InfoWatch Data Access Tracker. Руководство пользователя

12/01/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 6

2 Комплект документов 7

3 Техническая поддержка пользователей 8

4 Обзор 9

5 Интерфейс Центра расследований 10

6 Главная страница 13

6.1 Дашборды и виджеты 13

6.1.1 Дашборды 13

6.1.2 Виджеты 14

7 Единый фильтр 18

7.1 Фильтры 18

7.2 Работа с Единым фильтром 26

7.2.1 Активация фильтра 26

7.2.2 Добавление и удаление фильтров 26

7.2.3 Значения фильтров 27

7.2.4 Сохранение и загрузка наборов фильтров 28

8 Раздел "События" 30

8.1 Добавление событий в расследование 32

8.2 Просмотр и выгрузка данных событий 33

8.2.1 Просмотр используемых контактов 33

8.2.2 Просмотр данных в столбце 33

8.2.3 Фильтрация данных 34

8.2.4 Выгрузка данных события 34

8.3 Фильтрация событий по персонам и контактам 35

9 Раздел "Аналитика" 37

9.1 Виджеты статистики 37

9.2 Формирование, выгрузка и печать отчетов с данными статистики 39

10 Раздел "Инфраструктура" 41

10.1 Вкладка "Сводка" 41

10.1.1 Виджеты раздела "Инфраструктура" ... 43
10.2 Вкладка "Аудит службы каталогов" ... 45
10.2.1 Отчеты ... 45
10.3 Вкладка "Изменения групп" ... 49
10.4 Вкладка "Права на почтовые ящики" ... 50
10.4.1 Отчеты ... 51
10.5 Вкладка "Изменения прав на файлы и папки" ... 52
10.6 Просмотр отчетов ... 53
10.6.1 Скрытие меню вкладки ... 53
10.6.2 Полноэкранный режим ... 53
10.6.3 Детали события ... 53
10.6.4 Статус события ... 54
10.6.5 Группировка и сортировка записей ... 55
Сортировка записей ... 55
Группировка записей ... 56
10.7 Выгрузка отчетов ... 58
10.7.1 Отправка отчетов по расписанию ... 59
11 Раздел "Персоны" ... 61
11.1 Вкладка "Персональная информация" ... 61
11.2 Просмотр досье персоны ... 62
11.3 Создание, редактирование и удаление досье ... 64
11.4 Объединение досье ... 64
11.5 Добавление контактов персоны ... 64
11.6 Изменение руководителя персоны ... 65
11.7 Выгрузка статистики в досье персоны ... 65
12 Раздел "Расследования" ... 67
12.1 Создание и архивирование расследования ... 68
12.2 Добавление материалов в расследование ... 68
12.3 Совместное проведение расследования ... 69
12.4 Редактирование, выгрузка, печать и удаление расследования ... 69
13 Раздел "Отчеты" ... 71
13.1 Задачи на регулярную отправку ... 71
13.2 Архив отчетов ... 71
14 Пользовательское лицензионное соглашение ... 73

15 Глоссарий 78

В настоящем руководстве вы сможете найти сведения по работе и решению задач в 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, работающих с Системой. К работе с Системой относится: общая настройка перед использованием, анализ данных, проведение расследований и т. п.

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы 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 Обзор

Центр расследований представляет собой веб-консоль для работы с продуктами InfoWatch. У пользователя есть возможность установить как один, так и несколько продуктов. Весь набор установленных продуктов позволяет получать наиболее полную информацию о нарушениях, персонах, рисках и т.д.

Продукт DAT предоставляет результаты автоматического аудита службы каталогов и прав доступа к почтовым ящикам, а также позволяет отслеживать изменения прав доступа к объектам файловой системы. С помощью продукта вы можете выявить потенциальные угрозы информационной безопасности компании, такие как:

- изменения в составе привилегированных групп;
- длительное отсутствие активности учетных записей;
- неудачные попытки входа в систему;
- доступ пользователя к нескольким почтовым ящикам;
- отсутствие для учетной записи требования периодически менять пароль;
- отключение блокировки учетной записи при неудачных попытках входа;
- изменения прав доступа к папкам и файлам.

Кроме того, вы можете настроить отправку Офицеру безопасности почтовых уведомлений об изменениях групп службы каталогов домена.

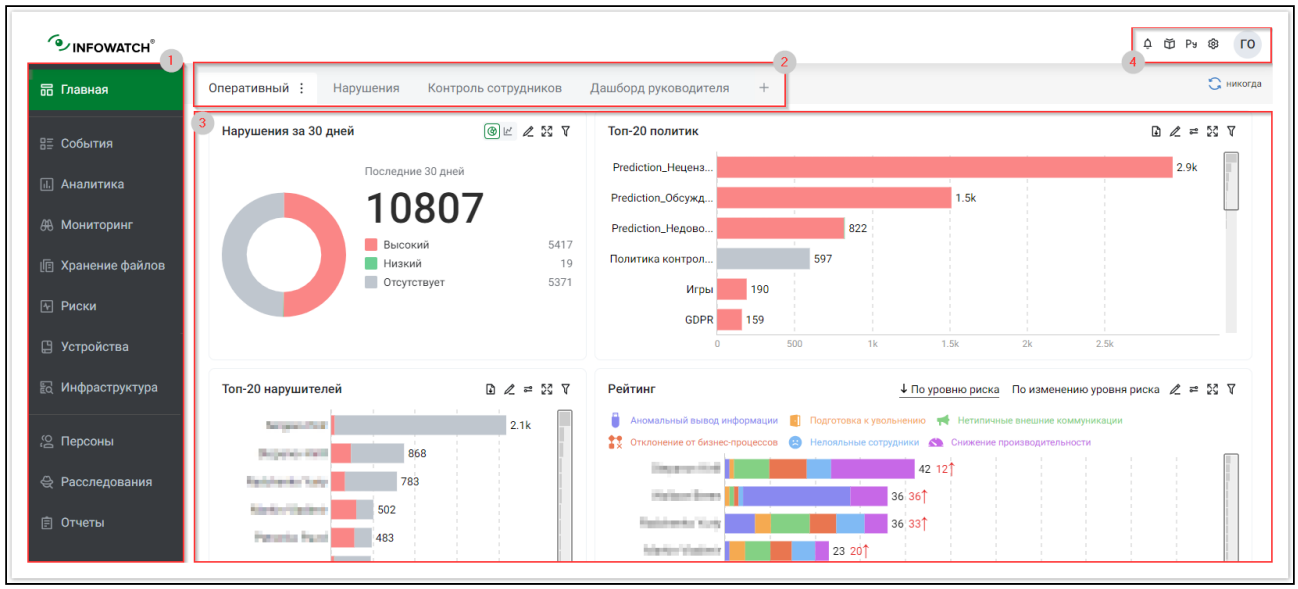
Для визуальной оценки рисков несанкционированного доступа реализованы виджеты на основе отчетов продукта.

5 Интерфейс Центра расследований

Центр расследований представляет собой единую графическую среду, в которой могут быть представлены и проанализированы данные установленных продуктов InfoWatch:

- Data Access Tracker;
- Activity Monitor;
- Data Discovery;
- Prediction;
- Vision.

В интерфейсе Центра расследований можно выделить несколько областей. На изображении ниже показана **Главная** страница.



Элементы интерфейса:

Номер на схеме	Элемент окна	Описание элемента
1	Панель навигации	Рабочие разделы Центра расследований. Вы можете скрыть панель навигации, нажав «**Свернуть меню** внизу.
2	Панель дашбордов	Список предустановленных дашбордов
3	Рабочая область	Отображение виджетов продуктов InfoWatch и работа с ними
4	Меню пользователя	Пользовательское меню, в котором вы можете: • отредактировать свою учетную запись; • сменить пароль;

Номер на схеме	Элемент окна	Описание элемента
		• включить использование горячих клавиш; • узнать контактные данные компании InfoWatch и службы поддержки; • выйти из Системы.
	 Настройки	Раздел настроек (подробнее см. документ "*InfoWatch Data Access Tracker. Руководство администратора*")
	 Уведомления	Папка уведомлений, в которую попадают сообщения Системы пользователю (подробнее см. документ "*InfoWatch Data Access Tracker. Руководство администратора*", "Системные уведомления")
	 Смена языка	Выбор языка интерфейса : *Русский* или *Английский*
	 Справочник	Справочник Центра расследований, в котором доступны: • *Сценарии работы с Системой* для наиболее эффективного использования продукта; • *Руководство администратора* с описанием настроек продукта; • *Руководство пользователя* с описанием работы в продукте; • Информация о новых возможностях продуктов (*Что нового*).

Работа в Центре расследований ведется в **тематических разделах**:

Раздел	Описание
Главная	Основной раздел, на котором размещены предустановленные дашборды с наборами виджетов, позволяющие быстро получить и отобразить информацию о нарушениях и нарушителях на каждом из них с учетом фильтров. Вы также можете создавать собственные дашборды с желаемым набором виджетов.
События	Список событий согласно установленным фильтрам
Аналитика	Статистическая информация о нарушениях/нарушителях, согласно установленным фильтрам, отображаемая на: • виджетах, содержащих графики, диаграммы и таблицы;

Раздел	Описание
	• графе связей с визуализацией событий. Вкладка *Статистика нарушений* доступна всем продуктам. На вкладке *Граф связей* представлена функциональность продукта InfoWatch Vision (см. документ "*InfoWatch Vision. Руководство пользователя*"). На вкладке *Статистика активности* представлена функциональность продукта InfoWatch Activity Monitor (см. документ "*InfoWatch Activity Monitor. Руководство пользователя*").
Мониторинг	Мониторинг активности сотрудников, а также наблюдения за рабочими станциями сотрудников в режиме онлайн Раздел продукта InfoWatch Activity Monitor (см. документ "*InfoWatch Activity Monitor. Руководство пользователя*")
Хранение файлов	Создание и запуск задач сканирования сетевых ресурсов, просмотр и анализ детальной информации о файлах, включая владельцев, поиск дубликатов файлов Раздел продукта InfoWatch Data Discovery (см. документ "*InfoWatch Data Discovery. Руководство пользователя"*)
Риски	Расчет рейтинга сотрудников для прогнозирования рисков информационной безопасности Раздел продукта InfoWatch Prediction (см. документ "*InfoWatch Prediction. Руководство пользователя"*)
Устройства	Контроль внешних устройств хранения Раздел продукта InfoWatch Device Control (см. "*InfoWatch Device Control. Руководство пользователя*")
Инфраструктура	Автоматический аудит службы каталогов и доступа к почтовым ящикам; отслеживание изменений прав доступа к папкам и файлам Раздел продукта InfoWatch Data Access Tracker
Персоны	Справочник персон компании, а также справочник внешних контактов
Расследования	Проведение расследований с использованием накопленных данных по нарушениям
Отчеты	Список созданных отчетов с возможностью выгрузить их файлы

6 Главная страница

Главная страница Центра Расследований содержит инструменты для получения актуальной информации о нарушениях – дашборды. Дашборды состоят из набора виджетов одного или нескольких продуктов InfoWatch. Вы можете создать свои дашборды и добавить на них любые из доступных виджетов или выбрать предустановленные дашборды с наиболее часто используемыми виджетами. Набор доступных для добавления виджетов зависит от установленных продуктов InfoWatch.

Предустановленные дашборды:

- **Оперативный** – представляет ключевые показатели для мониторинга нарушений:
  - графики с динамикой нарушений за последние три дня или за последние сутки, диаграммы с распределением по уровням нарушений;
  - лидеры по нарушениям среди сотрудников-отправителей;
  - топ наиболее нарушаемых политик безопасности;
- **Контроль сотрудников** – представляет статистику нарушений с участием сотрудников:
  - лидеры по нарушениям среди сотрудников-отправителей;
  - рейтинг сотрудников (при установленном продукте InfoWatch Prediction);
  - сотрудник под наблюдением;
- **Файлы** – представляет наиболее часто встречаемые в нарушениях файлы и аудит действий с ними:
  - топ сработавших объектов защиты;
  - топ использованных в операциях файлов;
  - топ использованных в операциях типов файлов;
  - статистика действий с файлами (при установленном продукте InfoWatch Activity Monitor);
- **Нарушения** – показывает аномалии в действиях сотрудников, изменения поведения, сравнительную статистику по нарушениям:
  - графики с динамикой нарушений за выбранную дату или период времени, диаграммы с распределением по уровням нарушений;
  - топ наиболее нарушаемых политик безопасности;
  - лидеры по нарушениям среди сотрудников-отправителей;
- **Дашборд руководителя** – представляет статистику для руководителя подразделения по действиям его сотрудников:
  - графики с динамикой нарушений за выбранную дату или период времени, диаграммы с распределением по уровням нарушений;
  - лидеры по нарушениям среди сотрудников-отправителей;
  - топ типов событий с нарушениями;
  - решения пользователей по событиям.

6.1 Дашборды и виджеты

6.1.1 Дашборды

Дашборды с виджетами доступны на **Главной** странице. По умолчанию на странице отображается *Оперативный* шаблон. Офицер безопасности может разместить на рабочей области предустановленные дашборды, создать пользовательские и далее добавить на них виджеты любого из установленных продуктов InfoWatch.

Чтобы добавить виджет:

1. Нажмите  на панели дашбордов (справа от вкладки *Оперативного* шаблона).
2. Выберите один из предустановленных дашбордов или **Новый дашборд**, при необходимости введите новое имя и нажмите **Сохранить**. Дашборд будет добавлен на панель.
3. Нажмите  и выберите **+ Добавить виджет**.
4. В окне **Добавить** в списке слева:
   - укажите, виджеты какого из установленных продуктов InfoWatch вы хотите добавить,
   - или выберите **Все**.

   Для быстрого поиска виджета по названию воспользуйтесь поисковой строкой.
5. Напротив интересующих виджетов нажмите **+ Добавить** и укажите количество. Можно добавить на дашборд не более 10 виджетов одного типа за раз.
6. Если требуется, выберите другие виджеты.
7. Нажмите **Применить**. Выбранные виджеты будут расположены на рабочей области.

Условия Единого фильтра, установленные в других разделах Центра расследований, не распространяются на виджеты дашбордов на **Главной** странице. Любой виджет настраивается независимо от других.

Чтобы настроить виджет:

1. Нажмите  в углу виджета.
2. Установите значения фильтра. Если необходимо, добавьте дополнительные атрибуты фильтра (см. "Единый фильтр").
3. Нажмите **Сохранить**.

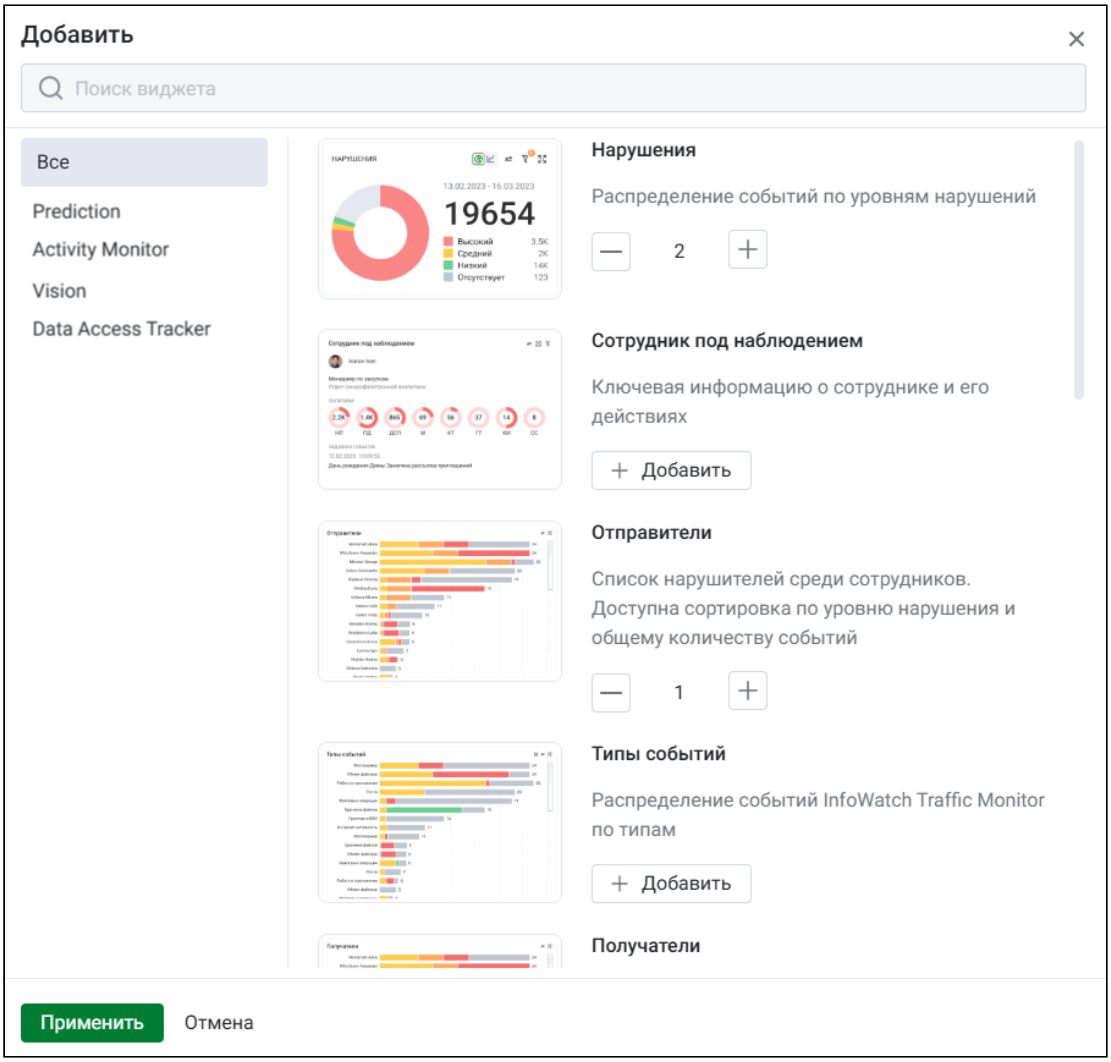
> **Примечание:**
>
> Данные на виджетах обновляются согласно установленному интервалу. Чтобы установить интервал обновления, в правом верхнем углу меню выберите одно из значений, которое может изменяться от 15 минут до 1 часа. Если данные обновлять не требуется, выберите **никогда**.
>
> Также вы можете обновить данные вручную. Для этого нажмите . Необходимо иметь в виду, что обновляются только виджеты, расположенные в видимой области на дашборде. Чтобы обновить все данные на всех виджетах, пролистайте отображение на экране всех виджетов и нажмите .

6.1.2 Виджеты

На дашбордах можно расположить виджеты разделов **Аналитика**, **Риски** и **Инфраструктура**.

> **Важно!**
>
> Подробнее о виджетах раздела **Инфраструктура** см. статью "Вкладка "Сводка"".

