

INFOWATCH

InfoWatch Activity Monitor 1.0.0 Руководство администратора

12/04/2021

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 5

2 Комплект документов 6

3 Техническая поддержка пользователей 7

4 Настройка защиты от подбора паролей Device Monitor 8

5 Настройка сервера Device Monitor 10

5.1 Настройка сбора статистических данных и перехвата событий 10

6 Управление пользователями 12

6.1 Создание нового пользователя 12

6.2 Добавление нового пользователя из LDAP 13

6.3 Просмотр профиля пользователя 14

6.4 Редактирование учетной записи 14

6.5 Смена пароля пользователя 14

6.6 Активация и деактивация пользователя 15

6.7 Удаление пользователя 15

7 Управление безопасностью 17

8 Настройки Системы 19

8.1 Состояние Системы 19

8.2 Фильтры 20

8.3 Основные настройки 21

8.3.1 Настройки сессии 21

8.3.2 Выбор часового пояса 21

8.3.3 Наименование персоны 21

8.4 Интеграции 22

8.4.1 Интеграция с InfoWatch Traffic Monitor 22

8.4.2 Интеграция с Active Directory 25

8.4.3 Интеграция с InfoWatch Person Monitor 28

8.5 Партиции событий 28

8.5.1 Ручное архивирование, удаление и восстановление партиций 29

8.5.2 Настройки хранения 29

9 Уведомления 31

10 Настройки продукта 32

10.1 Справочники 32

10.1.1 Типы активности 32

10.1.2 Приложения и веб-сайты 33

10.2 Правила маркировки событий 35

10.2.1 Работа с правилами маркировки событий 35

10.3 Настройка отображения событий 37

11 Лицензирование 38

Настоящее руководство содержит сведения по настройке и подготовке к работе InfoWatch Activity Monitor – программного обеспечения, предназначенного для контроля деятельности сотрудников.

1 Аудитория

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

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Microsoft Windows.

2 Комплект документов

В комплект документации InfoWatch Activity Monitor входят:

- «InfoWatch Activity Monitor. Руководство по установке». Содержит описание процесса установки, обновления и удаления Activity Monitor.
- «InfoWatch Activity Monitor. Руководство администратора». Содержит информацию по настройке и подготовке к работе Activity Monitor.
- «InfoWatch Activity Monitor. Руководство пользователя». Содержит описание порядка работы и решения задач в Activity Monitor.

3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, обращайтесь в службу технической поддержки:

- компании InfoWatch по адресу support@infowatch.com, если продукт приобретен напрямую у InfoWatch;
- партнера компании InfoWatch, если продукт приобретен у партнера компании InfoWatch.

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. Раздел технической поддержки также доступен на сайте: www.infowatch.ru/services/support.

Перед обращением в службу технической поддержки рекомендуется посетить раздел База знаний на сайте: https://kb.infowatch.com/. Возможно, он уже содержит ответ на ваш вопрос или решение возникшей ситуации.

4 Настройка защиты от подбора паролей Device Monitor

Для защиты Системы реализована блокировка авторизации пользователя при повторяющихся неудачных попытках авторизации. Защита от подбора паролей настраивается в базе данных. По умолчанию защита отключена.

Чтобы включить защиту для сервера Device Monitor:

1. Подключитесь напрямую к базе данных, которую использует сервер Device Monitor.
2. Найдите таблицу `PasswordProtection`.
3. Найдите 3 параметра, которые отвечают за настройку защиты:
   - **`MaxAuthFailCount`** - количество допустимых неудачных попыток авторизации;
   - **`MaxBlockingTimeInSeconds`** - время, на которое будет заблокирована возможность авторизации для пользователя, в секундах;
   - **`MaxFailAuthPeriodInSeconds`** - период неудачных попыток авторизации, в секундах.
4. Задайте значения всех трех параметров в соответствии с требованиями безопасности.

   > **Важно!**
   >
   > Если любому из параметров задано некорректное значение или 0, защита будет отключена.

5. Для применения настроек достаточно сохранить изменения в базе данных. Перезагрузка сервер не требуется, поддерживается динамическое изменение настроек защиты.

> **Важно!**
>
> Защита от подбора пароля будет работать только для пользователей Device Monitor. Учетным записям домена AD, которым назначаются права на вход в Device Monitor, необходимо будет настраивать защиту правилами ОС MS Windows.
> При перезапуске сервиса DM попытка авторизации будет считаться первой. Если пользователь совершил 3 неудачных попытки подряд, его четвертая попытка после перезапуска будет считаться первой.

При блокировании авторизации в журнале аудита (кнопка **Журнал** на Панели навигации консоли управления Device Monitor) будет создано соответствующее событие, в котором будет указано время разблокировки.

При очередной попытке авторизации заблокированный пользователь будет уведомлен о превышении числа неудачных попыток входа.

Пример настроек защиты:

- `MaxAuthFailCount – 5`
- `MaxBlockingTimeInSeconds – 300`
- `MaxFailAuthPeriodInSeconds – 120`

При данных настройках, если в течение 2 минут (120 секунд) от имени пользователя будут выполнены 5 неудачных попыток авторизации, для данного пользователя будет заблокирована возможность авторизации на 5 минут (300 секунд). Отсчет периода неудачных попыток начинается с первой. Если за

120 секунд пользователь совершит только 4 неудачные попытки, следующая попытка будет первой в новом периоде.

5 Настройка сервера Device Monitor

Сбор статистических данных и перехват событий в Activity Monitor (далее – Система) осуществляется посредством компонента Device Monitor (далее – DM).

Как настроить сервер DM см. раздел "Руководство администратора InfoWatch Traffic Monitor. Настройка Системы после установки. Настройка сервера InfoWatch Device Monitor".

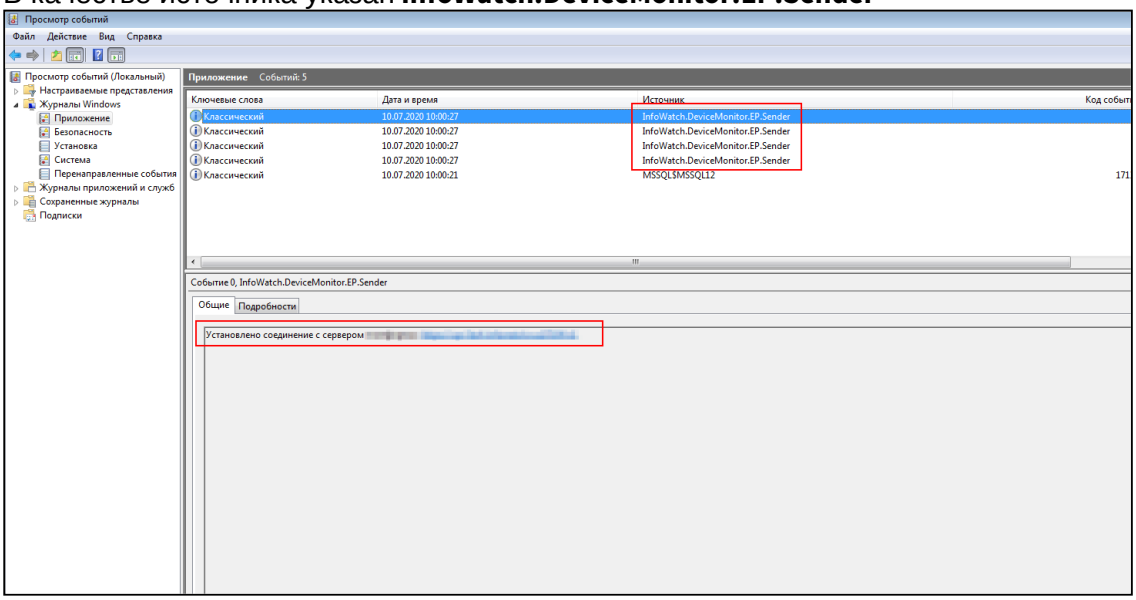
Информацию о том, как активировать возможность отправки событий в Систему, см. в статье "Настройка сбора статистических данных и перехвата событий".

