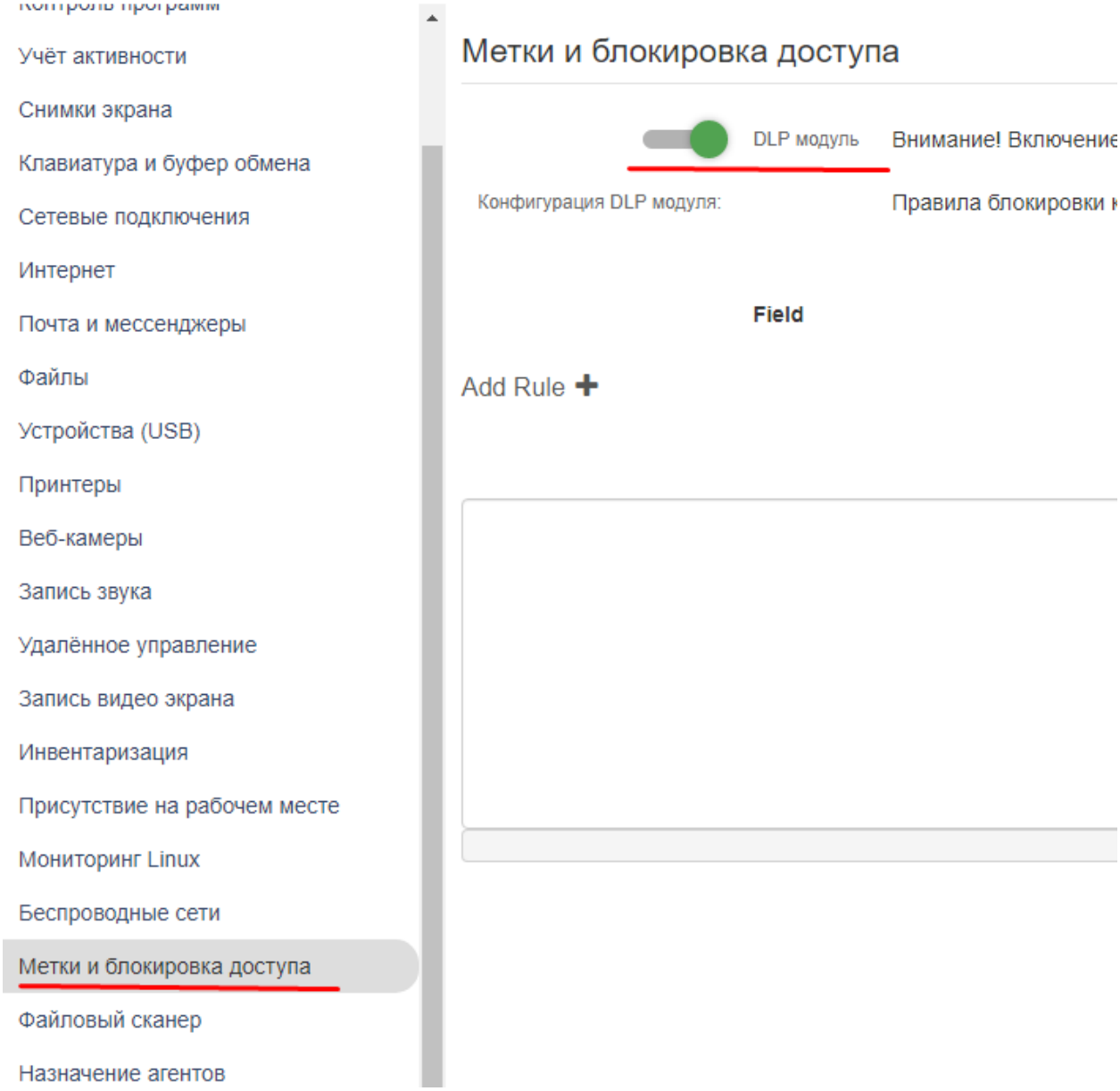
Содержание статьи:

- *Блокировка действий с файлами по атрибутам*;
- *Отслеживание «движения» файла в периметре организации*;
- *Доступ к данным только определённым сотрудникам*;
- *Запрет отправки файлов на флешку через RDP*;
- *Блокировать работу с файлом, если в нём содержится искомый текст.*

Блокировка действий с файлами по атрибутам

1. Активируем DLP модуль в конфигурации компьютеров.

Обращаю внимание, блокировка будет работать только на тех ПК где в конфигурации включен модуль.

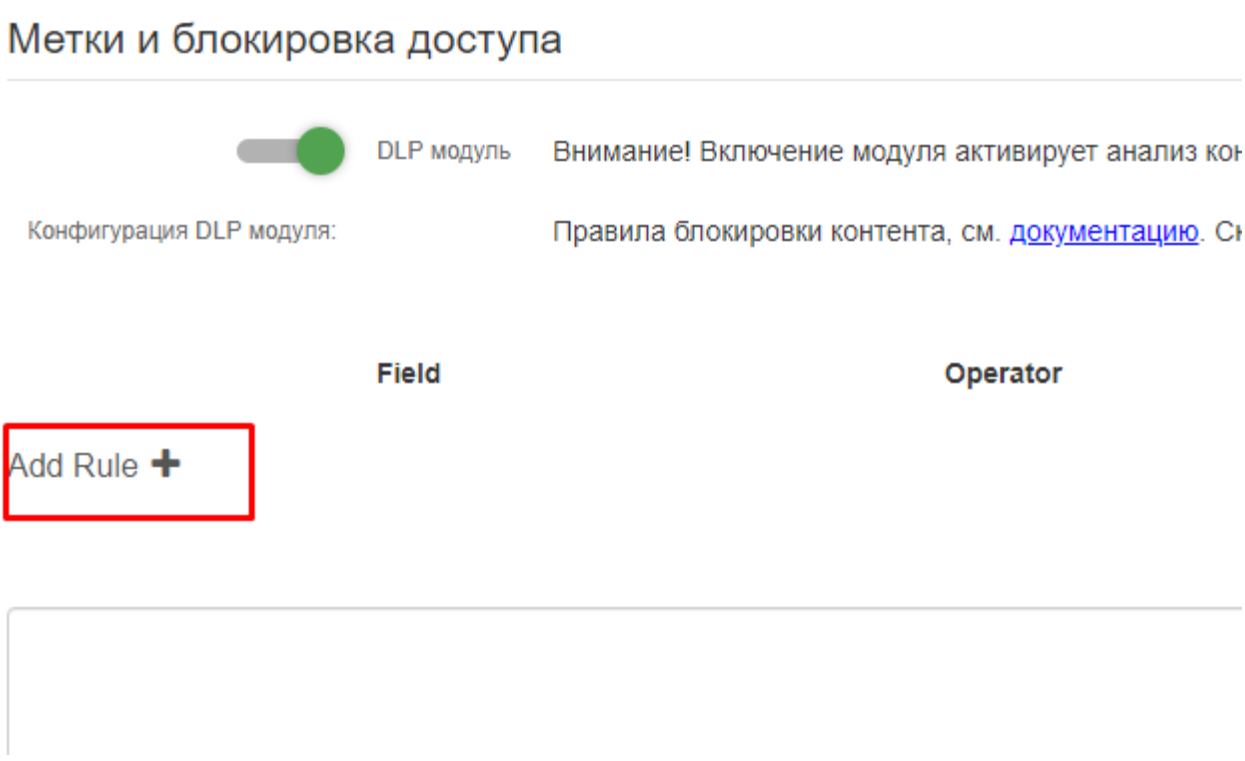


2. Создадим правило блокировки.

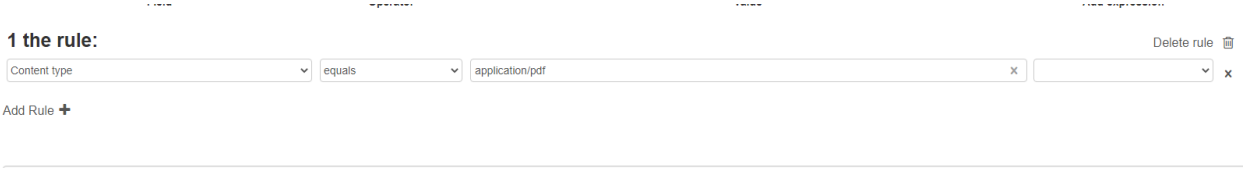
Для примера создадим правило, которое запрещает просмотр pdf файлов из любого приложения кроме AcrobatReader

---

Примечание: При составлении правила нужно помнить, что это правило блокировки, т.е. условия подразумевают запрет действий, когда правило истинно.



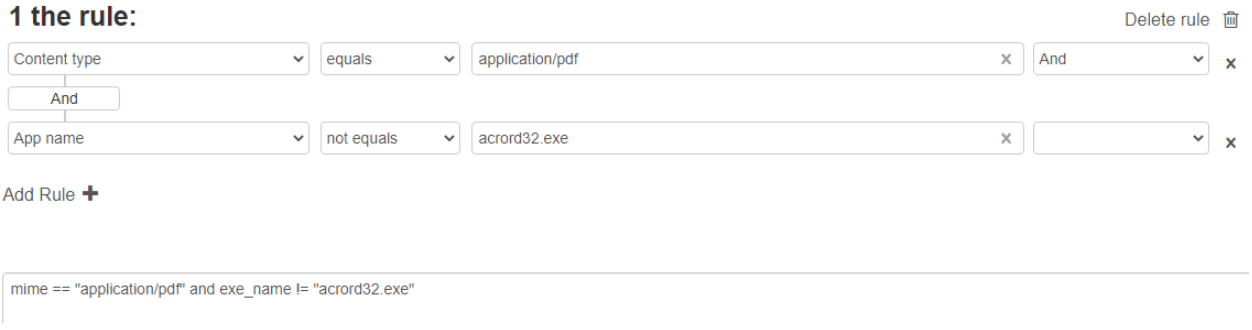
3. Выбираем условия следующим образом:



Содержимое файла равно типу pdf

4. В последнем боксе выбираем логическое условие «And» для добавления второго условия.

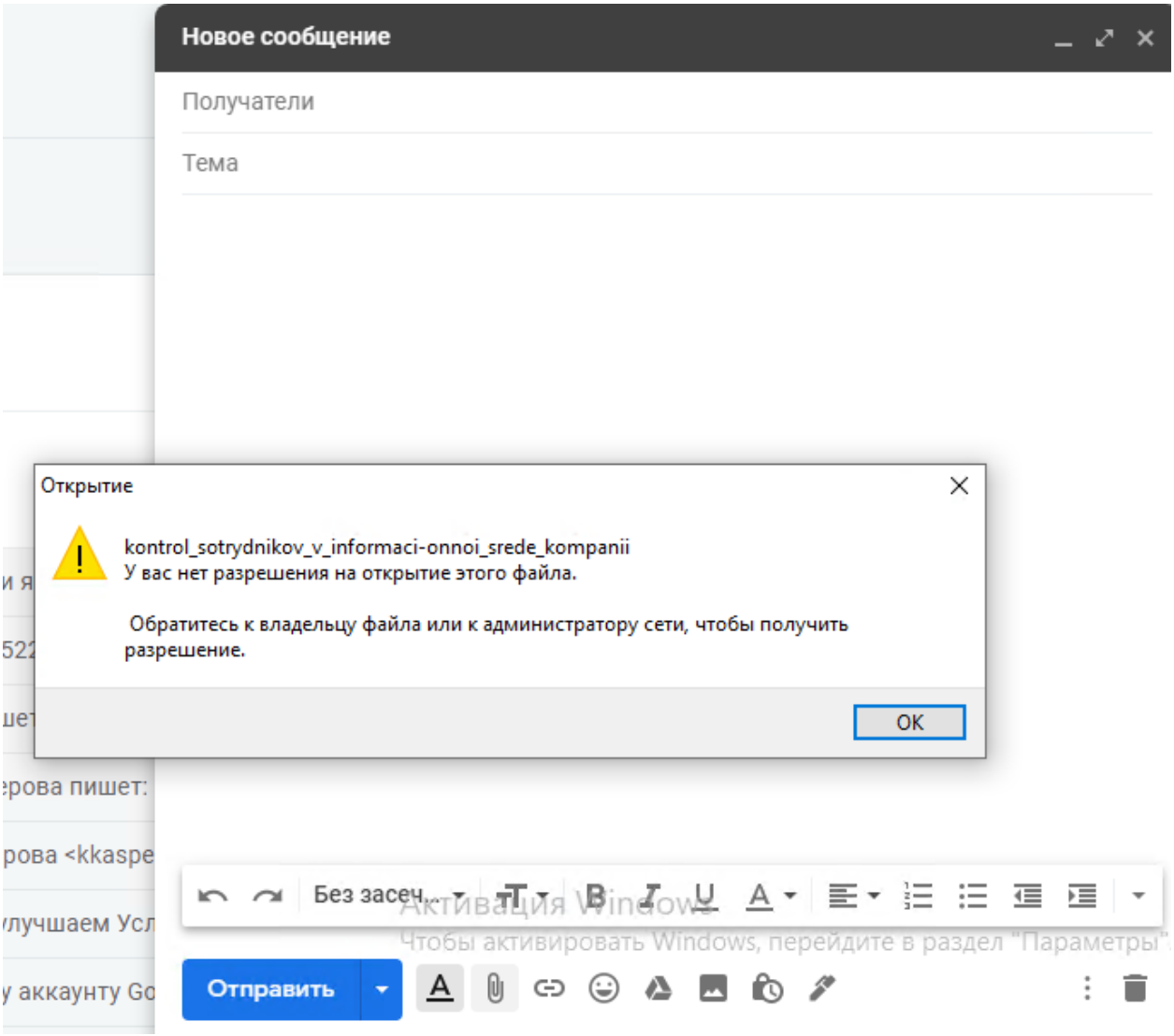
Вторым условием будет что программа имеющая доступ к файлу отличается от AcrobatReader



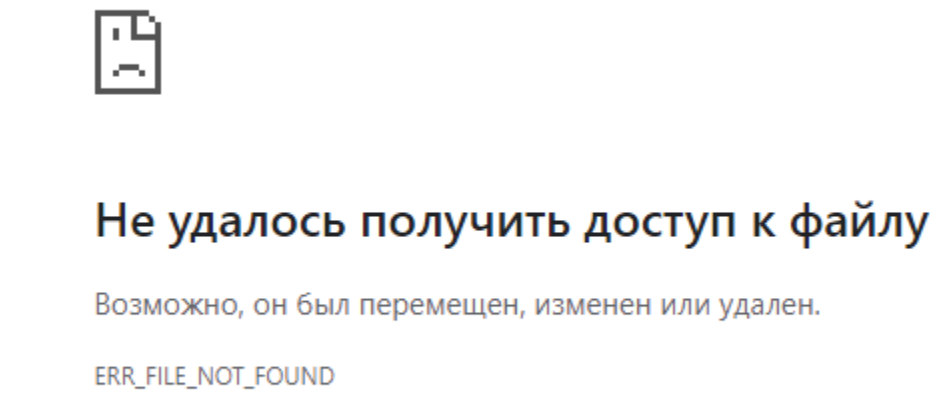

```
mime == "application/pdf" and exe_name != "acrord32.exe"
```

5. Сохраняем конфигурацию и проверяем на ПК сотрудника.

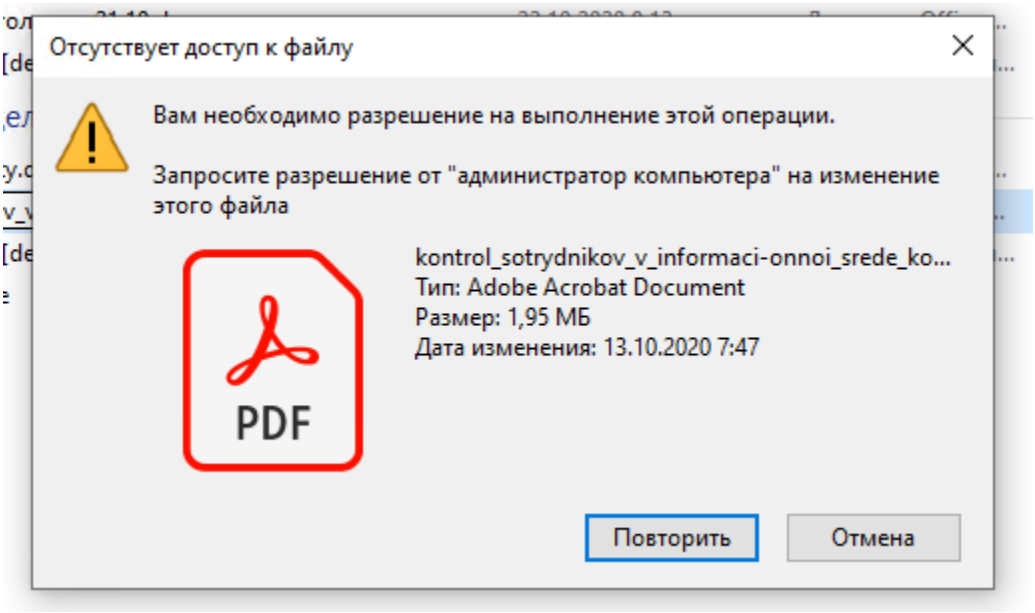
При попытке вложить файл pdf в письмо – запрет действия.



При попытке открыть файл в другой программе, например в браузере – запрет.



При попытке сменить расширение файла – запрет действия.



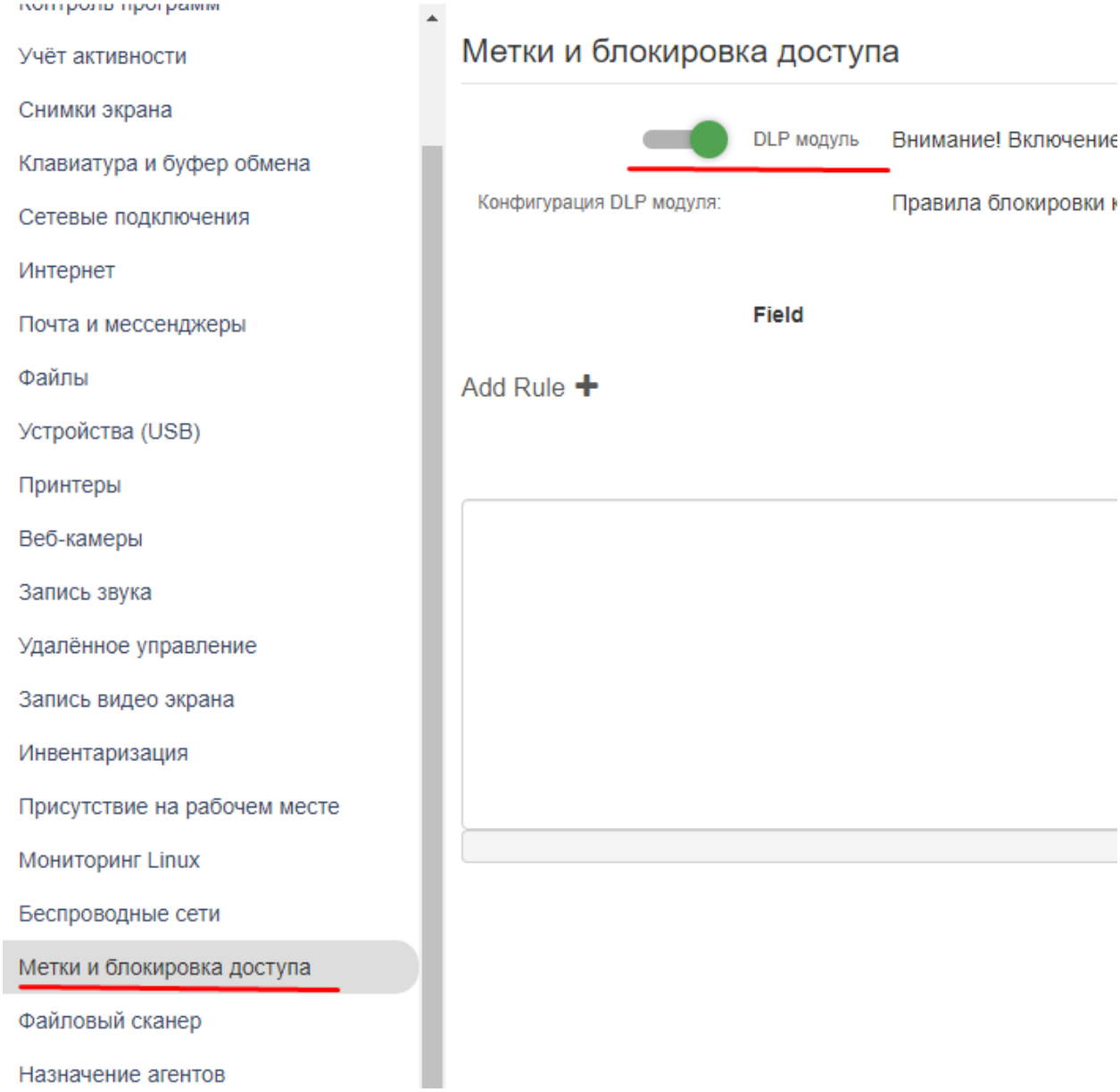
6. Таким образом мы можем запретить отправку файла используя почтовую программу или web-браузер. Для запрета записи на USB носитель нужно использовать модуль блокировки USB носителей.

Чтение файла и работа в разрешённом приложении доступны.

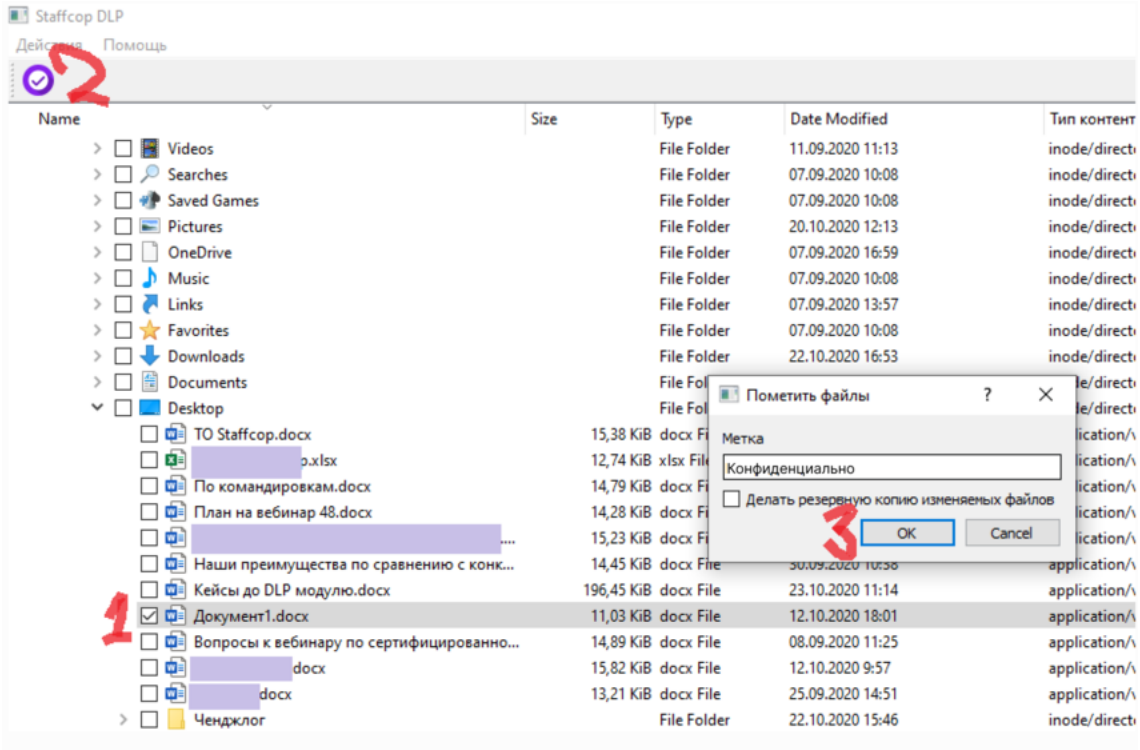
Отслеживание «движения» файла в периметре организации

1. Активируем DLP модуль в конфигурации компьютеров.

Обращаю внимание, отслеживание по метке будет работать только на тех ПК где в конфигурации включен модуль.

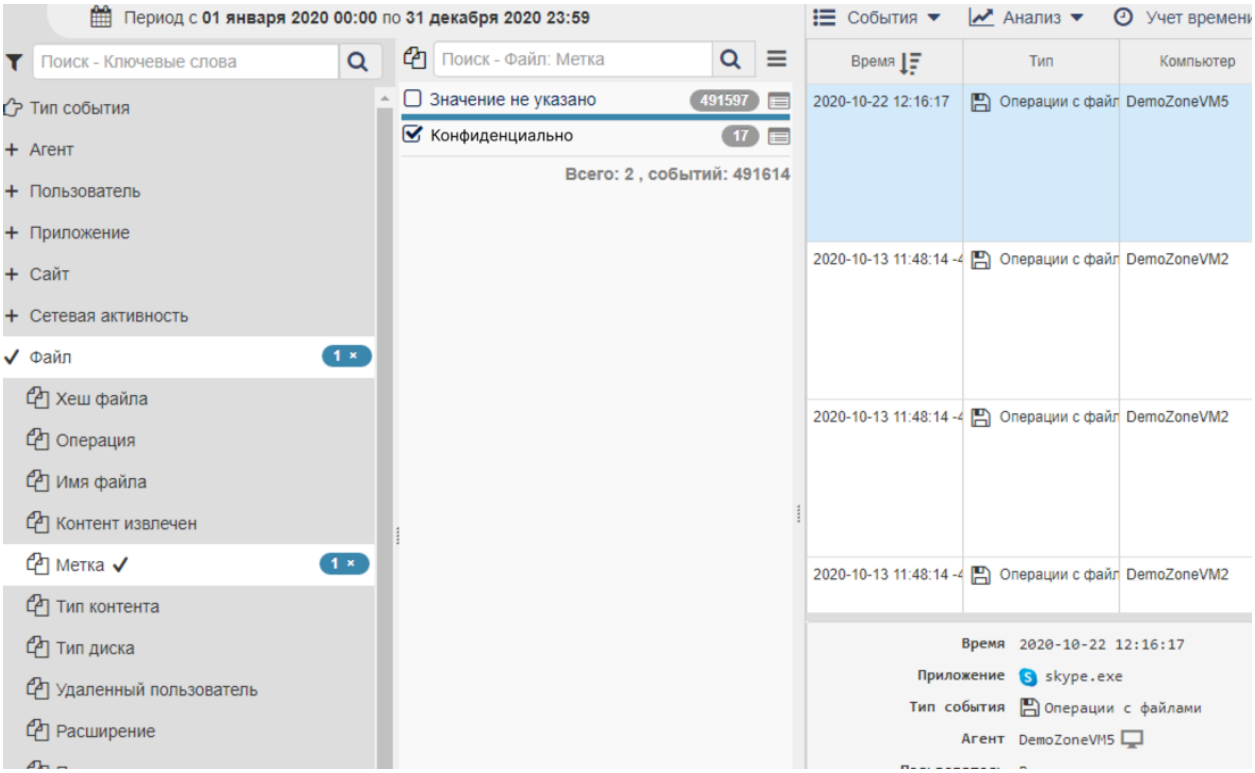


2. Используя утилиту, создаём метку в файле

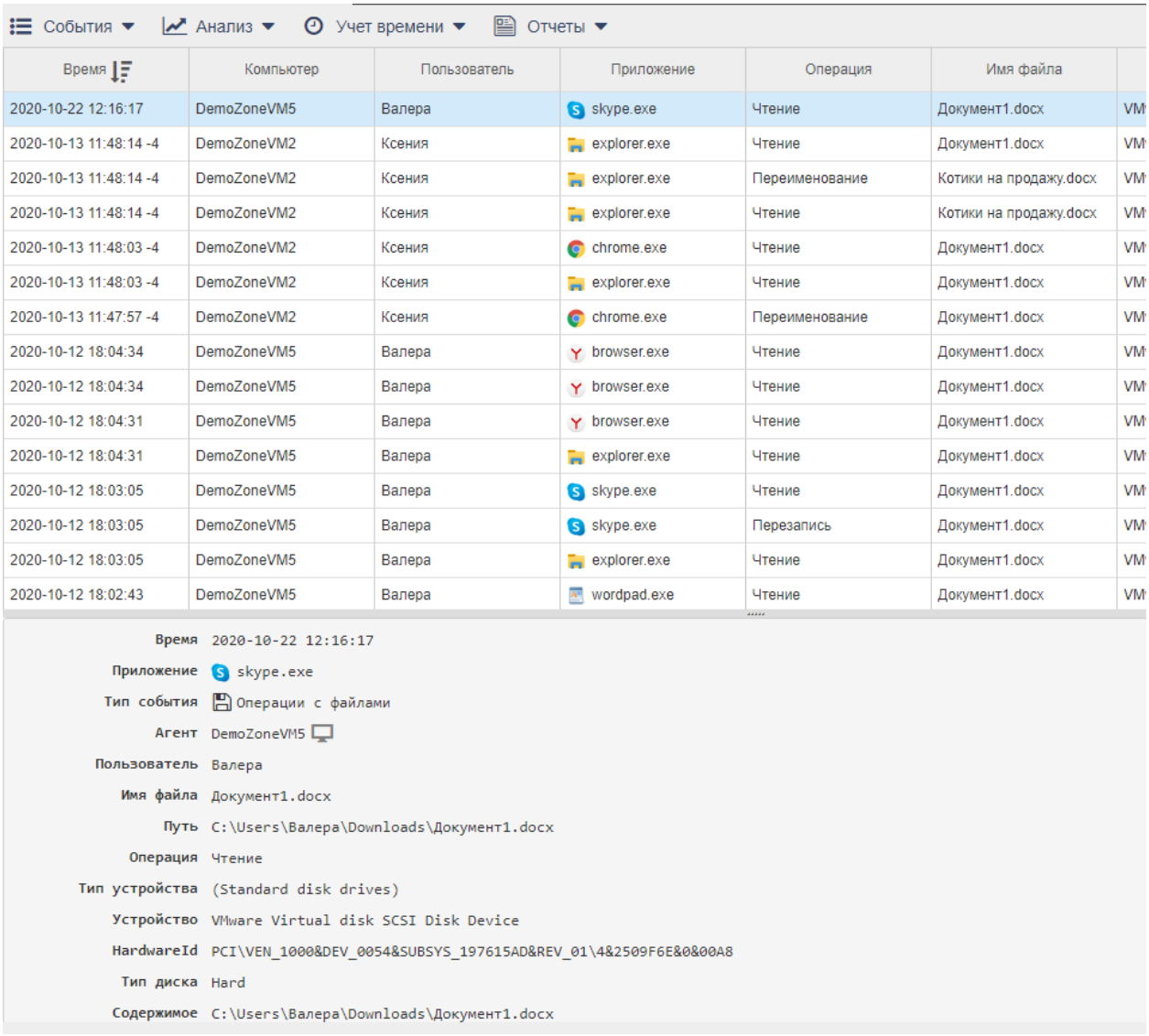


3. Теперь данный файл можно распространить внутри информационного контролируемого периметра и производить аналитику в web-консоли.

В измерении «Файл» выбираем параметр «Метка» и нужно значение – в линзе событий будут все события связанные с файлами с выбранной меткой.



4. Вид в линзе событий можно привести к компактному, если дополнительно выбрать значение «Операции с файлами» в «Типы событий»

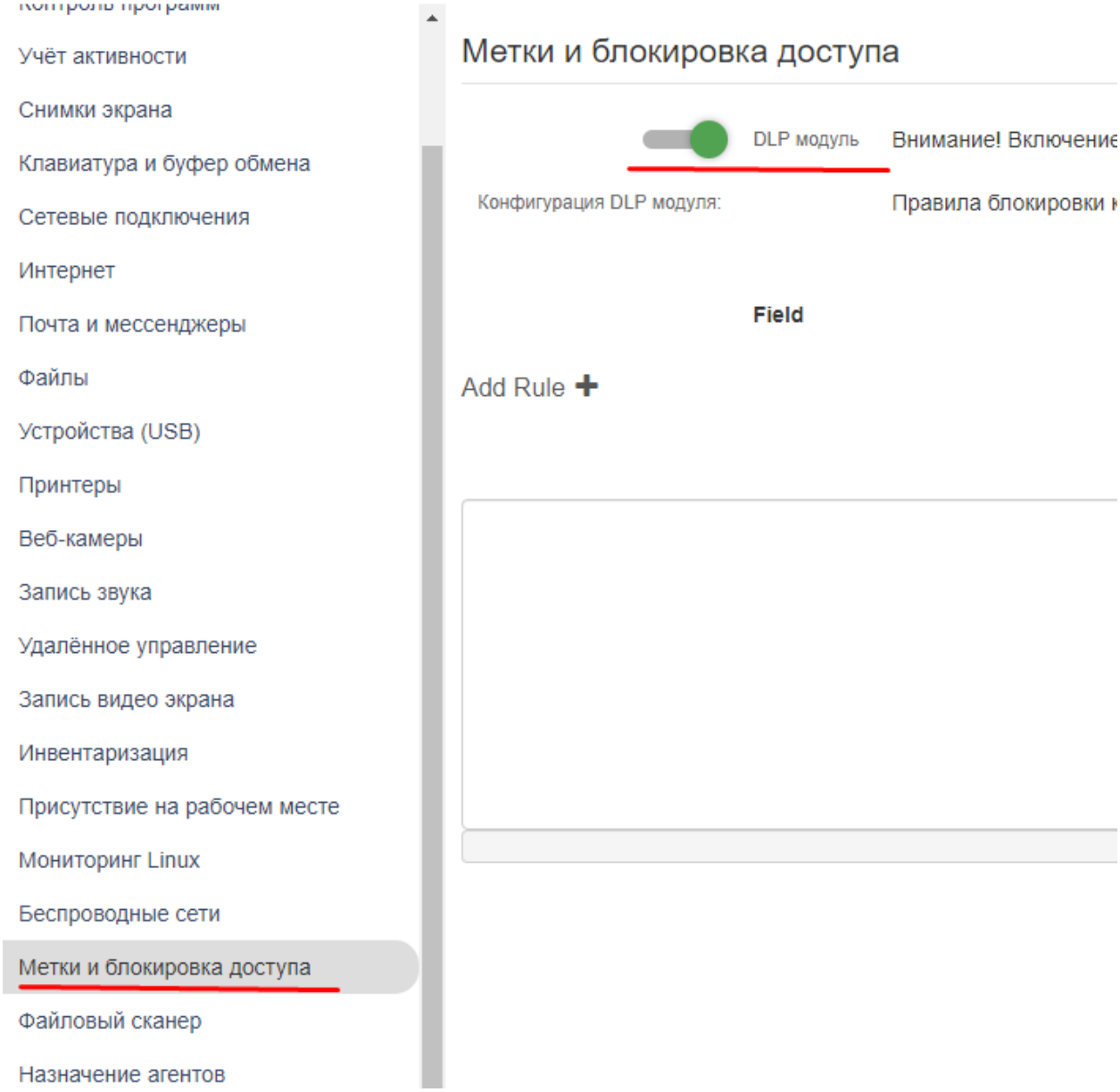


5. Далее уже можно проводить аналитическую и оперативную работу используя другие возможности web-консоли.

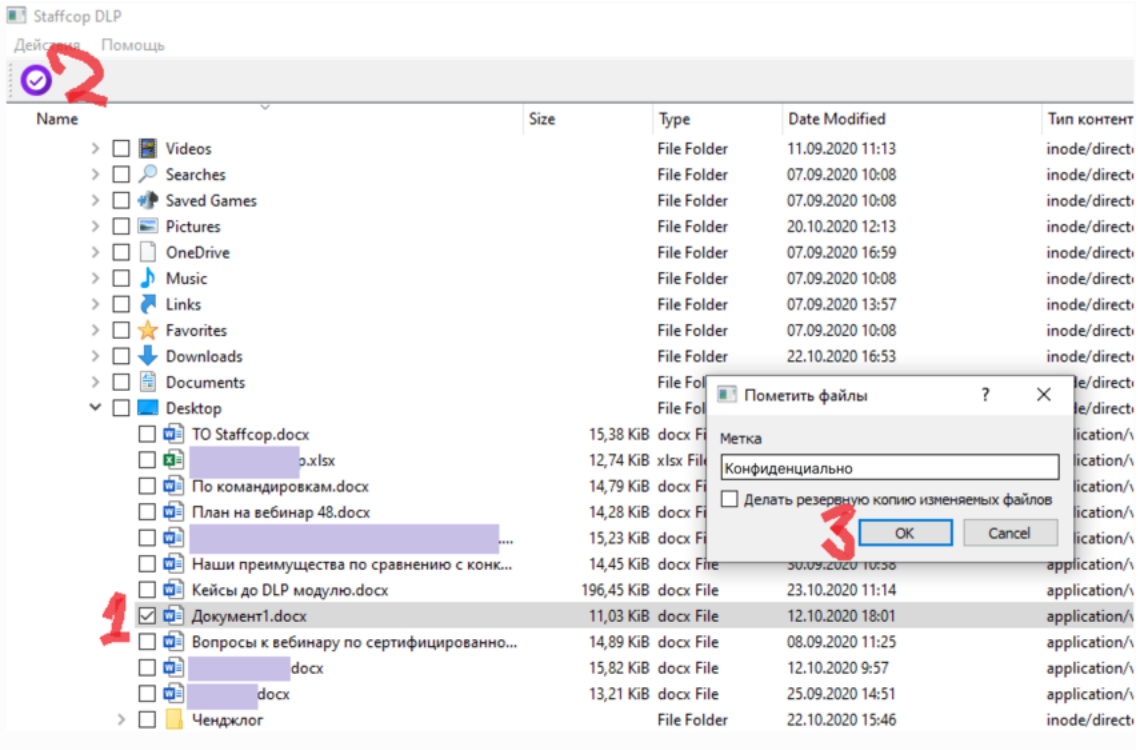
Доступ к данным только определённым сотрудникам

1. Активируем DLP модуль в конфигурации компьютеров.

Обращаю внимание, отслеживание по метке будет работать только на тех ПК где в конфигурации включен модуль.

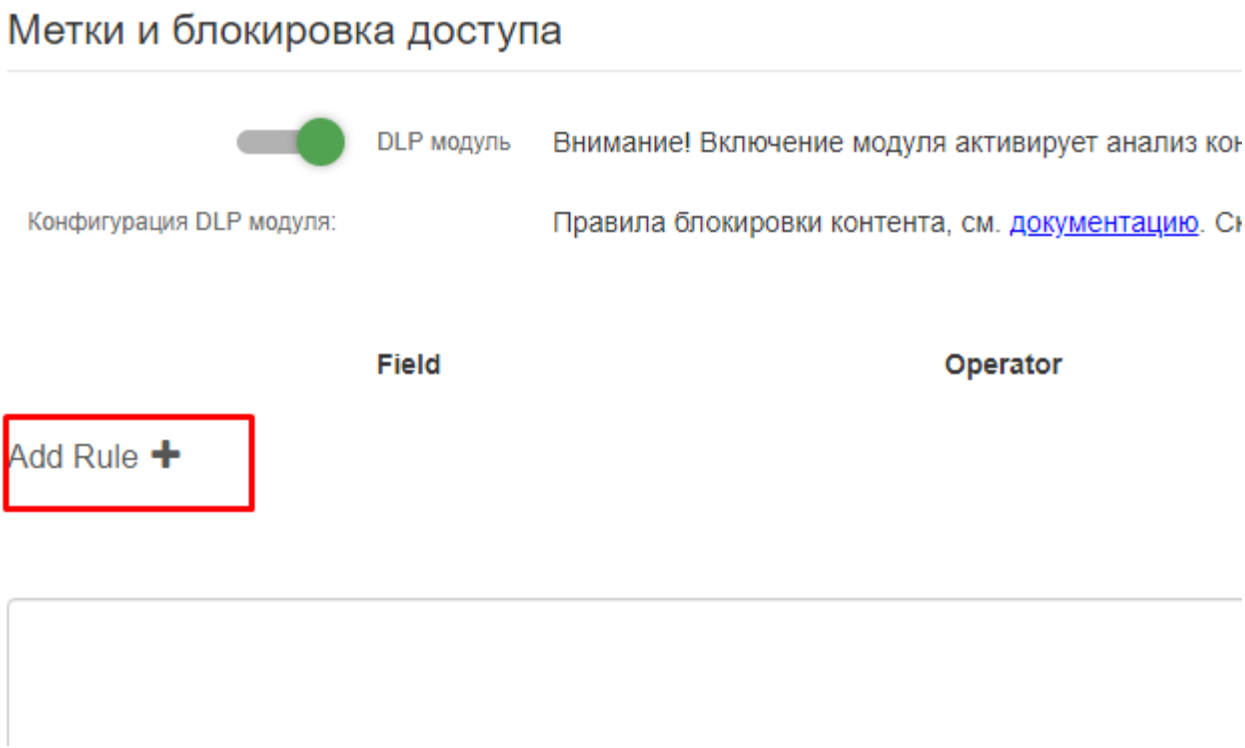


2. Используя утилиту создаём метку в файле

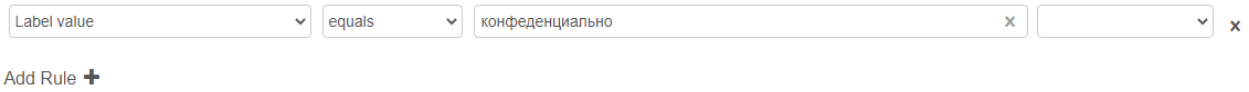


3. Создадим правило блокировки.

Примечание: При составлении правила нужно помнить, что это правило блокировки, т.е. условия подразумевают запрет действий когда правило истинно.

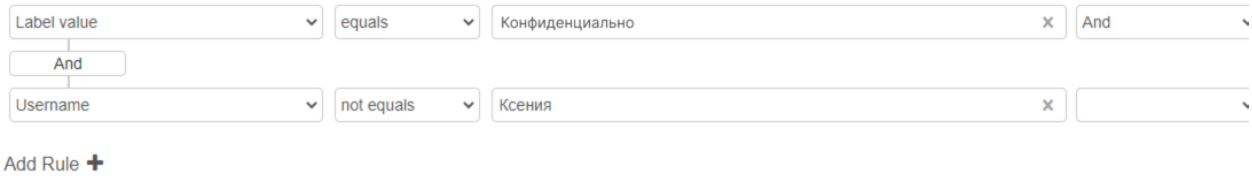


4. Укажем какую метку мы использовали и выбираем условия следующим образом:



5. В последнем боксе выбираем логическое условие «And» для добавления второго условия.

Вторым условием будет что имя пользователя отлично от «Ксения»



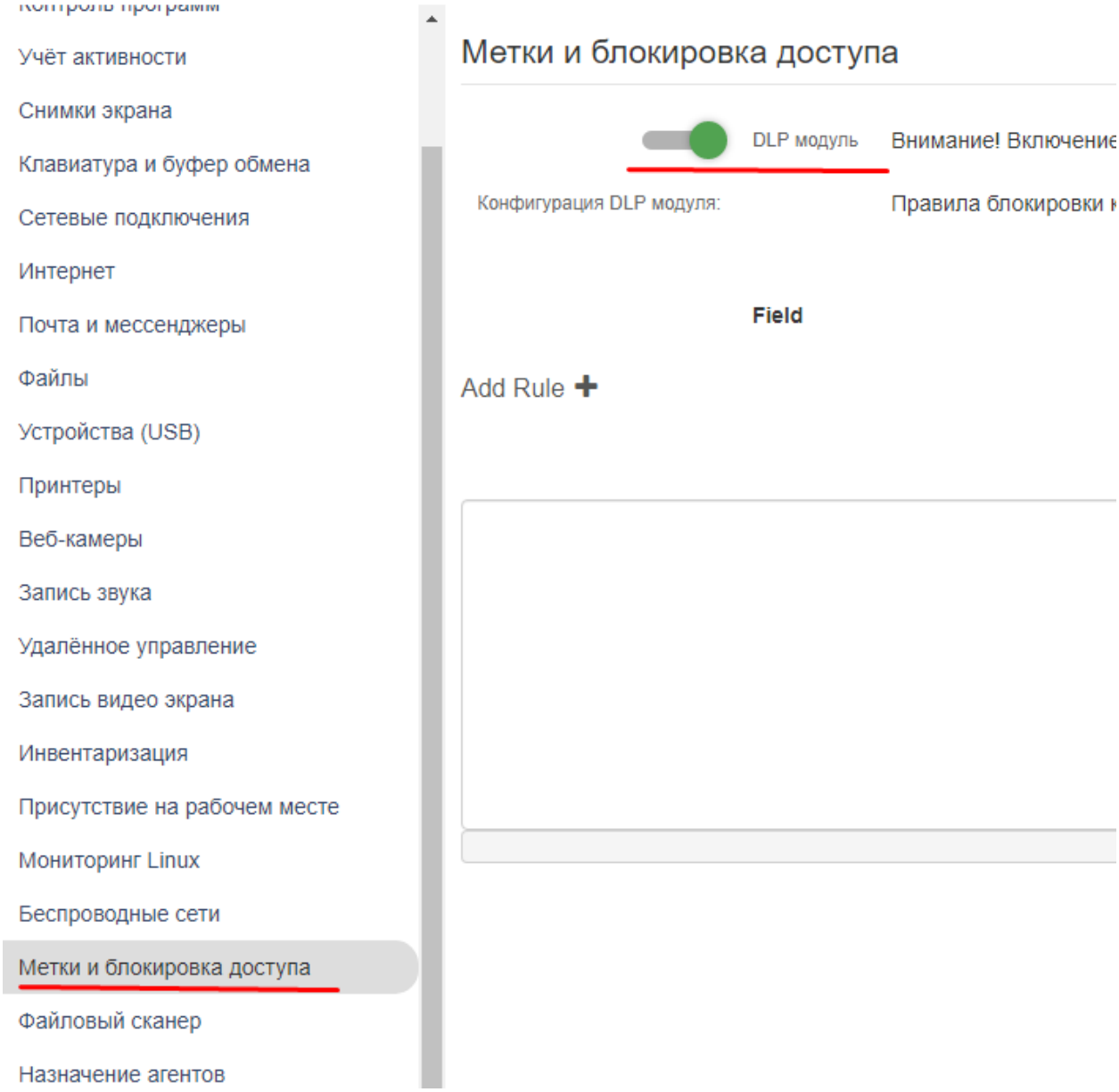
6. Сохраняем конфигурацию и проверяем на ПК сотрудников.

У Ксении есть доступ к файлам, У Валерия – нет.

Запрет отправки файлов на флешку через RDP

1. Активируйте DLP модуль в конфигурации компьютеров.

Обратите внимание, что блокировка будет работать только на тех ПК, где в конфигурации включен модуль.



2. Создайте правило блокировки, которое будет запрещать запись файлов на диски, проброшенные через RDP клиент.

Первое условие здесь указывает путь к сетевому диску, который нужно контролировать, а второе - ограничивает разрешенные файловые операции только чтением.

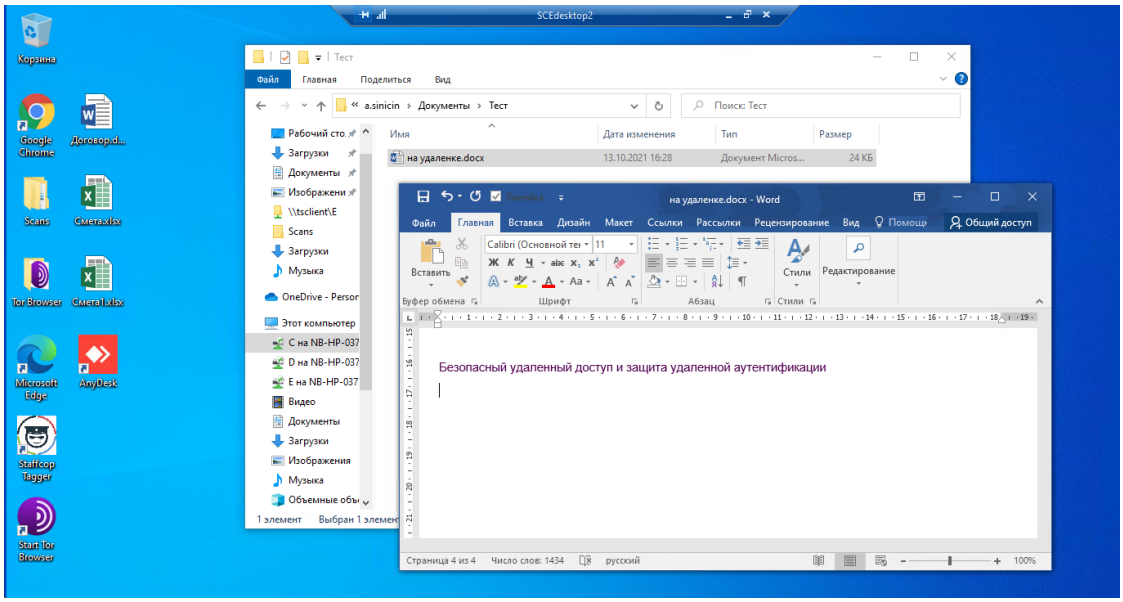
Примечание: При составлении правила помните, что это правило блокировки, т.е. условия подразумевают запрет действий, когда правило истинно.

