

INFOWATCH

InfoWatch Device Monitor for Linux. Руководство пользователя

13/01/2025

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 6

2 Комплект документов 7

3 Техническая поддержка пользователей 8

4 Обзор 9

5 Настройки пользователей 10

5.1 Пользователи 10

5.1.1 Создание нового пользователя 10

5.1.2 Просмотр профиля пользователя 11

5.1.3 Редактирование учетной записи 12

5.1.4 Смена пароля пользователя 12

5.1.5 Активация и деактивация пользователя 13

5.1.6 Удаление пользователя 13

5.2 Роли 13

6 Общие настройки 14

6.1 Управление безопасностью 14

6.2 Мониторинг состояния Системы 15

6.3 Интеграции 17

6.3.1 Интеграция с Active Directory 17

6.3.2 Редактирование и удаление интеграции 20

7 Настройка Device Monitor 21

7.1 Серверы 21

7.2 Синхронизации 23

7.3 Агенты 26

7.4 Каналы перехвата 28

7.5 Исключение приложений из перехвата 29

7.6 Контроль сетевых приложений 31

7.7 Настройка отправки данных в продукты 32

7.8 Диагностика событий 32

8 Интерфейс Веб-консоли Device Monitor 34

8.1 Политики ... 35
8.2 Сотрудники ... 37
8.3 Компьютеры ... 37
8.4 Задачи ... 38
8.5 Справочники ... 38
9 Настройка Системы после установки ... 41
9.1 Создание и редактирование групп компьютеров ... 41
9.2 Настройка состава групп компьютеров ... 42
9.3 Просмотр сведений о компьютерах ... 44
9.4 Задача первичного распространения и обновления ... 47
10 Настройка схемы безопасности ... 50
10.1 Политики безопасности ... 50
10.1.1 Создание и изменение политик ... 50
10.2 Создание правил ... 51
10.2.1 Правило контроля съемных устройств ... 52
10.2.2 Правило контроля сетевых ресурсов ... 54
10.2.3 Правило контроля терминальной сессии ... 55
10.2.4 Правило контроля печати ... 57
10.2.5 Правило контроля внешних устройств ... 58
10.2.6 Правило контроля FTP ... 60
10.2.7 Правило контроля HTTP(S) ... 61
10.2.8 Правило контроля почты ... 61
10.2.9 Правило контроля облачных хранилищ ... 63
10.2.10 Правило контроля экрана ... 64
10.2.11 Правило контроля буфера обмена ... 65
10.2.12 Правило контроля мессенджера VK ... 66
10.2.13 Правило контроля мессенджера Telegram ... 67
10.2.14 Правило контроля протокола XMPP ... 69
10.2.15 Правило контроля ввода текста с клавиатуры ... 69
10.2.16 Правило контроля активности сотрудника ... 71
10.3 Создание и изменение списков приложений ... 72
10.3.1 Создание списка приложения ... 72
10.3.2 Добавление приложений в список ... 72
Добавление приложения в список вручную ... 72
Добавление в список из Протокола приложений ... 73
Копирование и перемещение приложений ... 74
10.3.3 Редактирование и удаление списка приложений ... 74
10.4 Создание и редактирование групп сотрудников ... 75

10.5 Настройка состава групп сотрудников 76

11 Пользовательское лицензионное соглашение 79

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 модуль системы InfoWatch Traffic Monitor, позволяющий контролировать обмен данными на рабочих станциях сотрудников. Собранные данные передаются для анализа в систему InfoWatch Traffic Monitor и продукты на Платформе.

Основные функции InfoWatch Device Monitor:

Название функции	Соответствующее правило политик безопасности
Контроль буфера обмена	Правило контроля буфера обмена
Контроль облачных хранилищ	Правило контроля облачных хранилищ
Контроль доступа к внешним устройствам	Правило контроля внешних устройств
Контроль файлов, копируемых с/на съемные устройства	Правило контроля съемных устройств
Контроль файлов, копируемых с/на сетевые ресурсы	Правило контроля сетевых ресурсов
Контроль трафика, передаваемого по протоколам FTP и FTPS	Правило контроля FTP
Контроль трафика, передаваемого по протоколам HTTP и HTTPS	Правило контроля HTTP(S)
Контроль систем мгновенного обмена сообщениями: VK (ВКонтакте), Telegram, протокол XMPP	Правило контроля мессенджера VK, Правило контроля мессенджера Telegram, Правило контроля протокола XMPP
Контроль ввода текста с клавиатуры	Правило контроля ввода текста с клавиатуры
Контроль систем передачи почтовых сообщений по протоколам SMTP, POP3, IMAP и HTTPS	Правило контроля почты
Мониторинг печати на контролируемых компьютерах	Правило контроля печати
Контроль экрана компьютера	Правило контроля экрана
Контроль активности сотрудника и сбор статистики	Правило контроля активности сотрудника

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.
2. **Офицер безопасности** – имеет полный доступ к данным Системы, кроме раздела **Настройки**.

В данной версии Системы не поддерживается создание новых ролей.

6 Общие настройки

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

- Управление безопасностью
- Мониторинг состояния
- Серверы
- 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 настройки доменной авторизации в веб-интерфейс сервера DM и получения информации для распространения агентов необходимо настроить синхронизацию с Active Directory.

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`

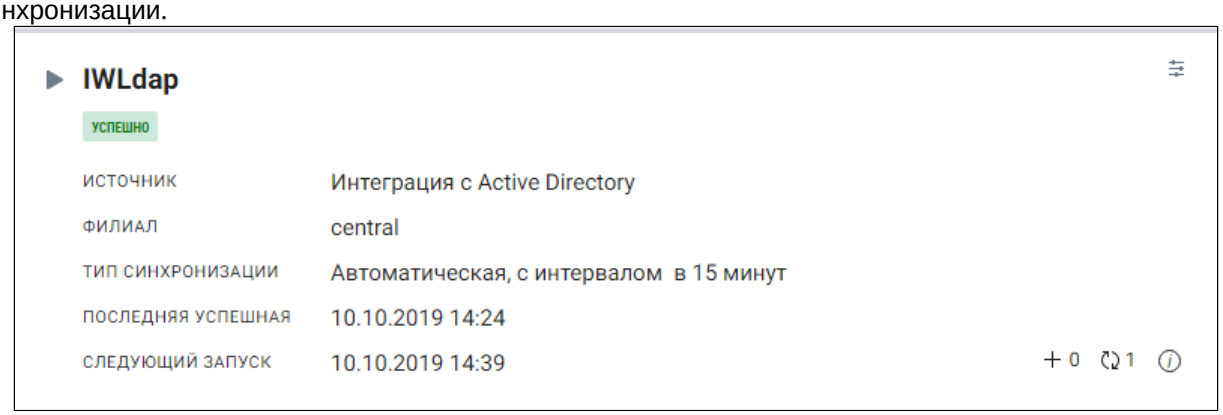
Логин	Логин для доступа к серверу Active Directory
Пароль	Пароль для доступа к серверу Active Directory
Синхронизация	*Ручная* или *Автоматическая*. Во втором варианте необходимо указать *Периодичность* и *Повторение*

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.

> **Примечание:**
>
> Синхронизация осуществляется с организационными подразделениями (Organizational units) и с группами безопасности (Security groups) Active Directory.

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:

- Серверы
- Синхронизации
- Агенты
- Каналы перехвата
- Исключение приложений из перехвата
- Контроль сетевых приложений
- Настройка отправки данных в продукты
- Диагностика событий

7.1 Серверы

Чтобы отправлять события на анализ в InfoWatch Traffic Monitor и/или продукты на Платформе, необходимо настроить:

- общие параметры для всех серверов Device Monitor;
- параметры хранения и удаления событий;
- параметры синхронизации политик Traffic Monitor;
- параметры соединения с сервером Traffic Monitor и/или сервером Платформы.

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").

     > **Примечание:**
     >
     > Все доступные версии расположены в директории `/opt/iw/iwdistribution/bin/SetupPackages/`.

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 настроить синхронизацию с Traffic Monitor для получения политик:

1. Перейдите в раздел **Настройки** > **Серверы**.
2. На вкладке **Синхронизация политик защиты данных на агенте** укажите:
   a. **Адрес сервера Traffic Monitor** – IP-адрес или имя сервера InfoWatch Traffic Monitor, с которого Device Monitor будет получать версию конфигурации. Полученная конфигурация распространяется на агенты Device Monitor.
   b. **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.
3. Нажмите **Применить**.

> **Примечание:**
>
> Конфигурация, полученная из Traffic Monitor, распространяется с серверов Device Monitor под управлением РЕД ОС, ОС Альт или ОС Astra Linux 1.7 на агенты Device Monitor под управлением РЕД ОС, ОС Альт, ОС Astra Linux 1.7 или ОС семейства Windows.

> **Примечание:**
>
> Версия конфигурации, используемой в Traffic Monitor, отображается в Консоли управления ТМ (подробнее см. "InfoWatch Traffic Monitor. Руководство пользователя", статья "Работа с конфигурацией Системы"). При необходимости вы можете сравнить номера версий в Traffic Monitor и Device Monitor и убедиться, что в Device Monitor используется актуальная версия.
>
> Чтобы увидеть актуальную версию конфигурации, используемой в Device Monitor, обновите страницу.

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

1. Перейдите в раздел **Настройки** > **Серверы**.
2. По умолчанию установлен только основной сервер Device Monitor. Выберите его в секции **Серверы Device Monitor**, 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;
4. На вкладке **Подключение к Traffic Monitor** укажите:
   - **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.
5. На вкладке **Подключение к Платформе** укажите:
   - **Адрес сервера Платформы** – IP-адрес или имя сервера Платформы, на который будут доставляться события. Возможные форматы записи: `host:port.` В качестве параметра `port` указывается порт сервера Платформы, через который будет осуществляться доставка событий. По умолчанию, порт сервера Платформы – 17104. Если не указать порт, будет использовано значение по умолчанию;
   - **Токен Платформы** – токен для подключения к API Платформы. Вы можете получить актуальный токен в консоли управления продукта на Платформе, в разделе **Основные настройки** в поле **Токен для Device Monitor Server**.
6. Если требуется установить соединение с другим сервером Traffic Monitor или Платформы, перейдите на нужную вкладку и измените адрес сервера и токен.
7. Нажмите **Применить**.

При соединении сервера Device Monitor с сервером Traffic Monitor или с сервером Платформы осуществляется проверка сертификата удаленного сервера. Для успешного соединения с удаленным сервером выполните настройку данной проверки. Подробнее см. "InfoWatch Device Monitor for Linux. Руководство по установке", статья "Настройка проверки сертификатов удаленных серверов".

7.2 Синхронизации

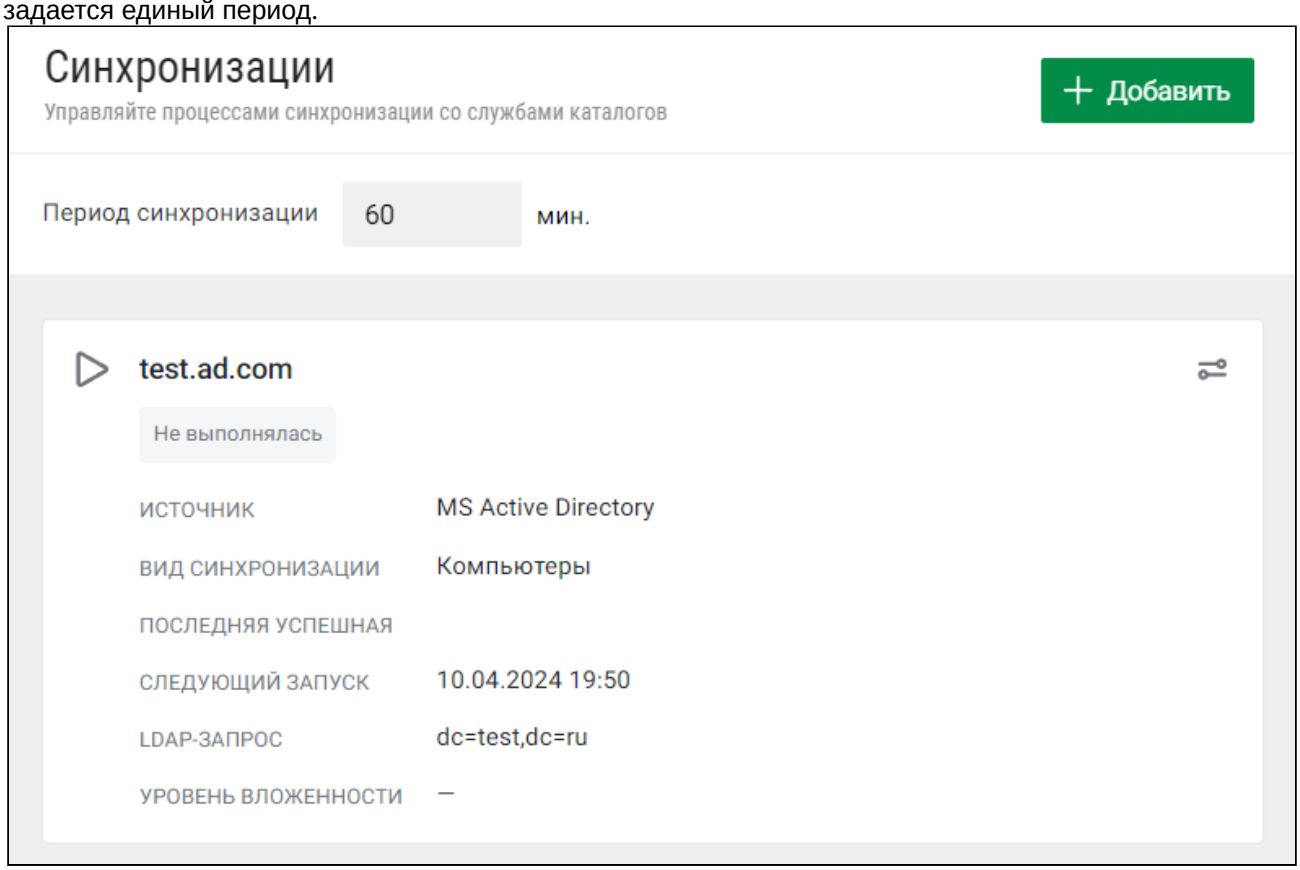
Чтобы получать информацию о компьютерах или сотрудниках из службы каталогов, в разделе **Настройки** > **Синхронизации** создайте и выполните синхронизацию с LDAP-сервером.

В центральной части рабочей области данного раздела отображаются все созданные синхронизации, их параметры и статусы.

Если вы выполните синхронизацию с компьютерами, то в разделе **Компьютеры** Веб-консоли Device Monitor в группе **Импортированные** появится новая подгруппа. Она будет содержать данные о компьютерах из службы каталогов, сохранив при этом иерархическую структуру источника. Аналогично вы можете выполнить синхронизацию с сотрудниками.

Далее синхронизация происходит автоматически с периодом, указанным в поле **Период синхронизации**.

Чтобы изменить период синхронизации, введите в поле требуемое значение и нажмите в любом месте рабочей области. Вы можете указать значение от 1 до 999 минут. Для всех синхронизаций задается единый период.



Чтобы создать новую синхронизацию:

1. Перейдите в раздел **Настройки** > **Синхронизации**.
2. В верхней правой части рабочей области нажмите **Добавить**.
3. В открывшемся окне укажите параметры для нового подключения:

Параметр	Описание
Адрес источника	Доменное имя или IP-адрес LDAP-сервера, с которым производится синхронизация
Тип источника	Тип службы каталогов. Имеет неизменяемое значение *MS Active Directory*
Порт	Порт для подключения к серверу синхронизации. Имеет неизменяемое значение *389*
LDAP-запрос	Атрибуты фильтрации, являющиеся полным путем к указанному каталогу. При этом может быть указан только один каталог в организационной структуре Active Directory.

	Примечание. Синхронизация осуществляется с организационными подразделениями (Organizational units) и с группами безопасности (Security groups) Active Directory. **Примечание.** Также вы можете синхронизировать объект типа Container, явно указав в запросе полный путь к нему, например: `cn=container_example,ou=ou_example,dc=company,dc=com` Если же объект типа Container находится внутри указанного в запросе каталога, то синхронизации данных с этим объектом не будет. **Примечание.** В атрибуте DC можно использовать следующие символы: • Цифры • Буквы (кириллица и латиница без учета регистра) • Символ "-" (не может быть в начале или конце значения атрибута) • Символ "_" В атрибутах OU и CN можно использовать следующие символы: • Цифры • Буквы (кириллица и латиница без учета регистра) • Символы * ( ) . & - _ [ ] ` ~ | @ $ % ^ ? : { } ! ' • Пробел, если он стоит не в начале или конце значения атрибута • Зарезервированные символы, экранированные с помощью обратного слеша "\" : • \ # + < > , ; " = • Пробелы в начале и в конце значения атрибута (например, " `OU=\ test` ") Длина значений атрибутов DC, OU, CN должна быть от 1 до 64 символов
Логин	Логин для доступа к серверу синхронизации
Пароль	Пароль учетной записи для доступа к серверу синхронизации
Вид синхронизации	Синхронизируемые объекты. Выберите значение *Компьютеры* или *Сотрудники*
Политика по умолчанию	Политика, которая будет назначена на синхронизируемые группы после первой синхронизации
Уровень вложенности	Уровень вложенности, до которого осуществляется синхронизация узлов дерева из службы каталогов. Группы данного уровня включают в себя все компьютеры или всех сотрудников входящих подгрупп. По умолчанию уровень вложенности не задан. В таком случае происходит синхронизация **всех** узлов дерева из службы каталогов.

4. Нажмите **Применить**.

Чтобы запустить синхронизацию:

1. На плитке синхронизации нажмите  **Запустить синхронизацию**.
2. Дождитесь окончания синхронизации. Статус синхронизации примет значение **Успешно**.

Чтобы редактировать синхронизацию:

1. На плитке синхронизации нажмите .
2. Из выпадающего списка выберите **Редактировать**.
3. Внесите требуемые изменения в синхронизацию.

> **Примечание:**
>
> Если изменить **Политику по умолчанию**, то новая политика будет применена только для новых групп, созданных в рамках синхронизации.

4. Нажмите **Сохранить**.

Чтобы удалить синхронизацию:

1. На плитке синхронизации нажмите .
2. Из выпадающего списка выберите **Удалить**.
3. В появившемся окне нажмите **Подтвердить**.

> **Важно!**
>
> При удалении синхронизации будут удалены все связанные с ней синхронизированные данные кроме:
>
> - компьютеров, на которых установлен Агент Device Monitor;
> - компьютеров и сотрудников, входящих не только в импортированные группы, но и в группы Device Monitor.
>
> Если компьютер, на котором установлен Агент Device Monitor, входит только в группы, импортированные из служб каталогов, то при удалении синхронизации он будет добавлен в группу компьютеров по умолчанию.

7.3 Агенты

Для эффективной работы агентских приложений Device Monitor необходимо задать ряд общих параметров.

Чтобы указать общие настройки работы агентов Device Monitor:

1. В главном меню выберите команду **Настройки** > **Агенты**.
2. Измените необходимые параметры:

Параметр	Описание
Соединение	

Отправлять на сервер уведомления о работе агента каждые	Периодичность, с которой агент отправляет на сервер уведомления о своей работе, в секундах. Значение по умолчанию – 600 сек.
Проверять работоспособность сервера каждые	Периодичность, с которой агент выполняет проверку доступности сервера, в секундах. Значение по умолчанию – 2400 сек.
Проверять изменения схемы безопасности каждые	Если агент работает в активном режиме (т.е. сам опрашивает Сервер об изменениях схемы безопасности), то проверка будет выполняться с указанной периодичностью, в секундах. Значение по умолчанию – 600 сек.
Контроль дискового пространства на Агентах	
Минимальное свободное дисковое пространство на агенте	Минимальный размер свободного пространства (в процентах) на контролируемом компьютере, при достижении которого, теневые копии не будут создаваться. Значение по умолчанию – 10%. Т.е. если при создании теневой копии свободного пространства на Агенте останется меньше чем указано, то копия создаваться не будет; частичной копии также не будет.
Если превышено максимальное количество событий на агенте	На том диске контролируемого компьютера, куда выполняется установка Агента Device Monitor, выделяется место, достаточное для хранения информации о 30000 событий. Если Агент Device Monitor настолько долго не имел связи с сервером Device Monitor, что накопилось более 30000 событий, контролируемых правилами, определенными для сотрудника/компьютера, то любые действия, контролируемые текущей политикой безопасности, могут быть запрещены. Чтобы запретить, выберите **Запрещать операции**. Чтобы все действия могли неконтролируемо выполняться, выберите **Разрешать операции**.
Скорость отправки данных с Агента	
Ограничивать скорость отправки данных	При узком канале связи, во избежание его чрезмерной загрузки, вы можете регулировать скорость отправки теневых копий на сервер. Для этого отметьте настройку и укажите верхнюю границу скорости, Кбит/с.
Логирование событий	

Логировать события от перехватчика устройств и облачных хранилищ	Степень детализации при сохранении сведений о работе с внешними устройствами и облачными хранилищами. Подробнее см. "Правило контроля внешних устройств" и "Правило контроля облачных хранилищ". Возможен один из следующих вариантов: • **Не логировать** – события не сохраняются; • **При отказе в доступе** (является значением по умолчанию) – события создаются только при попытках нарушения политик безопасности Device Monitor, то есть при блокировании использования устройства или облачного хранилища, включая блокирование попыток превышения уровня доступа. Использование внешних устройств и облачных хранилищ, не запрещенных политиками, не фиксируется. • **Логировать всегда** – события создаются всегда и содержат сведения обо всех действиях, в том числе о подключении/использовании устройств, занесенных в белые списки.

3. Чтобы внесенные изменения вступили в действие, нажмите **Применить**.

Примечание:

Для Агентов под управлением ОС Astra Linux 1.7, РЕД ОС и ОС Альт поддерживается отправка событий о подключении/использовании внешних устройств через USB. При этом:

- может не определяться имя учетной записи пользователя, которым было подключено устройство;
- может отсутствовать идентификатор устройства, если он не задан в этом устройстве производителем.

Для отправки таких событий необходимо для параметра **Логировать события от перехватчика устройств и облачных хранилищ** указать значение **Логировать всегда**.

7.4 Каналы перехвата

Чтобы настроить периодичность получения событий с теневыми копиями чата для правила "Контроль мессенджеров", укажите:

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

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

Чтобы настроить условия для правила "Контроль ввода текста с клавиатуры", укажите:

- через сколько секунд после остановки ввода с клавиатуры пользователем будет создано событие;
- минимальное количество символов, введенное пользователем и достаточное для создания события;
- реакцию на нажатие Enter / Ctrl+Enter / Shift+Enter.

Событие перехвата будет сформировано при соблюдении хотя бы одного условия, а также при смене пользователем активного окна.

После установки нужных значений и выбора условий нажмите **Применить**. Настройки будут действовать всегда.

Чтобы настроить параметры для снимков экрана, укажите:

- какого качества необходимо делать снимки (настройка применяется для "Правила автоматическое создание снимков экрана");
- на сколько изменять размер снимка (в %, значение по умолчанию – 80%);
- период от 120 до 1200 секунд, по истечении которого не требуется создавать снимок экрана (значение по умолчанию – 120 секунд);
- если нужно создавать снимок только активного окна.

Примечание:

Если при выбранной настройке **Создавать снимок экрана только активного окна** и при активном окне какого-либо приложения пользователь совершает действия не в данном приложении (например, открывает контекстное меню в системном трее на рабочей станции), то на снимке экрана может отображаться часть активного окна приложения.

7.5 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. Исключение приложений в ОС семейств MS Windows и Linux настраиваются на разных вкладках.
    a. **Для поддерживаемых ОС семейства Linux**
        i. Откройте вкладку Linux.
        ii. В открывшемся окне введите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.
        iii. 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.
        iv. 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.

v. Укажите ОС, для которой настраивается исключение. Чтобы исключение работало на всех поддерживаемых ОС семейства Linux, выберите вариант **Любой дистрибутив Linux**.

b. **Для поддерживаемых ОС семейства Windows**

i. Откройте вкладку Windows.

ii. На панели инструментов нажмите ⊞.

iii. В открывшемся окне введите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.

iv. В поле **Описание** введите произвольное описание приложения. Вместо имени приложения можно ввести символ *. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути или имеющие указанную цифровую подпись (см. п. vi).

v. В поле **Тип перехвата** отметьте:

1. **Исключить из сетевого перехвата** – если требуется исключить сетевую активность приложения из перехвата.
2. **Исключить приложение из внедрения модулей** – если требуется не создавать события и теневые копии при печати из данного приложения.

> **Примечание**
>
> Должен быть выбран хотя бы один из типов перехвата.
> Программы со встроенной проверкой целостности (например, клиент SWIFT) или содержащие внутри себя антиотладочные методы необходимо добавлять в исключение приложений из внедрения модулей. В противном случае их запуск будет невозможен.

vi. В поле **Расположение файла** укажите 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: `%ProgramFiles%\Citrix`, то из перехвата будут исключены все приложения в формате *.exe в папке Citrix, а также любой ее подпапке.

vii. В поле **Исходное имя файла** укажите название приложения (в контекстном меню исполняемого файла приложения выберите **Свойства**, вкладка **Подробно**, атрибут **Исходное имя файла**).

viii. В поле **Имя оставившего цифровую подпись** укажите значение из свойств исполняемого файла (в контекстном меню файла выберите **Свойства**, вкладка **Цифровые подписи**, атрибут **Имя подписавшего**). Можно указать имя целиком или часть имени. Например, если исключение задано в виде: `*Kaspersky`, то из перехвата будут исключены все приложения, в цифровой подписи которых есть подстрока "Kaspersky".

4. Нажмите **Создать**. Чтобы применить исключение приложения из перехвата или отмену такого исключения, перезапустите приложение.

7.6 Контроль сетевых приложений

Для контроля сетевого трафика на Агенте Device Monitor реализован прозрачный прокси-сервер. На этот сервер перенаправляются все соединения, вне зависимости от используемого протокола. Далее Агент Device Monitor разбирает протокол и определяет, относится ли данный протокол к перехватываемым.

Перехватываются протоколы: FTP, FTPS, POP3, SMTP, S/MIME, HTTP, HTTPS, XMPP и MMP. Если поток данных защищен с использованием протокола TLS\SSL, то прокси-сервер раскрывает трафик и определяет, нужно ли контролировать данный поток.

Вы можете задать список адресов серверов, при соединении с которыми протоколы не контролируются (трафик на эти серверы не перенаправляется на внутренний прокси-сервер) либо принудительно контролируются (трафик перенаправляется на внутренний прокси-сервер).

При добавлении адреса сервера в исключения, требуется указать IP-адрес сервера или FQDN.

Чтобы задать список разрешенных или запрещенных серверов:

1. Перейдите в раздел **Настройки** > **Контроль сетевых приложений**.
2. Нажмите [+].
3. В диалоговом окне **Добавить сервер в список исключенных из анализа** введите описание сервера:
   - чтобы добавить отдельный порт сервера:
     a. Выберите нужное действие: **Исключить из перехвата** или **Включить в перехват**;
     b. В поле **Тип адреса** выберите **Адрес и порт**;
     c. Укажите FQDN или IP-адрес (IPv4 или IPv6) сервера;
     d. В поле **Порт** укажите порт подключения;
   - чтобы добавить диапазон адресов:
     a. Выберите нужное действие: **Исключить из перехвата** или **Включить в перехват**.
     b. В поле **Тип адреса** выберите **Диапазон адресов**;
     c. Укажите IP-адреса (IPv4 или IPv6) в полях "с" - "по".
   - чтобы добавить шаблон для исключения группы ресурсов из перехвата при SSL/TLS-соединении:
     a. Выберите действие **Исключить из перехвата**;
     b. В поле **Тип адреса** выберите **Домен из MITM перехватчика**;
     c. Укажите домен.
4. Нажмите **Добавить**, затем **Применить**.

В текстовом виде адрес IPv4 записывается как nnn.nnn.nnn.nnn, где nnn принимает значения от 0 до 255, а каждая буква n представляет десятичную цифру. Незначащие нули можно не указывать.
В текстовом виде адрес IPv6 записывается как xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, где каждая буква x – это шестнадцатеричная цифра, представляющая 4 бита. Незначащие нули можно не указывать**.**

Примечание:

Включение в перехват имеет более высокий приоритет, чем исключение.

Настройка с указанием конкретного адреса имеет более высокий приоритет, чем диапазон адресов.

Чтобы изменить параметры сервера, выберите его в списке и нажмите . После внесения изменений нажмите **Сохранить**, затем **Применить**.

Чтобы удалить сервер из списка разрешенных, выберите его, нажмите . Подтвердите удаление, затем нажмите **Применить**.

7.7 Настройка отправки данных в продукты

Вы можете указать, в какие продукты InfoWatch необходимо отправлять данные.

Для этого:

1. В главном меню Консоли управления выберите **Настройки** > **Настройка отправки данных в продукты**.

2. В области **Настройка отправки в Traffic Monitor** снимите флаг, если вы не хотите:
   - **Отправлять события с текстом по правилу контроля ввода текста с клавиатуры** (настройка контроля событий производится в Правиле контроля ввода текста с клавиатуры);
   - **Отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры** (активна, если включена настройка "Отправлять события с текстом по правилу контроля ввода текста с клавиатуры"). Настройка контроля событий производится в Правиле контроля ввода текста с клавиатуры).
3. В области **Настройка отправки в Платформу** снимите флаг, если вы не хотите:
   - **Отправлять события с текстом по правилу контроля ввода текста с клавиатуры** (настройка контроля событий производится в Правиле контроля ввода текста с клавиатуры);
   - **Отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры** (активна, если включена настройка "Отправлять события с текстом по правилу контроля ввода текста с клавиатуры"). Настройка контроля событий производится в Правиле контроля ввода текста с клавиатуры.

По умолчанию включена отправка событий в Traffic Monitor и Платформу.

> **Важно!**
>
> Для того, чтобы события отправлялись в Платформу и снимки экрана отображались в InfoWatch Activity Monitor, настройте правило сбора статистики (Правило контроля активности сотрудника).

7.8 Диагностика событий

В данном разделе вы можете выгрузить отчет с событиями Агентов согласно заданным фильтрам. Для этого:

1. Перейдите в **Настройки** > **Диагностика событий**.
2. В фильтре *Дата событий* выберите период, за который необходимо выгрузить отчет. Если выбран период длиной в один день, вы также можете выбрать отрезок времени, за который необходимо сформировать отчет. По умолчанию в отчет включаются события с 00:00 до 23:59.
3. Нажмите **Выгрузить отчет**.

В папке Загрузки вашего компьютера будет выгружен отчет в формате CSV, содержащий поля:

- *Дата и время события*;
- *Компьютер*;
- *Сотрудник* (поле может быть пустым);
- *Приложение* (поле может быть пустым);
- *Правило* – название правила, в соответствии с которым создано событие (поле может быть пустым);
- *Операция* – действие, заданное в правиле;
- *Тип операции* – выполненная операция;
- *Статус события* с возможными значениями:
    - не определено,
    - ожидает обработки,
    - обработано,
    - ожидает отправки,
    - отправлено,
    - нет лицензии,
    - ожидает отправки в Traffic Monitor,
    - отправлено в Traffic Monitor;
- *Версия схемы безопасности*;
- *Вердикт операции* (поле может быть пустым);
- *Идентификатор события*.

Для событий с использованием устройств отчет также имеет дополнительные поля:

- *Тип устройства*;
- *Идентификатор экземпляра или модели устройства*;
- *Описание устройства*.

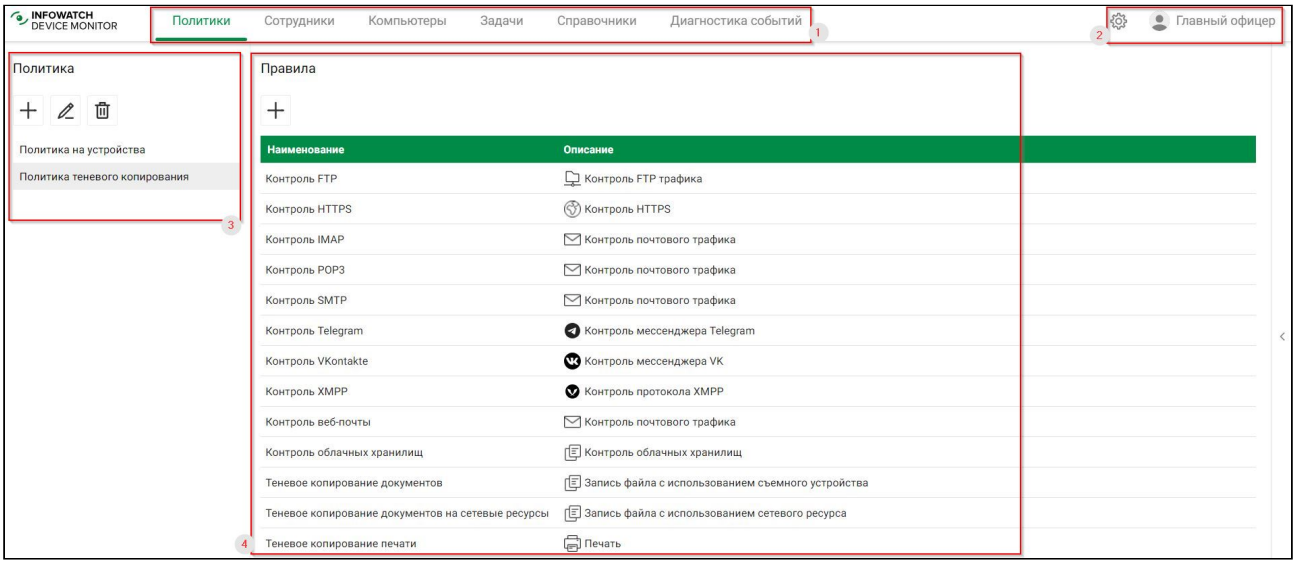
Данные в отчете отсортированы по дате и времени событий по убыванию.

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 и сотрудников;
- 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 • **Сотрудники** – управление учетными записями сотрудников и группами сотрудников • **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

Номер на схеме	Элемент окна	Назначение элемента
2	Меню пользователя	• **Справочники** – управление списками приложений для использования в правилах и просмотр протокола приложений
		Пользовательское меню, в котором вы можете: • 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 внешних устройств**. Правило позволяет разрешать, ограничивать доступ и запрещать использование съемных устройств хранения.
- **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 мессенджера Telegram**. Позволяет контролировать доступ сотрудников к сервису мгновенного обмена сообщениями Telegram: обмен новыми, пересылаемыми или исправленными сообщениями чата, в том числе группового, исходящими файлами и голосовыми сообщениями.
- **Контроль XMPP**. Позволяет контролировать обмен по протоколу **XMPP** входящими и исходящими текстовыми сообщениями, а также исходящими файлами.
- **Правило контроля экрана**. Позволяет создавать снимки экрана компьютера.
- **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.
- **Правило контроля активности сотрудника**. Позволяет собирать статистику активности сотрудника за контролируемым компьютером.
- **Правило контроля буфера обмена**. Позволяет контролировать вставку данных с использованием буфера обмена через приложение терминальной сессии.

8.2 Сотрудники

Регистрация контролируемых пользователей (сотрудников) в Системе осуществляется в соответствии со следующими принципами:

- Каждый сотрудник должен входить как минимум в одну группу сотрудников (группу «по умолчанию»). Это связано с тем, что политика безопасности не может быть назначена отдельному сотруднику.
  В группу «по умолчанию» входят учетные записи всех сотрудников, для которых не определены другие группы сотрудников: сотрудники, впервые зарегистрированные в Device Monitor, сотрудники, исключенные из всех прочих групп сотрудников.
  Исключить сотрудника из группы «по умолчанию» можно при условии, что учетная запись сотрудника добавлена хотя бы в одну группу сотрудников, помимо группы «по умолчанию».
- После установки Системы группе сотрудников «по умолчанию» назначена **Политика теневого копирования**, содержащая следующие правила:
  - Контроль FTP
  - Контроль HTTPS
  - Контроль IMAP
  - Контроль POP3
  - Контроль SMTP
  - Контроль Telegram
  - Контроль VKontakte
  - Контроль XMPP
  - Контроль веб-почты
  - Контроль облачных хранилищ
  - Теневое копирование документов
  - Теневое копирование документов на сетевые ресурсы
  - Теневое копирование печати

Подробную информацию о правилах см. в разделе "Политики".

О работе с разделом Сотрудники см. "Создание и редактирование групп сотрудников".

8.3 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 групп компьютеров
- Настройка состава групп компьютеров
- Просмотр сведений о компьютерах

8.4 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".

8.5 Справочники

Раздел **Справочники** содержит подразделы:

- **Приложения**
- **Протокол приложений**.

Подраздел **Приложения** содержит списки приложений, которые можно использовать в правилах для более точного контроля.

Вы можете использовать списки приложений в:

- Правиле контроля ввода текста с клавиатуры (подробнее см. "Правило контроля ввода текста с клавиатуры");
- Правиле контроля буфер обмена (подробнее см. "Правило контроля буфера обмена").

Подраздел **Протокол приложений** содержит таблицу с информацией о приложениях, которые запускались на контролируемых рабочих станциях под управлением ОС MS Windows.
После установки Агента InfoWatch Device Monitor на рабочие станции под управлением ОС MS Windows и их перезагрузки Система автоматически начинает получать информацию о запускаемых приложениях. Информация обо всех запусках и установках формирует *протокол приложений*.

Из протокола вы можете добавлять приложения в списки для ОС MS Windows. О создании списков и добавлении в них приложений см. "Создание и изменение списков приложений".

Примечание:

Для снижения нагрузки на CPU таблица базы данных, содержащая записи о запусках приложений, добавлена в очередь регулярной очистки. Подробнее см. в статье базы знаний "Удаление записей журнала приложений Device Monitor".

Важно!

Протокол приложений необходим для того, чтобы Офицер безопасности не мог запретить приложение, без которого компьютер перестанет функционировать в штатном режиме.

В протоколе приложений вы можете отфильтровать данные по следующим атрибутам:

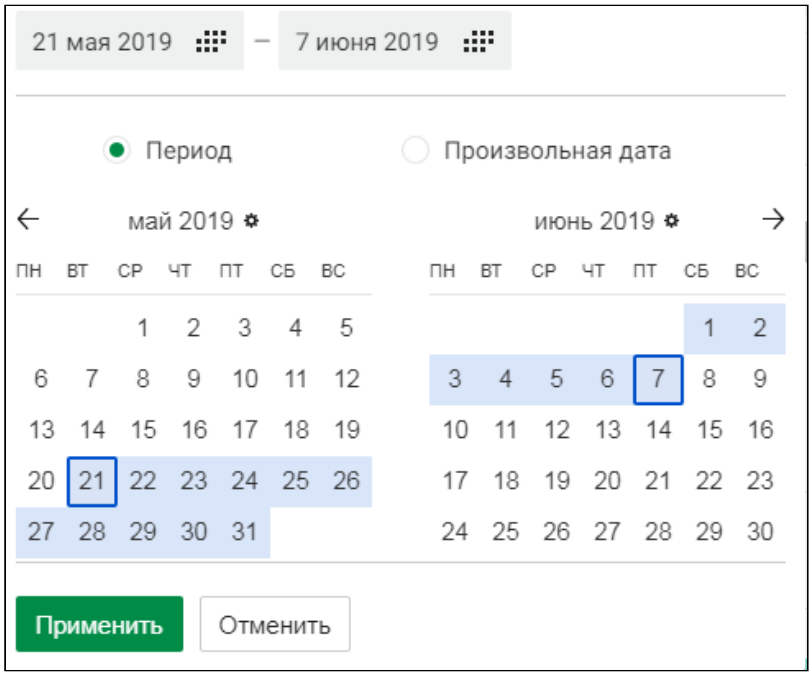
- Дата
- Компьютер
- Пользователь
- Имя приложения
- Описание
- Название продукта
- Издатель
- Расположение исполняемого файла

Для атрибута **Дата** вы можете выбрать период времени, за который необходимо получить данные:

- Сегодня;
- Последние 3 дня;
- Последние 7 дней;
- Последние 30 дней;
- Текущий месяц;
- Прошлый месяц;
- Произвольный период (укажите даты начала и конца периода, либо список произвольных дат):

Чтобы указать определенный период времени

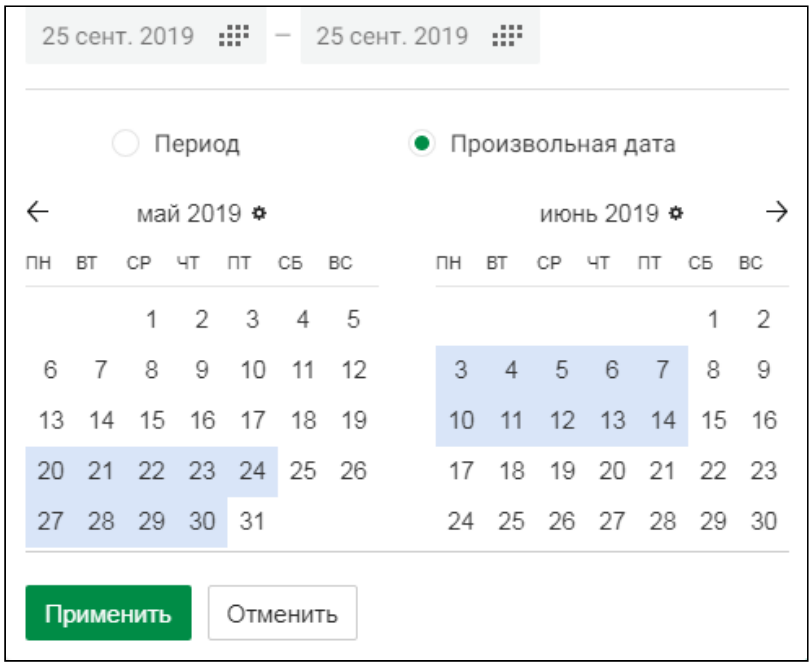
1. Используя указатель мыши, отметьте в календаре начальную и конечную дату. Выбранный период будет подсвечен:



2. Нажмите **Применить**.

Чтобы указать одну или несколько произвольных дат

1. Используя указатель мыши, отметьте в календаре одну или несколько дат. Выбранные даты будут подсвечены:



2. Нажмите **Применить**.

Для остальных атрибутов – начните вводить необходимое значение в поле **Поиск** нужного атрибута, затем выберите его, нажав .

Чтобы сбросить значение фильтров, нажмите **Очистить фильтры**.

9 Настройка Системы после установки

В этом разделе:

- Создание и редактирование групп компьютеров
- Настройка состава групп компьютеров
- Просмотр сведений о компьютерах
- Задача первичного распространения и обновления

9.1 Создание и редактирование групп компьютеров

Важно!

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

Примечание:

Чтобы получать информацию о компьютерах из службы каталогов, вы можете выполнить синхронизацию с LDAP-сервером. Подробнее см. "Синхронизации".

Чтобы добавить группу компьютеров:

1. Перейдите в раздел **Компьютеры**.
2. В левой части рабочей области нажмите .
3. Укажите следующие параметры:
   - **Наименование** группы;
   - **Политика**. Выберите из раскрывающегося списка политику, которая будет назначена данной группе компьютеров.
4. Нажмите . 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 .

Чтобы удалить группу компьютеров:

1. Выделите группу для удаления.

Примечание.

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**.

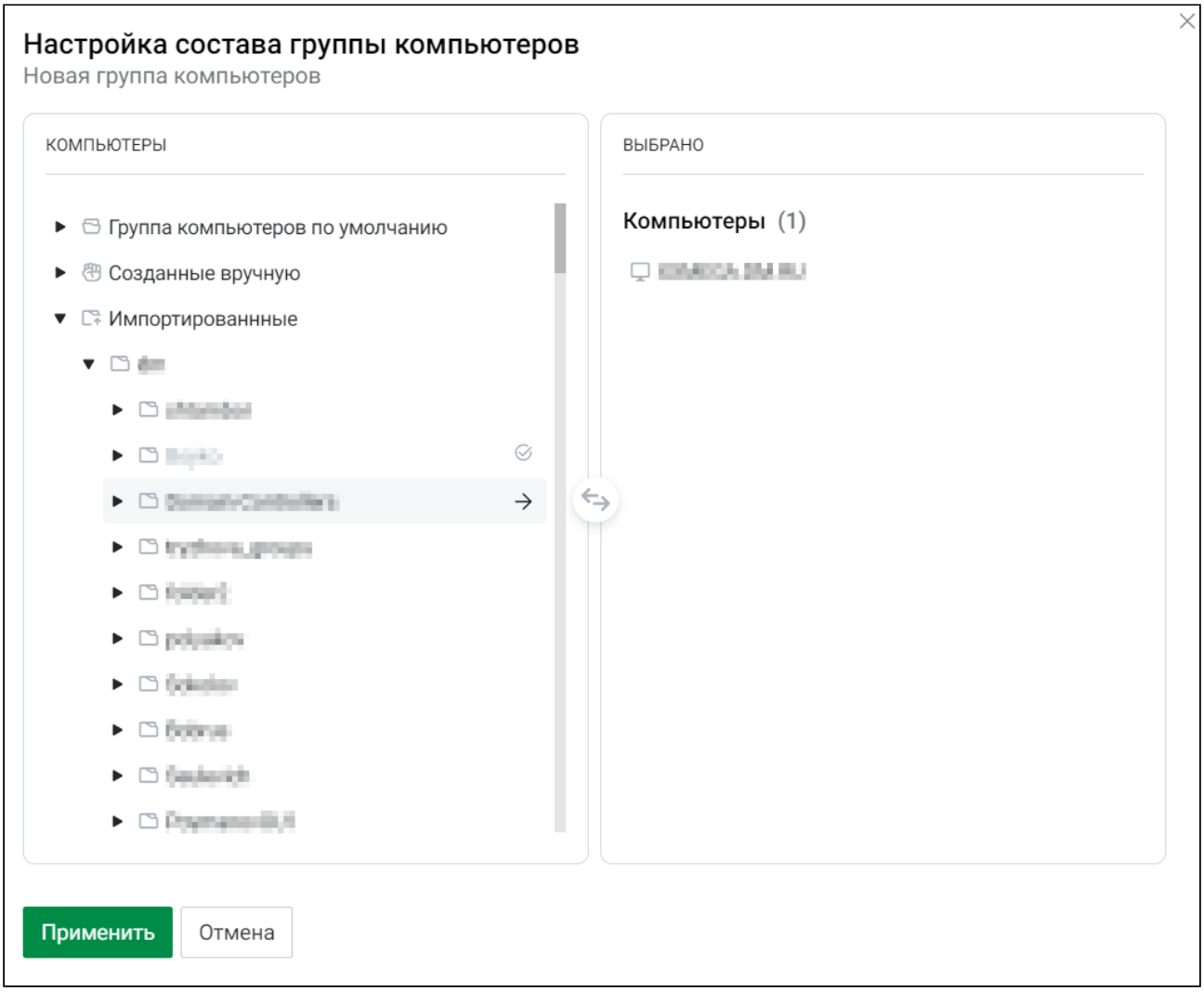
9.2 Настройка состава групп компьютеров

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 назначенная ей политика. В дальнейшем определение политик для компьютера происходит путем его включения в различные группы компьютеров.

Чтобы настроить состав группы компьютеров:

1. Перейдите в раздел **Компьютеры**.
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 

.
В открывшемся диалоговом окне в области слева отобразится список компьютеров из числа ранее зарегистрированных в Системе, т.е. компьютеры, на которых установлен Агент из группы «по умолчанию» и других групп.
4. Чтобы развернуть или свернуть группу, используйте .
5. В области слева наведите курсор на необходимый компьютер или группу и нажмите  **Добавить компьютеры в "<Название группы компьютеров>"**. Компьютер будет включен в выбранную группу. В области слева напротив группы или компьютера, которые были добавлены, появится значок .
6. Чтобы удалить из группы компьютер или группу, наведите курсор на удаляемую запись и нажмите  **Удалить из группы "<Название группы компьютеров>"**.
7. Нажмите **Применить**.

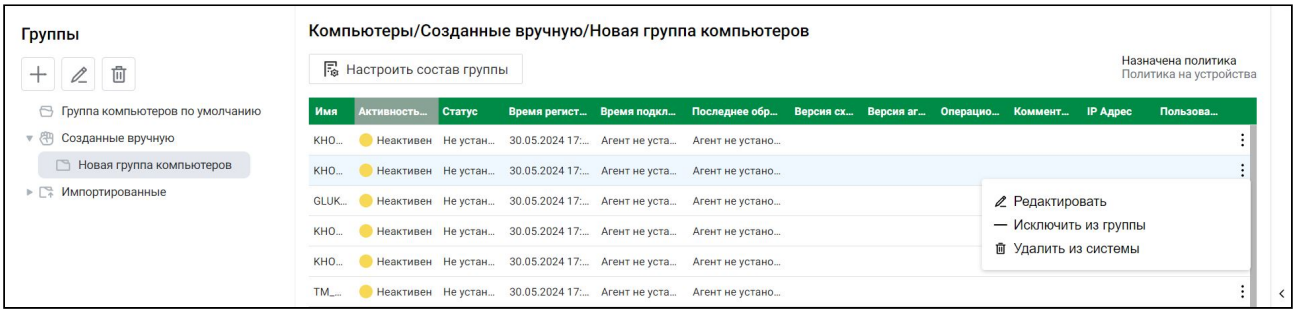


Примечание:

Если вы добавляете группу компьютеров, которая содержит подгруппы, то компьютеры из подгрупп не будут автоматически добавлены в выбранную группу. Вы можете добавить их отдельно.

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.

Внутри группы компьютеров вы можете работать с их списком: редактировать, исключать, удалять компьютеры из системы.



Примечание:

Для импортированных групп компьютеров внутри группы доступно только редактирование.

Чтобы исключить компьютер из группы компьютеров:

1. В строке с именем компьютера нажмите ⋮.
2. Выберите — **Исключить из группы**.
3. Нажмите **Да**. Если компьютер входил только в одну группу, то при исключении он будет автоматически добавлен в группу компьютеров «по умолчанию».

Чтобы добавить комментарий компьютеру:

1. В строке с именем компьютера нажмите ⋮.
2. Выберите ✎ **Редактировать**.
3. В поле **Комментарий** добавьте комментарий и нажмите **Сохранить**.

При необходимости вы можете удалить компьютер из списка зарегистрированных (например, если эксплуатация рабочей станции прекращена).

Чтобы удалить компьютер из схемы безопасности:

1. В строке с именем компьютера нажмите ⋮.
2. Выберите 🗑 **Удалить из системы**.
3. В открывшемся диалоговом окне нажмите **Подтвердить**.

Важно!

Удаление компьютера из схемы безопасности повлечет за собой его удаление из всех групп и политик.

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. "Настройка Device Monitor");
- **Версия настроек 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.

  > **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

Соблюдайте последовательность действий:

1. Создайте задачу первичного распространения.
2. Сформируйте список рабочих станций для установки Агентов.
3. Запустите задачу.
4. При наличии ошибок ознакомьтесь со сведениями о них или выгрузите лог.

Примечание:

Для установки агента на ОС Альт Рабочая станция 10 для пользователя, под учетной записью которого будет выполняться запуск задачи, необходимо:

1. Вручную включить доступ на рабочую станцию по SSH, выполнив команду: `service sshd start`.
2. В файле `/etc/openssh/sshd_config` раскомментировать строку `PermitRootLogin`.
3. Добавить пользователя в группу `/etc/sudoers`.

Чтобы создать задачу первичного распространения Агентов:

1. В левой части рабочей области нажмите ⊞.
2. Введите имя новой задачи.
3. Снимите флаг **Устанавливать компонент перехвата сетевого трафика**, если не хотите, чтобы этот компонент был установлен.
4. Если необходимо, добавьте описание задачи.
5. Задайте количество запусков задачи и их периодичность в минутах.
6. Укажите точку распространения Агентов, установленную ранее на сервере Device Monitor (подробнее см. "Установка Сервера Device Monitor", Шаг 20).
7. При необходимости измените версию Агентов, дистрибутивы которых необходимо установить. По умолчанию отображается версия, указанная в общих настройках (см. "Серверы").

Примечание:

Все доступные версии расположены в директории `/opt/iw/iwdistribution/bin/SetupPackages/`.

8. Укажите количество попыток загрузки пакета.
9. Нажмите . Новая задача будет отображена в списке задач.

Чтобы обновить версию Агентов на более новую:

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

Важно!

Для корректной блокировки съемных устройств после обновления Агента на ОС семейства Linux обязательно перезагрузите рабочую станцию.

Чтобы сформировать список рабочих станций:

1. В области **Выполнение задачи** нажмите .
2. Добавьте компьютеры одним из способов:
   - на вкладке **Выбрать из списка** выберите группы и/или компьютеры из доступной интеграции с Active Directory или ранее добавленных компьютеров Группы DM (подробнее см. "Настройка состава групп компьютеров").
     Для поиска компьютеров раскройте папки в дереве каталогов и начните вводить имя компьютера в строке поиска.
   - на вкладке **Добавить вручную** введите в поле ввода адреса компьютеров. Это могут быть IP-адреса или доменные имена, разделенные 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.
4. Чтобы удалить ошибочно добавленные адреса, выделите их и нажмите .

Чтобы запустить задачу:

1. Выберите задачу с добавленными адресами рабочих станций.
2. Нажмите .
3. В открывшемся окне введите учетные данные пользователя удаленной рабочей станции, от имени которого запускается задача.
4. Нажмите **Запустить**.
5. 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 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

Если в результате выполнения задачи был выставлен статус ***Ошибка***, вы можете перейти в журнал ошибок и ознакомиться с расширенными сведениями.

Чтобы просмотреть сведения об ошибках при установке Агентов и выгрузить логи:

1. Выберите строку в таблице со статусом задачи ***Ошибка***.
2. Нажмите . Будут отображены общие сведения и описания ошибок.
3. Нажмите , чтобы выгрузить логи в формате TXT.

Чтобы вернуться к списку рабочих станций, нажмите .

10 Настройка схемы безопасности

Настройка схемы безопасности включает в себя:

- Политики безопасности
- Создание и изменение списков приложений
- Создание правил
- Создание и редактирование групп сотрудников
- Настройка состава групп сотрудников

10.1 Политики безопасности

На агентах Device Monitor политики применяются в следующем порядке:

1. Запрещающие политики.
2. Политики защиты данных на агентах, созданные в ТМ.
3. Политика теневого копирования.

Каждая политика безопасности состоит из набора правил, при помощи которых осуществляется мониторинг операций, связанных с переносом файлов на съемные устройства и сетевые ресурсы, отправкой документов на печать и сетевой активностью; определяется уровень доступа к контролируемым периферийным устройствам.

Политики безопасности назначаются **группам сотрудников** и **группам компьютеров**. Политика безопасности, назначенная группе сотрудников, действует на всех сотрудников, включенных в эту группу. Политика безопасности, назначенная группе компьютеров, действует на всех сотрудников, работающих на контролируемых компьютерах, включенных в эту группу.

Работа с политиками безопасности ведется в разделе **Политики**. Чтобы перейти к этому разделу, воспользуйтесь кнопкой **Политики**, расположенной на Панели навигации.

Информация по работе с политиками безопасности содержится в подразделах:

- Создание и изменение политик

10.1.1 Создание и изменение политик

После установки в Device Monitor по умолчанию созданы две политики – **Политика теневого копирования** и **Политика на устройства**. **Политика на устройства** по умолчанию не содержит правил, **Политика теневого копирования** содержит следующие правила:

- Контроль FTP
- Контроль HTTPS
- Контроль IMAP
- Контроль POP3
- Контроль SMTP
- Контроль Telegram
- Контроль VKontakte
- Контроль XMPP
- Контроль веб-почты
- Контроль облачных хранилищ
- Теневое копирование документов
- Теневое копирование документов на сетевые ресурсы
- Теневое копирование печати

Чтобы создать новую политику:

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

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

Чтобы отредактировать политику:

1. В левой части рабочей области выберите политику.
2. Нажмите .
3. В поле **Наименование** укажите новое название политики.
4. Нажмите .

Чтобы удалить политику:

1. В левой части рабочей области выберите политику.
2. Нажмите .
3. Подтвердите действие.

Примечание:

Если политика безопасности назначена хотя бы одной группе сотрудников или группе компьютеров, ее невозможно удалить из схемы безопасности.

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 буфера обмена;
   - Правило контроля облачных хранилищ;
   - Правило контроля внешних устройств;
   - Правило контроля съемных устройств;
   - Правило контроля сетевых ресурсов;
   - Правило контроля терминальной сессии;
   - Правило контроля FTP;
   - Правило контроля HTTP(S);
   - Правило контроля мессенджера VK;
   - Правило контроля мессенджера Telegram;
   - Правило контроля протокола XMPP;
   - Правило контроля ввода текста с клавиатуры;
   - Правило контроля почты;
   - Правило контроля печати;
   - Правило контроля экрана;

- Правило контроля активности сотрудника.

5. После того как вы указали все необходимые параметры, нажмите **Создать**. Правило будет добавлено в политику.

Чтобы просмотреть детальную информацию о правиле, выберите его. Справа откроется панель **Подробно** с информацией о выбранном правиле. Вы также можете открыть панель с детальной информацией кнопкой  справа в середине экрана. Чтобы скрыть панель, нажмите .

Чтобы отредактировать правило:

1. Выберите правило, которое необходимо отредактировать.
2. Нажмите .
3. Внесите изменения.
4. Подтвердите действие, нажав **Сохранить**.

Чтобы удалить правило:

1. Перейдите в раздел **Политики**.
2. Выберите правило, которое необходимо удалить.
3. Нажмите .
4. Подтвердите действие, нажав **Подтвердить**.

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 переименования файлов на съемных устройствах;
- копирования файлов с/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, РЕД ОС и ОС Альт 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. Выберите направление перехвата копирования: *На устройство* или *С устройства*. Событие будет создано в результате копирования файла в выбранном направлении.

4. В **Действии** при срабатывании правила выберите реакцию Системы на копирование файла:
   - *Создать событие* – при этом будет создано событие с теневой копией.
   - *Исключить из перехвата* – при этом копирование будет разрешено, событие создано не будет. Заполните поле **Маска файла**.
5. Укажите условия для формирования событий:
   a. Отметьте **Маска файлов**, чтобы исключить из перехвата подходящие под нее файлы. Например, введите в строке:
      - ? – один неизвестный символ;
      - * – любое количество символов.
   b. Отметьте **Размер файла**, чтобы ограничить размер файлов, подлежащих контролю. При этом 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.
   Если условия не отмечены, событие будет сформировано без их учета.
6. 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.

Важно!

При копировании с/на съемные устройства блокировка по результатам анализа не осуществляется на компьютерах под управлением ОС Astra Linux версий 1.6 и 2.12.

На рабочих станциях под управлением ОС семейства Linux при блокировке копирования:

- Копируемые файлы удаляются (с возможностью восстановления при условии использования специального ПО).
- Если съемное устройство было извлечено принудительно, блокировка копирования файлов по результатам анализа может не произойти.
- При копировании файлов с рабочей станции на съемное устройство не определяется путь файла. Поэтому политики, настроенные на путь, как источник копирования, могут не сработать.
- Не осуществляется блокировка по результатам анализа при копировании файлов на медиа-устройства, подключённые по протоколу MTP.
- Если срабатывает блокировка файла по результатам анализа при его перемещении или осуществлении над ним операции *вырезать-вставить*, файл может быть удален из источника и отсутствовать в приемнике.

Система распаковывает архивы и применяет к ним политики Traffic Monitor, если:

- перехвачен архив формата 7Z, ZIP, TAR.GZ, AR, RAR или ISO на Агенте под управлением ОС Windows;
- перехвачен архив формата 7Z, ZIP, AR или TAR.GZ на Агенте под управлением ОС Альт, РЕД ОС или ОС Astra Linux 1.7.

Об особенностях работы правила см. статью Базы Знаний "Особенности и ограничения перехвата при копировании файлов с/на съемные устройства, сетевые ресурсы, FTP, перехвата исходящей почты. Особенности задания правил в политиках защиты данных на агентах".

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 с сетевых ресурсов на рабочую станцию под управлением ОС семейства Linux может быть заблокировано только при передаче по протоколу SMBv1/CIFS одним из способов:

- подключением к сетевым ресурсам с монтированием в файловую систему: `mount -t cifs`
- подключением к сетевым ресурсам с помощью стандартных проводников, встроенных и сторонних утилит

Система распаковывает архивы и применяет к ним политики Traffic Monitor, если:

- перехвачен архив формата 7Z, ZIP, TAR.GZ, AR, RAR или ISO на Агенте под управлением ОС Windows;
- перехвачен архив формата 7Z, ZIP, AR или TAR.GZ на Агенте под управлением ОС Альт, РЕД ОС или ОС Astra Linux 1.7.

Важно!

На компьютерах под управлением Astra Linux, РЕД ОС и ОС Альт:

- при копировании файлов на сетевые ресурсы известен только путь конечного назначения, а при копировании с сетевого ресурса, известен только путь источника;
- не перехватывается копирование файла на сетевой ресурс, если подключение осуществлялось вводом имени сервера в строке поиска файлового менеджера ОС.

Важно!

На компьютерах под управлением ОС Astra Linux версий 1.6 и 2.12 не осуществляется блокировка файла по результатам анализа при копировании с/на сетевые ресурсы.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль сетевых ресурсов**.
3. Выберите направление перехвата копирования: *На ресурс* или *С ресурса*. Событие будет создано в результате копирования файла в выбранном направлении.

4. В **Действии** при срабатывании правила выберите реакцию Системы на копирование файла:
   - *Создать событие* – при этом будет создано событие с теневой копией.
   - *Запретить копирование*
   - *Исключить из перехвата* – при этом копирование будет разрешено, событие создано не будет. Заполните поле **Маска файла**.
5. Если требуется, укажите **Ресурсы**, задав их адреса. Чтобы посмотреть правила заполнения, наведите курсор на .
6. 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 ОС Astra Linux или РЕД ОС маски файлов не учитываются.

7. 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.

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

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

10.2.3 Правило контроля терминальной сессии

Правило позволяет отслеживать операции:

- копирования файла в приложение терминальной сессии;

  Важно!

При копировании файла через терминальную сессию с помощью буфера обмена будет известно только короткое имя файла, а не полный путь.

Чтобы в событии был известен IP-адрес узла, на который были скопированы данные, необходимо наличие Агента Device Monitor на удалённом компьютере, к которому открыта терминальная сессия.
Если Агент Device Monitor установлен только на компьютере, с которого идет подключение к терминальной сессии, то в событии будет известно только приложение, через которое осуществлялось копирование данных, без указания IP-адреса получателя.

Примечание:

Для передачи файлов при использовании средств обеспечения терминального доступа рекомендуется использовать механизм "проброса" дисков в удаленный сеанс вместо передачи при помощи буфера обмена.

- копирования файла на ресурсы, подключенные через терминальную сессию (поддерживается перенаправление для сетевых папок и виртуальных устройств).

Важно!

Не будут созданы события терминальной сессии при копировании файлов не через границу терминальной сессии, а внутри локального клиента удаленного подключения. Например, при копировании файлов пользователем в окне **Параметры подключения** -> **Открытие файла**.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль терминальной сессии**.
3. Выберите направление перехвата копирования: *В сессию* или *Из сессии*. Событие будет создано в результате копирования файла в выбранном направлении.
4. В **Действии** при срабатывании правила выберите реакцию Системы на копирование файла:
   - *Создать событие* – при этом будет создано событие с теневой копией.
   - *Исключить из перехвата* – при этом копирование будет разрешено, событие создано не будет. Заполните поле **Маска файла**.
5. Если требуется, укажите **Ресурсы**, задав их адреса. Чтобы посмотреть правила заполнения, наведите курсор на .
6. Укажите условия для формирования событий:
   a. Отметьте **Маска файлов**, чтобы исключить из перехвата подходящие под нее файлы. Например, введите в строке:
      - ? – один неизвестный символ;
      - * – любое количество символов.
   b. Отметьте **Размер файла**, чтобы ограничить размер файлов, подлежащих контролю. При этом 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.

Если условия не отмечены, событие будет сформировано без их учета.

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.

10.2.4 Правило контроля печати

Правило позволяет осуществлять мониторинг операций, связанных с печатью документов на локальных и сетевых принтерах, в том числе с запуском печати через терминальную сессию.

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.
   Для Агентов на рабочих станциях под управлением ОС Windows есть возможность блокировки печати по результатам анализа. Для этого необходимо настроить политику защиты данных на агентах в Traffic Monitor.

   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, РЕД ОС и ОС Альт:

   - не определяется пользователь, отправивший файл на печать;
   - не определяется количество страниц в теневой копии;
   - не осуществляется перехват документов, отправленных на печать через терминальную сессию;
   - 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.

   Важно!

   События печати не будут сформированы при печати в файл на Агентах, установленных на ОС Astra Linux, РЕД ОС и ОС Альт, а также при печати на предустановленном принтере на Агентах, установленных на ОС Astra Linux.

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

10.2.5 Правило контроля внешних устройств

Правило позволяет контролировать доступ и использование съемных устройств хранения.

Важно!

На компьютерах под управлением ОС семейства Linux поддерживается контроль только следующих типов устройств:

- Съемное устройство хранения;

- MTP-устройство;
- CD/DVD;
- Флоппи-диск.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль внешних устройств**.
3. В поле **Тип устройства** выберите тип устройства, контролируемого данным правилом:
   - Съемное устройство хранения;
   - MTP-устройство;
   - CD/DVD;
   - Флоппи-диск;
   - Другое устройство USB;
   - Сетевой адаптер USB;
   - Bluetooth-устройство;
   - Локальный принтер;
   - Сетевой принтер;
   - Терминальный принтер;
   - Устройство работы с изображениями (камера, сканер).
4. Выберите необходимый вариант ограничения доступа на использование устройства:
   - *Запретить использование:*
     - на компьютерах под управлением ОС Windows – для съемных устройств хранения, CD/DVD, Флоппи-дисков и MTP-устройств;
     - на компьютерах под управлением ОС семейства Linux – только для съемных устройств хранения и MTP-устройств;
   - *Разрешить использование*;
   - *Разрешить только чтение* – разрешен доступ к устройствам хранения информации, а действия с изменением содержимого (запись, удаление, переименование, форматирование и т.п.) этого типа устройства блокируются. Этот вариант используется для: съемного устройства хранения, CD/DVD, флоппи-диска, MTP-устройства.

   Примечание:

   Контроль подключения через MTP-протокол осуществляется для устройств на платформах: Android, iOS, Windows Phone/10 Mobile; Blackberry 10.

   Примечание:

   Если созданы правила, запрещающие использование устройств, и правила, разрешающие их использование, то использование устройств будет разрешено.

5. Нажмите **Сохранить**. Правило будет действовать всегда.

Особенности применения правила при обновлении:

После обновления Агента на текущую версию для поддержки запрета доступа к MTP-устройствам необходимо перезагрузить рабочую станцию. При чистой установке перезагрузка не требуется.

10.2.6 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;
- ограничивать доступ к FTP-ресурсам.

> **Важно!**
>
> На компьютерах под управлением РЕД ОС и ОС Альт 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".

10.2.7 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 запросов, размер которых больше либо равен указанному.
   b. Отметьте **Максимальный**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для запросов, размер которых меньше либо равен указанному.
5. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Важно!

На компьютерах под управлением ОС Astra Linux, РЕД ОС или ОС Альт:

- политика защиты данных на агентах применяется только к тексту запроса, анализ файлов не поддерживается;
- не перехватываются соединения по протоколу IPv6;
- запросы, относящиеся к веб-почте, перехватываются как обычные HTTP-запросы.

Важно!

Блокировка HTTP(S)-трафика по результатам анализа не осуществляется на компьютерах под управлением ОС Astra Linux версий 1.6 и 2.12.

10.2.8 Правило контроля почты

Правило контроля почты позволяет перехватывать получение электронной почты по POP3, IMAP и отправку почты по SMTP, HTTPS, а также осуществлять запрет на отправку веб-почты по HTTPS.

Важно!

Перехват сообщений по протоколу HTTPS поддерживается только при использовании сервисов веб-почты: Gmail, Yandex, Mail.ru, Yahoo, Rambler, Outlook.com.

Не осуществляется перехват почты по протоколу HTTPS через Outlook Web App при использовании сервера MS Exchange.

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.

Важно!

На рабочих станциях под управлением ОС семейства Linux осуществляется блокировка только исходящего трафика (SMTP-протокол и веб-почта). При этом файлы, передаваемые по веб-почте, не анализируются. На компьютерах под управлением ОС Astra Linux версий 1.6 и 2.12 блокировка почтового трафика по результатам анализа в Traffic Monitor не поддерживается.

Важно!

Система распаковывает архивы и применяет к ним политики Traffic Monitor, если:

- перехвачен архив формата 7Z, ZIP, TAR.GZ, AR, RAR или ISO на Агенте под управлением ОС Windows;
- перехвачен архив формата 7Z, ZIP, AR или TAR.GZ, передаваемый по протоколу SMTP как вложение к письму, на Агенте под управлением ОС Альт, РЕД ОС или ОС Astra Linux 1.7.

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.

Важно!

При запрете доступа к хранилищу Google Drive возможны некорректная работа и запрет использования других сервисов Google, которые используют хост docs.google.com. Например, Google Docs, Google Tabs, Google Slides и т.д.

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.

10.2.10 Правило контроля экрана

Правило позволяет создавать снимки экрана в формате PNG:

- при смене активного окна любых приложений;
- всех мониторов, подключенных к незаблокированному контролируемому компьютеру.

> **Примечание:**
>
> Правило доступно для рабочих станций под управлением ОС Windows, РЕД ОС или ОС Альт.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль экрана**.
3. Укажите, когда необходимо создавать снимки экрана, или выберите оба условия:
   - *При смене активного окна* – распространяется на любые приложения, но не учитывается смена вкладок браузера;
   - *Через каждые n секунд* – период времени между снимками экрана.
4. Нажмите **Создать**. Правило будет действовать всегда.

> **Важно!**
>
> Снимок всего экрана создается в течение 5 секунд после активации окна/вкладки. Если переключение активного окна/вкладки происходит чаще, чем один раз в 5 секунд, снимок экрана не будет создан.

10.2.11 Правило контроля буфера обмена

Правило позволяет контролировать доступ сотрудников к буферу обмена.

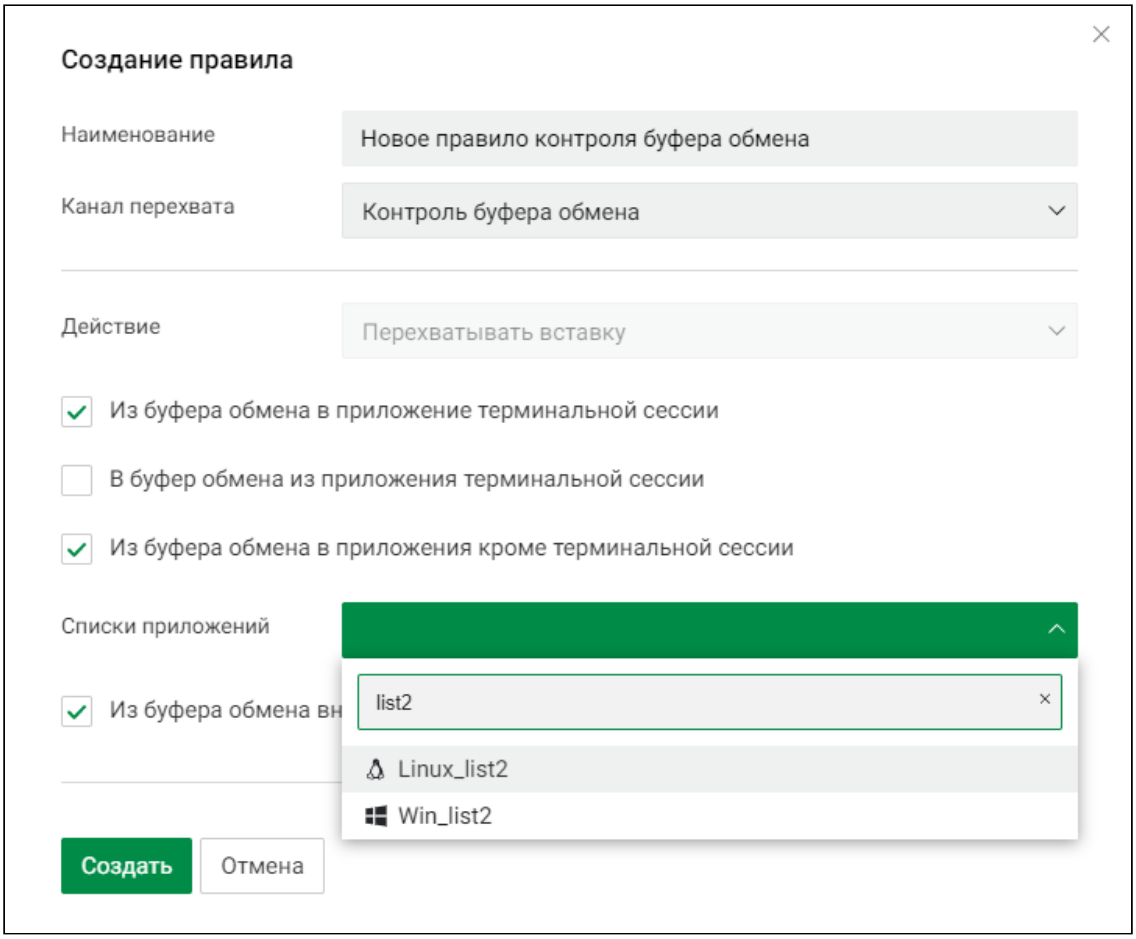
> **Важно!**
>
> Контроль буфера обмена работает на компьютерах под управлением ОС MS Windows, РЕД ОС и ОС Альт Рабочая станция.
>
> По правилу контроля буфера обмена Device Monitor перехватывает только текстовые данные.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль буфера обмена**.
3. В блоке **Действие** доступно только **Перехватывать вставку**.
   Укажите, когда должно срабатывать привило. Для создания правила должна быть выбрана хотя бы одна из опций:
   - **Из буфера обмена в приложение терминальной сессии**. Если выбрана эта опция, правило будет срабатывать при вставке данных в приложения терминальной сессии. При вставке данных внутри терминальной сессии правило срабатывать не будет.
   - **В буфер обмена из приложения в терминальной сессии**. Если выбрана эта опция, правило будет срабатывать при вставке данных из приложения терминальной сессии. При вставке данных внутри терминальной сессии правило срабатывать не будет.

     > **Важно!**
     >
     > На рабочих станциях под управлением РЕД ОС и ОС Альт Рабочая станция не поддерживаются опции:
     >
     > - **Из буфера обмена в приложение терминальной сессии**;
     > - **В буфер обмена из приложения в терминальной сессии**.
     >
     > Чтобы настроить правило для РЕД ОС и ОС Альт Рабочая станция, выберите опцию **Из буфера обмена в приложения кроме терминальной сессии** и выберите список приложений для Linux.
     > На рабочих станциях под управлением РЕД ОС и ОС Альт Рабочая станция не поддерживается использование опции **Из буфера обмена внутри одного и того же приложения**.

   - **Из буфера обмена в приложения кроме терминальной сессии**. Выберите эту опцию, если правило должно действовать при вставке данных в указанные приложения. Правило также будет срабатывать при вставке в приложения данных, скопированных из терминальной сессии.
     Для использования опции выберите списки в поле **Списки приложений** (о создании списков приложений см. "Создание и изменение списков приложений").
     Для выбора списков вы можете воспользоваться строкой поиска.



- Чтобы правило срабатывало также при вставке данных в приложение, из которого данные были скопированы, отметьте опцию **Из буфера обмена внутри одного и того же приложения**.
  Перехват в пределах одного приложения поддерживается, только если приложение использует системные механизмы буфера обмена.

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

10.2.12 Правило контроля мессенджера VK

Правило позволяет контролировать обмен сообщениями чата и любыми типами исходящих файлов в веб-версии системы мгновенного обмена сообщениями VK (ВКонтакте). При этом будет перехвачена вся история переписки на служебном компьютере, включая период до установки Агента Device Monitor.

Важно!

Не поддерживается перехват:

- файлов, загруженных с компьютера без установленного Агента Device Monitor;
- постов на стене;
- сообщений, содержащих геопозицию;
- истории отредактированных сообщений.

Чтобы создать и 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 задать условия для формирования событий, перейдите в раздел **Настройки > Каналы перехвата** (подробнее см. "Каналы перехвата").

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

10.2.13 Правило контроля мессенджера Telegram

Правило позволяет контролировать обмен новыми, пересылаемыми или исправленными сообщениями чата, в том числе группового, исходящими файлами и голосовыми сообщениями на толстом клиенте и в веб-версии системы мгновенного обмена сообщениями Telegram. При этом будет перехвачена вся история переписки на служебном компьютере, включая период до установки Агента Device Monitor.

> **Важно!**
>
> Не поддерживается запрет использования.
>
> Не поддерживается перехват:
>
> - стикеров;
> - gif-анимации;
> - контактов;
> - геоположения;
> - каналов;
> - аудиозвонков;
> - опросов;
> - текста, который был прикреплен в качестве ссылки.

Для Telegram на компьютерах под управлением **ОС семейства Linux**:

- поддерживается перехват только десктоп-версии Telegram;
- для перехвата должен быть включен системный вызов `ptrace()`;
- не поддерживается перехват Flatpak-приложения.

Для Telegram на компьютерах под управлением **MS Windows**:

- Правило позволяет перехватывать следующие версии Telegram:
  - десктоп-версию: приложение с официального сайта Telegram (desktop.telegram.org) или из Microsoft Store;
  - веб-версии: K, Z и устаревшую (Legacy).
- Перехват веб-версий имеет ряд особенностей:
  - разные веб-версии определяются Системой как разные приложения;
  - существует временная задержка начала перехвата - до 50 секунд с момента авторизации;
  - поддерживаются браузеры:
    - Google Chrome;
    - Microsoft Edge;
    - Mozilla Firefox;
    - Opera;
    - Яндекс Браузер.

При отправке сообщений в групповой чат Telegram, событие будет содержать Идентификатор группового чата.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль мессенджера Telegram**.
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 задать условия для формирования событий, перейдите в раздел **Настройки > Каналы перехвата** (подробнее см. "Каналы перехвата").

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

10.2.14 Правило контроля протокола XMPP

Правило позволяет контролировать обмен по протоколу **XMPP** входящими и исходящими текстовыми сообщениями, а также исходящими файлами.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль протокола XMPP**.
3. Если вы хотите передавать в Traffic Monitor, помимо события, и теневые копии исходящих файлов, отметьте поле **Создавать теневую копию исходящих файлов**.
   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 задать условия для формирования событий, перейдите в раздел **Настройки > Каналы перехвата** (подробнее см. "Каналы перехвата").

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

10.2.15 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 ОС MS Windows, ОС Альт и 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 символов, введенных с клавиатуры;
- при нажатии Enter / Ctrl+Enter / Shift+Enter.

Чтобы создать 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. Выберите одно из действий правила:
   - **Перехватывать ввод текста во всех приложениях**
   - **Перехватывать ввод текста для приложений из списка** - Device Monitor будет создавать событие при вводе текста в активном окне приложений из списка.

     Примечание:

     Поддерживается использование только списков для ОС MS Windows.

   - **Не перехватывать ввод текста для приложений из списка** - Device Monitor **не** будет создавать событие при вводе текста в активном окне приложений из списка.
4. Если выбрано действие, учитывающее списки приложений, в появившемся поле укажите их.
   Подробнее о создании списков приложений см. "Создание и изменение списков приложений".
5. Если требуется, включите опцию **Создавать снимок экрана при создании события**.

   Примечание:

   Создание снимка экрана при создании события поддерживается только на рабочих станциях под управлением ОС MS Windows.

   Примечание:

   Настройка и применение правила контроля ввода текста с клавиатуры и правила контроля экрана осуществляются независимо друг от друга.

6. Нажмите **Создать**.

Чтобы задать условия для формирования событий, перейдите в раздел **Настройки> Каналы перехвата** (подробнее см. "Каналы перехвата").

Важно!

Для Агента на ОС Альт или 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.

10.2.16 Правило контроля активности сотрудника

Правило позволяет собирать статистику активности сотрудника за контролируемым компьютером, формировать события и отправлять их в Activity Monitor.

> **Примечание:**
>
> Правило доступно для рабочих станций под управлением ОС Windows, РЕД ОС или ОС Альт.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Контроль активности сотрудника**.
3. Выберите действие:
   - **Собирать статистику активности**, чтобы контролировать активность и собирать данные по действиям сотрудника:
     - Локальный вход в сессию;
     - Локальный выход из сессии;
     - Удаленный вход в сессию;
     - Удаленный выход из сессии;
     - Локальная блокировка сессии;
     - Локальная разблокировка сессии;
     - Удаленная блокировка сессии;
     - Удаленная разблокировка сессии;
     - Запуск приложения;
     - Остановка приложения;
     - Переключение между приложениями;
     - Переключение между вкладками в браузере;
     - Выполнение поисковых запросов;
     - Получение и потеря фокуса активного окна;
     - Использование клавиатуры.
   - **Не собирать статистику активности**, чтобы контролировать активность без сбора данных.
4. Нажмите **Создать**. Правило будет действовать всегда.

Чтобы данные статистики успешно отправлялись в Activity Monitor, убедитесь, что установлено подключение к Платформе (подробнее см. "Серверы – Подключение к Платформе").

> **Важно!**
>
> Для операционной системы РЕД ОС контролируются следующие действия пользователя в Системе:
>
> - Локальный вход в сессию;
> - Локальный выход из сессии;
> - Локальная разблокировка сессии;
> - Локальная блокировка сессии;
> - Получение фокуса активного окна приложения;
> - Потеря фокуса активного окна приложения;

- Использование клавиатуры;
- Получение фокуса вкладкой браузера (для браузера Edge (Chromium).

Для операционной системы ОС Альт контролируются такие же действия пользователя, как для системы РЕД ОС, за исключением *Получения фокуса вкладкой браузера*.

Примечание:

Если выбрано действие **Не собирать статистику активности**, то события, сформированные в Device Monitor, не отправляются в Платформу.

Если вы хотите, чтобы какие-либо события (например, события создания снимков экрана по Правилу контроля экрана) отправлялись в Платформу, даже если выбрано действие **Не собирать статистику активности**, задайте значение `False` полю `SEND_EVENT_TO_PLATFORM_WITH_CHECK` таблицы Settings Базы Данных. По умолчанию данное поле имеет значение `True`.

10.3 Создание и изменение списков приложений

Для более точной работы Агентов на контролируемых рабочих станциях вы можете использовать списки приложений.

10.3.1 Создание списка приложения

Чтобы создать список приложений:

1. В консоли управления Device Monitor перейдите в раздел **Справочники**.
2. Слева в секции **Списки приложений** нажмите .
3. В открывшемся окне:
   a. В поле **Название** - укажите название списка.
   b. В поле **Операционная система** - выберите одно из семейств ОС:
      - **Windows** - список будет отмечен значком 
      - **Linux** - список будет отмечен значком 
4. Нажмите .

10.3.2 Добавление приложений в список

Чтобы наполнить список вы можете:

- Добавить приложение вручную;
- Добавить приложение из подраздела **Протокол приложений** (только в списки **для ОС MS Windows**);
- Переместить или скопировать приложение из другого списка.

Добавление приложения в список вручную

Чтобы добавить приложение в список:

1. В консоли управления Device Monitor перейдите в раздел **Справочники**.
2. В секции **Приложения** нажмите .
3. В открывшемся окне окне укажите:
    a. **Описание**
    b. **Имя приложения** – имя исполняемого файла с расширением.
    c. **Расположение исполняемого файла** – абсолютный (полный) путь к папке, содержащей исполняемый файл. При указании пути вы можете использовать переменные окружения.
    d. **Издатель** - только для списков приложений ОС MS Windows;
    e. **Название продукта** – поле доступно, если указан **Издатель**.

    > **Примечание:**
    >
    > Для добавления приложения в список обязательно должны быть заполнены поле **Описание** и одно из полей: **Имя приложения**, **Расположение исполняемого файла** или **Издатель**.
    >
    > Чтобы определить, соответствует ли запускаемое приложение приложению из списка, сравниваются значения атрибутов:
    >
    > - **Имя приложения**;
    > - **Расположение исполняемого файла**;
    > - **Издатель**.
    >
    > Проверка отличается в зависимости от ОС контролируемой рабочей станции:
    >
    > - ОС MS Windows – регистр **не** учитывается;
    > - ОС семейства Linux – регистр учитывается.
    >
    > Обратите на это внимание при указании атрибутов приложений.
    >
    > Если в списке приложений поле атрибута не заполнено, оно проходит проверку.
    >
    > **Пример**: Если добавить в список приложение, в котором будут заполнены только **Описание** и **Издатель**, ему будут соответствовать все приложения этого издателя, независимо от имени и расположения исполняемого файла.

4. После заполнения полей, нажмите **Добавить**.

Добавление в список из Протокола приложений

Вы можете добавлять приложения из протокола только в списки **для ОС MS Windows**.

Чтобы добавить приложение из протокола приложений:

1. В консоли управления Device Monitor перейдите в раздел **Справочники** -> **Протокол приложений**.
2. Выберите одно или несколько приложений, которые необходимо добавить в списки приложений.
3. Справа вверху нажмите 
4. В открывшемся окне в поле **Списки** выберите список, в который необходимо добавить приложения.
5. Нажмите **Сохранить**.

Если необходимо добавить приложения в новый список:

1. Выполните шаги 1-3 из инструкции выше.

2. В открывшемся окне нажмите **Новый список**.
3. В открывшемся окне в поле **Название** введите название списка.
4. Нажмите .

> **Примечание:**
>
> Если из протокола приложений добавляется приложение, у которого нет описания, то в поле **Описание** у данного приложения будет отображаться его имя

Копирование и перемещение приложений

Приложения можно копировать и перемещать из одного списка в другой.

> **Примечание:**
>
> Не поддерживается перемещение или копирование приложения в список для ОС другого семейства. То есть вы не можете скопировать или переместить в список для Linux приложение из списка для Windows, и наоборот.

Чтобы скопировать или переместить приложение:

1. Выделите приложения, которые планируете переместить или скопировать. Чтобы выделить несколько приложений, выбирайте их с зажатой клавишей Ctrl или Shift.
2. Нажмите:
   -  – для перемещения приложений;
   -  – для копирования приложений.
3. В открывшемся окне выберите список, в который планируете переместить или скопировать приложения.
4. Нажмите **Сохранить**.

10.3.3 Редактирование и удаление списка приложений

Чтобы отредактировать список или приложение:

1. Выберите необходимый элемент.
2. Нажмите .
3. В открывшемся окне внесите правки и сохраните изменения.

Чтобы удалить список или приложение:

1. Выберите необходимый элемент.
2. Нажмите .
3. В открывшемся окне подтвердите удаление выбранных элементов.

Примечание:

Список приложений нельзя удалить, если он используется в правиле политики.

10.4 Создание и редактирование групп сотрудников

Управление учетными записями сотрудников и их мониторинг ведется в разделе **Сотрудники**.

Важно!

Когда регистрируется новый сотрудник, информация о нем автоматически добавляется в схему безопасности (в группу сотрудников «по умолчанию»).

Примечание:

Чтобы получать информацию о сотрудниках из службы каталогов, вы можете выполнить синхронизацию с LDAP-сервером. Подробнее см. "Синхронизации".

Чтобы добавить группу сотрудников:

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

Чтобы отредактировать группу сотрудников:

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

Чтобы удалить группу сотрудников:

1. Выделите группу для удаления.

   Примечание

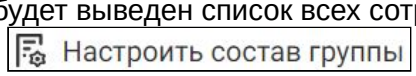
   Группу сотрудников «по умолчанию» удалить нельзя.

2. Нажмите . В группе сотрудников, которую вы удаляете, могут быть сотрудники, не включенные в другие группы. В этом случае сотрудники будут автоматически добавлены в группу сотрудников «по умолчанию».
3. В открывшемся окне нажмите **Подтвердить**.

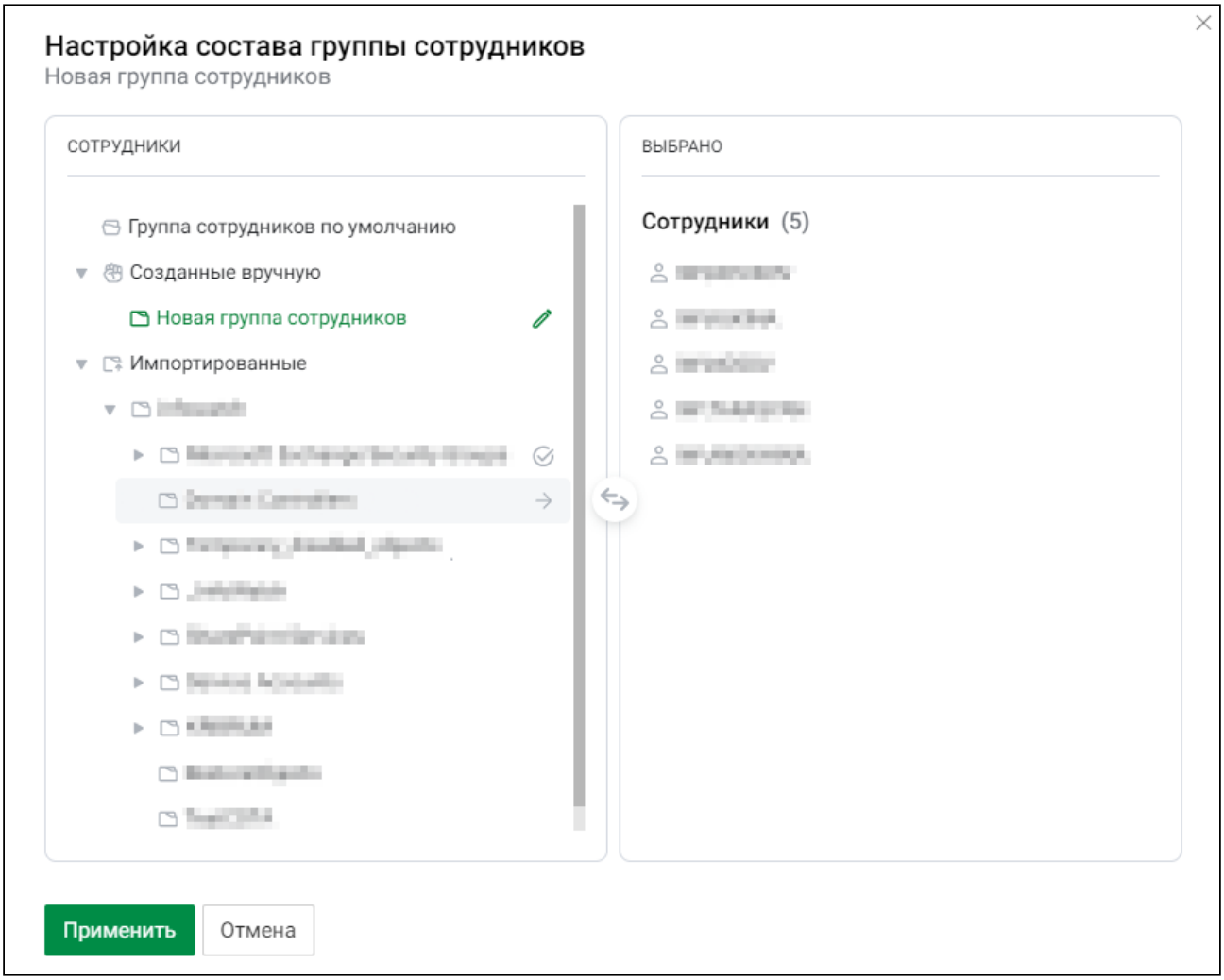
10.5 Настройка состава групп сотрудников

При установке Агента InfoWatch Device Monitor на рабочую станцию, в Системе автоматически создаются записи о пользователях этой рабочей станции. Эти записи добавляются в "Группу сотрудников по умолчанию". На всех сотрудников, входящих в эту группу, будет распространяться назначенная ей политика. В дальнейшем определение политик для сотрудника происходит путем его включения в различные группы сотрудников.

Чтобы настроить состав группы сотрудников:

1. Перейдите в раздел **Сотрудники**.
2. В левой части рабочей области выберите группу. В центральной части рабочей области будет выведен список всех сотрудников, уже входящих в группу.
3. Нажмите 

.
Откроется диалоговое окно. В его левой части отобразится список ранее зарегистрированных в Системе сотрудников.
4. Чтобы развернуть или свернуть какую-либо группу сотрудников в списке, используйте 
.
5. В области слева наведите курсор на необходимого сотрудника или группу и нажмите  **Добавить сотрудников в "<Название группы сотрудников>"**. Сотрудник будет включен в выбранную группу. В области слева напротив группы или сотрудника, которые были добавлены, появится значок .
6. Чтобы удалить из группы сотрудника или группу, наведите курсор на удаляемую запись и нажмите  **Удалить из группы "<Название группы сотрудников>"**. Это можно сделать, как в области справа, так и в области слева.
7. Нажмите **Применить**.



Примечание:

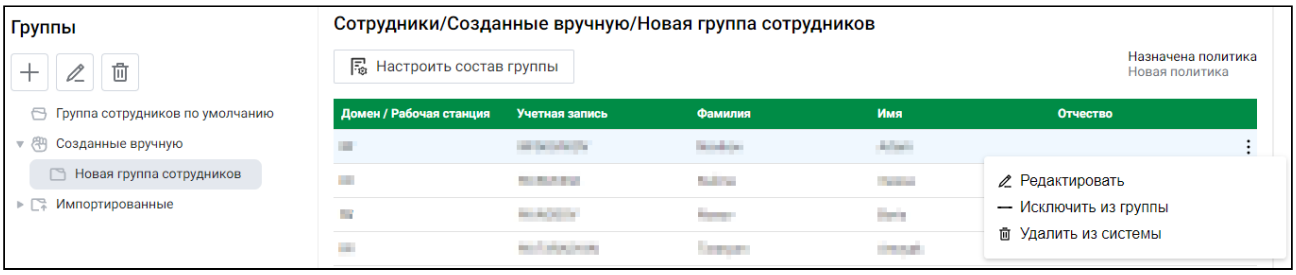
Если вы добавляете группу сотрудников, которая содержит подгруппы, то сотрудники из подгрупп не будут автоматически добавлены в выбранную группу. Вы можете добавить их отдельно.

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

Важно!

Если сотрудник никогда не выполнял вход на рабочую станцию с Агентом (например, подключался по SSH), то назначенная ему политика не сработает. В этом случае перехват производится в соответствии с правилами в политике по умолчанию. Если правил в политике по умолчанию нет, то перехват не будет осуществлен.

Внутри группы сотрудников вы можете работать с их списком: редактировать, исключать из группы, удалять сотрудников из системы.



Примечание:

Для импортированных групп сотрудников внутри группы доступно только редактирование.

Чтобы отредактировать запись сотрудника:

1. В строке с именем сотрудника нажмите ⋮.
2. Выберите ✎ **Редактировать**.
3. Если запись сотрудника создана при синхронизации со службой каталогов, нажмите **Получить имя**, чтобы получить актуальные данные этого сотрудника.
4. Также вы можете вручную изменить **Фамилию**, **Имя** и **Отчество** сотрудника.
5. После внесения необходимых изменений нажмите **Сохранить**.

Чтобы исключить сотрудника из группы:

1. В строке с именем сотрудника нажмите ⋮.
2. Выберите — **Исключить из группы**.
3. Нажмите **Да**. Если сотрудник входил только в одну группу, то при исключении он будет автоматически добавлен в группу сотрудников "по умолчанию".

При необходимости вы можете удалить сотрудника из списка зарегистрированных.

Чтобы удалить сотрудника из схемы безопасности:

1. В строке с именем сотрудника нажмите ⋮.
2. Выберите 🗑 **Удалить из системы**.
3. В открывшемся диалоговом окне нажмите **Подтвердить**.

Важно!

Удаление сотрудника из схемы безопасности повлечет за собой его удаление из всех групп и политик.

11 Пользовательское лицензионное соглашение

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

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

1. Предоставление лицензии

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

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

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

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

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

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

2. Условия использования

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

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

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

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

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

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

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

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

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

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

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

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

2.10. Вам не разрешается:

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

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

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

3. Ограничение гарантий и ответственности Правообладателя

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

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

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

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

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

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

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

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

4. Права на объекты интеллектуальной собственности

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

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

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

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

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

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

6. Открытое программное обеспечение

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

7. Заключительные положения

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

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

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

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

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

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

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

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

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

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

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

8. Контактная информация Правообладателя

Тел./факс: +7(495)229-00-22

Коммерческий департамент: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru