

INFOWATCH

# InfoWatch Vision 2.0. Руководство администратора

09/09/2019

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

# СОДЕРЖАНИЕ

1 Аудитория ..... 4

2 Комплект документов ..... 5

3 Техническая поддержка пользователей ..... 6

4 Управление интеграциями ..... 7

4.1 Интеграция с LDAP каталогами ..... 7

4.2 Интеграция с Infowatch Traffic Monitor ..... 9

5 Управление пользователями ..... 12

5.1 Создание нового пользователя ..... 12

5.2 Редактирование учетной записи ..... 13

5.3 Активация и деактивация пользователя ..... 13

5.4 Удаление пользователя ..... 13

6 Управление данными для анализа ..... 14

6.1 Создание фильтра ..... 14

6.2 Хранение событий ..... 15

6.3 Ручное архивирование и восстановление партиций ..... 16

7 Управление безопасностью ..... 17

8 Управление лицензиями ..... 19

9 Управление загрузкой оргструктуры ..... 20

9.1 Настройка отображения ..... 20

9.2 Внутренние домены ..... 21

10 Уведомления ..... 22

В настоящем руководстве вы сможете найти сведения по настройке и подготовке к работе InfoWatch Vision 2.0 – программного обеспечения, предназначенного для визуализации расследования инцидентов на основе данных, полученных от InfoWatch Traffic Monitor.

# 1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, работающих с Системой (выполняющих настройку конфигурации, анализ информационных объектов и т. п.).

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

# 2 Комплект документов

В комплект документации по InfoWatch Vision 2.0 входят:

- «InfoWatch Vision 2.0. Руководство по установке». Содержит описание процесса установки, обновления и удаления InfoWatch Vision 2.0.
- «InfoWatch Vision 2.0. Руководство администратора». Содержит информацию по настройке и подготовке к работе InfoWatch Vision 2.0.
- «InfoWatch Vision 2.0. Руководство пользователя». Содержит описание порядка работы и решения задач в InfoWatch Vision 2.0.

Сопутствующая документация по комплексу InfoWatch Traffic Monitor включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание порядка 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 порядка 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: https://www.infowatch.ru/support.

Перед обращением в службу технической поддержки рекомендуется посетить раздел База знаний на нашем сайте: https://kb.infowatch.com/. Возможно, там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

# 4 Управление интеграциями

Для проведения расследований по инцидентам Системе необходимо получить данные из систем-источников. Для этого нужно настроить интеграцию с :

- LDAP Integration – для получения актуального дерева каталогов Active Directory компании и формирования досье;
- Infowatch Traffic Monitor – для получения на анализ данных, необходимых для проведения расследования.

Источники используются в Системе для:

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

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

**Целевые действия:**

- Интеграция с LDAP каталогами
- Интеграция с Infowatch Traffic Monitor

## 4.1 Интеграция с LDAP каталогами

Интеграция с LDAP каталогами необходима для загрузки в Систему дерева каталогов компании: групп и персон. На них создаются досье (см. "Создание, редактирование и удаление досье"), которые становятся объектами расследования.

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 **LDAP Integration** и введите параметры:

| Параметр | Описание |
|---|---|
| *Имя интеграции* | Название соединения, которое используется в Консоли |
| *Адрес источника* | Сетевой адрессервера, с LDAP-каталогами которого производится синхронизация |
| *Глобальный порт* | Порт для подключения глобального LDAP-каталога |
| *Порт* | Порт для подключения локального каталога домена |

| | |
|---|---|
| *LDAP запрос* | Домен (LDAP base), в котором ведется поиск данных AD<br>Пример<br>Чтобы использовать в качестве базы поиска ветку `Users`, расположенную в домене компании `Company`, введите строку вида: `cn=users,dc=company,dc=com` |
| *Логин* | Логин для доступа к серверу Active Directory |
| *Пароль* | Пароль для доступа к серверу Active Directory |
| *Синхронизация* | *Ручная* или *Автоматическая*. Во втором варианте необходимо указать *Периодичность* и *Повторение* |
| *Периодичность* | Как часто необходимо запускать синхронизацию: *Ежеминутно*, *Ежечасно*, *Ежедневно*, *Еженедельно* |
| *Повторение* | День недели и время следующей синхронизации |

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

Синхронизация возможна с несколькими LDAP-каталогами одновременно. 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, тип синхронизации, а также сколько персон и рабочих станций 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 **Запустить синхронизацию**.

2. Дождитесь статуса выполнения СИНХРОНИЗИРУЕТСЯ => УСПЕШНО. Данный процесс может занять длительное время (например, при низкой скорости передачи данных по сети или при большом объеме передаваемых данных).
3. В случае получения статуса ОШИБКА проверьте, доступен ли сервер и введены ли корректные учетные данные.
4. Перейдите в раздел **Досье** и убедитесь, что данные перенесены и отображены в таблице.

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

## 4.2 Интеграция с Infowatch Traffic Monitor

Интеграция с Infowatch Traffic Monitor необходима для загрузки в Систему событий, а также групп, персон, объектов защиты и политик. На персоны заводятся досье (см. "Создание досье") и инициируются расследования.

При первом входе в Систему список интеграций пустой.

> **Примечание:**
>
> Интеграция с InfoWatch Traffic Monitor производится, начиная с версии 6.10.10.

> **Важно!**
>
> До начала синхронизации с Traffic Monitor определите внутренние домены организации (см. "Внутренние домены"). В этом случае загружаемые события будут корректно классифицироваться по внешним или внутренним контактам.

**Чтобы добавить новую синхронизацию с Infowatch Traffic Monitor и запустить ее:**

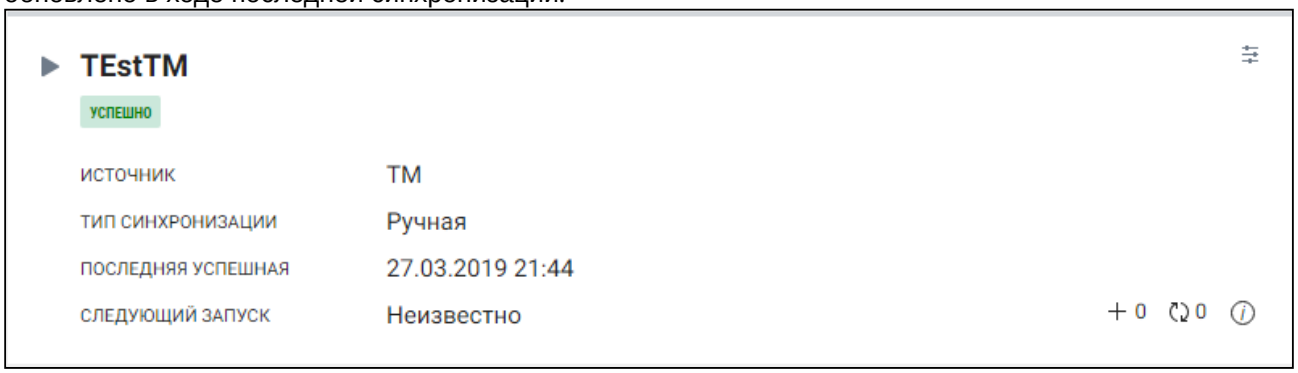
1. Перейдите в раздел **Настройки** -> **Интеграции**.
2. Нажмите **+Создать**.
3. Выберите **Infowatch Traffic Monitor** и введите параметры:

| Параметр | Описание |
|---|---|
| *Имя интеграции* | Название соединения, которое используется в Консоли |
| *Адрес источника* | Сетевой адрес функционирующего сервера ТМ |

| | |
|---|---|
| *Токен* | Ключ, необходимый для получения данных от сервера TM (см. "Установка лицензии и плагина в InfoWatch Traffic Monitor") |
| *Количество потоков загрузки* | Количество рабочих потоков, через которые загружаются данные из TM, на каждый драйвер отдельно: загрузку событий и загрузку справочников |
| *Интервал загрузки фактов (мин.)* | Интервал времени совершения событий в TM, данные о которых будут передаваться в Систему в одном пакете. По умолчанию: 120 минут. Уменьшение данного параметра позволяет снизить нагрузку в TM при отправке данных. |
| *Использовать параметры архивирования при загрузке* | При включении этого параметра, начальная и конечная даты загрузки фактов соответствует данным Настроек архивирования. По умолчанию: 12 недель. |
| *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, и дождитесь сообщения "*Соединение успешно установлено*".
5. Нажмите:
   - **Сохранить** - при этом новая синхронизация будет ожидать запуска позднее в статусе НЕ СИНХРОНИЗИРОВАЛОСЬ или
   - **Сохранить и синхронизировать**, чтобы запустить процесс синхронизации.

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

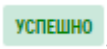
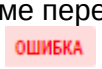


**Если необходимо настроить автоматическую синхронизацию по расписанию** (например, в ночное время для экономии времени и минимизации нагрузки на сеть):

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.

> **Важно!**
>
> При планировании первичной синхронизации с Infowatch Traffic Monitor стоит учитывать, что загрузка большого количества событий из БД может сильно уменьшить пропускную способность сети и общее быстродействие сервера и Консоли управления ТМ. Поэтому рекомендуется работы по синхронизации проводить в компании в нерабочее (ночное) время.

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

1. Нажмите **Запустить синхронизацию**.
2. Дождитесь статуса выполнения  => . Данный процесс может занять продолжительное время (например, при низкой скорости передачи данных по сети или при большом объеме передаваемых данных).
3. В случае получения статуса  проверьте корректность введенных учетных данных.
4. После успешной синхронизации с ТМ в Системе формируется справочник. Перейдите в раздел **События** и убедитесь, что данные перенесены и отображены в таблице.

**Чтобы оценить уровень нарушений в филиалах компании, нужно провести синхронизации с Traffic Monitor, установленных в филиалах:**

1. Создайте несколько интеграций с Traffic Monitor, установленных в разных филиалах.
2. Запустите синхронизации.
3. После успешной синхронизации с несколькими серверами ТМ в Системе можно анализировать события отдельно по каждому филиалу. Для этого:
   a. В разделах Системы и настройте параметры фильтрации (см. "Единый фильтр - Источник").
   b. В разделе **Статистика** добавьте в рабочей области соответствующий виджет (см. "Виджеты статистики - Источник").

> **Важно!**
>
> Для регистрации в Traffic Monitor установите плагин Vision 2.0. Подробнее см. "Установка лицензии и плагина в InfoWatch Traffic Monitor"

# 5 Управление пользователями

При установке Системы создается предустановленный пользователь – Главный офицер. Для входа в Систему Главный офицер использует логин и пароль, установленные по умолчанию:

| Логин | Пароль |
|---|---|
| officer | xxXX1234 |

При первом входе в Систему офицер должен сменить пароль на постоянный. Для этого:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. На панели пользователя *Главный офицер* нажмите **Смена пароля**.
3. Введите действующий пароль (значение по умолчанию), затем новый пароль, который соответствует требованиям к сложности (см. Управление безопасностью, подтвердите новый пароль и нажмите **Сохранить**.

**Целевые действия:**

- Создание нового пользователя
- Редактирование учетной записи
- Активация и деактивация пользователя
- Удаление пользователя

## 5.1 Создание нового пользователя

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

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

| Параметр | Обязательный параметр | Описание |
|---|---|---|
| *Фотография* | Нет | Фотография пользователя |
| *Имя пользователя* | Да | Имя нового пользователя (правила см . Настройки безопасности) |
| *Логин* | Да | Имя учетной записи пользователя (правила см. Настройки безопасности) |
| *Пароль* | Да | Пароль учетной записи (правила см . Настройки безопасности) |
| *Подтверждение пароля* | Да | Пароль учетной записи |
| *Язык консоли* | Нет | Язык интерфейса для нового пользователя: *Русский* или *Английский* |

| Параметр | Обязательный параметр | Описание |
|---|---|---|
| *Контакты* | Нет | Номер мобильного телефона или email-адрес. Можно добавить одно или несколько значений |

4. Нажмите **Создать**. Новый пользователь будет добавлен в Систему. При первом входе в Систему он должен поменять пароль своей учетной записи.



## 5.2 Редактирование учетной записи

Для внесения изменений в учетную запись пользователя:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Выберите требуемого пользователя, нажмите  напротив его имени и выберите **Редактировать**.
3. В открывшемся окне измените одну или несколько настроек.
4. Нажмите **Сохранить**. Новые настройки вступят в силу.

## 5.3 Активация и деактивация пользователя

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

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Напротив требуемого пользователя нажмите  , затем выберите **Деактивировать**. Учетная запись пользователя будет заблокирована.

Чтобы разблокировать ранее заблокированную учетную запись:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Напротив заблокированного пользователя нажмите  , затем выберите **Активировать**. Разблокированный пользователь может снова работать в Системе.

## 5.4 Удаление пользователя

Главный офицер может удалять учетные записи пользователей. Для этого:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Выберите требуемого пользователя, нажмите  напротив его имени и выберите **Удалить**.
3. В открывшемся окне нажмите **ОК**. Учетная запись пользователя со всеми данными будет удалена без возможности восстановления.

Учетная запись Главного офицера удалению не подлежит.

# 6 Управление данными для анализа

События, доступные в Системе, хранятся в виде партиций. В Системе создаются два вида партиций:

- события с нарушениями;
- события без нарушений.

В разделе **Настройки** -> **Данные для анализа** отображается список партиций, каждая из которых создается в Системе еженедельно. Параметры партиции:

| Параметр | Описание |
|---|---|
| *Дата создания* | Дата создания партиции. Заполняется автоматически |
| *Статус* | *Активная партиция* или *Архивированная партиция* |
| *Дата архивирования* | Дата архивирования партиции. Заполняется автоматически при создании архива с партицией |
| *Нарушение* | Есть ли в партиции события с нарушениями |
| *Неделя* | Граничные даты недели создания партиции<br><br>⚠ **Примечание:**<br>Если в течение недели не было перехвачено ни одного события, то в списке партиций такая неделя будет пропущена. |
| *Год* | Год создания данных в партиции |

Чтобы снизить объем обрабатываемых данных, Офицеру безопасности доступны:

- Фильтрация по событиям, входящим в партиции;
- Установка периода хранения событий;
- Ручное архивирование и восстановление партиций.

## 6.1 Создание фильтра

Фильтрация событий позволяет выборочно загружать события из партиций для анализа, что позволяет существенно сэкономить ресурсы.

⚠ Фильтрация событий в партициях доступна, если была выполнена хотя бы одна синхронизация с системой-источником.

Чтобы настроить фильтр:

1. Перейдите в раздел **Настройки** -> **Данные для анализа**.
2. Нажмите **Настройки фильтрации,** а затем **+Добавить фильтр**. Отфильтровать данные можно:
    a. по *Уровню нарушения*;

b. по *Источникам данных;*
c. или применить оба фильтра.

3. Выберите уровень нарушения, события с которым будут попадать в результаты фильтра. Возможные значения (можно выбрать одно или несколько значений):
   a. *Отсутствует;*
   b. *Низкий ;*
   c. *Средний ;*
   d. *Высокий*.
4. Выберите источники данных, представляющие типы событий, которые попадут в результаты фильтра:
   a. *Skype;*
   b. *Web-сообщение;*
   c. *FTP;*
   d. *Веб-почта;*
   e. *Рабочая почта;*
   f. *Мессенджеры (Yahoo!, Jabber, WhatsApp, Viber,Telegram, Mail.Ru Агент, ICQ);*
   g. *Соцсеть (ВКонтакте, Facebook);*
   h. *Облачные хранилища;*
   i. *SMS;*
   j. *Фотосъемка;*
   k. *Сетевой ресурс;*
   l. *Терминальная сессия;*
   m. *Краулер;*
   n. *Ввод с клавиатуры;*
   o. *Печать;*
   p. *Снимки экрана;*
   q. *Съемные устройства;*
   r. *Буфер обмена* и др.
5. Нажмите **Применить**. Процесс применения фильтров может занять продолжительное время. В этом случае сначала будут выгружены ранее загруженные события, затем загружены новые в соответствии с заданными фильтрами.
6. В таблице **Данные для анализа** партиции будут показаны с учетом фильтров.

## 6.2 Хранение событий

Чтобы снизить объем хранимых данных, Офицер безопасности может установить, как долго необходимо хранить партиции. Для этого:

1. Перейдите в раздел **Настройки** -> **Данные для анализа**.
2. Нажмите **Настройки архивирования**.
3. В открывшемся окне укажите, сколько недель будут храниться события с нарушениями и события без нарушений. При этом:
   a. Если значение не задано, то все партиции за все время будут сохранены.
   b. Партиции с событиями, выходящие за рамки указанного периода, будут заархивированы автоматически.
4. Нажмите **Применить**.

## 6.3 Ручное архивирование и восстановление партиций

Чтобы снизить объем загруженных в Систему данных, Офицер безопасности может вручную архивировать партиции. Для этого:

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

Чтобы восстановить партицию:

1. Выберите архивированную партицию ( ).
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.

# 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 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:<br>- обязательно для ввода ( ☑ ) - обязательно присутствие букв в пароле<br>- опционально ( ☐ ) - допускается пароль без букв |
| *Цифры* | Арабские цифры, которые используются для составления пароля. Можно установить:<br>- обязательно для ввода ( ☑ ) - обязательно присутствие цифр в пароле<br>- опционально ( ☐ ) - допускается пароль без цифр |
| *Специальные символы* | Перечень спецсимволов, которые могут быть в пароле. Можно установить:<br>- обязательно ( ☑ ) - обязательно присутствие спецсимволов в пароле<br>- 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 |
| *Время действия пароля* | Количество дней действия пароля.До истечения указанного срока пароль необходимо сменить. |
| *Период для безуспешных попыток* | Период (в минутах), в течение которого пользователь может вводить неверный пароль |
| *Кол-во неуспешных попыток ввода* | Количество неуспешных попыток ввода, после чего учетная запись будет заблокирована |

| Параметр | Описание |
| --- | --- |
| *Период блокирования пользователя* | Период блокировки учетной записи в днях |

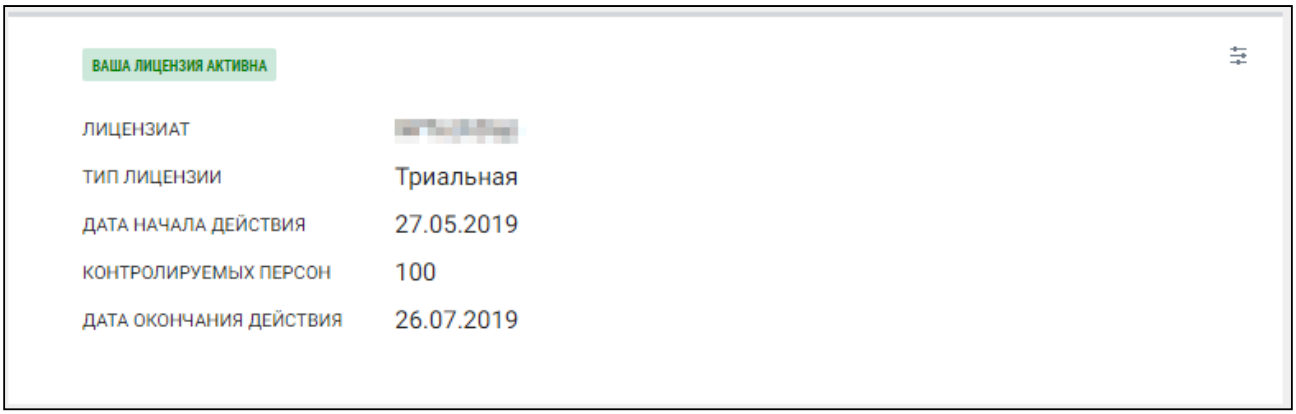
3. Нажмите **Сохранить**, чтобы новые параметры вступили в силу. Если нужно вернуться к прежним настройкам, нажмите **Настройки по умолчанию**.

   Пример
   Период для безуспешных попыток - 30
   Кол-во неуспешных попыток ввода - 4
   Период блокирования пользователя - 3
   Если установлены указанные параметры, то после 4-х неудачных попыток ввода пароля в течение 30 минут учетная запись пользователя будет заблокирована на 3 дня. После этого можно повторить ввод пароля.
   **Требования к учетной записи пользователя:**

- имя пользователя должно содержать не менее двух символов;
- логин пользователя в Системе должен содержать не менее двух символов.

# 8 Управление лицензиями

Работа в Системе возможна только при наличии действующей лицензии. При первом входе в Систему установлена срочная пробная лицензия сроком на один месяц:




Чтобы установить новую лицензию:

1. Перейдите в раздел **Лицензирование**.
2. Нажмите **+Добавить**.
3. В открывшемся окне укажите путь до файла с действующей лицензией.

Чтобы удалить лицензию:

1. Нажмите  в углу плитки лицензии и выберите **Удалить**.
2. В открывшемся окне подтвердите действие, нажав **ОК**.

**Важно!**

Перед тем, как удалить старую лицензию, убедитесь в наличии файла с новой действующей лицензией. Работа в Системе без лицензии невозможна. После смены лицензии рекомендуется провести заново все интеграции с источниками данных.

**Важно!**

При истечении срока действия срочной пробной лицензии будет прекращена загрузка данных из источников.

# 9 Управление загрузкой оргструктуры

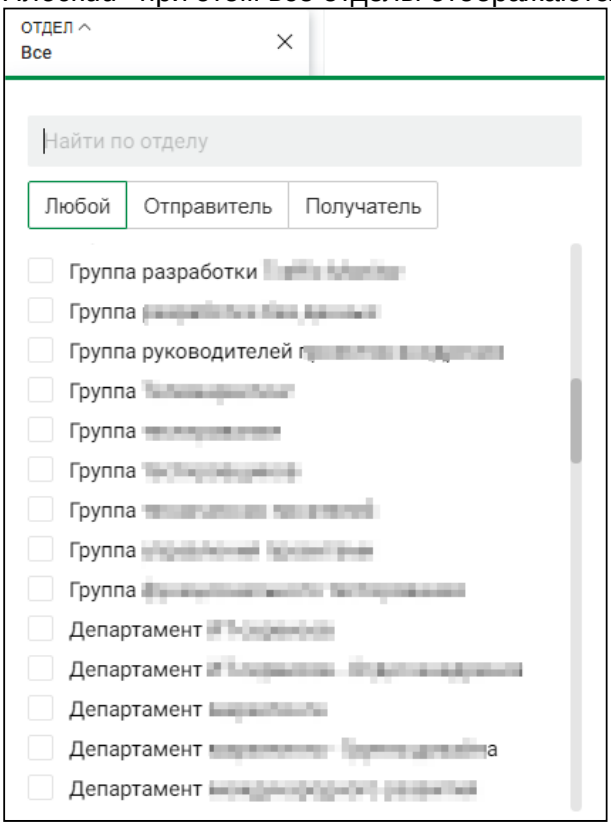
В разделе находятся настройки загрузки в Систему:

- Списков отделов компании;
- Внутренних доменов компании.

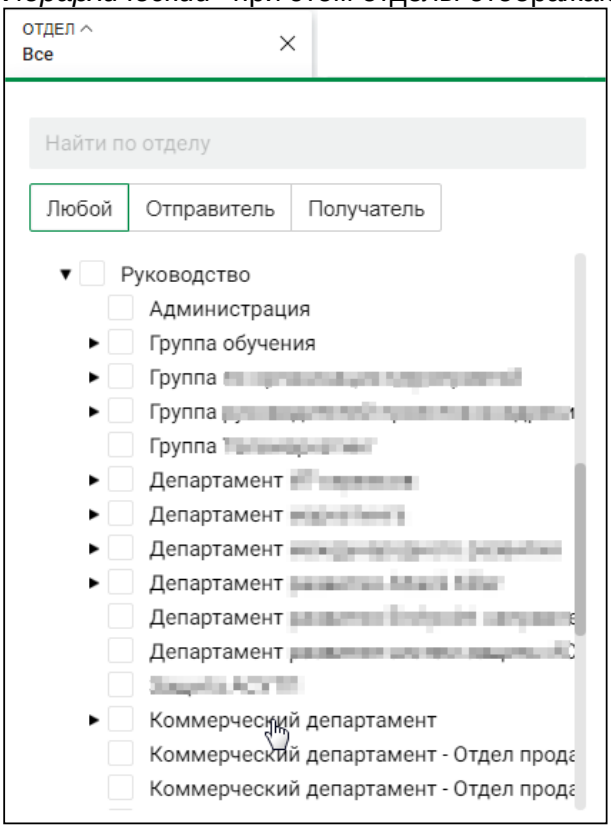
## 9.1 Настройка отображения

При синхронизации с ActiveDirectory Система получает список отделов. Офицер безопасности может настроить отображение этого списка в Едином фильтре:

- *Плоский* - при этом все отделы отображаются в списке на одном уровне;



- *Иерархический* - при этом отделы отображаются в виде дерева.




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

## 9.2 Внутренние домены

Офицер безопасности создает список доменов, контакты с которыми будут относиться к внутренним контактам.

Чтобы добавить внутренний домен:

1. На вкладке **Настройки** нажмите **Добавить новый**.
2. Введите имена доменов в формате *companyname.ru.*
3. Нажмите **Сохранить**. Дальнейшие контакты с этим доменом Система будет рассматривать как внутренние.

Чтобы удалить внутренний домен:

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

# 10 Уведомления

Уведомления сообщают пользователю о статусе синхронизаций с различными источниками, которые инициировал пользователь.