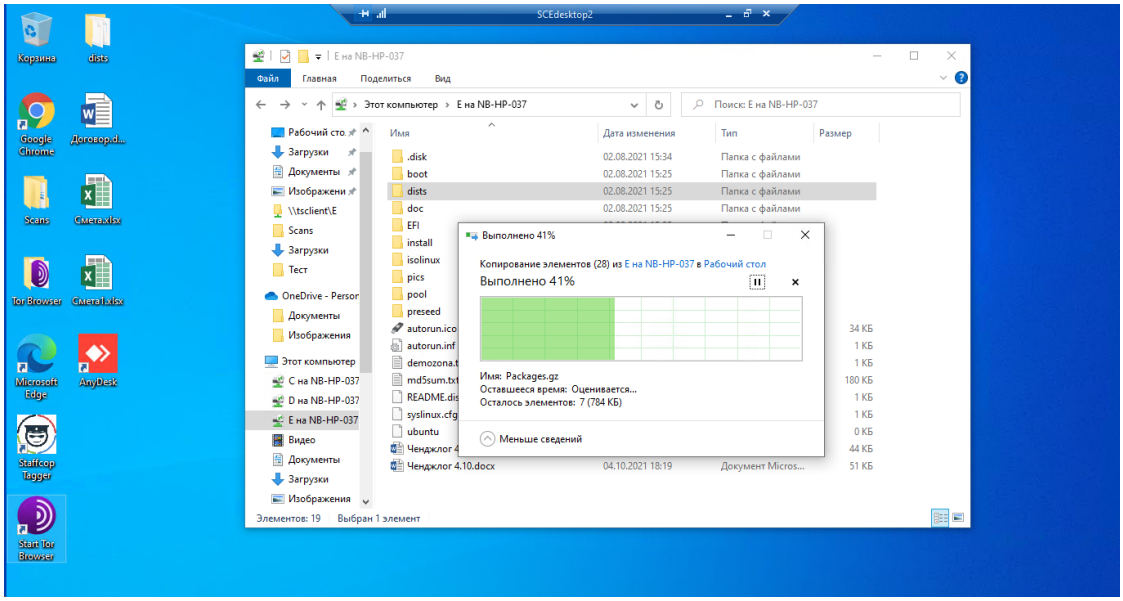
Готовый код такого правила будет иметь вид:

```
file_path matches "(\\\\tsclient\\)" and not file_operation in {"Read"}
```

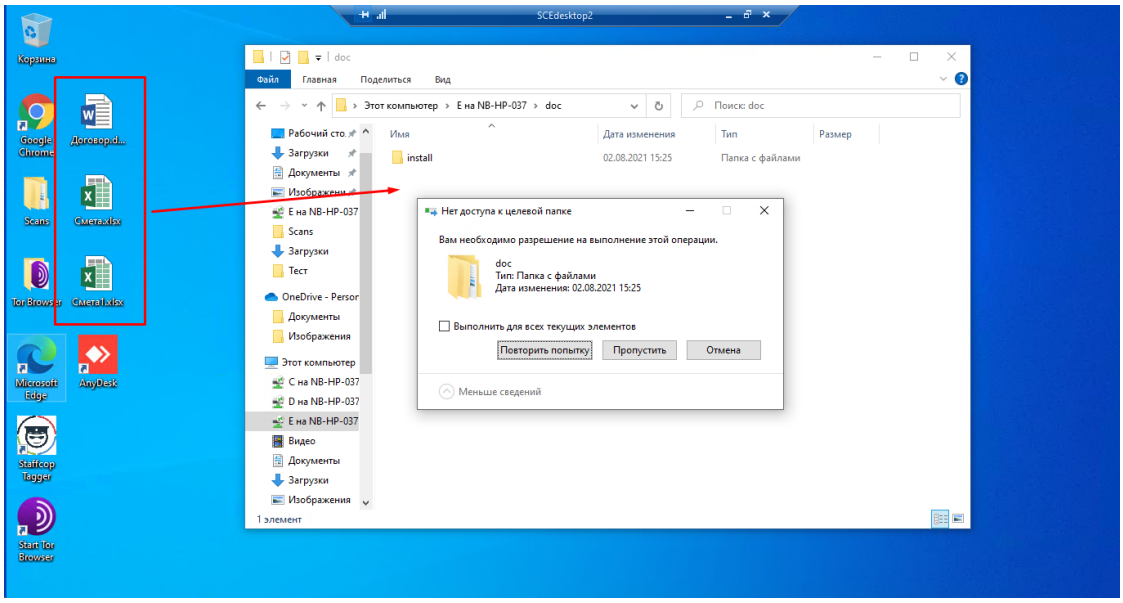
3. Сохраните конфигурацию и проверьте работу модуля на ПК сотрудника.

   При попытке открыть файл с подключенного диска, или скопировать файл для работы внутри терминальной сессии все работает.





Отправка рабочих файлов обратно на подключенный диск запрещена.



4. Таким образом можно запретить отправку файлов на любой подключенный через RDP клиент носитель.

Чтение файлов и работа внутри терминальной сессии доступны.

Блокировать работу с файлом, если в нём содержится искомый текст

DLP-модуль позволяет заблокировать работу с файлом, содержащим определённый текст. Это может помочь с предотвращением утечек информации за периметр безопасности.

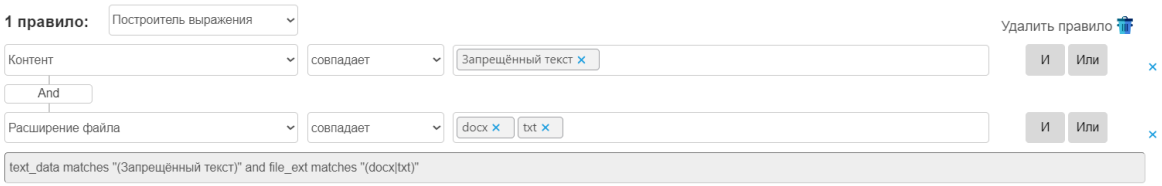
Заблокировать работу с файлом можно при помощи *правил работы DLP-модуля*. Чтобы эффективно блокировать работу с файлами, содержащими определённый текст, есть два варианта настройки правил:

- правило, отслеживающее файлы с определённым расширением;
- правило, отслеживающее файлы с определённым типом контента.

Первый вариант проще в настройке, второй - более надёжный.

Блокировка по расширению файла

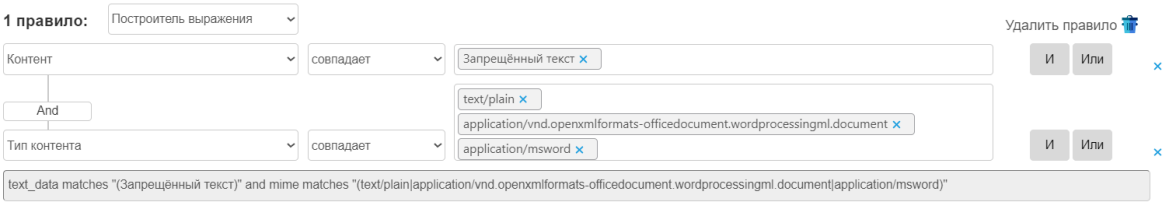
1. В веб-интерфейсе сервера iBatyr Monitor перейдите в раздел **Панель управления - Конфигурации компьютеров - Метки и блокировка доступа**.
2. Создайте новое правило:
   - **Контент - совпадает** - *Запрещённый текст*
   - **И**
   - **Расширение файла - совпадает** - *Укажите расширения файлов, которые необходимо контролировать*



3. Сохраните конфигурацию и примените её.

Блокировка по типу контента

1. В веб-интерфейсе сервера iBatyr Monitor перейдите в раздел **Панель управления - Конфигурации компьютеров - Метки и блокировка доступа**.
2. Создайте новое правило:
   - **Контент - совпадает -** *Запрещённый текст*
   - **И**
   - **Тип контента - совпадает -** *Укажите необходимый тип контента*



3. Сохраните конфигурацию и примените её.

Чтобы заблокировать файлы офисных форматов, добавьте в строку **Тип контента** следующие значения:

- text/plain;
- application/vnd.openxmlformats-officedocument.wordprocessingml.document;
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet;
- application/vnd.oasis.opendocument.text;
- application/vnd.openxmlformats-officedocument.presentationml.presentation;
- application/zip;
- text/x-csrc;
- application/vnd.oasis.opendocument.presentation.

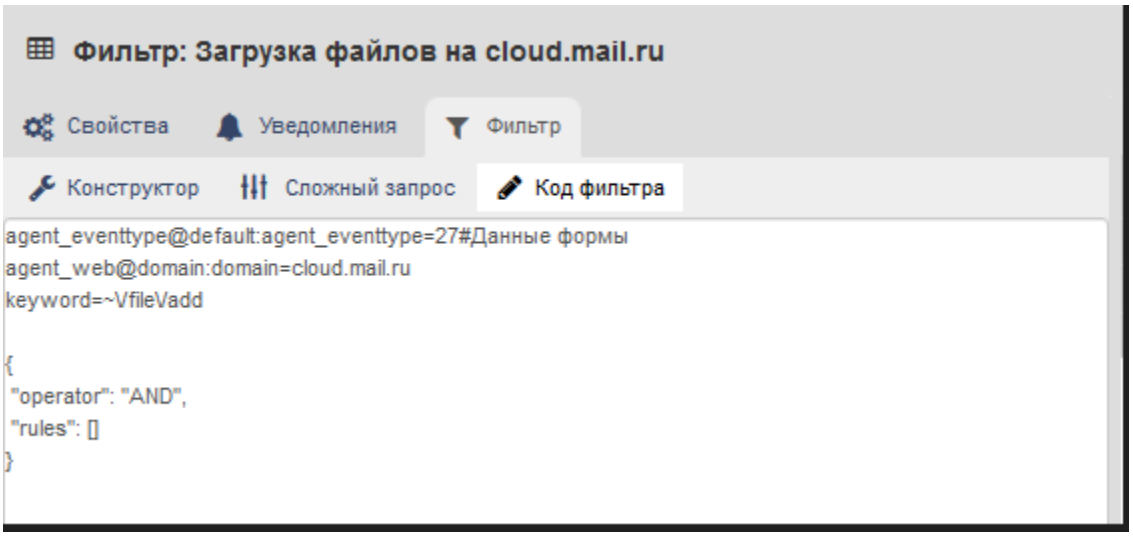
4.5.33 Перехват списка загруженных файлов в публичные облачные обменники через данные веб-форм iBatyr Monitor на примере https://cloud.mail.ru/

Попробуйте создать фильтр:

- Тип события - Данные форм
- Сайт - cloud.mail.ru
- В поиске по ключевым словам введите - «~/file/add» - без кавычек

Получится такой фильтр как на скриншоте.

2. Импортировать себе этот фильтр можно Создав новый фильтр и на вкладке Фильтр - Код фильтра:



Код фильтра который можно вставить в фильтр:

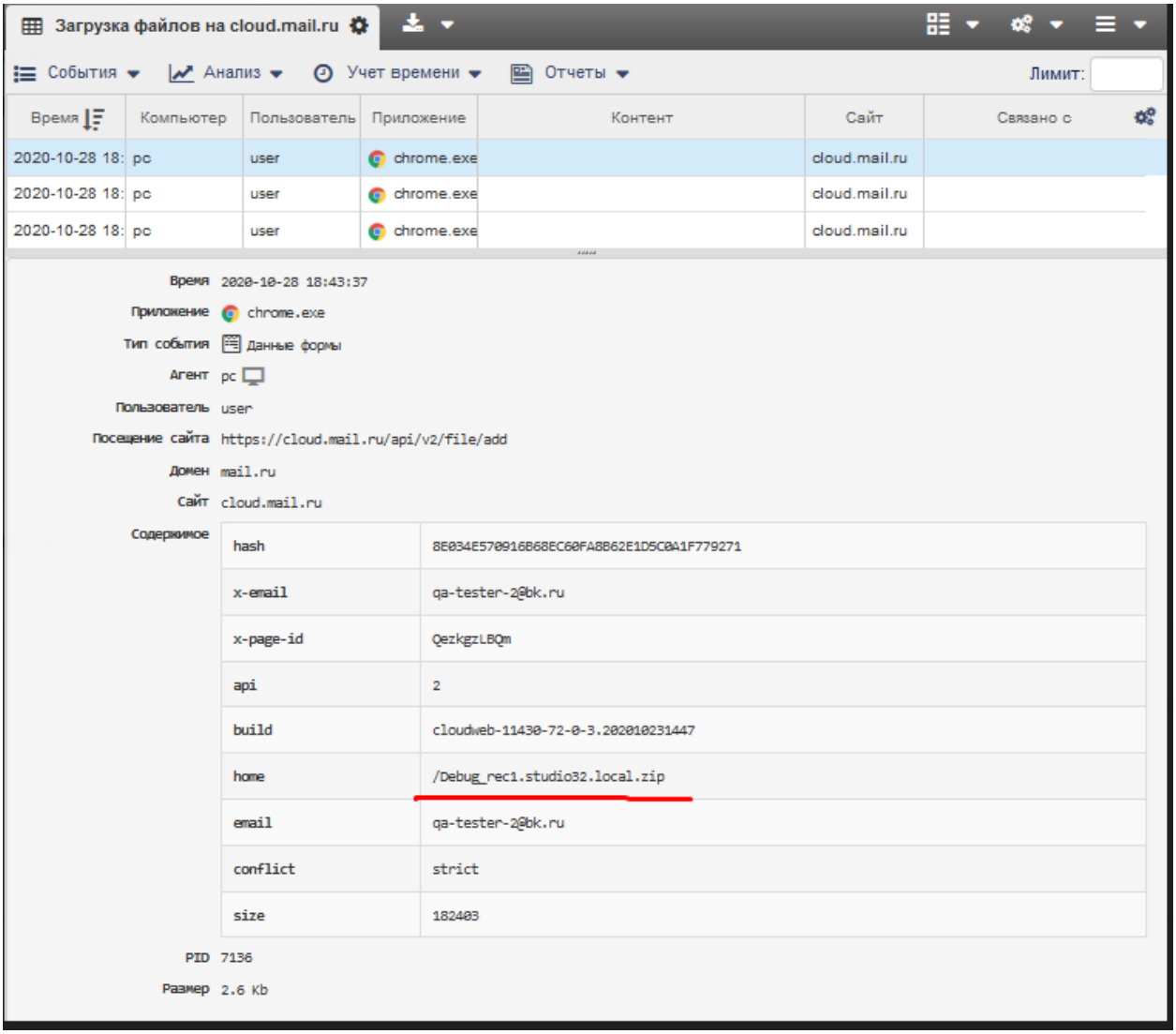
```
agent_eventtype@default:agent_eventtype=27#Данные формы
agent_web@domain:domain=cloud.mail.ru
keyword=~\/file\/add

{
 "operator": "AND",
 "rules": []
}
```

И нужно будет на вкладке «Уведомления» настроить кому отсылать письма, если такие события будут происходить

Этот фильтр показывает момент загрузки файла в облако mail.ru.

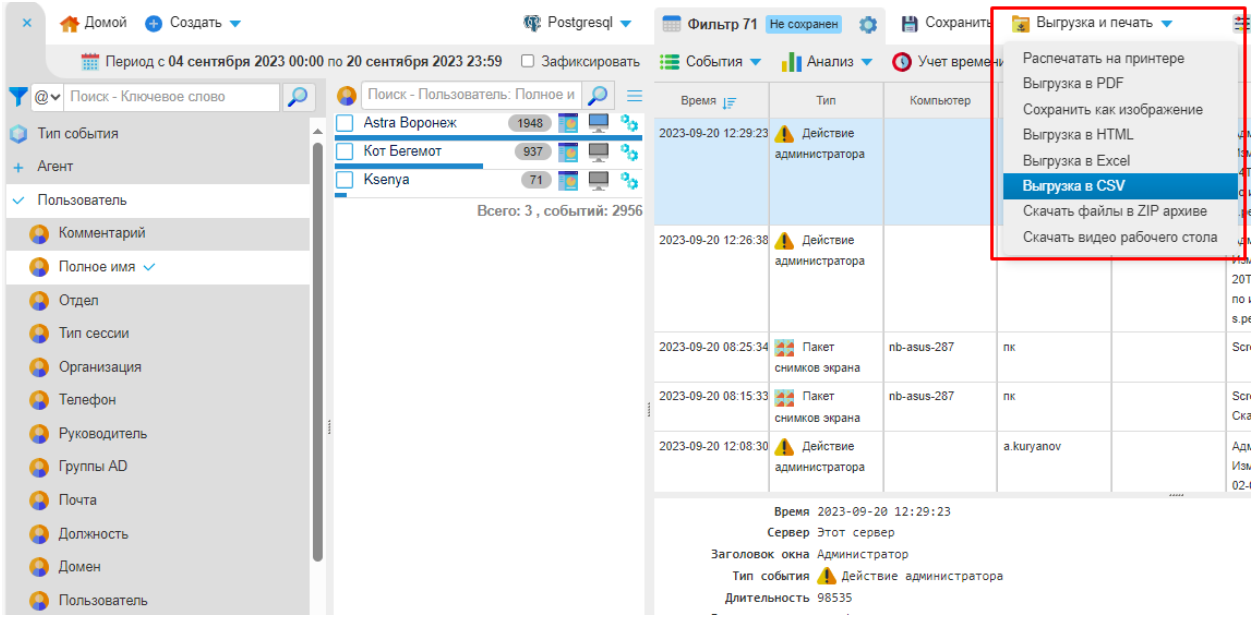
В самом событии видно, что за файл был передан:



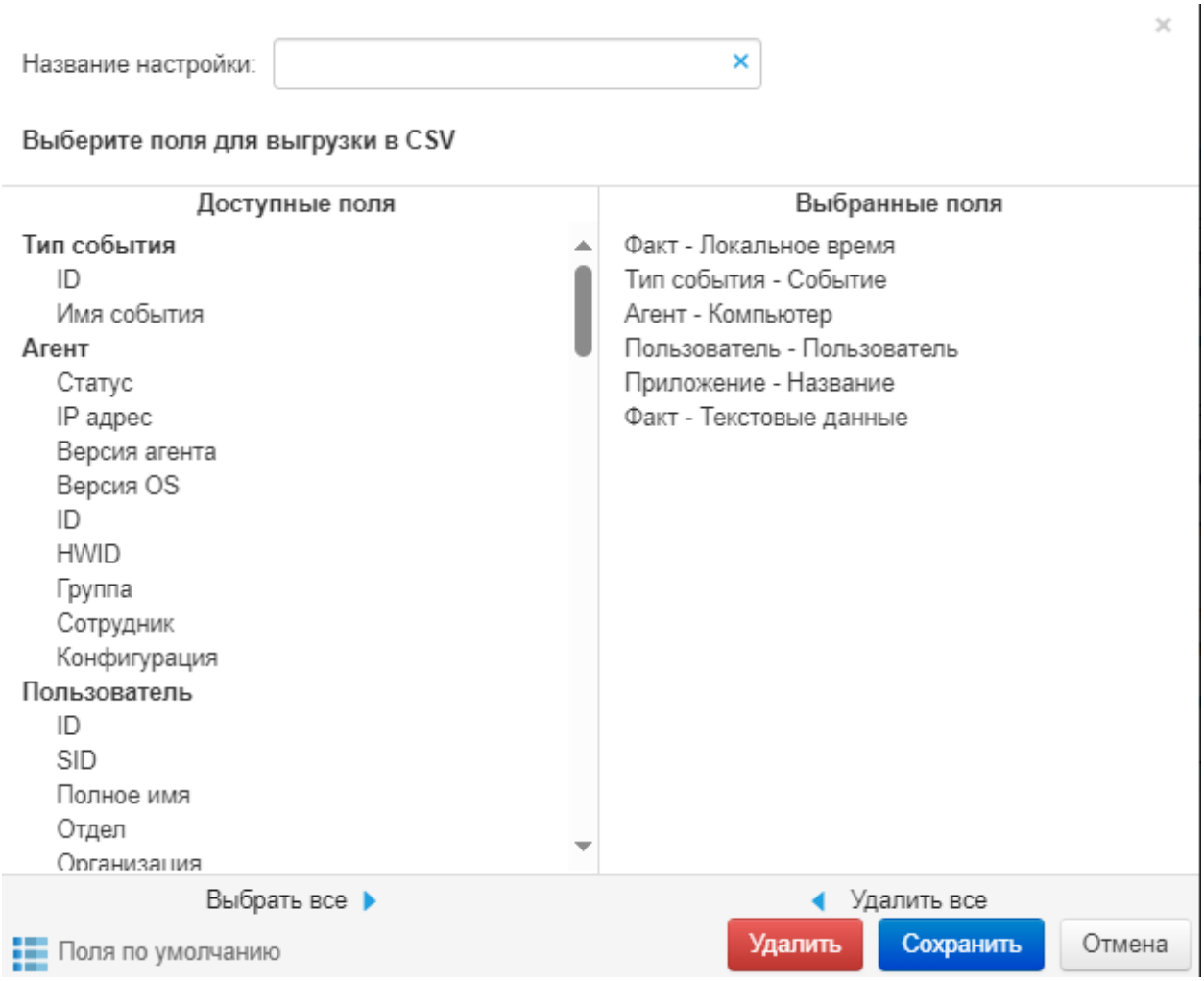
4.5.34 Выгрузка отчета в формате CSV в MS Excel

Созданные отчеты и выборки в iBatyr Monitor можно выгружать в отдельные файлы.

Один из доступных для выгрузки форматов — CSV.



После выбора формата выгрузки выберите поля, которые будут выгружены в файл:

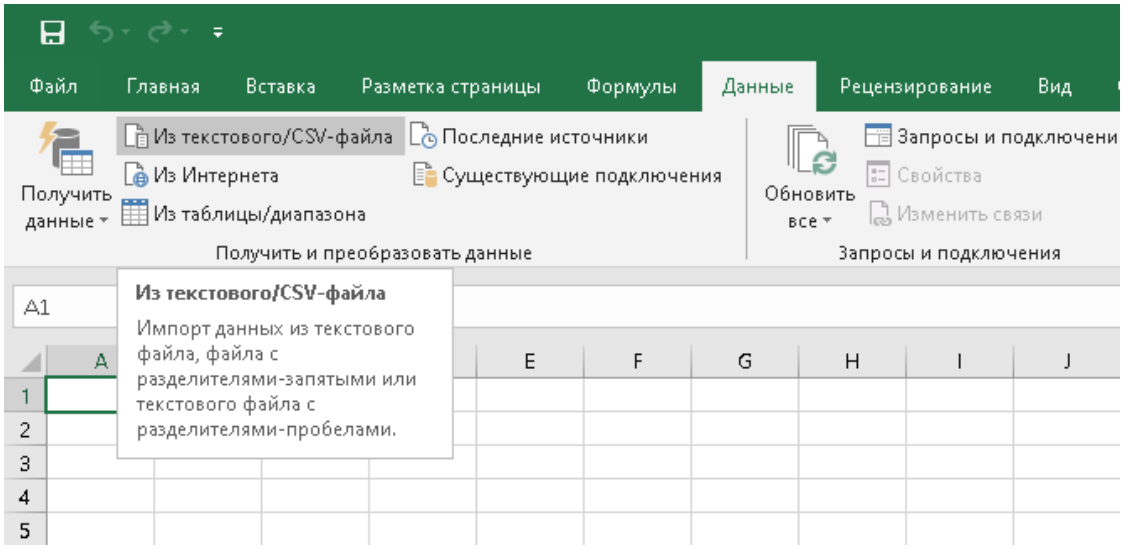


После нажатия кнопки **Сохранить** скачается архив с именем *Events_ login_ date.zip*. Здесь *login* — имя администратора, скачавшего архив, *date* — дата создания отчета.

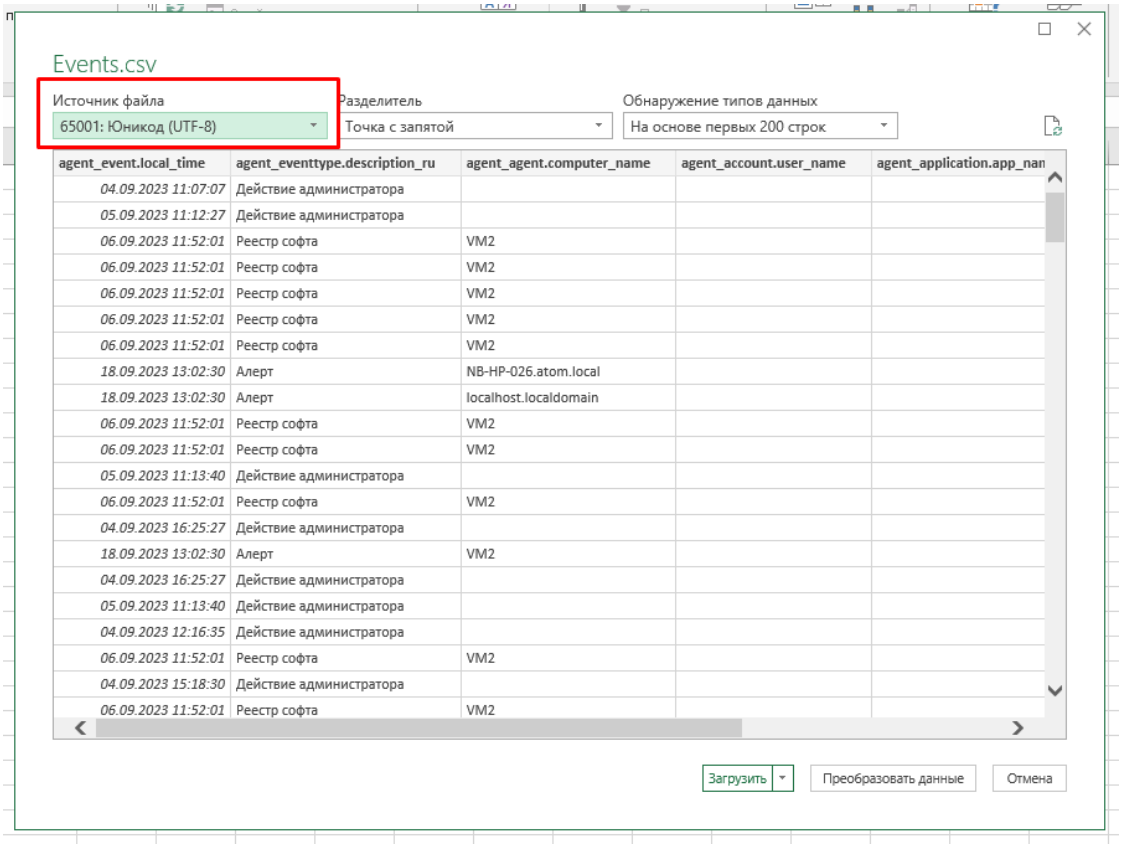
Если вы откроете файл напрямую, он отобразится в виде нечитаемых символов из-за различий в кодировках Excel и CSV.

Следуйте инструкции, чтобы корректно открыть отчет:

1. Извлеките из архива файл с отчетом.
2. В MS Excel на вкладке **Данные** выберите пункт **Из текстового/CSV файла**.



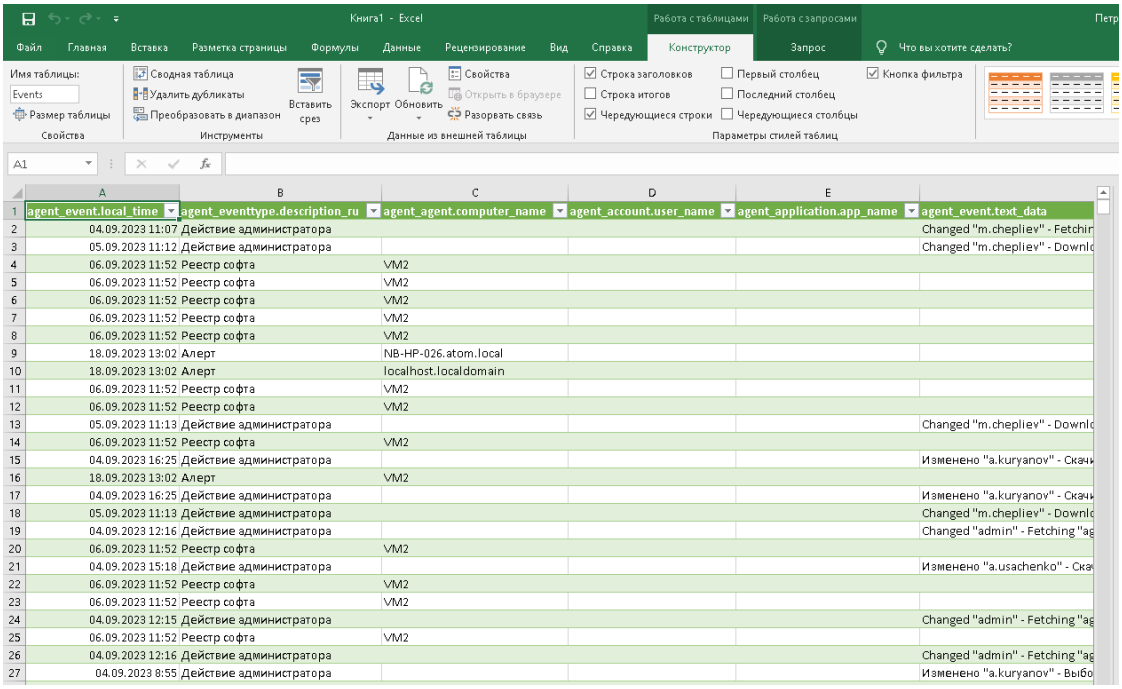
3. Выберите файл с отчетом.
4. В открывшемся окне импорта в строке **Источник файла** выберите кодировку **65001: Юникод (UTF-8)**.



agent_event.local_time	agent_eventtype.description_ru	agent_agent.computer_name	agent_account.user_name	agent_application.app_nam
04.09.2023 11:07:07	Действие администратора			
05.09.2023 11:12:27	Действие администратора			
06.09.2023 11:52:01	Реестр софта	VM2		
06.09.2023 11:52:01	Реестр софта	VM2		
06.09.2023 11:52:01	Реестр софта	VM2		
06.09.2023 11:52:01	Реестр софта	VM2		
06.09.2023 11:52:01	Реестр софта	VM2		
18.09.2023 13:02:30	Алерт	NB-HP-026.atom.local		
18.09.2023 13:02:30	Алерт	localhost.localdomain		
06.09.2023 11:52:01	Реестр софта	VM2		
06.09.2023 11:52:01	Реестр софта	VM2		
05.09.2023 11:13:40	Действие администратора			
06.09.2023 11:52:01	Реестр софта	VM2		
04.09.2023 16:25:27	Действие администратора			
18.09.2023 13:02:30	Алерт	VM2		
04.09.2023 16:25:27	Действие администратора			
05.09.2023 11:13:40	Действие администратора			
04.09.2023 12:16:35	Действие администратора			
06.09.2023 11:52:01	Реестр софта	VM2		
04.09.2023 15:18:30	Действие администратора			
06.09.2023 11:52:01	Реестр софта	VM2		

5. **Загрузить**.

В результате в Excel-файле откроется отчет:



agent_event.local_time	agent_eventtype.description_ru	agent_agent.computer_name	agent_account.user_name	agent_application.app_name	agent_event.text_data
04.09.2023 11:07	Действие администратора				Changed "m.chepliev" - Fetchir
05.09.2023 11:12	Действие администратора				Changed "m.chepliev" - Downlo
06.09.2023 11:52	Реестр софта	VM2			
06.09.2023 11:52	Реестр софта	VM2			
06.09.2023 11:52	Реестр софта	VM2			
06.09.2023 11:52	Реестр софта	VM2			
06.09.2023 11:52	Реестр софта	VM2			
18.09.2023 13:02	Алерт	NB-HP-026.atom.local			
18.09.2023 13:02	Алерт	localhost.localdomain			
06.09.2023 11:52	Реестр софта	VM2			
06.09.2023 11:52	Реестр софта	VM2			
05.09.2023 11:13	Действие администратора				Changed "m.chepliev" - Downlo
06.09.2023 11:52	Реестр софта	VM2			
04.09.2023 16:25	Действие администратора				Изменено "a.kuryanov" - Скачи
18.09.2023 13:02	Алерт	VM2			
04.09.2023 16:25	Действие администратора				Изменено "a.kuryanov" - Скачи
05.09.2023 11:13	Действие администратора				Changed "m.chepliev" - Downlo
04.09.2023 12:16	Действие администратора				Changed "admin" - Fetching "ag
06.09.2023 11:52	Реестр софта	VM2			
04.09.2023 15:18	Действие администратора				Изменено "a.usachenko" - Скач
06.09.2023 11:52	Реестр софта	VM2			
06.09.2023 11:52	Реестр софта	VM2			
04.09.2023 12:15	Действие администратора				Changed "admin" - Fetching "ag
06.09.2023 11:52	Реестр софта	VM2			
04.09.2023 12:16	Действие администратора				Changed "admin" - Fetching "ag
04.09.2023 8:55	Действие администратора				Изменено "a.kuryanov" - Выбо

4.5.35 Визуализация данных iBatyr Monitor в отчетах через PowerBI

Подготовка сервера iBatyr Monitor

По умолчанию удалённое подключение к базе на сервере iBatyr Monitor отключено. Чтобы его включить:

1. Создайте пользователя, который будет работать с PowerBI:

- запустите консоль PostgreSQL:

```
sudo -u postgres psql -d ibatyr
```

- в консоли создайте нового пользователя и выдайте ему права на работу с таблицами:

```
CREATE USER powerbi WITH PASSWORD 'password';
GRANT CONNECT ON DATABASE ibatyr TO powerbi;
GRANT USAGE ON SCHEMA public TO powerbi;
GRANT SELECT ON ALL TABLES IN SCHEMA public TO powerbi;
```

2. В конфигурационном файле базы данных **/etc/postgresql/15/main/pg_hba.conf** добавьте строку:

```
host ibatyr powerbi 00.00.00.000/32 md5
```

IP-адрес и маска подсети указывают, что доступ разрешен только с указанного IP-адреса. Замените 00.00.00.000/32 на реальный IP.

Если используете PostgreSQL 11, файл находится в **/etc/postgresql/11/main/pg_hba.conf**.

3. В файле **/etc/postgresql/15/main/postgresql.conf** укажите директиву:

```
listen_addresses = 'localhost, 00.00.00.00'
```

Замените 00.00.00.000 на IP-интерфейс, который будет прослушиваться.

4. Перезапустите PostgreSQL:

```
sudo systemctl stop postgresql && systemctl start postgresql
```

Готово! PostgreSQL прослушивает все доступные сетевые интерфейсы и ждёт подключения от PowerBI.

Настройка компьютера с установленным PowerBI

Чтобы получить данные в PowerBI:

1. Перейдите в раздел **Получить данные** → **Другие** → **База данных PostgreSQL**.
2. В открывшемся окне укажите IP-адрес сервера iBatyr Monitor и имя базы данных.
3. В открывшемся окне выберите таблицу, из которой хотите загрузить данные, и нажмите **Загрузить**.
4. После получения таблицы откройте **Расширенный редактор** и введите в нём SQL-запрос:

```
let

  Source = Value.NativeQuery(PostgreSQL.Database("192.168.0.56", "ibatyr",␣
```

(continues on next page)

(продолжение с предыдущей страницы)

```
↪[CreateNavigationProperties=false]), "

SELECT agent_time.year AS year,
     agent_time.month AS month,
     agent_time.day AS day,
     agent_agent.id AS id,
     agent_agent.guid AS guid,
     agent_agent.computer_name AS computer_name,
     analytics_filter.category AS category,
     analytics_filter.name_ru AS NAME,
     agent_web.site AS site,
     agent_application.app_name AS app_name,
     agent_time.time_zone AS time_zone,
     agent_time.year AS year,
     agent_time.month AS month,
     agent_time.day AS day,
     agent_time.hour AS hour,
     agent_time.quarter AS quarter,
     analytics_filter.type AS type,
     Min(analytics_session_extended.local_time) AS local_time_min,
     Max(analytics_session_extended.local_time) AS local_time_max,
     Max(analytics_session_extended.time_finish) AS time_finish_max,
     Min(analytics_session_extended.come) AS come_min,
     Max(analytics_session_extended.leave) AS leave_max,
     Min(analytics_session_extended.accounting_start) AS accounting_start_min,
     Max(analytics_session_extended.accounting_end) AS accounting_end_max,
     Min(analytics_session_extended.start_work_time) AS start_work_time_min,
     Max(analytics_session_extended.end_work_time) AS end_work_time_max,
     Min(analytics_session_extended.start_break_time) AS start_break_time_min,
     Max(analytics_session_extended.end_break_time) AS end_break_time_max,
     Max(analytics_session_extended.work_time) AS work_time_max,
     Every(analytics_session_extended.selected) AS selected_every,
     Array_agg(analytics_session_extended.source_table) AS source_table_array_
↪agg,
     Array_agg(analytics_session_extended.source_id) AS source_id_array_agg,
     Sum(COALESCE(analytics_session_extended.activity_time, 0)) AS activity_
↪time_sum,
     Sum(COALESCE(analytics_session_extended.idle_time, 0))     AS idle_time_
↪sum,
     Count(*) AS record_count FROM analytics_session_extended
     LEFT JOIN agent_agent ON analytics_session_extended.agent_id = agent_
↪agent.id
     LEFT JOIN agent_application ON analytics_session_extended.application_id =
               agent_application.id LEFT JOIN agent_time ON analytics_session_
↪extended.time_id = agent_time.id
     LEFT JOIN agent_web ON analytics_session_extended.web_data_id = agent_web.
↪id
     LEFT JOIN analytics_filter_events ON analytics_filter_events.event_id =␣
↪analytics_session_extended.id
     LEFT JOIN analytics_filter ON analytics_filter.id = analytics_filter_
↪events.filter_id
WHERE  ( analytics_session_extended.local_time <='2023-06-14 23:59:59.
```

(continues on next page)

(продолжение с предыдущей страницы)

```
↪999000+07:00'
       AND analytics_session_extended.local_time >='2023-06-14 00:00:00+07:00'␣
↪)
GROUP  BY agent_time.year,
        agent_time.month,
        agent_time.day,
        agent_agent.id,
        agent_agent.guid,
        agent_agent.computer_name,
        analytics_filter.category,
        analytics_filter.name_ru,
        agent_web.site,
        agent_application.app_name,
        agent_time.time_zone,
        agent_time.year,
        month,
        day,
        hour,
        quarter,
        analytics_filter.type
ORDER  BY agent_time.year,
        agent_time.month,
        agent_time.day,
        agent_agent.computer_name,
        start_work_time_min ASC

" , null, [EnableFolding=false])

in
  Source
```

4. В открывшемся окне с предупреждением нажмите **Изменить разрешение**.
5. После этого в окне **Собственный запрос к базе данных** нажмите **Выполнить**.

Готово! Данные из iBatyr Monitor загружены в редактор PowerBI. Можно приступать к настройке визуализации!

В случае возникновения ошибок

Проверьте, что созданный пользователь базы данных имеет доступ к просмотру таблиц. Для этого зайдите в консоль ыPostgreSQL от имени созданного пользователя:

```
sudo -u postgres psql -d ibatyr -U powerbi
```

и проверьте доступы пользователя к таблицам базы:

```
\dp
```

Если вывод команды будет пустым, выйдите из консоли PostgreSQL:

```
\q
```

и заново зайдите в неё, но уже от имени администратора:

```
sudo -u postgres psql -d ibatyr
```

После этого выполните команды:

```
ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT ALL ON TABLES TO powerbi;
GRANT SELECT ON ALL TABLES IN SCHEMA public TO powerbi;
```

Этого должно быть достаточно для устранения проблем с чтением данных из базы.

4.5.36 СКУД

Для взаимодействия системы СКУД и iBatyr Monitor необходимо проделать следующие действия:

Выгрузить данные из системы СКУД в файл в формате CSV.

CSV-файл с событиями должен быть в формате **UTF-8** и содержать три колонки: **timestamp, turnstile, card**.

Синхронизация с пользователями iBatyr Monitor производится по полю «пропуск» пользователя iBatyr Monitor, это значение должно совпадать с третьим столбцом **card** пользователя СКУД.

Примечание: В названии турникетов СКУД (второй столбец, **turnstile**) допустимо использование только латинских букв, цифр и пробелов.

Пример содержания файла:

```
timestamp,turnstile,card
2020-05-01T08:51:23+09:00,prohodnaya,повар
2020-05-01T08:52:34+09:00,prohodnaya,коптильщик
2020-05-01T09:12:34+09:00,konditerskiy tseh,повар
2020-05-01T09:12:35+09:00,tseh goryachego kopcheniya,коптильщик
2020-05-01T17:23:45+09:00,tseh goryachego kopcheniya vykhod,коптильщик
2020-05-01T17:23:46+09:00,konditerskiy tseh vykhod,повар
2020-05-01T17:34:56+09:00,prohodnaya vykhod,повар
2020-05-01T17:34:57+09:00,prohodnaya vykhod,коптильщик
```

Выгруженный файл с системы контроля и управления доступом (СКУД) нужно передать на сервер где установлен «iBatyr» любым удобным для вас способом.

- Если загрузка будет осуществляться с ОС Windows, то самый простой способ - воспользоваться программой WINSCP (официальная страница загрузки: https://winscp.net/eng/download.php).
- Если же с ОС Linux, то лучше воспользоваться программой для передачи файлов на удаленный сервер «rsync»:

```
rsync -zvra /local/source/загружаемый_файл.csv user@remotehost:/remote/destination/
```

Для непосредственной интеграции информации со СКУД системы в базу данных сервера «iBatyr Monitor» нужно ввести команду указав путь файла, который загрузили:

```
ibatyr scud_load_csv <путь к файлу>
```

Новые турникеты и пользователи будут добавлены автоматически.

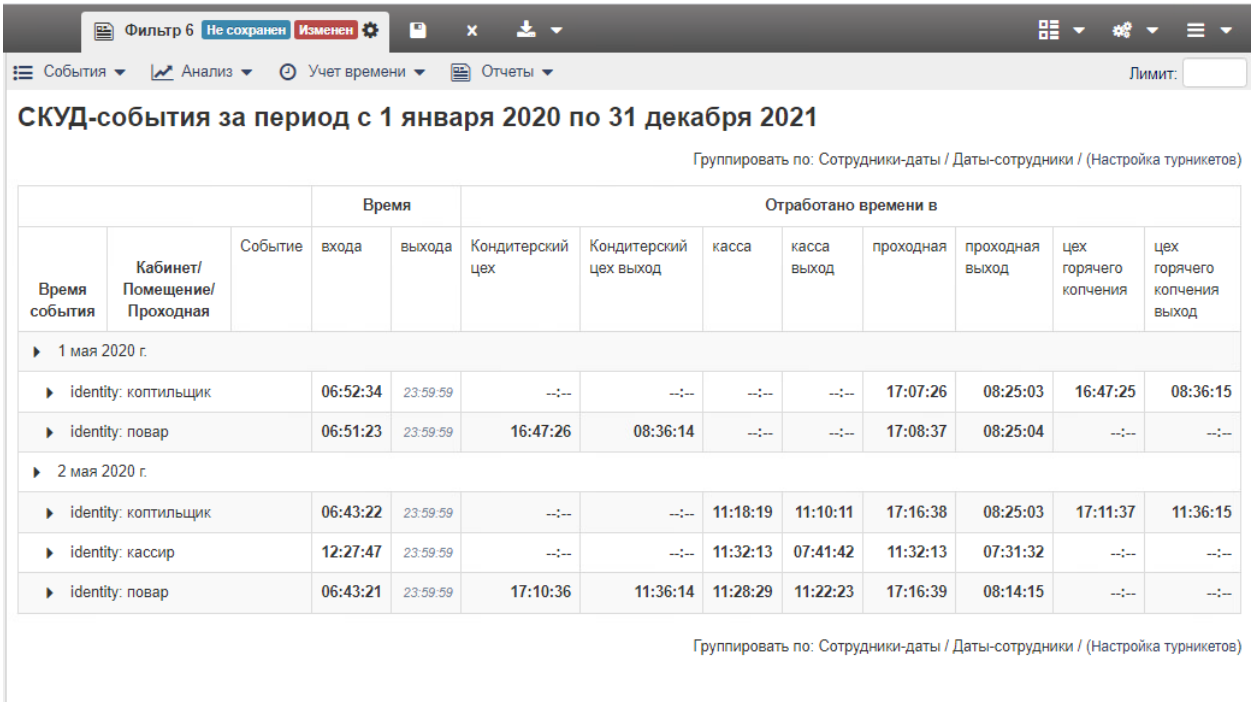
Логином нового пользователя будет строка вида:

```
identity: XXX
где XXX - значение поля "пропуск"
```

Для вновь добавленных устройств необходимо указать метку и расположение (вход/выход). Устройства с одной меткой будут объединены в отчете в единое помещение. Событие «Вход» или «выход» определяется настройкой устройства - см. карточку устройства.

Отчет

Данный отчет расположен в «Отчеты -> СКУД».



СКУД-события за период с 1 января 2020 по 31 декабря 2021

Группировать по: Сотрудники-даты / Даты-сотрудники / (Настройка турникетов)

			Время		Отработано времени в							
Время события	Кабинет/ Помещение/ Проходная	Событие	входа	выхода	Кондитерский цех	Кондитерский цех выход	касса	касса выход	проходная	проходная выход	цех горячего копчения	цех горячего копчения выход
1 мая 2020 г.												
identity: коптильщик			06:52:34	23:59:59	--:--	--:--	--:--	--:--	17:07:26	08:25:03	16:47:25	08:36:15
identity: повар			06:51:23	23:59:59	16:47:26	08:36:14	--:--	--:--	17:08:37	08:25:04	--:--	--:--
2 мая 2020 г.												
identity: коптильщик			06:43:22	23:59:59	--:--	--:--	11:18:19	11:10:11	17:16:38	08:25:03	17:11:37	11:36:15
identity: кассир			12:27:47	23:59:59	--:--	--:--	11:32:13	07:41:42	11:32:13	07:31:32	--:--	--:--
identity: повар			06:43:21	23:59:59	17:10:36	11:36:14	11:28:29	11:22:23	17:16:39	08:14:15	--:--	--:--

Группировать по: Сотрудники-даты / Даты-сотрудники / (Настройка турникетов)

События в отчете могут быть сгруппированы по дням и пользователям, либо по пользователям и дням - см.переключатель до и после таблицы. По-умолчанию события свернуты, раскрываются по клику на соответствующую пользователю/дню строку.

4.5.37 Импорт табеля 1С по отсутствию сотрудников в события календаря iBatyr Monitor

Теперь можно импортировать данные о больничных, отпусках и отгулах сотрудников из табеля 1С в календарь iBatyr Monitor.

Шаги

1. Экспортируете данные из 1С в Excel в формате XLSX.
2. Оформите данные *в правильном формате*.
3. Запустите команду импорта.

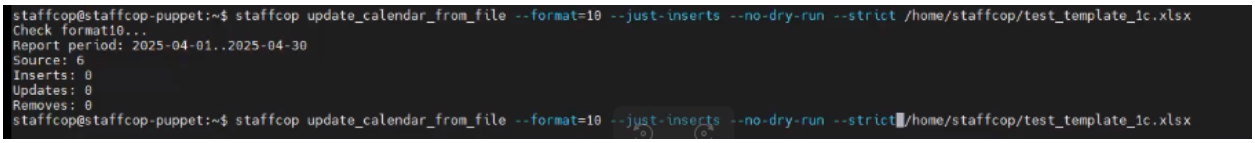
В результате скрипт проверит файл и по коду рабочего времени добавит больничные, отпуска и другие календарные события в iBatyr Monitor.

Команда импорта

```
ibatyr update_calendar_from_file --format=10 --strict --no-dry-run /path/to/file.xlsx
```

Примечание: Работает только с файлами в формате XLSX.

По итогам выполнения скрипта терминал выведет список операций:



При успешном переносе данных поле `Updates` изменится на количество календарных событий.

Описание флагов

tabularytabulary

Флаг
`--format`
`--strict`
`--data-offset`
`--ignore-worktime-codes`
`--errors-limit`
`--just-inserts`
`--no-dry-run`

Формат данных файла импорта

Примечание: Получить готовый шаблон файла импорта можно у *Технической поддержки*.

Используются только первые два листа.

Первый лист

Укажите на Листе 1 диапазон дат отчетного периода:

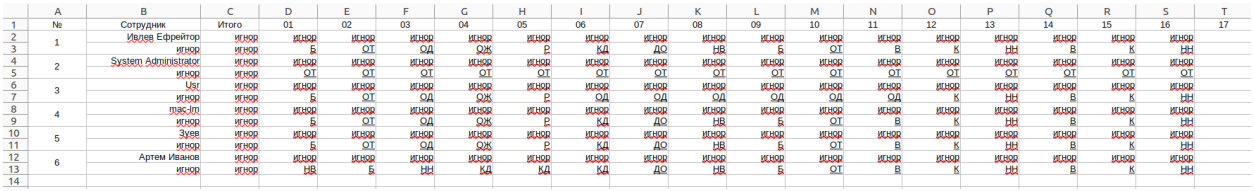
	A	B	C	D
1	**Отчётный период**			
2	с	по		
3	01.03.2025	30.03.2025		
4				
5				
6				
7				
8				
9				

- даты должны быть в формате dd.mm.yyyy: например, 12.05.2025;
- день и месяц могут быть одно- или двухзначными, но год всегда полный;
- формат даты должен быть **Текстовый**, а перед датой должна стоять кавычка ` ;
  - чтобы установить формат, перейдите в **Главная** → **Числовой формат** и выберите **Текстовый**.
- даты ищутся по ключевой фразе **Отчётный период**, на данный момент проверяются первые 20 строк.

Примечание: Во фразе **Отчётный период** должна быть буква Ё, иначе скрипт выведет ошибку парсинга и остановится.

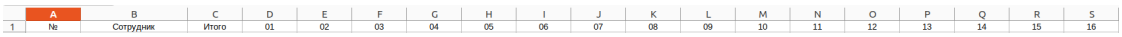
Второй лист

На Листе 2 укажите данные сотрудников.



Заголовки:

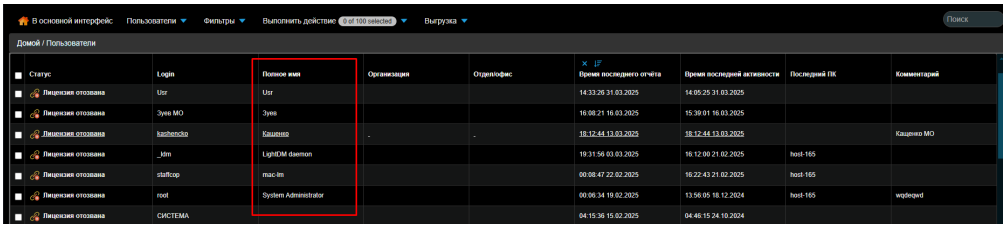
- заголовки должны располагаться в первой строке, начиная с первого столбца (ячейка A1);
- формат корректного заголовка: *№ | Сотрудник | Итого | 01 | 02 | ....*



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	№	Сотрудник	Итого	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16

Данные сотрудника:

- в первом столбце первой строки указывается номера, при этом порядок не имеет значения;
- ячейки в первых трёх столбцах могут быть объединены по вертикали;
- данные сотрудника должны занимать две строки:
  - в столбце **Сотрудник** в первой строке введите **Полное Имя** пользователя, которое указано в базе данных iBatyr Monitor:



  - во второй строке столбца **Сотрудник** и в столбце **Итого** должен стоять *игнор*;
  - в остальных столбцах второй строки должны быть данные: вещественные числа (игнорируются) или *код рабочего времени*. Каждый столбец соответствует одному дню.

Допустимые коды рабочего времени

- **Б** — больничный,
- **ОТ** — отпуск,
- **ОД** — отгул,
- **ОЖ** — ожидание,
- **Р** — работа,
- **КД** — командировка,
- **ДО** — день отдыха,
- **НВ** — неявка.

Другие коды приведут к ошибке или, при использовании флага `--ignore-worktime-codes`, будут проигнорированы.

Игнорируемые коды

Допустимы, но не отражаются в базе данных:

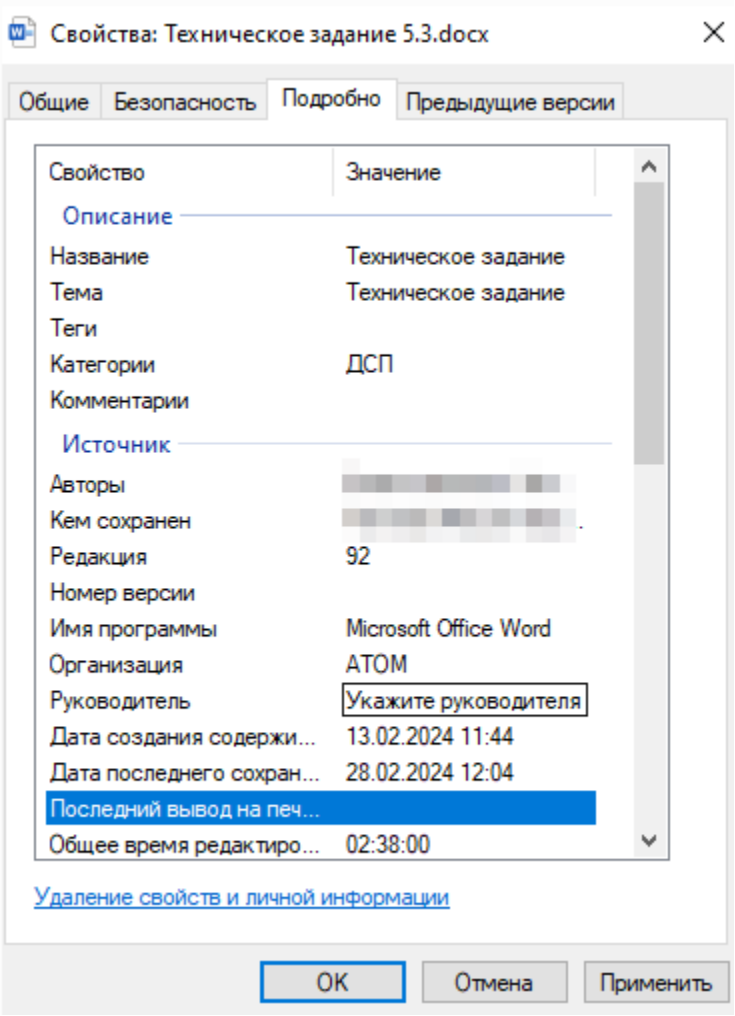
- **В** — выходной,
- **К** — командировка,
- **НН** — неявка.

4.5.38 Мониторинг и блокировка на основе метаданных офисных документов

С версии iBatyr Monitor 5.5 агент извлекает метаданные при сканировании файлов и передаёт их на сервер в виде измерения события **Файл**.

Метаданные — это данные, которые описывают свойства самого файла, но не содержат контент.

Метаданные можно использовать для более точной идентификации и блокировки файлов на рабочих местах пользователей. Используйте для этого одно из полей метаданных **Категория** (**Category**). Например, вы можете добавить в поле значение *Конфиденциально*, а затем настроить блокировку файлов, метаданные которых содержат это значение.



Примечание: Сбор метаданных для блокировки файловых операций необязателен, но рекомендуем использовать его для более точной блокировки.

Перед настройкой блокировки включите сбор метаданных.

Включение сбора метаданных

Чтобы агент начал собирать метаданные, *активируйте Файловое сканирование*. После включения сканирования агент будет присылать события типа **Файл**, у которых есть измерение **Метаданные**.

Сбор метаданных доступен только для документов в форматах:

tabularytabulary

Формат	Расширение
Microsoft Office Word	.docx
Microsoft Office Excel	.xlsx
Microsoft Office PowerPoint	.pptx
OpenOffice Text Document	.odt
OpenOffice Spreadsheet	.ods
OpenOffice Presentation	.odp

Содержание метаданных зависит от формата файла и кастомных настроек. Ниже приведены свойства, которые могут содержать метаданные:

- имя файла,
- тип файла,
- размер файла,
- дату создания,
- дату изменения,
- дату последнего доступа,
- права доступа,
- автора,
- расположение,
- категорию,
- другие свойства.

Нас интересует поле **Категория**, потому что в него вводится значение для идентификации файла.

Примечание: В зависимости от приложения поле **Категория** может отличаться. В приложениях пакета Microsoft Office уже есть поле **Категория**, а LibreOffice его нужно создать.

Настройка блокировки файлов через метаданные

Добавьте значение в метаданные, а затем на его основе настройте блокировку.

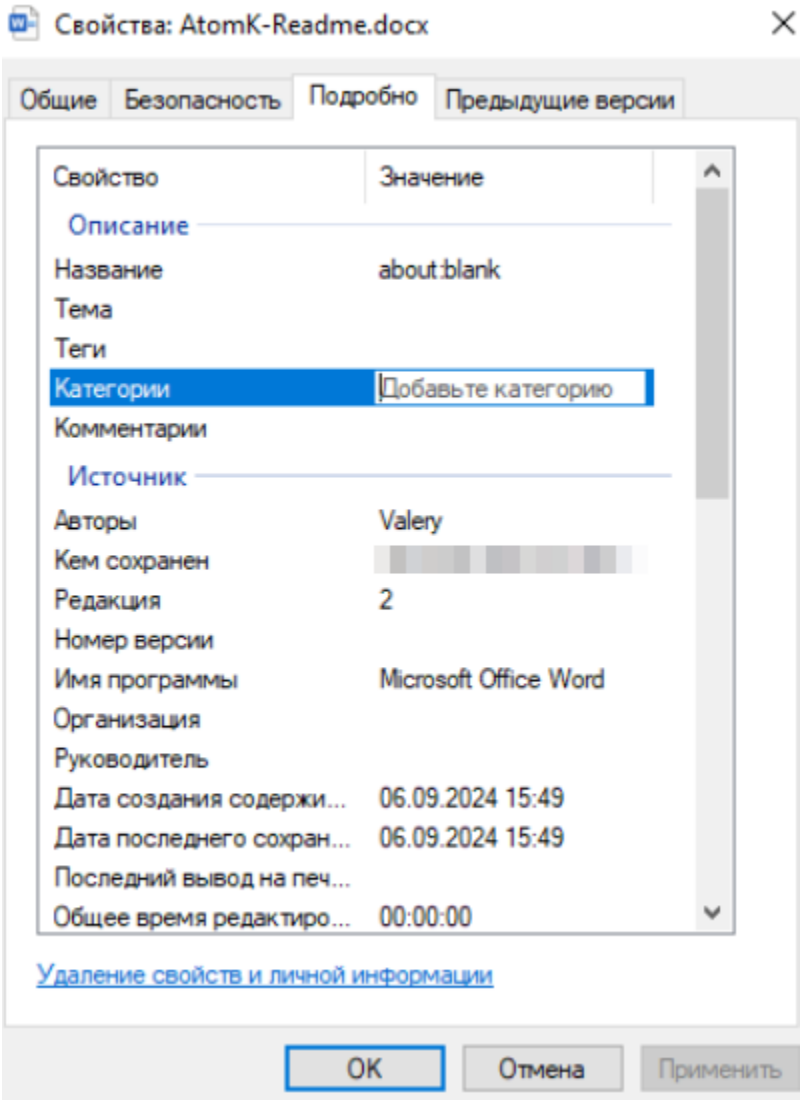
Добавьте значение в поле Category

Примечание: Перед настройкой убедитесь, что вы включили сбор метаданных *в Файловом сканировании*.

Ваши действия зависят от офисного пакета.

Microsoft Office

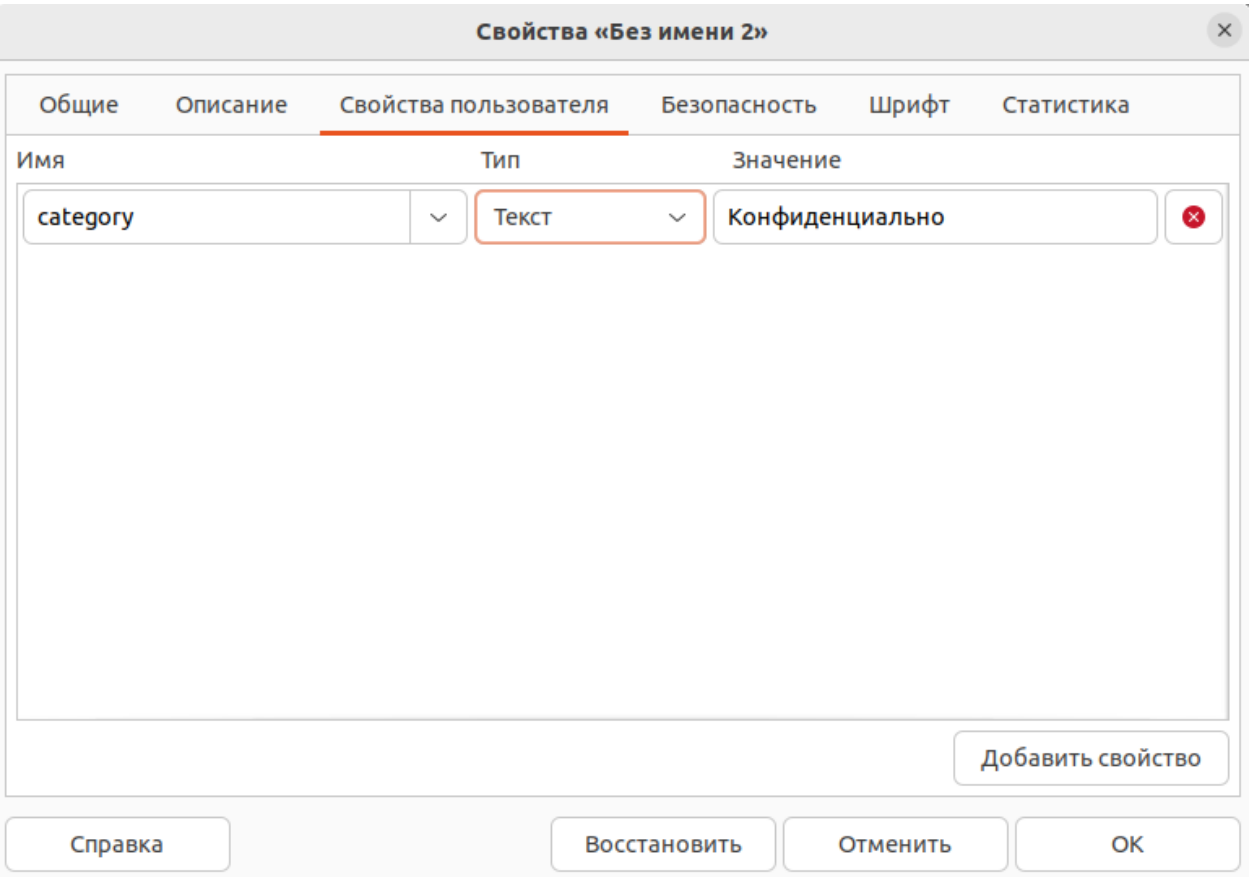
1. Откройте файл.
2. Перейдите **Файл** (**File**) → **Свойства** (**Properties**) → **Подробно** (**Summary**).
3. В поле **Категории** (**Add Propety**) введите название метки, например *Заблокировать*.
4. Сохраните изменения.



LibreOffice

1. Откройте файл.

2. Перейдите **Файл** (**File**) → **Свойства** (**Properties**) → **Дополнительные свойства** (**Custom Properties**).
3. Нажмите на **Добавить свойство** (**Add Property**).
4. В поле **Имя** (**Name**) введите с маленькой буквы *category*, в **Типе** (**Type**) выберите **Текст** (**Text**), в **Значение** (**Value**) введите название метки, например *Конфиденциально*.
5. Сохраните изменения.



Блокировка не зависит от регистра символов, например *КОНФИДЕНЦИАЛЬНО* и *Конфиденциально* расцениваются как один и тот же значение.

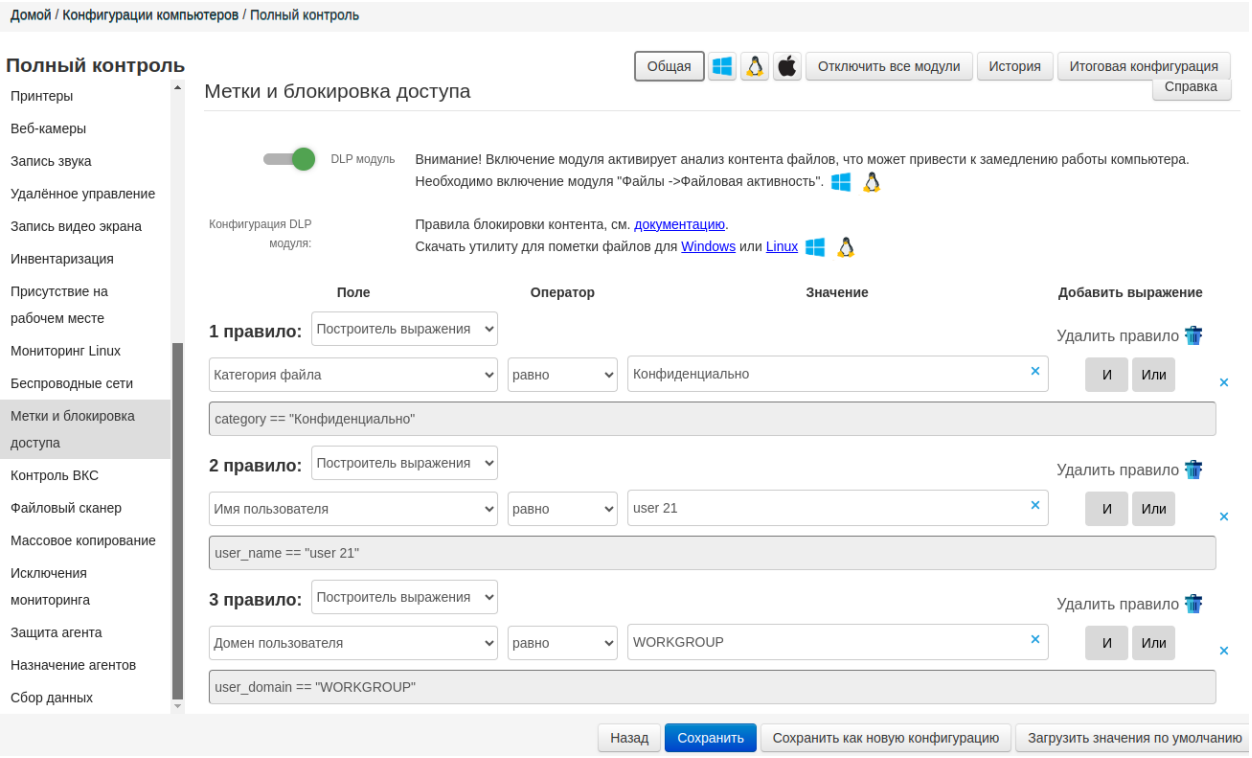
Если вы хотите присвоить полю **Категория** более одного значения, перечислите их через точку с запятой: *Конфиденциально; Важно*.

Добавьте правило блокировки в конфигурации

После добавления значения в поле **Category** файла откройте веб-интерфейс iBatyr Monitor и настройте блокировку.

1. Перейдите **Панель управления** → **Конфигурации компьютера** → *ваша конфигурация* → **Метки и блокировки доступа**.
2. Установите флажок **DLP-модуль**.
3. Нажмите **Добавить правило** +.

4. Заполните поля: **Категория файла** — **Равно** — значение поля **Категория**, в нашем случае *Конфиденциально*.
5. Добавьте при необходимости другие правила, например блокировку для конкретного пользователя или домена.
6. Сохраните изменения.



После сохранения изменений пользователь при попытке открыть файл увидит сообщение «Не удалось получить доступ к файлу».

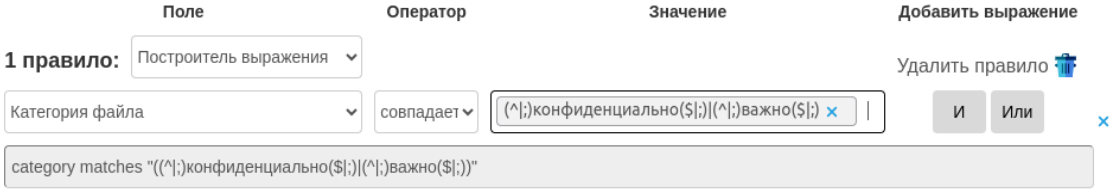
Правила блокировки для нескольких значений¶

Если вы присвоили несколько значений полю **Категория**, используйте для блокировки регулярные выражения.

1. Метаданные содержат значения *Конфиденциально; Важно*.

   Чтобы заблокировать по значению *Конфиденциально* или *Важно*, используйте оператор **Совпадает** и введите в поле **Значение**:

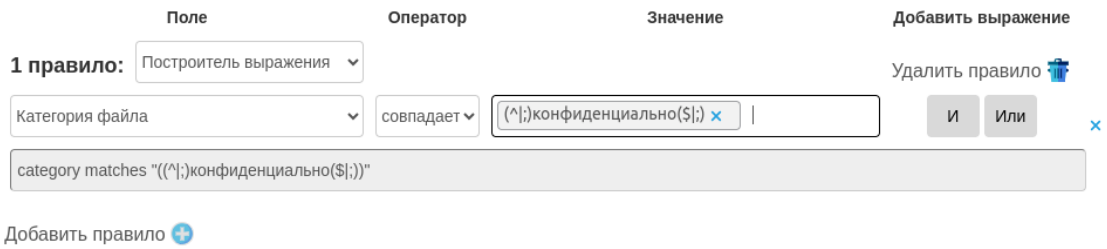
   ```
   (^|;)конфиденциально($|;)|(^|;)важно($|;)
   ```

2. Метаданные содержат значения *Конфиденциально; Важно*.

Чтобы заблокировать по значению *Конфиденциально*, используйте оператор **Совпадает** и введите в поле **Значение**:

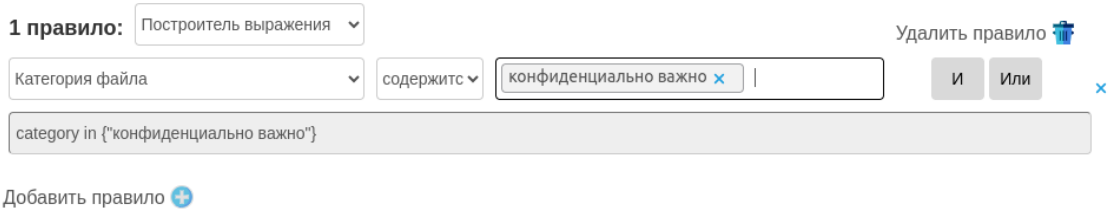
```
(^|;)конфиденциально($|;)
```



3. Метаданные содержат значения *Конфиденциально*.

   Чтобы заблокировать по значению *Конфиденциально* или *Важно*, используйте оператор **Содержится в** и введите в поле **Значение**:

```
конфиденциально важно
```



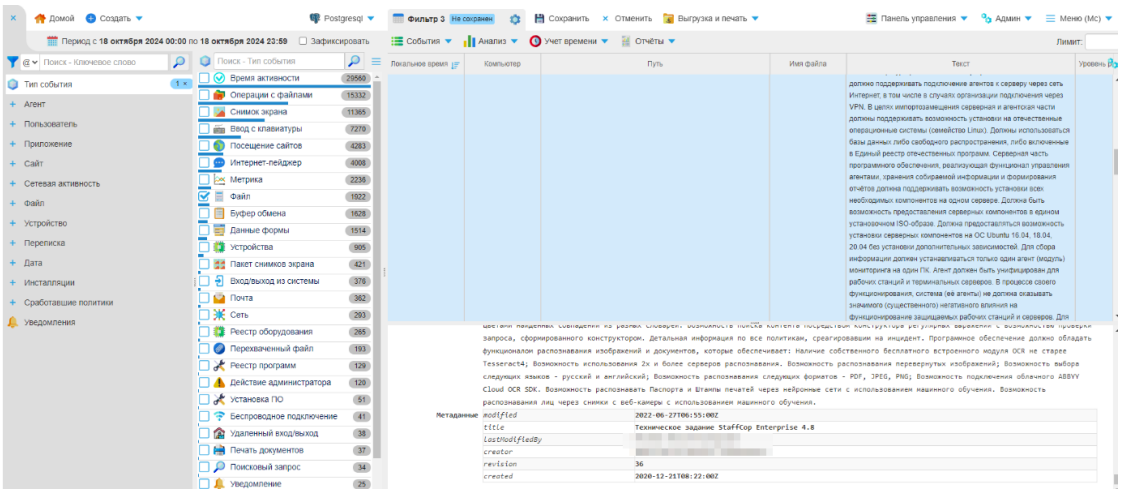
Управление метаданными

В веб-интерфейсе вы можете просматривать и фильтровать файлы по измерению **Метаданные**.

Просмотр метаданных в iBatyr Monitor

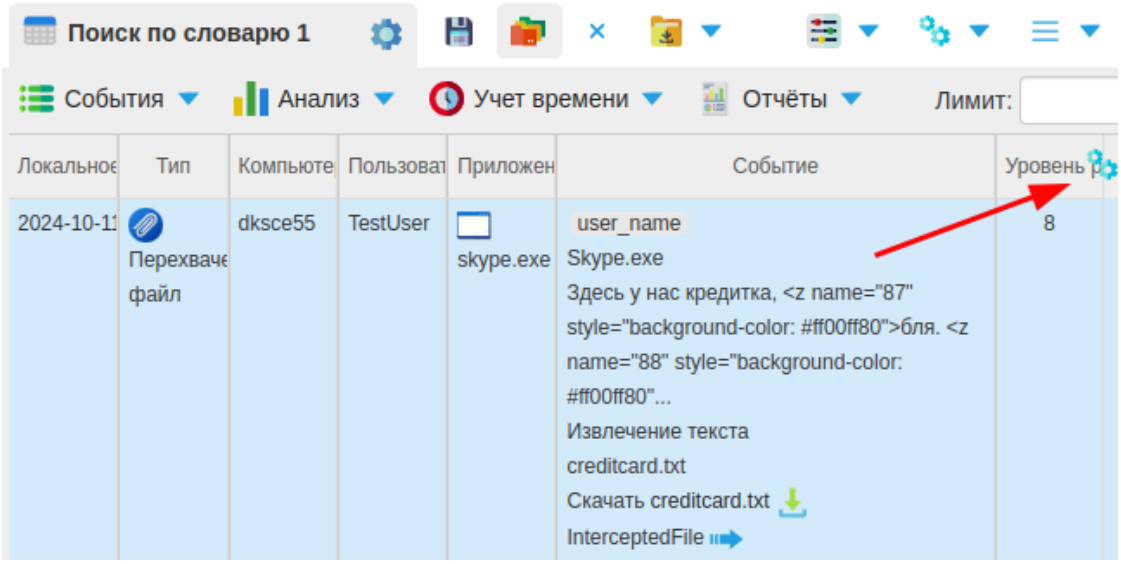
Метаданные файлов содержат информацию, которую можно использовать для мониторинга доступа, изменений и перемещения важных документов.

1. Выберите в **Конструкторе** тип события **Файл**.
2. При необходимости настройте другие измерения, например выберите компьютер, пользователя или расширение.
3. Найдите в **Линзе событий** файл.
4. Метаданные файла отображаются в информации о файле в поле **Метаданные**.

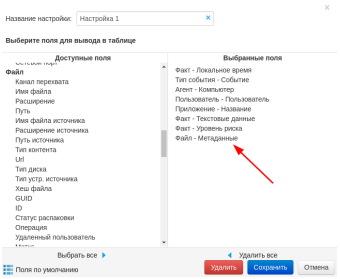


Для более удобного просмотра метаданных добавьте столбец **Метаданные** в таблицу событий:

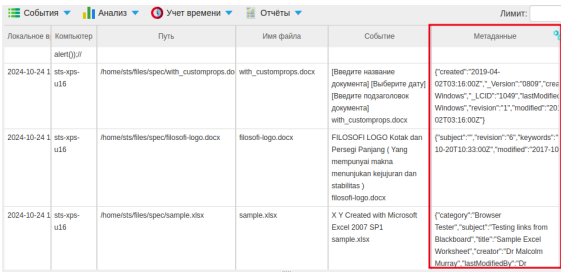
1. Нажмите на иконку с шестернями и выберите **Новая настройка**.



2. В разделе **Доступные поля** → **Файл** нажмите на строку **Метаданные**. Строка переместится в **Выбранные поля**.



3. После сохранения настройки в таблице появится столбец:



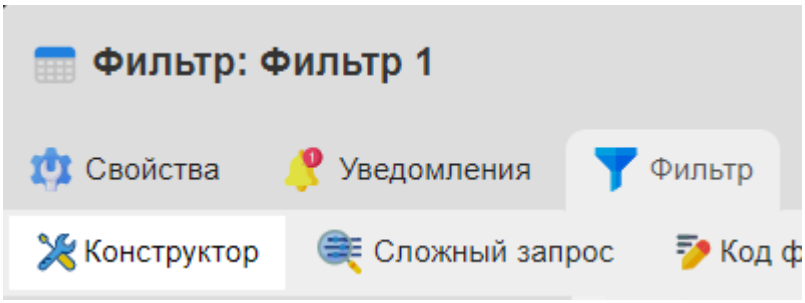
Фильтрация файлов по метаданным

Фильтрация метаданных позволяет находить файлы с нужными параметрами. Для этого можно использовать как стандартные фильтры в **Конструкторе**, так и более гибкие **Сложные запросы**.

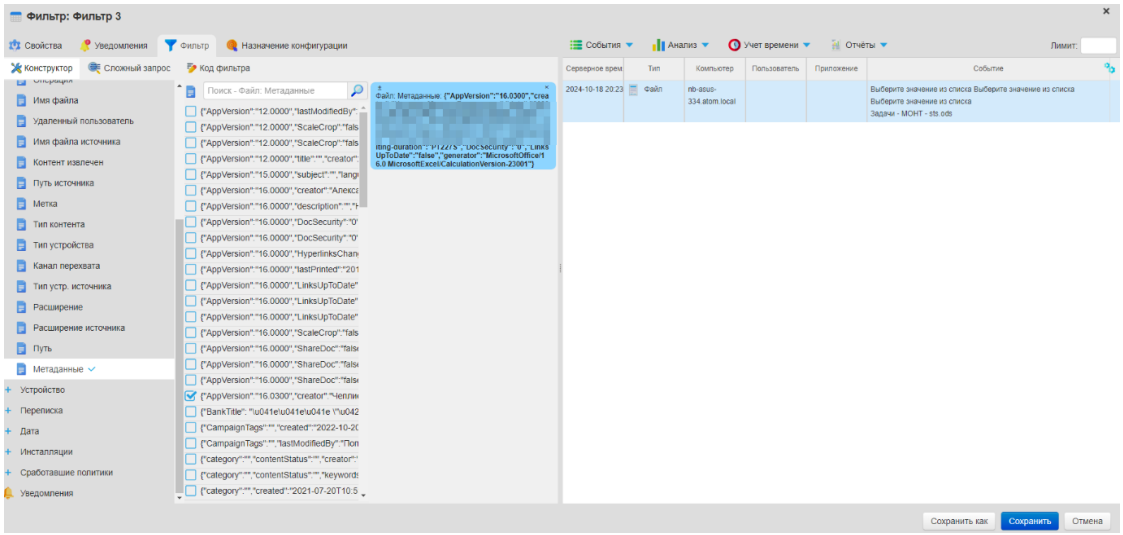
Примечание: Метаданные содержат большой объём данных, поэтому стандартные фильтры могут быть недостаточны. Для более точной работы с метаданными используйте сложные запросы с несколькими условиями.

Конструктор

1. *Откройте фильтр или создайте новый.*

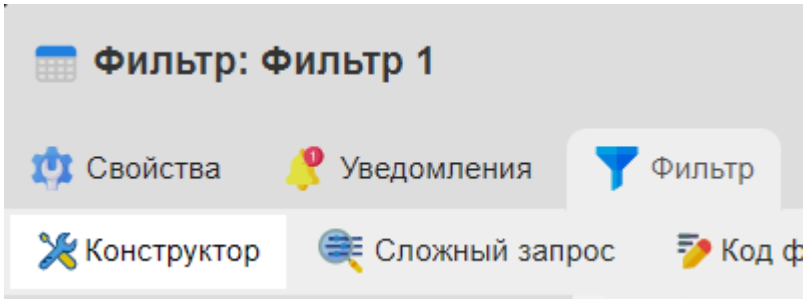


2. Перейдите во вкладку **Фильтр** → **Конструктор**.
3. Выберите в левой боковой панели **Файл**.
4. Добавьте измерение **Метаданные**.
5. При необходимости добавьте другие измерения.
6. Сохраните фильтр.

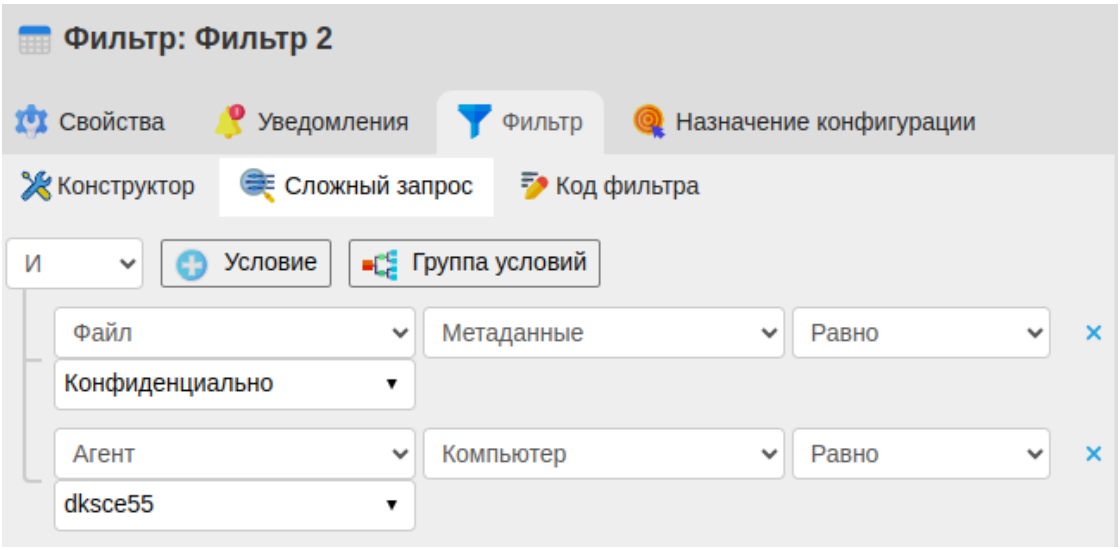


Сложный запрос

1. *Откройте фильтр или создайте новый.*



2. Перейдите во вкладку **Фильтр** → **Сложный запрос**.
3. Нажмите на кнопку +**Условие**.
4. Выставите значение **Файл** — **Метаданные** – **равно** — *значение* категории, например *Конфиденциально.*
5. При необходимости добавьте другие условия.
6. Сохраните фильтр.



4.5.39 Краулер

Содержание

- *Краулер*
  - *Принцип работы*
  - *Активация краулера*
  - *Начало работы*
  - *Фильтрация компьютеров*
  - *Сканирование файлов*
  - *Установка меток*
  - *Просмотр результатов сканирования в Конструкторе*
  - *Уведомления*
  - *Кейсы*

Краулер — компонент в составе iBatyr Monitor . Он позволяет сканировать файлы, которые находятся в состоянии покоя на компьютерах сотрудников, ставить метки на документы с конфиденциальной информацией и контролировать к ним доступ.

Требует лицензии, но в версиях iBatyr Monitor 5.5 и 5.6 предоставляется для всех клиентов в виде прототипа.

Функция доступна:

- для Windows-агентов версии **5.8.2585** и выше,
- Linux-агентов версии **0.16.18** и выше.

Принцип работы

1. **Сканирование файлов**: запустите сканирование файлов на компьютерах сотрудников.
2. **Установка меток**: после сканирования установите метки в выбранные файлы.

Примечание: При сканировании сервер находит файлы с расширениями: .pdf, .docx, .doc, .xlsx, .xls, .pptx, .ppt, .odt, .ods, .odp, .csv, .txt, .rtf. Установка меток возможна для файлов с расширениями: .docx, .doc, .xlsx, .pptx, .odt, .ods, .odp.

---

3. **Контроль доступа**: на основе меток настройте дополнительные меры защиты. Например, заблокируйте доступ к файлу с меткой *Конфиденциально* при копировании на флешку.
4. **Настройка уведомлений**: настройте уведомления, чтобы получать алерты о нерегламентированном перемещении и изменении файлов.

Таким образом можно предотвратить неправомерное использование документов.

Активация краулера

По умолчанию краулер выключен. Чтобы его активировать, откройте терминал на сервере и выполните:

1. Откройте файл *config*:

```
sudo nano /etc/ibatyr/config
```

2. Добавьте в конец файла строку и сохраните изменения:

```
FILE_TAG_MANAGER = True
```

3. Перезапустите сервер:

```
ibatyr restart
```

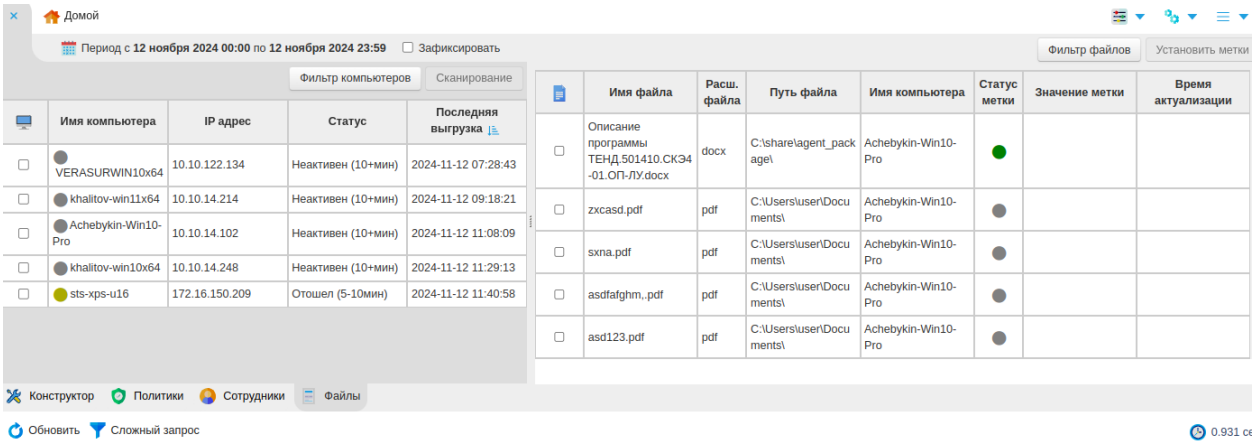
После этого во вкладке **Файлы** вместо дерева каталогов появятся инструменты централизованного сканирования.

Внимание: После активации краулера в конфигурации компьютеров исчезнет раздел *Файловый сканер*.

Начало работы

При клике на вкладку **Файлы** откроется страница для сканирования файлов и установки меток.

Изначально список файлов пустой. Файлы появятся после сканирования. Если раньше вы проводили сканирование через конфигурацию компьютера, список будет заполнен, но информация в нем может быть устаревшей.



Список компьютеров

В левой части вкладки **Файлы** располагается список компьютеров.

В списке отображаются компьютеры, который соответствуют **условиям**:

- на компьютере установлен агент;
- версия агента поддерживает метки;
- время передачи данных с компьютера на сервер соответствует дате в датапикере.

По умолчанию компьютеры отсортированы по времени последнего сканирования от новых к старым. Если время сканирования одинаковое или машина не отсканирована, компьютеры сортируются по имени.

В таблице компьютеров приведены:

- имя компьютера,
- IP-адрес,
- статус доступности,
- время последней передачи данных от агента на сервер.

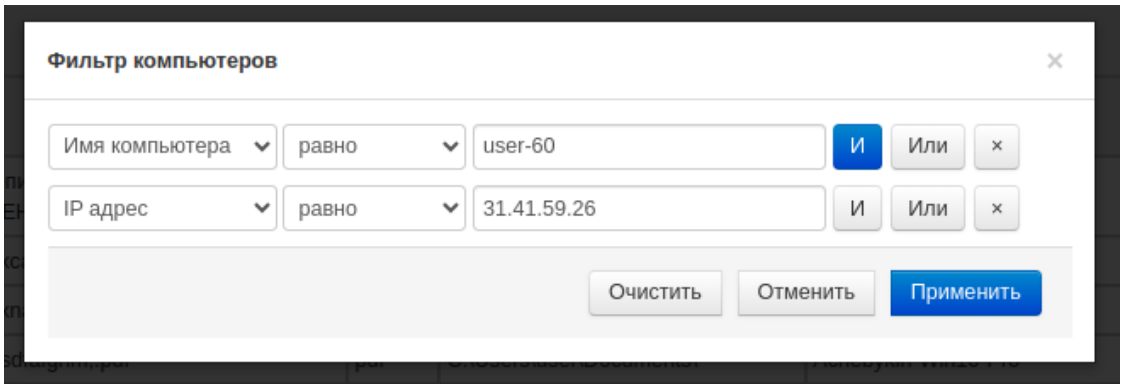
Фильтрация компьютеров

Вы можете отфильтровать компьютеры для сканирования по двум измерениям:

- по имени компьютера,
- IP-адресу.

Чтобы отфильтровать компьютеры:

1. Нажмите на кнопку **Фильтр компьютеров**. Откроется окно фильтрации.
2. Выберите *измерение* — *оператор* — *значение*. Например, для сканирования компьютеров подсети отфильтруйте список по IP.
3. При необходимости добавьте дополнительные условия с помощью кнопок **И** / **ИЛИ**.



4. Нажмите **Применить**.

После этого в списке останутся только отфильтрованные компьютеры.

Сканирование файлов

Чтобы запустить сканирование файлов:

1. Выберите компьютеры в списке или нажмите на иконку компьютера для сканирования всех машин. Если не выбран ни один компьютер, сервер отсканирует все активные компьютеры.
2. Нажмите кнопку **Сканировать**. Откроется окно настройки сканирования.
3. Выберите форматы документов, которые хотите отсканировать:
   - MS Word,
   - MS Power Point,
   - MS Excel,
   - OpenOffice Writer,
   - OpenOffice Impress,
   - OpenOffice Calc,
   - XPS,
   - RTF,
   - PDF,
   - TXT и CSV.

   Кнопка **Инверсия** позволяет выбрать все невыбранные форматы и дезактивирует невыбранные.
4. При необходимости запретите или, наоборот, включите сканирование файлов по определенным путям. Для этого укажите путь в полях **Запретить** и **Разрешить**.

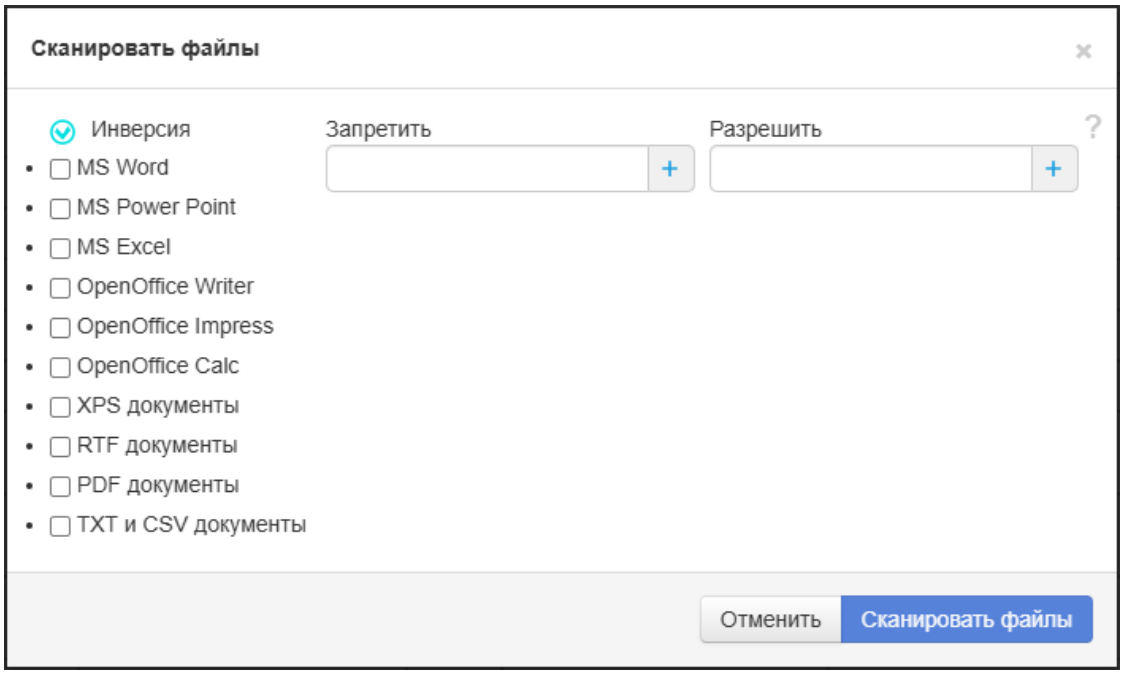
Примечание: Краулер в версии 5.6 сканирует директории без ограничений, игнорируя правила из *глобальной конфигурации*. Чтобы сканирование не генерировало огромное количество событий, добавьте в **Запретить** такие системные директории, как:

```
C:\Windows\*
C:\Documents and Settings\*\Application Data\*
```

(continues on next page)

(продолжение с предыдущей страницы)

```
C:\Documents and Settings\*\Local Settings\Temp\*
C:\Program Files\*
C:\Program Files (x86)\*
C:\ProgramData\*
*AppData*
```



6. Нажмите кнопку **Сканировать**.

После этого сервер начнет сканирование. Компьютеры, которые находятся не в сети, будут поставлены в очередь. Краулер просканирует их по мере появления в сети, поэтому сканирование может занять время.

Отсканированные файлы отобразятся в правой части экрана. После сканирования при выборе компьютеров в списке отобразятся только найденные на выбранных машинах файлы.

Фильтрация файлов

Чтобы отфильтровать отсканированные файлы:

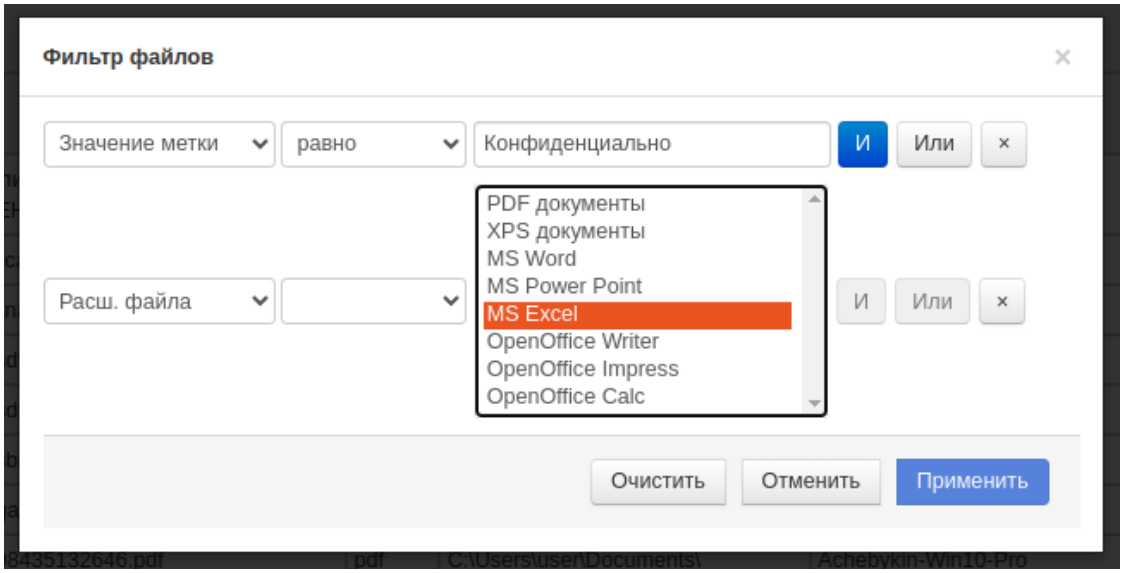
1. Нажмите на кнопку **Фильтр файлов** в верхнем правом углу.
2. Выберите *измерение* — *оператор* — *значение*. Например, чтобы найти файлы пользователя, используйте файловый путь, который содержит доменный логин пользователя.

