

INFOWATCH

InfoWatch Device Monitor 4.2

Руководство пользователя

INFOWATCH DEVICE MONITOR 4.2

Руководство пользователя

© ЗАО “ИнфоВотч”
Тел. +7 (495) 229-00-22 • Факс +7 (495) 229-00-22
http://www.infowatch.com
Дата редакции: Октябрь 2014 года

Содержание

Часть I Общие сведения об InfoWatch Device Monitor 8

1.1 Функции InfoWatch Device Monitor 9

1.1.1 Работа при загрузке операционной системы в безопасном режиме 10

1.2 Схема работы InfoWatch Device Monitor 11

1.3 Принципы организации схемы безопасности 13

1.3.1 Политики безопасности и правила 13

1.3.2 Сотрудники и группы сотрудников 15

1.3.3 Рабочие станции и группы рабочих станций 15

1.3.4 Загрузка схемы безопасности на контролируемые рабочие станции 15

1.4 Глоссарий 16

Часть II Установка и настройка InfoWatch Device Monitor 20

2.1 Требования к аппаратному и программному обеспечению 21

2.1.1 База данных 21

2.1.2 Сервер InfoWatch Device Monitor 21

2.1.3 Клиент InfoWatch Device Monitor 22

2.1.4 Консоль управления 22

2.2 Установка серверной части InfoWatch Device Monitor 23

2.2.1 Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server 23

2.2.2 Рекомендации по развертыванию базы данных под управлением СУБД Oracle 24

2.2.2.1 Настройка параметров соединения InfoWatch Device Monitor с сервером СУБД Oracle 24

2.2.3 Рекомендации по установке Сервера InfoWatch Device Monitor 25

2.2.4 Порядок установки серверной части InfoWatch Device Monitor 26

2.3 Установка Клиента InfoWatch Device Monitor 31

2.3.1 Установка Клиента стандартным способом 31

2.3.2 Установка Клиента с помощью средств распространения программного обеспечения 32

2.4 Настройка Сервера InfoWatch Device Monitor 35

2.4.1 Раздел <applicationSettings> 35

2.4.2 Раздел <system.diagnostics> 38

2.5 Обновление InfoWatch Device Monitor 40

2.5.1 Обновление серверной части InfoWatch Device Monitor 41
2.5.2 Обновление Клиента InfoWatch Device Monitor 42
2.6 Удаление InfoWatch Device Monitor 42
2.6.1 Удаление Клиента, установленного с помощью средств распространения программного обеспечения
Часть III Работа в Консоли Управления 43
3.1 Начало работы с Консолью управления 44
3.1.1 Авторизация и соединение с сервером InfoWatch Device Monitor 44
3.1.2 Главное окно Консоли управления 46
3.1.2.1 Настройка элементов главного окна Консоли управления 47
3.1.3 Разделы Консоли управления 47
3.2 Администрирование учетных записей Консоли управления 48
3.2.1 Просмотр сведений об учетных записях Консоли управления 50
3.2.2 Добавление учетной записи Консоли управления 51
3.2.3 Блокирование и разблокирование учетной записи Консоли управления 52
3.2.4 Редактирование учетной записи Консоли управления 52
3.2.5 Удаление учетной записи Консоли управления 52
3.2.6 Аудит действий по управлению схемой безопасности в Консоли управления 53
3.2.6.1 Просмотр журнала аудита 53
3.2.6.1.1Значения параметра Селектор 55
3.2.6.2 Фильтрация записей в журнале аудита 56
3.2.6.2.1Вкладка Дата и номер записи 58
3.2.6.2.2Вкладка Объект и действие 58
3.2.6.2.3Вкладка Дополнительно 59
3.2.6.3 Удаление записей из журнала аудита 59
3.2.6.4 Экспорт записей журнала аудита 59
3.2.6.5 Анализ журнала аудита в Microsoft Excel 60
3.3 Общие настройки Системы 60
3.3.1 Общие настройки работы Клиентов 61
3.3.2 Контроль сетевых соединений 62
3.3.3 Контроль сетевого трафика 65
3.3.4 Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor 67
3.3.5 Соединение с сервером LDAP 68

3.3.6 Настройка уведомлений сотрудников о нарушении правил 68
3.4 Управление схемой безопасности 70
3.4.1 Общие принципы работы со схемой безопасности 71
3.4.1.1 Просмотр действующей версии схемы безопасности 71
3.4.1.2 Просмотр предыдущих версий схемы безопасности 72
3.4.1.3 Комментарии к схеме безопасности 73
3.4.1.4 Редактирование схемы безопасности 73
3.4.1.4.1Блокировка схемы безопасности 74
3.4.1.5 Обновление схемы безопасности 75
3.4.1.6 Экспорт/импорт схемы безопасности 76
3.4.2 Настройка схемы безопасности 76
3.4.2.1 Политики безопасности 77
3.4.2.1.1Просмотр политик безопасности 77
3.4.2.1.2Создание и настройка политики безопасности 79
3.4.2.1.3Редактирование политики безопасности 81
3.4.2.1.4Удаление политики безопасности 81
3.4.2.2 Правила 82
3.4.2.2.1Применение правил 82
3.4.2.2.1.1 Особенности применения правил для Device Monitor 83
3.4.2.2.1.2 Работа при нехватке рабочего пространства 85
3.4.2.2.2Добавление правила 86
3.4.2.2.2.1 Настройка правила для File Monitor 86
3.4.2.2.2.2 Настройка правила для Print Monitor 89
3.4.2.2.2.3 Настройка правила для Device Monitor 90
3.4.2.2.2.4 Настройка правила для IM Client Monitor 93
3.4.2.2.2.5 Настройка правила для FTP Monitor 95
3.4.2.2.2.6 Настройка правила для HTTPS Monitor 97
3.4.2.2.2.7 Настройка правила для Network Monitor 98
3.4.2.2.3Редактирование правила 99
3.4.2.2.4Удаление правила 100
3.4.2.2.5Копирование правил 100
3.4.2.3 Сотрудники 101

3.4.2.3.1Просмотр сведений о сотрудниках и группах 101
3.4.2.3.2Создание и редактирование группы сотрудников 102
3.4.2.3.3Удаление группы сотрудников 104
3.4.2.3.4Добавление учетной записи сотрудника в группу 104
3.4.2.3.5Редактирование учетной записи сотрудника 105
3.4.2.3.6Исключение учетной записи сотрудника из группы 106
3.4.2.3.7Удаление учетной записи из схемы безопасности 107
3.4.2.4 Рабочие станции 107
3.4.2.4.1Просмотр сведений о рабочих станциях 108
3.4.2.4.2Просмотр эффективной политики на рабочей станции 109
3.4.2.4.3Создание и редактирование группы рабочих станций 110
3.4.2.4.4Удаление группы рабочих станций 111
3.4.2.4.5Добавление рабочей станции в группу 112
3.4.2.4.6Исключение рабочей станции из группы 113
3.4.2.4.7Удаление рабочей станции из схемы безопасности 114
3.4.2.4.8Обновление Клиентов на рабочих станциях 114
3.4.2.5 Белые списки 115
3.4.2.5.1Просмотр сведений о белых списках 115
3.4.2.5.2Добавление белого списка 116
3.4.2.5.2.1 Добавление записи об устройстве 118
3.4.2.5.2.2 Удаление записи об устройстве 119
3.4.2.5.3Установка периода действия записи 119
3.4.2.5.4Редактирование белого списка 120
3.4.2.5.5Удаление белого списка 121
3.4.2.6 Категории сигнатур 121
3.4.2.6.1Создание категории сигнатур 122
3.4.2.6.2Изменение категории сигнатур 123
3.4.2.6.3Удаление категории сигнатур 123
3.4.3 Предоставление сотруднику временного доступа 124
3.5 Просмотр событий 124
3.5.1 Фильтры событий 129
3.5.2 Удаление событий 130

3.6 Удаленная установка, обновление и удаление Клиентов 131
3.6.1 Просмотр задач 132
3.6.2 Подготовка к первичной установке Клиентов. Агент распространения 134
3.6.2.1 Включение административных разделяемых ресурсов 134
3.6.2.2 Настройки брандмауэра 135
3.6.3 Создание задачи первичного распространения 135
3.6.4 Создание задачи обновления 138
3.6.5 Создание задачи смены пароля деинсталляции 139
3.6.6 Создание задачи удаления 139
3.6.7 Запуск, остановка, редактирование и удаление задачи 140
3.6.8 Ошибки установки Клиентов 141
3.6.9 Создание пакета установки 142
3.7 Дополнительные возможности 144
3.7.1 Фильтрация табличных данных 144
3.7.1.1 Фильтрация по дате 144
3.7.1.2 Использование стандартных фильтров 145
3.7.1.3 Пользовательский фильтр 145
3.7.1.4 Редактирование фильтра 147
3.7.1.5 Отмена фильтра 147
3.7.2 Группирование и сортировка записей 148
3.7.3 Клавиши быстрого доступа 148

Часть IV Разрешение проблем 151

4.1 Просмотр сообщений сервера 152

Часть V Лицензионная информация 156

5.1 WiX Common Public License 157
5.2 Пользовательское лицензионное соглашение InfoWatch Device Monitor 159

1 Общие сведения об InfoWatch Device Monitor

InfoWatch Device Monitor (далее InfoWatch Device Monitor или Система) – это система, позволяющая контролировать доступ к периферийным устройствам компьютерной системы. Кроме того, в Системе имеется возможность проводить мониторинг информации, переносимой с рабочих станций на съемные устройства, передаваемой по сети или отправляемой на печать. Данные мониторинга передаются для анализа в систему InfoWatch Traffic Monitor.

Основные разделы руководства:

- Установка и настройка InfoWatch Device Monitor. Порядок установки, настройки, обновления и удаления InfoWatch Device Monitor.
- Работа в Консоли управления. Эксплуатация Системы: администрирование учетных записей сотрудников, работающих с InfoWatch Device Monitor; управление схемой безопасности; удаленная установка клиентских приложений.
- Разрешение проблем. Описание проблем, которые могут возникнуть в процессе эксплуатации InfoWatch Device Monitor, и способы их решения.
- Пользовательское лицензионное соглашение. Текст лицензии на использование Системы и ее компонентов.

Для получения общего представления о принципах работы Системы рекомендуется ознакомиться со следующими вводными разделами:

- Функции InfoWatch Device Monitor. Описание функциональных возможностей InfoWatch Device Monitor.
- Схема работы InfoWatch Device Monitor. Схема и описание принципа работы InfoWatch Device Monitor и его компонентов.
- Принципы организации схемы безопасности. Описание реализации схемы безопасности, в соответствии с которой осуществляется контроль InfoWatch Device Monitor, введение базовых понятий, необходимых при работе с Системой.
- Глоссарий. Список терминов, используемых в документации и интерфейсе программы, с определениями.

При возникновении проблем и вопросов, связанных с работой продукта, вы можете обратиться в службу технической поддержки:

- Если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера.
- Если продукт приобретен у компании InfoWatch напрямую, то вы можете обратиться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.
- Часы работы Службы технической поддержки – с 7-00 до 21-00 с понедельника по пятницу по московскому времени, исключая официальные выходные и праздничные дни в РФ.

Вы также можете посетить раздел технической поддержки на нашем сайте: http://www.infowatch.ru/support.html.

1.1 Функции InfoWatch Device Monitor

Основные функции системы InfoWatch Device Monitor:

- мониторинг контролируемых рабочих станций в режиме реального времени;
- контроль доступа сотрудников к периферийным устройствам компьютерной системы;
- мониторинг печати на контролируемых рабочих станциях;
- контроль систем мгновенного обмена сообщениями: Skype, Jabber (протокол XMPP) и Mail.Ru Агент (протокол MMP);
- контроль трафика, передаваемого по протоколу FTP;
- контроль трафика, передаваемого по протоколу HTTPS;
- контроль передачи данных по сетевым соединениям вне корпоративной сети;
- сбор данных, полученных от контролируемых рабочих станций;
- передача полученных данных в систему InfoWatch Traffic Monitor для анализа.

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 рабочих станциях. ***Контролируемые рабочие станции*** – это рабочие места сотрудников, через которые может быть осуществлен доступ к контролируемым файлам,контролируемым периферийным устройствам и сетевым ресурсам.

Контролируемые файлы – это файлы, за доступом к которым необходимо вести наблюдение согласно требованиям корпоративной политики безопасности.

Контролируемые периферийные устройства – это те устройства компьютерной системы, доступ к которым контролируется InfoWatch Device Monitor.

Для осуществления функций мониторинга и контроля на контролируемые рабочие станции устанавливаются клиентские модули Системы. В состав клиентского модуля входят перехватчики: **File Monitor**, **Print Monitor, Device Monitor**, **IM Client Monitor, FTP Monitor, HTTPS Monitor** и **Network Monitor**.

File Monitor позволяет отслеживать операции записи в файл на съемном устройстве, причем регистрируется факт успешного завершения операции. Это дает возможность отслеживать такие действия сотрудников, как:

- создание/редактирование файла непосредственно на съемном устройстве;
- копирование/перемещение файла на съемное устройство. В данном случае отслеживаются операции копирования/перемещения файла с контролируемой рабочей станции, другого съемного устройства или сетевых ресурсов.

Подробнее о порядке настройки правила, определяющего работу перехватчика, см. "Настройка правила для File Monitor".

Device Monitor предназначен для контроля доступа сотрудников к периферийным устройствам компьютерной системы. Возможности степени ограничения доступа на выполнение операций с периферийными устройствами зависят от типа устройства.

Подробнее о порядке настройки правила, определяющего работу перехватчика, см. "Настройка правила для Device Monitor".

Print Monitor позволяет осуществлять мониторинг операций, связанных с печатью документов на локальных и сетевых принтерах. При контроле печати документов, отправляемых на печать, создаётся копия задания на печать и передается в InfoWatch Traffic Monitor на анализ. Подробнее см. "Настройка правила для Print Monitor"

IM Client Monitor позволяет контролировать доступ сотрудников к системам мгновенного обмена сообщениями Skype, Jabber (протокол XMPP) и Mail.Ru Агент (протокол MMP). Система позволяет полностью запрещать использование приложения, либо только снимать копию чата. Также возможно создавать теневые копии передаваемых файлов и сообщений. Подробнее см. "Контроль сетевого трафика" и "Настройка правила для IM Client Monitor"

FTP Monitor позволяет контролировать обмен данными через протокол FTP. Система позволяет ограничивать или полностью запрещать использование FTP протокола, а также создавать теневые копии передаваемых файлов. Подробнее см. "Настройка правила для FTP Monitor"

Network Monitor позволяет запрещать передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами. Подробнее см. "Контроль сетевых соединений" и "Настройка правила для Network Monitor"

Все создаваемые теневые копии не хранятся в InfoWatch Device Monitor, а передаются в InfoWatch Traffic Monitor на анализ

1.1.1 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.

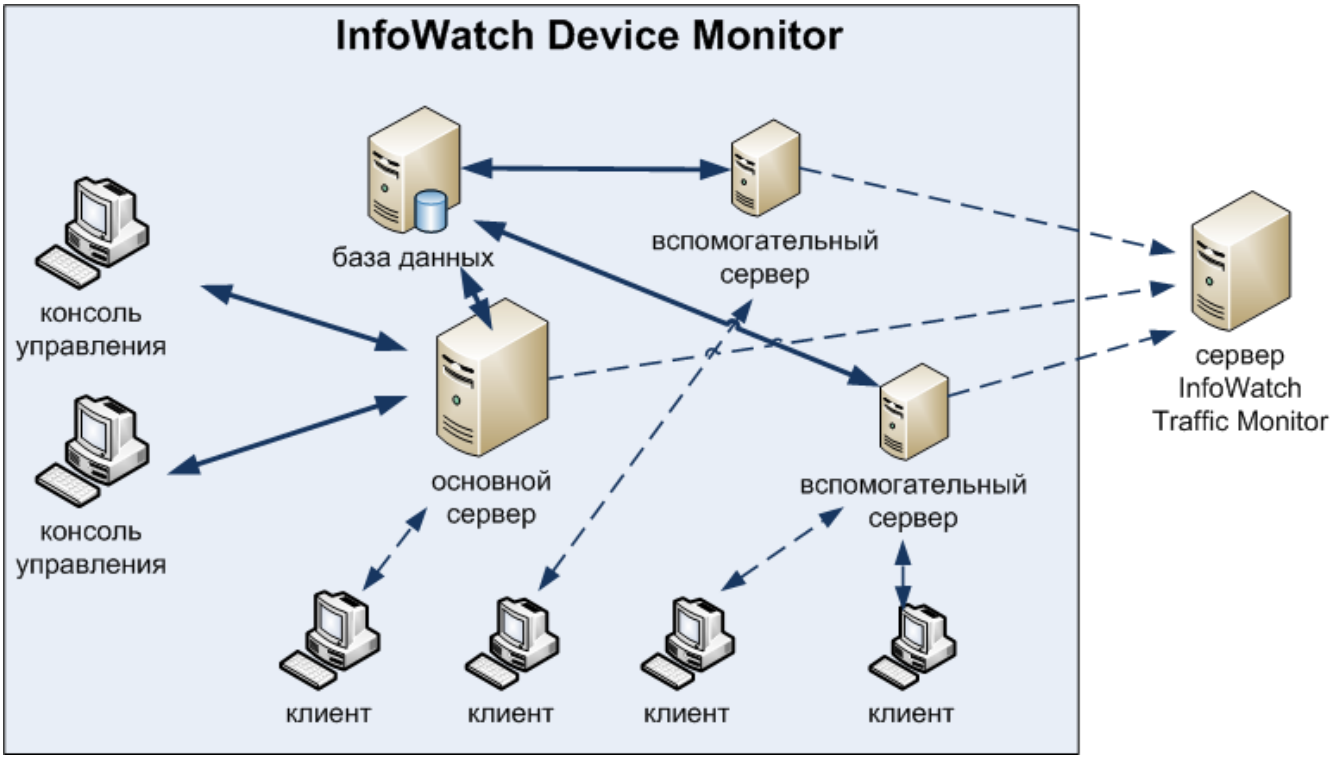
Функция InfoWatch Device Monitor	Режим работы операционной системы
Контроль доступа к периферийным устройствам (исключение составляют устройства, доступ к которым в безопасном режиме запрещен операционной системой)	Безопасный режим (Safe Mode) Безопасный режим с поддержкой сети (Safe Mode with Networking)
Контроль записи информации в файлы на съемных устройствах	Безопасный режим (Safe Mode) Безопасный режим с поддержкой сети (Safe Mode with Networking)
Мониторинг контролируемых рабочих станций	Безопасный режим с поддержкой сети (Safe Mode with Networking)
Контроль сетевой активности (Skype)	Безопасный режим с поддержкой сети (Safe Mode with Networking)
Контроль трафика, передаваемого по протоколу FTP	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)

1.2 Схема работы InfoWatch Device Monitor

Компоненты, входящие в состав InfoWatch Device Monitor, перечислены в следующей таблице.

Компонент	Назначение
InfoWatch Device Monitor Client (клиентское приложение InfoWatch Device Monitor, Клиент)	Перехват действий сотрудников на контролируемых рабочих станциях
InfoWatch Device Monitor Server (сервер InfoWatch Device Monitor, Сервер)	Конфигурирование клиентских приложений, сбор данных от клиентских приложений и передача этих данных системе InfoWatch Traffic Monitor
InfoWatch Device Monitor Database (база данных)	Хранение информации, необходимой для работы Системы
Консоль управления InfoWatch Device Monitor (Консоль управления)	Управление Системой

На следующем рисунке показан принцип работы Системы.



Система разворачивается и работает следующим образом:

1. Первым устанавливают **основной сервер**.
2. При установке основного сервера определяют используемый сервер **базы данных**: СУБД может располагаться как отдельно, так и на том же компьютере, что и основной сервер.
3. При установке основного сервера создается **схема базы данных**, где будет храниться **схема безопасности** и другие параметры Системы.
4. При необходимости, можно установить **вспомогательные сервера**, которые будут обеспечивать балансировку нагрузки в Системе.
5. **Консоль управления** может устанавливаться на любой компьютер, и подключаться к основному

серверу. С Консоли управления выполняется настройка схемы безопасности в соответствии с требованиями корпоративной политики безопасности.

6. На **рабочие станции** устанавливаются **Клиенты Device Monitor**. Они выполняют подключение к любому доступному серверу Device Monitor, обеспечивают реализацию и обновление схемы безопасности, а также получение теневых копий и их отправку на сервер Device Monitor.
7. Сервера Device Monitor получают из базы данных обновленные версии схемы безопасности и распространяют их на контролируемые рабочие станции. С контролируемых рабочих станций на сервер передается информация о событиях, подпадающих под правила схемы безопасности, а также теневые копии файлов. Информация о событиях передаётся в базу данных. Теневые копии передаются в систему InfoWatch Traffic Monitor.

Пример 1

1. Сотрудник, работающий на контролируемой рабочей станции, обращается к контролируемому периферийному устройству (например, дает команду распечатать документ через USB принтер).
2. Клиент проверяет, имеет ли сотрудник право на работу с периферийным устройством. Если такого разрешения нет, то сотруднику будет отказано в доступе к устройству (в рассматриваемом случае документ не будет отправлен на печать).

Печать документов на локальных и сетевых принтерах отслеживается перехватчиком Print Monitor. Копия задания на печать передаётся в InfoWatch Traffic Monitor для анализа. Отправка документов на печать возможна при условии, что сотруднику разрешен доступ к принтеру (проверяется перехватчиком Device Monitor).

Пример 2

В Системе задано правило, отслеживающее запись в PDF-файл на съемном устройстве. В правиле указано, что при выполнении этой операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к записи в файл на съемном устройстве (например, копирует файл на USB Flash Drive).
2. Если операция записи в файл на съемном устройстве успешно завершена, то Клиент InfoWatch Device Monitor генерирует событие и создает теневую копию файла.
3. Если создать теневую копию файла невозможно (например, при отсутствии свободного места на жестком диске), операция записи в файл на съемном устройстве будет произведена без создания теневой копии, о чём будет указано в информации о событии.
4. Клиент передает данные (событие и теневую копию файла) на Сервер InfoWatch Device Monitor. Если соединение с Сервером отсутствует, то данные сохраняются на контролируемой рабочей станции. После восстановления связи данные будут доставлены на Сервер.
5. Сервер отправляет данные в систему InfoWatch Traffic Monitor для анализа. Если соединение с сервером InfoWatch Traffic Monitor отсутствует, то данные сохраняются на рабочей станции. После восстановления связи данные будут доставлены в систему InfoWatch Traffic Monitor.

Попытки записи в файлы на съемных устройствах отслеживаются перехватчиком File Monitor. Полученные сведения передаются затем в InfoWatch Traffic Monitor для анализа. В то же время доступ к съемному устройству контролируется перехватчиком Device Monitor. Поэтому сотрудник может выполнять операцию записи в файл только на тех съемных устройствах, к которым у него есть доступ.

Пример 3

В Системе задано правило, отслеживающее печать DOC-файлов. В правиле указано, что при выполнении подобной операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к отправке документа на печать.
2. Если задание на печать сформировано успешно, то Клиент InfoWatch Device Monitor генерирует событие и создает теневую копию документа, отправленного на печать.
3. В случае если создать теневую копию документа невозможно (например, при отсутствии свободного места на жестком диске), операция печати будет произведена без создания теневой копии, о чём будет указано в информации о событии.
4. Клиент передает данные (событие и теневую копию документа) на Сервер InfoWatch Device Monitor. Если соединение с Сервером отсутствует, то данные сохраняются на контролируемой рабочей станции. После восстановления связи данные будут доставлены на Сервер.
5. Сервер отправляет данные в систему InfoWatch Traffic Monitor для анализа. Если соединение с

сервером InfoWatch Traffic Monitor отсутствует, то данные сохраняются в базе данных. После восстановления связи данные будут доставлены в систему InfoWatch Traffic Monitor.

1.3 Принципы организации 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 рабочих станций**. Каждой группе рабочих станций 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 рабочих станций и учетных записей сотрудников, которым не назначена политика безопасности, предусмотрены: группа сотрудников «по умолчанию» и группа рабочих станций «по умолчанию».

В процессе работы схема безопасности может неоднократно редактироваться. Причем 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 можно просмотреть любую версию схемы безопасности.

Далее в подразделе содержится следующая информация:

- Политики безопасности и правила
- Сотрудники и группы сотрудников
- Рабочие станции и группы рабочих станций
- Загрузка схемы безопасности на контролируемые рабочие станции

1.3.1 Политики безопасности и правила

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

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

- Каждой группе сотрудников и каждой группе рабочих станций обязательно должна быть назначена политика безопасности.

  Добавление новой группы сотрудников или новой группы рабочих станций невозможно, если для данной группы не определена политика безопасности. В процессе назначения политики безопасности группе сотрудников или группе рабочих станций выбор осуществляется из ранее созданных политик безопасности. Поэтому нужная политика безопасности должна быть создана перед добавлением соответствующей группы.

- Группе сотрудников или группе рабочих станций не может быть назначено более одной политики безопасности.
- Одна и та же политика безопасности может быть назначена нескольким группам сотрудников или группам рабочих станций, однако рекомендуется, чтобы каждой группе сотрудников и группе рабочих станций была назначена своя политика безопасности.

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

Уровень доступа сотрудника к контролируемым файлам и устройствам определяется двумя составляющими, а именно, политиками безопасности, назначенными:

- группам сотрудников, в состав которых включен данный сотрудник;
- группам рабочих станций, в которые включена та рабочая станция, на которой работает сотрудник.

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 рабочих станций, в состав которых включена рабочая станция, на которой работает данный сотрудник. Впоследствии можно изменять уровень доступа путем включения сотрудника в различные группы сотрудников.

Правила – это набор ограничений и условий, в соответствии с которыми осуществляется мониторинг операций, связанных с переносом файлов на съемные устройства, 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 Системе существуют следующие типы правил:

- **Правило для File Monitor**. Позволяет отслеживать действия, связанные с переносом и изменением файлов на съемных устройствах. Правило можно настроить таким образом, чтобы при сохранении файла на съемном устройстве создавалась теневая копия этого файла, которая затем передается в InfoWatch Traffic Monitor на анализ.
- **Правило для Device Monitor**. Позволяет контролировать доступ сотрудников к выбранному типу периферийных устройств.
- **Правило для Print Monitor**. Позволяет отслеживать действия, связанные с выводом документов на печать. Правило можно настроить таким образом, чтобы при печати документов создавалась теневая копия, которая затем передается в InfoWatch Traffic Monitor на анализ.
- **Правило для IM Client Monitor**. Позволяет контролировать доступ сотрудников к системам мгновенного обмена сообщениями Skype, Jabber (протокол XMPP) и Mail.Ru Агент (протокол MMP). С помощью правил можно полностью запрещать использование приложений, или только снимать копию сообщений, а также создавать теневые копии передаваемых файлов. Теневые копии файлов и сообщений не хранятся в InfoWatch Device Monitor, а передаются в InfoWatch Traffic Monitor на анализ.
- **Правило для FTP Monitor**. Позволяет контролировать обмен данными через протокол FTP. Возможен полный либо частичный запрет на использование FTP-протокола: например, можно разрешить только скачивать файлы с использованием FTP-протокола. также возможно , передаваемых в InfoWatch Traffic Monitor на анализ.
- **HTTPS Monitor** позволяет контролировать обмен данными через протокол HTTPS. Система позволяет создавать теневые копии запросов, передаваемых в InfoWatch Traffic Monitor на анализ
- **Правило для Network Monitor**. Позволяет запрещать передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами. В системе доступна глобальная настройка параметров того, какие сегменты сети считаются корпоративной сетью, и какие внешние адреса разрешены.

1.3.2 Сотрудники и группы сотрудников

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

- Каждый сотрудник должен быть включен как минимум в одну группу сотрудников (группу «по умолчанию»). Это связано с тем, что политика безопасности назначается только группе сотрудников.

  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.
  - **Теневое копирование печати**. Правило Print Monitor, задающее создание теневых копий всех заданий на печать.
  - **Контроль Skype**, **Контроль XMPP**, **Контроль MMP**. Правила IM Client Monitor, разрешающее использование соответствующих мессенджеров, но задающее создание теневых копий для всех сообщений и чатов, а также исходящих файлов.
  - **Контроль FTP**. Правило FTP Monitor, разрешающее использование протокола FTP, но задающее создание теневых копий для всех файлов, отправляемых с использованием этого протокола.

1.3.3 Рабочие станции и группы рабочих станций

Рабочая станция, зарегистрированная в Device Monitor, должна быть включена как минимум в одну группу рабочих станций (группу «по умолчанию»). Это связано с тем, что политика безопасности назначается только группе рабочих станций.

В группу «по умолчанию» входят все рабочие станции, для которых не определены другие группы рабочих станций (рабочие станции, впервые зарегистрированные в Device Monitor; рабочие станции, исключенные из всех прочих групп рабочих станций). После установки Системы группе рабочих станций «по умолчанию» назначена *Политика на устройства*. Эта политика не содержит ни одного правила.

Исключить рабочую станцию из группы «по умолчанию» можно при условии, что рабочая станция добавлена хотя бы в одну группу рабочих станций, помимо группы «по умолчанию».

1.3.4 Загрузка схемы безопасности на контролируемые рабочие станции

Схема безопасности, загруженная на контролируемые рабочие станции, должна находиться в актуальном состоянии. Это обеспечивается взаимодействием Сервера и Клиентов, установленных на контролируемых рабочих станциях.

Процесс передачи схемы безопасности на контролируемые рабочие станции 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 контролируемой рабочей станции 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 контролируемой рабочей станции с сервером InfoWatch Device Monitor, на ней будут актуализированы политики, а сохраненные теневые копии будут переданы на сервер.

1.4 Глоссарий

Термин	Определение
Device Monitor	Один из перехватчиков, входящих в состав клиентского модуля InfoWatch Device Monitor. Предназначен для контроля доступа сотрудников к периферийным устройствам компьютерной системы. См. также: *Перехватчик*
File Monitor	Один из перехватчиков, входящих в состав клиентского модуля InfoWatch Device Monitor. Предназначен для наблюдения за действиями сотрудников, создающих файлы на съемных носителях. См. также: *Перехватчик*
FTP Monitor	Один из перехватчиков, входящих в состав клиентского модуля InfoWatch Device Monitor. Предназначен для контроля обмена данными через протокол FTP. См. также: *Перехватчик*
HTTPS Monitor	Один из перехватчиков, входящих в состав клиентского модуля InfoWatch Device Monitor. Предназначен для контроля обмена данными через протокол HTTPS. См. также: *Перехватчик*
IM Client Monitor	Один из перехватчиков, входящих в состав клиентского модуля InfoWatch Device Monitor. Предназначен для наблюдения за сетевой активностью сотрудника, использующего системы мгновенного обмена сообщениями. См. также: *Перехватчик*
InfoWatch Device Monitor	Система, предназначенная для контроля доступа сотрудников к периферийным устройствам, мониторинга операций по созданию файлов на съемных устройствах, сетевой активности и отправке документов на печать
InfoWatch Traffic Monitor	Система для контроля над различными видами трафика (SMTP, HTTP, ICQ и Lotus Notes). Также в InfoWatch Traffic Monitor осуществляется анализ теневых копий файлов, полученных от системы InfoWatch Device Monitor
Network Monitor	Один из перехватчиков, входящих в состав клиентского модуля InfoWatch Device Monitor. Предназначен для ограничения передачи данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами. См. также: *Перехватчик*
Print Monitor	Один из перехватчиков, входящих в состав клиентского модуля InfoWatch Device Monitor. Предназначен для наблюдения за действиями, связанными с отправкой документов на печать. См. также: *Перехватчик*
Аудит действий сотрудников Консоли управления	Контроль действий, выполняемых с помощью Консоли управления. Система аудита позволяет отслеживать процесс создания и управления схемой безопасности (т.е. все действия, результатом которых является изменения схемы безопасности), действия, связанные с администрированием Системы. См. также: *Журнал аудита*, *Учетные записи Консоли управления*
Белый список	Список устройств, доступ к которым безусловно разрешен. См. также: *Политика безопасности*
База данных	См.: *База данных InfoWatch Device Monitor*

База данных InfoWatch Device Monitor	База данных, в которой хранится вся информация, необходимая для работы системы InfoWatch Device Monitor
Группа сотрудников	Один из параметров схемы безопасности. В состав группы включают тех сотрудников, которым, в соответствии с требованиями корпоративной политики безопасности, требуется назначить одинаковую политику безопасности. См. также: *Группа сотрудников «по умолчанию»*, *Политика безопасности*, *Уровень доступа сотрудника*
Группа сотрудников «по умолчанию»	Группа сотрудников, добавляемая автоматически при создании новой схемы безопасности. В эту группу включаются учетные записи всех сотрудников, для которых не определены другие группы сотрудников (при добавлении нового сотрудника, при исключении сотрудника из всех других групп). См. также: *Группа сотрудников*, *Политика безопасности*
Группа рабочих станций	Один из параметров схемы безопасности. В состав группы включают рабочие станции, которым требуется назначить одинаковую политику безопасности. Распределение рабочих станций по группам осуществляется в соответствии с требованиями корпоративной политики безопасности. См. также: *Группа сотрудников «по умолчанию»*, *Политика безопасности*, *Уровень доступа сотрудника*
Группа рабочих станций «по умолчанию»	Группа рабочих станций, добавляемая автоматически при создании новой схемы безопасности. В данную группу включаются рабочие станции, которые не входят в другие группы рабочих станции (при регистрации новой рабочей станции, при исключении рабочей станции из всех других групп). См. также: *Группа сотрудников*, *Политика безопасности*
Журнал аудита	Журнал, в котором содержатся записи о действиях, выполняемых пользователями Консоли управления в процессе управления Системой. См. также: *Аудит действий сотрудников*, *Пользователь Консоли управления*
Клиент	См.: *Клиент InfoWatch Device Monitor*
Клиент InfoWatch Device Monitor	Клиентский модуль InfoWatch Device Monitor. Предназначен для контроля за действиями сотрудников на рабочих станциях
Консоль управления	См.: *Консоль управления InfoWatch Device Monitor*
Консоль управления InfoWatch Device Monitor	Компонент графического пользовательского интерфейса. Предназначен для управления системой InfoWatch Device Monitor (администрирование Системы, настройка схемы безопасности и пр.).
Контролируемая рабочая станция	Рабочие места сотрудников, через которые может быть осуществлен доступ к контролируемым файлам и периферийным устройствам компьютерной системы
Контролируемое периферийное устройство	Периферийные устройства компьютерной системы (принтеры, сканеры, накопители информации и пр.), доступ к которым контролируется InfoWatch Device Monitor. Контроль доступа к периферийным устройствам осуществляется в соответствии с правилами корпоративной политики безопасности

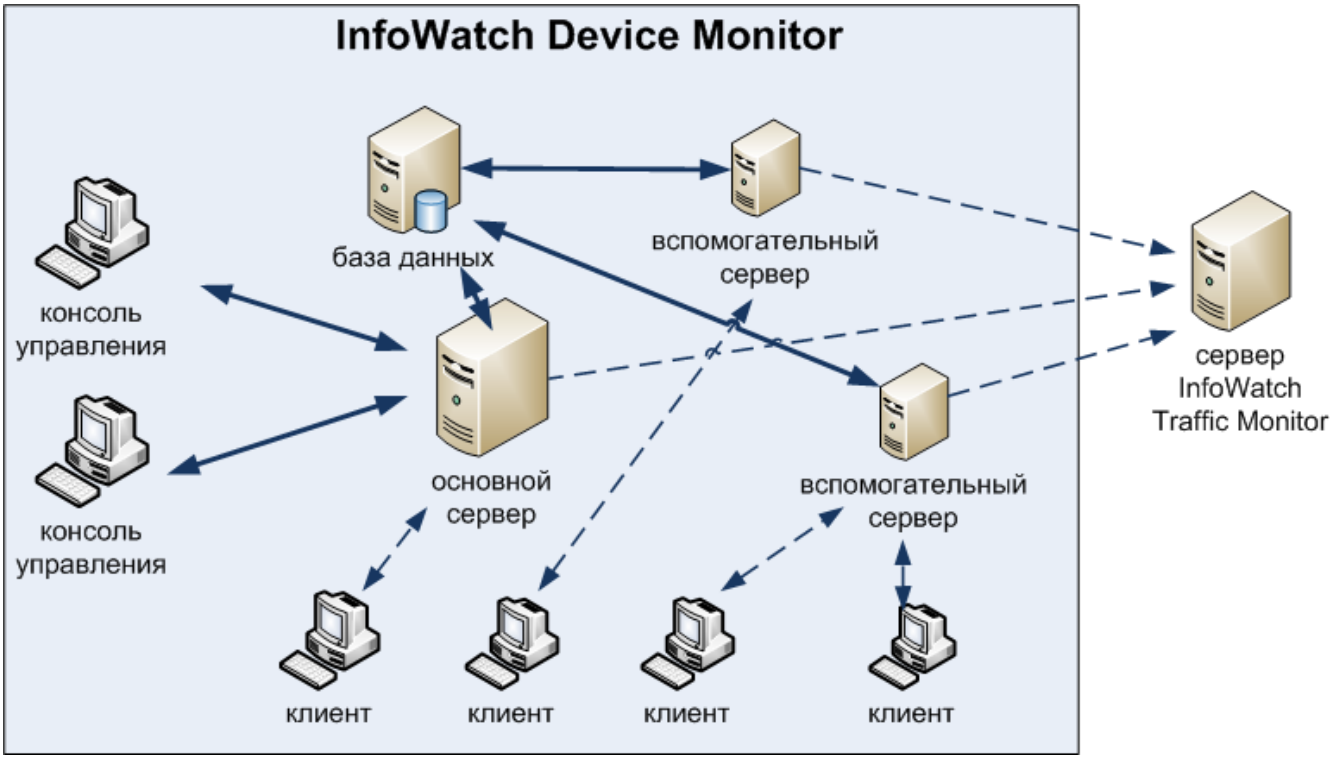
Контролируемый файл	Файл, доступ к которому отслеживается системой InfoWatch Device Monitor. Список контролируемых файлов определяется на основании требований корпоративной политики безопасности
Контроль доступа к периферийным устройствам	Разграничение прав на работу с периферийными устройствами компьютерной системы. Определение уровня доступа к различным типам периферийных устройств выполняется в соответствии с требованиями корпоративной политики безопасности. Для разных групп сотрудников и групп рабочих станций может быть настроен разный уровень доступа к тому или иному периферийному устройству
Локальный администратор	Роль, в задачи которой входит управление учетными записями Консоли управления.
Маска файла	Шаблон для поиска файла, соответствующего заданным критериям. В системе InfoWatch Device Monitor маска файла может применяться при составлении правил для File Monitor и Print Monitor
Офицер безопасности	Роль, предназначенная для управления политикой безопасности на контролируемых рабочих станциях, настройки соединения с сервером InfoWatch Traffic Monitor
Перехватчик	Компонент, входящий в состав клиентского модуля. Обеспечивает контроль действий сотрудников в соответствии с настройками схемы безопасности. В состав клиентского модуля входят перехватчики: File Monitor, Print Monitor, Device Monitor, IM Client Monitor, FTP Monitor, HTTPS Monitor, Network Monitor. См. также: *File Monitor*, *Device Monitor*, *Print Monitor*, *IM Client Monitor, FTP Monitor, HTTPS Monitor, Network Monitor*.
Политика безопасности	Один из параметров схемы безопасности. Набор 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. Политика безопасности может быть назначена только группе (сотрудников или рабочих станций). Степень контроля за действиями каждого сотрудника определяется уровнем доступа. См. также: *Схема безопасности*, *Уровень доступа*
Сотрудник	Любой пользователь, зарегистрированный в системе InfoWatch Device Monitor как сотрудник. Действия сотрудников контролируются клиентскими модулями, установленными на рабочих станциях.
Пользователь Консоли управления	Пользователь, в задачи которого входит выполнение различных функций по управлению системой InfoWatch Device Monitor. Каждому пользователю назначается роль в соответствии с требованиями корпоративной политики безопасности.
Правило	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 безопасности*
Рабочая станция	В терминах системы InfoWatch Device Monitor под рабочей станцией подразумевается контролируемая рабочая станция. См.: *Контролируемая рабочая станция*

Рендеринг задания печати	Процесс визуализации, в результате которого задание печати преобразуется в данные, которые могут быть выведены на печать принтером.
Селектор	Постоянный атрибут записи журнала аудита. Содержит инструкции для поиска объекта, над которым совершено действие. Значение параметра Селектор зависит от конкретного объекта и действий, выполняемых над этим объектом. См. также: *Журнал аудита*
Сервер	См.: *Сервер InfoWatch Device Monitor*
Сервер InfoWatch Device Monitor	Серверный модуль InfoWatch Device Monitor. Предназначен для управления контролируемыми рабочими станциями, а также для взаимодействия с InfoWatch Traffic Monitor.
СУБД	Система управления базами данных.
Суперпользователь	Роль Консоли управления, обладающая полным набором привилегий на управление системой InfoWatch Device Monitor. Назначение данной роли - настройка Консоли управления после установки; работа в аварийных условиях; удаление записей из журнала аудита.
Схема безопасности	Набор конфигурационных параметров, в соответствии с которыми ведется наблюдение и контроль за действиями сотрудников, контролируемых системой InfoWatch Device Monitor. См. также: *Группа сотрудников*, *Группа рабочих станций*, *Политика безопасности*
Теневая копия документа	Копия документа, отправленного на печать.
Теневая копия файла	Копия файла, записываемого на съемное устройство. Создается только при успешном завершении операции сохранения файла на съемное устройство. Анализ теневых копий файлов выполняется в системе InfoWatch Traffic Monitor.
Транзакция	Обязательный атрибут записи журнала аудита. Состоит из одного или нескольких элементарных действий (шагов). Транзакция считается завершенной только в том случае, если выполнены все, входящие в нее действия. В противном случае транзакция считается незавершенной, и Система возвращается к состоянию, имевшему место до выполнения транзакции.
Уровень доступа сотрудника	Совокупность политик безопасности, действие которых распространяется на данного сотрудника. А именно, политик безопасности назначенных: • группам сотрудников, в состав которых входит данный сотрудник; • группам рабочих станций, в которых зарегистрирована рабочая станция, используемая для выполнения контролируемых действий.
Учетная запись Windows	Учетная запись, от имени которой пользователь зарегистрирован в операционной системе Microsoft Windows. Данные учетной записи используются при регистрации сотрудник в системе InfoWatch Device Monitor.
Шаг транзакции	Элементарное действие, совершаемое в рамках одной транзакции (например, транзакция, результатом выполнения которой является включение сотрудника в группу сотрудников, содержит единственный шаг – включение сотрудника в группу).

2 Установка и настройка InfoWatch Device Monitor

Данный раздел содержит информацию по установке и настройке InfoWatch Device Monitor, рассчитанную на пользователей, знакомых с основами администрирования операционной системы Microsoft Windows, а также используемой СУБД.

На следующем рисунке показан пример развертывания Системы.



Пример развертывания InfoWatch Device Monitor

Для повышения производительности Системы, можно использовать кластеризацию. При этом одна схема базы данных будет использоваться несколькими серверами для хранения и распространения общей схемы безопасности.

Сервер и база данных могут находиться на одном компьютере. Однако для увеличения производительности Системы рекомендуется размещать базу данных и сервер на разных компьютерах.

Консоль управления может подключаться только к основному серверу. Используя Консоль управления можно управлять всеми серверами в кластере.

Процесс установки выполняется в следующей последовательности:

1. Установка серверной части InfoWatch Device Monitor.

   В состав серверной части входят следующие компоненты:

   - база данных,
   - сервер InfoWatch Device Monitor
   - консоль управления InfoWatch Device Monitor.

2. Установка клиентской части InfoWatch Device Monitor.

   Клиент устанавливается на каждую рабочую станцию, которую необходимо контролировать с помощью InfoWatch Device Monitor.

Требования, предъявляемые Системой, перечислены в разделе "Требования к аппаратному и программному обеспечению".

Также о настройке, обновлении и удалении компонентов Системы читайте:

- Настройка Сервера InfoWatch Device Monitor. Порядок подготовки InfoWatch Device Monitor к эксплуатации.
- Обновление InfoWatch Device Monitor. Порядок обновления всех компонентов InfoWatch Device Monitor.
- Удаление InfoWatch Device Monitor. Рекомендации по удалению компонентов InfoWatch Device Monitor.

2.1 Требования к аппаратному и программному обеспечению

В настоящем подразделе перечислены требования, предъявляемые к аппаратному и программному обеспечению каждого компонента Системы:

- База данных
- Сервер InfoWatch Device Monitor
- Клиент InfoWatch Device Monitor
- Консоль управления

2.1.1 База данных

InfoWatch Device Monitor поддерживает работу со следующими СУБД:

- Oracle Database 11;

> **Внимание!**
> В случае установки Системы на серверную ОС разрядностью x64, необходимо использовать приложение Oracle Client разрядностью также x64.

- Microsoft SQL Server 2005, 2008, 2012 (Express, Developer, Workgroup, Standart, Enterprise).

2.1.2 Сервер InfoWatch Device Monitor

Требования к программному обеспечению Сервера InfoWatch Device Monitor:

- операционная система (поддержка как x86, так и x64 платформ):
  - Microsoft Windows 2003 Server;
  - Microsoft Windows Server 2008;
  - Microsoft Windows Server 2008 R2;
  - Microsoft Windows Server 2012.
- клиент СУБД:
  - Oracle версии 11g R2.
  - Microsoft .NET Framework 2.0 Service Pack 1.

> **Внимание!**
> Перед началом работы, необходимо ввести Сервер в домен Active Directory.

Аппаратные требования, предъявляемые Сервером InfoWatch Device Monitor, соответствуют минимальным требованиям, предъявлемым используемой операционной системой. Кроме этого, предъявляются следующие требования к свободному месту на жестком диске:

- Пакет установки - до 120 Мб;

- Если не выполняется интеграция с системой InfoWatch Traffic Monitor, то необходимо предусмотреть достаточно свободного места для хранения перехваченных копий. Изменение хранилища перехваченных копий выполняется с помощью конфигурационного XML-файла: см. "Раздел <applicationSettings>", параметр `ShadowCopyTempDir`.

2.1.3 Клиент InfoWatch Device Monitor

Клиент InfoWatch Device Monitor может работать на следующих операционных системах (поддержка как x86, так и x64 платформ):

- Microsoft Windows XP Professional Service Pack 3 со всеми обновлениями;
- Microsoft Windows Vista Service Pack 2;
- Microsoft Windows 7 Service Pack 1;
- Microsoft Windows 8 (x86, x64);
- Microsoft Windows 8.1 (x86, x64).

Внимание!

Установка Клиента должна выполняться только в среде вышеперечисленных операционных систем. Корректное взаимодействие Клиента с другими операционными системами не гарантируется. Установка Клиента в среду других операционных систем может привести к неправильной работе приложений, повреждению операционной системы и/или данных (вплоть до полного уничтожения данных).

Аппаратные требования, предъявляемые Клиентом InfoWatch Device Monitor, соответствуют минимальным требованиям, предъявлемым используемой операционной системой. Кроме этого:

- Материнская плата должна обеспечивать аппаратную поддержку USB;
- Свободное место на жестком диске должно составлять не менее 300 Мб.

Примечание:

Если на компьютере с установленным Клиентом InfoWatch Device Monitor используются приложения, значительно нагружающие процессор и оперативную память, для наиболее комфортной работы рекомендуется следующая конфигурация:

- CPU Intel Core i3 или аналогичный;
- RAM 4 Gb;
- HDD 50 Gb.

2.1.4 Консоль управления

Консоль управления InfoWatch Device Monitor может работать на следующих операционных системах (поддержка как x86, так и x64 платформ):

- Microsoft Windows 2003 Server Service Pack 1;
- Microsoft Windows Server 2008;
- Microsoft Windows Server 2008 R2;
- Microsoft Windows Server 2012;
- Microsoft Windows XP Professional Service Pack 2;
- Microsoft Windows Vista Service Pack 2;
- Microsoft Windows 7 Service Pack 1

- Microsoft Windows 8;
- Microsoft Windows 8.1.

Аппаратные требования, предъявляемые Консолью управления InfoWatch Device Monitor, соответствуют минимальным требованиям, предъявлемым используемой операционной системой. Свободное место на жестком диске должно составлять не менее 30 Мб.

2.2 Установка серверной части InfoWatch Device Monitor

Серверная часть InfoWatch Device Monitor устанавливается при помощи универсальной программы установки.

Универсальная программа установки находится на диске с дистрибутивом Системы (каталог `Setup.Unified`). При помощи данной программы можно установить все компоненты Системы, за исключением Клиента: базу данных, собственно Сервер Device Monitor и Консоль управления.

Для управления базой данных в системе InfoWatch Device Monitor может использоваться СУБД Microsoft SQL Server или Oracle.

Консоль управления может подключаться к основному Серверу.

Подробнее об установке читайте в следующих разделах:

- Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server
- Рекомендации по развертыванию базы данных под управлением СУБД Oracle
- Рекомендации по установке Сервера InfoWatch Device Monitor
- Порядок установки серверной части InfoWatch Device Monitor

2.2.1 Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server

На компьютере, с которого будет запущен процесс создания базы данных, предварительно должен быть установлен пакет Microsoft .NET Framework 2.0 Service Pack 1.

Учетная запись, от имени которой будет создаваться база данных, должна быть подготовлена заранее. Выбор типа учетной записи зависит от того, какой способ аутентификации вы планируете использовать для подключения к серверу базы данных. В СУБД Microsoft SQL Server поддерживаются два способа аутентификации:

- **Аутентификация Windows**. Аутентификация выполняется с использованием учетных записей, принадлежащих к домену Windows. Данные аутентификации обрабатываются системой безопасности Microsoft Windows.
- **Встроенная в SQL Server**. Используются учетные записи СУБД Microsoft SQL Server. Аутентификация выполняется средствами СУБД.

Внимание!
Для обеспечения приемлемого уровня безопасности настоятельно рекомендуется использовать способ **Аутентификация Windows**.

Если вы планируете использовать способ Аутентификация Windows:

1. Убедитесь, что в домене Windows существует учетная запись, от имени которой будет создаваться база данных. Эта учетная запись должна иметь права локального администратора на том компьютере, с которого будет запущен процесс создания базы данных. При необходимости создайте новую учетную запись.
2. Включите учетную запись в состав учетных записей СУБД Microsoft SQL Server, выбрав при этом

Аутентификация Windows.
3. Назначьте учетной записи роль **dbcreator**.

Если вы планируете использовать способ Встроенная в SQL Server:

1. Создайте новую учетную запись Microsoft SQL Server. При настройке параметров записи: выберите **Встроенная в SQL Server**, задайте имя и пароль.
2. Назначьте учетной записи роль **dbcreator**.

Примечание:
Имя и пароль встроенной учетной записи указывают при настройке параметров базы данных (см. "Порядок установки серверной части InfoWatch Device Monitor", шаг 6).

2.2.2 Рекомендации по развертыванию базы данных под управлением СУБД Oracle

На компьютере, с которого будет запущен процесс создания схемы базы данных, предварительно должен быть установлен клиент СУБД Oracle и пакет Microsoft.NET Framework 2.0 Service Pack 1.

Внимание!
В связи с особенностями работы провайдера OLE DB на компьютере, с которого выполняется установка, должен быть установлен только один экземпляр клиента (т.е. должна быть только одна рабочая директория Oracle home). Соблюдение этого условия необходимо для корректной установки базы данных.

Перед тем как начать создание схемы базы данных, убедитесь, что идентификатор соединения с сервером базы данных прописан в файле tnsnames.ora (см. "Настройка параметров соединения с сервером СУБД ORACLE").

2.2.2.1 Настройка параметров соединения InfoWatch Device Monitor с сервером СУБД Oracle

Для корректного соединения с сервером СУБД Oracle на каждом компьютере, на котором установлен клиент СУБД Oracle, необходимо выполнить настройку файлов `tnsnames.ora`, расположенного в каталоге `[ORACLE_HOME]\network\admin`.

Настройка файла tnsnames.ora

Укажите параметры подключения к серверу СУБД Oracle. Для этого добавьте в файл `tnsnames.ora` запись следующего вида:

```
tns_name =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = host_name)(PORT = port_number))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = service_name)
    )
  )
```

Здесь нужно подставить действительные значения для следующих параметров:

- `tns_name` – псевдоним сервера СУБД Oracle;
- `host_name` – доменное имя или ip-адрес сервера СУБД Oracle;
- `port_number` – порт сервера, на котором запущен процесс прослушивания клиентских подключений;

- `service_name` – имя сервиса базы данных.

Пример записи в файле `tnsnames.ora`:

```
IWDM =
   (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = iwdm.example.com)(PORT = 1521))
      (CONNECT_DATA =
          (SERVER = DEDICATED)
          (SERVICE_NAME = orcl)
      )
   )
```

Внимание!
Файл `tnsnames.ora` чувствителен к форматированию. Поэтому, если вы редактируете его, копируя приведенный пример, обратите внимание: в скопированном фрагменте не должно быть пустых строк.

2.2.3 Рекомендации по установке Сервера InfoWatch Device Monitor

Для повышения производительности Системы рекомендуется развертывать Сервер и базу данных на отдельных компьютерах.

Внимание!
При развертывании пула из нескольких серверов, на каждом из них должна быть установлена одинаковая версия серверного приложения InfoWatch Device Monitor, соответствующая актуальной версии базы данных.

В процессе настройки параметров Сервера (см. "Порядок установки серверной части InfoWatch Device Monitor") необходимо указать учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor. Возможны следующие варианты:

- **Local System**. Запуск службы от имени системной учетной записи.
- **Пользователь**. Запуск службы от имени учетной записи домена Windows.

Для базы данных под управлением СУБД Microsoft SQL Server. Если для аутентификации пользователя, создающего базу данных, выбран способ **Аутентификация Windows** (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server"), а база данных и Сервер будут находиться на разных компьютерах, то выберите вариант **Пользователь**.

Внимание!
Не рекомендуется выбирать вариант **Local System**. В этом случае пользователь может получить неограниченные права, что противоречит принципам создания политики безопасности.

Учетная запись домена Windows (вариант **Пользователь**) должна быть подготовлена заранее. Для этого выполните следующие действия:

1. Разрешите учетной записи запускать процесс как службу. Для этого:
   a. В **Панели управления** откройте компонент **Администрирование > Локальная политика безопасности**.
   b. В открывшемся диалоговом окне выберите узел **Локальные политики > Назначение прав пользователя**.
   c. Справа в области сведений дважды щелкните право **Вход в качестве службы**.
   d. На вкладке **Параметр локальной безопасности** добавьте подготовленную учетную запись.
2. Включите учетную запись в состав учетных записей СУБД Microsoft SQL Server.

По окончании установки предоставьте учетной записи доступ к созданной базе данных. При выборе разрешения на доступ к базе данных укажите роль **db_owner**.

2.2.4 Порядок установки серверной части InfoWatch Device Monitor

Внимание!
Перед началом установки ознакомьтесь с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor".

Внимание!
При развертывании пула из нескольких серверов, на каждом из них должна быть установлена одинаковая версия серверного приложения InfoWatch Device Monitor, соответствующая актуальной версии базы данных.

Шаг 1. Запуск мастера установки

Вставьте диск с дистрибутивом Системы в дисковод для компакт-дисков. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы.

В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите кнопку **Далее**.

Шаг 2. Принятие лицензионного соглашения

Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите кнопку **Далее**.

Шаг 3. Выбор устанавливаемого компонента

В окне **Выборочная установка** по умолчанию выбраны все компоненты.

Если необходимо, измените состав устанавливаемых компонентов. Так, например, если вы рассчитываете использовать Консоль управления для работы с Сервером с другой машины, то вам не нужно устанавливать этот компонент: нажмите на кнопку **Консоль управления** и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**.

Нажмите кнопку **Далее**.

Шаг 4. Определение параметров сервера

В окне **Тип устанавливаемого сервера** выберите:

- **Основной сервер** – должен быть установлен первым. К нему будут подключаться Клиенты и Консоль управления.
- **Вспомогательный сервер** – дополнительный сервер, обеспечивающий балансировку нагрузки от Клиентов.

Для обеспечения быстрой актуализации информации о серверах, рекомендуется отметить **Опубликовать сервер в Active Directory**.

Внимание!
Актуализируя политики безопасности, рабочие станции периодически взаимодействуют с сервером Device Monitor. Поэтому, чтобы вновь добавленный сервер мог сразу же приступить к обслуживанию рабочих станций, а также для своевременного уведомления Клиентов о возможных изменениях портов серверов, рекомендуется при установке сервера публиковать его данные в домене.

Для публикации данных сервера Device Monitor в домене, учетной записи, от имени которой выполняется установка сервера, требуются права на создание и удаление точек подключения.

Если у вас есть база данных Device Monitor соответствующей версии, снимите отметку **Установить новую базу данных**.

Нажмите кнопку **Далее**.

Шаг 5. Выбор сервера базы данных

Укажите СУБД, под управлением которой будет находиться база данных Device Monitor, выбрав один из следующих вариантов:

- Microsoft SQL Server
- Oracle

Если на Шаге 4 вы решили не устанавливать новую базу данных (опция **Установить новую базу данных** не была выбрана), то вам будет необходимо дополнительно указать параметры соединения с существующей базой данных Device Monitor.

Нажмите кнопку **Далее**.

Шаг 6. Настройка базы данных

Этот шаг пропускается, если на Шаге 4 вы решили использовать уже существующую базу данных.

Принцип настройки базы данных зависит от типа используемой СУБД.

При использовании СУБД Microsoft SQL Server укажите следующие параметры:

- **Сервер БД**. NetBIOS имя сервера СУБД Microsoft SQL Server, на котором будет создана база данных.

  Не задавайте в поле **Сервер БД** ip-адрес, так как в этом случае вы не сможете подключиться к серверу базы данных.

  Если на сервере базы данных есть именованные экземпляры, то имя сервера нужно указывать в следующем виде: `<имя_сервера>\<имя_экземпляра>`.

- **Имя базы данных**. Имя создаваемой базы данных.

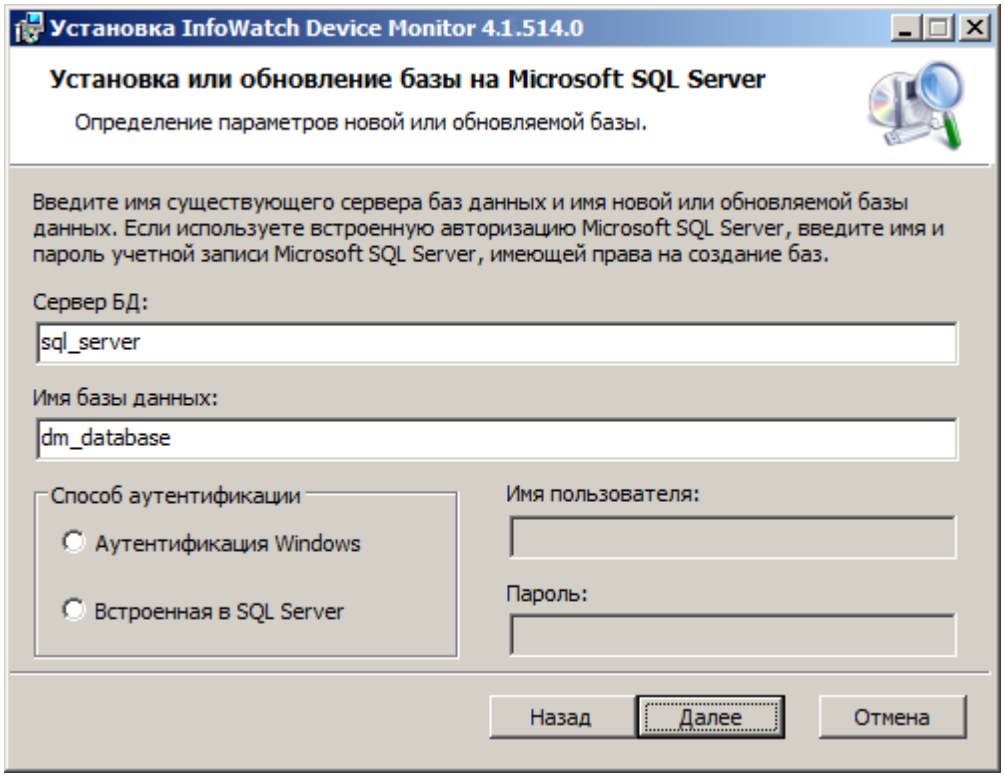
  Может содержать буквы латинского алфавита, цифры и прочие символы, за исключением пробелов и специальных символов: «*», «?», «/», «\», «|», «^», «:», «"». Должно начинаться с латинской буквы.

  Длина имени может составлять от 1 до 123 символов.

- **Способ аутентификации**. Способ аутентификации пользователя, от имени которого создается база данных и который будет использоваться для работы с БД. В качестве значения данного параметра укажите способ аутентификации, выбранный при подготовке учетной записи (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server").

  Если учетной записи назначена аутентификация Windows, то выберите значение **Аутентификация Windows**. В этом случае процесс создания БД будет выполняться от имени доменного пользователя, выполняющего установку.

  Если учетной записи назначена встроенная в SQL Server аутентификация, выберите значение **Встроенная в SQL Server**. Затем укажите имя и пароль подготовленной учетной записи в полях **Имя пользователя** и **Пароль** соответственно.



Настройка базы данных Microsoft SQL Server

При использовании СУБД Oracle настройте следующие параметры:

1. В области **Сервер БД** задайте параметры соединения с сервером базы данных:
   - **Сервер**. Имя сервера базы данных. В качестве значения данного параметра указывают псевдоним сервера из файла tnsnames.ora.
   - **Пароль для 'SYSTEM'**. Пароль учетной записи пользователя SYSTEM.
2. В области **Данные о схеме** укажите параметры учетной записи владельца создаваемой схемы базы данных:

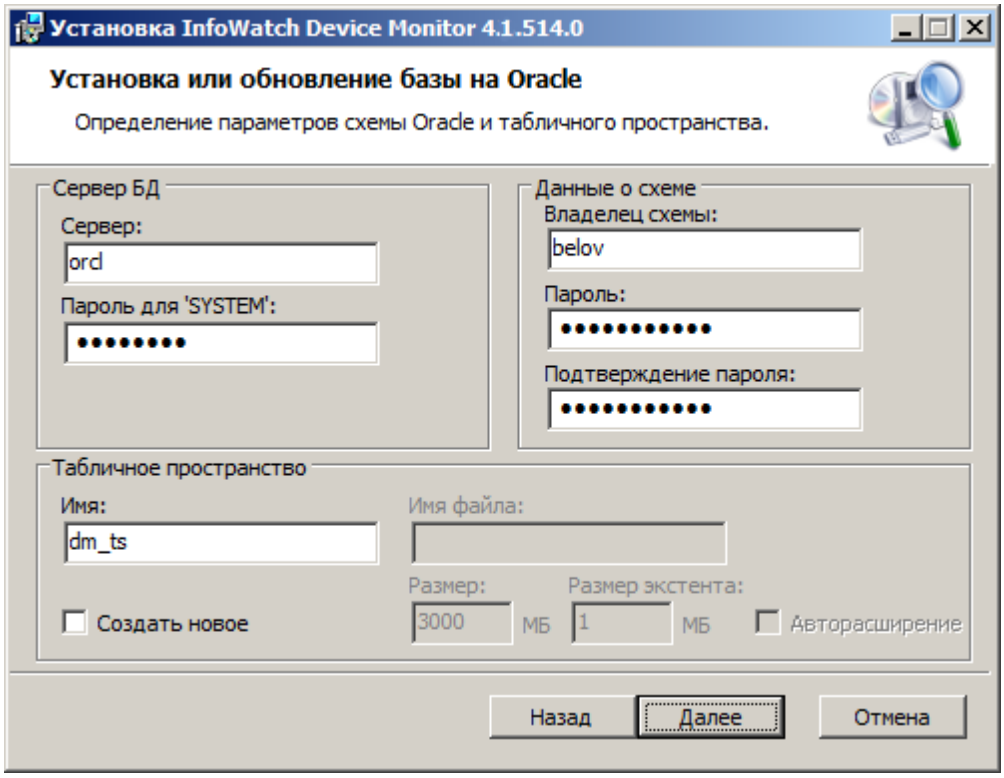
   Внимание!
   Не рекомендуется указывать параметры существующей схемы базы данных.

   - **Владелец схемы**. Имя учетной записи владельца схемы базы данных.
   - **Пароль**, **Подтверждение пароля**. Пароль учетной записи владельца схемы базы данных.

     Назначение пароля выполняется в соответствии с требованиями, указанными в документации к СУБД Oracle.
3. Настройте параметры табличного пространства в области **Табличное пространство**.

   Вы можете использовать существующее табличное пространство или создать новое. При использовании существующего табличного пространства, укажите имя табличного пространства в поле **Имя**.

   Чтобы создать новое табличное пространство, установите флажок в поле **Создать новое**. Затем укажите параметры табличного пространства:
   - **Имя**. Имя нового табличного пространства.
   - **Имя файла**. Имя файла данных, в котором будет храниться новое табличное пространство.
   - **Размер**. Максимальный размер (в Мб) файла данных (значение по умолчанию 3000 Мб).
   - **Размер экстента**. Максимальный размер (в Мб) непрерывного фрагмента пространства в файле данных (значение по умолчанию 1 Мб).
   - **Авторасширение**. Возможность автоматического расширения файла данных средствами СУБД Oracle. Если флажок в поле **Авторасширение** установлен, то функция авторасширения будет включена (по умолчанию данная функция отключена – флажок снят).



Настройка базы данных Oracle

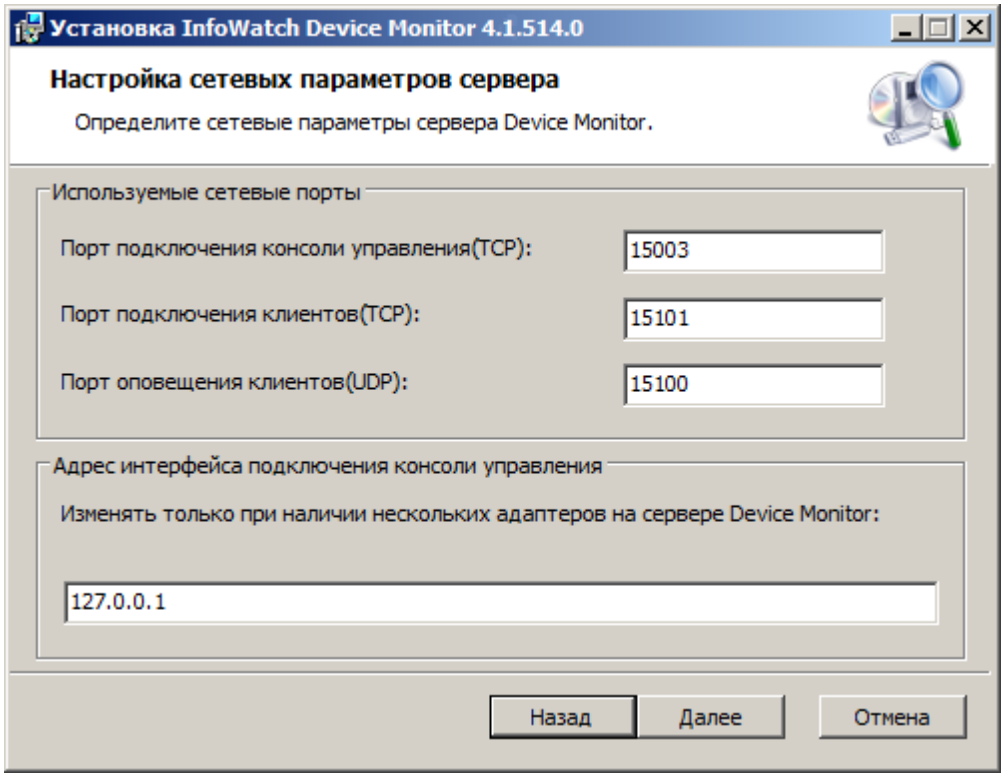
После того как все необходимые параметры будут заданы, нажмите кнопку **Далее**.

Шаг 7. Настройка рабочих параметров сервера

Настройте параметры Сервера:

1. В области **Используемые сетевые порты** задайте номера TCP и UDP портов, используемые для:
   - **подключения Клиентов** для передачи схем безопасности на контролируемые рабочие станции, отправки информации о событиях и теневых копий на сервер;
   - **оповещения Клиентов** об изменениях схем безопасности.
2. В области **Адрес интерфейса подключения Консоли управления** укажите IP-адрес, через который будет осуществляться взаимодействие между Сервером и Консолью управления.

> **Внимание!**
> Изменять значение данного параметра следует, только если Сервер будет установлен на компьютер с несколькими сетевыми адаптерами, подключенными к разным сетям. При наличии одного сетевого адаптера не допускается изменение данного параметра, иначе подключение Консоли управления к Серверу будет невозможно.
>
> Если в процессе работы на компьютер с установленным Сервером будут добавлены дополнительные сетевые адаптеры, то изменить настройку данного параметра можно в конфигурационном файле Сервера.



Настройка параметров сервера InfoWatch Device Monitor

После того как все необходимые параметры будут указаны, нажмите кнопку **Далее**.

Шаг 8. Настройка учетной записи сервера

Выберите учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor, в соответствии с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor". При выборе варианта **Пользователь** укажите имя и пароль подготовленной учетной записи домена Windows. Имя задается в формате `DOMAIN\USERNAME`.

Нажмите **Далее**.

Шаг 9. Настройка учетной записи администратора сервера

Укажите данные (имя и пароль) учетной записи администратора сервера. Данной учетной записи будет присвоена роль **Суперпользователь** (подробнее см. "Администрирование учетных записей Консоли управления"): она используется при первом подключении к Серверу с помощью Консоли управления.

Нажмите **Далее**.

Шаг 10. Настройка параметров соединения с сервером InfoWatch Traffic Monitor

Укажите параметры для взаимодействия с сервером InfoWatch Traffic Monitor:

- **Адрес сервера ТМ**. Адрес сервера InfoWatch Traffic Monitor. Взаимодействие с Traffic Monitor Server осуществляется по схеме *xml*. Запись адреса должна иметь следующий формат:

  ```
  xml://host:port
  ```

  Параметр *host* должен содержать доменное имя или IP-адрес сервера InfoWatch Traffic Monitor. Адрес сервера является стандартным URI-адресом (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 – 4101.

- **Количество соединений**. Количество соединений с сервером InfoWatch Traffic Monitor. Вы можете задать от 1 до 32 соединений.

- если в схеме развертывания Системы не планируется интеграция с InfoWatch Traffic Monitor, установите флажок в поле **Работать в автономном режиме**. В этом случае вы можете, установив флажок в поле **Сохранять теневые копии**, сохранять перехваченные теневые копии файлов в директорию установки сервера.

Нажмите кнопку **Далее**.

Шаг 11. Завершение установки

Нажмите кнопку **Установить**, чтобы начать установку Сервера. Следуйте дальнейшим указаниям мастера для завершения установки.

Примечание:
Этап установки сигнатур может занимать существенное время (до получаса).

2.3 Установка Клиента InfoWatch Device Monitor

Клиентская часть InfoWatch Device Monitor может быть установлена одним из следующих способов:

- Локальная установка. Выполняется при помощи универсальной программы установки непосредственно на каждой рабочей станции.
- Удаленная установка с помощью стороннего ПО. Осуществляется с использованием средств распространения программного обеспечения: например, посредством механизма групповых политик Microsoft Active Directory.
- Удаленная, через задачи распространения в Консоли управления InfoWatch Device Monitor.

Внимание!
Корректная работа Клиента InfoWatch Device Monitor требует запрета одновременной работы нескольких пользователей на рабочей станции. Для обеспечения данного требования Клиент разрешает работу только одной пользовательской сессии; другие сессии блокируются до тех пор, пока не будет завершена активная. Это может привести к блокировке функции быстрого переключения между пользователями (Fast User Switching) и терминального доступа к контролируемой рабочей станции.

2.3.1 Установка Клиента стандартным способом

Внимание!
Настоятельно не рекомендуется устанавливать Клиенты InfoWatch Device Monitor на компьютеры с одинаковыми именами. Такие компьютеры будут зарегистрированы как одна рабочая станция и, соответственно, на них будет распространяться одна политика, будет вестись единая регистрация событий и т.д.

Установку Клиента может выполнять пользователь, имеющий права локального администратора на том компьютере, на который выполняется установка.

Шаг 1. Запуск мастера установки

Вставьте диск с дистрибутивом Системы в дисковод для компакт-дисков. Затем откройте каталог `Client`. В данном каталоге найдите и запустите файл установки для требуемой платформы.

В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor Client. Нажмите на кнопку **Далее**, чтобы перейти к следующему окну мастера установки.

Шаг 2. Выбор каталога для установки

Укажите путь к каталогу, в который будет установлен Клиент.

Нажмите кнопку **Далее**.

Шаг 3. Настройка параметров

Укажите параметры соединения с Сервером InfoWatch Device Monitor:

- **Сервер**. Имя сервера InfoWatch Device Monitor.
- **Порт**. Номер порта, используемого для соединения между Клиентом и Сервером InfoWatch Device Monitor (по умолчанию задан порт 15101).

Нажмите кнопку **Далее**.

Шаг 4. Завершение установки

После перехода к окну **Подтверждение установки**, нажмите кнопку **Далее**, чтобы начать установку Клиента. Следуйте дальнейшим указаниям мастера для завершения установки. По окончании установки перезагрузите компьютер.

2.3.2 Установка Клиента с помощью средств распространения программного обеспечения

Установка Клиента на рабочие станции может выполняться администратором корпоративной сети централизованно, с помощью средств распространения программного обеспечения. В настоящем разделе описывается пример такой установки посредством Microsoft Active Directory.

Установка Клиента через Microsoft Active Directory осуществляется посредством механизма групповых политик. Для установки необходимо выбрать такую групповую политику, которая распространяется на все рабочие станции, подлежащие контролю при помощи Клиента. Это может быть политика, назначенная:

- контейнеру Active Directory, содержащему все рабочие станции, на которые будет выполняться установка Клиента.
- всему домену Active Directory, но не являющаяся доменной политикой по умолчанию (*Default Domain Policy*). Распространение этой политики должно быть назначено только той группе, которая включает в себя все рабочие станции, подлежащие контролю при помощи Клиента.

Шаг 1. Создание инсталляционного комплекта

Создайте установочный msi-пакет `Setup.Client.ru.msi`, как описано в разделе "Создание пакета установки". Разместите установочный пакет в сетевом каталоге, доступном для чтения всем компьютерам домена, на которые будет установлен Клиент.

Шаг 2. Отключение быстрого входа в систему Microsoft Windows XP Professional

Перед установкой Клиента через механизм групповых политик необходимо отключить оптимизацию быстрого входа в систему для компьютеров, на которых установлена операционная система Microsoft Windows XP Professional (так называемый асинхронный режим входа в систему). Подробная информация об этой функции доступна в базе знаний Microsoft (см. KB305293).

Чтобы отключить функцию оптимизации быстрого входа в систему:

1. Откройте редактор используемой групповой политики.
2. В дереве консоли выделите каталог **Computer Configuration > Administrative templates > System > Logon**. В области сведений выберите параметр **Always wait for the network at computer startup and logon**. Затем в окне свойств данного параметра установите значение **Enabled**.

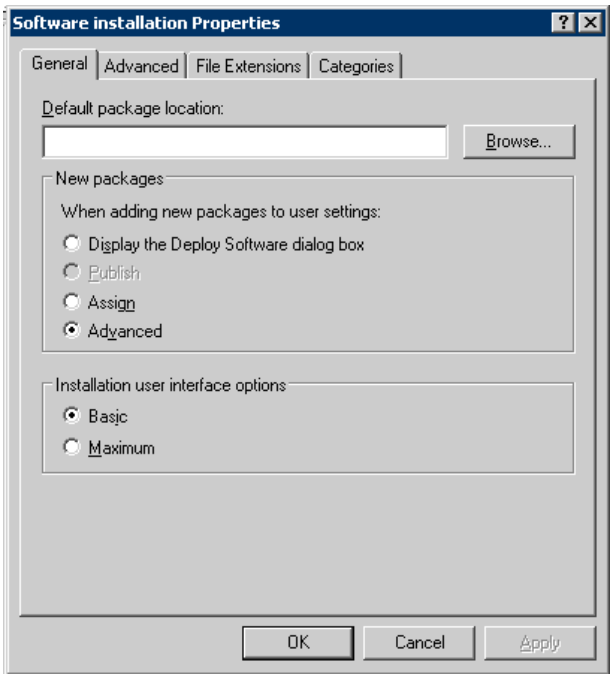
Примечание:
Если данная функция не отключена, то для установки Клиента потребуется еще одна дополнительная перезагрузка, связанная с механизмом распространения групповой политики Windows.

Шаг 3. Редактирование групповой политики

Перед установкой Клиента средствами Active Directory необходимо отредактировать используемую групповую политику.

Чтобы отредактировать групповую политику:

1. Откройте оснастку **Active directory users and computers** (**Start > Settings > Control Panel > Administrative tools > Active directory users and computers**).
2. В дереве консоли выберите контейнер Active Directory, содержащий все рабочие станции, на которые будет выполняться установка Клиента.
3. Откройте оснастку **Group Policy**. Для этого в контекстном меню контейнера Active Directory выберите команду **Properties**. Затем в открывшемся диалоговом окне перейдите на вкладку **Group policy**. На данной вкладке выделите объект групповой политики и нажмите на кнопку **Edit**.
4. В дереве консоли выберите расширение **Software Installation** (**Computer Configuration > Software Settings**).
5. В контекстном меню расширения **Software Installation** выберите команду **Properties**. В открывшемся диалоговом окне на вкладке **General** выполните следующие настройки (см. рисунок):
   - на панели **New packages** установите значение **Advanced**;
   - на панели **Installation user interface options** установите значение **Basic**.



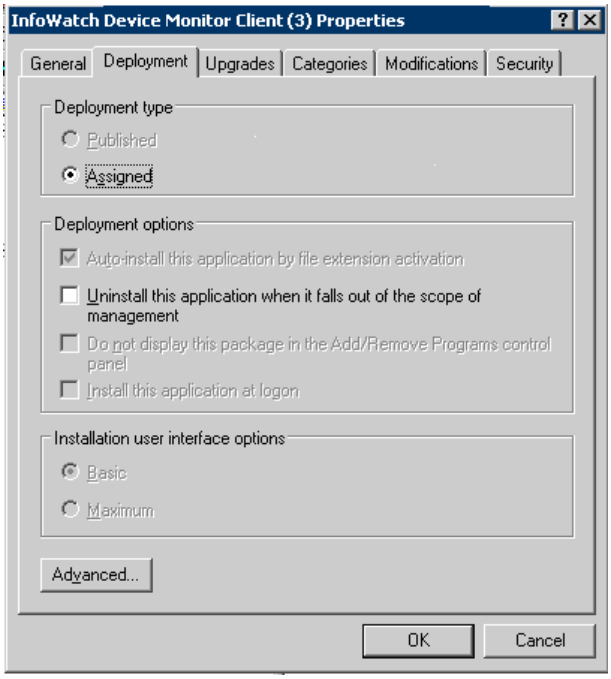
6. По окончании настройки нажмите на кнопку **OK**.

Шаг 4. Подготовка задания на установку Клиента

Создание и настройка задания на установку Клиента выполняется в окне **Group Policy Object Editor**:

1. После того как окно **Group Policy Object Editor** будет открыто, в дереве консоли выделите расширение **Software Installation** (**Computer Configuration > Software Settings**). Щелкните правой кнопкой мыши по названию выделенного пункта и в раскрывшемся контекстном меню выберите пункт **New > Package**.
2. В открывшемся диалоговом окне **Open** укажите установочный msi-пакет клиентского модуля `Setup.Client.ru.msi` (установочный пакет должен быть предварительно размещен в сетевом каталоге, доступном для чтения всем компьютерам домена, на которые будет установлен Клиент).

3. Выполните настройку свойств нового пакета:
   - Убедитесь, что установки, заданные на вкладке **Deployment**, соответствуют показанным на следующем рисунке.



   - После того как все необходимые настройки будут заданы, нажмите на кнопку **OK**.
4. В дереве консоли выделите каталог **Computer Configuration > Administrative templates > System > Scripts**. В области сведений выберите параметр **Run logon scripts synchronously**. Затем в окне свойств данного параметра установите значение **Enabled**.

Шаг 5. Выполнение установки

Добавленное задание отображается в списке заданий оснастки **Software Installation**. Задание выполняется при первой перезагрузке компьютера, на который должен быть установлен Клиент. Запуск службы InfoWatch Device Monitor Client осуществляется автоматически сразу после установки.

Способ установки отображается в столбце **Deployment state**. Состояние **assigned** означает, что установка осуществляется принудительно, т.е. без учета мнения пользователя, работающего за компьютером, на который выполняется установка Клиента. Состояние **published** соответствует установке с запросом согласия от пользователя.

Внимание!

Вы можете проверить успешность установки Клиента в Консоли управления InfoWatch Device Monitor. Все рабочие станции, на которые Клиент был успешно установлен, должны отображаться в списке раздела **Рабочие станции**. Чтобы просмотреть список всех контролируемых рабочих станций, воспользуйтесь кнопкой **Показать все рабочие станции**, расположенной в верхней части Панели навигации. Чтобы получить актуальные сведения об установленных Клиентах, воспользуйтесь кнопкой **Обновить**, расположенной на панели инструментов.

Если какая-либо из рабочих станций, на которые выполнялась установка, отсутствует в этом списке, проверьте возможность возникновения проблемы "*Сбой приложения групповой политики на компьютере с Windows XP с пакетом обновления 2 (SP2)*". Описание этой проблемы и действия по ее устранению описаны на сайте Microsoft: http://support.microsoft.com/kb/840669/ru.

2.4 Настройка Сервера InfoWatch Device Monitor

Настройка Сервера осуществляется с помощью конфигурационного XML-файла `InfoWatch.DeviceMonitor.Server.exe.config`. Конфигурационный файл размещается в том же каталоге, что и исполняемый файл Сервера `InfoWatch.DeviceMonitor.Server.exe`.

По умолчанию после установки Сервер расположен в каталоге

```
C:\Program Files\InfoWatch\Device Monitor\Server
```

Конфигурационный файл можно просматривать и редактировать при помощи любого текстового или XML-редактора. Кодировка файла UTF-8.

Корневым элементом конфигурационного файла является элемент `<configuration>`. Корневой элемент включает в себя дочерние элементы (конфигурационные разделы). Структура конфигурационного файла с описанием разделов приведена в следующей таблице. По ссылкам в названиях разделов содержится подробная информация об их настройке.

Конфигурационный раздел	Описание
<configSections>	Служебный раздел. Содержит описание всех остальных разделов. Редактирование этого раздела не разрешается.
<runtime>	Содержит настройки для среды выполнения Microsoft .NET Framework. Эти настройки необходимы для корректной работы Сервера. В разделе `<runtime>` определен элемент `gcServer`, предназначенный для настройки сборщика мусора. Элемент имеет атрибут `enabled`, принимающий значение `true` (включен параллельный сбор мусора) или `false` (выключен параллельный сбор мусора). Изменение этого раздела крайне не рекомендуется.
<applicationSettings>	Содержит настройки отдельных модулей Сервера, таких как порты, размеры буферов, таймауты и пр.
<system.diagnostics>	Содержит настройки протоколирования. Протоколирование может быть полезно при диагностике работы компонентов Сервера.

2.4.1 Раздел <applicationSettings>

Раздел `<applicationSettings>` предназначен для настройки отдельных модулей Сервера. Всего таких модулей шесть. Все разделы имеют одинаковую структуру: В состав любого из этих разделов входит набор элементов, предназначенных для настройки параметров модуля. Каждый элемент `<setting>` имеет следующие атрибуты:

- `name` — имя настройки.
- `serializeAs` — способ сериализации данных. Данные всегда сериализуются в виде строки (используется тип данных string).

Настройки параметров модуля определяется дочерним элементом `<value>`. Например:

```
<setting name="RemotingPort" serializeAs="String">
  <value>15003</value>
</setting>
```

Описание параметров для каждого модуля приводится в следующей таблице.

Параметр	Описание
<InfoWatch.DeviceMonitor.Server.Core.Properties.Settings> Настройки ядра Сервера	
RemotingPort	Порт TCP, обслуживающий подключения Консоли управления. Значение по умолчанию 15003 (крайне не рекомендуется изменять это значение)
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: • ru-RU • en-US
MachineName	IP-адрес сетевого интерфейса, посредством которого Сервер принимает соединения с Консолью управления. Значение по умолчанию 127.0.0.1. Изменять это значение нужно, только если Сервер имеет 2 или более сетевых интерфейсов. В этом случае для корректной работы необходимо явно задать адрес интерфейса, посредством которого сервер принимает входящие соединения от различных экземпляров Консоли управления
CheckServerSettingsInte	При наличии кластеризации – период (в секундах) синхронизации с базой данных. По истечении этого времени Сервер запрашивает базу данных об изменениях в схеме безопасности, произведенных с помощью основного Сервера, использующего ту же базу данных. Значение по умолчанию 10
<InfoWatch.DeviceMonitor.Server.Database.Properties.Settings> Настройки модуля, взаимодействующего с базой данных	
DatabaseType	Тип базы данных. Возможные значения: • Oracle • Microsoft
ConnectionString	Строка соединения с базой данных. Должна соответствовать правилам, установленным для строк соединения ADO.NET. Например: Data Source=isis\s2005;Initial Catalog=g1228_9;Integrated S
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: • ru-RU • en-US
ConnectionPoolSize	Количество соединений к БД, которые будут открыты и которые будет использовать сервер в своей работе. Значение по умолчанию 20
CommunicationPort	Номер порта, используемого при соединении сервера с Агентом распространения при установки Клиента через механизм задач. Не рекомендуется менять в процессе работы. Значение по умолчанию 15505
UpdateStatusTimeOut	Интервал времени, через который необходимо обновлять статус выполнения задачи на удалённом компьютере. С данным интервалом сервер опрашивает удалённые компьютеры, где разворачивается Клиент, о статусе установки продукта, для отображения информации на сервере. Значение по умолчанию 60
<InfoWatch.DeviceMonitor.Server.Gui.Properties.Settings> Настройки модуля, предоставляющего интерфейс для Консоли управления	

Параметр	Описание
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: • ru-RU • en-US
InitialLeaseTime	Время (в минутах), в течение которого сеанс соединения с Консолью управления считается действительным
RenewOnCallTime	Время (в минутах), на которое продлевается время жизни сеанса соединения Консоли с сервером.
<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings> Настройки модуля, обслуживающего клиентские подключения (контролируемые рабочие станции)	
Backlog	Длина очереди клиентских соединений, ожидающих подключения. Значение по умолчанию 128
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: • ru-RU • en-US
ShadowCopyTempDir	Полный путь к каталогу, в котором хранятся временные теневые копии, ожидающие отправки в InfoWatch Traffic Monitor. Значение по умолчанию: C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyT
DmpV1Adress	Список IP-адресов (разделитель в перечислении – «;»), на которых сервер должен прослушивать порты. Возможны следующие значения: • AllAny – порты на всех IP адресах, которые имеются на компьютере (значение по умолчанию); • AllIp4 – порты на всех IP адресах версии 4; • AllIp6 – порты на всех IP адресах версии 6.
Dmpv1TraceLevel	Уровень трассировки протокола взаимодействия клиента и сервера. Возможны следующие значения: • 1 – выключить трассировку (значение по умолчанию); • 2 – выполнять трассировку только для информации о пакете; • 3 – полная трассировка.
Dmpv1TraceClients	Список IP-адресов Клиентов (разделитель в перечислении – «;»), взаимодействие с которыми необходимо трассировать. При значении All выполняется трассировка для всех Клиентов.
Dmpv1ConnectionsLimit	Количество одновременно обрабатываемых соединений по протоколу TCP/IP с клиентами. Значение по умолчанию 200.
Dmpv1ConnectionsQueueLi	Максимальное количество соединений, ожидающих обработку. Если значение превышено, то соединения "урезаются" до значения, указанного в параметре Dmpv1ConnectionsQueueLengthAfterCut. Значение по умолчанию 500.
Dmpv1ConnectionsQueueLe	Количество соединений после урезания очереди при превышении очередью максимального размера. Значение по умолчанию 250.
TimeoutPeriodSeconds	Величина таймаута, по истечении которого зависшее соединене между Клиентом и Сервером будет закрыто, частично созданные теневые копии будут удалены (отправка теневых копий будет повторяться при следующем установленном соединении).

Параметр	Описание
	Значение по умолчанию 120.
<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings> Базовые настройки коннектора Traffic Monitor Server	
DBPollTime	Период (в миллисекундах) опроса базы данных, в процессе которого проверяется наличие событий в базе данных
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: • ru-RU • en-US
NumberOfConnections	Количество соединений с InfoWatch Traffic Monitor. Нормальное значение 4. Максимальное значение 32
QueueSendLimit	Максимальное количество событий, которые могут быть переданы из базы данных в InfoWatch Traffic Monitor за одну транзакцию. Значение по умолчанию 200
<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings> Настройки низкоуровневого драйвера базы данных	
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: • ru-RU • en-US
MaxConnectionWaitingTim	Время ожидания свободного соединения из пула в секундах. Значение по умолчанию - 150
CommandTimeoutSeconds	Время выполнения операции или запроса в секундах. Значение по умолчанию - 30 **Примечание:** данный параметр не работает для СУБД Oracle.
LongCommandTimeoutSecon	Время выполнения длительной операции или запроса в секундах. Применяется, когда время выполнения составляет значительный промежуток. Значение по умолчанию - 0 (бесконечность). **Примечание:** данный параметр не работает для СУБД Oracle.

2.4.2 Раздел <system.diagnostics>

Раздел предназначен для диагностики работы Сервера. Включает в себя следующие элементы:

- <trace>. Общие настройки модуля диагностики.
- <sources>. Настройки, необходимые для диагностики отдельных компонентов Сервера.
- <switches>. Управление уровнем детализации диагностической системы в целом. Включает в себя определения детализаторов. Как правило, существует один детализатор. Если для разных модулей требуются разные настройки детализации, то необходимо использовать фильтры. При этом общий детализатор, должен иметь значение, соответствующее максимальной детализации одного из модулей.

Элемент <*trace*>

Используется для описания глобальных настроек модуля диагностики. В данном элементе можно задавать величину отступов в сообщениях, параметры сохранения данных из потока диагностики на жесткий диск.

Элемент <*sources*>

Используется для настройки отдельных модулей приложения. Включает в себя дочерние элементы <source> – по одному на каждый модуль приложения (список модулей Сервера см. "Раздел

<applicationSettings>").

Элемент `<source>` имеет следующие атрибуты:

- `name`. Имя модуля сервера.
- `switchName`. Имя модуля, определяющего детализацию диагностики (детализатора).
- `switchType`. Тип модуля, определяющего детализацию диагностики. Всегда имеет значение `System.Diagnostics.SourceSwitch`.

В каждом элементе <source> также содержится определение приемника диагностических сообщений (`<listeners>`). Приемником диагностических сообщений может быть:

- журнал приложений Windows (Application log);
- системный отладочный вывод (можно просматривать с помощью специальных инструментов, например, DebugView);
- текстовый файл.

Элемент `<source>` имеет дочерний элемент `<listeners>`. В данном элементе содержатся параметры приемника диагностических сообщений. Элемент `<listeners>` может включать в себя следующие дочерние элементы:

- `<add>`. Добавление нового приемника диагностических сообщений.
- `<remove>`. Удаление приемника диагностических сообщений. Применяется только для удаления приемника сообщений по умолчанию (таковым является журнал приложений Windows). С этой целью нужно установить имя элемента равным `Default`:

```
<remove name="Default" />
```

Элемент *<add>*

Данный элемент добавляет приемник диагностических сообщений к модулю Сервера. Элемент содержит следующие атрибуты:

- `name`. Имя приемника диагностических сообщений.
- `type`. Тип приемника диагностических сообщений.
- `initializeData`. Идентификатор модуля Сервера. Как правило, это значение совпадает с именем соответствующего модуля Сервера. Если в качестве приемника используется журнал приложений Windows, то это информация, которая заносится в столбец `source`.

Тип приемника — это полное имя типа приемника из библиотеки классов .NET Framework или собственного типа, реализующего требуемый интерфейс приемника диагностических сообщений.

В библиотеке классов .NET Framework определены следующие типы приемников диагностических сообщений:

- `System.Diagnostics.EventLogTraceListener`. Журнал приложений Windows (Application log).
- `System.Diagnostics.ConsoleTraceListener`. Вывод сообщений в консольном приложении.
- `System.Diagnostics.TextWriterTraceListener`. Вывод в текстовый файл
- `System.Diagnostics.DefaultTraceListener`. Отладочный вывод Windows (по умолчанию включен).

Также элемент `<add>` содержит фильтр диагностических сообщений. Данный фильтр выводит только те сообщения, которым назначен уровень детализации, превышающий уровень, заданный в настройках фильтра. Определены следующие уровни детализации (приводятся в порядке убывания важности уровня):

- `Verbose`. Отладочный уровень. В журнале регистрируются все события. Этот уровень нужно применять только для отладки Системы. Не разрешается устанавливать данный уровень для Системы, работающей в нормальном режиме, так как это приводит к значительному снижению производительности.
- `Information`. Информационный уровень. Регистрируются события не связанные с ошибками, такие как, например, информация об изменении параметров сервера.
- `Warning`. Уровень предупреждения. Регистрируются некритичные ошибки в работе Системы, такие как неожиданное прекращение соединения с Сервером, истекший таймаут соединения и пр.
- `Error`. Уровень ошибок. Регистрируются ошибки, мешающие корректной работе Системы (т.е.

ошибки, требующие исправления).

- `Critical`. Критический уровень. Регистрируются серьёзные нарушения в работе, которые могут привести к неработоспособности Системы.

Пример 1

Для детализатора установлен уровень протоколирования *Verbose*, а для фильтра какого-либо модуля – *Warning*. Тогда детализатор пропускает события с уровнем *Warning*, *Error* и *Critical*, но отфильтровывает события с уровнем *Information* и *Verbose*.

Пример 2

Для детализатора установлен уровень протоколирования *Error*, а для фильтра какого-либо модуля – *Warning*. В этом случае детализатор пропускает события с уровнем *Error* и *Critical*, но отфильтровывает события с уровнем *Warning*, *Information* и *Verbose*. Это происходит потому, что общий уровень детализации Системы *Error*, т.е. вне зависимости от того, как настроены фильтры, регистрируются только сообщения с уровнем *Error* и выше.

Элемент <*remove*>

Удаление приемника сообщений. Как правило, применяется для удаления приемника по умолчанию, выводящего диагностические сообщения в отладочный вывод Windows:

```
<remove name="Default" />
```

Элемент <*switches*>

Определяет детализаторы Сервера. Как правило, определен только один детализатор, который устанавливает глобальный (для всего Сервера) уровень детализации диагностической системы. Если отдельным модулям Сервера требуется более низкий уровень детализации, то в этом случае можно воспользоваться фильтрами.

По-умолчанию элемент `<switches>` содержит только один дочерний элемент:

```
<add name="eventLog" value="Warning"/>
```

Уровень детализации задается как значение атрибута `value`.

2.5 Обновление InfoWatch Device Monitor

Если у вас установлена система InfoWatch Device Monitor, то вы можете обновить ее до более поздней версии.

Обновление Системы выполняется в том же порядке, что и установка:

1. Обновление серверной части InfoWatch Device Monitor (база данных, сервер, и консоль управления).

> **Внимание!**
> Если требуется обновить Систему версии 3.4, удалите старую версию сервера (не удаляя базу данных) и установите сервер заново, указав при этом параметры соединения с существующей базой данных. Начиная с версии 4.0 обновление выполняется стандартным способом.

2. Обновление Клиента InfoWatch Device Monitor.

Система поддерживает совместимость с прежними версиями Клиента, начиная с 3.4.875. Поэтому обновление Клиента выполняется по мере необходимости.

2.5.1 Обновление серверной части InfoWatch Device Monitor

Внимание!
Если требуется обновить Систему версии 3.4 - 4.0, удалите старую версию сервера (не удаляя базу данных) и установите сервер заново, указав при этом параметры соединения с существующей базой данных. Начиная с версии 4.0 обновление выполняется стандартным способом.

Шаг 1. Начало обновления

Вставьте диск с дистрибутивом Системы в дисковод для компакт-дисков. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы.

В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите кнопку **Далее**, чтобы перейти к следующему окну мастера установки.

Шаг 2. Настройка базы данных

При обновлении база данных сохраняется, и в окне **Настройка соединения с базой данных** по умолчанию указываются параметры ранее использовавшейся базы данных. Однако вам потребуется указать некоторые параметры, в зависимости от используемой СУБД.

Обновление базы данных под управлением СУБД Microsoft SQL Server

На панели **Способ аутентификации** выберите способ аутентификации, назначенный пользователю, от имени которого обновляется база данных.. В качестве значения данного параметра укажите способ аутентификации, выбранный при подготовке учетной записи (см. раздел "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server").

Если учетной записи назначена аутентификация Windows, то выберите значение **Аутентификация Windows**.

Если учетной записи назначена встроенная аутентификация SQL Server, выберите значение **Встроенная в SQL Server**. Затем укажите имя и пароль подготовленной учетной записи в полях **Имя пользователя** и **Пароль** соответственно.

Примечание:
В процессе обновления вы можете указать прежние параметры аутентификации или задать новые. Рекомендации по выбору способа аутентификации и подготовке необходимой учетной записи приведены в разделе "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server".

Обновление базы данных под управлением СУБД Oracle

На панели **Сервер БД** укажите параметр **Пароль для 'SYSTEM'** - пароль учетной записи пользователя SYSTEM, используемый для работы с обновляемой базой данных.

На панели **Данные о схеме** укажите параметры **Пароль**, **Подтверждение пароля** - пароль учетной записи владельца схемы базы данных, используемый для работы с обновляемой базой данных.

После того как необходимые параметры будут настроены, нажмите кнопку **Далее**.

Шаг 3. Завершение обновления

После перехода к следующему окну, нажмите на кнопку **Установить**, чтобы запустить процесс обновления серверной части Системы.

Следуйте дальнейшим указаниям мастера установки, чтобы завершить обновление серверной части Системы.

Важная информация!
При обновлении компонента **Консоль управления**, никаких долнительный действий со стороны пользователя не требуется. **Консоль управления** может быть установлена единовременно с компонентом **Сервер**. В случае обособленной установки компонента, установочный пакет обновит компонент при выборе его в меню установки.

2.5.2 Обновление Клиента InfoWatch Device Monitor

Система поддерживает совместимость с версиями Клиента, начиная от 3.4.875 включительно. Таким образом, обновленные компоненты Системы могут работать со старыми версиями Клиента. Однако вы можете обновить Клиента до более поздней версии.

Обновление Клиента выполняется аналогично установке:

- локальное обновление с использованием мастера установки;
- удаленное обновление с помощью средств распространения программного обеспечения;
- централизованное обновление через Консоль управления.

2.6 Удаление InfoWatch Device Monitor

Чтобы удалить серверную часть InfoWatch Device Monitor вместе с Консолью управления:

1. Выполните одно из следующих действий:
   - На диске с дистрибутивом системы откройте каталог `Setup\Unified`. В данном каталоге найдите и запустите файл установки для требуемой платформы.
   - В оснастке **Добавить или удалить программы** (**Add or remove programs**), входящей в состав операционной системы Windows, выберите **InfoWatch Device Monitor Server** и нажмите на кнопку **Изменить** (**Change**).

   На экране появится окно приветствия мастера установки. Нажмите на кнопку **Далее**, чтобы перейти к следующему окну.
2. В окне **Изменение, восстановление или удаление…** выберите команду **Удалить**.
3. Если вы хотите удалить систему вместе с базой данных, в окне **Удаление базы данных…** установите флажок в поле **Удалить базу**. В этом случае вам потребуется задать параметры удаления: состав параметров зависит от вида используемой СУБД:
   - **Microsoft SQL Server** – укажите используемый способ аутентификации, выбрав нужный вариант на панели **Способ аутентификации** (см. также "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server").

     Если аутентификация выполнялась средствами SQL-сервера (**Встроенная в SQL Server**), то на панели **Администратор базы данных**, в полях **Имя пользователя** и **Пароль** укажите параметры той учетной записи, при помощи которой осуществлялось подключение к базе данных.
   - **Oracle** – в поле **Пароль учетной записи SYSTEM** укажите необходимый пароль. В результате будет удалена учетная запись владельца схемы базы данных, а также все объекты, за исключением табличного пространства.
4. После того как необходимые параметры будут заданы, нажмите кнопку **Удалить**, чтобы запустить процесс удаления.

Чтобы удалить серверную часть InfoWatch Device Monitor или Консоль управления отдельно:

1. В оснастке **Добавить или удалить программы** (**Add or remove programs**) воспользуйтесь кнопкой **Изменить** (**Change**).
2. В окне выборочная установка нажмите  слева от компонента, который вы намерены удалить, и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**. Нажмите

Далее.

3. Если на предыдущем шаге вы выбрали для удаления сервер, то в окне **Удаление базы данных…** определите необходимость удаления базы данных и, при необходимости, задайте параметры учетной записи, имеющей на это права (подробнее см. выше).
4. Нажмите **Изменить**, чтобы запустить процесс удаления.

Чтобы удалить Клиент InfoWatch Device Monitor:

в оснастке **Добавить или удалить программы** (**Add or remove programs**) выберите **InfoWatch Device Monitor Client** и воспользуйтесь кнопкой **Удалить** (**Remove**).

Удаление Клиентов можно также выполнять централизованно:

- с помощью средств Active Directory (если Клиенты были установлены при помощи средств распространения программного обеспечения), как описано в разделе "Удаление Клиента, установленного с помощью средств распространения программного обеспечения".
- с помощью задач распространения в Консоли управления, как описано в разделе "Удаленная установка, обновление и удаление Клиентов".

2.6.1 Удаление Клиента, установленного с помощью средств распространения программного обеспечения

Клиенты, установленные с помощью средств распространения программного обеспечения, могут быть удалены тем же способом.

Например, если установка Клиентов была выполнена через Microsoft Active Directory, то администратор корпоративной сети может удалить назначенное задание на установку из соответствующей групповой политики. Порядок редактирования групповой политики описывается в разделе "Установка Клиента с помощью средств распространения программного обеспечения", шаг 3.

Чтобы удалить Клиента со всех контролируемых рабочих станций:

1. Выделите задание на установку, которое нужно удалить. Затем щелкните правой кнопкой мыши по выделенной строке и в раскрывшемся контекстном меню выберите пункт **All tasks > Remove**.
2. В открывшемся диалоговом окне **Remove software** выберите пункт **Immediately uninstall the software from users and computers**.

   Примечание:
   Если будет выбран другой пункт, то задание на установку будет удалено, но все ранее установленные Клиенты останутся. Удаление этих Клиентов средствами Microsoft Active Directory в дальнейшем будет невозможно.

3. Нажмите на кнопку **OK**.

Клиент будет удален со всех компьютеров, на которые распространяется выбранная групповая политика.

3 Работа в Консоли Управления

Консоль управления предназначена для решения следующих задач:

- управление доступом к системе InfoWatch Device Monitor;
- настройка системы мониторинга рабочих станций;
- контроль доступа к рабочим станциям.

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::

- Общие принципы работы с Консолью управления. Общие приемы при работе с Консолью управления InfoWatch Device Monitor (запуск, настройка интерфейса).
- Администрирование пользователей 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 рабочих станциях.
- Удаленная установка, обновление и удаление Клиентов. Описание установки и настройки Клиента 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.

3.1 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

3.1.1 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. Порядок установки серверной части InfoWatch Device Monitor).

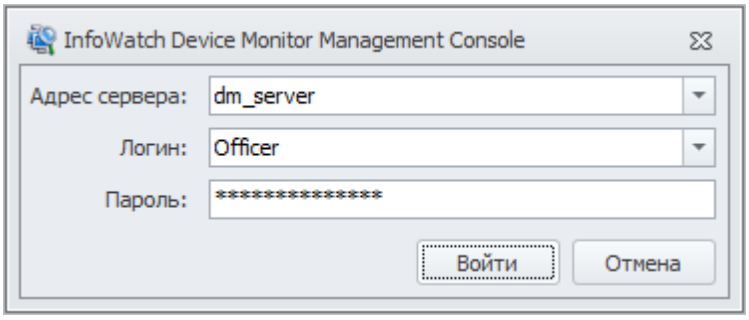
Чтобы начать работу с Консолью управления:

1. Запустите Консоль управления. Для этого в меню **Пуск** выберите пункт **Программы > InfoWatch > Device Monitor > Консоль управления**.
2. Выполните процедуру авторизации, как описано ниже.

Успешное прохождение авторизации возможно только при выполнении всех нижеперечисленных 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.

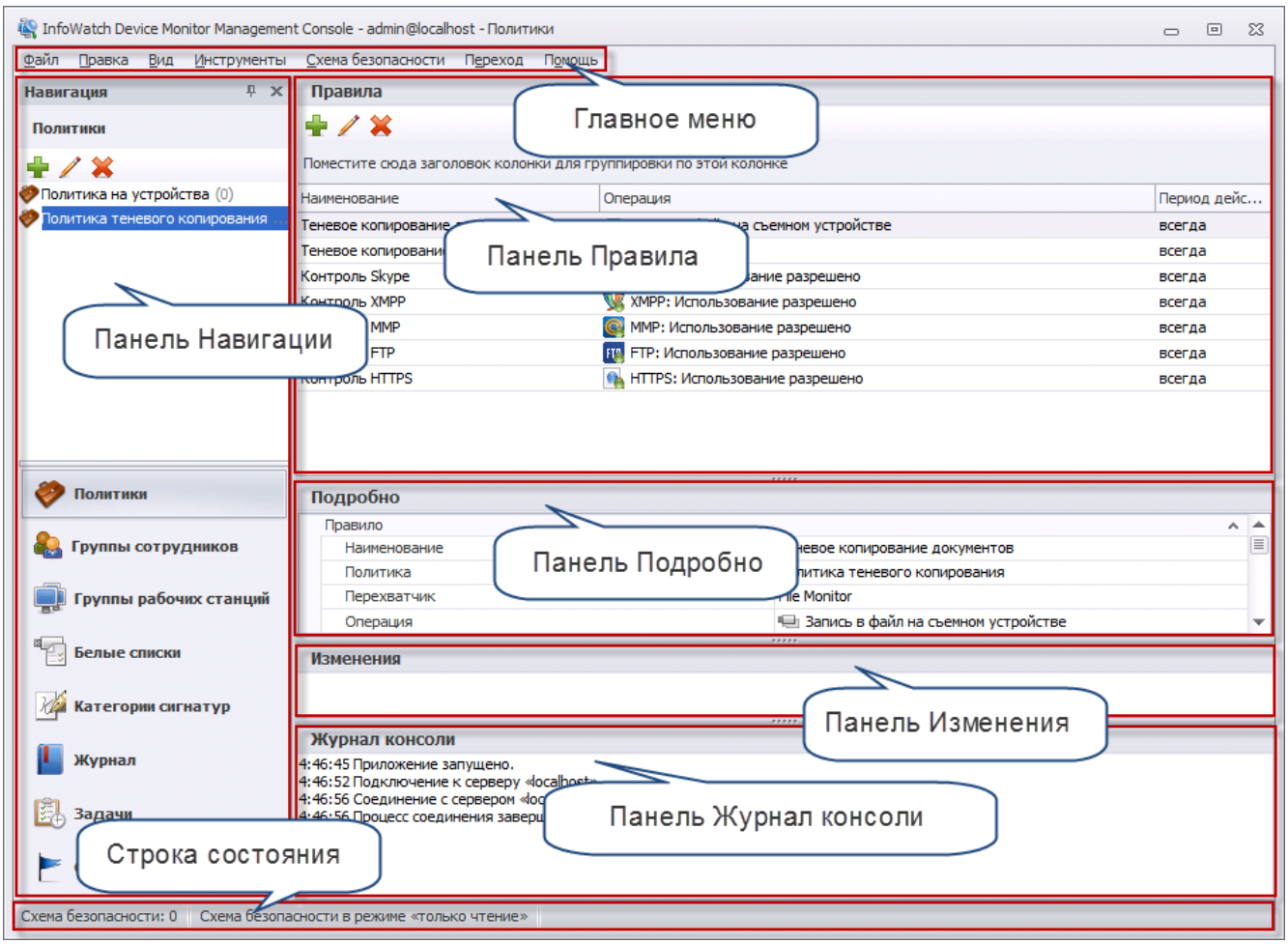
При первом запуске Консоли управления поля диалогового окна **Подключение** – пустые. В дальнейшем поля **Адрес сервера** и **Пользователь** будут заполнены данными, соответствующими последней попытке авторизации. Поле **Пароль** необходимо заполнять при каждой попытке авторизации.

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.

3.1.2 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.
- На **панелях инструментов** находятся ряды кнопок для быстрого доступа к некоторым функциям Консоли.
- **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 панели **Подробно** отображаются расширенные сведения о свойствах какого-либо элемента выбранной группы.
- На панели **Измения** 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 рабочих станций** - также версии различных элементов контроля.

3.1.2.1 Настройка элементов главного окна Консоли управления

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

Действие	Шаги
Убрать 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. или • Воспользуйтесь кнопкой ⊠, расположенной в правом верхнем углу панели.
Включить/отключить режим автоматического свертывания панели	Воспользуйтесь кнопкой 🗖, расположенной в правом верхнем углу панели
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

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 с двойной 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 флажками те элементы, которые будут отображены на экране (по умолчанию отмечены все элементы).

3.1.3 Разделы Консоли управления

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

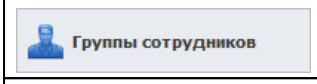
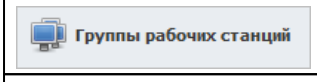
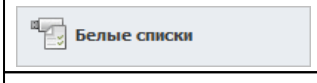
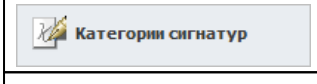
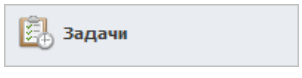
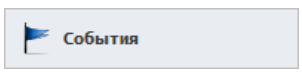
Чтобы перейти к нужному разделу, выполните одно из следующих действий:

- 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 рабочих станций**, **Белые списки** и **Категрии сигнатур** предназначены для управления схемой безопасности, раздел **Журнал** – для контроля действий по управлению схемой безопасности, **Задачи** - для управления задачами установки и удаления Клиентов, **События** - для просмотра событий с контролируемых рабочих станций. Подробное описание функций каждого раздела приведено в таблице:

Пиктограмма и название раздела	Назначение раздела
	Управление политиками безопасности: создание политик безопасности, настройка правил для каждой политики
	Управление сотрудниками: создание групп сотрудников, распределение сотрудников по группам)
	Управление контролируемыми рабочими станциями: создание групп рабочих станций, распределение контролируемых рабочих станций по группам
	Управление списками устройств, доступ к которым безусловно разрешен.
	Просмотр и управление категориями сигнатур, с помощью которых правила File Monitor могут распространяться на определенные форматы файлов.
	Аудит действий по управлению схемой безопасности
	Централизованная установка, обновление и удаление Клиентов InfoWatch Device Monitor на рабочие станции.
	Просмотр сведений о работе сотрудников на контролируемых рабочих станциях с использованием контролируемых средств.

3.2 Администрирование учетных записей Консоли управления

Для каждого пользователя, на которого возложены задачи по управлению 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.

Для разграничения полномочий пользователей, работающих с Консолью управления, используются **роли**. С каждой ролью сопоставлен набор полномочий на выполнение определенных действий по управлению зоной ответственности. Пользователь не может выполнять те действия, которые выходят за рамки полномочий назначенной ему роли.

Для разграничения прав в Консоли управления используются следующие роли:

- **Офицер безопасности** - конечный пользователь Консоли, выполняет управление схемой безопасности и настройками Сервера.
- **Локальный администратор** - администратор Консоли, управляющий другими учётными записями Консоли.
- **Суперпользователь** - роль предустановленного пользователя, обладающая всеми правами при работе в Консоли. Не предназначена для повседневной работы с Системой, рекомендуется использовать исключительно для первоначальной настройки Консоли управления, создания учетной записи для Локального администратора, а затем - только для использования в аварийных условиях.

В следующей таблице приведен общий перечень прав на те или иные действия для этих ролей.

Действия	Суперпользователь	Локальный администратор	Офицер безопасности
Первый запуск и настройка Консоли управления	+		
Работа в аварийных условиях	+		
Разблокирование схемы безопасности	+		
Просмотр журнала аудита	+		+
Экспорт записей журнала аудита	+		+
Удаление записей из журнала аудита	+		
Просмотр сведений об учетных записях Консоли управления	+	+	+
Добавление, редактирование, удаление учетных записей пользователей Консоли управления	+	+	
Назначение/ удаление ролей для пользователей Консоли управления	+	+	
Блокировка/разблокировка учетных записей пользователей Консоли управления	+	+	
Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor	+		+
Просмотр предыдущих версий схем безопасности	+		+
Редактирование схемы безопасности	+		+
Импорт/экспорт политик безопасности и правил	+		+
Просмотр событий	+		+
Удаленная установка, обновление и удаление Клиентов Device Mionitor	+		+
Предоставление временного доступа для сотрудника	+		+

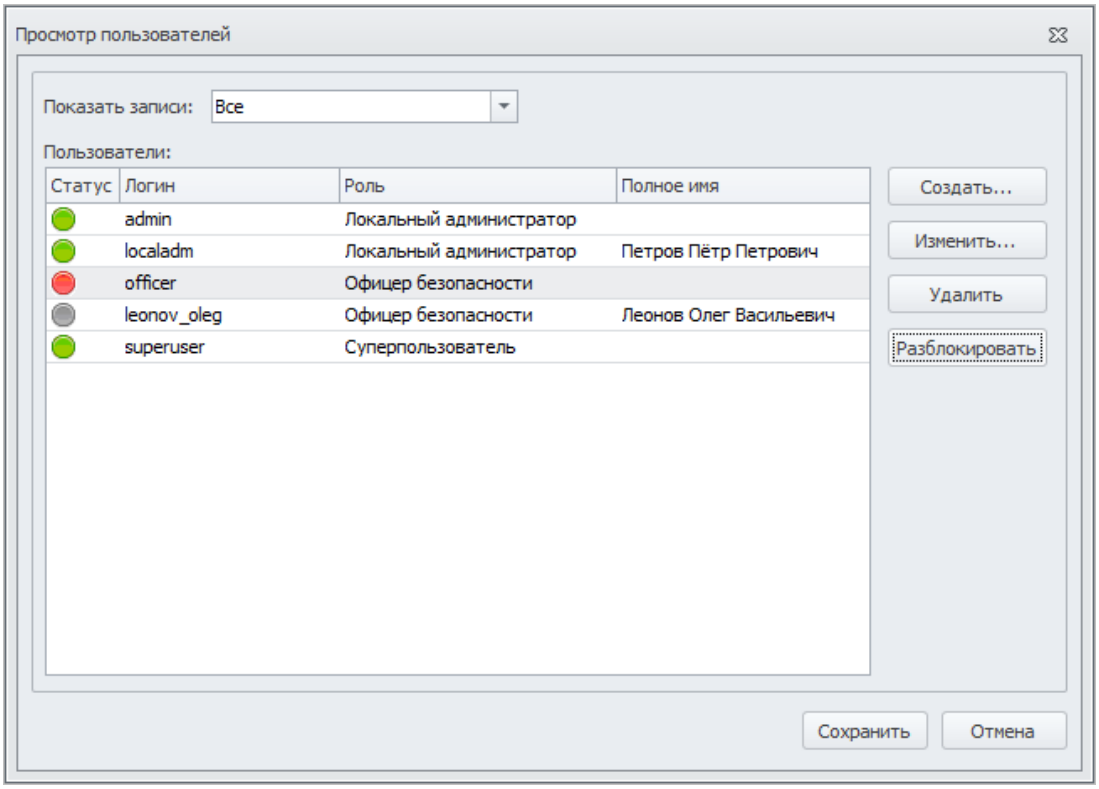
Более подробная информация о порядке управления учетными записями Консоли управления содержится в подразделах:

- Просмотр сведений об учетных записях Консоли управления
- Добавление учетной записи пользователя Консоли управления
- Блокирование и разблокирование учетной записи Консоли управления
- Редактирование учетной записи Консоли управления
- Удаление учетной записи Консоли управления
- Аудит действий по управлению схемой безопасности в Консоли управления

3.2.1 Просмотр сведений об учетных записях Консоли управления

Чтобы просмотреть информацию об учетных записях Консоли управления:

1. В главном меню выберите команду **Инструменты > Пользователи консоли**. На экран будет выведено диалоговое окно **Просмотр пользователей**.



2. В верхней части данного окна расположено поле **Показать записи**. Из раскрывающегося списка в этом поле выберите тип отображаемых учетных записей:
   - **Все**. Все учетные аписи, 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 и не подлежать восстановлению. Однако информация о действиях, которые эти пользователи выполнили, в Системе сохраняется.

> **Примечание:**
> Работа с Консолью управления может осуществляться от имени тех учетных записей, которые находятся в списке **Активные**. Удаленные учетные записи выводятся только для просмотра.

Сведения об учетных записях Консоли управления представлены в виде табличного списка. Каждая строка соответствует одной учетной записи. В столбцах отображаются значения следующих атрибутов учетных записей:

- **Статус.** Признак того, является ли учетная запись активной (), заблокированной () или удалённой ().
- **Логин**. Имя учетной записи.
- **Роль**. Роль, назначенная учетной записи.
- **Полное имя**. Фамилия, имя и отчество пользователя.

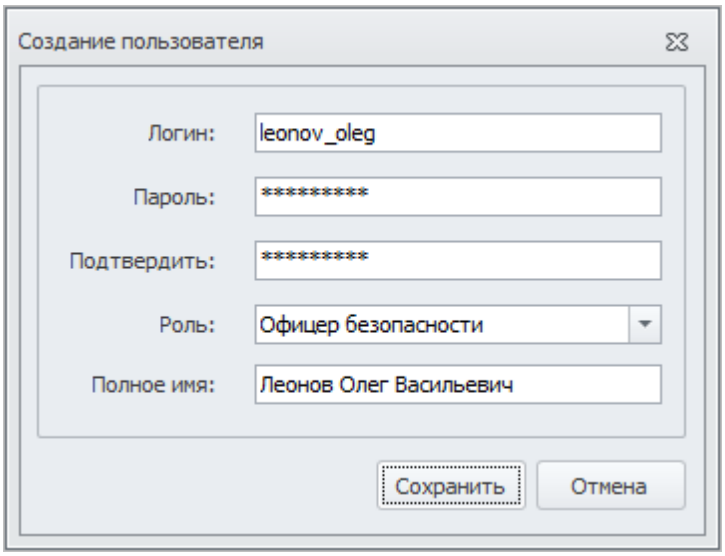
Обязательными атрибутами учетной записи являются имя и пароль, а также роль и признак блокирования. Подробное описание ролей вы можете найти в разделе "Администрирование учетных записей Консоли

управления".

3.2.2 Добавление учетной записи Консоли управления

Чтобы добавить учетную запись Консоли управления:

1. В главном меню выберите команду **Инструменты > Пользователи консоли**.
2. Нажмите на кнопку **Создать**, расположенную в правой части диалогового окна **Просмотр пользователей**.
3. В открывшемся диалоговом окне введите параметры учетной записи:



- **Логин**. Имя учетной записи.
- **Пароль**, **Подтвердить**. Пароль учетной записи.
- **Роль**. Роль, которая будет назначена данной учетной записи. Подробно о ролях см. раздел "Администрирование учетных записей Консоли управления".

> **Внимание!**
> Параметр **Роль** по умолчанию имеет значение **Нет роли**. Авторизация в Консоли управления с использованием данных такой учетной записи будет невозможна.
> Каждой учетной записи может быть назначена только одна роль.

- **Полное имя**. Фамилия, имя и отчество пользователя.

4. Нажмите **Сохранить**.
   После этого диалоговое окно **Настройка учетной записи** будет закрыто. Сведения о новой учетной записи появятся в диалоговом окне **Просмотр пользователей**.

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

3.2.3 Блокирование и разблокирование учетной записи Консоли управления

Сведения о состоянии блокировки учетных записей отображаются в диалоговом окне **Просмотр пользователей**.

Внимание!
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**. На экран будет выведено диалоговое окно **Просмотр пользователей**.
2. Выделите строку с названием нужной учетной записи.
3. Измените состояние блокировки учетной записи:

- Если учетная запись была заблокирована (статус ), нажмите на кнопку **Разблокировать**.
- Если учетная запись была разблокирована (статус ), нажмите на кнопку **Заблокировать**.

4. Чтобы сделанные изменения окончательно вступили в силу, нажмите на кнопку **Сохранить** в диалоговом окне **Просмотр пользователей**.

3.2.4 Редактирование учетной записи Консоли управления

Внимание!
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 несохраненные данные будут утеряны.

Чтобы отредактировать параметры учетной записи Консоли управления:

1. В главном меню выберите команду **Инструменты > Пользователи консоли**. На экран будет выведено диалоговое окно **Просмотр пользователей**.
2. Выделите 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, как описано 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 **Просмотр пользователей**.

3.2.5 Удаление учетной записи Консоли управления

После удаления учетная запись перемещается в список удаленных учетных записей. При этом сведения об учетной записи сохраняются в базе данных. Удаленные учетные записи можно просматривать в диалоговом окне **Учетные записи консоли управления**. Для этого нужно выбрать значение **Устаревшие** из раскрывающегося списка в поле **Учетные записи**.

Внимание!
Учетная запись Суперпользователя не может быть удалена.
Удаленные учетные записи не могут быть восстановлены для повторного использования.

Чтобы удалить учетную запись Консоли управления:

1. В главном меню выберите команду **Инструменты > Пользователи консоли**. На экран будет выведено диалоговое окно **Просмотр пользователей**.
2. Выделите 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 окончательно вступили в силу, нажмите на кнопку **Сохранить** в диалоговом окне **Просмотр пользователей**.

3.2.6 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, администрированием 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

3.2.6.1 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 выделите 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
Время	Дата и время выполнения действия
Объект	Название объекта, над которым выполнялось действие
Действие	Тип действия
Селектор	Содержит информацию, позволяющую однозначно идентифицировать объект, над которым было выполнено действие. Расшифровка значений параметра **Селектор** приводится 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, выполнившего транзакцию
Учетная запись Windows	Учетная запись, с данными которой пользователь авторизован в Windows
Рабочая станция	Название рабочей станции, на которой было выполнено действие
Порядковый номер	Порядковый номер, присвоенный этой записи, в базе данных

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 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 из шагов 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.

3.2.6.1.1 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 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*.

3.2.6.2 Фильтрация записей в журнале аудита

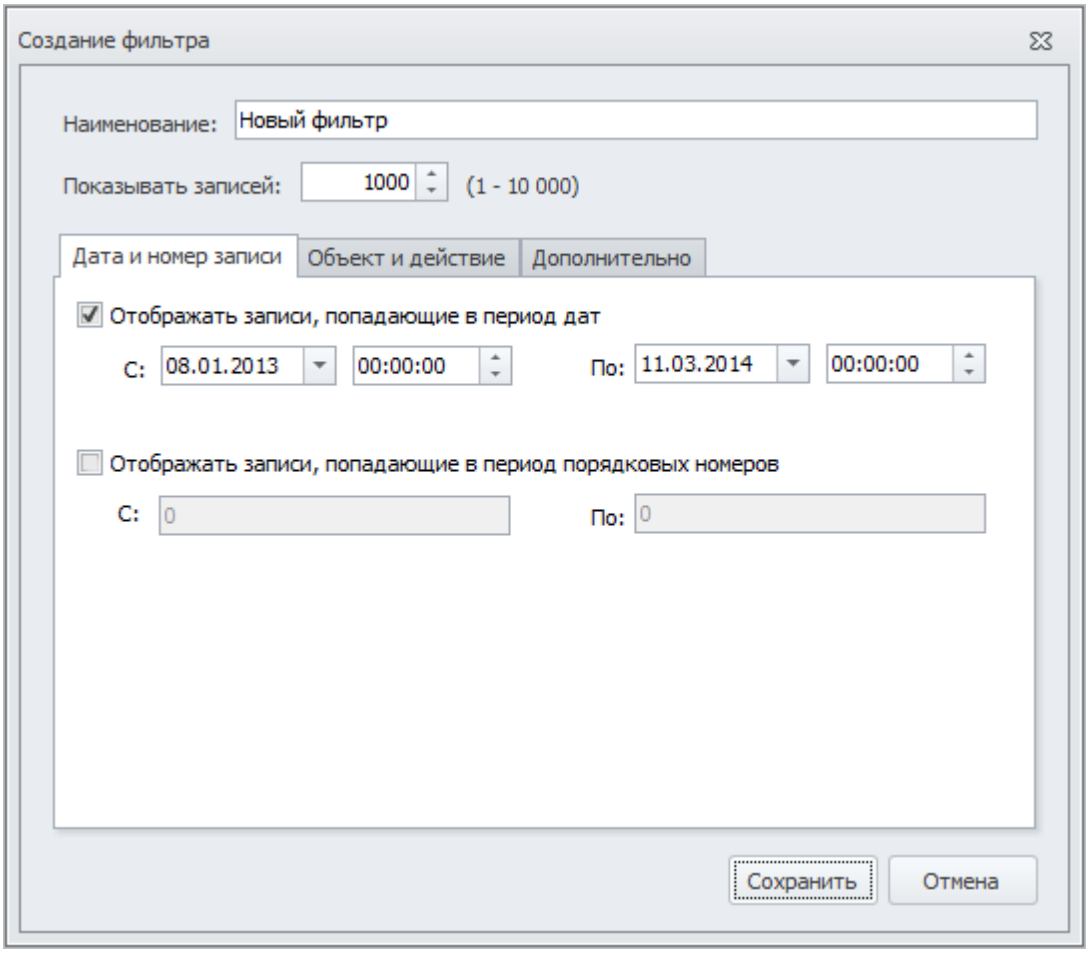
Для получения доступа к записям, удовлетворяющим определенным критериям, вы можете воспользоваться функциями фильтрации.

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.
Редактирование фильтра	1. В области **Журнал** на Панели навигации выделите 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.

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

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

3.2.6.2.1 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. Установите флажок в 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:

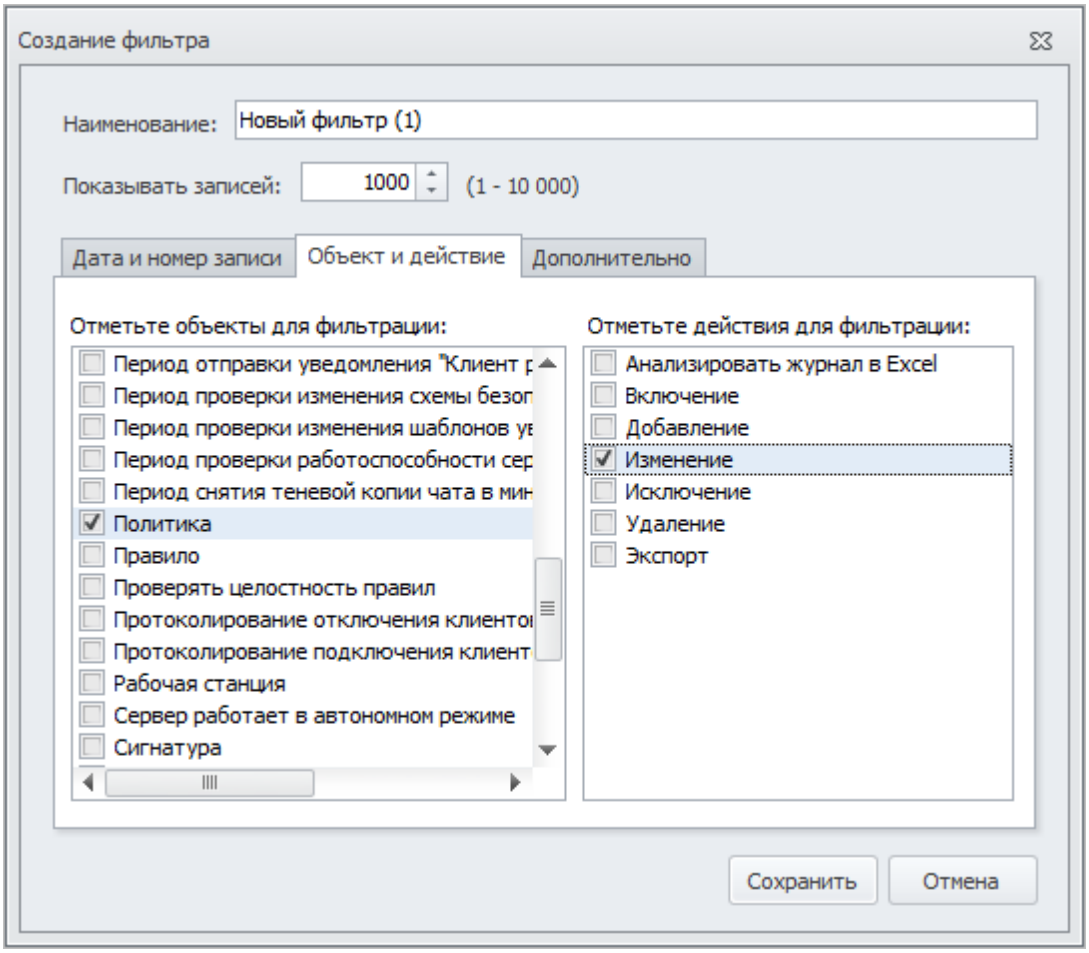
1. Установите флажок в поле **Отображать записи, попадающие в период порядковых номеров**.
2. Укажите диапазон порядковых номеров в полях **С** и **По** соответственно.

   Отсчет порядковых номеров записей в базе данных ведется со значения 1.

3.2.6.2.2 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 установите флажки рядом с объектами, по которым нужно выполнить фильтрацию.

2. Задайте условия фильтрации по действию. Для этого в правом столбце установите флажки рядом с действиями, по которым нужно выполнить фильтрацию.

3.2.6.2.3 Вкладка Дополнительно

На вкладке **Дополнительно** настраивают фильтрацию по некоторым дополнительным параметрам. К таким параметрам относятся:

- **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.
- **Рабочая станция**. Вывод списка записей о действиях, выполненных на указанной рабочей станции.

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

Примечание:
Значение дополнительного параметра фильтрации вводится без учета регистра символов.

3.2.6.3 Удаление записей из журнала аудита

Внимание!
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.

   Внимание!
   Обратите внимание, что из журнала аудита будут удалены записи, относящиеся к указанной транзакции и записи, относящиеся ко всем предыдущим транзакциям.
3. Нажмите на кнопку **OK**.

3.2.6.4 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**.

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.

3.2.6.5 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.

3.3 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 Клиентов
- Контроль сетевых соединений
- Контроль сетевого трафика
- Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor
- Соединение с сервером LDAP
- Настройка уведомлений сотрудников о нарушении правил

Внимание!

Измененные настройки вступят в силу на контролируемых рабочих станциях сразу же после того, как Клиенты на каждой рабочей станции, получив уведомление от Сервера (при проверке работоспособности сервера, или при проверке изменения схемы безопасности, или при проверке изменения шаблонов уведомлений), выполнят обновление.

3.3.1 Общие настройки работы Клиентов

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

Чтобы настроить общие настройки работы Клиентов 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 клиента каждые	Периодичность, с которой Клиент отправляет на сервер уведомления о своей работе, в секундах.
Проверять работоспособность сервера каждые	Периодичность, с которой Клиент выполняет проверку доступности сервера, в секундах.
Проверять изменения схемы безопасности каждые	Если Клиент работает в активном режиме (т.е. на рабочей станции не удалось открыть UDP-порт для получения уведомлений от Сервера), то Клиент сам опрашивает Сервер об изменениях схемы безопасности с указанной периодичностью, в секундах.
Проверять изменения шаблонов уведомлений для активных клиентов каждые	Если Клиент работает в активном режиме (т.е. на рабочей станции не удалось открыть UDP-порт для получения уведомлений от Сервера), то Клиент сам опрашивает Сервер об изменениях шаблонов уведомлений (см. "Настройка уведомлений сотрудников о нарушении правил") с указанной периодичностью, в секундах.
Контроль дискового пространства на клиентах	
Минимальное свободное пространство на клиенте	Минимальный размер свободного пространства (в процентах) на контролируемой рабочей станции, при достижении которого, теневые копии не будут создаваться. Т.е. если при создании теневой копии свободного пространства на клиенте останется меньше чем указано, то копия создаваться не будет; частичной копии также не будет. Подробнее см. "Создание теневых копий и запрет операций при нехватке свободного пространства на контролируемых рабочих станциях"
Если место под события на диске закончилось	На том диске контролируемой рабочей станции, куда выполняется установке Клиента Device Monitor, выделяется место, достаточное для хранения информации о 30000 событиях. Если Клиент Device Monitor настолько долго не имел связи с сервером Device Monitor, что накопилось более 30000 событий, контролируемых правилами, определёнными для сотрудника/рабочей станции, то любые действия, контролируемые текущей политикой безопасности, могут быть запрещены. Чтобы запретить, выберите **Запрещена операция**. Чтобы все действия могли неконтролируемо выполняться, выберите **Разрешена операция**.
События	
Логировать события от перехватчика устройств	Степень детализации при сохранении сведений о работе с внешними устройствами, получаемых перехватчиком Device Monitor: подробнее см. "Настройка правила для Device Monitor" и "Просмотр событий". Возможен один из следующих вариантов: • **Не логировать** - события не сохраняются;

Параметр	Описание
	• **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** - сохраняются сведения обо всех действиях (подключение/использование любых устройств, даже занесенных в белые списки)
Логировать соединения вне корпоративной сети	Степень детализации при сохранении сведений о передаче данных по сетевым соединениям, получаемых перехватчиком Network Monitor: подробнее см. "Настройка правила 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.
Уведомление сотрудника	
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"
Отображать иконку в трее	Признак того, что в области уведомлений панели задач Windows на компьютере, где установлен Клиент, будет отображаться значок . При нажатии на этот значок доступна информация о работе Клиента, а также список контролируемых в данный момент устройств.

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

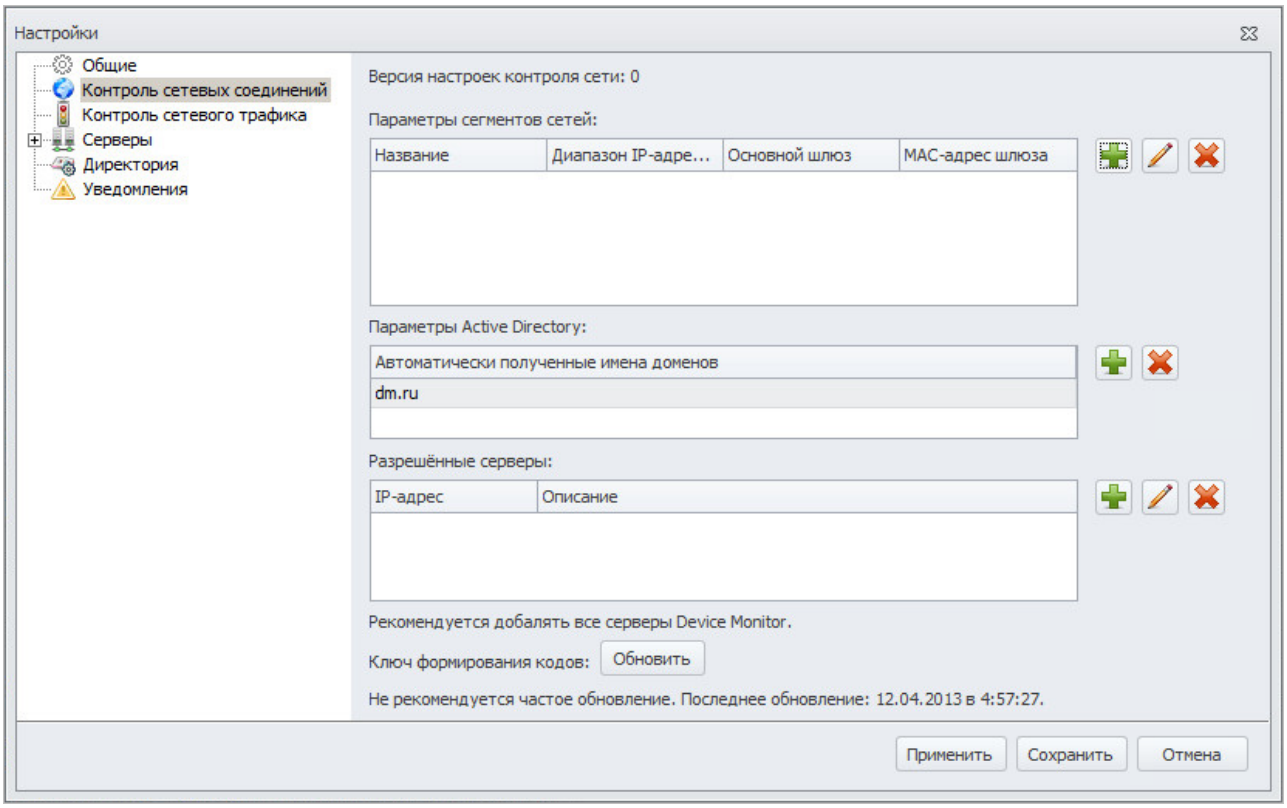
3.3.2 Контроль сетевых соединений

Для обеспечения контроля передачи данных по сетевым соединениям с помощью **Network Monitor** (о настройке правил для данного типа контроля см. "Настройка правила 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 клиент находится вне корпоративной сети, например с VPN сервером или корпоративной почтой.

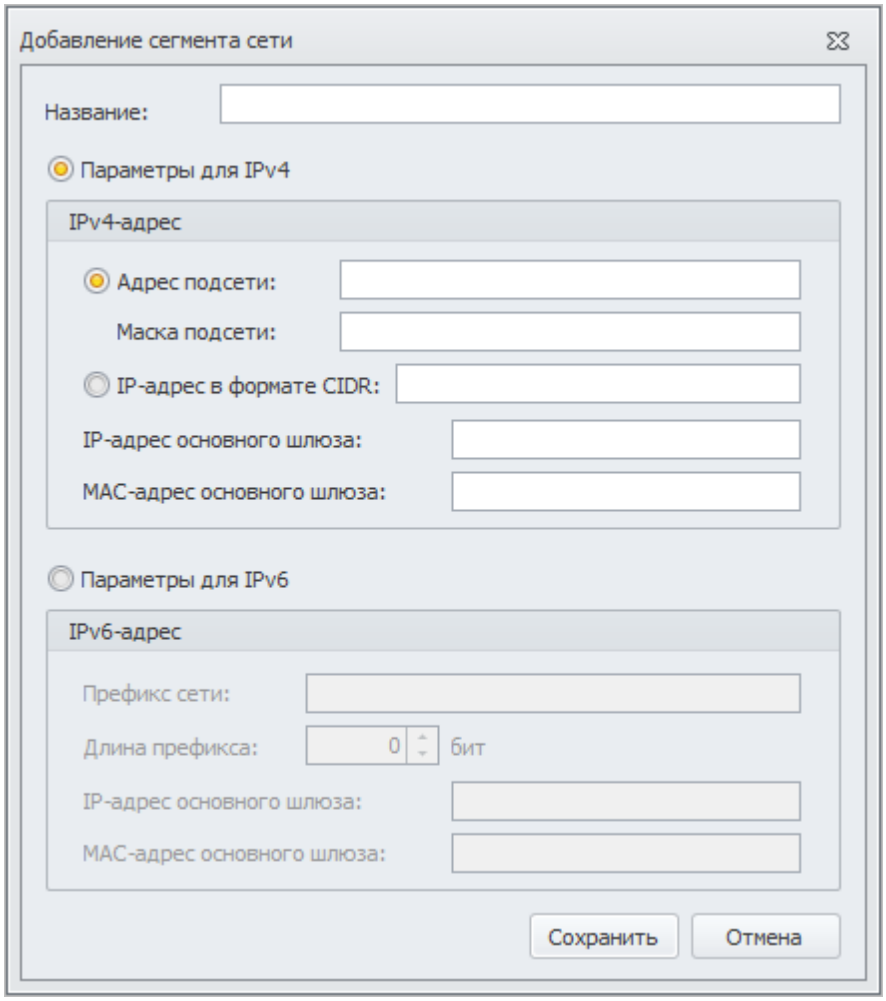
Чтобы настроить параметры контроля сетевых соединений:

1. В главном меню выберите команду **Инструменты > Настройки**.
2. На левой панели выберите **Контроль сетевых соединений**.



3. Чтобы задать параметры сегментов сетей:

   a. В области **Параметры сегментов сетей** нажмите . 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 **OK**.

e. Повторите действия для добавления других сегментов.

Чтобы изменить параметры сегмента, в области **Параметры сегментов сетей** выберите его в списке и нажмите .

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

4. Чтобы определить 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 .

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

6. Вы также можете обновить ключ формирования кодов временного доступа (см. "Предоставление сотруднику временного доступа"). Для этого нажмите **Обновить**.
7. Чтобы внесенные изменения вступили в действие, нажмите **Применить**.

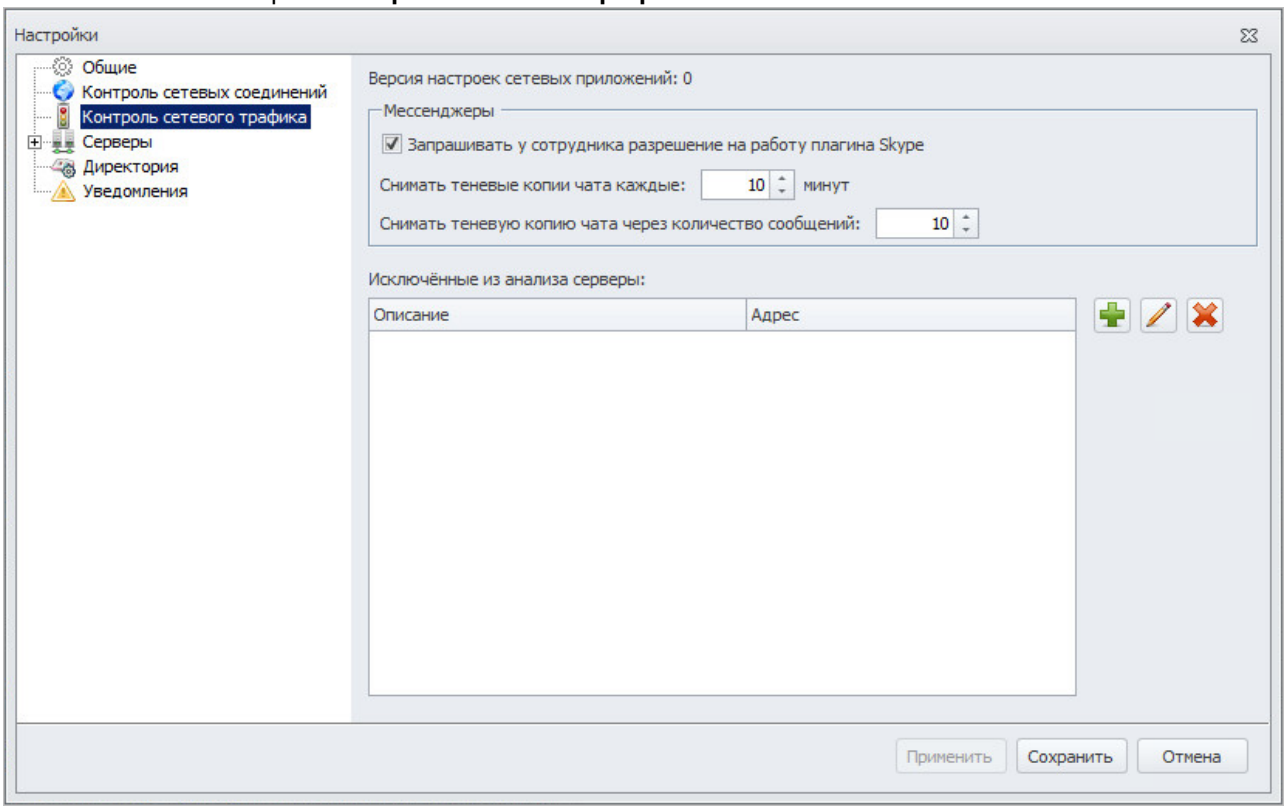
3.3.3 Контроль сетевого трафика

Для контроля сетевого трафика, передаваемого через по протоколам XMPP, MMP и FTP в Клиенте Device Monitor реализован прозрачный прокси-сервер, на который перенаправляются все соединения (не важно, относятся они к контролируемым протоколам или нет). Далее Клиенте Device Monitor разбирает протокол и определяет, относится ли данный протокол к перехватываемым; если поток данных защищён с использованием протокола TLS\SSL, то прокси-сервер строит атаку "Человек посередине" (Man in the middle) для открытия трафика и также определяет, нужно ли контролировать данный поток.

При контроле трафика вы можете задать некоторые дополнительные параметры работы с системами мгновенного обмена сообщениями (о настройке правил для данного типа контроля см. "Настройка правила для IM Client Monitor") и FTP-трафиком (см. "Настройка правила для FTP Monitor"), а также определить сервера-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 сетевого трафика**.



3. Укажите параметры контроля мессенджеров:
   - Если вы хотите, чтобы после установки Клиента сотруднику отображалось сообщение, запрашивающее разрешение на работу перехватчика, установите флажок в поле **Запрашивать у сотрудника разрешение на работу плагина**. Если флажок в данном поле не установлен, то подтверждения сотрудника при запуске перехватчика не требуется.

Внимание!

Чтобы разрешить контроль Skype, сотрудник должен войти в меню Skype: **Инструменты -> Настройки -> Дополнительно -> Контроль доступа других программ к Skype**, выбрать приложение **DM.Client.exe**, нажать **Изменить**, выбрать опцию **Разрешить этой программе пользоваться Skype** и нажать **ОК**.

- Если сотрудник разрешил работу перехватчика, то он будет работать до тех пор, пока сотрудник не запретит его работу в меню Skype. В последнем случае работа Skype будет принудительно остановлена.
- Если сотрудник запретил работу перехватчика, то работа Skype будет остановлена. При повторной попытке запуска Skype сотруднику опять будет предложено дать разрешение на использование перехватчика.

- 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 (**Снимать теневую копию чата каждые**), так и количество сообщений, по достижении которого будет сформирована теневая копия (**Снимать теневую копию чата через количество сообщений**).
  Если в чате осуществляется отправка файла, то теневая копия может формироваться раньше достижения указанного периода.
  Подробнее см. "Добавление правила для IM Client Monitor".

4. Вы можете задать перечень IP-адресов серверов, при соединении с которыми контроль протоколов проводиться не будет - то есть трафик на данные сервера не будет перенаправляться на внутренний прокси-сервер.

   Примечание:

   Разрешение внешних адресов может понадобиться, например, для обеспечения работы с внешними ресурсами и обновления установленных программ: так, для автоматического обновления Firefox в списке разрешенных серверов должны присутствовать **.mozilla.com* и **.mozilla.net*, а для работы dropbox - **.dropbox.com*.

   Чтобы задать список разрешенных серверов:

   a. В области **Укажите IP адреса...** нажмите .
   b. В диалоговом окне **Добавить разрешенный сервер** введите DNS имя или IP-адрес сервера, а также его описание.
   c. Нажмите **ОК**.
   d. Повторите действия для других разрешенных адресов.

   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.

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

Внимание!

При использовании на компьютере с установленным клиентом Device Monitor программного обеспечения Yandex Disk, в список исключенных из анализа серверов следует внести следующие сервера:

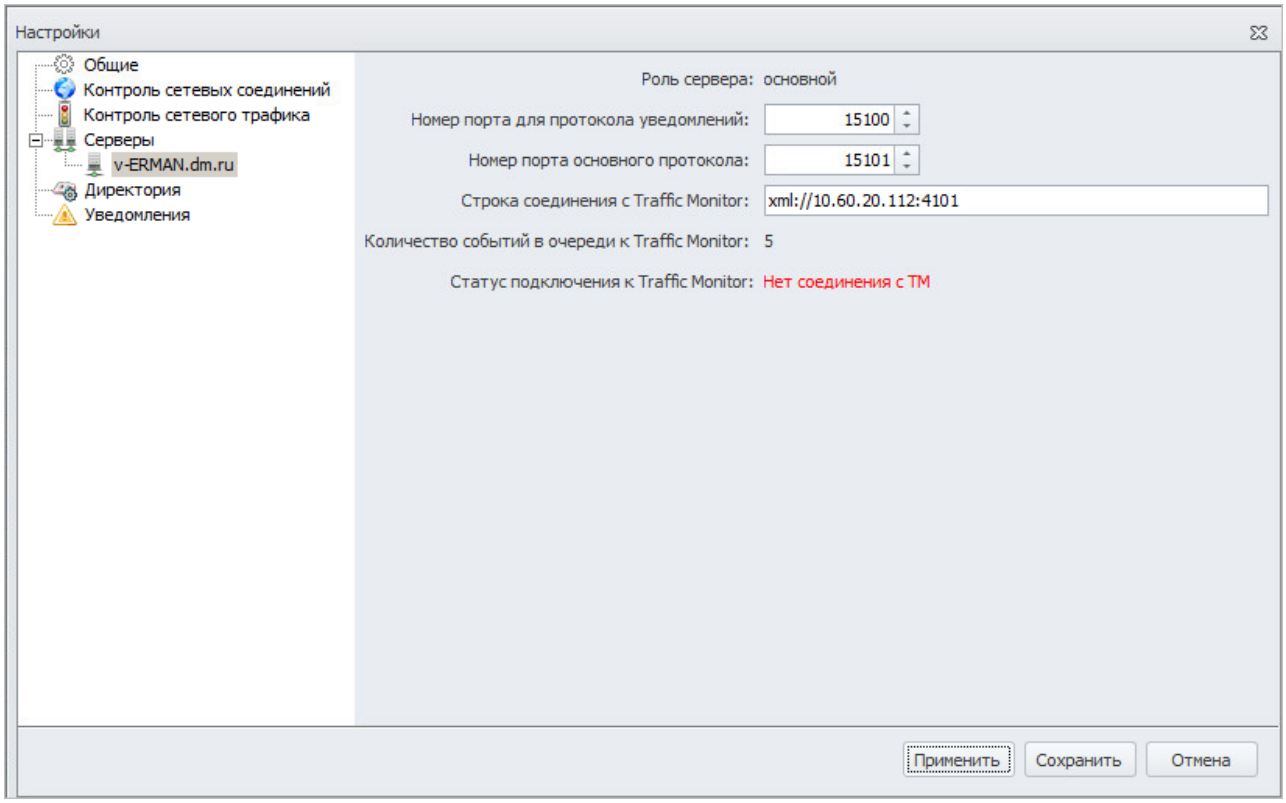
- oauth.yandex.ru;
- webdav.yandex.ru;
- clck.yandex.ru;
- push.xmpp.yandex.ru.

3.3.4 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** выберите имя необходимого сервера.



Будет выведена 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, Шаг 4.
- **Количество событий в очереди к Traffic Monitor** – статистика по событиям, ожидающим отправки в систему InfoWatch Traffic Monitor.
- **Статус подключения к Traffic Monitor**.

3. Вы можете изменить следующие параметры:
   - **Номер порта для протокола уведомлений**
   - **Номер порта основного протокола**

> **Внимание!**
> Измененния портов протоколов вступят в силу только после перезапуска сервиса.

- **Строка соединения с Traffic Monitor** – адрес сервера InfoWatch Traffic Monitor, на который будут доставляться события. Взаимодействие с сервером Traffic Monitor осуществляется по схеме *xml*. Запись адреса должна иметь следующий формат:

```
xml://host:port
```

Параметр *host* должен содержать доменное имя или IP-адрес сервера InfoWatch Traffic Monitor. Адрес сервера является стандартным URI-адресом (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 – 4101.

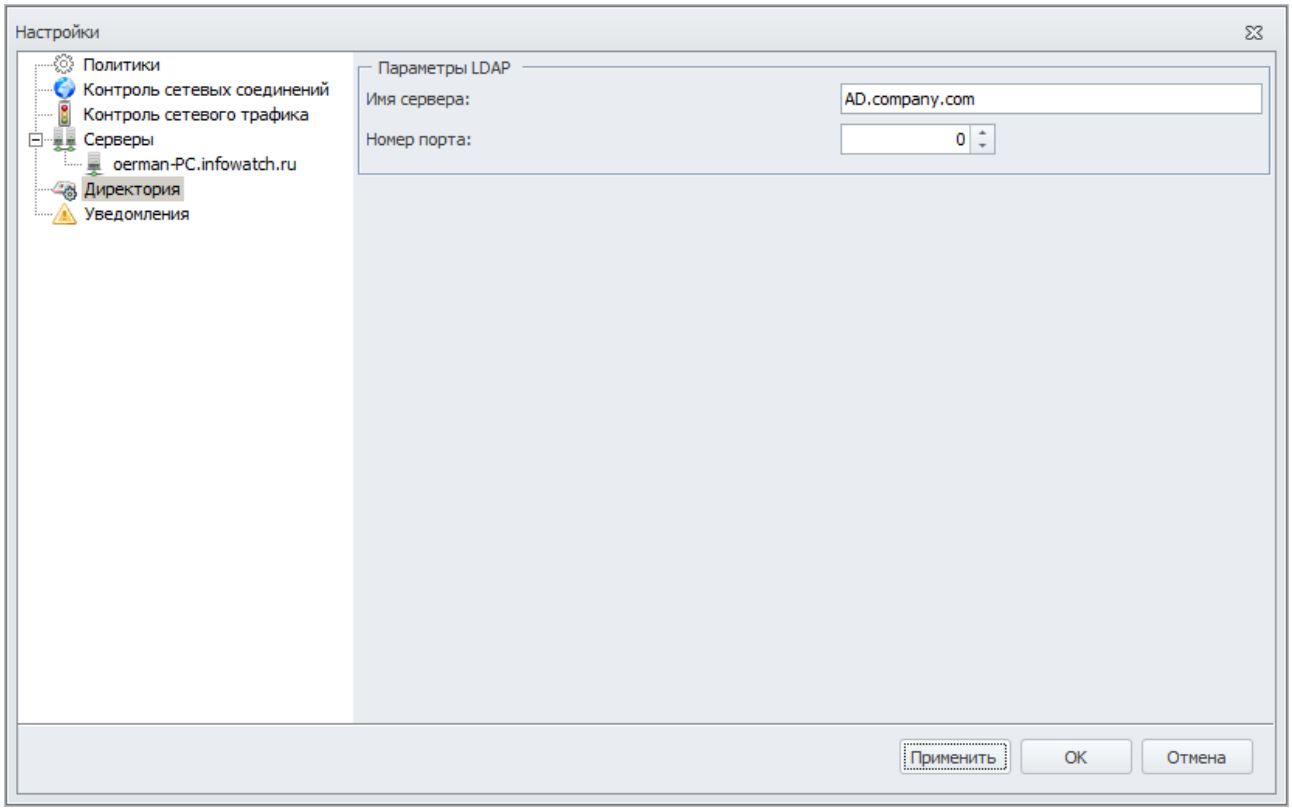
4. Нажмите на кнопку **OK**.

3.3.5 Соединение с сервером LDAP

Для того чтобы получать информацию о рабочих станциях и сотрудниках из служб каталогов, необходимо настроить параметры соединения с сервером LDAP.

Чтобы просмотреть и настроить параметры соединения с сервером LDAP:

1. В главном меню Консоли управления выберите команду **Инструменты > Настройки**.
2. Откройте узел **Директория**.
3. В поле **Имя сервера** укажите доменное имя или IP-адрес сервера LDAP.
4. При необходимости, укажите порт, к которому будут выполняться запросы в тех случаях, когда порт, используемый по умолчанию (389), недоступен.



5. Нажмите на кнопку **OK**.

3.3.6 Настройка уведомлений сотрудников о нарушении правил

Если на контролируемой рабочей станции сотрудник пытается выполнить действие, запрещенное политикой безопасности, то отображается уведомление о запрете. Уведомления отображаются в тех случаях, когда происходят следующие события:

- **Запрет доступа к устройству** – сработало правило Device Monitor, запрещающее чтение и запись на устройство (см. "Настройка правила для Device Monitor");
- **Запрет записи на устройство** – сработало правило Device Monitor, запрещающее запись на устройство (см. "Настройка правила для Device Monitor");
- **Запрет записи в открытую область** – сработало правило Device Monitor, запрещающее запись на незашифрованные флоппи-дисководы и съемные устройства (см. "Настройка правила для Device Monitor");

- **Запрет копирования/печати файла, если места для событий недостаточно** – если Клиент 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 Клиентов"), то запрещаются любые операции, контролируемые текущей политикой безопасности.
- **Запрет передачи данных по сетевым протоколам** – сработало правило FTP Monitor или IM Client Monitor, запрещающее обмен данными через протокол FTP/XMPP/MPP/Skype (см. "Настройка правила для FTP Monitor" и "Настройка правила для IM Client Monitor").
- **Запрет передачи данных по сетевым протоколам, если места для событий недостаточно** – если Клиент 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 Клиентов"), то запрещаются любые операции, контролируемые текущей политикой безопасности.
- **Запрет Skype из-за запрета сотрудником плагина Skype** – сработало правило IM Client Monitor, контролирующее использование Skype (см. "Настройка правила для IM Client Monitor", а также "Контроль сетевого трафика", настройка **Запрашивать у сотрудника разрешение на работу плагина**).
- **Запрет сетевого подключения. Сокращенное** – сработало правило Network Monitor, запрещающее передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами (см. "Настройка правила для Network Monitor")
- **Запрет сетевого подключени. Детализированное** – 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. "Настройка правила для Network Monitor" и "Предоставление сотруднику временного доступа").

Чтобы полностью отключить отображение уведомлений сотрудникам, или включить его обратно:

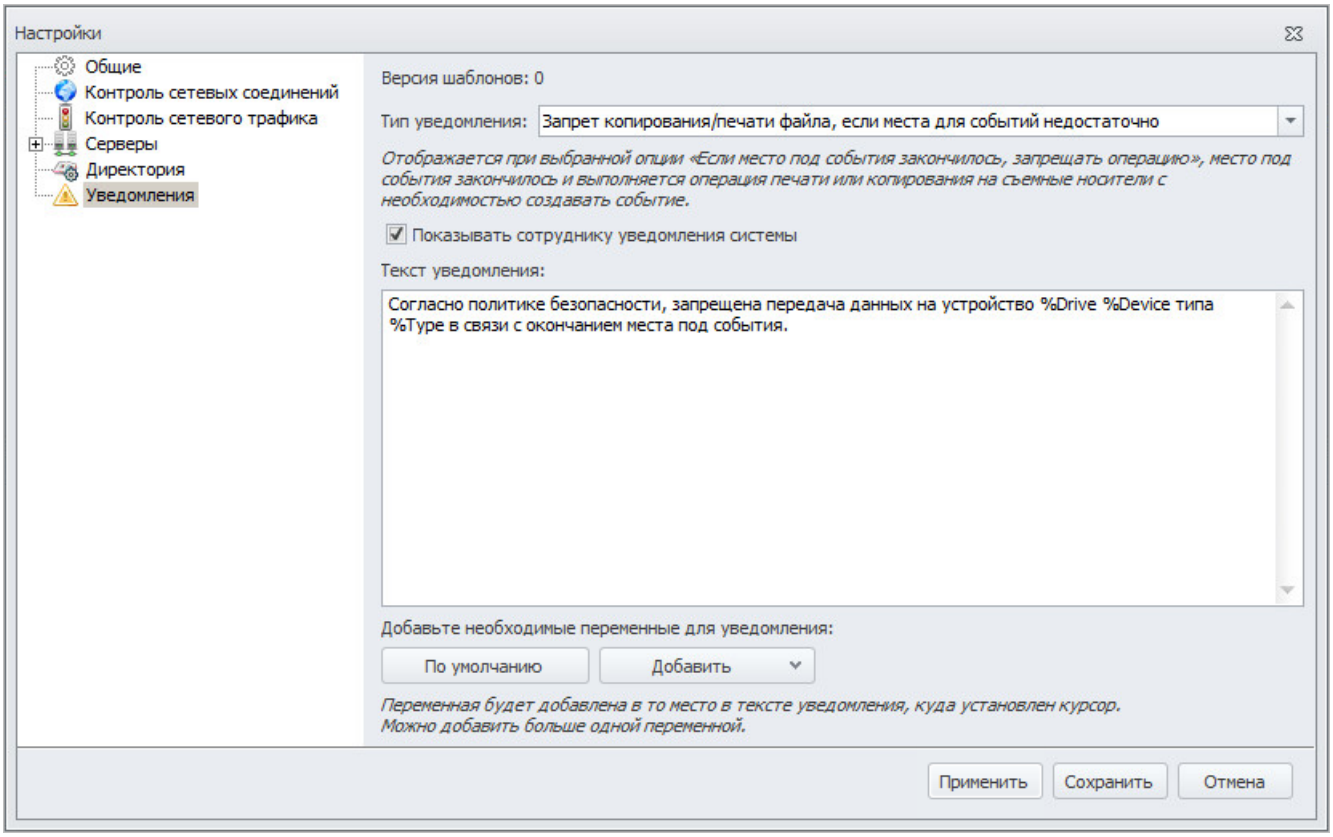
1. Выберите команду **Инструменты > Настройки** из главного меню.
   На экран будет выведено диалоговое окно **Настройки**.
2. На левой панели выберите **Общие**.
3. В поле **Отображать уведомления сотруднику** снимите флажок - чтобы отключить отображение уведомлений сотрудникам, или установите его - чтобы включить уведомления.
4. Нажмите **OK**.

При необходимости, вы можете изменить текст уведомлений, а также отключить отображение любого типа уведомлений, или включить отображение обратно.

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

Чтобы изменить текст уведомлений:

1. Выберите команду **Инструменты > Настройки** из главного меню.
   На экран будет выведено диалоговое окно **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, установите (снимите) флажок **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, щелкните **По умолчанию**.
6. Нажмите **Применить**. При необходимости, измените настройки для других уведомлений, повторяя шаги 2-5.
7. После того, как сделаны все необходимые изменения, нажмите **ОК**.

3.4 Управление схемой безопасности

В этой главе содержится следующая информация:

- Общие принципы работы со схемой безопасности
- Настройка схемы безопасности
- Предоставление сотруднику временного доступа

3.4.1 Общие принципы работы со 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 схемы безопасности

Общие сведения о схеме безопасности содержатся в разделе "Принципы организации схемы безопасности".

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

3.4.1.1 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 рабочих станций**, **Белые списки** и **Категрии 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 рабочих станций «по умолчанию»
	Группа рабочих станций
	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 рабочей станции
	Белый список устройств для группы рабочих станций
	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 выделите 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.

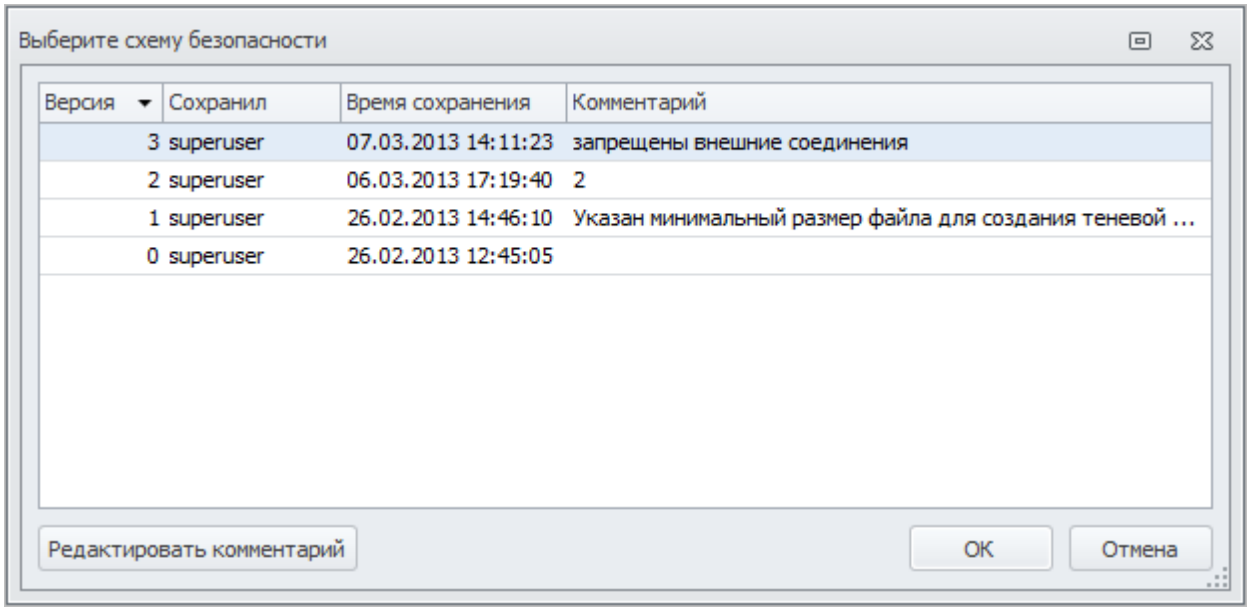
Примечание:
В процессе работы вы можете настраивать отображение элементов главного окна по своему усмотрению (см. "Настройка элементов главного окна").

3.4.1.2 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. раздел "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** выделите строку с номером той версии схемы безопасности, которую нужно просмотреть.
3. Нажмите на кнопку **OK**.

После нажатия кнопки **OK** указанная версия схемы безопасности будет загружена в Консоль управления. 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**.

3.4.1.3 Комментарии к схеме безопасности

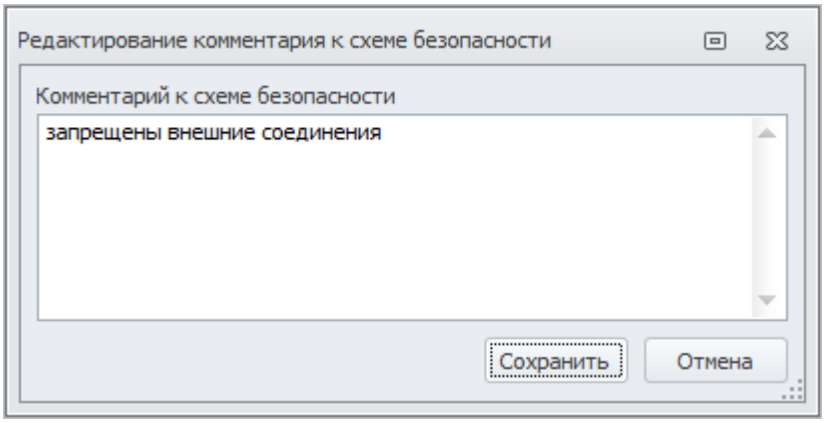
Вы можете указывать дополнительную информацию по схеме безопасности в виде комментария.
Комментариями может сопровождаться каждая версия схемы безопасности.
Комментарий к текущей схеме безопасности выводится на панели статуса, в скобках справа от номера версии схемы безопасности.
Комментарии ко всем 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 выделите строку с нужной версией схемы безопасности. Затем нажмите на кнопку **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.

   Примечание:
   Для перевода строки в тексте комментария, нажмите сочетание клавиш **<CTRL>+<ENTER>**.

3. Нажмите на кнопку **Сохранить**.

3.4.1.4 Редактирование схемы безопасности

Внимание!
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**.

Внимание!
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, рабочие станции, 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 > Смотреть последнюю схему безопасности** 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 рабочих станций (см. "Рабочие станции");
   - 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 рабочеё 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 рабочеё области, где отображается сообщение "*В схему безопасности были внесены изменения...*" нажмите **Откатить**;
- 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.

3.4.1.4.1 Блокировка схемы безопасности

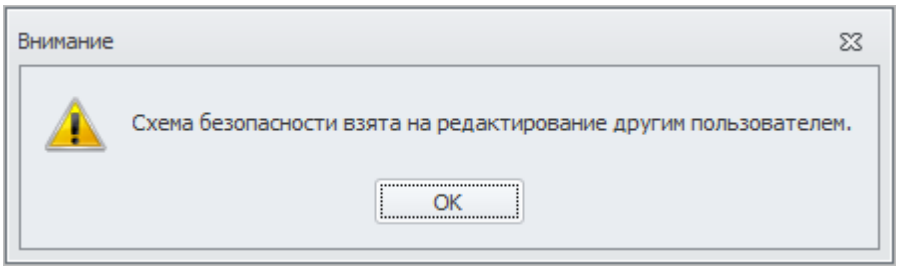
В каждый момент схема безопасности может редактироваться только одним пользователем. Внесенные изменения фиксируются только после того, как схема безопасности будет сохранена.

Когда схема безопасности уже редактируется другим пользователем, это отображается на панели,

расположенной в верхней части главного окна.

Если вы попытаетесь изменить какие-либо параметры схемы (политики безопасности, рабочие станции, сотрудники, белые списки устройств, категории сигнатур) в то время, когда схема безопасности взята на редактирование другим пользователем:

1. В Консоли управления будет отображено уведомляющее сообщение.



2. Когда другой пользователь сохранит свои изменения (или отменит их), 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, который заблокировал схему, опять подключится к серверу, схема безопасности будет автоматически разблокирована, а все несохранённые изменения, сделанные этим пользователем, - утеряны.

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

Внимание!
Разблокировать схему безопасности может только Суперпользователь.

Чтобы разблокировать схему безопасности,

в главном меню выберите команду **Схема безопасности > Разблокировать**.

Все несохраненные изменения схемы безопасности будут утеряны.

3.4.1.5 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:

- зарегистрирована новая рабочая станция;
- 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.

3.4.1.6 Экспорт/импорт схемы безопасности

В процессе работы могут возникнуть ситуации, когда вам потребуется сохранить имеющиеся настройки схемы безопасности. Необходимость в этом может возникнуть, например, при переустановке операционной системы или самой системы InfoWatch Device Monitor.
Функция экспорта схемы безопасности дает возможность сохранить в виде XML-файла текущую версию схемы безопасности, включая:

- политики безопасности с наборами правил;
- группы сотрудников;
- группы рабочих станций;
- белые списки устройств;
- категории сигнатур.

Впоследствии сохраненные настройки могут быть импортированы в новую схему безопасности.

Чтобы экспортировать схему безопасности:

1. В главном меню выберите команду **Схема безопасности > Экспортировать схему безопасности**.
2. В открывшемся диалоговом окне задайте имя XML-файла, в который будут экспортированы данные, и выберите каталог для хранения файла. После того как имя и каталог для файла будут заданы, нажмите на кнопку **Сохранить**.

Чтобы импортировать схему безопасности:

1. В главном меню выберите команду **Схема безопасности > Импортировать схему безопасности**.
2. В открывшемся диалоговом окне выберите XML-файл, в котором хранится сохранённая схема, и нажмите на кнопку **Открыть**.

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

3.4.2 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 рабочих станций «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 рабочих станций, которой будет назначена эта политика безопасности.
- Каждой группе сотрудников и группе рабочих станций рекомендуется назначать отдельную политику безопасности.
- Для каждой политики безопасности, которая назначается какой-либо группе, должен быть определен набор правил.

Особенности добавления рабочих станций в схему безопасности

Добавление контролируемых рабочих станций происходит одним из двух способов:

- автоматически при регистрации новой рабочей станции;
- вручную через Консоль управления.

Если рабочая станция зарегистрирована автоматически, то она включается в группу рабочих станций «по умолчанию». Затем она может быть добавлена в другие группы рабочих станций.

При добавлении вручную, рабочую станцию 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 контролируемой рабочей станции 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 создаётся белый список для конкретного сотрудника / группы сотрудников/ рабочей станции / группы рабочих станций, и определяется, какие устройства в него включены. Для этих сотрудников / рабочих станций 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
- Рабочие станции
- Белые списки
- Категории сигнатур
- Предоставление сотруднику временного доступа
- Разблокирование схемы безопасности

3.4.2.1 Политики безопасности

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

Каждая политика безопасности состоит из набора правил, в соответствии с которыми определяется уровень доступа сотрудников к контролируемым файлам и устройствам.

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

3.4.2.1.1 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. главу "Дополнительные возможности").

Чтобы просмотреть правила, включенные в политику безопасности,

выделите 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 (зелёный), запрещающим (красный) или частично ограничивающим (жёлтый).

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

Чтобы просмотреть все свойства правила,

в рабочей области главного окна выделите строку с названием нужного правила.

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

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.

Для правил File Monitor выводятся дополнительные сведения:

- **Исключить из перехвата**. Признак того, что файлы, соответствующие маске или категории, будут исключены из обработки.
- **Использовать маску файла**. Признак использования маски файла.
- **Маска файла**. Маска, заданная для отбора файлов, подпадающих под правило.
- **Использовать категорию**. Признак фильтрации файлов в соответствии с категориями сигнатур (см. "Сигнатуры").
- **Категория**. Категория сигнатур для отбора файлов определенных форматов.
- **Создавать теневую копию**. Признак теневого копирования сохраняемых файлов.
- **Ограничивать по минимальному размеру файла**. Признак наличия ограничений на минимальный размер файла, для которого может быть создана теневая копия.
- **Минимальный размер файла**. Нижняя граница размера файла.
- **Ограничивать по максимальному размеру файла**. Признак ограничения на максимальный размер файла, для которого может быть создана теневая копия.
- **Максимальный размер файла**. Верхняя граница размера файла.

Для правил Print Monitor выводятся дополнительные сведения:

- **Использовать маску задания**. Признак использования маски задания.
- **Маска задания**. Маска, определенная для отбора заданий на печать, подпадающих под правило.
- **Использовать маску процесса**. Признак использования маски процесса.
- **Маска процесса**. Маска, заданная для процесса, посредством которого было инициировано задание на печать.
- **Создавать теневую копию**. Признак теневого копирования документа, отправленного на печать.

Для правил Device Monitor выводятся дополнительные сведения:

- **Разрешать только на зашифрованные носители**. Действие будет разрешено, если будет определено, что носитель защищён программой шифрования данных.

Для правил IM Client Monitor выводятся дополнительные сведения:

- **Создавать теневую копию аудиозвонка**. Признак создания теневой копии голосового трафика при

использовании Skype.

- **Создавать теневую копию файлов**. Признак теневого копирования пересылаемых файлов.
- **Минимальный размер файла**. Нижняя граница размера файла.
- **Максимальный размер файла**. Верхняя граница размера файла.
- **Максимальный размер файла разговора**. Размер разговора, в минутах, который будет сохраняться в одном файле и передаваться на сервер для дальнейшей обработки.

Для правил FTP Monitor выводятся дополнительные сведения:

- **Создавать теневую копию**. Признак теневого копирования документа, отправленного по FTP.
- **Минимальный размер файла**. Нижняя граница размера файла.
- **Максимальный размер файла**. Верхняя граница размера файла.

Для правил HTTPS Monitor выводятся дополнительные сведения:

- **Создавать теневую копию файла**. Признак теневого копирования документа, отправленного по FTP.
- **Минимальный размер запроса, Байт**. Нижняя граница размера запроса.
- **Максимальный размер запроса, МБайт**. Верхняя граница размера запроса.
- **Не перехватывать запросы на внутренние ресурсы**. Признак перехвата запросов на указанные ресурсы (см. "Контроль сетевых соединений").

Для правил Network Monitor выводятся дополнительные сведения:

- **Доступ**. Всегда имеет значение *Запрет соединений вне корпоративной сети*.

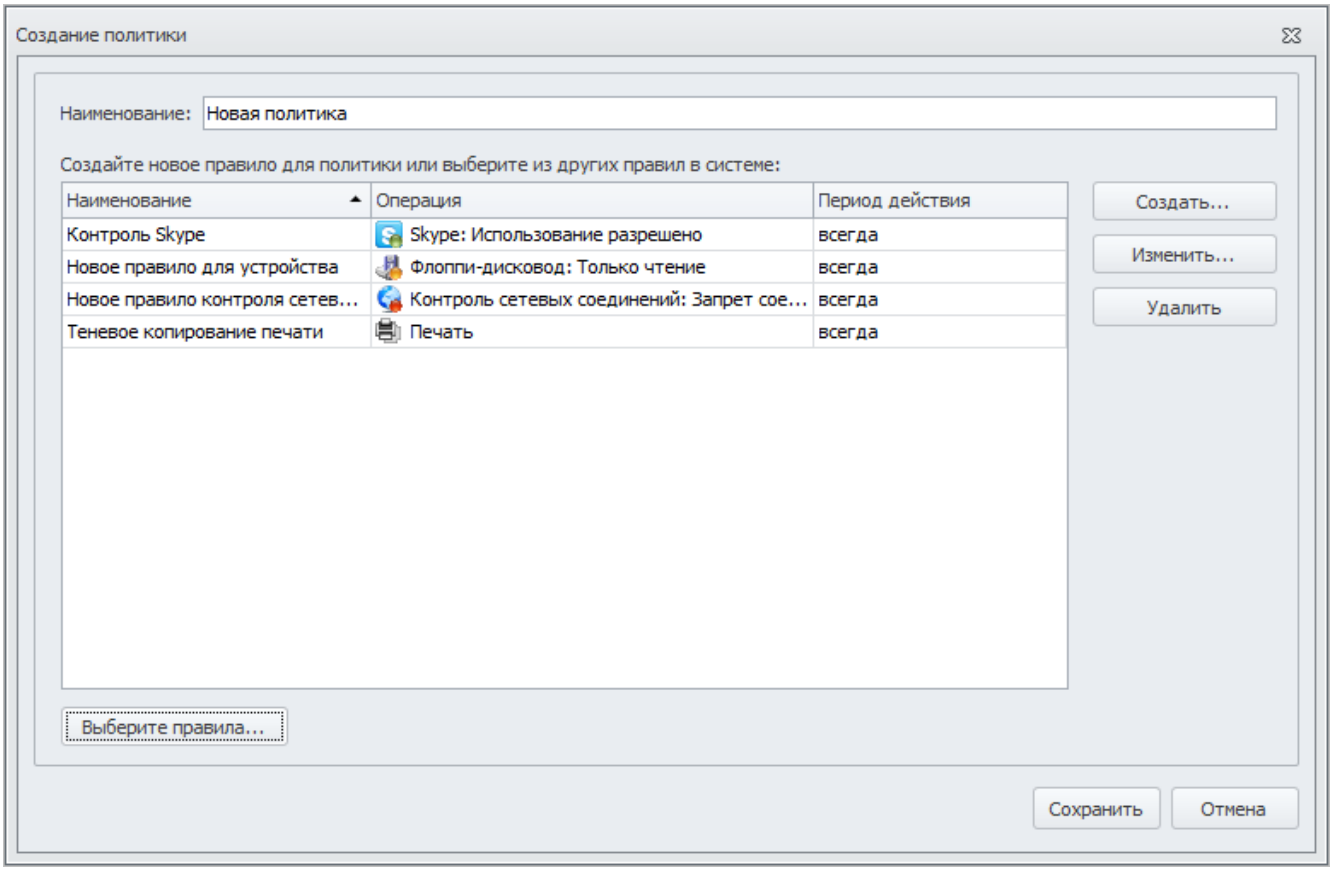
Примечание:
Информация, выводимая по некоторым свойствам, дублируется в рабочей области главного окна.

3.4.2.1.2 Создание и настройка политики безопасности

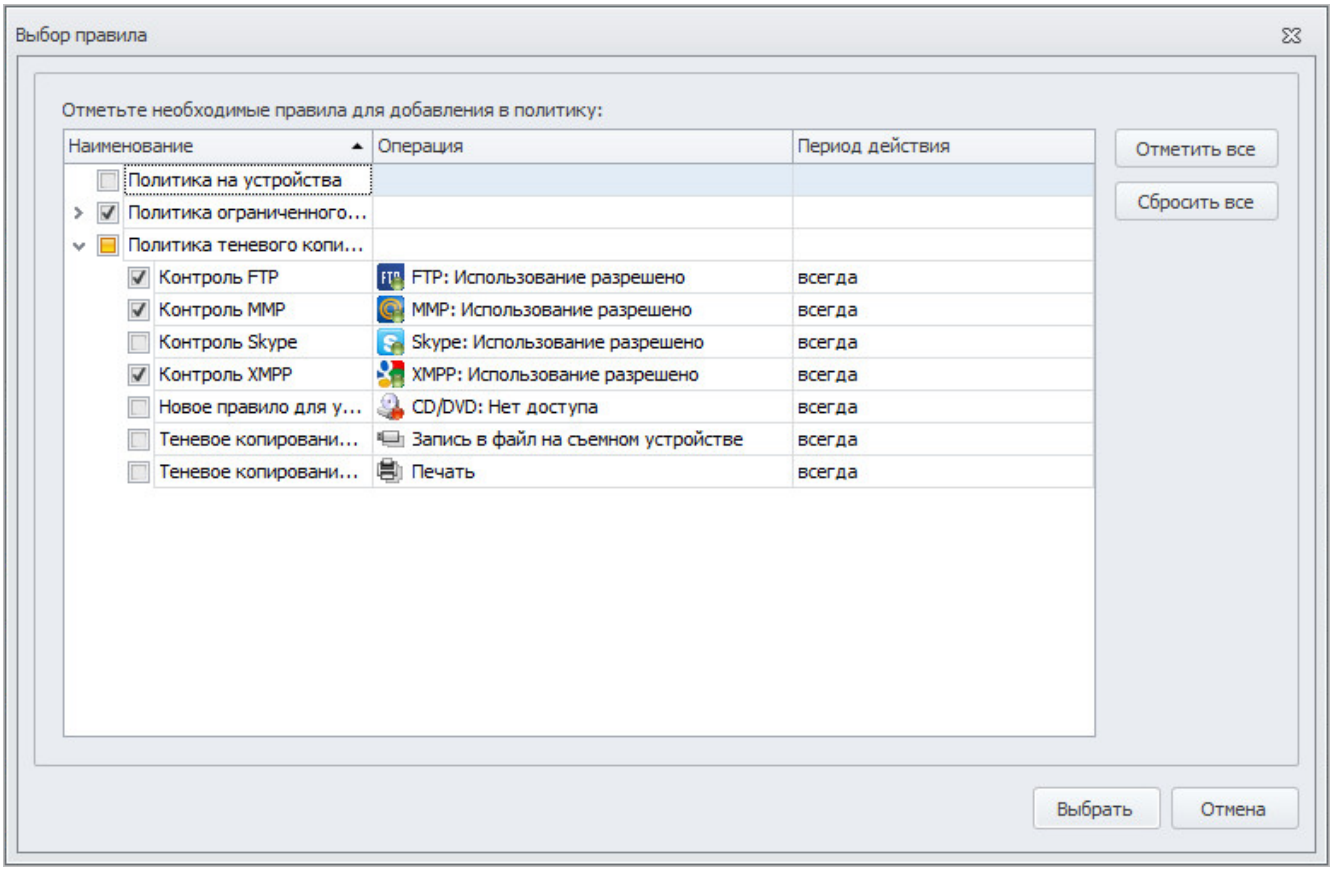
Чтобы создать и настроить политику безопасности:

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**.

   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 **Выберите 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:
  - Настройка правила для File Monitor
  - Настройка правила для Print Monitor
  - Настройка правила для Device Monitor
  - Настройка правила для IM Client Monitor
  - Настройка правила для FTP Monitor
  - Настройка правила для Network Monitor

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

5. После того, как вы определите все правила, которые должны входить в политику, нажмите **OK**.

Внимание!
Поскольку работа с политиками безопасности 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.

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 правила, Удаление правила, Копирование правил).

3.4.2.1.3 Редактирование политики безопасности

Чтобы отредактировать политику безопасности:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выделите название нужной политики безопасности.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Редактировать политику**;
   - воспользуйтесь кнопкой **Редактировать политику**, расположенной в верхней части Панели навигации;
   - дважды щелкните левой кнопкой мыши по названию выделенной политики безопасности.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно **Настройка политики**.
4. В данном окне отредактируйте название политики безопасности, указав новое название в поле **Наименование политики**.
5. Нажмите на кнопку **OK**.

Внимание!
Поскольку работа с политиками безопасности 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.

3.4.2.1.4 Удаление политики безопасности

Внимание!
Политику, назначенную хотя бы одной группе сотрудников или группе рабочих станций, невозможно удалить. Чтобы удалить политику, убедитесь,что всем группам сотрудников (см. "Просмотр сведений о

сотрудниках и группах сотрудников") и рабочих станций (см. "Просмотр сведений о рабочих станциях") не назначена удаляемая политика.

Чтобы удалить политику безопасности:

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

Внимание!

Поскольку работа с политиками безопасности 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.

3.4.2.2 Правила

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

Информация по работе с правилами содержится в подразделах:

- Применение правил
- Добавление правила
- Редактирование правила
- Удаление правила
- Копирование правил

3.4.2.2.1 Применение правил

Для того, чтобы набор правил в совокупности давал ожидаемый результат, необходимо учитывать особенности применения этих правил в различных случаях.

Событие считается удовлетворяющим правилу, если оно соответствует всем параметрам, указанным в правиле (например, и время события соответствует временному промежутку действия правила и размер передаваемого файла не менее минимального размера, указанного в правиле, и т.п.).

Если событие соответствует нескольким правилам одновременно, то в общем случае более ограничивающее правило имеет приоритет перед разрешающим. Более подробно:

1. Правило, исключающее из перехвата (выбрано **Исключить из перехвата**: см. "Настройка правила для File Monitor"), имеет наивысший приоритет.
2. Запрещающее правило имеет приоритет перед разрешающим. Например, для **Device Monitor** (см. "Настройка правила для Device Monitor") правило с ограничением *Нет доступа* имеет приоритет по сравнению с правилом, разрешающим *Только чтение*, а оно, в свою очередь, более приоритетно, чем с правилом, где выбрано *Полный доступ только к зашифрованным устройствам*. Также для **FTP Monitor** (см. "Настройка правила для FTP Monitor") правило с *Запретить использование FTP-протокола* применяется вместо *Разрешить только скачивать файлы с использованием FTP-протокола*, а оно - вместо *Разрешить использование FTP-протокола*. И так далее.
3. Правило, в котором указана необходимость сохранения теневой копии (выбрано **Создавать теневую копию**), имеет приоритет перед правилом без теневой копии.

4. Для правил **IM Client Monitor**, снимающих копию голосового трафика (выбрано **Создавать теневую копию голосового трафика**: см. "Настройка правила для IM Client Monitor"), правило с ограничением на меньшую продолжительность записи, имеет приоритет перед правилом с дольшей продолжительностью записи.

Другая информация, важная для понимания того, как применяются правила, изложена в следующих разделах:

- Особенности применения правил для Device Monitor
- Создание теневых копий и запрет операций при нехватке свободного пространства на контролируемых рабочих станциях

3.4.2.2.1.1 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 рабочих станций, в состав которых включена рабочая станция, используемая для доступа к устройству;
- белые списки.

В процессе установки Клиента доступ к контролируемым устройствам по умолчанию разрешен. Поэтому каждая запрещенная операция над устройством должна быть задана явно (т.е. в виде правила).

Первоначально каждая новая зарегистрированная рабочая станция попадает в группу рабочих станций 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 Система по умолчанию всегда разрешает доступ ко всем контролируемым устройствам.

Пример:

Для группы рабочих станций A задано правило, запрещающее запись CD/DVD дисков. Рабочая станция WS входит только в группу рабочих станций A. Сотрудник Ryzhov входит только в группу сотрудников B, для которой не определены правила работы с устройствами. Сотрудник Ryzhov пытается просмотреть содержимое компакт-диска на рабочей станции WS. 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 таких случаях возникает конфликт правил. Общий принцип разрешения конфликтов: приоритет – у более ограничивающего правила (подробнее см. таблицу).

Тип устройства	**Все устройства, кроме CD/DVD, Floppy и съемных устройств хранения**	**CD/DVD**	**Floppy и съемные устройства хранения**
Доступ, в порядке убывания приоритета	1. Использование запрещено	1. Нет доступа 2. Только чтение	1. Нет доступа 2. Только чтение 3. Полный доступ только к зашифрованным устройствам

Примеры:

Пример 1. Для группы рабочих станций C задано правило, запрещающее доступ к съемному устройству хранения. В политике на группу сотрудников D есть правило, разрешающее только чтение со съемного устройства хранения. Сотрудник Ryzhov входит в группу сотрудников D и пытается получить доступ к съемному устройству хранения с рабочей станции, входящей в группу рабочих станций C. Конфликт разрешается в пользу более ограничивающего правила, т.е. сотрудник Ryzhov не будет иметь доступ к съемному устройству хранения.

Пример 2. В политике для группы сотрудников E есть правило, дающее доступ к съемному устройству хранения только для чтения. В политике для группы сотрудников F есть правило разрешающее полный доступ только к зашифрованному съемному устройству хранения. Сотрудник Ryzhov входит в обе группы. Конфликт разрешается в пользу более ограничивающего правила: т.е. сотрудник Ryzhov сможет получить доступ к съемным устройствам только на чтение: причём как к зашифрованным, так и к незашифрованным (правило с меньшим приоритетом вообще не учитывается).

Для некоторых типов контролируемых устройств существуют пересекающиеся правила (см. таблицу). Эти правила также необходимо учитывать при настройке запрета на доступ к контролируемому устройству.

Примечание:
Список с типами контролируемых устройств и набор соответствующих им операций привенден в разделе "Настройка правила для Device Monitor".

Правило	Пересекающиеся правила	Примечания
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
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

Правило	Пересекающиеся правила	Примечания
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	Нет	
Сетевой принтер	Нет	
КПК (карманные компьютеры под управлением операционных систем Windows Mobile и Palm OS)	Нет	

3.4.2.2.1.2 Работа при нехватке рабочего пространства

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 не противоречит ограничениям, заданным в этом правиле.
2. Свободное место на контролируемой рабочей станции больше, чем минимальное значение, заданное политикой (см. "Общие настройки работы Клиентов", параметр **Минимальное свободное пространство на клиенте**, значение по умолчанию 10%).
3. На контролируемой рабочей станции больше свободного места, чем необходимо для создания теневой копии.

Внимание!
Если существует хотя бы одно действующее правило, задающее создание теневой копии, и на компьютере осталось меньше свободного места, чем определено политикой или чем требуется для сохранения файла, то контролируемая операция будет выполнена без сохранения теневой копии. Такое событие будет отображено в Консоли управления (см. "Просмотр событий") с состоянием "*Ошибка создания копии*".

Помимо теневых копий, на рабочей станции временно (до установления соединения с сервером Device Monitor) сохраняется информация о событиях. Для этого на том диске контролируемой рабочей станции, куда выполняется установке Клиента Device Monitor, выделяется место, достаточное для хранения информации о 30000 событиях (около 300 Мб). Если:

- Клиент Device Monitor настолько долго не имел связи с сервером Device Monitor, что накопилось более 30000 событий, контролируемых правилами, определёнными для сотрудника/рабочей станции

и

- в общих настройках работы Клиентов для параметра **Если место под события на диске**

закончилось установлено значение **Запрещена операция**,

то **любые действия сотрудника, контролируемые текущей политикой безопасности, будут запрещены**.

3.4.2.2.2 Добавление правила

Чтобы включить в политику новое правило:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выделите название той политики безопасности, в состав которой должно войти 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 сожчетание клавиш **Ctrl+Shift+N**.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно для настройки параметров правила.
4. Задайте необходимые параметры правила:
   - Настройка правила для File Monitor
   - Настройка правила для Print Monitor
   - Настройка правила для Device Monitor
   - Настройка правила для IM Client Monitor
   - Настройка правила для FTP Monitor
   - Настройка правила для HTTPS Monitor
   - Настройка правила для Network Monitor
5. После того как необходимые изменения будут внесены, нажмите **OK** в диалоговом окне настройки параметров правила.

Внимание!
Поскольку работа с правилами 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.

3.4.2.2.2.1 Настройка правила для File Monitor

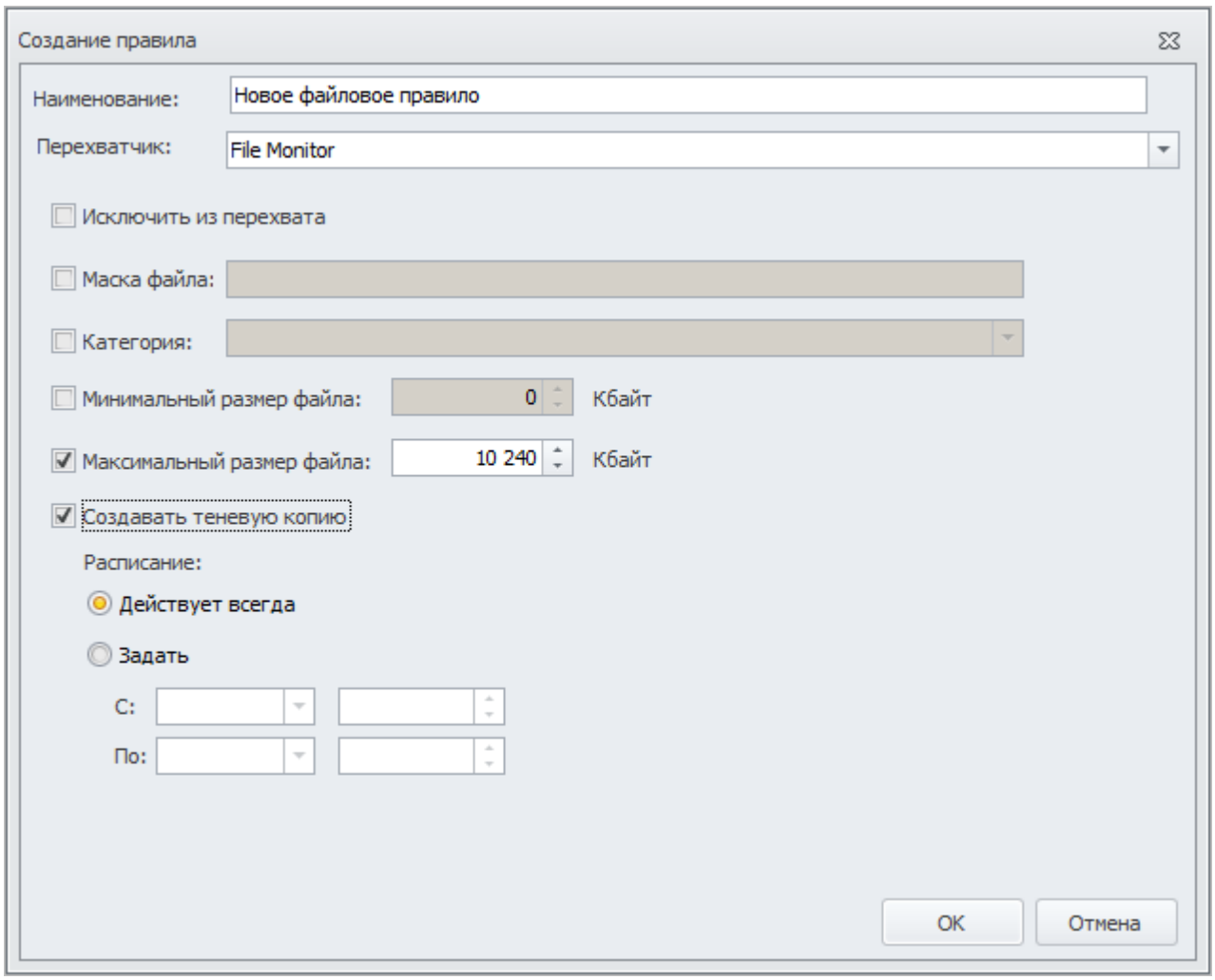
Перехватчик **File Monitor** позволяет отслеживать операции записи в файл на съемном устройстве, причем регистрируется факт успешного завершения операции. Это дает возможность отслеживать такие действия сотрудников, как:

- создание/редактирование файла непосредственно на съемном устройстве;
- копирование/перемещение файла на съемное устройство. В данном случае отслеживаются операции копирования/перемещения файла с контролируемой рабочей станции, другого съемного устройства или сетевых ресурсов.

Внимание!

Файл подпадает под действие правила **File Monitor**, если **ВСЕ** параметры файла удовлетворяют действующему правилу. Например, правило задаёт создание теневой копии и указан максимальный и минимальный размер файла, то обрабатываемый файл должен иметь размер, попадающий в диапазон указанный в правиле.

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



Чтобы настроить правило, задайте следующие параметры:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на панели навигации выделите название политики безопасности, в которую нужно 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;**
   - нажмите правой кнопкой мыши в пустом месте области **Политики** и в раскрывшемся меню выберите **Создать правило**.
4. В открывшемся диалоговом окне, в поле **Перехватчик**, выберите **File Monitor**.
5. В поле **Наименование** укажите название правила.
6. Если вы хотите, чтобы правило задавало исключение из контроля, выберите **Исключить из перехвата**. Для операций записи в файл на съемном устройстве, подпадающих под это правило, ни событий, ни теневых копий создаваться не будет.

> **Внимание!**
> Если событие записи файла соответствует нескольким правилам одновременно, правило, исключающее из перехвата, имеет наивысший приоритет.

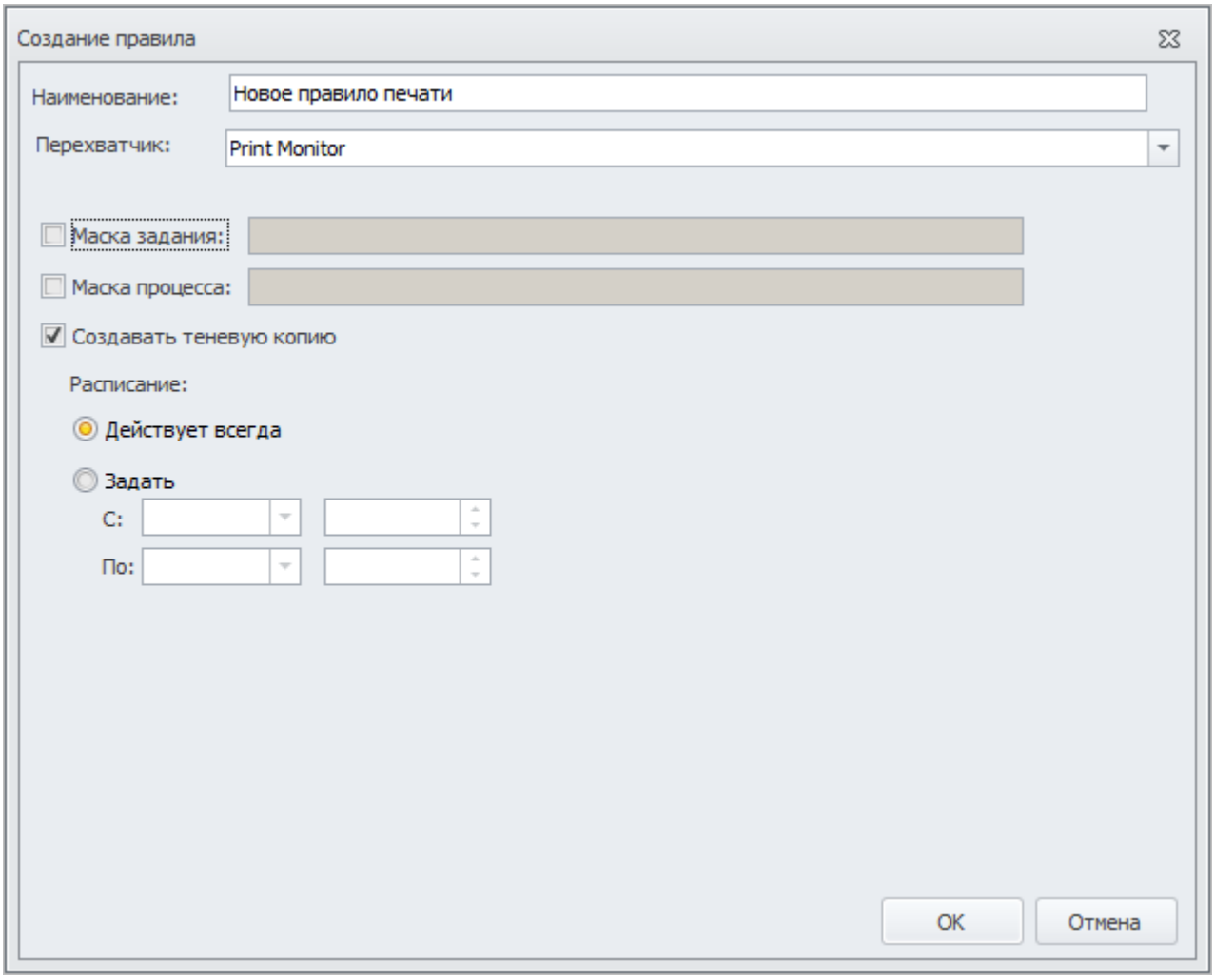
7. При необходимости, вы можете ограничить контролируемые файлы, задав маску файла. Для этого установите флажок в поле **Маска файла** и укажите маску: можно использовать символы: «?» для замены одного символа или «*» для замены набора символов. Например, `*.doc`. Знак пробела интерпретируется как часть имени файла.
8. Вы также можете ограничить применение правила определенной категорией сигнатур (см. "Сигнатуры") . Для этого установите флажок в поле **Категория** и выберите категорию из раскрывающегося списка: правило будет действовать для записи в файлы с типом, соответствующим выбранной категории сигнатур.
9. Если вы хотите создавать и передавать на Traffic Monitor теневые копии записываемых файлов, установите флажок в поле **Создавать теневую копию**.

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

10. В области **Расписание** определите период действия правила:
    - **Действует всегда**. По умолчанию правило действует бессрочно.
    - **Задать**. Укажите даты и время для необходимого периода в полях **С** и **По**.
11. После того, как вы определите все необходимые параметры, нажмите **ОК**.

3.4.2.2.2.2 Настройка правила для Print Monitor

Перехватчик **Print Monitor** позволяет осуществлять мониторинг операций, связанных с печатью документов на локальных и сетевых принтерах.



Чтобы настроить правило, задайте следующие параметры:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на панели навигации выделите название политики безопасности, в которую нужно 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;**
   - нажмите правой кнопкой мыши в пустом месте области **Политики** и в раскрывшемся меню выберите **Создать правило**.
4. В открывшемся диалоговом окне, в поле **Перехватчик**, выберите **Print Monitor**.
5. В поле **Наименование** укажите название правила.
6. 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 установите данный флажок и укажите маску задания.

     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 распечатываемого документа.

В маске задания можно использовать подстановочные символы: «?» для замены одного символа или «*» для замены набора символов. Знак пробела интерпретируется как часть имени задания.

- **Маска процесса**. Использование маски для процесса, который выводит задание на печать. Если нужно задать маску процесса, установите данный флажок 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.

7. Если вы хотите создавать и передавать на Traffic Monitor теневые копии печатаемых документов, установите флажок в поле **Создавать теневую копию**.

   Внимание!
   Если, в соответствии с действующим правилом Print Monitor, должна быть создана теневая копия печатаемого документа, но на рабочей станции осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного пространства на контролируемых рабочих станциях"), то печать будет осуществляться без создания теневой копии.

8. В области **Расписание** определите период действия правила:
   - **Действует всегда**. По умолчанию правило действует бессрочно.
   - **Задать**. Укажите даты и время для необходимого периода в полях **С** и **По**.
9. После того, как вы определите все необходимые параметры, нажмите **ОК**.

3.4.2.2.2.3 Настройка правила для Device Monitor

Перехватчик **Device Monitor** позволяет контролировать доступ сотрудников к периферийным устройствам. Возможности степени ограничения доступа на выполнение операций с периферийными устройствами зависят от типа устройства.

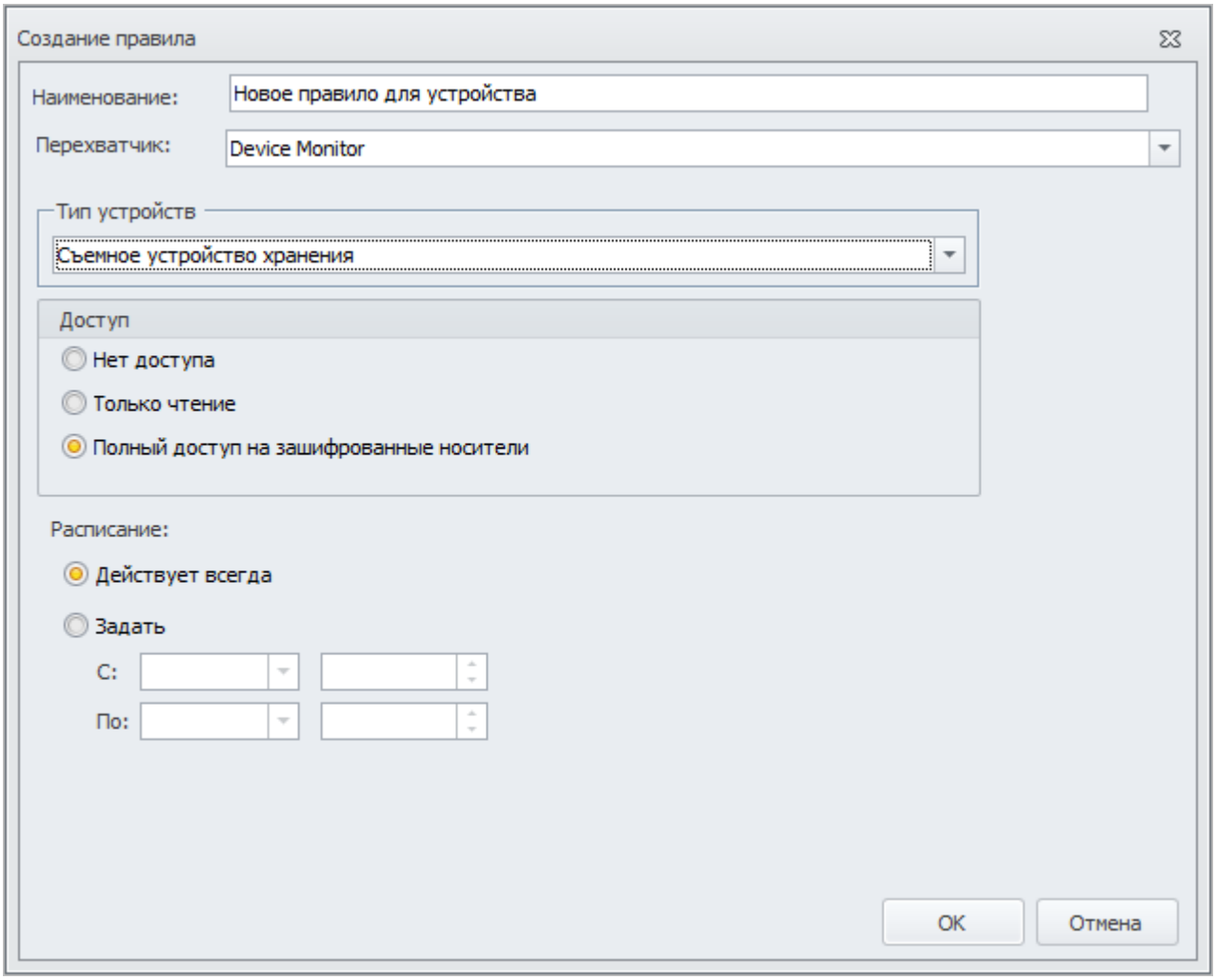
Варианты доступа на использование устройств того или иного типа

Типы устройств	Варианты ограничения доступа на использование устройства
Флоппи-дисковод	Полный доступ только к зашифрованным устройствам / Только чтение / Нет доступа
CD/DVD	Только чтение / Нет доступа
Параллельный порт (LPT)	Использование запрещено
Последовательный порт (COM)	Использование запрещено
Съемное устройство хранения (устройства, подключаемые через интерфейсы USB, IEEE 1394)	Полный доступ только к зашифрованным устройствам / Только чтение / Нет доступа
Локальный принтер (подключаемый через интерфейс USB, IEEE 1394, SCSI и пр.)	Использование запрещено
Устройства работы с изображениями (видеокамеры, сканеры)	Использование запрещено
Bluetooth устройство	Использование запрещено

Типы устройств	**Варианты ограничения доступа на использование устройства**
IrDA устройство	Использование запрещено
Другое USB устройство	Использование запрещено
FireWire	Использование запрещено
Модем	Использование запрещено
Считыватель смарт-карт (Smart Card Reader)	Использование запрещено
Ленточный накопитель	Использование запрещено
Многофункциональное устройство	Использование запрещено
PCMCI устройство	Использование запрещено
Сетевой адаптер USB	Использование запрещено
КПК (карманные компьютеры под управлением операционных систем Windows Mobile и Palm OS)	Использование запрещено
Сетевой принтер	Использование запрещено

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.

Внимание!
О порядке разрешения случаев, когда событие соответствует нескольким правилам, см. "Применение правил" и "Особенности применения правил для Device Monitor".



Чтобы настроить правило, задайте следующие параметры:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на панели навигации выделите название политики безопасности, в которую нужно 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;**
   - нажмите правой кнопкой мыши в пустом месте области **Политики** и в раскрывшемся меню выберите **Создать правило**.
4. В открывшемся диалоговом окне, в поле **Перехватчик**, выберите **Device Monitor**.
5. В поле **Наименование** укажите название правила.
6. В поле **Тип устройств** выберите тип устройства, контролируемого данным правилом.
7. В области **Доступ** отметьте необходимый вариант ограничения доступа на использование устройства (см. таблицу выше).
8. В области **Расписание** определите период действия правила:
   - **Действует всегда**. По умолчанию правило действует бессрочно.
   - **Задать**. Укажите даты и время для необходимого периода в полях **С** и **По**.

9. После того, как вы определите все необходимые параметры, нажмите **ОК**.

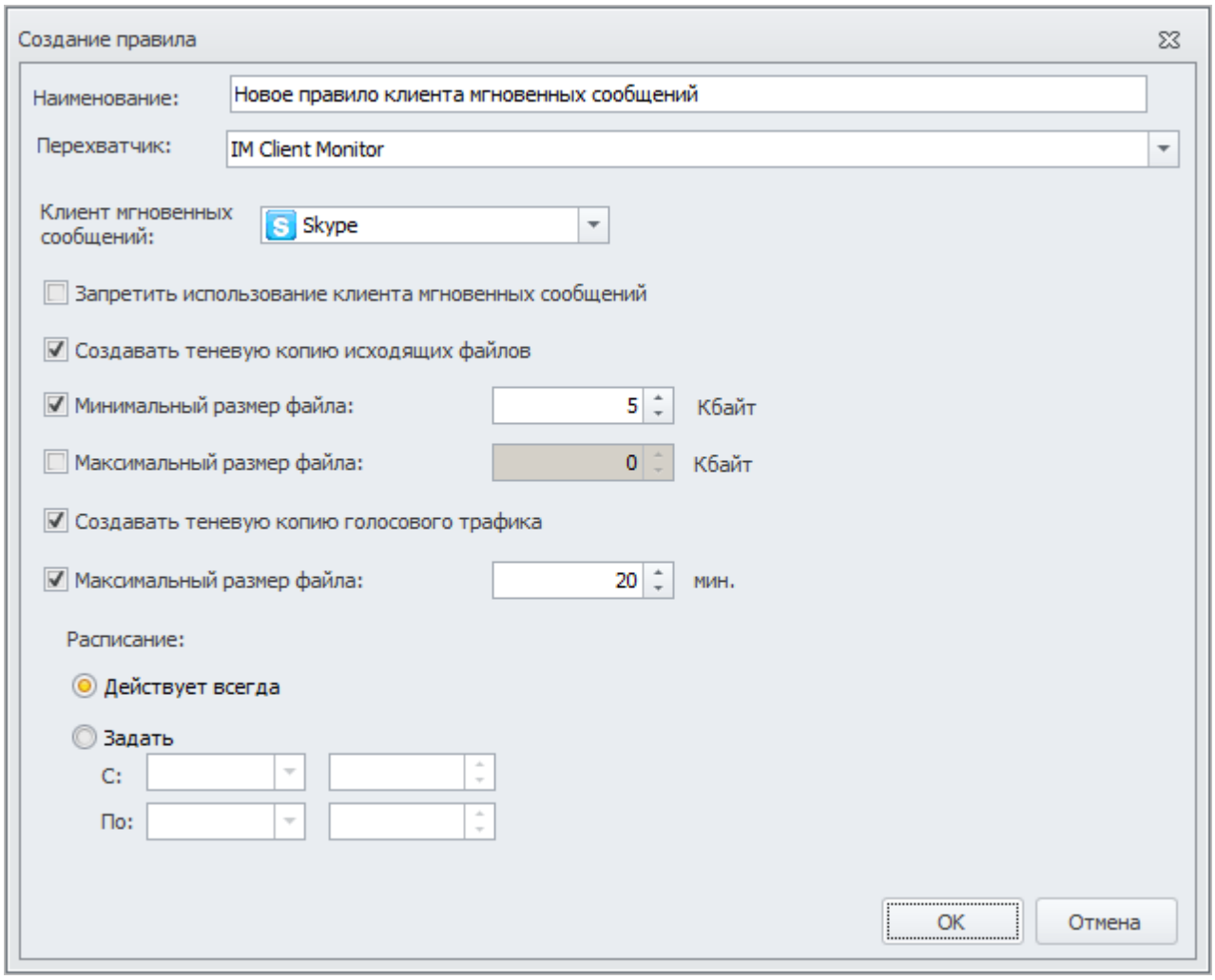
3.4.2.2.2.4 Настройка правила для IM Client Monitor

Перехватчик **IM Client Monitor** позволяет контролировать доступ сотрудников к системам мгновенного обмена сообщениями Skype, Jabber (протокол XMPP) и Mail.Ru Агент (протокол MMP).

Внимание!
Глобальные параметры работы перехватчика IM Client Monitor (запрос сотрудника на разрешение работы перехватчика, настройка периода снятия теневой копии чата) настраиваются вместе с общими настройками схемы безопасности: см. "Контроль сетевого трафика".

Внимание!

Файл подпадает под действие правила **IM Client Monitor**, если **ВСЕ** параметры файла удовлетворяют действующему правилу, **ЗА ИСКЛЮЧЕНИЕМ** параметров максимального и минимального размер файла. Поля **Минимальный размер файла** и **Максимальный размер файла** учитываются только для создания теневой копии. Таким образом, если размер файла попадает в диапазон, указанный в правиле, то событие о передаче файла будет содержать теневую копию; если не попадает, то событие будет сформировано без теневой копии.



Чтобы настроить правило, задайте следующие параметры:

1. Перейдите к разделу **Политики**.

2. В области **Политики** на панели навигации выделите название политики безопасности, в которую нужно 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;**
   - нажмите правой кнопкой мыши в пустом месте области **Политики** и в раскрывшемся меню выберите **Создать правило**.
4. В открывшемся диалоговом окне, в поле **Перехватчик**, выберите **IM Client Monitor**.
5. В поле **Наименование** укажите название правила.
6. В поле **Клиент мгновенных сообщений** выберите тип мессенджера, контролируемого данным правилом:
   - **Skype** - для контроля использования Skype
   - **XMPP** - для контроля использования Jabber
   - **MMP** - для контроля использования Mail.Ru Агент
7. Если вы хотите полностью запретить использование клиента данного типа, установите флажок в поле **Запрет использования клиента мгновенных сообщений**.
8. Если вы хотите создавать и передавать на Traffic Monitor теневые копии передаваемых файлов, установите флажок в поле **Создавать теневую копию исходящих файлов**. В этом случае вы также можете определить дополнительные параметры этих теневых копий:
   - **Минимальный размер файла**. Если флажок установлен, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
   - **Максимальный размер файла**. Если флажок установлен, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.

   Внимание!
   Теневые копии чатов и сообщений создаются всегда (независимо от настройки параметра **Создавать теневую копию**), если на рабочей станции действует хотя бы одно правило для **IM Client Monitor**.
   Порядок настройки периодичности снятия теневых копий чатов и сообщений (временной промежуток и количество сообщений, по достижении которых формируется теневая копия) описан в разделе "Контроль сетевого трафика".
9. Для клиента **Skype** вы также можете сохранять файлы с записями разговоров по Skype. Для этого у становите флажок в поле **Создавать теневую копию голосового трафика**. В поле **Максимальный размер файла** определите, как будет разбиваться разговор: если длительность разговора превышает указанный размер (в минутах), то будет создано более одной теневой копии (соответственно, и более одного события) для одного разговора.
10. В области **Расписание** определите период действия правила:
    - **Действует всегда**. По умолчанию правило действует бессрочно.
    - **Задать**. Укажите даты и время для необходимого периода в полях **С** и **По**.
11. После того, как вы определите все необходимые параметры, нажмите **ОК**.

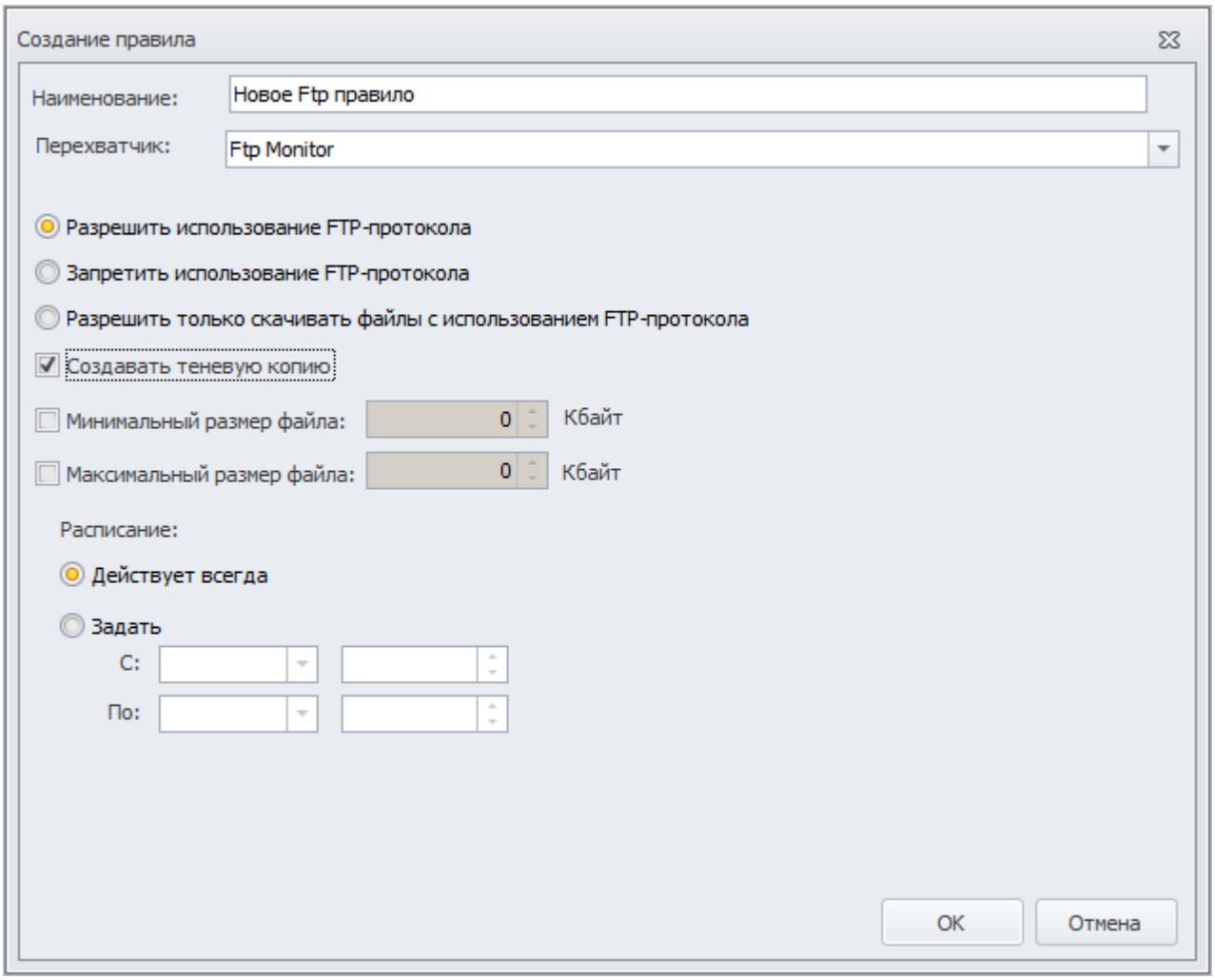
Внимание!
Если, в соответствии с действующим правилом IM Client Monitor, должна быть создана теневая копия файла, сообщения или чата, но на рабочей станции осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного пространства на контролируемых рабочих станциях"), то теневые копии сообщений всё ещё будут сохраняться, но файлы будут передаваться без создания теневой копии.

3.4.2.2.2.5 Настройка правила для FTP Monitor

Перехватчик **FTP Monitor** позволяет контролировать обмен данными через протокол FTP.

Внимание!

Файл подпадает под действие правила **FTP Monitor**, если **ВСЕ** параметры файла удовлетворяют действующему правилу, **ЗА ИСКЛЮЧЕНИЕМ** параметров максимального и минимального размер файла. Поля **Минимальный размер файла** и **Максимальный размер файла** учитываются только для создания теневой копии. Таким образом, если размер файла попадает в диапазон, указанный в правиле, то событие о передаче файла будет содержать теневую копию; если не попадает, то событие будет сформировано без теневой копии.



Чтобы настроить правило, задайте следующие параметры:

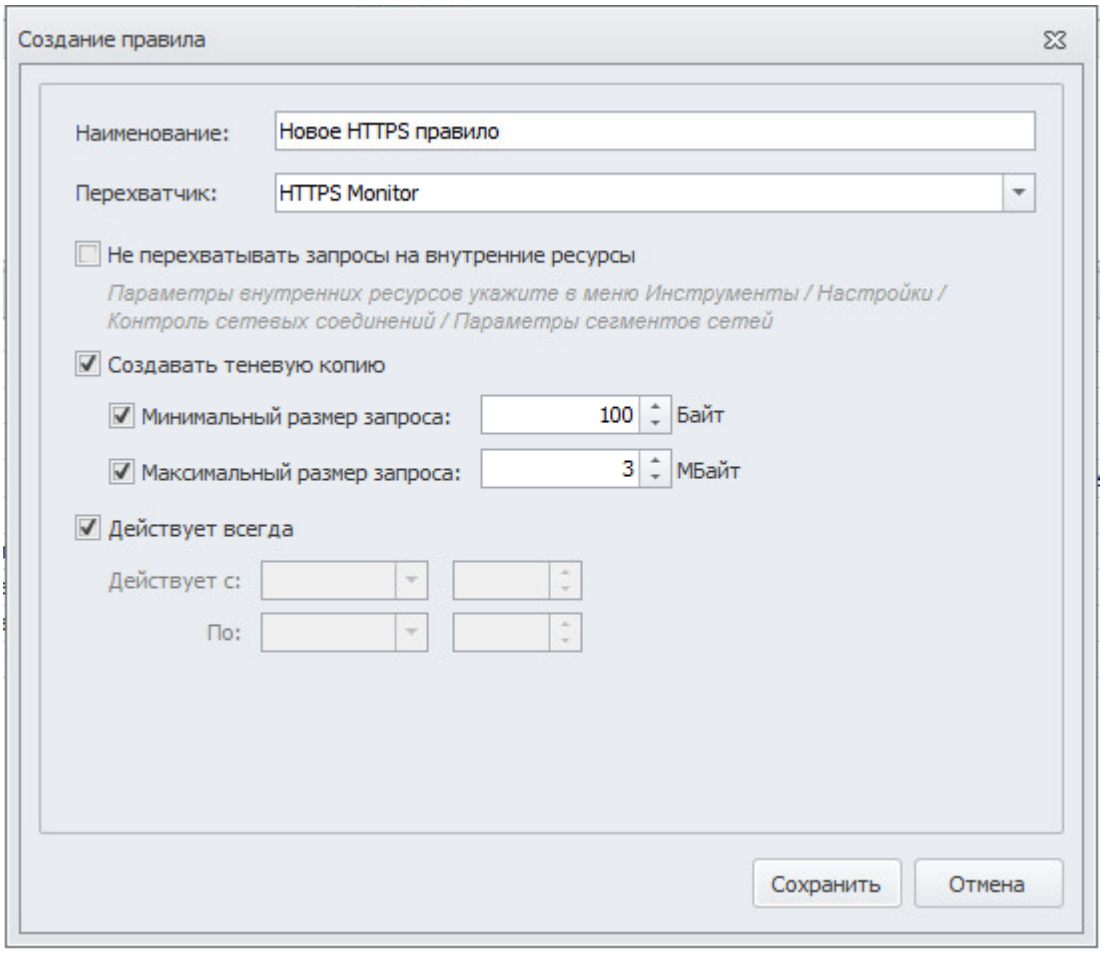
1. Перейдите к разделу **Политики**.
2. В области **Политики** на панели навигации выделите название политики безопасности, в которую нужно добавить правило.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Действие > Создать правило**
   - воспользуйтесь кнопкой **Создать правило**, расположенной в верхней части области **Политики;**
   - нажмите правой кнопкой мыши в пустом месте области **Политики** и в раскрывшемся меню выберите **Создать правило**.

4. В открывшемся диалоговом окне, в поле **Перехватчик**, выберите **FTP Monitor**.
5. В поле **Наименование** укажите название правила.
6. Выберите степень контроля обмена данными через протокол FTP:
   - **Разрешить использование FTP-протокола**
   - **Запретить использование FTP-протокола**
   - **Разрешить только скачивать файлы с использованием FTP-протокола**
7. Если вы разрешили использование FTP-протокола, то вы можете также настроить создание теневых копий отправляемых файлов. Для этого установите флажок в поле **Создавать теневую копию исходящих файлов**. Вы также можете определить дополнительные параметры этих теневых копий:
   - **Минимальный размер файла**. Если флажок установлен, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
   - **Максимальный размер файла**. Если флажок установлен, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.

   Внимание!
   Если, в соответствии с действующим правилом FTP Monitor, должна быть создана теневая копия файла, но на рабочей станции осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного пространства на контролируемых рабочих станциях"), то файл будет передан без создания теневой копии.
8. В области **Расписание** определите период действия правила:
   - **Действует всегда**. По умолчанию правило действует бессрочно.
   - **Задать**. Укажите даты и время для необходимого периода в полях **С** и **По**.
9. После того, как вы определите все необходимые параметры, нажмите **ОК**.

3.4.2.2.2.6 Настройка правила для HTTPS Monitor

Перехватчик **HTTPS Monitor** позволяет контролировать обмен данными через протокол HTTPS.



Чтобы настроить правило, задайте следующие параметры:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на панели навигации выделите название политики безопасности, в которую нужно добавить правило.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Действие > Создать правило**;
   - воспользуйтесь кнопкой **Создать правило**, расположенной в верхней части области **Правила**;
   - нажмите правой кнопкой мыши в пустом месте области **Политики** и в раскрывшемся меню выберите **Создать правило**.
4. В открывшемся диалоговом окне, в поле **Перехватчик**, выберите **HTTPS Monitor**.
5. В поле **Наименование** укажите название правила.
6. Настройте перехват запросов на внутренние ресурсы. Для этого в поле **Не перехватывать запросы на внутренние ресурсы**:
   - установите флажок - если не требуется перехватывать запрос;
   - снимите флажок - если требуется перехватывать запрос.
7. Настройте создание теневых копий отправляемых файлов. Для этого установите флажок в поле **Создавать теневую копию**. Вы также можете определить дополнительные параметры этих теневых копий:
   - **Минимальный размер запроса**. Если флажок установлен, то теневое копирование будет выполняться только для запросов, размер которых больше либо равен указанному.

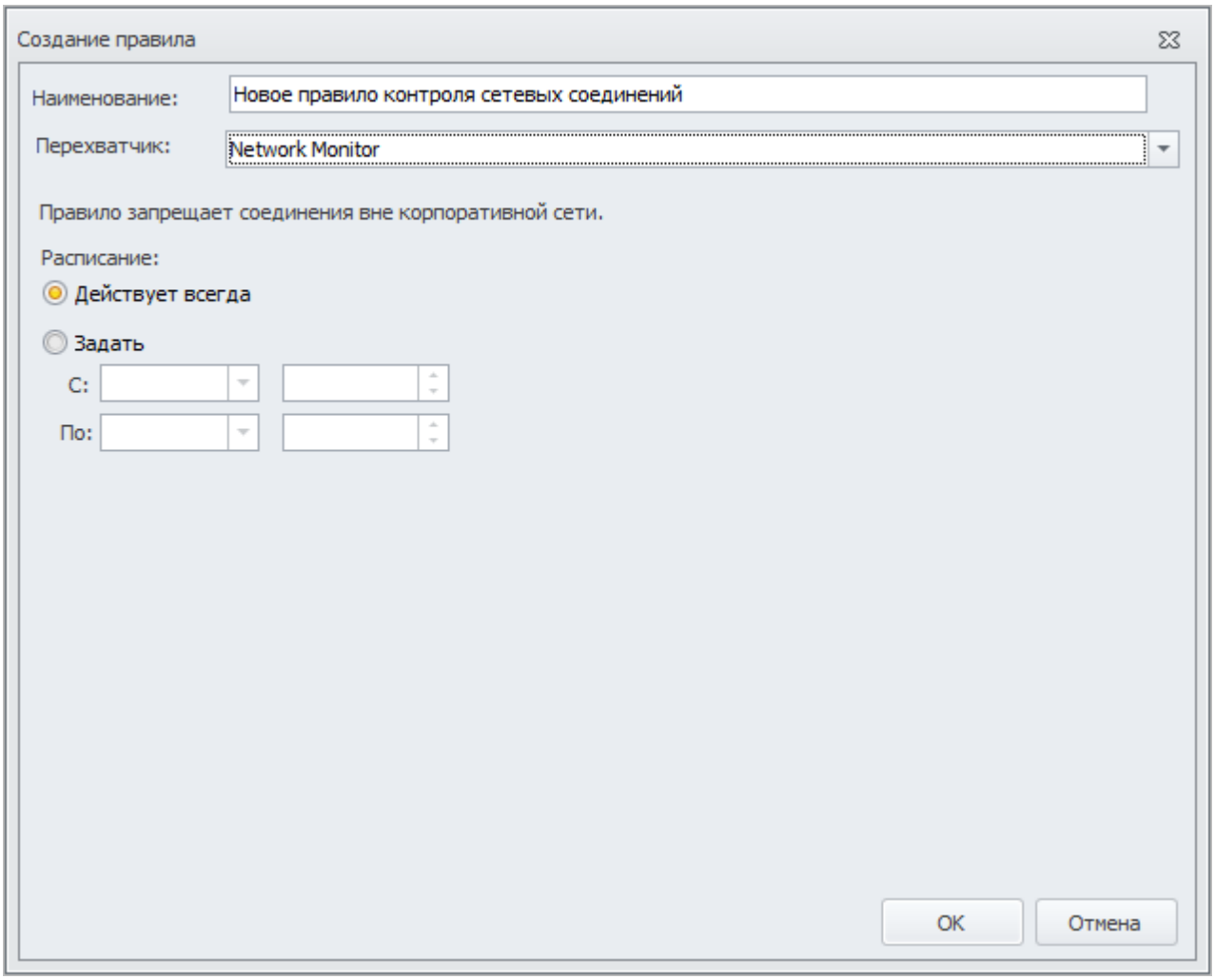
- **Максимальный размер запроса**. Если флажок установлен, то теневое копирование будет выполнятьсятолько для запросов, размер которых меньше либо равен указанному.

> **Внимание!**
> Если, в соответствии с действующим правилом HTTPS Monitor, должна быть создана теневая копия, но на рабочей станции осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного пространства на контролируемых рабочих станциях"), то запрос будет передан без создания теневой копии.

8. Настройте период действия правила. Для этого в поле **Действует всегда**:
   - установите флажок (по умолчанию флажок установлен) - правило будет действовать бессрочно.
   - снимите флажок - в полях **Действует с** и **По** потребуется указать даты и время для необходимого периода.
9. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

3.4.2.2.2.7 Настройка правила для Network Monitor

Перехватчик **Network Monitor** позволяет запрещать передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами. Настройка параметров того, какие сегменты сети считаются корпоративной сетью, и какие внешние адреса разрешены, выполняется как описано в разделе "Контроль сетевых соединений".



Чтобы настроить правило, задайте следующие параметры:

1. Перейдите к разделу **Политики**.

2. В области **Политики** на панели навигации выделите название политики безопасности, в которую нужно добавить правило.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Действие > Создать правило**
   - воспользуйтесь кнопкой **Создать правило**, расположенной в верхней части области **Политики;**
   - нажмите правой кнопкой мыши в пустом месте области **Политики** и в раскрывшемся меню выберите **Создать правило**.
4. В открывшемся диалоговом окне, в поле **Перехватчик**, выберите **Network Monitor**.
5. В поле **Наименование** укажите название правила.
6. В области **Расписание** определите период действия правила:
   - **Действует всегда**. По умолчанию правило действует бессрочно.
   - **Задать**. Укажите даты и время для необходимого периода в полях **С** и **По**.
7. После того, как вы определите все необходимые параметры, нажмите **ОК**.

3.4.2.2.3 Редактирование правила

Чтобы отредактировать правило:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выделите название той политики безопасности, в состав которой входит нужное правило. После этого в рабочей области главного окна будет выведен список всех правил данной политики.
3. Выделите строку с названием того правила, которое нужно отредактировать.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Изменить правило**;
   - дважды щелкните левой кнопкой мыши по выделенной строке;
   - воспользуйтесь кнопкой **Изменить правило**, расположенной в верхней части области **Политики**.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно для настройки параметров выбранного правила.
5. Отредактируйте необходимые параметры правила:
   - Настройка правила для File Monitor
   - Настройка правила для Print Monitor
   - Настройка правила для Device Monitor
   - Настройка правила для IM Client Monitor
   - Настройка правила для FTP Monitor
   - Настройка правила для Network Monitor.
6. После того как необходимые изменения будут внесены, нажмите **ОК** в диалоговом окне настройки параметров правила.

Внимание!
Поскольку работа с правилами 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.

3.4.2.2.4 Удаление правила

Чтобы удалить правило:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выделите название политики безопасности, содержащей нужное правило. После этого в рабочей области главного окна будет выведен список всех правил данной политики.
3. Выделите строку с названием правила, которое нужно удалить.

   Примечание:
   Чтобы удалить несколько правил, входящих в одну политику безопасности, выделите строки с названиями всех правил, которые нужно удалить.
4. Выполните одно из следующих действий:
   - нажмите кнопку **Delete**;
   - в главном меню выберите команду **Правка > Удалить правило**;
   - воспользуйтесь кнопкой **Удалить правило**, расположенной в верхней части области **Политики**.
5. В появившемся окне запроса нажмите **Да**, чтобы подтвердить удаление правила.

Внимание!
Поскольку работа с правилами 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.

3.4.2.2.5 Копирование правил

Правила можно копировать из одной политики безопасности в другую.

Чтобы скопировать правило:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выделите название политики безопасности, содержащей правило, которое нужно скопировать.
3. В рабочей области главного окна выделите строку с названием правила, которое нужно скопировать. Вы можете выделить несколько строк, чтобы скопировать группу правил в одну политику безопасности.
4. Щелкните левой кнопки мыши по выделенной строке 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.

В результате правило будет скопировано в выбранную политику безопасности.

Вы также можете выполнить копирование правил из диалогового окна редактирования той политики, куда вы хотите добавить правила, уже имеющиеся в других политиках.

Чтобы скопировать правило при редактировании политики:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выделите название политики безопасности, в которую вы хотите добавить правило.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Редактировать политику**;
   - воспользуйтесь кнопкой **Редактировать политику**, расположенной в верхней части Панели навигации;

- дважды щелкните левой кнопкой мыши по названию выделенной политики безопасности.

4. Нажмите **Выберите правила**. В раскрывшемся окне отметьте те правила, которые нужно скопировать в редактируемую политику. Можно выбрать целиком политику - в этом случае все правила, в ней содержащиеся, будут скопированы в редактируемую политику.
5. После того, как вы отметите все необходимые правила, нажмите **Выбрать**.

Внимание!
Поскольку работа с правилами политиками безопасности 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.

3.4.2.3 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.

Внимание!
На каждого сотрудника, помимо политики безопасности, назначенной группе сотрудников, также действует и политика безопасности, определенная для рабочей станции, на которой 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
- 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

3.4.2.3.1 Просмотр сведений о сотрудниках и группах

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. главу "Дополнительные возможности").

Чтобы просмотреть информацию по отдельной группе сотрудников,

выделите 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,

выделите строку с названием нужной учетной записи.
В результате на панели **Подробно** будет отображена таблица свойств, в которой вы сможете просмотреть следующую информацию:

- **Учетная запись**. Название учетной записи сотрудника.
- **Фамилия**, **Имя**, **Отчество**. Фамилия, имя и отчество сотрудника, для которого создана данная учетная запись.
- **Идентификатор**. Внутренний идентификатор операционной системы.

Примечание:
Часть свойств, выводимых на панели **Подробно**, дублируется в рабочей области главного окна.

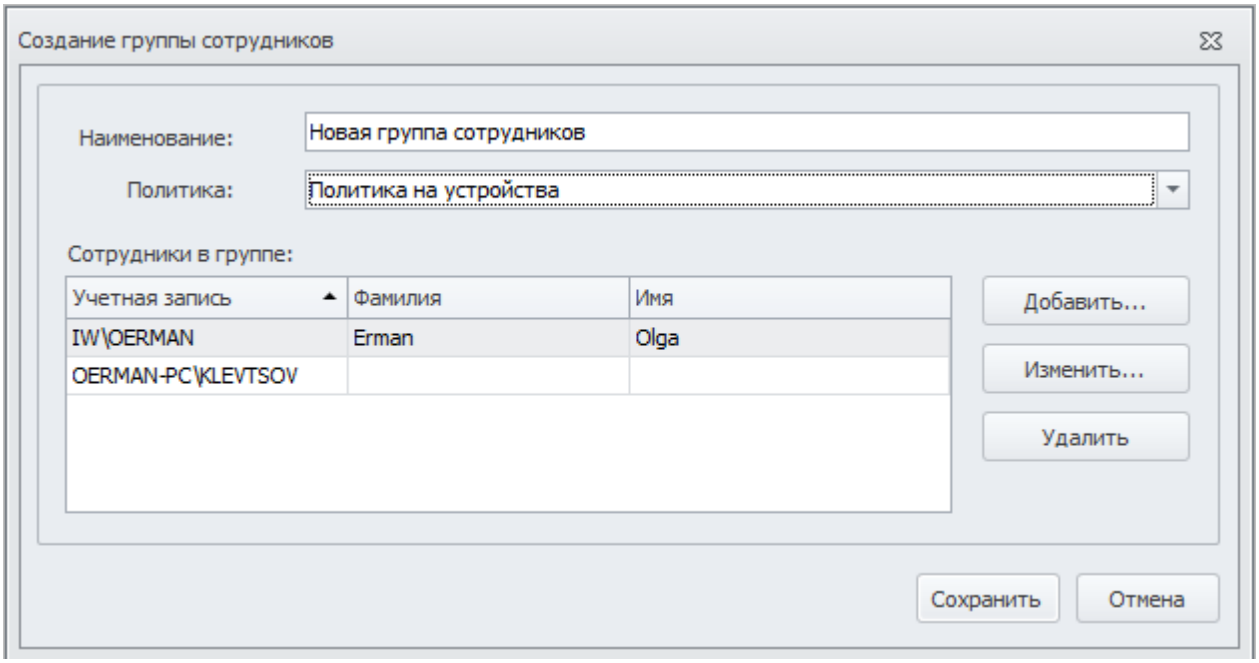
3.4.2.3.2 Создание и редактирование группы сотрудников

Чтобы добавить группу сотрудников:

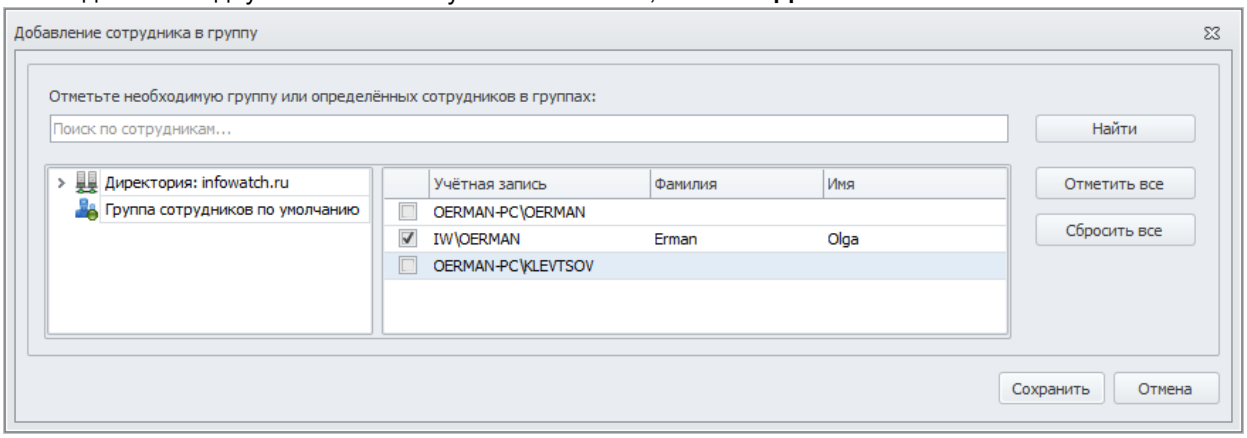
1. Перейдите к разделу **Группы сотрудников**.
2. Выполните необходимое действие:

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	1. В области **Группы сотрудников** на Панели навигации выделите название нужной группы сотрудников. 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 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 с сервером LDAP"), а также уже зарегистрированных в системе (например, при установке Клента Device Monitor на рабочие станции) 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 учётной записи по всем доступным элементам. Для этого в верхней строке введите часть имени учётной записи и нажмите **Найти**.

     После того, как все необходимые учётные записи выбраны, нажмите **Сохранить**, чтобы закрыть окно добавления сотрудников и вернуться к окну настройки параметров группы.
   - Чтобы изменить параметры учетной записи, выберите её в списке сотрудников, входящих в группу, и нажмите **Изменить**.
   - Чтобы удалить запись из группы, выберите её и нажмите **Удалить**.
5. Нажмите **Сохранить**.

Внимание!
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.

3.4.2.3.3 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 группу сотрудников**;
   - воспользуйтесь кнопкой **Удалить группу сотрудников**, расположенной в верхней части **Панели навигации**.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление группы сотрудников.

Внимание!
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.

3.4.2.3.4 Добавление учетной записи сотрудника в группу

В результате установки Клиента InfoWatch Device Monitor на компьютер (см. "Установка Клиента 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 учётной записи в различные группы рабочих станций.

Чтобы перенести сотрудника из одной группы в другую:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** на Панели навигации выделите название группы сотрудников, где уже есть его учётная запись.
3. В области **Сотрудники** выделите строку с учётной записью, которую нужно добавить в другую группу. Щелкните левой кнопкой мыши по выделенной строке и, не отпуская кнопку, перетащите учётную записьв область **Группы сотрудников** на Панели навигации. Подведите курсор мыши к названию той группы сотрудников, куда нужно добавить учётную запись. После того как слева от названия выбранной группы появится желтая стрелка, отпустите левую кнопку мыши.

В результате учётная запись будет включена в выбранную группу.

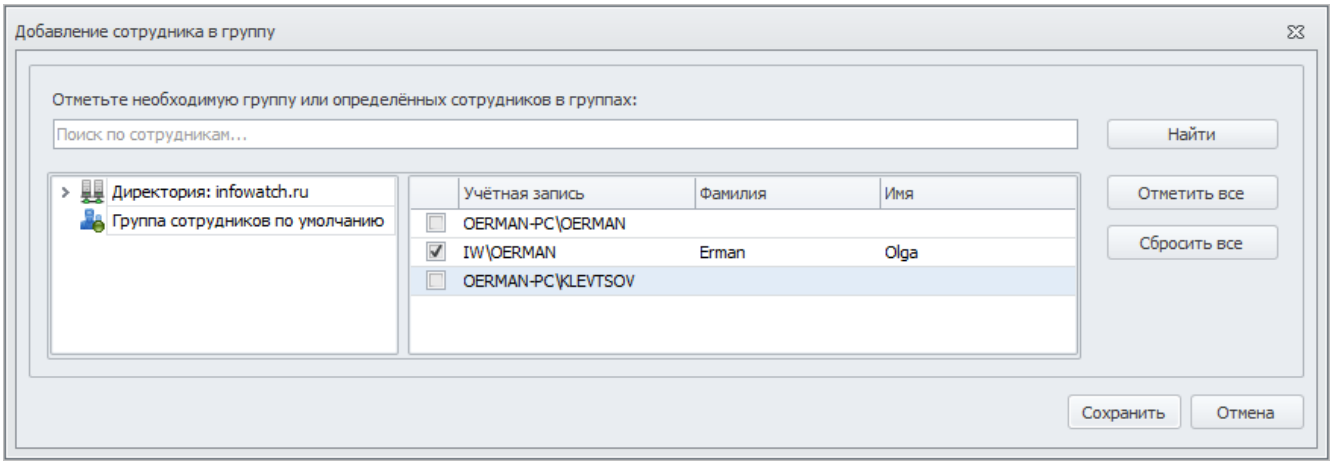
Вы также можете вручную импортировать в Систему информацию о сотруднике из службы каталогов (о настройке соединения см. "Соединение с сервером LDAP"). Тогда после регистрации данного сотрудника на компьютере, где установлен Клиент InfoWatch Device Monitor, на этого сотрудника будет распространяться политика той группы, в которую он был добавлен.

Чтобы добавить одну или несколько учетных записей в группу сотрудников:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** на Панели навигации выделите 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.



4. В окне добавления сотрудников отображается список учетных записей, импортированных из службы каталогов (см. "Соединение с сервером LDAP"), а также уже зарегистрированных в системе (например, при установке Клента Device Monitor на рабочие станции) 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 учётной записи по всем доступным элементам. для этого в верхней строке введите часть иени учётной записи и нажмите **Найти**.

     После того, как все необходимые учётные записи выбраны, нажмите **Сохранить**, чтобы закрыть окно добавления сотрудников и вернуться к окну настройки параметров группы.
   - Чтобы изменить параметры учетной записи, выберите её в списке сотрудников, входящих в группу, и нажмите **Изменить**.
   - Чтобы удалить запись из группы, выберите её и нажмите **Удалить**.
5. Нажмите **Сохранить**.

Внимание!
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.

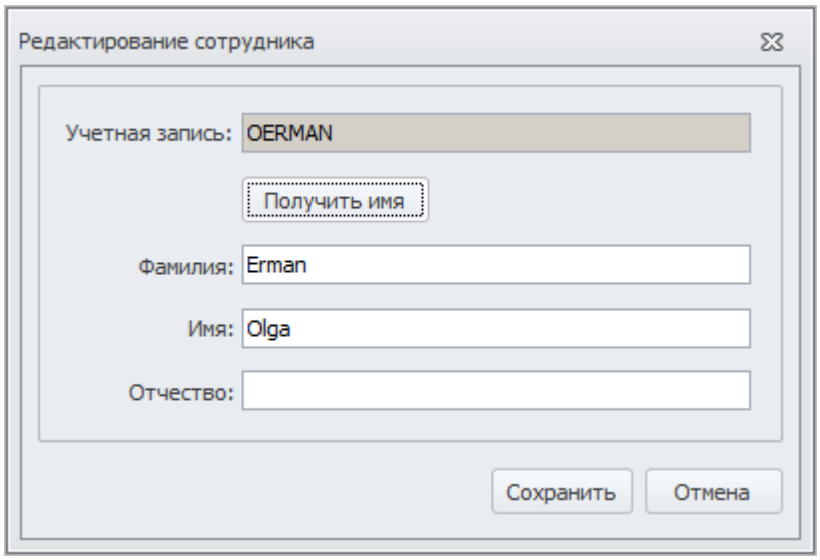
3.4.2.3.5 Редактирование учетной записи сотрудника

Параметры учётной записи сотрудника получаются Системой при импортировании его данных из из службы каталогов или при установке Клиента 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 сотрудник:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** на Панели навигации выделите название группы сотрудников, в которую входит нужная учетная запись.
3. Выделите строку с именем учетной записи, которую нужно отредактировать.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Изменить**;

- воспользуйтесь кнопкой **Изменить**, расположенной в верхней части области **Сотрудники**;
- дважды щелкните левой кнопкой мыши по выделенной строке.



5. В диалоговом окне **Редактирование сотрудника** вы можете изменять значения необязательных параметров **Фамилия**, **Имя** и **Отчество**. Новые значения можно вручную добавлять в соответствующие поля или импортировать из службы каталогов, воспользовавшись кнопкой **Получить имя**.
6. Нажмите **Сохранить**.

Внимание!
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.

3.4.2.3.6 Исключение учетной записи сотрудника из группы

Чтобы исключить учетную запись сотрудника из группы сотрудников:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** выделите название группы сотрудников, в которую входит нужная учетная запись.
3. Выделите строку с именем учетной записи, которую нужно исключить из данной группы.

   Примечание:
   Чтобы исключить несколько учетных записей из группы сотрудников, выделите строки с именами всех учетных записей сотрудников, которые нужно исключить из данной группы.

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**;
   - 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».

Внимание!

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.

3.4.2.3.7 Удаление учетной записи из схемы безопасности

Чтобы удалить учетную запись сотрудника из схемы безопасности:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** выделите название группы сотрудников, в которую входит нужная учетная запись.
3. Выделите строку с именем учетной записи, которую нужно удалить.

   Примечание:
   Чтобы удалить несколько учетных записей из схемы безопасности, выделите 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**;
   - нажмите сочетание клавиш клавиатуры **Shift+Delete**.
5. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление учетной записи.

Внимание!
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.

3.4.2.4 Рабочие станции

Под рабочими станциями в системе InfoWatch Device Monitor понимаются контролируемые рабочие станции - компьютеры, на которых установлены Клиенты InfoWatch Device Monitor.

Основные принципы работы с рабочими станциями описываются в разделе "Рабочие станции и группы рабочих станций".

Действующие политики безопасности могут быть назначены только группе рабочих станций. Определение политики безопасности для отдельной рабочей станции выполняется путем её включения в ту или иную группу.

Внимание!
На каждую рабочую станцию, помимо политики безопасности, назначенной группе рабочих станций, также действует и политика безопасности, определенная для сотрудника, который в данный момент авторизован на этой рабочей станции. О порядке определения приоритетов при пересечении правил см. "Применение правил".

Чтобы перейти к разделу Консоли управления, предназначенному для управления рабочими станциями, воспользуйтесь кнопкой **Группы рабочих станций**, расположенной на Панели навигации.

Информация по работе с контролируемыми рабочими станциями содержится в подразделах:

- Просмотр сведений о рабочих станциях
- Просмотр эффективной политики на рабочей станции
- Создание и редактирование группы рабочих станций
- Удаление группы рабочих станций
- Добавление рабочей станции в группу
- Исключение рабочей станции из группы

- Удаление рабочей станции из схемы безопасности
- Обновление Клиентов на контролируемых рабочих станциях

3.4.2.4.1 Просмотр сведений о рабочих станциях

В области **Группы рабочих станций** на Панели навигации выводится перечень групп рабочих станций. В рабочей области главного окна отображается перечень рабочих станций, входящих в состав выделенной группы рабочих станций.

Примечание:
Для более удобного просмотра вы можете настроить отображение списка рабочих станций, воспользовавшись дополнительными функциями (подробнее см. "Дополнительные возможности").

Чтобы просмотреть список рабочих станций, входящих в отдельную группу рабочих станций,

выделите название нужной группы в списке групп рабочих станций.

Чтобы просмотреть список всех зарегистрированных рабочих станций,

воспользуйтесь кнопкой **Показать все рабочие станции**, расположенной в верхней части Панели навигации.

Информация по рабочим станциям представлена в виде табличного списка. Каждая строка списка соответствует рабочей станции. В столбцах выводятся основные свойства рабочих станций. Расширенная информация по свойствам рабочей станции выводится на панели **Подробно**.

Чтобы просмотреть свойства отдельной рабочей станции,

в рабочей области главного окна выделите строку с описанием нужной рабочей станции.

После этого на панели **Подробно** будет отображена таблица свойств, в которой содержатся следующие сведения по выбранной рабочей станции:

- **Статус**. Состояние контролируемой рабочей станции и Клиента. Данный параметр может принимать одно из следующих значений:
  - **Работает нормально**. Контролируемая рабочая станция включена, Клиент запущен
  - **Неактивна**. Контролируемая рабочая станция выключена, либо долгое время недоступна. Этот же статус выводится при удалении Клиента с контролируемой рабочей станции.
- **Адрес**. Адрес рабочей станции. В качестве адреса может быть указано доменное имя или IP-адрес.
- **Время установки**. Дата и время первого обращения Клиента, установленного на рабочей станции, к Серверу.
- **Время подключения**. Дата и время запуска Клиента на рабочей станции.
- **Последнее обращение**. Дата и время последнего обращения Клиента, установленного на рабочей станции, к Серверу.
- **Версия схемы**. Номер версии схемы безопасности, загруженной на Клиент.
- **Версия клиента**. Номер версии Клиента, установленного на рабочей станции.
- **Версия настроек**. Номер версии общих настроек политики безопасности (см. "Общие настройки политики безопасности").
- **Версия шаблонов**. Номер версии шаблонов уведомления сотрудников (см. "Настройка уведомлений сотрудников о нарушении правил").
- **Версия настроек контроля сети**. Номер версии настроек контроля передачи данных по сетевым соединениям с помощью Network Monitor (см. "Контроль сетевых соединений").
- **Версия настроек контроля сетевых приложений**. Номер версии настроек контроля сетевого трафика, передаваемого через по протоколам XMPP, MMP и FTP (см. "Контроль сетевого трафика").
- **Свободное место на дисках рабочей станции**. Размер свободного места на дисках, куда сохраняются теневые копии (в т.ч. в процентах) и минимально допустимый размер этого свободного пространства.

Внимание!
Если на рабочей станции осталось меньше свободного места, чем определено политикой (см. "Создание теневых копий и запрет операций при нехватке свободного пространства на контролируемых рабочих станциях"), то теневые копии сохраняться не будут.

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

Каждая зарегистрированная рабочая станция автоматически добавляется в группу рабочих станций «по умолчанию». При этом рабочей станции назначается политика безопасности, определенная для группы рабочих станций «по умолчанию».

В процессе работы вы можете выполнять следующие действия:

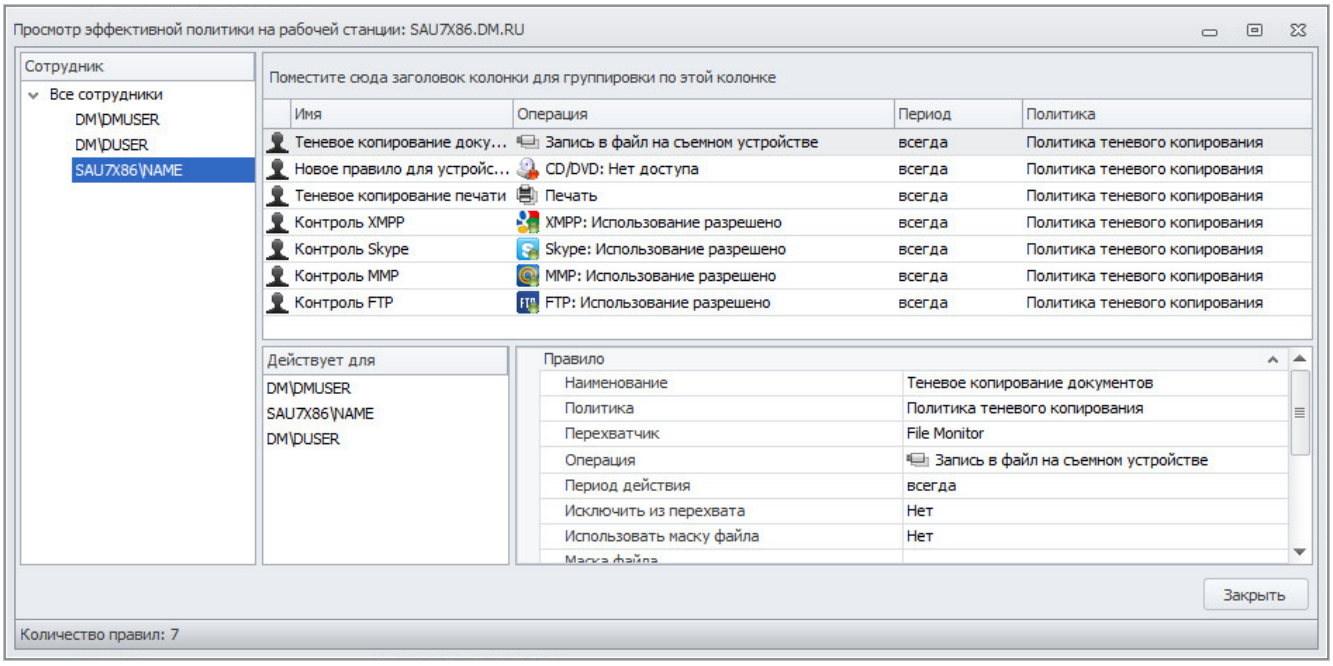
- управлять группами рабочих станций:
  - добавлять группы рабочих станций;
  - редактировать параметры групп рабочих станций;
  - удалять группы рабочих станций.
- управлять рабочими станциями:
  - добавлять информацию о компьютерах в группу рабочих станций и тем самым определять политику безопасности;
  - исключать рабочие станции из группы рабочих станций;
  - удалять рабочие станции из схемы безопасности;
  - обновлять Клиенты на контролируемых рабочих станциях.

3.4.2.4.2 Просмотр эффективной политики на рабочей станции

Чтобы посмотреть информацию о политике, действующей на рабочей станции:

1. В списке рабочих станций выделите название нужной.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Показать эффективную политику**.
   - дважды щелкните левой кнопкой мыши по названию рабочей станции.

В результате на экран будет выведено окно **Просмотр эффективной политики на рабочей станции: <имя рабочей станции>**.



На левой панели данного окна представлен список учетных записей всех сотрудников, получавших доступ к работе на этой рабочей станции, а на правой - перечень правил, действующих на рабочей станции. Перечень правил может складываться из правил, настроенных по умолчанию, правил, заданных для выбранной рабочей станции, и правил для сотрудников этой рабочей станции.

Чтобы просмотреть набор правил, действующих для определенного сотрудника,

в панели **Сотрудник** выберите его учетную запись.

Чтобы просмотреть подробную информацию по правилу,

выберите его в перечне правил.

На панели **Действует для** будет представлен список сотрудников на которых распространяется данное правило, а на панели **Правило** – подробная информация о выбранном правиле.

3.4.2.4.3 Создание и редактирование группы рабочих станций

Внимание!
Когда регистрируется новая рабочая станция, информация об этой рабочей станции автоматически добавляется в схему безопасности (в группу рабочих станций «по умолчанию»).

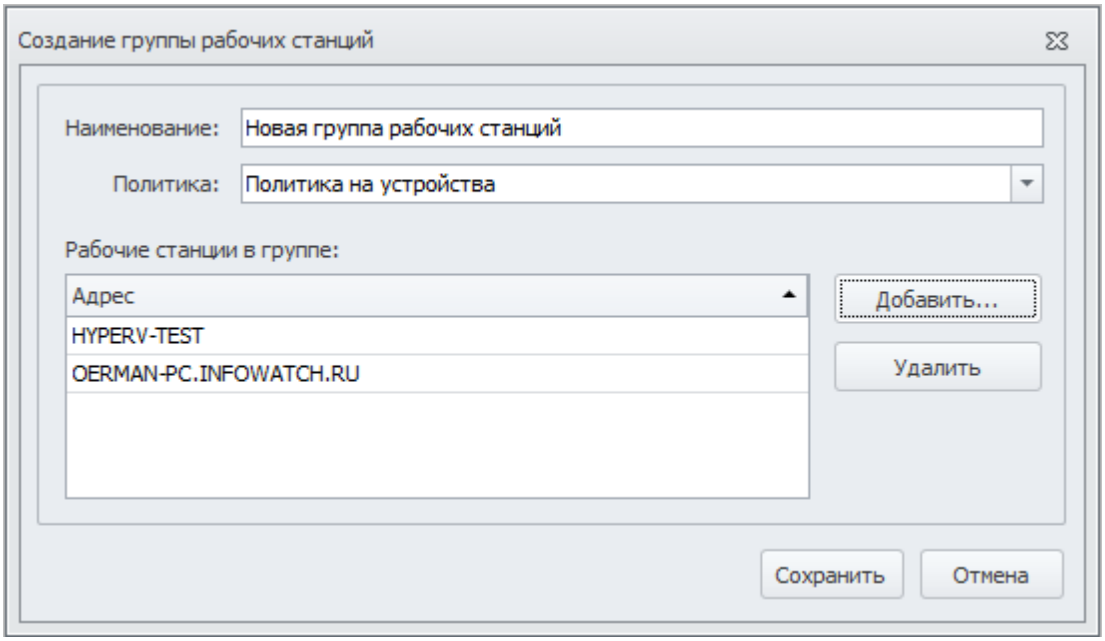
Чтобы добавить группу рабочих станций:

1. Перейдите к разделу **Группы рабочих станций**.
2. Выполните необходимое действие:

Действие	Шаги
Добавить группу рабочих станций	• в главном меню выберите команду **Правка > Создать группу рабочих станций**; • воспользуйтесь кнопкой **Создать группу рабочих станций**, расположенной в верхней части Панели навигации.
Отредактировать группу рабочих станций	1. В области **Группы рабочих станций** на Панели навигации выделите название нужной группы рабочих станций. 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 выделенной группы рабочих станций.

В результате выполнения любого из этих действий на экран будет выведено диалоговое окно определения параметров группы рабочих станций.



3. Укажите следующие параметры:
   - **Наименование**.
   - **Политика**. Выберите из раскрывающегося списка политику безопасности, которая будет назначена данной группе рабочих станций.
4. Определите перечень рабочих станций в группе:
   - Чтобы добавить одну или несколько рабочих станций, нажмите **Добавить**. В открывшемся окне вы можете выбрать рабочие станции:
     - из директории;
     - из сетевого окружения Microsoft Windows Network;
     - из числа ранее зарегистрированных в системе (например, в результате ручной установки Клента Device Monitor) и уже принадлежащих существующим группам Device Monitor.

     Чтобы добавить рабочую станцию, в левой области выберите необходимый узел в дереве групп, затем отметьте рабочие станции, которые нужно добавить в редактируемую группу.
     Вы также можете выполнить поиск рабочей станции по директории. Для этого в верхней строке введите часть имени рабочей станции и нажмите **Найти**.
     После того, как все необходимые рабочие станции выбраны, нажмите **Сохранить**, чтобы закрыть окно добавления и вернуться к окну настройки параметров группы.
   - Чтобы изменить параметры рабочей станции, выберите её в списке входящих в группу и нажмите **Изменить**.
   - Чтобы удалить рабочую станцию из группы, выберите её и нажмите **Удалить**.
5. Нажмите **Сохранить**.

Внимание!
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.

3.4.2.4.4 Удаление группы рабочих станций

Чтобы удалить группу рабочих станций:

1. Перейдите к разделу **Группы рабочих станций**.
2. В области **Группы рабочих станций** на Панели навигации выделите название необходимой группы

рабочих станций.

3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление группы рабочих станций.

   Внимание!
   В группе рабочих станций, которую вы удаляете, могут быть рабочие станции, не включенные в другие группы. Такие рабочие станции при удалении единственной группы, в которую они были включены, будут автоматически добавлены в группу рабочих станций «по умолчанию».
5. Нажмите на кнопку **OK**.

Внимание!
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.

3.4.2.4.5 Добавление рабочей станции в группу

При установке Клиента InfoWatch Device Monitor на компьютер (см. "Установка Клиента InfoWatch Device Monitor"), в Системе автоматически создаётся запись о рабочей станции. Эта рабочая станция добавляется в группу "по умолчанию". Соответственно, на все рабочие станции, входящие в группу «по умолчанию», будет распространяться политика безопасности, назначенная данной группе. В дальнейшем определение политик безопасности для рабочей станции происходит путем включения рабочей станции в различные группы рабочих станций.

Чтобы переместить рабочую станцию из одной группы в другую:

1. Перейдите к разделу **Группы рабочих станций**.
2. В области **Группы рабочих станций** на Панели навигации выделите название группы рабочих станций, в состав которой входит нужная рабочая станция.
3. В области **Рабочие станции** выделите строку с названием рабочей станции, которую нужно добавить в другую группу. Щелкните левой кнопкой мыши по выделенной строке и, не отпуская кнопку, перетащите рабочую станцию в область **Группы рабочих станций** на Панели навигации. Подведите курсор мыши к названию той группы рабочих станций, в которую нужно добавить рабочую станцию. После того как слева от названия выбранной группы появится желтая стрелка, отпустите левую кнопку мыши.

В результате рабочая станция будет включена в выбранную группу.

Вы также можете вручную добавить в Систему информацию о компьютере, на котором ещё не установлен Клиента InfoWatch Device Monitor. Информация о компьютере импортируется из службы каталогов (о настройке соединения см. "Соединение с сервером LDAP") или из сетевого окружения. Тогда после установки Клиента InfoWatch Device Monitor на такую рабочую станцию (см. "Создание задачи первичного распространения"), на неё будет распространяться политика той группы, в которую она была добавлена.

Внимание!
Настоятельно не рекомендуется добавлять компьютеры с одинаковыми именами. В системе InfoWatch Device Monitor такие компьютеры будут зарегистрированы как одна рабочая станция и, соответственно, на них будет распространяться одна политика, будет вестись единая регистрация событий и т.д.

Чтобы добавить рабочую станцию в группу:

1. Перейдите к разделу **Группы рабочих станций**.
2. В области **Группы рабочих станций** на Панели навигации выделите название необходимой группы рабочих станций. После этого в рабочей области главного окна будет выведен список всех рабочих

станций, уже входящих в группу.

3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Добавить рабочую станцию**;
   - воспользуйтесь кнопкой **Добавить рабочую станцию**, расположенной в верхней части области **Рабочие станции**;
   - нажмите правой кнопкой мыши в рабочей области и из раскрывшегося контекстного меню выберите **Добавить рабочую станцию**.

   В открывшемся диалоговом окне вы можете выбрать рабочие станции:
   - из директории;
   - из сетевого окружения Microsoft Windows Network.
4. Выберите необходимые рабочие станции или группы рабочих станций, отмечая их флажком. Свёрнутые группы отмечены пиктограммой ; развёрнутые - . Чтобы развернуть или свернуть группу, дважды нажмите на ней левой кнопкой мыши.

   Внимание!
   Если вы отметите флажком группу, то будут выбраны только компьютеры, непосредственно входящие в отмеченную группу. Подгруппы отмеченной группы и компьютеры, входящие в подгруппы отмеченной группы, в этом случае не выбираются: их следует отмечать дополнительно.

   Вы также можете указать имя рабочей станции в строке внизу диалогового окна. При перечислении нескольких имён разделяйте их точкой с запятой.
5. Нажмите **ОК**.

В результате диалоговое окно **Выбор компьютеров** будет закрыто, а в группу рабочих станций будет добавлена информация о выбранных компьютерах.

Внимание!
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.

3.4.2.4.6 Исключение рабочей станции из группы

Включение рабочей станции в определенную группу рабочих станций связано с назначением политик безопасности для данной рабочей станции. В процессе работы может возникнуть необходимость отменить действие какой-либо политики безопасности на рабочую станцию. Для выполнения данной процедуры необходимо исключить рабочую станцию из группы рабочих станций, которой назначена такая политика безопасности.

Примечание:
Если рабочая станция входит только в одну группу рабочих станций, то при исключении из группы такая рабочая станция будет автоматически добавлена в группу рабочих станций «по умолчанию».

Чтобы исключить рабочую станцию из группы рабочих станций:

1. Перейдите к разделу **Группы рабочих станций**.
2. В области **Группы рабочих станций** на Панели навигации выделите название группы рабочих станций, в которую входит нужная рабочая станция. После этого в рабочей области главного окна будет выведен список всех рабочих станций, включенных в выбранную группу рабочих станций.
3. Выделите строку с названием рабочей станции, которую нужно исключить из группы рабочих станций.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Исключить рабочую станцию из группы**;
   - воспользуйтесь кнопкой **Исключить рабочую станцию из группы**, расположенной в верхней

части области **Рабочие станции**;

- нажмите кнопку клавиатуры **Delete**.

После этого рабочая станция будет исключена из группы.

Внимание!
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.

3.4.2.4.7 Удаление рабочей станции из схемы безопасности

Рабочая станция может быть выведена из списка зарегистрированных (например, эксплуатация рабочей станции прекращена). Сведения о такой рабочей станции не будут удалены, но, так как Клиент на ней отключен, то рабочей станции присваивается статус **Неактивна**.
Если сохранение информации о неактивной рабочей станции не требуется, то вы можете удалить запись о ней.

Чтобы удалить рабочую станцию из схемы безопасности:

1. Перейдите к разделу **Группы рабочих станций**.
2. В области **Группы рабочих станций** на Панели навигации выделите название группы рабочих станций, в которую входит нужная рабочая станция.
3. В рабочей области главного окна выделите строку с названием неактивной рабочей станции, которую нужно удалить.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить рабочую станцию из схемы безопасности**;
   - воспользуйтесь кнопкой **Удалить рабочую станцию из схемы безопасности**, расположенной в верхней части области **Рабочие станции**;
   - щелкните правой кнопкой на строке необходимой рабочей станции и из раскрывшегося списка выберите **Удалить рабочую станцию 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 рабочей станции будут удалены из всех групп, в которые входила данная рабочая станция.

Внимание!
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.

3.4.2.4.8 Обновление Клиентов на рабочих станциях

Для контролируемых рабочих станций доступно упрощённое создание задачи обновления Клиентов Device Monitor (подробнее об этом типе задач см. "Удаленная установка, обновление и удаление Клиентов" и "Создание задачи обновления").

Чтобы обновить Клиенты Device Monitor на всех контролируемых рабочих станцях, входящих в группу:

1. Перейдите к разделу **Группы рабочих станций**.
2. В области **Группы рабочих станций** на Панели навигации выделите название необходимой группы рабочих станций.
3. Воспользуйтесь кнопкой **Обновить все рабочие станции**, расположенной в верхней части Панели навигации.

Чтобы обновить Клиенты Device Monitor выбранных контролируемых рабочих станцях:

1. Перейдите к разделу **Группы рабочих станций**.
2. В области **Группы рабочих станций** на Панели навигации выделите название необходимой группы рабочих станций.
3. В области **Рабочие станции** выделите строку с названием одной или нескольких контролируемых рабочих станций. Для выбора нескольких рабочих станций, отмечайте из, зажав клавишу **Shift** или **Ctrl** .
4. Воспользуйтесь кнопкой **Обновить рабочие станции**, расположенной в верхней части области **Рабочие станции**.

В результате выполнения любого из этих действий будет создана и автоматически запустится задача обновления для выбранных рабочих станций.

3.4.2.5 Белые списки

Для управления списками устройств, доступ к которым безусловно разрешен, 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

3.4.2.5.1 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:
Для более удобного просмотра вы можете настроить отображение белого списка при помощи дополнительных функций (см. главу "Дополнительные возможности").

Чтобы просмотреть информацию по отдельному белому списку,

выделите 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,

выделите 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 модели или экземпляра устройства**. Код модели (VID – Vendor ID) или серийного номера экземпляра (PID – Product ID) устройства.
- **Описание устройства**.
- **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 рабочей станции**. Имя рабочей станции, на которой 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.

3.4.2.5.2 Добавление белого списка

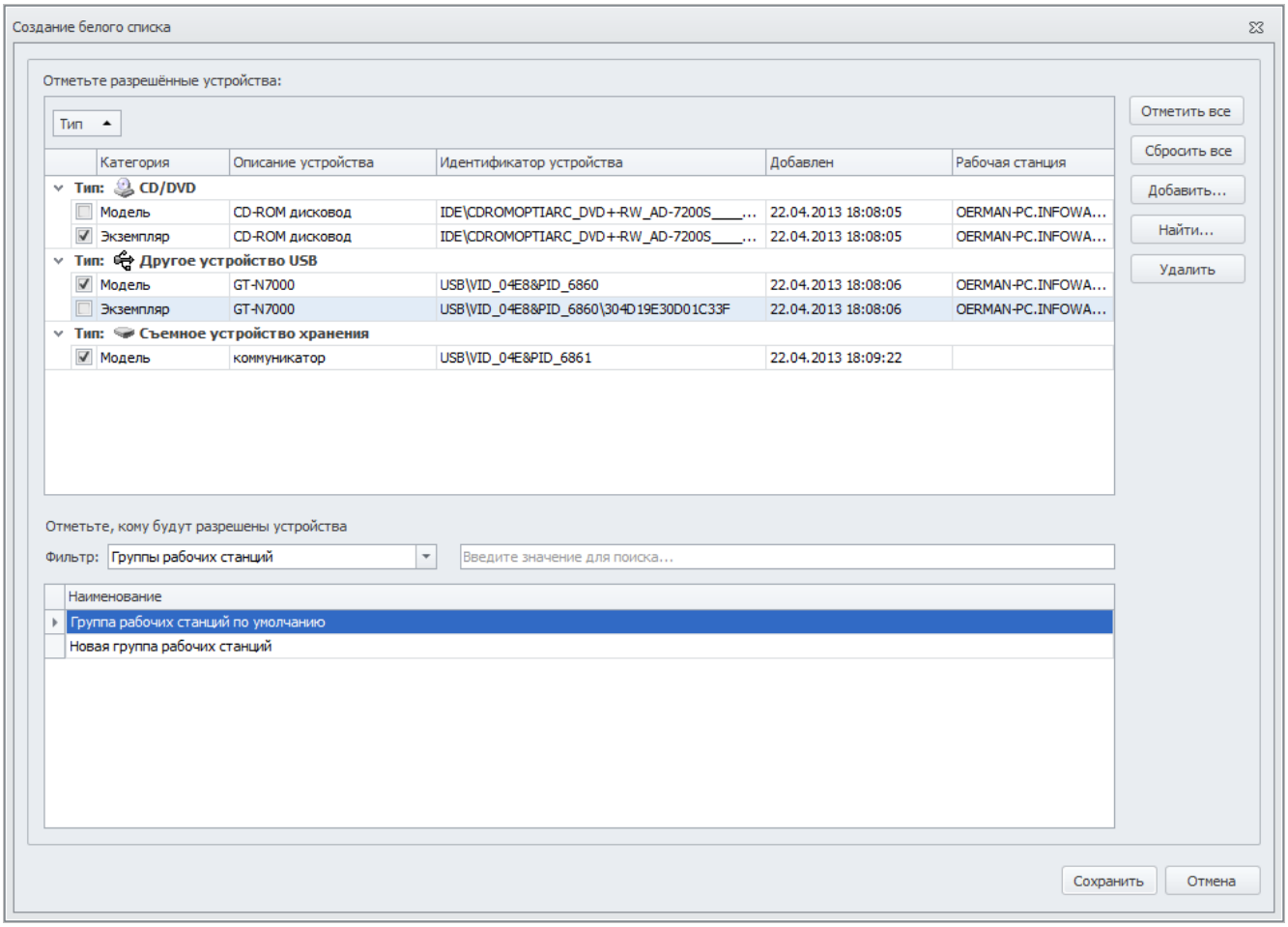
Действие белого списка распространяется на определенный (назначенный) объект: сотрудника, группу сотрудников, рабочую станцию или группу рабочих станций.

Внимание!
Для одного объекта назначения (сотрудника, группы сотрудников, рабочей станции или группы рабочих станций) может быть 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.

   На экран будет выведено диалоговое окно **Создание белого списка**.



3. В таблице с зарегистрированными в системе устройствами отметьте модели и экземпляры, доступ к которым должен быть безусловно разрешен.

   > **Внимание!**
   >
   > 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
   - рабочие станции
   - группы рабочих станций.

   Внизу отобразится перечень записей, соответствующих выбранному фильтру.

   Вы также можете воспользоваться строкой поиска, введя искомое имя или его часть.

5. Выберите сотрудника / группу сотрудников / рабочую станцию / группу рабочих станций, на которые должно распространяться действие белого списка.
6. Нажмите **Сохранить**.

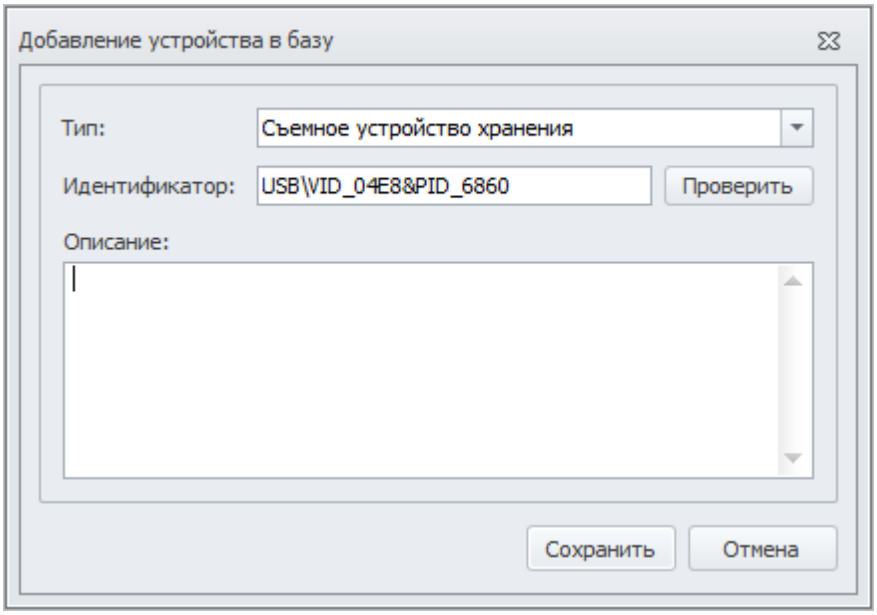
3.4.2.5.2.1 Добавление записи об устройстве

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 контролируемой рабочей станции.

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).

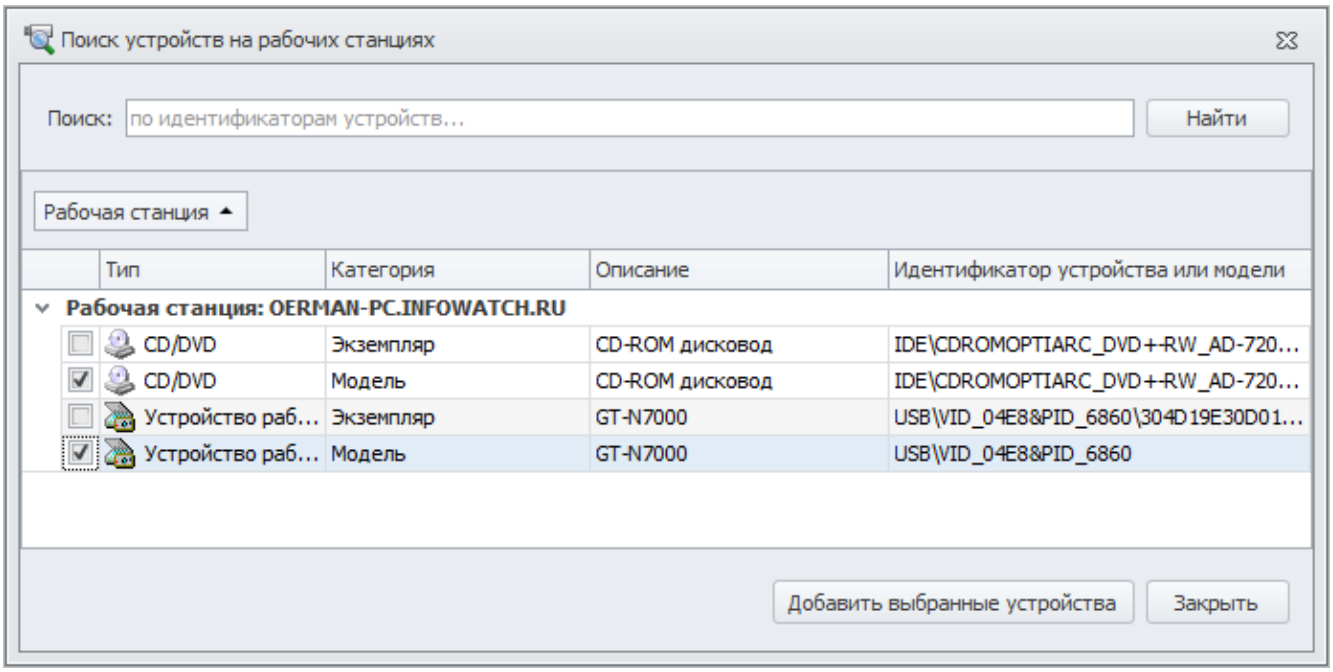
   Чтобы удостовериться в допустимости введённого кода, нажмите **Проверить**.

   Внимание!
   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.

   - в поле **Описание** введите описание устройства.
4. Нажмите **Сохранить**.

Чтобы добавить запись с помощью поиска устройств, подключавшихся к рабочим станциям:

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 рабочих станциях**.



3. В списке контролируемых рабочих станций выберите необходимую рабочую станцию одним из следующих способов:
   - нажмите кнопку ▸, соответствующую необходимой рабочей станции;
   - дважды щелкните левой кнопкой мыши на названии рабочей станции.

   Раскроется список всех устройств, которые подключались к выбранной рабочей станции за весь период работы на этой станции Клиента Device Monitor.
4. Отметьте флажками устройства, информацию о которых вы хотите добавить.
5. Нажмите **Добавить выбранные устройства**.

3.4.2.5.2.2 Удаление записи об устройстве

Чтобы удалить запись о зарегистрированном устройстве из системы:

1. Откройте диалоговое окно **Создание белого списка** (см. "Добавление белого списка").
2. В таблице с зарегистрированными устройствами выделите экземпляр или модель устройства и щелкните по нему правой кнопкой мыши. Затем в раскрывшемся контекстном меню выберите пункт **Удалить устройство**.
3. В открывшемся окне подтверждения нажмите на кнопку **ОК**.

3.4.2.5.3 Установка периода действия записи

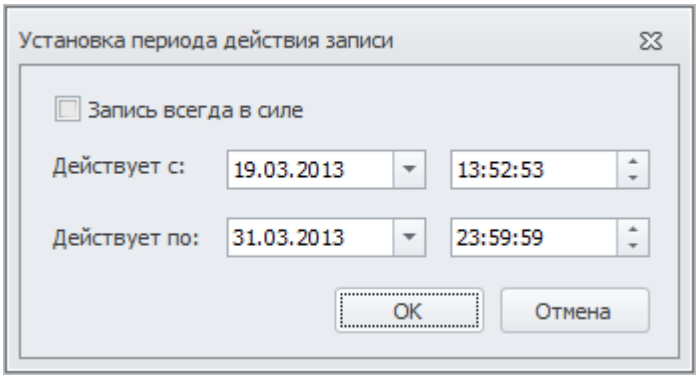
Для каждого экземпляра или модели устройства, внесенного в белый список, разрешение на его использование отображается в виде отдельной записи. По умолчанию эта запись (разрешение) действует в течение практически бесконечного периода времени (с 01.01.1753 по 31.12.9999). Вы можете установить ограничение 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 выделите 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**.

   В результате на экран будет выведено диалоговое окно **Установка периода действия записи**.



5. Укажите период действия записи и нажмите кнопку **ОК**.

3.4.2.5.4 Редактирование белого списка

Чтобы отредактировать параметры белого списка:

1. Перейдите к разделу **Белые списки**.
2. В области **Белые списки** на Панели навигации выделите 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.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно **Редактирование белого 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 из списка зарегистрированных (см. "Добавление устройства в базу" и "Удаление устройства из базы").
5. В таблице с зарегистрированными устройствами снимите или установите флажки, чтобы изменить список моделей и экземпляров устройств, включенных в белый список.
6. Нажмите **Сохранить**.

Внимание!
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.

раздел "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

3.4.2.5.5 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.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление белого списка.

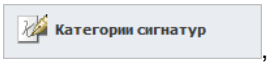
Внимание!
Поскольку работа с белыми списками ведется в режиме редактирования схемы безопасности, то для того, чтобы изменения окончательно вступили в силу, необходимо сохранить схему безопасности (см. раздел "Редактирование схемы безопасности"). Если схема безопасности не будет сохранена, то все изменения будут утеряны.

3.4.2.6 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.

   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.

Внимание!
Предустановленные категории сигнатур редактированию и удалению не подлежат. Создание сигнатур не предусмотрено.

Вы можете:

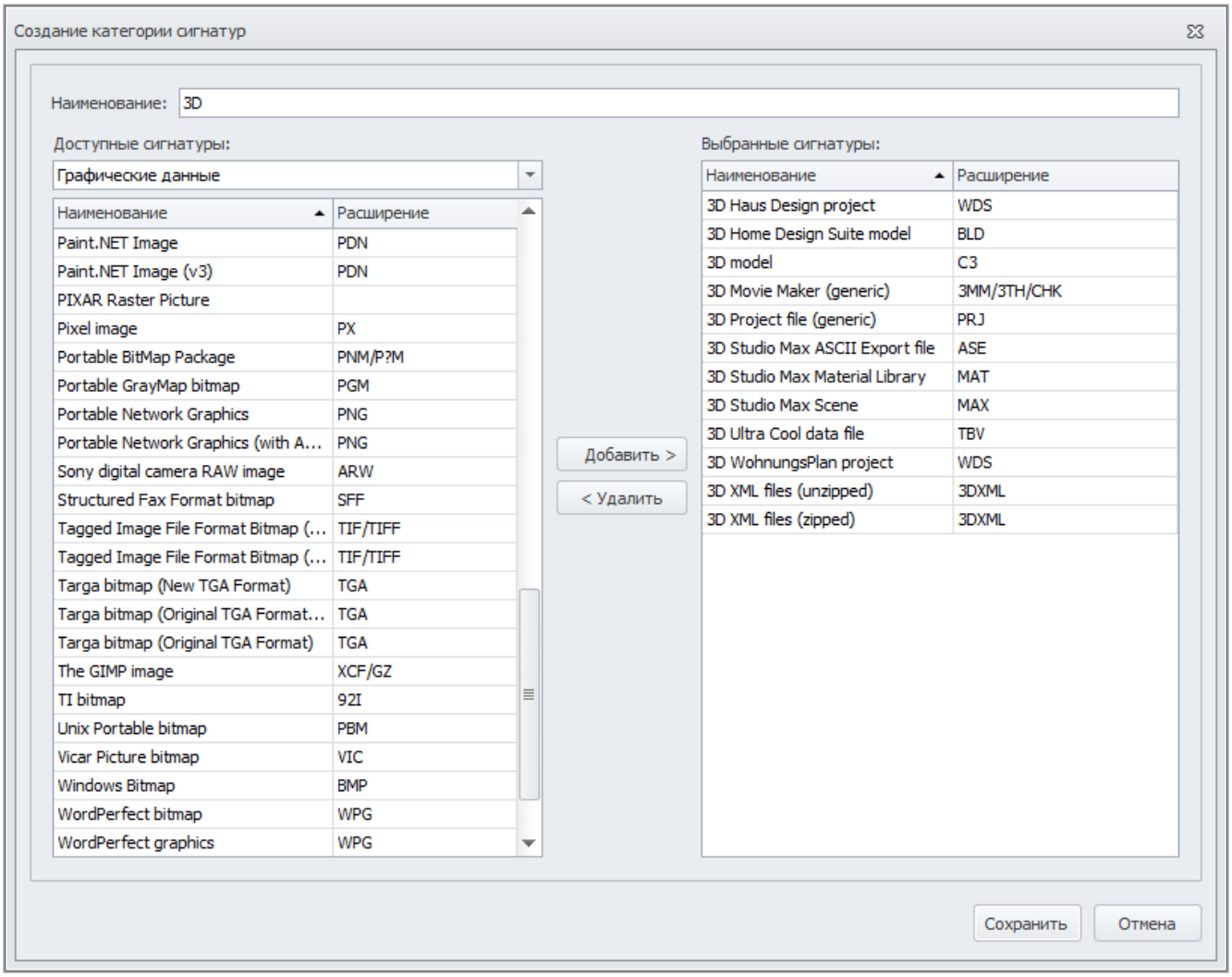
- создавать категории сигнатур;
- наполнять созданные категории, копируя в них сигнатуры из числа предустановленных;
- удалять созданные категории сигнатур, если они не используются ни в одном правиле.

3.4.2.6.1 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.

   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, выделите их на правой панели **Выбранные сигнатуры** и нажмите **Удалить**.
6. Нажмите **Сохранить**.

3.4.2.6.2 Изменение категории сигнатур

После того, как вы создали категорию сигнатур (см. "Создание категории сигнатур"), вы можете наполнить её:

- Вызвав окно редактирования сигнатуры (выбрать категорию и в главном меню выберать команду **Правка > Изменить**, либо нажать кнопку **Изменить** в верхней части Панели навигации, либо дважды щелкнуть левой кнопкой мыши по названию выделенной категории), и затем определить список сигнатур как описано в разделе "Создание категории сигнатур".

либо

- Копируя 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 выделите название предустановленной категории, которая содержит сигнатуру, которую нужно скопировать.
3. В рабочей области главного окна выделите 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,

выделите 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 сочетание клавиш **Ctrl+R**.

3.4.2.6.3 Удаление категории сигнатур

Внимание!
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.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление категории сигнатур.

Внимание!
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.

3.4.3 Предоставление сотруднику временного доступа

Сотрудник, для которого действует правило, запрещающее соединения вне корпоративной сети (см. "Контроль сетевых соединений" и "Настройка правила для Network Monitor"), может из меню Клиента InfoWatch Device Monitor, команда **Контроль сети**, запросить временный доступ к внешним соединениям.

Внимание!

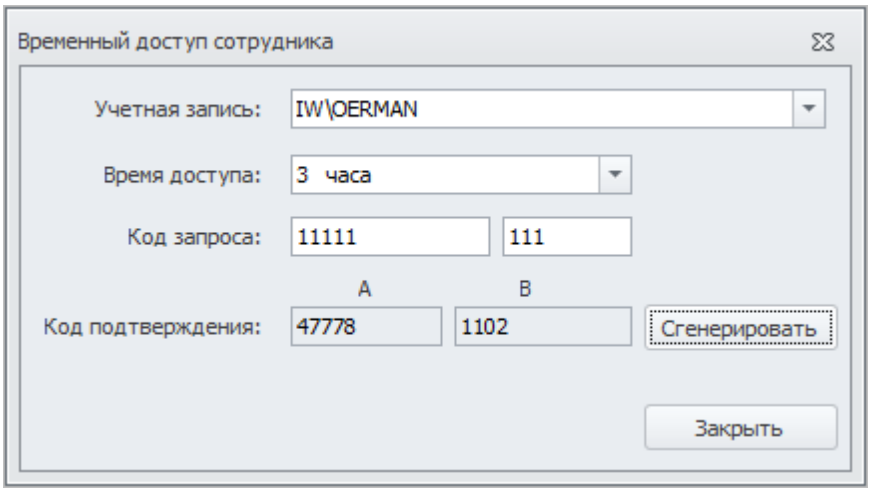
Возможность запросить доступ есть у сотрудника только в том случае, если для уведомлений сотрудника действует опция **Отображать иконку в трее** (подробнее см. "Общие настройки работы Клиентов").

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. Из раскрывающегося списка **Учетная запись** выберите запись сотрудника, которому требуется предоставить временный доступ.
3. Из раскрывающегося списка **Время доступа** выберите временной промежуток, на который предоставляется доступ.
4. В поле **Код запроса** введите код, переданный сотрудником.
5. Нажмите **Сгенерировать**.
   В поле **Код подтверждения** появится код, который нужно передать сотруднику для того, чтобы он смог получить требуемый доступ.
6. Нажмите **Закрыть**.

3.5 Просмотр событий

Клиенты InfoWatch Device Monitor, установленные на контролируемых рабочих станциях, обеспечивают сохранение сведений о работе с внешними устройствами, передачи файлов по сетевым соединениям и использовании мессенджеров для передачи данных. Данные сведения 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 Клиентов".

Просмотр событий производится в разделе **События**. Чтобы перейти к этому разделу, воспользуйтесь кнопкой **События**, расположенной на Панели навигации.

Чтобы просмотреть события,

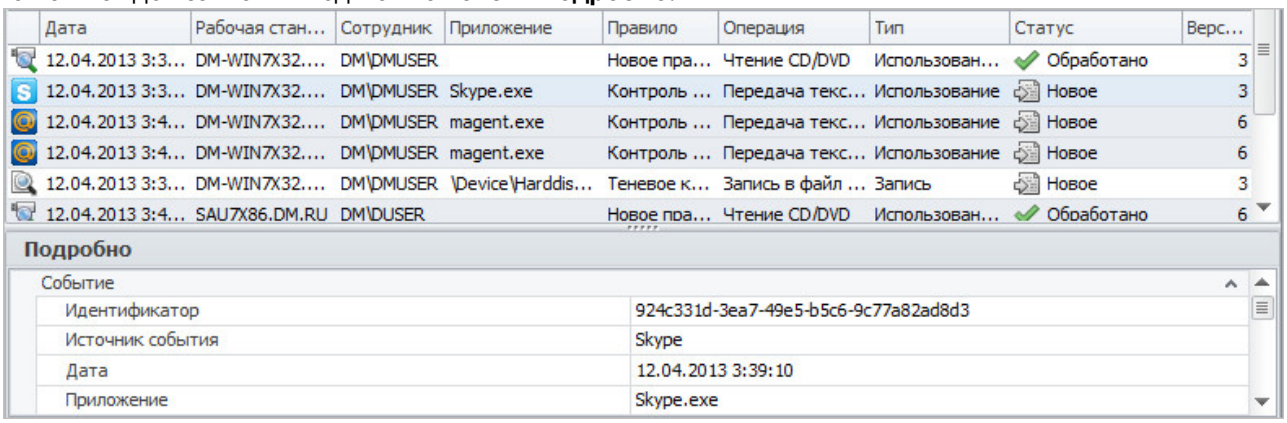
щелкните левой кнопкой мыши по названию нужного фильтра в списке фильтров.

Предусмотрено два предустановленных фильтра:

- **Все события**
- **За сегодня**

При необходимости, вы можете создать собственные фильтры для просмотра событий, как описано в разделе "Фильтры событий".

Сведения о событиях 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**.



Имя атрибута	Описание	Возможные значения
Общие атрибуты		
Идентификатор	Уникальный номер, присваваемый событию в Системе	
Источник события	Тип события в зависимости от перехватчика	- **Файловое** – File Monitor; - **От устройств** – Device Monitor; - **От принтера** – Print Monitor; - **Skype, XMPP, MMP** – IM Client Monitor; - **FTP** – FTP Monitor; - **Сетевое** – Network Monitor.
Дата	Дата и время (в часах и минутах) фиксации события на рабочей станции. На сервере Device Monitor событие сохраняется в UTC, а в Консоли управления отображается соответственно локальному времени того компьютера, где работает Консоль	
Приложение	Имя исполняемого файла и/или наименование процесса, выполняющего действие, если его удалось определить	
Рабочая станция	Наименование рабочей станции, где зафиксировано событие	
Сотрудник	Наименование домена (наименование рабочей станции 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	
Операция	Описание действия или попытки действия, выполненного сотрудником	
Сервер	Имя сервера InfoWatch Device Monitor, на который Клиент передал информацию о событии	
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; голосовой чат; пересылка данных по протоколу FTP - **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 Client, если этого требует политика безопасности. - **Запрет использования** – попытка передачи данных по запрещенному каналу.
Статус	Состояние обработки события на сервере	- **Новое** - **Обработано** - **Отправлено в Traffic Monitor**
Версия схемы безопасности	Номер версии схемы безопасности, используемой на рабочей станции 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
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 у спешно создана - **ошибка создания копии** – например, при нехватке свободного места на клиенте
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	
Описание устройства	Описание используемого устройства, полученное от операционной системы на рабочей станции, где установлен Клиент	
Для событий с источником *Skype, XMPP, MMP*		
Имя пользователя клиента мгновенных сообщений	UIN пользователя, авторизованного в мессенджере на рабочей станции	
Состояние	Результат теневого копирования	- **копия не создавалась** – правило не требует создания теневой копии - **копия создана** – теневая копия у спешно создана - **ошибка создания копии** – например, при нехватке свободного места на клиенте
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 или размер файла записи голосового чата	
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. Теневая копия задания на печать создана успешно. Задание содержало только графические данные; 5. Теневую копию не нужно было создавать 6. Теневая копия задания на печать создана частично. Графические данные обработаны полностью. Текстовые данные обработаны частично. 7. Теневая копия задания на печать создана частично. Графические данные обработаны частично. Текстовые данные обработаны полностью. 8. Теневая копия задания на печать создана успешно. Задание содержало только текстовые 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 у спешно создана - **ошибка создания копии** – например, при нехватке свободного места на клиенте
Для событий с источником *FTP*		
Состояние	Результат теневого копирования перемещаемых данных	- **копия не создавалась** – правило не требует создания теневой копии - **копия создана** – теневая копия у спешно создана - **ошибка создания копии** – например, при нехватке свободного места на клиенте

Отправитель	Имя, под которым сотрудник авторизован на FTP сервере	
FTP сервер	Имя или IP адрес 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, то - 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 *Сетевое*		
Время снятия запрета	Для операции *Временное снятие запрета сетевых подключений* - начало временного промежутка, на который предоставляется доступ. Подробнее см. "Предоставление сотруднику временного доступа".	
Время окончания действия пароля	Для операции *Временное снятие запрета сетевых подключений* - окончание временного промежутка, на который предоставляется доступ. Подробнее см. "Предоставление сотруднику временного доступа".	
Сервер подключения	Для операции *Соединение запрещено* - адрес или имя запрещенного сервера, к которому была попытка соединения.	
Порт	Для операции *Соединение запрещено* - номер порта, по которому была произведена попытка соединения.	

При необходимости, вы можете освободить место в базе данных, удалив из неё всю информацию об уже обработанных событиях (статус **Обработано** или **Отправлено в Traffic Monitor**). Подробнее см. "Удаление событий".

3.5.1 Фильтры событий

Помимо предустановленных фильтров вы можете создавать собственные фильтры для просмотра информации о событиях.

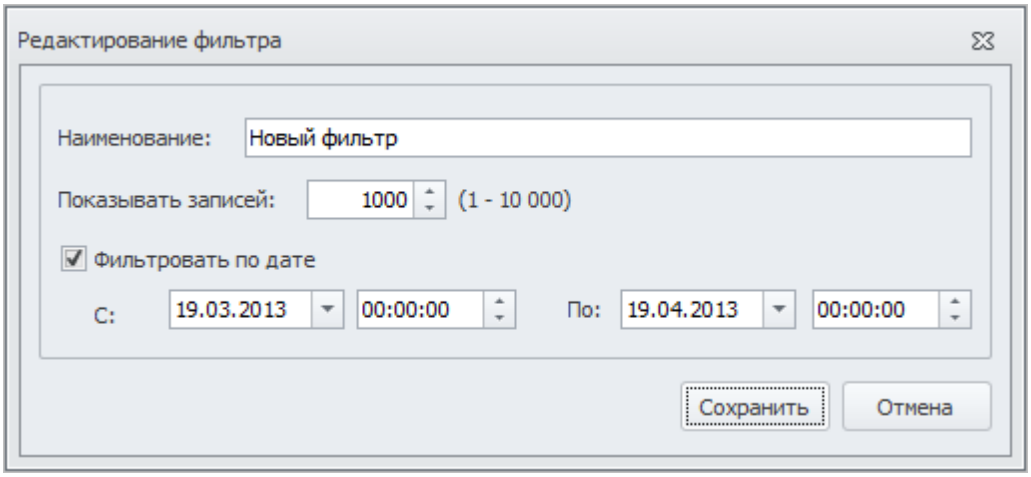
Чтобы добавить или отредактировать фильтр:

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

Действие	**Шаги**
Создание фильтра	• в главном меню выберите команду **Правка > Добавить фильтр**;

Действие	Шаги
	• воспользуйтесь кнопкой **Создать фильтр**, расположенной верхней части Панели навигации.
Редактирование фильтра	1. В области **События** на Панели навигации выделите 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

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, установите флажок в 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**.

3.5.2 Удаление событий

Информация об уже обработанных событиях (статус **Обработано** или **Отправлено в Traffic Monitor**) 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**.

3. В открывшемся диалоговом окне **Удаление 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**.
4. В открывшемся диалоговом окне подтверждения нажмите **Да**.

В результате будет отображено, сколько событий было удалено из базы данных.

3.6 Удаленная установка, обновление и удаление Клиентов

Установка, обновление и удаление Клиентов 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 клиентского ПО, смены пароля деинсталляции, а также наблюдать за состоянием выполнения этих процессов.

Задачи удаленного управления Клиентом выполняются с помощью специального **Агента распространения** , передаваемого на клиентские рабочие станции. Для его корректной работы необходимо обеспечить выполнение следующих условий:

- Рабочие станции, на которые производится установка, должны удовлетворять необходимым аппаратным и программным требованиям: см. "Требования к аппаратному и программному обеспечению Клиента InfoWatch Device Monitor".
- Проактивная антивирусная защита на рабочих станциях должна быть отключена.
- 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 Агента распространения InfoWatch Device Monitor.

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 Клиентов. Агент распространения
- Создание задачи первичного распространения
- Создание задачи обновления
- Создание задачи смены пароля деинсталляции
- Создание задачи удаления
- Запуск, остановка, редактирование и удаление задачи

- Ошибки установки Клиентов

Вы также можете осуществлять установку и обновление Клиента с помощью средств распространения программного обеспечения (например, в Microsoft Active Directory посредством механизма групповых политик). Для этого удобно использовать пакет установки, созданный как описано в разделе "Создание пакета установки".

3.6.1 Просмотр задач

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

На панели **Подробно** для выбранной задачи отображаются следующие параметры:

Параметр	Описание
Наименование	Имя задачи, указанное при её создании
Описание	Описание задачи, указанное при её создании
Тип	Один из следующих типов задач: • первичное распространение; • смена пароля; • обновление; • удаление.
Статус	Текущее состояние задачи. Возможные значения: • запущена, • остановлена, • выполнена
Период повторного запуска	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 производится не будет.
Количество попыток повторного запуска	Максимальное количество попыток перезапустить задачу распространения на рабочей станции.
Для задач первичного распространения	
Запрашивать у сотрудника разрешение на работу плагина Skype	Признак того, что после установки Клиента, в Skype будет отображено сообщение, запрашивающее разрешение на работу перехватчика Skype. Подробнее см. "Общие настройки политики безопасности" и "Создание пакета установки".
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. "Общие настройки политики безопасности", "Создание инсталляционного комплекта" и "Настройка уведомлений сотрудников о нарушении правил"
Отображать иконку в области уведомления панели задач Windows	Признак того, что в области уведомлений панели задач Windows на компьютере, где установлен Клиент, будет отображаться значок . При нажатии на этот значок доступна информация о работе Клиента, а также список контролируемых в данный момент устройств.
Пароль для деинсталляции	Признак того, задан ли пароль, запрашиваемый у сотрудника при попытке удалить Клиент Device Monitor.

Для задач первичного распространения и обновления	
Директория для установки	Папка на рабочих станциях, куда будет устанавливаться Клиент Device Monitor.
Имя пользователя для установки	Имя пользователя, от имени которого выполняется запущенная задача на рабочих станциях.
Продолжительность ожидания перезагрузки	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	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.
Для задач смены пароля деинсталляции	
Пароль для деинсталляции	Признак того, задан ли пароль, запрашиваемый у сотрудника при попытке удалить Клиент Device Monitor

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

Параметр	Описание
Адрес	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 Клиентов") • **Нет доступа** • **Выполнена**
Версия клиента	Версия Клиента, установленного в настоящий момент на рабочей станции
Операционная система	Операционная система, установленная на рабочей станции.
Разрядность опер. 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.

3.6.2 Подготовка к первичной установке Клиентов. Агент распространения

Удаленная установка Клиента средствами InfoWatch Device Monitor выполняется с применением специального **Агента распространения**.

Для того чтобы удаленная установка Клиента средствами InfoWatch Device Monitor была произведена корректно, необходимо обеспечить выполнение следующих условий:

- Рабочие станции, на которые производится установка, должны удовлетворять необходимым аппаратным и программным требованиям: см. "Требования к аппаратному и программному обеспечению Клиента InfoWatch Device Monitor".
- Проактивная антивирусная защита на рабочих станциях должна быть отключена.
- 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 Агента распространения InfoWatch Device Monitor

    или
  - в брандмауэре должен быть открыт порт **15505** (порт по умолчанию, по которому агент распространения ждёт соединения) для входящих соединений, если он не был изменён в настройках сервера (см. "Раздел <applicationSettings>", параметр **CommunicationPort**).

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:

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.

3.6.2.1 Включение административных разделяемых ресурсов

Для передачи Агента распространения InfoWatch Device Monitor на целевые рабочие станции через ад министративные разделяемые ресурсы необходимо выполнение следующих требований:

- Если рабочая станция с Windows XP не входит в домен, то в настройках политики безопасности этой рабочей станции необходимо для параметра **Network access: Sharing and security model for local accounts** указать значение `Classic`.
- На рабочих станциях должны быть включены административные разделяемые ресурсы вида `\\computername\admin$` (в Windows Vista и Windows 7 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**.

3.6.2.2 Настройки брандмауэра

Требования к настройкам брандмауера:

Протокол приложения	Транспортный протокол	Порт
RPC	TCP	135
RPC over HTTPS	TCP	593
NetBIOS Datagram Service	UDP	138
NetBIOS Name Resolution	UDP	137
NetBIOS Session Service	TCP	139
SMB	TCP	445

Для быстроты определения доступности рабочей станции требуется разрешить протокол ICMP.

Для брандмауера Windows необходимо разрешить предустановленное правило "**Общий доступ к файлам и принтерам**" ("**File printing and sharing**").

3.6.3 Создание задачи первичного распространения

Первичное распространение (установка средствами Консоли Управления) Клиентов 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 Клиента.

Внимание!

Если учетная запись, от имени которой запущен Сервер, не имеет прав администратора на всех рабочих станциях, где будет производиться установка, то для первичного распространения Клиентов 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 (WIndows предупреждает, что пароль истекает через 3 дня, нужно сменить), 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 Клиентов InfoWatch Device Monitor ("Создание пакета установки") и установить его другими способами ("Установка Клиента InfoWatch Device Monitor стандартным способом" и "Установка Клиента с помощью средств распространения программного обеспечения").

Чтобы создать задачу первичного распространения клиентских приложений 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 первичного распространения**, введите имя задачи и её описание, затем нажмите **Далее**.
4. Создайте список рабочих станций, на которые необходимо установить Клиент Device Monitor. Чтобы добавить рабочую станцию (или несколько рабочих станций):
   a. Нажмите **Добавить**. В открывшемся окне вы можете выбрать рабочие станции:
      - из директории;
      - из сетевого окружения Microsoft Windows Network;
      - из числа ранее зарегистрированных в системе (например, в результате ручной установки Клента Device Monitor) и уже принадлежащих существующим группам Device Monitor (узел **Группы рабочий станций DM**).

   b. Выберите необходимые рабочие станции или группы рабочих станций, отмечая их флажком. Свёрнутые группы отмечены пиктограммой ; развёрнутые - . Чтобы развернуть или свернуть группу, нажмите на или дважды нажмите на названии группы левой кнопкой мыши.

      Внимание!
      Если вы отметите флажком группу, то будут выбраны только компьютеры, непосредственно входящие в отмеченную группу. Подгруппы отмеченной группы и компьютеры, входящие в подгруппы отмеченной группы, в этом случае не выбираются: их следует отмечать дополнительно.

      Вы также можете указать имя или IP-адрес рабочей станции в строке внизу диалогового окна. При перечислении используйте точку с запятой.

   c. После того, как вы укажете добавляемые рабочие станции, нажмите **ОК**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи будет отображен перечень выбранных рабочих станций.

   Чтобы удалить рабочую станцию из списка, выделите её имя и нажмите **Удалить**.

   После того, как вы полностью определите список рабочих станций, нажмите **Далее**.
5. Отобразятся сервера, которые на данный момент зарегистрированы в Системе.
   Вы также можете изменить директорию на рабочих станциях, куда будет устанавливаться Клиент (по умолчанию – `%Program Files%\Infowatch\DeviceMonitor\Client`).
   Нажмите **Далее**.
6. Определите параметры запуска задачи:
   - Количество попыток запустить задачу и время между попытками, в минутах: эти параметры будут использованы, если первый запуск по каким-либо причинам не произошёл. Если запуск завершился с ошибкой, то повторный запуск производится не будет.
   - **Ожидать перезагрузки без уведомления сотрудника**. Начать уведомление сотрудника сразу (парамер *Не ожидать*), через указанное время (параметр *Ожидать* - требуется указать время до начала уведомлений), не уведомлять сотрудника вплоть до принудительной перезагрузки (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, Клиент Device Monitor начнёт 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.

- **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.

  Внимание!
  Предупреждение пред 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 завершён, и сотрудник не перезагрузил компьютер.

По окончании настройки, нажмите **Далее**.

7. Определите настройки работы Клиента:
   - Чтобы защитить клиентское приложение от удаления сотрудником, укажите пароль, который будет запрашиваться при попытке удалить Клиент Device Monitor, и подтвердите его.
   - **Запрашивать у сотрудника разрешение на работу плагина Skype** – признак того, что после установки Клиента, в Skype будет отображено сообщение, запрашивающее разрешение на работу перехватчика Skype:
     - Если сотрудник разрешил работу перехватчика, то он будет работать до тех пор, пока сотрудник не запретит его работу в меню Skype (**Tools -> Options -> Advanced settings -> Manage other programs' access to Skype**). В последнем случае работа Skype будет принудительно остановлена.
     - Если сотрудник запретил работу перехватчика, то работа Skype будет остановлена. При повторной попытке запуска Skype сотруднику опять будет предложено дать разрешение на использование перехватчика.
     - Если флажок в данном поле не установлен, то подтверждения сотрудника при запуске перехватчика не требуется. Клиент Device Monitor попытается (с негарантированным результатом) автоматически нажать кнопку разрешения за пользователя.

     Внимание!
     Неуведомление об использовании перехватчика может входить в конфликт с действующим законодательством вашей страны.
   - **Выводить сотруднику уведомления о работе Device Monitor Client** – признак того, что при попытке сотрудника выполнить действие, запрещенное политикой безопасности, ему будет отображаться предупреждающее уведомление. Подробнее см. "Настройка уведомлений сотрудников о нарушении правил"
   - **Отображать иконку в области уведомлений панели задач** – признак того, что в области уведомлений панели задач Windows на компьютере, где установлен Клиент, будет отображаться иконка . При нажатии на этот значок доступна информация о работе Клиента, а также список контролируемых в данный момент устройств.
   - Чтобы выполнение задачи началось немедленно после её сохранения, установите флажок в поле **Запустить задачу сразу после сохранения**. При необходимости, укажите параметры учетной записи с правами администратора на всех рабочих станциях, где будет производиться установка.
   - Укажите параметры учетной записи, от имени которой будет запущена задача. Эта учетная запись должна обладать правами администратора на всех рабочих станциях, где будет производиться установка.

     Внимание!
     Пароль учётной 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 (WIndows предупреждает, что пароль истекает через 3 дня, нужно сменить), то задача первичного распространения, запущенная от имени этого пользователя, не сможет быть выполнена.

   По окончании настройки, нажмите **Далее**.
8. Просмотрите сводку информации о задаче. Если какие-либо параметры требуется изменить, вы

можете вернуться к настройкам (кнопка **Назад**). Если всё указано верно, нажмите **Готово**.

3.6.4 Создание задачи обновления

Обновление клиентских приложений InfoWatch Device Monitor требуется после того, как было выполнено обновление серверной части InfoWatch Device Monitor: подробнее см. "Обновление серверной части InfoWatch Device Monitor".

> **Примечание:**
> Помимо нижеуказанного способа, вы можете использовать функцию автоматического создания задачи обновления для выбранных рабочих станций, как описано в разделе "Обновление Клиентов на контролируемых рабочих станциях".

Чтобы создать задачу обновления клиентских приложений 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 обновления**, введите имя задачи и её описание, затем нажмите **Далее**.
4. На шаге 2 создайте список рабочих станций, на которых необходимо обновить Клиент Device Monitor. Чтобы добавить рабочую станцию (или несколько рабочих станций):
   a. Нажмите **Добавить**. В открывшемся диалоговом окне **Выбор компьютеров**, в узле **Группы рабочих станций DM**, отобразится перечень рабочих станций, на которые установлен Клиент Device Monitor, версия которого не соответствует версии Сервера Device Monitor, но которые могут быть автоматически обновлены (версия клиентского ПО должна быть 4.0.651 и выше).
   b. Выберите необходимые рабочие станции или группы рабочих станций, отмечая их флажком. Свёрнутые группы отмечены пиктограммой ▸; развёрнутые - ▾. Чтобы развернуть или свернуть группу, нажмите на ▸ или дважды нажмите на названии группы левой кнопкой мыши.

      > **Внимание!**
      > Если вы отметите флажком группу, то будут выбраны только компьютеры, непосредственно входящие в отмеченную группу. Подгруппы отмеченной группы и компьютеры, входящие в подгруппы отмеченной группы, в этом случае не выбираются: их следует отмечать дополнительно.

   c. После того, как вы укажете добавляемые рабочие станции, нажмите **ОК**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи будет отображен перечень выбранных рабочих станций.

   Чтобы удалить рабочую станцию из списка, выделите её имя и нажмите **Удалить**.

   После того, как вы полностью определите список рабочих станций, нажмите **Далее**. Выберите **Задача обновления** и нажмите **Далее**.
5. На шаге 3 укажите:
   - Параметры перезапуска задачи: они будут использованы, если первый запуск по каким-либо причинам не произошёл; если запуск завершился с ошибкой, то повторный запуск производится не будет. Укажите количество попыток и время между попытками, в минутах.
   - При необходимости, установите флажок в поле **Запустить задачу немедленно**: задача будет запущена сразу же после её сохранения.

   Нажмите **Далее**.
6. Просмотрите сводку информации о задаче Если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). Если всё указано верно, нажмите **Готово**

3.6.5 Создание задачи смены пароля деинсталляции

Чтобы создать задачу смены пароля, требуемого у сотрудника при попытке удалить клиентское приложение 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 смены пароля деинсталляции**, введите имя задачи и её описание, затем нажмите **Далее.**
4. На шаге 2 создайте список рабочих станций, на которых необходимо сменить пароль деинсталляции. Чтобы добавить рабочую станцию (или несколько рабочих станций):
   a. Нажмите **Добавить**. В открывшемся диалоговом окне **Выбор компьютеров**, в узле **Группы рабочих станций DM**, отобразится перечень рабочих станций, на которые установлен Клиент Device Monitor.
   b. Выберите необходимые рабочие станции или группы рабочих станций, отмечая их флажком. Свёрнутые группы отмечены пиктограммой ; развёрнутые - . Для того, чтобы развернуть или свернуть группу, дважды нажмите на ней левой кнопкой мыши.

   > **Внимание!**
   > Если вы отметите флажком группу, то будут выбраны только компьютеры, непосредственно входящие в отмеченную группу. Подгруппы отмеченной группы и компьютеры, входящие в подгруппы отмеченной группы, в этом случае не выбираются: их следует отмечать дополнительно.

   c. После того, как вы укажете добавляемые рабочие станции, нажмите **ОК**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи будет отображен перечень выбранных рабочих станций.

   Чтобы удалить рабочую станцию из списка, выделите её имя и нажмите **Удалить**.

   После того, как вы полностью определите список рабочих станций, нажмите **Далее**.
5. На шаге 3 укажите:
   - Пароль, который будет запрашиваться у сотрудника при попытке удалить Клиент Device Monitor. Подтвердите пароль.
   - Параметры перезапуска задачи: они будут использованы, если первый запуск по каким-либо причинам не произошёл; если запуск завершился с ошибкой, то повторный запуск производится не будет. Укажите количество попыток и время между попытками, в минутах.
   - При необходимости, установите флажок в поле **Запустить задачу немедленно**: задача будет запущена сразу же после её сохранения.

   Нажмите **Далее**.
6. Просмотрите сводку информации о задаче Если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). Если всё указано верно, нажмите **Готово**

3.6.6 Создание задачи удаления

Чтобы создать задачу централизованного удаления клиентских приложений 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**, введите имя задачи и её описание, затем нажмите **Далее**.
4. На шаге 2 создайте список рабочих станций, с которых необходимо удалить Клиент Device Monitor. Чтобы добавить рабочую станцию (или несколько рабочих станций):
   a. Нажмите **Добавить**. В открывшемся диалоговом окне **Выбор компьютеров**, в узле **Группы рабочих станций DM**, отобразится перечень рабочих станций, на которые установлен Клиент Device Monitor.
   b. Выберите необходимые рабочие станции или группы рабочих станций, отмечая их флажком. Свёрнутые группы отмечены пиктограммой ▸; развёрнутые - ▾. Для того, чтобы развернуть или свернуть группу, дважды нажмите на ней левой кнопкой мыши.

      Внимание!
      Если вы отметите флажком группу, то будут выбраны только компьютеры, непосредственно входящие в отмеченную группу. Подгруппы отмеченной группы и компьютеры, входящие в подгруппы отмеченной группы, в этом случае не выбираются: их следует отмечать дополнительно.

   c. После того, как вы укажете добавляемые рабочие станции, нажмите **ОК**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи будет отображен перечень выбранных рабочих станций.

   Чтобы удалить рабочую станцию из списка, выделите её имя и нажмите **Удалить**.

   После того, как вы полностью определите список рабочих станций, нажмите **Далее**.
5. На шаге 3 определите параметры перезапуска задачи: они будут использованы, если первый запуск по каким-либо причинам не произошёл; если запуск завершился с ошибкой, то повторный запуск производится не будет. Укажите количество попыток и время между попытками, в минутах.

   Чтобы начать выполнение созданной задачи сразу же после её сохранения, установите флажок в 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 всё указано верно, нажмите **Готово**.

3.6.7 Запуск, остановка, редактирование и удаление задачи

Если при создании задачи вы установили флажок **Запустить задачу немедленно**, то задача начнет выполняться немедленно после её 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 её вновь.

О порядке выполнения этих и других операций см. следующую таблицу.

Для выполнения любого из этих действий необходимо сначала выбрать необходимую задачу из списка на панели **Задачи**.

Действие	Шаги
Запуск задачи	• в главном меню выберите команду **Правка > Выполнить**; • воспользуйтесь кнопкой **Выполнить**, расположенной верхней части панели **Задачи**.
Остановка задачи	• в главном меню выберите команду **Правка > Остановить**; • воспользуйтесь кнопкой **Остановить**, расположенной верхней части панели **Задачи**.

Действие	Шаги
Изменение списка рабочих станций в задаче	Щелкните правой кнопкой на строке необходимой рабочей станции и выберите **Добавить рабочую станцию в задачу** или **Исключить рабочую станцию из задачи**. **Внимание!** Удалить рабочую станцию с запущенной, но незавершённой задачей, нельзя.
Редактирование задачи	• в главном меню выберите команду **Правка > Редактировать задачу**; • воспользуйтесь кнопкой **Редактировать задачу**, расположенной верхней части панели навигации • щелкните правой кнопкой на названии задачи и выберите **Редактировать задачу**. Определите новые параметры задачи, как это делается при её 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**. **Внимание!** Удалить задачу, где есть рабочие станции с запущенной, но незавершённой задачей, нельзя.
Просмотр журнала ошибок для рабочей станции	• щелкните правой кнопкой на строке необходимой рабочей станции и выберите пункт **Журнал ошибок**; • дважды щелкните левой кнопкой мыши на строке необходимой рабочей станции.

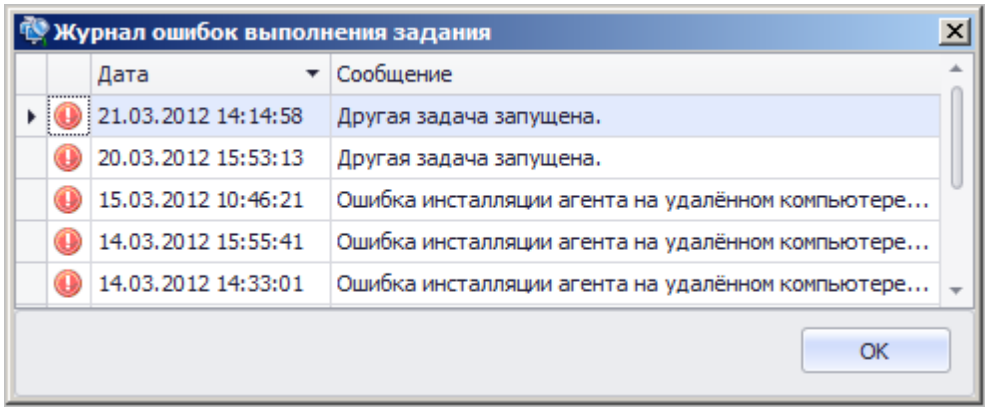
3.6.8 Ошибки установки Клиентов

В процессе выполнения задач на удаленную установку клиентских приложений 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 необходимой рабочей станции.



5. Для просмотра подробной информации об ошибке нажмите левой кнопкой мыши на необходимую строку. В результате будет отображено окно с описанием ошибки Windows.

Подробную информацию о причинах ошибки вы можете получить из её описания, кода ошибки или журнала, отображаемого в окне с описанием ошибки. В частности, 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 Клиента, 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.

3.6.9 Создание пакета установки

Пакет для установки Клиента InfoWatch Device Monitor, поставляемый в дистрибутиве, содержит следующие настройки по умолчанию:

- Папка на системном диске рабочих станций, куда будет устанавливаться Клиент – `%Program Files %\Infowatch\DeviceMonitor\Client`.
- Пароль деинсталляции – отсутствует.
- После установки Клиент 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 Клиента 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 сервера DM и каталог установки** отображаются сервера InfoWatch Device Monitor, которые на данный момент зарегистрированы в Системе. Они будут использоваться Клиентом для первоначальной установки.

   При необходимости, измените директорию на рабочих станциях, куда будет устанавливаться Клиент.

   Укажите локальную или сетевую директорию, куда будет сохранен готовый набор инсталляционных пакетов.

   Нажмите **Далее**.

3. На шаге **Укажите параметры запуска задачи и перезагрузки** определите следующие параметры:

   - **Ожидать перезагрузки компьютера**. Если данный флаг установлен, то Клиент Device Monitor

будет ожидать перезагрузки компьютера в течение указанного времени (в часах) без каких-либо уведомлений сотрудника.

- **Напоминать о необходимости перезагрузки**. Если данный флаг установлен, то после завершения ожидания перезагрузки в "молчаливом" режиме (см. настройку **Ожидать перезагрузки компьютера**), или сразу же после завершения процесса установки, Клиент Device Monitor начнёт уведомлять сотрудника о необходимости перезагрузки. При необходимости, измените длительность и частоту напоминаний и укажите текст сообщения, которое будет отображаться в напоминании о необходимости перезагрузки.

> **Внимание!**
> Если ни параметр **Ожидать перезагрузки компьютера**, ни параметр **Напоминать о необходимости перезагрузки** не установлен, или период действия их завершён и сотрудник не перезагрузил компьютер, то Клиент Device Monitor отобразит диалоговое окно о принудительной перезагрузке компьютера и даст сотруднику 5 минут до завершения своих операций. По истечении этих 5-и минут перезагрузка будет осуществлена принудительно.

Нажмите **Далее**.

4. Определите настройки работы Клиента до первого подключения к Серверу:
   - Чтобы защитить клиентское приложение от удаления сотрудником, укажите пароль, который будет запрашиваться при попытке удалить Клиент Device Monitor, и подтвердите его.
   - **Запрашивать у сотрудника разрешение на работу плагина Skype** – признак того, что после установки Клиента, в Skype будет отображено сообщение, запрашивающее разрешение на работу перехватчика Skype:
     - Если сотрудник разрешил работу перехватчика, то он будет работать до тех пор, пока сотрудник не запретит его работу в меню Skype (**Tools -> Options -> Advanced settings -> Manage other programs' access to Skype**). В последнем случае работа Skype будет принудительно остановлена.
     - Если сотрудник запретил работу перехватчика, то работа Skype будет остановлена. При повторной попытке запуска Skype сотруднику опять будет предложено дать разрешение на использование перехватчика.
     - Если флажок в данном поле не установлен, то подтверждения сотрудника при запуске перехватчика не требуется. Клиент Device Monitor попытается (с негарантированным результатом) автоматически нажать кнопку разрешения за пользователя.

   > **Внимание!**
   > Неуведомления об использовании перехватчика может входить в конфликт с действующим законодательством вашей страны.

   - **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"
   - **Отображать иконку в области уведомлений панели задач Windows** – признак того, что в области уведомлений панели задач Windows на компьютере, где установлен Клиент, будет отображаться значок . При нажатии на этот значок доступна информация о работе Клиента, а также список контролируемых в данный момент устройств.

   Нажмите **Далее**.
5. Просмотрите сводку информации о пакете установки Если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). Если всё указано верно, нажмите **Готово**.

В результате пакет для установки Клиента будет сохранен в папку, указанную на первом шаге создания пакета.

3.7 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.

3.7.1 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:

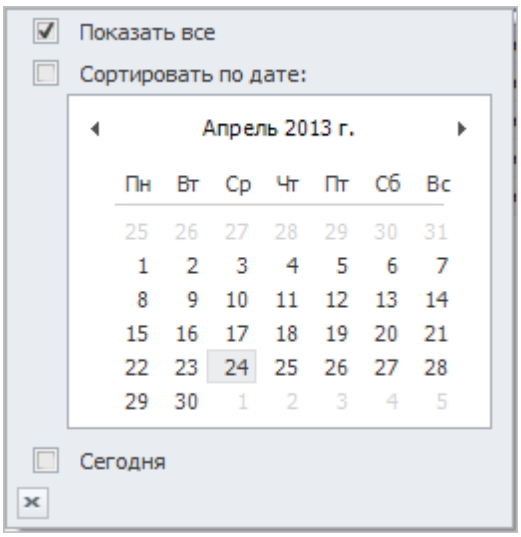
- Фильтрация по дате
- Использование стандартных фильтров
- Пользовательский фильтр
- Редактирование фильтра
- Отмена фильтра

3.7.1.1 Фильтрация по дате

Если в таблице отображается характеристика какого-либо временного параметра (например, дата и время установки Клиента, время записи в журнал Консоли, время последнего обращения к рабочей станции, дата зарегистрированного события и т.п.), то вы можете отфильтровать записи в 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** – установите флажок в этом поле, чтобы отобразились записи независимо от их даты.
   - **Сортировать по дате** – в календаре выберите необходимую дату.

     Чтобы выбрать временной период, выделите его, не отпуская левую копку 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. Установите флажок в этом поле, чтобы отобразились только те записи, дата которых находится описанном в диапазоне.

4. Нажмите ✖, чтобы применить выбранный фильтр и закрыть форму.

3.7.1.2 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).
   - **Не пустые**. 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. раздел "Пользовательский фильтр").

После этого в таблице будут отображены записи, удовлетворяющие заданным условиям фильтрации.

Чтобы отфильтровать записи по нескольким атрибутам,

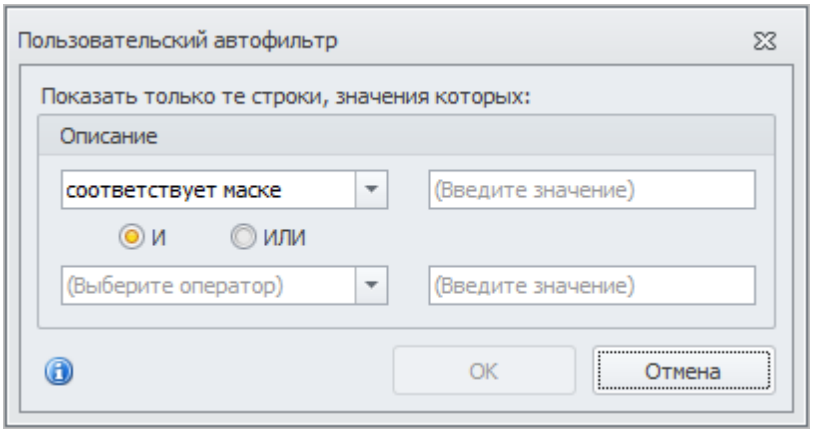
повторите процедуру создания простого фильтра для всех атрибутов, по которым будет производиться фильтрация.

В результате применения составного фильтра в таблице будут отображены записи, отфильтрованные по нескольким атрибутам одновременно.

3.7.1.3 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.

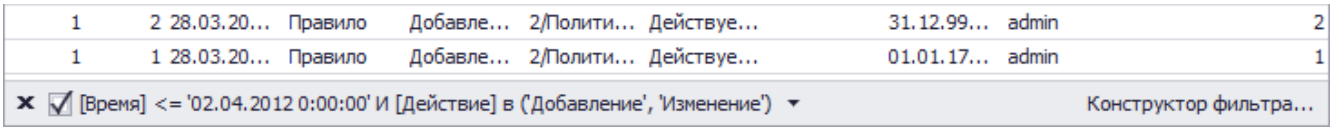
> **Примечание:**
> В качестве ограничения условия могут быть использованы операторы сравнения: *равно*, *не равно*, *больше*, *больше или равно*, *меньше*, *меньше или равно*; значения *пустые* (пустое поле) и *непустые* (непустое поле); а также текстовый фильтр с использованием маски. Чтобы получить 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 **OK**, 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.



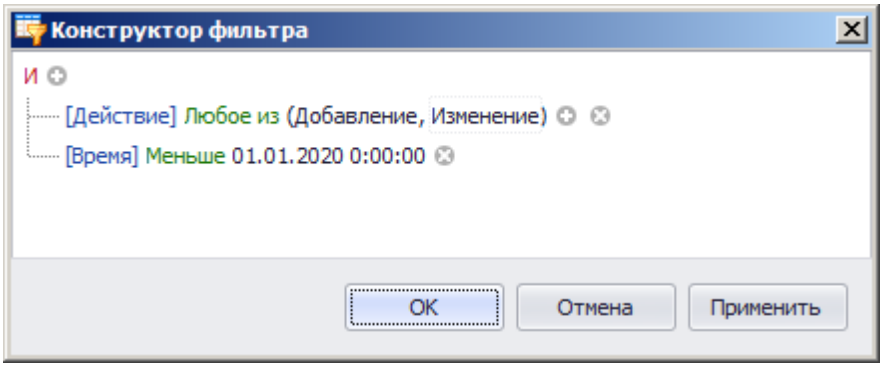
Чтобы отменить действие фильтра и просмотреть все записи таблицы, снимите флажок в строке фильтра. Чтобы применить фильтр вновь, установите флажок.

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.

3.7.1.4 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 пользоваться следующими действиями:

Действие	**Шаги**
Изменить атрибут, значение атрибута или оператор	1. Щелкните левой кнопкой мыши по названию атрибута/значения атрибута/оператора 2. 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	1. Щелкните левой кнопкой мыши по названию логического оператора 2. В меню выберите **Добавить группу**
Удалить группу условий	1. Щелкните левой кнопкой мыши по названию группы условий оператора 2. 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 **OK**.

3.7.1.5 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 флажок 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.

3.7.2 Группирование и сортировка записей

Функции группирования предназначены для организации записей таблицы в соответствии с выбранной схемой группы. Схема группы отображается на панели группы, распложенной над строкой заголовков столбцов. Группирование выполняется по одному или нескольким атрибутам записей (столбцам таблицы).

Чтобы сгруппировать записи по какому-либо атрибуту:

1. В строке заголовков столбцов таблицы щелкните левой кнопкой мыши по заголовку столбца, название которого соответствует нужному атрибуту.
2. Щелкните левой кнопкой мыши по выделенному заголовку 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.

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.

3.7.3 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	
Подключение к Серверу	F4

Название функции	**Клавиши быстрого доступа**
Выход из Консоли	Shift+F4
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+2
Переход к разделу Группы сотрудников	Ctrl+3
Переход к разделу Группы рабочих станций	Ctrl+4
Переход к разделу Белые списки	Ctrl+5
Переход к разделу Категории сигнатур	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
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

Название функции	Клавиши быстрого доступа
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
Работа с группами рабочих станций	
Создание группы рабочих станций	Ctrl+N
Редактирование группы рабочих станций	Ctrl+E
Удаление группы рабочих станций	Ctrl+D
Работа с контролируемыми рабочими станциями	
Добавление рабочей станции	Ctrl+Shift+I
Исключение рабочей станции из группы	Delete
Удаление рабочей станции из схемы безопасности	Shift+Delete
Работа с белыми списками	
Создание белого списка	Ctrl+N

Название функции	Клавиши быстрого доступа
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
Работа с задачами удаленной установки и обновления Клиентов	
Создание задачи	Ctrl+N
Редактирование задачи	Ctrl+E
Удаление задачи	Ctrl+D
Добавление рабочей станции в выбранную задачу	Ctrl+Shift+N
Исключение рабочей станции из выбранной задачи	Delete
Просмотр журнала ошибок для выбранной рабочей станции выбранной задачи	Ctrl+L

4 Разрешение проблем

В случае возникновения проблем в работе сервера, вы можете просмотреть ошибки и информационные сообщения от всех модулей сервера в журнале приложений Windows. Описания кодов возможных ошибок сервера в журнале приложений Windows приведены в разделе "Просмотр сообщений сервера".

Далее приведены некоторые возможные проблемы, их причины и решения.

Проблема: Офицер безопасности не может взять схему безопасности на редактирование

Причина: Команды, предназначенные для редактирования схемы безопасности, неактивны.

Решение: Редактировать можно только последнюю версию схемы безопасности. Сведения о том, какая схема загружена в Консоль управления, отображаются на панели статуса (при работе с последней версией схемы безопасности на панели статуса отображается номер версии и режим, в котором находится схема безопасности). Чтобы выйти из режима просмотра старой схемы безопасности, в главном меню выберите команду **Действие > Смотреть последнюю схему безопасности** или воспользуйтесь клавишей **F9**.

Проблема: Контролируемая рабочая станция была удалена из схемы безопасности, но сведения о ней выводятся в разделе **Рабочие станции**

Описание: Запись о контролируемой рабочей станции, удаленной из схемы безопасности, сохраняется в схеме безопасности и имеет статус **Агент выключен**.

Решение: Удаление записей о контролируемых рабочих станциях выполняется вручную по мере необходимости. Процедура удаления рабочей станции из схемы безопасности описывается в разделе "Удаление рабочей станции из схемы безопасности".

4.1 Просмотр сообщений сервера

В случае возникновения проблем в работе сервера, вы можете просмотреть ошибки и информационные сообщения от всех модулей сервера в журнале приложений Windows. В следующей таблице приведены описания кодов возможных ошибок сервера в журнале приложений Windows.

Внимание!

Если проблему не удалось решить стандартными средствами, обратитесь в службу поддержки InfoWatch, указав следующую информацию:

- описание проблемы,
- код ошибки,
- текст сообщения об ошибке,
- описание действий, предпринятых для решения проблемы.

Код ошибки	Критичность	Описание
Модуль `InfoWatch.DeviceMonitor.Server.Client` (клиентский фасад сервера) Источник события в журнале Windows: `InfoWatch.DeviceMonitor.Server.Client` Базовый номер ошибок модуля: 1000		
1000	Критическая ошибка	Ошибка формирования пакета для отправки клиенту. Обратитесь в службу поддержки InfoWatch.
1001	Ошибка	Невозможно записать событие об отключении/подключении клиента в базу данных. Как правило, проблема вызвана потерей соединения с базой данных. Очень редко может быть вызвана ошибками в коде сервера. Более подробную диагностику следует вести по тексту сообщения об ошибке
1002	Ошибка	Невозможно зарегистрировать новую рабочую станцию в базе данных. Как правило, проблема вызвана потерей соединения с базой данных. Очень редко может быть вызвана ошибками в коде сервера. Более подробную диагностику

Код ошибки	Критичность	Описание
		следует вести по тексту сообщения об ошибке
1003	Ошибка	Потеря соединения с клиентом. Может быть вызвана чем угодно, начиная от сетевых проблем, заканчивая ошибками в коде. Более подробную диагностику следует вести по тексту сообщения об ошибке
1004	Предупреждение	Превышено предельное время бездействия соединения с клиентом. Как правило, вызвано сетевыми проблемами или проблемами на стороне клиента (неожиданное завершение приложения и пр.)
1005	Предупреждение	Ошибка закрытия соединения с клиентом (сокета). Как правило, вызвана сетевыми проблемами.
1006	Ошибка	Необработанная ошибка сервера. Возникает при проблемах с установлением соединений с клиентами, а также при необработанных ошибках в момент остановки службы сервера.
1007	Ошибка	Возникает при ошибках обновления данных о рабочей станции, хранящихся в БД. Как правило, проблема вызвана потерей соединения с базой данных. Очень редко может быть вызвана ошибками в коде сервера. Более подробную диагностику следует вести по тексту сообщения об ошибке
1008	Ошибка	Возникает при ошибках (исключениях) мониторинга неактивных рабочих станций. Вызвана сетевыми проблемами либо ошибками в коде сервера. Более подробную диагностику следует вести по тексту сообщения об ошибке.
1009	Предупреждение	Компьютер с именем, указанным в тексте сообщения об ошибке, не найден в сети. Ошибка возникает при мониторинге неактивных рабочих станций. Вызвана либо сетевыми проблемами, либо неработоспособностью распознавания имен в сети, либо отсутствием такого хоста (в случае его удаления). Рекомендуется удалить эту рабочую станцию из схемы безопасности (см. "Удаление рабочей станции из схемы безопасности").
1010	Ошибка	Невозможно установить соединение с клиентом. Ошибка вызвана сетевыми проблемами либо ошибками в коде сервера. Более подробную диагностику следует вести по тексту сообщения об ошибке
1011	Ошибка	Ошибка подготовки данных для отправки клиенту. Практически всегда вызывается ошибками в коде клиентского фасада сервера. Обратитесь в службу поддержки InfoWatch.
1012	Ошибка	Ошибка разбора данных, полученных с клиента. Может быть вызвана ошибками в коде клиентского фасада сервера, порчей сетевых пакетов, ошибками при формировании пакетов на стороне клиентской части. Более подробную диагностику следует вести по тексту сообщения об ошибке
1013	Критическая ошибка	Неверная сигнатура пакета. Не соблюден протокол. Может быть вызвана ошибками в коде клиентского фасада сервера, порчей сетевых пакетов, ошибками при формировании пакетов на стороне клиентской части. Более подробную диагностику следует вести по тексту сообщения об ошибке
1014	Ошибка	Длина пакета (исключая пакет с пользователями) превышает максимально допустимую длину. Может быть вызвана порчей сетевых пакетов, ошибками при формировании пакетов на стороне клиентской части. Более подробную диагностику следует вести по тексту сообщения об ошибке
1015	Ошибка	Длина пакета с пользователями превышает максимально допустимую длину. Может быть вызвана порчей сетевых пакетов, ошибками при формировании пакетов на стороне клиентской части. Более подробную диагностику следует вести по тексту сообщения об ошибке.
1016	Ошибка	Неподдерживаемый тип пакета. Может быть вызвана порчей сетевых пакетов,

Код ошибки	Критичность	Описание
		ошибками при формировании пакетов на стороне клиентской части. Более подробную диагностику следует вести по тексту сообщения об ошибке
1017	Ошибка	Ошибка разбора пакета с событиями. Может быть вызвана ошибками в коде клиентского фасада сервера, порчей сетевых пакетов, ошибками при формировании пакетов на стороне клиентской части. Более подробную диагностику следует вести по тексту сообщения об ошибке.
1018	Предупреждение	Получен пустой пакет с событиями. Также возможно, что в пакете были «плохие события», из-за которых разбор пакета был неудачен. Может быть вызвана ошибками в коде клиентского фасада сервера, порчей сетевых пакетов, ошибками при формировании пакетов на стороне клиентской части. Более подробную диагностику следует вести по тексту сообщения об ошибке
1019	Ошибка	Ошибка сохранения событий в базу данных. Может быть вызвана нарушением ограничений целостности: например, событие содержит неизвестный серверу идентификатор правила. Также эта ошибка может возникнуть при попытке сохранения событий-дубликатов.
1020	Информация	Запущен клиентский фасад сервера.
1021	Информация	Остановлен клиентский фасад сервера.
1022	Предупреждение	Сервер получил неверную контрольную сумму (хэш) схемы безопасности от клиента. Возможно, схема безопасности на клиенте повреждена или намеренно изменена.
1023	Предупреждение	Превышение максимально допустимого количества клиентских соединений в демо-версии.
Модуль `InfoWatch.DeviceMonitor.TrafficMonitor.Connector` (Traffic Monitor коннектор) Источник (source) события в журнале Windows: `InfoWatch.DeviceMonitor.TrafficMonitor.Connector` Базовый номер ошибок модуля: 2000		
2000	Ошибка	Отрицательное значение количества соединений с TM в конфигурационном файле сервера. Внесите изменения в конфигурационный файл (см. "Раздел <applicationSettings>", параметр `NumberOfConnections`).
2001	Предупреждение	Слишком большое значение (>32) количества соединений с TM в конфигурационном файле сервера. Количество соединений устанавливается в 32. Внесите изменения в конфигурационный файл (см. "Раздел <applicationSettings>", параметр `NumberOfConnections`).
2002	Ошибка	Ошибка соединения с БД при выполнении запросов к БД во время отправки событий в TM. Проверьте работоспособность и доступность БД.
2003	Ошибка	Ошибка при выполнении запросов к БД во время отправки событий в TM. Может быть вызвана блокировками, гораздо реже – ошибками в коде сервера. Более подробную диагностику следует вести по тексту сообщения об ошибке.
2004	Ошибка	Неизвестная ошибка при отправке сообщений в TM. Более подробную диагностику следует вести по тексту сообщения об ошибке.
2005	Ошибка	Ошибка чтения длины очереди из БД. Проверьте работоспособность и доступность БД.
2006	Информация	Изменились настройки соединения с TM.
2007	Ошибка	Не удалось удалить теневую копию. Файл теневой копии может быть открыт другим приложением или отсутствовать. Также может быть ошибка в коде сервера. Более подробную диагностику следует вести по тексту сообщения об ошибке.

Код ошибки	Критичность	Описание
2008	Ошибка	Ошибка чтения ответа от ТМ. Может быть вызвана неверным форматом сообщения, проблемами в сети, и пр. Более подробную диагностику следует вести по тексту сообщения об ошибке.
2009	Ошибка	Во время сетевого обмена произошел сбой. Проверьте работоспособность сети.
2010	Ошибка	Потеряно соединение с ТМ. Может быть вызвано проблемами в сети или остановкой ТМ. Более подробную диагностику следует вести по тексту сообщения об ошибке.
2011	Ошибка	Неизвестная ошибка передачи сообщений в ТМ. Более подробную диагностику следует вести по тексту сообщения об ошибке.
2012	Ошибка	Попытка добавить отработавшее соединение в пул, который уже полностью заполнен. Обратитесь в службу поддержки InfoWatch.
2013	Предупреждение	Событие должно иметь теневую копию, но её нет на DM сервере. Она могла быть не передана с клиента, потеряна при передаче.
2014	Критическая ошибка	ТМ коннектор неправильно настроен. Есть ошибки в конфигурационном файле сервера. Проверьте конфигурационный файл сервера. Более подробную диагностику следует вести по тексту сообщения об ошибке
2015	Информация	Отправка сообщения в ТМ была отменена.
2016	Предупреждение	Почтовое сообщение, с помощью которого передаётся событие, превышает предельно допустимый размер. Актуально для ТМ 2.5
2017	Предупреждение	Неверный формат логина для передачи в ТМ 2.5. Ожидается DOMAIN\LOGIN. Проблема может быть вызвана клиентом, приславшим неверный логин. Также неверный логин мог быть добавлен вручную из консоли управления.
2018	Информация	Соединение с ТМ установлено успешно.
2019	Предупреждение	От ТМ пришел пустой ответ. Проблема на стороне ТМ.
2020	Предупреждение	Из ответа ТМ 3.x не был считан атрибут определяющий тип сообщений. Проблема вызвана ошибками в формировании ответов ТМ.
2021	Предупреждение	Неверный тип сообщения ТМ 3.x. Проблема вызвана ошибками в формировании ответов ТМ.
Модуль `InfoWatch.DeviceMonitor.Server.Core` (код запуска сервера) Источник события в журнале Windows: `InfoWatch.DeviceMonitor.Server.Core` Базовый номер ошибок модуля: 3000		
3000	Критическая ошибка	TCP порт GUI фасада (по умолчанию – 15003) уже используется. Проверить работающие приложения в системе на предмет использования этого порта и изменить либо их настройки, либо настройки сервера, назначив ему другой порт GUI фасада через конфигурационный файл сервера.
3001	Критическая ошибка	Невозможно соединиться с базой данных. Сервер стартует и будет пытаться установить соединение с БД. Проверьте работоспособность и доступность БД.
3002	Критическая ошибка	Коннектор ТМ не может быть запущен. Более подробную диагностику следует вести по тексту сообщения об ошибке.
3003	Ошибка	При удалении регистрации канала GUI фасада возникла ошибка. Обратитесь в службу поддержки InfoWatch.
Модуль `InfoWatch.DeviceMonitor.Server.Database` (модуль взаимодействия с БД)		

Код ошибки	Критичность	Описание
Источник (source) события в журнале Windows: `InfoWatch.DeviceMonitor.Server.Database` Базовый номер ошибок модуля: 4000		
4000	Критическая ошибка	Неподдерживаемая СУБД. Ошибка в конфигурационном файле сервера. Проверить конфигурационный файл сервера.
4001	Ошибка	Ошибка чтения настройки сервера из БД. Более подробную диагностику следует вести по тексту сообщения об ошибке
4002	Ошибка	Ошибка вставки новой настройки сервера в БД. Более подробную диагностику следует вести по тексту сообщения об ошибке
4003	Ошибка	Ошибка обновления настройки сервера в БД. Более подробную диагностику следует вести по тексту сообщения об ошибке
4004	Предупреждение	Ошибка чтения версии схемы безопасности из БД. Проблема вызвана отсутствием какой-либо схемы безопасности. Создайте новую схему безопасности.
4005	Предупреждение	Произошла конвертация правила запрета на чтение в правило нет доступа
4006	Предупреждение	Произошла конвертация правила запрета записи в правило разрешения только чтения.
4007	Предупреждение	Произошла конвертация правила разрешения записи в правило полного доступа.
4008	Информация	Рабочая станция, указанная в тексте сообщения, отсутствует в схеме безопасности.
4009	Информация	Не удалось считать версию последнего номера события из журнала аудита.
4010	Критическая ошибка	Неподдерживаемый тип базы данных. Обратитесь в службу поддержки InfoWatch.
4011	Ошибка	С клиента пришел пустой список пользователей. Следует искать проблему на стороне клиента или в разборе пакетов.
4012	Предупреждение	Произошло обновление БД с версии 3.1 до версии 3.2
4013	Предупреждение	Произошло обновление БД с версии 3.2 до версии 3.3
4014	Предупреждение	Правило на жесткий диск удалено из схемы безопасности как неподдерживаемое.

5 Лицензионная информация

Пользовательское лицензионное соглашение InfoWatch Device Monitor

При создании Системы также были использованы разработки третьих сторон:

- **WiX toolset** – WiX Common Public License

5.1 WiX Common Public License

WiX Common Public License

Top Previous Next

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors,

compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

5.2 Пользовательское лицензионное соглашение InfoWatch Device Monitor

ЗАО «ИнфоВотч»

Тел./факс:+7(495)229-00-22

Департамент продаж: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru

Настоящее Пользовательское лицензионное соглашение (далее - Соглашение) является Договором между Пользователем, физическим или юридическим лицом (далее - Пользователь), правомерно владеющим экземпляром программного обеспечения InfoWatch Device Monitor (далее – ПО), и ЗАО «ИнфоВотч» (далее – Правообладатель).

Правообладатель гарантирует наличие у него соответствующих прав (исключительных и неисключительных) на все в совокупности и каждый в отдельности из перечисленных элементов ПО (исходный текст, объектный код, все иные элементы) и сопроводительную документацию (Руководство пользователя, Руководство по установке и конфигурированию, Release Notes и т. д., далее - Документация) в печатном или электронном виде.

В случае, если Пользователь приобрел ПО через Интернет, выбор Вами пункта «Я принимаю условия Пользовательского лицензионного соглашения» при установке ПО и нажатии на кнопку «Далее» означает безоговорочное согласие с условиями настоящего Соглашения.

Если Пользователь не согласен с условиями данного Соглашения, то он должен прекратить установку ПО.

В случае, если Пользователь приобрел ПО на материальном носителе, то вскрытие упаковочного конверта с компакт-диском (нарушение целостности наклейки) означает его безоговорочное согласие с условиями настоящего Соглашения. Если Пользователь не согласен с условиями данного Соглашения, то он имеет право вернуть ПО продавшей его организации и получить обратно его полную стоимость.

После вскрытия упаковочного конверта или повреждения наклейки (в случае приобретения ПО на материальном носителе), либо после выбора Пользователем пункта «Я принимаю условия Пользовательского лицензионного соглашения» (при приобретении ПО через Интернет), он получает простую (неисключительную) лицензию на воспроизведение ПО, ограниченное правом установки (инсталляции), копирования и запуска ПО в соответствии с условиями настоящего Соглашения.

Пользователь имеет право использовать ПО в соответствии с условиями настоящего лицензионного соглашения:

1. ПО предназначено для мониторинга, фильтрации и предотвращения утечки данных, передаваемых за пределы сети компании при копировании на сменные носители, выводе на печать, передаче по беспроводным каналам связи, а также контроля доступа к портам компьютера.
2. ПО обеспечивает следующие возможности:
   - контроль операций пользователя:
     - доступ к портам – USB, LPT, COM и т. п.
     - копирование конфиденциальных документов или их частей на сменные носители (floppy, CD/DVD, внешние USB носители или внешние носители)
     - использование беспроводных протоколов, таких как IRDA и Bluetooth
     - вывод данных на печать;
   - снятие теневых копий с передаваемых или копируемых данных;
   - передача теневых копий на центральный сервер анализа и обработки данных;
   - протоколирование всех действий пользователя.
3. Срок использования ПО и количество защищаемых объектов указаны в Лицензионном договоре.
4. В случае использования ознакомительных версий продукта Пользователь имеет право в течение срока, указанного в файле лицензионного ключа, с момента получения ПО, получать от Правообладателя техническую поддержку (через веб-сайты Правообладателя).

   По окончании срока, указанного в Лицензионном договоре, доступный Пользователю функционал автоматически ограничивается. По окончании срока использования ПО Пользователю становятся недоступны следующие функции:
   - снятие теневых копий.
5. Право на получение технической поддержки использования ПО приобретается отдельно, срок ограничивается условиями договора на оказание технической поддержки. В течение срока, указанного в договоре на оказание технической поддержки, Пользователь имеет право получать от

Правообладателя или его Партнеров:

- новые версии ПО, включая обновления;
- техническую поддержку через веб-сайт компании, а также по электронной почте в рабочие часы.

6. Сервисы, описанные в п.5 настоящего Соглашения, предоставляются при условии установки Пользователем последнего обновления последней версии ПО.
7. Правообладатель не гарантирует Пользователю функциональность ПО в случае, если Пользователь не осуществляет обновления ПО, указанного в п.6.
8. Пользователь имеет право изготовить единственную копию ПО при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра ПО в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Указанная в настоящем пункте копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.
9. При использовании ПО, предназначенного для ознакомительных целей, Пользователь не имеет права продавать (передавать на иных условиях) имеющийся у него экземпляр ПО другим лицам.
10. Запрещается производить декомпиляцию, дизассемблирование и/или модификацию ПО.
11. Запрещается сдавать ПО в аренду, прокат или во временное пользование, в том числе создавать условия для использования ПО и его элементов лицами, не имеющими прав на использование ПО, предоставлять подписку на ПО, предоставлять услуги аутсорсинга с использованием ПО.
12. Запрещается разделять ПО на составляющие части для использования их на разных компьютерах.
13. Запрещается использовать ПО с целью создания данных или кода, предназначенных для использования другими программными продуктами.
14. Запрещается публиковать результаты стендовых испытаний ПО.
15. Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Руководстве Пользователя, а также в случае нарушения Пользователем условий настоящего Соглашения.
16. Правообладатель и/или его Партнеры не несут ответственности за какой-либо ущерб, связанный с использованием или невозможностью использования ПО.
17. За нарушение исключительных прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.
18. Использование стороннего программного обеспечения:

    ПО может включать компоненты (программные средства, информационные носители и т.д.) сторонних производителей. Пользователь получает права на использование этих компонент на основе Лицензий и Лицензионных Соглашений этих производителей, которые являются в совокупности неотъемлемой частью настоящего Соглашения.

    ПО и его компоненты являются интеллектуальной собственностью Правообладателя и, при наличии компонент сторонних производителей, интеллектуальной собственностью сторонних производителей и защищаются законодательством Российской Федерации, Международным законодательством об авторском и имущественном праве на объекты интеллектуальной собственности.

    В случае наличия компонент сторонних производителей, Правообладатель является законным и полномочным представителем сторонних производителей, если обратное не оговорено в Лицензиях и Лицензионных Соглашениях сторонних производителей или в других документах, регламентирующих отношения между Пользователем и сторонними производителями.