InfoWatch Data Access Tracker. Руководство администратора

12/01/2026

© 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 Лицензирование 8

5 Настройки Системы 9

5.1 Состояние Системы 9

5.1.1 Диагностические данные 11

5.2 Интеграции 11

5.2.1 Интеграция с Active Directory 12

Информация об интеграциях 14

5.2.2 Интеграция с InfoWatch Traffic Monitor 15

5.2.3 Редактирование и удаление интеграции 18

5.3 Пользователи 19

5.3.1 Создание нового пользователя 19

5.3.2 Добавление нового пользователя из LDAP 20

5.3.3 Редактирование учетной записи 21

5.3.4 Просмотр профиля пользователя 22

5.3.5 Смена пароля пользователя 22

5.3.6 Активация и деактивация пользователя 23

5.3.7 Удаление пользователя 23

5.4 Роли 23

5.4.1 Создание и настройка роли 24

5.4.2 Просмотр, редактирование и копирование роли пользователя 28

5.4.3 Снятие и удаление роли пользователя 29

5.5 Аудит 30

5.6 Настройки пароля 32

5.7 Основные настройки 34

5.8 Фильтры 36

5.9 Сервисы для уведомлений 37

5.10 Почтовые уведомления 39

6 Аудит инфраструктуры 42

6.1 Подключение к службе каталогов 42

6.2 Подключение к почтовому сервису ... 43
6.3 Запуск синхронизации ... 43
6.4 История синхронизаций ... 44
7 Системные уведомления ... 46
8 Добавление пользовательского сертификата ... 47

В настоящем руководстве вы сможете найти сведения по настройке и подготовке к работе InfoWatch Data Access Tracker (далее также DAT или Система). DAT – программное обеспечение, которое предоставляет результаты автоматического аудита службы каталогов и прав доступа к почтовым ящикам, а также позволяет отслеживать изменения прав доступа к объектам файловой системы.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, выполняющих настройку, поддержку, мониторинг и анализ работы Системы и т. п.

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

2 Комплект документов

В документацию по InfoWatch DAT входят:

- «InfoWatch Data Access Tracker. Руководство по установке». Содержит описание установки, обновления и удаления InfoWatch DAT.
- «InfoWatch Data Access Tracker. Руководство администратора». Содержит информацию по настройке и подготовке к работе InfoWatch DAT.
- «InfoWatch Data Access Tracker. Руководство пользователя». Содержит описание работы в InfoWatch DAT.

Сопутствующая документация по комплексу InfoWatch Traffic Monitor включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию Системы (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 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.

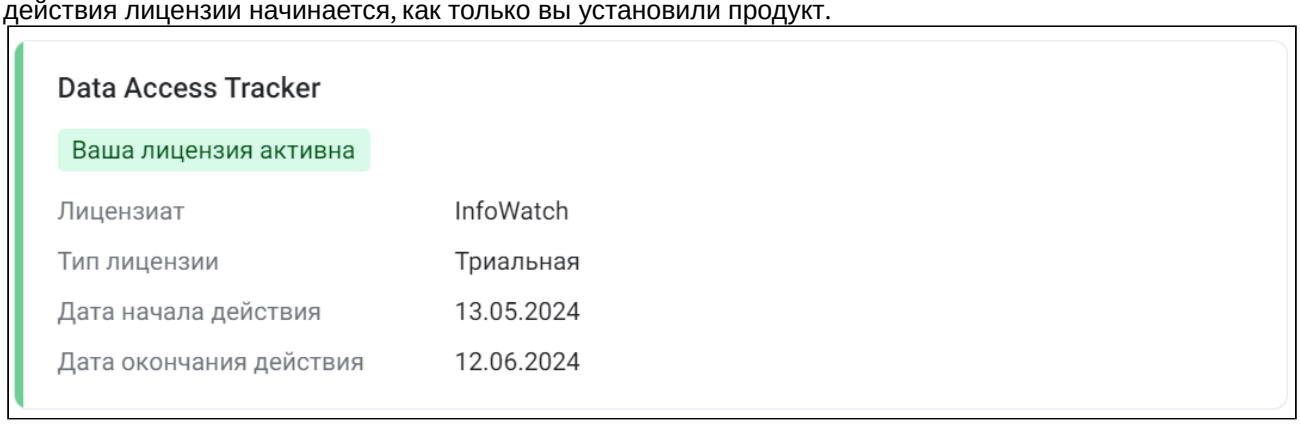
Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: www.infowatch.ru/services/support.

4 Лицензирование

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

Для подключения к контроллеру домена вам необходима активная лицензия в Системе.

По умолчанию в Систему добавлена пробная лицензия сроком на один месяц. Пробный период действия лицензии начинается, как только вы установили продукт.



Чтобы добавить лицензию:

1. Нажмите **+ Добавить**.
2. В открывшемся окне добавьте файл лицензии.

Чтобы удалить лицензию:

1. В углу плитки лицензии нажмите .
2. Нажмите **ОК**.

5 Настройки Системы

В разделе **Настройки** → **Настройки Системы** вы можете найти информацию по следующим настройкам:

- Состояние Системы
- Интеграции
- Пользователи
- Роли
- Аудит
- Настройки пароля
- Основные настройки
- Фильтры
- Сервисы для уведомлений
- Почтовые уведомления

> **Примечание:**
>
> Data Access Tracker не использует раздел **Данные для анализа**, т. к. не хранит и не использует данные в партициях.

5.1 Состояние Системы

Подсистема мониторинга проверяет работу 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** → **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
Последнее обновление состояния системы	Дата и время получения информации о статусе ноды
Версия ядра	Версия ядра ОС

Поле	Описание
Операционная система	ОС ноды продукта
Память	Общий и занимаемый размер оперативной памяти сервера продукта
ЦП	Загруженность центрального процессора сервера
Дисковое пространство (ClickHouse) *	Общее выделенное и занятое место на диске для хранения данных базы данных ClickHouse
Дисковое пространство (PostgreSQL) *	Общее выделенное и занятое место на диске для хранения данных базы данных 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 (Data Storage) *	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 отображены в списке.

Примечание:

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

Если ограничение превышено:

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

Чтобы снять это ограничение:

1. Перейдите в **Настройки** → **Состояние системы**.
2. Определите ноду и раздел, в котором осталось мало пространства.
3. Освободите раздел средствами ОС или продукта.

5.1.1 Диагностические данные

Все события мониторинга в Системе записываются в журнал.

Чтобы экспортировать диагностические данные, в правом верхнем углу нажмите **Экспорт диагностических данных**. В диагностические данные будут добавлены лог-файлы работающих служб со всех нод продукта. 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.

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 и формирования досье;
- InfoWatch Traffic Monitor – для загрузки в Систему событий, которые можно добавлять в расследования, а также для получения данных, используемых другими продуктами.

Источники используются в Системе для:

- формирования досье сотрудников;
- получения структуры компании;
- получения новых событий;
- получения справочников из источников, которые используются в событиях, таких как: политики безопасности, объекты защиты и другие.

В этом разделе вы можете:

- настроить интеграцию с Active Directory
- настроить интеграцию с InfoWatch Traffic Monitor

- редактировать или удалить интеграцию

Важно!

Интеграция с InfoWatch Traffic Monitor или Active Directory в разделе **Интеграции** не относится к функциональности продукта DAT.

О том, как настроить импорт данных с контроллера домена или почтового сервера, см. "Аудит инфраструктуры".

5.2.1 Интеграция с Active Directory

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:

Параметр	Описание
Имя интеграции	Название соединения, которое используется в Консоли
Филиал	Лейбл ноды продукта 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);

Параметр	Описание
	• 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 🔄.

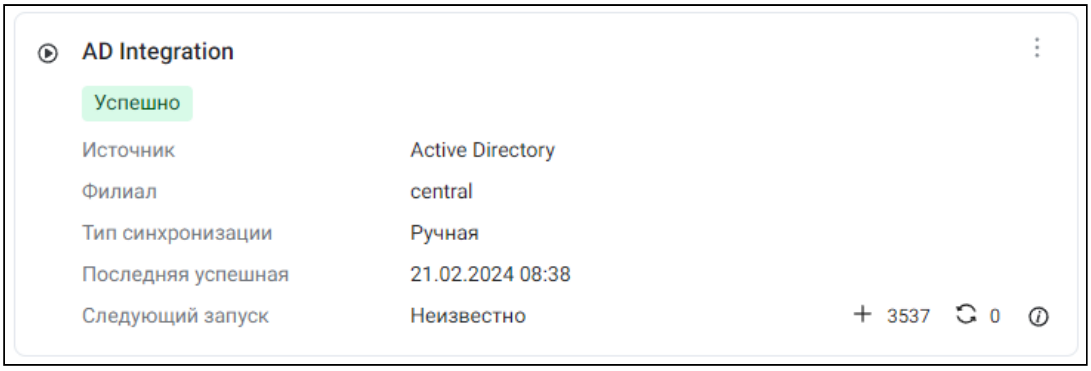
LDAP-запрос	Атрибуты фильтрации службы каталогов, являющиеся полным путем к указанному каталогу домена.
	Вы можете указать только один каталог в организационной структуре Active Directory. Для оптимизации поиска используйте отдельные уровни иерархии базы:
	`C – countryName`
	`O – organizationName`
	`OU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

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*. Пример настройки автоматической ночной синхронизации для экономии времени и минимизации нагрузки на сеть: • Периодичность: *Ежедневно*; • Время начала: *0:00*.
Периодичность	Как часто необходимо запускать синхронизацию : *Ежеминутно*, *Ежечасно*, *Ежедневно*, *Еженедельно*

Параметр	Описание
Повторение	День недели и/или время следующей синхронизации

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.



Чтобы запустить синхронизацию вручную, нажмите ▶ на панели интеграции. Процесс может занять длительное время.

Информация об интеграциях

Синхронизация возможна с несколькими LDAP-каталогами. Каждая интеграция отображается в отдельной панели.

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.

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 продукта; • в ходе синхронизации произошла ошибка.

5.2.2 Интеграция с InfoWatch Traffic Monitor

Интеграция с InfoWatch Traffic Monitor используется для загрузки в Центр расследований событий, а также персон, групп и рабочих станций. Добавление персон позволяет заводить досье и инициировать расследования. Подробнее см. документ "InfoWatch DAT. Руководство пользователя" статью "Создание, редактирование и удаление досье".

Примечание:

В случае, если в кластере Центра расследований установлен продукт Vision, интеграция с Traffic Monitor позволит Vision использовать информацию об объектах защиты и политиках.

Важно!

При планировании первичной синхронизации с InfoWatch Traffic Monitor стоит учитывать, что загрузка большого количества событий из базы данных может сильно уменьшить пропускную способность сети и общее быстродействие сервера и веб-консоли ТМ. Поэтому рекомендуется работы по синхронизации проводить в компании в нерабочее (ночное) время.

При первом входе в Систему список интеграций пустой.

Чтобы добавить новую синхронизацию с InfoWatch Traffic Monitor и запустить ее:

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. В правом верхнем углу нажмите **Добавить**.
4. Выберите **InfoWatch Traffic Monitor** и введите параметры:

Параметр	Описание
Имя интеграции	Название интеграции
Филиал	Лейбл ноды продукта для подключения к Active Directory
Адрес источника	Сетевой адрес сервера Traffic Monitor
Токен	Ключ, необходимый для получения данных от сервера Traffic Monitor (см. документ "*InfoWatch DAT. Руководство по установке*", статью "Установка лицензии и плагина Traffic Monitor")
Количество потоков загрузки	Количество рабочих потоков, через которые загружаются события и справочники из Traffic Monitor. Чем больше потоков, тем выше нагрузка на базу данных Traffic Monitor. Рекомендуется не задавать количество потоков больше, чем количество ядер процессора на сервере Traffic Monitor.
Интервал загрузки событий (мин.)	Данные событий, произошедших в Traffic Monitor за указанный интервал, будут загружаться в Систему одним потоком. По умолчанию: 120 минут. Вы можете уменьшить значение параметра, чтобы снизить нагрузку на ТМ при отправке данных.
Использовать параметры архивирования при загрузке	При включении этого параметра будут загружены события до текущей даты за последние N недель. Вы можете указать значение N в настройках архивирования. По умолчанию: 12 недель. Если вы не включите параметр, то будут загружены события за все время.
Не загружать данные LDAP	Включите параметр, если вы хотите загружать из Traffic Monitor только данные для анализа и при этом исключить загрузку персон, групп и рабочих станций. Если данные уже были добавлены в Центр расследований, включение параметра не удалит их.
Загружать детализацию по событиям	При использовании параметра Система загружает не только основные данные событий из Traffic Monitor, но также детальную информацию.
Отложенная загрузка	При включении этого параметра загрузка детализированных данных производится в указанное время.
Время отложенной загрузки	Время начала загрузки детализированных данных

Параметр	Описание
Синхронизация	Доступны два типа синхронизации: • *Ручная*; • *Автоматическая* по расписанию. Во втором варианте необходимо указать *Периодичность* и *Повторение*. Пример настройки автоматической ночной синхронизации для экономии времени и минимизации нагрузки на сеть: • Периодичность: *Ежедневно*; • Время начала: *0:00*.
Периодичность	Как часто необходимо запускать синхронизацию : *Ежеминутно*, *Ежечасно*, *Ежедневно*, *Еженедельно*
Повторение	День недели и/или время следующей синхронизации

Примечание:

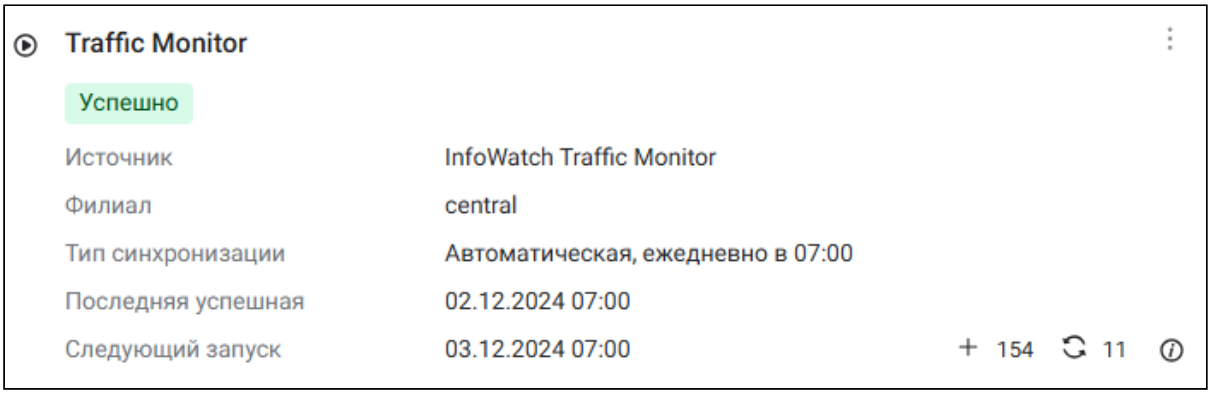
DAT не использует данные по событиям Traffic Monitor. Эту функциональность могут использовать другие продукты, установленные в кластере Центра расследований.

5. Нажмите **Проверить соединение**, чтобы проверить полноту и корректность введенных параметров, и дождитесь сообщения *Соединение успешно установлено*.
6. Нажмите:
   - **Сохранить** – при этом новая синхронизация будет ожидать запуска позднее в статусе *Не синхронизировалось*;
     или
   - **Сохранить и синхронизировать**, чтобы запустить процесс синхронизации.

Список интеграций с серверами Traffic Monitor 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.



Если необходимо провести еще одну синхронизацию с теми же параметрами:

1. Нажмите .
2. Дождитесь выполнения синхронизации. Процесс может занять продолжительное время (например, при низкой скорости передачи данных по сети или при большом объеме передаваемых данных).
3. После успешной синхронизации с Traffic Monitor перейдите в раздел **События** и убедитесь, что данные получены и отображаются в таблице.

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; • в Traffic Monitor отсутствует плагин/лицензия на экспорт данных в Центр расследований; • истек срок лицензии на использование продукта DAT; • в ходе синхронизации произошла ошибка.

5.2.3 Редактирование и удаление интеграции

Чтобы внести изменения в уже созданную интеграцию:

1. В правом верхнем углу нажмите и выберите **Редактировать**.
2. Внесите изменения.
3. Нажмите **Сохранить**.

Чтобы удалить интеграцию:

1. В правом верхнем углу нажмите .
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 (далее также 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. В правом верхнем углу нажмите **Создать**.
3. Выберите **Создать пользователя**.
4. Введите значения параметров согласно таблице:

Параметр	Описание
Фотография	Фотография пользователя
*Имя пользователя**	Имя нового пользователя. Должно содержать не менее четырех символов.
*Логин**	Имя учетной записи пользователя: • не зависит от регистра; • должна начинаться с буквы и не заканчиваться точкой; • может состоять из букв латинского алфавита, арабских цифр и содержать спецсимволы: "_", "-", "_", "."
*Пароль**	Пароль учетной записи (о требованиях к паролю см. "Настройки пароля")
*Подтверждение пароля**	Пароль учетной записи
Роль	Роль пользователя в Системе. Пользователю может быть присвоена только одна роль.
Язык консоли	Язык интерфейса для нового пользователя : *Русский* или *Английский*
Отображать только функции установленных продуктов	Переключатель, который скрывает от пользователя разделы и виджеты неустановленных продуктов
Контакты	Email-адрес. Можно добавить одно или несколько значений.
	Номер телефона. Можно добавить одно или несколько значений.

** – обязательный параметр.*

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. В правом верхнем углу 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 пользователя и нажмите **Добавить**.
7. Назначьте пользователю роль (см. подробнее "Редактирование учетной записи").

Пользователь будет добавлен в список пользователей Системы. Новый пользователь может входить в Систему с помощью доменных учетных данных. Логин учетной записи имеет вид: `domain\login` или `login@domain`. Логин учетной записи не чувствителен к регистру.

> **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. Откройте меню одним из способов:
   - в разделе **Пользователи** нажмите в строке пользователя;
   - откройте личную карточку пользователя и нажмите в правом верхнем углу.
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 поле **Роль** выберите роль из раскрывающегося списка. Пользователь без роли не сможет работать в Системе.
5. Нажмите **Сохранить**.
6. Чтобы изменения вступили в силу, пользователь с данной ролью должен выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессии

данного пользователя отметьте **Завершить активную сессию пользователей** в диалоговом окне.

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.

   Чтобы удалить 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

5.3.5 Смена пароля пользователя

Главный офицер может сменить пароль пользователю. Другие Офицеры безопасности могут менять пароли пользователей, если у них есть доступ к настройкам пользователей.

Чтобы сменить выданный 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** нажмите в строке пользователя;
   - откройте личную карточку пользователя и нажмите в правом верхнем углу.
3. Выберите **Сменить пароль**.
4. Введите новый пароль в полях *Новый пароль* и *Подтверждение пароля*.

   > **Важно!**
   >
   > Новый пароль должен удовлетворять настройкам безопасности. См. "Настройки пароля".

5. Нажмите **Сохранить**.

5.3.6 Активация и деактивация пользователя

Главный офицер может деактивировать выбранного пользователя. В этом случае пользователь не сможет выполнять никакие действия в Системе. Другие Офицеры безопасности могут деактивировать пользователей, если у них есть доступ к настройкам пользователей.

Чтобы заблокировать учетную запись:

1. Перейдите в раздел **Настройки** → **Настройки системы** → **Пользователи**.
2. Откройте меню одним из способов:
   - в разделе **Пользователи** нажмите в строке пользователя;
   - откройте личную карточку пользователя и нажмите в правом верхнем углу.
3. Выберите **Деактивировать**.

Чтобы разблокировать ранее заблокированную учетную запись, выполните шаги 1-2 и нажмите **Активировать**.

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** нажмите в строке пользователя;
   - откройте личную карточку пользователя и нажмите в правом верхнем углу.
3. Выберите **Удалить**.
4. В диалоговом 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 **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 пользовательские роли и две предустановленные:

- **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.
- **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 роль пользователю или снять роль.

Роль может быть назначена:

- при создании нового пользователя;
- при редактировании 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

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, необходимо:

- отредактировать роль;
- либо создать новую роль и назначить ее пользователю.

Если у всех пользователей разные компетенции, то необходимо создать столько ролей, сколько пользователей зарегистрировано 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. В списке **Функции** отметьте флажком , к каким из установленных продуктов и к каким их разделам нужно предоставить полный доступ пользователю. По умолчанию пользователь, для роли которого запрещен доступ к настройкам, функциям и данным, сможет авторизоваться в Системе и использовать функционал разделов **Главная** и **Персоны**.

Доступ к функциям Центра расследований

Доступ к *Событиям, Статистике нарушений* дает возможность использовать функционал разделов **События**, **Отчеты**, **Аналитика**, включая виджеты **Дата**, **Отправители**, **Получатели**, **Типы событий**.

Доступ к *Расследованиям* дает возможность работать в разделе **Расследования**.

Доступ к *Деталям событий* дает возможность переходить в Traffic Monitor для получения дополнительной информации о событии, а также использовать:

- виджеты **Типы файлов**, **Топ файлов**, **Краткий список событий**;
- фильтры **Имя файла**, **Наличие вложения**, **Тип файла**, **Тема письма**.

Доступ к *Деталям нарушений* дает возможность выгружать данные о деталях в отчет, использовать:

- виджеты **Нарушения**, **Уровень нарушений**, **Вердикт**, **Статистика**, **Решения пользователя**, включая соответствующие им фильтры;
- маркировку событий и раскраску виджетов по уровню нарушений.

Доступ к *Политикам, Объектам защиты и Периметрам* дает возможность использовать:

- виджеты **Политики**, **Объекты защиты**, **Статистика**, включая соответствующие им фильтры;
- дополнительные колонки в разделе **События**.

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

Доступ к функциям продуктов

Data Access Tracker

Доступ к *Инфраструктуре* дает возможность использовать вкладки в разделе **Инфраструктура**:

- виджеты продукта Data Access Tracker на вкладке **Сводка** (а также на **Главной** странице в дашбордах);
- отчеты о состоянии и изменениях объектов службы каталогов на вкладках **Аудит службы каталогов** и **Изменения групп**;
- отчеты о доступе к почтовым ящикам на вкладке **Права на почтовые ящики**;
- отчеты об изменениях прав доступа к папкам и файлам на вкладке **Изменения прав на файлы и папки**.

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 **Главной** странице;
- функционал отчетов в разделах **Аналитика**, **Мониторинг** и **Отчеты**.

Доступ к *Снимкам экрана* дает возможность:

- отображать снимки экрана в разделах **Мониторинг** и **Персоны**;
- отображать и фильтровать события, связанные со снимками.

Доступ к *Аудиозаписям* дает возможность:

- отображать данные по аудиозаписям в разделах **Мониторинг** и **Персоны**;
- отображать и фильтровать события, связанные с аудиозаписями.

Доступ к *Видеозаписям* дает возможность:

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

Доступ к *Наблюдению* дает возможность использовать функционал наблюдения и таймлайн в разделах **Мониторинг** и **Персоны**.

Доступ к *Онлайн наблюдению* дает возможность:

- просматривать экран персоны;
- прослушивать звуковое окружение персоны;
- блокировать сессию персоны;
- запрашивать список запущенных процессов на компьютере персоны.

Доступ к *Вводимому тексту* дает возможность:

- отображать введенный текст в связанных событиях;
- фильтровать события 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 Discovery

Доступ к *Хранению файлов* дает возможность:

- работать **в разделе Хранение файлов**:
  - на вкладке **Задачи** создавать и запускать задачи сканирования;
  - на вкладке **Информация о файлах** – анализировать результаты сканирования;
- работать в разделе **Персоны** в досье персон на вкладке **Хранение файлов**, которая включает в себя подразделы:
  - **Владелец файлов**;
  - **Доступные файлы**;
- выгружать отчеты с информацией из подразделов **Владелец файлов** и **Доступные файлы** досье персоны, а также из вкладки **Информация о файлах** раздела **Хранение файлов**.

Prediction

Доступ к *Досье, Рейтинг* дает возможность:

- работать с рейтингом персон в разделе **Риски**;
- работать в досье персоны на вкладках **Группы рисков** и **Карта паттернов**;
- отображать виджеты Prediction на **Главной** странице в дашбордах;
- выгружать отчеты в разделе **Риски** и на вкладке **Группы рисков** в досье персоны.

Vision

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

Доступ к Статистике нарушений дает возможность работать:

- со статистикой в разделах **Аналитика** и **Персоны**, выгружать отчеты;
- с виджетами Vision на **Главной** странице;
- с 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 требуется доступ на просмотр и редактирование к настройкам в разделе. По умолчанию доступ запрещен;
   - 👁 – если необходимы права только на просмотр;
   - ☐ – если требуется 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 для пользователя доступ к данным. 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 разрешенных участников (☑), но без доступа к любым отображениям на Графе связей, виджетах и в Едином фильтре.

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 в Traffic Monitor 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 Едином фильтре, 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 диалоговом окне в поле **Пользователи** выберите пользователя из выпадающего списка.
   c. Нажмите **Выдать**. Роль будет назначена данному пользователю.
9. После внесения всех настроек нажмите **Применить**.
10. Чтобы изменения вступили в силу, 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**, 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** → **Пользователи**.
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 имеющуюся 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 диалоговом 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;

Кроме того, будут указаны текущие дата и время в поле **Дата создания**.

Список пользователей, которым выдана роль, не копируется.

5.4.3 Снятие и удаление роли пользователя

Пользователь не может иметь несколько ролей одновременно. Если вы хотите выдать пользователю новую роль, вам необходимо снять действующую. Это можно сделать в карточке роли или в карточке пользователя:

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**.

> **Примечание:**
>
> Чтобы изменения вступили в силу, пользователь должен выйти из Системы. Для принудительного завершения сессии данного пользователя, в открывшемся диалоговом окне отметьте  **Завершить активную сессию пользователя**.

6. Подтвердите действие, нажав **Применить**. У данного пользователя роль будет снята. После этого можно назначить ему другую роль.

> **Примечание:**
>
> 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**.

> **Примечание:**
>
> Чтобы изменения вступили в силу, пользователи с данной ролью должны выйти из Системы. Для принудительного завершения сессий данных пользователей, в открывшемся диалоговом окне отметьте  **Завершить активные сессии пользователей**.

4. Подтвердите действие, нажав **Удалить**. Если роль была назначена пользователям, она будет снята для них и удалена из списка ролей. После этого можно назначить пользователям другую роль.

5.5 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**, который совершил действие;
- **Действие в системе**, которое было выполнено над объектом;
- **Тип объекта**: пользователь, интеграция, досье, роль;
- **Объект события**, над которым было совершено действие (например, роль или интеграция);
- **Название филиала**, где было зафиксировано событие аудита;
- **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:

- выгрузить отчет с событиями аудита в формате CSV;
- переместить колонки в таблице;
- отсортировать содержимое колонок (по умолчанию события отсортированы от последних к более ранним);
- при нажатии на пользователя – перейти в его карточку в разделе **Пользователи**;
- 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*.

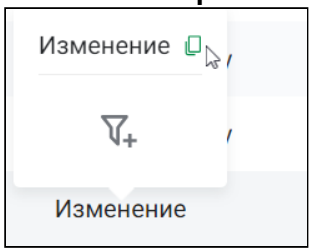
Для управления фильтрами воспользуйтесь кнопкой . Установите флаг , чтобы добавить фильтр на панель, или снимите флаг, чтобы удалить фильтр из набора.

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".

5.6 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 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 присутствие перечисленных букв в пароле; ☐ – допускается пароль без букв.
Цифры	Арабские цифры, которые используются для составления пароля. Можно установить: ☑ – обязательно присутствие перечисленных цифр в пароле; ☐ – допускается пароль без цифр.
Специальные символы	Перечень спецсимволов, которые могут быть в пароле. Можно установить: ☑ – обязательно присутствие перечисленных спецсимволов в пароле; ☐ – 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)

Примечание:

При необходимости вы можете изменить обязательные наборы букв, цифр и спецсимволов в соответствующих полях.

3. Нажмите **Сохранить**, чтобы активировать новые значения параметров. Если необходимо вернуться к прежним настройкам, нажмите **Сбросить настройки**.

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

5.7 Основные настройки

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

- задать настройки сессии;
- настроить период, за который отображаются данные;
- управлять токенами;
- создать шаблон имени;
- управлять сбором статистических данных.

> **Примечание:**
>
> Данные настройки в текущей версии продукта (Системы) не поддерживаются:
>
> - **Токен для Data Storage User**;
> - **Использовать прокси-сервер**.

Настройки сессии

Вы можете установить время жизни сессии – время ожидания активности пользователя в Консоли. Если в течение указанного отрезка времени Система не зафиксирует активность (движение мыши и нажатие клавиш на клавиатуре), произойдет автоматический выход из Консоли. В этом случае для продолжения работы пользователю необходимо заново авторизоваться в Системе.

Чтобы задать настройки:

1. В поле **Время жизни сессии** установите необходимое значение (в минутах, любое число менее 100000).
2. В правом верхнем углу нажмите **Сохранить**.

Отображение данных за период времени

Настройка позволяет задать период для атрибута Единого фильтра **Дата**. В выпадающем меню выберите нужный параметр:

- *любая дата*;
- *последние сутки*;
- *текущий день*;
- *последние 3 дня*;
- *последние 7 дней*;
- *последние 30 дней*;
- *текущий месяц*;
- *прошлый месяц*.

Период по умолчанию – 30 дней.

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. документацию для InfoWatch Device Monitor (сервер Windows): "*InfoWatch Device Monitor. Руководство пользователя*", разделы "Работа в Консоли Управления Device Monitor. Общие настройки Системы. Настройки сервера Device Monitor", статья "Соединение с сервером Платформы".

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.

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 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 в поле шаблона;
   - 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.

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**.

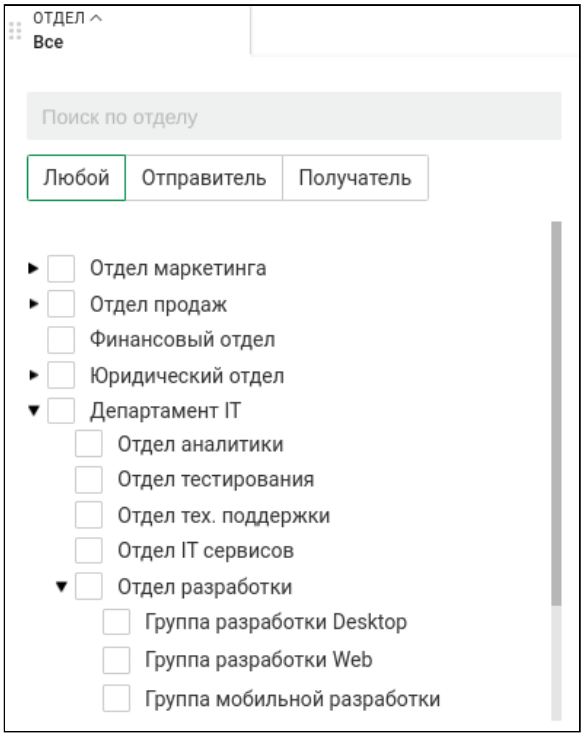
> **Примечание:**
>
> Система сбора статистики не накапливает, не анализирует и не передает персональные данные. Все ФИО пользователей и сотрудников заменяются на внутрисистемные ID-номера.

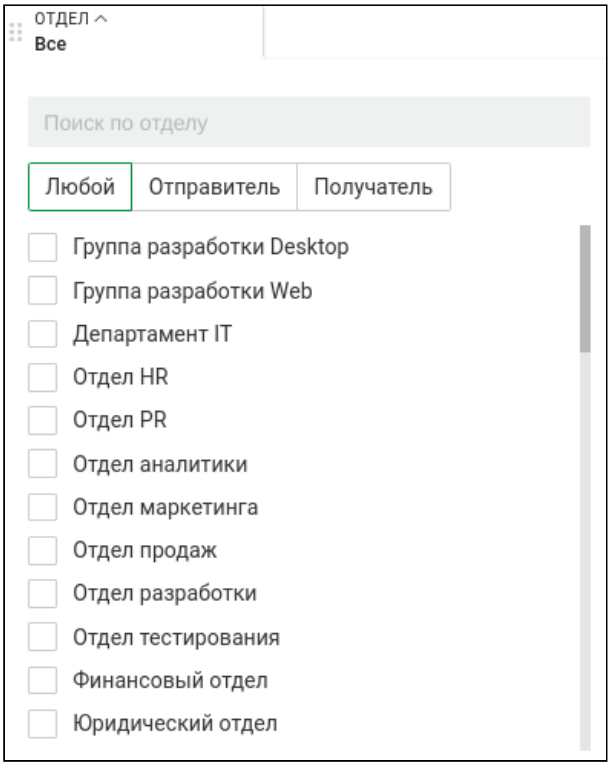
> **Примечание:**
>
> Остальные настройки этого раздела используются другими продуктами Центра расследований.

5.8 Фильтры

При синхронизации со службой каталогов Система получает список отделов. Вы можете настроить отображение этого списка в Едином фильтре:

Плоский – все отделы отображаются в списке на одном уровне	*Иерархический* – отделы отображаются в виде дерева





Если необходимо загружать отделы без сотрудников, установите ☑ **Загружать пустые отделы**.

Тип контактов

Вы можете создать список доменов, контакты с которыми будут относиться к внутренним контактам.

Чтобы добавить внутренний домен:

1. Нажмите **+ Добавить домен**.
2. Введите имя домена в формате ***companyname.ru***. Дальнейшие контакты с этим доменом Система будет рассматривать как внутренние.

При необходимости добавьте другие домены.

Чтобы удалить внутренний домен:

1. Нажмите 🗑 напротив имени домена.
2. В открывшемся окне нажмите **Ок**.

Чтобы новые настройки вступили в силу, нажмите **Сохранить**, а затем **Да**.

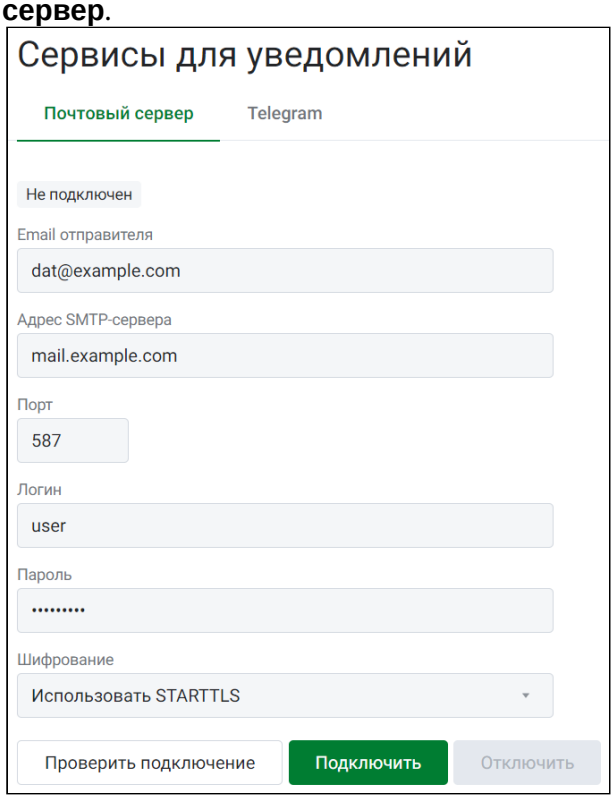
5.9 Сервисы для уведомлений

Вы можете настроить отправку на почту:

- уведомлений об изменениях в группах. Подробнее см. "Почтовые уведомления".
- XLSX-файлов с отчетами, представленными в разделе **Инфраструктура**. Подробнее см. документ *"InfoWatch Data Access Tracker. Руководство пользователя"*, статья "Раздел "Инфраструктура" → "Выгрузка отчетов".

Для этого настройте подключение к почтовому серверу:

1. Перейдите в раздел **Настройки** → **Сервисы для уведомлений** → **Почтовый сервер**.



2. Укажите параметры подключения:

Параметр	Описание
Email отправителя	Адрес электронной почты, от имени которого будут приходить уведомления
Адрес SMTP-сервера	Адрес почтового сервера, работающего по протоколу SMTP. Укажите доменное имя или IP-адрес
Порт	Порт подключения к почтовому серверу
Логин	Имя учетной записи, имеющей доступ к почтовому серверу
Пароль	Пароль учетной записи, имеющей доступ к почтовому серверу
Шифрование	Укажите протокол шифрования, который будет использован при подключении к почтовому серверу. Доступные протоколы: • STARTTLS • TLS

> **Примечание:**
>
> Все поля обязательны для заполнения.

3. Для проверки доступности сервера нажмите **Проверить подключение**.
4. Если проверка подключения прошла успешно, нажмите **Подключить**.

Чтобы изменить параметры подключения или подключиться к другому почтовому серверу, внесите изменения и нажмите **Обновить**.

Чтобы разорвать соединение с почтовым сервером, нажмите **Отключить**.

> **Примечание:**
>
> Работа с функциональностью на вкладке **Telegram** не поддерживается в Data Access Tracker версии 2.1.

5.10 Почтовые уведомления

Вы можете настроить отправку уведомлений об изменениях в группах службы каталогов, в том числе об изменениях состава привилегированных групп.

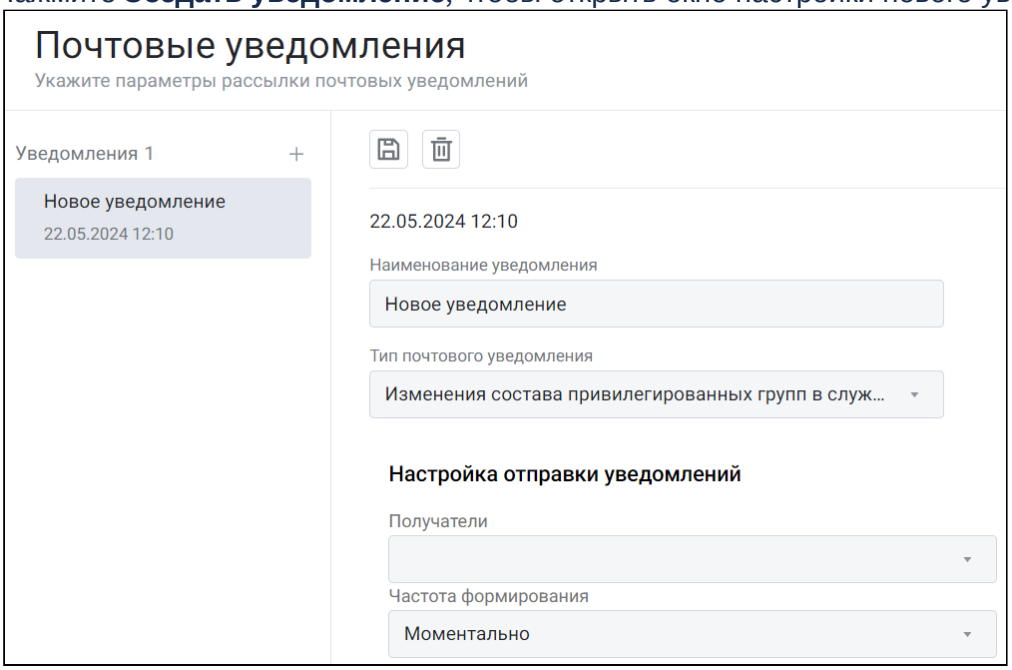
> **Важно!**
>
> Для отправки почтовых уведомлений обязательно настройте подключение к почтовому серверу. Подробнее см. "Сервисы для уведомлений".

> **Примечание:**
>
> Электронные письма с уведомлениями не содержат отчетов. Чтобы получать XLSX-файлы с отчетами, сгенерированными продуктом DAT, настройте отправку отчетов по расписанию. Подробнее см. документ *"InfoWatch Data Access Tracker. Руководство пользователя"*, статья "Раздел "Инфраструктура" → "Выгрузка отчетов".

Для создания рассылки почтовых уведомлений:

1. Перейдите в раздел **Настройки** → **Почтовые уведомления**.

2. Нажмите **Создать уведомление**, чтобы открыть окно настройки нового уведомления:



3. Укажите **Наименование уведомления**.
4. Выберите **Тип почтового уведомления**:
   - *Изменения состава привилегированных групп в службе каталогов* – чтобы получать моментальные уведомления при изменениях в привилегированных группах;
   - *Изменения в группах службы каталогов домена за сутки* – чтобы получать ежедневный отчет об изменениях в группах за сутки.
5. В поле **Получатели** нажмите , чтобы открыть список доступных пользователей, и укажите тех, кому должны приходить уведомления.

> **Примечание:**
>
> Для выбора доступны только пользователи, в контактах которых указан адрес электронной почты.

6. Частота отправки уведомлений задана автоматически:
   a. *Моментально* для уведомлений об изменениях состава привилегированных групп;
   b. *Ежедневно* для уведомлений об изменениях в группах службы каталогов домена за сутки.
7. Если вы выбрали тип отчета *Изменения в группах службы каталогов домена за сутки*, также укажите время отправки ежедневного отчета. Время отправки по умолчанию – 7:00.
8. Чтобы сохранить рассылку уведомлений, нажмите вверху.

Вы можете отредактировать или удалить имеющуюся рассылку почтовых уведомлений.

Чтобы отредактировать рассылку:

1. Выберите уведомление, которое хотите отредактировать.
2. Внесите необходимые изменения.

3. Нажмите .

Чтобы удалить рассылку, выберите ее и нажмите  вверху.

6 Аудит инфраструктуры

В разделе **Аудит инфраструктуры** вы можете настроить соединение со службой каталогов и почтовым сервисом, запустить синхронизацию, а также просмотреть запущенные и завершенные синхронизации.

> **Важно!**
>
> Перед подключением контроллера домена и почтового сервера убедитесь, что на них выполнены настройки для взаимодействия с DAT. Подробнее см. документ *«InfoWatch Data Access Tracker. Руководство по установке»*, статьи "Настройка контроллера домена в Active Directory", "Настройка учетной записи в Active Directory", "Настройка сервера MS Exchange".

6.1 Подключение к службе каталогов

Чтобы добавить интеграцию со службой каталогов:

1. Перейдите в раздел **Настройки** → **Настройки продуктов** → **Аудит инфраструктуры**.
2. На вкладке **Служба каталогов** выберите один из способов:
   - **Добавить контроллер вручную**:
     a. Укажите значения всех параметров:
        - *Адрес контроллера* – IP-адрес или доменное имя сервера контроллера домена;
        - *Логин* для доступа к серверу (пользователь должен иметь права на чтение каталога);
        - *Пароль* для доступа к серверу.
   - **Определить автоматически**:
     a. В окне **Автоматическое определение контроллеров** укажите значения параметров:
        - *Домен* – имя домена;
        - *IP-адрес сервера DNS* (необязательный параметр) – явное указание адреса DNS-сервера в случае некорректных настроек по умолчанию.
     b. Нажмите **Найти**. Начнется поиск контроллеров внутри домена, и отобразится список адресов.
     c. Ознакомьтесь со списком адресов и при необходимости удалите лишние, нажав ✕ справа от адреса.
     d. Нажмите **Добавить контроллеры**.
     e. В разделе **Настройки подключения к контроллерам доменов** укажите параметры подключения для каждого сервера:
        - *Логин* для доступа к серверу (пользователь должен иметь права на чтение каталога);
        - *Пароль* для доступа к серверу.
3. В правом верхнем углу нажмите **Сохранить**.
4. Для подключения к еще одному контроллеру нажмите **+ Добавить контроллер**, укажите его параметры и нажмите **Сохранить**.

Важно!

Подключите все контроллеры домена, с которых необходимо отправлять в DAT события из журналов безопасности системы. Синхронизация будет выполняться со всеми добавленными серверами одновременно.

Чтобы удалить подключение, на вкладке **Служба каталогов** нажмите  справа от строки, которую вы хотите удалить.

6.2 Подключение к почтовому сервису

Чтобы добавить интеграцию с почтовым сервисом:

1. Перейдите в раздел **Настройки**  → **Настройки продуктов** → **Аудит инфраструктуры**.
2. На вкладке **Почтовый сервис** укажите значения параметров:
   - *Адрес контроллера* – IP-адрес или доменное имя сервера контроллера домена;
   - *Адрес почтового сервера* – доменное имя почтового сервера;
   - *Логин* для доступа к серверу (пользователь должен быть добавлен в группу *View-Only Organization Management*);
   - *Пароль* для доступа к серверу.
3. В правом верхнем углу нажмите **Сохранить**.

Чтобы удалить подключение, на вкладке **Почтовый сервис** нажмите  справа от строки, которую вы хотите удалить.

6.3 Запуск синхронизации

Синхронизация выполняется одновременно для всех настроенных подключений. Например, если вы добавили три контроллера домена и почтовый сервер, синхронизация будет запущена для всех четырех подключений. Вы можете запустить синхронизацию вручную или настроить автоматическую.

Чтобы запустить синхронизацию вручную:

1. Перейдите на вкладку **История синхронизаций**;
2. В правом верхнем углу нажмите **Запустить синхронизацию вручную**.

Чтобы настроить автоматическую синхронизацию по расписанию:

1. Перейдите на вкладку **Автоматическая синхронизация**.
2. Нажмите на переключатель .
3. Из выпадающего списка **Период синхронизации** выберите значение интервала: *5*, *15*, *30* или *60* минут.
4. В правом верхнем углу нажмите **Сохранить**. Под списком отобразится время запуска следующей синхронизации.

Чтобы отключить автоматическую синхронизацию:

1. На вкладке **Автоматическая синхронизация** нажмите на переключатель .
2. В правом верхнем углу нажмите **Сохранить**.

Чтобы изменить интервал автоматической синхронизации:

1. На вкладке **Автоматическая синхронизация** выберите новое значение из выпадающего списка **Период синхронизации**.
2. В правом верхнем углу нажмите **Сохранить**.

6.4 История синхронизаций

Вкладка **История синхронизаций** содержит список всех запущенных и завершенных синхронизаций. Для них отображены:

- *Дата и время запуска*;
- *Дата и время завершения*;
- *Статус*: *Завершено*, *В процессе*, *Ошибка*, *Завершено с ошибками*;
- *Тип* загруженных записей: *События аудита*, *Каталог Active Directory*, *Доступ к почте Exchange*;
-  – детальная информация:
  - для типа *События аудита* – о количестве записей о событиях, загруженных в ходе данной синхронизации с указанными серверами, например:

Контроллер домена	Загруженные записи
10.60.44.35	13
10.60.44.174	7

  - для типа *Каталог Active Directory* – о количестве обнаруженных/удаленных при синхронизации учетных записей пользователей и компьютеров, а также подразделений (OU), например:

Контроллер домена	Пользователи		Компьютеры		Подразделения (OU)	
	Обнаружено	Удалено	Обнаружено	Удалено	Обнаружено	Удалено
10.60.44.174	102	0	16	0	38	0

  - для типа *Доступ к почте Exchange* – о количестве обнаруженных/удаленных при синхронизации записях о почтовых ящиках и правах доступа, например:

Контроллер домена	Почтовые ящики		Права доступа	
	Обнаружено	Удалено	Обнаружено	Удалено
10.60.3.63	57	0	1464	0

По умолчанию строки более поздних синхронизаций отображаются в верхних строках таблицы. Данные в столбцах можно отсортировать по возрастанию/убыванию. Для столбцов, в которых данные отсортированы, справа от названия отображается значок  или .

Чтобы отсортировать строки:

1. Нажмите на название столбца, по значениям которого вы хотите отсортировать строки.
2. Кликом мыши по значку отрегулируйте способ сортировки:
   - по возрастанию 
     или
   - по убыванию 

Строки в таблице будут отсортированы по значениям этого столбца:

Дата и время завершения	Тип	Статус	Дата и время запуска
22.05.2024 09:03:55	События аудита	Завершено	22.05.2024 09:01:32
22.05.2024 09:01:35	Каталог Active Directory	Завершено	22.05.2024 09:01:32
22.05.2024 08:43:34	События аудита	Завершено	22.05.2024 08:41:10
22.05.2024 08:41:14	Каталог Active Directory	Завершено	22.05.2024 08:41:10
20.05.2024 10:33:16	События аудита	Завершено	20.05.2024 10:22:54

Чтобы отсортировать значения по двум и более столбцам:

1. Отсортируйте значения по первому столбцу.

   > **Примечание:**
   >
   > Приоритет столбцов определяется слева направо. Вы можете менять порядок столбцов путем перетаскивания.

2. На клавиатуре зажмите **Ctrl** и отсортируйте строки в другом столбце.

> **Пример:**
>
> Строки в таблице отсортированы по приоритетному (т. к. он расположен левее) столбцу **Тип**. Записи во втором и третьем столбцах отсортированы относительно первого столбца.
>
> | Тип | Статус | Дата и время завершения |
> |---|---|---|
> | События аудита | В процессе | |
> | События аудита | Завершено | 14.05.2024 14:25:53 |
> | События аудита | Завершено | 20.05.2024 10:33:16 |
> | События аудита | Завершено | 22.05.2024 08:43:34 |
> | Каталог Active Directory | Завершено | 14.05.2024 14:23:35 |
> | Каталог Active Directory | Завершено | 20.05.2024 10:22:57 |

Чтобы отменить сортировку:

1. Наведите курсор на название столбца.
2. Нажмите на появившийся значок .
3. Выберите *Сбросить столбцы*.

7 Системные уведомления

Чтобы ознакомиться с системными уведомлениями Центра расследований, нажмите .



Уведомления сообщают о:

- статусе инициированных пользователем синхронизаций с различными источниками;
- добавлении лицензии;
- удалении лицензии;
- количестве досье, загруженных в Систему на данный момент;
- возможной нехватке места на жестком диске;
- скором истечении срока действия пароля.

8 Добавление пользовательского сертификата

Чтобы не допустить несанкционированный доступ к Системе и повысить защищенность канала передачи данных, можно добавить новый пользовательский сертификат для web-службы. Вы можете сделать это в любой момент использования Системы через командную строку. Для этого:

1. Разместите на диске два файла в формате PEM:
   - файл с сертификатом (например, `test.crt`);
   - файл с закрытым ключом (например, `test.key`).
2. В директории, содержащей `setup.py`, выполните команду от имени пользователя с правами `root`. При этом укажите полное имя файлов с сертификатом и закрытым ключом:

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

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