   Фильтрация доступна по измерениям:

   - имя файла,
   - расширение файла,
   - путь файла,
   - имя компьютера,

- *статус метки*;
- значение метки.

3. При необходимости добавьте другие условия с помощью кнопок **И** / **ИЛИ**.



4. Примените фильтр.

В таблице отобразятся отфильтрованные файлы.

Установка меток

Чтобы установить метку в файлах:

1. Во вкладке **Файлы** выберите из списка файлы для установки метки.
2. Нажмите кнопку **Установить метку**, откроется модальное окно.
3. Введите текст метки в поле, например *Конфиденциально*. Если оставить поле пустым, сервер установит метку *NULL*.
4. Нажмите **Выполнить**.

После этого сервер запустит установку метки. Файлам на компьютерах вне сети метки будут присвоены по мере появления в сети.

У меток есть статусы:

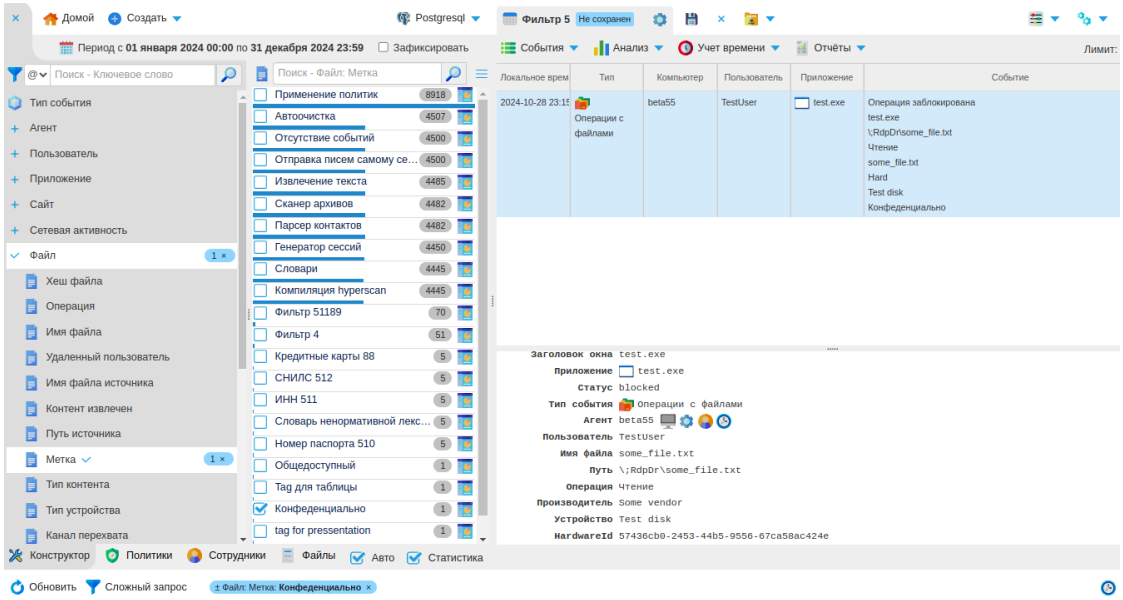
- **Актуально** — метка присвоена;
- **Ожидает** — метка в процессе присвоения, например, из-за того, что компьютер вне сети; после того, как агент установит метку, статус поменяется на **Актуально**;
- **Невозможно поставить** — относится к PDF-файлам, на которых установка меток невозможна.

Просмотр результатов сканирования в Конструкторе

Каждый файл сохраняется в событии **Перехваченный файл**.

Чтобы посмотреть файлы:

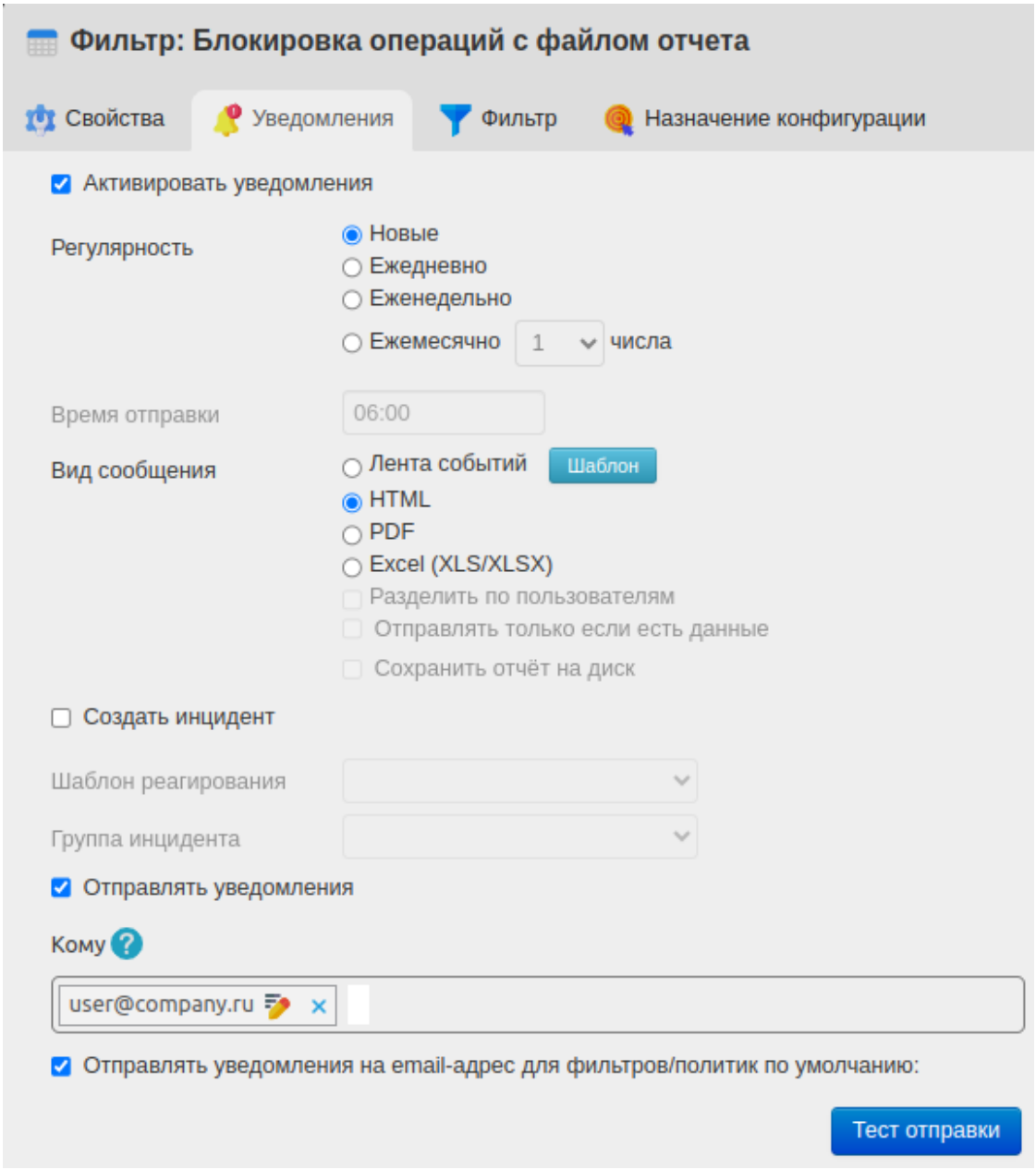
1. Перейдите во вкладку **Конструктор**.
2. Выберите в конструкторе **Файл** и настройте измерения. Например, найдите файл с помощью измерения **Метка**. В **Линзе событий** отобразятся найденные файлы.



Уведомления

Вы можете настроить уведомления в **Фильтрах**. Например, чтобы уведомления приходило при попытке передачи файла через мессенджер:

1. Создайте фильтр на главной странице
2. Во вкладке **Свойства** добавьте название фильтра.
3. Во вкладке **Уведомления** настройте уведомления и укажите почту для отправки.



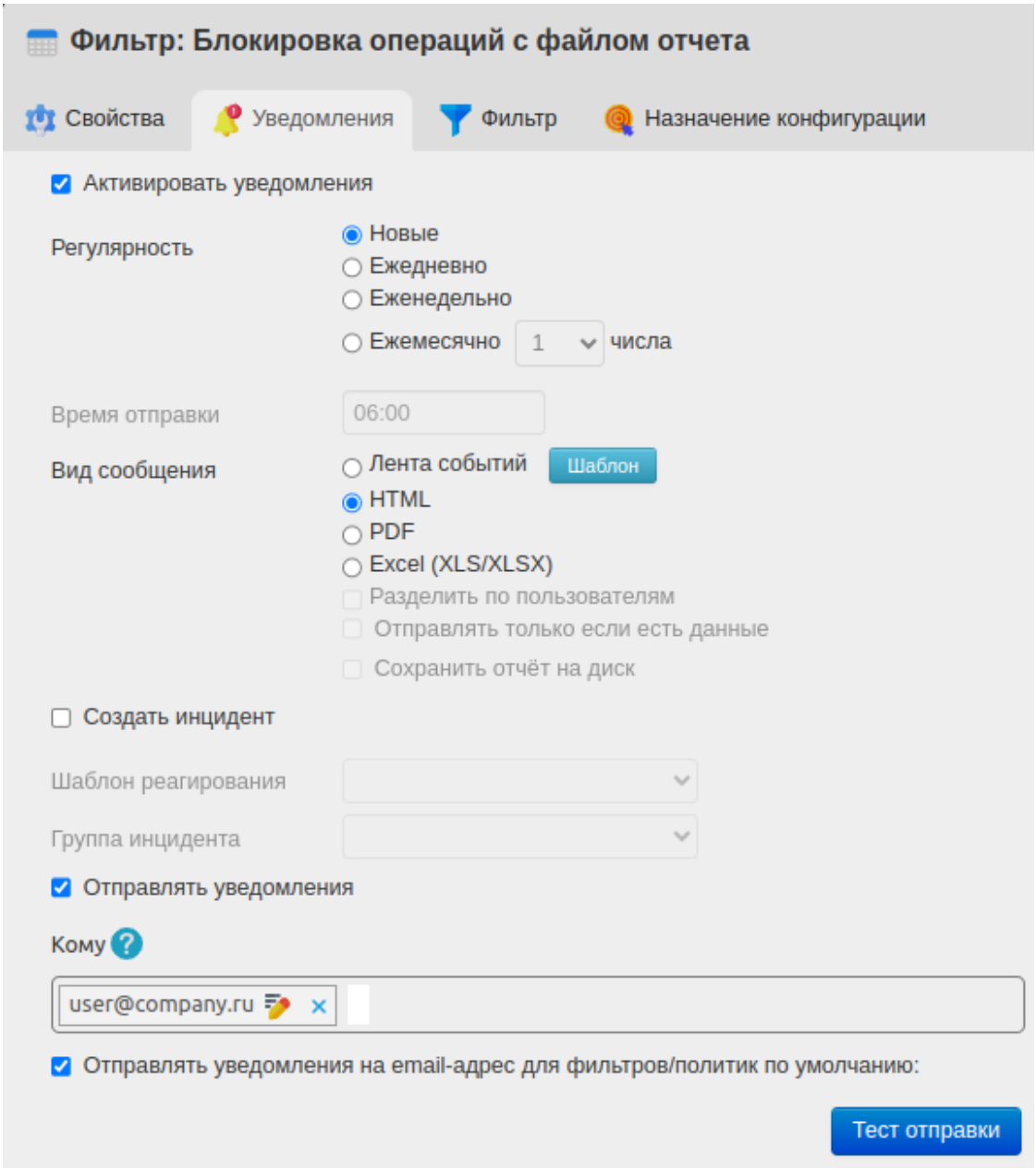
4. Во вкладке **Фильтр** выберите **Файл** → **Метка** → *имя метки*.
5. В **Приложении** выберите приложение, о передаче файлов в котором будет приходить уведомление, например *skype*.
6. При необходимости добавьте другие условия, например **Имя пользователя**.
7. Сохраните фильтр.

Кейсы

Выявить документы с грифом ДСП

Чтобы найти документы с грифом **ДСП** (документы с ограниченным доступом) на компьютерах пользователей из определенного департамента:

1. Откройте вкладку **Файлы**.
2. Отфильтруйте список компьютеров.
   - если отдел имеет свою подсеть, в фильтре укажите **IP** — **содержит** — *адрес подсети*;
   - если подсети нет, выберите все компьютеры.
3. Нажмите **Сканировать**.
4. В настройках сканирования выберите форматы файлов и пути, по которым могут находиться документы с грифом «ДСП».
   - рекомендуем отключить форматы ppt и xls, так как вряд ли такие документы будут иметь гриф «ДСП».
   - выбирайте директории пользователей — например, папку Users, — а системные папки Windows и Program Files исключите.
5. После завершения сканирования перейдите в конструктор, в **Агенте** нажмите **IP** и выберите подсеть.
   - если подсети нет, можете отфильтровать компьютеры по другим параметрам — например по сотрудникам или группе.
6. Выберите в конструкторе **Файл**.
7. В поиске по ключевому слову введите «ДСП». В Линзе событий отобразятся файлы с грифом «ДСП».



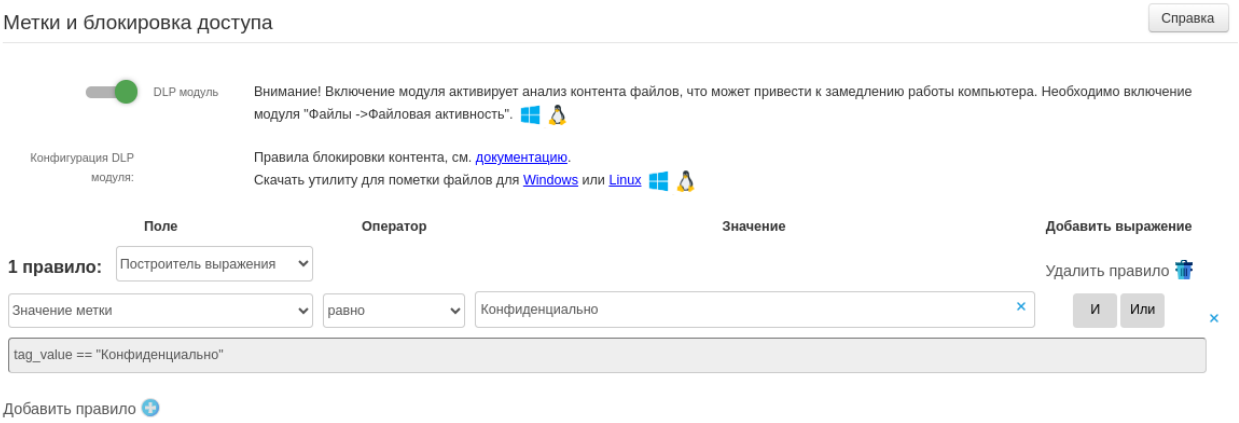
После этого в Линзе отобразятся файлы с грифом «ДСП».

Заблокировать загрузку отмеченного файла на флешку

Файлы с указанной меткой будут блокироваться при попытке загрузки на флешку.

1. Нажмите на кнопку **Домой** в левом верхнем углу, чтобы вернуться в основной интерфейс.
2. Перейдите **Панель управления** → **Конфигурации компьютеров** → *ваша конфигурация*.
3. Выберите **Метки и блокировка доступа**.
4. Убедитесь, что ползунок **Модуль DLP** находится в активном положении.
5. Нажмите **Добавить правило**+.

6. Добавьте в правило **Значение ветки** — *равно* — *имя метки*.
7. Сохраните настройки.



4.5.40 На клонированной системе данные приходят от имени одного пользователя

Проблема

После установки Windows-агента из золотого образа данные приходят от имени одного и того же пользователя.

Причина

При развертывании золотого образа стандартные локальные пользователи получают одинаковый SID, что приводит к отправке данных от имени одного пользователя. В результате нельзя определить, кто именно выполнил те или иные действия.

SID (Security Identifier) — уникальный идентификатор безопасности для различения учетных записей пользователей в Windows. Одинаковый SID появляется, потому что золотой образ — это точная копия системы, которая включает все настройки и идентификаторы. Windows не изменяет SID автоматически при клонировании.

Кроме того, золотой образ может содержать аппаратный идентификатор (**HWID**), который будет одинаков для всех компьютеров после установки агента.

Решение

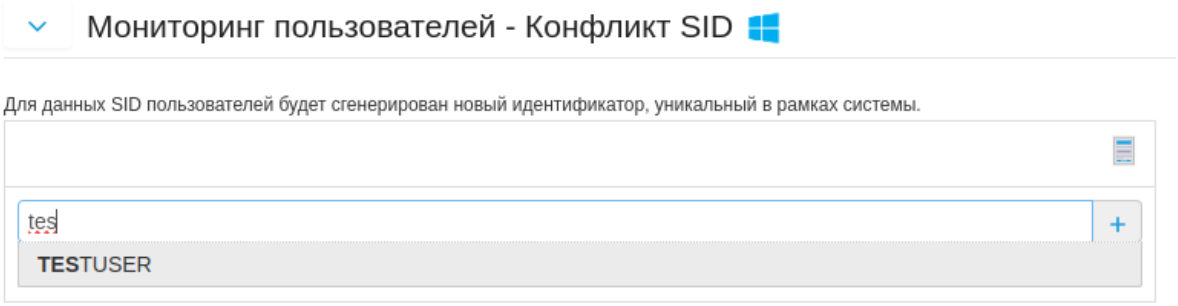
Установите новый уникальный идентификатор для каждого пользователя, основанный на комбинации аппаратного идентификатора компьютера (Hardware ID) и SID пользователя. Идентификатор HWID-SID позволяет различать пользователей, даже если у них одинаковое имя пользователя.

Возможны два сценария:

1. **Золотой образ содержит HWID**: сначала установите для компьютера уникальный HWID *по инструкции*. После этого присвойте пользователю уникальный идентификатор SID-HWID.
2. **Золотой образ без HWID**: сразу установите для пользователя HWID-SID.

Установка уникальных идентификаторов HWID-SID

1. Перейдите **Панель управления** → **Глобальная конфигурация**.
2. Найдите в списке **Мониторинг пользователей** — **Конфликт SID**.
3. С помощью поля **Разрешить** поочередно добавьте в список имена пользователей с одинаковым SID.



4. Сохраните изменения.
5. Перезагрузите сервер:

```
ibatyr restart
```

Результат: одинаковый SID изменится на уникальную для каждого компьютера пару HWID-SID, которая позволит идентифицировать пользователей.

4.6 Учёт рабочего времени для сотрудников на «удалёнке»

4.6.1 Введение

Работа без необходимости ежедневно присутствовать в офисе предприятия, на сегодняшний момент стала очень актуальной.

Исследования показывают, что на удалённую работу можно перевести как минимум 90% офисного персонала. Однако в этом случае возникает важный вопрос: как установить, чем занимается сотрудник на удалёнке — решением поставленных задач или просмотром развлекательных ресурсов?

Именно этому вопросу — как собрать информацию о деятельности коллег в рабочее время с помощью iBatyrMonitor , какие отчёты можно получить, как их интерпретировать — и будет посвящена настоящая статья.

Для начала работы нам понадобятся:

1. *Установленный, активированный и настроенный* сервер iBatyr Monitor . IP-адрес сервера определён, веб-интерфейс доступен, логин и пароль администратора известны.
2. *Корректно установленные* на рабочие станции пользователей агенты. По умолчанию, агенты начинают передачу информации сразу же после установки.

4.6.2 Учёт рабочего времени. Работа с календарём и расписанием

Конфигурация агента для учёта рабочего времени

Для учёта рабочего времени сотрудника используйте созданную по умолчанию конфигурацию **Учёт рабочего времени**. Она не требует значительных ресурсов от машины и не нагружает агент.

Список доступных конфигураций доступен в разделе **Панель управления** → **Конфигурации компьютеров**. При необходимости можно внести изменения в имеющиеся конфигурации и затем уже передать новую конфигурацию агентам.

Настройка календаря

Для корректной работы системы учёта рабочего времени настройте производственный календарь в разделе **Админ** → **Календарь**.

По умолчанию всем дням текущего месяца присваивается базовое рабочее расписание. Можно выделить один день или группу дней в календаре, и отредактировать их расписание для всех сотрудников либо для одного из отделов. Можно даже создать индивидуальный календарь для конкретного сотрудника.

Каждый день может быть отмечен как *Праздник* или *Рабочий*, если календарь назначается для подразделения или всех сотрудников. Для отдельного сотрудника день можно определить как входящий в отпуск или отгул. Также можно объявить выходной день (субботу или воскресенье) рабочим.

Таким образом можно настроить все дни в соответствии с производственным календарём. Только в этом случае гарантируется, что модуль учёта рабочего времени обработает все события, которые произошли в дни и часы, объявленные рабочими. Для всех остальных дней анализ событий не проводится, и в итоговые отчёты информация о них не попадёт.

Настройка рабочего расписания

Календарь содержит информацию из расписания, используемого по умолчанию: рабочий день начинается с 9:00 и заканчивается в 18:00, без указания точного времени обеденного перерыва. Это не всегда удобно: в учётную аналитику попадают абсолютно все события, включая произошедшие в то время, когда сотрудник обедает, а если он ушёл на перерыв, то это записывается как простой. Кроме того, существуют сотрудники, работающие в разные смены; им нужно назначать другое рабочее время.

Чтобы назначать каждому пользователю (или группе пользователей) специфические расписания, используйте разделы **Админ** → **Рабочее расписание** и **Админ** → **Назначение расписаний**.

В разделе **Рабочее расписание** представлен список расписаний, созданных на сервере. В открывшемся окне можно:

- создавать новые раписания;
- редактировать уже созданные расписания;
- задать расписание для всей рабочей недели или для каждого дня отдельно.

В разделе **Назначение расписаний** можно связать созданное ранее расписание с компьютером, отделом или пользователем.

Примечание: Обратите внимание, что все вышеописанные настройки будут успешно выполнены только в том случае, если правильно настроены профили пользователей: все поля (отдел, Ф.И.О.,

должность и т. д.) должны быть заполнены вручную или загружены из домена при синхронизации учётных записей.

4.6.3 Политики эффективности. Категоризация ресурсов

Сервер iBatyr Monitor предоставляет инструменты, которые позволяют в автоматическом режиме обрабатывать поступающие данные, сохранять полученные результаты и представлять их в удобном для восприятия виде. Эти инструменты называются **Политиками**.

Политика — именованный фильтр, который запускается в автоматическом режиме на сервере, обрабатывает поступившие от агентов события и формирует данные для отчётов в зависимости от заданных критериев. Политика может быть предустановленной (из коробки) или созданной администратором системы.

Продуктивность — качественный показатель оценки, определяющий, как веб-ресурс или приложение соотносятся с рабочей деятельностью сотрудника. Возможные значения продуктивности:

tabularytabulary

Значение
Премиально
Продуктивно
Нейтрально
Непродуктивно
Инцидент

Примечание: Категории ресурсов зависят от содержания работы сотрудника. Например, для спортивного журналиста посещение веб-сайта букмекерского агентства, принимающего ставки на исходы футбольных матчей, будет Продуктивным, а для рядового бухгалтера крупной компании может быть даже Инцидентом.

В ленточных графиках для наглядности категории ресурсов выделены цветом:

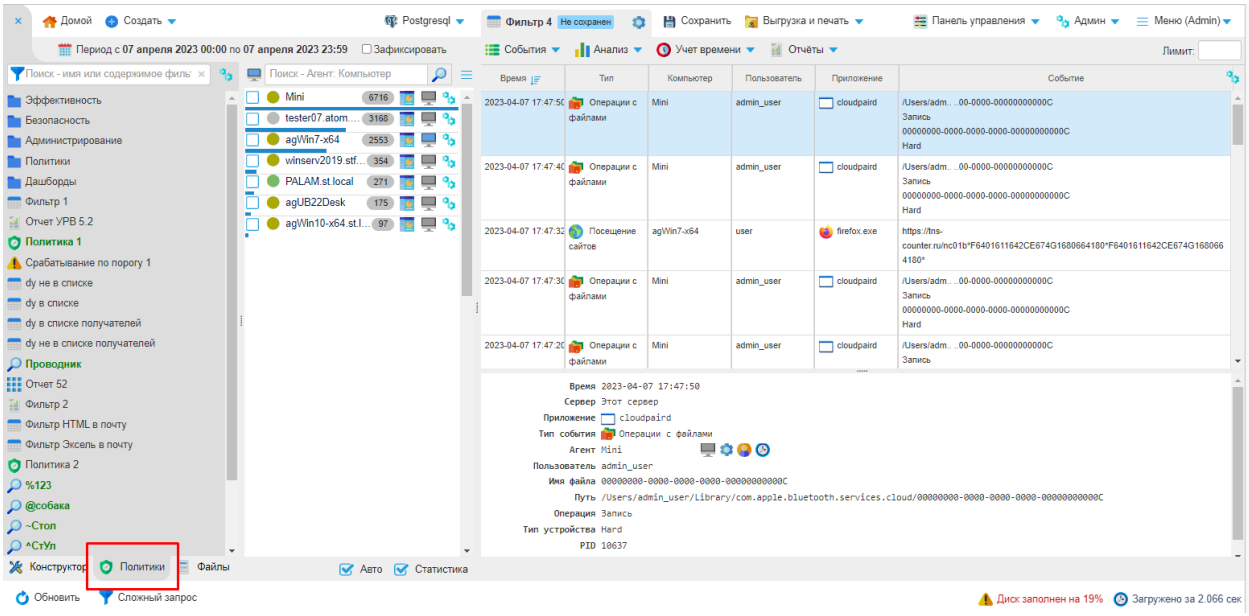
- **Премиально** — жёлтый;
- **Продуктивно** — зелёный;
- **Нейтрально** — серый;
- **Непродуктивно** — бледно-красный;
- **Инцидент** — ярко-красный;
- **Все остальное** — фиолетовый.

Эффективность — качественный и количественный индикатор, который показывает, какой процент рабочего времени сотрудник уделяет непосредственно работе.

Предопределённые политики. Продуктивность

iBatyr Monitor предлагает несколько предустановленных политик. С системой учёта рабочего времени связаны только политики продуктивности.

Группа политик продуктивности находится на вкладке **Политики**.



В папке **Эффективность** содержатся отчёты, имеющие отношение к рабочему времени. Для доступа к политикам обработки данных выберите каталог **Политики продуктивност**.

Все политики и категории ресурсов, находящиеся в них, являются предопределёнными (т. е. содержащимися на сервере «из коробки» после установки программного комплекса). Они могут быть отредактированы или отключены, но удалить их нельзя.

Создание политики учёта рабочего времени

В iBatyr Monitor есть возможность создания собственной политики учёта рабочего времени. Такая политика будет размещена в отдельной папке.

Создаётся новая пользовательская политика на вкладке фильтров базового экрана веб-интерфейса (см. рис. 3) с помощью кнопки **Создать** (значок в виде страницы с загнутым углом вверху). Как уже было отмечено, процесс полностью аналогичен редактированию предопределённой политики. После сохранения собственная политика размещается в папке самого верхнего уровня. В дальнейшем с помощью операций создания папок (вызываемых той же самой кнопкой) и перемещения политик между папками можно разместить их так, как удобно. На срабатывание политики её размещение не влияет.

Категории веб-ресурсов

Описания всех категорий веб-ресурсов имеют одинаковую структуру и дают возможность изменять базовые свойства политики (название, категория — продуктив / непродуктив, — признак активности политики, объём обрабатываемых событий — с момента изменения настроек политики или за весь период), а также настраивать уведомления о срабатывании: «из коробки» последние отключены.

Для того чтобы организовать рассылку уведомлений о срабатывании политик, сначала нужно настроить подключение сервера iBatyr Monitor к почтовому серверу. Решение этой задачи подробно описано в документации по iBatyr Monitor. Рекомендуется для рассылки уведомлений создать отдельного пользователя почтовой системы.

Политика содержит фильтр, который может быть настроен несколькими способами: с помощью структурированного «Сложного запроса», как в «Конструкторе» или путём редактирования текстового кода фильтра. Разница состоит в следующем: «Конструктор» основывается на уже собранных данных, а «Сложный запрос» позволяет сконфигурировать фильтр политики до сбора агентами информации о событиях; допускается одновременно настроить и фильтр «Конструктора», и «Сложный». Править текстовый код фильтра не рекомендуется вообще — он создаётся автоматически.

Категории приложений

Работа с категориями приложений практически не отличается от работы с категориями веб-ресурсов. Отличия есть только в событиях, которые обрабатываются политиками: здесь это — имена приложений, а не сайтов из адресов веб-страниц.

Исторически сложилось так, что при формировании фильтров в предопределённых политиках по приложениям использовался «Конструктор», а не технология «Сложного фильтра». В этом случае имена приложений задаются жёстко, причём из списка имён, уже обнаруженных в событиях, и достаточно изменить имя приложения, чтобы фильтр уже не сработал. Соответственно, использование приложения, которое, например, считается инцидентом, может не быть обнаружено.

Чтобы избежать такой ситуации, рекомендуется отредактировать политику, перейдя с фильтра, задаваемого в «Конструкторе», на фильтр «Сложный запрос»: там можно задавать условия на «неточное» имя, когда последнее включает в себя некоторую строку. В таком случае политика сработает при обнаружении агентом заданной строки в имени приложения.

4.6.4 Построение отчётов по учёту рабочего времени в программном комплексе iBatyr Monitor

Для того чтобы отчёты были точными и объективно отображали существующую на предприятии ситуацию с использованием рабочего времени сотрудниками, нужно убедиться, что календарь и все рабочие расписания настроены согласно реальным рабочим графикам.

Автор особо отмечает, что этот раздел описывает только формирование отчётов и их выгрузку. Анализу и интерпретации отчётов посвящена отдельная часть статьи.

Задание периода времени для построения отчётов

Все отчёты строятся за период времени, который установлен в веб-интерфейсе (рис. 4, выделен зелёной рамкой; серыми прямоугольниками на дальнейших иллюстрациях закрыты персональные данные пользователей).

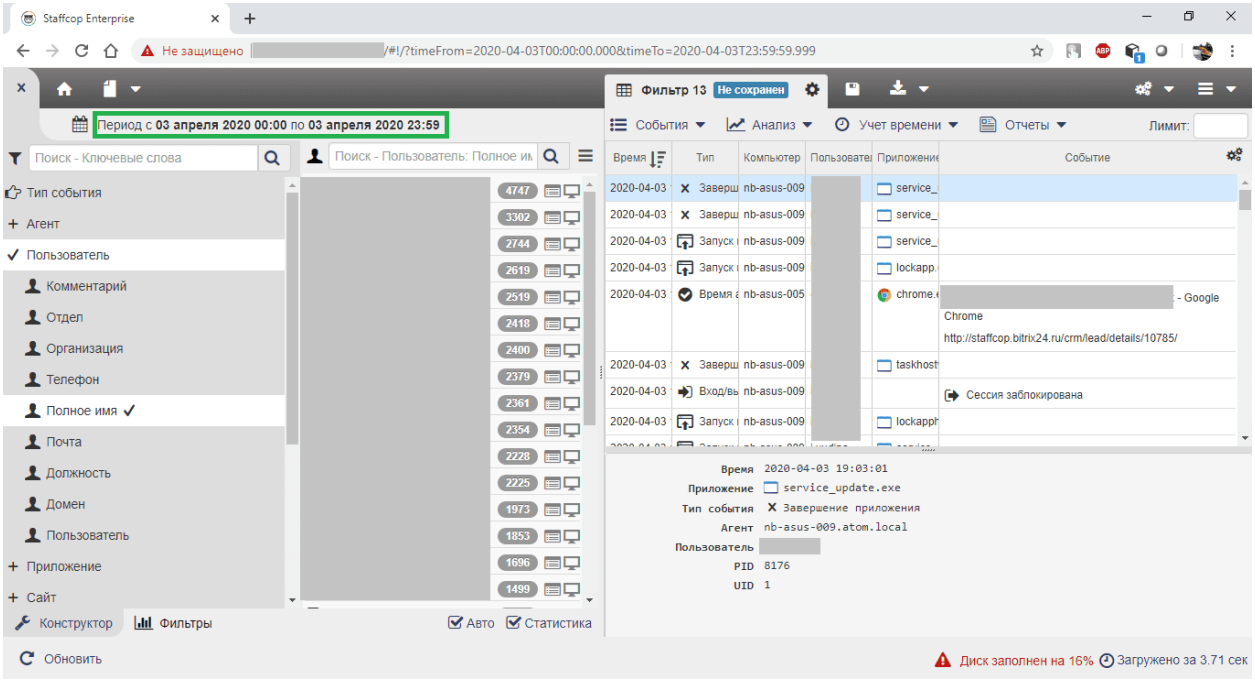


Рис. 1: Рисунок 4. Период времени, за который будут строиться отчёты

Перед построением любого отчёта (в том числе и по учёту рабочего времени) прежде всего необходимо установить период, за который он будет формироваться, если это не оговорено дополнительно. Для этого нужно щёлкнуть на любом месте в соответствующей строке, которая выделена на рисунке 4, и в открывшемся календаре указать нужные даты начала и конца периода.

После выбора периода времени в таблице будут отображены укладывающиеся в него события, и тогда можно будет переходить к формированию отчётов.

Формирование отчётов из меню базового дашборда

В меню базовой панели мониторинга, или «дашборда», iBatyr Monitor есть меню «Учёт времени». Там содержатся пункты для формирования соответствующих отчётов (рис. 5).

Рассмотрим каждый из этих пунктов, но не в том порядке, в котором они представлены в меню, а от простого к сложному.

Все отчёты могут не только формироваться в окне дашборда, но и выгружаться; это удобно для их дальнейшего просмотра, анализа и пересылки.

Таблица

Самый простой отчёт по учёту рабочего времени называется «Таблица». Он формируется по-разному в зависимости от количества выбранных пользователей.

Если отчёт «Таблица» создаётся по одному конкретному сотруднику, то он содержит сведения о работе последнего в табличном виде, а также разбивку по использованным ресурсам с указанием в процентах

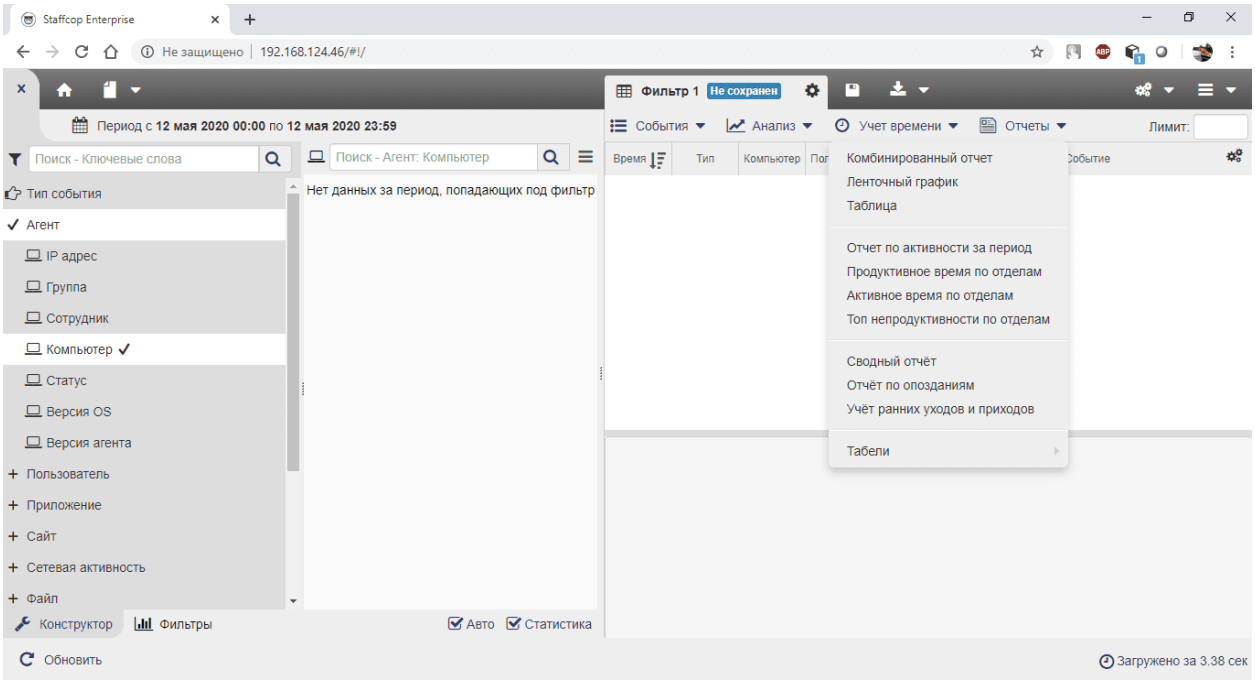


Рис. 2: Рисунок 5. Пункты меню построения отчётов по учёту рабочего времени

и часах-минутах-секундах, каким ресурсом сотрудник пользовался.

В остальных случаях (включая сценарий, когда не выбрано ничего) строится обычная таблица с указанием только времени, потраченного сотрудниками. Отображаются начало и окончание рабочего периода, вычисляется общее время работы, активное время и время простоя, информация об опоздании, сверхурочных и продуктивности. Данные отображаются в часах и минутах — сколько времени (и на что именно) было потрачено сотрудником в течение дня, без детализации.

Отчёт «Таблица» является интерактивным: при наведении указателя мыши на название ресурса появляется дополнительное всплывающее меню, которое позволяет либо просмотреть факты, соответствующие строке отчёта, либо включить дополнительный фильтр по ресурсу. При выборе фильтра формируется новый отчёт, который также можно выгрузить аналогично предыдущему.

Ленточный график

Ленточный график — наглядное представление работы пользователя за весь день с разбивкой по часам (рис. 6). Как уже говорилось ранее, зелёным цветом обозначается работа пользователя с категориями ресурсов «Премиально» и «Продуктивно», серым — «Нейтрально», красным — «Непродуктивно» и «Инцидент».

Комбинированный отчёт

Комбинированный отчёт является совокупностью ленточного графика и таблицы. Данные отображаются одновременно в обоих видах.

Отчёт по активности за период

Отчёт по активности за период очень похож на отчёт «Таблица». Отличий — два:

- «Таблица» даёт разбиение по дням, а «Отчёт по активности за период» — только суммарные значения;
- в отчёте по активности за период можно сворачивать и разворачивать элементы.

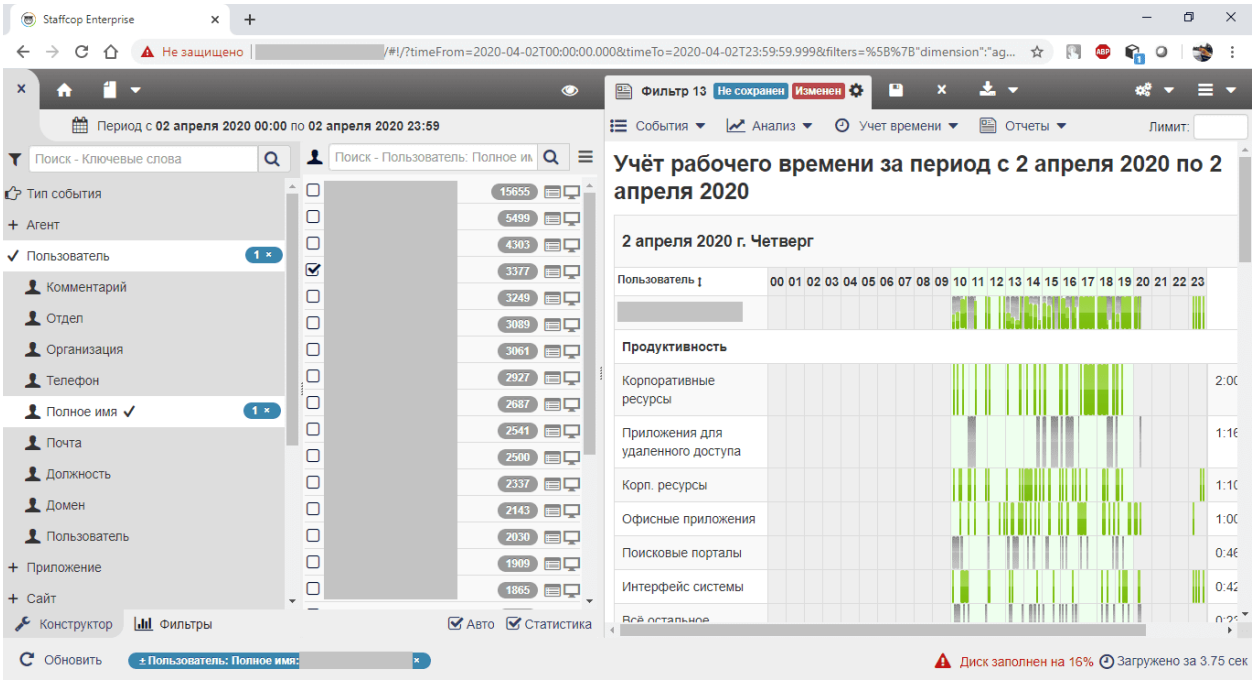


Рис. 3: Рисунок 6. Сформированный отчёт «Ленточный график»

В формат изображения отчёт выгружается точно в таком же виде, как он представлен в окне дашборда: если в интерфейсе группа данных свёрнута, то и в выгруженном изображении она будет выглядеть именно так.

Продуктивное время по отделам

Отчёт «Продуктивное время по отделам» отражает суммарное продуктивное (зелёный цвет) / непродуктивное (красный цвет) / нейтральное (серый цвет) время работы пользователей относительно их общей активности. Отчёт одновременно является и качественным, и количественным, т. е. показывает наглядно долю каждого вида активности в процентах и выполняет точный подсчёт времени (часы-минуты-секунды). Отчёт может формироваться для одного пользователя, но если берутся данные нескольких сотрудников, то он становится нагляднее: происходит группировка по отделам, и сразу становится ясно, какое подразделение содержит наибольшее число «ударников», а какое — «лентяев».

Максимально наглядный вид отчёт приобретает в том случае, если не задавать вообще никаких фильтров: тогда он соберёт информацию по всем сотрудникам и по всем отделам за указанный период (рис. 7). Как видно, внутри каждого подразделения информация свёрнута; нажав на кнопку в виде маленького треугольника, можно увидеть список сотрудников. Численность работников отображается после названия отдела.

Активное время по отделам

Отчёт «Активное время по отделам» похож на предыдущий, но отображает суммарное активное и неактивное время пользователей на рабочих местах за выбранный период времени по отношению к плановому. Плановым является время, указанное в назначенном пользователю, отделу или компьютеру расписании. Этот отчёт можно ещё назвать «дисциплинарным»: он показывает, насколько хорошо сотрудники соблюдают рабочий график в часах-минутах-секундах.

Топ непродуктивности по отделам

Отчёт «Топ непродуктивности по отделам» представляет собой форму табличного вида, в которой представлены соответствующие данные за указанный период для выбранных подразделений. Если не выбрано ничего, то отчёт формируется по всем отделам сразу.

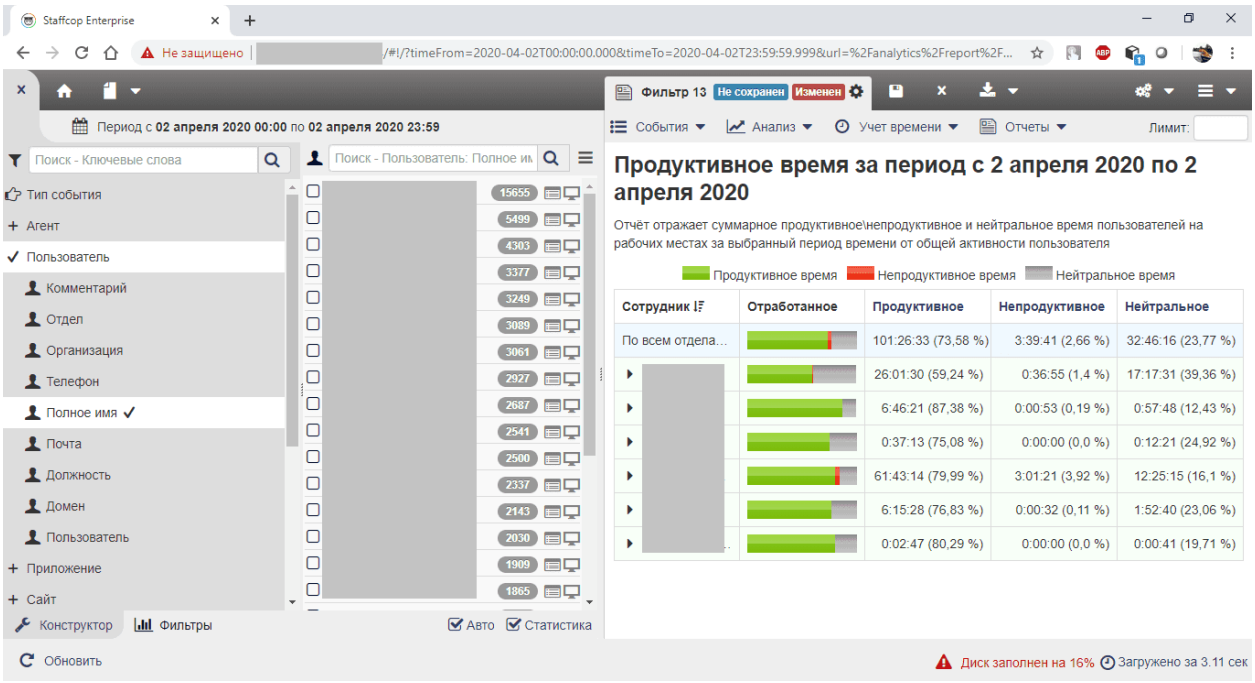


Рис. 4: Рисунок 7. Отчёт «Продуктивное время по отделам». Списки отделов свёрнуты

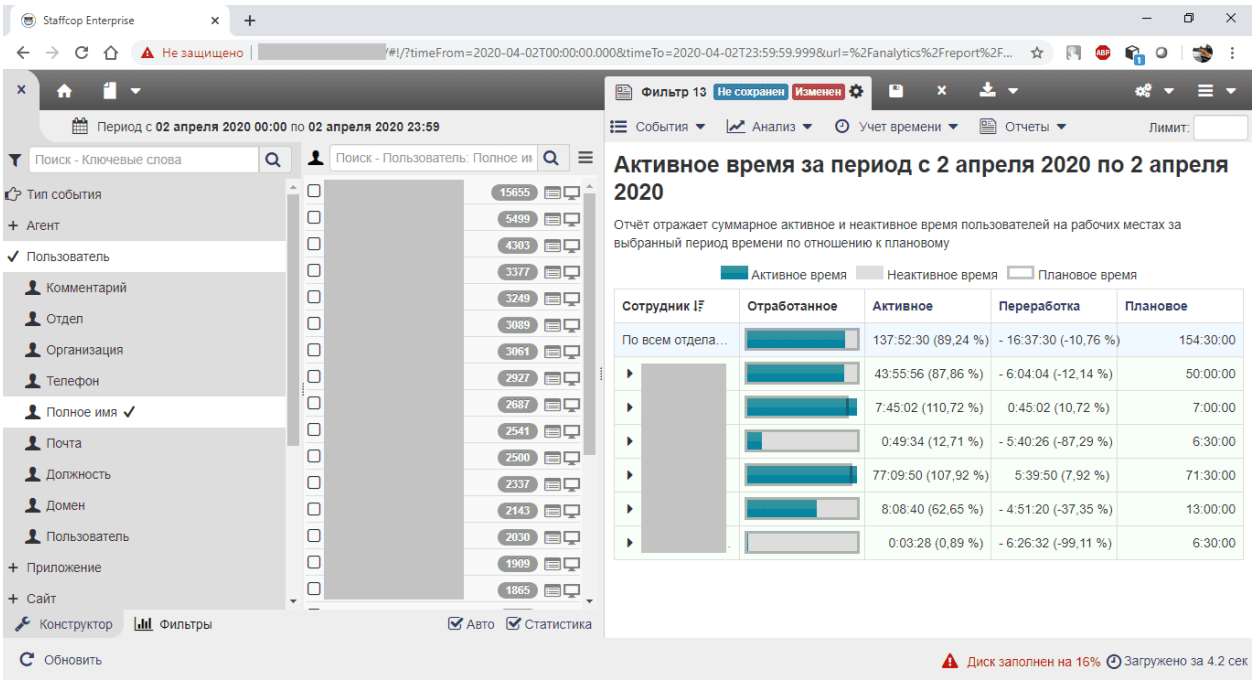


Рис. 5: Рисунок 8. Отчёт «Активное время по отделам». Списки отделов свёрнуты

Учёт ранних уходов и приходов / отчёт по опозданиям / сводный отчёт

Указанные в заголовке три вида отчётов во многом похожи. В частности, их объединяет то, что они не особенно актуальны при удалённой работе, за исключением тех случаев, когда строгое следование графику рабочего времени требуется даже в дистанционном режиме. Данные в любом из этих отчётов можно упорядочивать по возрастанию или убыванию, нажимая кнопки сортировки около каждого заголовка колонок таблицы. Отчёт «Учёт ранних уходов и приходов» формируется тогда, когда надо получить информацию о несоблюдении сотрудниками рабочего расписания. Он содержит корректную информацию только если для всех сотрудников настроен календарь и назначены расписания, соответствующие реальным графикам работы. Такой отчёт формируется в табличном виде, поэтому наиболее наглядной будет его выгрузка в формат Excel, хотя можно выгружать его и в формате изображения. Отчёт по опозданиям целесообразно формировать за длительный период. Он показывает количество и суммарное время опозданий сотрудников. Сводный отчёт содержит совокупную информацию об опозданиях, активности и продуктивности / непродуктивности сотрудников, выделяя тех, кто имеет наивысшие показатели (своеобразный «топ по категориям»). Его тоже целесообразно формировать за длительный период.

Группа отчётов «Табели»

Эта группа включает четыре отчёта стандартного формата:

- табель рабочего времени;
- табель активного времени;
- табель отсутствия на рабочем месте (эффективен при правильном заполнении календаря);
- табель использования принтера (содержит информацию о количестве заданий, направленных сотрудниками на печать).

Все табели формируются по месяцам. Указание периода времени (см. рис. 4) на эту группу отчётов влияет косвенно: если период захватывает какой-либо месяц, то табель за соответствующий месяц строится. Табели можно формировать как по отдельным сотрудникам или их группам, так и по отделам. Все отчёты имеют одинаковый формат, установленный действующим законодательством; меняется только их наполнение.

Отчёты из группы «Табели» можно выгружать в любом формате, но наиболее удобным является формат Excel. Популярен также формат изображения, позволяющий вставить отчёт, например, в документ Microsoft Word.

Отчёты по учёту рабочего времени в группе «Системные фильтры»

Нами было рассмотрено построение отчётов из пунктов меню базового дашборда. Помимо этого существует также и возможность строить отчёты из группы «Системные фильтры» (рис. 9).

Преимущество работы с отчётами в группе системных фильтров заключается в том, что можно настроить их отправку в автоматическом режиме по электронной почте. Механизм настройки одинаков для всех отчётов; более того, он абсолютно аналогичен настройкам отправки уведомлений о срабатывании политик (см. раздел «Политики эффективности. . . »).Настроив, например, ежемесячное автоматическое формирование табелей, можно значительно облегчить жизнь сотрудникам отдела кадров.

Отчёты в папке «Эффективность» — первой по порядку в списке слева на рис. 9 — в основном эквивалентны тем, которые находятся в пунктах меню «Учёт времени», несмотря на некоторые различия в названиях.

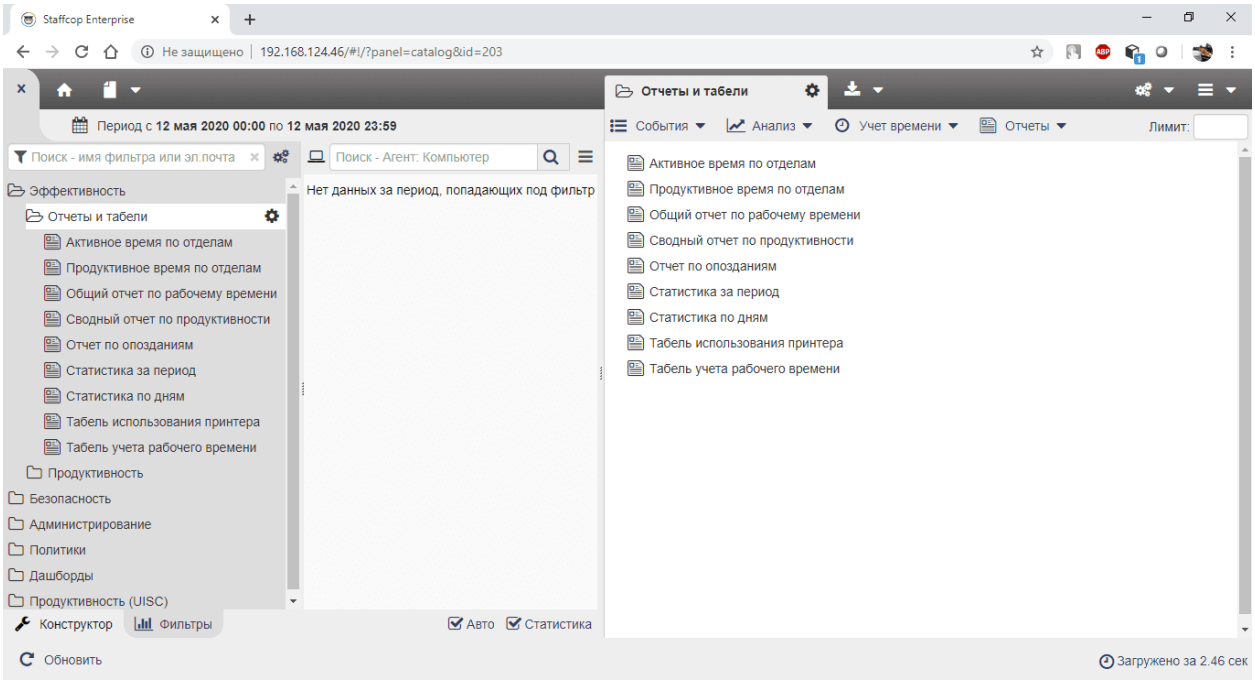


Рис. 6: Рисунок 9. Отчёты по учёту рабочего времени в группе «Системные фильтры»

Таблица 1: **Таблица 1. Соответствие имён отчётов в папке «Эффективность» отчётам в меню «Учёт времени»**

tabularytabulary

	Отчёт в группе «Системные фильтры — Эфф
	Активное время
	Продуктивное время
	Общий отчёт по рабоче
	Сводный отчёт по про
	Отчёт по
	Статистика за
	Статист
	Табель использован
	Табель учёта рабоч

(#) отчёт, не относящийся к учёту рабочего времени

Рассматривать эту группу подробно мы, таким образом, не будем.

Группа отчётов «Системные фильтры — Продуктивность»

Папка «Продуктивность» содержит две подпапки: «Продуктивная деятельность» и «Непродуктивная деятельность». Содержимое этих подпапок одинаково, каждая содержит три отчёта: «Топ пользователей», «Ленточный график» и «По категориям» (рис. 10).

Одинаковыми являются не только сами отчёты, но и все настройки; отличаются только исходные данные (выборки продуктивной и непродуктивной работы соответственно). Поэтому достаточно рассмотреть одну группу отчётов, чтобы понять, как устроена другая. Мы будем рассматривать группу «Непродуктивная деятельность», так как данных явно окажется меньше и можно будет наглядно их посмотреть.

Топ пользователей

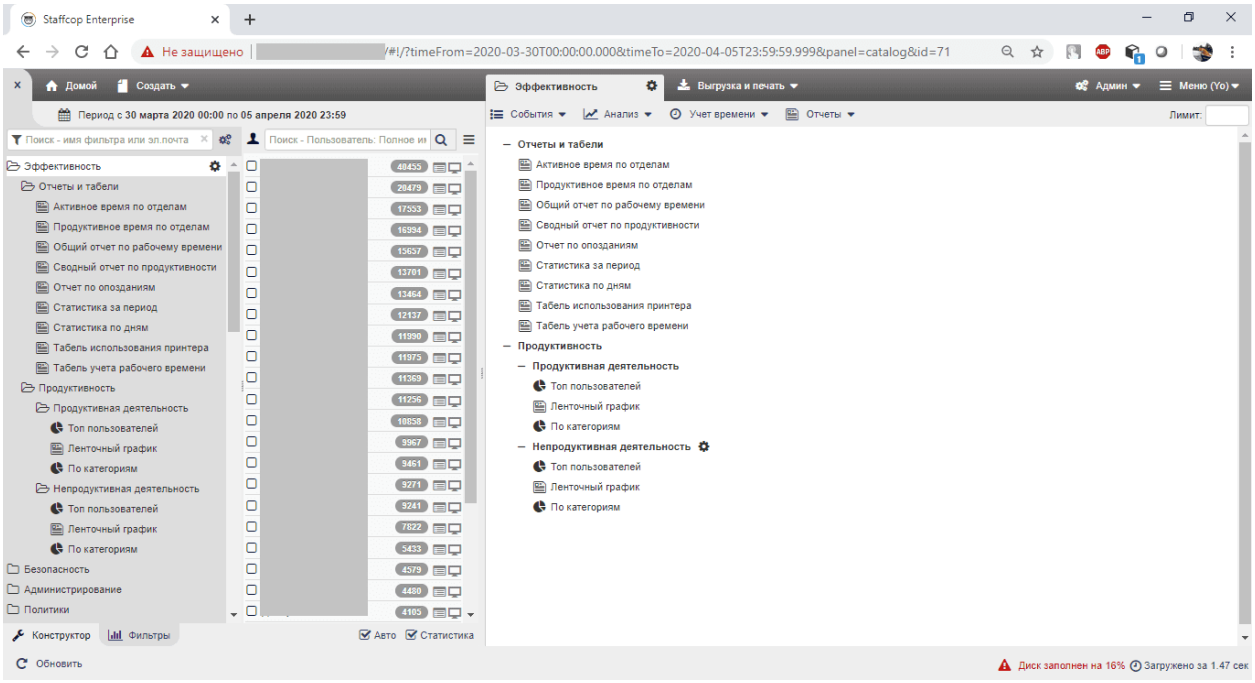


Рис. 7: Рисунок 10. Группа отчётов «Системные фильтры — Продуктивность»

Отчёт «Топ пользователей» отображает список сотрудников, работавших непродуктивно, в порядке убывания количества событий. Нажав на иконку шестерёнки (около названия отчёта), можно настроить периодическую отправку по электронной почте, установить фильтры и т. д.

По умолчанию отчёт формируется по измерению «Пользователь». Это не всегда удобно, поэтому можно щёлкнуть мышью по кнопке текущего измерения, открыть тем самым меню выбора (такое же, как в «Конструкторе») и указать то измерение, которое нужно. Заметим, что отчёт будет корректно сформирован только в том случае, если поля в профилях пользователей заполнены правильно. Можно также добавить измерение в отчёт.

Ленточный график

Отчёт «Ленточный график» в этой группе полностью аналогичен «Комбинированному отчёту» из меню «Учёт времени» — с той лишь разницей, что на обрабатываемые данные накладывается фильтр «Непродуктив / Инцидент» (если отчёт находится в папке «Продуктивная деятельность», то, соответственно, будет наложен фильтр «Продуктив»). Данный отчёт строится за период, указанный пользователем. Можно выполнить настройки, аналогичные описанным выше, и выгрузить его в любом удобном формате.

Отчёт «По категориям»

Отчёт «По категориям» показывает, какие из категорий чаще встречались в списке событий. Изначально отображается время активности пользователей на ресурсе; можно заменить его на количество событий. Этот отчёт также может быть настроен или выгружен в любом удобном формате.

4.6.5 Анализ и интерпретация отчётов

В данном разделе мы проанализируем полученные отчёты и покажем, какую информацию из них можно извлечь. Порядок изложения соответствует описаниям в разделе «Построение отчётов. . . ».

2 апреля 2020 г. Четверг

Пользователь	Начало	Окончание	Общее время	Активное	Простой	Опоздание	Сверхурочные	Продуктивное	Непродуктивное	Нейтральное
Пользователь 1	10:48:00	21:08:32	10:20:32	6:34:58	3:45:34	1:48:00	0:48:14	6:13:54	0:00:00	0:21:04
Пользователь 2	10:16:30	19:22:55	9:06:25	6:22:18	2:44:07	1:16:30	0:15:37	5:42:16	0:00:38	0:39:24
Пользователь 3	10:57:10	23:01:20	12:04:10	8:08:52	3:55:18	1:57:10	1:52:26	6:25:07	0:10:59	1:32:46
Пользователь 4	10:16:28	19:13:11	8:56:43	6:47:18	2:09:25	1:16:28	0:17:18	6:07:44	0:01:30	0:38:04
Пользователь 5	9:40:15	21:16:57	11:36:42	8:22:50	3:13:52	0:40:15	1:52:50	7:59:12	0:00:00	0:23:38
Пользователь 6	17:46:44	18:09:14	0:22:30	0:15:36	0:06:54	8:46:44	0:00:00	0:10:03	0:00:00	0:05:33
Пользователь 7	8:26:17	21:55:22	13:29:05	6:33:41	6:55:24	0:00:00	1:06:32	3:17:37	0:00:00	3:16:04
Пользователь 8	9:49:49	22:31:16	12:41:27	7:51:29	4:49:58	0:49:49	2:16:49	6:57:39	0:34:42	0:19:08
Пользователь 9	0:00:36	23:59:59	23:59:23	11:28:24	12:30:59	0:00:00	4:45:05	5:03:36	2:13:32	4:11:16
Пользователь 10	10:53:29	19:55:10	9:01:41	7:46:29	1:15:12	1:53:29	1:16:29	7:15:03	0:00:00	0:31:26
Пользователь 11	11:05:44	20:25:34	9:19:50	6:57:55	2:21:55	2:05:44	1:18:45	6:31:03	0:00:00	0:26:52

Рис. 8: Рисунок 11. Отчёт «Таблица» для нескольких сотрудников

Таблица состоит из 11 колонок и содержит столько строк, сколько пользователей было выбрано при генерации отчёта (выбор одного пользователя — это особый случай, который будет рассмотрен ниже). Перечислим колонки и дадим пояснения.

- Пользователь. В этой колонке указывается полное имя пользователя в том виде, в каком оно содержится в его профиле.
- Начало/ Окончание. Зафиксированное время первого / последнего действия пользователя в период, указанный в заголовке отчёта. Обычно это — время входа пользователя в систему и выхода из неё (login / logout).
- Общее время. Время работы пользователя, рассчитываемое как разница между окончанием и началом.
- Активное. Время любой (полной) активности на рабочей станции пользователя за сутки.
- Простой. Суммарное время, когда никакие действия пользователем не выполнялись. Значение фиксируется в рамках «Общего времени», т. е. простой засчитывается только между первым и последним событиями в сутках.
- Опоздание. Смещение времени первого зафиксированного действия пользователя по отношению ко времени начала рабочего дня.
- Сверхурочные. Суммарное продуктивное время, выходящее за рамки рабочего диапазона.
- Продуктивное /Непродуктивное / Нейтральное. Суммарное время, в течение которого пользователь работал с ресурсами (сайты, приложения), имеющими категорию «Продуктивно» или «Премиально» / категорию «Непродуктивно» / категорию «Нейтрально».

Если считать, что рабочее расписание сотрудников настроено в соответствии реальному графику работы, то по отчёту, показанному на рис. 11, можно сделать следующие выводы:

- В целом пользователи в основном занимаются работой. Пользователи 1, 5, 6, 7, 10 и 11 вообще не взаимодействовали с непродуктивными ресурсами. Самое большое время работы с непродуктивными ресурсами — у Пользователя 9; с продуктивными — у Пользователя 5.
- Дисциплина в отделе — «хуже не придумаешь». Опоздали на работу все, кроме Пользователей 7 и 9. Минимальное опоздание у Пользователя № 5 — 40 минут.
- «Чемпион по сверхурочной работе» — Пользователь 9 (почти 5 часов).

- Пользователь 6, скорее всего, находится в отпуске и заехал на работу по каким-то другим делам, потому что моменты начала и окончания работы очень близки.

Если отчёт «Таблица» строится по одному пользователю, то он имеет другой вид. Для улучшения восприятия отчёт «разрезан» на несколько частей.

Табличная часть в точности повторяет строку из отчёта для нескольких сотрудников. Колонки следуют в том же порядке. Отдельная иллюстрация здесь, таким образом, не нужна.

Графическая часть состоит из трёх компонентов (рис. 12-14).

Первый компонент показывает продуктивность работы пользователя и то, какие ресурсы занимают ту или иную долю времени. Помимо собственно доли в процентах отображается точная величина в часах-минутах-секундах (рис. 12).

Вторая графическая составляющая показывает, какие приложения пользователь применял в своей работе — также с указанием времени в часах-минутах-секундах и в процентном отношении.

По данным на рисунке видно, что наибольшую часть времени пользователь работал с браузером Opera, на втором месте было приложение для удалённого доступа TeamViewer, на третьем — приложение для работы с 1С-Битрикс, на четвёртом — «Проводник Windows», на пятом — клиент для работы с IP-телефонией. Игр в списке приложений нет, а значит, пользователь практически всё время уделял продуктивной работе.

Третий графический компонент отчёта «Таблица» посвящён сайтам, которые посещал пользователь (рис. 14).

Здесь тоже видно, что практически всё время пользователь посвятил своим рабочим обязанностям.

Ленточный график

Ленточный график показывает данные из предыдущего отчёта в привязке к разбиению по часам в сутках. Он также состоит из совокупного графика (рис. 15) и трёх вариантов детализации: «Продуктивность», «Топ приложений» и «Топ сайтов» (рис. 16-18).

Полоски на графике означают наличие активности в то или иное время. Цвет соответствует типу деятельности (зелёный — продуктивная / премиальная, красный — непродуктивная, серый — нейтральная), а высота отражает интенсивность работы за 5 минут. Разноцветная полоска означает совмещение в пятиминутный промежуток времени различных типов активности.

Из совокупного графика видно, что основное время работы сотрудника — с 10:00 до 20:00, причём в основном эта деятельность была продуктивной (зелёный цвет). Незначительное время после 11:00 было нейтральным; между 11:30 и 12:00, между 12:15 и 12:45 — простой. Отмечена также продуктивная деятельность между 23:00 и 23:45.

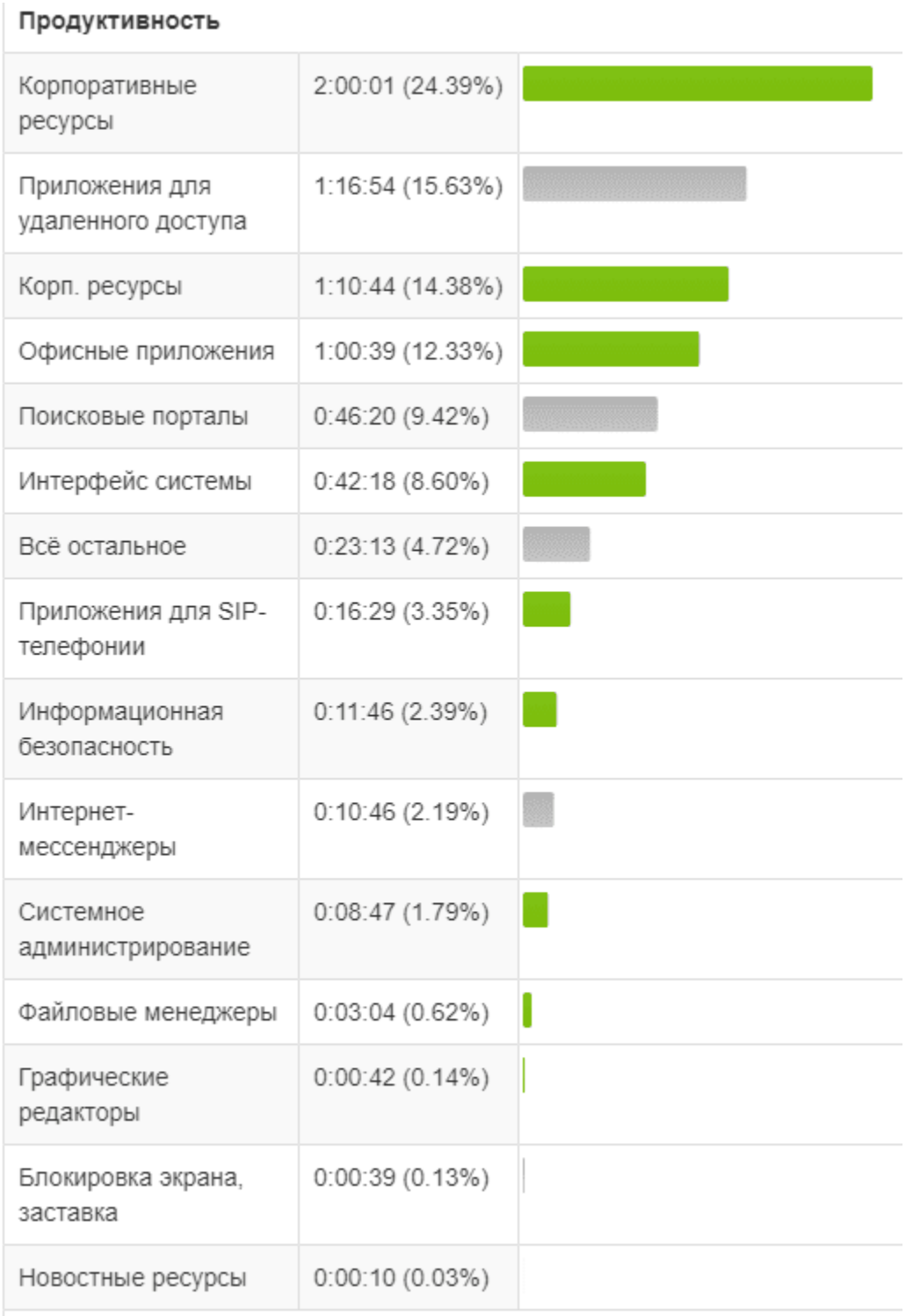
Остальные графики содержат уже знакомую нам детализацию по ресурсам, приложениям и сайтам с указанием доли в процентах и затраченного времени.

Из рисунка 16 видно, что единственный эпизод непродуктивного доступа (новостные ресурсы) был утром, между 10 и 11 часами. Работа после 23:00 была строго продуктивной. Также можно увидеть, какие ресурсы в какое время использовались.

Рисунок 17 показывает, что пользователь подключался с помощью TeamViewer около 10:45, около 15:45 и между 16:15-16:30, а также после 18:45. В основном сотрудник работал в браузере Opera.

На рисунке 18 показано, какие сайты в какое время посещались. Очевидно, что наиболее часто открывался сайт bitrix24.ru. Таким образом, основное время пользователь посвящал работе: единственный не связанный с работой домен — tayga.info — посещался в течение 10 секунд, которых хватит только для того, чтобы прочесть заголовки новостей.

Комбинированный отчёт / отчёт по активности за период



Продуктивность	
Корпоративные ресурсы	2:00:01 (24.39%)
Приложения для удаленного доступа	1:16:54 (15.63%)
Корп. ресурсы	1:10:44 (14.38%)
Офисные приложения	1:00:39 (12.33%)
Поисковые порталы	0:46:20 (9.42%)
Интерфейс системы	0:42:18 (8.60%)
Всё остальное	0:23:13 (4.72%)
Приложения для SIP-телефонии	0:16:29 (3.35%)
Информационная безопасность	0:11:46 (2.39%)
Интернет-мессенджеры	0:10:46 (2.19%)
Системное администрирование	0:08:47 (1.79%)
Файловые менеджеры	0:03:04 (0.62%)
Графические редакторы	0:00:42 (0.14%)
Блокировка экрана, заставка	0:00:39 (0.13%)
Новостные ресурсы	0:00:10 (0.03%)

Рис. 9: Рисунок 12. Графическая часть: продуктивность работы пользователя

Топ приложений

opera.exe	4:29:21 (54.75%)	
teamviewer.exe	1:10:53 (14.41%)	
bitrix24.exe	1:00:39 (12.33%)	
explorer.exe	0:41:39 (8.47%)	
mango-talker.exe	0:16:29 (3.35%)	
skype.exe	0:10:46 (2.19%)	
vmware-vmx.exe	0:08:14 (1.67%)	
mstsc.exe	0:06:01 (1.22%)	
far.exe	0:03:01 (0.61%)	
vmware.exe	0:01:37 (0.33%)	
mspaint.exe	0:00:42 (0.14%)	
searchui.exe	0:00:39 (0.13%)	
lockapp.exe	0:00:39 (0.13%)	
cmd.exe	0:00:33 (0.11%)	
vpndownloader.exe	0:00:26 (0.09%)	
shellexperiencehost.exe	0:00:24 (0.08%)	
tvtools_alterid.exe	0:00:19 (0.06%)	
totalcmd64.exe	0:00:02 (0.01%)	
telegram.exe	0:00:02 (0.01%)	
teamviewerportable.exe	0:00:02 (0.01%)	
rundll32.exe	0:00:01 (0.00%)	
заставка		
Новостные ресурсы	0:00:10 (0.03%)	

Рис. 10: Рисунок 13. Графическая часть: топ приложений

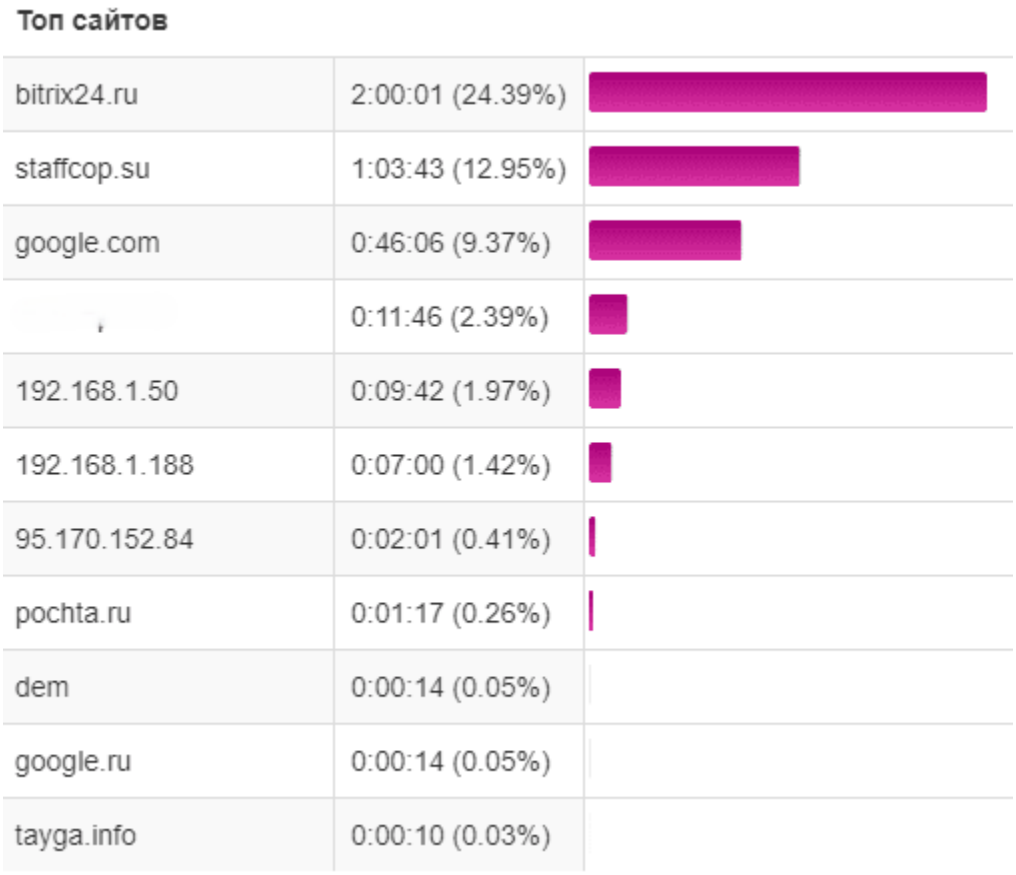


Рис. 11: Рисунок 14. Графическая часть: топ сайтов

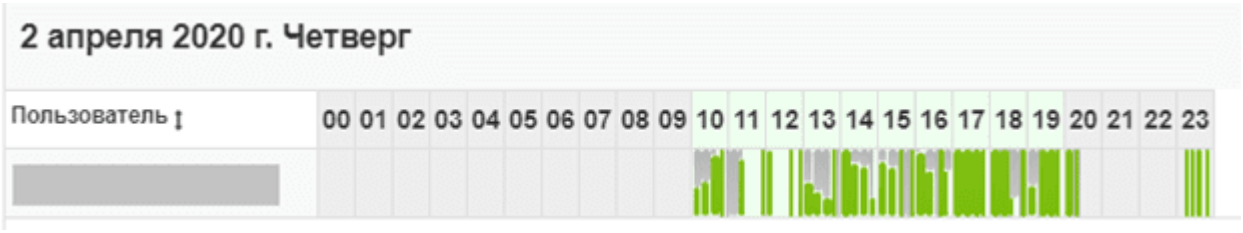


Рис. 12: Рисунок 15. Совокупный график

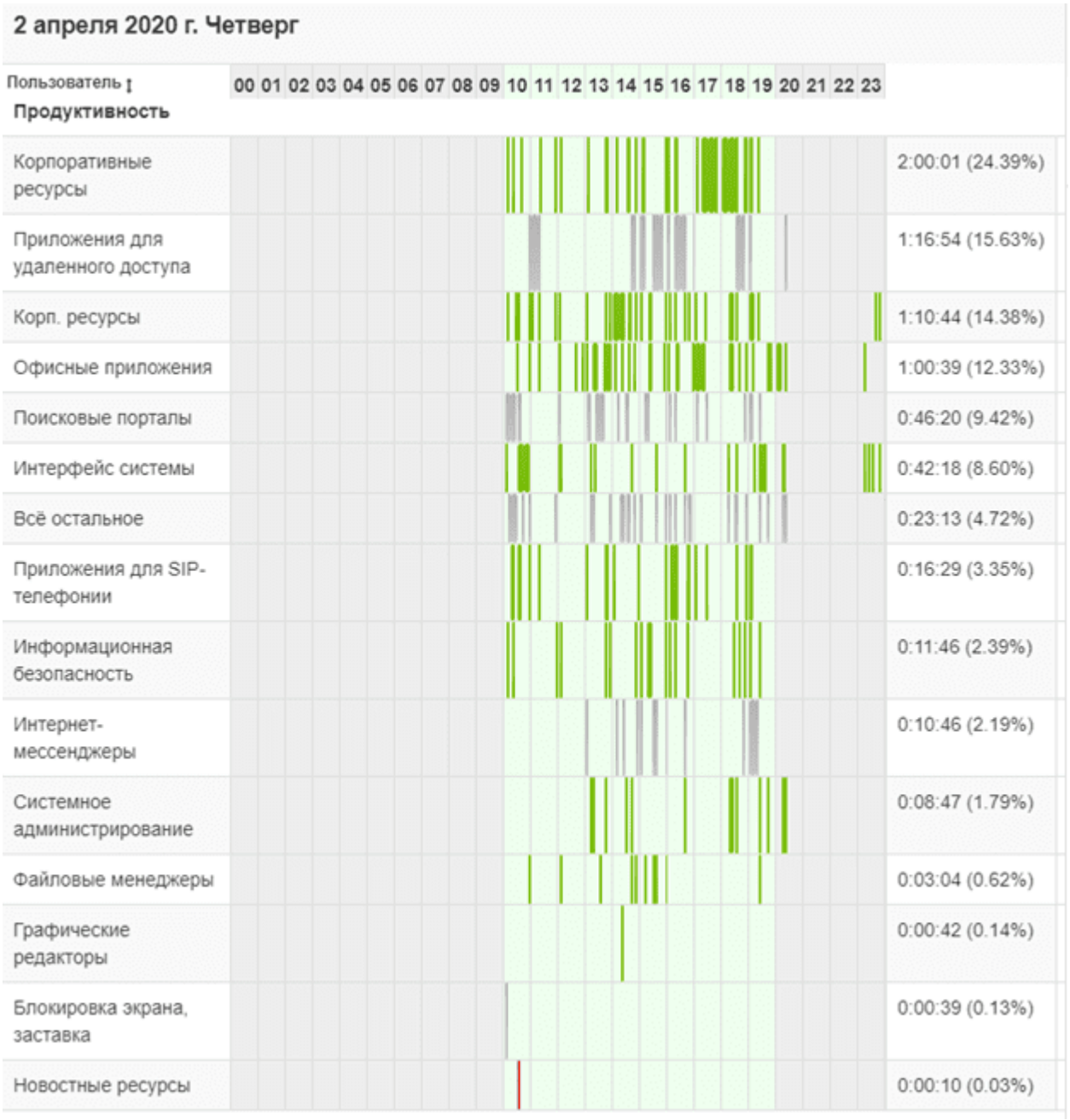


Рис. 13: Рисунок 16. Продуктивные и непродуктивные ресурсы: разбиение по часам (изображение сдвинуто, чтобы был виден заголовок графика)

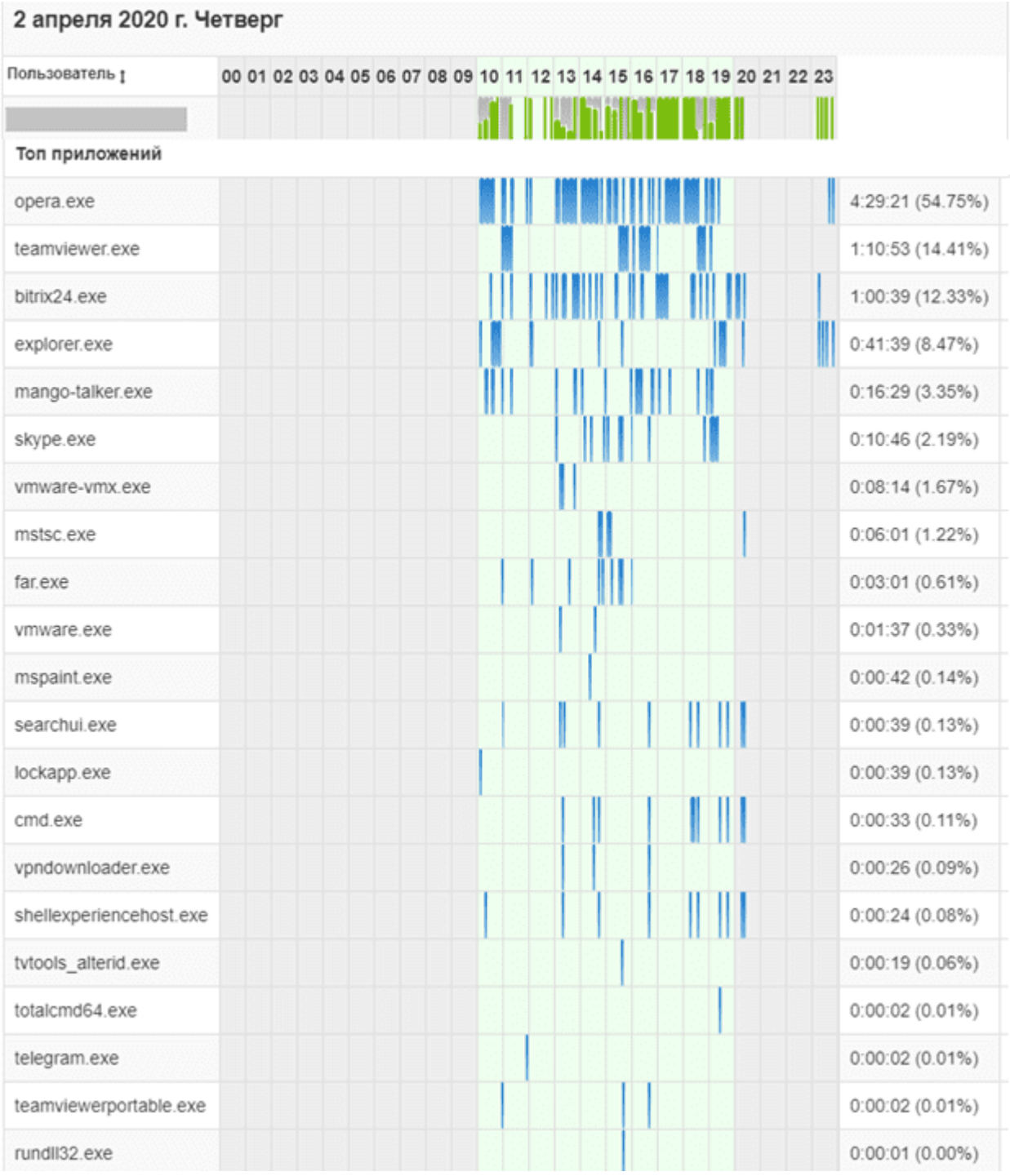


Рис. 14: Рисунок 17. Приложения: разбиение по часам (изображение сдвинуто, чтобы был виден заголовок графика)

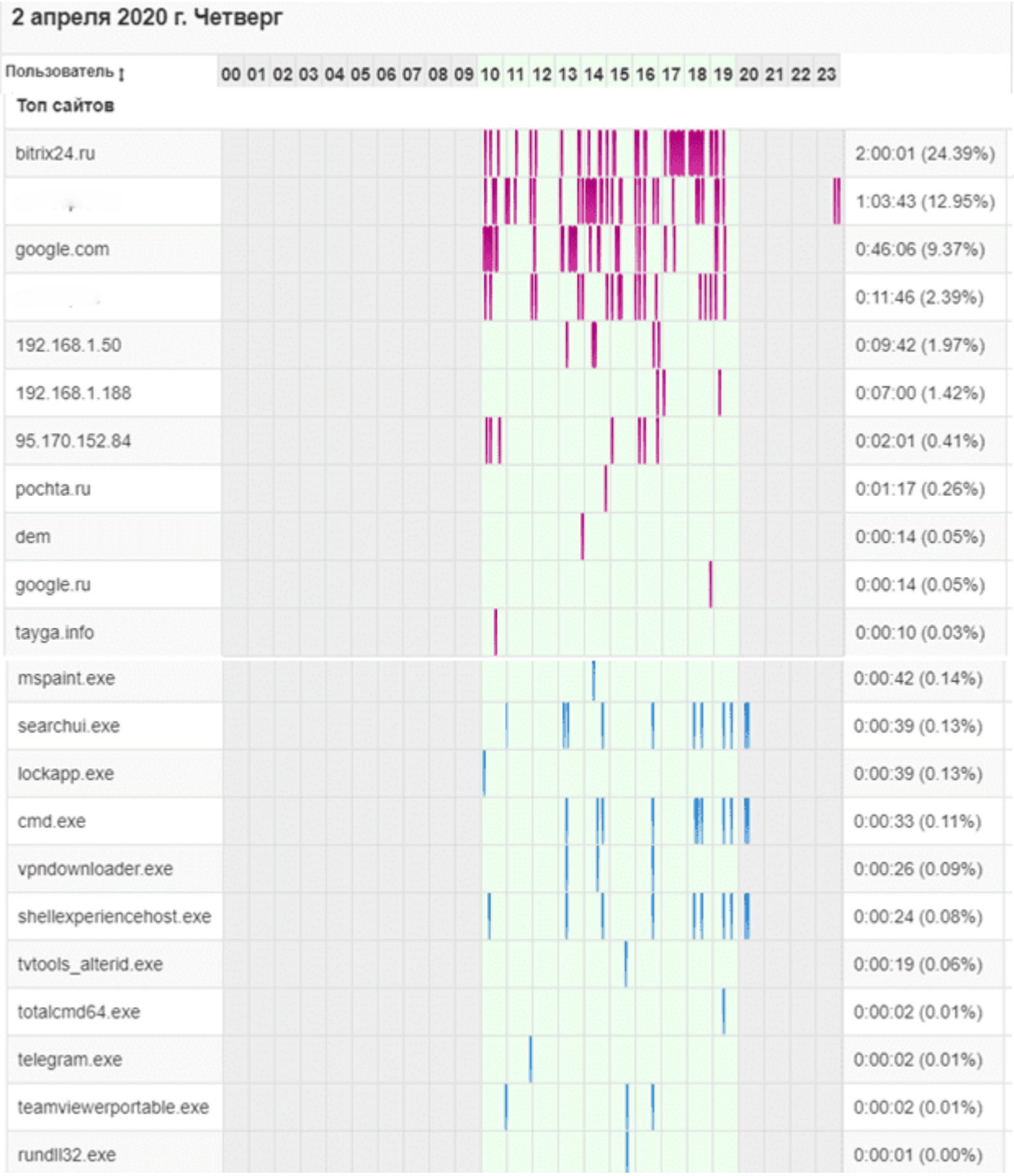


Рис. 15: Рисунок 18. Посещение сайтов: разбиение по часам (изображение сдвинуто, чтобы был виден заголовок графика)

Комбинированный отчёт представляет собой совокупность ленточного графика и таблицы, поэтому отдельно его комментировать смысла нет. Отчёт по активности за период позволяет отобразить суммарную информацию за выбранный период времени без разбиения по дням. Его интерпретация тоже не представляет сложности, так как идентична анализу отчёта «Таблица».

Активное время за период

Отчёт «Активное время за период» показывает время активности пользователей и время простоя по отношению к плановому (времени рабочего дня). Поскольку названия отделов и имена пользователей в целях неразглашения информации затёрты, присвоим отделам условные названия по цвету закраски: «тёмно-серый», «светло-серый», «оранжевый», «розовый» и «синий». Суммарные данные по отделам показаны в фиолетовой рамке, рядом — число сотрудников, работающих в отделе.

Пример отчёта показан на рис. 19.

Видно, что единственный сотрудник «светло-серого» отдела не только потратил на работу всё плановое время, но и имеет переработку. А вот сотрудник «оранжевого» отдела большую часть рабочего времени провёл не за компьютером; впрочем, это не значит, что он бездельничал — возможно, это был плановый выезд к клиенту или заказчику. То же самое можно сказать и о сотруднике № 6 «розового» отдела. Сотрудник № 2 «синего» отдела также больше половины рабочего дня провёл не за компьютером.

Зато в том же «розовом» отделе велико число тех сотрудников, которые провели за компьютером больше планового времени; соответственно, у всего отдела есть переработка. Насколько эта переработка полезна, нам покажет отчёт «Продуктивность за период», который будет рассмотрен ниже.

Как количественно (в часах-минутах-секундах), так и качественно (в процентах) информацию об активном времени сотрудников можно получить из таблицы, которая находится справа от графиков.

Следует отметить, что наиболее точным этот отчёт будет в том случае, если для всех пользователей настроены календарь и расписания, соответствующие реальным графикам их работы.

Отчёт «Продуктивное время по отделам»

Отчёт «Продуктивное время по отделам» очень похож на предыдущий, но отображает разбиение активного времени сотрудников на продуктивное, непродуктивное и нейтральное, при этом давая суммарную информацию по отделам, что позволяет выяснить эффективность работы не только сотрудников, но и подразделений в целом. Пример отчёта представлен на рис. 20. Цветовые обозначения отделов — те же, что и на рис. 19.

Видно, что в трёх отделах — «светло-сером», «оранжевом» и «синем» — сотрудники вообще не пользовались ресурсами, отнесёнными к категории непродуктивных. В «розовом» отделе есть «ударник»: у сотрудника, данные о котором отображены в первой строке, зафиксирована наибольшая доля продуктивных ресурсов относительно полного времени активности (почти 95%). Вторым по эффективности является сотрудник № 5 в «тёмно-сером» отделе: доля продуктивной деятельности — чуть более 90%. В том же «розовом» отделе работает и сотрудник, у которого отмечен самый большой процент использования непродуктивных ресурсов (почти 1/5 всего времени активности).

Если сравнивать подразделения, в которых количество сотрудников превышает 2, то можно заметить, что «тёмно-серый» отдел имеет больше продуктивной работы, нежели «розовый». Тем не менее главный «лентяй» фирмы работает именно в «тёмно-сером» отделе: это сотрудник № 4, у него наименьший процент времени посвящён продуктивной деятельности. Если же анализировать работу подразделений в целом, то наиболее продуктивной является работа «светло-серого» и «синего» отделов.

Аналогично предыдущему отчёту количественные и качественные показатели можно извлечь из таблицы, которая находится справа от графиков — там указаны точные значения в часах-минутах-секундах и доли продуктивной / непродуктивной / нейтральной деятельности в общей сумме активного времени.

Топ непродуктивности по отделам

Отчёт «Топ непродуктивности по отделам» лучше всего анализировать при выгрузке в формате Excel: так из него можно почерпнуть немало полезной информации. Общий вид представлен на рис. 21.