5.1 Настройка сбора статистических данных и перехвата событий

Для активации отправки данных сервером DM в Систему, необходимо произвести настройки в конфигурационном файле сервера DM (по умолчанию файл находится в `Program Files\InfoWatch\Device Monitor\Server\InfoWatch.DeviceMonitor.Server.exe.config`) в разделе **InfoWatch.DeviceMonitor.EP.Sender.Properties.Settings**. Для этого:

1. Остановите службу Windows сервера DM;
2. В конфигурационном файле сервера внесите следующие параметры:
   - *EPToken* – авторизационный токен Системы (находится в директории с распакованным архивом продукта `/license/dms_token.tok`);
   - *DBPollTime* – частота опроса БД (в миллисекундах);
   - *NumberOfConnections* – количество подключений сервера DM к серверу Системы;
   - *RequestEventCount* – количество событий статистики, допустимое для отправки в одном пакете;
   - *MaxSendEventCount* – количество событий, которое единовременно может быть отправлено из базы данных;
   - *WriteDisconnectEventLogInvervalMinute* – интервал записи лог-файла в случае отсутствия или обрыва связи (в минутах).
3. *EPAddress* – адрес сервера Системы в формате https://<example.domain.ru или IP-адрес>:17104/v1, на который будут отправляться данные;
4. Запустите службу.
5. Чтобы убедиться, что настройка сервера прошла успешно, перейдите в в **Журналы Windows** -> **Приложение**. Проверьте, что:
   a. Установлено соединение с сервером AM

b. В качестве источника указан **InfoWatch.DeviceMonitor.EP.Sender**



После настройки сервера DM необходимо настроить правила DM для сбора данных статистики и перехвата событий Системы. Подробнее об этом см. InfoWatch Activity Monitor 1.0.0 Руководство пользователя, статья "Настройка правил InfoWatch Device Monitor для сбора данных статистики и перехвата событий".

6 Управление пользователями

Во время установки Системы создается предустановленный пользователь – Главный офицер. Если на сервере установлено несколько продуктов InfoWatch, для входа в Систему необходимо выбрать **Activity Monitor** в списке установленных продуктов компании InfoWatch. Затем ввести логин и пароль по умолчанию:

Логин	Пароль
officer	xxXX1234

Важно!

В целях соблюдения требований безопасности при первом входе в Систему Офицеру необходимо сменить пароль на постоянный (см. "Смена пароля пользователя").

Главная страница раздела **Пользователи** содержит список пользователей, допущенных к работе в Системе:

- Главный офицер безопасности;
- другие Офицеры безопасности (ОБ), подчиненные ему.

В разделе также доступны следующие действия:

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

6.1 Создание нового пользователя

Главный офицер создает новых пользователей, которые также могут выполнять функции Офицеров безопасности (далее - ОБ). Чтобы добавить пользователя:

1. Перейдите в раздел **Настройки** -> **Настройки пользователей** -> **Пользователи**.
2. Нажмите **+ Создать**.
3. Введите параметры согласно таблице:

Параметр	Обязательный параметр	Описание
Фотография	Нет	Фотография пользователя
Имя пользователя	Да	Имя нового пользователя (см. Управление безопасностью)

Логин	Да	Имя учетной записи пользователя (см. Управление безопасностью)
Пароль	Да	Пароль учетной записи (см. Управление безопасностью)
Подтверждение пароля	Да	Пароль учетной записи
Язык консоли	Да	Язык интерфейса для нового пользователя: *Русский* или *Английский*
Контакты	Нет	Email-адрес. Можно добавить одно или несколько значений
	Нет	Номер телефона. Можно добавить одно или несколько значений
Права Администратора	Нет	При выборе этого пункта ОБ получит права на работу в разделе **Настройки.** Главный ОБ имеет эти права по умолчанию. Другие ОБ не могут забрать права Администратора у Главного ОБ

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

6.2 Добавление нового пользователя из LDAP

Главный офицер может выбрать из LDAP новых пользователей, которые также могут выполнять функции Офицеров безопасности (далее – ОБ). Для этого:

1. Перейдите в раздел **Настройки** -> **Настройки пользователей** -> **Пользователи**.
2. Нажмите **+ Создать**.
3. Выберите **Добавить из LDAP**.
4. Выберите доступный LDAP-сервер, интеграция с которым настроена в Системе.
5. В строке поиска начните вводить ФИО или логин пользователя.
6. В результатах поиска выберите нужного пользователя и нажмите **Добавить**.

Пользователь будет добавлен в список ОБ Системы. Такой пользователь входит в Систему по своим доменным учетным данным. Логин учетной записи имеет вид: *domain\login* или *login@domain*.

Примечание:

Полномочия ОБ в филиалах определяет Главный Офицер.

Примечание:

Требования к безопасности (см. "Управление безопасностью") не распространяются на пользователей, добавленных из LDAP. Также для таких пользователей недоступно изменение пароля.

Важно!

Изменения учетной записи, внесенные в Active Directory, будут доступны в Системе только после ее повторного добавления: учетную запись необходимо удалить, а затем добавить.

6.3 Просмотр профиля пользователя

На странице профиля представлена личная карточка пользователя с данными, указанными при создании:

- фото пользователя;
- имя пользователя;
- логин пользователя в Системе;
- язык веб-консоли для данного пользователя, выбранный при создании пользователя в Системе;
- адрес электронной почты (если указан);
- номер телефона (если указан);
- статус пользователя:  – активный;  – неактивный.

6.4 Редактирование учетной записи

Чтобы изменить учетную запись пользователя:

1. Перейдите в раздел **Настройки**  -> **Настройки пользователей** -> **Пользователи**.
2. Нажмите  на странице профиля пользователя.
3. Выберите **Редактировать**.
4. В открывшемся окне измените один или несколько параметров. Доступны параметры, заданные при создании пользователя, кроме логина и пароля (см. "Создание нового пользователя").
5. Нажмите **Сохранить,** чтобы применить изменения.



6.5 Смена пароля пользователя

Чтобы сменить пароль, выданный для первого входа в Систему или скомпрометированный пароль:

1. Нажмите  в профиле пользователя.
2. Выберите **Сменить пароль**.
3. Заполните поля:

Поле	Описание
Пароль	Введите новый пароль, удовлетворяющий настройкам безопасности (см. "Управление безопасностью")
Подтверждение пароля	Повторно введите новый пароль

4. Нажмите **Сохранить**.

6.6 Активация и деактивация пользователя

Главный офицер может запретить выбранному пользователю выполнять какие-либо действия, заблокировав его учетную запись в Системе. Для этого:

1. Перейдите в раздел **Настройки** -> **Настройки пользователей** -> **Пользователи**.
2. Нажмите в профиле пользователя.
3. Выберите **Деактивировать**. Учетная запись пользователя будет заблокирована.

Чтобы разблокировать ранее заблокированную учетную запись:

1. Перейдите в раздел **Настройки** -> **Настройки пользователей** -> **Пользователи**.
2. Нажмите на плашке пользователя, учетную запись которого необходимо разблокировать.
3. Выберите **Активировать**. Разблокированный пользователь может снова работать в Системе.

или

1. В разделе **Настройки** -> **Настройки пользователей -> Пользователи** перейдите в профиль пользователя, которого требуется разблокировать.
2. Нажмите .
3. Выберите **Активировать**. Разблокированный пользователь может снова работать в Системе.

6.7 Удаление пользователя

Главный офицер может удалять учетные записи пользователей. Для этого:

1. Перейдите в раздел **Настройки** -> **Настройки пользователей** -> **Пользователи**.
2. Нажмите на плашке пользователя, учетную запись которого необходимо удалить.
3. Выберите **Удалить**. В открывшемся окне нажмите **ОК**. Учетная запись пользователя будет удалена без возможности восстановления.

или

1. В разделе **Настройки** -> **Настройки пользователей -> Пользователи** перейдите в профиль пользователя, учетные данные которого требуется удалить.

2. Нажмите  .
3. Выберите **Удалить**. В открывшемся окне нажмите **ОК**. Учетная запись пользователя будет удалена без возможности восстановления.

Учетная запись Главного офицера не может быть удалена.

7 Управление безопасностью

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

1. Перейдите в раздел **Настройки** -> **Настройки пользователей** -> **Настройки пароля**.
2. В открывшемся окне установлены настройки по умолчанию. Чтобы внести новые требования к паролю учетной записи, измените параметры:

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

Параметр	Описание
Количество неуспешных попыток ввода	Количество неуспешных попыток ввода, после чего учетная запись будет заблокирована
Период блокировки пользователя	Период блокировки учетной записи в минутах

3. Нажмите **Сохранить**, чтобы новые параметры вступили в силу. Если нужно вернуться к прежним настройкам, нажмите **Сбросить настройки по умолчанию**.
   Пример
   Период для безуспешных попыток – 5.
   Кол-во неуспешных попыток ввода – 4.
   Период блокировки пользователя – 15.
   Если установлены указанные параметры, то после 4 неудачных попыток ввода пароля в течение 5 минут учетная запись пользователя будет заблокирована на 15 минут. По истечении указанного времени будет разрешено повторить ввод пароля.
   Требования к учетной записи пользователя:
   - имя пользователя должно содержать не менее четырех символов;
   - логин пользователя в Системе должен содержать не менее одного символа.

8 Настройки Системы

В разделе **Настройки** -> **Настройки Системы** Офицер безопасности может задать общие настройки работы в Консоли:

- тип фильтра отдела;
- продолжительность сессии работы в Системе;
- выбор часового пояса;
- наименование персоны.

Подробную информацию см. в статьях "Состояние Системы", "Фильтры", "Основные настройки", "Интеграции", "Партиции событий".

8.1 Состояние Системы

В разделе Состояние Системы представлены следующие данные о состоянии серверов, входящих в состав Системы: доступность сервера, информация от его основных аппаратных компонентов, а также информация о состоянии всех служб Системы.

Раздел **Настройки** -> **Настройки системы** -> **Состояние системы** содержит панели, отражающие состояние филиалов. Каждая панель содержит следующую информацию:

Поле	Описание
Адрес	IP-адрес сервера InfoWatch Activity Monitor
Последнее обновление статуса	Дата и время получения информации о статусе сервиса: • *Ready* – доступен и готов к работе; • *Not Ready* – не готов к работе; • *Unknown* – зарегистрирован, но не отвечает на запросы.
Версия ядра	Версия ядра ОС
Операционная система	ОС ноды InfoWatch Activity Monitor
Память	Общий и занимаемый размер оперативной памяти сервера
ЦПУ	Загрузка центрального процессора сервера InfoWatch Activity Monitor
*Дисковое пространство (Clickhouse)**	Общее выделенное и занятое место на диске для хранения данных БД Clickhouse
*Дисковое пространство (Postgre)**	Общее выделенное и занятое место на диске для хранения данных БД PostgreSQL
*Дисковое пространство (Root)**	Общее выделенное и занятое место, отведенное для системных данных в корневой директории
Список всех служб филиала InfoWatch Activity Monitor	

Поле	Описание
Статус	Один из статусов службы: • *Запущена* – работает; • *Недоступна* – невозможно получить статус; • *Не инициализирована* – находится в процессе запуска; • *Не найдена* – должна быть в филиале, но отсутствует; • *Ошибка* – завершена с ошибкой.
Имя	Имя службы в Системе
Версия	Версия сборки службы
Просмотреть детали	Вывод информации о состоянии, событиях и внутренних сообщениях службы

*Если используется более 80% от общего объема дискового пространства, в Уведомления поступает сообщение о превышении допустимого значения по лимиту использования дискового пространства.

Все события мониторинга в Системе записываются в журнал.

Чтобы скачать весь журнал:

Нажмите Экспорт диагностических данных. После формирования начнется загрузка.

Чтобы скачать диагностические данные отдельной службы:

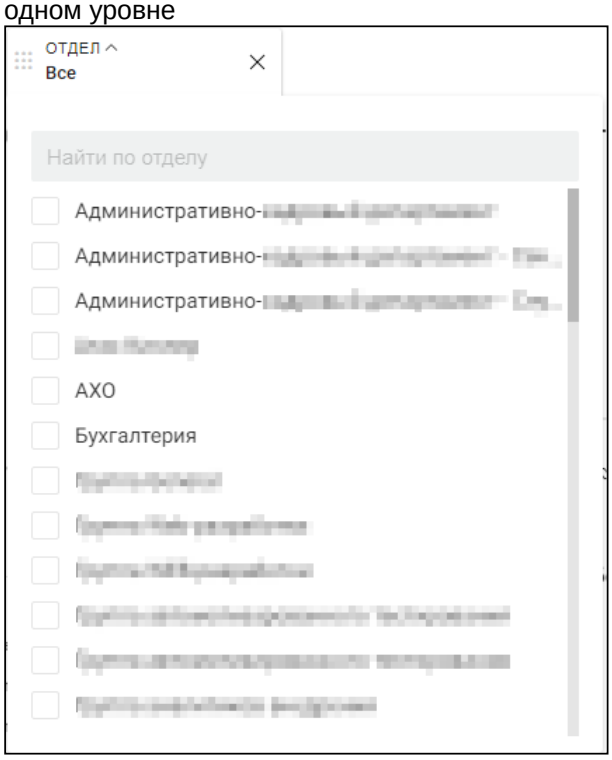
Нажмите напротив нужной службы. Начнется формирование лог-файла, а затем загрузка.

8.2 Фильтры

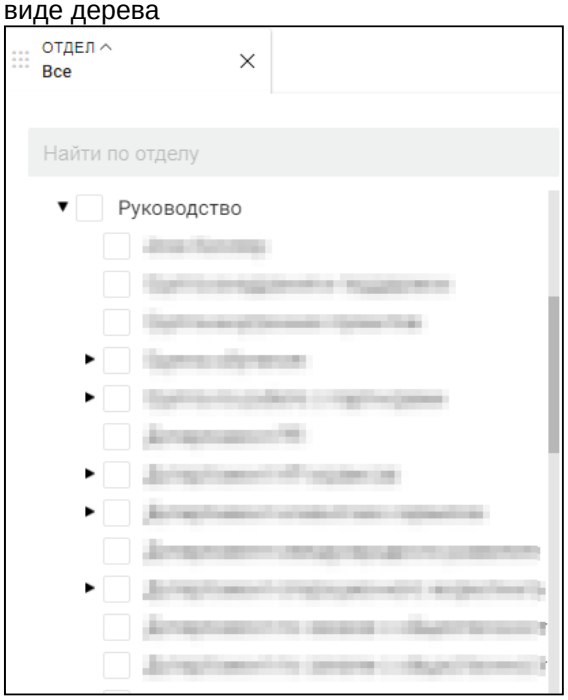
В этом разделе Офицер безопасности (далее – ОБ) имеет возможность настроить фильтрацию отделов и типов контактов.

При синхронизации с Active Directory Система получает список отделов. ОБ может настроить отображение этого списка в Едином фильтре:

Плоский – все отделы отображаются в списке на одном уровне



Иерархический – отделы отображаются в виде дерева



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

8.3 Основные настройки

8.3.1 Настройки сессии

Офицер безопасности (далее – ОБ) может установить время жизни сессии – время ожидания активности пользователя в Консоли. Если в течение указанного отрезка времени не было зафиксировано активности (движения мыши и нажатия кнопок на клавиатуре), произойдет автоматический выход из Консоли. В этом случае для продолжения работы необходимо заново авторизоваться в Системе.

8.3.2 Выбор часового пояса

Для правильного отображения статистики по событиям, произошедшим за выбранный период времени, рекомендуется установить в Системе значение часового пояса, соответствующее месту нахождения Консоли InfoWatch Activity Monitor. Для этого в поле **Часовой пояс** выберите из списка или введите город пребывания.

Чтобы применить настройки, нажмите **Сохранить**.

8.3.3 Наименование персоны

Наименование персоны – это заданное с помощью шаблона правило настройки отображаемого имени персоны. Данное правило распространяется на всех персон.

Чтобы задать и отредактировать правило наименования персон:

- Перейдите в **Настройки**  -> **Настройки Системы** -> **Основные настройки** -> **Создать шаблон имени**;
- Чтобы создать шаблон имени, нажмите ;
- Выберите параметры, которые необходимо отображать в наименовании персоны (в данном поле также возможно добавить любой текст, расположив его перед, между или после выбранных параметров);
- Если требуется очистить поле ввода, нажмите ;
- Чтобы вернуться к значениям по умолчанию, нажмите .
- После того, как параметры выбраны, нажмите **Сохранить**;
- В открывшемся диалоговом окне подтвердите действие, нажав **Да**. Шаблон с выбранными параметрами будет создан. Если не требуется выполнять действие, нажмите **Отмена**.

8.4 Интеграции

Для проведения расследований инцидентов в Систему должны быть загружены данные из систем-источников. Для получения информации о пользователях и связанных с ними данных требуется настроить интеграцию с:

- Active Directory – чтобы получать актуальное дерево каталогов Active Directory компании и формировать досье;
- InfoWatch Traffic Monitor – чтобы получать для анализа данные (события), необходимые для проведения расследования.

Системы-источники используются для следующих целей:

- формирование досье сотрудников;
- получение групп персон;
- получение структуры компании;
- получение информации о рабочих станциях;
- получение информации об объектах защиты, политиках, которые являются частью данных событий.

В разделе **Настройки**  -> **Интеграции** вы можете настроить интеграции с вышеперечисленными системами-источниками и управлять ими.

Подробнее о настройке интеграций см. разделы**:**

- Интеграция с Active Directory
- Интеграция с InfoWatch Traffic Monitor
- Интеграция с InfoWatch Person Monitor

8.4.1 Интеграция с InfoWatch Traffic Monitor

Интеграция с InfoWatch Traffic Monitor (далее – TM) необходима для загрузки в Систему групп, персон, рабочих станций, объектов защиты, политик. Для персон формируются досье (см. "Создание досье").

Примечание:

Интеграция может производиться, начиная с версии ТМ 6.10.10.

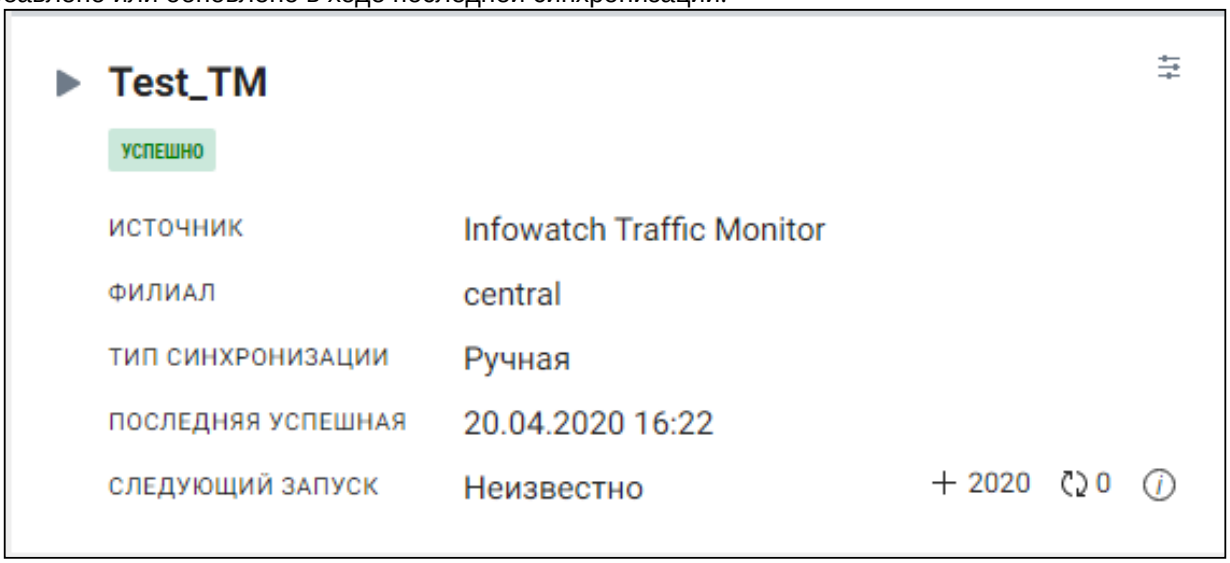
Чтобы добавить новую синхронизацию с ТМ и запустить ее:

1. Перейдите в раздел **Настройки**  -> **Интеграции**.
2. Нажмите **+Создать**.
3. Выберите **InfoWatch Traffic Monitor** и введите параметры:

Параметр	Описание
Имя интеграции	Название соединения, которое используется в Консоли
Филиал	Нода для подключения
Адрес источника	Сетевой адрес функционирующего сервера ТМ
Токен	Ключ, необходимый для получения данных от сервера ТМ (см. "Установка лицензии и плагина в InfoWatch Traffic Monitor")
Синхронизация	*Ручная* или *Автоматическая*. Во втором варианте необходимо указать *Периодичность* и *Повторение*
Периодичность	Как часто необходимо запускать синхронизацию: *Ежеминутно*, *Ежечасно*, *Ежедневно*, *Еженедельно*
Повторение	День недели и время следующей синхронизации

4. Нажмите **Проверить соединение**, чтобы проверить полноту и корректность введенных параметров. Дождитесь сообщения **Соединение успешно установлено**.
   Также возможно появление следующих статусов:
   - **Задан некорректный токен –** был введен некорректный токен;
   - **Не удалось установить соединение** – был введен неверный адрес или сервер недоступен;
   - **Превышено время ожидания ответа от сервиса** – высокая нагрузка на ТМ, проблемы в сети, или иные проблемы (при этом ТМ может быть доступен и синхронизация выполнится)
   - **Доступ к данным не разрешен** – в ТМ отсутствует лицензия Vision или истек срок ее действия.
5. Нажмите:
   - **Сохранить –** при этом новая синхронизация будет ожидать запуска позднее или
   - **Сохранить и синхронизировать**, чтобы запустить процесс синхронизации немедленно.

Список интеграций с серверами InfoWatch Traffic Monitor отображается в центральной области. В нижней строке указано количество добавленных сущностей при последней синхронизации (+) и количество сущностей, данные которых обновились в ходе последней синхронизации . Детальная информация показывает тип синхронизации, а также сколько групп, персон, рабочих станций было добавлено или обновлено в ходе последней синхронизации:



Примечание:

Если в дополнение к InfoWatch Activity Monitor на сервере установлен InfoWatch Vision, в детальной информации об интеграции будут также отображаться добавленные в процессе последней синхронизации объекты защиты и политики.

Если необходимо настроить автоматическую синхронизацию по расписанию (например, в ночное время для экономии времени и минимизации нагрузки на сеть):

1. Нажмите и выберите **Редактировать**.
2. Выберите тип синхронизации: **Автоматическая**.
3. Выберите периодичность: **Ежедневно**.
4. Установите время начала: **0:00**.
5. Нажмите **Сохранить**. Система запустит синхронизацию по расписанию.

Если необходимо провести еще одну синхронизацию с теми же параметрами (например, при изменении групп):

1. Нажмите **Запустить синхронизацию**.
2. Дождитесь выполнения синхронизации. Процесс может занять продолжительное время (например, при низкой скорости передачи данных по сети или при большом объеме передаваемых данных).
3. После успешной синхронизации с ТМ в Систему будет загружен справочник.

Ниже представлены возможные статусы синхронизаций и их описание:

Статус синхронизации	Описание
НЕ СИНХРОНИЗИРОВАЛОСЬ	Синхронизация сохранена и ожидает запуска позднее
СИНХРОНИЗИРУЕТСЯ	Идет процесс синхронизации
УСПЕШНО	Синхронизация завершилась успешно
ОШИБКА	Данный статус может обозначать следующее: • введен некорректный токен • отсутствует плагин/лицензия на использование Vision в ТМ • истек срок лицензии на использование продукта Activity Monitor

Примечание:

Параметры подключения к ТМ необходимо обновить, если:

- был добавлен новый продукт и требуется получить новые данные из ТМ;
- продукт, использующий данные из ТМ, был удален.

Для обновления параметров подключения к ТМ откройте и сохраните интеграцию с ТМ.

8.4.2 Интеграция с Active Directory

Интеграция с Active Directory необходима для загрузки в Систему дерева каталогов компании: групп, персон. На персоны создаются досье (см. "Создание, редактирование и удаление досье").

При первом входе в Систему список интеграций пустой.

Чтобы добавить новую интеграцию с Active Directory и запустить ее:

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

Параметр	Описание
Имя интеграции	Название соединения, которое используется в Консоли
Филиал	Центральный узел подключения для создания интеграции
Адрес источника	Сетевой адрес сервера, с LDAP-каталогами которого производится синхронизация

Параметр	Описание
Тип соединения	Выбор типа соединения, которое будет установлено: • Незащищенное соединение (LDAP); • Защищенное соединение по протоколу LDAP + StartTLS; • Защищенное соединение по протоколу LDAPS (SSL). **Важно!** Соединение без сертификатов небезопасно.
Глобальный порт	Порт для подключения глобального LDAP-каталога. В зависимости от типа соединения или при нажатии  будут использованы значения по умолчанию: • 3268 для незащищенного соединения и защищенного соединения по протоколу LDAP + StartTLS; • 3269 для защищенного соединения по протоколу LDAPS.
Порт	Порт для подключения локального каталога домена. В зависимости от типа соединения или при нажатии  будут использованы порты по умолчанию: • 389 для незащищенного соединения и защищенного соединения по протоколу LDAP + StartTLS; • 636 для защищенного соединения по протоколу LDAPS.

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

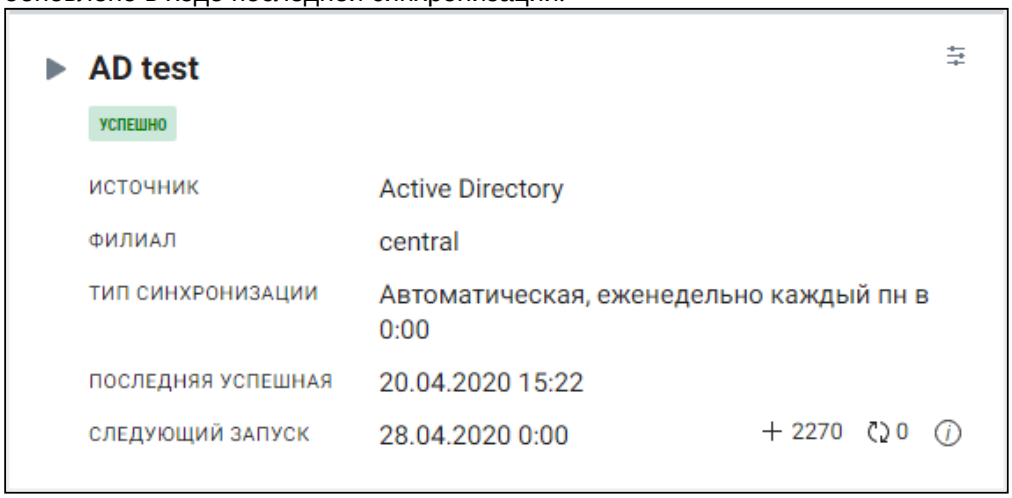
Сертификат	Загрузка файла сертификата в форматах .pem, .der/.cer. для защищенных соединений
Логин	Логин для доступа к серверу Active Directory (для пользователя с правами на чтение каталога)
Пароль	Пароль для доступа к серверу Active Directory

Параметр	Описание
Синхронизация	*Ручная* или *Автоматическая*. Во втором варианте необходимо указать *Периодичность* и *Повторение*
Периодичность	Как часто необходимо запускать синхронизацию: *Ежеминутно*, *Ежечасно*, *Ежедневно*, *Еженедельно*
Повторение	День недели и время следующей синхронизации

4. Нажмите **Проверить соединение**, чтобы проверить, что все параметры заполнены и корректны и дождитесь сообщения **Соединение успешно установлено**. В случае появления статусов:
   - **Не удалось установить соединение** – проверьте, что были введены корректные адрес или локальный порт;
   - **Заданы неверные логин или пароль –** проверьте, что были введены корректные логин и пароль.
5. Нажмите:
   - **Сохранить –** при этом новая синхронизация будет ожидать запуска позднее

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

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



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

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

Ниже представлены возможные статусы синхронизаций и их описание:

Статус синхронизации	Описание
НЕ СИНХРОНИЗИРОВАЛОСЬ	Синхронизация сохранена и ожидает запуска позднее
СИНХРОНИЗИРУЕТСЯ	Идет процесс синхронизации
УСПЕШНО	Синхронизация завершилась успешно
ОШИБКА	Данный статус может обозначать следующее: • введены некорректные логин, пароль, или адрес • истек срок лицензии на использование продукта Activity Monitor

Важно!

Настоятельно рекомендуется проводить первую синхронизацию с Active Directory в ночное время. Это связано с большой нагрузкой на Active Directory и сеть в процессе синхронизации.

8.4.3 Интеграция с InfoWatch Person Monitor

При наличии InfoWatch Vision, установленного совместно с Activity Monitor, также добавится и интеграция с Infowatch Person Monitor. Подробнее о данной интеграции см. документ "Документация для IW Vision 2.2.0. InfoWatch Vision 2.2.0. Руководство администратора. Настройки Системы. Интеграции. Интеграция с InfoWatch Person Monitor".

8.5 Партиции событий

События Activity Monitor хранятся в партициях, которые доступны в соответствующем разделе настроек Системы. Партиции разделены по следующим видам событий:

- Статистика активности ОС;
- Статистика активности клавиатуры;
- Статистика активности мыши;
- Статистика скриншотов;
- Статистика использования приложений;
- Статистика событий поиска.

В разделе доступны следующие действия:

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

Подробнее см. в следующих статьях: "Ручное архивирование, удаление и восстановление партиций ", "Настройки фильтрации".

8.5.1 Ручное архивирование, удаление и восстановление партиций

Чтобы снизить объем данных в Системе, Офицер безопасности имеет возможность вручную архивировать партиции. Для этого:

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

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

Чтобы восстановить партицию:

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

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

Чтобы удалить партицию:

> **Важно!**
>
> При удалении партиции данные в ней удаляются без возможности восстановления. Если потребуется получить данные, которые были удалены, будет необходимо создать новую или повторно создать старую интеграцию и загрузить данные заново.

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

Удаление возможно только для партиций в статусе **Архивированная**.

8.5.2 Настройки хранения

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

Чтобы настроить период хранения партиций:

- Перейдите в **Настройки**  -> **Настройки системы** -> **Партиции событий**;
- Нажмите **Настройки хранения**;
- В открывшемся диалоговом окне выберите желаемые настройки хранения;
- Нажмите **Применить**. Настройки хранения партиций будут применены. Если не нужно применять действие, нажмите **Отмена**.

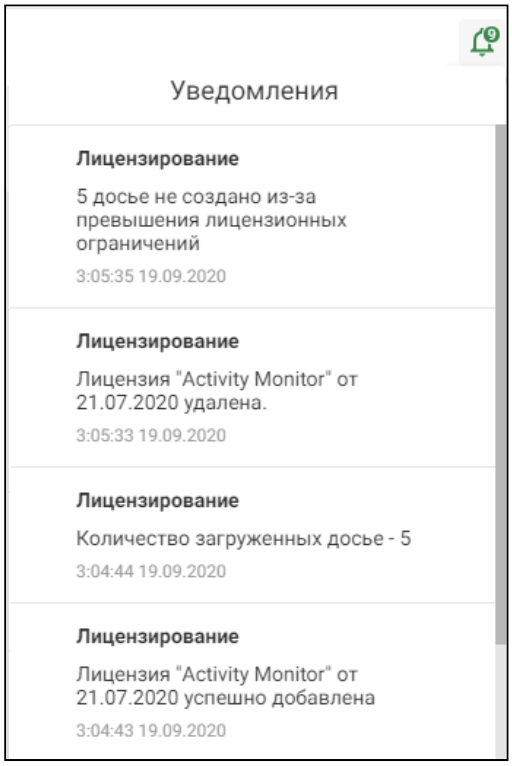
Внимание!

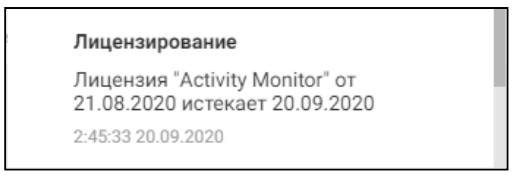
Для корректного отображения данных период хранения в **Партициях событий** и Настройке отображения событий должен совпадать.

9 Уведомления

Чтобы просмотреть уведомления, нажмите . Уведомления сообщают о следующем:

- добавление лицензии;
- удаление лицензии;
- скорое истечение срока действия лицензии;
- количество созданных досье;
- невозможность создать досье (в случае окончания срока действия лицензии);
- скорое переполнение дисковых пространств (уведомления начинают поступать, если используется более 80% от общего объема).







10 Настройки продукта

В разделе **Настройки продукта** доступно управление следующими параметрами:

- типы активности;
- приложения и веб-сайты;
- правила маркировки событий;
- настройки отображения событий.

Подробнее см. в статьях: "Справочники", "Правила маркировки событий", "Настройка отображения событий".

10.1 Справочники

В этом разделе вы можете управлять настройками типов активности, а также приложений и веб-сайтов.

Подробнее см. в статьях "Типы активности" и "Приложения и веб-сайты".

10.1.1 Типы активности

Данный раздел предназначен для работы с типами активности. Тип активности – признак, который позволяет классифицировать деятельность сотрудников в соответствии с настроенными правилами.

По умолчанию в Системе существуют следующие типы активности:

- Рабочая;
- Нерабочая;
- Прочая;
- Смешанная.

Система назначает событию тип активности Смешанная, если фиксирует одновременную работу на нескольких рабочих станциях под одной учетной записью. К данному типу активности может относиться как работа с использованием протокола удаленного доступа и рабочей станции, так и работа на нескольких компьютерах одновременно.

Чтобы просмотреть или изменить настройки типов активности, перейдите в **Настройки** -> **Настройки продукта** -> **Справочники** -> **Типы активности**.

Чтобы создать тип активности:

- Нажмите **Создать**;
- В появившемся диалоговом окне заполните следующие поля: **Название**, **Цвет**, **Описание**;
- Для выбора цвета, который необходимо присвоить типу активности, щелкните в области поля **Цвет** левой кнопкой мыши. В открывшемся окне выбора цветов определите желаемый цвет для типа активности, нажмите **Ok**;
- После заполнения каждого поля нажмите **Создать**. Новый тип активности будет добавлен;
- Если не требуется выполнять действие, нажмите **Отмена**.

Примечание:

По умолчанию при создании активности используется черный цвет.

Чтобы отредактировать тип активности:

- Выберите тип активности, который требуется отредактировать;
- Нажмите **Редактировать**;
- В открывшемся окне редактирования внесите необходимые изменения;
- Нажмите **Обновить**. Тип активности будет изменен. Если не требуется выполнять действие, нажмите **Отмена**.

Примечание:

Редактирование типа активности коснется только событий, созданных после сохранения изменений. События, созданные до редактирования типа активности, не изменятся.

Пример:
Если параметр Цвет для типа активности "Рабочая" был изменен с зеленого на серый, Система отобразит события с данным типом активности, с учетом двух цветов, до и после редактирования.

Если отсутствует необходимость различного отображения событий с параметрами до и после редактирования типа активности, пользователь может внести изменения в тип активности событий, созданных до редактирования, воспользовавшись опцией смены типа активности в разделе События.

Чтобы удалить тип активности:

- Выберите тип активности, который требуется удалить;
- Нажмите **Удалить**;
- В открывшемся диалоговом окне выберите Удалить. Тип активности будет удален. Для отмены действия нажмите **Отмена**.

Примечание:

Предустановленные в Системе типы активности недоступны для удаления.

Для поиска типа активности воспользуйтесь полем **Поиск**.

10.1.2 Приложения и веб-сайты

В данном разделе вы можете управлять списками приложений и веб-сайтов.

Все приложения и веб-сайты входят в категории, которые позволяют объединить приложения и/или веб-сайты в группы по определенному признаку. Например, категория по умолчанию **Мессенджеры** включает десктоп и веб-версии распространённых мессенджеров.

Для работы с разделом перейдите в **Настройки** -> **Настройки продукта** -> **Справочники** -> **Приложения и веб-сайты**.

Чтобы создать в списке новую категорию приложения и/или веб-сайта (далее - категория):

- Выберите **Создать**;
- Заполните поля в появившемся диалоговом окне;
- Нажмите **Создать**. Новая категория будет добавлена;
- Если не требуется выполнять действие, нажмите **Отмена**.

Чтобы отредактировать категорию:

- Выберите категорию, которую требуется отредактировать;
- Нажмите **Редактировать** или дважды щелкните по ней левой кнопкой мыши;
- Внесите необходимые изменения. Нажмите **Сохранить**. Категория будет изменена;
- Если не требуется выполнять действие, нажмите **Отмена**.

Чтобы удалить категорию, нажмите **Удалить** на плашке категории, затем подтвердите действие в появившемся диалоговом окне. Категория будет удалена.

Чтобы подробнее посмотреть конкретную категорию и поработать с ее составом, нажмите **Открыть** на плашке этой категории. На экране отобразится список приложений и веб-сайтов, входящих в состав категории. Для поиска внутри категории воспользуйтесь строкой **Поиск**. Поиск осуществляется по названию приложения или веб-сайта.

Чтобы добавить новое приложение или веб-сайт в список приложений и веб-сайтов категории:

> **Примечание:**
>
> В событиях отображается строка, заданная в поле **Описание**, идентификация приложений/веб-сайтов в событии происходит по **Названию**.

- Откройте или создайте категорию, к которой необходимо отнести приложение или веб-сайт;
- Выберите нужный список: **Приложения** или **Веб-сайты**;
- Нажмите **Добавить**;
- Заполните поля в открывшемся окне;
- Нажмите **Создать**. Приложение или сайт будут созданы. Если не требуется выполнять действие, нажмите **Отмена**.

Чтобы выйти из категории и вернуться к списку категорий, нажмите .

Чтобы отредактировать конкретное приложение или веб-сайт, входящие в категорию:

- Войдите в категорию, нажав **Открыть** на плашке категории;
- Перейдите в нужный список: **Приложения** или **Веб-сайты**;
- Выберите из списка то приложение или веб-сайт, которые нужно отредактировать;
- Нажмите **Редактировать** или дважды кликните по нему левой кнопкой мыши;
- В открывшемся диалоговом окне внесите необходимые изменения;
- Нажмите **Обновить**;
- Если не требуется выполнять действие, нажмите **Отмена**.

Чтобы удалить приложение или веб-сайт из списка категории:

- Войдите в категорию, нажав **Открыть** на плашке категории;
- Перейдите в нужный список: **Приложения** или **Веб-сайты**;
- Выберите приложение или веб-сайт, которые требуется удалить;
- Нажмите **Удалить**;
- В открывшемся диалоговом окне подтвердите действие, выбрав **Удалить**. Приложение или веб-сайт будут удалены. Если не требуется выполнять действие, нажмите **Отмена**.

Для поиска категории воспользуйтесь строкой поиска **Поиск**.

> **Примечание:**
>
> Для более эффективного анализа одно приложение можно отнести к разным категориям. Например, Facebook.exe:
>
> - категория «Социальные сети»,
> - категория «Мессенджеры».

10.2 Правила маркировки событий

Данный раздел предназначен для работы с правилами маркировки событий.

Правила маркировки событий – это правила, на основании которых Система присваивает событию тип активности. Правила маркируют события категориями, в которые входят приложения и веб-сайты. Подробнее о типах активности, а также категориях, приложениях и веб-сайтах см. в статьях "Типы активности", "Приложения и веб-сайты".

По умолчанию в Системе существуют следующие правила маркировки событий:

- нерабочая активность;
- рабочая активность;
- прочая активность.

> **Примечание:**
>
> Категорией «Прочие» маркируются события, не подходящие под категории «Рабочие» или «Нерабочие».
>
> События с приложениями и веб-сайтами, используемыми впервые, маркируются категорией «Новые». Данная категория относится к типу активности «Прочая».

О работе с правилами маркировки событий см. Работа с правилами маркировки событий.

10.2.1 Работа с правилами маркировки событий

При работе с правилами маркировки событий Офицер может:

- изменить порядок приоритета применения правил в Системе;
- добавить правила;
- отредактировать правила;
- удалить правила.

Правила размещены в списке в порядке приоритета их применения в Системе. Наивысший приоритет принадлежит правилу, расположенному первым в списке.
Чтобы изменить приоритет применения правила:

1. Наведите курсор на  на плашке слева от правила.
2. С помощью мыши переместите правило вверх или вниз списка. Перемещение правила автоматически изменит порядок в списке для других правил, затронутых изменением.

Примечание:

Правило **Прочая активность** является предустановленным и не может быть отредактировано, перемещено в списке или удалено. Данное правило срабатывает тогда, когда не срабатывают остальные правила в списке.

Чтобы добавить новое правило:

1. Перейдите в **Настройки** -> **Настройки продукта** -> **Правила маркировки событий**.
2. Нажмите **Добавить**.
3. В открывшемся диалоговом окне заполните необходимые поля.
4. Нажмите **Сохранить**.
5. Чтобы применить изменения, повторите команду **Сохранить** на панели сверху. Новое правило будет добавлено. Чтобы отменить действие, нажмите **Отмена**.

Чтобы отредактировать правило:

1. Перейдите в **Настройки** -> **Настройки продукта** -> **Правила маркировки событий**.
2. Нажмите справа на плашке правила, которое необходимо отредактировать.
3. Выберите **Редактировать**.
4. Внесите требуемые изменения.
5. Нажмите **Сохранить**.
6. Чтобы применить изменения, повторите команду **Сохранить** на панели сверху. Чтобы отменить действие, нажмите **Отмена**.

Примечание:

В случае если правило, редактируемое одним Офицером безопасности, будет необходимо изменить другому Офицеру безопасности, он получит сообщение, что правило уже находится в процессе редактирования и должен будет или отменить сделанные изменения, или сохранить. И после этого сможет внести изменения в правило.

Примечание:

Если при редактировании или удалении тега была активирована опция **Оставить старый тег для элементов до редактирования**, данный тег останется в правилах маркировки событий, но будет иметь отметку о том, что он был изменен или удален.

Примечание:

Максимальное количество тегов, которое можно добавить одному правилу маркировки событий – 30.

Чтобы удалить правило:

1. Перейдите в **Настройки** -> **Настройки продукта** -> **Правила маркировки событий**.
2. Нажмите справа на плашке правила, которое требуется удалить.
3. Выберите **Удалить**.

4. В открывшемся диалоговом окне подтвердите действие, нажав **Удалить**.
5. Чтобы применить изменения, повторите команду **Сохранить** на панели сверху. Чтобы отменить действие, нажмите **Отмена**.

> **Примечание:**
>
> Изменения в конфигурации правил (создание, редактирование, удаление правила) будут действовать только для событий, созданных после применения изменений.

10.3 Настройка отображения событий

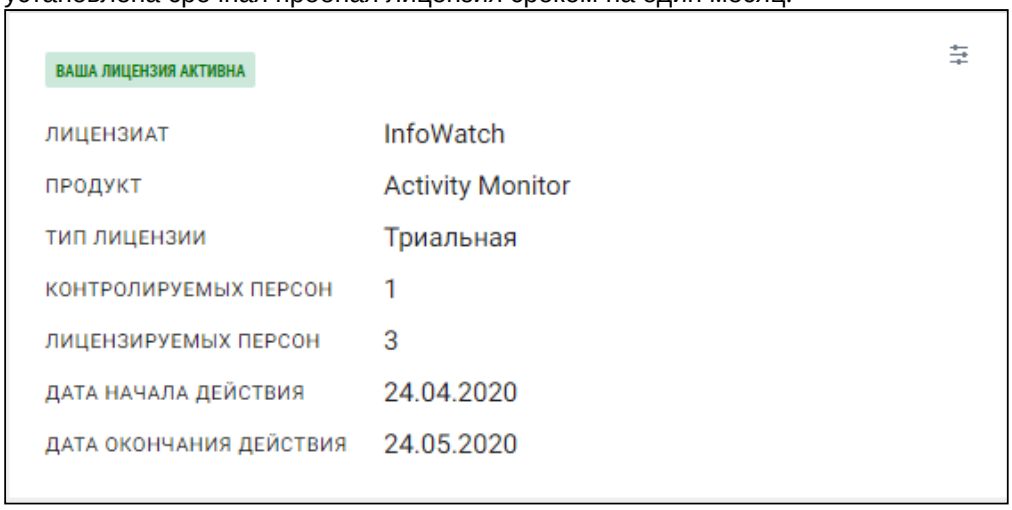
Настройка отображения событий – опция, позволяющая задать период, за который события в Activity Monitor будут доступны Офицеру безопасности для просмотра и фильтрации. Данный период может быть увеличен для того, чтобы иметь возможность анализировать данные за более длительный промежуток времени или сокращен с целью повышения производительности Системы.

По умолчанию настроено отображение событий за 12 недель. Чтобы отобразить события за все время, перейдите в **Настройки** -> **Настройки продукта** -> **Настройка отображения событий**, выберите отображение **За все время**, затем нажмите **Применить**.

> **Внимание!**
>
> Для корректного отображения данных периоды хранения, указанные в меню **Настройка отображения событий** и Настройки хранения партиций должны совпадать.

11 Лицензирование

Работа в Системе возможна только при наличии действующей лицензии. По умолчанию в Системе установлена срочная пробная лицензия сроком на один месяц:



Чтобы установить новую лицензию:

1. Перейдите в раздел **Лицензирование**.
2. Нажмите **+Добавить**.

В открывшемся окне укажите путь до файла с действующей лицензией. Также файл можно добавить, переместив в окно добавления файлов.

Чтобы удалить лицензию:

1. Нажмите в правом верхнем углу плашки лицензии и выберите **Удалить**.
2. В появившемся меню подтвердите действие, нажав **ОК**.

Важно!

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

Важно!

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