InfoWatch Data Explorer. Руководство администратора

10/09/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 5

2 Комплект документов 6

3 Техническая поддержка пользователей 7

4 Вход в систему 8

5 Лицензирование 10

6 Настройки 11

6.1 Состояние системы 11

6.2 Интеграции 13

6.2.1 Интеграция с Active Directory 14

Добавление интеграции 14

Список интеграций 16

6.2.2 Редактирование и удаление интеграции 17

6.3 Пользователи 18

6.3.1 Создание нового пользователя 18

6.3.2 Добавление нового пользователя из LDAP 19

6.3.3 Редактирование учетной записи 20

6.3.4 Просмотр профиля пользователя 21

6.3.5 Смена пароля пользователя 21

6.3.6 Активация и деактивация пользователя 22

6.3.7 Удаление пользователя 23

6.3.8 Сброс двухфакторной аутентификации 23

Сброс в интерфейсе Центра расследований 23

Сброс при помощи скрипта 23

6.4 Роли 24

6.4.1 Создание и настройка роли 25

6.4.2 Просмотр, редактирование и копирование роли пользователя 30

6.4.3 Снятие и удаление роли пользователя 30

6.5 Аудит 31

6.6 Настройки пароля 34

6.6.1 Требования к имени пользователя и логину 35

6.7 Основные настройки 35

6.7.1 Настройки сессии 36

6.7.2 Сбор статистических данных 36

6.7.3 Облегченная версия Платформы 36

7 Метки 37

8 Уведомления 38

9 Добавление пользовательского сертификата 39

10 Расширенный фильтр 40

В настоящем руководстве вы можете найти сведения по настройке и подготовке к работе InfoWatch Data Explorer.
InfoWatch Data Explorer (далее Модуль/Система или Data Explorer) это – модуль, позволяющий автоматически систематизировать документы, найденные с помощью InfoWatch Data Discovery. Для работы Data Explorer необходим InfoWatch Data Analysis Service.

1 Аудитория

Данное руководство предназначено для пользователей Модуля, которые будут работать с ним и заниматься его администрированием.

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и СУБД PostgreSQL.

2 Комплект документов

В документацию по InfoWatch Data Explorer входят:

- *InfoWatch Data Explorer. Руководство по установке*. Содержит описание установки, обновления и удаления Модуля;
- *InfoWatch Data Explorer. Руководство администратора*. Документ содержит информацию по настройке Модуля.
- *InfoWatch Data Explorer. Руководство пользователя*. Содержит описание работы с Модулем.

Сопутствующая документация по продукту InfoWatch Data Discovery включает в себя:

- *InfoWatch Data Discovery. Руководство по установке*. Документ содержит описание процесса установки, обновления и удаления Data Discovery.
- *InfoWatch Data Discovery. Руководство администратора*. Документ содержит информацию по настройке Data Discovery.
- *InfoWatch Data Discovery. Руководство пользователя*. Содержит описание работы с задачами сканирования.

Сопутствующая документация по сервису InfoWatch Data Analysis Service включает в себя:

- *InfoWatch Data Analysis Service. Руководство по установке, конфигурированию и администрированию*. Содержит описание установки, обновления, удаления и настройки Data Analysis Service.

Сопутствующая документация по продукту InfoWatch Traffic Monitor включает в себя:

- *InfoWatch Traffic Monitor. Руководство по установке*. Содержит описание установки, настройки и удаления системы InfoWatch Traffic Monitor;
- *InfoWatch Traffic Monitor. Руководство администратора*. Содержит информацию по администрированию InfoWatch Traffic Monitor (база данных, серверная часть);
- *InfoWatch Traffic Monitor. Руководство пользователя*. Содержит описание работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, составление политик для обработки объектов);
- *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*. Содержит пояснения к часто используемым конфигурационным файлам.

3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Модуля, вы можете обратиться в службу технической поддержки:

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера;
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

4 Вход в систему

Вы можете войти в Систему с помощью следующих учетных записей:

- предустановленный пользователь Главный офицер с предустановленной ролью *Главный офицер безопасности* (логин *officer*);
- добавленные пользователи с предустановленными (*Главный офицер безопасности, Офицер безопасности*) или пользовательскими ролями.

Подробнее см. *Пользователи*, *Роли*.

В Системе реализовано два способа аутентификации:

- стандартная, путем ввода логина и пароля;
- строгая, или двухфакторная, с использованием TOTP-приложения.

Изменение способа аутентификации доступно только пользователю с ролью *Главный офицер безопасности* и применяется ко всем учетным записям в Системе.

Чтобы **включить** двухфакторную аутентификацию для всех пользователей:

1. Войдите в Систему стандартным способом с использованием логина и пароля учетной записи с ролью *Главный офицер безопасности*.
2. Перейдите в раздел **Настройки** → **Основные настройки**.
3. Включите настройку **Включить аутентификацию по алгоритму TOTP для всех пользователей**.
4. Нажмите **Сохранить**.

При новом входе в Систему каждый пользователь должен будет **настроить** двухфакторную аутентификацию:

1. Установить приложение с поддержкой алгоритма TOTP, например Google Authenticator или Яндекс ID (Ключ), на мобильное устройство, или использовать аналогичное десктопное приложение на рабочей станции.
2. В окне авторизации ввести логин и пароль своей учетной записи.
3. В случае мобильного приложения:
    a. Запустить приложение на мобильном устройстве.
    b. В консоли Центра расследований отсканировать QR-код. В приложении отобразится 6-значный код.
    c. Ввести полученный код в поле **Код подтверждения**.
    d. Нажать **Войти**.
4. В случае десктопного приложения:
    a. Открыть приложение на рабочей станции. В таких приложениях можно выбрать один из двух способов получения ключа: сканированием QR-кода или вводом ключа вручную.
    b. Для второго способа нажать скопируйте ключ в консоли Центра расследований и вставить ключ в приложение.
    c. Указать период действия выдаваемого одноразового пароля в 60 секунд. В приложении отобразится 6-значный код.
    d. Ввести полученный код в поле **Код подтверждения**.
    e. Нажать **Войти**.

Следующий вход в Систему осуществляется посредством ввода логина и пароля, а затем одноразового 6-значного кода, получаемого каждый раз через приложение с поддержкой алгоритма TOTP.

Чтобы **выключить** использование двухфакторной аутентификации для всех пользователей:

1. Войдите в Систему стандартным способом с использованием логина и пароля учетной записи с ролью *Главный офицер безопасности*.
2. Перейдите в раздел **Настройки** → **Основные настройки**.
3. Выключите настройку **Включить аутентификацию по алгоритму TOTP для всех пользователей**.
4. Нажмите **Сохранить**. После этого вход в Систему будет осуществляться вводом логина и пароля.

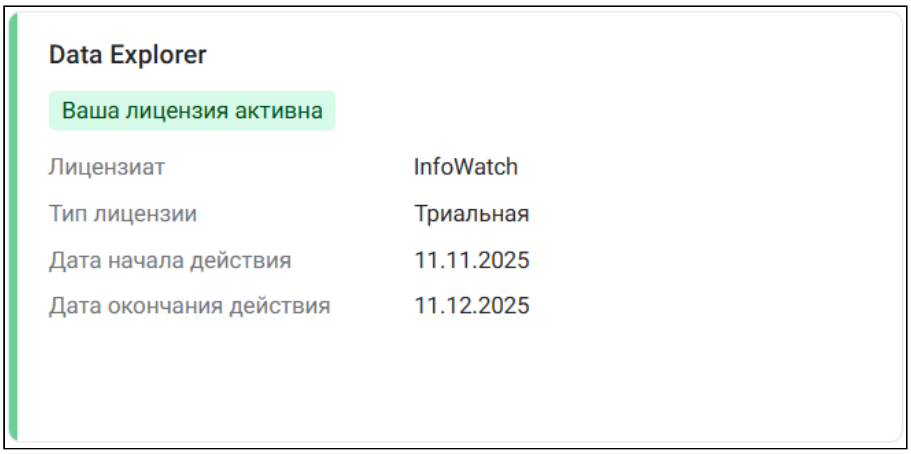
Все действия по включению или отключению двухфакторной аутентификации фиксируются в журнале раздела **Настройки** → **Аудит**, см. *Аудит*.

В случае потери доступа к приложению с поддержкой алгоритма TOTP следует сбросить использование двухфакторной аутентификации, см. *Сброс двухфакторной аутентификации*.

5 Лицензирование

В разделе **Настройки** → **Лицензирование** вы можете управлять лицензиями.

Работа в Data Explorer возможна только при наличии действующей лицензии. По умолчанию для Data Explorer установлена пробная лицензия сроком на один месяц. Дата установки Модуля является датой начала действия этой лицензии.



Чтобы установить новую лицензию:

1. В правом верхнем углу рабочей области нажмите **+ Добавить**.
2. В открывшемся окне укажите путь до файла с действующей лицензией. Также файл можно добавить, переместив его в окно добавления файлов.

Чтобы удалить лицензию:

1. В правом верхнем углу плитки лицензии нажмите .
2. В появившемся окне подтвердите действие, нажав **ОК**.

Важно!

Перед тем как удалить лицензию, которую нужно заменить, убедитесь в наличии файла с новой действующей лицензией. Работа в Data Explorer без лицензии невозможна.

6 Настройки

Раздел **Настройки** содержит:

- **Настройки пользователей**:
  - Пользователи
  - Роли
  - Аудит
- **Настройки системы**:
  - Состояние системы
  - Интеграции
  - Настройки пароля
  - Основные настройки
- Специфичные настройки установленных продуктов. У **Data Explorer** таких настроек нет.

> **Примечание:**
>
> Data Explorer не использует следующие общие настройки:
>
> - **Данные для анализа** – Data Explorer не хранит данные в партициях и не использует их;
> - **Сервисы для уведомлений** – Data Explorer не отправляет почтовые уведомления;
> - **Фильтры** – Data Explorer использует отдельные фильтры, которые переносятся только в раздел "Хранение файлов" Data Discovery.

6.1 Состояние системы

Подсистема мониторинга выполняет проверку работы всех элементов Системы. При этом анализируется доступность элементов распределенной сети, информация об основных аппаратных компонентах, а также информация о состоянии всех служб Системы.

Раздел **Настройки → Настройки системы → Состояние системы** содержит панели с информацией о серверах кластера Центра расследований. Каждая панель содержит следующую информацию:

Поле	Описание
Лейбл (имя)	Лейбл и имя ноды в формате `лейбл(имя)`
Статус	Статус ноды: • *Ready* – доступна и готова к работе; • *Not Ready* – не готова к работе; • *Unknown* – зарегистрирована, но не отвечает на запросы.
Адрес	IP-адрес ноды продукта

Поле	Описание
Последнее обновление состояния системы	Дата и время получения информации о статусе ноды
Версия ядра	Версия ядра ОС
Операционная система	ОС ноды продукта
Память	Общий и занимаемый размер оперативной памяти сервера
ЦП	Загрузка центрального процессора сервера
Дисковое пространство (Clickhouse) *	Общее выделенное и занятое место на диске для хранения данных БД Clickhouse
Дисковое пространство (PostgreSQL) *	Общее выделенное и занятое место на диске для хранения данных БД PostgreSQL
Дисковое пространство (Root) *	Общее выделенное и занятое место, отведенное для системных данных в корневой директории
Дисковое пространство (NATS) *	Общее выделенное и занятое место на диске для хранения данных NATS
Дисковое пространство (Datastorage) *	Общее выделенное и занятое место на диске для хранения бинарных данных
Список служб ноды продукта	
Статус	Один из статусов службы: • *Запущена* – работает; • *Остановлена* – невозможно получить статус; • *Не инициализирована* – находится в процессе запуска; • *Не найдена* – должна быть на узле, но отсутствует; • *Ошибка* – завершена с ошибкой.
Имя	Имя службы в Системе *(контейнеры, поды)*
Версия	Версия сборки службы
Просмотреть детали	Вывод информации о состоянии, событиях и внутренних сообщениях службы

Примечание:

Если на сервере установлены и другие продукты Центра расследований InfoWatch, их службы также будут в списке.

Примечание:

* Если в одном из разделов осталось 10 ГБ или меньше свободного пространства, в веб-интерфейсе Центра расследований будет выведено неотключаемое предупреждение том, что превышено ограничение по использованию дискового пространства.
Если ограничение превышено:

- на **офисной ноде Платформы** - будут остановлены интеграции, настроенные на этой ноде;
- на **центральной ноде Платформы** - будут остановлены все интеграции в кластере.

Чтобы снять это ограничение, в **Настройки → Настройки системы → Состояние системы** определите ноду и раздел, в котором осталось мало пространства, и освободите его средствами ОС или продукта.

Все события мониторинга записываются в журнал.

Чтобы скачать весь журнал, в правом верхнем углу нажмите нажмите **Экспорт диагностических данных**. В диагностические данные будут добавлены лог-файлы работающих служб. После формирования диагностических данных начнется загрузка ZIP-архива, содержащего TXT-файлы с логами, на ваш компьютер.

Чтобы скачать диагностические данные *отдельной* службы, нажмите напротив службы. На компьютер будет загружен ZIP-архив, содержащий TXT-файлы с логами службы.

6.2 Интеграции

В разделе **Настройки → Настройки системы → Интеграции** вы можете настроить интеграции с источником данных:

- Active Directory – для получения актуального дерева каталогов Active Directory компании;
- InfoWatch Traffic Monitor – для загрузки в Платформу:
  - конфигурации (объекты защиты) InfoWatch Traffic Monitor, которую Data Discovery использует для контентного анализа – обнаружения объектов защиты в извлеченных текстовых контентах. Эти объекты также будут отображаться в Data Explorer при просмотре содержимого файлов;
  - событий Traffic Monitor, которые можно добавлять в расследования, а также для получения данных, используемые другими продуктами.

Данные из Active Directory используются для следующих целей:

- получение групп персон;
- получение структуры компании;
- получение информации о рабочих станциях.

В этом разделе:

- Интеграция с Active Directory
- Редактирование и удаление интеграции

Подробнее об интеграции с InfoWatch Traffic Monitor см. *InfoWatch Data Discovery. Руководство администратора. Интеграция с InfoWatch Traffic Monitor*.

6.2.1 Интеграция с Active Directory

Интеграция с Active Directory необходима для загрузки в Центр расследований актуального дерева каталогов компании: групп, персон.

При первом входе в Систему список интеграций пуст.

Добавление интеграции

Чтобы добавить интеграцию с Active Directory:

1. Перейдите в раздел  **Настройки** → **Настройки системы** → **Интеграции**.
2. Нажмите:
   - **+ Добавить интеграцию** в центре окна, если еще не было настроено ни одной интеграции;
   - **+ Добавить** в правом верхнем углу, если ранее была настроена другая синхронизация.
3. Выберите **Active Directory**.
4. Укажите значения параметров согласно таблице ниже.
5. Нажмите **Проверить соединение** и дождитесь сообщения *Соединение успешно установлено*. В случае появления статуса:
   - *Не удалось установить соединение*, убедитесь, что были введены корректные адрес и порт;
   - *Заданы неверные логин или пароль*, убедитесь, что были введены корректные логин и пароль.
6. Нажмите:
   - **Сохранить**, чтобы сохранить интеграцию без проведения синхронизации;
   - **Сохранить и синхронизировать**, чтобы сохранить интеграцию и запустить процесс синхронизации немедленно.

> **Важно!**
>
> Синхронизация с Active Directory может создавать высокую нагрузку на серверы домена и сеть, поэтому рекомендуем проводить первую синхронизацию с Active Directory в ночное время.

Параметры интеграции с сервером Active Directory

При создании интеграции с сервером Active Directory необходимо ввести параметры:

Параметр	Описание
Имя интеграции	Название соединения, которое используется в Консоли управления
Филиал	Лейбл ноды Data Explorer для подключения к Active Directory
Адрес источника	Сетевой адрес сервера Active Directory
Тип соединения	Выбор типа соединения, которое будет установлено: • незащищенное соединение (Plain); • защищенное соединение по протоколу LDAP (StartTLS); • защищенное соединение по протоколу LDAPS (TLS). **Важно!** Соединение без сертификатов небезопасно.
Сертификат	Загрузка файла сертификата в формате CER. Параметр используется, если выбран защищенный тип соединения.
Глобальный порт	Порт для подключения глобального LDAP-каталога. По умолчанию используются значения: • 3268 для: • незащищенного соединения (Plain); • защищенного соединения по протоколу LDAP (StartTLS); • 3269 для защищенного соединения по протоколу LDAPS (TLS). Чтобы указать значения, используемые по умолчанию, нажмите .
Порт	Порт для подключения локального каталога домена. По умолчанию используются значения: • 389 для: • незащищенного соединения (Plain); • защищенного соединения по протоколу LDAP (StartTLS); • 636 для защищенного соединения по протоколу LDAPS (TLS). Чтобы указать значения, используемые по умолчанию, нажмите .

LDAP-запрос	Атрибуты фильтрации службы каталогов, являющиеся полным путем к указанному каталогу домена.
	Вы можете указать только один каталог в организационной структуре Active Directory. Для оптимизации поиска используйте отдельные уровни иерархии базы:
	`C – countryName`
	`O – organizationName`
	`OU – organizationalUnit`
	`DC – domainComponent`
	`CN – commonName`

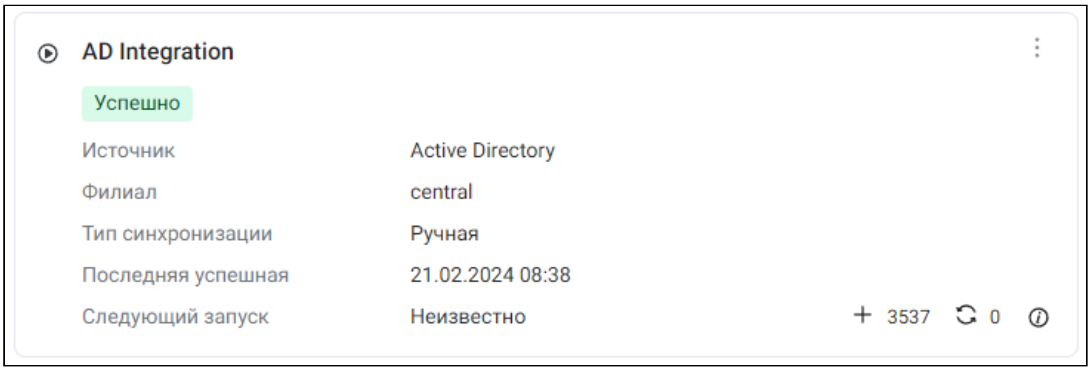
Параметр	Описание
	Пример: Чтобы использовать в качестве базы поиска ветку `Users`, расположенную в домене компании, необходимо ввести: `cn=users,dc=company,dc=com` Если вам необходимо исключить получение определенных групп из Active Directory, ознакомьтесь со статьей *Исключение групп из LDAP-запроса с помощью фильтра DN_Filter*
Логин	Логин для доступа к серверу Active Directory (пользователь должен иметь права на чтение каталога)
Пароль	Пароль для доступа к серверу Active Directory
Синхронизация	Доступны два типа синхронизации: • *Ручная*; • *Автоматическая* по расписанию. Во втором варианте необходимо указать *Периодичность* и *Повторение*.
Периодичность	Как часто необходимо запускать синхронизацию : *Ежеминутно*, *Ежечасно*, *Ежедневно*, *Еженедельно*
Повторение	День недели и/или время следующей синхронизации

Список интеграций

Синхронизация возможна с несколькими LDAP-каталогами. Каждая интеграция отображается в отдельной панели. Список интеграций с серверами Active Directory отображается в центральной области.

В нижней строке панели указано:

-  – количество добавленных в ходе синхронизаций персон, групп и рабочих станций;
-  – общее количество персон, групп и рабочих станций, данные которых обновились в ходе последней синхронизации;
-  – детальная информация о количестве персон, групп и рабочих станций, добавленных или обновленных в ходе последней синхронизации.



Повторный запуск синхронизации

Если необходимо запустить вручную еще одну синхронизацию с теми же параметрами:

1. Нажмите  на панели интеграции.
2. Дождитесь выполнения синхронизации. Процесс может занять продолжительное время (например, при низкой скорости передачи данных по сети или при большом объеме передаваемых данных).

Статус интеграции

Для каждой интеграции указывается статус синхронизации:

Статус	Описание
Не синхронизировалось	Интеграция сохранена, синхронизация еще ни разу не запускалась.
Синхронизируется	Идет процесс синхронизации.
Успешно	Синхронизация завершилась успешно.
Прервана	Синхронизация остановлена пользователем. В статусе также указаны дата и время остановки.
Ошибка	Данный статус может обозначать следующее: • введены некорректные логин, пароль, или адрес; • истек срок лицензии на использование модуля; • в ходе синхронизации произошла ошибка.

6.2.2 Редактирование и удаление интеграции

Чтобы внести изменения в уже созданную интеграцию:

1. Нажмите  в правом верхнем углу и выберите **Редактировать**.
2. Внесите изменения.
3. Нажмите **Сохранить**:
   - Чтобы создать новую интеграцию с указанными настройками вместо текущей интеграции, нажмите **Создать новую**. Текущая интеграция будет удалена.
   - Если требуется изменить настройки интеграции, нажмите **Продолжить в этой**.

Чтобы удалить интеграцию:

1. Нажмите  в правом верхнем углу.
2. Выберите **Удалить**, затем нажмите **Ок**.

> **Примечание:**

Данные, полученные в результате синхронизаций, не будут удалены после удаления интеграции.

6.3 Пользователи

Во время установки Системы создается предустановленный пользователь – Главный офицер. Для входа в Систему введите логин и пароль по умолчанию:

Логин	Пароль
officer	xxXX1234

При первом входе в Систему Офицеру безопасности необходимо сменить пароль на постоянный (см. *Смена пароля пользователя*).

Главная страница раздела **Пользователи** содержит список пользователей, допущенных к работе с Системой:

- Главного Офицера безопасности;
- других Офицеров безопасности (ОБ), подчиненных ему.

Действия пользователя:

- Создание нового пользователя
- Добавление нового пользователя из LDAP
- Редактирование учетной записи
- Просмотр профиля пользователя
- Смена пароля пользователя
- Активация и деактивация пользователя
- Удаление пользователя
- Сброс двухфакторной аутентификации

6.3.1 Создание нового пользователя

Главный офицер может добавить новых пользователей, которые также могут выполнять функции Офицеров безопасности. Для этого:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Пользователи**.
2. Нажмите справа + Создать.
3. Выберите **Создать пользователя**.
4. Введите значения параметров согласно таблице:

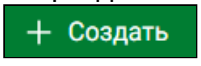
Параметр	Обязательный параметр	Описание
Фотография	Нет	Фотография пользователя
Имя пользователя	Да	Имя нового пользователя (о требованиях к имени

Параметр	Обязательный параметр	Описание
		пользователя см. *Настройки пароля*).
Логин	Да	Имя учетной записи пользователя (о требованиях к логину см. *Настройки пароля*). Логин не чувствителен к верхнему или нижнему регистру.
Пароль	Да	Пароль учетной записи (о требованиях к паролю см. *Настройки пароля*)
Подтверждение пароля	Да	Пароль учетной записи
Роль	Нет	Роль пользователя в Системе. Пользователю может быть присвоена только одна роль.
Язык консоли	Нет	Язык интерфейса для нового пользователя: *Русский* или *Английский*
Отображать только функции установленных продуктов	Нет	Переключатель, который скрывает для пользователя разделы и виджеты неустановленных продуктов
Контакты	Нет	Email-адрес. Можно добавить одно или несколько значений.
	Нет	Номер телефона. Можно добавить одно или несколько значений.

5. Нажмите **Создать**. Новый пользователь будет добавлен в Систему. При первом входе в Систему он должен поменять пароль своей учетной записи (см. *Смена пароля пользователя*).

6.3.2 Добавление нового пользователя из LDAP

Главный офицер может выбрать из LDAP-каталога новых пользователей, которые также могут выполнять функции Офицеров безопасности. Чтобы добавить нового пользователя в Систему из LDAP-каталога:

1. Перейдите в раздел  **Настройки** → **Настройки пользователей** → **Пользователи**.
2. Нажмите 

.

3. Выберите **Добавить из LDAP**.
4. Выберите доступный LDAP-сервер, интеграция с которым настроена в Системе (подробнее про интеграцию см. *Интеграция с Active Directory*).
5. В строке поиска начните вводить ФИО или логин пользователя.
6. В результатах поиска выберите нужного пользователя и нажмите **Добавить**.
7. Назначьте пользователю роль (см. подробнее *Редактирование учетной записи*).

Пользователь будет добавлен в список пользователей Системы. Новый пользователь входит в Систему с помощью доменных учетных данных. Логин учетной записи имеет вид: `domain\login` или `login@domain`. Для логина учетной записи не учитывается регистр.

> **Примечание:**
>
> Требования к безопасности (см. *Настройки пароля*) не распространяются на пользователей, добавленных из LDAP-каталога. Для таких пользователей недоступно изменение пароля в Системе.

> **Важно!**
>
> Изменения учетной записи, внесенные в Active Directory, будут доступны в Системе только после повторного добавления учетной записи: ее нужно удалить, а затем добавить повторно.

6.3.3 Редактирование учетной записи

Чтобы изменить учетную запись пользователя:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Пользователи**.
2. Нажмите напротив пользователя или на странице его профиля справа вверху.
3. Выберите **Редактировать**.
4. В открывшемся окне измените одну или несколько настроек. Настройки описаны в статье *Создание нового пользователя*.
5. Нажмите **Сохранить**. Новые настройки вступят в силу.

Чтобы назначить роль пользователю:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Пользователи**.
2. Выберите пользователя.
3. В личной карточке пользователя перейдите на вкладку **Права доступа** и нажмите на ссылку Назначить роль.
4. В поле **Роль** выберите роль из раскрывающегося списка. Пользователь без роли не сможет работать в Системе.
5. Нажмите **Сохранить**.
6. Чтобы применить изменения, пользователь с данной ролью должен выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессии данного пользователя, в открывшемся диалоговом окне отметьте **Завершить активную сессию пользователя**.
7. Подтвердите действие, нажав **Применить**. Пользователю будет назначена новая роль.

6.3.4 Просмотр профиля пользователя

На странице профиля представлены:

1. Вкладка **Персональная информация**. Содержит данные, указанные при создании:
    - фото пользователя;
    - имя пользователя;
    - логин пользователя в Системе;
    - язык, используемый пользователем в Системе;
    - контактные данные: номера телефонов, адреса электронной почты;
    - журнал последних активностей с учетной записью;
    - переключатель *Отображать только функции установленных продуктов*, который скрывает от пользователя разделы и виджеты неустановленных продуктов.
2. Вкладка **Права доступа**. Содержит информацию о правах пользователя в Системе:
    - роль, назначенная пользователю;
    - доступные для выполнения функции:
        - доступ, который имеет данный пользователь к настройкам и продуктам;
        - совокупность данных, к которым пользователь имеет доступ.

    Чтобы снять или назначить новую роль, перейдите в окно редактирования учетной записи (см. *Редактирование учетной записи*).

Действия пользователя:

- Редактирование учетной записи
- Смена пароля пользователя
- Активация и деактивация пользователя

6.3.5 Смена пароля пользователя

Чтобы сменить выданный пароль при первом входе в Систему или скомпрометированный пароль:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Пользователи**.
2. Откройте меню одним из способов:
   - в разделе **Пользователи** в таблице нажмите напротив пользователя;
   - откройте профиль пользователя и нажмите в правом верхнем углу.
3. Выберите **Сменить пароль**.
4. Заполните поля:

Поле	Описание
Старый пароль	Введите действующий пароль
Новый пароль	Введите новый пароль. Новый пароль должен удовлетворять настройкам безопасности (см. *Настройки пароля*)
Подтверждение пароля	Введите повторно новый пароль

5. Нажмите **Сохранить**.

6.3.6 Активация и деактивация пользователя

Главный офицер может запретить выбранному пользователю выполнять любые действия в Системе. Для этого:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Пользователи**.
2. Откройте меню одним из способов:
   - в разделе **Пользователи** в таблице нажмите напротив активного пользователя;
   - откройте профиль активного пользователя и нажмите в правом верхнем углу.
3. Выберите **Деактивировать**. Учетная запись пользователя будет заблокирована.

Чтобы разблокировать ранее заблокированную учетную запись:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Пользователи**.
2. Откройте меню одним из способов:
   - в разделе **Пользователи** в таблице нажмите напротив заблокированного пользователя;
   - откройте профиль заблокированного пользователя и нажмите в правом верхнем углу.
3. Выберите **Активировать**. Разблокированный пользователь может снова работать в Системе.

Другие офицеры безопасности могут деактивировать пользователей, если у них есть доступ к настройкам пользователей.

6.3.7 Удаление пользователя

Главный офицер может удалять учетные записи пользователей. Для этого:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Пользователи**.
2. Откройте меню одним из способов:
   - в разделе **Пользователи** в таблице нажмите напротив пользователя;
   - откройте профиль пользователя и нажмите в правом верхнем углу.
3. Выберите **Удалить**.
4. В открывшемся окне нажмите **Ок**. Учетная запись пользователя со всеми данными будет удалена без возможности восстановления.

> **Примечание:**
>
> Учетная запись Главного офицера не может быть удалена.

6.3.8 Сброс двухфакторной аутентификации

Сброс в интерфейсе Центра расследований

Если пользователь потерял доступ к устройству с приложением для двухфакторной аутентификации, пользователь с ролью *Главный офицер безопасности* может сбросить для него двухфакторную аутентификацию в интерфейсе Центра расследований:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Пользователи**.
2. Нажмите в строке пользователя.
3. Выберите **Сбросить синхронизацию TOTP**.
4. В открывшемся окне нажмите **Сбросить**.

После этого пользователю необходимо заново пройти процесс настройки двухфакторной аутентификации при входе в Систему (подробнее см. *Вход в систему*).

Сброс при помощи скрипта

В случае, если доступ утерян пользователем с ролью *Главный офицер безопасности*, а другие пользователи не имеют возможности сбросить для него двухфакторную аутентификацию через Центр расследований, следует воспользоваться скриптом. Скрипт `reset_totp.sh` делает секрет приложения TOTP для пользователя неподтвержденным.

Чтобы выполнить сброс:

1. В директории инсталлятора перейдите в `/platform/resources/scripts`.
2. Выполните команду вида:

```
./reset_totp.sh [USER_ID] [NAMESPACE]
```

где:

- `USER_ID` – идентификатор пользователя для сброса TOTP. По умолчанию: `master-officer-id`
- `NAMESPACE` – Kubernetes namespace, где находится под с PostgreSQL. По умолчанию: `infowatch`

Пример команды:

```
./reset_totp.sh master-officer-id infowatch
```

Дождитесь завершения сброса. Ответ о завершении будет выглядеть следующим образом:

```
Resetting TOTP secret for user 'master-officer-id' in pod 'postgresql-central-667f54d4f5-
zpnk9' (ns='infowatch')
Defaulted container "postgresql-central" out of: postgresql-central, pgupdate (init)
DELETE 1
```

После этого пользователю необходимо заново пройти процесс настройки двухфакторной аутентификации при входе в Систему (подробнее см. *Вход в систему*).

6.4 Роли

Пользователи Системы могут иметь разные роли, которые определяют их права в Системе. Если пользователю не назначена роль, он не имеет доступа в Систему.

Пользователь, который работает в Системе, имеет только одну **Роль.** Эта **Роль** содержит в себе **Функции** и **Данные**, доступ к которым может быть ***открыт полностью***, ***только на просмотр*** или ***запрещен***

На главной странице раздела **Настройки** → **Настройки пользователей** → **Роли** отображены все используемые в Системе роли. Они включают в себя вновь созданные пользовательские роли и две предустановленные:

1. **Главный офицер** – имеет полный доступ ко всем данным Системы, ее настройкам и управлению ролями, включая:
   - создание новых пользователей;
   - создание новых ролей и назначение их пользователям.
2. **Офицер безопасности** – имеет полный доступ к данным Системы, за исключением раздела **Настройки**.

Информация о роли содержится на следующих вкладках:

- **Функции** – доступ пользователя с этой ролью к продуктам, отдельным их функциям и настройкам;
- **Данные** – доступ пользователя с этой ролью к данным;
- **Пользователи** – на вкладке Главный офицер может назначить или снять роль с пользователей.

Роль может быть назначена:

- при создании нового пользователя;
- при создании новой роли;
- добавлена из списка существующих ролей в карточке пользователя на вкладке **Права доступа**.

Действия пользователя:

- Создание и настройка роли
- Просмотр, редактирование и копирование роли пользователя
- Снятие и удаление роли пользователя

6.4.1 Создание и настройка роли

Пользователь с ролью **Главный офицер безопасности** может создавать роли и назначать их пользователям. Роль определяет функции пользователя в Системе. Если компетенции пользователя изменились, нужно либо отредактировать роль, либо создать новую роль и назначить ее пользователю. Если у всех пользователей разные компетенции, то необходимо создать столько ролей, сколько пользователей есть в Системе.

Чтобы создать роль:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Роли**.
2. Нажмите **+ Создать**.
3. В открывшемся окне введите название роли и, если необходимо, краткое описание.
4. Нажмите **Сохранить**.
5. На вкладке **Функции** определите доступ пользователя с данной ролью к продуктам и настройкам:
   a. Отметьте в списке **Функции**, к каким из установленных продуктов и к каким их разделам нужно предоставить полный доступ пользователю. По умолчанию пользователь с ролью, не содержащей открытых доступов, сможет авторизоваться в Системе и использовать функциональность разделов **Главная** и **Персоны**.
   Раздел **Кластеризация**, содержащий функциональность **Data Explorer**, также доступен всем пользователям по умолчанию.

> **Доступ к функциям Центра расследований**
>
> Доступ к *Событиям, Статистике нарушений* дает возможность использовать функциональность разделов **События**, **Отчеты**, **Аналитика**, включая виджеты **Дата**, **Отправители**, **Получатели**, **Типы событий**.
>
> Доступ к *Расследованиям* дает возможность работать в этом разделе.
>
> Доступ к *Деталям событий* дает возможность просмотреть дополнительную информацию о событии в разделе **События** или перейти для этого в InfoWatch Traffic Monitor. Также доступ к *Деталям событий* позволяет использовать:
>
> - виджеты **Типы вложений**, **Топ вложений**, **Список событий (краткий)**;
> - фильтры **Имя вложения**, **Наличие вложения**, **Тип вложения**, **Тема письма**.
>
> Доступ к *Деталям нарушений* дает возможность выгружать данные о деталях в отчет, использовать:
>
> - виджеты **Уровень нарушений**, **Вердикт**, **Статистика**, **Решение пользователя**, включая соответствующие им фильтры;
> - маркировку событий и раскраску виджетов по уровню нарушений.
>
> Доступ к *Политикам, ОЗ, Периметрам* дает возможность использовать:

- виджеты **Политики**, **Объекты защиты**, **Статистика**, **Теги DLP**, включая соответствующие им фильтры, а также фильтры **Периметр** и **Вошло**/**Покинуло периметр**;
- дополнительные колонки в разделе **События**.

Доступ к *Статусам досье* дает возможность использовать атрибут фильтра и виджет **Статусы** в досье персоны.

Доступ к *Отправке и получению уведомлений* дает доступ к разделу **Уведомления** и возможность создавать и получать уведомления. Без доступа к этой функции раздел **Уведомления** не будет отображаться у пользователя.

Доступ к функциям продуктов

- **Activity Monitor**

  Доступ к *Аналитике* дает возможность использовать:

  - статистику и события активности в разделах **Аналитика** и **Мониторинг**
  - соответствующие доступным виджетам атрибуты фильтра для событий активности
  - виджеты Activity Monitor в разделе **Персоны** и на странице **Аналитика** (**Статистика активности**)
  - функциональность отчетов в разделах **Аналитика**, **Мониторинг** и **Отчеты**

  Доступ к *Снимкам экрана* дает возможность:

  - отображать снимки экрана в разделах **Мониторинг** и **Персоны**
  - отображать и фильтровать связанные с ними события

  Доступ к *Аудиозаписям* дает возможность:

  - отображать данные по аудиозаписям в разделах **Мониторинг** и **Персоны**
  - отображать и фильтровать связанные с ними события

  Доступ к *Видеозаписям* дает возможность:

  - отображать данные по видеозаписям в разделах **Мониторинг** и **Персоны**

  Доступ к *Наблюдению* дает возможность пользоваться функциональностью наблюдения и таймлайна в разделах **Мониторинг** и **Персоны**

  Доступ к *Онлайн наблюдению* дает возможность:

  - просмотру экрана персоны,
  - прослушиванию звукового окружения персоны,
  - блокировке сессии персоны,
  - запросить список запущенных процессов на компьютере персоны

  Доступ к *Вводимому тексту* дает возможность:

  - отображать введенный текст в связанных событиях,
  - фильтровать по наличию введенного текста

  Доступ к *Поисковым запросам* дает возможность:

- отображать поисковые запросы в связанных событиях
- фильтровать по наличию поисковых запросов

Доступ к *Действиям с файлами* дает возможность:

- отображать действия с файлами и связанные с ними события в разделах **Мониторинг** и **Досье**
- фильтровать события по действиям с файлами
- выгружать отчеты в разделе **Мониторинг**

- **Data Access Tracker**

  Доступ к *Инфраструктуре* дает возможность использовать функциональность раздела **Инфраструктура**:

  - виджеты продукта Data Access Tracker на вкладке **Сводка** и в разделе **Аналитика** в дашбордах;
  - вкладку **Отчеты инфраструктуры**:
    - отчеты на основе данных, полученных во время синхронизации с контроллерами домена через WinRM/LDAP:
      - уязвимые учетные записи;
      - события службы каталогов, связанные с риском несанкционированного доступа;
    - отчеты о доступе к почтовым ящикам, папкам и файлам, а также правах локального администратора.
  - вкладки **Записи аудита**, **Угрозы**, **Критерии угроз**:
    - события изменений объектов домена, полученные во время синхронизации с контроллерами домена через DirSync/Syncrepl;
    - обнаруженные среди них угрозы;
    - критерии обнаружения угроз.

- **Data Discovery**

  Доступ к *Хранению файлов* дает возможность:

  - работать **в разделе Хранение файлов**:
    - на вкладке **Задачи** - создавать и запускать задачи сканирования;
    - на вкладках **Информация о файлах**, **Дубликаты файлов, Похожие файлы** - анализировать результаты сканирования, контентного анализа и группировки файлов по дубликатам или похожим.
  - работать **в досье персон на вкладке Хранение файлов**, которая включает в себя подразделы:
    - **Владелец файлов**
    - **Доступные файлы**
  - работать с виджетами Data Discovery в разделе **Аналитика** в дашбордах
  - выгружать отчеты с информацией из подразделов **Владелец файлов** и **Доступные файлы** досье персоны, а также - из вкладок **Информация о файлах**, **Дубликаты файлов** и **Похожие файлы** раздела **Хранение файлов**

- **Device Control**

Доступ к *Внешним устройствам* дает возможность работать в подразделе **Устройства** → **Внешние устройства**:

- создавать правила контроля внешних устройств
- просматривать события их использования

Доступ к *Приложениям* дает возможность работать в подразделе **Устройства** → **Приложения**:

- создавать правила контроля приложений
- просматривать события запрета их использования

- **Prediction**

  Доступ к *Досье, Рейтинг* дает возможность:

  - работать с рейтингом персон и карточками групп риска в разделе **Риски**
  - работать в досье персоны на вкладках **Группы рисков** и **Карта паттернов**
  - работать с виджетами Prediction в разделе **Аналитика** в дашбордах
  - выгружать отчеты в разделе **Риски** и на вкладке **Группы рисков** в досье персоны

- **Vision**

  Доступ к *Графу связей* дает возможность использовать функциональность графа.

  Доступ к Статистике нарушений дает возможность работать со:

  - статистикой в разделах **Аналитика** и **Персоны**, выгружать отчеты
  - виджетами Vision в разделе **Аналитика**
  - файлами отчетов в разделе **Отчеты**

  Доступ к *Комментариям и файлам в Досье* дает возможность:

  - использовать виджеты Комментарии и Файлы в досье персоны
  - сформировать выгрузку или скриншот виджета или графа с сохранением в досье

b. Отметьте в списке **Настройки**:
   - ☑ - если нужен полный доступ (просмотр и редактирование) к настройкам в разделе ⚙ **Настройки**. По умолчанию доступ запрещен;
   - 👁 - если нужны права только на просмотр;
   - ☐ - если нужно запретить доступ к отдельным разделам.
     При этом доступ к персональной информации в собственном профиле у пользователя есть всегда.

6. На вкладке **Данные** вы можете настроить доступ к данным для пользователя. Для изменения прав доступа к выборочным данным, укажите их в категориях: *Персоны*, *Группы, Отделы, Контакты*, *Филиалы*, *Политики*, *Объекты защиты*. При этом можно:
   - ☐ - ограничить доступ к выбранным данным;
   - ☑ - разрешить доступ к выбранным данным;
   - ☒ - закрыть доступ к выбранным данным.

Пример:

Если отметить Персону знаком ☒, то эта роль запретит пользователю доступ к любой информации о ней в Системе.

Если отметить Персону знаком ☑ (или оставить по умолчанию ☐ у всех Персон), то эта роль предоставит пользователю полный доступ к данным персоны: событиям, досье, в Едином фильтре, отображениях на Графе связей и виджетах.

Если отметить Персону знаком ☐ при одновременном выборе других Персон, то эта роль предоставит пользователю доступ к ее событиям с участием отмеченных персон (☑), но без доступа к любым отображениям на Графе связей, виджетах и в Едином фильтре.

Примечание:

Главный офицер безопасности должен следить за добавляемыми условиями, так как при использования различных элементов в роли может получиться не увеличение, а уменьшение количества доступных данных из-за использования между категориями оператора И.

Например:

a. Был настроен доступ к Группе-1 ИЛИ Группе-2.
b. Добавили доступ к Персоне-1, Персоне-2, Персоне-3.
   В итоге количество доступных пользователю данных уменьшилось, потому что получилось условие:
   (Группа-1 ИЛИ Группа-2) И (Персона-1 ИЛИ Персона-2 ИЛИ Персона-3).

Чтобы настроить общее ограничение и на группы и на персоны, создайте сводную группу, которая включает в себя все необходимые группы и персоны. Используйте ее в настройках доступа.

Чтобы проверить правильность добавления новых областей видимости и исключений, задайте аналогичные условия в Едином фильтре или, например, в фильтре *Владелец*, и проверьте результаты на виджетах.

7. Если требуется закрыть доступ ко всем данным, отметьте ☑ **Запретить доступ к данным.**

Примечание:

Для корректной работы с Data Explorer не запрещайте пользователю доступ к данным.

8. На вкладке **Пользователи** выберите доступного пользователя без роли, которому необходимо назначить данную роль. Для этого:
   a. Нажмите **+ Добавить**.
   b. В открывшемся диалоговом окне выберите пользователя в поле **Пользователи**.
   c. Нажмите **Выдать**. Роль будет назначена данному пользователю.
9. После внесения всех настроек нажмите **Применить**.
10. Для применения настроек, пользователи должны выйти из системы и повторно авторизоваться. До выхода из системы будут распространяться старые правила ролевого доступа. Чтобы принудительно завершить сессии пользователей с данной

ролью, отметьте **Завершить активные сессии пользователей** в открывшемся окне, а затем **Применить.**

6.4.2 Просмотр, редактирование и копирование роли пользователя

Главный офицер может просматривать и редактировать выданные пользователям роли в их личных профилях. Для этого:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Роли**.
2. Выберите пользователя, профиль которого необходимо просмотреть. На странице профиля представлена карточка пользователя с его личными данными.
3. Перейдите на вкладку **Права доступа**. На вкладке содержится информация о назначенной пользователю роли, а также:
   - функции– имеет ли пользователь доступ к настройкам продукта;
   - данные (области видимости) – совокупность данных, к которым пользователь имеет доступ.
4. Чтобы поменять роль пользователю, нажмите и выберите **Редактировать**.
5. В открывшемся окне сначала удалите настоящую роль, нажав .
6. Назначьте новую роль, нажав и выбрав необходимую роль из списка.
7. Нажмите **Сохранить**.
8. Для применения настроек пользователь должен выйти из Системы и повторно авторизоваться. Чтобы принудительно завершить сессию пользователей с данной ролью, отметьте **Завершить активную сессию пользователя** в открывшемся окне, а затем нажмите **Применить**.

Чтобы скопировать любую роль пользователя, например, при расширении штата или для аудиторской проверки:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Роли**.
2. Нажмите на плашке роли, которую необходимо скопировать и выберите **Копировать роль**. При этом будут скопированы следующие атрибуты роли:
   - **Название** – при каждом копировании роли к названию будет добавляться слово **Копия**, пока не получится уникальное название роли:

     Пример: Название *Офицер* в результате копирования поменяется на *Офицер копия*. Чтобы переименовать роль, отредактируйте ее;

   - **Описание**;
   - **Настройки доступа** – копируются все настройки: элементы функций и данных;
   - **Дата создания** – указываются текущие дата и время.

Список пользователей, которым выдана роль, не копируется.

6.4.3 Снятие и удаление роли пользователя

Пользователь не может иметь несколько ролей одновременно. Поэтому если требуется выдать пользователю новую роль, нужно снять действующую.

Чтобы снять роль в карточке роли:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Роли**.

2. Выберите роль, которую необходимо удалить для пользователей.
3. Перейдите на вкладку **Пользователи**.
4. Отметьте пользователей, у которых необходимо снять данную роль.
5. Нажмите **Удалить**. Для данных пользователей роль будет снята. После этого можно назначить им другую роль.
6. Нажмите **Применить**.

Чтобы снять роль в карточке пользователя:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Роли**.
2. Выполните одно из следующих действий:
   - Нажмите на плашке пользователя, для которого необходимо удалить данную роль.
   - Выберите пользователя и затем нажмите в его личной карточке.
3. В меню выберите **Редактировать**.
4. В открывшемся окне в поле **Роли** удалите роль пользователя, нажав .
5. Нажмите **Сохранить**.
6. Чтобы применить изменения, пользователь с данной ролью должен выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессии данного пользователя, в открывшемся диалоговом окне отметьте **Завершить активную сессию пользователя**.
7. Подтвердите действие, нажав **Применить**. У данного пользователя роль будет снята.

Главный офицер может удалять любые роли, кроме предустановленных.

Чтобы удалить роль из Системы:

1. Перейдите в раздел **Настройки** → **Настройки пользователей** → **Роли**.
2. Выполните одно из следующих действий:
   - Нажмите на плашке пользовательской роли, которую требуется удалить.
   - Выберите роль и затем нажмите .
3. В окне меню выберите **Удалить**.
4. Чтобы применить изменения, пользователи с данной ролью должны выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессий данных пользователей, в открывшемся диалоговом окне отметьте **Завершить активные сессии пользователей**.
5. Подтвердите действие, нажав **Удалить**. Если роль была назначена пользователям, она будет снята для них и удалена из списка ролей.

6.5 Аудит

В разделе отображается журнал действий пользователей в Системе. Данные журнала может просматривать только пользователь, которому разрешен доступ к разделу (подробнее см. *Роли*).

Журнал содержит следующую информацию:

- **Пользователь** – пользователь, который совершил действие;
- **Действие в системе** – действие, которое было выполнено над объектом;
- **Тип объекта** – пользователь, интеграция, досье, роль;

- **Объект события** – название объекта, над которым было совершено действие (например, название роли или интеграции);
- **Филиал** – название филиала, где было зафиксировано событие аудита;
- **Дата** – дата и время создания события аудита;
- **IP-адрес источника события** – IP-адрес, с которого было совершено действие.

> **Примечание:**
>
> События в журнале аудита хранятся бессрочно и удалению не подлежат.

Выполняется аудит следующих действий:

Пользователи	• успешная авторизация • неуспешная авторизация • неуспешное введение кода доступа[1] • создание • изменение • удаление • изменение пароля • блокировка пользователя • разблокировка пользователя • настройка двухфакторной аутентификации • сброс синхронизации по TOTP
Роли	• создание • изменение • удаление
Интеграции	• создание • изменение • удаление • ручной запуск
Досье	• просмотр • создание • изменение • удаление • объединение

> **Примечание:**
>
> [1] Если при настроенной двухфакторной аутентификации пользователь после ввода логина и пароля закрывает страницу с Системой, не введя 6-значный код, событие аудита *Неуспешное введение кода доступа* создано не будет.

В разделе **Аудит** вы можете:

- выгрузить отчет с событиями аудита в формате CSV;

- переместить колонки в таблице;
- отсортировать содержимое колонок (по умолчанию события отсортированы от последних к более ранним);
- перейти в карточку пользователя в разделе **Пользователи** – при нажатии на пользователя;
- добавить и удалить фильтры на панели;
- отсортировать события, выбрав фильтры;
- скопировать содержимое ячейки в таблице.

По умолчанию в разделе отображаются все фильтры:

- *Дата события*
- *Действие в системе*
- *Объект события*
- *Пользователь*
- *Тип объекта*
- *Филиал*
- *IP-адрес источника события*

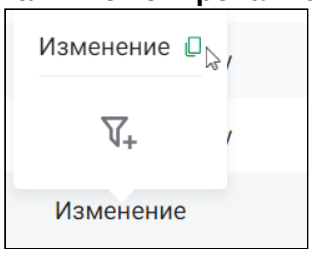
Для управления фильтрами воспользуйтесь кнопкой . Установите флаг , чтобы добавить фильтр на панель, или снимите флаг, чтобы удалить фильтр из набора.

Чтобы отсортировать события, выберите атрибут фильтра:

- на панели над таблицей;
- непосредственно в таблице. Для этого:
  a. Наведите курсор на содержимое ячейки.
  b. Во всплывающем окне нажмите **Добавить в фильтр** . Содержимое таблицы будет отсортировано в соответствии с выбранным атрибутом.

Чтобы скопировать содержимое ячейки:

1. Наведите курсор на содержимое ячейки.
2. Во всплывающем окне поместите курсор на строку с содержимым, затем нажмите **Копировать** .



В колонке **Дата** кнопка **Копировать** отображается справа при наведении курсора на содержимое ячейки.

Чтобы выгрузить отчет с выбранными событиями аудита:

1. Нажмите **Сохранить отчет** .
2. Перейдите в папку **Загрузки** вашего компьютера.

При выгрузке сохраняется порядок колонок в таблице по умолчанию.

Для просмотра отчета в MS Excel необходимо поменять кодировку на UTF-8. Подробнее см. статью Базы знаний *Как сменить кодировку файла на UTF-8 в Excel*.

6.6 Настройки пароля

Чтобы предотвратить несанкционированный вход в Систему и максимально обезопасить пользователя от компрометации его учетных данных третьими лицами, Офицер безопасности может устанавливать правила формирования паролей учетных записей и сроки их действия. Для этого:

1. Перейдите в раздел  **Настройки** → **Настройки системы** → **Настройки пароля**.
2. В открывшемся окне установлены настройки по умолчанию. Чтобы ввести новые требования к паролю учетной записи, измените значения параметров:

Параметр	Описание
Буквы	Заглавные и строчные буквы русского и латинского алфавитов, которые используются для составления пароля. Можно установить: - обязательно для ввода (☑) – обязательно присутствие букв в пароле - опционально (☐) – допускается пароль без букв
Цифры	Арабские цифры, которые используются для составления пароля. Можно установить: - обязательно для ввода (☑) – обязательно присутствие цифр в пароле - опционально (☐) – допускается пароль без цифр
Специальные символы	Перечень спецсимволов, которые могут быть в пароле. Можно установить: - обязательно (☑) – обязательно присутствие спецсимволов в пароле - опционально (☐) – допускается пароль без спецсимволов
Минимальная длина	Минимально допустимая длина пароля в символах
Невозможно использование последних N паролей	Чтобы избежать компрометации, запрещено использовать пароли за предыдущие периоды
Срок действия пароля	Количество дней действия пароля. Пароль нужно сменить до истечения указанного срока
Период неудачных попыток авторизации	Период (в минутах), в течение которого пользователь может вводить неверный пароль

Параметр	Описание
Количество неудачных попыток ввода	Количество неуспешных попыток ввода пароля, после которого учетная запись будет заблокирована
Период блокировки пользователя	Период блокировки учетной записи (в минутах)

3. Нажмите **Сохранить**, чтобы активировать новые значения параметров. Если нужно вернуться к прежним настройкам, нажмите **Сбросить настройки до значений по умолчанию**.

> **Пример**
>
> `Период неудачных попыток авторизации – 5.`
>
> `Количество неудачных попыток ввода – 4.`
>
> `Период блокировки пользователя – 15.`
>
> Если установлены указанные значения параметров, то после 4 неудачных попыток ввода пароля в течение 5 минут учетная запись пользователя будет заблокирована на 15 минут. После этого можно будет повторить ввод пароля.

6.6.1 Требования к имени пользователя и логину

Имя пользователя должно содержать не менее четырех символов.

Логин пользователя:

- должен начинаться с буквы и не заканчиваться точкой
- может состоять из букв латинского алфавита, арабских цифр и содержать спецсимволы: "_", "-", "–", "."

6.7 Основные настройки

В разделе  **Настройки** → **Настройки системы** → **Основные настройки** вы можете:

- задать настройки сессии;
- управлять сбором статистических данных;
- включить режим облегченной версии Платформы.

> **Важно!**
>
> Другие настройки этого раздела не используются для Data Explorer.

6.7.1 Настройки сессии

Вы можете установить время жизни сессии – время ожидания активности пользователя в Консоли. Если в течение указанного отрезка времени не было зафиксировано активности (движения мыши и нажатия клавиш на клавиатуре), произойдет автоматический выход из Консоли. В этом случае для продолжения работы необходимо заново авторизоваться в Системе. Чтобы задать настройки:

1. В поле **Время жизни сессии** установите необходимое значение (в минутах).
2. В правом верхнем углу нажмите **Сохранить**.

6.7.2 Сбор статистических данных

Система сбора статистики накапливает и обобщает данные о работе пользователя в Консоли управления. По решению пользователя эти данные могут быть скачаны и отправлены в компанию InfoWatch для обработки. Это делается для повышения качества продукта, оценки востребованности той или иной функциональности и разработки новых сценариев работы.

Сбор статистических данных включен по умолчанию. Чтобы отключить сбор данных, снимите флажок в поле **Включить** и нажмите **Сохранить**.

> **Примечание:**
>
> Система сбора статистики не накапливает, не анализирует и не передает персональные данные. Все ФИО пользователей и сотрудников заменяются на внутрисистемные ID-номера.

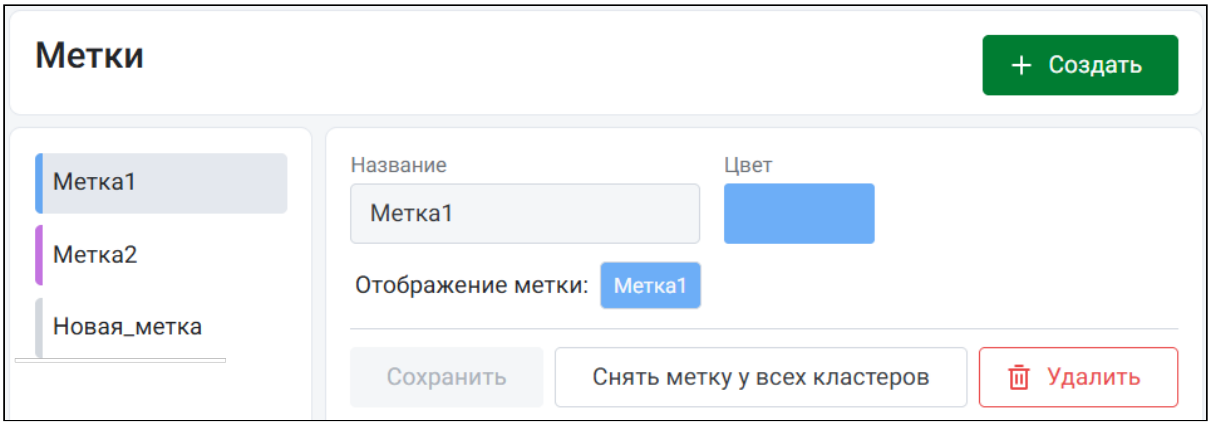
6.7.3 Облегченная версия Платформы

Режим работы для продуктов Центра расследований, исключающий получение событий из Traffic Monitor. Для корректной работы после включения или выключения режима повторно сохраните настройки интеграции с Traffic Monitor.

Режим напрямую не затрагивает функциональность Data Explorer. Не включайте режим, если в кластере установлены продукты, использующие события Traffic Monitor.

7 Метки

В разделе **Настройки** → **Data Explorer** → **Метки** вы можете просматривать список существующих меток, создавать их и редактировать.



Изначально в Системе нет меток. Вы создаете их при добавлении к кластерам в разделе **Кластеризация** или в данном разделе.

Все существующие метки отображаются в списке слева. Чтобы выбрать метку, кликните по ней в этом списке. В области справа вы можете настроить метку и посмотреть, как она отображается в разделе **Кластеризация**.

Чтобы создать метку:

1. Нажмите **+ Создать**.
2. Введите название метки.
3. Измените цвет, если необходимо.
4. Нажмите **Сохранить**.

Чтобы отредактировать метку:

1. Выберите метку в списке.
2. Измените название и цвет, если необходимо.
3. Нажмите **Сохранить**.

Также здесь вы можете **снять метку у всех кластеров**, которым она была ранее добавлена, и **удалить** метку из Системы. При удалении она будет автоматически снята у кластеров.

8 Уведомления

Уведомления в Системе могут быть двух видов:

- **системные**, которые приходят автоматически;
- **пользовательские**, отправку которых настраивает Офицер безопасности вручную и может получать как в Центре расследований, так и по электронной почте или в Телеграм-канале.
  Data Explorer не работает с пользовательскими уведомлениями.

Чтобы ознакомиться с системными уведомлениями Центра расследований, нажмите .
Уведомления содержат информацию о:

- статусе синхронизаций с различными источниками, которые инициировал пользователь;
- добавлении лицензии;
- удалении лицензии;
- скором истечении срока действия лицензии;
- возможной нехватке места на жестком диске;
- скором истечении срока действия пароля;
- попытках входа в аккаунт с других компьютеров и блокировки аккаунта.



9 Добавление пользовательского сертификата

Чтобы не допустить несанкционированный доступ к Системе и повысить защищенность канала передачи данных, можно добавить новый пользовательский сертификат для веб-службы. Это действие доступно в любой момент использования Системы и выполняется через командную строку. Чтобы добавить пользовательский сертификат:

1. Разместите на диске два файла в формате PEM:
   - файл с сертификатом (например: `test.crt`);
   - файл с закрытым ключом (например: `test.key`).
2. Перейдите в директорию, в которую был распакован архив с дистрибутивом при установке Системы.

   > **Примечание:**
   >
   > Платформа не поддерживает использование ключей, защищенных паролем.
   >
   > Дополнительно рекомендуем проверить хеш-суммы сертификата и ключа с помощью команд:
   >
   > ```
   > openssl x509 -noout -modulus -in test.crt | openssl md5
   >
   > openssl rsa -noout -modulus -in test.key | openssl md5
   > ```
   >
   > Значение в выводе команд должно совпадать.

3. Выполните команду от имени пользователя с правами root:

   ```
   ./setup.py setwebkeys --certificate=/folder/test.crt --privatekey=/folder/test.key
   ```

   В нашем примере:
   - `/folder/test.crt` – полный путь к файлу с сертификатом;
   - `/folder/test.key` – полный путь к файлу с закрытым ключом.

Последний добавленный сертификат считается действительным. После добавления или замены сертификата обновите вручную все открытые вкладки браузера, используемые Системой.

10 Расширенный фильтр

Расширенный фильтр дополняет возможности Единого фильтра, позволяя использовать в фильтрах условие ИЛИ и группы фильтров.

Data Explorer поддерживает только **обычный режим** Единого фильтра.

По умолчанию расширенный фильтр включен. Если вы хотите отключить его, выполните команду вида:

```
curl 'https://<адрес_центральной_ноды>/api/configStorage/v1/value/platform/AdvancedFilters' \
-H 'Cookie: iwAccessToken=<значение_токена>' \
-H 'Content-Type: application/json' \
--data '{"obj":false}'
```

В команде обязательно укажите **адрес центральной ноды Платформы**.

Значение `iwAccessToken` вы можете скопировать из cookie браузера. Например, в браузере Google Chrome для этого:

1. Авторизуйтесь в веб-интерфейсе Центра расследований.
2. Откройте режим разработчика и перейдите на вкладку `Application`.
3. В разделе `Storage` → `Cookies` выберите текущее подключение.
4. Скопируйте значение поля `iwAccessToken`.

Пример команды с адресом и токеном:

```
curl 'https://10.60.12.34/api/configStorage/v1/value/platform/AdvancedFilters' \
-H 'Cookie:
iwAccessToken=eyShbGciOiJFUzI1NiIsInR5cCI7IkpXVCJ9.eyJleHAiOjE2ODMzMjQ4MzksImlhdCI6MTc4MzMyMTIzOSwiaXNzIjoi
aXdwbGYiLCJqdGkiOiJlYmVkOTVjZi1kMTkxLTRhMzctOTVkMS1jNWM0OGUxZDkwZjkiLCJwcm2kdWS0cyI6WyJwbGF0Zm9ybSJdLCJzZXJ
2aWNlQWxsb3dMaW5rcyI6bnVsbCwic3ViIjoibWFzdGVyLW9mZmljZXItaWQiLCJzdWJuIjoib2ZmaWNlciIsInN1YnQiOiJ1c2VyIiwidm
VyIjoyfQ.srIVe3myI2bM_xpdrQnJfP4Q3s_d75A5XG3Cjg_9Ys51VbGU36Q3CsWBdZTp_dMDDp0VtcidtSyBrjz6FLtNpQ' \
-H 'Content-Type: application/json' \
--data '{"obj":false}'
```

Чтобы включить расширенный фильтр, выполните ту же команду, используя значение `true` вместо `false`.