

INFOWATCH

InfoWatch Device Monitor for Linux. Руководство пользователя

05/11/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 7

2 Комплект документов 8

3 Техническая поддержка пользователей 9

4 Обзор 10

5 Настройки пользователей 12

5.1 Пользователи 12

5.1.1 Создание нового пользователя 12

5.1.2 Просмотр профиля пользователя 13

5.1.3 Редактирование учетной записи 14

5.1.4 Смена пароля пользователя 14

5.1.5 Активация и деактивация пользователя 15

5.1.6 Удаление пользователя 15

5.2 Роли 15

6 Общие настройки 16

6.1 Настройки пароля 16

6.2 Мониторинг состояния Системы 17

6.3 Интеграции 19

6.3.1 Интеграция с Active Directory 19

6.3.2 Редактирование и удаление интеграции 22

7 Настройка Device Monitor 24

7.1 Серверы 24

7.2 Синхронизация 27

7.3 Исключение приложений из перехвата 31

7.4 Универсальный перехватчик файлов 33

7.5 Каналы перехвата 37

7.5.1 Хосты для VK+ 40

7.6 Контроль сетевых ресурсов 41

7.7 Уведомления 42

7.8 Агенты 45

7.9 Корпоративные сети 48

7.10 Отправка данных в продукты ... 49
7.10.1 Отправка событий в Traffic Monitor и Платформу ... 49
7.10.2 Пример настроек отправки данных ... 51
7.11 Конфигурация ... 51
7.12 Диагностика событий ... 53
8 Интерфейс Центра Администрирования (Device Monitor) ... 55
8.1 Раздел "Политики" ... 57
8.2 Раздел "Группы" ... 59
8.3 Раздел "Задачи" ... 60
8.4 Раздел "Ресурсы" ... 61
8.4.1 Списки веб-ресурсов ... 61
8.4.2 Списки приложений ... 61
Обнаруженные приложения ... 62
8.4.3 Категории файлов ... 62
8.5 Раздел "Агенты" ... 63
8.6 Раздел "Файловая статистика" ... 63
9 Обнаружение рабочих станций для установки Агентов ... 65
10 Задача первичного распространения и обновления ... 67
11 Настройка схемы безопасности ... 71
11.1 Режимы редактирования конфигурации ... 71
11.1.1 Режим запрета синхронного редактирования ... 72
11.1.2 Автоматический сброс несохраненных изменений конфигурации ... 72
11.1.3 Описание режима запрета редактирования ... 73
11.1.4 Восстановление доступа к заблокированной конфигурации ... 73
11.1.5 Редактирование конфигурации при запущенной синхронизации со службой каталогов ... 74
11.2 Создание политик ... 74
11.3 Создание правил ... 76
11.3.1 Правило контроля съемных носителей ... 77
11.3.2 Правило контроля сетевых ресурсов ... 80
11.3.3 Правило контроля терминальной сессии ... 82
11.3.4 Правило контроля печати ... 84
11.3.5 Правило контроля внешних устройств ... 85
11.3.6 Правило контроля FTP ... 85
11.3.7 Правило контроля HTTP(S) ... 87
11.3.8 Правило контроля почты ... 88
11.3.9 Правило контроля облачных хранилищ ... 89
11.3.10 Правило проксирования сетевого трафика ... 90

11.3.11 Правило контроля буфера обмена ... 91
11.3.12 Правило контроля мессенджера VK ... 93
11.3.13 Правило контроля мессенджера Telegram ... 94
11.3.14 Правило контроля Яндекс Мессенджера ... 96
11.3.15 Правило контроля мессенджера WhatsApp ... 97
11.3.16 Правило контроля мессенджера MAX ... 98
11.3.17 Правило контроля протокола XMPP ... 99
11.3.18 Правило контроля создания снимков экрана ... 100
11.3.19 Правило мониторинга экрана ... 101
11.3.20 Правило мониторинга ввода текста с клавиатуры ... 102
11.3.21 Правило мониторинга активности сотрудника ... 104
Контроль действий ... 105
11.3.22 Правило мониторинга звукового окружения ... 108
11.3.23 Правило записи видео с экрана ... 110
11.3.24 Правило контроля файлов в приложениях ... 111
11.4 Создание и изменение списков приложений ... 113
11.4.1 Создание списка приложения ... 113
11.4.2 Добавление приложений в список ... 113
Добавление приложения в список вручную ... 114
Добавление обнаруженных приложений в список ... 115
Копирование и перемещение приложений ... 115
11.4.3 Редактирование и удаление списков и приложений ... 116
11.5 Создание и изменение списков ресурсов ... 117
11.5.1 Создание списка ресурсов ... 117
Определение соответствия посещаемого ресурса ресурсу из списка ... 117
11.5.2 Редактирование списка ресурсов ... 118
11.5.3 Удаление списка ресурсов ... 119
11.6 Создание и изменение категорий файлов ... 120
11.6.1 Создание категории файлов ... 120
11.6.2 Изменение состава категории файлов ... 120
11.6.3 Редактирование и удаление категории файлов ... 121
11.7 Работа с группами компьютеров ... 121
11.7.1 Создание и редактирование групп компьютеров ... 121
11.7.2 Настройка состава групп компьютеров ... 123
11.7.3 Просмотр сведений о компьютерах ... 126
11.7.4 Просмотр результирующей политики компьютера ... 127
11.8 Работа с группами сотрудников ... 129
11.8.1 Создание и редактирование групп сотрудников ... 129
11.8.2 Настройка состава групп сотрудников ... 131
11.8.3 Просмотр результирующей политики сотрудника ... 134
11.9 Работа с Агентами ... 135
11.9.1 Просмотр сведений об Агентах ... 135

Работа с данными в таблице ... 136
Состояния Агентов ... 138
11.9.2 Фильтрация записей ... 139
11.9.3 Перезагрузка компьютера ... 145
11.9.4 Обновление конфигурации ... 145
11.9.5 Диагностика Агентов ... 145
11.9.6 Установка статуса "Золотой образ" ... 147
11.9.7 Запуск и остановка Агентов ... 147
11.9.8 Удаление Агентов ... 148
11.9.9 Политики распространения ... 148
Работа с политиками ... 148
11.10 Работа с файловой статистикой ... 152
11.10.1 Настройка параметров конфигурации ... 152
11.10.2 Включение/исключение приложения из файловой статистики ... 153
11.10.3 Включение/исключение файлов с определенным расширением из перехвата ... 154
11.10.4 Включение/исключение файлов/папок, расположенных по определенному пути, из перехвата ... 154
12 ПОЛЬЗОВАТЕЛЬСКОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ... 155

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.

Кроме основных руководств для пользователей и администраторов Системы предусмотрена База знаний lk.infowatch.ru, которая включает материалы по устранению неисправностей и ответы на вопросы. В случае отсутствия доступа к Базе знаний, просьба обращаться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

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.

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 носителей
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, Яндекс Мессенджер, WhatsApp, MAX, протокол XMPP	• Правило контроля мессенджера VK • Правило контроля мессенджера Telegram • Правило контроля Яндекс Мессенджера • Правило контроля мессенджера WhatsApp • Правило контроля мессенджера MAX • Правило контроля протокола XMPP
Мониторинг ввода текста с клавиатуры	Правило мониторинга ввода текста с клавиатуры
Контроль систем передачи почтовых сообщений по протоколам SMTP, POP3, IMAP и HTTPS	Правило контроля почты

Название функции	Соответствующее правило политик безопасности
Контроль печати на компьютерах	Правило контроля печати
Мониторинг экрана компьютера	Правило мониторинга экрана
Мониторинг активности сотрудника и сбор статистики	Правило мониторинга активности сотрудника
Контроль файлов в приложениях	Правило контроля файлов в приложениях
Мониторинг звукового окружения	Правило мониторинга звукового окружения
Запись видео с экрана	Правило записи видео с экрана
Проксирование сетевого трафика	Правило проксирования сетевого трафика

Важно!

Для рабочих станций под управлением macOS доступны следующие функции контроля:

Название функции	Соответствующее правило политик безопасности
Контроль трафика, передаваемого по протоколам HTTP и HTTPS	Правило контроля HTTP(S)
Контроль печати на компьютерах	Правило контроля печати

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. "Настройки пароля")
Логин	Да	Имя учетной записи пользователя (правила см. "Настройки пароля"). Логин не зависит от верхнего или нижнего регистра
Пароль	Да	Пароль учетной записи (правила см. "Настройки пароля")
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. "Настройки пароля")
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:

- Настройки пароля
- Мониторинг состояния
- Интеграции

6.1 Настройки пароля

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

Поле	Описание
Лейбл (имя)	Лейбл и имя ноды в формате `лейбл(имя)`

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

* Если в одном из разделов Системы (например, `/opt/data`) остается 10 ГБ (или меньше) свободного пространства, появится сообщение о том, что превышено ограничение по использованию дискового пространства. Будут остановлены все интеграции.

Чтобы снять это ограничение, в **Настройки** → **Настройки системы** → **Состояние системы** определите ноду и раздел, в котором осталось мало пространства, и освободите его средствами ОС или продукта.

Все события мониторинга в Системе записываются в журнал.

Чтобы скачать весь журнал:

1. Для сбора данных по всем службам и активности пользователя нажмите **Экспорт диагностических данных** и дождитесь загрузки.
2. Скачайте zip-архив, содержащий txt-файлы с логами и csv-файл с данными активности пользователя.

Чтобы скачать диагностические данные отдельной службы:

1. В списке служб 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 Device Monitor и получения информации для распространения агентов необходимо настроить синхронизацию с Active Directory или Samba DC.

Важно!

Вы можете настроить Samba DC только как вторичный контроллер. Основным контроллером является Active Directory.

Настройка синхронизации с Samba DC идентична настройке синхронизации 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** → **Настройки системы** → **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 (Plain); • Защищенное соединение по протоколу LDAP + StartTLS; • Защищенное соединение по протоколу LDAPS (TLS). **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`

Параметр	Описание

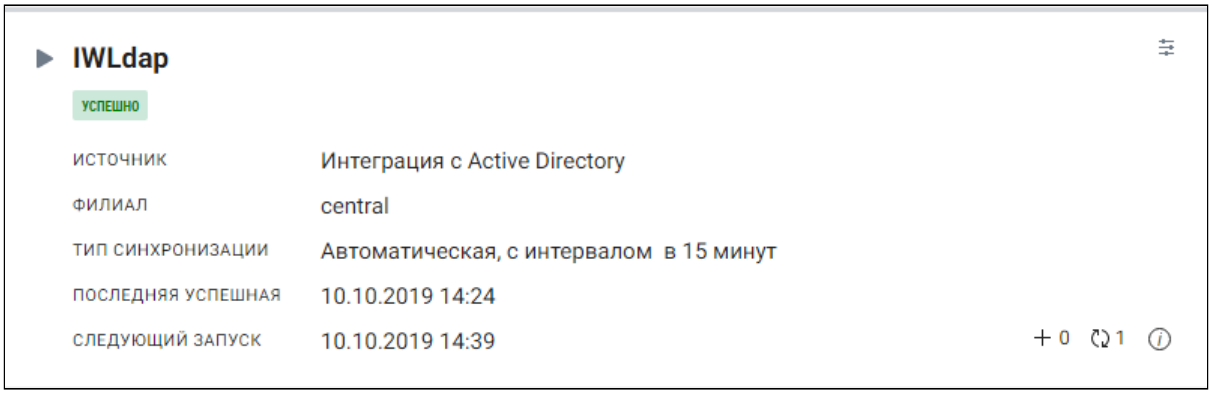
	`DC-domainComponent`
	`CN-commonName`
	Пример: Чтобы использовать в качестве базы поиска ветку `Users`, расположенную в домене компании, необходимо ввести: `cn=users,dc=company,dc=com`

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*
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. Нажмите ⋮ в правом верхнем углу и выберите **Редактировать**.
2. Внесите изменения.
3. Нажмите:
   - **Сохранить** – при этом синхронизация будет ожидать запуска;
     или
   - **Сохранить и синхронизировать**, чтобы запустить процесс синхронизации.
4. Если вы изменили ключевые параметры интеграции, например, **Адрес источника** или **LDAP-запрос**, то нажмите:
   - **Создать новую**, чтобы создать новую интеграцию с указанными настройками вместо текущей интеграции. Текущая интеграция будет удалена;
     или
   - **Продолжить в этой**, если требуется изменить настройки текущей интеграции.

Чтобы удалить интеграцию:

1. Нажмите ⋮ в правом верхнем углу.
2. Выберите **Удалить**, затем нажмите **Удалить**.

Примечание:

Данные, полученные в результате синхронизаций, не будут удалены после удаления интеграции.

7 Настройка Device Monitor

В этом разделе:

- Серверы
- Синхронизация
- Агенты
- Каналы перехвата
- Исключение приложений из перехвата
- Контроль сетевых ресурсов
- Отправка данных в продукты
- Диагностика событий
- Корпоративные сети
- Уведомления
- Универсальный перехватчик файлов
- Конфигурация

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.

Вы также можете отключить взаимодействие сервера Device Monitor с Traffic Monitor, переведя его в автономный режим.

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

1. Перейдите в раздел **Настройки** → **Device Monitor** → **Серверы**.
2. В области **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;
   - **Версия агента DM для установки и обновления** – 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*, *Политики распространения*).

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

Чтобы настроить параметры хранения и удаления событий:

1. Перейдите в раздел **Настройки** → **Device Monitor** → **Серверы**.
2. В области **Хранение событий** укажите:
   - **Удалять события в статусе "Отправлено в Traffic Monitor"** – чтобы удалять события, отправленные на сервер Traffic Monitor для последующего анализа. При этом события со статусами **Обработано** и **Отправлено в Traffic Monitor** 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 Traffic Monitor** 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.

> **Примечание:**
>
> При изменении параметра **Разделять по периодам** партиции с новыми параметрами будут создаваться в базе данных после того, как закончится период последней активной партиции событий. Пример:
>
> Если вы установили период 6 месяцев, а затем, спустя какое-то время, изменили его на 3 месяца, то эти изменения вступят в силу, когда закончится предыдущий установленный период – 6 месяцев.

Если параметры для удаления не отмечены, события со статусами **Обработано** и **Отправлено в Traffic Monitor** 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** → **Device Monitor** → **Серверы**.
2. В области **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 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.

Версия конфигурации, используемой в Traffic Monitor, отображается в Консоли управления Traffic Monitor (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** → **Device Monitor** → **Серверы**.
2. По умолчанию установлен только основной сервер Device Monitor. Выберите его в области **Серверы Device Monitor** , чтобы перейти в настройки.

   Примечание:

   Чтобы установить вспомогательный сервер Device Monitor, пройдите шаги *InfoWatch Device Monitor. Руководство по установке*, инструкции *Новая установка*.

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 Device Monitor.
     В качестве параметра `port` указывается порт сервера InfoWatch Traffic Monitor, через который будет о существляться доставка событий. По умолчанию, порт сервера InfoWatch Traffic Monitor – 9100;
   - **Токен Traffic Monitor** – токен для подключения к API, который указывается на этапе установки Device Monitor. Вы можете получить актуальный токен от администратора Traffic Monitor или сформировать токен самостоятельно в Консоли управления.
     Ниже будет отображен статус подключения к Traffic Monitor.
5. На вкладке **Подключение к Платформе** укажите:
   - **Адрес сервера Activity Monitor** – IP-адрес или имя сервера Activity Monitor. Возможные форматы записи: `host:port` .
     В качестве параметра `port` указывается порт сервера Activity Monitor (по умолчанию – 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**.
     Ниже будет отображен статус подключения к Платформе.
   - **Получение управляющих команд из Activity Monitor** – параметр для включения настройки взаимодействия между DM и Activity Monitor.

- **Адрес центральной ноды Платформы** – IP-адрес или имя сервера Платформы, откуда сервер DM будет получать команды Activity Monitor. Возможные форматы записи: `host:port`.
  В качестве параметра `port` указывается порт веб-интерфейса Платформы, через который сервер DM будет получать команды Activity Monitor. По умолчанию, порт веб-интерфейса Платформы – 443. Если не указать порт, будет использовано значение по умолчанию.
- **Токен Activity Monitor** – токен для подключения к API Activity Monitor. Вы можете получить актуальный токен в разделе "Основные настройки" Activity Monitor (подробнее см. *InfoWatch Activity Monitor. Руководство администратора. Основные настройки*).

6. Если требуется установить соединение с другим сервером Traffic Monitor или Платформы, перейдите на нужную вкладку и измените адрес сервера и токен.
7. Нажмите **Сохранить**.

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*. Если сертификат не прошел проверку, то статус подключения будет иметь значение *Ошибка проверки сертификата*.

Чтобы перевести сервер Device Monitor в автономный режим:

1. Перейдите в раздел **Настройки** → **Device Monitor** → **Серверы**.
2. В области **Отправка событий в Traffic Monitor** активируйте переключатель **Автономный режим работы сервера**.
   Учитывайте, что после переключения в автономный режим:
   - Из базы данных сервера Device Monitor будут удалены все события, которые относятся к Traffic Monitor, включая теневые копии файлов. События буду удалены на следующие сутки в 01:00;
   - Сервер не будет сохранять новые события Traffic Monitor;
   - Переключение в автономный режим влияет только на взаимодействие с Traffic Monitor. Взаимодействие с остальными продуктами не поменяется.

7.2 Синхронизация

> **Важно!**
>
> Синхронизацию нельзя создавать/запускать/редактировать, если вы или другой офицер безопасности вносите изменения в конфигурацию в разделе **Группы** Центра администрирования при включенном запрете синхронного редактирования. Кнопки изменения будут недоступны. В верхней части экрана станет доступна информация о редактировании конфигурации.
>
> Подробнее о запрете синхронного редактирования см. "Режимы редактирования конфигурации".

Чтобы получать информацию о компьютерах или сотрудниках из службы каталогов, в разделе **Настройки** → **Device Monitor** → **Синхронизация** 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. В случае настройки синхронизации на сервере под управлением ОС Astra Linux, отредактируйте конфигурационный файл LDAP-клиента и перезапустите сервис веб API. Для этого выполните команды в терминале:

```
echo "TLS_CACERT /etc/ssl/certs/ca-certificates.crt" > /etc/ldap/ldap.conf
systemctl restart iwdms_webapi
```

2. Перейдите в раздел **Настройки** → **Device Monitor** → **Синхронизация**.
3. В верхней правой части рабочей области нажмите **Добавить**.
4. 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*
Безопасность соединения	Уровень безопасности соединения. Возможные значения: • *STARTTLS*[1] • *LDAPS*[2] • *Kerberos*[3] • *Без защиты* (по умолчанию) **Примечание:** [1] Для работы с уровнем безопасности STARTTLS необходимы дополнительные настройки. Обратитесь к специалистам технической поддержки компании InfoWatch или партнера, у которого вы приобрели продукт. На сервере Device Monitor, установленном с поддержкой контейнеризации, синхронизация с уровнем безопасности STARTTLS не поддерживается. [2] В случае, если сервер Device Monitor был установлен с поддержкой контейнеризации, для работы с уровнем безопасности LDAPS необходимо:

Параметр	Описание
	a. Перед созданием синхронизации импортировать корневые сертификаты по пути `/opt/iw/dmserver/cert`. b. После установки сертификата обязательно перезапустить службу `webapi`: `systemctl restart iwdms_webapi` [3] Для работы с уровнем безопасности Kerberos: • Подготовьте сервер для работы с Kerberos, как описано в *InfoWatch Device Monitor. Руководство по установке. Подготовка окружения*. • Обратите внимание на чувствительность к регистру логина для доступа к серверу синхронизации (см. описание ниже в таблице).
Порт	Порт для подключения к серверу синхронизации. Вы можете выбрать одно из предустановленных значений: *389* или *636*, либо ввести значение вручную
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 * ( ) . & - _ [ ] ` ~ | @ $ % ^ ? : { } ! '

Параметр	Описание
	• 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 Если вы выбрали уровень безопасности Kerberos, для доменной части логина используйте заглавные буквы. Например: *user@EXAMPLE.RU*
Пароль	Пароль учетной записи для доступа к серверу синхронизации. Поле обязательно к заполнению
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.

5. Нажмите **Проверить соединение**, чтобы проверить полноту и корректность введенных параметров, и дождитесь сообщения "*Соединение успешно установлено*".
6. Нажмите **Применить**.

Чтобы запустить синхронизацию:

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

> **Примечание:**
>
> В случае ошибки синхронизации на РЕД ОС 8, убедитесь, что при подготовке сервера к установке Device Monitor вы установили пакет `openldap-compat`. В противном случае установите его. Подробнее см. *InfoWatch Device Monitor for Linux. Руководство по установке. Подготовка окружения*.

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 Исключение приложений из перехвата

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

Чтобы просмотреть и настроить параметры исключения приложений из перехвата:

1. В главном меню выберите **Настройки → Device Monitor → Исключение приложений из перехвата**.
2. Исключение приложений на рабочих станциях под управлением разных ОС настраивается на разных вкладках. Откройте вкладку с названием соответствующего семейства ОС: **Windows**, **Linux**, **macOS**.
3. В левой части рабочей области нажмите .
4. Следуйте инструкциям для выбранной ОС:
   - **Для ОС Windows:**
     a. Введите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.
     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. пп. *d*, *f*).

b. В поле **Описание** введите произвольное описание приложения.
c. В поле **Тип перехвата** отметьте:
   - **Исключить приложение из сетевого перехвата** – если требуется исключить сетевую активность приложения из перехвата;
   - **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.

d. В поле **Путь** 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 в любой ее подпапке.
e. В поле **Исходное имя файла** укажите название приложения (в контекстном меню исполняемого файла приложения выберите **Свойства**, вкладка **Подробно**, атрибут **Исходное имя файла**).
f. 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`".

- **Для поддерживаемых ОС семейства Linux:**

a. Введите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.
   Вместо имени приложения можно ввести символ `*`. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути (см. п. *d*).
b. Введите краткое описание. Поле обязательно для заполнения.
c. Укажите ОС, для которой настраивается исключение. Чтобы исключение работало на всех поддерживаемых ОС семейства Linux, выберите вариант **Любой дистрибутив Linux**.
d. 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 в папке `myapps`, а также в любой ее подпапке.

- **Для macOS:**

  a. Введите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.
  Вместо имени приложения можно ввести символ *. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути (см. п. *c*).
  b. В поле **Описание** введите произвольное описание приложения.
  c. В поле **Путь** 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: `/opt/myapps`, то из перехвата будут исключены все приложения в папке `myapps`, а также в любой ее подпапке.

5. Нажмите **Добавить**.
6. Нажмите **Применить**.

> **Важно!**
>
> Чтобы применить исключение приложения из перехвата или отмену такого исключения, перезапустите приложение.

Чтобы отредактировать настройку исключения:

1. В конце строки настройки нажмите  и выберите **Редактировать**.
2. Внесите изменения и нажмите **Сохранить**.
3. Нажмите **Применить**.

Чтобы удалить настройку исключения:

1. В конце строки настройки нажмите  и выберите **Удалить**.
2. Подтвердите действие в диалоговом окне.
3. Нажмите **Применить**.

Чтобы удалить сразу несколько настроек:

1. Установите флажки в строках настроек, которые требуется удалить.
2. На панели внизу нажмите . Чтобы сбросить выделение, нажмите .
3. Нажмите **Применить**.

7.4 Универсальный перехватчик файлов

Система использует добавленные профили приложений для перехвата операций чтения и записи файлов приложениями, а также блокирования этих операций по политикам Traffic Monitor.

Информация о профилях приложений автоматически синхронизируется с Traffic Monitor. Подробнее о настройке соответствующих правил Traffic Monitor см. *InfoWatch Traffic Monitor. Руководство пользователя. Правило файловых операций*.

Важно!

Блокировка операций чтения и записи файлов по политикам Traffic Monitor доступна только на агентах под управлением поддерживаемых ОС семейства Linux и только начиная с версии Device Monitor 7.20.4.

Примечание:

Если в течение 30 секунд осуществлено несколько операций с файлом, Система фиксирует их в одном событии перехвата. При этом в случае настроенной блокировки Система заблокирует каждую попытку операции с файлом в течение этого времени.

Чтобы импортировать профиль приложения:

1. Перейдите в раздел **Настройки** → **Device Monitor** → **Универсальный перехватчик файлов**.
2. Перейдите во вкладку **Приложения**.
3. Нажмите кнопку **Импорт** и в открывшемся окне выберите профиль приложения формата `.xml`.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Примечание:

Для получения необходимого профиля обратитесь к специалистам компании InfoWatch.

Чтобы удалить профиль приложения:

1. Нажмите  у необходимого профиля приложения и выберите пункт **Удалить**.
2. Подтвердите действие, нажав **Удалить**.
3. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Важно!

Удаленный профиль приложения не может быть использован при настройке политик в Traffic Monitor. Если он использовался в политике ранее, она будет повреждена.

Чтобы отредактировать настройки перехвата приложения:

1. Нажмите  у необходимого профиля приложения и выберите пункт **Редактировать**.
2. В открывшемся окне внесите необходимые изменения в настройки:

Название параметра	Описание
Исполняемые файлы	Исполняемые файлы, которые буду перехвачены. Файлы изменить нельзя

Название параметра	Описание
Перехватывать все файлы, кроме тех, что соответствуют одному из следующих исключений	
Файлы с расширением	Перечисление расширения файлов. Разделитель между расширениями – "**;**", перенос строки недопустим
Файлы, расположенные по пути	Указание пути к файлам. • допускается использование масок • разделителем служит "**;**", перенос строки недопустим • путь должен начинаться со стандартного символа разделения элементов пути на файловой системе "\", либо со спецсимвола (например, "*****") • исключаемые пути должны задавать относительный путь к файлу, то есть имена дисков недопустимы
Вне зависимости от настроек исключений, всегда перехватывать файлы, соответствующие одному из следующих критериев	
Файлы с расширением	Перечисление расширения файлов. Разделитель между – расширениями "**;**", перенос строки недопустим
Файлы, расположенные по пути	Указание пути к файлам. • допускается использование масок • разделителем служит "**;**", перенос строки недопустим • путь должен начинаться со стандартного символа разделения элементов пути на файловой системе "\", либо со спецсимвола (например, "*****") • включаемые пути должны задавать относительный путь к файлу, то есть имена дисков недопустимы

3. После внесения изменений нажмите **Сохранить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы отредактировать настройки перехвата профиля ОС:

1. Перейдите во вкладку **Общие настройки**.
2. Выберите необходимый профиль ОС и нажмите  **Редактировать**.
3. В открывшемся окне внесите необходимые изменения в настройки:

Название параметра	Описание
Перехватывать все файлы, кроме тех, что соответствуют одному из следующих исключений	
Файлы с расширением	Перечисление расширения файлов. Разделитель между расширениями "**;**", перенос строки недопустим. Значения по умолчанию: **ОС Windows** .000;.386;.ADV;.ANI;.ANN;.AUTOMATICDESTINATIONS-MS;.BCD;.BIN;.BIO;.BK1;.BK2;.BMK;.BUD;.CAB;.CAT;.CHG;.CHS;.CHT;.CI;.CLB;.CNT;.CPI;.CPL;.CUR;.CUSTOMDESTINATIONS-MS;.DAT;.DESKLINK;.DESKTHEMEPACK;.DEV;.DEVICEMETADATA-MS;.DIT;.DLL;.DMP;.DRV;.EBD;.ETL;.EVT;.EVTX;.EXE;.FFA;.FFL;.FFO;.FFX;.FID;.GRL;.GROUP;.GRP;.H1S;.HDMP;.HHC;.HHK;.HIV;.HLP;.HPJ;.HSH;.HVE;.ICL;.ICN;.ICO;.ICONPACKAGE;.IDX;.IME;.INF;.INF_LOC;.INI;.ITEMDATA-MS;.JS;.JOB;.JPN;.KBD;.KOR;.LIBRARY-MS;.LNK;.MANIFEST;.MBR;.MDMP;.MEM;.MLC;.MSC;.MSI;.MSP;.MSSTYLE;.MSSTYLES;.MTZ;.MUI;.MUM;.NFO;.NLS;.NT;.NTFS;.PDR;.PFX;.POL;.PPD;.PPM;.PRF;.PRINTEREXPORT;.PS1;.PS2;.PWL;.REG;.REGLNK;.REGTRANS-MS;.RS;.SCF;.SCR;.SEARCHCONNECTOR-MS;.SHD;.SPL;.SPX;.STR;.SWP;.SYS;.THEME;.TRX_DLL;.UCE;.VGA;.VX_;.VXD;.WDF;.WER;.WSF;.WSH;.XRM-MS;.ZONE.IDENTIFIER;.URL **ОС Astra Linux** .so;.o;.ko;.a Для РЕД ОС и ОС Альт значение по умолчанию пустое
Файлы, расположенные по пути	Указание пути к файлам. • допускается использование масок • разделителем служит "**;**", перенос строки недопустим • путь должен начинаться со стандартного символа разделения элементов пути на файловой системе "\", либо со спецсимвола (например, "*****") • исключаемые пути должны задавать относительный путь к файлу, то есть имена дисков недопустимы Значения по умолчанию: **ОС Windows** \Recovery\;\System Volume Information\;\MSOCache\;\Windows\;\Program Files\;\Program Files (x86)\;\Users\\AppData\;\ShaderCache\ **ОС Astra Linux** /etc/\;/lib/\;/usr/lib/\;/usr/share/\;/.genisoimagerc\;/.mkisofsrc\;/tmp/*\ Для РЕД ОС и ОС Альт значение по умолчанию пустое

Название параметра	Описание
Вне зависимости от настроек исключений, всегда перехватывать файлы, соответствующие одному из следующих критериев	
Файлы с расширением	Перечисление расширения файлов. Разделитель между – расширениями "**;**", перенос строки недопустим Значение по умолчанию пустое для всех ОС
Файлы, расположенные по пути	Указание пути к файлам. • допускается использование масок • разделителем служит "**;**", перенос строки недопустим • путь должен начинаться со стандартного символа разделения элементов пути на файловой системе "\", либо со спецсимвола (например, "*****") • включаемые пути должны задавать относительный путь к файлу, то есть имена дисков недопустимы Значение по умолчанию пустое для всех ОС

4. После внесения изменений нажмите **Сохранить**.
5. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

7.5 Каналы перехвата

Задайте параметры перехвата:

Чтобы настроить периодичность получения событий с теневыми копиями чата для правила *Контроль мессенджеров*:

1. В главном меню Консоли управления выберите **Настройки** → **Device Monitor** → **Каналы перехвата**.
2. Укажите, через сколько минут после начала общения в чате необходимо создать теневую копию.
3. Укажите 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 *Мониторинг ввода текста с клавиатуры*, укажите:

1. Через сколько секунд после остановки ввода с клавиатуры пользователем необходимо создать событие.
2. Минимальное количество символов, введенное пользователем и достаточное для создания события;
3. 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[1], укажите:

1. Качество, размер и цвет снимков, которые необходимо создавать:
   - низкое, минимальный, цветной;
   - среднее, минимальный, оттенки серого;
   - высокое, максимальный, цветной.
2. На сколько изменять размер снимка (в %, значение по умолчанию – 80%).
3. Период от 120 до 1200 секунд, по истечении которого не требуется создавать снимок экрана (значение по умолчанию – 120 секунд).
4. Если нужно создавать снимок только активного окна[2] [3].

Важно!

[1] Если на диске недостаточно свободного места, автоматические снимки экрана не создаются.

[2] Если настройка **Создавать снимок только активного окна** отмечена, снимки экрана, полученные на рабочих станциях под управлением ОС Альт 11 с графической оболочкой Wayland, будут содержать черную рамку.

На рабочих станциях под управлением других ОС семейства Linux поддерживается только создание снимка всего экрана.

[3] Если при выбранной настройке **Создавать снимок 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.

Чтобы настроить параметры записи звукового окружения при срабатывании правила, в поле **Аудиозапись** укажите:

1. Продолжительность ведения записи в минутах. Минимальное значение – 1, максимальное – 120. Значение по умолчанию – 5 минут.

Примечание:

Когда сотрудник использует ресурс, указанный в правиле мониторинга звукового окружения, Device Monitor записывает звуковое окружение рабочей станции непрерывно в течение заданного в настройках периода. По его окончании, Система прекращает аудиозапись. Если сотрудник пользовался несколькими ресурсами, заданными в правиле, то при переключении с одного ресурса на другой Device Monitor сбрасывает таймер и начинает отсчет заново.

Пример 1

В правиле указаны ресурсы, при посещении которых необходимо вести запись звукового окружения: https://example.ru/, https://example.com. Задана продолжительность ведения записи – 5 минут.

Сотрудник переходит на ресурс https://example.ru/, Система начинает аудиозапись. Через 3 минуты сотрудник покидает этот ресурс и переходит на https://example.com, также контролируемый правилом. Система продолжает вести запись звукового окружения, при этом заново начав отсчет интервала в 5 минут.

По истечении 5 минут использования ресурса Device Monitor завершает запись и отправляет события в Activity Monitor. В результате для этого сотрудника в AM будет создано событие о посещении 2 ресурсов продолжительностью 8 минут.

Пример 2

В правиле указаны ресурсы, при посещении которых необходимо начинать вести запись звукового окружения: https://example.ru/, https://example.com. Задана продолжительность ведения записи – 5 минут.

Сотрудник использует ресурс https://example.ru/, а через 3 минуты переходит на https://example1.ru/ (не включен в список контролируемых ресурсов) и пользуется им в течение 1 минуты. Device Monitor ведет запись звукового окружения.

Затем сотрудник возвращается на контролируемый ресурс https://example.ru/. Device Monitor обновляет таймер записи звукового окружения для этого ресурса. По истечении 5 минут Система завершает запись. В результате в Activity Monitor для этого сотрудника будет сформировано событие о посещении 1 ресурса продолжительностью 9 минут.

Пример 3

В правиле указаны ресурсы, при посещении которых необходимо начинать вести запись звукового окружения: https://example2.ru/, https://example2.com. Задана продолжительность ведения записи – 120 минут.

Сотрудник использует ресурс https://example2.ru/ в течение 20 минут, затем переходит на https://example.ru/ (не включен в список контролируемых ресурсов) и пользуется им в течение 10 минут. Все это время Device Monitor ведет запись звукового окружения.

Затем сотрудник переходит на контролируемый ресурс https://example2.com/. Device Monitor обновляет таймер записи звукового окружения для этого ресурса. По истечении 120 минут Система завершает запись. В результате в Activity Monitor для этого сотрудника будет сформировано событие о посещении 2 ресурсов продолжительностью 150 минут.

2. Чтобы Система не вела запись в периоды тишины, включите настройку **Записывать только при наличии речи**. При активации этой настройки, Device Monitor отправляет в Activity Monitor только события с распознанным человеческим голосом.

   Важно!

   Для применения настройки, выйдите из Системы и зайдите в нее снова.

   Подробнее об аудиозаписи см. *Правило мониторинга звукового окружения*.

Чтобы настроить продолжительность ведения видеозаписи экрана при срабатывании правила, укажите значение в поле **Видео экрана**.

Значение задается в минутах. Минимальное значение – 1, максимальное – 120 (значение по умолчанию – 5 минут).

Примечание:

Device Monitor записывает видео с экрана рабочей станции непрерывно в течение заданного в настройках периода. В момент, когда сотрудник начал использовать ресурс, указанный в правиле записи видео с экрана, Device Monitor запускает запись экрана рабочей станции. По окончании периода, заданного в настройках, Система прекращает видеозапись. Если сотрудник пользовался несколькими ресурсами, включенными в данное правило, то при переключении с ресурса на ресурс Device Monitor сбрасывает таймер и начинает отсчет заново.

Важно!

При работе с агентами версий 7.20 и более ранних в качестве настройки продолжительности ведения записи звукового окружения и видеозаписи экрана рабочей станции используется только **Аудиозапись**.

Пример

На сервере установлен Device Monitor версии 7.21, на агенте – 7.20. На агент распространяются правила мониторинга звукового окружения и записи видео с экрана.

В настройках выставлены значения продолжительности:

- для **Аудиозаписи** – 2 минуты;
- для **Видеозаписи** – 3 минуты.

При срабатывании обоих правил записи и для видео с экрана, и для звукового окружения будут длиться по 2 минуты.

Для перехвата веб-почты VK+ задайте хосты. Подробнее см. "Хосты для VK+".

7.5.1 Хосты для VK+

Для перехвата веб-почты VK+ необходимо задать хосты (о настройке перехвата веб-почты см. "Правило контроля почты"). Это можно сделать на вкладке **Хосты для VK+** раздела **Настройки** → **Device Monitor** → **Каналы перехвата**.

Чтобы добавить хост:

1. Справа вверху нажмите 

.
2. Введите имя хоста в формате *<схема>:<хост>*, например, *address.ru:15101* или *10.60.3.8:15101*.
3. Нажмите **Добавить**.

Чтобы отредактировать хост:

1. Напротив хоста нажмите , затем  **Редактировать**.
2. В окне редактирования внесите правки и нажмите **Сохранить**.

Чтобы удалить хост:

1. Напротив хоста нажмите , затем  **Удалить**.
2. В открывшемся окне подтвердите действие, нажав **Удалить**.

7.6 Контроль сетевых ресурсов

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(S)
- POP3
- SMTP
- S/MIME
- HTTP(S)
- XMPP
- 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. В главном меню выберите **Настройки → Device Monitor → Контроль сетевых ресурсов**.
2. Нажмите ⊞ или **+ Добавить настройку**.
3. В диалоговом окне **Добавление сервера в список исключенных из анализа** введите описание сервера:
    - чтобы добавить *отдельный порт сервера*:
        a. Выберите нужное действие: **Исключать** или **Перехватывать**;
        b. Добавьте **Описание**;
        c. В поле **Тип адресов** выберите **Адрес и порт**;
        d. Укажите FQDN или IP-адрес (IPv4 или IPv6) сервера;
        e. В поле **Порт** укажите порт подключения (может быть пустым).
    - чтобы добавить *диапазон адресов*:
        a. Выберите нужное действие: **Исключать** или **Перехватывать**;
        b. Добавьте **Описание**;
        c. В поле **Тип адресов** выберите **Диапазон адресов**;
        d. 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 **Исключать**;
        b. В поле **Тип адресов** 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  **Редактировать**. После внесения изменений нажмите **Сохранить**, затем **Применить**.

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

7.7 Уведомления

Если на контролируемом компьютере сотрудник пытается выполнить действие, запрещенное политикой безопасности, ему отображается уведомление о запрете.

В зависимости от ОС на компьютере, где установлен Агент Device Monitor, отображаются следующие уведомления:

Тип уведомления	Причина отправки уведомления	ОС Windows	ОС Linux
Запрет доступа к устройству	Сработало правило, запрещающее чтение и запись на устройство (см. "Правило контроля съемных носителей").	+	+
Запрет записи на устройство	Сработало правило, запрещающее запись на устройство (см. "Правило контроля съемных носителей").	+	+
Запрет записи в открытую область	Сработало правило, запрещающее запись на незашифрованные флоппи-дисководы и съемные устройства (см. "Правило контроля съемных носителей").	+	-
Запрет копирования/ печати файла, если места для событий недостаточно	Если Агент Device Monitor настолько долго не имел связи с сервером, что закончилось место, выделенное для хранения информации о событиях, контролируемых правилами (30000 событий), а в общих настройках работы агентов для такого случая выбрано **Запрещать операции** (подробнее см. "Агенты"), то запрещаются любые операции, контролируемые текущей политикой безопасности.	+	-
Запрет вставки из буфера обмена при		+	-

Тип уведомления	Причина отправки уведомления	ОС Windows	ОС Linux
нехватке места для событий			
Запрет передачи данных по сетевым протоколам, если места для событий недостаточно		+	-
Запрет передачи данных по сетевым протоколам	Сработало правило, запрещающее обмен данными по сетевому протоколу FTP(S), почте и в мессенджерах (см. "Правило контроля FTP", "Правило контроля почты", "Правило контроля протокола XMPP" и др.).	+	+
Запрет передачи данных по сетевым протоколам при срабатывании политики защиты данных	Отображается при блокировании передачи данных по почтовым протоколам, FTP, HTTP(S) в результате применения политики защиты данных Traffic Monitor.	+	+
Запрет использования буфера обмена при срабатывании политики защиты данных	Отображается при блокировании копирования текста в результате применения политики защиты данных Traffic Monitor.	+	-
Запрет печати при срабатывании политики защиты данных	Отображается при блокировании копирования файла на принтер в виде задания на печать в результате применения политики защиты данных Traffic Monitor.	+	-

Тип уведомления	Причина отправки уведомления	ОС Windows	ОС Linux
Запрет копирования файла на съемное устройство при срабатывании политики защиты данных	Отображается при блокировании копирования файла на съемное устройство в результате применения политики защиты данных Traffic Monitor.	+	+
Запрет доступа к облачному хранилищу	Сработало правило, контролирующее использование веб-клиентов облачных хранилищ (см. "Правило контроля облачных хранилищ", настройка **Запретить доступ**).	+	+
Запрет записи в облачное хранилище	Сработало правило, контролирующее использование веб-клиентов облачных хранилищ (см. "Правило контроля облачных хранилищ", настройка **Разрешить только скачивание**).	+	+
Запрет снимка экрана	Сработало правило, контролирующее создание снимков экрана (см. "Правило контроля создания снимков экрана").	+	+
Запрет копирования файла на сетевой ресурс	Сработало правило, запрещающее копирование файла на сетевые ресурсы (см. "Правило контроля сетевых ресурсов").	+	-
Запрет записи файла при срабатывании политики защиты данных	Отображается при блокировании записи или чтения файла заданного профиля (см. "Правило контроля файлов в приложениях").	+	+
Запрет чтения файла при срабатывании политики защиты данных		+	+

Чтобы полностью отключить отображение уведомлений сотрудникам или включить его обратно:

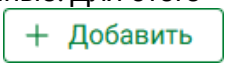
1. В Центре Администрирования перейдите в раздел **Настройки** → **Device Monitor** → **Агенты**.

2. Снимите флажок с поля **Показывать уведомления сотруднику** – чтобы отключить отображение уведомлений сотрудникам, или установите его – чтобы включить уведомления.
3. Справа вверху нажмите **Применить.**

Вы можете изменить текст уведомлений, а также отключить отображение любого типа уведомлений, или включить отображение обратно.

> **Важно!**
>
> Если вы отключили уведомления способом, описанным выше, то уведомления, включенные способом, описанным далее, отображаться не будут.

Чтобы изменить текст уведомлений или включить/отключить отдельные уведомления:

1. В Центре Администрирования, перейдите в раздел **Настройки** → **Device Monitor** → **Уведомления**.
2. Из раскрывающегося списка **Тип уведомления** выберите тот, который вы хотите настроить.
3. Чтобы включить/отключить отображение выбранного типа уведомлений, установите/снимите флажок **Показывать сотруднику уведомление системы**.
4. В поле **Текст уведомления** задайте текст уведомления.
   В сообщении вы можете использовать переменные, которые при выводе сотруднику будут преобразовываться в актуальные данные: например, тип заблокированного устройства или протокол, по которому сотрудник пытался передать данные. Для этого установите курсор в необходимое место текста уведомления, нажмите 

   и в раскрывшемся списке выберите необходимую переменную.

   Чтобы отменить внесенные изменения, нажмите .

   Чтобы вернуть системный текст уведомления, нажмите .

   > **Примечание:**
   >
   > По умолчанию текст уведомлений – на том языке, который был выбран при установке сервера Device Monitor. При смене языка веб-интерфейса язык текста уведомлений не изменяется.

5. После того, как изменения для выбранного типа уведомления внесены, справа вверху нажмите **Сохранить**.
6. При необходимости, измените настройки для других типов уведомлений, повторяя шаги 2-5.

7.8 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 **Настройки** → **Device Monitor** → **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	
Критический остаток места на диске	Минимальный размер свободного пространства (ГБ) на контролируемом компьютере, при достижении которого теневые копии не будут создаваться. Значение по умолчанию 10 ГБ.
Порог предупреждения	При достижении этого порога (ГБ) система с помощью цветовой индикации будет указывать, что скоро может закончиться место на диске, необходимое системе для бесперебойной работы по созданию теневых копий. Значение по умолчанию 20 ГБ.
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	

Параметр	Описание
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, Кб/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.
Поведение Агента на компьютере	
Скрывать присутствие агента на компьютере	Признак того, что Система будет скрывать присутствие Агента на компьютерах. Если данная настройка не отмечена, в области уведомлений панели задач Windows на компьютере, где установлен Агент, будет отображаться значок . При нажатии на этот значок будет доступна информация о работе Агента, а также список контролируемых в данный момент устройств. **Важно!** Если на контролируемом компьютере включена антивирусная защита, то антивирус может выявлять работу Device Monitor: например, в списке процессов, запущенных на контролируемом компьютере или в списке программ, инициирующих контроль.

Параметр	Описание
	Примечание: Поддерживается для агентов под управлением ОС Windows.
Показывать уведомления сотруднику	Если флажок установлен, то сотрудник будет получать уведомление, когда пытается выполнить действие, запрещенное политикой безопасности. Отображение отдельных типов уведомлений вы можете настроить в разделе Уведомления.

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**.

7.9 Корпоративные сети

Чтобы не создавать события для запросов на внутренние ресурсы при работе правила контроля HTTP(S)-трафика, вы можете исключить сегменты корпоративной сети. Для этого:

1. Перейдите в раздел **Настройки** → **Device Monitor** → **Корпоративные сети**.
2. В верхней правой части рабочей области нажмите **Добавить**.
3. В открывшемся окне укажите:
   - Название сети;
   - Адрес подсети в формате CIDR, например:
     - `182.0.7.1/21` (протокол IPv4)
     - `2001:4f8:3:ba::/64` (протокол IPv6).
4. Нажмите **Добавить**.

> **Примечание:**
>
> Если задать сегменты, в параметрах агентов под управлением ОС Windows будет некорректно отображаться информация о нахождении адаптеров в корпоративной сети.

7.10 Отправка данных в продукты

В разделе **Настройки → Device Monitor → Отправка данных в продукты** вы можете указать, в какие продукты InfoWatch необходимо отправлять данные.

7.10.1 Отправка событий в Traffic Monitor и Платформу

1. В области **Настройка отправки в Traffic Monitor** снимите флаг, если вы не хотите:
   - **Отправлять события с автоматическими снимками экрана**;
   - **Отправлять события с текстом по правилу контроля ввода текста с клавиатуры**;
   - **Отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры** (настройка доступна, если включена отправка событий с текстом по этому правилу);
2. В области **Настройка отправки в Платформу** снимите флаг, если вы не хотите:
   - **Отправлять события с автоматическими снимками экрана**;
   - **Отправлять события с текстом по правилу контроля ввода текста с клавиатуры**;
   - **Отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры** (настройка доступна, если включена отправка событий с текстом по этому правилу);
   - **Отправлять события использования/подключения устройств**.

> **Примечание:**
>
> Настройки контроля событий производятся в правилах:
>
> - Правило мониторинга экрана
> - Правило мониторинга ввода текста с клавиатуры
> - Правило мониторинга активности сотрудника
>
> Чтобы события использования/подключения устройств отображались в InfoWatch Activity Monitor:
>
> - В **Настройках** в разделе **Агенты** для параметра **Логировать события от перехватчика устройств и облачных хранилищ** задайте значение *Логировать всегда* или *При отказе в доступе*. См. "Агенты".
> - Настройте правило контроля съемных носителей.

Отправка событий в Activity Monitor напрямую с агентов

Чтобы события активности пользователя (работа в приложениях и на веб-сайтах, ввод текста с клавиатуры, использование мыши и пр.) отправлялись в Activity Monitor напрямую с агентов, а не через сервер **Device Monitor**, в области **Настройка отправки с агента в Activity Monitor** активируйте переключатель **Отправлять события напрямую** и укажите параметры:

- **Адрес сервера** – адрес сервера Activity Monitor. Если не задать порт, по умолчанию используется номер порта 11008;

- **Токен** – токен сервера Activity Monitor. Вы можете получить актуальный токен в консоли управления Центра расследований, в разделе **Основные настройки** в поле **Токен для Device Monitor Server**;
- **Отправлять события каждые...** – интервал между отправками событий с агента в секундах;
- **Максимальное количество одновременно отправляемых событий** – можно задать значение не более 1000.

Если требуется, снимите флажок **Не разрывать связь после установки соединения**.

Важно!

Отправка событий в Activity Monitor напрямую возможна только с агентов под управлением ОС Windows.

Одновременное использование прямой (с агента в Activity Monitor) и непрямой (через сервер Device Monitor в Activity Monitor) отправки событий строго не рекомендуется, так как это может привести к следующему сценарию:

Если акаунт одной и той же персоны будет использован на агентах с разными настройками отправки событий:

- агент на ОС Windows, на котором настроена прямая отправка,
- и агент на ОС Linux, где работает только непрямая отправка,

то в этом случае события персоны с агента на ОС Linux не поступят в Activity Monitor.

Рекомендуется учитывать данный сценарий при планировании поступления данных с агентов, работающих как на ОС Windows, так и на ОС Linux, а так же агентов с версией без поддержки прямой отправки (например, агентов старых версий – 7.14 и более ранних).

При включении отправки событий напрямую необходимо изменить эту настройку одновременно (в течение короткого времени) **на всех** серверах Device Monitor, данные с которых передаются на сервер Activity Monitor. Впоследствии не рекомендуется возвращать настройку в исходное состояние (отправки через сервер Device Monitor), так как это потребует дополнительных изменений.

В случае, если это все же необходимо, выполните следующие шаги:

1. Запретите получение данных напрямую на сервер Activity Monitor, закрыв порт TCP 11008 (опциональное действие). Подробнее о настройке сетевых соединений см. *InfoWatch Activity Monitor. Руководство по установке. Настройка сетевых правил доступа.*
2. Отключите настройку прямой отправки в Device Monitor.
3. На каждой ноде Activity Monitor в кластере удалите из Clickhouse данные, которые были сформированы при прямой отправке, с помощью команд:

```
kubectl scale deployment --replicas=0 datacollector-NODENAME -n infowatch
crictl exec -it $(crictl ps | grep click | awk '//{print $1;}') clickhouse-client --user default
truncate table datacollector.activityMonitorObjects
kubectl scale deployment --replicas=1 datacollector-NODENAME -n infowatch
```

где NODENAME – имя ноды Activity Monitor в кластере.

После очистки таблицы список сотрудников в разделе “Наблюдение” также будет сброшен – до появления первого события у персоны.

При выборе отправки статистики напрямую в Activity Monitor не будет формироваться тип активности *Смешанная*. Подробнее о типах активности см. "*InfoWatch Activity Monitor. Руководство администратора. Настройки продукта. Справочники. Типы активности*".

7.10.2 Пример настроек отправки данных

Для рабочей станции настроены правила:

- правило контроля ввода текста с клавиатуры, в рамках которого включена опция Создавать снимок экрана при создании события.
- правило мониторинга активности сотрудника. Выбран сбор статистики активности.

Также заданы настройки:

- **Настройка отправки в Traffic Monitor** – не отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры;
- **Настройка отправки в Платформу** – отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры;
- **Настройка отправки с агента в Activity Monitor** – отправлять события напрямую в Activity Monitor.

Результат при наступлении события:

- в Traffic Monitor снимки экрана не отправляются;
- в Платформу снимки экрана отправляются;
- события активности пользователя отправляются агентом напрямую в Activity Monitor.

7.11 Конфигурация

В разделе **Настройки** → **Device Monitor** → **Конфигурация** вы можете:

- экспортировать/импортировать конфигурацию
- настроить время для автоматического сброса несохраненных изменений конфигурации

Чтобы экспортировать конфигурацию:

1. Нажмите **Экспорт** .
2. В открывшемся окне выберите  элементы для экспорта и нажмите **Экспортировать**.
3. Файл архива конфигурации будет сохранен в папку **Загрузки** вашего компьютера.

Чтобы импортировать конфигурацию:

1. Нажмите **Импорт** .
2. В открывшемся окне перетащите файл конфигурации в поле или выберите файл на компьютере.
3. Выберите  элементы для импорта и нажмите **Импортировать**.
4. Нажмите **Импортировать**.
   В результате в Систему будут добавлены элементы из файла конфигурации. Старые элементы при этом не будут удалены. При совпадении имен, к имени импортированного элемента будет добавлено число, например, "*Политика на устройства (1)*".
   Дубликаты компьютеров и сотрудников созданы не будут.

Вы можете экспортировать/импортировать следующие элементы конфигурации:

- **Схема безопасности**
  При выборе схемы безопасности также будет автоматически выбран элемент **Настройки синхронизаций с Active Directory**.
- **Протокол приложений**
  При этом будут экспортирован/импортирован только список приложений **Обнаруженные** (см. Раздел "Ресурсы").

  > **Важно!**
  >
  > При импорте протокола приложений необходимо также импортировать схему безопасности. Если после импорта не будет связи между приложением из протокола и рабочей станцией, на которой оно было обнаружено, это приложение не будет добавлено в Систему.

- **Настройки:**
  - Настройки корпоративных сетей
  - Настройки контроля сетевых ресурсов
  - Список исключенных из перехвата приложений
  - Настройки каналов перехвата – Хосты для VK+

Если вы выбрали элемент **Схема безопасности**, то в составе конфигурации будут экспортированы/импортированы:

- Правила:
  - Правило контроля съемных носителей;
  - Правило контроля сетевых ресурсов;
  - Правило контроля терминальной сессии;
  - Правило контроля печати;
  - Правило контроля FTP;
  - Правило контроля HTTP(S);
  - Правило контроля почты;
  - Правило контроля буфера обмена;
  - Правило контроля облачных хранилищ;
  - Правило контроля мессенджера VK;
  - Правило контроля мессенджера Telegram;
  - Правило контроля Яндекс Мессенджера;
  - Правило контроля мессенджера WhatsApp;
  - Правило контроля мессенджера MAX;
  - Правило контроля создания снимков экрана;
  - Правило мониторинга экрана;
  - Правило мониторинга ввода текста с клавиатуры;
  - Правило мониторинга активности сотрудника;
  - Правило мониторинга звукового окружения;
  - Правило контроля файлов в приложениях.

> **Важно!**

Если в файле импорта есть правило *Контроля файлов в приложениях* для какого-либо профиля, но этот профиль отсутствует на компьютере, куда импортируется конфигурация, то в результате импорта в системе будет отсутствовать это правило.

Подробнее о профилях см. Универсальный перехватчик файлов.

Подробнее о правилах см. Создание правил;

- Группы компьютеров (подробнее о группах компьютеров см. Раздел "Группы");
- Группы сотрудников (подробнее о группах сотрудников см. Раздел "Группы");
- Ресурсы:
  - Списки веб-ресурсов;
  - Список приложений;
  - Категории файлов.

Подробнее о ресурсах см. Раздел "Ресурсы".

Чтобы настроить автоматический сброс несохраненных изменений конфигурации:

1. В области *Автоматический сброс несохраненных изменений конфигурации* укажите время в диапазоне от 00:05 до 23:59, по истечении которого необходимо сбрасывать несохраненные изменения.
2. Нажмите **Сохранить**.

Важно!

Если вы меняете время автоматического сброса при редактировании конфигурации, то изменения вступят в силу только после применения/сброса конфигурации. Подробнее о редактировании конфигурации см. Режимы редактирования конфигурации.

7.12 Диагностика событий

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

1. Перейдите в **Настройки → Device Monitor → Диагностика событий**.
2. В фильтре **Начало периода** и **Окончание периода** выберите дату и время, за которые необходимо выгрузить отчет. По умолчанию в отчет включаются события с 00:00 до 23:59.
3. Чтобы выбрать пользователя, нажмите кнопку **Выбрать пользователя**.
4. В открывшемся окне, нажав на нужную группу, выберите пользователя или воспользуйтесь полем поиска. Поиск пользователя доступен только по его идентификатору.
5. Нажмите . Напротив пользователя, который был добавлен, появится значок . Для удаления пользователя из выбранных наведите курсор на его имя пользователя и нажмите .
6. Нажмите **Применить**.
7. Чтобы выбрать компьютер, нажмите кнопку **Выбрать компьютер**.
8. В открывшемся окне, нажав на нужную группу, выберите компьютер или воспользуйтесь полем поиска.

9. Нажмите . Напротив компьютера, который был добавлен, появится значок . Для удаления компьютера из выбранных наведите курсор на его имя и нажмите .
10. Нажмите **Применить**.
11. Задайте количество событий в выгрузке в поле **Максимальное количество событий в выгрузке**. По умолчанию выгрузка содержит 10 000 событий, максимальное количество событий в выгрузке – 1000 000.
12. 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*.

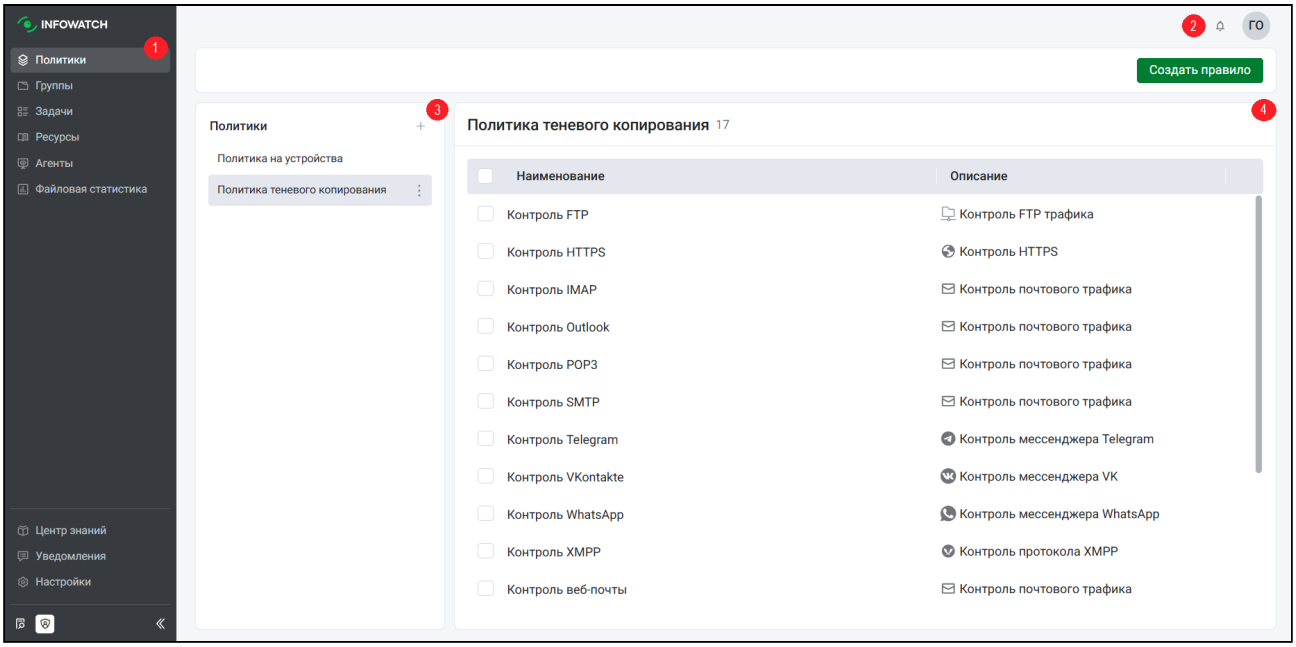
Данные в отчете отсортированы по дате и времени событий по убыванию.

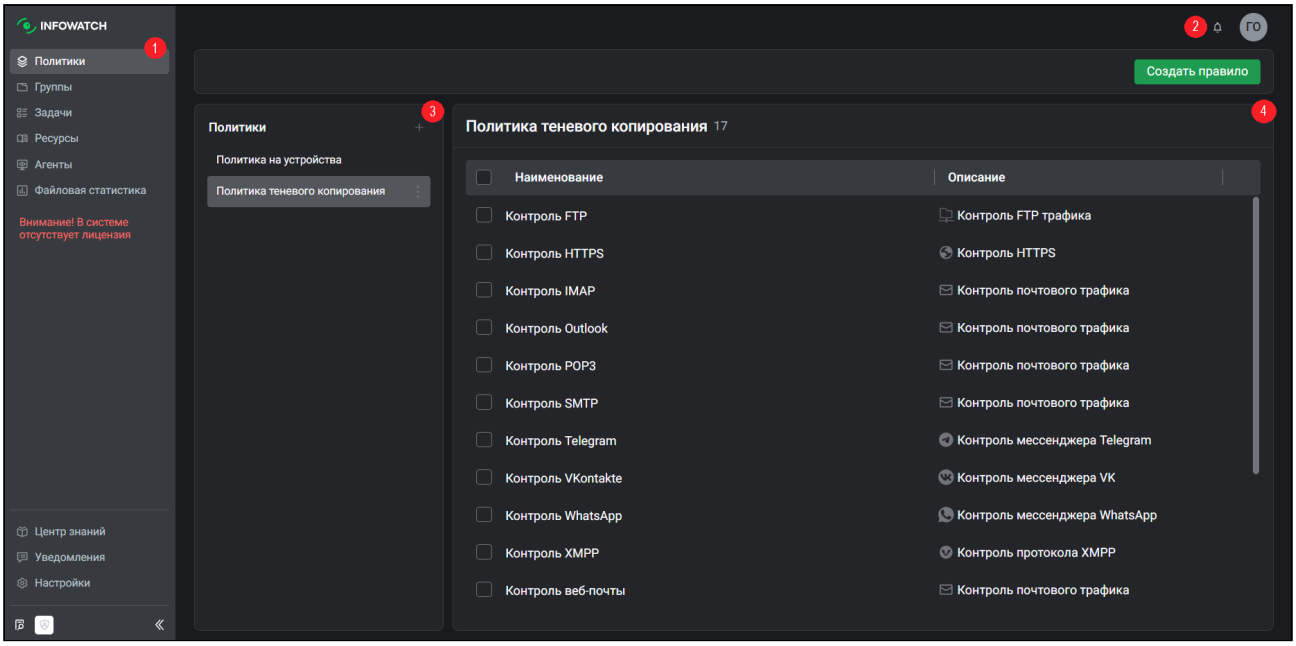
8 Интерфейс Центра Администрирования (Device Monitor)

Веб-консоль Центра администрирования (Device Monitor) предназначена для решения следующих задач:

- управление доступом к системе InfoWatch Device Monitor;
- централизованная установка и обновление Агентов Device Monitor на рабочих станциях;
- настройка системы мониторинга компьютеров, сотрудников и устройств;
- контроль доступа к компьютерам и устройствам.

Интерфейс Центра администрирования содержит несколько областей с настройками и данными (на примере раздела **Политики**).





Элементы интерфейса:

Номер на схеме	Элемент окна	Назначение элемента
1	Панель навигации	Разделы Центра администрирования (Device Monitor): • **Политики** – управление политиками Device Monitor: создание политик, настройка правил для каждой политики; • **Раздел "Группы"** – управление учетными записями сотрудников и группами сотрудников (вкладка **Сотрудники**), управление контролируемыми компьютерами: создание групп компьютеров, распределение контролируемых компьютеров по группам (вкладка **Компьютеры**); • **Раздел "Задачи"** – централизованная установка, обновление и удаление Агентов InfoWatch Device Monitor на компьютеры; • **Раздел "Ресурсы"** – управление списками веб-ресурсов, приложений и категорий файлов для использования в правилах; • **Агенты** – отслеживание состояния Агентов на рабочих станциях; • **Файловая статистика** – управление конфигурацией файловой статистики пользоваетеля; • раздел **Центр знаний** с документацией и базой знаний; • раздел **Уведомления** для настройки и просмотра пользовательских уведомлений; • раздел **Настройки** (подробнее см. Настройки пользователей, Общие настройки, Настройка Device Monitor). Вы можете скрыть панель навигации, нажав « внизу. Переход между Центром расследований и Центром администрирования можно выполнить с помощью переключателей и
2	Меню пользователя	Пользовательское меню, в котором вы можете:

Номер на схеме	Элемент окна	Назначение элемента
		• выбрать светлую или темную тему отображения на экране; • отредактировать свою учетную запись; • сменить пароль; • получить справку по горячим клавишам; • узнать сведения о версии, контактные данные компании InfoWatch и службы поддержки; • выбрать язык интерфейса: Русский или Английский; • выйти из Системы
		Папка системных уведомлений с сообщениями пользователю, полученными в автоматическом режиме
3-4	Рабочие области	Отображение элементов выбранного раздела Центра администрирования (Device Monitor) и работа с ними

8.1 Раздел "Политики"

Раздел **Политики** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  слева внизу на Панели навигации.

Политика – это совокупность правил, в соответствии с которыми проводятся 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 терминальной сессии**. Позволяет отслеживать операции копирования файлов в приложение терминальной сессии и копирования файлов на ресурсы, подключенные через терминальную сессию.
- **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**. 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 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 облачных хранилищ**. Позволяет контролировать получение и отправку любых данных на облачные хранилища и доступ к их веб-клиентам.
- **Мониторинг экрана**. Позволяет создавать снимки экрана компьютера.
- **Контроль буфера обмена**. Позволяет контролировать вставку данных с использованием буфера обмена через приложение терминальной сессии.
- **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 Яндекс Мессенджера**. Позволяет контролировать доступ сотрудников к сервису мгновенного обмена сообщениями Яндекс Мессенджер: обмен новыми, пересылаемыми или исправленными сообщениями чата, в том числе группового, исходящими файлами.

- **Контроль мессенджера WhatsApp**. Позволяет контролировать доступ сотрудников к сервису мгновенного обмена сообщениями WhatsApp: обмен новыми, пересылаемыми или исправленными сообщениями чата, в том числе группового, исходящими файлами.
- **Контроль мессенджера MAX**. Позволяет контролировать доступ сотрудников к сервису мгновенного обмена сообщениями MAX: обмен сообщениями чата, в том числе группового, исходящими файлами.
- **Контроль XMPP**. Позволяет контролировать обмен по протоколу XMPP входящими и исходящими текстовыми сообщениями, а также исходящими файлами.
- **Мониторинг ввода текста с клавиатуры**. Позволяет перехватывать ввод текста с клавиатуры в окне любого приложения на рабочих станциях и формировать события при смене активного окна.
- **Мониторинг активности сотрудника**. Позволяет собирать статистику активности сотрудника за контролируемым компьютером.
- **Мониторинг звукового окружения**. Позволяет отслеживать действия сотрудника при помощи контроля звукового окружения его рабочей станции.
- **Контроль перехвата видео**. Позволяет отслеживать действия сотрудника с помощью записи видео экрана рабочей станции.
- **Контроль создания снимков экрана**. Позволяет запрещать сотрудникам создавать снимки экрана.
- **Контроль файлов в приложениях**. Позволяет перехватывать события чтения и/или записи файлов в приложении.

> **Важно!**
>
> Контроль мессенджера Skype не поддерживается начиная с версии 7.19.

О настройке политик смотрите:

- Создание политик
- Создание правил

8.2 Раздел "Группы"

Раздел **Группы** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  на панели навигации. Раздел **Группы** содержит подразделы:

- **Компьютеры**
- **Сотрудники**

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 о работе с контролируемыми компьютерами содержится в подразделе "Работа с группами компьютеров".

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 Outlook
  - Контроль POP3
  - Контроль SMTP
  - Контроль Telegram
  - Контроль VKontakte
  - Контроль WhatsApp
  - Контроль XMPP
  - Контроль веб-почты
  - Контроль облачных хранилищ
  - Контроль Яндекс Мессенджера
  - Теневое копирование документов
  - Теневое копирование документов в терминальную сессию
  - Теневое копирование документов на сетевые ресурсы
  - Теневое копирование печати

Подробнее о правилах см. в разделе "Раздел "Политики"".

Информация о работе с контролируемыми сотрудниками содержится в подразделе "Работа с группами сотрудников".

8.3 Раздел "Задачи"

Важно!

Раздел "Задачи" будет отключен в последующих версиях. Управление установкой, обновлением и удалением доступно в новом разделе с расширенными возможностями контроля и приоритизации. Рекомендуем перейти к "Политикам распространения" в разделе "Агенты", чтобы продолжить работу. См. статью "Политики распространения".

Раздел **Задачи** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  на панели навигации. В этом разделе представлен список всех задач, созданных пользователем. Это могут быть задачи первичного распространения или обновления.

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 .

Чтобы создать и запустить задачу, смотрите статью "Задача первичного распространения и обновления".

8.4 Раздел "Ресурсы"

Раздел **Ресурсы** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  на панели навигации.

Раздел **Ресурсы** содержит подразделы:

- **Списки веб-ресурсов**
- **Списки приложений**
- **Категории файлов**

8.4.1 Списки веб-ресурсов

В подразделе **Списки веб-ресурсов** вы можете создавать списки ресурсов для использования в правиле автоматического создания снимков экрана. С помощью списков вы можете задать, какие веб-ресурсы правило должно контролировать или исключить из контроля.

О работе со списками ресурсов см. "Создание и изменение списков ресурсов".

8.4.2 Списки приложений

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

Вы можете использовать списки приложений в:

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

Список приложений содержит следующую информацию:

- *Имя приложения*
- *Описание*
- *Название продукта* *
- *Издатель* *
- *Расположение исполняемого файла*

Примечание:

* Столбцы *Название продукта* и *Издатель* доступны только для Windows-приложений.

Вы можете изменить ширину столбца в таблице и переместить столбец.

О создании списков и добавлении в них приложений см. "Создание и изменение списков приложений".

Обнаруженные приложения

Список **Обнаруженные** 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 список обнаруженных приложений.

Таблица содержит следующую информацию о приложениях:

- *Дата добавления*
- *Компьютер*
- *Пользователь*
- *Описание*
- *Название продукта*
- *Издатель*
- *Расположение исполняемого файла*

Вы можете переместить колонки в таблице и изменить их размер.

Из таблицы 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!

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

8.4.3 Категории файлов

В разделе **Категории файлов** определен список расширений файлов, которые может распознавать Device Monitor. Для удобства использования расширения сгруппированы по **категориям**:

- CAD системы;
- Архивы;

- Аудио-видео;
- Базы данных и таблицы;
- Графические данные;
- Документы (офисные файлы, PDF);
- Другие файлы;
- Защищенные данные (зашифрованные, элементы PKI, хранилища паролей);
- Исполняемые файлы;
- Образы (виртуальные машины, образы дисков, дампы памяти);
- Форматы данных мобильных устройств.

Для следующих правил вы можете указать, на какую категорию файлов они будут распространяться:

- Правило контроля съемных носителей
- Правило контроля сетевых ресурсов
- Правило контроля терминальной сессии

Из предустановленных расширений вы можете создавать свои категории файлов. О работе с категориями файлов см. "Создание и изменение категорий файлов".

8.5 Раздел "Агенты"

Раздел **Агенты** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  на панели навигации. Раздел содержит вкладку **Состояние**, на которой вы можете отслеживать состояние Агентов на рабочих станциях.

О просмотре сведений об Агентах и назначении им статусов см. "Работа с Агентами".

8.6 Раздел "Файловая статистика"

Раздел **Файловая статистика** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  на панели навигации. С помощью данного раздела вы можете редактировать предустановленную конфигурацию файловой статистики пользователя.

Конфигурация файловой статистики – это набор включений/исключений приложений, файловых расширений, путей к файлам и другие параметры настройки файловой статистики пользователя.

Примечание:

Конфигурация по умолчанию содержит следующие исключения:

- файловые расшрения: 000; .386; .adv; .ani; .ann; .automaticdestinationsms; .bcd; .bin; .bio; .bk1; .bk2; .bmk; .bud; .cab; .cat; .chg; .chs; .cht; .ci; .clb; .cnt; .cpi; .cpl; .cur; .cust omdestinations-ms; .dat; .desklink; .deskthemepack; .dev; .devicemetadatams; .dit; .dll; .dmp; .drv; .ebd; .etl; .evt; .evtx; .exe; .ffa; .ffl; .ffo; .ffx; .fid; .grl; .group; .grp; .h1s; .hdmp; .hhc; .hhk; .hiv; .hlp; .hpj; .hsh; .hve; .icl; .icn; .ico; .iconpackage; .idx; .ime; .inf; .inf_loc; .ini; .itemdat a-ms; .js; .job; .jpn; .kbd; .kor; .libraryms; .lnk; .manifest; .mbr; .mdmp; .mem; .mlc; .msc; .msi; .msp; .msstyle; .msstyles; .mtz; .mui; .mum; .nfo; .nls; .nt; .ntfs; .pdr; .pfx; .pol; .ppd; .ppm; .prf; .printerexport; .ps1; .ps2; .pwl; .reg; .reglnk; .reg trans-ms; .rs; .scf; .scr; .searchconnectorms; .shd; .spl; .spx; .str; .swp; .sys; .theme; .trx_dll; .uce; .vga; .vx_; .vxd; .wdf; .wer; .wsf; .wsh; .xrmms; .zone.identifier; .tmp; .crdownloads; .thumbs.db

- файловые пути: \Recovery\;\System Volume Information\;\MSOCache\;\Windows\; \Program Files\;\Program Files (x86)\; \Users*\AppData\

В рабочей области отображаются подразделы:

- **Общее** – редактирование конфигурации файловой статистики и списка приложений, которые включены в перехват или исключены из него;
- **Перехваты** – настройка включений и исключений файловых расширений и путей к файлам.

> **Важно!**
>
> Включение/исключение расширений и путей распространяется только на те файлы и папки, над которыми непосредственно выполняется действие.
>
> **Пример 1**
>
> Если в исключениях настроены файлы с расширением `.docx`, то при работе пользователя с папкой, которая содержит файлы с этим расширением, событие на действие с файлом `*.docx` формируется и отправлено в Платформу.
> **Пример 2**
>
> Если в исключениях настроена *папка 2*, которая является подпапкой *папки 1*:
>
> - действие выполняется с *папкой 1*, то события на все файлы, которые находятся в *папке 2*, будут сформированы и отправлены в Платформу;
> - действие выполняется с *папкой 2*, она попадает под исключения и событие папки не формируется на стороне агента.

Чтобы отредактировать конфигурацию, смотрите статью *Работа с файловой статистикой*.

9 Обнаружение рабочих станций для установки Агентов

В дистрибутиве для установки сервера Device Monitor есть утилита сканирования диапазона IP-адресов. Она устанавливается автоматически вместе с консолью управления Device Monitor. Результат сканирования – это текстовый файл со списком "IP-адрес или доменное имя – операционная система" для тех рабочих станций, на которые Агент Device Monitor не установлен.

Утилита не имеет графического интерфейса и запускается из командной строки. Ниже описаны параметры, которые нужно или можно указать при запуске. Чтобы просмотреть их описание, вызовите справку: `Iw.Util.MachineDiscovery -- help`.

`--mode arg (=icmp)*`	Режим сканирования сети (обязательный параметр): • `nmap` – сканирование сети с помощью утилиты `nmap`, которая может дополнительно определить тип операционной системы по эвристическим алгоритмам; • `icmp` – сканирование сети по протоколу ICMP.
`--ip-range arg`	Диапазон IP-адресов в одном из форматов, валидных для `nmap` (обязательный параметр). Например: " `--ip-range 10.60.3-35.1-254` ".
`--ip-cidr-range arg`	Диапазон IP-адресов в формате CIDR (обязательный параметр). Например " `--ip-cidr-range 10.60.3.4/24` ".
`--ipv6-cidr-range arg`	Диапазон IPv6-адресов в формате CIDR (обязательный параметр, если используется протокол IPv6). Например: `"--ipv6-cidr-range fe80::98b9:ec9:f9a9:9104/120"`. **Важно!** Для IPv6-адресов поддерживается только формат CIDR.
`--threads arg (=2)`	Количество потоков для обработки асинхронных запросов на сканирование сети.
`--icmp-attempts arg (=2)`	Количество попыток обратиться по протоколу ICMP к IP-адресу, чтобы признать его недоступным. Так как протокол ICMP не гарантирует доставку пакетов (в отличии от TCP), то они могут теряться, и для большей уверенности в недоступности адресата нужно несколько попыток.
`--icmp-timeout arg (=5000)`	Время ожидания ответа от адресата для каждой попытки проверки его доступности.
`--deploy-agent-port arg (=15505)`	Порт агента распространения, на котором он слушает сеть. Нужно оставить значение по умолчанию.
`--output-file arg`	Путь к файлу с результатами работы утилиты.

`--nmap-path arg (nmap mode)`	Путь к кроссплатформенной утилите `nmap` в случае использования режима `nmap`.
`--nmap-os-info arg (=1)`	Определять (=1) или не определять (=0) операционную систему рабочих станций при сканировании в режиме `nmap`.
`--nmap-save-output-to-file arg (=1)`	Сохранить `stdout` и `stderr` из `nmap` в файл `Nmap_output_%Y-%m-%d_%H-%M-%S.log`
`--nmap-timing arg (=3)`	Частота сканирования `nmap`-ом: • от 0 – самого медленного и точного сканирования; • до 5 – самого быстрого и неточного сканирования.
`--nmap-min-hostgroup arg (=16)`	Минимальный размер группы для параллельного сканирования `nmap`-ом.
`--nmap-max-hostgroup arg (=16)`	Максимальный размер группы для параллельного сканирования `nmap`-ом (до 1024).
`--nmap-min-parallelism arg (=10)`	Минимальное количество запросов для группы хостов (от 1).
`--nmap-max-parallelism arg (=10)`	Максимальное количество запросов для группы хостов.
* – в скобках указано значение по умолчанию.	

Чтобы запустить утилиту:

1. В командной строке на рабочей станции с консолью Device Monitor перейдите в директорию с утилитой `Iw.Util.MachineDiscovery` с помощью команды `cd`:

   ```
   cd  <путь_до_утилиты>
   ```

2. Запустите утилиту, обязательно указав при этом диапазон IP-адресов, а также другие параметры, если они нужны. Например:

   ```
   Iw.Util.MachineDiscovery --ip-range 10.60.3-35.1-254
   ```

3. Дождитесь окончания сканирования.
4. По завершении сканирования результаты будут записаны в текстовый файл `iw_machine_discovery.output.txt` в директории размещения утилиты. Используйте полученные данные при создании списка компьютеров для установки Агентов на них (см. *Задача первичного распространения и обновления*).

10 Задача первичного распространения и обновления

> **Важно!**
>
> Раздел "Задачи" будет отключен в последующих версиях. Управление установкой, обновлением и удалением доступно в новом разделе с расширенными возможностями контроля и приоритизации. Рекомендуем перейти к "Политикам распространения" в разделе "Агенты", чтобы продолжить работу. См. статью "Политики распространения".

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.

Чтобы создать задачу первичного распространения Агентов:

1. В левой части рабочей области нажмите .
2. Выберите ОС рабочих станций, на которые требуется распространить Агенты: *Windows*/*Linux*.
3. Введите имя новой задачи.
4. Снимите флаг **Устанавливать компонент перехвата сетевого трафика**, если не хотите, чтобы этот компонент был установлен.
5. Начиная с **Device Monitor 7.18.5**, **при первичной установке Агента** инсталлятор проверяет, получен ли список приложений, которые должны быть исключены из перехвата. Если список исключений не получен, установка этого Агента будет остановлена. В этом случае в лог ошибок будет добавлена запись:
   - для Linux – `ERROR: exclusions not received (rc=255); abort install (exit 2)`
   - для Windows – `CustomAction GetExclusionsFromServerWithCheck returned actual error`

   Проверка включена по умолчанию, если вы хотите отключить проверку, снимите флаг **Отменять установку при сбое получения списка приложений, исключаемых из перехвата**.
6. Если необходимо, добавьте описание задачи.
7. Задайте количество запусков задачи и их периодичность в минутах.
8. Укажите точку распространения Агентов, установленную ранее на сервере Device Monitor (подробнее см. "Установка "Все-в-одном"", Шаг 30). Или установите флаг **Использовать все доступные точки распространения**, чтобы использовать все точки распространения.
9. Последняя доступная версия Агентов, дистрибутивы которых необходимо установить, отображается в поле **Версия** (см. "Серверы").

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

10. Укажите количество попыток загрузки пакета. Количество попыток по умолчанию – 10.

11. Нажмите **Добавить**. Новая задача будет отображена в списке задач.

Чтобы обновить версию Агентов на рабочих станциях под управлением ОС семейства Linux:

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 **Добавить**.

> **Важно!**
>
> Для корректной блокировки съемных устройств обязательно перезагрузите рабочую станцию после обновления Агента.

Чтобы сформировать список рабочих станций:

Добавьте компьютеры одним из способов:

1. Чтобы добавить компьютер вручную, в выбранной задаче нажмите .
2. В открывшемся окне введите IP-адрес или DNS-имя компьютера, разделенные точкой с запятой или переносом строки (имя компьютера может состоять из любых символов любых алфавитов, указанных в Unicode).
3. Нажмите **Добавить**.

или

1. Чтобы добавить компьютеры из списка, нажмите **Настроить состав задачи** :
2. В открывшемся окне будет отображен список компьютеров из доступной интеграции с Active Directory или ранее добавленных компьютеров Группы Device Monitor (подробнее см. "Настройка состава групп компьютеров") с указанием полного имени для установки Агентов. Выберите рабочие станции в области *Компьютеры* и нажмите . При добавлении группы добавляются компьютеры только из выбранной группы, не включая компьютеры в подгруппах. Вы можете воспользоваться полем поиск, чтобы быстро найти нужный компьютер и добавить его в задачу. Введите не менее 3 и не более 64 символов.
3. Нажмите **Применить**. В области с именем 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 или нажмите  напротив нужной задачи в списке слева.
2. Нажмите **Запустить** .
3. В открывшемся окне введите учетные данные пользователя удаленной рабочей станции, от имени которого запускается задача.

4. Если вы запускаете задачу распространения агентов на рабочие станции под управлением ОС семейства Linux:
    a. Выберите механизм повышения привилегии `sudo` / `su` .
    b. Если вы выбрали механизм повышения привилегии `su` :
        - Введите учетные данные пользователя, от имени которого будет осуществлено распространение агентов.
          или
        - Отметьте **Использовать указанные учетные данные**, чтобы осуществить распространение агентов от имени пользователя, указанного на шаге 3.
5. Нажмите **Запустить**.
6. 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: • ***Ошибка*** • ***Проигнорирована*** • ***Запланирована*** • ***Идет установка*** • ***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 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.

Примечание:

Если при установке Агента возникла ошибка, то вы можете выгрузить лог ошибок только последнего запуска задачи.

Чтобы вернуться к списку рабочих станций, нажмите .

11 Настройка схемы безопасности

Схема безопасности в Device Monitor представляет собой набор конфигурационных параметров, в соответствии с которыми ведется наблюдение за действиями контролируемых сотрудников. Схема безопасности создается в процессе установки Сервера и хранится в базе данных.

В набор параметров схемы безопасности входят:

- **Политики** с заданным для каждой из них набором правил.
- **Группы сотрудников** с назначенной на каждую из них политикой безопасности.
- **Группы компьютеров** с назначенной на каждую из них политикой безопасности.
- **Списки приложений**, разрешенных или запрещенных к использованию в правилах.
- **Категории файлов**, с помощью которых правила контроля съемных устройств могут распространяться на заданные форматы файлов.
- **Конфигурация файловой статистики** для настройки контроля действий сотрудника с файлами.

> **Примечание.**
>
> Чтобы исключить возможность существования в Системе компьютеров и учетных записей сотрудников, которым не назначена политика безопасности, предусмотрены: группа сотрудников «по умолчанию» и группа компьютеров «по умолчанию».

Остальные сущности Системы в схему безопасности не входят.

Схема безопасности может неоднократно редактироваться. Отредактированная схема безопасности будет сохранена как новая версия существующей схемы безопасности. Старые версии схемы безопасности при этом не удаляются, а хранятся в базе данных. В Центре расследований вы можете просмотреть политики и содержащиеся в них правила любой версии схемы безопасности.

Подробная информация о настройке содержится в подразделах:

- Режимы редактирования конфигурации
- Создание политик
- Создание правил
- Создание и изменение списков приложений
- Создание и изменение списков ресурсов
- Создание и изменение категорий файлов
- Работа с группами компьютеров
- Работа с группами сотрудников
- Работа с Агентами
- Работа с файловой статистикой

11.1 Режимы редактирования конфигурации

В текущей версии Device Monitor доступно два режима редактирования конфигурации в настройках Device Monitor **Универсальный перехватчик файлов** и в разделах **Группы, Политики** и **Ресурсы** Центра администрирования:

- ***синхронное редактирование***. В этом режиме все пользователи могут редактировать конфигурацию одновременно. Редактирование конфигурации будет недоступно только когда запущена синхронизация со службой каталогов;

- ***запрет синхронного редактирования*** (по умолчанию). В каждый момент конфигурацию может редактировать только один пользователь. Все изменения, внесенные пользователем, начинают действовать только после сохранения конфигурации. Для других пользователей редактирование конфигурации в этот момент недоступно. Также редактирование будет заблокировано для всех пользователей, когда запущена синхронизация со службой каталогов.

11.1.1 Режим запрета синхронного редактирования

Запрет режима редактирования включен по умолчанию.

Чтобы настроить режим запрета синхронного редактирования, необходимо добавить параметр `"SandboxSettings"` в конфигурацию. Для этого:

1. Откройте файл конфигурации `/opt/iw/dmserver/webapibin/webapi.appsettings.json`.
2. В последней конфигурации найдите строку:

   ```
   "ConnectionString": "Server=<server_name>;Port=<port>;Database=<database_name>;User Id=<user_id>;Password=<password>;",
   ```

   и после нее добавьте:

   ```
   "SandboxSettings":
   {
       "UseSandbox": "False",
   }
   ```

   где:
   - `UseSandbox` – настройка запрета синхронного редактирования. Чтобы отключить режим редактирования, вставьте значение False. Для дальнейшей настройки или включения режима, вставьте значение True.
3. При необходимости добавьте к параметру настройку `ResetTimeMinutes`, которая позволяет любому пользователю сбрасывать конфигурацию, находящуюся на редактировании. Значение задается в минутах. Минимальное значение – 5, максимальное – 999.
4. Перезапустите сервис командой:

   ```
   systemctl restart iwdms_webapi.service
   ```

11.1.2 Автоматический сброс несохраненных изменений конфигурации

При отсутствии активности пользователя в течение установленного времени редактирование конфигурации автоматически сбрасывается. По умолчанию конфигурация сбрасывается через 20 минут бездействия пользователя.

Для изменения времени сброса, перейдите в **Настройки** > **Конфигурация** (подробнее см. "Конфигурация").

Важно!

Если вы меняете время автоматического сброса при редактировании конфигурации, то изменения вступят в силу только после применения/сброса конфигурации.

11.1.3 Описание режима запрета редактирования

Все ваши изменения в конфигурации доступны только в текущей сессии браузера до их сохранения.

После редактирования конфигурации вы можете сохранить изменения или сбросить их нажатием соответствующих кнопок на информационной панели в верхней части экрана.



Если конфигурация уже редактируется другим пользователем, то действия по редактированию становятся недоступными или скрываются. В верхней части экрана появится сообщение *Конфигурация редактируется другим пользователем*. Если попытаться изменить заблокированную схему, появится сообщение *Ошибка сохранения*.

Сбросить конфигурацию другого пользователя можно только по истечении времени, заданного в параметре.

Важно!

Если редактирование конфигурации завершилось ошибкой, Система все равно считает ее заблокированной.

При сбросе конфигурации другого пользователя все изменения в незавершенных сессиях будут утеряны.

Действия, которые не изменяют конфигурацию, не блокируют ее. Например, когда вы редактируете информацию об одном компьютере/сотруднике, то возможность редактирования конфигурации для других пользователей не будет заблокирована.

Если пользователь не взаимодействует с Консолью управления указанное в параметре время, то происходит автоматический сброс внесенных изменений и разблокирование конфигурации.

11.1.4 Восстановление доступа к заблокированной конфигурации

В ходе работы может возникнуть ситуация, когда ни один из пользователей не редактирует конфигурацию, но она находится в заблокированном состоянии. Такое возможно, если процесс редактирования конфигурации был завершен некорректно (например, при смене пользователем браузера или очистке кэша браузера во время редактирования).

Конфигурация автоматически разблокируется через заданное в параметре время, если пользователь, который вносил изменения, не взаимодействует с Консолью управления в течение этого времени.

Чтобы восстановить доступ раньше автоматической разблокировки, перезапустите службу `iwdms_webapi.service` командой:

```
systemctl restart iwdms_webapi.service
```

Важно!

При перезапуске службы `iwdms_webapi.service` все изменения в незавершенных сессиях будут утеряны.

11.1.5 Редактирование конфигурации при запущенной синхронизации со службой каталогов

Когда запущена синхронизация со службой каталогов (см. подробнее "Синхронизация"), действия по редактированию становятся недоступными или скрываются. В верхней части экрана появится сообщение *Идет процесс синхронизации. Запрещено редактирование конфигурации*.

Данная функциональность включена по умолчанию.

11.2 Создание политик

Важно!

При обновлении сервера Device Monitor до версии 7.15 и выше подключенные к этому серверу агенты версии 7.13 и более ранних прекратят получать данные об изменении схемы безопасности. Поэтому для получения агентами правил, политик, компьютеров, сотрудников и т.д. необходимо также обновить агенты до версии 7.14 или более поздней.

На Агентах Device Monitor политики применяются в следующем порядке:

1. Запрещающие политики.
2. Политики защиты данных на агентах, созданные в Traffic Monitor.
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 назначаются **группам сотрудников** и **группам компьютеров**. Политика, 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.

После установки Центра администрирования (Device Monitor) по умолчанию созданы две политики – **Политика теневого копирования** и **Политика на устройства**.

Политика теневого копирования содержит следующие правила:

- Контроль FTP;
- Контроль HTTPS;
- Контроль IMAP;
- Контроль Outlook;
- Контроль POP3;

- Контроль SMTP;
- Контроль Telegram;
- Контроль VK;
- Контроль WhatsApp;
- Контроль MAX;
- Контроль XMPP;
- Контроль веб-почты;
- Контроль облачных хранилищ;
- Контроль Яндекс Мессенджера;
- Теневое копирование документов;
- Теневое копирование документов в терминальную сессию;
- Теневое копирование документов на сетевые ресурсы;
- Теневое копирование печати.

Политика на устройства по умолчанию не содержит правил.

Чтобы создать новую политику:

1. В левой части рабочей области нажмите  .
2. В поле **Наименование** укажите название политики.
3. Нажмите **Создать**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

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  напротив выбранной политики.
3. В раскрывшемся списке нажмите  **Редактировать политику**.
4. В поле **Наименование** укажите новое название политики.
5. Нажмите **Сохранить**.
6. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы удалить политику:

1. В левой части рабочей области выберите политику.
2. Нажмите  напротив выбранной политики.
3. Нажмите  **Удалить политику**.
4. Подтвердите действие.

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

5. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

11.3 Создание правил

Чтобы добавить в политику новое правило:

1. Перейдите в раздел **Политики** Центра администрирования.
2. В левой части рабочей области выберите политику безопасности, в которую вы хотите добавить правило.
3. Нажмите  напротив выбранной политики. Затем в раскрывшемся списке нажмите  **Создать правило**.
   или
   В правой верхней части рабочей области нажмите кнопку **Создать правило**.
4. В открывшемся окне укажите параметры правила. Доступные для создания правила:
   - Контроль каналов передачи данных:
     - Правило контроля съемных носителей;
     - Правило контроля сетевых ресурсов;
     - Правило контроля терминальной сессии;
     - Правило контроля печати;
     - Правило контроля внешних устройств;
     - Правило контроля FTP;
     - Правило контроля HTTP(S);
     - Правило контроля почты;
     - Правило контроля облачных хранилищ;
     - Правило проксирования сетевого трафика;
     - Правило контроля буфера обмена.
   - Контроль мессенджеров:
     - Правило контроля мессенджера VK;
     - Правило контроля мессенджера Telegram;
     - Правило контроля Яндекс Мессенджера
     - Правило контроля мессенджера WhatsApp;
     - Правило контроля мессенджера MAX;
     - Правило контроля протокола XMPP.

     > **Важно!**
     >
     > Контроль мессенджера Skype не поддерживается начиная с версии 7.19.

   - Мониторинг активности пользователей:
     - Правило мониторинга экрана;
     - Правило мониторинга ввода текста с клавиатуры;
     - Правило мониторинга активности сотрудника;
     - Правило мониторинга звукового окружения;
     - Правило записи видео с экрана.
   - Контроль использования:
     - Правило контроля создания снимков экрана.
   - Контроль приложений:
     - Правило контроля файлов в приложениях.
5. После того как вы указали все необходимые параметры, нажмите **Создать**. Правило будет добавлено в политику.

6. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

> **Примечание:**
>
> Device Monitor позволяет перехватывать действия сотрудника, подключенного к рабочей станции через терминальную сессию:
>
> - на ОС семейства **Linux только через xRDP**. Особенности такого перехвата указаны отдельно для каждого правила;
> - на ОС **MS Windows через RDP**, без ограничений.

Чтобы просмотреть детальную информацию о правиле, выберите его. Справа откроется панель **Подробно** с информацией о выбранном правиле. Чтобы скрыть панель, нажмите  справа вверху или повторно нажмите на выбранное правило.

Чтобы отредактировать правило:

1. Перейдите в раздел **Политики** Центра администрирования.
2. Выберите политику.
3. Выберите правило, которое необходимо отредактировать.
4. Нажмите  напротив выбранного правила.
5. Нажмите **Редактировать**.
6. Внесите изменения.
7. Нажмите **Сохранить**.
8. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы удалить правило:

1. Перейдите в раздел **Политики** Центра администрирования.
2. Выберите политику.
3. Если нужно удалить одно правило, нажмите  напротив него и выберите **Удалить**.

   Если нужно удалить несколько правил, отметьте слева каждое из них  и нажмите  на панели внизу.

   Если нужно удалить все правила в выбранной политике, отметьте  в заголовке таблицы, чтобы выбрать все правила, и нажмите  на панели внизу.
4. Подтвердите действие.
5. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

11.3.1 Правило контроля съемных носителей

Правило позволяет отслеживать операции:

- копирования файлов с/на съемные носители;
- создания новых файлов на съемных носителях;
- изменения и переименования файлов на съемных носителях;

- копирования файлов с/на медиа-устройства, использующие для подключения протокол MTP;
- копирования файлов на съемных носителях (например, из одной папки USB-устройства в другую).

К съемным носителям 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 ОС семейства Linux 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** раскройте выпадающий список и выберите **Контроль каналов передачи данных** -> **Съемные носители**.
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:
   - *Создавать событие* – при этом будет создано событие с теневой копией.
   - *Исключить из перехвата* – при этом копирование будет разрешено, событие создано не будет. Для создания правила заполните ниже хотя бы одно из полей: **Маска файла** или **Категория файла**.
5. Выберите **Формировать теневую копию**, если необходимо создавать теневую копию в событии (настройка доступна при выборе **Создать событие** в поле **Действие**).

   Примечание:

   В Traffic Monitor в событии без теневой копии отображается название и размер файла.

6. Укажите условия для формирования событий:
   a. Отметьте и укажите **Маску файлов**, чтобы применить правило для подходящих под нее файлов. Вы можете использовать групповые символы:
      - ? – один неизвестный символ;
      - * – любое количество символов.
   b. Вы можете ограничить применение правила определенной категорией файлов, для этого отметьте поле и выберите **Категорию файла** из выпадающего списка.

      Примечание:

Вы можете ознакомиться с категориями файлов в разделе **Раздел "Ресурсы"**, а также в статье базы знаний "Перехватываемые расширения файлов в Device Monitor (для правил с выбором Категории файла)".

Если вы указали и маску файлов, и категорию, для срабатывания правила должны выполниться оба указанных условия.

На компьютерах под управлением ОС семейства Linux категории расширений не учитываются – правило сработает на копирование любых файлов, вне зависимости от указанных категорий файлов.

c. Задайте **Размер файла**, чтобы ограничить размер файлов, подлежащих контролю. При этом укажите диапазон значений для минимального и максимального размера файла и единицы измерения. Если заполнены оба поля, то правило будет действовать только для файлов, размер которых находится внутри указанного диапазона.
По умолчанию условие отмечено и задан размер файлов от 0 до 10 МБ.
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.

Важно!

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

- копируемые файлы удаляются (с возможностью восстановления при условии использования специального ПО);
- если съемный носитель был извлечен принудительно, блокировка копирования файлов по результатам анализа может не произойти;
- при копировании файлов с рабочей станции на съемный носитель 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. Операция перемещения (`move`) не поддерживается:
  - в РЕД ОС 8 при использовании файлового менеджера *Dolphin* (графическая среда *KDE*);
  - в ОС Astra Linux при использовании файлового менеджера *Fly*;
  - в файловом менеджере *Midnight Commander*;
  - через Bash-команды.

  Операция перемещения поддерживается:
  - в РЕД ОС при использовании файлового менеджера *Caja* (графическая среда *MATE*). В случае запрета операции политиками *Caja* отображает сообщение `error.png` ;
  - в ОС Альт 11.1 при использовании файлового менеджера *Nautilus* (графическая среда *GNOME*).

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".

11.3.2 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.

На рабочей станции под управлением ОС семейства Linux при подключении к терминальной сессии через xRDP в атрибут события **Сетевой адрес терминального клиента** может быть записан IP-адрес удаленного компьютера.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Контроль каналов передачи данных** -> **Сетевые ресурсы**.
3. Выберите направление перехвата копирования: *На ресурс* или *С ресурса*. Событие будет создано в результате копирования файла в выбранном направлении.
4. Вы можете выбрать режим **Запретить копирование**. Запрет доступен только при направлении копирования *На ресурс*. При этом поле **Действие** примет значение Создавать событие и будет недоступно для редактирования. Также будут недоступны поля **Маска файла**, **Категория файла** и **Размер файла**.
5. В **Действии при срабатывании правила** выберите реакцию Системы на копирование файла:
   - *Создавать событие* – при этом будет создано событие с теневой копией;
   - *Исключить из перехвата* – при этом копирование будет разрешено, событие создано не будет. Для создания правила заполните ниже хотя бы одно из полей: **Маска файла** или **Категория файла**.
6. Выберите **Формировать теневую копию**, если необходимо создавать теневую копию в событии (настройка доступна при выборе *Создавать событие* в поле **Действие**).

   Примечание:

   В Traffic Monitor в событии без теневой копии отображается название и размер файла.

7. Если требуется, укажите **Ресурсы**, задав их адреса. Чтобы посмотреть правила заполнения, наведите курсор на .
8. 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.

9. Вы можете ограничить применение правила определенной категорией файлов, для этого отметьте поле и выберите **Категорию файла** из выпадающего списка.

> **Примечание:**
>
> Вы можете ознакомиться с категориями файлов в разделе **Раздел "Ресурсы"**, а также в статье базы знаний "Перехватываемые расширения файлов в Device Monitor (для правил с выбором Категории файла)".
>
> Если вы указали и маску файлов, и категорию, для срабатывания правила должны выполниться оба указанных условия.
>
> На компьютерах под управлением ОС семейства Linux категории расширений не учитываются – правило сработает на копирование любых файлов, вне зависимости от указанных категорий файлов.

10. Чтобы ограничить размер файлов, подлежащих контролю, укажите диапазон значений для минимального и максимального размера файла и единицы измерения. Если заполнены оба поля, то правило будет действовать только для файлов, размер которых попадает в указанный диапазон.
    По умолчанию условие отмечено и задан размер файлов от 0 до 10 МБ.
11. 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".

11.3.3 Правило контроля терминальной сессии

Правило позволяет отслеживать операции:

- копирования файла в приложение терминальной сессии[1];
- копирования файла на ресурсы, подключенные через терминальную сессию (поддерживается перенаправление для сетевых папок и виртуальных устройств)[1 2].

> **Важно!**
>
> [1] Под терминальной сессией понимаются соответствующие технологии Microsoft и Citrix.
>
> 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 удаленном 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.
>
> Для передачи файлов при использовании средств обеспечения терминального доступа рекомендуется использовать механизм "проброса" дисков в удаленный сеанс вместо передачи при помощи буфера обмена.

[2] 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**.

Для Агентов на рабочих станциях под управлением ОС семейства Linux не поддерживается перехват файловых операций с устройствами, подключенными через терминальную сессию.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Контроль каналов передачи данных** -> **Терминальная сессия**.
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:
   - *Создавать событие* – при этом будет создано событие с теневой копией.
   - *Исключить из перехвата* – при этом копирование будет разрешено, событие создано не будет. Для создания правила заполните ниже хотя бы одно из полей: **Маска файла** или **Категория файла**.
5. Выберите **Формировать теневую копию**, если необходимо создавать теневую копию в событии (настройка доступна при выборе **Создать событие** в поле **Действие**)[3].
6. Укажите условия для формирования событий:
   a. Отметьте и укажите **Маску файлов**, чтобы применить правило для подходящих под нее файлов. Вы можете использовать групповые символы:
      - ? – один неизвестный символ;
      - * – любое количество символов.
   b. Вы можете ограничить применение правила определенной категорией файлов[4], для этого отметьте поле и выберите **Категорию файла** из выпадающего списка.
   c. Задайте **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.
   По умолчанию условие отмечено и задан размер файлов от 0 до 10 МБ.
   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.

Примечание:

[3] В Traffic Monitor в событии без теневой копии отображается название и размер файла.

[4] Вы можете ознакомиться с категориями файлов в разделе **Раздел "Ресурсы"**, а также в статье базы знаний "Перехватываемые расширения файлов в Device Monitor (для правил с выбором Категории файла)".

Если вы указали и маску файлов, и категорию, для срабатывания правила должны выполниться оба указанных условия.

На компьютерах под управлением ОС семейства Linux категории расширений не учитываются – правило сработает на копирование любых файлов, вне зависимости от указанных категорий файлов.

11.3.4 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** раскройте выпадающий список и выберите **Контроль каналов передачи данных** -> **Печать**.
3. При необходимости отключите опцию **Формировать теневую копию**, сняв соответствующий флажок, – тогда событие будет сохранено без теневой копии. По умолчанию опция включена.
   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.
4. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Важно!

Агент на ОС Astra Linux, РЕД ОС и macOS 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 семейства Linux:

- 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.

Если Агент Device Monitor установлен на ОС семейства Linux:

- не формируются события печати в файл, а на Агентах, установленных на ОС Astra Linux – также события печати на предустановленном принтере.

Если Агент Device Monitor установлен на РЕД ОС:

- не перехватывается задание печати, отправленное из некоторых приложений (например, редактора Pluma) на удаленный сервер печати в случае, если печать настроена на локальный сервер CUPS (т.е. при отсутствии в `/etc/cups/client.conf` директивы `ServerName`).

Если Агент Device Monitor установлен на macOS:

- перехват печати может перестать осуществляться в случае, когда при работающем Агенте система печати CUPS была перенастроена так, чтобы копии печатаемых файлов не создавались;
- могут создаваться события в случае отмены печати.

Важно!

В случае, если при действующем правиле процесс печати с сетевого принтера занимает больше времени, чем обычно, добавьте IP-адрес принтера в исключения из сетевого перехвата. Убедитесь, что адрес постоянный.

11.3.5 Правило контроля внешних устройств

Важно!

Начиная с версии Device Monitor 7.15 работа с данным правилом доступна в системе Device Control (раздел "Устройства" Центра расследований) и недоступна в Device Monitor. См. подробнее "Обновление Сервера Device Monitor", " InfoWatch Device Control. Руководство пользователя".

11.3.6 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** раскройте выпадающий список и выберите **Контроль каналов передачи данных** -> **FTP(S)**.

3. В **Действиях** при срабатывании правила выберите реакцию Системы при обмене данными:
   - *Создавать события для случаев записи на FTP* - запись на указанные FTP-ресурсы будет разрешена, но при этом будет создаваться событие;
   - *Исключать операции на указанных серверах FTP* - операции на указанных серверах будут исключены из перехвата, т.е. разрешены;
   - *Запретить запись на FTP*;
   - *Запретить вход на FTP-адреса.*
4. Выберите **Формировать теневую копию**, если необходимо создавать теневую копию в событии (настройка доступна при выборе **Создавать события для случаев записи на FTP** в поле **Действие**).

   > **Примечание:**
   >
   > В Traffic Monitor в событии без теневой копии отображается название и размер файла.

5. 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.

6. Если требуется, укажите ограничение на размер файла:
   a. Отметьте **Размер файла**.
   b. Обозначьте диапазон значений и единицы измерения.
   Если заполнены оба поля, то правило будет действовать только для файлов, размер которых находится внутри указанного диапазона.
   По умолчанию условие отмечено и задан размер файлов от 0 до 10 МБ.
   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.
7. 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".

11.3.7 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** раскройте выпадающий список и выберите **Контроль каналов передачи данных** -> **HTTP(S)**.
3. В **Действии** при срабатывании правила выберите:
   - *Создавать события для ресурсов из списков;*
   - *Не создавать события для ресурсов из списков;*
   - *Не создавать события для внутренних ресурсов* – в этом случае добавьте сегменты корпоративной сети в исключения, подробнее см. *Корпоративные сети;*
   - *Создавать события для всех ресурсов.*
4. Если выбрали одно из действий для ресурсов из списков, то укажите один или несколько ранее созданных списков, подробнее см. *Создание списка ресурсов.*
5. Определите размеры запросов, для которых будет создана теневая копия. Для этого:
   a. Активируйте **Минимальный**, укажите значение и единицы измерения. Если настройка задана, то теневое копирование будет выполняться только для запросов, размер которых больше либо равен указанному. Значение по умолчанию: 40 Б.
   b. Активируйте **Максимальный**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для запросов, размер которых меньше либо равен указанному. Значение по умолчанию: 40 МБ.
6. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Важно!

Перехват сетевого трафика, идущего через HTTPS прокси-сервер, не поддерживается.

Важно!

На компьютерах под управлением ОС семейства Linux:

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

Важно!

Агент Device Monitor под управлением ОС Windows при работе с сервером Device Monitor на ОС семейства Linux будет передавать на сервер некорректную информацию о нахождении адаптеров в корпоративной сети. Причина в том, что для корректного определения нахождения в корпоративной сети необходимо верное указание сегментов сетей, включая адреса шлюзов.

Важно!

При миграции с сервера Device Monitor с ОС Windows на ОС семейства Linux

В случае, если на Device Monitor с ОС Windows было задано только одно правило HTTP, которое исключало перехват запросов на внутренние ресурсы, то после перехода на ОС семейства Linux это правило будет означать создание событий для всех ресурсов, кроме внутренних. Например: в Device Monitor с ОС Windows существовало правило "Не создавать события для запросов на внутренние ресурсы". После миграции на ОС семейства Linux правило будет означать "Создавать события только для внешних ресурсов".

В Device Monitor с ОС Windows существовало правило "Создавать события для запросов, передаваемых по какому-либо из каналов" с указанием размеров запросов. После миграции на ОС семейства Linux правило будет означать "Создавать события для всех ресурсов" с теми же размерами.

11.3.8 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, VK+ (VK WorkSpace).

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** раскройте выпадающий список и выберите **Контроль каналов передачи данных** > **Почта**.
3. Выберите, какие действия с почтой должны быть доступны пользователю:
   - *Запретить использование почты*;
   - *Разрешить использование почты.*
4. В поле **Протокол** выберите канал, который должен контролироваться правилом:
   - *Все протоколы*;
   - *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, VK+ (VK WorkSpace);

   Примечание:

   Для перехвата почты VK+ необходимо указать хосты в меню **Настройки** > **Настройки продуктов** > **Каналы перехвата** > **Хосты для VK+**.

- MAPI/Outlook – для входящей и исходящей 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* или *MAPI/Outlook*.

   > **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. Если требуется, задайте **Максимальный размер письма**. Для этого введите его значение и единицы измерения. В этом случае теневое копирование будет выполняться только для писем, размер которых меньше либо равен указанному. По умолчанию условие отмечено и задан максимальный размер файлов 40 МБ. Чтобы создавать событие с теневой копией для писем любого размера, снимите флажок.
7. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Применение политик Traffic Monitor

- 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.
- 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.

События перехвата

Особенности создания событий перехвата почтовых сообщений:

- Набор атрибутов события перехвата веб-почты зависист от особенностей реализации конкретного веб-приложения.
- 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.

11.3.9 Правило контроля облачных хранилищ

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

- Dropbox;
- Evernote;
- Google Drive;
- 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** раскройте выпадающий список и выберите **Контроль каналов передачи данных** -> **Облачные хранилища**.
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;
     По умолчанию задано значение 1 КБ.
   - **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.
     По умолчанию задано значение 10 МБ.
6. После того, как вы определите все необходимые параметры, нажмите **Создать**.
   Правило будет действовать всегда.

11.3.10 Правило проксирования сетевого трафика

Правило проксирования сетевого трафика позволяет настроить исключение приложений из перехвата.

> **Важно!**
>
> Проксирование сетевого трафика работает только на компьютерах под управлением ОС MS Windows.
>
> Если запущенное приложение было исключено из сетевого перехвата с помощью данного правила, то последующее удаление его из этого правила не отменяет исключение. Чтобы перехват начался, приложение нужно перезапустить.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле Канал перехвата раскройте выпадающий список и выберите **Контроль каналов передачи данных** –> **Проксирование сетевого трафика**.
3. В блоке **Исключать приложения из перехвата** выберите списки в поле **Списки приложений** (о создании списков приложений см. *Создание и изменение списков приложений*). Для выбора списков вы можете воспользоваться строкой поиска.
4. После того, как вы определите все необходимые параметры, нажмите **Сохранить**. Правило будет действовать всегда.

11.3.11 Правило контроля буфера обмена

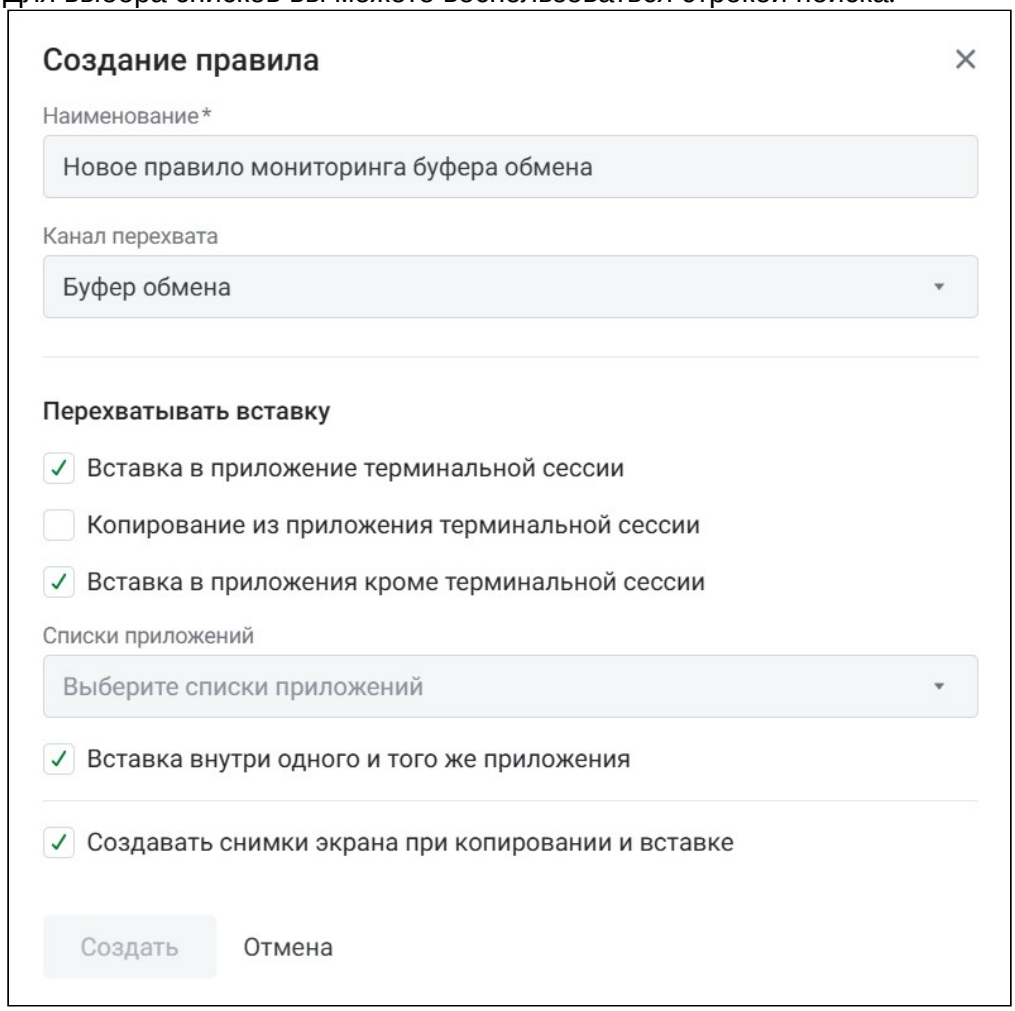
Правило позволяет контролировать доступ сотрудников к буферу обмена.

> **Важно!**
>
> Контроль буфера обмена работает на компьютерах под управлением MS Windows и ОС семейства Linux .
>
> 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** раскройте выпадающий список и выберите **Контроль каналов передачи данных** -> **Буфер обмена**.
3. В области **Перехватывать вставку** укажите, когда должно срабатывать правило. Для создания правила должна быть выбрана хотя бы одна из опций:
   - **Вставка в приложение терминальной сессии**[1]. Если выбрана эта опция, правило будет срабатывать при вставке данных в приложения терминальной сессии. При вставке данных внутри терминальной сессии правило срабатывать не будет.
   - **Копирование из приложения в терминальной сессии**[1]. Если выбрана эта опция, правило будет срабатывать при вставке данных из приложения терминальной сессии. При вставке данных внутри терминальной сессии правило срабатывать не будет.
   - **Вставка 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 **Вставка внутри одного и того же приложения**[2].
  Перехват в пределах одного приложения поддерживается, только если приложение использует системные механизмы буфера обмена.
- Для создания снимков экрана при срабатывании правила отметьте опцию **Создавать снимки экрана при копировании и вставке**[3].

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

Важно!

[1] Под приложением терминальной сессии понимается клиентское или системное приложение из поставки серверной части ПО, предоставляющее терминальный доступ:

- клиентские приложения:
  - Microsoft RDS и следующее клиентское ПО (для подключения к серверу терминалов): Remote Desktop Connection (mstsc.exe), SysInternals RDCMan, MobaXterm;
  - Remote Desktop Connection Manager;

- Citrix Receiver.
- системные приложения поддерживаются в соответствии с версией поставки ОС или версии Citrix.

На рабочих станциях под управлением ОС семейства Linux поддерживается только перехват вставки в приложения кроме терминальных сессий. Не поддерживается использование опции **Вставка внутри одного и того же приложения**. Чтобы настроить правило для ОС семейства Linux, выберите опцию **В приложения кроме терминальных сессий** и укажите список приложений Linux.

На рабочей станции под управлением ОС семейства Linux при подключении к терминальной сессии через xRDP в атрибут события **Сетевой адрес терминального клиента** может быть записан IP-адрес удаленного компьютера.

[2] Вставка внутри одного и того же приложения не поддерживается на рабочих станциях под управлением Astra Linux.

[3] Создание снимков экрана в этом правиле поддерживается только на рабочих станция под управление ОС MS Windows.

Примечание:

В случае перехвата текста на латинице длиной менее, чем 10 символов, или на кириллице менее 5 символов, текст события не будет отображен в Traffic Monitor.

11.3.12 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** раскройте выпадающий список и выберите **Мессенджеры > VK**.
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.

11.3.13 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.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Мессенджеры > Telegram**.
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.

Важно!

Не поддерживается запрет использования.

Не поддерживается перехват:

- стикеров;
- GIF-анимации;
- контактов;
- геоположения;
- каналов;
- аудиозвонков;
- опросов;
- текста, который был прикреплен в качестве ссылки.

В случае группового чата:

- На момент отправки сообщения в чат событие содержит только идентификатор и название чата; состав чата неизвестен, но может быть доступен, если наблюдаемый сотрудник просмотрел состав чата.
- Удаление участника может быть обнаружено, только если его произвел наблюдаемый сотрудник. В событиях этого же чата, получаемых от других сотрудников, состав участников остается прежним.

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

- правило позволяет перехватывать следующие версии Telegram:
  - десктоп-версию, в том числе при переименовании исполняемого модуля (Telegram.exe);
  - веб-версии: A, 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;
    - Mozilla Firefox;
    - Яндекс Браузер.
- 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. Перехват поддерживается в том числе при переименовании исполняемого модуля (Telegram.exe);
  - веб-версии: A, 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.

11.3.14 Правило контроля Яндекс Мессенджера

Правило позволяет контролировать обмен сообщениями веб- и десктоп версии и исходящими файлами веб-версии системы мгновенного обмена сообщениями Яндекс Мессенджер. Правило позволяет перехватывать новые, пересылаемые и исправленные сообщения чатов, в том числе групповых. Система перехватывает историю переписки на служебном компьютере с момента установки на него Агента Device Monitor и создания данного правила.

Важно!

Перехват веб-версии Яндекс поддерживается в следующих браузерах:

- Google Chrome;
- Microsoft Edge;
- Mozilla Firefox;
- Opera;
- Яндекс Браузер.

Не поддерживается запрет использования и перехват аудио сообщений.

В событиях группового звонка не содержится информация об участниках (получателях), которые не отправляли сообщения в групповой чат.
В случае, если одиночный звонок был переведен в групповой, не будет создано событие ни для одиночного, ни для группового звонка.

При перехвате исходящего файла в групповом чате в событии не будет наименования чата.

События для исправленных сообщений в групповом чате могут не содержать название чата.

При отправке сообщений в групповой чат, событие будет содержать идентификатор чата, а также может содержать название группового чата.

На Агентах под управлением ОС семейства Linux не поддерживается перехват десктоп-версии мессенджера.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Мессенджеры > Яндекс Мессенджер**.
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.

11.3.15 Правило контроля мессенджера WhatsApp

Правило позволяет контролировать обмен сообщениями и исходящими файлами десктоп- и веб-версии системы мгновенного обмена сообщениями WhatsApp. Правило позволяет перехватывать новые, пересылаемые и исправленные сообщения чатов, в том числе групповых. Система перехватывает историю переписки на служебном компьютере с момента установки на него Агента Device Monitor и создания данного правила.

> **Важно!**
>
> Перехват веб-версии WhatsApp поддерживается в следующих браузерах:
>
> - Google Chrome;
> - Microsoft Edge;
> - Mozilla Firefox;
> - Opera;
> - Яндекс Браузер.
>
> Не поддерживается запрет использования.
>
> Не поддерживается перехват:
>
> - аудио- и видеозвонков;
> - метаинформации контакта (никнейма);
> - файлов, пересылаемых из одного чата в другой;
> - текста, который был прикреплен в качестве ссылки.
>
> Перехват не будет осуществляться, если сотрудник вошел в веб-версию WhatsApp:
>
> - когда Агент еще не был установлен;
> - когда Агент был отключен.
>
> В этих случаях после запуска новой версии Агента необходимо очистить кеш браузера.
>
> Если Агент активируется при уже запущенном WhatsApp, он может завершить его процессы, чтобы при новом запуске WhatsApp встроить в него перехват. До тех пор пока WhatsApp не будет перезапущен, перехват осуществляться не будет.
>
> При запуске сервера анализа (процесс IWProxy) все обнаруженные процессы WhatsApp могут быть принудительно завершены.

При перехвате фото- и видеофайлов, событие может содержать не оригинальный файл, а его превью. В этом случае имя файла будет иметь формат `"Embedded <Тип содержимого: image/video> <Время отправки данных в миллисекундах>"`.

Если перехвачено несколько сообщений с одинаковым текстом и отправителем, отправленных с разницей порядка 3 секунд, то для них будет сформировано одно событие. Дублирующие события созданы не будут.

При отправке сообщений в групповой чат WhatsApp, событие будет содержать идентификатор чата и название группового чата.
События для исправленных сообщений в групповом чате могут не содержать название чата.

На Агентах под управлением ОС семейства Linux не поддерживается перехват файлов.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Мессенджеры > WhatsApp**.
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.

11.3.16 Правило контроля мессенджера MAX

Правило позволяет контролировать обмен сообщениями и файлами на толстом клиенте и в веб-версии системы мгновенного обмена сообщениями MAX.

Важно!

Не поддерживается перехват:

- исправленных сообщений;
- ответных сообщений (т.е. прикрепленных к исходным);

- аудиосообщений;
- входящих файлов;
- файлов, пересылаемых из одного чата в другой;
- истории сообщений;
- опросов.

Если после исходящих сообщений не было входящих, в качестве получателя в событии отображается текущий пользователь мессенджера.

Если сотрудник загрузил файл, но не отправил его, при закрытии мессенджера Система сформирует событие попытки загрузки файла. В качестве отправителя и получателя будет указан текущий пользователь мессенджера.

Если сотрудник попытался загрузить файл, не поддерживаемый мессенджером, при закрытии мессенджера Система сформирует событие попытки загрузки файла с неполной теневой копией. В качестве отправителя и получателя будет указан текущий пользователь мессенджера.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Контроль мессенджеров** > **MAX**.
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.

11.3.17 Правило контроля протокола XMPP

Правило позволяет контролировать обмен входящими и исходящими текстовыми сообщениями по протоколу **XMPP**.

Чтобы создать и настроить правило:

1. Откройте окно создания правила (see "Создание правил") и в поле **Наименование** укажите название правила.

2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Мессенджеры > XMPP**.
3. В поле **Действие** по умолчанию выбрано **Перехватывать сообщения**. Если вы хотите запретить обмен сообщениями по протоколу XMPP на компьютере с Агентом Device Monitor, выберите опцию **Запретить использование**.

> **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.

11.3.18 Правило контроля создания снимков экрана

Правило позволяет запрещать создание сотрудниками снимков экрана.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Контроль использования** -> **Запрет создания снимков экрана**.
3. В блоке **Запрещать сотруднику создавать снимок экрана** выберите, когда должно срабатывать правило. Для создания правила должна быть выбрана хотя бы одна из опций:
   - **Всегда**.
   - **Если запущены приложения**. Если выбрана эта опция, правило будет срабатывать для указанных приложений.
4. В случае выбора работы правила при использовании приложений, в поле **Списки приложений** выберите приложения, для которых будет срабатывать правило.

> **Примечание:**
>
> Возможно добавить только приложения Windows.

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

> **Примечание:**
>
> Поддерживается запрет создания снимков экрана с помощью нажатия клавиши PrtScr или комбинации клавиш PrtScr+Alt.

11.3.19 Правило мониторинга экрана

Правило позволяет создавать снимки экрана в формате PNG при смене активного окна любых приложений. Снимки создаются для всех мониторов, подключенных к незаблокированному контролируемому компьютеру.

> **Примечание:**
>
> Правило доступно для рабочих станций под управлением ОС Windows и ОС семейства Linux.
>
> На рабочей станции под управлением ОС семейства Linux при подключении к терминальной сессии через xRDP в атрибут события **Сетевой адрес терминального клиента** может быть записан IP-адрес удаленного компьютера.

> **Примечание:**
>
> Настройте правило мониторинга активности сотрудника, чтобы отправлять события со снимками экрана в InfoWatch Activity Monitor.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Мониторинг активности пользователей -> Автоматическое создание снимков экрана**.
3. Определите, в каком случае правило будет действовать. Возможные значения:
   - **Создавать снимки экрана для любых приложений или ресурсов**;
   - **Создавать снимки экрана для приложений или ресурсов из списка**;
   - **Не создавать снимки экрана для приложений или ресурсов из списка**.
4. Если выбрано действие, учитывающее списки приложений или ресурсов, укажите их в появившихся полях.
   Подробнее о создании списков приложений и ресурсов см. "Раздел "Ресурсы"".

   > **Важно!**
   >
   > Проверка на соответствие посещаемого ресурса ресурсу из списка производится, только если пользователь работает в браузерах:
   >
   > - Chrome;
   > - Яндекс Браузер;
   > - Mozilla Firefox;
   > - Edge (Chromium);
   > - Opera;
   > - IE.

5. 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.

Важно!

Вы также можете определить работу правила в зависимости от активности на контролируемых компьютерах. Для этого в общих настройках каналов перехвата задайте параметр **Не создавать снимок экрана, если мышь/клавиатура неактивны более...** (см. Каналы перехвата).

На рабочих станциях под управлением ОС семейства Linux Система может определить смену вкладки браузера только если сотрудник работает в следующих браузерах: Яндекс Браузер, Edge (Chromium).

На рабочих станциях под управлением ОС Astra 1.7 и 1.8 Система не определяет открытие нового документа в офисных многооконных приложениях, например, в LibreOffice.

6. 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.

Примечание:

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

Примечание:

О том, как во время создания снимка выбирается приоритет применения правила, см. в статье базы знаний "Определение приоритетов при создании снимка экрана по правилу мониторинга экрана".

11.3.20 Правило мониторинга ввода текста с клавиатуры

Правило позволяет перехватывать ввод текста с клавиатуры и сочетания клавиш 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 MS Windows и ОС семейства Linux.

На рабочей станции под управлением ОС семейства Linux при подключении к терминальной сессии через xRDP в значение атрибута события **Сетевой адрес терминального клиента** может быть записан IP-адрес удаленного компьютера.

По умолчанию перехватывается ввод текста и/или сочетания клавиш 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** раскройте выпадающий список и выберите **Мониторинг активности пользователей > Ввод текста с клавиатуры**.
3. Выберите одно из действий правила:
   - **Перехватывать ввод текста во всех приложениях и ресурсах**.
   - **Перехватывать ввод текста для приложений и ресурсов из списка** – Device Monitor будет создавать событие при вводе текста в активном окне приложений из списка.
   - **Не перехватывать ввод текста для приложений и ресурсов из списка** – Device Monitor **не** будет создавать событие при вводе текста в активном окне приложений из списка.

     Примечание:

     Поддерживается использование только списков для ОС MS Windows.

4. Если выбрано действие, учитывающее списки приложений и ресурсов, в появившихся полях укажите их.
   Подробнее о создании списков приложений и ресурсов см. "Создание и изменение списков приложений", "Создание и изменение списков ресурсов".
5. Если требуется, включите опцию **Создавать снимок экрана при создании события**.
   Настройка и применение правила мониторинга ввода текста с клавиатуры и правила мониторинга 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!

- Перехват текста с клавиатуры корректно работает для русского и английского языков. При добавлении других языков требуется перезагрузка рабочей станции.
- Для Агента на рабочей станции под управлением **ОС семейства Linux** 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.

Система сгенерирует одно событие на ввод текста в приложении, а не на каждую вкладку.

- Для Агента на рабочей станции под управлением **ОС Альт 11** (с графической оболочкой Wayland) или **Astra Linux**, если при вводе текста пользователь зажал символ, Система перехватывает данный символ в единственном экземпляре. **Пример:** Текст "*exaaample*", в котором повторяющийся символ вводился не последовательным нажатием, а посредством зажатия клавиши, будет перехвачен как "*example*".
- Для Агента на рабочей станции под управлением **ОС Astra Linux** Система не перехватывает текст, вводимый в стандартный менеджер текста, если текст начинается со слеша, например "*/sample/text*".
- Для Агента на рабочей станции под управлением **ОС Альт 11** (с графической оболочкой Wayland) после обновления на версию 7.21 или более позднюю перехват доступен только после перезапуска пользовательской сессии.

11.3.21 Правило мониторинга 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 и ОС семейства Linux.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Мониторинг активности пользователей > Активность сотрудника**.
3. В разделе **Типы статистики** выберите, какие действия пользователя необходимо контролировать (список контролируемых действий для каждого типа см. ниже):
   - **Контролировать активность**
   - **Контролировать действия с файлами**
   - **Контролировать печать**
4. Если при контроле каких-либо действий пользователя не требуется собирать статистические данные, отметьте **Отключить сбор**. События, сформированные в Device Monitor, не будут отправляться в Платформу.
5. 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*).

> **Примечание:**
>
> Если вы хотите, чтобы какие-либо события (например, события создания снимков экрана по Правилу мониторинга экрана) отправлялись в Платформу, даже если отключен сбор статистики, задайте значение `False` полю `SEND_EVENT_TO_PLATFORM_WITH_CHECK` таблицы Settings базы данных. По умолчанию данное поле имеет значение `True`.

На рабочей станции под управлением ОС семейства Linux при подключении к терминальной сессии через xRDP в атрибут события **Сетевой адрес терминального клиента** может быть записан IP-адрес удаленного компьютера.

Контроль действий

Контроль активности

Система контролирует следующие действия пользователя:

- вход в сессию (локальный, удаленный);
- выход из сессии (локальный, удаленный);
- блокировка сессии (локальная, удаленная);
- разблокировка сессии (локальная, удаленная);
- запуск приложения;
- остановка приложения;
- получение и потеря фокуса активного окна;
- переключение между приложениями;
- переключение между вкладками в браузере. Поддерживаются следующие браузеры:
  - Chrome
  - Яндекс Браузер
  - Mozilla Firefox
  - Edge (Chromium)
  - Opera
  - IExplore
- выполнение поисковых запросов. Поддерживаются следующие поисковые системы:
  - Google
  - Яндекс
- использование мыши и клавиатуры.

Примечание:

- Если Агент запускается после логина пользователя, то для такого пользователя не будет сформировано событие Входа в систему, будет только Выход из системы/блокировка.
- Если на рабочую станцию вошли несколько пользователей, то при ее выключении/перезагрузке событие Выход из системы будет сформирован только для того пользователя, который вошел первым.
- События получения/потери фокуса для UWP (Universal Windows Platform) приложений могут быть не созданы.
- Для статистических событий по работе с веб-сайтами в браузере и веб-поиска, атрибут *сайт* может иметь значение "about:blank", если структура URL не соответствует домену или IP-адресу сайта.
- Если в Системе одновременно настроено *Правило контроля создания снимков экрана* и сбор статистики, то при нажатии клавиши **Print Screen** будет сформировано только событие отпускания клавиши.

- Статистика использования мыши и клавиатуры создается каждые 15 минут (неизменяемый параметр) или при смене фокуса активного окна. Если в течение 15 минут действий не было, событие не будет создано.
- При удерживании клавиши Агент будет генерировать множество событий нажатия и одно событие отпускания клавиши.

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 вкладки браузера (для браузера Edge (Chromium));
- выполнение поисковых запросов (для браузеров Edge (Chromium) и Mozilla Firefox).

Для операционных систем ОС Альт и ОС Astra Linux контролируются такие же действия пользователя, как для системы РЕД ОС, за исключением получения фокуса вкладкой браузера.

Для Агента на рабочей станции под управлением **ОС Альт 11** (с графической оболочкой Wayland) после обновления на версию 7.21 или более позднюю перехват переключения окон приложений доступен только после перезапуска пользовательской сессии.

Примечание:

На рабочих станциях под управлением РЕД ОС:

- Если URL-адрес был изменен (без применения или отмены изменений при помощи клавиш **Enter** или **Esc**), то будет создано событие смены вкладки браузера.
- Если сайт был добавлен из вкладки браузера в закладки, создается событие смены вкладки браузера.
- Если URL был изменен, может быть создано несколько событий смены вкладки браузера.
- Событие *Локального выхода из сессии* может не быть сформировано в случае:
  - перезагрузки/выключения рабочей станции с помощью кнопок **Перезагрузить**/**Выключить** меню **Пуск**.
  - перезагрузки/выключения рабочей станции через консоль с помощью команд shutdown, reboot и им подобных.

Контроль действий с файлами

Важно!

Контроль действий с файлами доступен только для Агентов под управлением ОС Windows.

Система контролирует следующие действия пользователя:

- создание файла;
- открытие файла;
- переименование файла;
- перемещение файла/папки;
- копирование файла/папки;
- удаление файла/папки;
- перемещение файла/папки в корзину;
- восстановление файла/папки из корзины;
- удаление файла/папки из корзины.

Примечание:

- Событие может быть создано в случае, если копирование/удаление/перемещение файла/папки было инициировано, а затем отменено.
- Если Система не может определить оригинальное имя файла при его удалении из корзины, в событии будет указано имя файла, отображаемое в корзине. Оригинальное имя файла – это имя файла до перемещения в корзину (если ОС изменяет его при перемещении).
- События для подпапок и пустых папок не создаются.
  Пример:

  Папка содержит 4 файла и вложенную папку с 2 файлами. При действии с родительской папкой будет создано событие для родительской папки и 6 событий для файлов. Событие для подпапки создано не будет.
- Данные о размере файла извлекаются из контекста файлового объекта. Если Система не получила эти данные, в значении размера файла будет указано значение 0.

Сбор статистики по работе с файлами производится для следующих источников:

- компьютер;
- съемные устройства;
- сетевые ресурсы;
- терминальная сессия.

Важно!

Сбор статистики работы с файлами не поддерживается для FTP, HTTP, Cloud Storage.

Контроль печати

Важно!

Контроль печати доступен только для Агентов под управлением ОС Windows.

Система контролирует отправку файлов на печать для следующих типов принтеров:

- локальный;
- сетевой;
- терминальный.

Система собирает данные о количестве копий документа, отправленного на печать, а также о количестве страниц каждой копии.

Примечание:

Количество копий документа не всегда может быть указано точно.

11.3.22 Правило мониторинга звукового окружения

Правило позволяет отслеживать действия сотрудника при помощи контроля звукового окружения рабочей станции данного сотрудника, формировать события и отправлять их в Activity Monitor.

В правиле вы можете настроить:

- **Источник звукового окружения** – вы можете выбрать один или два типа источника звукового окружения: микрофон и/или динамики.
- **Перехват из списка ресурсов ресурсов** – запись звукового окружения при использовании выбранных ресурсов.
- **Перехват активности сессии** – запись звукового окружения в течение всего периода рабочей сессии, с момента входа пользователя в систему до момента выхода. При блокировке рабочей станции запись звукового окружения не прерывается.

Важно!

Для формирования и отправки событий записи звукового окружения в Activity Monitor необходимо также настроить *Правило мониторинга активности сотрудника*.

Примечание:

Правило применяется на агентах под управлением операционной системы MS Windows.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле Канал перехвата раскройте выпадающий список и выберите **Мониторинг активности пользователей** > **Звуковое окружение**.

3. Выберите, с какого типа источника вести запись звукового окружения:
   - *Микрофон*
     и/или
   - *Динамики*
     Если к рабочей станции подключено несколько устройств одного типа, то для ведения записи среди них будет выбрано одно с самой большой амплитудой аудиосигнала.
4. При необходимости добавьте ресурсы для перехвата в поле **Списки ресурсов**.
   Вы можете настроить продолжительность ведения записи в настройках. Подробнее см. *Каналы перехвата*.
5. Если вы хотите включить перехват активности сессии, включите опцию **Записывать звуковое окружение при входе в сессию**.

   Важно!

   Запись звукового окружения на нескольких десятках рабочих станций может значительно повысить нагрузку на систему.

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

Вы также можете настроить продолжительность ведения записи, а также исключить из записи периоды тишины. Подробнее см. *Каналы перехвата*.

Примечание:

- одна и та же запись может относиться к нескольким событиям одновременно. Если пользователь последовательно посещает несколько разных ресурсов, для которых срабатывает правило, то запись ведется непрерывно, но создаются отдельные события для разных ресурсов;
- при проведении конференции осуществляется запись не голоса, а звуков вокруг рабочей станции;
- если во время срабатывания правила произошло что-то, что не позволяет записывать звук (например, отключился микрофон), то событие может содержать аудиозапись без звука (при воспроизведении слышна тишина);
- проверка на соответствие посещаемого ресурса ресурсу из списка производится только если пользователь работает в браузерах:
  - Chrome;
  - Яндекс.Браузер;
  - Mozilla Firefox;
  - Edge (Chromium);
  - Opera.
- при выходе из системы через меню *Пуск* процесс перехвата звукового окружения принудительно завершается операционной системой. В связи с этим последний фрагмент аудиоданных не может быть перехвачен. Длительность данного фрагмента составляет не более 1 минуты;
- запись звукового окружения ведется при заблокированной сессии;

- для агентов под управлением ОС Windows 11 и позднее факт записи аудио будет скрыт от пользователя. Иконка микрофона будет скрыта даже в том случае, если микрофон уже используется другим приложением;
- захват микрофона другими приложениями в эксклюзивном режиме невозможен;
- если пользователь использует Bluetooth-гарнитуру для воспроизведения звука, перехват звука через микрофон гарнитуры может привести к остановке воспроизведения. Дальнейшее воспроизведение звука во время перехвата будет доступно в более низком качестве, через профили Hands-Free Profile (HFP) или Headset Profile (HSP).

11.3.23 Правило записи видео с экрана

Правило позволяет отслеживать следующие действия сотрудника с помощью записи видео экрана рабочей станции:

- вход на веб-сайт, заданный в правиле;
- использование приложения, заданного в правиле;
- использование буфера обмена в приложении, заданном в правиле;
- ввод текста в приложении, заданном в правиле.

При срабатывании правила Система формирует события и отправляет их в Activity Monitor.

Важно!

Для формирования и отправки событий видеозаписи в Activity Monitor необходимо также настроить *Правило мониторинга активности сотрудника*.

Примечание:

Правило применяется на компьютерах под управлением операционной системы MS Windows.

Не поддерживается работа правила на агенте под управлением ОС Windows 7.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Мониторинг активности пользователей** > **Запись видео с экрана**.
3. В поле **Списки ресурсов** выберите ресурсы, при использовании которых должно срабатывать правило (подробнее о создании списков см. *Создание списка ресурсов*).
4. Далее выберите условия срабатывания правила в приложении:
   - Использование приложения;
   - Ввод текста;
   - Использование буфера обмена.
5. В поле **Списки приложений** выберите приложения, при использовании которых должно срабатывать правило (подробнее о создании списков см. *Создание и изменение списков приложений*).
6. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Вы можете настроить продолжительность ведения записи в настройках. Подробнее см. *Каналы перехвата*.

Примечание:

- в связи с особенностями работы технологии захвата видео на агенте длительность видеозаписи экрана может отличаться от заданного времени в меньшую сторону;
- смещение старта захвата видео может не соответствовать продолжительности предыдущего видео;
- видеозапись производится со всех доступных экранов;
- одна и та же видеозапись может относиться к нескольким событиям одновременно. Если пользователь последовательно посещает несколько разных ресурсов, для которых срабатывает правило, то запись ведется непрерывно, но создаются отдельные события для разных ресурсов;
- при срабатывании правила производится только видеозапись. Запись звукового окружения рабочей станции недоступна;
- запись видео производится с момента входа пользователя в сессию или разблокировки экрана и до выхода из сессии или блокировки экрана пользователя;
- при перехвате с использованием буфера обмена запись производится при любом обращении из приложения к буферу обмена. Т.е., если приложение может самостоятельно записывать информацию в буфер обмена или извлекать ее из него, это будет распознано как действие пользователя и начнется запись;
- при вводе текста в приложении запись начинается с ввода первого символа и продолжается до смещения фокуса из приложения, либо до истечения предельного времени записи;
- Если выбран перехват приложений при "Вводе текста"

запись производится при нажатии в поле ввода:	запись не производится при нажатии в поле ввода:
• сочетаний клавиши Ctrl и букв, например, Ctrl+a, Ctrl+t и т.д.; • функциональных клавиш, например, Esc, Backspace, Enter, Tab и т.д.; • клавиш без ввода в какое-либо поле.	• клавиш навигации, например, PgUp, PgDown, Home и т.д.; • клавиш F1-F12; • клавиши Delete; • сочетаний клавиш, которые обращаются не к приложению, например, Alt + F4.

11.3.24 Правило контроля файлов в приложениях

Правило позволяет перехватывать события чтения и/или записи файлов в приложении, если Офицер безопасности создал хотя бы одно правило перехвата.

Важно!

При одновременном перехвате событий чтения и записи одного файла, приоритет имеет операция записи.

Примечание:

- перехват файлов будет осуществляться по заданному в профиле приложения расширению, даже если путь к файлу находится в исключениях (подробнее о профиле приложения см. «Универсальный перехватчик файлов»);
- перехват файлов будет осуществляться по заданному в профиле приложения пути, даже если расширение файла находится в исключениях (подробнее о профиле приложения см. «Универсальный перехватчик файлов»).

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** раскройте выпадающий список и выберите **Универсальный перехватчик файлов → Контроль файлов в приложениях**.
3. В поле **Приложение** выберите профиль приложения из списка (подробнее о создании профиля приложения см. «Универсальный перехватчик файлов»).
4. Выберите **Создавать снимки экрана при формировании события** и/или **Формировать теневую копию**, если эти действия необходимы при перехвате событий.

   Примечание:

   Если действие **Формировать теневую копию** не было выбрано, но размер отправленного в приложении файла превышает 50 МБ, то события отправки таких файлов создаются без теневой копии.

5. Укажите условия для формирования событий:
   a. Выберите операцию **Чтение** и/или **Запись**.
   b. Отметьте и укажите **Маску файлов**, чтобы применить правило для подходящих под нее файлов. Вы можете использовать групповые символы:
      - ? – один неизвестный символ;
      - * – любое количество символов.
   c. Вы можете ограничить применение правила определенной категорией файлов, для этого отметьте поле и выберите **Категорию файла** из выпадающего списка.

      Примечание:

      Вы можете ознакомиться с категориями файлов в разделе **Раздел "Ресурсы"**, а также в статье базы знаний "Перехватываемые расширения файлов в Device Monitor (для правил с выбором Категории файла)".

Если вы указали и маску файлов, и категорию, для срабатывания правила должны выполниться оба указанных условия.

На компьютерах под управлением ОС семейства Linux категории расширений не учитываются – правило сработает на копирование любых файлов, вне зависимости от указанных категорий файлов.

d. Задайте **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.
По умолчанию условие отмечено и задан размер файлов от 0 до 10 МБ.
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.

11.4 Создание и изменение списков приложений

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

11.4.1 Создание списка приложения

Чтобы создать список приложений:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. В разделе **Ресурсы** откройте вкладку **Списки приложений**.
3. Слева в секции **Списки приложений** нажмите .
4. В окне **Создание списка приложений**:
   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 
5. Нажмите **Создать**.
6. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

11.4.2 Добавление приложений в список

Чтобы наполнить список, вы можете:

- Добавить приложение вручную;
- Добавить в список обнаруженное приложение (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. Перейдите в Центр администрирования, нажав  на панели навигации.
2. В разделе **Ресурсы** откройте вкладку **Списки приложений**.
3. Слева в секции **Списки приложений** кликните список, в который вы хотите добавить приложение.
4. Нажмите **Создать приложение**:
   - в правом верхнем углу;
   - в окне списка, если список пустой.
5. В окне **Создание приложения** укажите:
   - **Описание**;
   - Для ОС Windows:
     - **Имя приложения** – имя исполняемого файла с расширением, например *notepad.exe*;
     - **Расположение исполняемого файла** – абсолютный (полный) путь к папке, содержащей исполняемый файл, например *C:\Windows\System32*. При указании пути вы можете использовать переменные окружения;
     - **Издатель** – Organization (O), Location (L), State (S), Country (C) из свойств;
     - **Название продукта** – необязательный параметр. Поле доступно, если указан **Издатель**.
   - Для ОС Linux:
     - **Имя приложения** – имя (без дополнительных символов), соответствующее запускаемому процессу, например *pluma*;
     - **Расположение исполняемого файла** – абсолютный (полный) путь к папке, содержащей исполняемый файл, например */usr/bin/*. При указании пути вы можете использовать переменные окружения.
6. После заполнения полей нажмите **Создать**.
7. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

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.

Добавление обнаруженных приложений в список

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

Чтобы добавить обнаруженное приложение:

1. В консоли управления Device Monitor перейдите в раздел **Ресурсы** > **Списки приложений**.
2. Откройте список **Обнаруженные**.
3. Выберите одно или несколько приложений .
4. На появившейся внизу экрана плашке нажмите **Добавить в список приложений**.
5. В открывшемся диалоговом окне выберите список, в который необходимо добавить приложение.
6. Нажмите **Сохранить**. В правом верхнем углу Система отобразит уведомление о том, что приложения были добавлены.
7. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

или

1. В списке приложений наведите курсор на строку приложения справа и нажмите **Добавить приложение в список**.
2. В открывшемся диалоговом окне выберите список, в который необходимо добавить приложение.
3. Нажмите **Сохранить**. В правом верхнем углу Система отобразит уведомление о том, что приложение были добавлено.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Примечание:

Если из списка обнаруженных 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 приложения:

1. Нажмите  напротив приложения, а затем выберите  **Скопировать**
   или
   отметьте одно или несколько приложений  и внизу рабочей области нажмите .
2. В окне **Копирование приложений** выберите список, в который хотите скопировать приложения.
3. Нажмите **Скопировать в список**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы переместить приложения:

1. Нажмите  напротив приложения, а затем выберите  **Переместить**
   или
   отметьте одно или несколько приложений  и внизу рабочей области нажмите .
2. В окне **Перемещение приложения** выберите список, в который хотите переместить приложения.
3. Нажмите **Переместить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

11.4.3 Редактирование и удаление списков и приложений

Чтобы отредактировать список или приложение:

1. Выберите необходимый элемент.
2. Нажмите  напротив него, а затем выберите  **Редактировать**.
3. В окне редактирования внесите правки и нажмите **Сохранить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы удалить список или приложения:

1. Нажмите  напротив удаляемого элемента, а затем выберите  **Удалить**
   или
   отметьте одно или несколько приложений  и внизу рабочей области нажмите .
2. В окне подтвердите действие, нажав **Удалить**.
3. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

> **Примечание:**
>
> Список приложений нельзя удалить, если он используется в правиле политики.

11.5 Создание и изменение списков ресурсов

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

Информация по работе с ними содержится в подразделах:

- Добавление списка ресурсов
- Редактирование списка ресурсов
- Удаление списка ресурсов

11.5.1 Создание списка ресурсов

Чтобы создать список ресурсов:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. Перейдите на вкладку **Списки веб-ресурсов** раздела **Ресурсы**.
3. Слева, в области **Списки ресурсов**, нажмите .
4. Введите имя списка ресурсов.
5. Нажмите **Создать**.
6. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы добавить ресурсы в созданный список:

1. Нажмите 

.
2. Выберите тип идентификации: **домен**, **URL** или **URL содержит**. Для вызова справки по типам идентификации наведите курсор на  в поле **Тип идентификации**.
3. Введите ресурс и его описание.
4. Нажмите **Создать**.
5. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Определение соответствия посещаемого ресурса ресурсу из списка

Система определяет соответствие посещаемого ресурса ресурсу из списка по следующему принципу:

1. Для типа **Домен**:

Выполняется проверка на точное совпадение *<хост>,* включая поддомены. Регистр не учитывается.

Пример: Если в списке задан ресурс *example.com*, то ресурсы *one.example.com* или *ExamPle.com* будут считаться соответствующими ресурсу из списка. Но ресурс *example1.com* не будет соответствовать заданному в списке значению.

2. Для типа **URL**:

- если URL в списке содержит только домен, выполняется проверка на точное совпадение *<хост>* без учета поддоменов;
- если URL в списке содержит параметры и якорь (есть разделители /, ?, #), выполняется проверка на точное совпадение *<хост> <порт>* и *[/<URL-путь>][?<параметры>] [#<якорь>]* ;
- если URL в списке содержит порт, выполняется проверка на точное совпадение с учетом порта;

- если URL в списке не содержит порт, выполняется проверка только на точное совпадение.

Регистр учитывается везде кроме части *<хост>*.

Пример: Если в списке задан ресурс *example.com/example?example#example*, то ресурс *EXAMPLE.com/example?example#example* будет считаться соответствующим ресурсу из списка. Но ресурсы *one.example.com*, *one.example.com/example* и *example.com:8080/example?example#example* не будут соответствовать заданному в списке значению.

3. Для типа **URL содержит**:

Выполняется проверка на совпадение текста, введенного в списке, с текстом в любой части URL (по подстроке) *<хост>[:<порт>]][/<URL-путь>][?<параметры>][#<якорь>]*, включая поддомены. Регистр не учитывается.

Пример: Если в справочнике задан ресурс *example*, то ресурс *one.com/example?example#example* будет считаться соответствующим ресурсу из списка. Но ресурс *one.com/one?onet#o* не соответствует заданному в списке значению, так как URL не содержит подстроки *example*.

Важно!

Определение соответствия ресурсов имеет следующие особенности:

- Технологии определения URL ресурса, отображаемого в текущей активной вкладке поддерживаемого приложения (интернет-браузера), основаны на анализе элементов графического интерфейса приложений. Поэтому определенный URL может не полностью соответствовать фактическому URL ресурса, к которому обратилось приложение;
- Отсутствует преобразование имени ресурса в IP-адрес;
- Отсутствует обратное преобразование имени ресурса, если оно было задано в виде IP-адреса;
- Отсутствует преобразование символов, закодированных при помощи схемы Punycode (https://tools.ietf.org/html/rfc3492);
- Система определяет соответствие посещаемого ресурса ресурсу из списка, только если Пользователь работает в следующих браузерах:
  - Chrome;
  - Яндекс.Браузер;
  - Mozilla Firefox;
  - Edge (Chromium);
  - Opera;
  - IE.

11.5.2 Редактирование списка ресурсов

Для изменения списка ресурсов перейдите на вкладку **Списки веб-ресурсов** раздела **Ресурсы**.

Чтобы изменить имя списка ресурсов:

1. В области **Списки ресурсов** выберите список, который хотите изменить, кликнув по нему левой кнопкой мыши.
2. Напротив выбранного списка нажмите  и выберите **Редактировать**.
3. В открывшемся окне отредактируйте имя списка.

4. Нажмите **Сохранить**.
5. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы отредактировать ресурс из списка:

1. В области **Списки ресурсов** выберите список.
2. Выберите ресурс, который хотите изменить, кликнув по нему левой кнопкой мыши.
3. Нажмите  напротив него и выберите **Редактировать**.
4. В открывшемся окне внесите необходимые изменения.
5. Нажмите **Сохранить**.
6. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы скопировать / переместить ресурс из одного списка в другой:

1. В области **Списки ресурсов** выберите список, содержащий ресурс.
2. Выберите ресурс, который хотите скопировать / переместить.
3. Напротив него нажмите  и выберите **Скопировать** / **Переместить**
   или
   внизу центральной области нажмите  / .
4. В открывшемся окне выберите список, в который необходимо скопировать / переместить ресурс.
5. Нажмите **Копировать**.
6. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Также вы можете скопировать / переместить сразу несколько ресурсов, выбрав их и нажав  / .

Чтобы удалить ресурс из списка:

1. В области **Списки ресурсов** выберите список.
2. Выберите ресурс, который хотите удалить.
3. Напротив него нажмите  и выберите **Удалить**
   или
   внизу центральной области нажмите .
4. В открывшемся окне подтвердите удаление.
5. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Также вы можете удалить сразу несколько ресурсов, выбрав их и нажав .

11.5.3 Удаление списка ресурсов

Чтобы удалить список ресурсов:

1. Перейдите на вкладку **Списки веб-ресурсов** раздела **Ресурсы**.
2. В области **Списки ресурсов** выберите список, который хотите удалить, кликнув по нему левой кнопкой мыши.
3. Напротив выбранного списка нажмите  и выберите **Удалить**.

4. В открывшемся окне подтвердите удаление.
5. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

11.6 Создание и изменение категорий файлов

При настройке правил контроля файловых операций вы можете указать категорию файлов в качестве условия формирования события.

Чтобы просмотреть существующие категории, перейдите в раздел **Раздел "Ресурсы"** > **Категории файлов** и в области **Категории файлов** выберите интересующую. В рабочей области будет отображен перечень расширений, входящих в состав выбранной категории.

> **Важно!**
>
> Предустановленные категории файлов редактированию и удалению не подлежат. Создание расширений файлов не предусмотрено.

11.6.1 Создание категории файлов

Чтобы создать категорию файлов:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. В разделе **Ресурсы** откройте вкладку **Категории файлов**.
3. Слева в области **Категории файлов** нажмите .
4. Введите наименование категории файлов.
5. Нажмите **Добавить**.
6. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").
7. Чтобы добавить расширения файлов в созданную категорию, скопируйте их из предустановленных или других созданных вами категорий файлов.

11.6.2 Изменение состава категории файлов

Чтобы скопировать расширения из одной категории в другую:

1. Выберите категорию, которая содержит расширения, которые нужно скопировать.
2. В рабочей области наведите курсор на расширение, нажмите , затем  **Скопировать в другой список**.
   или
   отметьте одно или несколько расширений  и внизу рабочей области нажмите .
3. В открывшемся окне выберите категорию из выпадающего списка.
4. Нажмите **Выбрать**.
5. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы исключить расширения из категории файлов:

1. Выберите категорию, из которой нужно исключить расширения.
2. В рабочей области наведите курсор на расширение, нажмите , затем  **Удалить**.
   или
   отметьте одно или несколько расширений  и внизу рабочей области нажмите .
3. В открывшемся окне подтвердите удаление.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

11.6.3 Редактирование и удаление категории файлов

Чтобы изменить имя категории файлов:

1. Выберите категорию, которую хотите изменить, кликнув по ней левой кнопкой мыши.
2. Нажмите , затем  **Редактировать**.
3. В окне редактирования внесите правки и нажмите **Сохранить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы удалить категорию файлов:

1. Выберите категорию, которую хотите удалить, кликнув по ней левой кнопкой мыши.
2. Нажмите , затем **Удалить**.
3. В открывшемся окне подтвердите удаление.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

11.7 Работа с группами компьютеров

Политики безопасности можно назначать группам компьютеров. Работа с группами компьютеров осуществляется в разделе **Группы** Центра администрирования и включает в себя:

- Создание и редактирование групп компьютеров
- Настройку состава групп компьютеров
- Просмотр сведений о компьютерах
- Просмотр результирующей политики компьютера

11.7.1 Создание и редактирование групп компьютеров

Важно!

При регистрации нового компьютера, 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. "Синхронизация".

Чтобы добавить группу компьютеров:

1. Перейдите в **Центр администрирования**, нажав  на панели навигации.
2. Откройте вкладку **Группы > Компьютеры**.
3. На панели **Группы** нажмите .
4. Укажите следующие параметры:
   - **Наименование** группы;
   - **Политика**. Выберите из раскрывающегося списка политику, которая будет назначена данной группе компьютеров.
5. Нажмите **Добавить**. Будет создана новая группа компьютеров, в которую необходимо добавить компьютеры.
6. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы отредактировать группу компьютеров:

1. Выделите нужную группу и нажмите  справа от ее названия.
2. Выберите **Редактировать** и внесите изменения.
3. Нажмите **Сохранить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы найти компьютер или группу компьютеров:

1. В верхней части рабочей области введите в строку поиска текст запроса, состоящий хотя бы из 3 символов.
   В раскрывшемся списке будут показаны первые 5 компьютеров и первые 5 групп компьютеров, параметры которых включают введенный текст.
2. Выберите результаты поиска для отображения:
   - Чтобы просмотреть все элементы, удовлетворяющие запросу, нажмите **Enter** или **Смотреть все результаты**. Результаты будут отображены в иерархическом списке в области слева, найденные группы при этом будут выделены синим цветом.
     Если одним из результатов поиска является группа, то будут показаны все входящие в нее элементы, в том числе не подходящие под условие поиска.
   - Чтобы перейти к одному элементу, нажмите на группу или компьютер. В рабочей области откроется выбранная группа или группа, включающая выбранный компьютер.

Важно!

Если не осуществляется поиск объектов с использованием кириллицы, убедитесь, что для базы данных, с которой взаимодействует сервер Device Monitor, установлена русская локаль (`ru_RU.utf8`). Подробнее см. статью Базы знаний "Проверка и изменение локали базы данных PostgreSQL".

Чтобы отменить фильтр, примененный с помощью поиска, нажмите  в строке поиска.

Чтобы удалить группу компьютеров:

1. Выделите группу для удаления и нажмите  справа от ее названия.

   > **Примечание.**
   >
   > Группу компьютеров «по умолчанию» удалить нельзя.

2. Нажмите **Удалить**. 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 **Удалить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

11.7.2 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 **Центр администрирования**, нажав  на панели навигации.
2. Откройте вкладку **Компьютеры** в разделе **Группы**.
3. 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.

   > **Примечание:**
   >
   > Чтобы найти группу в списке, вы можете воспользоваться поиском. Подробнее см. "Создание и редактирование групп компьютеров".

4. Откройте окно **Настройка состава группы компьютеров** одним из способов:
   - В правом верхнем углу рабочей области нажмите  **Настроить состав группы**.
   - Справа от названия группы нажмите  >  **Настроить состав группы**.

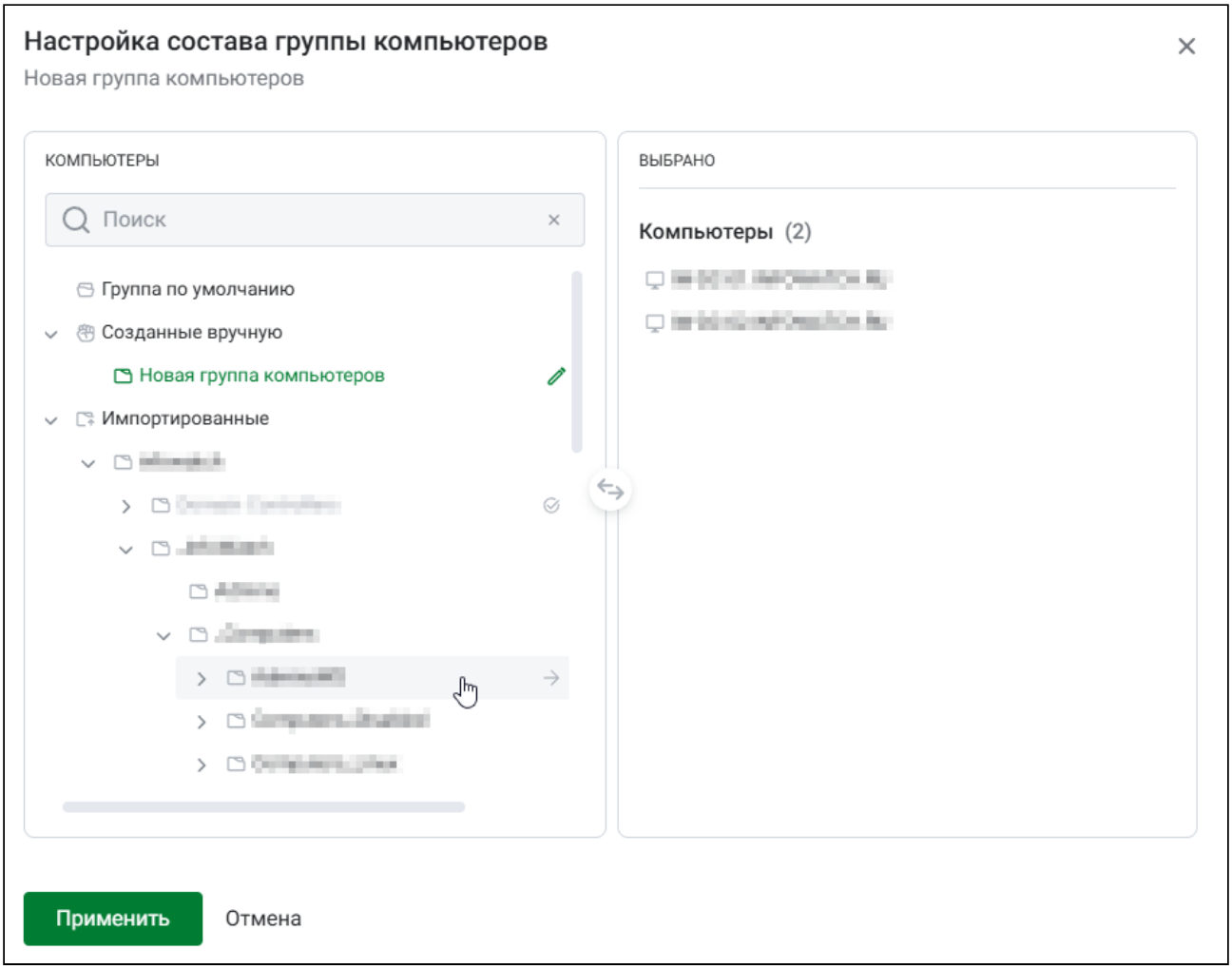
5. В области слева просмотрите список **Компьютеры**. В нем отображаются компьютеры из числа ранее зарегистрированных в Системе, т.е. компьютеры, на которых установлен Агент, из группы «по умолчанию» и других групп.

   Чтобы развернуть или свернуть группу, используйте .
   Чтобы найти компьютер или группу, введите в строку поиска текст запроса, состоящий

хотя бы из 3 символов. Результаты будут отображены в иерархическом списке в области слева и выделены синим цветом. Если одним из результатов поиска является группа, то будут показаны все входящие в нее элементы, в том числе не подходящие под условие поиска.

6. Для добавления в группу, в области слева наведите курсор на компьютер или группу и нажмите → **Добавить компьютеры в "<Название группы компьютеров>"**.

   Напротив группы или компьютера, которые были добавлены, появится значок ✓. В случае, если имя компьютера очень длинное, вы можете просмотреть его, используя полосу прокрутки внизу окна.
7. Для удаления из группы наведите курсор на удаляемую запись и нажмите ← **Удалить из группы "<Название группы компьютеров>"**. Это можно сделать как в области справа, так и в области слева.
8. Нажмите **Применить**.
9. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

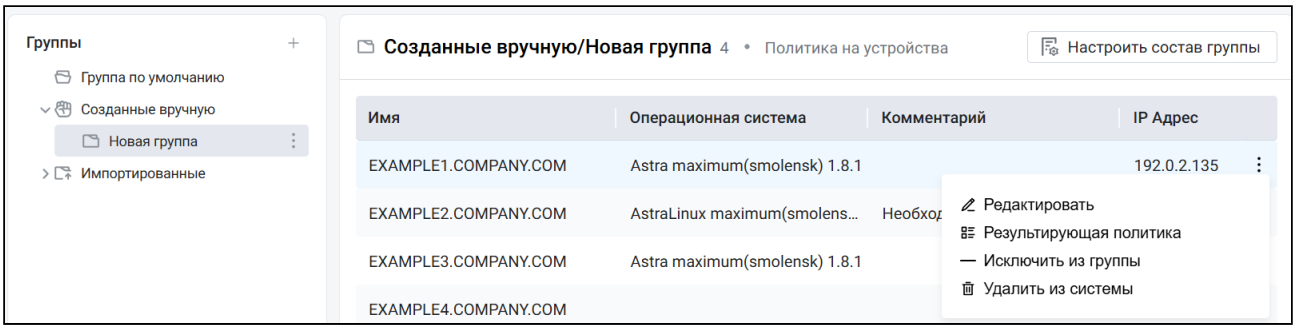


Примечание:

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.
Чтобы найти группу в списке, вы можете воспользоваться поиском. Подробнее см. "Создание и редактирование групп компьютеров".



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 **Исключить**. Если компьютер входил только в одну группу, то при исключении он будет автоматически добавлен в группу компьютеров «по умолчанию».
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы исключить несколько или все компьютеры из группы:

1. Отметьте чекбоксами необходимые компьютеры.
2. Выберите **Исключить из группы**.
3. В открывшемся диалоговом окне нажмите **Исключить**. Если компьютер входил только в одну группу, то при исключении он будет автоматически добавлен в группу компьютеров «по умолчанию».
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

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 компьютеры 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 **Удалить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы удалить несколько или все компьютеры из группы:

1. Отметьте чекбоксами необходимые компьютеры.
2. Выберите  **Удалить из системы**.
3. В открывшемся диалоговом окне нажмите **Удалить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

> **Важно!**
>
> Удаление компьютера из схемы безопасности повлечет за собой его удаление из всех групп и политик.

11.7.3 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.
- **Операционная система**. Версия операционной системы;
- **Комментарий**. Поле для ввода комментария. Этот же комментарий к рабочей станции отображается на вкладке **Состояние** раздела **Агенты**;
- **IP-адрес**. IP-адрес рабочей станции;
- **Пользователь**. Имя пользователя, заходившего на рабочую станцию последним.

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

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

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

- **Версия схемы**. Номер версии схемы безопасности, загруженной на Агент;
- **Версия настроек сетевых ресурсов**. 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 настроек**. Версия общих настроек политики безопасности (Device Monitor) (см. "Настройка Device Monitor");
- **Версия конфигурации ТМ**. Последняя версия конфигурации Traffic Monitor, доставленная на данную рабочую станцию;
- **Версия контроля сети**. Версия настроек контроля передачи данных по сетевым соединениям;
- **Версия шаблонов**. Версия шаблонов уведомлений, отображаемых пользователю.

> **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 (Device Monitor), определенная для группы компьютеров «по умолчанию».

11.7.4 Просмотр результирующей политики компьютера

Результирующая политика представляет собой совокупность правил, являющихся результирующими на компьютере. Результирующие правила складываются из правил, настроенных по умолчанию, и правил, заданных для данного компьютера.

Чтобы просмотреть результирующую политику, действующую на компьютере:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. Откройте вкладку **Компьютеры** в разделе **Группы**.
3. В области **Группы** выберите ту, которая содержит интересующий компьютер. В рабочей области будет выведен список всех компьютеров, входящих в группу.
4. В строке с именем интересующего компьютера нажмите .

5. Выберите  **Результирующая политика**.

Откроется окно **Результирующая политика**, в котором вы можете просмотреть результирующие правила на данном компьютере. Чтобы просмотреть подробную информацию по правилу, в области **Перехватчики** выберите интересующий вас канал перехвата.

Вы можете просмотреть следующие результирующие правила:

- Контроль каналов передачи данных:
  - Правило контроля съемных носителей;
  - Правило контроля сетевых ресурсов;
  - Правило контроля терминальной сессии;
  - Правило контроля печати;
  - Правило контроля FTP;
  - Правило контроля HTTP(S);
  - Правило контроля почты;
  - Правило контроля облачных хранилищ;
  - Правило контроля буфера обмена;
- Контроль мессенджеров:
  - Правило контроля мессенджера VK;
  - Правило контроля мессенджера Telegram;
  - Правило контроля Яндекс Мессенджера;
  - Правило контроля мессенджера WhatsApp;
  - Правило контроля мессенджера MAX;
  - Правило контроля протокола XMPP;
- Мониторинг активности пользователей:
  - Правило мониторинга экрана;
  - Правило мониторинга ввода текста с клавиатуры;
  - Правило мониторинга звукового окружения;
  - Правило записи видео с экрана;
- Контроль использования:
  - Правило контроля создания снимков экрана;
- Контроль приложений:
  - Правило контроля файлов в приложениях.

> **Примечание:**
>
> В окне **Результирующая политика** для правил **Контроль ввода текста с клавиатуры** и **Контроль HTTP(S)** также отображаются списки ресурсов (подробнее о списках ресурсов см. *Правило мониторинга ввода текста с клавиатуры*, *Правило контроля HTTP(S)*).

Чтобы посмотреть политику, назначенную на группу компьютеров по умолчанию, выберите значение **Новый компьютер** в поле **Компьютер**.

Вы можете дополнительно посмотреть результирующую политику для сотрудника, относящегося к выбранному компьютеру. Для этого в поле **Сотрудник** выберите объект для просмотра:

- **Новый сотрудник** – отображается правило, назначенное на группу сотрудников по умолчанию;
- **Известные сотрудники** – отображается правило для выбранного сотрудника из списка пользователей, которые когда-либо регистрировались на данном компьютере.

В поле доступен поиск по всем сотрудникам. При выборе сотрудника, который не связан с компьютером, значение в поле **Компьютер** сбрасывается.

> **Примечание:**
>
> Для сотрудника аналогичным образом доступен выбор компьютеров, к которым он относится. Подробнее см. *Просмотр результирующей политики сотрудника*.

11.8 Работа с группами сотрудников

Политики безопасности можно назначать группам сотрудников. Работа с группами сотрудников осуществляется в разделе **Группы** Центра администрирования и включает в себя:

- Создание и редактирование групп сотрудников
- Настройку состава группы сотрудников
- Просмотр результирующей политики сотрудника

11.8.1 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. "Синхронизация".

Чтобы добавить группу сотрудников:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. Откройте вкладку **Сотрудники** в разделе **Группы**.
3. На панели **Группы** нажмите .
4. Укажите следующие параметры:
   - **Наименование** группы;
   - **Политика**. Выберите из раскрывающегося списка политику, которая будет назначена данной группе сотрудников.
5. Нажмите **Добавить**. Будет создана новая группа сотрудников, в которую необходимо добавить сотрудников.
6. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы отредактировать группу сотрудников:

1. Выделите нужную группу и нажмите  справа от ее названия.
2. Выберите  **Редактировать** и внесите изменения.
3. Нажмите **Сохранить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы найти сотрудника или группу сотрудников:

1. В верхней части рабочей области введите в строку поиска текст запроса, состоящий хотя бы из 3 символов. Поиск сотрудника возможен по его идентификатору, фамилии, имени или отчеству.
   В раскрывшемся списке будут показаны первые 5 сотрудников и первые 5 групп сотрудников, параметры которых включают введенный текст.
2. Выберите результаты поиска для отображения:
   - Чтобы просмотреть все элементы, удовлетворяющие запросу, нажмите **Enter** или **Смотреть все результаты**. Результаты будут отображены в иерархическом списке в области слева, найденные группы при этом будут выделены синим цветом.
     Если одним из результатов поиска является группа, то будут показаны все входящие в нее элементы, в том числе не подходящие под условие поиска.
   - Чтобы перейти к одному элементу, нажмите на группу или сотрудника. В рабочей области откроется выбранная группа или группа, включающая выбранного сотрудника.

Важно!

Если не осуществляется поиск объектов с использованием кириллицы, убедитесь, что для базы данных, с которой взаимодействует сервер Device Monitor, установлена русская локаль (`ru_RU.utf8`). Подробнее см. статью Базы знаний "Проверка и изменение локали базы данных PostgreSQL".

Чтобы отменить фильтр, примененный с помощью поиска, нажмите  в строке поиска.

Чтобы удалить группу сотрудников:

Примечание

Группу сотрудников по умолчанию удалить нельзя.

1. Напротив нужной группы нажмите .
2. Нажмите  **Удалить**. 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 подтвердите действие, нажав **Удалить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

11.8.2 Настройка состава групп сотрудников

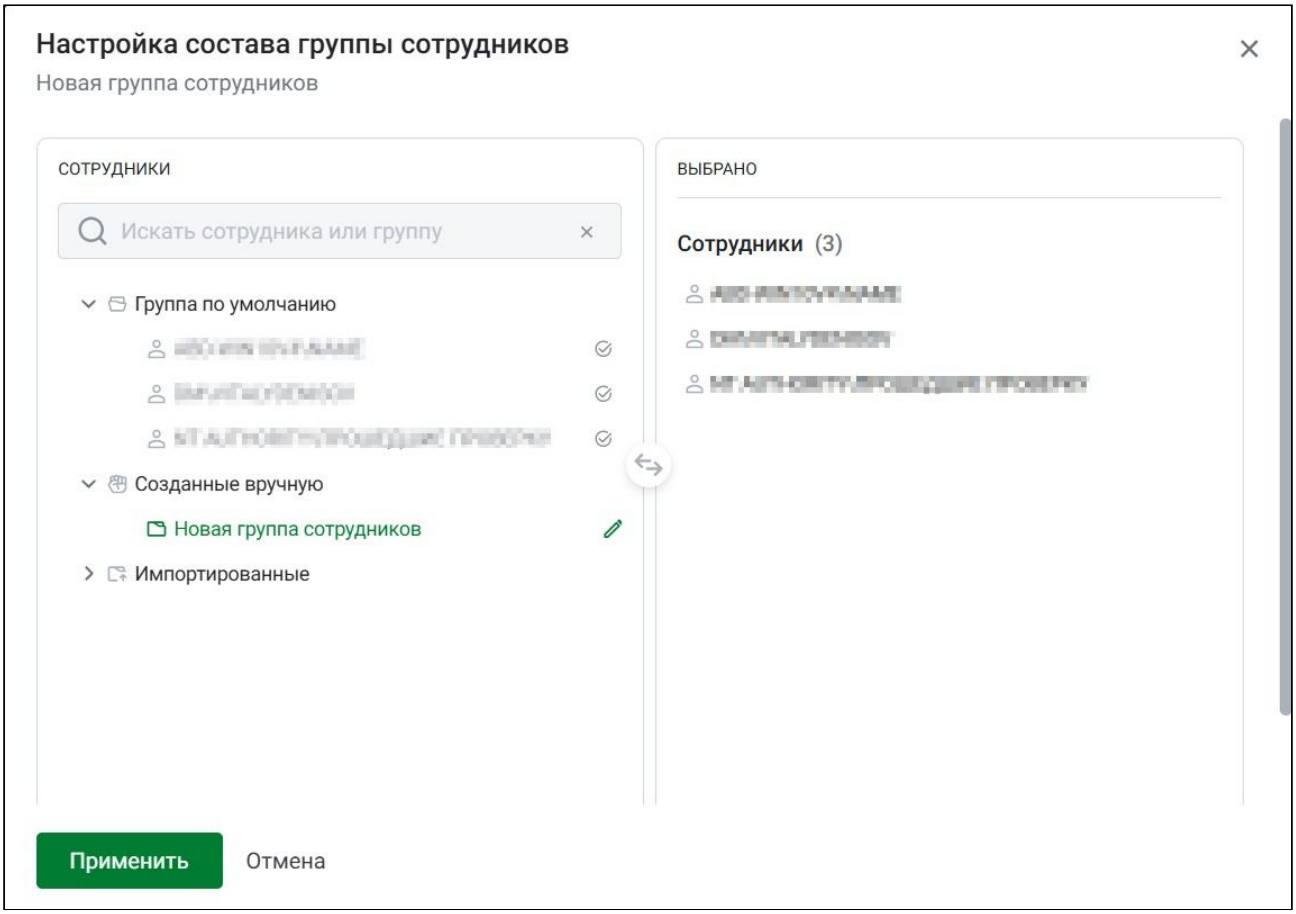
При установке Агента InfoWatch Device Monitor на рабочую станцию, в Системе автоматически создаются записи о пользователях этой рабочей станции. Эти записи добавляются в "Группу сотрудников по умолчанию". На всех сотрудников, входящих в эту группу, будет распространяться назначенная ей политика. В дальнейшем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

Чтобы настроить состав группы сотрудников:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. Откройте вкладку **Сотрудники** в разделе **Группы**.
3. В левой части рабочей области выберите группу. В центральной части рабочей области будет выведен список всех сотрудников, уже входящих в группу.

   > **Примечание:**
   >
   > Чтобы найти группу в списке, вы можете воспользоваться поиском. Подробнее см. "Создание и редактирование групп сотрудников".

4. Напротив группы нажмите , затем выберите , или выберите группу и в правом верхнем углу рабочей области нажмите .
   Откроется диалоговое окно. В его левой части отобразится список ранее зарегистрированных в Системе сотрудников.
   Чтобы развернуть или свернуть какую-либо группу сотрудников в списке, используйте .
   Чтобы найти сотрудника или группу, введите в строку поиска текст запроса, состоящий хотя бы из 3 символов. Поиск сотрудника доступен только по его идентификатору. Результаты будут отображены в иерархическом списке в области слева и выделены синим цветом. Если одним из результатов поиска является группа, то будут показаны все входящие в нее элементы, в том числе не подходящие под условие поиска.
5. Для добавления в группу, в области слева наведите курсор на сотрудника или группу и нажмите  **Добавить сотрудников в "<Название группы сотрудников>"**.
   Напротив группы или сотрудника, которые были добавлены, появится значок .
6. Для удаления из группы наведите курсор на удаляемого сотрудника или группу и нажмите  **Удалить из группы "<Название группы сотрудников>"**. Это можно сделать, как в области справа, так и в области слева.
7. Нажмите **Применить**.
8. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").



Примечание:

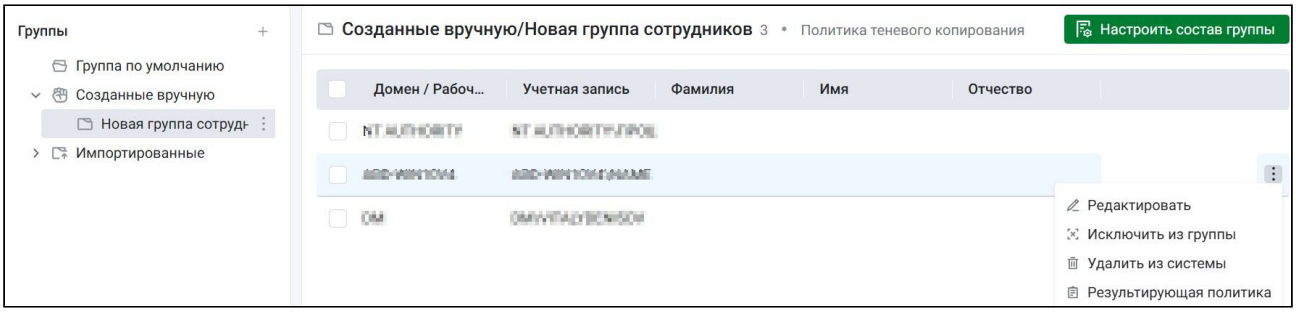
Если вы добавляете группу сотрудников, которая содержит подгруппы, то сотрудники из подгрупп не будут автоматически добавлены в выбранную группу. Вы можете добавить их отдельно.

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.
Чтобы найти сотрудника в списке групп, вы можете воспользоваться поиском. Подробнее см. "Создание и редактирование групп сотрудников".



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. В открывшемся диалоговом окне подтвердите действие, нажав **Исключить**. Если сотрудник входил только в одну группу, то при исключении он будет автоматически добавлен в группу сотрудников "по умолчанию".
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы исключить нескольких или всех сотрудников из группы:

1. Отметьте чекбоксами необходимых сотрудников.
2. Выберите ⛶ **Исключить из группы**.
3. В открывшемся диалоговом окне нажмите **Исключить**. Если сотрудник входил только в одну группу, то при исключении он будет автоматически добавлен в группу сотрудников "по умолчанию".
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

При необходимости вы можете удалить сотрудников 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 **Удалить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

Чтобы удалить нескольких или всех сотрудников из схемы безопасности:

1. Отметьте чекбоксами необходимых сотрудников.
2. Выберите  **Удалить из системы**.
3. В открывшемся диалоговом окне нажмите **Удалить**.
4. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее "Режимы редактирования конфигурации").

> **Важно!**
>
> Удаление сотрудника из схемы безопасности повлечет за собой его удаление из всех групп и политик.

11.8.3 Просмотр результирующей политики сотрудника

Результирующая политика представляет собой совокупность правил, являющихся результирующими для сотрудника. Результирующие правила складываются из правил, настроенных по умолчанию, и правил, заданных для данного сотрудника.

Чтобы просмотреть результирующую политику, действующую на сотрудника:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. Откройте вкладку **Сотрудники** в разделе **Группы**.
3. В области **Группы** выберите ту, которая содержит интересующего сотрудника. В рабочей области будет выведен список всех сотрудников, входящих в группу.
4. В строке с именем интересующего сотрудника нажмите .
5. Выберите  **Результирующая политика**.

Откроется окно **Результирующая политика**, в котором вы можете просмотреть результирующие правила для данного сотрудника. Чтобы просмотреть подробную информацию по правилу, в области **Перехватчики** выберите интересующий вас канал перехвата. Подробнее о всех результирующих правилах, доступных для просмотра, см. "Просмотр результирующей политики компьютера".

Вы можете посмотреть политику другого сотрудника, выбрав его из списка **Все** в поле **Сотрудник**. При необходимости воспользуйтесь поиском. Поиск сотрудника возможен по его идентификатору, фамилии, имени или отчеству.

Для просмотра политики, назначенную на группу сотрудников по умолчанию, выберите значение **Новый сотрудник**.

Вы можете дополнительно просмотреть результирующую политику компьютера, к которому относится сотрудник. Для этого в поле **Компьютер** выберите объект для просмотра:

- **Новый компьютер** – отображается правило, назначенное на группу компьютеров по умолчанию;
- **Известные компьютеры** – отображается правило для компьютера, выбранного из списка ранее использованных пользователем компьютеров.

В поле доступен поиск по компьютерам.

> **Примечание:**
>
> Для компьютера аналогичным образом доступен выбор сотрудников, относящихся к нему. Подробнее см. "Просмотр результирующей политики компьютера".

11.9 Работа с Агентами

Работа с Агентами осуществляется в разделе **Агенты** Центра администрирования. Информация о работе с Агентами содержится в подразделах:

- Просмотр сведений об Агентах
- Фильтрация записей
- Перезагрузка компьютера
- Обновление конфигурации
- Диагностика Агентов
- Установка статуса "Золотой образ"
- Запуск и остановка Агентов
- Удаление Агентов
- Политики распространения

11.9.1 Просмотр сведений об Агентах

Информация об Агентах представлена в виде табличного списка. В столбцах выводятся основные свойства рабочих станций. Вы можете менять порядок столбцов.

Табличный список содержит следующие основные сведения:

- **Состояние**. Состояние Агента, установленного на компьютере. См. список ниже.
- **Место на диске**. Данные об объеме диска с Агентом, отображаемые в формате Объем свободного места/Общий объем. Возможные значения:
  -  – места достаточно (т.е. оно больше или равно значению, указанному для настройки *Порог предупреждения* в блоке **Контроль дискового пространства**. Подробнее о настройке см. *Агенты*).
  -  – место скоро закончится (остаток места меньше значения *Порог предупреждения* или равен значению, заданному для параметра *Критический остаток места на диске*).
  -  – место закончилось, теневые копии не собираются (остаток места на диске меньше значения, заданного для параметра *Критический остаток места на диске*).

  Если на Агенте под управлением ОС Windows есть несколько дисков, информация отображается для диска с максимальным свободным размером.
- **Компьютер**. Доменное имя рабочей станции.
- **IP-адрес**. IP-адрес рабочей станции.
- **Последнее обращение**. Дата и время последнего обращения к серверу Агента, установленного на компьютере.
- **Подключение**. Дата и время подключения к серверу Агента, установленного на компьютере.
  Подключение выполняется при старте клиента. Также, для распределения нагрузки,

периодически происходит переподключение Агента к пулу серверов. При каждом успешном подключении дата и время в поле **Подключение** меняются. При запуске Агента после остановки будет установлено соединение с сервером и значение поля **Подключение** обновится.

- **Регистрация**. Дата и время регистрации рабочей станции (добавление в БД).
- **Версия Агента**. Номер версии Агента, установленного на компьютере.
- **Операционная система**. Версия операционной системы.
- **Пользователь**. Имя пользователя, заходившего на рабочую станцию последним. Пользователь не отображается для рабочих станций под управлением ОС Linux.
- **Комментарий**. Комментарий, введенный на вкладке **Компьютеры** раздела **Группы**.
- **Активность агента**. Активность установленного агента отображается при помощи цветового индикатора в начале строки:
  -  – *Неактивен более часа*, то есть Сервер не может установить с ним соединение.
  -  – *Агент активен*;
  -  – *Неактивен более одного дня*;
  -  – *Неактивен более двух недель*;
  -  – *Неактивен более месяца*.
- **Версия схемы**. Номер версии схемы безопасности, загруженной на агент. Для компьютера с состоянием инсталляции ***Не установлен*** должно отображаться значение "0".
- **Версия конфигурации ТМ**. Последняя версия конфигурации Traffic Monitor, доставленная на данную рабочую станцию.
- **Версия настроек**. Версия общих настроек политики безопасности. В скобках указывается номер последней примененной версии на агенте.
- **Версия шаблонов**. Версия шаблонов уведомлений, которые могут быть показаны пользователю.
- **Версия настроек контроля сети**. Версия настроек контроля сетевого трафика, передаваемого по протоколам XMPP, MMP, FTP, FTPS, SMTP/S/MIME/Outlook/POP3, HTTPS.
- **Версия настроек контроля сетевых ресурсов**. Версия настроек контроля передачи данных по сетевым соединениям.
- **Версия настроек исключений**. Версия настроек исключения приложений из перехвата на сервере. В скобках указывается номер последней примененной версии на агенте.

Работа с данными в таблице

При работе с таблицей вы можете:

- изменять отображение столбцов:
  - перемещать столбцы или добавлять новые
  - сортировать значения
  - группировать Агенты
  - фильтровать записи, см. *Фильтрация записей*
- просматривать подробную информацию
- обновлять данные

Отображение столбцов в таблице

По умолчанию отображаются следующие столбцы:

- Активность агента;
- Состояние;
- Компьютер;
- IP-адрес;
- Последнее обращение;
- Версия Агента;
- ОС;
- Комментарий.

Вы можете настроить отображение столбцов в таблице. Для этого:

1. В правом верхнем углу нажмите .
2. Выберите  из списка колонки, которые необходимо добавить в таблицу.
3. Чтобы включить отображение колонок в таблице по умолчанию, нажмите **Вернуть системные настройки**.

Чтобы переместить колонку:

1. На верхней панели выберите колонку, которую необходимо переместить.
2. Нажмите кнопку мыши и не отпуская ее, передвиньте колонку.

Сортировка значений в столбцах

В таблице применяется следующий принцип сортировки:

- По возрастанию/убыванию: *Активность*, *Место на диске*, *IP-адрес*
- По возрастанию/убыванию алфавитном порядке: *Компьютер*, *Комментарий*, *ОС*, *Пользователь*
- От последнего к более раннему значению: *Версия Агента*, *Версия конфигурации TM*, *Версия настроек*, *Версия настроек исключений*, *Версия настроек контроля сети*, *Версия настроек сетевых приложений*, *Версия схемы*, *Версия шаблонов*, *Подключение*, *Последнее обращение*, *Регистрация*

Для столбца *Состояние* сортировка реализована следующим образом: поскольку у Агента может быть несколько состояний одновременно, применяется последовательная сортировка от первого состояния в списке к последнему, т.е. Система вначале сортирует по первому отображаемому состоянию, далее по второму и т.д.

Чтобы изменить сортировку:

1. В нужной колонке нажмите на ячейку с наименованием этой колонки.
2. Нажмите появившуюся кнопку  **Сортировать**.
3. Чтобы изменить порядок сортировки, повторно нажмите на кнопку.

Группировка Агентов

Также вы можете группировать Агентов по значениям в колонках.

> **Важно!**
>
> Группировка доступна только для колонок с соответствующей кнопкой.

Чтобы сгруппировать Агентов:

1. В нужной колонке нажмите на ячейку с наименованием этой колонки.

2. Нажмите появившуюся кнопку  **Сгруппировать**.

При группировке Система формирует группы из Агентов, у которых значения в выбранной колонке совпадают. При этом название колонки отображается над таблицей Агентов. Чтобы убрать группировку, нажмите  рядом с названием колонки или кнопку **Сброс** в правом верхнем углу.

Группа **Отсутствует** – это группа, в которой находятся Агенты с незаполненным значением в колонке.

Вы можете сгруппировать Агенты по нескольким колонкам. При этом группировка происходит иерархически: сначала Агенты разделяются по первой выбранной колонке, затем внутри каждой сформированной группы по второй и т.д. Для изменения порядка над таблицей Агентов перетащите название колонки на нужную позицию в иерархии.

Просмотр подробной информации

Расширенная информация по состоянию Агента выводится на панели **Подробно**, которая отображается при нажатии на строку Агента.

Помимо данных, представленных в таблице, на панели отображается раздел **Версии** со следующей информацией:

- **Версия схемы**;
- **Версия агента**;
- **Версия конфигурации ТМ**;
- **Версия настроек**;
- **Версия шаблонов**;
- **Версия настроек контроля сетевых ресурсов**;
- **Версия настроек контроля сети**;
- **Версия настроек исключений**.

Чтобы скрыть панель, нажмите  справа от ее названия.

> **Примечание:**
>
> Если Агент отправляет событие на сервер Device Monitor, Агент удаляет данные этого события с диска.
>
> В некоторых случаях не поддерживается удаление данных на Агентах. Файл с метаданными события может остаться на диске Агента, даже если Агент отправил событие.

Обновление данных

Вы можете обновить данные в таблице Агентов, нажав кнопку . При этом сохранятся выбранные значения фильтра, сортировки и группировки. Эти значения также сохранятся при смене вкладки.

Состояния Агентов

Агент может принимать следующие **состояния**[1]:

- *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. Состояние не отображается при наличии других состояний;
- *Работает с ограничениями*. Агент установлен на рабочую станцию, но работает частично. Например, это состояние будет выставлено после запуска Агента при проверке на загрузку и совместимость необходимых драйверов ядра ОС;
- *Останавливается*. На Агенте запущен процесс остановки;
- *Остановлен*[2]. Агент установлен на рабочую станцию и остановлен через Консоль Device Monitor;
- *Запускается*. На Агенте запущен процесс запуска;
- *Переход в диагностический режим*. На Агенте запущен процесс перехода в диагностический режим;
- *Диагностический режим*. Агент установлен на рабочую станцию и переведен в диагностический режим работы через Консоль Device Monitor;
- *Выход из диагностического режима*. На Агенте запущен процесс выхода из диагностического режима;
- *Золотой образ*[3]. Агент установлен на рабочую станцию, которой назначено состояние *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*[4]. Агент удален с рабочей станции через задачу удаления продукта или средствами самой рабочей станции.

Примечание:

[1] При миграции сервера Device Monitor for Windows на Device Monitor for Linux состояние Агентов перезаписывается на предустановленные в Device Monitor for Linux.

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

[3] При изменении имени рабочей станции с состоянием *Золотой образ* Система создает новую запись для рабочей станции с новым именем, т.е. определяет ее как клонированную. Если вы действительно переименовали рабочую станцию (не клонировали ее):

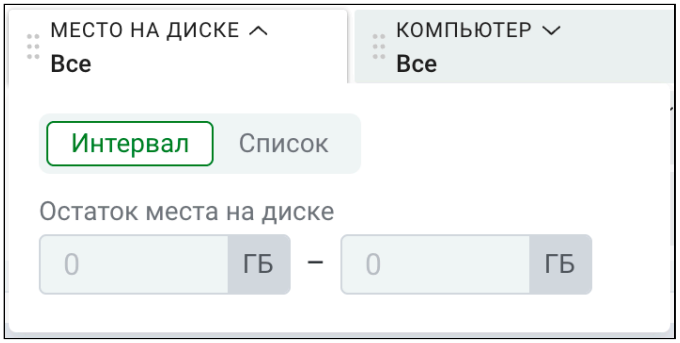
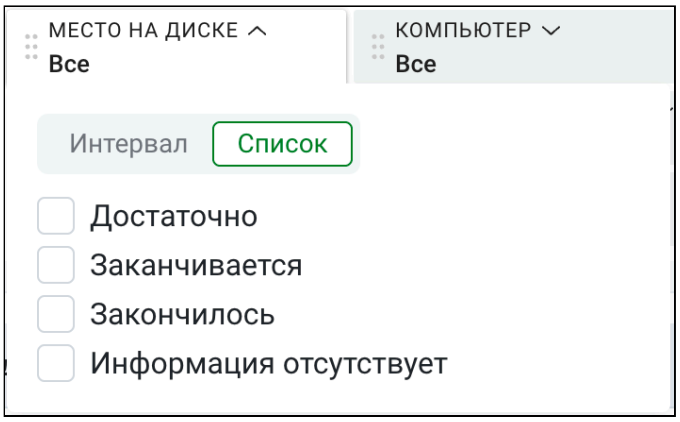
1. В разделе **Группы** > **Компьютеры** удалите запись со старым именем.
2. В разделе Агенты присвойте состояние *Золотой образ* записи с новым именем.

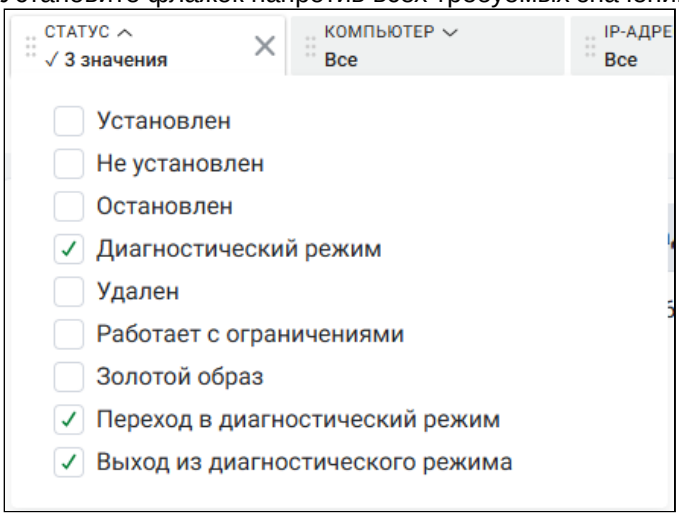
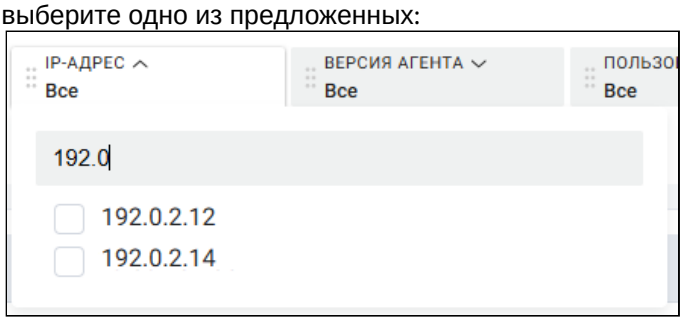
[4] При удалении Device Monitor состояние отправляется Агентом по протоколу UDP, не гарантирующему доставку. Кроме того, Агент отправляет уведомление в случае, если с сервером Device Monitor уже была установлена сессия и сообщение отправляется тому серверу, с которым Агент взаимодействует в данный момент.

11.9.2 Фильтрация записей

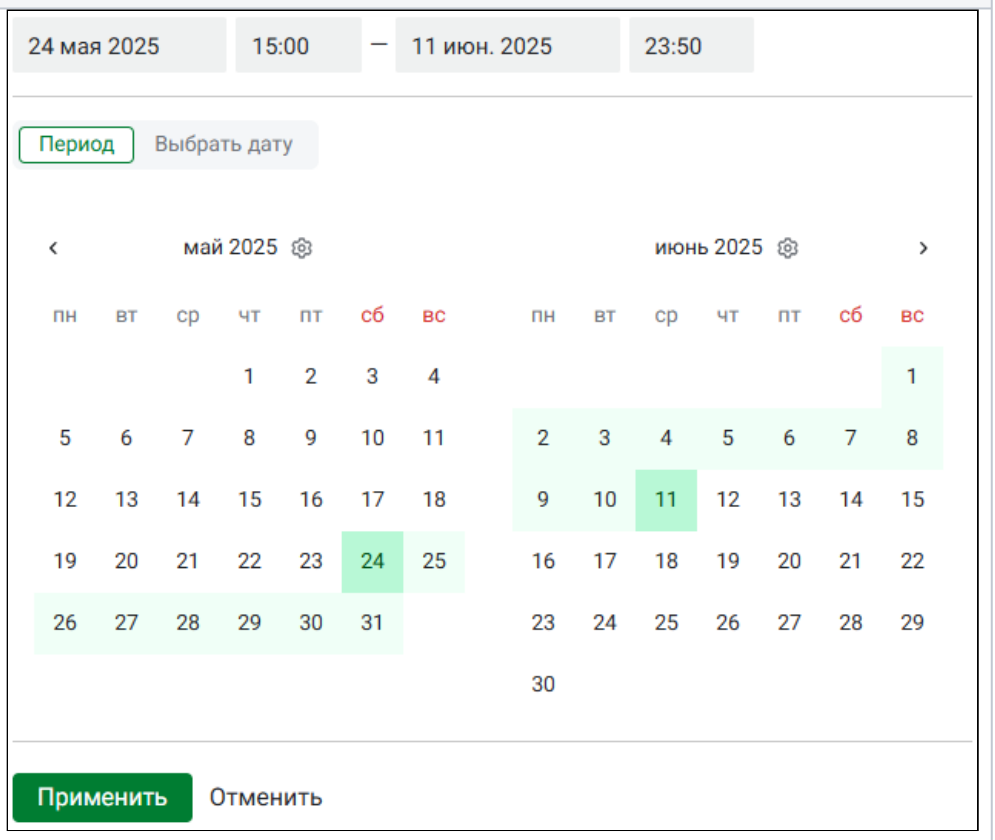
Над табличным списком Агентов расположена панель фильтров. С ее помощью вы можете исключить из анализа часть данных, чтобы скрыть лишнюю информацию.

Вы можете отфильтровать записи в разделе Агенты по значениям следующих столбцов:

Столбец	Установка значений фильтра
Активность	• Активен • Неактивен более часа • Неактивен более одного дня • Неактивен более двух недель • Неактивен более месяца • Отсутствует информация
Место на диске	Вы можете задать значение в виде Интервала (в ГБ):  или Списка атрибутов:  Для агентов версий 7.18.x и более ранних будет отображаться значение – информация отсутствует.

Столбец	Установка значений фильтра
Состояние	Установите флажок напротив всех требуемых значений: 
Версия агента **Версия схемы** **Версия конфигурации ТМ** **Версия настроек** **Версия настроек исключений** **Версия настроек контроля сетевых ресурсов** **Версия настроек контроля сети** **Версия шаблонов**	При большом количестве значений фильтров Комментарий и IP-адрес воспользуйтесь поиском. Для этого начните вводить значение в поле фильтра и выберите одно из предложенных: 

Столбец	Установка значений фильтра
ОС	
Комментарий	
IP-адрес	
Компьютер	Выбор значений аналогичен процессу добавления компьютеров/сотрудников в группы. См. статьи *Настройка состава групп компьютеров* и *Настройка состава групп сотрудников*.
Пользователь	
Последнее обращение	Выберите период времени, данные за который необходимо получить: • *Последние сутки;* • *Текущий день;* • *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:

Столбец	Установка значений фильтра
Подключение	

Также вы можете указать даты в полях вверху.

2. При необходимости задайте время начала и конца периода.
3. Нажмите **Применить**.

Чтобы указать одну или несколько произвольных дат

Столбец	Установка значений фильтра
Регистрация	1. Используя указатель мыши, отметьте в календаре одну или несколько дат. Выбранные даты будут подсвечены:  2. Нажмите **Применить**.

Для значений внутри одного столбца применяется логическое *ИЛИ*, между столбцами – логическое *И*.

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

Чтобы скрыть панель фильтров, нажмите  в правом верхнем углу панели.

Чтобы скрыть фильтр с панели, нажмите  в правом верхнем углу панели и снимите флажок с фильтра.

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

Примечание:

При работе с фильтрами учитывайте, что:

- все настройки фильтра распространяются только в рамках одной вкладки в браузере;
- при обновлении страницы или при выходе из Системы все атрибуты фильтра пользователя сохраняются.

11.9.3 Перезагрузка компьютера

Чтобы удаленно перезагрузить рабочую станцию, на котором установлен Агент:

1. В разделе **Агенты** наведите курсор на строку с информацией об Агенте.
2. В конце строки нажмите .
3. Выберите **Перезагрузить компьютер**.

> **Важно!**
>
> Перезагрузка рабочей станции не доступна для Агентов в статусе *Не установлен* и *Удален*.

11.9.4 Обновление конфигурации

Чтобы обновить конфигурацию и настройки Агента:

1. В разделе **Агенты** наведите курсор на строку с информацией об Агенте.
2. В конце строки нажмите .
3. Выберите **Обновить конфигурацию и настройки агента**.

> **Примечание:**
>
> Для успешного обновления конфигурации через консоль Device Monitor необходимо, чтобы между моментом последних правок в конфигурации в консоли и запросом на обновление конфигурации на Агенте прошло как минимум 5 минут.

11.9.5 Диагностика Агентов

Вы можете удаленно собрать диагностические данные с рабочих станций. Данные запрашиваются из Центра администрирования через сервер Device Monitor, который обращается к Агентам.

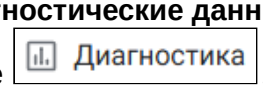
Чтобы Агент начал сбор диагностической информации, его необходимо перевести в диагностический режим.

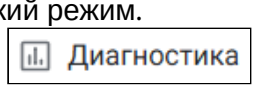
Чтобы включить диагностический режим:

1. Перейдите к разделу **Агенты**. Выберите один из способов:
   - Если необходимо включить режим для одного Агента:
     a. Наведите курсор на строку с Агентом и в конце строки нажмите .
     b. Нажмите **Включить диагностический режим**.
   - Если необходимо включить режим для нескольких Агентов:
     a. Выберите  нужные Агенты. Или нажмите  на плашке вверху списка Агентов, чтобы выбрать сразу все Агенты. Внизу экрана появится плашка с количеством выбранных Агентов и кнопками управления.
     b. Нажмите  **Включить диагностический режим**.
     c. Чтобы скрыть плашку, нажмите .

Собранную диагностическую информацию можно выгрузить в виде архива с файлами.

Чтобы получить архив с диагностическими данными:

1. Включите диагностический режим для всех интересующих вас Агентов.
2. Соберите диагностические данные одним из способов:
   - Если необходимо собрать данные для одного Агента:
     a. В разделе **Агенты** наведите курсор на строку с Агентом и в конце строки нажмите .
     b. Нажмите **Собрать диагностические данные**.
     c. Справа вверху нажмите 

.
   - Если необходимо собрать данные для нескольких Агентов:
     a. В разделе **Агенты** выберите  нужные или все Агенты.
     b. Включите диагностический режим.
     c. Справа вверху нажмите 

.
     d. В окне **Управление диагностикой** в начале строки с Агентом нажмите .
3. Дождитесь, когда данные будут собраны и для выбранных Агентов появится статус .
4. В начале строки с Агентом нажмите  **Скачать диагностические данные**.
5. Чтобы закрыть окно **Управление диагностикой**, нажмите  справа вверху.

До выгрузки с сервера диагностическая информация хранится в директории `/opt/iw/dmserver/AgentLogs`. Доступ к директории ограничен.

Чтобы отключить диагностический режим:

1. Перейдите к разделу **Агенты**.
2. Выберите  нужные или все Агенты.
3. На появившейся внизу экрана плашке нажмите  **Выключить диагностический режим**.

или

1. Перейдите к разделу **Агенты**.
2. Наведите курсор на строку с Агентом и в конце строки нажмите .
3. Нажмите **Отключить диагностический режим**.

Чтобы удалить диагностические данные:

1. Наведите курсор на строку с Агентом и в конце строки нажмите .
2. Нажмите **Удалить диагностические данные**.

> **Примечание:**
>
> Доступно удаление только детальных (verbose) диагностических данных и только для Windows-агентов. При этом:
>
> - не удаляются данные процессов Device Monitor;

- для успешного удаления данных других приложений необходимо, чтобы процессы приложения были завершены;
- диагностические данные недоступны для скачивания, если запущена политика.

11.9.6 Установка статуса "Золотой образ"

Чтобы присвоить Агенту статус *Золотой образ*:

1. В разделе **Агенты** наведите курсор на строку с информацией об Агенте.
2. В конце строки нажмите .
3. Выберите **Присвоить статус Золотой образ**.

Чтобы снять статус *Золотой образ*, повторите действия и в шаге 3 выберите **Снять статус Золотой образ**.

11.9.7 Запуск и остановка Агентов

Важно!

Запуск и остановка доступна для Агентов на рабочих станциях под управлением ОС MS Windows, macOS и ОС семейства Linux.

Может не осуществляться перехват процессов, запущенных до того, как Агент был перезапущен. Для корректной работы необходимо перезагрузить компьютер с Агентом.

Чтобы остановить Агенты:

1. Наведите курсор на строку с Агентом и в конце строки нажмите .
2. Нажмите **Остановить агента**.
   или
1. В разделе **Агенты** выберите  нужные Агенты. Или нажмите  на плашке вверху списка, чтобы выбрать сразу все Агенты.
2. На появившейся внизу экрана плашке нажмите .

Чтобы снова запустить Агенты:

1. Наведите курсор на строку с Агентом и в конце строки нажмите .
2. Нажмите **Запустить агента**.
   или
1. В разделе **Агенты** выберите  нужные Агенты. Или нажмите  на плашке вверху списка, чтобы выбрать сразу все Агенты.
2. На появившейся внизу экрана плашке нажмите  **Запустить агенты**.

Чтобы перезагрузить компьютер с Агентом:

1. Наведите курсор на строку с Агентом и в конце строки нажмите .

2. Нажмите **Перезагрузить компьютер**.

11.9.8 Удаление Агентов

Чтобы удалить Агент из схемы безопасности:

1. Наведите курсор на строку с Агентом и в конце строки нажмите .
2. Нажмите **Удалить из системы**.

Агент будет удален из всех групп и политик.

> **Важно!**
>
> Удаление недоступно, если:
>
> - Агент был добавлен в результате синхронизации. Такие Агенты могут быть удалены только при удалении синхронизации.
> - конфигурация редактируется хотя бы одним из пользователей Системы;
> - запущена синхронизации с Active Directory.

11.9.9 Политики распространения

В разделе **Агенты** на вкладке **Распространение** доступно управление установкой, обновлением и удалением. Политики могут быть применены к выбранным компьютерам и группам, запущены вручную и выполнены до остановки. Если на один компьютер распространено несколько политик, сработает политика с более высоким приоритетом.

Работа с политиками

Чтобы **создать** и **запустить** политику:

1. В правом верхнем углу нажмите **+ Создать политику**.
2. В окне **Создание политики**:
   - выберите тип политики: *Установка и обновление* или *Удаление*;
   - введите название политики.
3. Нажмите **Создать**. Политика отобразится слева в списке **Политики распространения**.
4. Нажмите на политику в списке. Справа отобразится панель политики со вкладками:
   - Настройка политики:
     - Параметры политики
     - Состав
     - Параметры запуска (доступно только для политики установки и обновления)
   - Просмотр списка рабочих станций, статуса выполнения политики и деталей:
     - Компьютеры
5. После завершения настройки политики нажмите **Сохранить** и **Запустить**.

Чтобы **отредактировать** политику, выберите ее в списке, внесите изменения и нажмите **Сохранить**.

Чтобы **запустить**/**остановить** или **удалить** политику:

- выделите название политики в списке, справа от названия нажмите  и выберите нужное действие
  или
- откройте окно редактирования политики, нажав на ее название в списке, и на верхней панели выберите нужное действие.

> **Примечание:**
>
> Если в результате выполнения задачи выставлен статус ***Ошибка***, вы можете ознакомиться с расширенными сведениями, открыв на сервере файл лога `/var/log/iwdms/webapi-<date>.txt`, где `<date>` – дата запуска задачи. Для получения записей в логе убедитесь, что в файле `/opt/iw/dmserver/webapibin/webapi.appsettings.json` в секции `MinimumLevel` указан уровень логирования `Verbose`.

> **Примечание:**
>
> Приоритет политик определяется следующим образом:
>
> - Политики удаления имеют более высокий приоритет по отношению к политикам установки и обновления.
> - Чтобы повысить/понизить приоритет политики установки и обновления, переместите ее к началу/концу списка.

Вкладка Параметры политики

Введите название политики и добавьте описание.

Для политик установки и обновления: по умолчанию Система распространяет последнюю доступную версию Агента. Чтобы указать более раннюю версию, деактивируйте переключатель **Последняя версия** и введите версию в поле справа.

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

Вкладка Состав

На вкладке **Состав** добавьте рабочие станции и/или группы, на которые требуется распространить политику. Для этого нажмите **Выбрать компьютеры** и выберите способ:

- *Выбрать из списка*
  В открывшемся окне отображается список компьютеров из доступной интеграции с Active Directory или ранее добавленных компьютеров Группы Device Monitor (подробнее см. *Настройка состава групп компьютеров*) с указанием полного имени для установки Агентов.

  a. Выберите рабочие станции в области *Компьютеры* и нажмите . При добавлении группы добавляются компьютеры только из выбранной группы, не

включая компьютеры в подгруппах. Вы можете воспользоваться полем поиска, чтобы быстро найти нужный компьютер и добавить его в задачу. Введите не менее 3 и не более 64 символов.

b. Нажмите **Применить**. В области с именем 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.

c. Чтобы удалить ошибочно добавленные адреса, выделите их и нажмите .

- *Добавить вручную*
  В открывшемся окне введите DNS-имя компьютера и нажмите **Добавить**.
  Имя компьютера может состоять из любых символов любых алфавитов, указанных в Unicode. Чтобы ввести несколько имен, используйте точку с запятой или перенос строки в качестве разделителя.

Чтобы очистить список компьютеров, нажмите **Исключить все компьютеры**.

Чтобы быстро проверить, входит ли интересующий вас компьютер/группа в политику, воспользуйтесь полем поиска над списком добавленных компьютеров.

Вкладка Параметры запуска

Для политики установки и обновления задайте параметры в четырех подразделах.

Подраздел Основные

В подразделе **Основные параметры** укажите логин и пароль пользователя, от имени которого будет запущена задача.

По умолчанию Система использует все точки распространения. Чтобы указать конкретные, нажмите на переключатель **Все точки распространения** и выберите точки из выпадающего списка.

Подраздел Операционная система

Подраздел содержит параметры операционных систем рабочих станций, на которые планируется распространить политику. Если не нужно применять политику к рабочим станциями под управлением одной из операционных систем, деактивируйте переключатель **Задать параметры** для этой ОС.

- **Windows**
  Каталог установки по умолчанию: `%ProgramFiles%\Infowatch\DeviceMonitor\Client`.
  Вы можете изменить расположение файлов Агента.
- **Linux**
  Укажите порт SSH. По умолчанию указано значение 22. Минимальное значение – 1, максимальное – 65535.
  Укажите механизм повышения привилегии: **sudo** или **su**.
  При необходимости укажите для механизма **su** учетные данные пользователя, от имени которого ведется распространение.
  Если введение учетных данных не требуется, снимите флажок **Использовать логин и пароль запуска**.

Подраздел Перезагрузка

Укажите, ожидать ли перезагрузки без уведомления:

- *Не ожидать*;

- *Ожидать*. В этом случае укажите количество часов ожидания;
- *Ожидать бесконечно*.

Также укажите, уведомлять ли сотрудника о необходимости перезагрузки, как часто и каким сообщением.

Подраздел Дополнительно

Если необходимо, введите пароль защиты от удаления Агента (доступно для рабочих станций под управлением ОС Windows).

Уникальное имя для сертификата прокси-сервера Device Monitor (Issuer Distinguished name, Proxy Root Issuer DN) по умолчанию: `CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow`. Вы можете изменить его параметры. Имя должно содержать поле CN (Common Name), поля внутри имени должны быть разделены запятой.

Используя чекбоксы определите, требуется ли:

- Устанавливать компонент перехвата сетевого трафика
- Отменять установку при сбое получения списка приложений, исключаемых из перехвата[1]

Примечание:

[1] Начиная с Device Monitor 7.18.5, при первичной установке Агента инсталлятор проверяет, получен ли список приложений, которые должны быть исключены из перехвата. Если список исключений не получен, установка этого Агента будет остановлена.

Проверка включена по умолчанию, вы можете отключить ее.

Вкладка Компьютеры

На вкладке представлен список рабочих станций с версиями установленных на них Агентов и динамически обновляющимися пиктограммами статуса выполнения политики.

Вы можете **отфильтровать** рабочие станции по статусу выполнения политики. Для этого выберите нужные значения в фильтре **Состояние**:

- *Ошибка*
- *Проигнорирован*
- *Запланирована*
- *Идет установка*
- *Успешно*

Вы можете посмотреть лог установки агента, если выполнение политики завершилось со статусом *Ошибка*. Чтобы скачать лог, нажмите кнопку  **Скачать лог ошибки** в строке нужной рабочей станции.

Важно!

Возможно скачивание только последнего возникшего по времени лога.

При удалении компьютера/политики логи также удаляются.

При нажатии на рабочую станцию открывается панель с **подробной информацией**:

- Статус выполнения политики;
- Тип задачи;
- Текущая и устанавливаемые версии;
- IP-адрес, ОС и разрядность;
- Кнопка скачивания лога ошибки, если выполнение политики завершилось со статусом *Ошибка*.

11.10 Работа с файловой статистикой

Для настройки контроля действий сотрудника с файлами управляйте конфигурацией файловой статистики.

В разделе **Файловая статистика** вы можете:

- настроить параметры конфигурации файловой статистики пользователя;
- включить/исключить приложение из файловой статистики пользователя;
- включить/исключить из перехвата файлы с определенными расширениями;
- включить/исключить из перехвата файлы/папки, расположенные по определенному пути.

При срабатывании правила Система формирует события и отправляет их в Activity Monitor.

> **Важно!**
>
> Для формирования и отправки событий в Activity Monitor необходимо также настроить *Правило мониторинга активности сотрудника* → *Контролировать действия с файлами*.
>
> После изменения конфигурации файловой статистики, она должна быть распространена на агенты. Подробнее см. *Политики распространения*.
>
> Чтобы скачать/загрузить новую конфигурацию в Систему, перейдите в **Настройки** → **Device Monitor** → **Конфигурация**. Подробнее см. *Конфигурация*.

11.10.1 Настройка параметров конфигурации

Чтобы отредактировать параметры файловой статистики, в области **Общее** укажите:

1. *Создавать ли события для альтернативных файловых потоков*. По умолчанию параметр выключен.
   Если приложение и/или файловая система используют не основной (контролируемый) поток данных, а альтернативные (метаданные, связанные с объектом файловой системы), то события могут не создаваться. Настройка применяется, чтобы создавать события по сбору информации для альтернативных файловых потоков. Например, для обнаружения нарушителя, который прикрепляет файл с чувствительной информацией к разрешенному и копирует его вовне.
2. *Отслеживать ли только явно включенные в мониторинг приложения*. По умолчанию параметр выключен.
   Активируйте настройку, если необходимо отслеживать только те приложения, которые включены в мониторинг.

3. *Время накопительной сессии*. Значение по умолчанию – 30 сек.
   Настройка позволяет регулировать момент создания событий (в секундах). Если в Activity Monitor приходит много низкоуровневых событий, которые не соответствуют действиям пользователя, вы можете увеличить время накопительной сессии. Значение по умолчанию также можно уменьшить, в этом случае количество событий может увеличиться.
4. *Процент вычитанных данных*. Значение по умолчанию – 0.
   Настройка применяется, чтобы снизить количество системных событий открытия файла в Activity Monitor. Чем выше значение, тем меньше таких событий будет создаваться.

После внесения изменений нажмите кнопку **Сохранить** в правом верхнем углу. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее *Режимы редактирования конфигурации*).

11.10.2 Включение/исключение приложения из файловой статистики

Чтобы включить/исключить приложение из файловой активности пользователя:

1. В области **Общее** нажмите **Добавить приложение**.
2. В открывшемся окне выберите действие с приложением: **Исключить** или **Перехватывать**.
3. Укажите следующие параметры:
   - Имя приложения (обязательный параметр);
   - Описание;
   - Минимальная версия;
   - Максимальная версия;
   - Название продукта;
   - Издатель;
   - Расположение.
4. Нажмите **Добавить**.
5. После внесения изменений нажмите кнопку **Сохранить** в правом верхнем углу. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее *Режимы редактирования конфигурации*).

Чтобы отредактировать приложение в списке:

1. Наведите на нужное приложение и нажмите .
2. Внесите изменения и нажмите **Добавить**.
3. После внесения изменений нажмите кнопку **Сохранить** в правом верхнем углу. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее *Режимы редактирования конфигурации*).

Чтобы удалить приложение из списка:

1. Наведите на нужное приложение и нажмите .
2. После удаления приложения нажмите кнопку **Сохранить** в правом верхнем углу. Если включен запрет синхронного редактирования, нажмите **Сохранить** на информационной панели (см. подробнее *Режимы редактирования конфигурации*).

11.10.3 Включение/исключение файлов с определенным расширением из перехвата

Чтобы исключить из перехвата файлы с определенным расширением, добавьте расширение в поле **Не перехватывать файлы с расширением** в области **Перехваты**.

Чтобы включить в перехват файлы с определенным расширением, добавьте расширение в поле **Перехватывать файлы с расширением** в области **Перехваты**.

11.10.4 Включение/исключение файлов/папок, расположенных по определенному пути, из перехвата

Чтобы исключить из перехвата файлы/папки, расположенные по определенному пути, укажите путь в поле **Не перехватывать файлы, расположенные по пути** в области **Перехваты**.
Вводить пути к папкам следует, разделяя их ";" (точкой с запятой). Также поддерживается использование стандартных символов поиска:

- ? (знак вопроса) – заменяется один неизвестный символ;
- * (символ звездочки) – заменяется любое количество символов.

Значение поля должно содержать не более 4000 символов.

Чтобы включить в перехват файлы/папки, расположенные по определенному пути, укажите путь в поле **Перехватывать файлы, расположенные по пути** в области **Перехваты**.
Вводить пути к папкам следует, разделяя их ";" (точкой с запятой). Также поддерживается использование стандартных символов поиска:

- ? (знак вопроса) – заменяется один неизвестный символ;
- * (символ звездочки) – заменяется любое количество символов.

Чтобы не собирать информацию при выполнении действий с папкой, отметьте поле **Отключить сбор при выполнении действий с папкой**. По умолчанию параметр выключен.

12 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. ПО предназначено только для использования в вашей текущей операционной деятельности. 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, модернизировать, исправлять явные ошибки, модифицировать ПО и/или его компоненты, осуществлять попытки предпринять аналогичные действия в отношении ПО и/или его компонентов, а также создавать производные работы, основанные на ПО и/или Документации;
- использовать ПО сверх лицензируемого количества учетных записей, предусмотренных договором с вашим непосредственным лицензиаром;

- 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;
- использовать ПО с целью извлечения прибыли, сдавать ПО в аренду, прокат или во временное пользование, предоставлять подписку на ПО, предоставлять услуги аутсорсинга с использованием ПО, сублицензировать, распространять или иным образом предоставлять любому физическому или юридическому лицу любые права в отношении ПО и/или Документации, разглашать результаты стендовых испытаний ПО, за исключением случаев, прямо разрешенных настоящим Соглашением либо письменным согласием Правообладателя;
- передавать и предоставлять ссылку на дистрибутив и/или доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения и Договора, заключенного между вами и вашим лицензиаром;
- использовать ПО с целью создания данных или кода, предназначенных для использования другими программными продуктами;
- самостоятельно устанавливать дополнительные приложения к ПО, заменять компоненты ПО;
- 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, его несанкционированная передача третьим лицам запрещена. 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.**

Вы соглашаетесь с тем, что входящие в состав ПО программные компоненты внешних поставщиков предоставляются без гарантий доступа к обновленным версиям компонент и к иным программам, оборудованию, сертификатам на обучение или услугам внешних поставщиков.

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