

INFOWATCH

InfoWatch Device Monitor for Linux. Руководство пользователя

22/06/2023

© 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 Обзор 8

5 Настройки пользователей 9

5.1 Пользователи 9

5.1.1 Создание нового пользователя 9

5.1.2 Просмотр профиля пользователя 10

5.1.3 Редактирование учетной записи 11

5.1.4 Смена пароля пользователя 11

5.1.5 Активация и деактивация пользователя 12

5.1.6 Удаление пользователя 12

5.2 Роли 12

6 Общие настройки 13

6.1 Управление безопасностью 13

6.2 Мониторинг состояния Системы 14

6.3 Интеграции 16

6.3.1 Интеграция с Active Directory 16

6.3.2 Редактирование и удаление интеграции 19

7 Настройка Device Monitor 20

7.1 Соединение с сервером Traffic Monitor 20

7.2 Исключение приложений из перехвата 21

7.3 Настройки перехвата мессенджеров 22

8 Интерфейс Веб-консоли Device Monitor 23

8.1 Политики 24

8.2 Компьютеры 25

8.3 Задачи 26

9 Настройка Системы после установки 27

9.1 Создание и редактирование группы компьютеров 27

9.2 Добавление компьютера в группу ... 27
9.3 Просмотр сведений о компьютерах ... 28
9.4 Задача первичного распространения и обновления ... 31
10 Настройка схемы безопасности ... 33
10.1 Создание политик ... 33
10.2 Создание правил ... 33
10.2.1 Правило контроля съемных устройств ... 33
10.2.2 Правило контроля сетевых ресурсов ... 34
10.2.3 Правило контроля печати ... 36
10.2.4 Правило контроля FTP ... 37
10.2.5 Правило контроля мессенджера VK ... 38
10.2.6 Правило контроля HTTP(S) ... 38
10.2.7 Правило контроля почты ... 39
10.2.8 Правило контроля ввода текста с клавиатуры ... 40
10.2.9 Правило контроля облачных хранилищ ... 41
11 Пользовательское лицензионное соглашение ... 42

В настоящем документе содержится инструкция по работе в Веб-консоли InfoWatch Device Monitor for Linux (далее Система или Device Monitor).

1 Аудитория

Данное руководство предназначено для инженеров внедрения и офицеров безопасности, которые будут работать с Системой и заниматься ее администрированием. Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Windows и Linux.

2 Комплект документов

В документацию входят:

- «InfoWatch Device Monitor for Linux. Руководство по установке». Документ содержит описание установки Сервера, Веб-консоли и Агентов, входящих в Систему.
- «InfoWatch Device Monitor for Linux. Руководство пользователя». Содержит описание работы в Веб-консоли для решения задач.

Сопутствующая документация по системе InfoWatch Traffic Monitor (далее 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 InfoWatch Traffic Monitor (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, подготовка 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 РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

4 Обзор

InfoWatch Device Monitor – это система, позволяющая контролировать обмен данными на рабочих станциях сотрудников. Собранные данные передаются для анализа в систему InfoWatch Traffic Monitor.

Основные функции InfoWatch Device Monitor:

- контроль файлов, копируемых со съемных устройств и сетевых ресурсов ("Правило контроля съемных устройств");
- мониторинг печати на контролируемых компьютерах ("Правило контроля печати");
- контроль систем передачи почтовых сообщений по протоколам SMTP, POP3, IMAP и HTTPS ("Правило контроля почты");
- контроль трафика, передаваемого по протоколам HTTP и HTTPS ("Правило контроля HTTP(S)");
- контроль обмена данными по протоколу FTP/FTPS ("Правило контроля FTP");
- контроль обмена сообщениями и файлами в мессенджере VK ("Правило контроля мессенджера VK");
- контроль обмена данными с сетевыми ресурсами ("Правило контроля сетевых ресурсов");
- контроль ввода текста с клавиатуры ("Правило контроля ввода текста с клавиатуры") для рабочих станций под управлением РЕД ОС;
- контроль облачных хранилищ ("Правило контроля облачных хранилищ");
- передача полученных данных в систему InfoWatch Traffic Monitor для анализа.

5 Настройки пользователей

Раздел содержит справочник пользователей – Офицеров безопасности, которые могут работать в Системе, и описание ролей, которые определяют компетенции пользователя в Системе.

Для каждого пользователя, в задачи которого входит управление схемой безопасности, создается учетная запись в веб-консоли. Данные учетной записи используются при авторизации в Системе, на их основании определяются права на выполнение тех или иных действий.

В веб-консоли используется один предустановленный пользователь – **Суперпользователь,** обладающий всеми правами при работе в ней. Для разграничения полномочий пользователей используются роли. Есть возможность для одного пользователя задать разные роли на разные группы. Для каждой роли определен набор полномочий. Пользователь не может выполнять действия, которые выходят за рамки назначенной ему роли.

В веб-консоли используются следующие предустановленные роли:

- **Главный офицер безопасности** – роль администратора, позволяющая управлять другими учетными записями;
- **Офицер безопасности** – роль пользователя, позволяющая управлять схемой безопасности и настройками Сервера.

5.1 Пользователи

При установке Системы создается предустановленный пользователь – Главный офицер. Чтобы войти в Систему, выберите **InfoWatch Device Monitor** в списке установленных продуктов и введите логин и пароль по умолчанию:

Логин	Пароль
officer	xxXX1234

При первом входе в Систему вы должны будете сменить пароль на постоянный (см. "Смена пароля пользователя").

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

- Главный Офицер безопасности;
- Офицер безопасности (ОБ), подчиненный ему.

Целевые действия:

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

5.1.1 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 таблице:

Параметр	Обязательный параметр	Описание
Фотография	Нет	Фотография пользователя
Имя пользователя	Да	Имя нового пользователя (правила составления имени см. "Управление безопасностью")
Логин	Да	Имя учетной записи пользователя (правила см. "Управление безопасностью"). Логин не зависит от верхнего или нижнего регистра
Пароль	Да	Пароль учетной записи (правила см. "Управление безопасностью")
Подтверждение пароля	Да	Пароль учетной записи
Роли	Нет	Роль пользователя в Системе. Пользователю может быть назначена только одна роль
Язык консоли	Нет	Язык интерфейса для нового пользователя: *Русский* или *Английский*
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 (см. "Смена пароля пользователя").

5.1.2 Просмотр профиля пользователя

На странице профиля представлены:

1. Вкладка **Персональная информация**. Содержит данные, указанные при создании:
   - фото пользователя;
   - имя пользователя;
   - логин пользователя в Системе;
   - язык, используемый пользователем в Системе;
   - статус пользователя: – активный, – деактивирован;
   - контактные данные: номера телефонов, адреса электронной почты;
   - журнал последних активностей с учетной записью .
2. Вкладка **Права доступа**. Содержит информацию о правах пользователя в Системе:

- роль, назначенная пользователю;
- доступные для выполнения функции:
    - доступ, который имеет данный пользователь к настройкам и продуктам;
    - совокупность данных, к которым пользователь имеет доступ.

Чтобы снять или назначить новую роль, перейдите в окно редактирования учетной записи (см. "Редактирование учетной записи").

Действия пользователя:

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

5.1.3 Редактирование учетной записи

Для внесения изменений в учетную запись пользователя:

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

5.1.4 Смена пароля пользователя

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

1. Выполните одно из следующих действий:
    - в разделе **Настройки** -> **Пользователи** нажмите  напротив нужного пользователя;
    - в профиле пользователя нажмите ;
    - войдите в главное меню пользователя.
2. Выберите **Сменить пароль**.
3. Заполните поля:

Поле	Описание
Старый пароль	Введите действующий пароль
Новый пароль	Введите новый пароль. Новый пароль должен удовлетворять настройкам безопасности (см. "Управление безопасностью")
Подтверждение пароля	Введите новый пароль еще раз

4. Нажмите **Сохранить**.

5.1.5 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  (или  в профиле пользователя).
3. Выберите **Деактивировать**. Учетная запись пользователя будет заблокирована.

Чтобы разблокировать ранее заблокированную учетную запись:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Напротив заблокированного пользователя нажмите  (или  в профиле пользователя).
3. Выберите **Активировать**. Разблокированный пользователь может снова работать в Системе.

Учетная запись Главного офицера деактивации не подлежит.

5.1.6 Удаление пользователя

Главный офицер может удалять учетные записи пользователей. Для этого:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Нажмите  напротив нужного пользователя (или  на странице профиля пользователя).
3. Выберите **Удалить**.
4. В открывшемся окне нажмите **ОК**. Учетная запись пользователя со всеми данными будет удалена без возможности восстановления.

Учетная запись Главного офицера удалению не подлежит.

5.2 Роли

Пользователи Системы могут иметь разные роли, которые определяют их права в Системе. Один пользователь может иметь только одну роль. В случае если пользователю не назначена ни одна роль, его доступ в Систему невозможен.

В Системе есть две предустановленные роли:

1. **Главный офицер безопасности** – имеет полный доступ ко всем данным Системы и ее настройкам и управлению ролями, включая:
    - создание новых пользователей;
    - создание новых ролей и назначение их пользователям.
2. **Офицер безопасности** – имеет полный доступ к данным Системы, кроме раздела **Настройки**.

6 Общие настройки

Раздел содержит общие настройки, распространяющиеся на установленные продукты InfoWatch, и включает в себя:

- Управление безопасностью
- Мониторинг состояния
- Соединение с сервером Traffic Monitor
- Исключение приложений из перехвата

6.1 Управление безопасностью

Чтобы предотвратить несанкционированный вход в Систему и максимально обезопасить пользователя от компрометации его учетных данных, вы можете 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 ввести 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 присутствие букв в пароле - опционально (☐) – допускается пароль без букв
Цифры	Арабские цифры, которые используются для составления пароля. Можно установить: - обязательно для ввода (☑) – обязательно присутствие цифр в пароле - опционально (☐) – допускается пароль без цифр
Специальные символы	Перечень спецсимволов, которые могут быть в пароле. Можно установить: - обязательно (☑) – обязательно присутствие спецсимволов в пароле - опционально (☐) – допускается пароль без спецсимволов
Минимальная длина	Минимально допустимая длина пароля в символах
Нельзя использовать последние N паролей	Чтобы избежать компрометации, запрещено использовать пароли за предыдущие периоды

Параметр	Описание
Время действия пароля	Количество дней действия пароля. До истечения указанного срока пароль необходимо сменить
Период неудачных попыток авторизации	Период (в минутах), в течение которого пользователь может вводить неверный пароль
Количество неудачных попыток ввода	Количество неуспешных попыток ввода пароля, после которого учетная запись будет заблокирована
Период блокировки пользователя	Период блокировки учетной записи (в минутах)

3. Нажмите **Сохранить**, чтобы новые параметры вступили в силу. Если нужно вернуться к прежним настройкам, нажмите **Сбросить настройки до значений умолчанию**.

> **Пример**
>
> `Период неудачных попыток авторизации – 5.`
>
> `Количество неудачных 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. После этого можно повторить ввод пароля.

Требования к имени пользователя и учетной записи

Имя пользователя должно содержать не менее четырех символов.

Логин пользователя:

- должен начинаться с буквы и не заканчиваться точкой;
- может состоять из букв латинского алфавита, арабских цифр и содержать спецсимволы: "_", "-", "–", ".".

6.2 Мониторинг состояния Системы

Подсистема мониторинга выполняет проверку работы всех узлов распределенной сети, входящих в состав Системы. При этом анализируется доступность узла, информация от его основных аппаратных компонентов, а также информация о состоянии всех служб Системы.

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

Поле	Описание
Адрес	IP-адрес ноды InfoWatch Device Monitor

Поле	Описание
Последнее обновление статуса	Дата и время получения информации о статусе узла: • *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 Device Monitor
Память	Общий объем оперативной памяти сервера и сколько памяти занято
ЦПУ	Загрузка центрального процессора сервера InfoWatch Device Monitor
Дисковое пространство (Root)	Общее выделенное и занятое место, отведенное для системных данных в корневой директории
Дисковое пространство (DataStorage)	Общее выделенное и занятое место на диске для DataStorage
Дисковое пространство (Tarantool)	Общее выделенное и занятое место на диске для хранения данных БД Tarantool
Дисковое пространство (Clickhouse)	Общее выделенное и занятое место на диске для хранения данных БД Clickhouse
Дисковое пространство (PostgreSQL)	Общее выделенное и занятое место на диске для хранения данных БД PostgreSQL
Список всех служб узла InfoWatch Vision	
Статус	Служба может иметь один из следующих статусов: • *Запущена* – работает; • *Недоступна* – невозможно получить статус; • *Не инициализирована* – находится в процессе запуска; • *Не найдена* – должна быть на узле, но отсутствует; • *Ошибка* – завершена с ошибкой.
Имя	Имя службы в Системе

Поле	Описание
Версия	Версия сборки службы
Просмотреть детали	Вывод информации о состоянии, событиях и внутренних сообщениях службы

Все события мониторинга в Системе записываются в журнал.

Чтобы скачать весь журнал:

1. Сформируйте лог-файлы по всем службам. Для этого нажмите **Экспорт диагностических данных**. После формирования начнется загрузка.
2. Скачайте zip-архив, содержащий txt-файлы с логами.

Чтобы скачать диагностические данные отдельной службы:

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

6.3 Интеграции

Для получения данных о персонах, группах и рабочих станций в виде актуального дерева каталогов необходимо настроить синхронизацию с Active Directory. Полученные данные используются в для построения актуального дерева каталогов, распространения и обновления Агентов.

В этом разделе:

- Интеграция с Active Directory
- Редактирование и удаление интеграции

6.3.1 Интеграция с Active Directory

Чтобы добавить новую интеграцию с Active Directory и запустить ее:

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

Параметр	Описание
Имя интеграции	Название интеграции
Филиал	Нода для подключения: головное отделение или филиал
Адрес источника	Сетевой адрес сервера, с LDAP-каталогами которого производится синхронизация
Тип соединения	Выбор типа соединения, которое будет установлено: • Незащищенное соединение (LDAP);

Параметр	Описание
	• Защищенное соединение по протоколу LDAP + StartTLS; • Защищенное соединение по протоколу LDAPS (SSL). **Важно!** Соединение без сертификатов небезопасно.
Сертификат	Загрузка файла сертификата в формате .pem для защищенных соединений
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.

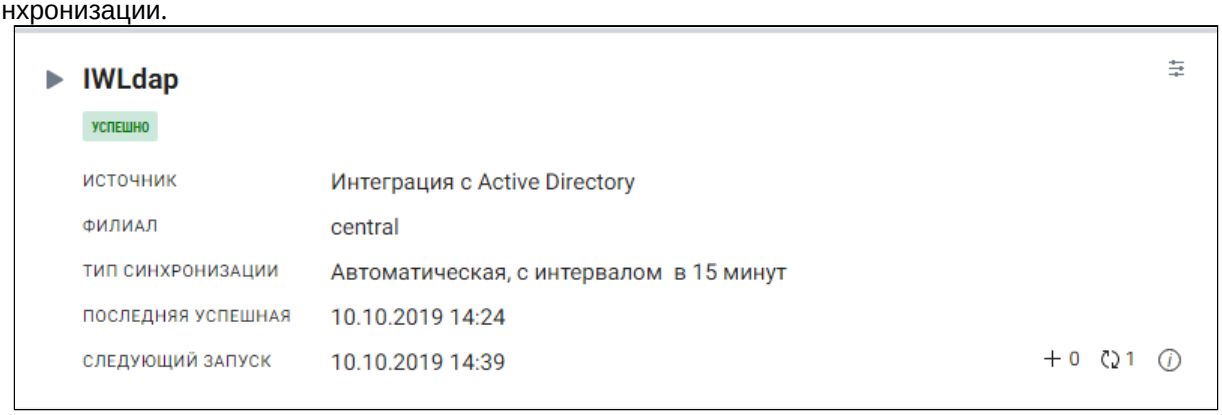
LDAP запрос	Атрибуты фильтрации, являющиеся полным путем к указанному каталогу. При этом может быть указан только один каталог в организационной структуре Active Directory. Для оптимизации поиска вы можете использовать отдельные уровни иерархии базы:
	`C-countryName`
	`O-organizationName`
	`OU-organizationalUnitName`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

Логин	Логин для доступа к серверу Active Directory
Пароль	Пароль для доступа к серверу Active Directory
Синхронизация	*Ручная* или *Автоматическая*. Во втором варианте необходимо указать *Периодичность* и *Повторение*

Параметр	Описание
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.

Возможна последовательная синхронизация с несколькими различными 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, сколько 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 .
2. Дождитесь изменения 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.

Важно!

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

6.3.2 Редактирование и удаление интеграции

Чтобы внести изменения в уже созданную интеграцию:

1. Дождитесь, пока данные синхронизируются или нажмите  в левом углу, чтобы остановить процесс синхронизации.
2. Нажмите  в правом углу и выберите **Редактировать**.
3. Внесите нужные изменения.
4. Нажмите **Сохранить**.

Чтобы удалить устаревшую интеграцию:

1. Нажмите  в правом углу.
2. Выберите **Удалить**, а затем нажмите **ОК**.

7 Настройка Device Monitor

В этом разделе:

- Соединение с сервером Traffic Monitor
- Исключение приложений из перехвата
- Настройки перехвата мессенджеров

7.1 Соединение с сервером Traffic Monitor

Для того чтобы иметь возможность отправлять события на анализ в InfoWatch Traffic Monitor, необходимо настроить:

- общие параметры для всех серверов Device Monitor;
- параметры хранения и удаления событий;
- параметры соединения с сервером Traffic Monitor.

Чтобы задать общие настройки, которые распространяются на основной и все вспомогательные сервера Device Monitor:

1. Перейдите в раздел **Настройки** > **Серверы**.
2. На вкладке **Общие** задайте следующие настройки:
   - **Количество теневых копий, получаемых сервером одновременно** – определяет количество копий, которые могут поступить на сервер в один момент времени;
   - **Количество агентов, одновременно обрабатывающих уведомления от сервера** – определяет количество агентов, которые могут получать уведомления (например, политику безопасности) от сервера в один момент времени;
   - **Рабочая версия для установки и обновления агентов** – определяет версию для задач распространения агентов Device Monitor. Эта же версия задана по умолчанию для задач первичного распространения и обновления, если они создаются вручную (см. "Задача первичного распространения и обновления").

Чтобы настроить параметры хранения и удаления событий:

1. Перейдите в раздел **Настройки** > **Серверы**.
2. На вкладке **Хранение событий** укажите:
   - **Удалять события в статусе "Отправлено на ТМ"** – чтобы удалять события, отправленные на сервер Traffic Monitor для последующего анализа. При этом события со статусами **Обработано** и **Отправлено в ТМ**, будут удаляться раз в сутки либо при старте сервера;
   - **Хранить события** – чтобы определить время, в течение которого событие будет находиться в базе данных и отображаться в консоли управления, в том числе для событий со статусом **Ошибка отправки в ТМ** или **Нет лицензии**. По умолчанию срок хранения событий – 1 неделя. При этом будут удалены все события, сформированные ранее указанного периода;
   - **Разделять по периодам** – чтобы разделить события на блоки по времени создания для ускорения процессов обращения.

Если параметры для удаления не отмечены, события со статусами **Обработано** и **Отправлено в ТМ** должны храниться в соответствии с параметрами хранения, после чего должно быть произведено удаление.

Чтобы просмотреть или настроить параметры соединения с сервером InfoWatch Traffic Monitor:

1. Перейдите в раздел **Настройки** > **Серверы**.
2. По умолчанию установлен только основной сервер Device Monitor. Выберите его, чтобы перейти в настройки.

> **Примечание:**
>
> Чтобы установить вспомогательный сервер Device Monitor, пройдите шаги инструкции "Установка Сервера Device Monitor".

3. На странице настроек сервера подключения отображается информация по следующим параметрам соединения:
   - **Роль сервера** – роль сервера (*основной* или *вспомогательный*), назначенная при его установке;
   - **Номер порта для протокола уведомлений**. По умолчанию – 15100;
   - **Номер порта для основного протокола**. По умолчанию – 15101;
   - **Адрес сервера Traffic Monitor** – IP-адрес или имя сервера InfoWatch Traffic Monitor, на который будут доставляться события. Возможные форматы записи: `host:port.` Адрес указывается на этапе установки InfoWatch Device Monitor. В качестве параметра `port` указывается порт сервера InfoWatch Traffic Monitor, через который будет осуществляться доставка событий. По умолчанию, порт сервера InfoWatch Traffic Monitor – 9100;
   - **Токен Traffic Monitor** – токен для подключения к API, который указывается на этапе установки InfoWatch Device Monitor. Вы можете получить актуальный токен от администратора Traffic Monitor или сформировать токен самостоятельно в Консоли управления.
4. Если требуется установить соединение с другим сервером Traffic Monitor, измените адрес сервера и токен.
5. Нажмите **Применить**.

7.2 Исключение приложений из перехвата

Вы можете указать приложения, активность которых не будет перехватываться Системой.

Чтобы просмотреть и настроить параметры исключения приложений из перехвата:

1. Перейдите в раздел **Настройки** > **Исключение приложений из перехвата**.
2. В правой части рабочей области нажмите [+].
3. В открывшемся окне введите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.
4. Введите краткое описание. Поле обязательно для заполнения. Вместо имени приложения можно ввести символ *. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути.
5. Укажите расположение файла – папку на компьютере с Агентом Device Monitor, содержащую исполняемый файл приложения, либо папку верхнего уровня (возможно использование системных переменных). Заданная строка должна быть в начале пути к файлу. Например, если исключение задано в виде: `/opt/myapps`, то из перехвата будут исключены все приложения папке `myapps`, а также любой ее подпапке.

6. Укажите ОС, для которой настраивается исключение. Чтобы исключение работало на всех поддерживаемых ОС семейства Linux, выберите вариант **Любой дистрибутив Linux**.
7. Нажмите **Создать**. Чтобы применить исключение приложение из перехвата или отмену такого исключения, перезапустите приложение.

7.3 Настройки перехвата мессенджеров

Для настройки периодичности получения событий с теневыми копиями чата укажите:

- через сколько минут после начала общения в чате необходимо создать теневую копию.
- количество сообщений в чате, при достижении которого необходимо создать теневую копию.

После установки значений нажмите **Применить**. Настройки будут действовать для всех правил контроля мессенджеров.

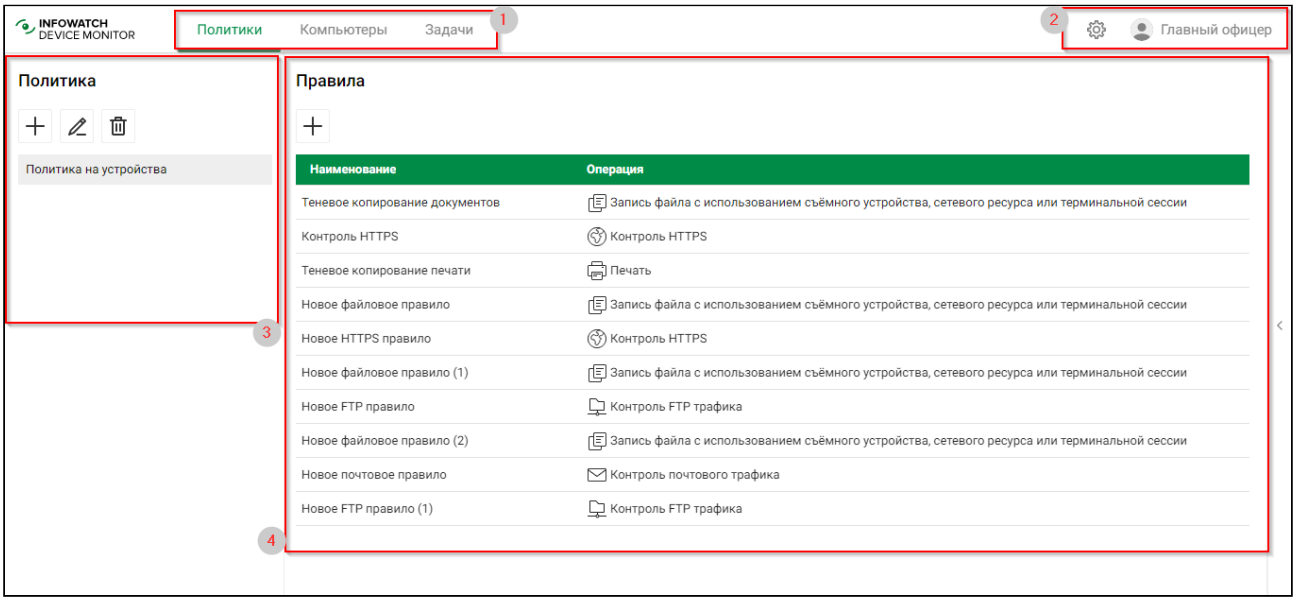
Создание каждой последующей теневой копии по установленным настройкам осуществляется в зависимости от того, какая из настроек сработала первой.

8 Интерфейс Веб-консоли Device Monitor

Веб-консоль Device Monitor предназначена для решения следующих задач:

- управление доступом к системе InfoWatch Device Monitor;
- настройка системы мониторинга компьютеров;
- контроль доступа к компьютерам.

Интерфейс InfoWatch Device Monitor содержит несколько областей с настройками и данными (на примере основного раздела **Политики**).



Элементы интерфейса:

Номер на схеме	Элемент окна	Назначение элемента
1	Панель навигации	Выбор рабочего раздела Device Monitor: • **Политики** – управление политиками Device Monitor: создание политик, настройка правил для каждой политики • **Компьютеры** – управление контролируемыми компьютерами: создание групп компьютеров, добавление распределение контролируемых компьютеров по группам • **Задачи** – централизованная установка, обновление и удаление Агентов InfoWatch Device Monitor на компьютеры
2	Меню пользователя	Пользовательское меню, в котором вы можете:

Номер на схеме	Элемент окна	Назначение элемента
		• выбрать язык интерфейса: *Русский* или *Английский*; • узнать контактные данные компании InfoWatch и службы поддержки; • выйти из Системы.
	Настройки	Раздел настроек, содержащий: • Настройки пользователей • Общие настройки • Настройка Device Monitor
3-4	Рабочая область	Отображение элементов выбранного раздела Device Monitor и работа с ними

8.1 Политики

Политика – совокупность правил, в соответствии с которыми проводится анализ и обработка объектов перехвата.

Назначение политики группе компьютеров происходит в соответствии со следующими принципами:

- Каждой группе компьютеров обязательно должна быть назначена политика. Добавление новой группы компьютеров невозможно, если для данной группы не определена политика. Поэтому сначала нужно создать политику, после чего создать группу и выбрать для нее политику.
- Группе компьютеров не может быть назначено более одной политики.
- Одна и та же политика безопасности может быть назначена нескольким группам компьютеров, однако рекомендуется, чтобы каждой группе компьютеров была назначена своя политика безопасности.

Важно!

В случае многопользовательского доступа к рабочей станции и при невозможности определения инициатора процесса (события) правила перехвата для сотрудников учитываться не будут. Будут работать правила перехвата только для данной рабочей станции. В связи с этим необходима настройка правил перехвата не только для сотрудников, но и для рабочей станции, к которой возможен многопользовательский доступ.

Правила – это набор ограничений и условий, в соответствии с которыми осуществляется мониторинг операций, связанных с переносом файлов на съемные устройства и сетевые ресурсы, сетевой активностью и отправкой документов на печать. Для каждой политики создается свой набор правил.

В Device Monitor существуют следующие типы правил:

- **Контроль съемных устройств**. Позволяет отслеживать действия с файлами на съемных устройствах:
    - создание файла непосредственно на съемном устройстве;
    - копирование/перемещение файла на съемное устройство. В данном случае отслеживаются операции копирования/перемещения файла с контролируемого компьютера, другого съемного устройства или сетевых ресурсов.
- **Контроль сетевых ресурсов**. Позволяет отслеживать действия с сетевыми ресурсами:
    - копирование файла на сетевые ресурсы с использованием UNC (например, *Server**SharedFolder**Folder**File*);
    - перехват копирования файлов с сетевых ресурсов;
    - запрет копирование файлов на сетевые ресурсы.
- **Контроль HTTP(S)**. Позволяет контролировать обмен данными по протоколам HTTP и HTTPS. Система позволяет создавать теневые копии передаваемых файлов.
- **Контроль почты**. Позволяет контролировать отправку и получение электронной почты. Система позволяет полностью запрещать или разрешать использование почты, либо разрешать только получение почты, а также создавать теневые копии передаваемых файлов.
- **Контроль печати**. Позволяет отслеживать действия, связанные с печатью документов на локальных и сетевых принтерах. Также возможно создавать теневую копию задания на печать.
- **Контроль FTP**. Позволяет контролировать обмен данными по протоколу FTP/FTPS. Система позволяет ограничивать или полностью запрещать использование FTP/FTPS протокола, а также создавать теневые копии передаваемых файлов.
- **Контроль мессенджера VK**. Позволяет контролировать доступ сотрудников к сервису мгновенного обмена сообщениями VK. Система позволяет снимать копию чата и создавать теневые копии исходящих файлов.
- **Контроль ввода текста с клавиатуры**. Позволяет перехватывать ввод текста с клавиатуры в окне любого приложения на рабочих станциях и формировать события при смене активного окна.
- **Контроль облачных хранилищ**. Позволяет контролировать веб-клиенты облачных хранилищ.

8.2 Компьютеры

Под компьютерами в системе Device Monitor понимаются контролируемые компьютеры, на которых установлены Агенты Device Monitor.

Действующие политики могут быть назначены только группе компьютеров. Определение политики для отдельного компьютера выполняется путем включения компьютера в ту или иную группу.

Компьютер, зарегистрированный в Device Monitor, должен входить как минимум в одну группу компьютеров (**Группу компьютеров по умолчанию**). Это связано с тем, что политика безопасности не может быть назначена отдельному компьютеру.

В **Группу компьютеров по умолчанию** входят все компьютеры, для которых не определены другие группы компьютеров:

- компьютеры, впервые зарегистрированные в Device Monitor;
- компьютеры, исключенные из всех прочих групп компьютеров.

После установки Системы на **Группу компьютеров по умолчанию** назначена **Политика на устройства**.

Исключить компьютер из **Группы компьютеров по умолчанию** можно при условии, что компьютер добавлен хотя бы в одну группу компьютеров, помимо нее.

Информация по работе с контролируемыми компьютерами содержится в подразделах:

- Создание и редактирование группы компьютеров
- Добавление компьютера в группу
- Просмотр сведений о компьютерах

8.3 Задачи

В разделе **Задачи** выводится перечень всех созданных, выполненных и невыполненных задач. В рабочей области главного окна отображается список рабочих станций, для которых выполняется выбранная задача.

На панели **Подробно** отображаются параметры, заданные при создании выбранной задачи. Чтобы скрыть панель, нажмите .

Подробнее о задачах см. "Задача первичного распространения и обновления".

9 Настройка Системы после установки

В этом разделе:

- Создание и редактирование группы компьютеров
- Добавление компьютера в группу
- Просмотр сведений о компьютерах
- Задача первичного распространения и обновления

9.1 Создание и редактирование группы компьютеров

> **Важно!**
>
> Когда регистрируется новый компьютер, информация о нем автоматически добавляется в схему безопасности (в группу компьютеров «по умолчанию»).

Чтобы добавить группу компьютеров:

1. Перейдите в раздел **Компьютеры**.
2. В левой части рабочей области нажмите 
3. В открывшемся окне укажите следующие параметры:
   - **Наименование** группы;
   - **Политика**. Выберите из раскрывающегося списка политику, которая будет назначена данной группе компьютеров.
4. Нажмите **Сохранить**. Будет создана новая группа компьютеров, в которую необходимо добавить компьютеры.

Чтобы отредактировать группу компьютеров:

1. Выделите нужную группу.
2. Нажмите  и внесите изменения.
3. Нажмите **Сохранить**.

Чтобы удалить группу компьютеров:

1. Выделите группу для удаления. Группу компьютеров «по умолчанию» удалить нельзя.
2. Нажмите . В группе компьютеров, которую вы удаляете, могут быть компьютеры, не включенные в другие группы. В этом случае компьютеры будут автоматически добавлены в группу компьютеров «по умолчанию».
3. В открывшемся окне нажмите **Подтвердить**.

9.2 Добавление компьютера в группу

При установке Агента InfoWatch Device Monitor на компьютер в Системе автоматически создается запись о компьютере. Эта запись добавляется в группу «по умолчанию». На все компьютеры, входящие в эту группу, будет распространяться политика, назначенная данной группе. В дальнейшем определение политик для компьютера происходит путем его включения в различные группы компьютеров.

Чтобы добавить компьютер в группу:

1. Перейдите в раздел **Группы компьютеров**.

2. В левой части рабочей области выберите название необходимой группы. После этого в рабочей области главного окна будет выведен список всех компьютеров, уже входящих в группу.
3. Нажмите .
4. В открывшемся диалоговом окне выберите компьютеры из числа ранее зарегистрированных в Системе, т.е. компьютеры, на которых установлен Агент из группы «по умолчанию» и других групп.
5. Отметьте необходимые компьютеры или группы компьютеров. Чтобы развернуть или свернуть группу, используйте .
6. Нажмите **Добавить**. Компьютер будет включен в выбранную группу.

Если компьютер включен в определенную группу компьютеров, ему будут назначены политики выбранной группы. Чтобы отменить действие какой-либо политики безопасности на компьютер, исключите его из группы, которой назначена эта политика.

Чтобы исключить компьютер из группы компьютеров:

1. Выберите строку с именем компьютера, который нужно исключить из группы компьютеров.
2. Нажмите .
3. Нажмите **Да**. Если компьютер входил только в одну группу, то при исключении он будет автоматически добавлен в группу компьютеров «по умолчанию».

9.3 Просмотр сведений о компьютерах

В левой части рабочей области выводится перечень групп компьютеров. В правой части отображается перечень компьютеров, входящих в состав выделенной группы компьютеров.

Информация по компьютерам представлена в виде табличного списка. В столбцах выводятся основные свойства компьютеров. Вы можете менять порядок столбцов, а также скрывать столбцы, отображать которые не требуется.

Табличный список содержит следующие основные сведения:

- **Имя**. Доменное имя рабочей станции.
- **Статус**. Состояние Агента, установленного на компьютере. Данный параметр может принимать одно из следующих значений:
  - **Не установлен**. Агент никогда не устанавливали на рабочую станцию, либо она была добавлена в схему безопасности без агента;
  - **Установлен**. Агент установлен на рабочую станцию через задачу первичного распространения, или в схему безопасности была добавлена рабочая станция с установленным Агентом;
  - **Работает с ограничениями функциональности**. Агент установлен на рабочую станцию, но работает частично. Например, этот статус будет выставлен после старта Агента при проверке на загрузку и совместимость необходимых драйверов ядра ОС;
  - **Остановлен**. Агент установлен на рабочую станцию и остановлен через Консоль Device Monitor;

    Примечание:

Если остановленный агент был обновлен, то после завершения обновления он будет запущен.

- **Работает в диагностическом режиме**. Агент установлен на рабочую станцию и переведен в диагностический режим работы через Консоль Device Monitor;
- **Золотой образ**. Агент установлен на рабочую станцию, которой назначен статус «Золотой образ» – образ компьютера, из которого будут создаваться новые виртуальные машины (например, для создания однотипных серверов или рабочих станций для пользователей, решающих однотипные задачи);
- **Удален**. Агент удален с рабочей станции через задачу удаления продукта или средствами самой рабочей станции.

- **Активность Агента**. Статус активности Агента, установленного на компьютере. Данный параметр может принимать одно из следующих значений:
  - **Активен**. Агент регулярно выходит на связь с сервером, передает события, данные;
  - **Не активен**. Агент регулярно не выходит на связь с сервером или отключен;
  - **Не активен более недели**. Агент не выходит на связь с сервером более недели;
  - **Не активен более месяца**. Агент не выходит на связь с сервером более месяца.

Примечание:

При удалении Device Monitor статус отправляется Агентом по протоколу UDP, не гарантирующему доставку. Кроме того, уведомление отправляется в случае, если с сервером Device Monitor уже была установлена сессия и сообщение отправляется тому серверу, с которым Агент взаимодействует в данный момент.

- **Время регистрации**. Дата и время регистрации рабочей станции (добавление в БД);
- **Время подключения**. Дата и время подключения к серверу Агента, установленного на компьютере. Подключение выполняется при старте клиента. Также, чтобы распределить нагрузку, периодически происходит переподключение к пулу серверов. При каждом успешном подключении дата и время в поле **Время подключения** меняется. При запуске Агента после остановки будет установлено соединение с сервером и значение поля **Время подключения** обновится;

Примечание.

Для компьютера со статусом Агента **Не установлен** отображается значение **Неактивен**.

- **Последнее обращение**. Дата и время последнего обращения к серверу Агента, установленного на компьютере. Для компьютера со статусом Агента **Не установлен** отображается значение **Агент не установлен**;
- **Версия схемы**. Номер версии схемы безопасности, загруженной на Агент;
- **Версия Агента**. Номер версии Агента, установленного на компьютере;
- **Операционная система**. Версия операционной системы;
- **Комментарий**. Поле для ввода комментария;
- **IP-адрес**. IP-адрес рабочей станции;
- **Пользователь**. Имя пользователя, заходившего на рабочую станцию последним.

> **Примечание:**
>
> Пользователь не отображается для рабочих станций под управлением Linux.

Расширенная информация по свойствам компьютера выводится на панели **Подробно**. Чтобы просмотреть свойства отдельного компьютера, в рабочей области главного окна выберите строку с описанием нужного компьютера и нажмите .

На панели **Подробно** будет отображена таблица свойств, в которой содержатся дополнительные сведения по выбранному компьютеру:

- **Версия настроек**. Версия общих настроек политики безопасности (DM) (см. "Общие настройки политики безопасности");
- **Версия шаблонов**. Версия шаблонов уведомлений, которые могут быть показаны пользователю;
- **Версия настроек контроля сети**. Версия настроек контроля передачи данных по сетевым соединениям с помощью Network Monitor (см. "Контроль сетевых соединений");
- **Версия настроек контроля сетевых приложений**. Версия настроек контроля сетевого трафика, передаваемого по протоколам XMPP, MMP, FTP, FTPS, SMTP/S/MIME/ Outlook/POP3, HTTPS;
- **Версия настроек исключений**. Версия настроек исключения приложений из перехвата. В скобках указывается номер последней примененной версии.
- **Версия конфигурации ТМ**. Последняя версия конфигурации Traffic Monitor, доставленная на данную рабочую станцию;
- **Свободное место на дисках компьютера**. Размер свободного места на дисках, куда сохраняются теневые копии (в т.ч. в процентах).

> **Примечание:**
>
> Если Агент отправляет событие на сервер Device Monitor, Агент удаляет данные этого события с диска.

> **Важно!**
>
> В некоторых случаях не поддерживается удаление данных на Агентах. Файл с метаданными события может остаться на диске Агента, даже если Агент отправил событие.

Информация, выводимая по некоторым свойствам, дублируется в рабочей области главного окна.

Каждый зарегистрированный компьютер автоматически добавляется в группу компьютеров «по умолчанию». При этом компьютеру назначается политика безопасности (DM), определенная для группы компьютеров «по умолчанию».

9.4 Задача первичного распространения и обновления

> **Примечание:**
>
> Для установки агента на ОС Альт Рабочая станция 10 для пользователя, под учетной записью которого будет выполняться запуск задачи, необходимо:
>
> - вручную включить доступ на рабочую станцию по SSH, выполнив команду: `service sshd start`
> - раскомментировать в файле `/etc/openssh/sshd_config` строку `PermitRootLogin`
> - добавить пользователя в группу `/etc/sudoers`

Чтобы создать задачу первичного распространения агентов:

1. Слева в рабочей области нажмите .
2. Введите имя новой задачи и ее описание, если необходимо.
3. Задайте количество запусков задачи и их периодичность в минутах.
4. Укажите точку распространения Агентов, установленную ранее на сервере Device Monitor (подробнее см. "Установка Сервера Device Monitor", Шаг 20).
5. Укажите рабочую версию Агентов, дистрибутивы которых необходимо установить, и количество попыток загрузки пакета.
6. Нажмите **Сохранить**. Новая задача будет отображена в списке задач.

Чтобы сформировать список рабочих станций:

1. В области **Выполнение задачи** нажмите .
2. Добавьте компьютеры одним из способов:
   - на вкладке **Выбор из списка** выберите группы и/или компьютеры из доступной интеграции с Active Directory или ранее добавленных компьютеров Группы DM (подробнее см. "Добавление компьютера в группу").
     Для поиска компьютеров раскройте папки в дереве каталогов и начните вводить имя компьютера в строке поиска.
   - или на вкладке **Ручное добавление** внесите в поле ввода адреса компьютеров. Это могут быть IP-адреса или доменные имена, разделенных точкой с запятой или переносом строки.
3. Нажмите **Добавить**. В области **Выполнение задачи** будет отображен список компьютеров с указанием полного имени для установки Агентов. Если на указанных компьютерах не были ранее установлены Агенты или версии Агентов ниже версии, указанной в задаче, то после запуска задачи Агенты будут установлены или обновлены.

   Чтобы удалить ошибочно добавленные адреса, выделите их и нажмите .

Чтобы запустить задачу:

1. В задаче с добавленными адресами рабочих станций нажмите .
2. Введите в открывшемся окне учетные данные пользователя на удаленной рабочей станции, от имени которого запускается задача.

3. Нажмите **Запустить**.
4. Дождитесь окончания работы задачи.

Для каждой рабочей станции, на которую распространяется задача, в рабочей области главного окна отображаются следующие параметры:

Параметр	Описание
Имя	IP-адрес или доменное имя рабочей станции
Статус выполнения задачи	Текущее состояние задачи для данной станции. Возможные значения: • ***Не выполняется*** • ***Подготовка*** • ***В процессе*** • ***Ожидание перезагрузки*** • ***Ошибка*** • ***Нет доступа*** • ***Выполнена***
Версия агента	Версия Агента, установленного в настоящий момент на рабочей станции
Операционная система	Операционная система, установленная на рабочей станции
Разрядность операционной системы	Разрядность операционной системы на рабочей станции
Количество подключений	Количество сделанных попыток подключения к недоступной рабочей станции
Время последнего обращения	Дата и время последнего подключения к рабочей станции

Чтобы обновить Агентов на более новые версии:

1. Откройте на редактирование созданную задачу, нажав .
2. В поле **Версия** укажите новую версию Агента, директория с которой находится в точке распространения. При этом если в задаче указан компьютер с установленным Агентом более старой версии, то он будет обновлен после выполнения задачи.
3. Нажмите **Сохранить**.
4. Запустите задачу.

10 Настройка схемы безопасности

Настройка схемы безопасности включает в себя:

- Создание политик
- Создание правил

10.1 Создание политик

После установки в Device Monitor по умолчанию создана только одна политика – **Политика на устройства**.

Чтобы создать новую политику:

1. В левой части рабочей области нажмите .
2. В поле **Наименование** укажите название политики.
3. Нажмите **Сохранить**.

После создания политики добавьте в нее одно или несколько правил. Подробнее об особенностях применения правил смотрите в подразделе "Создание правил".

10.2 Создание правил

Чтобы добавить в политику новое правило:

1. Перейдите в раздел **Политики**.
2. На панели навигации выберите политику безопасности, в которую вы хотите добавить правило.
3. В области **Правила** нажмите .
4. В открывшемся окне укажите параметры правила. Доступные для создания правила:
   - Правило контроля съемных устройств;
   - Правило контроля сетевых ресурсов;
   - Правило контроля печати;
   - Правило контроля FTP;
   - Правило контроля HTTP(S);
   - Правило контроля почты;
   - Правило контроля ввода текста с клавиатуры;
   - Правило контроля облачных хранилищ.
5. После того как вы указали все необходимые параметры, нажмите **Создать**. Правило будет добавлено в политику.

10.2.1 Правило контроля съемных устройств

Правило позволяет отслеживать операции:

- копирования файлов с/на съемные устройства;
- создания новых файлов на съемных устройствах;
- изменения и переименование файлов на съёмных устройствах;
- копирования файлов на медиа-устройства, использующие для подключения протокол MTP;
- копирования файлов на съемных устройствах (например, из одной папки USB-устройства в другую).

К съемным устройствам относятся:

- устройства, подключенные через порты USB и IEEE 1394 (FireWire, i-Link);
- накопители на гибких магнитных дисках (Floppy-disk, ZIP);
- оптические диски (CD, DVD, BD) в режиме Live File System;
- медиа-устройства.

> **Важно!**
>
> На компьютерах под управлением Astra Linux или РЕД ОС не контролируются операции записи на CD/DVD-диски, в том числе подключенные через порты USB.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль съемных устройств**.
3. Задайте направление перехвата копирования: *Источник копирования* или *Приемник копирования*.
4. В **Действиях** при срабатывании правила выберите степень контроля обмена данными с сетевыми ресурсами:
   - *Разрешить копирование на съемные устройства;*
   - *Разрешить копирование со съемных устройств;*
   - *Исключить файлы при копировании на устройства;*
   - *Исключить файлы при копировании с устройств.* В случаях разрешения копирования файлов будут созданы теневые копии файлов. В этом случае вы можете указать **Размер файла**.
     В случаях исключения файлов из перехвата заполните поле **Маска файла**.
5. Задайте **Маску файлов**, чтобы исключить из перехвата подходящие под нее файлы. Например:
   - ? – один неизвестный символ;
   - * – любое количество символов.
6. Чтобы ограничить размер файлов, подлежащих контролю:,
   a. Отметьте **Размер файла**.
   b. Укажите диапазон значений для минимального и максимальный размера файла и единицы измерения. Если заполнены оба поля, то правило будет действовать только для файлов, размер которых находится внутри указанного диапазона.
7. После того, как вы определите все необходимые параметры, нажмите **Создать**.
   Правило будет действовать всегда и разрешать копирование с созданием события с теневыми копиями. Далее такие события отправляются на анализ в Traffic Monitor.

10.2.2 Правило контроля сетевых ресурсов

Правило контролирует действия с сетевыми ресурсами и позволяет:

- перехватывать копирование файлов на сетевые ресурсы с использованием UNC (например, *\\Server\SharedFolder\Folder\File*);
- перехватывать копирование файлов с сетевых ресурсов;
- запрещать копирование файлов на сетевые ресурсы.

Важно!

Копирование файла на сетевые ресурсы перехватывается только при передаче по протоколу SMBv1/CIFS.

Важно!

На компьютерах под управлением Astra Linux или РЕД ОС не контролируются операции:

- копирования/перемещения файлов на ресурсы, подключенные через терминальную сессию;
- копирование файла на сетевой ресурс, если подключение осуществлялось вводом имени сервера в строке поиска файлового менеджера ОС.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль FTP**.
3. В **Действиях** при срабатывании правила выберите степень контроля обмена данными с сетевыми ресурсами:
   - *Разрешить копирование на сетевые ресурсы;*
   - *Разрешить копирование с сетевых ресурсов;*
   - *Запретить копирование на сетевые ресурсы;*
   - *Исключить файлы при копировании с сетевых ресурсов;*
   - *Исключить файлы при копировании на сетевые ресурсы.*
4. Если требуется, укажите **Ресурсы**, задав их адреса. Чтобы посмотреть правила заполнения, наведите курсор на .
5. При необходимости вы можете ограничить набор контролируемых файлов, задав маску файла. Для этого отметьте поле **Маска файла** и укажите маску. Можно использовать символы: **?** для замены одного символа или ***** для замены набора символов. Например, `*.doc`. Знак пробела интерпретируется как часть имени файла.

   Важно!

   Для одного правила может быть только одна маска. Если необходимо ввести несколько масок, следует создать по одному правилу на каждую из масок.

   Примечание:

   На компьютерах под управлением Astra Linux или РЕД ОС маски файлов не учитываются.

6. Чтобы ограничить размер файлов, подлежащих контролю:
   a. Отметьте **Размер файла**.
   b. Укажите диапазон значений для минимального и максимальный размера файла и единицы измерения. Если заполнены оба поля, то правило будет действовать только для файлов, размер которых попадает в указанный диапазон.

> **Важно!**
>
> Отправка событий без теневой копии в Traffic Monitor не осуществляется.

7. После того, как вы определите все необходимые параметры, нажмите **Сохранить**. Правило будет действовать всегда.

10.2.3 Правило контроля печати

Правило позволяет осуществлять мониторинг операций, связанных с печатью документов на локальных и сетевых принтерах.

> **Примечание.**
>
> Если сервер печати и Агент Device Monitor установлены на ОС Astra Linux или РЕД ОС:
>
> - не определяется пользователь, отправивший файл на печать;
> - возможно изменение формата теневых копий перехваченных событий печати.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль печати**.
   Отправляемые в Traffic Monitor события будут содержать теневые копии печатаемых документов.

   > **Важно!**
   >
   > Агент на ОС Astra Linux или РЕД ОС при перехвате печати в некоторых случаях может создавать несколько событий. Такая ситуация может возникнуть, если задание печати было передано через несколько серверов печати и было на них перехвачено с большими временными интервалами.
   >
   > Если сервер печати и Агент Device Monitor установлены на ОС Astra Linux или РЕД ОС:
   >
   > - не определяется пользователь, отправивший файл на печать;
   > - возможно изменение формата теневых копий перехваченных событий печати. При этом:
   >   - одностраничный EXCEL-документ разбивается на фрагменты, и каждый фрагмент конвертируется в формат JPEG;
   >   - многостраничный документ формата PDF разбивается постранично, и каждая страница конвертируется в формат JPEG;
   >   - документ WORD конвертируется в набор JPEG-файлов, где каждая страница является отдельным JPEG-файлом.

3. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

10.2.4 Правило контроля FTP

Правило позволяет контролировать обмен данными по протоколу FTP/FTPS, в том числе:

- разрешать или запрещать передачу информации по протоколу FTP;
- перехватывать трафик по протоколу FTP с созданием теневых копий.

> **Важно!**
>
> На компьютерах под управлением РЕД ОС не перехватывается копирование файла на FTP-сервер, если подключение осуществлялось вводом имени сервера в строке поиска файлового менеджера ОС.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль FTP**.
3. В **Действиях** при срабатывании правила выберите степень контроля при обмене данными:
   - *Разрешить скачивание и запись на FTP* – при этом будет создано событие с теневой копией в случае записи на FTP;
   - *Исключать файлы при скачивании и записи на FTP* – введите адреса FTP-серверов для исключения копирования файлов из перехвата;
   - *Запретить запись на FTP*;
   - *Запретить вход на FTP-адреса.*
4. Заполните поле **FTP-адреса**. Наведите указатель мыши на **?** (знак вопроса), чтобы узнать правила его заполнения. Если адреса не заданы, то правило будет применено ко всем адресам.

   > **Примечание:**
   >
   > Следует иметь ввиду, что:
   >
   > - разрешающие правила на конкретные адреса имеют больший приоритет, чем запрещающие;
   > - разрешающие правила без указания адресов менее приоритетны, чем любые запрещающие;
   > - если в качестве адреса для запрета указать только адрес сервера, то будет запрещен доступ на все папки этого сервера;
   > - если в качестве адреса для запрета указать адрес сервера и подпапки, то будут разрешены переходы между папками на этом сервере, но доступ к копированию файлов будет запрещен только для указанной папки.

5. Если требуется, укажите ограничение на размер файла:
   a. Отметьте **Размера файла**.
   b. Обозначьте диапазон значений и единицы измерения.
   Этот параметр доступен только при создании событий с теневыми копиями отправляемых файлов и при создании события без теневых копий для случаев записи, если на компьютере осталось меньше свободного места, чем определено политикой.

6. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Подробнее о работе правила см. "Особенности и ограничения перехвата при копировании файлов с/на съемные устройства, сетевые ресурсы, FTP".

10.2.5 Правило контроля мессенджера VK

Правило позволяет контролировать обмен сообщениями чата и исходящие файлы в веб-версии системы мгновенного обмена сообщениями VK (ВКонтакте). При этом будет перехвачена история переписки с момента установки на компьютер Агента и заведения данного правила.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль мессенджера VK**.
3. Если вы хотите передавать в Traffic Monitor, помимо события, и теневые копии исходящих файлов, отметьте поле **Создавать теневую копию**. Если вы хотите определить дополнительные параметры теневых копий:
   a. Отметьте *Минимальный размер файла*, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
   b. Отметьте *Максимальный размер файла*, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.
   Эти поля учитываются только при создании теневой копии: если размер файла попадает в указанный диапазон, то событие будет содержать теневую копию; в противном случае событие будет сформировано без теневой копии.

   > **Примечание:**
   >
   > Чтобы установить настройки для формирования событий чата, перейдите в раздел **Настройки> Настройки перехвата мессенджеров**.

4. После того как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

10.2.6 Правило контроля HTTP(S)

Правило позволяет контролировать обмен данными по протоколам HTTP и HTTPS.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль HTTP(S)**.
3. В **Действиях** при срабатывании правила выберите:
   - *Контролировать зашифрованный канал;*
   - *Контролировать все каналы.*
4. Определите размеры запросов, для которых будет создана теневая копия. Для этого:

a. Отметьте **Минимальный**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для для запросов, размер которых больше либо равен указанному.
b. Отметьте **Максимальный**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только длязапросов, размер которых меньше либо равен указанному.

5. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Особенности применения правила на компьютерах под управлением ОС Astra Linux и РЕД ОС:

- не перехватываются соединения по протоколу IPv6;
- запросы, относящиеся к веб-почте, перехватываются как обычные HTTP-запросы.

10.2.7 Правило контроля почты

Правило контроля почты позволяет перехватывать получение электронной почты по POP3, IMAP и отправку почты по SMTP, HTTPS (включая сервисы вэб-почты: Gmail, Yandex, Mail.ru, Yahoo, Rambler, outlook.com), а также осуществлять запрет на отправку веб-почты по HTTPS.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль почты**.
3. В поле **Протокол** выберите канал, который должен контролироваться правилом:
   - *Все каналы*;
   - *SMTP* – только для исходящей почты;
   - *POP3* – только для входящей почты;
   - *IMAP* – только для входящей почты;
   - *HTTPS* – только для исходящей почты сервисов: Gmail, Yandex, Mail.ru, Yahoo, Rambler, outlook.com.
4. Выберите, какие действия с почтой должны быть доступны пользователю:
   - *Запретить использование почты;*
   - *Разрешить использование почты.*
5. Выберите, если требуется создавать события с теневой копией для:
   - *Входящих,* если в поле **Протокол** выбрано *POP3* или *IMAP;*
   - *Исходящих,* если в поле **Протокол** выбрано *SMTP* или *HTTPS;*
   - обоих значений, если в поле **Протокол** выбрано *Все каналы.*

   > **Важно!**
   >
   > Если в правиле установлено **Разрешить использование почты**, должно быть выбрано создание теневой копии хотя бы для одного из направлений почты: *Входящие* или *Исходящие*.

6. Укажите, если требуется создавать теневые копии для сообщений, передаваемых по всем каналам или только по зашифрованным.

   > **Примечание.**

Для протокола HTTPS значение **Все** недоступно.

Важно!

В теневой копии события веб-почты будут только те данные, которые были в перехваченном в трафике. Например, события будут содержать все атрибуты письма, кроме вложений, в случаях если:

- сотрудник отправляет письмо из черновиков после того, как событие было уже отправлено в Traffic Monitor по окончании таймаута с момента последней активности сотрудника с письмом;
- сотрудник отправляет письмо из черновиков, созданных на другой рабочей станции;
- сотрудник пересылает отправленное ранее письмо.

7. Если требуется, отметьте параметр **Макс. размер письма**, введите его значение и единицы измерения. В этом случае теневое копирование будет выполняться только для писем, размер которых меньше либо равен указанному.
8. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

10.2.8 Правило контроля ввода текста с клавиатуры

Правило позволяет перехватывать ввод текста с клавиатуры в окне любого приложения на рабочих станциях и формировать события при смене активного окна. Далее события, содержащие теневые копии введенных с клавиатуры данных, будут отправлены в Traffic Monitor для обработки и анализа.

Примечание:

Правило применяется на рабочих станциях под управлением РЕД ОС.

По умолчанию перехватывается ввод текста с клавиатуры на рабочих станциях:

- при смене активного окна;
- по истечении 20 секунд с момента окончания ввода;
- при накоплении 100 символов в одном слове или 200 в общей сложности, введенных с клавиатуры;
- при нажатии Enter / Ctrl+Enter / Shift+Enter.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль ввода текста с клавиатуры**.
3. Нажмите **Создать**. Правило будет действовать всегда.

Важно!

Для Агента на РЕД ОС смена вкладки в браузере игнорируется.

Пример: открыто приложение, с которого ведется перехват ввода текста с клавиатуры. Сотрудник переключается между вкладками и вводит в них текст. Такое поведение сгенерирует одно событие на ввод текста в приложении, а не на каждую вкладку.

Важно!

Перехват текста с клавиатуры корректно работает для русского и английского языков. При добавлении других языков требуется перезагрузка рабочей станции.

10.2.9 Правило контроля облачных хранилищ

Правило позволяет контролировать отправку и получение любых данных, доступ к веб-клиентам следующих облачных хранилищ:

- Dropbox;
- Evernote;
- Google Диск;
- OneDrive;
- SugarSync;
- Яндекс.Диск.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль облачных хранилищ**.
3. Выберите действие, которое будет применено. Для всех облачных хранилищ доступны следующие варианты:
   - **Запретить доступ**;
   - **Разрешить только скачивание**;
   - **Перехватывать загрузку файлов**.
4. Выберите одно или несколько файловых хранилищ для контроля.
5. При перехвате загрузки файлов будут создаваться теневые копии. В этом случае вы можете дополнительно указать:
   - **Минимальный размер файла для создания события**, установив значение и единицы измерения. Если поле заполнено, то правило будет создавать событие только для файлов, размер которых больше либо равен указанному;
   - **Максимальный размер теневой копии**, установив значение и единицы измерения. Если поле заполнено, то теневая копия будет создана только для файлов, размер которых меньше либо равен указанному.
6. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

11 Пользовательское лицензионное соглашение

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями пользовательского соглашения перед началом работы с программным обеспечением.
Использование устанавливаемого программного обеспечения означает Ваше безоговорочное согласие с условиями настоящего пользовательского соглашения. Если Вы не согласны с условиями настоящего пользовательского соглашения, Вы должны прервать установку и/или использование программного обеспечения.

1. Предоставление лицензии

1.1. Вам предоставляется неисключительная лицензия на использование программного обеспечения (далее — ПО) (Правообладатель прав на ПО — ООО «Лаборатория ИнфоВотч») в рамках функциональности, описанной в Документации к ПО (Руководство Пользователя, Руководство Администратора, Руководство по Установке), при условии соблюдения Вами всех технических требований, описанных в Документации к ПО, а также всех ограничений и условий использования ПО, указанных в настоящем Соглашении и Договоре, заключенном между Вами и Вашим лицензиаром.

1.2. 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.

1.3. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей и 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.

1.4. 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. Ограничения

2.1. Вы не вправе декомпилировать, дизассемблировать, модифицировать или выполнять производные работы, основанные на ПО, целиком или частично.

2.2. Вам запрещается передавать право на использование ПО третьим лицам.

2.3. Запрещается передавать и предоставлять доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения и Договора, заключенного между Вами и Вашим лицензиаром. Лицензионный ключ является конфиденциальной информацией. Правообладатель оставляет за собой право использовать средства для проверки подлинности установленного у Вас лицензионного ключа.

2.4. Запрещается сдавать ПО в аренду, прокат или во временное пользование, а также разглашать результаты стендовых испытаний ПО.

2.5. Запрещается использовать ПО в противоречащих законодательству целях.

2.6. Правообладатель имеет право заблокировать лицензионный ключ в случае нарушения Вами условий настоящего Соглашения и Договора, заключенного между Вами и Вашим лицензиаром.

2.7. За нарушение интеллектуальных прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством.

2.8. Вы не вправе использовать ПО для любых целей или способом, ограниченным или запрещенным применимым законодательством. Вы самостоятельно несете ответственность за неправомерное использование ПО.

2.9. В случае нарушения Вами какого-либо из условий данного Соглашения или Договора, заключенного между Вами и Вашим лицензиаром, Правообладатель или Ваш лицензиар вправе

прервать действие лицензии на использование ПО в любое время без уведомления Вас и без возмещения стоимости ПО или его части.

3. Ограниченная гарантия

3.1. Правообладатель гарантирует работу ПО в соответствии с описанием, изложенным в Документации к ПО. Однако все Ваши требования относительно работоспособности ПО Вы можете предъявлять только к своему лицензиару в рамках заключенного между вами лицензионного договора.

3.2. Вы соглашаетесь с тем, что никакое ПО не свободно от ошибок и Вам рекомендуется регулярно создавать резервные копии своих файлов.

4. Права на интеллектуальную собственность

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. 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.

4.3. Вы не можете удалять или изменять уведомления об авторских правах или другие проприетарные уведомления на любой копии ПО.

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, доступ к которой получен Вами в рамках осуществления настоящего Соглашения.

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

5.3. Указанная выше информация будет использоваться Вами только в целях осуществления предоставленных Вам по договору прав на ПО без права использования указанной информации в собственных интересах и за пределами Договора, заключенного между Вами и Вашим лицензиаром.

6. Вы проинформированы о том, что ПО содержит открытое программное обеспечение, распространяемое под определенными лицензиями, с которыми Вы можете ознакомиться в файле licenses.inf, распространяемом с ПО в составе дистрибутива. Каждый из предоставляемых дистрибутивов ПО содержит файл licenses.inf, соответствующий составу конкретного дистрибутива.

7. Уведомление о сборе информации об использовании ПО

7.1. Вы настоящим уведомляетесь о том, что при включении в ПО функции сбора статистики использования, в ПО осуществляется сбор и запись информации:

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) об активности пользователя – анонимизированные (без указания сведений о самом пользователе или информации введенной пользователем) данные о действиях конечного пользователя в пользовательском интерфейсе ПО.

7.2. Правообладатель вправе использовать указанные данные в целях анализа особенностей эксплуатации ПО и особенностей использования ПО конечным пользователем для принятия решений о развития функциональности и улучшения эксплуатационных характеристик ПО.

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

8. Контактная информация Правообладателя ООО «Лаборатория ИнфоВотч»

Тел./факс: +7(495)229-00-22

Коммерческий департамент: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru