

INFOWATCH

InfoWatch Device Control. Руководство администратора

27/01/2025

© 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 Лицензирование 8

5 Настройки 9

5.1 Состояние системы 9

5.2 Интеграции 11

5.2.1 Интеграция с Active Directory 11

5.2.2 Редактирование и удаление интеграции 14

5.3 Пользователи 15

5.3.1 Создание нового пользователя 15

5.3.2 Добавление нового пользователя из LDAP 16

5.3.3 Редактирование учетной записи 17

5.3.4 Просмотр профиля пользователя 18

5.3.5 Смена пароля пользователя 18

5.3.6 Активация и деактивация пользователя 19

5.3.7 Удаление пользователя 19

5.4 Роли 20

5.4.1 Создание и настройка роли 20

5.4.2 Просмотр, редактирование и копирование роли пользователя 22

5.4.3 Снятие и удаление роли пользователя 23

5.5 Данные для анализа 24

5.5.1 Партиции Traffic Monitor 24

5.5.2 Партиции Device Monitor 24

5.5.3 Настройки хранения 25

5.5.4 Ручное архивирование, восстановление и удаление партиций 26

5.6 Аудит 27

5.7 Настройки пароля 29

5.7.1 Требования к имени пользователя и учетной записи 31

5.8 Основные настройки 31

5.8.1 Настройки сессии 31

5.8.2 Отображение данных за период времени 31

5.8.3 Управление токенами 31

5.8.4 Выбор цвета для уровня нарушения 32

5.8.5 Создание шаблона имени 32
5.8.6 Выбор часового пояса 33
5.8.7 Чтобы настроить сбор статистической информации 33
6 Уведомления 34
7 Добавление пользовательского сертификата 35

Настоящее руководство содержит сведения по настройке и подготовке к работе InfoWatch Device Control (далее также Система или Device Control) - программного обеспечения, позволяющего управлять правами доступа к съемным устройствам.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, которые будут работать с Системой и заниматься ее администрированием.

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем семейств Linux и Microsoft Windows.

2 Комплект документов

В комплект документации по InfoWatch Device Control входят:

- «InfoWatch Device Control. Руководство по установке». Содержит описание установки, обновления и удаления InfoWatch Device Control.
- «InfoWatch Device Control. Руководство администратора». Содержит информацию по настройке и подготовке к работе InfoWatch Device Control.
- «InfoWatch Device Control. Руководство пользователя». Содержит описание работы с InfoWatch Device Control.

Сопутствующая документация по модулю InfoWatch Device Monitor for Linux включает в себя:

- «InfoWatch Device Monitor for Linux. Руководство по установке». Содержит описание установки, обновления и удаления модуля InfoWatch Device Monitor for Linux.
- «InfoWatch Device Monitor for Linux. Руководство пользователя». Содержит описание работы с InfoWatch Device Monitor for Linux.

3 Техническая поддержка пользователей

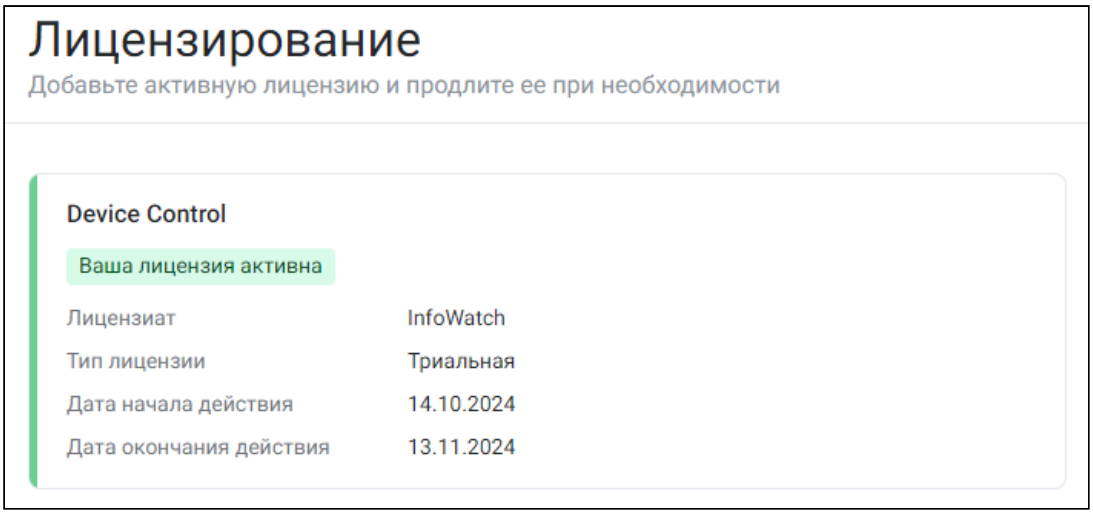
При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

- 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.

Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: www.infowatch.ru/services/support.

4 Лицензирование

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



Чтобы установить новую лицензию:

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

Чтобы удалить лицензию:

1. В правом верхнем углу плитки лицензии нажмите и выберите **Удалить**.
2. В появившемся меню подтвердите действие, нажав **ОК**.

Важно!

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

Важно!

По истечении срока действия пробной лицензии загрузка данных из систем-источников будет прекращена.

5 Настройки

Раздел **Настройки**  → **Настройки Системы** включает в себя следующие подразделы:

- Состояние системы
- Интеграции
- Пользователи
- Роли
- Данные для анализа
- Аудит
- Настройки пароля
- Основные настройки

> **Примечание:**
>
> Device Control не использует подразделы:
>
> - **Сервисы для уведомлений**, **Почтовые уведомления** - Device Control не отправляет почтовые уведомления;
> - **Фильтры** - Device Control использует отдельные фильтры, которые не переносятся в разделы других продуктов.

5.1 Состояние системы

В разделе **Настройки**  → **Состояние системы** представлены данные о состоянии сервера Device Control. Это доступность сервера, информация о состоянии его основных аппаратных компонентов и служб:

Поле	Описание
Лейбл (имя)	Лейбл и имя ноды в формате `лейбл(имя)`
Статус	• *Ready* – доступен и готов к работе; • *Not Ready* – не готов к работе; • *Unknown* – зарегистрирован, но не отвечает на запросы.
Адрес	IP-адрес сервера Device Control
Последнее обновление состояния системы	Дата и время получения информации о статусе сервиса
Версия ядра	Версия ядра ОС
Операционная система	ОС сервера Device Control
Память	Размер оперативной памяти сервера: всего и используется на данный момент

Поле	Описание
ЦП	Загрузка центрального процессора сервера Device Control
*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 данных Datastorage
*Дисковое пространство (PostgreSQL)**	Общее выделенное и занятое место на диске для хранения данных БД PostgreSQL
*Дисковое пространство (Clickhouse)**	Общее выделенное и занятое место на диске для хранения данных БД Clickhouse
*Дисковое пространство (Root)**	Общее выделенное и занятое место, отведенное для системных данных в корневой директории
Список всех служб Device Control	
Статус	Один из статусов службы: • *Запущена* – работает; • *Недоступна* – невозможно получить статус; • *Не инициализирована* – находится в процессе запуска; • *Не найдена* – должна быть в филиале, но отсутствует; • *Ошибка* – завершена с ошибкой.
Имя	Имя службы
Версия	Версия сборки службы
Просмотреть детали	Вывод информации о состоянии, событиях и внутренних сообщениях службы

* Если в одном из разделов Системы (например, /mnt/data) остается 10 ГБ (или меньше) свободного пространства, появится сообщение о том, что превышено ограничение по использованию дискового пространства. Будут остановлены все интеграции.

Чтобы снять это ограничение, в **Настройки** → **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:

1. Для сбора данных по всем службам и активности пользователя нажмите **Экспорт диагностических данных** и дождитесь загрузки.
2. Скачайте zip-архив, содержащий txt-файлы с логами и csv-файл с данными активности пользователя.

Чтобы скачать диагностические данные отдельной службы:

1. В списке служб нажмите  напротив нужной службы. Начнется формирование лог-файла, а затем загрузка.
2. Скачайте zip-архив, содержащий txt-файлы с логами службы.

5.2 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.

> **Важно!**
>
> Интеграция с InfoWatch Traffic Monitor не относится к функциональности продукта Device Control.

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

5.2.1 Интеграция с Active Directory

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

При первом входе в Систему список интеграций пустой.

Чтобы добавить новую интеграцию с Active Directory и запустить ее:

1. Перейдите в раздел **Настройки**  -> **Интеграции**.
2. Нажмите **+ Добавить**.
3. Выберите **Active Directory** и введите параметры:

Параметр	Описание
Имя интеграции	Название соединения, которое используется в Консоли
Филиал	Лейбл ноды Device Control для подключения к Active Directory, имеет значение `central`

Параметр	Описание
Адрес источника	Сетевой адрес сервера, с LDAP-каталогами которого производится синхронизация
Тип соединения	Выбор типа соединения, которое будет установлено: • Незащищенное соединение (LDAP) • Защищенное соединение по протоколу LDAP + StartTLS • Защищенное соединение по протоколу LDAPS (SSL) **Важно!** Соединение без сертификатов небезопасно.
Сертификат	Загрузка файла сертификата в форматах .pem, .der/.cer. для защищенных соединений
Глобальный порт	Порт для подключения глобального LDAP-каталога. В зависимости от типа соединения при нажатии  будут использованы значения по умолчанию: • 3268 для незащищенного соединения и защищенного соединения по протоколу LDAP + StartTLS; • 3269 для защищенного соединения по протоколу LDAPS.
Порт	Порт для подключения локального каталога домена. В зависимости от типа соединения или при нажатии  будут использованы порты по умолчанию: • 389 для незащищенного соединения и защищенного соединения по протоколу LDAP + StartTLS; • 636 для защищенного соединения по протоколу LDAPS.

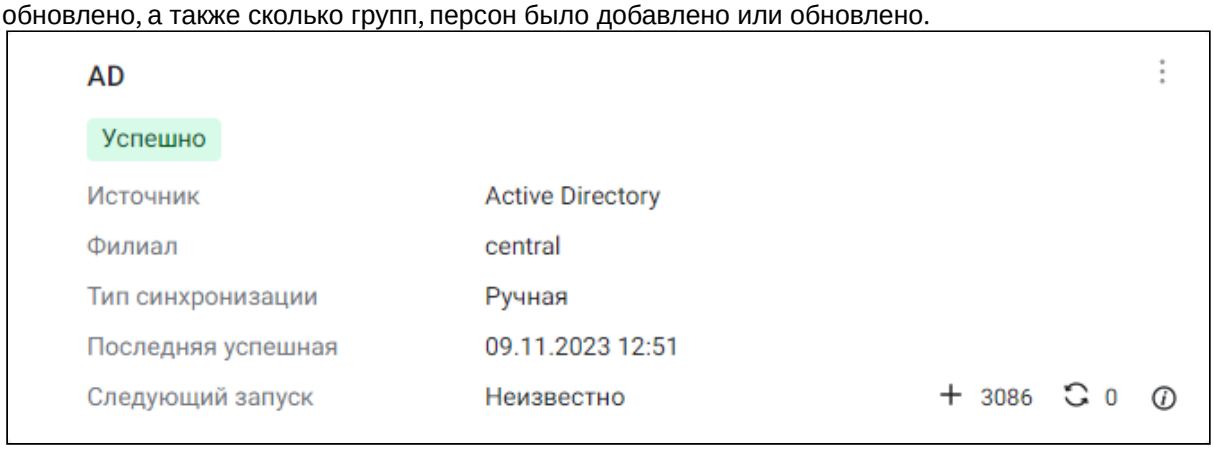
LDAP-запрос	Атрибуты фильтрации, являющиеся полным путем к указанному каталогу. При этом может быть указан только один каталог в организационной структуре Active Directory. Для оптимизации поиска вы можете использовать отдельные уровни иерархии базы:
	`C-countryName`
	`O-organizationName`
	`OU-organizationalUnit`
	`DC-domainComponent`
	`CN-commonName`
	Пример: Чтобы использовать в качестве базы поиска ветку `Users`, расположенную в домене компании, необходимо ввести: `cn=users,dc=company,dc=com`

Параметр	Описание
Логин	Логин для доступа к серверу Active Directory (для пользователя с правами на чтение каталога)
Пароль	Пароль для доступа к серверу Active Directory
Синхронизация	*Ручная* или *Автоматическая*. Во втором варианте необходимо указать *Периодичность* и *Повторение*
Периодичность	Как часто необходимо запускать синхронизацию : *Ежеминутно*, *Ежечасно*, *Ежедневно*, *Еженедельно*
Повторение	День недели и время следующей синхронизации

4. Нажмите **Проверить соединение**, чтобы проверить, что все параметры заполнены и корректны, и дождитесь сообщения "*Соединение успешно установлено*".
5. Нажмите:
   - **Сохранить** – при этом новая синхронизация будет ожидать запуска позднее

   или
   - **Сохранить и синхронизировать**, чтобы запустить процесс синхронизации немедленно.

Возможна последовательная синхронизация возможна с несколькими LDAP-каталогами. Список серверов, синхронизация с LDAP-каталогами которых настроена, отображается в центральной области. В нижней строке указано количество добавленных (+) персон, а также тех, данные которых обновились в ходе последней синхронизации . Детальная информация показывает операцию – создано/обновлено, а также сколько групп, персон было добавлено или обновлено.



Если необходимо провести ручную синхронизацию с теми же параметрами (например, при изменении в дереве каталогов компании):

1. Нажмите , чтобы начать синхронизацию.
2. Дождитесь выполнения синхронизации. Данный процесс может занять длительное время (например, при низкой скорости передачи данных по сети или при большом объеме передаваемых данных).
3. Перейдите в раздел **Досье** и убедитесь, что данные перенесены и отображены в списке.

Ниже представлены возможные статусы синхронизаций и их описание:

Статус синхронизации	Описание
Не синхронизировалось	Синхронизация сохранена и ожидает запуска позднее
Синхронизируется	Идет процесс синхронизации
Успешно	Синхронизация завершилась успешно
Прервана	Синхронизация остановлена пользователем. В статусе также указаны дата и время остановки
Ошибка Синхронизация проходит с ошибками	Данный статус может обозначать следующее: • введены некорректные логин, пароль, или адрес • истек срок лицензии на использование продукта Device Control • в ходе синхронизации произошла ошибка

Важно!

Синхронизация с Active Directory может создавать высокую нагрузку на сервера домена и сеть, поэтому настоятельно рекомендуется проводить первую синхронизацию с Active Directory в ночное время.

5.2.2 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.

5.3 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

5.3.1 Создание нового пользователя

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

1. Перейдите в раздел **Настройки** → **Настройки системы** → **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 пользователя см. "Настройки пароля").

Параметр	Обязательный параметр	Описание
Логин	Да	Имя учетной записи пользователя (о требованиях к логину см. "Настройки пароля"). Логин не зависит от верхнего или нижнего регистра
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").

5.3.2 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 системы** → **Пользователи**.
2. Нажмите + Создать.
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: учетную запись необходимо удалить, а затем добавить повторно.

5.3.3 Редактирование учетной записи

Для внесения изменений в учетную запись пользователя:

1. Перейдите в раздел **Настройки**  -> **Настройки системы** -> **Пользователи**.
2. Нажмите  напротив пользователя или на странице его профиля справа вверху.
3. Выберите **Редактировать**.
4. В открывшемся окне измените одну или несколько настроек. Доступны настройки, заданные при создании пользователя (см. "Создание нового пользователя").
5. Нажмите **Сохранить**. Новые настройки вступят в силу.

Чтобы назначить роль пользователю:

1. Перейдите в раздел **Настройки**  -> **Настройки системы** -> **Пользователи**.
2. Выберите пользователя.
3. В личной карточке пользователя перейдите на вкладку **Права доступа** и нажмите на ссылку Назначить роль.
4. В открывшемся окне в поле **Роль** выберите роль для назначения пользователю в раскрывающемся списке. 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 активные сессии пользователей**.
7. Подтвердите действие, нажав **Применить**. Пользователю будет назначена новая роль.

5.3.4 Просмотр профиля пользователя

На странице профиля представлена личная карточка пользователя со следующими данными:

1. Вкладка **Персональная информация** содержит:
   - 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.
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.

   Удаление или назначение новой роли осуществляется в окне редактирования учетной записи (см. "Редактирование учетной записи").

Действия пользователя:

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

5.3.5 Смена пароля пользователя

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

1. Перейдите в раздел **Настройки**  → **Настройки системы** → **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**.

5.3.6 Активация и деактивация пользователя

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

1. Перейдите в раздел **Настройки** → **Настройки системы** → **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 системы** → **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.

5.3.7 Удаление пользователя

Главный офицер может удалять учетные записи пользователей. Для этого:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **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.

5.4 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 системы** → **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

5.4.1 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 Device Control и настройкам:
   a. Отметьте ☑ в списке **Функции** пункт *Device Control → Устройства*, чтобы предоставить пользователю полный доступ к разделу **Устройства**.
   b. Отметьте в списке **Настройки**:
      - ☑ - если нужен полный доступ (просмотр и редактирование) к настройкам в разделе ⚙. 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, в фильтрах, отображениях на виджетах.

Если отметить Персону знаком ☐ при одновременном выборе других Персон, то эта роль предоставит пользователю доступ к ее событиям с участием разрешенных участников (☑), но без доступа к любым отображениям на виджетах и в фильтрах.

Примечание:

Главному офицеру безопасности необходимо внимательно следить за добавляемыми условиями, так как в случае использования различных элементов в роли может получиться не расширение, а сужение доступных данных из-за использования между разными 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.

Правильность добавления новых областей видимости и исключений следует проверять путем задания аналогичных условий в фильтре Персона, и далее проверять результаты на виджетах.

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

5.4.2 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 системы** → **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 системы** → **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.

5.4.3 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 системы** → **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 системы** → **Пользователи**.
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 системы** → **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.

5.5 Данные для анализа

Данные, получаемые Device Control, хранятся в партициях, которые доступны в разделе **Настройки** ⚙ → **Данные для анализа**.

В Центре расследований представлены данные от Device Monitor и Traffic Monitor.

> ⓘ **Примечание:**
>
> Доступ к партициям определяется ролью пользователя. Если в роли, назначенной пользователю, не разрешен доступ к продукту, партиции для пользователя будут недоступны.

5.5.1 Партиции Traffic Monitor

Device Control не получает и не использует партиции от Traffic Monitor.

5.5.2 Партиции Device Monitor

Статистические данные, полученные от Device Monitor, хранятся в партициях и сгруппированы по суткам. По одному типу событий отображается одна партиция за сутки. Если событий с данным типом за сутки не было зафиксировано, партиция за данные сутки не будет создана. Device Control использует партиции только с типом событий **Подключение/блокирование внешних устройств**.

Параметры партиции:

Параметр	Описание
Дата	Дата создания данных в партиции
Продукт	Продукты, которые используют данные партиции. **Примечание:** Столбец присутствует только при совместной установке. Если продукт установлен отдельно, столбец отсутствует.
Статистика	Тип события

Параметр	Описание
Статус	Статус партиции в Системе: • *Активная;* • *Архивированная;* • *Частично восстановленная* – архивная партиция с доступными пользователю новыми событиями
Размер	Объем, занимаемый партицией на диске.
Дата создания	Дата создания партиции. Заполняется автоматически
Дата архивирования	Дата архивирования партиции. Заполняется автоматически при создании архива с партицией
Дата удаления	Дата удаления партиции. Заполняется автоматически

Чтобы снизить объем обрабатываемых данных, доступны следующие действия:

- настройка хранения партиций по различным видам статистики;
- архивирование, удаление, восстановление партиций событий вручную.

5.5.3 Настройки хранения

События хранятся в партициях. В этом разделе вы можете настроить период времени, за который требуется хранить партиции. По истечении данного периода, в зависимости от настроек, партиции будут автоматически архивированы либо удалены. О ручном архивировании партиций см. в статье "Ручное архивирование, восстановление и удаление партиций".

> **Примечание:**
>
> Служебные операции выполняются в Системе в ночное время.

Чтобы настроить период хранения партиций:

1. Перейдите в **Настройки** → **Данные для анализа**.
2. Выберите вкладку **Device Monitor**.
3. Нажмите **Настройки хранения**.
4. В открывшемся диалоговом окне задайте настройки хранения для типа событий **Подключение/блокирование внешних устройств**:
   - за какой период хранить партиции;
   - через какое время необходимо удалять партиции;

> **Важно!**

Настройки хранения доступны для каждого типа событий Device Monitor, но Device Control использует только партиции с типом событий **Подключение/ блокирование внешних устройств**.

Данные архивированных партиций не доступны для анализа.

Если выбрать значение **За все время**, данные, собранные за все время, будут сохранены. При этом архивация и удаление будут недоступны.

5. Нажмите **Применить**.

Примечание:

Сроки архивирования и удаления партиций отсчитываются от даты создания партиции.

Пример:

Для созданной 01.01.2021 партиции применены настройки: срок хранения 1 месяц, удаление через 3 месяца. Партиция будет архивирована 01.02.2021, удалена 01.04.2021.

Архивирование и удаление партиций запускается в 3:00 по московскому времени.

Если требуется быстро освободить место на диске, удалите партиции вручную (см. "Ручное архивирование, восстановление и удаление партиций").

Если периоды архивирования не заданы, партиции автоматически архивируются через 12 недель. Автоматическое удаление партиций по умолчанию отключено.

Чтобы удалить все заархивированные партиции:

1. Нажмите **Настройки хранения**.
2. Включите **Удалять сразу** и нажмите **Применить**.

Примечание:

Удаление сразу применяется только для партиций, для которых был настроен период автоматического удаления.

Процесс удаления начнется немедленно. Это потребует значительных аппаратных ресурсов, поэтому работа в Системе должна быть приостановлена.

5.5.4 Ручное архивирование, восстановление и удаление партиций

Чтобы снизить объем данных в Системе, вы имеете возможность вручную архивировать партиции. Для этого:

1. Перейдите в раздел **Настройки**  -> **Данные для анализа**.
2. Выберите партиции, которые требуется архивировать .
3. Нажмите **Действие** и выберите **Архивировать партицию**.
4. Убедитесь, что статус партиции изменился на **Архивированная**. События из такой партиции не будут попадать в анализ.

Вы также можете использовать сочетание клавиши Ctrl+нажатие клавиши мыши, чтобы выделить партицию или несколько партиций последовательно или снять выделение.

Используйте Shift+нажатие клавиши мыши, чтобы одновременно выделить множество партиций или снять выделение. Для этого:

1. Выделите первую партицию в группе (чек-бокс или строку).
2. Удерживая клавишу Shift, выделите последнюю партицию в группе. Все партиции, находящиеся между ними, также будут выделены. Чтобы снять выделение, нажмите на любой из выделенных строк (или чек-боксе).

Архивирование возможно только для *активных* или *частично восстановленных* партиций.

Чтобы восстановить партицию:

1. Выберите партиции, которые требуется восстановить ☑.
2. Нажмите **Действие** и выберите **Восстановить партиции из архива**.
3. Убедитесь, что статус партиции изменился на **Активная**. События из такой партиции будут доступны для анализа. События из *частично восстановленных* партиций не будут попадать на анализ.

Восстановить можно только *архивированные* или *частично восстановленные* партиции.

Чтобы удалить партицию:

> **Важно!**
>
> При удалении партиций Device Monitor данные удаляются без возможности восстановления.

1. Выберите выберите одну или несколько партиций, которые требуется удалить ☑.
2. Нажмите **Действие** и выберите **Удалить партиции**.
3. Партиция будет удалена, события из такой партиции не будут доступны для анализа.

5.6 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.

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

Выполняется аудит следующих действий:

Пользователи	- вход в систему - выход из системы - создание - изменение - удаление - изменение пароля - блокировка пользователя
Роли	- создание - изменение - удаление
Интеграции	- создание - изменение - удаление - ручной запуск
Досье	- просмотр - создание - изменение - удаление - объединение

В разделе Аудит вы можете:

- Переместить колонки в таблице (при выгрузке отчета сохраняется порядок по умолчанию);
- Отсортировать содержимое колонок (по умолчанию события отсортированы от последних к наиболее ранним);
- При нажатии на пользователя – перейти в его карточку в разделе Пользователи;
- Добавить и удалить фильтры на панели;
- Отсортировать события, выбрав фильтры;
- Выгрузить отчет с событиями аудита (в формате .csv);
- Скопировать содержимое ячейки в таблице.

По умолчанию в разделе отображаются все фильтры:

- *Дата события*;
- *Действие в системе*;
- *Объект события*;
- *Пользователь*;
- *Тип объекта*;
- *Филиал*.

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

Вы можете отсортировать события:

- выбрав атрибут фильтра на панели над таблицей;
- выбрав нужный атрибут фильтр непосредственно в таблице.

Для этого:

1. Наведите курсор на содержимое ячейки.
2. 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 Excel необходимо поменять кодировку на utf-8. Подробнее об этом см. статью в базе знаний "Как сменить кодировку файла на UTF-8 в Excel".

5.7 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 их сроки 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

Параметр	Описание
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. До истечения указанного срока пароль необходимо сменить
Период неудачных попыток авторизации	Период (в минутах), в течение которого пользователь может вводить неверный пароль
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.

5.7.1 Требования к имени пользователя и учетной записи

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: "_", "-", "–", "."

5.8 Основные настройки

5.8.1 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**.

5.8.2 Отображение данных за период времени

Данная настройка в текущей версии Device Control не используется.

5.8.3 Управление токенами

Вы можете подключать компоненты к Системе с помощью токена. Для этого необходимо получить токен и указать его в подключаемом компоненте. В настоящей версии Системы поддерживается подключение сервера Device Monitor. Токен создается в момент установки Системы и представляет собой текстовую строку. Подробнее о настройке сервера Device Monitor см. "Документация для InfoWatch Device Monitor for Linux → InfoWatch Device Monitor. Руководство пользователя → Настройка Device Monitor → Серверы DM".

Вы можете просмотреть токен, а также скопировать его в буфер обмена, нажав  в поле **Токен для Device Monitor Server**.

Если токен был скомпрометирован, нажмите , чтобы сгенерировать новый.

Примечание:

Данные настройки в текущей версии продукта (Системы) не используются:

- **Токен для Data Storage User**

- **Использовать прокси-сервер**

5.8.4 Выбор цвета для уровня нарушения

Данная настройка в текущей версии Device Control не используется.

5.8.5 Создание шаблона имени

Вы можете создать шаблон отображения основной информации о персоне, используя атрибуты:

- имя;
- отчество;
- фамилия;
- полное имя;
- отображаемое имя;
- обязательное имя;
- инициалы;
- логин.

Чтобы создать шаблон:

1. Нажмите  и добавьте в поле нужные атрибуты. Можно добавить все указанные атрибуты.
2. Нажмите **Сохранить**. Через некоторое время изменения будут отображены в разделах Системы.

Чтобы изменить шаблон:

1. Удалите ненужные атрибуты из строки шаблона одним из способов:
   - вручную,
   - нажмите , чтобы очистить шаблон;
   - нажмите , чтобы шаблон принял первоначальный вид: *Фамилия Имя Отчество.*
2. Нажмите **Сохранить**.

Вид отображения будет распространяться на все персоны в Системе, полученные в результате синхронизации с Active Directory.

Примечание:

В данном поле также возможно добавить любой текст, расположив его перед, между или после выбранных параметров. Например, в компании есть полные тезки. Чтобы отличить их в Системе, можно добавить в отображаемое имя название отдела: Иванов Александр Иванович АХО, АХО Иванов Александр Иванович. Если отчества отличаются, можно добавить первую букву отчества после имени: Мария (А) Петрова.

5.8.6 Выбор часового пояса

Для правильного отображения статистики по событиям, произошедшим за выбранный период времени, рекомендуется установить в Системе значение часового пояса, соответствующее месту нахождения сервера Device Control. Для этого:

1. В поле **Часовой пояс** выберите из списка или введите часовую зону пребывания.
2. В правом верхнем углу нажмите **Сохранить**.

5.8.7 Чтобы настроить сбор статистической информации

Система сбора статистики накапливает и обобщает данные о работе пользователя в консоли. 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.

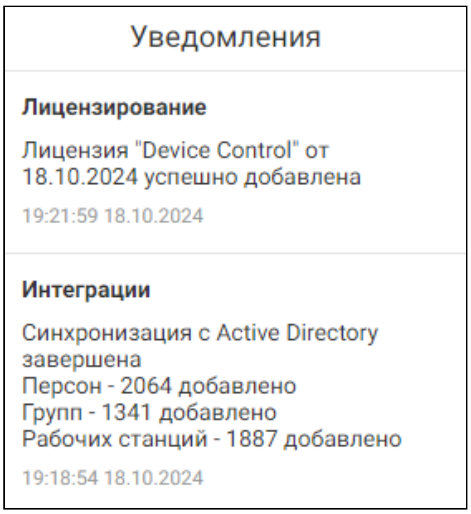
Сбор статистических данных включен по умолчанию. Чтобы отключить сбор данных, снимите галочку в поле **Включить** и нажмите **Сохранить**.

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

6 Уведомления

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

- статусе синхронизаций с различными источниками, которые инициировал пользователь;
- добавлении лицензии;
- удалении лицензии;
- возможной нехватке места на жестком диске;
- скором истечении срока действия пароля.



7 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.
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.