Активное время за период с 2 апреля 2020 по 2 апреля 2020

Отчёт отражает суммарное активное и неактивное время пользователей на рабочих местах за выбранный период времени по отношению к плановому

Активное время | Неактивное время | Плановое время

Сотрудник	Отработанное	Активное	Переработка	Плановое
По всем отделам (23)		137:52:30 (89,24 %)	- 16:37:30 (-10,76 %)	154:30:00
(7)		43:55:56 (87,86 %)	- 6:04:04 (-12,14 %)	50:00:00
		7:46:47 (97,25 %)	- 0:13:13 (-2,75 %)	8:00:00
		8:12:00 (117,14 %)	1:12:00 (17,14 %)	7:00:00
		8:17:05 (118,35 %)	1:17:05 (18,35 %)	7:00:00
		1:23:16 (19,83 %)	- 5:36:44 (-80,17 %)	7:00:00
		3:52:39 (55,39 %)	- 3:07:21 (-44,61 %)	7:00:00
		6:41:03 (95,49 %)	- 0:18:57 (-4,51 %)	7:00:00
		7:43:06 (110,26 %)	0:43:06 (10,26 %)	7:00:00
(1)		7:45:02 (110,72 %)	0:45:02 (10,72 %)	7:00:00
		7:45:02 (110,72 %)	0:45:02 (10,72 %)	7:00:00
(1)		0:49:34 (12,71 %)	- 5:40:26 (-87,29 %)	6:30:00
		0:49:34 (12,71 %)	- 5:40:26 (-87,29 %)	6:30:00
(11)		77:09:50 (107,92 %)	5:39:50 (7,92 %)	71:30:00
		6:34:58 (101,27 %)	0:04:58 (1,27 %)	6:30:00
		6:22:18 (98,03 %)	- 0:07:42 (-1,97 %)	6:30:00
		8:08:52 (125,35 %)	1:38:52 (25,35 %)	6:30:00
		6:47:18 (104,44 %)	0:17:18 (4,44 %)	6:30:00
		8:22:50 (128,93 %)	1:52:50 (28,93 %)	6:30:00
		0:15:36 (4,0 %)	- 6:14:24 (-96,0 %)	6:30:00
		6:33:41 (100,94 %)	0:03:41 (0,94 %)	6:30:00
		7:51:29 (120,89 %)	1:21:29 (20,89 %)	6:30:00
		11:28:24 (176,51 %)	4:58:24 (76,51 %)	6:30:00
		7:46:29 (119,61 %)	1:16:29 (19,61 %)	6:30:00
		6:57:55 (107,16 %)	0:27:55 (7,16 %)	6:30:00
(2)		8:08:40 (62,65 %)	- 4:51:20 (-37,35 %)	13:00:00
		5:08:24 (79,08 %)	- 1:21:36 (-20,92 %)	6:30:00
		3:00:16 (46,22 %)	- 3:29:44 (-53,78 %)	6:30:00
Отдел не заполнен (1)		0:03:28 (0,89 %)	- 6:26:32 (-99,11 %)	6:30:00
Имя не заполнено		0:03:28 (0,89 %)	- 6:26:32 (-99,11 %)	6:30:00

Рис. 16: Рисунок 19. Отчёт «Активное время за период»

Продуктивное время за период с 2 апреля 2020 по 2 апреля 2020

Отчёт отражает суммарное продуктивное\непродуктивное и нейтральное время пользователей на рабочих местах за выбранный период времени от общей активности пользователя

Продуктивное время Непродуктивное время Нейтральное время

Сотрудник	Отработанное	Продуктивное	Непродуктивное	Нейтральное
По всем отделам (23)		101:26:33 (73,58 %)	3:39:41 (2,66 %)	32:46:16 (23,77 %)
(7)		26:01:30 (59,24 %)	0:36:55 (1,4 %)	17:17:31 (39,36 %)
		5:30:53 (70,89 %)	0:07:32 (1,61 %)	2:08:22 (27,5 %)
		5:34:14 (67,93 %)	0:00:10 (0,03 %)	2:37:36 (32,03 %)
		3:33:28 (42,94 %)	0:00:54 (0,18 %)	4:42:43 (56,88 %)
		0:22:11 (26,64 %)	0:00:31 (0,62 %)	1:00:34 (72,74 %)
		3:32:44 (91,44 %)	0:00:00 (0,0 %)	0:19:55 (8,56 %)
		3:31:30 (52,74 %)	0:00:09 (0,04 %)	3:09:24 (47,23 %)
		3:56:30 (51,07 %)	0:27:39 (5,97 %)	3:18:57 (42,96 %)
(1)		6:46:21 (87,38 %)	0:00:53 (0,19 %)	0:57:48 (12,43 %)
		6:46:21 (87,38 %)	0:00:53 (0,19 %)	0:57:48 (12,43 %)
(1)		0:37:13 (75,08 %)	0:00:00 (0,0 %)	0:12:21 (24,92 %)
		0:37:13 (75,08 %)	0:00:00 (0,0 %)	0:12:21 (24,92 %)
(11)		61:43:14 (79,99 %)	3:01:21 (3,92 %)	12:25:15 (16,1 %)
		6:13:54 (94,67 %)	0:00:00 (0,0 %)	0:21:04 (5,33 %)
		5:42:16 (89,53 %)	0:00:38 (0,17 %)	0:39:24 (10,31 %)
		6:25:07 (78,78 %)	0:10:59 (2,25 %)	1:32:46 (18,98 %)
		6:07:44 (90,29 %)	0:01:30 (0,37 %)	0:38:04 (9,35 %)
		7:59:12 (95,3 %)	0:00:00 (0,0 %)	0:23:38 (4,7 %)
		0:10:03 (64,42 %)	0:00:00 (0,0 %)	0:05:33 (35,58 %)
		3:17:37 (50,2 %)	0:00:00 (0,0 %)	3:16:04 (49,8 %)
		6:57:39 (88,58 %)	0:34:42 (7,36 %)	0:19:08 (4,06 %)
		5:03:36 (44,1 %)	2:13:32 (19,4 %)	4:11:16 (36,5 %)
		7:15:03 (93,26 %)	0:00:00 (0,0 %)	0:31:26 (6,74 %)
		6:31:03 (93,57 %)	0:00:00 (0,0 %)	0:26:52 (6,43 %)
(2)		6:15:28 (76,83 %)	0:00:32 (0,11 %)	1:52:40 (23,06 %)
		3:47:22 (73,72 %)	0:00:17 (0,09 %)	1:20:45 (26,18 %)
		2:28:06 (82,16 %)	0:00:15 (0,14 %)	0:31:55 (17,71 %)
Отдел не заполнен (1)		0:02:47 (80,29 %)	0:00:00 (0,0 %)	0:00:41 (19,71 %)
Имя не заполнено		0:02:47 (80,29 %)	0:00:00 (0,0 %)	0:00:41 (19,71 %)

Рис. 17: Рисунок 20. Отчёт «Продуктивное время по отделам»

Компьютер	Пользователь	Должность	Отдел	Название	Время активности
			Отдел 1		**3:01:38**
PC001.domain1.com	Пользователь 1		**Отдел 1**	Развлекательные ресурсы	2:09:23
PC001.domain2.local	Пользователь 2		**Отдел 1**	Новостные ресурсы	0:28:07
PC002.domain2.local	Пользователь 3	Руководитель отдела 1	**Отдел 1**	Развлекательные ресурсы	0:11:00
PC003.domain2.local	Пользователь 4		**Отдел 1**	Чаты не корпоративные	0:05:52
PC002.domain1.com	Пользователь 5		**Отдел 1**	Новостные ресурсы	0:04:18
PC004.domain2.local	Пользователь 6	менеджер отдела 1	**Отдел 1**	Развлекательные ресурсы	0:01:32
PC005.domain2.local	Пользователь 7		**Отдел 1**	Развлекательные ресурсы	0:00:48
PC006.domain2.local	Пользователь 8	Специалист отдела 1	**Отдел 1**	Развлекательные ресурсы	0:00:38
			Отдел 2		**0:37:01**
DESKTOP01	Пользователь 9		**Отдел 2**	Чаты не корпоративные	0:22:17
PC003.domain1.com	Пользователь 10		**Отдел 2**	Развлекательные ресурсы	0:06:43
DESKTOP01	Пользователь 11		**Отдел 2**	Развлекательные ресурсы	0:05:22
PC004.domain1.com	Пользователь 12		**Отдел 2**	Развлекательные ресурсы	0:00:49
PC005.domain1.com	Пользователь 13		**Отдел 2**	Торговые площадки и доски объявлений	0:00:45
PC007.domain2.local	Пользователь 14	Инженер отдела 2	**Отдел 2**	Развлекательные ресурсы	0:00:20
PC007.domain2.local	Пользователь 15	Инженер отдела 2	**Отдел 2**	Новостные ресурсы	0:00:12
DESKTOP02	Пользователь 16		**Отдел 2**	Новостные ресурсы	0:00:10
DESKTOP03	Пользователь 18		**Отдел 2**	Новостные ресурсы	0:00:09
PC009.domain2.local	Пользователь 19		**Отдел 2**	Сайты по трудоустройству	0:00:08
PC0010.domain2.local	Пользователь 20		**Отдел 2**	Новостные ресурсы	0:00:04
DESKTOP04	Пользователь 21		**Отдел 2**	Мультимедийные плееры	0:00:02

Рис. 18: Рисунок 21. Отчёт «Топ непродуктивности по отделам»

Как видно, отчёт сформирован по двум подразделениям. Первое, что бросается в глаза, — время активности, отмеченной как непродуктивная, в Отделе 1 оказалось намного крупнее, чем в Отделе 2: более 3 часов против 37 минут. Основной вклад в непродуктивность Отдела 1 внёс Пользователь 1, у которого зафиксировано почти 2 часа и 10 минут такой деятельности. У «лидера непродуктивности» Отдела 2 — Пользователя 9 — набралось чуть больше 22 минут.

При этом непродуктивная деятельность «лидеров» — принципиально разная: Пользователь 1 посвятил время развлекательным ресурсам, а Пользователь 9 — некорпоративным чатам. И если администратор безопасности опытен, то отныне больше внимания он станет уделять Пользователю 9, так как неизвестно, о чём он беседовал в этих чатах. Пусть Пользователь 1 смотрит мемы на «Пикабу» — в этом нет большой беды с точки зрения информационной безопасности; а вот через некорпоративные чаты, напротив, может произойти утечка конфиденциальных данных.

Обратимся теперь к колонке 1 («Компьютер»). Мы увидим, что в сети есть не только компьютеры, входящие в разные домены — domain1.com, domain2.local, — но и машины, вообще не входящие ни в какой домен; их имена начинаются с «DESKTOP». Поскольку данные по профилям рабочих станций собираются на самих терминалах (это делает агент, который потом передаёт информацию на сервер), сведениям в таблице можно доверять. Соответственно, мы видим, что в организации используются несколько доменов, а также рабочие станции, не входящие в домен — и по всем ним агенты iBatyr Monitor успешно собирают данные.

Имя рабочей станции «PC007.domain2.local» встречается в этой колонке дважды, а пользователи — разные. Следует выяснить у начальника отдела, в котором установлена эта рабочая станция, действительно ли разрешается разным пользователям садиться по очереди за один компьютер и соответствует ли это регламенту работы.

Последнее, на что стоит обратить внимание, — это колонка «Должность». Она заполнена не у всех сотрудников. Учитывая, что сервер iBatyr Monitor должен быть подключён к домену, необходимо выяснить, почему не заполнены профили пользователей. Является ли это упущением системного администратора, отвечающего за домен, или администратора безопасности, отвечающего за работу сервера iBatyr Monitor ?

Таким образом, мы видим, что внимательный анализ такого в общем-то простого отчёта может по-

ставить перед руководителем вопросы, которые на первый взгляд далеки от темы непродуктивности как таковой, но, тем не менее, пренебрежение ими может повлиять на информационную безопасность компании.

Учёт ранних уходов и приходов

Как уже обсуждалось в разделе «Построение отчётов. . . », достоверная информация будет содержаться здесь только в том случае, если всем сотрудникам назначены расписания, соответствующие их реальным графикам работы, включая обеденные перерывы. В противном случае этот отчёт информативным не будет.

3 апреля 2020 г.

Пользователь	Опоздал	Ушел на обед раньше	Опоздал с обеда	Ушел с работы раньше	Задержался на работе	Пришел на работу раньше
Пользователь 1	9:37:36	0:00:00	3:37:36	0:00:00	0:49:23	0:00:00
Пользователь 2	3:07:22	0:00:00	0:00:00	0:00:00	0:32:07	0:00:00
Пользователь 3	3:22:17	0:00:00	0:00:00	0:35:29	0:00:00	0:00:00
Пользователь 4	7:20:20	0:00:00	0:00:00	0:00:00	0:53:13	0:00:00
Пользователь 5	0:54:29	0:00:00	0:00:00	0:00:00	2:15:32	0:00:00
Пользователь 6	0:57:13	0:00:00	0:00:00	0:00:00	0:15:01	0:00:00
Пользователь 7	2:16:35	0:00:00	0:00:00	0:00:00	3:44:56	0:00:00
Пользователь 8	0:18:23	0:00:00	0:00:00	0:00:00	1:13:43	0:00:00
Пользователь 9	9:51:52	0:00:00	0:00:00	0:00:00	1:49:50	0:00:00
Пользователь 10	1:18:22	0:00:00	0:00:00	0:00:00	4:44:25	0:00:00
Пользователь 11	0:07:06	0:00:00	0:00:00	0:36:20	0:00:00	0:00:00
Пользователь 12	1:55:10	0:00:00	0:00:00	0:00:00	3:40:16	0:00:00
Пользователь 13	2:20:35	0:00:00	0:00:00	0:00:00	1:08:57	0:00:00
Пользователь 14	0:42:19	0:00:00	0:00:00	0:00:00	3:28:44	0:00:00
Пользователь 15	8:23:27	0:00:00	0:00:00	0:00:00	2:05:22	0:00:00
Пользователь 16	3:53:25	0:00:00	0:00:00	0:00:00	2:17:44	0:00:00
Пользователь 17	1:35:44	0:00:00	0:00:00	0:00:00	0:13:11	0:00:00
Пользователь 18	3:10:16	0:00:00	0:00:00	0:00:00	2:52:32	0:00:00
Пользователь 19	1:59:25	0:00:00	0:00:00	0:00:00	1:47:54	0:00:00

DESKTOP04	Пользователь 21		**Отдел 2**	Мультимедийные плееры	0:00:02

Рис. 19: Рисунок 22. Отчёт «Учёт ранних уходов и приходов»

На рисунке 22 показана часть отчёта, сформированного на один день. Значения в колонках интуитивно понятны, и интерпретация данных не должна вызывать сложностей.

Отчёт по опозданиям

Отчёт по опозданиям состоит из двух частей: графической и табличной.

Отчёт на рисунке 23 показывает максимальное количество опозданий, равное шести. Поскольку он охватывает календарную неделю, очевидно, что в компании, для руководства которой сформирован этот отчёт, суббота считается рабочим днём — и есть человек, который явился с опозданием во все дни рабочей недели (фамилии сотрудников закрашены).

В левой части приводится количество опозданий сотрудников (первые 10 записей по убыванию) с указанием полных имён; в правой — суммарное количество времени опозданий в часах-минутах-секундах по каждому отдельному пользователю, тоже с указанием полных имён. В верхней части отображается полное рабочее время за указанный период и общее время опозданий для всех сотрудников.

Табличная часть «Отчёта по опозданиям» приведена на рис. 24.

Таблица упорядочена по фамилиям сотрудников, однако это можно изменить перед выгрузкой, нажимая соответствующие кнопки в заголовке таблицы. Назначение колонок интуитивно понятно из их заголовков, обсуждалось ранее и дополнительных разъяснений не требует.

Сводный отчёт

Рис. 20: Рисунок 23. Графическая часть «Отчёта по опозданиям»

Пользователь	Кол-во опозданий	Общее время опозданий	Общее время	Активное время	Время простоя
Значение не указано	2	10:00:00	2:22:57	0:56:41	1:27:30
	3	8:11:00	24:09:36	14:04:44	10:04:52
	2	11:57:00	10:02:12	1:00:44	9:01:28
	1	1:51:55	79:39:27	36:59:18	42:40:09
	3	17:51:59	4:15:14	1:13:38	3:01:36
	4	5:02:32	60:11:51	38:35:18	21:36:33
	3	10:54:38	13:14:17	9:46:45	3:27:32
	2	1:13:23	46:15:51	39:05:26	7:10:25
	3	1:07:42	51:51:44	29:07:18	22:44:26
	4	9:55:20	61:52:25	22:14:33	39:37:52
	1	1:52:17	5:53:03	4:15:06	1:37:57
	5	15:25:19	40:39:01	31:45:32	8:53:29
	3	5:19:59	72:04:37	38:56:22	33:08:15
	5	6:19:10	53:59:09	33:50:29	20:08:40
	5	4:23:37	46:37:23	32:09:11	14:28:12
	2	4:00:08	53:52:20	27:42:27	26:09:53
	1	8:23:27	17:48:34	1:47:24	16:01:10
	1	0:53:11	41:00:50	6:24:48	34:36:02
	5	8:55:44	51:08:25	36:16:10	14:52:15
	1	7:20:20	3:24:45	3:05:16	0:19:29
	4	5:08:22	52:10:46	37:53:50	14:16:56
	1	2:46:50	22:38:01	8:07:39	14:30:22
	2	2:30:57	62:07:06	41:05:58	21:01:08
	6	14:53:06	56:07:32	38:04:31	18:03:01
	2	2:59:15	94:49:48	50:59:02	43:50:46
	4	8:40:16	60:12:01	42:23:15	34:33:20
	1	5:59:19	0:01:40	0:01:18	0:00:22
Всего	76	183:56:46	1088:30:35	627:52:43	477:23:40

Рис. 21: Рисунок 24. Табличная часть «Отчёта по опозданиям»

Как уже говорилось, сводный отчёт содержит совокупную информацию об опозданиях, активности и продуктивности / непродуктивности работы сотрудников. Он тоже состоит из двух частей — графической и табличной. Табличная часть отчёта показана на рис. 25.

Пользователь	Общее время	Активное время	Время простоя	Продуктивное время	Непродуктивное время	Кол-во опозданий	Общее время опозданий
	2:22:57	0:56:41	1:27:30	0:33:57	0:03:53	2	10:00:00
	24:09:36	14:04:44	10:04:52	10:27:24	0:01:17	3	8:11:00
	10:02:12	1:00:44	9:01:28	0:25:54	0:00:00	2	11:57:00
	79:39:27	36:59:18	42:40:09	17:02:53	1:36:37	1	1:51:55
	4:15:14	1:13:38	3:01:36	0:50:02	0:00:00	3	17:51:59
	60:11:51	38:35:18	21:36:33	33:29:19	0:11:49	4	5:02:32
	13:14:17	9:46:45	3:27:32	5:12:15	0:19:22	3	10:54:38
	46:15:51	39:05:26	7:10:25	22:58:13	0:35:58	2	1:13:23
	51:51:44	29:07:18	22:44:26	15:00:57	0:15:56	3	1:07:42
	61:52:25	22:14:33	39:37:52	16:54:44	0:00:34	4	9:55:20
	5:53:03	4:15:06	1:37:57	2:03:46	0:07:22	1	1:52:17
	40:39:01	31:45:32	8:53:29	29:05:31	0:07:27	5	15:25:19
	72:04:37	38:56:22	33:08:15	33:58:44	0:02:31	3	5:19:59
	53:52:20	27:42:27	26:09:53	16:30:51	0:01:38	2	4:00:08
	46:37:23	32:09:11	14:28:12	28:38:30	0:01:43	5	4:23:37
	53:59:09	33:50:29	20:08:40	30:39:47	0:00:33	5	6:19:10

Рис. 22: Рисунок 25. Табличная часть «Сводного отчёта» (фрагмент)

Как видно, здесь содержатся точные измерения по каждому типу времени, а также количество и общее время опозданий. Напомним, что данная информация будет достоверной только в том случае, если у всех пользователей корректно настроен календарь и им присвоены расписания, соответствующие реальным графикам работы сотрудников.

В свою очередь графическая часть содержит три компонента: сведения об опозданиях, об активности (рис. 26) и о продуктивности (рис. 27). Первый из названных компонентов полностью совпадает с графической частью «Отчёта об опозданиях», которую мы показывали на рисунке 23, поэтому отдельно его иллюстрировать мы не станем.

Компонент со сведениями об активности показывает суммарное время по каждому пользователю за заданный при формировании отчёта период, выделяя по 10 наиболее и наименее активных пользователей.

Третий компонент показывает суммарное время продуктивной и непродуктивной работы сотрудников за заданный период, схожим образом выделяя 10 пользователей, которые активнее всех пользовались ресурсами категорий «Продуктивно» и «Премиально», и 10 человек, которые больше всего времени посвящали ресурсам из категории «Непродуктивно».

Группа отчётов «Табели» «Табели» — это группа стандартных регламентированных отчётов за месяц, используемых в бухгалтерии и отделах кадров для начисления заработной платы. Их чтение не вызывает трудностей, поэтому просто приведём примеры фрагментов трёх отчётов из этой группы: табель рабочего времени (рис. 28) — основной отчёт для бухгалтерии и отдела кадров; табель активного времени (рис. 29); табель использования принтера (рис. 30).

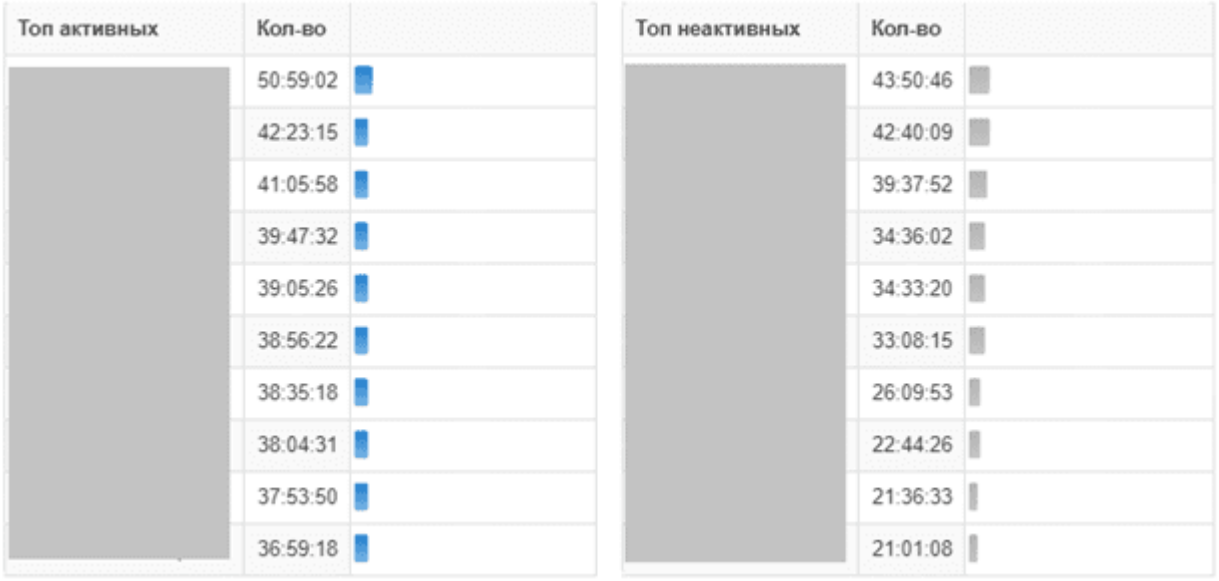


Рис. 23: Рисунок 26. Графическая часть «Сводного отчёта»: сведения об активности

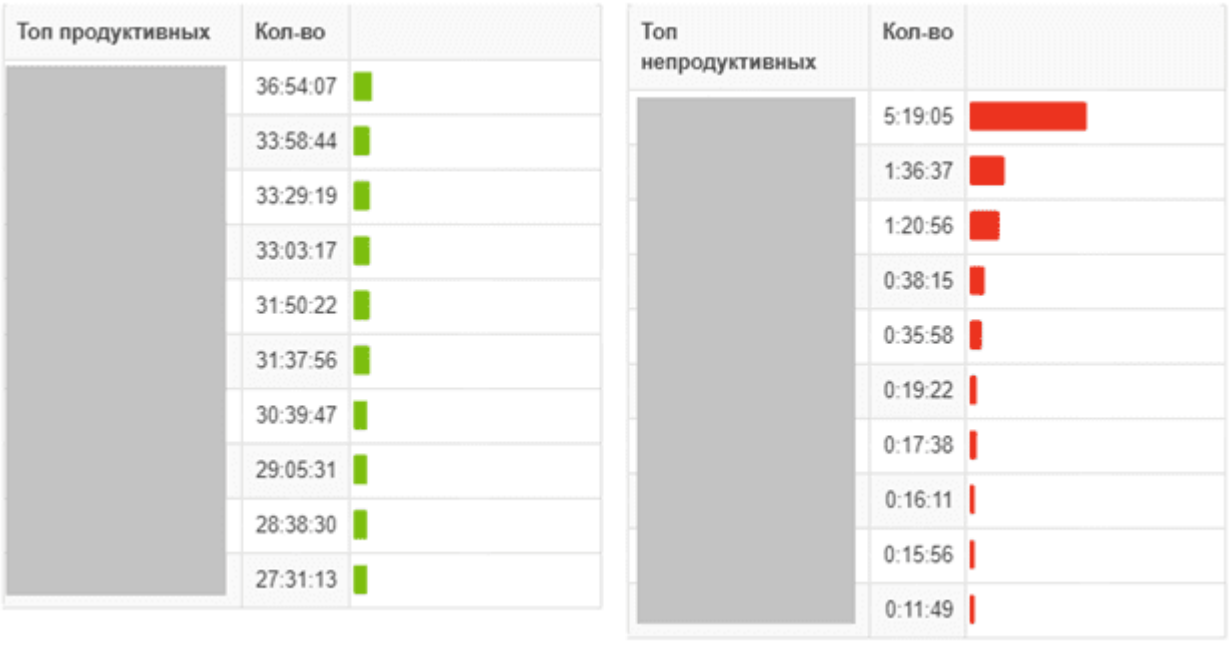


Рис. 24: Рисунок 27. Графическая часть «Сводного отчёта»: сведения о продуктивности

Пользователь	Отметки по числам месяца																За		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	x	I половину месяца	II половину месяца	месяц
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	дни	дни	дни
																	кол-во (чч:мм)	кол-во (чч:мм)	кол-во (чч:мм)
																	0	12	12
Сотрудник 1			0:52	9:40	9:29			11:58	8:41	10:18	10:14	14:52	6:08	1:11	11:43	13:40	0:00	108:52:00	108:52:00
	21:04																1	12	13
Сотрудник 2			0:54	6:42	7:52			9:09	9:06	8:56	9:02	8:09	0:45	0:21	11:58	20:59	21:04	93:59:00	115:03:00
																	0	10	10
Сотрудник 3				1:27	11:11			11:12	8:59	11:01	8:56	8:59	4:09		11:43	9:23	0:00	87:05:00	87:05:00
																	0	10	10
Сотрудник 4				9:13	10:46			9:21	9:04	9:03	8:49	8:41		1:16	10:11	9:03	0:00	85:30:00	85:30:00
																	0	3	3
Сотрудник 5									3:53						0:20	9:30	0:00	13:44	13:44
																	0	10	10
Сотрудник 6					6:12			9:58	9:00	9:58	8:58	8:48	0:05	13:20	9:44	9:07	0:00	85:14:00	85:14:00
		9:26	9:13	9:52	9:33	8:22				10:09	9:38	8:42	8:05				9	12	21
Сотрудник 7	8:54	9:09	8:20	9:02	8:49			8:59	9:05	8:58	9:08	9:05			10:31	11:14	83:02:00	111:20:00	194:23:00
																	0	2	2
Сотрудник 8										5:59	1:31						0:00	7:30	7:30
		10:27	10:28	11:50	10:05	10:12				11:24	9:39	12:33	11:18				9	14	23
Сотрудник 9	11:35	8:46	12:25	10:38	10:36			10:58	12:35	10:45	9:32	9:07	6:21	13:05	22:55	12:33	98:00:00	161:58:00	259:58:00
	20:57																1	3	4

Рис. 25: Рисунки 28. Табель рабочего времени

Пользователь	Отметки по числам месяца																За		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	x	I половину месяца	II половину месяца	месяц
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	дни	дни	дни
																	кол-во	кол-во	кол-во
																	0	12	12
Сотрудник 1			0:17	5:50	6:58			9:08	6:10	7:59	8:52	9:44	0:32	0:50	8:16	8:39	0:00	73:23:00	73:23:00
	7:35																1	12	13
Сотрудник 2			0:20	4:45	6:04			7:11	7:12	5:53	7:03	5:14	0:49	0:16	7:36	7:46	7:35	60:14:00	67:49:00
																	0	10	10
Сотрудник 3				1:02	6:08			5:14	6:04	5:22	6:02	7:35	1:33		6:41	6:49	0:00	52:34:00	52:34:00
																	0	10	10
Сотрудник 4				6:42	7:28			6:16	6:28	6:37	5:56	5:23		0:44	6:38	7:15	0:00	59:33:00	59:33:00
																	0	3	3
Сотрудник 5									3:20						0:16	6:59	0:00	10:37	10:37
																	0	10	10
Сотрудник 6					3:46			4:56	7:35	7:09	7:10	9:37	0:08	0:19	6:34	7:30	0:00	54:49:00	54:49:00
		6:36	5:56	6:54	6:46	5:44				7:29	6:42	6:49	5:04				9	12	21
Сотрудник 7	6:13	6:18	5:54	6:42	5:09			5:47	6:38	6:27	6:25	7:47			5:53	7:32	58:03:00	76:51:00	134:55:00
																	0	2	2
Сотрудник 8										5:00	1:27						0:00	6:27	6:27
		8:14	6:58	7:08	7:00	6:04				7:21	7:20	7:47	7:11				9	14	23
Сотрудник 9	6:44	7:05	7:13	7:03	8:20			7:22	7:21	7:11	7:08	8:08	9:49	12:52	8:00	9:47	65:06:00	114:09:00	179:16:00

Рис. 26: Рисунки 29. Табель активного времени

Пользователь	Отметки по числам месяца																За		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	x	I половину месяца	II половину месяца	месяц
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	кол-во	кол-во	кол-во
Сотрудник 1		45	40									18					0	103	103
Сотрудник 2				30	93	10		5									133	5	138
Сотрудник 3									17	10							0	27	27
Сотрудник 4			38	1				26	7	11	3	2	3				5	88	93
Сотрудник 5					6												0	6	6
Сотрудник 6		1															1	0	1
Сотрудник 7	1			10	1						6	15					31	35	66
Сотрудник 8				1				5									0	6	6
Сотрудник 9											2						0	2	2
		2		25		1					1		12						

Рис. 27: Рисунки 30. Табель использования принтеров (фрагменты)

4.6.6 Выводы

Учёт рабочего времени, активности и эффективности сотрудников является важной частью деятельности любого предприятия. Система учёта рабочего времени, входящая в программный комплекс iBatyr Monitor , позволит руководству оперативно (в том числе и «на лету») анализировать эффективность работы сотрудников, выделяя «лентяев», к которым стоит применить меры финансового и дисциплинарного воздействия, и «стахановцев», которых можно (и нужно!) поощрить. В свою очередь, использование стандартных отчётов (табелей) облегчит работу сотрудников отдела кадров — они смогут получать документы для расчёта заработной платы в бухгалтерии буквально одним щелчком мыши.

Глава 5

Часто задаваемые вопросы

5.1 Время активности

Содержание

- *Время активности*
  - *Как включить*
  - *Как рассчитывается время активности*
  - *Для чего используется время активности*
    - *Как это работает*
  - *Что влияет на учет активного времени*

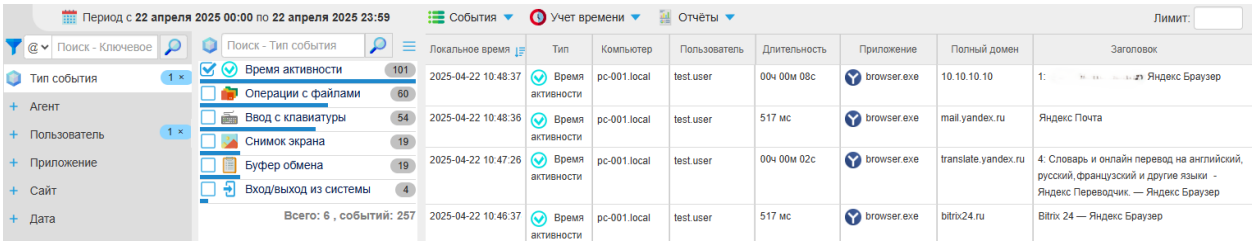
Время активности — это событие, которое помогает понять, насколько эффективно сотрудник использует рабочее время. Широко применяется *в политиках и отчётах* для оценки продуктивности.

5.1.1 Как включить

Для активации события **Время активности** включите модули:

- *Контроль программ* → *Запуск приложений*,
- *Учет активности* → *Активность приложений*.

Чтобы посмотреть события с данными активности сотрудников, выберите в конструкторе *Тип события* → *Время активности*.



5.1.2 Как рассчитывается время активности

Время считается активным, если фиксируются нажатия клавиш, клики мыши или другие действия с устройствами ввода. По умолчанию 120 секунд после последнего действия засчитываются как активные.

Пример работы:

Время	Действие	Статус активности	Комментарий
14:30:00	Ввод поискового запроса в браузере	Активен	Начало периода активности
14:30:45	Клик мышью в Excel	Активен	Продолжение периода активности
14:31:30	**Последнее действие**	**Активен**	Продолжение периода активности
14:32:00	Нет действий	Активен	Период все еще считается активным, прошло 30 сек.
14:33:30	**Нет действий**	**Неактивен**	Завершился период активности, так как прошло **120** секунд
14:34:00	Новый ввод текста	Активен	Начало нового периода активности

Примечание: Период в **120 секунд** можно изменить в поле *Считать период активным после совершения действий клавиатурой или мышью в течение, секунд*. Например, увеличить для дизайнеров и проектировщиков, в работе которых возможны длительные паузы из-за работы графических редакторов и CAD-систем.

5.1.3 Для чего используется время активности

Время активности используется для работы политик и построения отчетов.

Политика — инструмент, который анализирует входящие события на продуктивность и потенциальные риски.

Как это работает

1. События поступают на сервер, где их обрабатывают политики.
2. Если событие подходит под условия политики, ему присваивается *категория*:
   - **Премиально** — важные задачи, которые нужно выделить среди всей работы.
   - **Продуктивно** — время, проведенное за реальной работой.
   - **Нейтрально** — нейтральная деятельность, которую нельзя однозначно отнести к продуктивной или непродуктивной. Например, работа в Проводнике или RDP-подключение.
   - **Все остальное** — события **Времени активности**, для которых не сработала ни одна политика.

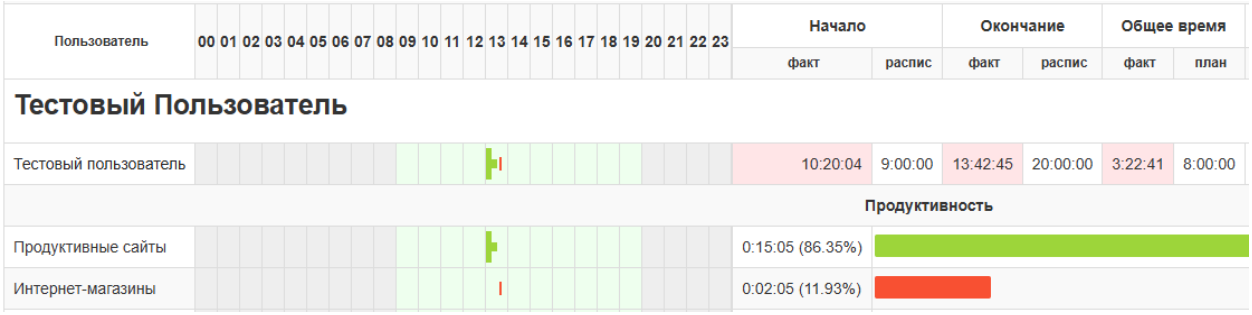
     Примечание: Чтобы отчеты были точнее, настройте политики для событий из категорий **Все остальное**.

   - **Непродуктивно** — непродуктивная деятельность. Явно нерабочая активность, например, развлекательные ресурсы или игровые приложения.
   - **Инциденты** — нарушение политик безопасности организации.

Пример. Пользователь *TestUser* в *13:36:21* зашел в интернет-магазин и скроллил страницу, а в *13:42:35* закрыл вкладку.

Локальное время	Тип	Компьютер	Пользователь	Длительность	Приложение	Полный домен	Заголовок
2025-04-22 13:42:35	Время активности	pc-001.local	test.user	00ч 00м 02с	browser.exe	www.ozon.ru	Купить с доставкой на OZON по низкой цене — Яндекс Браузер
2025-04-22 13:38:22	Время активности	pc-001.local	test.user	00ч 00м 02с	browser.exe	www.ozon.ru	Купить с доставкой на OZON по низкой цене — Яндекс Браузер
2025-04-22 13:37:21	Время активности	pc-001.local	test.user	00ч 01м 01с	browser.exe	www.ozon.ru	Купить с доставкой на OZON по низкой цене — Яндекс Браузер
2025-04-22 13:36:21	Время активности	pc-001.local	test.user	00ч 01м 01с	browser.exe	www.ozon.ru	Купить с доставкой на OZON по низкой цене — Яндекс Браузер

Политика **Социальные сети** присвоит этому событию категорию **Непродуктивно**. В **Комбинированном отчете** время с *13:36:21* до *18:38:22* отобразится красным, так как активность считается «живой» еще 120 секунд после последнего действия.



Примечание: График зависит от разрешения экрана и приблизительно отображает активность сотрудника, так как дробные значения отрисовываются целыми пикселями.

См.также:

Подробнее о настройке политик

Для анализа активности и продуктивности сотрудника используйте *Отчеты* и инструменты *Анализа*.

5.1.4 Что влияет на учет активного времени

На учет рабочего времени может влиять несколько факторов.

Рабочее расписание сотрудников
Определяет часы рабочей активности в зависимости от графика сотрудника. Настроить график можно в **Админ** → **Рабочее расписание**.

Календарь
Если в календаре указано, что день не рабочий из-за праздника, выходного, больничного, отгула и др., активность в этот день не фиксируется.

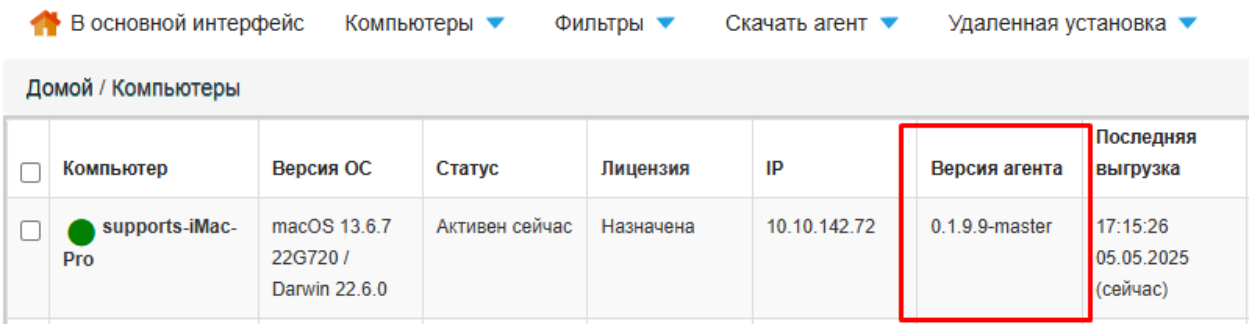
Учёт активности
В разделе конфигурации **Учёт активности** можно задать интервал бездействия для окончания активности. Для этого укажите значение в поле **Считать период активным после совершения действий клавиатурой или мышью в течение, секунд**.

Параметры сервера
Используйте настройку **Минимальное время активности**, чтобы установить время начала дня. Она помогает избежать ложного старта дня: например, если кто-то подвигал мышкой десять секунд в 7:30 утра, это не считается началом рабочего дня при пороге пять минут.

Присутствие на рабочем месте
Укажите в этом модуле **Начало и Конец рабочего дня** и активируйте **Собирать данные только в течение рабочего дня**, чтобы ограничить мониторинг активности рамками рабочего дня.

5.2 Как узнать версию агента?

Перейдите в **Панель управления** → **Компьютеры** в веб-интерфейсе. Номер версии указан в столбце **Версия агента**.



Кроме того, эту информацию можно посмотреть на компьютере, где установлен агент.

5.2.1 Windows-агент

Командная строка

Откройте **Командную строку** и введите команду:

```
# для 64-битной системы:

C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe version

# для 32-битной системы:

C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe version
```

Команда вернет версию агента.

Проводник

1. Откройте **Проводник** и перейдите по пути `C:\Windows\SysWOW64\TimeControlSvc\`.
2. Нажмите правой кнопкой мыши по файлу:

- `vmnetdrv64.exe` для 64-битных систем,
- `vmnetdrv32.exe` для 32-битных систем.

3. Выберите **Свойства**. Откроется окно свойств.
4. Переидите в вкладку **Подробнее**. В поле **Версия файла** будет указана версия агента.

5.2.2 Linux-агент

Терминал

Выполните в терминале команду:

```
sudo /usr/share/ibatyr/agent info
```

В выводе команды найдите строку `Agent` - она содержит версию агента.

5.2.3 MacOS-агент

Терминал

Откройте **Терминал** и введите команду:

```
sudo /Library/Application\ Support/.AtomSec/StaffAgent.app/Contents/MacOS/StaffAgent␣
↪version
```

Примечание: В зависимости от версии и сборки агента имя приложения может отличаться, например, *StaffService* вместо *StaffAgent*.

Finder

1. Откройте **Finder**.
2. Нажмите **Переход** → **Переход к папке...** или используйте сочетание клавиш Command+Shift+G.
3. Введите путь: `/Library/Application Support/.AtomSec/`.
4. Кликните правой кнопкой мыши по **StaffAgent**.
5. Выберите **Свойства**. В разделе **Версия** будет указана версия агента.

5.3 Не поступают данные от агентов

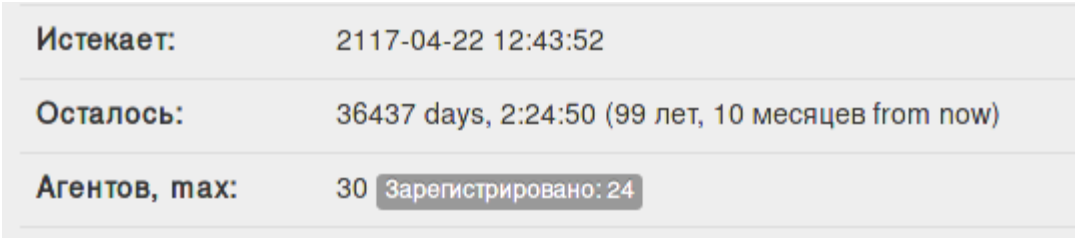
Если агент установлен на машине, но данные не поступают, выполните:

1. Убедитесь, что для агента указан корректный адрес сервера.

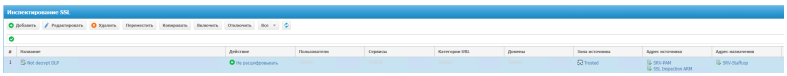
   URL сервера находится в отделе реестра:

   ```
   *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TimeSvc3\
   ↪ServiceConfiguration*.
   ```

2. Проверьте количество доступных лицензий. Количество лицензий отображается в веб-интерфейсе в разделе **Админ — Информация о лицензии**:



3. *Настройте исключения для антивируса*, в том числе запрет подмены сертификатов.
4. Добавьте адрес сервера в исключения, если в сети используются системы для инспекции SSL-трафика и подмены сертификатов.



См.также:

Официальную документацию Usergate по настройке правил инспектирования SSL.

5. Убедитесь, что процесс **vmnetdrv** запущен на клиентской машине.
6. Удостоверьтесь, что веб-интерфейс сервера доступен на машине агента по протоколу **https** на 443 порту.
7. Проверьте *права доступа администратора на просмотр событий*.
8. Синхронизируйте часовой пояс и время на клиентской машине и сервере. Часовой пояс и время сервера отображаются в разделе *Админ — Общая информация о сервере*.
9. Убедитесь, что в логе сервера нет записей типа **Conflict: HWID**.

   Для проверки запустите в консоли сервера команду:

```
sudo cat /var/log/ibatyr/ibatyr.log | grep -i "conflict"
```

   Если команда обнаружила конфликты HWID, *задайте агенту новый HWID*.

```
[WARNING] helpers:102 Conflict: HWID HWID123ABC567DE890F is same for PC-001.
↪testdomain.com and PC-002.testdomain.com
```

Если всё в порядке, но связи с агентами по-прежнему нет, *обратитесь в службу технической поддержки*.

5.4 HWID - Уникальный идентификатор диска

Уникальный идентификатор служит для закрепления агента в системе и данных, которые он передаёт на сервер. **hwid** агент берет в таком порядке:

- Серийный номер жесткого диска.
- Если ошибка, то MAC.
- Если ошибка, то серийный номер тома.

Примечание: В агенте, начиная с версии **5.8.2478** и новее, генерация **hwid** в реестре производится автоматически.

Примечание: С версии iBatyr Monitor 5.5 для Windows-агентов с версии 5.8.2583 возможна генерация HWID через *добавление параметров HWID в командную строку или название MSI-файла установки агента.*

В агенте, начиная с версии **5.8.2450** и новее, есть возможность задать **hwid** в реестре Windows, нужно создать значение вида **REG_SZ**.

```
[HKEY_LOCAL_MACHINE\SYSTEM\SCHWID]
«hwid»=«1111-2223»
```

Также корректировку **HWID** целесообразно делать, если в логе агента есть ошибка **Wrong CN!**

Редактируем значение реестра **hwid**, исключая оттуда пробелы.

Или создать файл с содержимым (значение HWID задайте свой по шаблону XXXX-YYYY)

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\SCHWID]
«hwid»=«1111-2223»
```

5.4.1 Автоматическая генерация HWID

Создает/заменяет значение hwid в реестре. Указанный ниже текст, нужно скопировать и вставить в файл, например **hwid.bat**.

```
@echo off
reg query "HKLM\SYSTEM\SCHWID" /v "hwid" > null
set I=22
set N=16
set CHAR=0 1 2 3 4 5 6 7 8 9 A B C D E F
set Hex=0
:LOOP
set /a R=1+%N%*%random%/32768
for /f "tokens=%R%" %%q in ("%CHAR%") do (set Hex=%%q%Hex%)
Set /a I-=1
If %I% GTR 0 goto LOOP
echo %Hex%
reg add HKLM\SYSTEM\SCHWID /f /v hwid /t REG_SZ /d %Hex%
:end
```

Выполнить этот скрипт можно с помощью такой команды:

```
cmd.exe /c hwid.cmd
```

После этого уникальный идентфикатор запишется в реестр системы и никогда больше не сможет поменяться.

5.4.2 Уникальный HWID

В некоторых случаях возникает конфликт HWID и информация по агентам некорректно отображается. Пример, есть доменные компьютеры и VDI, где используется образ рабочей станции с предустановленным ПО и слои с данными профиля для пользователей. Для решения проблемы была придумана новая опция, которая работает начиная с версии агента 5.8.2539.

Для создания уникального **HWID** необходимо добавить в ветку реестра HKEY_LOCAL_MACHINE\SYSTEM\SCHWID ключ формата **DWORD (32)** с названием **use_fqdn** со следующими значениями:

0 или отсутствие — логика получения HWID как сейчас

1 — вместо ID диска используется полное доменное имя (FQDN) компьютера в нижнем регистре, сохраняется в реестре и в дальнейшем используется из реестра.

2 — используется полное доменное имя (FQDN), но не сохраняется в реестре (**параметр hwid не используется**). В случае смены имени компьютера меняется HWID.

Внимание: Если HWID сформирован, то необходимо удалить из реестра. В противном случае HWID не изменится.

5.5 Vmnetdrv

Процесс агента называется **vmnetdrv32.exe** либо **vmnetdrv64.exe** в зависимости от разрядности ОС.

Если у вас на терминальном сервере очень много процессов **vmnetdrv**, то это нормально.

Число процессов **vmnetdrv64** равно количеству залогиненных сессий пользователей на терминальном сервере × 2 + 1

5.6 Замедление работы ПК

Если отдельные приложение или вся система после установки агента стали работать заметно медленнее, убедитесь, что программы расположены в стандартных папках:

- *C:|Program Files*,
- *C:|Program Files (x86)*,
- *C:|Programdata*,
- *C:|Windows*,
- *C:|Users|*AppData*.

Если приложение создаёт свои папки, добавьте их в исключения файлового мониторинга, чтобы не отслеживать системную активность приложений.
Например, **Файловый мониторинг** → **Пути и маски** → **Запретить**: *C:|1Cbuh|**

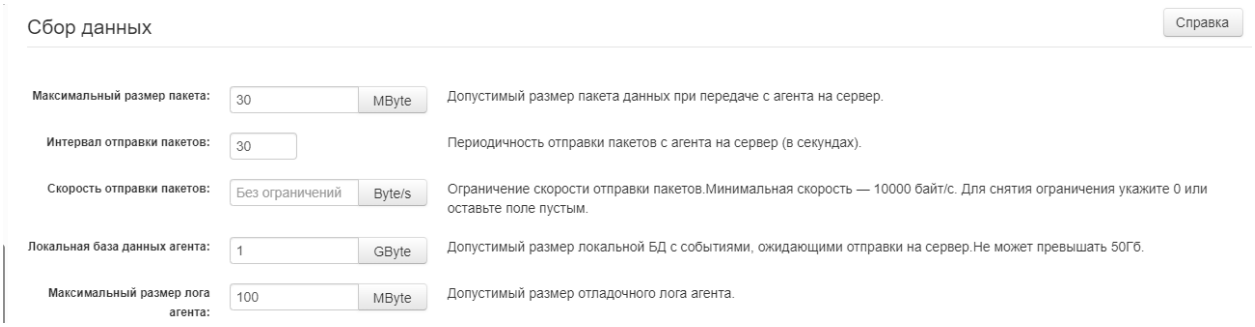
При медленной работе MS Excel запретите мониторинг буфера обмена: таблицы при копировании создают большую нагрузку.

5.7 Как сбросить накопленные данные на агенте?

Иногда возникает такая ситуация, когда применённая конфигурация неверна и агенты собирают или собрали слишком много данных, которые не имеют значения с точки зрения анализа и обработки этих данных на сервере.

Чтобы очистить накопленные данные на рабочих станциях пользователей:

1. Перейдите в раздел **Панель управления - Конфигурация компьютеров**.
2. Выбрите вашу конфигурацию.
3. В разделе **Сбор данных** установите значение **Локальная база данных агента** равным **0**.



После применения этой конфигурации, все сохраненные данные на локальных рабочих станциях пользователей будут удалены, а все новые события будут передаваться на сервер исправно.

5.8 Сертификат

Находится по пути

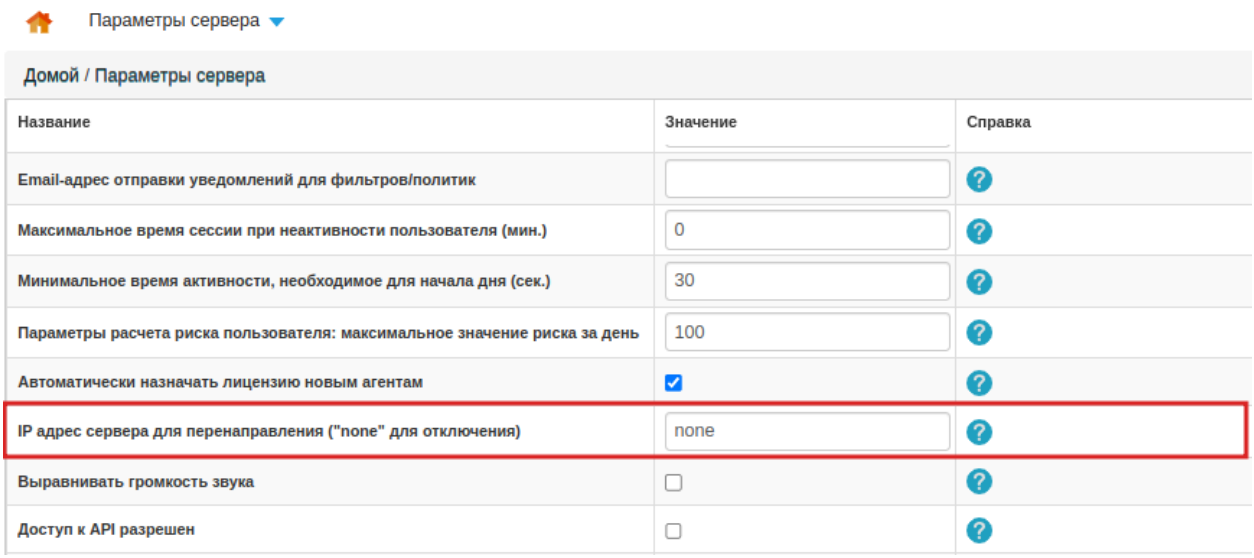
```
C:\Windows\System32\config\systemprofile\AppData\Roaming\TimeSvc3\TLS
```

Файл - **NeonLightInc.cer** - это самоподписанный корневой сертификат iBatyr Monitor .

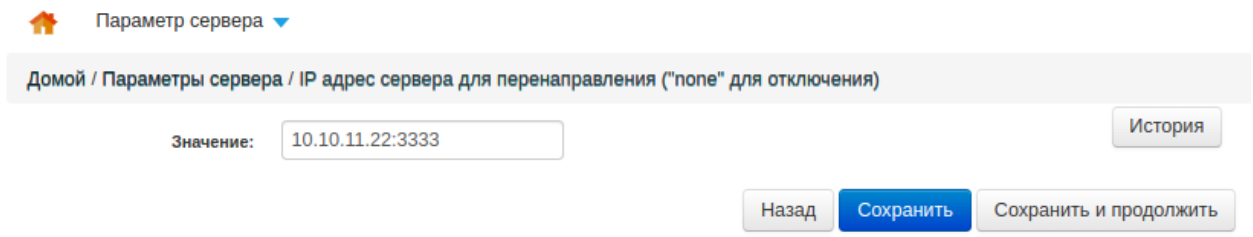
5.9 Смена IP-адреса сервера на агентах

5.9.1 Для всех агентов

IP-адрес сервера можно изменить в параметрах сервера: **Панель управления** → **Параметры сервера** → **IP-адрес сервера для перенаправления(«none» для отключения)**.



Порт указывается после двоеточия, например, 10.10.11.22:3333:



После сохранения настройки агенты будут перезапущены и направлены на новый сервер.

5.9.2 Windows

IP-адрес сервера или его доменное имя хранится в реестре Windows в ветке `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TimeSvc3\ServiceConfiguration` в параметре `Url`. Вы можете изменить IP-адрес сервера в параметре `Url`:

- вручную,
- с помощью команды:

```
REG ADD HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TimeSvc3\
↪ServiceConfiguration /v Url /t REG_EXPAND_SZ /d <ip-address> /f
```

  где `<ip-address>` — IP-адрес нового сервера.

После изменения параметра перезагрузите компьютер или перезапустите службу агента:

```
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe restart
```

При необходимости добавьте адрес резервного сервера с помощью скрипта:

```
set var=<ip-address:443>
set var2=<ip-address:порт>
REG ADD HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TimeSvc3\ServiceConfiguration /
```

(continues on next page)

(продолжение с предыдущей страницы)

```
↪v Url /t REG_EXPAND_SZ /d %var% /f
REG ADD HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TimeSvc3\ServiceConfiguration /
↪v Url2 /t REG_EXPAND_SZ /d %var2% /f
C:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe restart
```

Примечание: Скрипт необходимо запускать от имени администратора.

5.9.3 Linux

Смена IP-адреса сервера для Linux-агента:

```
sudo /usr/share/ibatyr/agent <ip-адрес> <порт> restart
```

где

<ip-address> — IP-адрес нового сервера. <порт> — порт сервера. Параметр можно пропустить, если вы не меняли порт по инструкции *Смена стандартного порта 443*.

5.10 Перестали скачиваться файлы в Skype

Если при включенном перехвате переписки перестали скачиваться файлы в Skype (веб-версия или приложение):

1. Перейдите в раздел **Панель управления — Глобальная конфигурация**.
2. Проверьте Правила на соответствие приведённым значениям:

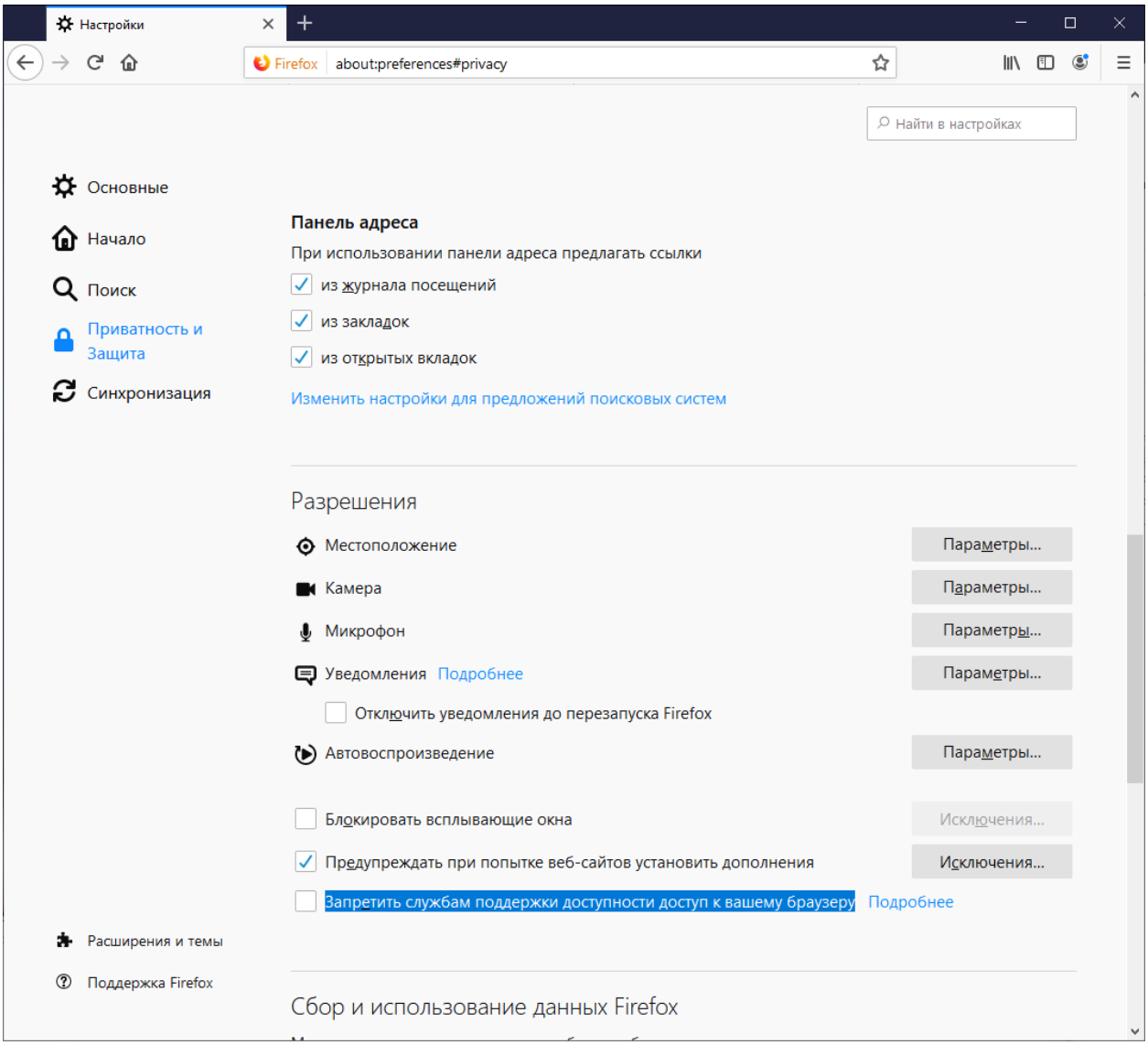
tabularytabulary

Правило
Сетевой мониторинг – Приложения - Запретить
Подмена сертификата – Разрешить
Подмена сертификата – Запретить

5.11 Отсутствует время активности в Mozilla Firefox

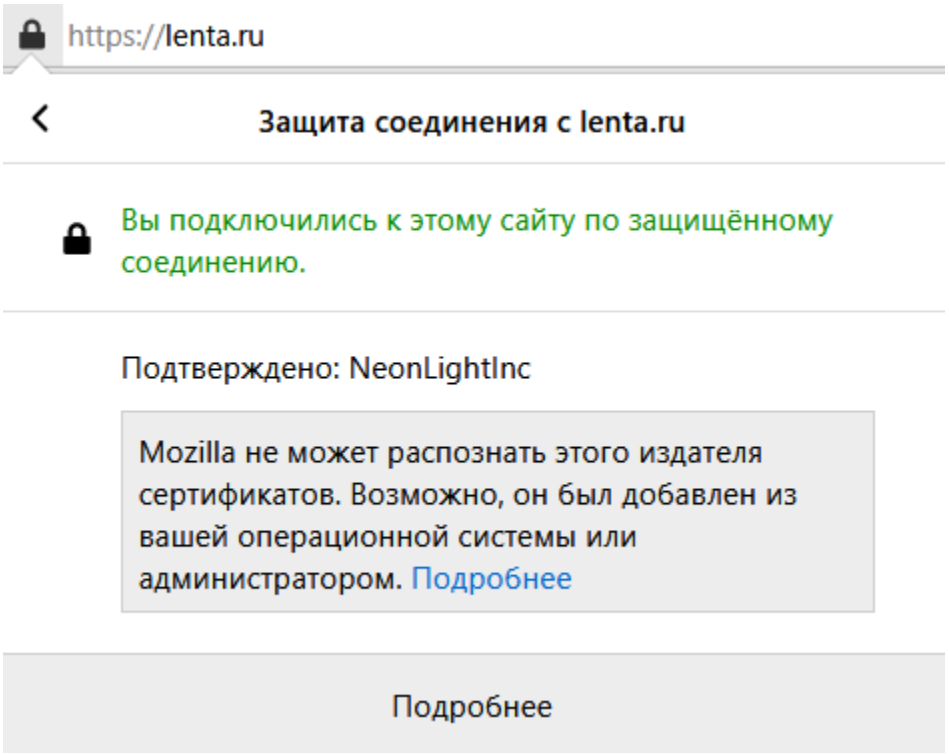
Если у вас отсутствует время активности на сайтах при использовании браузера Firefox:

1. Проверьте, не включен ли параметр «Запретить службам поддержки доступности доступ к вашему браузеру».

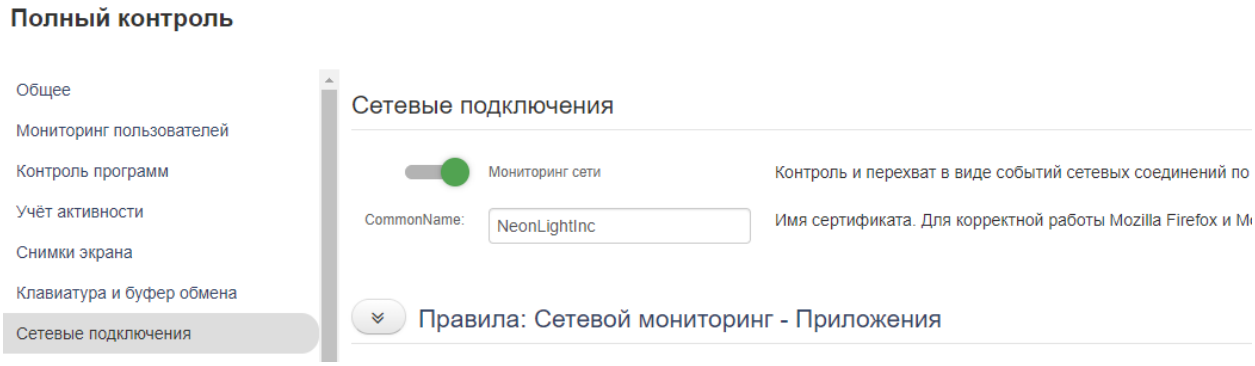


2. Проверьте, подменяется ли сертификат в браузере.

Имя сертификата iBatyr Monitor - NeonLightInc



3. Проверьте, включен ли модуль «Мониторинг сети» в конфигурации компьютеров.



Если все пункты выполнены, но время активности при посещении сайтов не отображается в веб-интерфейсе, обратитесь в службу технической поддержки по адресу support@ibatyr.kz.

5.12 Не открываются сайты в Google Chrome

5.12.1 Проблема

Некоторые сайты не открываются в браузере Google Chrome.

5.12.2 Причина

Возможно, у вас включен криптографический алгоритм **Kyber** (**TLS 1.3 hybridized Kyber support**), предназначенный для защиты данных от будущих квантовых угроз.
Kyber — экспериментальная технология, поэтому её поддерживают не все сайты.

5.12.3 Решение

Отключите поддержку Kyber в настройках Google Chrome.

1. **Откройте настройки экспериментальных опций в Chrome:**

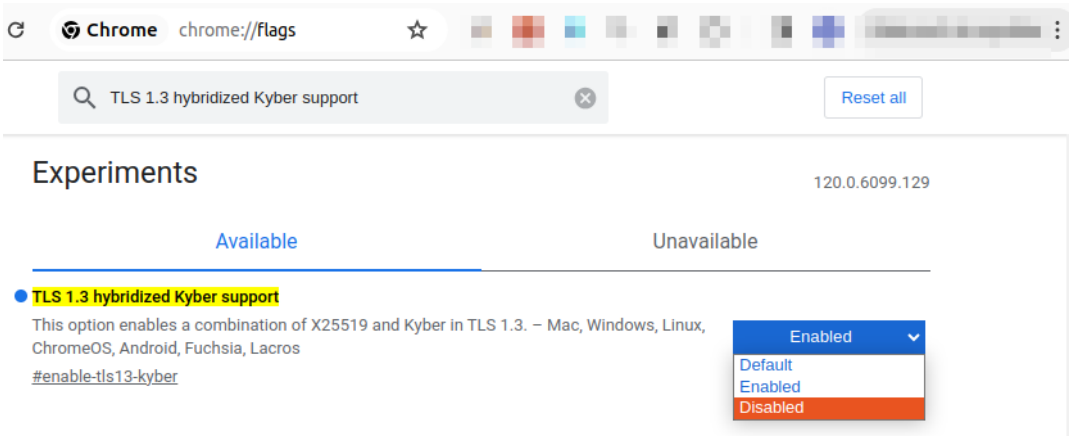
   Введите в адресной строке браузера *chrome://flags/* и нажмите Enter.

2. **Найдите Kyber:**

   В поле поиска введите *TLS 1.3 hybridized Kyber support*.

3. **Отключите поддержку Kyber:**

   Измените у **TLS 1.3 hybridized Kyber support** значение с **Default** на **Disabled**.



4. **Перезапустите Chrome:**

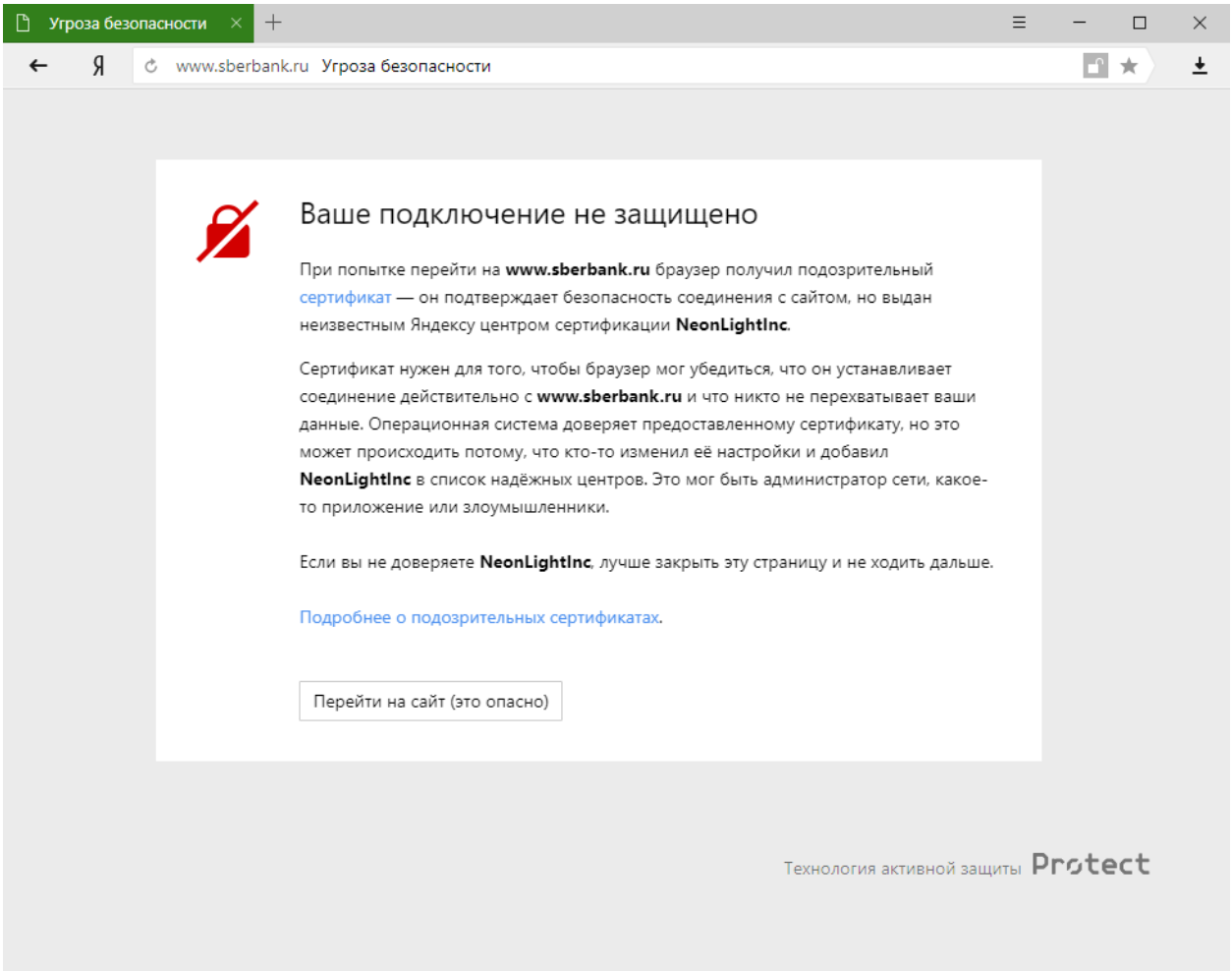
   Нажмите кнопку **Relaunch**.

После перезапуска браузера поддержка Kyber будет отключена. Сайты должны загружаться корректно.

Если проблема с загрузкой сайтов не исчезнет, рекомендуем проверить другие настройки браузера или сетевые параметры.

5.13 Яндекс Браузер показывает ошибки SSL-соединений

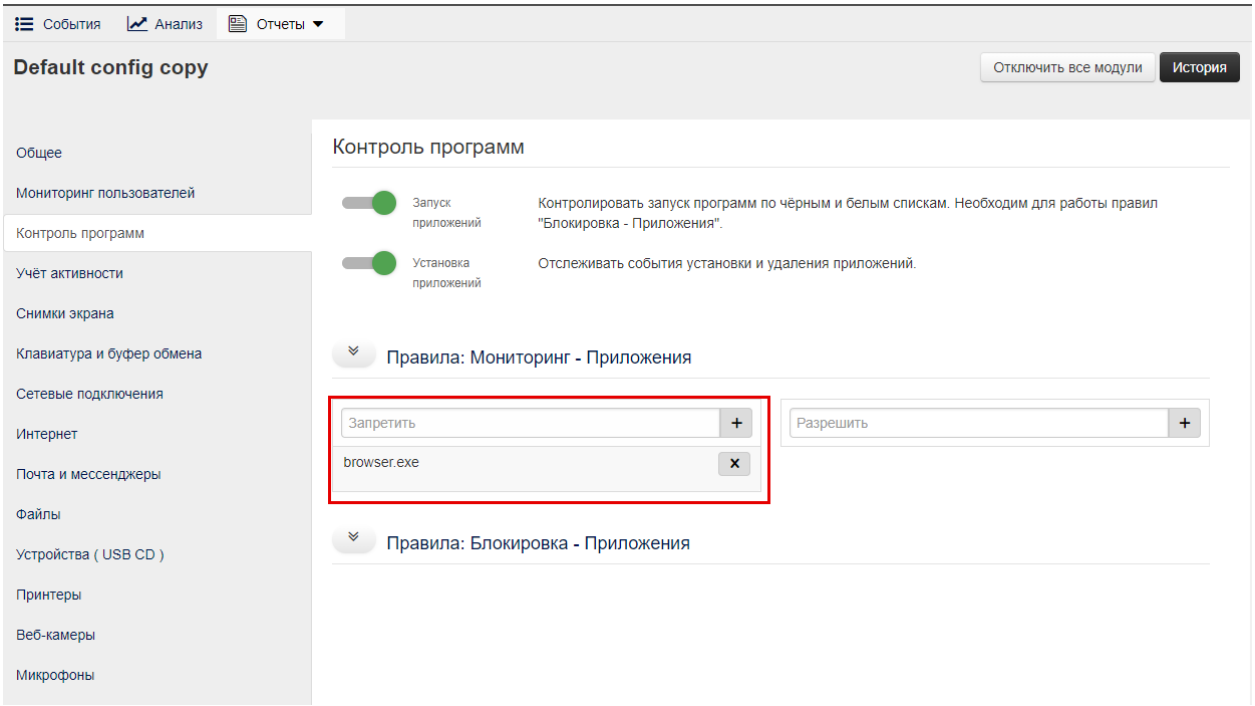
Ошибка незащищенного подключения означает, что Яндекс Браузер перестал доверять SSL-сертификату iBatyr Monitor.



Яндекс регулярно удаляет сертификат из-за особеностей технологии Protect .

Чтобы решить проблему:

1. Перейдите **Панель управления** → **Конфигурация комьютеров**.
2. Выберите текущую конфигурацию.
3. Перейдите в **Контроль программ** → **Правило: Блокировка — Приложение**.
4. Добавьте *browser.exe* в поле **Запретить** для запрета перехвата процесса Яндекс Браузера.



Второе решение — используйте Яндекс Браузер для организаций.

5.14 502 Error

В некоторых случаях вместо веб-интерфейса отображается белая страница, на которой написано *502 Error*.

В этом случае откройте серверную консоль и выполните:

1. Проверьте статус СУБД.

```
sudo service postgresql status
```

если служба не запущена, перезапустите ее.

```
sudo service postgresql restart
```

2. Если запуск не происходит, то, скорее всего, проблема в базе данных. Проблем может быть много, но наиболее вероятная — переполнение диска.

```
df -h
```

Если диск заполнен на 100%, выполните *автоматическую* или *ручную* очистку диска.

3. Перезапустите сервис iBatyr Monitor:

```
sudo service ibatyr restart
```

5.15 Изменение шаблонов отчетов

Чтобы изменить шаблон отчета:

1. Найдите нужный шаблон в папке /**usr**/**share**/**ibatyr**/**reports**/**templates**/.
2. Создайте папку для своего отчета в разделе /**usr**/**share**/**ibatyr**/**override**/ :

```
mkdir -p /usr/share/ibatyr/override/report/
```

3. Скопируйте файл шаблона в созданную папку:

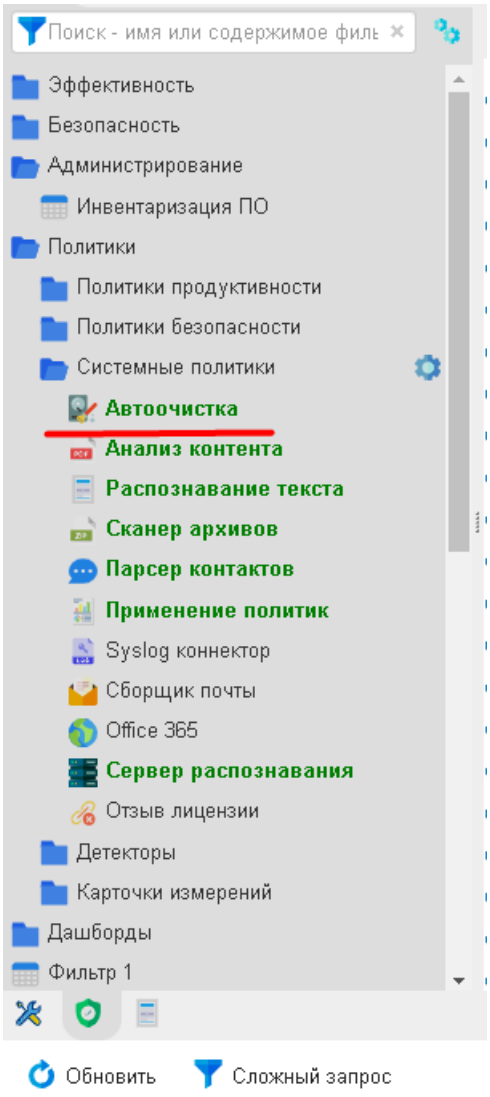
```
cp /usr/share/ibatyr/reports/templates/report/template_name.html /usr/share/
↪ibatyr/override/report/
```

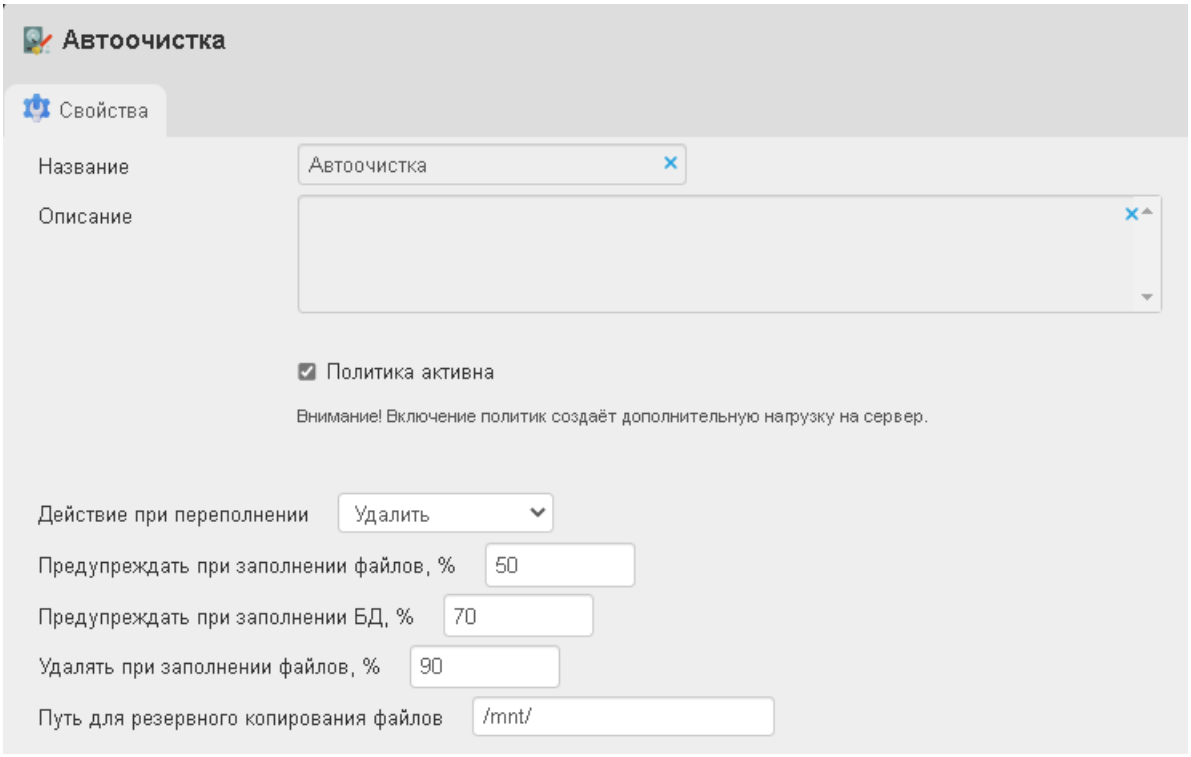
4. Отредактируйте скопированный шаблон.

5.16 Автоочистка

Чтобы проблема с переполнением жёсткого диска не возникала, заранее оцените объёмы данных, которые необходимо будет хранить, и настройте автоматическую очистку диска.

Автоочистка — системная предустановленная политика. Чтобы настроить её, в разделе **Политики** перейдите в папку **Политики** → **Системные политики** и выберите **Автоочистка**.


Поиск - имя или содержимое филь
Эффективность
Безопасность
Администрирование
Инвентаризация ПО
Политики
Политики продуктивности
Политики безопасности
Системные политики
Автоочистка
Анализ контента
Распознавание текста
Сканер архивов
Парсер контактов
Применение политик
Syslog коннектор
Сборщик почты
Office 365
Сервер распознавания
Отзыв лицензии
Детекторы
Карточки измерений
Дашборды
Фильтр 1
Обновить
Сложный запрос



При заполнении диска данными больше, чем на указанный процент, iBatyr Monitor будет выполнять указанные действия.

Доступные для заполнения поля:

Поле	Описание
Действие при переполнении	Доступные варианты: • *Удалить* — удаляет 1% самых старых файлов; • *Переместить* — перемещает 1% самых старых файлов; • *Ничего* — ничего не делает (используется только при ручной очистке).
Предупреждать при заполнении файлов	Пороговый процент заполнения диска, с которого срабатывает оповещение.
Предупреждать при заполнении БД	Пороговый процент заполнения базы данных, с которого срабатывает оповещение.
Удалять, при заполении файлов	Удаление файлов при достижении порогового значения, если выбрано *Удалять*.
Путь для резервного копирования	Путь до каталога, на который примонтирован диск для сохранения бэкапов БД при превышении порога, если выбрано действие *Переместить*.

Если базы данных и файлы хранятся на разных дисках, то оповещение об их заполнении выглядит так:

Если базы данных и файлы хранятся на одном диске, то сообщение принимает вид: *Диск заполнен на %*.

5.17 Активация ключа

После установки сервера iBatyr Monitor при первом входе в веб-консоль необходимо пройти активацию сервера.

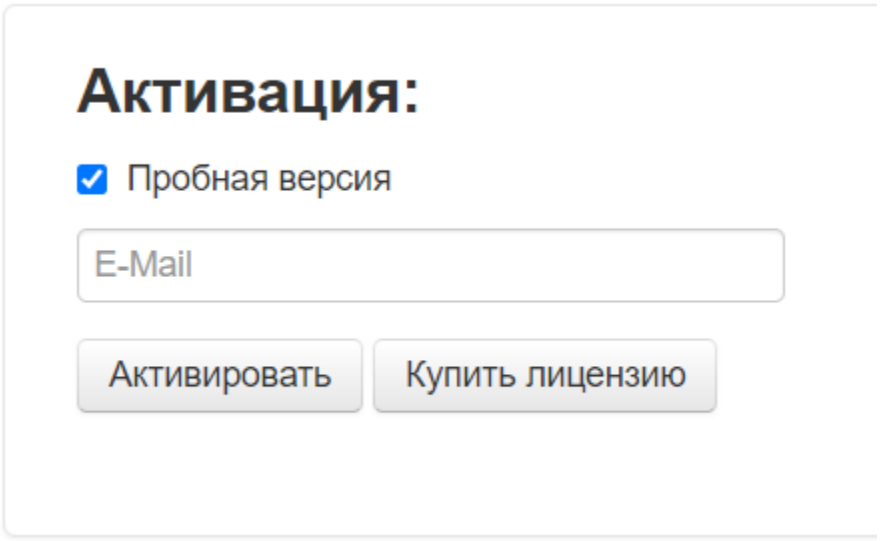
5.17.1 Активация пробной версии

Пробная версия предоставляет временную лицензию на 5 агентов сроком на 15 дней. Активировать пробную версию можно только онлайн.

Чтобы активировать пробную версию:

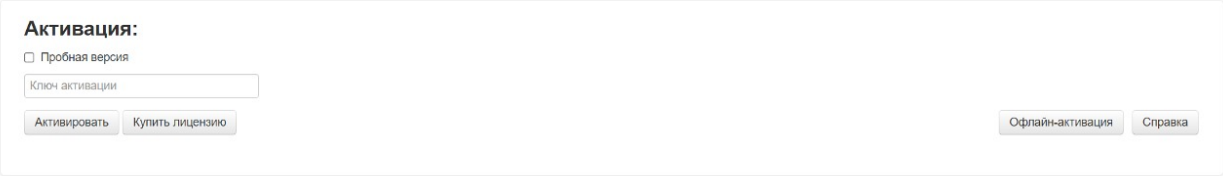
1. В окне выбора вариантов укажите **Пробная версия**.
2. Введите email для регистрации.
3. Нажмите **Активировать**.

В течение минуты откроется веб-интерфейс iBatyr Monitor .



5.17.2 Онлайн-активация по ключу

Если ваш ключ для пробной версии действует дольше 15 дней или у вас есть постоянный ключ, введите его в поле **Ключ активации** и нажмите кнопку **Активировать**. В течение минуты откроется веб-интерфейс iBatyr Monitor .



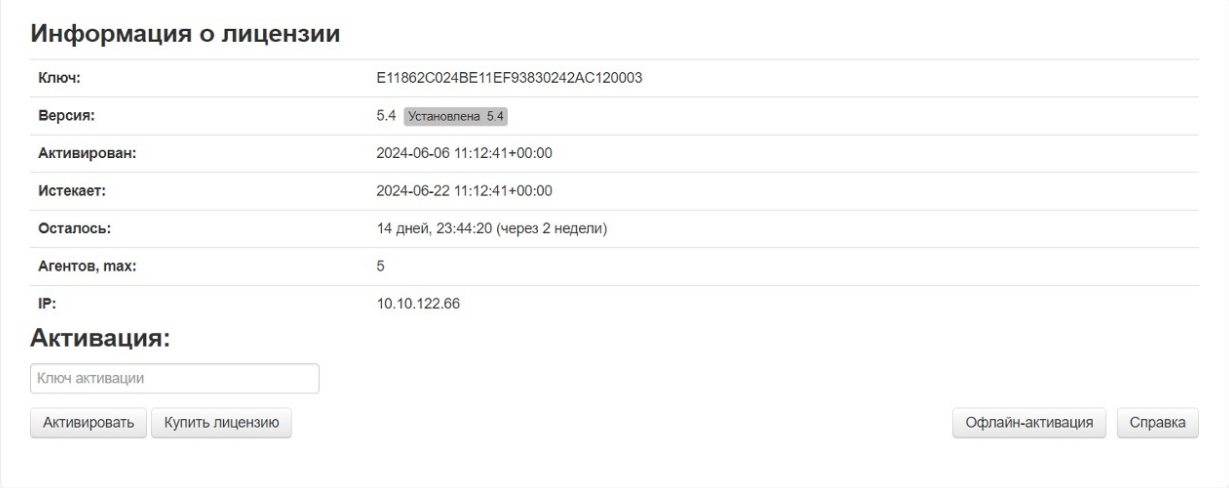
Также можно активировать сервер из командной строки:

```
ibatyr activate КЛЮЧ
```

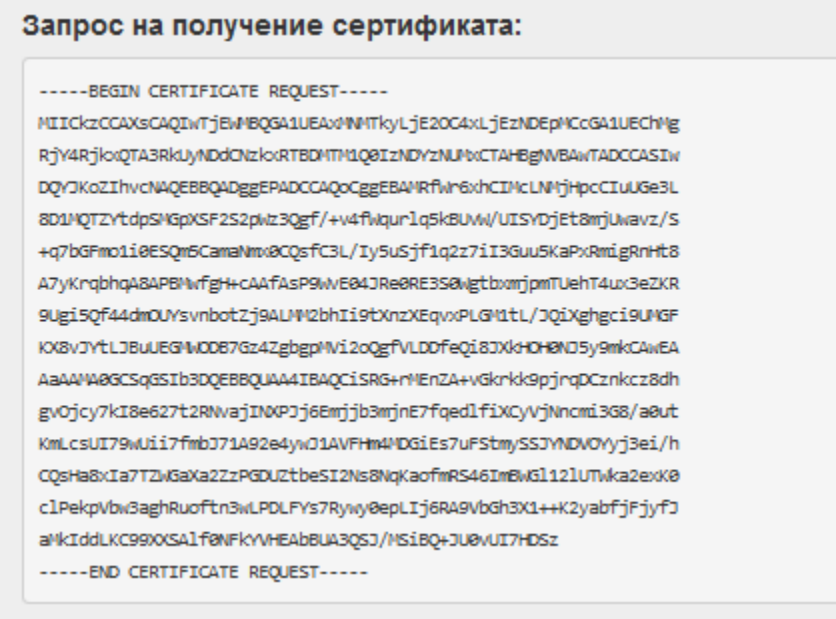
где КЛЮЧ — ключ активации сервера.

5.17.3 Офлайн-активация

Для офлайн-активации вставьте ключ в поле **Ключ активации** и нажмите кнопку **Офлайн-активация**.

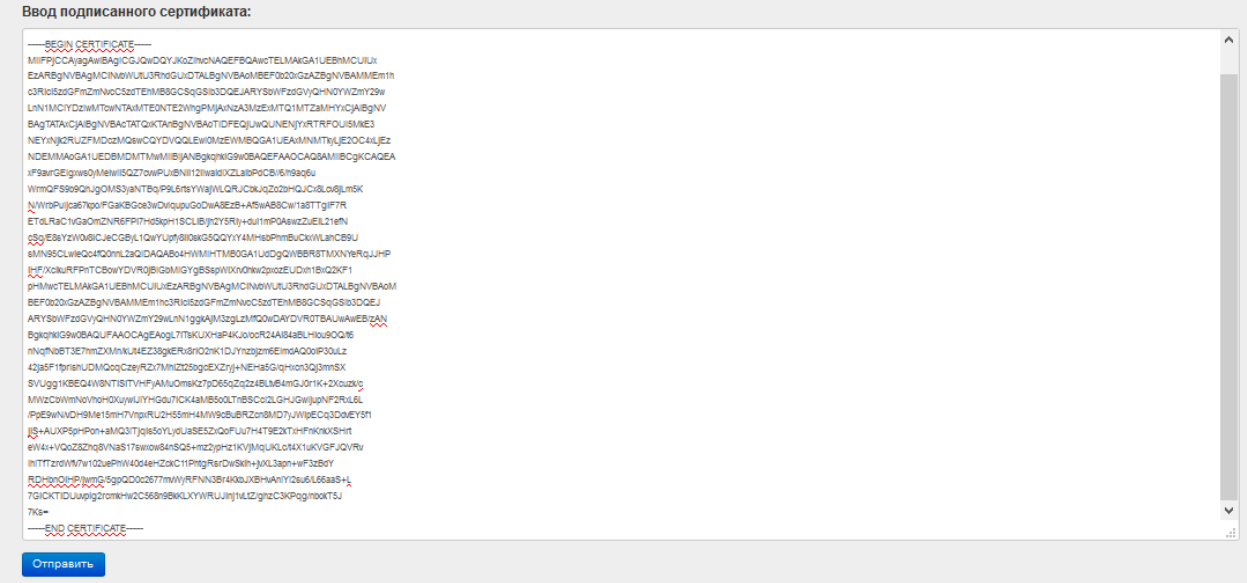


В открывшемся окне появится запрос на получение сертификата.



Скопируйте его и вместе с вашим ключом отправьте своему менеджеру iBatyr Monitor или в техподдержку на адрес *support@ibatyr.kz*.

В ответном письме придёт сертификат. Вставьте его в поле **Ввод подписанного сертификата** и нажмите **Отправить**. После этого в течение нескольких секунд откроется веб-интерфейс iBatyr Monitor .



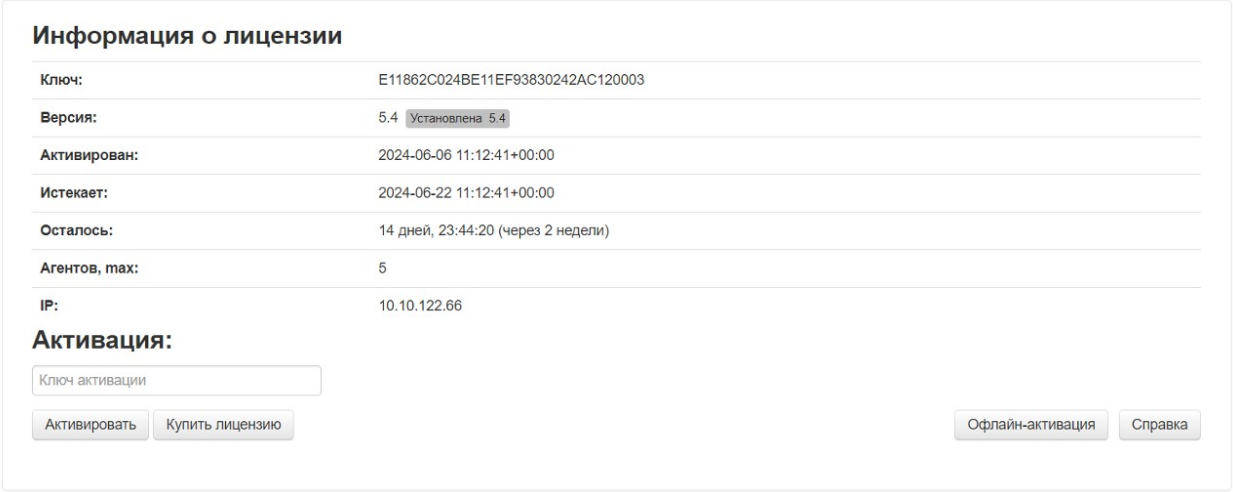
5.17.4 Повторная активация сервера

При повторной активации сервера из-за переноса сервера или новой установки обратитесь к вашему менеджеру или *в техническую поддержку*.

5.17.5 Новая активация уже зарегистрированного ключа

Если активация сервера уже произведена и вы хотите ввести расширенный ключ:

1. В веб-интерфейсе iBatyr Monitor зайдите в раздел **Админ** → **Информация о лицензии**.
2. В поле **Ключ активации** введите новый ключ.
3. Нажмите **Активировать** или **Офлайн-активация**.



5.18 Блокировка сайтов

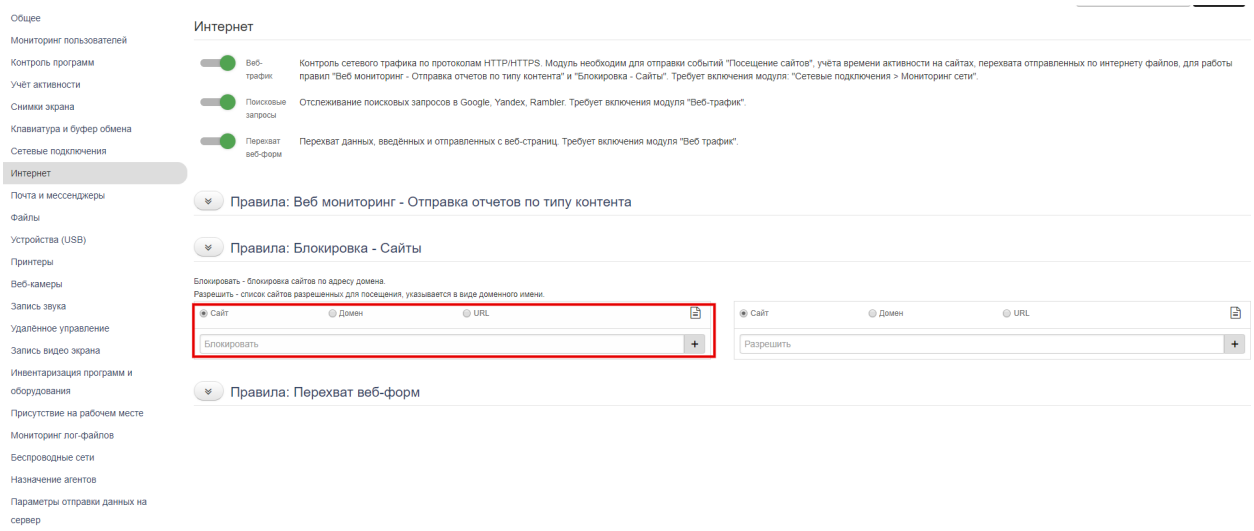
Сайты могут быть блокированы посредством черного, либо белого списков.

Для работы блокировки требуется включение модулей «Веб-трафик» и «Мониторинг сети».

5.18.1 Черный список:

Для того чтобы запретить доступ к определенным сайтам нужно выполнить следующее:

1. Перейти в конфигурацию, где находятся контролируемые пк, на которых нужно запретить доступ к этому сайту.
2. Выбрать пункт «Интернет» и в меню «Правила - Блокировка сайты» в пункте «блокировать» ввести сайты и нажать «Enter».

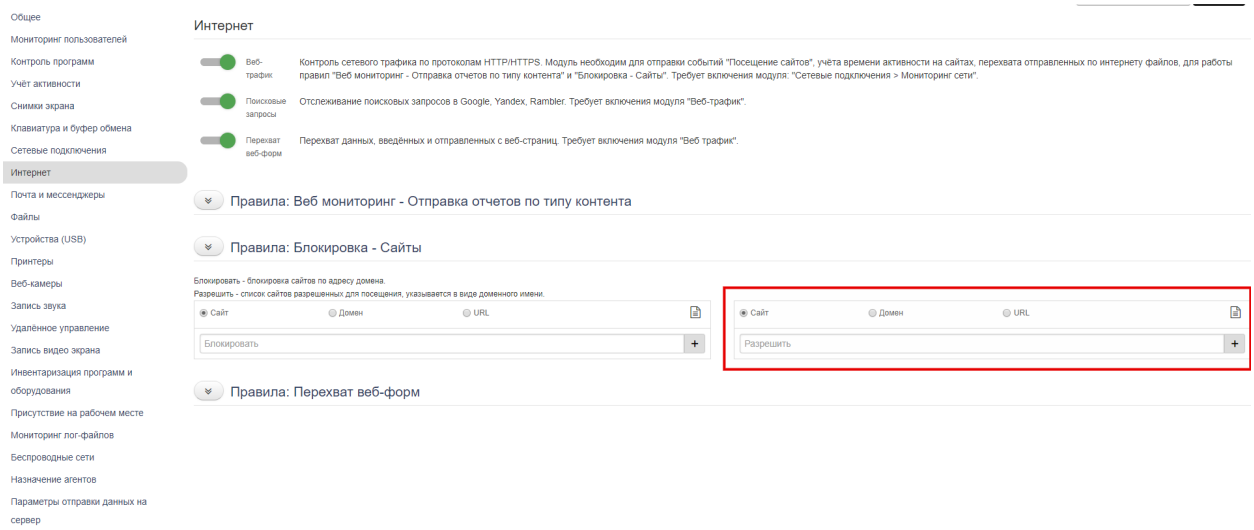


3. Нужно вписать все сайты, которые должны быть блокированы. Сайты пишутся в столбик, один под другим. Блокировка основного сайта блокирует поддомены.

5.18.2 Белый список:

Белый список позволяет задать сайты, которые посещать можно. Все остальные сайты будут заблокированы.

1. Так же, как и в предыдущем случае, переходим в нужную нам конфигурацию.
2. Выбрать пункт «Интернет» и в меню «Правила - Блокировка сайты» в пункте «разрешить» ввести сайты и нажать «Enter».

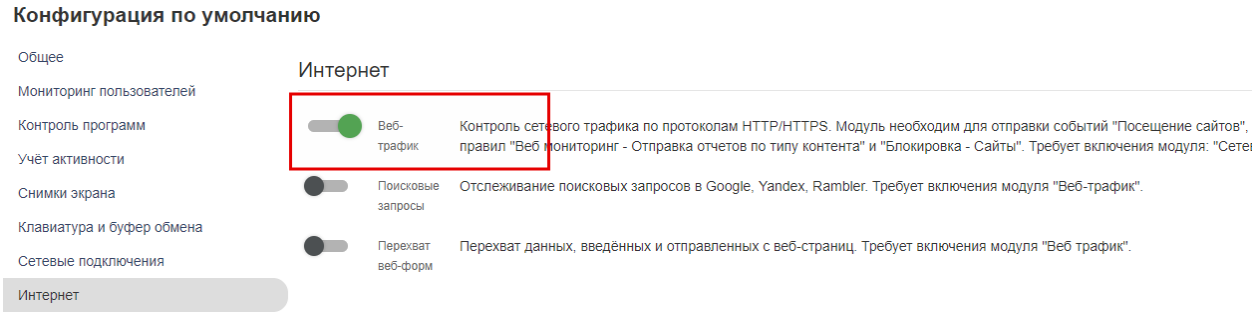


3. Задаем список разрешенных к посещению сайтов. Все остальные сайты будут запрещены.

5.18.3 Блокировка сайтов для Linux-агента

Начиная с версии 0.5.19, Linux агент позволяет блокировать сайты, которые находятся в «Правила - Блокировка сайты» - «Запретить»

Для этого нужно чтобы в конфигурации был включен «Веб-трафик»



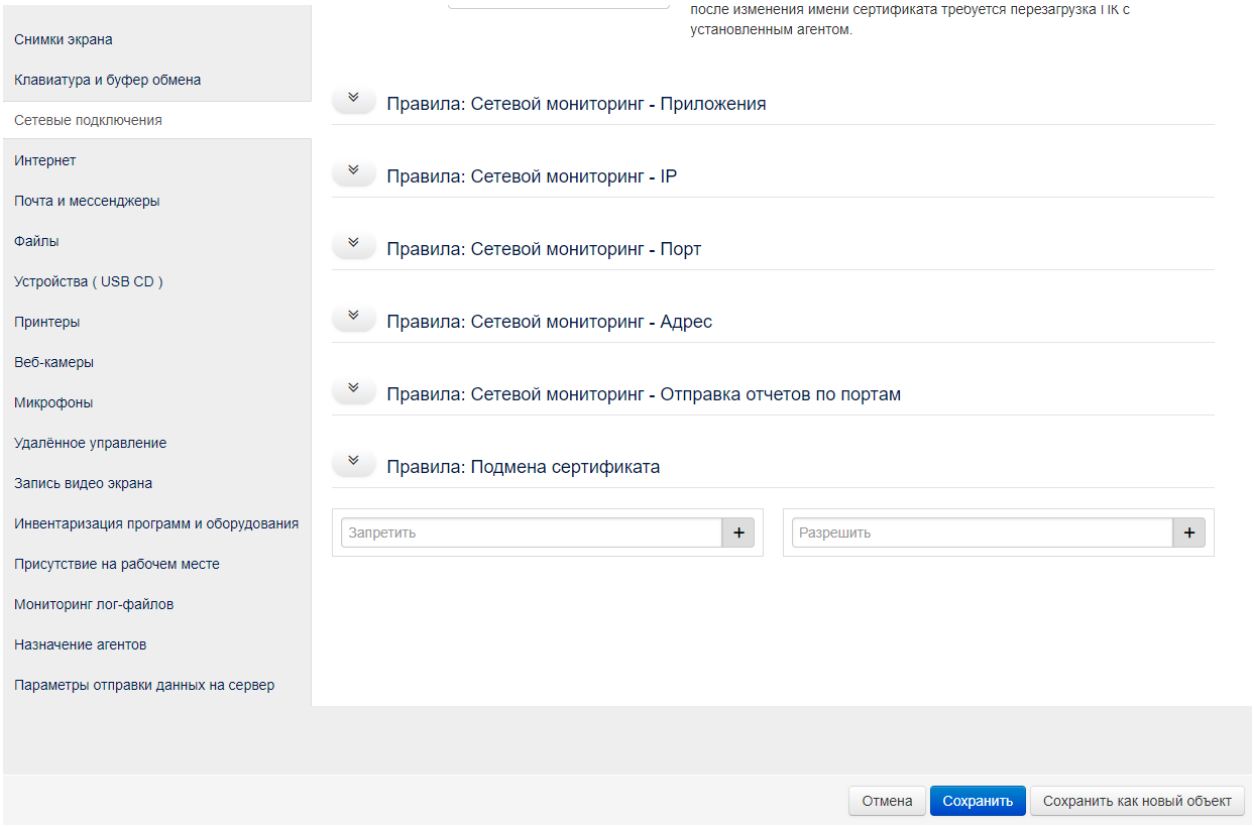
Поддерживается только BLACKLIST. Блокировки возможны по ipv4, ipv6 и по подстроке.

Примечание: в «Заблокировать» - указывается подстрока. то есть если написать mail - то будет заблокирован и gmail.com и mail.ru. Ipv4 - можно прописать 192.168.1.0/24 или просто 1.2.3.4

5.19 Госзакупки, электронные торговые площадки

Если после установки агента наблюдаются проблемы с сайтами госзакупок, электронными торговыми площадками, сайтами банков и т.д., следует запретить подмену сертификата на целевых ресурсах.

Для этого, перейдите в «Меню» - «Конфигурация агентов», выберите вашу конфигурацию и в поле «Запретить» введите сайты, на которых не нужно подменять сертификат.



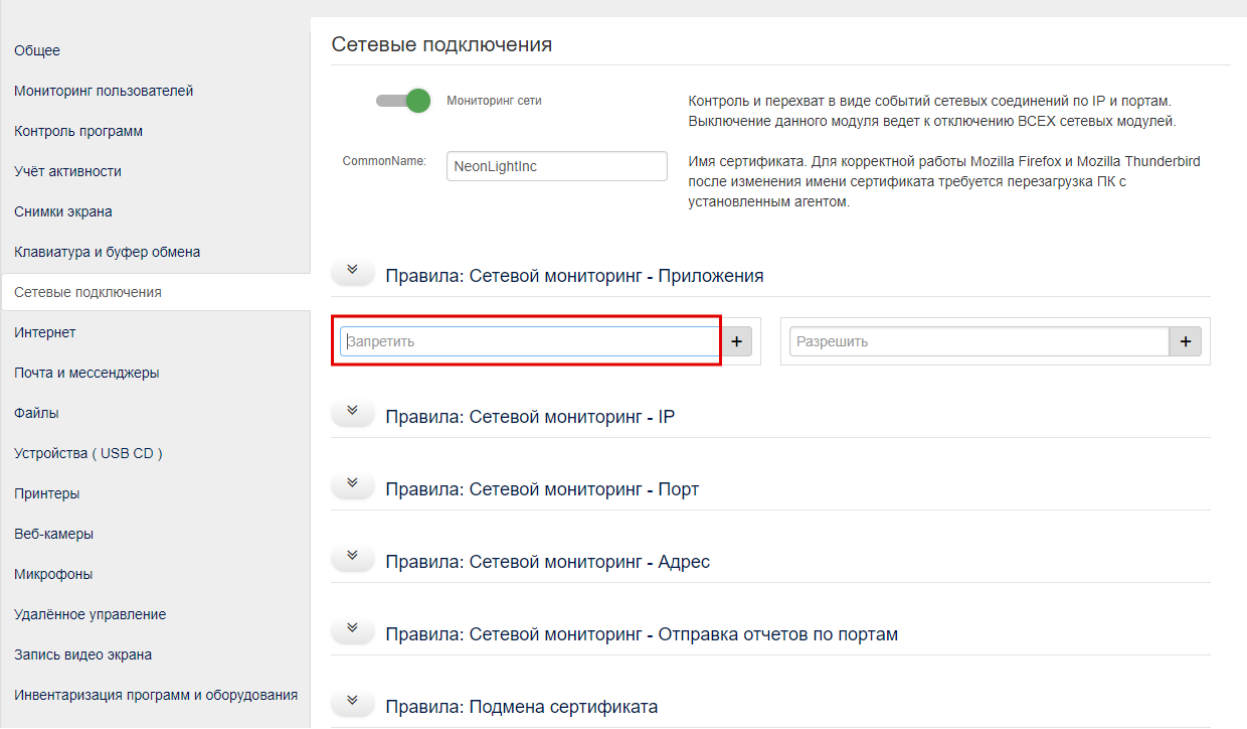
5.20 Не работает перехват Майл.Ру-Агент

Для корректной работы системы мониторинга с mail.ru-агентом - рекомендуется добавить дополнительные правила в две конфигурации:

1. В глобальной конфигурации (**Админ - Панель управления - Глобальная конфигурация**) добавить следующее правило: «**Сетевой мониторинг - Порты - Разрешить **2042**» - это порт MRIM-протокола.
2. Аналогично добавить правило в конфигурацию агента: «**Подмена сертификата - Разрешить** и добавить - **magent.exe**.

5.21 Не работает внешняя база данных

В случае, если не работает внешняя база данных, например БД 1С размещена на сетевом хранилище, следует выполнить добавление IP-адреса ресурса в исключения для сетевого мониторинга.



5.22 Отправка уведомлений по фильтрам, отчетам и политикам

Уведомления по фильтрам, отчетам или политикам, созданным в iBatyr Monitor , можно отправлять на email или в Telegram.

Предупреждение: При отправке уведомлений учитывается язык, указанный в *параметрах сервера*, а не в меню сервера.

Настройка почтовых уведомлений описана на странице *Почтовые настройки*.

Чтобы настроить отправку уведомлений в Telegram:

1. Настройте iBatyr Monitor для отправки уведомлений.
2. Настройте пользователя на приём уведомлений от iBatyr Monitor.

5.22.1 Настройка iBatyr Monitor

1. Найдите в Telegram официального бота BotFather.
2. В диалоговом окне введите команду /**newbot** и задайте имя для бота.

Примечание: Имя бота должно состоять только из строчных букв и содержать в конце слово **bot**. Например: **ibatyrbot** или **ibatyr_bot**.

---

3. Скопируйте токен **HTTP API**, который будет указан в сообщении об успешной регистрации бота.
4. В web-интерфейсе iBatyr Monitor откройте раздел **Панель управления** → **Параметры сервера**.
5. Вставьте скопированный токен в строку **Telegram: Ключ API (токен)**.

На этом настройка системы завершена.

5.22.2 Настройка пользователя для приёма уведомлений

Чтобы настроить отправку уведомлений пользователю:

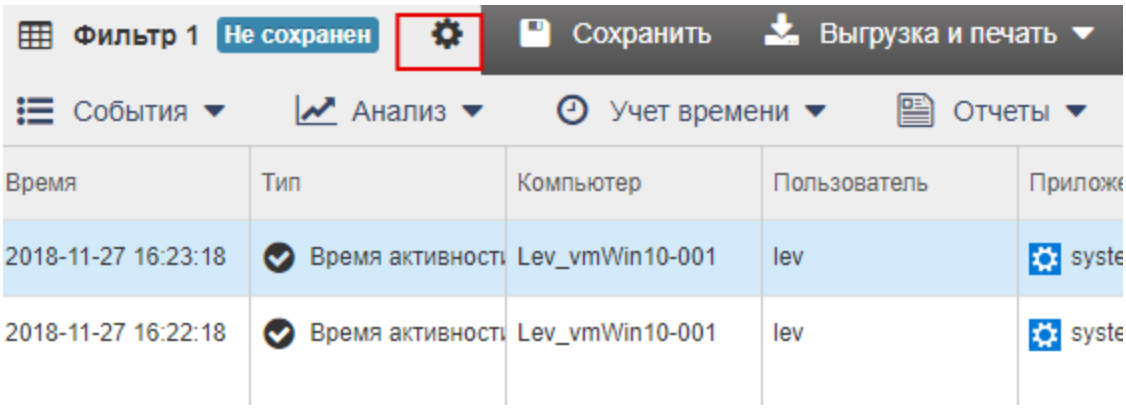
1. В профиле Telegram задайте **имя пользователя**.
2. Отправьте боту в чат любое сообщение с аккаунта, на который нужно отправлять уведомления.

Чтобы настроить отправку уведомлений в групповой чат:

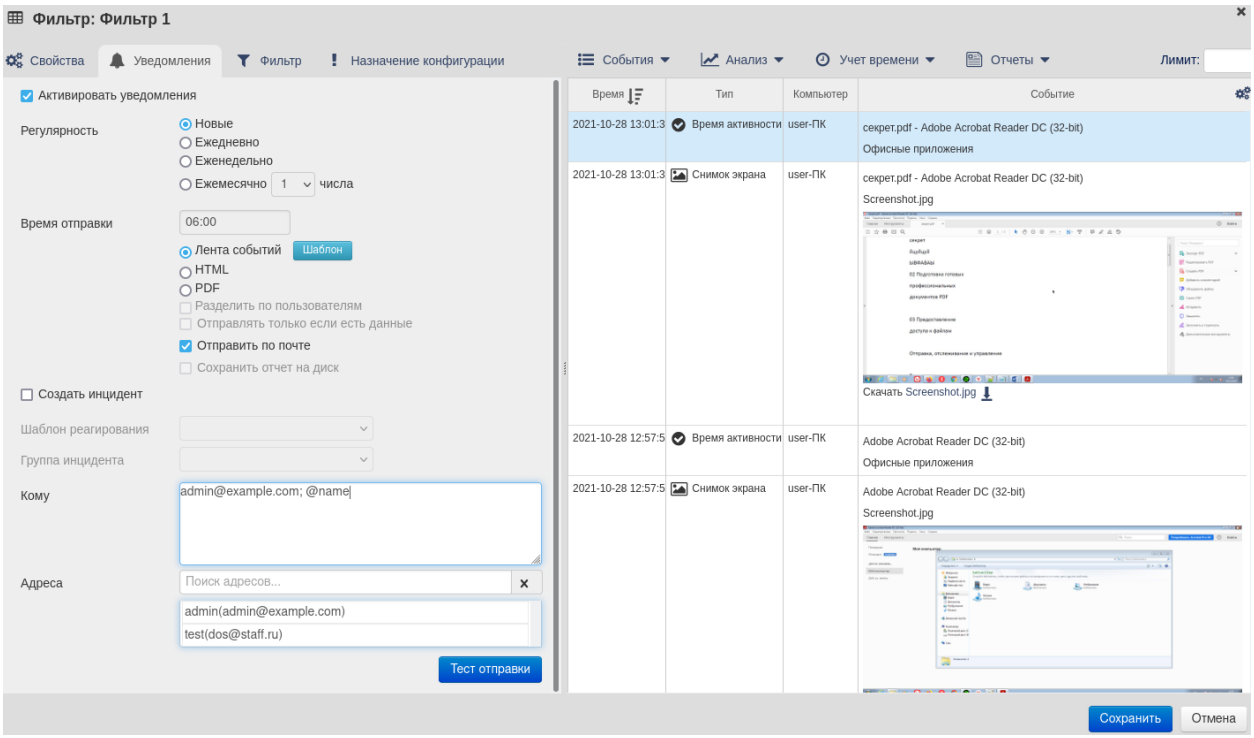
1. Отправьте боту в чат любое сообщение с аккаунта, который будет настраивать групповой чат.
2. Создайте группу. Статус группы по умолчанию — **Приватная**.
3. В разделе редактирования группы укажите статус группы **Публичная**.
4. В публичной ссылке укажите имя группы.
5. Добавьте бота в группу.
6. Отправьте в сообщения группы сообщение /**start** и ещё одно, чтобы бот увидел чат.
7. При настройке отправки, в поле **Кому** укажите название чата из п.4.

5.22.3 Отправка уведомлений

1. Нажмите на значок шестеренки справа от названия фильтра, отчета или политики и перейдите в его свойства.



2. Перейдите на вкладку **Уведомления**



3. Выберите регулярность отправки уведомлений:
   - Новые
   - Ежедневно
   - Еженедельно
   - Ежемесячно

Примечание: Уведомление будет содержать данные за выбранный период: за прошлый день, прошлую неделю или прошлый месяц.

---

4. Выберите формат, в котором будет отправлен фильтр, отчёт или политика:

- Лента событий. **Шаблон** позволит отредактировать вид уведомления, которое будет приходить.
- HTML

- PDF

5. В пункт **Кому** впишите адреса для рассылки уведомлений:

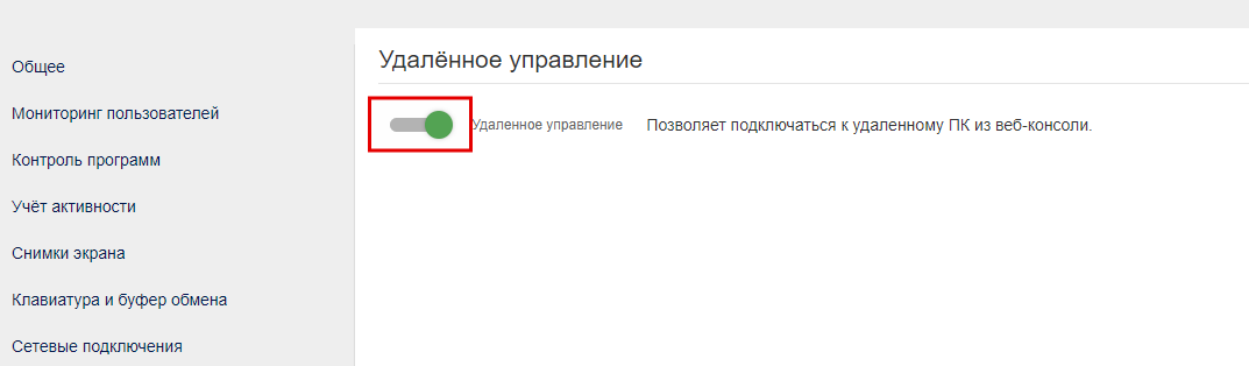
- формат указания почты: **admin@example.com**;
- Telegram-уведомления: **@name** — используйте только имена пользователей, ботов не указывайте;
- Для разделения адресов или имён используйте точку с запятой **;**.

6. Проверьте корректность настройки, отправив тестовое письмо кнопкой **Тест отправки**.

Чтобы не получать пустые отчеты при отсутсвии событий, укажите парметр **Отправлять только если есть данные**.

5.23 Не работает удаленный рабочий стол

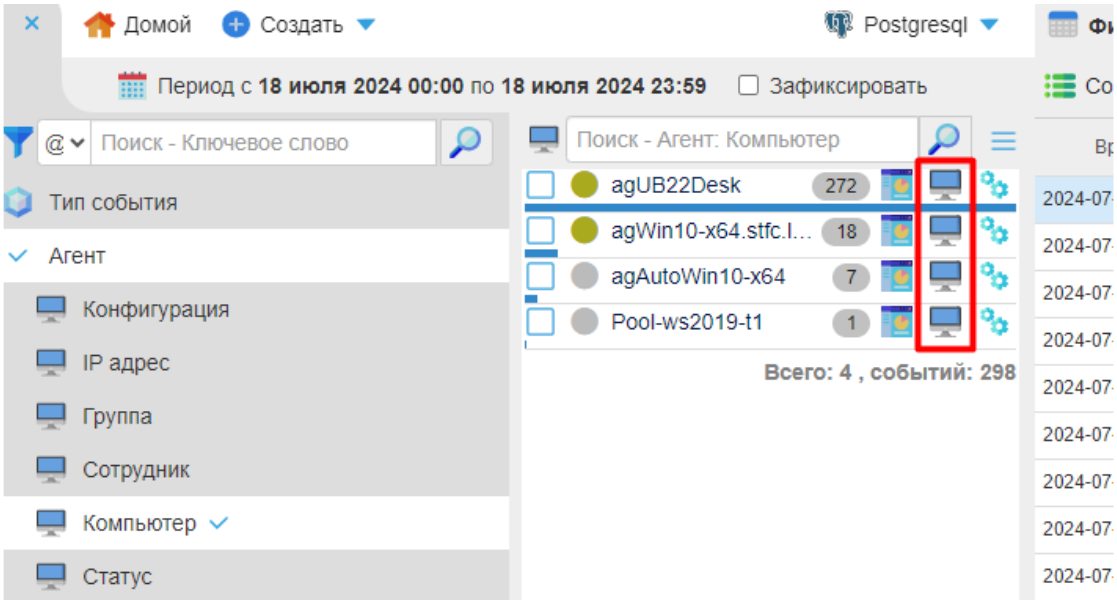
1. Убедитесь, что в конфигурации агента включен модуль **Удаленное управление**.



2. Добавьте *исключения антивируса*.
3. Попробуйте временно остановить антивирус на ПК, на котором просматриваете удалённые рабочие столы.
4. Обновите браузер. Версия браузера должна быть актуальной, потому что старые версии не всегда поддерживают удаленный просмотр.
5. Попробуйте подключиться к веб-консоли iBatyr Monitor через **https**, например так:

```
https://192.168.1.134/
```

6. Проверьте, к каким агентам можно подключиться удаленно.



Второй способ — перейдите по адресу:

```
http://192.168.1.134/analytics/remote_list/
```

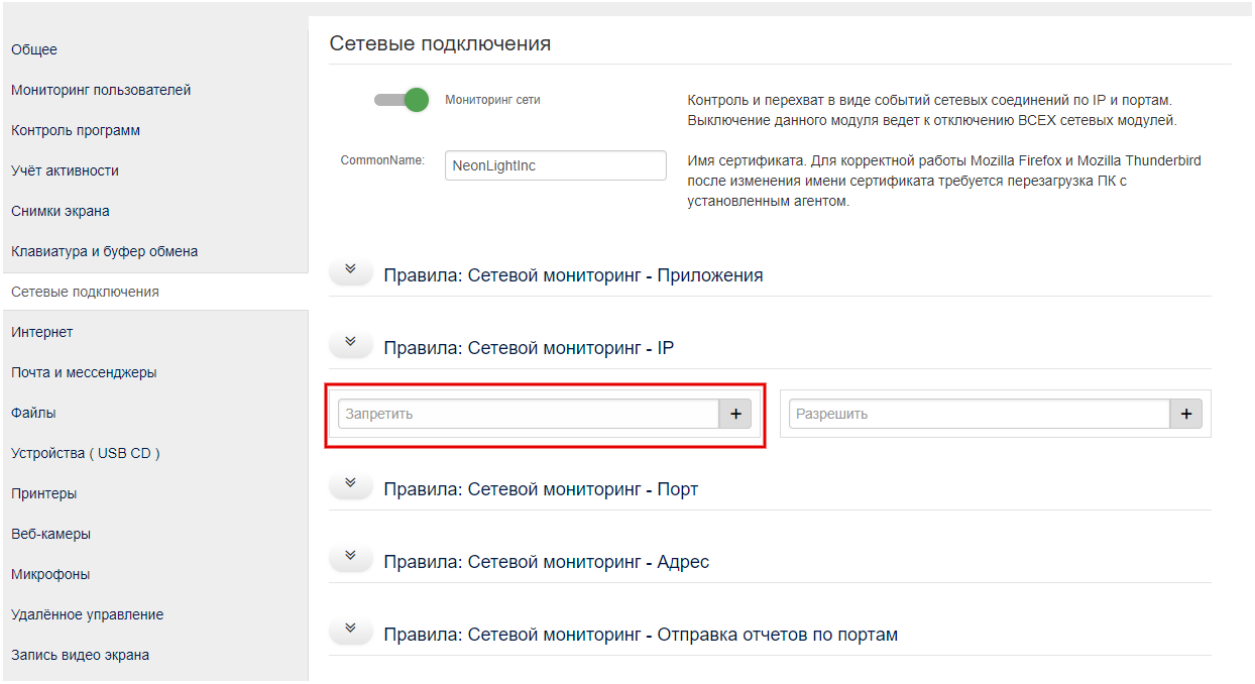
где `192.168.1.134` — IP вашего iBatyr Monitor-сервера. Откроется страница со списком агентов.

7. Попробуйте перезапустить iBatyr Monitor командой из меню **Админ** → **Рестарт сервера**.

5.24 Файловое хранилище в сети

После установки агента не доступно файловое сетевое хранилище.

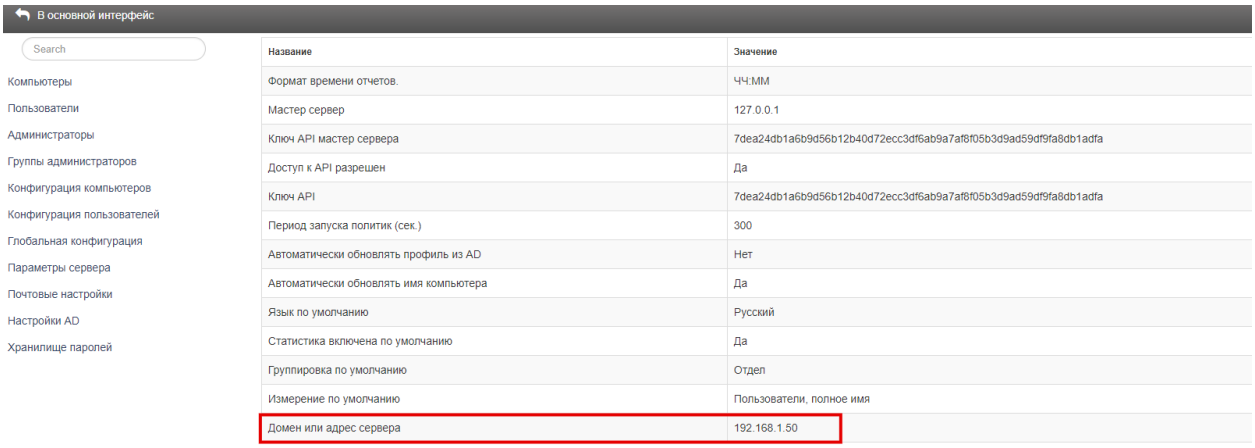
Для исправления ситуации добавьте IP ресурса в список исключений сетевого мониторинга.



5.25 Нет скринов от Linux-агента

Если в настройках профиля выставлено снятие скринов с отслеживаемых машин, но вы видите вместо них иконки, проверьте следующее:

Домен или адрес сервера в конфиге соответствует адресной строке в **Админ** → **Панель управления** → **Параметры сервера** → **Домен или адрес сервера**:



2. Если параметры сервера выставлены верно, но вместо картинок всё равно белые иконки, проверьте права на доступ к папке с изображениями:

```
sudo ls -lR /var/lib/ibatyr/upload/filedata
```

Владельцем папки должен быть пользователь *ibatyr*.

Если это не так, замените владельца командой:

```
sudo chown -R ibatyr:ibatyr /var/lib/ibatyr/upload
sudo chmod -R 755 /var/lib/ibatyr/upload
```

5.26 Нет скринов от macOS-агента

После обновления или переустановки агент делает пустые скриншоты вместо изображений экрана, несмотря на разрешение в настройках приватности macOS.

Проблема связана с **TCC** (Transparency, Consent, and Control) — системой безопасности macOS, которая управляет разрешениями приложений на устройстве, включая доступ к файлам и запись экрана. При удалении агента TCC не всегда удаляет разрешения. В результате при повторной установке или обновлении агента с идентичным Bundle ID в базе разрешений не обновляется сигнатура пакета.

Чтобы разрешить съемку экрана, удалите все правила TCC для агента:

1. Сначала удалите агент:

   ```
   bash ./agent-macos.sh uninstall
   ```

2. Убедитесь, что агента нет в списке разрешенных приложений. Если он все еще там, удалите его:

   - нажмите правой кнопкой мыши на разрешении и выберите **Открыть в Finder**;
   - удалите **StaffAgent.app** из папки **Application**.

3. Сбросьте правила TCC через терминал:

   ```
   tccutil reset ALL com.atomsec.ibatyr.service
   tccutil reset ALL com.atomsec.ibatyr
   tccutil reset ALL com.atomsec.ibatyr.fmon
   ```

4. Повторно *установите агент и настройте разрешения в Настройках приватности.*

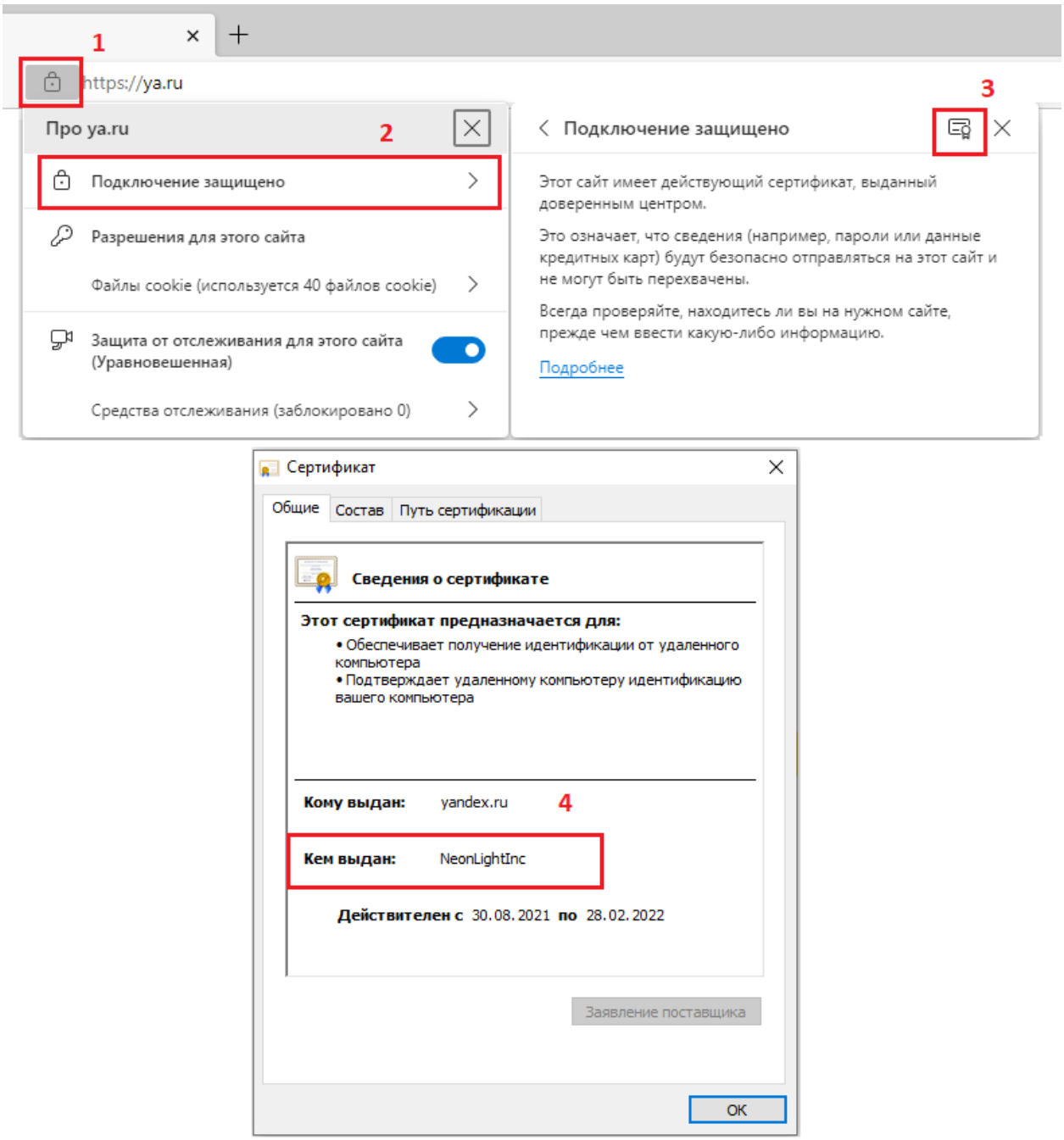
После этого снимки экрана должны заработать.

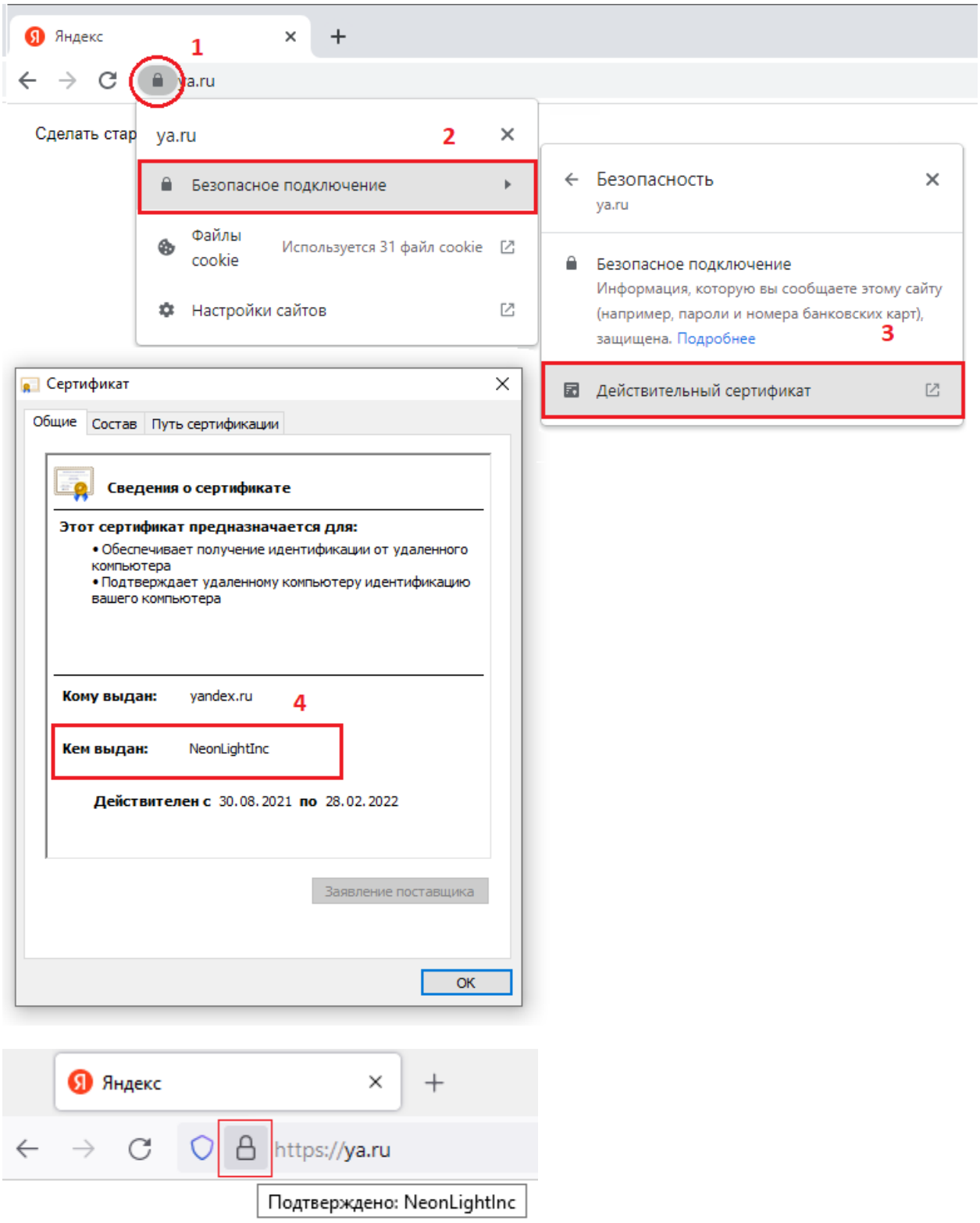
5.27 Что делать, если не открываются сайты после смены конфигурации

После включения конфигурации с сетевым перехватом наш агент прописывает свой сертификат в доверенных, возможно браузеры уже были открыты в этот момент и не получили информацию о новом доверенном сертификате. При появлении подобных проблем рекомендуем:

1. Проверить работу сайтов в другом браузере
2. Если в другом браузере открываются - закрыть текущий браузер и заново открыть
3. Если все равно не открываются- перезагрузить машину
4. Если после всех этих действий сохраняется неработоспособность сайтов - отключить сетевой перехват в конфигурации и проверить, какой сертификат указывается при открытии данных сайтов. Возможно у вас уже производится подмена, например на стороне антивирусного решения. В таком случае нужно отключить перехват SSL/TLS в антивирусе и включить наш перехват.
5. Также имейте в виду, что некоторые сайты используют двунаправленное, либо ГОСТовское шифрование - для них не будет работать подмена сертификата, поэтому их надо вносить в исключения *подмены сертификата*.

Как посмотреть сертификат на примере Edge / Chrome / Firefox




Яндекс
1
ya.ru
Сделать стар
ya.ru
2
Безопасное подключение
Файлы cookie
Используется 31 файл cookie
Настройки сайтов
Безопасность
ya.ru
Безопасное подключение
Информация, которую вы сообщаете этому сайту (например, пароли и номера банковских карт), защищена. Подробнее
3
Действительный сертификат
Сертификат
Общие
Состав
Путь сертификации
Сведения о сертификате
Этот сертификат предназначается для:
• Обеспечивает получение идентификации от удаленного компьютера
• Подтверждает удаленному компьютеру идентификацию вашего компьютера
Кому выдан: yandex.ru
4
Кем выдан: NeonLightInc
Действителен с 30.08.2021 по 28.02.2022
Заявление поставщика
OK
Яндекс
https://ya.ru
Подтверждено: NeonLightInc

5.28 Дополнительные диски для хранения данных

В случае заполнения данными всего доступного дискового пространства можно:

- *настроить автоочистку диска*;
- подключить дополнительные диски.

5.28.1 Подключение дополнительных дисков

Для управления дополнительными дисками используется модуль **mergerfs**.

Чтобы использовать **mergerfs**, установите его командой:

```
sudo ibatyr merger install
```

После завершения установки, **mergerfs** можно переходить к его использованию.

Команды и параметры для использования **mergerfs** представлены в таблице:

tabularytabulary

Команда
ibatyr merger install
ibatyr merger list
ibatyr merger add /path/to/disk
ibatyr merger remove /path/to/disk
ibatyr merger mount /path/to/archive
ibatyr merger unmount /path/to/archive

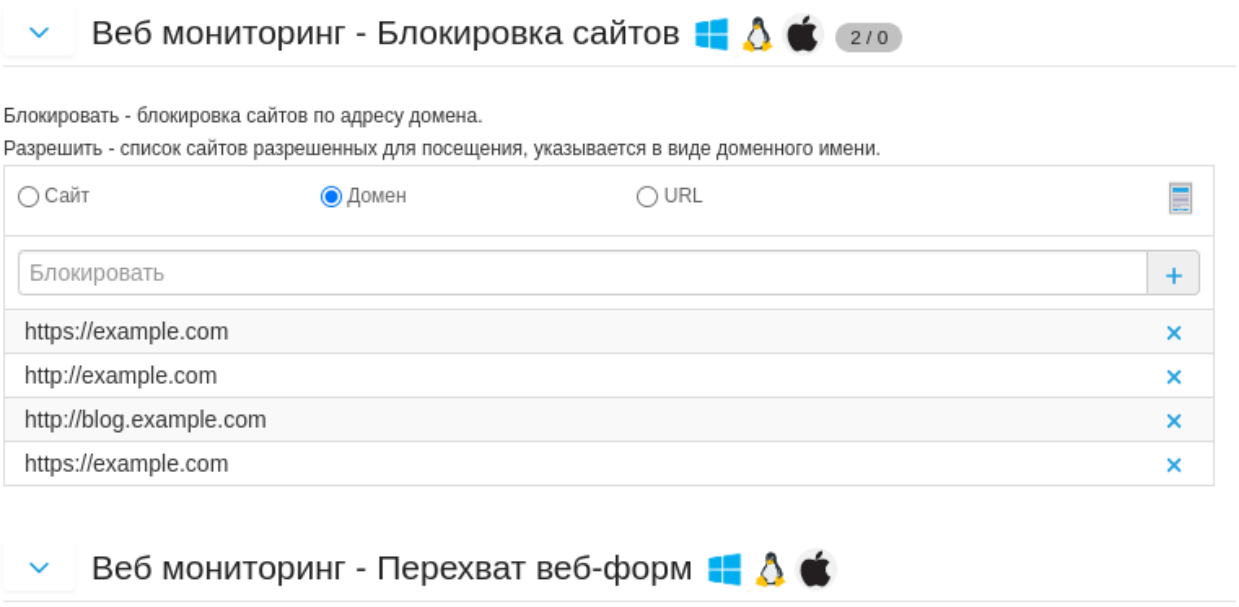
Запись производится на последний диск в списке **etc/ibatyr/merger.list** .

5.29 Как работают чёрные и белые списки

При добавлении сайтов в чёрный или белый список вы можете выбрать один из трёх типов:

- **URL** — для мониторинга конкретной страницы, например: страница входа https://example.com/login;
- **Сайт** — мониторинг всех запросов к сайту с одинаковым протоколом: https://example.com, но не http://example.com;
- **Домен** — мониторинг всех поддоменов и протоколов: https://example.com, http://blog.example.com, ftp://example.com.

После добавления записи в список тип не отображается. Таким образом в списке может оказаться несколько одинаковых записей, но одна может относиться к сайту, а другая — к домену. Рекомендуем учитывать это при анализе списка.



Агенту передаётся только финальный список адресов, сайтов и доменов.

См.также:

Черно-белые списки используются в модулях:

- *Снимки экрана*,
- *Сетевые подключения*,
- *Интернет*,
- *Запись видео экрана*.

Глава 6

Контакты

6.1 Техническая поддержка

tabularytabulary

Время работы	С 10:00 до 18:00
Телефон	+7(717)276-78-64
Почта	support@ibatyr.kz

6.2 Отдел продаж

tabularytabulary

Телефон	+7(717)276-78-64
Почта	sales@ibatyr.kz

6.3 Фактический адрес

ТОО «iBatyr»

00001, г. Астана, ул. Жумабека Ташенова, дом 25, 2-3 подъезд

ibatyr.kz

Глава 7

Что нового в версии 5.6

Версия 5.6 включает обновления, направленные на повышение безопасности, удобство администрирования и расширение интеграций. Добавлены новые механизмы защиты, включая водяные знаки и защиту инцидентов от удаления. Улучшены отчёты по активности и продуктивности, расширена поддержка операционных систем и реализованы сценарии для распределённых инфраструктур.

Новые фичи и улучшения

Windows-агент теперь отображает водяные знаки на мониторе, когда пользователь открывает заданные в настройках сайты и приложения.

- на знаке отображаются логин, имя ПК, время;
- можно настроить условия отображения, расположение и прозрачность надписи;
- защищает от утечек через скриншоты и фотографирование экрана.

Связанная статья

В новой версии можно загрузить проигрыватель для просмотра записей экрана, сохранённых агентом.

- доступен для Windows, Linux и macOS:
- позволяет просматривать записи локально без доступа к серверу.

Связанная статья

Добавлен механизм защиты от удаления связанных с инцидентами событий и файлов.

- сохраняет события и файлы для расследования;
- защищает от случайного или преднамеренного удаления;
- исключает потерю информации при очистке базы данных.

Примечание: По умолчанию защита выключена. Чтобы включить, обратитесь к инструкции в связанной статье.

Связанная статья

Теперь можно задать порог уровня риска — система будет формировать отчеты и уведомления только для пользователей, чей риск превышает это значение. При дальнейшем росте риска создаются дополнительные уведомления.

- помогает сосредоточиться на действительно критичных пользователях;
- позволяет фиксировать резкий рост или устойчивое повышение уровня риска;
- поддерживается автоматическая рассылка отчетов ответственным лицам раз в сутки.

Связанная статья

Добавлена поддержка форматов документов для сканирования. Сканирование этих форматов возможно только через краулер:

- устаревших офисных форматов: .doc, .xls, .ppt — помогает выявить чувствительную информацию в старых документах;
- форматов .cvs, .txt, .rtf — обеспечивают возможность поиска в черновиках, логах и исходном коде.

Доступно для Windows- и Linux-агентов.

Связанная статья

В отчет по активности добавлена настройки отчета для отображения активности по отделу.

В отчет **Продуктивное время по отделам** добавлена категория **Все остальное**.

- учитывает активность, которая не попала ни под одну из продуктивных, нейтральных или непродуктивных политик;
- помогает выявить неклассифицированные действия пользователя и донастроить политики.

Обновления сервера

В новой версии дополнительно поставляется ISO-образ с Ubuntu 22 и PostgreSQL 15.

- содержит последние версии ОС и СУБД без необходимости дополнительной настройки;
- повышает стабильность и безопасность системы.

Связанная статья

Добавлена поддержка версий:

- сервер распознавания — Astra Linux 1.7 Smolensk.

Безопасность

Добавлен инструмент сверки контрольных сумм системных файлов с эталонными значениями, зафиксированными при установке или обновлении.

- работает на сервере и агенте;
- выявляет изменения, внесённые вручную или вредоносным ПО;
- помогает проверить целостность ПО.

Пример работы: после установки сервера сохраняются контрольные суммы системных файлов. Если через неделю они изменились, а обновлений не было — кто-то мог внести в систему несанкционированные изменения.

Связанная статья

Агент непрерывно собирает системные логи и по запросу администратора передаёт их на сервер:

- сбор не может быть остановлен пользователем или операционной системой;
- логи доступны через кнопку в веб-интерфейсе без подключения к рабочей станции;
- не требует дополнительной настройки или изменения конфигурации.

Связанная статья

Работа в распределённых системах

Ранее при синхронизации политик на подчинённые узлы автоматически передавались и системные политики. Теперь их можно исключить. Это решение:

Появилась возможность исключать политики из синхронизации. Основной сценарий использования ориентирован на исключение системных политик. Если исключить из синхронизации пользовательскую политику, она будет удалена с подчинённого сервера.

Это решение:

- даёт больше гибкости при настройке политик на уровне нод;
- позволяет учитывать различия в инфраструктуре и аппаратной конфигурации;
- позволяет разгрузить серверы при обработке изображений.

В новой версии можно создать архивную БД на основе удаленной БД с помощью скрипта.

- подходит для распределённых конфигураций, в которых сервер и база данных находятся на разных машинах;
- упрощает архивирование;
- позволяет хранить основную и архивную БД на отдельных серверах.

Связанная статья

В новой версии можно указать порт мастер-сервера в настройках сервера.

- позволяет корректно настроить подключение слейв-серверов к мастеру через нестандартный порт;
- исправляет ошибку, из-за которой параметры сервера не сохранялись при использовании нестандартного порта.

Теперь сервера кластера можно разворачивать и мигрировать на базу данных PostgreSQL 15 и операционную систему Ubuntu 22.

- кластер работает с PostgreSQL 15;
- новейшая версия позволяет более эффективно распределять нагрузку.

Агенты

Добавлен перехват сообщений:

- поддерживается локальная версия Bitrix24 с уникальным доменным именем;
- адрес сервера Bitrix указывается в конфигурации агента;
- агент перехватывает сообщения локального Bitrix24.

Добавлен перехват сообщений:

- поддерживается on-premise версия Outlook с уникальным доменным именем;
- имя сервера Exchange указывается в конфигурации агента;
- агент перехватывает сообщения для локального Outlook.

Примечание: Exchange-сервер – это корпоративный почтовый сервер от Microsoft. При развертывании на локальном сервере (on-premise) позволяет организациям полностью контролировать почтовую систему.

Добавлен перехват ввода и вывода команд в терминале PowerShell. По результатам перехвата создается событие **Терминал ввода команд**.

Агент отслеживает активность на всех портах, указанных в разрешённом списке:

- позволяет фиксировать сетевую активность даже через нестандартные порты;
- помогает отслеживать трафик, когда антивирусное ПО блокирует стандартный порт.

Связанная статья

Теперь агент фиксирует передачу данных через POST-запросы, включая логины и пароли.

С версии 5.6 Linux-агент отслеживает передачу данных по протоколу POP3.

- расширяет охват мониторинга почтовых каналов;
- фиксирует получение писем через почтовые клиенты.

Агент фиксирует список файлов на внешних устройствах.

- фиксируются названия всех файлов;
- для каждого файла создается событие **Операция с файлом**;
- доступна настройка теневого копирования файлов.

Связанная статья