

INFOWATCH

InfoWatch Device Monitor. Руководство пользователя

26/12/2025

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 6

2 Комплект документов 7

3 Функции InfoWatch Device Monitor 8

3.1 Работа при загрузке операционной системы в безопасном режиме 11

4 Работа в Консоли Управления Device Monitor 13

4.1 Начало работы с Консолью управления 13

4.1.1 Авторизация и соединение с сервером InfoWatch Device Monitor 13

4.1.2 Главное окно Консоли управления 14

Настройка элементов главного окна Консоли управления 16

4.1.3 Разделы Консоли управления 17

4.2 Управление учетными записями и ролями Консоли управления 18

4.2.1 Учетные записи пользователей Консоли управления 20

Добавление учетной записи Консоли управления 21

Редактирование учетной записи Консоли управления 25

Блокирование и разблокирование учетной записи Консоли управления 26

Удаление и восстановление учетной записи Консоли управления 26

4.2.2 Роли пользователей Консоли управления 27

Добавление роли пользователя Консоли управления 28

Редактирование роли пользователя Консоли управления 31

Удаление роли пользователя Консоли управления 32

4.2.3 Аудит действий по управлению схемой безопасности в Консоли управления 32

Просмотр журнала аудита 33

Фильтрация записей в журнале аудита 36

Удаление записей из журнала аудита 40

Экспорт записей журнала аудита 40

Анализ журнала аудита в Microsoft Excel 40

4.3 Общие настройки Системы 41

4.3.1 Общие настройки работы Агентов 42

4.3.2 Перехват веб-почты 45

4.3.3 Контроль сетевых соединений 45

4.3.4 Контроль мессенджеров 48

4.3.5 Контроль сетевого трафика 49

Добавление серверов 51

4.3.6 Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor 54

4.3.7 Настройки сервера Device Monitor. Соединение с сервером Платформы 57

Параметры соединения ... 58
4.3.8 Соединение и синхронизация со службами каталогов ... 60
Автоматическая установка Агентов ... 64
4.3.9 Настройка уведомлений сотрудников о нарушении правил ... 66
4.3.10 Исключение приложений из перехвата ... 69
4.3.11 Контроль приложений и снимки экрана ... 75
4.3.12 Контроль ввода с клавиатуры ... 77
4.3.13 Хранение событий ... 78
4.3.14 Синхронизация политик Traffic Monitor ... 80
4.3.15 Работа с Менеджером управления серверами ... 81
4.3.16 Настройка статусов активности Агентов ... 82
4.3.17 Остановка и запуск агента Device Monitor ... 85
Удаленная остановка/запуск агента на рабочей станции под управлением ОС MS Windows или macOS ... 85
Локальная остановка/запуск агента на рабочей станции под управлением ОС MS Windows ... 86
4.3.18 Настройка распространения Агентов ... 87
4.3.19 Автоматическое обновление Агентов ... 89
4.3.20 Настройка перехвата звукового окружения ... 91
4.3.21 Настройка отправки данных в продукты ... 93
4.3.22 Инженерные настройки агента ... 96
Настройки агента ... 98
4.4 Управление схемой безопасности ... 100
4.4.1 Организация схемы безопасности ... 101
Политики безопасности и правила ... 101
Сотрудники и группы сотрудников ... 105
Компьютеры и группы компьютеров ... 105
Загрузка схемы безопасности на контролируемые компьютеры ... 106
4.4.2 Общие действия при управлении схемой безопасности ... 106
Просмотр действующей версии схемы безопасности ... 106
Просмотр предыдущих версий схемы безопасности ... 108
Комментарии к схеме безопасности ... 109
Редактирование схемы безопасности ... 109
Обновление схемы безопасности ... 112
Экспорт/импорт конфигурации ... 112
4.4.3 Настройка схемы безопасности ... 114
Политики безопасности ... 115
Правила ... 120
Сотрудники ... 183
Компьютеры ... 193
Белые списки устройств ... 211
Категории сигнатур ... 219
Приложения ... 223
Блокада приложений ... 229

Ресурсы ... 235
Файловая статистика ... 240
Исключение мусорного трафика ... 246
4.4.4 Временный доступ сотрудника к сети ... 250
4.4.5 Временный доступ сотрудника к устройствам ... 251
4.5 Просмотр событий DM ... 253
4.5.1 Фильтры событий ... 265
4.5.2 Удаление событий ... 267
4.6 Удаленная установка, обновление и удаление Агентов ... 268
4.6.1 Просмотр задач ... 269
4.6.2 Подготовка к первичной установке Агентов. Агент распространения ... 272
Включение административных разделяемых ресурсов ... 274
Настройки брандмауэра ... 274
4.6.3 Обнаружение рабочих станций для установки агентов ... 275
4.6.4 Создание задачи первичного распространения ... 276
4.6.5 Создание задачи обновления ... 282
4.6.6 Создание задачи смены пароля деинсталляции ... 284
4.6.7 Создание задачи удаления ... 285
4.6.8 Запуск, остановка, редактирование и удаление задачи ... 286
4.6.9 Ошибки установки Агентов ... 288
4.6.10 Создание пакета установки ... 290
4.6.11 Создание шаблона задачи распространения ... 292
4.7 Дополнительные возможности ... 295
4.7.1 Фильтрация табличных данных ... 295
Фильтр по дате ... 296
Использование стандартных фильтров ... 296
Пользовательский фильтр ... 297
Редактирование фильтра ... 298
Отмена фильтра ... 299
4.7.2 Группирование и сортировка записей ... 299
4.7.3 Клавиши быстрого доступа ... 300
5 ПОЛЬЗОВАТЕЛЬСКОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ... 305
6 Глоссарий ... 310

В настоящем руководстве вы сможете найти сведения по работе и решению задач.
InfoWatch Device Monitor (далее Device Monitor или Модуль/Система) – программный продукт, позволяющий осуществлять перехват данных в информационных потоках компании.

1 Аудитория

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

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Microsoft Windows.

2 Комплект документов

В комплект документации по InfoWatch Device Monitor входят:

- «InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию». Содержит описание установки, удаления и настройки модуля.
- «InfoWatch Device Monitor. Руководство пользователя». Содержит описание порядка работы с компонентами модуля.

Сопутствующая документация по продукту InfoWatch Traffic Monitor включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание порядка установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor (далее Traffic Monitor).
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию Системы (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание порядка работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, составление политик для обработки объектов).
- «InfoWatch Traffic Monitor. Справочник по конфигурационным файлам». Содержит пояснения к часто используемым конфигурационным файлам.

Сопутствующая документация по продукту InfoWatch Activity Monitor включает в себя:

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

3 Функции InfoWatch Device Monitor

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 модуля InfoWatch Device Monitor:

Название функции	Соответствующее правило политик безопасности
Контроль приложений	Правило для Application Monitor
Контроль звукового окружения. Используется только системой InfoWatch Activity Monitor	Правило для Audio Record Control
Контроль буфера обмена	Правило для Clipboard Monitor
Контроль облачных хранилищ	Правило для Cloud Storage Monitor
Контроль доступа к внешним устройствам	Правило для Device Monitor
Контроль подключения с помощью Microsoft RDP или Citrix ICA	Правило для Device Monitor
Контроль файлов, копируемых с/на съемные устройства, сетевые ресурсы и ресурсы, подключенные через терминальную сессию	Правило для File Monitor
Контроль чтения и записи файлов приложениями	Правило для File Operations Monitor
Контроль трафика, передаваемого по протоколам FTP и FTPS	Правило для FTP Monitor
Контроль трафика, передаваемого по протоколам HTTP и HTTPS	Правило для HTTP(S) Monitor
Контроль систем мгновенного обмена сообщениями: Skype, Telegram, Facebook, WhatsApp, VK (ВКонтакте), Jabber (протокол XMPP), протокол MMP, Яндекс Мессенджер	Правило для IM Client Monitor
Контроль ввода текста с клавиатуры	Правило для Keyboard Monitor

Название функции	Соответствующее правило политик безопасности
Контроль систем передачи почтовых сообщений по протоколам SMTP, IMAP, POP3, Outlook, HTTPS	Правило для Mail Monitor
Контроль передачи данных по сетевым соединениям вне корпоративной сети	Правило для Network Monitor
Мониторинг печати на контролируемых компьютерах	Правило для Print Monitor
Контроль снимков экрана	Правило для ScreenShot Control Monitor
Контроль экрана компьютера	Правило для ScreenShot Monitor
Видеозапись экрана с запуском по триггерам	Правило для Screen Record Video
Контроль активности сотрудника и сбор статистики. Используется только системами InfoWatch Activity Monitor и InfoWatch Prediction	Правило для Statistics

Важно!

Входящие соединения для серверных приложений будут перехвачены только на агентах Device Monitor, установленных на рабочих станциях с ОС Windows 8 и более поздних.

Важно!

Для рабочих станций под управлением ОС Astra Linux, РЕД ОС или ОС Альт Рабочая станция доступны следующие функции контроля:

Название функции	Соответствующее правило политик безопасности	Примечание
Контроль буфера обмена	Правило для Clipboard Monitor	Не поддерживается на ОС Astra Linux
Контроль облачных хранилищ	Правило для Cloud Storage Monitor	–

Название функции	Соответствующее правило политик безопасности	Примечание
Контроль доступа к внешним устройствам	Правило для Device Monitor	Поддерживается контроль только съемных устройств хранения и MTP-устройств
Контроль файлов, копируемых с /на съемные устройства и сетевые ресурсы	Правило для File Monitor	–
Контроль трафика, передаваемого по протоколам FTP и FTPS	Правило для FTP Monitor	–
Контроль трафика, передаваемого по протоколам HTTP и HTTPS	Правило для HTTP(S) Monitor	–
Контроль систем мгновенного обмена сообщениями: Facebook, Telegram, VK (ВКонтакте), Jabber (протокол XMPP)	Правило для IM Client Monitor	На рабочих станциях под управлением ОС семейства Linux доступен контроль только десктопной версии Telegram
Контроль ввода текста с клавиатуры	Правило для Keyboard Monitor	Не поддерживается на ОС Astra Linux
Контроль систем передачи почтовых сообщений по протоколам SMTP, POP3, IMAP и HTTPS	Правило для Mail Monitor	–
Мониторинг печати на контролируемых компьютерах	Правило для Print Monitor	–
Контроль снимков экрана	Правило для ScreenShot Control Monitor	Не поддерживается на ОС Astra Linux
Контроль активности сотрудника и сбор статистики	Правило для Statistics	Не поддерживается на ОС Astra Linux

Примечание.

Часть функций доступна как в нормальном, так и в безопасном режиме работы операционной системы (см. "Работа при загрузке операционной системы в безопасном режиме").

Мониторинг и контроль действий сотрудников выполняется на контролируемых компьютерах. На контролируемые компьютеры устанавливаются агентские модули Системы.
В состав модуля входят перехватчики:

- Application Monitor
- Audio Record Control
- Clipboard Monitor
- Cloud Storage Monitor
- Device Monitor
- File Monitor
- File Operations Monitor
- FTP Monitor
- HTTP(S) Monitor
- IM Client Monitor
- Keyboard Monitor
- Mail Monitor
- Network Monitor
- Print Monitor
- ScreenShot Control Monitor
- ScreenShot Monitor
- Statistics

Подробнее о работе перехватчиков см. "Правила".

> **Примечание.**
>
> Для рабочих станций под управлением ОС Astra Linux работа перехватчиков поддержана в ограниченном режиме (подробнее об особенностях работы перехватчиков на различных ОС смотрите в описаниях правил).

На агентах Device Monitor проводится анализ перехваченных данных с использованием технологий детектирования:

- форматов файлов;
- текстовых объектов;

  > **Примечание:**
  >
  > В качестве текстовых объектов могут быть заданы названия и значения свойств, которые извлекаются агентом Device Monitor из PDF-документов (подробнее см. Пример 3 в статье "Работа с текстовыми объектами", "*Решение задач при работе в консоли Traffic Monitor*". "*Traffic Monitor. Руководство пользователя*").

- терминов/баз контентной фильтрации (БКФ).

3.1 Работа при загрузке операционной системы в безопасном режиме

Часть функций InfoWatch Device Monitor доступна, если операционная система загружена в безопасном режиме (с поддержкой или без поддержки сети).

В следующей таблице перечислены функции, доступные при загрузке операционной системы в безопасном режиме.

Функция InfoWatch Device Monitor	Режим работы операционной системы
Контроль доступа к периферийным устройствам (исключение составляют устройства, доступ к которым в безопасном режиме запрещен операционной системой)	Безопасный режим (Safe Mode) Безопасный режим с поддержкой сети (Safe Mode with Networking)
Контроль записи информации в файлы на съемных устройствах	Безопасный режим (Safe Mode) Безопасный режим с поддержкой сети (Safe Mode with Networking)
Мониторинг контролируемых компьютеров	Безопасный режим с поддержкой сети (Safe Mode with Networking)
Контроль сетевой активности (Skype, Telegram, WhatsApp)	Безопасный режим с поддержкой сети (Safe Mode with Networking)
Контроль трафика, передаваемого по протоколу FTP/FTPS	Безопасный режим с поддержкой сети (Safe Mode with Networking)
Контроль передачи данных по сетевым соединениям вне корпоративной сети	Безопасный режим с поддержкой сети (Safe Mode with Networking)

4 Работа в Консоли Управления Device Monitor

Консоль управления предназначена для решения следующих задач:

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

Для работы в Консоли управления пользователи должны быть знакомы с основами работы в среде операционной системы Microsoft Windows.
Информация о порядке работы в Консоли управления изложена в следующих разделах:

- Начало работы с Консолью управления. Общие приемы при работе с Консолью управления InfoWatch Device Monitor (запуск, настройка интерфейса).
- Управление учетными записями и ролями Консоли управления. Способы выполнения задач, связанных с администрированием InfoWatch Device Monitor: управление учетными записями Консоли управления InfoWatch Device Monitor, работа с журналом аудита и др.
- Общие настройки Системы. Определение глобальных параметров, единых для всех политик и правил.
- Управление схемой безопасности. Порядок работы со схемой безопасности, настройка конфигурационных параметров схемы безопасности.
- Просмотр событий. Просмотр сведений о работе с контролируемыми устройствами и каналами передачи данных на контролируемых компьютерах.
- Удаленная установка, обновление и удаление Агентов. Описание установки и настройки Агента InfoWatch Device Monitor с помощью Консоли управления.
- Дополнительные возможности. Описание вспомогательных функций, используемых для более удобной работы с Консолью управления InfoWatch Device Monitor: фильтрация, группирование и сортировка записей; сочетания клавиш для быстрого доступа к функциям Консоли управления.

4.1 Начало работы с Консолью управления

Общие принципы работы с Консолью управления изложены в следующих подразделах:

- Авторизация и соединение с сервером InfoWatch Device Monitor
- Главное окно Консоли управления
- Разделы Консоли управления

4.1.1 Авторизация и соединение с сервером InfoWatch Device Monitor

При работе с Консолью управления требуется постоянное соединение с Сервером InfoWatch Device Monitor. Для этого необходимо выполнить **авторизацию**, в процессе которой определяются права пользователя на запуск Консоли управления.

При первом запуске Консоли управления используются данные (имя пользователя и пароль) учетной записи, которой назначена роль **Суперпользователь** (учетная запись Суперпользователя создается в процессе установки Сервера, подробнее см. "Traffic Monitor. Руководство по установке", статья "Порядок установки серверной части InfoWatch Device Monitor").

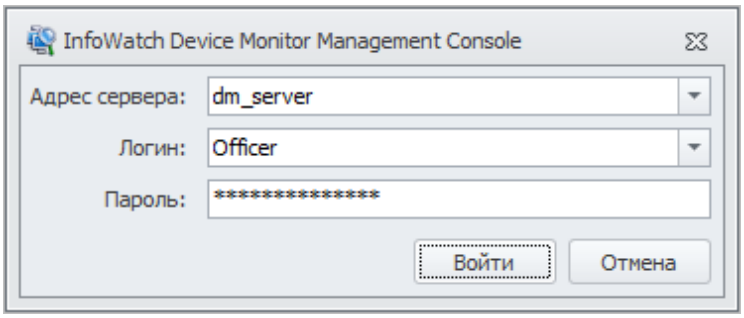
Чтобы начать работу с Консолью управления:

1. Запустите Консоль управления. Для этого в меню **Пуск** выберите пункт **Программы** > **InfoWatch** > **Device Monitor** > **Консоль управления** либо используйте ярлык на рабочем столе (создается по умолчанию при установке).
2. Выполните процедуру авторизации, как описано ниже.

Успешное прохождение авторизации возможно только при выполнении следующих условий:

- в базе данных существует учетная запись с указанными параметрами;
- учетной записи назначена роль;
- учетная запись является активной (не удалена);
- учетная запись не заблокирована.

Данные для авторизации вводят в диалоговом окне подключения.



Параметр	Описание
Адрес сервера	Доменное имя сервера, к которому будет подключена Консоль управления. По умолчанию взаимодействие между сервером и Консолью управления осуществляется через порт 15003. Если этот порт был изменен, то адрес сервера нужно записывать в виде: `dm_server:port`.
Логин	Имя учетной записи пользователя
Пароль	Пароль пользователя. Перед заполнением проверьте раскладку клавиатуры.

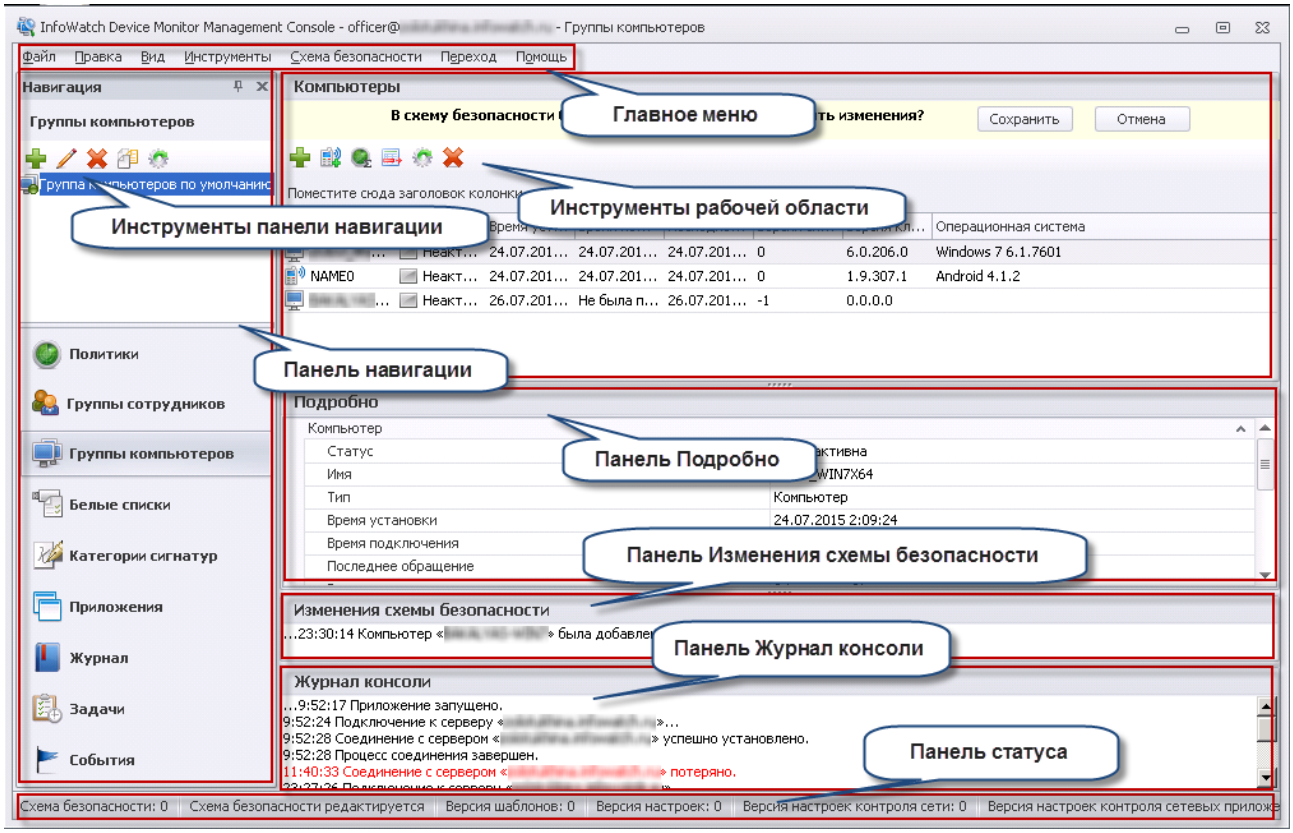
При первом запуске Консоли управления поля диалогового окна **Подключение** – пустые. В дальнейшем поля **Адрес сервера** и **Пользователь** будут заполнены данными, соответствующими последней попытке авторизации. Поле **Пароль** необходимо заполнять при каждой попытке авторизации.

Проследить состояние соединения с Сервером можно, просмотрев системные сообщения, выводимые на панели **Журнал консоли** (см. "Главное окно Консоли управления ").

При необходимости, вы можете вызвать окно авторизации и изменить введенные параметры, подключившись к тому же или другому серверу, от имени той же или другой учетной записи. Для этого в главном меню выберите команду **Файл** > **Подключиться**, затем подключитесь к Серверу, как описано выше.

4.1.2 Главное окно Консоли управления

После успешной авторизации в Консоли управления на экран выводится главное окно:



Информация по настройке внешнего вида главного окна содержится в подразделе "Настройка элементов главного окна Консоли управления".

В состав главного окна входят элементы, необходимые для работы с Консолью управления:

- В **главном меню** находятся команды, при помощи которых осуществляется доступ ко всем основным функциям Консоли управления.
- **Панель навигации** предназначена для перехода между разделами Консоли управления и управления группами элементов, входящих в выбранный раздел.
- **Рабочая область главного окна** предназначена для просмотра элементов выбранной группы и выполнения операций над данными элементами.
- На **панелях инструментов** находятся ряды кнопок для быстрого доступа к некоторым функциям Консоли. Панели инструментов располагаются в Панели навигации (для элементов выбранного раздела) и в рабочей области (для выбранного элемента раздела).
- На панели **Подробно** отображаются расширенные сведения о свойствах выбранного элемента.
- На панели **Изменения схемы безопасности** отображаются все изменения, сделанные текущим пользователем и не сохраненные в схеме безопасности.
- Панель **Журнал консоли** предназначена для вывода системных сообщений.

При выполнении действий над отдельным объектом доступ ко многим командам можно получить из контекстного меню объекта. Для вызова контекстного меню щелкните правой кнопкой мыши по нужному объекту.

Общая информация по состоянию на текущий момент выводится в строке статуса, расположенной в нижней части главного окна. В частности, отображаются сведения:

- номер текущей версии схемы безопасности;
- режим, в котором находится схема безопасности;

- в разделе **Группы компьютеров** - также версии различных элементов контроля.

Настройка элементов главного окна Консоли управления

В процессе работы вы можете настраивать вид и местоположение **Панели навигации** и панелей **Подробно**, **Журнал консоли**.

Действие	Шаги
Удалить панель с экрана	Откройте пункт **Вид** в главном меню и щелкните левой кнопкой мыши по названию панели, которую вы хотите удалить с экрана. Чтобы снова вывести панель на экран, повторите данное действие. **Примечание**: Чтобы удалить **Панель навигации**, можно также использовать кнопку ⊠ в правом верхнем углу панели.
Включить/отключить режим автоматического свертывания панели	Воспользуйтесь кнопкой 📌, расположенной в правом верхнем углу панели (при этом возможность изменить расположение панели будет заблокирована)
Изменить местоположение панели	Щелкните левой кнопкой мыши по заголовку панели и, не отпуская кнопку, перетащите панель в другое место экрана. Затем отпустите левую кнопку мыши, чтобы установить панель на новое место
Вернуть панель в первоначальное положение	Дважды щелкните левой кнопкой мыши по заголовку панели
Изменить размер панели	Подведите курсор мыши к границе панели. Когда курсор мыши примет вид двунаправленной стрелки, нажмите левую кнопку мыши и, не отпуская кнопку, перетащите границу в нужном направлении. Когда панель достигнет нужного размера, отпустите левую кнопку мыши
Вернуть предустановленные настройки интерфейса	Откройте пункт **Вид** в главном меню и выберите пункт **Сбросить настройки интерфейса**. После этого необходимо перезапустить Консоль DM. **Примечание:** В этом случае будет установлен прежний порядок следования колонок и группировка на **Рабочей области главного окна**, а также возвращены предустановленные настройки **Панели навигации.**

На панели **Подробно** выводятся свойства отдельных элементов. Вы можете свернуть или раскрыть таблицу свойств любого элемента.

Чтобы настроить отображение панели Подробно, дважды щелкните левой кнопкой мыши по строке заголовка таблицы свойств или воспользуйтесь кнопкой со стрелкой, расположенной в правой части строки заголовка таблицы свойств.

Чтобы скрыть/отобразить панель инструментов или панель статуса, щелкните правой кнопки мыши в области панели инструментов или панели статуса. Затем в раскрывшемся контекстном меню

отметьте те элементы, которые будут отображены на экране (по умолчанию выделена только панель статуса).

4.1.3 Разделы Консоли управления

Консоль управления включает в себя следующие разделы: **Политики**, **Группы сотрудников**, **Группы компьютеров**, **Белые списки**, **Категории сигнатур**, **Приложения**, **Журнал**, **Задачи и События**. Каждому разделу соответствует одноименная область Панели навигации.

Чтобы перейти к нужному разделу, выполните одно из следующих действий:

- в главном меню выберите пункт **Переход**. Затем в раскрывшемся меню щелкните левой кнопкой мыши по названию того раздела, к которому вам нужно перейти;
- воспользуйтесь кнопками Панели навигации.

Разделы **Политики** , **Группы сотрудников**, **Группы компьютеров**, **Белые списки** и **Категории сигнатур** предназначены для управления схемой безопасности, раздел **Приложения** - для контроля запуска приложений, раздел **Журнал** - для контроля действий по управлению схемой безопасности, **Задачи** - для управления задачами установки и удаления Агентов, **События** - для просмотра событий с контролируемых компьютеров. Подробное описание функций каждого раздела приведено в таблице:

Название раздела	Назначение раздела
Политики	Управление политиками безопасности: создание политик безопасности, настройка правил для каждой политики
Группы сотрудников	Управление сотрудниками: создание групп сотрудников, распределение сотрудников по группам
Группы компьютеров	Управление контролируемыми компьютерами: создание групп компьютеров, распределение контролируемых компьютеров по группам
Белые списки	Управление списками устройств, доступ к которым безусловно разрешен
Категории сигнатур	Просмотр и управление категориями сигнатур, с помощью которых правила File Monitor могут распространяться на определенные форматы файлов
Приложения	Формирование и создание списков приложений для контроля их запуска
Журнал	Аудит действий по управлению схемой безопасности
Задачи	Централизованная установка, обновление и удаление Агентов InfoWatch Device Monitor на компьютеры
События	Просмотр сведений о работе сотрудников на контролируемых компьютерах с использованием контролируемых средств

4.2 Управление учетными записями и ролями Консоли управления

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

В Консоли управления используется один предустановленный пользователь – **Суперпользователь,** обладающий всеми правами при работе в Консоли. Он не предназначен для повседневной работы с Системой, рекомендуется использовать исключительно для первоначальной настройки Консоли управления, создания учетной записи для Администратора, а затем – только в аварийных условиях.

Для разграничения полномочий пользователей, работающих с Консолью управления, 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 Консоли управления используются следующие предустановленные роли:

- **Администратор** – роль администратора Консоли, управляющая другими учетными записями Консоли;
- **Офицер безопасности** – роль конечного пользователя Консоли, которая управляет схемой безопасности и настройками Сервера;
- **Офицер безопасности группы** – роль конечного пользователя Консоли, которая управляет группами сотрудников или компьютеров.

Вы можете настроить пользовательские роли, которые будут основаны на предустановленных и включать в себя более тонкие настройки управления (см. "Добавление роли пользователя Консоли управления").

Список доступных действий для предустановленных ролей:

Действия	Администратор	Офицер безопасности	Офицер безопасности группы
Просмотр журнала аудита		+	
Экспорт записей журнала аудита		+	
Удаление записей из журнала аудита			
Учетные записи пользователей Консоли управления	+	+	
Добавление, редактирование, удаление учетных записей пользователей Консоли управления	+		

Действия	Администратор	Офицер безопасности	Офицер безопасности группы
Назначение/ удаление ролей для пользователей Консоли управления	+		
Блокировка/разблокировка учетных записей пользователей Консоли управления	+		
Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor		+	
Настройки сервера Device Monitor. Соединение с сервером Платформы (для отправки данных в Activity Monitor и Prediction)		+	
Просмотр предыдущих версий схем безопасности		+	
Редактирование схемы безопасности		+	
Импорт/экспорт политик безопасности и правил		+	
Просмотр событий		+	
Удаленная установка, обновление и удаление Агентов Device Mionitor		+	
Временный доступ сотрудника к сети		+	
Временный доступ сотрудника к устройствам		+	
Создание группы			+
Просмотр и управление группами сотрудников, Просмотр и управление			+

Действия	Администратор	Офицер безопасности	Офицер безопасности группы
группами компьютеров, Просмотр событий группы			
Просмотр белых списков, управление белыми списками			+
Управление агентами		+	+

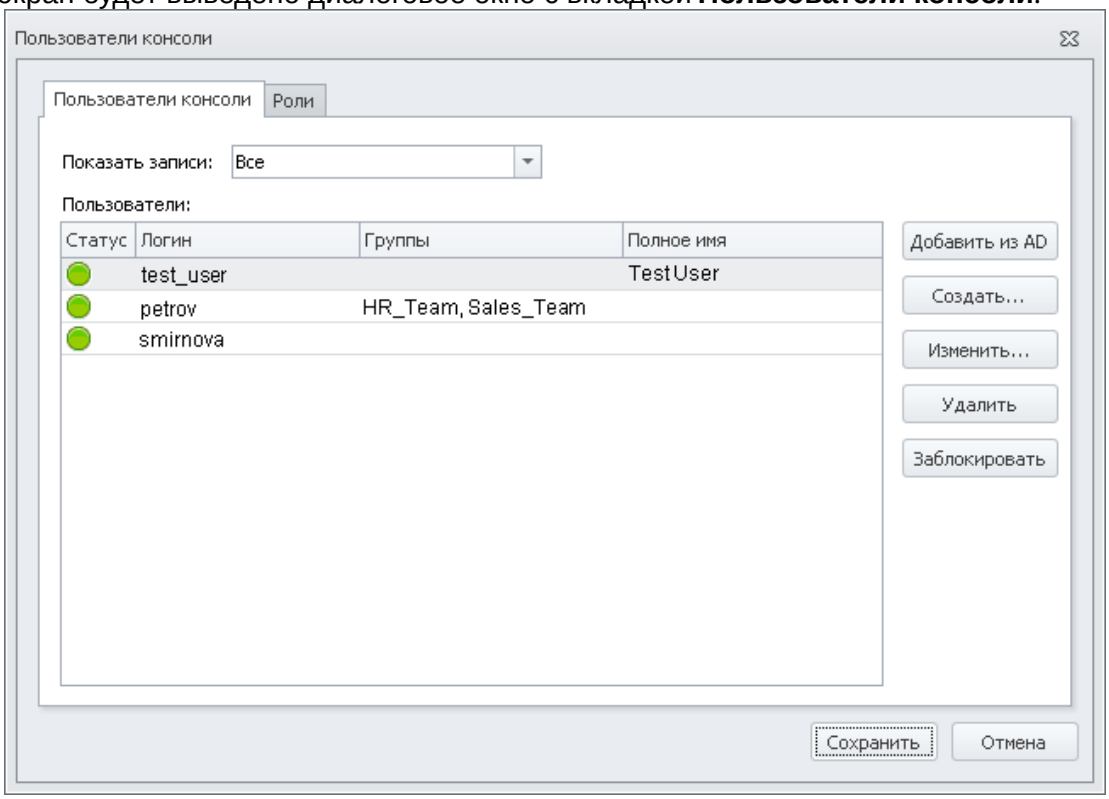
Более подробная информация об управлении учетными записями Консоли управления содержится в подразделах:

- Учетные записи пользователей Консоли управления
- Добавление учетной записи Консоли управления
- Блокирование и разблокирование учетной записи Консоли управления
- Редактирование учетной записи Консоли управления
- Удаление и восстановление учетной записи Консоли управления
- Аудит действий по управлению схемой безопасности в Консоли управления

4.2.1 Учетные записи пользователей Консоли управления

Чтобы просмотреть информацию об учетных записях Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**. На экран будет выведено диалоговое окно с вкладкой **Пользователи консоли**.



2. В верхней части данного окна расположено поле **Показать записи**. Из раскрывающегося списка в этом поле выберите тип отображаемых учетных записей:

- **Все**. Все учетные записи, независимо от их статуса.
- **Активные**. Список всех действующих учетных записей.
- **Заблокированные**. Учетные записи, которые были заблокированы, но могут быть разблокированы (см. "Блокировка/разблокировка учетных записей пользователей Консоли управления").
- **Удаленные**. Список учетных записей, которые были удалены. Информация о действиях, которые эти пользователи выполнили, сохраняется в Системе. Удаленные учетные записи могут быть восстановлены (см. "Удаление и восстановление учетной записи Консоли управления").

> **Примечание.**
>
> Работа с Консолью управления может осуществляться от имени тех учетных записей, которые находятся в списке **Активные**.

Для учетной записи отображаются следующие элементы:

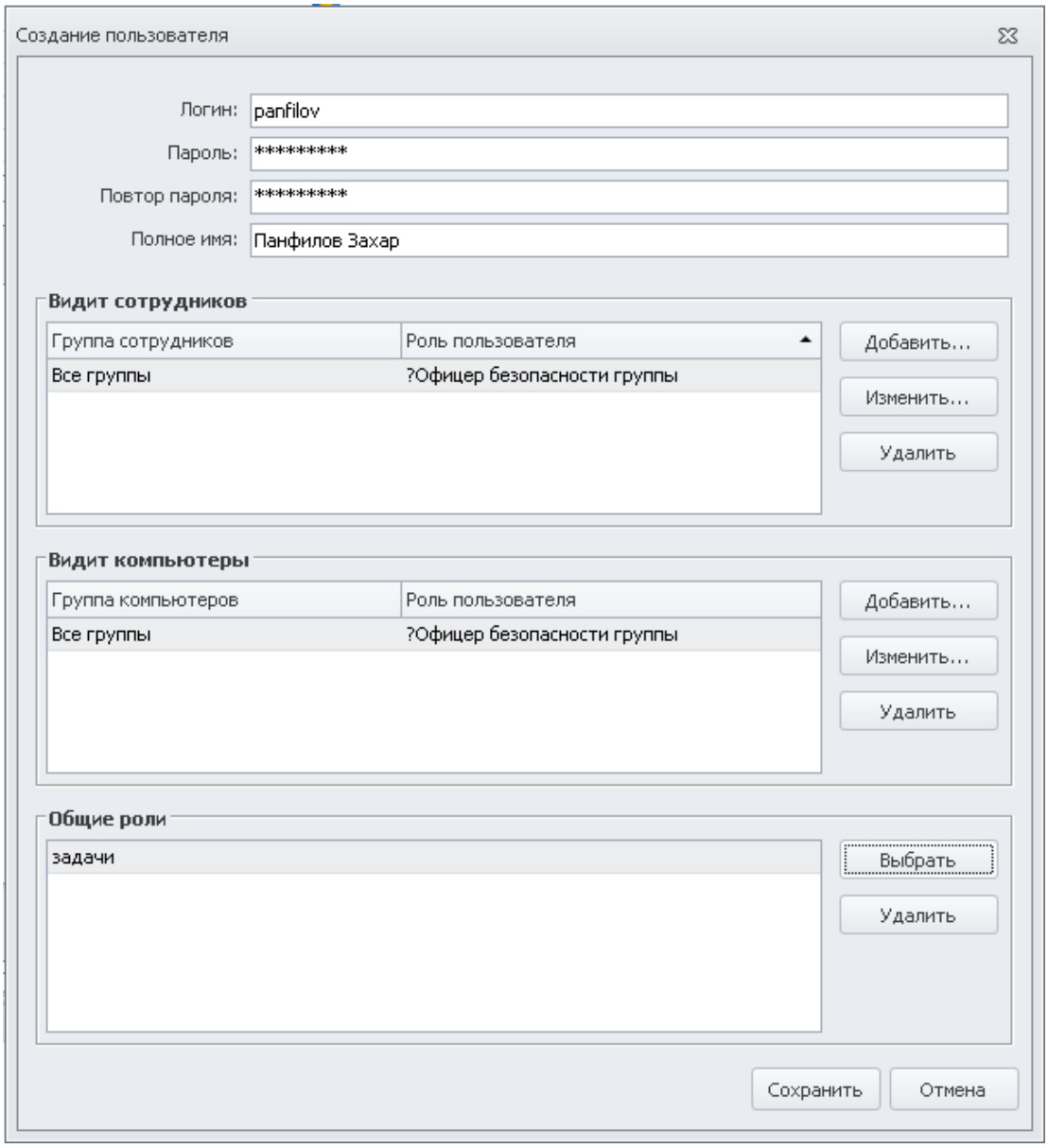
- **Статус**. Признак того, является ли учетная запись активной (), заблокированной () или удаленной ().
- **Логин**. Имя учетной записи.
- **Группы**. Группы, доступные пользователю.
- **Полное имя**. Фамилия, имя и отчество пользователя.

Обязательными атрибутами учетной записи являются имя, пароль, роль и признак блокирования. Подробное описание ролей вы можете найти в разделе "Роли пользователей Консоли управления".

Добавление учетной записи Консоли управления

Чтобы добавить новую учетную запись Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**.
2. Нажмите на кнопку **Создать**, расположенную в правой части диалогового окна на вкладке **Пользователи консоли**.
3. В открывшемся диалоговом окне введите данные учетной записи:
   - **Логин**. Имя учетной записи.
   - **Пароль**, **Повтор пароля**. Пароль учетной записи.
   - **Полное имя**. Фамилия, имя и отчество пользователя.



4. Задайте видимость сотрудников и компьютеров для пользователя (см. страницу "Назначение ролей пользователю"):
   - **Видит сотрудников**. Задание списка доступных пользователю групп сотрудников и ролей, назначенных на них.
   - **Видит компьютеры**. Задание списка доступных пользователю групп компьютеров и ролей, назначенных на них.
   - **Общие роли**. Список дополнительных ролей пользователя из имеющихся в Системе.

> **Важно!**
>
> Необходимо назначить пользователю как минимум одну роль любого типа, а также роль на каждую группу, доступную пользователю.

5. Нажмите **Сохранить**.
   После этого диалоговое окно **Создание пользователя** будет закрыто. Сведения о новой учетной записи появятся в диалоговом окне **Пользователи консоли** на одноименной вкладке.

> **Примечание.**
>
> Новая учетная запись находится в активном состоянии. При необходимости вы можете заблокировать учетную запись (см. раздел "Блокирование и разблокирование учетной записи Консоли управления").

Чтобы добавить пользователя из Active Directory или ALD:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**.
2. Нажмите на кнопку **Добавить из AD**, расположенную в правой части диалогового окна на вкладке **Пользователи консоли**.
3. В открывшемся окне **Добавление пользователя из AD** выберите пользователя из группы (или воспользуйтесь поиском).
4. Назначьте роли добавленному пользователю (подробнее см. "Назначение ролей пользователю").
5. Нажмите **Сохранить.**

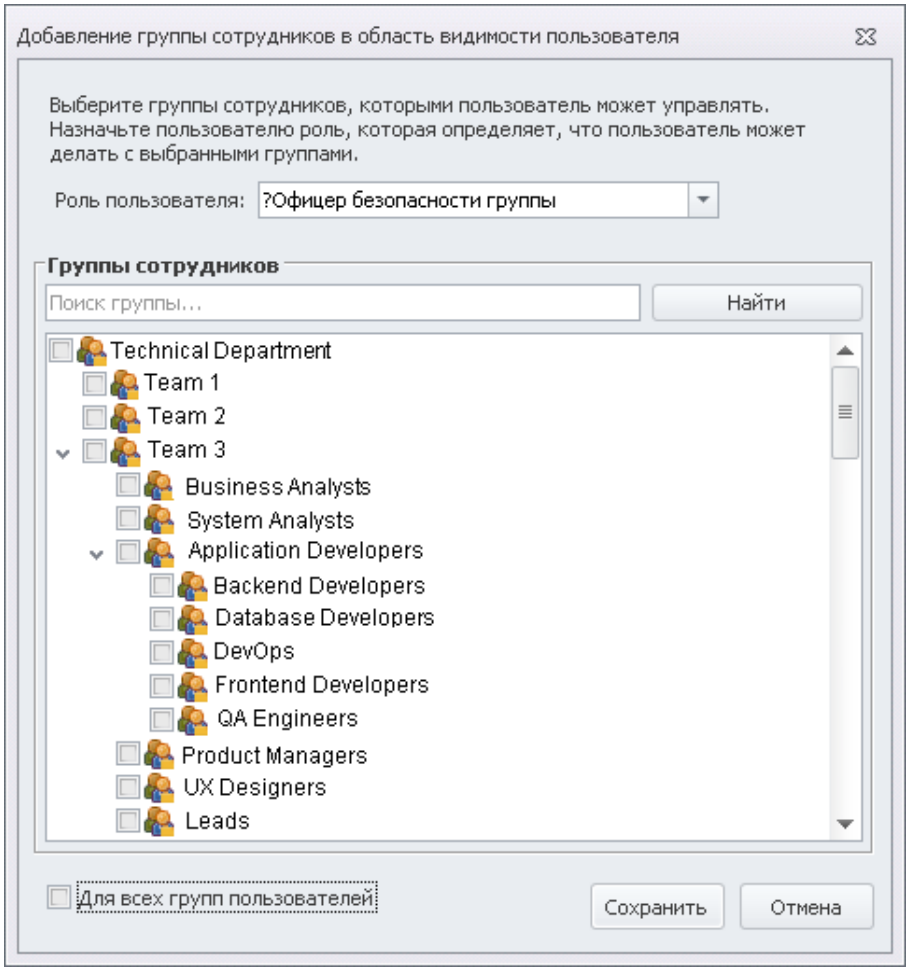
> **Примечание.**
>
> В окне **Пользователи консоли** будут автоматически заполнены логин и полное имя импортированного пользователя. Пароль пользователя будет соответствовать его паролю в AD.

Назначение ролей пользователю

Добавление роли пользователя на группы сотрудников (компьютеров)

Чтобы добавить группу сотрудников в область видимости пользователя:

1. Перейдите в окно **Создание пользователя** (**Изменение пользователя**).
2. В блоке **Видит сотрудников** (**Видит компьютеры**) нажмите кнопку **Добавить**.



3. В открывшемся окне:
   - Укажите **Роль пользователя** из предложенных;
   - Выберите одну или несколько групп сотрудников (групп компьютеров) из древовидной структуры или воспользуйтесь поиском. Выберите **Для всех групп пользователей** (**Для всех групп компьютеров**), если необходимо добавить все группы сразу.
   - Нажмите **Сохранить**.
4. В окне **Изменение пользователя** нажмите **Сохранить**.

Редактирование роли пользователя на группы сотрудников (компьютеров)

Чтобы изменить права доступа в область видимости пользователя:

1. Перейдите в окно **Изменение пользователя**.
2. В блоке **Видит сотрудников** (**Видит компьютеры**) выберите нужную группу.
3. Нажмите кнопку **Изменить**.
4. В открывшемся окне назначьте роль, определяющую действия пользователя на группу. Дальнейшие возможности по действиям с сотрудниками (компьютерами) будут осуществляться согласно привилегиям выбранной роли.
5. Нажмите **Сохранить**.

Чтобы снять роль с пользователя:

1. Перейдите в окно **Изменение пользователя**.
2. В блоке **Видит сотрудников** (**Видит компьютеры**) выберите нужную группу.

3. Нажмите кнопку **Удалить**.
4. Нажмите **Да** для подтверждения. Выбранная роль будет снята с пользователя.

Настройка общих ролей пользователя

Чтобы назначить общие роли пользователю:

1. Перейдите в окно **Создание пользователя** или **Изменение пользователя**.
2. В блоке **Общие роли** нажмите кнопку **Выбрать**.
3. В открывшемся окне выберите нужные роли, которые определят доступные пользователю действия, из списка.
4. Нажмите **Сохранить**.

Чтобы снять общие роли с пользователя:

1. Перейдите в окно **Изменение пользователя**.
2. В блоке **Общие роли** выберите роль для удаления.
3. В открывшемся окне нажмите кнопку **Удалить**. Общая роль будет снята с пользователя.

Редактирование учетной записи Консоли управления

Важно!

При редактировании роли, назначенной учетной записи, в настоящий момент авторизованной в Консоли управления, происходит следующее. После сохранения результатов редактирования учетной записи, соединение с сервером автоматически прерывается. Затем пользователю предлагается пройти авторизацию с новыми параметрами. При этом все не сохраненные данные будут утеряны.

Чтобы отредактировать параметры учетной записи Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**. На экран будет выведено диалоговое окно **Пользователи консоли**.
2. На вкладке **Пользователи консоли** выберите строку с названием учетной записи, которую нужно отредактировать.
3. Нажмите на кнопку **Изменить**, расположенную в правой части данного окна, или дважды щелкните левой кнопкой мыши по выделенной строке.
4. В открывшемся диалоговом окне **Изменение пользователя** отредактируйте параметры учетной записи, описанные в разделе "Добавление учетной записи Консоли управления").
5. После того как все необходимые параметры будут настроены, нажмите на кнопку **Сохранить**.
6. Чтобы сделанные изменения окончательно вступили в силу, нажмите на кнопку **Сохранить** в диалоговом окне **Пользователи консоли**.

Важно!

Недоступно любое редактирование предустановленных пользователей, кроме изменения пароля.

Блокирование и разблокирование учетной записи Консоли управления

Сведения о состоянии блокировки учетных записей отображаются в диалоговом окне **Пользователи консоли**.

Важно!

Вы можете заблокировать любую учетную запись, за исключением учетной записи Суперпользователя и той учетной записи, которую вы использовали для авторизации в Системе.
Пользователь, учетная запись которого заблокирована, не может авторизоваться в Системе.

Чтобы заблокировать/разблокировать учетную запись Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**. Откроется диалоговое окно **Пользователи консоли**.
2. На вкладке **Пользователи консоли** выберите строку с названием нужной учетной записи.
3. Измените состояние блокировки:
   - Если учетная запись была заблокирована (статус ), нажмите **Разблокировать**.
   - Если учетная запись была разблокирована (статус ), нажмите **Заблокировать**.
4. Чтобы сделанные изменения вступили в силу, нажмите **Сохранить**.

Удаление и восстановление учетной записи Консоли управления

После удаления учетная запись перемещается в список удаленных учетных записей. При этом сведения об учетной записи сохраняются в базе данных.

Важно!

Учетные записи Суперпользователя и предустановленных пользователей не могут быть удалены.

Удаленные учетные записи можно просматривать в диалоговом окне **Пользователи консоли**. Для этого нужно выбрать значение **Удаленные** из раскрывающегося списка в поле **Показать записи**.

Чтобы удалить учетную запись Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**. На экран будет выведено диалоговое окно **Пользователи консоли**.
2. Выберите строку с именем учетной записи, которую нужно удалить.
3. Нажмите на кнопку **Удалить**, расположенную в нижней части данного окна.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление.
5. Чтобы сделанные изменения вступили в силу, нажмите на кнопку **Сохранить** в диалоговом окне **Пользователи консоли**.

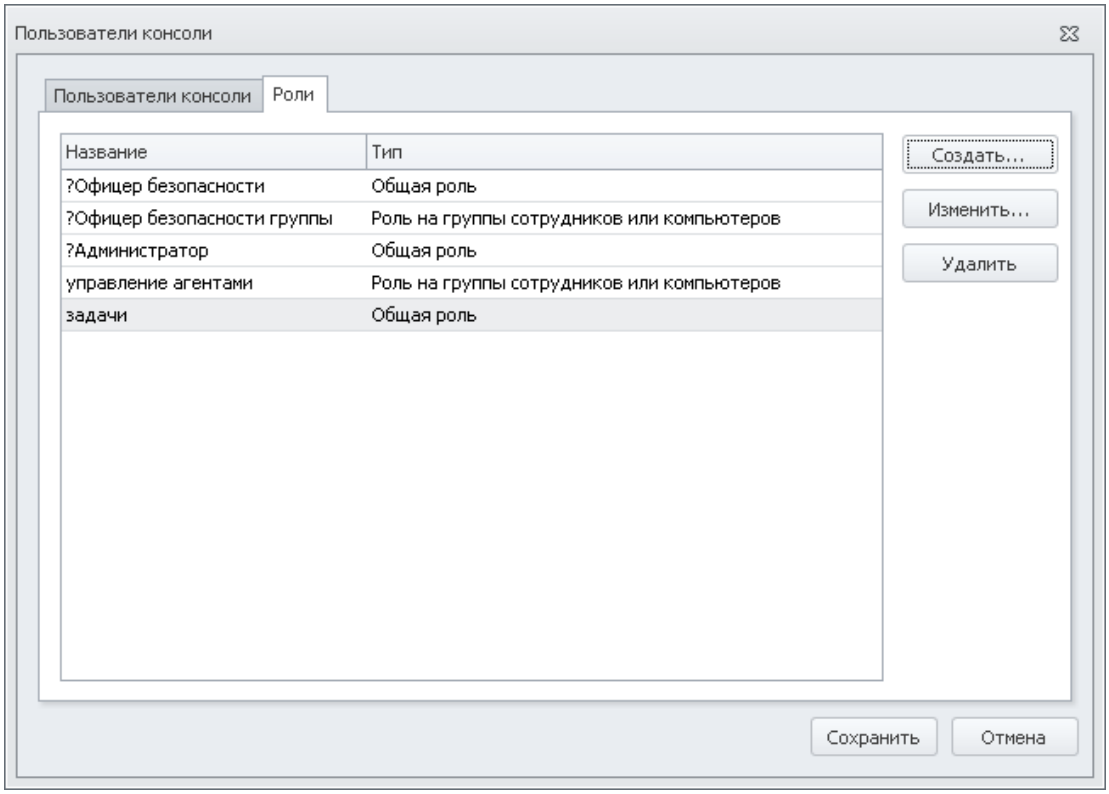
Восстановление учетной записи

Чтобы восстановить учетную запись, добавьте учетную запись повторно, указав тот же логин (см. "Добавление учетной записи Консоли управления").

4.2.2 Роли пользователей Консоли управления

Чтобы просмотреть информацию о ролях пользователей Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**. На экран будет выведено диалоговое окно **Пользователи консоли**.
2. Перейдите на вкладку **Роли.**



3. Сведения о ролях Консоли управления представлены в виде табличного списка. Каждая строка соответствует одной роли. В столбцах отображаются значения следующих атрибутов ролей:

- **Название**.
- **Тип**. Может принимать значения:
  - **Роль на группы сотрудников или компьютеров** - содержит права (привилегии) на действия с группами сотрудников или компьютеров.
  - **Общая роль** - содержит права (привилегии) на выполнение общих действий в Консоли.

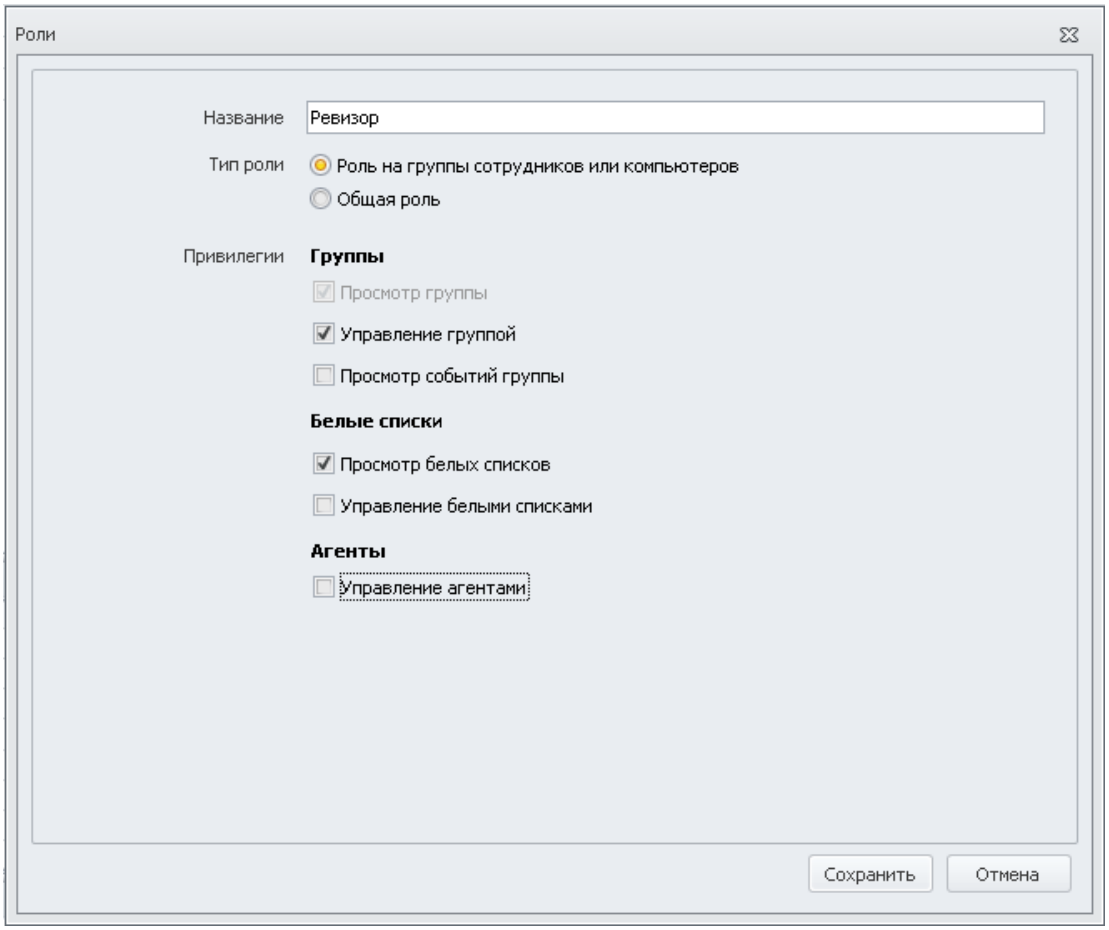
Подробное описание привилегий вы можете найти на странице "Добавление роли пользователя Консоли управления".

Добавление роли пользователя Консоли управления

Чтобы добавить новую роль пользователя Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**.
2. Перейдите на вкладку **Роли.**
3. Нажмите на кнопку **Создать**, расположенную в правой части диалогового окна **Пользователи консоли**
4. В открывшемся диалоговом окне укажите параметры роли:
   - **Название,**
   - **Тип роли,**
   - **Привилегии.**

> **Примечание:**
>
> Каждому типу роли соответствует свой набор привилегий.



5. Нажмите **Сохранить**.
6. После этого диалоговое окно **Создание роли** будет закрыто. Сведения о новой роли появятся в диалоговом окне **Пользователи консоли** на вкладке **Роли**.

Привилегии пользователей

Привилегии в Консоли управления DM представляют собой действия, доступные пользователю:

- по отношению к конкретной группе компьютеров или сотрудников;

- по отношению к Системе в целом (общие привилегии).

Привилегии на группы сотрудников/компьютеров

Привилегия	Доступные действия
Группы	
Просмотр группы	• Просмотр группы в списке групп • Просмотр настроек группы • Просмотр списка компьютеров/сотрудников, входящих в группу • Просмотр эффективной политики на компьютер/сотрудника • Просмотр всех подгрупп группы
Управление группой	• Редактирование настроек группы (в том числе назначение политики на группу - из политик, доступных пользователю на чтение или редактирование) • Добавление/удаление компьютеров/сотрудников в группе • Копирование компьютеров/сотрудников или подгрупп из группы • Управление всеми подгруппами данной группы • Удаление группы **Примечание:** при добавлении данной привилегии привилегия **Просмотр группы** добавляется автоматически.
Просмотр событий группы	Просмотр событий, полученных от рабочих станций или от сотрудников данной группы и всех ее подгрупп. **Примечание:** при добавлении данной привилегии привилегия **Просмотр группы** добавляется автоматически.
Белые списки	
Просмотр белых списков	Просмотр белых списков, относящихся к данной группе и ее подгруппам
Управление белыми списками	Создание/редактирование/удаление белых списков для данной группы и для компьютеров/сотрудников, входящих в группу и ее подгруппы. **Примечание:** при добавлении данной привилегии привилегия **Просмотр белых списков** добавляется автоматически.
Агенты	

Привилегия	Доступные действия
Управление агентами группы	Добавление рабочих станций из данной группы и ее подгрупп в задачи распространения/обновления/удаления агентов, смены пароля деинсталляции **Примечание:** при добавлении данной привилегии привилегия **Просмотр группы** добавляется автоматически.

Общие привилегии

Привилегия	Доступные действия
Политики	
Просмотр всех политик	Просмотр всех имеющихся в Системе политик, доступных на чтение или редактирование, и входящих в них правил
Управление всеми политиками	• Редактирование всех имеющихся в Системе политик (независимо от владельца и уровня доступа к политике) и входящих в них правил • Создание новой политики • Удаление политики (доступно только владельцу политики)
Управление доступными политиками	• Редактирование доступных пользователю политик (политик, для которых пользователь является владельцем, и политик, доступных на редактирование всем пользователям) • Создание новой политики • Удаление политики (доступно только владельцу)
Другие привилегии	
Просмотр журнала аудита	Доступ в раздел "Журнал"
Удаление записей журнала	Удаление записей из журнала аудита, очистка журнала аудита **Примечание:** при добавлении данной привилегии привилегия **Просмотр журнала аудита** добавляется автоматически.
Управление пользователями	▪ Просмотр пользователей и ролей консоли ▪ Создание пользователей и ролей консоли ▪ Редактирование пользователей и ролей консоли

Привилегия	Доступные действия
	▪ Удаление пользователей и ролей консоли
Создание групп	Создание новых групп компьютеров или сотрудников. Новая группа автоматически добавляется в группы, доступные пользователю. На группу назначается предустановленная роль "Офицер безопасности группы". **Примечание:** при добавлении данной привилегии привилегия **Просмотр всех политик** добавляется автоматически.
Управление агентами на отдельных компьютерах	• Добавление компьютеров из сетевого окружения и через подключение к AD или ALD в задаче распространения агентов • Добавление компьютеров через импорт файла и по имени/IP в задаче распространения агентов • Создание пакета установки
Управление настройками	Управление глобальными настройками DM (кроме раздела "Интеграция с AD" в меню **Инструменты** -> **Настройки**)
Синхронизация с AD	Настройка синхронизации рабочих станций и сотрудников с AD и ALD (раздел "Интеграция с AD" в меню **Инструменты** -> **Настройки**)
Импорт/экспорт конфигурации	Импорт и экспорт схемы безопасности и настроек **Важно!** Данная привилегия позволяет пользователю Консоли импортировать и экспортировать конфигурацию вне зависимости от наличия у него прав на импортируемые/экспортируемые объекты
Предоставление временного доступа	Предоставление по запросу сотрудника временного доступа к сети или устройствам

Редактирование роли пользователя Консоли управления

Важно!

При редактировании роли, назначенной учетной записи, в настоящий момент авторизованной в Консоли управления, происходит следующее. После сохранения результатов редактирования соединение с сервером автоматически прерывается. Затем пользователю предлагается пройти авторизацию с новыми параметрами. При этом все не сохраненные данные будут утеряны.

Чтобы отредактировать параметры роли пользователя Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**. На экран будет выведено диалоговое окно **Пользователи консоли** .
2. На вкладке **Роли** выберите строку с названием роли, которую нужно отредактировать.
3. Нажмите на кнопку **Изменить**, расположенную в правой части данного окна, или дважды щелкните левой кнопкой мыши по выделенной строке.
4. В открывшемся диалоговом окне **Роли** отредактируйте параметры роли, описанные в разделе "Добавление роли пользователя Консоли управления". Тип роли не подлежит изменению.
5. Нажмите кнопку **Сохранить**.
6. Чтобы сделанные изменения вступили в силу, нажмите на кнопку **Сохранить** в диалоговом окне **Пользователи консоли** .

Важно!

Недоступно любое редактирование предустановленных ролей: Администратор, Офицер безопасности, Офицер безопасности группы.

Удаление роли пользователя Консоли управления

Чтобы удалить роль пользователя Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**. На экран будет выведено диалоговое окно **Пользователи консоли**.
2. На вкладке **Роли** выберите строку с названием роли, которую нужно удалить.
3. Нажмите на кнопку **Удалить**, расположенную в правой части данного окна.
4. В появившемся окне запроса нажмите на кнопку **ОК**, чтобы подтвердить удаление.

   Внимание!

   Роль, которая назначена пользователю в данный момент, не может быть удалена. Для удаления такой роли необходимо снять ее со всех пользователей.

5. Чтобы сделанные изменения вступили в силу, нажмите на кнопку **Сохранить** в диалоговом окне **Пользователи консоли**.

4.2.3 Аудит действий по управлению схемой безопасности в Консоли управления

В процессе работы с Консолью управления выполняются различные операции по управлению схемой безопасности. Записи о действиях, связанных с изменением информации, хранящейся в базе данных (настройка схемы безопасности, администрирование Системы) сохраняются в журнале аудита.

Информация по работе с журналом аудита содержится в следующих подразделах:

- Просмотр журнала аудита

- Фильтрация записей в журнале аудита
- Удаление записей из журнала аудита
- Экспорт записей журнала аудита
- Анализ журнала аудита в Microsoft Excel

Просмотр журнала аудита

Работа с журналом аудита ведется в разделе **Журнал**. Чтобы перейти к этому разделу, воспользуйтесь кнопкой **Журнал**, расположенной на Панели навигации.

Действия по управлению схемой безопасности выполняются в виде транзакций. Транзакции отображаются как набор записей в журнале аудита. Каждая запись содержит сведения о выполнении одного элементарного действия (шага транзакции). Транзакция может состоять только из одного шага и, соответственно, будет представлена в журнале аудита одной записью.

Для того чтобы выбрать из журнала аудита записи, удовлетворяющие определенным условиям, вы можете настроить фильтры (о работе с фильтрами рассказывается в разделе "Фильтрация записей в журнале аудита"). Список фильтров выводится в разделе **Журнал** на Панели навигации. В рабочей области главного окна отображается список записей для выбранного фильтра.

> **Примечание.**
>
> Для более удобного просмотра вы можете настроить отображение записей журнала аудита, воспользовавшись дополнительными функциями (см. главу "Дополнительные возможности").

Чтобы просмотреть все записи журнала аудита, воспользуйтесь кнопкой **Показать все записи**, расположенной в верхней части Панели навигации.

Чтобы просмотреть записи, удовлетворяющие критериям какого-либо фильтра, щелкните левой кнопкой мыши по названию нужного фильтра в списке фильтров.

Сведения о записях журнала отображаются в виде табличного списка, где каждая строка соответствует одной записи. В столбцах выводятся основные свойства записей журнала. Расширенная информация по свойствам каждой записи выводится на панели **Подробно**.

Чтобы просмотреть расширенную информацию о свойствах отдельной записи, в рабочей области главного окна выберите строку с названием нужной записи.

В результате на панели **Подробно** будет отображена таблица свойств, в которой содержатся следующие сведения по выбранной записи:

Свойство	Описание
Транзакция (#)	Номер транзакции
Шаг	Порядковый номер элементарного действия, выполненного в рамках данной транзакции
Дата	Дата и время выполнения действия
Объект	Название объекта, над которым выполнялось действие
Действие	Тип действия

Свойство	Описание
Селектор	Содержит информацию, позволяющую однозначно идентифицировать объект, над которым было выполнено действие. Расшифровка значений параметра Селектор приведена в разделе "Значения параметра Селектор".
Поле	Атрибут объекта, измененный в ходе выполнения действия
Старое значение	Значение атрибута до изменения
Новое значение	Новое значение атрибута
Пользователь	Имя учетной записи Консоли управления, под которой выполнялась транзакция
Учетная запись Windows	Учетная запись, с данными которой пользователь авторизован в Windows
Компьютер	Название компьютера, на котором было выполнено действие
Порядковый номер	Порядковый номер, присвоенный этой записи, в базе данных

Примечание:

При изменении статуса состояния Агента через Консоль DM, будет создана запись с атрибутами, указанными в таблице выше.

Часть информации, выводимой на панели **Подробно**, дублируется в рабочей области главного окна.

Количество шагов транзакции (и, следовательно, количество записей в журнале аудита) варьируется в зависимости от объекта и действий, выполняемых над этим объектом.

Пример:

На рисунке ниже показано несколько записей журнала аудита, относящихся к разным транзакциям.

Шаг	#	Время	Объект	Действие	Селектор	Поле	Ст...	Новое значение	Польз...	Пор...
2	28	07.09.2...	Схема безопасности	Добавление	11/Добавлена файловая по...	Комментарий		Добавлена фай...	admin	368
1	28	07.09.2...	Политика	Добавление	11/Файловая политика 01	Политика		Файловая полит...	admin	367
1	27	07.09.2...	Учетная запись	Изменение	leonov_oleg	Роль	Офиц...	Локальный адм...	admin	366
5	26	07.09.2...	Схема безопасности	Добавление	10/Добавлено правило для...	Комментарий		Добавлено прав...	admin	365
4	26	07.09.2...	Правило	Добавление	10/Политика по умолчанию...	Разрешать ...		Да	admin	364
3	26	07.09.2...	Правило	Добавление	10/Политика по умолчанию...	Операция		Съемное устрой...	admin	363
2	26	07.09.2...	Правило	Добавление	10/Политика по умолчанию...	Действует по		31.12.9999 23:5...	admin	362
1	26	07.09.2...	Правило	Добавление	10/Политика по умолчанию...	Действует с		01.01.1753 0:00...	admin	361

Транзакция под номером 26 соответствует одному изменению схемы безопасности. Это было сделано в 5 шагов. На шагах 1-4 было добавлено правило *Файловое правило 01* в политику безопасности *Политика по умолчанию*. Каждый шаг соответствует настройке одного параметра правила: например, на шаге 1 было указано время начала действия правила, на шаге 2 задано время окончания действия правила и т. д. На шаге 5 был внесен комментарий к изменению схемы безопасности.

Транзакция под номером 27 связана с изменением в настройках учетной записи Консоли управления. Данная транзакция включает один шаг – изменение роли для учетной записи *leonov_oleg*.

Транзакция под номером 28 связана с добавлением политики безопасности *Файловая политика 01*. Это соответствует двум шагам транзакции: собственно добавлению политики и внесению комментария к изменению схемы безопасности.

Значения параметра Селектор

Параметр **Селектор** содержит инструкцию для поиска объекта, над которым было совершено действие. Значение параметра **Селектор** зависит от объекта и действий, выполняемых над этим объектом. Каждому объекту соответствует свой набор значений параметра **Селектор**.

Для изменяемых параметров схемы безопасности отображается версия редактируемой схемы безопасности и, через символ " / " - название редактируемого параметра безопасности.

При редактировании объекта (действие **Изменить**) в качестве значения параметра **Селектор** отображается имя объекта до редактирования.

Далее рассматривается несколько примеров расшифровки значений параметра **Селектор**.

Пример 1:

В журнале аудита имеется следующая запись:

Шаг	#	Время	Объ...	Действие	Селектор	Поле	Старое зна...	Новое значение	Пользова...	Порядковый но...
1	7	05.09.2011 16:58:35	Политика	Добавление	4/Файловая политика	Политика		Файловая политика	Officer	20

Из данной записи следует, что в схему безопасности была добавлена новая политика безопасности.

Расшифровка значения Селектора

В момент выполнения транзакции действовала 4 версия схемы безопасности. Новой политике безопасности присвоено название Файловая политика.

Пример 2:

В журнале аудита имеется следующая запись:

...	#	Вр...	Объект	Действие	Селектор	Поле	Старое значение	Новое значение	..	П...
10	7	05.09....	Правило	Изменение	4/Политика на устройства/Доступ к флоппи диску	Операция	Флоппи-дисковод: Полный доступ	Флоппи-дисковод: Только чтение	Of...	29

Из данной записи следует, что в политике *Политика на устройства* право доступа к флоппи-диску изменилось с полного доступа к устройству на доступ только для чтения.

Расшифровка значения Селектора

В момент выполнения данной транзакции действовала 4-я версия схемы безопасности. Изменения проводились в политике *Политика на устройства*, над правилом *Доступ к флоппи диску*.

Пример 3:

В журнале аудита имеется следующая запись:

Шаг	#	Время	Объект	Действие	Селектор	Поле	Стар...	Нов...	Пол...	Порядков...
1	24	06.09.2011 17:59:46	Журнал	Экспорт	Объект в (Правило, Политика)				admin	348

Из данной записи следует, что был выполнен экспорт записей из журнала аудита.

Расшифровка значения Селектора

В процессе выполнения данной транзакции были экспортированы все записи о действиях над объектами *Политика* и *Правило*.

Фильтрация записей в журнале аудита

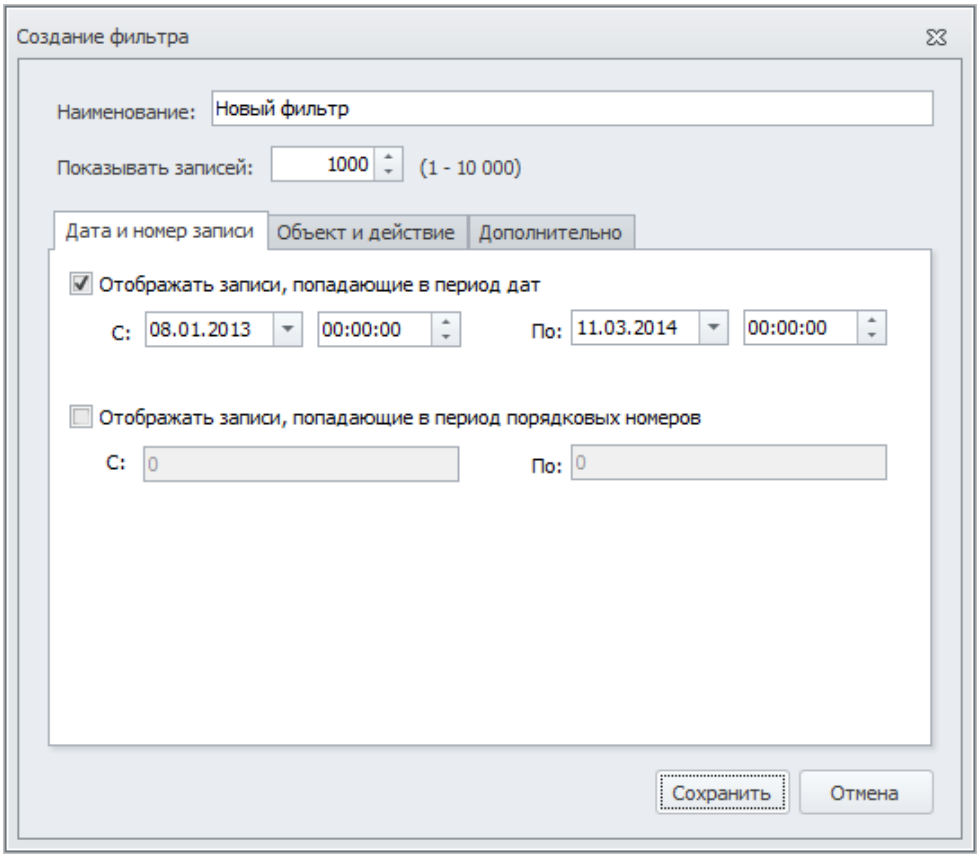
Для получения доступа к записям журнала аудита, удовлетворяющим определенным критериям, вы можете воспользоваться функциями фильтрации.

Чтобы создать фильтр или изменить существующий:

1. Перейдите к разделу **Журнал**.
2. Выполните необходимые шаги:

Действие	Шаги
Создание фильтра	- в главном меню выберите команду **Правка** > **Создать фильтр**; - воспользуйтесь кнопкой **Создать фильтр**, расположенной верхней части Панели навигации; - щелкните правой кнопкой мыши и в контекстном меню выберите **Создать фильтр**; - используйте сочетание клавиш **Ctrl+N**.
Редактирование фильтра	a) В области **Журнал** на Панели навигации выберите название фильтра, который нужно отредактировать. b) Выполните одно из следующих действий: - в главном меню выберите команду **Правка** > **Изменить**; - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации; - дважды щелкните левой кнопкой мыши по названию выделенного фильтра; - щелкните правой кнопкой мыши и в контекстном меню выберите **Изменить**; - используйте сочетание клавиш **Ctrl+E**.

После выполнения любого из этих действий на экран будет выведено диалоговое окно с параметрами фильтра.



3. Укажите общие параметры фильтра:
   - **Наименование**
   - **Показывать записей**. Максимальное количество записей, которые могут быть выведены в рабочей области Консоли управления (значение по умолчанию 1000 записей).
4. Задайте критерии фильтрации. Настройка фильтрации выполняется на нескольких вкладках и описана в следующих подразделах:
   - Вкладка Дата и номер записи
   - Вкладка Объект и действие
   - Вкладка Дополнительно

> **Важно!**
>
> Если в диалоговом окне редактирования фильтра не задано ни одного условия, то фильтрация ни по одному параметру выполняться не будет. В результате применения такого фильтра будут выведены все записи, имеющиеся в журнале аудита.

5. Нажмите **Сохранить**.

Чтобы удалить фильтр:

1. Перейдите к разделу **Журнал**.
2. В области **Журнал** на Панели навигации выберите название фильтра, который нужно удалить.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;

- воспользуйтесь кнопкой  **Удалить**, расположенной в верхней части Панели навигации;
- щелкните правой кнопкой мыши и в контекстном меню выберите **Удалить**;
- используйте сочетание клавиш **Ctrl+D**.

4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление фильтра.

Вкладка Дата и номер записи

На вкладке **Дата и номер записи** настраивают фильтрацию по следующим критериям:

- дата и время, когда было выполнено действие;
- порядковый номер записи в базе данных.

Чтобы задать условия фильтрации по дате и времени:

1. Отметьте поле **Отображать записи, попадающие в период дат**.
2. Укажите нужный промежуток времени.
   Начало и окончание периода указывают в полях **С** и **По** соответственно. Дату задают в левом поле, время – в правом.

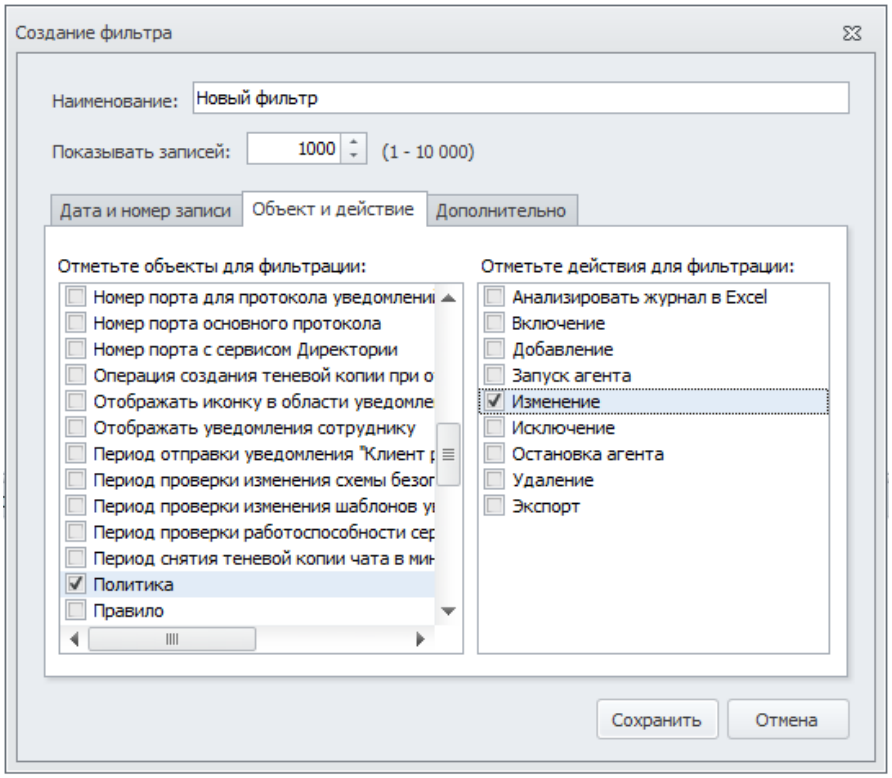
Чтобы задать условия фильтрации по порядковому номеру:

1. Отметьте поле **Отображать записи, попадающие в период порядковых номеров**.
2. Укажите диапазон порядковых номеров в полях **С** и **По** соответственно.
   Отсчет порядковых номеров записей в базе данных ведется со значения 1.

Вкладка Объект и действие

На вкладке **Объект и действие** задают условия фильтрации по следующим критериям:

- объект, над которым было выполнено действие;
- действие, выполненное над объектом.



Чтобы задать условия фильтрации:

1. Задайте условия фильтрации по объекту. Для этого в левом столбце отметьте объекты, по которым нужно выполнить фильтрацию.
2. Задайте условия фильтрации по действию. Для этого в правом столбце отметьте действия, по которым нужно выполнить фильтрацию.

Вкладка Дополнительно

На вкладке **Дополнительно** настраивают фильтрацию по дополнительным параметрам:

- **Селектор**. Фильтрация записей по значению параметра Селектор.
- **Поле**. Фильтрация записей по названию одного из атрибутов правила (например, *Операция*, *Действие* и т. д.).
- **Старое значение**. Фильтрация записей по тому значению, которое было у атрибута правила до изменения.
- **Новое значение**. Фильтрация записей по измененному значению атрибута правила.
- **Пользователь**. Вывод списка записей о действиях пользователя.
- **Учетная запись**. Вывод списка записей о действиях, выполненных от имени указанной учетной записи Windows.
- **Компьютер**. Вывод списка записей о действиях, выполненных на указанном компьютере.

Чтобы настроить условия фильтрации по дополнительному параметру, введите значение нужного параметра в соответствующее поле.

> **Примечание.**
>
> Значение дополнительного параметра фильтрации вводится без учета регистра символов.

Удаление записей из журнала аудита

> **Важно!**
>
> Удалять записи из журнала аудита может только Суперпользователь.

Чтобы удалить записи из журнала аудита:

1. В главном меню выберите команду **Правка** > **Удалить записи журнала**.
2. В открывшемся диалоговом окне **Удаление** укажите номер транзакции.

   > **Важно!**
   >
   > Обратите внимание, что из журнала аудита будут удалены записи, относящиеся к указанной транзакции и записи, относящиеся ко всем предыдущим транзакциям.

3. Нажмите **OK**.

Экспорт записей журнала аудита

Записи журнала можно экспортировать в файлы формата XLS, HTM или TXT. Впоследствии можно будет просмотреть экспортированные записи при помощи приложений, ассоциированных с файлами соответствующих форматов.

Чтобы экспортировать записи журнала аудита:

1. Перейдите к разделу **Журнал**.
2. Выполните одно из следующих действий:
   - Чтобы экспортировать записи, отобранные в результате применения одного из фильтров, выберите нужный фильтр на Панели навигации.
   - Чтобы экспортировать все записи журнала аудита, воспользуйтесь кнопкой  **Показать все записи**, расположенной в верхней части Панели навигации.
3. Выполните одно из следующих действий:
   - Нажмите кнопку  **Экспортировать журнал**, расположенную в верхней части области **Записи**.
   - В главном меню выберите команду **Правка** >  **Экспортировать журнал**.
   - В области **Записи** щелкните правой кнопкой мыши и в контекстном меню выберите **Экспортировать журнал**.
4. В открывшемся диалоговом окне укажите имя и тип файла, в который будут экспортированы записи, а также каталог для хранения этого файла.
5. Нажмите на кнопку **Сохранить**.

После этого записи журнала аудита будут экспортированы в указанный файл.

Анализ журнала аудита в Microsoft Excel

Для обеспечения возможности анализа журнала аудита в Microsoft Excel, это приложение должно быть установлено на компьютере, где должен выполняться анализ журнала.

Чтобы просмотреть записи журнала аудита в Microsoft Excel:

1. Перейдите к разделу **Журнал**.
2. Выполните одно из следующих действий:
   - Чтобы просмотреть записи, отобранные в результате применения одного из фильтров, выберите нужный фильтр на Панели навигации.
   - Чтобы просмотреть все записи журнала аудита, воспользуйтесь кнопкой  **Показать все записи**, расположенной в верхней части Панели навигации.
3. В главном меню выберите команду **Правка** > **Анализировать журнал в Excel**.

В результате выбранный список записей будет выведен в программе Microsoft Excel.

4.3 Общие настройки Системы

В системе предусмотрен ряд глобальных параметров, которые должны быть едиными для всех политик и правил, действующих в системе Device Monitor. Настройка этих параметров осуществляется в отдельном меню: команда **Инструменты** > **Настройки**. Более подробно:

- Общие настройки работы Агентов
- Перехват веб-почты
- Контроль сетевых соединений
- Контроль мессенджеров
- Контроль сетевого трафика
- Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor
- Настройки сервера Device Monitor. Соединение с сервером Платформы
- Соединение и синхронизация со службами каталогов
- Настройка уведомлений сотрудников о нарушении правил
- Исключение приложений из перехвата
- Контроль приложений и снимки экрана
- Контроль ввода с клавиатуры
- Хранение событий
- Синхронизация политик Traffic Monitor
- Работа с Менеджером управления серверами
- Остановка и запуск агента Device Monitor
- Настройка статусов активности Агентов
- Настройка распространения Агентов
- Автоматическое обновление Агентов
- Настройка перехвата звукового окружения
- Настройка отправки данных в продукты
- Инженерные настройки агента

Измененные настройки вступают в силу сразу после обновления Агентов на контролируемых компьютерах. Обновление Агентов происходит следующим образом:

1. Агент, установленный на компьютере, отправляет запрос на Сервер и проверяет работоспособность Сервера, изменения схемы безопасности и изменения шаблонов уведомлений.
2. При наличии изменений Агент получает уведомление от Сервера.
3. На Агенте выполняется обновление.

4.3.1 Общие настройки работы Агентов

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

Чтобы указать общие настройки работы Агентов Device Monitor:

1. В главном меню выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Общие**.
3. 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.
Проверять изменения шаблонов уведомлений для активных Агентов каждые	Если Агент работает в активном режиме (т.е. сам опрашивает Сервер об изменениях шаблонов уведомлений, то проверка будет выполняться с указанной периодичностью, в секундах. Значение по умолчанию – 1800 сек. **Примечание**: Подробнее о настройке уведомлений см. "Настройка уведомлений сотрудников о нарушении правил".
Контроль дискового пространства на Агентах	
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. Подробнее см. "Создание теневых копий и запрет операций при нехватке свободного места".
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

Параметр	Описание
	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	
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, в поле **Максимальная скорость отправки данных**.
События	
Логировать события от перехватчика устройств и облачных хранилищ	Степень детализации при сохранении сведений о работе с внешними устройствами, получаемых перехватчиками Device Monitor и Cloud Storage Monitor: подробнее см. "Правило для Device Monitor", "Правило для Cloud Storage Monitor" и "Просмотр событий". Возможен один из следующих вариантов: - **Не логировать** - события не сохраняются; - **При отказе в доступе** - события создаются только при попытках нарушения политики безопасности - то есть при блокировании использования устройства, включая блокирование попыток превышения уровня доступа. Использование внешних устройств, не запрещенных политиками, не фиксируется. - **Логировать всегда** - сохраняются сведения обо всех действиях (подключение/использование любых устройств, даже занесенных в белые списки)

Параметр	Описание
Логировать соединения вне корпоративной сети	Степень детализации при сохранении сведений о передаче данных по сетевым соединениям, получаемых перехватчиком Network Monitor: подробнее см. "Правило для Network Monitor". Возможен один из следующих вариантов: - **Не логировать** - события не сохраняются; - **При отказе в доступе** - события создаются только при попытках нарушения политики безопасности - то есть при блокировании попыток соединения.
Поведение Агента на компьютере	
Отображать уведомления сотруднику	Признак того, что при попытке сотрудника выполнить действие, запрещенное политикой безопасности, ему будет отображаться предупреждающее уведомление. Подробнее см. "Настройка уведомлений сотрудников о нарушении правил"
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.
Ключ формирования кодов	
Обновить ключ формирования кодов	Нажмите **Обновить**, чтобы Система сгенерировала новый ключ, используемый для формирования кодов снятия запрета доступа к сетевым соединениям или устройствам. Подробнее о кодах см. "Временный доступ сотрудника к сети" и "Временный доступ сотрудника к устройствам", параметры **Код запроса** и **Код подтверждения**. Частое обновление ключа не рекомендуется.

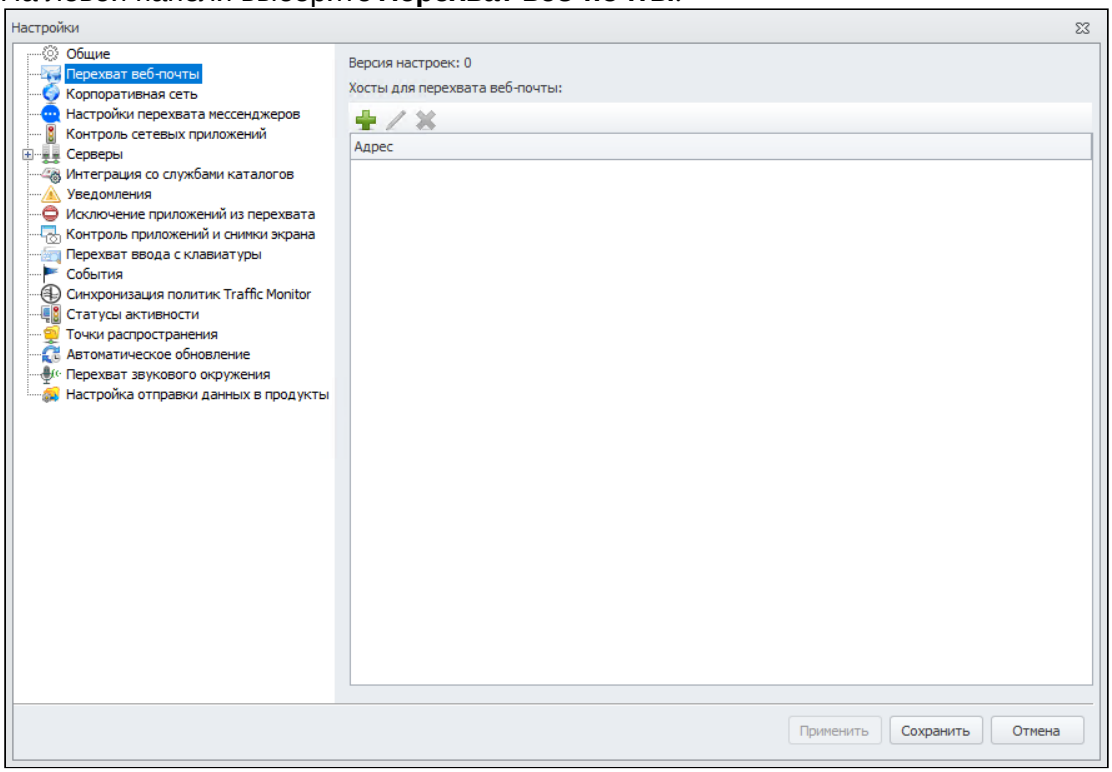
4. Чтобы внесенные изменения вступили в действие, нажмите **Применить**, а затем **Сохранить**.

4.3.2 Перехват веб-почты

Для перехвата веб-почты VK+ необходимо задать хосты. О настройке перехвата веб-почты см. "Правило для Mail Monitor".

Чтобы добавить хост:

1. В главном меню выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Перехват веб-почты**.



3. В области **Хосты для перехвата веб-почты** нажмите .
4. Введите адрес хоста в формате *<схема>:<хост>*, например, *address.ru:15101* или *10.60.3.8:15101*.
5. Нажмите **ОК**.

Чтобы отредактировать хост:

1. Выберите его в списке и нажмите .
2. В окне редактирования внесите правки и нажмите **ОК**.

Чтобы удалить хост:

1. Выберите его в списке и нажмите .
2. В открывшемся окне подтвердите удаление, нажав **Да**.

4.3.3 Контроль сетевых соединений

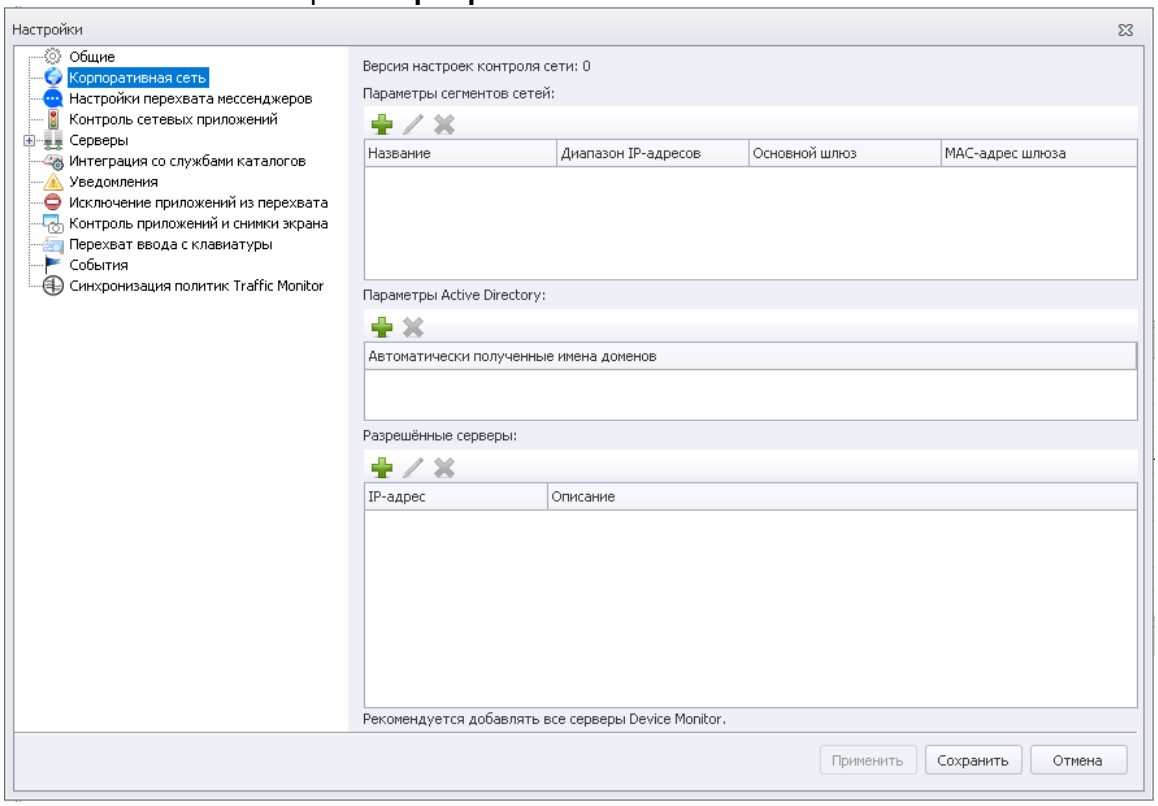
Для обеспечения контроля передачи данных по сетевым соединениям с помощью **Network Monitor** (о настройке правил для данного типа контроля см. "Правило для Network Monitor") необходимо задать параметры того, какие сегменты сети считаются корпоративной сетью, и какие внешние адреса разрешены.

Примечание.

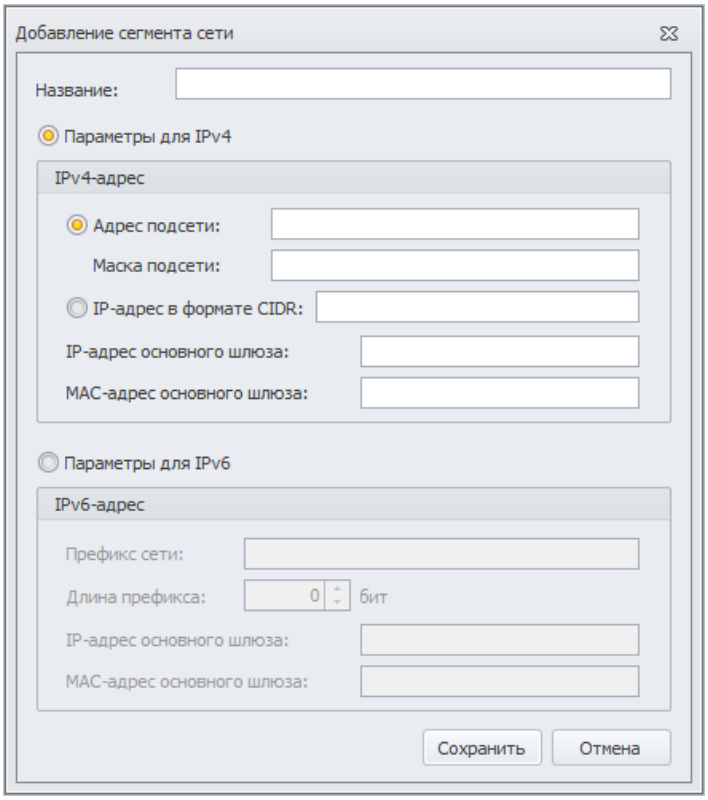
Разрешение внешних адресов может понадобиться, например, для обеспечения работы с внешними ресурсами, когда агент находится вне корпоративной сети, например с VPN сервером или корпоративной почтой.

Чтобы настроить параметры контроля сетевых соединений:

1. В главном меню выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Корпоративная сеть**.



3. Чтобы задать параметры сегментов сетей:
   a. В области **Параметры сегментов сетей** нажмите (либо используйте сочетание клавиш Ctrl+Shift+S). В результате будет открыто диалоговое окно **Добавление сегмента сети**.



b. Укажите название (описание) сегмента.
c. Выберите используемую версию протокола: **IPv4** или **IPv6**.
   Если вы выбрали **Параметры для IPv4**, то выберите формат адреса (CIDR либо адрес и маска) и укажите требуемые параметры. Также задайте IP-адрес и MAC-адрес основного шлюза (default gateway).
   Если вы выбрали **Параметры для IPv6**, то укажите префикс сети и его длину. Также задайте IP-адрес и MAC-адрес основного шлюза (default gateway).
d. Нажмите **Сохранить**.
e. Повторите действия для добавления других сегментов.
   Чтобы изменить параметры сегмента, в области **Параметры сегментов сетей** выберите его в списке и нажмите (либо используйте сочетание клавиш Ctrl+E).
   Чтобы удалить сегмент из списка, выберите его, нажмите (либо нажмите клавишу **Delete**), затем нажмите **Да** в окне подтверждения.

4. Чтобы определить параметры Active Directory, в области **Параметры Active Directory** нажмите . В результате Система автоматически определит имя и GUID домена, в котором находится сервер Device Monitor.
5. Чтобы задать список серверов, соединение с которыми должно быть разрешено:
   a. В области **Разрешенные сервера** нажмите .
   b. В диалоговом окне **Добавить разрешенный сервер** введите DNS имя или IP-адрес сервера, а также его описание.
   c. Нажмите **OK**.
   d. Повторите действия для других разрешенных адресов.
      Чтобы изменить параметры сервера, выберите его в списке и нажмите (либо используйте сочетание клавиш Ctrl+E).
      Чтобы удалить сервер из списка разрешенных, выберите его, нажмите (либо нажмите клавишу **Delete**), затем нажмите **Да** в окне подтверждения.
6. Чтобы внесенные изменения вступили в действие, нажмите **Применить**.

Определение наличия подключения к корпоративной сети для различных вариантов заполнения:

1. Заданы **только параметры сегментов сетей**. В этом случае считается, что доменная и не доменная рабочие станции находятся в корпоративной сети, если:
   a. IP-адрес рабочей станции входит в один из указанных сегментов.
   b. IP-адрес и MAC-адрес default gateway соответствуют значениям, указанным для этого сегмента.
2. Заданы **только параметры Active Directory**. В этом случае:
   a. Считается, что доменная рабочая станция находится в корпоративной сети, если:
      i. В сети есть домен с указанными параметрами.
      ii. Есть возможность подключения через определенный сетевой адаптер к контроллеру домена, к которому принадлежит рабочая станция.
   b. Считается, что не доменная рабочая станция всегда находится в корпоративной сети.
3. Заданы **параметры сегментов сетей и параметры Active Directory**. В этом случае:
   a. Считается, что не доменная рабочая станция находится в корпоративной сети, если:
      i. IP-адрес рабочей станции входит в один из указанных сегментов.
      ii. IP-адрес и MAC-адрес default gateway соответствуют значениям, указанным для этого сегмента.
   b. Считается, что доменная рабочая станция находится в корпоративной сети, если:
      i. IP-адрес рабочей станции входит в один из указанных сегментов.
      ii. IP-адрес и MAC-адрес default gateway соответствуют значениям, указанным для этого сегмента.

      ИЛИ
      i. В сети есть домен с указанными параметрами.
      ii. Есть возможность подключения через определенный сетевой адаптер к контроллеру домена, к которому принадлежит рабочая станция.

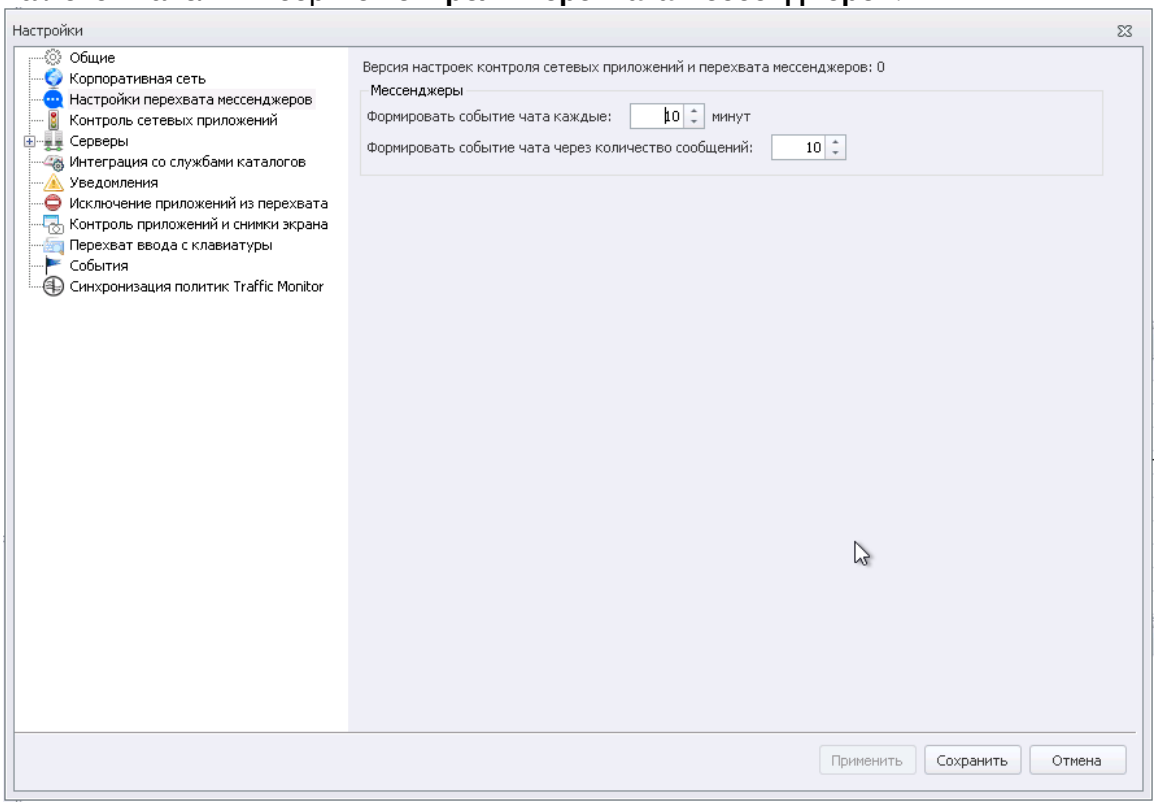
4.3.4 Контроль мессенджеров

При контроле трафика вы можете задать дополнительные параметры работы с системами мгновенного обмена сообщениями (о настройке правил) для данного типа контроля см. "Правило для IM Client Monitor")

Чтобы настроить параметры контроля мессенджеров:

1. В главном меню выберите команду **Инструменты** > **Настройки**.

2. На левой панели выберите **Контроль перехвата мессенджеров**.



3. Укажите параметры контроля мессенджеров: задайте частоту формирования теневой копии чата для отправки на анализ в Traffic Monitor. Вы можете задать как время (в минутах), по истечении которого будет сформирована теневая копия (**Формировать событие чата каждые**), так и количество сообщений, по достижении которого будет сформирована теневая копия (**Формировать событие чата через количество сообщений**). Если в чате осуществляется отправка файла, то теневая копия может формироваться раньше достижения указанного периода.

4.3.5 Контроль сетевого трафика

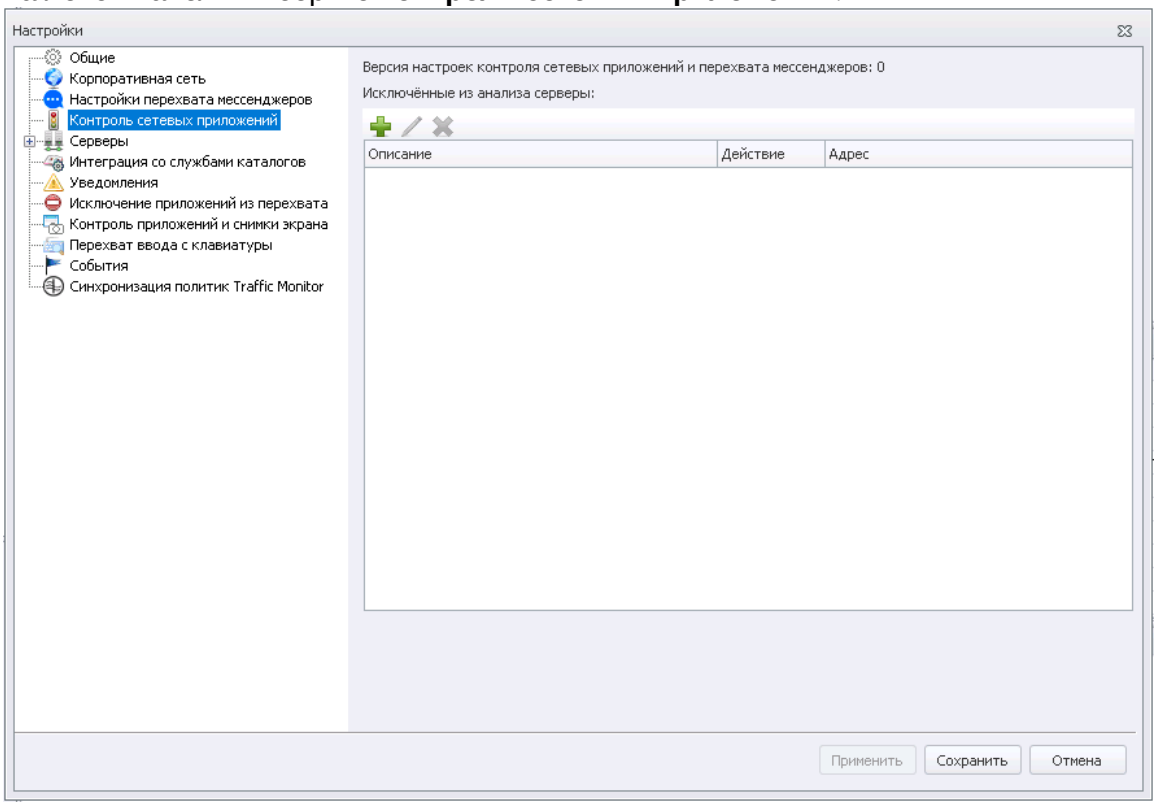
Для контроля сетевого трафика на Агенте Device Monitor реализован прозрачный прокси-сервер. На этот сервер перенаправляются все соединения, вне зависимости от используемого протокола. Далее Агент Device Monitor разбирает протокол и определяет, относится ли данный протокол к перехватываемым. Перехватываются протоколы: FTP, FTPS, POP3, SMTP, S/MIME, Outlook, HTTP, HTTPS[1], XMPP и MMP. Если поток данных защищен с использованием протокола TLS\SSL, то прокси-сервер раскрывает трафик и определяет, нужно ли контролировать данный поток.

При контроле трафика вы можете задать дополнительные параметры работы с почтовыми системами (см. "Правило для Mail Monitor") и FTP/FTPS-трафиком (см. "Правило для FTP Monitor"), а также определить серверы-исключения, трафик на которые не должен контролироваться.

Чтобы настроить параметры контроля сетевого трафика:

1. В главном меню выберите команду **Инструменты** > **Настройки**.

2. На левой панели выберите **Контроль сетевых приложений**.



3. Вы можете задать перечень адресов серверов, при соединении с которыми контроль протоколов проводиться не будет[23] (то есть трафик на данные серверы не будет перенаправляться на внутренний прокси-сервер) либо принудительно контролироваться (будет перенаправляться на внутренний прокси-сервер).
   Чтобы задать список разрешенных или запрещенных серверов:
   a. В области **Исключенные из анализа серверы** нажмите .
   b. В диалоговом окне **Добавить сервер в список исключенных из анализа** введите описание сервера. Подробнее о добавляемых адресах см. "Добавление серверов".
   c. Выберите нужное действие: **Исключить из перехвата** или **Включить в перехват**.
   d. Укажите адреса одним из способов:
      - Выберите **Адрес и порт** и задайте:
        - DNS-имя или IP-адрес сервера;
        - порт подключения.
      - Выберите **Диапазон адресов** и задайте интервал IP-адресов.
      - Выберите **Домен из MitM перехватчика** и введите доменное имя. Используйте этот способ для исключения трафика домена при SSL-соединении.
   e. Нажмите **OK**.
   f. Повторите действия для других разрешенных адресов.
   g. Чтобы изменить параметры сервера, выберите его в списке и нажмите .
   h. Чтобы удалить сервер из списка разрешенных, выберите его, нажмите , затем нажмите **Да** в окне подтверждения удаления.
4. Чтобы внесенные изменения начали действовать, нажмите **Применить**.

Примечание:

[1] Если сотрудник использует Яндекс.Браузер на рабочей станции с установленным Агентом, то браузер может показывать предупреждения при подключении к HTTPS-ресурсам.
Если Агент перехватывает HTTPS-трафик для ресурса, то при подключении к ресурсу Яндекс.Браузер предупреждает, что:

- Device Monitor может иметь доступ к информации, которую пользователь просматривает или вводит на ресурсе;
- соединение может быть небезопасным.

[2] Разрешение внешних адресов может понадобиться для обеспечения работы с внешними ресурсами и обновления установленных программ, например:

- для автоматического обновления Firefox в списке разрешенных серверов должны присутствовать:
  - `*.mozilla.com`
  - `*.mozilla.net`
- для работы FileZilla:
  - `update.filezilla-project.org`
- для работы Dropbox:
  - `*.dropbox.com`
- для работы Yandex Disk:
  - `oauth.yandex.ru`
  - `webdav.yandex.ru`
  - `clck.yandex.ru`
  - `push.xmpp.yandex.ru`
- для работы App Store и других сервисов Apple:
  - `*mzstatic.com`
  - `*apple.com`

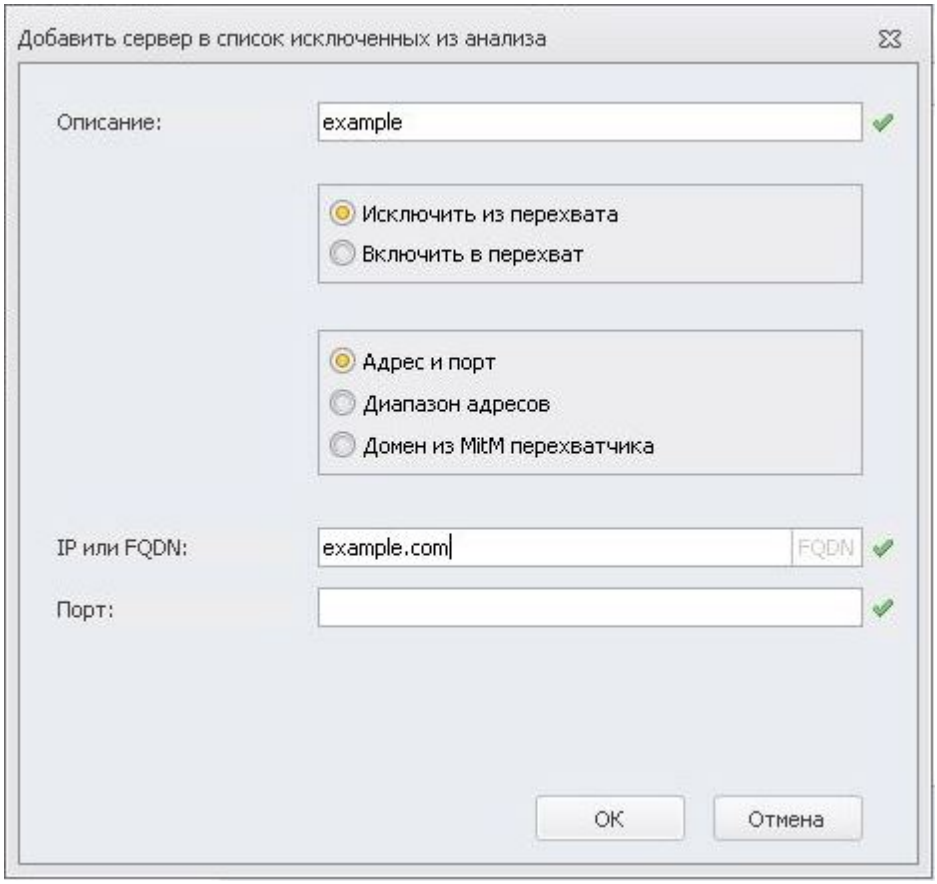
[3] Для агентов, установленных на рабочих станциях под управлением ОС Astra Linux или РЕД ОС, из перехвата исключается только трафик, передаваемый на сервер через SSL-протокол.

Добавление серверов

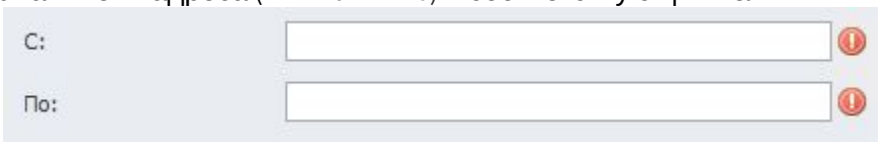
При добавлении адреса сервера в исключения (см. "Контроль сетевого трафика"), требуется указать IP-адрес сервера или FQDN.

Чтобы задать список разрешенных или запрещенных серверов:

1. В области **Исключенные из анализа серверы** нажмите .
   Откроется окно добавления сервера:

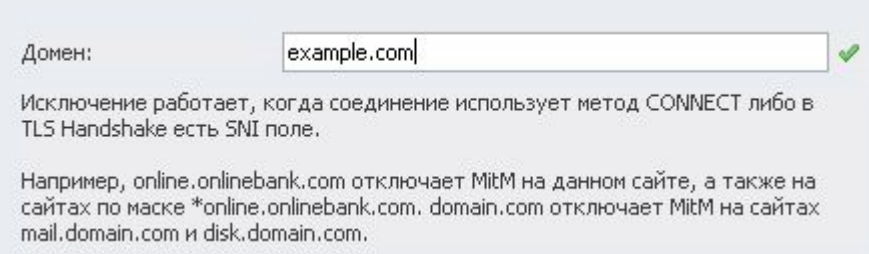


2. В диалоговом окне **Добавить сервер в список исключенных из анализа** введите описание сервера:
   - чтобы добавить отдельный порт сервера:
     a. Выберите нужное действие: **Исключить из перехвата** или **Включить в перехват**;
     b. Установите флажок в поле **Адрес и порт**;
     c. Укажите FQDN или IP-адрес (IPv4 или IPv6) сервера и порт подключения;
   - чтобы добавить диапазон адресов:
     a. Выберите нужное действие: **Исключить из перехвата** или **Включить в перехват**.
     b. Установите флажок в поле **Диапазон адресов**;
     c. Укажите IP-адреса (IPv4 или IPv6) в соответствующих полях



   - чтобы добавить шаблон для исключения группы ресурсов из перехвата при SSL/TLS-соединении:
     a. Выберите действие **Исключить из перехвата**;
     b. Установите флажок в поле **Домен из MitM перехватчика**;

c. Укажите домен



3. Нажмите **OK**.

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**.**

Важно!

Включение в перехват имеет более высокий приоритет, чем исключение.

Шаблонные исключения будут работать, только если агент подключается через прокси-сервер.

Адрес 0.0.0.0 применяется только в сочетании с портом, так как является специальным адресом для исключения всех адресов с указанным портом.

Пример 1:

Чтобы исключить из перехвата весь трафик на адрес `10.128.0.2`, кроме трафика на порт `8080:`

1. Исключите из перехвата сервер с IP-адресом `10.128.0.2` без указания порта;
2. Включите в перехват сервер с IP-адресом `10.128.0.2`, указав порт `8080`.

Пример 2:

Чтобы исключить из перехвата диапазон адресов `192.168.0.1 - 192.168.0.255` за исключением отдельного адреса `192.168.0.5:`

1. Исключите из перехвата диапазон серверов `192.168.0.1 - 192.168.0.255`;
2. Включите в перехват сервер с IP-адресом `192.168.0.5`.

Пример 3:
Чтобы исключить из перехвата порт `8080` на всех серверах, исключите из перехвата сервер с IP-адресом `0.0.0.0`, указав порт `8080`.

Чтобы изменить параметры сервера, выберите его в списке и нажмите .

Чтобы удалить сервер из списка разрешенных, выберите его, нажмите , затем нажмите **Да** в окне подтверждения удаления.

4.3.6 Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor

Для того чтобы иметь возможность отправлять события на анализ в InfoWatch Traffic Monitor, необходимо настроить параметры соединения с его сервером.

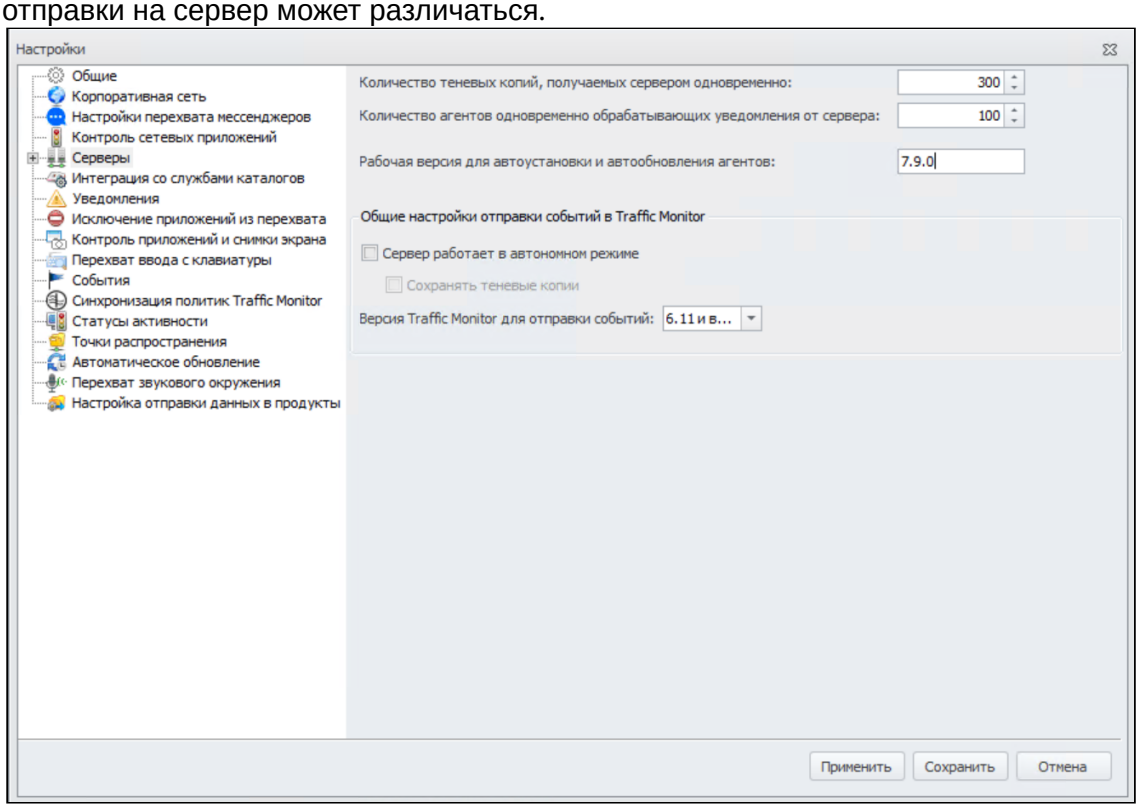
Чтобы просмотреть и настроить параметры соединения с сервером InfoWatch Traffic Monitor:

1. В главном меню Консоли управления выберите команду **Инструменты** > **Настройки**.
2. В узле **Серверы** определите следующие настройки:
   - **Количество теневых копий, получаемых сервером одновременно** – определяет количество копий, которые могут поступить на сервер в один момент времени.
   - **Количество агентов, одновременно обрабатывающих уведомления от сервера** – определяет количество агентов, которые могут получать уведомления (например, политику безопасности) от сервера в один момент времени.
   - **Рабочая версия для автоустановки и автообновления агентов** – определяет версию для автоматической установки или автоматического обновления агентов Device Monitor. Версия отображается при создании новой задачи первичного распространения. Необходимо указать первые три цифры версии, например, 7.9.0.

     > **Примечание:**
     >
     > Все доступные версии расположены в директории `C:\ProgramData\InfoWatch\SetupPackages\`.

   - **Сервер работает в автономном режиме** – сервер работает без интеграции с Traffic Monitor: события хранятся на сервере Device Monitor и не отправляются в Traffic Monitor.
     - **Сохранять теневые копии** – теневые копии сохраняются на локальном диске сервера по пути установки в папке `ShadowCopyTempDir`.
   - **Версия Traffic Monitor для отправки событий** – текущая версия Traffic Monitor, с которой происходит интеграция. В зависимости от версии, формат событий для

отправки на сервер может различаться.



3. При выборе сервера подключения отображается информация по следующим параметрам соединения:
   - **Роль сервера** – роль сервера (*основной* или *вспомогательный*), назначенная при установке данного сервера (см. "Порядок установки серверной части InfoWatch Device Monitor").
   - **Номер порта для протокола уведомлений**.
   - **Номер порта основного протокола**.

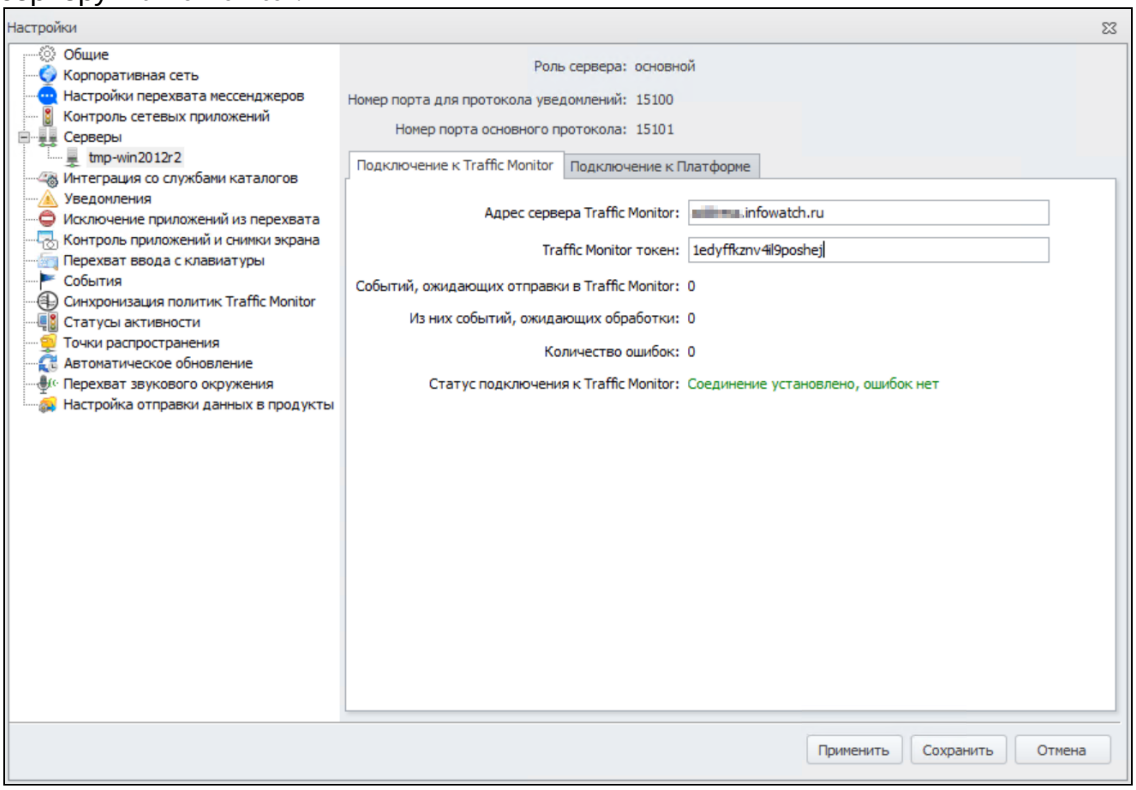
   > **Примечание.**
   >
   > Изменение роли сервера (*Основной* или *Второстепенный*) и атрибутов **Номер порта для протокола уведомления** и **Номер порта основного протокола** выполняется с помощью Менеджера управления серверами (см. "Работа с Менеджером управления серверами").

   - **Адрес сервера Traffic Monitor** – адрес сервера InfoWatch Traffic Monitor для работы в Консоли управления, на который будут доставляться события.
     Возможные форматы записи:
     - `host:port`
     - `protocol://host:port/`, где в качестве `protocol` используется `xml` для версий Traffic Monitor меньше 6.0 и `rcp` для версий Traffic Monitor от 6.0 и выше
     - `host:port/`

     Адрес должен быть заполнен в формате URI (Uniform Resource Identifier), формальный синтаксис которого описан в RFC 3986 http://tools.ietf.org/html/rfc3986.
     В качестве параметра `port` указывается порт сервера InfoWatch Traffic Monitor,

через который будет осуществляться доставка событий. По умолчанию, порт сервера InfoWatch Traffic Monitor – 9100.

- **Traffic Monitor токен** – токен для подключения к API. Необходимо указывать при работе с Traffic Monitor версии 6.0 и выше. Вы можете получить актуальный токен от администратора Traffic Monitor.
- **Событий, ожидающих отправки в ТМ** – общее количество событий для отправки в систему InfoWatch Traffic Monitor.
- **Из них событий, ожидающих обработки** – количество событий, ожидающих обработки перед отправкой в систему InfoWatch Traffic Monitor.
- **Количество ошибок** – количество событий, помещенных в отдельную очередь ошибок.
- **Статус подключения к Traffic Monitor** – информация о состоянии подключения к серверу Traffic Monitor.



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

Если сертификат службы XAPI Traffic Monitor не прошел проверку, то параметр **Статус подключения к Traffic Monitor** будет иметь значение *Ошибка проверки сертификата*.

4. Нажмите **Применить**.
5. Нажмите **Сохранить**.

4.3.7 Настройки сервера Device Monitor. Соединение с сервером Платформы

> **Важно!**
>
> Функциональность используется для взаимодействия с Activity Monitor и Prediction.

Чтобы иметь возможность отправлять события в Платформу, необходимо настроить параметры соединения с ее сервером.

> **Примечание:**
>
> Вы также можете отправлять в Платформу информацию об устройствах из белых списков. О настройке см. статью базы знаний "Отправка данных об устройствах из белых списков DM в Платформу".

Чтобы просмотреть параметры соединения с сервером Платформы и с сервером Activity Monitor:

1. В главном меню Консоли управления DM выберите команду **Инструменты** > **Настройки**.
2. В узле **Серверы** выберите сервер.
3. Выберите вкладку **Подключение к Платформе**.

Чтобы настроить соединение с сервером Платформы:

1. В главном меню Консоли управления DM выберите команду **Инструменты** > **Настройки**.
2. В узле **Серверы** выберите сервер.
3. Выберите вкладку **Подключение к Платформе**.
4. Укажите значения параметров **Адрес сервера Платформы** и **Токен Платформы**.
5. Нажмите **Применить**.
6. Нажмите **Сохранить**.

Чтобы настроить соединение с сервером Activity Monitor:

> **Важно!**
>
> Данная настройка необходима, чтобы подключиться к рабочей станции сотрудника для проведения онлайн-наблюдения (доступно, начиная с версии DM 7.9.0).
>
> Настройки соединения сервера DM с Activity Monitor для получения запросов производятся только на основном сервере.

1. В главном меню Консоли управления DM выберите команду **Инструменты** > **Настройки**.
2. В узле **Серверы** выберите сервер.
3. Выберите вкладку **Подключение к Платформе**.
4. Активируйте  **Получение управляющих команд из Activity Monitor**.

5. Укажите значения параметров **Адрес сервера Activity Monitor** и **Токен Activity Monitor**.
6. Нажмите **Применить**.
7. Нажмите **Сохранить**.

Параметры соединения

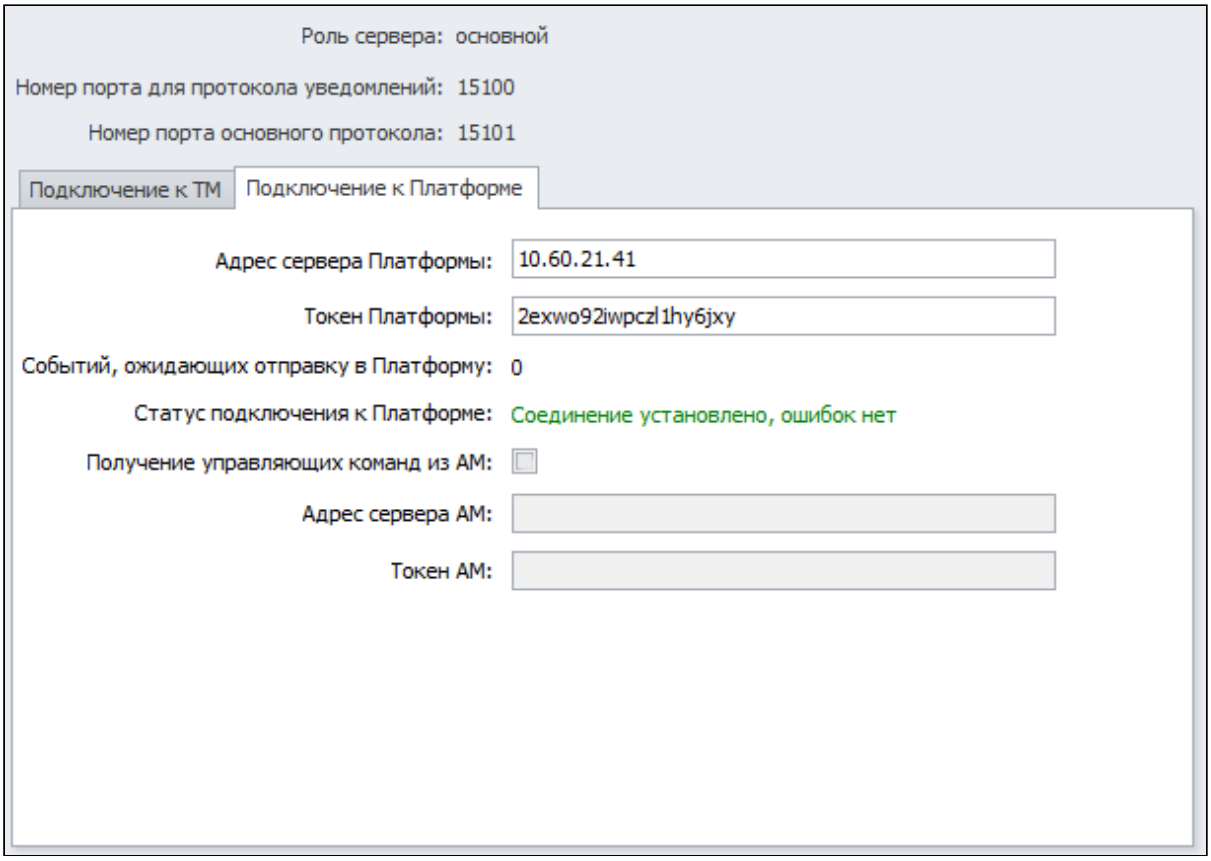
- **Роль сервера** – роль сервера (*основной* или *вспомогательный*), назначенная при установке данного сервера (см. "Порядок установки серверной части InfoWatch Device Monitor").
- **Номер порта для протокола уведомлений**.
- **Номер порта основного протокола**.

> **Примечание:**
>
> Изменение роли сервера (*Основной* или *Вспомогательный*), атрибутов *Номер порта для протокола уведомления* и *Номер порта основного протокола* выполняется с помощью Менеджера управления серверами (см. "Работа с Менеджером управления серверами").

> **Важно!**
>
> При распределенной установке, если Центр расследований установлен в кластере из нескольких серверов, где Activity Monitor установлен на офисной ноде Платформы, настройки сервера Device Monitor для подключения к Платформе необходимо производить в следующем порядке:
>
> - **Адрес сервера Платформы**: указать сервер офисной ноды Платформы, где установлен Activity Monitor;
> - **Адрес сервера Activity Monitor**: указать сервер, где установлена центральная нода Платформы.

- **Адрес сервера Платформы** – строка соединения с Платформой для работы в Консоли управления, куда будут доставляться события. Строку подключения необходимо заполнять в формате (адрес сервера):(порт), где порт – необязательное значение (по умолчанию порт сервера Платформы – 17104). Возможные форматы записи:
  - host
  - host:port
- **Токен Платформы** – токен для подключения к API. Необходимо указывать, начиная с версии Платформы 1.5.0. Вы можете получить актуальный токен в разделе "Основные настройки" Activity Monitor (подробнее см. "InfoWatch Activity Monitor. Руководство администратора", "Основные настройки").
- **Событий, ожидающих отправку в Платформу** – общее количество событий для отправки в Платформу.
- **Статус подключения к Платформе** – информация о состоянии подключения к серверу Платформы.
- **Получение управляющих команд от Activity Monitor** – параметр для включения настройки взаимодействия между DM и Activity Monitor.
- **Адрес сервера Activity Monitor** – строка соединения с Activity Monitor для работы в Консоли управления, куда будут доставляться события. Строку подключения

необходимо заполнять в формате (адрес сервера). Или (адрес сервера):(порт), если для подключения необходимо использовать порт не по умолчанию (по умолчанию порт сервера Activity Monitor – 443). Возможные форматы записи:
    - host
    - host:port.
- **Токен Activity Monitor** – токен для подключения к API. Необходимо указывать, начиная с версии Activity Monitor 2.1.X. Вы можете получить актуальный токен в разделе "Основные настройки" Activity Monitor (подробнее см. "InfoWatch Activity Monitor. Руководство администратора", "Основные настройки").



Примечание:

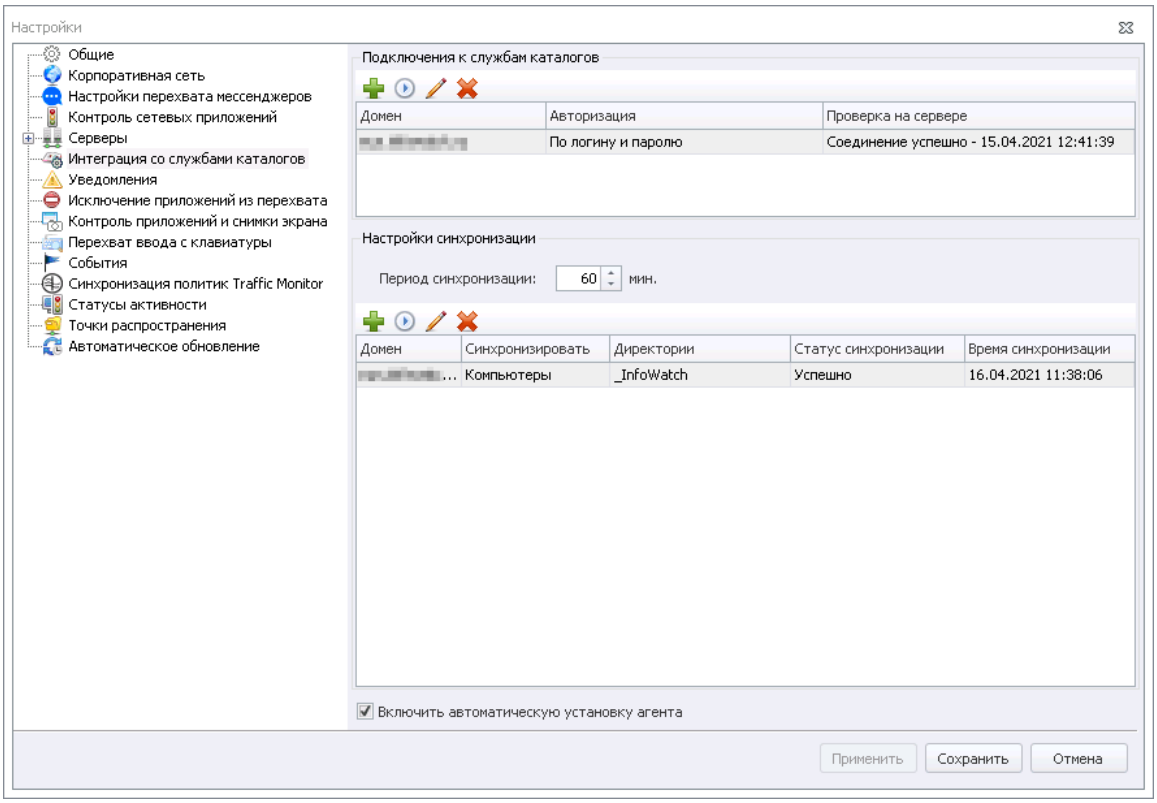
Параметры **Получение управляющих команд из АМ**, **Адрес сервера АМ** и **Токен АМ** используются для Activity Monitor 2.0.x и выше.

Примечание:

При соединении сервера Device Monitor с сервером Платформы осуществляется проверка сертификата удаленного сервера. Подробнее см. "InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию", статья "Настройка проверки сертификатов удаленных серверов".
Если сертификат службы EPEVENTS Платформы не прошел проверку, то параметр **Статус подключения к Платформе** будет иметь значение *Ошибка проверки сертификата*.

4.3.8 Соединение и синхронизация со службами каталогов

В настройке устанавливаются все атрибуты подключения к службам каталогов и синхронизации, задаются параметры установки агентов на новые компьютеры. При подключении к LDAP из Консоли управления необходимо указать настройки подключения. Для того чтобы получать информацию о компьютерах и сотрудниках из служб каталогов, необходимо настроить параметры соединения с LDAP-сервером.

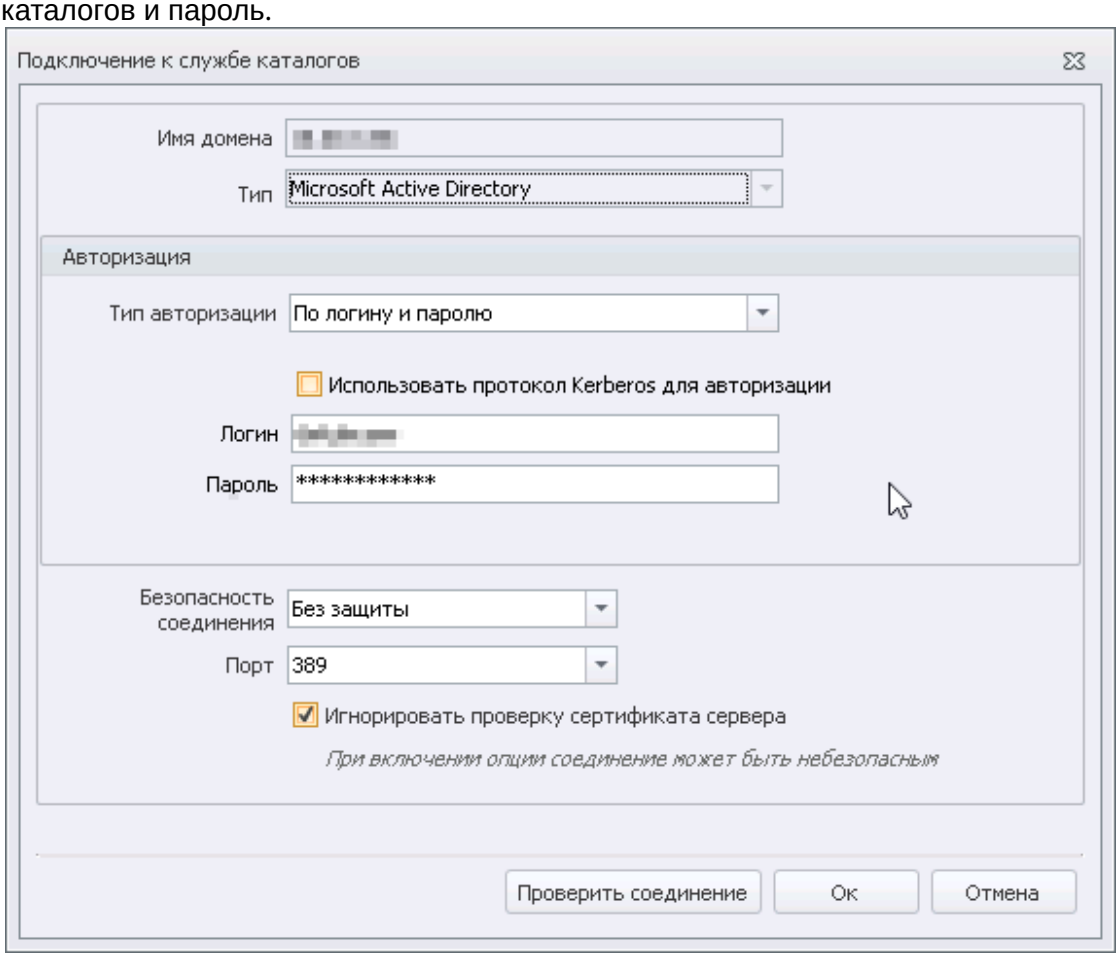


Чтобы настроить параметры соединения с LDAP-сервером:

1. В главном меню Консоли (DM) управления выберите команду **Инструменты** > **Настройки**.
2. Откройте узел **Интеграция со службами каталогов**.
3. Если до этого не было подключений к службе каталогов, то нажмите  в разделе **Подключение к службе каталогов**.
4. В поле **Имя сервера** укажите на выбор доменное имя, IP-адрес сервера LDAP или выберите вручную, нажав **Выбрать домен из леса**. При этом лес выбирается на основе пользователя, запустившего Консоль управления.
5. Укажите тип службы каталогов, если он известен, или установите значение **Авто**. После удачного подключения тип **Авто** будет изменен на тип LDAP, с которым удалось выполнить соединение.

> **Важно!**
>
> После сохранения настроек соединения изменить тип службы каталогов будет невозможно.

6. Укажите данные **Авторизации** для подключения к службе каталогов:
   - **По логину и паролю.** При этом заполните актуальные имя пользователя службы каталогов и пароль.



   - **По учетным данным пользователя.** При этом в качестве данных авторизации используются учётные данные текущей сессии Windows, из под которой запущена Система.
   - **По сертификату клиента.** При этом необходимо указать полное имя секретного ключа и сертификата в формате `.p12` или `.pfx`, а также пароля к ключу.
   - **Анонимная.**
7. При типах авторизации **Учетные данные** пользователя и **По логину и паролю** можно дополнительно установить поддержку протокола Kerberos. При подключении к службе каталогов ALD использование протокола Kerberos не поддерживается.
8. Нажмите **Дополнительно**, чтобы установить безопасность соединения на выбор: **Авто**, **STARTTLS**, **LDAPS** или **Без защиты**. При включении поддержки протокола Kerberos и типа авторизации **По сертификату клиента** будет установлено значение **Авто**.

> **Важно!**
>
> Синхронизация с использованием защищенного соединения поддерживается только для ActiveDirectory.

9. Укажите порт, к которому будут выполняться запросы в тех случаях, когда используемый по умолчанию (389), недоступен: **Авто**, **636**. При выборе типа

авторизации **По сертификату клиента**, включении поддержки протокола Kerberos и выборе **Авто** в предыдущем пункте будет установлено значение **Авто**.

10. Включите настройку **Игнорировать проверку сертификата сервера**, если не требуется делать проверку сертификата, который высылается сервером при установке защищенного соединения.
11. Нажмите **Проверить соединение** и убедитесь, что оно успешно установлено.
12. Нажмите **ОК**.

Чтобы проверить соединение с ранее созданными подключениями:

1. В области **Настройки синхронизации** выберите строку в таблице с нужным соединением.
2. Нажмите  (ручной запуск).
3. Для обновления статуса соединения выберите команду **Вид** > **Обновить** или нажмите **F5**.

После настройки параметров подключения необходимо определить, какую информацию требуется получить от служб каталогов по установленным соединениям и какие политики применить далее.

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

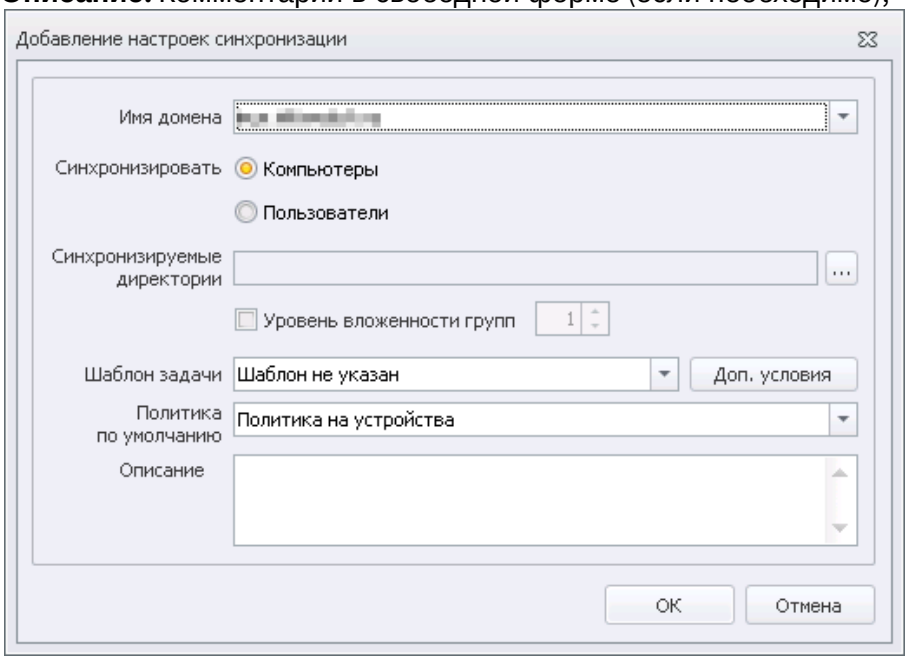
Чтобы добавить настройку синхронизации с Active Directory:

> **Важно!**
>
> Синхронизация групп компьютеров и сотрудников для Astra Linux Directory не поддерживается.

1. В области **Настройки синхронизации** нажмите .
2. В диалоговом окне укажите параметры синхронизации:

- **Имя домена.** Имя домена, с которым ранее было установлено соединение;
- **Синхронизировать.** Объекты синхронизации - **Компьютеры** или **Пользователи**;
- **Синхронизируемые директории.** Директории Active Directory или Astra Linux Directory, которые необходимо синхронизировать. Для этого:
    1. Нажмите .
    2. В дереве укажите одну или несколько директорий для синхронизации.
    3. Нажмите **Выбрать.**
- **Уровень вложенности групп** (если необходимо)**.** Максимальный уровень вложенности равен 100;
- **Шаблон задачи**. Шаблон для синхронизируемой директории, по умолчанию не задан.
- **Политика по умолчанию**. Политика, которая будет назначена на синхронизируемые группы после первой синхронизации;

- **Описание.** Комментарии в свободной форме (если необходимо);



- Нажмите **ОК**.
- Чтобы настройки вступили в силу, нажмите **Применить** в окне **Настройки.**
- Ознакомьтесь с настройками и результатами синхронизации в сводной таблице:

Параметр	Описание
Домен	IP-адрес или DNS-имя домена
Синхронизировать	Объект синхронизации: компьютеры или пользователи
Директории	Папки и группы, назначенные для синхронизации
Статус синхронизации	Может принимать значения: • **Выполняется** (идет процесс синхронизации), • **Успешно** (процесс синхронизации выполнен), • **Не успешно** (процесс синхронизации не выполнен).
Время синхронизации	Дата и время последней синхронизации

Примечание:

Настроить синхронизации компьютеров и пользователей можно только отдельно друг от друга. Поэтому на один домен могут быть заведены две настройки синхронизации.

Чтобы запустить синхронизацию с Active Directory:

1. В области **Настройки синхронизации** выберите нужную строку в таблице.

2. Нажмите  (ручной запуск).
3. Для обновления статуса синхронизации выберите команду **Вид** > **Обновить** или нажмите **F5**.

> **Примечание:**
>
> Синхронизация может запускаться автоматически через выбранный интервал времени. Для этого установите период синхронизации (по умолчанию: один раз в час) и нажмите **Применить**.

После каждой синхронизации, в том числе и первичной, будет автоматически создана задача первичного распространения на компьютеры, добавленные в схему безопасности после синхронизации, при условии, что в записи синхронизации выбран шаблон (подробнее см. "Автоматическая установка Агентов").

Чтобы отредактировать настройки синхронизации с Active Directory:

1. В области **Настройки синхронизации** выберите нужную настройку синхронизации в таблице.
2. Нажмите .
3. Отредактируйте настройки синхронизации.
4. Нажмите **OK**.

Чтобы отключить синхронизацию с Active Directory:

1. В области **Настройки синхронизации** выберите нужную настройку синхронизации в таблице.
2. Нажмите .
3. В диалоговом окне подтверждения нажмите **Да.**

> **Важно!**
>
> При удалении настройки синхронизации будут удалены все связанные с ней группы компьютеров или пользователей.

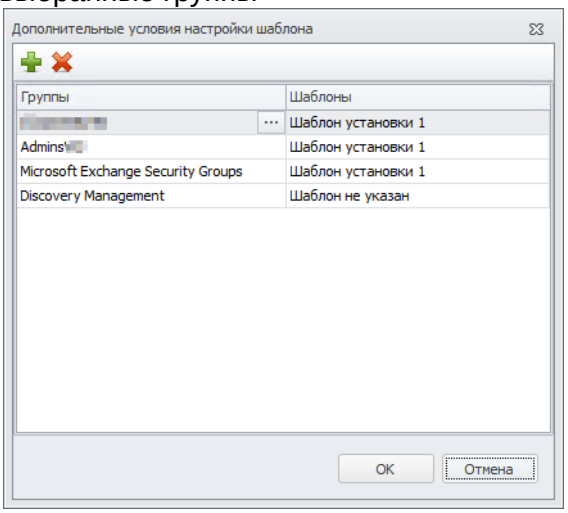
Автоматическая установка Агентов

> **Примечание:**
>
> Автоматическая установка агентов поддерживается на рабочих станциях под управлением ОС Windows или ОС семейства Linux.

Чтобы настроить автоматическую установку агентов на новые компьютеры или компьютеры выбранных подразделений организации:

1. Создайте новую синхронизацию или выберите уже созданную и откройте ее на редактирование.
2. Выберите **Синхронизировать > Компьютеры**
3. Укажите директории Active Directory, для вложенных групп которых необходима автоматическая установка агентов.

4. В настройках синхронизации с Active Directory укажите шаблон задачи, если он был ранее создан для задачи распространения. По этому шаблону после выполнения синхронизации и при наличии новых компьютеров в указанных на предыдущем шаге директориях будет создана и запущена задача первичного распространения. Перейдите к шагу 7.
5. Чтобы отдельно настроить установку агентов для вложенных групп, нужно задать другой шаблон для этих групп. В этом случае на группу, включая ее подгруппы, будет создана задача первичного распространения, указанная в дополнительных условиях записи синхронизации. И наоборот: при исключении использования шаблона задача распространения создана не будет. Нажмите **Доп. условия**.
6. В окне **Дополнительные условия настройки шаблона:**
   a. нажмите , затем 
   b. выберите группы, входящие в указанные на шаге 3, и нажмите **Выбрать**
   c. укажите нужный шаблон, по которому производить установку агентов на выбранные группы



   d. после формирования всех дополнительных условий нажмите **ОК**
7. Нажмите **ОК**
8. Если настройка **Включить автоматическую установку агента** в разделе **Инструменты > Настройки > Интеграция со службами каталогов** выключена, то будут сформированы задачи по шаблонам или добавлены компьютеры в уже существующие задачи после синхронизации. Задачу установки необходимо запустить вручную.
   Включение настройки **Включить автоматическую установку агента** автоматически запустит задачу первичного распространения агентов на новые компьютеры, появившиеся после синхронизации с Active Directory. При этом, если не задан шаблон, то данная настройка ни на что не влияет.
9. В окне **Настройки** нажмите **Сохранить.**

После выполнения синхронизации при наличии новых компьютеров в OU по шаблону создается задача первичного распространения:

- для каждой записи синхронизации,
- для каждой версии шаблона,
- для каждой рабочей версии

Если по шаблону уже сформирована задача, то новые компьютеры будут добавлены в существующую задачу.

4.3.9 Настройка уведомлений сотрудников о нарушении правил

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

Уведомления на компьютерах под управлением ОС Windows с установленным Агентом Device Monitor отображаются при следующих событиях:

- **Запрет доступа к устройству** – сработало правило Device Monitor, запрещающее чтение и запись на устройство (см. "Правило для Device Monitor").
- **Запрет записи на устройство** – сработало правило Device Monitor, запрещающее запись на устройство (см. "Правило для Device Monitor").
- **Запрет записи в открытую область** – сработало правило Device Monitor, запрещающее запись на незашифрованные флоппи-дисководы и съемные устройства (см. "Правило для Device Monitor").
- **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 для такого случая установлена настройка **Запрещена операция** (подробнее см. "Общие настройки работы Агентов"), то запрещаются любые операции, контролируемые текущей политикой безопасности
- **Запрет передачи данных по сетевым протоколам** – сработало правило FTP Monitor, Mail Monitor или IM Client Monitor, запрещающее обмен данными по протоколу FTP/FTPS/SMTP/POP3/Outlook/XMPP/MMP/Skype/Telegram (см. "Правило для FTP Monitor", "Правило для Mail Monitor" и "Правило для IM Client Monitor").
- **Запрет вставки из буфера обмена при нехватке места для событий** – сработала опция «Если место под события закончилось, запрещать операцию», место под события закончилось и выполняется операция вставки из буфера обмена в какое-либо приложение.
- **Запрет доступа к буферу обмена в приложениях** – сработало правило, запрещающее доступ к буферу обмена для приложения при попытке вставки/копирования данных в этом приложении.
- **Запрет использования буфера обмена при срабатывании политики защиты данных** – отображается при блокировании копирования текста в результате применения политики защиты данных.
- **Запрет печати в приложениях** – сработало правило, запрещающее печать для приложения при попытке печати из этого приложения.
- **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.
- **Запрет копирования файла при срабатывании политики защиты данных** – отображается при блокировании копирования файла в результате применения политики защиты данных.
- **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
- **Запрет передачи данных по сетевым протоколам, 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 (DM) (30000 событий), а в общих настройках для такого случая установлена настройка **Запрещена операция** (подробнее см. "Общие

настройки работы Агентов"), то запрещаются любые операции, контролируемые текущей политикой безопасности.

- **Запрет сетевого подключения** – сработало правило Network Monitor, запрещающее передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами (см. "Правило для Network Monitor").
- **Запрет сетевого подключения и запрос временного сетевого подключения** – сработало правило Network Monitor, запрещающее передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами. При этом сотрудник может запросить временный доступ к внешним соединениям (см. "Правило для Network Monitor" и "Временный доступ сотрудника к сети").
- **Запрос временного доступа к устройству по телефону** – текст, отображаемый при выборе пользователем в интерфейсе Агента InfoWatch Device Monitor, вкладка **Список устройств**, команды **Запросить доступ** (см. "Временный доступ сотрудника к устройствам").
- **Запрос временного доступа к устройству по почте** – текст, отображаемый при выборе пользователем в интерфейсе Агента InfoWatch Device Monitor, вкладка **Список устройств,** команды **Запросить доступ** (см. "Временный доступ сотрудника к устройствам").
- **Запрет доступа к облачному хранилищу** – сработало правило Cloud Storage Monitor, контролирующее использование веб-клиентов облачных хранилищ (см. "Правило для Cloud Storage Monitor", настройка **Доступ запрещен**).
- **Запрет записи в облачное хранилище** – сработало правило Cloud Storage Monitor, контролирующее использование веб-клиентов облачных хранилищ (см. "Правило для Cloud Storage Monitor", настройка **Только скачивание**).
- **Запрет запуска приложения** – сработало правило Application Monitor, контролирующее доступ сотрудников к приложениям при помощи черных и белых списков (см. "Правило для Application Monitor").
- **Запрет снимка экрана** – сработало правило ScreenShot Control Monitor, контролирующее снятие снимков экрана (см. "Правило для ScreenShot Control Monitor").
- **Запрет вставки данных** - сработало правило Clipboard Monitor, контролирующее вставку данных из буфера обмена (см. "Правило для Clipboard Monitor").

Уведомления на компьютерах под управлением ОС семейства Linux с установленным Агентом Device Monitor отображаются при следующих событиях:

- **Запрет доступа к устройству** – сработало правило Device Monitor, запрещающее чтение и запись на устройство (см. "Правило для Device Monitor").
- **Запрет записи на устройство** – сработало правило Device Monitor, запрещающее запись на устройство (см. "Правило для Device Monitor").
- **Запрет передачи данных по сетевым протоколам** – сработало правило FTP Monitor или Mail Monitor, запрещающее обмен данными по протоколу FTP/FTPS/SMTP/POP3/ Outlook/XMPP (см. "Правило для FTP Monitor", "Правило для Mail Monitor").
- **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.
- **Запрет доступа к облачному хранилищу** – сработало правило Cloud Storage Monitor, контролирующее использование веб-клиентов облачных хранилищ (см. "Правило для Cloud Storage Monitor", настройка **Доступ запрещен**).
- **Запрет копирования файла при срабатывании политики защиты данных** – отображается при блокировании копирования файла в результате применения политики защиты данных.

Чтобы полностью отключить отображение уведомлений сотрудникам или включить его обратно:

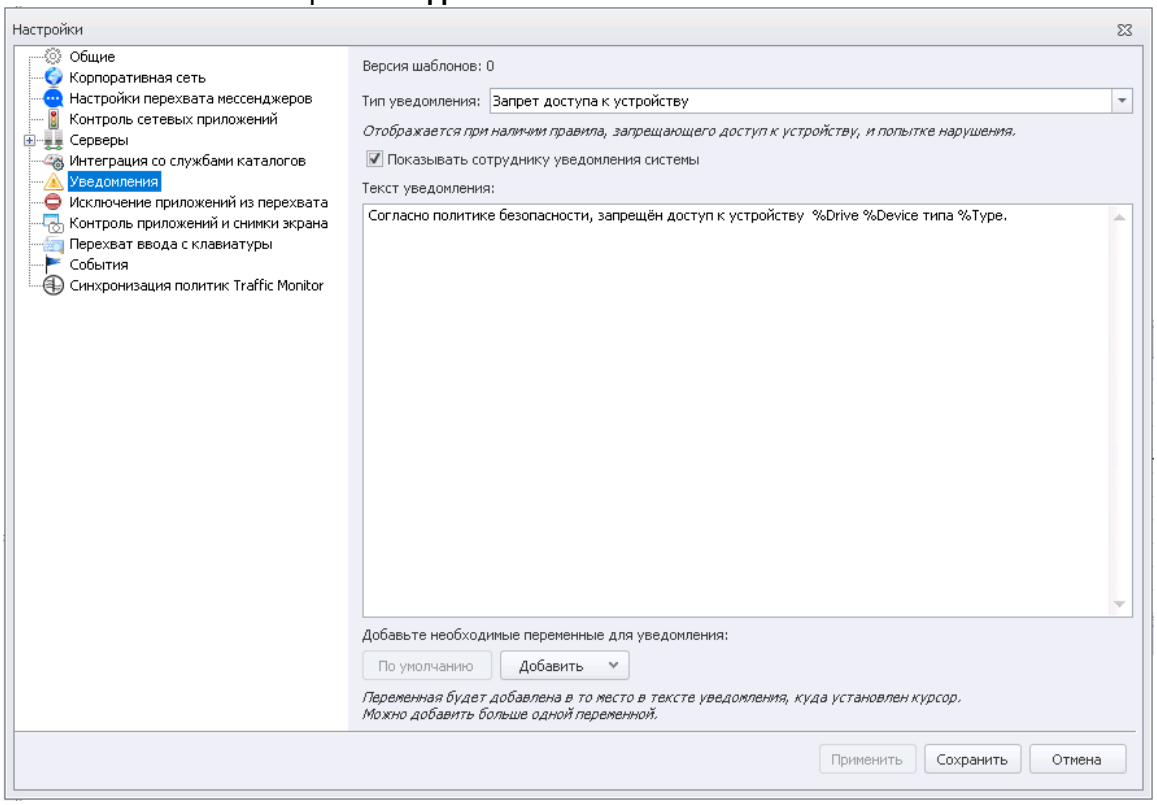
1. В главном меню Консоли управления выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Общие**.
3. Снимите отметку с поля **Отображать уведомления сотруднику** – чтобы отключить отображение уведомлений сотрудникам, или отметьте его – чтобы включить уведомления.
4. Нажмите **Сохранить.**

При необходимости, 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 главном меню Консоли управления (DM) выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Уведомления**.



3. Из раскрывающегося списка **Тип уведомления** выберите необходимый тип уведомлений.
4. Чтобы включить (отключить) отображение данного типа уведомлений, отметьте поле (снимите отметку с поля) **Показывать сотруднику уведомления системы**.
5. В поле ввода текста введите необходимый текст уведомления.
   В сообщении вы можете использовать переменные, которые при выводе сотруднику

будут преобразовываться в актуальные данные: например, тип заблокированного устройства или IP-адрес разрешенного хоста. Для этого установите курсор в необходимое место текста уведомления, затем нажмите **Добавить** и в раскрывшемся списке выберите необходимую переменную.
Чтобы отменить сделанные изменения и вернуть настройки по умолчанию, нажмите **По умолчанию**.

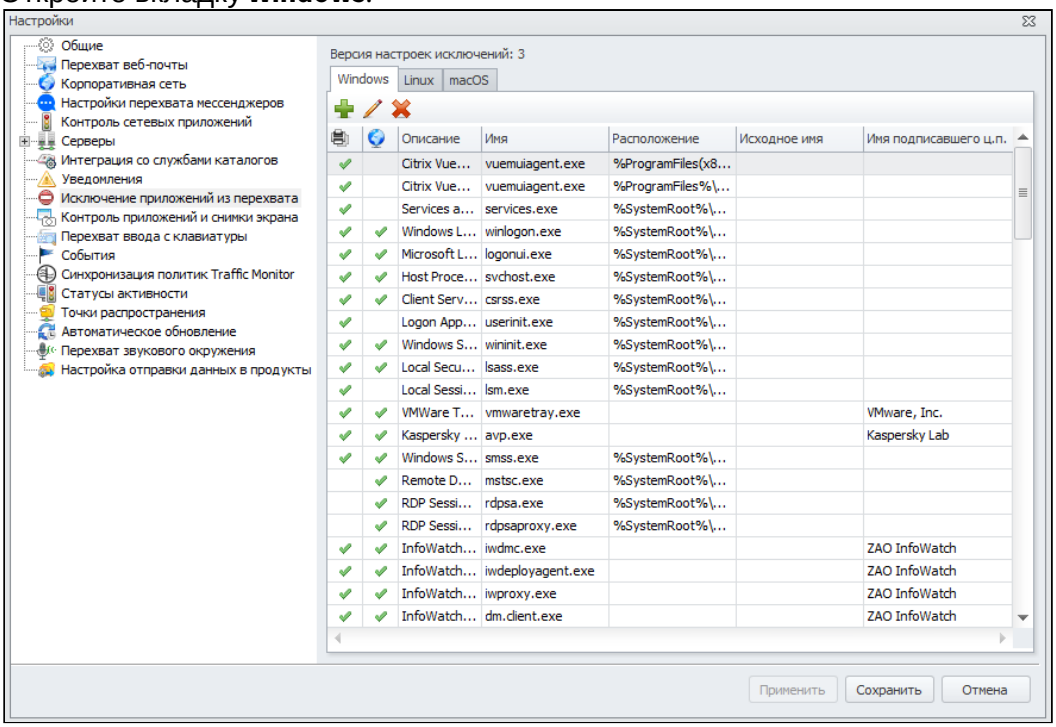
6. Нажмите **Применить**. При необходимости, измените настройки для других уведомлений, повторяя шаги 3-5.
7. После того, как сделаны все необходимые изменения, нажмите **Сохранить**.

4.3.10 Исключение приложений из перехвата

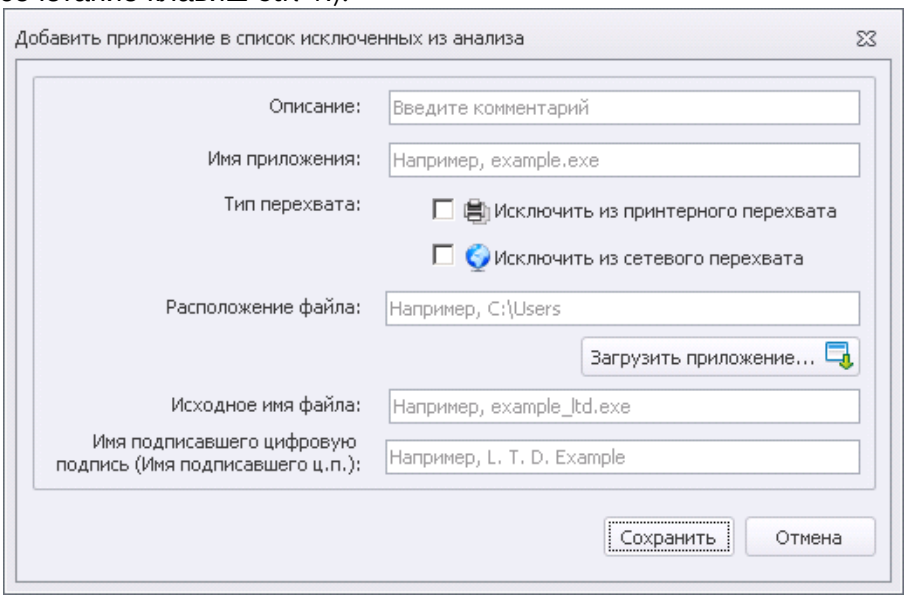
Вы можете настроить параметры приложений, чья активность не будет перехватываться Системой. Данные исключения вступят в силу с момента распространения политик Device Monitor на компьютерах.

Чтобы просмотреть и настроить параметры исключения приложений из перехвата:

1. В главном меню Консоли управления выберите команду **Инструменты** > **Настройки**.
2. Откройте узел **Исключение приложений из перехвата**.
3. Исключение приложений на рабочих станциях под управлением разных ОС настраиваются на разных вкладках.
   - **Для ОС семейства MS Windows:**
     a. Откройте вкладку **Windows**.



b. На панели инструментов нажмите **Добавить** (либо используйте сочетание клавиш Ctrl+N).



c. В поле **Описание** введите произвольное описание приложения. Поле обязательно для заполнения.

d. В поле **Имя приложения** укажите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.

> **Примечание:**
>
> Вместо имени приложения можно ввести символ *. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути или имеющие указанную цифровую подпись (см. п. vi).

e. В поле **Тип перехвата** отметьте:

   i. **Исключить из принтерного перехвата** - если требуется не создавать события и теневые копии при печати из данного приложения;

   ii. **Исключить из сетевого перехвата** - если требуется исключить сетевую активность приложения из перехвата (см. "Контроль сетевого трафика").

> **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 из принтерного перехвата. В противном случае их запуск будет невозможен.

> **Важно!**
>
> Особенности исключения **Outlook** из перехвата:
>
> - При исключении из принтерного перехвата также будет отключен перехват почты Outlook (MAPI). В этом случае для перехвата почты настройте правила по другим протоколам (см. пример в статье Настройка правила для Mail Monitor);
> - Также при исключении из принтерного перехвата будет отключена проверка почты Outlook в соответствии с политиками, настроенными в консоли Traffic Monitor.

f. Вы можете указать параметры файла приложения вручную либо автоматически:
   - Чтобы указать параметры файла приложения вручную:
     i. В поле **Расположение файла** укажите папку на компьютере с Агентом Device Monitor, содержащую исполняемый файл приложения, либо папку верхнего уровня (возможно использование системных переменных). Заданная строка должна быть в начале пути к файлу. Например, если исключение задано в виде: `%ProgramFiles%\Citrix`, то из перехвата будут исключены все приложения в формате *.exe в папке Citrix, а также любой ее подпапке.
     ii. В поле **Исходное имя файла** укажите название приложения (в контекстном меню исполняемого файла приложения выберите **Свойства**, вкладка **Подробно**, атрибут **Исходное имя файла**).
     iii. В поле **Имя подписавшего цифровую подпись** (**Имя подписавшего ц.п.**) 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".

> **Примечание:**
>
> Для полей **Расположение файла** и **Исходное имя файла** значения указываются без учета регистра. Поле **Имя подписавшего цифровую подпись** (**Имя подписавшего ц.п.**) заполняется с учетом регистра.

   - Чтобы указать параметры файла приложения автоматически, нажмите **Загрузить приложение** и укажите необходимый файл. Параметры **Исходное имя файла** и **Имя подписавшего цифровую подпись** будут заполнены автоматически.

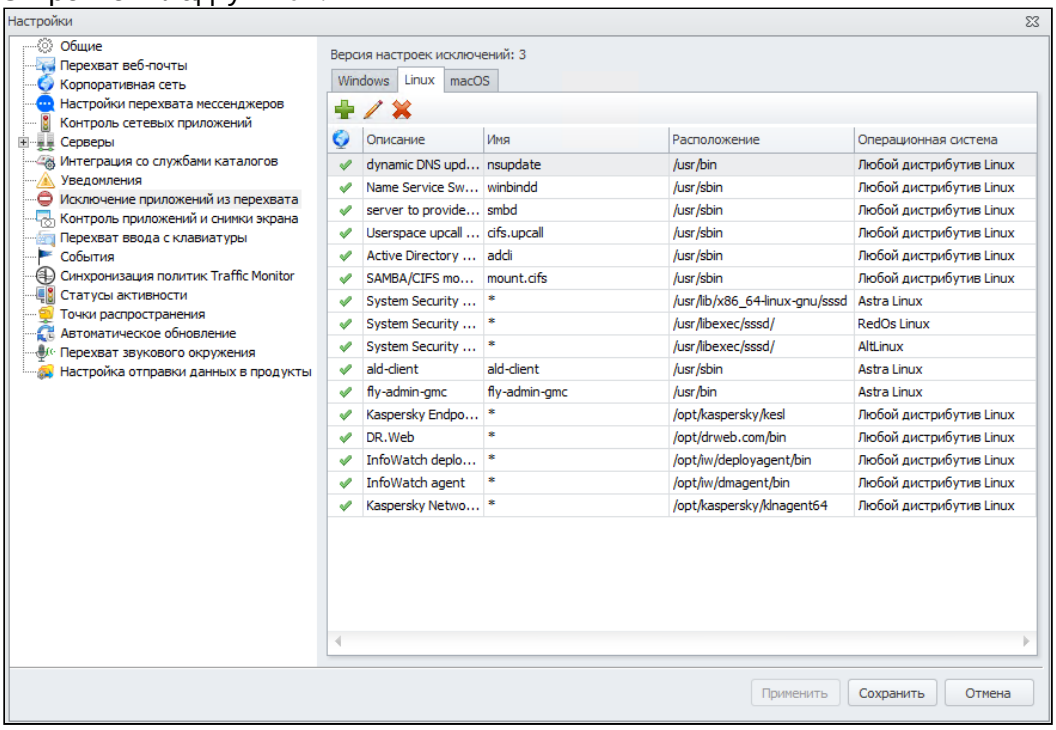
Примечание:

Заполнение полей **Исходное имя файла** и **Имя подписавшего цифровую подпись** (**Имя подписавшего ц.п.**) дает защиту от преднамеренных попыток пользователя, например, переименовать перехватываемое приложение в одно из исключенных.

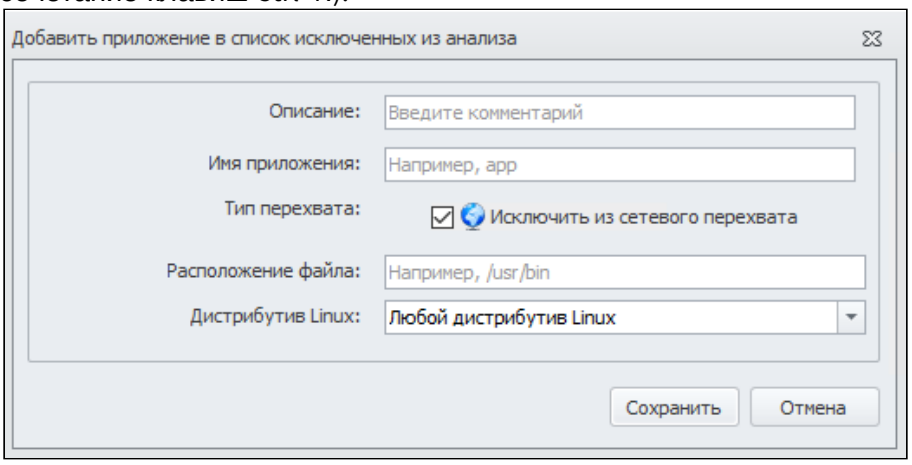
Важно!

Если на рабочих станциях вашей компании в ОС используются разные языки интерфейса по умолчанию, например, английский и китайский, то не рекомендуется задавать исключения приложений из перехвата, используя опцию **Загрузить приложение**. В таком случае указывайте параметры файла приложения вручную.

- **Для поддерживаемых ОС семейства Linux:**
  a. Откройте вкладку **Linux**.



b. На панели инструментов нажмите **Добавить** (либо используйте сочетание клавиш Ctrl+N).



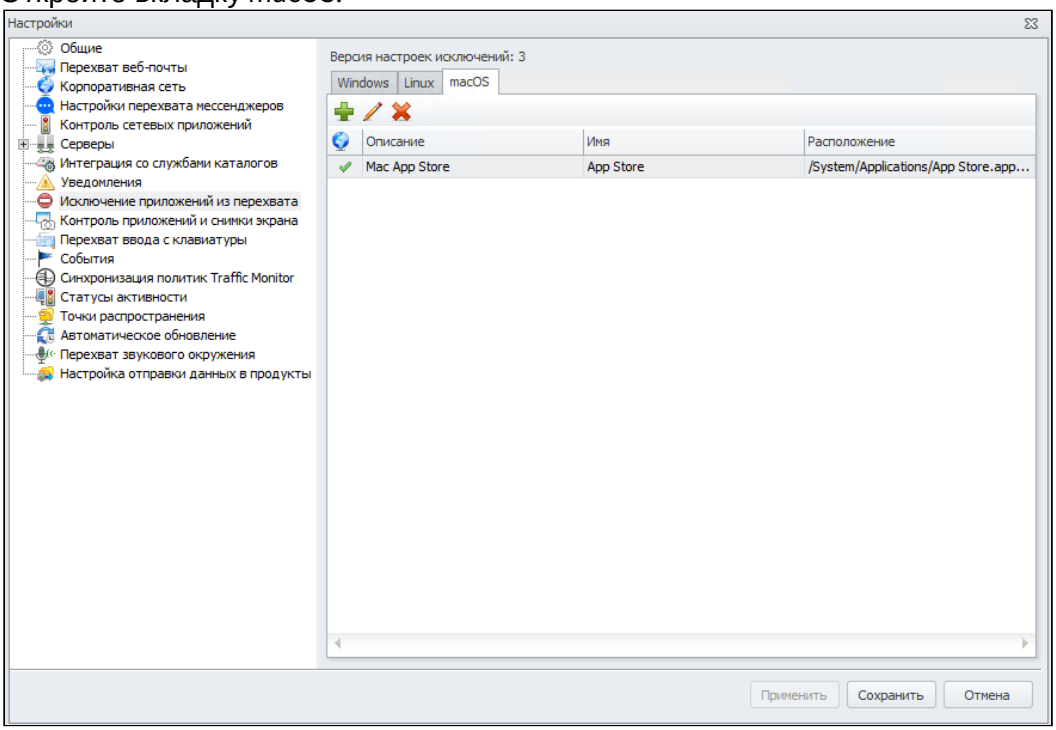
c. В поле **Описание** введите произвольное описание приложения. Поле обязательно для заполнения.
d. В поле **Имя приложения** укажите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.

> **Примечание:**
>
> Вместо имени приложения можно ввести символ *. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути.

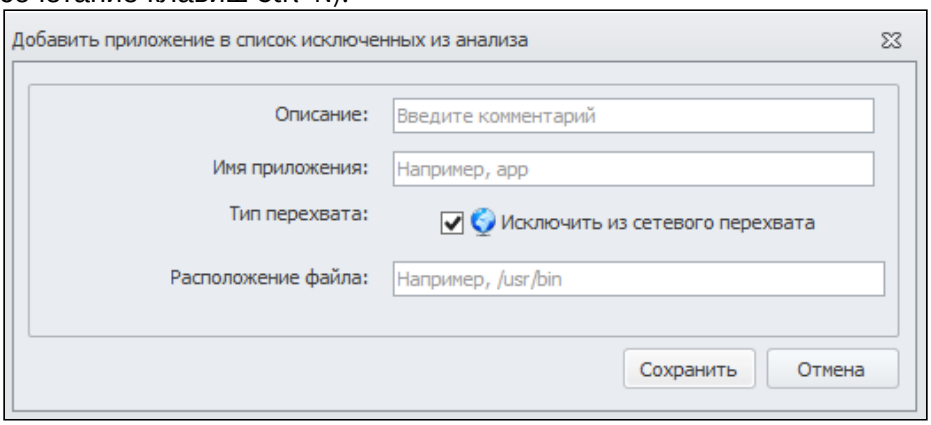
e. В поле **Тип перехвата** выбрано **Исключить из сетевого перехвата** для исключения сетевой активности приложения из перехвата (см. "Контроль сетевого трафика").
f. В поле **Расположение файла** укажите папку на компьютере с Агентом Device Monitor, содержащую исполняемый файл приложения, либо папку верхнего уровня (возможно использование системных переменных). Заданная строка должна быть в начале пути к файлу. Например, если исключение задано в виде: `/opt/myapps`, то из перехвата будут исключены все приложения папке `myapps`, а также любой ее подпапке.
g. В поле **Дистрибутив Linux** в выпадающем списке укажите ОС, для которой настраивается исключение.
Чтобы исключение работало на всех поддерживаемых ОС семейства Linux, выберите вариант **Любой дистрибутив Linux**.

- **Для macOS:**

a. Откройте вкладку macOS.



b. На панели инструментов нажмите **Добавить** (либо используйте сочетание клавиш Ctrl+N).



c. В поле **Описание** введите произвольное описание приложения. Поле обязательно для заполнения.
d. В поле **Имя приложения** укажите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.

> **Примечание:**
>
> Вместо имени приложения можно ввести символ *. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути.

e. В поле **Тип перехвата** выбрано **Исключить из сетевого перехвата** для исключения сетевой активности приложения из перехвата (см. "Контроль сетевого трафика").
f. В поле **Расположение файла** укажите папку на компьютере с Агентом Device Monitor, содержащую исполняемый файл приложения, либо папку верхнего уровня (возможно использование системных переменных). Заданная строка должна быть в начале пути к файлу. Например, если исключение задано в виде: `/opt/myapps`, то из перехвата будут исключены все приложения папке `myapps`, а также любой ее подпапке.

4. Нажмите **Сохранить**. Исключение приложения из перехвата, а также отмена такого исключения, будет применено при следующем запуске этого приложения. Поэтому для применения исключений необходимо перезапустить указанное приложение.

4.3.11 Контроль приложений и снимки экрана

Device Monitor позволяет контролировать запуск приложений на компьютерах, разрешая или запрещая запуск тех или иных приложений. Для обеспечения этой возможности предусмотрено два режима работы с приложениями:

- **Активных белых списков приложений** - сотрудникам и компьютерам, для которых, согласно результирующей политике (DM), действует правило Application Monitor, будет разрешен запуск всех приложений из списков, выбранных в этом правиле. Иные приложения будут запрещены для запуска.
- **Активных черных списков приложений** - сотрудникам и компьютерам, для которых, согласно результирующей политике (DM), действует правило Application Monitor, будет запрещен запуск всех приложений из списков, выбранных в этом правиле. Иные приложения будут разрешены для запуска.

О порядке формирования списков приложений см. "Приложения".

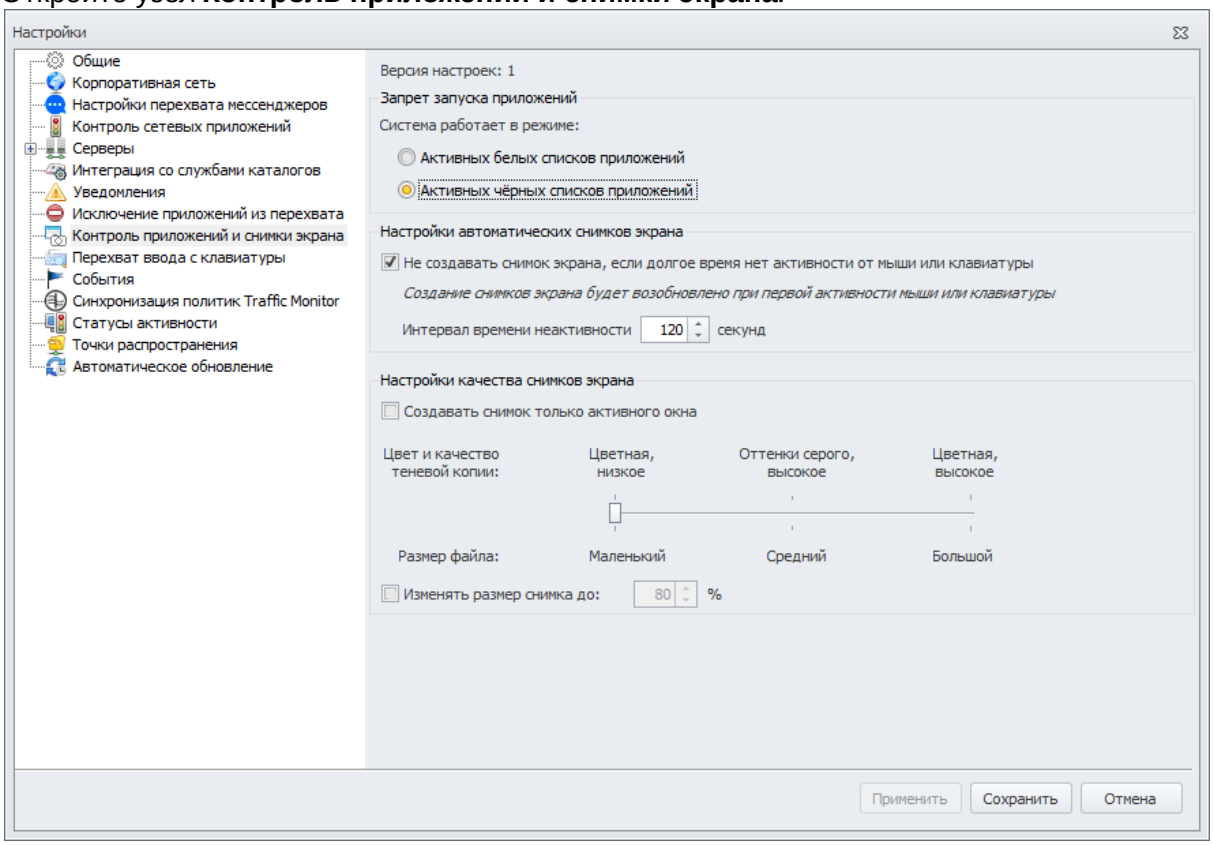
О порядке применения списков в правилах, регулирующих доступ к приложениям, см. "Правило для Application Monitor".

О просмотре результирующей политики см. "Просмотр результирующих политик и белого списка для сотрудника" и "Просмотр результирующих настроек, политик и белого списка на компьютере".

Чтобы выбрать режим работы Device Monitor с приложениями:

1. В главном меню Консоли управления (DM) выберите команду **Инструменты** > **Настройки**.

2. Откройте узел **Контроль приложений и снимки экрана**.



3. В области **Настройка автоматических снимков экрана** определите, нужно ли создавать снимки экрана, если на контролируемом компьютере в течение заданного времени отсутствует активность.
   Если отмечена настройка **Не создавать снимок экрана, если долгое время нет активности от мыши или клавиатуры**, то создание снимков будет прекращено при достижении значения, указанного в поле **Интервал времени неактивности**, и возобновлено при первой активности мыши или клавиатуры.
4. В области **Настройки качества снимков экрана** задайте:
   - **Создавать снимок только активного окна**. Если настройка отмечена, Система создает снимок не всего экрана, а только активного окна.
   - **Цвет и качество теневой копии**. Доступны следующие режимы:
     - **Цветная, низкое**. Будет сохранен цветной файл в низком разрешении. Используйте этот режим, если требуется получать файлы маленького размера.
     - **Оттенки серого, высокое**. Файл будет сохранен в режиме оттенки серого, в высоком разрешении.
     - **Цветная, высокое**. Будет сохранен цветной файл в высоком разрешении. Используйте этот режим, если требуется получать изображения хорошего качества независимо от их размера.
   - **Изменять размер снимка до**. Если при сохранении требуется уменьшить размер изображения, отметьте эту настройку и укажите значение в процентах (процент считается от размера исходного файла).

Важно!

На рабочих станциях под управлением ОС семейства Linux:

- поддерживается только создание снимка всего экрана;
- настройки качества снимков не используются. По умолчанию создаются цветные снимки низкого качества.

6. При необходимости измените режим.
7. Нажмите **Сохранить**.

Примечание:

Система получает снимки экрана, создаваемые в рамках следующих правил (DM): **Правило (DM) для Keyboard Monitor** (создание снимков необходимо настроить в правиле) и **Правило (DM) для ScreenShot Monitor**.

О том, как настроить правило для автоматического создания снимков экрана, см. "Правило для ScreenShot Monitor".

О том, как настроить отправку снимков экрана в разные продукты, см. "Настройка отправки данных в продукты".

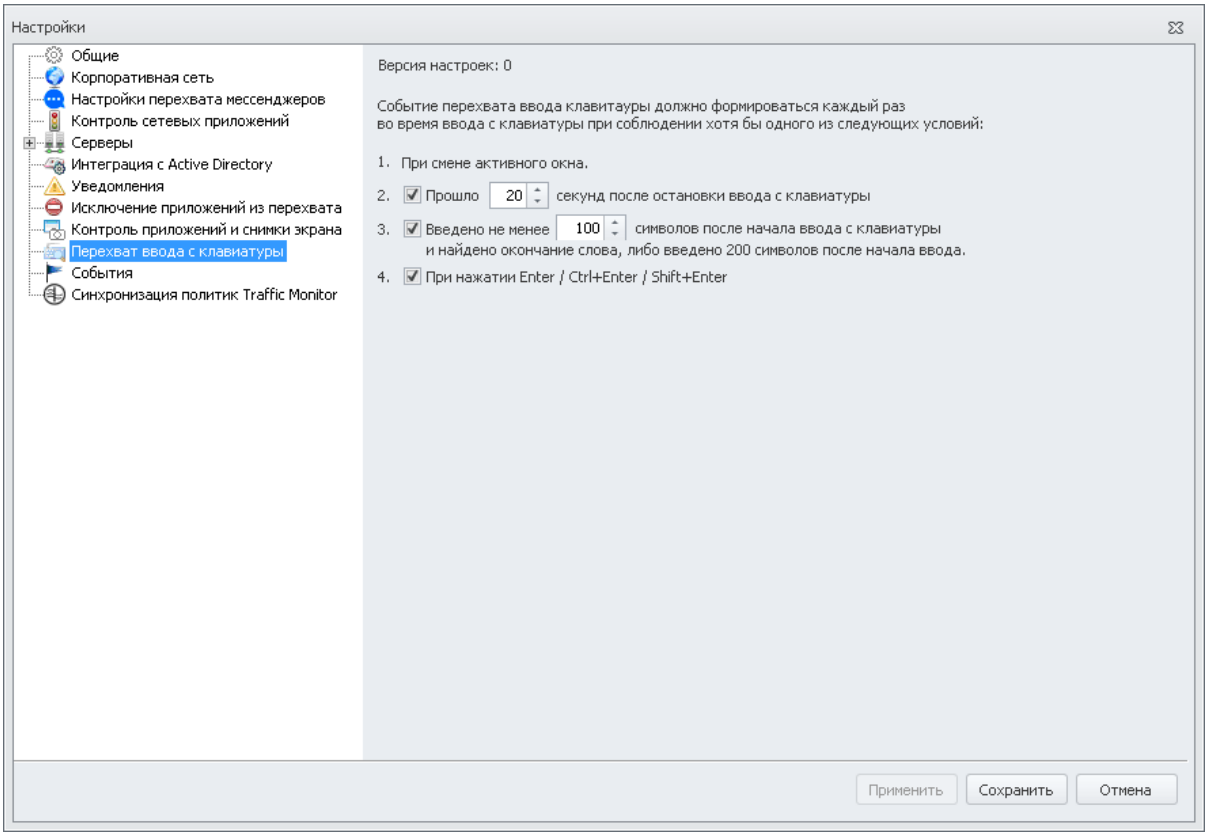
Чтобы применить новую версию настроек приложений и снимков экрана, перезагрузите контролируемые компьютеры.

4.3.12 Контроль ввода с клавиатуры

На закладке **Перехват ввода с клавиатуры** вы можете указать общие условия срабатывания правила.

Для этого:

1. В главном меню Консоли управления выберите команду **Инструменты** > **Настройки**.
2. Откройте узел **Перехват ввода с клавиатуры**.



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

   > **Примечание.**
   >
   > Событие создается безусловно при смене активного окна пользователем

4. Нажмите **Применить**, а затем **Сохранить.**

> **Примечание:**
>
> Начиная с версии Traffic Monitor 7.2, для правила **Контроль ввода с клавиатуры** Офицер безопасности может в Консоли управления DM настроить список ресурсов для перехвата. Подробнее об этом см. раздел «Ресурсы».

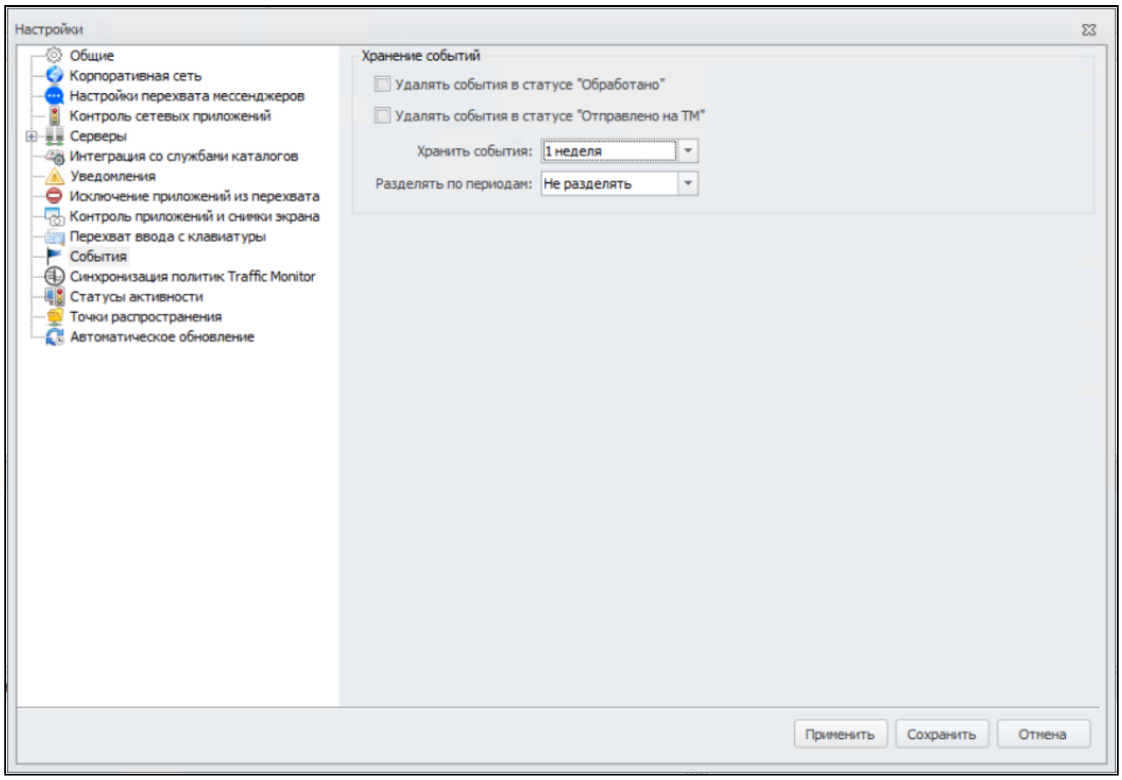
4.3.13 Хранение событий

В разделе **События** вы можете настроить параметры автоматизированного хранения и удаления событий.

Чтобы настроить хранение событий:

1. В главном меню выберите **Инструменты** > **Настройки**.
2. Перейдите в **События**.
3. Выберите:
    - **Удалять события в статусе "Обработано"** – чтобы удалять отработанные события Device Monitor или события сервера, работающего в автономном режиме. При выборе этого пункта стоит учитывать, что в автономном режиме события со статусом **Обработано** не могут быть отправлены на анализ в Traffic Monitor;
    - **Удалять события в статусе "Отправлено на ТМ"** – чтобы удалять события, отправленные на сервер Traffic Monitor для последующего анализа.

> **Примечание:**
>
> Если действия по удалению не выбраны, события со статусами "**Обработано**" и "**Отправлено в ТМ**" будут храниться, как указано в поле "**Хранить события**".



4. В раскрывающихся списках выберите:
    - **Хранить события** – чтобы определить время, в течении которого событие будет находиться в базе данных и отображаться в консоли управления, в том числе для событий со статусом **Ошибка отправки в ТМ** или **Нет лицензии.** По умолчанию – 1 неделя;
    - **Разделять по периодам** – чтобы разделить события на блоки по времени создания для ускорения процессов обращения.

4.3.14 Синхронизация политик Traffic Monitor

В узле **Синхронизация политик Traffic Monitor** нужно указать сервер Traffic Monitor, с которого Device Monitor будет получать версию конфигурации. Полученная конфигурация распространяется на агенты Device Monitor.

При синхронизации политик сервер Device Monitor осуществляет проверку сертификата Traffic Monitor. Для успешной синхронизации настройте данную проверку. См. "Настройка проверки сертификатов удаленных серверов"

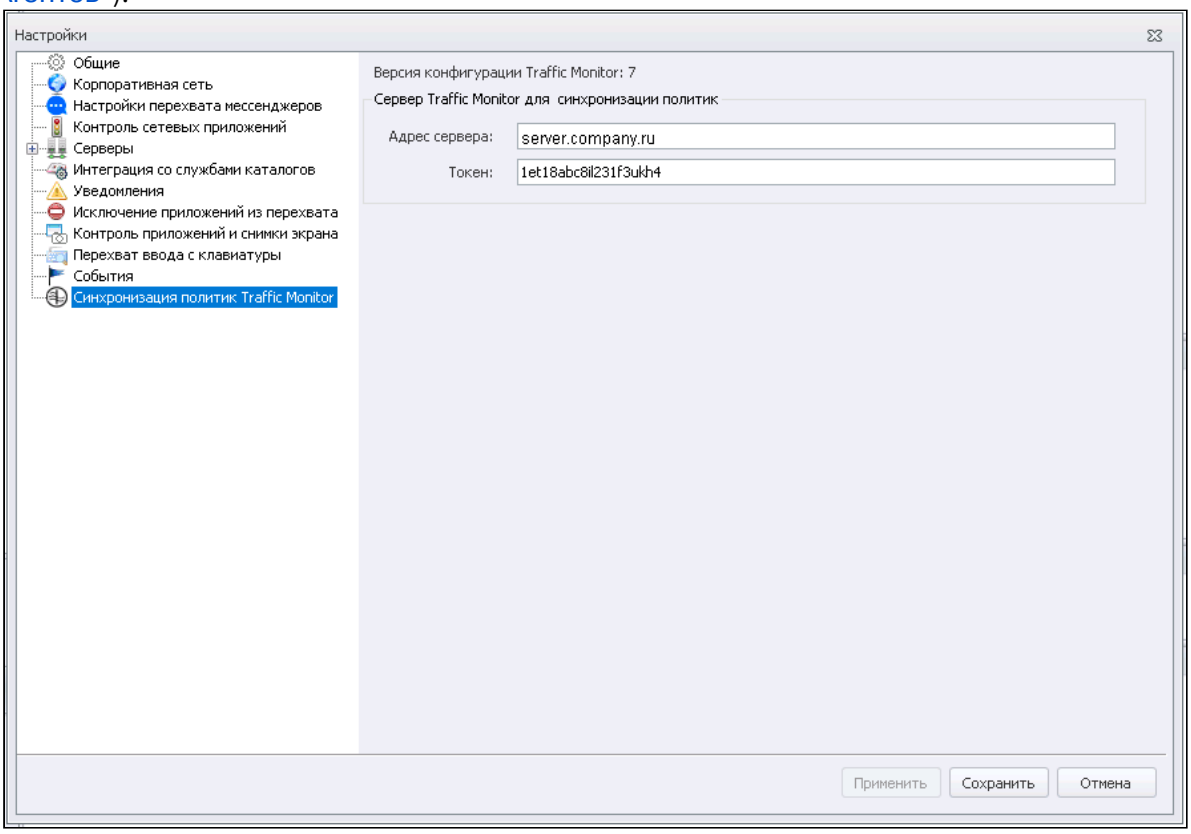
> **Примечание:**
>
> Версия конфигурации, используемой в Traffic Monitor, отображается в консоли ТМ (подробнее см. "InfoWatch Traffic Monitor. Руководство пользователя", статья "Работа с конфигурацией Системы"). При необходимости вы можете сравнить номера версий в Traffic Monitor и Device Monitor и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

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

Чтобы синхронизировать конфигурацию:

1. В главном меню Консоли управления выберите команду **Инструменты** > **Настройки**.
2. Откройте узел **Синхронизация политик Traffic Monitor**.
3. Введите адрес сервера (host), на котором планируется работать в Консоли управления, и токен (см. "Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor"). Убедитесь, что соединение устанавливается с сервером Traffic Monitor той же версии (см. статью Базы знаний "Особенности совместимости разных версий ТМ, DM и

Агентов").



4. Нажмите **Применить**.
5. Нажмите **Сохранить**.

4.3.15 Работа с Менеджером управления серверами

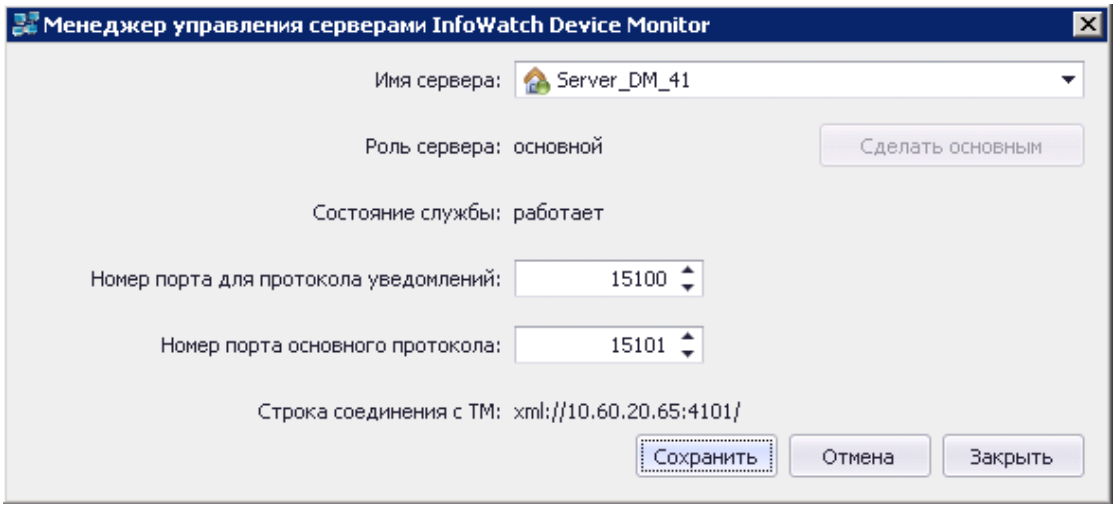
Для определения ролей и изменения некоторых настроек серверов, установленных в Системе, используется Менеджер управления серверами.

Важно!

Для работы утилиты "Менеджер управления серверами" требуется следующее:

- компьютер, на котором запускается утилита, должен входить в домен;
- пользователь, от имени которого запускается утилита, должен иметь роль Администратор на каждом из изменяемых серверов;
- имена серверов должны успешно разрешаться через службу DNS локальной сети заказчика в IP-адрес (проверка: ping <имя_сервера>.<имя_домена>);
- запуск утилиты должен производиться от имени администратора (опция в меню, раскрывающемся по нажатию правой кнопкой мыши на значке утилиты); либо на компьютере должен быть отключен UAC - контроль учетных записей пользователей.

Чтобы присвоить серверу роль Основной:

1. В меню Windows выберите **Пуск** -> **Все программы** -> **InfoWatch** -> **Device Monitor** -> **Менеджер управления серверами**.
   Откроется окно приложения **Менеджер управления серверами InfoWatch Device Monitor**.
   

2. В раскрывающемся списке **Имя сервера** выберите требуемый сервер.
3. Нажмите **Сделать основным**.

> **Примечание.**
>
> Для изменения роли сервера на *Второстепенный* достаточно присвоить другому серверу, используемому в Системе, роль *Основной*.

> **Важно!**
>
> При смене основного сервера все пароли для задач и синхронизаций со службами каталогов нужно повторно ввести через консоль администратора.

4. Нажмите **Сохранить**.
5. Нажмите **Закрыть**.

Чтобы настроить порты сервера:

1. Откройте окно приложения **Менеджер управления серверами InfoWatch Device Monitor**.
2. В раскрывающемся списке **Имя сервера** выберите требуемый сервер.
3. Отредактируйте значения полей **Номер порта для протокола уведомления** и **Номер порта основного протокола**.
4. Нажмите **Сохранить**.
5. Нажмите **Закрыть**.

4.3.16 Настройка статусов активности Агентов

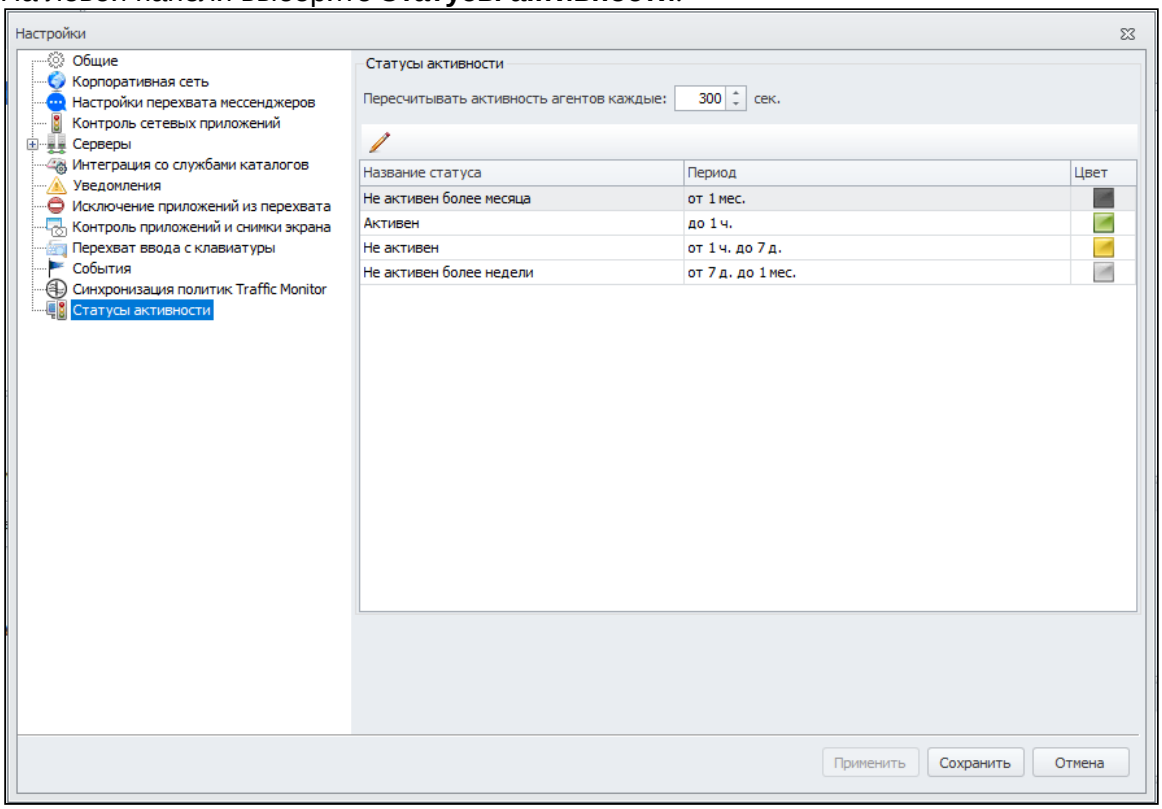
Пользователю доступна настройка статусов активности Агентов. Выполните ее, задав следующие параметры:

- периодичность пересчета активности Агентов (в секундах);

- название статуса;
- период времени, который прошел с момента последнего обращения Агента к серверу.

Чтобы настроить указанные параметры:

1. В главном меню выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Статусы активности**.



3. Используя кнопку  задайте время (в секундах), по истечении которого будет пересчитываться активность Агентов.

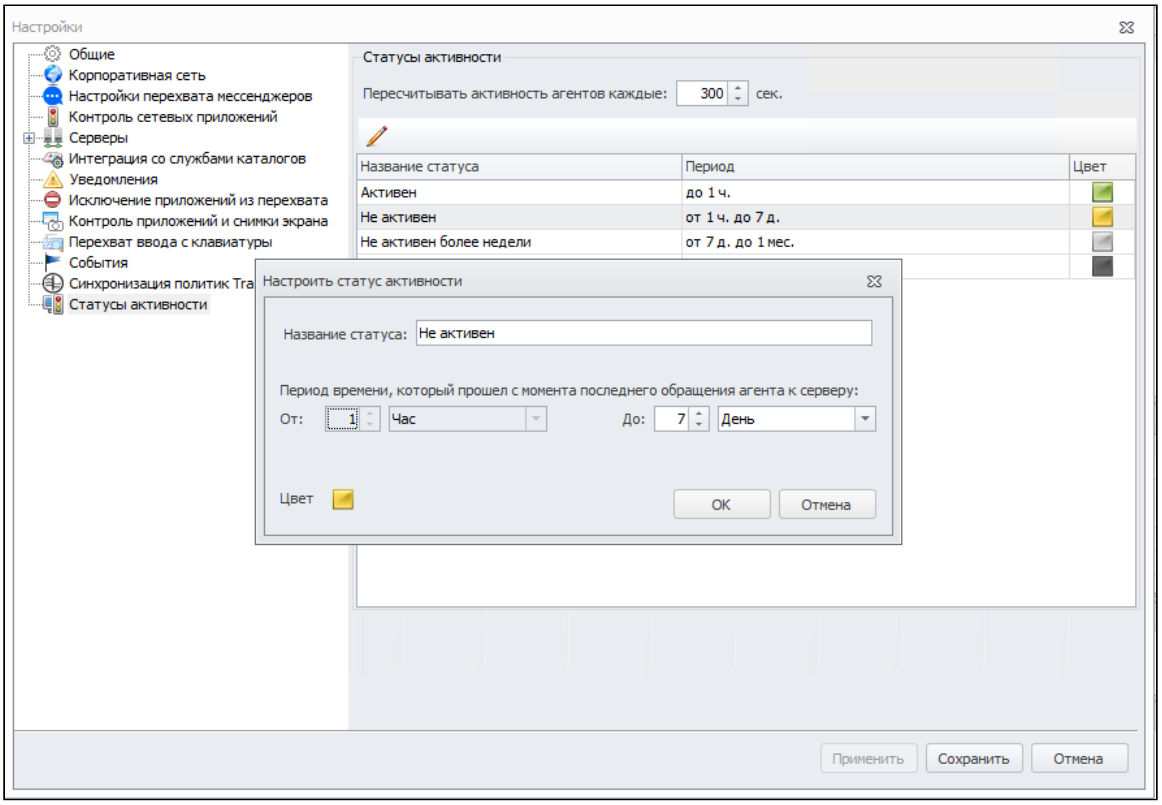
> **Важно!**
>
> Не рекомендуется устанавливать период времени, который прошёл с момента последнего обращения Агента к серверу **меньше**, чем периодичность, с которой Агент отправляет на сервер уведомления о своей работе (значение по умолчанию – 600 секунд, см. Общие настройки работы Агентов). Иначе это приведет к некорректному отображению статусов Агента в Консоли управления DM, так как дата последнего обращения будет обновляться реже, чем статус Агента, который рассчитывается на основе этой даты.

4. Дважды кликните на строке статуса активности и в открывшемся диалоговом окне настройте его:
   a. Задайте название статуса;
   b. Выберите период времени, который прошел с момента последнего обращения Агента к серверу. В течении данного времени будет сохраняться заданный статус активности.

Примечание:

Для компьютера со статусом Агента **Не установлен** статус активности Агента будет **Не активен**, расчет статуса активности не будет зависеть от заданных настроек.

5. Цвета статусов активности заданы по умолчанию и недоступны для редактирования.
6. Чтобы применить внесенные изменения, нажмите **ОК**. В противном случае нажмите **Отмена**.



Примечание:

Обновление статусов в Консоли управления DM происходит:

- автоматически с периодичностью, установленной в настройках Статусов активности;
- вручную, при помощи горячих клавиш Ctrl+F5.

При обновлении статусов осуществляется их актуализация в Консоли управления DM, то есть отображение актуальной информации из БД в Консоли (но не сбор информации от Агентов, т.к. в этот момент соединение с Агентом не устанавливается).

4.3.17 Остановка и запуск агента Device Monitor

При возникновении конфликтов со сторонним ПО, а также внештатных критических ситуаций пользователь может остановить работу агента Device Monitor на рабочей станции. Сделать это можно как локально, так и удаленно.

Примечание.

Некоторые ограничения:

- При остановке агента DM модуль самозащиты агента не отключается.
- Во время сбора результатов логирования (логов) пункт контекстного меню **Диагностика** недоступен.
- Если остановленный агент был обновлен, то после завершения обновления он будет запущен.
- Если агент скрыт на рабочей станции, то он не может быть остановлен локально.

Для рабочих станций под управлением ОС семейства Linux доступна только локальная остановка/запуск агента.

Важно!

Чтобы избежать сбоев в работе сети, перед остановкой агента Device Monitor требуется отключить самозащиту в антивирусных программах, работающих на целевых компьютерах.

После остановки/запуска агента DM необходимо перезагрузить рабочую станцию.

Важно!

Для корректного изменения статуса состояния на/с **Работает в диагностическом режиме** и **Остановлен** рекомендуется использовать консоль DM.

Удаленная остановка/запуск агента на рабочей станции под управлением ОС MS Windows или macOS

Удаленная остановка агента DM осуществляется из консоли управления DM. Для этого в контекстном меню рабочей станции (пункт **Диагностика**) необходимо выбрать действие **Остановить агент** (если агент на рабочей станции запущен).

При выборе действия **Остановить агент** его работа будет приостановлена, статус состояния изменится на **Остановлен**, а статус активности на **Не активен**.

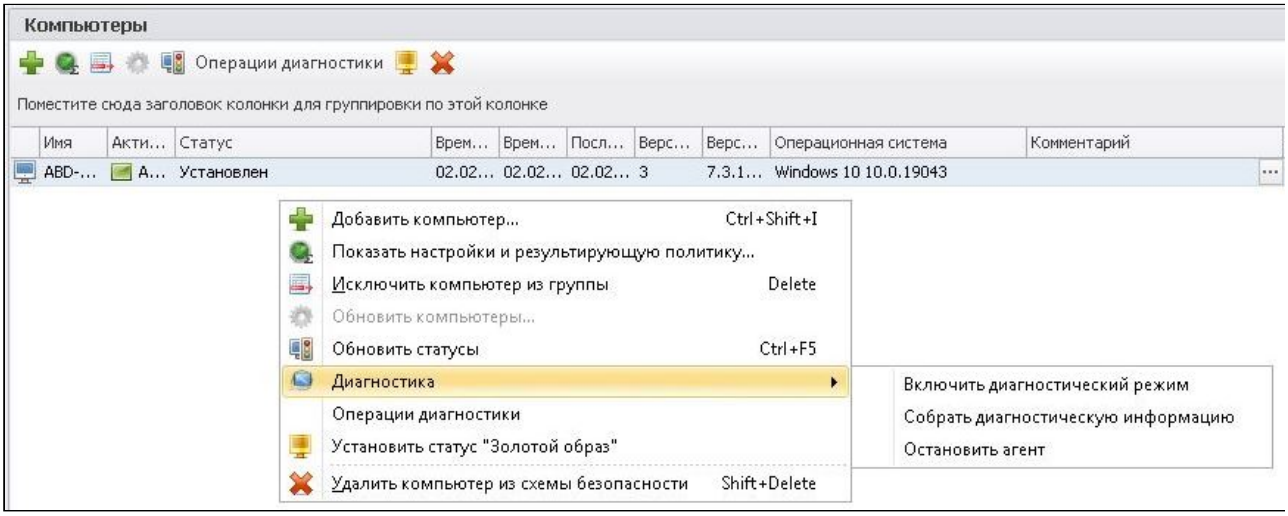
Примечание.

Остановленный агент доступен для обновления или удаления, но в процессе обновления/удаления агента остановка недоступна.

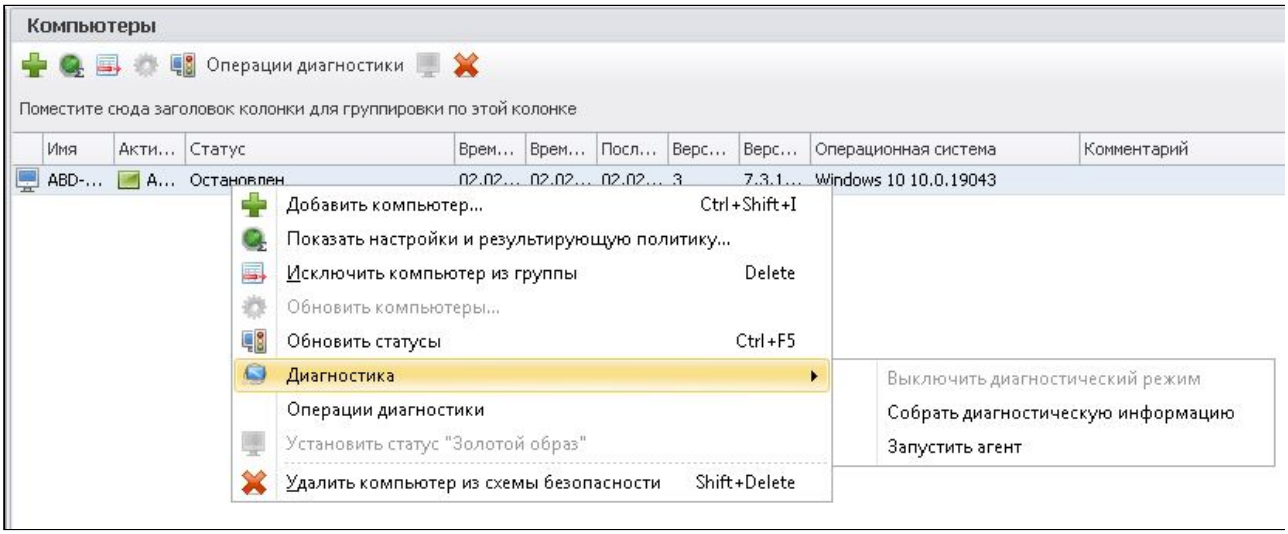
Если с агентом нет связи, то остановка/запуск недоступны.

Стоит иметь ввиду, что после остановки агента на рабочей станции **не** осуществляются:

- перехват событий;
- запрет действий;
- отображение уведомлений, а также значка агента DM на панели инструментов.



Для удаленного запуска агента DM в контекстном меню рабочей станции (пункт **Диагностика**) необходимо выбрать действие **Запустить агент** (если агент на рабочей станции остановлен).



При выборе действия **Запустить агент** его работа будет возобновлена, а статус рабочей станции изменится на **Установлен**.

Локальная остановка/запуск агента на рабочей станции под управлением ОС MS Windows

Локальная остановка/запуск агента осуществляется из командной строки Windows от имени администратора. Для этого необходимо запустить приложение **rmtdiag.exe**, указав полный путь к нему

на рабочей станции (по умолчанию C:\Program Files\InfoWatch\DeviceMonitor\Client), с нужным параметром, Например:

- **C:\Program Files\InfoWatch\DeviceMonitor\Client\rmtdiag.exe /cle** - для запуска агента;
- **C:\Program Files\InfoWatch\DeviceMonitor\Client\rmtdiag.exe /cld** - для остановки агента.

Важно!

Для остановки агента необходимо ввести пароль деинсталляции агента DM. Пароль вводится через пробел после ключа **/cld**. Для запуска агента пароль необязателен.

Подробнее о пароле деинсталляции смотрите в статье "Создание задачи смены пароля деинсталляции".

Локальная остановка/запуск агента на рабочей станции под управлением ОС Astra Linux или РЕД ОС

Локальная остановка/запуск агента осуществляется из консоли рабочей станции.
Для действий с агентом войдите в консоль и введите команду:

- `sudo systemctl start iwdm.target` - для запуска агента;
- `sudo systemctl stop iwdm.target` - для остановки агента;
- `sudo systemctl status iwdm.target` - для проверки статуса агента.

Важно!

После ввода команды для остановки/запуска агента будет запрошен пароль деинсталляции. Подробнее о пароле деинсталляции смотрите в статье "Создание задачи смены пароля деинсталляции".

Если выполнена авторизация от имени суперпользователя `root`, команды вводите без sudo, также в этом случае не потребуется ввод пароля.

Также имеется возможность остановки/запуска отдельных сервисов:

- `iwdmc.service`;
- `iwdmproxy.service`;
- `iwdminstca.service`.

4.3.18 Настройка распространения Агентов

Для быстрого получения дистрибутива Агента на рабочих станциях используется сервис распространения дистрибутивов. После установки сервиса создаются директории с дистрибутивами, которые регистрируются в Системе и являются точками распространения с протоколом Infowatch. Чем больше точек распространения добавлено в Систему, тем быстрее будет проходить распространение или обновление Агентов. Точками распространения могут быть:

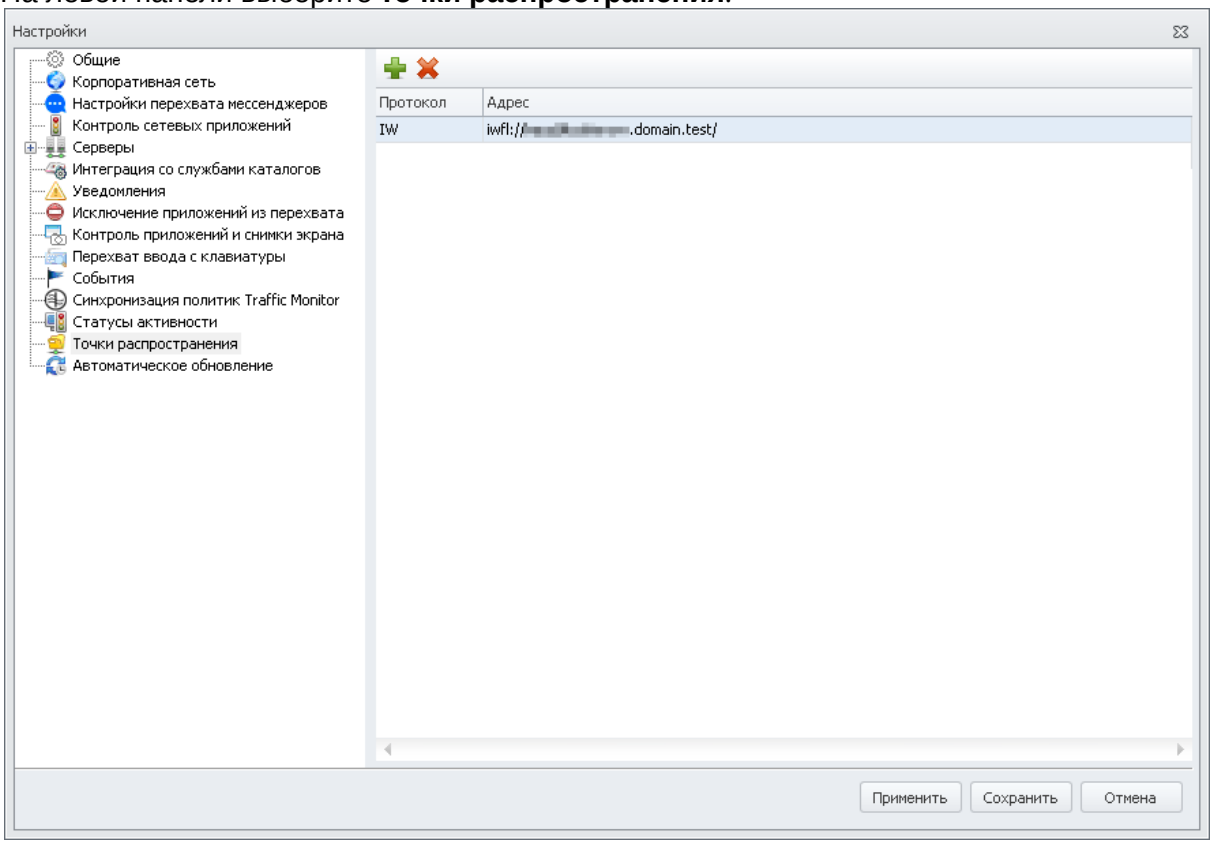
- FTP или SMB-папка, в которую можно вручную загружать дистрибутивы.

> **Важно!**
>
> Чтобы использовать общую SMB-папку в качестве точки распространения, необходимо настроить для этой папки анонимный доступ (для настройки анонимного доступа в системе семейства MS Windows см. Параметры безопасности Windows).

- Любая рабочая станция, на которой установлен сервис распространения. В этом случает точка распространения создается по умолчанию.

Чтобы добавить новую точку распространения:

1. В главном меню выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Точки распространения**.



3. Нажмите  и введите параметры:
   - Протокол (на выбор):
     - Сетевые ресурсы Windows (SMB);
     - Протокол передачи файлов (FTP);
     - Протокол InfoWatch (рекомендуется использовать).
       Примечание: протокол Infowatch отображается только у записей, добавленных автоматически, т.е. на рабочих станциях, на которых установлен сервис распространения дистрибутивов
   - Имя сервера, на котором открыт доступ к папке с дистрибутивами
   - Порт (для протокола FTP: номер порта или по умолчанию).
4. Нажмите **Проверить подключение** и убедитесь, что точка публикации доступна.
5. Нажмите **ОК**, и далее **Сохранить**. При сохранении будет проверена доступность точки распространения.

Таким образом формируется список точек распространения. Далее он отправляется на Агент вместе с заданием установки или обновления. Если запустить задачу на Агенте, а потом удалить точку распространения, то новая информация на Агент не придёт. В этом случае он получит дистрибутив из одной из действующих точек распространения.

В любой точке распространения должна сохраняться следующая структура папок для публикации дистрибутивов:

- Версия Device Monitor (например, "7.4.0")
  - Операционная система 1 (поддерживаются: "Windows", "AstraLinux-1.7", "RedOS-7.3")
    - Платформа (x86 или x64)
      - Дистрибутив агента для данной ОС и платформы

> **Важно!**
>
> Невозможно удалить точку распространения, если она связана с одной из задач.
>
> Недоступно удаление точек распространения с протоколом Infowatch. Они будут удалены автоматически при удалении сервиса распространения с рабочей станции.

4.3.19 Автоматическое обновление Агентов

> **Важно!**
>
> Чтобы обновить Агенты версий 7.2–7.16 **до версии 7.18** через Консоль управления Device Monitor, используйте **Задачу первичного распространения**. При обновлении с версии 7.17 и выше используется процедура, описанная в этой статье.

Для настройки автоматического обновления Агентов до рабочей версии сервера:

1. Перейдите в раздел **Инструменты** > **Настройки** > **Серверы**.
2. В поле **Рабочая версия для автоустановки и автообновления агентов** укажите целевую версию.
3. Перейдите в раздел **Инструменты** > **Настройки** > **Автоматическое обновление**.
4. Включите автообновление и укажите периодичность проверки его наличия:
   - ежечасно или с периодичностью в несколько часов;
   - ежедневно;
   - еженедельно по заданным дням недели.

   > **Примечание:**
   >
   > Первая проверка каждые N часов будет выполняться в момент запуска Системы, если настройка задана, или в момент получения смены настроек, когда ее включили, и далее каждые N часов.
   >
   > Ежедневная и еженедельная проверка будет выполняться в 13:00 (значение указано в БД).

5. Укажите параметры автообновления:

a. Укажите количество попыток скачивания обновления.
b. На вкладке **Исключения компьютеров** укажите рабочие станции, которые стоит исключить из обновления, выбрав их из дерева каталога или с помощью поиска по имени.
c. На вкладке **Параметры установки** укажите:
    i. когда следует установить обновление при его наличии: *Сразу после загрузки*, *Ежедневно*, *Еженедельно по заданным дням недели*;
    ii. наиболее подходящее время суток для обновления;
    iii. производить ли принудительное обновление по истечении выбранного количества попыток.
d. На вкладке **Параметры перезагрузки** укажите:
    i. как долго ожидать перезагрузки без уведомления: *Не ожидать*, *Ожидать n часов*, *Ожидать бесконечно*;
    ii. уведомлять ли сотрудника о необходимости перезагрузки, как часто и каким сообщением.

> **Важно!**
>
> Для корректной блокировки съемных устройств после обновления Агента на ОС семейства Linux обязательно перезагрузите рабочую станцию.
>
> Уведомления не будут отображаться, если:
>
> - на компьютере включено скрытие присутствия Агента;
> - Агент установлен на ОС Astra Linux или РЕД ОС.

6. Нажмите **ОК**, а затем **Сохранить**.

После сохранения настроек запускается процесс автоматического обновления. Согласно заданным параметрам (закладка **Параметры автообновления**) в пункте меню **Результаты автообновления** отображаются рабочие станции с одним из статусов:

- *Обновление разрешено* – скачан дистрибутив Агента нужной версии, необходимость обновления подтверждена расписанием в настройках;
- *Скачивание дистрибутива* – скачивание дистрибутива Агента с ближайшей точки распространения;
- *Ожидание обновления* – ожидание в соответствии с расписанием установки обновлений;
- *Выполняется обновление* – наступило указанное в настройках время установки обновления или немедленная установка обновления после скачивания;
- *Обновление завершено* – успешное обновление;
- *Обновление завершено с ошибкой* – невозможность успешного обновления с записью в журнал ошибок;
- *Разрешено повторное обновление* – запуск обновления после устранения ошибок;
- *Ожидание перезагрузки* – запрос на перезагрузку рабочей станции вручную или по истечении заданного в параметрах автообновления времени.

Пользователь может:

- отфильтровать рабочие станции по дате их появления в списке. Для этого создайте фильтр, нажав  на панели **Навигация** и задайте параметры фильтра;
- ограничить общее количество выдаваемых записей;
- просмотреть параметры обновления и перейти в **Настройки** для их изменения;
- просмотреть ошибки в случае их возникновения;

- повторно запустить обновление, если оно завершилось с ошибкой.

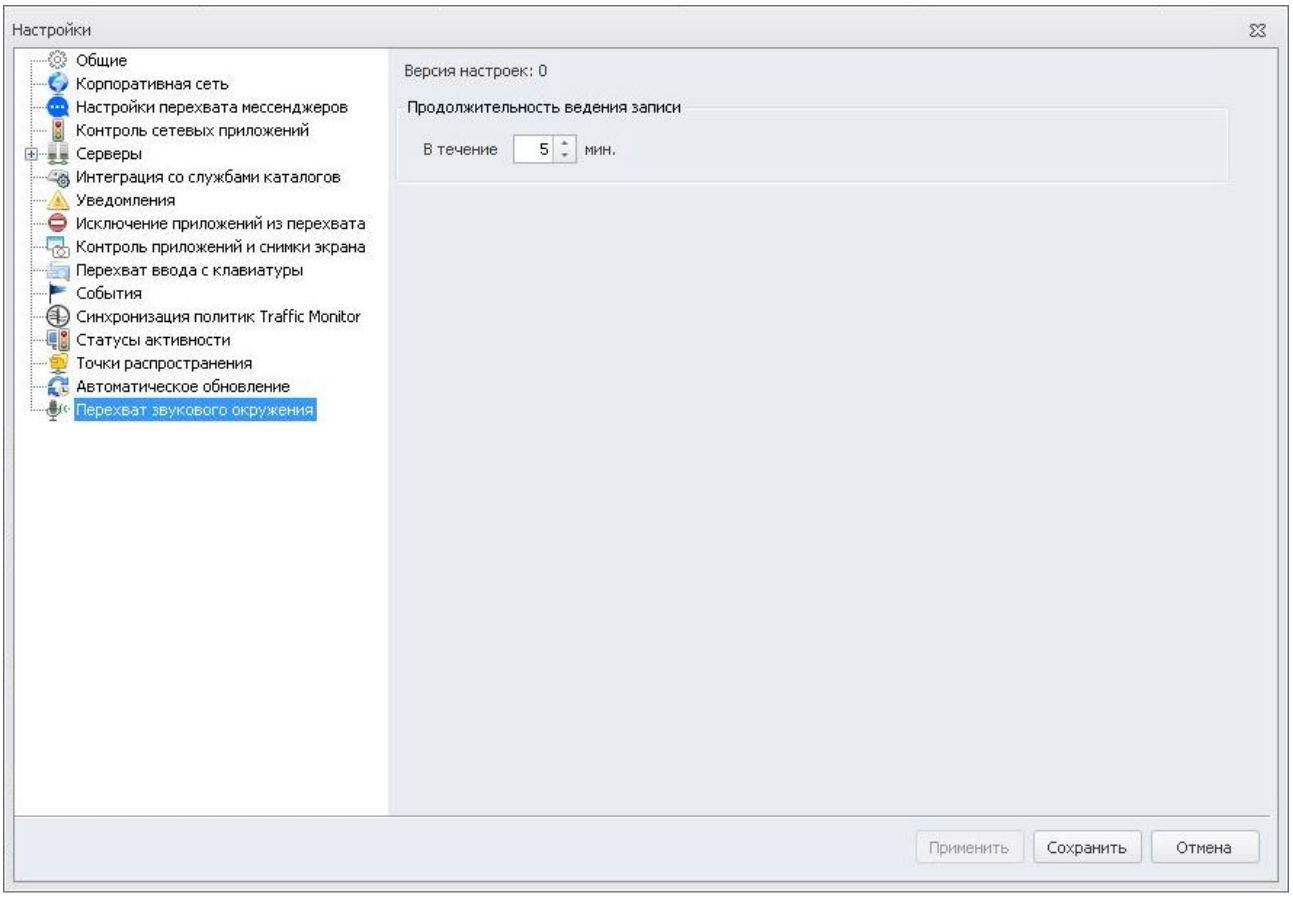
4.3.20 Настройка перехвата звукового окружения

> **Важно!**
>
> Функциональность предназначена только для InfoWatch Activity Monitor.
>
> Функциональность онлайн-наблюдения не поддерживается на агентах под управлением ОС Windows 7.

Перехват звукового окружения – это ведение записи звука вокруг рабочей станции в соответствии с правилом Audio Record Control.

Пользователю доступна настройка перехвата звукового окружения. Чтобы задать параметры настройки:

1. В главном меню выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Перехват звукового окружения**.
3. Используя кнопку , задайте время от 1 до 120 минут. В течение указанного времени Система будет вести запись звукового окружения рабочей станции пользователя. По окончании заданного периода запись будет прекращена.
4. Нажмите **Применить**, затем **Сохранить**.



Важно!

В области уведомлений панели задач Windows на компьютере, где установлен Агент, значок микрофона не будет отображаться, если:

- сработало правило перехвата звукового окружения;
- вручную была запущена онлайн-запись звукового окружения.

Если до начала записи микрофон использовался каким-либо приложением и отображался, то он также будет скрыт. Доступно для Агентов с ОС Windows 10.

Примечание:

DM записывает звуковое окружение рабочей станции непрерывно в течение заданного в настройках периода. В момент, когда сотрудник начал использовать ресурс, указанный в правиле **Audio record control**, DM запускает аудиозапись окружения рабочей станции. По окончании периода, заданного в настройках правила перехвата звукового окружения, DM прекращает аудиозапись. Если сотрудник пользовался несколькими ресурсами, включенными в данное правило, то при переключении с ресурса на ресурс DM продлевает запись.

Пример 1

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 переходит на ресурс https://example.ru/. DM начинает вести запись звукового окружения и создает событие.

Через 3 минуты после начала ведения первой записи сотрудник покидает данный ресурс и переходит на другой, также контролируемый правилом, https://example.com. Система продолжает вести запись звукового окружения, при этом заново начав отсчет интервала в 5 минут.

По истечении 5 минут использования ресурса DM завершает запись. В результате в Activity Monitor будут созданы 2 события (для каждого из ресурсов), содержащие аудиозапись длиной 3 и 5 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, контролируемый правилом. Затем переходит на ресурс, не включенный в правило, после чего возвращается на контролируемый ресурс.

Сотрудник переходит на ресурс https://example.ru/. DM начинает вести запись звукового окружения и создает событие. Через 3 минуты после начала ведения первой записи сотрудник покидает ресурс, переходит на https://example1.ru/ (не включен в список контролируемых ресурсов) и пользуется им 4 минуты. DM продолжает вести запись звукового окружения.

Примечание: Если до истечения периода записи (т.е. в рамках заданных в примере 5 минут) сотрудник перестает использовать ресурс, контролируемый правилом, и начинает использовать ресурс, не включенный в список контролируемых, то DM завершает запись по истечении 5 минут.

Затем сотрудник возвращается на контролируемый ресурс https://example.ru/. DM начинает вести запись звукового окружения и создает событие. По истечении 5 минут DM завершает запись. В результате в Activity Monitor будут 2 события, содержащие аудиозапись длиной 5 и 5 минут.

Пример 3

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, контролируемый правилом. Затем переходит на ресурс, не включенный в правило, после чего возвращается на контролируемый ресурс.

Сотрудник переходит на ресурс https://example.ru/. DM начинает вести запись звукового окружения и создает событие. Через 3 минуты после начала ведения первой записи сотрудник покидает ресурс, переходит на https://example1.ru/ (не включен в список контролируемых ресурсов) и пользуется им в течение 1 минуты. DM продолжает вести запись звукового окружения.

Затем сотрудник возвращается на контролируемый ресурс https://example.ru/. DM продлевает запись звукового окружения для этого ресурса на 5 минут и создает событие. По истечении 5 минут DM завершает запись. В результате в Activity Monitor будут 2 события, содержащие аудиозапись длиной 4 и 5 минут.

4.3.21 Настройка отправки данных в продукты

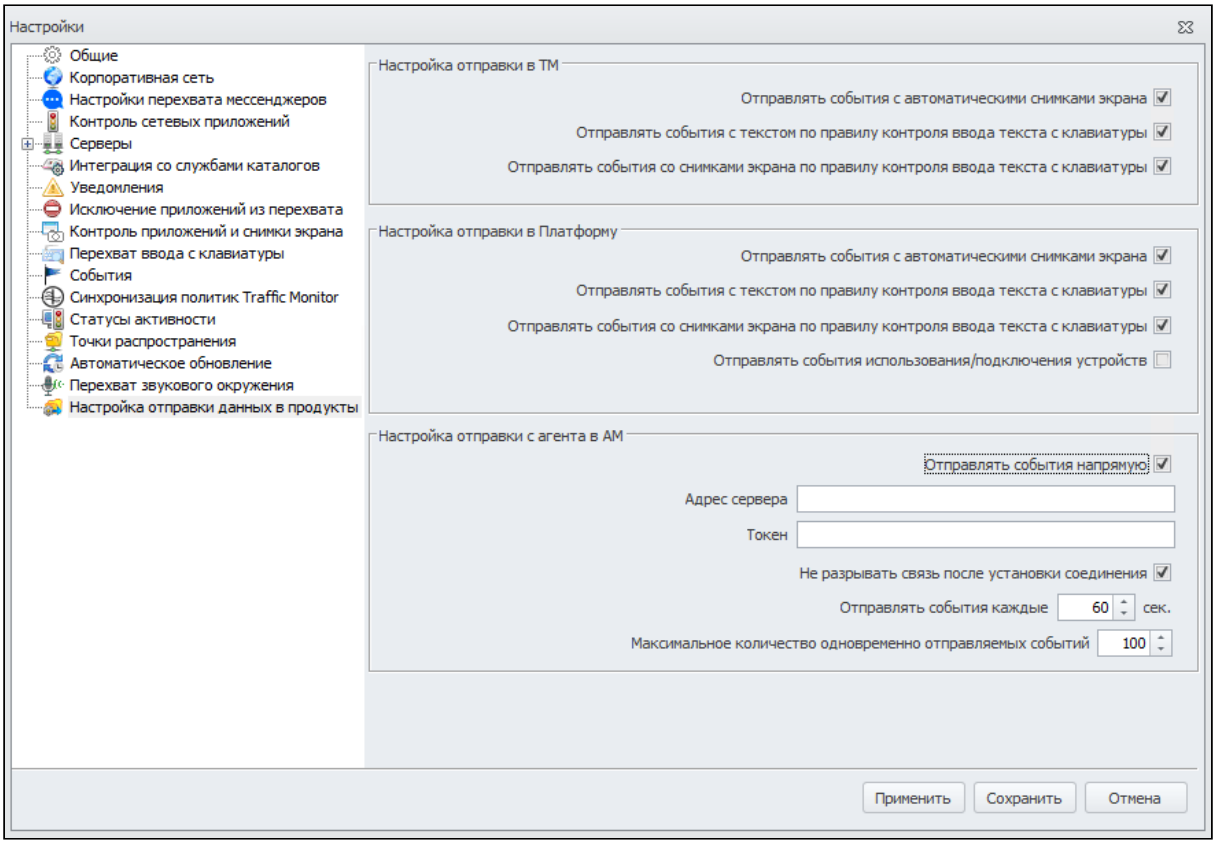
Обработка снимков экрана настраивается в правилах автоматического создания снимков экрана (Правило для ScreenShot Monitor) и контроля текста с клавиатуры (Правило для Keyboard Monitor).

Контроль использования/подключения устройств настраивается в Правиле для Device Monitor.

Дополнительно вы можете настроить отправку данных в продукты InfoWatch. На вкладке **Настройки** вы можете указать, в какие продукты необходимо отправлять данные.

Для этого:

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



3. В области **Настройка отправки в ТМ** снимите флаг, если вы не хотите:
   - **Отправлять события с автоматическими снимками экрана** (настройка контроля событий производится в Правиле для ScreenShot Monitor);
   - **Отправлять события с текстом по правилу контроля ввода текста с клавиатуры** (настройка контроля событий производится в Правиле для Keyboard Monitor);
   - **Отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры** (настройка контроля событий производится в Правиле для Keyboard Monitor).
4. В области **Настройка отправки в Платформу** снимите флаг, если вы не хотите:
   - **Отправлять события с автоматическими снимками экрана** (настройка контроля событий производится в Правиле для ScreenShot Monitor);
   - **Отправлять события с текстом по правилу контроля ввода текста с клавиатуры** (настройка контроля событий производится в Правиле для Keyboard Monitor);
   - **Отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры** (настройка контроля событий производится в Правиле для Keyboard Monitor).
5. В области **Настройка отправки в Платформу** снимите флаг, если вы не хотите:
   - **Отправлять события использования/подключения устройств** (настройка контроля событий производится в Правиле для Device Monitor)
6. В области **Настройка отправки с агента в АМ** установите флаг, если вы хотите:
   - **Отправлять события напрямую**;

Важно!

Настройка **Отправлять события напрямую** применяется только для событий активности пользователя (например, работа в приложениях и на веб-сайтах, ввод текста с клавиатуры, использование мыши и пр.).

При включении отправки событий напрямую необходимо изменить эту настройку одновременно (в течение короткого времени) **на всех** серверах DM, данные с которых передаются на сервер Activity Monitor. Также не рекомендуется менять настройку впоследствии. В противном случае, формирование статистики будет некорректным.

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

- Укажите значения параметров:
  - **Адрес сервера Activity Monitor** (в формате "xxx.xxx.xxx.xxx", например: 193.156.2.76);
  - **Токен Activity Monitor** (см. "Настройки сервера Device Monitor. Соединение с сервером Платформы").
- Снимите флаг **Не разрывать связь после установки соединения**, если хотите, чтобы система разрывала связь между агентом и платформой после установки соединения. Доступно только при включенной настройке **Отправлять события напрямую**;
- Укажите:
  - периодичность отправки событий (в секундах);
  - максимальное количество одновременно отправляемых событий.

Данные параметры доступны только при включенной настройке **Отправлять события напрямую**.

Важно!

Начиная с версии Device Monitor 7.15, по умолчанию включена отправка событий использования/подключения устройств. При этом, при обновлении на версию Device Monitor 7.15 и более новые сохраняется значение настройки **Отправлять события использования/подключения устройств**. То есть, если до обновления было выбрано значение "не отправлять", то после обновления на версию 7.15 и более новые события также не будут отправляться.

Для того, чтобы события отправлялись в Платформу и снимки экрана отображались в InfoWatch Activity Monitor, настройте правило сбора статистики (Правило для Statistics).

7. Нажмите **Применить**, затем **Сохранить**.

Пример

1. На рабочей станции настроено правило *Контроля ввода текста с клавиатуры*, в рамках которого включена опция **Создавать снимок экрана при создании события**.
2. Также настроено правило сбора статистики. Параметр **Контролировать активность** активирован. Для него указано значение **Собирать**.

3. Заданы настройки:
    - **Настройка отправки в ТМ** – 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 Платформу** – отправлять события напрямую в AM.
4. 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.

> **Важно!**
>
> Для того, чтобы события использования/подключения устройств отображались в InfoWatch Activity Monitor:
>
> - В Общих настройках работы Агентов для параметра "**Логировать события от перехватчика устройств и облачных хранилищ**" задайте значение "**Логировать всегда**" или "**При отказе в доступе**"
> - Настройте Правило для Device Monitor

Вы также можете добавить отображение настройки **Отправлять белые списки устройств** (по умолчанию данная настройка не отображается). Чтобы настроить отображение:

1. Откройте файл конфигурации Консоли DeviceMonitor `InfoWatch.DeviceMonitor.Gui.exe.config.`
2. Для параметра `ShowSendWhiteListToEpSettings` задайте значение `True` (по умолчанию параметр имеет значение `False`).

> **Важно!**
>
> Экспорт и импорт данных настроек не поддерживается.
>
> При обновлении Device Monitor настройки, заданные в конфигурационном файле Консоли управления Device Monitor, не сохраняются.

4.3.22 Инженерные настройки агента

Вы можете настроить включение/отключение некоторых настроек агента. По умолчанию узел не отображается.

Чтобы включить настройку:

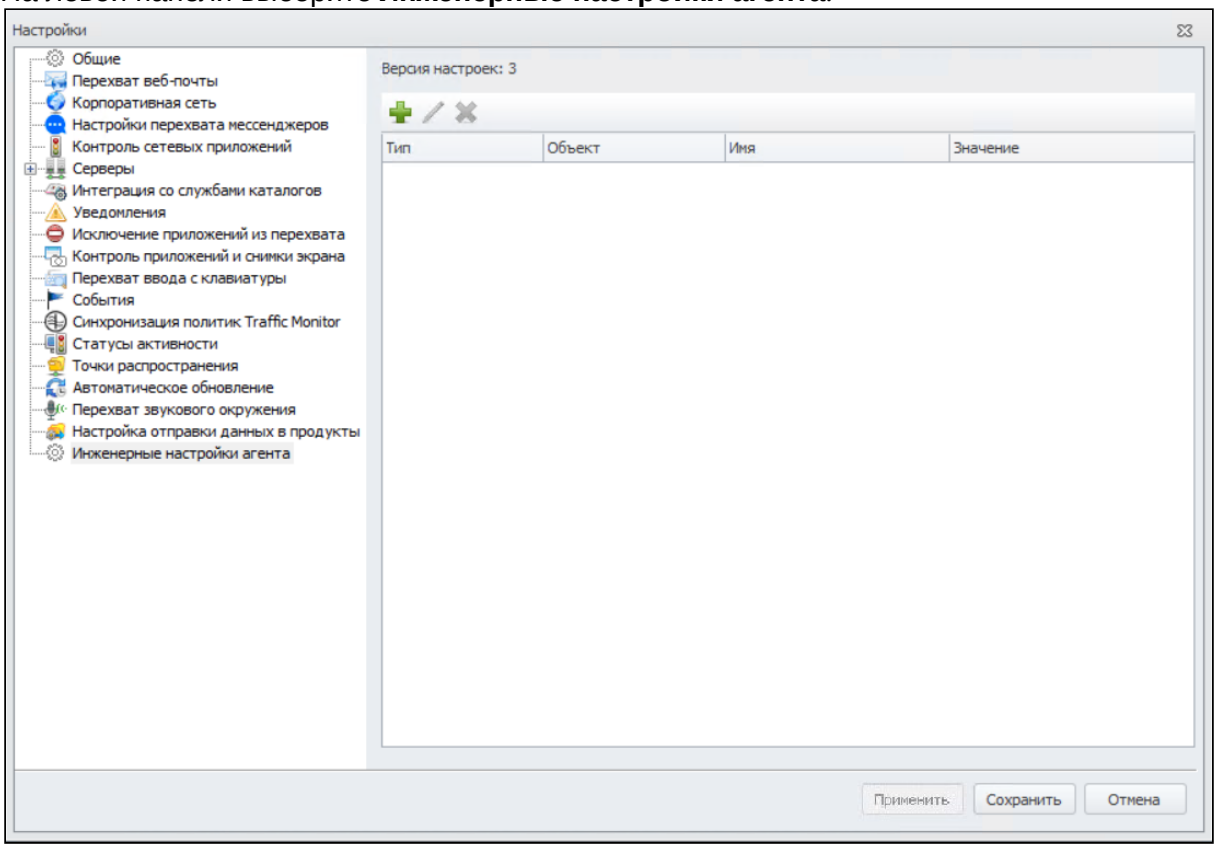
1. Откройте файл конфигурации Консоли Device Monitor `InfoWatch.DeviceMonitor.Gui.exe.config`.
2. В секции `<InfoWatch.DeviceMonitor.Gui.Properties.Settings>` (блок `<applicationSettings>`) вставьте строки:

```
<setting name="ShowAgentGenericSettings" serializeAs="String">
  <value>True</value>
</setting>
```

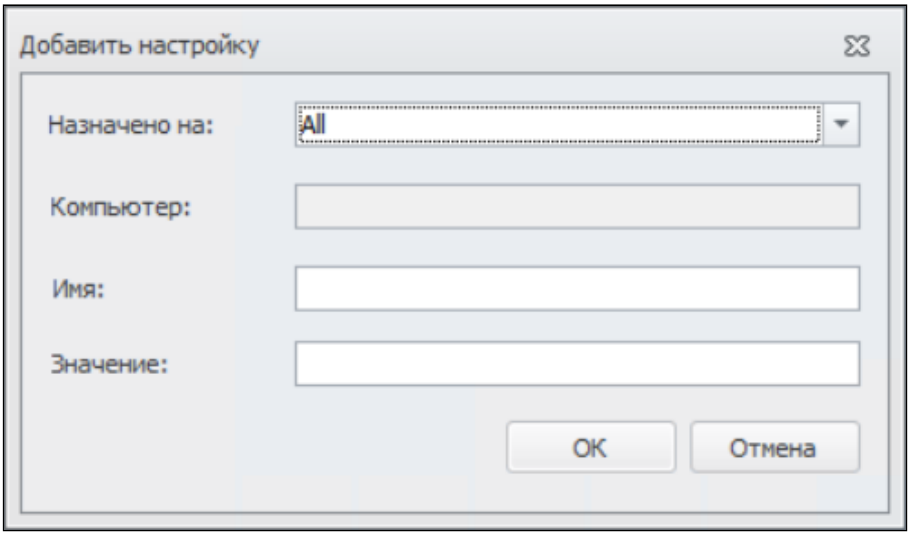
3. Сохраните изменения и перезапустите Консоль управления.

Чтобы добавить настройку:

1. В главном меню выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Инженерные настройки агента**.



3. В верхней области окна нажмите . Откроется диалоговое окно для ввода параметров:



a. В поле **Назначено на** выберите параметр из списка:
   - **All** – настройка будет назначена на все компьютеры;
   - **Workstation** – настройка будет назначена на выбранный далее компьютер.

b. Если выбрали параметр **Workstation**, то в поле **Компьютер** введите значение компьютера, к которому будет применяться настройка.

c. В поле **Имя** введите наименование настройки Системы (доступные настройки см ниже).

d. В поле **Значение** введите значение настройки Системы (доступные значения для настроек см. ниже).

4. Нажмите **OK**.

Чтобы отредактировать настройку:

1. Выберите ее в списке и нажмите .
2. В окне редактирования внесите правки и нажмите **OK**.

Чтобы удалить настройку:

1. Выберите ее в списке и нажмите .
2. В открывшемся окне подтвердите удаление, нажав **Да**.

Настройки агента

Настройки для прокси

Наименование настройки	Значение настройки	Описание
proxy.enable_connection_check_ipv4	true/false	Необходимость проверки доступности соединения с конечной точкой перед перенаправлением для IPv4-соединения
proxy.enable_connection_check_ipv6	true/false	Необходимость проверки доступности соединения с конечной точкой перед перенаправлением для IPv6-соединения

Наименование настройки	Значение настройки	Описание
proxy.block_unavailable_connection_ipv4	true/false	Блокировка недоступной конечной точки (IPv4) после проверки
proxy.block_unavailable_connection_ipv6	true/false	Блокировка недоступной конечной точки (IPv6) после проверки

Настройки IFilter

Наименование настройки	Значение настройки	Описание
tm.text_extractor.ifilter.enabled	1/0	Использование модуля IFilter на Агентах Device Monitor. По умолчанию настройка включена. Если значение настройки равно "1", то IFilter включен

Настройки звукового перехвата

Наименование настройки	Значение настройки	Описание
Перехват устройств типа "Микрофон"		
am.mic.frequency_searching_devices_sec	Задается в секундах	Период поиска доступных устройств. Поиск выполняется каждые N секунд, где N – значение настройки. При значении 0 повторный поиск не производится
am.mic.timeout_restart_capture_sec	Задается в секундах	Время ожидания после сбоя захвата устройства перед новой попыткой. При значении 0 повторная попытка захвата не производится
am.mic.reselect_source_if_data_missing_msec	Задается в миллисекундах	Время, через которое запускается повторный выбор источника звука, если отсутствуют данные с текущего источника. Значение по умолчанию: 100 мс
Перехват устройств типа "Аудиоколонки"		
am.speaks.frequency_searching_devices_sec	Задается в секундах	Период поиска доступных устройств. Поиск выполняется каждые N секунд, где N – значение настройки. При значении 0 повторный поиск не производится

Наименование настройки	Значение настройки	Описание
am.speaks.timeout_restart_capture_sec	Задается в секундах	Время ожидания после сбоя захвата устройства перед новой попыткой. При значении 0 повторная попытка захвата не производится
am.speaks.reselect_source_if_data_missing_msec	Задается в миллисекундах	Время, через которое запускается повторный выбор источника звука, если отсутствуют данные с текущего источника. Значение по умолчанию: 100 мс

Настройка выбора доступного агенту сервера

Наименование настройки	Значение настройки	Описание
server_choosing.check_connection_sec	Задается в секундах	Выявление доступных агенту серверов из пула и случайный выбор одного из них для передачи данных. Поиск выполняется N секунд, где N – значение настройки. Значение по умолчанию: 10 с. При значении 0 настройка выключена

Настройка Telegram

Наименование настройки	Значение настройки	Описание
im.max_accumulation_time_of_chat_participants_sec	Задается в секундах	Выявление активности участников группового чата в течение N времени, где N – значение настройки. При обнаружении неактивного участника Система исключает его из состава группового чата. Значение по умолчанию: 604 800 с (7 дней). При значении 0 настройка выключена

4.4 Управление схемой безопасности

Информация о схеме безопасности InfoWatch Device Monitor, а также порядок управления этой схемой описаны в следующих разделах:

- Организация схемы безопасности
- Общие действия при управлении схемой безопасности
- Настройка схемы безопасности
- Временный доступ сотрудника к сети
- Временный доступ сотрудника к устройствам

4.4.1 Организация схемы безопасности

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

В набор параметров схемы безопасности входят:

- **Политики безопасности** с заданным для каждой политики безопасности набором правил.
- **Группы сотрудников**, зарегистрированных в Device Monitor. Каждой группе сотрудников должна быть назначена политика безопасности.
- **Группы компьютеров**. Каждой группе компьютеров должна быть назначена политика безопасности.
- **Белые списки устройств**, доступ к которым безусловно разрешен.
- **Категории сигнатур**, с помощью которых правила File Monitor могут распространяться на заданные форматы файлов.

> **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. При помощи Консоли управления вы можете просмотреть политики и содержащиеся в них правила любой версии схемы безопасности.

Далее в подразделе содержится следующая информация:

- Политики безопасности и правила
- Сотрудники и группы сотрудников
- Компьютеры и группы компьютеров
- Загрузка схемы безопасности на контролируемые компьютеры

Политики безопасности и правила

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.

Назначение политики безопасности группе сотрудников или группе компьютеров происходит в соответствии со следующими принципами:

- Каждой группе сотрудников и каждой группе компьютеров обязательно должна быть назначена политика безопасности.
  Добавление новой группы сотрудников или новой группы компьютеров невозможно, если для данной группы не определена политика безопасности. В процессе назначения политики безопасности группе сотрудников или группе компьютеров выбор

осуществляется из ранее созданных политик безопасности. Поэтому нужная политика безопасности должна быть создана перед добавлением соответствующей группы;
- Группе сотрудников или группе компьютеров не может быть назначено более одной политики безопасности;
- Одна и та же политика безопасности может быть назначена нескольким группам сотрудников или группам компьютеров, однако рекомендуется, чтобы каждой группе сотрудников и группе компьютеров была назначена своя политика безопасности.

> **Примечание:**
>
> Политика безопасности, назначенная хотя бы одной группе сотрудников или группе компьютеров, не может быть удалена из схемы безопасности.

Учетная запись сотрудника, впервые зарегистрированного в Device Monitor, автоматически включается в группу сотрудников «по умолчанию». Поэтому первоначально для каждого нового сотрудника уровень доступа будет определяться политикой безопасности, назначенной группе сотрудников «по умолчанию», а также политиками безопасности, назначенными группам компьютеров, в состав которых включен компьютер, на котором работает данный сотрудник. Впоследствии можно изменять уровень доступа путем включения сотрудника в различные группы сотрудников.

> **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; определяется уровень доступа к контролируемым периферийным устройствам. Для каждой политики безопасности создается свой набор правил.

Все правила имеют определенный срок действия, по истечении которого работа правила прекращается.

В InfoWatch Device Monitor существуют следующие типы правил:

- **Правило для Application Monitor**. Позволяет контролировать доступ сотрудников к приложениям при помощи черных и белых списков путем наложения запрета на:
  - запуск приложений;
  - буфер обмена;
  - печать.
- **Правило для Audio Record Control**. Позволяет отслеживать действия сотрудника при помощи контроля звукового окружения рабочей станции сотрудника.
- **Правило для Clipboard Monitor**. Позволяет контролировать вставку данных из буфера обмена. Система позволяет запрещать вставку данных в приложения из списка либо все операции вставки данных в приложения терминальной сессии.
- **Правило для Cloud Storage Monitor**. Позволяет контролировать веб-клиенты облачных хранилищ.
- **Правило для Device Monitor**. Позволяет контролировать доступ сотрудников к выбранному типу периферийных устройств.

- **Правило для File Monitor**. Позволяет отслеживать следующие действия с файлами на съемных и сетевых ресурсах:
  - копирование файла с сетевых устройств на рабочую станцию;
  - копирование файла на сетевые ресурсы с использованием UNC (например, *Server**SharedFolder**Folder**File*);
  - копирование файла со съемных устройств на рабочую станцию;
  - 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;
  - редактирование файла непосредственно на съемном устройстве, в том числе переименование;
  - копирование файла на медиа-устройства, использующие для подключения протокол MTP;
  - копирование файла в приложение терминальной сессии;
  - копирование файла с ресурсов, подключенных через терминальную сессию, на рабочую станцию;
  - копирование файла на ресурсы, подключенные через терминальную сессию. Поддерживается перенаправление для сетевых папок и виртуальных устройств.
- **Правило для File Operations Monitor**. Позволяет контролировать чтение и запись файла приложением. Также возможно создавать теневую копию файла и снимок экрана.
- **Правило для FTP Monitor**. Позволяет контролировать обмен данными по протоколу FTP/FTPS. Система позволяет ограничивать или полностью запрещать использование протокола FTP/FTPS, а также создавать теневые копии передаваемых файлов.
- **Правило для HTTP(S) Monitor**. Позволяет контролировать обмен данными по протоколам HTTP и HTTPS. Система позволяет создавать теневые копии передаваемых файлов.
- **Правило для IM Client Monitor**. Позволяет контролировать доступ сотрудников к клиентам мгновенного обмена сообщениями и протоколам передачи данных: Skype, Telegram, XMPP, MMP, Facebook, WhatsApp, VK (ВКонтакте). Система позволяет полностью запрещать использование приложения, либо только снимать копию чата. Для Skype возможно делать запись голосовых сообщений. Также возможно создавать теневые копии передаваемых файлов и сообщений.
- **Правило для Keyboard Monitor**. Позволяет перехватывать ввод текста с клавиатуры на рабочих станциях и создавать события:
  - при смене активного окна или вкладок в браузере;
  - по истечении временного интервала, указанного в настройках, с момента окончания ввода;
  - при накоплении заданного в настройках количества символов, введенных с клавиатуры;
  - при нажатии Enter / Ctrl+Enter / Shift+Enter, если это указано в настройках (см. "Контроль ввода с клавиатуры").
- **Правило для Mail Monitor**. 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.
- **Правило для Network Monitor**. Позволяет запрещать передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными

разрешенными серверами. Вы можете указать, какие сегменты сети считаются корпоративной сетью и какие внешние адреса разрешены.

- **Правило для Print Monitor**. Позволяет отслеживать действия, связанные с печатью документов на локальных и сетевых принтерах.
- **Правило для ScreenShot Monitor**. Позволяет автоматически создавать снимки экрана на контролируемых компьютерах.
- **Правило для ScreenShot Control Monitor**. Позволяет контролировать снимки экрана со стороны Агента.
- **Правило для Statistics**. Позволяет собирать статистику об активности пользователя и действиях с файлами/папками на контролируемых компьютерах:
  - вход в сессию, выход из сессии (локальный, удаленный);
  - блокировка/разблокировка сессии (локальная, удаленная);
  - запуск/остановка приложения;
  - получение/потеря фокуса активного окна приложения;
  - получение фокуса вкладкой браузера. Сбор статистики по работе с сайтами поддерживается для браузеров Chrome, Яндекс.Браузер, Mozilla Firefox, Edge (Chromium), Opera, IExplore;
  - выполнение поисковых запросов. Поддерживается для поисковых систем Google и Яндекс;
  - использование мыши и клавиатуры.

Примечание:

Если для одного сотрудника или компьютера задано несколько правил, то применяется результирующая политика, которая складывается из всех правил, заданных для сотрудника или компьютера. Подробнее об определении приоритета правил см. "Применение правил".

Важно!

Не рекомендуется добавлять действия по умолчанию в политику защиты данных на Агенте при наличии правила на маршрут *Любой отправитель – Любой получатель*. Это связано с тем, что если в политике присутствует настроенное правило с разрешающим вердиктом и предустановленное правило (по умолчанию) с блокирующим вердиктом, то при одинаковом весе правил применяются действия по умолчанию.

Важно!

Для корректного перехвата сервисов Google (Gmail, Google Drive и пр.) рекомендуется отключить в Google Chrome использование экспериментального протокола QUIC. Подробнее см. в статье базы знаний "Отключение протокола QUIC в Google Chrome".

Для каждого правила определен список операционных систем, на которых оно может применяться. Особенности применения правила на Агенте также зависят от используемой операционной системы. Подробнее об особенностях применения правил смотрите в подразделе "Правила".

Сотрудники и группы сотрудников

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:
  - **Теневое копирование документов**. Правило File Monitor, задающее создание теневых копий всех файлов, записываемых на съемные устройства и копируемых на сетевые ресурсы.
  - **Теневое копирование печати**. Правило Print Monitor, задающее создание теневых копий всех заданий на печать.
  - **Контроль Telegram, Facebook, WhatsApp, Контроль XMPP, Контроль MMP**. Правила IM Client Monitor, разрешающие использование соответствующих мессенджеров, но задающие создание теневых копий для всех сообщений и чатов, а также исходящих файлов.
  - **Контроль FTP**. Правило FTP Monitor, разрешающее использование протокола FTP/FTPS, но задающее создание теневых копий для всех файлов, отправляемых с использованием этого протокола.
  - **Контроль HTTPS**. Правило HTTP(S) Monitor, создающее событие для пост-запросов всегда, вне зависимости от их размера, если передача производится по зашифрованному каналу. Теневая копия создается, если размер запроса, передаваемого по зашифрованному каналу, находится в диапазоне от 40 Б до 40 МБ.
  - **Контроль системы передачи почтовых сообщений**. Правило Mail Monitor, разрешающее отправку и получение почты и задающее создание теневых копий для исходящих по зашифрованному каналу писем, если их размер не превышает 40 МБ.

Компьютеры и группы компьютеров

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

> **Примечание:**
>
> В поле **Пользователь**, на вкладке **Группы компьютеров**, отображается имя пользователя, который последним заходил на компьютер.
>
> Пользователь не отображается для рабочих станций под управлением Linux.

В группу «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 группе компьютеров «по умолчанию» назначена *Политика на устройства*. Эта политика не содержит ни одного правила.

Исключить компьютер из группы «по умолчанию» можно при условии, что компьютер добавлен хотя бы в одну группу компьютеров, помимо группы «по умолчанию».

Загрузка схемы безопасности на контролируемые компьютеры

Схема безопасности, загруженная на контролируемые компьютеры, должна находиться в актуальном состоянии. Это обеспечивается взаимодействием Сервера и Агентов, установленных на контролируемых компьютерах.

Процесс передачи схемы безопасности на контролируемые компьютеры выполняется Сервером автоматически в следующих случаях:

- после сохранения созданной или отредактированной схемы безопасности;
- если зарегистрирован сотрудник, для которого не определен уровень доступа в текущей версии схемы безопасности. Такой сотрудник автоматически включается в группу сотрудников «по умолчанию», а затем схема безопасности обновляется.

При отключении контролируемого компьютера от сети, где развернута система InfoWatch Device Monitor, действие политик будет продолжаться, но их обновление происходить не будет, а теневые копии будут копиться на компьютере. После соединения контролируемого компьютера с сервером InfoWatch Device Monitor, на нем будут актуализированы политики, а сохраненные теневые копии будут переданы на сервер.

4.4.2 Общие действия при управлении схемой безопасности

Информация по работе со схемой безопасности содержится в следующих подразделах:

- Просмотр действующей версии схемы безопасности
- Просмотр предыдущих версий схемы безопасности
- Комментарии к схеме безопасности
- Редактирование схемы безопасности
- Обновление схемы безопасности
- Экспорт/импорт конфигурации

Общие сведения о схеме безопасности содержатся в разделе "Организация схемы безопасности".

Настройка конфигурационных параметров схемы безопасности описывается в разделе "Настройка схемы безопасности".

Просмотр действующей версии схемы безопасности

По умолчанию в Консоли управления отображается та версия схемы безопасности, которая действует на данный момент.

Информация о настройках схемы безопасности отображается в разделах **Политики**, **Группы сотрудников**, **Группы компьютеров**, **Белые списки** и **Категории сигнатур** (см. "Разделы Консоли управления").

Конфигурационные параметры схемы безопасности отображаются в виде групп элементов. Список групп элементов, входящих в выбранный раздел, отображается в области просмотра на Панели навигации. С каждой группой элементов сопоставлена определенная пиктограмма (см. таблицу).

Пиктограмма	Группа элементов
	Группа компьютеров «по умолчанию»
	Группа компьютеров
	Группа сотрудников «по умолчанию»
	Группа сотрудников
	Категория сигнатур «по умолчанию»
	Категория сигнатур
	Белый список устройств для сотрудника
	Белый список устройств для группы сотрудников
	Белый список устройств для компьютера
	Белый список устройств для группы компьютеров
	Фильтр в журнале аудита
	Политика безопасности

Чтобы просмотреть информацию по определенному разделу схемы безопасности:

1. Откройте нужный раздел (см. "Разделы Консоли управления"). Список групп элементов, входящих в данный раздел, будет выведен на Панели навигации.
2. На Панели навигации выберите название группы элементов, по которой вам нужно получить дополнительную информацию. В результате все элементы выбранной группы будут отображены в рабочей области главного окна.
3. Чтобы просмотреть подробную информацию по отдельному элементу группы, щелкните левой кнопкой мыши по строке с названием нужного элемента. После этого на панели **Подробно** будет отображена таблица свойств выбранного элемента.

Примечание.

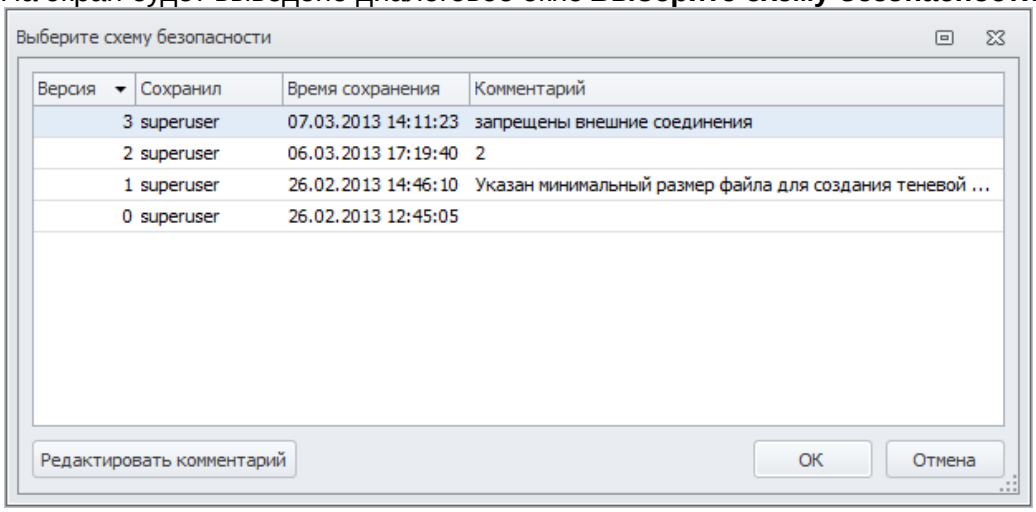
В процессе работы вы можете настраивать отображение элементов главного окна по своему усмотрению (см. "Настройка элементов главного окна").

Просмотр предыдущих версий схемы безопасности

> **Примечание.**
>
> В процессе редактирования схемы безопасности просматривать предыдущие версии без потери внесенных изменений невозможно.

Чтобы просмотреть раннюю версию схемы безопасности:

1. В главном меню выберите команду **Схема безопасности** > **Выбрать схему для просмотра**.
   На экран будет выведено диалоговое окно **Выберите схему безопасности**.



   По каждой версии выводится следующая информация:
   - **Версия**. Номер версии схемы безопасности.
   - **Сохранил**. Имя учетной записи того пользователя, который сохранил данную версию.
   - **Время сохранения**. Дата и время сохранения версии.
   - **Комментарий**. Дополнительная информация о схеме безопасности.

   > **Примечание.**
   >
   > В окне выбора схемы безопасности вы можете отредактировать комментарий к любой версии схемы безопасности (см. "Комментарии к схеме безопасности"). Информация о схеме безопасности (номер версии и комментарий), которая загружена в Консоль управления на данный момент, отображается на панели статуса.

2. В диалоговом окне **Выберите схему безопасности** выберите строку с номером той версии схемы безопасности, которую нужно просмотреть.
3. Нажмите **ОК**.

В Консоль управления будут загружены политики и содержащиеся в них правила для выбранной версии схемы безопасности. При работе со старой версией в строке состояния указывается: "*Старая схема безопасности*".

Чтобы вернуться к просмотру и работе с активной схемой безопасности, в главном меню выберите команду **Схема безопасности** > **Просмотреть последнюю схему**.

Комментарии к схеме безопасности

Вы можете указывать дополнительную информацию по схеме безопасности в виде комментария. Комментариями может сопровождаться каждая версия схемы безопасности.

Комментарий к текущей схеме безопасности выводится на панели статуса, в скобках справа от номера версии схемы безопасности.

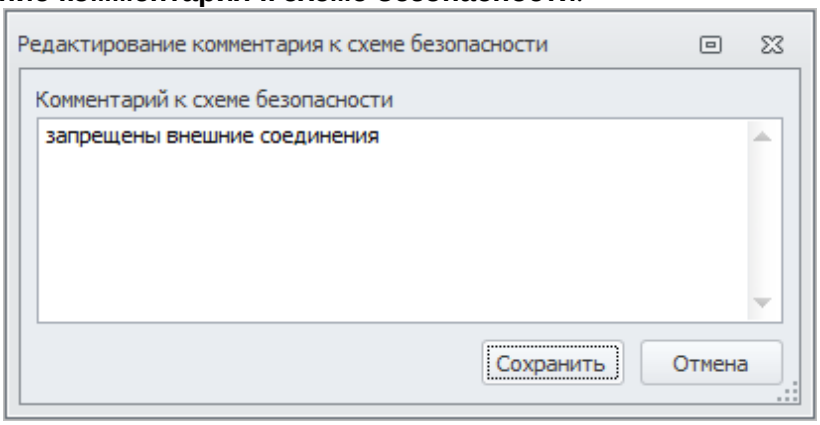
Комментарии ко всем версиям схемы безопасности можно просмотреть в диалоговом окне **Выберите схему безопасности** (см. раздел "Просмотр предыдущих версий схемы безопасности").

> **Примечание:**
>
> Комментарий к текущей схеме безопасности можно добавлять вне зависимости от состояния схемы безопасности (редактируется/не редактируется).

Чтобы добавить/отредактировать комментарий к схеме безопасности:

1. Выполните одно из следующих действий:
   - *(Только для текущей схемы безопасности)*. В главном меню выберите команду **Схема безопасности** > **Изменить комментарий текущей схемы**.
   - *(Для любой версии схемы безопасности, кроме текущей)*. В главном меню выберите команду **Схема безопасности** > **Выбрать схему для просмотра**. На экран будет выведено диалоговое окно **Выберите схему безопасности**. В этом окне выберите строку с нужной версией схемы безопасности. Затем нажмите **Редактировать комментарий**.

   После выполнения любого из этих действий на экран будет выведено диалоговое окно **Редактирование комментария к схеме безопасности**.



2. В открывшемся диалоговом окне введите текст комментария.
3. Нажмите **Сохранить**.

Редактирование схемы безопасности

> **Важно!**

В каждый момент схема безопасности может редактироваться только одним пользователем. Если схема безопасности редактируется, информация о редактирующем пользователе и компьютере, где это происходит, отображается на строке, выделенной красным и расположенной в верхней части главного окна. Подробнее см. "Ожидание окончания редактирования. Разблокирование схемы безопасности".

Все операции, связанные с изменением схемы безопасности, выполняются в режиме редактирования. Данный режим используется для защиты существующей схемы безопасности от возможных ошибок в ходе редактирования. Система переходит в режим редактирования автоматически, после того, как любой из пользователей Консоли управления выполняет любые изменения параметров схемы безопасности. Все изменения сохраняются только после команды Сохранить схему безопасности.

Если в процессе редактирования схемы безопасности соединение с сервером было прервано, то все несохраненные изменения будут утеряны.

Чтобы отредактировать схему безопасности:

1. Выполните одно из следующих действий:
   - в главном меню выберите команду **Схема безопасности** > **Редактировать**;
   - воспользуйтесь кнопкой **Редактировать**, расположенной на панели инструментов;
   - выполните любое изменение параметров схемы безопасности (политики безопасности, компьютеры, учетные записи сотрудников, белые списки устройств, категории сигнатур).
     После выполнения любого из этих действий схема безопасности будет переведена в режим редактирования.

     Примечание:

     Редактировать можно только последнюю версию схемы безопасности. Поэтому редактирование схемы безопасности недоступно в режиме просмотра предыдущих версий. Чтобы перейти к текущей версии схемы безопасности, воспользуйтесь командой **Схема безопасности** > **Просмотреть последнюю схему** из главного меню.
     Информация о том, какая схема безопасности загружена в Консоль управления на данный момент, выводится на панели статуса.

2. Отредактируйте необходимые параметры схемы безопасности:
   - политики безопасности (см. "Политики безопасности");
   - группы компьютеров (см. "Компьютеры");
   - группы учетных записей сотрудников (см. "Сотрудники");
   - белые списки устройств (см "Белые списки")
   - категории сигнатур файлов (см. "Категории сигнатур").
3. После того как все необходимые изменения будут сделаны, сохраните схему безопасности. Для этого выполните одно из следующих действий:
   - в верхней строке рабочей области, где отображается сообщение "*В схему безопасности были внесены изменения...*" нажмите **Сохранить**;
   - в главном меню выберите команду **Схема безопасности** > **Сохранить**;

- воспользуйтесь кнопкой **Сохранить**, расположенной на панели инструментов.

В результате выполнения любого из этих действий все изменения будут сохранены, и схема безопасности будет выведена из режима редактирования.

Примечание:

Чтобы отменить внесенные изменения:

- в верхней строке рабочей области, где отображается сообщение "*В схему безопасности были внесены изменения...*" нажмите **Отмена**;
- в главном меню выберите команду **Схема безопасности** > **Отменить редактирование**;
- воспользуйтесь кнопкой **Отменить редактирование**, расположенной на панели инструментов.

После этого схема безопасности будет выведена из режима редактирования с потерей всех изменений.

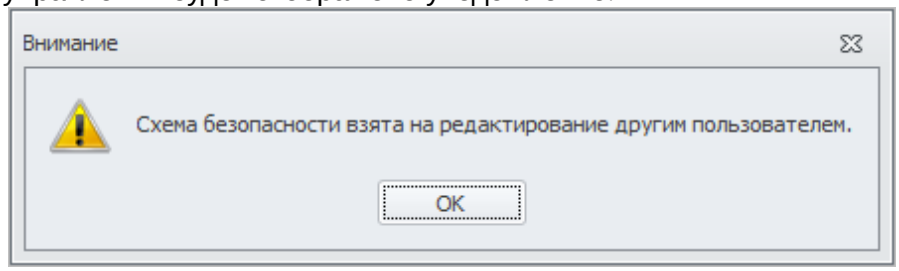
Ожидание окончания редактирования. Разблокирование схемы безопасности

В каждый момент схема безопасности может редактироваться только одним пользователем. Внесенные изменения фиксируются только после сохранения схемы безопасности.

Если схема безопасности уже редактируется другим пользователем, информация об этом отображается на панели в верхней части главного окна.

Если схема редактируется другим пользователем, то при попытке изменить какие-либо параметры схемы (политики безопасности, компьютеры, сотрудники, белые списки устройств, категории сигнатур):

1. В Консоли управления будет отображено уведомление.



2. После того как другой пользователь сохранит или отменит изменения, в области уведомлений панели задач Windows появится всплывающее уведомление: "***Схема свободна для редактирования***".

Информация о том, кто в настоящее время редактирует схему, отображается на панели, расположенной в верхней части главного окна, а также в строке статуса.

В ходе работы может возникнуть ситуация, когда ни один из пользователей не редактирует схему безопасности, но схема безопасности находится в заблокированном состоянии (редактируется). Такое возможно, если процесс редактирования схемы безопасности был завершен некорректно (например, при потере соединения с сервером).

Когда пользователь, заблокировавший схему, опять подключится к серверу, схема безопасности будет автоматически разблокирована, а все несохраненные изменения, сделанные этим пользователем, будут утеряны.

Также для разрешения данной проблемы предусмотрена специальная функция – разблокирование схемы безопасности.

Важно!

Разблокировать схему безопасности может только Суперпользователь.

Чтобы разблокировать схему безопасности, в главном меню выберите команду **Схема безопасности** > **Разблокировать**.

При этом все несохраненные изменения схемы безопасности будут утеряны.

Обновление схемы безопасности

В Системе могут работать одновременно несколько пользователей. Для того чтобы поддерживать в актуальном состоянии сведения о схеме безопасности, отображаемые в Консоли управления, необходимо периодически выполнять операцию обновления. Обновление схемы безопасности выполняется автоматически (в процессе подключения к Серверу) или вручную (при работе с Консолью управления).

Необходимость в обновлении схемы безопасности может потребоваться в следующих случаях:

- зарегистрирован новый компьютер;
- зарегистрирован сотрудник, о котором нет информации в схеме безопасности;
- схема безопасности была изменена.

Чтобы вручную обновить схему безопасности, выполните одно из следующих действий:

- в главном меню выберите команду **Вид** > **Обновить**;
- воспользуйтесь кнопкой **Обновить**, расположенной на панели инструментов;
- нажмите F5.

Экспорт/импорт конфигурации

Текущие настройки конфигурации можно сохранить в виде файла. Сохраненный файл можно использовать, например, для быстрой настройки сервера Device Monitor после его переустановки или при разворачивании новых серверов Device Monitor.

Функция экспорта конфигурации дает возможность сохранить в виде файла специального формата (*.dmc) текущую версию схемы безопасности, включая:

- **Схема безопасности** (включая политики безопасности с наборами правил, группы сотрудников и компьютеров, категории сигнатур, списки ресурсов) (см. "Управление схемой безопасности")
- **Протокол приложений** (см. "Приложения")
- **Настройки контроля сети** (см. "Контроль сетевых соединений")
- **Список исключенных из анализа серверов** (см. "Контроль сетевого трафика")
- **Список исключенных из перехвата приложений** (см. "Исключение приложений из перехвата")
- **Список точек распространения** (см. "Настройка распространения Агентов")
- **Настройки автоматического обновления** (см. "Автоматическое обновление Агентов")
- **Пользователи и роли** (см. "Управление учетными записями и ролями Консоли управления").

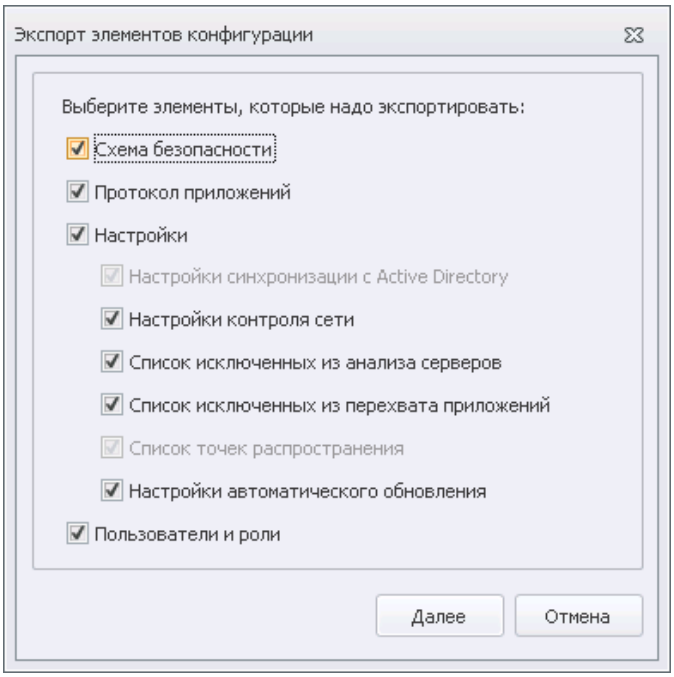
Важно!

В Систему версии 7.2 можно импортировать файл конфигурации только данной версии.

Впоследствии сохраненные настройки могут быть импортированы в новую схему безопасности.

Чтобы экспортировать конфигурацию Системы:

1. В главном меню выберите команду **Инструменты** > **Экспорт конфигурации**.
2. В открывшемся диалоговом окне отметьте элементы конфигурации, которые вы хотите экспортировать.



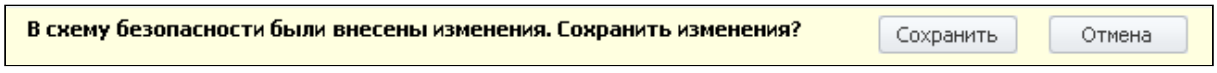
3. Нажмите **Далее**.
4. В окне сохранения файла задайте имя файла, в который будут экспортированы данные, и выберите каталог для его хранения. Нажмите **Сохранить**.

Важно!

Для корректной связки ролей и групп необходимо экспортировать роли и схему безопасности.

Чтобы импортировать схему безопасности:

1. В главном меню выберите команду **Инструменты** > **Импорт конфигурации**.
2. В открывшемся диалоговом окне выберите файл формата *.dmc, в котором хранится сохраненная конфигурация,
3. Нажмите **Открыть**.
4. В окне **Импорт элементов конфигурации** выберите элементы, которые надо импортировать.
5. Нажмите **Далее**.
6. В диалоговом окне с подтверждением импорта нажмите **ОК**.
7. Нажмите **Сохранить** в информационном сообщении.



В результате сохраненные настройки схемы безопасности будут импортированы в действующую схему и добавлены к существующим. Если в текущей схеме безопасности имеются записи с названиями, аналогичными импортируемым, то к названиям импортируемых записей будет добавлена цифра **1**.

> **Примечание:**
>
> Если Агент имеет статус "Золотой образ", то данный статус сохранится при импорте/экспорте конфигурации независимо от схемы безопасности, к которой принадлежит компьютер. Подробнее о статусе "Золотой образ" см. Установка статуса "Золотой образ" на Агенте.
>
> Компьютеры с другими статусами, которые будут импортированы в схему безопасности (то есть новые компьютеры) будут иметь статус Агента **Не установлен**.
>
> Статус Агента компьютеров, которые уже были в схеме, не изменится.

4.4.3 Настройка схемы безопасности

После установки Системы необходимо выполнить настройку конфигурационных параметров схемы безопасности. Конфигурирование схемы безопасности выполняют в такой последовательности:

1. Настройка группы сотрудников «по умолчанию» и группы компьютеров «по умолчанию».
2. Настройка остальных конфигурационных параметров схемы безопасности.

При настройке конфигурационных параметров нужно придерживаться следующих принципов:

- Политику безопасности необходимо создавать перед созданием той группы сотрудников или группы компьютеров, которой будет назначена эта политика безопасности.
- Каждой группе сотрудников и группе компьютеров рекомендуется назначать отдельную политику безопасности.
- Для каждой политики безопасности, которая назначается какой-либо группе, должен быть определен набор правил.

Особенности добавления компьютеров в схему безопасности

Добавление контролируемых компьютеров происходит одним из двух способов:

- автоматически при регистрации нового компьютера;
- вручную через Консоль управления.

Если компьютер зарегистрирован автоматически, то он включается в группу компьютеров «по умолчанию». Затем он может быть добавлена в другие группы компьютеров.

При добавлении вручную, компьютер можно сразу поместить в нужную группу.

Особенности добавления учетных записей сотрудников в схему безопасности

Сведения об учетной записи нового сотрудника могут быть добавлены в схему безопасности либо вручную, либо автоматически. Вручную сотрудника можно зарегистрировать при редактировании схемы безопасности. Однако если на контролируемом компьютере регистрируется сотрудник, о котором нет сведений в схеме безопасности, то учетная запись такого сотрудника будет автоматически добавлена в схему безопасности (группа сотрудников «по умолчанию»).

Особенности добавления белых списков в схему безопасности

Перед созданием белого списка необходимо внести в базу устройств данные о включаемых в него моделях и экземплярах устройств. Затем нужно создать белый список для конкретного сотрудника / группы сотрудников / компьютера / группы компьютеров, и определить, какие устройства в него

включены. Для этих сотрудников / компьютеров доступ к моделям и экземплярам устройств из белого списка разрешен, невзирая на назначенные политики. По окончании периода действия записи в белом списке, доступ к устройству производится согласно назначенным политикам.

Подробная информация о настройке конфигурационных параметров схемы безопасности содержится в подразделах:

- Политики безопасности
- Правила
- Сотрудники
- Компьютеры
- Белые списки
- Категории сигнатур
- Приложения
- Блокада приложений
- Ресурсы
- Файловая статистика
- Исключение мусорного трафика
- Временный доступ сотрудника к сети
- Временный доступ сотрудника к устройствам

Политики безопасности

На агентах Device Monitor политики применяются в следующем порядке:

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

> **Примечание.**
>
> Рекомендации по настройке политик безопасности приводятся в разделе "Политики безопасности и правила".

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

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

Работа с политиками безопасности ведется в разделе **Политики**. Чтобы перейти к этому разделу, воспользуйтесь кнопкой **Политики**, расположенной на Панели навигации, или выберите в главном меню команду **Переход** > **Политики**.

Информация по работе с политиками безопасности содержится в подразделах:

- Просмотр политик безопасности
- Создание и настройка политики безопасности
- Редактирование политики безопасности
- Удаление политики безопасности

Просмотр политик безопасности

В области **Политика** на Панели навигации выводится перечень политик безопасности, определенных для схемы безопасности. В рабочей области главного окна отображается перечень правил для выбранной политики безопасности.

> **Примечание.**
>
> Для более удобного просмотра вы можете настроить отображение списка правил, воспользовавшись дополнительными функциями (подробнее см. "Дополнительные возможности").

Чтобы просмотреть правила, включенные в политику безопасности, выберите название политики безопасности в области **Политика** на Панели навигации.

Правила выводятся в виде табличного списка, где каждая строка соответствует одному правилу. В столбцах отображаются общие свойства правил. Каждому правилу соответствует пиктограмма, изображающая, на что распространяется это правило, а также цветовое обозначение, указывающее на то, является правило разрешающим (зеленый), запрещающим (красный) или частично ограничивающим (желтый).

Расширенная информация по каждому правилу выводится на панели **Подробно**.

Чтобы просмотреть все свойства правила, в рабочей области главного окна выберите строку с названием нужного правила.

После этого на панели **Подробно** будет отображена таблица со сведениями по выбранному правилу.

Для каждого правила отображаются общие сведения, а также дополнительные сведения, характерные для правил выбранного типа.

Общие сведения:

- **Наименование**. Название правила.
- **Политика**. Название политики безопасности, в состав которой входит правило.
- **Перехватчик**. Тип перехватчика, для которого создано правило.
- **Операция**. Операция, контролируемая правилом.
- **Период действия**. Время начала и окончания действия правила.

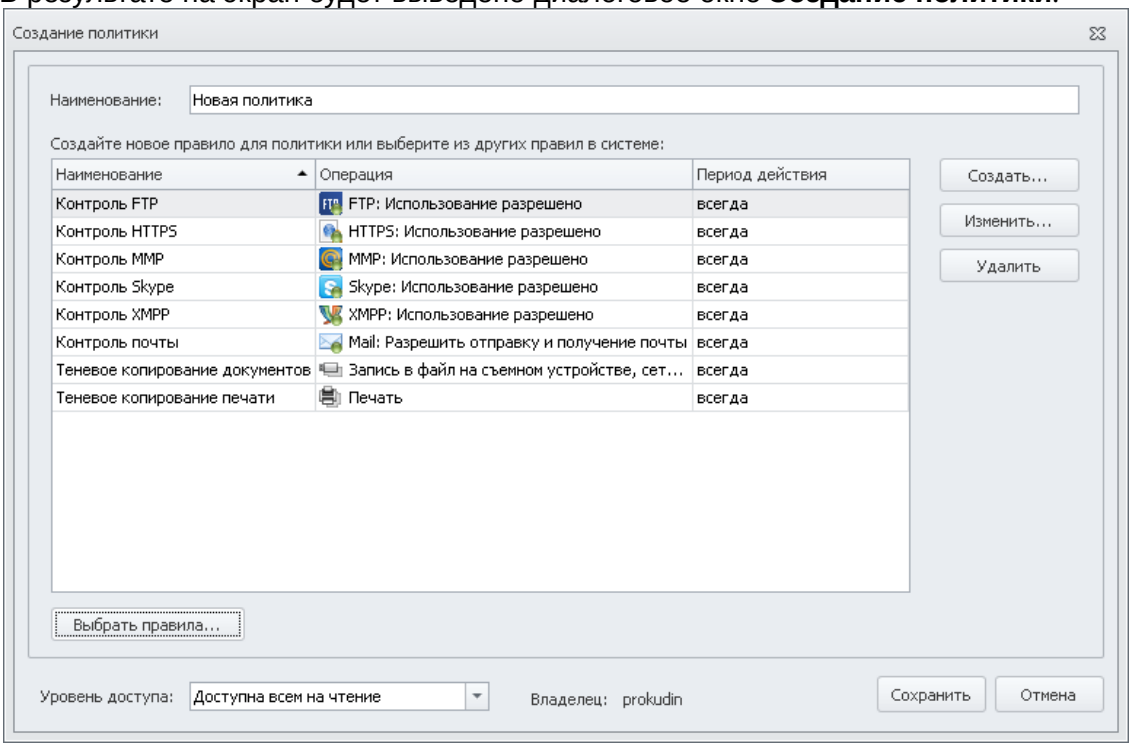
> **Примечание.**
>
> Информация по некоторым свойствам дублируется в рабочей области главного окна.

Создание и настройка политики безопасности

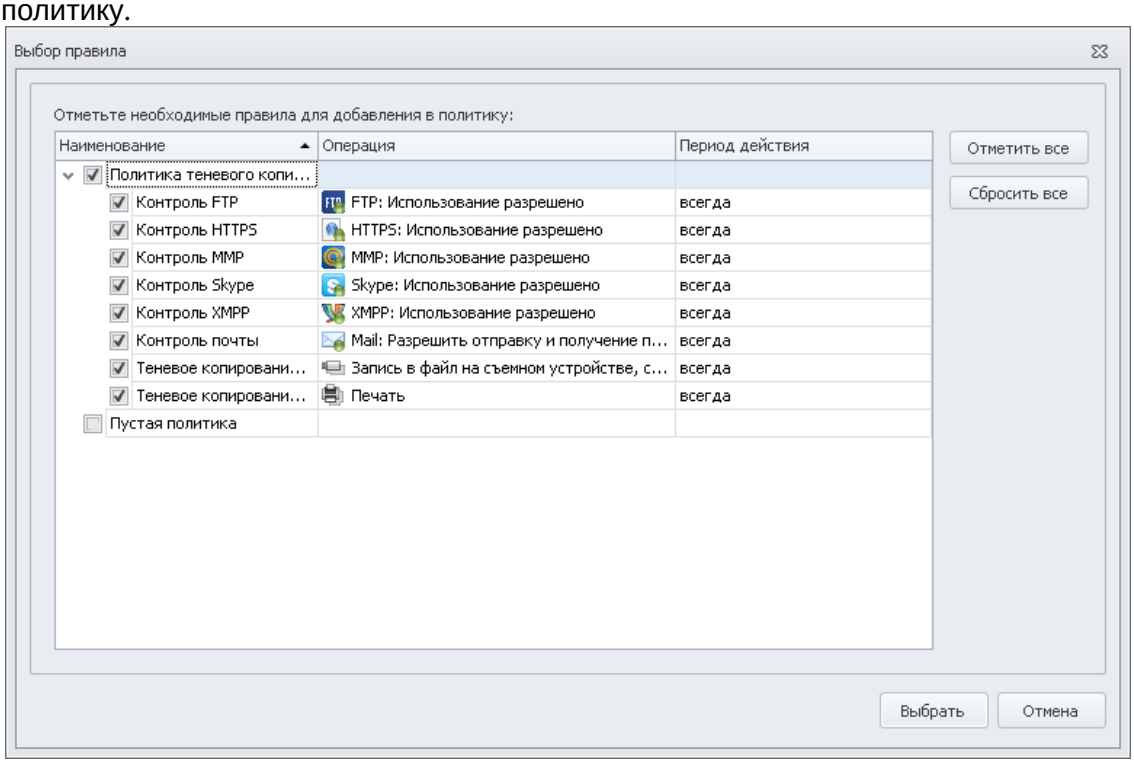
Чтобы создать и настроить политику безопасности:

1. Перейдите к разделу **Политики**.
2. Выполните одно из следующих действий:
   - воспользуйтесь кнопкой **Создать политику**, расположенной в верхней части Панели навигации;
   - в главном меню выберите команду **Правка** > **Создание политики**;

- на клавиатуре нажмите сочетание клавиш **Ctrl+N**.
  В результате на экран будет выведено диалоговое окно **Создание политики**.



3. В поле **Наименование политики** укажите название новой политики безопасности.
4. Составьте список правил для новой политики безопасности:
   - Чтобы скопировать правило из других политик, нажмите **Выбрать правила**. В раскрывшемся окне отметьте те правила, которые нужно скопировать в новую политику.



Вы можете также отметить целиком политику – в этом случае все правила, в ней

содержащиеся, будут скопированы в новую политику.
После того, как вы отметите все необходимые правила, нажмите **Выбрать**.

- Чтобы создать новое правило, нажмите **Создать** и задайте параметры правила как описано в одном из следующих разделов:
  - Правило для Application Monitor;
  - Правило для Audio Record Control;
  - Правило для Cloud Storage Monitor;
  - Правило для Clipboard Monitor;
  - Правило для Device Monitor;
  - Правило для File Monitor;
  - Правило для File Operations Monitor;
  - Правило для FTP Monitor;
  - Правило для HTTP(S) Monitor;
  - Правило для IM Client Monitor;
  - Правило для Keyboard Monitor;
  - Правило для Mail Monitor;
  - Правило для Network Monitor;
  - Правило для Print Monitor;
  - Правило для ScreenShot Control Monitor;
  - Правило для ScreenShot Monitor;
  - Правило для Statistics.

  Вы также можете отредактировать или удалить правило из политики, выбрав правило и нажав **Изменить** или **Удалить** соответственно.

5. В выпадающем списке **Уровень доступа** задайте права на чтение и редактирование политики.
6. После того, как вы определите все правила, которые должны входить в политику, и назначите права, нажмите **Сохранить**.

> **Важно!**
>
> Чтобы изменения вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, все изменения будут утеряны.

В дальнейшем вы сможете редактировать и удалять как сами политики безопасности (см. "Редактирование политики безопасности", "Удаление политики безопасности"), так и правила, определенные для них (см. "Добавление правила").

Редактирование политики безопасности

Чтобы отредактировать политику безопасности:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выберите название нужной политики безопасности.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить**;
   - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации;
   - на клавиатуре нажмите сочетание клавиш **Ctrl+E**;

- дважды щелкните левой кнопкой мыши по названию выделенной политики безопасности;
- щелкните по названию политики правой кнопкой и в контекстном меню выберите **Изменить**.

В результате выполнения любого из этих действий на экран будет выведено диалоговое окно **Редактирование политики**.

4. Именование политики безопасности и определение правил, входящих в нее, производится аналогично созданию политики: см. "Создание и настройка политики безопасности", шаги 3-4.
5. Нажмите **Сохранить**.

> **Важно!**
>
> Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Удаление политики безопасности

> **Важно!**
>
> Политику, назначенную хотя бы одной группе сотрудников или группе компьютеров, невозможно удалить. Чтобы удалить политику, убедитесь, что всем группам сотрудников (см. "Просмотр сведений о сотрудниках и группах сотрудников") и компьютеров (см. "Просмотр сведений о компьютерах") не назначена удаляемая политика.

Чтобы удалить политику безопасности:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выберите название нужной политики безопасности.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - на клавиатуре нажмите сочетание клавиш **Ctrl+D**.
4. В появившемся окне нажмите **Да**, чтобы подтвердить удаление политики безопасности.

> **Важно!**
>
> Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Правила

Работа с правилами ведется в рамках той политики безопасности, для которой определены эти правила. Каждой политике безопасности соответствует свой набор правил.

Информация по работе с правилами содержится в подразделах:

- Создание правил;
- Применение правил;
- Настройка правил Device Monitor для сбора данных статистики и перехвата событий.

Создание правил

Чтобы добавить в политику новое правило:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выберите политику безопасности, в которую вы хотите добавить правило.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Создать правило**;
   - воспользуйтесь кнопкой **Создать правило**, расположенной в верхней части области **Политики**;
   - в области **Правила** нажмите правой кнопкой мыши и из раскрывшегося списка выберите **Создать правило**;
   - нажмите сочетание клавиш **Ctrl+Shift+N**.
4. В открывшемся диалогом окне выберите тип правила и укажите остальные параметры правила. Доступные типы правил:
   - Правило для Application Monitor
   - Правило для Audio Record Control
   - Правило для Clipboard Monitor
   - Правило для Cloud Storage Monitor
   - Правило для Device Monitor
   - Правило для File Monitor
   - Правило для File Operations Monitor
   - Правило для FTP Monitor
   - Правило для HTTP(S) Monitor
   - Правило для IM Client Monitor
   - Правило для Keyboard Monitor
   - Правило для Mail Monitor
   - Правило для Network Monitor
   - Правило для Print Monitor
   - Правило для ScreenShot Control Monitor
   - Правило для ScreenShot Monitor
   - Правило для Screen Record Video
   - Правило для Statistics
5. После того как вы указали все необходимые параметры, нажмите **Сохранить**.

Чтобы отредактировать правило:

1. В списке правил политики выберите правило, которое вы хотите изменить.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить правило**;
   - дважды щелкните левой кнопкой мыши по выделенной строке;

- щелкните по выделенной строке правой кнопкой мыши и в контекстном меню выберите **Изменить правило**;
- воспользуйтесь кнопкой  **Изменить правило**, расположенной в верхней части области **Политики**;
- на клавиатуре нажмите сочетание клавиш **Ctrl+Shift+E**.

3. В открывшемся диалогом окне внесите необходимые изменения, после чего нажмите **Сохранить**.

Чтобы удалить правило:

1. В списке правил политики выберите правило, которое вы хотите удалить.

> **Примечание.**
>
> Для выделения нескольких правил используйте клавиши Shift или Ctrl. Чтобы выделить все правила, нажмите Ctrl+A.

2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить правило**;
   - воспользуйтесь кнопкой  **Удалить правило**, расположенной в верхней части области **Политики**;
   - щелкните по строке правила правой клавишей мыши и в контекстном меню выберите **Удалить правило**;
   - нажмите клавишу **Delete**.
3. В окне подтверждения нажмите **Да**.

Чтобы скопировать правило:

1. В списке правил политики выберите правило, которое вы хотите скопировать. Если требуется скопировать несколько правил, выделите все нужные строки.
2. Щелкните левой кнопки мыши по выделенному правилу и, не отпуская кнопку, перетащите правило в область **Политики** на Панели навигации. Подведите курсор мыши к названию политики безопасности, в которую нужно добавить правило. После того как слева от названия выбранной политики появится желтая стрелка, отпустите левую кнопку мыши.
   Правило будет скопировано в выбранную политику безопасности.

Вы также можете скопировать правила при редактировании политики безопасности. Для этого:

1. Перейдите в режим редактирования выбранной политики безопасности.
2. Нажмите **Выбрать правила**. В раскрывшемся списке отметьте правила, которые нужно скопировать в редактируемую политику. Можно выбрать всю политику целиком – в этом случае все правила выбранной политики будут добавлены в редактируемую политику.
3. После того, как вы отметите все необходимые правила, нажмите **Выбрать**.
4. Нажмите **Сохранить**.

> **Важно!**
>
> Поскольку работа с правилами ведется в режиме редактирования схемы безопасности, то для того, чтобы изменения вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, все изменения будут утеряны.

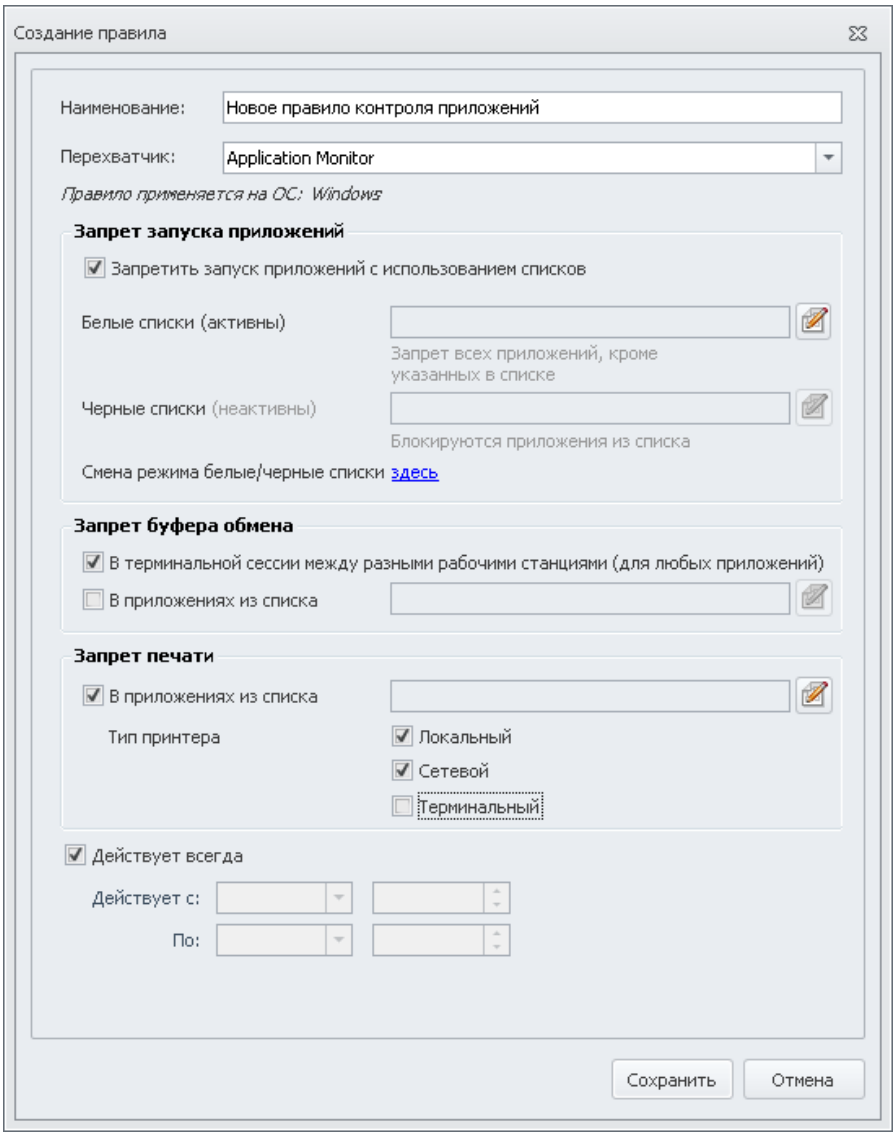
Правило для Application Monitor

Через сторонние приложения, установленные на рабочей станции и не контролируемые InfoWatch Device Monitor, сотрудник может совершить действия, приводящие к утечке конфиденциальной информации.
Перехватчик Application Monitor позволяет контролировать доступ сотрудников к приложениям при помощи наложения запрета на:

- запуск приложений;
- буфер обмена;
- печать.

Эти запреты можно активировать как по отдельности, так и совместно.

> **Примечание:**
>
> Правило применяется на компьютерах под управлением операционной системы MS Windows.

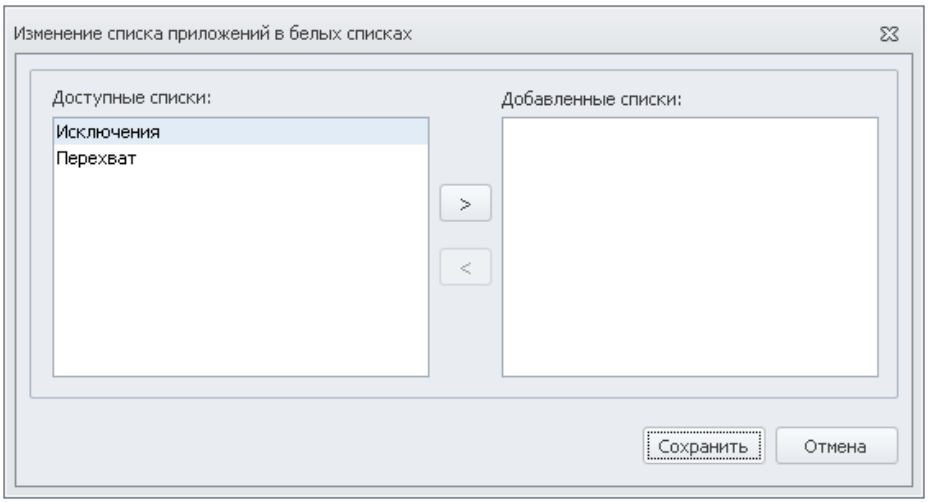


Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **Application Monitor**.
3. В блоке **Запрет запуска приложений** установите флажок напротив **Запретить запуск приложений с использованием списков**, если нужно блокировать только выборочные приложения из списков. В противном случае будет разрешен запуск всех приложений.

> **Примечание:**
>
> Для переключения между режимами активных белых и черных списков приложений нажмите ссылку здесь.
>
> О порядке формирования списков приложений см. "Приложения".

4. Добавьте белые или черные списки приложений нажатием кнопки .



5. В открывшемся окне, в области **Доступные списки**, выберите нужные списки и перенесите их в область **Добавленные списки** нажатием кнопки .
6. Нажмите **Сохранить**.
7. В блоке **Запрет буфера обмена** для включения запрета буфера обмена установите флажки напротив групп приложений, для которых следует запретить копирование данных:
   - в терминальной сессии между разными рабочими станциями (для любых приложений);
   - в приложениях из списка (добавьте списки нажатием кнопки ).

> **Важно!**
>
> Буфер обмена блокируется полностью и для всех типов данных, без разделения на копирование/вставку, независимо от режима черных/белых списков.

8. В блоке **Запрет печати** установите флажок напротив **В приложениях из списка,** чтобы включить запрет печати и укажите список приложений, печать из которых требуется запретить, а также тип принтера:
    - локальный;
    - сетевой;
    - терминальный.

    Пользователь не сможет отправить на печать данные в указанных приложениях. Также ему будут недоступны выбранные типы принтеров.
9. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
10. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Правило для Audio Record Control

> **Важно!**
>
> Функциональность предназначена только для InfoWatch Activity Monitor.
>
> Device Monitor версии 7.18.X совместим с Activity Monitor версии 3.4.X. Не поддерживается совместимость Device Monitor версии 7.18.X с более ранними версиями Activity Monitor.

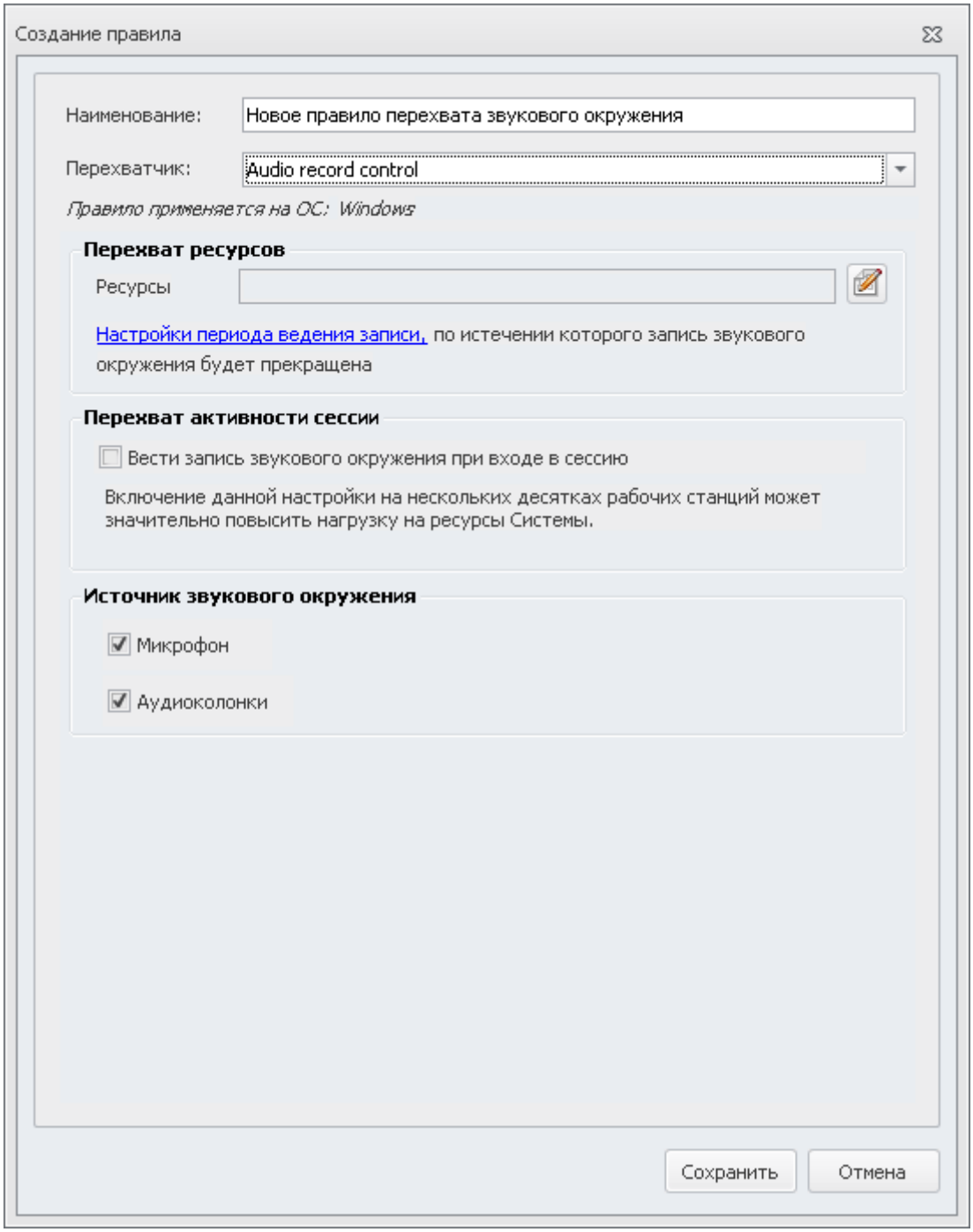
Перехватчик Audio record control позволяет отслеживать действия сотрудника при помощи контроля звукового окружения рабочей станции данного сотрудника[1].

В правиле вы можете настроить:

- **Перехват ресурсов** – запись звукового окружения при использовании выбранных ресурсов[2].
- **Перехват активности сессии** – запись звукового окружения в течение всего периода рабочей сессии, с момента входа пользователя в систему до момента выхода[3]. При блокировке рабочей станции запись звукового окружения не прерывается.
- **Источник звукового окружения** – вы можете выбрать один или два типа источника звукового окружения: микрофон[4] и/или аудиоколонки.

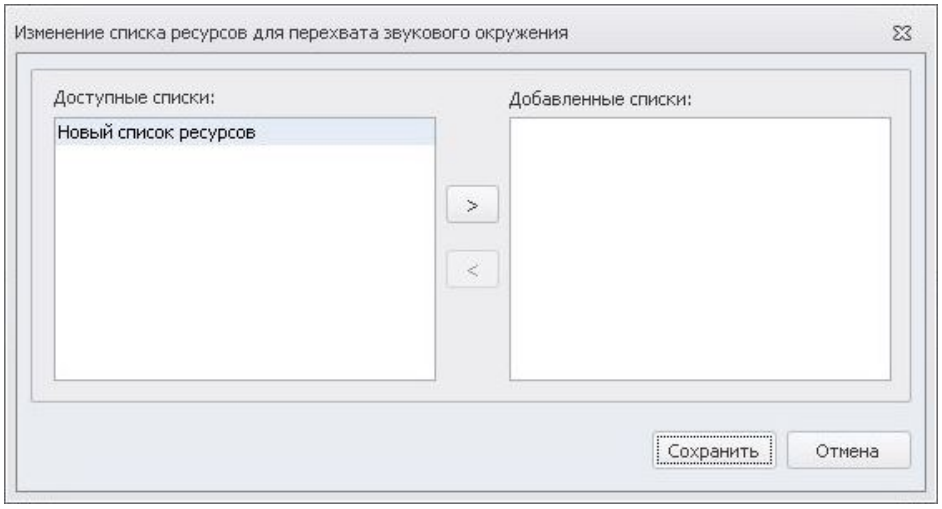
> **Важно!**
>
> Перехват ресурсов доступен начиная с версии Device Monitor 7.8.0.
>
> Перехват активности сессии доступен начиная с версии Device Monitor 7.12.0.
>
> Выбор источника звукового окружения доступен с версии Device Monitor 7.15.0.
>
> При этом для срабатывания перехвата номер версии Агента не должен быть ниже номера версии сервера Device Monitor.

> **Примечание:**
>
> Правило применяется на компьютерах под управлением операционной системы MS Windows.



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **Audio record control**.
3. Если вы хотите добавить ресурсы для перехвата:
   a. Нажмите 



b. В открывшемся окне в области **Доступные списки** выберите нужные списки ресурсов (при использовании которых необходимо начинать запись звукового окружения) и перенесите их в область **Добавленные списки**, нажав > .
c. Нажмите **Сохранить**.
d. Нажмите **Настройки периода ведения записи**, чтобы задать продолжительность ведения записи. Подробнее см. "Настройка перехвата звукового окружения".

4. Если вы хотите включить перехват активности сессии:
   a. Установите флажок в поле **Вести запись звукового окружения при входе в сессию**.
   b. В открывшемся предупреждающем окне нажмите **Да**.

> **Важно!**
>
> Перехват активности сессии на нескольких десятках рабочих станций на регулярной основе может вызвать чрезмерный рост количества событий и серьезно увеличить нагрузку на сеть и серверы Device Monitor и Activity Monitor.

5. Выберите, с источника какого типа вести запись звукового окружения:
   - *Микрофон*
     и/или
   - *Аудиоколонки*
     Если к рабочей станции подключено несколько устройств одного типа, то для ведения записи среди них будет выбрано одно с самой большой амплитудой аудиосигнала. Также вы можете задать дополнительные параметры выбора устройства для звукового перехвата в инженерных настройках агента.
6. После определения всех параметров нажмите **Сохранить**.

> **Примечание:**
>
> [1] 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).
>
> [2] Проверка на соответствие посещаемого ресурса ресурсу из списка производится только если пользователь работает в браузерах:

- Chrome;
- Яндекс.Браузер;
- Mozilla Firefox;
- Edge (Chromium);
- Opera.

[3] 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.

[4] Если персона 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).

Правило для Clipboard Monitor

Перехватчик Clipboard Monitor позволяет контролировать доступ сотрудников к буферу обмена.

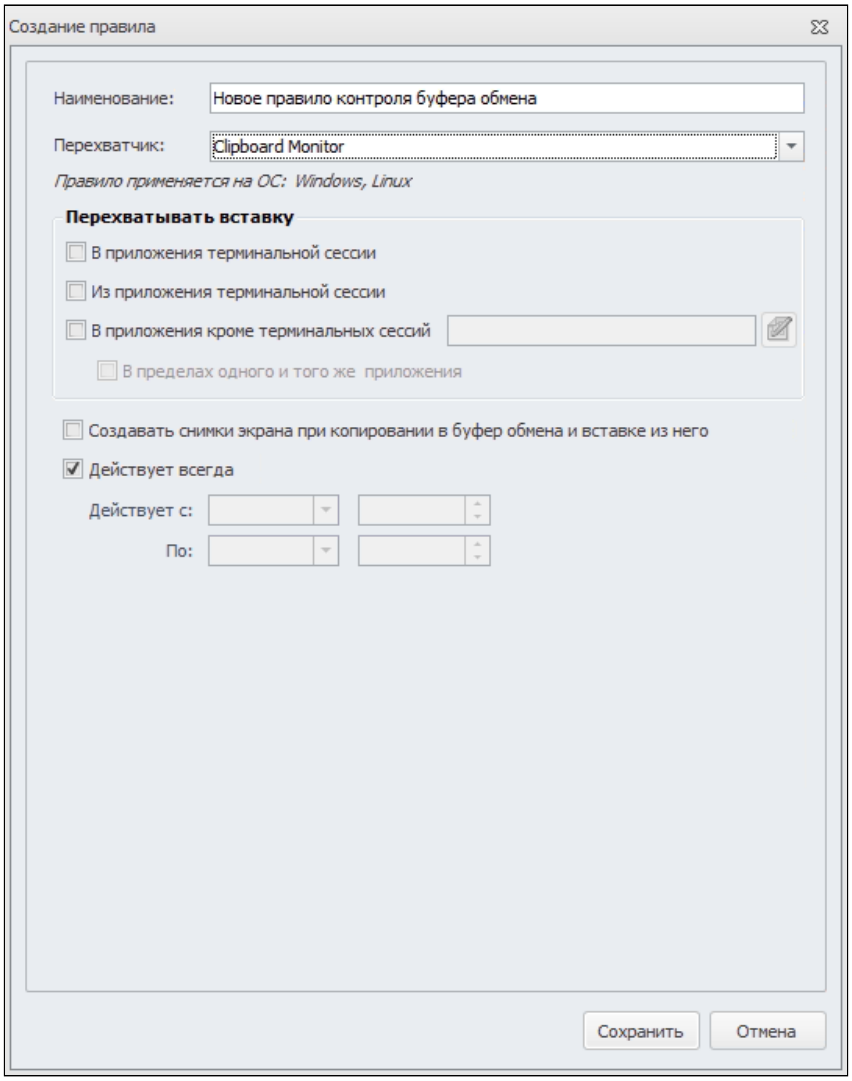
Важно!

С помощью этого правила Device Monitor перехватывает только текстовые данные.

Чтобы контролировать копирование файлов, используйте правило для File Monitor (см. "Правило для File Monitor").

Примечание.

Правило применяется на компьютерах под управлением операционных систем MS Windows, РЕД ОС, Альт Рабочая станция и Astra Linux.



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **Clipboard Monitor**.
3. В области **Перехватывать вставку из буфера обмена** определите, в каком случае правило будет действовать:

> **Важно!**
>
> На рабочих станциях под управлением РЕД ОС и ОС Альт Рабочая станция не поддерживаются опции:
>
> - **В приложения терминальной сессии**;
> - **Из приложения терминальной сессии**.

Чтобы настроить правило для РЕД ОС и ОС Альт Рабочая станция, выберите опцию **В приложения кроме терминальных сессий** и выберите список приложений Linux.
На рабочих станциях под управлением РЕД ОС, ОС Альт Рабочая станция и и Astra Linux не поддерживается использование опции **В пределах одного и того же приложения**.

- **В приложения терминальной сессии**. Если выбрана эта опция, то правило будет срабатывать при вставке данных в приложения терминальной сессии. При вставке данных внутри терминальной сессии правило срабатывать не будет.
- **Из приложения терминальной сессии**. Если выбрана эта опция, то правило будет срабатывать при вставке данных из приложения терминальной сессии. При вставке данных внутри терминальной сессии правило срабатывать не будет.
- **В приложения кроме терминальных сессий**:
  - Выберите эту опцию, если правило должно действовать только в случае вставки данных в указанные приложения.

    Выберите списки приложений с помощью кнопки  (см. "Приложения"). Правило также будет срабатывать при вставке в указанные приложения данных, скопированных из терминальной сессии.
  - Если требуется, чтобы правило срабатывало также при вставке данных в приложение, из которого данные были скопированы, отметьте опцию **В пределах одного и того же приложения**. Перехват в пределах одного приложения поддерживается, только если приложение использует системные механизмы буфера обмена.

4. Установите флажок в поле **Создавать снимки экрана при копировании в буфер обмена и вставке из него** для активации соответствующей опции.

Важно!

Создание снимка экрана в этом правиле не поддерживается на рабочих станциях под управлением РЕД ОС, ОС Альт Рабочая станция и и Astra Linux.

5. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
6. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Примечание:

Блокировка по результатам анализа в Traffic Monitor осуществляется только на агентах под управлением ОС Windows для операций с использованием приложений терминальной сессии.

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.

Правило для Cloud Storage Monitor

Перехватчик **Cloud Storage Monitor** позволяет контролировать веб-клиенты следующих облачных хранилищ:

- Google Drive
- DropBox
- YandexDisk
- OneDrive
- EverNote
- SugarSync

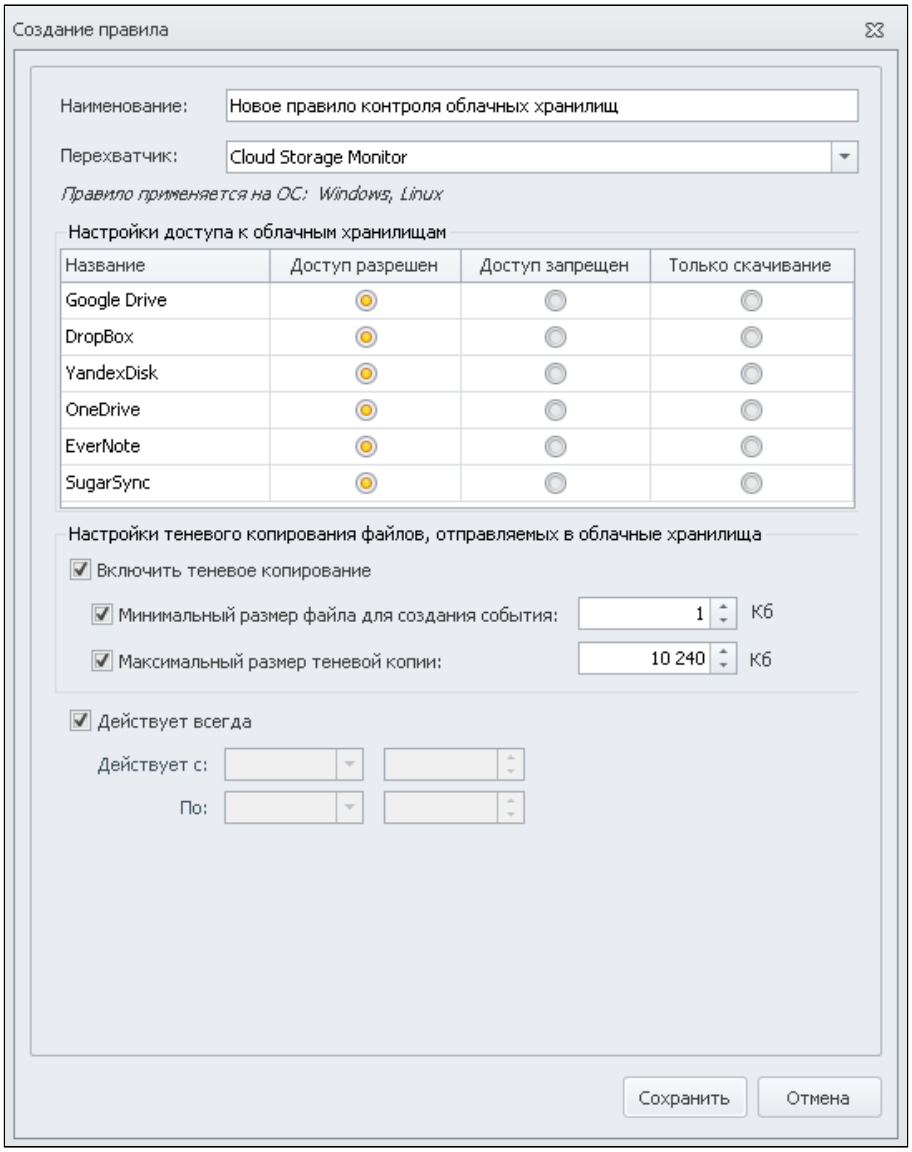
Для всех облачных хранилищ доступны следующие варианты ограничения доступа: **Доступ запрещен** и **Только скачивание**.

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.

Примечание.

Правило применяется на компьютерах под управлением операционных систем MS Windows, Astra Linux, РЕД ОС и ОС Альт.



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **Cloud Storage Monitor**.
3. В области **Настройка доступа к облачным хранилищам** отметьте необходимый вариант ограничения доступа.
4. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
5. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Примечание:

Блокировка по результатам анализа в Traffic Monitor осуществляется только на агентах под управлением ОС Windows.

Правило для Device Monitor

Перехватчик **Device Monitor** позволяет контролировать доступ сотрудников к периферийным устройствам, мобильным телефонам и фотокамерам, подключенным к компьютеру; а также устройствам, подключенным к тонким и толстым терминальным клиентам.

Важно!

На компьютерах под управлением ОС семейства Linux:

- Настройка доступа и контроль поддерживается только для следующих типов устройств:
  - Съемное устройство хранения;
  - MTP-устройство;
  - CD/DVD;
  - Флоппи-диск.
- Недоступно ограничение **Полный доступ к зашифрованным устройствам**.

При блокировании устройство будет отображаться в операционной системе, но будет недоступно для использования.

Вы можете настроить соответствующие ограничения для следующих типов устройств, подключаемых непосредственно к компьютеру:

Полный доступ к зашифрованным устройствам / Только чтение / Нет доступа / Использование разрешено	Только чтение / Нет доступа / Использование разрешено	Нет доступа / Использование разрешено
• Флоппи-дисковод • Съемное устройство хранения (устройства, подключаемые через интерфейсы USB, IEEE 1394)	• CD/DVD • MTP совместимое устройство (устройства, подключаемые через MTP- или PTP-протокол)*	• Параллельный порт (LPT) • Последовательный порт (COM) • Локальный принтер (подключаемый через интерфейс USB, IEEE 1394, SCSI и пр.) • Устройства работы с изображениями (видеокамеры, сканеры) • Bluetooth устройство • IrDA устройство • Другое USB устройство • FireWire • Модем • Считыватель смарт-карт (Smart Card Reader) • Ленточный накопитель • Многофункциональное устройство

Полный доступ к зашифрованным устройствам / Только чтение / Нет доступа / Использование разрешено	Только чтение / Нет доступа / Использование разрешено	Нет доступа / Использование разрешено
		• PCMCI устройство • Сетевой адаптер USB • Сетевой принтер • КПК (карманные компьютеры под управлением операционных систем Windows Mobile и Palm OS)

* – разрешено чтение и удаление с устройства

Примечание.

InfoWatch Device Monitor поддерживает работу с устройствами, информация на которых зашифрована с помощью InfoWatch CryptoStorage SOHO 2.1, InfoWatch CryptoStorage Enterprise 1.0, Kaspersky KryptoStorage 1.0 и TrueCrypt 7.1.

Мобильные устройства могут быть подключены к компьютеру:

- как съемное устройство хранения;
- как MTP- или PTP-устройство;
- как сетевой адаптер USB.

Контроль подключения через MTP- и PTP-протокол осуществляется для телефонов на платформе Android, iOS, Windows Phone/10 Mobile; Blackberry 10.

Фотокамера может быть подключена к компьютеру:

- как съемное устройство хранения;
- как PTP-устройство.

Важно!

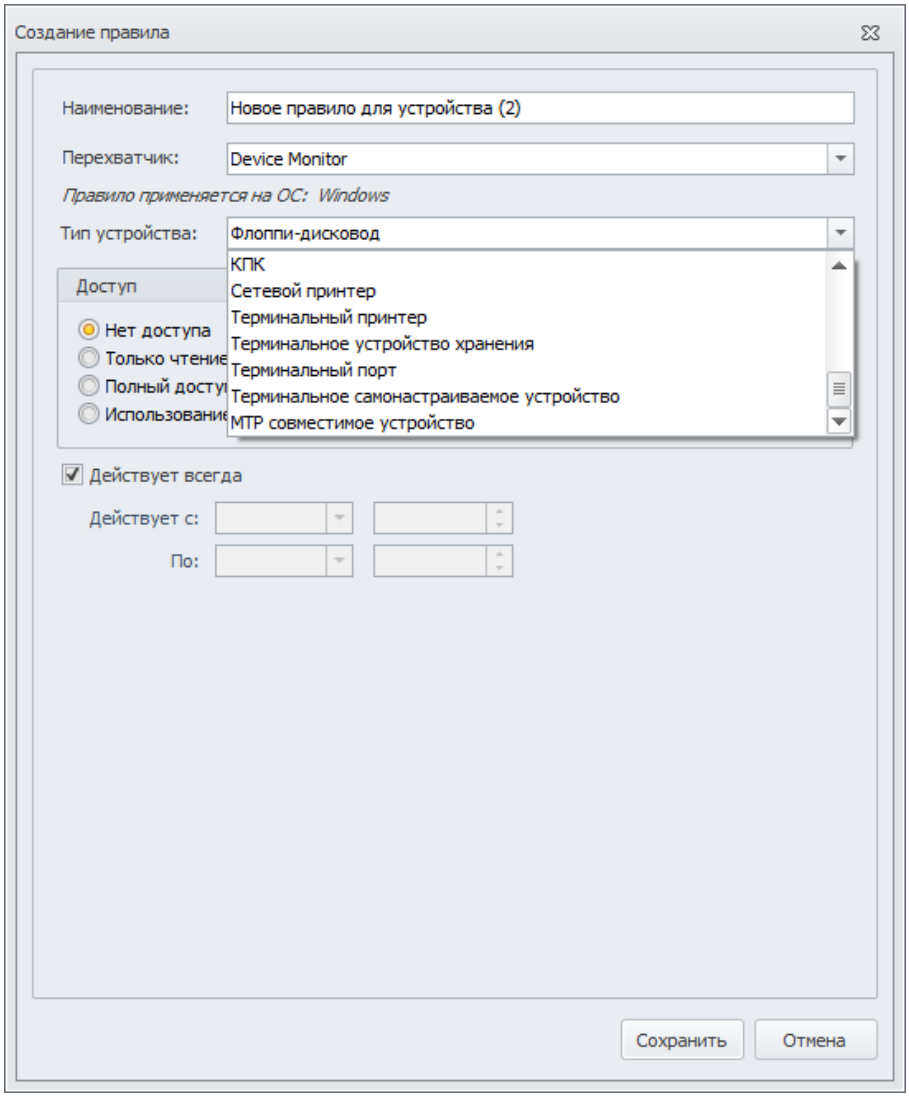
Копирование файлов на съемные устройства и MTP-устройства можно контролировать также с помощью правила File Monitor. При этом необходимо учитывать, что правило File Monitor позволяет отслеживать операции копирования, в то время как правило Device Monitor позволяет полностью запретить подобные операции. О порядке разрешения конфликтов, когда событие соответствует нескольким правилам, см. "Применение правил" и "Особенности применения правил для Device Monitor".

Также правило позволяет контролировать следующие типы устройств, подключаемые через Microsoft RDP или Citrix ICA со следующими ограничениями:

Только чтение / Нет доступа / Использование разрешено	Нет доступа / Использование разрешено
• Терминальное устройство хранения	• Терминальный принтер • Терминальный порт (порты тонкого клиента) • Терминальное самонастраиваемое устройство (например, смартфоны)

Контроль терминальных клиентов, подключенных с помощью Microsoft RDP или Citrix ICA, актуален в следующей ситуации:

1. Удаленный пользователь с терминального клиента подключается к компьютеру с установленным агентом Device Monitor.
2. К терминальному клиенту подключено устройство хранения или принтер.
3. Удаленный пользователь пытается распечатать/скопировать данные с компьютера (при этом локальные терминальные принтер/устройство хранения должны быть подключены к компьютеру посредством Microsoft RDP или Citrix ICA).



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите выберите **Device Monitor**.
3. В поле **Тип устройства** выберите тип устройства, контролируемого данным правилом.
4. В области **Доступ** отметьте необходимый вариант ограничения доступа на использование устройства. Вы можете:
   - полностью запретить доступ к устройству;
   - разрешить только чтение (только для типов **CD/DVD**, **MTP совместимое устройство**, **Флоппи-дисковод**, **Съемное устройство хранения** и **Терминальное устройство хранения**);

     > **Примечание.**
     >
     > Для типа **MTP совместимое устройство** при выборе уровня доступа *Только чтение* пользователю также доступно удаление файлов с устройства.

   - разрешить полный доступ только к зашифрованным устройствам (только для типов **Флоппи-дисковод** и **Съемное устройство хранения**).
   - полностью разрешить доступ к устройству;
5. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
6. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

> **Примечание:**
>
> Вы можете отправлять события использования/подключения устройств в Платформу. Начиная с Device Monitor версии 7.15 по умолчанию включена отправка событий использования/подключения устройств в Платформу. Подробнее см. "Настройка отправки данных в продукты".

Особенности применения правила на некоторых устройствах:

Мобильные устройства на платформе BlackBerry 10 при включенной настройке "Режим USB-накопителя" определяются как два устройства: *MTP совместимое устройство* и *Съемное устройство хранения*. Чтобы запретить копирование данных на устройство, необходимо установить запрет для типа *Съемное устройство хранения*.

Особенности применения правила при обновлении:

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

Правило для File Monitor

Перехватчик **File Monitor** позволяет отслеживать операции копирования файлов с/на съемные устройства и сетевые ресурсы (в том числе сетевые тома), а также записи в файл на съемном устройстве, причем регистрируется факт успешного завершения операции.

> **Примечание.**

Правило применяется на компьютерах под управлением операционных систем MS Windows, Astra Linux, РЕД ОС и ОС Альт.

К съемным устройствам относятся:

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

Отслеживаются такие действия сотрудников, как:

- копирование файла на сетевые ресурсы с использованием UNC (например, *Server**SharedFolder**Folder**File*);
- копирование/перемещение файла с/на съемное устройство. Отслеживаются операции копирования/перемещения файла с контролируемого компьютера, другого съемного устройства или сетевых ресурсов;
- создание файла непосредственно на съемном устройстве;
- редактирование файла непосредственно на съемном устройстве, в том числе переименование;
- копирование файла с/на медиа-устройства, использующие для подключения протокол MTP;
- копирование файла в приложение терминальной сессии;

Важно!

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

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

Примечание:

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

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

Важно!

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

Важно!

На компьютерах под управлением РЕД ОС или ОС Альт не перехватывается копирование файла на сетевой ресурс, если подключение осуществлялось вводом имени сервера в строке поиска файлового менеджера ОС.

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

- копирования/перемещения файлов на ресурсы, подключенные через терминальную сессию;
- записи на CD/DVD-диски, в том числе подключенные через порты USB.

Блокировка по результатам анализа в Traffic Monitor осуществляется:

- только на агентах под управлением ОС Windows, Альт, РЕД ОС и Astra Linux 1.7 при копировании с/на съемные устройства и сетевые ресурсы;
- только на агентах под управлением ОС Windows при копировании/перемещении файлов на ресурсы, подключенные через терминальную сессию.

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.

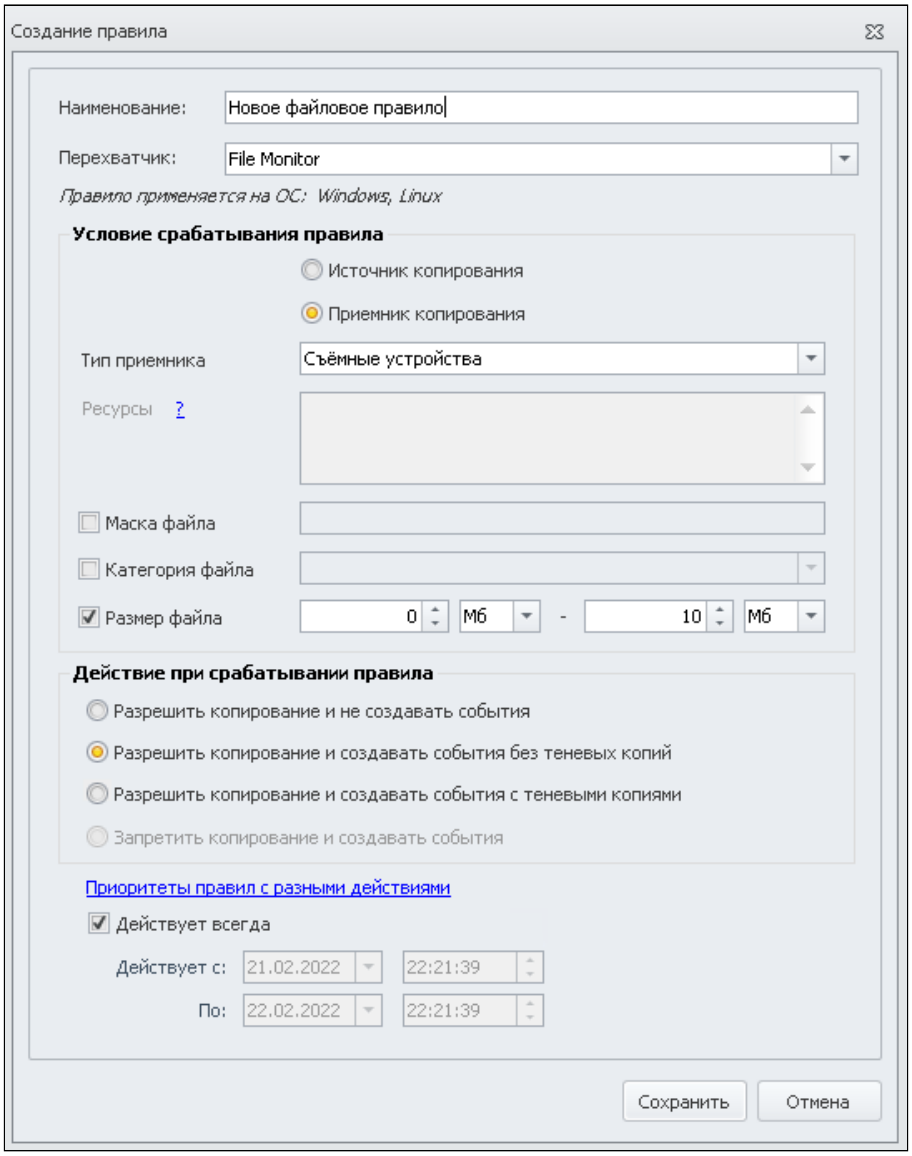
Система распаковывает архивы и применяет к ним политики Traffic Monitor, если:

- 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!

Доступ к съемным устройствам и MTP-устройствам можно контролировать также с помощью правила Device Monitor. При этом правило Device Monitor позволяет полностью запретить доступ к устройству.

О порядке разрешения случаев, когда событие соответствует нескольким правилам, см. "Применение правил".



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **File Monitor**.
3. Укажите **Условия срабатывания правила**:
   a. Задайте направление перехвата копирования: *Источник копирования* или *Приемник копирования*.
   b. Укажите тип источника: *Съемные устройства*, *Сетевые ресурсы* или *Терминальная сессия.*
   c. Если требуется, укажите сетевые ресурсы, задав их адреса.
4. 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.

5. Вы также можете ограничить применение правила определенной категорией сигнатур (см. "Сигнатуры"). Для этого отметьте поле **Категория файла** и выберите категорию из раскрывающегося списка: правило будет действовать для записи в файлы с типом, соответствующим выбранной категории сигнатур.

Примечание:

На компьютерах под управлением Astra Linux, РЕД ОС и ОС Альт категории сигнатур не учитываются – правило сработает на копирование любых файлов, вне зависимости от указанных категорий файлов

6. Чтобы ограничить размер файлов, подлежащих контролю, отметьте поле **Размер файла** и укажите:
   - Минимальный размер файла. Если поле заполнено, то правило будет действовать только для файлов, размер которых больше либо равен указанному.
   - Максимальный размер файла. Если поле заполнено, то правило будет действовать только для файлов, размер которых меньше либо равен указанному.
7. Выберите действие, которое будет наступать при срабатывании правила. Вы можете:
   a. разрешить копирование и не создавать события;
   b. разрешить копирование с созданием события без теневых копий;
   c. разрешить копирование с созданием события с теневыми копиями;
   d. запретить любое копирование и создавать при этом события.

Важно!

Если, в соответствии с действующим правилом File Monitor, должна быть создана теневая копия файла, но на компьютере осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного места"), то сохранение файлов будет осуществляться без создания теневой копии.

Примечание:

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

8. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
9. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

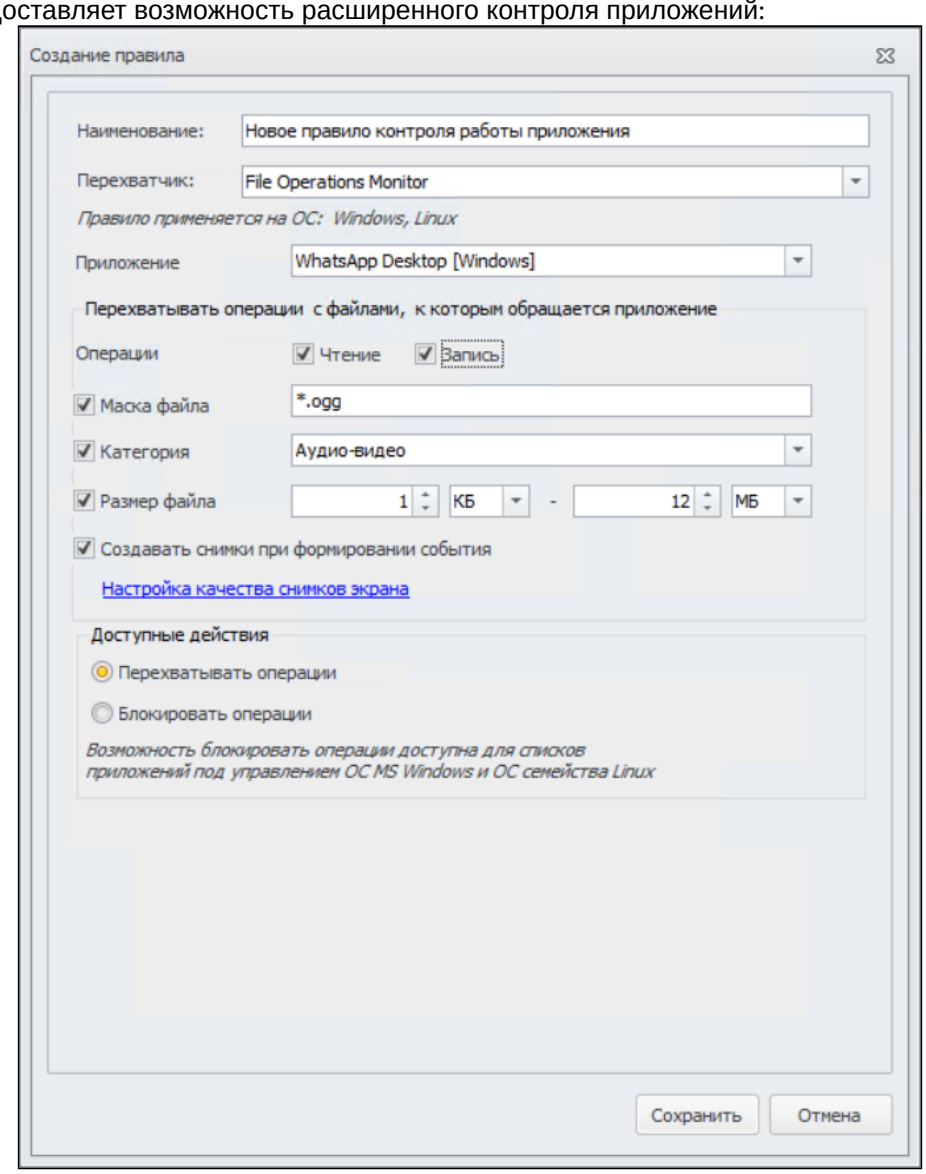
Подробнее о работе правила см. статью Базы Знаний "Особенности и ограничения перехвата при копировании файлов с/на съемные устройства, сетевые ресурсы, FTP, перехвата исходящей почты. Особенности задания правил в политиках защиты данных на агентах".

Правило для File Operations Monitor

Перехватчик **File Operations Monitor** позволяет контролировать чтение и запись файлов приложением, а также создавать теневые копии файлов и снимки экрана.

> **Важно!**
>
> Правило недоступно по умолчанию. Чтобы использовать правило для File Operations Monitor, добавьте в схему безопасности Device Monitor конфигурацию Блокады приложений (см. "Блокада приложений").

Правило предоставляет возможность расширенного контроля приложений:



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **File Operations Monitor**.

3. В поле **Приложение** выберите контролируемое приложение из списка.

> **Примечание:**
>
> Список доступных приложений определяет конфигурация Блокады приложений.

4. В поле **Операции** укажите действия, которые необходимо контролировать:
   - Чтение;
   - Запись.
5. При необходимости вы можете ограничить набор контролируемых файлов, задав маску файла. Для этого отметьте поле **Маска файла** и укажите маску, используя символы:
   - «?» - для замены одного символа;
   - «*» - 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.

6. Вы также можете ограничить применение правила определенной категорией сигнатур (см. "Сигнатуры"). Для этого отметьте поле **Категория** и выберите категорию из раскрывающегося списка: правило будет действовать для файлов с типом, соответствующим выбранной категории сигнатур.
7. Чтобы ограничить размер файлов, подлежащих контролю, в поле **Размер файла** укажите:
   - Минимальный размер файла. Если поле заполнено, то правило будет действовать только для файлов, размер которых больше либо равен указанному.
   - Максимальный размер файла. Если поле заполнено, то правило будет действовать только для файлов, размер которых меньше либо равен указанному.

> **Примечание:**
>
> По умолчанию поле **Размер файла** отмечено и указан максимальный размер файла – 10 МБ. Рекомендуется ограничивать размер контролируемых файлов, так как это позволяет снизить нагрузку на систему.
>
> Чтобы перехватывать все файлы вне зависимости от размера, снимите флажок с поля **Размер файла**.

8. Установите флажок в поле **Создавать снимки при формировании события** для активации соответствующей опции.
9. При необходимости укажите настройки качества снимков экрана: см. "Контроль приложений и снимки экрана".
10. В поле **Доступные действия** выберите один из вариантов:
    - Перехватывать операции;
    - Блокировать операции.

Примечание:

Поддерживается только блокировка операции чтения. При этом необходимо задать маску файла.

Возможность блокировать операции доступна для списков приложений под управлением ОС MS Windows и ОС семейства Linux.

11. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Примечание:

Если в Telegram или Яндекс Мессенджере изображение было скопировано из одного чата в другой, то событие чтения не будет создано.

В Telegram, если сообщение содержит файл с расширением, которое должно быть заблокировано, пересылка этого сообщения из одного чата в другой не блокируется.

Правило для FTP Monitor

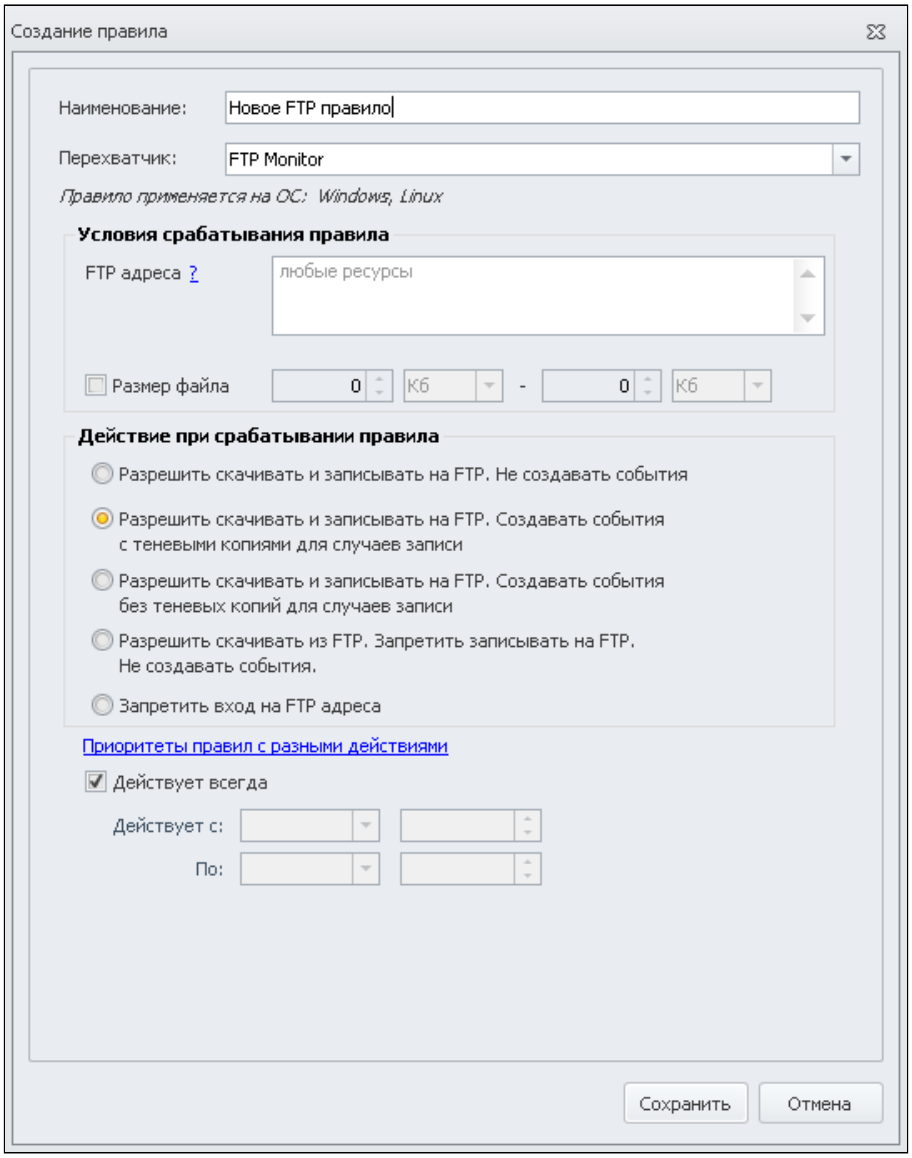
Перехватчик **FTP Monitor** позволяет контролировать обмен данными по протоколу FTP/FTPS.

Примечание.

Правило применяется на компьютерах под управлением операционных систем MS Windows, Astra Linux, РЕД ОС и ОС Альт.

Важно!

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



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **FTP Monitor**.
3. В **Условиях срабатывания правила** укажите **адреса FTP.** Нажав на **?** (знак вопроса), вы узнаете правила заполнения данного поля. Вы также можете указать ограничения файла, установив галочку напротив **Размера файла** и обозначив диапазон значений. 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, что определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного места").
4. Выберите степень контроля обмена данными по протоколу FTP:
   - **Разрешить скачивать и записывать на FTP. Не создавать события**
   - **Разрешить скачивать и записывать на FTP. Создавать события с теневыми копиями для случаев записи**

- **Разрешить скачивать и записывать на FTP. Создавать события без теневых копий для случаев записи**

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

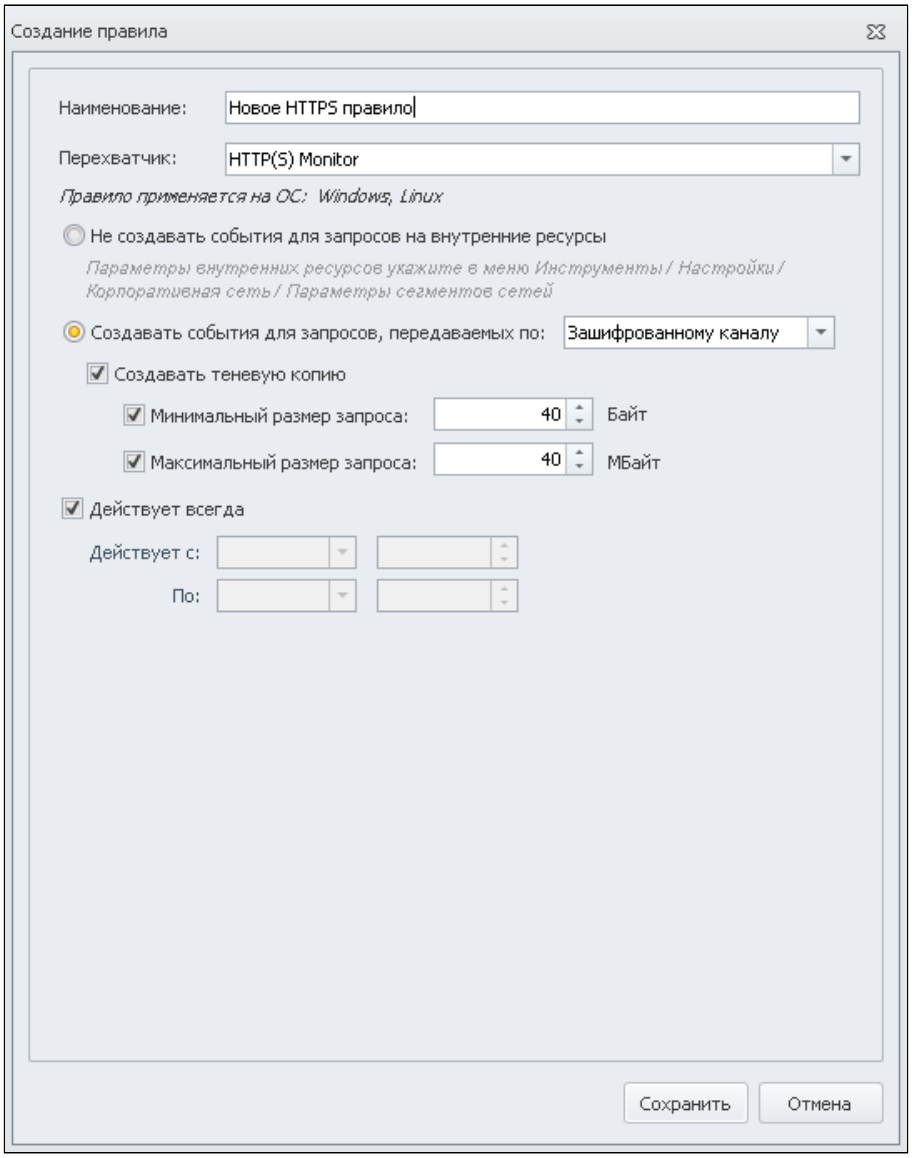
- **Разрешить скачивать из FTP/ Запретить записывать на FTP. Не создавать события**
- **Запретить вход на FTP адреса**

5. Настройте период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
6. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

> **Примечание:**
>
> Блокировка по результатам анализа в Traffic Monitor осуществляется только на агентах под управлением ОС Windows.

Правило для HTTP(S) Monitor

Перехватчик **HTTP(S) Monitor** позволяет контролировать обмен данными по протоколам HTTP и HTTPS[1].



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **HTTP(S) Monitor**.
3. Настройте параметры событий, создаваемых при перехвате трафика. Вы можете:
   - Исключить перехват запросов на внутренние ресурсы[2]. Отметьте поле **Не создавать события для запросов на внутренние ресурсы**, если вы хотите, чтобы все запросы, передаваемые внутри корпоративной сети не перехватывались. О том, как настроить сегменты сети, см. "Контроль сетевых соединений", группа **Параметры сегментов сетей**.
   - Настроить перехват данных только по шифрованным каналам, либо по всем каналам. Для этого:
     - Отметьте **Создавать события для запросов, передаваемых по** и из раскрывающегося списка выберите:
       - **Всем каналам**
       - **Зашифрованному каналу**

- Если вы хотите сохранять теневые копии[3] отправляемых файлов, отметьте поле **Создавать теневую копию**. Вы также можете определить дополнительные параметры этих теневых копий:
  - **Минимальный размер запроса**. Если поле отмечено, то теневое копирование будет выполняться только для запросов, размер которых больше либо равен указанному.
  - **Максимальный размер запроса**. Если поле отмечено, то теневое копирование будет выполняться только для запросов, размер которых меньше либо равен указанному.

4. Настройте период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
5. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Важно!

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

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

- Политика защиты данных на агентах применяется только к тексту запроса, анализ файлов не поддерживается.
- Не перехватываются соединения по протоколу IPv6.
- Запросы, относящиеся к веб-почте, перехватываются как обычные HTTP-запросы.
- Правила с выбранной настройкой **Не создавать события для запросов на внутренние ресурсы** игнорируются.

На рабочих станциях под управлением Mac OS:

- Файлы, передаваемые по протоколу HTTP(S), перехватываются как POST-запрос.
- Для работы сервисов Apple необходимо вручную добавить исключения на сервере Device Monitor. Подробнее см. "Контроль сетевого трафика".

[2] Если выбрать исключение перехвата запросов на внутренние ресурсы, то создание теневой копии в данном правиле станет недоступно. Если вам необходимо, чтобы:

- не создавались события для запросов на внутренние ресурсы, и при этом
- теневая копия создавалась,

то создайте два правила: по одному на каждое из требований.

[3] Если на компьютере осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного места"), то событие будет создано без теневой копии.

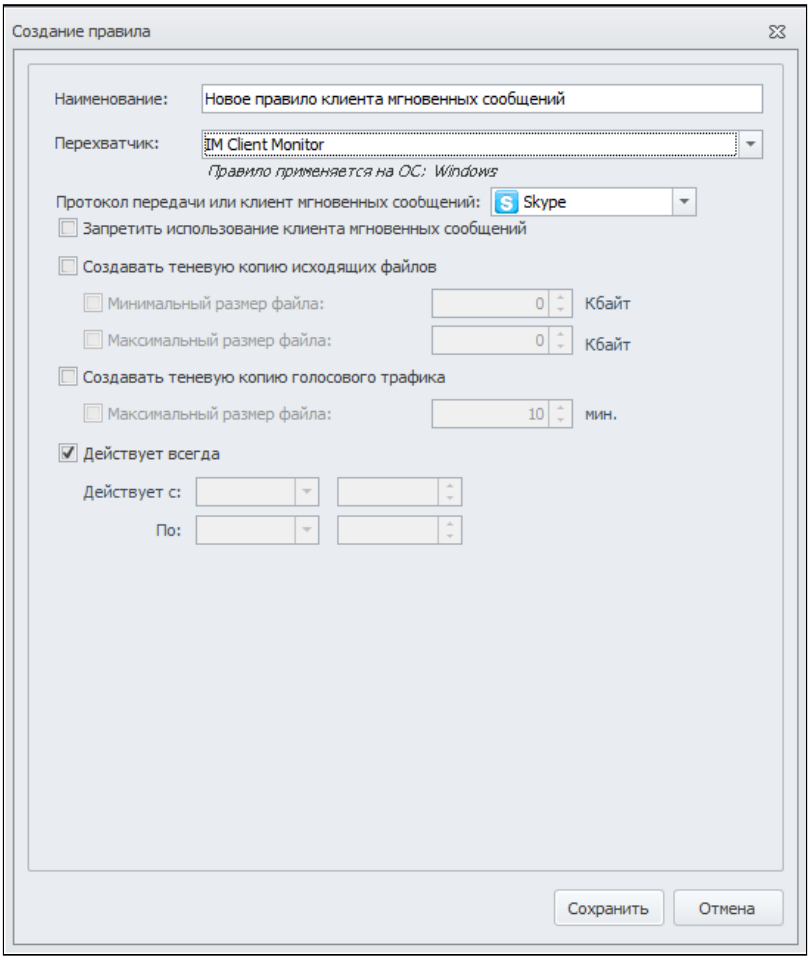
Правило для IM Client Monitor

Перехватчик **IM Client Monitor** позволяет контролировать:

- доступ сотрудников к системам мгновенного обмена сообщениями Skype, Telegram, Jabber (протокол XMPP), Facebook, WhatsApp, VK (ВКонтакте), протокол MMP, Яндекс Мессенджер;
- обмен новыми, пересылаемыми или исправленными сообщениями чата, в том числе группового, исходящими файлами и голосовыми сообщениями.

При этом будет перехвачена вся история переписки на служебном компьютере, включая период до установки Агента Device Monitor.

> **Примечание.**
>
> В зависимости от ОС, установленной на компьютере, контролируются клиенты мгновенных сообщений:
>
> - для MS Windows: Facebook, Jabber (XMPP), VK (ВКонтакте), Skype, MMP, Telegram, WhatsApp, Яндекс Мессенджер;
> - для РЕД ОС, Astra Linux, ОС Альт: Facebook, Jabber (XMPP), VK (ВКонтакте), Telegram Desktop.



Чтобы настроить правило:

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

2. В поле **Перехватчик**, выберите **IM Client Monitor**.
3. В поле **Протокол передачи или клиент мгновенных сообщений** выберите тип мессенджера, контролируемого данным правилом:
   - Skype - для контроля использования десктопных приложений Skype версий 7 и 8, а также веб-версии Skype For Web;
   - XMPP - для контроля использования Jabber;
   - MMP - для контроля программ, использующих протокол MMP;
   - Telegram - для контроля использования Telegram;

     Примечание:

     Не поддерживается запрет использования.

     Не поддерживается перехват:

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

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

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

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

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

   - Facebook - для контроля использования Facebook;
   - VK - для контроля использования VK (ВКонтакте);
   - WhatsApp - для контроля использования WhatsApp;

Примечание:

Правило позволяет перехватывать следующие версии WhatsApp:

- десктоп-версию: приложение с официального сайта WhatsApp (whatsapp.com) или из Microsoft Store;
- веб-версию в браузерах: Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium), Яндекс.Браузер, Opera.

Перехват десктоп-версии из Microsoft Store имеет следующие ограничения:

- перехватываются только текстовые сообщения, изображения и вложения;
- не перехватываются: цитаты, пересланные сообщения и аннотации к вложениям;
- не определяется номер телефона отправителя;
- если сотрудник отправляет сообщение в групповой чат:
  - могут быть некорректно определены получатели;
  - событие отправляется на сервер Device Monitor с задержкой до 10 минут;
  - время перехвата в событии может быть позже фактического времени сообщения;
  - идентификатор и название чата могут отсутствовать в событии или иметь некорректное значение;
- возможно появление дубликатов и нарушение порядка сообщений.

Важно!

Перехват не будет осуществляться, если сотрудник вошел в веб-версию WhatsApp:

- когда Агент еще не был установлен;
- когда Агент был отключен;
- когда работал Агент версии ниже 7.8.0.

В этих случаях после запуска новой версии Агента необходимо очистить кеш браузера.

- Яндекс - для контроля использования Яндекс Мессенджера.

Примечание:

Для веб-версии мессенджера могут быть перехвачены:

- текст;
- эмодзи;
- исходящие файлы;
- факты исходящих и входящих звонков.

Поддерживается перехват сообщений в тредах личных и групповых чатов. Тред – это ветка комментариев под отдельным сообщением.

При перехвате сообщения в групповом чате:

- в событии может не быть названия чата. Например, при перехвате отредактированного сообщения или сообщения в треде;
- среди получателей могут присутствовать удаленные или отсутствовать добавленные участники чата;
- до момента открытия группового чата пользователем, в событиях перехвата входящих сообщений будет отсутствовать полный перечень участников чата.

При перехвате исходящего файла, к имени теневой копии файла может быть добавлен текст в формате " `[text]` ".
При пересылке файла из одного чата в другой, событие не будет сформировано, так как будет отсутствовать теневая копия файла.
Отправка файлов в Яндекс Мессенджере осуществляется с помощью облачного хранилища YandexDisk. Поэтому, если активно правило Device Monitor, запрещающее использовать YandexDisk (см. "Правило для Cloud Storage Monitor"), то в Яндекс Мессенджере файлы не будут отправляться.

При перехвате групповых звонков отсутствует информация об участниках (получателях), которые ничего не писали в чат.

При смене типа звонка с личного на групповой не будут сформированы события ни по личному, ни по групповому звонку.

Перехват исходящих и входящих файлов не поддерживается в десктоп-версии.

4. Если требуется перехватывать голосовые сообщения в Skype и создавать события в Traffic Monitor, отметьте поле **Создавать теневую копию голосового трафика** и при необходимости укажите максимальный размер файла (звуковой файл будет сохранен в формате `*.ogg`):
   - если поле **Максимальный размер файла** отмечено, то для разговоров, длительность которых превышает указанное значение, будет создано несколько отдельных событий с теневыми копиями.
5. Если вы хотите полностью запретить использование клиента данного типа, отметьте поле **Запретить использование клиента мгновенных сообщений** (недоступно для мессенджеров **Telegram**, **Facebook**, **WhatsApp**, **VK**, **Яндекс Мессенджер**).

> **Примечание.**
>
> Для Skype настройка работает следующим образом: перехватчик выполняет проверку, запущено ли приложение, и, если приложение запущено, принудительно закрывает его. Проверка выполняется с частотой 1 раз в минуту.

> **Важно!**
>
> Чтобы запретить использование Telegram, Facebook, WhatsApp, VK и Яндекс Мессенджер, необходимо использовать правила Application Monitor: см. "Правило для Application Monitor".

6. Если вы хотите передавать в Traffic Monitor, помимо события, и теневые копии пересылаемых файлов, отметьте поле **Создавать теневую копию исходящих файлов**. В этом случае вы также можете определить дополнительные параметры теневых копий:

- **Минимальный размер файла**. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
- **Максимальный размер файла**. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.

7. Если вы хотите передавать в Traffic Monitor, помимо события, и теневые копии голосовых сообщений, отметьте поле **Создавать теневую копию голосового трафика** и укажите максимальную длительность звукового файла. Для этого в поле **Максимальный размер файла** установите нужное значение в минутах.
8. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
9. После того как вы определите все необходимые параметры, нажмите **Сохранить**.

> **Важно!**
>
> Поля **Минимальный размер файла** и **Максимальный размер файла** 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. Также событие будет сформировано без теневой копии, если на компьютере осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного места").
>
> Если на компьютере действует правило для **IM Client Monitor**, то копии чатов и сообщений создаются всегда, независимо от выбранных настроек **Создавать теневую копию исходящих файлов** и **Создавать теневую копию голосового трафика**. Снятие теневых копий чатов и сообщений настраивается в разделе " Контроль сетевого трафика ".

> **Важно!**
>
> При отправке сообщений в групповой чат WhatsApp, событие будет содержать идентификатор и название группового чата. Список получателей в событии также будет содержать идентификатор чата.
> Если первым сообщением в групповом чате WhatsApp является отправка файла, в списке получателей в событии будет указан только идентификатор чата.
>
> При отправке сообщений в групповой чат Telegram, событие будет содержать идентификатор и название группового чата. Состав участников группового чата на момент отправки сообщения неизвестен. Он определяется путем накопления данных об участниках, которые проявляли перехватываемую активность в чате в течение определенного инженерными настройками времени (см. подробнее "Инженерные настройки агента"), или если пользователь посмотрел состав группового чата.
> Система также обнаруживает удаление участника из группового чата Telegram, если его произвел отслеживаемый пользователь. Однако состав участников изменится только в событиях, получаемых от данного пользователя. В событиях, получаемых от других пользователей, состав остается прежним.

При отправке сообщений в групповой чат Яндекс, событие будет содержать название группового чата. Список получателей в событии будет содержать идентификатор чата в формате "0/0/<chat_ID_part>".
При перехвате тредов в групповых чатах событие будет содержать только идентификатор группового чата в формате "100/0/<chat_ID_part>".

Идентификатор чата можно использовать в запросах для поиска нужных событий (см. "Создание запросов"). Вводить идентификатор нужно с использованием маски: *. Например: d57efb0b486c4*.

Важно!

В Telegram версии 2.4.3 и выше не определяется список отправителей при отправке сообщения в групповой чат от имени администратора группы.

Правило для Keyboard Monitor

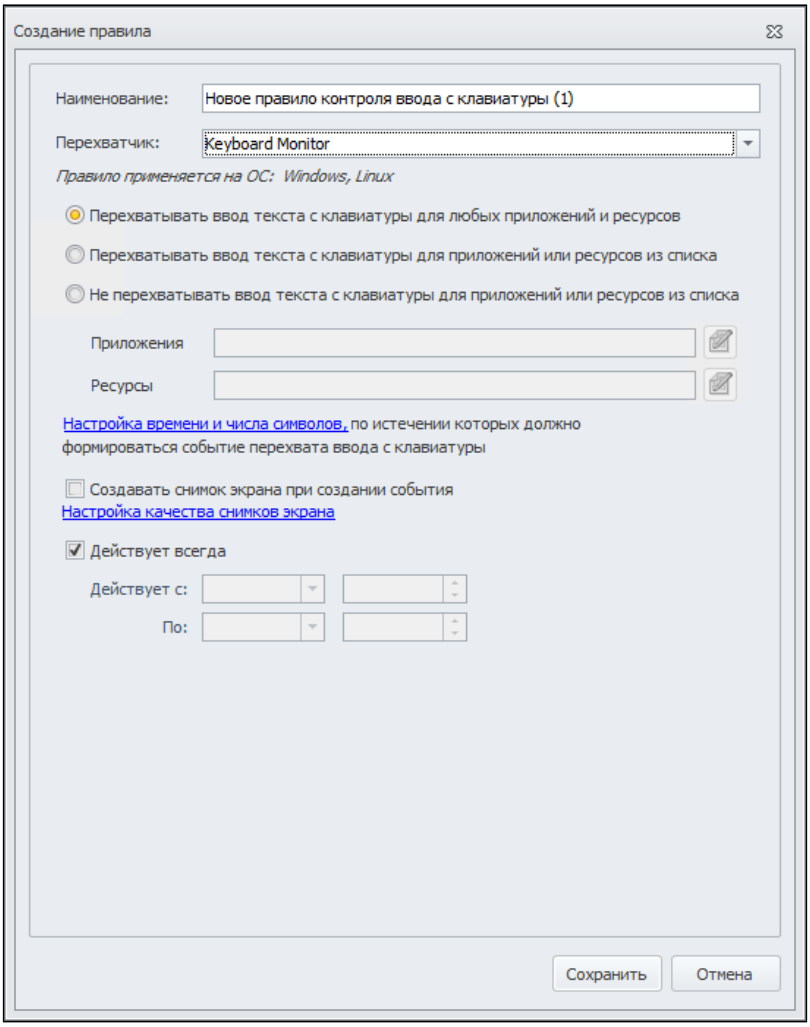
Перехватчик **Keyboard Monitor** позволяет перехватывать ввод текста с клавиатуры на рабочих станциях и создавать события:

- при смене активного окна или вкладок в браузере (для Агентов на ОС семейства Linux – только при смене активного окна);
- по истечении временного интервала, указанного в настройках, с момента окончания ввода;
- при накоплении заданного в настройках количества символов, введенных с клавиатуры;
- при нажатии Enter / Ctrl+Enter / Shift+Enter, если это указано в настройках (см. "Контроль ввода с клавиатуры").

Примечание:

Правило применяется на рабочих станциях под управлением операционных систем MS Windows, ОС Альт Рабочая станция 10, Astra Linux и РЕД ОС.

Далее сформированные из перехваченных данных события будут отправлены в Traffic Monitor для обработки и анализа.



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **Keyboard Monitor**.
3. Определите, в каком случае правило будет действовать. Возможные значения:
   - **Перехватывать ввод текста с клавиатуры для любых приложений и ресурсов**;
   - **Перехватывать ввод текста с клавиатуры для приложений или ресурсов из списка**;
   - **Не перехватывать ввод текста с клавиатуры для приложений или ресурсов из списка**.

> **Примечание:**
>
> Проверка на соответствие посещаемого приложения приложению из списка производится только для Агентов на ОС Windows.
>
> Проверка на соответствие посещаемого ресурса ресурсу из списка производится только для Агентов на ОС Windows и если пользователь работает в браузерах:

- Chrome;
- Яндекс.Браузер;
- Mozilla Firefox;
- Edge (Chromium);
- Opera;
- IE.

Если правило должно действовать только в случае активности определенных приложений или ресурсов, выберите их из списков с помощью кнопки  в полях **Приложения** и **Ресурсы**: см. "Приложения" и "Ресурсы".

4. Если требуется, укажите более точные условия формирования события: см. "Контроль ввода с клавиатуры".
5. Если требуется, укажите настройки качества снимков экрана: см. "Контроль приложений и снимки экрана".

> **Примечание:**
>
> Для получения снимков экрана необходимо, чтобы их отправка была также настроена в разделе **Настройка отправки данных в продукты** (по умолчанию отправка активирована). Если в настройках отправки данных в продукты отключена отправка, а в правиле задано создание снимков экрана, то снимки экрана не будут отправляться. Подробнее см. в статье "Настройка отправки данных в продукты".
>
> Настройка и применение правил ScreenShot Monitor и Keyboard Monitor осуществляются взаимонезависимо. Не учитывается возможное пересечение действия списков ресурсов в настройках включения/исключения при формировании событий и создании снимков экрана. Например, если в правиле ScreenShot Monitor настроено создание снимка всего экрана, а не только активного окна, на снимок может попасть информация из приложений или ресурсов, которые находятся в списке исключений в правиле Keyboard Monitor (но не исключены в правиле ScreenShot Monitor).

6. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
7. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

> **Важно!**
>
> Перехват текста с клавиатуры корректно работает для русского и английского языков. При добавлении других языков требуется перезагрузка рабочей станции.
>
> Если на рабочих станциях вашей компании в ОС используются разные языки интерфейса по умолчанию, например, английский и китайский, то не рекомендуется задавать исключения для правила Keyboard Monitor, используя приложения с атрибутом проверки "**по подробной информации**". В таком случае при создании правила с опцией "**Не перехватывать ввод текста с клавиатуры для приложений или ресурсов из списка**", убедитесь, что используемые приложения из списка имеют один из следующих атрибутов для проверки соответствия:
>
> - **Только по имени приложения**
> - **По расположению**

Подробнее о параметрах, по которым проверяется соответствие приложения см. "Создание и изменение списка приложений".

Примечание:

Для Агента на рабочей станции под управлением ОС 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*".
- Система не перехватывает текст, вводимый в стандартный менеджер текста, если текст начинается со слеша, например "*/sample/text*".

Правило для Mail Monitor

Перехватчик **Mail Monitor** позволяет контролировать отправку и получение электронной почты.

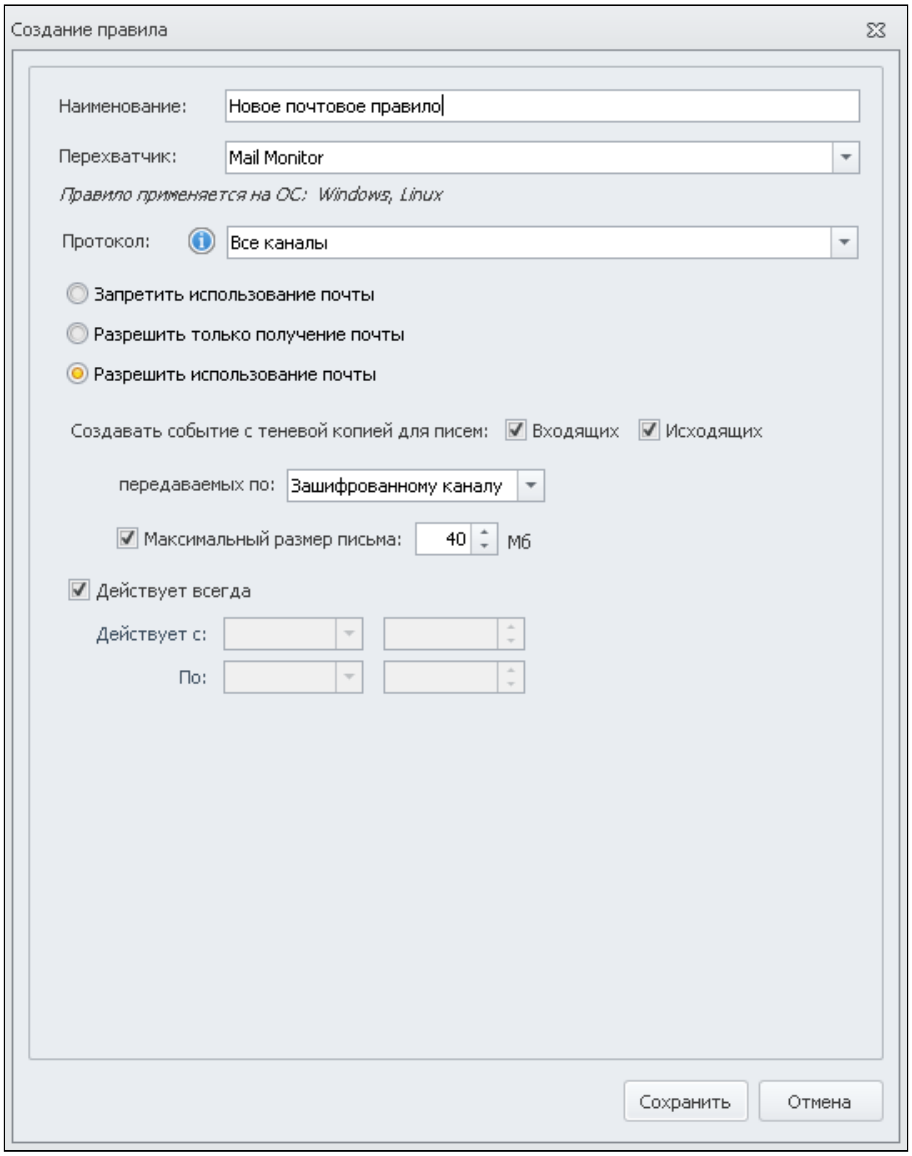
Правило Mail Monitor обеспечивает контроль трафика, передаваемого по протоколам SMTP, IMAP, POP3, Outlook и HTTPS. Для HTTPS контролируется отправка сообщений с помощью следующих сервисов:

- Gmail
- Yandex
- Mail.ru
- Yahoo
- Rambler
- Outlook.com
- VK+ (VK WorkSpace)

Важно!

Правило применяется на компьютерах под управлением операционных систем MS Windows, Astra Linux, РЕД ОС и ОС Альт.

На рабочих станциях под управлением ОС семейства Linux не осуществляется контроль канала Outlook.



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **Mail Monitor**.
3. В поле **Протокол** выберите канал, который должен контролироваться правилом. Возможные значения:
   - **Все каналы**;
   - **SMTP** – только для исходящей почты;
   - **POP3** – только для входящей почты;
   - **Outlook** – как для входящей, так и для исходящей почты;
   - **IMAP** – только для входящей почты;
   - **HTTPS** – только для исходящей почты.

> **Примечание:**

Для перехвата почты VK+ необходимо указать хосты в меню **Инструменты** > **Настройки** > **Перехват веб-почты**.

4. Выберите, какие действия с почтой должны быть доступны пользователю. Возможные значения:
   - **Запретить использование почты**;
   - **Разрешить только получение почты** – доступно только если в поле **Протокол** выбрано *Outlook* или *Все каналы*;
   - **Разрешить использование почты**.

   В строке **Создавать событие с теневой копией для писем** укажите, для каких писем требуется создать теневую копию. В зависимости от канала, выбранного на шаге 6, вы можете указать следующие значения:
   - для каналов **POP3** и **IMAP** – доступно только направление **Входящие**;
   - для **SMPT** и **HTTPS** – доступно только направление **Исходящие**;
   - для **Outlook** или **Все каналы** – доступны направления **Входящие** и **Исходящие**. Вы можете выбрать одно или оба значения.

   Важно!

   В правиле с атрибутом **Разрешить использование почты** должно быть выбрано создание теневой копии хотя бы одного из направлений почты (**Входящие** или **Исходящие**), иначе сохранить правило не удастся.

   Вы также можете определить дополнительные параметры создания теневых копий:
   - В поле **передаваемых по** укажите, требуется ли создавать теневые копии для сообщений, передаваемых по всем каналам или только по зашифрованным. Для протокола HTTPS значение **Всем каналам** недоступно.
   - **Максимальный размер письма**. Если поле отмечено, то теневое копирование будет выполняться только для писем, размер которых меньше либо равен указанному.

     Об особенностях создания теневых копий см. раздел "События перехвата" ниже.
5. Настройте период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы указать другой период действия, снимите отметку и в полях **Действует с** и **По** укажите требуемый период.
6. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Пример:

Для перехвата почты Outlook по протоколам IMAP, SMTP, POP3 на сетевом уровне:

1. Отмените исключение **Outlook** из сетевого перехвата (см. "Исключение приложений из перехвата"). Данная опция включена по умолчанию.
2. Создайте правила для перехвата по этим протоколам, как описано выше.
3. Удалите правило для протокола Outlook/MAPI.

Важно!

При включении Outlook в сетевой перехват возможна некорректная работа с почтовым сервером MS Exchange.

Применение политик Traffic Monitor

На рабочих станциях под управлением ОС семейства Linux блокировка по результатам анализа в Traffic Monitor применяется только к исходящему трафику (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.
- Если действующее правило имеет параметры:
  - **Разрешить использование почты**;
  - **Создавать теневую копию для писем: Входящие и Исходящие, передаваемые по: Всем каналам**.

  и в почтовой программе настроено хранение на сервере (например, в MS Outlook выбрано **Сохранять отправленные элементы в следующей папке на сервере** в окне **Настройки электронной почты Интернета** на вкладке **Отправленные**), то для каждого события отправки сообщения отображаются два объекта перехвата: одно с типом **Исходящее**, другое – **Входящее**. В зависимости от программы название опции может меняться.
- Если на компьютере осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного места"), то письмо передается без создания теневой копии.
- В теневой копии события веб-почты отображаются 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.

Правило для Network Monitor

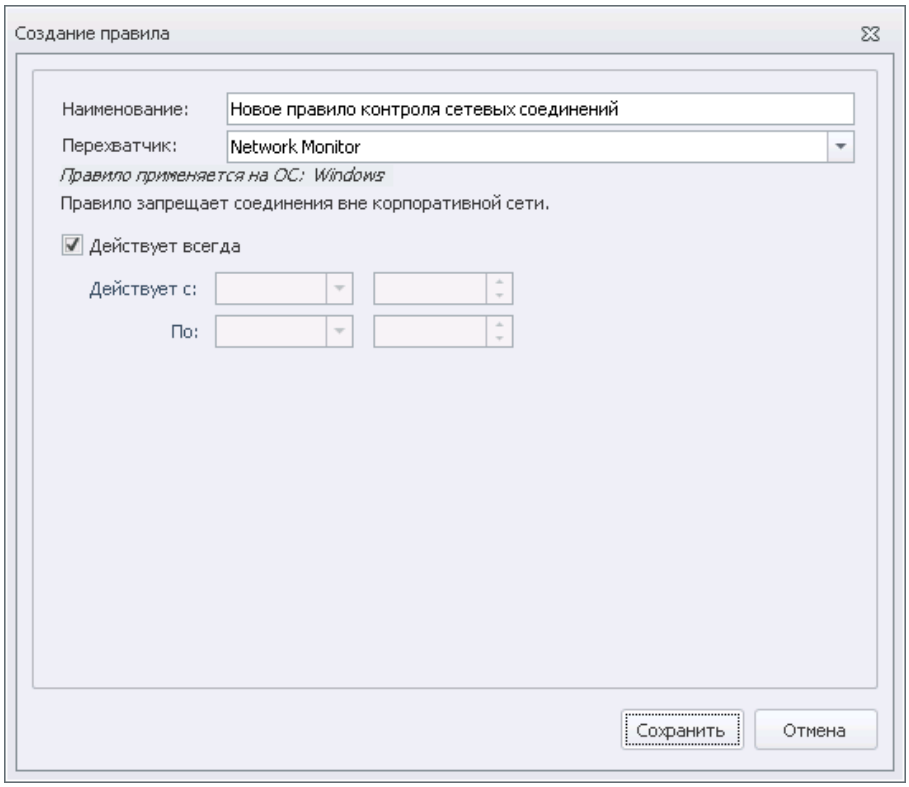
Перехватчик Network Monitor позволяет запрещать передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами. Определение сегментов корпоративной сети и разрешенных внешних адресов выполняется, как описано в разделе "Контроль сетевых соединений".

Примечание.

Правило применяется на компьютерах под управлением операционной системы MS Windows.

Важно!

После того, как в действие вступит хотя бы одно правило Network Monitor, Агент Device Monitor, установленный на компьютере, будет пытаться разрешать DNS-имена открываемых интернет-страниц. Поэтому для исключения проблем с внешними соединениями необходимо на корпоративном DNS-сервере настроить использование серверов пересылки: подробнее см. интернет-статью "Настройка DNS-сервера для использования серверов пересылки".



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **Network Monitor**.
3. Настройте период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
4. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Правило для Print Monitor

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

Примечание:

Правило применяется на компьютерах под управлением операционных систем MS Windows, Astra Linux, РЕД ОС, ОС Альт и macOS.

Агент на ОС Astra Linux, РЕД ОС и Mac OS при перехвате печати в некоторых случаях может создавать несколько событий. Такая ситуация может возникнуть, если задание печати было передано через несколько серверов печати и было на них перехвачено с большими временными интервалами.

Если сервер печати и Агент Device Monitor установлены на ОС Astra Linux, РЕД ОС или ОС Альт:

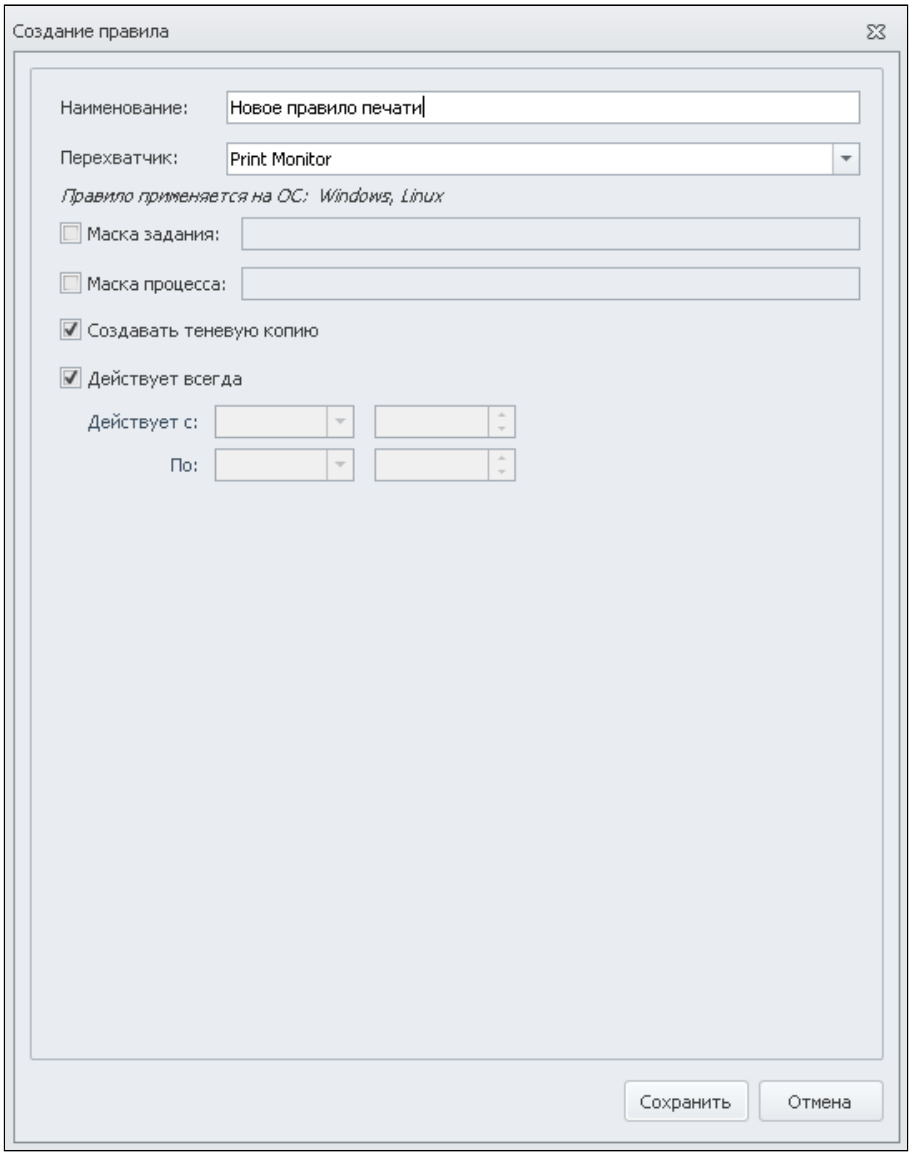
- не определяется пользователь, отправивший файл на печать;
- не определяется количество страниц в теневой копии;
- не осуществляется перехват документов, отправленных на печать через терминальную сессию;
- возможно изменение формата теневых копий перехваченных событий печати.

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.



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **Print Monitor**.
3. При необходимости вы можете ограничить контролируемые задания на печать с помощью масок:
   - **Маска задания**. Использование маски для задания (документа), выводимого на печать. Если требуется указать маску задания, то отметьте данное поле и укажите маску задания.
     В маске задания можно использовать подстановочные символы: «?» для замены одного символа или «*» для замены набора символов. Знак пробела интерпретируется как часть имени задания.

     Важно!

Наименование задания печати формируется приложением, из которого документ передается на печать. Поэтому наименование может представлять собой любую текстовую строку, в том числе вообще не связанную с типом и именем распечатываемого документа.

- **Маска процесса**. Использование маски для процесса, который выводит задание на печать. Если нужно задать маску процесса, отметьте данное поле и укажите маску процесса.
  Имя (полный путь) процесса будет получено для процесса, в контексте которого осуществляется рендеринг задания печати. В некоторых случаях (локальные LPT- и COM-принтеры) подсистема печати может осуществлять рендеринг в контексте службы Диспетчер очереди печати (Print Spooler). Путь к исполняемому файлу службы: `%SystemRoot%\system32\spoolsv.exe`.
  Для того чтобы имя процесса определялось корректно, необходимо в свойствах принтера установить параметр **Печатать прямо на принтер** (**Свойства принтера** > **Дополнительно**). Тогда обработка задания печати будет осуществляться в контексте приложения, из которого документ был отправлен на печать. Однако в этом случае печать будет происходить синхронно, т.е. работа с приложением будет невозможна до окончания печати.
  При задании маски процесса можно использовать подстановочные символы: «?» для замены одного символа или «*» для замены набора символов. Знак пробела интерпретируется как часть имени процесса.

4. Если вы хотите передавать на Traffic Monitor теневые копии печатаемых документов, отметьте поле **Создавать теневую копию**.

> **Важно!**
>
> Если на компьютере осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного места"), то печать будет осуществляться без создания теневой копии.

5. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
6. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Пример:
Для перехвата задания на печать файла с расширением `.txt` с помощью программы `notepad.exe`:

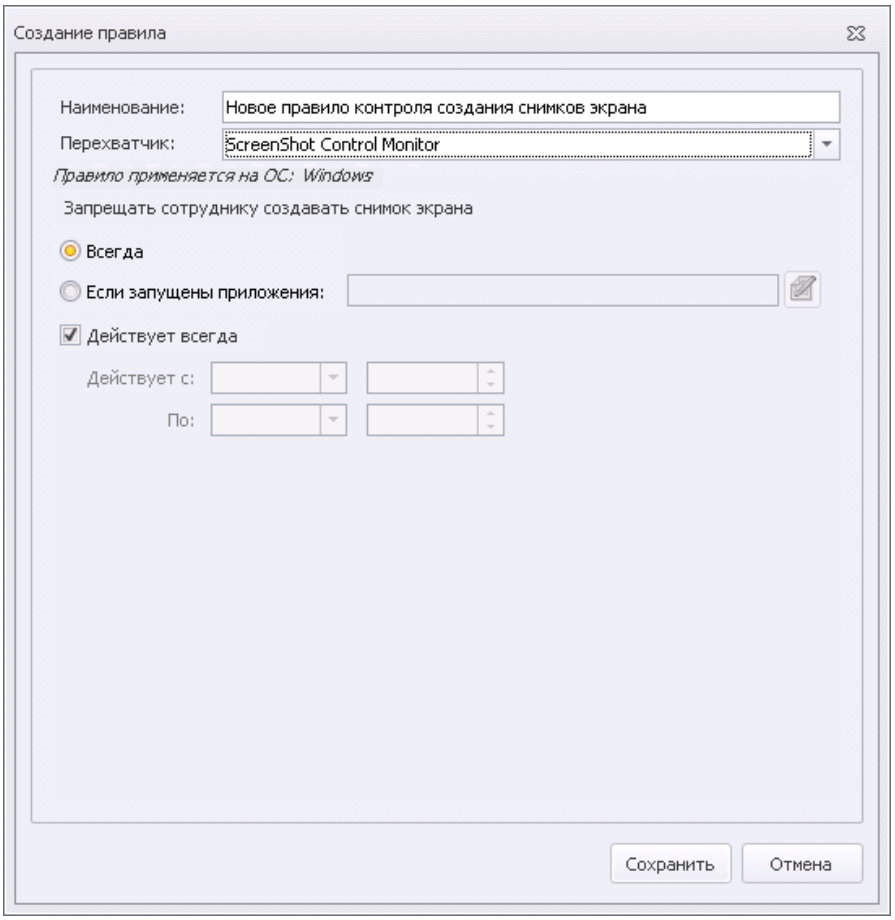
1. В строке Маска задания введите `*.txt*`
2. В строке Маска процесса введите `*nodepad.exe`

> **Важно!**
>
> Задания на печать будут перехватываться при условии, что в операционной системе пользователя отображаются расширения файлов (в Параметрах папок снят флажок в поле **Скрывать расширения для зарегистрированных типов файлов**).

Правило для ScreenShot Control Monitor

Перехватчик **ScreenShot Control Monitor** позволяет осуществлять контроль снимков экрана со стороны агента.

> **Примечание.**
>
> Правило применяется на компьютерах под управлением операционной системы MS Windows.



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **ScreenShot Control Monitor**.
3. В области **Запрещать сотруднику создавать снимок экрана** определите, в каком случае накладывается запрет. Возможные значения:
   - **Всегда**;
   - **Если запущены приложения**. Если выбрана эта опция, нажмите , чтобы указать приложения (см. "Приложения").
4. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
5. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Правило для ScreenShot Monitor

Перехватчик **ScreenShot Monitor** позволяет автоматически создавать снимки экрана на контролируемых компьютерах.

Примечание.

Правило применяется на компьютерах под управлением MS Windows, РЕД ОС, ОС Альт и ОС Astra Linux.

Примечание:

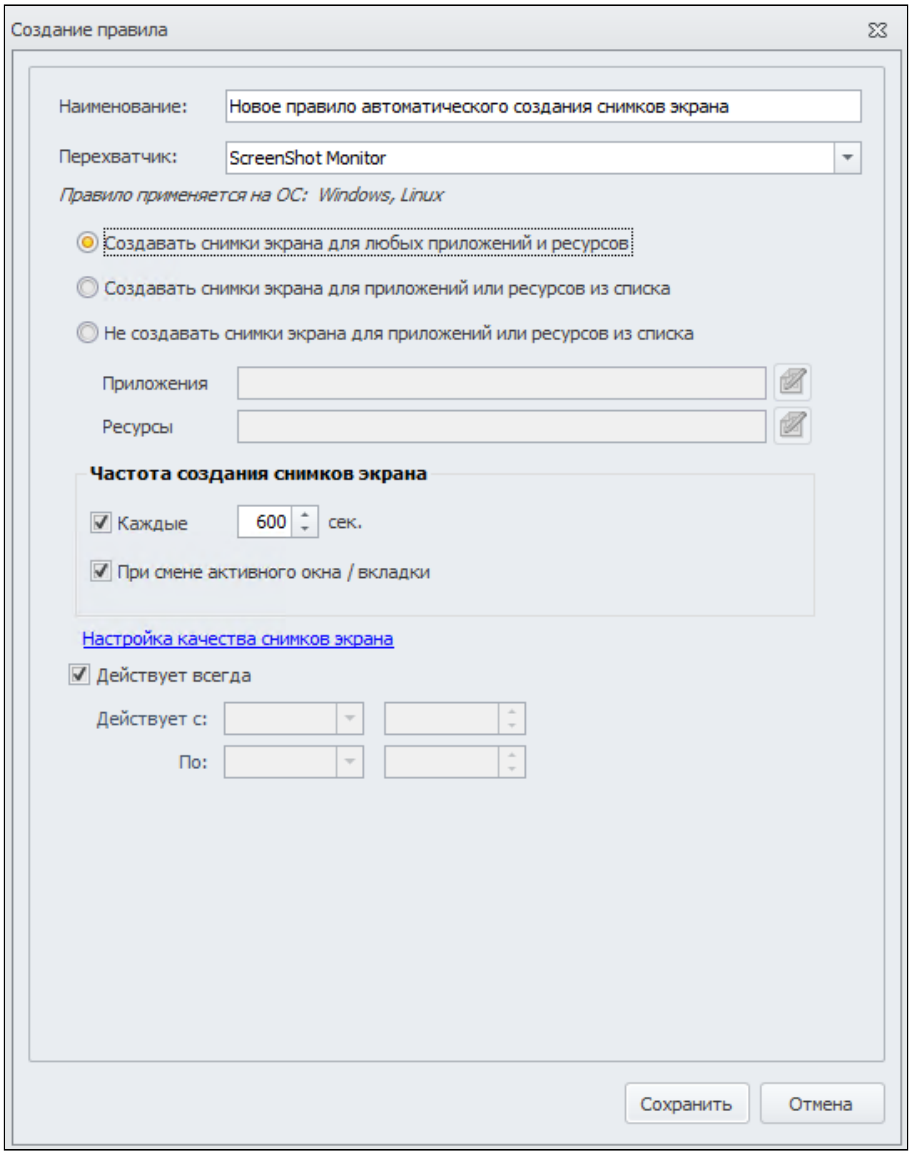
Настройте правило Statistics (см. "Правило для Statistics"), чтобы отправлять события со снимками экрана в InfoWatch Activity Monitor.

Важно!

Создание снимков экрана при копировании данных в буфер обмена или вставке из буфера обмена настраивается в правиле Clipboard Monitor (см. "Правило для Clipboard Monitor"). Создание снимков экрана при перехвате ввода текста с клавиатуры на рабочих станциях настраивается в правиле Keyboard Monitor (см. "Правило для Keyboard Monitor").

Важно!

Параметр **Не создавать снимок экрана, если долгое время нет активности от мыши или клавиатуры**, определяющий работу правила в зависимости от активности на контролируемых компьютерах, настраивается вместе с общими настройками схемы безопасности: см. "Контроль приложений и снимки экрана".



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **ScreenShot Monitor**.
3. Определите, в каком случае правило будет действовать. Возможные значения:
   - **Создавать снимки экрана для любых приложений и ресурсов**;
   - **Создавать снимки экрана для приложений или ресурсов из списка**;
   - **Не создавать снимки экрана для приложений или ресурсов из списка**.

> **Важно!**
>
> Для получения снимков экрана необходимо, чтобы их отправка была также настроена в разделе **Настройка отправки данных в продукты** (по умолчанию отправка активирована).

Если в настройках отправки данных в продукты отключена отправка, а в правиле задано создавать снимки экрана, то снимки экрана не будут отправляться. Подробнее см. в статье "Настройка отправки данных в продукты".

Если правило должно действовать только в случае активности определенных приложений или ресурсов, выберите их из списков с помощью кнопки  в полях **Приложения** и **Ресурсы**: см. "Приложения" и "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.

Важно!

Для рабочих станций под управлением РЕД ОС, ОС Альт и ОС Astra Linux поддерживается только опция **Создавать снимки экрана для любых приложений и ресурсов**. Списки приложений и ресурсов не поддерживаются.

4. В поле **Частота создания снимков экрана** укажите, когда необходимо создавать снимки экрана:
   - **Каждые n секунд**;
   - **При смене активного окна/вкладки**.

   Важно!

   На рабочих станциях под управлением РЕД ОС и ОС Astra 1.8 Система может определить только смену активного окна. Смена вкладки браузера не определяется.

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

5. Если требуется, укажите настройки качества снимков экрана: см. "Контроль приложений и снимки экрана".
6. Определите период действия правила. По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
7. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Важно!

Снимок 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.

Важно!

Если на рабочих станциях вашей компании в ОС используются разные языки интерфейса по умолчанию, например, английский и китайский, то не рекомендуется задавать исключения для правила ScreenShot Monitor, используя приложения с атрибутом проверки "**по подробной информации**". В таком случае при создании правила с опцией "**Не создавать снимки экрана для приложений или ресурсов из списка**", убедитесь, что используемые приложения из списка имеют один из следующих атрибутов для проверки соответствия:

- **Только по имени приложения**
- **По расположению**

Подробнее о параметрах, по которым проверяется соответствие приложения см. "Создание и изменение списка приложений".

Важно!

Для Агента на ОС Windows настройка и применение правил ScreenShot Monitor и Keyboard Monitor осуществляются взаимонезависимо. Не учитывается возможное пересечение действия списков ресурсов в настройках включения/исключения при формировании событий и создании снимков экрана. Например, если в правиле ScreenShot Monitor настроено создание снимка всего экрана, а не только активного окна, на снимок может попасть информация из приложений или ресурсов, которые находятся в списке исключений в правиле Keyboard Monitor (но не исключены в правиле ScreenShot Monitor).

Примечание:

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

Правило для Screen Record Video

Важно!

Функциональность предназначена только для InfoWatch Activity Monitor.

Device Monitor версии 7.18.X совместим с Activity Monitor версии 3.4.X. Не поддерживается совместимость Device Monitor версии 7.18.X с более ранними версиями Activity Monitor.

Перехватчик **Screen Record Video** позволяет отслеживать действия сотрудника с помощью записи видео экрана рабочей станции. В случае, если сотрудник использует ресурсы из списка контролируемых, срабатывает правило и производится видеозапись.

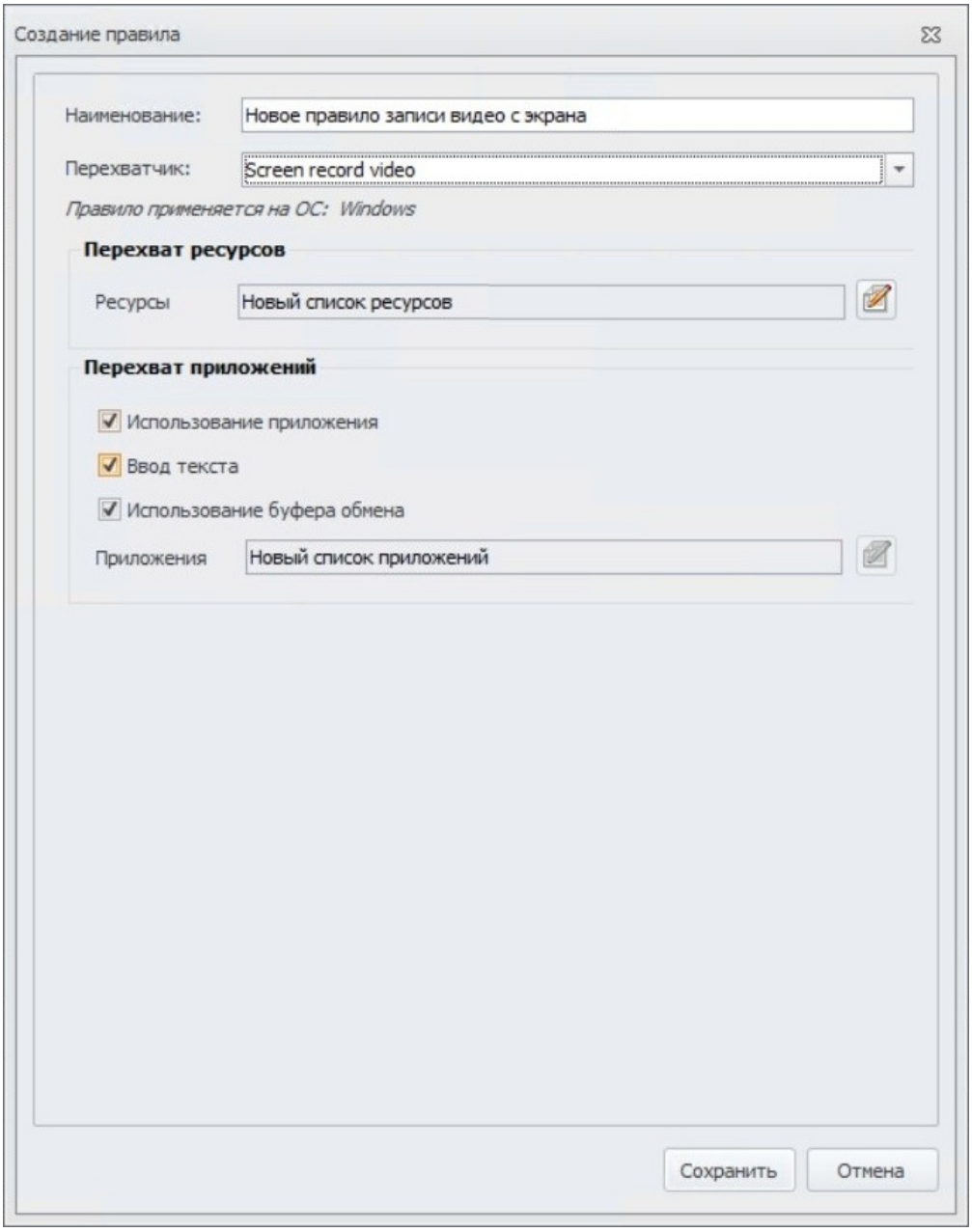
Примечание.

Правило применяется на компьютерах под управлением операционной системы MS Windows.

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

Примечание:

Для создания и отправки событий видеозаписи в Activity Monitor необходимо также настроить "Правило для Statistics".



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **Screen Record Video**.
3. В поле **Ресурсы** нажмите , чтобы указать ресурсы, при использовании которых должно срабатывать правило (см. "Ресурсы").
4. В области **Перехват приложений** выберите условия срабатывания правила:
   - Использование приложения;
   - Ввод текста;
   - Использование буфера обмена.
5. В поле **Приложения** нажмите , чтобы указать приложения, при использовании которых должно срабатывать правило.
6. Нажмите **Сохранить**.

Примечание:

- Производится видеозапись только основного монитора.
- Продолжительность одной видеозаписи равна примерно 5 минутам.
- 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 вы можете настроить в отдельном правиле "Правило для Audio Record Control".
- 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.
Если выбран перехват приложений при "Вводе текста"	
запись 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.	запись не производится при нажатии в поле ввода: • клавиш навигации, например, PgUp, PgDown, Home и т.д.; • клавиш F1-F12; • клавиши Delete; • сочетаний клавиш, которые обращаются не к приложению, например, Alt + F4.

Правило для Statistics

Чтобы получать статистику о:

- активности персон,
- действиях персон с файлами/папками,
- событиях печати,

необходимо произвести настройки в Device Monitor. Для этого существует правило Device Monitor для Statistics. Перехватчик **Statistics** позволяет собирать статистику об активности пользователя и действиях с файлами/папками, а также событиях печати на контролируемых компьютерах.

Примечание:

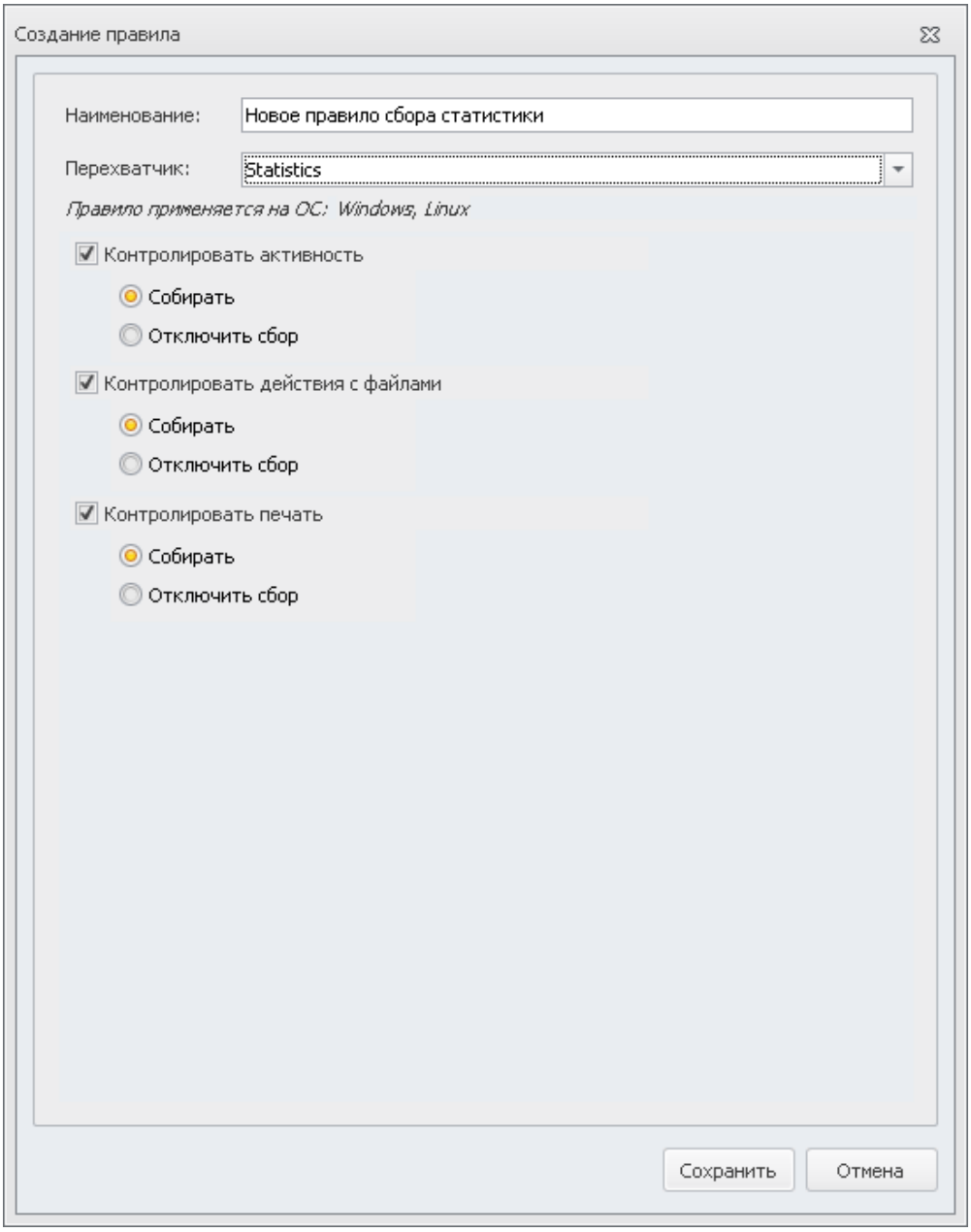
Правило применяется на компьютерах под управлением операционных систем MS Windows, РЕД ОС, ОС Альт и ОС Astra Linux.

Важно!

Функциональность предназначена для InfoWatch Activity Monitor и InfoWatch Prediction.

Device Monitor версии 7.18.X совместим с Activity Monitor версии 3.4.X. Не поддерживается совместимость Device Monitor версии 7.18.X с более ранними версиями Activity Monitor.

Для срабатывания правила версия Агента должна быть не ниже версии сервера Device Monitor.



В рамках данного правила вы можете выбрать тип статистики, которую хотите собирать. Например, собирать статистику активности пользователя и не собирать статистику действий с файлами и печати. Если параметр **Контролировать активность** / **Контролировать действия с файлами** / **Контролировать печать** не активирован, контроль данного типа статистики осуществляться не будет.

Примечание:

Если параметр **Контролировать активность** не активирован, то события, сформированные в Device Monitor, не отправляются в Платформу.

Если вы хотите, чтобы какие-либо события (например, события создания снимков экрана по Правилу для ScreenShot Monitor) отправлялись в Платформу, даже если параметр **Контролировать активность** не активирован, задайте значение `False` полю `SEND_EVENT_TO_PLATFORM_WITH_CHECK` таблицы Settings Базы Данных. По умолчанию данное поле имеет значение `True`.

Контроль активности пользователя

Система контролирует следующие действия пользователя в Системе:

- Вход в сессию (локальный, удаленный);
- Выход из сессии (локальный, удаленный);
- Блокировка сессии (локальная, удаленная);
- Разблокировка сессии (локальная, удаленная);
- Запуск приложения;
- Остановка приложения;
- Получение фокуса активного окна приложения;
- Потеря фокуса активного окна приложения;
- Получение фокуса вкладкой браузера. Сбор статистики по работе с сайтами в браузерах поддерживается для следующих браузеров:
  - Chrome;
  - Яндекс.Браузер;
  - Mozilla Firefox;
  - Edge (Chromium);
  - Opera;
  - IExplore.
- Выполнение поисковых запросов. Поддерживается для:
  - Google;
  - Яндекс.
- Использование мыши и клавиатуры.

Примечание:

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 вкладкой браузера (для браузера Edge (Chromium)).

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*.

Примечание:

- Если URL-адрес был изменен (без применения или отмены изменений при помощи клавиш **Enter** или **Esc**), то будет создано событие смены вкладки браузера на Агентах, работающих на РЕД ОС.
- Если сайт был добавлен из вкладки браузера в закладки, создается событие смены вкладки браузера на Агентах, работающих на РЕД ОС.
- Если URL был изменен, может быть создано несколько событий смены вкладки браузера на Агентах, работающих на РЕД ОС.
- Событие *Локального выхода из сессии* на РЕД ОС возможно не будет 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 на Агентах под управлением ОС Windows.

Сбор статистики по работе с файлами производится для следующих источников:

- Компьютер;
- Съемные устройства;
- Сетевые устройства;
- Терминальная сессия.

Важно!

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

Система контролирует следующие действия:

- 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 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.
- Если в Системе одновременно настроено правило запрета снимков экрана "Правило для ScreenShot Control Monitor" и сбор статистики, то при нажатии клавиши **Print Screen** будет сформировано только событие отпускания клавиши.
- События получения/потери фокуса для UWP (Universal Windows Platform) приложений возможно не будут 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 Система не может определить оригинальное имя файла при удалении его из корзины, в событии будет указано имя файла, отображаемое в корзине. Оригинальное имя файла – 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.

Контроль печати

Сбор статистики по файлам, отправленным на печать, производится для следующих типов принтеров:

- Локальный;
- Сетевой;
- Терминальный.

Важно!

Контроль печати доступен только на Агентах под управлением ОС Windows.

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.

Чтобы настроить правило:

1. В Консоли управления Device Monitor выберите раздел **Политики**.
2. В области **Правила** откройте  окно создания правила (подробнее см. "Создание правил").
3. В поле **Наименование** укажите название правила.
4. В поле **Перехватчик** выберите **Statistics**.
5. Выберите **Контролировать активность**, чтобы активировать контроль активности пользователя (параметр включен по умолчанию).
6. Выберите, **Собирать** или **Отключить сбор** статистики (по умолчанию сбор осуществляется).
7. Выберите **Контролировать действия с файлами**, чтобы активировать контроль действий пользователя с файлами (параметр включен по умолчанию).
8. Выберите, **Собирать** или **Отключить сбор** статистики (по умолчанию сбор осуществляется).
9. Выберите **Контролировать печать**, чтобы активировать контроль файлов, отправляемых пользователем на печать (параметр включен по умолчанию).
10. Выберите, **Собирать** или **Отключить сбор** статистики (по умолчанию сбор осуществляется).
11. Нажмите **Сохранить**.

Важно!

Правила всех политик, назначенных на рабочую станцию и сотрудника, объединяются. Правила с разными типами статистики а также параметрами включения/выключения объединяются. Если в одном правиле настроен контроль активности, а в другом контроль работы с файлами, то на компьютере применяются оба правила и контроль осуществляется как для активности пользователя, так и для его действий с файлами.

Чтобы указать явный запрет на сбор статистики (например, для определенной группы сотрудников или компьютеров), выберите **Отключить сбор**. При этом в результирующем правиле сбор будет запрещен, так как при объединении правил, действующих для рабочих станций и сотрудников, приоритетным будет то, в котором сбор отключен.

Пример 1

Для группы компьютеров настроен сбор статистики, но если на компьютере из данной группы авторизуется сотрудник из группы, для которой сбор запрещен, события не будут создаваться.

Пример 2

Для пользователя действуют несколько правил.

В правиле 1

- Включен контроль статистики активности пользователя;
- Включен сбор статистики активности пользователя;
- Отключен контроль действий с файлами.

В правиле 2

- Отключен контроль статистики активности пользователя;

- Включен контроль действий с файлами;
- Отключен сбор статистики действий с файлами.

В правиле 3

- Включен контроль активности пользователя;
- Включен сбор статистики активности пользователя;
- Включен контроль действий с файлами;
- Включен сбор статистики действий с файлами.

В результирующем правиле для этого пользователя будет осуществляться сбор статистики активности, и не будет производиться сбор статистики действий с файлами.

Подробнее о настройке схемы безопасности, политиках и правилах Device Monitor см. "Настройка схемы безопасности".

Настройка конфигурации файловой статистики производится в разделе "Файловая статистика".

Примечание:

Размер файла определяется после окончания работы приложения с файлом (в момент создания события). Для действия по удалению файла указывается размер при его открытии.

Данные о размере файла извлекаются из контекста файлового объекта. Если Система не получила эти данные, в значении размера файла будет указано значение 0. Для оригинальных файлов размера 0 событие не будет создано.

Важно!

На Агентах версий до 7.6.0 правила статистики активности будут работать только для компьютеров. Правила, назначенные на группу сотрудников, будут проигнорированы.

Применение правил

Событие считается удовлетворяющим правилу, если оно соответствует всем параметрам, указанным в правиле.

Если событие соответствует нескольким правилам одновременно, то приоритет определяется следующим образом:

1. Правило, исключающее из перехвата (опция **Исключить из перехвата** доступна для правила File Monitor), имеет наивысший приоритет.
2. Правило полного доступа имеет приоритет перед запрещающим, в то время как запрещающее правило имеет приоритет перед разрешающим только чтение и доступ на зашифрованные носители.
   Пример 1. Для Device Monitor правило *Использование разрешено* имеет приоритет над ограничением *Нет доступа*, которое в свою очередь имеет приоритет по сравнению с правилом, разрешающим *Только чтение*, а оно, соответственно, более приоритетно чем правило, где выбран *Полный доступ только к зашифрованным устройствам*.
   Пример 2. Если задано несколько правил HTTP(S) Monitor, то правило с включенной опцией *Не перехватывать запросы на внутренние ресурсы* имеет больший приоритет, чем правило, для которого данная опция не выбрана.

3. Правило, в котором отмечена опция **Создавать теневую копию**, имеет приоритет перед правилом без теневой копии.

См. также:

- Особенности применения правил для Device Monitor
- Создание теневых копий и запрет операций при нехватке свободного места

Создание теневых копий и запрет операций при нехватке свободного места

Теневая копия файла, документа, сообщения или чата создается в случае, если выполнены следующие условия:

1. В правиле, под действие которого попадает файл, установлена отметка о создании теневой копии, и размер файла входит в диапазон, указанный в правиле.
2. На контролируемом компьютере имеется больше свободного места, чем указано в значении параметра **Критический остаток места на диске** (см. "Общие настройки работы Агентов"). Значение по умолчанию - 10 ГБ.
3. На контролируемом компьютере больше свободного места, чем необходимо для создания теневой копии.

Примечание:

Если в правиле задано создание теневой копии, но на компьютере осталось меньше свободного места, чем определено политикой или чем требуется для сохранения файла, то событие будет создано без теневой копии. Для таких событий в Консоли управления отображается состояние "*Ошибка создания копии*" (см. "Просмотр событий").

Важно!

При перехвате печати Агент сохраняет поток в файле EMF-формата. При размере этого файла более 512 МБ теневая копия обрезается. Пользователю будет доступна только часть распечатанного файла.

Помимо теневых копий, на компьютере временно (до установления соединения с сервером Device Monitor) сохраняется информация о событиях. Для этого на диске компьютера, где установлен Агент Device Monitor, выделяется место, достаточное для хранения информации о 30000 событиях (около 300 МБ).

Вариант 1

Если:

- Места на диске достаточно, но Агент Device Monitor долго не имел связи с сервером Device Monitor, в результате чего накопилось 30000 или более событий, и
- в общих настройках работы Агентов для параметра **Если место под события на диске закончилось** установлено значение **Запрещать операции**,

то действия сотрудника, для которых в текущей политике действуют правила, содержащие запрет, будут заблокированы.

Вариант 2

Если:

- Переполнилось место на диске, при этом количество событий меньше 30000, и

- в общих настройках работы Агентов для параметра **Если место под события на диске закончилось** установлено значение **Запрещать операции**,

то действия сотрудника, для которых в текущей политике действуют правила, содержащие запрет, будут заблокированы.

Особенности применения правил для Device Monitor

Доступ ко всем периферийным устройствам, контролируемым перехватчиком Device Monitor, определяется совокупностью правил, назначенных каждому из этих устройств.

При определении прав доступа сотрудника к какому-либо устройству учитываются:

- правила, распространяющиеся на группы сотрудников, в которые входит сотрудник;
- правила, распространяющиеся на группы компьютеров, в состав которых включен компьютер, используемый для доступа к устройству;
- белые списки.

При установке Агента доступ к контролируемым устройствам по умолчанию разрешен. Поэтому каждая запрещенная операция для устройства должна быть задана явно в виде правила.

Каждый новый зарегистрированный компьютер попадает в группу компьютеров по умолчанию. Этой группе назначена *Политика на устройства*, не содержащая ни одного правила. Для сотрудников по умолчанию правила работы с устройствами не определены.

Таким образом, после установки доступ ко всем контролируемым устройствам по умолчанию разрешен.

Пример:

> Для группы компьютеров *A* задано правило, запрещающее запись CD/DVD дисков. Сотрудник входит только в группу сотрудников *B*, для которой не определены правила работы с устройствами, а его компьютер входит в группу компьютеров *A*. Сотрудник пытается просмотреть содержимое компакт-диска на своем компьютере. В этом случае сотрудник не сможет просматривать содержимое диска и записывать новую информацию на диск.

Вы можете назначить с помощью Консоли управления несколько правил, в том числе и в разных политиках, с разным уровнем доступа на одно и то же устройство. В этом случае более приоритетным будет разрешающее правило (подробнее см. таблицу ниже).

Тип устройства	Доступ в порядке убывания приоритета
Все устройства, кроме CD/DVD, Floppy и съемных устройств хранения	1. Использование разрешено 2. Использование запрещено
CD/DVD	1. Использование разрешено 2. Нет доступа 3. Только чтение
Floppy и съемные устройства хранения	1. Использование разрешено 2. Нет доступа 3. Только чтение 4. Полный доступ только к зашифрованным устройствам
Облачные хранилища	1. Нет доступа

Тип устройства	Доступ в порядке убывания приоритета
	2. Только чтение 3. Использование разрешено

Пример:

> Для группы сотрудников *E* действует правило, предоставляющее доступ к съемному устройству хранения только для чтения. Для группы сотрудников *F* действует правило, разрешающее полный доступ только к зашифрованному съемному устройству хранения. Сотрудник *Иванов*, входящий в обе группы, сможет получить доступ к съемным устройствам только на чтение: причем как к зашифрованным, так и к незашифрованным, так как правило с меньшим приоритетом не учитывается.

Для некоторых типов устройств, контролируемых перехватчиком Device Monitor, правила могут пересекаться (см. таблицу ниже). Это нужно учитывать при настройке доступа к контролируемому устройству.

Правило	Пересекающиеся правила	Примечание
Флоппи-дисковод	Нет	
CD/DVD	Нет	
Параллельный порт (LPT)	Локальный принтер (LPT) Устройства работы с изображениями (LPT)	При запрете на использование LPT-порта взаимодействие с устройством, подключенным к этому порту, будет невозможно
Последовательный порт (COM)	Модем Локальный принтер (COM) Устройства работы с изображениями (COM)	Доступ к модему, подключенному через COM-порт, определяется только правилом использования COM-порта При запрете на использование COM-порта взаимодействие с устройством, подключенным к этому порту, будет невозможно
Съемное устройство хранения (устройства, подключаемые через интерфейсы USB, IEEE 1394)	FireWire (IEEE 1394)	При запрете на использование порта FireWire (IEEE 1394) взаимодействие с подключенным к порту устройством становится невозможным
Локальный принтер (подключаемый через интерфейс USB, IEEE 1394, SCSI и пр.)	FireWire (IEEE 1394) Последовательный порт (COM) Параллельный порт (LPT)	При запрете на использование порта FireWire (IEEE 1394), COM, LPT взаимодействие с подключенным к этому порту устройством становится невозможным

Правило	Пересекающиеся правила	Примечание
Устройства работы с изображениями (видеокамеры, сканеры)	FireWire (IEEE 1394) Последовательный порт (COM) Параллельный порт (LPT)	При запрете на использование FireWire (IEEE 1394), COM, LPT порта взаимодействие с устройством, подключенным к этому порту, будет невозможно
Bluetooth устройство	Нет	
IrDA устройство	Нет	
Другое USB устройство	Нет	
FireWire	Съемное устройство хранения (IEEE 1394) Локальный принтер (IEEE 1394) Устройства работы с изображениями (IEEE 1394)	При запрете на использование порта FireWire (IEEE 1394) взаимодействие с устройством, подключенным к этому порту, будет невозможно
Модем	Последовательный порт (COM)	Правила, определяющие доступ к модему, не распространяются на модемы, подключаемые через COM-порт. Возможность доступа к модему, подключенному через COM-порт, определяется только правилами использования COM-порта
Считыватель смарт-карт (Smart Card Reader)	Нет	
Ленточный накопитель	Нет	
Многофункциональное устройство	Нет	
PCMCI устройство	Нет	
Сетевой адаптер USB	MTP совместимое устройство	Мобильный телефон при подключении к компьютеру может быть определен как MTP-устройство или как сетевой адаптер USB
Сетевой принтер	Нет	

Правило	Пересекающиеся правила	Примечание
КПК (карманные компьютеры под управлением операционных систем Windows Mobile и Palm OS)	Нет	
MTP совместимое устройство	Сетевой адаптер USB	Мобильный телефон при подключении к компьютеру может быть определен как MTP-устройство или как сетевой адаптер USB

Настройка правил Device Monitor для сбора данных статистики и перехвата событий

Важно!

Данные статистики могут использоваться InfoWatch Activity Monitor и InfoWatch Prediction.

Чтобы активировать сбор статистических событий с помощью InfoWatch Device Monitor, настройте правила в Консоли управления DM:

- Правило для Keyboard Monitor;
- Правило для ScreenShot Monitor;
- Правило для Statistics.

Примечание:

Перехват статистики событий клавиатуры и перехват набора с клавиатуры являются разными событиями, которые настраиваются и могут работать как отдельно, так и вместе. Статистика событий клавиатуры необходима для подсчёта активного времени работы пользователя. События набора с клавиатуры необходимы для перехвата текста, набираемого на клавиатуре.

Статистические события, собираемые DM:

- События сессии пользователя:
  - Вход в сессию (локальный, удаленный)
  - Выход из сессии (локальный, удаленный)
  - Блокировка сессии (локальная, удаленная)
  - Разблокировка сессии (локальная, удаленная)
- События работы в приложении:
  - Запуск приложения
  - Остановка приложения
  - Получение фокуса активного окна приложения
  - Потеря фокуса активного окна приложения
- События работы в браузере;
  - Получение фокуса вкладкой браузера
- События веб-поиска
- События использования мыши и клавиатуры

- События действий с файлами

Важно!

Для РЕД ОС события статистики создаются только для:

- Локального входа в сессию;
- Локального выхода из сессии;
- Локальной блокировки сессии;
- Локальной разблокировки сессии;
- Получения фокуса активного окна приложения;
- Потери фокуса активного окна приложения;
- Использования клавиатуры;
- Получения фокуса вкладкой браузера (для браузера Edge (Chromium));
- События веб-поиска (для браузеров Edge (Chromium) и Mozilla Firefox).

Для операционных систем ОС Альт и ОС Astra Linux события создаются в тех же случаях, что и для системы РЕД ОС, за исключением *Получения фокуса вкладкой браузера*.

В редких случаях при выключении/перезагрузке рабочей станции с использованием кнопок выключения/перезагрузки возможна потеря событий локального выхода из сессии.

При выключении/перезагрузке рабочей станции с использованием встроенной в ОС консоли управления (с помощью команд shutdown, reboot и проч.) с высокой вероятностью будут потеряны события локального выхода из сессии.

Важно!

Если в DM отключен контроль сетевых соединений (перехват трафика), это повлияет на сбор данных о событиях браузера следующим образом: в Систему будут поступать события получения фокуса вкладкой браузера, и не будут поступать события веб-поиска.

Сотрудники

Основные принципы работы с сотрудниками (контролируемыми пользователями) и группами сотрудников описываются в разделе "Сотрудники и группы сотрудников".

Действующие политики безопасности могут быть назначены только группе сотрудников. Определение политики безопасности для отдельного сотрудника выполняется путем включения его учетной записи в ту или иную группу.

Важно!

На каждого сотрудника, помимо политики безопасности, назначенной группе сотрудников, также действует и политика безопасности, определенная для компьютера, на котором работает сотрудник. О порядке определения приоритетов при пересечении правил см. "Применение правил".

Чтобы перейти к разделу Консоли управления, предназначенному для управления учетными записями сотрудников и группами сотрудников, воспользуйтесь кнопкой **Группы сотрудников**, расположенной на Панели навигации.

Информация по работе с сотрудниками и группами сотрудников содержится в подразделах:

- Просмотр сведений о сотрудниках и группах сотрудников
- Просмотр результирующих политик и белого списка для сотрудника
- Создание и редактирование группы сотрудников
- Удаление группы сотрудников
- Добавление учетной записи сотрудника в группу
- Редактирование учетной записи сотрудника
- Исключение учетной записи сотрудника из группы сотрудников
- Удаление учетной записи сотрудника из схемы безопасности

Просмотр сведений о сотрудниках и группах сотрудников

В области Группы сотрудников на Панели навигации выводится перечень групп сотрудников. В рабочей области главного окна отображается перечень сотрудников, входящих в состав выделенной группы сотрудников.

> **Примечание:**
>
> Для более удобного просмотра вы можете настроить отображение списка сотрудников, при помощи дополнительных функций (см. "Дополнительные возможности").

Чтобы просмотреть информацию по отдельной группе сотрудников, выберите название нужной группы в списке групп сотрудников.

Чтобы просмотреть информацию по всем сотрудникам, зарегистрированным в Системе, воспользуйтесь кнопкой **Показать всех сотрудников**, расположенной в верхней части Панели навигации.

Информация по учетным записям сотрудников представлена в виде табличного списка. Каждая строка списка соответствует одной учетной записи. В столбцах выводятся общие свойства учетных записей. Расширенная информация по свойствам учетной записи выводится на панели **Подробно**.

Чтобы просмотреть подробную информацию по свойствам отдельной учетной записи, выберите строку с названием нужной учетной записи. В результате на панели **Подробно** будет отображена таблица свойств, в которой вы сможете просмотреть следующую информацию:

Свойство	Описание
Учетная запись	Название учетной записи сотрудника
Фамилия	Фамилия, имя и отчество сотрудника, для которого создана данная учетная запись
Имя	
Отчество	
Идентификатор	Идентификатор учетной записи

Свойство	Описание
	Для рабочих станций под управлением MS Windows: • Device Monitor получает данные об учетной записи из операционной системы; • поддерживается получение SID для доменной учетной записи из Active Directory. **Для рабочих станций под управлением Linux:** • поддерживается получение SID для доменной учетной записи из Active Directory, только если одновременно выполняются следующие условия: • рабочая станция находится под управлением РЕД ОС, Astra Linux 1.7 или Альт Рабочая станция 10; • рабочая станция введена в домен Active Directory с использованием SSSD (System Security Services Daemon); • если получение SID для доменной учетной записи невозможно, Device Monitor считает учетную запись локальной.

Важно!

Получение доменного SID из Active Directory поддерживается для рабочих станций под управлением Linux:

- **начиная с версии Device Monitor 7.8.0**: для РЕД ОС;
- **начиная с версии Device Monitor 7.9**: для Astra Linux 1.7 или Альт Рабочая станция 10.

Device Monitor версии ниже указанных определяет доменную учетную запись как локальную. После обновления Агента до требуемых версий или выше:

- Для учетных записей, которые определялись как локальные до обновления, может быть определен доменный SID. Если в Системе нет сотрудника с этим SID, то будет добавлен новый сотрудник.
- Если на рабочей станции определен доменный SID, то будут использоваться правила, которые настроены для сотрудника с доменной учетной записью.

Примечание.

Часть свойств, выводимых на панели **Подробно**, дублируется в рабочей области главного окна.

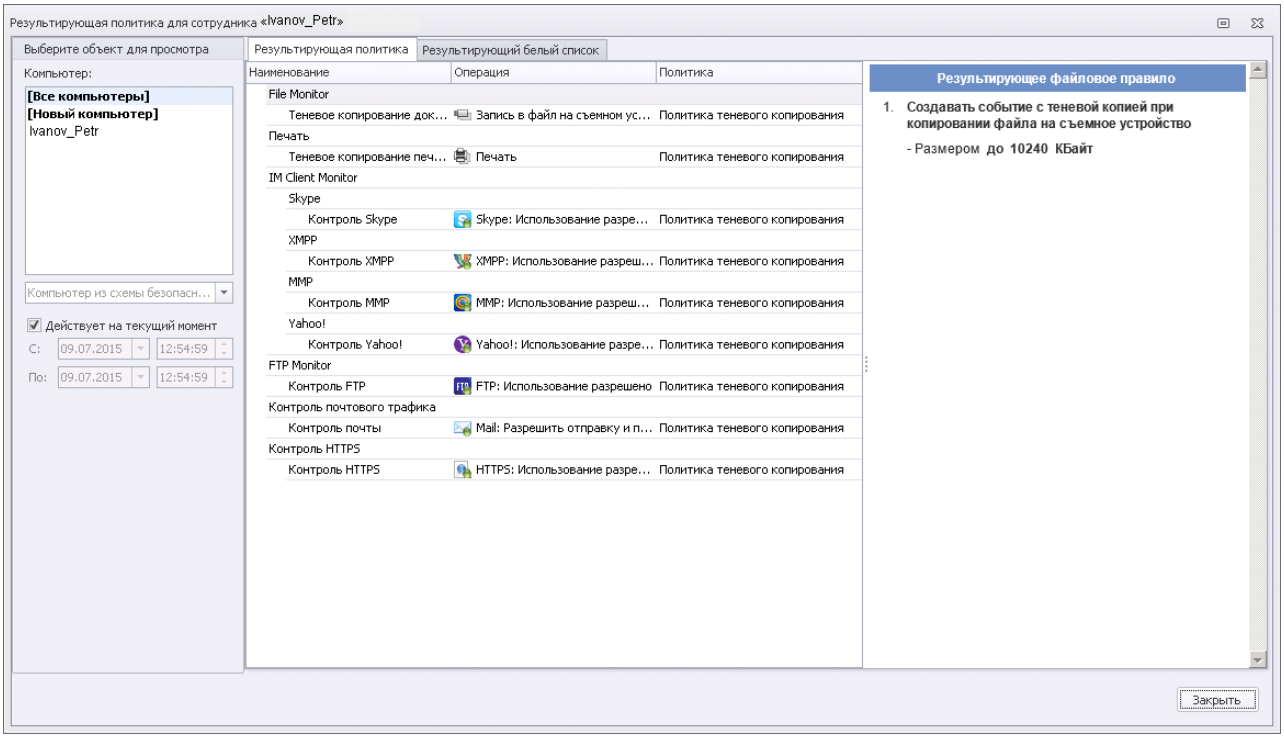
Просмотр результирующих политик и белого списка для сотрудника

Чтобы посмотреть информацию о политике и белом списке, действующих для сотрудника:

1. В списке сотрудников выберите запись требуемого сотрудника.
2. Выполните одно из следующих действий:

- в главном меню выберите команду **Правка** > **Показать результирующую политику**.
- на панели **Сотрудники** нажмите **Показать результирующую политику**.

В результате на экран будет выведено окно **Результирующая политика для сотрудника <имя сотрудника>**, где по умолчанию отображается результирующая политика для всех компьютеров выбранного сотрудника.



Основная область окна **Результирующая политика для сотрудника** содержит две вкладки:

- **Результирующая политика** - отображаются правила, являющиеся результирующими для данного сотрудника. Результирующая политика складывается из правил, настроенных по умолчанию, правил, заданных для выбранного компьютера, и правил для выбранного сотрудника (см. "Особенности применения правил для Device Monitor"). Чтобы просмотреть подробную информацию по правилу, выберите его из списка: на панели, находящейся справа, отобразится подробная информация о выбранном правиле.
- **Результирующий белый список** - отображаются устройства, являющиеся разрешенными для данного сотрудника (см. "Белые списки"). Чтобы просмотреть подробную информацию об устройстве, выберите его из списка: на панели, находящейся справа, отобразится подробная информация о выбранном устройстве.

На панели **Компьютер** вы можете выбрать объект для просмотра:

- **Все компьютеры** - при выборе отображается результирующая политика\белый список для сотрудника, вне зависимости от того, на какой компьютер он выполнил вход.
- **Новый компьютер** - при выборе отображается результирующая политика пользователя на новом компьютере (которого еще нет в схеме безопасности).
- Чтобы просмотреть результирующую политику для выбранного пользователя на определенном компьютере:
  - из списка **Компьютер** выберите имя компьютера, на котором зарегистрирована выбранная учетная запись сотрудника

или

- из раскрывающегося списка **Компьютер из схемы безопасности** выберите любую учетную запись компьютера, зарегистрированную в Системе (см. "Компьютеры").

Вы можете выбрать время, для которого будет показана результирующая политика\белый список:

- по умолчанию выбрана настройка **Действует на текущий момент** и отображаются текущие результирующие политика и белый список;
- чтобы просмотреть результирующие политику\белый список для выбранного сотрудника за интересующий вас период времени, снимите отметку с поля **Действует на текущий период** и укажите необходимый временной промежуток.

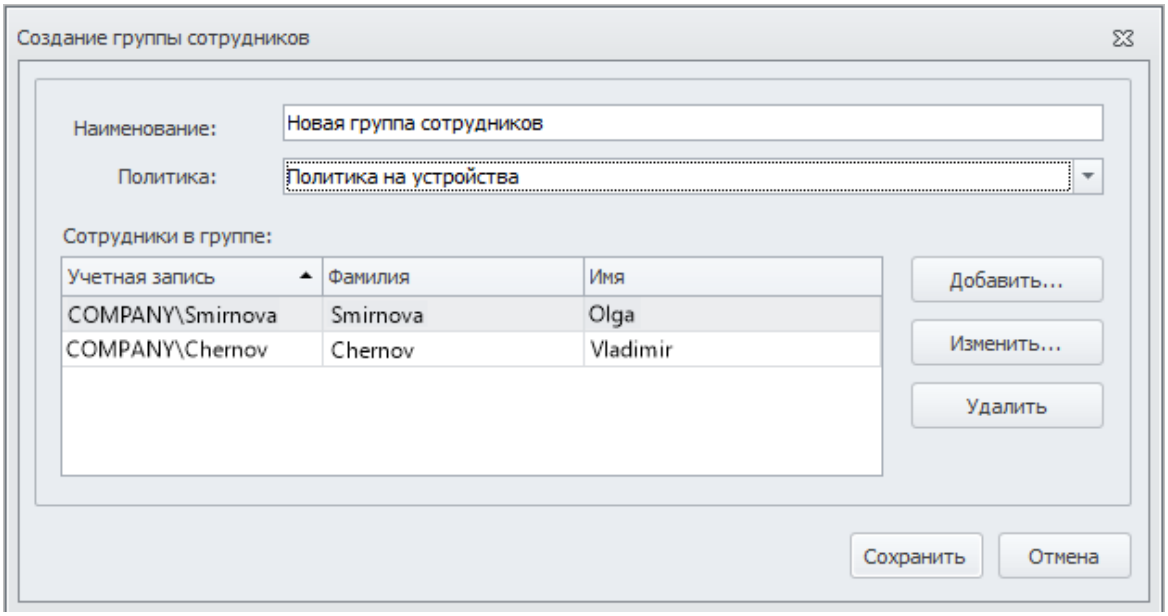
Создание и редактирование группы сотрудников

Чтобы добавить группу сотрудников:

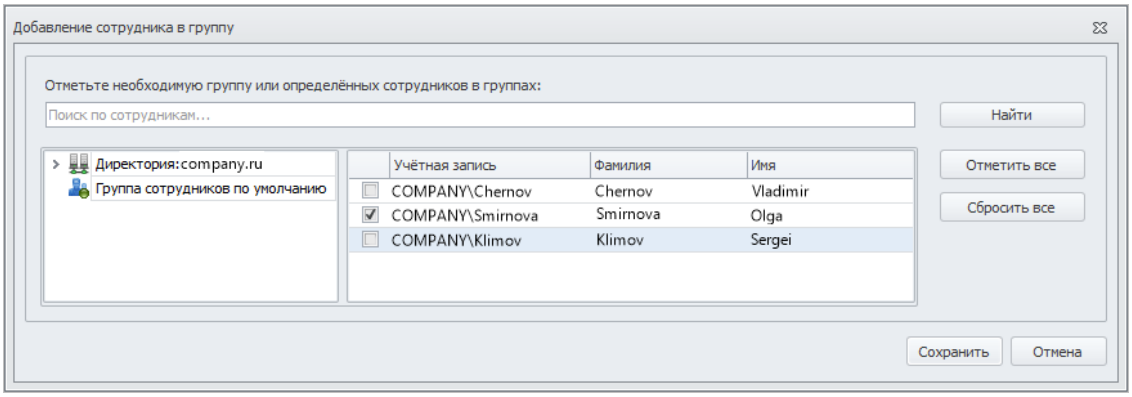
1. Перейдите к разделу **Группы сотрудников**.
2. Выполните необходимое действие:

Действие	Шаги
Добавить группу сотрудников	• в главном меню выберите команду **Правка** > **Создать группу сотрудников**; • воспользуйтесь кнопкой **Создать группу сотрудников**, расположенной в верхней части Панели навигации.
Отредактировать группу сотрудников	a. В области Группы сотрудников на Панели навигации выберите название нужной группы сотрудников. b. Выполните одно из следующих действий: • в главном меню выберите команду **Правка** > **Изменить**; • воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации; • дважды щелкните левой кнопкой мыши по названию выделенной группы сотрудников.

В результате выполнения любого из этих действий на экран будет выведено диалоговое окно определения параметров группы сотрудников.



3. Укажите следующие параметры:
   - **Наименование**. Название группы сотрудников.
   - **Политика**. Выберите из раскрывающегося списка политику безопасности, которая будет назначена данной группе сотрудников.
4. Определите перечень сотрудников в группе:
   - Чтобы добавить одну или несколько учетных записей, нажмите **Добавить**.



В окне добавления сотрудников отображается список учетных записей, импортированных из службы каталогов (см. "Соединение и синхронизация со службами каталогов"), а также уже зарегистрированных в системе (например, при установке Агента Device Monitor на компьютеры) и принадлежащих существующим группам сотрудников Device Monitor.

Чтобы добавить сотрудника, в левой области выберите необходимый узел в дереве групп, затем отметьте учетные записи, которые нужно добавить в редактируемую группу.

Чтобы отметить все учетные записи, принадлежащие выбранному узлу, нажмите **Отметить все**. Чтобы снять выделение, нажмите **Сбросить все**.

Вы также можете выполнить поиск учетной записи по всем доступным элементам. Для этого в верхней строке введите часть имени учетной записи и нажмите **Найти**.

После того, как все необходимые учетные записи выбраны, нажмите **Сохранить**,

чтобы закрыть окно добавления сотрудников и вернуться к окну настройки параметров группы.
- Чтобы изменить параметры учетной записи, выберите ее в списке сотрудников, входящих в группу, и нажмите **Изменить**. О порядке редактирования учетной записи см. "Редактирование учетной записи сотрудника".
- Чтобы удалить запись из группы, выберите ее и нажмите **Удалить**.

5. Нажмите **Сохранить**.

> **Важно!**
>
> Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Удаление группы сотрудников

Чтобы удалить группу сотрудников:

1. Перейдите к разделу **Группы сотрудников**.
2. Щелкните левой кнопкой мыши по названию нужной группы сотрудников.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - щелкните по выбранной группе правой кнопкой мыши и в контекстном меню выберите **Удалить**;
   - нажмите Ctrl+D.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление группы сотрудников.

> **Важно!**
>
> Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Добавление учетной записи сотрудника в группу

В результате установки Агента InfoWatch Device Monitor на компьютер (см. "Traffic Monitor. Руководство по установке", статья "Установка Агента InfoWatch Device Monitor"), сведения обо всех пользователях, зарегистрированных на компьютере, автоматически добавляются в схему безопасности, в группу сотрудников "по умолчанию". Соответственно, на всех сотрудников, входящих в группу «по умолчанию», будет распространяться политика безопасности, назначенная данной группе. В дальнейшем определение политик безопасности для сотрудника происходит путем включения его учетной записи в различные группы сотрудников.

Чтобы перенести сотрудника из одной группы в другую:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** на Панели навигации выберите название группы сотрудников, где уже есть его учетная запись.

3. В области **Сотрудники** выберите строку с учетной записью, которую нужно добавить в другую группу. Щелкните левой кнопкой мыши по выделенной строке и, не отпуская кнопку, перетащите учетную запись в область **Группы сотрудников** на Панели навигации. Подведите курсор мыши к названию той группы сотрудников, куда нужно добавить учетную запись. После того как слева от названия выбранной группы появится желтая стрелка, отпустите левую кнопку мыши.

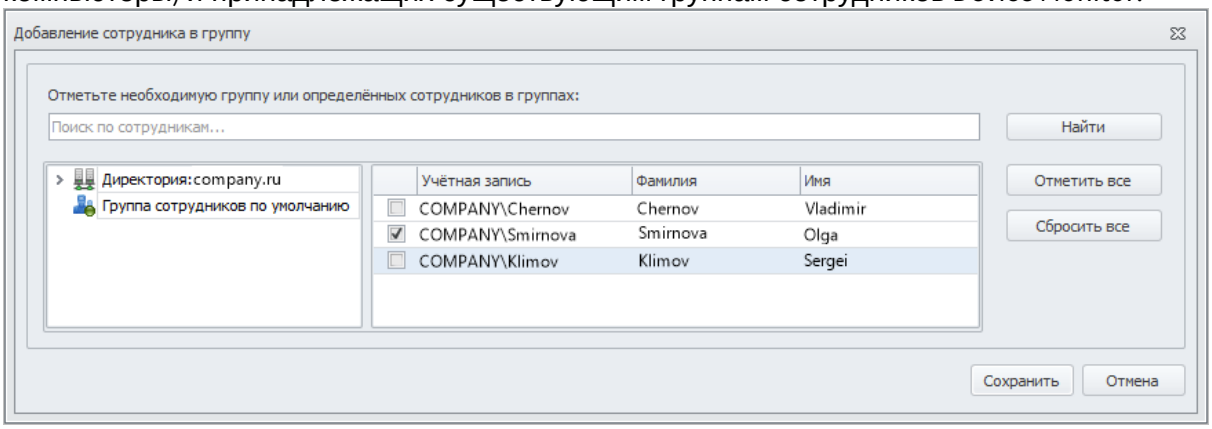
В результате учетная запись будет включена в выбранную группу.

Вы также можете вручную импортировать в Систему информацию о сотруднике из службы каталогов (о настройке соединения см. "Соединение и синхронизация со службами каталогов"). Тогда после регистрации данного сотрудника на компьютере, где установлен Агент InfoWatch Device Monitor, на этого сотрудника будет распространяться политика той группы, в которую он был добавлен.

Чтобы добавить одну или несколько учетных записей, импортированных из службы каталогов или уже зарегистрированных в Системе, в группу сотрудников:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** на Панели навигации выберите название группы, в которую нужно добавить учетную запись сотрудника.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить сотрудника**;
   - воспользуйтесь кнопкой **Добавить сотрудника**, расположенной в верхней части области **Сотрудники**;
   - нажмите правой кнопкой мыши в рабочей области и из раскрывшегося контекстного меню выберите **Добавить сотрудника**.

   В результате на экран будет выведено диалоговое окно добавления сотрудников, где отображается список учетных записей, импортированных из службы каталогов (см. "Соединение и синхронизация со службами каталогов"), а также уже зарегистрированных в системе (например, при установке Агента Device Monitor на компьютеры) и принадлежащих существующим группам сотрудников Device Monitor.



4. Чтобы добавить сотрудника, в левой области выберите необходимый узел в дереве групп, затем отметьте учетные записи, которые нужно добавить в редактируемую группу.
   Чтобы отметить все учетные записи, принадлежащие выбранному узлу, нажмите **Отметить все**. Чтобы снять выделение, нажмите **Сбросить все**.
   Вы также можете выполнить поиск учетной записи по всем доступным элементам. Для этого в верхней строке введите часть имени учетной записи и нажмите **Найти**.
5. После того, как вы выбрали все необходимые учетные записи, нажмите **Сохранить**, чтобы закрыть окно **Добавление сотрудника в группу** и вернуться в окно настройки параметров группы.

6. Нажмите **Сохранить**.

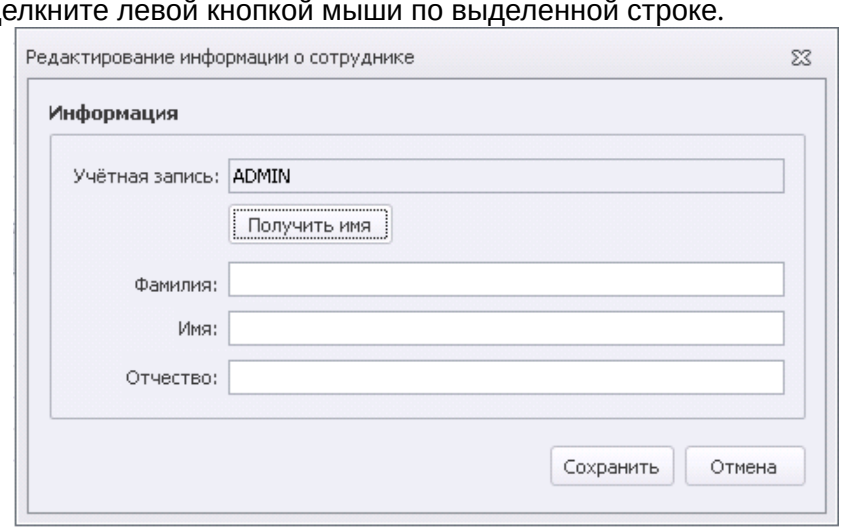
> **Важно!**
>
> Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. раздел "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Редактирование учетной записи сотрудника

Параметры учетной записи сотрудника могут быть импортированы из службы каталогов или при установке Агента InfoWatch Device Monitor на компьютер, где этот сотрудник зарегистрирован. Если вы хотите дополнить полученные данные, то вы можете внести ФИО сотрудника, как описано ниже.

Чтобы отредактировать учетную запись сотрудника:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** на Панели навигации выберите название группы сотрудников, в которую входит нужная учетная запись.
3. Выберите строку с именем учетной записи, которую нужно отредактировать.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить** из нижней части раскрывающегося списка;
   - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части области Сотрудники;
   - дважды щелкните левой кнопкой мыши по выделенной строке.



5. В диалоговом окне **Редактирование информации о сотруднике** вы можете изменять значения необязательных параметров **Фамилия**, **Имя** и **Отчество**. Новые значения параметров **Фамилия** и **Имя** можно вручную добавлять в соответствующие поля или импортировать из службы каталогов, воспользовавшись кнопкой **Получить имя**. Значение параметра **Отчество** можно добавить только вручную.
6. Нажмите **Сохранить**.

> **Важно!**

Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Исключение учетной записи сотрудника из группы сотрудников

Чтобы исключить учетную запись сотрудника из группы сотрудников:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** выберите название группы сотрудников, в которую входит нужная учетная запись.
3. Выберите строку с именем учетной записи, которую нужно исключить из данной группы.

   Примечание:

   Чтобы исключить несколько учетных записей из группы сотрудников, выберите строки с именами всех учетных записей сотрудников, которые нужно исключить из данной группы. Для выбора нескольких строк используйте клавиши Stift или Ctrl. Чтобы выделить все строки, нажмите Ctrl+A.

4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Исключить сотрудника из группы**;
   - воспользуйтесь кнопкой **Исключить сотрудника из группы**, расположенной в верхней части области **Сотрудники**;
   - щелкните по строке правой кнопкой мыши и в контекстном меню выберите **Исключить сотрудника из группы**;
   - нажмите кнопку клавиатуры **Delete**.

После этого учетная запись сотрудника будет исключена из выбранной группы сотрудников.

Примечание:

Если учетная запись сотрудника входит только в одну группу сотрудников, то при исключении из группы такая учетная запись будет автоматически добавлена в группу сотрудников «по умолчанию».

Важно!

Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Удаление учетной записи сотрудника из схемы безопасности

Чтобы удалить учетную запись сотрудника из схемы безопасности:

1. Перейдите к разделу **Группы сотрудников**.

2. В области **Группы сотрудников** выберите название группы сотрудников, в которую входит нужная учетная запись.
3. Выберите строку с именем учетной записи, которую нужно удалить.

> **Примечание:**
>
> Чтобы удалить несколько учетных записей из схемы безопасности, выберите строки с именами всех учетных записей, которые нужно удалить.

4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить сотрудника из схемы безопасности**;
   - воспользуйтесь кнопкой **Удалить сотрудника из схемы безопасности**, расположенной в верхней части области **Сотрудники**;
   - щелкните по строке правой кнопкой мыши и в контекстном меню выберите **Удалить сотрудника из схемы безопасности**;
   - нажмите сочетание клавиш клавиатуры **Shift+Delete**.
5. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление учетной записи.

> **Важно!**
>
> Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Компьютеры

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

Основные принципы работы с компьютерами описываются в разделе "Компьютеры и группы компьютеров".

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

> **Важно!**
>
> На каждый компьютер, помимо политики безопасности, назначенной группе компьютеров, также распространяется и политика безопасности, определенная для сотрудника, который в данный момент авторизован на компьютере. О порядке определения приоритетов при пересечении правил см. "Применение правил".

Чтобы перейти к разделу Консоли управления, предназначенному для управления компьютерами, воспользуйтесь кнопкой **Группы компьютеров**, расположенной на Панели навигации.

Информация по работе с контролируемыми компьютерами содержится в подразделах:

- Просмотр сведений о компьютерах;
- Просмотр результирующих политики и белого списка на компьютерах;
- Создание и редактирование группы компьютеров;
- Удаление группы компьютеров;
- Добавление компьютера в группу;
- Исключение компьютера из группы;
- Удаление компьютера из схемы безопасности;
- Обновление Агентов на контролируемых компьютерах;
- Диагностика рабочей станции;
- Обновление статусов Агентов на контролируемых компьютерах;
- Установка статуса "Золотой образ" на Агенте.

Просмотр сведений о компьютерах

В области Группы компьютеров на Панели навигации выводится перечень групп компьютеров. В рабочей области главного окна отображается перечень компьютеров, входящих в состав выделенной группы компьютеров.

> **Примечание.**
>
> Для более удобного просмотра вы можете настроить отображение списка компьютеров, воспользовавшись дополнительными функциями (подробнее см. "Дополнительные возможности").

Чтобы просмотреть список компьютеров, входящих в группу, на панели **Группы компьютеров** выберите название нужной группы: перечень компьютеров, входящих в нее, отобразится в рабочей области.
Чтобы просмотреть список всех зарегистрированных компьютеров, воспользуйтесь кнопкой  **Показать все компьютеры**, расположенной в верхней части Панели навигации.

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

Табличный список содержит следующие основные сведения:

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

> **Примечание:**
>
> Если остановленный агент был обновлен, то после завершения обновления он будет запущен.

  - **Работает в диагностическом режиме**. Агент установлен на рабочую станцию и переведен в диагностический режим работы через Консоль DM.
  - **Золотой образ**. Агент установлен на рабочую станцию, для которой назначен статус "Золотой образ".
  - **Удален**. Агент удален с рабочей станции через задачу удаления продукта или средствами на самой рабочей станции.
- **Активность Агента**. Статус активности Агента, установленного на компьютере. Данный параметр может принимать одно из следующих значений:
  -  **Активен**. Агент регулярно выходит на связь с сервером, передает события, данные.
  -  **Не активен**. Агент регулярно не выходит на связь с сервером или отключен.
  -  **Не активен более недели**. Агент не выходит на связь с сервером более недели.
  -  **Не активен более месяца**. Агент не выходит на связь с сервером более месяца.

Пользователю доступна возможность настройки статусов активности Агента (см. Настройка статусов активности Агентов).

> **Примечание:**
>
> При работе Системы возможно появление невалидных статусов Агентов на рабочих станциях. Это может происходить в случае, если одновременно выполняется несколько операций смены статуса состояния. Например, офицер безопасности через консоль переводит рабочую станцию в режим поддержки и в то же время, но немного раньше, приходит уведомление об удалении Агента.

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

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

Для компьютера со статусом Агента **Не установлен** отображается значение **Агент не установлен**.

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

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

> **Примечание**
>
> Комментарий рабочей станции сохраняется немедленно при редактировании, не изменяя версии схемы безопасности. При этом необходимо учитывать следующие ограничения:
>
> - при изменении комментария существующей рабочей станции он записывается в БД немедленно даже при редактировании схемы безопасности;
> - при изменении комментария только что добавленной рабочей станции он будет сохранен только при сохранении схемы безопасности.

Расширенная информация по свойствам компьютера выводится на панели Подробно.

Чтобы просмотреть свойства отдельного компьютера, в рабочей области главного окна выберите строку с описанием нужного компьютера.

На панели Подробно будет отображена таблица свойств, в которой содержатся дополнительные (к указанным выше) сведения по выбранному компьютеру:

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

Важно!

Если на компьютере осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного места"), то теневые копии сохраняться не будут.

Важно!

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

В некоторых случаях не поддерживается удаление данных на Агентах под управлением ОС Linux. Файл с метаданными события может остаться на диске Агента, даже если Агент отправил событие.

Примечание.

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, определенная для группы компьютеров «по умолчанию».
В процессе работы вы можете выполнять следующие действия:

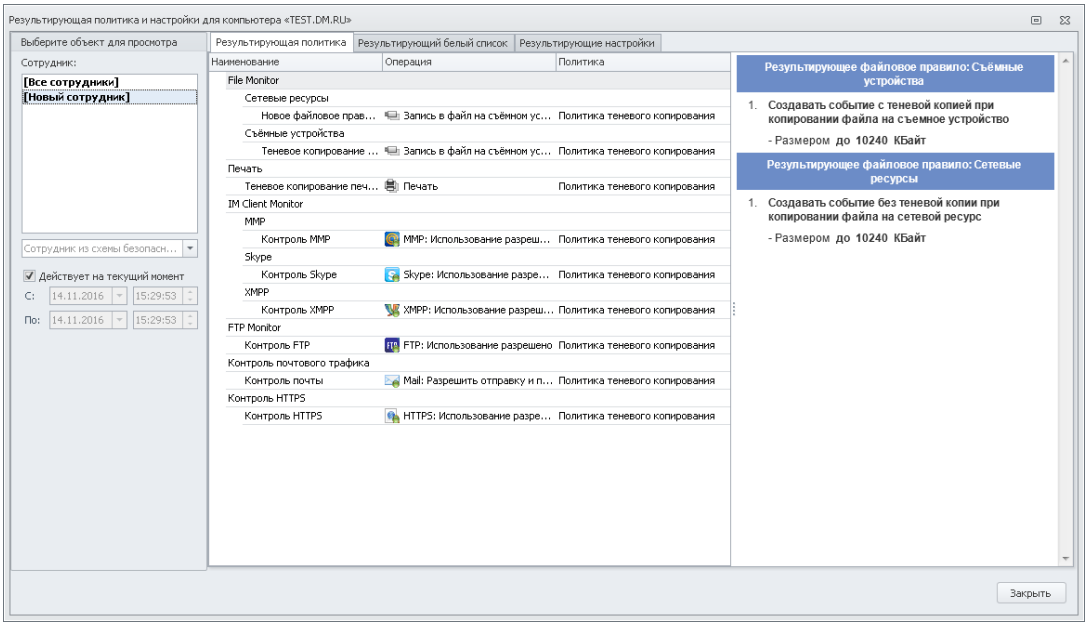
- управлять группами компьютеров:
  - добавлять группы компьютеров;
  - редактировать параметры групп компьютеров;
  - удалять группы компьютеров.
- управлять компьютерами:
  - добавлять информацию о компьютерах в группу компьютеров и тем самым определять политику безопасности;
  - исключать компьютеры из группы компьютеров;
  - обновлять Агенты на контролируемых компьютерах;
  - удалять компьютеры из схемы безопасности.

Просмотр результирующих настроек, политик и белого списка на компьютере

Чтобы посмотреть информацию о настройках, политике и белом списке, действующих на компьютере:

1. В списке компьютеров выберите название нужного.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Показать настройки и результирующую политику**.
   - на панели Компьютеры нажмите **Показать настройки и результирующую политику**.

В результате на экран будет выведено окно **Результирующая политика и настройки для компьютера: <имя компьютера>**, где по умолчанию отображается результирующая политика для всех сотрудников на выбранном компьютере.



Основная область окна **Результирующая политика и настройки для компьютера** содержит три вкладки:

- **Результирующая политика** - отображаются правила, являющиеся результирующими на компьютере. Результирующая политика складывается из правил, настроенных по умолчанию, правил, заданных для данного компьютера, и правил для сотрудников этого компьютера (см. "Особенности применения правил для Device Monitor"). Чтобы просмотреть подробную информацию по правилу, выберите его из списка: на панели, находящейся справа, отобразится подробная информация о выбранном правиле.
- **Результирующий белый список** - отображаются устройства, являющиеся разрешенными для компьютера (см. "Белые списки"). Чтобы просмотреть подробную информацию об устройстве, выберите его из списка: на панели, находящейся справа, отобразится подробная информация о выбранном устройстве.
- **Результирующие настройки** - отображаются настройки Скорости отправки данных с агента и Контроля дискового пространства на агентах, являющиеся результирующими на компьютере. Результирующие настройки складываются из настроек по умолчанию и настроек для группы компьютеров, в которую входит выбранный компьютер (см. "Общие настройки работы агентов" и "Создание и редактирование группы компьютеров").

На панели **Сотрудник** вы можете выбрать объект для просмотра:

- **Все сотрудники** - при выборе отображается результирующая политика\белый список\настройки для всех сотрудников, вне зависимости от того, кто выполнил вход на выбранный компьютер.
- **Новый сотрудник** - при выборе отображается результирующая политика\белый список\настройки на выбранном компьютере для нового сотрудника (которого еще нет в схеме безопасности).
- Чтобы просмотреть результирующую политику\белый список\настройки для определенного пользователя:

- из списка **Сотрудник** выберите имя учетной записи, зарегистрированной на выбранном компьютере
  или
- из раскрывающегося списка **Сотрудник** из схемы безопасности выберите любую учетную запись, зарегистрированную в Системе (см. "Сотрудники").

Вы можете выбрать время, для которого будет показана результирующая политика\белый список\настройки:

- по умолчанию выбрана настройка **Действует на текущий момент** и отображаются текущие результирующие политика\белый список\настройки;
- чтобы просмотреть результирующие политику\белый список\настройки за интересующий вас период времени, снимите отметку с поля **Действует на текущий период** и укажите необходимый временной промежуток.

Создание и редактирование группы компьютеров

Важно!

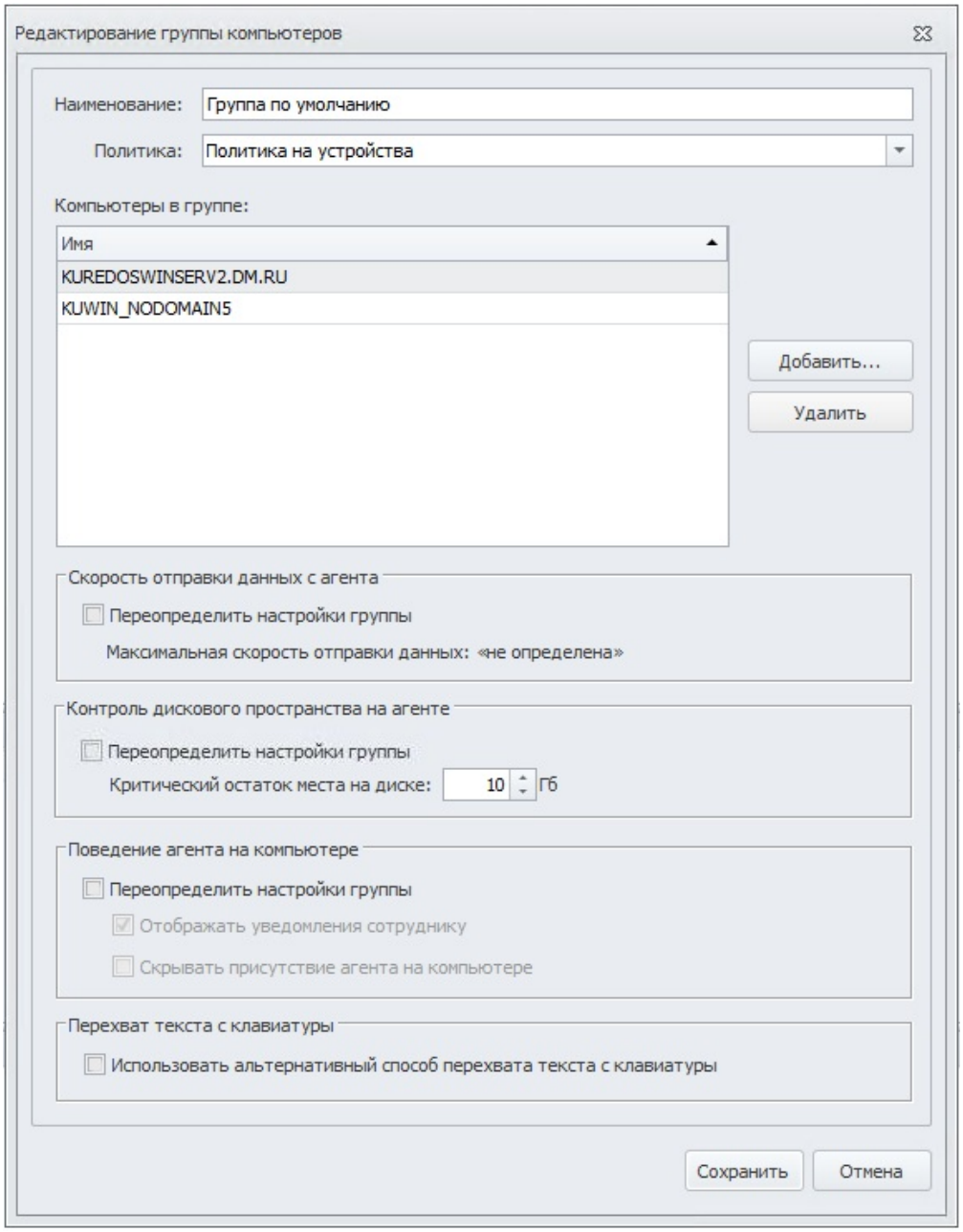
Когда регистрируется новый компьютер, информация о нем автоматически добавляется в схему безопасности (в группу компьютеров «по умолчанию»).

Чтобы добавить группу компьютеров:

1. Перейдите к разделу **Группы компьютеров**.
2. Выполните необходимое действие:

Действие	Шаги
Добавить группу компьютеров	- в главном меню выберите команду **Правка** > **Создать группу компьютеров**; - воспользуйтесь кнопкой **Создать группу компьютеров**, расположенной в верхней части Панели навигации.
Отредактировать группу компьютеров	a. В области **Группы компьютеров** на Панели навигации выберите название нужной группы компьютеров. b. Выполните одно из следующих действий: - в главном меню выберите команду **Правка** > **Изменить** - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации; - дважды щелкните левой кнопкой мыши по названию выделенной группы компьютеров.

В результате выполнения любого из этих действий на экран будет выведено диалоговое окно определения параметров группы компьютеров.



3. Укажите следующие параметры:
   - **Наименование**.
   - **Политика**. Выберите из раскрывающегося списка политику безопасности, которая будет назначена данной группе компьютеров.
4. Определите перечень компьютеров в группе:
   - Чтобы добавить один или несколько компьютеров, нажмите **Добавить**. В открывшемся окне вы можете выбрать компьютеры:
     - из сетевого окружения Microsoft Windows Network;
     - из дерева AD и/или ALD;
     - из числа ранее зарегистрированных в системе (например, в результате ручной установки Агента Device Monitor) и уже принадлежащих существующим группам Device Monitor.

     В левой области выберите необходимый узел в дереве групп, затем отметьте компьютеры, которые нужно добавить в редактируемую группу.

Вы также можете выполнить поиск компьютера по директории. Для этого в верхней строке введите часть имени компьютера и нажмите **Найти**.
После того, как все необходимые компьютеры выбраны, нажмите Сохранить, чтобы закрыть окно добавления и вернуться к окну настройки параметров группы.

- Чтобы удалить компьютер из группы, выберите его и нажмите **Удалить**.

5. Вы можете назначить для компьютеров, входящих в группу, собственную максимальную скорость отправки данных с Агента (об общих значениях см. "Общие настройки работы Агентов", параметр **Ограничивать скорость отправки данных**). Для этого:
   a. в области **Скорость отправки данных с агента** выберите настройку Переопределить настройки группы;
   b. в поле **Максимальная скорость отправки данных** укажите необходимое значение, в Кб/с.

   По умолчанию настройка не выбрана.
6. Вы можете назначить для компьютеров, входящих в группу, другое значение минимального размера свободного пространства на контролируемом компьютере, при достижении которого теневые копии не будут создаваться (об общих значениях см. "Общие настройки работы Агентов", параметр **Критический остаток места на диске**). Для этого:
   a. в области **Контроль дискового пространства на агенте** выберите настройку **Переопределить настройки группы**;
   b. в поле **Критический остаток места на диске** укажите необходимое значение, в ГБ.

   По умолчанию настройка не выбрана.
7. Вы можете назначить для компьютеров, входящих в группу, другой режим работы Агента на контролируемом компьютере или дополнить функционал Агента (об общих значениях см. "Общие настройки работы Агентов", группа параметров **Поведение Агента на компьютере**). Для этого:
   a. в области **Поведение Агента на компьютере** выберите настройку **Переопределить настройки группы.**
   b. определите, нужно ли **Отображать уведомления сотруднику** и необходимо ли **Скрывать присутствие агента на компьютере** во время работы.

   По умолчанию настройка не выбрана.
8. Вы можете включить альтернативный способ перехвата текста с клавиатуры, который предусматривает перехват диакритических символов. Для этого:
   - В области **Перехват текста с клавиатуры** выберите настройку **Использовать альтернативный способ перехвата текста с клавиатуры.**

> **Примечание:**
>
> Работа функциональности поддерживается на агентах под управлением ОС Windows 8 и более поздних.
>
> В некоторых случаях может не срабатывать перехват при использовании консольных приложений, например, Far Manager.

> **Примечание:**
>
> После включения настройки необходима перезагрузка агента, а также перезапуск процесса приложения.

По умолчанию настройка не выбрана.

9. Нажмите **Сохранить**.

> **Важно!**
>
> Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Удаление группы компьютеров

Чтобы удалить группу компьютеров:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - щелкните по названию выделенной группы правой кнопкой мыши и в контекстном меню выберите **Удалить**;
   - нажмите Ctrl+D.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление группы.

   > **Важно!**
   >
   > В группе компьютеров, которую вы удаляете, могут быть компьютеры, не включенные в другие группы. Такие компьютеры при удалении единственной группы, в которую они были включены, будут автоматически добавлены в группу компьютеров «по умолчанию».

5. Нажмите на кнопку **ОК**.

> **Важно!**
>
> Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Добавление компьютера в группу

При установке Агента InfoWatch Device Monitor на компьютер (см. "Traffic Monitor. Руководство по установке", статья "Установка Агента InfoWatch Device Monitor"), в Системе автоматически создается запись о компьютере. Эта запись добавляется в группу "по умолчанию". Соответственно, на все компьютеры, входящие в группу «по умолчанию», будет распространяться политика безопасности, назначенная данной группе. В дальнейшем определение политик безопасности для компьютера происходит путем его включения в различные группы компьютеров.

Чтобы скопировать компьютер из одной группы в другую:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы, в состав которой входит нужный компьютер.
3. В области **Компьютеры** выберите строку с именем компьютера, который нужно добавить в другую группу. Щелкните левой кнопкой мыши по выделенной строке и, не отпуская кнопку, перетащите компьютер в область **Группы компьютеров** на Панели навигации. Подведите курсор мыши к названию той группы, куда нужно добавить компьютер. После того как слева от названия выбранной группы появится желтая стрелка, отпустите левую кнопку мыши.

В результате компьютер будет включен в выбранную группу.

Вы также можете вручную добавить в Систему информацию о рабочей станции, на которой еще не установлен Агент InfoWatch Device Monitor. Информация о рабочей станции импортируется из службы каталогов (о настройке соединения см. "Соединение и синхронизация со службами каталогов") или из сетевого окружения. Тогда после установки Агента InfoWatch Device Monitor на такую рабочую станцию (см. "Создание задачи первичного распространения"), на нее будет распространяться политика той группы, в которую она была добавлена.

> **Важно!**
>
> Настоятельно не рекомендуется добавлять компьютеры с одинаковыми именами. В системе InfoWatch Device Monitor такие компьютеры будут зарегистрированы как один и, соответственно, на них будет распространяться одна политика, будет вестись единая регистрация событий и т.д.

Чтобы добавить компьютер в группу:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы. После этого в рабочей области главного окна будет выведен список всех компьютеров, уже входящих в группу.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить компьютер**;
   - воспользуйтесь кнопкой **Добавить компьютер**, расположенной в верхней части области Компьютеры;
   - нажмите правой кнопкой мыши в рабочей области и из раскрывшегося контекстного меню выберите **Добавить компьютер**.

   В открывшемся диалоговом окне вы можете выбрать компьютеры:
   - из сетевого окружения Microsoft Windows Network;
   - из дерева AD и/или ALD;

- из числа ранее зарегистрированных в Системе. Для этого введите имя компьютера в поисковой строке и нажмите **Искать**.

> **Важно!**
>
> Любое подключение компьютера или его поиск осуществляется только в подключенных директориях (отмечены ●).

4. Отметьте необходимые компьютеры или группы компьютеров (☑):
   a. Разверните группы, отмеченные пиктограммой ▶; развернутые - ▼. Чтобы развернуть или свернуть группу, дважды нажмите на ней левой кнопкой мыши.
   b. Укажите имя компьютера в строке внизу диалогового окна. При перечислении нескольких имен разделяйте их точкой с запятой.
   c. Выберите **Подключиться ко всем директориям.** При этом будут последовательно подключены все директории при указании авторизационных данных.
5. Нажмите **Сохранить**.

В результате диалоговое окно **Выбор компьютеров** будет закрыто, а в группу компьютеров будет добавлена информация о выбранных компьютерах.

> **Важно!**
>
> Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Исключение компьютера из группы

Включение компьютера в определенную группу компьютеров влечет за собой назначение этому компьютеру политик безопасности выбранной группы. Поэтому если вам понадобится отменить действие какой-либо политики безопасности на компьютер, исключите его из группы, которой назначена эта политика безопасности.

> **Примечание.**
>
> Если компьютер входит только в одну группу, то при исключении он будет автоматически добавлен в группу компьютеров «по умолчанию».

Чтобы исключить компьютер из группы компьютеров:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы, куда входит нужный компьютер. После этого в рабочей области главного окна будет выведен список всех компьютеров, включенных в выбранную группу.
3. Выберите строку с именем компьютера, которого нужно исключить из группы компьютеров.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Исключить компьютер из группы**;

- воспользуйтесь кнопкой  **Исключить компьютер из группы**, расположенной в верхней части области **Компьютеры**;
- щелкните по компьютеру правой кнопкой мыши и в контекстном меню выберите **Исключить компьютер из группы**;
- нажмите кнопку клавиатуры **Delete**.

После этого компьютер будет исключен из группы.

Важно!

Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Удаление компьютера из схемы безопасности

Компьютер может быть выведен из списка зарегистрированных (например, эксплуатация рабочей станции прекращена). Удаление компьютера возможно при любом статусе Агента. Сведения о таком компьютере не будут удалены, но, так как Агент на нем отключен, то компьютеру присваивается статус **Неактивен**.

Если сохранение информации о неактивном компьютере не требуется, то вы можете удалить запись о нем.

Чтобы удалить компьютер из схемы безопасности:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы компьютеров, в которую входит нужный компьютер.
3. В рабочей области главного окна выберите строку с названием неактивного компьютера, который нужно удалить.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить компьютер из схемы безопасности**;
   - воспользуйтесь кнопкой **Удалить компьютер из схемы безопасности**, расположенной в верхней части области Компьютеры;
   - щелкните правой кнопкой на строке необходимого компьютера и из раскрывшегося списка выберите **Удалить компьютер из схемы безопасности**;
   - нажмите сочетание клавиш клавиатуры **Shift+Delete**.
5. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление.

В результате сведения о компьютере будут удалены из всех групп, в которые входил данный компьютер.

Важно!

Чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Обновление Агентов на контролируемых компьютерах

> **Важно!**
>
> На ОС Astra Linux не поддерживается обновление Агентов с версий ниже 7.0.

Для контролируемых компьютеров доступно упрощенное создание задачи обновления Агентов Device Monitor (подробнее об этом типе задач см. "Удаленная установка, обновление и удаление Агентов" и "Создание задачи обновления").

Перед началом обновления убедитесь, что в настройках Сервера Device Monitor задана корректная новая версия для автоустановки и автообновления агентов (подробнее см. "Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor").

Чтобы обновить Агенты Device Monitor на всех контролируемых компьютерах, входящих в группу:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы.
3. Воспользуйтесь кнопкой  **Обновить все компьютеры**, расположенной в верхней части Панели навигации.

Чтобы обновить Агенты Device Monitor выбранных контролируемых компьютерах:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы компьютеров.
3. В области **Компьютеры** выберите строку с именем одного или нескольких контролируемых компьютеров. Для выбора нескольких компьютеров отмечайте их, зажав клавишу **Shift** или **Ctrl**.
4. Воспользуйтесь кнопкой  **Обновить компьютеры**, расположенной в верхней части области **Компьютеры**.

В результате выполнения любого из этих действий будет создана и автоматически запущена задача обновления для выбранных компьютеров.

Диагностика рабочей станции

Система предоставляет возможность удаленного сбора диагностических данных с рабочих станций. Диагностические данные запрашиваются из Консоли управления через сервер Device Monitor, который обращается к Агентам. Для защищенного соединения между сервером и Агентами используется протокол TLS с двусторонней аутентификацией.

> К Агентам версий ниже 7.3 сервер подключается по незащищенному каналу. Рекомендуем обновлять Агенты до актуальной версии.

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

Чтобы включить диагностический режим:

1. Перейдите к разделу **Группы компьютеров**.

2. В области **Группы компьютеров** на Панели навигации выберите название группы, в которую входит необходимая рабочая станция.
3. В списке компьютеров нажмите правой кнопкой мыши на название нужной рабочей станции и из раскрывшегося контекстного меню выберите команду **Диагностика** > **Включить диагностический режим**.

Чтобы выключить диагностический режим:

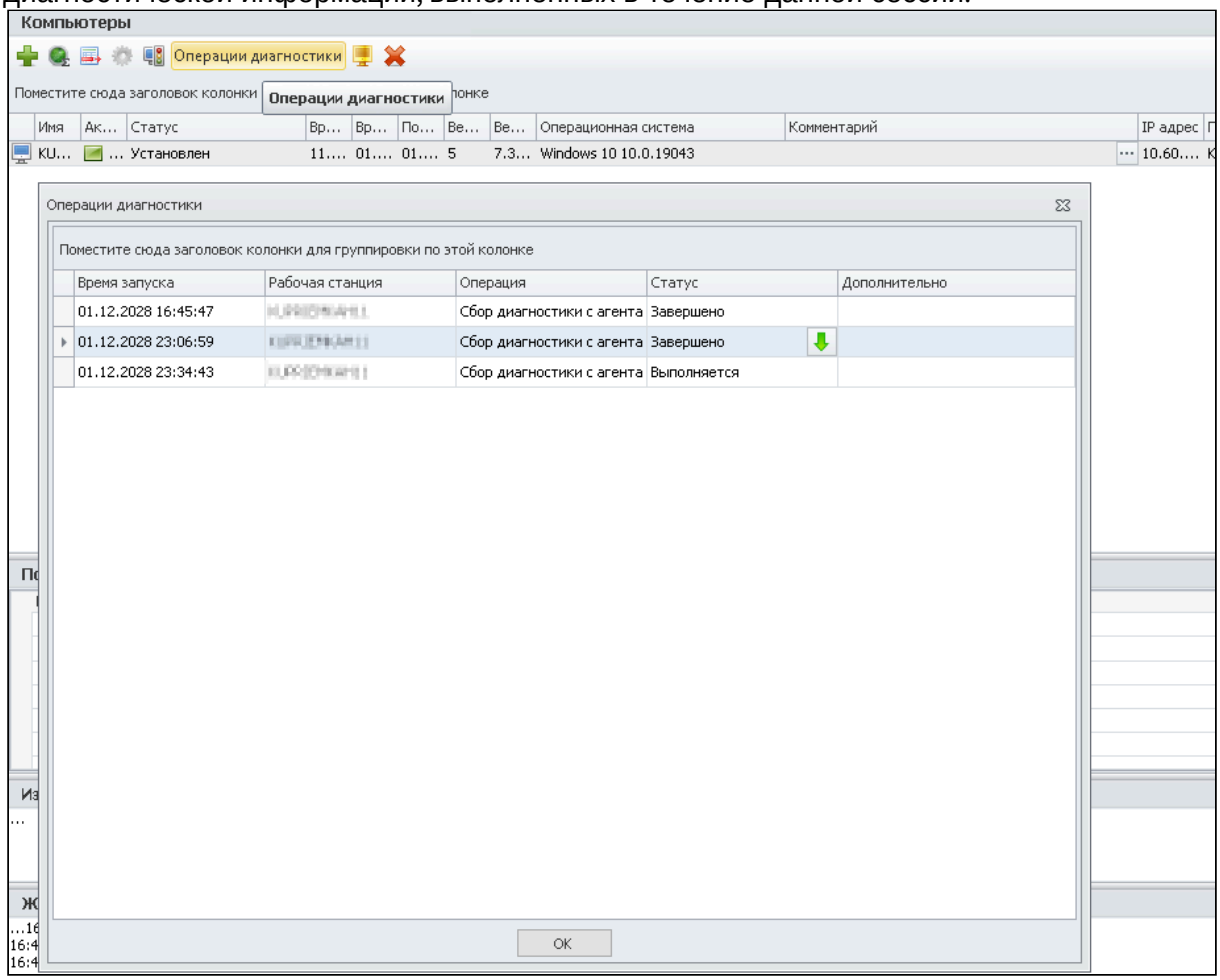
1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы, в которую входит необходимая рабочая станция.
3. В списке компьютеров нажмите правой кнопкой мыши на название нужной рабочей станции и из раскрывшегося контекстного меню выберите команду **Диагностика** > **Выключить диагностический режим**.

Собранную диагностическую информацию можно выгрузить в виде архива с файлами.

Чтобы получить архив со всеми собранными диагностическими данными:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы, в которую входит необходимая рабочая станция.
3. В списке компьютеров нажмите правой кнопкой мыши на название нужной рабочей станции и из раскрывшегося контекстного меню выберите команду **Диагностика** > **Собрать диагностическую информацию**.
4. На панели инструментов нажмите кнопку **Операции диагностики**.
   Откроется окно **Операции диагностики**, которое содержит историю запросов

диагностической информации, выполненных в течение данной сессии.



> Собранная диагностическая информация хранится на сервере в течение активного подключения Консоли управления к серверу Device Monitor. Если сессия будет завершена или прервана, в целях безопасности вся собранная диагностическая информация будет удалена.
>
> При одновременном подключении нескольких пользователей каждому доступна только информация, собранная в рамках его сессии.
>
> Пока на рабочей станции выполняется сбор диагностической информации, выполнение аналогичного запроса от имени другой сессии будет невозможно.

> До выгрузки с сервера диагностическая информация хранится в директории `C:\Program Files\InfoWatch\Device Monitor\Server\AgentLogs`. Доступ к директории ограничен. По умолчанию доступ имеют:
>
> - пользователь System;
> - пользователи из группы Администраторы;
> - пользователь, от имени которого сервис выполняет запрос на сбор информации.

5. Дождитесь, когда статус запроса изменится на **Завершено**.

6. Чтобы выгрузить результаты выполненного запроса нажмите кнопку .
7. В открывшемся окне **Выберите путь сохранения архива с диагностической информацией** укажите расположение и имя архива, затем нажмите кнопку **Сохранить**.

> После сохранения архива повторная его выгрузка будет недоступна, а собранная по данному запросу диагностическая информация будет удалена с сервера.

8. Чтобы закрыть окно **Операции диагностики** нажмите кнопку **ОК**.

> **Примечание:**
>
> Если статус состояния Агента на рабочей станции **Не установлен** или **Удален**, то при выборе пункта **Диагностика** Система выдаст сообщение об ошибке – отсутствии агента.

> **Примечание:**
>
> При включении диагностического режима работы Агента будет отображаться статус состояния Агента **Работает в диагностическом режиме**. Если пользователь останавливает Агент, работающий в диагностическом режиме, статус состояния Агента изменится на **Остановлен**. После возобновления работы в диагностическом режиме, статус состояния Агента также изменится на **Работает в диагностическом режиме**.

> **Важно!**
>
> Для корректной смены статуса на/с **Работает в диагностическом режиме** и **Остановлен** настоятельно рекомендуется использовать консоль DM.
>
> Если отключение и перевод Агента в диагностический режим будут выполняться локально на агенте с помощи утилиты, то новый статус Агента не будет отправлен на сервер. Актуализировать статус возможно через Консоль, пункт меню Диагностика. При этом Консоль напрямую обращается к Агенту, получает его актуальный статус, записывает его в БД и обновляет внутри себя.

Обновление статусов Агентов на контролируемых компьютерах

Для контролируемых компьютеров доступно обновление статусов Агентов Device Monitor с помощью кнопки или сочетания клавиш.

Чтобы обновить статусы Агентов Device Monitor на всех контролируемых компьютерах, входящих в группу:

1. Перейдите в раздел **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы.
3. Выполните одно из следующих действий:

   - воспользуйтесь кнопкой  **Обновить статусы**, расположенной в верхней части Панели навигации;

- щелкните по названию выделенной группы правой кнопкой мыши и в раскрывшемся списке выберите **Обновить статусы**;
- нажмите **Ctrl+F5**.

Чтобы обновить статусы Агентов Device Monitor на выбранных контролируемых компьютерах:

1. Перейдите в раздел **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы компьютеров.
3. В области **Компьютеры** выберите строку с именем одного или нескольких контролируемых компьютеров. Чтобы выбрать несколько компьютеров, отметьте их, одновременно зажав клавишу **Shift** или **Ctrl**.
4. Выполните одно из следующих действий:

   - воспользуйтесь кнопкой **Обновить статусы**, расположенной в верхней части Панели навигации;
   - щелкните по названию выделенной группы правой кнопкой мыши и в раскрывшемся списке выберите **Обновить статусы**;
   - нажмите **Ctrl+F5**.

Установка статуса "Золотой образ" на Агенте

В системах виртуализации возможно создание образа компьютера, из которого будут создаваться новые виртуальные машины (например, для создания однотипных серверов или рабочих станций для пользователей, решающих однотипные задачи).

Под образом понимается компьютер с установленными ОС и ПО, где среди прочего ПО установлена клиентская часть Device Monitor. Если в организации используется образ при подготовке новых рабочих станций, то в этот образ необходимо установить агент Device Monitor.

ОБ вручную назначает такому компьютеру статус состояния "**Золотой образ**", чтобы этот компьютер не переименовывался, и сервер Device Monitor различал новые машины, разворачиваемые из него, и регистрировал их в одной с данным компьютером группе.

Статус Агента "**Золотой образ**" возможно установить только на компьютере со статусом Агента **Установлен**. Автоматически статус "**Золотой образ**" установлен быть не может.

ОБ может установить статус Агента "**Золотой образ**" двумя способами:

1. Выбрать **Компьютеры** в окне навигации слева;
2. Выбрать компьютер, на котором необходимо установить статус Агента "**Золотой образ**";
3. Нажать на кнопку **Установить статус** "**Золотой образ**" на панели сверху;
4. Подтвердить действие, выбрав **Да** в открывшемся диалоговом окне. Статус "**Золотой образ**" будет назначен Агенту на данном компьютере.

или

1. Выбрать **Компьютеры** в окне навигации слева;
2. Щелкнуть правой кнопкой мыши на строке компьютера, на котором Агенту необходимо назначить статус "**Золотой образ**";
3. В открывшемся списке выбрать **Установить статус** "**Золотой образ**";
4. Подтвердить действие, выбрав **Да** в открывшемся диалоговом окне. Статус "**Золотой образ**" будет назначен Агенту на данном компьютере.

Удалить статус Агента "**Золотой образ**" также возможно двумя способами:

1. Выбрать **Компьютеры** в окне навигации слева;
2. Выбрать компьютер, на котором необходимо установить статус Агента "**Золотой образ**";
3. Нажать на кнопку  **Удалить статус "Золотой образ"** на панели сверху;
4. Подтвердить действие, выбрав **Да** в открывшемся диалоговом окне. Статус Агента "**Золотой образ**" будет удален на данном компьютере.

или

1. Выбрать **Компьютеры** в окне навигации слева;
2. Щелкнуть правой кнопкой мыши на строке компьютера, на котором необходимо удалить статус Агента "**Золотой образ**";
3. В открывшемся списке выбрать  **Удалить статус "Золотой образ**";
4. Подтвердить действие, выбрав **Да** в открывшемся диалоговом окне. Статус Агента "**Золотой образ**" будет удален на данном компьютере.

Важно!

В случае, если необходимо переименовать компьютер с Агентом, имеющим статус "**Золотой образ**"**,** Система отработает так же, как при развертывании из данного компьютера новой машины. Поэтому при переименовании сохранится старое имя данной рабочей станции. Оно будет отображаться в Консоли DM, откуда ОБ необходимо удалить его вручную.

Если компьютера еще нет в схеме безопасности, то:

- он будет зарегистрирован с новым именем, а Агенту назначен статус **Установлен**;
- для Агента на данном компьютере ОБ будет необходимо установить статус "**Золотой образ**";
- компьютер будет добавлен в схему безопасности в те же группы, в которых находится компьютер со статусом Агента "**Золотой образ**".

Если компьютер уже находится в схеме безопасности, то Агент получит информацию, что компьютер с данным именем уже зарегистрирован.

Белые списки устройств

Для управления списками устройств, доступ к которым безусловно разрешен (сотруднику, группе сотрудников, компьютеру или группе компьютеров), предназначен раздел **Белые списки**. Чтобы перейти к этому разделу, воспользуйтесь кнопкой **Белые списки**, расположенной на Панели навигации.

Информация по работе с белыми списками содержится в подразделах:

- Просмотр сведений о белых списках
- Добавление белого списка
- Установка периода действия записи
- Редактирование белого списка
- Удаление белого списка

Вы можете просмотреть информацию о действующих белых списках как описано в разделах "Просмотр результирующих политик и белого списка для сотрудника" и "Просмотр результирующих настроек, политик и белого списка на компьютере".

Примечание:

Вы можете отправлять в Платформу информацию об устройствах из белых списков. О настройке см. статью базы знаний "Отправка данных об устройствах из белых списков DM в Платформу".

Просмотр сведений о белых списках

В области Белые списки на Панели навигации выводится перечень белых списков. В рабочей области главного окна отображается список устройств (моделей и экземпляров), входящих в состав выделенного белого списка.

Примечание.

Вы можете выполнять поиск в перечне белых списков, вводя наименование списка в строке поиска, находящейся под перечнем в Панели навигации.

Для выбранного белого списка можно настроить его отображение при помощи дополнительных функций (см. "Дополнительные возможности").

Чтобы просмотреть информацию по отдельному белому списку, выберите название нужного белого списка группы в перечне белых списков.

Информация по белым спискам представлена в виде списка устройств, сгруппированного по их типам. Каждая строка списка соответствует одной модели или экземпляру устройства. В столбцах выводятся общие свойства устройств. Расширенная информация по свойствам устройства выводится на панели **Подробно**.

Чтобы просмотреть подробную информацию по свойствам отдельного устройства, выберите строку с названием нужной модели или экземпляра устройства.

В результате на панели **Подробно** будет отображена таблица свойств, в которой вы сможете просмотреть следующую информацию:

- **Идентификатор экземпляра или модели устройства**. Код модели (VID – Vendor ID) или серийного номера экземпляра (PID – Product ID) устройства.
- **Описание устройства**.
- **Комментарий**.
- **Тип устройств**.
- **Категория**. Модель или экземпляр.
- **Период действия**. Дата и время начала и окончания периода, в течение которого доступ к данному устройству безусловно разрешен.
- **Обнаружено на компьютере**. Имя компьютера, на котором обнаружено устройство.
- **Добавлено в базу данных**. Дата добавления информации об устройстве в базу данных (см. "Добавление устройства в базу").

Примечание.

Часть свойств, выводимых на панели **Подробно**, дублируется в рабочей области главного окна.

Добавление белого списка

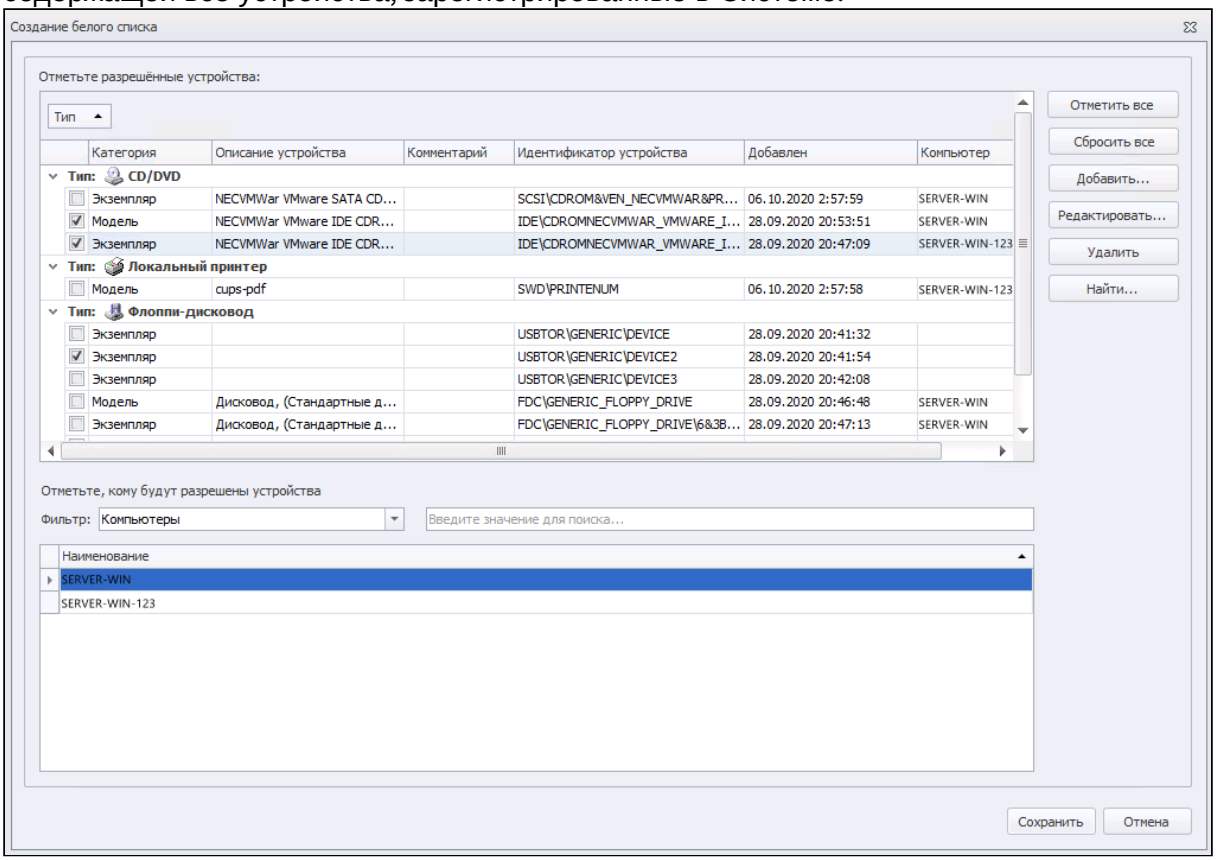
Действие белого списка распространяется на определенный (назначенный) объект: сотрудника, группу сотрудников, компьютер или группу компьютеров.

> **Важно!**
>
> Одному объекту назначения (сотруднику, группе сотрудников, компьютеру или группе компьютеров) может быть назначен только один белый список.

Чтобы добавить белый список:

1. Перейдите к разделу **Белые списки**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Создать белый список**;
   - воспользуйтесь кнопкой **Создать белый список**, расположенной в верхней части Панели навигации;
   - щелкните в области **Белые списки** правой кнопкой мыши и в контекстном меню выберите **Создать белый список**;
   - нажмите Ctrl+N.

   На экран будет выведено диалоговое окно **Создание белого списка** с таблицей, содержащей все устройства, зарегистрированные в Системе.



3. В таблице отметьте модели и экземпляры, доступ к которым должен быть безусловно разрешен.

Важно!

Информация о том, как изменять список зарегистрированных моделей и экземпляров устройств, содержится в следующих разделах:

- Добавление записи об устройстве
- Удаление записи об устройстве

4. В области **Отметьте, кому будут разрешены устройства** выберите фильтр: на кого будет распространяться действие белого списка:
   - сотрудники
   - группы сотрудников
   - компьютеры
   - группы компьютеров

   Внизу отобразится перечень записей, соответствующих выбранному фильтру.
   Вы также можете воспользоваться строкой поиска, введя искомое имя или его часть.
5. Выберите сотрудника / группу сотрудников / компьютер / группу компьютеров, на которые должно распространяться действие белого списка.
6. Нажмите **Сохранить**.

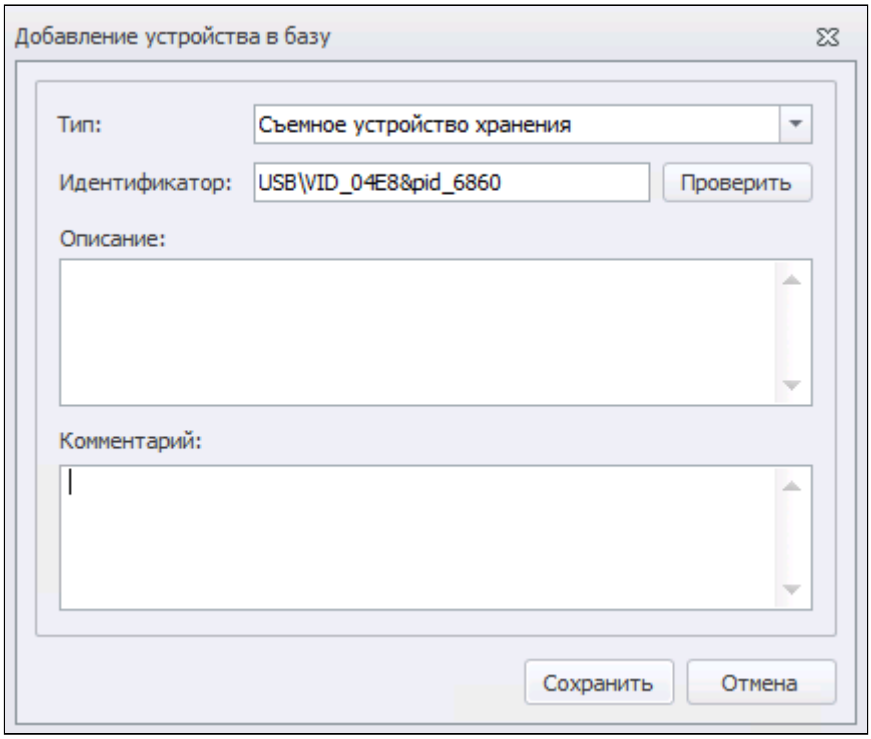
Добавление записи об устройстве

Вы можете включать в белые списки только те модели и экземпляры устройства, информация о которых была предварительно зарегистрирована в системе. Добавить информацию об устройстве вы можете одним из двух способов:

- вручную, если вы знаете идентификатор этого устройства;
- с помощью поиска, если это устройство подключено к контролируемому компьютеру.

Чтобы добавить запись об устройстве вручную:

1. Откройте диалоговое окно **Создание белого списка** (см. "Добавление белого списка").
2. Нажмите кнопку **Добавить**, расположенную в правой части окна.
   В результате на экран будет выведено диалоговое окно **Добавление устройства в базу**.



3. Укажите параметры устройства:
   - из раскрывающегося списка **Тип** выберите тип устройства;
   - в поле **Идентификатор** введите код экземпляра или модели устройства;

> **Примечание.**
>
> Чтобы узнать код устройства, подключите это устройство и с помощью стандартных средств Windows (например, Диспетчер устройств) просмотрите свойства этого устройства. Код экземпляра устройства отображается на вкладке **Сведения**.
>
> Код экземпляра устройства имеет вид XXX\YYY\ZZZ, где XXX – тип устройства (обычно - наименование шины, к которой подключено устройство, например, USB, IDE или ACPI), YYY - строка, характеризующая модель устройства (Vendor ID), а ZZZ – строка, характеризующая данный экземпляр устройства (Product ID).
>
> Код модели устройства имеет вид XXX\YYY, где XXX – тип устройства, а YYY - строка, характеризующая модель (VID).

Чтобы удостовериться в допустимости введенного кода, нажмите **Проверить**.

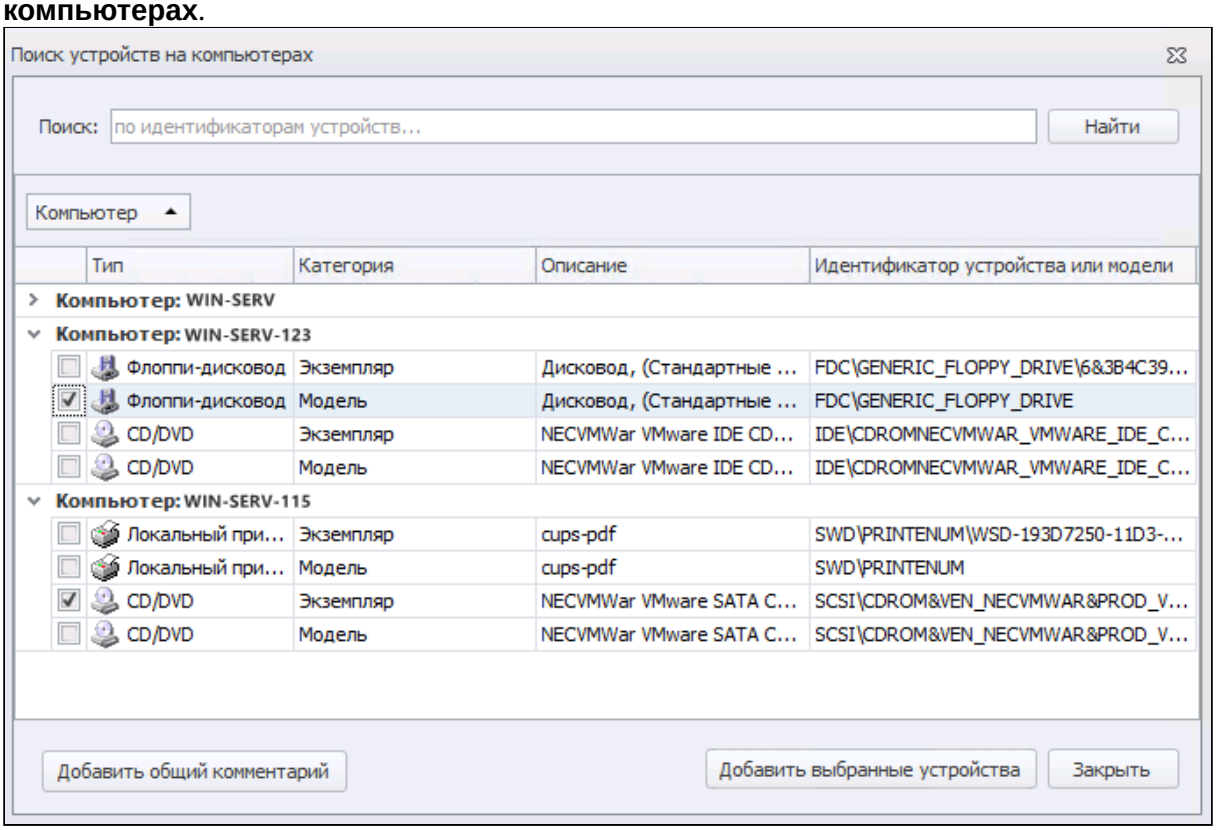
> **Важно!**
>
> При использовании кода экземпляра следует учитывать, что некоторые устройства не имеют уникального идентификатора: идентификатор может изменяться динамически и отличаться даже при подключении к разным портам одной рабочей станции.
>
> В таких случаях рекомендуется использовать код модели устройства.

- при необходимости в поле **Описание** введите описание устройства;
- при необходимости в поле **Комментарий** добавьте комментарий к устройству.

4. Нажмите **Сохранить**.

Чтобы добавить запись с помощью поиска устройств, подключавшихся к компьютерам:

1. Откройте диалоговое окно Создание белого списка (см. "Добавление белого списка").
2. Нажмите кнопку **Найти**, расположенную в правой части окна.
   В результате на экран будет выведено диалоговое окно **Поиск устройств на компьютерах**.



3. В списке контролируемых компьютеров выберите необходимый одним из следующих способов:
   - нажмите кнопку , соответствующую необходимому компьютеру;
   - дважды щелкните левой кнопкой мыши на названии компьютера.

   Раскроется список всех устройств, которые подключались к выбранному компьютеру за все время работы Агента Device Monitor на нем.

> **Примечание:**
>
> Если устройство было подключено и отключено в период, когда отсутствовало соединение между компьютером с Агентом Device Monitor и сервером Device Monitor, то оно не попадет в список.

> **Примечание:**

Для компьютеров под управлением ОС семейства Linux будут отображены только USB-устройства.

Примечание:

Следует обратить внимание на то, что подключенные к компьютеру устройства подсвечены в списке белым цветовым фоном, в то время как отключенные выделены серым.

4. Отметьте устройства, информацию о которых вы хотите добавить.

Примечание:

Кнопка **Добавить общий комментарий** станет активной, если отмечено несколько устройств. После нажатия кнопки откроется окно, в котором можно будет указать общий комментарий для всех выделенных в этот момент устройств.

5. Нажмите **Добавить выбранные устройства**.

Удаление записи об устройстве

Чтобы удалить запись о зарегистрированном устройстве из Системы:

1. Откройте диалоговое окно **Создание белого списка** (см. "Добавление белого списка").
2. Выполните одно из следующих действий:
   - в таблице с зарегистрированными устройствами щелкните правой кнопкой мыши по выбранному экземпляру или модели устройства и в контекстном меню выберите **Удалить устройство**.
   - нажмите Ctrl+D.
3. В открывшемся окне подтверждения нажмите **Да**.

Примечание:

При удалении устройства добавленный к нему комментарий также будет удален.

Установка периода действия записи

Для каждого экземпляра или модели устройства, внесенного в белый список, разрешение на его использование отображается в виде отдельной записи. По умолчанию эта запись (разрешение) действует в течение практически бесконечного периода времени (с 01.01.1753 по 31.12.9999). Вы можете установить ограничение по времени действия безусловного разрешения на работу с этим устройством. До и после указанного периода работа с устройством будет подчиняться общим правилам работы с устройствами данного типа.

Чтобы установить период действия записи в белом списке:

1. Перейдите к разделу **Белые списки**.
2. В области **Белые списки** на Панели навигации выберите название белого списка, куда входит нужная запись.

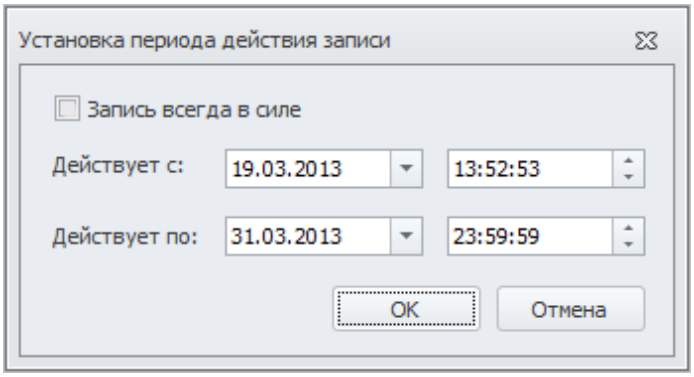
3. Если записи в белом списке сгруппированы (например, по типу устройств), разверните группу (см. "Группирование записей").

   Примечание.

   Если установить период действия для всей группы, то изменение вступит в силу только для первой записи в группе.

4. Выделите строку с записью об экземпляре или модели устройства, которому нужно установить период действия, и выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить запись**;
   - воспользуйтесь кнопкой **Изменить запись**, расположенной в верхней части области **Разрешенные устройства**;
   - дважды щелкните левой кнопкой мыши по названию выделенной записи;
   - щелкните по строке правой кнопкой мыши, затем в раскрывшемся контекстном меню выберите пункт **Изменить запись**;
   - нажмите Ctrl+Shift+E.

   В результате на экран будет выведено диалоговое окно **Установка периода действия записи**.



5. Укажите период действия записи и нажмите кнопку **ОК**.

Редактирование белого списка

Чтобы отредактировать параметры белого списка:

1. Перейдите к разделу **Белые списки**.
2. В области **Белые списки** на Панели навигации выберите название белого списка.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить**;
   - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации;
   - дважды щелкните левой кнопкой мыши по названию выделенного белого списка;
   - щелкните по названию выделенного белого списка правой кнопкой мыши и в контекстном меню выберите **Изменить**;
   - нажмите Ctrl+E.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно **Редактирование белого списка <Имя списка>**. Содержание этого окна аналогично окну **Создание белого списка**, но область **Отметьте, кому будут разрешены устройства** недоступна для изменения.

4. При необходимости, добавьте или удалите устройства в перечне зарегистрированных в Системе (см. "Добавление устройства в базу" и "Удаление устройства из базы").
   Вы также можете изменить описание ранее зарегистрированного устройства: для этого выберите устройство в перечне и нажмите кнопку **Редактировать**, расположенную в правой части окна. В открывшемся окне отредактируйте текст описания или комментарий и нажмите **Сохранить**.
5. В таблице с зарегистрированными устройствами отметьте или снимите отметки, чтобы изменить список моделей и экземпляров устройств, включенных в белый список.
6. Нажмите **Сохранить**.

Важно!

Поскольку работа с белыми списками ведется в режиме редактирования схемы безопасности, то для того, чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Удаление белого списка

Чтобы удалить белый список:

1. Перейдите к разделу **Белые списки**.
2. Щелкните левой кнопкой мыши по названию нужного белого списка.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - щелкните по названию выделенного белого списка правой кнопкой мыши и в контекстном меню выберите **Удалить**;
   - нажмите Ctrl+D.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление белого списка.

Важно!

Поскольку работа с белыми списками ведется в режиме редактирования схемы безопасности, то для того, чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Категории сигнатур

Правила File Monitor можно настроить таким образом, что под правило будут подпадать только файлы, обладающие структурой, характерной для определенного формата файлов. Для этого в системе InfoWatch Device Monitor предусмотрено определение формата файла по **сигнатуре**.

В разделе Категории сигнатур определен список сигнатур, которые может распознавать Система. Для удобства использования сигнатуры сгруппированы по **категориям**.

Чтобы просмотреть имеющиеся сигнатуры:

1. Перейдите к разделу **Категории сигнатур**, воспользовавшись кнопкой, расположенной на Панели навигации. Вы также можете использовать команду меню **Переход** > **Категории сигнатур** или сочетание клавиш Ctrl+5.
   В области **Категории сигнатур** на Панели навигации будет выведен перечень **категорий**, по которым сгруппированы сигнатуры.
2. Выберите категорию сигнатур из перечня.
   В рабочей области главного окна будет отображен перечень сигнатур, входящих в состав выделенной категории.

Важно!

Предустановленные категории сигнатур редактированию и удалению не подлежат. Создание сигнатур не предусмотрено.

Вы можете:

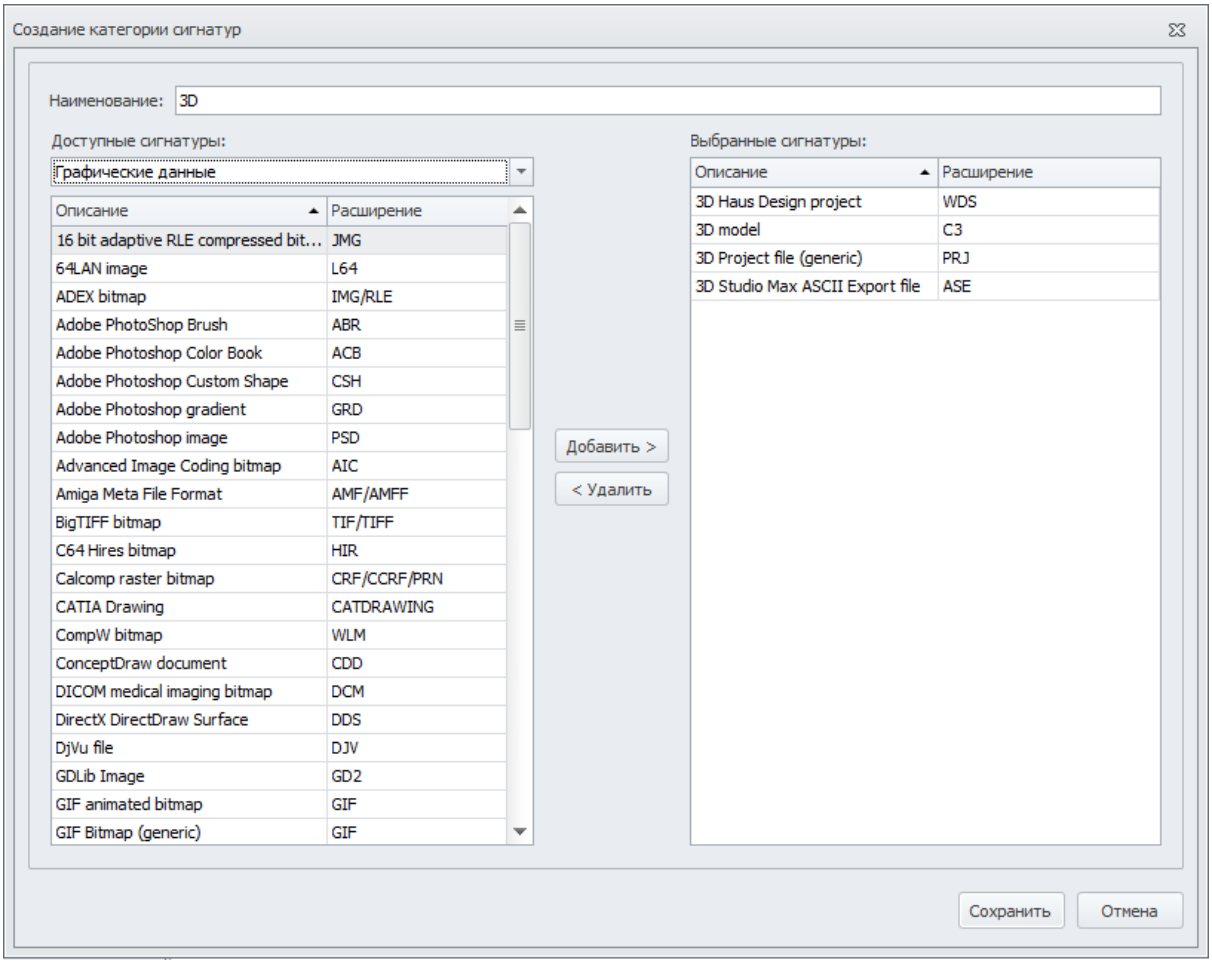
- создавать категории сигнатур;
- наполнять созданные категории, копируя в них сигнатуры из числа предустановленных;
- удалять созданные категории сигнатур, если они не используются ни в одном правиле.

Создание категории сигнатур

Чтобы добавить категорию сигнатур:

1. Перейдите к разделу **Категории сигнатур**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Создать категорию сигнатур**;
   - воспользуйтесь кнопкой **Создать категорию сигнатур**, расположенной в верхней части Панели навигации;
   - щелкните правой кнопкой мыши в области **Категории сигнатур** и в контекстном меню выберите **Создать категорию сигнатур**;
   - нажмите Ctrl+N.

   На экран будет выведено диалоговое окно **Создание категории сигнатур**.



3. В поле **Наименование** введите название создаваемой категории.
4. На панели **Доступные сигнатуры** вы можете выбрать из раскрывающегося списка одну из предустановленных категорий сигнатур. По умолчанию отображаются все предустановленные сигнатуры.
5. На левой панели выберите сигнатуры, которые вы хотите включить в новую категорию. Чтобы выделить несколько сигнатур сразу, используйте клавиши **Ctrl** и **Shift**. Чтобы перенести выбранные сигнатуры в новую категорию, нажмите **Добавить**. Чтобы удалить сигнатуры из списка вносимых в новую категорию, выберите их на правой панели **Выбранные сигнатуры** и нажмите **Удалить**.
6. Нажмите **Сохранить**.

Изменение категории сигнатур

После того, как вы создали категорию сигнатур (см. "Создание категории сигнатур"), вы можете наполнить ее одним из следующих способов:

1. Перейдите в режим редактирования сигнатуры и определите список сигнатур, как описано в разделе "Создание категории сигнатур". Для перехода в режим редактирования выбранной категории выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить**;
   - нажмите кнопку **Изменить** в верхней части Панели навигации;
   - дважды щелкните левой кнопкой мыши по названию выделенной категории;
   - щелкните по по названию выделенной категории правой кнопкой мыши и в контекстном меню выберите **Изменить**;

- нажмите Ctrl+E.

2. Копировать сигнатуры из других категорий непосредственно в рабочей области Консоли.

Чтобы скопировать сигнатуру из одной категории в другую:

1. Перейдите к разделу **Категории сигнатур**.
2. В области **Категории сигнатур** на Панели навигации выберите название предустановленной категории, которая содержит сигнатуру, которую нужно скопировать.
3. В рабочей области главного окна выберите строку с названием сигнатуры, которую нужно скопировать. Вы можете выделить несколько сигнатур сразу, используя клавиши **Ctrl** и **Shift**.
4. Щелкните левой кнопки мыши по выделенной строке и, не отпуская кнопку, перетащите курсор в область **Категории сигнатур** на Панели навигации. Подведите курсор мыши к названию созданной ранее категории, куда нужно добавить сигнатуры. После того как слева от названия выбранной категории появится желтая стрелка, отпустите левую кнопку мыши.

В результате сигнатура будет скопирована в выбранную категорию.

Чтобы исключить сигнатуру из категории, выберите эту сигнатуру и выполните одно из следующих действий:

- нажмите кнопку **Исключить сигнатуру из категории**, расположенную вверху области **Сигнатуры**;
- щелкните правой кнопкой мыши и в раскрывшемся меню выберите **Исключить сигнатуру из категории**;
- нажмите клавишу **Delete**.

Удаление категории сигнатур

Важно!

Удалению не подлежат:

- категории сигнатур, используемые в каком-либо правиле File Monitor;
- предустановленные категории сигнатур.

Чтобы удалить категорию сигнатур:

1. Перейдите к разделу **Категории сигнатур**.
2. Щелкните левой кнопкой мыши по названию нужной категории сигнатур.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - щелкните по по названию выделенной категории правой кнопкой мыши и в контекстном меню выберите **Удалить**;
   - нажмите Ctrl+D.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление категории сигнатур.

Важно!

Поскольку работа с категориями сигнатур ведется в режиме редактирования схемы безопасности, то для того, чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. раздел "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

Приложения

Чтобы перейти к разделу **Приложения**, воспользуйтесь кнопкой **Приложения**, расположенной на Панели навигации, или выберите в главном меню команду **Переход** > **Приложения**.

В этом разделе Панель навигации разделена на две группы элементов:

- **Списки приложений**
- **Протокол приложений**

Группа элементов **Списки приложений** содержит списки, используемые для контроля доступа сотрудников к приложениям:

- запрет запуска приложений в режиме черных и белых списков: подробнее см. "Правило для Application Monitor";
- запрет создания снимков экрана сотрудником: подробнее см. "Правило для ScreenShot Control Monitor";
- автоматическое создание снимков экранов Системой: подробнее см. "Правило для ScreenShot Monitor";
- контроль вставки данных в приложения: подробнее см. "Правило для Clipboard Monitor".

Группа элементов **Протокол приложений** позволяет, используя фильтры, просмотреть информацию обо всех приложениях, запускаемых на контролируемых рабочих станциях под управлением ОС семейства MS Windows. Из **Протокола приложений** вы можете добавлять приложения в списки для ОС MS Windows.

После установки Агента InfoWatch Device Monitor на рабочие станции под управлением ОС семейства MS Windows и их перезагрузки Система автоматически начинает получать информацию о приложениях, запускаемых на контролируемых рабочих станциях.

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".

Информация обо всех запусках и установках формирует *протокол приложений*.

Важно!

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

Информация о работе с протоколами и списками приложений содержится в подразделах:

- Создание и изменение списка приложений
- Создание и изменение фильтра приложений
- Экспорт протокола приложений

Создание и изменение списка приложений

Списки используются для разрешения или запрещения запуска определенных приложений на компьютерах.

Для управления черными и белыми списками, Система поддерживает функционал создания списков приложений, в том числе из **Протокола приложений** (см. "Протокол приложений").

Создание списка приложений

Чтобы создать пустой список приложений:

1. Перейдите к разделу **Приложения**.
2. На Панели навигации установите курсор в группе элементов **Списки приложений** и выполните одно из следующих действий:
   - в меню группы элементов **Списки приложений** нажмите **Создать список приложений**;
   - в главном меню выберите команду **Правка** > **Создать список приложений**;
   - нажмите правой кнопкой мыши в группе элементов **Списки приложений** и из раскрывшегося списка выберите **Создать список приложений**;
   - нажмите **Ctrl**+**N**.
3. В поле **Наименование списка** введите название для списка.
4. В поле **Операционная система** выберите одно из семейств ОС:
   - **Windows** – список будет отмечен значком
   - **Linux** – список будет отмечен значком

   > **Примечание:**
   >
   > Вы можете использовать списки приложений для ОС семейства Linux только в правиле Clipboard Monitor.

5. Нажмите **Сохранить**.

После создания списка, добавьте в него приложения.

Добавление приложений в список

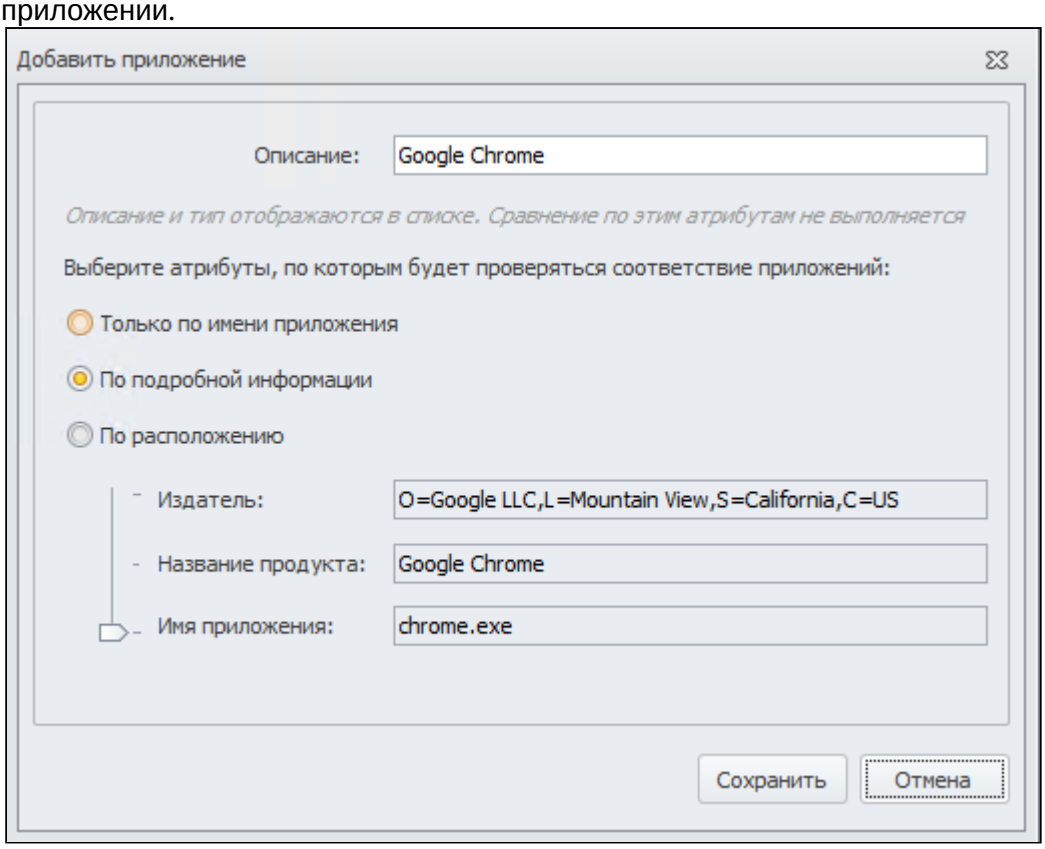
Вы можете:

- Добавить приложение, указав исполняемый файл (доступно только для списков приложений **для ОС семейства MS Windows**);
- Добавить приложение в список вручную;
- Добавить приложение в список автоматически из протокола приложений (доступно только для списков приложений **для ОС семейства MS Windows**);
- Добавить приложение из уже существующего списка.

Добавление в список с помощью исполняемого файла

1. Перейдите в раздел **Приложения**.
2. Слева вверху в группе элементов **Списки приложений** выберите список, в который хотите добавить приложение.

3. Правее на панели **Список приложений** нажмите кнопку
4. В открывшемся окне укажите исполняемый файл приложения.
5. В открывшемся окне для добавления будут заполнены поля с информацией о приложении.



Для добавления нажмите **Сохранить**.

Добавление приложения в список вручную

1. Перейдите в раздел **Приложения**.
2. Слева вверху в группе элементов **Списки приложений** выберите список, в который хотите добавить приложение.
3. Правее на панели **Список приложений** нажмите кнопку .
4. В открывшемся окне **Добавить приложение** укажите параметры, по которым будет проверяться соответствие приложения:
   - **Только по имени приложения**
     В поле **Имя приложения** введите:
     - для приложений ОС Windows: имя исполняемого файла с расширением, например *notepad.exe*;
     - для приложений ОС Linux: имя (без дополнительных символов), соответствующее запускаемому процессу, например *pluma*;
   - **По подробной информации**
     Фильтрация приложений по уточняющей информации в порядке уточнения **Издатель**, **Название продукта**, **Имя приложения**.

     Примечание:

Добавление по подробной информации доступно только для списков приложений **для ОС семейства MS Windows**.

- **По расположению**
  Фильтрация приложений по уточняющей информации от **Расположения** до **Имени приложения**.

  Примечание:

  Не указывайте имя файла в поле **Расположение**, только путь к директории. Например: *C:\Windows\System32*, */usr/bin/*.

5. Для добавления приложения нажмите **Сохранить**.

Вы также можете добавить приложения в список вручную из **Протокола приложений**.
Действие доступно только для списков приложений **для ОС семейства MS Windows**.

Для этого

1. Перейдите к разделу **Приложения**.
2. На Панели навигации, в группе элементов **Протокол приложений**, выберите необходимый фильтр (о создании фильтра приложений см. "Создание и изменение фильтра приложений").
3. На панели **Протокол приложений** выберите одну или несколько записей. Для выбора нескольких записей отмечайте их курсором, зажав клавишу **Shift** или **Ctrl**.
4. Выполните одно из следующих действий:
   - на панели **Протокол приложений** нажмите **Добавить приложение в список вручную**;
   - в главном меню выберите команду **Правка** > **Добавить приложение в список вручную**;
   - нажмите правой кнопкой мыши на панели Протокол приложений и из раскрывшегося списка выберите **Добавить приложение в список вручную**.
5. В открывшемся окне **Добавить приложение** вы можете изменить параметры.
6. Для добавления нажмите **Сохранить**.
7. Если вы выбрали несколько записей приложений, повторите шаги 5 и 6 для остальных записей.
8. В окне, информирующем об успешном добавлении приложений, нажмите **OK**.

Добавление в список автоматически из протокола приложений
Система позволяет наполнять списки приложений автоматически, на основании данных из протокола приложений.
Действие доступно только для списков приложений **для ОС семейства MS Windows**.

Чтобы добавить одно или несколько приложений в список автоматически:

1. Перейдите в раздел **Приложения**.
2. На Панели навигации, в группе элементов **Протокол приложений**, выберите необходимый фильтр (о создании фильтра приложений см. "Создание и изменение фильтра приложений").
3. На панели **Протокол приложений** выберите одну или несколько записей. Для выбора нескольких записей отмечайте их курсором, зажав клавишу **Shift** или **Ctrl**.
4. Выполните одно из следующих действий:

- на панели Протокол приложений нажмите **Добавить приложение в список автоматически**;
- в главном меню выберите команду **Правка** > **Добавить приложение в список автоматически**;
- нажмите правой кнопкой мыши на панели **Протокол приложений** и из раскрывшегося списка выберите **Добавить приложение в список автоматически**.

5. В появившемся окне:
   - выберите существующий список

   или
6. нажмите **Создать новый**, в открывшемся окне, в поле **Наименование списка**, введите название для списка и нажмите **Сохранить**.
7. Нажмите **Выбрать**.
8. В окне, информирующем об успешном добавлении приложений, нажмите **ОК**.

Добавление приложения из другого списка

1. Перейдите к разделу **Приложения**.
2. Установите курсор в группе элементов **Списки приложений**.
3. Нажмите кнопку на панели **Список приложений**.
4. Выберите приложение из списка/списков и нажмите **Добавить приложение в список**.
5. Из раскрывающегося списка выберите **Добавить автоматически** или **Выбрать вручную**.

Примечание:

Не поддерживается добавление приложения из списка для ОС другого семейства. То есть вы не можете добавить в список для Linux приложение из списка для Windows, и наоборот.

Редактирование и удаление приложений из списка

Чтобы отредактировать приложение в списке:

1. На панели **Список приложений** нажмите либо щелкните по приложению правой кнопкой мыши и в контекстном меню выберите **Изменить**.
2. Здесь вы можете настроить параметры, которые будут использованы для фильтрации приложений (см. Добавление приложения в список вручную)

Чтобы удалить приложение из списка:

1. На панели **Список приложений** нажмите либо щелкните по приложению правой кнопкой мыши и в контекстном меню выберите **Удалить**.
2. Нажмите **Да**, чтобы удалить приложение из схемы безопасности.

Создание и изменение фильтра приложений

Фильтры позволяют настроить формирование протокола приложений (см. "Приложения") так, что будет отображаться информация только о приложениях, соответствующих выбранным вами условиям.

Важно!

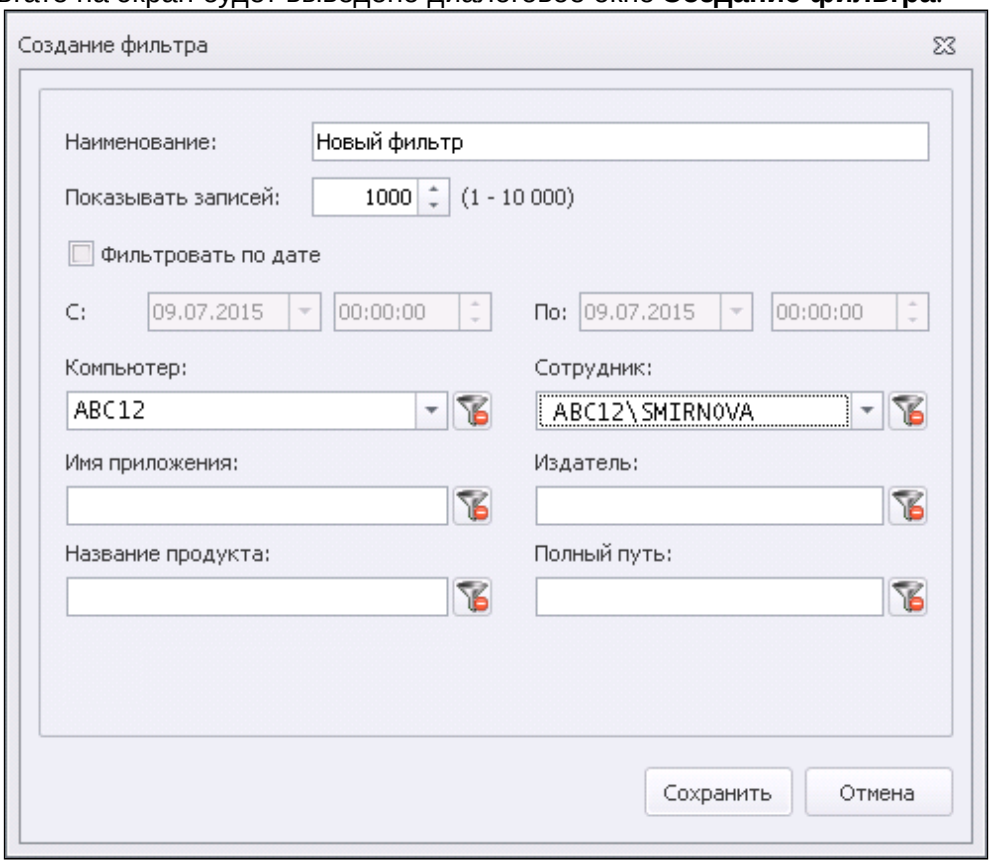
Предустановленный фильтр **За сегодня** показывает только приложения, запущенные в конкретный выбранный день впервые с момента установки Агента на компьютер.

Приложения, запущенные сразу после установки Агента, будут показаны в фильтре **Все**.

Чтобы создать новый фильтр:

1. Перейдите к разделу **Приложения**.
2. На Панели навигации установите курсор в группе элементов **Протокол приложений** и выполните одно из следующих действий:
   - в меню группы элементов **Протокол приложений** нажмите **Создать фильтр**;
   - в главном меню выберите команду **Правка** > **Создать фильтр**;
   - нажмите правой кнопкой мыши в группе элементов **Протокол приложений** и из раскрывшегося списка выберите **Создать фильтр**.

   В результате на экран будет выведено диалоговое окно **Создание фильтра**.



3. В поле **Наименование** введите название фильтра.
4. В поле **Показывать записей** укажите количество записей, которые должно отображаться в **Протоколе приложений**.
5. Для фильтрации приложений по дате отметьте поле **Фильтровать по дате** и укажите продолжительность отображаемого периода в полях **С** и **По**.
6. При необходимости, определите дополнительные условия фильтрации:
   - В поле **Компьютер** выберите компьютер, протокол приложений с которого вы хотите просматривать;
   - В поле **Сотрудник** выберите учетную запись сотрудника, запускающего приложения;
   - В поле **Имя приложения** введите название файла приложения;
   - В поле **Издатель** укажите издателя программного обеспечения;

- В поле **Название продукта** введите его название;
- В поле **Полный путь** укажите расположение приложения;

Для удаления ненужного условия фильтрации нажмите  в строке этого условия.

7. Нажмите **Сохранить**.

Чтобы изменить фильтр, воспользуйтесь кнопкой  в разделе **Протокол приложений** на Панели навигации, в контекстном меню или нажмите сочетание клавиш **Ctrl+E**.

Чтобы удалить фильтр:

1. Воспользуйтесь кнопкой  в разделе **Протокол приложений** на Панели навигации, в контекстном меню или нажмите сочетание клавиш **Ctrl+D**.
2. Нажмите **Да**, чтобы подтвердить удаление.

Экспорт протокола приложений

Чтобы экспортировать протокол приложений:

1. Перейдите в раздел **Приложения** на панели навигации.
2. На панели навигации, в группе элементов **Протокол приложений** выберите необходимый протокол.
3. В меню группы **Протокол приложений** нажмите  **Экспортировать протокол приложений** либо используйте меню **Правка**>**Экспортировать протокол приложений**.
4. Укажите директорию и имя файла экспорта и нажмите **Сохранить**.
   Протокол будет сохранен в формате **.xls**.

Блокада приложений

Блокада приложений – функциональность, с помощью которой Device Monitor перехватывает чтение и запись файлов приложениями. Для этого Device Monitor использует модуль File Operations Monitor. Device Monitor отправляет события перехвата в Traffic Monitor, который анализирует их с учетом своих политик безопасности.

Чтобы использовать правило для File Operations Monitor (см. "Правило для File Operations Monitor"), **обязательно** добавьте конфигурацию Блокады приложений в схему безопасности Device Monitor.

> **Примечание:**
>
> Если вы не добавите конфигурацию Блокады приложений, правило для File Operations Monitor будет недоступно.

Конфигурация состоит из профилей приложений и профилей ОС. Профили приложений используются при настройке правила перехвата. При перехвате используются оба типа профилей.

Вы можете добавить профили вручную или импортировать подготовленную конфигурацию из файла.

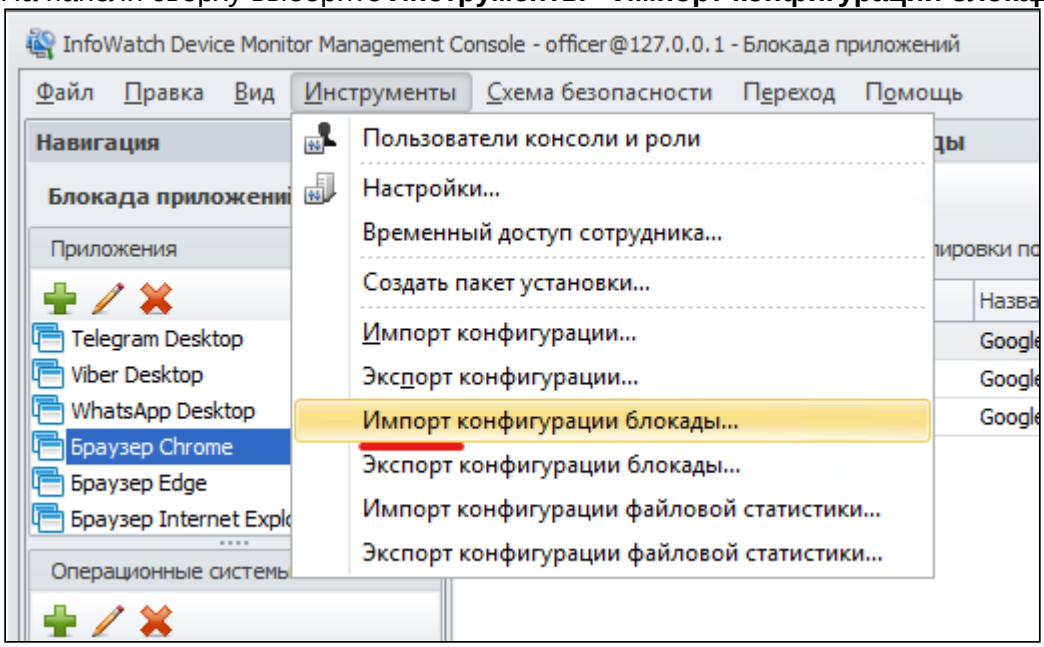
> **Важно!**
>
> Рекомендуем использовать подготовленную конфигурацию Блокады приложений из файлов. Для получения конфигурации обратитесь к специалистам компании InfoWatch.

Чтобы Device Monitor передавал события Блокады приложений в Traffic Monitor, должны быть также доступны соответствующие профили. Создайте их самостоятельно, как описано ниже, или запросите у специалистов компании InfoWatch.

Импорт и экспорт конфигурации Блокады приложений

Чтобы импортировать подготовленную конфигурацию Блокады приложений:

1. На панели сверху выберите **Инструменты > Импорт конфигурации блокады**.



2. В открывшемся окне выберите файл конфигурации с расширением `.xml`. Импортированная конфигурация будет доступна для просмотра и редактирования на вкладке **Блокада приложений**.

Важно!

Импорт или редактирование конфигурации Блокады приложений – это изменение схемы безопасности. После изменения распространите новую схему на Агенты Device Monitor.

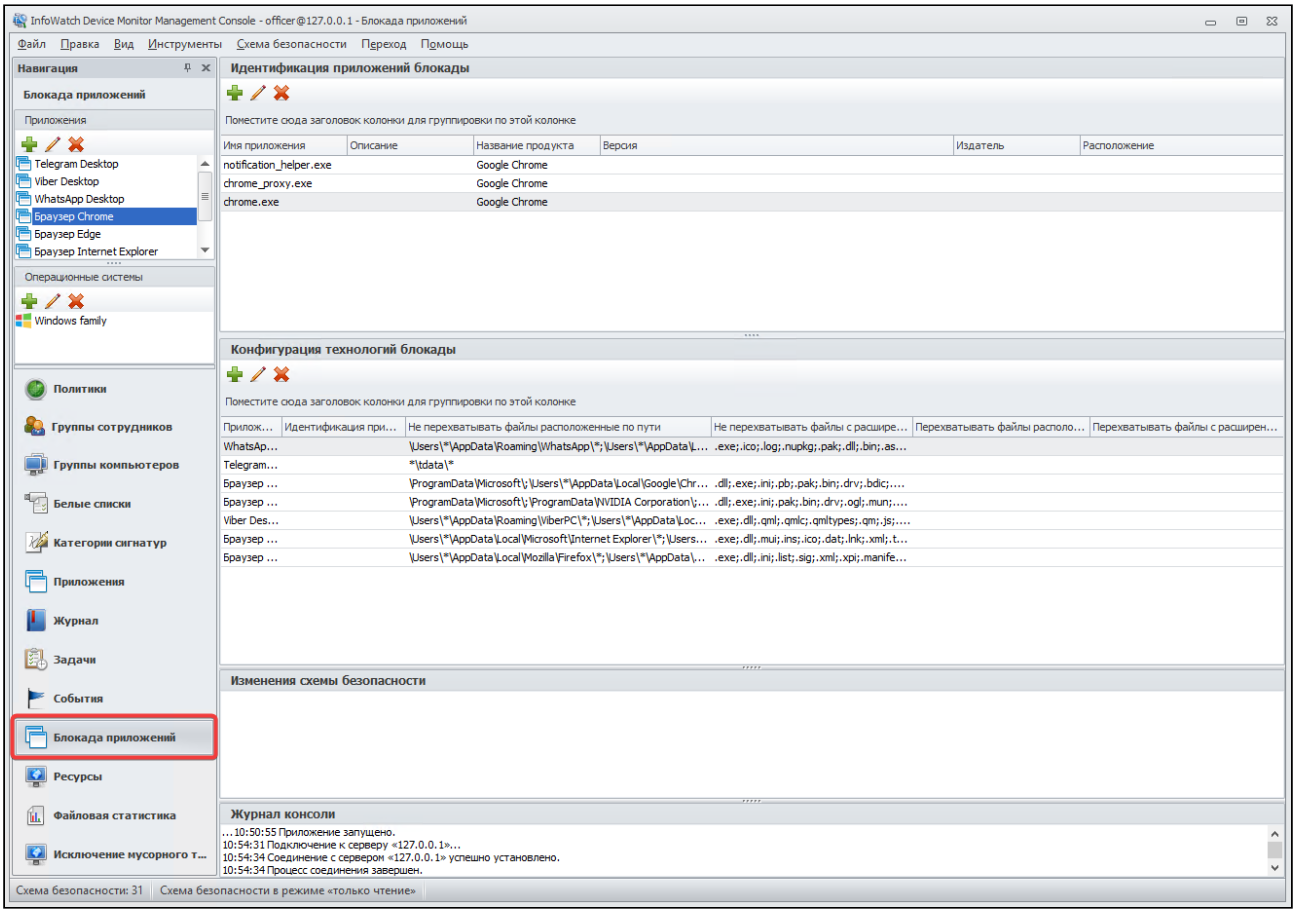
Вы также можете экспортировать текущую конфигурацию Блокады приложений для использования на другом сервере Device Monitor.

Чтобы экспортировать конфигурацию Блокады приложений:

1. На панели сверху выберите **Инструменты > Экспорт конфигурации блокады**.
2. В открывшемся окне укажите расположение и имя файла конфигурации и нажмите **Сохранить**.
   В результате на компьютере будет сохранен файл конфигурации с расширением `.xml`.

Редактирование конфигурации и добавление профилей вручную

Для просмотра и редактирования конфигурации, на панели внизу слева выберите вкладку **Блокада приложений**.



Примечание:

В настройках профилей при указании расширений и путей:

- допускается использование масок;
- разделителем служит "`;`";
- путь должен начинаться со стандартного символа разделения элементов пути на файловой системе "`\`", либо со спецсимвола (например, `*`);
- исключаемые/включаемые пути должны задавать относительный путь к файлу, то есть имена дисков недопустимы.

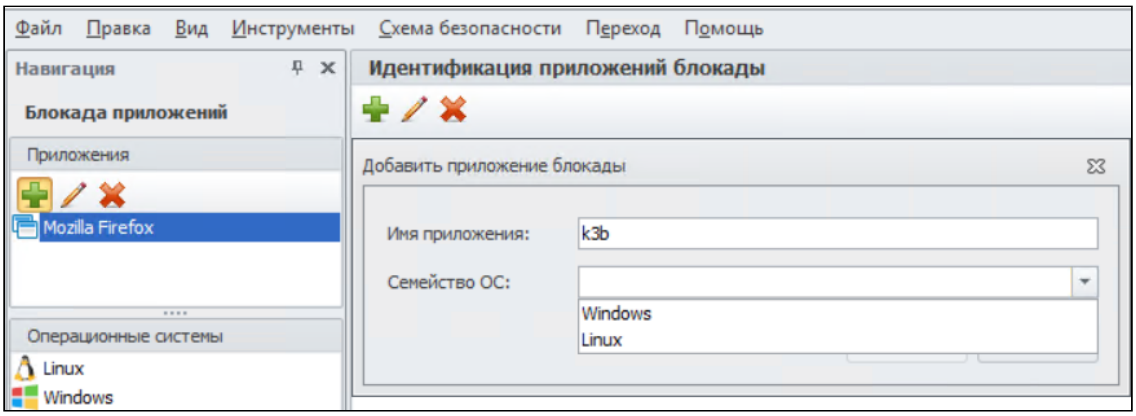
Для редактирования элементов конфигурации используйте кнопку .

Настройка профиля приложения

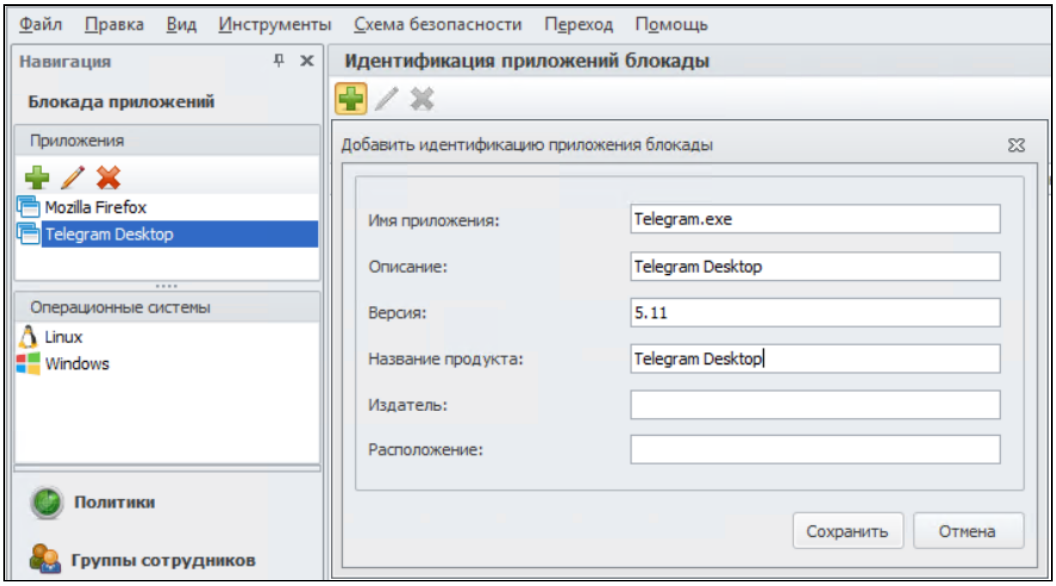
Для настройки профиля приложения выполните действия:

1. Чтобы добавить профиль приложения, нажмите кнопку  в блоке **Приложения**. В открывшемся окне задайте:
   - **Имя приложения**;

- **Семейство ОС** – Windows или Linux.

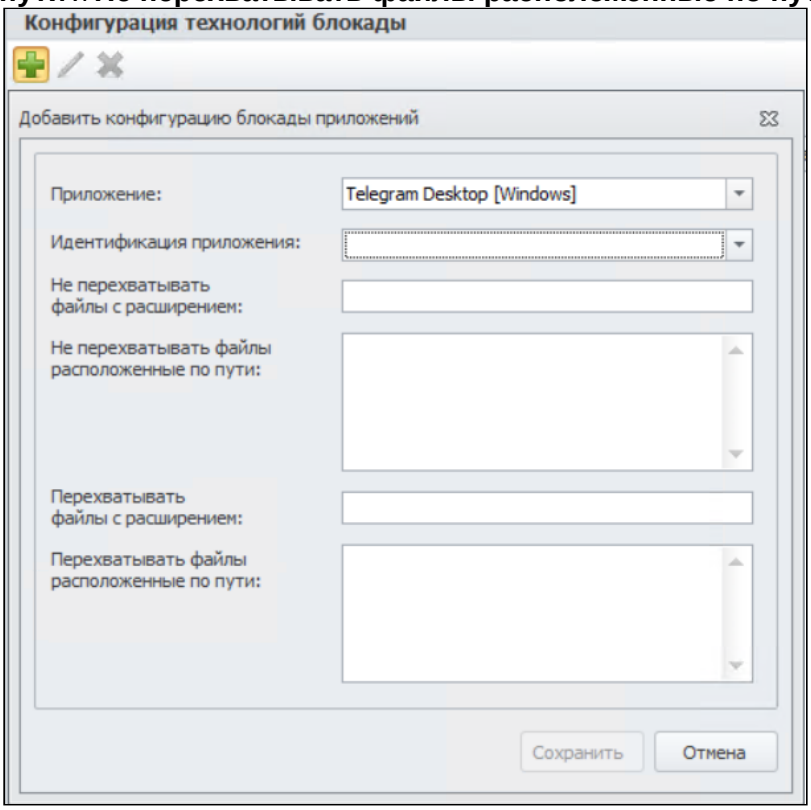


2. Выберите настраиваемый профиль и заполните блок **Идентификация приложений блокады**. Нажмите кнопку  и задайте идентификацию приложения:
   a. Для ОС Windows:
      - **Имя приложения** – исходное имя исполняемого файла;
      - **Описание** – описание файла;
      - **Версия** – версия (диапазон версий) приложения;
      - **Название продукта**;
      - **Издатель**;
      - **Расположение**.
   b. Для ОС Linux:
      - **Имя приложения**;
      - **Описание**;
      - **Расположение**.



   c. Вы можете указать более одного контролируемого приложения в одном профиле.
3. Добавьте конфигурации технологий блокады:
   a. В поле **Приложение** выберите имя профиля из списка.
   b. В поле **Идентификация приложения** выберите версию приложения из списка приложений, относящихся к выбранному профилю, или оставьте пустым, чтобы конфигурация относилась ко всему профилю.
   c. При необходимости ниже укажите:

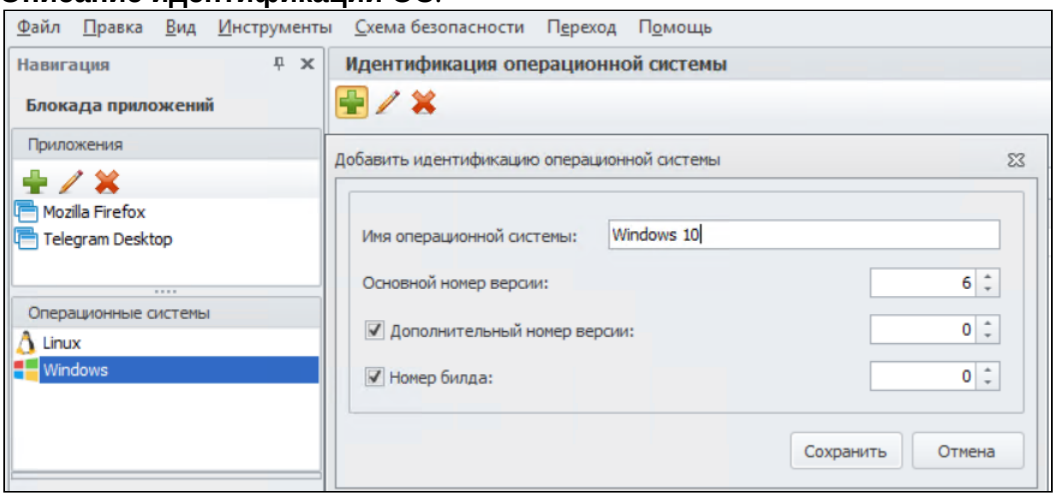
- расширения файлов, которые требуется перехватывать или исключить из перехвата (поля **Перехватывать файлы с расширением** и **Не перехватывать файлы с расширением**);
- пути расположения файлов, которые требуется перехватывать или исключить из перехвата (поля **Перехватывать файлы расположенные по пути** и **Не перехватывать файлы расположенные по пути**).



Настройка профиля ОС

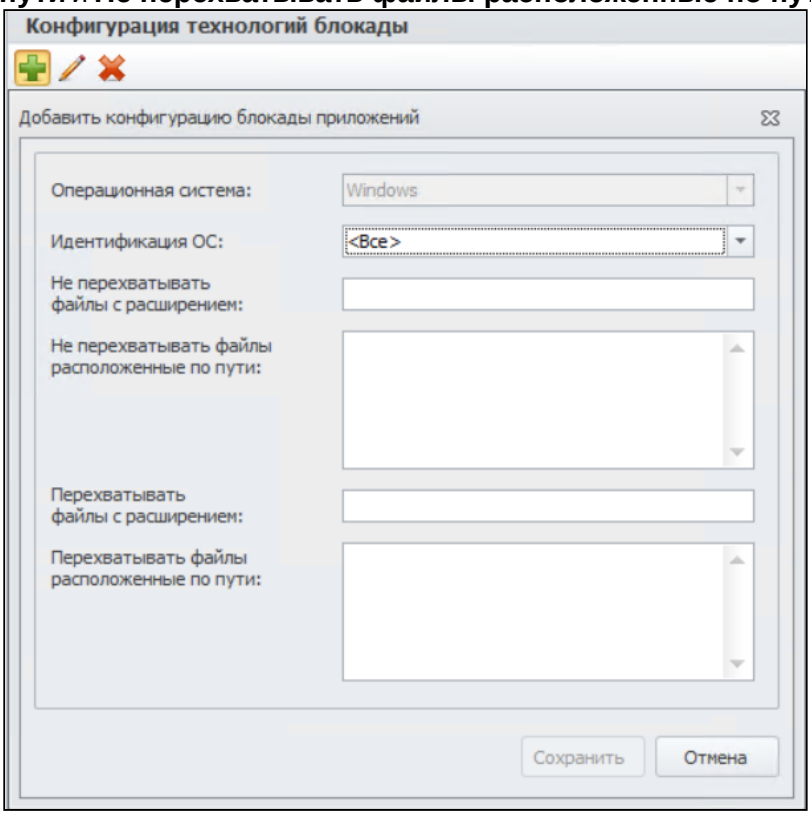
1. Чтобы добавить профиль ОС, в блоке **Операционные системы**:
   a. выберите нужную ОС;
   b. нажмите кнопку ;
   c. задайте в открывшемся окне имя новому профилю.
2. Выберите настраиваемый профиль и заполните блок **Идентификация операционной системы**. Нажмите кнопку задайте идентификацию ОС:
   a. Для ОС Windows:
      - **Имя операционной системы**;
      - **Основной номер версии**;
      - При необходимости вы можете также указать:
        - **Дополнительный номер версии**;
        - **Номер билда**.
   b. Для ОС Linux:
      - **Имя дистрибутива**;

- **Описание идентификации ОС**.



c. Вы можете указать более одной ОС в одном профиле.

3. Добавьте конфигурации технологий блокады:
   a. В поле **Идентификация ОС** выберите версию ОС из списка версий, относящихся к выбранному профилю, или оставьте пустым, чтобы конфигурация относилась ко всему профилю.
   b. При необходимости ниже укажите:
      - расширения файлов, которые требуется перехватывать или исключить из перехвата (поля **Перехватывать файлы с расширением** и **Не перехватывать файлы с расширением**);
      - пути расположения файлов, которые требуется перехватывать или исключить из перехвата (поля **Перехватывать файлы расположенные по пути** и **Не перехватывать файлы расположенные по пути**).



4. Сохраните схему безопасности.

События Блокады приложений

События, передаваемые в Traffic Monitor, содержат следующие данные об операции с файлом:

- Тип файловой операции:
  - чтение;
  - запись.
- Данные о приложении, в котором проводилась операция.
- Данные активной вкладки браузера (если операция с файлом проводилась в браузере). URL-адрес активной вкладки отображается в событиях Traffic Monitor версии 7.6.0 и выше.

> **Примечание:**
>
> Система создает событие и сохраняет данные об активной вкладке, когда приложение читает/записывает файл. Вкладка может быть определена некорректно, если пользователь переключился на другую вкладку до момента создания события.

- Данные о файле.
- Теневую копию файла.
- Снимок экрана (если создание снимка настроено в правиле).

Вы также можете просмотреть события Блокады приложений в консоли управления Device Monitor, в разделе **События** (см. "Просмотр событий DM").

Ресурсы

Для правил автоматического создания снимков экрана и контроля ввода с клавиатуры ОБ имеет возможность определить, какие конкретно веб-ресурсы контролировать/исключить из контроля. Для этого ОБ может создать список таких ресурсов.

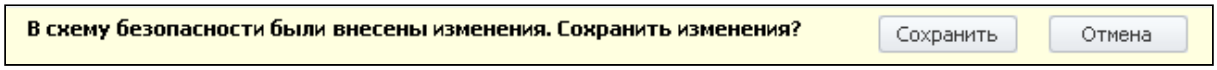
Для работы с ресурсами предназначен раздел **Ресурсы**. Чтобы перейти к этому разделу, воспользуйтесь кнопкой **Ресурсы**, расположенной на Панели навигации.
Информация по работе с ресурсами содержится в подразделах:

- Добавление списка ресурсов
- Редактирование списка ресурсов
- Удаление списка ресурсов
- Создание списка ресурсов из файла
- Выгрузка списка ресурсов в файл

Добавление списка ресурсов

Чтобы создать список ресурсов:

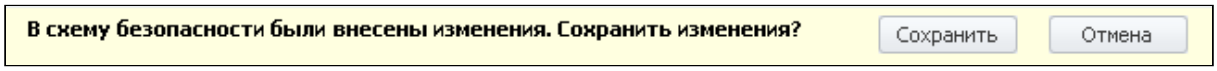
1. Перейдите в **Ресурсы**.
2. Нажмите **Добавить список ресурсов** вверху панели навигации.
3. Введите наименование списка.
4. Нажмите **Сохранить**.
5. Нажмите **Сохранить** в информационном сообщении.



Список ресурсов будет создан.

Чтобы наполнить созданный список необходимыми ресурсами:

1. Перейдите в **Ресурсы**.
2. Нажмите **Добавить ресурс** на вкладке **Ресурсы**.
3. Выберите тип ресурса: домен, Url, Url содержит. Для вызова справки по типам ресурсов наведите курсор на в поле **Тип**.
4. Введите ресурс и его описание в соответствующих полях.
5. Нажмите **Сохранить**. Нажмите **Сохранить** в информационном сообщении.



Ресурс будет создан в списке ресурсов. Подробная информация о нем отобразится ниже в области **Подробно**.

Примечание:

Ниже приведен принцип, по которому Система устанавливает соответствие посещаемого ресурса ресурсу из списка:

Для типа **Домен**

Соответствие производится на точное совпадение *<хост>,* включая поддомены. Регистр не учитывается.

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

Для типа **URL**

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

Регистр учитывается (кроме части *<хост>*).

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

Для типа **URL содержит**

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

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

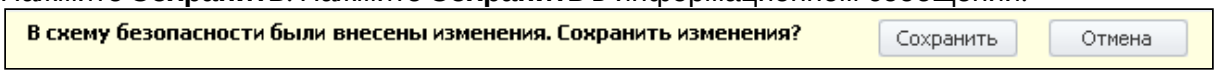
Важно!

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

Редактирование списка ресурсов

Чтобы отредактировать список ресурсов:

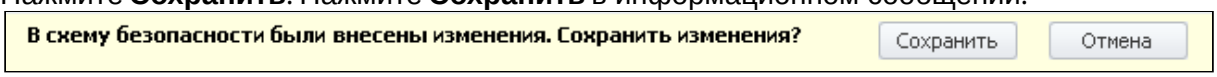
1. Перейдите в раздел **Ресурсы**.
2. Нажмите **Редактировать список ресурсов** вверху панели навигации.
3. В открывшемся окне отредактируйте наименование списка.
4. Нажмите **Сохранить**. Нажмите **Сохранить** в информационном сообщении.



Отредактированный список ресурсов будет сохранен.

или

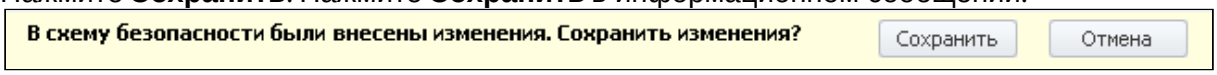
1. Перейдите в раздел **Ресурсы**.
2. На панели навигации дважды щелкните по списку, который необходимо отредактировать.
3. В открывшемся окне отредактируйте наименование списка.
4. Нажмите **Сохранить**. Нажмите **Сохранить** в информационном сообщении.



Отредактированный список ресурсов будет сохранен.

Чтобы отредактировать ресурс из списка:

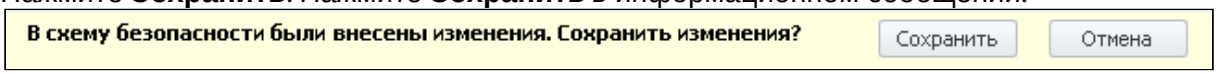
1. Перейдите в раздел **Ресурсы**.
2. Справа в области **Ресурсы** щелчком выберите ресурс из списка, который необходимо отредактировать.
3. Нажмите **Редактировать ресурс** на панели в области **Ресурсы**.
4. В открывшемся окне внесите необходимые изменения.
5. Нажмите **Сохранить**. Нажмите **Сохранить** в информационном сообщении.



Изменения будут сохранены. Подробная информация о ресурсе отобразится ниже в области **Подробно**.

или

1. Перейдите в раздел **Ресурсы**.
2. Справа в области **Ресурсы** двойным щелчком откройте на редактирование требуемый ресурс из списка.
3. В открывшемся окне внесите изменения.
4. Нажмите **Сохранить**. Нажмите **Сохранить** в информационном сообщении.

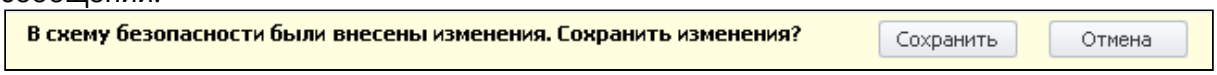


Изменения будут сохранены. Подробная информация о ресурсе отобразится ниже в области **Подробно**.

Удаление списка ресурсов

Чтобы удалить список ресурсов:

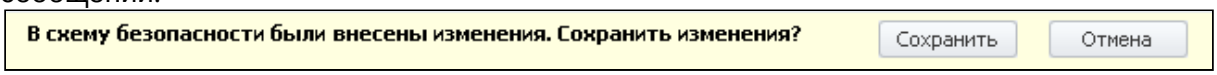
1. Перейдите в раздел **Ресурсы**.
2. Нажмите **Удалить список ресурсов** вверху панели навигации.
3. В открывшемся окне подтвердите действие. Нажмите **Сохранить** в информационном сообщении.



Список ресурсов будет удален.

Чтобы удалить ресурс из списка:

1. Перейдите в раздел **Ресурсы**.
2. Справа в области **Ресурсы** щелчком выберите ресурс из списка, который необходимо удалить.
3. Нажмите **Удалить ресурс** на панели в области **Ресурсы**.
4. В открывшемся окне подтвердите действие. Нажмите **Сохранить** в информационном сообщении.



Ресурс будет удален.

Создание списка ресурсов из файла

При необходимости ОБ имеет возможность создать список ресурсов из файла. Это может понадобиться, например, чтобы быстро перенести данные при миграции или развертывании нового сервера Device Monitor. Загружаемый файл должен соответствовать следующим параметрам:

- иметь расширение .txt;
- иметь кодировку UTF-8;

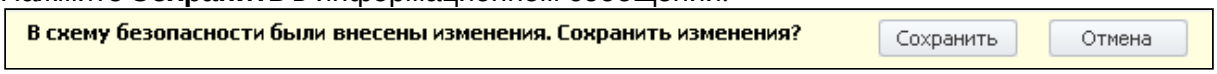
- строка должна содержать информацию:
  - тип ресурса: domain/URL/URL contains;
  - ресурс;
  - описание;
- в качестве разделителя использовать табуляцию;
- одна строка в файле – это одна запись в списке.

Примечание:

Наименование загружаемого файла будет записано как наименование списка в Системе. Если в Системе уже существует список с таким названием, то к названию списка добавится (n+1), где n - число, использующееся в предыдущем списке. Дублирующие записи (не имеющие уникального сочетания тип + ресурс) не будут загружены в Систему.

Чтобы создать список ресурсов из файла:

1. Перейдите в раздел **Ресурсы**.
2. Нажмите  на панели навигации.
3. Выберите файл, содержащий ресурсы, которые необходимо добавить в Систему. Нажмите **Сохранить** в информационном сообщении.



Список ресурсов будет добавлен.

Примечание:

Если при загрузке файла произошла ошибка, Система сообщит об этом с указанием в какой строке она была обнаружена. Список ресурсов не будет создан.
При загрузке файла могут произойти следующие типы ошибок:

- некорректно сформирована строка (например, отсутствует табуляция или не заполнено обязательное значение);
- не определен тип (указан тип, отличный от domain/URL/URL contains);
- тип не соответствует ресурсу (например, указан тип domain, а значение соответствует типу URL).

Выгрузка списка ресурсов в файл

Чтобы выгрузить список ресурсов в файл:

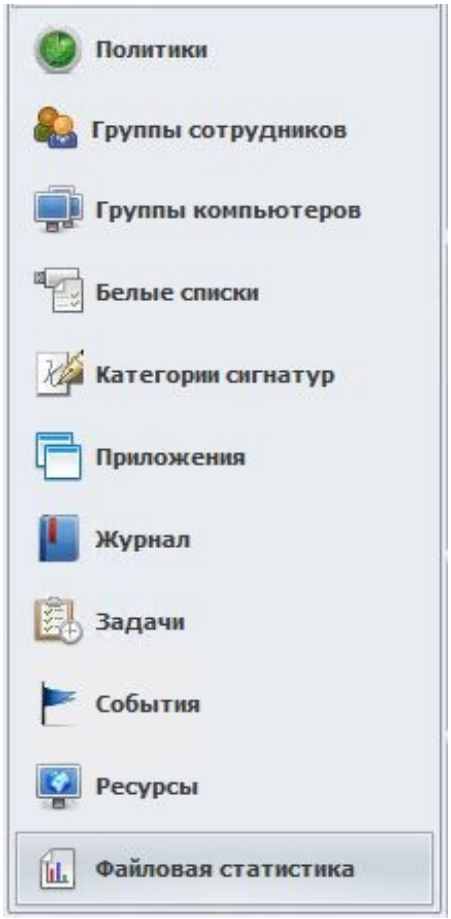
1. Перейдите в раздел **Ресурсы**.
2. Нажмите  **Выгрузить список ресурсов в файл** на панели навигации.
3. Выберите, куда необходимо сохранить список ресурсов. Нажмите **Сохранить**. Файл со списком ресурсов будет сохранен в выбранную директорию.

Файловая статистика

Важно!

Функциональность предназначена только для InfoWatch Activity Monitor и InfoWatch Prediction.

Файловая статистика позволяет отслеживать действия персоны при работе с файлами. Чтобы перейти к разделу, воспользуйтесь кнопкой **Файловая статистика**, расположенной на Панели навигации.



В разделе Файловая статистика вы можете работать с приложениями файловой статистики и настраивать ее конфигурацию. Настройка перехвата чтения и записи файлов производится в правиле **Statistics** (подробнее см. "Правило для Statistics").

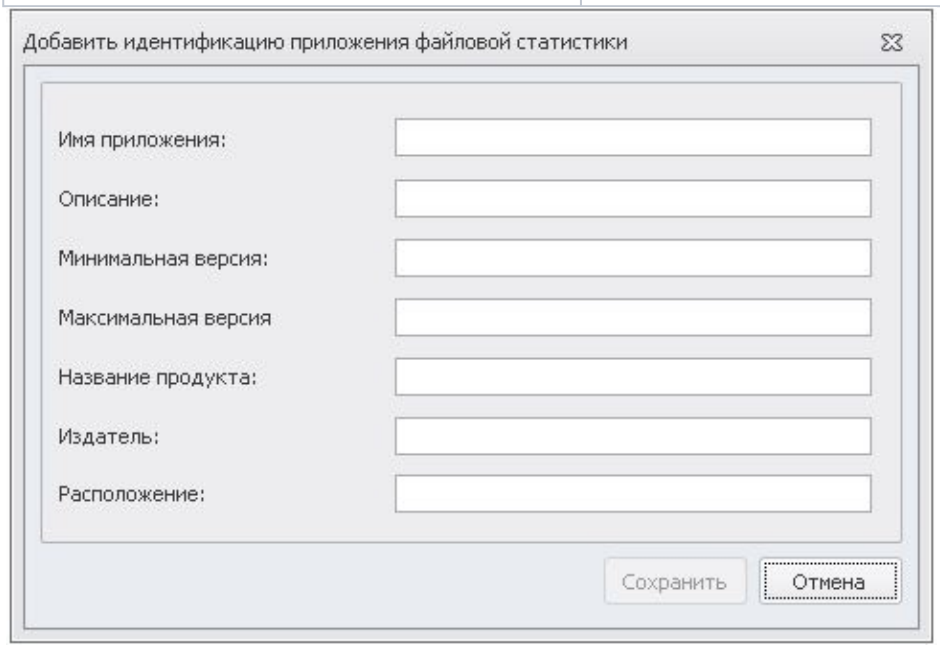
Чтобы добавить или отредактировать приложение файловой статистики:

Важно!

Чтобы внесенные изменения вступили в силу, необходимо сохранить схему безопасности (см. "Руководство пользователя InfoWatch Traffic Monitor. Работа в Консоли. Управления Device Monitor. Управление схемой безопасности. Общие действия при управлении схемой безопасности. Редактирование схемы безопасности"). В противном случае, все изменения будут утеряны.

1. В Консоли управления Device Monitor выберите раздел **Файловая статистика**.
2.

Действие	Шаги
Добавить приложение файловой статистики	В области **Приложения файловой статистики** на панели навигации нажмите **Добавить приложение** в верхней части панели навигации.
Отредактировать приложение файловой статистики	a. В области **Приложения файловой статистики** на панели навигации выберите название нужного приложения. b. Нажмите **Изменить приложение** в верхней части панели навигации, или дважды нажмите левой кнопкой мыши на названии приложения. Откроется диалоговое окно определения параметров приложения:



3. Укажите следующие параметры:
   - **Имя приложения** (например: Outlook.exe)
   - **Описание** (например: Outlook)
   - **Минимальная версия** (например: Outlook 2016)
   - **Максимальная версия** (например: Outlook 2021)
   - **Название продукта** (например: Outlook 2016)

- **Издатель** (например: Microsoft)
- **Расположение** (например: C:\Program Files)

4. Нажмите **Сохранить**.
5. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

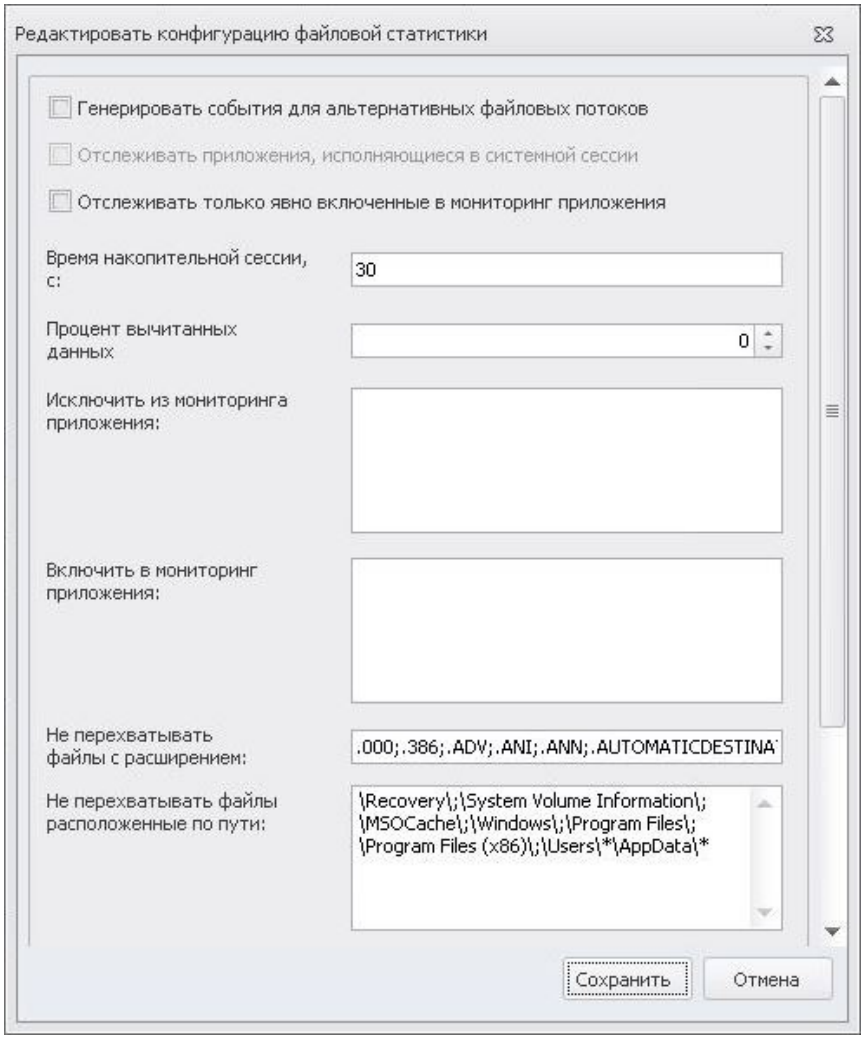
Чтобы удалить приложение файловой статистики:

1. Перейдите в раздел **Файловая статистика**.
2. Выберите приложение, которое необходимо удалить.
3. Нажмите **Удалить приложение** в верхней части панели навигации. Или дважды нажмите левой кнопкой мыши на названии приложения и в открывшемся списке выберите **Удалить приложение**.
4. Нажмите **Сохранить**.
5. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

Важно!

Чтобы изменения вступили в силу, необходимо сохранить схему безопасности (см. "Руководство пользователя InfoWatch Traffic Monitor. Работа в Консоли. Управления Device Monitor. Управление схемой безопасности. Общие действия при управлении схемой безопасности. Редактирование схемы безопасности"). В противном случае, все изменения будут утеряны.

1. В области **Конфигурация файловой статистики** нажмите **Редактировать конфигурацию файловой статистики**. Откроется диалоговое окно определения параметров конфигурации:



2. Выберите необходимые действия:
   - **Генерировать события для альтернативных файловых потоков**. 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. По умолчанию параметр выключен.
   - **Отслеживать приложения, исполняющиеся в системной сессии**.

     > **Важно!**
     >
     > Данная настройка отображается, однако отсутствует возможность ее включить. Мониторинг приложений, исполняющихся в системной сессии, не осуществляется.

   - **Отслеживать только явно включенные в мониторинг приложения**. Активируйте настройку, если необходимо отслеживать только те приложения, которые включены в мониторинг. По умолчанию параметр выключен.
3. Задайте значения параметров:

- **Время накопительной сессии**. 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 – 30 сек. Значение по умолчанию также можно уменьшить, в этом случае количество событий может увеличиться.
- **Процент вычитанных данных**. Настройка применяется, чтобы снизить количество системных событий открытия файла в Activity Monitor. Чем выше значение, тем меньше таких событий будет создаваться. Значение по умолчанию – 0.

4. **Исключить из мониторинга приложения**. Укажите приложения, которые необходимо исключить из мониторинга.
5. **Включить в мониторинг приложения**. Укажите приложения, которые необходимо включить в мониторинг.
6. Чтобы исключить перехват файлов с определенным расширением, добавьте расширение в поле **Не перехватывать файлы с расширением**.

> **Примечание:**
>
> Конфигурация по умолчанию содержит следующие исключения:
>
> .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; .tmp; .crdownloads; .thumbs.db

7. Чтобы исключить перехват файлов/папок, расположенных по определенному пути, укажите путь в поле **Не перехватывать файлы расположенные по пути**. 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.

> **Пример:**
>
> `\Docs\` – будет исключена папка `Docs` и все вложенные вне зависимости от расположения.
> `\Docs` или `\Docs*` – будет исключена папка `Docs` и любые варианты: `Docs1`, `Docs2` и т.д.
> `\Docs????*` – будет исключена любая папка, которая имеет имя `Docs` с четырьмя дополнительными символами (`Docs1234`)

Значение поля должно содержать не более 2000 символов.

> **Примечание:**
>
> Конфигурация по умолчанию содержит следующие исключения: \Recovery\;\System Volume Information\;\MSOCache\;\Windows\;\Program Files\;\Program Files (x86)\; \Users*\AppData\

8. Чтобы перехватывать файлы с определенным расширением, добавьте расширение в поле **Перехватывать файлы с расширением**.
9. Чтобы перехватывать файлы/папки, расположенные по определенному пути, укажите путь в поле **Перехватывать файлы расположенные по пути**. Правила указания папок смотрите выше в п.7.

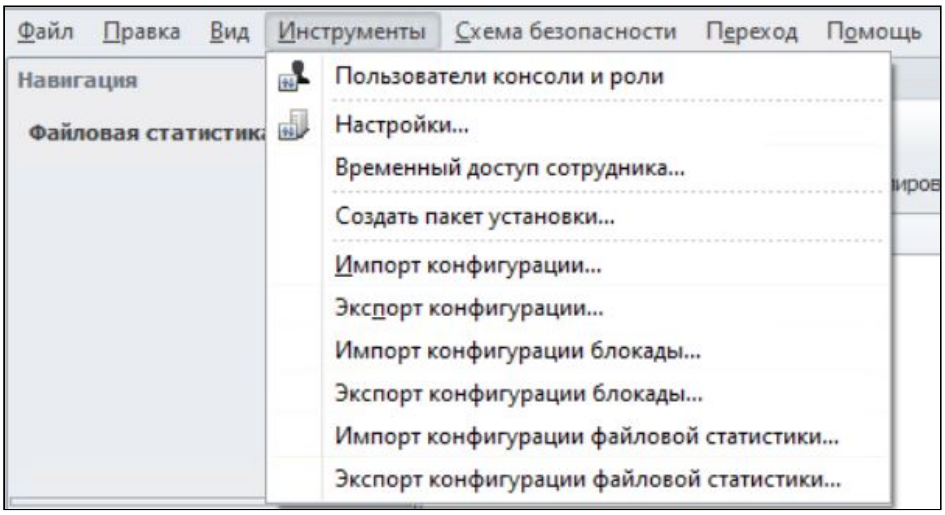
> **Важно!**
>
> Включение/исключение путей и расширений распространяется только на те файлы и папки, над которыми непосредственно выполняется действие.
>
> Например:
>
> Если настроено исключение файлов с расширением .docx, то при действиях пользователя с папкой, содержащей файлы с этим расширением, будет создано событие для действия с файлом *.docx.
>
> Если настроено исключение для папки 2, которая является подпапкой папки 1:
>
> - действие выполняется с папкой 1: будут созданы события для всех файлов папки 2.
> - действие выполняется с папкой 2: для нее настроено исключение, поэтому событие для папки не создается на стороне Агента.

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

> **Важно!**
>
> При перемещении папки с файлами в корзину, восстановлении папки из корзины и перемещении папки внутри тома, файловая система воспринимает эти действия как низкоуровневые операции переименования. Однако если файлов много и на каждый из них необходимо сформировать событие, это может сильно загрузить систему.
>
> Например, при перемещении папки, содержащей 1000 файлов, в Activity Monitor необходимо создать 1000 событий для каждого файла. Чтобы разгрузить систему, существует возможность отключить сбор статистики для таких операций. Если сбор отключен, события с файлами внутри папки, которые перемещают в корзину, восстанавливают из корзины и перемещают внутри тома, не будут создаваться.

11. Нажмите **Сохранить**.
12. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

Чтобы импортировать конфигурацию Файловой статистики:



1. На панели сверху выберите **Инструменты > Импорт конфигурации файловой статистики**.
2. В открывшемся окне выберите файл, который необходимо импортировать. Нажмите **Открыть**.
3. Сверху на панели нажмите **Сохранить**, чтобы сохранить изменения, внесенные в схему безопасности.

Чтобы экспортировать конфигурацию Файловой статистики:

1. На панели сверху выберите **Инструменты > Экспорт конфигурации файловой статистики**.
2. В открывшемся окне выберите директорию, куда необходимо экспортировать файл. Нажмите **Сохранить**.

Исключение мусорного трафика

Исключение позволяет указать URL-адреса, которые не требуется перехватывать в HTTP/HTTPS трафике. Если запрос HTTP/HTTPS отправляется по исключенному URL-адресу, Система не создает событие и теневую копию.

Списки исключений передаются на Агенты в составе схемы безопасности и применяются для всех Агентов. Агент проверяет URL-адрес, на который отправляется запрос. URL-адрес состоит из имени хоста и запроса к ресурсу.

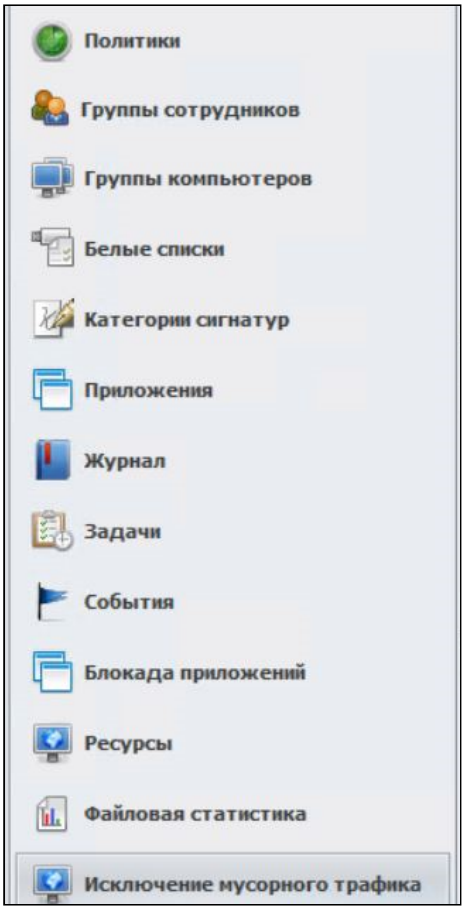
Пример:

Имя хоста: `www.google.ru`

Запрос к ресурсу: `/log?format=json&hasfast=true`

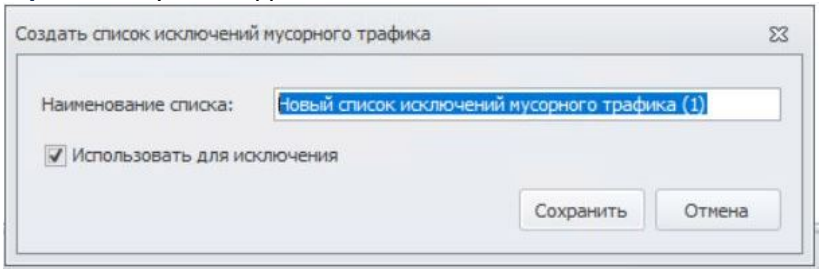
Агент проверяет URL-адрес: `www.google.ru/log?format=json&hasfast=true`

Настройка исключений производится в разделе **Исключение мусорного трафика** на панели навигации.



Чтобы добавить список исключений мусорного трафика

1. Нажмите **Исключение мусорного трафика** на панели навигации Консоли управления Device Monitor.
2. В верхней части панели навигации нажмите **Добавить список исключений мусорного трафика**. Откроется диалоговое окно:



3. Укажите название списка. Выберите **Использовать для исключения**, чтобы сделать список активным.
4. Нажмите **Сохранить**.
5. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

Список может иметь статус:

- Активный : список используется для исключения трафика
- Неактивный : список не используется для исключения трафика

Чтобы сделать список активным, включите параметр **Использовать для исключения** при добавлении/редактировании списка.

Чтобы отредактировать список исключений мусорного трафика

1. В области **Исключение мусорного трафика** в верхней части панели навигации выберите список.
2. Нажмите **Изменить список исключений мусорного трафика** в верхней части панели навигации.
3. В открывшемся диалоговом окне внесите изменения.
4. Нажмите **Сохранить**.
5. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

Чтобы удалить список исключений мусорного трафика

1. В области **Исключение мусорного трафика** в верхней части панели навигации выберите список, который необходимо удалить.
2. Нажмите **Удалить список исключений мусорного трафика** в верхней части панели навигации.
3. Нажмите **Да**.
4. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

Чтобы импортировать список исключений мусорного трафика

1. В области **Исключение мусорного трафика** в верхней части панели навигации нажмите **Импортировать список исключений мусорного трафика** .
2. Выберите файл, который необходимо импортировать.
3. Нажмите **Открыть**.
4. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

Чтобы экспортировать список исключений мусорного трафика

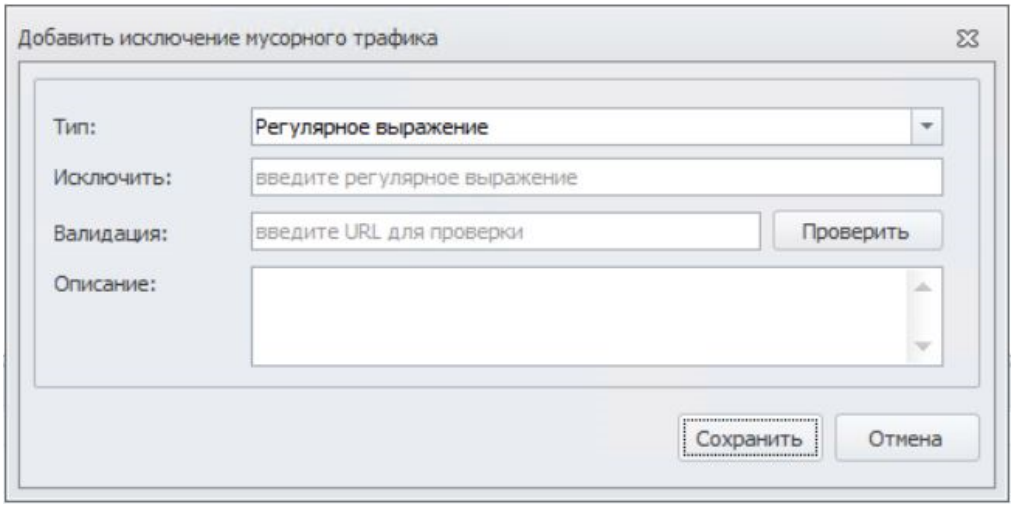
1. В области **Исключение мусорного трафика** в верхней части панели навигации нажмите **Экспортировать список исключений мусорного трафика** .
2. Нажмите **Сохранить**.
3. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

Вы также можете импортировать/экспортировать списки исключений в составе схемы безопасности.

Вы можете настроить исключения выбранного списка.

Чтобы добавить исключение в список мусорного трафика

1. В области **Список исключений мусорного трафика** в верхней части панели навигации нажмите **Добавить исключение**. Откроется диалоговое окно:



2. Укажите:

Параметр	Описание
Тип	Доступен один тип исключения – регулярное выражение **Примечание**: Если URL-адрес соответствует регулярному выражению, то Система исключает запрос из перехвата. Используемый диалект регулярных выражений – ECMAScript
Исключить	Регулярное выражение для исключения. Например, чтобы исключить любой URL-адрес, который содержит строку "google", укажите: .*google.*
Описание	Описание исключения

3. Нажмите **Сохранить**.
4. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

Чтобы отредактировать исключение в списке мусорного трафика

1. В области **Список исключений мусорного трафика** в верхней части панели навигации выберите исключение, которое необходимо отредактировать.
2. Нажмите **Изменить исключение** в верхней части панели навигации.
3. В открывшемся диалоговом окне внесите изменения.
4. Нажмите **Сохранить**.
5. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

Чтобы удалить исключение в списке мусорного трафика

1. В области **Список исключений мусорного трафика** в верхней части панели навигации выберите выберите исключение, который необходимо удалить.
2. Нажмите **Удалить исключение** в верхней части панели навигации.
3. Нажмите **Да**.

4. Подтвердите изменение схемы безопасности, нажав **Сохранить**.

4.4.4 Временный доступ сотрудника к сети

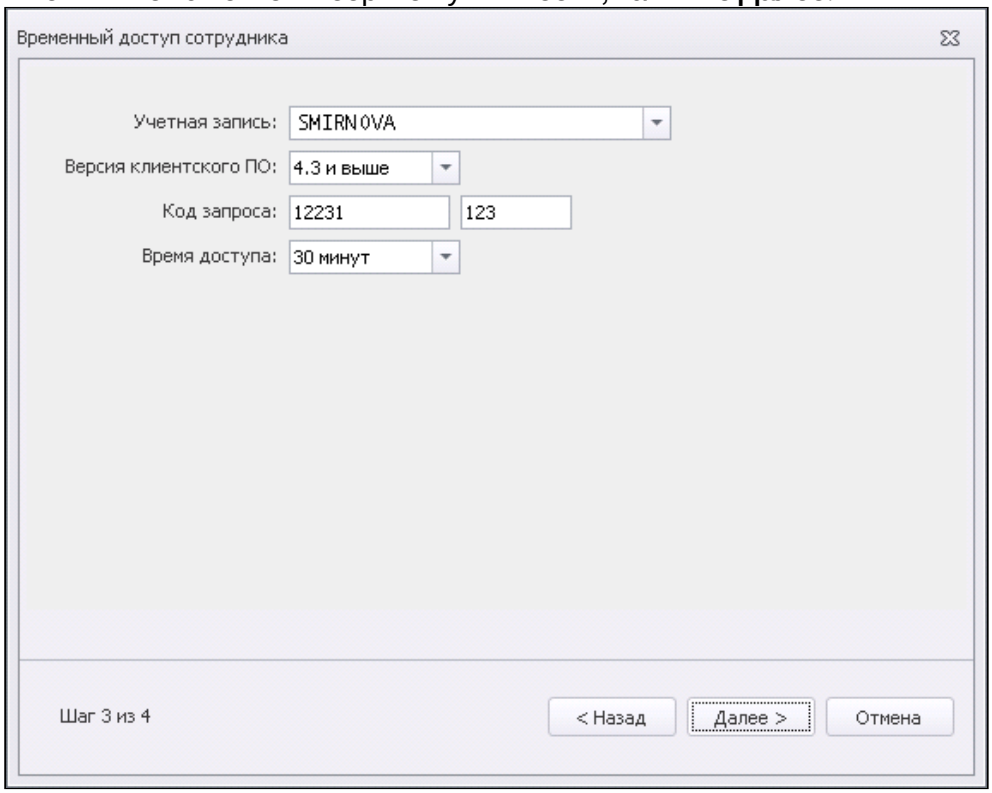
Сотрудник, для которого действует правило, запрещающее соединения вне корпоративной сети (см. "Контроль сетевых соединений" и "Правило для Network Monitor"), может из меню Агента InfoWatch Device Monitor, команда Контроль сети, запросить временный доступ к внешним соединениям.

> **Важно!**
>
> Возможность запросить доступ есть у сотрудника только в том случае, если для уведомлений сотрудника не действует настройка **Скрывать присутствие агента на компьютере** (подробнее см. "Общие настройки работы Агентов").
> О том, как настроить текст, отображаемый сотруднику, см. "Настройка уведомлений сотрудников о нарушении правил", тип уведомления **Запрет сетевого подключения, детализированное**.

Получив код запроса, сотрудник должен передать его офицеру безопасности.

Чтобы предоставить сотруднику временный доступ к внешним соединениям:

1. В главном меню выберите команду **Инструменты** > **Временный доступ сотрудника**.
2. В появившемся окне выберите **Продиктован по телефону (цифровой код запроса)**, нажмите **Далее**.
3. В появившемся окне выберите пункт **К сети**, нажмите **Далее**.



4. Из раскрывающегося списка **Учетная запись** выберите запись сотрудника, которому требуется предоставить временный доступ.

5. Из раскрывающегося списка **Версия клиентского ПО** выберите номер версии приложения Device Monitor Agent, установленной на компьютере сотрудника.
6. В поле **Код запроса** введите код, переданный сотрудником.
7. Из раскрывающегося списка **Время доступа** выберите временной промежуток, на который предоставляется доступ.
8. Нажмите **Далее**.
   В поле **Код подтверждения** появится код, который нужно передать сотруднику для того, чтобы он смог получить требуемый доступ.
9. Нажмите **Готово**.

4.4.5 Временный доступ сотрудника к устройствам

Сотрудник, для которого действует правило, запрещающее использование устройств (см. "Правило для Device Monitor"), может в интерфейсе Агента InfoWatch Device Monitor, вкладка Список устройств, запросить временный доступ к устройствам (подробнее см. "Получение сотрудником временного доступа к устройствам").

> **Важно!**
>
> Возможность запросить доступ есть у сотрудника только в том случае, если для уведомлений сотрудника не действует настройка **Скрывать присутствие агента на компьютере** (подробнее см. "Общие настройки работы Агентов").
> О том, как настроить текст, отображаемый сотруднику, см. "Настройка уведомлений сотрудников о нарушении правил", тип уведомления **Запрет доступа к устройству**.

Получив код запроса, сотрудник должен передать его офицеру безопасности.

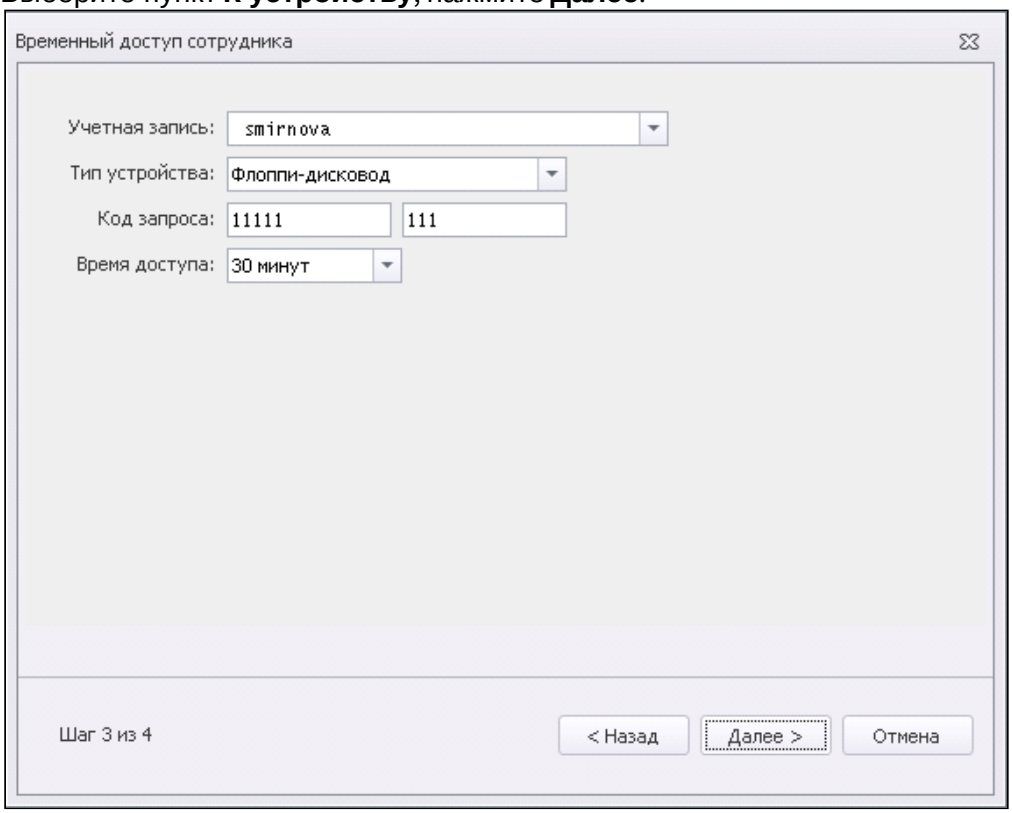
В зависимости от ситуации, вы можете использовать один из двух варианта взаимодействия с сотрудником:

- по телефону;
- по электронной почте.

Чтобы предоставить временный доступ к устройствам сотруднику, обратившемуся по телефону:

1. В главном меню выберите команду **Инструменты** > **Временный доступ сотрудника**.
2. В появившемся окне выберите пункт **Продиктован по телефону**, нажмите **Далее**.

3. Выберите пункт **К устройству**, нажмите **Далее**.

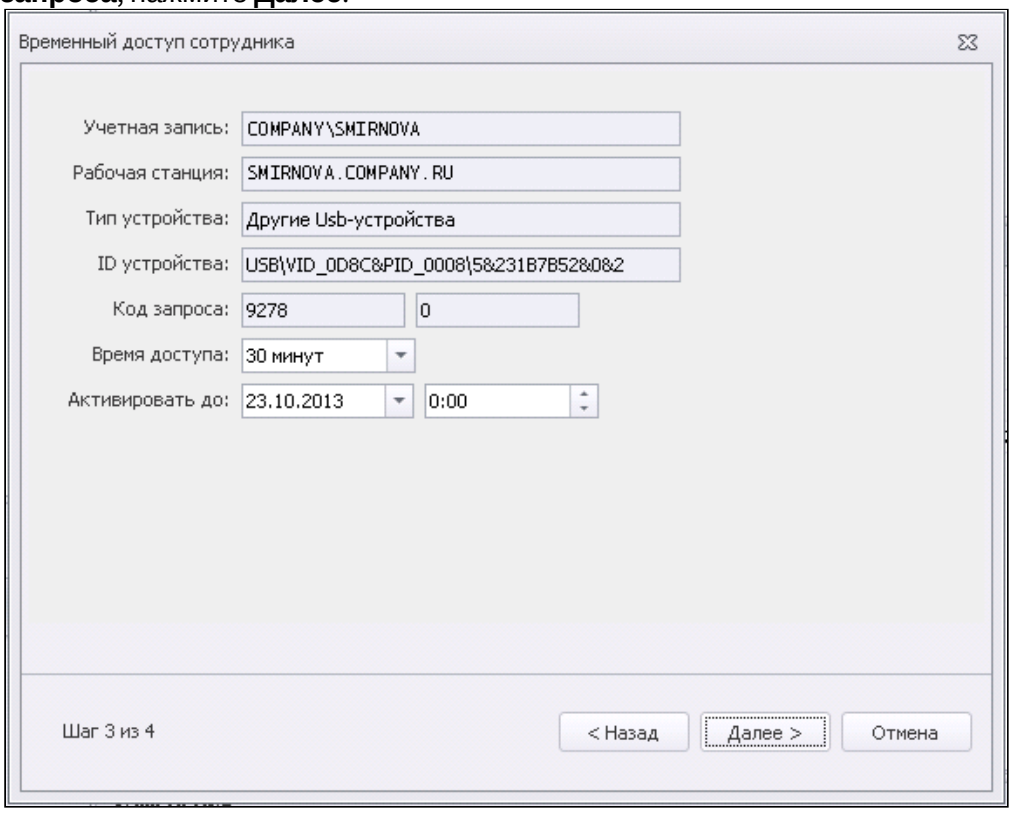


4. Из раскрывающегося списка **Учетная запись** выберите запись сотрудника, которому требуется предоставить временный доступ.
5. Из раскрывающегося списка **Тип устройства** выберите требуемый тип устройств.
6. В поле **Код запроса** введите код, переданный сотрудником.
7. Из раскрывающегося списка **Время доступа** выберите временной промежуток, на который предоставляется доступ.
8. Нажмите **Далее**.
   В поле **Код подтверждения** появится код, который нужно передать сотруднику для того, чтобы он смог получить требуемый доступ.
9. Нажмите **Готово**.

Чтобы предоставить временный доступ к устройствам сотруднику, обратившемуся по электронной почте:

1. В главном меню выберите команду **Инструменты** > **Временный доступ сотрудника**.
2. В появившемся окне выберите пункт **Получен через электронную почту или другие средства связи**, нажмите **Далее**.

3. Введите полученный по электронной почте текст запроса в поле **Введите текст запроса**, нажмите **Далее**.



4. Из раскрывающегося списка **Время доступа** выберите временной промежуток, на который предоставляется доступ.
5. Из группы раскрывающихся списков **Активировать до** выберите временной промежуток, в который сотрудник сможет активировать свой доступ к устройству (после активации доступ будет предоставлен на время, указанное в пункте **Время доступа**).
6. Нажмите **Далее**.
   В поле **Скопируйте в буфер обмена текст ответа** появится код, который нужно передать сотруднику для того, чтобы он смог получить требуемый доступ.
7. Нажмите **Готово**.

4.5 Просмотр событий DM

Данные, полученные в процессе работы агентов InfoWatch Device Monitor на контролируемых компьютерах, фиксируются в виде **событий** и передаются на сервера Device Monitor вместе с данными теневого копирования. События (в отличие от теневых копий) сохраняются в базе данных InfoWatch Device Monitor и доступны для просмотра в Консоли управления.

Уровень логирования сведений (сохранять всю информацию о попытках доступа; сохранять только нарушения политик или не сохранять вообще) вы можете определить в общих настройках схемы безопасности: подробнее см. "Общие настройки работы Агентов".

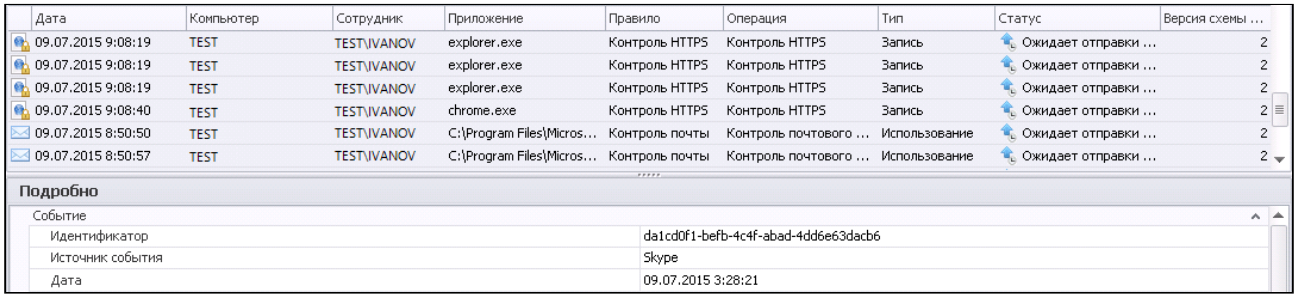
В разделе **События** вы можете просмотреть информацию о событиях. Для перехода к разделу нажмите кнопку **События** на Панели навигации.

Чтобы просмотреть события, выберите нужные фильтры в списке.

Вы можете выбрать один из предустановленных фильтров или создать новый фильтр, как описано в статье "Фильтры событий". Предустановленные фильтры:

- **За последние 4 часа**
- **За сегодня**

Сведения о событиях отображаются в виде таблицы. Расширенная информация по свойствам каждой записи выводится на панели **Подробно**.



Имя атрибута	Описание	Возможные значения
Общие атрибуты		
Идентификатор	Уникальный номер, присваиваемый событию в Системе	
Источник события	Тип события в зависимости от перехватчика	• **Файловое** – File Monitor; • **От устройств** – Device Monitor; • **Буфер обмена** – Clipboard monitor; • **Приложение** – File Operations Monitor; • **Принтер** – Print Monitor; • **Skype, XMPP, MMP, Telegram, WhatsApp** – IM Client Monitor; • **FTP/FTPS** – FTP Monitor; • **HTTP/HTTPS** – HTTP(S) Monitor; • **Cloud Storage** – Cloud Storage Monitor; • **Сетевое** – Network Monitor; • **Электронная почта** – Mail Monitor; • **Снимок экрана** – ScreenShot Monitor; • **Системное** – событие об окончании места на диске для сохранения теневой копии. *Такое событие не передается в систему Traffic Monitor.*
Дата	Дата и время (в часах и минутах) фиксации события на компьютере. На сервере Device Monitor событие сохраняется в	

Имя атрибута	Описание	Возможные значения
	UTC, а в Консоли управления отображается соответственно локальному времени того компьютера, где работает Консоль	
Имя компьютера	Имя компьютера, где зафиксировано событие	
Операция	Описание действия или попытки действия, выполненного сотрудником	
Сервер	Имя сервера InfoWatch Device Monitor, на который агент передал информацию о событии	
Приложение	Имя исполняемого файла и/или наименование процесса, выполняющего действие, если его удалось определить	Если в событии типа **Снимок экрана** не удалось определить приложение, указывается значение **Не определено**. В этом случае событие не передается в Activity Monitor.
Тип	Тип события в зависимости от выполненного действия	• **Запись** – размещение или изменение данных (включая изменение имени файла) на внешнем устройстве; пересылка файла средствами мессенджера; отправка задания на печать на принтер; пересылка данных по протоколу FTP/ FTPS; загрузка данных в облачное хранилище. • **Использование** – подключение внешнего устройства, для которого отдельно не контролируются операции чтения/записи; отправка сообщений через мессенджер; • **Нарушение** – нарушение сотрудником работы перехватчика IM Client; • **Предупреждение** – запрет сотрудником или отсутствие согласия сотрудника на использование плагина IM

Имя атрибута	Описание	Возможные значения
		Client, если этого требует политика безопасности. • **Запрет использования** – попытка передачи данных по запрещенному каналу.
Статус	Состояние обработки события на сервере и его отправки на сервер Traffic Monitor	• **Не определено** • **Ожидает обработки** • **Обработано** • **Нет лицензии** • **Ожидает отправки в ТМ** • **Ошибка отправки в ТМ** • **Отправлено в ТМ** **Примечание:** В случае работы сервера в автономном режиме статус событий может быть только **Обработано**
Версия схемы безопасности	Номер версии схемы безопасности, используемой на компьютере в момент фиксации события	
Вердикт операции	Признак разрешения контролируемого действия. Для событий с источником *От устройств* (сработало правило **Device Monitor**) также возможна блокировка действия.	• **Операция разрешена** • **Запрет** – только для событий от устройств • **Запрет копирования незащищенных данных** – только для событий от устройств • **Разрешено (В белом списке)** – для событий от устройств, состоящих в белом списке
Сотрудник	Наименование домена (наименование компьютера вне домена) и логин пользователя, в сессии которого фиксировалось событие, или ссылка на операционную систему, если событие зафиксировано вне сессий пользователей	
Правило	Название правила политики, в соответствии с которым контролируется событие	

Имя атрибута	Описание	Возможные значения
Для событий с источником Файловое, От устройств, Приложение, Принтер, FTP/FTPS, HTTP/HTTPS, Cloud Storage, Сетевое, Системное		
Терминальный Клиент	Имя терминального клиента, если определено	
Сетевой адрес терминального клиента	IP терминального клиента, если определено	
Для событий с источником Файловое		
Назначение	Полное имя целевого файла	
Размер файла	Размер целевого файла	
Состояние	Результат теневого копирования перемещаемых данных	• **копия не создавалась** – правило не требует создания теневой копии • **копия создана** – теневая копия успешно создана • **закончилось свободное место на диске** – при нехватке свободного места на агенте • **ошибка создания копии** – при возникновении ошибки создания копии
Описание устройства	Идентификатор экземпляра или модели устройства, на которое записывался файл	
Для событий с источником *От устройств*		
Тип устройств	Поддерживаемый перечень типов устройств см. "Функции InfoWatch Device Monitor"	
Идентификатор экземпляра или модели устройства	Идентификатор модели (VID) и серийный номер (PID) применяемого внешнего устройства или принтера, используемого в операции	

Имя атрибута	Описание	Возможные значения
Описание устройства	Описание используемого устройства, полученное от операционной системы на компьютере, где установлен Агент	
Для событий с источником *Буфер обмена*		
Копирование через терминальную сессию	Признак, показывающий, что данные пересекли границу терминальной сессии	• **Да** • **Нет**
Тип данных	Тип вставленных данных	
Приложение-приемник	Подзаголовок для описания атрибутов приложения-приемника, в которое вставляются данные из буфера обмена	
Приложение-источник	Подзаголовок для описания атрибутов приложения-источника, которое поместило данные в буфер обмена	
Имя приложения	Имя приложения-приемника или приложения-источника	
Описание	Описание приложения-приемника или приложения-источника	
Название продукта	Название продукта приложения-приемника или приложения-источника	
Издатель	Издатель приложения-приемника или приложения-источника	
Расположение	Расположение приложения-приемника или приложения-источника	
Версия файла	Версия файла приложения-приемника или приложения-источника	

Имя атрибута	Описание	Возможные значения
Версия продукта	Версия продукта приложения-приемника или приложения-источника	
Приложение терминальной сессии	Входит ли приложение в список поддерживаемых систем виртуализации	• **Да** • **Нет**
Снимок экрана при вставке в приложение	Признак, показывающий был ли сохранён снимок экрана при вставке из буфера обмена	• **Да** • **Нет**
Снимок экрана при копировании из приложения	Признак, показывающий был ли сохранён снимок экрана при копировании в буфер обмена	• **Да** • **Нет**
Для событий с источником *Приложение*		
Путь	Полный путь к файлу на рабочей станции	
Размер файла	Размер файла в байтах	
Снимок экрана	Признак, показывающий был ли сохранён снимок экрана	• **Да** – снимок сохранен; • **Нет** – снимок не сохранен.
Для событий с источником Skype, XMPP, MMP, Telegram, WhatsApp		
Имя пользователя клиента мгновенных сообщений	UIN пользователя, авторизованного в мессенджере на компьютере	
Состояние	Результат теневого копирования	• **копия не создавалась** – правило не требует создания теневой копии • **копия создана** – теневая копия успешно создана • **закончилось свободное место на диске** – на агенте нет свободного дискового пространства • **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки

Имя атрибута	Описание	Возможные значения
Список отправителей	UIN пользователей мессенджера, отправивших сообщение/файл в диалоге мессенджера	
Список получателей	UIN пользователей мессенджера, получивших сообщение/файл в диалоге мессенджера	
Имя файла	Полное имя пересылаемого файла	
Размер файла	Размер пересылаемого файла	
Теневая копия	Результат теневого копирования файла, чата или сообщения	• **Нет** – теневая копия не создавалась • **Да** – теневая копия успешно создана
Для событий с источником *От принтера*		
Документ	Полное имя файла, отправленного на печать	
Принтер	Сетевое имя принтера, на который было отправлено задание на печать	
Статус печати	Результат теневого копирования задания на печать	1. Теневая копия задания на печать создана успешно. Задание содержало графические и текстовые данные; 2. Теневую копию задания на печать не удалось создать. Задание не содержало графических и текстовых данных; 3. Ошибка при создании теневой копии задания на печать; 4. Теневую копию не нужно было создавать 5. Теневая копия задания на печать создана частично. Графические данные обработаны полностью.

Имя атрибута	Описание	Возможные значения
		Текстовые данные обработаны частично. 6. Теневая копия задания на печать создана частично. Графические данные обработаны частично. Текстовые данные обработаны полностью. 7. Теневая копия задания на печать создана успешно. Задание содержало только текстовые данные; 8. Теневая копия задания на печать создана успешно. Задание содержало только графические данные; 9. Теневая копия задания на печать создана частично. Графические данные обработаны частично. Задание не содержало текстовых данных. 10. Теневая копия задания на печать создана частично. Задание не содержало графических данных. Текстовые данные обработаны частично.
Состояние	Результат теневого копирования задания на печать	• **копия не создавалась** – правило не требует создания теневой копии • **копия создана** – теневая копия успешно создана • **закончилось свободное место на диске** – на агенте нет свободного дискового пространства • **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки
Для событий с источником *FTP/FTPS*		
Состояние	Результат теневого копирования перемещаемых данных	• **копия не создавалась** – правило не требует создания теневой копии

Имя атрибута	Описание	Возможные значения
		• **копия создана** – теневая копия успешно создана • **закончилось свободное место на диске** – на агенте нет свободного дискового пространства • **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки
Отправитель	Имя, под которым сотрудник авторизован на FTP сервере	
FTP сервер	Имя или IP адрес FTP сервера	**Примечание:** При использовании FTP через proxy-сервер данное поле может содержать адрес proxy-сервера, а не адрес используемого FTP-сервера.
Относительный путь	Директория на FTP сервере, куда осуществляется передача файла	
Имя файла	Полное имя пересылаемого файла	
Фактический размер файла	Размер переданного файла по результату передачи	
Заявленный размер файла	Размер передаваемого файла по данным приложения, выполняющего передачу на FTP сервер (например, браузера)	
Начальная позиция	При передаче файла по частям, это – позиция, с которой начата передача этой части.	
Теневая копия	Результат теневого копирования файла	• **Нет** – теневая копия не создавалась • **Да** – теневая копия успешно создана
Для событий с источником *HTTP/HTTPS*		
Состояние	Результат теневого копирования данных	• **копия не создавалась** – правило не требует создания теневой копии

Имя атрибута	Описание	Возможные значения
		• **копия создана** – теневая копия успешно создана • **закончилось свободное место на диске** – на агенте нет свободного дискового пространства • **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки
DNS получателя	Сетевое имя компьютера, на который был отправлен запрос	
IP получателя	IP-адрес компьютера, на который был отправлен запрос	
Размер запроса	Размер отправленного запроса в КБ	
Правило	Название правила политики, в соответствии с которым контролируется событие	
Для событий с источником *Cloud Storage*		
Название облачного хранилища	Название облачного хранилища, в которое выполняется загрузка данных	• Google Drive • DropBox • YandexDisk • SkyDrive • EverNote • SugarSync
Имя файла	Целевое имя файла	
Размер файла	Размер файла (в байтах), отправляемого в облачное хранилище	
Для событий с источником *Терминальная сессия*		
Путь	Короткое имя копируемого файла	
Имя устройства	Имя устройства, если определено	

Имя атрибута	Описание	Возможные значения
ID устройства	ID устройства, если определено	
Для событий с источником *Электронная почта*		
Состояние	Результат теневого копирования данных	• **копия не создавалась** – правило не требует создания теневой копии • **копия создана** – теневая копия успешно создана • **закончилось свободное место на диске** – на агенте нет свободного дискового пространства • **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки
Список отправителей	Адрес электронной почты отправителя письма	
Список получателей	Список адресов, на которые было отправлено письмо	**Примечание:** Для событий с большим количеством получателей необходимо иметь в виду, что при просмотре события через Консоль Device Monitor данное поле не отображает более 1024 символов. Однако если для события настроено создание теневой копии, то в результате передачи события в Traffic Monitor поле Получатели будет отображать полный список получателей (ограничение в 4000 байт).
Правило	Название правила политики, в соответствии с которым контролируется событие	
Для событий с сетевым источником		
Время отмены блокировки доступа	Для операции *Временная отмена блокировки доступа* – начало периода временного доступа. см. "Временный доступ сотрудника к сети".	

Имя атрибута	Описание	Возможные значения
Время возобновления блокировки доступа	Для операции *Временная отмена блокировки доступа* – конец периода временного доступа. см. "Временный доступ сотрудника к сети".	
Сервер соединения	Для операции *Соединение запрещено* – адрес или имя сервера, доступ к которому запрещен	
Порт	Для операции *Соединение запрещено* – номер порта, доступ к которому запрещен	

При необходимости, вы можете освободить место в базе данных, удалив из нее всю информацию об уже обработанных событиях (статус **Обработано** или **Отправлено в Traffic Monitor**). Подробнее см. "Удаление событий".

Примечание:

Для Агентов под управлением РЕД ОС поддерживается отправка событий о запрете чтения со съемного устройства хранения и записи с/на съемное устройство хранения.

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 в Общих настройках работы Агентов для параметра **Логировать события от перехватчика устройств и облачных хранилищ** указать значение **Логировать всегда**.

4.5.1 Фильтры событий

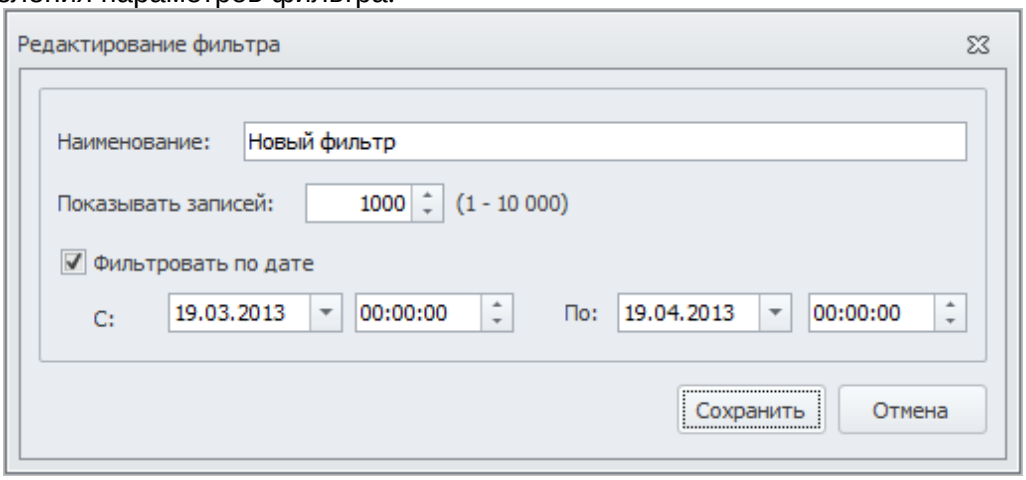
Помимо предустановленных фильтров вы можете создавать собственные фильтры для просмотра информации о событиях.

Чтобы добавить или отредактировать фильтр:

1. Перейдите к разделу **События**.
2. Выполните необходимые шаги:

Действие	Шаги
Создание фильтра	- в главном меню выберите команду **Правка** > **Создать фильтр**; - воспользуйтесь кнопкой **Создать фильтр**, расположенной в верхней части Панели навигации.
Редактирование фильтра	1. В области **События** на Панели навигации выберите название фильтра, который нужно отредактировать. 2. Выполните одно из следующих действий: - в главном меню выберите команду **Правка** > **Изменить**; - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации; - дважды щелкните левой кнопкой мыши по названию выделенного фильтра; - щелкните по названию выделенного фильтра правой кнопкой мыши и в контекстном меню выберите **Изменить**; - нажмите Ctrl+E.

После выполнения любого из этих действий на экран будет выведено диалоговое окно определения параметров фильтра.



3. В диалоговом окне **Редактирование фильтра** укажите параметры фильтра:
   - **Наименование**.
   - **Показывать записей**. Ограничение на количество записей, которые могут быть выведены в рабочей области Консоли управления (значение по умолчанию 1000 записей).
   - Чтобы задать условия фильтрации по дате, отметьте поле **Фильтровать по дате** и укажите начало и окончание интересующего вас периода в полях **С** и **По** соответственно. Дату задают в левом поле, время – в правом.

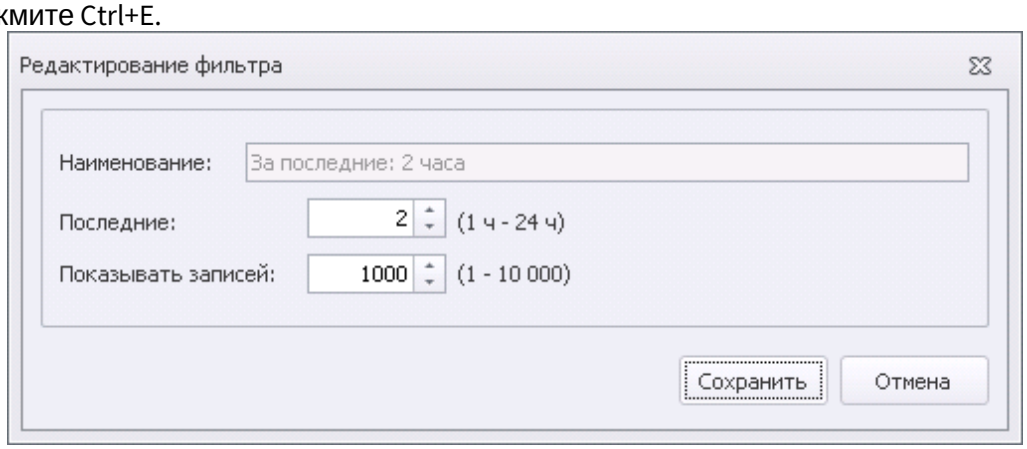
> **Примечание.**
>
> Для предустановленных фильтров параметры **Наименование** и **Фильтровать по дате** изменять нельзя.

4. Нажмите **Сохранить**.

Предустановленный фильтр **За последние 4 часа** имеет другой интерфейс редактирования и позволяет создавать фильтры, отображающие события за последние несколько часов.

Чтобы отредактировать предустановленный фильтр так, чтобы отображались события за указанное количество часов:

1. В области **События** на Панели навигации выберите фильтр **За последние 4 часа**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить**;
   - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации;
   - дважды щелкните левой кнопкой мыши по названию фильтра;
   - щелкните по названию фильтра правой кнопкой мыши и в контекстном меню выберите **Изменить**;
   - нажмите Ctrl+E.



3. В диалоговом окне **Редактирование фильтра** укажите параметры фильтра:
   - **Последние**. Укажите количество часов, записи за которые должны быть выведены в рабочей области Консоли управления.
   - **Показывать записей**. Ограничение на количество записей, которые могут быть выведены (значение по умолчанию 1000 записей).
4. Нажмите **Сохранить**.

4.5.2 Удаление событий

Информация об уже обработанных событиях (статус **Обработано, Отправлено в ТМ, Ошибка отправки в ТМ, Нет лицензии**) может быть удалена.

Вы можете удалить события:

- за указанный период времени;
- все, соответствующие выбранному фильтру.

Чтобы удалить из журнала аудита информацию обо всех событиях за период:

1. Перейдите к разделу **События**.

2. Выполните одно из следующих действий:
    - воспользуйтесь кнопкой  **Удалить события**, расположенной на Панели навигации;
    - в главном меню выберите команду **Правка** > **Удалить события**;
    - нажмите Ctrl + Shift + D;
3. В открывшемся диалоговом окне **Удаление событий из базы данных** укажите необходимый диапазон дат, информация за который должна быть удалена.
4. Нажмите **Удалить**.

В результате будет отображено, сколько событий было удалено из базы данных.

Чтобы удалить из журнала аудита информацию о событиях, соответствующих выбранному фильтру:

1. Перейдите к разделу **События**.
2. В списке фильтров выберите название нужного фильтра.
3. Выполните одно из следующих действий:
    - воспользуйтесь кнопкой  **Удалить события фильтра**, расположенной в верхней части раздела События;
    - в главном меню выберите команду **Правка** > **Удалить события фильтра**;
    - выберите пункт **Удалить события фильтра** в контекстном меню фильтра;
    - Нажмите Shift + Delete.
4. В открывшемся диалоговом окне подтверждения нажмите **Да**.

В результате будет отображено, сколько событий было удалено из базы данных.

4.6 Удаленная установка, обновление и удаление Агентов

> **Важно!**
>
> Задачи удаленного управления Агентом поддерживаются на рабочих станциях под управлением ОС Windows или ОС семейства Linux.
>
> На ОС Astra Linux не поддерживается обновление Агентов с версий ниже 7.0.

Задачи удаленного управления Агентом выполняются с помощью специального Агента распространения, передаваемого на агентские рабочие станции. Для его корректной работы необходимо обеспечить выполнение следующих условий:

- Установка, обновление и удаление Агентов InfoWatch Device Monitor на рабочие станции может выполняться централизованно средствами Консоли управления InfoWatch Device Monitor. Для этого предусмотрен механизм задач. Задачи позволяют запускать процессы установки, обновления и удаления агентского ПО, смены пароля деинсталляции, а также наблюдать за состоянием выполнения этих процессов.
- Рабочие станции, на которые производится установка, должны удовлетворять необходимым аппаратным и программным требованиям (см. документ "*InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию*", статья "Аппаратные и программные требования").
- На момент установки Агента проактивная антивирусная защита на рабочих станциях должна быть отключена (только для Агентов, установленных на ОС Windows).
- Сервер Device Monitor и рабочие станции должны распознавать доменные имена друг друга.

- На рабочих станциях, где установлен межсетевой экран (firewall), отличный от стандартного брандмауэра Windows, этот межсетевой экран должен быть отключен, или в нем должно присутствовать разрешение на работу любых сетевых соединений для следующих компонент Device Monitor: *IWDeployAgent.exe*, *iwdmc.exe*, *DM.Client.exe*, *IWProxy.exe*, *rmtlogctr.exe* (только для Агентов, установленных на ОС Windows).

  > **Примечание.**
  >
  > Для установки Агента на Windows 7 зайдите в **Панель управления** -> **Центр управления сетями и общим доступом** -> **Изменить дополнительные параметры общего доступа** и выберите опцию **Включить общий доступ к файлам и принтерам**. После этого Агент распространения сможет быть скопирован на рабочую станцию. Брандмауэр будет настроен автоматически.

Чтобы перейти к разделу Консоли управления, предназначенному для работы с задачами, воспользуйтесь кнопкой **Задачи**, расположенной на Панели навигации.
Информация по управлению задачами содержится в подразделах:

- Просмотр задач
- Подготовка к первичной установке Агентов
- Обнаружение рабочих станций для установки агентов
- Создание задачи первичного распространения
- Создание задачи обновления
- Создание задачи смены пароля деинсталляции
- Создание задачи удаления
- Запуск, остановка, редактирование и удаление задачи
- Ошибки установки Агентов
- Создание шаблона задачи распространения

Вы также можете осуществлять установку и обновление Агента с помощью средств распространения программного обеспечения (например, в Microsoft Active Directory посредством механизма групповых политик). Подробное описание такой установки см. в документе "*InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию*", статья "Установка Агента с помощью средств распространения программного обеспечения". Для этого удобно использовать пакет установки, созданный как описано в разделе "Создание пакета установки".

4.6.1 Просмотр задач

В области **Задачи** на Панели навигации выводится перечень всех созданных, выполненных и невыполненных задач, а также шаблонов, по которым задачи первичного распространения будут создаваться автоматически. В рабочей области главного окна отображается список рабочих станций, для которых выполняется выбранная задача.

На панели **Подробно** для выбранной задачи отображаются следующие параметры:

Параметр	Описание
Наименование	Имя задачи, указанное при ее создании
Описание	Описание задачи, указанное при ее создании

Параметр	Описание
Тип	Один из следующих типов задач: • первичное распространение; • смена пароля; • обновление; • удаление.
Статус	Текущее состояние задачи. Возможные значения: • создана; • запущена; • остановлена; • выполнена.
Период повторного запуска, мин	Время (в минутах), по истечении которого будет повторно запущена задача распространения для рабочих станций, к которым при предыдущем запуске не было доступа. Данное время начинает отсчитываться после завершения обработки последней станции из списка при предыдущем запуске задач. Если запуск завершился с ошибкой, то повторный запуск производиться не будет.
Количество попыток повторного запуска	Максимальное количество попыток перезапустить задачу распространения на рабочей станции.
Для задач первичного распространения	
Отображать сотруднику уведомления о работе агентского модуля	Признак того, что при попытке сотрудника выполнить действие, запрещенное политикой безопасности, ему будет отображаться предупреждающее уведомление. Подробнее см. "Общие настройки политики безопасности", "Создание инсталляционного комплекта" и "Настройка уведомлений сотрудников о нарушении правил"
Скрывать присутствие агента на рабочей станции	Признак того, что Система будет скрывать присутствие Агента на рабочих станциях. Иначе в области уведомлений панели задач Windows на компьютере, где установлен Агент, будет отображаться пиктограмма . При нажатии на этот значок доступна информация о работе Агента, а также список контролируемых в данный момент устройств. **Внимание!** 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
Устанавливать компонент перехвата сетевого трафика	Признак того, что на компьютер будет установлен компонент `iw_proxy`.
Устанавливать компонент контроля сетевых соединений	Признак того, что на компьютер будет установлен перехватчик Network Monitor.
Пароль для деинсталляции	Признак того, задан ли пароль, запрашиваемый у сотрудника при попытке удалить Агент Device Monitor.
Proxy Root Issuer DN	Уникальное имя для сертификата proxy-сервера Device Monitor (Issuer Distinguished name)
Для задач первичного распространения и обновления	
Директория для установки	Папка на рабочих станциях, куда будет устанавливаться Агент Device Monitor.
Имя пользователя для установки	Имя пользователя, от имени которого выполняется запущенная задача на рабочих станциях.
Продолжительность ожидания перезагрузки, часов	Время, в течение которого будет ожидаться перезагрузка рабочей станции (в часах); если за указанное время рабочая станция не будет перезагружена, Система приступит к уведомлению сотрудника (если параметры уведомления заданы), а затем - к принудительной перезагрузке операционной системы.
Продолжительность уведомлений о перезагрузке компьютера	Время, в течение которого сотруднику будут отображаться сообщения о необходимости перезагрузки компьютера, в часах.
Частота уведомлений о перезагрузке компьютера, мин	Промежуток времени, с которым будут повторяться сообщения о необходимости перезагрузки компьютера, в минутах.
Сообщения о перезагрузке	Текст, отображаемый сотруднику в сообщении о необходимости перезагрузки.
Показать предупреждение перед принудительной перезагрузкой	Признак того, будет ли показано окно о принудительной перезагрузке компьютера (сотруднику даются 5 минут на завершение своих операций) или перезагрузка будет осуществлена принудительно.
Пароль для деинсталляции	Признак того, задан ли пароль, запрашиваемый у сотрудника при попытке удалить Агент Device Monitor

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

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

4.6.2 Подготовка к первичной установке Агентов. Агент распространения

Удаленная установка Агента средствами InfoWatch Device Monitor выполняется с применением специального **Агента распространения**.

Для того чтобы удаленная установка Агента средствами InfoWatch Device Monitor была произведена корректно, рабочие станции, на которые производится установка, должны удовлетворять необходимым аппаратным и программным требованиям: см. "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Требования к аппаратному и программному обеспечению Агента InfoWatch Device Monitor".

Также для рабочих станций под управлением ОС **Windows** должны выполняться следующие условия:

- Проактивная антивирусная защита на рабочих станциях должна быть отключена.

- На рабочих станциях, где установлен межсетевой экран (firewall), отличный от стандартного фаервола Windows, этот межсетевой экран:
  - должен быть отключен
    или
  - в нем должно присутствовать разрешение на работу Агента распространения InfoWatch Device Monitor
    или
  - в межсетевом экране должен быть открыт порт **15505** (порт по умолчанию, по которому агент распространения ждет соединения) для входящих соединений, если он не был изменен в настройках сервера (см. "*Traffic Monitor. Руководства администратора*", статья "Раздел <applicationSettings>", параметр **CommunicationPort**).

Для рабочих станций под управлением ОС **Astra Linux** или **РЕД ОС** должны выполняться следующие условия:

- Должны быть установлены средства удаленного доступа **SSH**.
  Если SSH не был установлен во время установки ОС Astra Linux или РЕД ОС, его можно установить, выполнив в консоли сервера команду:

  ```
  sudo apt-get install ssh
  ```

  Для запуска сервиса используйте команду:

  ```
  service ssh start
  ```

- Пользователь, от имени которого будет произведена установка Агента, должен на целевой рабочей станции обладать правами на установку пакетов и регистрацию служб (root-правами).
  По умолчанию `ssh` запрещает подключаться через пользователя `root`.

Дополнительные требования зависят от способа распространения:

Способ 1:

Административными средствами распространить на целевые рабочие станции установочный пакет Агента распространения `Setup.DeployAgent.msi`, входящий в поставляемый дистрибутив.

Способ 2:

Для рабочих станций под упралением ОС Windows, выполнить действия, необходимые для передачи Агента распространения через административные разделяемые ресурсы:

- Межсетевые экраны (firewall) на рабочих станциях должны быть либо отключены, либо в них заданы необходимые разрешения: см. "Настройки брандмауэра".
- Необходимо определить параметры сетевого доступа к разделяемым ресурсам: см. "Включение административных разделяемых ресурсов".

Если все необходимые требования соблюдены, вы можете переходить к созданию, а затем – к запуску задачи первичного распространения.

Включение административных разделяемых ресурсов

Для передачи Агента распространения InfoWatch Device Monitor на целевые рабочие станции под управлением ОС Windows через административные разделяемые ресурсы необходимо выполнение требования:

На рабочих станциях должны быть включены административные разделяемые ресурсы вида `\\computername\admin$` (в Windows Vista, Windows 7, Windows 8, Windows 10 и Windows 11 они по умолчанию отключены). Для этого:

1. Убедитесь, что включен общий доступ к файлам и принтерам. В Панели управления откройте **Центр управления сетями и общим доступом** -> **Изменить дополнительные параметры общего доступа**. В нужном профиле включите общий доступ к файлам и принтерам.
2. В реестре, в ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`, добавьте параметр **DWORD (32-bit)** с названием **LocalAccountTokenFilterPolicy**. Установите для него значение **1**.

> **Примечание.**
>
> После того как вы добавили параметр в реестре, необходимо заново выполнить вход в Систему.

Настройки брандмауэра

Требования к настройкам брандмауэра:

Сервер Device Monitor (DM)	Агент DM	Протокол приложения	Транспортный протокол	Порт
Источник	Получатель	RPC	TCP	135
Источник	Получатель	RPC over HTTPS	TCP	593
Источник	Получатель	NetBIOS Datagram Service	UDP	138
Источник	Получатель	NetBIOS Name Resolution	UDP	137
Источник	Получатель	NetBIOS Session Service	TCP	139
Источник	Получатель	SMB	TCP	445

Для быстроты определения доступности рабочей станции требуется разрешить протокол ICMP.

Для брандмауэра Windows необходимо разрешить предустановленное правило "**Общий доступ к файлам и принтерам**" ("**File printing and sharing**").

4.6.3 Обнаружение рабочих станций для установки агентов

В состав дистрибутива для установки Сервера Device Monitor входит утилита сканирования диапазона IP-адресов. Она устанавливается автоматически вместе с консолью управления DM. Результатом сканирования является текстовый файл, который содержит список "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 необходимо или возможно указать при запуске. Их описание доступно по вызову справки: `Iw.Util.MachineDiscovery.exe -- 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 пакеты 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. Следует оставить по умолчанию
`--output-file arg`	Путь к файлу с результатами работы утилиты.

`--nmap-path arg (nmap mode)`	Путь к кросплатформенной утилите nmap в случае использования режима работы "nmap".
`--nmap-os-info arg (=1)`	Определять (=1) или не определять (=0) операционную систему рабочих станций при сканировании в режиме работы "nmap"
`--nmap-save-output-to-file arg (=1)`	Сохранить stdout и stderr Nmap'а в файл Nmap_output_%Y-%m-%d_%H-%M-%S.log
`--nmap-timing arg (=3)`	Частота сканирования nmap'ом: • от 0 - самое медленное и точное • до 5 - самое быстрое и неточное
`--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 установленное по умолчанию значение	

Чтобы запустить утилиту:

1. В командной строке на рабочей станции с консолью Device Monitor перейдите в директорию с утилитой Iw.Util.MachineDiscovery.exe с помощью команды cd:
   cd <путь_до_утилиты>
2. Запустите утилиту, обязательно указав при этом диапазон IP-адресов, а также другие параметры, если требуется. Например:
   `Iw.Util.MachineDiscovery.exe --ip-range 10.60.3-35.1-254`
3. Дождитесь окончания сканирования.
4. По завершению сканирования результаты будут записаны в текстовый файл `iw_machine_discovery.output.txt` в директории размещения утилиты `C:\Program Files\InfoWatch\Device Monitor\Management Console\Utils`. Полученный файл загрузите в задаче первичного распространения при создании списка компьютеров для установки Агентов на них (см. "Создание задачи первичного распространения").

4.6.4 Создание задачи первичного распространения

Первичное распространение (установка средствами Консоли управления) Агентов InfoWatch Device Monitor выполняется с помощью **агентов установки**. Агент установки – это исполняемый файл. В ходе

выполнения задачи он передается на рабочие станции и автоматически запускается, получая с сервера актуальную версию Агента.

Важно!

Если учетная запись, от имени которой запущен Сервер, не имеет прав администратора на всех рабочих станциях, где будет производиться установка, то для первичного распространения Агентов Device Monitor потребуется ввод имени и пароля учетной записи, обладающей правами администратора на:

- всех целевых рабочих станциях;
- компьютере, где работает Консоль управления;
- компьютере, где работает сервер Device Monitor.

Если у используемой учетной записи истекает пароль учетной записи Windows (предупреждение о необходимости смены пароля отображается в Windows за 3 дня до истечения пароля), то задача первичного распространения, запущенная от имени этого пользователя, не сможет быть выполнена.

Если ввод имени и пароля администратора невозможен, вы можете создать собственный установочный комплект Агентов InfoWatch Device Monitor (см. "Создание пакета установки") и установить его другими способами (см. "*InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию*", статьи "Локальная установка Агента" и "Установка Агента с помощью средств распространения программного обеспечения").

Важно!

Если на рабочей станции установлено программное обеспечение Kaspersky Internet Security, то для установки Агента InfoWatch Device Monitor необходимо отключить самозащиту Kaspersky Internet Security.

О том, как выключить самозащиту, см. интернет-статью "Как включить или выключить самозащиту в Kaspersky Internet Security".

Чтобы создать задачу первичного распространения Агента InfoWatch Device Monitor:

1. Перейдите к разделу **Задачи**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить задачу**;
   - нажмите **Добавить задачу** в верхней части раздела **Задачи**.

   Откроется диалоговое окно **Мастера создания задачи**.
3. Выберите **Задача первичного распространения** (для установки Агента на компьютеры под управлением ОС Windows) или **Задача первичного распространения (Linux)** (для установки Агента на компьютеры под управлением ОС Astra Linux, РЕД ОС или ОС Альт Рабочая Станция), введите имя задачи и ее описание, затем нажмите **Далее**.
4. Мастер создания задачи отобразит:
   - адреса хранилищ, которые служат точками распространения Агентов на рабочие станции;
   - версию Агента на этих точках, указанную в общих настройках. См. статью "Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor".

При необходимости вы можете изменить эти параметры и задать другое количество попыток загрузки обновления. Нажмите **Далее**.

> **Примечание:**
>
> Все доступные версии расположены в директории `C:\ProgramData\InfoWatch\SetupPackages\`.

5. Создайте список компьютеров, на которые необходимо установить Агент Device Monitor. Чтобы добавить компьютер (или несколько компьютеров):
   a. Нажмите **Добавить**. В открывшемся окне вы можете выбрать компьютеры:
      - по имени в строке поиска в директориях, к которым удалось подключиться ( );
      - из директории;
      - из сетевого окружения Microsoft Windows Network;
      - из дерева ALD;
      - из числа ранее зарегистрированных в Системе (например, в результате ручной установки Агента Device Monitor) и уже принадлежащих существующим группам Device Monitor (узел **Группы компьютеров DM**).

   b. Нажмите **Подключиться ко все категориям**, если требуется выбрать компьютеры из еще не подключенных директорий.
   c. Выберите необходимые компьютеры или группы компьютеров. Свернутые группы отмечены пиктограммой ; развернутые – . Чтобы развернуть или свернуть группу, нажмите на или дважды нажмите на названии группы левой кнопкой мыши.
      Вы также можете указать имена или IP-адреса компьютеров следующими способами:
      - вручную в строке, расположенной внизу диалогового окна. При перечислении используйте точку с запятой;
      - нажать **Импорт** и загрузить текстовый файл, где перечислены IP-адреса или DNS-имена компьютеров: каждая запись должна начинаться с новой строки; пустых строк быть не должно. Сформировать такой файл можно с помощью утилиты сканирования (подробнее см. "Обнаружение рабочих станций для установки агентов").

   d. После того, как вы выберете компьютеры, нажмите **ОК**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи отобразится список выбранных компьютеров.
      Чтобы удалить компьютер из списка, выберите его имя и нажмите **Удалить**.
      Когда вы полностью определите список компьютеров, нажмите **Далее**.
6. Мастер создания задачи отобразит сервера, которые на данный момент зарегистрированы в Системе.
   Вы также можете изменить директорию на компьютерах, куда будет устанавливаться Агент (по умолчанию – `%Program Files%\InfoWatch\DeviceMonitor\Client`).

> **Важно!**
>
> Путь к каталогу может содержать следующие символы: 0-9, a-z, A-Z, ":", ".", "_", "-", "\", " ". При наличии в пути других символов, установка Агента будет некорректной.

Нажмите **Далее**.

7. Мастер создания задачи отобразит уникальное имя для сертификата proxy-сервера Device Monitor (Issuer Distinguished name, Proxy Root Issuer DN). При необходимости вы можете изменить его параметры; при этом имя должно соответствовать стандарту X.509, обязательно содержать поле CN (Common Name), поля внутри имени должны быть разделены запятой.
   Нажмите **Далее**.
8. Определите настройки работы Агента:
   - Чтобы защитить Агент от удаления сотрудником, укажите пароль, который будет запрашиваться при попытке удалить Агент Device Monitor, и подтвердите его.
   - **Скрывать присутствие агента на компьютере до получения конфигурации с сервера DM** – признак того, что Система будет скрывать присутствие Агента на рабочих станциях до установки связи с сервером DM.

     Важно!

     Неуведомление об использовании перехватчика может входить в конфликт с действующим законодательством вашей страны.

     Важно!

     Настройки скрытия/оповещения используются на Агенте до первого обращения к серверу. После обращения к серверу будут действовать настройки той группы компьютеров, к которой принадлежит данный компьютер.

     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.

     Если данная настройка не отмечена, в области уведомлений панели задач Windows на компьютере, где установлен Агент, будет отображаться пиктограмма . При нажатии на этот значок доступна информация о работе Агента, а также список контролируемых в данный момент устройств.
   - **Устанавливать компонент перехвата сетевого трафика** – если настройка отмечена, на компьютер будет установлен компонент **iw_proxy**.
   - **Устанавливать компонент контроля сетевых соединений** – если настройка отмечена, на компьютер будет установлен перехватчик **Network Monitor**.

     Важно!

Не рекомендуется устанавливать компонент контроля сетевых соединений в образ, который впоследствии будет являться базовым для инфраструктуры VDI под управлением Citrix Provisioning Services, т.к. это приведет к нарушению данной технологии и негативно повлияет на работоспособность всей схемы.

- 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**.
- Определите параметры перезапуска задачи: они будут использованы, если первый запуск по каким-либо причинам не произошел; если запуск завершился с ошибкой, то повторный запуск производиться не будет. Укажите количество попыток и время между попытками, в минутах.
- Чтобы выполнение задачи началось немедленно после ее сохранения, отметьте настройку **Запустить задачу сразу после сохранения**.
- Укажите параметры учетной записи, от имени которой будет запущена задача. Распространение агентов может быть осуществлено только от имени учетной записи, обладающей правами администратора на всех компьютерах, где будет произведена установка.
  Если на шаге 3 была выбрана задача распространения на компьютеры под управлением ОС семейства Linux, выберите механизм повышения привилегии `sudo` / `su`.
  Если вы выбрали механизм повышения привилегии `su`:
  - Оставьте неактивной опцию **Использовать указанные учетные данные**, чтобы осуществить распространение агентов от имени пользователя, указанного ранее на этом шаге.
    или
  - Отметьте опцию **Использовать указанные учетные данные** и введите учетные данные пользователя, от имени которого будет осуществлено распространение агентов.

Важно!

Пользователь, от имени которого запускается задача первичного распространения, обязательно должен иметь пароль. В противном случае задача запущена не будет.

Пароль учетной записи, от имени которой производится запуск задачи, в Системе не сохраняется.

Если по окончании создания задачи она не будет запущена немедленно, то при последующем запуске этой задачи из Консоли управления потребуется ввод пароля.

Если у используемой учетной записи истекает пароль учетной записи Windows (предупреждение о необходимости смены пароля отображается в Windows за 3 дня до истечения пароля), то задача первичного распространения, запущенная от имени этого пользователя, не сможет быть выполнена.

Важно!

На рабочих станциях под управлением ОС Astra Linux Special Edition версии 1.7 необходимо настроить максимальный уровень мандатного доступа для пользователя, от имени которого будет произведена установка Агента. Например, чтобы повысить уровень доступа для пользователя `root`, используйте команду:

```
sudo pdpl-user -i 63 root
```

По окончании настройки нажмите **Далее**.

9. Определите параметры перезагрузки компьютера.

Примечание:

Если на предыдущем шаге была выбрана настройка **Скрывать присутствие агента на компьютере до получения конфигурации с сервера DM**, то данные настройки будут недоступны.

Возможные значения:

- **Ожидать перезагрузки без уведомления сотрудника**. Агент может:
  - начать уведомление сотрудника сразу (параметр *Не ожидать*);
  - начать уведомление сотрудника через указанное время (параметр *Ожидать* – требуется указать время до начала уведомлений);
  - не уведомлять сотрудника вообще (параметр *Ожидать бесконечно*).
- **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки**. После завершения ожидания перезагрузки в "молчаливом" режиме (см. настройку **Ожидать перезагрузки без уведомления сотрудника**), или сразу же после завершения процесса установки, Агент Device Monitor начнет уведомлять сотрудника о необходимости перезагрузки:
  - в течение указанного времени (параметр *Уведомлять в течение*);
  - постоянно (параметр *Уведомлять бесконечно*);
  - не уведомлять сотрудника вообще (параметр *Не уведомлять*).

  При необходимости, измените длительность и частоту напоминаний и укажите текст сообщения, которое будет отображаться в напоминании о необходимости перезагрузки. Сообщение может содержать не более 255 символов.

- **Показать предупреждение перед принудительной перезагрузкой**. Если параметр отмечен, то сотруднику будет показано окно о принудительной перезагрузке компьютера и дано 5 минут на завершение своих операций. После этого перезагрузка будет осуществлена принудительно. Если параметр не отмечен, то принудительная перезагрузка (если она вообще должна производиться согласно сделанным настройкам) будет произведена неожиданно для сотрудника.

  > **Важно!**
  >
  > Для корректной блокировки съемных устройств после обновления Агента на ОС семейства Linux обязательно перезагрузите рабочую станцию.
  >
  > Принудительная перезагрузка будет произведена, если ни параметр **Ожидать перезагрузки без уведомления сотрудника**, ни параметр **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки** не установлены, либо период ожидания завершен, а сотрудник так и не перезагрузил компьютер.

По окончании настройки нажмите **Далее**.

10. Просмотрите сводку информации о задаче. Если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). Если все указано верно, нажмите **Готово**.

4.6.5 Создание задачи обновления

> **Важно!**
>
> При обновлении Device Monitor версий 7.2–7.16 необходимо обновлять Агенты только с помощью задач первичного распространения (см. статью *Создание задачи первичного распространения*). При обновлении с версии 7.17 и выше используется процедура, описанная в этой статье.

Агенты InfoWatch Device Monitor необходимо обновить после обновления серверной части InfoWatch Device Monitor: подробнее см. *InfoWatch Traffic Monitor. Руководство по установке*, раздел *Обновление серверной части InfoWatch Device Monitor*.

> **Примечание.**
>
> Помимо описанного ниже способа, вы можете использовать функцию автоматического создания задачи обновления для выбранных компьютеров, как описано в разделе *Обновление Агентов на контролируемых рабочих станциях* (см. документ *InfoWatch Traffic Monitor. Руководство по установке*).

Чтобы создать задачу обновления Агентов InfoWatch Device Monitor, перейдите в раздел **Задачи** и выполните одно из следующих действий:

- в главном меню выберите **Правка** > **Добавить задачу**;
- нажмите **Добавить задачу** в верхней части раздела **Задачи**.

В открывшемся диалоговом окне **Мастер создания задачи** выполните следующие шаги:

1. Выберите **Задача обновления** (для обновления компьютеров с ОС Windows) или **Задача обновления (Linux)** (для обновления компьютеров с ОС Astra Linux), введите имя задачи и ее описание, а затем нажмите **Далее**.
2. Мастер создания задачи отобразит адреса хранилищ, которые служат точками распространения Агентов на рабочие станции и последнюю версию Агента на этих точках. При необходимости вы можете изменить эти параметры и задать другое количество попыток загрузки обновления.
   Нажмите **Далее**.
3. Создайте список компьютеров, на которых необходимо обновить Агент Device Monitor.
   Чтобы добавить компьютер (или несколько компьютеров):
   a. Нажмите **Добавить**. Откроется диалоговое окно **Выбор компьютеров**. В узле **Группы компьютеров DM** отобразится перечень компьютеров, на которые установлен Агент Device Monitor с версией, не соответствующей версии Сервера Device Monitor. Эти компьютеры могут быть автоматически обновлены (версия агентского ПО должна быть 4.0.651 и выше).
   b. Выберите необходимые компьютеры или группы компьютеров. Свернутые группы отмечены значком , развернутые – . Чтобы развернуть или свернуть группу, нажмите или дважды нажмите на названии группы левой кнопкой мыши. Вы также можете использовать строку поиска **Фильтр по названию компьютера**. Чтобы начать поиск компьютера, нажмите **Найти**.
   c. После того как вы укажете добавляемые компьютеры, нажмите **ОК**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи отобразятся выбранные компьютеры.

   Чтобы удалить компьютер из списка, выберите его имя и нажмите **Удалить**.
   После того, как вы полностью определите список компьютеров, нажмите **Далее**.
4. Мастер создания задачи отобразит уникальное имя для сертификата proxy-сервера Device Monitor (Issuer Distinguished name, Proxy Root Issuer DN). При необходимости вы можете изменить его параметры. При этом имя должно соответствовать стандарту X.509, обязательно содержать поле CN (Common Name), поля внутри имени должны быть разделены запятой.
   Нажмите **Далее**.
5. Укажите параметры перезагрузки компьютеров:
   - **Ожидать перезагрузки без уведомления сотрудника**. Агент может:
     - Уведомить сотрудника сразу (параметр *Не ожидать*);
     - Уведомить сотрудника через указанное время (параметр *Ожидать* – требуется указать время до начала уведомлений);
     - Не уведомлять сотрудника (параметр *Ожидать бесконечно*).
   - **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки**. После завершения ожидания перезагрузки в "молчаливом" режиме (см. настройку **Ожидать перезагрузки без уведомления сотрудника**) или сразу же после завершения процесса установки Агент Device Monitor начнет уведомлять сотрудника о необходимости перезагрузки в течение указанного времени (параметр *Уведомлять в течение*) или постоянно (параметр *Уведомлять бесконечно*), либо не будет уведомлять (параметр *Не уведомлять*). При необходимости измените длительность и частоту напоминаний и укажите текст сообщения, которое будет отображаться в напоминании о необходимости перезагрузки. Сообщение может содержать не более 255 символов.
   - **Показать предупреждение перед принудительной перезагрузкой** – признак того, будет ли показано окно о принудительной перезагрузке компьютера

(сотруднику дается 5 минут на завершение операций) или перезагрузка будет осуществлена принудительно.

> **Важно!**
>
> Для корректной блокировки съемных устройств после обновления Агента на ОС семейства Linux обязательно перезагрузите рабочую станцию.
>
> Если на рабочей станции включена настройка **Скрывать присутствие агента на рабочей станции**, то уведомления отображаться не будут.

6. Укажите **Параметры запуска задачи**: они будут использованы, если первый запуск по каким-либо причинам не произошел. Если запуск завершился с ошибкой, то повторный запуск производиться не будет. Укажите количество попыток и время между попытками (в минутах).
   При необходимости отметьте поле **Запустить задачу сразу после сохранения**: задача будет запущена сразу же после ее сохранения.
   Нажмите **Далее**.
7. Просмотрите сводку информации о задаче. Если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). Если все указано верно, нажмите **Готово**.

> **Важно!**
>
> Если на компьютере используется программное обеспечение Kaspersky Internet Security, то для обновления Агентов InfoWatch Device Monitor необходимо отключить самозащиту Kaspersky Internet Security.
>
> О том, как выключить самозащиту, см. статью *Как включить/выключить самозащиту Kaspersky Internet Security*.

4.6.6 Создание задачи смены пароля деинсталляции

Чтобы создать задачу смены пароля, требуемого у сотрудника при попытке удалить Агента InfoWatch Device Monitor:

1. Перейдите к разделу **Задачи**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить задачу**;
   - воспользуйтесь кнопкой **Добавить задачу**, расположенной в верхней части раздела Задачи.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно Мастера создания задачи.
3. Выберите **Задача смены пароля деинсталляции**, введите имя задачи и ее описание, затем нажмите **Далее**.
4. Создайте список компьютеров, на которых необходимо сменить пароль деинсталляции. Чтобы добавить компьютер (или несколько компьютеров):
   a. Нажмите **Добавить**. В открывшемся диалоговом окне **Выбор компьютеров**, в узле **Группы компьютеров DM**, отобразится перечень компьютеров, на которые

установлен Агент Device Monitor. Вы также можете использовать строку поиска **Фильтр по названию компьютера**. Чтобы найти компьютер, нажмите **Найти**.

b. Выберите необходимые компьютеры или группы компьютеров, отмечая их. Свернутые группы отмечены пиктограммой ; развернутые - . Для того, чтобы развернуть или свернуть группу, дважды нажмите на ней левой кнопкой мыши.

c. После того, как вы укажете компьютеры, нажмите **Выбрать**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи будет отображен перечень выбранных компьютеров.

Чтобы удалить компьютер из списка, выберите его имя и нажмите **Удалить**.

После того, как вы полностью определите список компьютеров, нажмите **Далее**.

5. Укажите:
   - **Пароль**, который будет запрашиваться у сотрудника при попытке удалить Агент Device Monitor. Подтвердите пароль.
   - **Параметры перезапуска задачи**: они будут использованы, если первый запуск по каким-либо причинам не произошел; если запуск завершился с ошибкой, то повторный запуск производиться не будет. Укажите количество попыток и время между попытками, в минутах.
   - При необходимости, отметьте поле **Запустить задачу немедленно**: задача будет запущена сразу же после ее сохранения.

   Нажмите **Далее**.
6. Просмотрите сводку информации о задаче. если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). если все указано верно, нажмите **Готово**.

4.6.7 Создание задачи удаления

Чтобы создать задачу централизованного удаления Агентов InfoWatch Device Monitor:

1. Перейдите к разделу **Задачи**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить задачу**;
   - воспользуйтесь кнопкой **Добавить задачу**, расположенной в верхней части раздела **Задачи**.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно **Мастера создания задачи**.
3. На шаге 1 выберите **Задача удаления продукта** (для удаления агента с компьютеров с ОС Windows) или **Задача удаления продукта (Linux)** (для удаления агента с компьютеров с ОС Astra Linux или РЕД ОС), введите имя задачи и ее описание, затем нажмите **Далее**.
4. На шаге 2 создайте список компьютеров, с которых необходимо удалить Агент Device Monitor. Чтобы добавить компьютер (или несколько компьютеров):
   a. Нажмите **Добавить**. В открывшемся диалоговом окне **Выбор компьютеров**, в узле **Группы компьютеров DM**, отобразится перечень компьютеров, на которые установлен Агент Device Monitor. Также вы можете использовтаь строку поиска **Фильтр по названию компьютера**. Чтобы начать поиск компьютера, нажмите **Найти**.

   b. Выберите необходимые компьютеры или группы компьютеров. Свернутые группы отмечены пиктограммой ; развернутые - . Для того, чтобы развернуть или свернуть группу, дважды нажмите на ней левой кнопкой мыши.
   Вы также можете перечислить имена или IP-адреса компьютеров:

- вручную, в строке внизу диалогового окна; при перечислении используйте точку с запятой;
- нажать **Импорт** и загрузить текстовый файл, где перечислены IP-адреса или DNS-имена компьютеров: каждая запись должна начинаться с новой строки; пустых строк быть не должно.

c. После того, как вы укажете добавляемые компьютеры, нажмите **Выбрать**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи отобразятся выбранные компьютеры.

Чтобы удалить компьютер из списка, выберите его имя и нажмите **Удалить**.
После того, как вы полностью определите список компьютеров, нажмите **Далее**.

5. На шаге 3 определите параметры перезапуска задачи: они будут использованы, если первый запуск по каким-либо причинам не произошел; если запуск завершился с ошибкой, то повторный запуск производиться не будет. Укажите количество попыток и время между попытками, в минутах.
   Чтобы начать выполнение созданной задачи сразу же после ее сохранения, отметьте поле **Запустить задачу немедленно**.
   Нажмите **Далее**.
6. Просмотрите сводку информации о задаче. если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). если все указано верно, нажмите **Готово**.

> **Важно!**
>
> В случае наличия на компьютере программного обеспечения Kaspersky Internet Security для удаления Агентов InfoWatch Device Monitor необходимо отключить самозащиту Kaspersky Internet Security.
>
> Чтобы выключить самозащиту см. интернет-статью "Как включить/выключить самозащиту Kaspersky Internet Security"

4.6.8 Запуск, остановка, редактирование и удаление задачи

Если при создании задачи вы выбрали настройку **Запустить задачу сразу после сохранения**, то задача начнет выполняться немедленно после ее создания. В противном случае вам будет необходимо выполнить запуск задачи вручную. Также это может потребоваться в том случае, если по каким-либо причинам вам потребовалось остановить задачу, и необходимо запустить ее вновь.

О порядке выполнения этих и других операций см. таблицу ниже.

Для выполнения любого из этих действий необходимо сначала выбрать необходимую задачу из списка на панели **Задачи**.

> **Важно!**
>
> При запуске задач распространения/обновления/удаления агентов на Astra Linux или РЕД ОС запрашивается логин и пароль для авторизации на рабочих станциях. При этом пользователь, логин и пароль которого указывается при запуске, должен находиться в списке `sudo users` на указанных в задаче рабочих станциях.

Примечание:

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

- вручную включить доступ на рабочую станцию по SSH, выполнив команду: `service sshd start`
- раскомментировать в файле `/etc/openssh/sshd_config` строку `PermitRootLogin`

Действие	Шаги
Запуск задачи	▪ в главном меню выберите команду **Правка** > **Выполнить**; ▪ воспользуйтесь кнопкой **Выполнить**, расположенной в верхней части панели Задачи; ▪ щелкните по задаче правой кнопкой мыши и в контекстном меню выберите **Выполнить**.
Остановка задачи	▪ в главном меню выберите команду **Правка** > **Остановить**; ▪ воспользуйтесь кнопкой **Остановить**, расположенной верхней части панели Задачи; ▪ щелкните по задаче правой кнопкой мыши и в контекстном меню выберите **Остановить**.
Изменение списка компьютеров в задаче	▪ воспользуйтесь кнопками **Добавить компьютер в задачу** или **Исключить компьютер из задачи**, расположенными в верхней части рабочей области; ▪ щелкните правой кнопкой на строке необходимого компьютера и выберите **Добавить компьютер в задачу** или **Исключить компьютер из задачи**; ▪ нажмите Ctrl+Shift+N для добавления компьютера в задачу или Delete для исключения компьютера из задачи. **Внимание!** Удалить рабочую станцию с запущенной, но незавершенной задачей, нельзя.
Редактирование задачи	▪ в главном меню выберите команду **Правка** > **Редактировать задачу**;

Действие	Шаги
	▪ воспользуйтесь кнопкой **Редактировать задачу**, расположенной верхней части панели навигации; ▪ щелкните правой кнопкой на названии задачи и выберите **Редактировать задачу**; ▪ дважды щелкните по задаче левой кнопкой мыши; ▪ нажмите Ctrl+E. Определите новые параметры задачи, как это делается при ее создании (см. "Создание задачи первичного распространения", "Создание задачи обновления", "Создание задачи смены пароля деинсталляции", "Создание задачи удаления").
Удаление задачи	▪ в главном меню выберите команду **Правка** > **Удалить задачу**; ▪ воспользуйтесь кнопкой **Удалить задачу**, расположенной верхней части панели навигации; ▪ щелкните правой кнопкой на названии задачи и выберите **Удалить задачу**; ▪ нажмите Ctrl+D. **Внимание!** Удалить задачу, где есть компьютеры с запущенной, но незавершенной задачей, нельзя.
Просмотр журнала ошибок для компьютера	▪ воспользуйтесь кнопкой **Журнал ошибок**, расположенной в верхней части рабочей области; ▪ щелкните правой кнопкой на строке необходимого компьютера и выберите пункт **Журнал ошибок**; ▪ нажмите Ctrl+L.

4.6.9 Ошибки установки Агентов

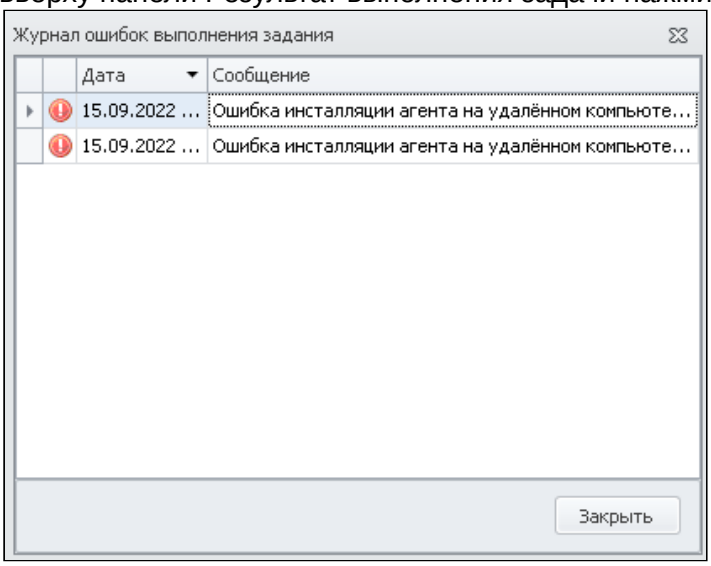
В процессе выполнения задач на удаленную установку Агентов InfoWatch Device Monitor на рабочие станции возможно возникновение проблем установки. На это будет указывать значение параметра **Статус выполнения задачи** в перечне задач: см. "Просмотр задач".

Чтобы просмотреть ошибки, возникавшие при выполнении задачи:

1. Перейдите к разделу **Задачи**.
2. На панели **Задачи** выберите задачу, ошибки выполнения которой необходимо просмотреть.
3. В столбце **Статус выполнения задачи** выберите значение фильтра Ошибка (о работе с фильтрами см. "Использование стандартных фильтров").

> **Примечание:**
>
> Статус **Нет доступа** свидетельствует о том, что рабочая станция недоступна (выключена или отключена от сети).

4. В строке рабочей станции, на которой возникла ошибка, выполните одно из следующих действий:
   - нажмите правой кнопкой мыши и в контекстном меню выберите **Журнал ошибок**;
   - дважды щелкните левой кнопкой мыши на строке рабочей станции;
   - вверху панели Результат выполнения задачи нажмите **Журнал ошибок**.



5. Для просмотра информации об ошибке нажмите левой кнопкой мыши на необходимую строку. В результате будет отображено окно с описанием ошибки Windows. Информацию о причинах ошибки вы можете получить из:
   - описания ошибки;
   - кода ошибки;
   - лог-записей, которые отображаются в окне с описанием ошибки.

> **Важно!**
>
> Лог-записи доступны только для ошибки с самой поздней датой возникновения.

Ошибки могут быть обусловлены следующими причинами:

- рабочая станция недоступна (выключена или отключена от сети);
- другая задача или пользователь блокирует процесс установки или необходимую перезагрузку компьютера (типичное описание - "Другая задача запущена");
- на целевой рабочей станции запрещено использование административных ресурсов;
- учетная запись, используемая для установки, имеет недостаточно прав на целевой рабочей станции.

Если все условия, необходимые для выполнения удаленной установки Агента, перечисленные в разделе "Подготовка к установке" выполнены, и исключена блокировка выполнения задачи пользователем, но, тем не менее, ошибку устранить не удается, вы можете обратиться в службу

технической поддержки компании InfoWatch по адресу support@infowatch.com, приложив к письму описание ошибки и содержимое лога.

4.6.10 Создание пакета установки

Пакет для установки Агента InfoWatch Device Monitor, поставляемый в дистрибутиве, содержит следующие настройки по умолчанию:

- Папка на системном диске рабочих станций, куда будет устанавливаться Агент – `%Program Files%\Infowatch\DeviceMonitor\Client`.
- Пароль деинсталляции – отсутствует.
- После установки Агент Device Monitor начинает уведомлять сотрудника о необходимости перезагрузки компьютера с сообщением. Текст сообщения - "*Необходимо как можно скорее перезагрузить компьютер*". Уведомления отображаются бесконечно, с интервалом в 10 минут.

Для того чтобы изменить эти настройки, вы можете создать собственный инсталляционный комплект.

Чтобы создать пакет для установки Агента InfoWatch Device Monitor:

1. В главном меню выберите команду **Инструменты** > **Создать пакет установки**.
   На экран будет выведено диалоговое окно Мастера создания пакета установки.
2. На шаге **Отметьте серверы DM и каталог установки** отображаются серверы InfoWatch Device Monitor, которые на данный момент зарегистрированы в Системе. Они будут использоваться Агентом для первоначальной установки.
   При необходимости, измените директорию на рабочих станциях, куда будет устанавливаться Агент. Укажите локальную или сетевую директорию, куда будет сохранен готовый набор инсталляционных пакетов.
   Нажмите **Далее**.
3. Мастер создания задачи отобразит уникальное имя для сертификата proxy-сервера Device Monitor (Issuer Distinguished name, Proxy Root Issuer DN). При необходимости вы можете изменить его параметры; при этом имя должно соответствовать стандарту X.509, содержать поле CN (Common Name), поля внутри имени должны быть разделены запятой. Нажмите **Далее**.
4. Определите настройки работы Агента до первого подключения к Серверу:
   - Чтобы защитить Агента от удаления сотрудником, укажите пароль, который будет запрашиваться при попытке удалить Агент Device Monitor, и подтвердите его.
   - **Отображать сотруднику уведомления о работе клиентского модуля** – признак того, что при попытке сотрудника выполнить действие, запрещенное политикой безопасности, ему будет отображаться предупреждающее уведомление. Подробнее см. "Настройка уведомлений сотрудника о нарушении правил".
   - **Скрывать присутствие агента на рабочей станции** – признак того, что Система будет скрывать присутствие Агента на рабочих станциях.

     > **Важно!**
     >
     > Неуведомления об использовании перехватчиков может входить в конфликт с действующим законодательством вашей страны.

> **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.

> **Важно!**
>
> Уведомление о перезагрузке компьютера не будет отображаться, если включено "скрывать присутствие агента на компьютере".

Если данная настройка не отмечена, в области уведомлений панели задач Windows на компьютере, где установлен Агент, будет отображаться пиктограмма . При нажатии на нее доступна информация о работе Агента, а также список контролируемых в данный момент устройств.

- **Устанавливать компонент перехвата сетевого трафика** - устанавливает на рабочую станцию компонент **iw_proxy**.
- **Устанавливать компонент контроля сетевых соединений** - устанавливает на рабочую станцию перехватчик **Network Monitor**.

> **Важно!**
>
> На сервер с Citrix Provisioning Services нельзя устанавливать компонент контроля сетевых соединений: это может привести к серьезным проблемам в работе сервера.

Нажмите **Далее**.

5. На шаге **Укажите параметры перезагрузки** определите следующие параметры:
   - **Ожидать перезагрузки без уведомления сотрудника**. Агент может:
     - Начать уведомление сотрудника сразу (параметр *Не ожидать*),
     - Начать уведомление сотрудника через указанное время (параметр *Ожидать* - требуется указать время до начала уведомлений),
     - Не уведомлять сотрудника вообще (параметр *Ожидать бесконечно*).
   - **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки**. После завершения ожидания перезагрузки в "молчаливом" режиме (см. настройку **Ожидать перезагрузки без уведомления сотрудника**), или сразу же после завершения процесса установки, Агент Device Monitor начнет уведомлять сотрудника о необходимости перезагрузки в течение указанного времени (параметр *Уведомлять в течение*) или постоянно (параметр *Уведомлять бесконечно*), либо не будет уведомлять (параметр *Не уведомлять*). При необходимости, измените длительность и частоту напоминаний и укажите текст сообщения, которое будет отображаться в напоминании о необходимости перезагрузки. Сообщение может содержать не более 255 символов.
   - **Показать предупреждение перед принудительной перезагрузкой** - признак того, отобразит ли Агент уведомление окно о принудительной перезагрузке компьютера и даст ли сотруднику 5 минут на завершение своих операций. если

опция не выбрана, то принудительная перезагрузка (если она предусмотрена другими настройками) будет осуществлена неожиданно для сотрудника.

> **Важно!**
>
> Предупреждение перед принудительной перезагрузкой возникает, если ни параметр **Ожидать перезагрузки без уведомления сотрудника**, ни параметр **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки** не установлены, или период действия их завершен, и сотрудник не перезагрузил компьютер.

Нажмите **Далее**.

6. Просмотрите сводку информации о пакете установки. если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). если все указано верно, нажмите **Готово**.

В папку, указанную на первом шаге создания пакета, будут размещены оригинальные установочные пакеты Агента InfoWatch Device Monitor вместе с дополняющими их файлами скриптов, для развёртывания в соответствии с заданными при формировании пакетов параметрами. Имена скриптов формируются по принципу: "<Имя msi-пакета>.msi.cmd". Содержимое скрипта содержит командную строку для msiexec, предназначенную для развёртывания соответствующего пакета. Если сторонняя система распространения поддерживает возможность указания параметров развёртывания, то данные из файла скрипта можно использовать для непосредственной передачи системе распространения. Если такой возможности не предусмотрено, то развёртывание должно выполняться запуском скрипта вручную.

> **Важно!**
>
> При развёртывании пакета без явного указания параметров или использования скрипта установка будет выполняться со значениями по умолчанию, указанными выше. В зависимости от контекста выполнения установки, это может привести к развёртыванию Агента, не подключённому ни к одному серверу InfoWatch Device Monitor.

4.6.11 Создание шаблона задачи распространения

Чтобы создать шаблон задачи распространения Агента InfoWatch Device Monitor:

1. Перейдите к разделу **Задачи**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Создать шаблон задачи**;
   - на панели **Шаблоны** нажмите .

   Откроется диалоговое окно **Мастера создания шаблона**.
3. Введите имя шаблона, которое должно быть уникальным, и его описание, затем нажмите **Далее**.
4. Мастер создания задачи отобразит параметры установки Агентов со значениями по умолчанию:
   a. Введите директорию на компьютерах, куда будет устанавливаться Агент (по умолчанию – `%Program Files%\Infowatch\DeviceMonitor\Client`).

> **Важно!**
>
> Путь к директории может содержать следующие символы: 0-9,a-z,A-Z, ":", ".", "_", "-", "\", " ". При наличии в пути других символов установка Агента будет некорректной.

b. Укажите точку распространения – адрес хранилища, откуда будет загружен дистрибутив Агента:
   i. Нажмите **Изменить**,
   ii. Выберите при необходимости другую точку из ранее заданных (подробнее см. раздел "Настройка распространения Агентов")
   iii. Нажмите **Сохранить**

c. Установите количество попыток загрузки обновления.

Нажмите **Далее**.

5. Мастер создания задачи отобразит уникальное имя для сертификата proxy-сервера Device Monitor (Issuer Distinguished Name, Proxy Root Issuer DN). При необходимости вы можете изменить его параметры; при этом имя должно соответствовать стандарту X.509, обязательно содержать поле CN (Common Name), поля внутри имени должны быть разделены запятой.
   Нажмите **Далее**.
6. Определите настройки работы Агента:
   - Чтобы защитить Агент от удаления сотрудником, укажите пароль, который будет запрашиваться при попытке удалить Агент Device Monitor, и подтвердите его.
   - **Скрывать присутствие агента на компьютере до получения конфигурации с сервера DM** – признак того, что Система будет скрывать присутствие Агента на рабочих станциях до установки связи с сервером DM.
     Если данная настройка не отмечена, в области уведомлений панели задач Windows на компьютере, где установлен Агент, будет отображаться пиктограмма . При нажатии на этот значок доступна информация о работе Агента, а также список контролируемых в данный момент устройств.

     > **Важно!**
     >
     > - Неуведомление об использовании перехватчика может входить в конфликт с действующим законодательством вашей страны.
     > - Настройки скрытия/оповещения используются на Агенте до первого обращения к серверу. После обращения к серверу будут действовать настройки той группы компьютеров, к которой принадлежит данный компьютер.
     > - 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.

   - **Устанавливать компонент перехвата сетевого трафика** – если настройка отмечена, на компьютер будет установлен компонент **iw_proxy**.
   - **Устанавливать компонент контроля сетевых соединений** – если настройка отмечена, на компьютер будет установлен перехватчик **Network Monitor**.

> **Важно!**
>
> Не рекомендуется устанавливать компонент контроля сетевых соединений в образ, который впоследствии будет являться базовым для инфраструктуры VDI под управлением Citrix Provisioning Services, т.к. это приведет к нарушению данной технологии и негативно повлияет на работоспособность всей схемы.

- Определите параметры перезапуска задачи: они будут использованы, если первый запуск по каким-либо причинам не произошел; если запуск завершился с ошибкой, то повторный запуск производиться не будет. Укажите количество попыток и время между попытками, в минутах.
- Чтобы выполнение задачи началось немедленно после ее сохранения, отметьте настройку **Запустить задачу сразу после сохранения**.
- Укажите параметры учетной записи, от имени которой будет запущена задача. Эта учетная запись должна обладать правами администратора на всех компьютерах, где будет производиться установка.

> **Важно!**
>
> - Пароль учетной записи, от имени которой производится запуск задачи, в Системе не сохраняется.
> - Если по окончании создания задачи она не будет запущена немедленно, то при последующем запуске этой задачи из Консоли управления потребуется ввод пароля.
> - Если у используемой учетной записи истекает пароль учетной записи Windows (предупреждение о необходимости смены пароля отображается в Windows за 3 дня до истечения пароля), то задача первичного распространения, запущенная от имени этого пользователя, не сможет быть выполнена.

По окончании настройки нажмите **Далее**.

7. Определите параметры перезагрузки компьютера.

> **Примечание:**
>
> Если на предыдущем шаге была выбрана настройка **Скрывать присутствие агента на компьютере до получения конфигурации с сервера DM**, то данные настройки будут недоступны.

Возможные значения:

- **Ожидать перезагрузки без уведомления сотрудника**. Агент может:
  - начать уведомление сотрудника сразу (параметр *Не ожидать*),
  - начать уведомление сотрудника через указанное время (параметр *Ожидать* – требуется указать время до начала уведомлений),
  - не уведомлять сотрудника вообще (параметр *Ожидать бесконечно*).
- **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки**. После завершения ожидания перезагрузки в "молчаливом" режиме (см. настройку **Ожидать перезагрузки без уведомления сотрудника**),

или сразу же после завершения процесса установки, Агент Device Monitor начнет уведомлять сотрудника о необходимости перезагрузки:
  - в течение указанного времени (параметр *Уведомлять в течение*);
  - постоянно (параметр *Уведомлять бесконечно*);
  - не уведомлять сотрудника вообще (параметр *Не уведомлять*).

  При необходимости, измените длительность и частоту напоминаний и укажите текст сообщения, которое будет отображаться в напоминании о необходимости перезагрузки. Сообщение может содержать не более 255 символов.
- **Показать предупреждение перед принудительной перезагрузкой**. если параметр отмечен, то сотруднику будет показано окно о принудительной перезагрузке компьютера и дано 5 минут на завершение своих операций. После этого перезагрузка будет осуществлена принудительно. если параметр не отмечен, то принудительная перезагрузка (если она вообще должна производиться согласно сделанным настройкам) будет произведена неожиданно для сотрудника.

  > **Важно!**
  >
  > Принудительная перезагрузка будет произведена, если ни параметр **Ожидать перезагрузки без уведомления сотрудника**, ни параметр **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки** не установлены, либо период ожидания завершен, а сотрудник так и не перезагрузил компьютер.

По окончании настройки нажмите **Далее**.

8. Просмотрите сводку информации о шаблоне. Если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). если все указано верно, нажмите **Готово**.

4.7 Дополнительные возможности

Для более удобной работы с Консолью управления вы можете воспользоваться функциями фильтрации, группировки и сортировки данных, выводящихся в таблицах.
Также некоторые функции системы доступны для выполнения с помощью клавиш быстрого доступа.

4.7.1 Фильтрация табличных данных

Информация в таблицах может быть отфильтрована по одному или нескольким признакам с помощью фильтров различной степени сложности. После применения фильтра в таблице отображаются только те записи, которые удовлетворяют заданным условиям фильтрации.

Работа с фильтрами описана в следующих подразделах:

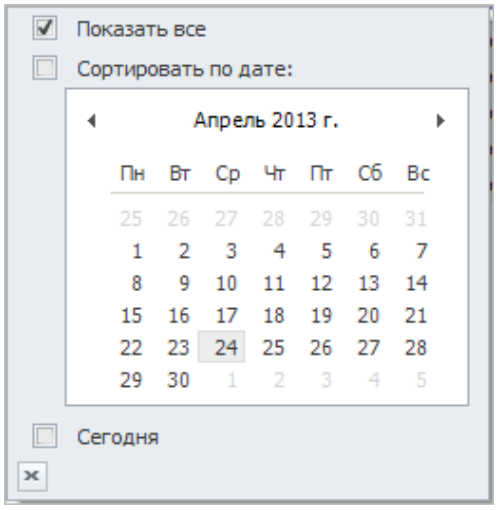
- Фильтр по дате
- Использование стандартных фильтров
- Пользовательский фильтр
- Редактирование фильтра
- Отмена фильтра

Фильтр по дате

Если в таблице отображается характеристика какого-либо временного параметра (например, дата и время установки Агента, время записи в журнал Консоли, время последнего обращения к рабочей станции, дата зарегистрированного события и т.п.), то вы можете отфильтровать записи по этому столбцу, выбрав необходимую дату или период.

Чтобы просмотреть записи, относящиеся к определенной дате или периоду времени:

1. В строке заголовков столбцов таблицы подведите курсор мыши к атрибуту, характеризующему время/дату.
2. Нажмите на кнопку , расположенную справа от названия столбца.



3. В раскрывшейся форме выберите один из следующих фильтров:
   - **Показать все** – отметьте поле, чтобы отобразились записи независимо от их даты.
   - **Сортировать по дате** – в календаре выберите необходимую дату.
     Чтобы выбрать временной период, выберите его, не отпуская левую кнопку мыши.
     Чтобы перейти от отображения дат месяца к отображению месяцев или лет, нажмите на названии месяца/года левой кнопкой мыши.
     Чтобы перейти на месяц вперед или назад, пользуйтесь стрелками.
   - **Сегодня**; **Вчера**; **На прошлой неделе**; **Ранее на этой неделе**; **Ранее в этом году** – состав полей зависит от значений в столбце: например, если записей за текущую дату нет, то поле **Сегодня** будет отсутствовать. Отметьте это поле, чтобы отобразились только те записи, дата которых находится в описанном диапазоне.
4. Чтобы применить выбранный фильтр и закрыть форму, нажмите ✕ либо щелкните левой клавишей мыши по пространству за пределами формы.

Использование стандартных фильтров

Чтобы отфильтровать записи по одному атрибуту:

1. В строке заголовков столбцов таблицы подведите курсор мыши к заголовку того столбца, название которого соответствует нужному атрибуту.
2. Чтобы раскрыть список фильтров, нажмите на кнопку , расположенную справа от названия столбца.

3. В раскрывшемся списке выберите один из следующих фильтров:
   - **Пустые**. Отображение записей, в которых выбранный атрибут имеет значение `<Is Null>` (пустое поле).
   - **Непустые**. Отображение записей, в которых выбранный атрибут имеет значение `<Is Not Null>` (т.е. в поле содержится любое значение атрибута).
   - `<значение атрибута>`. Отображение записей, в которых выбранный атрибут имеет указанное значение.

> **Примечание.**
>
> Выбрав пункт **Условие** из списка фильтров, вы сможете настроить собственные условия фильтрации (подробнее см. "Пользовательский фильтр").

После этого в таблице будут отображены записи, удовлетворяющие заданным условиям фильтрации.

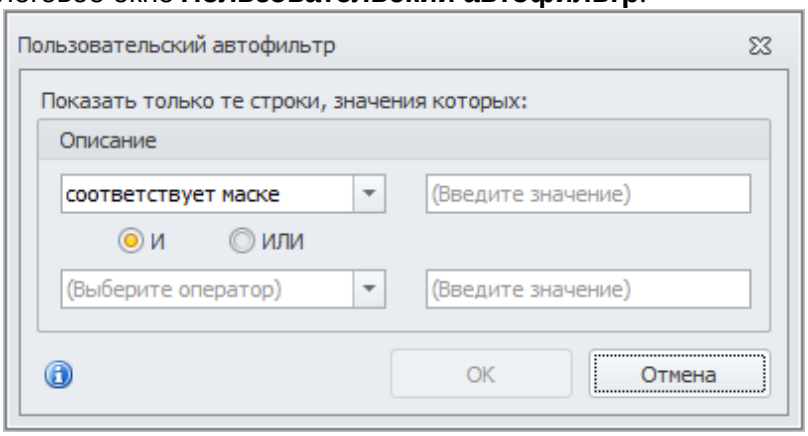
Чтобы отфильтровать записи по нескольким атрибутам, повторите процедуру создания простого фильтра для всех атрибутов, по которым будет производиться фильтрация.

В результате применения составного фильтра в таблице будут отображены записи, отфильтрованные по нескольким атрибутам одновременно.

Пользовательский фильтр

Чтобы задать собственные условия фильтрации:

1. В строке заголовков столбцов таблицы подведите курсор мыши к заголовку того столбца, название которого соответствует нужному атрибуту.
2. Раскройте список фильтров, нажав на кнопку , расположенную справа от названия столбца.
3. В раскрывшемся списке выберите пункт **Условие**. После этого на экран будет выведено диалоговое окно **Пользовательский автофильтр**.



4. В данном окне задайте условия фильтрации:
   - Выберите ограничение условия из раскрывающегося списка в верхнем левом поле.

> **Примечание.**

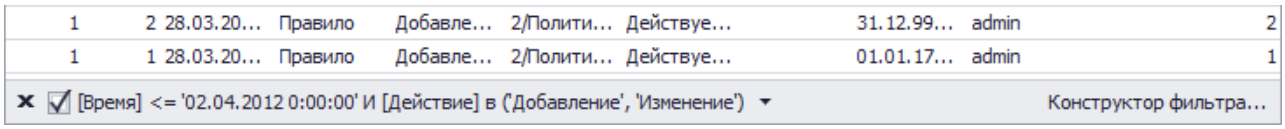
В качестве ограничения условия могут быть использованы операторы сравнения: *равно*, *не равно*, *больше*, *больше или равно*, *меньше*, *меньше или равно*; значения *пустые* (пустое поле) и *непустые* (непустое поле); а также текстовый фильтр с использованием маски. Чтобы получить подсказку по синтаксису текстового фильтра, нажмите .

- В верхнем правом поле укажите значение условия.
- Если необходимо задайте дополнительное условие, для чего выберите нужный логический оператор и укажите второе условие в нижней строке.

> **Примечание.**
>
> Логический оператор **И** выбирают, если нужно отфильтровать записи, удовлетворяющие и первому, и второму условию одновременно.
> Выбор логического оператора **ИЛИ** указывает на то, что будут отфильтрованы записи, удовлетворяющие хотя бы одному из заданных условий.

5. Нажмите **ОК**, чтобы применить фильтр.

После применения фильтра в таблице будут отображены только те записи, которые соответствуют заданным условиям фильтрации. В нижней части того окна, в котором используется фильтр, отобразится строка с условиями фильтрации.



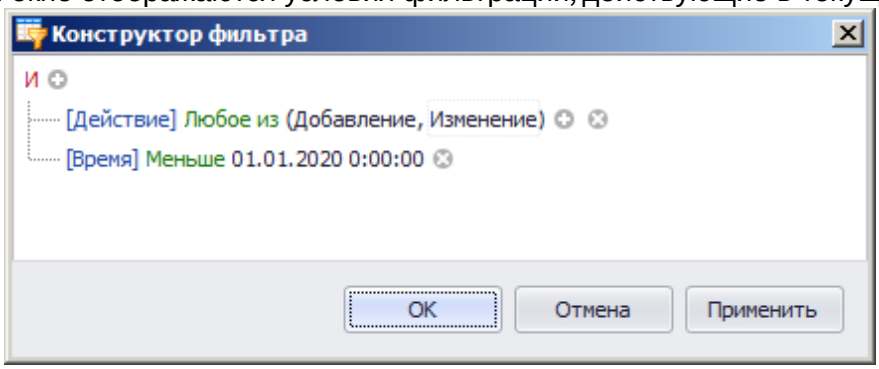
Чтобы отменить действие фильтра и просмотреть все записи таблицы, снимите отметку в строке фильтра. Чтобы применить фильтр вновь, установите отметку.

Чтобы повторно использовать фильтр, щелкните левой кнопкой мыши по строке фильтра и выберите нужный фильтр из раскрывшегося списка последних применявшихся фильтров. Пользовательские фильтры сохраняются до тех пор, пока не будет закрыто окно, в котором применялся данный фильтр.

Редактирование фильтра

Чтобы отредактировать действующий фильтр:

1. В строке с условиями фильтрации нажмите **Конструктор фильтра**. В открывшемся диалоговом окне отображаются условия фильтрации, действующие в текущий момент.



2. Отредактируйте условия фильтрации. При этом можно выполнять следующие действия:

Действие	Шаги
Изменить атрибут, значение атрибута или оператор	a. Щелкните левой кнопкой мыши по названию атрибута/значения атрибута/оператора b. В меню выберите необходимое значение
Добавить простое условие	Нажмите на кнопку справа от логического оператора или Выберите команду **Добавить условие** в меню логического оператора
Удалить условие	Нажмите на кнопку в конце строки условия
Добавить группу условий	a. Щелкните левой кнопкой мыши по названию логического оператора b. В меню выберите **Добавить группу**
Удалить группу условий	a. Щелкните левой кнопкой мыши по названию группы условий оператора b. В меню выберите **Удалить группу**
Удалить все условия	Выберите команду **Очистить все** в меню логического оператора

3. Нажмите **Применить**, чтобы применить фильтр и просмотреть результаты фильтрации, не закрывая окна **Конструктор фильтров**.
4. Нажмите **ОК**.

Отмена фильтра

Чтобы отменить назначенный фильтр, выполните одно из следующих действий:

- Щелкните левой кнопкой мыши по заголовку столбца, к которому был применен фильтр, и в раскрывшемся списке фильтров выберите пункт **Все**.
  Если был задан составной фильтр, повторите данную операцию для каждого условия, которое нужно отменить.
- Снимите отметку в левой части строки с условиями фильтрации.
- Нажмите на кнопку , расположенную в левой части строки с условиями фильтрации. После этого строка с условиями фильтрации будет закрыта.

4.7.2 Группирование и сортировка записей

Функции группирования предназначены для организации записей таблицы в соответствии с выбранной схемой группы. Схема группы отображается на панели группы, расположенной над строкой

заголовков столбцов. Группирование выполняется по одному или нескольким атрибутам записей (столбцам таблицы).

Чтобы сгруппировать записи по какому-либо атрибуту, в строке заголовков столбцов таблицы щелкните левой кнопкой мыши по заголовку столбца, название которого соответствует нужному атрибуту, и не отпуская кнопку, перетащите заголовок столбца на панель группы. Название атрибута, по которому производилось группирование записей, будет отображено на панели группы.

Чтобы сгруппировать записи по нескольким атрибутам, повторите шаги 1 – 2 для всех атрибутов, которые должны участвовать в группировании.

> **Примечание.**
>
> Порядок группирования записей можно изменить, меняя местами заголовки столбцов в схеме группы. Первым в группировании участвует столбец, заголовок которого расположен слева на верхнем уровне схемы группы.

Сгруппированные записи отображаются в свернутом виде. Чтобы просмотреть информацию по отдельной записи, нажмите на кнопку , расположенную слева от записи, которую нужно просмотреть в развернутом виде. Чтобы свернуть запись, нажмите на кнопку , расположенную слева от записи.

Вы можете отменить группирование по одному или нескольким атрибутам, удаляя столбцы из схемы группы.

Чтобы отменить группирование записей по какому-либо атрибуту:

1. На панели группы щелкните левой кнопкой мыши по заголовку столбца, который вы хотите удалить из схемы группы, и, не отпуская кнопку, перетащите его в строку заголовков таблицы. Местоположение столбца при этом будет указываться прямоугольной рамкой.
2. Перемещайте заголовок столбца вдоль строки заголовков, чтобы выбрать нужное положение, и затем отпустите левую кнопку мыши. В результате столбец будет перемещен на указанное место.
   Вы также можете переместить заголовок столбца на свободное пространство. В этом случае заголовок вернется на место, которое он занимал до группирования.

При помощи функции сортировки вы можете настроить отображение записей в порядке либо возрастания, либо убывания значений какого-либо атрибута таблицы.

Чтобы изменить порядок сортировки значений атрибута в столбце, подведите курсор мыши к заголовку того столбца, по которому нужно выполнить сортировку. Когда нужный заголовок будет выделен, щелкните левой кнопкой мыши. В результате все записи таблицы будут отсортированы по возрастанию/убыванию значений выбранного атрибута.

Чтобы вернуть прежний порядок сортировки, щелкните по выделенному заголовку еще раз.

4.7.3 Клавиши быстрого доступа

В следующей таблице перечислены клавиши и сочетания клавиш, используемые для быстрого доступа к различным функциям Системы.

Название функции	Клавиши быстрого доступа
Соединение с Сервером	

Название функции	Клавиши быстрого доступа
Подключение к Серверу	F4
Выход из Консоли	Alt+F4
Получение справки	
Вызов офлайн-справки в формате .pdf	F1
Вызов онлайн-справки	Ctrl+F1
Настройка элементов главного окна	
Скрытие/отображение Панели навигации	Ctrl+Shift+1
Скрытие/отображение панели Подробно	Ctrl+Shift+2
Скрытие/отображение панели Журнал консоли	Ctrl+Shift+3
Разделы Консоли управления	
Переход к разделу Политики	Ctrl+1
Переход к разделу Группы сотрудников	Ctrl+2
Переход к разделу Группы компьютеров	Ctrl+3
Переход к разделу Белые списки	Ctrl+4
Переход к разделу Категории сигнатур	Ctrl+5
Переход к разделу Приложения	Ctrl+6
Переход к разделу Журнал	Ctrl+7
Переход к разделу Задачи	Ctrl+8
Переход к разделу События	Ctrl+9
Работа со схемой безопасности (общее)	
Переход к режиму редактирования схемы безопасности	F11
Сохранение схемы безопасности	F12

Название функции	Клавиши быстрого доступа
Отмена сохранения схемы безопасности	Shift+F11
Разблокировка схемы безопасности (только Суперпользователь)	Ctrl+Shift+U
Обновление схемы безопасности	F5
Переход к последней версии схемы безопасности (при просмотре одной из предыдущих версий)	F9
Работа с политиками безопасности	
Создание политики безопасности	Ctrl+N
Редактирование политики безопасности	Ctrl+E
Удаление политики безопасности	Ctrl+D
Работа с правилами	
Создание правила	Ctrl+Shift+N
Редактирование правила	Ctrl+Shift+E
Удаление правила	Delete
Работа с группами сотрудников	
Создание группы сотрудников	Ctrl+N
Редактирование группы сотрудников	Ctrl+E
Удаление группы сотрудников	Ctrl+D
Работа с учетными записями сотрудников	
Добавление учетной записи сотрудника в группу	Ctrl+Shift+N
Редактирование учетной записи сотрудника	Ctrl+Shift+E
Исключение сотрудника из группы	Delete
Удаление сотрудника из схемы безопасности	Shift+Delete

Название функции	Клавиши быстрого доступа
Работа с группами компьютеров	
Создание группы компьютеров	Ctrl+N
Редактирование группы компьютеров	Ctrl+E
Удаление группы компьютеров	Ctrl+D
Работа с контролируемыми компьютерами	
Добавление компьютера	Ctrl+Shift+I
Исключение компьютера из группы	Delete
Удаление компьютера из схемы безопасности	Shift+Delete
Работа с белыми списками	
Создание белого списка	Ctrl+N
Редактирование белого списка	Ctrl+E
Удаление белого списка	Ctrl+D
Редактирование записи в белом списке	Ctrl+Shift+E
Работа с сигнатурами	
Создание категории сигнатур	Ctrl+N
Редактирование категории сигнатур	Ctrl+E
Удаление категории сигнатур	Ctrl+D
Исключение сигнатуры из категории	Delete
Настройка фильтров для Журнала аудита и просмотра событий	
Создание фильтра	Ctrl+N
Редактирование фильтра	Ctrl+E
Удаление фильтра	Ctrl+D

Название функции	Клавиши быстрого доступа
Работа с задачами удаленной установки и обновления Агентов	
Создание задачи	Ctrl+N
Редактирование задачи	Ctrl+E
Удаление задачи	Ctrl+D
Добавление компьютера в выбранную задачу	Ctrl+Shift+N
Исключение компьютера из выбранной задачи	Delete
Просмотр журнала ошибок для выбранного компьютера выбранной задачи	Ctrl+L

5 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

6 Глоссарий

Термин	Определение
"В разрыв"	Схема развертывания IW TM, при которой возможно блокирование исходящих из периметра почтовых сообщений с последующей досылкой. При этом сервер IW TM используется в качестве relay-сервера.
Active Directory	LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT
AJAX	Asynchronous Javascript and XML (асинхронный JavaScript и XML) – подход к построению интерактивных пользовательских интерфейсов веб-приложений, заключающийся в «фоновом» обмене данными браузера с веб-сервером
CLI	Command Line Interface – интерфейс командной строки
Domino directory	IBM Lotus Domino Directory – это директория с информацией о пользователях, серверах и группах. Domino Directory – это инструмент, используемый для администрирования системы Domino.
FTP	File Transfer Protocol (протокол передачи файлов) – сетевой протокол, предназначенный для передачи файлов по TCP-сетям
GTalk	Google Talk – программное обеспечения для мгновенного обмена сообщениями, разработанное компанией Google
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста) – протокол прикладного уровня передачи данных в виде текстовых сообщений. См. также: HTTPS, HTTP(S) Monitor
HTTPS	HyperText Transfer Protocol Secure (защищенный протокол передачи гипертекста) – расширение протокола HTTP, поддерживающее шифрование. См. также: HTTP, HTTP(S) Monitor
HTTP-запрос	Запрос, удовлетворяющий требованиям протокола HTTP (POST-запрос, GET-запрос и т. д.). См. также: HTTP, Событие
ICAP	Internet Content Adaptation Protocol – протокол, позволяющий контролировать входящий и исходящий HTTP-трафик. Предоставляет возможность модификации содержимого HTTP-запросов.

Термин	Определение
ICQ	Служба мгновенного обмена сообщениями в сети Интернет. Использует протокол OSCAR.
ICQ-сообщение	Сообщение, передаваемое по протоколу ICQ-OSCAR. См. также: Событие
IMAP	Internet Message Access Protocol Version 4 (протокол доступа к электронной почте Интернета) – сетевой протокол для доступа к электронной почте.
InfoWatch Activity Monitor	Программное обеспечение, предназначенное для контроля деятельности сотрудников
InfoWatch Device Monitor	IW DM: программный комплекс, предназначенный для контроля доступа сотрудников к периферийным устройствам и сетевым ресурсам, мониторинга операций (копирование данных на съемные носители и сетевые хранилища, отправка данных на печать, сетевая активность, использование приложений) и перехвата трафика систем мгновенного обмена сообщениями (Skype, GTalk и Jabber) и т. п.
InfoWatch Prediction	Программное обеспечение, являющееся инструментом предиктивной и поведенческой аналитики
InfoWatch Traffic Monitor	IW TM: программный комплекс, предназначенный для осуществления контроля различных видов трафика (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) и теневых копий данных, копируемых на съемные носители и отправляемых на печать
IW Lync Adapter	Перехватчик событий обмена данными через серверы MS Lync, установленные в инфраструктуре компании
Jabber	Система для быстрого обмена сообщениями и информацией о присутствии на основе открытого протокола XMPP
LAN	Local Area Network – локальная вычислительная сеть
Lotus Adapter	Перехватчик, который устанавливается на почтовом сервере IBM Lotus для перенаправления писем для анализа при помощи IW TM. См. также: Перехватчик
Lotus Domino	Почтовый сервер компании IBM, сообщения которого перехватываются при помощи Lotus Adapter

Термин	Определение
MAPI	Messaging Application Programming Interface – программный интерфейс, позволяющий приложениям работать с различными системами передачи электронных сообщений
MS Lync	Универсальный клиент Microsoft для общения и обмена информацией
MTProto	Криптографический протокол, используемый в системе обмена сообщениями для шифрования переписки пользователей
POP3	Post Office Protocol Version 3 (протокол почтового отделения) – сетевой протокол, используемый для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению
POST-запрос	Метод запроса POST предназначен для запроса, при котором веб-сервер принимает данные, заключенные в тело сообщения, для хранения. Он часто используется для загрузки файла или представления заполненной веб-формы
Relay-сервер	Сервер, выполняющий получение/пересылку электронной почты
RPC	Класс технологий, позволяющих компьютерным программам вызывать функции или процедуры в другом адресном пространстве (как правило, на удаленных компьютерах)
Skype	Служба, обеспечивающая текстовую, голосовую и видеосвязь через Интернет
SMB	Server Message Block – сетевой протокол для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SMTP	Simple Mail Transfer Protocol (простой протокол передачи почты) – сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
S/MIME	Secure/Multipurpose Internet Mail Extensions – стандарт для шифрования и подписи в электронной почте с помощью открытого ключа
SMTP-письмо	Письмо, удовлетворяющее требованиям протокола SMTP. См. также: SMTP, Событие

Термин	Определение
SPAN	Switched Port Analyzer – технология зеркального копирования трафика с одного порта на другой
SPAN-копия	Разновидность транспортного режима Копия. Передача трафика в этом режиме осуществляется через коммутатор CISCO. Копия трафика передается для анализа на сервер Traffic Monitor. См. также: SPAN
SSL	Secure Sockets Layer (уровень защищенных сокетов) – криптографический сетевой протокол, обеспечивающий защищенный обмен данными
Telegram	Мессенджер, позволяющий пересылать текстовые сообщения, изображения, аудио- и видео-файлы (использует протокол MTProto)
WAN	Wide Area Network – глобальная компьютерная сеть
WhatsApp	Мессенджер, позволяющий пересылать текстовые сообщения, изображения, аудио- и видео-файлы (использует собственный протокол)
XMPP	Extensible Messaging and Presence Protocol – сетевой протокол, обеспечивающий мгновенный обмен сообщениями и информацией о присутствии
Агент Consul	Участник кластера Consul. Может быть как сервером, так и клиентом
Администратор	Предустановленная роль и учетная запись Консоли управления, имеющая права на управление другими учетными записями и их правами. Также Администратор – пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. также: Роль пользователя, Офицер безопасности, Пользователь
Активная политика	Политика, действующая в конфигурации, загруженной на хост. См. также: Политика, Хост
Анализ события	Процедура обработки атрибутов, вложенных файлов и текста перехваченных событий и назначения событию дополнительных атрибутов. См. также: Политика, Атрибуты события, Событие
Атрибуты события	Структурированные данные, извлеченные из перехваченных событий и назначенные по результатам их

Термин	Определение
	обработки. См. также: Событие, Политика, Вердикт, Решение, Транспортный режим
Аудит	Контроль действий, выполняемых пользователями Консоли управления: создание и управление схемой безопасности, администрирование Системы. См. также: Журнал аудита, Учетные записи Консоли управления
База данных	Совокупность данных, хранимых в соответствии с используемой схемой данных. Хранит всю информацию, необходимую для работы Системы.
Бланки	Технология поиска заполненных бланков, форм, например, анкет, квитанций и т. п. Бланки хранятся в Системе в виде, недоступном для просмотра ни пользователям, ни администраторам Системы. См. также: Технологии, Элемент технологий
Вердикт	Атрибут события, содержащий заключение о наличии или отсутствии нарушений в анализируемом событии. В сочетании с атрибутом Транспортный режим определяет возможность дальнейшей транспортировки события. См. также: Транспортный режим, Состояние доставки, Атрибуты события, Событие
Версия конфигурации	Фиксированное состояние конфигурации, используемое для контроля изменений в настройках анализа событий. Версия конфигурации фиксируется в момент ее загрузки на хост, и может быть активной (используемой в настоящий момент), редактируемой (последняя версия с текущими изменениями) или сохраненной (имеющей изменения и доступной для редактирования пользователями). См. также: Конфигурация
Вес термина	Степень того, насколько данный термин характеризует категорию; целое число в диапазоне от 1 до 10. Если термин имеет высокий вес (значимость), то при его обнаружении в объекте существует большая вероятность того, что данный объект может быть отнесен к категории, содержащей данный термин. См. также: Термин
Виджет	Элемент интерфейса в виде обособленной области, выводящий заданную статистическую информацию о нарушениях и нарушителях. См. также: Консоль управления, Нарушение, Нарушитель
Вложение	Файл, приложенный к перехваченному событию, любой степени вложенности. См. также: Событие

Термин	Определение
Выгрузки из БД	Технология поиска цитат из базы данных. Выгрузками из БД могут быть списки заработных плат сотрудников, другие личные данные и т. п. См. также: Технологии
Графические объекты	Технология поиска изображений (например, изображений паспорта или банковской карты) в тексте и вложениях перехваченных событий. См. также: Технологии, Событие, Объект защиты
Группа персон и компьютеров	Группа, объединяющая информацию о компьютерах организации, сотрудниках организации, а также внешних контактах. Группы делятся на Группы AD (импортированные из Active Directory), Группы DM (импортированные из Domino Directory) и Группы TM (созданные средствами IW TM). См. также: Персона, Компьютер, Контакт
Заголовки	Вспомогательные данные, размещаемые в начале блока хранимых или передаваемых данных. Используются для формирования в Системе сущности события и определения значений атрибутов этого события. См. также: Событие, Атрибуты события
Защищаемые данные	Набор объектов защиты, их каталогов и файловых форматов, обнаружение которых в событии позволяет характеризовать это событие как подпадающее под ту политику защиты данных, в которой этот набор определен. См. также: Объект защиты, Файловый формат, Политика защиты данных
Инициатор, также: Инициатор события	Персона, чьи действия привели к созданию события в Системе
Интерфейс пользователя	Совокупность средств и методов, при помощи которых пользователь взаимодействует с Системой
Канал перехвата данных	Среда перехвата данных, состоящая из технических средств перехвата данных, средств программного обеспечения и протоколов передачи данных. В Системе поддерживаются следующие каналы перехвата данных: электронная почта (SMTP, IMAP и POP3), веб (HTTP, HTTPS), сервисы мгновенных сообщений (Jabber, ICQ и Skype), теневые копии файлов, события подключения/отключения рабочих станций, задания на печать.
Категории и термины	Технология, выявляющая в тексте события наличие слов и выражений из базы терминов и относящая событие к категории, к которой принадлежат найденные термины. Ранее: Классификатор, БКФ. См. также: Событие, Термин, Категория, Технологии, Объект защиты

Термин	Определение
Категория	Именованная группа терминов, характеризующих определенную тематику. Если Система обнаруживает какой-либо из терминов категории в тексте перехваченного события, то она относит событие к этой категории. См. также: Термин
Компьютер	В терминах Системы под компьютером подразумевается контролируемая рабочая станция или терминальное устройство. См. также: Рабочая станция, Терминальное устройство
Консоль управления (TM)	Графический интерфейс пользователя. Предназначен для управления Системой Traffic Monitor (администрирование Системы, настройка конфигурации, анализ событий и т. п.).
Консоль управления (DM)	Компонент графического пользовательского интерфейса. Предназначен для управления Системой InfoWatch Device Monitor (настройка схемы безопасности, администрирование Системы и пр.).
Контекст события	Внутреннее представление перехваченного события в Системе. XML данные (атрибуты, текст), извлеченные из события и его вложений. После обработки с помощью технологий к контексту добавляются результаты анализа и информация о решении по событию. См. также: Событие, Технологии, Решение
Контролируемые персоны	Набор персон, групп персон и статусов персон, обнаружение которых в событии позволяет характеризовать это событие как подпадающее под ту политику контроля персон, в которой этот набор определен. См. также: Персоны, Группа персон, Статус персоны, Политика контроля персон
Конфигурация	Набор настроек, необходимых для проверки событий а также для мониторинга и анализа данных. См. также: Событие, Технологии, Списки, Политика
Корпоративная политика безопасности	Принятая в компании совокупность технических, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, регламентирующих все вопросы обеспечения безопасности информации
Лицензия	Право на использование Системы. Получается при приобретении Системы и определяет допустимое количество пользователей, используемые технологии и перехватчики и т. п. Также см.: Технологии, Перехватчики

Термин	Определение
Маска	Шаблон поиска — метод описания поискового запроса с использованием метасимволов. Маски используют для поиска файлов и папок
Мобильное устройство	Тип компьютера: смартфон или планшетный компьютер с установленной ОС семейства Android, Windows Phone или iOS. См. также: Компьютер
Монитор	См. Перехватчик
Морфология	Параметр термина: при использовании морфологии поиск по тексту будет осуществляться с учетом всех форм этого термина. См. также: Термин
Нарушение	Значение атрибута «Решение», означающее, что зарегистрировано нарушение корпоративной политики безопасности. См. также: Решение, Корпоративная политика безопасности
Нормальный транспортный режим	Режим, в котором выполняется анализ и фильтрация проходящего трафика. В этом режиме возможна блокировка запрещенного Системой трафика. См. также: Транспортный режим, "В разрыв"
Область видимости	Способ разделения перехваченных событий для ограничения доступа к ним пользователей Консоли управления. События, удовлетворяющие критериям вхождения в какую-либо область видимости, будут видны только тем пользователям, которые имеют доступ к этой области видимости (при условии, что пользователь имеет привилегии на просмотр и/или работу с объектами). См. также: Событие, Привилегия
Объект защиты	Набор элементов технологий, обнаружение которых в событии позволяет отнести это событие к определенному типу бизнес-документов (каталогу объектов защиты). Объекты защиты используются при определении политик защиты данных. См. также: Элемент технологий, Политика защиты данных.
Основание вердикта	Атрибут события, описывающий причину, по которой событию был присвоен вердикт. См. также: Атрибуты события, Вердикт
Отчет	Выборка, обеспечивающая наглядное отображение статистических данных о событиях. См. также: Консоль управления, Событие

Термин	Определение
Офицер безопасности	Основной пользователь Консоли управления. Также – предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в Системе, за исключением административных. См. также: Консоль управления, Пользователь, Роль пользователя, Привилегия, Администратор
Перехват данных	Процесс получения, разбора, рубрикации и преобразования данных (или их копии) в контекст. Осуществляется перехват данных, передаваемых по протоколам SMTP, IMAP, POP3, HTTP, HTTPS, ICQ/OSCAR, Skype, IXP, XMPP, MMP, FTP. См. также: Перехватчик, Контекст события
Периметр	Контейнер, содержащий элементы инфраструктуры компании (персоны, компьютеры, домен и прочие) и контактные данные. Используется для того, чтобы логически разделить организацию на структурные элементы и следить за трафиком каждого из таких элементов. См. также: Группа персон и компьютеров
Персона	Учетная запись сотрудника организации или внешнего контакта, содержащаяся в справочнике Системы и позволяющая обрабатывать данные, принадлежащие этой учетной записи, как единое целое, а также отображать события, относящиеся к ней, в удобном для пользователя виде. См. также: Группа персон и компьютеров
Плагин	Расширение, позволяющее Системе осуществлять прием событий предустановленных или новых типов от внешних перехватчиков, автоматическое обновление эталонных выгрузок данными от внешних систем (таких как SAP или 1С), предоставление сторонним системам данных об объектах ТМ
Платформа	Комплекс, состоящий из компонентов, подсистем, интерфейсов и производственных процессов. Платформа выступает в качестве базы для развертывания семейства продуктов ИнфоВотч и сборки готовых изделий из стандартизированных компонентов.
Политика	Совокупность правил, в соответствии с которыми проводится анализ и обработка событий. См. также: Политика, Активная политика, Правило
Политика DM	Совокупность правил, при помощи которых осуществляется мониторинг операций по созданию файлов на съемных устройствах, сетевой активности, печати документов на принтере; определяется уровень доступа к контролируемым периферийным устройствам и

Термин	Определение
	т. д. Политика может быть назначена только группе (сотрудников или компьютеров). См. также: Правило DM
Политика контроля персон	Политика для оперативного добавления правил контроля персон, групп персон или персон с указанным статусом. См. также: Политика, Правило контроля персон, Персона, Статус персоны
Пользователь	Пользователь Системы Traffic Monitor – администратор, Офицер безопасности и др. См. также: Администратор, Офицер безопасности, Персона
Пользователь Консоли управления	Пользователь, в задачи которого входит выполнение различных функций по управлению Системой. Каждому пользователю назначается роль в соответствии с требованиями корпоративной политики безопасности.
Порог встречаемости	Количество текстовых объектов, найденных в событии, достаточное для обнаружения объекта защиты, в котором определен данный порог встречаемости. См. также: Событие, Текстовые объекты, Объект защиты
Порог цитируемости	Процент эталонного документа, найденный в событии в виде цитат, достаточный для отнесения события к этому эталонному документу. См. также: Событие, Эталонный документ, Цитата
Правило	Сущность, определяющая действия Системы в ответ на те или иные действия персон с защищаемыми объектами. Правило состоит из набора условий, по которым ведется проверка событий, и действий, осуществляемых при выполнении или невыполнении заданных условий. См. также: Событие, Политика, Защищаемый объект, Правило контроля персон, Правило копирования, Правило передачи, Правило хранения
Правило DM	Набор ограничений и условий, в соответствии с которыми осуществляется мониторинг операций по созданию файлов на съемных устройствах, сетевой активности, печати документов на принтере; определяется уровень доступа к контролируемым периферийным устройствам. С каждым перехватчиком сопоставлен отдельный тип правила. Правило действует в пределах той политики безопасности, в которую входит это правило. См. также: Политика DM
Правило контроля персон	Правило, назначающее атрибуты событию с указанным уровнем нарушения, и в котором среди отправителей или получателей есть персоны, указанные в политике, куда входит это правило. Позволяет переназначать статус

Термин	Определение
	персонам и отправлять уведомления. См. также: Правило, Атрибуты события, Персона, Уровень нарушения, Статус персоны, Уведомление, Политика контроля персон
Правило копирования	Правило, регулирующее копирование или печать защищаемых данных. См. также: Правило, Защищаемые данные, Политика защиты данных
Правило передачи	Правило, регулирующее отправку и получение защищаемых данных. См. также: Правило, Защищаемые данные, Политика защиты данных
Правило хранения	Правило, регулирующее хранение защищаемых данных. См. также: Правило, Защищаемые данные, Политика защиты данных
Привилегия	Сущность, определяющая возможность пользователя выполнять какое-либо действие (набор действий) при работе с Системой
Прокси-сервер	Служба, позволяющая выполнять косвенные запросы к другим сетевым службам. Прокси передает все запросы программ абонента в сеть, и, получив ответ, отправляет его обратно абоненту.
Рабочая станция	Тип компьютера: десктоп или ноутбук с ОС семейства Windows, Linux или Mac. См. также: Компьютер
Режим копии	Один из транспортных режимов Системы IW TM. В этом режиме реальный трафик не проходит через Систему. Анализу подвергается копия трафика. В данном режиме невозможна фильтрация трафика средствами Системы. См. также: Транспортный режим
Решение	Заключение Офицера безопасности о том, является ли событие нарушением корпоративной политики безопасности. Может принимать значения «Решение не принято», «Нарушение» и «Нет нарушений». См. также: Офицер безопасности, Корпоративная политика безопасности, Событие, Атрибуты события, Нарушение, Политика, Вердикт
Роль пользователя	Совокупность привилегий, определяющих набор действий, которые пользователь может выполнять при работе с Системой. См. также: Администратор, Офицер безопасности, Консоль управления, Привилегия

Термин	Определение
Сводка	Раздел Консоли управления, отображающий статистическую информацию по нарушениям и нарушителям на виджетах. См. также: Консоль управления, Виджет, Нарушение
Сигнатура файла	Целочисленная константа, используемая для однозначной идентификации файлов определенного типа
Событие	Объекты перехвата трафика (SMTP-, IMAP-, POP3-письма, HTTP-запросы, ICQ-сообщения, Skype-сообщения), теневые копии файлов и задания на печать. Создаются Системой в результате обмена данных между сотрудниками организации и другими людьми, включая публикацию в общедоступных источниках, копирование на внешние устройства и печать.
Состояние доставки	Атрибут события, определяющий возможность доставки события получателям после анализа. Если доставка события была разрешена, то значение атрибута отражает состояние доставки (выполнена/не выполнена). См. также: Атрибуты события
Списки	Списки однотипных данных, создаваемые средствами Консоли управления, для использования при составлении политик. См. также: Конфигурация, Политика
Справочники персон, рабочих станций и групп	Данные о пользователях, рабочих станциях, а также группах персон и рабочих станций, импортированные из Active Directory, а также созданные средствами Консоли управления. Используются для удобства работы с информацией о событиях.
Статус	Характеристика персон и компьютеров, позволяющая разделять их по группам для удобства анализа и отслеживания активности, а также отображать в сводке и в отчетах с особой цветовой индикацией. См. также: Персоны, Компьютеры, Сводка, Отчет
Стоп-слово	Цифры, буквы и слова, нахождение которых в ячейках не приводит к срабатыванию этих ячеек. Стоп-слова используются для исключения ложноположительных срабатываний.
Тег	Текстовая метка, дающая краткую характеристику событию. См. также: Атрибуты события
Текст события	Текстовая информация, извлеченная из тела события и его вложений. Не содержит элементов форматирования или

Термин	Определение
	разметки. Используется для решения задач анализа и поиска. См. также: Событие, Тело события
Текстовые объекты	Технология, соотносящая данные из текста событий с заданными шаблонами (например, с правилами формирования номеров банковских карт). См. также: Технологии, Событие, Элемент технологий, Шаблон текстового объекта
Теневая копия документа	Копия документа, отправленного на печать с контролируемого компьютера. См. также: InfoWatch Device Monitor
Теневая копия файла	Копия файла, записываемого на съемное устройство. Создается только при успешном завершении операции сохранения файла на съемное устройство. См. также: InfoWatch Device Monitor
Термин	Один из набора слов и словосочетаний, в совокупности определяющих предметную область. См. также: Категория
Технологии	Набор инструментов анализа, выполняющих поиск заданных элементов в контексте событий и добавляющие событию атрибуты, характеризующие это событие. См. также: Элемент технологий, Контекст события, Категории, Термины, Эталонные документы, Бланки, Выгрузки из БД, Текстовые объекты, Графические объекты
Транспортный режим	Атрибут события, определяющий степень контроля доставки событий получателям. В сочетании с атрибутом "Вердикт" определяет возможность дальнейшей транспортировки события. См. также: Событие, Атрибуты события, Вердикт, Режим копии, Нормальный транспортный режим, Состояние доставки
Уведомление	Сообщение, отправляемое в случае срабатывания политики на событии. Отправляется средствами Консоли управления для уведомления пользователей Консоли управления, сотрудников или третьих лиц. Содержит краткую информацию о перехваченных событиях и сопроводительное сообщение. См. также: Политика, Событие
Уровень нарушения	Атрибут события, с помощью цветовой метки указывающий на степень угрозы для корпоративной политики безопасности. См. также: Событие, Атрибуты события, Нарушение

Термин	Определение
Учет регистра	Параметр термина: при учете регистра в анализируемом тексте будет выполняться поиск только тех словоформ, в которых есть полное соответствие с заглавными и строчными буквами, заданными в термине. См. также: Термин
Цитата	Отрывок эталонного документа, найденный в тексте события. См. также: Эталонный документ
Цитируемость	Показатель того, насколько полно эталонный документ присутствует в тексте анализируемого документа. См. также: Эталонный документ, Цитата
Цифровой отпечаток	Способ хранения эталонного документа в базе данных в виде набора цитат. См. также: Эталонный документ, Цитата
Шаблон текстового объекта	Унифицированное описание всех возможных текстовых объектов с типичной структурой: номера паспортов, кредитных карт, телефонные номера, код медицинского диагноза и т. д. См. также: Текстовые объекты
Элемент технологий	Составляющая настройки технологий, входящих в состав Системы. Пример конфиденциальных данных. К элементам технологий относятся: категории и термины, эталонные документы, бланки, выгрузки, текстовые объекты и графические объекты. См. также: Технологии, Категории, Термины, Эталонные документы, Бланки, Выгрузки из БД, Текстовые объекты, Графические объекты, Объект защиты.
Эталонная контрольная сумма	В отличие от текущей контрольной суммы, фиксирует образцовое состояние файлов Системы. См. также: Контроль целостности
Эталонные документы	Технология поиска цитат из конфиденциальных документов: например, образцы текстов приказов, финансовых отчетов, договоров и др. Эталонные документы хранятся в Системе в виде цифровых отпечатков, текст недоступен для просмотра ни пользователям, ни администраторам Системы. См. также: Технологии, Элемент технологий, Цифровой отпечаток, Цитата