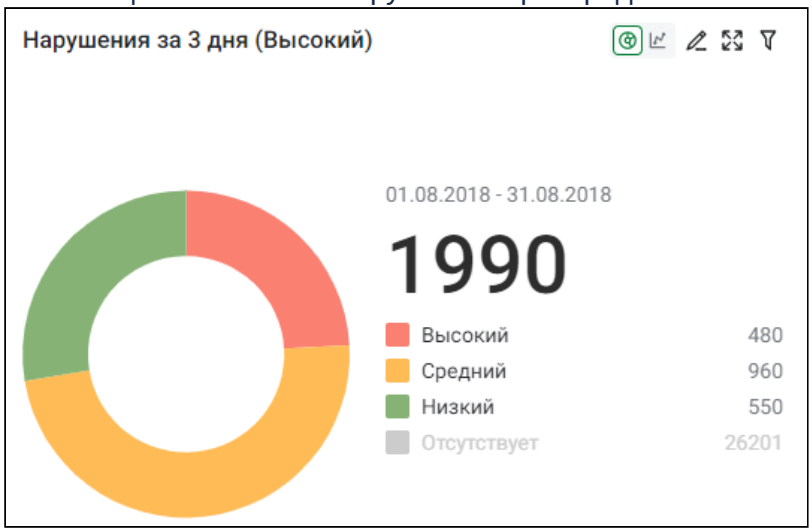
Набор виджетов, доступных для добавления на дашборды, зависит от продуктов, которые установлены в кластере Центра расследований.



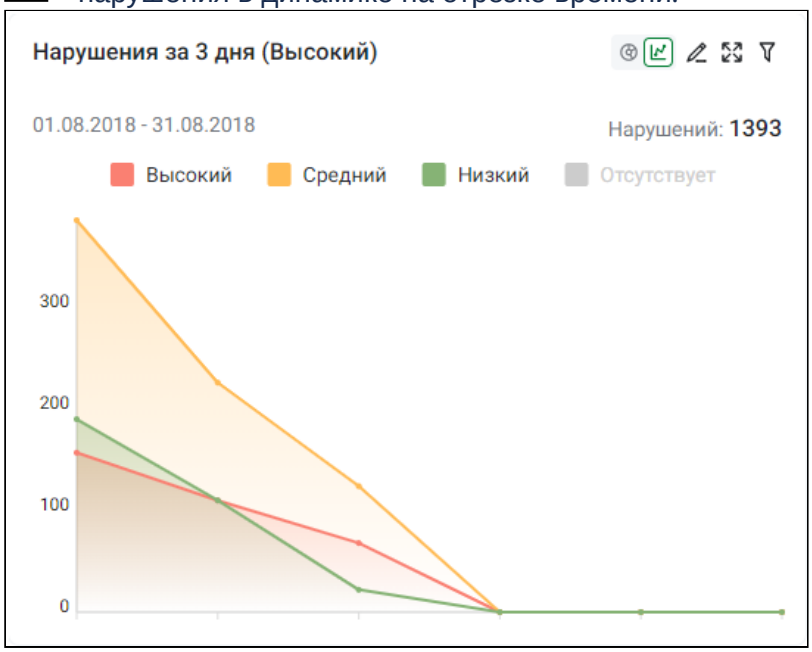
Виджеты **Нарушения** и **Сотрудник под наблюдением** доступны только на **Главной** странице.

Виджет **Нарушения** обрабатывает данные, полученные из Traffic Monitor, и может отображать:

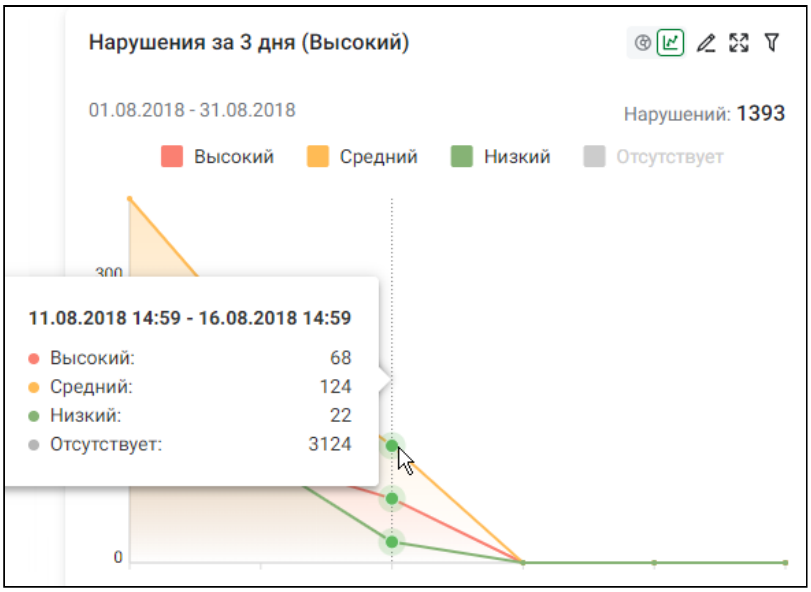
- – общее количество нарушений с распределением по их уровням:



- – нарушения в динамике на отрезке времени:



В обоих вариантах вы можете управлять отображением, используя легенду, на которой можно включить или отключить графики уровней нарушений:



Виджет **Сотрудник под наблюдением** собирает о сотруднике информацию, на основании которой в дальнейшем Офицер безопасности может начать расследование или взять сотрудника на особый контроль.

Для настройки виджета:

1. Нажмите и задайте атрибуты фильтров, применимых к этому виджету.
2. В фильтре **Персона** укажите одну персону из числа сотрудников. При необходимости добавьте другие фильтры и укажите их значения.
3. Нажмите **Сохранить**. Виджет будет отображать:

- персональную информацию о сотруднике и политики безопасности, в которых сотрудник является участником. Одновременно на виджете может быть не больше 8 политик с наибольшим количеством событий с высоким уровнем нарушений;
- последнее событие, связанное с персоной, с указанием даты, действия и политики;
- другие персоны из событий, связанных с сотрудником;

4. Нажмите , если требуется изменить вид отображения виджета:
   - размер фото сотрудника;
   - диаграммы политик с высоким уровнем нарушений.

7 Единый фильтр

Единый фильтр – универсальный инструмент, позволяющий управлять поиском и отображением данных в Центре расследований InfoWatch.

С помощью Единого фильтра вы можете:

- сохранять различные наборы фильтров, для того чтобы быстро получать интересующие срезы информации;
- исключить из анализа часть данных, чтобы скрыть лишнюю информацию.

Важно!

При работе с Единым фильтром учитывайте, что:

- все настройки Единого фильтра распространяются только в рамках одной вкладки в браузере;
- при перемещении на шаг назад или вперед (кнопка **Назад**/**Вперед** браузера) фильтр возвращается в то состояние, в каком он был на этом шаге;
- при выходе из Системы все атрибуты фильтра сбрасываются в исходное состояние.

7.1 Фильтры

Единый фильтр – панель, которая содержит группу фильтров.

Примечание:

Подробнее про настройку панели фильтров см. "Работа с Единым фильтром".

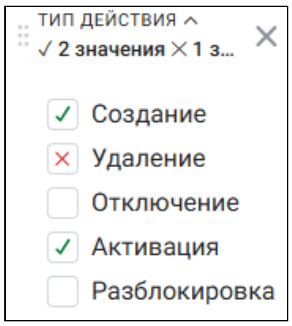
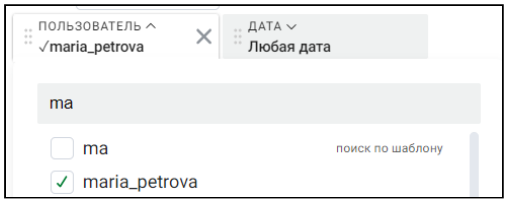
Фильтры на вкладках раздела *Инфраструктура*

Примечание:

Фильтры Data Access Tracker, за исключением фильтра *Дата*, уникальны и работают только на вкладках раздела **Инфраструктура**. Их значения не переносятся при переходе в другие разделы и влияют только на фильтрацию данных Data Access Tracker.

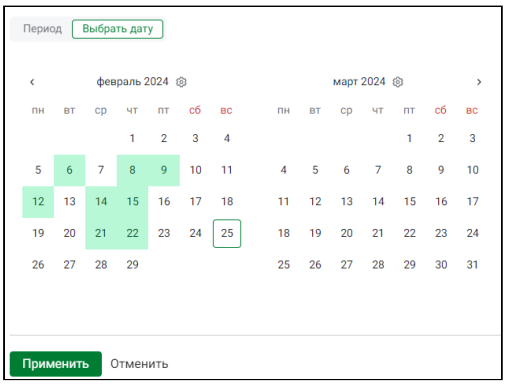
Пользователь с доступом к разделу **Инфраструктура** может использовать фильтры Data Access Tracker без дополнительных настроек.

Фильтр	Описание	Установка значений
Сервисный аккаунт	Учетная запись, используемая для запуска служб или приложений	Вы можете оставить в отчете только учетные записи с заданным признаком. Доступные значения: *Нет*/*Да*

Фильтр	Описание	Установка значений
Просмотрено	Была ли учетная запись отмечена просмотренной	
Имя пользователя	Имя пользователя, чья учетная запись содержится в отчете	Вы можете просмотреть информацию по одному или нескольким значениям или, наоборот, исключить некоторые записи из таблицы. Атрибуты фильтра, в которых можно установить несколько значений, имеют признаки: • ☐ – значение не выбрано; • ☑ – значение включено в фильтрацию; • ☒ – значение исключено из фильтрации. Таким образом, для одного атрибута фильтра вы можете использовать значения с комбинацией этих признаков:  При большом количестве значений фильтров воспользуйтесь поиском. Для этого начните вводить значение в поле фильтра и выберите одно из предложенных:  **Примечание:**

Фильтр	Описание	Установка значений
Имя компьютера	Имя компьютера, на котором произошли изменения	Поиск по значениям доступен для следующих фильтров: • на вкладке **Сводка**: *Имя пользователя*; • на вкладке **Аудит службы каталогов**: *Кем изменено*, *Имя пользователя*; • на вкладке **Изменения групп**: *Кем изменено*, *Объект*, *Группа*; • на вкладке **Права на почтовые ящики**: *Адрес ящика*, *Владелец*, *Тип ящика*, *Пользователь/группа*; • на вкладке **Изменения прав на файлы и папки**: *Кем изменено*, *Сетевой ресурс*, *Имя компьютера*, *Локальный путь*, *Субъект доступа*.
Группа	Имя группы, в которой произошли изменения	
Тип действия	Тип действия с объектом службы каталогов	
Кем изменено	Имя пользователя, от чьего лица произведены изменения	
Объект	Объект службы каталогов, который был создан, добавлен, изменен или удален	
Субъект доступа	Пользователь (группа/компьютер), чьи права доступа к файлу/папке были изменены. **Примечание:** Учетные записи или группы, удаленные из Active Directory, отображаются серым цветом.	
Тип прав доступа	Уровень доступа к файлу или папке: *Файловая система* / *Доступ по сети*	
Сетевой ресурс	Имя сетевой папки, права доступа к которой были изменены	
Локальный путь	Путь до сетевой папки, права доступа к которой были изменены	
Ошибка входа	Причина неудачной попытки входа: • *Нет доступных серверов* • *Неверное имя пользователя* • *Неверный пароль* • *Неверные учетные данные* • *Несанкционированное время входа* • *Компьютер не зарегистрирован* • *Учетная запись отключена* • *Тип входа недоступен* • *Не запустилась служба Netlogon*	

Фильтр	Описание	Установка значений
	• *Истек срок действия учетной записи* • *Вход запрещен сетевым экраном* • *Требование смены пароля* • *Учетная запись заблокирована* • *В локальном хранилище отсутствуют данные* для аутентификации учетной записи • *Системная ошибка* • *Недостаточно системных ресурсов* • *Время не синхронизировано* • *Истек срок действия пароля*	
Адрес ящика	Адрес ящика с общим доступом	
Владелец	Пользователь MS Active Directory, которому принадлежит ящик	
Тип ящика	Тип почтового ящика MS Exchange	
Пользователь/группа	Учетная запись (группа), которой предоставлен доступ к почтовым ящикам других пользователей	
Дата события службы каталогов	Период времени, за который вас интересуют данные: • *Последние сутки;* • *Текущий день;* • *Последние 3 дня;* • *Последние 7 дней;* • *Последние 30 дней;* • *Текущий месяц;* • *Прошлый месяц;* • *Произвольный период* (можно выбрать даты начала и окончания периода либо список произвольных дат)	Отметьте интересующий период времени либо задайте произвольный период/несколько произвольных дат. **Чтобы указать интересующий произвольный период времени** 1. В календаре выберите указателем мыши начальную дату, затем конечную. Выбранный период будет подсвечен: 

Фильтр	Описание	Установка значений
Дата создания учетной записи **Дата последнего входа** в систему с компьютера **Дата предыдущего входа** в систему		2. Нажмите **Применить**. **Чтобы указать одну или несколько произвольных дат** 1. Выберите указателем мыши одну или несколько дат в календаре. Выбранные даты будут подсвечены:  2. Нажмите **Применить**.

После выбора одного или нескольких атрибутов Система отобразит события с учетом выбранных атрибутов. При этом будут перестроены:

- таблицы и виджеты в разделе **Инфраструктура**;
- диаграммы, графики и таблицы на вкладке **Статистика нарушений** раздела **Аналитика**;
- таблица с данными событий в разделе **События**;
- таблица с данными персон и виджеты в разделе **Персоны**.

Фильтры в разделах *События* и *Аналитика* → *Статистика нарушений*

В таблице указаны фильтры и виджеты, доступные в **События** и **Аналитика** → **Статистика нарушений**.

Примечание:

По умолчанию из таблицы ниже доступны виджеты:

- *Дата*;
- *Отправители*;
- *Типы событий*;
- *Уровень нарушений*;
- *Получатели*.

Примечание:

Поиск по значениям доступен для следующих фильтров:

- В разделе **События**: *Статус*, *Отдел*, *Группа*, *Тип события*, *Объект защиты*, *Политика*, *Персона*, *Периметр*.
- В разделе **Аналитика → Статистика нарушений**: *Статус*, *Отдел*, *Группа*, *Тип события*, *Объект защиты*, *Политика*, *Персона*.
- В разделе **Персоны**: *Персона*, *Должность*, *Статус*, *Отдел*, *Группа*.

Важно!

Чтобы фильтрация данных была доступна, убедитесь, что в роли пользователя открыт доступ к разделам **События**, **Аналитика → Статистика нарушений**. Подробнее о настройках ролей см. "*InfoWatch Data Access Tracker. Руководство администратора*", раздел "Настройки Системы", статья "Роли".

Название фильтра	Описание и возможные значения
Дата	См. фильтр *Дата* в таблице с фильтрами раздела **Инфраструктура**.
Уровень нарушения	Атрибуту соответствует виджет **Уровень нарушения**. Выберите уровень нарушения (соответствует аналогичному в Traffic Monitor): • *Высокий;* • *Средний;* • *Низкий;* • *Отсутствует.*
Тип события	Атрибуту соответствует виджет **Типы событий**. Создайте выборку по типу события. Для этого выберите тип события Traffic Monitor: • *Работа с приложениями:* • *Буфер обмена;* • *Ввод с клавиатуры;* • *Почта:* • *Электронная почта;* • *Веб-почта;* • *Принтер и МФУ:* • *Печать;* • *Хранение файлов:* • *Data Discovery;* • *Интернет-активность:* • *Web-сообщение;* • *Мессенджер:* • *Facebook;* • *ICQ;* • *MS Lync;* • *Mail.Ru Агент;* • *MS Teams;*

Название фильтра	Описание и возможные значения
	• *Skype;* • *Telegram;* • *Viber;* • *WhatsApp;* • *ВКонтакте;* • *XMPP;* • *Yahoo!;* • *Обмен файлами:* • *Облачные хранилища;* • *Съемное устройство;* • *FTP;* • *Сетевой ресурс;* • *Терминальная сессия;* • *Файловые операции:* • *Чтение файла;* • *Запись файла;* • *Другие:* • *Фотосъемка;* • *SMS.*
Объекты защиты	Атрибуту соответствует виджет **Объекты защиты**. Выберите из списка объекты защиты, созданные в Traffic Monitor.
Политика	Атрибуту соответствует виджет **Политики**. Выберите из списка политики, созданные в Traffic Monitor.
Тип контакта	Позволяет отобразить события по различным типам контактов, используемых в Системе. Выберите одно или несколько значений: • *Уволенные* – фильтр по событиям, в которых одним из участников является уволившийся ранее сотрудник. Если при интеграции с другими системами не были автоматически загружены личные контакты сотрудника, следует добавить их вручную (подробнее см. "Добавление контактов персоны"); • *Внешние* – фильтр по событиям, в которых хотя бы один участник не принадлежит к списку внутренних доменов; • *Внутренние* – фильтр по событиям, в которых хотя бы один участник принадлежит к списку внутренних доменов; • *Новые* – фильтр по событиям, в которых данный идентифицированный или неидентифицированный контакт, полученный из Traffic Monitor, встречается впервые в указанную дату или временной интервал в фильтре **Дата**; • *Личные* – фильтр по событиям с сообщениями, отправленными на личные адреса, в том числе при отправке письма одним сотрудником на личный адрес другого сотрудника;

Название фильтра	Описание и возможные значения
	• *Самому себе* – фильтр по событиям, в которых отправителем и получателем является одна и та же персона. При одновременном выборе значений *Личные* и *Самому себе* будут отображены события с письмами, отправленными сотрудником на свой личный почтовый адрес.
Периметр, **Вошло в периметр**, **Покинуло периметр**	Выберите периметр из списка. Если требуется, задайте модификатор: • *Периметр* – поиск по всем событиям, у которых в атрибутах указаны выбранные периметры; • *Вошло в периметр* – поиск по событиям, у которых в атрибуте **Вошло в периметр** указаны выбранные периметры; • *Покинуло периметр* – поиск по событиям, у которых в атрибуте **Покинуло периметр** указаны выбранные периметры. Если выбрать значение *Неизвестный периметр*, то будут найдены события, в которых периметр входа и/или периметр выхода не был определен в Traffic Monitor.
Персона*, **Отправитель***, **Получатель***	Позволяет отобразить события, участником которых являлись указанные персоны. В строке поиска можно указывать как имя сотрудника, так и его контактные данные. Дополнительно фильтр можно настроить с помощью модификаторов: • **Содержит значение** – фильтр по событиям с участием хотя бы одной из выбранных персон; • **Точное совпадение** – фильтр по событиям, в каждом из которых участвуют все выбранные персоны.
Группа*, **Группа получателей***, **Группа отправителей***	Атрибуту соответствует виджет **Аналитика по группам/персонам**. Создает выборку по группам AD и Traffic Monitor. Укажите группы в иерархии в компании, синхронизированные с Traffic Monitor или AD.
Отдел*, **Отдел отправителя***, **Отдел получателя***	Укажите все интересующие вас отделы в компании, добавленные при синхронизации с Traffic Monitor или AD.
Статус*, **Статус отправителя***,	Укажите все интересующие вас статусы сотрудников в компании, добавленные при синхронизации с Traffic Monitor.

Название фильтра	Описание и возможные значения
Статус получателя*	

* – Для атрибутов, связанных с персонами, можно установить модификаторы:

- *Любой;*
- *Отправитель;*
- *Получатель.*

Если установить модификатор *Отправитель/Получатель*, то выбранные персоны, группы персон или контакты будут являться отправителями или получателями в событиях.

Если установить модификатор *Любой*, то будут выбраны все участники события: все персоны, группы персон или контакты.

7.2 Работа с Единым фильтром

7.2.1 **Активация фильтра**

Чтобы **применить** фильтр, нажмите  в поле фильтра и укажите значение. В таблице отобразятся только те строки, которые отвечают условию заданного фильтра.

Чтобы **сбросить** значения фильтра, нажмите на панели фильтра . Для фильтра будет установлено значение по умолчанию.

7.2.2 **Добавление и удаление фильтров**

В панели фильтров можно использовать один или несколько фильтров.

Чтобы добавить фильтр на панель фильтров:

1. Нажмите .
2. Выберите фильтр из списка.
3. Щелкните вне окна со списком фильтров.

Фильтр будет добавлен на панель фильтров.

Чтобы удалить фильтр с панели фильтров:

1. Нажмите .
2. Снимите флажок с фильтра в списке.
3. Щелкните вне окна со списком фильтров.

Фильтр будет удален с панели фильтров.

Чтобы переместить фильтр на другое место на панели, зажмите  у выбранного фильтра перетащите на любое другое место.

Чтобы скрыть панель Единого фильтра, нажмите .

7.2.3 Значения фильтров

В фильтре необходимо выбрать минимум одно значение. Если не выбрано ни одно значение, то используется значение по умолчанию.

> **Важно!**
>
> При выходе из Системы сбрасываются значения фильтров. Рекомендуется сохранить фильтры перед выходом из Системы (см. "Сохранение и загрузка наборов фильтров").

Условие с несколькими фильтрами

Если заданы значения для нескольких фильтров, то условия нескольких фильтров объединяются с помощью логического "И".

Пример:

Укажите значение для нескольких фильтров:

- в фильтре **Дата события** укажите *Прошлый месяц*;
- в фильтре **Уровень нарушения** укажите *Высокий*.

В результате настройки в таблице событий, полученных из Traffic Monitor, отображаются только события с высоким уровнем нарушения за прошлый месяц.

Включение и исключение значений фильтра

Доступные состояния для значений фильтров:

-  – значение не выбрано (состояние по умолчанию);
-  – значение включено;
-  – значение исключено.

Чтобы изменить состояние значения, щелкните по флажку состояния.

Вы можете включить и/или исключить несколько значений, при этом:

- несколько включенных значений объединяются с помощью логического "ИЛИ";
- несколько исключенных значений объединяются с помощью логического "ИЛИ";
- условие из нескольких включенных значений и условие из нескольких исключенных значений объединяются с помощью логического "И".

Сброс значений фильтра

Чтобы сбросить значения фильтра, нажмите на панели фильтра . Для фильтра будет установлено значение по умолчанию.

Чтобы сбросить значения для всех фильтров, нажмите .

7.2.4 Сохранение и загрузка наборов фильтров

Чтобы использовать заданные значения фильтров в дальнейшем, вы можете сохранить их в каталоги одного из типов:

- *Личные* – каталоги и их содержимое доступны только создавшему их пользователю;
- *Общие* – каталоги и их содержимое доступны всем пользователям Системы.

Чтобы сохранить фильтр:

1. Установите требуемые значения фильтров и нажмите .
2. В окне **Сохранить фильтр** задайте имя нового фильтра.
3. Выберите тип каталога, в который Система сохранит фильтр: *Личный* или *Общий*.
4. Выберите каталог, в котором следует сохранить фильтр, или создайте новый. Если каталогов много, используйте поиск по названию.

> **Примечание:**
>
> Если не выбрать каталог, Система сохранит фильтр в корневой директории указанного типа каталогов.

5. Нажмите **Сохранить**.

Чтобы воспользоваться ранее созданным фильтром:

1. В области Единого фильтра нажмите **Сохраненные фильтры**.
2. Откройте каталог, который содержит интересующий фильтр.
3. Нажмите на фильтр, чтобы его активировать.

Чтобы отредактировать каталоги и фильтры:

1. В области Единого фильтра нажмите **Сохраненные фильтры** или на имя примененного фильтра.
2. Нажмите  над списком с фильтрами.
3. В окне **Настройка фильтров и каталогов** вы можете:
    - изменить иерархию каталогов путем перетаскивания;
    - в строке типа каталога:
        -  создать каталог;
    - при наведении курсора на каталог:
        -  переименовать каталог;
        -  создать дочерний каталог;
        -  удалить каталог;
    - перемещать фильтры внутри каталогов и между каталогами;
    - при наведении курсора на имя фильтра:
        -  переименовать фильтр;
        -  записать текущий фильтр, т.е. сохранить с этим названием примененные на данный момент значения фильтров;
        -  удалить фильтр.

При этом Главный офицер может редактировать и удалять личные и общие каталоги и/или их содержимое. Другие офицеры безопасности могут редактировать и удалять только личные каталоги и/или фильтры.

8 Раздел "События"

> **Примечание:**
>
> DAT не использует в работе события из Traffic Monitor.

В этом разделе для просмотра доступны данные событий, загруженных в Центр расследований после синхронизации с Traffic Monitor:

- Уровень нарушения в событии;
- Тип события;
- Решение Офицера безопасности по событию;
- Вердикт Системы по событию;
- *Дата* создания события в Traffic Monitor;
- *Отправитель* – лицо, совершившее нарушение;
- *Рабочая станция* – компьютеры, связанные с событием;
- *Получатель* – лица, которым субъект передал данные;

> **Примечание:**
>
> Отметка  рядом с контактом *Отправителя* или *Получателя* означает, что это новый контакт, который появился в Системе в дату или период времени, указанные в фильтре **Дата**.

- *Вложения* – наличие файлов-вложений в событии, их названия и размер;
- *Действие/Описание* переданных данных;
- *Политики*, сработавшие на данном виде нарушения;
- *Объекты защиты*, которые были переданы;
- *Источник/ID в источнике* – идентификатор события в Traffic Monitor.



Получите интересующую выборку по событиям, настроив фильтры на панели Единого фильтра (подробнее см. "Единый фильтр"). События представлены в разделе в виде таблицы.

Чтобы получить расширенную информацию или анализ выбранного события, можно:

- нажать  внизу списка событий. При этом вместе с основными данными события будут отображены и такие, как реплики в чате, текст письма, вложенные изображения и т.д. В детализации событий цветом выделяются слова, которые относятся к обнаруженным объектам защиты;

- нажать , чтобы перейти в режим просмотра диалогов в мессенджерах (доступно, если у вас установлен продукт Vision);
- нажать , чтобы добавить событие в новое или ранее созданное расследование;
- нажать , чтобы посмотреть событие на графе связей (доступно, если у вас установлен продукт Vision);
- нажать , чтобы скопировать ID события для быстрого поиска его в Traffic Monitor;
- нажать , чтобы просмотреть снимки экрана в событии (доступно, если у вас установлен продукт Activity Monitor);
- нажать , чтобы просмотреть событие на таймлайне персоны (доступно, если у вас установлен продукт Activity Monitor).

Чтобы оперативно обработать сразу несколько событий:

1. В списке выберите события:
   - зажав клавишу ***Ctrl*** и выделив нужные события;
   - зажав клавишу ***Shift*** и выбрав диапазон событий (от и до).
2. Нажмите на панели сверху:
   -  для построения частного графа связей по такой выборке (доступно, если у вас установлен продукт Vision);
   -  для начала расследования с указанной выборкой событий (подробнее см. "Добавление материалов в расследование");
   - **Просмотр событий**, чтобы перейти в раздел **События** Traffic Monitor для более подробного анализа. При этом будут отображены только 300 событий из всех отфильтрованных в Центре расследований. Если события принадлежат нескольким источникам, то они будут открыты в разных вкладках браузера.

     Чтобы снять выделение с выбранных событий, нажмите  **Сбросить выбранные события**.

Совет:

Если вы часто переключаетесь между Центром расследований и Traffic Monitor, рекомендуем настроить сквозную аутентификацию, которая позволяет не вводить повторно имя пользователя и пароль. Подробнее о настройке см. документ *"InfoWatch Traffic Monitor. Руководство администратора*", раздел "*Настройка сквозной аутентификации между продуктами InfoWatch*".

Примечание:

Столбцы таблицы с событиями отображаются с учетом настроек роли, выданной пользователю. Поэтому необходимо, чтобы пользователю были выданы нужные права доступа:

- для столбцов *Дата, Тип события, Отправитель, Получатель* включите пункты **События**, **Статистика нарушений** на вкладке **Функции** в настройке роли;

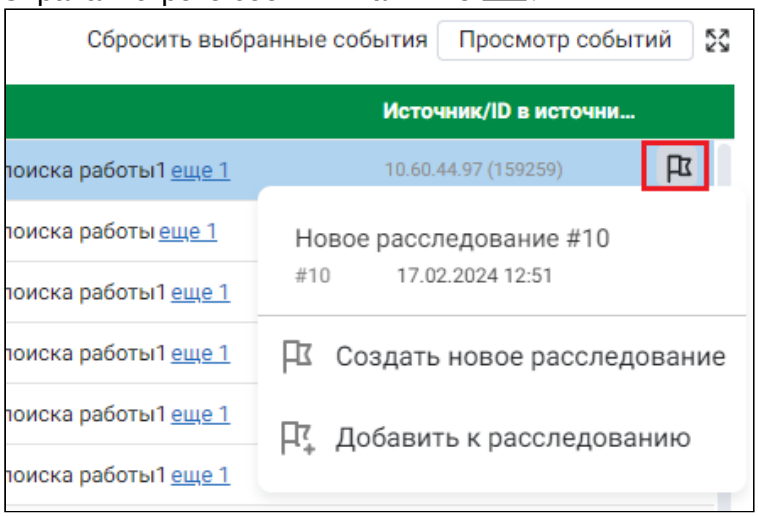
- для столбцов *Описание, Вложения, Источник, ID события* – пункт **Детали событий**;
- для столбцов *Уровень нарушения, Решение пользователя, Вердикт* – пункт **Детали нарушений**;
- для столбцов *Политики, Объекты защиты, Периметры* – пункт **Политики, Объекты защиты и Периметры**.

8.1 Добавление событий в расследование

Вы можете добавить события из списка в расследование или создать новое расследование на их основе.

Чтобы добавить событие в расследование:

1. Выделите событие в списке щелчком мыши.
2. Справа в строке события нажмите .



3. Выберите:
   - **Добавить к расследованию**. Затем:
     a. Начните вводить название расследования, в которое необходимо добавить событие.
     b. Выберите название в выпадающем списке.
     c. Нажмите **Добавить**.

   или

   - **Создать новое расследование**. В этом случае новое расследование будет создано автоматически.

Чтобы добавить одно или несколько событий в расследование:

1. Выделите события, используя клавиши *Ctrl* или *Shift*.
2. В правой части экрана над таблицей с событиями нажмите:
   - **Добавить к расследованию**. Затем:
     a. Начните вводить название расследования, в которое необходимо добавить событие.
     b. Выберите название в выпадающем списке.
     c. Нажмите **Добавить**.

или

- **Создать новое расследование**. В этом случае новое расследование будет создано автоматически.

События, участвующие в расследованиях, помечены знаком . Такие события также можно добавлять в новые или уже существующие расследования.

Чтобы перейти в расследование из события:

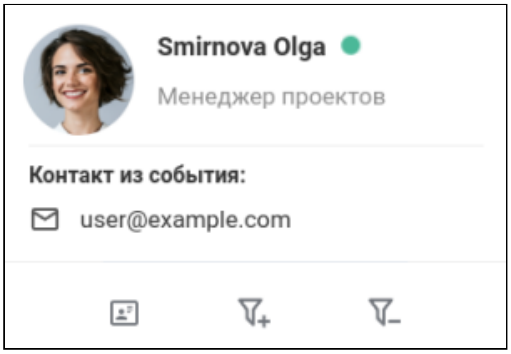
1. Нажмите .
2. Выберите расследование в списке. Оно откроется на новой вкладке браузера.

Чтобы просмотреть события, участвующие в расследованиях, воспользуйтесь фильтром **Расследования** (подробнее см. "Единый фильтр").

8.2 Просмотр и выгрузка данных событий

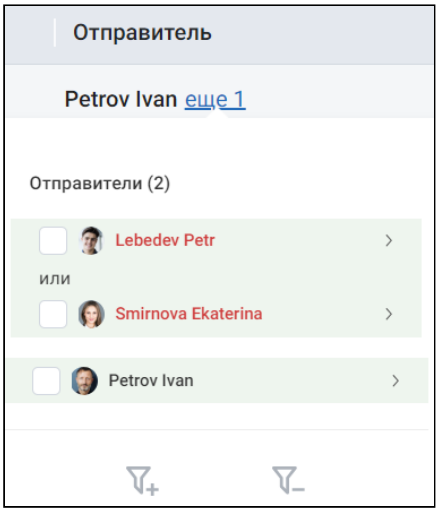
8.2.1 Просмотр используемых контактов

Карточка персоны в разделе **События** содержит контакты сотрудников, которые участвовали в выбранном событии:



8.2.2 Просмотр данных в столбце

Если столбец содержит несколько объектов, их список представлен в свернутом виде. Чтобы развернуть список, нажмите **еще**. В появившемся списке будут представлены все объекты этого столбца:



8.2.3 Фильтрация данных

Вы можете добавить один или несколько объектов в фильтр, и в списке будут только содержащие эти объекты события. Для этого выберите необходимые объекты и нажмите , чтобы добавить их в фильтр, или , чтобы исключить события с данными объектами из списка.

> **Примечание:**
>
> Просмотр данных и фильтрация данных по значениям столбца доступны только для столбцов **Получатель**, **Отправитель**, **Вложение**, **Политики** и **Объект защиты**.

> **Примечание:**
>
> Для корректной работы необходимо, чтобы были разрешены всплывающие окна с указанных источников в браузере.

8.2.4 Выгрузка данных события

При подготовке отчетов по инцидентам, проведении расследования или составлении подборки интересующих вас событий можно выгрузить таблицу с событиями в виде документа Excel или сохранить ее в досье. Для этого:

1. В разделе **События** установите значения атрибутов фильтра. Список событий будет обновлен.
2. В правой верхней части экрана нажмите  → **Выгрузить отчет**.
3. Выберите интересующий вас состав отчета и нажмите **Сохранить**.
4. Дождитесь, пока сформируется отчет.
5. Перейдите в раздел **Отчеты** и скачайте XLSX-файл с отчетом, нажав на ссылку.
6. Откройте XLSX-файл. На листе **Дополнительная информация** указаны дата и время создания отчета, примененные к выборке фильтры и их значения, а также ссылка на

раздел формирования отчета. На листе **Список событий** приведена таблица с событиями. Если требуется, вы можете отредактировать ее вручную.

Чтобы настроить регулярную отправку:

1. Установите значения атрибутов фильтра. Список событий будет обновлен.
2. Нажмите  → **Настроить регулярную отправку**.
3. Выберите состав отчета, а также укажите параметры:

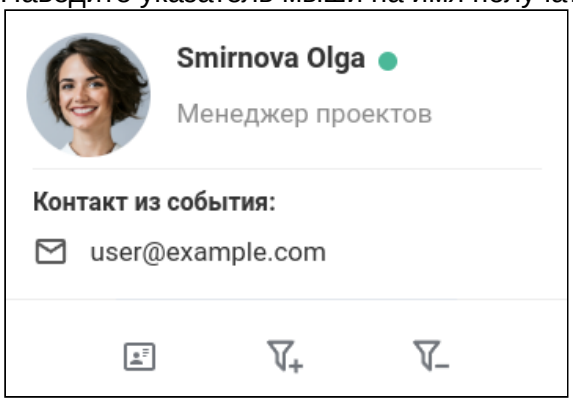
Параметр	Описание
Период формирования отчета	Укажите, за какой период необходимо отправлять отчет: • Текущий день • Последние сутки • Последние 3 дня • Последние 7 дней • Последние 30 дней
Получатели	Укажите получателей отчета
Частота отправки	Укажите, с какой периодичностью Офицеру необходимо получать отчет: • Каждый день • Каждую неделю • Каждый месяц
Время	Укажите время отправки отчета

4. Нажмите **Сохранить**. Будет создана задача на регулярную отправку. Список таких задач вы можете просмотреть в разделе **Отчеты** на вкладке **Задачи на регулярную отправку**. Подробнее см. "Задачи на регулярную отправку".

8.3 Фильтрация событий по персонам и контактам

Чтобы отфильтровать события по получателям или отправителям:

1. Наведите указатель мыши на имя получателя/отправителя/контакт:



2. Нажмите:

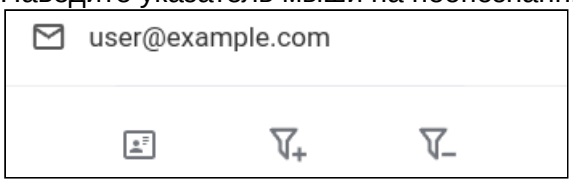
- – данный получатель/отправитель будет добавлен как включенный атрибут фильтра **Персона**, и список событий обновится;

  или

- – данный получатель/отправитель будет добавлен как исключенный атрибут фильтра **Персона**, и список событий обновится.

Чтобы отфильтровать события по неопознанным контактам:

1. Наведите указатель мыши на неопознанный контакт в событии:



2. Нажмите на выбор:
   - – данный контакт будет добавлен как включенный атрибут фильтра **Контакты**, и список событий обновится;

     или

   - – данный контакт будет добавлен как исключенный атрибут фильтра **Контакты**, и список событий обновится.

Чтобы присвоить неопознанный контакт персоне:

1. Наведите указатель мыши на неопознанный контакт в событии.
2. Нажмите .
3. Если требуется завести новое досье с этим контактом:
   a. Нажмите **Создать досье**.
   b. Введите все необходимые данные, как указано в статье "Создание, редактирование и удаление досье".
4. Если требуется добавить контакт в уже существующее досье:
   a. Нажмите **Добавить в досье**.
   b. Укажите досье сотрудника и нажмите **Добавить**.

9 Раздел "Аналитика"

Раздел **Аналитика** предоставляет Офицеру безопасности наглядную статистику в виде таблиц, диаграмм и графиков, построенных по заданным условиям Единого фильтра, по всем полученным из Traffic Monitor событиям. В разделе представлены вкладки:

- **Статистика нарушений** – виджеты статистики (см. "Виджеты статистики");
- **Граф связей** – граф связей продукта Vision (см. *"InfoWatch Vision. Руководство пользователя"*);
- **Статистика активности** – виджеты Activity Monitor (см. *"InfoWatch Activity Monitor. Руководство пользователя"*).

9.1 Виджеты статистики

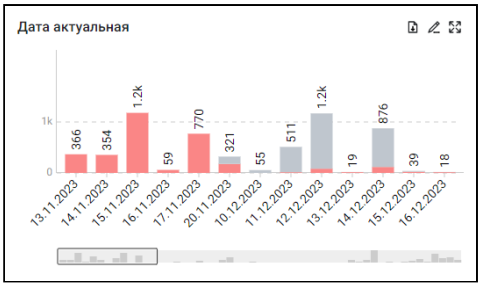
Виджеты на вкладке **Статистика нарушений** наглядно отображают данные от Traffic Monitor, хранящиеся в Системе.

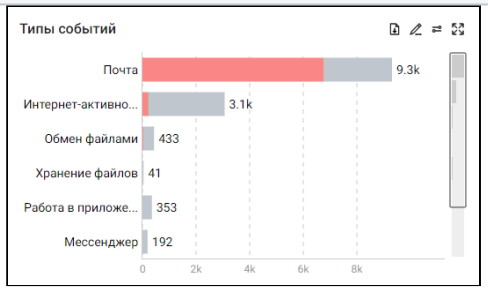
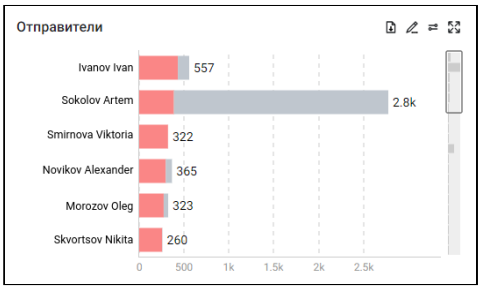
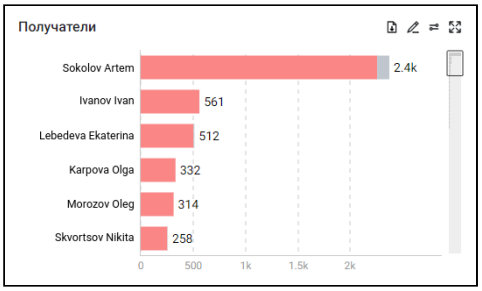
Примечание:

В таблице ниже представлены общедоступные виджеты статистики:

- дата;
- типы событий;
- уровень нарушений;
- отправители;
- получатели.

Остальные виджеты статистики доступны только при наличии в кластере продукта Vision.

Название виджета	Описание
Дата 	Отображает распределение событий по указанным датам с учетом уровней нарушений. Можно выбрать одну или несколько дат и отфильтровать события за указанный день.
Типы событий	Отображает распределение событий Traffic Monitor с разными уровнями нарушений по типам. **Чтобы получить расширенную информацию:** Если навести курсор на имя источника, выводится расширенная информация о количестве событий с разными уровнями нарушения в них:

Название виджета	Описание
	
Уровень нарушений 	Отображает распределение событий по уровням нарушений.
Отправители 	Отображает список персон-отправителей с наибольшим количеством нарушений. Выводятся первые 50 нарушителей, отсортированных по событиям с максимальным уровнем нарушений. **Чтобы настроить отображение на виджете:** 1. Нажмите ⚙ в углу виджета. 2. В открывшемся окне установите: a. Количество отображаемых отправителей: от *3* до *20*; b. Принцип их сортировки: *по уровню нарушения* или *по общему количеству событий.* 3. Нажмите **Сохранить**.
Получатели 	Отображает список получателей, участвующих в событиях. Получатели могут быть идентифицированными или неидентифицированными. Выводятся первые 50 наиболее популярных контактов. **Чтобы добавить контакт из события в фильтр:** 1. Наведите указатель мыши на контакт в событии. 2. Нажмите ⊽+. Выбранный контакт добавится в Единый фильтр, и данные событий будут перестроены с его учетом. Чтобы исключить контакт из фильтрации, нажмите ⊽−.

Название виджета	Описание
	Чтобы добавить неизвестный контакт в досье: 1. Наведите указатель мыши на неизвестный контакт на диаграмме. 2. Нажмите . 3. Введите данные, как указано в "Создание, редактирование и удаление досье".

9.2 Формирование, выгрузка и печать отчетов с данными статистики

Вы можете выгрузить данные с виджетов в виде отчета, а также настроить регулярную отправку отчета.

Чтобы сформировать и выгрузить отчет в формате XLSX:

1. Задайте все требуемые значения атрибутов фильтра, чтобы Система отобразила необходимую информацию.
2. Нажмите  → **Выгрузить отчет**. Отчет с данными со всех виджетов, которые в момент формирования выгрузки были добавлены на рабочую область, будет сохранен в журнале.
3. В окне **Выгрузка отчета** вы можете определить состав **Детализированного** отчета, который содержит данные из виджетов в виде таблиц.
4. Вы можете включить в отчет сразу все виджеты, установив  напротив **Состав выгрузки**.

   Если требуется включить в отчет только определенные виджеты, установите  только напротив их названий.
5. Нажмите **Сохранить**. На экране отобразится сообщение о процессе сохранения отчета.
6. Перейдите в раздел **Отчеты** → **Архив отчетов**.
7. Нажмите  напротив отчета. XLSX-файл с отчетом будет загружен на жесткий диск компьютера.

Загруженный отчет представляет собой файл в формате XLSX, содержащий несколько листов. На листе **Дополнительная информация** указаны дата и время формирования отчета, примененные фильтры и ссылка для перехода в раздел, в котором был сформирован отчет. Каждый последующий лист содержит текстовую информацию с каждого из виджетов, отображаемых на рабочей области раздела на момент создания отчета.

Чтобы настроить регулярную отправку:

1. Выберите значения атрибутов фильтра. Список событий будет обновлен.
2. Нажмите  → **Настроить регулярную отправку**.
3. В окне **Выгрузка отчета** определите состав **Детализированного** отчета, который содержит данные из виджетов в виде таблиц. Вы можете включить в отчет сразу все виджеты, установив  напротив **Выбрать все**.

   Если требуется включить в отчет только определенные виджеты, установите  только напротив их названий.

4. Задайте следующие параметры:

Параметр	Описание
Период отправки	Укажите, за какой период необходимо отправлять отчет: • *Текущий день* • *Последние сутки* • *Последние 3 дня* • *Последние 7 дней* • *Последние 30 дней*
Получатели	Укажите получателей отчета
Частота отправки	Укажите, с какой периодичностью Офицеру безопасности необходимо получать отчет: • *Каждый день* • *Каждую неделю* • *Каждый месяц*
Время	Укажите время отправки отчета

5. Нажмите **Сохранить**. Будет создана задача на регулярную отправку. Список таких задач вы можете просмотреть в разделе **Отчеты → Задачи на регулярную отправку**. Подробнее см. "Задачи на регулярную отправку".

При подготовке отчета для руководства иногда требуется предоставить информацию в бумажном виде или файле.

Чтобы сохранить или распечатать отчет:

1. В разделе **Статистика нарушений** настройте виджеты, необходимые для создания отчета.
2. Выберите набор данных с помощью фильтров.
3. Скройте панель фильтров, нажав .
4. Пролистайте экран до конца страницы, чтобы все виджеты загрузили данные.
5. Нажмите **Ctrl**+**P** или выберите **Печать** в меню браузера.
6. В окне печати:
   - выберите установленный принтер
   или
   - нажмите **Сохранить как PDF**, если требуется отчет в виде файла.
7. Выберите вариант ориентации: *Книжная* или *Альбомная*.
8. Чтобы все виджеты поместились на странице, укажите параметры масштабирования на вкладке **Дополнительные настройки**. Рекомендуется указать значения:
   - 50% для книжной ориентации
   или
   - 70% для альбомной ориентации.

   Также для изменения масштаба и количества выводимых виджетов на странице можно использовать сочетания клавиш **Ctrl**++ и **Ctrl**+-.
9. В зависимости от действия, выбранного в пункте 5, нажмите **Печать** или **Сохранить**.

10 Раздел "Инфраструктура"

Раздел **Инфраструктура** содержит функциональность InfoWatch DAT. В нем Офицер безопасности просматривает результаты автоматического аудита службы каталогов домена и доступа к почтовым ящикам, отслеживает изменения прав доступа к папкам и файлам.

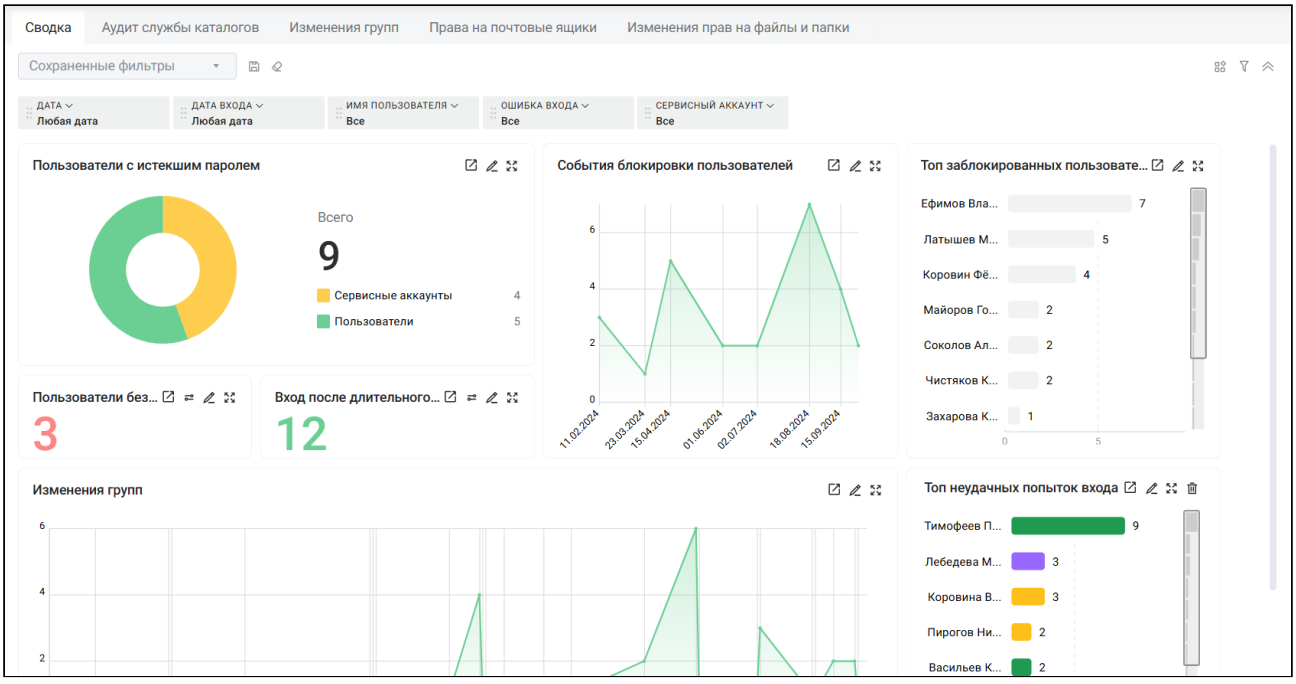
В разделе доступны вкладки:

- **Сводка** – виджеты на основе отчетов, представленных в разделе;
- **Аудит службы каталогов** – отчеты по уязвимым учетным записям, а также по событиям службы каталогов, связанным с риском несанкционированного доступа;
- **Изменения групп** – отслеживание действий с группами службы каталогов;
- **Права на почтовые ящики** – мониторинг доступа к почтовым ящикам;
- **Изменения прав на файлы и папки** – отслеживание действий по предоставлению/отозванию прав доступа пользователей к объектам файловой системы.

10.1 Вкладка "Сводка"

Для визуальной оценки рисков несанкционированного доступа на вкладке **Сводка** представлены виджеты, построенные на основе отчетов со вкладок **Аудит службы каталогов** и **Изменения групп**:

- *Пользователи с истекшим паролем*
- *События блокировки пользователей*
- *Топ заблокированных пользователей*
- *Топ неудачных попыток входа*
- *Вход после длительного перерыва*
- *Пользователи без пароля*
- *Изменения групп*
- *Изменения привилегированных групп*



При работе с виджетами вы можете:

- развернуть выбранный виджет на весь экран. Чтобы вернуться в обычный режим, нажмите **Свернуть** ;
- перейти в отчет, на основе которого построен виджет. Отчет откроется в новой вкладке браузера;
- переименовать виджет;
- редактировать виджет; редактирование виджетов доступно для отчетов *Вход после длительного перерыва*, *Пользователи без пароля* и *Изменения привилегированных групп*.

Отчеты и их настройка описаны в статье "Виджеты раздела "Инфраструктура"".

Настройки рабочей области позволяют:

- установить размер виджета;
- выбрать набор виджетов и фильтров, отображаемых на вкладке;
- изменить расположение виджета на рабочей области.

Чтобы настроить отображение виджетов:

1. Нажмите **Настройка виджетов** в правом верхнем углу рабочей области.
2. Выполните действия по настройке:
   - Если необходимо скрыть виджет с рабочей области, нажмите **Удалить виджет** справа от его названия.
   - Если необходимо переместить виджет на экране, нажмите и удерживайте указатель мыши на его названии, чтобы расположить виджет в любом месте рабочей области.
   - Если необходимо изменить размер виджета, зажмите кнопку мыши и переместите границы виджета.
3. Нажмите **Сохранить**, чтобы применить изменения.

Чтобы добавить виджет:

1. Нажмите **Настройка виджетов** → **Добавить** в правом верхнем углу рабочей области.
2. В окне нажмите **+ Добавить** напротив виджета.

> **Примечание:**
>
> Чтобы быстрее найти интересующий вас виджет, введите название/часть названия виджета в поле поиска.

3. Укажите количество копий виджета, которое необходимо добавить. Можно добавить на дашборд не более 10 виджетов одного типа за раз.
4. Подтвердите действие, нажав **Применить**. Новый виджет будет добавлен на рабочую область.
5. Нажмите **Сохранить**, чтобы сохранить изменения и выйти из режима управления виджетами.

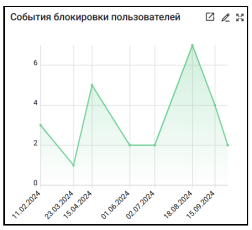
Чтобы отфильтровать информацию на виджетах:

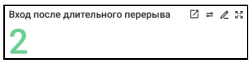
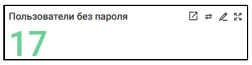
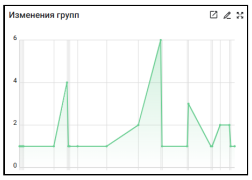
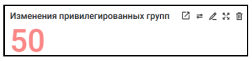
1. Измените набор фильтров, отображаемых на вкладке:
    a. Нажмите **Добавить/удалить фильтр** в правом верхнем углу рабочей области.
    b. В списке фильтров установите/снимите флажок рядом с необходимыми фильтрами.
2. Укажите значения фильтров. Будут обновлены все виджеты, использующие данные параметры.

Чтобы **скрыть/показать панель фильтров**, используйте кнопки и .

10.1.1 Виджеты раздела "Инфраструктура"

На вкладке **Сводка** представлены виджеты, построенные на основе отчетов со вкладок **Аудит службы каталогов** и **Изменения групп**:

Виджет	Описание
Пользователи с истекшим паролем 	Круговая диаграмма, отражающая число пользовательских учетных записей и сервисных аккаунтов с истекшим паролем Построен на основе отчета *Пользователи с истекшим паролем* со вкладки **Аудит службы каталогов**
События блокировки пользователей 	Распределение событий автоматической блокировки пользователей по датам Построен на основе отчета *События блокировки пользователей* со вкладки **Аудит службы каталогов** Доступен фильтр *Дата*
Топ заблокированных пользователей 	Список наиболее часто блокируемых учетных записей Построен на основе отчета *События блокировки пользователей* со вкладки **Аудит службы каталогов** Доступен фильтр *Дата*
Топ неудачных попыток входа	Список учетных записей с наибольшим количеством неудачных попыток входа. Каждый тип ошибки входа имеет уникальное цветовое отображение

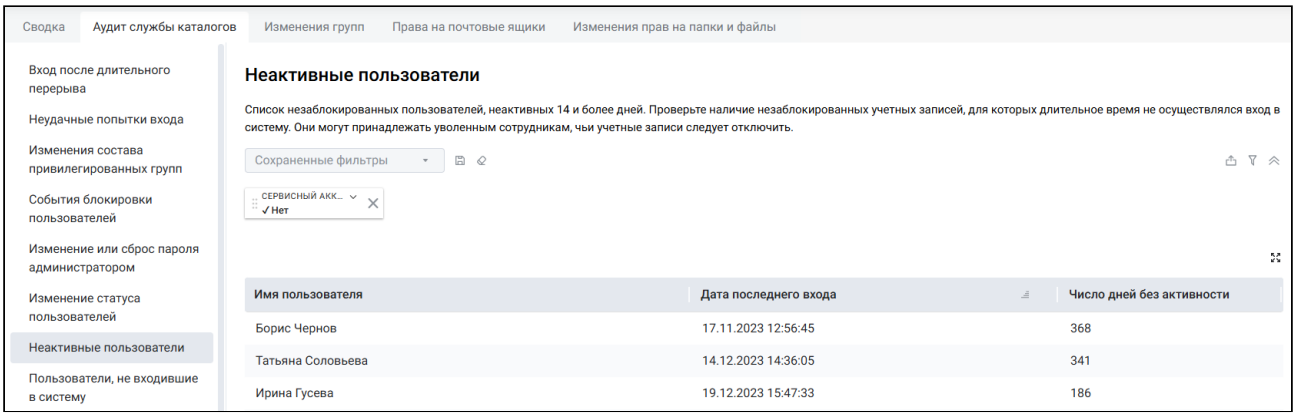
Виджет	Описание
	Построен на основе отчета *Неудачные попытки входа* со вкладки **Аудит службы каталогов** Доступны фильтры *Дата*, *Ошибка входа*
Вход после длительного перерыва 	Число непросмотренных событий входа в учетную запись после перерыва более 30 дней Построен на основе отчета *Вход после длительного перерыва* со вкладки **Аудит службы каталогов** Вы можете задать значение, начиная с которого цвет числа на виджете будет изменяться на красный Доступен фильтр *Дата входа*
Пользователи без пароля 	Число учетных записей пользователей с признаком "Пароль необязателен" Построен на основе отчета *Пользователи без пароля* со вкладки **Аудит службы каталогов** Вы можете задать значение, начиная с которого цвет числа на виджете будет изменяться на красный Доступен фильтр *Сервисный аккаунт*
Изменения групп 	Распределение событий изменения групп по датам Построен на основе данных со вкладки **Изменения групп** Доступен фильтр *Дата*
Изменения привилегированных групп 	Число непросмотренных событий изменения состава привилегированных групп Построен на основе отчета **Изменения состава привилегированных групп** со вкладки **Аудит службы каталогов** Вы можете задать значение, начиная с которого цвет числа на виджете будет изменяться на красный Доступен фильтр *Дата*

Чтобы задать пороговое значение, начиная с которого цвет числа на виджете будет изменяться на красный:

1. Справа от названия виджета нажмите  **Редактировать виджет**.
2. В окне **Редактировать виджет** введите необходимое число.
3. Нажмите **Сохранить**.

10.2 Вкладка "Аудит службы каталогов"

На вкладке представлены результаты автоматического аудита каталога Microsoft Active Directory. Доступны отчеты о состоянии учетных записей и событиях службы каталогов.



10.2.1 **Отчеты**

Вид отчета	Описание	Доступная информация	Доступный фильтр
Вход после длительного перерыва	Пользователи, для учетных записей которых разница между значениями признака *LastLogonDate* при последней и предыдущей синхронизациях превышает 30 дней. Среди таких пользователей могут быть уволенные сотрудники, чьи учетные записи не были отключены.	• *Дата входа* • *Имя пользователя* • *Дата предыдущего входа* • *Число дней без активности*	• *Дата входа* • *Просмотрено*
Неактивные пользователи	Незаблокированные пользователи, неактивные 14 и более дней. Учетные записи, для которых длительное время не осуществлялся вход в систему, могут принадлежать уволенным сотрудникам.	• *Имя пользователя* • *Дата последнего входа* • *Число дней без активности*	*Сервисный аккаунт*
Неактивные компьютеры	Незаблокированные компьютеры, неактивные 14 и более дней. Злоумышленники могут использовать такие компьютеры для несанкционированного входа в систему.	• *Дата последнего входа* • *Имя компьютера* • *Операционная система* • *Число дней без активности*	*Дата последнего входа*

Вид отчета	Описание	Доступная информация	Доступный фильтр
Пользователи, не входившие в систему	Пользователи, чьи учетные записи созданы 14 и более дней назад и которые ни разу не входили в систему. Такие учетные записи могут принадлежать злоумышленникам, пытающимся получить несанкционированный доступ к системе.	• *Имя пользователя* • *Статус пользователя* • *Дата создания* учетной записи	*Сервисный аккаунт*
Компьютеры, с которых не входили в систему	Компьютеры, для которых учетные записи были созданы 14 и более дней назад и откуда не выполнялся вход в систему. Злоумышленники могут использовать такие компьютеры для несанкционированного входа в систему.	• *Дата создания* учетной записи • *Имя компьютера* • *Статус компьютера*	*Дата создания*
Пользователи с постоянным паролем	Пользователи с учетными записями без указания срока смены пароля. Указывать срок смены пароля необязательно для служебных учетных записей. Убедитесь, что для остальных учетных записей указан срок смены пароля.	• *Имя пользователя* • *Статус пользователя* • *Дата создания* учетной записи • *Дата последнего входа*	*Сервисный аккаунт*
Пользователи без пароля	Пользователи с признаком *Пароль необязателен (Password Not Required)*. Среди них могут быть пользователи с пустым паролем.	• *Имя пользователя* • *Статус пользователя* • *Дата создания учетной записи* • *Дата последнего входа*	*Сервисный аккаунт*
Заблокированные пользователи	Автоматически заблокированные пользователи. Среди них могут быть пользователи, пытавшиеся осуществить подбор пароля или получить несанкционированный доступ другим способом.	• *Имя пользователя* • *Дата последнего входа*	*Сервисный аккаунт*
Пользователи с истекшим паролем	Пользователи с учетными записями, для которых истек срок смены пароля. Для таких учетных записей повышен риск подбора пароля или получения	• *Имя пользователя* • *Дата последней смены пароля* • *Дата создания* учетной записи	*Сервисный аккаунт*

Вид отчета	Описание	Доступная информация	Доступный фильтр
	несанкционированного доступа другим способом.	• *Дата последнего входа*	
Неудачные попытки входа	События неудачных попыток авторизации. Среди них могут быть инциденты подбора пароля или получения несанкционированного доступа другим способом.	• *Имя пользователя* • *Дата* попытки • *IP-адрес компьютера* • *Имя компьютера* • *Ошибка входа*	• *Дата* • *Ошибка входа*
Изменения состава привилегированных* групп	Изменения в группах с повышенным уровнем прав доступа. Любые изменения в составе таких групп могут свидетельствовать о возможных инцидентах безопасности.	• *Дата* события • *Имя измененной группы* • *Тип действия* • *Имя добавленного или удаленного пользователя/ группы* • *Кем изменено*	• *Дата* • *Просмотрено*
События блокировки пользователей	События автоматической блокировки пользователей. Среди таких пользователей могут быть те, кто пытался осуществить подбор пароля или получить несанкционированный доступ другим способом.	• *Имя пользователя* • *Дата* блокировки • *Дата последнего входа*	• *Имя пользователя* • *Дата блокировки*
Изменение или сброс пароля администратором	Пользователи, чей пароль был изменен администратором. Сброс пароля для пользователей с повышенными привилегиями может свидетельствовать об активности злоумышленников. **Примечание:** При создании нового пользователя в событиях аудита создается отдельное событие об изменении пароля. Такое событие, как правило, не свидетельствует о подозрительной активности.	• *Имя пользователя* • *Статус пользователя* • *Дата* события • *Кем изменено*	*Дата*
Изменение статуса пользователей	Действия администраторов с учетными записями пользователей: • создание учетной записи; • удаление учетной записи;	• *Имя пользователя* • *Дата* события • *Кем изменено* • *Тип действия*	• *Имя пользователя* • *Дата* • *Кем изменено*

Вид отчета	Описание	Доступная информация	Доступный фильтр
	• отключение учетной записи; • активация учетной записи; • разблокировка учетной записи. Такие изменения могут свидетельствовать о подозрительной активности.		• *Тип действия* • *Просмотрено*

Вы можете:

- скрыть меню вкладки;
- просматривать отчеты в полноэкранном режиме;
- отмечать события просмотренными;
- просматривать детали события.

Действия описаны в статье "Просмотр отчетов".

Кроме того, вы можете **фильтровать** записи в таблице по значениям столбцов, перечисленных в столбце **Доступный фильтр** таблицы **Отчеты**. Фильтры описаны в статье "Единый фильтр".

Вы также можете **сгруппировать** записи в отчетах по значениям следующих столбцов:

- *Статус пользователя*;
- *Имя измененной группы*;
- *Имя пользователя*;
- *IP-адрес компьютера*;
- *Имя компьютера*;
- *Имя добавленного или удаленного пользователя/группы*;
- *Тип действия*;
- *Кем изменено*;
- *Статус*.

Сортировка записей доступна по значениям всех столбцов, кроме:

- *Число дней без активности*;
- *Имя компьютера*.

* **Привилегированные группы**

Список групп службы каталогов Active Directory, действия с которыми отображены в отчете **Изменения состава привилегированных групп**:

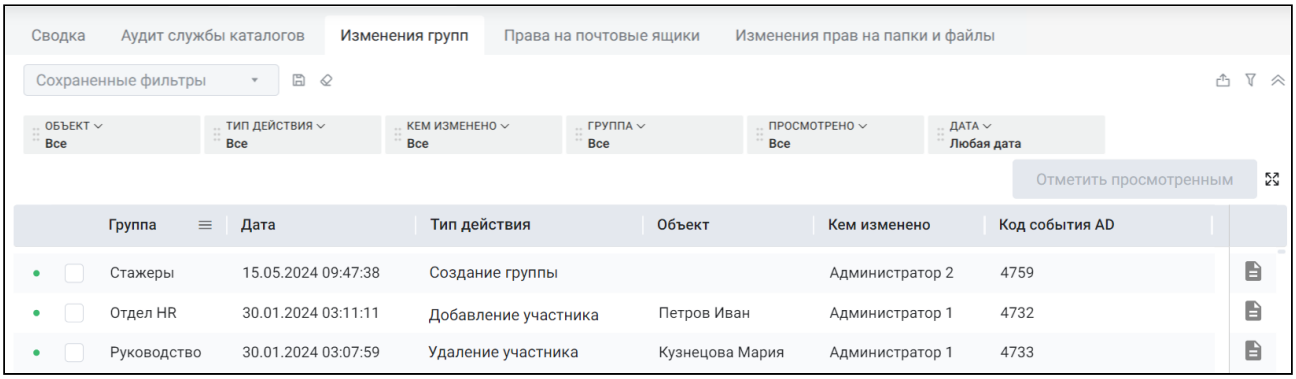
- *Account Operators*
- *Administrators*
- *Backup Operators*
- *Certificate Authority Server*
- *Delegated Setup*
- *DHCP Server*
- *Discovery Management*
- *DNS Server*
- *DNSAdmins*

- *Domain Admins*
- *Domain Controllers*
- *Enterprise Admins*
- *Enterprise Read-only Domain Controllers*
- *Exchange Organization Administrators*
- *Exchange Public Folder Administrators*
- *Exchange Recipient Administrators*
- *Exchange Servers*
- *Exchange Trusted Subsystem*
- *Exchange View-Only Administrators*
- *Group Policy Creator Owners*
- *Incoming Forest Trust Builders*
- *Managed Availability Servers*
- *Microsoft Exchange Server*
- *Microsoft Exchange Servers*
- *Network Configuration Operators*
- *Organization Management*
- *Power Users*
- *Print Operators*
- *Public Folder Management*
- *Read-only Domain Controllers*
- *Replicators*
- *Schema Admins*
- *Server Operators*
- *View-Only Organization Management*
- *WSUS Administrators*

10.3 Вкладка "Изменения групп"

На вкладке вы можете просмотреть все события, связанные с изменением групп. Данные представлены в виде таблицы со следующими столбцами:

- **Группа**, которая была изменена;
- **Дата** события;
- **Тип действия**: изменение атрибута группы, создание/удаление группы, добавление/удаление участника;
- **Объект** события – имя пользователя/группы, добавленного в состав группы или удаленного из нее;
- **Кем изменено** – имя пользователя, который внес изменения в группу;
- **Код события AD**;
- **Детали события**.



Вы можете:

- просматривать таблицу в полноэкранном режиме;
- отмечать события просмотренными;
- просматривать детали события.

Действия описаны в статье "Просмотр отчетов".

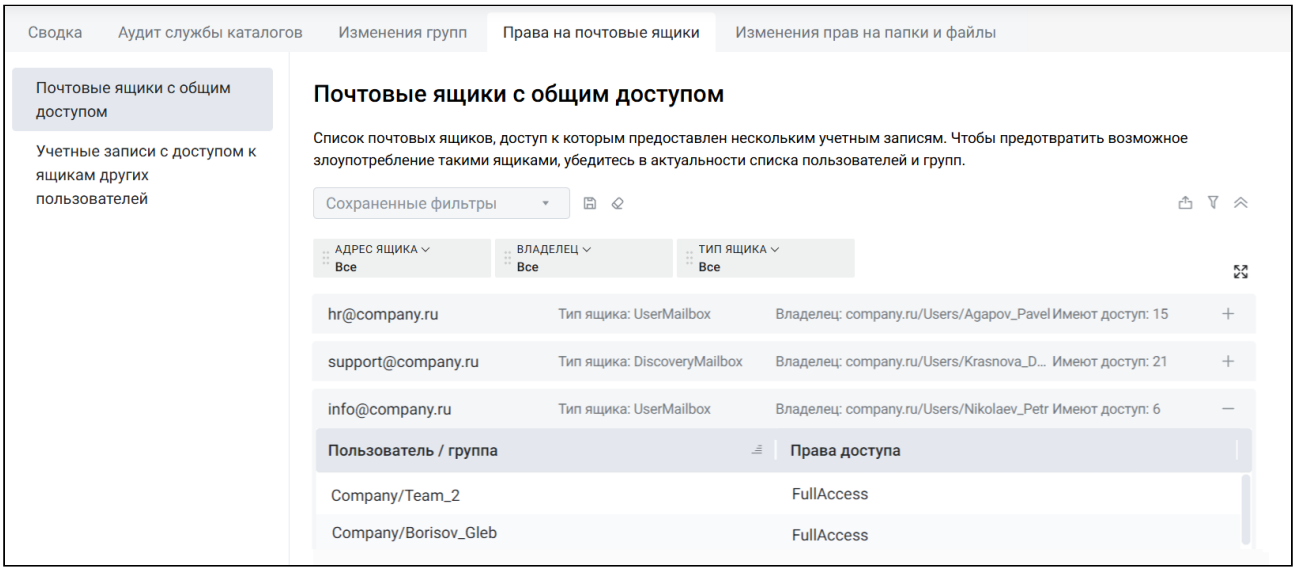
Кроме того, вы можете **фильтровать** записи в таблице по значениям столбцов: *Кем изменено*, *Объект*, *Группа*, *Тип действия*, *Просмотрено*, *Дата*. Фильтры описаны в статье "Единый фильтр".

Записи в таблице также могут быть **сгруппированы** или **отсортированы** по значениям следующих столбцов:

- *Группа*;
- *Кем изменено*;
- *Объект*;
- *Тип действия*.

10.4 Вкладка "Права на почтовые ящики"

На вкладке представлены отчеты о правах доступа пользователей и групп к почтовым ящикам Microsoft Exchange. При нажатии на любую строку отчета раскрывается дополнительный уровень отчета.



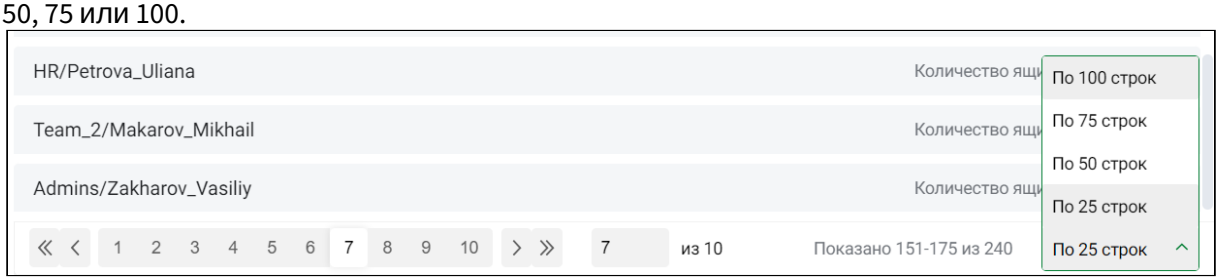
10.4.1 Отчеты

Вид отчета	Описание	Доступная информация	Фильтры
Почтовые ящики с общим доступом	Почтовые ящики, доступ к которым предоставлен нескольким учетным записям. Список пользователей и групп, имеющих доступ к таким ящикам, должен быть актуальным.	Основной уровень: • Адрес почтового ящика; • **Тип ящика**, например: *DiscoveryMailbox*, *UserMailbox*; • **Владелец**; • **Имеют доступ** – количество пользователей/групп, имеющих доступ к ящику. Дополнительный уровень: • **Пользователь/группа** – список всех пользователей/групп с доступом к ящику; • **Права доступа** – уровень доступа к ящику для каждого пользователя/группы.	• **Адрес ящика** • **Владелец** • **Тип ящика**
Учетные записи с доступом к ящикам других пользователей	Пользователи и группы, которым предоставлен доступ к почтовым ящикам других пользователей. Пользователь или группа должны иметь только необходимые права доступа.	Основной уровень • **Пользователь/группа**; • **Количество ящиков**, к которым учетная запись имеет доступ. Дополнительный уровень: • **Адрес ящика**, к которому учетная запись имеет доступ; • **Тип ящика**; • **Владелец** почтового ящика; • **Права доступа**.	• **Пользователь/группа**

Данные в отчетах представлены постранично. При помощи плашки под отчетом вы можете:

- выбрать номер страницы;
- перейти к первой, последней, следующей или предыдущей странице;

- из выпадающего списка выбрать количество строк для отображения на страницах: 25, 50, 75 или 100.



Кроме того, для удобства просмотра вы можете:

- скрыть меню вкладки;
- открывать отчеты в полноэкранном режиме;
- сортировать записи.

Действия представлены в статье "Просмотр отчетов".

Вы также можете **фильтровать** записи в таблице по значениям столбцов, перечисленных в столбце **Фильтры** таблицы **Отчеты.** Фильтры описаны в статье "Единый фильтр".

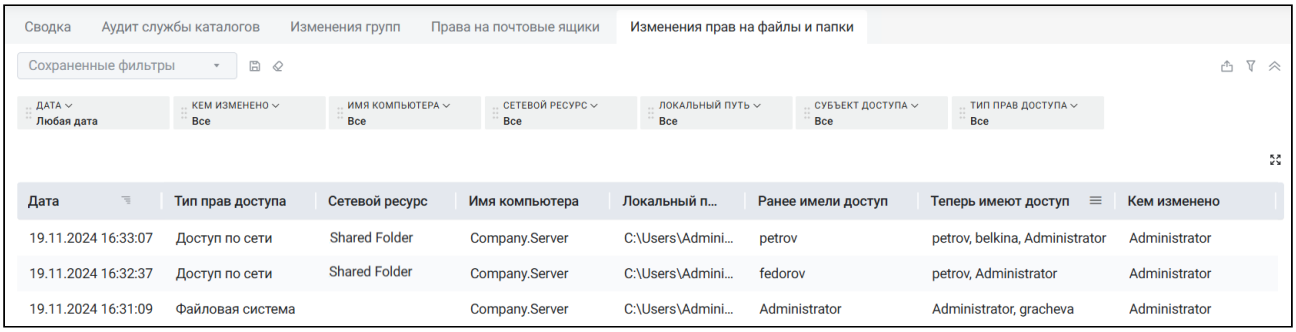
10.5 Вкладка "Изменения прав на файлы и папки"

На вкладке представлен отчет о событиях изменения списка учетных записей и групп, имеющих доступ к объектам файловой системы. Данные представлены в виде таблицы со следующими столбцами:

- **Дата** события;
- **Тип прав доступа**: *Файловая система* (код событий Active Directory 4670) или *Доступ по сети* (код 5143);

> **Примечание:**
>
> Учетная запись (группа) имеет доступ к файлу/папке только в том случае, если ей получены права как на уровне файловой системы, так и на уровне сетевого доступа. Выдача прав лишь одного из перечисленных типов не обеспечивает доступ к объекту. Поэтому фактической датой получения доступа считается дата, когда учетная запись (группа) получила права обоих типов.
>
> Обратите внимание, что учетной записи (группе) могли быть предоставлены права одного из типов до начала отслеживания изменений прав доступа системой IW Data Access Tracker. Такое событие не будет отображено в DAT.

- **Сетевой ресурс** – имя сетевой папки (отображается только для событий типа *Доступ по сети*);
- **Имя компьютера**, на котором произошли изменения;
- **Локальный путь** к папке;
- **Ранее имели доступ** – список учетных записей и групп, которые имели доступ к объекту до изменений;
- **Теперь имеют доступ** – список учетных записей и групп, которые получили доступ к объекту после изменений;
- **Кем изменено** – имя пользователя, внесшего изменения.



Действия с таблицей:

- Просмотр в **полноэкранном режиме** (см. "Просмотр отчетов");
- **Фильтрация** записей по значениям столбцов:
  - *Дата*
  - *Кем изменено*
  - *Сетевой ресурс*
  - *Имя компьютера*
  - *Тип прав доступа*
  - *Локальный путь*
  - *Субъект доступа*

  Фильтры описаны в статье "Единый фильтр";
- **Сортировка** записей по значениям столбца *Дата*.

10.6 Просмотр отчетов

Для удобства работы с отчетами вы можете:

- скрыть меню вкладки;
- просматривать отчеты в полноэкранном режиме;
- просматривать детали события;
- отмечать события просмотренными;
- группировать и сортировать записи.

10.6.1 Скрытие меню вкладки

Чтобы освободить место для просмотра отчетов, вы можете свернуть меню вкладок **Аудит службы каталогов** и **Права на почтовые ящики**. Для этого под списком отчетов нажмите « **Свернуть меню**.

10.6.2 Полноэкранный режим

Чтобы просматривать отчеты на вкладках в полноэкранном режиме, нажмите **Открыть на весь экран** .

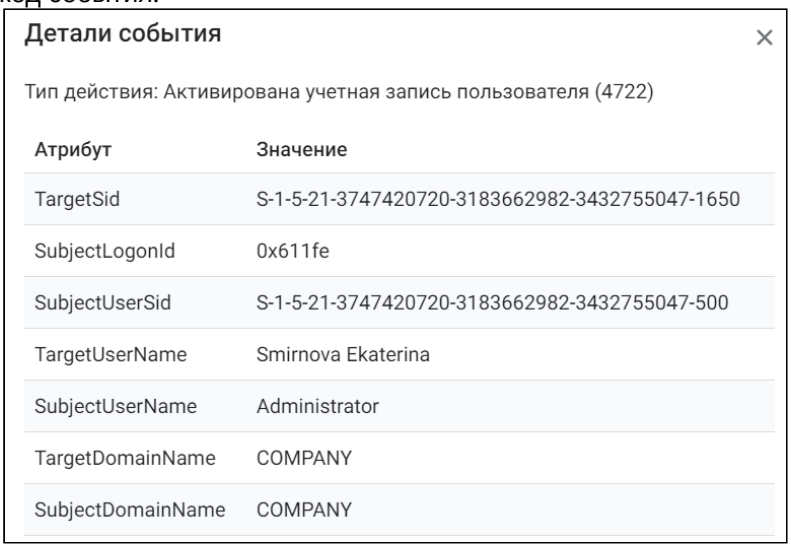
Чтобы выйти из полноэкранного режима, нажмите **Свернуть** .

10.6.3 Детали события

Вы можете просматривать детали событий:

- в отчете на вкладке **Изменения групп**;
- в отчетах на вкладке **Аудит службы каталогов**:
  - **Изменения состава привилегированных групп**;
  - **Изменение статуса пользователей**;
  - **События блокировки пользователей**;
  - **Изменение или сброс пароля администратором**;
  - **Неудачные попытки входа**.

Чтобы просмотреть подробную информацию из службы каталогов, нажмите **Детали события** в конце строки. Откроется окно с атрибутами события Microsoft Active Directory и их значениями, включая код события:



Чтобы выйти из режима просмотра, нажмите или кликните вне окна.

10.6.4 Статус события

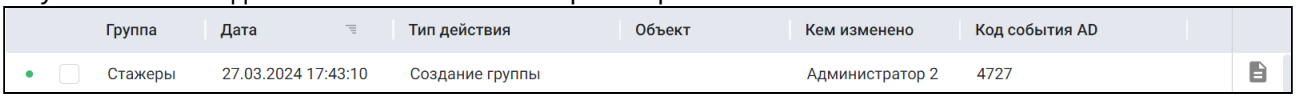
Вы можете отмечать события просмотренными/непросмотренными:

- в отчете на вкладке **Изменения групп**;
- в отчетах на вкладке **Аудит службы каталогов**:
  - **Вход после длительного перерыва**;
  - **Изменения состава привилегированных групп**;
  - **Изменение статуса пользователей**.

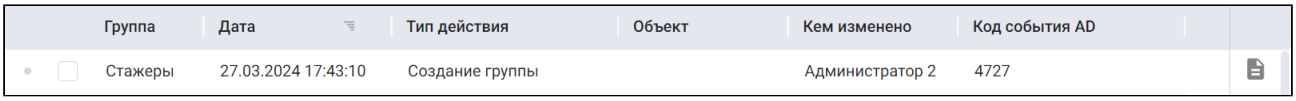
Слева от события отображается цветовой индикатор статуса:

- – непросмотренные события;
- – просмотренные события.

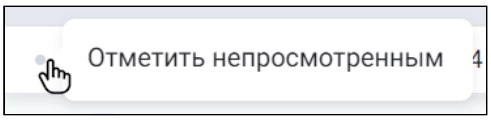
По умолчанию каждое событие считается непросмотренным:



Чтобы отметить событие просмотренным, кликните указателем мыши по индикатору. Цвет индикатора сменится, и запись будет отображаться как просмотренная:

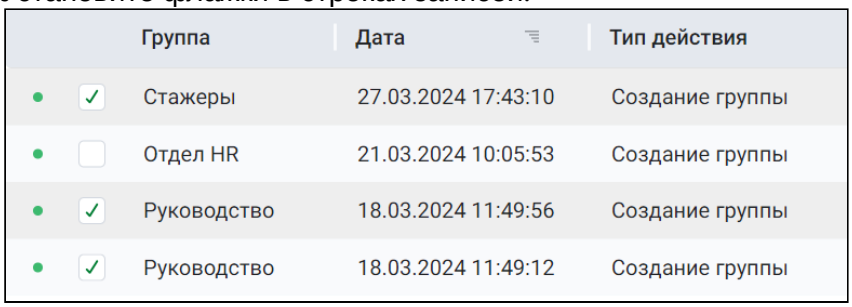


Аналогичным образом вы можете вернуть событию статус непросмотренного:



Чтобы отметить несколько событий как просмотренные:

1. Установите флажки в строках записей:



2. Над таблицей справа нажмите **Отметить просмотренным**.

10.6.5 Группировка и сортировка записей

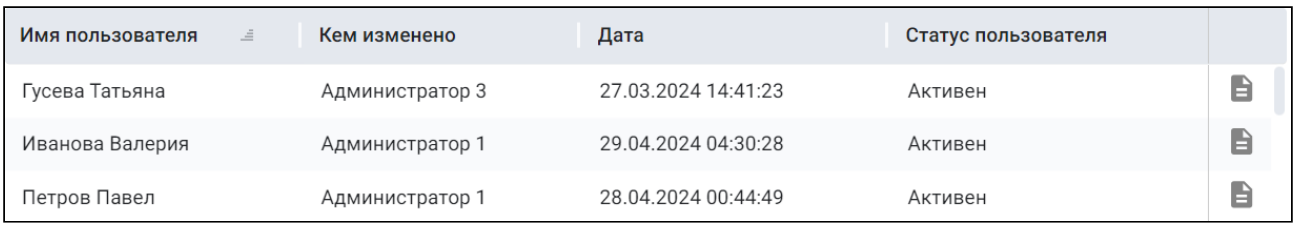
Сортировка записей

Данные в столбцах можно отсортировать по возрастанию/убыванию. Для столбцов, в которых данные отсортированы, справа от названия отображается значок  или .

Чтобы отсортировать значения в столбце таблицы:

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

Записи в таблице будут отсортированы по значениям этого столбца:



Чтобы отсортировать значения по двум и более столбцам:

1. Отсортируйте значения по приоритетному столбцу.

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

> **Пример:**
>
> Записи в отчете отсортированы по приоритетному (т. к. он расположен левее) столбцу **Кем изменено**. Записи во втором столбце отсортированы относительно первого столбца.

Кем изме...	Имя пользователя	Статус пользователя	Дата	
Администратор 1	Иванова Валерия	Активен	16.05.2024 11:03:38	
Администратор 1	Соколов Петр	Активен	16.05.2024 11:03:01	
Администратор 1	Цветков Василий	Активен	05.05.2024 11:12:23	
Администратор 2	Гусева Татьяна	Активен	12.04.2024 07:14:54	

Чтобы отменить сортировку:

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

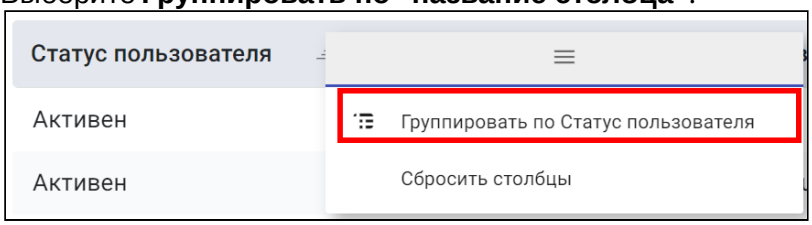
> **Примечание:**
>
> Для таблиц в отчете на вкладке **Права на почтовые ящики** недоступны сортировка по нескольким столбцам и кнопка **Сбросить столбцы**.

Группировка записей

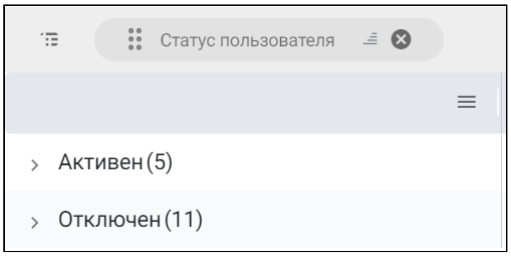
К записям в отчетах на вкладках **Аудит службы каталогов** и **Изменения групп** можно применить группировку.

Чтобы сгруппировать записи:

1. Наведите курсор на название столбца.
2. Нажмите на появившийся значок .
3. Выберите **Группировать по <название столбца>**:



В результате все события будут распределены по группам:



Множественная группировка

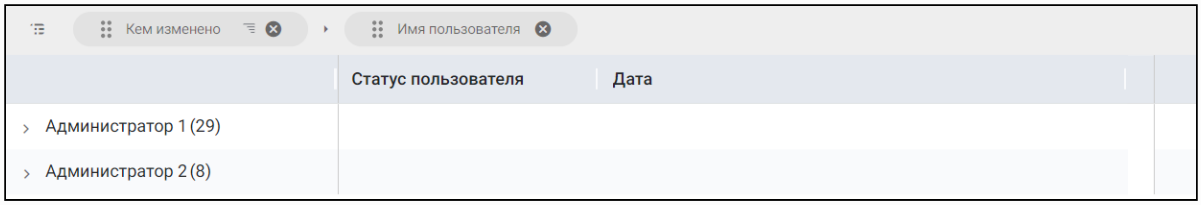
Для некоторых отчетов возможна группировка по нескольким столбцам. Для этого вам необходимо определить приоритет столбцов и применить группировку к каждому столбцу.

Примечание:

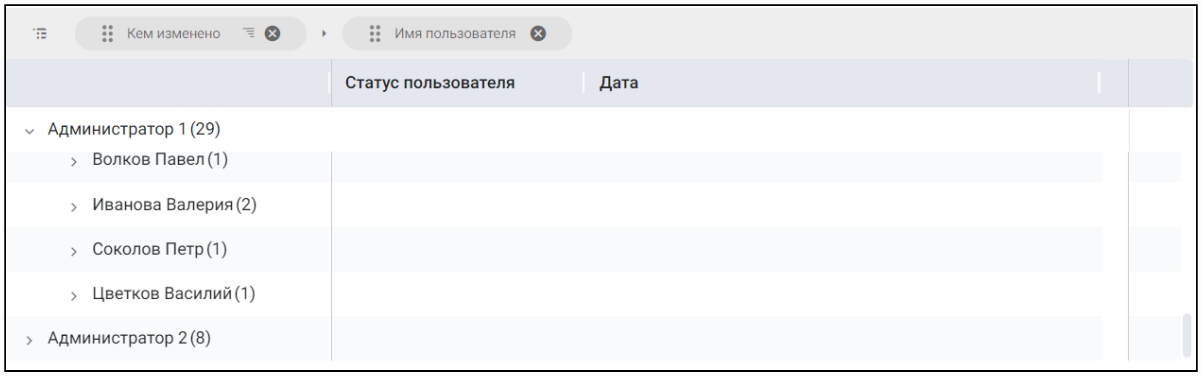
Приоритет столбцов определяется слева направо. Вы можете изменять порядок столбцов путем перетаскивания.

Пример:

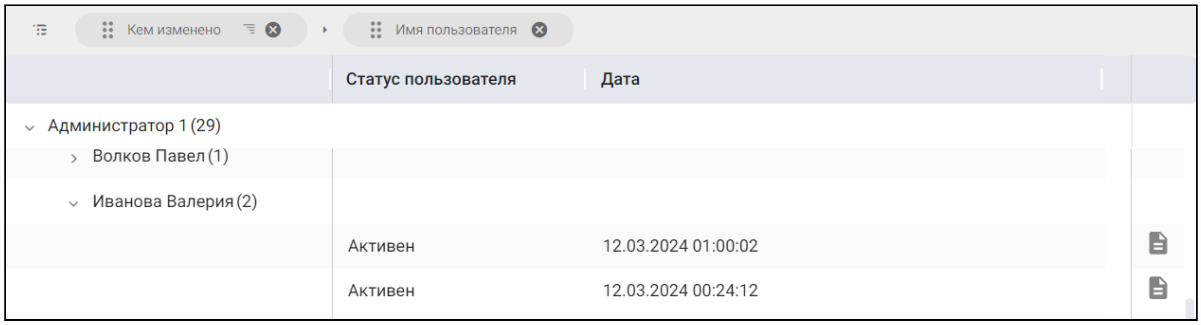
Записи в отчете **Изменение или сброс пароля администратором** на вкладке **Аудит службы каталогов** сгруппированы по столбцу **Кем изменено**: *Администратор 1* и *Администратор 2* с указанием количества записей в скобках:



Внутри группы пользователей, чьи учетные записи изменил *Администратор 1*, записи сгруппированы по столбцу **Имя пользователя**:



При раскрытии группы доступна информация по остальным столбцам каждой записи:



Чтобы отменить группировку:

- на плашке с названием столбца над таблицей с записями нажмите
или
- нажмите на значок , появляющийся при наведении курсора на название столбца, и выберите **Сбросить столбцы**.

10.7 Выгрузка отчетов

Вы можете выгрузить в XLSX-отчет и сохранить себе на компьютер информацию, представленную на следующих вкладках раздела **Инфраструктура**:

- **Аудит службы каталогов**
- **Изменения групп**
- **Права на почтовые ящики**
- **Изменения прав на файлы и папки**

Вы также можете настроить регулярную отправку файлов с отчетами на почту.

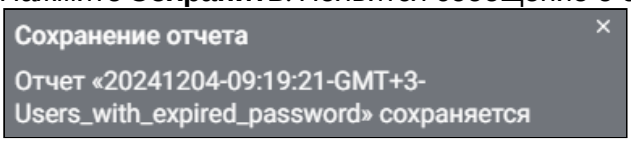
Чтобы выгрузить данные:

1. При необходимости настройте фильтры и отсортируйте записи. В отчет будут выгружены данные в выбранном представлении.

   > **Примечание:**
   >
   > Если после фильтрации таблица содержит более 10 000 записей (на вкладке **Права на почтовые ящики** – учитывая записи дополнительного уровня), то в отчет добавляются только первые 10 000 записей.
   >
   > На вкладке **Права на почтовые ящики** в выгрузку добавляются записи только с выбранной страницы отчета.

2. В правой верхней области над отчетом нажмите .
3. Выберите **Выгрузить отчет**.
4. В окне **Выгрузка отчета** определите состав файла:
   a. Чтобы добавить лист с дополнительной информацией в отчет, в списке установите флажок в опцию **Дополнительная информация**. Лист содержит:
      - дату и время формирования отчета;
      - настройки фильтров;
      - ссылку для перехода в Консоль управления.

b. Добавьте в файл основные данные отчета, установив флажок рядом с названием отчета.
c. Нажмите **Сохранить**. Появится сообщение о сохранении отчета:



5. Перейдите в раздел **Отчеты** → **Архив отчетов**. Подробнее см. Раздел "Отчеты".
6. На строке с названием файла отчета нажмите , чтобы сохранить файл на ваш компьютер.

10.7.1 Отправка отчетов по расписанию

Вы можете настроить регулярную отправку отчетов на почту:

- на вкладке **Аудит службы каталогов** для отчетов:
  - *Вход после длительного перерыва*;
  - *Неудачные попытки входа*;
  - *Изменения состава привилегированных групп*;
  - *События блокировки пользователей*;
  - *Изменение или сброс пароля администратором*;
- для отчета на вкладке **Изменения групп**.

Для этого:

1. При необходимости настройте фильтры и отсортируйте записи. В отчет будут выгружены данные в выбранном представлении.

> **Примечание:**
>
> Если после фильтрации таблица содержит более 10 000 записей, то в отчет добавляются только первые 10 000 записей.

2. В правой верхней области над отчетом нажмите .
3. Выберите **Настроить регулярную отправку**.
4. В окне **Выгрузка отчета** определите состав файла:
   a. Чтобы добавить лист с дополнительной информацией в отчет, выберите в списке **Дополнительная информация**. Лист содержит:
      - дату и время формирования отчета;
      - настройки фильтров;
      - ссылку для перехода в Консоль управления.
   b. Добавьте в файл основные данные отчета, установив флажок рядом с названием отчета.
5. Также задайте параметры отправки:

Параметр	Описание
Период формирования отчета	Укажите, за какой период необходимо отправлять отчет: • *Последние сутки* • *Текущий день*

Параметр	Описание
	• *Последние 3 дня* • *Последние 7 дней* • *Последние 30 дней*
Получатели	Укажите получателей отчета
Частота отправки	Укажите, с какой периодичностью Офицеру необходимо получать отчет: • *Каждый день* • *Каждую неделю* Вы можете выбрать дни недели, по которым Система будет отправлять отчеты. • *Каждый месяц* Отчет будет отправляться первого числа месяца, следующего за отчетным.
Время	Укажите время отправки отчета

6. Нажмите **Сохранить**. Будет создана задача на регулярную отправку. Список задач вы можете просмотреть в разделе **Отчеты** на вкладке **Задачи на регулярную отправку**. Подробнее см. "Задачи на регулярную отправку".

Важно!

Для регулярной отправки отчетов в Центре расследований должно быть настроено соединение с почтовым сервером. Подробнее см. документ "*InfoWatch Data Access Tracker. Руководство администратора*", статью "Сервисы для уведомлений".

Примечание:

Вы также можете настроить отправку уведомлений (без отчетов):

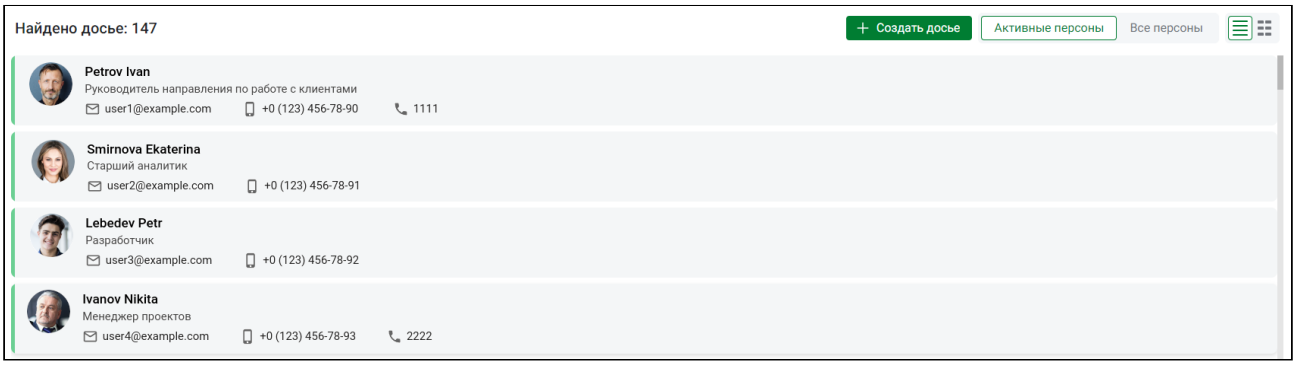
- ежедневных об изменениях в группах службы каталогов домена;
- мгновенных об изменениях состава привилегированных групп.

Подробнее см. документ "*InfoWatch Data Access Tracker. Руководство администратора*", статью "Почтовые уведомления".

11 Раздел "Персоны"

Раздел содержит справочник персон, данные которых загружены в Систему при синхронизации с Active Directory или Traffic Monitor, и персон, данные которых внесены вручную.

Для просмотра досье персоны выберите ее левой кнопкой мыши. Для возврата к списку персон нажмите  в левом верхнем углу рабочей области.



В списке персон отображаются только персоны, удовлетворяющие условиям Единого фильтра. Для настройки отображения досье используйте кнопки в правой части рабочей области:

- **Активные персоны** – отобразить досье только сотрудников с активной учетной записью в Active Directory и хотя бы одним событием;

  > **Примечание:**
  >
  > Если у персоны нет событий, либо она заблокирована/удалена в AD, то такая персона считается неактивной и отображается в списке **Все персоны**.
  >
  > Для просмотра активных персон используйте фильтры. Если ни в одном фильтре не выбрано ни одно значение, Система не выведет список активных персон.

- **Все персоны** – отобразить досье всех персон, включая когда-либо работавших в компании;
-  – отображать в виде таблицы;
-  – отображать в виде плитки.

В этом разделе также доступны следующие действия:

- Просмотр досье персоны
- Просмотр и настройка виджетов персональной информации
- Создание, редактирование и удаление досье
- Добавление контактов персоны
- Изменение руководителя персоны
- Объединение досье
- Выгрузка статистики в досье персоны

11.1 Вкладка "Персональная информация"

Виджеты на вкладке **Персональная информация** позволяют Офицеру безопасности просмотреть все данные о персоне, хранящиеся в Системе.

Название виджета	Описание
Руководитель	Отображает список руководителей персоны, а также позволяет задать руководителя вручную.
Контакты	Позволяет управлять контактами персоны, а также отображает контакты, загруженные из подключенных источников.
Общая информация	Отображает состояние персоны в различных источниках: дата приема, стаж работы, рабочее место, дата увольнения.
Статусы	Отображает статусы персоны, назначенные ей в Traffic Monitor.
Описание	Отображает описание персоны, позволяет задавать и редактировать его вручную.

Чтобы развернуть виджет на весь экран, нажмите .

Чтобы отредактировать данные на виджете, нажмите .

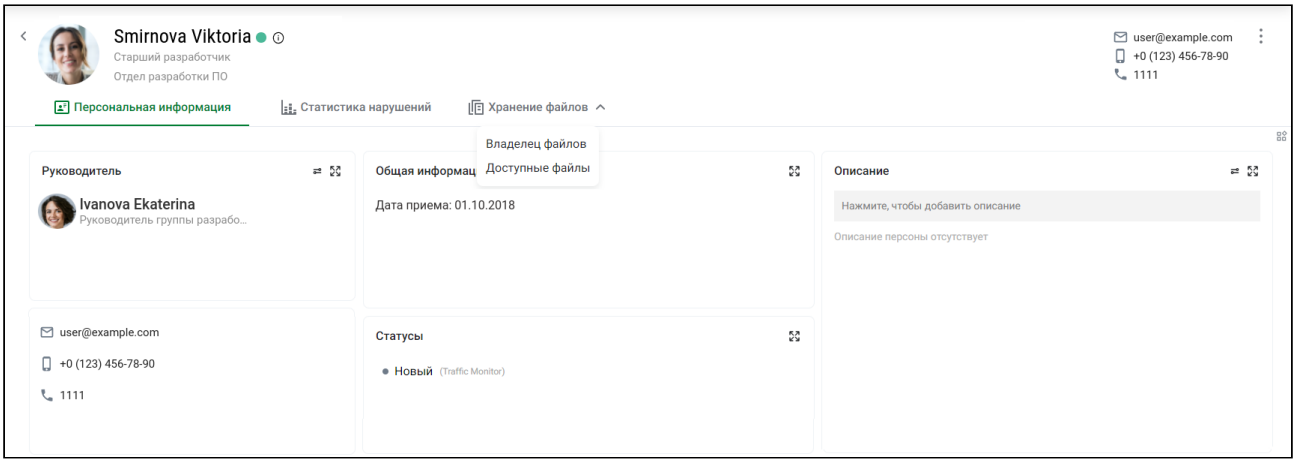
11.2 Просмотр досье персоны

Досье содержит информацию о конкретном сотруднике в организации.

В Досье персоны отображается:

- ФИО сотрудника;
- Должность;
- Отдел;
- Контакты: учетная запись из Active Directory вида *login@company.com*, личные или рабочие контакты персоны, включая адрес электронной почты, номер телефона, номер мобильного телефона.

> **Примечание:**
>
> Все персоны, добавленные при интеграции с Active Directory, имеют тип контакта SID, используемый для их идентификации.



Справа от имени персоны отображается цветовой индикатор статуса:

- – активные сотрудники, в том числе персоны, добавленные вручную, а также персоны, у которых истек срок действия учетной записи в AD, но статус в AD остается Активным;
- – сотрудники, отключенные в AD или имеющие неопределенный статус.

Нажмите на иконку справа от имени персоны, чтобы увидеть:

- дату создания досье;
- дату обновления досье;
- владельца досье – Система или Офицер безопасности (если досье было добавлено вручную).

Чтобы изменить данные в досье, используйте кнопку в правой части рабочей области (подробнее см. "Создание, редактирование и удаление досье").

Информация в досье персоны представлена на вкладках:

- **Персональная информация** – содержит виджеты досье, специфичные для персоны: **Общая информация**, **Руководитель**, **Контакты**, **Статусы**, **Описание** (см. "Вкладка "Персональная информация");
- **Статистика нарушений** – виджеты статистики, относящиеся к персоне (см. "Виджеты статистики").

> **Примечание:**
>
> Выше указаны вкладки, доступные при установке DAT.
>
> Набор вкладок в досье персоны зависит от продуктов, установленных в кластере Центра расследований.

Чтобы вернуться к списку персон, нажмите в верхнем левом углу рабочей области.

11.3 Создание, редактирование и удаление досье

Чтобы создать досье новой персоны или дополнительное досье существующей в Системе персоны:

1. Перейдите в раздел **Персоны**.
2. Нажмите **+ Создать досье**.
3. Заполните персональные данные:
    - Имя персоны
    - Должность в организации
    - Отдел, где работает персона
    - Дополнительное описание
4. Добавьте фотографию.
5. Добавьте контактные данные персоны: личный или рабочий номер телефона, адрес электронной почты, аккаунты в социальных сетях.
6. Нажмите **Создать досье**. Новое досье будет доступно в списке досье сотрудников.

Чтобы внести изменения в досье:

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

Чтобы удалить досье:

1. Откройте досье.
2. Нажмите  в правом верхнем углу и выберите **Удалить**.
3. Нажмите **Ок**. Досье будет удалено без возможности восстановления.

11.4 Объединение досье

Вы можете объединить два или несколько досье в одно. При этом новое досье будет содержать всю информацию из досье, существовавших до объединения. Для этого:

1. Откройте досье, которое требуется объединить с другими.
2. Нажмите  и выберите **Объединить досье**.
3. В открывшемся окне в поле **Объединить с** выберите для объединения одно или несколько досье из списка.
4. Нажмите **Объединить**.

11.5 Добавление контактов персоны

При синхронизации с Active Directory и InfoWatch Traffic Monitor становятся доступны контакты персон: номера телефона, адреса электронной почты, аккаунты в социальных сетях (при синхронизации с TM) и прочее. При этом вы можете добавить дополнительные контакты вручную. Для этого:

1. Перейдите в досье персоны.
2. На вкладке **Персональная информация** на виджете **Контакты** нажмите .
3. В открывшемся окне будут отображены все автоматически добавленные при интеграции из других систем контакты персоны. При этом по умолчанию показаны по

одному контакту типа: логин в домене, телефон, электронная почта, мобильный телефон.
Нажмите **Добавить контакт**.

4. Укажите тип контакта (например, личный номер телефона) и введите его значение. Вы также можете:
   - добавить несколько позиций;
   - оставить комментарий к контакту, нажав .
5. Нажмите **Сохранить**. Новый контакт доступен в досье. Наличие комментария к контакту отмечается значком . Чтобы прочитать комментарий, нажмите на него.

11.6 Изменение руководителя персоны

На вкладке **Персональная информация** на виджете **Руководитель** указан руководитель персоны. Данная информация добавляется при синхронизации с Active Directory и InfoWatch Traffic Monitor.

Офицер безопасности может изменить руководителя персоны, который был добавлен вручную. Руководитель персоны, загруженный из системы-источника, не редактируется.

Чтобы изменить руководителя:

1. На виджете нажмите .
2. В открывшемся окне **Изменение руководителя** в поле *Добавлено вручную* введите имя нового руководителя из числа персон, зарегистрированных в Системе. Допускается добавить несколько имен.
3. Нажмите **Сохранить**. На виджете **Руководитель** отображаются указанные руководители.

Для перехода в досье руководителя щелкните левой клавишей мыши на его имени на виджете **Руководитель**.

11.7 Выгрузка статистики в досье персоны

В досье персоны вы можете выгрузить статистику активности персоны (виджеты вкладки **Статистика нарушений** раздела **Аналитика**) в виде файла в формате XLSX. Для этого:

1. В досье персоны, по которой требуется сформировать отчет, перейдите на вкладку **Статистика нарушений**.
2. Выберите виджеты и настройте фильтры, чтобы Система отобразила необходимую информацию.
3. В правом верхнем углу экрана нажмите  и нажмите **Выгрузить отчет**.
4. В окне **Выгрузка отчета** выберите виджеты, которые необходимо включить в отчет.
   - Вы можете включить в отчет сразу все виджеты для выгрузки, выбрав  **Выбрать все**.
   - Если необходимо включить в отчет только определенные виджеты, выберите  их из списка.
5. Нажмите **Сохранить**. На экране отобразится сообщение о том, что идет процесс сохранения отчета.
6. Перейдите в раздел **Отчеты**.
7. Выберите и скачайте отчет. Файл с отчетом будет сохранен в папку **Загрузки**.

Загруженный отчет представляет собой файл, который содержит несколько листов – по количеству виджетов. Подробнее скачивании отчета и о данных, представленных в отчете, см. "Формирование, выгрузка и печать отчетов с данными статистики".

12 Раздел "Расследования"

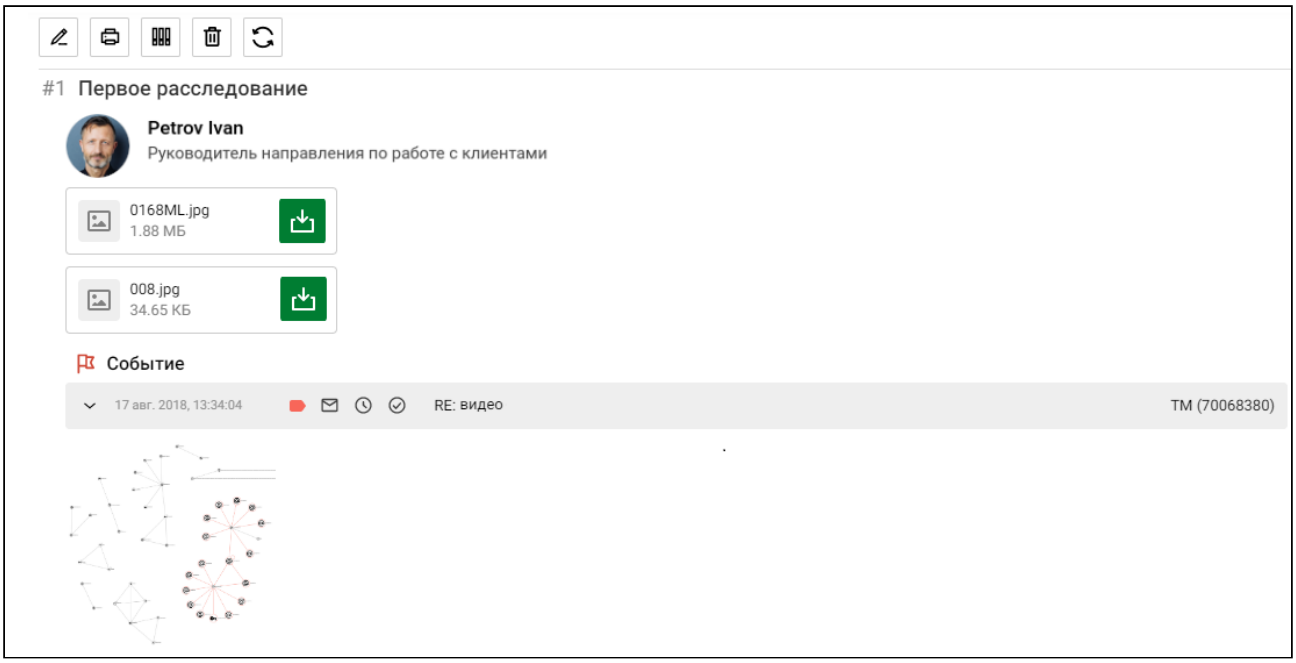
В этом разделе вы можете накапливать собранную из разных источников информацию и обобщать в расследования для последующего принятия решений или формирования отчетов. Сбор материалов и проведение расследования происходит следующим образом:

1. Система представляет факты нарушения политик в виде событий.
2. Офицер безопасности вручную добавляет такие события в расследование. При необходимости дает описания, прикрепляет файлы, снимки экрана, а также досье персон, подозреваемых в нарушении.
3. К расследованию подключаются другие Офицеры безопасности, вносят свои комментарии, прикладывают другие материалы, таким образом оперативно обмениваясь информацией.
4. По результатам расследования накопленная информация оформляется ими в виде отчета.

На панели навигации находится список всех открытых расследований и архив – база расследований, работа с которыми в данный момент не ведется.

На рабочей области отображается карточка выбранного расследования, которая может включать:

- ссылки на досье персон, имеющих отношение к расследованию;
- карточки события Traffic Monitor из раздела **События**;
- файлы-вложения различных форматов;
- графические файлы;
- текстовый комментарий в свободной форме.



Чтобы подробнее ознакомиться с приложенными материалами, можно:

- нажать на ссылку досье и перейти в раздел **Персоны**;
- нажать  и скачать на жесткий диск приложенный файл-вложение;
- раскрыть карточку события и ознакомиться с расширенной информацией по нему;
- просмотреть графические файлы.

Для удобства порядок следования материалов в карточке расследования можно менять. Для этого зажмите  и перетащите материал в нужное место. Чтобы удалить неактуальный материал из расследования, нажмите  напротив него и выберите **Удалить**.

Чтобы обновить состояние карточки расследования, нажмите .

Действия пользователя:

- Создание и архивирование расследования
- Добавление событий в расследование
- Добавление материалов в расследование
- Совместное проведение расследования
- Редактирование, выгрузка, печать и удаление расследования

12.1 Создание и архивирование расследования

Чтобы создать расследование:

1. На панели навигации слева нажмите .
2. В открывшемся окне введите наименование для нового расследования.
3. Нажмите **Сохранить**. Карточка нового расследования будет открыта для добавления материалов.

Чтобы в процессе работы над расследованием другой пользователь случайно не отредактировал данные, заархивируйте расследование. Также следует архивировать расследование после его окончания.

Чтобы поместить расследование в архив:

1. Перейдите в расследование на панели навигации.
2. Нажмите .
3. Подтвердите действие, нажав **Поместить в архив**. При этом вы сможете просматривать расследование в архиве без возможности внесения изменений.

Чтобы вернуться к работе над архивированным расследованием:

1. Выберите архив.
2. Нажмите .
3. Подтвердите действие, нажав **Разархивировать**. После этого вы сможете вносить изменения в расследование.

12.2 Добавление материалов в расследование

Для проведения расследования необходимо собрать материалы в как можно более полном объеме. Для этого:

1. Перейдите в карточку расследования на панели навигации.
2. В рабочей области вы можете добавить различные виды материалов в расследование:
   - **Текстовый комментарий** – для этого:
     a. Введите в строке комментарий в свободной форме.
     b. Если необходимо, отформатируйте текст комментария с помощью встроенных стандартных инструментов. Они станут доступны по двойному клику указателем мыши на тексте комментария.

c. Нажмите **Enter**, чтобы сохранить комментарий.

- **Ссылку на досье персоны** – для этого:
  a. Нажмите .
  b. В открывшемся окне выберите досье и нажмите **Применить.**
- **Файлы-вложения** – для этого:
  a. Нажмите .
  b. Выберите на диске компьютера один или несколько файлов любого формата и нажмите **Открыть**. Процесс может занять некоторое время и зависит от размера файлов. За один раз можно загрузить до 10 файлов общим размером до 100 МБ. Выбранные файлы будут прикреплены к расследованию. Просмотреть их можно после скачивания на жесткий диск любым из допущенных к расследованию Офицеров безопасности.
- **Графические файлы** – для этого:
  a. Нажмите .
  b. Выберите на жестком диске компьютера один или несколько графических файлов с расширениями JPG, JPEG, PNG, WebP, GIF и нажмите **Открыть**. Файлы будут отображены в карточке в режиме предварительного просмотра.
- **Ссылку на событие Traffic Monitor** (подробнее см. "Добавление событий в расследование").

12.3 Совместное проведение расследования

Одной из основных возможностей достижения высокой эффективности в расследованиях является коллективная работа над ними. Для этого реализовано совместное редактирование любого расследования. При этом стоит учитывать, что Система реагирует на совместные действия следующим образом:

Действия	Реакция Системы
Первый Офицер безопасности открыл на просмотр расследование, и в этот же момент другой ОБ добавил новый материал.	Первому ОБ придет сообщение, что расследование было изменено. Первый ОБ будет иметь возможность сохранить свои изменения поверх изменений второго ОБ, и все внесенные ими изменения будут объединены.
Второй Офицер безопасности отредактировал и сохранил объект, который первый ОБ ранее удалил.	Второй ОБ получит уведомление о невозможности сохранить изменения, так как удаленный материал уже недоступен.

12.4 Редактирование, выгрузка, печать и удаление расследования

Чтобы поменять название расследования:

1. Перейдите в карточку расследования.
2. Нажмите .
3. Введите новое название и нажмите **Сохранить**.

Чтобы выгрузить или распечатать карточку расследования:

1. Перейдите в карточку расследования.
2. Нажмите .
3. Выберите действие:
    - Распечатать PDF-документ. Информация, содержащаяся в карточке, будет распечатана с помощью стандартных средств браузера.
      или
    - Сохранить архив на жестком диске. Архив содержит PDF-документ с текстовым содержимым расследования и файлы вложений.

Чтобы удалить расследование:

1. Перейдите в карточку расследования.
2. Нажмите .
3. Подтвердите действие, нажав **Удалить**. Удалить расследование может только его автор.

13 Раздел "Отчеты"

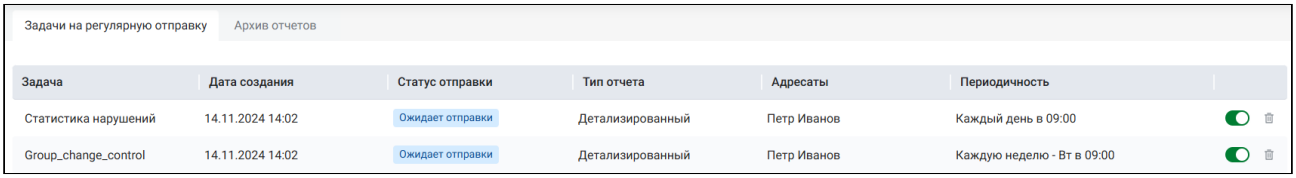
В разделе вы можете:

- просматривать список отчетов и скачивать отчеты на вкладке **Архив отчетов**;
- просматривать и редактировать список задач на регулярную отправку на вкладке **Задачи на регулярную отправку**.

13.1 Задачи на регулярную отправку

Список задач на регулярную отправку содержит следующие поля:

- **Задача** – название отчета, для которого создана задача на отправку;
- **Дата создания** – дата и время, когда был создана задача на отправку;
- **Статус отправки**;
- **Тип отчета** – детализированный;
- **Адресаты** – Офицер безопасности, который получает отчет;
- **Периодичность** – дни недели и время, когда Офицер безопасности получает отчет.



На вкладке **Задачи на регулярную отправку** вы можете:

- **Изменить название задачи**. Для этого нажмите на текущее название задачи и введите новое.
- **Отключить отправку отчета** на заданный период. Для этого воспользуйтесь кнопкой .
- **Удалить задачу**. Для этого:
  1. В строке задачи нажмите .
  2. В открывшемся диалоговом окне нажмите **ОК**. Задача будет удалена.

13.2 Архив отчетов

На вкладке представлена таблица с файлами всех отчетов, созданных в Центре расследований.

Для каждого отчета указаны:

- название;
- размер;
- дата и время формирования.

Чтобы скачать отчет, нажмите  напротив него. Отчет будет сохранен в папку **Загрузки** вашего компьютера. Подробнее о выгрузке отчетов см. "Формирование, выгрузка и печать отчетов с данными статистики", "Просмотр и выгрузка данных событий".

В архиве могут содержаться отчеты разных установленных продуктов InfoWatch и только одного пользователя. Список содержит последние 500 отчетов. Скачать файлы можно в течение 30 дней после

их формирования. В случае, если количество файлов в списке превысит 500, Система удалит файлы, созданные первыми.

Для удобства просмотра вы можете изменять ширину столбцов таблицы.

14 Пользовательское лицензионное соглашение

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями настоящего Лицензионного соглашения с конечным пользователем (далее – «Соглашение») перед началом работы с программным обеспечением. Установка и/или использование программного обеспечения означает ваше полное и безоговорочное согласие со всеми условиями настоящего Соглашения.

Если вы не согласны с условиями настоящего Соглашения, или если вы заключаете настоящее Соглашение от имени юридического лица, но у вас нет таких полномочий, вы должны прервать установку и/или прекратить использование программного обеспечения и удалить его копии.

1. Предоставление лицензии

1.1. Настоящее Лицензионное соглашение с конечным пользователем является договором присоединения, заключаемым между вами и ООО «Лаборатория ИнфоВотч», ИНН 7734583888 (далее – «Правообладатель»).

1.2. По настоящему Соглашению вам на условиях личной, не подлежащей передаче неисключительной лицензии предоставляются права на использование программного обеспечения Правообладателя (далее — «ПО»), а именно права загрузки, установки, резервного копирования и использования программного обеспечения по функциональному назначению в соответствии с условиями, указанными в Документации к ПО (Руководстве Пользователя, Руководстве Администратора, Руководстве по установке), настоящем Соглашении и Договоре, заключенном между вами и вашим лицензиаром. Документация к ПО признается частью настоящего Соглашения.

1.3. В случае если вы получили, загрузили и/или установили ПО, предназначенное для ознакомительных целей, вы имеете право использовать ПО только в целях ознакомления и только в течение ознакомительного периода. Любое использование ПО для других целей или по завершении ознакомительного периода запрещено.

1.4. Если вы используете ПО разных версий или версии ПО для разных языков, если вы получили ПО на нескольких носителях, если вы иным способом получили несколько копий ПО или получили ПО в составе пакета другого программного обеспечения, то общее число используемых вами лицензий не должно превышать их количества, определенного Договором между вами и вашим лицензиаром.

1.5. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Такая копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.

1.6. Вы самостоятельно несете ответственность и обеспечиваете соблюдение применимого экспортного и импортного законодательства, а также применимых торговых санкций и эмбарго в отношении передачи прав и использования ПО.

2. Условия использования

2.1. Программное обеспечение предназначено исключительно для использования в целях анализа и контроля информационных потоков в корпоративной среде, в том числе, для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.

2.2. Вы обязаны использовать ПО исключительно в соответствии с применимыми к вам требованиями законодательства Российской Федерации и иных стран, которые, не ограничиваясь, могут включать:

- законодательство о персональных данных;
- законодательство о коммерческой тайне;
- законодательство о противодействии неправомерному использованию инсайдерской информации;
- законодательство о противодействии коррупции;
- законодательство о критической информационной инфраструктуре;
- законодательство о государственных информационных системах;

- законодательство о защите данных в Национальной платежной системе;
- нормы Трудового кодекса РФ;
- а также иные применимые источники права.

2.3. Вы не вправе использовать ПО для любых целей или любым способом, нарушающим применимое законодательство, настоящее Соглашение и/или права третьих лиц. Правообладатель не несет ответственность за нарушение вами условий настоящего пункта.

2.4. Если вы не являетесь резидентом РФ, вы обязаны использовать ПО в соответствии с применимым правом, включая законы и нормативные акты, регламентирующие защиту персональных данных и коммерческой тайны.

2.5. Во избежание нарушения вами статей 138, 138.1 УК РФ, статьи 23 Конституции РФ и иных правовых норм перед началом использования программного обеспечения вам рекомендовано письменно проинформировать сотрудников о том, что:

- на рабочей станции используется данное ПО, о функциональности данного ПО и о данных, которые могут быть получены в результате применения данного ПО;
- рабочая станция и используемые каналы связи (электронная почта, локальная корпоративная сеть, телефония и IP-телефония и прочее) являются вашей собственностью и передаются им во временное пользование для выполнения служебных обязанностей;
- вся информация, созданная на рабочей станции, является вашей собственностью и подлежит контролю и логированию на законных основаниях.

2.6. Обращаем ваше внимание, что вам необходимо получить согласие лиц, данные которых будут обрабатываться при использовании ПО, на соответствующий сбор, хранение, использование, обработку, распространение и иную обработку указанных данных.

2.7. Напоминаем, что установка программы на компьютере другого лица без его ведома, получение личной информации третьих лиц без их ведома, нарушение неприкосновенности частной жизни, нарушение тайны переписки, телефонных переговоров, телеграфных и иных видов сообщений является уголовно наказуемым деянием и преследуется в соответствии с действующим законодательством Российской Федерации.

2.8. Правообладатель не имеет доступа к данным, созданным и/или полученным в рамках использования вами ПО. Вы имеете исключительный доступ к указанным данным. С учетом этого Правообладатель не осуществляет сбор, хранение, использование и распространение указанных данных.

2.9. Вы самостоятельно несете риск того, что данные, созданные и/или полученные в рамках использования вами ПО, могут содержать данные неэтического и/или противоправного характера, компьютерные вирусы или программы (или ссылки на них), способные прервать или нарушить нормальную функциональность компьютерного оборудования, программного обеспечения или средств телекоммуникации любых лиц.

2.10. Вам не разрешается:

- целиком или частично редактировать, изменять, адаптировать, переводить, декомпилировать, дизассемблировать, осуществлять инженерный анализ, создавать или воссоздавать исходный код, модифицировать ПО, осуществлять попытки предпринять аналогичные действия в отношении ПО, а также создавать производные работы, основанные на ПО и/или Документации;
- осуществлять интеграцию ПО в сторонние сайты и программные продукты, за исключением случаев, когда такая интеграция прямо разрешена Правообладателем и правообладателем сторонних сайтов и программных продуктов. Допускается интеграция ПО в сторонние программные продукты посредством встроенного модуля API в рамках функциональных возможностей указанного модуля;

- удалять или изменять уведомления об авторских правах, правах собственности на ПО и/или его элементы;
- сдавать ПО в аренду, прокат или во временное пользование, сублицензировать, распространять или иным образом предоставлять любому физическому или юридическому лицу любые права в отношении ПО и/или Документации, а также разглашать результаты стендовых испытаний ПО, за исключением случаев, прямо разрешенных настоящим Соглашением;
- передавать и предоставлять доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения и Договора, заключенного между вами и вашим лицензиаром;
- осуществлять незаконный сбор, систематизацию, хранение и распространение конфиденциальной и/или персональной информации;
- использовать ПО для несанкционированного удаленного доступа к компьютерам третьих лиц, а также изменения конфигурации компьютера так, чтобы такие возможности могли появиться у стороннего ПО;
- собирать, хранить, использовать, обрабатывать и распространять с помощью ПО любые информационные данные, которые нарушают применимое законодательство, права и законные интересы третьих лиц.

2.11. Лицензионный ключ является конфиденциальной информацией. Правообладатель оставляет за собой право использовать средства для проверки подлинности установленного у вас лицензионного ключа.

3. Ограничение гарантий и ответственности Правообладателя

3.1. Программное обеспечение предоставляется «КАК ЕСТЬ» («AS IS») в соответствии с общепринятым в международной практике обычаем делового оборота. За проблемы, возникающие в процессе эксплуатации ПО, в том числе: проблемы совместимости с другими программными продуктами (пакетами, драйверами и др.), проблемы, возникающие из-за неоднозначного толкования Документации в отношении ПО, несоответствия результатов использования ПО вашим ожиданиям и т.п.) и иные, Правообладатель ответственности не несет.

3.2. Вы подтверждаете, что вам известны функциональные свойства ПО, в отношении которых предоставляется право использования, и самостоятельно несете риск соответствия ПО своим индивидуальным пожеланиям и потребностям, а также за результаты, полученные с его помощью.

3.3. Правообладатель не предоставляет никаких гарантий, выраженных или подразумеваемых, и настоящим отказывается от всех гарантий.

Правообладатель не гарантирует, что ПО не содержит ошибок, будет работать непрерывно, быстро, без неточностей, и не несет никакой ответственности за прямые или косвенные последствия использования ПО, в том числе возникшие из-за возможных ошибок в ПО или опечаток в ПО и/или прилагаемой или переданной позднее Документации.

Правообладатель не дает никаких гарантий и не несет никакой ответственности перед вами в случае любых изменений в программном обеспечении третьих лиц, произошедшее после установки/ внедрения ПО и повлекшее потерю функциональности ПО (включая, но не ограничиваясь, изменением протокола передачи данных, формата хранения данных, логике работы стороннего программного обеспечения, обновлением программного обеспечения, которое перестает поддерживать работу с ПО). Правообладатель не дает никаких гарантий, условий, представлений или положений (выражаемых в явной или в подразумеваемой форме) на все, включая без ограничений нарушения прав третьих лиц, коммерческое качество, интеграцию или пригодность для определенных целей.

3.4. Данные, которые становятся доступными при использовании ПО, включая файлы, ссылки, изображения и текст, являются исключительной ответственностью физического или юридического лица, от которого они были получены, и являются собственностью соответствующего лица. Настоящее Соглашение не дает никаких прав на такие данные. Вы принимаете на себя ответственность за

возможные последствия, риски безопасности и любые убытки, вызванные такими данными, просмотренными или полученными Вами с помощью ПО.

3.5. Правообладатель не несет ответственности за какие-либо убытки, ущерб, независимо от причин его возникновения (включая, но не ограничиваясь прямым или косвенным ущербом, убытками связанными с недополученной прибылью, прерыванием коммерческой или производственной деятельности, утратой деловой информации, небрежностью, или какими-либо иными убытками), возникшие вследствие использования или невозможности использования ПО, даже если Правообладатель был уведомлен о возможных убытках. При любых обстоятельствах ответственность Правообладателя ограничена возмещением документально подтвержденного реального ущерба, ограниченного 3 000 (тремя тысячами) рублей, и возлагается на него при наличии в его действиях вины.

4. Права на объекты интеллектуальной собственности

4.1. Вы соглашаетесь с тем, что исключительные права на любые объекты интеллектуальной собственности, воплощенные в ПО и /или любой предоставленной вам документации, принадлежат Правообладателю. По настоящему Соглашению ПО не передается в собственность, не продается, а предоставляются права его использования на условиях ограниченной неисключительной лицензии. Ничто в данном Соглашении не предоставляет вам никаких прав на указанные объекты интеллектуальной собственности иные, чем предоставленные вам по Договору, заключенному между вами и вашим лицензиаром.

4.2. Вы соглашаетесь с тем, что исходный код, лицензионный ключ для ПО являются собственностью Правообладателя.

5. Права на информацию, доступ к которой получен вами в рамках осуществления настоящего Соглашения

5.1. Вы соглашаетесь с тем, что вам не принадлежат никакие права на любую информацию, не являющуюся объектом интеллектуальной собственности в соответствии с разделом 4, доступ к которой получен вами в рамках осуществления настоящего Соглашения.

5.2. К указанной информации, включая, но не ограничиваясь, относятся системы, методы работы, иная информация.

5.3. Указанная выше информация будет использоваться Вами только в целях осуществления прав на ПО, предоставленных вам по настоящему Соглашению и Договору с лицензиаром, без права использования указанной информации в собственных интересах и за пределами Соглашения и Договора, заключенного между вами и вашим лицензиаром.

6. Открытое программное обеспечение

Вы проинформированы **о том, что ПО содержит открытое программное обеспечение, распространяемое под определенными лицензиями, с которыми вы можете ознакомиться в файле licenses.inf (license.info), распространяемом с ПО в составе дистрибутива.**

7. Заключительные положения

7.1. Настоящее Соглашение вступает в силу с начала установки ПО и действует на протяжении всего периода использования.

7.2. В случае нарушения вами какого-либо из условий Соглашения и/или Договора, заключенного между вами и вашим лицензиаром, или в случае, если исполнение Соглашения или Договора, заключенного между вами и вашим лицензиаром будет нарушать или нарушает применимое право, Правообладатель вправе отказаться от исполнения Соглашения и расторгнуть его (включая, но не ограничиваясь, путем блокировки лицензионного ключа, прекращения предоставления прав) в любое время без уведомления вас. В указанном в настоящем пункте случае стоимость ПО/размер вознаграждения за права на ПО, а также возможные убытки по настоящему Соглашению и/или Договору, заключенному между вами и вашим лицензиаром, вам не возмещаются.

7.3. При расторжении или прекращении Соглашения Пользователь обязан уничтожить все копии установленного ПО.

7.4. Вы настоящим уведомляетесь о том, что при включении в ПО функции сбора статистики использования, ПО может осуществлять сбор и запись информации в обезличенном виде:

а) об аппаратном обеспечении, об операционной системе устройства, на котором установлено и эксплуатируется ПО, а также иная техническая информация, содержащая сведения об использовании аппаратных средств, нагрузке на аппаратные средства и быстродействии ПО;

б) данные о действиях конечного пользователя в пользовательском интерфейсе ПО.

Правообладатель вправе использовать указанные данные для принятия решений о развитии функциональности и улучшении эксплуатационных характеристик ПО.

Правообладатель обязуется обеспечить конфиденциальность полученных данных, не разглашать и не передавать их третьим лицам.

7.5. Настоящее Соглашение, а также любые споры, возникающие из или в связи с настоящим Соглашением, регулируются и истолковываются в соответствии с законодательством Российской Федерации.

7.6. Все споры и разногласия, возникающие в процессе исполнения Соглашения, будут по возможности разрешаться путем переговоров. В случае недостижения согласия, споры будут рассматриваться в судебном порядке в Арбитражном суде г. Москвы.

7.7. Настоящее Соглашение может быть изменено Правообладателем в любой момент без какого-либо уведомления. Новая редакция Соглашения вступает в силу с момента ее размещения по указанному в настоящем пункте адресу. С условиями действующей редакции Соглашения вы всегда можете ознакомиться по адресу https://kb.infowatch.com/display/EULA/. При этом продолжение использования ПО после внесения изменений и/или дополнений в настоящее Соглашение означает согласие с такими изменениями и/или дополнениями. В случае несогласия с условиями такого измененного Соглашения, вы обязаны немедленно отказаться от дальнейшего использования ПО.

8. Контактная информация Правообладателя

Тел./факс: +7(495)229-00-22

Коммерческий департамент: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru

15 Глоссарий

Термин	Определение
Администратор	Администратор – пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. *Главный офицер безопасности*, *Пользователь*
Главный офицер безопасности	Предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в Системе См. *Офицер безопасности*, *Пользователь*
Интерфейс пользователя	Совокупность средств и методов, при помощи которых пользователь взаимодействует с Системой
Консоль управления	Графический интерфейс пользователя, предназначенный для управления системой DAT (администрирование и настройка Системы, просмотр результатов аудита службы каталогов, прав доступа к почтовым ящикам и изменений прав доступа к объектам файловой системы)
Контроллер домена	Сервер, предназначенный для управления доступом к сети внутри домена. Физически информация службы каталогов хранится на одном или нескольких равнозначных контроллерах доменов. Каждый контроллер домена хранит копию данных службы каталогов, предназначенную для чтения и записи. Изменения, сделанные на одном контроллере, синхронизируются на все контроллеры домена. При этом между контроллерами не синхронизируются записи об изменениях объектов. См. *Служба каталогов*
Лицензия	Право на использование Системы. Получается при приобретении Системы и определяет допустимые действия с Системой
Объект службы каталогов	Отдельная сущность службы каталогов, например, пользователь или компьютер. См. *Служба каталогов*, *Active Directory*
Офицер безопасности	Основной пользователь Консоли управления. Также предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в Системе, за исключением административных

Термин	Определение
Персона	Учетная запись сотрудника организации или внешнего контакта, содержащаяся в справочнике Системы и позволяющая обрабатывать данные, принадлежащие этой учетной записи, как единое целое, а также отображать события, относящиеся к ней, в удобном для пользователя виде.
Платформа	Принципиальная конструкция продукта – комплекс частей, подсистем, интерфейсов и производственных процессов. Продуктовая Платформа выступает в качестве базы для развертывания семейства продуктов и сборки готовых изделий из стандартизированных компонентов.
Пользователь	Пользователь системы DAT – администратор, Офицер безопасности и др. См. *Администратор*, *Офицер безопасности*
Привилегированная группа, Критическая группа	Группа учетных записей, которым предоставляются права, привилегии и разрешения, позволяющие пользователям выполнять практически любые действия в службе каталогов и в системах, присоединенных к домену. См. *Служба каталогов*, *Персона*
Рабочая станция / Компьютер	В терминах Системы подразумевается контролируемая рабочая станция или терминальное устройство
Сервис ClickHouse	Распределенная аналитическая столбцовая СУБД, предназначенная для проведения анализа по хранящимся данным в реальном времени. Компонент продуктовой Платформы
Сервис PostgreSQL	СУБД, которая используется в продукте DAT для хранения событий службы каталогов. Компонент продуктовой Платформы
Служба каталогов	Средство иерархического представления ресурсов организации (персонал, материальные и сетевые ресурсы и т.д.) и информации об этих ресурсах. Позволяет управлять доступом к объектам и устанавливает правила безопасности. См. *Active Directory*, *Контроллер домена*
Active Directory (AD)	LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT См. *Служба каталогов*, *Контроллер домена*

Термин	Определение
Exchange	Служба корпоративной электронной почты корпорации Microsoft
FTP	Протокол передачи данных по сети
InfoWatch Traffic Monitor (InfoWatch TM)	Traffic Monitor: программный комплекс, предназначенный для контроля различных видов трафика (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) и теневых копий данных, копируемых на съемные носители и отправляемых на печать
Kubernetes	Программное обеспечение для оркестрации контейнеризированных приложений – автоматизации их развертывания, масштабирования и координации в условиях кластера
NATS	Система обмена сообщениями для компонентов
SMB (Server Message Block)	Сетевой протокол для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SSH (Secure Shell)	Сетевой протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов)