INFOWATCH

InfoWatch Traffic Monitor 4.1

Руководство пользователя

INFOWATCH TRAFFIC MONITOR 4.1

Руководство пользователя

© ЗАО “ИнфоВотч”
Тел. +7 (495) 229-00-22 • Факс +7 (495) 229-00-22
http://www.infowatch.ru
Дата редакции: Апрель 2015 года

Содержание

Часть I Введение 11

1.1 Глоссарий 12

1.2 Дополнительная документация 17

Часть II Обзор InfoWatch Traffic Monitor 17

2.1 InfoWatch Traffic Monitor Standard и InfoWatch Traffic Monitor Enterprise 19

2.2 Перехват и анализ объектов 19

2.2.1 Перехват объектов 19

2.2.2 Транспортные режимы InfoWatch Traffic Monitor 20

2.2.3 Анализ объекта и вынесение вердикта 22

2.2.4 Загрузка объекта в базу данных 23

2.2.5 Ретроспективный анализ данных, решение пользователя по объекту 24

2.2.6 Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов 24

2.2.7 Работа системы без сценария анализа объектов 25

Часть III Общие принципы работы с Консолью управления 26

3.1 Запуск Консоли управления и подключение к серверу базы данных 26

3.1.1 Настройка списка подлючений к базе данных 28

3.2 Интерфейс Консоли управления 30

3.2.1 Главное окно Консоли управления 30

3.2.2 Разделы Консоли управления 32

3.2.3 Клавиши быстрого доступа 33

3.3 Обновление данных в Консоли управления 38

3.4 Изменение пользователем собственного пароля 38

Часть IV Администрирование Консоли управления 39

4.1 Управление доступом к Консоли управления 39

4.1.1 Роли пользователей консоли управления 40

4.1.1.1 Список привилегий 41

4.1.1.2 Создание и редактирование роли 45

4.1.1.3 Удаление роли 48

4.1.2 Управление доступом к содержимому объектов 48
4.1.3 Учетные записи Консоли управления 49
4.1.3.1 Рекомендации по составлению имен и паролей пользователей 50
4.1.3.2 Создание и редактирование учетной записи пользователя 51
4.1.3.3 Блокирование/разблокирование учетной записи пользователя 54
4.1.3.4 Удаление учетной записи пользователя 55
4.2 Настройка параметров отправки/получения рапортов по объектам 56
4.2.1 Настройка почтового сервера для отправки рапортов 56
4.3 Настройка уведомлений о нарушениях 57
4.4 Настройка запроса о выходе из Консоли управления 59
4.5 Работа с хостами 59
4.5.1 Добавление описания хоста 62
4.5.2 Удаление хоста 62
4.6 Просмотр статистики использования базы данных 63
Часть V Справочник сотрудников и рабочих станций 64
5.1 Настройка подключения и синхронизации с Active Directory 65
5.2 Справочник сотрудников 67
5.2.1 Создание и редактирование записи о сотруднике 68
5.2.2 Удаление и восстановление записи о сотруднике 71
5.2.3 Просмотр и фильтрация записей о сотруднике 72
5.3 Справочник рабочих станций 73
5.3.1 Редактирование записи о рабочей станции 73
5.3.2 Просмотр и фильтрация записей о рабочей станции 75
5.4 Справочник групп 76
5.4.1 Создание, просмотр и редактирование группы 77
5.4.2 Добавление члена группы TM 79
5.4.3 Удаление члена группы TM 80
5.4.4 Удаление и восстановление группы TM 80
5.5 Загрузка справочников на хост 81
Часть VI Краулер 81
6.1 Схема работы Crawler 83

6.2 Настройка соединения Консоли управления с сервером Crawler 85
6.3 Настройка параметров работы сканера Crawler 86
6.4 Создание и редактирование задания на сканирование 89
6.4.1 Сканирование разделяемых сетевых ресурсов 90
6.4.2 Сканирование локальных дисков рабочих станций 95
6.4.3 Сканирование файлового хранилища SharePoint 100
6.5 Удаление задания на сканирование 104
6.6 Выполнение и остановка задания 104
6.7 Очистка базы хешей 106
Часть VII Настройка параметров анализа объектов 106
7.1 Управление конфигурацией 107
7.1.1 Версии конфигурации 108
7.1.1.1 Просмотр информации по конфигурации 109
7.1.1.2 Добавление описания к версии конфигурации 110
7.1.1.3 Сравнение двух версий конфигурации 110
7.1.1.4 Загрузка конфигурации на хосты 112
7.1.1.5 Возврат к старой версии конфигурации 112
7.1.1.6 Удаление версии конфигурации 113
7.1.2 Классификатор 113
7.1.2.1 Принципы составления классификатора 115
7.1.2.2 Создание категории 116
7.1.2.3 Добавление термина в категорию 117
7.1.2.3.1Создание термина 117
7.1.2.3.2Импорт терминов из файла 118
7.1.2.3.3Перемещение термина из другой категории 119
7.1.2.4 Редактирование категории 120
7.1.2.5 Смена уровня вложенности категории 121
7.1.2.6 Настройка параметров термина 121
7.1.2.7 Поиск термина 123
7.1.2.8 Удаление категории 124
7.1.2.9 Экспорт/импорт классификатора 125
7.1.3 Списки 126

7.1.3.1 Создание группы списков 127
7.1.3.2 Создание списка 128
7.1.3.3 Создание элемента списка 129
7.1.3.4 Редактирование списка или группы списков 129
7.1.3.5 Просмотр и фильтрация элементов списка 131
7.1.3.6 Удаление списка или группы списков 131
7.1.4 Сценарий анализа объектов 132
7.1.4.1 Создание сценария 132
7.1.4.2 Загрузка сценария из файла 133
7.1.4.3 Редактирование сценария 134
7.1.4.4 Активирование сценария 134
7.1.4.5 Сохранение сценария в файл 135
7.1.4.6 Удаление сценария 135
7.1.5 Текстовые объекты 135
7.1.5.1 Загрузка типовых текстовых объектов из XML-файлов 137
7.1.5.2 Создание и редактирование пользовательского текстового объекта 138
7.1.5.3 Добавление значения пользовательского объекта 140
7.1.5.4 Включение и выключение текстового объекта и его значений 141
7.1.5.5 Удаление пользовательского текстового объекта или его значения 143
7.1.5.6 Группировка и фильтрация записей 144
7.1.6 База эталонных документов 145
7.1.6.1 Составление базы эталонных документов 145
7.1.6.2 Редактирование информации об эталонном документе 146
7.1.6.3 Удаление эталонного документа 147
7.1.6.4 Группировка записей 148
7.1.7 Зоны ответственности: разграничение доступа к объектам 149
7.1.7.1 Создание и редактирование зоны ответственности 149
7.1.7.2 Изменение приоритетов для зон ответственности 152
7.1.7.3 Удаление зоны ответственности 152
7.2 Справочники 153
7.2.1 Теги 153
7.2.1.1 Создание группы тегов 154

7.2.1.2 Создание тега 155
7.2.1.3 Редактирование тегов и групп тегов 156
7.2.1.4 Удаление группы тегов 157
7.2.2 Цвета 157
7.2.2.1 Создание и редактирование цвета 157
7.2.2.2 Удаление цвета 158
7.3 Настройка сценария анализа объектов (LUA) 159
7.3.1 Особенности составления сценария на языке LUA 160
7.3.2 Модель данных InfoWatch Traffic Monitor 161
7.3.3 Типы данных 162
7.3.3.1 Корневой элемент root 162
7.3.3.2 Конверт объекта (Envelope) 163
7.3.3.3 Содержимое объекта и результаты контентного анализа (Object) 166
7.3.3.4 Заголовки объекта (ObjectHeaders) 167
7.3.3.5 Имена заголовков объекта (ObjectHeader) 167
7.3.3.6 Результаты контентного анализа (ObjectProcessing) 167
7.3.3.7 Список вложений (Objects) 168
7.3.3.8 Результаты обработки объекта (Processing) 168
7.3.4 Операторы 170
7.3.4.1 Оператор присваивания 170
7.3.4.2 Оператор сравнения 171
7.3.4.3 Оператор условия 171
7.3.4.4 Оператор цикла 172
7.3.5 Методы 172
7.3.5.1 Добавление сообщения 173
7.3.5.2 Добавление тега 173
7.3.5.3 Проверка вхождения строки в список 174
7.3.5.4 Поиск строки в группе списков 175
7.3.5.5 Поиск по элементам XML-контекста 175
7.3.5.6 Проверка вхождения отправителя в группу 176
7.3.5.7 Проверка вхождения получателя в группу 176
7.3.5.8 Проверка вхождения рабочей станции в группу 176

7.3.5.9 Проверка вхождения элементов списка в текст 177
7.3.6 Библиотека вспомогательных функций 177
7.3.6.1 Проверка присутствия категорий 178
7.3.6.2 Проверка наличия категории из списка 179
7.3.6.3 Проверка присутствия цитат из эталонных документов 179
7.3.6.4 Проверка присутствия текстовых объектов 179
7.3.6.5 Проверка присутствия текстового объекта из отрасли 179
7.3.6.6 Проверка присутствия вложений неопределенного типа 180
7.3.6.7 Проверка присутствия зашифрованных вложений 180
7.3.6.8 Проверка наличия любых ошибок обработки объекта 180
7.3.6.9 Проверка наличия ошибок обработки вложений 180
7.3.6.10 Проверка наличия ошибок контентного анализа 181
7.3.6.11 Проверка мусорного трафика 181
7.3.6.12 Поиск первого элемента из списка нод 181
7.3.6.13 Проверка наличия конфликта идентификации 182
7.3.6.14 Отправка уведомления для офицера безопасности 182
7.3.6.15 Отправка уведомления для нарушителя 182
7.3.6.16 Проверка присутствия текстового объекта из указанной отрасли 182
7.3.7 Пример сценария 183

Часть VIII Анализ объектов 190

8.1 Составление запросов по объектам 190
8.1.1 Правила оптимизации запросов 191
8.1.1.1 Общие атрибуты объекта 191
8.1.1.2 Заголовки конвертов и заголовки объектов 194
8.1.2 Реализация поиска по тексту, извлеченному из перехваченных объектов 198
8.1.2.1 Построение текстового индекса 198
8.1.2.2 Синтаксис при построении условий в запросах на поиск по тексту перехваченных объектов
8.1.2.3 Примеры обработки поисковых запросов 200
8.1.3 Создание и редактирование запроса 204
8.1.3.1 Общие параметры запроса (вкладка Общее) 206
8.1.3.2 Выбор полей просмотра (вкладка Поля просмотра) 207
8.1.3.3 Настройка условий запроса (вкладка Условия) 208

8.1.3.3.1Создание условия запроса 209
8.1.3.3.2Параметры условия 211
8.1.3.3.3Редактирование условий запроса 214
8.1.3.4 Настройка условий сортировки (вкладка Сортировка) 216
8.1.3.5 Настройка порядка группирования (вкладка Группировка) 217
8.1.3.6 Распределение прав на работу с запросом (вкладка Разрешенные пользователи) 218
8.1.4 Копирование запроса 218
8.1.5 Удаление запроса 219
8.2 Работа пользователя с объектами 219
8.2.1 Пользовательский анализ объектов 219
8.2.1.1 Настройка режима просмотра содержимого объекта 221
8.2.1.2 Настройка размера загружаемых SMTP-писем и заданий на печать 222
8.2.1.3 Настройка панели информации об объекте 222
8.2.1.4 Выполнение запроса по объектам 223
8.2.1.5 Автоматическое обновление 224
8.2.1.6 Работа с Менеджером запросов 225
8.2.1.7 Просмотр информации по объектам 226
8.2.1.7.1Просмотр общей информации по объекту 227
8.2.1.7.2Детальная форма просмотра объекта 230
8.2.1.7.3Настройка поиска по заголовкам объектов 234
8.2.1.7.4Просмотр журнала объекта 234
8.2.1.8 Обработка данных отправителя, получателя и рабочей станции 235
8.2.1.9 Вынесение решения по объекту 237
8.2.1.10 Постановка на контроль 239
8.2.2 Перемещение объекта в другую зону ответственности 242
8.2.3 Отправка рапорта по объекту 242
8.2.4 Назначение тегов объекту 244
8.2.5 Выделение объектов цветом 245
8.2.6 Добавление примечания к объекту 245
8.2.7 Выгрузка вложений, писем и xml-контекста 246
8.2.7.1 Выгрузка вложений объекта 246
8.2.7.2 Выгрузка SMTP-писем 247

8.2.7.3 Выгрузка контекста 247
8.3 Составление отчетов по объектам 248
8.3.1 Типы отчетов 249
8.3.2 Создание и редактирование отчета 254
8.3.3 Просмотр результатов отчета 256
8.3.4 Перестроение отчета 256
8.3.5 Печать отчета 257
8.3.6 Копирование отчета 257
8.3.7 Экспорт отчета 257
8.3.8 Удаление отчета 258
8.4 Управление папками запросов и отчетов 258
8.4.1 Создание и редактирование папки 258
8.4.2 Перемещение запросов и отчетов между папками 260
8.4.3 Копирование папки 260
8.4.4 Удаление папки 261
Часть IX Лицензионная информация 261
9.1 Пользовательское лицензионное соглашение 262
9.2 Лицензии третьих сторон 265

1 Введение

InfoWatch Traffic Monitor (далее InfoWatch Traffic Monitor или Система) – это распределенная многокомпонентная система, предназначенная для контроля над различными видами трафика (SMTP, HTTP, ICQ). Кроме того, Система выполняет анализ данных, полученных от системы InfoWatch Device Monitor.

Приложение Management Console (далее: Management Console, Консоль управления) является частью системы InfoWatch Traffic Monitor, позволяет управлять настройками Системы и осуществлять мониторинг работы Системы.

В настоящем руководстве вы можете найти сведения по работе с консолью управления.
Информация, содержащаяся в руководстве, предназначена для пользователей, работающих с Системой (выполняющих настройку конфигурации, анализ информационных объектов и т. п.).
Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Microsoft Windows. Выполнение задач по составлению сценария анализа объектов требует знания языка программирования Lua.

Для настройки условий поиска по контексту с использованием Oracle Text необходимы навыки работы с функцией Oracle Text (см. Oracle Text Reference, версия 11g).

Основные разделы руководства:

- Обзор InfoWatch Traffic Monitor – Содержит общие сведения о Системе, принципах проверки данных. Описывает запуск Консоли управления (Management Console), принципы авторизации. Содержит вводную информацию по работе с консолью управления (описание интерфейса, настройка интерфейса, порядок обновления данных).
- Администрирование консоли управления – В разделе рассматривается выполнение операций, связанных с администрированием Системы (управление учетными записями пользователей, распределение ролей и т. д.), порядок настройки параметров отправки рапортов по объектам, описывается работа с хостами, и приводится информация о получении статистики по использованию базы данных, а также принципы управления данными сотрудников и рабочих станций, полученными из Active Directory и созданными средствами Системы.
- Справочник сотрудников и рабочих станций – Содержит описание управления информацией об отправителях и получателях (сотрудниках), а также рабочих станциях с помощью специальных справочников.
- Краулер – Описывает работу с перехватчиком, обеспечивающим проверку файлов, находящихся в корпоративной сети: сканирование сетевых папок, открытых для удалённого доступа по протоколу SMB; сканирование локальных дисков рабочих станций, работающих под управлением ОС Windows; сканирование файлового хранилища SharePoint.
- Настройка параметров анализа объектов – Описывает порядок настройки параметров и правил, используемых для проверки перехваченных данных, а также для мониторинга и анализа данных. Содержит описание дополнительных настроек, необходимых для анализа (тегов, зон ответственности и цветов), а также сведения о принципах составления сценария анализа объектов, поступающих в Систему (писем, запросов и т. д.).
- Анализ объектов – Описывает принципы создания и настройки запросов для выборки данных и отчетов для получения статистической информации по перехваченным данным. Содержит сведения о порядке анализа перехваченных Системой объектов.

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.

Перед обращением в службу технической поддержки мы рекомендуем вам посетить раздел *База знаний* на нашем сайте: http://cp.infowatch.com/kb. Возможно, там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

1.1 Глоссарий

Термин	Определение
Active Directory	LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT
Device Monitor	InfoWatch Device Monitor: программно-аппаратный комплекс, предназначенный для контроля доступа пользователей к периферийным устройствам и мониторинга операций (копирование данных на съемные носители и FTP, отправка данных на печать, использование мессенджеров).
DeviceLock Adapter	Перехватчик модуля Device Monitor, обеспечивающий интеграцию с системой DeviceLock (Смарт Лайн Инк.), выполняющей перехват теневых копий файлов, переносимых на съемные устройства. См. также: *Device Monitor*, *Теневая копия файла*
HTTP	HyperText Transfer Protocol - (протокол передачи гипертекста) - протокол прикладного уровня передачи данных в виде текстовых сообщений
HTTP-запрос	Запрос, удовлетворяющий требованиям протокола HTTP (POST-запрос, GET-запрос и т. д.). См. также: *HTTP*, *Объект*
ICAP	(Internet Content Adaptation Protocol) - протокол, позволяющий контролировать входящий/исходящий HTTP-трафик. Предоставляет возможность модификации содержимого HTTP-запросов (В рамках InfoWatch Traffic Monitor контролируется только исходящий трафик.)
ICQ	Служба мгновенного обмена сообщениями в сети Интернет, принадлежащая Digital Sky Technologies
ICQ - сообщение	Сообщение, передаваемое по протоколу ICQ-OSCAR. См. также: *Объект*
InfoWatch Traffic Monitor	Программный комплекс InfoWatch Traffic Monitor (IW TM). Предназначен для осуществления контроля различных видов трафика (SMTP, HTTP, ICQ) и теневых копий данных, копируемых на съемные носители и отправляемых на печать.
Management Console	См. *Консоль управления*
Oracle Text	Технология Oracle, используемая при выполнении поиска по тексту объекта. См. также: *Объект*
SMTP	Simple Mail Transfer Protocol - (простой протокол передачи почты) - сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
SMTP-письмо	Письмо, удовлетворяющее требованиям протокола SMTP. См. также: *SMTP*, *Объект*
SPAN	Switched Port Analyzer - технология зеркального копирования трафика с одного порта на другой
SPAN-копия	Разновидность транспортного режима Копия. Передача трафика в этом режиме осуществляется через коммутатор CISCO. Копия трафика передается для анализа на сервер Traffic Monitor. См. также: *SPAN*

Автолингвист	Программа InfoWatch Автолингвист, позволяющая на основе коллекции текстов автоматически создавать совокупность категорий и терминов, которую впоследствии можно использовать в классификаторе. См. также: *Лингвистический анализ*, *Классификатор*
Администратор	Предустановленная роль и учетная запись консоли управления, имеющая права на управление другими учетными записями и их правами.Также Администратор - пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. также: *Роль пользователя*, *Офицер безопасности*
Активный сценарий	Сценарий, действующий в конфигурации, загруженной на хост. См. также: *Сценарий*
Анализ объекта	Процедура обработки атрибутов, вложенных файлов и текста перехваченных объектов и назначении объекту дополнительных атрибутов. См. также: *Сценарий*, *Атрибуты объекта*
Атрибуты объекта	Структурированные данные, извлеченные из перехваченных объектов и назначенные по результатам их обработки. См. также: *Сценарий*, *Вердикт*, *Решение*, *Транспортный режим* , *Цвет*, *Тег*
База эталонных документов	Хранилище цифровых отпечатков, сделанных с эталонных документов. Предназначено для поиска цитат в анализируемых текстах. См. также: *Эталонный документ*, *Детектирование цифровых отпечатков*, *Цифровой отпечаток*, *Цитата*
Вердикт	Атрибут объекта, содержащий заключение о наличии или отсутствии нарушений в анализируемом объекте. В сочетании с атрибутом Транспортный режим определяет возможность дальнейшей транспортировки объекта (атрибут *Состояние доставки*). Обязательный атрибут объекта. См. также: *Транспортный режим*, *Состояние доставки*, *Атрибуты объекта*
Версия конфигурации	Фиксированное состояние конфигурации, используемое для контроля изменений в настройках параметров анализа объектов. Версия конфигурации фиксируется в момент её загрузки на хост, и может быть активной (используемой в настоящий момент), редактируемой (последняя версия с текущими изменениями) или архивной (одной из ранее использовавшихся). См. также: *Конфигурация*
Вес термина	Степень того, насколько данный термин характеризует категорию. Т.е. если термин имеет высокую значимость, то при его обнаружении в анализируемом тексте, существует большая вероятность того, что данный текст может быть отнесен к категории, содержащей данный термин. В консоли управления - целое число в диапазоне от 1 до 10. См. также: *Термин*
Вложение	Файл, приложенный к перехваченному объекту, любой степени вложенности. См. также: *Объект*
Группа	Группы пользователей и рабочих станций, хранящиеся в справочниках Системы. Делятся на группы AD (импортированные из Active Directory) и Группы TM (созданные средствами InfoWatch Traffic Monitor). См. также: *Справочники сотрудников, рабочих станций и групп*
Детектирование текстовых объектов	Технология поиска текстовых объектов (например, номеров кредитных карт) в тексте объектов. См. также: *Текстовый объект*, *Шаблон текстового объекта*
Детектирование цифровых отпечатков	Технология поиска цитат из эталонных документов в тексте объектов. См. также: *Эталонный документ*, *Цитата*
Заголовки конверта	Предопределенный набор заголовков для объекта любого типа. Формат заголовка конверта определяется в соответствии с контекстом. См. также: *Атрибуты объекта*
Заголовки объекта	Динамически пополняемый, произвольный набор заголовков. См. также: *Атрибуты объекта*
Зона ответственно	Способ разделения перехваченных объектов для ограничения доступа к ним пользователей консоли управления. Объекты, принадлежащие какой-либо зоне ответственности, будут

сти	видны только тем пользователям, которые входят в эту зону ответственности (при условии, что пользователь имеет привилегии на просмотр и/или работу с объектами). См. также: *Привилегия*
Канал перехвата данных	Среда перехвата данных, состоящая из технических средств перехвата данных, средств программного обеспечения и протоколов передачи данных. В системе поддерживаются следующие каналы перехвата данных: электронная почта (SMTP), веб (HTTP), сервисы мгновенных сообщений (ICQ и Skype), теневые копии файлов, события подключения/ отключения рабочих станций, задания на печать.
Капитализация	Параметр термина, определяющий, учитывается ли при поиске терминов тексте регистр символов (различия между строчными и прописными буквами) или нет. См. также: *Термин*
Категория	Элемент классификатора, соответствующий определённой предметной области (например, грифы секретности или термины проекта). Содержит либо перечень категорий (подкатегорий), либо перечень терминов, характерных для данной категории. См. также: *Термин*, *Классификатор*
Корпоративная политика безопасности	Принятая в компании совокупность технических, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, регламентирующих все вопросы обеспечения безопасности информации.
Классификатор	Набор данных, необходимых для проведения лингвистического анализа. Содержит перечень категорий, классифицирующих возможные нарушения политики безопасности. Наличие в тексте термина, принадлежащего к определенной категории, позволяет соотнести текст с этой категорией. См. также: *Категория*, *Термин*, *Лингвистический анализ*
Классификация	Отнесение анализируемого текста к той или иной категории классификатора. См. также: *Классификатор*, *Контекст объекта*
Консоль управления	Графический интерфейс пользователя. Предназначен для управления системой InfoWatch Traffic Monitor (администрирование Системы, настройка конфигурации, анализ объектов и т. п.).
Контекст объекта	Внутреннее представление перехваченного объекта в системе. XML данные (атрибуты, текст), извлеченные из объекта и его вложений. После обработки к контексту добавляются результаты анализа объекта и информация о решении по объекту. См. также: *Объект*
Конфигурация	Набор настроек, необходимых для проверки объектов, а также для мониторинга и анализа данных. См. также: *Классификатор*; *Сценарий*, *Списки*, *Текстовый объект*
Лингвистический анализ	Технология классификации текста объекта путем поиска соответствия этого текста каким-либо категориям. См. также: *Классификатор*, *Категория*
Монитор	См. *Перехватчик*
Морфология	Параметр термина: при использовании морфологии, поиск по тексту будет осуществляться с учетом всех форм этого термина. См. также: *Термин*
Нарушение	Значение атрибута «Решение», означающее, что зарегистрировано нарушение корпоративной политики безопасности. См. также: *Решение*, *Корпоративная политика безопасности*
Нормальный транспортный режим	Режим, в котором выполняется анализ и фильтрация проходящего трафика. В этом режиме возможна блокировка запрещенного Системой трафика. См. также: *Транспортный режим*
Объект	Объекты трафика (SMTP-письма, HTTP-запросы, ICQ-сообщения, Skype-сообщения), теневые копии файлов и задания на печать.
Запрос	Запрос к базе данных, создаваемый средствами консоли управления, для получения актуальных данных. См. также: *Консоль управления*

Основание вердикта	Атрибут объекта, описывающий причину, по которой объекту был присвоен вердикт. См. также: *Вердикт*
Отчет	Выборка, обеспечивающая наглядное отображение статистических данных о перехваченных объектах. См. также: *Консоль управления*
Офицер безопасности	Предустановленная роль и учетная запись консоли управления, имеющая все привилегии, кроме управления пользователями и ролями. См. также: *Роль пользователя*, *Администратор*
Ошибка идентификации	Конфликтная ситуация, когда одному значению атрибута Отправитель, Список получателей или Рабочая станция было найдено несколько соответствий в справочнике сотрудников и рабочих станций. См. также: *Справочники сотрудников, рабочих станций и групп*
Параметр хоста	Набор параметров, соответствующих кругу задач, которые выполняет данный хост. См. также: *Профиль хоста*
Перехват данных	Процесс получения, разбора, рубрикации и преобразования данных (или их копии) в контекст. Осуществляется перехват данных, передаваемых по протоколам SMTP, HTTP, ICQ/OSCAR, Skype, IXP, XMPP, MMP, FTP. См. также: *Перехватчик*, *Контекст объекта*
Перехватчик	Также: Sniffer, Сниффер, Анализатор сетевого трафика, Монитор. Компонент InfoWatch Traffic Monitor, получающий данные (SMTP, HTTP, ICQ трафик) от внешних клиентов, подготавливающий эти данные к дальнейшему анализу и передающий их на сервер Traffic Monitor.
Привилегия	Сущность, определяющая возможность пользователя выполнять какое-либо действие (набор действий) при работе с системой
Прозрачный транспортный режим	Режим, в котором трафик передается через Систему без фильтрации. Задачей Системы является только анализ перехваченного трафика. См. также: *Транспортный режим*
Профиль хоста	Набор параметров, соответствующих кругу задач, которые выполняет данный хост. См. также: *Параметр хоста*
Рапорт	E-mail- сообщение, отправляемое средствами консоли управления, для уведомления других пользователей консоли управления об особенностях одного или нескольких перехваченных объектов. Содержит номера выбранных объектов и сопроводительное сообщение
Режим копии	Один из транспортных режимов системы InfoWatch Traffic Monitor. В этом режиме реальный трафик не проходит через Систему. Анализу подвергается копия трафика. В данном режиме невозможна фильтрация трафика средствами Системы. См. также: *Транспортный режим*
Решение	Заключение пользователя о том, является ли перехваченный объект нарушением корпоративной политики безопасности. Может принимать значения «`Решение не принято`», «`Нарушение`» и «`Нет нарушений`». См. также: *Вердикт*, *Атрибуты объекта*
Роль пользователя	Совокупность привилегий, определяющих набор действий, которые пользователь может выполнять при работе с системой. См. также: *Администратор*, *Офицер безопасности*, *Консоль управления*, *Привилегия*
Сигнатура файла	Целочисленная константа, используемая для однозначной идентификации файлов определенного типа
Состояние доставки	Атрибут объекта, определяющий возможность доставки объекта получателям после анализа. Если доставка объекта была разрешена, то значение атрибута отражает состояние доставки (выполнена/не выполнена). См. также: *Атрибуты объекта*
Списки	Списки однотипных данных, создаваемые средствами консоли управления, для использования при составлении сценария анализа объектов. См. также: *Конфигурация*, *Сценарий*
Справочники сотрудников, рабочих	Данные о пользователях, рабочих станциях, а также группах пользователей и рабочих станций, импортированные из Active Directory, а также созданные средствами консоли управления. Используются для удобства работы с информацией о перехваченных объектах

станций и групп	
Сценарий	Совокупность правил, в соответствии с которыми проводится анализ и обработка объектов. Правило состоит из набора условий, по которым ведется проверка объекта, и действий, осуществляемых при выполнении или невыполнении заданных условий. См. также: *Активный сценарий*
Тег	Текстовая метка, дающая краткую характеристику перехваченному объекту. См. также: *Атрибуты объекта*
Текст объекта	Текстовая информация, извлечённая из тела объекта и его вложений. Не содержит элементов форматирования или разметки. Используется для решения задач анализа и поиска. См. также: *Объект*
Текстовый индекс	Список слов, сформированный Oracle Text из текста перехваченных объектов и их вложений, со ссылками на объекты, в которых встречаются данные слова. Используется в поиске по тексту объектов и вложений при выполнении запросов к базе данных. См. также: *Запрос*, *Oracle Text*
Текстовый объект	Данные из анализируемого текста, которые в результате проверки с помощью модуля детектирования текстовых объектов были признаны соответствующими шаблону. См. также: *Шаблон текстового объекта*, *Детектирование текстовых объектов*
Тело объекта	Объект без учёта вложений. См. также: *Объект*
Теневая копия файла	Копия файла, создаваемого на съемном устройстве. Создается только при успешном завершении операции сохранения файла на съемное устройство. Анализ теневых копий файлов выполняется в системе InfoWatch Traffic Monitor
Термин	Слово или словосочетание, нахождение которого в анализируемом тексте увеличивает степень соответствия этого текста той категории, к которой относится найденный термин. См. также: *Категория*
Транспортный режим	Атрибут объекта, определяющий степень контроля доставки объектов получателям. Назначается подсистемой анализа и принятия решений при анализе объекта. В сочетании с атрибутом "`Вердикт`" определяет возможность дальнейшей транспортировки объекта. См. также: *Вердикт*, *Режим копии*, *Нормальный транспортный режим*, *Прозрачный транспортный режим*, *Состояние доставки*, *Атрибуты объекта*
Характеристический термин	Параметр термина: если в тексте найден характеристический термин, относящийся к определенной категории, то текст автоматически считается соответствующим этой категории. См. также: *Термин*
Цвет	Атрибут объекта, присваиваемый ему в результате обработки в подсистеме принятия решений, либо назначенный этому объекту пользователем консоли управления. Определяет цвет, которым объект выделяется при отображении в консоли управления. См. также: *Атрибуты объекта*
Цитата	Отрывок документа из базы эталонных документов, найденный в тексте перехваченного объекта. См. также: *Эталонный документ*
Цитируемость	Показатель того, насколько полно эталонный документ присутствует в тексте анализируемого документа. См. также: *Эталонный документ*
Цифровой отпечаток	Способ хранения эталонного документа в базе данных в виде набора цитат. См. также: *Эталонный документ*, *Цитата*
Шаблон текстового объекта	Унифицированное описание всех возможных текстовых объектов с типичной структурой: номера паспортов, кредитных карт, телефонные номера, код медицинского диагноза и т.д. См. также: *Детектирование текстовых объектов*
Эталонный документ	Документ, цитаты из которого ищутся в анализируемом тексте. Эталонными документами могут быть образцы текстов приказов, финансовых отчетов, договоров и других конфиденциальных документов. Эталонные документы хранятся в системе в виде цифровых отпечатков, текст недоступен для просмотра ни пользователям, ни

	администраторам системы. См. также: *Детектирование текстовых объектов*, *Цифровой отпечаток*, *Цитата*

1.2 Дополнительная документация

Сведения по некоторым дополнительным вопросам вы можете найти в следующих документах:

- *«InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*
  В документе описывается установка и первоначальная настройка InfoWatch Traffic Monitor.
- *«InfoWatch Traffic Monitor. Руководство администратора»*
  Содержит информацию по администрированию базы данных (работа с табличными пространствами), администрированию серверной части системы InfoWatch Traffic Monitor.
- *«InfoWatch Device Monitor. Руководство пользователя»*
  Содержит описание принципов работы системы InfoWatch Device Monitor а также инструкции по установке, настройке и эксплуатации системы.
- *«InfoWatch DeviceLock Adapter. Руководство по установке и конфигурированию»*
  В документе описывается установка и первоначальная настройка InfoWatch DeviceLock Adapter.
- *«InfoWatch DeviceLock Adapter. Руководство администратора»*
  В документе приводятся сведения по настройке и мониторингу работы InfoWatch DeviceLock Adapter.
- *«InfoWatch Автолингвист. Руководство пользователя»*
  В документе приводятся сведения по работе с системой InfoWatch Автолингвист.

Перечисленные документы поставляются вместе с дистрибутивами соответствующих программных продуктов.

2 Обзор InfoWatch Traffic Monitor

InfoWatch Traffic Monitor позволяет контролировать информационные потоки в корпоративной среде для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.

Основные функции InfoWatch Traffic Monitor:

- Перехват SMTP-трафика. Возможен перехват трафика (или копии трафика), передаваемого через почтовый relay-сервер, и перехват копии трафика, проходящего через оборудование с поддержкой технологии CISCO SPAN.
- Перехват HTTP-трафика. Возможен перехват трафика, передаваемого через прокси-сервер, поддерживающий ICAP-протокол, и перехват копии трафика, проходящего через оборудование с поддержкой технологии CISCO SPAN.

  Примечание

  При интеграции с прокси-сервером Blue Coat возможен перехват HTTPS-трафика, если прокси-сервер обрабатывает HTTPS-трафик как HTTP-трафик.
- Перехват копии ICQ-трафика (протокол OSCAR), проходящего через оборудование с поддержкой технологии CISCO SPAN. При подключении ICQ через HTTP Система перехватывает ICQ-трафик аналогично трафику HTTP.

Важная информация!

Система не поддерживает перехват и анализ зашифрованного ICQ-трафика, в том числе по зашифрованного протоколу SSL.

- Проверка файлов, находящихся в корпоративной сети (открытых сетевых папок, локальных дисков рабочих станций и файлового хранилища SharePoint 2007), с помощью подсистемы Crawler.
- Анализ Skype-трафика, теневых копий файлов и заданий на печать, передачи трафика по протоколу FTP, контроль обмена данными через Jabber (протокол XMPP) и через Mail.Ru Агент (протокол MPP) Перехват перечисленных данных осуществляется системой InfoWatch Device Monitor.
- Анализ теневых копий файлов, перехваченных системой DeviceLock ЗАО «Смарт Лайн Инк» (версии 6.3 и выше).
- Анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности.
- Фильтрация перехваченного трафика путем выдачи разрешения/запрещения на доставку определенных данных.

Важная информация!

Функция недоступна при работе с копией трафика.

Состав InfoWatch Traffic Monitor

Компонент InfoWatch Traffic Monitor	**Назначение компонента**
Серверная часть	**Traffic Monitor Server**: перехват, анализ и фильтрация трафика, анализ данных, получаемых от систем InfoWatch Device Monitor, DeviceLock. **Sniffer**: перехват и передача на анализ копии трафика, проходящего через SPAN-порт коммутатора. **Модуль IW ICAP**: перехват, анализ и фильтрация HTTP-трафика, передаваемого по протоколу ICAP. **Crawler**: Проверка файлов, находящихся в корпоративной сети (открытых сетевых папок, локальных дисков рабочих станций и файлового хранилища SharePoint 2007). **Модуль взаимодействия с удаленной базой данных**: передача данных на хранение в удаленную базу данных по медленным каналам связи
База данных	Хранение информации, связанной с работой Системы (перехваченные данные, результаты анализа перехваченных данных)
Консоль управления (Management Console)	Настройка правил анализа и фильтрации трафика, анализ полученных данных

2.1 InfoWatch Traffic Monitor Standard и InfoWatch Traffic Monitor Enterprise

В InfoWatch Traffic Monitor предусмотрено две редакции Системы: Traffic Monitor Standard и Traffic Monitor Enterprise.

InfoWatch Traffic Monitor Standard имеет более низкие, чем Traffic Monitor Enterprise, аппаратно-программные требования (подробнее см. документ «*InfoWatch Traffic Monitor. Руководство по установке и конфигурированию*») и имеет ряд ограничений по функциям, а именно:

- Обеспечивается перехват объектов только в режиме копии (подробнее о режимах см. в разделе " Перехват объектов");
- Выполняется периодическое удаление объектов при превышении определенного объема, занимаемого хранящимися в базе данных объектами. Существует возможность установки защиты от этого удаления на отдельные объекты путем назначения специального тега (см. "Назначение тегов объекту").

InfoWatch Traffic Monitor Enterprise обеспечивает полный набор предоставляемых Системой функций (см. "Обзор InfoWatch Traffic Monitor").

2.2 Перехват и анализ объектов

Эта глава содержит следующую информацию:

- Перехват объектов
- Транспортные режимы InfoWatch Traffic Monitor
- Анализ объекта и вынесение вердикта
- Загрузка объекта в базу данных
- Ретроспективный анализ данных, решение пользователя по объекту
- Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов
- Работа системы без сценария анализа объектов

2.2.1 Перехват объектов

Под *объектами* в системе понимаются:

- объекты трафика (SMTP-письма, HTTP-запросы, ICQ-сообщения, Skype-сообщения);
- теневые копии файлов;
- задания на печать.

Возможны несколько вариантов перехвата в зависимости от типа объектов:

Тип объекта	Варианты перехвата объектов
SMTP	• Система выполняет перехват и доставку SMTP-трафика. Возможна фильтрация перехваченных объектов (разрешение/запрещение доставки). *Только для InfoWatch Traffic Monitor Enterprise.*

Тип объекта	Варианты перехвата объектов
	• Система получает копию SMTP-трафика от корпоративного почтового relay-сервера. Система не участвует в доставке трафика. • Система получает копию SMTP-трафика, проходящего через коммутатор, оборудованный SPAN-портом. Перехват копии осуществляется посредством Sniffer. Система не участвует в доставке трафика.
HTTP	• Система перехватывает HTTP-трафик путем интеграции с ICAP-сервером. Возможна фильтрация перехваченных объектов (разрешение/запрещение) доставки. *Только для InfoWatch Traffic Monitor Enterprise.* • Система получает копию HTTP-трафика, проходящего через коммутатор, оборудованный SPAN-портом. Перехват копии осуществляется посредством Sniffer. Система не участвует в доставке трафика.
ICQ	• Система получает копию ICQ-трафика, проходящего через коммутатор, оборудованный SPAN-портом. Перехват копии осуществляется посредством Sniffer. Система не участвует в доставке трафика. • При подключении ICQ через HTTP Система перехватывает ICQ-трафик аналогично трафику HTTP.
Сообщения Skype, GTalk или Mail.Ru Агент	Система получает копию Skype-трафика от InfoWatch Device Monitor.
Файлы, расположенные в корпоративной сети	Система получает копии файлов от подсистемы Crawler
Теневые копии файлов и задания на печать, полученные от InfoWatch Device Monitor	Система получает копию трафика. Блокирование действий пользователя (печать, доступ к устройствам) доступно только через InfoWatch Device Monitor
Теневые копии файлов, полученные от DeviceLock	Система получает копию трафика. Блокирование действий пользователя (доступ к устройствам) доступно только через DeviceLock

Варианты перехвата и последующая доставка объектов связаны с транспортными режимами InfoWatch Traffic Monitor (см. "Транспортные режимы InfoWatch Traffic Monitor").

2.2.2 Транспортные режимы InfoWatch Traffic Monitor

Система InfoWatch Traffic Monitor имеет три транспортных режима: *Нормальный*, *Прозрачный* и *Копия*. Условия, в соответствии с которыми определяется транспортный режим для различных объектов, задаются в сценарии анализа объектов. Назначение объекту транспортного режима происходит в процессе анализа на Traffic Monitor Server (см. "Анализ объекта и вынесение вердикта"). Дальнейшие действия, связанные с транспортировкой объекта, выполняются с учетом выбранного транспортного режима.



Важная информация!

Для каждого объекта транспортный режим может быть задан только один раз.

Различие между режимами работы заключается в особенностях транспортировки объектов (см. таблицу).

Транспортный режим	Описание
Нормальный	Перехват, анализ и дальнейшая транспортировка объектов выполняются посредством Системы InfoWatch Traffic Monitor. В этом режиме возможность доставки объекта получателям определяется вердиктом, вынесенным объекту. Кроме того, в некоторых случаях состояние доставки SMTP-писем может изменяться после смены решения пользователя (см. "Особенности блокировки HTTP-запросов и писем, отправляемых с помощью веб-сервисов"). *Только для InfoWatch Traffic Monitor Enterprise.*
Прозрачный	Отличается от предыдущего режима только тем, что доставка объекта получателям осуществляется всегда (т.е. вне зависимости от вынесенного вердикта). В прозрачном режиме смена решения пользователем не оказывает влияние на доставку объекта получателям. *Только для InfoWatch Traffic Monitor Enterprise.*
Копия	В данном режиме Система получает копии объектов. Отличие режима копии от двух других заключается в том, что транспортировка объектов выполняется без участия Системы. Таким образом, задачей Системы является только анализ объектов. А поскольку анализ выполняется для копии объекта, то вердикт и решение пользователя, вынесенные по результатам анализа, не оказывают влияния на доставку этого объекта получателям

В следующей таблице приведены допустимые транспортные режимы для объектов разного типа.

Тип объекта	Транспортные режимы		
	Нормальный	**Прозрачный**	**Копия**
SMTP-письмо	Да	Да	Да (для копии трафика, полученной от почтового relay-сервера или от Sniffer)
HTTP-запрос	Да (только при перехвате трафика по протоколу ICAP)	Да (только при перехвате трафика по протоколу ICAP)	Да
ICQ-сообщение	Нет	Нет	Да (только для копии трафика, полученной от Sniffer)
Сообщение Skype, GTalk или Mail.Ru Агент	Нет	Нет	Да
Теневая копия файла	Нет	Нет	Да

О подробностях реализации транспортных режимов для различных типов объектов см. документы «*InfoWatch Traffic Monitor. Руководство по установке и конфигурированию*» и «*InfoWatch Traffic Monitor.*

Руководство администратора».

2.2.3 Анализ объекта и вынесение вердикта

Обработка и анализ перехваченных объектов, а также применение к ним политик безопасности, осуществляется следующими подсистемами InfoWatch Traffic Monitor.

Подсистема Traffic Monitor	**Модули подсистемы**	**Функции подсистемы/модуля**
Подсистема Обработки	Модуль Обработки SMTP-трафика (режим копии), Модуль Обработки HTTP-трафика (режим копии), Модуль Обработки ICQ-трафика (режим копии), Модуль Обработки Теневых Копий, Модуль Обработки SMTP-трафика (блокирующий режим), Модуль Обработки HTTP-трафика (блокирующий режим)	Извлечение из перехваченных объектов значимой информации и вложений, определение форматов вложений и передача извлеченных текстов в Подсистему Анализа
Подсистема Анализа	Модуль Лингвистического Анализа	Классификация текста объекта путем поиска соответствия этого текста каким-либо категориям
	Модуль Детектирования Текстовых Объектов	Поиск текстовых объектов (например, номеров кредитных карт) в тексте объектов
	Модуль Детектирования Цифровых Отпечатков	Поиск цитат из эталонных документов в тексте объектов
Подсистема Применения Политик	Модуль Интеграции с Active Directory	Обеспечение первоначального импорта и периодической синхронизации структуры каталога Active Directory со справочником сотрудников и рабочих станций для выполнения дальнейшей привязки этой информации к данным из перехваченных объектов
	Модуль Принятия Решений	Обеспечение применения политики информационной безопасности путем выполнения для объектов правил из сценария обработки объектов.

Анализ объекта выполняется в следующем порядке:

1. **Выделение атрибутов объекта** – Подсистема Обработки выделяет у объектов имеющиеся атрибуты. Например, у SMTP-писем – адреса отправителя и получателей, тема письма и т.п.

Подробный перечень возможных атрибутов объекта приведен в разделах "Общие атрибуты объекта" и "Заголовки конвертов и заголовки объектов"

2. **Извлечение вложенных файлов** – Модуль Принятия Решений анализирует вложенные файлы на основании таких атрибутов, как название и тип файла.

3. **Анализ текста –** Подсистема Анализа обрабатывает текстовые данные: тексты писем, сообщений, запросов, а также тексты, извлеченные из вложений поддерживаемых форматов.

   В системе предусмотрены несколько видов анализа, доступность которых зависит от приобретённой лицензии на продукт:

Технология контентного анализа	**Описание технологии**
Лингвистический анализ	Определение тематики и содержания текста по терминам (словам и словосочетаниям), найденным в тексте. Поиск терминов выполняется на основании классификатора. Классификатор включает в себя терминологию отражающую специфику организации. Все термины распределены по категориям (каждый термин можно соотнести с одной или несколькими категориями). Таким образом, наличие термина, принадлежащего к определенной категории, позволяет соотнести текст с этой категорией. Например, термин *Заработная плата* может принадлежать сразу нескольким категориям (*Внутренние выплаты*, *Условия труда*). Присутствие в тексте этого термина означает, что текст может принадлежать к указанным категориям
Детектирование текстовых объектов	Поиск текстовых объектов, соответствующих заданным шаблонам (например, поиск номеров кредитных карт в текстах перехваченных объектов)
Детектирование цифровых отпечатков	Поиск фрагментов текста, принадлежащих к заранее заданным эталонным документам (например, тексты приказов, финансовых отчетов, договоров и пр.)

4. На основании результатов анализа Модуль Принятия Решений выносит **вердикт** – заключение о возможности наличия нарушений политики информационной безопасности в объекте. Правила вынесения вердикта задаются в сценарии анализа объектов. Предусмотрены следующие вердикты:
   - *Запрещено*. Объект является потенциальным нарушением. В нормальном транспортном режиме доставка такого объекта блокируется.
   - *Разрешено*. Объект не является потенциальным нарушением. В нормальном транспортном режиме по окончании проверки выполняется доставка объекта получателям.

2.2.4 Загрузка объекта в базу данных

После того, как объект проанализирован и по нему принято решение системы (подробнее см. "Анализ объекта и вынесение вердикта"), в базу данных загружается объект и XML-контекст объекта. XML-контекст включает в себя:

- данные (атрибуты, текст), извлеченные из объекта, в том числе из вложений, имеющихся у объекта;
- результаты анализа объекта;
- информацию о решении по объекту.

2.2.5 Ретроспективный анализ данных, решение пользователя по объекту

Объекты, хранящиеся в базе данных, доступны для анализа в консоли управления. При анализе пользователь может просматривать результаты анализа, проведенного Системой, и выносить собственное решение по объекту (атрибут *Решение*).

Первоначально атрибут *Решение* у каждого объекта имеет значение *Решение не принято.* Затем пользователь может вынести по объекту одно из следующих решений:

- *Нарушение*. По результатам анализа пользователь пришел к выводу, что объект нарушает корпоративную политику безопасности.
- *Нет нарушений*. Пользователь проанализировал объект и пришел к выводу, что объект не нарушает корпоративную политику безопасности.

Когда система настроена на фильтрацию SMTP-трафика, принятие решения может привести к разрешению или запрещению доставки SMTP-письма (см. раздел "Вынесение решения по объекту").

Примечание

Фильтрация SMTP-трафика возможна только при условии, что доставка писем осуществляется с участием Системы и для SMTP-трафика установлен нормальный транспортный режим.

2.2.6 Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов

Важная информация!

Блокировка объектов возможна только в InfoWatch Traffic Monitor Enterprise.

Если в нормальном транспортном режиме (см. "Транспортные режимы InfoWatch Traffic Monitor") Система принимает решение о блокировке HTTP-запроса или письма, отправляемого с помощью веб-сервиса (например, mail.ru и т.п.), то в браузере пользователя, отправившего такой запрос или письмо, будет отображена страница с сообщением о блокировке.

Если отправка почты выполняется через почтовые сервисы, построенные по технологии AJAX (такие как Gmail, Windows Live Hotmail и др.), то пользователю может не выдаваться сообщение о том, что доставка письма заблокирована. Как правило, в таких случаях выдается сообщение, определенное самим почтовым сервисом.

POST-запросы на ряд веб-ресурсов (см. таблицу ниже) Система обрабатывает в соответствии со специальными правилами:

- на панели информации об объекте (см. "Просмотр общей информации по объекту") отображаются атрибуты *От*, *Кому*, *Копия*, *Тема* и *Отправлено*, а также вложения, в случае их наличия;
- запросы, для которых нельзя определить эти атрибуты и выделить в их заголовках какой-либо текст, можно удалять как "мусорный" трафик. Таким мусорным трафиком являются, например, фоновые запросы для обновления статуса в социальных сетях. Об использовании этой возможности см. " Проверка мусорного трафика" и "Пример сценария".

Тип веб-ресурса	Ресурсы	
	Без ограничений	**С ограничениями**
Веб-почта	mail.ru, yandex.ru, rambler.ru, pochta.ru, km.ru, newmail.ru, gmail.com, aim.com, gmx.com, yahoo.com, inbox.com, hotmail.com, hotmail.ru, mail.com	gmx.com, yahoo.com, mail.com, aol.com, aim.com На панели информации об объекте отображаются только вложения
Интернет-дневники и социальные сети	livejournal.com (.ru), blogs.mail.ru, liveinternet.ru (li.ru), my.ya.ru, diary.ru, blogspot.com (blogger.com), loveplanet.ru/a-journal, myspace.com, mylivepage.com, privet.ru, perfspot.com, linkedin.com, odnoklassniki.ru, vkontakte.ru (vk.com), facebook.com, twitter.com, wordpress.com	myspace.com, facebook.com На панели информации об объекте отображаются только вложения
Сайты поиска работы и размещения резюме		moikrug.ru, hh.ru, job.ru, rabota.ru, jobs.com, eurojobs.com На панели информации об объекте отображаются только вложения. Не отображается текст, введенный при заполнении формы (например, при заполнении резюме онлайн)
Форумы	forum.ru-board.com, sysadmins.ru, talk.mail.ru, dom.bankir.ru, forum.exler.ru, forum.ixbt.com, groups.google.ru (.com), biznet.ru	

2.2.7 Работа системы без сценария анализа объектов

В процессе работы Системы может возникнуть ситуация, когда подсистема анализа и принятия решений не может использовать сценарий анализа объектов (см. "Настройка сценария анализа объектов"): например, сценарий не создан или был удален, при выполнении сценария произошла ошибка. Кроме того, в сценарии могут быть не заданы или неверно заданы значения для обязательных атрибутов объекта *Транспортный режим* или *Вердикт*. В этом случае объектам назначаются следующие значения для обязательных атрибутов:

- вердикт – *Запрещено*;
- транспортный режим – *Копия*.

Кроме того, для атрибута *Основание вердикта* задается значение *No verdict from script* (Сценарий не определил вердикт).

3 Общие принципы работы с Консолью управления

В следующих разделах содержится общая информация о порядке первоначальной работы пользователя в Консоли управления:

- Запуск консоли управления и подключение к серверу базы данных
- Интерфейс консоли управления
- Обновление данных в консоли управления
- Изменение пользователем собственного пароля

3.1 Запуск Консоли управления и подключение к серверу базы данных

Для работы с консолью управления необходимо наличие постоянного соединения с сервером базы данных. Чтобы подключиться к серверу базы данных, вам необходимо выполнить процедуру авторизации. В процессе авторизации проверяется выполнение следующих условий:

- в базе данных существует учетная запись с указанными параметрами;
- учетная запись не заблокирована.

Если хотя бы одно из условий не соблюдается, вы не сможете авторизоваться в Системе.

Примечание

При первом запуске консоли управления используются данные (имя пользователя и пароль) учетной записи администратора пользователей. Эта учетная запись добавляется в процессе создания схемы базы данных (см. *«InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*).

Подключение к серверу базы данных выполняется при запуске консоли управления. Кроме того, вы можете переподключиться к серверу базы данных в процессе работы с консолью. Как правило, повторное подключение выполняется, если необходимо:

- восстановить прерванное соединение с сервером базы данных;
- подключиться от имени другой учетной записи;
- подключиться к другому серверу базы данных.

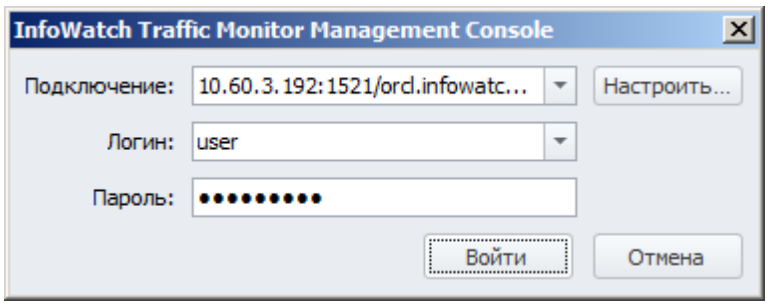
Примечание

Сведения о текущем соединении (*Пользователь@Сервер*) отображаются в строке заголовка главного окна и в левой части строки состояния.

Чтобы начать работу с консолью управления:

1. Выполните нужное действие:

Необходимое действие	Порядок выполнения
Запустить консоль управления и подключиться к серверу базы данных	Выполните одно из следующих действий: • в меню **Пуск** выберите пункт **Программы > InfoWatch > Traffic Monitor > Management Console** • запустите файл программы из каталога, куда она была установлена
Подключиться к серверу базы данных из работающей консоли управления	Выполните одно из следующих действий: • в главном меню выберите команду **Файл > Подключиться**; • нажмите кнопку **Подключиться** на панели инструментов; • нажмите сочетание клавиш клавиатуры `CTRL+SHIFT+C`.



2. В диалоговом окне **InfoWatch Traffic Monitor Management Console** укажите параметры авторизации:

Параметр	Описание
Подключение	Псевдоним сервера базы данных, к которому будет подключена консоль управления. Чтобы выбрать подключение, нажмите на стрелку справа от поля и из раскрывающегося списка выберите необходимое подключение. Если нужного подключения нет в списке, создайте его, как описано в разделе "Настройка списка подключений к базе данных"
Пользователь	Имя учетной записи пользователя
Пароль	Пароль пользователя

Важная информация!

После 10 последовательных попыток авторизации с неправильным паролем, доступ к консоли управления для данного пользователя будет заблокирован на 24 часа (ограничение СУБД Oracle по умолчанию). Чтобы разблокировать консоль до того, как истечет указанный период, обратитесь к администратору базы данных.

Примечание

При первом запуске консоли управления поля диалогового окна **InfoWatch Traffic Monitor Management Console** пустые. В дальнейшем поля **Сервер** и **Пользователь** будут заполнены данными, соответствующими последней успешной попытке авторизации. Поле **Пароль** необходимо заполнять при каждой авторизации.

Если ранее вы уже авторизовались в Системе, то выбрать пару *Пользователь@Сервер* можно, воспользовавшись кнопкой ..., справа от поля **Сервер**.

3. Нажмите кнопку **Войти**.

Если авторизация прошла успешно, то вы получите доступ к главному окну Консоли управления. В противном случае на экран будет выведено сообщение об ошибке.

Важная информация!

Максимальное время ожидания при подключении к серверу базы данных составляет 15 с. Если в течение этого периода соединение с сервером не было установлено, повторите процедуру подключения.

Важная информация!

Если при входе в Консоль вы увидели предупреждение об истечении срока действии лицензии, обратитесь к администратору Traffic Monitor. О подробностях установки и обновления лицензии см. документ *«InfoWatch Traffic Monitor. Руководство администратора»*.

3.1.1 Настройка списка подлючений к базе данных

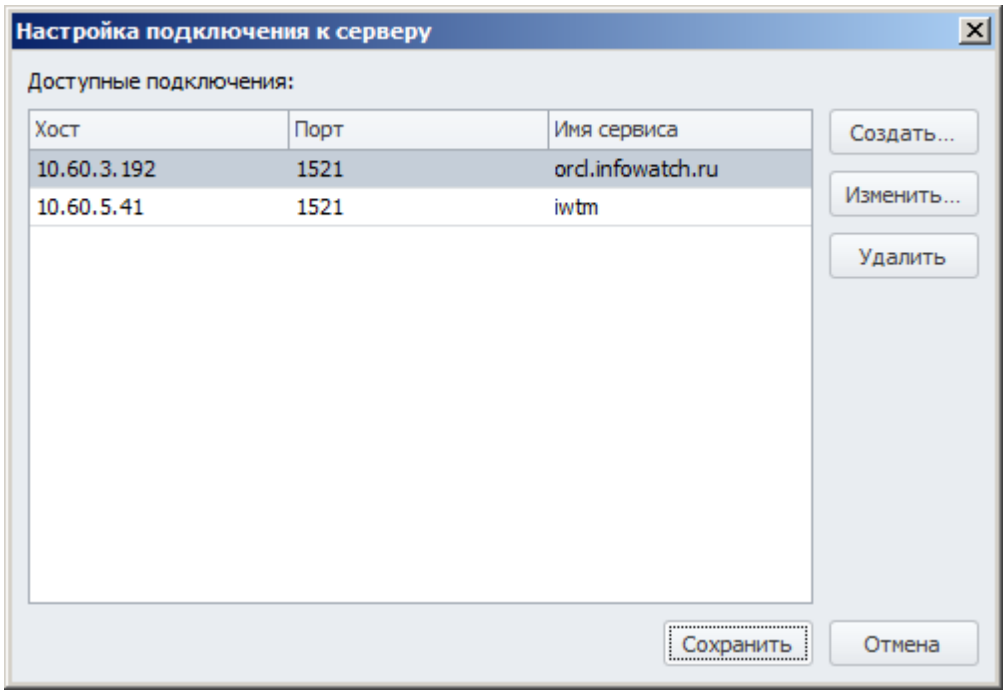
Если при авторизации в Консоли управления (см. "Запуск консоли управления и подключение к серверу базы данных"), в поле **Подключение**, отсутствует запись о необходимом подключении к базе данных InfoWatch Traffic Monitor, вы можете отредактировать список подключений.

Чтобы добавить или изменить запись о параметрах подключения Консоли управления к базе данных:

1. В окне авторизации нажмите кнопку **Настроить**.

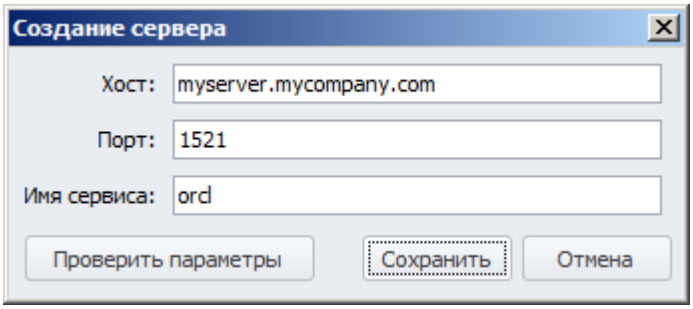
2. В открывшемся окне **Настройка подключения к серверу** выполните одно из следующих действий:

- нажмите кнопку **Создать,** чтобы создать новое подключение;
- выделите строку с подключением и нажмите **Изменить**, чтобы отредактировать параметры существующего.



3. В открывшемся окне **Создание сервера** (**Редактирование сервера**) укажите параметры подключения:

- **Хост** – имя или IP-адрес компьютера, на котором работает сервер базы данных Traffic Monitor;
- **Порт** – порт сервера базы данных, на котором запущен процесс прослушивания клиентских подключений;
- **Имя сервиса** – имя сервиса базы данных.



Вы можете проверить правильность введенных данных, нажав кнопку **Проверить параметры**. При неудачном соединении будет отображено сообщение, уведомляющее о причинах: в этом случае проверьте корректность введенных данных или обратитесь к администратору Системы. В случае установки связи с сервером будет отображено сообщение "*Соединение установлено*".

4. Нажмите **Сохранить**, чтобы сохранить указанные параметры соединения с базой данных и вернуться в диалоговое окно подключения к Консоли управления.

Чтобы удалить запись о подключении:

1. В диалоговом окне **Настройка подключения к серверу** выделите строку с необходимым подключением и нажмите **Удалить**.

2. Нажмите **Сохранить**, чтобы сохранить изменения.

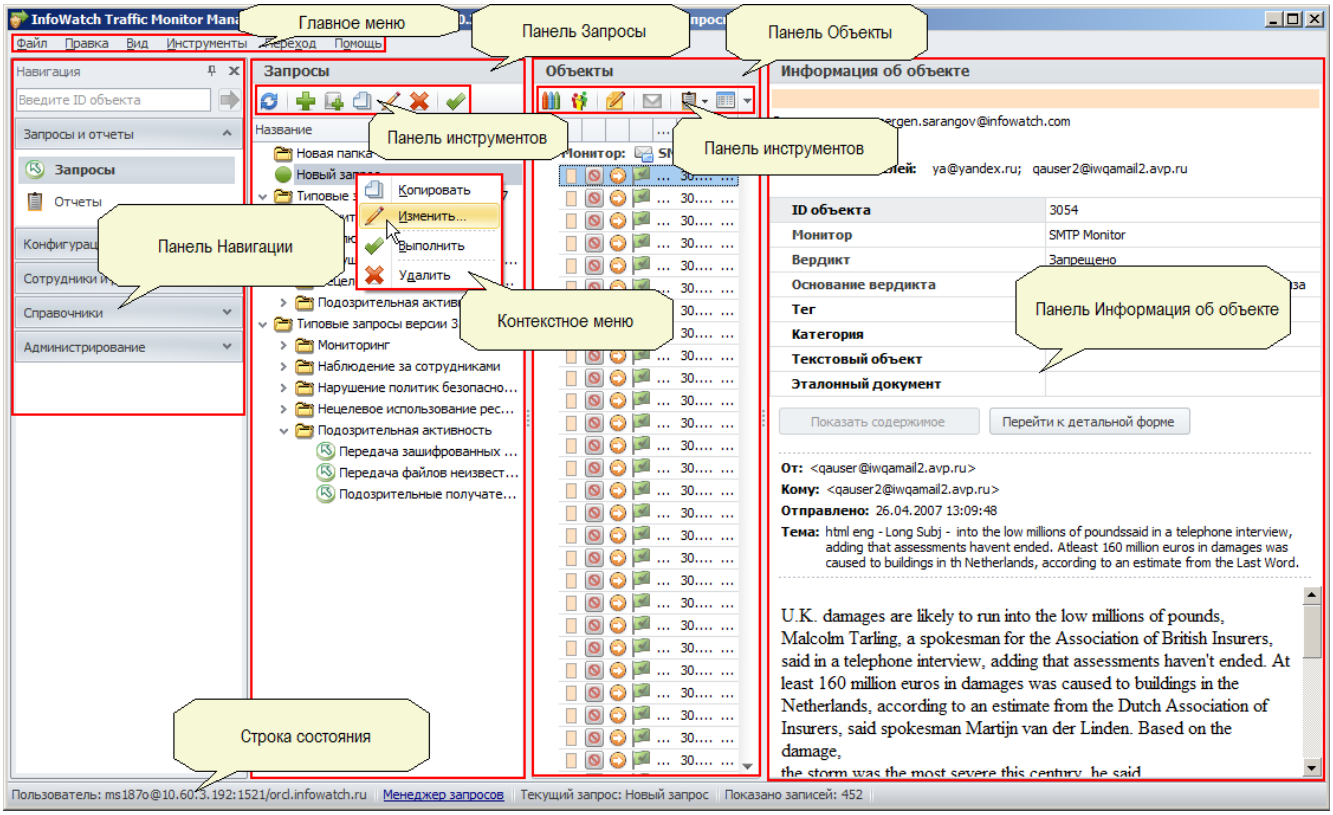
3.2 Интерфейс Консоли управления

В этой главе:

- Главное окно Консоли управления
- Разделы Консоли управления
- Клавиши быстрого доступа

3.2.1 Главное окно Консоли управления

На следующем рисунке показано главное окно Консоли управления InfoWatch Traffic Monitor.



Главное окно после запуска консоли управления

Элементы главного окна перечислены в следующей таблице.

Элемент главного окна	Назначение элемента
Главное меню	Вызов основных функций консоли управления
Панель инструментов	Быстрый доступ к некоторым функциям консоли управления **Примечание:** В некоторых разделах имеются дополнительные панели инструментов

Элемент главного окна	**Назначение элемента**
Контекстное меню (вызывается при щелчке правой кнопки мыши по выбранному объекту)	Управление выбранным объектом (дублирует часть команд главного меню)
Панель **Навигация**	Переход между разделами консоли управления
Панель **Запросы** в разделе **Запросы**	Просмотр и создание запросов на загрузку объектов из базы данных, управление списком запросов
Панель **Объекты** в разделе **Запросы**	Отображение списка объектов, отвечающих выполненному запросу
Панель **Информация об объекте** в разделе **Запросы**	Отображение информации по объекту (при работе с запросами)
Рабочая область главного окна	Отображение элементов выбранного раздела консоли управления, работа с элементами выбранного раздела
Строка состояния	Отображение информации о текущем соединении (*Пользователь@Сервер*). Ссылка на **Менеджер запросов**. При работе со справочниками Active Directory также выводится состояние синхронизации с Active Directory и статус отправки справочника на сервер Traffic Monitor. При работе с запросами также выводится название текущего запроса, количество загруженных записей и т. д.

Вы можете настраивать вид и местоположение панелей **Навигация**, **Список запросов** и **Информация об объекте**.

Чтобы убрать панель с экрана,

в главном меню выберите пункт **Вид** и щелкните левой кнопкой мыши по названию панели, которую вы хотите удалить с экрана. Чтобы снова вывести панель на экран, повторите данное действие.

Чтобы настроить параметры отображения панели Навигация,

выполните одно из следующих действий:

- чтобы перевести панель в режим автоматического свертывания, нажмите кнопку в правом верхнем углу панели **Навигация**. Чтобы отменить режим автоматического свертывания, снова нажмите на эту кнопку.
- чтобы скрыть панель **Навигация**, нажмите кнопку в правом верхнем углу панели.
- чтобы свернуть панель **Навигация** в оконный режим, дважды щелкните левой кнопкой мыши по заголовку панели.

Чтобы изменить местоположение панели Навигация,

щелкните левой кнопкой мыши по заголовку панели и, не отпуская кнопку, переместите панель в другое место экрана. Затем отпустите левую кнопку мыши, чтобы установить панель на новое место.

Чтобы изменить размер панели,

подведите курсор мыши к границе панели. Когда курсор мыши примет вид двунаправленной стрелки, нажмите и не отпускайте левую кнопку мыши. Переместите границу в нужном направлении. Когда панель достигнет необходимого размера, отпустите левую кнопку мыши.

3.2.2 Разделы Консоли управления

Консоль управления InfoWatch Traffic Monitor Management Console включает в себя несколько разделов. Каждый раздел предназначен для выполнения определенных задач по управлению Системой. На панели **Навигация** разделы сгруппированы по областям: **Запросы и отчеты**, **Конфигурация**, **Сотрудники и рабочие станции**, **Справочники**, **Администрирование**.

Чтобы перейти к нужному разделу,

выполните одно из следующих действий:

- в главном меню выберите пункт **Переход** и щелкните левой кнопкой мыши по названию нужного раздела.
- воспользуйтесь ссылками панели **Навигация**.

В следующей таблице приведено описание разделов консоли управления (разделы сгруппированы по областям панели **Навигация**).

Название раздела	Пиктограмма раздела	Назначение раздела
Запросы и отчеты		
Запросы		Вывод информации об обработанных Системой данных. Работа с полученными в результате запроса данными (разрешение/ запрещение на доставку объекта, отправка рапорта, перемещение объекта в другую зону ответственности, присваивание тегов объекту и др.)
Отчеты		Составление отчетов по обработанным Системой данным.
Конфигурация		
Версии конфигурации		Управление версиями конфигурации (просмотр и сравнение различных версий, изменение текущей версии, возврат к прежней версии). Загрузка конфигурации на хосты
Категории и термины		Создание классификатора (наполнение его категориями и терминами). Экспорт/импорт базы классификатора
Текстовые объекты		Составление перечня текстовых объектов и их значений. Выбор текстовых объектов, подлежащих детектированию
Эталонные документы		Составление базы эталонных документов для использования в технологии анализа цифровых отпечатков
Скрипты		Создание сценариев для анализа объектов, активация сценариев, экспорт/ импорт сценариев
Списки		Составление списков (данные списки используются при составлении сценария анализа объектов)

Название раздела	Пиктограмма раздела	Назначение раздела
Сотрудники и рабочие станции		
Сотрудники		Управление импортированными из Active Directory учетными записями сотрудников. Создание учетных записей сотрудников средствами InfoWatch Traffic Monitor
Группы		Управление импортированными из Active Directory группами сотрудников и рабочих станций. Создание групп сотрудников и рабочих станций средствами InfoWatch Traffic Monitor
Рабочие станции		Управление импортированными из Active Directory учетными записями рабочих станций
Справочники		
Теги		Управление группами тегов (создание групп, добавление тегов)
Цвета		Создание списка цветов (применяются для цветового выделения объектов)
Администрирование		
Краулер		Настройка параметров работы сканера файлов Crawler, создание и выполнение задач сканирования сетевых ресурсов
Пользователи		Управление учетными записями пользователей. Распределение ролей. Выбор разрешенных пользователю адресатов для отправки рапорта
Роли		Управление ролями пользователей. Распределение ролей
Зоны ответственности		Управление зонами ответственности (создание зон ответственности, определение пользователей для каждой зоны ответственности).
Хосты		Просмотр списка серверов Traffic Monitor. Просмотр статуса доставки конфигурации на сервера.
Использование БД		Просмотр сведений по использованию базы данных

3.2.3 Клавиши быстрого доступа

В следующей таблице перечислены клавиши и сочетания клавиш, используемые для быстрого доступа к различным функциям Консоли управления InfoWatch Traffic Monitor ("горячие" клавиши, hotkeys).

Название функции	Клавиши быстрого доступа
Общие функции	
Подключиться/переподключиться к серверу базы данных	Ctrl+Shift+C
Вызвать справку	F1

Выйти из Консоли	Alt+F4
Обновить данные (результаты запроса, состояние отчетов, версии конфигурации, категории, сценарии, списки, эталонные документы, сотрудники, рабочие станции, теги, цвета, хосты, статистика использования БД)	F5
Построитель условий в запросах и отчетах	
Создать условие	Ctrl+T
Создать блок условий	Ctrl+И
Редактировать условие	Ctrl+У
Удалить условие	Ctrl+Del
Просмотр объекта: вложения	
Выбрать все вложения	Ctrl+A
Выбрать несколько вложений	Ctrl+левая кнопка мыши
Выбрать диапазон	Shift+левая кнопка мыши

Также вы можете вызывать функции из главного меню: для этого (вначале, при необходимости, выбрав необходимый элемент: объект, запрос, запись..) последовательно нажимайте указанные клавиши (буквы), не отпуская нажатую кнопку **Alt**.

Название функции	Клавиши быстрого доступа
Подключиться/переподключиться к серверу базы данных	Alt+(Ф->П)
Выйти из Консоли	Alt+(Ф->Ы)
Просмотреть информацию о версии Консоли	Alt+(О->О)
Обновить данные	Alt+(В->О)
Включить/отключить панель навигации	Alt+(В->Н)
Включить/отключить панель запросов	Alt+(В->П)
Включить/отключить панель информации об объекте	Alt+(В->И)
Сменить пароль	Alt+(И->И)
Пользовательские настройки	Alt+(И->П)
Глобальные настройки	Alt+(И->Г)
Создать новую запись	Alt+(П->С)
Редактировать запись	Alt+(П->И)
Удалить запись	Alt+(П->У)

Работа с запросами	
Создать запрос	Alt+(П->С)
Создать папку	Alt+(П->П)
Копировать запрос	Alt+(П->К)
Редактировать запрос	Alt+(П->И)
Удалить запрос	Alt+(П->У)
Выполнить запрос	Alt+(П->В)
Обновить список запросов	Alt+(П->Б)
Работа с отчетами	
Создать отчет	Alt+(П->О)
Создать папку	Alt+(П->П)
Редактировать	Alt+(П->И)
Удалить	Alt+(П->У)
Копировать запрос	Alt+(П->К)
Выполнить отчет	Alt+(П->Ы)
Работа с объектами	
Присвоить решение *Нет нарушений*	Alt+(П->О->Н)
Присвоить решение *Нарушение*	Alt+(П->О->А)
Изменить зону ответственности	Alt+(П->О->З)
Добавить описание	Alt+(П->О->Д)
Отправить рапорт	Alt+(П->О->О)
Выгрузить SMTP-письмо	Alt+(П->О->Х)
Выгрузить XML-контекст	Alt+(П->О->Ь)
Открыть форму детального просмотра	Alt+(П->О->Ф)
Открыть системный лог объекта	Alt+(П->О->С)
Просмотреть содержимое	Alt+(П->О->П)
Работа с версиями конфигурации	
Удалить версию	Alt+(П->У)
Откатиться к выбранной версии конфигурации	Alt+(П->О)

Открыть конфигурацию	Alt+(П->К)
Сравнить две версии	Alt+(П->А)
Загрузить редактируемую конфигурацию в базу данных: сделать её активной	Alt+(П->Е)
Работа с категориями и терминами	
Экспортировать классификатор в XML-файл	Alt+(П->Э)
Импортировать классификатор	Alt+(П->З)
Создать категорию	Alt+(П->С)
Редактировать категорию	Alt+(П->И)
Удалить категорию	Alt+(П->У)
Работа с эталонными документами	
Удалить эталонный документ	Alt+(П->У)
Редактировать эталонный документ	Alt+(П->И)
Добавить эталонный документ	Alt+(П->Д)
Работа со сценариями (скриптами)	
Активировать	Alt+(П->А)
Удалить	Alt+(П->У)
Загрузить из файла	Alt+(П->З)
Создать LUA-скрипт	Alt+(П->С)
Редактировать LUA-скрипт	Alt+(П->И)
Работа с группами списков	
Удалить	Alt+(П->У)
Редактировать	Alt+(П->И)
Создать	Alt+(П->П)
Создать группу	Alt+(П->Г)
Работа со списками	
Удалить	Alt+(П->Э->У)
Редактировать	Alt+(П->Э->И)
Создать	Alt+(П->Э->П)
Работа с сотрудниками	

Создать	Alt+(П->С)
Редактировать	Alt+(П->И)
Удалить	Alt+(П->Д)
Работа с группами тегов	
Создать	Alt+(П->С)
Редактировать	Alt+(П->И)
Удалить	Alt+(П->У)
Работа с тегами	
Создать	Alt+(П->Т->С)
Редактировать	Alt+(П->Т->И)
Удалить	Alt+(П->Т->У)
Работа с цветами	
Создать	Alt+(П->С)
Редактировать	Alt+(П->И)
Удалить	Alt+(П->У)
Работа с пользователями	
Создать	Alt+(П->С)
Редактировать	Alt+(П->И)
Удалить	Alt+(П->У)
Работа с ролями	
Создать	Alt+(П->С)
Редактировать	Alt+(П->И)
Удалить	Alt+(П->У)
Работа с зонами ответственности	
Создать	Alt+(П->С)
Редактировать	Alt+(П->И)
Удалить	Alt+(П->У)
Работа с хостами	
Редактировать	Alt+(П->И)

3.3 Обновление данных в Консоли управления

В Системе могут одновременно работать несколько пользователей. Для того чтобы поддерживать в актуальном состоянии сведения о Системе, необходимо периодически выполнять обновление данных. Обновление данных осуществляется автоматически и вручную.

Автоматическое обновление данных, относящихся к определенному разделу консоли управления, выполняется при переходе к этому разделу. Для обновления данных о перехваченных системой объектах вы можете также настроить автоматическое обновление результатов выполнения запроса.

В любом из разделов консоли вы также можете обновлять данные **вручную**.

Чтобы вручную обновить данные:

Необходимое действие	Порядок выполнения
Обновить данные в разделе	Выполните одно из следующих действий: • в главном меню выберите команду **Вид > Обновить**; • нажмите кнопку **Обновить** на панели **Объекты**.
Обновить список запросов в разделе **Запросы**	Нажмите кнопку **Обновить список запросов** на панели **Запросы**

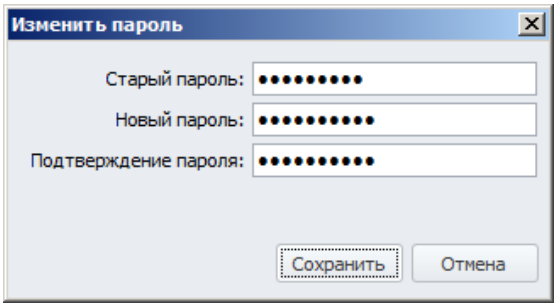
3.4 Изменение пользователем собственного пароля

Пользователь может изменить пароль учетной записи, от имени которой он авторизован в Системе, воспользовавшись специальной функцией.

Чтобы изменить собственный пароль:

1. В главном меню выберите команду **Инструменты > Изменить пароль**.

   На экран будет выведено диалоговое окно **Изменить пароль**.



Смена пароля пользователя

2. В открывшемся диалоговом окне укажите параметры:

Параметр	Описание
Старый пароль	Действующий пароль
Новый пароль **Подтверждение пароля**	Пароль, который будет назначен учетной записи

> **Примечание**
>
> Подробные рекомендации по составлению паролей см. "Рекомендации по составлению имен и паролей пользователей".

3. Нажмите кнопку **Сохранить**.

4 Администрирование Консоли управления

Для организации работы пользователей консоли управления предназначены следующие административные задачи:

- Управление доступом к консоли управления
- Настройка параметров отправки/получения рапортов по объектам
- Настройка уведомлений о нарушениях
- Настройка запроса о выходе из консоли управления
- Работа с хостами
- Просмотр статистики использования базы данных

Также см. "Зоны ответственности: разграничение доступа к объектам"

4.1 Управление доступом к Консоли управления

Возможность выполнять различные действия в консоли управления определяется набором привилегий, которые назначены пользователю. Привилегии передаются пользователю в составе ролей. Причем каждому пользователю (за исключением администратора пользователей) может быть назначена одна или несколько ролей. Пользователь, которому не назначено роли или назначена роль, не имеющая ни одной привилегии, может только изменять свой пароль.

Таким образом, чтобы предоставить пользователю возможность работать с консолью управления, необходимо создать для него учетную запись и назначить учетной записи роли с необходимыми привилегиями.



Важная информация!

В консоли имеется возможность ограничить доступ пользователей, выполняющих анализ объектов, к личной информации, хранящейся в перехваченных объектах (информация о получателях, тексты сообщений, вложения и т. п.). Подробнее см. "Управление доступом к содержимому объектов".

Посмотреть информацию о ролях и учетных записях пользователей можно в разделах **Роли** и **Пользователи** (область **Администрирование** на панели **Навигация**).

Начальная настройка консоли управления осуществляется от имени учетной записи администратора пользователей. С учетной записью администратора пользователей сопоставлена предустановленная роль *Администратор*, имеющая все необходимые права для начальной настройки учетных записей Консоли управления, а именно:

- управление ролями (просмотр, создание, правка и удаление);
- управление учетными записями пользователей (просмотр, создание, правка, блокирование/разблокирование, удаление);
- управление зонами ответственности (просмотр, создание, правка, удаление).

Также в консоли управления есть предустановленная учетная запись *Офицер безопасности*, которой назначена предустановленная роль *Офицер безопасности*, имеющая все привилегии, кроме управления пользователями и ролями (см. "Список привилегий").

Более подробная информация об управлении доступом к консоли управления приведена в следующих подразделах:

- Роли пользователей консоли управления
- Управление доступом к содержимому объектов
- Учетные записи консоли управления
- Изменение пользователем собственного пароля

4.1.1 Роли пользователей консоли управления

Роль пользователя - это совокупность привилегий, определяющих набор действий, которые пользователь может выполнять при работе с системой.

В Системе имеются предустановленные роли пользователей:

- **Администратор** - роль, имеющая все необходимые права для начальной настройки учетных записей Консоли управления.
- **Офицер безопасности** - роль, обладающая всеми привилегиями, кроме управления пользователями и ролями.

Посмотр ролей и управление ими выполняется в Консоли управления, раздел **Роли** (область **Администрирование** на панели **Навигация**).

Более подробно об управлении ролями пользователей:

- Список привилегий
- Создание и редактирование роли
- Удаление роли

4.1.1.1 Список привилегий

В следующей таблице приведен список привилегий, которые могут быть назначены роли. Часть привилегий может быть доступна только при наличии других привилегий. Функции, которые могут быть доступны только при наличии соответствующей привилегии, приведены в столбце *Зависимые функции* и снабжены ссылкой на раздел, в котором они описаны.

Привилегия	**Зависимые функции**
Глобальные настройки: редактирование предупреждений о режимах просмотра объектов	Изменение текста предупреждения, который должен отображаться при просмотре содержимого объекта Изменение текста предупреждения, который отображается при активации режима «Показать содержимое объектов»
Глобальные настройки: редактирование настроек подключения к Active Directory	Изменение настроек подключения к Active Directory и расписания синхронизации
Глобальные настройки: редактирование настроек подключения к серверу краулера	Настройка соединения Консоли управления с сервером
Пользовательские настройки: редактирование	Настройка размера загружаемых SMTP-писем и заданий на печать Включение режима «Показывать содержимое объектов»
Пользователи: просмотр	Просмотр списка учетных записей пользователей
Пользователи: правка	Добавление / редактирование учетной записи пользователя Блокирование / разблокирование учетной записи пользователя
Пользователи: удаление	Удаление учетной записи пользователя
Роли: просмотр	Просмотр списка ролей
Роли: правка	Добавление / редактирование роли
Роли: удаление	Удаление роли
Конфигурация: просмотр	Просмотр информации о конфигурации Сравнение версий конфигурации

Привилегия	Зависимые функции
Конфигурация: удаление	Удаление версии конфигурации
Конфигурация: откат	Возврат к предыдущей версии конфигурации
Конфигурация: описание	Добавление / изменение примечания
Конфигурация: рассылка	Загрузка конфигурации на хост
Списки: просмотр	Просмотр списков Просмотр элементов списка
Списки: правка	Добавление группы списков Добавление списка Редактирование параметров списка / группы списков / элемента списка Добавление элемента списка
Списки: удаление	Удаление списка Удаление элемента списка
Классификатор: просмотр	Просмотр классификатора Просмотр списка терминов Поиск термина
Классификатор: правка	Добавление категории Редактирование категории Смена уровня категории Добавление термина Импорт термина из файла Редактирование термина Перемещение термина между категориями Экспорт / импорт классификатора
Классификатор: удаление	Удаление категории Удаление термина
Скрипт: просмотр	Просмотр списка сценариев
Скрипт: правка	Добавление сценария Экспорт / Импорт сценария Редактирование сценария Активирование сценария
Скрипт: удаление	Удаление сценария
Цвет: просмотр	Просмотр цветов

Привилегия	**Зависимые функции**
Цвет: правка	Добавление / редактирование цвета
Цвет: удаление	Удаление цвета
Теги: просмотр	Просмотр тегов / групп тегов
Теги: правка	Добавление группы тегов Редактирование параметров группы тегов Добавление тега Редактирование тега
Теги: удаление	Удаление тега / группы тегов
Статистика использования базы данных: просмотр	Просмотр статистики использования базы данных
Зоны ответственности: просмотр	Просмотр зон ответственности
Зоны ответственности: правка	Добавление / редактирование зоны ответственности
Зоны ответственности: удаление	Удаление зоны ответственности
Хосты: просмотр	Просмотр сведений о хостах Просмотр профиля хоста
Хосты: правка	Добавление примечания для хоста
Хосты: удаление	Удаление хоста
Объекты: запуск запросов	Просмотр результатов запроса в списке объектов Применение запроса Настройка панели информации об объекте
Объекты: правка запросов	Добавление папки запросов Редактирование папки запросов ("Создание и редактирование папки" и " Перемещение запросов и отчетов между папками") Копирование папки запросов Добавление / редактирование запроса Копирование запроса
Объекты: удаление запросов	Удаление папки запросов Удаление запроса
Объекты: операции по тегам	Назначение тегов объекту
Объекты:	Вынесение решения по объекту

Привилегия	Зависимые функции
пользовательское решение	
Объекты: примечания	Добавление примечания к объекту
Объекты: операции по зонам ответственности	Перемещение объекта в другую зону ответственности
Объекты: рапорт	Составление и отправка рапорта
Объекты: цвет	Выделение объектов цветом
Объекты: просмотр содержимого	Активация режима «Показывать содержимое объектов» Просмотр содержимого объекта на панели информации об объекте (если не включена пользовательская настройка «Показывать содержимое объектов») Просмотр атрибутов объекта на детальной форме просмотра Просмотр системного журнала объекта Выгрузка вложений Сохранение SMTP-сообщения Выгрузка контекста
Отчеты: запуск	Выполнение отчета Перестроение отчета
Отчеты: правка	Добавление папки отчетов Редактирование папки отчетов ("Создание и редактирование папки" и " Перемещение запросов и отчетов между папками") Копирование папки отчетов Добавление / редактирование отчета Копирование отчета
Отчеты: удаление	Удаление папки отчетов Удаление отчета
Текстовые объекты: просмотр	Просмотр текстовых объектов
Текстовые объекты: правка	Редактирование параметров текстовых объектов
Эталонные документы: просмотр	Просмотр списка эталонных документов
Эталонные документы: правка	Добавление эталонного документа и создание цифрового отпечатка Редактирование информации об эталонном документе
Эталонные документы: удаление	Удаление эталонного документа

Привилегия	Зависимые функции
Интеграция с Active Directory: просмотр	Просмотр и фильтрация записей о сотруднике Просмотр и фильтрация записей о рабочей станции
Интеграция с Active Directory: правка	Настройка подключения и синхронизации с Active Directory Редактирование описаний о сотрудников, рабочих станций и групп, импортированных из Active Directory ("Создание и редактирование записи о сотруднике", "Редактирование записи о рабочей станции", "Создание, просмотр и редактирование группы") Создание / редактирование / удаление / восстановление записей о сотрудниках и группах Traffic Monitor ("Справочник сотрудников", "Справочник групп") Создание / изменение контактов сотрудников Загрузка справочников Active Directory на сервер
Краулер: правка	Настройка параметров работы сканера Crawler Создание и редактирование задания на сканирование Удаление задания на сканирование Выполнение и остановка задания Очистка базы хешей

4.1.1.2 Создание и редактирование роли

Важная информация!

Изменения, связанные со сменой привилегий или ролей, назначенных пользователю, авторизованному в Системе, вступают в силу только при следующей авторизации этого пользователя в Системе.

Примечание

Встроенная роль *Администратор* не может быть отредактирована.

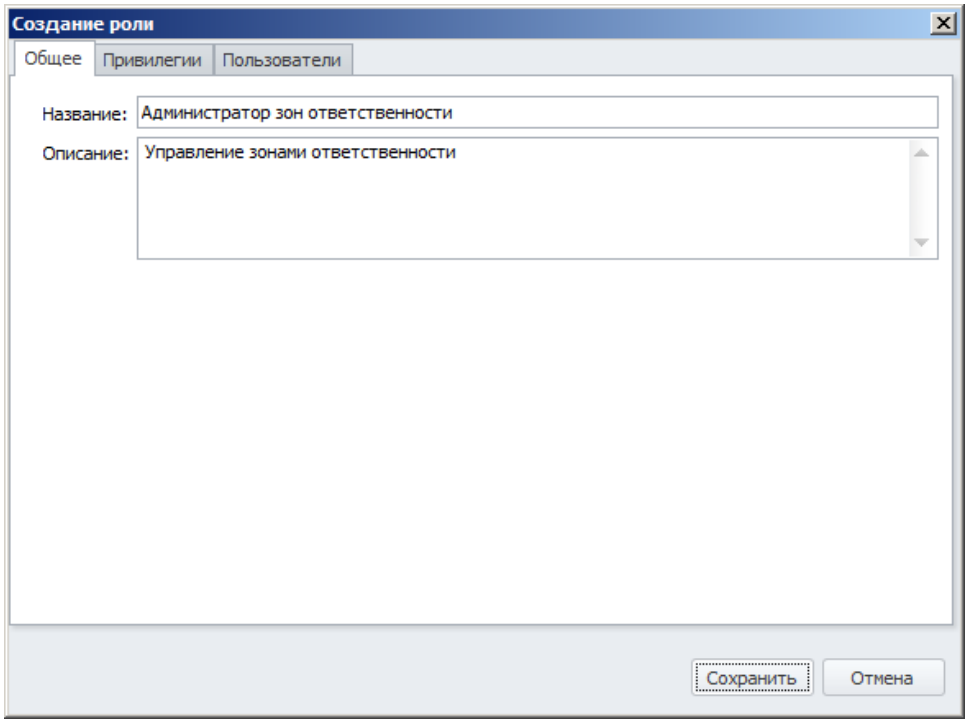
Чтобы создать или отредактировать роль:

1. Перейдите к разделу **Роли**.
2. Выполните необходимые действия:

Действие	Порядок выполнения
Создать роль	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Создать роль** • нажмите кнопку **Создать роль** на панели инструментов
Отредактировать роль	1. В списке ролей выделите строку с нужной ролью. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**;

Действие	Порядок выполнения
	• нажмите кнопку **Изменить** на панели инструментов; • дважды щелкните левой кнопкой мыши по выделенной строке.

На экран будет выведено диалоговое окно с параметрами роли.



Настройка общих параметров роли

3. На вкладке **Общее** настройте общие параметры роли:

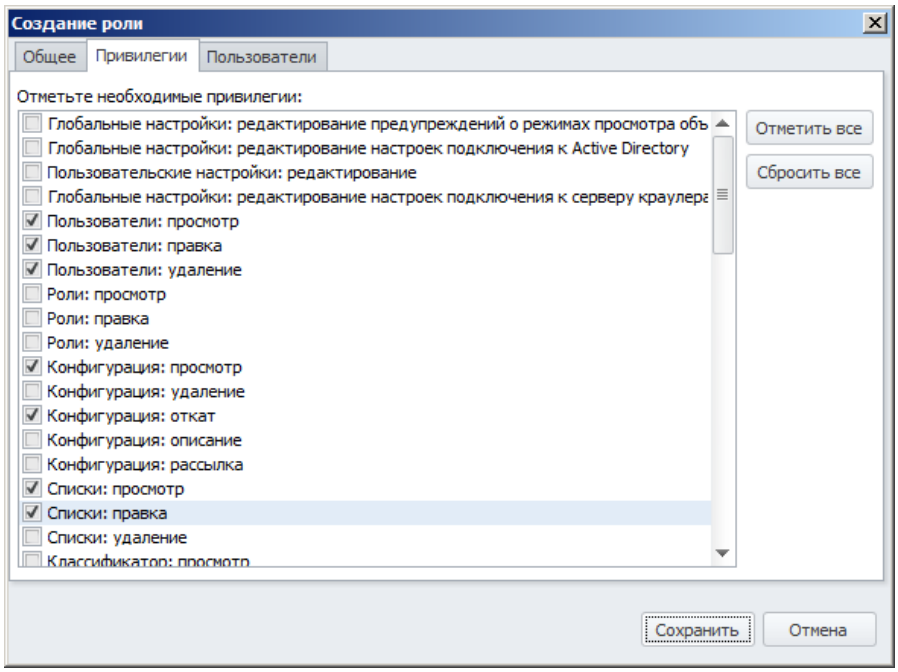
   - **Название**. Название роли (обязательный параметр). Должно быть уникальным.
   - **Описание**. Дополнительная информация.

4. На вкладке **Привилегии** отметьте флажками привилегии, которые будут назначены роли. Чтобы установить или снять все флажки используйте кнопки **Отметить все** и **Сбросить все**.

Важная информация!

Некоторые привилегии могут быть доступны, только в сочетании с другими привилегиями. При выборе таких зависимых привилегий автоматически выбираются те привилегии, от которых они зависят: например, при выборе привилегии «*Теги: правка*» роли также добавляется привилегия «*Теги: просмотр*».

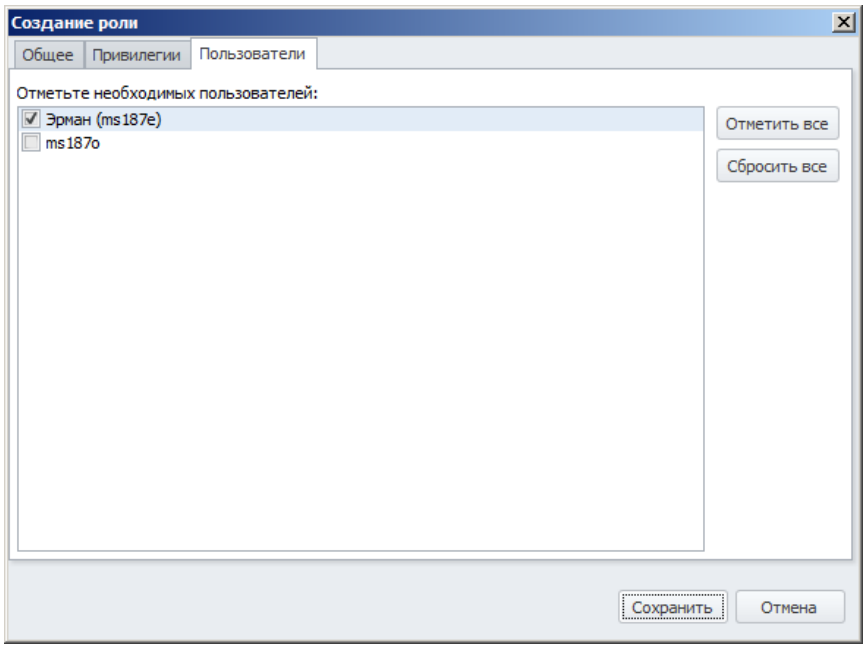
Полный перечень возможных привилегий приведен в разделе "Список привилегий".



Назначение привилегий для роли

5. На вкладке **Пользователи** отметьте флажками учетные записи, которым будет назначена роль. Чтобы установить или снять все флажки используйте кнопки **Отметить все** и **Сбросить все**.

> **Важная информация!**
>
> Роли также можно назначать при создании и редактировании учетных записей пользователей (см. "Создание и редактирование учетной записи пользователя").



Назначение роли пользователям

6. Нажмите кнопку **Сохранить**.

4.1.1.3 Удаление роли

Важная информация!

Встроенная роль *Администратор* не может быть удалена.

Роль, назначенная хотя бы одному пользователю, не может быть удалена.

Чтобы удалить роль:

1. Перейдите к разделу **Роли**.
2. В списке ролей выделите строку с названием нужной роли.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку **Удалить** на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление роли.

4.1.2 Управление доступом к содержимому объектов

Каждый объект, перехватываемый Системой, состоит из содержимого и служебных данных. Под служебными данными в Системе понимаются данные, не содержащие информации личного характера. Содержимое объекта (текст, вложения, некоторые свойства такие, как список получателей, тема и пр.) может включать в себя данные личного характера. В разделах "Общие атрибуты объекта" и "Заголовки конвертов и заголовки объектов" приводятся списки служебных атрибутов и атрибутов содержимого.

Информация по объекту, и в т.ч. содержимое объекта, выводится в запросах и отчетах. Доступ к содержимому объекта имеют только те пользователи, которым назначена роль с привилегией *Объекты: просмотр содержимого*. Для остальных пользователей содержимое объекта в запросах и отчетах не выводится.

Чтобы дать пользователю права на просмотр содержимого:

1. В разделе **Роли** выделите роль, назначенную пользователю.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Изменить**;
   - нажмите кнопку **Изменить** на панели инструментов
   - дважды щелкните левой кнопкой мыши по выделенной строке.
3. В диалоговом окне **Редактирование роли** откройте вкладку **Привилегии** и установите флажок для привилегии *Объекты: просмотр содержимого*.
4. Нажмите кнопку **Сохранить**.

Важная информация!

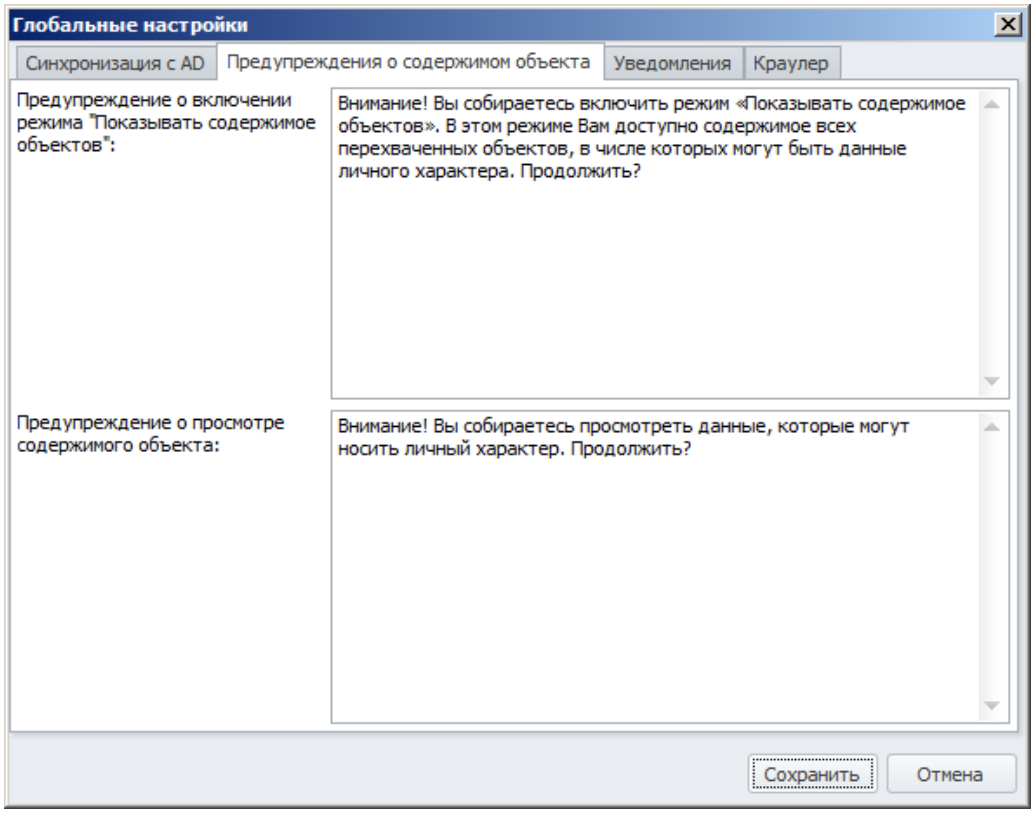
Изменения вступят в действие только при следующей авторизации пользователя в Системе.
При смене привилегий роли убедитесь, что эта роль назначена только тем пользователям, которые имеют право на просмотр личных данных.

По умолчанию содержимое объекта не могут просматривать даже пользователи, имеющие доступ к этому содержимому. Требуется выполнение специальной команды *Показать содержимое* или включение режима показа содержимого (см. "Настройка режима просмотра содержимого объекта"). При выполнении команды *Показать содержимое* и включении режима показа содержимого пользователю выдается предупреждение. Тексты предупреждающих сообщений можно изменять.

Чтобы изменить предупреждение:

1. В главном меню выберите команду **Инструменты > Глобальные настройки**.

2. В диалоговом окне **Глобальные настройки** откройте вкладку **Предупреждения о содержимом объекта** и отредактируйте тексты сообщений:
   - **Предупреждение о просмотре содержимого объекта**. Это уведомление выводится, когда пользователь, работающий с объектом, выполняет команду *Показать содержимое*.
   - **Предупреждение о включении режима «Показывать содержимое объектов»**. Это уведомление выводится, если пользователь изменяет режим отображения содержимого.



Настройка предупреждений о просмотре содержимого объекта

3. Нажмите кнопку **Сохранить**.

4.1.3 Учетные записи Консоли управления

Управление учетными записями пользователей Консоли управления осуществляется путем решения следующих административных задач:

- Создание и редактирование учетной записи пользователя
- Блокирование/разблокирование учетной записи пользователя

- Удаление учетной записи пользователя

Также в данном разделе приведены рекомендации по составлению имен и паролей пользователей

4.1.3.1 Рекомендации по составлению имен и паролей пользователей

Требования к именам пользователей

- Длина имени пользователя может составлять от 1 до 20 символов.
- Имя пользователя может состоять из букв латинского алфавита, цифр и символа подчеркивания «_». Должно начинаться с буквы

Требования к паролям пользователей

- Длина пароля может составлять от 1 до 30 символов.
- Пароль пользователя может состоять из букв латинского алфавита, цифр и символов:

  ! ? # $ % ^ * ( ) _ + - < > , . | \ ; : ~ ` ' [ ] { }

  Может начинаться с буквы, цифры или символа.
- Пароль чувствителен к регистру символов.

Рекомендации по составлению надежных паролей

- Рекомендуемая длина пароля: от 10 до 30 символов.
- Пароль должен представлять собой смешанный набор букв, цифр и символов.
- Не рекомендуется:
  - включать в состав пароля слова и словосочетания;
  - включать в состав пароля несколько идущих подряд одинаковых символов;
  - начинать и заканчивать пароль одним и тем же символом;
  - создавать новый пароль путем добавления символов к текущему паролю.

Общие рекомендации

Не рекомендуется начинать имена и пароли пользователей с последовательностей: SYS_ и ORA_.

В составе имени и пароля пользователя не рекомендуется использовать зарезервированные слова СУБД Oracle:

ACCESS	EXCLUSIVE	MODE	SELECT
ADD	EXISTS	MODIFY	SESSION
ALL	FILE	NOAUDIT	SET
ALTER	FLOAT	NOCOMPRESS	SHARE

AND	FOR	NOT	SIZE
ANY	FROM	NOWAIT	SMALLINT
AS	GRANT	NULL	START
ASC	GROUP	NUMBER	SUCCESSFUL
AUDITBETWEEN	HAVING	OF	SYNONYM
BY	IDENTIFIED	OFFLINE	SYSDATE
CHAR	IMMEDIATE	ON	TABLE
CHECK	IN	ONLINE	THEN
CLUSTER	INCREMENT	OPTION	TO
COLUMN	INDEX	OR	TRIGGER
COMMENT	INITIAL	ORDER	UID
COMPRESS	INSERT	PCTFREE	UNION
CONNECT	INTEGER	PRIOR	UNIQUE
CREATE	INTERSECT	PRIVILEGES	UPDATE
CURRENT	INTO	PUBLIC	USER
DATE	IS	RAW	VALIDATE
DECIMAL	LEVEL	RENAME	VALUES
DEFAULT	LIKE	RESOURCE	VARCHAR
DELETE	LOCK	REVOKE	VARCHAR2
DESC	LONG	ROW	VIEW
DISTINCT	MAXEXTENTS	ROWID	WHENEVER
DROP	MINUS	ROWNUM	WHERE
ELSE	MLSLABEL	ROWS	WITH

4.1.3.2 Создание и редактирование учетной записи пользователя

Важная информация!

Изменения, связанные со сменой привилегий или ролей, назначенных пользователю, авторизованному в Системе вступят в силу только при следующей авторизации этого пользователя в Системе.

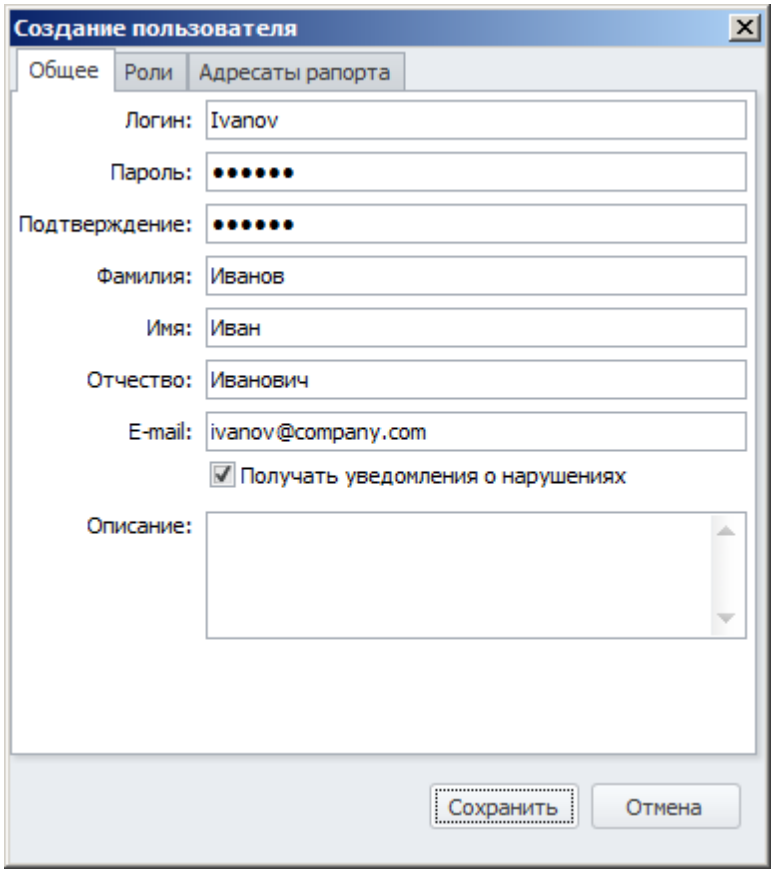
Чтобы создать или отредактировать учетную запись пользователя:

1. Перейдите к разделу **Пользователи**.
2. Выполните необходимые действия:

Действие	**Порядок выполнения**
Создать учетную запись пользователя	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Создать пользователя** • нажмите кнопку **Создать пользователя** на панели инструментов

Действие	Порядок выполнения
Отредактировать учетную запись пользователя	1. В списке учетных записей выделите строку с нужной записью. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку **Изменить** на панели инструментов; • дважды щелкните левой кнопкой мыши по выделенной строке.

На экран будет выведено диалоговое окно с параметрами учетной записи пользователя.



Учетная запись пользователя (общие настройки)

3. На вкладке **Общее** укажите общие параметры учетной записи.

- **Логин**. Имя учетной записи пользователя (обязательный параметр). Может состоять из букв латинского алфавита, цифр и символа подчеркивания; должно начинаться с буквы. Должно быть уникальным.

- **Пароль**, **Подтверждение пароля**. Пароль пользователя (обязательный параметр).

Примечание

Подробные рекомендации по составлению имен пользователей и паролей см. "Рекомендации по составлению имен и паролей пользователей".

- **Фамилия**, **Имя**, **Отчество**. Персональные данные пользователя.

- **Адрес E-mail**. Поле заполняется только для тех пользователей, в задачи которых входит отправка/прием рапортов (настройка системы доставки рапортов см. "Настройка параметров отправки/получения рапортов по объектам").

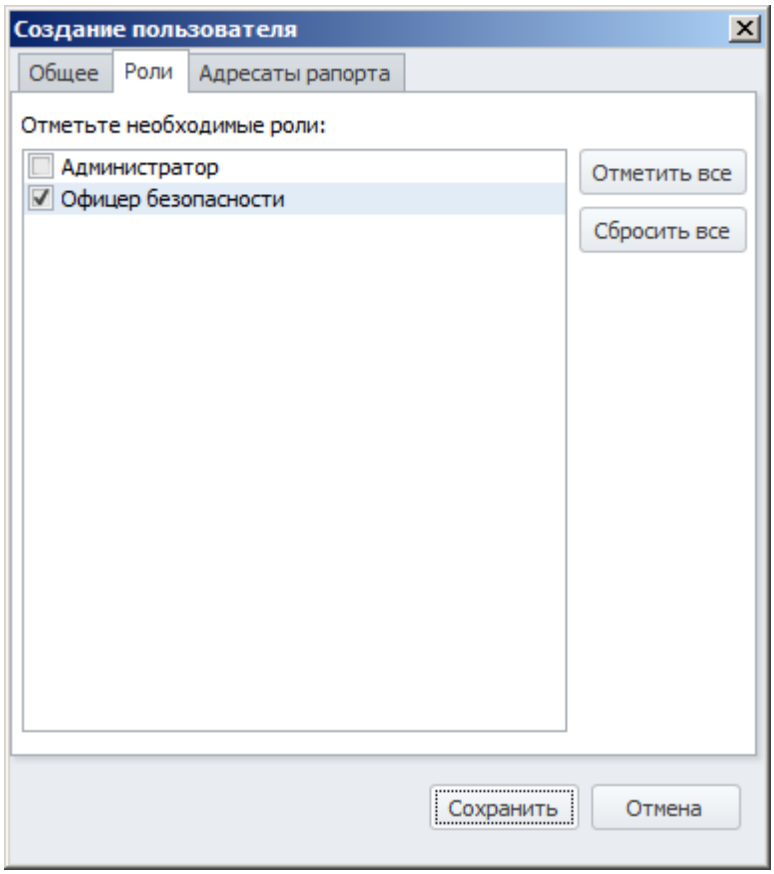
- **Получать оповещение о нарушении**. Отметьте данный пункт, если офицер безопасности должен получать почтовые уведомления о том, что Система перехватила объект, нарушивший политику безопасности. Подробнее об этой возможности см. "Настройка уведомлений о нарушениях".

- **Описание**. Дополнительная информация: комментарии к учетной записи пользователя.

4. На вкладке **Роли** отметьте флажками роли, которые будут назначены учетной записи. Чтобы установить или снять все флажки, используйте кнопки **Отметить все** и **Сбросить все**.

> **Примечание**
>
> Назначить пользователю определенную роль можно также при создании/редактировании роли (см. "Создание и редактирование роли").

> **Важная информация!**
>
> Пользователь, которому не назначено роли или назначена роль, не имеющая ни одной привилегии, может только изменять свой пароль.
> При назначении нескольких ролей происходит объединение привилегий. Поэтому пользователь будет иметь все привилегии, доступные для выбранных ролей.



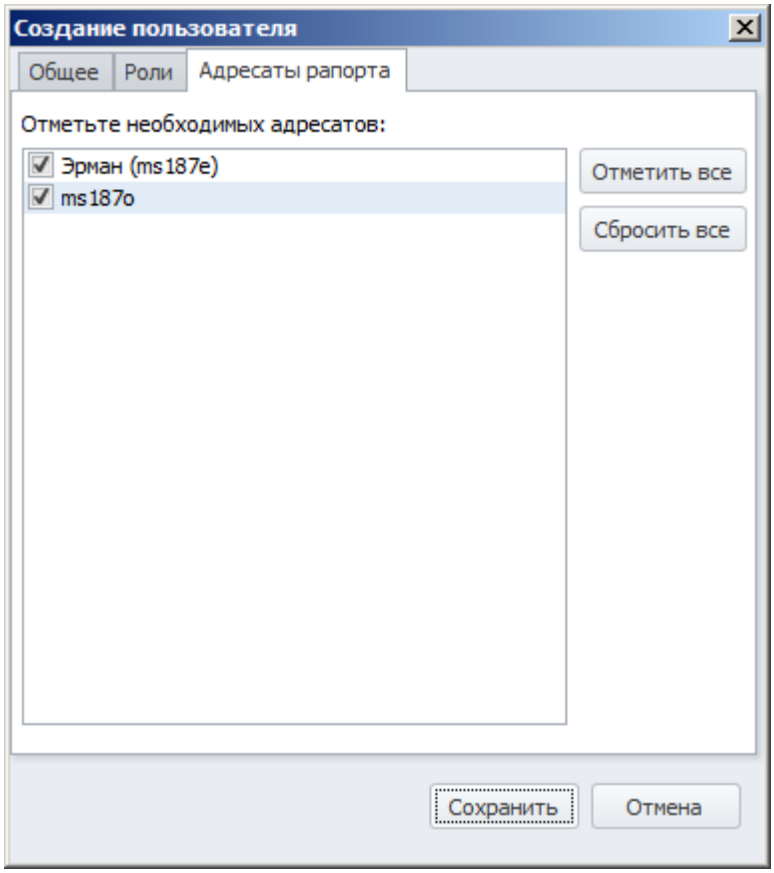
Назначение ролей для учетной записи пользователя

5. Если пользователь, для которого создается учетная запись, должен отправлять рапорты по объектам (см. "Отправка рапорта по объекту"), отметьте флажками тех пользователей, которым пользователь

сможет направлять рапорт. Чтобы установить или снять все флажки, используйте кнопки **Отметить все** и **Сбросить все**.

Важная информация!

Доставка рапорта будет осуществляться через почтовый сервер, адрес которого задан в окне **Пользовательские настройки** (см. "Настройка почтового сервера для отправки рапортов").



Выбор адресатов для доставки рапортов

6. Нажмите кнопку **Сохранить**.

4.1.3.3 Блокирование/разблокирование учетной записи пользователя

Учетная запись может находиться в одном из двух состояний: *Активен* или *Заблокирован*. Состояние учетной записи определяет наличие или отсутствие у пользователя прав на работу с Системой. Пользователь, учетная запись которого находится в заблокированном состоянии, не может авторизоваться в Системе, даже при наличии необходимых привилегий.

Важная информация!

Если состояние учетной записи (блокирование/разблокирование) было изменено, то это изменение вступит в силу только при очередной авторизации пользователя в Системе.

Чтобы изменить статус учетной записи:

1. Перейдите к разделу **Пользователи**.
2. В списке учетных записей выделите строку с нужной учетной записью.
3. Выполните одно из следующих действий:
   - Чтобы заблокировать учетную запись, в главном меню выберите команду **Правка > Заблокировать**. Или нажмите кнопку **Заблокировать** на панели инструментов.

   После этого учетной записи будет присвоен статус *Заблокирован*.
   - Чтобы разблокировать учетную запись, в главном меню выберите команду **Правка > Разблокировать**. Или нажмите кнопку **Разблокировать** на панели инструментов.

   После этого учетной записи будет присвоен статус *Активен*.

4.1.3.4 Удаление учетной записи пользователя

Вы можете удалить любую учетную запись, за исключением учетной записи администратора пользователей и той учетной записи, от имени которой вы авторизованы в текущий момент.

Важная информация!

Если в Системе есть запросы или отчеты, которые назначены только удаляемому пользователю, то в результате удаления учетной записи этого пользователя, такие запросы или отчеты будут также удалены. Перед удалением такой учетной записи Система выдает соответствующее предупреждение.

Поэтому рекомендуется предварительно авторизоваться в Системе под учетной записью пользователя, которого планируется удалить (см. "Запуск Консоли управления и подключение к серверу базы данных "), и изменить права доступа к тем отчетам (см. "Создание и редактирование отчета") или запросам (см. "Распределение прав на работу с запросом"), к которым имеет доступ только он.

Перед удалением учетной записи пользователя закройте все активные соединения этого пользователя с базой данных (в т.ч. открытые не через Консоль управления).

Чтобы удалить учетную запись пользователя:

1. Перейдите к разделу **Пользователи**.
2. В списке учетных записей выделите строку с нужной учетной записью.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку **Удалить** на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

4.2 Настройка параметров отправки/получения рапортов по объектам

Чтобы пользователи имели возможность отправлять/получать рапорты по объектам (подробнее см. " Отправка рапорта по объекту"), выполните следующие настройки:

1. Задайте почтовый сервер, через который будет выполняться доставка рапортов ("Настройка почтового сервера для отправки рапортов").

2. Настройте учетные записи тех пользователей, которым может быть направлен рапорт. Для этого в параметрах учетной записи нужно указать e-mail адрес, на который будет осуществляться доставка рапорта.

3. Настройте учетные записи пользователей, которые будут отправлять рапорты, следующим образом:

   - задайте e-mail адрес, с которого будет выполняться отправка рапорта.

   - назначьте пользователю роль с обязательным набором привилегий: *Объекты: запуск запросов, Объекты: рапорт*.

   - выберите адресатов, которым данный пользователь сможет направлять рапорт.

О создании и редактировании учетных записей см. "Создание и редактирование учетной записи пользователя".

О создании и редактировании ролей см. "Создание и редактирование роли".

Примечание

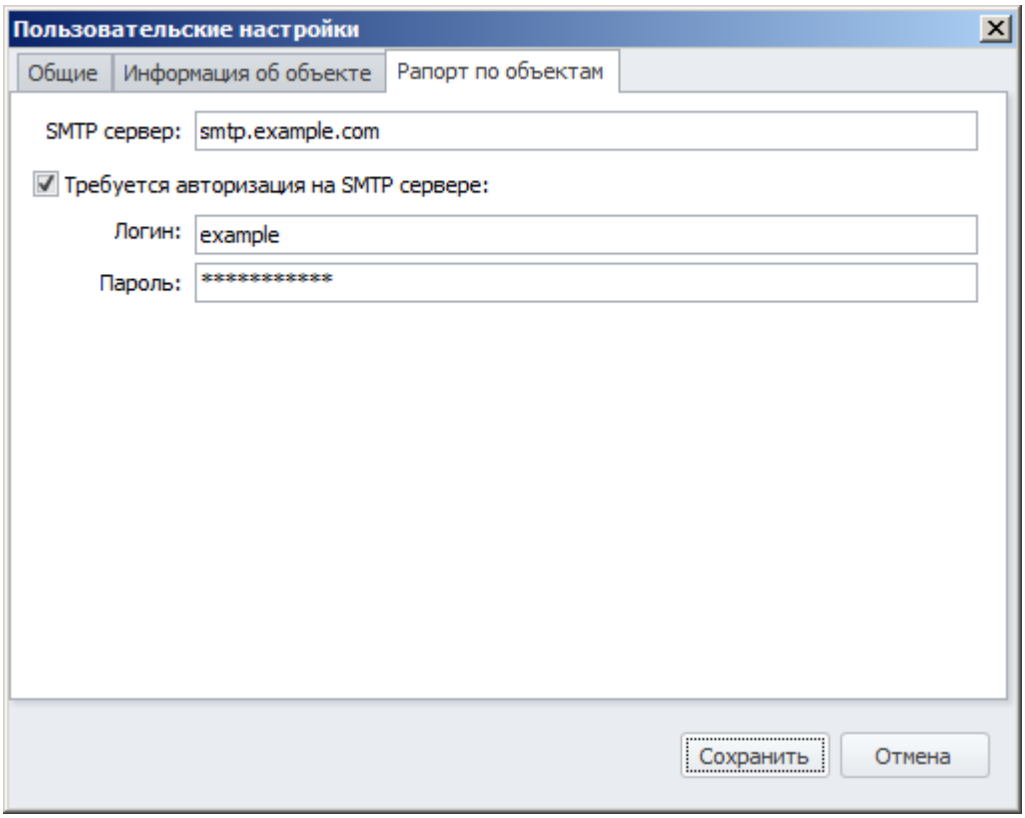
На компьютере, с которого будут отправляться рапорты, необходимо внести изменения в настройки операционной системы. Для этого откройте **Панель управления** (**Пуск** > **Настройки** > **Панель управления**). Затем выберите компонент **Язык и региональные стандарты**. В открывшемся диалоговом окне перейдите на вкладку **Дополнительно** и выберите русский язык для программ, не поддерживающих Unicode.

4.2.1 Настройка почтового сервера для отправки рапортов

Чтобы указать почтовый сервер, через который будет осуществляться доставка рапорта адресатам:

1. В главном меню выберите команду **Инструменты > Пользовательские настройки**.

2. В диалоговом окне **Пользовательские настройки**, на вкладке **Рапорт по объектам** укажите параметры сервера:



Настройка почтового сервера для отправки рапорта

- в поле **SMTP сервер** укажите доменное имя или IP-адрес почтового сервера, через который будет выполняться отправка рапортов;

  Важная информация!

  Если данный параметр не задан, то доставка рапортов осуществляться не будет.

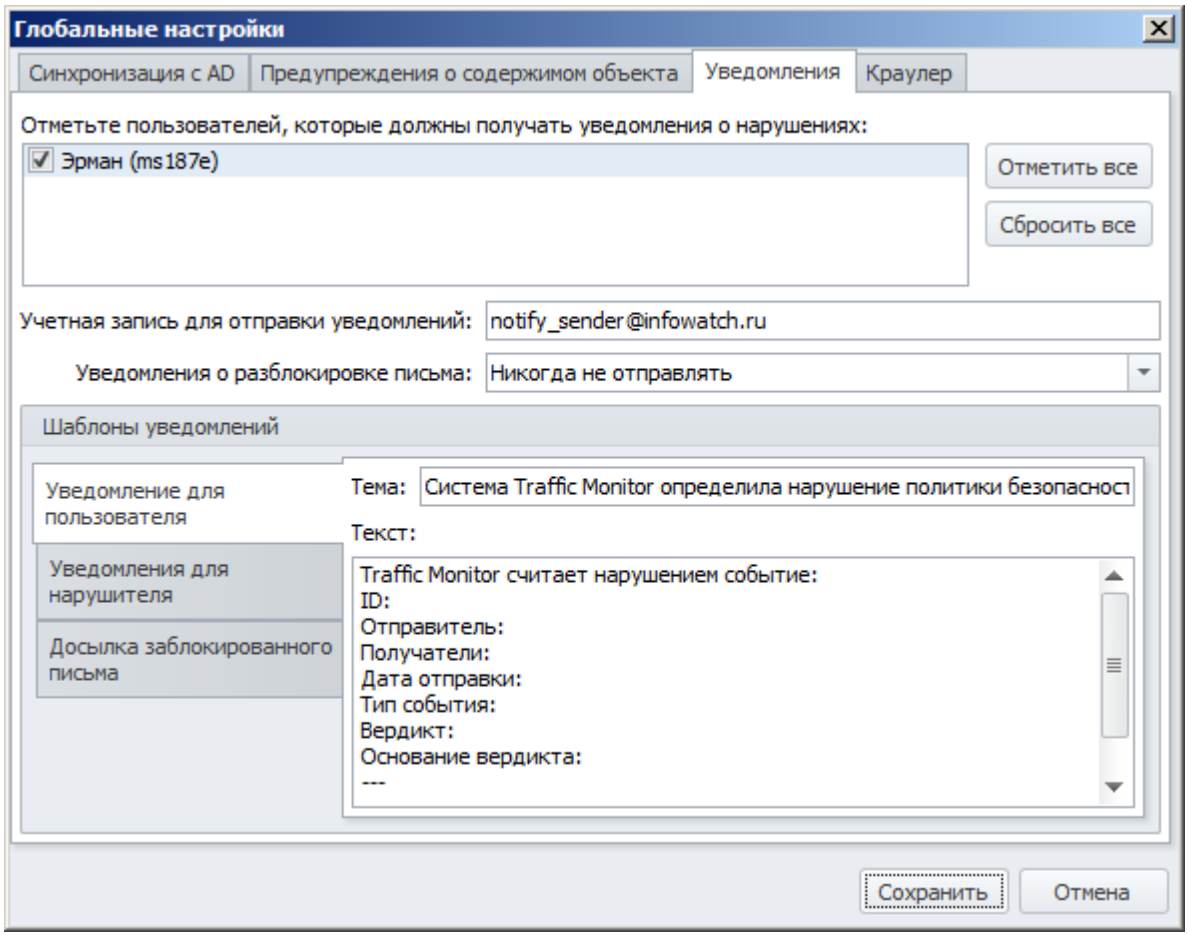
- если на почтовом сервере требуется авторизация по паролю, то установите флажок **Требуется авторизация на SMTP сервере** и укажите параметры авторизации в полях **Логин** и **Пароль**.

3. Нажмите кнопку **Сохранить**.

4.3 Настройка уведомлений о нарушениях

Система может автоматически отправлять почтовые уведомления о том, что перехвачен объект, признанный потенциальным нарушением политики безопасности, а также о том, что по объекту (SMTP-письмо), ранее признанном потенциальным нарушением и заблокированному, разрешена отправка (решение *Нет нарушений*) и оно было дослано Системой.

Данные настройки выполняются с помощью команды **Инструменты > Глобальные настройки**, на вкладке **Уведомления**.



Настройка уведомлений о нарушениях

В этом диалоговом окне можно настроить следующие уведомления:

- **Уведомление для офицера безопасности** – письмо с данными о перехваченном объекте, нарушившем политику безопасности. Настройте перечень офицеров безопасности (пользователей Консоли управления Traffic Monitor), получающих данные уведомления. Для того, чтобы офицер мог получать такие уведомления и отображался в данном списке, в параметрах его учётной записи должна быть отмечена настройка **Получать оповещение о нарушении** (см. "Создание и редактирование учетной записи пользователя").
  Настройка того, должно ли для того или иного объекта производиться оповещение, выполняется в сценарии анализа объектов, с помощью параметра функции `SendNotificationUser` (подробнее см. "Отправка уведомления для офицера безопасности").
- **Уведомление для нарушителя** – письмо пользователю (сотруднику), отправившему объект, который был признан системой потенциальным нарушением политики безопасности. Настройка того, должно ли для того или иного объекта производиться оповещение, выполняется в сценарии анализа объектов, с помощью функции `SendNotificationEmployee` (подробнее см. "Отправка уведомления для нарушителя").
- **Досылка заблокированного письма** – Если пользователь (сотрудник) отправил SMTP-письмо, признанное потенциальным нарушением политики безопасности и заблокированное системой (*Нормальный* транспортный режим), то впоследствии офицер безопасности может разрешить его отправке (см. "Вынесение решения по объекту", решение *Нет нарушений*). В этом случае письмо будет "дослано", а сотруднику будет отправлено уведомление с указанным текстом.

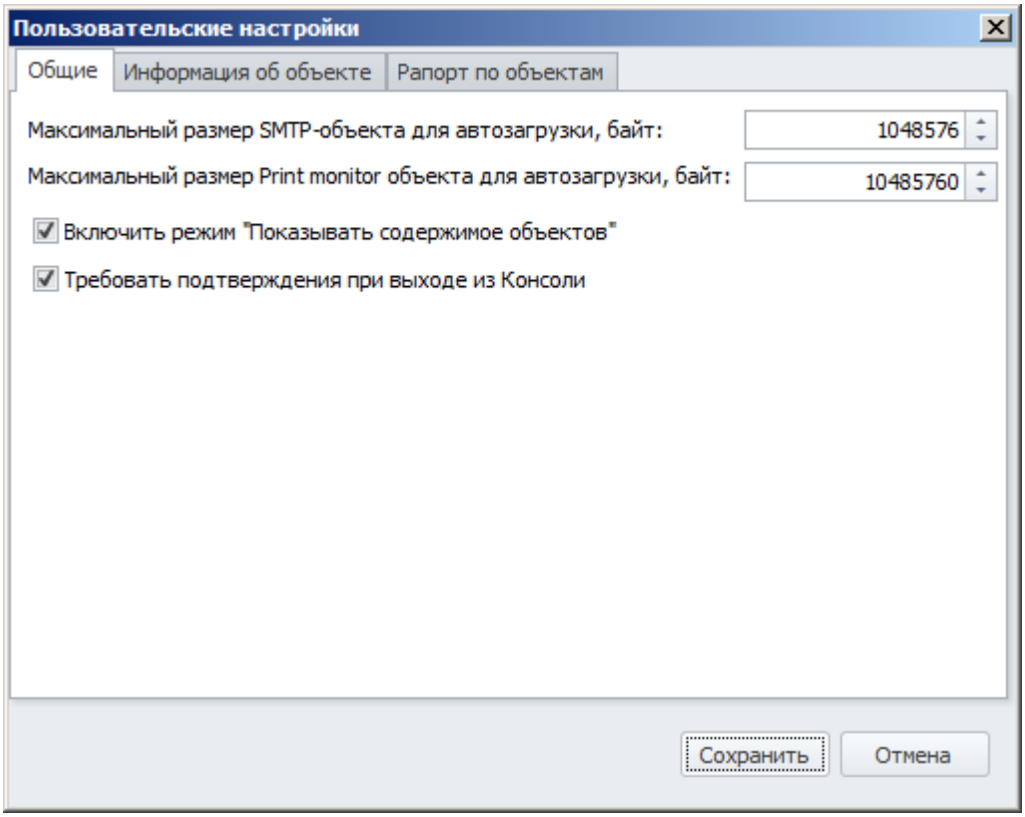
4.4 Настройка запроса о выходе из Консоли управления

Исключить возможность случайного закрытия консоли управления можно, настроив запрос на выход из консоли управления.

Чтобы настроить подтверждение:

1. Выберите команду **Инструменты > Пользовательские настройки** из главного меню.

2. В диалоговом окне **Пользовательские настройки** на вкладке **Общие** установите флажок **Требовать подтверждения при выходе из Консоли**.



Настройка запроса о выходе из Консоли управления

3. Нажмите кнопку **Сохранить**.

4.5 Работа с хостами

Под хостом в Системе понимается компьютер, на который установлен сервер Traffic Monitor.

Каждый хост имеет свой профиль, определяемый набором параметров, соответствующих выполняемым задачам. Существуют следующие параметры хостов:

Параметр хоста	Задачи хоста
Категории и термины	Поиск в тексте, извлеченном из объекта, терминов (слов и словосочетаний) из классификатора (см. "Классификатор"): • получение из базы данных актуального классификатора в рамках загрузки конфигурации на хост (см. "Загрузка конфигурации на хосты"); • получение от хоста с параметром **Скрипты** информации об обрабатываемых объектах; • поиск терминов в тексте объекта; • передача информации о найденных терминах и категориях на хост с параметром **Скрипты**.
Текстовые объекты	Поиск в тексте, извлеченном из объекта, данных со структурой, соответствующей заданным шаблонам (номера паспортов, кредитных карт, телефонные номера и т.п.) (см. "Текстовые объекты"): • получение из базы данных актуальных шаблонов текстовых объектов в рамках загрузки конфигурации на хост (см. "Загрузка конфигурации на хосты"); • получение от хоста с параметром **Скрипты** информации об обрабатываемых объектах; • поиск текстовых объектов по шаблонам; • передача информации о найденных соответствиях на хост с параметром **Скрипты**.
Списки	Поиск в тексте, извлеченном из объекта, элементов списков (см. "Списки"): • получение из базы данных актуальных списков в рамках загрузки конфигурации на хост (см. "Загрузка конфигурации на хосты"); • получение от хоста с параметром **Скрипты** информации об обрабатываемых объектах; • поиск элементов списков по тексту объекта; • передача информации о найденных списках на хост с параметром **Скрипты**.
Скрипты	Обработка перехваченных объектов согласно активному сценарию обработки объектов: • получение из базы данных текста активного пользовательского сценария в рамках загрузки конфигурации на хост (см. "Загрузка конфигурации на хосты"); • обработка перехваченных объектов согласно правилам, указанным в активном сценарии; • передача хосту с параметром **Active Directory** информации об отправителях и получателях объекта; • при необходимости контентного анализа – передача хостам контентного анализа (**Категории и термины**, **Текстовые объекты** и **Эталонные документы**) информации об обрабатываемых объектах и искомых элементах; • получение результатов контентного анализа и анализа данных отправителя и получателей; • назначение объектам атрибутов (вердикт, основание вердикта, цвета и др.) согласно условиям, указанным в активном сценарии; • передача информации о результатах анализа в базу данных.

Параметр хоста	Задачи хоста
	Примечание: Блокировка либо отправка объектов согласно принятым вердиктам выполняется независимо от профиля хоста и определяется администратором Traffic Monitor Server, как описано в документе «*InfoWatch Traffic Monitor. Руководство администратора*».
Состояние каталога	Поиск в атрибутах объекта данных сотрудников и рабочих станций ("Справочник сотрудников и рабочих станций"): • получение из базы данных актуальной информации о справочниках сотрудников и рабочих станциях в рамках загрузки на хост только справочников ("Загрузка справочников на хост") либо всей конфигурации (см. "Загрузка конфигурации на хосты"); • получение от хоста с параметром **Скрипты** информации об обрабатываемых объектах; • обработка данных для поиска соответствия с записями из справочников сотрудников и рабочих станций; • передача информации о найденных соответствиях на хост с параметром **Скрипты**. **Примечание:** Синхронизация Traffic Monitor Server с Microsoft Active Directory выполняется независимо от профиля хоста и определяется администратором Traffic Monitor Server, как описано в документе «*InfoWatch Traffic Monitor. Руководство администратора*». О настройке подключения и синхронизации с сервером Active Directory см. "Настройка подключения и синхронизации с Active Directory".
Эталонные документы	Поиск в тексте, извлеченном из объекта, цитат из базы эталонных документов (см. " База эталонных документов"): • получение из базы данных актуальных списков в рамках загрузки конфигурации на хост (см. "Загрузка конфигурации на хосты"); • получение от хоста с параметром **Скрипты** информации об обрабатываемых объектах; • поиск цитат по тексту объекта; • передача информации об обнаруженных цитатах на хост с параметром **Скрипты**.

Параметры **Категории и термины**, **Текстовые объекты** и **Эталонные документы** совместно обеспечивают контентный анализ текста, извлеченного из перехваченных объектов, и могут назначаться серверу только вместе.

Параметры **Списки** и **Скрипты** совместно обеспечивают анализ и изменение атрибутов перехваченного объекта, обеспечивают принятие решения о нарушении объектом корпоративной политики безопасности и могут назначаться серверу только вместе.

Список хостов и их параметров определяется администратором Traffic Monitor Server, как описано в документе «*InfoWatch Traffic Monitor. Руководство администратора*».

В Консоли управления работа с хостами ведется в разделе **Хосты** (область **Администрирование** на панели **Навигация**). Пользователь может выполнить с хостами только следующие действия:

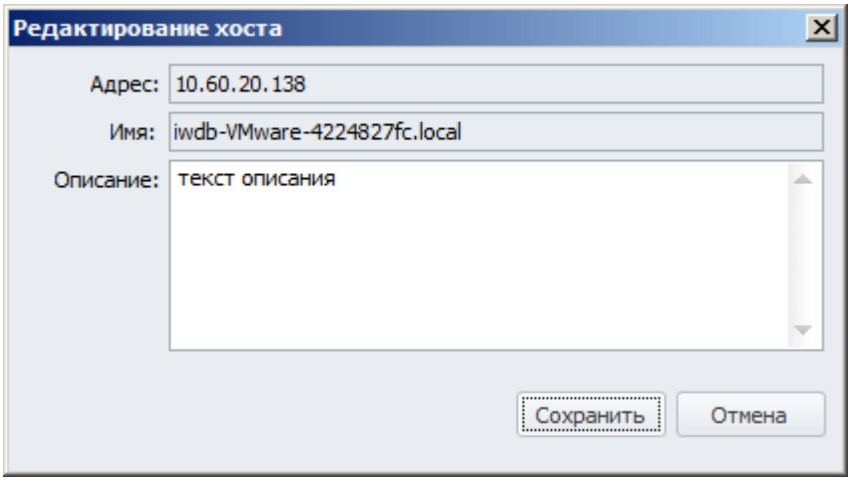
- Добавить описание к записи о хосте ("Добавление описания хоста").
- Удалить из списка запись о хосте, ставшем неактивным ("Удаление хоста").

4.5.1 Добавление описания хоста

Чтобы добавить или изменить описание хоста:

1. Перейдите к разделу **Хосты**.
2. На панели хостов выделите нужный хост.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Изменить**;
   - нажмите кнопку **Изменить** на панели инструментов.

   На экран будет выведено диалоговое окно **Редактирование хоста**.



Добавление описания хоста

4. В поле **Описание** укажите необходимые сведения о хосте.
5. Нажмите кнопку **Сохранить**.

4.5.2 Удаление хоста

Работающие хосты имеют статус **Активный** и отмечаются пиктограммой ; если хост становится недоступным, то он получает статус **Неактивный** и отмечается пиктограммой . Если хост стал неактивным, то вы можете удалить запись о нём из списка хостов.

Чтобы удалить хост:

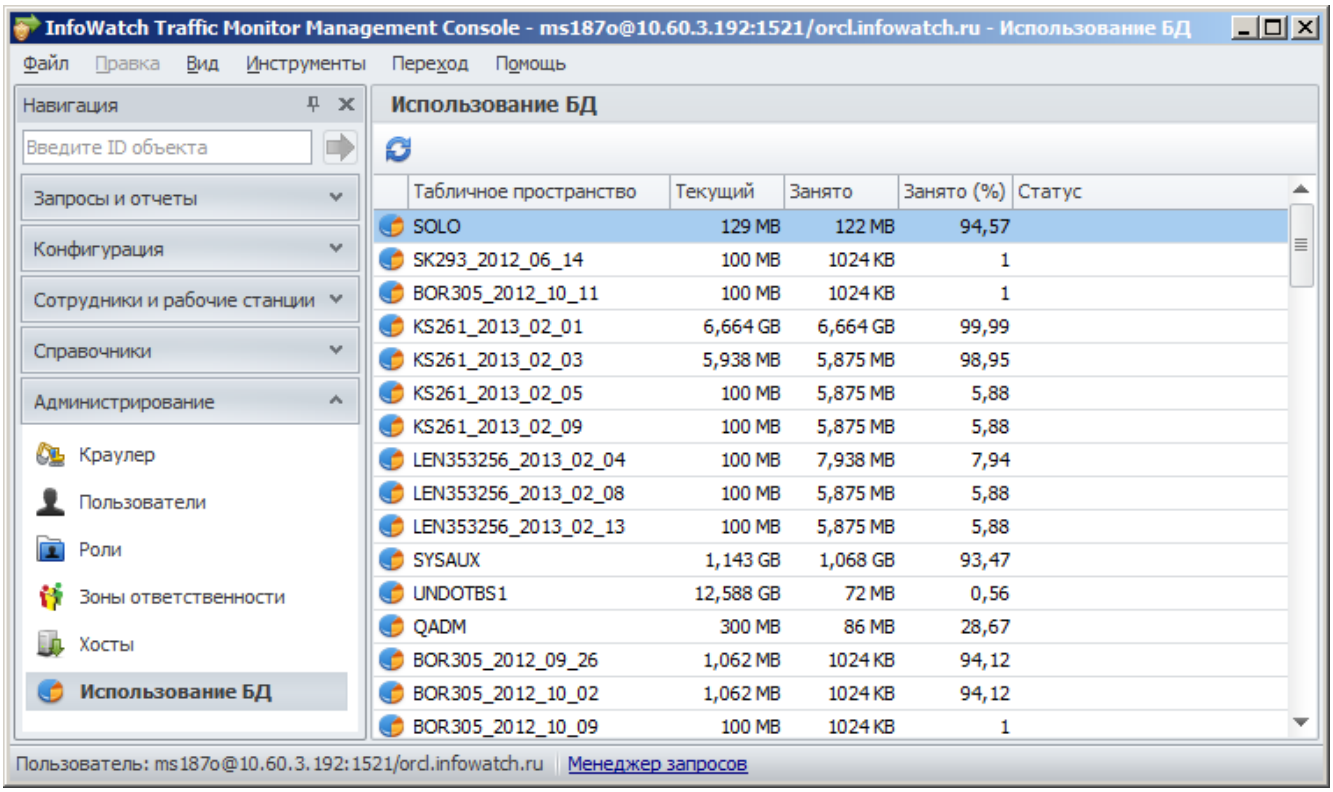
1. Перейдите к разделу **Хосты**.
2. На панели хостов выделите нужный хост.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку **Удалить** на панели инструментов.

4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

Когда связь с хостом будет восстановлена, он автоматически появится в списке хостов.

4.6 Просмотр статистики использования базы данных

Просмотреть сведения об использовании ежедневных табличных пространств базы данных можно в разделе **Использование БД** (область **Администрирование** на панели **Навигация**).



Статистика использования базы данных

В данном разделе выводятся следующие сведения о заполнении табличных пространств Oracle:

Атрибут	Значение
Табличное пространство	Имя табличного пространства
Текущий предел	Текущий размер, занимаемый табличным пространством на жестком диске
Занято	Текущий объем табличного пространства, занятый данными (в байтах). **Примечание:** единицы измерения табличного пространства определяются настройками и версией СУБД Oracle. За более подробной информацией вы можете обратиться к документации по СУБД Oracle

Атрибут	Значение
Занято (%)	Текущий объем табличного пространства, занятый данными. Рассчитывается в процентах от текущего предела
Статус	Статус ежедневного табличного пространства. Отображается только для ежедневных табличных пространств используемой схемы базы данных.

5 Справочник сотрудников и рабочих станций

Интеграция Системы с Active Directory облегчает пользователю работу с перехваченными объектами. Это реализовано за счет учета информации об отправителях и получателях (сотрудниках), а также рабочих станциях с помощью специальных справочников. Система обеспечивает:

- синхронизацию информации в справочниках с актуальной информацией, импортируемой из Active Directory;
- возможность указывать дополнительные параметры сотрудника: контакты и описание;
- возможность создавать группы сотрудников и рабочих станций, а также записи о сотрудниках средствами Traffic Monitor;
- отображение информации об отправителе, рабочей станции и получателях перехваченных объектов с использованием данных из справочников;
- возможность работы с данными отправителя, рабочей станции и получателей непосредственно из панели информации об объекте (подробнее об этой возможности см. "Обработка данных отправителя, получателя и рабочей станции").

Эта и другая информация о работе со справочниками приведена в следующих подразделах:

- Настройка подключения и синхронизации с Active Directory
- Справочник сотрудников
- Справочник рабочих станций
- Справочник групп
- Загрузка справочников на хост

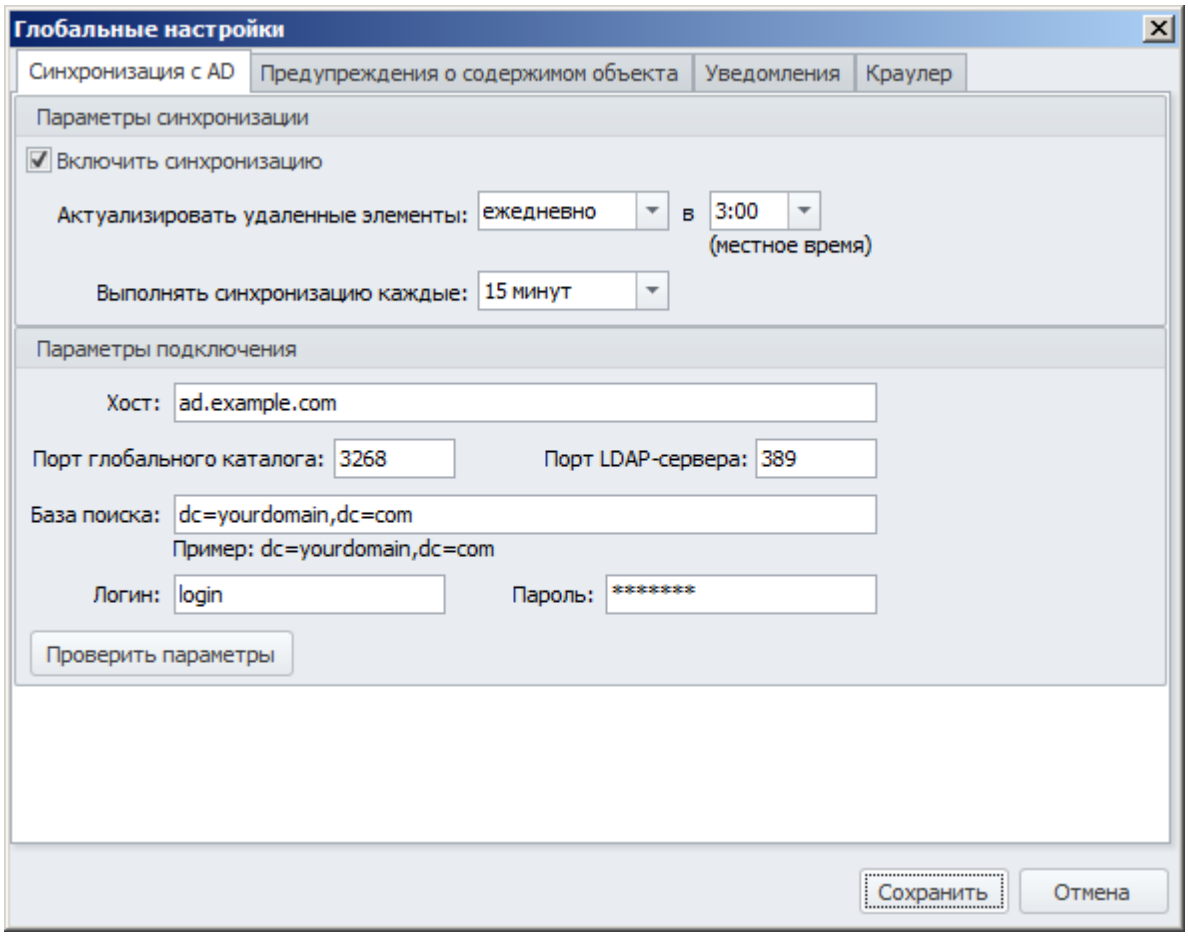
5.1 Настройка подключения и синхронизации с Active Directory

Для получения информации из Microsoft Active Directory, необходимо указать параметры подключения к серверу AD.

Чтобы настроить параметры подключения к Active Directory:

1. В главном меню выберите команду **Инструменты > Глобальные настройки**.

   На экран будет выведено диалоговое окно **Глобальные настройки**



Настройка подключения и синхронизации с Active Directory

2. На вкладке **Синхронизация с AD** укажите параметры подключения и синхронизации:

Параметр	**Описание**
Параметры синхронизации	
Включить синхронизацию	Установите флажок в данном поле, чтобы Система автоматически выполняла синхронизацию записей справочников с информацией из Active Directory, согласно указанному расписанию.

Параметр	Описание
Актуализировать удаленные элементы	Выберите периодичность, с которой должно выполняться получение информации об удаленных элементах Active Directory.
Выполнять синхронизацию каждые	Выберите периодичность, с которой должно выполняться получение информации о добавленных и измененных элементах Active Directory.
Параметры подключения	
Хост	Имя или IP-адрес сервера Microsoft Active Directory **Примечание**: Для использования имени сервера AD в настройке параметров подключения необходимо задать адрес DNS сервера Active Directory на сервере базы данных. О порядке настройки см. документ "InfoWatch Traffic Monitor. Руководство администратора"
Порт глобального каталога	Порт, по которому будут происходить поисковые запросы к службе каталогов Active Directory (по умолчанию – `3268`).
Порт LDAP-сервера	Порт, по которому будет происходить запросы поиска LDAP, в разделе каталога одного домена (по умолчанию – `389`).
База поиска	Базовый домен (LDAP base), в котором ведется поиск данных AD
Логин	Учетная запись пользователя, от имени которого выполняется подключение к Microsoft Active Directory. Запись указывается в формате `Domain\Login`
Пароль	Пароль пользователя, от имени которого выполняется подключение к Microsoft Active Directory

Чтобы убедиться в правильности введенных настроек подключения, нажмите кнопку **Проверить параметры**. Если сервер Active Directory доступен, отобразится сообщение об успешном прохождении проверки. В противном случае будет выведено сообщение, уведомляющее о неудачной проверке.

3. Нажмите кнопку **Сохранить**.

После изменения настроек подключения и синхронизации Система автоматически запускает синхронизацию, получая информацию о добавленных и удаленных элементах AD, а также актуализирует данные об удаленных элементах AD.

Статус синхронизации с AD и статус отправки каталога на хост отображаются в строке состояния для разделов **Сотрудники**, **Рабочие станции** и **Группы**. Ниже приведен перечень возможных состояний синхронизации и отправки каталога.

Пиктограмма	Описание статуса синхронизации	Описание статуса отправки каталога на хост
	Предыдущая синхронизация и актуализация удаленных элементов были успешно выполнены.	Предыдущая отправка справочников на хост была успешно выполнена.

Пиктограмма	Описание статуса синхронизации	Описание статуса отправки каталога на хост
	При наведении курсора на пиктограмму указываются дата и время следующих событий: • успешно завершенная синхронизация, • следующая синхронизация, • успешно завершенная актуализация удаленных элементов • следующая актуализация удаленных элементов.	При наведении курсора на пиктограмму указывается дата и время успешно завершенной отправки.
	Синхронизация выключена Актуализация удаленных элементов выключена	Хотя бы на одном хосте возникла ошибка отправки справочников. При наведении курсора на пиктограмму указываются адреса хостов, на которых возникли ошибки, и время, когда это произошло.
	Во время выполнения синхронизации (актуализации удаленных элементов) произошла ошибка При наведении курсора на пиктограмму указывается информация об ошибке, полученная от LDAP.	Все хосты недоступны (имеют статус *Неактивный*). Подробнее см. "Удаление хоста".
	Выполняется синхронизация (актуализация удаленных элементов)	Выполняется отправка справочников на хост



Важная информация!

Если на компьютере, где запущена Консоль управления, была изменена временная зона, то для корректного отображения времени синхронизации и актуализации, а также прежде чем изменять расписание синхронизации или актуализации, Консоль управления необходимо перезапустить.

5.2 Справочник сотрудников

Работа со справочником сотрудников ведется в разделе **Сотрудники** (область **Сотрудники и рабочие станции** на панели **Навигация**). При переходе к данному разделу рабочая область главного окна будет поделена на две части. Слева располагается список сотрудников, справа – область просмотра параметров выбранного сотрудника.

Информация о сотрудниках импортируется автоматически при синхронизации с Active Directory (см. " Настройка подключения и синхронизации с Active Directory").

Если вам необходимо учитывать информацию о сотруднике, данные о котором отсутствуют в Active Directory, вы можете создать для такого сотрудника запись средствами Traffic Monitor.

Записи, созданные средствами Traffic Monitor, в отличие от записей, импортированных из Active Directory, не

имеют ряда параметров: **Домен**, **Логин**, **E-mail** и **Группы AD**. Перечисленные параметры импортируются из AD и не могут быть отредактированы средствами Traffic Monitor.

Кроме того, для записей, импортированных из Active Directory, параметр **Статус** соответствует статусу сотрудника в AD и может принимать значения: *Активный*, *Заблокированный, Удаленный*. Для записей, созданных средствами Traffic Monitor, параметр **Статус** может принимать только значения *Активный* или *Удаленный* и изменяться пользователем (см. "Удаление и восстановление записи о сотруднике").

Важная информация!

При обработке перехваченных объектов учитывается информация только о сотрудниках со статусом *Активный* и *Заблокированный*.

В остальном работа с записями, созданными средствами Traffic Monitor, аналогична работе с записями, импортированными из Active Directory.

Более подробно порядок работы со справочником сотрудников описан в следующих разделах:

- Создание и редактирование записи о сотруднике
- Удаление и восстановление записи о сотруднике
- Просмотр и фильтрация записей о сотруднике

5.2.1 Создание и редактирование записи о сотруднике

Примечание

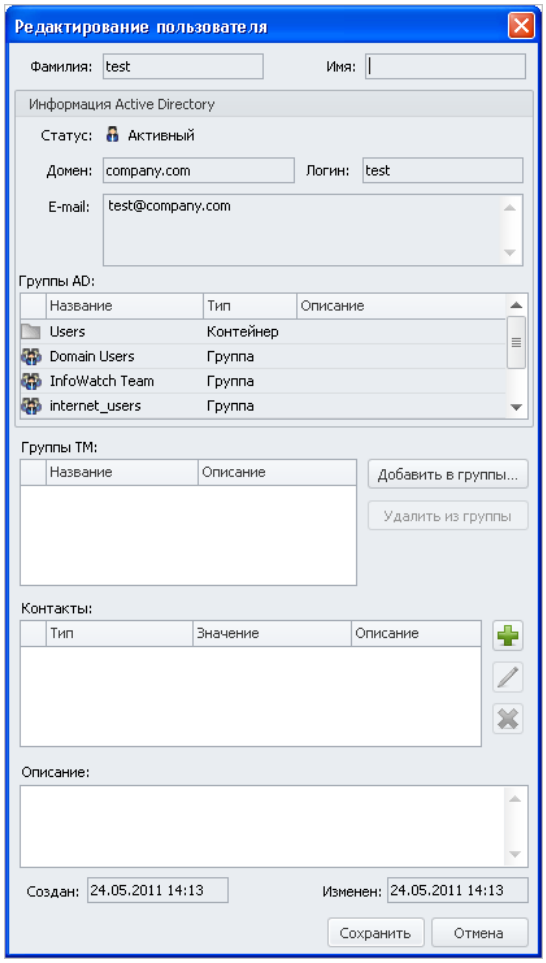
В справочнике сотрудников может быть не более 4194304 записей.

Чтобы создать или изменить запись о сотруднике:

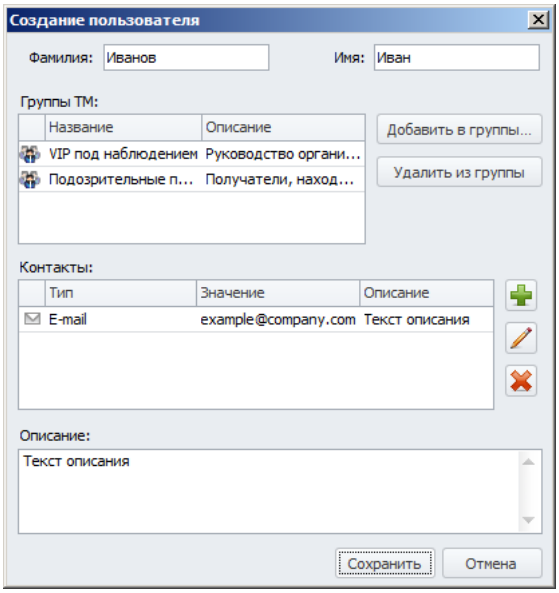
1. Перейдите к разделу **Сотрудники**.
2. Выполните необходимое действие:

Действие	Порядок выполнения
Создать запись о сотруднике	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Создать** • нажмите кнопку **Создать** на панели инструментов
Отредактировать запись о сотруднике	1. На панели **Сотрудники** выберите из списка запись о нужном сотруднике. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку **Изменить** на панели инструментов; • нажмите кнопку **Редактировать** в области просмотра параметров выбранного сотрудника; • дважды щелкните левой кнопкой мыши по выделенной строке.

На экран будет выведено диалоговое окно с параметрами сотрудника.



Редактирование записи о сотруднике, импортированной из Active Directory



Создание и редактирование записи о сотруднике, созданной средствами Traffic Monitor

3. Укажите параметры записи о сотруднике:

Параметр	Описание
Фамилия, **Имя**	Фамилия и имя сотрудника. Доступно для изменения только для записей, созданных средствами Traffic Monitor.
Группы TM	Группы Traffic Monitor, в которые включен сотрудник. • Чтобы добавить сотрудника в группу, нажмите **Добавить в группы**. В открывшемся диалоговом окне **Выбор групп** отметьте флажками группы, в которые вы хотите включить сотрудника. Чтобы установить или снять все флажки, используйте кнопки **Отметить все** и **Сбросить все**. После того, как вы выберете необходимые группы, нажмите **Сохранить**. • Чтобы удалить сотрудника из группы, выберите необходимую группу и нажмите **Удалить из группы**. **Примечание:** О порядке создания групп TM см. "Создание, просмотр и редактирование группы".
Контакты	Контактные данные (e-mail адрес или номер ICQ) сотрудника. • Чтобы добавить контакт, нажмите кнопку **Создать**. В открывшемся диалоговом окне укажите параметры контакта: – **Тип контакта**. Из раскрывающегося списка выберите тип контакта: *E-mail*, *ICQ*, *Skype* или *Phone*. – **Значение контакта**. E-mail адрес, или номер ICQ, Skype или телефона, соответственно параметру, выбранному на предыдущем шаге. – **Описание**. Дополнительные сведения о контакте. После того, как параметры будут указаны, нажмите **ОК**. • Чтобы изменить контакт, выберите его в списке и нажмите кнопку **Изменить**. Отредактируйте параметры как описано выше и нажмите **ОК**. • Чтобы удалить контакт, выберите его в списке и нажмите кнопку **Удалить**.
Описание	Дополнительные сведения о сотруднике

4. После того, как параметры сотрудника будут успешно определены, нажмите кнопку **Сохранить**.

Важная информация!

Данные нового сотрудника или изменения в этих данных будут использоваться Системой только после того, как будет выполнена загрузка справочников на хосты (см. "Загрузка справочников на хост").

Примечание

Запись о сотруднике также можно изменить при работе с группой, в которую она входит. Для этого в разделе **Группы** выберите название нужной группы и на панели выбранной группы выделите строку с нужной записью. Затем выполните одно из следующих действий:

- в главном меню выберите команду **Правка > Члены группы TM > Изменить**;

- нажмите кнопку  **Изменить** на панели членов группы
- дважды щелкните левой кнопкой мыши по выделенной записи о сотруднике.

Окно редактирования записи о сотруднике и порядок изменения параметров аналогичны вышеописанному.

5.2.2 Удаление и восстановление записи о сотруднике

Запись о сотруднике, созданную средствами Traffic Monitor, можно удалить.

Чтобы удалить запись о сотруднике:

1. Перейдите к разделу **Сотрудники**.
2. В списке сотрудников выделите нужную запись.
3. Выполните одно из следующих действий:
   - щелкните на записи правой кнопкой мыши и в раскрывшемся меню выберите  **Удалить**;
   - в главном меню выберите команду **Правка > Удалить**;
   - воспользуйтесь кнопкой  **Удалить**, расположенной на панели инструментов;
   - нажмите кнопку **Удалить** в области просмотра параметров выбранного сотрудника.

В результате сотрудник получит статус *Удаленный* и, после отправки справочника на хосты (см. "Загрузка справочников на хост"), информация о нём перестанет использоваться Системой.

Если потребуется вновь использовать удаленную запись о сотруднике, вы можете её восстановить.

Чтобы восстановить запись о сотруднике:

1. Перейдите к разделу **Сотрудники**.

    **Примечание**

   Для просмотра удаленных записей, на панели **Сотрудник** должен быть выбран фильтр **Все** или **Удаленные**.

2. В списке сотрудников выделите нужную запись.
3. Выполните одно из следующих действий:
   - щелкните на записи правой кнопкой мыши и в раскрывшемся меню выберите  **Восстановить**;
   - в главном меню выберите команду **Правка > Восстановить**;
   - воспользуйтесь кнопкой  **Восстановить**, расположенной на панели инструментов;
   - нажмите кнопку **Восстановить** в области просмотра параметров выбранного сотрудника.

В результате сотрудник получит статус *Активный* и, после отправки справочника на хосты (см. "Загрузка справочников на хост"), информация о нём вновь будет использоваться Системой.

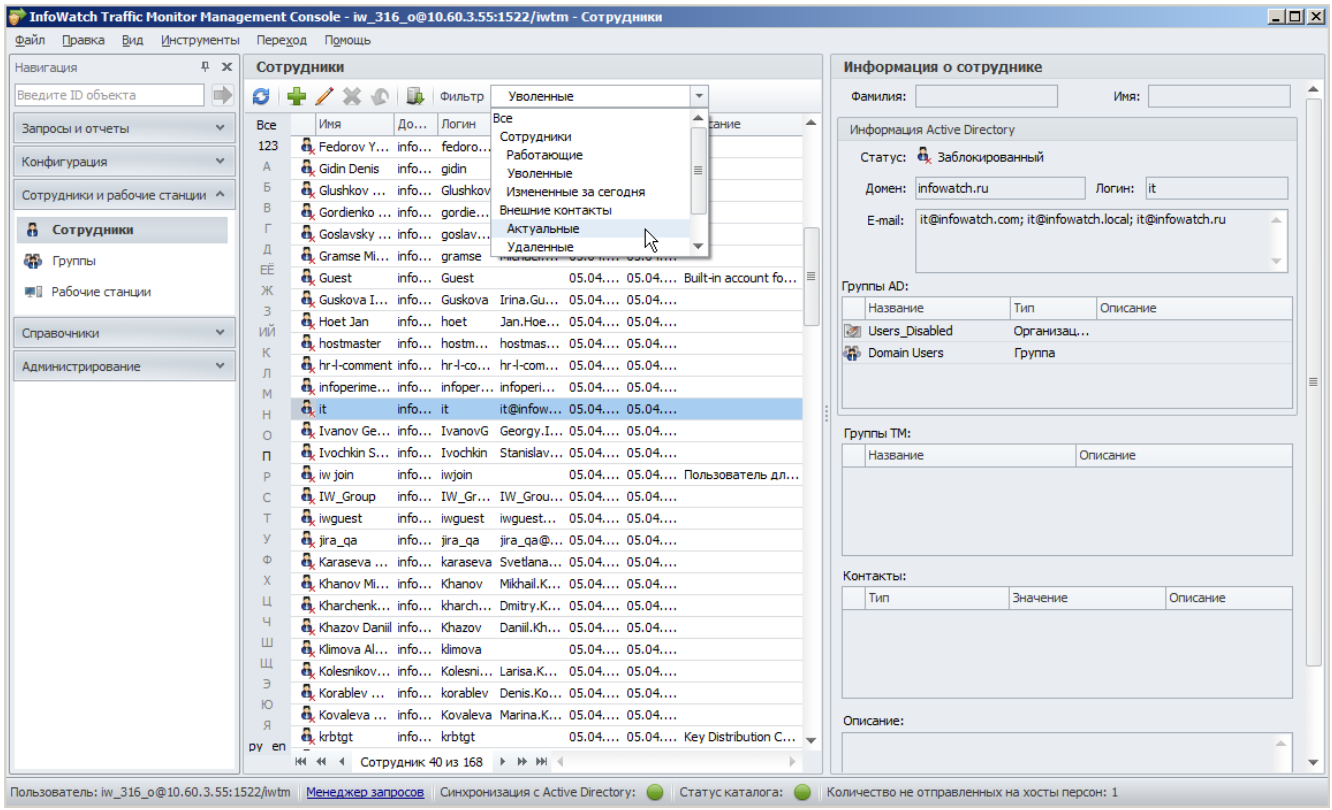
5.2.3 Просмотр и фильтрация записей о сотруднике

Для того чтобы отсеивать записи о сотрудниках, просматривать которые нет необходимости, применяется фильтрация. По умолчанию выбран тип фильтрации "Все", и Система отображает записи обо всех сотрудниках. Вы можете применить также другие типы фильтрации:

- **Сотрудники** - список сотрудников, полученный из Active Directory. Список включает пункты:
  - **Работающие** - список штатных сотрудников организации;
  - **Уволенные** - список бывших сотрудников организации;
  - **Измененные за сегодня** - список сотрудников, информация о которых была изменена, но не отправлена на хосты (см. "Загрузка спавочников на хост").
- **Внешние контакты** - список сотрудников, созданных средствами Traffic Monitor Management Console. Список включает пункты:
  - **Актуальные** - список штатных сотрудников организации;
  - **Удаленные** - список бывших сотрудников организации;
  - **Измененные за сегодня** - список сотрудников, информация о которых была изменена, но не отправлена на хосты (см. "Загрузка спавочников на хост").
- или **Еще не отправленные на хосты** - список сотрудников, измененная или добавленная информация о которых не была отправлена на хосты (см. "Загрузка спавочников на хост").

Чтобы отфильтровать записи,

на панели инструментов панели **Сотрудники** выберите из раскрывающегося списка нужный параметр фильтрации.



Фильтрация записей о сотрудниках

5.3 Справочник рабочих станций

Работа со списком рабочих станций ведется в разделе **Рабочие станции** (область **Сотрудники и рабочие станции** на панели **Навигация**). При переходе к данному разделу рабочая область главного окна будет поделена на две части. Слева располагается список рабочих станция, справа – область просмотра параметров выбранной рабочей станции.

Информация о рабочих станциях импортируется автоматически при синхронизации с Active Directory (см. " Настройка подключения и синхронизации с Active Directory").

Важная информация!

При обработке перехваченных объектов учитывается информация только о рабочих станциях со статусом *Активный* и *Заблокированный*.

Более подробно порядок работы со справочником рабочих станций описан в следующих разделах:

- Редактирование записи о рабочей станции
- Просмотр и фильтрация записей о рабочей станции

5.3.1 Редактирование записи о рабочей станции

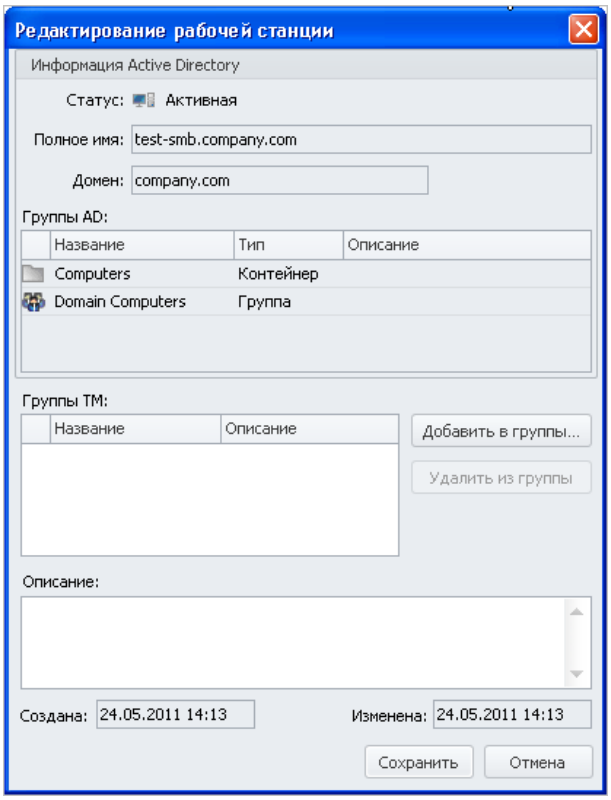
Примечание

В справочнике рабочих станций может быть не более 4194304 записей.

Чтобы изменить запись о рабочей станции:

1. Перейдите к разделу **Рабочие станции**.
2. Выберите из списка запись о нужной рабочей станции.
3. Выполните одно из следующих действий:
   - дважды щелкните левой кнопкой мыши по выделенной рабочей станции;
   - щелкните на записи правой кнопкой мыши и в раскрывшемся меню выберите **Изменить**;
   - в главном меню выберите команду **Правка > Изменить**;
   - нажмите кнопку **Изменить** на панели категорий;
   - нажмите кнопку **Редактировать** в области просмотра параметров выбранной рабочей станции.

   На экран будет выведено окно с параметрами рабочей станции.



Параметры рабочей станции

4. Отредактируйте необходимые параметры рабочей станции:

Параметр	Описание
Группы TM	Группы Traffic Monitor, в которые включена рабочая станция. • Чтобы добавить рабочую станцию в группу, нажмите **Добавить в группы**. В открывшемся диалоговом окне **Выбор групп** отметьте флажками группы, в которые вы хотите включить рабочую станцию. Чтобы установить или снять все флажки, используйте кнопки **Отметить все** и **Сбросить все**. После того, как вы выберете необходимые группы, нажмите **Сохранить**. • Чтобы удалить рабочую станцию из группы, выберите необходимую группу и нажмите **Удалить из группы**. **Примечание:** О порядке создания групп TM см. "Создание, просмотр и редактирование группы"
Описание	Дополнительные сведения о рабочей станции. Импортируются из Active Directory. **Важная информация!** Если в справочнике Active Directory описание рабочей станции было изменено, то при следующей синхронизации (см. "Настройка подключения и синхронизации с Active Directory") значение поля **Описание** также будет заменено на обновлённое

5. После того, как параметры рабочей станции будут успешно определены, нажмите кнопку **Сохранить**.

Важная информация!

Изменения параметров рабочей станции будут использоваться Системой только после того, как будет выполнена загрузка справочников на хосты (см. "Загрузка справочников на хост").

Примечание

Запись о рабочей станции также можно изменить при работе с группой, в которую она входит. Для этого в разделе **Группы** выберите название нужной группы и на панели выбранной группы выделите строку с нужной записью. Затем выполните одно из следующих действий:

- в главном меню выберите команду **Правка > Члены группы ТМ > Изменить**;
- нажмите кнопку **Изменить** на панели членов группы
- дважды щелкните левой кнопкой мыши по выделенной записи о сотруднике.

Окно редактирования рабочей станции и порядок изменения параметров аналогичны вышеописанному.

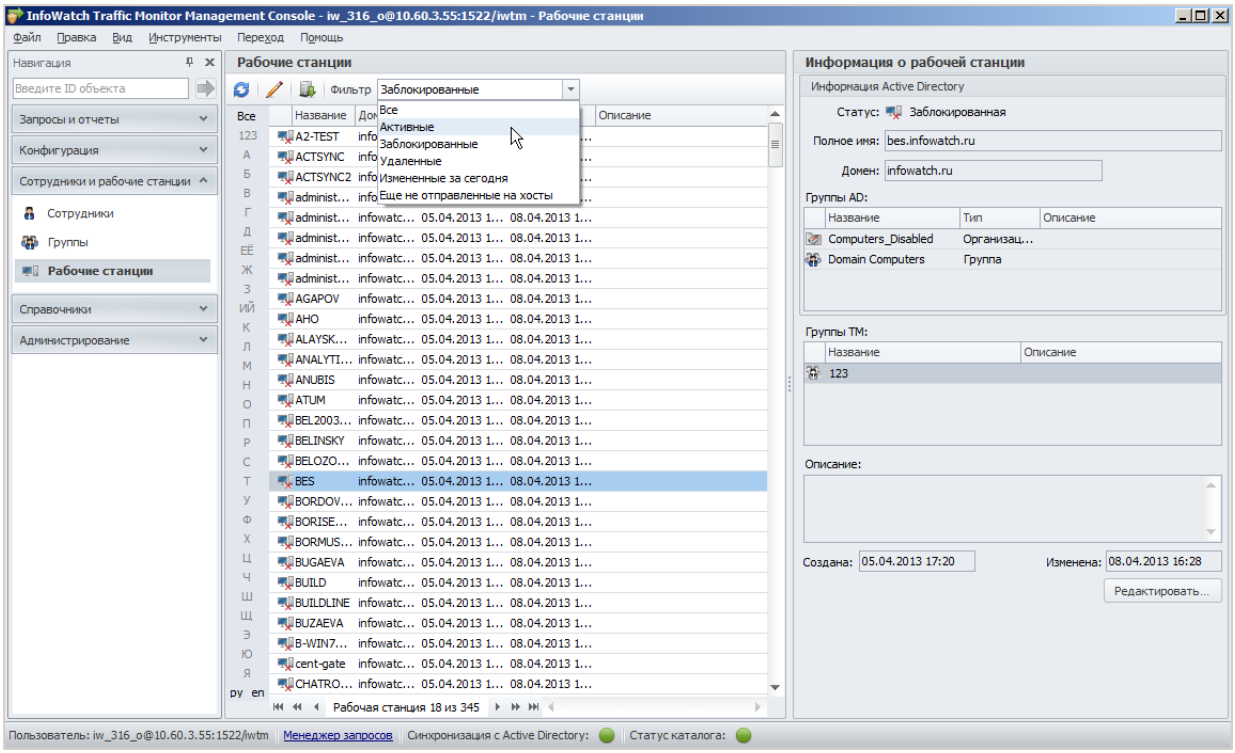
5.3.2 Просмотр и фильтрация записей о рабочей станции

Для того чтобы отсеивать записи о рабочих станциях, просматривать которые нет необходимости, применяется фильтрация. По умолчанию выбран тип фильтрации "Все", и Система отображает записи обо всех рабочих станциях. Вы можете применить также другие типы фильтрации:

- **Активные** - список рабочих станций, используемых пользователями;
- **Заблокированные** - список рабочих станций, временно недоступных для пользователей;
- **Удаленные** - список рабочих станций, недоступных для пользователей;
- **Измененные за сегодня** - список рабочих станций, информация о которых была изменена, но не отправлена на хосты (см. "Загрузка спавочников на хост");
- или **Еще не отправленные на хосты** - список рабочих станций, информация о создании или изменении которых не была отправлена на хосты (см. "Загрузка спавочников на хост").

Чтобы отфильтровать записи,

на панели инструментов панели **Рабочие станции** выберите из раскрывающегося списка нужный параметр фильтрации.



Фильтрация записей о рабочих станциях

5.4 Справочник групп

Группы Active Directory объединяют записи о сотрудниках и рабочих станциях.

В Системе предусмотрено два типа групп:

- **Группы AD** – группы, контейнеры или организационные единицы, импортированные автоматически при синхронизации с Active Directory (см. "Настройка подключения и синхронизации с Active Directory "). Для таких групп пользователь может изменить только их код и описание.
- **Группы TM** – группы, созданные средствами Traffic Monitor. Пользователи могут создавать и изменять их параметры, а также редактировать состав членов этих групп.

Работа с группами сотрудников и рабочих станций ведется в разделе **Группы** (область **Сотрудники и рабочие станции** на панели **Навигация**). При переходе к данному разделу рабочая область главного окна будет поделена на две части: **Группы AD и Группы TM**. В свою очередь, каждая из этих областей также поделена на две части: слева располагается список групп, справа – список членов выбранной группы.

Примечание

Просмотр и фильтрация групп происходит аналогично просмотру и фильтрации записей сотрудников и рабочих станций (см. "Просмотр и фильтрация записей о сотруднике" и "Просмотр и фильтрация записей о рабочей станции").

Более подробно порядок работы со справочником групп описан в следующих разделах:

- Создание, просмотр и редактирование группы
- Добавление члена группы TM
- Удаление члена группы TM

- Удаление и восстановление группы ТМ

5.4.1 Создание, просмотр и редактирование группы

Примечание

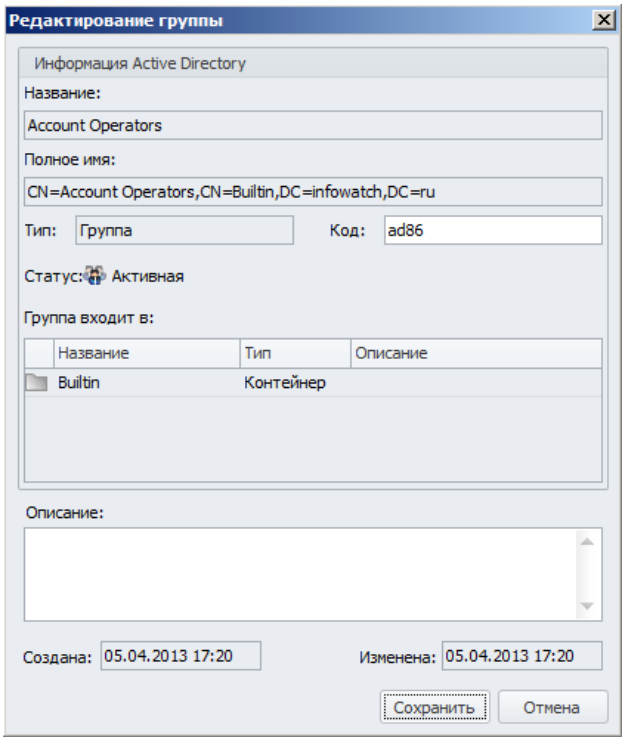
В справочнике групп может быть не более 4194304 записей.

Чтобы создать или изменить группу:

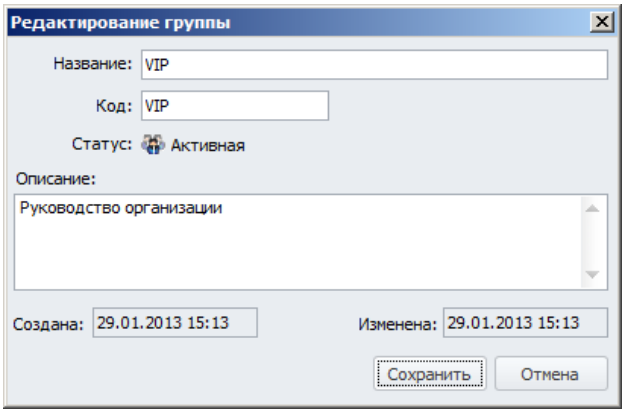
1. Перейдите к разделу **Группы**.
2. Выполните необходимое действие:

Действие	Порядок выполнения
Создать группу ТМ	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Группы ТМ > Создать** • нажмите кнопку **Создать** на панели **Группы ТМ**
Отредактировать группу	1. На панели **Группы AD** или **Группы ТМ** выберите из списка название нужной группы. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Группы ТМ / Группы AD > Изменить**; • нажмите кнопку **Изменить** на панели **Группы AD** или **Группы ТМ**; • щелкните по выделенной строке правой кнопкой мыши и в раскрывшемся меню выберите **Изменить**; • дважды щелкните левой кнопкой мыши по выделенной строке.

На экран будет выведено диалоговое окно с параметрами группы.



Просмотр и редактирование группы AD



Настройка параметров группы TM

3. Укажите параметры группы:

Параметр	Описание
Название	Наименование группы. Должно быть уникальным. Доступно для изменения только для групп TM
Код	Кодовое название группы, которое будет использоваться при составлении сценария. Может состоять из букв латинского алфавита, цифр и символа подчеркивания; должно начинаться с буквы. Код должен быть уникальным
Описание	Дополнительные сведения о группе

4. После того, как параметры группы будут успешно определены, нажмите кнопку **Сохранить**.

Новые группы ТМ должны быть наполнены требуемыми сотрудниками и рабочими станциями: см. " Добавление члена группы ТМ".

Важная информация!

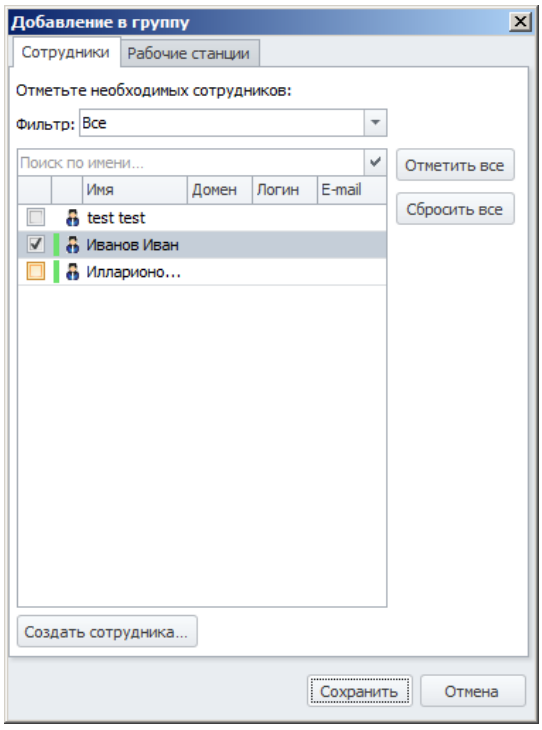
Данные новой группы или изменения в этих данных смогут использоваться Системой только после того, как будет выполнена загрузка справочников на хосты (см. "Загрузка справочников на хост").

5.4.2 Добавление члена группы ТМ

Чтобы добавить в группу ТМ сотрудника или рабочую станцию:

1. Перейдите к разделу **Группы**.
2. На панели **Группы ТМ** выберите из списка название нужной группы.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Члены группы ТМ > Добавить**;
   - нажмите кнопку **Создать** на панели выбранной группы.

   На экран будет выведено диалоговое окно **Добавление в группу**.



Добавление члена группы ТМ

В данном окне есть две вкладки:

- **Сотрудники** – список сотрудников, которых вы можете добавить в группу;
- **Рабочие станции** – список рабочих станций, которые вы можете добавить в группу.

Вы можете ограничить список отображаемых сотрудников / рабочих станций, выбрав требуемый тип из раскрывающегося списка в поле **Фильтр**.

Также доступен поиск по имени сотрудника / рабочей станции. Чтобы выполнить поиск, укажите имя или часть имени в соответствующем поле и нажмите кнопку .

На вкладке **Сотрудники** вы можете добавить запись о сотруднике, нажав кнопку **Создать сотрудник**а. Подробно о порядке создания записи сотрудника см. "Создание и редактирование записи о сотруднике".

4. В списке сотрудников / рабочих станций отметьте флажками элементы, которые вы хотите добавить в группу.

   Чтобы установить или снять все флажки, используйте кнопки **Отметить все** и **Сбросить все**.

5. Нажмите кнопку **Сохранить**.

5.4.3 Удаление члена группы ТМ

Чтобы удалить сотрудника или рабочую станцию из группы ТМ:

1. Перейдите к разделу **Группы**.
2. На панели **Группы ТМ** выберите из списка название нужной группы
3. На панели выбранной группы выделите строку с нужной записью.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Члены группы ТМ > Удалить**;
   - нажмите кнопку **Удалить из группы ТМ** на панели членов группы.

5.4.4 Удаление и восстановление группы ТМ

Чтобы удалить группу ТМ:

1. Перейдите к разделу **Группы**.
2. На панели **Группы ТМ** выберите из списка название нужной группы.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Группы ТМ > Удалить**;
   - нажмите кнопку **Удалить** на панели **Группы ТМ**.

В результате группа ТМ получит статус *Удаленная* и, после отправки справочника на хосты (см. "Загрузка справочников на хост"), информация о ней перестанет использоваться Системой.

Если потребуется вновь использовать удаленную группу ТМ, вы можете её восстановить.

Чтобы восстановить запись о группе ТМ:

1. Перейдите к разделу **Группы**.

> **Примечание**
>
> Для просмотра удаленных групп, на панели **Группы ТМ** должен быть выбран фильтр **Все** или

Удаленные.

2. На панели **Группы ТМ** выберите из списка название нужной группы.

3. Выполните одно из следующих действий:
   - щелкните на записи правой кнопкой мыши и в раскрывшемся меню выберите **Восстановить**;
   - в главном меню выберите команду **Правка > Группы ТМ > Восстановить**;
   - воспользуйтесь кнопкой **Восстановить**, расположенной на панели **Группы ТМ**.

В результате группа ТМ получит статус *Актуальная* и, после отправки справочника на хосты (см. "Загрузка справочников на хост"), информация о ней вновь будет использоваться Системой.

5.5 Загрузка справочников на хост

Информация, импортированная из Active Directory, а также введенная пользователем Консоли управления, сохраняется в базе данных. Чтобы эта информация могла использоваться при анализе объектов или для отображения данных об отправителях и получателях, необходимо выполнить загрузку справочников Active Directory на хост.

Загрузка справочников выполняется, в частности, при автоматической синхронизации с AD (см. "Настройка подключения и синхронизации с Active Directory"), а также при загрузке всей конфигурации на хост (см. " Загрузка конфигурации на хосты"). Однако, для более быстрой актуализации информации можно выполнять загрузку справочников на хост отдельно.

Вы можете запустить загрузку на хост из любого раздела **Сотрудники и рабочие станции** (**Сотрудники**, **Рабочие станции** или **Группы**). В результате на сервере Traffic Monitor будет актуализированы данные всех справочников Active Directory.

Чтобы загрузить справочники на хост,

нажмите кнопку **Отправить каталог на хосты** на панели инструментов.

Статус загрузки справочников на хост и (в случае успешной загрузки) время последней отправки отображаются в строке состояния для любого раздела **Сотрудники и рабочие станции** (**Сотрудники**, **Рабочие станции** или **Группы**).

6 Краулер

Подсистема Crawler системы InfoWatch Traffic Monitor позволяет выполнять проверку файлов, находящихся в корпоративной сети, на предмет нарушения корпоративных политик безопасности. Таким образом InfoWatch Crawler позволяет контролировать файловые ресурсы компании для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.

InfoWatch Crawler обеспечивает выполнение следующих функций:

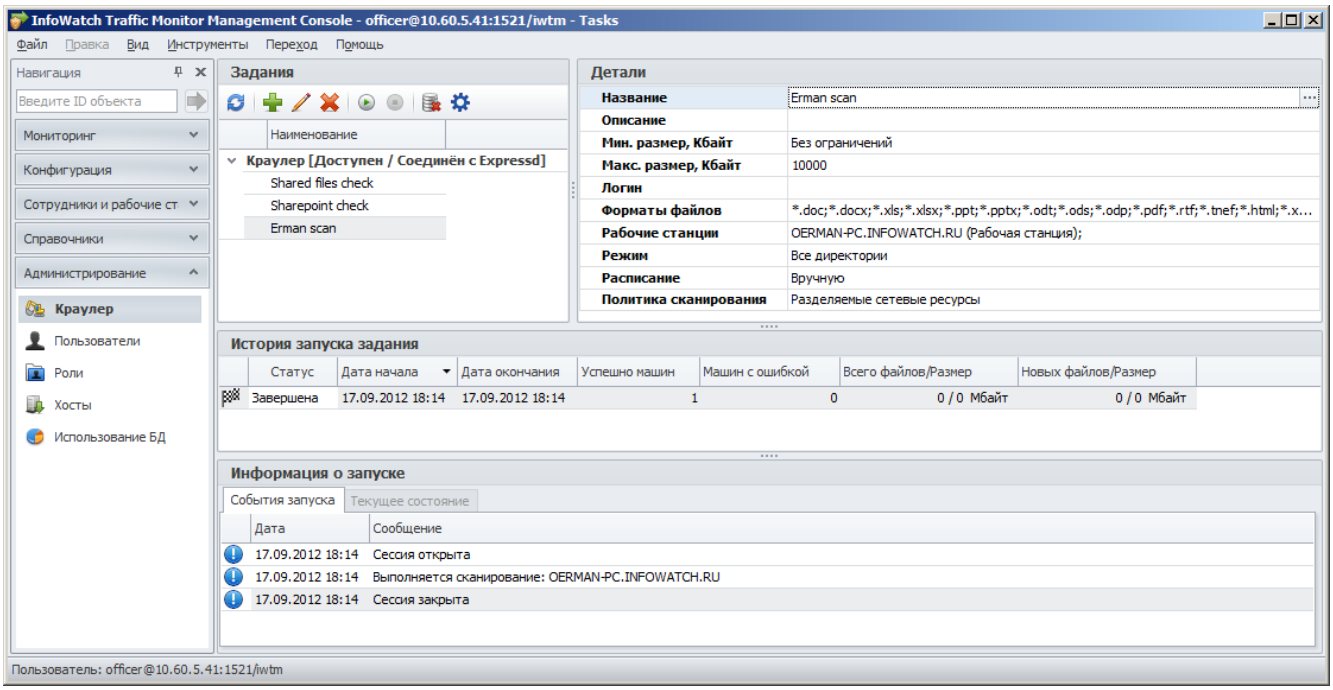
- Сканирование сетевых папок, открытых для удалённого доступа по протоколу SMB.

- Сканирование локальных дисков рабочих станций, работающих под управлением ОС Windows.
- Сканирование файлового хранилища SharePoint. Выполняет проверку документов, хранящихся в БД Microsoft SharePoint 2007. При этом рассматриваются только текущие версии файлов: история изменений не исследуется.
- Пользовательская настройка параметров сканирования: скорость загрузки файлов со сканируемых ресурсов и параметры файловой очереди для загрузки объектов на сервер Traffic Monitor.
- Создание задания сканирования с возможностью указывать:
  - перечень папок и сетевых узлов, на которых будет выполняться сканирование;
  - маски обрабатываемых файлов;
  - ограничения по размеру обрабатываемых файлов;
  - расписание выполнения задания (также возможен ручной запуск).
- Отбор только новых и измененных файлов: ранее обработанные файлы повторно на сервер InfoWatch Traffic Monitor не отправляются.
- Передача файлов для анализа на сервер InfoWatch Traffic Monitor с заданными пользователем параметрами передачи.
- Сохранение файлов согласно настройкам политики (по умолчанию – инцидентов: файлов, признанных потенциальным нарушением действующей политики безопасности).
- Предоставление результатов сканирования в Консоли управления: с помощью запросов на просмотр объектов и в виде отчётов, в том числе предустановленных.

InfoWatch Crawler не выполняет удаления, перемещения, переименования, шифрования или каких-либо иных действий над файлами – даже в тех случаях, когда они признаны потенциальным нарушением. Происходит только информирование офицера безопасности о наличии инцидента: из Консоли управления InfoWatch Traffic Monitor доступен просмотр файлов, признанных потенциальным нарушением, с указанием подробной информации об их расположении и пользователях, имеющих к нему доступ.

Работа с Crawler ведется в Консоли управления InfoWatch Traffic Monitor, в разделе Краулер (группа **Администрирование** на панели **Навигация**). В данном разделе рабочая область разделена на несколько частей:

- **Задания** – перечень заданий сканирования, зарегистрированных в системе. В названии сканера краулера указан его статус. Так, статус [**Доступен**/**Соединен с Expressd**] свидетельствует о полной работоспособности сканера. Если в статусах присутствует:
  - **Не доступен** – служба сканера `Crawler.Scanner` не запущена, необходимо проверить работу компьютера, где он установлен.
  - **Нет связи с ТМ** – не обнаружена работа процесса `iw_expressd`.
- **Детали** – подробная информация о задании, выбранном пользователем в перечне заданий.
- **История запуска задания** – список сессий выполнения задания, выбранного пользователем. Отображается статус задания; дата и время начала и окончания сессии и общая статистика (количество обработанных рабочих станций и файлов).
- **Информация о запуске** – журнал сессии, выбранной в истории запусков. На вкладке **«События запуска»** отображается информация о событиях, возникших в ходе сканирования. На вкладке **«Текущее состояние»** отображается, какие ресурсы, папки и файлы сканируются в настоящий момент в текущей сессии (сессия со статусом **Работает**).



Более подробно работа с Crawler описана в следующих разделах:

- Схема работы Crawler
- Настройка соединения Консоли управления с сервером
- Настройка параметров работы сканера Crawler
- Создание и редактирование задания на сканирование
- Удаление задания на сканирование
- Выполнение и остановка задания
- Очистка базы хешей

6.1 Схема работы Crawler

InfoWatch Crawler работает как один из перехватчиков Traffic Monitor.

В работе Crawler участвуют следующие компоненты системы InfoWatch Traffic Monitor:

- **Crawler** – программный пакет, обеспечивающий выполнение основных функций. Реализован в виде двух служб Windows:
  - `InfoWatch.Crawler.Scanner` – выполняет сканирование сетевых папок и файловых хранилищ согласно заданным пользователем параметрам;
  - `InfoWatch.Crawler.Server` – управляет службой сканирования и обеспечивает связь с Консолью управления Traffic Monitor.
- **База данных** – Crawler использует схему БД InfoWatch Traffic Monitor для хранения как объектов, признанных потенциальным нарушением, так и информации о заданиях сканирования.
- **Консоль управления InfoWatch Traffic Monitor**: Элементы управления Crawler представлены в специальном разделе **Краулер**.

Файлы, полученные в результате работы Crawler, вместе с информацией об их расположении, пользователях, имеющих к нему доступ, задании сканирования, в результате которого они были получены и другие сопутствующие данные, рассматриваются в системе InfoWatch Traffic Monitor как объекты от перехватчика Crawler Monitor.

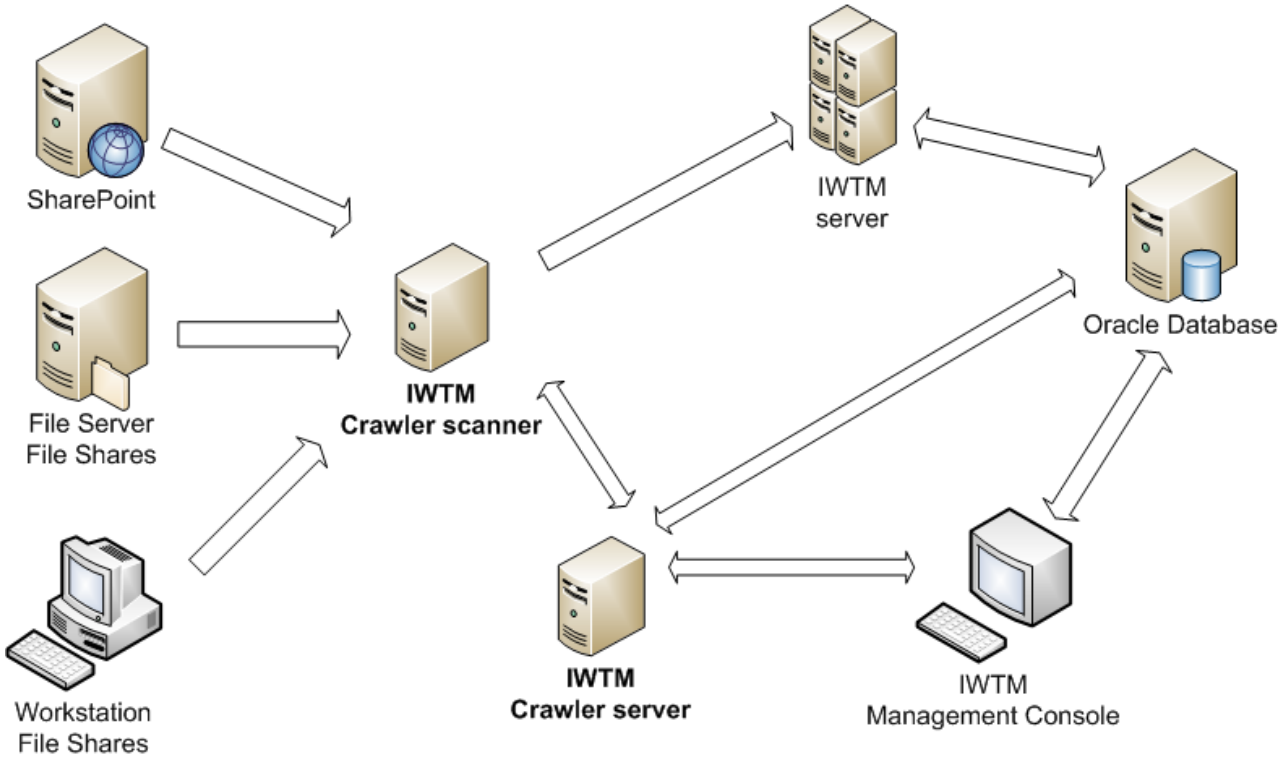


Схема работы InfoWatch Crawler

InfoWatch Crawler выполняет сканирование в следующем порядке:

1. Рабочие станции, группы рабочих станций, файловые сервера или файловые хранилища, перечисленные в задании сканирования (см. "Создание и редактирование задания на сканирование "), проверяются на наличие данных, доступных для учётной записи, от имени которой запущено это задание сканирования.
2. Для каждого найденного файла:
   - выполняется проверка, удовлетворяет ли файл условиям поиска (маска файла, размеры)
   - файл временно копируется в рабочую директорию сканера
   - определяется, был ли ранее обработан файл: если файл уже передавался в систему и с тех пор не изменялся, его временная копия удаляется.
3. Если файл удовлетворяет условиям поиска и не обрабатывался ранее, то ему присваиваются дополнительные атрибуты:
   - владелец файла;
   - список учетных записей, имеющих доступ на чтение данного файла.
4. Файл отправляется для анализа на сервер InfoWatch Traffic Monitor, где обрабатывается в соответствии с действующим сценарием обработки объектов (см. "Настройка сценария анализа объектов").

Если на сервере Traffic Monitor действуют настройки по умолчанию:

- объект Crawler, признанный потенциальным нарушением (вынесен вердикт ***Forbidden***), сохраняется в базе данных, при этом копия файла является вложением к объекту (подробнее см. "Просмотр общей информации по объекту")

- объект Crawler, не являющийся потенциальным нарушением (вынесен вердикт ***Allowed***), удаляется.

6.2 Настройка соединения Консоли управления с сервером Crawler

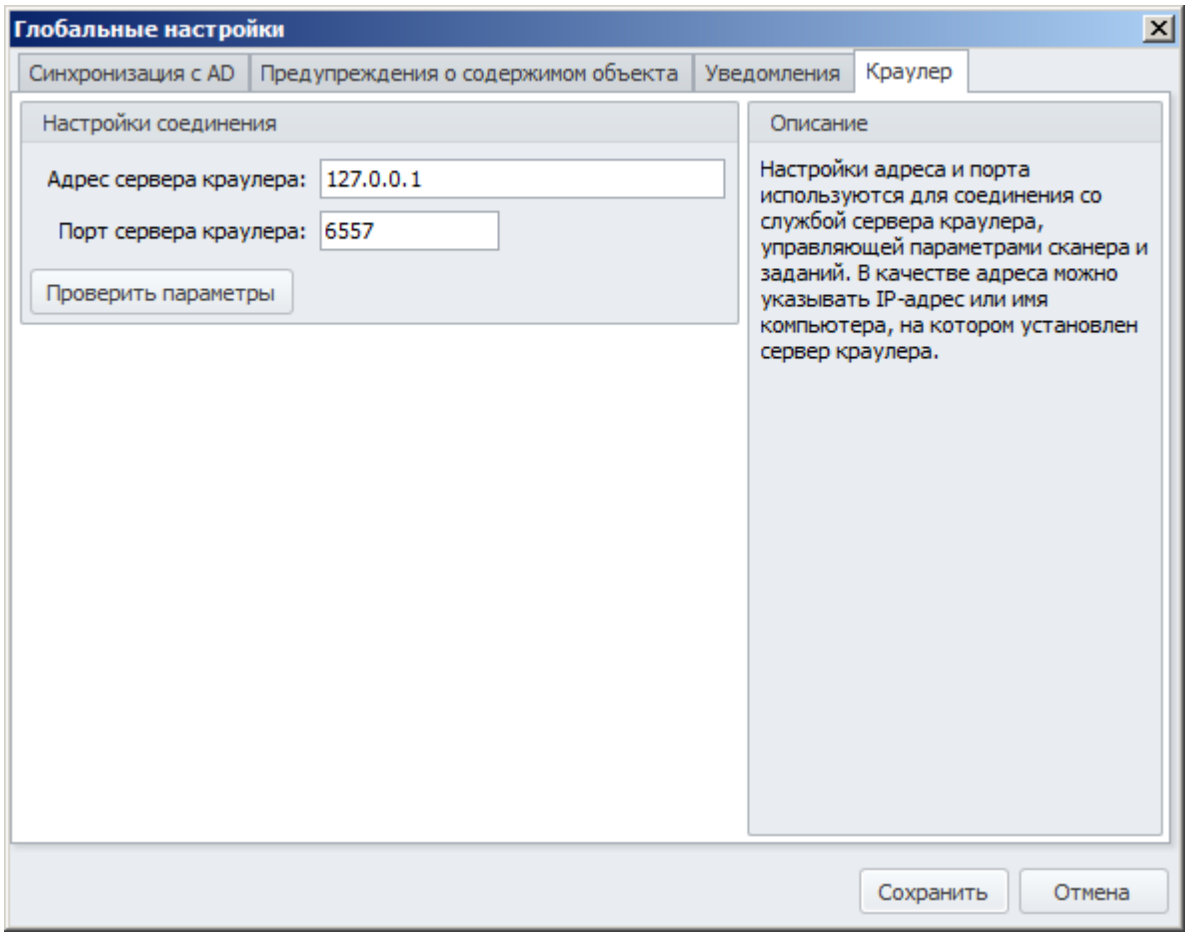
Чтобы настроить соединение Консоли управления с сервером Crawler:

1. В главном меню Консоли управления выберите команду **Инструменты > Глобальные настройки**.
2. В диалоговом окне Глобальные настройки откройте вкладку Краулер и укажите параметры соединения с сервером Crawler:
   - **Адрес сервера краулера**. Вы можете указывать как IP-адрес, так и имя компьютера, на котором установлен сервер Crawler.

     Важная информация!

     Настройки соединения распространяются на все экземпляры Консоли управления, работающие в Системе. Поэтому если предполагается, что с подсистемой Crawler будет работать несколько Консолей управления, то в данной настройке должен быть указан актуальный адрес сервера, на котором установлен сервер Crawler (а не localhost 127.0.0.1).
   - **Порт сервера краулера**
3. Проверьте корректность указанных настроек, нажав **Проверить параметры**.



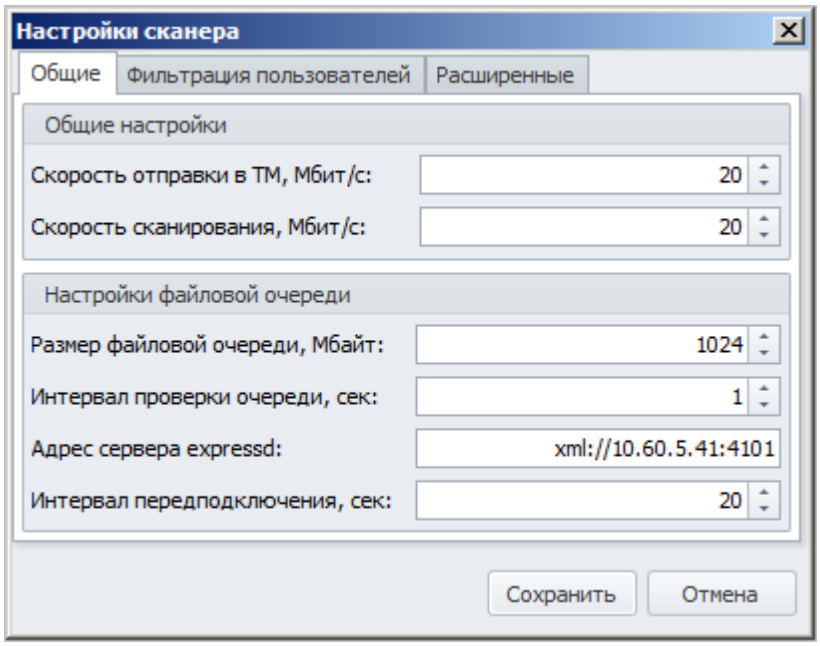
4. Нажмите **Сохранить**.

6.3 Настройка параметров работы сканера Crawler

Чтобы настроить общие параметры работы сканера Crawler:

1. В Консоли управления перейдите к разделу **Краулер**.
2. Нажмите кнопку **Настройки сканера** на панели инструментов.

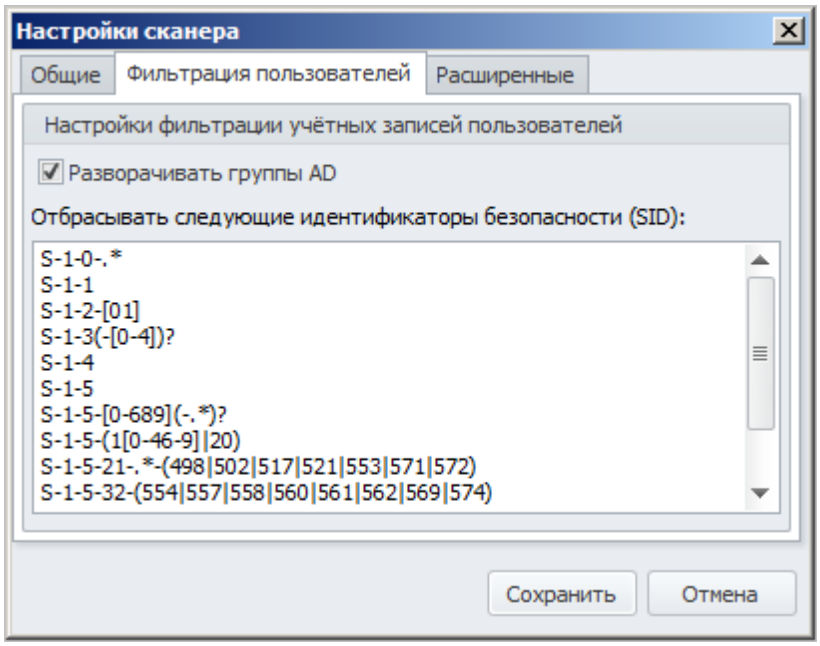
   На экран будет выведено диалоговое окно для настройки параметров работы сканера Crawler.



3. Укажите общие настройки:

- **Скорость отправки в ТМ** – максимальная скорость загрузки файлов на сервер Traffic Monitor, Мбит/с
- **Скорость сканирования** – максимальная скорость загрузки файлов с проверяемых ресурсов во временное хранилище, Мбит/с
- **Размер файловой очереди** – максимальный размер очереди, куда помещаются найденные файлы перед отправкой на сервер Traffic Monitor, Мбайт
- **Интервал проверки очереди** – с указанным интервалом (в секундах) сервер Crawler будет проверять, есть ли какие-либо объекты в очереди для загрузки на сервер Traffic Monitor. Если в очереди есть хотя бы один объект, будет выполняться передача этого объекта на сервер Traffic Monitor.
- **Адрес сервера expressd** – Строка соединения с сервером InfoWatch Traffic Monitor, на котором работает процесс `iw_expressd`. Должен быть задан в формате `xml://IP_address:port`.
- **Интервал переподключения** – с указанным интервалом (в секундах) сервер Crawler будет пытаться восстановить подключение к серверу Traffic Monitor в случае потери этого подключения.

4. При необходимости, на вкладке **Фильтрация пользователей** настройте общие правила фильтрации учетных записей пользователей при отображении информации об объектах Crawler в Консоли управления:



- **Разворачивать группы AD**. Если флажок установлен, то при отображении информации об объекте, перехваченном Crawler (см. "Просмотр информации по объектам"), группы пользователей AD, имеющих права на доступ к файлу (параметр **Получатели**) будут показываться развёрнутыми, в виде ссылок на карточки сотрудников.

  Если флажок не установлен, то группы AD будут отображаться в виде записей вида `имя_группы@домен`. Если группа локальная, то вместо домена будет отображаться имя рабочей станции, с которой получен объект.

- **Отбрасывать следующие идентификаторы безопасности (SID)**. В данном поле перечислены стандартные SID служебных записей. При необходимости, вы можете добавить в этот список собственные SID и задавать маски, используя регулярные выражения.

  Пример записи:

  `S-1-5-21-.*-(498|502|517|527)`

  Данная запись означает, что при отображении информации об объекте в Консоли управления не будет отображаться информация о том, что данный файл доступен учетным записям с любыми SID, начинающимися со строки "S-1-5-21-", имеющими в середине 0 или больше любых букв, цифр, и др. символов, и оканчивающихся на "-498", или "-502", или "-517", или "-527".

  Подходящие SID:

  `S-1-5-21-12345-ABCDEF-498`

  `S-1-5-21--527`

  Неподходящие SID:

  `1S-1-5-21-12345-ABCDEF-498` - начинается не с "S-1-5-21-"

  `S-1-5-21-527` - начинается с "S-1-5-21-", но заканчивается на "527", а не на "-527"

  `S-1-5-21-ABCDEF-100` - не заканчивается на "-498", или "-502", или "-517", или "-527".

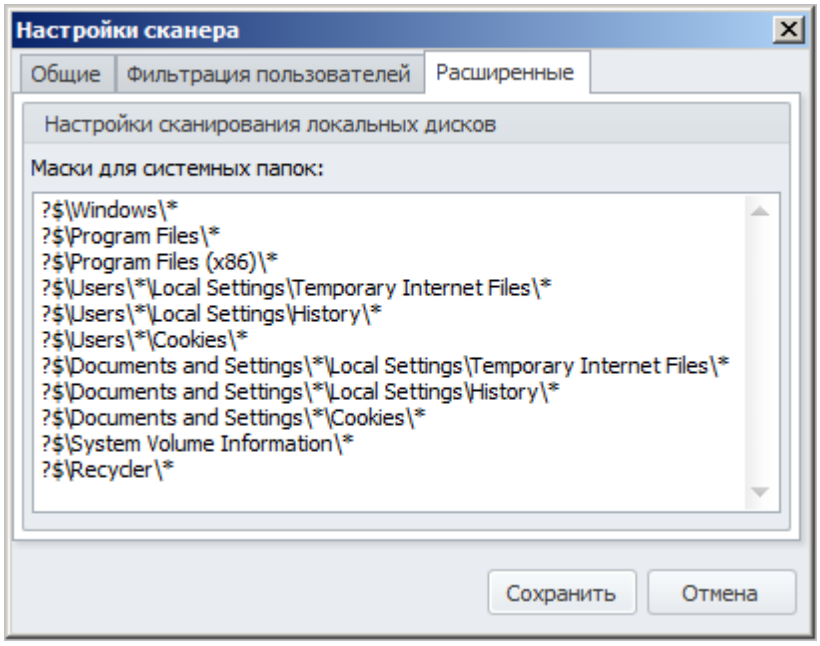
`S-1-5-21-ABCDEF-502-` - не заканчивается на "-498", или "-502", или "-517", или "-527".

`S-1-6-21-ABCDEF-502` - начинается не с "S-1-5-21-".

Примечание

Формат языка регулярных выражений можно изучить тут: http://msdn.microsoft.com/ru-ru/library/az24scfc(v=vs.100).aspx.

5. На вкладке **Расширенные** перечислены маски папок, которые будут проигнорированы при сканировании локальных дисков рабочих станций, если при создании задания отмечена настройка **Исключить системные папки** (подробнее см. п. 3.3.4 на стр. 25):



При необходимости, удалите или добавьте папки.

Примечание

Каждая папка должна быть задана на отдельной строке.

Для замены одного или нескольких символов можно использовать символы «?» или «*» соответственно.

Если при указании имени папки в конце имени не было указано «*», то при сохранении настроек к строке автоматически добавляется «*».

6. По окончании настройки нажмите **Сохранить**.

После этого система должна отобразить сообщение об успешном обновлении конфигурации сканера.

6.4 Создание и редактирование задания на сканирование

InfoWatch Crawler выполняет следующие типы сканирования:

- **Сканирование открытых сетевых папок**: политика сканирования «Разделяемые сетевые

ресурсы». Выполняет сканирование папок, открытых для удалённого доступа по протоколу SMB. Для выполнения задания необходима учётная запись, обладающая правом чтения сетевых папок на целевых рабочих станциях.

Подробнее о порядке создания и редактирования задания данного типа см. "Сканирование разделяемых сетевых ресурсов".

- **Сканирование локальных дисков рабочих станций**: политика сканирования «Локальные диски рабочих станций». Выполняет сканирование локальных дисков рабочих станций, работающих под управлением ОС Windows. Для выполнения задания необходима учётная запись, обладающая правами администратора на целевых рабочих станциях.

  Подробнее о порядке создания и редактирования задания данного типа см. "Сканирование локальных дисков рабочих станций".

- **Сканирование файлового хранилища SharePoint**: политика сканирования «Файловое хранилище: SharePoint 2007», выполняет проверку документов, хранящихся в БД Microsoft SharePoint 2007. При этом рассматриваются только текущие версии файлов: история изменений не исследуется. Для выполнения задания необходима учётная запись, обладающая правами на чтение данных из проверяемого файлового хранилища

  Подробнее о порядке создания и редактирования задания данного типа см. "Сканирование файлового хранилища SharePoint".

Запущенное задание (имеет статус ***Работает***) или редактируемое в другой Консоли управления, не доступно для изменения или удаления.

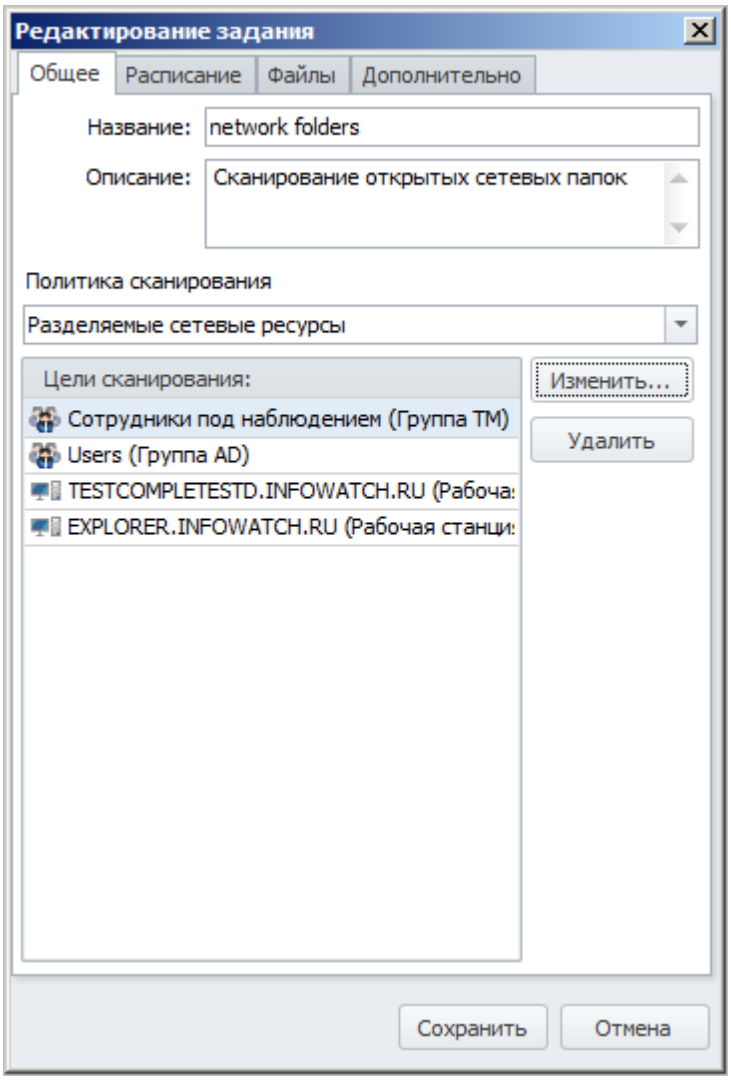
6.4.1 Сканирование разделяемых сетевых ресурсов

Задача сканирования разделяемых сетевых ресурсов обеспечивает проверку открытых сетевых папок. Для выполнения задания необходима учётная запись, обладающая правом чтения сетевых папок на целевых рабочих станциях (параметры учётной записи задаются на вкладке **Дополнительно**).

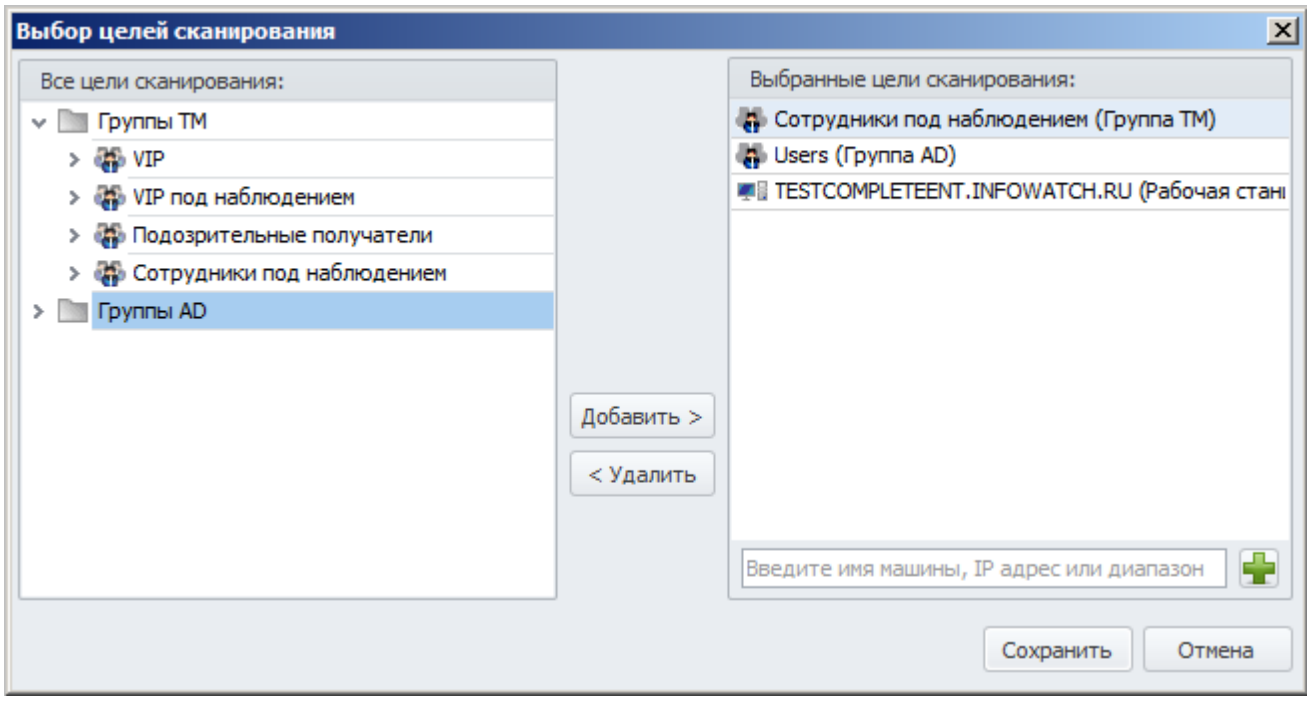
Чтобы создать или изменить задание на сканирование разделяемых сетевых ресурсов:

1. В Консоли управления перейдите к разделу **Краулер**.
2. Выполните одно из следующих действий:
   - чтобы добавить задание, нажмите кнопку **Создать** на панели инструментов
   - чтобы изменить имеющееся задание, выберите его в списке и нажмите кнопку **Изменить** на панели инструментов.

   На экран будет выведено диалоговое окно для настройки задания.
3. На вкладке **Общее** укажите общие параметры задания:
   - **Название** – имя задания.
   - **Описание** – необязательное поле с произвольным текстом
   - **Политика сканирования** – из раскрывающегося списка выберите **Разделяемые сетевые ресурсы**.



4. В области **Цели сканирования** определите список рабочих станций и групп, подлежащих сканированию. Чтобы добавить рабочие станции или группы в список, нажмите **Изменить**; в раскрывшемся диалоговом окне выбирайте группы и рабочие станции и переносите их в список, нажимая **Добавить**.



Важная информация!

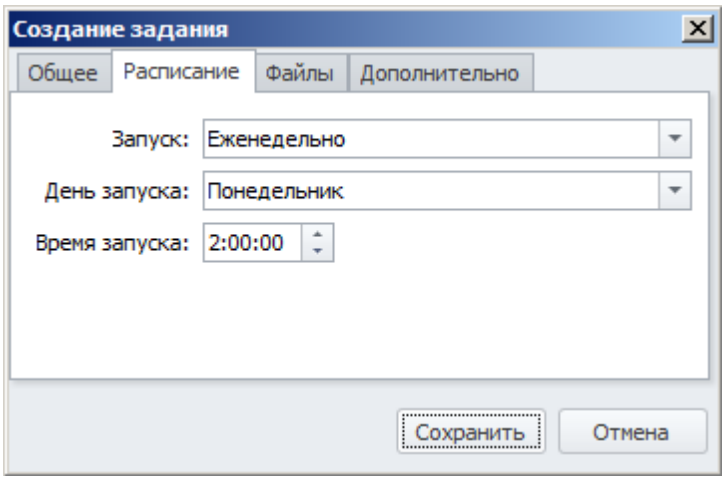
Если каталоги AD имеют большой размер, то первое открытие окна выбора рабочих станций может занять некоторое время (несколько минут).

Вы также можете задать FQDN-имя или IP-адрес рабочей станции в поле ввода под списком, затем нажать . Чтобы задать диапазон IP-адресов, укажите его через дефис (-) или косую черту (/).

После того, как список рабочих станций определен, нажмите **Сохранить**.

Чтобы удалить рабочие станции или группы из списка, в диалоговом окне настройки задания выделите их и нажмите **Удалить**.

5. На вкладке **Расписание** настройте расписание автоматического запуска задания.



Выберите один из вариантов запуска задания:

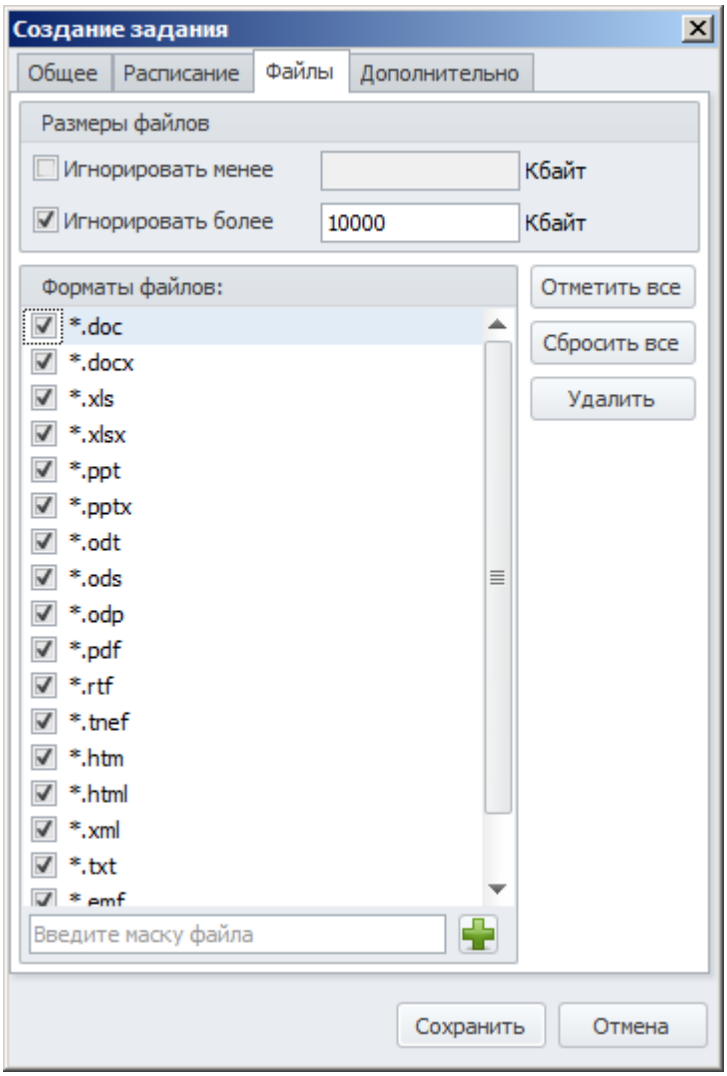
- **Еженедельно** – укажите день недели и время автоматического запуска
- **Ежедневно** – укажите день недели и время автоматического запуска
- **Вручную** – в этом случае запуск задания может осуществляться только способом, описанным в разделе "Выполнение и остановка задания".

Важная информация!

Если при наступлении времени запуска предыдущая сессия запуска этого задания ещё не завершила свою работу, то задание повторно запущено не будет.

По умолчанию задание запускается только вручную, по команде пользователя.

6. На вкладке **Файлы** определите размеры и форматы файлов, которые нужно отправлять на анализ.



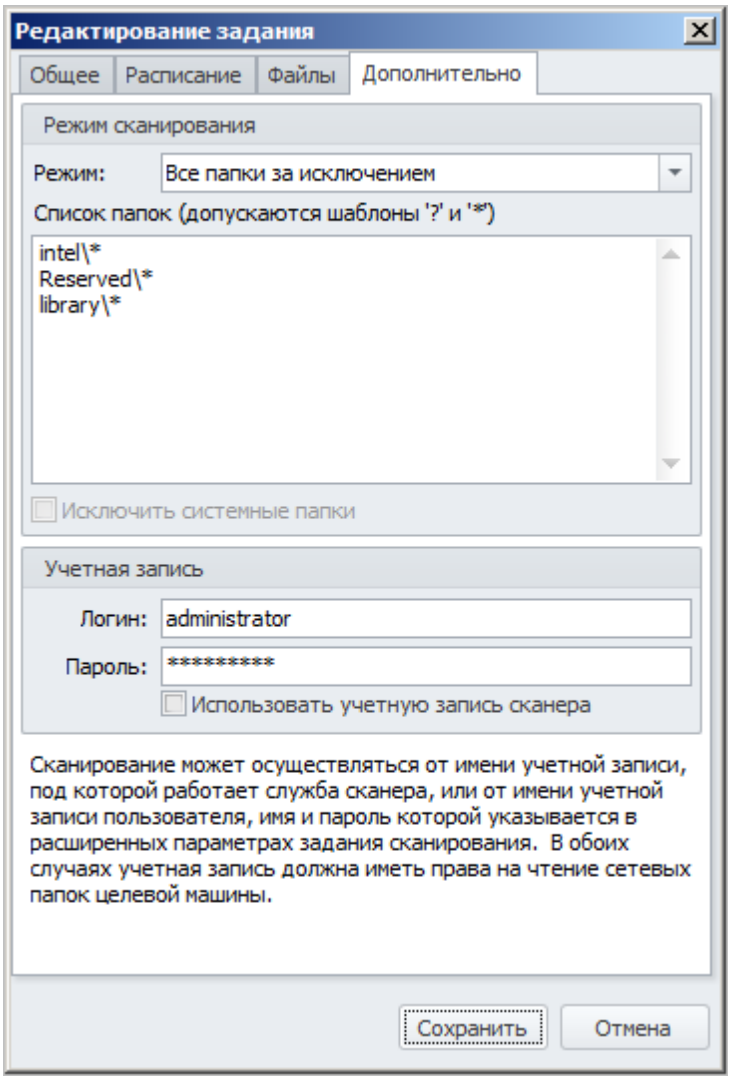
Определите:

- **Размеры файлов** – нижнюю и верхнюю границу размера файлов, которые нужно отправлять на анализ
- **Форматы файлов** – выберите маски файлов из списка предустановленных или добавляйте собственные маски, вводя их в поле ввода внизу списка и нажимая .

Важная информация!

Использование маски *.* может значительно снизить скорость сканирования и существенно увеличить нагрузку на сервер Traffic Monitor.

7. На вкладке **Дополнительно** вы можете ограничить цели сканирования, задав список сканируемых папок, а также указать параметры учётной записи, от имени которой будет запускаться задание. Сканирование разделяемых сетевых ресурсов должно осуществляться от имени учётной записи, обладающей правами на чтение сетевых папок целевых рабочих станций.



Укажите необходимый режим сканирования папок:

- Все папки;
- Все папки за исключением;
- Только перечисленные папки.

При задании списка папок:

- Каждая папка должна быть задана на отдельной строке.
- Для замены одного или нескольких символов можно использовать символы «?» или «*» соответственно.
- Если при указании имени папки в конце имени не было указано «*», то при сохранении настроек к строке автоматически добавляется «*».
- Использование символа «:» не допускается: чтобы задать путь к директории, используйте маски вида «Windows*».

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

Сохранённое задание может выполняться либо автоматически согласно заданному расписанию (если оно было определено), либо вручную, как описано в разделе "Выполнение задания".

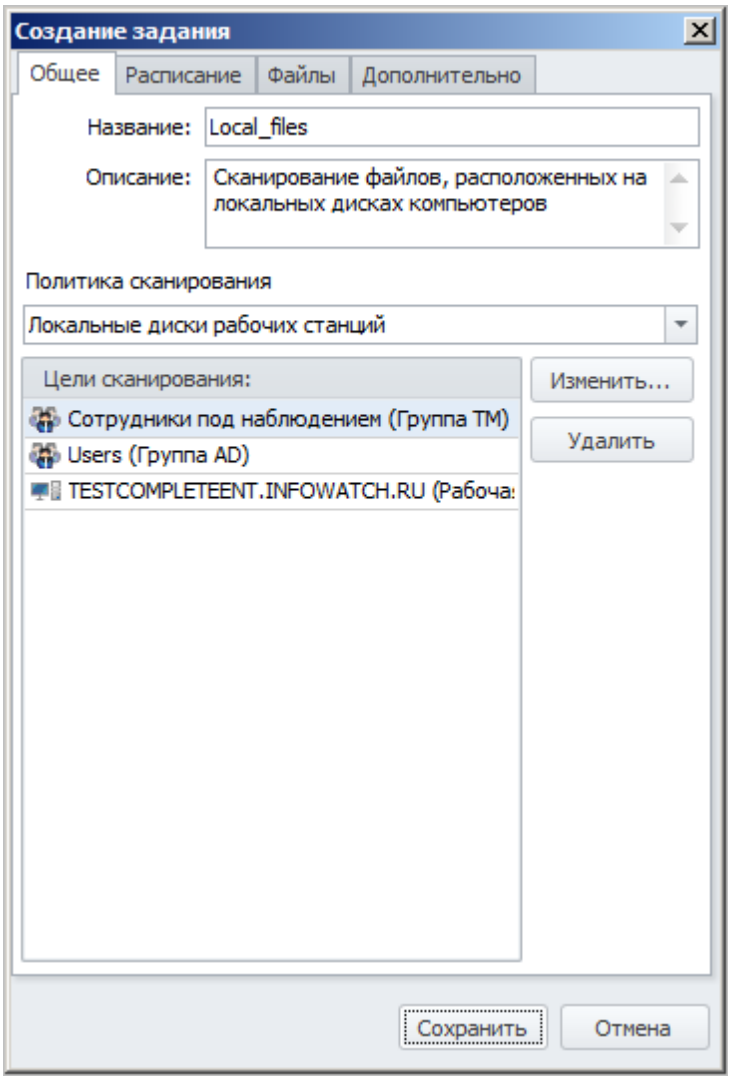
6.4.2 Сканирование локальных дисков рабочих станций

Задача сканирования локальных дисков рабочих станций обеспечивает проверку файлов, расположенных на локальных дисках компьютеров, работающих под управлением ОС Windows. Для выполнения задания необходима учётная запись, обладающая правами администратора на целевых рабочих станциях (параметры учётной записи задаются на вкладке **Дополнительно**).

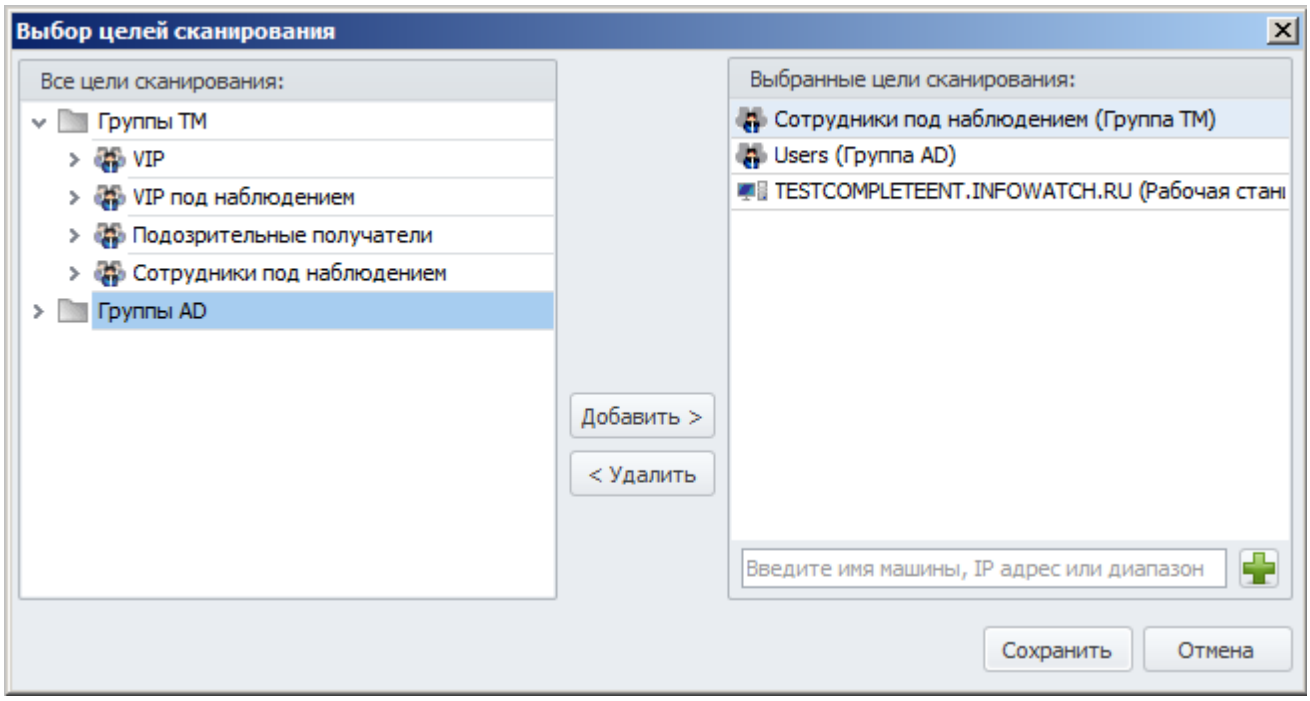
Чтобы создать или изменить задание на сканирование локальных дисков рабочих станций:

1. В Консоли управления перейдите к разделу **Краулер**.
2. Выполните одно из следующих действий:
   - чтобы добавить задание, нажмите кнопку  **Создать** на панели инструментов
   - чтобы изменить имеющееся задание, выберите его в списке и нажмите кнопку  **Изменить** на панели инструментов.

   На экран будет выведено диалоговое окно для настройки задания.
3. На вкладке **Общее** укажите общие параметры задания:
   - **Название** – имя задания.
   - **Описание** – необязательное поле с произвольным текстом
   - **Политика сканирования** – из раскрывающегося списка выберите **Локальные диски рабочих станций**



4. В области **Цели сканирования** определите список рабочих станций и групп, подлежащих сканированию. Чтобы добавить рабочие станции или группы в список, нажмите **Изменить**; в раскрывшемся диалоговом окне выбирайте группы и рабочие станции и переносите их в список, нажимая **Добавить**.



Важная информация!

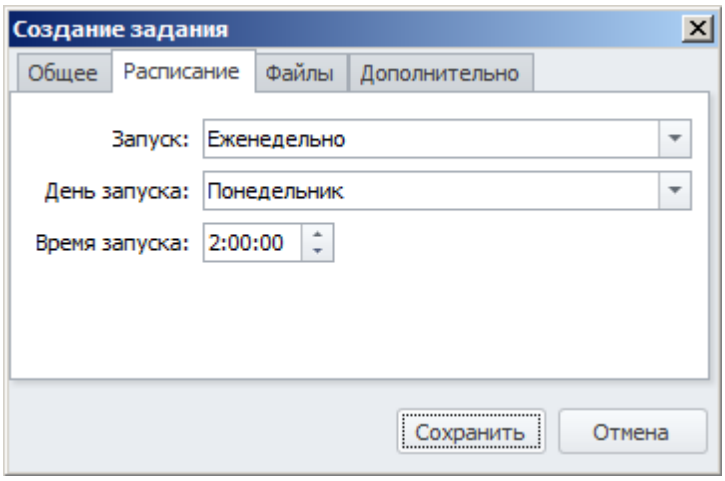
Если каталоги AD имеют большой размер, то первое открытие окна выбора рабочих станций может занять некоторое время (несколько минут).

Вы также можете задать FQDN-имя или IP-адрес рабочей станции в поле ввода под списком, затем нажать . Чтобы задать диапазон IP-адресов, укажите его через дефис (-) или косую черту (/).

После того, как список рабочих станций определен, нажмите **Сохранить**.

Чтобы удалить рабочие станции или группы из списка, в диалоговом окне настройки задания выделите их и нажмите **Удалить**.

5. На вкладке **Расписание** настройте расписание автоматического запуска задания.



Выберите один из вариантов запуска задания:

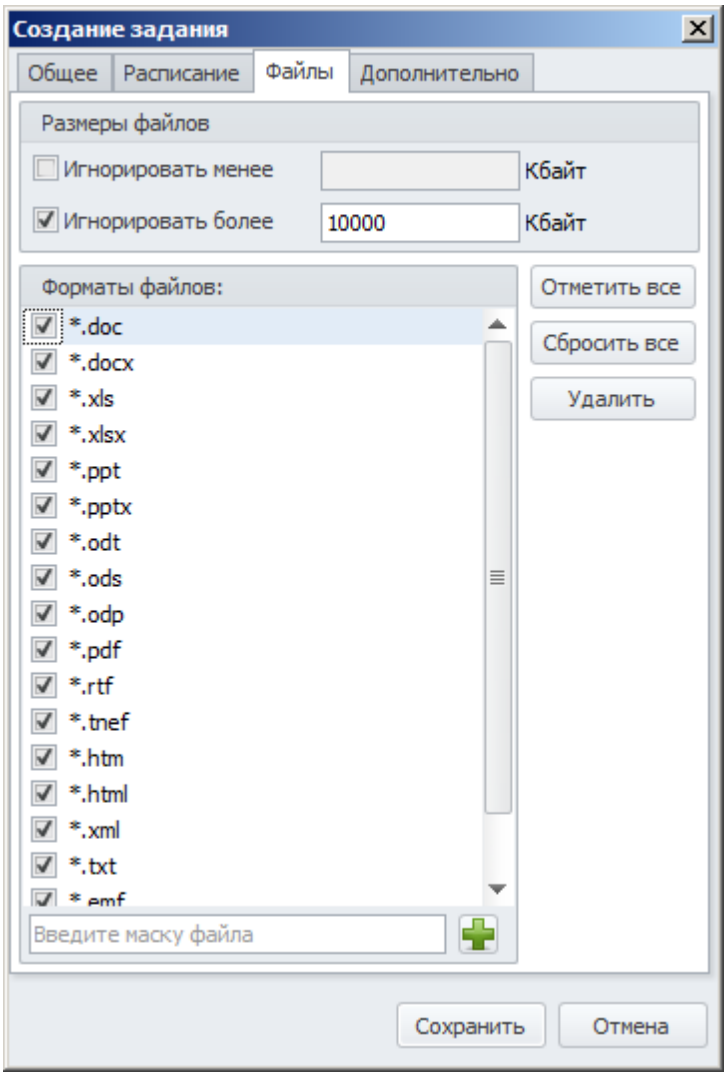
- **Еженедельно** – укажите день недели и время автоматического запуска
- **Ежедневно** – укажите день недели и время автоматического запуска
- **Вручную** – в этом случае запуск задания может осуществляться только способом, описанным в разделе "Выполнение и остановка задания".

Важная информация!

Если при наступлении времени запуска предыдущая сессия запуска этого задания ещё не завершила свою работу, то задание повторно запущено не будет.

По умолчанию задание запускается только вручную, по команде пользователя.

6. На вкладке **Файлы** определите размеры и форматы файлов, которые нужно отправлять на анализ.



Определите:

- **Размеры файлов** – нижнюю и верхнюю границу размера файлов, которые нужно отправлять на анализ
- **Форматы файлов** – выберите маски файлов из списка предустановленных или добавляйте собственные маски, вводя их в поле ввода внизу списка и нажимая .

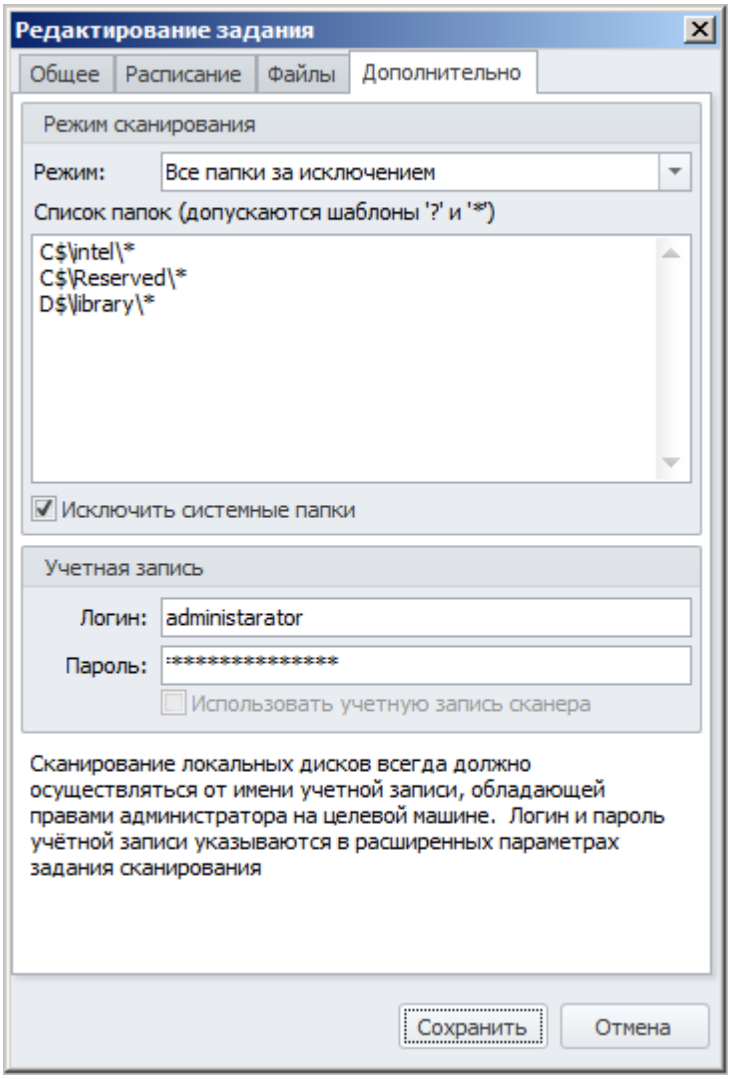
Важная информация!

Использование маски *.* может значительно снизить скорость сканирования и существенно увеличить нагрузку на сервер Traffic Monitor.

7. На вкладке **Дополнительно** вы можете ограничить цели сканирования, задав список сканируемых папок, а также указать параметры учётной записи, от имени которой будет запускаться задание. Сканирование локальных дисков должно осуществляться от имени учётной записи, обладающей правами администратора на целевых рабочих станциях.

Примечание

Для сканирования рабочих станций под управлением MS Windows Vista, MS Windows 7 или MS Windows 8 рекомендуется использовать учетную запись доменного администратора.



Укажите необходимый режим сканирования папок:

- Все папки;
- Все папки за исключением;
- Только перечисленные папки.

При задании списка папок:

- Каждая папка должна быть задана на отдельной строке.
- Для замены одного или нескольких символов можно использовать символы «?» или «*» соответственно.
- Если при указании имени папки в конце имени не было указано «*», то при сохранении настроек к строке автоматически добавляется «*».
- Использование символа «:» не допускается: чтобы задать путь к директории, используйте маски вида «C$\Windows*» или «?$\Windows*».

Для данного типа задания по умолчанию отмечена настройка **Исключить системные папки**. Список исключаемых системных папок можно посмотреть и отредактировать в диалоговом окне настройки параметров работы сканера (подробнее см. "Настройка параметров работы сканера Crawler").

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

Сохранённое задание может выполняться либо автоматически согласно заданному расписанию (если оно было определено), либо вручную, как описано в разделе "Выполнение задания".

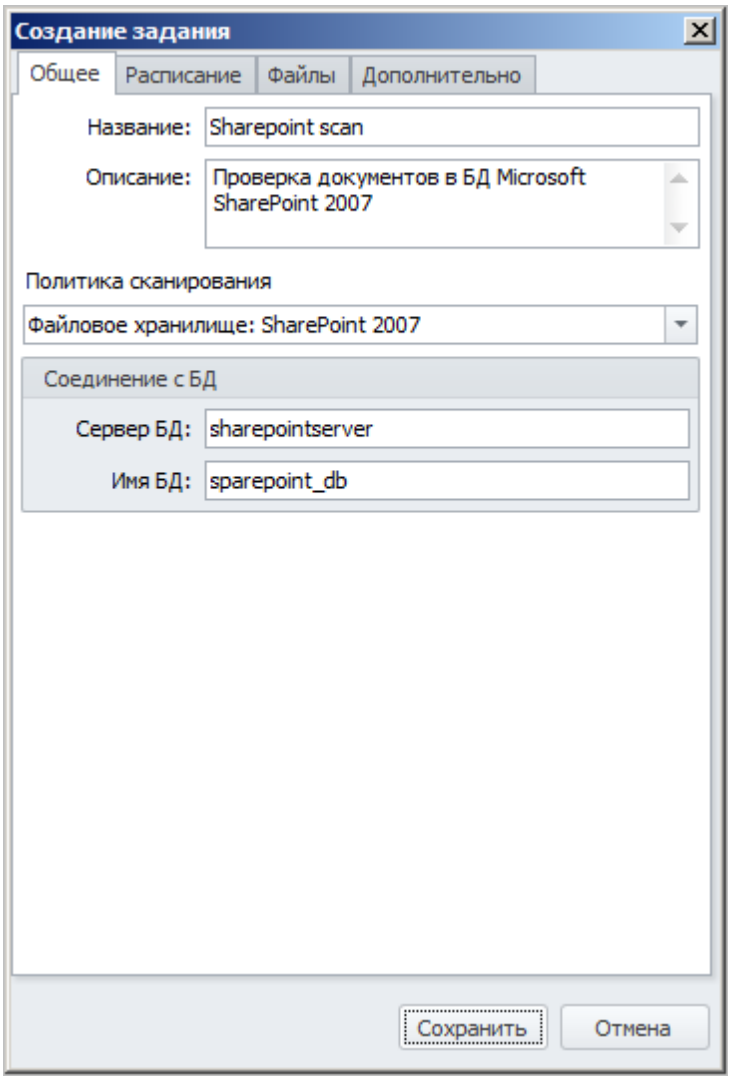
6.4.3 Сканирование файлового хранилища SharePoint

Задача сканирования файлового хранилища SharePoint обеспечивает проверку документов, хранящихся в базе данных Microsoft SharePoint 2007. Для выполнения задания необходима учётная запись, обладающая правами на чтение данных из проверяемого файлового хранилища (параметры учётной записи задаются на вкладке **Дополнительно**).

Чтобы создать или изменить задание на сканирование файлового хранилища SharePoint:

1. В Консоли управления перейдите к разделу **Краулер**.
2. Выполните одно из следующих действий:
   - чтобы добавить задание, нажмите кнопку  **Создать** на панели инструментов
   - чтобы изменить имеющееся задание, выберите его в списке и нажмите кнопку  **Изменить** на панели инструментов.

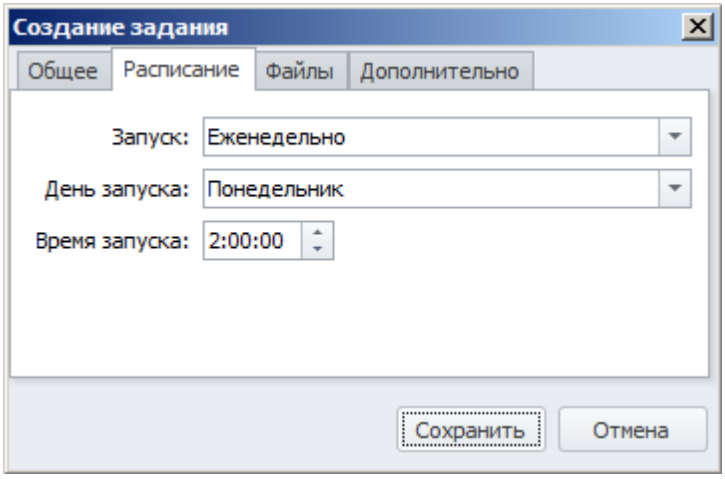
   На экран будет выведено диалоговое окно для настройки задания.
3. На вкладке **Общее** укажите общие параметры задания:
   - **Название** – имя задания.
   - **Описание** – необязательное поле с произвольным текстом
   - **Политика сканирования** – из раскрывающегося списка выберите **Файловое хранилище: SharePoint 2007**



4. В области **Соединение с БД** укажите параметры целевой базы данных SharePoint:

- **Сервер БД** – адрес сервера базы данных SharePoint
- **Имя БД** – имя экземпляра базы данных SharePoint

5. На вкладке **Расписание** настройте расписание автоматического запуска задания.



Выберите один из вариантов запуска задания:

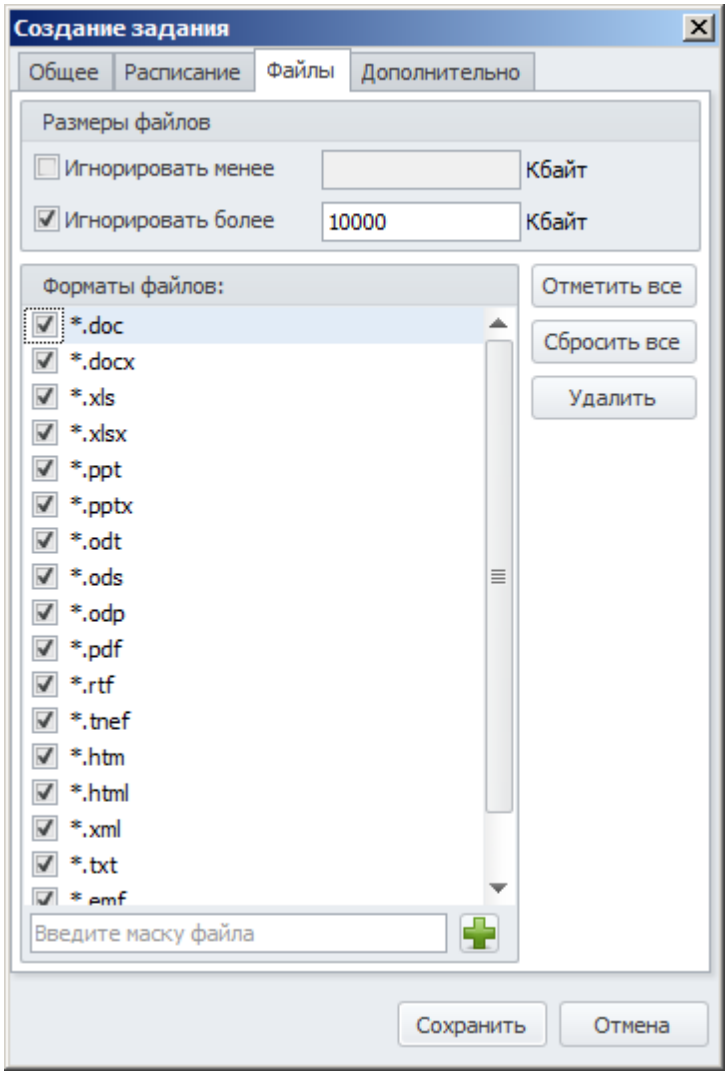
- **Еженедельно** – укажите день недели и время автоматического запуска
- **Ежедневно** – укажите день недели и время автоматического запуска
- **Вручную** – в этом случае запуск задания может осуществляться только способом, описанным в разделе "Выполнение и остановка задания".

Важная информация!

Если при наступлении времени запуска предыдущая сессия запуска этого задания ещё не завершила свою работу, то задание повторно запущено не будет.

По умолчанию задание запускается только вручную, по команде пользователя.

6. На вкладке **Файлы** определите размеры и форматы файлов, которые нужно отправлять на анализ.



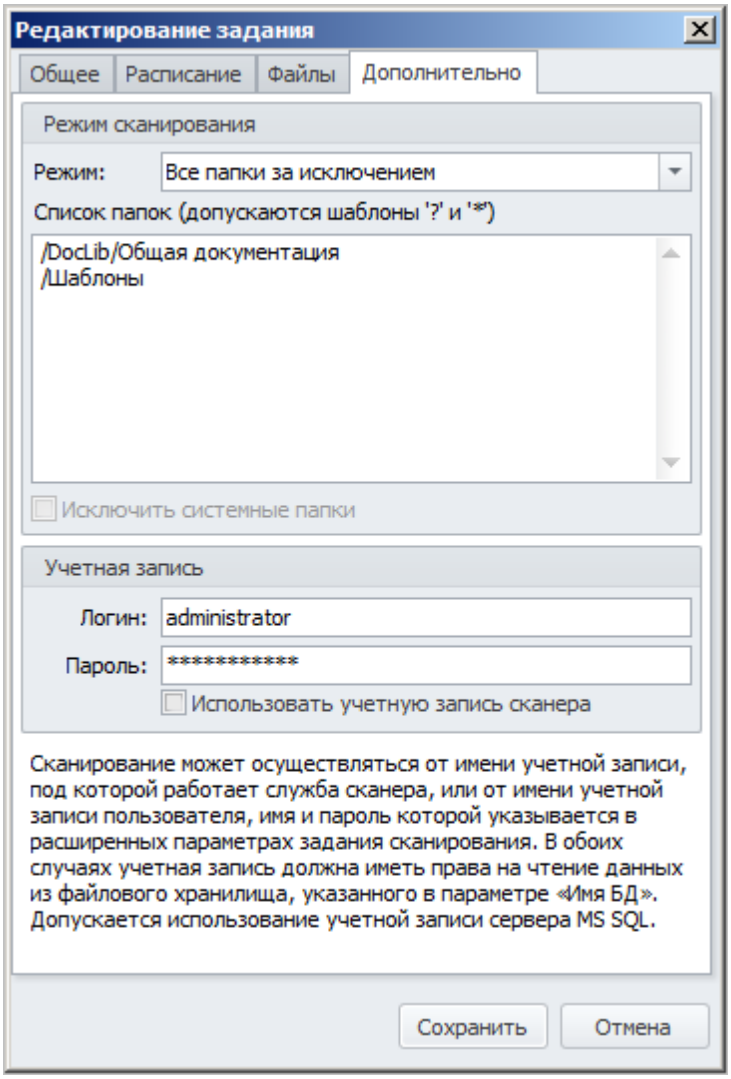
Определите:

- **Размеры файлов** – нижнюю и верхнюю границу размера файлов, которые нужно отправлять на анализ
- **Форматы файлов** – выберите маски файлов из списка предустановленных или добавляйте собственные маски, вводя их в поле ввода внизу списка и нажимая .

Важная информация!

Использование маски *.* может значительно снизить скорость сканирования и существенно увеличить нагрузку на сервер Traffic Monitor.

7. На вкладке **Дополнительно** вы можете ограничить цели сканирования, задав список сканируемых папок, а также указать параметры учётной записи, от имени которой будет запускаться задание. Сканирование файлового хранилища SharePoint должно осуществляться от имени доменной учётной записи или учётной записи MS SQL. Эта запись должна обладать правами на чтение данных из сканируемого файлового хранилища.



Укажите необходимый режим сканирования папок:

- Все папки;
- Все папки за исключением;
- Только перечисленные папки.

При задании списка папок:

- Указывайте пути относительно корневого каталога хранилища, в формате Windows Explorer. Вы можете посмотреть путь к текущей папке хранилища, выбрав в меню SharePoint: **Actions -> Open with Windows Explorer**
- Каждая папка должна быть задана на отдельной строке.
- Для замены одного или нескольких символов можно использовать символы «?» или «*» соответственно.
- Если при указании имени папки в конце имени не было указано «*», то при сохранении настроек к строке автоматически добавляется «*».

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

Сохранённое задание может выполняться либо автоматически согласно заданному расписанию (если оно было определено), либо вручную, как описано в разделе "Выполнение задания".

6.5 Удаление задания на сканирование

Чтобы удалить задание на сканирование:

1. Консоли управления перейдите к разделу **Краулер**.
2. Выберите задание из списка.
3. Выполните одно из следующих действий:
   - нажмите кнопку **Удалить** на панели инструментов
   - нажмите на задании правой кнопкой мыши и из раскрывшегося списка выберите **Удалить**.

6.6 Выполнение и остановка задания

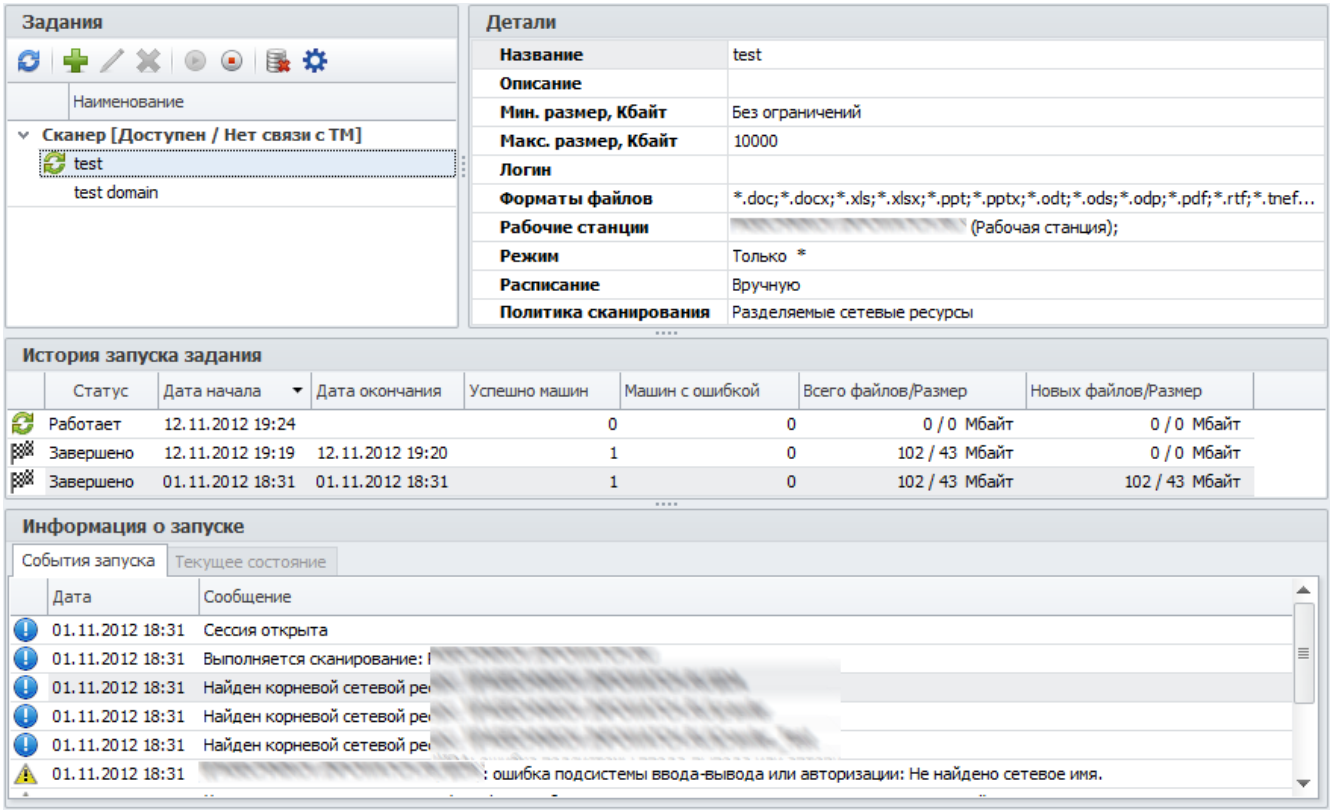
Если при создании задания (см. "Создание и редактирование задания на сканирование") на вкладке **Расписание** вы выбрали еженедельный или ежедневный запуск, то задание будет выполняться автоматически без вмешательства офицера безопасности. Если вы выбрали способ запуска **Вручную**, то запуск задания может осуществляться только с помощью способа, описанного ниже.

Ручной запуск задания может также потребоваться в том случае, если по каким-либо причинам вам потребовалось остановить задачу, и необходимо запустить её вновь.

Чтобы запустить выполнение задания на сканирование:

1. В Консоли управления перейдите к разделу **Краулер**.
2. Выберите необходимое задание из списка.
3. Выполните одно из следующих действий:
   - нажмите кнопку **Запустить** на панели инструментов
   - нажмите на задании правой кнопкой мыши и из раскрывшегося списка выберите **Запустить**.

В области **История запуска задания** появится запись о новой сессии со статусом **Работает**.



События, возникающие в ходе сканирования, отображаются в области **Информация о запуске**, вкладка **События запуска**.

На вкладке **Текущее состояние** вы можете просмотреть, какие ресурсы, папки и файлы сканируются в настоящий момент. Также отображается общий объём данных, обработанных за текущую сессию.

По окончании сессии задание получит статус **Завершена**.

Чтобы остановить выполнение задания на сканирование, не дожидаясь завершения:

1. Выберите запущенное задание из списка.
2. Выполните одно из следующих действий:
   - нажмите кнопку **Остановить** на панели инструментов
   - нажмите на задании правой кнопкой мыши и из раскрывшегося списка выберите **Остановить**.

Задание получит статус **Остановлена**.

Примечание

Если в задании сканируется много машин, оно может останавливаться не сразу. На время останавливания блокируется возможность остановить/запустить/отредактировать/удалить это задание.

6.7 Очистка базы хешей

Для оптимизации работы в Crawler предусмотрено хранение **хешей** – контрольных сумм файлов. Если в ходе предыдущего запуска задания сканирования был сохранен хеш какого-либо файла и при очередном запуске того же самого задания сканирования хеш для этого файла не изменился, это означает, что в данный файл не подвергался изменениям и его не следует отправлять его на обработку на сервер Traffic Monitor. Это позволяет уменьшить нагрузку на канал между Crawler и сервером Traffic Monitor, а также на сам сервер Traffic Monitor, а также исключает дублирование идентичных событий для каждого запуска задания на сканирование.

Особенности хранения базы хешей:

- База хешей сохраняется отдельно для каждого задания сканирования. Следовательно, если какой-либо файл уже был обработан другим заданием, то при создании и запуске другого задания это учитываться не будет.
- Хеш-суммы хранятся для файлов с учетом рабочих станций, на которых эти файлы были обнаружены. Таким образом, если один и тот же файл находится на нескольких рабочих станциях, он будет обрабатываться отдельно для каждой рабочей станции.

Рекомендуется выполнять периодическую очистку базы хешей: например, в том случае, когда изменилась конфигурация Traffic Monitor – то есть согласно изменившемуся сценарию обработки объектов или списку терминов и т.п. решение о том, является ли перехваченный объект потенциальным нарушением, будет приниматься системой по другому алгоритму. В результате очистки базы хешей задание «забудет» о том, что оно когда-либо обрабатывало какие-либо файлы, и будет отправлять для анализа на сервер Traffic Monitor все файлы, соответствующие условиям данного задания.

Чтобы очистить базу хешей:

1. В Консоли управления перейдите к разделу **Краулер**.
2. Выберите необходимое задание из списка.
3. Выполните одно из следующих действий:
   - нажмите кнопку **Очистить базу хешей** на панели инструментов
   - нажмите на задании правой кнопкой мыши и из раскрывшегося списка выберите **Очистить базу хешей**.

7 Настройка параметров анализа объектов

Вы можете настроить порядок анализа объектов Системой с помощью действий, описанных в следующих разделах:

- Управление конфигурацией
- Справочники
- Настройка сценария анализа объектов

7.1 Управление конфигурацией

Конфигурация представляет собой набор различных настроек, необходимых для проверки объектов на Traffic Monitor Server, а также для мониторинга и анализа данных. В Консоли управления (раздел **Конфигурация**) отображается информация по всем версиям конфигурации (см. "Версии конфигурации").

Каждый объект, передаваемый в Traffic Monitor, обрабатывается в соответствии с той версией конфигурации, которая в данный момент действует на сервере, а затем сохраняется в базу данных вместе со всеми атрибутами, присвоенными данному объекту по результатам обработки.



Важная информация!

Система не выполняет повторную обработку объекта по новой, измененной конфигурации.

Настройка конфигурации включает в себя:

- *Только при использовании технологии Лингвистический анализ*. Составление классификатора (см. " Классификатор").
- *Только при использовании технологии Детектирование текстовых объектов.* Выбор типов текстовых объектов, подлежащих детектированию (см. "Текстовые объекты").
- Составление списков, которые будут использоваться при анализе объектов (см. "Списки").
- Создание пользовательского сценария, в соответствии с которым будет выполняться проверка объектов на Traffic Monitor Server (см. "Сценарий анализа объектов").

Кроме того, для корректной работы сценария вам потребуется выполнить дополнительные настройки:

- *Только при использовании технологии Цифровые отпечатки.* Создать базу эталонных документов (см. "База эталонных документов").
- Создать зоны ответственности, по которым будут распределяться объекты, проверяемые в Системе (см. "Зоны ответственности").
- Создать теги, которые могут быть присвоены объектам (см. "Теги").
- Создать набор цветов, которые будут использоваться для выделения объектов (см. "Цвета").

После того как все настройки будут выполнены, загрузите конфигурацию на хосты (см. "Загрузка конфигурации на хосты").

7.1.1 Версии конфигурации

Версии конфигурации используются для контроля изменений в настройках параметров анализа объектов. Изменения по версиям поддерживаются только для элементов конфигурации. К таким элементам относятся:

- классификатор;
- сценарии анализа объектов;
- списки;
- текстовые объекты.

Состояние каждой версии определяется ее статусом:

Статус версии конфигурации	Описание статуса
Редактируемая	Версия находится в состоянии редактирования. После того как все необходимые параметры будут заданы, можно загрузить редактируемую версию на хост.
Активная	Конфигурация загружена на Traffic Monitor Server (список серверов, на которые загружается конфигурация, можно посмотреть в разделе **Хосты**). Traffic Monitor Server выполняет анализ объектов в соответствии с настройками этой версии. Активная версия недоступна для редактирования
Архивная	Версия хранится в базе данных, но не может быть отредактирована или загружена на Traffic Monitor Server

При необходимости вы можете возвратиться к одной из предыдущих версий конфигурации (см. "Возврат к старой версии конфигурации").



Примечание

Возврат к прежней версии осуществляется для конфигурации, находящейся в базе данных. Изменение версии конфигурации на хосте происходит только после очередной процедуры загрузки конфигурации на хост.

Более подробную информацию о работе с версиями конфигурации вы можете найти в следующих разделах:

- Просмотр информации по конфигурации
- Добавление описания к версии конфигурации
- Сравнение двух версий конфигурации
- Загрузка конфигурации на хосты
- Возврат к старой версии конфигурации
- Удаление версии конфигурации

7.1.1.1 Просмотр информации по конфигурации

Общие параметры конфигурации можно посмотреть в разделе **Версии конфигурации** (область **Конфигурация** на панели **Навигация**). В рабочей области главного окна отображается список конфигураций.

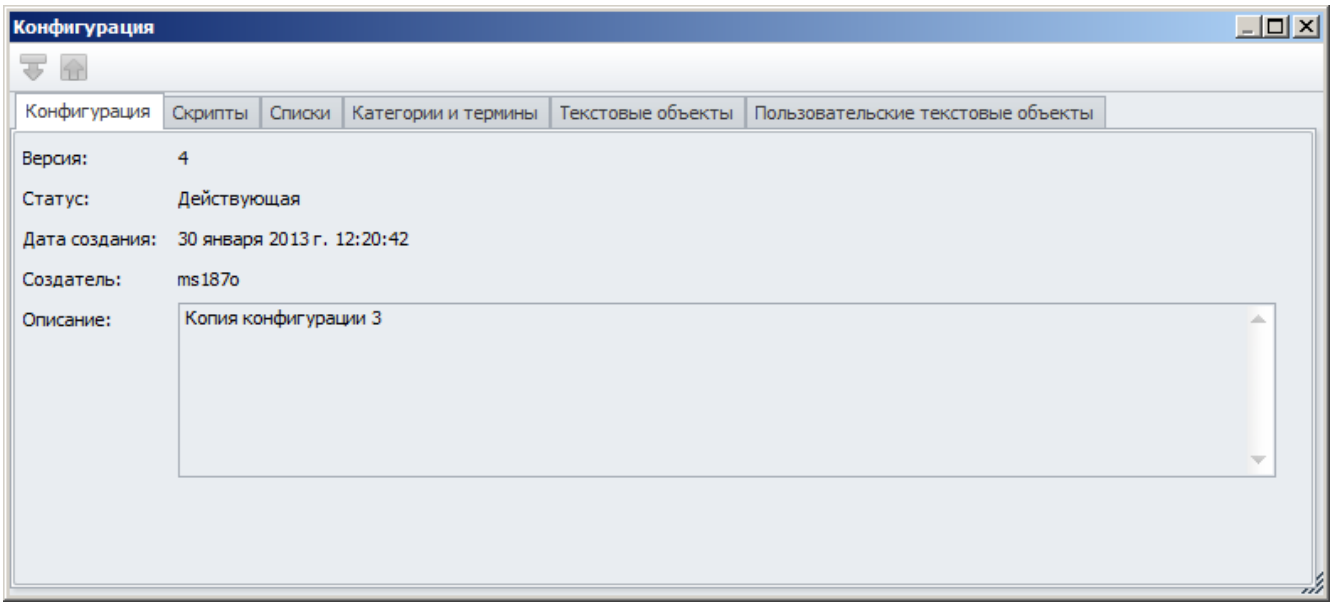
По каждой версии конфигурации в рабочей области главного окна выводится общая информация:

Атрибут конфигурации	**Описание**
Версия	Номер версии конфигурации
Статус	Состояние версии на текущий момент. Каждая версии конфигурации может находиться в одном из следующих состояний: • **Редактируемая** (выделена зеленым цветом). Версия конфигурации, которая находится в состоянии редактирования. Чтобы найти эту версию в списке, на панели инструментов нажмите кнопку **Найти редактируемую конфигурацию**. • **Активная** (выделена желтым цветом). Версия конфигурации, загруженная на Traffic Monitor Server. Чтобы найти эту версию в списке, на панели инструментов нажмите кнопку **Найти активную конфигурацию**. • **Архивная**. Сохраненная версия конфигурации.
Дата создания	Дата и время создания версии
Создатель	Имя учетной записи пользователя, сохранившего версию
Описание	Дополнительные сведения о версии.

Чтобы просмотреть подробную информацию по определенной версии конфигурации:

1. В дереве конфигурации выделите строку с нужной версией конфигурации.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Просмотреть**;
   - нажмите кнопку **Просмотреть** на панели инструментов;
   - щелкните по выделенной строке правой кнопкой мыши и в раскрывшемся меню выберите **Просмотреть**;
   - дважды щелкните левой кнопкой мыши по выделенной строке.

   На экран будет выведено окно для просмотра параметров версии.



Просмотр информации по выбранной версии конфигурации

На вкладке **Конфигурация** отображаются общие параметры конфигурации, такие как номер версии, статус, дата создания и т. д. На других вкладках выводится подробная информация по элементам конфигурации.

7.1.1.2 Добавление описания к версии конфигурации

Чтобы добавить или изменить описание к версии конфигурации:

1. В дереве конфигураций выделите строку с нужной версией.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Изменить описание;**
   - нажмите кнопку **Изменить описание** на панели инструментов;
   - щелкните по выделенной строке правой кнопкой мыши и в раскрывшемся меню выберите **Изменить описание**.

   В открывшемся диалоговом окне добавьте комментарии к версии и нажмите кнопку **Сохранить**.

7.1.1.3 Сравнение двух версий конфигурации

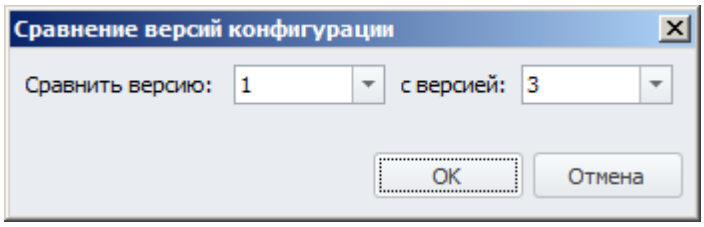
Проследить за изменениями, внесенными в конфигурацию, можно путем сравнения двух версий конфигурации.

Чтобы сравнить две версии конфигурации:

1. Перейдите к разделу **Версии конфигурации**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Сравнить**.

- нажмите кнопку **Сравнить** на панели инструментов.

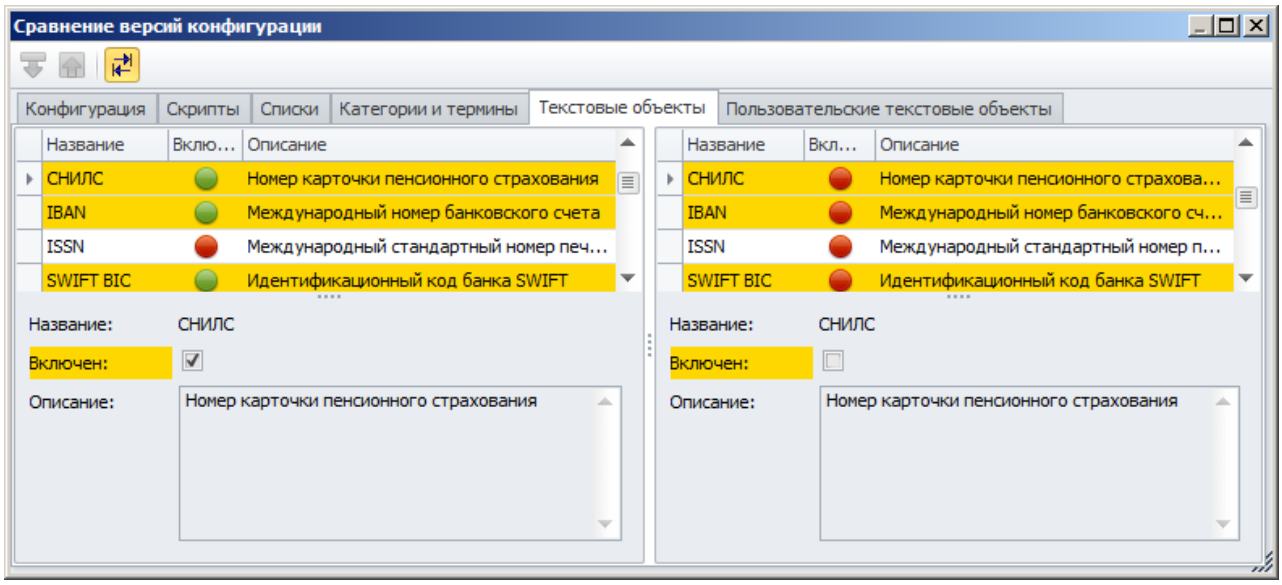
На экран будет выведено диалоговое окно **Сравнение версий конфигурации**.



Выбор сравниваемых версий

3. Выберите нужные версии конфигурации, затем нажмите кнопку **OK**.

После этого на экран будет выведено окно для сравнения версий.



Просмотр различий между двумя версиями

Данное окно аналогично тому, в котором выводится информация по одной версии (см. "Просмотр информации по конфигурации"). Но при сравнении двух версий окно поделено на две части: слева выводится информация по исходной версии, справа – по сравниваемой.

Работая со списками или древовидными структурами, вы можете использовать функцию синхронного просмотра. Если данная функция включена, то возможен синхронный просмотр значений, совпадающих для обеих версий. Чтобы активизировать синхронный просмотр, нажмите кнопку **Синхронизировать фокус**. После этого вид кнопки изменится на (режим синхронного просмотра).

Изменения, внесенные в процессе редактирования конфигурации, выделяются цветами:

- **Зеленый**. Добавлено новое значение.
- **Желтый**. Значение существующего параметра было изменено.
- **Красный**. Данное значение было удалено.

7.1.1.4 Загрузка конфигурации на хосты

Конфигурация хранится в базе данных. По команде пользователя конфигурация со статусом **Редактируемая** (в том числе справочники Active Directory) загружается на хосты. В процессе обновления конфигурации на хосте присутствуют старая и новая версии конфигурации. Причем обе версии имеют статус **Активная**. Администратору, который переходит к разделу **Версии конфигурации** или обновляет данные раздела в это время, выдается предупреждение о том, что в текущий момент имеются две конфигурации со статусом **Активная**.

После того как процесс обновления конфигурации будет завершен, статус **Активная** будет только у конфигурации, отправленной на сервер. Средняя длительность обновления конфигурации составляет 10 минут. Если по истечении более 15 минут после обновления в разделе **Версии конфигурации** все еще отображаются две версии со статусом **Активная**, это свидетельствует о возникновении аварийной ситуации. Такая ситуация требует немедленного разрешения и до устранения проблемы работать с Консолью управления не рекомендуется. Поэтому перейдите к разделу **Хосты** и проверьте, на каких хостах не обновлена конфигурация (если хосту назначено несколько параметров, то проверяются все параметры). Затем проверьте состояние процесса, отвечающего за загрузку конфигурации на Traffic Monitor (такая проверка выполняется администратором Traffic Monitor Server: см. документ «*InfoWatch Traffic Monitor. Руководство администратора*»). Запустите или перезапустите этот процесс. После этого повторите загрузку конфигурации на хосты.

Чтобы загрузить конфигурацию в базу данных:

1. Перейдите к разделу **Версии конфигурации**.

2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Ввести в действие редактируемую конфигурацию**;
   - нажмите кнопку  **Ввести в действие редактируемую конфигурацию** на панели инструментов.

   После выполнения любого из этих действий конфигурация (а также справочники сотрудников и рабочих станций) будет загружена в базу данных. Загрузка конфигурации на хост будет выполнена при обращении хоста к базе данных.

 **Примечание**

Загрузка конфигурации может занять некоторое время. По завершении операции будут обновлены статусы загрузки конфигурации на хосты и версия активной конфигурации в разделе **Версии конфигурации**.

Статус загрузки конфигурации на хост, а также дата и время последнего обновления отображаются на панели профиля хоста (см. "Работа с хостами").

7.1.1.5 Возврат к старой версии конфигурации

В процессе работы у вас может возникнуть необходимость вернуться к одной из предыдущих версий конфигурации. Вернуться можно как к архивной версии, так и к версии, загруженной на хост.

Процесс возврата заключается в следующем. Версия со статусом **Редактируемая** сохраняется в базе данных и получает статус **Архивная**. Версия, к которой выполняется возврат, сохраняется в базе данных как новая версия со статусом **Редактируемая**. Редактируемая версия может быть снова отредактирована и загружена на хост.

Важная информация!

Возврат к старой версии осуществляется для конфигурации, находящейся в базе данных. Изменение версии конфигурации на хосте происходит только при загрузке редактируемой конфигурации на хост (см. "Загрузка конфигурации на хосты").

Чтобы вернуться к старой версии конфигурации:

1. Перейдите к разделу **Версии конфигурации**.
2. Выделите строку с той версией, к которой нужно выполнить возврат.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Откатить**;
   - нажмите кнопку **Откатить** на панели инструментов;
   - щелкните по выделенной строке правой кнопкой мыши и в раскрывшемся меню выберите **Откатить**.
4. В появившемся окне запроса нажмите кнопку **Да**, чтобы вернуться к выбранной версии.

7.1.1.6 Удаление версии конфигурации

Если дальнейшее использование какой-либо версии конфигурации не предполагается, то такая версия может быть удалена из Системы. Вы можете удалять любые версии, за исключением следующих:

- версия со статусом **Редактируемая**;
- версия со статусом **Активная**;
- версия со статусом **Архивная**, если ранее она загружалась на сервер, и в базе данных есть объекты, связанные с этой версией;
- начальная версия (версия 0).

Чтобы удалить версию конфигурации:

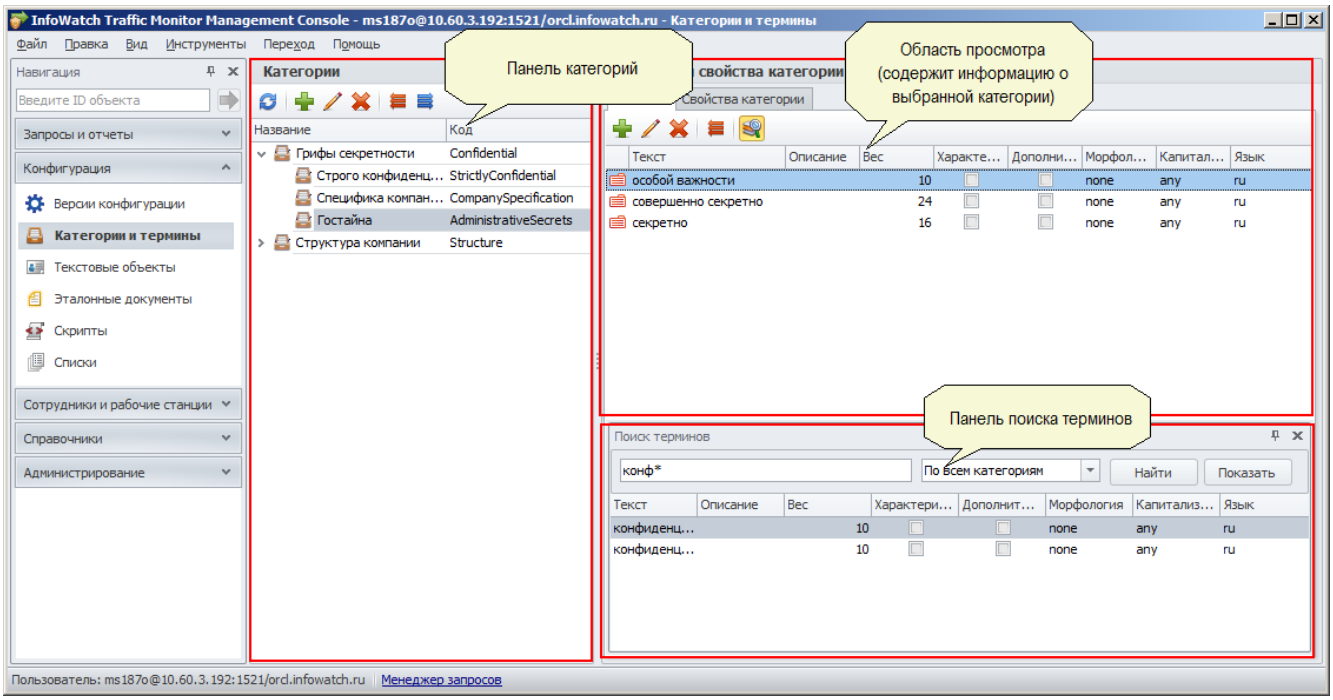
1. Перейдите к разделу **Версии конфигурации**.
2. Выделите строку с нужной версией.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку **Удалить** на панели инструментов;
   - щелкните по выделенной строке правой кнопкой мыши и в раскрывшемся меню выберите **Удалить**.
4. В появившемся окне запроса нажмите кнопку **Да**.

7.1.2 Классификатор

Классификатор - это база данных, представляющая собой выделенный на основе вероятностных и математических методов иерархически организованный список (дерево) **категорий**, каждая из которых отражает специфику какой-либо предметной области. Категории содержат **термины** - слова и выражения, наличие которых в документе позволяет определить тематику и степень конфиденциальности информации.

Например, категория *Финансы* содержит финансовую терминологию (*платеж*, *инвесторы*, *цены* и пр.). Таким образом, наличие в тексте термина, принадлежащего к определенной категории, позволяет соотнести текст с этой категорией.

Работа с классификатором ведется в разделе **Категории и термины** (область **Конфигурация** на панели **Навигация**). При переходе к данному разделу рабочая область главного окна будет поделена на две части. Слева располагается панель категорий, справа – область просмотра параметров категории.



Раздел Категории и термины

На панели категорий отображается **дерево категорий** – иерархический список категорий. С элементом *Категория* сопоставлена пиктограмма .

Чтобы просмотреть подробные сведения о категории,

в дереве категорий выделите строку с названием нужной категории.

Параметры выбранной категории будут отображены справа, в области просмотра. На вкладке **Свойства категории** выводятся общие параметры категории. Сведения о терминах выводятся на вкладке **Термины**.

Более подробную информацию о работе с классификатором вы можете найти в следующих разделах:

- Принципы составления классификатора
- Создание категории
- Добавление термина в категорию
- Редактирование категории
- Смена уровня вложенности категории
- Настройка параметров термина
- Поиск термина
- Удаление категории
- Экспорт/импорт классификатора

7.1.2.1 Принципы составления классификатора

Использование поставляемых классификаторов

В результате установки системы из поставляемого дистрибутива доступен стандартный классификатор: русскоязычный либо англоязычный, в зависимости от опций установки. Стандартная конфигурация содержит термины, встречающиеся практически в любых областях, и гарантирует детектирование данных по таким тематикам, как *«Счета»*, *«Бухгалтерия»*, *«Кредиты»*, *«Тендеры»*, *«HR»* и т.д.

Дополнительно могут предоставляться отраслевые классификаторы (банковская, нефтегазовая, телекомумуникационная тематика); классификатор, позволяющий находить термины, связанные с нарушением законодательства РФ и некоторые другие тематические классификаторы. Также разработаны классификаторы, обеспечивающие определение терминов на различных языках: испанский, узбекский, казахский, арабский и некоторые другие.

InfoWatch также предоставляет услугу кастомизации классификатора: он может быть доработан с учетом специфики деятельности конкретной компании. Дополнение такой отраслевого классификатора категориями, отражающими специфику деятельности данной компании, обеспечивает лучшую категоризацию и более точное детектирование конфиденциальной информации в информационных потоках компании. Кастомизация классификатора может выполняться вручную специалистами-лингвистами, либо с использованием специального программного продукта – InfoWatch Автолингвист, позволяющего на основе коллекции текстов автоматически создавать совокупность категорий и терминов, и позволяющий оценить качество этой коллекции.

Подключение дополнительных классификаторов выполняется с помощью импортирования предоставленного XML-файла: см. "Экспорт/импорт классификатора"

Создание классификатора вручную

Чтобы составить классификатор, необходимо составить список категорий и наполнить каждую категорию терминами. Один и тот же термин можно включать в несколько категорий. Например, термин *Заработная плата* может входить в категории *Внутренние платежи* и *Условия труда*.

При классификации проверяемых объектов по категориям важно, сколько терминов было найдено в анализируемом тексте, как часто каждый из этих терминов встречался в документе и к какому типу этот термин принадлежит. Различают следующие типы терминов:

- **Характеристический**. Если в тексте найден характеристический термин, относящийся к определенной категории, то текст безусловно считается релевантным (соответствующим) этой категории. Для таких терминов подсчет суммы веса выполняется только с целью получения дополнительной статистической информации.
  Пример: В категории *Финансы* задан характеристический термин *Финансовый отчет*. Если в тексте перехваченного объекта хотя бы один раз встречается словосочетание «финансовый отчет», то текст будет считаться релевантным категории *Финансы*.
- **Обыкновенный**. Обыкновенные термины (в отличие от характеристических) не могут служить абсолютным признаком того, что текст соответствует категории. Решение о том, соответствует ли текст категории, принимается по общей сумме веса терминов этой категории, найденных в тексте. При подсчете общей суммы веса терминов учитываются обыкновенные и дополнительные термины, относящиеся к одной категории.
- **Дополнительный**. Дополнительные термины используются как вспомогательные: их вес также будет учитываться при подсчете общей суммы веса обыкновенных терминов.

Лингвистический анализ объекта может осуществляться с учетом словоизменения (морфологии). Параметры морфологии задаются при настройке параметров термина (см. "Настройка параметров термина"). Классификатор поддерживает морфологию для следующих языков:

- русский (ru)
- английский (en)
- французский (fr)
- немецкий (de)
- испанский (es)
- итальянский (it)
- арабский (ara)
- украинский (ukr)

Также поддерживается более широкий перечень языков, для которых осуществляется проверка на полное совпадение терминов в анализируемом тексте и заданных терминов.

7.1.2.2 Создание категории

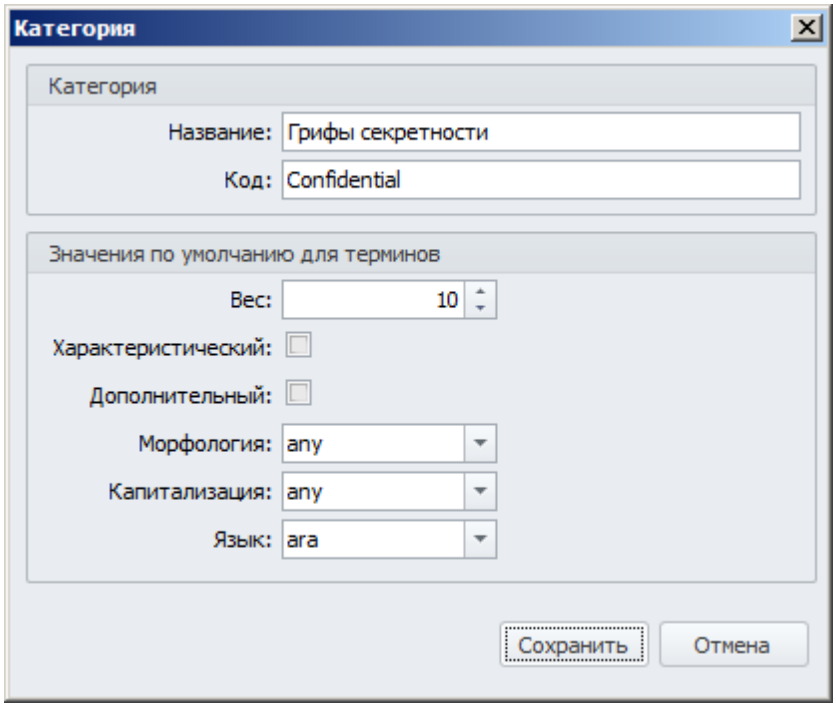
Чтобы создать категорию:

1. Перейдите к разделу **Категории и термины**.

2. Если вы хотите создать подкатегорию, выделите название родительской категории в дереве категорий.

3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Создать категорию**;
   - нажмите кнопку  **Создать категорию** на панели категорий.

   На экран будет выведено диалоговое окно **Категория**.



Настройка параметров категории

4. Укажите параметры категории.

   На панели **Категория** настройте общие параметры:

   - **Название**. Название категории (обязательный параметр). К названиям не предъявляется

требование уникальности, однако не рекомендуется давать категориям одинаковые названия.

- **Код**. Кодовое название категории, которое будет использоваться при составлении сценария (обязательный параметр). Может состоять из букв латинского алфавита, цифр и символа подчеркивания; не должно начинаться с цифры. Код должен быть уникальным.

На панели **Значения по умолчанию для терминов** настройте значения параметров для терминов данной категории (см. "Настройка параметров термина"). Указанные значения будут использоваться как значения по умолчанию для всех терминов, входящих в данную категорию.

5. Нажмите кнопку **Сохранить**.

После того как новая категория будет добавлена в классификатор, необходимо составить список терминов, принадлежащих к этой категории. Добавить термин в категорию можно несколькими способами:

- Создать термин
- Импортировать термины из файла
- Переместить термин из другой категории

7.1.2.3 Добавление термина в категорию

Вы можете добавлять термины в категорию одним из следующих способов:

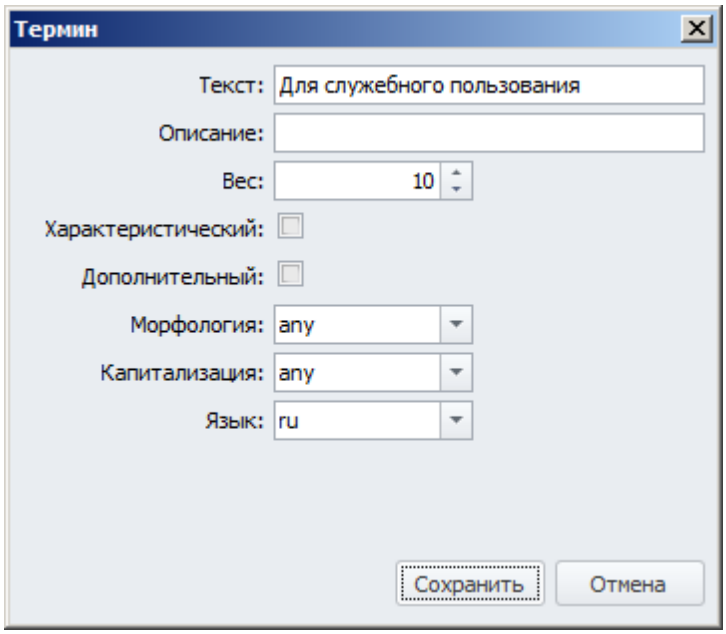
- Создать термин
- Импортировать термины из файла
- Переместить термины из другой категории

7.1.2.3.1 Создание термина

Чтобы создать термин:

1. Перейдите к разделу **Категории и термины**.
2. В дереве категорий выделите название нужной категории.
3. В области просмотра параметров категории перейдите на вкладку **Термины**.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка >Термин > Создать**;
   - нажмите кнопку  **Создать термин** на панели инструментов вкладки **Термины**.

   На экран будет выведено диалоговое окно **Термин**.



Настройка параметров термина

5. Задайте параметры термина (см. "Настройка параметров термина").
6. Нажмите кнопку **Сохранить**.

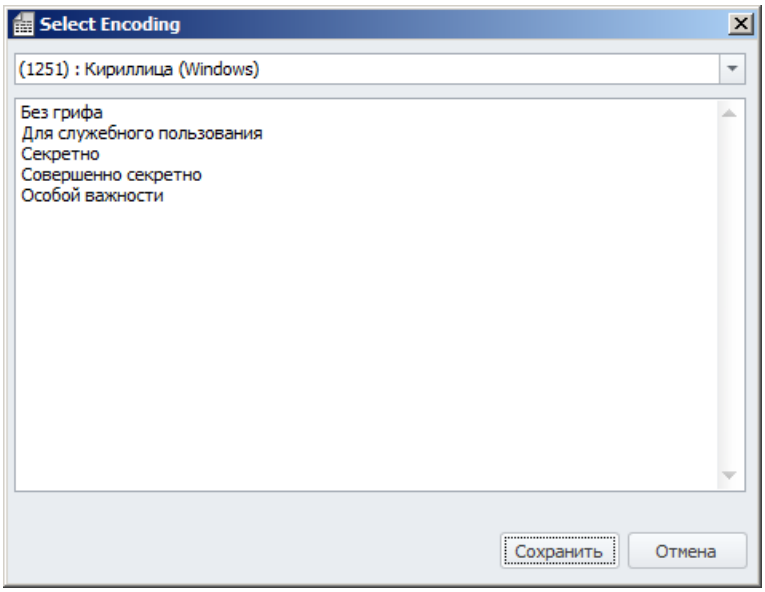
7.1.2.3.2 Импорт терминов из файла

Термины можно импортировать в классификатор из текстовых файлов формата `.txt`.

Чтобы импортировать термин:

1. Перейдите к разделу **Категории и термины**.
2. В дереве категорий выделите название нужной категории.
3. В области просмотра параметров категории перейдите на вкладку **Термины**.
4. Нажмите кнопку **Импорт** в верхней части вкладки **Термины**.
5. В открывшемся диалоговом окне выберите нужный текстовый файл и нажмите кнопку **Открыть**.

   На экран будет выведено диалоговое окно с содержанием выбранного файла.



Настройка импортируемых терминов

6. В верхней части данного окна выберите тип кодировки символов из раскрывающегося списка.

7. Отредактируйте текст таким образом, чтобы в каждой строке содержался один термин. Удалите термины, которые не нужно импортировать. Если необходимо, введите дополнительные термины.

   Важная информация!

   Изменения, выполняемые в этом диалоговом окне, относятся только к импорту терминов и не влияют на исходный текстовый файл.

8. Нажмите кнопку **Сохранить**, чтобы начать процедуру импорта.

В результате термины будут импортированы в выбранную категорию. Термины импортируются с параметрами по умолчанию. По окончании процедуры импорта вы можете изменить параметры терминов (см. "Настройка параметров термина").

7.1.2.3.3 Перемещение термина из другой категории

Чтобы переместить термин из одной категории в другую:

1. Перейдите к разделу **Категории и термины**.

2. В дереве категорий выделите название категории, в которую входит нужный термин.

3. В области просмотра параметров категории перейдите на вкладку **Термины**.

4. Щелкните левой кнопкой мыши по термину, который нужно переместить. Затем, не отпуская левую кнопку мыши, подведите курсор мыши к строке с названием той категории, в которую будет перемещен термин. После того, как слева от названия выбранной категории появится желтая стрелка, отпустите левую кнопку мыши.

7.1.2.4 Редактирование категории

При редактировании категории доступны следующие операции:

- редактирование параметров категории;
- добавление нового термина в категорию;
- редактирование термина, входящего в категорию;
- удаление термина из категории.

Чтобы отредактировать параметры категории:

1. Перейдите к разделу **Категории и термины**.
2. В дереве категорий выделите название нужной категории.
3. Выполните необходимое действие:

Необходимое действие	Порядок выполнения
Отредактировать параметры категории	1. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку  **Изменить** на панели категорий. • дважды щелкните левой кнопкой мыши по выделенной категории. 2. В открывшемся диалоговом окне **Категория** отредактируйте необходимые параметры (см. "Настройка параметров термина"). 3. Нажмите кнопку **Сохранить**.
Добавить в категорию новый термин	Порядок действий описан в подразделах: • Создание термина • Импорт терминов из файла • Перемещение термина из другой категории
Отредактировать параметры термина	1. В области просмотра параметров категории перейдите на вкладку **Термины**. 2. На панели терминов выделите нужный термин. 3. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Термин > Изменить**; • нажмите кнопку  **Изменить** на панели терминов; • дважды щелкните левой кнопкой мыши по выделенному термину. В открывшемся диалоговом окне **Термин** отредактируйте необходимые параметры (см. "Настройка параметров термина"). 4. Нажмите кнопку **Сохранить**.

Необходимое действие	**Порядок выполнения**
Удалить термин из категории	1. В области просмотра параметров категории перейдите на вкладку **Термины**. 2. На панели терминов выделите нужный термин. 3. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Термин > Удалить**; • нажмите кнопку **Удалить** на панели терминов; • щелкните по выделенной строке правой кнопкой мыши и в раскрывшемся меню выберите **Удалить**. 4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

7.1.2.5 Смена уровня вложенности категории

Чтобы изменить уровень вложенности категории:

1. Перейдите к разделу **Категории и термины**.
2. Выделите название нужной категории.
3. Выполните одно из следующих действий:
   - Чтобы понизить уровень категории, щелкните левой кнопкой мыши по названию той категории, которую нужно переместить. Затем, не отпуская левую кнопку мыши, подведите курсор к названию категории, которая будет родительской по отношению к перемещаемой категории. После того как слева от названия выбранной категории появится желтая стрелка, отпустите левую кнопку мыши.
   - Чтобы повысить уровень категории, нажмите и удерживайте клавишу **<SHIFT>**. Щелкните левой кнопкой мыши по названию той категории, которую нужно переместить. Затем, не отпуская левую кнопку мыши, подведите курсор мыши к названию любой категории, находящейся на том уровне, на который нужно переместить категорию. После того как слева от названия выбранной категории появится синяя стрелка, отпустите левую кнопку мыши.

   В результате выполнения одного из этих действий категория будет перемещена на выбранный уровень.

7.1.2.6 Настройка параметров термина

Параметры термина задают в диалоговом окне настройки термина.

Все параметры, за исключением параметров **Текст** и **Описание**, имеют значения по умолчанию. Значения по умолчанию задаются при настройке параметров категории и распространяются на все термины, принадлежащие этой категории.

В данном подразделе указаны стандартные значения по умолчанию, которые имеют параметры термина при

создании новой категории.

Общие параметры термина:

- **Текст**. Текст термина (обязательный параметр). Должен быть уникальным в пределах той категории, в состав которой он входит.

  Примечание

  При контентном анализе учитываются только алфавитные символы поддерживаемых языков.

- **Описание**. Дополнительная информация (необязательный параметр).

Параметры, влияющие на принятие решения о соответствии текста той категории, в которую входит термин:

- **Вес**. Степень того, насколько данный термин характеризует категорию. Значение – целое число в диапазоне от 0 до 25. По умолчанию вес термина имеет значение, заданное при настройке параметров категории (см. "Создание категории").

- Тип термина. Каждый термин может принадлежать только к одному типу. Чтобы указать тип термина установите флажок в поле **Характеристический** или **Дополнительный**. Если флажки в указанных полях сняты, термин считается *Обыкновенным* (значение по умолчанию).

  Примечание

  Описание типов терминов приведено в разделе "Основные принципы составления классификатора"

Правила поиска термина в тексте:

- **Морфология**. Данный параметр задает режим использования морфологии при поиске терминов в тексте. Может принимать следующие значения:

  - **any** – морфология используется. Поиск термина ведется с учетом словоформ;

  - **none** – морфология не используется. Термин будет найден только при полном совпадении.

  Значение по умолчанию **any**.

- **Капитализация**. Задает режим учета регистра символов (использование строчных/прописных букв) при поиске терминов в тексте. Может принимать следующие значения:

  - **any** – поиск ведется без учета регистра символов;

  - **native** – поиск выполняется с учетом регистра символов, заданного в образце.

    Важная информация!

    В результате выбора капитализации **native** будет отключено использование морфологии.

Возможны следующие варианты образцов:

Тип образца	Описание образца	Пример
lowercase	Каждое слово образца состоит из строчных букв (нижний регистр)	торговое соглашение

Тип образца	Описание образца	Пример
titlecase	Каждое слово образца начинается с прописной буквы	Смирнов Павел
uppercase	Каждое слово образца состоит из прописных букв (верхний регистр)	АКТ ПРИЕМКИ
nocase	Образец состоит из символов, регистр которых не учитывается (цифры, знаки пунктуации и т. п.)	256

При выборе капитализации **native** результаты поиска будут следующими («+» означает, что заданный термин будет найден):

Слово в тексте	Образец			
	lowercase	**titlecase**	**uppercase**	**nocase**
lowercase	+	–	–	–
titlecase	–	+	–	–
uppercase	–	–	+	–
nocase	–	–	–	+

- **no** – все буквы термина, найденного в тексте, должны быть строчными;
- **all** – все буквы термина, найденного в тексте, должны быть заглавными;
- **first** – первая буква термина, найденного в тексте, должна быть заглавной;
- **word** – первые буквы всех слов найденного термина должны быть заглавными.

Значение по умолчанию **any**.

- **Язык**. Язык термина. Значение по умолчанию **ru**.

7.1.2.7 Поиск термина

Чтобы найти термин:

1. Перейдите к разделу **Категории и термины**.
2. В дереве категорий выделите название той категории, по которой нужно выполнить поиск термина. Если название категории, к которой может принадлежать искомый термин, неизвестно, то выделите название любой категории.
3. В области просмотра параметров категории перейдите на вкладку **Термины**. В нижней части данной вкладки расположена панель **Поиск терминов**.

> **Примечание**
>
> Скрыть/отобразить панель **Поиск терминов** можно, воспользовавшись кнопкой **Найти**, расположенной в верхней части вкладки **Термины**.

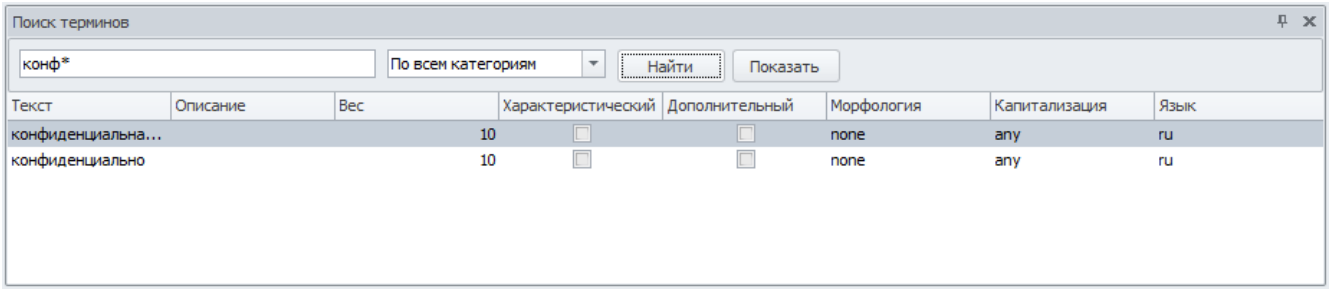
4. На панели **Поиск терминов** введите нужный термин в поле ввода слева.

> **Примечание**
>
> Поиск терминов ведется без учета регистра символов.
>
> При поиске термина вы можете использовать маски: «*» для замены нескольких символов и «?» для замены одного символа.
>
> Для поиска терминологических словосочетаний вводите все словосочетание целиком или используйте маски.

5. Из раскрывающегося списка, расположенного слева от кнопки **Найти**, выберите подходящий способ поиска:
   - **По всем категориям**. Поиск термина будет выполнен по всем категориям.
   - **В текущей категории**. Поиск термина будет выполнен только в пределах выбранной категории. При выборе данного варианта нужно предварительно выделить в дереве категорий ту категорию, по которой будет выполняться поиск термина.
6. После того как нужный вариант будет выбран, нажмите кнопку **Найти**.

Результаты поиска отображаются в области просмотра на панели **Поиск терминов**.

Чтобы перейти к категории, в состав которой входит найденный термин, выделите строку с этим термином и нажмите кнопку **Показать**.



Результаты поиска термина

7.1.2.8 Удаление категории

Чтобы удалить категорию:

1. Перейдите к разделу **Категории и термины**.
2. В дереве категорий выделите название нужной категории.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной на панели инструментов;

- щелкните по выделенной категории правой кнопкой мыши и в раскрывшемся меню выберите **Удалить**.

4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

7.1.2.9 Экспорт/импорт классификатора

Классификатор может быть экспортирован в указанное место на жестком диске, в сетевую папку или на сменный носитель информации. Классификатор экспортируется в виде XML-файла и впоследствии может быть снова загружен в Систему.

Примечание

Экспортируется классификатор, входящий в состав конфигурации со статусом **Редактируемая**.

Категории и термины экспортируются со всеми параметрами, за исключением примечаний к терминам.

Доступ к функциям экспорта/импорта классификатора осуществляется из раздела **Категории и термины** (область **Конфигурация** на панели **Навигация**).

Важная информация!

Если у вас уже есть классификатор, то в результате импорта новый классификатора будет добавлен к уже существующему. Если при этом в текущем классификаторе есть категории, имена которых совпадают с именами категорий из классификатора, то такие категории будут при импорте заменены.

Чтобы экспортировать классификатор:

1. Перейдите к разделу **Категории и термины**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Экспорт**;
   - нажмите кнопку **Экспорт** на панели категорий.
3. В диалоговом окне **Сохранить как** укажите папку, в которую будет сохранен классификатор, и имя XML-файла.
4. Нажмите кнопку **Сохранить**, чтобы экспортировать классификатор в XML-файл.

Чтобы импортировать классификатор:

1. Перейдите к разделу **Категории и термины**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Импорт**;
   - нажмите кнопку **Импорт** на панели инструментов.
3. В диалоговом окне **Открыть** выберите XML-файл, из которого будет импортирован классификатор.
4. Нажмите кнопку **Открыть**, чтобы начать импорт классификатора из XML-файла.

После завершения операции импорта, сведения о классификаторе появятся в разделе **Категории и термины**.

7.1.3 Списки

Список представляет собой набор элементов одного типа, который используется в сценарии при составлении правил анализа объекта (см. "Настройка сценария анализа объектов (LUA)").

Например, если известно несколько статических IP-адресов серверов, трафик от которых не может содержать конфиденциальную информацию (к примеру, они выполняют только автоматическое обновление ПО), то эти адреса могут быть объединены в специальный список. Затем в тексте сценария можно поместить условие, задающее проверку IP-адреса отправителя на принадлежность к этому списку (см. пример в разделе "Проверка вхождения строки в список").

Примечание

Наборы данных отправителей, получателей и рабочих станций (например, имена, e-mail адреса, домены и т.п.) настоятельно рекомендуется учитывать с помощью справочника сотрудников (см. "Справочник сотрудников") и использовать в сценарии с помощью методов, описанных в разделах "Проверка вхождения отправителя в группу", "Проверка вхождения получателя в группу", "Проверка вхождения рабочей станции в группу".

Списки объединяются в группы списков, которые также могут быть использованы при определении правил анализа объектов в тексте сценария.

В Системе есть предустановленные группы списков: *Типы файлов*, *Веб-ресурсы* и *Ресурсы*. Они используются для назначения объектам тегов из соответствующих предустановленных групп тегов *Типы файлов*, *Веб-ресурсы* и *Ресурсы*. Предустановленные списки не подлежат редактированию, однако некоторые входящие в них элементы доступны для изменения.

Примечание

Неизменяемые списки, элементы списков и группы списков внешне отличаются от изменяемых тем, что имеют в пиктограмме знак принадлежности к системным файлам - зубчатое колесо (шестерню).

Пример:

- *Неизменяемые* списки, элементы списков и группы списков.
- *Изменяемые* списки, элементы списков и группы списков.

Работа со списками ведется в разделе **Списки** (область **Конфигурация** на панели **Навигация**).

Правила работы со списками

1. Списки, включаемые в состав сценария, должны быть заданы в Консоли управления.
2. В список можно включить набор значений, относящихся к любому свойству, которое присваивается объекту в процессе анализа и обработки. Эти свойства описаны в модели данных InfoWatch Traffic Monitor (см. "Модель данных InfoWatch Traffic Monitor").
3. Все значения в списке должны быть однотипными. Например, не допускается объединять в одном списке IP-адреса и доменные имена хостов.

Более подробную информацию о работе со списками вы можете найти в следующих разделах:

- Создание группы списков
- Создание списка
- Создание элемента списка

- Редактирование списка или группы списков
- Просмотр и фильтрация элементов списка
- Удаление списка или группы списков

7.1.3.1 Создание группы списков

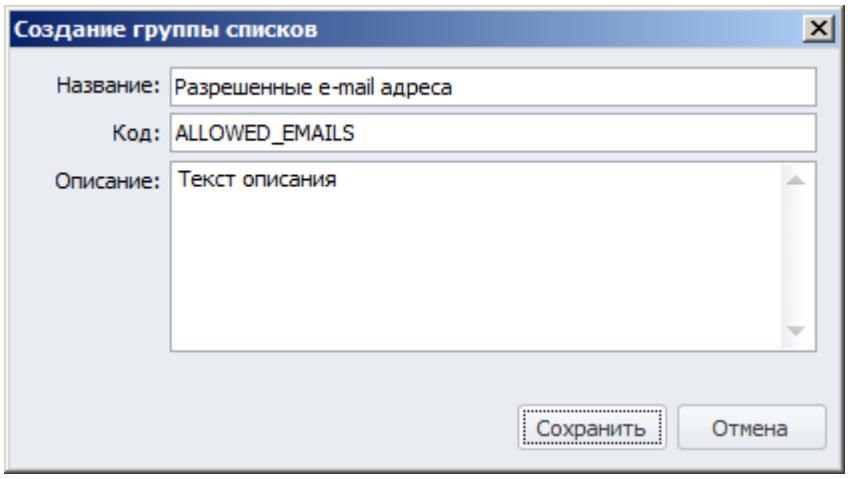
Примечание

В Системе может быть не более 4194304 групп списков.

Чтобы создать группу списков:

1. Перейдите к разделу **Списки**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Создать группу списков**.
   - нажмите кнопку **Создать группу списков** на панели групп списков.

   На экран будет выведено диалоговое окно **Создание группы списков**.



Создание группы списков

3. Укажите параметры группы списков:
   - **Название**. Наименование группы списков (обязательный параметр).
     Название должно быть уникальным.
   - **Код**. Название группы списков, которое будет использоваться при составлении сценария (обязательный параметр).
     Кодовое название группы списков может состоять из букв латинского алфавита, цифр и символа подчеркивания. Должно начинаться с буквы.
     Код группы списков должен быть уникальным.
   - **Описание**. Дополнительная информация о группе списков.
4. Нажмите кнопку **Сохранить**.

После того как группа списков будет создана, нужно наполнить её списками (см. "Создание списка").

Примечание

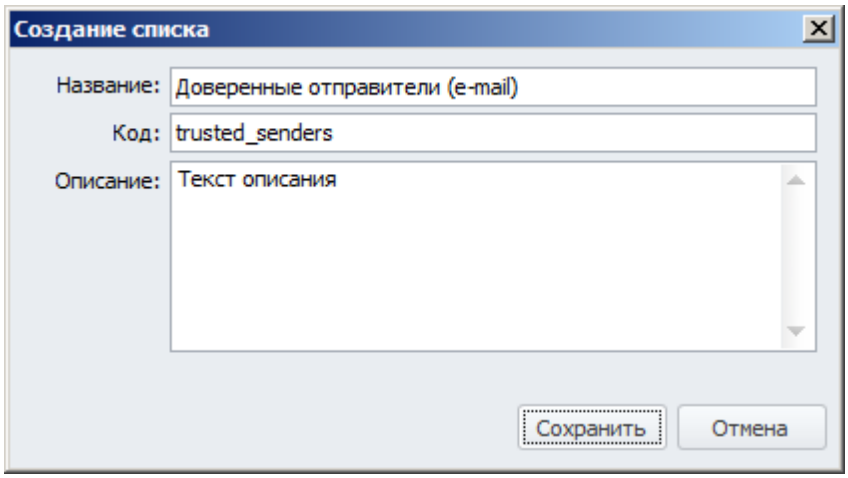
Вы можете наполнять группу списками, как создавая новые списки (см. "Создание списка"), так и перемещая списки между группами. Чтобы переместить список из одной группы в другую, щелкните левой кнопкой мыши по названию списка, который нужно переместить. Затем, не отпуская левую кнопку мыши, подведите курсор к названию группы, в которую этот список должен войти. После того как слева от названия выбранной группы появится желтая стрелка, отпустите левую кнопку мыши.

7.1.3.2 Создание списка

Чтобы создать список:

1. Перейдите к разделу **Списки**.
2. Если список должен входить в какую-либо группу списков, то выберите эту группу в перечне списков.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Создать список**;
   - нажмите кнопку **Создать список** на панели инструментов.

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



Настройка параметров списка

4. Укажите параметры списка:
   - **Название**. Наименование списка (обязательный параметр). Название должно быть уникальным.
   - **Код**. Название списка, которое будет использоваться при составлении сценария (обязательный параметр).
     Кодовое название списка может состоять из букв латинского алфавита, цифр и символа подчеркивания. Должно начинаться с буквы. Код должен быть уникальным.
   - **Описание**. Дополнительные сведения о списке.
5. Нажмите кнопку **Сохранить**.

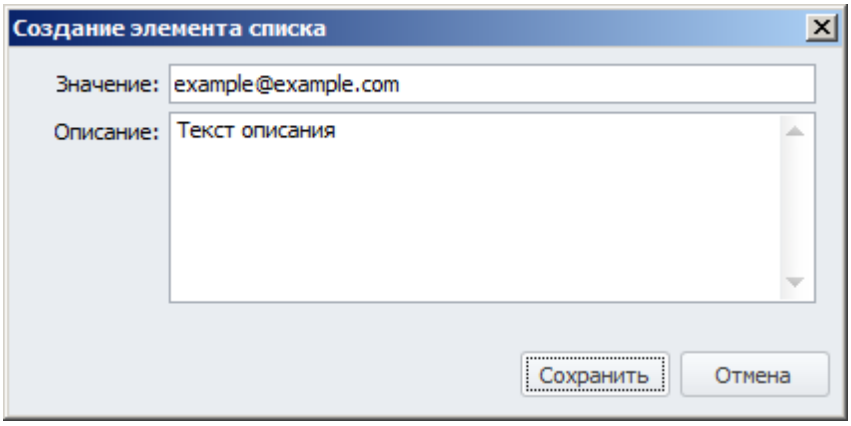
После того как новый список будет создан, нужно наполнить этот список данными (см. "Создание элемента списка").

7.1.3.3 Создание элемента списка

Чтобы создать элемент списка:

1. Перейдите к разделу **Списки**.
2. На панели списков выделите нужный список.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Элемент списка > Создать**;
   - на панели элементов списка нажмите кнопку **Создать**.

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



Настройка параметров элемента для списка

4. Укажите параметры элемента:
   - **Значение**. Значение элемента списка в формате, соответствующем типу списка (обязательный параметр).
   - **Описание**. Дополнительные сведения об элементе.
5. Нажмите кнопку **Сохранить**.

Повторите шаги 3-4, чтобы добавить в список другие элементы.

7.1.3.4 Редактирование списка или группы списков

При редактировании списков доступны следующие операции:

- редактирование параметров группы списков;
- редактирование параметров списка;
- добавление нового элемента в список;
- редактирование элемента, входящего в список;
- удаление элемента из списка.

Чтобы отредактировать список:

1. Перейдите к разделу **Списки**.

2. На панели списков выделите название нужного списка (группы списков).

3. Выполните необходимое действие:

Необходимое действие	Порядок выполнения
Отредактировать параметры списка (группы списков): название списка, код, описание	1. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку **Изменить** на панели списков. • дважды щелкните левой кнопкой мыши по выделенному списку (группе списков). 2. В открывшемся диалоговом окне **Список** или **Группа списков** отредактируйте необходимые параметры (см. "Создание группы списков"; "Создание списка"). 3. Нажмите кнопку **OK**.
Добавить в список новый элемент	См. "Создание элемента списка"
Отредактировать параметры элемента списка (значение, код, описание)	1. На панели элементов списка выделите нужный элемент списка. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Элемент списка > Изменить**; • нажмите кнопку **Изменить** на панели элементов списка. • дважды щелкните левой кнопкой мыши по выделенному элементу списка. В открывшемся диалоговом окне **Элемент списка** отредактируйте необходимые параметры (см. "Создание элемента списка"). 3. Нажмите кнопку **OK**.
Удалить элемент из списка	1. На панели элементов списка выделите нужный элемент списка. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Элемент списка > Удалить**; • нажмите кнопку **Удалить** на панели элементов списка; • щелкните по выделенной строке правой кнопкой мыши и в раскрывшемся меню выберите **Удалить**. 3. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление. **Примечание:** Исключите удаленный элемент из текста каждого сценария, в котором он использовался.

7.1.3.5 Просмотр и фильтрация элементов списка

При просмотре списков на панели элементов отображаются только первые 1000 элементов списка. Вы можете уточнить перечень отображаемых элементов списка с помощью функции фильтрации.

Чтобы отфильтровать список:

1. Перейдите к разделу **Списки**.
2. В дереве списков выделите название того списка, по которому нужно выполнить фильтрацию.
3. На панели элементов списка, в поле **Фильтр** введите шаблон фильтрации.

   Примечание

   Фильтрация элементов списка ведется без учета регистра символов.

   При задании шаблона фильтрации вы можете использовать маски: «*» для замены нескольких символов и «?» для замены одного символа.

4. После ввода шаблона нажмите кнопку **Применить**.

Результаты поиска отображаются в области просмотра на панели элементов списка.

Внизу панели элементов отображается информация о количестве элементов:

- **Показано** – количество показанных элементов списка;
- **По фильтру** – количество записей, удовлетворяющих заданному шаблону фильтрации;
- **Всего** – общее количество элементов в выбранном списке.

При переходах между списками используемый шаблон сохраняется; для отмены фильрации очистите поле **Фильтр** и нажмите .

7.1.3.6 Удаление списка или группы списков

Чтобы удалить список (группу списков):

1. Перейдите к разделу **Списки**.
2. На панели списков выделите название нужного списка (группы списков).
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку **Удалить** на панели списков;
   - щелкните по выделенной строке правой кнопкой мыши и в раскрывшемся меню выберите **Удалить**.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

Примечание

Исключите удаленный список (группу списков) из текста каждого сценария, в котором он использовался.

7.1.4 Сценарий анализа объектов

Сценарий – это совокупность правил, в соответствии с которыми проводится анализ и обработка всех объектов, перехваченных Системой. Работа со сценариями анализа объектов ведется в разделе **Скрипты** (область **Конфигурация** на панели **Навигация**).

После установки в Консоли управления присутствует сценарий по умолчанию, который является активным. Активный сценарий (отмечен пиктограммой ) используется для анализа объектов на Traffic Monitor Server. Остальные сценарии являются неактивными (отмечены пиктограммой ). Для изменения правил проверки объектов на Traffic Monitor Server вам нужно настроить и активировать собственный сценарий.



Важная информация!

Для составления сценария используется язык программирования Lua. О принципах составления сценария см. "Настройка сценария анализа объектов (LUA)".

Более подробную информацию о работе с сценариями вы можете найти в следующих разделах:

- Создание сценария
- Загрузка сценария из файла
- Редактирование сценария
- Активирование сценария
- Сохранение сценария в файл
- Удаление сценария

7.1.4.1 Создание сценария



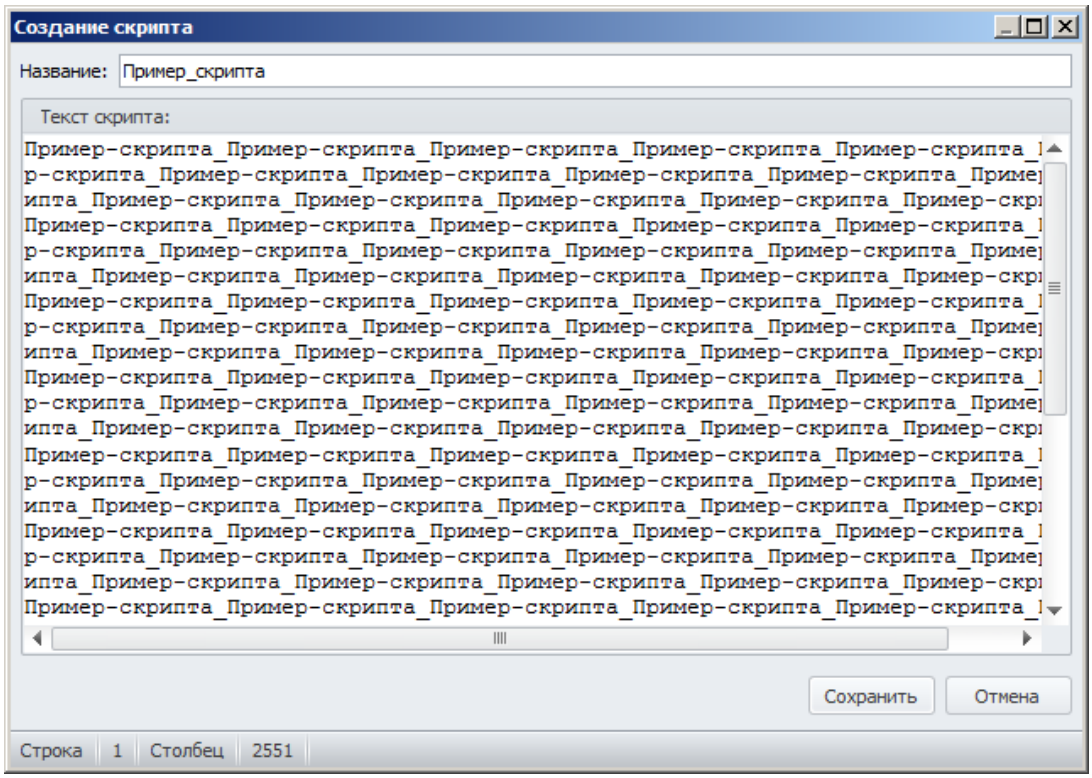
Важная информация!

Конфигурация может содержать несколько сценариев. Но в каждый момент времени активным может быть только один сценарий.

Чтобы создать сценарий:

1. Перейдите к разделу **Скрипты**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Создать скрипт**;
   - нажмите кнопку  **Создать** на панели инструментов.

   На экран будет выведено диалоговое окно **Создание скрипта**.



Настройка сценария

3. Настройте общие параметры сценария:
   - **Название**. Название сценария (обязательный параметр). Название должно быть уникальным.
   - **Текст скрипта**. В текстовом поле введите текст сценария.

> **Важная информация!**
>
> Для составления сценария используется язык программирования Lua. О принципах составления сценария см. "Настройка сценария анализа объектов (LUA)".

   Текст сценария может быть довольно большим, поэтому для удобства работы вы можете использовать поиск по тексту, а также замены. Нажмите сочетание клавиш **Ctrl + F**: будет открыто стандартное окно Windows для поиска по тексту.

4. Нажмите кнопку **Сохранить**.

7.1.4.2 Загрузка сценария из файла

Сценарии анализа объектов, хранящиеся в файлах (см. "Сохранение сценария в файл"), могут быть снова загружены в Консоль управления.

Чтобы загрузить сценарий из файла:

1. Перейдите к разделу **Скрипты**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Загрузить из файла**;

- нажмите кнопку  **Загрузить из файла** на панели инструментов.

3. В диалоговом окне **Открыть** выберите LUA-файл, из которого будет загружен сценарий.
4. Нажмите кнопку **Открыть**, чтобы начать импорт сценария из LUA-файла.

7.1.4.3 Редактирование сценария

Чтобы отредактировать сценарий:

1. Перейдите к разделу **Скрипты**.
2. В списке сценариев выделите строку с нужным сценарием.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Изменить**;
   - нажмите кнопку  **Изменить** на панели инструментов;
   - дважды щелкните левой кнопкой мыши по названию выделенного правила.
4. В диалоговом окне **Редактирование скрипта** отредактируйте параметры сценария. Вы можете изменять название или текст сценария.



Важная информация!

Для составления сценария используется язык программирования Lua. О принципах составления сценария см. "Настройка сценария анализа объектов (LUA)".

Текст сценария может быть довольно большим, поэтому для удобства работы вы можете использовать поиск по тексту, а также замены. Нажмите сочетание клавиш **Ctrl + F**: будет открыто стандартное окно Windows для поиска по тексту.

5. Когда в сценарий будут внесены необходимые изменения, нажмите кнопку **Сохранить**.

7.1.4.4 Активирование сценария

Конфигурация может содержать несколько сценариев. Однако в составе конфигурации на Traffic Monitor Server будет загружаться только один сценарий – тот, который в данный момент времени является активным.

Чтобы активировать сценарий:

1. Перейдите к разделу **Скрипты**.
2. В списке сценариев выделите строку со сценарием, который нужно активировать.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Активировать**;
   - нажмите кнопку  **Активировать** на панели инструментов.

В результате выбранный сценарий станет активным, а остальные сценарии будут находиться в неактивном состоянии.

7.1.4.5 Сохранение сценария в файл

Вы можете сохранять сценарии на жесткий диск, в сетевую папку или на сменный носитель информации. Сценарий сохраняется в виде файла, имеющего формат LUA, и впоследствии может быть снова загружен в Систему (см. "Загрузка сценария из файла").

Чтобы сохранить сценарий в файл:

1. Перейдите к разделу **Скрипты**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Сохранить в файл**;
   - нажмите кнопку **Сохранить в файл** на панели инструментов.
3. В диалоговом окне **Сохранить как** укажите папку, в которую будет сохранен сценарий, и имя LUA-файла.
4. Нажмите кнопку **Сохранить**, чтобы сохранить сценарий в LUA-файл.

7.1.4.6 Удаление сценария

Чтобы удалить сценарий:

1. Перейдите к разделу **Скрипты**.
2. В списке сценариев выделите строку с нужным сценарием.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку **Удалить** на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

7.1.5 Текстовые объекты

Текстовые объекты – это данные, имеющие фиксированную структуру. К таким объектам относятся номера паспортов, кредитных карт, телефонные номера, адреса электронной почты, номера социального страхования, реквизиты банковских счетов, коды по различным классификаторам (ОКПО, ОКАТО и пр.), регистрационные номера (ОГРН, ОГРНИП) и пр.

Система позволяет обнаруживать текстовые объекты при контентном анализе текста путем поиска по заранее определенным шаблонам. В системе имеется ряд предустановленных шаблонов для наиболее часто используемых типов текстовых объектов. Чтобы выполнять поиск текстовых объектов по этим шаблонам, необходимо включить их в конфигурацию, загружаемую на хост. О включении текстовых объектов и исключении их из конфигурации см. п. "Включение и выключение текстового объекта и его значений"; о порядке загрузки конфигурации на хост см. "Загрузка конфигурации на хосты".

Пример:

В конфигурации, загруженной на хост, включен только тип текстового объекта *Электронный адрес*.

Проверяется текст письма, содержащий такие строки:

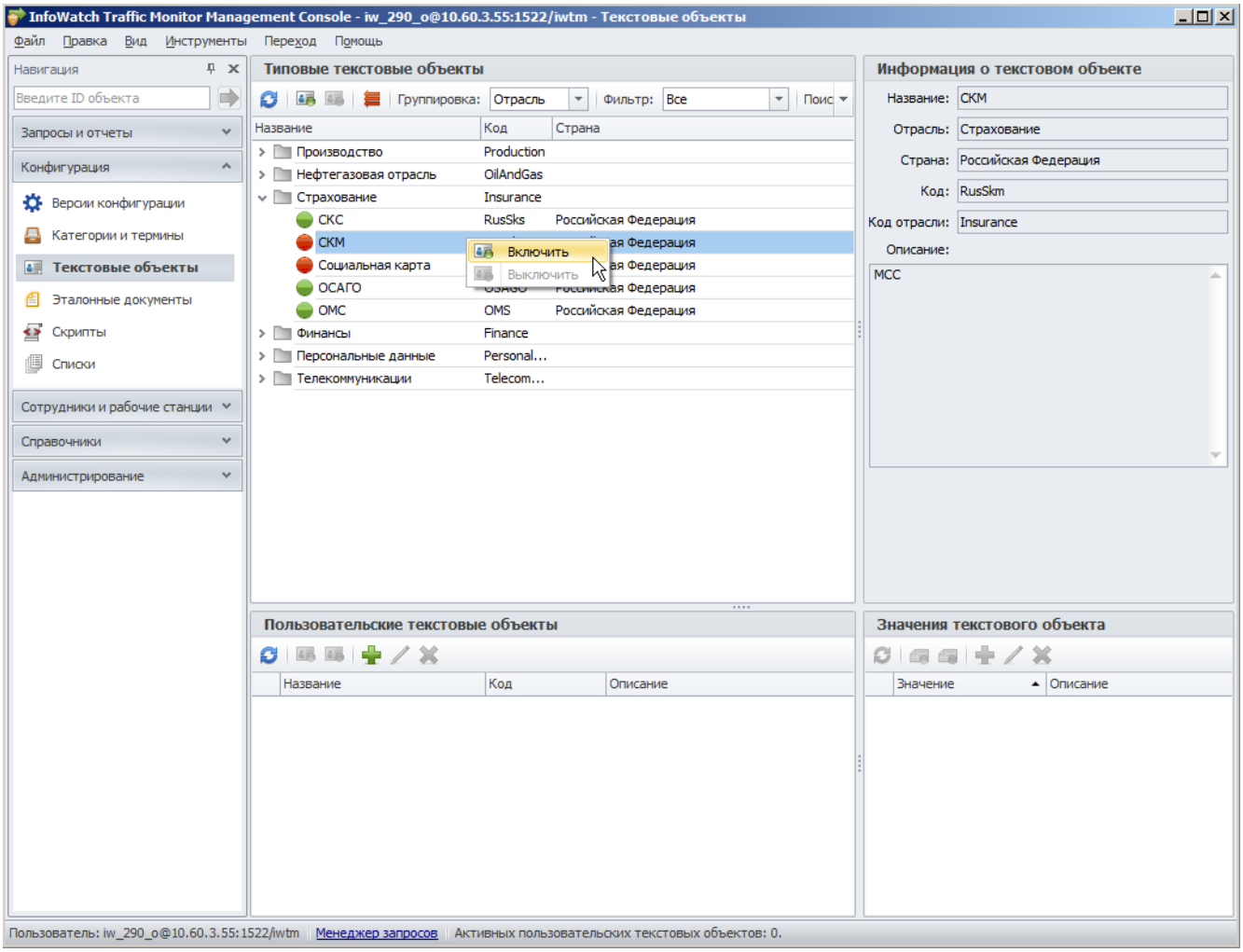
Сообщаю интересующие вас данные: belov@company.com, т. 357-4555, sedov@company.ru, т. 357-3586.

По результатам анализа в письме будут детектированы два текстовых объекта с типом *Электронный адрес*:

belov@company.com

sedov@company.ru

Номера телефонов *357-4555* и *357-3586* не будут детектированы, так как в конфигурации на сервере не включен тип текстового объекта *Номер телефона*.



Раздел Текстовые объекты

Работа с текстовыми объектами ведется в разделе **Текстовые объекты** (область **Конфигурация** на панели **Навигация**).

В Системе предусмотрено два вида текстовых объектов:

- **Типовые текстовые объекты** – являются предустановленными, не доступны для удаления или редактирования. Вы может только включать их в конфигурацию и исключать из неё.
- **Пользовательские текстовые объекты** – создаются пользователями, доступны для всех операций.

На панели **Информация о типовых текстовых объектах** представлены данные о выбранном типовом

текстовом объекте:

- **Название** - наименование объекта в Системе;
- **Отрасль** - принадлежность объекта к финансовой, производственной или другой отрасли;
- **Страна** - государство, к которому относится объект;
- **Код** - уникальный идентификатор объекта;
- **Код отрасли** - уникальный идентификатор отрасли объекта;
- **Описание** - поясняющая информация об объекте.

Более подробную информацию о работе с текстовыми объектами вы можете найти в следующих разделах:

- Создание и редактирование пользовательского текстового объекта
- Добавление значения пользовательского объекта
- Включение и выключение текстового объекта и его значений
- Удаление пользовательского текстового объекта или его значения

7.1.5.1 Загрузка типовых текстовых объектов из XML-файлов

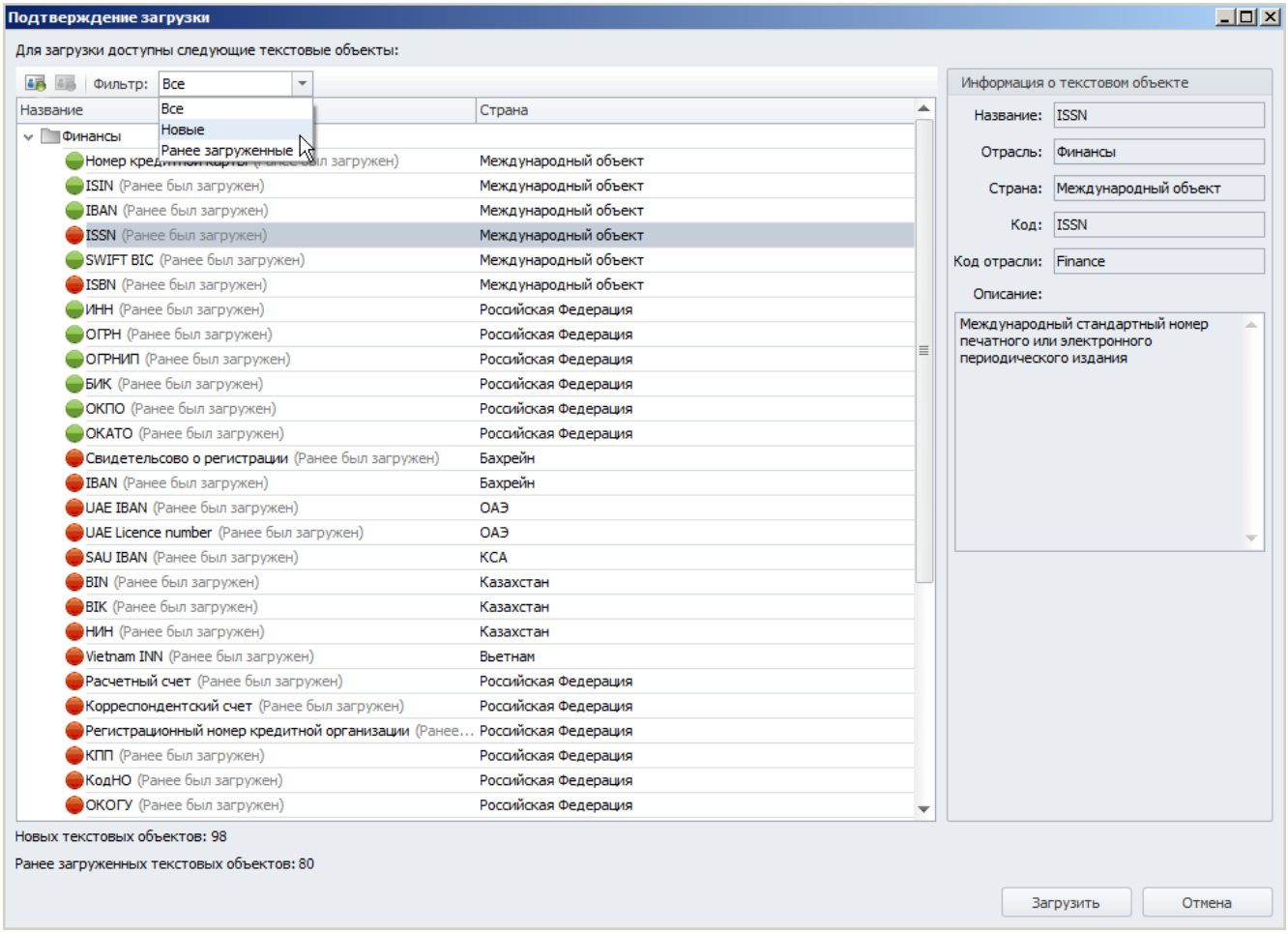
Типовые текстовые объекты, хранящиеся в файлах с расширением XML, могут быть загружены в Консоль управления. XML-файлы могут поставляться в рамках обновлений или по заказу.

Чтобы загрузить типовые текстовые объекты из XML файла:

1. Перейдите к разделу **Текстовые объекты**.
2. Нажмите кнопку **Загрузить из файла** на панели инструментов.
3. В диалоговом окне **Открыть** выберите XML-файл, из которого будет загружен объект.
4. Нажмите кнопку **Открыть**, чтобы начать импорт объекта из XML-файла.
5. В появившемся списке выберите нужный объект или группу объектов.
6. Нажмите **Загрузить**, чтобы добавить выбранные файлы в Консоль управления.

В диалоговом окне **Подтверждение загрузки**, поле **Фильтр**, можно настроить осуществить фильтрацию, чтобы отображались и использовались для загрузки:

- все объекты;
- новые;
- ранее загруженные.



Выбор типа фильтрации

Также любой из *новых* обектов можно загружать уже включенным или выключенным из анализа (см. " Включение и выключение типового текстового объекта"). Для этого определите статус выбранного объекта, нажав на кнопку **Включить** или **Выключить** на панели инструментов. По умолчанию новые объекты выключены.

Примечание

Ранее загруженные типовые текстовые объекты при загрузке нельзя включить или выключить.

7.1.5.2 Создание и редактирование пользовательского текстового объекта

Примечание

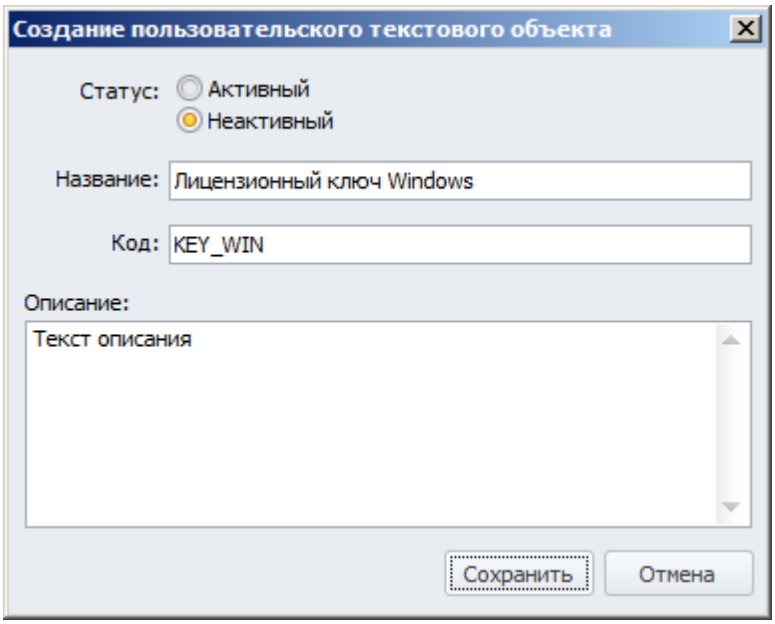
Типовые текстовые объекты не доступны для редактирования.

Чтобы создать или отредактировать текстовый объект:

1. Перейдите к разделу **Текстовые объекты**.
2. Выполните необходимые действия:

Действие	**Порядок выполнения**
Создать текстовый объект	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Пользовательские текстовые объекты > Добавить** • в области **Пользовательские текстовые объекты** нажмите кнопку **Добавить** на панели инструментов
Отредактировать текстовый объект	1. В списке пользовательских текстовых объектов выделите строку с нужной записью. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Пользовательские текстовые объекты > Редактировать**; • в области **Пользовательские текстовые объекты** нажмите кнопку **Редактировать** на панели инструментов; • дважды щелкните левой кнопкой мыши по выделенной строке.

На экран будет выведено диалоговое окно с параметрами текстового объекта.



Пользовательский текстовый объект

3. Укажите параметры текстового объекта.

- **Статус**. Если вы хотите, чтобы после загрузки конфигурации на Сервер контентного анализа текстовый объект мог использоваться в сценарии для поиска соответствующего текста, то установите флажок в поле **Активный**.
- **Название**. Имя текстового объекта.
- **Код**. Обозначение текстового объекта, которое будет использоваться при составлении сценария (обязательный параметр).

  Код может состоять из букв латинского алфавита, цифр и символа подчеркивания. Должен начинаться с буквы. Должен быть уникальным.
- **Описание**. Дополнительная информация по текстовому объекту.

4. Нажмите кнопку **Сохранить**.

Для созданного пользовательского текстового объекта также необходимо задать его значения, как описано в разделе "Добавление значения пользовательского объекта".

Чтобы Система осуществляла поиск активных текстовых объектов, необходимо загрузить обновленную конфигурацию на хост. О порядке действий см. "Загрузка конфигурации на хосты".

7.1.5.3 Добавление значения пользовательского объекта

Важная информация!

Для каждого пользовательского объекта может быть не более 256 активных значений.

Чтобы создать или отредактировать элемент в списке значений пользовательского объекта:

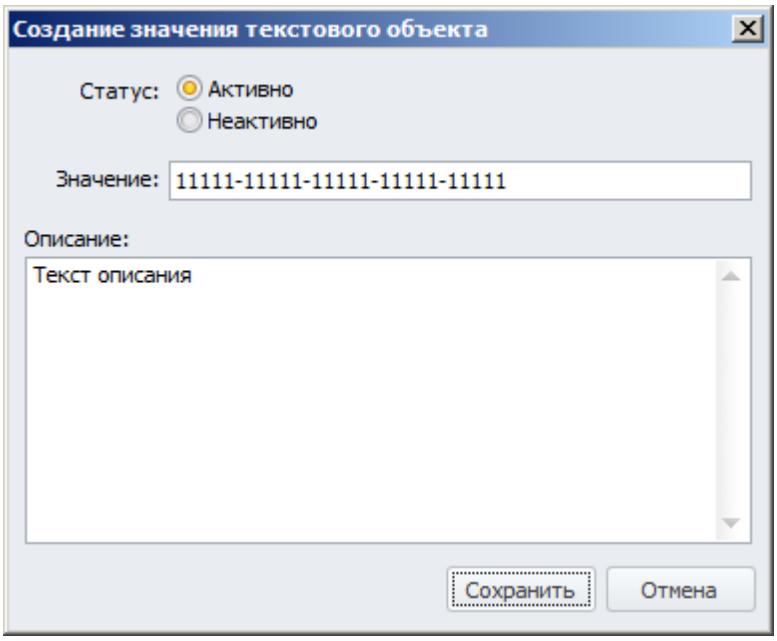
1. Перейдите к разделу **Текстовые объекты**.

2. В области **Пользовательские текстовые объекты** выделите нужный пользовательский текстовый объект.

3. Выполните необходимые действия:

Действие	Порядок выполнения
Создать значение текстового объекта	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Значения текстового объекта > Добавить** • на панели инструментов области **Значения текстового объекта** нажмите кнопку **Добавить**
Отредактировать значение текстового объекта	1. В области **Значения текстового объекта** выделите строку с нужной записью. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Значения текстового объекта > Редактировать**; • на панели инструментов области **Значения текстового объекта** нажмите кнопку **Редактировать**; • дважды щелкните левой кнопкой мыши по выделенной строке.

На экран будет выведено диалоговое окно с параметрами значения текстового объекта.



Значение текстового объекта

4. Укажите параметры элемента:
   - **Статус**. Если вы хотите, чтобы после загрузки конфигурации на Сервер контентного анализа значение текстового объекта могло использоваться в сценарии для поиска соответствующего текста, то установите флажок в поле **Активно**.
   - **Значение**. Значение текстового объекта.
   - **Описание**. Дополнительные сведения о значении.
5. Нажмите кнопку **Сохранить**.

Повторите шаги 3-5, чтобы добавить другие значения.

Чтобы Система осуществляла поиск активных значений текстовых объектов, необходимо загрузить обновленную конфигурацию на хост. О порядке действий см. "Загрузка конфигурации на хосты".

7.1.5.4 Включение и выключение текстового объекта и его значений

Важная информация!

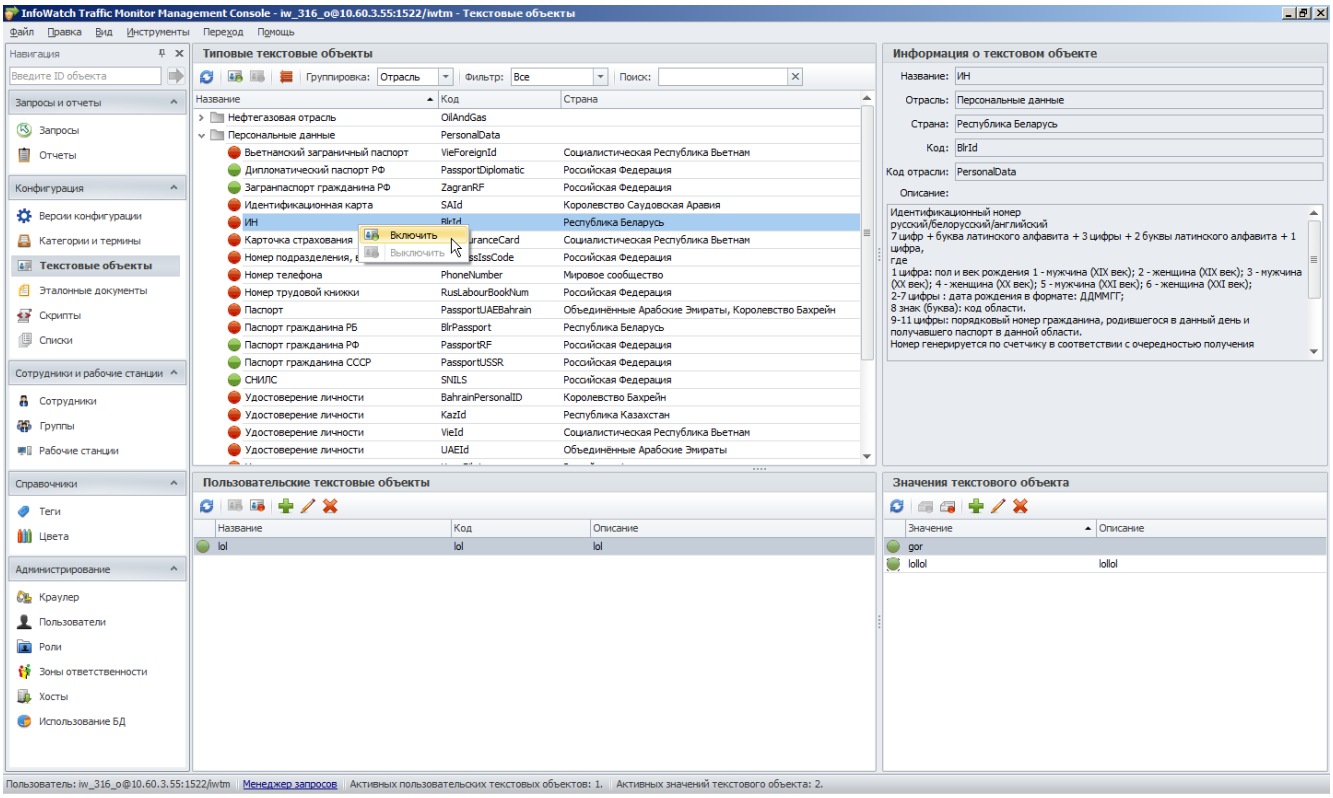
В каждом списке текстовых объектов (типовых либо пользовательских) может быть не более 256 активных объектов.

Чтобы включить текстовый объект в конфигурацию:

1. На панели текстовых объектов выделите один или несколько текстовых объектов.
2. Выполните одно из следующих действий:
   - щелкните на выбранном объекте правой кнопкой мыши, и в раскрывшемся контекстном меню выберите пункт **Включить**;
   - нажмите кнопку в верхней части панели текстовых объектов
   - в главном меню выберите команду **Правка > Типовые текстовые объекты > Включить** (для

типовых текстовых объектов) или **Правка > Пользовательские текстовые объекты > Включить** (для пользовательских текстовых объектов).

Текстовый объект получит статус *Активный*.



Включение типового текстового объекта

Чтобы исключить текстовый объект из конфигурации:

1. На панели текстовых объектов выделите один или несколько текстовых объектов.
2. Выполните одно из следующих действий:
   - нажмите кнопку в верхней части панели текстовых объектов.
   - щелкните на выбранном объекте правой кнопкой мыши, и в раскрывшемся контекстном меню выберите пункт **Выключить**;
   - в главном меню выберите команду **Правка > Типовые текстовые объекты > Выключить** (для типовых текстовых объектов) или **Правка > Пользовательские текстовые объекты > Выключить** (для пользовательских текстовых объектов).

Текстовый объект получит статус *Неактивный*.

Важная информация!

Для каждого пользовательского объекта может быть не более 256 активных значений.

Чтобы включить значение пользовательского текстового объекта в конфигурацию:

1. В области **Пользовательские текстовые объекты** выделите текстовый объект, значение которого вы хотите включить.
2. В области **Значения текстовых объектов** выберите необходимое значение.
3. Выполните одно из следующих действий:

- на панели области **Значения текстовых объектов** нажмите кнопку .
- щелкните на выбранном значении правой кнопкой мыши, и в раскрывшемся контекстном меню выберите пункт **Включить**;
- в главном меню выберите команду **Правка > Значения текстового объекта > Включить**.

Если текстовый объект, значение которого активируется, сам является неактивным, то поиск по таким значениям производиться не будет. Поэтому в такой ситуации Система отобразит сообщение, предлагающее активировать сам текстовый объект. Чтобы активировать текстовый объект, нажмите **Да**.

Значение текстового объекта получит статус *Активно*.

7.1.5.5 Удаление пользовательского текстового объекта или его значения

Примечание

Типовые текстовые объекты не доступны для удаления.

Чтобы удалить значение текстового объекта:

1. Перейдите к разделу **Текстовые объекты**.
2. В области **Пользовательские текстовые объекты** выделите строку с нужной записью.
3. В области **Значения текстовых объектов** выберите необходимое значение.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Значения текстового объекта > Удалить**;
   - на панели области **Значения текстовых объектов** нажмите кнопку **Удалить**;
   - щелкните на выбранном значении правой кнопкой мыши, и в раскрывшемся контекстном меню выберите пункт **Удалить**.
5. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

Чтобы удалить текстовый объект:

1. Перейдите к разделу **Текстовые объекты**.
2. В области **Пользовательские текстовые объекты** выделите строку с нужной записью.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Пользовательские текстовые объекты > Удалить**;
   - на панели области **Пользовательские текстовые объекты** нажмите кнопку **Удалить**.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

7.1.5.6 Группировка и фильтрация записей

Для удобства просмотра типовых текстовых объектов реализованы функции группировки и фильтрации.

Существует два типа группировки объектов: территориальный (Страна) и тематический (Отрасль). По умолчанию объекты сгруппированы по параметру Отрасль.

Чтобы сгруппировать записи,

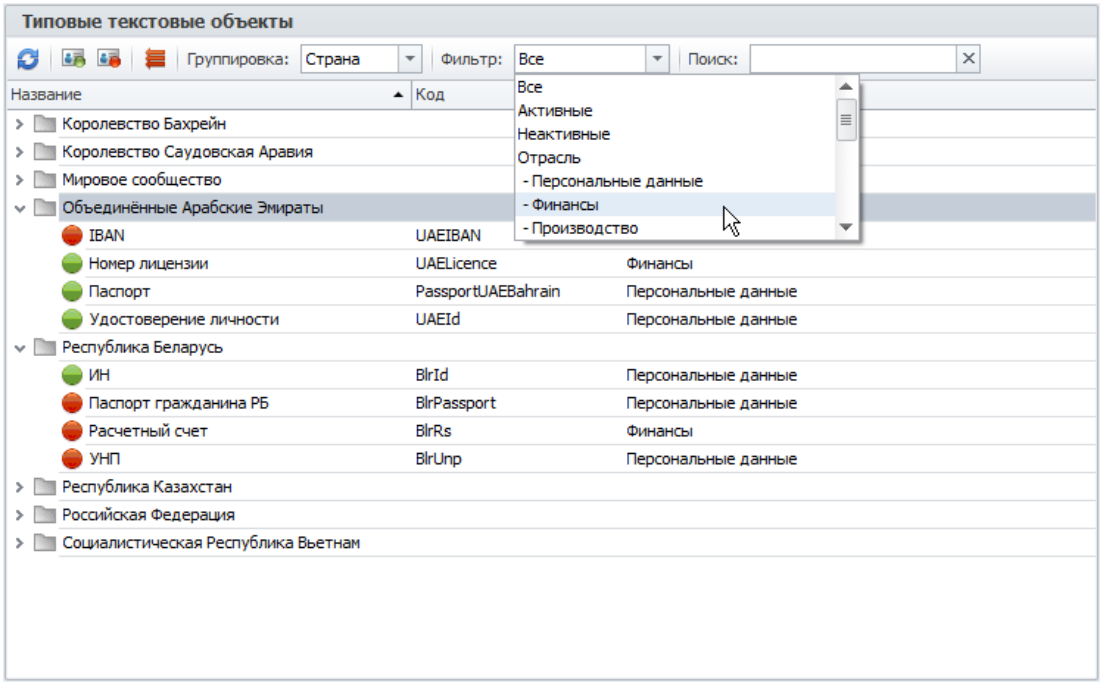
на панели управления панели типовых текстовых объектов выберите из раскрывающегося списка нужный параметр группировки.

Для того чтобы отсеивать объекты, просматривать которые нет необходимости, применяется фильтрация. По умолчанию выбран тип фильтрации "Все", и Система отображает все объекты согласно группировке. Вы можете применить также другие типы фильтрации:

- только активные;
- только неактивные;
- соответствующие одной из отраслей;
- соответствующие одной из стран.

Чтобы отфильтровать записи,

на панели управления панели типовых текстовых объектов выберите из раскрывающегося списка нужный параметр фильтрации.



Группировка и фильтрация записей

Записи на панели отображаются в свернутом виде. Чтобы развернуть группу, нажмите на кнопку, расположенную слева от значения параметра группировки. Чтобы свернуть группу, нажмите на кнопку.

7.1.6 База эталонных документов

База эталонных документов – это набор типовых документов, которые применяются в технологии *Цифровые отпечатки*. При использовании этой технологии в тексте перехваченных объектов (письма, файлы, задания на печать и пр.) ищутся цитаты из базы эталонных документов. В качестве эталонных документов могут использоваться тексты, относящиеся к конфиденциальной документации компании (например, тексты приказов, финансовых отчетов, договоров и пр.): в результате создания цифровых отпечатков эталонные документы недоступны для просмотра ни пользователям, ни администраторам Системы.

Важная информация!

При наличии в Системе нескольких хостов (см. "Работа с хостами"), анализ цифровых отпечатков с использованием эталонных документов может выполняться только на одном из них.

Более подробную информацию о работе с базой эталонных документов вы можете найти в следующих разделах:

- Составление базы эталонных документов
- Редактирование информации об эталонном документе
- Удаление эталонного документа
- Группировка записей

7.1.6.1 Составление базы эталонных документов

Составление базы эталонных документов подразумевает:

1. Добавление эталонных документов.
2. Снятие цифровых отпечатков с эталонных документов.

Важная информация!

В результате снятия цифрового отпечатка в базе данных сохраняется не сам документ, а отдельные цитаты из него, причем в зашифрованном виде и без возможности восстановить исходный документ по цитатам из него. Это обеспечивает безопасность конфиденциальной информации, которая может содержаться в эталонных документах.

Работа с базой эталонных документов ведется в разделе **Эталонные документы** (область **Конфигурация** на панели **Навигация**).

Чтобы добавить один или несколько эталонных документов в базу:

1. Выполните одно из следующих действий:
   - в главном меню выберите команду Правка > Добавить эталонный документ;
   - нажмите кнопку Добавить эталонный документ на панели инструментов панели эталонных объектов.
2. В открывшемся диалоговом окне выделите один или несколько документов, которые нужно загрузить в базу как эталонные. Вы можете выделять несколько документов, удерживая клавишу Shift или Ctrl.

> **Примечание**
>
> По умолчанию, добавленный файл не должен превышать 128 Мб. При добавлении документа, превышающего допустимый размер, отображается соответствующее предупреждение. Корректировка максимально допустимого размера выполняется администратором системы: см. документ *«InfoWatch Traffic Monitor. Руководство администратора»*.

3. Нажмите кнопку **Открыть**.

В результате документ будет включен в базу со статусом *Новый*. Также эталонному документу автоматически присваиваются значения параметров **ID**, **Путь**, **Имя файла**, **Статус**, **Размер**, **Тип**, **Создан** (дата и время создания), **Добавлен** (дата и время добавления документа в базу).

Поля **Название**, **Автор** и **Описание** по умолчанию не заполнены. При необходимости вы можете добавить информацию в эти поля (см. "Редактирование информации об эталонном документе").

> **Примечание**
>
> Для некоторых типов документов (таких как, документы Word) информация о названии и авторе извлекается из свойств документа в процессе создания цифрового отпечатка.

Для того чтобы использовать эталонный документ при анализе текста, необходимо снять с этого документа цифровой отпечаток.

Чтобы создать цифровые отпечатки для всех эталонных документов со статусом *Новый*,

выполните одно из следующий действий:

- в главном меню выберите команду **Правка > Создать эталонные документы**;
- нажмите кнопку **Создать эталонные документы** в верхней части панели эталонных документов.

В результате успешного завершения процесса эталонному документу будет присвоен статус *Цифровой отпечаток готов*. Если цифровой отпечаток создать не удалось, эталонному документу будет присвоен статус *Ошибка обработки*.

> **Важная информация!**
>
> Если статус сопровождается пиктограммой или , вы можете щелкнуть левой кнопкой мыши на статусе документа: будет отображено информационное сообщение с описанием проблем, возникших при формировании цифрового отпечатка.

7.1.6.2 Редактирование информации об эталонном документе

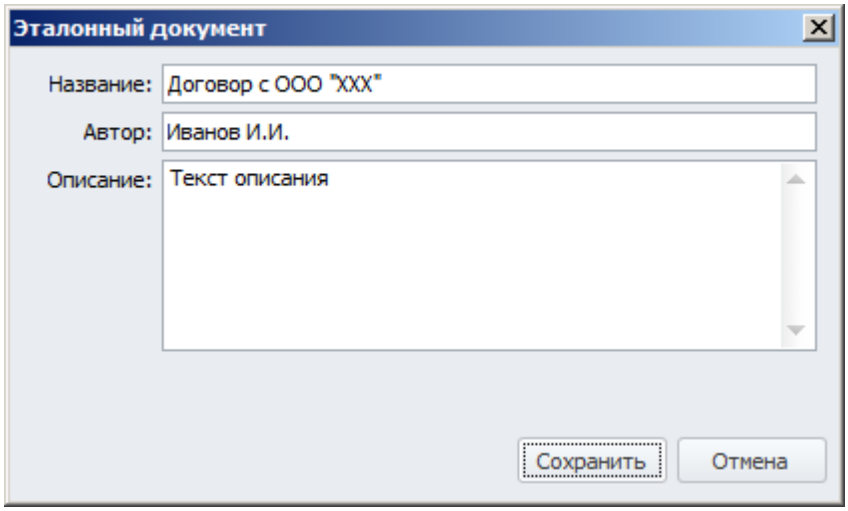
Вы можете редактировать информацию о документах, находящихся в любом статусе.

Чтобы отредактировать информацию об эталонном документе:

1. Перейдите к разделу **Эталонные документы**.
2. На панели эталонных документов выделите нужный эталонный документ.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Изменить**;

- нажмите кнопку **Изменить** в верхней части панели эталонных документов;
- дважды щелкните левой кнопкой мыши по выделенному документу.

На экран будет выведено диалоговое окно **Эталонный документ**.



Добавление эталонного документа в базу

4. Укажите параметры эталонного документа:
   - **Название**. Название в базе эталонных документов.
   - **Автор**. Пользователь, загрузивший эталонный документ в базу.
   - **Описание**. Дополнительная информация.
5. Нажмите кнопку **Сохранить**.

7.1.6.3 Удаление эталонного документа

Удаление эталонного документа может производиться в двух случаях:

- Если цифровой отпечаток для данного документа ещё не был создан и, следовательно не мог ранее использоваться при анализе. Это относится к документам со статусом *Новый* и *Ошибка обработки*. В таком случае вы можете полностью удалить и документ, и запись о нём.
- Документы с любыми другими статусами (*Ожидает обработки, Обрабатывается, Цифровой отпечаток готов*, *Ошибка удаления*) могут быть удалены, однако запись о них останется для корректного отображения информации о ранее проанализированных объектах. Такие эталонные документы в результате удаления получают статус *Удален*, и они больше не используются при анализе текста

Важная информация!

Невозможно возобновить использование удаленного документа. Если вам снова потребуется использовать удаленный эталонный документ, то повторно загрузите его в базу и снимите с него цифровой отпечаток (см. "Составление базы эталонных документов").

Чтобы удалить эталонный документ:

1. Перейдите к разделу **Эталонные документы**.

2. На панели эталонных документов выделите нужный эталонный документ.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку **Удалить** в верхней части панели эталонных документов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

7.1.6.4 Группировка записей

Для удобства просмотра записей в большой таблице вы можете использовать группировку. Группирование выполняется по одному или нескольким параметрам записи: заголовкам (колонкам) таблицы. Данная возможность доступна только в разделе **Эталонные документы**.

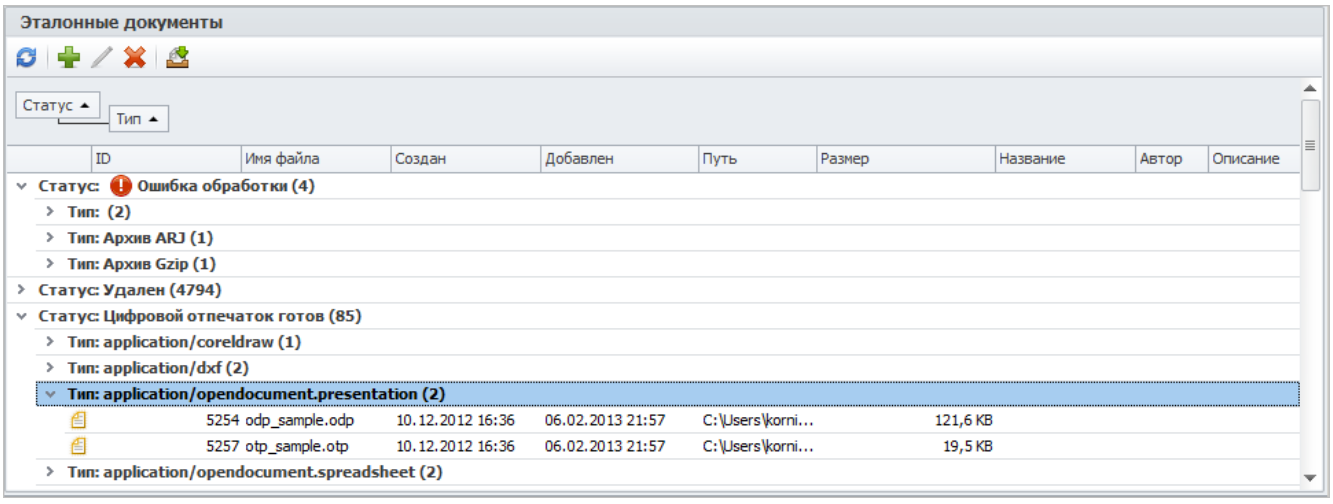
Чтобы сгруппировать записи:

1. В строке с заголовками таблицы щелкните левой кнопкой мыши по нужному параметру.
2. Не отпуская кнопку, перетащите заголовок колонки на панель группировки. Название параметра, по которому производилось группирование записей, будет отображено на панели группировки.

Чтобы сгруппировать записи по нескольким заголовкам, повторите шаги 1 – 2 для всех заголовков, которые должны участвовать в группировании.

Примечание:

Порядок группирования записей можно изменить, меняя местами заголовки. Первым в группировании участвует колонка, заголовок которой расположен слева вверху.



Сгруппированные записи отображаются в свернутом виде. Чтобы развернуть группу, нажмите на кнопку , расположенную слева от значения параметра группировки. Чтобы свернуть группу, нажмите на кнопку .

Вы можете отменить группирование по одному или нескольким параметрам, удаляя заголовки из схемы группировки.

Чтобы отменить группирование записей по какому-либо параметру:

1. На панели группировки щелкните левой кнопкой мыши по заголовку, который вы хотите удалить из схемы, и, не отпуская кнопку, перетащите его в строку заголовков таблицы. Местоположение столбца при этом будет указываться двумя стрелками.
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.

7.1.7 Зоны ответственности: разграничение доступа к объектам

Зоны ответственности используются для того, чтобы разграничить доступ пользователей к перехваченным объектам. Объекты, принадлежащие какой-либо зоне ответственности, будут видны только тем пользователям, которые входят в эту зону ответственности (при условии, что пользователь имеет привилегии на просмотр и/или работу с объектами).

Для настройки и управления зонами ответственности предназначен раздел **Зоны ответственности** (область **Администрирование** на панели **Навигация**).

Каждый объект одновременно может находиться только в одной зоне ответственности. Принадлежность объекта к той или иной зоне ответственности определяется исходя из условий для помещения объекта в зону ответственности (обнаружение атрибутов категорий, групп AD или TM, тегов, текстовых объектов или эталонных документов) (см. "Создание и редактирование зоны ответственности") и с учетом их приоритетов (см. "Изменение приоритетов для зон ответственности"). Обработанные Системой объекты можно перемещать из одной зоны ответственности в другую (см. "Перемещение объекта в другую зону ответственности") согласно списку возможных переходов, определенных для текущей зоны (см. "Создание и редактирование зоны ответственности").

Более подробную информацию о работе с зонами ответственности вы можете найти в следующих разделах:

- Создание и редактирование зоны ответственности
- Изменение приоритетов для зон ответственности
- Удаление зоны ответственности

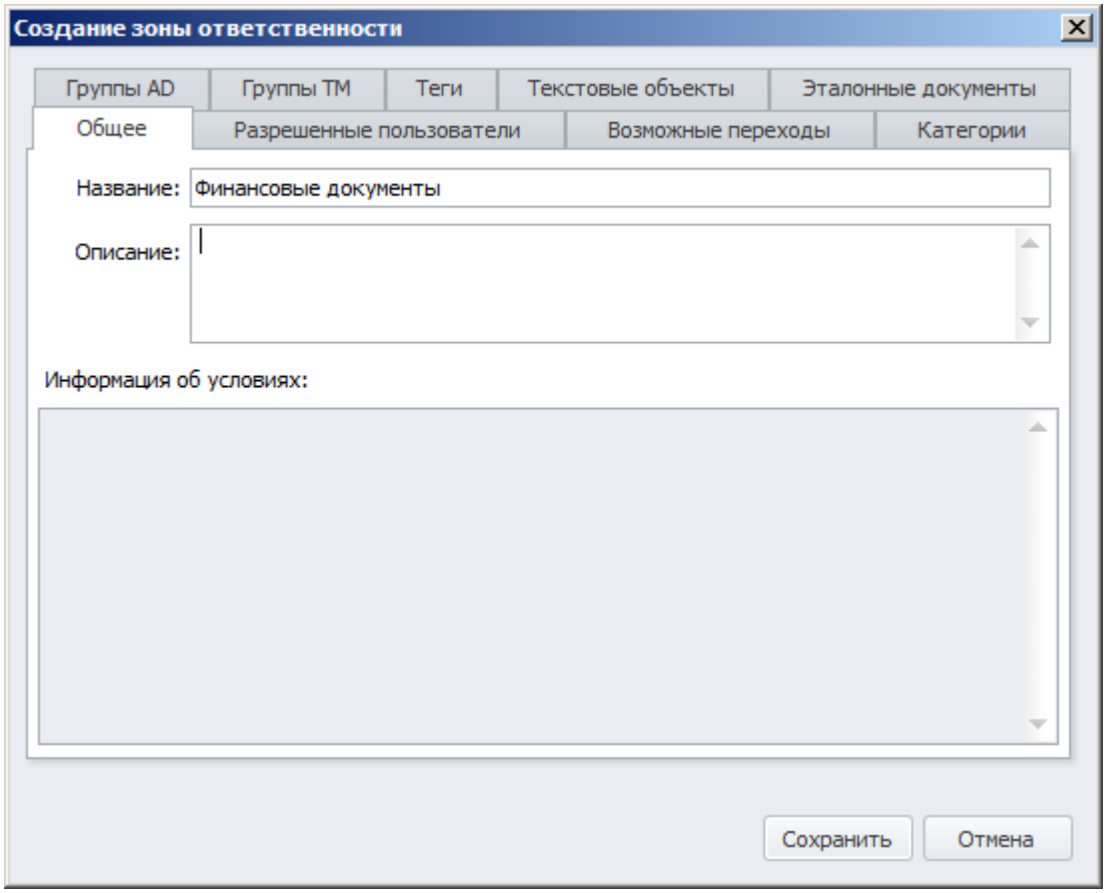
7.1.7.1 Создание и редактирование зоны ответственности

Чтобы создать или отредактировать зону ответственности:

1. Перейдите к разделу **Зоны ответственности**.
2. Выполните необходимое действие:

Действие	**Порядок выполнения**
Создать зону ответственности	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Создать зону ответственности** • нажмите кнопку **Создать зону ответственности** на панели инструментов
Отредактировать зону ответственности	В списке зон ответственности выделите строку с нужной зоной ответственности и выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку **Изменить** на панели инструментов; • дважды щелкните левой кнопкой мыши по выделенной строке.

На экран будет выведено диалоговое окно с параметрами зоны ответственности.



Настройка общих параметров зоны ответственности

3. На вкладке **Общее** укажите следующие параметры:

   - **Название**. Наименование зоны ответственности (обязательный параметр).

Название должно быть уникальным.

> **Примечание**
>
> Для зоны ответственности *Default* изменение параметра **Название** не допускается.

   - **Описание**. Дополнительные сведения о зоне ответственности.

4. Определите условия для помещения объекта в зону ответственности с помощью следующих вкладок. Объект будет включен в зону ответственности, если в нем будет обнаружен любой атрибут из числа отмеченных флажками.

Вкладка	Условие для включения в зону ответственности
Категории	Объекту присвоена категория (без учета версии конфигурации)
Группы AD	Для отправителя объекта определена группа AD
Группы TM	Для отправителя объекта определена группа TM

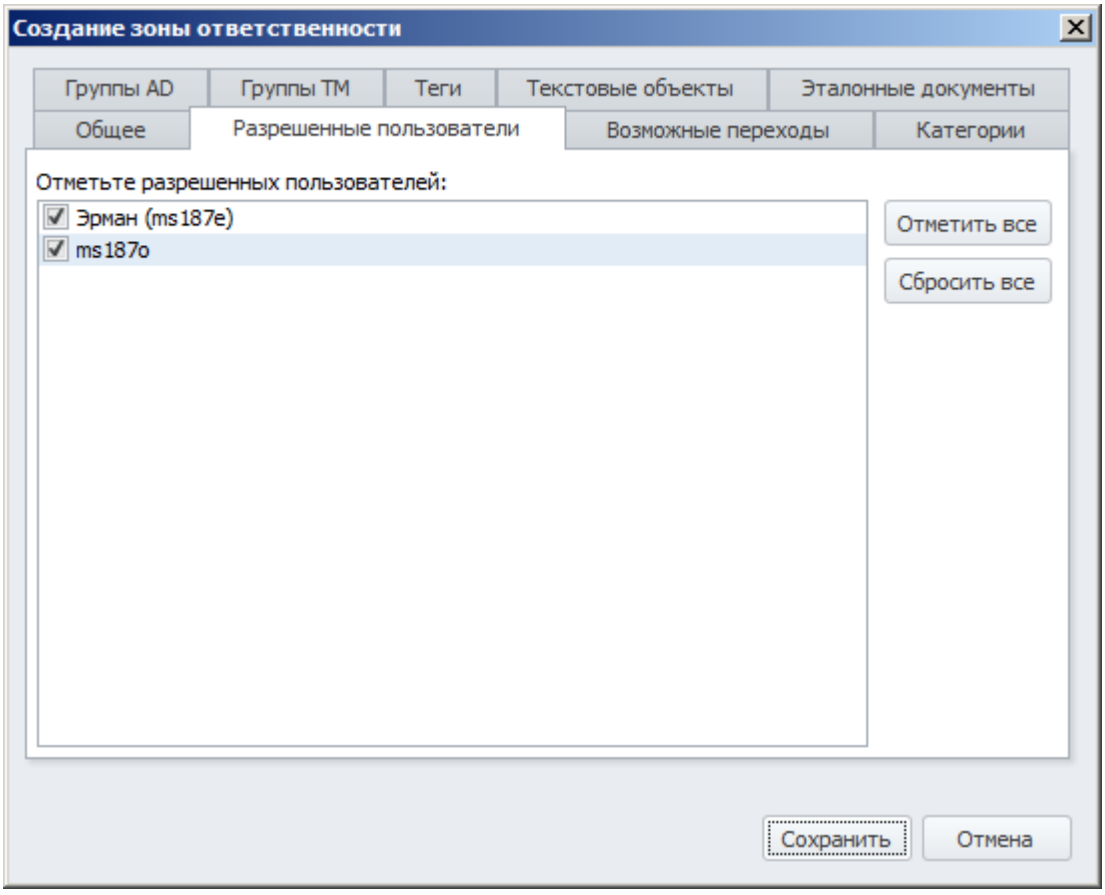
Вкладка	Условие для включения в зону ответственности
Теги	Объекту присвоена группа тегов или тег
Текстовые объекты	В объекте обнаружен тип текстового объекта
Эталонные документы	В объекте обнаружен фрагмент эталонного документа

Чтобы установить или снять все флажки, используйте кнопки **Отметить все** и **Сбросить все**.

Важная информация!

Для зоны ответственности *Default* изменение условий для помещения объекта в зону ответственности не допускается. Объект попадает в зону *Default*, если он не удовлетворил ни одному условию для других зон ответственности.

5. На вкладке **Разрешенные пользователи** отметьте флажками пользователей, которым будет разрешен доступ к объектам из этой зоны ответственности.



Включение пользователей в зону ответственности

Важная информация!

Среди объектов, отнесенных к зоне *Default*, могут быть сообщения и запросы высокой конфиденциальности. Поэтому настоятельно рекомендуется включать в число разрешенных пользователей для зоны *Default* только пользователей с наивысшими привилегиями.

Чтобы установить или снять все флажки, используйте кнопки **Отметить все** и **Сбросить все**.

Важная информация!

Изменение зон ответственности пользователя, авторизованного в Системе, вступит в силу только после его следующей авторизации в Консоли управления.

6. На вкладке **Возможные Переходы** отметьте флажками зоны ответственности, в которые будет разрешено перемещать объект из данной зоны ответственности. Чтобы установить или снять все флажки, используйте кнопки **Отметить все** и **Сбросить все**.

7. Нажмите кнопку **Сохранить**.

7.1.7.2 Изменение приоритетов для зон ответственности

При определении зоны ответственности объект последовательно проверяется на соответствие зонам ответственности по всем зонам и помещается в первую зону ответственности, для которой выполнились условия. Порядок проверки зон ответственности определяется приоритетами зон: в первую очередь проверяется зона с наивысшим приоритетом; предустановленная зона ответственности *Default* имеет самый низкий приоритет (1).

Примечание

Приоритет зоны ответственности *Default* (1) не может быть изменен.

Чтобы изменить приоритет зоны ответственности:

1. Перейдите к разделу **Зоны ответственности**.
2. В списке зон ответственности выделите нужную зону ответственности.
3. Выполните одно из следующих действий:
   - чтобы повысить приоритет зоны ответственности, нажмите кнопку **Повысить приоритет** на панели инструментов или в главном меню выберите команду **Правка > Повысить приоритет**;
   - чтобы понизить приоритет зоны ответственности, нажмите кнопку **Понизить приоритет** на панели инструментов или в главном меню выберите команду **Правка > Понизить приоритет**.

В результате зона ответственности будет перемещена на одну позицию вверх или вниз; параметр **Приоритет** увеличится на единицу или уменьшится соответственно.

7.1.7.3 Удаление зоны ответственности

Важная информация!

Зона ответственности *Default* не может быть удалена.

Также вы не сможете удалить зону ответственности, которая назначена хотя бы одному пользователю и/или зону ответственности, в которой находится хотя бы один объект.

Чтобы удалить зону ответственности:

1. Перейдите к разделу **Зоны ответственности**.
2. В списке зон ответственности выделите нужную зону ответственности.

3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку  **Удалить** на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

7.2 Справочники

Для корректной работы сценария анализа объектов, а также для последующего анализа данных в Консоли управления, помимо настройки конфигурации и составления базы эталонных документов, необходимо определить теги и создать цвета. Для этого предназначены специальные справочники:

- Теги
- Цвета

7.2.1 Теги

Теги представляют собой текстовые метки, дающие краткую характеристику объекта. Теги можно присваивать объекту как при анализе на сервере Traffic Monitor, так и в Консоли управления (см. " Назначение тегов объекту").

Предустановленные теги

В Системе присутствуют предустановленные группы тегов: *Типы файлов*, *Веб-ресурсы* и *Ресурсы*:

- Теги из группы *Типы файлов* характеризуют содержимое вложений (музыка, видео, изображение, и т. п.).
- Теги из группы *Веб-ресурсы* характеризуют сайты, на которые направляются HTTP-запросы (блоги, файлообменники, сайты для поиска работы и т.п).
- Теги из группы *Ресурсы* характеризуют ресурсы (локальные и внешние), трафик от которых не должен обрабатываться системой и сохраняться в базу данных.

Этим тегам сопоставлены соответствующие предустановленные группы списков: каждому списку соответствует тег с таким же кодом. Так например, тегу *Блоги* (код `_BLOGS_`) из группы тегов *Веб-ресурсы* (код `_WEBRESOURCES_`) соответствует список *Блоги* (код `_BLOGS_`) из группы списков *Веб-ресурсы* (код `_WEBRESOURCES_`).

Если в процессе обработки объекта было обнаружено его соответствие какому-либо списку (например, в URL запроса был обнаружен адрес, соответствующий одному из элементов списка *Блоги*), то такому объекту будет присвоен соответствующий тег (в рассматриваемом примере – тег *Блоги*).

В Traffic Monitor Standard также предусмотрен тег **«**`_DELETE_PROTECT_TAG_`**»**. Назначение этого тега выполняется только вручную пользователем (см. "Назначение тегов объекту"). В IW TMS периодически выполняется проверка: если свободное место в базе данных меньше, чем нужно для сохранения новых объектов, то старые объекты удаляются. Однако объекты, которым назначен тег **«**`_DELETE_PROTECT_TAG_`**»**, при этом удаляться не будут.

Предустановленные теги не подлежат редактированию.

Использование тегов в сценарии

Вы можете создать собственные группы тегов и теги, характеризующие объекты необходимым образом. А затем создать в сценарии правило, по которому всем файлам определенного типа будет присвоен определенный тег.

Важная информация!

Теги и группы тегов, которые будут включены в сценарий анализа объектов, нужно создать перед работой над сценарием.

Работа с тегами ведется в разделе **Теги** (область **Конфигурация** на панели **Навигация**).

Более подробную информацию о работе с тегами вы можете найти в следующих разделах:

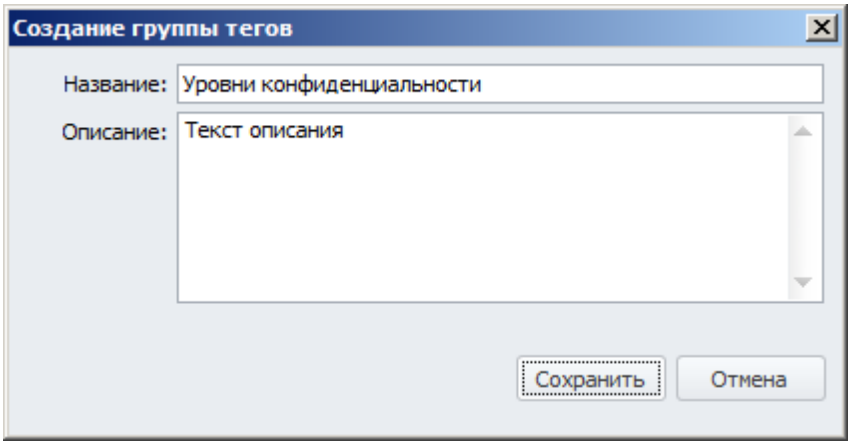
- Создание группы тегов
- Создание тега
- Редактирование тегов и групп тегов
- Удаление группы тегов

7.2.1.1 Создание группы тегов

Чтобы создать группу тегов:

1. Перейдите к разделу **Теги**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Создать группу тегов**.
   - нажмите кнопку **Создать группу тегов** на панели групп тегов.

   На экран будет выведено диалоговое окно **Создание группы тегов**.



Создание группы тегов

3. Укажите параметры группы тегов:
   - **Название**. Наименование группы тегов (обязательный параметр). Должно быть уникальным.
   - **Описание**. Дополнительная информация о группе тегов.
4. Нажмите кнопку **Сохранить**.

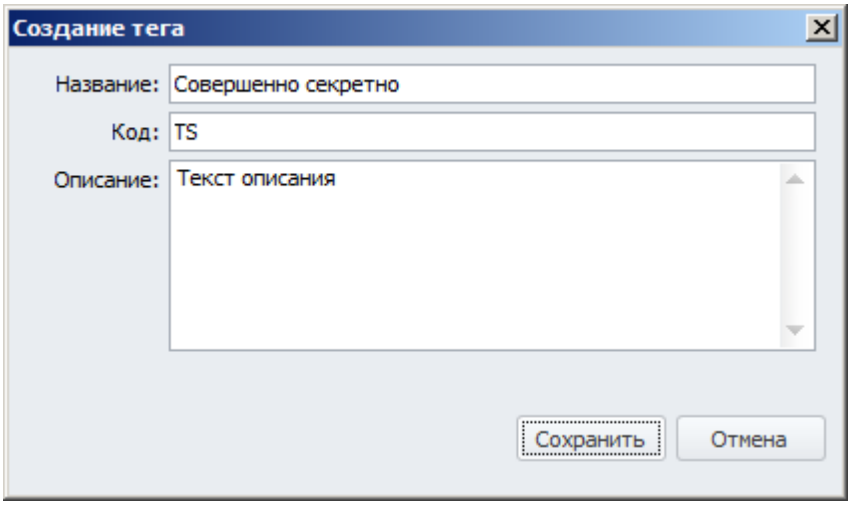
После того как группа тегов будет создана, нужно наполнить группу тегами (см. "Создание тега").

7.2.1.2 Создание тега

Чтобы создать тег:

1. Перейдите к разделу **Теги**.
2. На панели группы тегов выделите название группы, в которую нужно добавить тег.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Тег > Создать**.
   - на панели тегов нажмите кнопку **Создать тег**.

   На экран будет выведено диалоговое окно **Создание тега**.



Настройка параметров тега

4. Укажите параметры тега:
   - **Название**. Имя тега (обязательный параметр). Название должно быть уникальным.
   - **Код**. Название тега, которое будет использоваться при составлении сценария (обязательный параметр).
     Кодовое название может состоять из букв латинского алфавита, цифр и символа подчеркивания. Не должно начинаться с цифры. Код должен быть уникальным.
   - **Описание**. Дополнительные сведения о теге.
5. Нажмите кнопку **Сохранить**.

Повторите шаги 3 – 4, чтобы добавить в группу другие теги.

7.2.1.3 Редактирование тегов и групп тегов

Вы можете изменять теги и группы тегов при помощи следующих операций:

- редактирование параметров группы тегов;
- добавление нового тега в группу;
- редактирование тега, входящего в группу;
- удаление тега из группы.

Чтобы отредактировать группу тегов:

1. Перейдите к разделу **Теги**.

2. На панели группы тегов выделите название нужной группы.

3. Выполните необходимое действие:

Действие	Порядок выполнения
Отредактировать параметры группы тегов (название группы, описание)	1. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку **Изменить** на панели группы тегов. • дважды щелкните левой кнопкой мыши по выделенной группе тегов. 2. В открывшемся диалоговом окне **Редактирование группы тегов** отредактируйте необходимые параметры (см. "Создание группы тегов"). 3. Нажмите кнопку **Сохранить**.
Добавить в группу новый тег	См. "Создание тега"
Отредактировать параметры тега (название, код, описание)	1. На панели тегов выделите нужный тег. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Тег > Изменить**; • нажмите кнопку **Изменить** на панели тегов. • дважды щелкните левой кнопкой мыши по выделенному тегу. В открывшемся диалоговом окне **Редактирование тега** отредактируйте необходимые параметры (см. "Создание тега"). 3. Нажмите кнопку **Сохранить**.
Удалить тег из группы	1. На панели тегов выделите нужный тег. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Тег > Удалить**; • нажмите кнопку **Удалить** на панели тегов.

Действие	Порядок выполнения
	3. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление. **Примечание:** Исключите удаленный тег из текста каждого сценария, в котором он использовался.

7.2.1.4 Удаление группы тегов

Чтобы удалить группу тегов:

1. Перейдите к разделу **Теги**.
2. На панели группы тегов выделите название нужной группы.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку  **Удалить**, на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

 **Примечание**

Исключите удаленную группу тегов из текста каждого сценария, в котором он использовался.

7.2.2 Цвета

Для большей наглядности при анализе объектов в консоли управления вы можете использовать выделение различных объектов цветами.

Порядок настройки цветового отображения объектов:

1. Настройте необходимую цветовую схему (см. "Создание и редактирование цвета", "Удаление цвета")
2. Задайте правила автоматического назначения цветов для перехваченных объектов (см. " Редактирование сценария" и описание свойства `root.processing.color` в разделе "Настройка сценария анализа объектов (LUA)")
3. При анализе объектов вы можете назначать и изменять цвет объекта (см. "Выделение объектов цветом ").

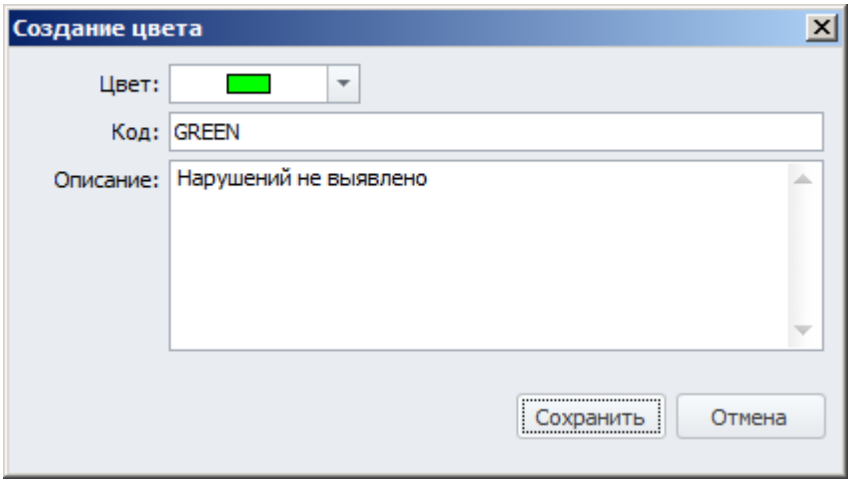
7.2.2.1 Создание и редактирование цвета

Чтобы добавить цвет или изменить его параметры:

1. Перейдите к разделу **Цвета**.
2. Выполните необходимое действие:

Действие	Порядок выполнения
Создать цвет	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Создать цвет** • нажмите кнопку **Создать цвет** на панели инструментов
Отредактировать цвет	1. В списке цветов выделите строку с нужным цветом. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку **Изменить** на панели инструментов; • дважды щелкните левой кнопкой мыши по выделенной строке.

На экран будет выведено диалоговое окно с параметрами цвета.



Настройка параметров цвета

3. Укажите параметры цвета:

   - **Цвет**. Цвет для выделения объекта (обязательный параметр). Цвет должен быть уникален.
   - **Код**. Название цвета, которое будет использоваться при составлении сценария (обязательный параметр).

     Код может состоять из букв латинского алфавита, цифр и символа подчеркивания; не должен начинаться с цифры. Должен быть уникальным.
   - **Описание**. Дополнительные сведения о цвете.

4. Нажмите кнопку **Сохранить**.

7.2.2.2 Удаление цвета

Чтобы удалить цвет:

1. Перейдите к разделу **Цвета**.

2. В списке цветов выделите нужный цвет.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку  **Удалить** на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.



Примечание

Исключите удаленный цвет из текста каждого сценария, в котором он использовался.

7.3 Настройка сценария анализа объектов (LUA)

Сценарий анализа объектов составляется на языке программирования Lua версии 5.1 (документация для Lua версии 5.1 находится по адресу http://www.lua.org/manual/5.1/).

Текст сценария представляет собой набор правил, в соответствии с которыми будет проводиться анализ и обработка объектов на сервере Traffic Monitor. Правило состоит из набора условий, по которым ведется проверка объекта, и действий, осуществляемых при выполнении/невыполнении заданных условий.

В сценарии обязательно должны быть заданы действия, выполняемые для каждого объекта:

- выбор транспортного режима;
- присвоение вердикта объекту.

Если любое из вышеперечисленных действий отсутствует в сценарии или же для определяемого атрибута задано неверное значение, то в этом случае используются значения из сценария «по умолчанию»: см. " Работа системы без сценария анализа объектов".

Условия проверки и действия над объектами задаются, исходя из определения данных, принятого в модели типов InfoWatch Traffic Monitor. При составлении правил вы можете задавать условия для данных любого типа. Но действия могут быть определены только для данных с типами *Processing* и *ObjectProcessing*.



Важная информация!

Перед составлением сценария задайте в Консоли управления те элементы, которые потребуется указывать в сценарии. К таким элементам относятся: списки, группы, категории, теги, цвета.

Более подробную информацию о настройке сценария вы можете найти в следующих разделах:

- Особенности составления сценария на языке LUA
- Модель данных InfoWatch Traffic Monitor
- Типы данных
- Методы
- Операторы
- Пример сценария

7.3.1 Особенности составления сценария на языке LUA

Язык программирования Lua чувствителен к регистру символов. В Системе используются следующие соглашения:

- со строчной буквы пишутся названия свойств и методов;
- с прописной буквы пишутся имена типов данных и значения типов-перечислений.

Например:

```
root. processing. transport_mode = TransportMode. Normal
```

Здесь:

- `root. processing` – путь доступа к данным типа *Processing*;
- `transport_mode` – свойство данных типа *Processing*;
- `TransportMode` – тип данных;
- `Normal` – одно из значений типа *TransportMode*.

Все правила сценария анализа объектов должны быть оформлены в следующем виде:

```
function Process( root)
   ---правило 1 -----
   ---правило 2 -----
   ---    …     -----
   ---правило N -----
end;
```

До начала блока правил `function Process( root)` необходимо:

- Подключить предустановленную библиотеку вспомогательных функций `usertoolkit` с помощью следующей строки:

  ```
  require('usertoolkit');
  ```

- Определить вспомогательные функции и переменные, если такие будут использоваться в сценарии.

При составлении условий указывается значение, на соответствие которому проверяются данные. В действиях задается значение, которое будет присвоено данным определенного типа. Чтобы указать значение, нужно задать путь доступа к данным и собственно значение.

Путь всегда задается от корневого элемента, после которого перечисляются свойства данных. (В качестве разделителя используется точка.)

Пример

Пусть нужно задать действие, в результате которого объекту будет назначен определенный вердикт. Вердикт (*verdict*) является одним из свойств данных типа *Processing*. В свою очередь, данные этого типа являются одним из свойств (*processing*) корневого элемента *root*. Таким образом, путь к данным типа *Verdict* будет выглядеть следующим образом:

```
root. processing. verdict
```

Если обращение к каким-либо данным выполняется неоднократно, то вы можете создать псевдоним. Например, чтобы задать псевдоним для данных `root. processing`, нужно ввести следующую строку:

```
processing = root. processing;
```

Тогда обращение к свойству `verdict` можно записать, как:

```
processing. verdict
```

Значения данных, имеющих тип *string*, задаются в кавычках (двойных или одинарных). Например:

```
root. processing. color = "GREEN";
```

Данные, принадлежащие к типу-перечислению, задаются следующим образом:

```
ТипДаннных. Значение
```



Примечание

Тип данных, в отличие от свойств, пишется без знаков подчеркивания.

Например:

```
root. processing. verdict = Verdict. Forbidden;
```

7.3.2 Модель данных InfoWatch Traffic Monitor

Модель InfoWatch Traffic Monitor включает в себя типы данных.

Тип данных используется для отображения информации о какой-либо сущности (предмет, пользователь). В модели типов InfoWatch Traffic Monitor используются следующие типы данных:

Тип данных	Описание
string (простой тип)	Базовый тип для отображения строковых значений
integer (простой тип)	Базовый тип для отображения числовых значений
boolean (простой тип)	Базовый тип для отображения логических данных, которые могут принимать только одно из двух значений: *true* или *false*
составной тип	Пользовательский тип. Может содержать не только объекты, но и методы, применимые к этим объектам. Примеры составных типов: *Processing* (результат обработки объекта), *ObjectProcessing* (результат контентного анализа текста), *Envelope* (сведения, извлеченные из конверта объекта)
тип-коллекция	Пользовательский тип для отображения объектов одного типа. Примеры типов-коллекций: *Objects* (список вложений), *SemanticMirror* (набор категорий), *Tags* (список тегов)
тип-перечисление	Пользовательский тип. Содержит набор значений, из которых объекту может быть присвоено только одно значение. Примеры типов-перечислений: *Monitor* (перехватчики), *TransportMode* (транспортные режимы)

Каждый тип данных имеет набор свойств.

Свойство – это характерная черта (атрибут) данных определенного типа. Например, данные типа *Envelope* имеют такие свойства, как: *id* (уникальный номер объекта), *capture_date* (дата и время перехвата объекта),

monitor (тип перехватчика) и др.

Метод – действие, которое можно применять к данным определенного типа. В частности, метод *addTag* (присвоение тега объекту) применяется к данным типа *Processing*.

7.3.3 Типы данных

В модели InfoWatch Traffic Monitor все типы данных объединены в дерево, вершиной которого является *корневой элемент root*.

Для использования в сценарии доступны следующие типы данных:

- **Анализ конверта объекта**
  - Envelope (конверт объекта)
- **Анализ объекта**
  - Object (содержимое объекта и результаты контентного анализа)
  - ObjectHeaders (заголовки, извлеченные из объекта)
  - ObjectHeader (имена заголовков объекта)
  - ObjectProcessing (результаты контентного анализа)
  - Objects (список вложений)
- **Обработка объекта**
  - Processing (результаты обработки объекта)

7.3.3.1 Корневой элемент root

Корневой элемент *root* представляет собой вершину дерева, узлами которого являются типы данных. Элемент *root* имеет составной тип данных *RootObject*.

Путь доступа к данным:

```
root.название_свойства
```

Список свойств приведен в следующей таблице:

Название свойства	Тип данных	Описание
envelope	Составной тип Envelope	Общая информация (версия конфигурации, тип перехватчика, дата перехвата), адрес отправителя и получателя(-ей), содержимое заголовков конверта
object	Составной тип Object	Информация о содержимом перехваченного объекта и о результатах контентного анализа

Название свойства	Тип данных	Описание
processing	Составной тип Processing	Результаты обработки перехваченного объекта

Методы, применяемые к корневому элементу *root: xFind*.

Методы, применяемые к свойству *processing*, имеющему составной тип данных *Processing: addTag*.

7.3.3.2 Конверт объекта (Envelope)

Составной тип данных *Envelope* предназначен для представления содержимого, которое было извлечено из конверта перехваченного объекта.

Путь доступа к данным:

```
root.envelope.название_свойства
```

Список свойств приведен в следующей таблице.

Название свойства	Тип данных	Описание
monitor	Тип-перечисление Monitor	Перехватчик, посредством которого был задержан объект (письмо, запрос, сообщение). Возможные значения: • `Smtp` – контроль SMTP-трафика. • `Icq` – контроль ICQ-трафика. • `Http` – контроль HTTP-трафика. • `Print` – получение теневых копий текста, отправляемого на печать и перехваченного InfoWatch Device Monitor. • `Skype` – получение теневых копий сообщений и файлов, отправленных с помощью Skype и перехваченных InfoWatch Device Monitor. • `Device` – получение теневых копий файлов, переносимых на съемные устройства и перехваченных InfoWatch Device Monitor. • `Crawler` – сканирование сетевых папок, локальных дисков рабочих станций, и/или файлового хранилища SharePoint. • `MPP` – контроль обмена данными через Mail.Ru Агент (протокол MPP) • `XMPP` – контроль обмена данными через Jabber (протокол XMPP) • `FTP` – мониторинг передачи трафика по протоколу FTP • `Dla` – получение теневых копий файлов, переносимых на съемные устройства (DeviceLock Adapter).
id	string	Уникальный номер объекта

Название свойства	Тип данных	Описание
capture_date	string	Дата и время, в которые объект был перехвачен Системой
headers	Тип-перечисление Headers	Информация, извлеченная из заголовков конверта. Возможные значения перечислений приведены в нижеследующей таблице
config_version	integer	Версия конфигурации, которая была актуальна при анализе данного объекта
identity	Тип-перечисление Identity	Информация об отправителе и получателе объекта
summary	string	Полная характеристика объекта

В следующей таблице приведены значения, которые может принимать перечисление типа *Headers* для различных типов объектов.

Примечание

При работе с объектами HTTP Monitor предполагается, что URL имеет следующую структуру:

<scheme>://<username>:<password>@<host>:<port>/<path>?<parameters>.

Тип объекта	Значение	Описание
Все типы	source_ip	IP-адрес, с которого был отправлен объект
	destination_ip	IP-адрес сервера назначения
	destination_port	Порт сервера назначения
	creator_application	Агент (из значения заголовка User-Agent)
	capture_server	Сервер Traffic Monitor, который перехватил объект
SMTP Monitor	mail_from	E-mail адрес отправителя из SMTP-конверта
	rcpt_to	E-mail адреса получателей из SMTP-конверта
HTTP Monitor	source_port	Порт, с которого был отправлен запрос
	url_schema	Значение параметра <scheme> из URL
	url_username	Значение параметра <username> из URL
	url_password	Значение параметра <password> из URL
	url_host	Значение параметра <host> из URL
	url_host_fqdn	Имя домена запрашиваемого хоста
	url_host_ip	IP домена запрашиваемого хоста
	url_port	Значение параметра <port> из URL

Тип объекта	Значение	Описание
	url_path	Значение параметра <path> из URL
	url_parameters	Значение параметра <parameters> из URL
ICQ Monitor	initiator_uin	UIN инициатора ICQ-сессии
Device Monitor, DeviceLock Monitor, Skype Monitor, Mail.Ru Agent Monitor, XMPP Monitor	device_name	Имя устройства
	device_type	Тип устройства
	destination_path	Путь назначения объекта при копировании
	policy_name	Имя политики, по которой был перехвачен объект
	rule_name	Имя правила, по которому был перехвачен объект
	action	Признак, была ли операция разрешена или запрещена
	operation	Тип операции
	domain	Имя домена Microsoft Windows, в котором зарегистрирована рабочая станция
	workstation	Имя рабочей станции
	login	Имя учетной записи, от имени которой пользователь авторизован в операционной системе
	userlastname	Фамилия пользователя
	userfirstname	Имя пользователя
	job	Имя задания
	sender	Отправитель
	date	Дата и время отправки
	participant	Учетная запись или телефонный номер получателя/получателей/участников
Crawler Monitor	policy_name	Политика сканирования
	rule_name	Имя правила сканирования
	destination_path	Сетевой путь к файлу
	capture_server	Имя сервера краулера
	workstation	Имя рабочей станции, на которой размещен файл
	owner	Владелец файла
	recipient	Пользователи, имеющие доступ к файлу
FTP Monitor	event_type	Признак формирования теневой копии: • `FtpEventFull` - с теневой копией; • `FtpEventNoShadowCopy` - без теневой копии.
	creator_application	Приложение, отправляющее данные

Тип объекта	Значение	Описание
	url_host	URL ресурса, на который передается файл
	url_host_fqdn	Полный URL ресурса, на который передается файл
	url_path	Директория на ресурсе, куда передается файл
	url_port	Порт, на который передается файл
	sender	Логин отправителя
	byte_start	Позиция в байтах, с которой началась передача
	byte_size	Планируемый размер передаваемых данных
	byte_size_fact	Размер фактически переданных данных
	destination_name	Имя файла, под которым он будет сохранен на сервере
	source_name	Исходное имя файла

7.3.3.3 Содержимое объекта и результаты контентного анализа (Object)

Составной тип данных *Object* предназначен для вывода информации о содержимом перехваченного объекта и результатах контентного анализа.

Путь доступа к данным:

```
root.object.название_свойства
```

Список свойств приведен в следующей таблице:

Свойство	Тип данных	Описание
type	string	Тип объекта
objects	Тип-коллекция Objects	Список вложений, имеющихся у объекта
processing	Составной тип ObjectProcessing	Результаты контентного анализа текста. Сообщения, генерируемые в процессе анализа и обработки перехваченного объекта
headers	Тип-коллекция ObjectHeaders	Список заголовков, извлеченных из объекта
smark	Тип-перечисление SmarkType	Атрибут объекта, принимающий одно из следующих значений: `from`; `to`; `cc`; `bcc`; `subject`; `body`; `file`
object_id	integer	Идентификатор объекта

Методы, применяемые к свойству *processing*, имеющему составной тип данных *ObjectProcessing*:

- addMessage.

7.3.3.4 Заголовки объекта (ObjectHeaders)

Тип-коллекция *ObjectHeaders* предназначен для вывода информации о заголовках, извлеченных из объекта.

Путь доступа к данным:

```
root. object. headers. название_свойства
```

Список свойств приведен в следующей таблице:

Название свойства	Тип данных	Описание
header	Составной тип ObjectHeader	Заголовок, извлеченный из объекта

7.3.3.5 Имена заголовков объекта (ObjectHeader)

Тип данных *ObjectHeader* предназначен для вывода списка заголовков, извлеченных из перехваченного объекта.

Путь доступа к данным:

```
root. object. headers. header. название_свойства
```

Список свойств приведен в следующей таблице.

Название свойства	Тип данных	Описание
name	string	Имя заголовка, извлеченного из объекта
smark	Тип-перечисление SmarkType	Атрибут объекта, принимающий одно из следующих значений: `from`; `to`; `cc`; `bcc`; `subject`; `body`; `file`

7.3.3.6 Результаты контентного анализа (ObjectProcessing)

Тип данных *ObjectProcessing* предназначен для отображения результатов контентного анализа текста. Также этот тип данных используется для вывода сообщений, генерируемых в процессе анализа и обработки перехваченного объекта.

Путь доступа к данным:

```
root. object. processing. название_свойства
```

Список свойств приведен в следующей таблице.

Название свойства	Тип данных	Описание
messages	Тип-коллекция Messages	Сообщения, генерируемые в процессе анализа и обработки объекта
semantic_mirror	Тип-коллекция SemanticMirror	Список категорий, найденных при контентном анализе текста
text_obj_detector	Тип-коллекция TextObjectDetector	Список категорий и терминов, присвоенных детектированным текстовым объектам
copyright_analysis	Тип-коллекция CopyrightAnalysis	Список сообщений, которые были сгенерированы в процессе анализа и обработки объекта

7.3.3.7 Список вложений (Objects)

Тип-коллекция *Objects* предназначен для отображения списка вложений перехваченного объекта.

Путь доступа к данным:

```
root.object.objects.название_свойства
```

Список свойств приведен в следующей таблице.

Название свойства	Тип данных	Описание
object	Составной тип Object	Информация об одном вложении перехваченного объекта

Примечание

Так как тип данных *objects*, являющийся свойством типа данных *object*, в свою очередь, имеет тип данных *object*, то для перехваченных объектов с вложениями некоторой глубины, путь доступа к данным может иметь следующий формат:

```
root.object.objects[.object.objects[...object.objects]...].название_свойства
```

где глубина вложенности больше или равна единице.

7.3.3.8 Результаты обработки объекта (Processing)

Составной тип данных *Processing* содержит информацию о результатах обработки перехваченного объекта.

Путь доступа к данным:

```
root.processing.название_свойства
```

Список свойств приведен в следующей таблице.

Свойство объекта	**Тип данных**	**Описание**
verdict	Тип-перечисление Verdict	Вердикт, присвоенный объекту. По умолчанию объекту присваивается вердикт *Forbidden* (*Запрещено*). Возможные значения: • `Allowed` – разрешено • `Forbidden` – запрещено
transport_mode	Тип-перечисление TransportMode	Транспортный режим, назначенный объекту. Возможные значения: • `Normal` – нормальный • `Transparent` – прозрачный • `Copy` – режим копии Правила установки транспортного режима в сценарии приводятся в таблице, приведенной ниже
delivery_state	Тип-перечисление DeliveryState	Состояние доставки объекта. Возможные значения: • `Pending` – доставка объекта разрешена • `Blocked` – доставка заблокирована • `Delivered` – успешная доставка • `DeliveryFailed` – ошибка в процессе доставки • `DeliveryAttemptFailed` – попытка доставки не удалась
delete_content	boolean	Свойство, определяющее, нужно ли удалять объект без сохранения в базу данных. Возможные значения: • `true` – удалять объект без сохранения в базу данных; • `false` – сохранять объект в базу данных
verdict_reazon	string	Описание причины, по которой объекту был вынесен определенный вердикт
tags	Тип-коллекция Tags	Список тегов, присвоенных объекту в процессе обработки
color	string	Код цвета, которым будет выделен объект при отображении в Консоли управления (используется название, заданное в поле **Код** при создании цвета)

В следующей таблице приведены правила установки транспортного режима в сценарии.

Способ перехвата объектов	**Транспортный режим**	**Значение свойства transport_mode в сценарии**
SMTP		

Способ перехвата объектов	Транспортный режим	Значение свойства transport_mode в сценарии
Система осуществляет перехват и доставку SMTP-трафика посредством интеграции с Postfix. Установите нормальный транспортный режим, если требуется фильтрации трафика – разрешение/запрещение доставки	Нормальный	Normal
	Прозрачный	Transparent
Система получает копию SMTP-трафика от корпоративной почтовой системы или от Sniffer	Копия	Copy
HTTP		
Система осуществляет перехват и доставку HTTP-трафика по протоколу ICAP. Установите нормальный транспортный режим, если требуется фильтрации трафика – разрешение/запрещение доставки	Нормальный	Normal
	Прозрачный	Transparent
Система получает копию HTTP-трафика от Sniffer	Копия	Copy
Другие типы объектов		
Система получает копию ICQ-трафика, задания на печать от Sniffer	Копия	Copy
Система получает копию Skype-трафика, теневые копии файлов и задания на печать от InfoWatch Device Monitor	Копия	Copy
Система получает теневые копии файлов от DeviceLock	Копия	Copy

7.3.4 Операторы

Для использования в сценарии доступны следующие операторы:

- Оператор присваивания
- Оператор сравнения
- Оператор условия
- Оператор цикла

7.3.4.1 Оператор присваивания

Оператор присваивания применяется для того, чтобы задавать значения различным данным.

Синтаксис:

```
путь_к_данным = Тип_данных.Значение
```

Здесь:

- `путь_к_данным`. Путь к данным, которые нужно изменить. Задается от корневого элемента (в качестве разделителя используется точка), причем имя каждого элемента указывается в полном соответствии с моделью типов InfoWatch Traffic Monitor.

- `ТипДанных.Значение`. Тип данных и собственно присваиваемое значение.

Например:

```
root.processing.verdict = Verdict.Forbidden
```

7.3.4.2 Оператор сравнения

Оператор сравнения применяется для выполнения сличения текущего значения со значением, указанным в операторе.

Синтаксис:

```
путь_к_данным == ТипДанных.Значение
```

Здесь:

- `путь_к_данным`. Путь доступа к данным, над которыми выполняется операция сравнения. Задается от корневого элемента (в качестве разделителя используется точка), причем имя каждого элемента указывается в полном соответствии с моделью типов InfoWatch Traffic Monitor.
- `ТипДанных.Значение`. Тип данных и, значение, с которым сравнивается текущее значение.

Например:

```
If root.processing.verdict == Verdict.Forbidden
```

7.3.4.3 Оператор условия

Оператор условия применяется для проверки на соответствие заданному условию. Используется с любыми выражениями, возвращающими тип `boolean`.

Синтаксис:

```
if выражение_1 then
   выражение_2;
else
   выражение_3;
end;
```

Если `выражение_1` истинно, то выполняется `выражение_2`. В противном случае выполняется `выражение_3`, а при отсутствии оператора `else` – следующее правило, заданное в сценарии.

Например:

```
if root.envelope.monitor == Monitor.ICQ then
   root.processing.verdict = Verdict.Allowed;
   root.processing.transport_mode = TransportMode.Normal;
end;
```

В данном примере задается правило обработки объектов, перехваченных ICQ-монитором. Сначала выполняется проверка условия. Если объект перехвачен ICQ-монитором, то такому объекту присваивается вердикт *Allowed* (Разрешено) и назначается транспортный режим *Normal* (Нормальный).

7.3.4.4 Оператор цикла

Оператор цикла применяется для выполнения действий над однотипными данными. Используется с типами-коллекциями.

Синтаксис:

```
for свойство in путь_к_коллекции_данных do
   набор_действий;
end;
```

Здесь:

- `свойство`. Свойство типа-коллекции данных. Например, recipient является свойством типа-коллекции Recipients.
- `путь_к_данным`. Путь доступа к данным, над которыми выполняется операция сравнения. Задается от корневого элемента, в качестве разделителя используется точка. Причем имя каждого элемента указывается в полном соответствии с моделью типов InfoWatch Traffic Monitor.
- `набор_действий`. Одно или несколько действий, которые нужно выполнить для каждого объекта из указанной коллекции.

Например:

```
for header in root.envelope.headers do
   if(header.name == 'source_ip') then
      if vademecum:IsStringInList('SERVERS_IP', header.value, SearchMode.Exact) then
      root.processing.delete_content = true;
      end;
   end;
end;
```

В данном примере выполняется проверка IP-адреса отправителя объекта на принадлежность к списку `SERVERS_IP` – списку IP-адресов серверов, использующихся в служебных целях, трафик от которых не может содержать конфиденциальную информацию. Если IP-адрес отправителя входит в указанный список, то перехваченный объект удаляется без сохранения в базе данных.

7.3.5 Методы

Список методов, доступных для использования при составлении сценария, приведен в следующей таблице:



Важная информация!

Начиная с Traffic Monitor версий 3.4 и 3.4 MP1, для некоторых методов введены обновленные аналоги. Старые методы не рекомендуются для использования. Методы *equal_wild* и *equal_incase* больше не поддерживаются; вместо них можно использовать функции Lua 5.1 (например, *string.find* и *string.upper*). Подробнее см. в документации для Lua версии 5.1 по адресу http://www.lua.org/manual/5.1/.

Имя метода	Применение	Применяется к типу данных
addMessage	Добавление сообщения	ObjectProcessing, Processing
addTag	Добавление тега	Processing

IsStringInList (старое название – is_in)	Проверка вхождения строки в список	-
GetListNames (старое название – Lookup)	Поиск строки в группе списков	-
xFind	Поиск по элементам XML-контекста	RootObject
IsSenderInGroup (старое название – IsSenderInGroupCode)	Проверка вхождения отправителя в группу	-
IsRecipientInGroup (старое название – IsAnyRecipientInGroupCode)	Проверка вхождения получателя в группу	-
IsWorkstationInGroup (старое название – IsWorkstationInGroupCode)	Проверка вхождения рабочей станции в группу	-
IsListItemInText	Проверка вхождения элементов списка в текст	-

7.3.5.1 Добавление сообщения

Метод добавления сообщения к объекту используется только с данными типа *ObjectProcessing*.

Синтаксис:

```
путь_к_данным: addMessage( Message. Тип_сообщения, "Текст")
```

Здесь в качестве параметра `Тип_сообщения` нужно указать тип сообщения, в зависимости от его уровня важности:

- `Info` – информационное;
- `Warning` – предупреждающее;
- `Error` – сообщение об ошибке.

Пример использования метода:

```
root. object. processing: addMessage( Message. Info, "Script run successfully")
```

7.3.5.2 Добавление тега

Метод добавления тега к объекту используется только с данными типа *Processing*.

Синтаксис:

```
путь_к_данным: addTag( "Код_тега")
```



Примечание

Кодовое название тега можно посмотреть в свойствах нужного тега (поле **Код**).

Пример использования метода:

```
root.processing:addTag("MUSIC")
```

7.3.5.3 Проверка вхождения строки в список

Метод проверки вхождения строки в список проверяет наличие указанной строки в определенном списке или группе списков.

Синтаксис:

```
vademecum:IsStringInList("код_списка_или_группы", "строка", SearchMode.Режим_поиска)
```

Параметр SearchMode определяет режим сопоставления при поиске по спискам и может принимать одно из следующих значений:

- `SearchMode.Exact` – поиск точного соответствия указанной строке.
- `SearchMode.DomainExplicit` и `SearchMode.DomainImplicit` – используются для списков и групп списков, созданных пользователем (см. "Списки") и содержащих возможные адреса запросов. Ищется максимальное соответствие адреса с учетом иерархии доменной системы имен (согласно RFC1034 – http://www.ietf.org/rfc/rfc1034).

  Для `SearchMode.DomainExplicit` поиск производится в последовательности от полного соответствия домена до соответствия для поддоменов вышестоящего домена. Например, если ищется вхождение адреса «**info.mail.ru**», то сначала будет найдено вхождение в список, содержащий элемент **info.mail.ru**. Если такого списка нет, то будут последовательно искаться вхождения элементов ***.mail.ru** , ***.ru** и **.ru**.

  Для `SearchMode.DomainImplicit` поиск производится в последовательности от полного соответствия домена до соответствия для поддоменов вышестоящего домена, затем – для вышестоящего домена, причём соответствие для вышестоящего домена неявно покрывает и поддомены. Например, если ищется вхождение адреса «**info.mail.ru**», то сначала будет найдено вхождение в список, содержащий элемент **info.mail.ru**. Если такого элемента в списке нет, то будут последовательно искаться вхождения элементов ***.mail.ru** , **mail.ru**, ***.ru**, **.ru** и **ru**.

Таким образом, в большинстве случаев необходимо использовать значение `SearchMode.Exact`. Другие значения могут использоваться только в специфическом случае, когда требуется выполнить поиск по спискам доменов, не присутствующих в системном списке *Веб-ресурсы*.

Пример использования метода:

```
for header in root.envelope.headers do
   if(header.name == 'source_ip') then
      if vademecum:IsStringInList('SERVERS_IP', header.value, SearchMode.Exact) then
      root.processing.delete_content = true;
      end;
   end;
end;
```

В данном примере выполняется проверка IP-адреса отправителя объекта на принадлежность к списку `SERVERS_IP` – списку IP-адресов серверов, использующихся в служебных целях, трафик от которых не может содержать конфиденциальную информацию. Если IP-адрес отправителя входит в указанный список, то перехваченный объект удаляется без сохранения в базе данных.

7.3.5.4 Поиск строки в группе списков

Метод поиска строки в группе списков осуществляет поиск тех списков, входящих в заданную группу списков, в которых встречается указанная строка.

Синтаксис:

```
vademecum: GetListNames("код_группы_списков", "строка", SearchMode.Режим_поиска)
```

Описание параметра `SearchMode` приведено в разделе "Проверка вхождения строки в список". В режимах поиска с учетом доменной иерархии (`DomainExplicit`, `DomainImplicit`) результаты группируются по найденным соответствиям для доменов верхнего уровня.

Данный метод может использоваться в следующем случае. Например, в Консоли управления пользователем создана группа списков `COMPANY_ADDRESSES`, где перечислены домены компаний-конкурентов, компаний контрагентов и т.п. Также в Консоли управления создана группа тегов, соответствующих спискам из этой группы. В таком случае для присвоения HTTP-запросу тегов в зависимости от того, на какой веб-ресурс этот запрос адресован, в сценарий необходимо включить следующее правило:

```
for tag in vademecum: GetListNames('COMPANY_ADDRESSES', url_host, SearchMode.DomainImplicit)
do
   --- переменной tag присваиваются значения, соответствующие кодам списков, в которые
   ----- входит url_host ---
end;
```

Это реализуется следующим образом. Параметр `url_host` (полученный из URL запроса) проверяется на предмет вхождения в списки из группы списков `COMPANY_ADDRESSES`. Каждому списку, входящему в группу списков `COMPANY_ADDRESSES`, сопоставляется тег из соответствующей группы тегов. В результате проверяемому объекту присваиваются теги для каждого из списков, в котором он был обнаружен.

7.3.5.5 Поиск по элементам XML-контекста

Поиск по элементам XML-контекста объекта (подробнее об XML-контексте см. "Загрузка объекта в базу данных" и "Просмотр информации по объектам") используется только с данными типа *`RootObject`*.

Синтаксис:

```
root: xFind("XPath-выражение").XPath-метод
```

Здесь:

- `xPath-выражение`. Выражение, составленное по правилам языка xPath.
- `XPath-метод`. Метод объекта `XPath` (объект `XPath` возвращается методом `xFind`).

  Методы объекта `XPath`:

  - `count`. Количество объектов, соответствующих заданному условию.
  - `nodes`. Коллекция объектов, принадлежащих классу `XMLNode`.

Пример использования метода:

```
if root: xFind('object[type == "video/avi"]').count then
   …
end;
```

В данном случае ведется поиск вложений формата `AVI`.

7.3.5.6 Проверка вхождения отправителя в группу

Метод проверки вхождения отправителя в группу осуществляет поиск данных отправителя объекта в справочниках сотрудников (см. "Справочник сотрудников").

Синтаксис:

```
GCC: IsSenderInGroup( root, 'groupcode')
```

где `groupcode` – это код группы, относительно которой делается проверка. Можно перечислять несколько групп, используя в качестве разделителей символы «, », «| » и «; ».

Пример использования метода:

```
if GCC: IsSenderInGroup( root, 'Group1| Group2') then
   root. object. processing: addMessage( Message. Info, 'Отправитель принадлежит группе
   пользователей «Group1» или «Group2»');
end;
```

В данном примере выполняется проверка данных отправителя на принадлежность к спискам `Group1` и `Group2`. Если адрес отправителя входит в указанный список, то проверяемому объекту добавляется сообщение «*Отправитель принадлежит группе пользователей «Group1» или «Group2»*».

7.3.5.7 Проверка вхождения получателя в группу

Метод проверки вхождения получателя в группу осуществляет поиск данных получателя объекта в справочниках сотрудников (см. "Справочник сотрудников").

Синтаксис:

```
GCC: IsRecipientInGroup( root, 'groupcode')
```

где `groupcode` – это код группы, относительно которой делается проверка. Можно перечислять несколько групп, используя в качестве разделителей символы «, », «| » и «; ».

Пример использования метода:

```
if GCC: IsRecipientInGroup( root, 'BLACK_RECIPIENTS_LIST') then
   root. object. processing: addMessage( Message. Info, 'Один из получателей входит в черный
   список');
end;
```

В данном примере выполняется проверка данных получателей на принадлежность к списку BLACK_RECIPIENTS_LIST. Если какой-либо из параметров получателей входит в указанный список, то проверяемому объекту добавляется сообщение «*Один из получателей входит в черный список*».

7.3.5.8 Проверка вхождения рабочей станции в группу

Метод проверки вхождения рабочей станции в группу осуществляет поиск данных рабочей станции отправителя объекта в справочниках сотрудников (см. "Справочник рабочих станций").

Синтаксис:

```
GCC: IsWorkstationInGroup( root, 'groupcode')
```

где `groupcode` – это код группы, относительно которой делается проверка. Можно перечислять несколько групп, используя в качестве разделителей символы «, », «| » и «; ».

Пример использования метода:

```
if GCC:IsWorkstationInGroup(root, 'BLACK_SENDER_LIST') then
   root.object.processing:addMessage(Message.Info, 'Рабочая станция входит в черный список
   отправителей');
end;
```

В данном примере выполняется проверка данных рабочей станции на принадлежность к группе ТМ с кодом BLACK_SENDER_LIST. Если какой-либо из параметров отправителя входит в указанную группу, то проверяемому объекту добавляется сообщение «*Рабочая станция входит в черный список отправителей* ».

7.3.5.9 Проверка вхождения элементов списка в текст

Метод проверки вхождения элементов списка в текст осуществляет поиск наличия в заданном тексте каких-либо элементов из пользовательских списков (см. "Списки").

Синтаксис:

```
vademecum:IsListItemInText('text', 'list')
```

где `text` – это текст, по которому выполняется поиск, а `list` – код пользовательского списка, относительно которого делается проверка. Можно перечислять несколько списков, используя в качестве разделителей символы «, », «| » и «; ».

Примечание

Для списков из предустановленных групп списков *Типы файлов* и *Веб-ресурсы* метод *IsListItemInText* не применяется.

Пример использования метода:

```
for header in obj.headers do
    if vademecum:IsListItemInText(header.value, 'GARBAGE_LIST') then
        root.processing.delete_content = true;
    end;
end;
```

В данном примере выполняется проверка значений заголовка объекта любой степени вложенности на принадлежность к списку GARBAGE_LIST. Данный список содержит перечень слов, служащих признаком паразитного трафика. Если в заголовке проверяемого объекта присутствует какой-либо из элементов этого списка, то проверяемый объект не передается в базу данных.

7.3.6 Библиотека вспомогательных функций

Библиотека вспомогательных функций usertoolkit предназначена для упрощенного использования в сценарии наиболее популярных проверок. Библиотека usertoolkit включает в себя следующий набор вспомогательных функций:

Имя функции	Применение
CategoryDetected	Проверка присутствия категорий
CategoriesFromListDetected	Проверка наличия категории из списка

Имя функции	Применение
SampleDocumentDetected	Проверка присутствия цитат из эталонных документов
TextObjectDetected	Проверка присутствия текстовых объектов
root_has_sector_text_object	Проверка присутствия текстового объекта, относящегося к указанной отрасли
UnknownFormatDecteted	Проверка присутствия вложений неопределенного типа
EncryptedContentDecteted	Проверка присутствия зашифрованных вложений
AnyError	Проверка наличия любых ошибок при обработке объекта
ExctactorError	Проверка наличия ошибок при обработке вложений объекта
ContentAnalysisError	Проверка наличия ошибок контентного анализа
IsGarbage	Проверка мусорного трафика
first	Поиск первого элемента из списка нод
IsIdentityConflict	Проверка наличия конфликта идентификации
SendNotificationUser	Отправка уведомления для офицера безопасности
SendNotificationEmployee	Отправка уведомления для нарушителя
TagsFromListDetected	Проверка наличия какого-либо тега из списка

Важная информация!

Чтобы иметь возможность использовать библиотеку вспомогательных функций, в самом начале сценария укажите строку:

```
require('etc/scripts/usertoolkit')
```

7.3.6.1 Проверка присутствия категорий

Чтобы проверить, присутствуют ли в контексте объекта какие-либо категории (см. "Классификатор"), используйте следующую функцию:

```
CategoryDetected(root)
```

Например:

```
if CategoryDetected(root) then
   root.object.processing:addMessage(Message.Info, 'Обнаружены категории');
end;
```

7.3.6.2 Проверка наличия категории из списка

Чтобы проверить, присутствуют ли в контексте объекта категории (см. "Классификатор"), используйте следующую функцию:

```
CategoriesFromListDetected( root, { category })
```

где `category` – это код искомой категории. Вы можете перечислить несколько категорий, используя в качестве разделителей символы «,», «|» и «;».

Например:

```
if CategoriesFromListDetected( root, {'CONFIDENTIAL','STRUCTURE'}) then
  return true, Verdict. Forbidden,'Утечка конфиденциальной информации','RED';
end;
```

7.3.6.3 Проверка присутствия цитат из эталонных документов

Чтобы проверить, присутствуют ли в контексте объекта какие-либо цитаты из эталонных документов (см. " База эталонных документов"), используйте следующую функцию:

```
SampleDocumentDetected( root)
```

Например:

```
if SampleDocumentDetected( root) then
   root. object. processing: addMessage( Message. Info, 'Обнаружены цитаты');
end;
```

7.3.6.4 Проверка присутствия текстовых объектов

Чтобы проверить, присутствуют ли в контексте объекта какие-либо текстовые объекты (см. "Текстовые объекты"), используйте следующую функцию:

```
TextObjectDetected( root)
```

Например:

```
if TextObjectDetected( root) then
   root. object. processing: addMessage( Message. Info, 'Обнаружены текстовые объекты');
end;
```

7.3.6.5 Проверка присутствия текстового объекта из отрасли

Чтобы проверить, присутствуют ли в контексте объекта текстовые объекты, относящиеся к указанной отрасли (например, финансовой, производственной и др.) (подробнее см. "Текстовые объекты"), используйте следующую функцию:

```
root_has_sector_text_object( root, 'sector')
```

где `sector` – код искомой отрасли.

Например:

```
if root_has_sector_text_object( root, 'PersonalData') then
```

```
    return true,Verdict.Forbidden,'Утечка персональных данных','RED';
end;
```

7.3.6.6 Проверка присутствия вложений неопределенного типа

Чтобы проверить, содержит ли объект вложения, для которых не определен тип, используйте следующую функцию:

```
UnknownFormatDecteted(root)
```

Например:

```
if UnknownFormatDecteted(root) then
   root.object.processing:addMessage(Message.Info, 'Обнаружены вложения неопределенного
   типа');
end;
```

7.3.6.7 Проверка присутствия зашифрованных вложений

Чтобы проверить, содержит ли объект зашифрованные вложения, используйте следующую функцию:

```
EncryptedContentDecteted(root)
```

Например:

```
if EncryptedContentDecteted(root) then
   root.object.processing:addMessage(Message.Info, 'Обнаружены зашифрованные вложения');
end;
```

7.3.6.8 Проверка наличия любых ошибок обработки объекта

Чтобы проверить, произошли ли какие-либо ошибки при обработке объекта, используйте следующую функцию:

```
AnyError(root)
```

Например:

```
if AnyError(root) then
   root.object.processing:addMessage(Message.Info, 'Присутствуют ошибки обработки
   объекта');
end;
```

7.3.6.9 Проверка наличия ошибок обработки вложений

Чтобы проверить, произошли ли какие-либо ошибки при обработке вложений объекта, используйте следующую функцию:

```
ExctactorError(root)
```

Например:

```
if ExctactorError(root) then
   root.object.processing:addMessage(Message.Info, 'Присутствуют ошибки обработки вложений
   объекта');
end;
```

7.3.6.10 Проверка наличия ошибок контентного анализа

Чтобы проверить, произошли ли какие-либо ошибки при обработке текста объекта, используйте следующую функцию:

```
ContentAnalysisError( root)
```

Например:

```
if ContentAnalysisError( root) then
   root. object. processing: addMessage( Message. Info, ' Присутствуют ошибки контентного анализа
   объекта');
end;
```

7.3.6.11 Проверка мусорного трафика

В сценарии можно выполнить проверку, является ли объект "мусорным трафиком" - то есть таким POST-запросом, для которого нельзя формализовать текст и тело объекта; в заголовках которого не выделен какой-либо текст. Например, мусорным трафиком являются фоновые запросы вроде обновления статуса.

Список веб-ресурсов, для которых возможно определение мусорного трафика, приведен в разделе " Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов".

Чтобы осуществить проверку на мусорный трафик, используйте следующую функцию:

```
IsGarbage( root)
```

Например:

```
if IsGarbage( root) then
   return true, Verdict. Allowed,' Бесполезный трафик',' GREY';
end;
```

7.3.6.12 Поиск первого элемента из списка нод

Для поиска первого элемента из списка нод, описанных в xPath (см. "Поиск по элементам XML-контекста"), используйте следующую функцию:

```
first( root: xFind('/root/envelope/headers/url_host'). nodes)
```

Например, вместо использования следующей конструкции с двумя циклами:

```
local url_node = root: xFind('/root/envelope/headers/url_host'). nodes;
local url_path = root: xFind('/root/envelope/headers/url_path'). nodes;
    for url_host_nodes in url_node do
        for url_path_nodes in url_path do
            full_url_path = url_host_nodes. text.. url_path_nodes. text;
        end;
    end;
```

Вы можете использовать следующий вариант:

```
local url_node = first( root: xFind('/root/envelope/headers/url_host'). nodes);
local url_path = first( root: xFind('/root/envelope/headers/url_path'). nodes);
full_url_path = url_node. text .. url_path. text;
```

7.3.6.13 Проверка наличия конфликта идентификации

Чтобы проверить, не было ли найдено для атрибутов объекта несколько разных соответствий с данными записей из справочников сотрудников и рабочих станций (подробнее от ошибках идентификации см. " Обработка данных отправителя, получателя и рабочей станции"), используйте следующую функцию:

```
IsIdentityConflict( root)
```

Например:

```
if IsIdentityConflict( root) then
   root. object. processing: addMessage( Message. Info, ' Ошибка идентификации' );
end;
```

7.3.6.14 Отправка уведомления для офицера безопасности

Для того, чтобы при перехвате объекта, нарушившего политику безопасности, офицер безопасности получал e-mail оповещение (подробнее см. "Настройка уведомлений о нарушениях"), используйте следующую функцию:

```
SendNotificationUser( root)
```

Например, для политики обработки нарушений может использоваться фрагмент вида:

```
result, verdict, verdict_reason, color = CheckViolationPolicy( root);
if result then
  SendNotificationUser( root);
  return;
end;
```

7.3.6.15 Отправка уведомления для нарушителя

Для того, чтобы при перехвате объекта, нарушившего политику безопасности, нарушитель (сотрудник), отправивший объект, получал e-mail уведомление об этом (подробнее см. "Настройка уведомлений о нарушениях"), используйте следующую функцию:

```
SendNotificationEmployee( root)
```

Например, для политики обработки нарушений может использоваться фрагмент вида:

```
result, verdict, verdict_reason, color = CheckViolationPolicy( root);
if result then
  SendNotificationEmployee( root);
  return;
end;
```

7.3.6.16 Проверка присутствия текстового объекта из указанной отрасли

Чтобы проверить, присутствуют ли в контексте объекта текстовые объекты, относящиеся к указанной отрасли (например, финансовой, производственной и др.) (подробнее см. "Текстовые объекты"), используйте следующую функцию:

```
root_has_sector_text_object( root, ' sector' )
```

где `sector` – код искомой отрасли.

Например:

```
if root_has_sector_text_object( root, 'PersonalData') then
    return true, Verdict. Forbidden,'Утечка персональных данных','RED';
end;
```

7.3.7 Пример сценария

Пример сценария содержит набор рекомендованных предустановленных политик – наборов правил обработки, определяющих, какие из перехваченных объектов являются нарушениями, и как Система должна реагировать на все типы перехваченных объектов. Сценарий работает следующим образом:

1. Устанавливаются значения по умолчанию (определяется транспортный режим для каждого монитора).
2. Перехваченный объект проверяется на возможность применения одной из политик.
3. Если объект подпадает под условия политики, к нему применяются действия этой политики.
4. Применяется политика обработки штатных объектов – для объектов, которые не были признаны нарушениями при проверке предыдущих политик.

В примере сценария используются следующие политики обработки перехваченных объектов:

- Политика, разрешающая передачу любой информации отправителю из VIP группы;
- Политика, выявляющая передачу информации, признанную нарушением;
- Политика, выявляющая подозрительную активность сотрудников;
- Политика, выявляющая нецелевое использование ресурсов организации;
- Политика, разрешающая передачу штатной информации. Применяется в последнюю очередь для обработки штатных событий – событий, которые не подпали под условия ни одной из предыдущих политик.

Если к Вашей организации применимы данные политики, для корректной работы сценария в Консоли управления необходимо добавить сотрудников в предустановленную группу ТМ «*VIP*», а нежелательных получателей в предустановленную группу ТМ «*Подозрительные получатели*». В противном случае при обработке объектов, проверка отправителей и получателей на принадлежность к этим группам выполняться не будет.

Важная информация!

Если вы хотите создать собственный сценарий на основе примера, и при этом изменяете предустановленный режим работы с копией (`TransportMode. Copy`) на нормальный (`TransportMode. Normal`), то необходимо учитывать, что в этом случае Система будет блокировать дальнейшую доставку всех объектов, которым в результате обработки был присвоен вердикт «*Запрещено*» (`Verdict. Forbidden`).

Предполагается, что для лингвистического анализа используется стандартный классификатор, входящий в комплект поставки Системы, который необходимо загрузить в Консоль управления, а также заданы все необходимые эталонные документы. В противном случае поиск категорий и цитат эталонных документов выполняться не будет.

Также перед началом сценария должна быть включена библиотека вспомогательных функций (‘usertoolkit’).

Сценарий

```
--- Определение вспомогательных функций ------------------------------------------------
--
-- функция задания транспортного режима (для каждого монитора)

function SetDefaultTransportMode (root)
  if root.envelope.monitor == Monitor.Smtp then
    -- SMTP
    root.processing.transport_mode = TransportMode.Copy;
    return;
  elseif root.envelope.monitor == Monitor.Device then
    --DEVICE MONITOR
    root.processing.transport_mode = TransportMode.Copy;
    return;
  elseif root.envelope.monitor == Monitor.Dla then
    --DEVICE LOCK ADAPTER [DLA]
    root.processing.transport_mode = TransportMode.Copy;
    return;
  elseif root.envelope.monitor == Monitor.Print then
    --PRINT MONITOR
    root.processing.transport_mode = TransportMode.Copy;
    return;
  elseif root.envelope.monitor == Monitor.Http then
    -- HTTP
    root.processing.transport_mode = TransportMode.Copy;
    return;
  elseif root.envelope.monitor == Monitor.Icq then
    -- ICQ
    root.processing.transport_mode = TransportMode.Copy;
    return;
  end;
  root.processing.transport_mode = TransportMode.Copy;
end;

-- функция проверки применимости разрешающей политики, возвращает признак - применима политика или нет,
-- вердикт, основание вердикта и цвет, которым будет выделен объект

function CheckPermissionPolicy(root)
  -- проверяется, входит ли отправитель в группу VIP
  if GCC:IsSenderInGroup(root, 'VIP') then
    -- если входит, возвращается признак того, что политика применима и перечень параметров;
    return true, Verdict.Allowed, 'Отправитель обнаружен в группе VIP','LIGHT_GREEN';
  end;
  -- иначе возвращается признак того, что политика не применима
  return false;
end;

-- функция проверки применимости политики обработки нарушений, возвращает признак - применима политика или
нет,
-- вердикт, основание вердикта и цвет, которым будет выделен объект
--
-- Нарушения условно подразделяются на утечки сведений ограниченного распространения и нарушение
законодательства РФ.
-- Объекты, для которых выявлена утечка сведений ограниченного распространения, выделяются красным цветом.
-- Объекты, для которых выявлено нарушение законодательства РФ, выделяются светло-красным цветом.

function CheckViolationPolicy(root)
  -- проверяется присвоена ли объекту хотя бы одна категория с родительскими категориями "Конфиденциальная
информация",
  -- "Структура компании"
```

```
  if CategoriesFromListDetected(root, {'CONFIDENTIAL','STRUCTURE'}) then
    -- если есть такие категории, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Утечка конфиденциальной информации','RED';
  end;

  -- проверяется, обнаружена ли в объекте хотя бы одна цитата из любого эталонного документа
  if SampleDocumentDetected(root) then
    -- если цитаты обнаружены, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Утечка конфиденциальной информации','RED';
  end;

  -- проверяется, обнаружен ли в объекте хотя бы один текстовый объект, характеризующий персональные данные
  if root_has_sector_text_object(root, 'PersonalData') then
    -- если есть текстовые объекты, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Утечка персональных данных','RED';
   end;

  -- проверяется обнаружен ли в объекте хотя бы один текстовый объект, характеризующий финансовую информацию
физических лиц
  if root_has_sector_text_object(root, 'Finance') then
    return true,Verdict.Forbidden,'Утечка финансовой информации','RED';
  end;

  --
  if root_has_sector_text_object(root, 'Insurance') then
    return true,Verdict.Forbidden,'Утечка страховой информации','RED';
  end;

  --
  if root_has_sector_text_object(root, 'OilAndGas') then
    return true,Verdict.Forbidden,'Утечка отраслевой информации (Нефть-Газ)','RED';
  end;

  --
  if root_has_sector_text_object(root, 'Production') then
    return true,Verdict.Forbidden,'Утечка производственной информации','RED';
  end;

  --
  if root_has_sector_text_object(root, 'Telecommunications') then
    return true,Verdict.Forbidden,'Утечка отраслевой информации (Телекоммуникации)','RED';
  end;

  -- проверяется присвоена ли объекту хотя бы одна категория с родительской категорией "Нарушение
законодательства РФ"
  if CategoryFromListDetected(root,'BAZA_PROTIVOD') then
    -- если есть такая категория, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Нарушение законодательства РФ','LIGHT_RED';
  end;

  -- проверяется обнаружена ли в объекте информация, указывающая на посещение запрещенных веб-ресурсов
  if TagsFromListDetected(root,{'_DANGEROUS_','_AGGRESSIVE_','_ADULT_'}) then
    -- если есть такая информация, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Нарушение законодательства РФ','LIGHT_RED';
  end;

  -- иначе возвращается признак того, что политика не применима
  return false;
end;

-- функция проверки применимости политики обработки потенциальных нарушений, возвращает признак - применима
политика или нет,
-- вердикт, основание вердикта и цвет, которым будет выделен объект
```

```
--
-- Объект потенциально может являться нарушением, если Система не смогла провести полноценный анализ его
содержимого
-- или в объекте обнаружены подозрительные данные.
-- Объекты, для которых Система не смогла провести полноценный анализ содержимого, выделяются светло-оранжевым
цветом.
-- Объекты, получатели которых обнаружены в группе подозрительных получателей, выделяются оранжевым цветом.

function CheckPotentialViolationPolicy(root)
  -- проверяется входит ли хотя бы один получатель в группу подозрительных получателей
  if GCC:IsRecipientInGroup(root, 'SUSPICIOUS_RECIPIENTS') then
    -- если входит, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Получатель обнаружен в группе подозрительных получателей','ORANGE';
  end;

  -- проверяется если конфликт идентификации отправителя, получателя, или рабочей станции
  if IsIdentityConflict(root) then
    -- если конфликт есть, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Конфликт идентификации','ORANGE';
  end;

  -- проверяется содержит ли объект вложения, для которых не определен тип содержимого
  if UnknownFormatDecteted(root) then
    -- если содержит, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Файл неизвестного формата','LIGHT_ORANGE';
  end;

  -- проверяется, содержит ли объект зашифрованные данные
  if EncryptedContentDecteted(root) then
    -- если содержит, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Зашифрованный текст','LIGHT_ORANGE';
  end;

  -- проверяется произошла ли ошибка в процессе обработки объекта
  if ExtractorError(root) then
    -- если произошла, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Ошибка распаковки','LIGHT_ORANGE';
  end;

  -- проверяется произошла ли ошибка в процессе контентного анализа
  if ContentAnalysisError(root) then
    -- если произошла, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Ошибка выполнения контентного анализа','LIGHT_ORANGE';
  end;

  -- иначе возвращается признак того, что политика не применима
  return false;
end;


-- функция проверки применимости политики нецелевого использования ресурсов, возвращает признак - применима
политика или нет,
-- вердикт, основание вердикта и цвет, которым будет выделен объект

function CheckNoPurposeResourcesUsagePolicy(root)

  --проверяется содержит ли объект вложения развлекательного характера: видео, музыка, изображения
  if TagsFromListDetected(root,{'_VIDEO_','_MUSIC_','_IMAGE_'}) then
    -- если содержит, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Пересылка развлекательного контента','LIGHT_YELLOW';
  end;

  --проверяется содержит ли объект информацию о посещении развлекательных веб-ресурсов
```

```
  if TagsFromListDetected(root,{'_BLOGS_','_MEDIA_','_ENTERTAINMENT_','_FILESHARING_'}) then
    -- если содержит, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Посещение развлекательных веб-ресурсов','LIGHT_YELLOW';
  end;

  --проверяется содержит ли объект информацию о посещении веб-ресурсов по поиску работы
  if Tagged(root,'_JOBSEARCH_') then
    -- если содержит, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Посещение веб-ресурса по поиску работы','LIGHT_YELLOW';
  end;

  -- иначе возвращается признак того, что политика не применима
  return false;
end;

-- функция применения предустановленных политик, содержит перечень действий, которые необходимо выполнить, в
случае если политика применима

function ApplyPolicy(root, delete_content, verdict, verdict_reason, color)
  -- устанавливается вердикт
  root.processing.verdict = verdict;

  -- проверяется требуется ли сохранять объект в базе данных, если требуется
  if not delete_content then
    -- указывается основание вердикта
    root.processing.verdict_reason = verdict_reason;
    -- объект выделяется цветом
    root.processing.color = color;
  else
    -- иначе объект не сохраняется в базе данных
    root.processing.delete_content = true;
  end;
end;


function CheckGarbage(root)
    --проверяется является ли объект бесполезным трафиком
    local garbage, tag;

    garbage,tag=IsGarbage(root);

    if garbage then
    -- если объект является бесполезным трафиком
        return true,Verdict.Allowed,'Бесполезный трафик','GREY';
    end;

    -- иначе возвращается признак того, что политика не применима
    return false;
end;

function CheckCrawlerPolicy(root)
  -- проверяется присвоена ли объекту хотя бы одна категория с родительскими категориями "Конфиденциальная
информация",
  -- "Структура компании"
  if CategoriesFromListDetected(root, {'CONFIDENTIAL','STRUCTURE'}) then
    -- если есть такие категории, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Утечка конфиденциальной информации','RED';
  end;

  -- проверяется, обнаружена ли в объекте хотя бы одна цитата из любого эталонного документа
  if SampleDocumentDetected(root) then
    -- если цитаты обнаружены, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Утечка конфиденциальной информации','RED';
```

```
end;

-- проверяется, обнаружен ли в объекте хотя бы один текстовый объект, характеризующий персональные данные
if root_has_sector_text_object(root, 'PersonalData') then
  -- если есть текстовые объекты, возвращается признак того, что политика применима и перечень параметров
  return true,Verdict.Forbidden,'Утечка персональных данных','RED';
 end;

-- проверяется обнаружен ли в объекте хотя бы один текстовый объект, характеризующий финансовую информацию
if root_has_sector_text_object(root, 'Finance') then
  return true,Verdict.Forbidden,'Утечка финансовой информации','RED';
end;

--
if root_has_sector_text_object(root, 'Insurance') then
  return true,Verdict.Forbidden,'Утечка страховой информации','RED';
end;

--
if root_has_sector_text_object(root, 'OilAndGas') then
  return true,Verdict.Forbidden,'Утечка отраслевой информации (Нефть-Газ)','RED';
end;

--
if root_has_sector_text_object(root, 'Production') then
  return true,Verdict.Forbidden,'Утечка производственной информации','RED';
end;

--
if root_has_sector_text_object(root, 'Telecommunications') then
  return true,Verdict.Forbidden,'Утечка отраслевой информации (Телекоммуникации)','RED';
end;

-- проверяется присвоена ли объекту хотя бы одна категория с родительской категорией "Нарушение
законодательства РФ"
if CategoryFromListDetected(root,'BAZA_PROTIVOD') then
  -- если есть такая категория, возвращается признак того, что политика применима и перечень параметров
  return true,Verdict.Forbidden,'Нарушение законодательства РФ','LIGHT_RED';
end;

-- проверяется обнаружена ли в объекте информация, указывающая на посещение запрещенных веб-ресурсов
if TagsFromListDetected(root,{'_DANGEROUS_','_AGGRESSIVE_','_ADULT_'}) then
  -- если есть такая информация, возвращается признак того, что политика применима и перечень параметров
  return true,Verdict.Forbidden,'Нарушение законодательства РФ','LIGHT_RED';
end;

-- проверяется входит ли хотя бы один получатель в группу подозрительных получателей
if GCC:IsRecipientInGroup(root, 'SUSPICIOUS_RECIPIENTS') then
  -- если входит, возвращается признак того, что политика применима и перечень параметров
  return true,Verdict.Forbidden,'Получатель обнаружен в группе подозрительных получателей','ORANGE';
end;

-- проверяется если конфликт идентификации отправителя, получателя, или рабочей станции
if IsIdentityConflict(root) then
  -- если конфликт есть, возвращается признак того, что политика применима и перечень параметров
  return true,Verdict.Forbidden,'Конфликт идентификации','ORANGE';
end;

-- проверяется содержит ли объект вложения, для которых не определен тип содержимого
if UnknownFormatDecteted(root) then
  -- если содержит, возвращается признак того, что политика применима и перечень параметров
  return true,Verdict.Forbidden,'Файл неизвестного формата','LIGHT_ORANGE';
end;
```

```
  -- проверяется, содержит ли объект зашифрованные данные
  if EncryptedContentDecteted(root) then
    -- если содержит, возвращается признак того, что политика применима и перечень параметров
    return true,Verdict.Forbidden,'Зашифрованный текст','LIGHT_ORANGE';
  end;

  -- иначе возвращается признак того, что политика не применима
  return false;
end;


-- Сценарий ---------------------------------------------------------------------------

function Process(root)
  -- * Установка транспортного режима (задается для каждого монитора)
  SetDefaultTransportMode(root);

  -- определение локальных переменных
  local result,verdict, verdict_reason,color;

  if root.envelope.monitor == Monitor.Crawler then
    result,verdict,verdict_reason,color=CheckCrawlerPolicy(root);

    if result then
      ApplyPolicy(root,false,verdict,verdict_reason,color);
      return;
    end;

    ApplyPolicy(root,true,Verdict.Allowed,'Ничего не обнаружено','');
    return;

  end;

  -- Мусорный трафик
  result,verdict,verdict_reason,color = CheckGarbage(root);
  -- если объект удовлетворяет условиям политики
  if result then
    -- применить политику, удаляем объект
    ApplyPolicy(root,true,verdict,verdict_reason,color);
    -- прекратить обработку объекта, другие политики не применять
    return;
  end;

  -- * Проверка перехваченного объекта на возможность применения одной из политик

  -- Проверка возможности применения разрешающей политики
  result,verdict,verdict_reason,color = CheckPermissionPolicy(root);
  -- если объект удовлетворяет условиям политики
  if result then
    -- применить политику
    ApplyPolicy(root,false,verdict,verdict_reason,color);
    -- если требуется не сохранять объект в базе данных, установите второй параметр (delete_content) в true
    -- прекратить обработку объекта, другие политики не применять
    return;
  end;

  -- Проверка возможности применения политики обработки нарушений
  result,verdict,verdict_reason,color = CheckViolationPolicy(root);
  -- если объект удовлетворяет условиям политики
  if result then
    -- уведомить офицера безопасности
    SendNotificationUser(root);
```

```
    -- применить политику
    ApplyPolicy(root,false,verdict,verdict_reason,color);
    -- прекратить обработку объекта, другие политики не применять
    return;
  end;

  -- Проверка возможности применения политики обработки потенциальных нарушений
  result,verdict,verdict_reason,color = CheckPotentialViolationPolicy(root);
  -- если объект удовлетворяет условиям политики
  if result then
    -- применить политику
    ApplyPolicy(root,false,verdict,verdict_reason,color);
    -- прекратить обработку объекта, другие политики не применять
    return;
  end;

  -- Проверка возможности применения политики нецелевого использования ресурсов
  result,verdict,verdict_reason,color = CheckNoPurposeResourcesUsagePolicy(root);
  -- если объект удовлетворяет условиям политики
  if result then
    -- применить политику
    ApplyPolicy(root,false,verdict,verdict_reason,color);
    -- прекратить обработку объекта, другие политики не применять
    return;
  end;

  -- Применение политики, разрешающей передачу штатных объектов
  ApplyPolicy(root,false,Verdict.Allowed,'Ничего не обнаружено','');

end;
```

8 Анализ объектов

При анализе объектов, обработанных Системой, пользователю доступны следующие основные действия:

- Составление запросов по объектам
- Работа пользователя с объектами
- Составление отчетов по объектам
- Управление папками запросов и отчетов

8.1 Составление запросов по объектам

Объекты, проверенные Системой, сохраняются в базу данных. Чтобы просмотреть в Консоли управления информацию по объектам, загруженным в базу данных, нужно создать и применить запрос.

Работа с запросами ведется в разделе **Запросы** (область **Запросы и отчеты** на панели **Навигация**). Для более удобной работы, запросы можно группировать по папкам (см. "Управление папками запросов и отчетов").

Подробную информацию о порядке составления запросов вы можете найти в следующих разделах:

- Правила оптимизации запросов
- Реализация поиска по тексту, извлеченному из перехваченных объектов

- Создание и редактирование запроса
- Копирование запроса
- Удаление запроса

8.1.1 Правила оптимизации запросов

С целью оптимизации выполнения запросов, атрибуты объекта (подробный список см. "Общие атрибуты объекта" и "Заголовки конвертов и заголовки объектов") разделены на три группы:

- **Общие атрибуты**. Информация, связанная с обработкой объекта системой InfoWatch Traffic Monitor. Здесь же выводятся сведения об отправителе и получателе объектов.

- **Заголовки конверта**. Под конвертом в Системе понимается набор данных, связанных с транспортировкой объекта, например, *IP-адрес источника*, *Сервер перехвата*, *Порт назначения* и т. п.

- **Заголовки объекта**. В данной группе выводится информация о заголовках, входящих в состав объекта. Набор заголовков определяется типом объекта, например, *From*, *To*, *Cc*, *Subject* и т.п.

Запросы по общим атрибутам имеют наименьшее время выполнения. При добавлении в условия запроса заголовков конверта и/или объекта время выполнения запроса увеличивается.

Чтобы сократить время выполнения запроса к базе данных, придерживайтесь следующих правил (расположены в порядке убывания эффективности – т.е. наименьшее время выполнения запроса достигается при соблюдении первого правила, последнее, наоборот, имеет наименьшую эффективность):

1. Составьте условие для поиска объектов по атрибуту *ID объекта*. Поиск объектов по идентификатору выполняется с наивысшей скоростью.

2. Составьте условие для поиска объектов по атрибуту *Дата перехвата*. Чем меньше будет промежуток времени, указанный в этом условии, тем быстрее будет выполняться запрос.

3. Составьте условие для поиска объектов по следующим общим атрибутам: *Вердикт*, *Версия конфигурации, Дата вставки*, *Зона ответственности*, *Логин*, *Монитор*, *Отправитель*, *Список получателей, Фамилия пользователя.*

4. Составьте условие для поиска объектов по заголовкам конверта либо по заголовкам объекта, либо по следующим общим атрибутам: *Категория*, *Тег*, *Тип объекта*, *Цвет*.

5. Старайтесь как можно меньше объединять условия посредством логического оператора *ИЛИ*.

Если вам необходимо оптимизировать запрос, в котором присутствуют лишь общие атрибуты, не указанные в правилах 3 и 4, то обратитесь в службу технической поддержки.

8.1.1.1 Общие атрибуты объекта

В этом разделе перечислены общие атрибуты объектов и указано, доступны ли эти атрибуты для пользователя:

- **запросы/отчеты** (см. "Создание и редактирование запроса" и "Создание и редактирование отчета"):
  - **условия запроса/отчета** - доступно ли создание запроса по значению данного атрибута (см. " Настройка условий запроса");
  - **поля просмотра** - является ли данный атрибут полем просмотра на панели объектов (см. "Выбор

полей просмотра");

- **сортировка** - возможна ли сортировка записей по значениям данного атрибута (см. "Настройка условий сортировки");
- **группировка** - возможна ли группировка записей по значениям данного атрибута (см. "Настройка порядка группирования");

- **панель информации об объекте** - отображается ли информация по данному атрибуту на панели информации об объекте (см. "Настройка панели информации об объекте");
- **видимость** - отображается ли информация по данному атрибуту на панели информации об объекте при выключенном режиме "*Показывать содержимое объектов*" (см. "Настройка режима просмотра содержимого объекта")

Атрибут объекта	Описание	Запросы / Отчеты				Панель информации об объекте	Видимость
		Условия запроса/ отчета	Поля просмотра	Сортировка	Группировка		
ID объекта	Уникальный идентификационный номер объекта в базе данных **Примечание**: уникальный идентификатор назначается не только самим объектам, но и вложениям. Поэтому при сортировке записей по этому атрибуту идентификаторы могут отображаться с непоследовательной нумерацией (1, 3, 5 и т. п.)	+	+	+	+	+	+
Вердикт	Вердикт, присвоенный объекту	+	+	+	+	+	+
Версия конфигурации	Версия конфигурации, по которой был проверен объект	+	+	+	+	+	+
Вложения	Признак наличия у объекта вложений	+	+	+	+	-	-
Дата вставки	Дата и время сохранения объекта в базу данных	+	+	+	+	+	+
Дата доставки	Дата и время передачи объекта на дальнейшую доставку.	+	+	+	+	+	+
Дата перехвата	Дата и время перехвата объекта Системой	+	+	+	+	+	+
Зона ответственности	Зона ответственности, назначенная объекту в процессе обработки	+	+	+	+	+	+
Категория	Категории, назначенные объекту в процессе анализа	+	-	-	-	+	+

Монитор	Тип перехватчика	+	+	+	+	+	+
Описание	Описание объекта. Формируется Системой по шаблону: `<Монитор> object from <Отправитель>`	+	+	+	+	+	+
Описание рабочей станции	Дополнительные сведения о рабочей станции. Импортируются из Active Directory	-	+	+	+	+	+
Основание вердикта	Описание причины, по которой объекту был присвоен вердикт	+	+	+	+	+	+
Отправитель	Информация об отправителе объекта; для Skype Monitor - информация о пользователе Skype, с рабочей станции которого был получен объект	+	+	+	+	+	+
Ошибки идентификации	Признак наличия ошибок, произошедших при идентификации объекта: если при определении атрибутов *Отправитель*, *Список получателей* или *Рабочая станция* одному значению было найдено несколько соответствий в справочниках Active Directory (см. "Обработка данных отправителя, получателя и рабочей станции").	+	-	-	-	-	-
Ошибки объекта	Признак наличия ошибок, произошедших в процессе обработки объекта	+	+	+	+	+	+
Список получателей	Один или несколько получателей объекта	+	+	+	+	+	-
Попытки доставки	Количество попыток, предпринятых для доставки объекта получателю	+	+	+	+	+	+
Рабочая станция	Рабочая станция, с которой был отправлен объект **Примечание**: Значение данного атрибута может отображаться в одном из следующих форматов: • имя рабочей станции из Acrive Directory, если определено; • DNS, если имя рабочей	+	+	+	+	+	+

	станции из Acrive Directory не определено; • IP-адрес, если имя рабочей станции из Acrive Directory или DNS не определены.						
Размер объекта	Размер объекта	+	+	+	+	+	+
Решение	Решение, принятое пользователем по объекту	+	+	+	+	+	+
Состояние доставки	Статус доставки объекта	+	+	+	+	+	+
Тег	Теги, назначенные объекту	+	-	-	-	+	+
Текст объекта	Текст, извлеченный из перехваченного объекта	+	-	-	-	+	-
Текстовый объект	Типы текстовых объектов, обнаруженные в объекте в процессе анализа	+	-	-	-	+	+
Тип объекта	Тип объекта	+	-	-	-	+	+
Транспортный режим	Режим транспортировки, определенный для объекта	+	+	+	+	+	+
Цвет	Цвет, назначенный объекту	+	+	-	-	+	+
Эталонный документ	Эталонные документы, цитаты из которых были обнаружены в объекте в процессе анализа. Для каждого документа отображаются код (уникальный идентификатор), имя файла, путь	+	-	-	-	+	+

8.1.1.2 Заголовки конвертов и заголовки объектов

В этом разделе приведены заголовки конвертов и заголовки объектов с указанием их названий в контексте (см. "Детальная форма просмотра объекта") и описанием.

Название заголовка	Название заголовка в контексте	Описание
Заголовки конвертов		
Домен	auth_domain	Домен или аналог домена (из данных авторизации)
Рабочая станция	auth_host	Информация о рабочей станции (из данных авторизации)
Схема	auth_scheme	Название схемы авторизации (basic, digest, ntlm, local, radius)

Аутентификация	auth_source	Исходная строка с данными авторизации после декодирования и снятия форматных префиксов
Пользователь	auh_user	Идентификатор пользователя (из данных авторизации)
Домен	domain	Домен
Пользователь	login	Логин
Имя	userfirstname	Имя пользователя
Фамилия	userlastname	Фамилия пользователя
ICQ-инициатор	initiator_uin	UIN сотрудника, со стороны которого производится перехват объекта
ICQ-инициатор	session_initiator_uin	UIN инициатора сессии
IM-инициатор	im_initiator	Имя учетной записи сотрудника, со стороны которого производится перехват объекта
SMTP-отправитель	mail_from	E-mail отправителя (из SMTP-конверта)
SMTP-получатель	rcpt_to	E-mail адреса получателей (из SMTP-конверта)
Рабочая станция	workstation	Идентификатор рабочей станции, на стороне которой производится перехват объекта
IP-адрес источника	source_ip	IP-адрес, с которого был отправлен запрос
Порт	source_port	порт, с которого был отправлен запрос
Путь	source_path	Путь к источнику запроса
Путь к файлу	destination_path	Сетевой путь к файлу
IP-адрес назначения	destination_ip	IP-адрес сервера (соответствует IP-адресу, для которого открыта TCP-сессия)

Порт назначения	destination_port	Порт сервера (соответствует порту, для которого открыта TCP-сессия)
Тип устройства	device_type	Тип периферийного устройства
Имя устройства	device_name	Наименование периферийного устройства
URL, полный	url_host_fqdn	Полный URL ресурса, на который передается файл
URL, IP-адрес	url_host_ip	URL, включая IP-адрес ресурса, на который передается файл
URL ресурса	url_host	URL ресурса, на который передается файл
URL, параметры	url_parameters	Значение параметра <parameter> из URL
URL, пароль	url_password	Значение параметра <password> из URL
URL, путь	url_path	Директория на ресурсе, на который передается файл
URL, порт	url_port	Порт, на который передается файл
URL, схема	url_schema	Значение параметра <scheme> из URL
URL, пользователь	url_username	Значение параметра <username> из URL
Тип операции	operation	Совершаемая операция
Задание	job	Название задания
Приложение	creator_applicaion	Приложение, из которого была осуществлена передача данных
Перехватчик	interceptor	Название монитора-перехватчика
Результат перехвата	action	Информация о результатах обработки перехваченного объекта
Политика	policy_name	Название политики сканирования
Правило	rule_name	Название правила сканирования
Правило политики	policy_rule	Имя правила политики (используется для обеспечения совместимости разных версий Системы)

Сервер перехвата	capture_server	Идентификатор сервера, который перехватил объект
Наличие теневой копии	event_type	Тип события. Может принимать одно из следующих значений: • `[НазваниеМонитора]EventFull` - с теневой копией, • `[НазваниеМонитора]EventNoShadowCopy` - без теневой копии
VLAN 802.1AD	vlan_802_1ad	Данные об использованных VLAN в точке перехвата объекта
VLAN 802.1Q	vlan_802_1q	
Заголовки объектов		
Скрытая копия	cc	Копия файла, успешно созданного на съемном устройстве
Cookie	cookie	Служебные данные, связанные с использованием рабочей станцией протокола HTTP
Дата	date	Дата и время отправки сообщения
Отправитель	from	Информация об отправителе объекта. Для Skype Monitor - информация о пользователе Skype, с рабочей станции которого был получен объект
Важность	importance	Уровень важности объекта, указанный пользователем для SMTP-объекта
Имя	name	Название объекта
Приоритет	priority	Условие для определения очередности проверки объекта
Тема	subject	Тема сообщения
Получатель	(to)	Информация о получателе объекта
Цепочка адресов	x-forvarded-for	Установившаяся цепочка передачи информации – пара «Отправитель – Получатель»

8.1.2 Реализация поиска по тексту, извлеченному из перехваченных объектов

Поиск по тексту объектов и вложений осуществляется средствами Oracle Text. Поэтому при составлении запросов необходимо учитывать специфику работы с Oracle Text.

Подробную информацию об особенностях поиска по тексту вы можете найти в следующих разделах:

- Построение текстового индекса
- Синтаксис при построении условий в запросах на поиск по тексту перехваченных объектов
- Примеры обработки поисковых запросов

8.1.2.1 Построение текстового индекса

Для поиска слов в тексте используются *текстовые индексы*. Текстовый индекс – это список слов, сформированный Oracle Text из текста перехваченных объектов и их вложений, со ссылками на объекты, в которых встречаются данные слова.

В запросе по текстовому индексу пользователь задает текст, который должен быть найден в объекте. При выполнении запроса данный текст обрабатывается по тем же правилам, что и исходный текст – при построении текстового индекса, что обеспечивает корректность поиска в текстовом индексе.

При построении текстового индекса из текста выделяются отдельные слова или символы. Для западноевропейских языков разделителями слов считаются пробел и символ табуляции.

Далее выделенные слова, которые могут состоять из различных символов, преобразуются в слова, состоящие из только символов буквенно-цифрового набора:

- Символы «-» и «\» считаются знаками переноса. Если такой символ стоит в конце строки, то часть слова до символа переноса и часть, находящаяся на следующей строке, считается одним словом.

  Пример:

Исходное слово	Обработанное слово
желто- зеленый	желтозеленый
желто-зеленый	желто зеленый

- Символы «.», «!» и «?» считаются знаками препинания. При индексировании такие символы будут удалены.

Поиск по тексту не чувствителен к регистру символов. Например, слова «ДоМ» и «дом» являются для него идентичными.

При индексировании сохраняется порядок следования слов, что делает возможным поиск словосочетаний.

Также при построении текстовых индексов Oracle Text исключает слова, перечисленные в стоп-листе. Такими

словами обычно являются местоимения, предлоги, частицы. Например, для английского языка определены такие стоп-слова: *just*, *some*, *Mrs* и т.д.

Более подробные инструкции по работе с Oracle Text (порядок построения стоп-листов, определение правил преобразования текста и т.д.) вы можете найти в документации к СУБД Oracle (руководство Oracle Text Reference, версия 11g).

8.1.2.2 Синтаксис при построении условий в запросах на поиск по тексту перехваченных объектов

Для создания условий в запросах можно использовать следующие специальные символы и ключевые слова:

Символ	Ключевое слово	Описание оператора
&	AND	В условие включается каждое из объединенных оператором слов
=	EQUIV	Объединенные оператором слова считаются в условии эквивалентными
~	NOT	Из условия исключается слово, следующее за оператором
|	OR	В условие включается любое из объединенных оператором слов
{ }		Экранирует слово, заключенное в скобки. Используется, если необходимо найти зарезервированное слово (см. следующую таблицу)
\		Экранирует следующий символ. Используется, если необходимо найти зарезервированный символ (см. следующую таблицу)
( )		Выражение внутри скобок имеет более высокий приоритет
[ ]		Выражение внутри скобок имеет более высокий приоритет
%		При поиске заменяет любое количество любых символов в слове
_		При поиске заменяет один любой символ в слове

При построении условий в поисковых запросах необходимо экранировать следующие зарезервированные слова и символы:

ABOUT	MINUS	TR	-
ACCUM	NEAR	TRSYN	;
AND	NOT	TT	~
BT	NT	WITHIN	|
BTG	NTG	,	$
BTI	NTI	&	!
BTP	NTP	=	>
EQUIV	OR	?	*
FUZZY	PT	{ }	%

HASPATH	RT	\	_
INPATH	SQE	( )	
MDATA	SYN	[ ]	

8.1.2.3 Примеры обработки поисковых запросов

В системе InfoWatch Traffic Monitor текстовые индексы создаются с параметрами по умолчанию. Это необходимо учитывать при составлении поисковых запросов. Далее приводятся примеры обработки поисковых запросов.

Пусть имеется несколько фрагментов текста, содержащегося в различных документах:

Д1	В деревне Новоспасская, находящейся на юге Смоленской области, была обнаружена большая водо- мерка. Ее длина составляет 5 сантиметров, а ширина 4,32 сантиметра.
Д2	Жители деревни говорят, что она имеет иссиня-черный цвет и очень быстро пере#вигается.
Д3	Впервые она была замечена 14.05.2008. Ранее, огромная водомерка обсуждалась жителями села Григорово, которые заявляли о еще более невероятных размерах насекомого. Ее цвет они называли темно-зеленым.
Д4	The suite includes two walk-in closets and a bath-room with a deep Jacuzzi tub and separate white tile shower.

В процессе анализа из документа будут выделены следующие слова:

Д1	**Д2**	**Д3**	**Д4**
4,32	БЫСТРО	05	BATH
5	ВИГАЕТСЯ	14	CLOSETS
А	ГОВОРЯТ	2008	DEEP
БОЛЬШАЯ	ДЕРЕВНИ	БОЛЕЕ	INCLUDES
БЫЛА	ЖИТЕЛИ	БЫЛА	JACUZZI
В	И	ВОДОМЕРКА	ROOM
ВОДОМЕРКА	ИМЕЕТ	ВПЕРВЫЕ	SEPARATE
ДЕРЕВНЕ	ИССИНЯ	ГРИГОРОВО	SHOWER
ДЛИНА	ОНА	ЕЕ	SUITE
ЕЕ	ОЧЕНЬ	ЕЩЕ	TILE
НА	ПЕРЕ	ЖИТЕЛЯМИ	TUB
НАХОДЯЩЕЙСЯ	ЦВЕТ	ЗАМЕЧЕНА	TWO
НОВОСПАССКАЯ	ЧЕРНЫЙ	ЗАЯВЛЯЛИ	WALK
ОБЛАСТИ	ЧТО	ЗЕЛЕНЫМ	WHITE
ОБНАРУЖЕНА		КОТОРЫЕ	
САНТИМЕТРА		НАЗЫВАЛИ	
САНТИМЕТРОВ		НАСЕКОМОГО	
СМОЛЕНСКОЙ		НЕВЕРОЯТНЫХ	
СОСТАВЛЯЕТ		О	

Д1	**Д2**	**Д3**	**Д4**
ШИРИНА ЮГЕ		ОБСУЖДАЛАСЬ ОГРОМНАЯ ОНА ОНИ РАЗМЕРАХ РАНЕЕ СЕЛА ТЕМНО ЦВЕТ	

Число *4,32* включено в индекс, несмотря на то, что символ запятой разделяет строку на части. Это объясняется тем, что слева и справа от запятой находятся символы-цифры и, следовательно, весь набор символов считается единым числом.

Дата *14.05.2008* разделена на отдельные числа.

Во втором документе (Д2) слово *передвигается* написано с ошибкой – *пере#вигается*. Поэтому индекс содержит два слова: *ПЕРЕ* и *ВИГАЕТСЯ*.

Слово *иссиня-черный* разделено на два слова *ИССИНЯ* и *ЧЕРНЫЙ*.

В следующих примерах показаны принципы составления поисковых запросов.

Пример 1. Поиск одного слова

Условие запроса: *водомерка*

Результат: Д1 и Д3

Пояснение: В тексте документа Д1 слово *водомерка* перенесено на следующую строку при помощи символа переноса. Поэтому оно было объединено в одно слово и найдено по запросу. В тексте документа Д3 слово присутствует в том же виде, что и в запросе.

Пример 2. Поиск словосочетания

Условие запроса: *иссиня черный*

Результат: Д2

Пояснение: Слова *иссиня* и *черный* находятся в документе Д2 рядом. Таким образом, словосочетание *иссиня черный* будет найдено в документе Д2.

Приведенный пример позволяет найти слова, идущие друг за другом, т.е. образующие словосочетание. В примере 4 показан запрос для поиска слов, разделенных другими словами.

Пример 3. Экранирование зарезервированного символа

Условие запроса: *иссиня\-черный*

Результат: Д2

Пояснение: Зарезервированный символ «-» экранирован символом «\» и поэтому воспринимается как обычный символ. После того как поисковый запрос будет приведен в соответствие с общими правилами, останется словосочетание *иссиня черный*, которое и содержится в тексте документа Д2.

Пример 4. Поиск слов, стоящих непоследовательно

Если необходимо найти слова, которые не образуют словосочетания (т.е. разделены в тексте другими словами), то поиск словосочетаний не даст результата. Например:

Условие запроса: *иссиня быстро*

Результат: ничего не найдено

Пояснение: В тексте документа Д2 присутствуют слова *иссиня* и *быстро*. Однако эти слова разделены другим словом. Поэтому ничего не будет найдено.

Для поиска слов, стоящих непоследовательно, используйте символ & или оператор AND. Например:

Условие запроса: *водомерка & длина*

или

водомерка AND длина

Результат: Д1

Пояснение: В данном случае символ «&» и слово AND зарезервированы для поиска. Эта запись означает, что в документе присутствуют слова *водомерка* и *длина*. Оба этих слова присутствуют только в документе Д1.

Пример 5. Использование EQUIV

Условие запроса: *большая EQUIV огромная водомерка*

или

большая = огромная водомерка

Результат: Д1 и Д3

Пояснение: Оператор EQUIV определяет, что слова слева и справа от него являются эквивалентными частями запроса. Фактически это означает, что будут выполнены следующие запросы *большая водомерка* и *огромная водомерка*. Таким образом, будут найдены документы Д1 и Д3.

Пример 6. Использование NOT

Условие запроса: *водомерка NOT григорово*

Результат: Д1

Пояснение: Данное выражение интерпретируется следующим образом: в документе должно содержаться слово *водомерка* и не должно содержаться слово *григорово.* Под эти условия подходит только документ Д1.

Пример 7. Использование OR

Условие запроса: *новоспасская OR григорово*

Результат: Д1 и Д3

Пояснение: Данное выражение интерпретируется следующим образом: в документе должно содержаться слово *новоспасская* или слово *григорово.* Под эти условия подходят документы Д1 и Д3.

Пример 8. Экранирование зарезервированного слова и символа

Условие запроса: *closets {and} a bath\-room*

Результат: Д4

Пояснение: В данном примере экранировано слово AND и символ «_». Результат поиска – документ Д4.

Пример 9. Использование скобок

Условие запроса 1: *(водомерка OR очень) AND цвет*

Результат 1: Д2 и Д3

Условие запроса 2: *водомерка OR (очень AND цвет)*

Результат 2: Д1, Д2 и Д3

Пояснение: Условие 1 означает, что в документе должно быть одно из слов: *водомерка* или *очень,* и при этом обязательно должно быть слово *цвет.* Документ Д2 включает в себя слова *цвет* и *очень,* документ Д3 включает слова *водомерка* и *цвет*.

Условие 2 означает, что в документе должно быть слово *водомерка* или одновременно содержатся слова *очень* и *цвет.* В документах Д1 и Д3 содержится слово *водомерка* а в документе Д2 содержатся одновременно слова *очень* и *цвет*.

Пример 10. Использование маски %

Условие запроса: *жител%*

Результат: Д2 и Д3

Пояснение: Маска «%» заменяет любое количество символов, поэтому результат запроса – документ Д2, содержащий слово *Жители,* и документ Д3, содержащий слово *жителями*.

Пример 11. Использование маски _

Условие запроса: *деревн_*

Результат: Д1 и Д2

Пояснение: Маска «_» заменяет один символ, поэтому результат запроса – документ Д1, содержащий слово *деревне,* и документ Д2, содержащий слово *деревни.*

Пример 12. Использование нескольких возможностей

Условие запроса: *(жител% сел_=деревн_) OR walk\-in*

Результат: Д2, Д3 и Д4

Пояснение: Условие *(жител% сел_=деревн_)* дает в результате документы Д2 и Д3, содержащие тексты *Жители деревни* и *жителями села* соответственно. Условие *walk\-in* дает в результате документ Д4. Поскольку эти условия объединены оператором OR, то результатом запроса будут все три документа.

8.1.3 Создание и редактирование запроса

Важная информация!

В разделе "Правила оптимизации запросов" приведены рекомендации по сокращению времени выполнения запросов.

Примечание

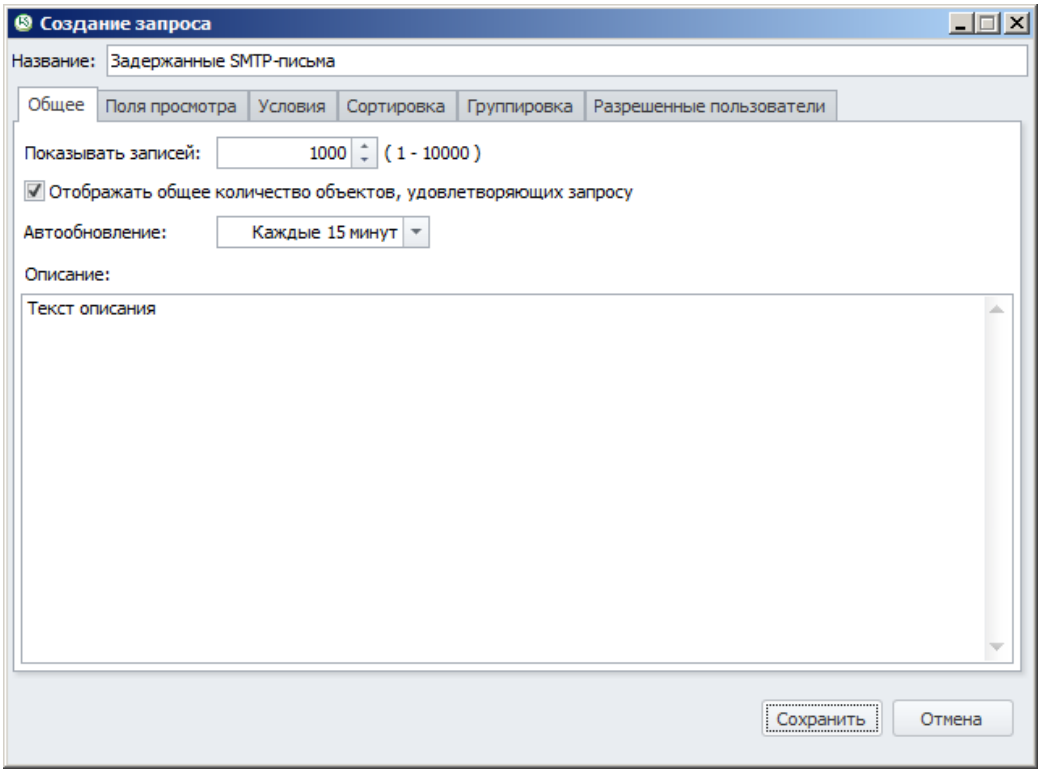
Редактировать запрос можно, если запрос имеет статус *Готов* или *Ошибка*.

Чтобы создать запрос:

1. Перейдите к разделу **Запросы**.
2. Выполните необходимые действия:

Необходимое действие	Порядок выполнения
Создать запрос	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Создать запрос** • нажмите кнопку **Создать запрос** на панели инструментов
Отредактировать запрос	1. В списке запросов выделите строку с нужным запросом. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку **Изменить** на панели инструментов.

На экран будет выведено диалоговое окно для настройки запроса.



Диалоговое окно настройки запроса

3. Укажите имя запроса в поле **Название**.
4. Настройте параметры запроса, используя вкладки:

Название вкладки	**Действие**
Общее	Настройка общих параметров
Поля просмотра	Выбор атрибутов объекта, которые будут отображаться на панели объектов
Условия	Настройка условий запроса
Сортировка	Назначение порядка сортировки объектов
Группировка	Назначение порядка группирования объектов
Разрешенные пользователи	Выбор пользователей, которые смогут выполнять запрос

5. Когда все параметры запроса будут заданы, нажмите кнопку **Сохранить**.

Примечание

Чтобы просмотреть записи, удовлетворяющие новому запросу, необходимо выполнить этот запрос (см. "Выполнение запроса по объектам").

8.1.3.1 Общие параметры запроса (вкладка Общее)

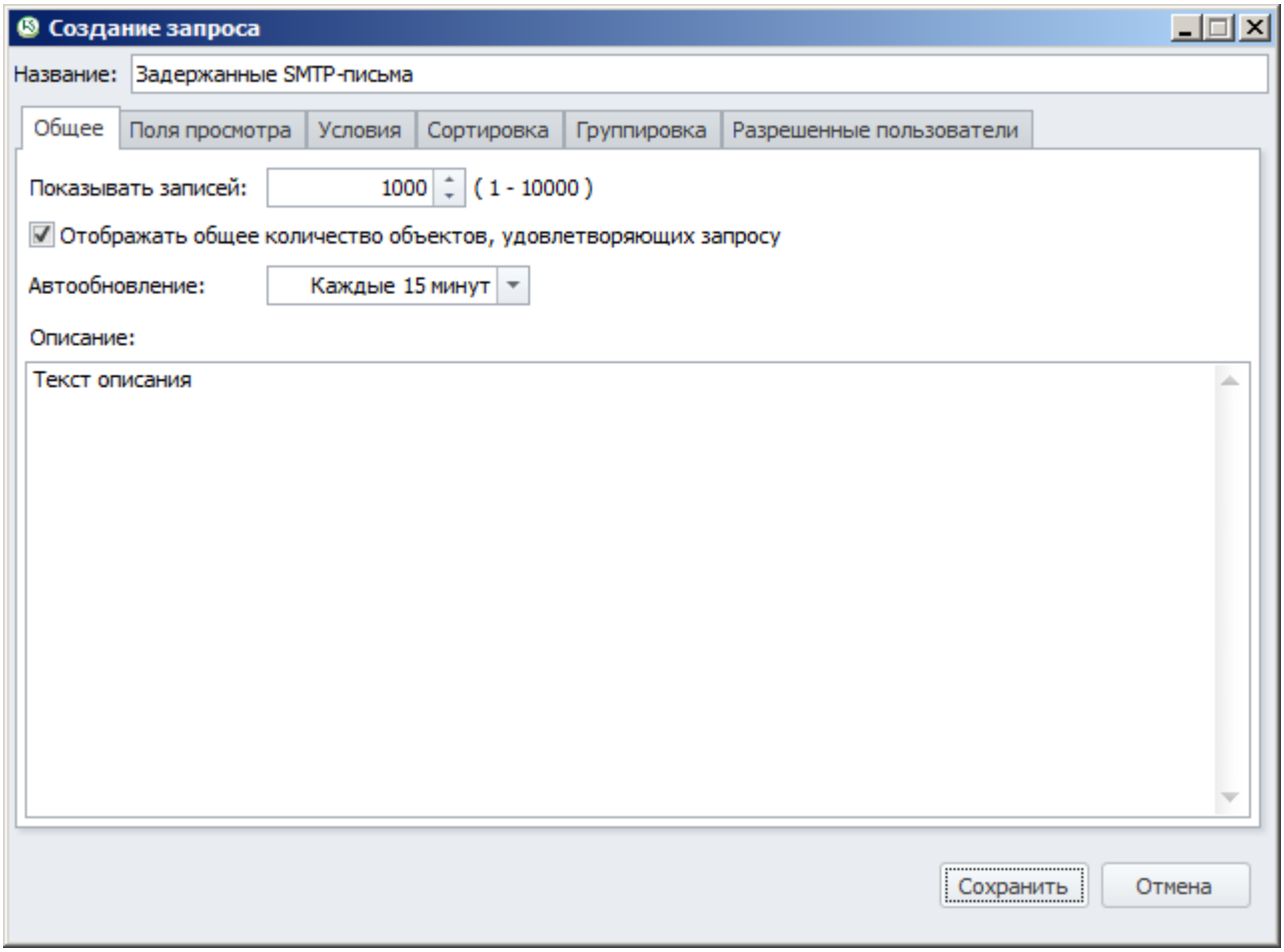
На вкладке **Общее** настраивают общие параметры запроса:

- **Показывать записей**. Ограничение на количество записей, выводимых в рабочей области Консоли управления (можно указывать любые значения в диапазоне от **1** до **10000** писем). Значение по умолчанию **1000** записей.

- **Автообновление**. Вы можете настроить автоматическое обновление результатов запроса. Для этого в раскрывающемся списке выберите необходимый период обновления (о том, как изменить параметры автоматического обновления для уже созданного запроса см. "Автоматическое обновление").

- **Отображать общее количество объектов, удовлетворяющих запросу**. Если данный флажок установлен, и количество записей по запросу превышает значение, указанное в поле **Количество записей**, то в строке состояния будет отображаться общее количество записей в БД, удовлетворяющих запросу. По умолчанию флажок снят.

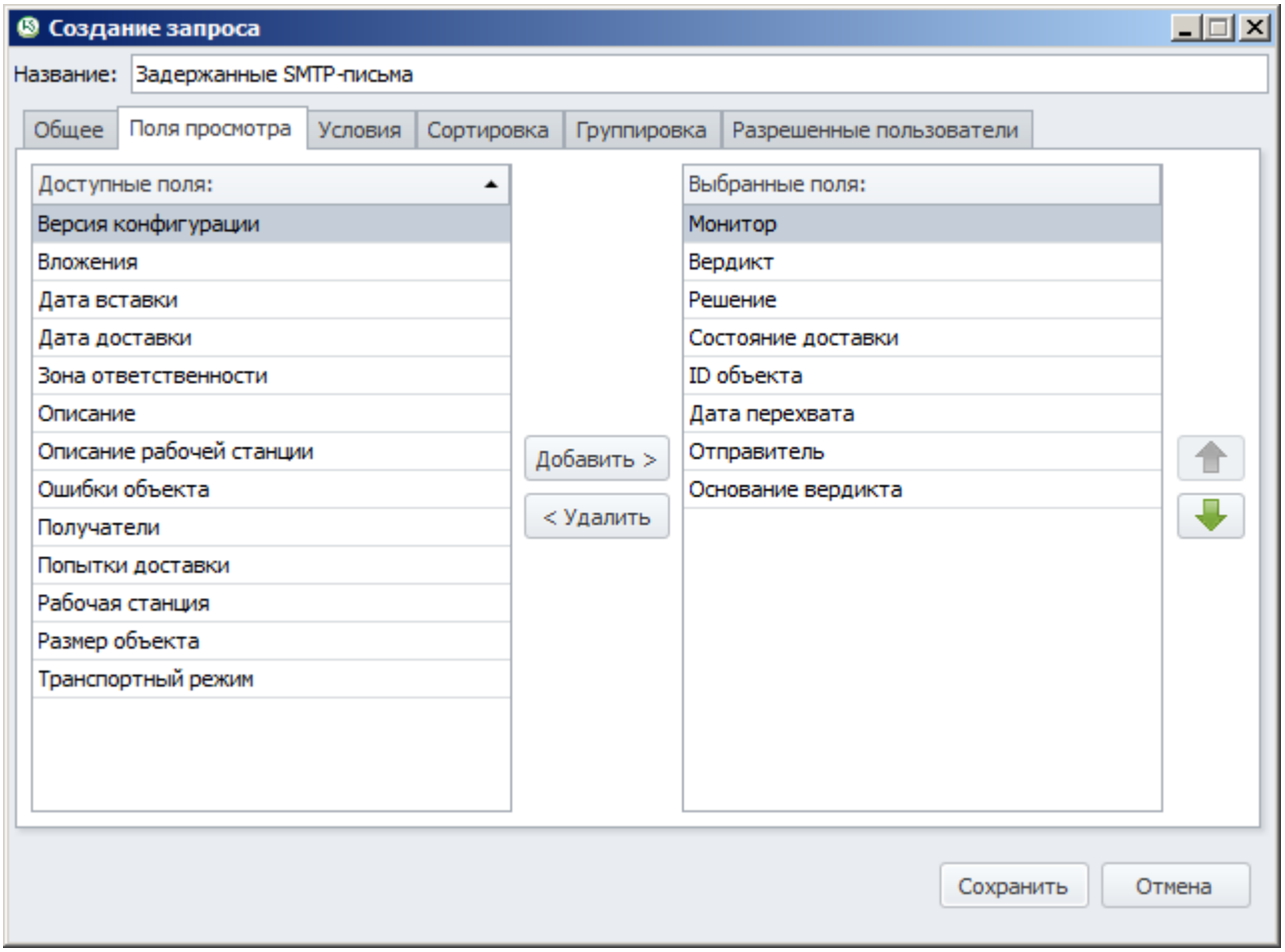
- **Описание**. Указывается описание запроса.



Вкладка "Общее"

8.1.3.2 Выбор полей просмотра (вкладка Поля просмотра)

На вкладке **Поля просмотра** указывают атрибуты записей, по которым нужно отображать информацию в области просмотра (по умолчанию отображается только часть общих атрибутов).



Вкладка "Поля просмотра"

Настройка полей просмотра осуществляется при помощи следующих кнопок:

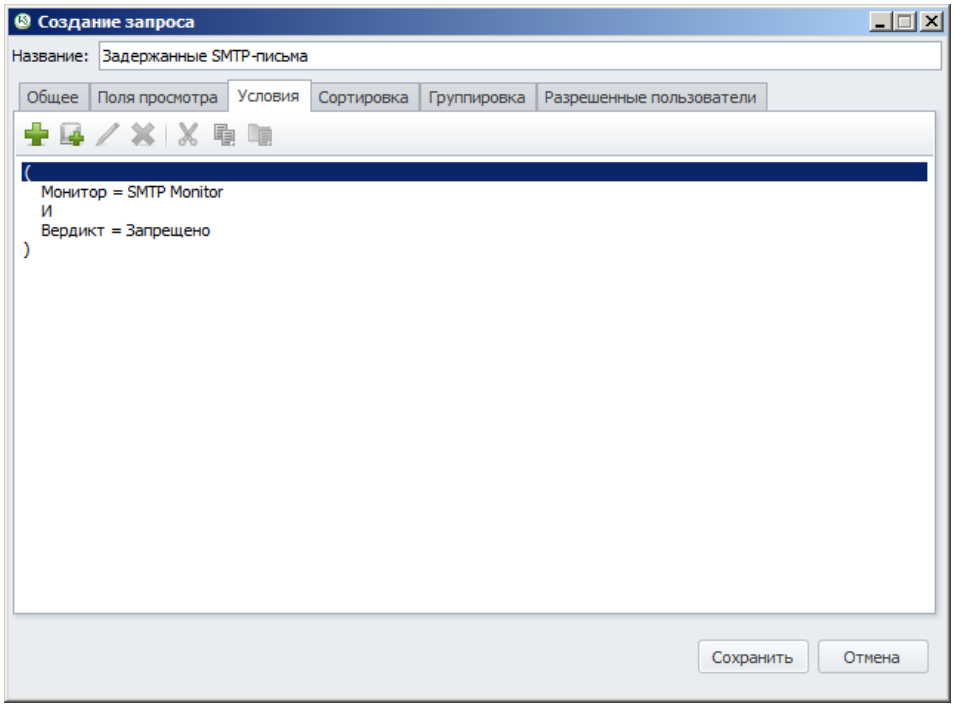
Кнопка	Название кнопки	Назначение кнопки
Добавить >	**Добавить**	Перенести поле, выделенное в списке доступных, в список выбранных.
< Удалить	**Удалить**	Перенести поле, выделенное в списке выбранных, в список доступных.
	**Вверх**	Переместить выделенное поле просмотра на одну строку вверх (столбец со значениями данного параметра будет отображаться левее в области просмотра)
	**Вниз**	Переместить выделенное поле просмотра на одну строку вниз (столбец со значениями данного параметра будет отображаться правее в области просмотра)

Важная информация!

После удаления атрибутов из списка, информация по этим атрибутам выводиться не будет. Причем все параметры запроса (условия запроса, порядок сортировки, группировки), настроенные для такого атрибута, будут потеряны.

8.1.3.3 Настройка условий запроса (вкладка Условия)

При составлении запроса вы можете настроить поиск по общим атрибутам и/или контекстный поиск по заголовкам объекта. Критерии для выбора записей из базы данных задают на вкладке **Условия**.



Вкладка "Условия"

Примечание

Для обеспечения возможности контекстного поиска, в системе предусмотрена процедура переиндексации, которая по умолчанию выполняется каждые 10 минут. Администратор базы данных может при необходимости изменить этот интервал (см. документ «*InfoWatch Traffic Monitor. Руководство администратора*»).

Информация по работе с условиями содержится в подразделах:

- Создание условия запроса
- Параметры условия
- Редактирование условий запроса

8.1.3.3.1 Создание условия запроса

Примечание

Перед тем как создавать условия ознакомьтесь с рекомендациями по увеличению скорости выполнения запросов ("Правила оптимизации запросов").

Условие может быть как простым (не содержащим логических операторов), так и составным. В составном условии содержится несколько простых условий, разделенных логическими операторами. Для формирования составного условия применяются логические операторы **И** и **ИЛИ**.

При использовании логического оператора **И** будут найдены записи, удовлетворяющие одновременно всем заданным условиям. Если нужно найти записи, удовлетворяющие хотя бы одному условию, используйте логический оператор **ИЛИ**.

Ниже показан пример объединения двух условий при помощи логического оператора **ИЛИ**.

```
(
  Категория = [1] [Все конфигурации] HR
  ИЛИ
  Категория = [1] [Все конфигурации] Внутренние выплаты
)
```

Объединение двух условий

Для создания более сложных условий можно использовать блоки условий. **Блоком условий** называется группа, состоящая из простого или составного условия, отделенная от другого условия или группы условий логическим оператором и скобками.

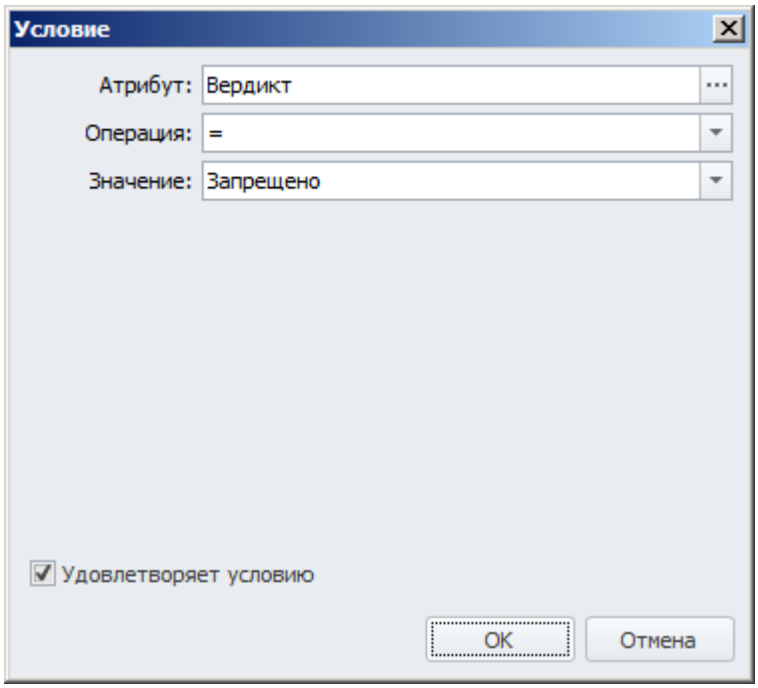
Особенности работы с блоками условий:

- Все условия вставляются в корневой блок, который не может быть удален.
- В состав блока условий могут быть добавлены другие блоки условий. Таким образом, внутри корневого блока может быть создано несколько блоков условий, объединенных логическими операторами.
- Условия, принадлежащие к одному блоку, отделяются от остальных условий скобками.

Чтобы добавить простое условие:

1. Выделите строку с открывающей или закрывающей скобкой.
2. Нажмите кнопку **Добавить условие** в верхней части вкладки.

   На экран будет выведено диалоговое окно **Условие**.



Настройка условий запроса

3. Настройте параметры условия (см. "Параметры условия").
4. Нажмите кнопку **OK**.

   После нажатия кнопки **OK** новое условие будет отображено на вкладке **Условия**.

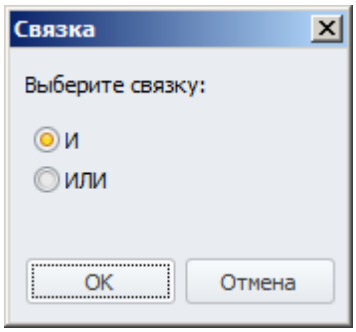
Чтобы добавить составное условие:

1. Выделите строку с открывающей или закрывающей скобкой.
2. Нажмите кнопку **Добавить условие** в верхней части вкладки. В открывшемся диалоговом окне **Условие** настройте параметры первого условия (см. "Параметры условия").
3. Выделите строку, после которой нужно вставить условие.

   Примечание

   При выделении закрывающей скобки новое условие будет вставлено перед этой скобкой.

4. Нажмите кнопку **Добавить условие**. Задайте второе условие и нажмите кнопку **OK**. После этого на экран будет выведено диалоговое окно **Связка**.



Выбор логического оператора

5. Выберите нужный логический оператор и нажмите кнопку **OK**.

   После этого на вкладке **Условия** будут отображены два условия, объединенные выбранным логическим оператором.

Чтобы вставить блок условий:

1. Выделите строку, после которой нужно вставить блок условий.

   Примечание

   При выделении закрывающей скобки новый блок условий будет вставлен перед этой скобкой.

2. Нажмите кнопку **Добавить блок**.

   Если в скобках уже содержится условие или блок условий, то после нажатия кнопки **Добавить блок** будет открыто диалоговое окно **Связка**, в котором вам нужно выбрать один из доступных логических операторов. Выбрав подходящий логический оператор, нажмите кнопку **OK**.

   После этого на вкладке **Условия** диалогового окна запроса появится новый блок условий.

3. Добавьте в блок простое или составное условие.

Вы можете создавать и более сложные условия. Пример запроса, в котором объединено несколько условий, показан на рисунке.

```
(
  Монитор = Device Monitor
  И
  (
    Категория = [1] [Все конфигурации] HR
    ИЛИ
    Категория = [1] [Все конфигурации] Внутренние выплаты
  )
)
```

Пример составления сложного условия

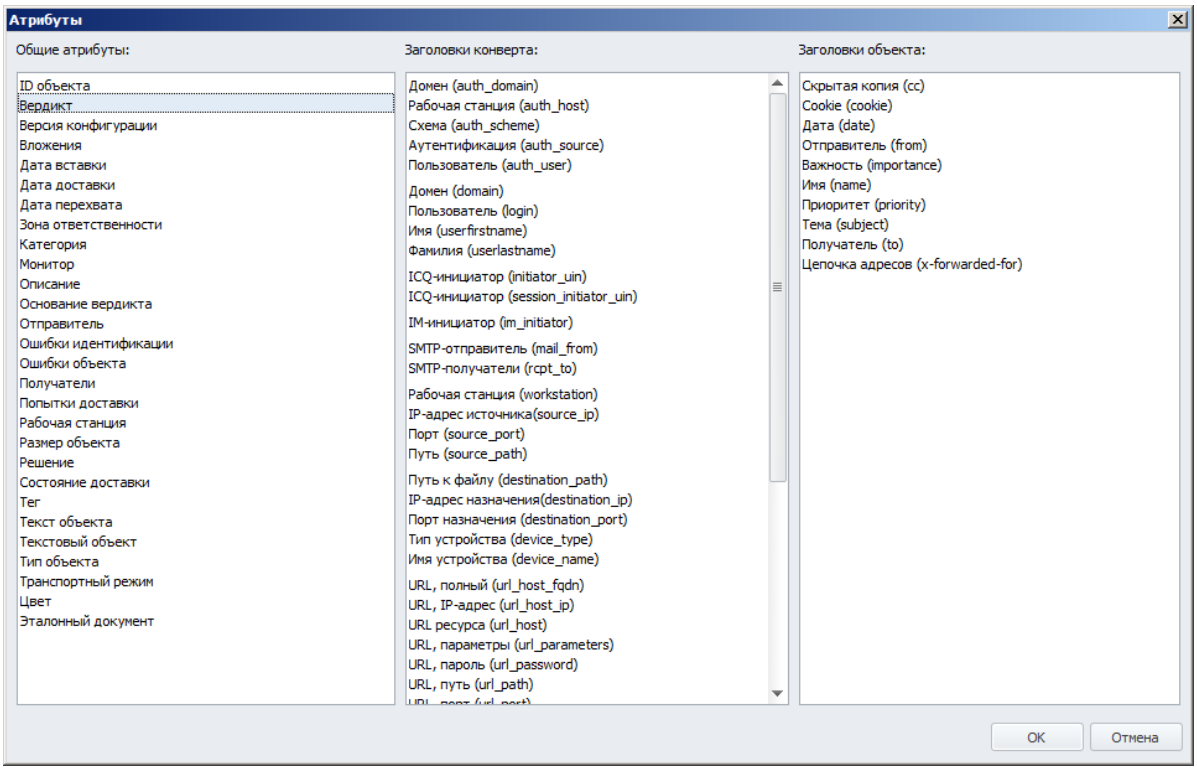
8.1.3.3.2 Параметры условия

Примечание

Перед тем как создавать условия ознакомьтесь с рекомендациями по увеличению скорости выполнения запросов (см. "Правила оптимизации запросов").

В диалоговом окне **Условие** задаются параметры условия:

- **Атрибут**. Нажмите кнопку . В открывшемся диалоговом окне выберите атрибут, для которого нужно задать условие запроса. Вы можете задавать условия как по общим атрибутам объекта, так и по заголовкам. Типы атрибутов описаны в разделе "Правила оптимизации запросов"; описание общих атрибутов приведено в разделе "Общие атрибуты объекта"; описание заголовков конвертов и объектов приведено в разделе "Заголовки конвертов и заголовки объектов"; настройка списка заголовков объектов, доступных для включения в условия запроса, описана в разделе "Настройка поиска по заголовкам объектов".



Выбор атрибута записи

- **Интервал**. Параметр используется только при поиске записей по дате. Нужный период времени выбирают из раскрывающегося списка. Список доступных интервалов приводится в следующей таблице.

Интервал	**Описание интервала**
Последние {0} часа(ов)	Последние N часов (начало периода определяется вычитанием N часов из времени выполнения запроса). Нужное значение задается в поле счетчика (значение по умолчанию 3 часа)
Текущий день	От 00 ч 00 мин 00 с текущих суток до времени выполнения запроса
Текущая неделя	От 00 ч 00 мин 00 с первых суток текущей недели до времени выполнения запроса
Текущий месяц	От 00 ч 00 мин 00 с первого числа текущего месяца до времени выполнения запроса
Последние сутки	От 00 ч 00 мин 00 с предыдущих суток до времени выполнения запроса Например, запрос выполняется 16 мая, в 16 ч 00 мин 00 с. Тогда в результирующей выборке будут содержаться сведения, начиная с 00 ч 00 мин 00 с 15 мая и по 16 ч 00 мин 00 с 16 мая
Последняя неделя	От 00 ч 00 мин 00 с первых суток предыдущей недели до времени выполнения запроса Например, запрос выполняется в пятницу 16 мая, в 16 ч 00 мин 00 с. Тогда в результирующей выборке будут содержаться сведения, начиная с 00 ч 00 мин 00 с 5 мая и по 16 ч 00 мин 00 с 16 мая
Последний месяц	От 00 ч 00 мин 00 с первого числа предыдущего месяца до времени выполнения запроса Например, запрос выполняется 16 мая в 16 ч 00 мин 00 с. Тогда в

Интервал	Описание интервала
	результирующей выборке будут содержаться сведения, начиная с 00 ч 00 мин 00 с 1 апреля и по 16 ч 00 мин 00 с 16 мая
Произвольный период	Период задается пользователем. Настройка интервала выполняется в полях **Операция** и **Значение**.

- **Операция**. Из раскрывающегося списка выберите требуемый оператор сравнения.

Каждому атрибуту соответствует свой набор операторов сравнения. Расшифровка значений операторов сравнения приведена в следующей таблице.

Оператор	Значение
=	Равно
!=	Не равно
>	Больше
<	Меньше
>=	Больше или равно
<=	Меньше или равно
between	Диапазон значений
is null	В объекте присутствует атрибут, но его значение пусто
exists	В объекте присутствует выбранный атрибут
is empty	Для атрибута ***Текст объекта*** – из объекта и его приложений не было получено текста; для остальных атрибутов – у выбранного заголовка нет значения
contains (оператор контекстного поиска)	Текст содержит указанное значение
Присвоены все из списка / Входит в группу / Не определены … и т.п	Для атрибутов ***Тег***, ***Отправитель***, ***Список получателей*** и ***Рабочая станция*** доступен выбор значений из справочников. Возможные операторы зависят от выбранного атрибута.

- **Значение**. Выберите или введите значение атрибута.

> **Примечание**
>
> Для поиска записей по атрибутам, содержащим пустые поля, используйте оператор **is null**.

При вводе значений атрибутов вы можете использовать маски: «_» и «?» – замена одного символа; «%» и «*» – замена нескольких символов.

При выборе атрибутов ***Тег***, ***Отправитель***, ***Список получателей*** и ***Рабочая станция*** вы можете выбирать значения из справочников. Для этого нажмите **Выбрать**, в открывшемся окне отметьте

необходимые значения, затем нажмите **Сохранить**.

При выборе оператора **between** в полях **Значения** можно задавать границы диапазона значений: в верхнем поле – минимальное значение атрибута, в нижнем – максимальное.

При выборе оператора **contains** осуществляется поиск по тексту объекта с использованием функции Oracle Text. Сведения о настройке параметров поиска приведены в разделе "Особенности поиска по тексту". При вводе значений атрибутов в операторе **contains** вы можете использовать только маски: «_» (замена одного символа) и «%» (замена нескольких символов). Чтобы проверить корректность введенного текста условия, нажмите кнопку **Проверить**.

Важная информация!

Маски «?» и «*» в операторе **contains** не применяются.

- **Конфигурация**. Параметр используется только при составлении условий по атрибуту ***Категория***. Вы можете задать в условии определенную версию конфигурации. В этом случае в запросе будут выведены данные только по тем объектам, которые были задержаны тогда, когда на сервере действовала указанная версия конфигурации.

  Для выбора версии нажмите кнопку ... В открывшемся диалоговом окне выделите строку с нужной версией и нажмите кнопку **OK**.

  Примечание

  Чтобы выполнить поиск объектов вне зависимости от версии конфигурации, установите флажок в поле **Искать выбранное значение во всех конфигурациях, в которых оно существует**.

- **Без учета регистра**. Укажите, нужно ли при поиске по атрибутам, имеющим текстовое значение, учитывать регистр вводимых символов. Если флажок в данном поле установлен, то поиск ведется без учета регистра символов. По умолчанию флажок снят – поиск ведется с учетом регистра символов.

- **Удовлетворяет условию**. Снимите флажок в данном поле, если необходимо вывести записи, не удовлетворяющие заданным условиям. По умолчанию флажок установлен.

8.1.3.3.3 Редактирование условий запроса

При редактировании условий запроса вам доступны следующие действия:

- изменить условие поиска;
- вырезать условие поиска;
- скопировать условие поиска;
- вставить условие поиска;
- изменить логический оператор, объединяющий условия;
- удалить простое условие запроса;
- удалить блок условий.

Кнопки, с помощью которых выполняется редактирование условий запроса, расположены в верхней части вкладки **Условия**.

Чтобы отредактировать условия запроса,

выполните нужное действие:

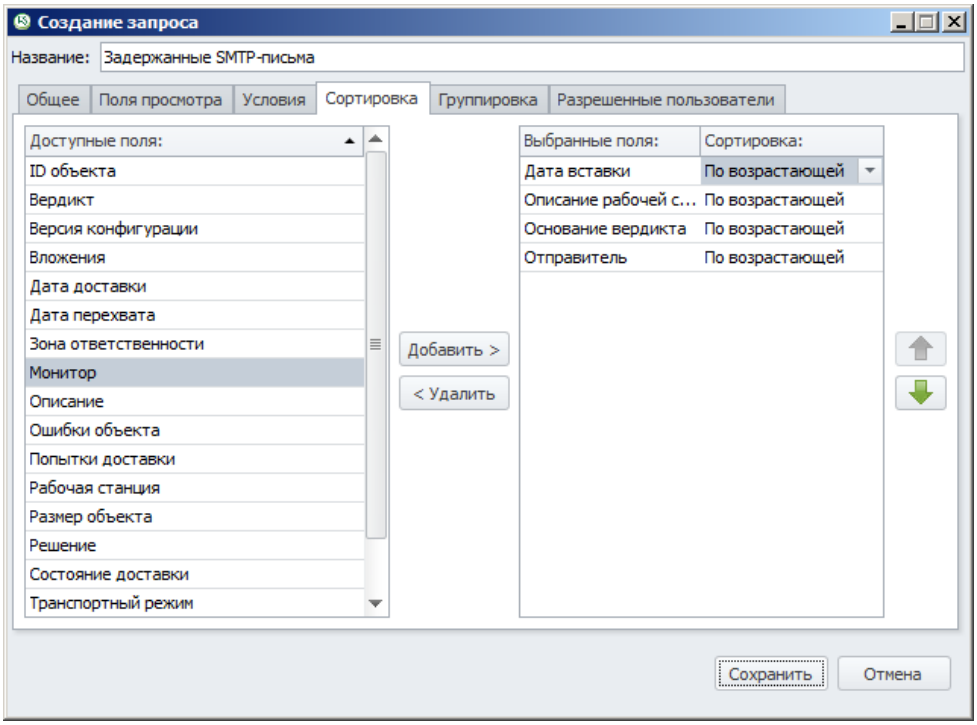
Необходимое действие	**Порядок выполнения**
Изменить условие поиска	1. Выделите строку условия, которое нужно изменить. 2. Выполните одно из следующих действий: • нажмите кнопку **Изменить**; • дважды щелкните левой кнопкой мыши по выделенной строке. 3. В диалоговом окне **Условие** отредактируйте параметры выбранного условия (см. "Параметры условия"). 4. Нажмите кнопку **OK**.
Вырезать в буфер условие поиска	1. Выделите строку условия, которую нужно вырезать. 2. Нажмите кнопку **Вырезать**.
Скопировать в буфер условие поиска	1. Выделите строку условия, которую нужно скопировать. 2. Нажмите кнопку **Копировать**.
Вставить условие поиска	1. Установите курсор на то место, куда вы хотите вставить условие из буфера. 2. Нажмите кнопку **Вставить**. По умолчанию, условие вставляется с использованием логического оператора **И**. При необходимости, вы можете изменить этот оператор как описано ниже.
Изменить логический оператор, объединяющий условия	1. Выделите строку с логическим оператором, который нужно изменить. 2. Выполните одно из следующих действий: • нажмите кнопку **Изменить**; • дважды щелкните левой кнопкой мыши по выделенной строке. 3. В диалоговом окне **Связка** выберите другой логический оператор.
Удалить простое условие запроса	1. Выделите строку, содержащую нужное условие. 2. Нажмите кнопку **Удалить**. **Примечание:** Чтобы удалить составное условие, нужно последовательно удалить все простые условия, входящие в него.
Удалить блок условий	1. Выделите открывающую или закрывающую скобку того блока условий, который нужно удалить. 2. Нажмите кнопку **Удалить**.

8.1.3.4 Настройка условий сортировки (вкладка Сортировка)

На вкладке **Сортировка** задают правила сортировки записей. Если настроена сортировка по нескольким атрибутам, то первым в сортировке будет участвовать атрибут, занимающий самую верхнюю строку в списке. Затем сортировка выполняется по второму атрибуту и т. д.

Примечание

Если в условии запроса не заданы параметры сортировки, то при выполнении запроса объекты будут отсортированы в порядке убывания атрибута *ID объекта*.



Вкладка "Сортировка"

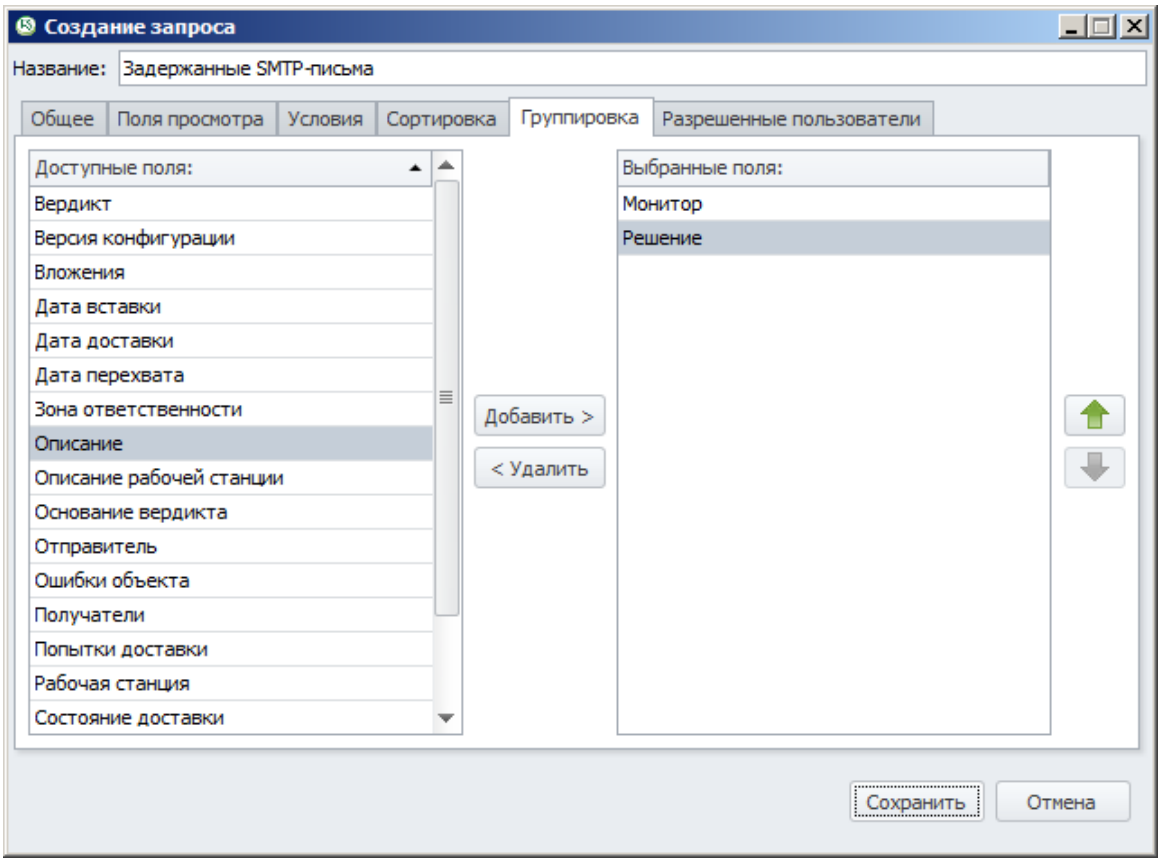
Настройка условий сортировки осуществляется при помощи кнопок, расположенных в верхней части вкладки. Назначение кнопок:

Кнопка	Название кнопки	Назначение кнопки
Добавить >	**Добавить**	Перенести поле, выделенное в списке доступных, в список выбранных.
< Удалить	**Удалить**	Перенести поле, выделенное в списке выбранных, в список доступных.
	Вверх	Переместить выделенное поле на одну строку вверх
	Вниз	Переместить выделенное поле на одну строку вниз

Для выбранных полей вы можете определить направление сортировки: **По возрастающей** или **По убывающей**, выбрав необходимое значение из раскрывающегося списка в столбце **Сортировка**. По умолчанию используется сортировка по возрастающей.

8.1.3.5 Настройка порядка группирования (вкладка Группировка)

На вкладке **Группировка** задают порядок группирования записей. Если настроена группировка по нескольким атрибутам, то сначала группировка выполняется по атрибуту, занимающему самую верхнюю строку в списке. Затем группировка выполняется по второму атрибуту и т. д.



Вкладка "Группировка"

Настройка условий группировки осуществляется при помощи кнопок, расположенных в верхней части вкладки. Назначение кнопок:

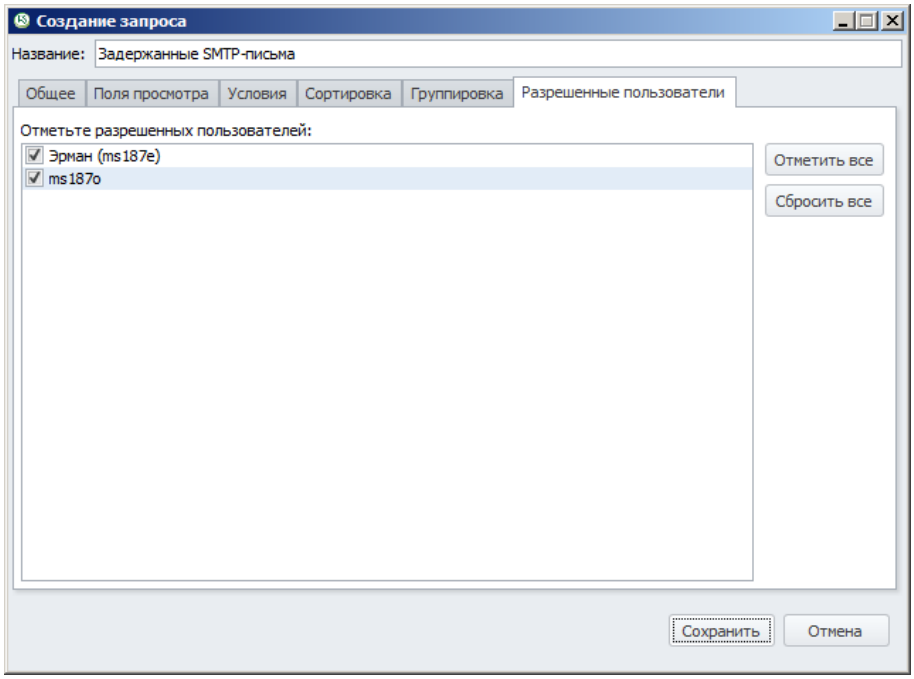
Кнопка	Название кнопки	Назначение кнопки
Добавить >	**Добавить**	Перенести поле, выделенное в списке доступных, в список выбранных.
< Удалить	**Удалить**	Перенести поле, выделенное в списке выбранных, в список доступных.
	**Вверх**	Переместить выделенное поле группировки на одну строку вверх
	**Вниз**	Переместить выделенное поле группировки на одну строку вниз

8.1.3.6 Распределение прав на работу с запросом (вкладка Разрешенные пользователи)

На вкладке **Разрешенные пользователи** указывают пользователей, которые будут иметь права на работу с запросом (изменение, удаление, выполнение, объединение запросов в группу).

Важная информация!

Работа с запросами возможна при условии, что роль, назначенная пользователю, обладает соответствующими привилегиями.



Вкладка "Разрешенные пользователи"

Чтобы назначить пользователю права на работу с запросом,

установите флажок слева от имени учетной записи пользователя.

Чтобы дать всем пользователям права на просмотр данного запроса, воспользуйтесь кнопкой **Отметить все** . Если ни один из пользователей не должен иметь прав на просмотр данного запроса, воспользуйтесь кнопкой **Сбросить все**.

8.1.4 Копирование запроса

Вы можете создать запрос на основе уже существующего, путём его копирования.

Чтобы скопировать запрос:

1. Перейдите к разделу **Запросы**.
2. Выделите нужный запрос.

3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Копировать**;
   - нажмите кнопку **Копировать** на панели инструментов.

Запрос-копия будет иметь те же параметры, что и исходный, с добавлением к названию номера копии. Например, копия отчета «*Все события за период*» будет иметь название «*Все события за период (1)*».

8.1.5 Удаление запроса

Чтобы удалить запрос:

1. Перейдите к разделу **Запросы**.
2. Выделите нужный запрос.
3. Нажмите кнопку **Удалить** на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление запроса.

8.2 Работа пользователя с объектами

Основные возможности пользователя по работе с объектами описаны в следующих разделах:

- Пользовательский анализ объектов
- Перемещение объекта в другую зону ответственности
- Отправка рапорта по объекту
- Назначение тегов объекту
- Выделение объектов цветом
- Добавление примечания к объекту
- Выгрузка вложений, писем и xml-контекста

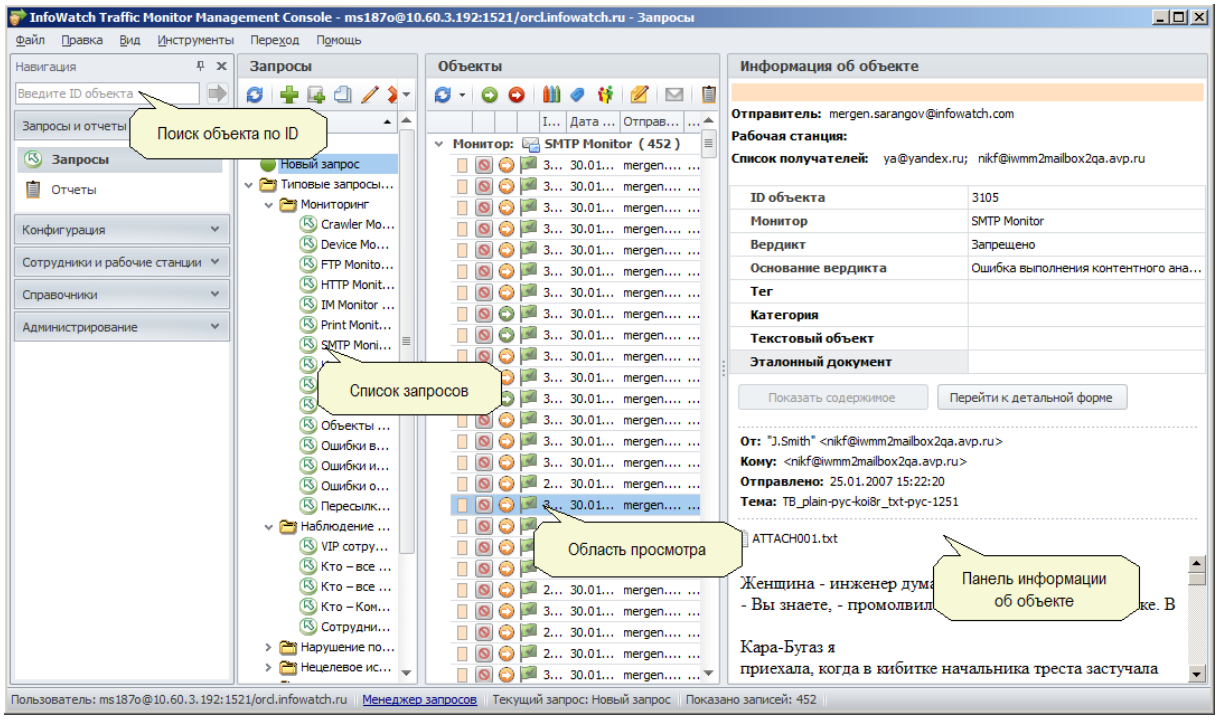
8.2.1 Пользовательский анализ объектов

Информация по объектам выводится в разделе **Запросы** (область **Запросы и отчеты** на панели **Навигация**). В каждом разделе рабочая область главного окна состоит из трех панелей:

Название панели	Назначение панели
Запросы	Списки запросов, доступных для использования. Если панель **Запросы** не отображается в главном окне, в главном меню выберите пункт **Вид > Список запросов**.
Объекты	Отображение общей информации по объектам. На данной панели отображается информация только по тем атрибутам (поля

Название панели	Назначение панели
	просмотра), которые заданы в условиях запроса
Информация об объекте	Основная информация по объекту, в том числе список вложений и текст объекта. Если панель информации об объекте не отображается в главном окне, в главном меню выберите пункт **Вид > Информация об объекте**. О настройке полей, отображаемых на панели информации об объекте, см. " Настройка панели информации об объекте".

Вы также можете открыть форму детального просмотра (см. "Детальная форма просмотра объекта") для объекта с известным ID, без необходимости выполнять запрос. Для этого в поле ввода, вверху панели навигации укажите номер объекта и нажмите кнопку .



Просмотр общей информации по объектам

Более подробную информацию о том, как пользователь может выполнять анализ объектов, вы можете найти в следующих разделах:

- Настройка режима просмотра содержимого объекта
- Настройка размера загружаемых SMTP-писем и заданий на печать
- Настройка панели информации об объекте
- Выполнение запроса по объектам
- Автоматическое обновление
- Работа с Менеджером запросов
- Просмотр информации по объектам
- Обработка данных отправителя, получателя и рабочей станции
- Вынесение решения по объекту
- Постановка на контроль

8.2.1.1 Настройка режима просмотра содержимого объекта

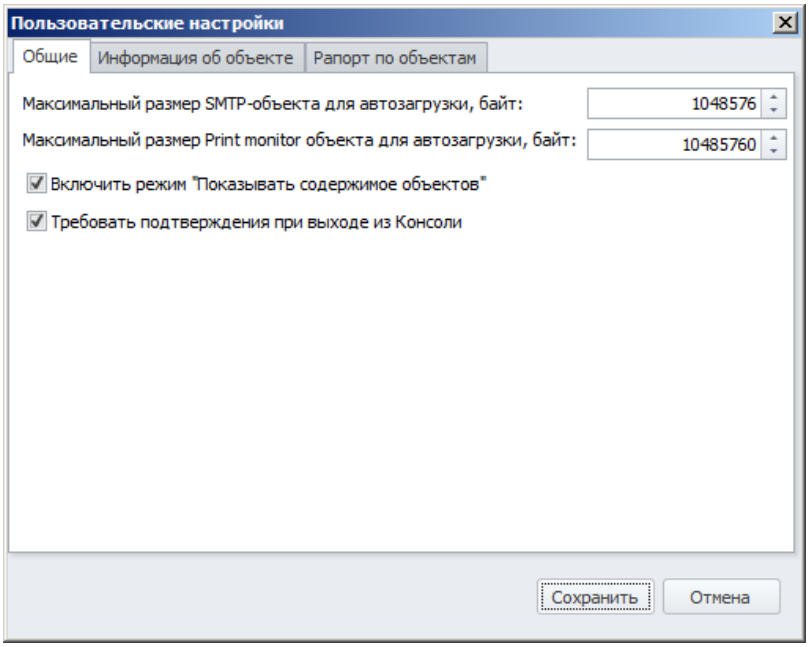
Каждый объект, перехватываемый Системой, состоит из содержимого и служебных данных. Под служебными данными в Системе понимаются данные, не содержащие информации личного характера. Содержимое объекта (текст, вложения, некоторые свойства, такие как список получателей, тема и пр.) может включать в себя данные личного характера. Списки служебных атрибутов и атрибутов содержимого приведены в разделах "Общие атрибуты объекта" и "Заголовки конвертов и заголовки объектов".

По умолчанию показ содержимого отключен даже для пользователей, имеющих права на просмотр содержимого объекта. Для отображения содержимого требуется выполнение специальной команды (**Правка> Объект > Показать содержимое**). Если необходимо просматривать содержимое всех объектов, то вы можете включить режим показа содержимого. В этом случае содержимое будет отображаться сразу после выбора нужного объекта.

Чтобы настроить режим показа содержимого:

1. В главном меню выберите команду **Инструменты > Пользовательские настройки**.

   На экран будет выведено диалоговое окно **Пользовательские настройки**.



Настройка режима показа содержимого

2. На вкладке **Общие** выполните одно из следующих действий:
   - Если нужно отключить показ содержимого по умолчанию, снимите флажок в поле **Включить режим "Показывать содержимое объектов"**.
   - Если нужно выводить содержимое объектов без предварительного уведомления, установите флажок в поле **Включить режим "Показывать содержимое объектов"**.
3. Нажмите кнопку **Сохранить**.

8.2.1.2 Настройка размера загружаемых SMTP-писем и заданий на печать

Одним из важных факторов, влияющих на длительность выполнения запросов, является размер загружаемых писем и заданий на печать. Поэтому в Консоли управления предусмотрена возможность настройки ограничения на автозагрузку в зависимости от размера файлов. Если размер объекта с письмом или заданием на печать превышает указанное ограничение, то в Консоль управления будет загружена только информация о результатах его проверки.

Примечание

SMTP-письма и задания на печать, превышающие размер автозагрузки, можно загружать вручную (см. "Просмотр общей информации по объекту").

Чтобы настроить ограничение на автозагрузку:

1. В главном меню выберите команду **Инструменты > Пользовательские настройки**.

   На экран будет выведено диалоговое окно **Пользовательские настройки**.

2. На вкладке **Общие :**

   - в поле **Максимальный размер SMTP-объекта для автозагрузки** укажите нужный размер письма в байтах (по умолчанию значение составляет 1 048 576 байт).
   - в поле **Максимальный размер Print monitor объекта для автозагрузки** укажите нужный размер pdf-файла с заданием на печать, в байтах (по умолчанию значение составляет 10 485 760 байт).

3. Нажмите кнопку **Сохранить**.

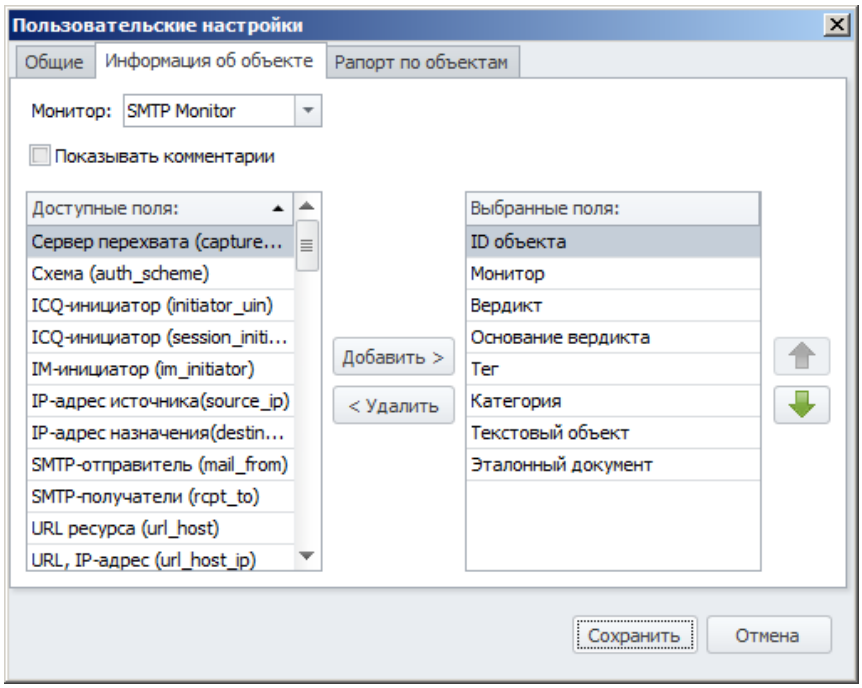
8.2.1.3 Настройка панели информации об объекте

Вы можете настроить поля, отображаемые на панели информации об объекте, для объектов, перехваченных различными мониторами. Этот же состав полей по умолчанию будет отображаться на вкладке **Общая информация** детальной формы просмотра объекта.

Чтобы настроить поля для отображения в форме быстрого просмотра объектов:

1. В главном меню выберите команду **Инструменты > Пользовательские настройки**.

2. В открывшемся диалоговом окне **Пользовательские настройки** выберите вкладку **Информация об объекте**.



Настройка режима показа содержимого

3. Установите флажок **Показывать комментарии**, если хотите, чтобы на панели информации об объекте отображалось последнее добавленное объекту примечание.

4. Выберите нужный тип монитора и настройте для него список полей аналогично тому, как это делается при создании или редактировании запросов на вкладке **Поля просмотра** (см. "Создание и редактирование запроса").

5. Нажмите кнопку **Сохранить**.

8.2.1.4 Выполнение запроса по объектам

Объекты загружаются в Консоли управления в результате выполнения запроса к базе данных. Работа с запросами имеет следующие особенности:

- Длительность выполнения запроса зависит как от количества загружаемых объектов, так и от размера этих объектов. По умолчанию в Консоли управления установлено ограничение на автозагрузку писем размером свыше 1 Мб. Если размер писем превышает заданный предел, то в области чтения выводится соответствующее уведомление. В этом случае загрузить объект можно, щелкнув левой кнопкой мыши по данному уведомлению.

> **Примечание**
>
> Настройка размера автоматически загружаемых объектов описана в разделе "Настройка размера загружаемых SMTP-писем и заданий на печать".

- Содержимое объекта отображается только для тех пользователей, у которых есть права на просмотр содержимого объекта. Список служебных атрибутов и атрибутов содержимого приведен в разделах "Общие атрибуты объекта" и "Заголовки конвертов и заголовки объектов".
- Если в запросе содержится условие на поиск файлов определенного типа, то в этом случае будут выведены все объекты, содержащие файлы указанного типа во вложениях, в том числе и во вложенных архивах.
- Если в условии запроса не заданы параметры сортировки, то сортировка объектов выполняется по

атрибуту ID объекта (в порядке по убыванию).

- Если в результате работы с объектом (например, перемещения объекта в другую зону ответственности – см. "Перемещение объекта в другую зону ответственности", назначения тега – см. "Назначение тегов объекту", изменения цвета – см. "Выделение объектов цветом", и т.п.), объект перестаёт соответствовать условиям запроса, то он не будет сразу же исключен из отображаемого результата запроса, а останется до тех пор, пока запрос не будет повторно выполнен.

Чтобы выполнить запрос:

1. Перейдите к разделу **Запросы**.
2. Выполните одно из следующих действий:
   - выделите нужный запрос левой кнопкой мыши и нажмите кнопку **Выполнить** на панели инструментов;
   - дважды щелкните левой кнопкой мыши по названию выделенного запроса.
   - щелкните правой кнопкой мыши по названию выделенного запроса и в раскрывшемся меню выберите **Выполнить**.

   О возможностях управления выполняемыми запросами см. "Работа с Менеджером запросов".

В результате успешного выполнения запроса в области просмотра будет выведен список записей, удовлетворяющих его условиям. О просмотре информации о каждом объекте см. в разделе "Просмотр информации по объектам".

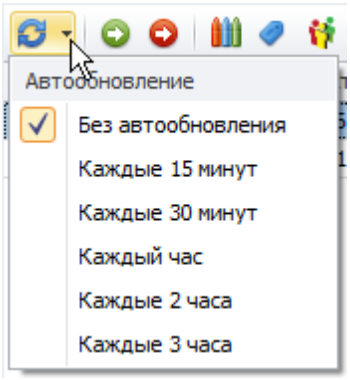
Вы можете включить функцию **Автообновление**, чтобы запрос выполнялся автоматически через указанные промежутки времени (см. "Автоматическое обновление").

8.2.1.5 Автоматическое обновление

Возможность автообновления позволяет получать обновлённые результаты запроса автоматически, с указанной вами периодичностью. Вы можете включить автоматическое обновление любого запроса, к которому имеете доступ (о создании запросов и их редакитровании см. "Создание и редактирование запроса "). О том, как задать параметры автообновления при создании или редактировании запроса, см. "Общие параметры запроса".

Чтобы включить/отключить автообновление или изменить его период:

1. Перейдите к разделу **Запросы**.
2. Выделите нужный запрос левой кнопкой мыши.
3. На панели инструментов в области **Объекты** нажмите стрелку рядом с кнопкой **Обновить**. Откроется список периодов автообновления.



4. В открывшемся списке выберите необходимый временной интервал для автоматического обновления результатов запроса. Чтобы прекратить автоматическое обновление, выберите "*Без автообновления*".

Важная информация!

При отмене запроса с включенным автообновлением (см. "Работа с менеджером запросов"), его автоматическое выполнение прекратится. Чтобы возобновить автообновление, повторно выполните этот запрос.

8.2.1.6 Работа с Менеджером запросов

Менеджер запросов:

- отображает список выполняемых запросов (название, статус, время запуска и выполнения)
- позволяет отменить или повторно запустить выполнение запроса, находящегося в списке
- позволяет переходить к результатам выполнения выбранного запроса (см. "Просмотр информации по объектам")

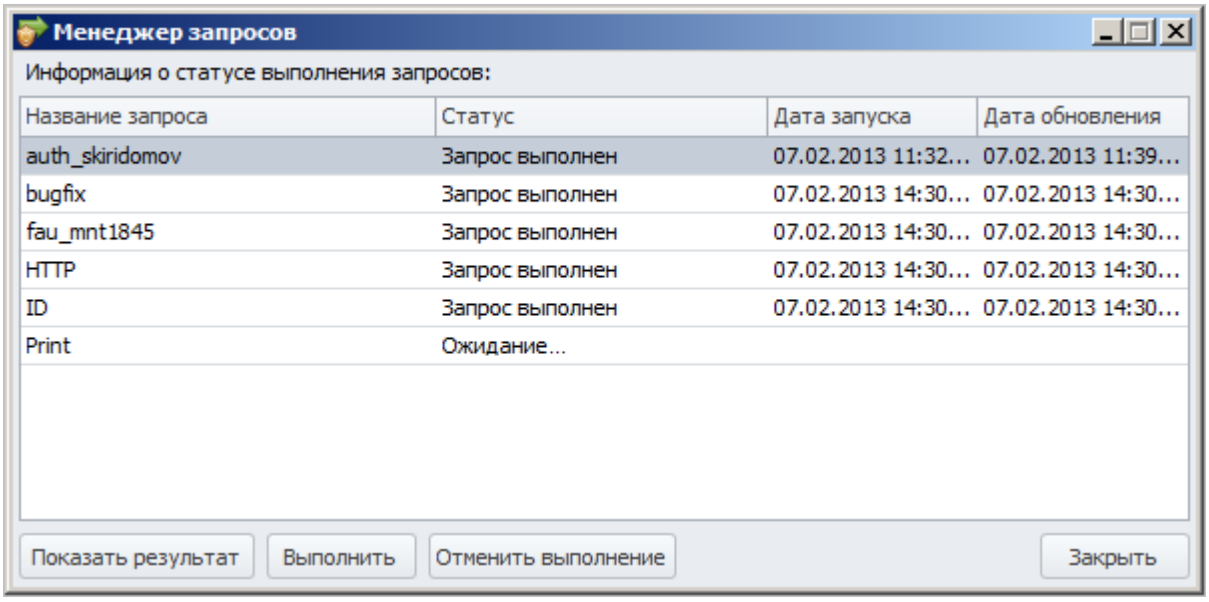
Менеджер запросов может быть вызван из любого раздела Консоли управления.

Чтобы запустить Менеджер запросов,

выполните одно из следующих действий:

- в главном меню выберите команду **Инструменты > Менеджер запросов**.
- на строке состояния (нижняя часть окна Консоли управления) нажмите ссылку **Менеджер запросов**.

На экран будет выведено диалоговое окно **Менеджер запросов**.



Вид окна Менеджера запросов

Чтобы перейти к результатам запроса:

1. Выберите выполненный запрос (статус "*Запрос выполнен*"), результаты выполнения которого вы хотите просмотреть.
2. Нажмите **Показать результат**.

В результате вы перейдёте в раздел **Запросы**, где в списке выбран требуемый выполненный запрос.

Менеджер запросов содержит список всех запросов, которые пользователь отправил на выполнение в течение своей сессии работы в Консоли управления. Однако, Система может хранить результаты выполнения максимум для **пяти** запросов. Все последующие отправленные на выполнение запросы получают статус "*Ожидание*" и формируют очередь на выполнение.

Чтобы выполнить запрос, находящийся в статусе "*Ожидание*":

1. Выберите выполненный запрос (статус "*Запрос выполнен*"), результаты прошлого выполнения которого вы более не намерены просматривать.
2. Нажмите **Отменить выполнение**.

Выполненный запрос будет удалён из списка, а тот запрос со статусом "*Ожидание*", который был отправлен на выполнение раньше других, начнёт выполняться.

Важная информация!

При отмене запроса с включенным автообновлением (о настройке см. "Общие параметры запроса"), его автоматическое выполнение прекратится. Чтобы возобновить автообновление, повторно выполните этот запрос (см. "Выполнение запроса по объектам", "Автоматическое обновление").

8.2.1.7 Просмотр информации по объектам

В результате выполнения запроса (см. "Выполнение запроса по объектам") в Консоли управления отображается список записей, удовлетворяющих условиям этого запроса. Порядок просмотра информации по объектам описан в следующих разделах:

- Просмотр общей информации по объекту
- Детальная форма просмотра объекта
- Настройка поиска по заголовкам объектов
- Просмотр системного журнала объекта

8.2.1.7.1 Просмотр общей информации по объекту

В результате выполнения запроса, в области просмотра выводится список объектов, найденных по запросу. Набор атрибутов, отображаемых в области просмотра, зависит от параметров выполненнного запроса (см. " Выбор полей просмотра"). Полный перечень возможных атрибутов перечислен в разделах "Общие атрибуты объекта" и "Заголовки конвертов и заголовки объектов". Сведения по некоторым атрибутам отображаются в виде пиктограмм.

Значения пиктограмм для атрибутов объектов

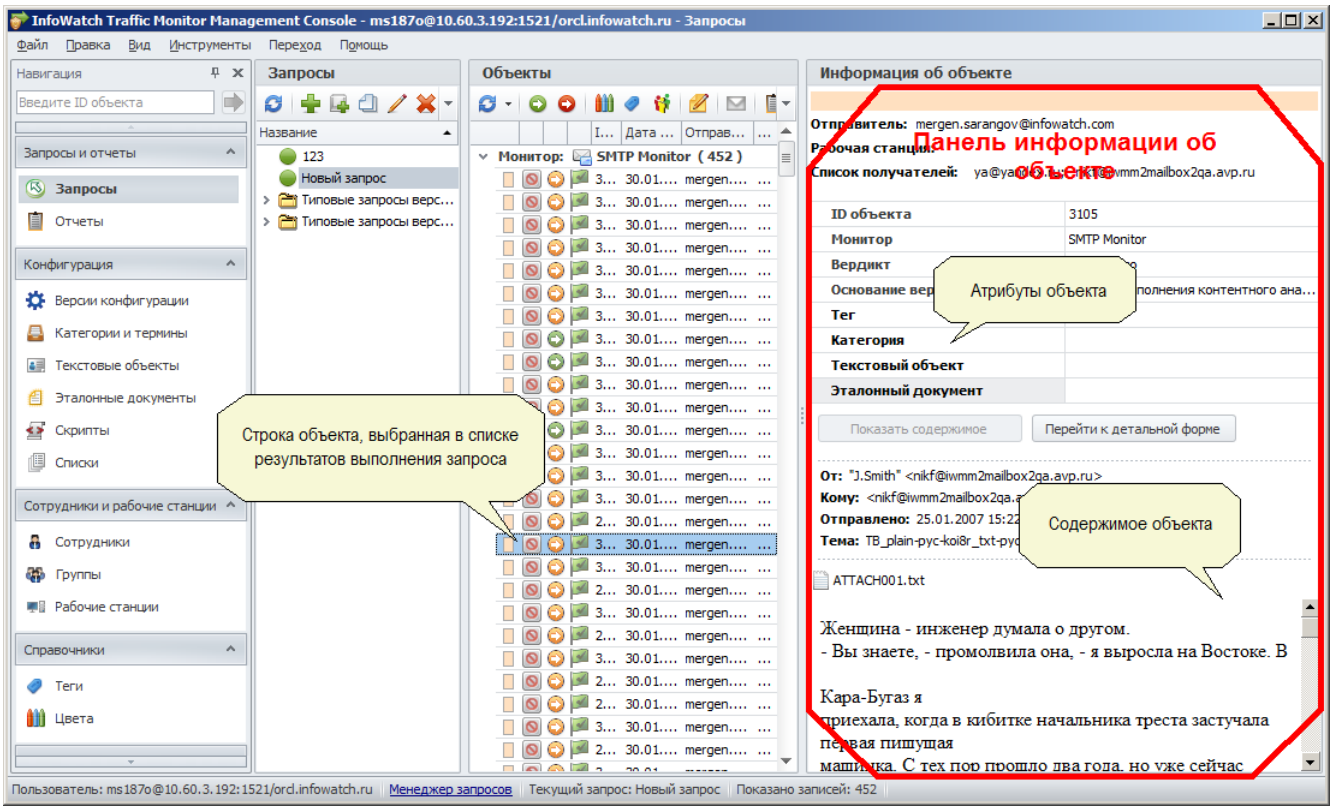
Пиктограмма	Значение атрибута
Атрибут *Монитор*	
	SMTP Monitor
	HTTP Monitor
	ICQ Monitor
	Print Monitor
	Device Monitor
	DeviceLock Monitor
	Skype Monitor
	Crawler Monitor
	FTP Monitor
	Lotus Notes Monitor
	MMP Monitor
	XMPP Monitor
Атрибут *Вердикт*	
	Разрешено
	Запрещено
Атрибут *Решение*	
	Решение не принято
	Нет нарушений
	Нарушение
Атрибут *Состояние доставки*	
	Ожидание
	Доставлено
	Неудачно

Пиктограмма	Значение атрибута
	Попытка не удалась
	Заблокировано
Атрибут *Транспортный режим*	
	Нормальный
	Прозрачный
	Копия
Атрибут *Ошибки объекта*	
	Да
Атрибут *Вложения*	
	Да

Основные сведения по конкретному объекту (в т.ч. текст объекта и список вложений) можно посмотреть на панели информации об объекте.

Чтобы вывести сведения по объекту на панель информации об объекте:

в области просмотра выделите строку, содержащую сведения о нужном объекте.



Вверху панели информации об объекте отображаются атрибуты *Отправитель*, *Рабочая станция* и *Список получателей*.

Ниже отображается перечень значений атрибутов, настроенный как описано в разделе "Настройка панели информации об объекте".

Если включен режим просмотра комментариев (см. "Настройка панели информации об объекте"), то также отображается последнее добавленное объекту примечание.

Если режим «*Показывать содержимое объектов*» отключен (см. "Настройка режима просмотра содержимого объекта"), и у вас есть привилегия на просмотр содержимого объекта, то вы можете просмотреть содержимое одним из следующих способов:

- на панели информации об объекте нажмите кнопку **Показать содержимое**;
- в главном меню выберите команду **Правка> Объект > Показать содержимое**.

При включенном режиме *«Показывать содержимое объектов»* содержание объекта может не отображаться:

- если размер SMTP-объекта или задания на печать превышает заданный размер автозагрузки (см. " Настройка размера загружаемых SMTP-писем и заданий на печать").
- если размер извлеченного из объекта текста превышает 32 Мб.

В любом из этих случаев на панели информации об объекте будет отображаться соответствующее уведомление. Чтобы просмотреть текст объекта и получить возможность выгрузить вложение, щелкните левой кнопкой мыши по уведомлению.

Для различных типов объектов содержимое показывается различными способами.

- Для SMTP-писем отображаются, в случае их наличия, вложения и параметры *От*, *Кому*, *Копия*, *Тема* и *Отправлено*.
- Для ICQ-сообщений диалог отображается в виде таблицы со столбцами *От*, *Кому*, *Отправлено, Сообщение*. Количество сообщений, отображаемых в диалоге (по умолчанию – 2), зависит от настроек конфигурационного файла (см. документ «*InfoWatch Traffic Monitor. Руководство администратора*»: описание настройки файла `tm.conf`, секция `[PROXY_ICQ]`, параметр `MessageWindow`).
- Для сообщений Skype, GTalk или Mail.Ru Агент отображаются параметры *От*, *Отправлено* и *Сообщение*. Для сообщений с пересылаемыми файлами отображаются вложения.
- Для объектов Device Monitor, FTP Monitor и DeviceLock отображаются теневые копии файлов.
- Для объектов Print Monitor отображаются pdf-файлы с копиями заданий на печать. Также может отображаться текст, извлеченный из заданий на печать средствами Device Monitor или OCR-экстракторов (если они используются).
- Для POST-запросов на ряд веб-ресурсов (перечень ресурсов см. "Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов") в Системе определены правила соответствия переменных POST-запроса общим атрибутам объекта. Для запросов на эти ресурсы в качестве содержимого отображаются, в случае их наличия, вложения и параметры *От*, *Кому*, *Копия*, *Тема* и *Отправлено*. Для остальных HTTP-запросов в качестве содержимого отображаются только вложения (в случае их наличия).

  Примечание

  Если структура HTTP-запроса подразумевает передачу каких-либо данных в заголовках запроса, то такие данные могут быть не найдены при поиске по тексту – даже если эти данные отображаются на панели информации об объекте.

При работе с текстом объекта вы можете использовать контекстное меню, которое содержит стандартный набор команд Internet Explorer.

Примечание

Если текст письма отображается в неверной кодировке, то щелкните правой кнопкой мыши по тексту объекта. В раскрывшемся меню выберите пункт **Кодировка** (**Encoding**). Затем укажите нужную кодировку или выберите пункт **Автовыбор**.

Чтобы просмотреть вложение объекта:

1. В области просмотра выделите строку, содержащую сведения о нужном объекте.
2. На панели информации об объекте выделите нужное вложение.
3. Выполните одно из следующих действий:
   - щелкните правой кнопкой мыши по выделенному вложению и в раскрывшемся контекстном меню выберите команду **Открыть**;
   - дважды щелкните левой кнопкой мыши по названию выделенного запроса.

Вложение будет открыто с помощью приложения, ассоциированного на вашем компьютере с данным типом файла.

8.2.1.7.2 Детальная форма просмотра объекта

На детальной форме просмотра объектов отображается подробная информация о служебных данных объекта и о содержимом объекта. Так как содержимое объекта представляет собой информацию личного характера (текст, вложения, некоторые свойства такие, как список получателей, тема и пр.), то по умолчанию режим показа содержимого отключен и для объекта отображаются только служебные данные.

Примечание

Список атрибутов содержимого и служебных данных объекта приведен в разделах "Общие атрибуты объекта" и "Заголовки конвертов и заголовки объектов".

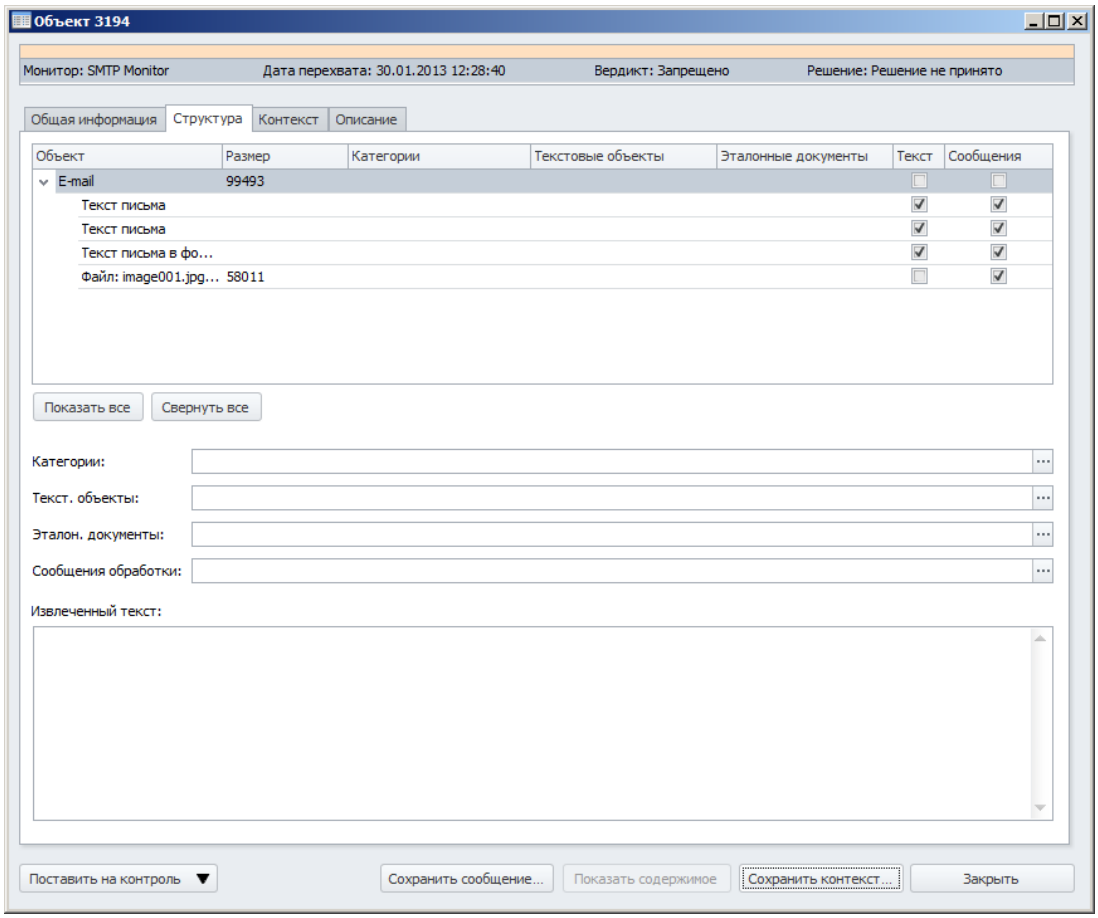
Чтобы по умолчанию содержимое отображалось для всех объектов, включите режим показа содержимого (см. "Настройка режима просмотра содержимого объекта").

Чтобы открыть форму детального просмотра для объекта, показанного в результатах запроса:

1. В области просмотра выделите строку с нужным объектом.
2. Выполните одно из следующих действий:
   - дважды щелкните левой кнопкой мыши по выделенной строке;
   - нажмите кнопку **Форма детального просмотра**;
   - в главном меню выберите команду **Правка > Объект > Детальная форма**;
   - на панели информации об объекте нажмите кнопку **Перейти к детальной форме**.

Если вы знаете номер объекта (ID), вы можете открыть форму детального просмотра этого объекта без необходимости выполнять запрос. Для этого в поле ввода, вверху панели навигации укажите номер объекта и нажмите кнопку . Если объект с таким номером не существует или не входит в доступную вам зону ответственности (см. "Зоны ответственности"), то будет отображено уведомление "*Объект не найден*".

Форма детального просмотра объекта выводится в виде диалогового окна **Объект <ID объекта>**.



Просмотр атрибутов объекта

В верхней части детальной формы просмотра отображается общая информация об объекте: перехватчик, дата и время перехвата, вердикт и решение по объекту. Также присутствует полоса с цветом, присвоенным объекту.

Детальная форма просмотра имеет четыре вкладки:

- **Общая информация**. Информация по общим атрибутам объекта. Отображаются параметры **Отправитель**, **Рабочая станция** и **Список получателей**, а также поля, отображаемые на панели информации об объекте (см. "Настройка панели информации об объекте").

- **Структура**. Информация о содержании объекта и результатах контентного анализа. В основном поле содержимое объекта представлено в древовидной форме, где перечень узлов зависит от типа объекта.

  Для каждого элемента дерева структуры отображаются следующие параметры:

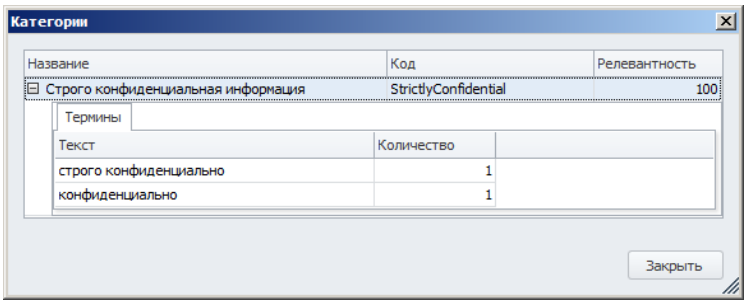
  - **Размер** – размер элемента в байтах. Указывается только для корневых узлов и файлов;
  - **Категории**, **Текстовые объекты**, **Эталонные документы** – результаты контентного анализа;
  - **Текст** – поле отмечено флажком, если из элемента извлечен текст;
  - **Сообщения** – поле отмечено флажком, если есть сообщения, возникшие в результате обработки элемента.

  Под деревом структуры отображаются поля с информацией о результатах контекстного анализа:

Примечание

Если вы просматриваете объект в режиме сокрытия содержимого, то в этих полях будет отображаться информация для всего объекта. Если вы просматриваете объект в режиме показа содержимого, то в этих полях будет отображаться информация только для выбранной строки в древовидном списке.

- **Категории** – перечислены через запятую присвоенные категории. Для просмотра подробной информации нажмите кнопку ⋯. На экран будет выведено диалоговое окно, где перечислены присвоенные категории с указанием их кодов и релевантности (степени соответствия текста объекта данной категории).



Просмотр присвоенных категорий

Чтобы просмотреть найденные в объекте термины, в соответствии с которыми была присвоена категория, нажмите на кнопку ⊞ слева от названия категории.

Примечание

Просмотр терминов доступен только в режиме показа содержимого.

- **Текст. объекты** – перечислены через запятую обнаруженные текстовые объекты. Для просмотра подробной информации нажмите кнопку ⋯. На экран будет выведено диалоговое окно, где перечислены обнаруженные текстовые объекты с указанием их описания и количества.
- **Эталон. документы** – перечислены через запятую обнаруженные эталонные документы. Для просмотра подробной информации нажмите кнопку ⋯. На экран будет выведено диалоговое окно, где перечислены обнаруженные эталонные документы с указанием их идентификатора, названия, имени файла и релевантности (степени соответствия текста объекта данному эталонному документу).
- **Сообщения обработки** – отображается первое информационное сообщение для данного объекта. Для просмотра подробной информации нажмите кнопку ⋯. На экран будет выведено диалоговое окно, где перечислены все сообщения, созданные при обработке объекта. Для каждого сообщения указывается его уровень, сгенерировавший его модуль и собственно текст.
- **Извлеченный текст** – отображается текст, извлеченный из объекта. Вы можете выполнить поиск по извлечённому тексту: для этого

- **Контекст**. Подробная информация о данных, полученных в процессе анализа и обработки объекта. Представлена в виде дерева xml-контекста.

Примечание

Представление контекста основано на модели типов InfoWatch Traffic Monitor (см. "Типы данных ").

При работе с контекстом вы можете использовать фильтрацию элементов как по атрибутам, так и по их значениям.

- **Примечания**. Дополнительная информация по объекту. Содержит историю всех примечаний, добавленных к объекту. Чтобы добавить новое примечание, введите нужный текст в поле **Добавить**

примечание и нажмите кнопку **Добавить**.

На форме детального просмотра вы можете выполнять ряд общих действий:

Необходимое действие	**Порядок выполнения**
Развернуть/свернуть данные	Нажать кнопку **Показать все** / **Свернуть все**
Выгрузить SMTP-письмо в формате EML	Нажать кнопку **Сохранить сообщение**
Отображение содержимого объекта (при наличии прав на просмотр содержимого объекта)	Нажать кнопку **Показать содержимое**
Выгрузить xml-контекст объекта в файл	Нажать кнопку **Сохранить контекст**
Поиск фрагмента в извлеченном тексте	На вкладке **Структура**, щелкнуть левой кнопкой мыши в поле **Извлеченный текст** и нажать **Ctrl+F**
Постановка объекта на контроль	Нажать кнопку **Поставить на контроль** (см. "Постановка объекта на контроль")

Представление информации на вкладках **Общие**, **Структура** и **Контекст** зависит от того, разрешен ли для данного объекта показ содержимого (см. таблицу ниже). Об ограничениях на показ содержимого объекта см. "Управление доступом к содержимому объектов".

Показ содержимого объекта	**Вкладка Общие**	**Вкладка Контекст**
Показ содержимого разрешен	Отображаются все поля просмотра	Представление контекста полностью соответствует модели типов InfoWatch Traffic Monitor
Показ содержимого отключен	Отображаются только поля со служебными данными	Дерево контекста отображается с изменениями: • ветвь *envelope* содержит только служебные данные; • ветвь *object* не отображается: служебные данные из этой ветви отображаются в составе ветви *processing*

8.2.1.7.3 Настройка поиска по заголовкам объектов

При создании запросов ("Настройка условий запроса") и отчетов ("Создание и редактирование отчета") используется построитель запросов, позволяющий осуществлять поиск по заголовкам конвертов и объектов. По умолчанию в построителе запросов используются следующие заголовки объекта:

- `From`
- `To`
- `Cc`
- `Date`
- `Subject`
- `Importance`
- `Priority`
- `X-Forwarded-For`

На детальной форме просмотра вы можете включить извлеченные Системой из объекта заголовки в список доступных для использования в построителе запросов.

Чтобы изменить список заголовков объектов, используемых в построителе запросов:

1. Откройте форму детального просмотра для нужного объекта (см."Детальная форма просмотра объекта ").
2. На вкладке **Контекст** разверните узел `root > object > headers`.

   Все заголовки, включенные в список доступных для использования в построителе запросов, отмечаются пиктограммой .
3. Щелкните правой кнопкой мыши по необходимому заголовку и в раскрывшемся контекстном меню выберите нужную команду:
   - Чтобы сделать заголовок доступным в построителе запросов, выберите команду **Разрешить поиск по заголовку в построителе запросов**.
   - Чтобы убрать заголовок из списка доступных в построителе запросов, выберите команду **Запретить поиск по заголовку в построителе запросов**.

8.2.1.7.4 Просмотр журнала объекта

В журнале объекта, отображается информация, связанная с анализом объекта на Traffic Monitor Server (в частности, выводятся сообщения об ошибках).

Чтобы открыть журнал объекта:

1. В области просмотра выделите строку с нужным объектом.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Объект > Системный лог объекта**;
   - нажмите кнопку  **Системный лог объекта** на панели инструментов.

На экран будет выведено окно **Системный лог объекта**. В этом окне выводятся сообщения сгенерированные в процессе обработки объекта. По каждому сообщению отображается следующая информация:

- **Дата и время**. Дата и время генерации системного сообщения.
- **Уровень**. Уровень важности сообщения. Могут быть информационные (*info*), предупреждающие (*warning*) сообщения и сообщения об ошибках (*error*).
- **Модуль**. Модуль, сгенерировавший сообщение.
- **Содержание**. Текст сообщения.

8.2.1.8 Обработка данных отправителя, получателя и рабочей станции

При анализе объекта Система извлекает из объекта информацию об отправителе, отправившей рабочей станции и списке получателей этого объекта. Затем Система выполняет поиск соответствия значения атрибута (*Отправитель*, *Список получателей* и *Рабочая станция*) и данных записей из справочников Active Directory: справочника сотрудников (см. "Справочник сотрудников") или справочника рабочих станций (см. "Справочник рабочих станций").

В результате поиска соответствия значения атрибутов с данными записей из справочников сотрудников и рабочих станций возможны следующие ситуации:

- не было найдено ни одного соответствия с данными существующих в Системе записей из справочников;
- найдено одно соответствие между информацией об отправителе/получателе/рабочей станции объекта и какой-либо записью из справочников;
- было найдено несколько соответствий в справочниках.

Если одному значению атрибута было найдено несколько соответствий, то это считается **ошибкой идентификации** (конфликтом). Для события с конфликтом идентификации:

- По умолчанию, в области просмотра результатов запроса такое событие выделяется оранжевым цветом.
- По умолчанию, событию выносится вердикт "*Запрещено*" с основаним вердикта "*Конфликт идентификации*".
- При просмотре события на панели информации об объекте значение атрибута с несколькими соответствиями выделяется красным шрифтом.
- При нажатии на атрибут с конфликтом раскрывается контекстный список записей, соответствующих этому значению. Выберите необходимую запись из списка, чтобы открылось окно редактирования записи из справочника сотрудников или рабочих станций.

Важная информация!

Объекты с ошибками идентификации рекомендуется обрабатывать в первую очередь.

Чтобы просмотреть перечень объектов, для которых произошли ошибки идентификации, создайте запрос с условием по атрибуту *Ошибки идентификации* (подробнее см. "Настройка условий запроса").

Важная информация!

Возможна ситуация, когда для объектов, перехваченных с одного IP-адреса, постоянно определяется ошибка идентификации рабочей станции. Это может быть обусловлено тем, что на сервере DNS одному IP-адресу соответствует несколько имен компьютеров. Чтобы избежать подобных ситуаций, администратору локальной сети рекомендуется внести изменения в конфигурацию DNS таким образом,

чтобы один IP-адрес соответствовал только одной рабочей станции.

Если Система сопоставила информацию о получателе/отправителях/рабочей станции объекта с какой-либо записью справочника, то в качестве значения атрибута значение на панели информации об объекте будет отображаться имя и фамилия сотрудника либо название рабочей станции. В этом случае вы можете перейти к просмотру и редактированию соответствующей записи справочника, либо добавить сотрудника или рабочую станцию в группу Traffic Monitor.

Примечание

Перед добавлением сотрудника или рабочей станции в группу убедитесь, что необходимая группа TM уже создана (см. "Создание, просмотр и редактирование группы") и загружена на хост (см. "Загрузка справочников на хост").

Чтобы открыть запись справочника,

выполните одно из следующих действий:

- дважды щелкните левой кнопкой мыши по значению атрибута;
- нажмите на значении атрибута правой кнопкой мыши и из контекстного меню выберите **Открыть**.

Примечание

О порядке редактирования записи о сотруднике см. "Создание и редактирование записи о сотруднике". О порядке редактирования записи о рабочей станции см. "Создание, просмотр и редактирование группы".

Чтобы добавить сотрудника или рабочую станцию в группу TM:

1. Нажмите на значении атрибута правой кнопкой мыши.
2. Из контекстного меню выберите **Добавить в группу**.
3. В открывшемся диалоговом окне **Выбор группы** установите флажок для той группы TM, в которую нужно добавить данного сотрудника или рабочую станцию.
4. Нажмите **Сохранить**.

Если информации об отправителе или получателе не было найдено соответствия среди данных существующих записей из справочников, то значение атрибута *Отправитель* или *Список получателей* на панели информации об объекте будет отображаться в виде адреса e-mail, номера ICQ, Skype ID или номера телефона. В этом случае у вас есть возможность добавить это значение в качестве контакта одному из существующих сотрудников, либо создать новую запись о сотруднике с таким контактом прямо из панели информации об объекте.

Чтобы добавить значение атрибута в качестве контакта одному из существующих сотрудников

1. Нажмите на значении атрибута правой кнопкой мыши.
2. Из контекстного меню выберите **Добавить контакт сотруднику**.
3. В открывшемся диалоговом окне **Отметьте необходимых сотрудников** выделите строку, содержащую запись о сотруднике и нажмите **ОК**.

   В результате будет отображено окно **Редактирование сотрудника** с открытым диалоговым окном **Создание контакта**.

Примечание

Если вы выберете несколько контактов (например, удерживая клавиши **Ctrl** или **Shift**), контакт добавится только одному из них - тому, который находится в списке сотрудников выше остальных выбранных.

4. Укажите информацию о контакте:
   - Из раскрывающегося списка **Тип контакта** выберите необходимый тип (**E-mail**, **ICQ**, **Skype**, **Phone** или **IP**), который соответствует данным, отображенным в поле **Значение контакта**.
   - В поле **Описание** укажите дополнительную информацию о добавленном контакте.
5. Нажмите **ОК**.

Примечание

Если контакт уже был добавлен какому- либо пользователю, после нажатия кнопки **ОК** на экране появится диалоговое окно с предупреждением. Вы можете либо согласиться и добавить контакт выбраному сотруднику (кнопка **Да**), либо отказаться и отменить добавление контакта сотруднику (кнопка **Нет**).

6. При необходимости, дополнительно отредактируйте запись о сотрудника (подробно о порядке редактирования записи о сотруднике см. "Создание и редактирование записи о сотруднике"). Затем нажмите **Сохранить**.

Чтобы создать новую запись о сотруднике с контактом из объекта:

1. Нажмите на значении атрибута правой кнопкой мыши.
2. Из контекстного меню выберите **Создать сотрудника с этим контактом**.

   В результате будет отображено окно **Создание пользователя** с открытым диалоговым окном **Создание контакта**.
3. Укажите информацию о контакте:
   - Из раскрывающегося списка **Тип контакта** выберите необходимый тип (**E-mail**, **ICQ**, **Skype**, **Phone** или **IP**), который соответствует данным, отображенным в поле **Значение контакта**.
   - В поле **Описание** укажите дополнительную информацию о добавленном контакте.
4. Нажмите **ОК**.

Примечание

Если контакт уже был добавлен какому- либо пользователю, после нажатия кнопки **ОК** на экране появится диалоговое окно с предупреждением. Вы можете либо согласиться и добавить контакт создаваемому сотруднику (кнопка **Да**), либо отказаться и отменить создание сотрудника (кнопка **Нет**).

5. Укажите остальную информацию о сотруднике, как описано в разделе "Создание и редактирование записи о сотруднике". Затем нажмите **Сохранить**.

8.2.1.9 Вынесение решения по объекту

Каждому объекту, прошедшему анализ в Системе, присваиваются определенные значения атрибутов: *Транспортный режим*, *Вердикт* и *Состояние доставки*. При анализе объекта в Консоли управления вы можете вынести собственное решение (*Решение пользователя*). Решение пользователя не влияет на вердикт, вынесенный объекту.

Во всех транспортных режимах, кроме нормального, принятие решения пользователя не влияет на доставку объекта. Поэтому атрибут *Состояние доставки* сохраняет свое первоначальное значение. Однако если Система настроена на фильтрацию трафика (для объекта установлен нормальный транспортный режим), то в некоторых случаях пользовательское решение может изменить состояние доставки объекта.

Пример 1

SMTP-письмо разрешено к доставке, но еще не было отправлено получателю. После анализа в Консоли управления письмо было признано нарушающим корпоративную политику безопасности. Тогда можно заблокировать доставку письма. Для этого смените решение пользователя по письму на *Нарушение*.

Пример 2

SMTP-письмо было признано нарушающим корпоративную политику безопасности. Однако дополнительный анализ в Консоли управления показал, что письмо не содержит нарушений и может быть доставлено получателям. В этом случае смените решение пользователя по письму на *Нет нарушений*.

Возможные варианты решений пользователя, которые приводят к смене состояния доставки, перечислены в следующей таблице. В остальных случаях решение пользователя на состояние доставки не влияет.

Исходное состояние доставки	Решение пользователя	Новое состояние доставки	Операция доступна для объектов
Неудачно	Нарушение	Заблокировано	SMTP
Ожидание	Нарушение	Заблокировано	SMTP, HTTP
Попытка доставки не удалась	Нарушение	Заблокировано	SMTP
Заблокировано	Нет нарушений	Ожидание	SMTP

Информация о решении пользователя отображается при просмотре объектов (см. "Просмотр информации по объектам") в поле **Решение**. Первоначально для каждого объекта установлено значение *Решение не принято*. Этому значению соответствует пиктограмма .

Чтобы вынести решение по объекту:

1. Перейдите к разделу **Запросы**.
2. Выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).
3. В области просмотра выделите одну или несколько строк с нужными объектами.
4. Выполните необходимое действие:

Необходимое действие	Порядок выполнения
Присвоить объекту решение *Нет нарушений*	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Объект > Нет нарушений** • нажмите кнопку  **Нет нарушений** на панели инструментов • щелкните правой кнопкой мыши по строке с объектом и в

Необходимое действие	Порядок выполнения
	контекстном меню выберите пункт **Нет нарушений**
Присвоить объекту решение *Нарушение*	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Объект > Нарушение** • нажмите кнопку **Нарушение** на панели инструментов • щелкните правой кнопкой мыши по строке с объектом и в контекстном меню выберите пункт **Нарушение**

8.2.1.10 Постановка на контроль

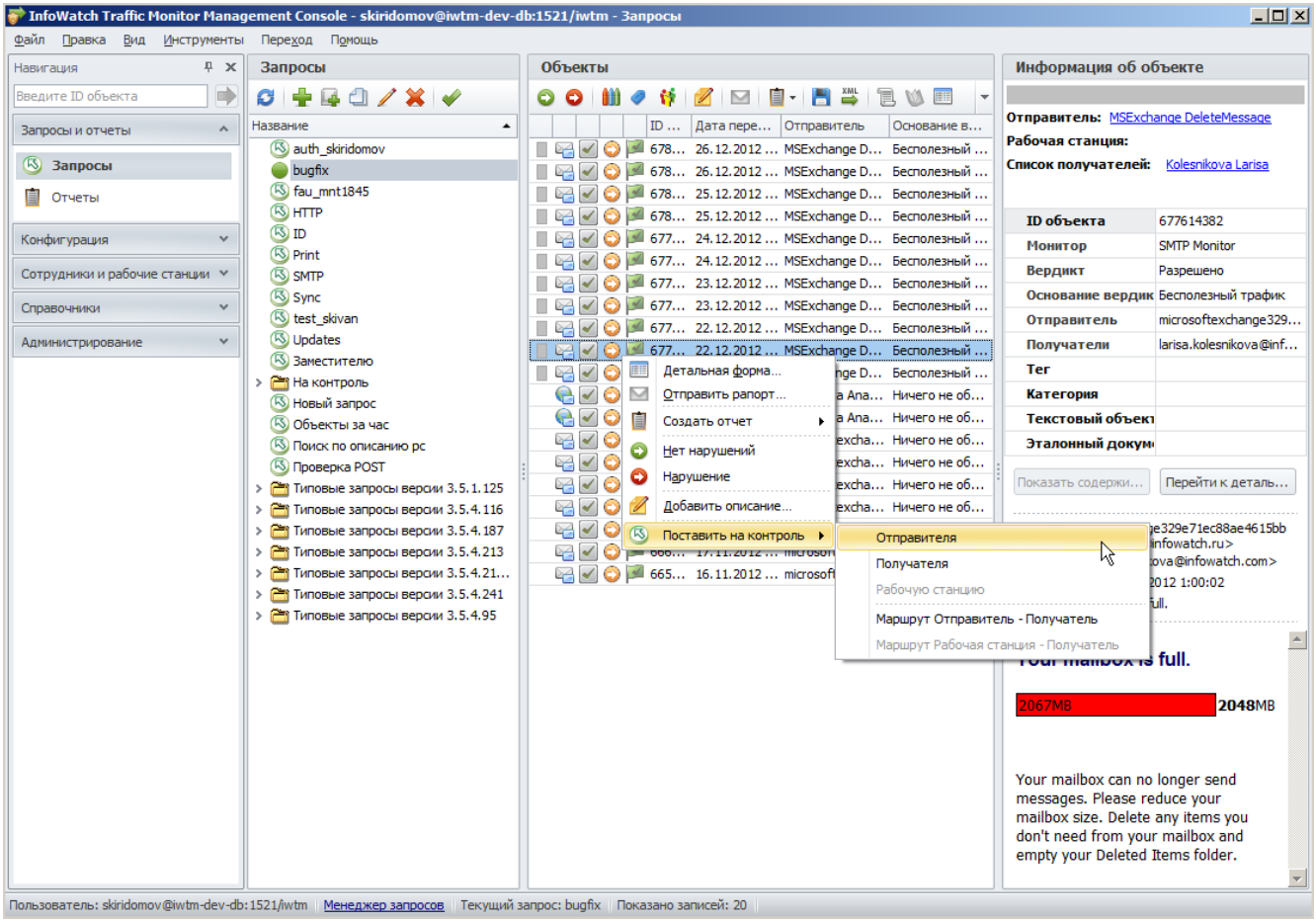
При расследовании инцидентов вы можете воспользоваться функцией постановки на контроль. В результате вызова функции постановки на контроль для необходимого объекта, и определения дополнительных атрибутов, Система автоматически создаст запрос, который поможет вам контролировать:

- **Отправителя** - сведения обо всех объектах, отправленных отправителем выбранного объекта;
- **Получателя** - сведения обо всех объектах, полученных отправителем выбранного объекта;
- **Рабочую станцию** - сведения обо всех объектах, отправленных с той же рабочей станции, что и выбранный объект;
- **Маршрут Отправитель - Получатель** - сведения обо всех объектах, отправленных отправителем и получателем выбранного объекта друг другу;
- **Маршрут Рабочая стация - Получатель** - сведения обо всех объектах, пересылавшихся между рабочей станцией и получателями выбранного объекта.

Таким образом, вы можете контролировать возможные каналы утечки, анализируя данные, представленные в удобном виде.

Контроль объекта осуществляется следующим образом:

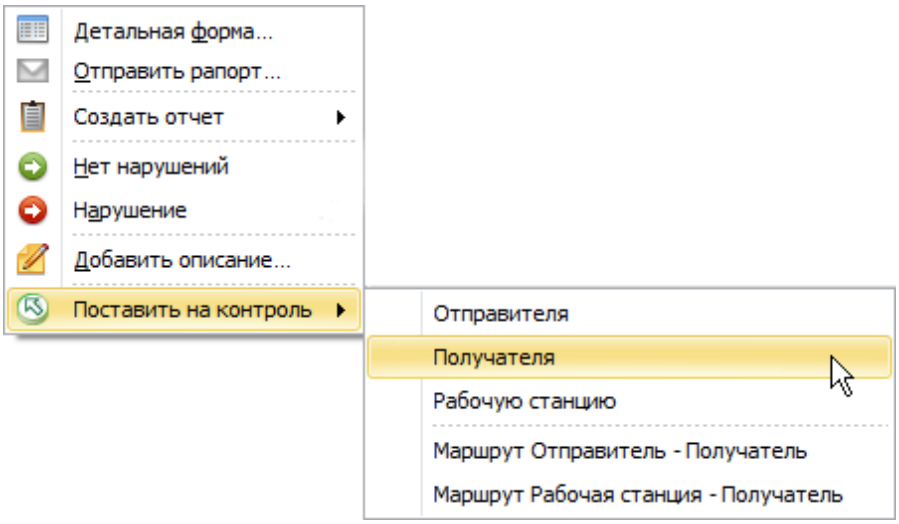
1. Офицер безопасности ставит объект на контроль.
2. Система создает новый запрос согласно выбранным атрибутам.
3. Офицер безопасности работает с созданным запросом: отправляет на выполнение, изменяет параметры, обновляет и т.п.



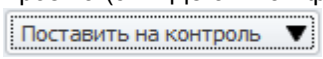
Постановка объекта на контроль

Чтобы поставить объект на контроль:

1. Перейдите к разделу **Запросы** и выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).
2. В области просмотра выделите одну или несколько строк с нужными объектами.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Объект > Поставить на контроль**;
   - нажмите кнопку **Поставить на контроль** на панели инструментов;
   - в области просмотра, в контекстном меню для выбранных объектов, выберите команду **Поставить на контроль**;



Постановка объекта на контроль через контекстное меню

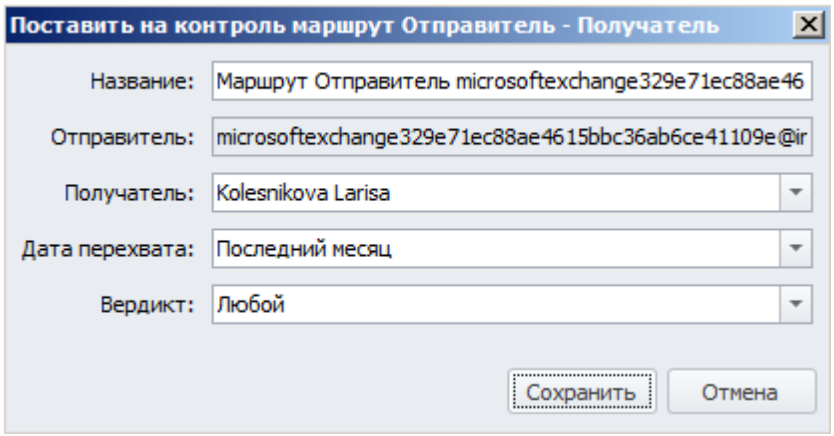
- откройте окно просмотра детальной формы проекта (см. "Детальная форма просмотра объекта") и в левом нижнем углу окна нажмите кнопку 

Поставить на контроль.

4. В раскрывшемся списке атрибутов для постановки на контроль выберите нужный.

5. В открывшемся диалоговом окне вы можете уточнить дополнительные параметры запроса: например, если объект имеет нескольких получателей, выберите одного из раскрывающегося списка. Также вы можете задать значения параметров *«Дата и время перехвата»* (по умолчанию запрос будет отображать объекты за последний месяц) и *«Вердикт»*.

> **Примечание**
>
> Значение атрибута может отображаться красным, если имеется конфликт идентификации (см. "Обработка данных отправителя, получателя и рабочей станции").



Диалоговое окно **Поставить на контроль маршрут Отправитель - Получатель**

6. Нажмите **Сохранить**.

В результате вы перейдёте в папку запросов "*На контроль*", где будет выбран созданный Системой запрос.

Созданный запрос:

- имеет условия запроса, соответствующие выбранным атрибутам;
- доступен только пользователю, который выполнил постановку на контроль;
- не выполнен;

- автоматическое обновление запроса по умолчанию отключено: вы можете выполнять запрос вручную (см. "Выполнение запроса по объектам") или настроить его автообновление (см. " Автоматическое обновление" и "Настройка общих параметров").

8.2.2 Перемещение объекта в другую зону ответственности

Объект, находящийся в определенной зоне ответственности, доступен для просмотра всем пользователям, входящим в эту зону ответственности. В то же время объект может содержать информацию, которая не предназначена для просмотра пользователями, входящими в эту зону ответственности. Тогда можно переместить объект в другую зону ответственности.

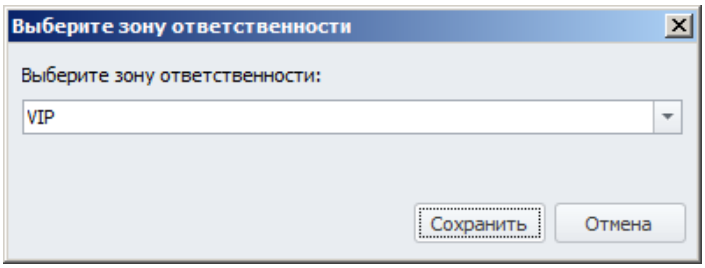
Важная информация!

Передача объекта может выполняться только в те зоны ответственности, которые указаны как зоны возможных переходов для той зоны ответственности, в которой находится объект.

Чтобы переместить объект в другую зону ответственности:

1. Перейдите к разделу **Запросы** и выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).
2. В области просмотра выделите одну или несколько строк с нужными объектами.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Объект > Изменить зону ответственности**;
   - нажмите кнопку **Изменить зону ответственности** на панели инструментов.

   На экран будет выведено диалоговое окно **Выберите зону ответственности**.



Изменение зоны ответственности для объекта

4. Выберите нужную зону ответственности из раскрывающегося списка.
5. Нажмите кнопку **Сохранить**.

   После этого выбранный объект исключается из текущей зоны ответственности и помещается в выбранную зону ответственности.

8.2.3 Отправка рапорта по объекту

Если вам нужно обратить внимание других пользователей Системы на какие-либо объекты, вы можете отправить им рапорт – e-mail, содержащий номера выбранных объектов и сопроводительное сообщение (текст рапорта). Чтобы один пользователь мог отправить рапорт другому:

- в учетной записи получателя должен быть указан его e-mail адрес;
- в учетной записи отправителя получатель должен быть выбран в качестве адресата рапорта.

О настройке этих параметров учетной записи пользователя см. "Создание и редактирование учетной записи пользователя".

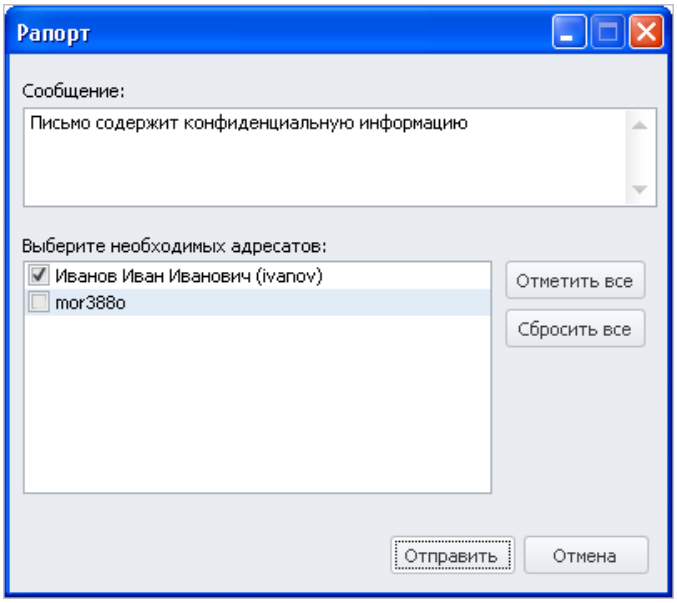
Важная информация!

На компьютере, с которого будут отправляться рапорты, необходимо внести изменения в настройки операционной системы. Для этого откройте **Панель управления** (**Пуск** > **Настройки** > **Панель управления**). Затем выберите компонент **Язык и региональные стандарты**. В открывшемся диалоговом окне перейдите на вкладку **Дополнительно** и выберите русский язык для программ, не поддерживающих Unicode.

Чтобы отправить рапорт по объекту:

1. Перейдите к разделу **Запросы**.
2. Выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).
3. В области просмотра выделите одну или несколько строк с нужными объектами.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Объект > Отправить рапорт**;
   - нажмите кнопку **Отправить рапорт** на панели инструментов;
   - щелкните правой кнопкой мыши по строке с объектом и в контекстном меню выберите пункт **Отправить рапорт**.

   На экран будет выведено диалоговое окно **Рапорт**.



Отправка рапорта по объекту

5. В поле **Сообщение** введите текст рапорта.
6. В списке адресатов отметьте флажками пользователей, которым нужно доставить рапорт. Чтобы установить/снять все флажки используйте кнопки **Отметить все** или **Сбросить все**.
7. Нажмите кнопку **Отправить**.

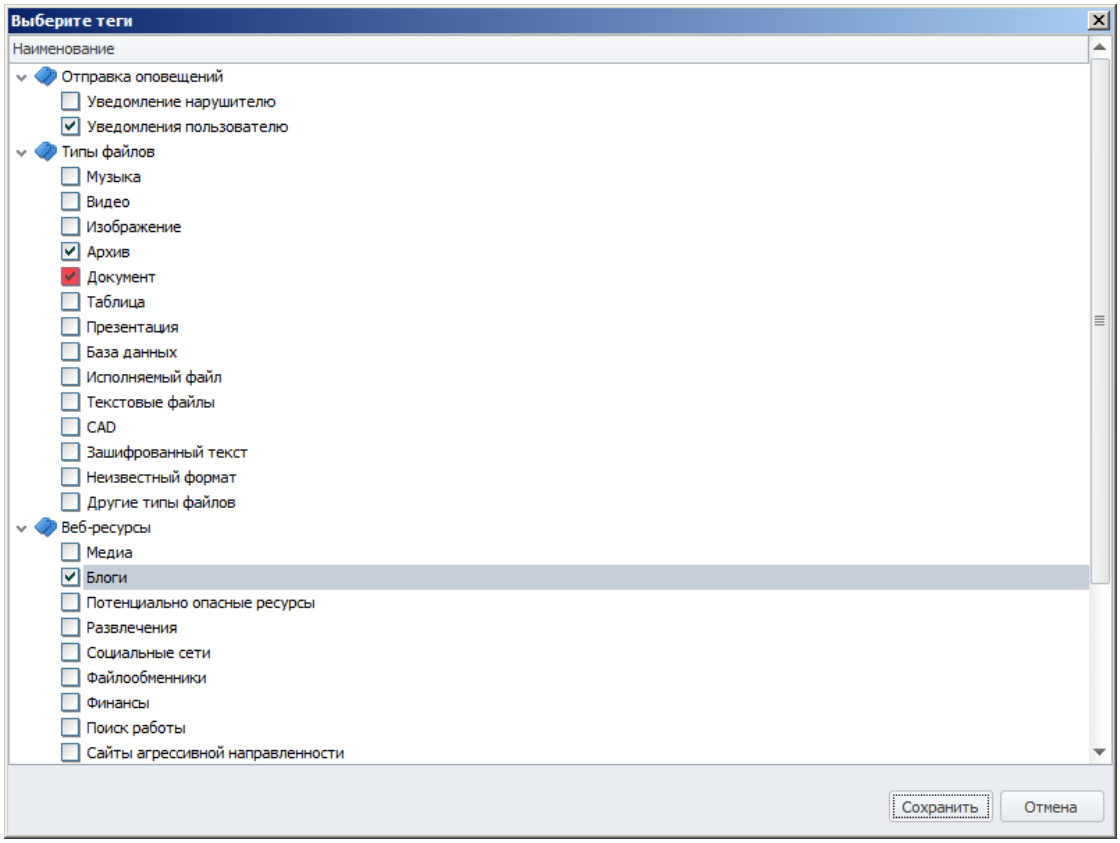
8.2.4 Назначение тегов объекту

Теги представляют собой текстовые метки, дающие краткую характеристику объекта. Например, если в конфигурации имеется тег MUSIC, то можно присвоить этот тег звуковому файлу с музыкальной записью.

Чтобы назначить тег объекту:

1. Перейдите к разделу **Запросы** и выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).
2. В области просмотра выделите одну или несколько строк с нужными объектами.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Объект > Теги**;
   - нажмите кнопку **Теги** на панели инструментов.

   На экран будет выведено диалоговое окно **Выберите теги**.



Настройка тегов для объекта

4. Отметьте флажками все теги, которые нужно присвоить объекту.

   При необходимости отменить назначенный тег, снимите флажок напротив него.

> **Примечание**
>
> Теги, назначенные объекту в результате контентного анализа, выделены в списке красным, и не могут быть отменены.

5. Нажмите кнопку **Сохранить**.

Важная информация!

В InfoWatch Traffic Monitor Standard выполняется периодическое освобождение свободного места в базе данных: если оно меньше объема, необходимого для хранения новых объектов, то выполняется удаление старых объектов.

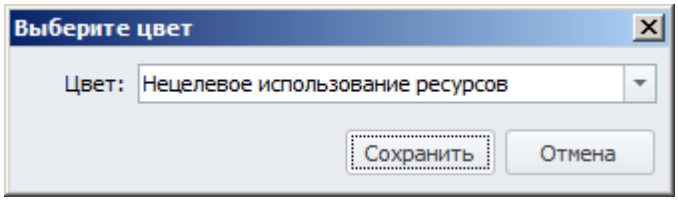
Если вам нужно, чтобы какой-либо объект не мог быть удален вышеописанным способом, назначьте ему тег **«Защитить от удаления»**.

8.2.5 Выделение объектов цветом

Чтобы выделить объект цветом или отменить выделение цветом:

1. Перейдите к разделу **Запросы**.
2. Выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).
3. В области просмотра выделите одну или несколько строк с нужными объектами.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Объект > Цвет**;
   - нажмите кнопку **Цвет** на панели инструментов.

   На экран будет выведено диалоговое окно.



Выбор цвета для выделения объекта

5. Из раскрывающегося списка выберите цвет, которым будет выделен объект.
6. Нажмите кнопку **Сохранить**.

В результате объект будет выделен выбранным цветом. Если вам потребуется снять цветовое выделение, то повторите шаги 1 – 4. В открывшемся диалоговом окне нажмите сначала на кнопку **Очистить**, а затем на кнопку **Сохранить**.

8.2.6 Добавление примечания к объекту

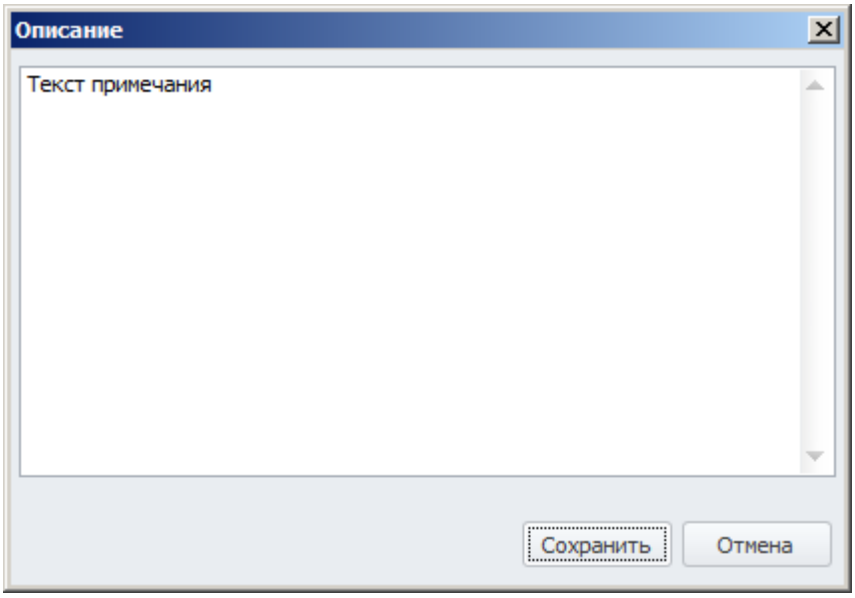
При анализе объекта вы можете добавлять примечания. Примечания отображаются в области чтения при выделении объекта (раздел *Примечание*).

Чтобы добавить примечание к объекту:

1. Перейдите к разделу **Запросы**.
2. Выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).
3. В области просмотра выделите одну или несколько строк с нужными объектами.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Объект > Добавить примечание**;

- нажмите кнопку **Добавить примечание** на панели инструментов;
- щелкните правой кнопкой мыши по строке с объектом и в контекстном меню выберите пункт **Добавить примечание**.

На экран будет выведено диалоговое окно.



Добавление примечания к объекту

5. Введите текст примечания.

6. Нажмите кнопку **Сохранить**.

8.2.7 Выгрузка вложений, писем и xml-контекста

Информация из перехваченных и обработанных объектов может быть выгружена из Системы и сохранена одним из следующих способов:

- Выгрузка вложений объекта
- Сохранение SMTP-сообщения
- Выгрузка контекста

8.2.7.1 Выгрузка вложений объекта

Важная информация!

Для просмотра вложений на вашем компьютере должно быть установлено программное обеспечение, с которым могут быть ассоциированы вложенные файлы.

Чтобы выгрузить вложение путем копирования или сохранения:

1. Перейдите к разделу **Запросы**.
2. Выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).

3. В области просмотра выделите строку, содержащую сведения о нужном объекте.

4. На панели информации об объекте выделите нужное вложение.

5. Щелкните правой кнопкой мыши по выделенному вложению и в раскрывшемся контекстном меню выберите нужную команду:

   - Чтобы скопировать вложение в буфер обмена Windows, выберите команду **Копировать**. Затем вставьте вложение в нужный каталог.
   - Чтобы сохранить вложение, выберите команду **Сохранить**; чтобы сохранить все имеющиеся вложения - **Сохранить все**. Затем в открывшемся диалоговом окне **Обзор папок** выберите каталог, в который нужно сохранить вложение.

6. Нажмите кнопку **OK**.

8.2.7.2 Выгрузка SMTP-писем

Если у вас включен просмотр содержимого объекта (см. "Настройка режима просмотра содержимого объекта" и "Просмотр информации по объектам"), то вы можете выгружать SMTP-письма в виде файлов формата EML.

Чтобы выгрузить SMTP-письмо в файл:

1. Перейдите к разделу **Запросы**.
2. Выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).
3. В области просмотра выделите строку, содержащую сведения о нужном SMTP-письме.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Объект > Сохранить сообщение**;
   - нажмите кнопку  **Сохранить сообщение** на панели инструментов.
5. В открывшемся диалоговом окне укажите имя и местоположение файла. Затем нажмите кнопку **Сохранить**.

8.2.7.3 Выгрузка контекста

Вы можете сохранить xml-контексты обработанных объектов (одного или сразу нескольких) в виде файлов.



Важная информация!

Содержание выгруженного xml-контекста будет зависеть от того, отображается ли в Консоли управления содержимое объекта в момент выгрузки (подробнее см. "Просмотр информации по объектам").

Чтобы выгрузить xml-контекст объектов:

1. Перейдите к разделу **Запросы**.
2. Выполните необходимый запрос (например, дважды щелкните по нему левой кнопкой мыши).
3. В области просмотра выделите строки с необходимыми объектами.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Объект > Сохранить контекст**;

- нажмите кнопку  **Сохранить контекст** на панели инструментов.

5. В открывшемся диалоговом окне укажите, куда вы хотите сохранить выгруженные файлы. Затем нажмите кнопку **Сохранить**.

Вы также можете выгрузить xml-контекст объекта из детальной формы просмотра объекта. Для этого на детальной форме нажмите кнопку **Сохранить контекст.**

8.3 Составление отчетов по объектам

Отчеты по объектам позволяют получить наглядное отображение статистической информации по перехваченным и обработанным данным.

Работа с отчетами производится в Консоли управления, в разделе **Отчеты**.

Отчеты рассчитаны на работу с данными большого объема, поэтому выборка данных по отчету может занимать продолжительное время. Текущее состояние отчета отображается в рабочей области главного окна, в столбце **Статус**:

Статус отчета	Описание статуса
Ожидание обновления	Присваивается новому отчету
Обновляется	Осуществляется построение выборки в базе данных
Готов	Построение выборки завершено успешно
Ошибка	При построении выборки возникла ошибка

Выполнять отчет можно, если он имеет статус *Готов*. В результате выполнения отчета выводятся только данные, имеющиеся в текущем представлении. Чтобы в представлении отображались актуальные данные, необходимо периодически выполнять перестройку представления (см. "Перестроение отчета").



Важная информация!

Возможность перестройки отчетов доступна только пользователям, имеющим право на выполнение отчетов.

Для более удобной работы, отчеты можно группировать по папкам (см. "Управление папками запросов и отчетов").

Информацию о порядке составления отчетов по объектам вы можете найти в следующих разделах:

- Типы отчетов
- Создание и редактирование отчета
- Перестроение отчета
- Просмотр результатов отчета

- Печать отчета
- Экспорт отчета
- Копирование отчета
- Удаление отчета

8.3.1 Типы отчетов

Все отчеты в Системе базируются на основных типах отчетов. При создании отчета вы можете уточнить выборку отчетных данных, указав дополнительные условия: см. "Создание и редактирование отчета".

Описание типов отчетов приведено в следующей таблице.

Тип отчета	**Описание**	**Атрибут группировки результатов**	**Настройки на закладке Параметры**	**Тип диаграммы**
Категории – самые популярные	Отчет показывает, какие категории наиболее часто встречаются в перехваченном трафике. Содержит данные в абсолютном значении и в процентном соотношении.	Категории	**Количество отображаемых записей** **Сортировка результатов отчета** (количество объектов для данной категории)	Линейчатая диаграмма
Категории – частота срабатывания	Отчет показывает, насколько часто в перехваченном трафике встречаются объекты, соответствующие выбранным категориям. Содержит данные в абсолютном значении и в процентном соотношении.	Категории	**Сортировка результатов отчета** (количество объектов для данной категории) **Выберите категории, по которым нужна детальная информация**	Линейчатая диаграмма
Контентные маршруты – распределение по мониторам	**Контентный маршрут** – это установившаяся цепочка передачи информации – пара «Отправитель – Получатель». Цепочка передачи информации считается установившейся, если для данной пары «Отправитель – Получатель» Система перехватила более L объектов, где L – **параметр установившейся цепочки передачи информации**. В отчете отображается количество (абсолютное и в процентах) выявленных	Монитор	**Параметр установившейся цепочки передачи информации**	Круговая диаграмма

Тип отчета	Описание	Атрибут группировки результатов	Настройки на закладке Параметры	Тип диаграммы
	контентных маршрутов для каждого монитора.			
Контентные маршруты – самые популярные	**Контентный маршрут** – это установившаяся цепочка передачи информации – пара «Отправитель - Получатель». Цепочка передачи информации считается установившейся, если для данной пары «Отправитель - Получатель» Система перехватила более L объектов, где L - **параметр установившейся цепочки передачи информации**. В отчете отображаются наиболее часто встречаемые контентные маршруты.	пара «Отправитель - Получатель»	**Количество отображаемых записей** **Параметр установившейся цепочки передачи информации** **Сортировка результатов отчета** (количество объектов, переданных по одному маршруту)	Линейчатая диаграмма
Отправители – использование веб-ресурсов	Отправители, для которых было зафиксировано максимальное количество объектов перехваченных HTTP монитором. Для каждого отправителя отображается количество (абсолютное и в процентах) запросов на сайт той или иной тематики. Тематика сайта определяется по наличию у объекта соответствующего тега из предустановленной группы тегов *Тематика сайтов*. Для каждой тематики адреса соответствующих сайтов определяются с помощью предустановленной группы списков *Веб-ресурсы*.	Отправитель	**Количество отображаемых записей** **Сортировка результатов отчета** (количество объектов для данного отправителя)	Линейчатая диаграмма
Отправители – пересылаемые типы файлов	Отправители, для которых зафиксировано максимальное количество фактов отправки файлов. Для каждого отправителя отображается количество (абсолютное и в процентах) того или иного типа файлов. Тип файла	Отправитель	**Количество отображаемых записей** **Сортировка результатов отчета** (количество объектов для данного отправителя)	Линейчатая диаграмма

Тип отчета	**Описание**	**Атрибут группировки и результатов**	**Настройки на закладке Параметры**	**Тип диаграммы**
	определяется наличием в объекте соответствующего тега из предустановленной группы тегов *Типы файлов*			
Отправители – самые активные	Отправители, для которых было зафиксировано максимальное количество перехваченных при отправке объектов, с указанием количества перехваченных объектов (абсолютное и в процентах от общего кол-ва)	Отправитель	**Количество отображаемых записей** **Сортировка результатов отчета** (количество объектов для данного отправителя)	Линейчатая диаграмма
Список получателей – самые популярные	Почтовые адреса, на которые было отправлено максимальное количество перехваченных объектов. Для каждого получателя указывается количество перехваченных объектов (абсолютное и в процентах от общего кол-ва)	Получатель	**Количество отображаемых записей** **Сортировка результатов отчета** (количество объектов для данного получателя)	Линейчатая диаграмма
Рабочие станции – самые активные	Рабочие станции, для которых было зафиксировано максимальное количество перехваченных при отправке объектов, с указанием количества перехваченных объектов (абсолютное и в процентах от общего кол-ва)	Рабочие станции	**Количество отображаемых записей** **Сортировка результатов отчета** (количество объектов для данного получателя)	Линейчатая диаграмма
Статистика – активность пользователей	Динамика количества перехваченных объектов за заданный период, с детализаций по вердиктам Системы: • **Количество** – общее число перехваченных объектов; • **Запрещено** – вердикт *Forbidden* • **Разрешено** – вердикт *Allowed*	Дата перехвата объекта (детализация по выбранному интервалу: год, месяц, неделя…)	**Интервал** (год, месяц, неделя…) Детализация: • **Показать все** • **Показать разрешенные** • **Показать запрещенные**	Линейный график
Статистика – ложные	Количество (абсолютное и в процентах) объектов, сгруппированное по	Пользовательское	-	Круговая диаграмма

Тип отчета	Описание	Атрибут группировки результатов	Настройки на закладке Параметры	Тип диаграммы
срабатывания	следующим типам пользовательских решений: • **Анализ вердикта не проводился**: пользовательское решение не принято; • **Вердикт подтвержден пользователем**: пользовательское решение принято и совпадает с вердиктом системы; • **Ложноположительный вердикт**: вердикт Системы – *Forbidden*, пользовательское решение – *Нет нарушений*; • **Ложноотрицательный вердикт**: вердикт Системы – *Allowed*, пользовательское решение – *Нарушение*.	решение		
Статистика – наличие категорий	Количество (абсолютное и процентное) объектов, в которых обнаружены какие-либо категории.	Категории	**Показывать значение как процент**	Круговая диаграмма
Статистика – наличие текстовых объектов	Количество (абсолютное и процентное) объектов, в которых обнаружены какие-либо текстовые объекты	Эталонные документы	**Показывать значение как процент**	Круговая диаграмма
Статистика – наличие эталонных документов	Количество (абсолютное и процентное) объектов, в которых обнаружены какие-либо эталонные документы.	Типы текстовых объектов	**Показывать значение как процент**	Круговая диаграмма
Статистика – обработка объектов	Количество (абсолютное и в процентах) объектов, сгруппированное по пользовательскому решению: • **Не обработано** – пользовательское решение не принято; • **Обработано** пользовательское решение принято.	Пользовательское решение	-	Круговая диаграмма

Тип отчета	**Описание**	**Атрибут группировки и результатов**	**Настройки на закладке Параметры**	**Тип диаграммы**
Статистика – соотношение объектов по вердиктам	Количество (абсолютное и процентное) перехваченных объектов по вердиктам.	Вердикт	**Показывать значение как процент**	Круговая диаграмма
Статистика – соотношение объектов по мониторам	Количество (абсолютное и процентное) перехваченных объектов по мониторам.	Монитор	**Показывать значение как процент**	Круговая диаграмма
Теги – частота срабатывания	Отчет показывает, сколько перехваченных объектов было помечено тем или иным тегом из выбранной группы тегов. Содержит данные в абсолютном значении и в процентном соотношении	Теги выбранной группы тегов	**Сортировка результатов отчета** (количество объектов с этим тегом из выбранной группы тегов) **Выберите группы тегов, по которым нужна детальная информация**	Линейчатая диаграмма
Текстовые объекты – самые популярные	Типы текстовых объектов, к которым отнесено максимальное количество объектов в перехваченном трафике. Для каждого типа текстовых объектов указывается количество перехваченных объектов (абсолютное и в процентах от общего кол-ва)	Типы текстовых объектов	**Количество отображаемых записей** **Сортировка результатов отчета** (количество объектов для данного типа текстовых объектов)	Линейчатая диаграмма
Текстовые объекты – частота срабатывания	Количество (абсолютное и в процентах от общего кол-ва) объектов, в которых обнаружены выбранные текстовые объекты.	Типы текстовых объектов	**Сортировка результатов отчета** (количество объектов для данного типа текстового объекта) **Выберите текстовые объекты, по которым нужна детальная информация**	Линейчатая диаграмма
Эталонные документы – самые популярные	Эталонные документы, к которым отнесено максимальное количество объектов в перехваченном трафике. Для каждого эталонного документа указывается количество перехваченных объектов	Эталонные документы	**Количество отображаемых записей** **Сортировка результатов отчета** (количество объектов для данного эталонного документа)	Линейчатая диаграмма

Тип отчета	Описание	Атрибут группировки результатов	Настройки на закладке Параметры	Тип диаграммы
	(абсолютное и в процентах от общего кол-ва)			
Эталонные документы – частота срабатывания	Количество (абсолютное и в процентах от общего кол-ва) объектов, в которых обнаружены выбранные эталонные документы.	Эталонные документы	**Сортировка результатов отчета** (количество объектов для данного эталонного документа) **Выберите эталонные документы, по которым нужна детальная информация**	Линейчатая диаграмма

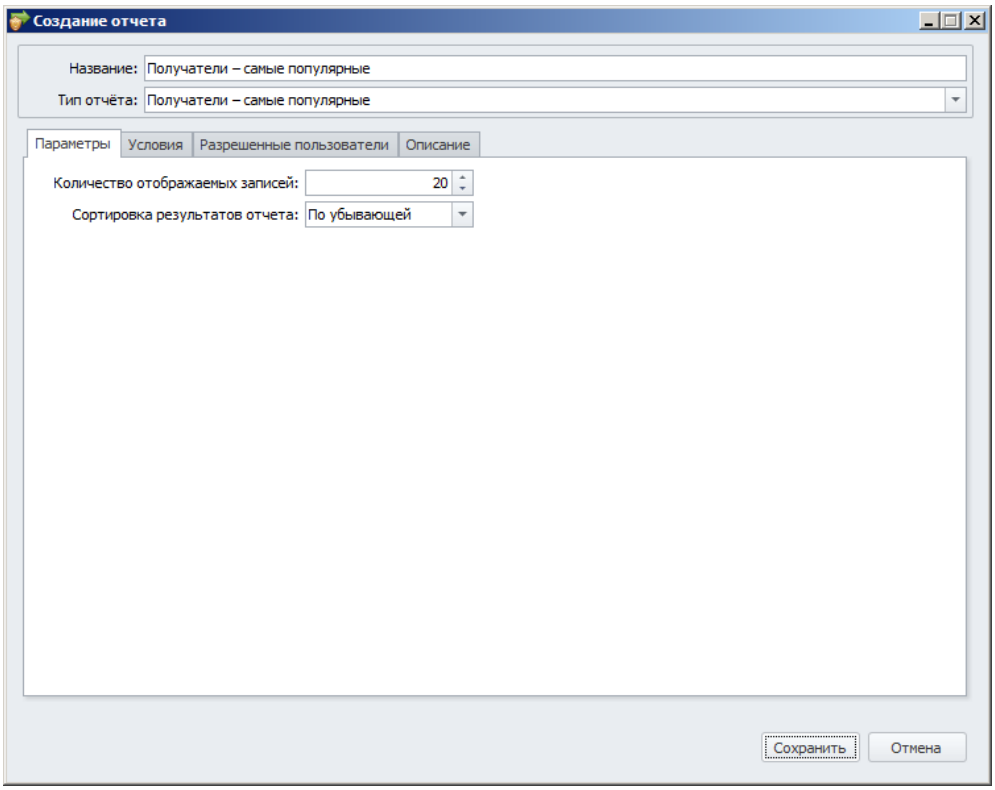
8.3.2 Создание и редактирование отчета

Чтобы составить запрос для создания отчета:

1. Перейдите к разделу **Отчеты**.
2. Выполните необходимые действия:

Необходимое действие	Порядок выполнения
Создать отчет	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Создать отчет** • нажмите кнопку **Создать отчет** на панели инструментов.
Отредактировать отчет	1. В списке отчетов выделите строку с нужным отчетом. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку **Изменить** на панели инструментов; • щелкните правой кнопкой мыши на названии отчета и в раскрывшемся контекстном меню выберите команду **Изменить**.

На экран будет выведено диалоговое окно с параметрами отчета.



Составление отчета

3. В открывшемся диалоговом окне настройте параметры отчета:

   - **Наименование**. Укажите название отчета.

   - **Тип отчета**. Из раскрывающегося списка выберите необходимый тип отчета.

   - На вкладке **Параметры** определите параметры создаваемого отчета. Набор параметров зависит от типа отчета, выбранного на предыдущем шаге. Описание параметров для каждого типа отчета приведено в разделе "Типы отчетов".

   - На вкладке **Условия** задайте условия для составления отчета. Настройка условия при составлении отчетов выполняется так же, как и при создании запросов (см. "Настройка условий запроса (вкладка Условия)").

   - На вкладке **Разрешенные пользователи** отметьте флажками учетные записи тех пользователей, которые смогут просматривать этот отчет. Чтобы установить/снять все флажки используйте кнопки **Отметить все** и **Сбросить все**.

   - На вкладке **Описание** введите описание отчета.

4. Нажмите кнопку **Сохранить**.

После создания отчёт имеет статус *Ожидание обновления*. Когда отчет получит статус *Готов* (используйте функцию обновления: см. "Обновление данных в Консоли управления"), вы можете просматривать его результаты, печатать отчет и экспортировать его в файл.

8.3.3 Просмотр результатов отчета

Вы можете просмотреть данные по отчётам, находящимся в состоянии *Готов*. В результате построения отчета будет отображена информация (в том числе – графическая) по количеству объектов, удовлетворяющих определенным условиям.

Примечание

Подсчет общего количества объектов в отчете ведется только по тем зонам ответственности, которые назначены пользователю, генерирующему отчет.

Чтобы построить отчет:

1. Перейдите к разделу **Отчеты**.
2. В рабочей области главного окна выделите нужный отчет.
3. Выполните одно из следующих действий:
   - дважды щелкните левой кнопкой мыши по выделенному отчету;
   - нажмите кнопку **Выполнить** на панели инструментов.

   После этого будет открыто окно **Просмотр** с отчетом по выбранным объектам.

Примечание

Многостраничные отчеты можно просматривать с помощью стандартных кнопок перемещения, расположенных на панели инструментов в окне отчета.

Отчеты можно печатать (см. "Печать отчета") и экспортировать в файл (см. "Экспорт отчета").

8.3.4 Перестроение отчета

Данные, которые выводятся в результате построения отчета, соответствуют представлению, ассоциированному с этим отчетом. Однако в процессе работы данные постоянно обновляются. Чтобы получать отчеты на основании актуальных данных, перед построением отчета рекомендуется выполнить процедуру обновления.

Чтобы обновить данные по отчету:

1. Перейдите к разделу **Отчеты**.
2. В рабочей области главного окна выделите нужный отчет.
3. Нажмите кнопку **Перестроить**, расположенную на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **ОК**, чтобы запустить обновление данных.

8.3.5 Печать отчета

Печать отчета выполняется из окна **Просмотр**, в котором выводится отчет.

Чтобы настроить параметры печати и распечатать отчет:

1. Выполните одно из следующих действий:
   - в главном меню выберите команду **Файл > Печать**;
   - нажмите кнопку **Печать**, на панели инструментов.
2. В диалоговом окне **Печать** настройте параметры печати.

Чтобы отправить отчет на печать без предварительной настройки параметров печати,

выполните одно из следующих действий:

- в главном меню выберите команду **Файл** > **Печать на принтере по умолчанию**
- нажмите кнопку **Печать на принтере по умолчанию** на панели инструментов.

8.3.6 Копирование отчета

Вы можете создать отчет на основе уже существующего путём его копирования.

Чтобы скопировать отчет:

1. Перейдите к разделу **Отчеты**.
2. В рабочей области главного окна выделите нужный отчет.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Копировать**;
   - нажмите кнопку **Копировать** на панели инструментов.

Отчет-копия будет иметь те же параметры, что и исходный, с добавлением к названию номера копии. Например, копия отчета «*Общее количество инцидентов, выявленных Системой*» будет иметь название « *Общее количество инцидентов, выявленных Системой (1)*».

8.3.7 Экспорт отчета

Отчет можно экспортировать в файл одного из поддерживаемых форматов:. `pdf`, `.xls`, `.rtf`, `.html`, файлы графических форматов и др. Экспортированный отчет можно просматривать и обрабатывать средствами той программы, с которой ассоциирован выбранный формат файла.

Экспорт отчета выполняется из окна **Просмотр**, в котором выводится отчет.

Чтобы экспортировать отчет в файл:

1. Выполните одно из следующих действий:
   - в главном меню выберите команду **Файл > Экспорт** и в раскрывшемся подменю выберите подходящий тип файла;

- нажмите кнопку  **Экспорт** на панели инструментов. Нажмите на стрелку справа от кнопки **Экспорт** и в раскрывшемся списке выберите нужный тип файла.

2. В диалоговом окне **Сохранить** выберите папку для хранения отчета и укажите имя файла, в который будет экспортирован отчет.

8.3.8 Удаление отчета

Чтобы удалить отчет:

1. Перейдите к разделу **Отчеты**.
2. В рабочей области главного окна выделите нужный отчет.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Удалить**;
   - нажмите кнопку  **Удалить** на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы подтвердить удаление.

8.4 Управление папками запросов и отчетов

Для более удобного просмотра запросы и отчеты можно группировать по папкам. Информация по работе с папками приведена в подразделах:

- Создание и редактирование папки
- Перемещение запросов и отчетов между папками
- Копирование папки
- Удаление папки

8.4.1 Создание и редактирование папки

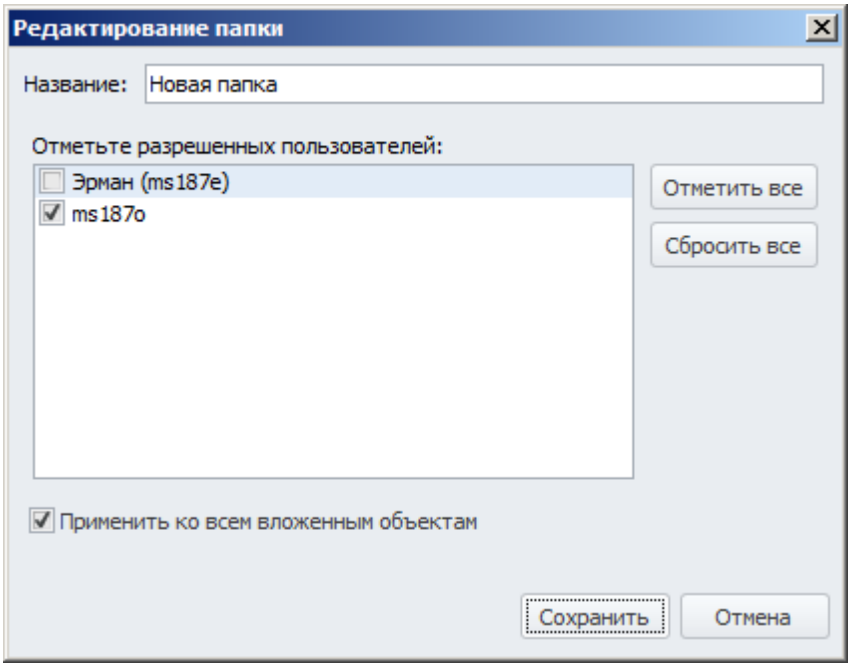
Чтобы создать или отредактировать папку:

1. Перейдите к нужному разделу (**Запросы** или **Отчеты**).
2. Выполните необходимые действия:

Необходимое действие	Порядок выполнения
Создать папку	Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Создать папку**;

Необходимое действие	**Порядок выполнения**
	• нажмите кнопку **Создать папку** на панели инструментов.
Отредактировать папку	1. Выделите нужную папку. 2. Выполните одно из следующих действий: • в главном меню выберите команду **Правка > Изменить**; • нажмите кнопку **Изменить** на панели инструментов; • щелкните правой кнопкой мыши на названии папки и в раскрывшемся контекстном меню выберите команду **Изменить**.

После этого на экран будет выведено диалоговое окно.



Настройка параметров папки

3. Настройте параметры папки:
   - **Название**. Наименование папки.
   - **Отметьте разрешенных пользователей**. Отметьте флажками учетные записи тех пользователей, которым будет дано право на управление данной папкой. Чтобы установить или снять все флажки, воспользуйтесь кнопками **Отметить все** и **Сбросить все**.

     Важная информация!

     Папка может быть создана при условии, что указан хотя бы один разрешенный пользователь.

   - **Применить ко всем вложенным объектам**. Если вы редактируете папку и хотите, чтобы какой-либо из пользователей получил права (лишился прав) на управление всеми запросами или отчетами, находящимися в папке, то отметьте (снимите) флажок напротив имени этого пользователя в списке разрешенных пользователей и установите флажок в поле **Применить ко всем вложенным объектам**.

Примечание

Если при добавлении пользователя в список разрешенных, флажок в поле **Применить ко всем вложенным объектам** не будет отмечен, то такой пользователь будет видеть эту папку пустой и сможет только добавлять в неё свои запросы/отчеты.

Важная информация!

Добавление пользователя в список разрешенных для всех вложенных объектов приведет к тому, что он сможет изменить, скопировать или удалить все разрешенные ему папки и запросы/отчеты.

4. Нажмите кнопку **Сохранить**.

В новой папке вы можете создавать запросы (см. "Создание и редактирование запроса") или отчеты (см. " Создание и редактирование отчета"), или перемещать в неё другие запросы/отчеты/папки (см. " Перемещение запросов и отчетов между папками").

8.4.2 Перемещение запросов и отчетов между папками

Чтобы переместить запрос, отчет или папку из одной папки в другую:

1. Перейдите к нужному разделу (**Запросы** или **Отчеты**).
2. Щелкните левой кнопкой мыши по названию нужного запроса/отчета/папки. Чтобы выделить несколько, нажмите и удерживайте кнопку **Ctrl** или **Shift**
3. Не отпуская левую кнопку мыши, перетащите строку с названием запроса/отчета/папки к нужной папке. Когда слева от названия нужной папки появится желтая стрелка, отпустите левую кнопку мыши.

В результате запрос/отчет/папка будет перемещен в выбранную папку.

Чтобы переместить запрос на уровень выше:

1. Щелкните левой кнопкой мыши по названию нужного запроса/отчета/папки, одновременно нажимая клавишу клавиатуры `Shift`.
2. Не отпуская левую кнопку мыши и клавишу клавиатуры `Shift`, переместите строку с названием запроса/отчета/папки к той папке, выше которой нужно ее переместить. Когда слева появится синяя стрелка, отпустите левую кнопку мыши и клавишу клавиатуры `Shift`.

В результате запрос/отчет/папка будет перемещен в папку, находящуюся выше уровнем.

8.4.3 Копирование папки

Чтобы создать копию папки:

1. Перейдите к нужному разделу (**Запросы** или **Отчеты**).
2. Выделите нужную папку.

3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка > Копировать**;
   - нажмите кнопку  **Копировать** на панели инструментов.

Будет создана папка-копия, содержащая копии всех подпапок и отчетов/запросов из исходной копируемой папки. Название папки-копии будет аналогично исходной папке, с добавлением к названию номера копии. Например, копия отчета «*Все события за период*» будет иметь название «*Все события за период (1)*». Названия подпапок и отчетов/запросов, скопированных из исходной папки, будут аналогичны оригиналам.

Права на работу с папкой-копией и её содержимым по умолчанию получает только тот пользователь, который выполнил копирование.

При необходимости, вы можете изменить название папки-копии и список разрешенных пользователей, как описано в разделе "Создание и редактирование папки".

8.4.4 Удаление папки



Примечание

В папке могут содержаться скрытые запросы, отчеты или другие папки, т.е. такие запросы (отчеты, папки), на которые у вас нет прав просмотра. Такая папка может быть удалена только пользователем, имеющим права на работу со всеми запросами/отчетами, хранящимися в этой папке.

Чтобы удалить папку:

1. Перейдите к нужному разделу (**Запросы** или **Отчеты**).
2. Выделите нужную папку.
3. Нажмите кнопку  **Удалить** на панели инструментов.
4. В открывшемся окне запроса нажмите кнопку **Да**, чтобы удалить папку с группой запросов.

9 Лицензионная информация

Краткое содержание части:

- Пользовательское лицензионное соглашение
- Лицензии третьих сторон

9.1 Пользовательское лицензионное соглашение

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями лицензионного соглашения перед началом работы с программным обеспечением.

Нажатие Вами кнопки подтверждения согласия в окне с текстом лицензионного соглашения при установке программного обеспечения или использование устанавливаемого программного обеспечения означает Ваше безоговорочное согласие с условиями настоящего лицензионного соглашения. Если Вы не согласны с условиями настоящего лицензионного соглашения, Вы должны прервать установку и/или использование программного обеспечения.

Лицензионное соглашение

Настоящее пользовательское лицензионное соглашение (далее – Соглашение) является Договором присоединения между ЗАО «ИнфоВотч» (далее – Правообладатель) и Вами, физическим или юридическим лицом (далее – Пользователь), правомерно владеющим экземпляром программного комплекса InfoWatch Traffic Monitor – (далее – Система).

Система предназначена для мониторинга, фильтрации и предотвращения утечки данных, передаваемых за пределы компании по электронной почте, через Интернет и интернет-пейджеры, а также сетевой и локальной печати. Система также позволяет контролировать доступ к портам персональных компьютеров и осуществлять мониторинг данных, копируемых на сменные устройства.

1. **Определения**

   1.1. ПО – обозначает, как вместе, так и по отдельности, Систему, сопроводительные материалы, Документация к Системе, дополнительно заказанные обновления Системы, правообладателем которых является ЗАО «ИнфоВотч».

   1.2. Компьютер – оборудование, для работы на котором предназначено ПО, на которое устанавливается Система и/или на котором используется Система.

   1.3. Пользователь (Вы) – лицо, которое устанавливает или использует ПО от своего лица или правомерно владеет копией ПО. Если ПО было загружено или приобретено от имени юридического лица, то под термином Пользователь (Вы) далее подразумевается юридическое лицо, для которого ПО было загружено или приобретено и которое поручило отдельному физическому лицу принять данное соглашение от своего лица.

   1.4. Партнеры – организации, осуществляющие распространение ПО на основании договора с Правообладателем.

   1.5. Документация к Системе – сопроводительные печатные и иные материалы, Руководство Пользователя, Руководство Администратора, справочник, файл справки и аналогичные им сопроводительные печатные и электронные документы в отношении Системы, правообладателем которых является ЗАО «ИнфоВотч».

2. **Предоставление лицензии**

   2.1. Правообладатель предоставляет Вам неисключительную лицензию на использование ПО в рамках функциональности, описанной в Документации к Системе, при условии соблюдения Вами всех технических требований, описанных в Документации к Системе, а также всех ограничений и условий использования Системы, указанных в настоящем Соглашении.

   2.2. В случае если Вы получили, загрузили и/или установили ПО, предназначенное для

ознакомительных целей, Вы имеете право использовать ПО только в целях ознакомления и только в течение одного ознакомительного периода, если не прописано иначе, начиная с даты начальной установки ПО. Любое использование ПО для других целей или по завершении ознакомительного периода запрещено.

2.3. Если Вы используете ПО разных версий или версии ПО для разных языков, если Вы получили ПО на нескольких носителях, если Вы иным способом получили несколько копий ПО или получили ПО в составе пакета другого программного обеспечения, то общее количество Ваших компьютеров, на которых установлены и/или используются все версии Системы, должно соответствовать количеству лицензий, полученных от Правообладателя в том случае, если условия лицензии не утверждают иное; каждая купленная лицензия дает Вам право установить и использовать Систему на таком количестве компьютеров и/или в отношении определенного количества лицензионных объектов, которое указано в п.2.2.

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

2.5. Любая правомерная передача прав в отношении пользования ПО возможна только при условии присоединения к настоящему соглашению и с предварительного согласия Правообладателя или его уполномоченного Партнера. При этом, правопреемник Пользователя в отношении использования ПО становится законным правопреемником Пользователя в отношении использования ПО только при условии полного замещения Пользователя по настоящему соглашению.

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

3. Ограничения

3.1. Вы не вправе декомпилировать, дизассемблировать, модифицировать или выполнять производные работы, основанные на ПО, целиком или частично, за исключением случаев, предусмотренных законодательством.

3.2. Запрещается передавать право на использование ПО третьим лицам за исключением случая, указанного в п. 2.6.

3.3. Запрещается передавать и предоставлять доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения, за исключением случая, указанного в п.2.6 настоящего Соглашения. Лицензионный ключ являются конфиденциальной информацией. Правообладатель оставляет за собой право использовать средства для проверки подлинности установленного у Вас лицензионного ключа.

3.4. Запрещается сдавать ПО в аренду, прокат или во временное пользование, а так же разглашать результаты стендовых испытаний Системы.

3.5. Правообладатель имеет право заблокировать лицензионный ключ в случае нарушения Пользователем условий настоящего Соглашения.

3.6. При использовании Вами ПО, предназначенного для ознакомительных целей, Вы не имеете права передавать имеющийся у Вас экземпляр ПО третьим лицам.

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

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

3.9. В случае нарушения Вами какого-либо из условий данного Соглашения Правообладатель вправе прервать действие Соглашения на использование ПО в любое время без Вашего уведомления и без возмещения стоимости ПО или его части.

4. Ограниченная гарантия и отказ от предоставления гарантий

4.1. Правообладатель гарантирует работу ПО в соответствии с описанием, изложенным в Документации к Системе.

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

4.3. Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Документации к Системе, а также в случае нарушения Пользователем условий настоящего Соглашения.

4.4. ЗА ИСКЛЮЧЕНИЕМ УСТАНАВЛИВАЕМОЙ В НАСТОЯЩЕМ ПУНКТЕ ОГРАНИЧЕННОЙ ГАРАНТИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ НА ЕГО ИСПОЛЬЗОВАНИЕ ИЛИ ПРОИЗВОДИТЕЛЬНОСТЬ. ЗА ИСКЛЮЧЕНИЕМ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ, СТЕПЕНЬ КОТОРЫХ НЕ МОЖЕТ БЫТЬ ИСКЛЮЧЕНА ИЛИ ОГРАНИЧЕНА ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ (ВЫРАЖАЕМЫХ В ЯВНОЙ ИЛИ В ПОДРАЗУМЕВАЕМОЙ ФОРМЕ) НА ВСЕ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ НЕНАРУШЕНИЕ ПРАВ ТРЕТЬИХ ЛИЦ, КОММЕРЧЕСКОЕ КАЧЕСТВО, ИНТЕГРАЦИЮ ИЛИ ПРИГОДНОСТЬ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ВЫ СОГЛАШАЕТЕСЬ С ТЕМ, ЧТО ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ВЫБОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, ЗА УСТАНОВКУ И ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ ЗА РЕЗУЛЬТАТЫ, ПОЛУЧЕННЫЕ С ЕГО ПОМОЩЬЮ.

5. Ограничение ответственности

В МАКСИМАЛЬНОЙ СТЕПЕНИ, ДОПУСКАЕМОЙ ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И/ИЛИ ЕГО ПАРТНЕРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКИЕ-ЛИБО УБЫТКИ И/ИЛИ УЩЕРБ (В ТОМ ЧИСЛЕ УБЫТКИ В СВЯЗИ С НЕДОПОЛУЧЕННОЙ КОММЕРЧЕСКОЙ ПРИБЫЛЬЮ, ПРЕРЫВАНИЕМ ДЕЯТЕЛЬНОСТИ, УТРАТОЙ ИНФОРМАЦИИ ИЛИ ИНОЙ ИМУЩЕСТВЕННЫЙ УЩЕРБ), ВОЗНИКАЮЩИЕ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ИЛИ НЕВОЗМОЖНОСТЬЮ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ БЫЛИ УВЕДОМЛЕНЫ О ВОЗМОЖНОМ ВОЗНИКНОВЕНИИ ТАКИХ УБЫТКОВ И/ИЛИ УЩЕРБА. В ЛЮБОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ ПРАВООБЛАДАТЕЛЯ И ЕГО ПАРТНЕРОВ ПО ЛЮБОМУ ИЗ ПОЛОЖЕНИЙ НАСТОЯЩЕГО СОГЛАШЕНИЯ ОГРАНИЧИВАЕТСЯ СУММОЙ, ФАКТИЧЕСКИ УПЛАЧЕННОЙ ВАМИ ЗА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. НАСТОЯЩИЕ ОГРАНИЧЕНИЯ НЕ МОГУТ БЫТЬ ИСКЛЮЧЕНЫ ИЛИ ОГРАНИЧЕНЫ В СООТВЕТСТВИИ С ПРИМЕНИМЫМ ПРАВОМ.

6. Программные продукты

6.1. Технология третьих лиц, которая может быть целесообразна или необходима для использования в составе ПО определена в Документации к Системе. Такая технология лицензируется конечному пользователю на условиях лицензионного соглашения третьего лица, определенного в Документации к Системе. Такое лицензионное соглашение третьего лица дополняет положения настоящего Соглашения.

6.2. Входящие в состав Системы программные продукты лицензированы для ограниченного использования только в составе Системы. По истечении срока лицензионного использования ПО, пользователь обязан прекратить использование ПО и уничтожить все имеющиеся копии.

7. Открытое (свободное) программное обеспечение

Данный продукт может содержать программы, которые лицензируются (или сублицензируются) Пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду ("ПО с открытым исходным кодом"). Если такая лицензия предусматривает предоставление исходного кода пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса Правообладателю или сопровождается с продуктом. Если какая-либо лицензия на ПО с открытым исходным кодом требует, чтобы Правообладатель предоставлял права на использование, копирование или модификацию ПО с открытым исходным кодом, выходящие за рамки прав, предоставляемых настоящим Соглашением, такие права имеют преимущественную силу над правами и ограничениями, оговоренными в настоящем Соглашении.

8. Права на интеллектуальную собственность

8.1. Вы соглашаетесь с тем, что ПО, документация, как и все другие объекты авторского права, а также системы, идеи и методы работы, другая информация, которая содержится в ПО, товарные знаки являются объектами интеллектуальной собственности Правообладателя или его Партнеров. Данное Соглашение не дает Вам никаких прав на использование объектов интеллектуальной собственности, включая товарные знаки и знаки обслуживания Правообладателя или его Партнеров, за исключением прав, предоставленных настоящим Соглашением.

8.2. Вы соглашаетесь с тем, что исходный код, лицензионный ключ для ПО являются собственностью Правообладателя или его соответствующих контрагентов.

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

9. Контактная информация Правообладателя

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

9.2 Лицензии третьих сторон

При создании Системы были использованы разработки третьих сторон, распространяемые на условиях лицензии MIT (http://www.opensource.org/licenses/mit-license.html):

- Lua – http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

Также использовалось программное обеспечение:

- распространяемое на условиях лицензий BSD (http://www.opensource.org/licenses/bsd-license.php):
  - Stringencoders – http://code.google.com/p/stringencoders/
- распространяемое на условиях GNU GENERAL PUBLIC LICENSE (http://www.gnu.org/licenses/gpl-2.0.html):
  - Pdftotext – http://www.foolabs.com/xpdf/
  - Tnef – http://sourceforge.net/projects/tnef/
  - Unzip – http://www.info-zip.org/UnZip.html
  - libcole.so – arturo@directmail.org; andy.scriven@research.natpower.co.uk
  - libhtmltree.so – pauljlucas@mac.com