

INFOWATCH

InfoWatch Traffic Monitor

Руководство пользователя

05/10/2023

СОДЕРЖАНИЕ

1 Обзор InfoWatch Traffic Monitor 9
1.1 Перехват объектов 11
1.2 Анализ объекта и вынесение решения по объекту 13
1.3 Ретроспективный анализ данных, решение пользователя по объекту 16
1.4 Транспортные режимы InfoWatch Traffic Monitor 17
1.5 Загрузка объекта в базу данных 18
1.6 Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов 18
2 Работа в консоли управления Traffic Monitor: общие принципы 20
2.1 Работа Системы до конфигурирования 21
2.2 Работа с конфигурацией Системы 22
2.3 Отображение актуальных данных в Консоли управления 24
3 Интерфейс Консоли управления Traffic Monitor 25
3.1 Раздел "Сводка" 28
3.1.1 Виджеты сводки 29
Динамика нарушений за период 30
Топ нарушителей 30
Количество нарушений за период 32
Подборка 32
Динамика статусов за период 33
Статистика по политикам 34
Статистика по объектам защиты 34
Статистика по каталогам объектов защиты 36
3.1.2 Выгрузка сводки 36
3.2 Раздел "События" 38
3.2.1 Запросы 39
Обычный режим создания запроса 42
Расширенный режим создания запроса 51
Поиск по тексту события 52
3.2.2 Объекты перехвата 54
Плитка события 57
Табличное представление событий 57
Краткая форма просмотра событий 59
Детальная форма просмотра событий 61

3.2.3 Идентификация контактов в событии ... 64
3.3 Раздел "Отчеты" ... 65
3.3.1 Форма создания отчета ... 66
3.3.2 Виджеты отчетов ... 67
3.3.3 Запросы ... 70
3.4 Раздел "Технологии" ... 72
3.4.1 Категории и термины ... 73
Категории ... 73
Термины ... 74
3.4.2 Текстовые объекты ... 76
Шаблоны текстовых объектов ... 77
3.4.3 Эталонные документы ... 79
Автоматические эталонные документы ... 80
3.4.4 Бланки ... 81
3.4.5 Печати ... 83
3.4.6 Выгрузки из БД ... 83
Автоматически обновляемые выгрузки из БД ... 86
3.4.7 Графические объекты ... 87
3.4.8 Автолингвист ... 89
3.5 Раздел "Объекты защиты" ... 90
3.5.1 Элементы технологий ... 91
3.5.2 Условия обнаружения ... 92
3.6 Раздел "Персоны" ... 96
3.6.1 Персоны ... 98
3.6.2 Компьютеры ... 100
3.6.3 Снимки экрана ... 101
3.7 Раздел "Политики" ... 101
3.7.1 Правила и форма их просмотра ... 103
Правило передачи ... 105
Правило копирования ... 106
Правило хранения ... 108
Правило работы в приложениях ... 109
Правило контроля персон ... 110
Правило файловых операций ... 110
3.8 Раздел "Списки" ... 111
3.8.1 Теги ... 112
3.8.2 Веб-ресурсы ... 112
3.8.3 Статусы ... 113
3.8.4 Периметры ... 114
3.8.5 Файловые типы ... 115
3.9 Раздел "Управление" ... 116

4 Решение задач при работе в консоли Traffic Monitor 118
4.1 Типовые действия 118
4.1.1 Вход в Консоль управления 119
4.1.2 Применение конфигурации Системы 119
4.1.3 Редактирование элемента 121
4.1.4 Удаление элемента 121
4.1.5 Навигация по страницам 121
4.1.6 Изменение пароля пользователя 122
4.1.7 Выбор языка интерфейса 123
4.1.8 Вызов справки 123
4.1.9 Просмотр сведений о Системе 123
4.2 Работа с персонами и компьютерами 123
4.2.1 Создание группы персон и компьютеров 124
4.2.2 Создание персон и компьютеров 126
4.2.3 Экспорт и импорт персон 127
Особенности экспорта и импорта организационной структуры 127
4.2.4 Настройка карточки персоны 128
Добавление контакта персоне 128
Добавление компьютера для персоны 130
Добавление персоны в группу 130
4.2.5 Настройка карточки компьютера 131
Добавление компьютеру контакта 131
Добавление персоны для компьютера 131
Добавление компьютера в группу 132
4.2.6 Назначение статуса персонам и компьютерам 132
4.2.7 Просмотр снимков экрана 133
4.3 Работа со справочниками 135
4.3.1 Работа с тегами 136
4.3.2 Работа с веб-ресурсами 136
4.3.3 Работа со статусами 137
4.3.4 Работа с периметрами 138
4.4 Работа с базой технологий 142
4.4.1 Определение конфиденциальной информации 143
Работа с категориями и терминами 145
Работа с текстовыми объектами 148
Работа с эталонными документами 151
Работа с бланками 154
Работа с печатями 156
Работа с выгрузками 157
Работа с графическими объектами 162
Работа с Автолингвистом 164

4.4.2 Экспорт и импорт базы технологий ... 166
4.5 Работа с объектами защиты ... 168
4.5.1 Создание каталога объектов защиты ... 169
4.5.2 Создание объекта защиты ... 169
4.5.3 Добавление элементов технологий ... 179
4.5.4 Добавление условий обнаружения ... 180
4.5.5 Создание политики для объектов защиты и их каталогов ... 182
4.5.6 Импорт и экспорт объектов защиты ... 183
4.5.7 Активация и деактивация объектов защиты ... 184
4.6 Работа с объектами перехвата ... 185
4.6.1 Просмотр сводки по нарушениям/нарушителям ... 186
Создание панели ... 187
Создание и настройка виджета ... 188
Создание выгрузки сводки ... 189
Просмотр выгрузки сводки ... 191
4.6.2 Просмотр событий ... 192
Создание запросов ... 192
Выбор полей просмотра событий ... 205
Просмотр краткой формы события ... 206
Просмотр детальной формы события ... 207
4.6.3 Вынесение решения по объекту ... 208
4.6.4 Добавление и удаление тега ... 209
4.6.5 Сохранение события (для SMTP-писем) ... 209
4.6.6 Выгрузка событий ... 209
4.6.7 Досылка события, находящегося в карантине ... 212
4.7 Настройка реакций Системы ... 213
4.7.1 Общие сведения о политиках ... 214
4.7.2 Предустановленные политики ... 223
Политики защиты конфиденциальных данных ... 223
Политика контроля персон ... 225
Политика, регулирующая передачу данных, защищенных паролем ... 225
Политики, контролирующие посещение веб-ресурсов ... 226
Политика, исключающая из перехвата почтовые рассылки ... 228
4.7.3 Создание политики защиты данных ... 229
Примеры использования политики защиты данных ... 230
4.7.4 Создание политики защиты данных на агентах ... 233
4.7.5 Создание политики контроля персон ... 236
4.7.6 Создание правил ... 238
4.7.7 Определение действий Системы в случае нарушения правил ... 239
4.7.8 Настройка уведомлений в правилах ... 242
4.7.9 Определение действий Системы по умолчанию ... 243
4.7.10 Фильтрация списка политик ... 244
4.7.11 О политике защиты данных на агентах ... 245

4.7.12 О политике защиты данных ... 246
4.7.13 О политике контроля персон ... 246
4.8 Работа с отчетами ... 247
4.8.1 Создание и просмотр отчетов ... 248
Создание папки с отчетами ... 250
Создание отчета ... 251
Создание и настройка виджета ... 253
Просмотр готовых отчетов ... 254
4.8.2 Примеры использования отчетов ... 255
4.9 Управление Системой ... 260
4.9.1 Управление интеграцией с LDAP каталогами ... 261
Создание подключения к серверу ... 261
Редактирование подключения к серверу ... 265
Удаление подключения к серверу ... 266
Запуск синхронизации с сервером вручную ... 266
4.9.2 Управление пользователями Системы и их ролями ... 267
Пользователи ... 267
Роли ... 271
Области видимости ... 273
4.9.3 Управление лицензиями ... 277
Проверка валидности лицензии ... 278
Установка лицензии ... 278
Удаление лицензии ... 279
Запрос лицензии ... 279
4.9.4 Состояние системы ... 279
Настройка уведомлений ... 281
4.9.5 Сбор диагностических данных, сохранение логов служб ... 281
4.9.6 Аудит действий пользователя ... 283
События аудита ... 284
Фильтрация и поиск ... 285
4.9.7 Контроль целостности ... 285
Ручная проверка целостности ... 285
Автоматическая проверка целостности ... 286
Принятие результата за эталонный ... 286
4.9.8 Плагины ... 286
Добавление плагина ... 289
Удаление плагина ... 289
Работа с токенами ... 290
4.9.9 Настройка подключения к почтовому серверу ... 291
4.9.10 Настройка уведомлений ... 292
Создание уведомления ... 293
Тестирование уведомления ... 295

Предустановленные уведомления 295

5 Лицензионная информация 297

5.1 Пользовательское лицензионное соглашение 297

6 Глоссарий 300

1 Обзор InfoWatch Traffic Monitor

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

Ниже перечислены основные функции, выполняемые системой InfoWatch Traffic Monitor.

> **Примечание:**
>
> В зависимости от операционной системы, установленной на сервере, различается набор поддерживаемых функций (подробнее см. статью базы знаний "О различиях в функциональности в зависимости от используемой ОС").

Основные функции InfoWatch Traffic Monitor:

- Перехват SMTP, IMAP и POP3-трафика. Возможен перехват трафика (или копии трафика), передаваемого через почтовый relay-сервер; перехват копии трафика, проходящего через управляемый коммутатор.
- Перехват HTTP- и HTTPS-трафика. Возможен перехват трафика, передаваемого через прокси-сервер, поддерживающий ICAP-протокол; перехват копии трафика, проходящего через управляемый коммутатор.

  > **Примечание:**
  >
  > Перехват HTTPS-трафика возможен при интеграции с прокси-сервером Blue Coat, если прокси-сервер обрабатывает HTTPS-трафик как HTTP-трафик.

- Перехват копии ICQ-трафика (протокол OSCAR), проходящего через управляемый коммутатор. При подключении ICQ через HTTP Система перехватывает ICQ-трафик аналогично HTTP-трафику.

  > **Важно!**
  >
  > Система не поддерживает перехват и анализ зашифрованного ICQ-трафика, в том числе трафика, передаваемого по зашифрованному протоколу SSL.

- Анализ Skype-трафика, теневых копий файлов и заданий на печать, передачи трафика по протоколам HTTP, HTTPS и FTP, загрузки данных в облачные хранилища по протоколу HTTPS, приема и передачи электронных писем по протоколам SMTP, POP3, IMAP, Outlook, контроль обмена данными через Jabber (протокол XMPP), Telegram, WhatsApp (десктопная версия). Также поддерживается перехват голосового трафика в Skype. Перехват перечисленных данных осуществляется системой InfoWatch Device Monitor.
- Перехват и анализ объектов MS Lync при помощи IW Lync Adapter, который устанавливается на MS Lync сервер.
- Анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности.
- Фильтрация перехваченного трафика путем выдачи разрешения/запрещения на доставку определенных данных.

Важно!

Функция недоступна при работе с копией трафика.

Состав InfoWatch Traffic Monitor:

Компонент InfoWatch Traffic Monitor	Назначение компонента
Сервер Traffic Monitor	**IW_SNIFFER**, **IW_ICAP** и **IW_SMTPD** - перехватчики. **Подсистема анализа**: получение контекста события и проверка на содержание элементов технологий и на соответствие объектам защиты. **Подсистема применения политик**: выполнение действий, заданных пользователем согласно корпоративной политике безопасности.
База данных	Хранение информации, связанной с работой Системы (перехваченные данные и результаты их анализа).
Device Monitor	Взаимодействует с рабочими станциями. Контроль доступа пользователей к периферийным устройствам, мониторинг операций (копирование данных с/на съемные носители, сетевые ресурсы и FTP, отправка данных на печать, использование мессенджеров), контроль передачи данных через буфер обмена и перехват трафика систем мгновенного обмена сообщениями.
Коннекторы	Интеграция со сторонними системами, формирование событий.
Консоль управления	Настройка правил анализа и фильтрации трафика, анализ полученных данных.

Действующие лица

Действующие лица в Системе разделены на два типа:

- **Контролирующие**
  Офицер безопасности - лицо (или несколько лиц), в обязанности которого входит формирование политик безопасности, заведение правил, расследование инцидентов по нарушениям. Также ОБ занимается администрированием Системы, составлением отчетов и т.д.
- **Контролируемые**
  Персоны - все лица организации, входящие в ее периметр. В случае нарушения политик, правил персона становится *Отправителем события* и попадает в поле зрения ОБ.

Функциональные возможности

Функционал Системы позволяет контролировать два направления:

- Устройства (рабочие станции, периферия, съемные носители и т.д.);
- Трафик по каналам связи (почта, мессенджеры, внешние ресурсы и т.д.).

Для контроля данных направлений используются перехватчики.

Описание базовых принципов работы Системы содержится в следующих вводных разделах:

- Перехват объектов;
- Транспортные режимы InfoWatch Traffic Monitor;
- Анализ объекта и вынесение решения по объекту;
- Загрузка объекта в базу данных;
- Ретроспективный анализ данных, решение пользователя по объекту;
- Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов;
- Функции InfoWatch Device Monitor (подробнее см. *"InfoWatch Device Monitor. Руководство пользователя"*).

1.1 Перехват объектов

Под *объектами* в Системе понимаются:

- объекты трафика (SMTP-, IMAP4- и POP3-письма, HTTP- и HTTPS-запросы, ICQ-сообщения, Skype (сообщения и голос), XMPP, MS Lync, Telegram, Facebook, WhatsApp (десктопная версия), VK (ВКонтакте));
- теневые копии файлов;
- задания на печать.

Важно!

В таблице приведен общий список типов объектов перехвата для всех поддерживаемых ОС. Более точная информация находится в соответствующих разделах:

- ОС Red Hat Enterprise Linux - смотрите документ "InfoWatch Traffic Monitor. Руководство администратора", раздел "Перехват трафика в потоке/на шлюзе";
- ОС Astra Linux - смотрите документ "InfoWatch Traffic Monitor. Руководство администратора", раздел "Функции InfoWatch Traffic Monitor".

Также рекомендуется ознакомиться со статьей в базе знаний о различиях в функциональности Traffic Monitor и Device Monitor в зависимости от используемой ОС.

Возможно несколько вариантов перехвата в зависимости от типа объектов:

Тип объекта	Варианты перехвата объектов
SMTP, IMAP и POP3	• Система выполняет перехват и доставку SMTP-, IMAP- и POP3-трафика. Возможна фильтрация перехваченных объектов (разрешение/запрещение доставки). • Система получает копию SMTP-, IMAP- и POP3-трафика от корпоративного почтового relay-сервера. Система не участвует в доставке трафика.

Тип объекта	Варианты перехвата объектов
	• Система получает копию SMTP-, IMAP- и POP3-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. • Система получает копию HTTP-трафика, проходящего через коммутатор, оборудованный SPAN-портом. Перехват копии осуществляется посредством Sniffer. Система не участвует в доставке трафика.
HTTPS	Система получает копию трафика от InfoWatch Device Monitor.
Outlook	Система получает копию трафика от InfoWatch Device Monitor.
FTP	Система получает копию трафика от InfoWatch Device Monitor.
ICQ (OSCAR)	• 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 мессенджеров	Система получает копию трафика Skype (в том числе голосовой трафик), Telegram, Facebook, VK (ВКонтакте), WhatsApp (десктопная версия) от InfoWatch Device Monitor.
MS Lync	Система получает копию объектов от lW Lync Adapter, установленного на сервере MS Lync.
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.

Варианты перехвата и последующая доставка объектов определяются транспортными режимами InfoWatch Traffic Monitor.

1.2 Анализ объекта и вынесение решения по объекту

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

Подсистема IW TM	Модули подсистемы	Функции подсистемы/модуля
Подсистема Обработки	Модуль Обработки SMTP- и POP3-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 • Извлечение текстовой информации из eml-файлов, в том числе в виде вложений • Передача извлеченных текстов в Подсистему Анализа
Подсистема Анализа	Модуль Лингвистического Анализа	Проверка текста на соответствие 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
	Модуль Детектирования Бланков	Поиск бланков в тексте объектов
	Модуль Детектирования Печатей	Поиск изображений печатей в тексте объектов
	Модуль Детектирования Выгрузок из БД	Поиск цитат из базы данных в тексте событий
	Модуль Детектирования Графических Объектов	Поиск изображений, принадлежащих определенным классам, в тексте и вложениях объектов

Подсистема IW TM	Модули подсистемы	Функции подсистемы/модуля
	Модуль Автолингвист	Проверка текста на соответствие категориям с помощью обученного классификатора
Подсистема Применения Политик	Модуль Интеграции с Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro и FreeIPA	Обеспечение первоначального импорта и периодической синхронизации структуры каталога Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro и FreeIPA со справочником персон и компьютеров для выполнения дальнейшей привязки этой информации к данным из перехваченных объектов
	Модуль Принятия Решений	Обеспечение корпоративной политики безопасности путем выполнения для объектов правил из набора политик

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. Перечень возможных атрибутов объекта приведен в статье "Плитка события".
2. **Извлечение вложенных файлов** – Модуль Принятия Решений анализирует вложенные файлы на основании таких атрибутов, как название и формат файла.
3. **Анализ текста и графических объектов** – Подсистема Анализа обрабатывает текстовые и графические данные: тексты писем, сообщений, запросов; тексты, извлеченные из вложений поддерживаемых форматов, а также файлы изображений.

> **Примечание:**
>
> Извлечение и анализ текстовых данных возможен для документов MS Office 2003, 2007 и выше.

> **Примечание:**
>
> Возможен анализ названий и значений свойств, которые извлекаются агентом Device Monitor из PDF-документов (подробнее см. *Пример 3* в статье "Работа с текстовыми объектами").

В Системе предусмотрены несколько видов анализа, доступность которых зависит от приобретенной 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 основе базы категорий и терминов, отражающих 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.)
Детектирование бланков	Поиск бланков установленного шаблона. Бланками могут быть различные анкеты, квитанции и проч.
Детектирование паспортов граждан РФ	Поиск изображений паспортов граждан РФ. Технология работает при включенном текстовом объекте *Паспорт гражданина РФ*
Детектирование печатей	Поиск изображения печати установленного вида. Печатями могут быть изображения круглых и треугольных оттисков, которые используются в организациях
Детектирование выгрузок из БД	Поиск цитат из заданной базы данных. Выгрузками из БД могут быть списки заработных плат сотрудников, другие личные данные и проч.
Детектирование графических объектов	Поиск изображений, соответствующих какой-либо из предустановленных категорий. К графическим объектам относятся изображения паспортов, кредитных карт и проч.
Автолингвист	Определение категории текста с помощью обученного классификатора. Обучение автоматического классификатора производится на типовых текстовых

	документах. Примеры категорий Автолингвиста: *Бухгалтерия*, *Договоры и контракты*, *Маркетинг*.

- На основании результатов анализа Модуль Принятия Решений выносит заключение о возможном нарушении политики информационной безопасности и определяет, какие действия должны быть выполнены в случае нарушения. Правила, определяющие действия Системы в случае нарушения, задаются в политике. Предусмотрены следующие действия (набор возможных действий определяется типом правила):
  - **Назначить событию уровень нарушения**. Возможные значения: **Высокий**, **Средний**, **Низкий**, **Отсутствует**.
  - **Назначить персонам статус**. Статус, который будет присвоен нарушителям (подробнее см. "Статусы").
  - **Назначить событию теги**. Теги, которые будут назначены событию в случае нарушения политики (подробнее см. "Теги").
  - **Назначить событию вердикт**. Решение Системы, является ли событие потенциальным нарушением. Возможные значения: **Разрешить**, **Заблокировать**, **Поместить на карантин**.
  - **Удалить событие**. Событие не будет сохранено в базу данных.

> **Примечание:**
>
> При детектировании файлов некоторых форматов, таких как **xls**, **pdf**, **jpg**, **docx**, возможно:
>
> - некорректное срабатывание политики "Склейка файлов". Подробнее см. в статье в базе знаний «Перехваченные файлы некорректно определяются как склеенные»;
>
> - некорректные детектирование формата и извлечение данных из файла или полная их невозможность, если структура перехваченного файла не соответствует спецификации формата (например, плавающая сигнатура формата, которая может располагаться не в начале файла). Подробнее см. в статье в базе знаний "Не детектируется формат файла, и не происходит распаковка".

1.3 Ретроспективный анализ данных, решение пользователя по объекту

Объекты, хранящиеся в базе данных, доступны для анализа в Консоли управления. При этом 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 нарушения*. Пользователь проанализировал объект и пришел к выводу, что объект не нарушает корпоративную политику безопасности.
- *Решение не принято*. Пользователь проанализировал объект и не пришел к выводу, нарушает ли объект корпоративную политику безопасности.
- *Требуется дополнительный анализ*. Пользователь проанализировал объект и решил, что для принятия решения требуются дополнительные действия.

В результате решения пользователя также может измениться вердикт, вынесенный событию Системой (см. "Вынесение решения по объекту"), и статус отправки SMTP-письма (см. "Досылка события, находящегося в карантине").

> **Примечание:**
>
> При работе системы "*В разрыв*" при назначении вердикта *Разрешено*, письмо покидает периметр компании вне зависимости от дальнейшего редактирования решения.

1.4 Транспортные режимы InfoWatch Traffic Monitor

Система InfoWatch Traffic Monitor имеет два транспортных режима: *Копия* и *Блокировка*. Условия, в соответствии с которыми определяется транспортный режим, задаются при настройке перехватчиков (подробнее см. документ *"Infowatch Traffic Monitor. Руководство администратора"*. Действия, связанные с транспортировкой объекта, выполняются с учетом выбранного транспортного режима.

В таблице 1 приведены допустимые транспортные режимы для объектов разного типа. Различие между режимами работы заключается в особенностях транспортировки объектов (см. таблицу 2).

Табл. 1

Транспортный режим	Описание
Блокировка	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. "Досылка события, находящегося в карантине").
Копия	В данном режиме Система получает копии объектов. Отличие режима *Копия* от режима *Блокировка* заключается в том, что транспортировка объектов выполняется без участия Системы. Таким образом, задачей Системы является только анализ объектов. Поскольку анализ выполняется для копии объекта, то вердикт и решение пользователя, вынесенные по результатам анализа, не оказывают влияния на доставку этого объекта получателям.

Табл. 2

Тип объекта	Транспортный режим "Блокировка"	Транспортный режим "Копия"
SMTP	Да	Да (для копии трафика, полученной от почтового relay-сервера или от Sniffer)
HTTP-запрос	Да (только при перехвате трафика по протоколу ICAP)	Да

Тип объекта	Транспортный режим "Блокировка"	Транспортный режим "Копия"
ICQ-сообщение	Нет	Да (только для копии трафика, полученной от Sniffer)
Сообщение Skype, Jabber, Telegram, WhatsApp	Нет	Да
MS Lync	Нет	Да
Теневая копия файла	Нет	Да

1.5 Загрузка объекта в базу данных

После того как объект проанализирован и по нему принято решение Системы (подробнее см. "Анализ объекта и вынесение решения по объекту"), 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 объекта;
- результаты анализа объекта;
- информацию о решении по объекту.

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

Если в транспортном режиме *Блокировка* (см. "Транспортные режимы InfoWatch Traffic Monitor") Система принимает решение о блокировке HTTP-запроса или письма, отправляемого с помощью веб-сервиса (например, *mail.ru*), то в браузере пользователя, отправившего запрос или письмо, отобразится сообщение 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. "Объекты перехвата") 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.

Перехват HTTP/HTTPS-запросов поддерживает форумы на базе IP Board, phpBB и vBulletin.

Поддерживаемые веб-ресурсы:

Тип веб-ресурса	Ресурсы	
	Без ограничений	С ограничениями
Веб-почта	mail.ru, mail.yandex.ru, rambler.ru, pochta.ru, km.ru, newmail.ru, inbox.com, hotmail.com, hotmail.ru, live.com	gmail.com, yahoo.com, mail.com, aol.com, gmx.com
Интернет-дневники и социальные сети	blogs.mail.ru, liveinternet.ru (li.ru), my.ya.ru, diary.ru, blogspot.com (blogger.com), loveplanet.ru/a-journal, myspace.com, perfspot.com	facebook.com, myspace.com, blogger.com, vkontakte.ru (vk.com), odnoklassniki.ru, twitter.com, livejournal.com (.ru), wordpress.com, linkedin.com
Сайты поиска работы и размещения резюме		moikrug.ru, hh.ru, job.ru, rabota.ru, jobs.com, eurojobs.com
Форумы	forum.ru-board.com, sysadmins.ru, talk.mail.ru, dom.bankir.ru, biznet.ru	forum.ixbt.com, groups.google.ru (.com)

Также поддерживаются следующие файловые хранилища и хостинги**:**

- blogspot,
- box.net,
- cloud.mail.ru,
- disk.yandex.ru,
- file.qip.ru,
- google drive,
- google plus,
- mail.qip.ru,
- onedrive.live.com,
- office365,
- talk.mail.ru.

2 Работа в консоли управления Traffic Monitor: общие принципы

Для работы в Консоли управления требуется наличие постоянного соединения с сервером базы данных. Чтобы подключиться к серверу базы данных, пользователю необходимо выполнить процедуру авторизации.

При 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, пользователь не сможет авторизоваться в Системе.

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

В зависимости от того, какая роль назначена учетной записи, от имени которой производится вход в Систему, пользователь может иметь разные права:

- Администратор - роль, имеющая все необходимые права для первичной настройки Консоли управления.
- Офицер безопасности (ОБ) - роль, обладающая всеми привилегиями, кроме первичной настройки Консоли управления.

> **Примечание:**
>
> Действия Администратора частично описаны в разделе "Управление Системой". Прочие сведения по первичной настройке Системы см. в документе «*Infowatch Traffic Monitor. Руководство администратора*».

При наличии других установленных продуктов InfoWatch, например, Vision, можно настроить сквозную аутентификацию между ними, чтобы быстро и безопасно переходить из одного в другой и обратно, не вводя при этом авторизационные данные. Описание настройки см. в документе "*Traffic Monitor. Руководство администратора*", раздел "*Настройка сквозной аутентификации между продуктами InfoWatch*".

После того, как вход выполнен, пользователь может сконфигурировать Систему (о работе Системы сразу после установки см. "Работа Системы до конфигурирования"). Конфигурация Системы состоит из следующих действий:

- настройка базы технологий;
- составление справочников;
- создание объектов защиты;
- настройка уведомлений;
- настройка политик, определяющих реакцию Системы на нарушения корпоративной политики безопасности.

Настройка конфигурирования Системы завершается применением обновленной конфигурации (см. "Работа с конфигурацией Системы").

> **Примечание:**

Если Система уже сконфигурирована ранее, и задачи пользователя обеспечиваются примененной конфигурацией, дополнительного конфигурирования Системы не требуется.

Список типовых действий пользователя приведен в разделе "Решение задач при работе в консоли Traffic Monitor". После завершения конфигурирования Системы офицер безопасности может просмотреть сводку о нарушениях правил корпоративной безопасности (см. "Работа с объектами перехвата").

Также пользователь имеет возможность настраивать внешний вид Консоли управления и выполнять другие задачи.

Если с Консолью управления одновременно работает несколько пользователей, то для получения актуальных данных следует применять обновление данных (см. "Отображение актуальных данных в Консоли управления").

Важно!

Для корректной работы Системы требуется, чтобы в антивирусных программах и другом блокирующем ПО не блокировался интернет-контент. Например, в антивирусе G DATA Security требуется снять флажок в поле **Process Internet content (HTTP)**.

2.1 Работа Системы до конфигурирования

Установленная Система, для которой еще не выполнялось конфигурирование (о конфигурировании Системы см. "Решение задач при работе в консоли Traffic Monitor"), функционирует следующим образом:

- Осуществляет перехват трафика и проверку объектов перехвата на соответствие установленным категориям. В случае соответствия объекта перехвата какой-либо категории, Система присваивает объекту соответствующий атрибут.

  Важно

  Если во время установки Системы была выбрана опция **Don't preinstall loadable technology settings** (позволяет не устанавливать базу элементов технологий), то для корректной работы анализа потребуется загрузить базу технологий (см. статью "Экспорт и импорт базы технологий").

- Позволяет пользователю войти в Систему, используя одну из предустановленных учетных записей:
  - **Administrator** (роль Администратор);
  - **Officer** (роль Офицер безопасности).
- Отображает в Консоли управления информацию об объектах перехвата. Чтобы отображать информацию об отправителях и получателях трафика, необходимо выполнить настройку списков персон и рабочих станций (см. "Работа с персонами и компьютерами").
- Сохраняет в базу данных объекты перехвата. При этом никаких действий по отношению к объектам в процессе анализа не предпринимается. Чтобы указать, какие действия требуется выполнять с объектами перехвата, необходимо настроить

периметр компании (см. "Работа с периметрами"). После этого при анализе объектов перехвата Система будет применять действия, заданные в политиках по умолчанию.

2.2 Работа с конфигурацией Системы

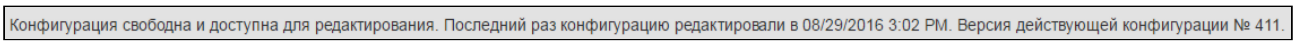
Конфигурация представляет собой набор настроек, необходимых для проверки объектов на сервере Traffic Monitor, а также для мониторинга и анализа данных.

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.

Важно!

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

Версия действующей конфигурации отображается в верхней части рабочей области.



Также на основе действующей конфигурации Система формирует версию конфигурации, которая затем распространяется на агенты Device Monitor.

Примечание.

Версия конфигурации, используемой в Device Monitor, отображается в консоли Device Monitor (см. "Синхронизация политик Traffic Monitor" в *"InfoWatch Device Monitor. Руководство пользователя"*). При необходимости вы можете сравнить номера версий в Traffic Monitor и Device Monitor и убедиться, что в Device Monitor используется актуальная версия.

Настройка конфигурации включает в себя:

- Составление базы технологий (см. "Настройка базы технологий"):
  - выбор терминов, подлежащих детектированию - только при использовании технологии **Лингвистический анализ** (см. "Термины");
  - выбор типов текстовых объектов, подлежащих детектированию - только при использовании технологии **Детектирование текстовых объектов** (см. "Текстовые объекты");
  - выбор эталонных документов, подлежащих детектированию - только при использовании технологии **Детектирование эталонных документов** (см. "Эталонные документы");
  - выбор бланков, подлежащих детектированию - только при использовании технологии **Детектирование бланков** (см. "Бланки");
  - выбор печатей, подлежащих детектированию - только при использовании технологии **Детектирование печатей** (см. "Печати");
  - выбор выгрузок из БД, подлежащих детектированию - только при использовании технологии **Детектирование выгрузок из БД** (см. "Выгрузки из БД");
  - выбор типов графических объектов, подлежащих детектированию - только при использовании технологии **Детектирование графических объектов** (см. "Графические объекты").

- Создание объектов защиты на основе элементов базы технологий (см. "Объекты защиты").
- Составление справочников:
  - персон и компьютеров (см. "Работа с персонами и компьютерами");
  - тегов (см. "Работа с тегами");
  - веб-ресурсов (см. "Работа с веб-ресурсами");
  - статусов (см. "Работа со статусами");
  - периметров (см. "Работа с периметрами").
- Добавление уведомлений о нарушении политики безопасности (см. "Настройка уведомлений").
- Настройка политик, в соответствии с которыми будет выполняться проверка объектов на сервере Traffic Monitor (см. " Настройка реакций Системы ").

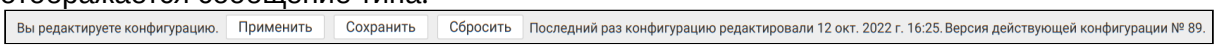
Примечание.

Конфигурация, передаваемая на Device Monitor, включает только следующие элементы:

- персоны и компьютеры;
- периметры;
- политики защиты данных на агентах;
- категории и текстовые объекты;
- объекты защиты, в составе которых есть только категории и текстовые объекты.

После того как хотя бы один из параметров конфигурации был изменен, редактируемая версия конфигурации сохраняется в Системе. При этом:

- в верхней части рабочей области браузера пользователя, изменяющего конфигурацию, отображается сообщение типа:



- в верхней части рабочей области браузера пользователей, которым недоступно изменение конфигурации, отображается сообщение типа:
  Конфигурация редактируется пользователем <security_officer> начиная с 15.06.2015 15:54

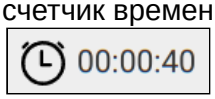
Важно!

До применения или сохранения конфигурации измененная версия доступна только пользователю, который ее изменяет. Другие пользователи Консоли управления работают с последней примененной конфигурацией Системы без права на ее изменение.

После завершения редактирования вы можете выбрать одно из действий:

- **Применить конфигурацию** (см. "Применение конфигурации Системы") – измененная конфигурация начнет действовать на сервере.
  Применение новой конфигурации может занять некоторое время. Длительность применения не превышает 3-х часов. В верхней части рабочей области отображается

счетчик времени, прошедшего с начала применения конфигурации:



Вы можете отредактировать конфигурацию и применить ее, даже если другая конфигурация находится в процессе применения. В этом случае применение конфигурации будет прервано, начнется применение отредактированной конфигурации.

- **Сохранить конфигурацию** – измененная конфигурация станет доступна другим пользователям Консоли управления, но не будет использоваться в Системе для контроля трафика и анализа данных.
- **Сбросить изменения** – конфигурация в Консоли управления будет соответствовать последней примененной на сервере конфигурации, и все сделанные изменения конфигурации удалятся. Для отмены изменений нажмите **Сбросить** в появившемся окне списка изменений. В поле **Описание** при необходимости укажите причину отмены изменений. Эта информация будет сохранена в базе данных.

При интеграции с LDAP-каталогами, а также при добавлении новых контактов персон с помощью механизма пост-идентификации происходит автоматическое редактирование конфигурации. Обновление конфигурации выполняется независимо от ее текущего статуса.

Примечание.

Информация о контактах, добавленных в результате пост-идентификации, обновляется в Системе раз в 15 минут.

2.3 Отображение актуальных данных в Консоли управления

В Системе могут одновременно работать несколько пользователей. При этом каждому пользователю, работающему в Консоли управления, доступны данные из последней примененной конфигурации (см. "Применение конфигурации Системы"), а также изменения, сделанные данным пользователем за текущую сессию редактирования конфигурации.

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. Вы можете также настроить обновление статистических данных о нарушениях/нарушителях.

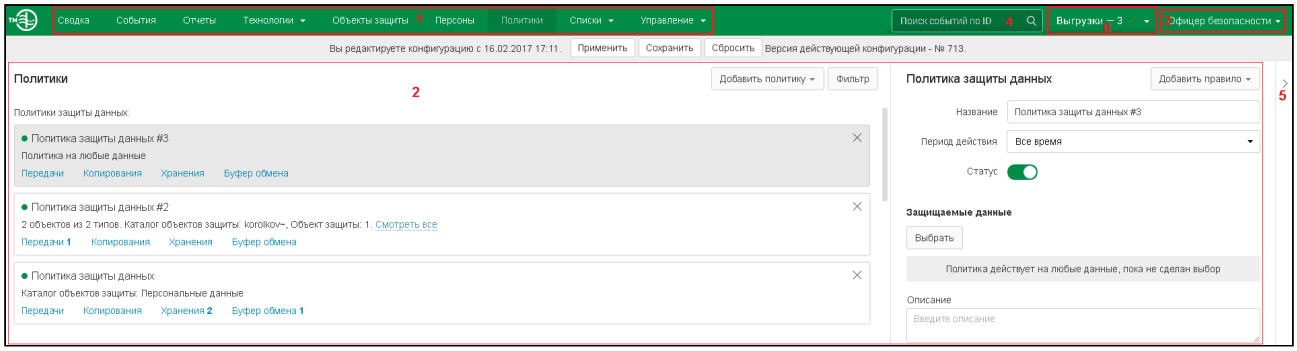
В любом из разделов Консоли управления вы также можете обновлять данные вручную. Для этого воспользуйтесь стандартным средством обновления страницы интернет-браузера (по умолчанию обновление выполняется при нажатии функциональной клавиши F5).

Примечание:

В тех случаях, когда запрашиваемые данные находятся в процессе загрузки, в Системе может отображаться символ вида  либо информационное сообщение.

3 Интерфейс Консоли управления Traffic Monitor

Все окна Консоли управления InfoWatch Traffic Monitor имеют ряд общих элементов.



Элементы окна Консоли управления:

Номер на схеме	Элемент окна консоли	Назначение элемента
1	Панель Навигации	Отображение кнопок разделов. При нажатии на кнопку раздела выполняется переход к выбранному разделу Консоли управления.
2	Рабочая область	Отображение элементов выбранного раздела Консоли управления, работа с элементами выбранного раздела.
3	Кнопка меню пользователя	Отображение имени пользователя. При нажатии раскрывается список, в котором пользователь может: • Сменить пароль своей учетной записи (см. "Изменение пароля пользователя") • Сменить язык интерфейса (см. "Выбор языка интерфейса ") • Вызвать справку по Системе (см. "Вызов справки") • Получить сведения о Системе (см. "Просмотр сведений о Системе") • Выполнить выход из Консоли управления (см. "Вход в Консоль управления")
4	Поле поиска событий по ID	Отображается во всех разделах Консоли. Позволяет найти нужные события по их ID. Если поиск осуществляется не из раздела "События", будет выполнен переход в раздел "События", где показаны результаты поиска.

5	Кнопка скрытия панели	Отображается в разделах, где рабочая область разделена на панели (например, список событий на панели в левой части рабочей области и информация о выбранном событии в правой). Позволяет скрыть панель для более удобного просмотра информации на других панелях. Повторное нажатие на кнопку (стрелочка при этом будет указывать в обратную сторону) восстанавливает скрытую панель.
6	Кнопка просмотра информации о выгрузках	Отображается, если в Системе содержатся выгрузки событий или сводки либо запущена генерация выгрузки. При нажатии на кнопку отображается информация о сформированных выгрузках сводки и событий, а также выгрузках событй, которые формируются в данный момент. Подробнее о выгрузках см. "Просмотр выгрузки сводки" и "Выгрузка событий".

Работа в Консоли управления ведется в тематических разделах:

Раздел	Назначение
Сводка	Раздел содержит статистическую информацию о нарушениях /нарушителях
События	Раздел содержит список объектов перехвата и средства для работы с ними
Отчеты	Раздел содержит выборку статистических данных о перехваченных объектах
Технологии	Раздел содержит описание используемых технологий анализа (категории и термины, текстовые объекты, эталонные документы и т.д.)
Объекты защиты	Раздел содержит список объектов защиты и средства для работы с ними
Персоны	Раздел содержит справочник персон и рабочих станций информационной системы организации, а также внешних контактов.
Политики	Раздел содержит список предполагаемых действий персон и алгоритм ответных действий Системы

Раздел	Назначение
Списки	Раздел содержит редактируемые справочники тегов, ресурсов, статусов и периметров
Управление	Раздел позволяет выполнить первичную настройку Системы, просматривать события аудита и настраивать отправку уведомлений

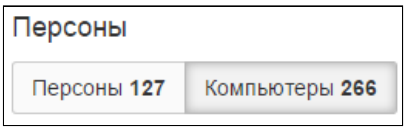
Переход к разделу происходит после нажатия на кнопку раздела.



Кнопка раздела **События**

В Консоли управления используются следующие элементы интерфейса:

- **Вкладка** - позволяет в одном окне переключение между несколькими определенными наборами элементов интерфейса.



Раздел **Персоны**, вкладки **Персоны** и **Компьютеры**

- **Панель** - область интерфейса, отображающая набор данных или содержащая набор элементов интерфейса, и отделенная от остальных областей.

> **Примечание:**
>
> Также *Панелью* в Системе называется сущность раздела **Сводка** (см. "Раздел Сводка").



Панель инструментов

- **Часть рабочей области** - фрагмент рабочей области, обособленный от другого при помощи разделительной вертикальной линии.
- **Плитка** - весь набор данных для одной записи (все атрибуты объекта) в виде отдельного объекта.



Раздел **События**, плитка события

Вы можете настраивать интерфейс Консоли управления (подробную информацию см. в тематических разделах).

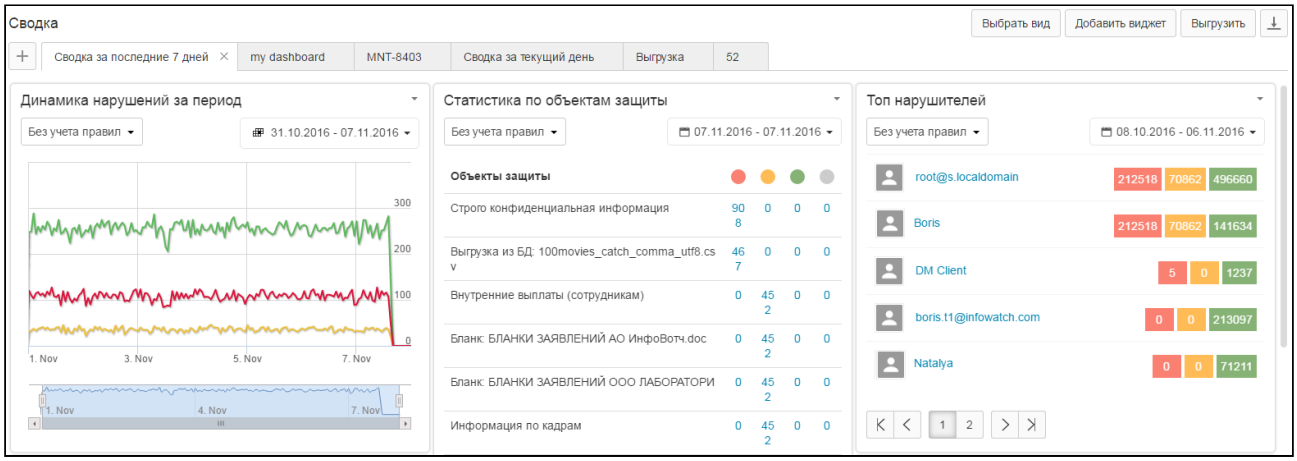
> **Примечание:**
>
> В тех случаях, когда запрашиваемые данные находятся в процессе загрузки, в Системе может отображаться символ вида  либо информационное сообщение.

3.1 Раздел "Сводка"

О разделе:

Раздел содержит статистическую информацию о нарушениях/нарушителях. Информация отображается на виджетах. Для эргономичного использования рабочей области виджеты располагаются на панелях (вкладках). Панели позволяют группировать виджеты, объединенные общей тематикой.

Виджеты удобно использовать для ежедневного мониторинга, так как они позволяют быстро просмотреть статистику по событиям.



С помощью кнопки **Выбрать вид** вы можете выбрать способ отображения виджетов на панели. Возможные варианты:

-  – деление на 3 равные части;
-  – деление в отношении 2:1;
-  – деление на 2 равные части;
-  – деление в отношении 1:2.

> **Примечание.**
>
> Для каждой панели вид выбирается отдельно.

Для добавления виджета на панель используется кнопка **Добавить виджет** в левом верхнем углу рабочей области (подробнее см. "Создание и настройка виджета").

Кнопка **Выгрузить** позволяет перейти к формированию выгрузки сводки в формате PDF или HTML (подробнее см. "Выгрузка сводки"). Для просмотра списка ранее сформированных выгрузок используется кнопка .**Действия пользователя:**

- настройка панелей и виджетов для отображения информации о нарушениях/нарушителях (см. "Создание панели" и "Создание и настройка виджета")
- просмотр информации о нарушениях/нарушителях (см. "Просмотр событий")
- формирование выгрузки сводки (см. "Создание выгрузки сводки")

3.1.1 Виджеты сводки

Рабочая область раздела **Сводка** содержит панели, на которых расположены виджеты.

Виджеты содержат статистическую информацию по нарушениям/нарушителям. Внешний вид и параметры работы виждета определяются его типом.

Назначение различных типов виджетов и ссылки на их подробное описание приведены в таблице:

Виджет	Описание
Динамика нарушений за период	Количественные изменения по выбранным типам нарушений за выбранный период времени
Топ нарушителей	Список наиболее отличившихся нарушителей по выбранной группе за выбранный период времени
Количество нарушений за период	Для каждого из типа нарушений (передачи, размещения, копирования на съемные носители) отображается количество нарушений высокого, среднего, низкого уровня за выбранный период времени
Подборка	События для выбранной подборки (по выбранному фильтру)
Динамика статусов за период	Динамика статусов за выбранный период времени
Статистика по политикам	Количество нарушений по политикам в разрезе правил передачи, копирования и хранения за выбранный период времени
Статистика по объектам защиты	Количество нарушений по объектам защиты в разрезе уровней нарушений за выбранный период времени
Статистика по каталогам объектов защиты	Количество нарушений по каталогам объектов защиты в разрезе уровней нарушений за выбранный период времени

Действия пользователя:

- настройка виджетов для отображения информации о нарушениях/нарушителях (см. "Создание и настройка виджета")
- перемещение плиток виджетов (см. "Создание и настройка виджета")

Динамика нарушений за период

Виджет **Динамика нарушений** отображает количественные изменения по выбранным типам нарушений за выбранный период времени. Данные на виджете сгруппированы по дням.



Нарушения высокого, среднего и низкого уровня представлены на отдельных графиках. При наведении курсора на график в точках пересечения времени и количества нарушений отображаются маркеры. При нажатии на маркер выполняется переход в раздел "События", где будут показаны нарушения за выбранный день, с выбранным уровнем нарушений и типом правил.

В правом верхнем углу виджета отображается период, за который выводятся данные. Вы можете выбрать требуемый период в раскрывающемся списке.

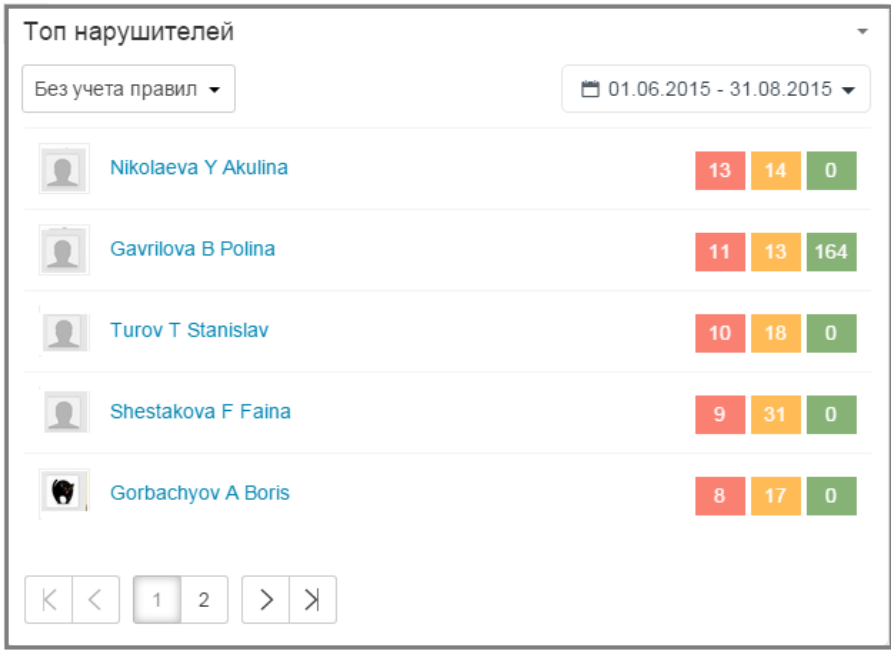
В верхнем левом углу виджета выберите, нарушения каких правил должны отображаться на виджете. Возможные значения: *Правила передачи*, *Правила копирования*, *Правила хранения*, *Без учета правил*.

Чтобы изменить название виджета и выбрать интервал обновления, в верхнем правом углу виджета нажмите и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

Топ нарушителей

Виджет **Топ нарушителей** отображает список наиболее активных нарушителей в разрезе количества нарушений высокого, среднего и низкого уровня за выбранный период времени.

С помощью данного виджета вы можете посмотреть, кто из сотрудников совершил наибольшее количество действий, нарушающих политику безопасности, за определенный период (например, за текущий день), после чего перейти к расследованию инцидентов.



Нажмите на количество нарушений, чтобы перейти в раздел "События" и просмотреть события, удовлетворяющее заданным в настройках виджета условиям.

При нажатии на имя нарушителя раскрывается карточка персоны (если персона была проидентифицирована; подробнее см, "Идентификация контактов в событии"). Для просмотра подробной информации о нарушителе в разделе "Персоны" нажмите на ссылку "Перейти к персоне". Для нарушителей, которые не были проидентифицированы, отображается контакт отправителя.

В правом верхнем углу виджета отображается период, за который выводятся данные. Вы можете выбрать требуемый период в раскрывающемся списке.

В верхнем левом углу виджета выберите, нарушения каких правил должны отображаться на виджете. Возможные значения: *Правила передачи*, *Правила копирования*, *Правила хранения*, *Без учета правил*.

Чтобы отредактировать остальные параметры виджета, в верхнем правом углу виджета нажмите и в раскрывающемся списке нажмите **Редактировать**.

Для редактирования доступны следующие параметры:

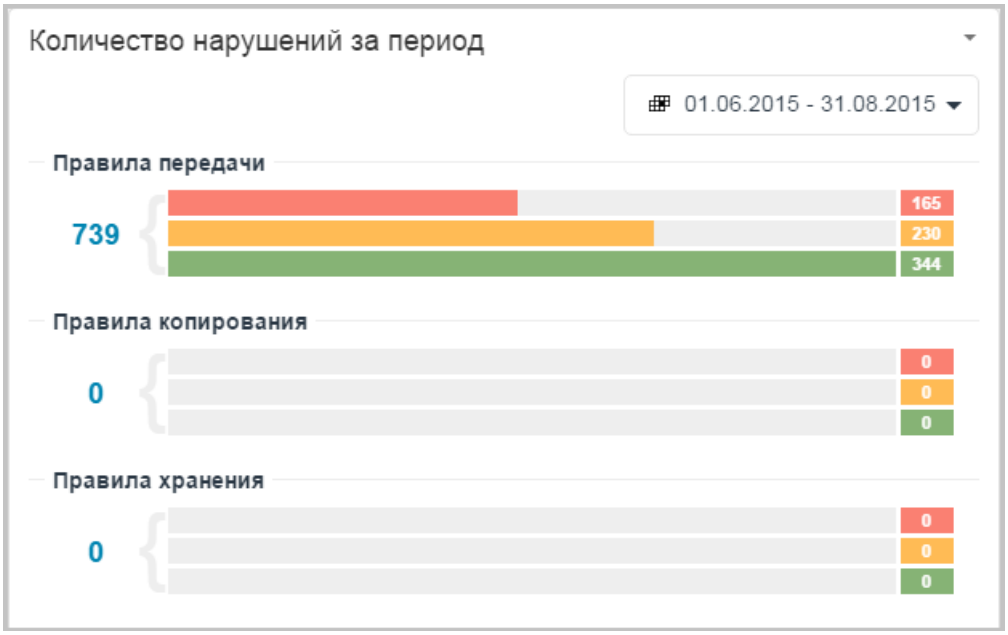
- **Название**;
- **Интервал обновления** данных на виджете;
- **Количество нарушителей**, по которым будет отображаться статистика;
- **Группы**, в которые могут входить нарушители. На виджете будет отображаться статистика по выбранным группам. Начните вводить название группы или нажмите и выберите требуемые группы из списка;
- **Статусы** персон, информация по которым будет отображаться. Начните вводить название статуса или нажмите и выберите требуемые статусы из списка.

Отредактируйте требуемые параметры, после чего нажмите **Сохранить**.

Количество нарушений за период

Виджет **Количество нарушений за период** отображает количество нарушений высокого, среднего и низкого уровня для каждого типа правил (передачи, размещения, копирования) за выбранный период времени.

При нажатии на число, обозначающее общее количество нарушений для выбранного типа правил (выделено синим цветом), выполняется переход в раздел "События", где будут показаны нарушения за выбранный период для выбранного типа правил.



В правом верхнем углу виджета отображается период, за который выводятся данные. Вы можете выбрать требуемый период в раскрывающемся списке.

Чтобы отредактировать остальные параметры виджета, в верхнем правом углу виджета нажмите и в раскрывающемся списке нажмите **Редактировать**.

Для редактирования доступны следующие параметры:

- **Название**;
- **Интервал обновления**;
- **Тип предоставления** - способ отображения данных на виджете. Возможные значения: *Столбчатая диаграмма (горизонтальная)* и *Таблица*.

Отредактируйте требуемые параметры, после чего нажмите **Сохранить**.

Подборка

Виджет **Подборка** отображает события, удовлетворяющие условиям выбранного запроса.



При нажатии на **ID** события (выделен синим цветом) выполняется переход в раздел "**События**", к краткой форме просмотра выбранного события.

Чтобы изменить параметры виджета, в верхнем правом углу виджета нажмите и в раскрывающемся списке нажмите **Редактировать**.

Для редактирования доступны следующие параметры:

- **Название**;
- **Интервал обновления** данных на виджете;
- **Подборка** - запрос, по которому будет осуществляться подборка. Выберите требуемый запрос из раскрывающегося списка (подробнее см. "Запросы");
- **Событий на странице** - количество событий, которое будет отображаться на странице.

Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

Динамика статусов за период

Виджет **Динамика статусов за период** отображает изменения статусов персон за выбранный промежуток времени.



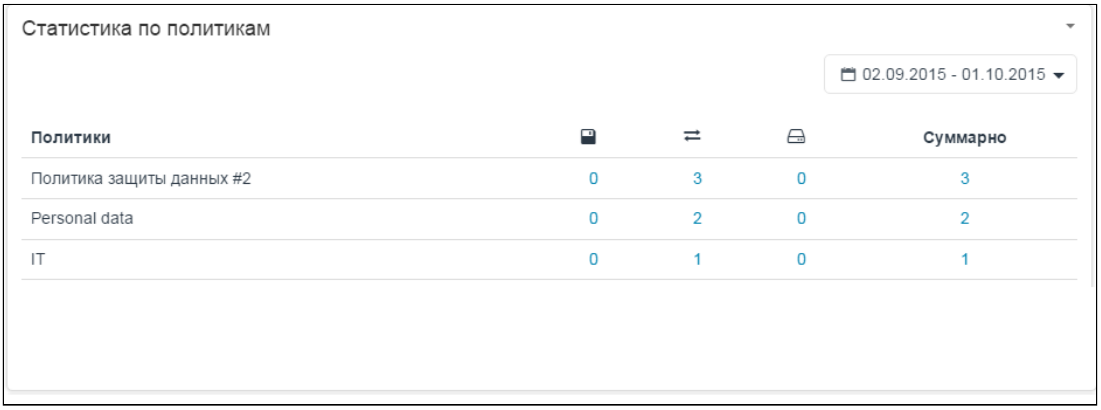
При нажатии на количество персон или компьютеров (выделено синим цветом), выполняется переход в раздел "Персоны" (к вкладке **Персоны** или **Компьютеры** соответственно), где будут показаны персоны (или компьютеры), удовлетворяющие заданным в виджете условиям.

В правом верхнем углу виджета отображается период, за который выводятся данные. Вы можете выбрать требуемый период в раскрывающемся списке.

Чтобы изменить название виджета и выбрать интервал обновления, в верхнем правом углу виджета нажмите и в раскрывающемся списке нажмите **Редактировать**. Отредактируйте требуемые параметры, после чего нажмите **Сохранить**.

Статистика по политикам

Виджет **Статистика по политикам** отображает количество нарушений по политикам в разрезе правил передачи, копирования, хранения и буфера обмена за выбранный период времени.



При нажатии на число нарушений правил копирования, передачи, размещения (выделено синим цветом), выполняется переход в раздел "События", где будут показаны события, удовлетворяющее заданным в виджете условиям.

В правом верхнем углу виджета отображается период, за который выводятся данные. Вы можете выбрать требуемый период в раскрывающемся списке.

Чтобы отредактировать остальные параметры виджета, в верхнем правом углу виджета нажмите и в раскрывающемся списке нажмите **Редактировать**.

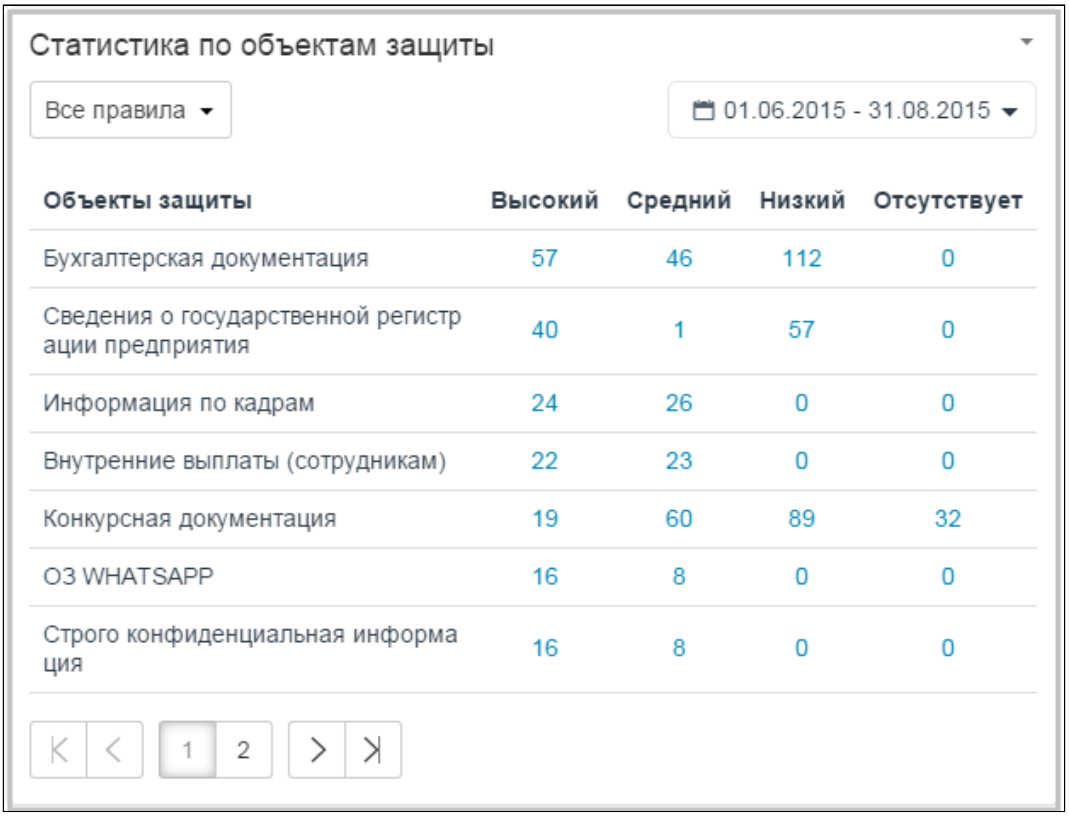
Для редактирования доступны следующие параметры:

- **Название**;
- **Интервал обновления** данных на виджете;
- **Политики**, статистика по которым будет отображаться. Начните вводить название политики или нажмите + и выберите нужные политики из списка.

Отредактируйте требуемые параметры, после чего нажмите **Сохранить**.

Статистика по объектам защиты

Виджет **Статистика по объектам защиты** отображает количество нарушений по объектам защиты в разрезе уровней нарушений за выбранный период времени.



Событие отображается в статистике, если в событии присутствует какой-либо из выбранных объектов защиты или какой-либо объект защиты из выбранных каталогов, в том числе вложенных.

При нажатии на число нарушений для каждого из объектов защиты (выделено синим цветом), выполняется переход в раздел "События", где будут показаны события, удовлетворяющее заданным в настройках виджета условиям.

В правом верхнем углу виджета отображается период, за который выводятся данные. Вы можете выбрать требуемый период в раскрывающемся списке.

В верхнем левом углу виджета выберите, нарушения каких правил должны отображаться на виджете. Возможные значения: *Правила передачи*, *Правила копирования*, *Правила хранения*, *Без учета правил*.

Чтобы отредактировать остальные параметры виджета, в верхнем правом углу виджета нажмите и в раскрывающемся списке нажмите **Редактировать**.

Для редактирования доступны следующие параметры:

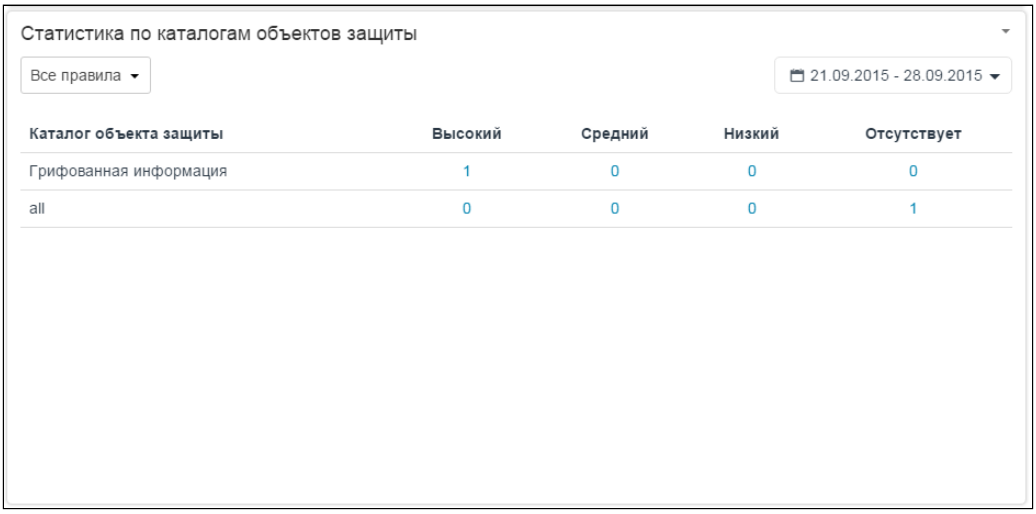
- **Название**;
- **Интервал обновления** данных на виджете;
- **Объект защиты** - объекты защиты, по которым будет отображаться статистика.

  Начните вводить название объекта защиты или нажмите + и выберите требуемые объекты из списка;
- **Каталог объекта защиты** - каталоги объектов защиты, по которым будет отображаться статистика. Начните вводить название каталога или нажмите + и выберите требуемые каталоги из списка.

Отредактируйте требуемые параметры виджета, после чего нажмите **Сохранить**.

Статистика по каталогам объектов защиты

Виджет **Статистика по каталогам объектов защиты** отображает количество нарушений по каталогам объектов защиты в разрезе уровней нарушений за выбранный период времени.



Событие отображается в статистике по выбранному каталогу, если в событии присутствукт какой-либо объект защиты из этого каталога. Наличие объектов защиты из вложенных каталогов не учитывается.

При нажатии на число нарушений для каждого из каталогов объектов защиты (выделено синим цветом) выполняется переход в раздел "События", где будут показаны события, удовлетворяющее заданным в виджете условиям.

В правом верхнем углу виджета отображается период, за который выводятся данные. Вы можете выбрать требуемый период в раскрывающемся списке.

В верхнем левом углу виджета выберите, нарушения каких правил должны отображаться на виджете. Возможные значения: *Правила передачи*, *Правила копирования*, *Правила хранения*, *Без учета правил*.

Чтобы отредактировать остальные параметры виджета, в верхнем правом углу виджета нажмите и в раскрывающемся списке нажмите **Редактировать**.

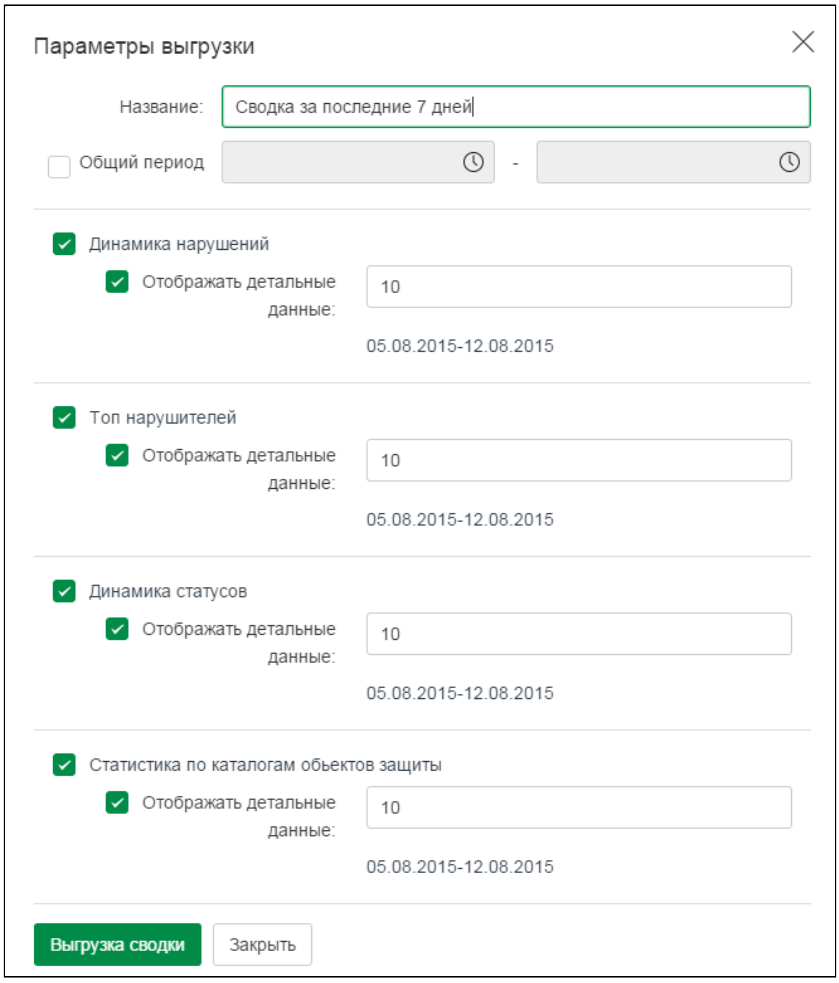
Для редактирования доступны следующие параметры:

- **Название**;
- **Интервал обновления** данных на виджете;
- **Каталог объекта защиты** - каталог объектов защиты, сводка по которому будет отображаться. Начните вводить название каталога или нажмите + и выберите требуемые каталоги из списка.

Отредактируйте требуемые параметры, после чего нажмите **Сохранить**.

3.1.2 Выгрузка сводки

Выгрузка сводки требуется для наглядного отображения статистических данных о перехваченных объектах, и может быть представлена в формате PDF или HTML. Вы также можете распечатать ее на принтере.



Перед формированием выгрузки укажите ее название и убедитесь, что отмечены все виджеты, которые вы хотите включить в выгрузку.

По умолчанию выгрузка формируется для всех виджетов панели. Если вы не хотите включать данные какого-либо виджета, снимите флажок напротив его названия.

Отметьте настройку **Отображать детальные данные**, если хотите, чтобы в выгрузке отображались отдельные объекты. При необходимости измените количество объектов, которые будут отображать в выгрузке (по умолчанию отображается 10 объектов). Например, для виджета "Динамика статусов за период" данный параметр определяет, сколько персон и компьютеров для каждого статуса будут добавлены в выгрузку.

Отметьте настройку **Общий период**, если требуется сформировать сводку для всех виджетов за общий период. Укажите начальную и конечную дату.

> **Примечание.**
>
> По умолчанию сводка для каждого виджета генерируется за период, указанный в настройках виджета.

Действия пользователя:

- составление выгрузки сводки (см. "Создание выгрузки сводки")

3.2 Раздел "События"

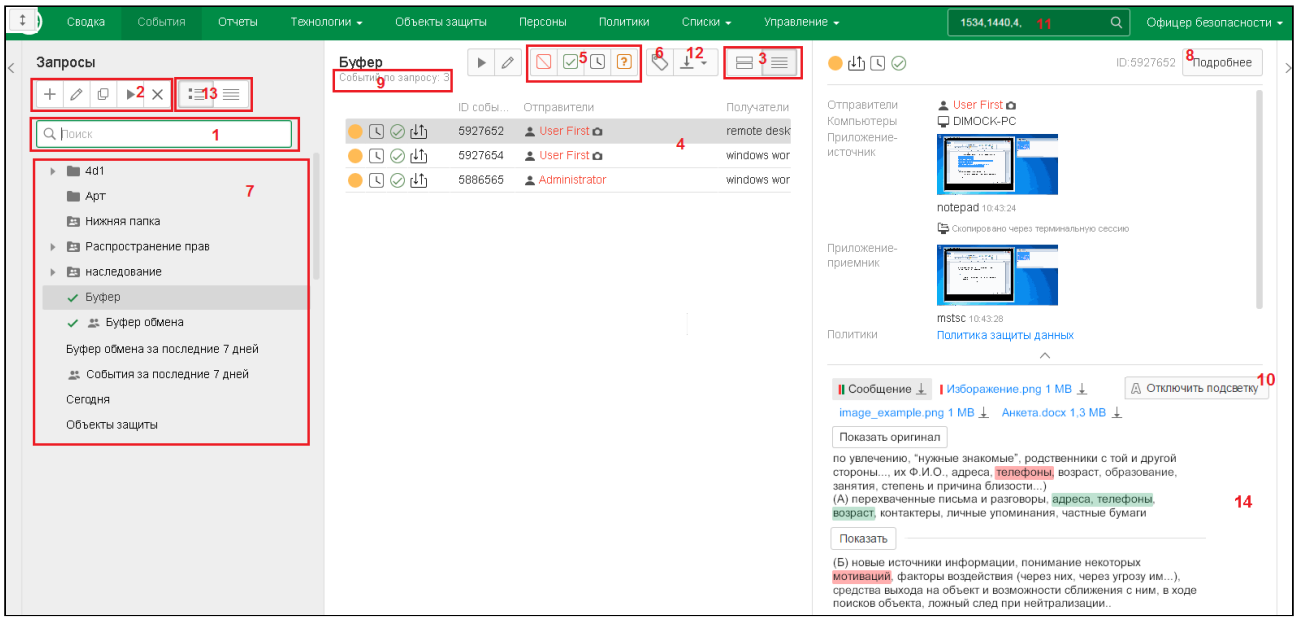
Справочная информация:
Событие – объект перехвата сетевого трафика.

События создаются Системой в результате перехвата трафика при:

- передаче данных сотрудниками другим людям;
- публикации данных в общедоступных источниках;
- копировании данных на внешние устройства;
- печати данных.

О разделе:

Раздел содержит список событий (объектов перехвата) и средства для работы с ними.
В Системе может содержаться большое число событий, поэтому список событий отображается по результатам применения пользовательских запросов.



Список запросов расположен в левой части рабочей области (№ 7 на изображении). Запросы могут создаваться как на верхнем уровне, так и внутри папок. Для работы с запросами и папками используются инструменты на панели (№ 2 на изображении). Вы можете выбрать режим отображения элементов в списке (№13 на изображении):

-  – в виде папок;
-  – в виде плоского списка.

При выборе папки отображаются входящие в нее подпапки и запросы.

Для поиска нужных событий, выберите запрос из списка (№ 7 на изображении) или создайте новый запрос с помощью кнопки  на панели инструментов (№ 2 на изображении).

Вы также можете воспользоваться полем поиска, чтобы найти папку или запрос по названию (№ 1 на изображении).

Чтобы запустить выполнение выбранного запроса, нажмите  на панели инструментов (№ 2 на изображении).

Если известно ID события, вы можете использовать поле поиска события по ID (№ 11 на изображении).

> **Примечание.**
>
> Вы можете ввести несколько ID, разделенных запятой, точкой с запятой или пробелом.

В результате выполнения запроса или поиска по ID отображается список найденных событий (№ 4 на изображении).

Под названием запроса отображается общее количество найденных событий (№ 9 на изображении).

Вы можете выбрать способ отображения событий (№ 3 на изображении):

-  – в виде списка из плиток событий;
-  – в виде таблицы.

В правой части рабочей области отображается краткая форма просмотра выбранного события (№14 на изображении). Для более наглядного отображения результатов анализа в краткой форме просмотра события используется подсветка сработавших объектов защиты (выделены красным цветом) и результатов поиска по тексту события (выделены зеленым цветом). Вы можете полностью отключить подсветку результатов, нажав кнопку **Отключить подсветку** (№ 10 на изображении).

Для перехода к детальной форме просмотра события используется кнопка **Подробнее** (№8 на изображении).

Для выбранного события вы можете выполнить следующие действия:

- вынести решение по событию (выберите нужное решение, используя кнопки на панели – № 5 на изображении);
- назначить событию тег (№ 6 на изображении);
- выгрузить событие или сохранить отладочную информацию по событию (№ 12 на изображении).

Действия пользователя:

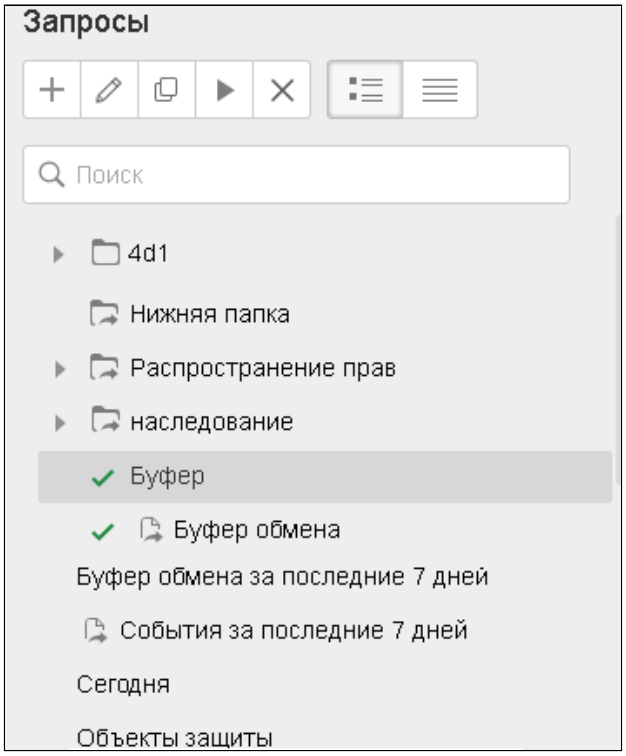
- фильтрация событий (см. "Создание запросов")
- просмотр информации по событию (см. "Просмотр краткой формы события" и "Просмотр детальной формы события")
- вынесение решения по событию (см. "Вынесение решения по объекту")
- добавление/удаление тега события (см. "Добавление/удаление тега")
- сохранение события (см. "Сохранение события (для SMTP-писем)")
- досылка заблокированного события (см. "Досылка события, находящегося в карантине")
- выгрузка событий (см. "Выгрузка событий")
- просмотр контактов отправителей и получателей в событии (см. "Идентификация контактов в событии")

3.2.1 Запросы

Объекты, проверенные Системой, сохраняются в базу данных. Чтобы просмотреть в Консоли управления информацию по объектам, загруженным в БД, нужно создать и применить запрос.

Запрос позволяет получить выборку объектов перехвата по заданным условиям.

Для удобства работы с запросами используются папки. Папки позволяют группировать запросы, объединенные общей тематикой, определять права доступа сразу для всей группы запросов, наследовать права доступа и т.д. Папка может включать как запросы, так и подпапки.



При создании папки указываются права доступа. Для вложенных папок права доступа могут наследоваться от родительской папки либо настраиваться отдельно (подробнее см. "Создание папки с запросами"). Папки, доступные только владельцу, отмечены значком . Если папка доступна также другим пользователям Консоли, она имеет значок .

Вы можете создать запрос внутри выбранной папки либо на верхнем уровне. При создании запроса внутри папки права доступа либо наследуются из папки, либо задаются отдельно. Если, помимо владельца, запрос доступен также другим пользователям Консоли, запрос отмечен значком .

Если запрос уже выполнялся ранее и содержит актуальные данные, такой запрос отмечен значком . При выборе такого запроса найденные события отображаются на форме просмотра справа.

Примечание.

Срок хранения результатов настраивается администратором. По умолчанию результаты выполнения запроса удаляются один раз в сутки.

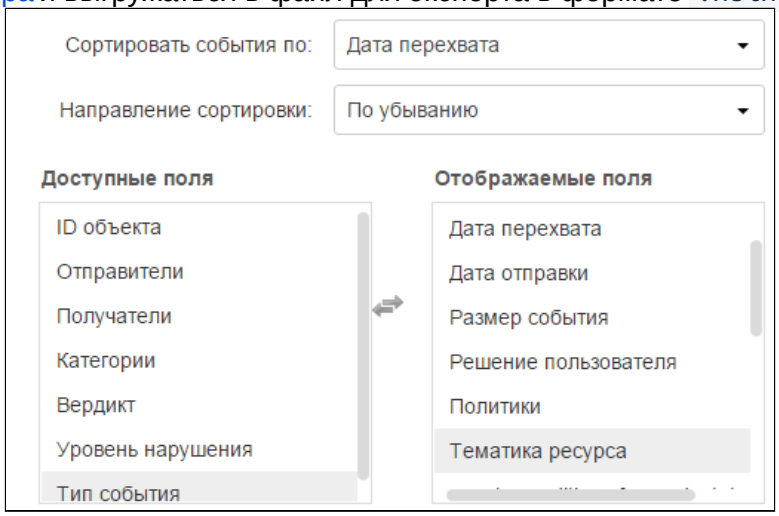
Если запрос в данный момент выполняется, рядом с его названием отображается значок . Для запросов, выполнение которых завершилось с ошибкой, отображается значок .

Чтобы создать новый запрос, нажмите  на панели инструментов и в раскрывающемся списке выберите, какой запрос требуется создать.

Предусмотрено два режима создания запроса: обычный (позволяет выбрать нужные условия из списка) и расширенный (позволяет выполнить гибкую настройку параметров поиска).

Форма создания запроса содержит следующие вкладки:

- Вкладка **Запрос**. На этой вкладке вы можете указать условия поиска в обычном или расширенном режиме.
- Вкладка **Столбцы**. На этой вкладке вы можете выбрать, какие поля будут отображаться для события. В списке **Доступные поля** представлены атрибуты события, а в списке **Отображаемые поля** - те атрибуты события, которые будут отображаться в табличной форме просмотра и выгружаться в файл для экспорта в формате `.xslx`.



Если не выбран ни один атрибут, то в табличной форме просмотра и при выгрузке будут отображаться все атрибуты.

> **Важно!**
>
> Агрегирующий столбец **Атрибуты приемника** не попадает в выгрузку событий, даже если он находится в списке **Отображаемые поля** (подробнее про столбец **Атрибуты приемника** см. в статье "Табличное представление событий").

Также вы можете выбрать, по какому полю сортировать список, и указать направление сортировки.

- Вкладка **Доступ**. На этой вкладке указываются параметры доступа к запросу. Возможные варианты:
  - Если запрос создается внутри папки и для папки установлена настройка **Применить права для дочерних папок и запросов**, то права доступа к запросу будут совпадать с правами, указанными для папки. Редактирование параметров доступа к запросу недоступно.
  - Если запрос создается внутри папки и настройка **Применить права для дочерних папок и запросов** не установлена, либо запрос создается на верхнем уровне, то вы можете указать для него параметры доступа. По умолчанию запрос доступен только владельцу. Чтобы открыть доступ к запросу другим пользователям, выберите нужных пользователей в списке и установите напротив имени пользователя флажок в поле с требуемым уровнем доступа (**Просмотр и выполнение** либо **Полный доступ**).

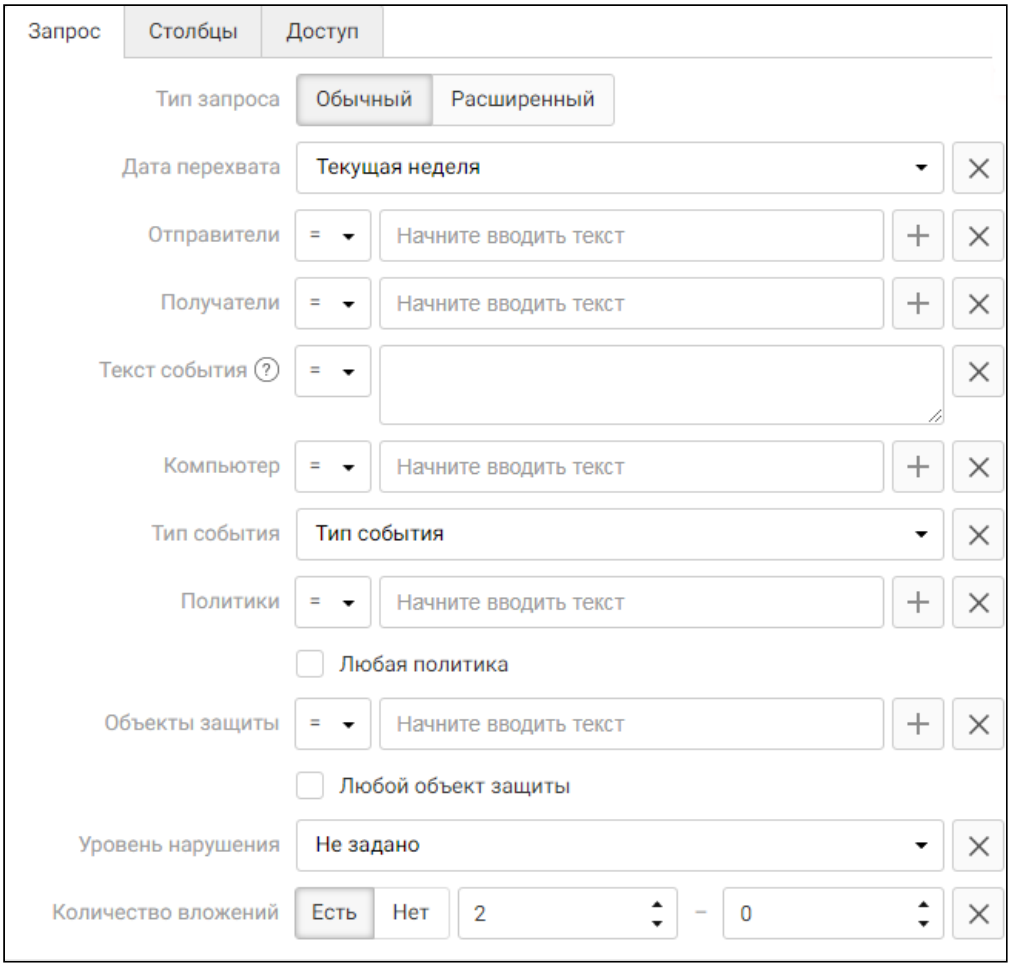
Действия пользователя:

- создание папки, содержащей запросы (см. "Создание папки с запросами")
- настройка параметров запроса (см. "Создание запросов")
- определение полей просмотра (см. "Выбор полей просмотра событий")

Обычный режим создания запроса

В обычном режиме вы можете указать значения требуемых параметров, при необходимости применяя отрицание. Значения параметров указываются на вкладке **Запрос**.

Все условия объединены с помощью конъюнкции (логическое "И"). Значения, указанные для одного условия, объединяются с помощью дизъюнкции (логическое "ИЛИ").



По умолчанию отображаются наиболее часто используемые условия.

В выпадающем списке **Добавить условие** вы можете выбрать дополнительные параметры, по которым будет выполняться поиск.

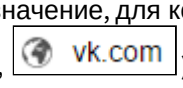
Полный список доступных условий:

Условие	**Описание**
Основные	

ID события	Уникальный идентификатор события. Может быть указано несколько значений через запятую.
Дата перехвата	Время создания события. По умолчанию будут показаны события за текущую неделю. Доступные значения: • Все время • Начиная с • Заканчивая • Текущий день/неделя/месяц • Последние несколько часов/дней • Последние 3/7/30 дней • Период (на календаре)
Тип события	Характеристика, указывающая на принадлежность события к тому или иному перехватчику. Типы событий сгруппированы по категориям. При выборе категории будут выбраны все входящие в нее типы событий. Доступные значения: • Запись мультимедиа: - Снимок экрана • Работа в приложениях: - Буфер обмена - Ввод с клавиатуры • Интернет-активность: - Веб-сообщение • Обмен файлами: - FTP - Съемные устройства - Облачное хранилище - Терминальная сессия - Сетевые ресурсы • Принтеры и МФУ: - Печать • Хранение файлов: - Data Discovery • Почта: - Почта на Клиенте - Почта в Браузере • Мессенджер: - Telegram - Facebook - WhatsApp - VKontakte - MS Lync - ICQ - XMPP - MMP - Skype

	- MS Teams (если установлен адаптер MS Teams) - Kribrum • Файловые операции - Чтение файла - Запись файла
Перехватчик	Перехватчик, с помощью которого было получено событие. Возможные значения: • ICAP • DM • Adapter • SMTPD • Sniffer • PushAPI • Data Discovery
Протокол	Тип перехватываемого протокола. Возможные значения: • FTP • HTTP • HTTPS • IMAP • MAPI • MMP • NRPC • OSCAR • POP3 • SIP • Skype • SMTP/ ESMTP • Telegram • XMPP • WhatsApp
Источники и приемники копирования	Источники и приемники, с которых/на которые выполнена операция копирования. Параметры настройки: • Приемник копирования: - Компьютер - Съемное устройство - Сетевой ресурс - Терминальная сессия - FTP - Облачное хранилище • Источник копирования: - Компьютер - Съемное устройство - Сетевой ресурс - Терминальная сессия

	• Направление маршрута: - В одну сторону - В оба направления Есть возможность указать Путь к файлу или адрес, Имя устройства, ID устройства. Вы можете указать значение с использованием групповых символов: • "?" – заменяет один символ в начале или в конце строки; • "*" – заменяет любое количество символов в начале или в конце строки **Примечание**: В зависимости от выбранного типа источника или приемника копирования у поля **Путь к файлу или адрес** могут быть особенности заполнения (см. Особенности заполнения поля "Путь к файлу или адрес"). **Важно**: Тип значения атрибута **Путь к файлу или адрес** для приемника копирования типа *Терминальная сессия* зависит от версии Traffic Monitor. Типы значений различаются для этого атрибута в событиях обмена файлами по терминальной сессии: • **Для событий, созданных в Traffic Monitor версии ниже 7.5**: в атрибуте указывается имя скопированного файла, например: `file.txt` • **Для событий, созданных в Traffic Monitor версии 7.5 и выше**: в атрибуте указывается IP-адрес устройства, с которого осуществлялось удаленное подключение к рабочей станции сотрудника и на которое был скопирован файл, например: `192.0.2.0` Чтобы искать события, созданные в Traffic Monitor версии 7.5 и выше, рекомендуется отредактировать существующие запросы. Существующие запросы необходимо отредактировать, если в них используется устаревший тип значения атрибута **Путь к файлу или адрес** для приемника копирования типа *Терминальная сессия*. Если в запросе в этом атрибуте указано имя файла, то нужные события могут не соответствовать условиям запроса, так как у новых событий в этом атрибуте указан IP-адрес.
Мандатный уровень	Мандатный уровень конфиденциальности. Параметр учитывается в Traffic Monitor на ОС Astra Linux Special Edition "Смоленск".
Адресаты	
Отправители	Список отправителей объекта. Могут быть указаны персоны, группы персон, статусы или значения контактов

	(кроме SID). Для контактов вы можете указать значение с использованием групповых символов: ▪ "?" – заменяет один символ в начале или в конце строки; ▪ "*" – заменяет любое количество символов в начале или в конце строки.
Получатели	Список получателей объекта. Могут быть указаны персоны, группы персон и статусы. Для контактов вы можете указать значение с использованием групповых символов: • "?" – заменяет один символ в начале или в конце строки; • "*" – заменяет любое количество символов в начале или в конце строки.
Число получателей	Количество получателей объекта
Вошло в периметры	Периметр, в котором находится получатель трафика
Покинуло периметры	Периметр, в котором находится отправитель трафика
Компьютеры	Компьютер, с которого был отправлен объект. Может быть указано имя компьютера или IP-адрес. Вы можете указать значение с использованием групповых символов: • "?" – заменяет один символ в начале или в конце строки; • "*" – заменяет любое количество символов в начале или в конце строки.
Тип компьютера	Тип компьютера, с которого был отправлен объект. Возможные значения: • рабочая станция • терминальный сервер
Ресурсы	Интернет-ресурс или группа ресурсов (см. "Веб-ресурсы"). Начните вводить название ресурса или группы и выберите требуемое значение из списка подсказок, предложенных Системой. Вы можете указать значение с использованием групповых символов: • "?" – вместо одного символа; • "*" – вместо нескольких символов. **Примечание**. При указании конкретного ресурса необходимо выбирать значение, для которого отображается символ  (например, ).

Работа в приложениях	
Приложение-источник	Приложение, из которого были скопированы данные
Приложение-приемник	Приложение, в которое были вставлены данные из буфера обмена
Результаты анализа	
Уровень нарушения	Уровень нарушения политики корпоративной безопасности. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует*.
Теги	Теги, присвоенные объекту (см. "Теги")
Политики	Список политик, сработавших на объекте
Тип нарушения	Тип правила, которое было нарушено. Возможные значения: ▪ *Нарушение передачи;* ▪ *Нарушение копирования;* ▪ *Нарушение хранения.*
Решение пользователя	Решение, принятое пользователем по объекту. Возможные значения: ▪ *Нарушение*; ▪ *Нет нарушения;* ▪ *Решение не принято*; ▪ *Требует дополнительной обработки.*
Вердикт	Вердикт, вынесенный Системой по объекту. Возможные значения: ▪ *Разрешено;* ▪ *Заблокировано;* ▪ *Карантин*.
Технологии	Элементы технологий, обнаруженные в перехваченных данных в составе сработавших объектов защиты. При добавлении текстового объекта вы также можете указать его значение. Если указан текстовый объект и к атрибуту применено отрицание, то из результатов поиска будут исключены события, в которых содержится указанный текстовый объект с заданным значением. См. также *Пример 6* в статье "Примеры использования запросов". **Примечание:** Для добавления в поиск доступны также текстовые и графические объекты, смигрированные из

	прошлых версий Системы, а также ранее удаленные. Их названия в строке будут обозначены красным.
Объекты защиты	Список сработавших объектов защиты. Вы можете выбрать как отдельные объекты защиты, так и каталоги.
Содержимое события	
Количество вложений	С помощью переключателя **Есть**/**Нет** укажите, содержит ли событие вложения. Для событий с вложениями укажите минимальное и максимальное количество вложений, которое может содержать событие. Если выбрать **Есть** и не указывать количество вложений, то в результаты попадут все события, содержащие вложения. Вложения в архивах тоже учитываются
Название вложения	Название вложения, содержащегося в событии. Указывается имя файла и его расширение. Вы можете указать значение с использованием групповых символов: • "?" – заменяет один символ в начале или в конце строки; • "*" – заменяет любое количество символов в начале или в конце строки. **Примечание**. Если название вложения содержит запятую, ее необходимо экранировать с помощью символа \. Например, название вложения 'тест1,2.txt' следует указывать как 'тест1\,2.txt'. См. также статью базы знаний "Как найти событие по имени файла".
Формат вложения	Формат файла вложения. Можно выбрать несколько значений, а также указать, если требуется найти: • Зашифрованный файл; • Склеенный файл; • Несоответствие сигнатуры и расширения
Путь к файлу	Источник файла. Вы можете указать значение с использованием групповых символов: • "?" – заменяет один символ в начале или в конце строки; • "*" – заменяет любое количество символов в начале или в конце строки.
Размер вложения	Размер вложенного файла. Можно указать минимальный или максимальный размер файла либо оба параметра.

Текст события	Укажите текст для поиска. Будут найдены события, в тексте которых присутствуют все перечисленные слова без учета регистра, морфологии, порядка следования и расположения слов. Поиск выполняется по всему содержимому события. Использование групповых символов ("*", "?") не допускается. При отрицании условия из результатов поиска будут исключены события, в тексте которых присутствуют все указанные слова. **Примечание:** В результате поиска по тексту события будут найдены только те события, которые уже были проиндексированы на момент выполнения запроса. Индексация событий выполняется каждые десять минут, однако при большой нагрузке на сервер этот интервал может увеличиться.
Data Discovery	
Название задачи	О значениях атрибутов см. "InfoWatch Data Discovery. Руководство пользователя", "Экспорт данных".
Дата запуска задачи	
Дата создания файла	
Дата изменения файла	
Цель сканирования	Всегда указывается значение **Разделяемые сетевые ресурсы**.
Пользовательские атрибуты	
	Атрибуты, которые могут быть добавлены в Систему с помощью плагинов, регистрируемых в Traffic Monitor (см. статью Плагины). Эта возможность позволяет расширить объем обрабатываемой и передаваемой информации, добавив атрибуты сторонних систем-источников событий. Пользовательские атрибуты можно использовать в правилах политик защиты данных. Примеры возможных пользовательских атрибутов: • длительность разговора; • идентификатор события в исходной системе; • гиперссылка на событие в исходной системе; • тип действия в социальной сети.
Имя терминальной станции	Имя устройства, с которого было осуществлено удаленное подключение к рабочей станции сотрудника. Атрибут указывается для приемника копирования типа

	Терминальная сессия в событиях обмена файлами по терминальной сессии. Имя терминальной станции является пользовательским атрибутом предустановленного плагина InfoWatch Device Monitor.
Адрес вкладки браузера	Адрес активной вкладки браузера в момент создания события. Адрес вкладки браузера является пользовательским атрибутом предустановленного плагина InfoWatch Device Monitor.

После выбора условия укажите его значение в строке. Поиск по введенным начальным символам выдаст первые 10 результатов в полях: *Отправители, Получатели, Вошло в периметры, Покинуло периметры, Технологии, Компьютер, Ресурсы, Теги, Приложение, Приложение-источник, Приложение-приемник*.

Например, для условия *Отправители* будет выдано не более 10 статусов, 10 персон, 10 групп. Чтобы найти сущность, которой нет в предложенных вариантах, введите следующие несколько символов.

По умолчанию все атрибуты проверяются на равенство указанным значениям (параметр  рядом с названием атрибута). Результаты выполнения запроса будут включать события, параметры которых имеют указанные значения.

Чтобы исключить из результатов события, параметры которых имеют указанные значения, примените к нужным параметрам отрицание .

Настройка равенства или отрицания доступна для следующих атрибутов:

- ID события;
- Отправители;
- Получатели;
- Вошло в периметры;
- Покинуло периметры;
- Компьютеры;
- Ресурсы;
- Теги;
- Политика;
- Название вложения;
- Формат вложения;
- Текста события;
- Результаты анализа;
- Объекты защиты;
- Имя терминальной станции;
- Адрес вкладки браузера.

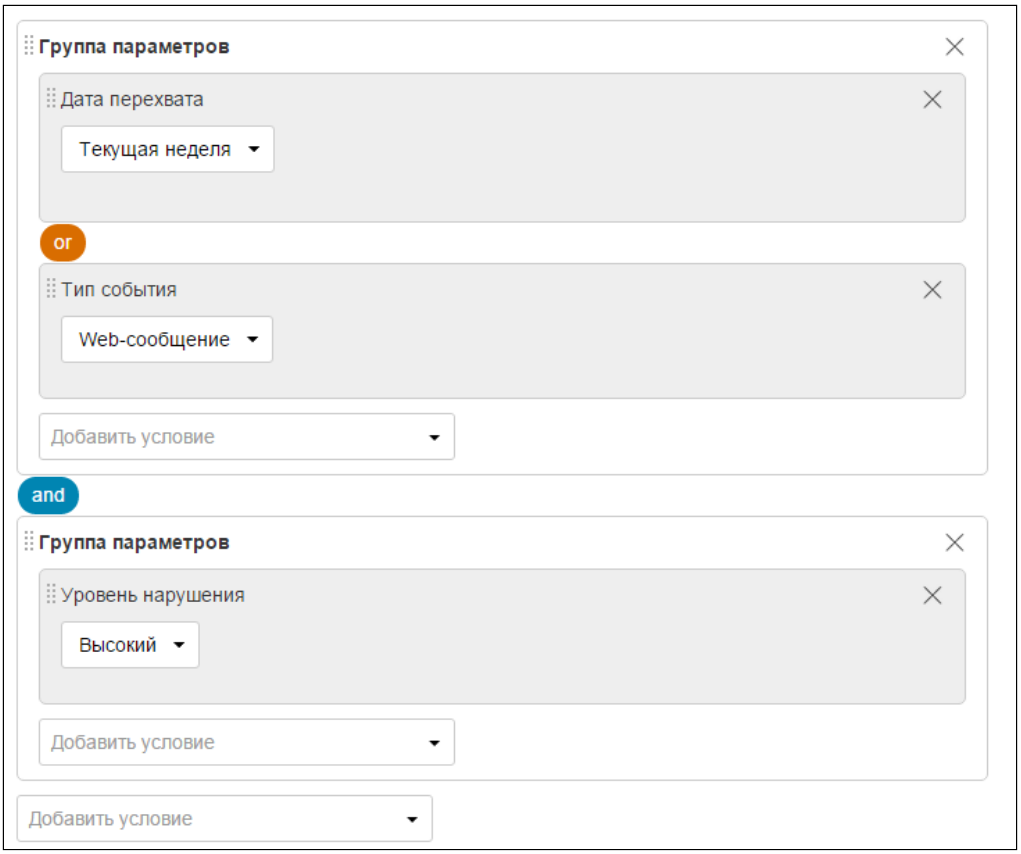
Если отрицание применяется к атрибуту с множественными значениями, то из результатов поиска будут исключены события, содержащие указанные значения. Например, если в качестве отправителей указаны адреса `user1@example.com` и `user2@example.com`, из результатов поиска будут исключены события, в которых отправителем является `user1@example.com` или `user2@example`.

Действия пользователя:

- Создание стандартного запроса (см. "Создание запроса в обычном режиме")

Расширенный режим создания запроса

Расширенный режим предназначен для гибкой настройки параметров запроса.



Для составления запроса используются:

- список атрибутов событий – набор атрибутов, которые присваиваются объекту перехвата в результате анализа Системой;
- элемент *Группа параметров* – контейнер, предназначенный для логического разделения запроса на части;
- – параметр равенства атрибуту. Индикатор того, что результаты запроса будут включать события с указанными значениями атрибутов;
-  – параметр отрицания атрибута. Индикатор того, что из результатов запроса будут исключены события с указанными значениями атрибутов.

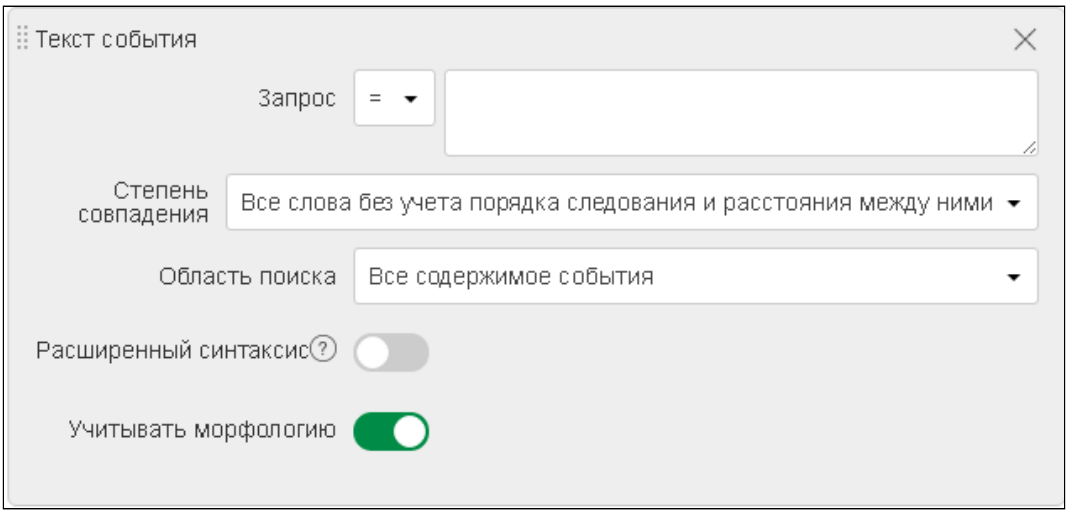
Также при создании запроса в расширенном режиме вы можете выполнить гибкую настройку условий поиска по тексту события.

Действия пользователя:

- Создание расширенного запроса (см. "Создание запроса в расширенном режиме")

Поиск по тексту события

При создании запроса в расширенном режиме вы можете указать условия поиска по тексту события.



Параметры полнотекстового поиска:

Параметр	Описание
Запрос	Искомый текст, который должен или НЕ должен содержаться в событии: ▪ должен – если выбран параметр равенства  ▪ не должен – если к атрибуту применено отрицание 
Степень совпадения	Укажите требуемую степень совпадения: • **Все слова в указанном порядке, расположенные друг за другом** – будут найдены события, в тексте которых все перечисленные слова присутствуют в заданном порядке. При отрицании условия будут найдены события, в тексте которых отсутствуют перечисленные слова в заданном порядке. • **Все слова без учета порядка, но следующие друг за другом** – будут найдены события, в тексте которых все перечисленные слова расположены одно за другим в произвольном порядке. При отрицании условия будут найдены события, в тексте которых отсутствуют перечисленные слова в произвольном порядке. • **Все слова без учета порядка следования и расстояния между ними** – будут найдены события, в тексте которых присутствуют все перечисленные слова без учета порядка их следования и расстояния между ними.

Параметр	Описание
	При отрицании условия будут найдены события, не содержащие перечисленные слова либо содержащее не все перечисленные слова. • **Хотя бы одно из указанных слов** – будут найдены события, в тексте которых присутствует хотя бы одно из указанных слов. При отрицании условия будут найдены события, в тексте которых не содержится ни одно из указанных слов.
Область поиска	Укажите область, в которой будет выполняться поиск: • **Все содержимое события** – поиск будет выполняться по всему содержимому событий; • **Текст сообщения** – поиск будет выполняться по тексту сообщений и темам писем; • **Тема письма** – поиск будет выполняться по темам писем; • **Вложение** – поиск будет выполняться по тексту, темам и именам файлов вложений; • **Имя файла** – поиск будет выполняться по именам файлов вложений.
Расширенный синтаксис	Включите эту настройку, если вы хотите указать слова для поиска с помощью логических операторов. Подробнее см. "Использование расширенного синтаксиса"
Учитывать морфологию	Если данная настройка отключена, то в результате поиска будут найдены события, содержащие искомые слова только в заданной грамматической форме. **Примечание:** Поиск на точное совпадение (то есть без учёта морфологии) возможен только в случае, если события были проиндексированы с включённой опцией "`IndexExactWords`". Подробнее об этой настройке смотрите документ *«Справочник по конфигурационным файлам».*

Особенности задания условий для поиска:

- в качестве разделителя между словами используется пробел;
- регистр при поиске не учитывается;
- использование групповых символов ("*", "?") не допускается;
- дефис ("-") при поиске не учитывается. Поиск осуществляется по каждому из двух слов, входящих в состав слова с дефисом.

Примечание:

В результате поиска по тексту события будут найдены только те события, которые уже были проиндексированы на момент выполнения запроса. Индексация событий выполняется каждые десять минут, однако при большой нагрузке на сервер этот интервал может увеличиться.

Действия пользователя:

- Настройка расширенного запроса (см. "Создание запроса в расширенном режиме")
- Создание запроса с использованием расширенного синтаксиса (см. "Использование расширенного синтаксиса")

3.2.2 Объекты перехвата

В результате выполнения запроса (см. "Запросы") отображается список событий, удовлетворяющие заданным условиям.

Информация о событии представлена в следующих видах:

- в плитке события отображается основная информация о событии;
- в строке события в таблице отображается информация по атрибутам, выбранным на вкладке **Столбцы**;
- в краткой форме просмотра события отображается наиболее часто требуемая информация;
- в детальной форме просмотра события отображается наиболее полная информация об объекте перехвата.

Атрибуты событий:

Элемент	Описание
ID объекта	Уникальный идентификатор события в Системе
Решение пользователя	Принятое пользователем решение по событию. Возможные варианты: • *Решение не принято*; • *Нарушение*; • *Нет нарушения*; • *Требуется дополнительная обработка*.
Тип события	Характер действий, повлекших создание события. Возможные варианты: • – Работа в приложениях (копирование и вставка данных через буфер обмена, ввод с клавиатуры); • – Интернет-активность (post-запросы к веб-ресурсам);

Элемент	Описание
	•  – Обмен файлами (копирование файлов на внешнее устройство и на сетевые ресурсы, передача по протоколу FTP, загрузка данных в облачные хранилища); •  – Принтер и МФУ (отправка на печать); •  – Запись мультимедиа (снимки экрана создаются модулем Device Monitor в соответствии со схемой безопасности); •  – Электронная почта (отправка и получение данных через почту на клиенте и почту в браузере); •  – Мессенджер (отправка или получение сообщений через Skype, MS Teams (если установлен адаптер), MS Lync, ICQ (OSCAR), XMPP, Telegram, WhatsApp); •  – Файловые операции (запись и чтение файла); •  – Хранение файлов (в файловом хранилище SharePoint 2007/2010/2013, в разделяемых сетевых ресурсах и на локальных дисках рабочих станций).
Дата отправки	Дата и время получения письма почтовым сервером (только для электронных писем)
Отправители	Список отправителей трафика
Компьютер отправителя	Наименование компьютера, с которого был передан трафик
Получатели	Список получателей трафика
Политики	Список политик, сработавших при анализе данного события
Категории	Список категорий, присвоенных данному событию
Объекты защиты	Список объектов защиты, сработавших для события
Элементы анализа	Список элементов анализа в составе сработавшего объекта защиты
Тематика сайта	Тип нецелевых ресурсов, посещенных сотрудником
Теги	Список тегов, присвоенных данному объекту

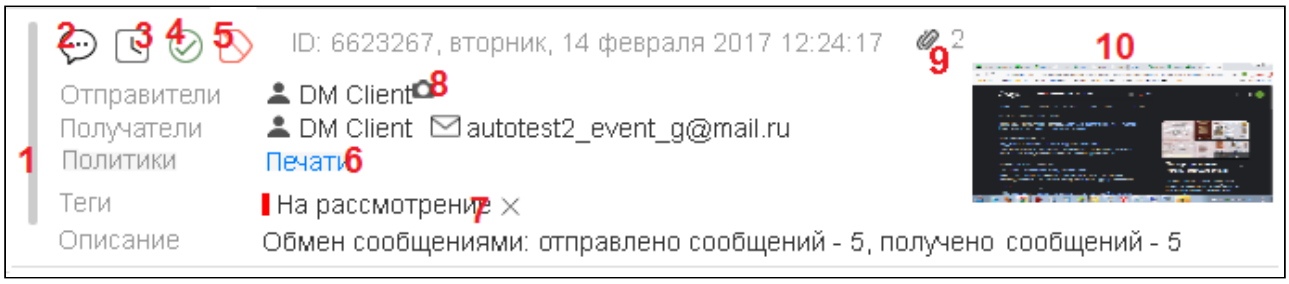
Элемент	Описание
Дата перехвата	Дата и время, когда трафик был перехвачен Системой
Дата вставки	Дата и время, когда данное событие было сохранено в БД
Размер	Размер события (в байтах)
Уровень нарушения	Характеристика нарушения, присвоенная событию. Возможные варианты: • *Отсутствует* – обозначается на плитке серым ( ) цветом; • *Высокий* – обозначается на плитке красным ( ) цветом; • *Средний* – обозначается на плитке оранжевым ( ) цветом; • *Низкий* – обозначается на плитке зеленым ( ) цветом.
Состояние доставки	Показатель того, было ли доставлено сообщение (только для SMTP-писем при работе Системы "в разрыв" см. документ "*Infowatch Traffic Monitor. Руководство по установке и настройке*"). Возможные варианты: ▪ *Ожидание*; ▪ *Доставлено*; ▪ *Неудачно*; ▪ *Попытка не удалась*; ▪ *Заблокировано.*
Вердикт	Присвоенное в результате анализа Системой заключение по данному объекту. Возможные варианты: • *Разрешено* (пиктограмма) • *Заблокировано* (пиктограмма) • *Карантин* (пиктограмма)
Сервер перехвата	Имя или IP-адрес сервера, которым был перехвачен объект

См. также:

- "Плитка события" – о представлении события и его атрибутов
- "Табличное представление событий" – о представлении информации по выбранным атрибутам события
- "Краткая форма просмотра событий" – о представлении общей информации о событии
- "Детальная форма просмотра событий" – о представлении расширенной информации о событии

Плитка события

В списке событий каждое событие отображается в виде плитки:



Плитка события содержит общую информацию о событии: список отправителей и получателей события, ID события, дата и время создания события, описание.

Также на плитке отображается следующая информация (номер соответствует номеру элемента на скриншоте)

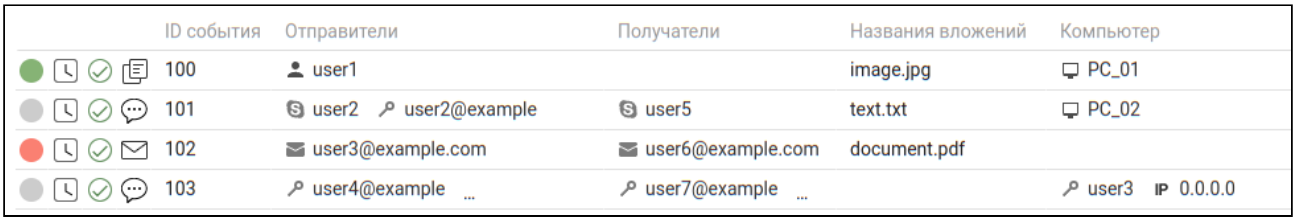
> **Примечание.**
>
> Набор отображаемых атрибутов зависит от типа события.

1. Цвет уровня нарушения. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует.*
2. Тип события. Возможные значения: *Буфер обмена, Ввод с клавиатуры, Снимок экрана, Веб-сообщение, Facebook, WhatsApp, ICQ, MS Lync, Mail.ru Агент, Skype, MS Teams* (если установлен адаптер) *, Telegram, XMPP, ВКонтакте, Почта на Клиенте, Почта в Браузере, FTP, Внешнее устройство, Облачное хранилище, Терминальная сессия, Печать, Чтение файла, Запись файла, Data Discovery.*
3. Решение пользователя. Возможные значения: *Нарушение, Нет нарушения, Решение не принято, Требуется дополнительный анализ.*
4. Вердикт. Возможные значения: *Разрешено, Заблокировано, Карантин.*
5. Статус отправки. Возможные значения*: Отправлено, Не отправлено, Ожидает отправки.*
6. Список сработавших политик.
7. Теги, присвоенные событию. Подробнее см. "Теги".
8. Индикатор снимков экрана. Отображается, если для персоны или компьютера были созданы снимки экрана.
9. Индикатор вложений. При наличии вложения отображается индикатор с указанием количества вложений. Вложения в архивах тоже учитываются.
10. Миниатюра снимка экрана. При наличии в событии снимка экрана отображается его уменьшенное изображение. Если нажать на миниатюру, будет открыто исходное изображение.

Дополнительную информацию о событии можно получить в краткой и детальной форме просмотра события.

Табличное представление событий

При просмотре событий в режиме таблицы отображается **табличное представление событий**:



Столбцы таблицы соответствуют атрибутам события. На вкладке **Столбцы** при создании или редактировании запроса можно выбрать те поля, которые будут отображаться в таблице (подробнее см. "Запросы").

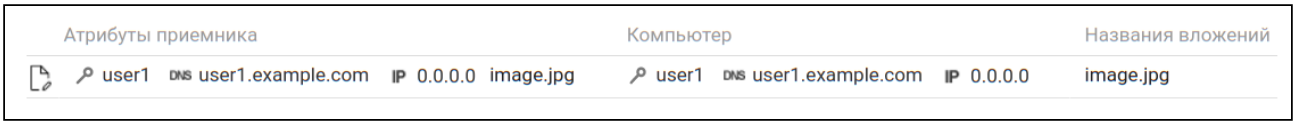
Чтобы изменить порядок сортировки строк в таблице, щелкните левой кнопкой мыши по заголовку того столбца, по которому нужно выполнить сортировку. Все записи таблицы будут отсортированы по возрастанию/убыванию значений выбранного атрибута.

Примечание:

Сортировка невозможна по столбцам *Тема письма*, *Тип компьютера*, *Дата создания файла*, *Дата изменения файла*, *Цель сканирования*, *Название задачи*, *Дата запуска задачи*, *Атрибуты приемника*, *Имя терминальной станции*, *Адрес вкладки браузера*.

Чтобы переместить столбец, щелкните левой кнопкой мыши по заголовку нужного столбца и, не отпуская кнопку, перемещайте заголовок столбца вдоль строки заголовков столбцов. Отпустите левую кнопку мыши, столбец будет перемещен на указанное место.

Столбец Атрибуты приемника:
Кроме столбцов, соответствующих одному атрибуту события, доступен агрегирующий столбец **Атрибуты приемника**.



В зависимости от типа события, столбец **Атрибуты приемника** может включать в себя информацию из следующих столбцов:

- *Название вложения*;
- *Путь к файлу или адрес приемника*;
- *Компьютер*;
- *Имя устройства приемника*;
- *Приложение-источник*;
- *Приложение-приемник*;
- *Получатели*.

Примечание:

По умолчанию столбец **Атрибуты приемника** не отображается в таблице и находится в списке **Доступные поля**.

Важно!

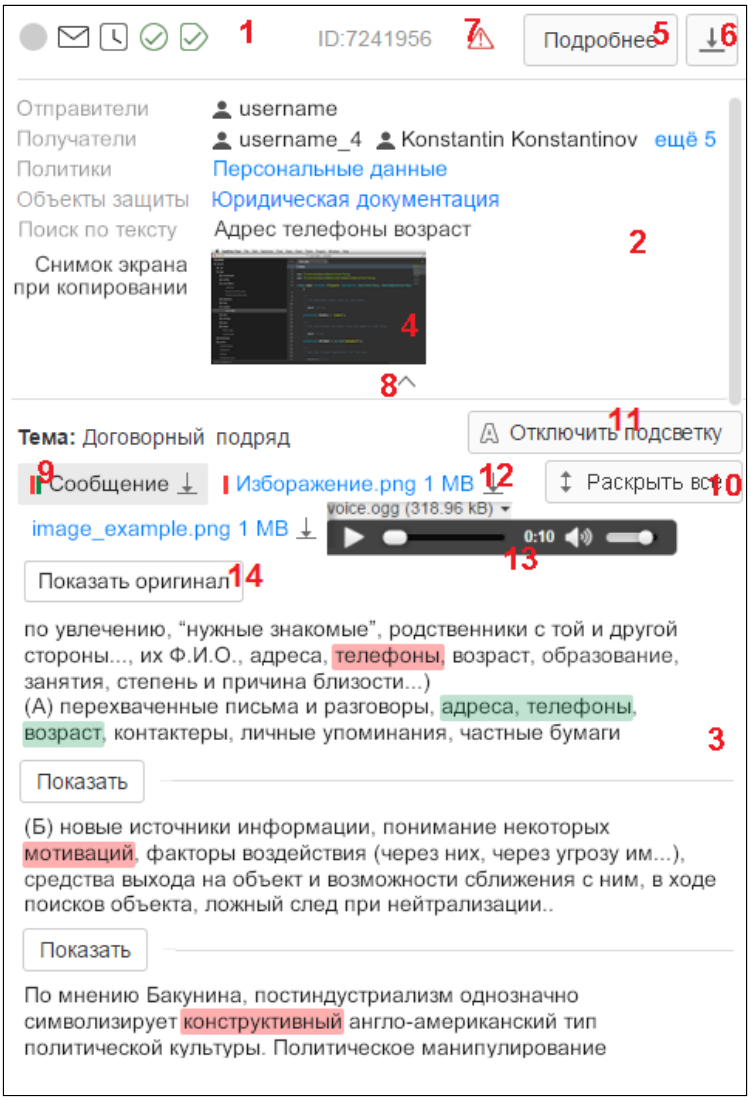
Столбец **Атрибуты приемника** не попадает в выгрузку событий, даже если он находится в списке **Отображаемые поля**.

Действия пользователя:

- Просмотр информации по событиям (см. "Просмотр событий")
- Определение полей просмотра (см. "Выбор полей просмотра событий")

Краткая форма просмотра событий

Краткая форма просмотра отображается в правой части рабочей области при выборе события в списке и позволяет получить основную информацию о событии.



Краткая форма просмотра содержит следующие области (набор элементов в каждой области может различаться в зависимости от типа события):

1. Верхняя часть формы (№ 1 на рисунке), где отображаются:
   - ID события;

- индикаторы атрибутов события: уровень нарушения, тип события, решение пользователя, вердикт, статус отправки (возможные значения атрибутов см. в статье "Плитка события");
- кнопка **Подробнее** (№ 5 на рисунке) для перехода к детальной форме просмотра события (см. "Детальная форма просмотра событий");
- кнопка  (№ 6 на рисунке), с помощью которой вы можете сохранить теневую копию события (см. "Сохранение события"). Отображается только для SMTP-писем;
- индикатор наличия ошибок обработки (№ 7 на рисунке). Отображается, если при обработке возникли ошибки. Подробную информацию о возникших ошибках можно получить в детальной форме просмотра.

2. Область просмотра параметров события (№ 2 на рисунке).
   В области просмотра параметров отображается информация об отправителях, получателях, мандатном уровне (для Traffic Monitor на ОС Astra Linux Special Edition "Смоленск"), сработавших политиках и объектах защиты. Ранее удаленные из Системы объекты защиты и политики обозначены красным.
   Для событий, содержащих снимок экрана, отображается его миниатюра (№ 4 на рисунке). Если нажать на миниатюру, будет открыто исходное изображение.
   Чтобы скрыть область просмотра параметров события, нажмите  (№8 на рисунке). Чтобы восстановить область просмотра параметров события, нажмите  .
3. Область просмотра содержимого события (№ 3 на рисунке).
   В области просмотра содержимого события отображаются текст письма, вложения, звуковые файлы.
   По умолчанию при отображении содержимого события используется подсветка результатов анализа: сработавшие объекты защиты выделены красным цветом, результаты поиска по тексту события – зеленым цветом. Цветовой индикатор (№ 9 на рисунке) указывает на наличие в событии сработавших объектов защиты и/или найденного текста.

   > **Примечание.**
   >
   > В краткой форме просмотра события все сработавшие объекты защиты выделены одним цветом. Чтобы получить наглядную информацию о том, каким объектам защиты соответствует выделенный текст, воспользуйтесь детальной формой просмотра события.

   По умолчанию отображается не весь текст события, а только фрагменты, в которых содержатся сработавшие объекты защиты или искомый текст. Чтобы раскрыть текст события между двумя фрагментами текста, нажмите **Показать**. Чтобы просмотреть весь текст события, нажмите **Раскрыть все** (№ 10 на рисунке).
   Для писем, содержащих HTML-разметку, и вложений, которые могут быть показаны в оригинальном формате (изображения, PDF), отображается кнопка, позволяющая выбрать режим просмотра сообщения (№ 14 на рисунке). Возможные значения:
   - **Показать извлеченный текст** – текст будет отображаться без форматирования. Позволяет увидеть скрытый текст (например, текст белого цвета или текст, содержащийся в названии картинки);
   - **Показать оригинал** – позволяет просмотреть картинки, таблицы и разметку текста.

Чтобы полностью отключить подсветку результатов анализа, нажмите **Отключить подсветку** (№ 11 на рисунке).
Если событие содержит перехваченное голосовое сообщение Skype, вы можете прослушать сообщение, используя инструменты для работы с голосовыми сообщениями (№ 13 на рисунке).

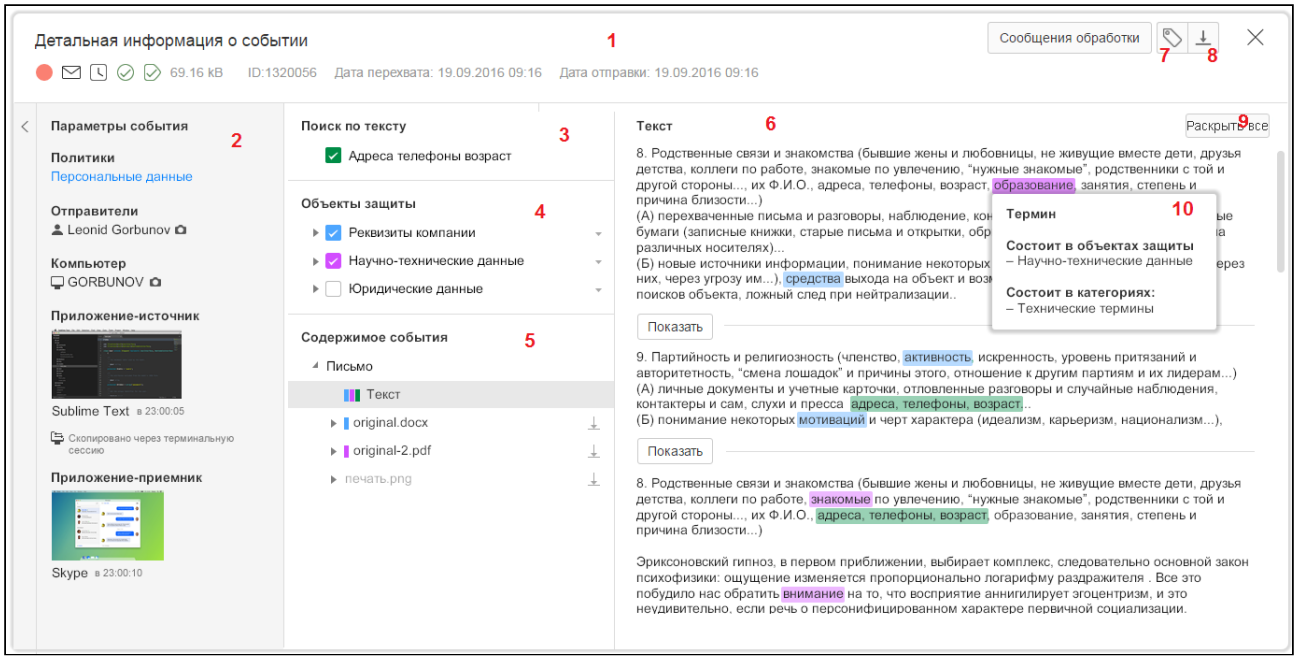
Чтобы сохранить вложение на компьютер, нажмите  (№ 12 на рисунке) рядом с названием нужного вложения.

Действия пользователя:

- Просмотр краткой формы события

Детальная форма просмотра событий

Детальная форма просмотра выбранного события открывается при нажатии кнопки **Подробно** в краткой форме просмотра (см. "Краткая форма просмотра событий").



Детальная форма просмотра содержит следующие области (набор элементов в каждой области может различаться в зависимости от типа события):

1. Верхняя часть формы (№ 1 на рисунке), где отображаются:
   - индикаторы атрибутов события: уровень нарушения, тип события, решение пользователя, вердикт, статус отправки (возможные значения атрибутов см. в статье "Плитка события");
   - размер события;
   - ID события;
   - дата и время перехвата события;
   - перехватчик, с помощью которого было получено событие;
   - кнопка **Сообщения обработки**, при нажатии на которую открывается окно, где отображаются системные сообщения об этапах обработки события и возникших ошибках;
   - кнопка  (№ 7 на рисунке), позволяющая установить событию тег (подробнее см. "Теги");

- кнопка  (№ 8 на рисунке), с помощью которой вы можете сохранить теневую копию события (см. "Сохранение события"). Отображается только для SMTP-писем.

2. Область **Параметры события** (№ 2 на рисунке), в которой отображается информация об отправителях, получателях, сработавших политиках, мандатном уровне (для Traffic Monitor на ОС Astra Linux Special Edition "Смоленск"), объектах защиты, периметрах и т.д. Для событий, содержащих снимок экрана, отображается его миниатюра.
3. Область **Поиск по тексту** (№ 3 на рисунке). Отображается, если в параметрах запроса был задан поиск по тексту события.
4. Область **Объекты защиты** (№ 4 на рисунке). Список сработавших объектов защиты и входящих в них элементов технологий. Ранее удаленные объекты защиты и элементы технологий обозначаются красным.
5. Область **Содержимое события** (№ 5 на рисунке). Отображает содержимое события: текст письма, вложения, звуковые файлы.

   Кнопка  напротив названия вложения позволяет сохранить выбранный файл на компьютер.

   > **Примечание:**
   >
   > Если событие содержит вложение, но имя вложения не было извлечено, то вместо имени будет отображаться MIME-тип файла.

6. Область просмотра (№ 6 на рисунке). Позволяет просмотреть текст сообщения и текст, извлеченный из вложений.

   > **Примечание:**
   >
   > Если текст извлечен агентом Device Monitor из PDF-документа, то текст будет включать в себя информацию о свойствах документа.

По умолчанию текст в области просмотра (№ 6 на рисунке) отображается в виде фрагментов, содержащих сработавшие объекты защиты или искомый текст.

Чтобы раскрыть текст события между двумя фрагментами текста, нажмите кнопку **Показать** между выбранными фрагментами. Чтобы просмотреть весь текст события, нажмите **Раскрыть все** (№ 9 на рисунке).

Для наглядного отображения объектов защиты и найденного текста внутри фрагментов используется подсветка. При включенной подсветке элементы выделяются следующим образом:

- Для каждого объекта защиты используется отдельный цвет. Все сработавшие элементы технологий, относящиеся к данному объекту защиты, выделены тем же цветом.
- Для сработавшей категории Автолингвиста в тексте выделяется до 50 терминов, относящихся к категории.

  > **Примечание:**

Подсветка терминов для категорий Автолингвиста не поддерживается для событий, созданных в Traffic Monitor версии 7.4 и ниже.

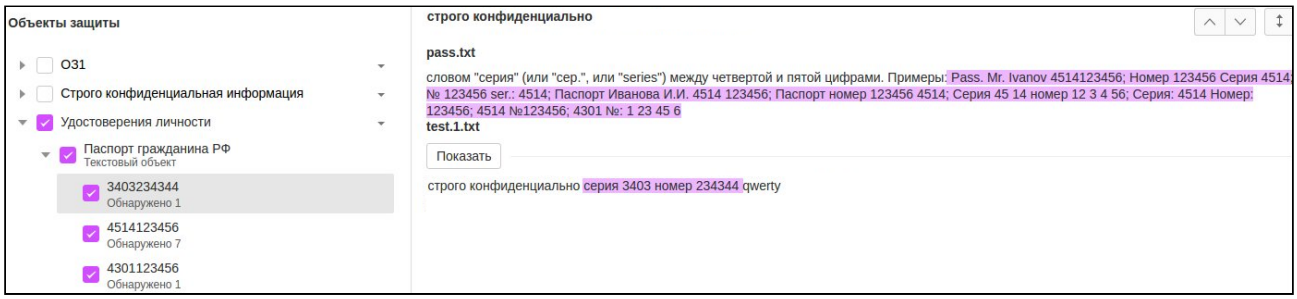
- Если часть текста относится сразу к нескольким элементам технологий, то такая часть текста выделяется серым цветом.
- Результаты поиска по тексту события выделены зеленым цветом. Результат выделяется зеленым цветом, даже если результат относится к элементам технологий.

Важно!

Если для анализа перехваченного текста применялась транслитерация, подсветка результатов анализа может отображаться со смещением.

Вы можете настроить подсветку в областях **Поиск по тексту** и **Объекты защиты**, устанавливая флажки напротив требуемых значений. Вы можете включить подсветку для выбранного поискового запроса по тексту события, для выбранных объектов защиты или отдельных элементов технологий, входящих в выбранный объект защиты.

Значения системных текстовых объектов, найденные в перехваченных данных, приводятся к нормальной форме. В результате в области **Объекты защиты** (№ 4 на рисунке) все значения одного системного текстового объекта будут иметь единую форму записи.



Примечание.

Для пользовательских текстовых объектов значения не приводятся к единой форме записи, поэтому в области **Объекты защиты** будет отображаться фактическое значение текстового объекта.

При наведении курсора на подсвеченный текст в области просмотра вы можете посмотреть дополнительную информацию об элементе (№ 10 на рисунке):

- для термина – категорию, в которую входит термин;
- для текстового объекта – название текстового объекта.

Чтобы полностью отключить подсветку, снимите все установленные флажки - в этом случае будет показан весь текст события без использования подсветки.

В области **Содержимое события** цветовой индикатор указывает, какие технологии сработали для данного элемента. Например, в событии на рисунке сработали следующие технологии:

- для вложения `original.docx` – объект защиты *Реквизиты компании*;
- для вложения `original-2.pdf` – объект защиты *Научно-технические данные*;

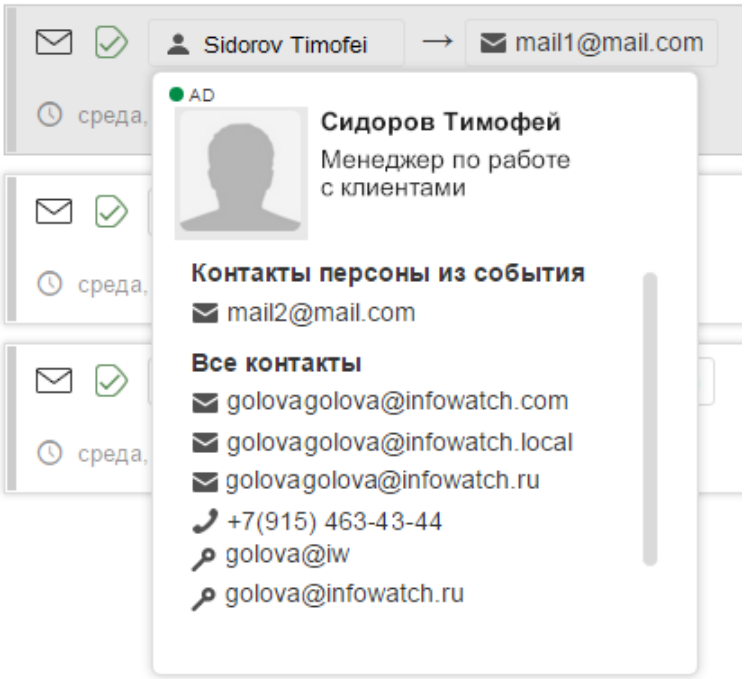
- для текста события – объект защиты *Реквизиты компании*, объект защиты *Научно-технические данные*, а также найден искомый текст.

Действия пользователя:

- Просмотр детальной формы события

3.2.3 Идентификация контактов в событии

На основе информации, извлеченной из события, Система определяет отправителей и получателей трафика (персон, группы персон, а также компьютеры). Этот процесс называется ***идентификацией*** контактов. Для идентифицированных отправителей и получателей на плитке события отображается имя персоны, имя компьютера или название группы, при нажатии на которое раскрывается карточка отправителя или получателя. Карточка содержит контакты, извлеченные из события, а также контактные данные, хранящиеся в Системе.



Если при обработке события Система определяет новые личные контакты персоны, найденные контакты автоматически добавляются в карточку персоны. Процесс автоматического добавление новых контактов имеющимся персонам называется ***пост-идентификацией***. В результате пост-идентификации в карточку персоны могут быть добавлены такие данные как адрес электронной почты, учетные данные мессенджеров (ICQ, Skype, Telegram, MS Teams (если установлен адаптер), WhatsApp), мобильный телефон, а также учетные записи в социальных сетях Facebook и Вконтакте.

Примечание.

Пост-идентификация позволяет определить контакты только для отправителей трафика. Для получателей трафика пост-идентификация не используется.

Примечание.

Для следующих ресурсов пост-идентификация не поддерживается:

- odnoklassniki.ru
- gmail.com

Пример:

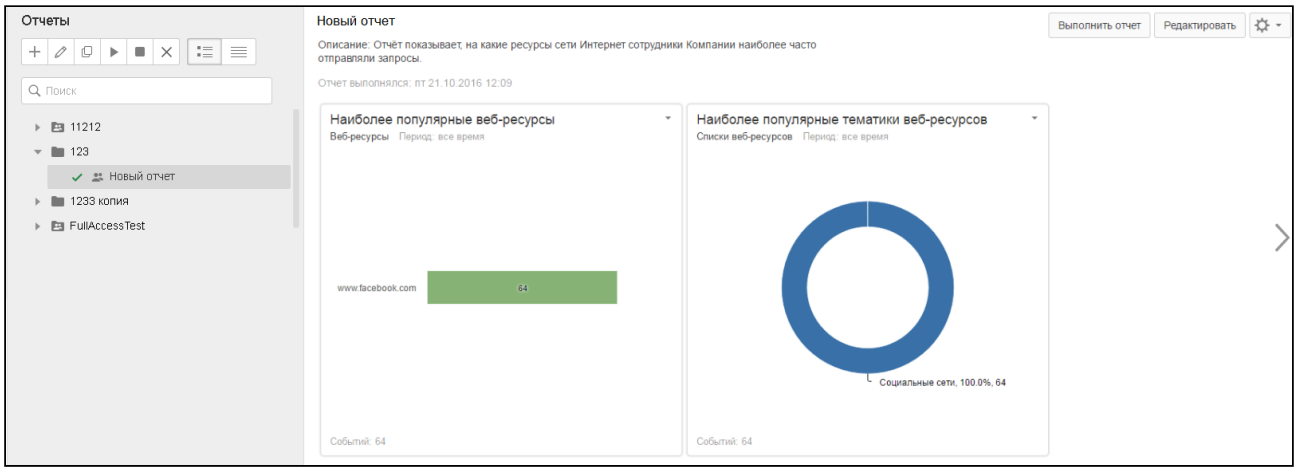
У разных пользователей, работающих на разных ПК, в личных карточках в Системе появляются одинаковые аккаунты мессенджеров (например, Skype) в виде контактов. Это происходит, если эти пользователи ранее заходили под одним доменным именем на разные ПК, либо под разными доменными именами на один и тот же ПК.

3.3 Раздел "Отчеты"

О разделе:

Раздел содержит список отчетов и средства для работы с ними.

Отчет представляет собой набор виджетов, на которых в виде графиков и диаграмм представлена выборка статистических данных о перехваченных объектах (см. "Виджеты отчетов").



В левой части рабочей области расположен список отчетов, панель инструментов и область поиска. В правой части рабочей области отображается форма просмотра выбранного отчета или форма создания/редактирования отчета (см. "Форма создания отчета").

Отчеты в списке могут располагаться как на верхнем уровне, так и внутри папок. Использование папок позволяет группировать отчеты, объединенные общей тематикой, определять права доступа сразу для всей группы отчетов, наследовать права доступа для вложенных папок и отчетов и т. д. Папка может включать как отчеты, так и вложенные папки. О том, как создать папку с отчетами, см. "Создание папки с отчетами".

Вы можете выбрать режим отображения папок и отчетов в списке: в виде папок (кнопка  на панели) или в виде плоского списка (кнопка  на панели).

Папки, доступные только владельцу, отмечены значком . Если папка доступна также другим пользователям Консоли, она имеет значок .

В папке **Предустановленные отчеты** содержатся следующие отчеты, доступные всем пользователям:

- *Статистика активности за последние 7 дней* – показывает информацию о количестве перехваченных Системой событий, наиболее активных отправителях и получателях, а также о наиболее популярных контентных маршрутах отправителей-получателей;
- *Активность в сети Интернет за последние 7 дней* – показывает, на какие ресурсы сети Интернет сотрудники компании наиболее часто отправляли запросы;
- *Передача защищаемых данных за последние 7 дней* – показывает, какие объекты защиты содержались в перехваченных Системой событиях, а также какие политики информационной безопасности были применены к событиям.

При создании отчета внутри папки права доступа либо наследуются из папки, либо задаются отдельно. Если, помимо владельца, отчет доступен также другим пользователям Консоли, отчет отмечен значком .

Чтобы просмотреть требуемую статистическую информацию, выберите нужный отчет в списке или создайте новый отчет (см. "Создание отчета").

> **Совет.**
>
> Для поиска папки или отчета по названию вы можете использовать поле **Поиск**.

Чтобы запустить выбранный отчет, нажмите  на панели инструментов или кнопку **Выполнить отчет** в правом верхнем углу формы. После того как выполнение отчета завершится, Система отобразит уведомление.

Если отчет уже выполнялся ранее и содержит актуальные данные, такой отчет отмечен значком . При выборе такого отчета справа отображаются виджеты со статистической информацией по объектам перехвата.

Если отчет в данный момент выполняется, рядом с его названием отображается значок . Для отчетов, выполнение которых завершилось с ошибкой, отображается значок .

При выборе отчета в списке в правом верхнем углу отображается кнопка , при нажатии на которую вы можете выбрать в раскрывающемся списке требуемое действие с отчетом:

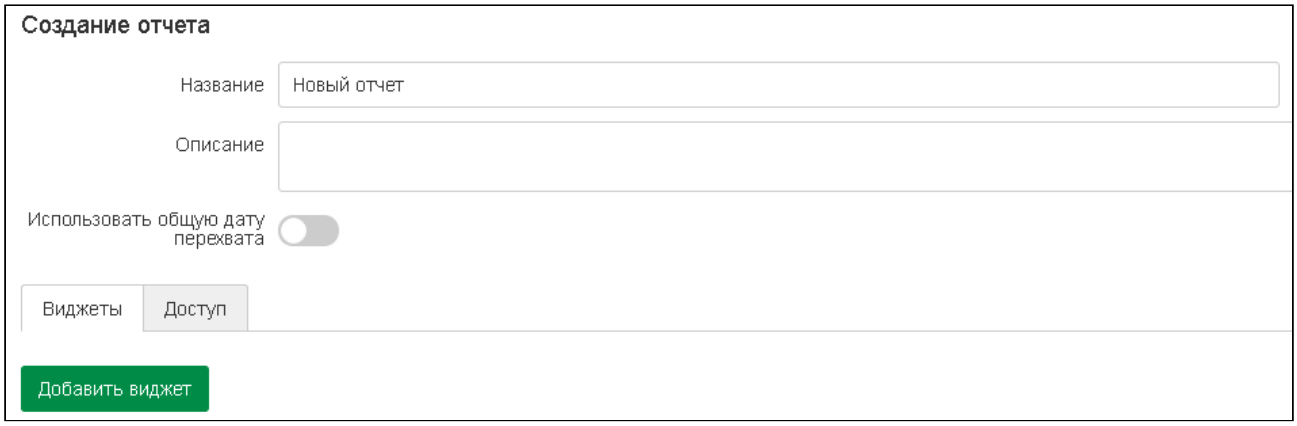
- перейти к истории выполнения отчета;
- копировать отчет;
- удалить отчет;
- сохранить отчет в виде файла в одном из поддерживаемых форматов.

Действия пользователя:

- Создание папки с отчетами
- Формирование отчета
- Создание и настройка виджета
- Просмотр готовых отчетов

3.3.1 Форма создания отчета

При создании или редактировании отчета отображается форма, где вы можете указать параметры отчета.



Для отчета указываются следующие параметры:

- **Название**;
- **Описание** (необязательный параметр);
- **Использовать общую дату перехвата** - отметьте эту опцию, если вы хотите, чтобы все запросы, используемые в виджетах отчета, формировались за один и тот же период. При выборе данной настройки появится выпадающий список, в котором вы можете указать требуемый период. По умолчанию эта настройка отключена, и для каждого виджета дата перехвата настраивается отдельно в параметрах запроса.
- **Виджеты** - с помощью кнопки **Добавить виджет** на вкладке **Виджеты** добавьте в отчет виджеты для отображения требуемой статистической информации (подробнее см. "Виджеты отчетов").
- **Доступ** - на вкладке **Доступ** укажите параметры доступа к отчету. Возможные варианты:
  - Если отчет создается внутри папки и для папки установлена настройка **Применить права для дочерних папок и отчетов**, то права доступа к отчету будут совпадать с правами, указанными для папки. Редактирование параметров доступа к отчету недоступно.
  - Если отчет создается внутри папки и настройка **Применить права для дочерних папок и отчетов** не установлена, либо отчет создается на верхнем уровне, то вы можете указать для него параметры доступа. По умолчанию отчет доступен только владельцу. Чтобы открыть доступ к отчету другим пользователям, выберите нужных пользователей в списке и установите напротив имени пользователя флажок в поле с требуемым уровнем доступа (**Просмотр и выполнение** либо **Полный доступ**).

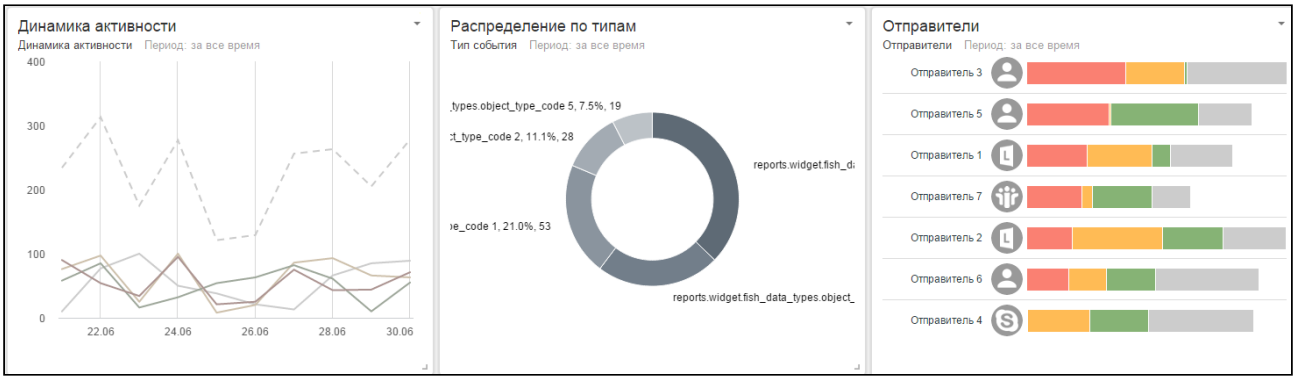
Действия пользователя:

- Создание отчета

3.3.2 Виджеты отчетов

Виджеты служат для отображения статистической информации в отчетах.

В результате выполнения отчета в правой части рабочей области отображаются виджеты с данными по перехваченным объектам за выбранный период времени.



Виджеты могут быть созданы для следующих данных:

Тип статистики	Описание
Веб-ресурсы	Веб-ресурсы, на которые сотрудники отправляли наибольшее число запросов
Диалоги	Маршруты передачи сообщений (без учета направления), для которых Системой зафиксировано наибольшее количество событий
Динамика активности	Динамика количества событий, перехваченных Системой
Каталоги объектов защиты	Каталоги объектов защиты, наиболее часто встречающиеся в перехваченных Системой данных
Компьютеры	Компьютеры, для которых Системой зафиксировано наибольшее количество событий
Объекты защиты	Объекты защиты, наиболее часто встречающиеся в перехваченных Системой данных
Отправители	Отправители, для которых Системой зафиксировано наибольшее количество событий
Политики	Политики, наиболее часто применявшиеся к перехваченным данным
Получатели	Получатели, для которых Системой зафиксировано наибольшее количество событий
Решения пользователей	Статистика решений, принятых офицером безопасности по событиям, перехваченным Системой
Списки веб-ресурсов	Наиболее частые тематики веб-ресурсов, на которые сотрудники отправляли запросы

Тип статистики	Описание
Типы событий	Распределение количества событий по типам (почта, Skype, внешние устройства и т.д.)

Для выбранного типа статистики можно указать один из следующих способов отображения данных:

-  – линейчатая диаграмма с группировкой;
-  – линейчатая диаграмма с накоплением;
-  – круговая диаграмма;
-  – график.

> **Примечание:**
>
> Для типа статистики "Динамика активности" можно использовать только диаграмму "График". Для всех остальных типов статистики диаграмма "График" недоступна.

Параметры виджета для типа статистики "Динамика активности":

Параметр	Описание
Уровни нарушений	В виджет будут добавлены события с указанным уровнем нарушения. Установите флажки напротив требуемых значений.
Период группировки	Укажите период, за который будут сгруппированы события. Доступные значения: • минута; • час; • день; • неделя; • месяц; • квартал; • год.

Параметры виджета для остальных типов статистики:

Параметр	Описание
Тип диаграммы	Доступны следующие типы: • линейчатая диаграмма с группировкой; • линейчатая диаграмма с накоплением; • круговая диаграмма (недоступно для типа статистики "Диалоги")

Параметр	Описание
Число записей	Число записей, которые будут отображаться на виджете. Укажите значение от 1 до 100. **Примечание**. Для типа статистики "Решения пользователей" данная настройка не отображается
Объединить остальные записи в пункт "Другое"	Отметьте эту настройку, если Вы хотите, чтобы на виджет был добавлен элемент "Другое", объединяющий оставшиеся записи. **Примечание**. Для типа статистики "Решения пользователей" данная настройка не отображается
Показывать значения	Отметьте эту настройку, если Вы хотите, чтобы на виджете отображались количественные значения
Показывать доли	Данная настройка доступна, если используется круговая диаграмма

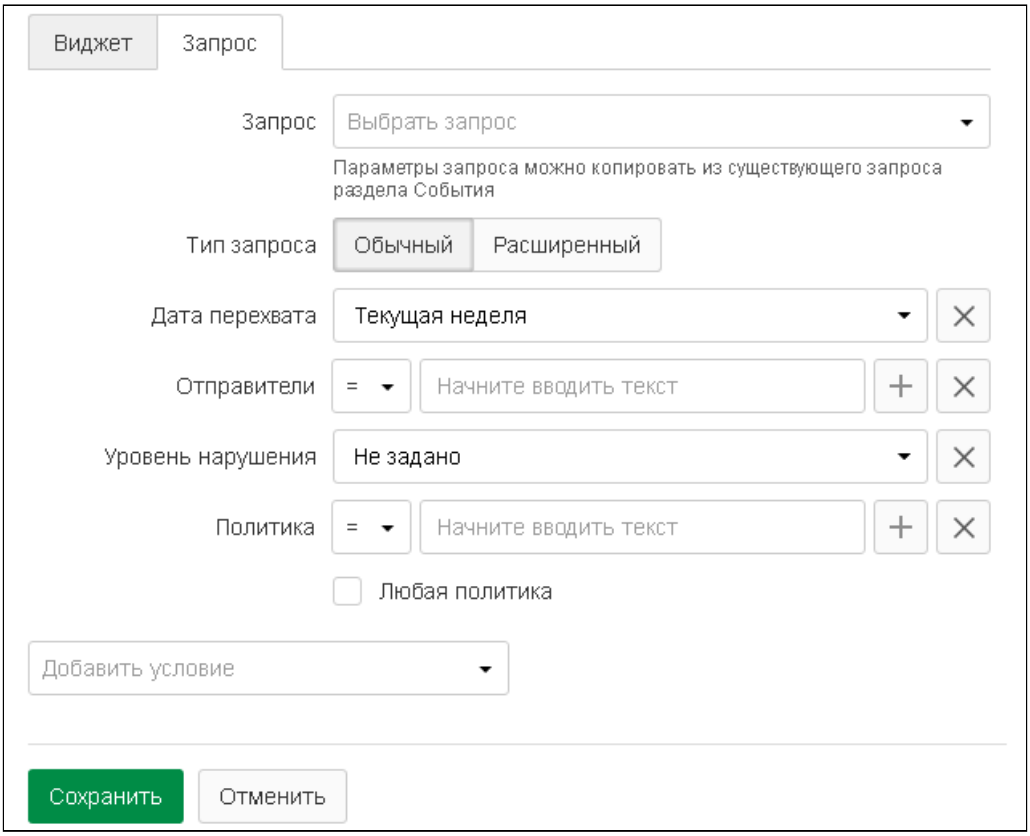
Действия пользователя:

- Настройка виджетов для отображения статистической информации (см. "Создание и настройка виджета")

3.3.3 Запросы

Запрос позволяет указать условия, в соответствии с которыми на виджете будет отображаться информация об объектах перехвата.

Для создания запроса перейдите на вкладку **Запрос** в окне создания виджета (см. "Виджеты отчетов").



Вкладка **Запрос** в окне создания виджета

Вы можете скопировать параметры запроса, добавленного в разделе "События" (для этого выберите название нужного запроса из раскрывающегося списка в поле **Запрос**), либо создать новый запрос.

Вы можете создать запрос в обычном или расширенном режиме:

- *Обычный режим* – позволяет указать значения параметров, при необходимости применяя к параметру знак неравенства ≠. При этом все условия будут объединены с помощью конъюнкции (логического "И"). Подробнее см. "Обычный режим создания запроса".
- *Расширенный режим* – позволяет выполнить более гибкую настройку условий поиска с использованием конъюнкции (логического "И") и дизъюнкции (логического "ИЛИ"). Подробнее см. "Расширенный режим".

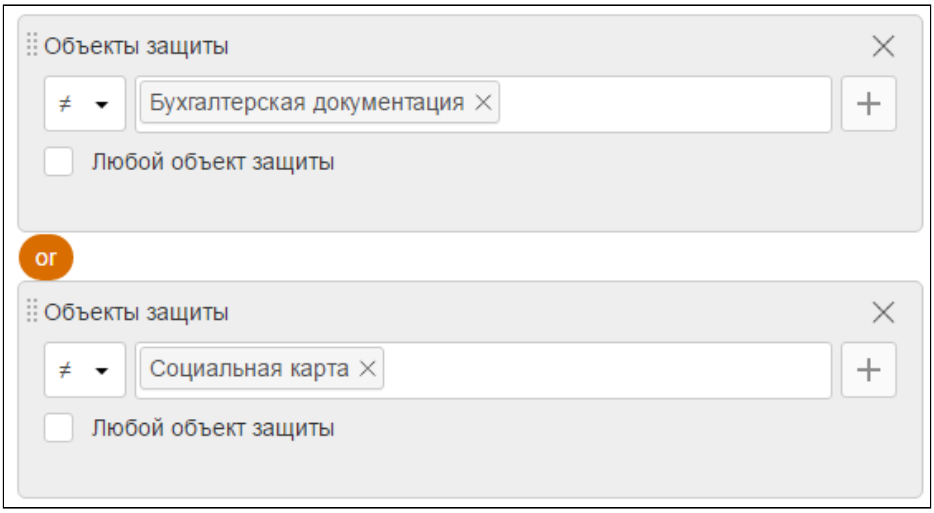
Для выбора режима используйте кнопки **Обычный** и **Расширенный** в поле **Тип запроса**.

Совет.

Если в процессе создания запроса в обычном режиме вы обнаружите, что вам требуется более гибкая настройка параметров, вы можете переключиться в расширенный режим создания запроса. При этом все введенные параметры запроса сохранятся.

Пример использовании дизъюнкции при создании запроса:

Если в условии параметры объединены с помощью логического "ИЛИ" и к ним применено отрицание, то отчет будет включать события, в которых одновременно не присутствуют все указанные элементы.



В данном примере событие не будет включено в отчет, если в нем присутствуют объекты защиты "Бухгалтерская документация" и "Социальная карта" одновременно.

Действия пользователя:

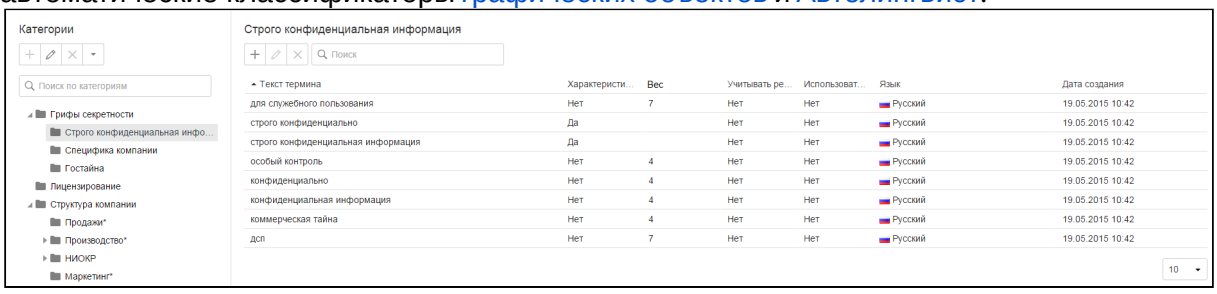
- Сформировать запрос (см. "Создание запроса в обычном режиме" и "Создание запроса в расширенном режиме").

3.4 Раздел "Технологии"

Справочная информация:
Технологии представляют собой совокупность данных, используемых при анализе объектов перехвата.

О разделе:
Раздел содержит:

- редактируемые справочники категорий и терминов, текстовых объектов, эталонных документов, бланков, печатей, выгрузок из БД;
- автоматические классификаторы графических объектов и Автолингвист.



Раздел **Технологии**, подраздел **Категории и термины**

Действия пользователя:

- Создание категорий и терминов
- Работа с текстовыми объектами
- Работа с эталонными документами
- Создание эталонных бланков
- Работа с печатями
- Работа с выгрузками
- Работа с графическими объектами

- Работа с Автолингвистом

3.4.1 Категории и термины

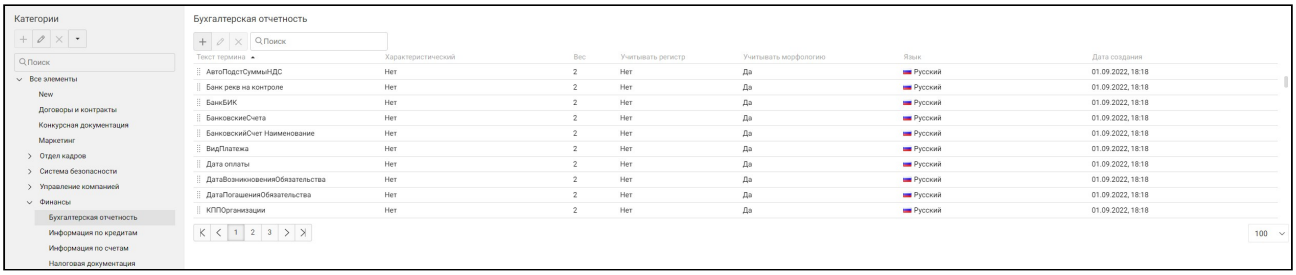
Справочная информация:

Категории и термины – это набор слов и словосочетаний, необходимых для проведения лингвистического анализа. Каждая категория содержит набор терминов.

Категории классифицируют возможные нарушения политики безопасности. Наличие в тексте термина, принадлежащего определенной категории, позволяет соотнести текст с этой категорией.

Например, категория *Бухгалтерская отчетность* содержит финансовую терминологию (*баланс*, *прочие расходы*, *ожидаемый бюджет* и пр.). Таким образом, наличие в тексте терминов "баланс", "прочие расходы" и "ожидаемый бюджет" позволяет соотнести текст с категорией *Бухгалтерская отчетность*.

В правой части рабочей области расположен список терминов внутри выделенной категории. Системой может осуществляться сквозной поиск термина по названию, поиск ведется в выбранной и во вложенных категориях. Чтобы осуществлять поиск во всех категориях раздела, выберите корневой каталог. Название термина вводится в строке поиска в правой части рабочей области.



Действия пользователя:

- Создание категорий и терминов (см. "Создание категорий и терминов")
- Импорт и экспорт категорий и терминов в составе базы технологий (см. "Экспорт и импорт базы технологий")
- Добавление категорий в объекты защиты (см. "Создание объекта защиты")

Категории

Справочная информация:

Категория представляет собой набор элементов, соответствующих определенной предметной области (например, *Договоры и контракты* или *Налоговая документация*). Содержит либо перечень категорий (подкатегорий), либо перечень терминов, характерных для данной категории.

Для категории указывается ее название и при необходимости добавляется описание.

Для терминов, входящих в категорию, указываются следующие атрибуты:

- Вес – значение от 1 до 10, указываемое для всех терминов категории в качестве атрибута **Вес.** Значение по умолчанию – 5;
- Язык – язык терминов категории. По молчанию установлен русский язык;
- Учитывать морфологию – при выборе данной настройки анализ выполняется с учетом всех морфологических форм термина. По умолчанию параметр включен;
- Учитывать регистр – при выборе данной настройки анализ выполняется с учетом регистра. По умолчанию параметр выключен.

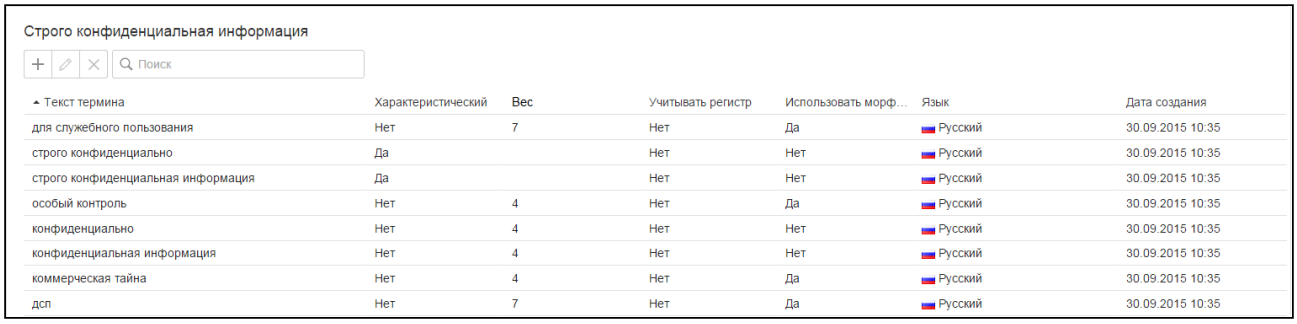
Для того чтобы категория детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

Действия пользователя:

- Создание категорий (см. "Создание категорий и терминов")
- Включение категорий в объекты защиты (см. "Создание объекта защиты")

Термины

Справочная информация:
Термин – слово или словосочетание, нахождение которого в анализируемом тексте увеличивает степень соответствия этого текста той категории, к которой относится найденный термин.


Строго конфиденциальная информация

Поиск

Текст термина	Характеристический	Вес	Учитывать регистр	Использовать морф…	Язык	Дата создания
для служебного пользования	Нет	7	Нет	Да	Русский	30.09.2015 10:35
строго конфиденциально	Да		Нет	Нет	Русский	30.09.2015 10:35
строго конфиденциальная информация	Да		Нет	Нет	Русский	30.09.2015 10:35
особый контроль	Нет	4	Нет	Да	Русский	30.09.2015 10:35
конфиденциально	Нет	4	Нет	Нет	Русский	30.09.2015 10:35
конфиденциальная информация	Нет	4	Нет	Нет	Русский	30.09.2015 10:35
коммерческая тайна	Нет	4	Нет	Да	Русский	30.09.2015 10:35
дсп	Нет	7	Нет	Да	Русский	30.09.2015 10:35

Атрибуты термина:

Параметр	Описание
Текст термина	Слово или словосочетание, длиной до 256 символов, состоящее только из букв, пробелов и дефисов
Характеристический	Если данный атрибут включен, нахождение в трафике термина обязательно присваивает объекту категорию, содержащую термин
Вес	Показатель относительной частоты встречаемости термина
Учитывать регистр	Показатель учета регистра при анализе трафика
Учитывать морфологию	Показатель использования морфологии при анализе трафика
Язык	Язык термина

Примечание:

Настройки параметров **Язык**, **Вес**, **Учитывать регистр** и **Учитывать морфологию для термина** задаются по умолчанию при указании аналогичных параметров для категории. Параметры термина могут быть отредактированы и сохранены отдельно, но при изменении настроек регистра и морфологии для категории данные изменения не будут повторно применяться к терминологии.

Действия пользователя:

- Создание и редактирование терминов (см. "Создание категорий и терминов")

Рекомендации по созданию категорий с терминами

Документы со сложнопредсказуемой структурой подлежат анализу так же, как все остальные типы документов. Подобные документы в больших объемах хранятся в системе документооборота организации: их создают, пересылают, распечатывают и т.д. Анализу подлежит содержание документов ввиду их принадлежности ограниченному числу тематик.

Пример:

Существует потребность фиксировать сообщения, содержащие документы налоговой отчетности, т.е. необходимо отследить все виды налоговых деклараций, отчетов о доходах или о налоговой задолженности, расчетам по авансовым платежам, справок о доходах, уведомлений в налоговые органы и др. Для решения этой задачи следует определить *ключевые слова*, которые могу встречаться во всех подобных документах. Такими словами могут быть, например, "вмененный доход", "расчет доходов и расходов", "представитель налогоплательщика" и т.д. В результате перехвачены могут быть совершенно разные документы: справка, декларация или статистическая форма по налогам . Система анализирует тематику документа.

Основные рекомендации для создания категорий с терминами:

1. В качестве терминов рекомендуется выбирать словосочетания (единицы, состоящие из нескольких слов). Если требуется сузить поиск и детектировать только один тип документов (например, только налоговые декларации, а статистические формы по налогам или справки относить к категории не нужно), то лучше выбирать словосочетание длиннее. Чем длиннее словосочетание, тем выше вероятность того, что оно не будет встречаться в других документах.

   Примечание:

   Максимальная длина термина составляет 256 символов.

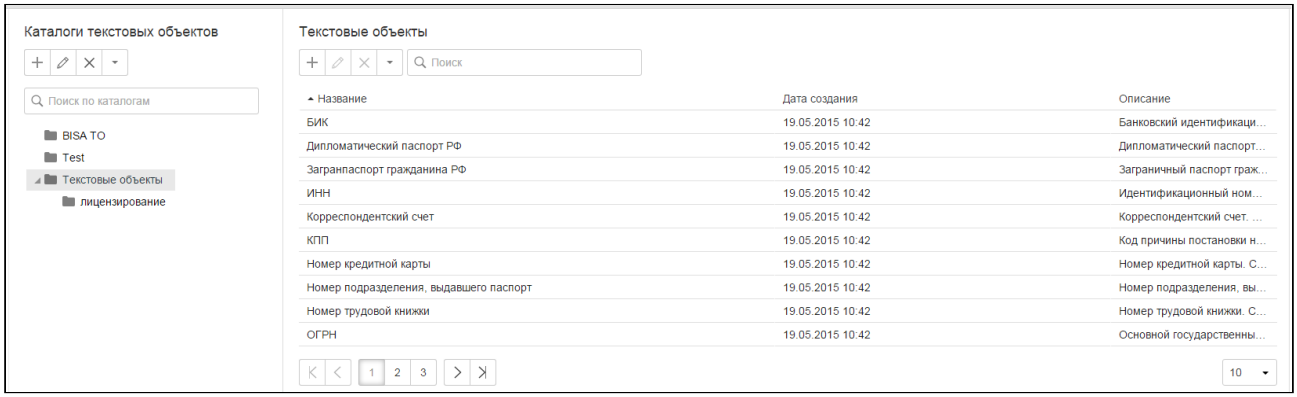
2. Следует избегать однословных терминов (особенно если слово является общеупотребимым – например, "труд", "высший", "проверил"), многозначных слов (например, "утечка" газа vs информации), служебных слов и слов с малой смысловой нагрузкой (например, "следовательно", "является" и пр.).
3. Текст термина может содержать алфавитные символы, пробел и дефис. Т.к. при лингвистическом анализе все знаки пунктуации и небуквенные символы игнорируются, то, например, термин "план на год" будет найден как в тексте "план на год", так и в тексте "план на 2022 год". Если же необходимо детектировать сообщения, содержащие небуквенные символы (к примеру, выражение "ТО.П234.67"), то выражение нужно внести как текстовый объект.
4. Характеристический термин показывает, что если он встречается в сообщении, то оно однозначно является релевантным данной категории. Таким образом, для отнесения

документа к той или иной тематике достаточно одного характеристического термина. Разных нехарактеристических терминов в тексте должно быть не меньше трех. Это необходимо, чтобы сработала категория с соответствующей тематикой.

5. Вес показывает частоту встречаемости терминов относительно друг друга в тексте. Мы рекомендуем не высчитывать частоту встречаемости каждого слова в текстах, а оставлять значение веса по умолчанию. Если при беглом взгляде на текст очевидно, какие слова встречаются чаще или реже остальных, то рекомендуется для более частотных терминов указывать вес выше, для менее частотных – ниже (например, в договорах термин "настоящий договор" встречается довольно часто, т.е. ему можно поставить максимальный вес). Это не скажется на точности детектирования и сократит время создания категории.
6. Язык терминов указывается для того, чтобы к терминам были корректно применены правила словоизменения (морфологии) того или иного языка.
7. Параметры морфологии и регистра связаны между собой: если выбрать значение "Учитывать морфологию", то регистр будет неактивным. И, наоборот. Также вы можете одновременно отключить оба параметра. Учет морфологии подразумевает возможность детектирования термина в его словоизменительных формах: например, на термин "тендеры" при включенной морфологии будут срабатывать слова "тендерами", "тендером", "тендера" и т.д. Учет регистра демонстрирует именно то написание, которое было внесено в текст термина. Например, если был создан термин "Котировок" с учетом регистра, то в текстах он будет детектироваться только в таком виде, т.е. на слова "котировок", "КОТИРОВОК", "кОтИрОвОк" категория срабатывать не будет.

3.4.2 Текстовые объекты

Справочная информация:
Текстовый объект – текстовая информация, извлеченная из тела объекта и его вложений. Не содержит элементов форматирования или разметки. Используется для решения задач анализа и поиска.



Текстовые объекты создаются внутри каталогов. Для работы с каталогами (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области. Текстовые объекты, входящие в каталог, и инструменты для работы с текстовыми объектами (создание, редактирование, удаление, сквозной поиск по каталогам) расположены в правой части рабочей области. Сквозной поиск осуществляется по названию текстового объекта и ведется в выбранном и во вложенных каталогах. Чтобы осуществлять поиск во всех каталогах раздела, выберите корневой каталог.

В Системе могут использоваться как системные текстовые объекты, так и текстовые объекты, созданные пользователем. Значение текстового объекта указывается с помощью шаблона.

При создании текстового объекта указывается его название и при необходимости добавляется описание. Чтобы добавить шаблон текстового объекта, перейдите в режим редактирования текстового объекта.

Для того чтобы текстовый объект детектировался в перехваченных данных, его необходимо включить в объект защиты.

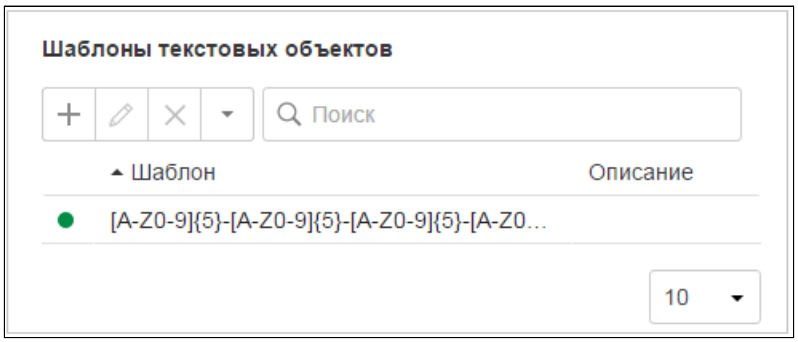
Действия пользователя:

- Создание текстовых объектов и их каталогов (см. "Работа с текстовыми объектами")
- Добавление системных текстовых объектов в выбранный каталог (см. "Работа с текстовыми объектами")
- Импорт и экспорт текстовых объектов в составе базы технологий (см. "Экспорт и импорт базы технологий")
- Добавление текстовых объектов в объекты защиты (см. "Создание объекта защиты")

Шаблоны текстовых объектов

Справочная информация:
Шаблон текстового объекта – значение текстового объекта, заданное в виде точной последовательности символов либо с помощью регулярного выражения. С помощью шаблона для каждого текстового объекта может быть задано одно или несколько значений.

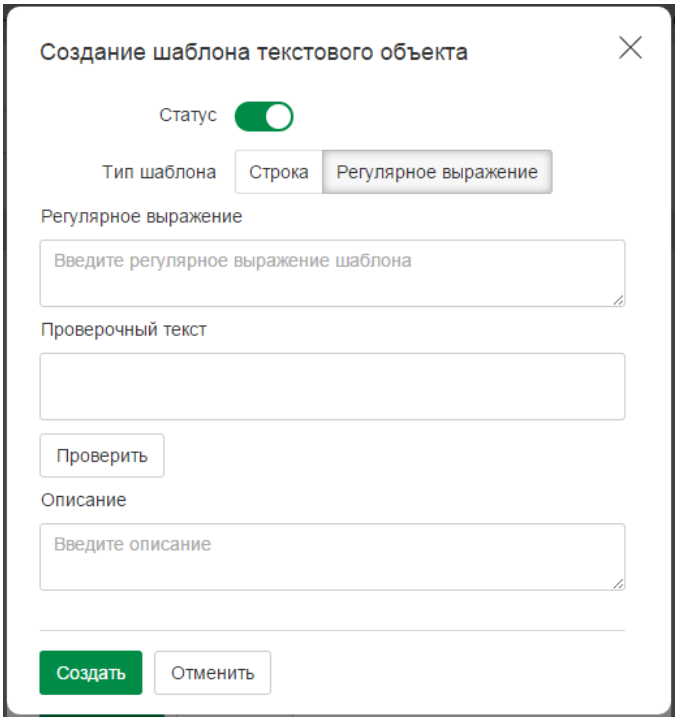
Шаблоны для выбранного текстового объекта отображаются при переходе в режим редактирования текстового объекта.



Панель инструментов содержит кнопки для создания, редактирования и удаления шаблонов. Кнопка позволяет изменить статус шаблона: для этого в раскрывающемся списке выберите **Активировать**/**Деактивировать**. Текущий статус шаблона отображается в левом столбце таблицы: активные шаблоны отмечены пиктограммой , неактивные - пиктограммой .

Важно!

Изменение и удаление предустановленных шаблонов для системных текстовых объектов недоступно.



При создании и редактировании шаблона вы можете указать следующие атрибуты:

Параметр	Описание
Статус	Показатель того, используется ли данный шаблон. Может принимать значения: *Активный* и *Неактивный*
Тип шаблона	Укажите, каким образом будет задан шаблон: в виде строки или регулярного выражения
Строка	Отображается, если выбран тип шаблона - *Строка*. Точное значение текстового объекта, заданное в виде последовательности символов. *Например*, шаблон `example@company.com` выявит в тексте только точное совпадение – `example@company.com`
Регулярное выражение	Отображается, если выбран тип шаблона – *Регулярное выражение*. Настраиваемый шаблон. Подробнее о регулярных выражениях см. статьи Базы знаний: "Синтаксис регулярных выражений" и "Описание макросов для шаблонов текстовых объектов"
Проверочный текст	Отображается, если выбран тип шаблона – *Регулярное выражение*. Пример текста для проверки нахождения регулярного выражения. Введите проверочный текст в поле и нажмите **Проверить**

Параметр	Описание
Описание	При необходимости добавьте описание шаблона

Действия пользователя:

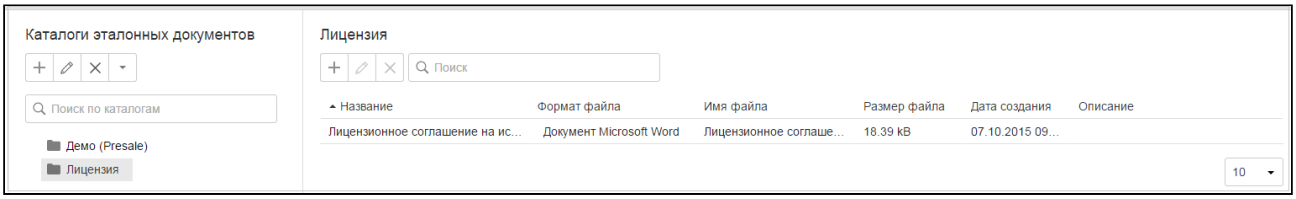
- Создание текстового объекта

3.4.3 Эталонные документы

Справочная информация:
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.

> **Важно!**
>
> Для корректной работы в Системе эталонный документ должен иметь следующие характеристики:
>
> - размер бинарных данных – от 128 байт до 128 Мбайт;
> - размер текстовых данных – от 128 байт до 30 Мбайт;
> - длина простого текста для текстовых данных – от 10 символов;
> - размер изображения – от 100 пикселей по одной стороне;
> - соотношение сторон изображения – не более 5:1;
> - размер векторных данных – от 300 Кбайт (800 примитивов);

Эталонные документы создаются внутри каталогов. Для работы с каталогами эталонных документов (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области.
В правой части рабочей области расположен список эталонных документов внутри выделенного каталога, а также инструменты для работы с эталонными документами (добавление, редактирование, удаление, сквозной поиск по каталогам). Сквозной поиск осуществляется по названию эталонного документа и ведется в выбранном и во вложенных каталогах. Чтобы осуществлять поиск во всех каталогах раздела, выберите корневой каталог.

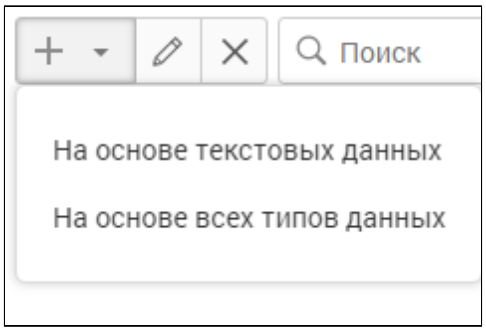


При создании каталога эталонных документов вы можете указать следующие атрибуты:

- **Название**;
- **Порог цитируемости для текстовых данных** – процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу. Для детектирования текстовых объектов (текста документов);

- **Порог цитируемости для бинарных данных** – процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу. Для детектирования бинарных объектов (рисунков, исполнимых файлов и проч.);
- **Описание**.

При добавлении в каталог эталонного документа укажите тип добавляемых данных (**Текстовые** или **Все типы**) и выберите файлы для загрузки.



При редактировании выбранного эталонного документа вы можете указать следующие атрибуты:

- **Название**;
- **Порог цитируемости для текстовых данных** – процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу. Используется для детектирования текстовых объектов (текста документов);
- **Порог цитируемости для бинарных данных** – процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу. Используется для детектирования бинарных объектов (рисунков, исполняемых файлов и проч.);
- **Описание**.

Переход в режим обновления эталонного документа выполняется с помощью кнопки **Обновить** в окне редактирования документа.

Для того чтобы эталонный документ детектировался в перехваченных данных, его необходимо включить в объект защиты.

Действия пользователя:

- Создание эталонных документов и их каталогов (см. "Работа с эталонными документами")
- Импорт и экспорт эталонных документов в составе базы технологий (см. "Экспорт и импорт базы технологий")
- Обновление эталонного документа (см. "Работа с эталонными документами")
- Добавление эталонных документов в объекты защиты (см. "Создание объекта защиты")
- Работа с автоматическими эталонными документами (см. "Автоматические эталонные документы")

Автоматические эталонные документы

Автоматически эталонные документы созданы внешней системой и добавлены в Traffic Monitor одним или несколькими способами:

- с помощью адаптера из сетевого каталога (об установке и работе адаптера см. документ "InfoWatch Sample Documents Autoupdate Adapter. Руководство по установке и

конфигурированию").
или

- через программный интерфейс (подробнее см. "InfoWatch Traffic Monitor. Руководство администратора", раздел "Загрузка эталонных документов и выгрузок из БД в Traffic Monitor (REST API SDK)").

Внешняя система (коннектор) инициирует добавление и последующее обновление автоматических эталонных документов.

> **Важно!**
>
> Одновременное редактирование конфигурации через Консоль управления и через SDK может вызвать конфликт, поэтому при разработке коннектора рекомендуется ознакомиться с общими принципами работы с конфигурацией Системы. В случае возникновения конфликта следует, в первую очередь, просмотреть ошибки, возвращаемые коннектору от SDK.

Эталонные документы, созданные внешней системой, помещаются в предустановленный каталог **Автоматические эталонные документы**. Авторизация внешней системы в Traffic Monitor осуществляется с помощью плагина (об установке плагина см. документ "*InfoWatch Traffic Monitor*. Руководство администратора").

Просмотр и редактирование каталога **Автоматические эталонные документы** доступны по умолчанию. Для всех автоматических эталонных документов, содержащихся в каталоге, доступны операции редактирования и удаления. Данные операции выполняются с помощью кнопок на панели инструментов в правой части рабочей области. Обновление автоматических эталонных документов выгрузки невозможно произвести вручную в консоли Traffic Monitor. Чтобы автоматический эталонный документ детектировался в перехваченных данных, его необходимо включить в объект защиты.

3.4.4 Бланки

Справочная информация:
Бланк – бланк, версия которого ищется в сетевом трафике. Бланки хранятся в Системе в виде цифровых отпечатков, текст недоступен для просмотра ни пользователям, ни администраторам Системы.
В качестве бланков могут выступать анкеты, опросные листы и другие документы, заполняемые по заранее заданной форме.
На техническом уровне бланк – это файл, каждая строка которого содержит одно поле бланка, строки отделяются друг от друга переносом строки, и бланк содержит минимум 2 поля.

> **Важно!**
>
> Для корректной работы в Системе бланк должен иметь следующие характеристики:
>
> - размер текстовых данных – до 30 Мбайт;
> - размер векторных данных – от 300 Кбайт (800 примитивов);
> - количество полей, состоящих из более, чем 1 слова, – 1-2 поля.

Принцип работы технологии: осуществляется поиск наименования полей бланка в тексте события и затем проверяется порядок их следования, при необходимости проверяется присутствие текста между полями бланка, на базе чего определяется, был ли бланк заполнен.

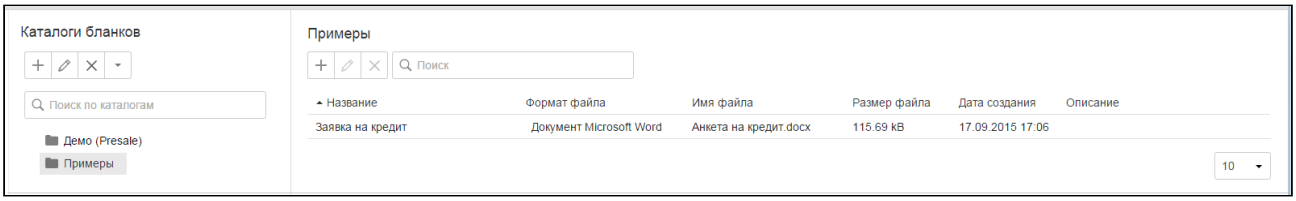
Для того чтобы бланк детектировался в перехваченных данных, его необходимо включить в объект защиты.

Важно!

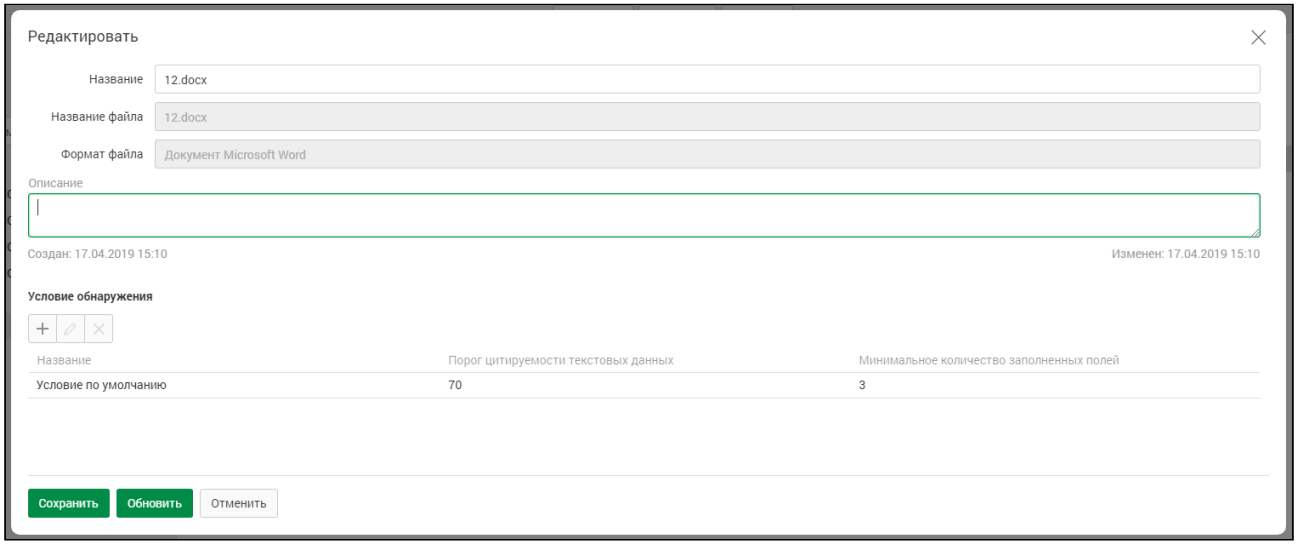
Для соотнесения объекта перехвата с бланком необходимо, чтобы выполнялись следующие условия:

- в тексте объекта должно содержаться хотя бы одно поле из бланка;
- если количество обнаруженных в тексте объекта полей более одного, то поля должны располагаться в том порядке, который имеется в загруженном в Систему цифровом отпечатке;
- если настроено детектирование заполненных бланков, то между парой соседних строк должен быть хотя бы один символ.

Бланки создаются внутри каталогов. Для работы с каталогами бланков (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области. В правой части рабочей области расположен список бланков внутри выделенного каталога, а также инструменты для работы с бланками (добавление, редактирование, удаление, сквозной поиск по каталогам). Сквозной поиск осуществляется по названию бланка и ведется в выбранном и во вложенных каталогах. Чтобы осуществлять поиск во всех каталогах раздела, выберите корневой каталог.



В режиме редактирования бланка вы можете просмотреть и при необходимости изменить атрибуты выбранного бланка, а также перейти к обновлению бланка, нажав на кнопку **Обновить**.
Условия обнаружения задаются только в режиме редактирования бланка.



Действия пользователя:

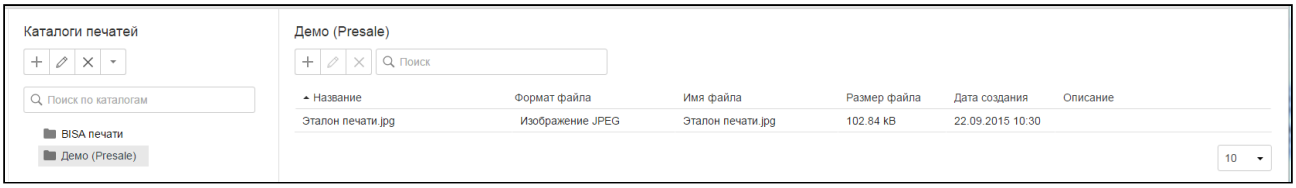
- Создание бланков и их каталогов (см. "Работа с бланками")

- Импорт и экспорт бланков в составе базы технологий (см. "Экспорт и импорт базы технологий")
- Создание условий обнаружения и обновление бланка (см. "Работа с бланками")
- Добавление бланков в объекты защиты (см. "Создание объекта защиты")

3.4.5 Печати

Справочная информация:
Печать – изображение печати, которое ищется в сетевом трафике. Печатями могут быть изображения круглых и треугольных оттисков, которые используются в организациях.

Печати создаются внутри каталогов. Для работы с каталогами печатей (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области. В правой части рабочей области расположен список печатей внутри выделенного каталога, а также инструменты для работы с печатями (добавление, редактирование, удаление, сквозной поиск по каталогам). Сквозной поиск осуществляется по названию и ведется в выбранном и во вложенных каталогах. Чтобы осуществлять поиск во всех каталогах раздела, выберите корневой каталог.



Для успешной загрузки печати (круглой или треугольной) в Систему необходимо соблюсти следующие условия:

- изображение печати выполнено на белом фоне с минимальным количеством белого пространства по краям от печати;
- разрешение печати не менее 150 dpi;
- минимальный размер изображения – 500x500 пикселей;
- максимальный размер изображения – до 30 Мбайт;
- все элементы печати хорошо видны;
- печать имеет сплошную рамку по периметру;
- ***треугольная*** печать расположена основанием вниз, основание – строго горизонтально.

Для того чтобы печать детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

Действия пользователя:

- Создание печатей и их каталогов (см. "Работа с печатями")
- Добавление печатей в объекты защиты (см. "Создание объекта защиты")
- Экспорт и импорт печатей в составе базы технологий (см. "Экспорт и импорт базы технологий")

3.4.6 Выгрузки из БД

Справочная информация:
Выгрузка из БД – часть базы данных, цитаты из которой ищутся в анализируемом тексте. Выгрузкой из БД может быть список заработных плат сотрудников, личные данные и прочее.

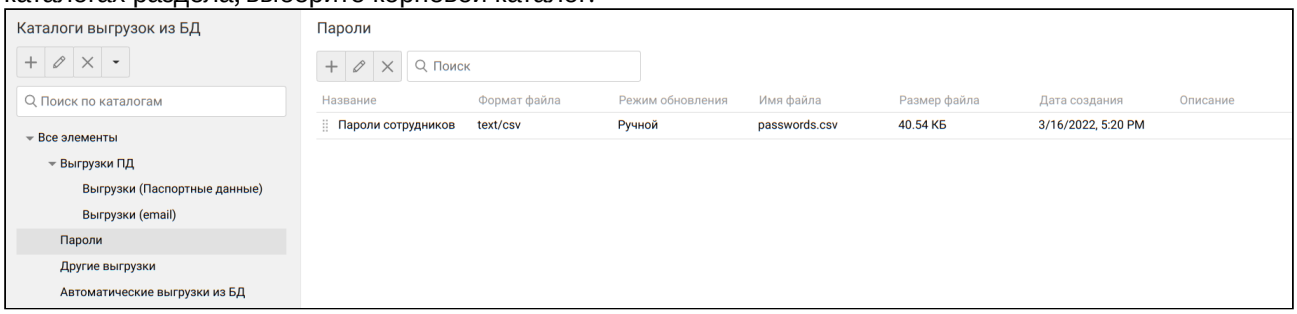
Важно!

Для корректной работы в Системе выгрузка из БД должна иметь следующие характеристики:

- формат файла выгрузки – CSV или TSV;
- размер файла – от 128 байт до 300 МБ;
- количество столбцов – не более 32;
- количество слов в ячейке – не более 256;
- количество строк – не более 1 млн (при объеме оперативной памяти сервера 8 ГБ) или не более 3,5 млн (при объеме оперативной памяти сервера 16 ГБ);
- количество символов в шапке таблицы (первой строке) – не более 4000, включая названия столбцов и дополнительные символы, используемые форматами CSV и TSV для разделения столбцов: кавычки, запятые.

Выгрузки создаются внутри каталогов. Для работы с каталогами выгрузок (создание, редактирование, перемещение, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области. Выгрузки, входящие в каталог, и инструменты для работы с выгрузками расположены в правой части рабочей области.

В правой части рабочей области расположен список выгрузок внутри выделенного каталога, а также инструменты для работы с выгрузками (создание, редактирование, удаление, перемещение и копирование выгрузок; сквозной поиск по каталогам). Сквозной поиск осуществляется по названию выгрузки и ведется в выбранном и во вложенных каталогах. Чтобы осуществлять поиск во всех каталогах раздела, выберите корневой каталог.



Предустановленный каталог **Автоматические выгрузки из БД** содержит выгрузки, полученные от внешней системы (подробнее см. "Автоматически обновляемые выгрузки из БД").

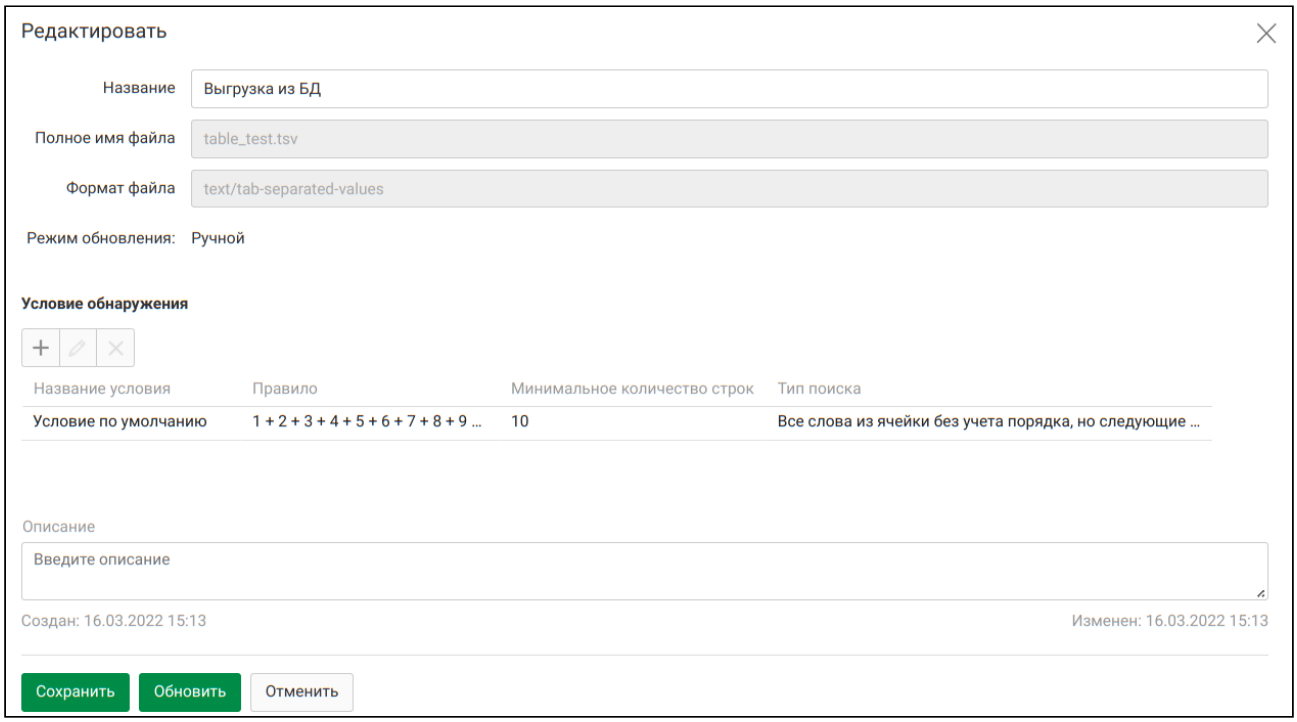
Примечание:

Каталог **Автоматические выгрузки из БД** является системным, и для него недоступна операция удаления.

В режиме редактирования выгрузки отображаются условия обнаружения. Условия обнаружения определяют:

- логические взаимоотношения между столбцами таблицы;
- минимальное количество строк из выгрузки в анализируемом тексте, которое необходимо для выполнения условия;
- тип поиска цитат в тексте.

Чтобы перейти в режим обновления выгрузки, нажмите **Обновить**.



Для того чтобы выгрузка детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

Устаревшие выгрузки:
Устаревшая выгрузка – выгрузка, созданная в Traffic Monitor версии ниже 7.4. Устаревшая выгрузка может быть добавлена в Систему:

- при импорте базы технологий/объектов защиты из Traffic Monitor версии ниже 7.4;
- при обновлении Traffic Monitor с версии ниже 7.4.

Устаревшие выгрузки отмечены в интерфейсе символом .

Важно!

Для устаревшей выгрузки недоступно редактирование и обновление. Рекомендуется удалить устаревшую выгрузку и создать ее повторно.

Действия пользователя:

- Создание выгрузок из БД и их каталогов (см. "Работа с выгрузками")
- Обновление выгрузки (см. "Работа с выгрузками")
- Перемещение/копирование выгрузок (см. "Работа с выгрузками")
- Добавление условий обнаружения выгрузки (см. "Условия обнаружения выгрузки")
- Автоматическое обновление выгрузки (см. "Автоматически обновляемые выгрузки из БД")

- Добавление выгрузок в объекты защиты (см. "Создание объекта защиты")

Автоматически обновляемые выгрузки из БД

Автоматически обновляемые выгрузки из БД – это выгрузки, созданные внешней системой. Внешняя система (коннектор) инициирует добавление и последующее обновление автоматических выгрузок.

> **Важно!**
>
> Одновременное редактирование конфигурации через Консоль управления и через SDK может вызвать конфликт, поэтому при разработке коннектора рекомендуется ознакомиться с общими принципами работы с конфигурацией Системы. В случае возникновения конфликта следует, в первую очередь, просмотреть ошибки, возвращаемые коннектору от SDK.

Выгрузки, созданные внешней системой, помещаются в предустановленный каталог **Автоматические выгрузки из БД**. Авторизация внешней системы в Traffic Monitor осуществляется с помощью плагина (об установке плагина см. документ "*InfoWatch Traffic Monitor*. Руководство администратора").

> **Примечание.**
>
> Просмотр и редактирование каталога **Автоматические выгрузки из БД** доступны при наличии лицензии на использование данной технологии.

При создании выгрузки атрибуты автоматической выгрузки формируются на основе следующих данных, переданных от внешней системы:

Параметр	Описание
Наименование	Название выгрузки из БД
Список столбцов	Список столбцов выгрузки. На основе списка формируется условие обнаружения выгрузки по умолчанию (см. "Условия обнаружения выгрузки")
Комментарий	Сопроводительная информация

> **Примечание.**
>
> При создании новой выгрузки файл выгрузки может быть пустым, если:
>
> - загрузка содержимого завершилась принудительно;
> - при загрузке содержимого оборвалась связь;
> - валидация содержимого завершилась с ошибкой.

Если в Системе создалась пустая выгрузка, то при восстановлении работоспособности стороннее приложение может воспользоваться уже созданной пустой выгрузкой и наполнить ее, не создавая выгрузку заново.

Обновление автоматической выгрузки невозможно произвести вручную в консоли Traffic Monitor.

Для всех выгрузок, содержащихся в каталоге, доступны операции редактирования и удаления. Данные операции выполняются с помощью кнопок на панели инструментов в правой части рабочей области.

Важно!

При удалении выгрузки, созданной внешней системой, автоматическое обновление данной выгрузки будет недоступно.

Важно!

Для устаревших автоматических выгрузок недоступно редактирование и обновление. Рекомендуется удалить устаревшую выгрузку и создать ее повторно.

Для того чтобы автоматическая выгрузка детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

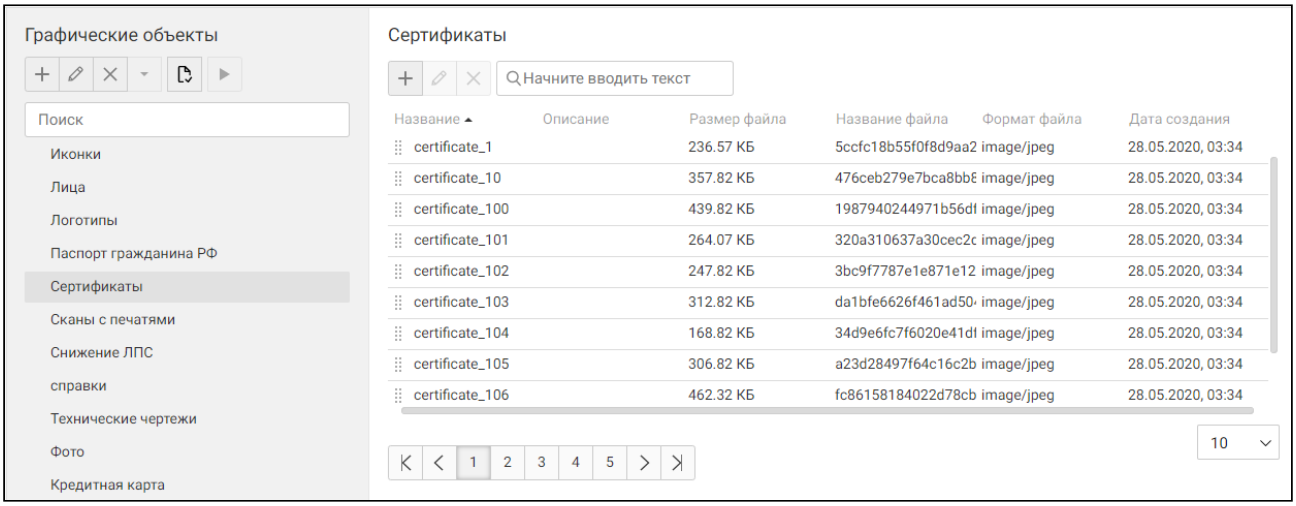
3.4.7 Графические объекты

Справочная информация:

Графические объекты – технология анализа изображений или иных графических данных, извлеченных из тела объекта и его вложений.

Графические объекты состоят из категорий, содержащих документы. Для работы с категориями (создание, редактирование, удаление категорий, проверка, обучение, поиск по категориям) используются инструменты в левой части рабочей области.

В правой части рабочей области расположен список документов внутри выбранной категории графических объектов, а также инструменты для работы с документами: добавление, редактирование, удаление, сквозной поиск, который осуществляется по названию документа и ведется только в выбранной категории.



В соответствии с типом действующей лицензии в Системе могут содержатся следующие предустановленные графические объекты:

- Паспорт гражданина РФ;
- Технические чертежи;
- Географические карты;
- Сертификаты;
- Лица;
- Фото;
- Сканы с печатями;
- Иконки;
- Логотипы;
- Снижение ЛПС;
- а также нередактируемые графические объекты:

Название	Описание
Кредитная карта	Изображение лицевой стороны банковских карт VISA, Visa Electron, MasterCard, Maestro, Мир
Идентификационная карта гражданина Малайзии	Группа идентификационных документов граждан Малайзии, включающая в себя: • MyKad – общая карточка для граждан Малайзии старше 12 лет (лицевая сторона) • MyKid – карточка для детей младше 12 лет (лицевая сторона) • MyPR – карточка для жителей Малайзии, получивших вид на жительство (лицевая сторона) • MyTentera – карточка для служащих армии (лицевая сторона)

При необходимости вы можете расширить набор графических объектов, обучив Автоматический классификатор детектировать другие типы изображений: паспорт гражданина РФ, сертификаты, изображения лиц, фото, технические чертежи, географические карты, отсканированные изображения печатей, иконки, логотипы, снижение ЛПС, а также создать собственные графические

объекты. Обучение предустановленной коллекции графических объектов произойдет автоматически при установке действующей лицензии на технологию.

Чтобы графический объект детектировался в перехваченных данных, его необходимо включить в объект защиты. Для этого создайте объект защиты с использованием графических объектов (см. "Создание объекта защиты").

Действия пользователя:

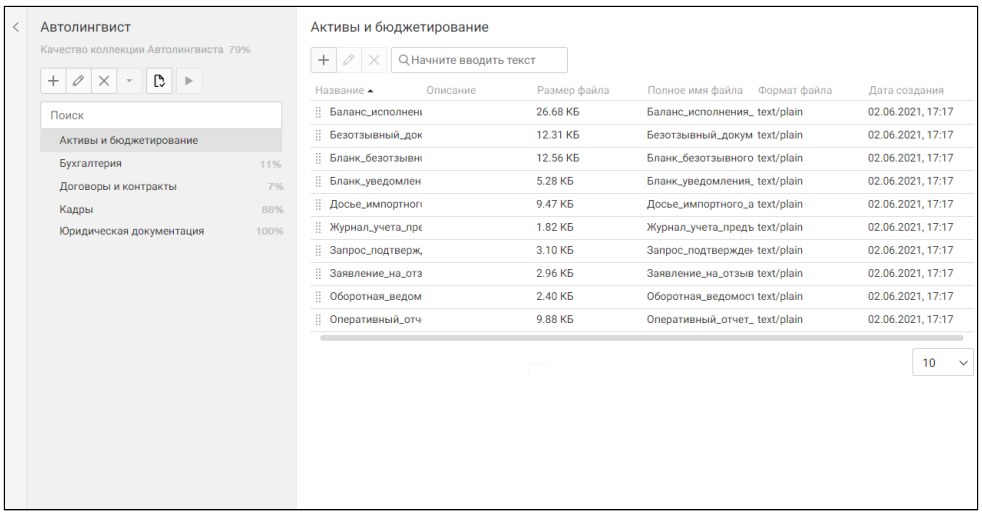
- Создание категорий (см. "Работа с графическими объектами")
- Добавление документов (см. "Работа с графическими объектами")
- Обучение классификатора (см. "Работа с графическими объектами")
- Проверка файлов на классификаторе (см. "Работа с графическими объектами")
- Импорт и экспорт графических объектов в составе базы технологий (см. "Экспорт и импорт базы технологий")
- Добавление графических объектов в объекты защиты (см. "Создание объекта защиты")

3.4.8 Автолингвист

Справочная информация:

Автолингвист – технология анализа текстовых данных. Если вам необходимо защитить большой набор типовых документов компании, данная технология позволяет автоматически классифицировать подобные документы для максимально эффективного обнаружения конфиденциальных данных в перехваченном трафике. При этом все типовые документы разделяются по тематикам - категориям, которые могут соответствовать различным департаментам внутри организации: документы о неразглашении, тендерная документация и т.д. Текстовые документы, загруженные на обучение в Автолингвист, используются при создании объектов защиты.

Для работы с категориями документов (создание, редактирование, удаление категорий, поиск по категориям) используются инструменты в левой части рабочей области. Внутри категорий Автолингвиста создаются документы.
В правой части рабочей области расположен список документов внутри выделенной категории, а также инструменты для работы с документами (добавление, редактирование, удаление, сквозной поиск по документам). Сквозной поиск осуществляется по названию документа и ведется только в выбранной категории.



Действия пользователя:

- Создание категорий (см. "Работа с Автолингвистом")
- Добавление документов (см. "Работа с Автолингвистом")
- Обучение классификатора (см. "Работа с Автолингвистом")
- Проверка файлов на классификаторе (см. "Работа с Автолингвистом")
- Импорт и экспорт текстовых объектов в составе базы технологий (см. "Экспорт и импорт базы технологий")
- Добавление текстовых объектов в объекты защиты (см. "Создание объекта защиты")

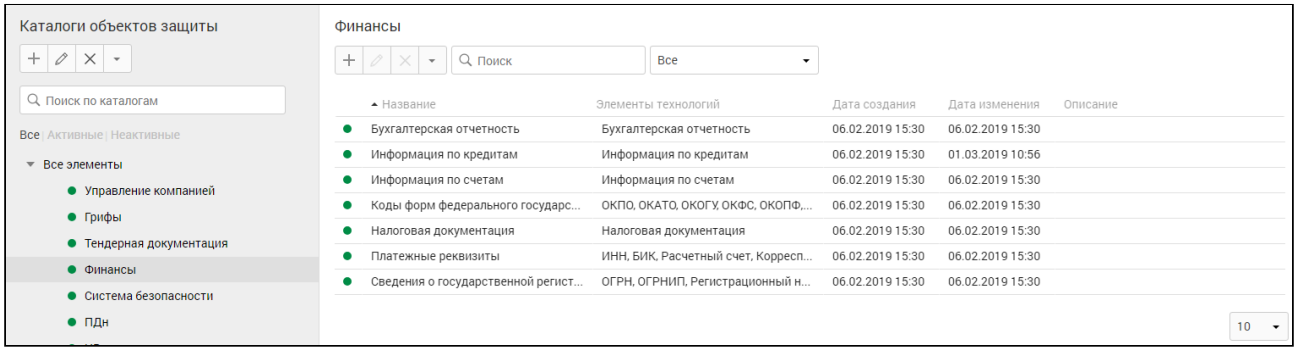
3.5 Раздел "Объекты защиты"

Справочная информация:

Объект защиты представляет собой совокупность элементов технологий в содержимом событий. Объекты защиты используются для определения соответствия перехваченных данных определенным бизнес-документам.

О разделе:

Раздел содержит объекты защиты, сгруппированные в каталоги, и инструменты для работы с ними.



Список каталогов расположен в левой части рабочей области, содержит как пользовательские, так и предустановленные каталоги объектов защиты.

Для каждого каталога отображается его статус (*Активный*  или *Неактивный* ). Статус каталога применяется ко всем вложенным каталогам и входящим в них объектам защиты.

В правой части рабочей области отображаются объекты защиты для выбранного каталога и инструменты для работы с ними, включая сквозной поиск объектов защиты по каталогам.

Сквозной поиск осуществляется по названию объекта защиты, а также по названию элементов технологий, входящих в объект защиты. Поиск ведется в выбранном и во вложенных каталогах. Чтобы осуществлять сквозной поиск во всех каталогах раздела, выберите корневой каталог.

С помощью переключателя можно выбрать: отображать все объекты защиты в каталоге или только объекты защиты, доступные для политик защиты данных на агентах.

Для каждого объекта защиты отображается его статус (*Активный*  или *Неактивный* ), название, входящие в объект защиты элементы технологий, даты создания и последнего изменения объекта защиты, описание.

Чтобы добавить комментарий, дважды щелкните левой кнопкой мыши в поле Описание напротив объекта защиты.

Примечание:

Если объект защиты выбран в результатах сквозного поиска по каталогам, изменить его статус невозможно.

При создании нового объекта защиты отображается окно добавления элементов технологий, где вы можете выбрать элементы или каталоги, на основе которых будет создан объект защиты (подробнее о технологиях, используемых в Системе, см. "Определение конфиденциальной информации").

Примечание:

Если выбрана настройка **Создать объект защиты на каждый выбранный элемент**, то для каждого элемента технологий будет создан отдельный объект защиты. Атрибуты объектов защиты задаются Системой по умолчанию.

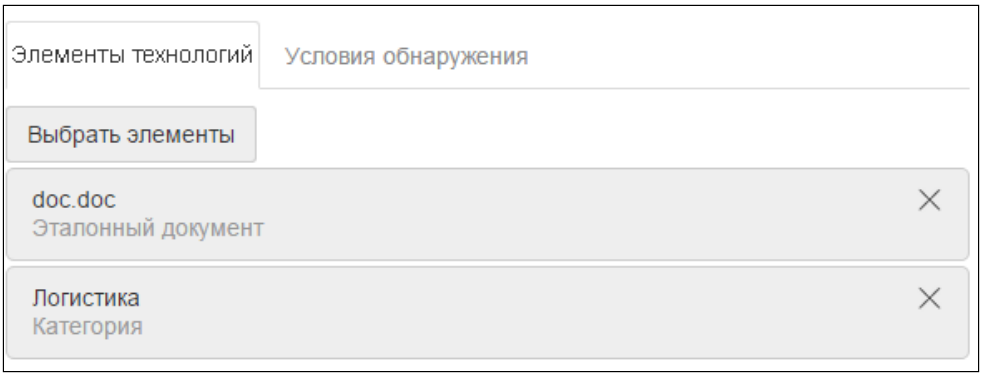
В режиме редактирования объекта защиты вы можете изменить список элементов технологий для выбранного объекта защиты и указать условия обнаружения.

Действия пользователя:

- Создание каталога объектов защиты
- Создание объекта защиты
- Добавление элементов технологий
- Создание политики для объектов защиты и их каталогов
- Импорт и экспорт объектов защиты

3.5.1 Элементы технологий

Справочная информация:
Элементы технологий – элементы или каталоги, на основе которых формируются объекты защиты. К элементам технологий относятся текстовые объекты, эталонные документы и пр.



Вкладка **Элементы технологий** для объекта защиты

Вкладка **Элементы технологий** отображается при создании объекта защиты, после того как требуемые элементы или каталоги выбраны в окне добавления элементов технологий, или при переходе в режим редактирования ранее созданного объекта защиты.

На вкладке **Элементы технологий** вы можете добавить дополнительные элементы или каталоги в объект защиты (кнопка **Выбрать элементы**) или удалить их (кнопка X в правом верхнем углу панели элемента).

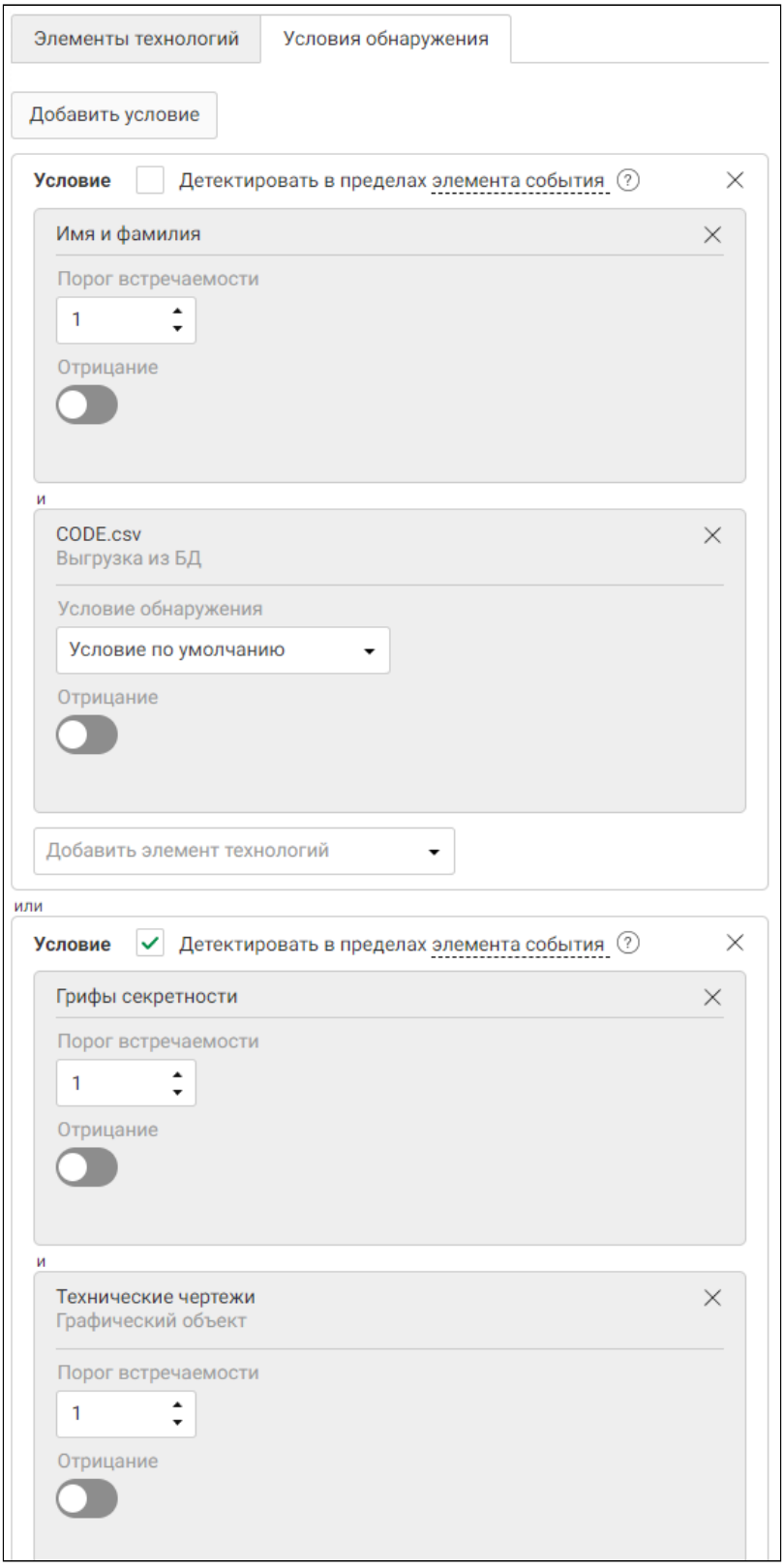
Условия детектирования добавленных элементов технологий указываются на вкладке **Условия обнаружения**.

Действия пользователя:

- Добавление элементов технологий

3.5.2 Условия обнаружения

Вкладка **Условия обнаружения** отображается при создании или редактировании объекта защиты.



Вы можете указать условия обнаружения при создании объекта защиты, после того как требуемые элементы выбраны в окне добавления элементов технологий, или при переходе в режим редактирования ранее созданного объекта защиты.

Условия обнаружения могут быть добавлены внутри одного блока и объединены с помощью операции конъюнкции (логическое "И"), либо добавлены в различные блоки, объединенные между собой с помощью операции дизъюнкции (логическое "ИЛИ").

Каталог детектируется, если детектируется хотя бы один из содержащихся в нем элементов.

Для каждого условия можно включить детектирование в пределах элемента события. В этом случае для детектирования объекта защиты все искомые элементы технологий из условия должны быть обнаружены в одном элементе события.

Элемент события – это перехваченный в трафике:

- текст письма;
- тема письма;
- переписка в мессенджере. Все сообщения из события являются одним элементом;
- файл;
- имя файла.

К элементу технологий можно применить отрицание, чтобы при его обнаружении Система не детектировала объект защиты.

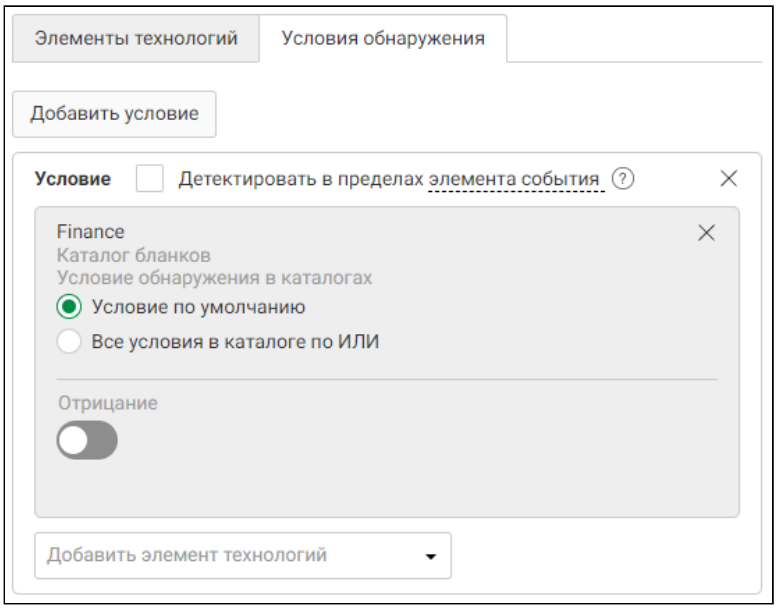
Примечание:

В условии обнаружения обязательно должен быть хотя бы один элемент без отрицания.

Если объект защиты добавлен в политику защиты данных на Агентах, включение отрицания и детектирования в пределах элемента события недоступно.

Условия обнаружения элементов технологий:

Название элемента	Условие обнаружения
Эталонный документ	Проверяется, содержит ли объект перехвата указанный эталонный документ
Категория	Проверяется соответствие объекта перехвата указанной категории. Для категорий, содержащих подкатегории, проверяется соответствие объекта перехвата какой-либо подкатегории
Текстовый объект	Проверяется, содержит ли объект перехвата указанный текстовый объект. Дополнительное условие обнаружения - порог встречаемости. Определяет, сколько раз минимум текстовый объект должен присутствовать в объекте перехвата. Значение по умолчанию – 1. Максимально возможное значение – 20000. В зависимости от типа используемого шаблона количество вхождений текстового объекта определяется следующим образом: • если шаблон текстового объекта задан в виде регулярного выражения, то одно его значение,

Название элемента	Условие обнаружения
	найденное в пределах одного документа несколько раз, считается одним вхождением; • если шаблон текстового объекта задан в виде строки, то считаются все его вхождения. Для каталога также задается порог встречаемости. Входящие в него текстовые объекты детектируются по его условию обнаружения.
Бланк	Проверяется, содержит ли объект перехвата хотя бы один из указанных бланков. Дополнительное условие обнаружения – Условие обнаружения бланка. Оно создается при редактировании бланка и состоит из: • порога цитируемости текстовых данных - процента совпадения перехваченного бланка с эталонным. В Условии по умолчанию – 70%; • минимального количества заполненные полей. В Условии по умолчанию – 3. Для детектирования перехваченный бланк должен удовлетворять **обоим** условиям. Всегда должно быть выбрано одно из условий обнаружения. Если элементом технологии выбран каталог бланков, необходимо выбрать один из вариантов: • **Условие по умолчанию** – для бланков внутри каталога будут применены их Условия по умолчанию; • **Все условия из каталога по ИЛИ** – для каждого бланка внутри каталога будет применено любое из его условий обнаружения. 

Название элемента	Условие обнаружения
Печать	Проверяется, содержит ли объект перехвата указанную печать
Графический объект	Проверяется, содержит ли объект перехвата указанный графический объект. Дополнительное условие обнаружения – порог встречаемости. Определяет, сколько раз минимум графический объект должен присутствовать в объекте перехвата. Значение по умолчанию – 1. Максимально возможное значение – 20000. Условие указывается для всей категории. **Примечание:** Порог встречаемости не может быть указан для следующих предустановленных графических объектов: • Кредитная карта; • Идентификационная карта гражданина Малайзии.
Выгрузка из базы данных	Проверяется, содержит ли объект перехвата указанную выгрузку. Дополнительное условие обнаружения – Условие обнаружения выгрузки. Оно создается при редактировании выгрузки. Всегда должно быть выбрано одно из условий обнаружения. Если элементом технологии выбран каталог выгрузок из БД, необходимо выбрать один из вариантов: • **Условие по умолчанию** – для бланков внутри каталога будут применены их Условия по умолчанию; • **Все условия из каталога по ИЛИ** – для каждой выгрузки внутри каталога будет применено любое из ее условий обнаружения.

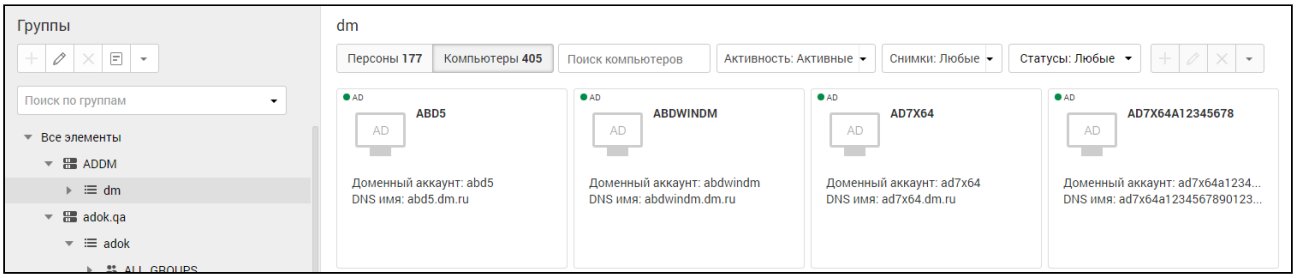
См. также: Элементы технологий

Действия пользователя:

- Добавление условий обнаружения

3.6 Раздел "Персоны"

О разделе:
Раздел содержит справочник персон и компьютеров информационной системы организации.



В левой части рабочей области отображаются группы персон и компьютеров.

Группы персон и компьютеров могут быть добавлены из Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro и FreeIPA, а также созданы средствами Traffic Monitor (см. "Создание группы персон и компьютеров").

Примечание.

Группы, для которых была выполнена синхронизация с LDAP, отмечены значком:

– если выполнена синхронизация с Active Directory;

– если выполнена синхронизация с Domino Directory;

– если выполнена синхронизация с Astra Linux Directory, Astra Linux Directory Pro или FreeIPA;

– если выполнена синхронизация с Samba DC.

С помощью панели инструментов в левой части рабочей области вы можете создать, отредактировать или удалить ранее созданную пользовательскую группу.

Кнопка позволяет перейти к созданию политики контроля персон для выбранной группы (подробнее см. "Создание политики контроля персон").

Также есть возможность экспортировать или импортировать группы, персоны и компьютеры (подробнее см. "Экспорт и импорт персон").

При выборе группы в списке в правой части рабочей области отображаются персоны и компьютеры, входящие в группу. Для просмотра списка персон и компьютеров используйте вкладки **Персоны** и **Компьютеры** соответственно.

Для поиска нужной персоны или компьютера воспользуйтесь полями **Поиск персон** или **Поиск компьютеров** соответственно. Переключение полей для поиска происходит при переключении вкладок **Персоны** и **Компьютеры**. Сквозной поиск в зависимости от выбранной вкладки осуществляется по имени и фамилии персоны, названию компьютера и значениям контактов и ведется в выбранной и во вложенных группах. Чтобы осуществлять поиск во всех группах раздела, выберите корневой каталог. Допускается ввод символов с маской (например: `*name`).

Важно!

Использование * в поисковом запросе может негативно отразиться на скорости поиска при большом количестве персон, загруженных из Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro и FreeIPA.

При поиске нужных персон и компьютеров вы также можете использовать следующие фильтры:

- выбор активных/неактивных персон и компьютеров (персон и компьютеров, полученных из LDAP);
- фильтрация по наличию снимков экрана;
- выбор персон и компьютеров с определенным статусом (подробнее см. "Статусы").

Для работы с персонами и компьютерами внутри выбранной группы используйте панель инструментов в правой части рабочей области.

Целевые действия пользователя:

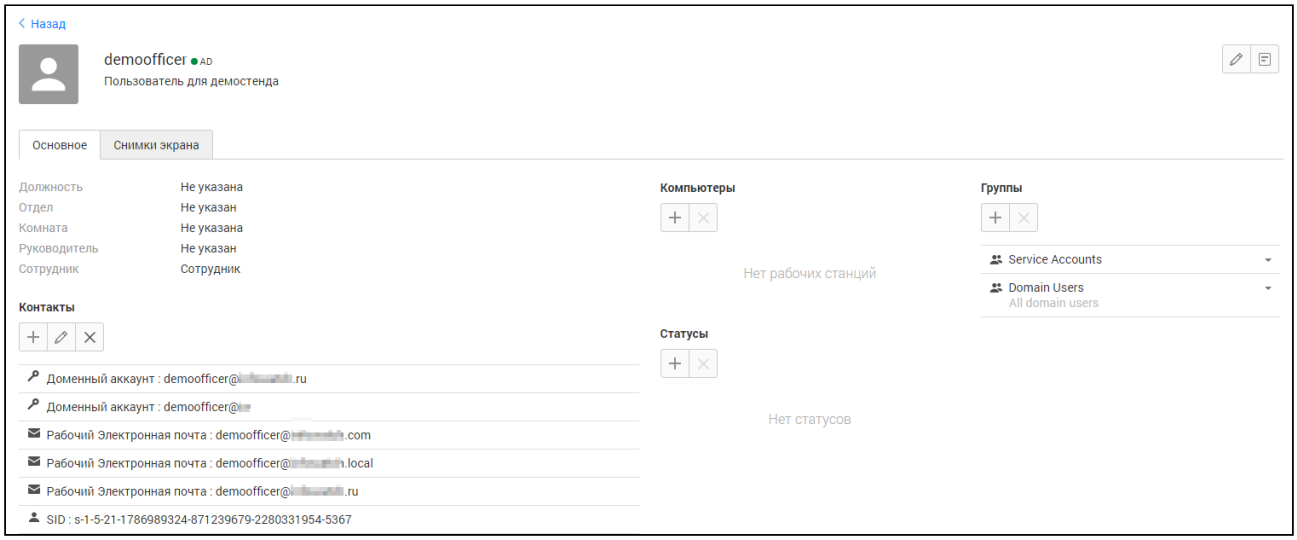
- Создание группы персон и компьютеров (см. "Создание группы персон и компьютеров")
- Создание персон и компьютеров (см. "Создание персон и компьютеров")
- Экспорт и импорт персон (см. "Экспорт и импорт персон")
- Просмотр виджетов с информацией о персонах и компьютерах (см. "Просмотр сводки по персоне/компьютеру")
- Создание фильтра по персонам и компьютерам (см. "Просмотр событий по персоне/компьютеру")
- Создание политики для персон и компьютеров (см. "Добавление персоны/компьютера в политику")
- Работа со статусами персон и компьютеров (см. "Добавление статуса персоне/компьютеру")
- Просмотр снимков экрана для персон и компьютеров (см. "Просмотр снимков экрана")
- Добавление персон в периметры (см. "Добавление персоны в периметр компании")

3.6.1 Персоны

Список персон, входящих в выбранную группу, отображается на вкладке **Персоны** в правой части рабочей области.

> **Примечание:**
>
> Для персон, данные которых импортированы из Active Directory, Samba DC, Astra Linux Directory, Astra Linux Directory Pro и FreeIPA отображается цветовой индикатор в левом верхнем углу фотографии профиля:
> – для активных сотрудников, в том числе с истекшим сроком действия учетной записи в AD/Samba DC/ALD/ALD Pro/FreeIPA;
> – для сотрудников, отключенных в AD/Samba DC/ALD/ALD Pro/FreeIPA.

Чтобы просмотреть карточку персоны, дважды щелкните левой клавишей мыши по выбранной персоне. Карточка персоны содержит две вкладки: **Основное** и **Снимки экрана**.



На вкладке **Основное** указаны следующие атрибуты персоны:

- Должность
- Отдел
- Комната
- Руководитель
- Сотрудник
- Контакты (можно указать личные или рабочие контакты персоны, включая адрес электронной почты, номер телефона, логин Skype, ICQ или адрес сайта в интернете, аккаунт в социальных сетях и мессенджерах)
- Компьютеры (компьютеры, привязанные к учетной записи персоны)
- Статусы (статусы, присвоенные персоне)
- Группы (группы, в которые включена персона)

Для изменения указанных атрибутов, а также атрибутов **Имя**, **Фамилия**, **Принадлежность компании** и редактирования фотографии персоны используется кнопка  в правой части рабочей области.

На вкладке **Снимки экрана** вы можете просмотреть снимки экрана, присутствующие в событиях для данной персоны (см. "Снимки экрана").

Для возврата к списку персон нажмите **< Назад**.

Кнопка  позволяет перейти к созданию политики для выбранной персон в разделе "Политики".

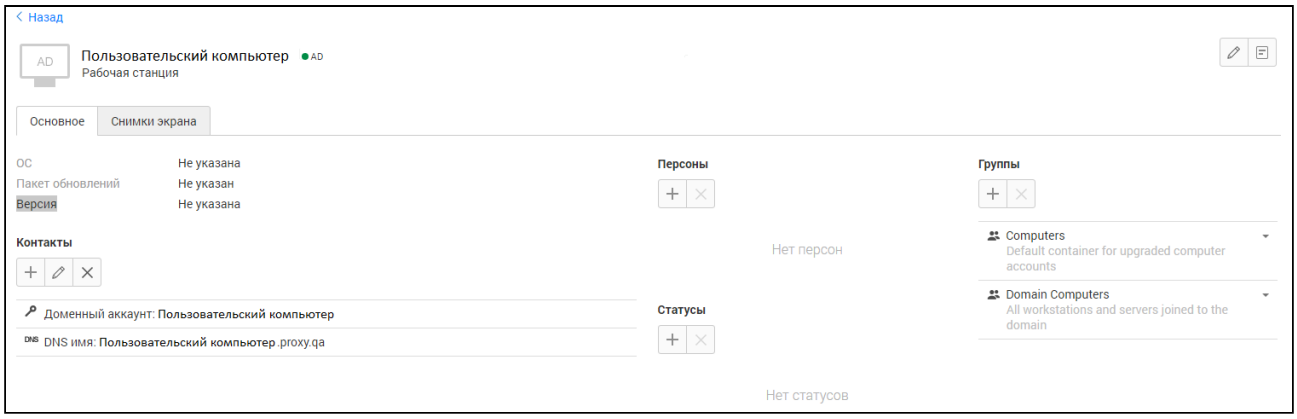
Действия пользователя:

- Создание фильтра по персонам (см. "Создание запросов")
- Настройка карточки персоны (см. "Настройка карточки персоны")
- Формирование политики для персон (см. "Добавление персоны/компьютера в политику")
- Работа со статусами персон (см. "Добавление статуса персоне/компьютеру")
- Добавление персоны в периметр (см. "Добавление персоны в периметр компании")
- Просмотр снимков экрана для персоны (см. "Просмотр снимков экрана")

3.6.2 Компьютеры

Список компьютеров, входящих в выбранную группу, отображается на вкладке **Компьютеры** в правой части рабочей области.

Чтобы просмотреть карточку компьютера, дважды щелкните левой клавишей мыши по выбранному компьютеру. Карточка компьютера содержит две вкладки: **Основное** и **Снимки экрана**.



На вкладке **Основное** указаны следующие атрибуты компьютера:

- ОС (установленная операционная система);
- Пакет обновлений (установленный пакет обновлений);
- Версия (версия пакета обновлений);
- Контакты (можно указать DNS-имя, IP-адрес и доменный аккаунт);
- Персоны (персоны, к учетной записи которых привязан компьютер);
- Статусы (статусы, присвоенные компьютеру);
- Группы (группы, в которые включен компьютер).

Для изменения указанных атрибутов, а также названия и типа компьютера используйте кнопку  в правой части рабочей области.

На вкладке **Снимки экрана** вы можете просмотреть снимки экрана, присутствующие в событиях для данного компьютера (см. "Снимки экрана").

Для возврата к списку компьютеров нажмите **< Назад**.

Кнопка  позволяет перейти к созданию политики для выбранного компьютера в разделе "Политики".

Действия пользователя:

- Работа с группами компьютеров (см. "Создание группы персон и компьютеров")
- Работа с компьютерами внутри группы (см. "Создание персон и компьютеров")
- Формирование политики для компьютера (см. "Добавление персоны/компьютера в политику")
- Работа со статусами компьютера (см. "Добавление статуса персоне/компьютеру")
- Просмотр снимков экрана для компьютера (см. "Просмотр снимков экрана")

3.6.3 Снимки экрана

Карточки персон (см. "Персоны") и компьютеров (см. "Компьютеры") содержат вкладку **Снимки экрана**, где вы можете просмотреть информацию о снимках экрана для выбранной персоны или выбранного компьютера.

Также переход к снимкам экрана можно выполнить из раздела "События" при просмотре информации о персоне или компьютере в краткой форме просмотра события (см. "Просмотр краткой формы события").



По умолчанию показаны снимки экрана, сделанные за все время и для всех приложений. Снимки экрана отсортированы по дате.

Фильтры **Приложение**, **Компьютер**/**Персона** и **Дата** позволяют выполнить поиск снимков экрана по заданным условиям.

При нажатии на снимок экрана отображается увеличенное изображение снимка и его атрибуты:

- **Персона** – персона, под учетной записью которой велась работа в момент снятия снимка экрана;
- **Компьютер** – компьютер, на котором был сделан снимок экрана;
- **Время** – дата и время создания снимка экрана;
- **Приложение** – приложение, в котором велась работа на момент создания снимка экрана.

С помощью инструментов в правой части рабочей области вы можете изменить масштаб изображения (кнопки **+** и **-**) и сохранить изображение на ваш компьютер (кнопка ).

Для перехода к предыдущему или следующему изображению используйте кнопки **<** и **>**. Вы также можете найти нужный снимок в списке элементов в нижней части рабочей области. Для быстрого перемещения между элементами списка, наведите указатель мыши на список, зажмите левую клавишу мыши и пролистывайте список в требуемом направлении.

Чтобы закрыть окно просмотра и вернуться к работе с выбранной персоной или выбранный компьютером, нажмите **X**.

Действия пользователя:

- Просмотр снимков экрана

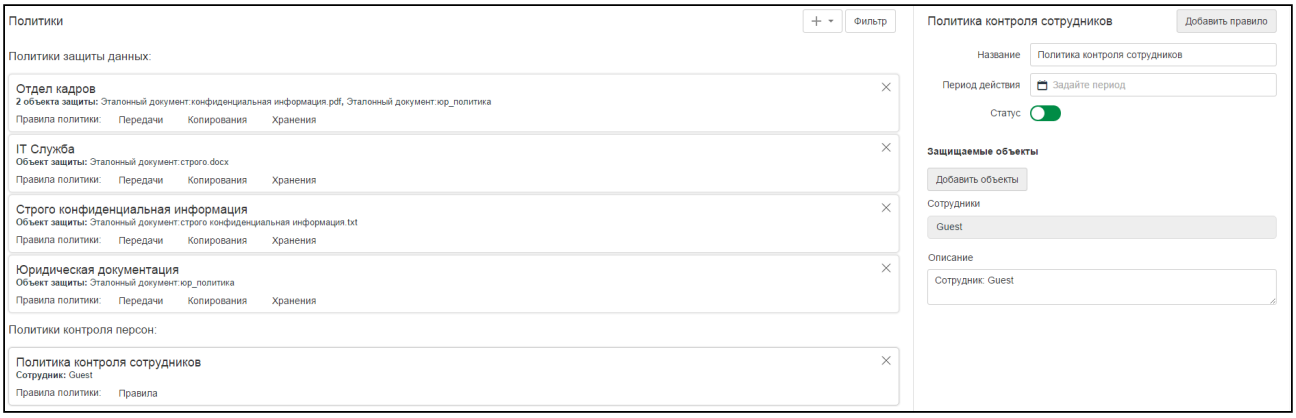
3.7 Раздел "Политики"

Справочная информация:
Политики – совокупность *правил*, в соответствии с которыми проводится анализ и обработка

объектов перехвата. ***Правило*** состоит из набора условий, по которым выполняется проверка объекта, и действий, осуществляемых при выполнении или невыполнении заданных условий.

> **Важно!**
>
> В результате анализа Система не будет производить никаких действий, если выполняется хотя бы одно из следующих условий:
>
> - в Системе нет ни одной политики;
> - все имеющиеся в Системе политики неактивны;
> - ни одна имеющаяся в Системе политика не имеет активных правил (или действия по умолчанию для активных политик не определены).

О разделе:
Раздел содержит список политик и инструменты для работы с ними.



Политики в списке сгруппированы по типам: политики защиты данных, политики защиты данных на агентах и политики контроля персон.

При выборе политики в списке в правой части рабочей области отображается форма просмотра выбранной политики, где вы можете отредактировать ее атрибуты. При добавлении правила для политики в правой части рабочей области отображается форма просмотра правила.

Для добавления новой политики используется кнопка . В раскрывающемся списке необходимо указать тип добавляемой политики, после чего новая политика будет добавлена в список, а в правой части рабочей области отобразится форма просмотра политики.

На форме просмотра политики вы можете:

- указать ее атрибуты (название, период действия, статус, описание);
- выбрать защищаемые данные (для политик защиты данных). В качестве защищаемых данных могут выступать объекты защиты, их каталоги, а также файловые форматы;
- указать отправителей, действия которых будут контролироваться политикой (для политик контроля персон). Вы можете выбрать отдельных персон, группу персон или персон, объединенных общим статусом;
- добавить правила для политики.

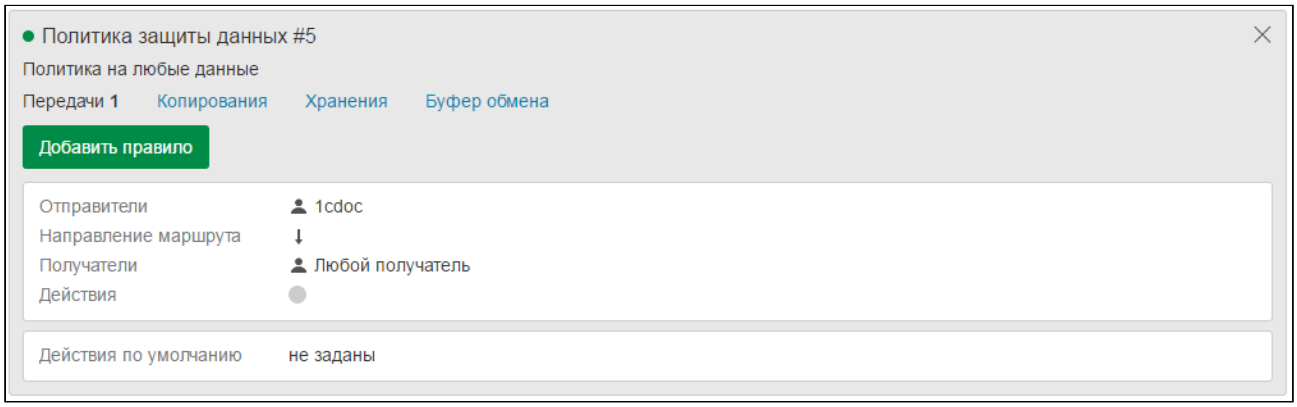
При нажатии кнопки **Фильтр** в правой части рабочей области отображается область **Настройка фильтра**, где вы можете отфильтровать политики по названию или объектам исследования.

Действия пользователя:

- Добавление новой политики (см. "Создание политики защиты данных", "Создание политики защиты данных на агентах" и "Создание политики контроля персон")
- Добавление правил в политику (см. "Создание правил")
- Фильтрация политик (см. "Фильтрация списка политик")

3.7.1 Правила и форма их просмотра

Информация о правилах указывается в плитке выбранной политики. При нажатии на ссылку с типом правил в плитке политики раскрывается список добавленных правил этого типа.



При выборе правила в списке в правой части рабочей области отображается форма просмотра выбранного правила.

Также в правом верхнем углу плитки правила отображается значок ×, нажав на который вы можете удалить выбранное правило.

Для каждой **политики защиты данных** вы можете настроить одно или несколько правил:

- Правило передачи – регулирует отправку и получение защищаемых данных;
- Правило копирования – регулирует копирование и печать защищаемых данных;
- Правило хранения – регулирует хранение защищаемых данных;
- Правило работы в приложениях – регулирует использование буфера обмена и ввод с клавиатуры;
- Правило файловых операций – регулирует чтение и запись файлов приложением.

Для каждой **политики защиты данных на агенте** вы можете настроить одно или несколько правил:

- Правило передачи;
- Правило копирования;
- Правило работы в приложениях.

При создании правил передачи и копирования для выбора LDAP-домена в качестве *Отправителя* или *Получателя* необходимо предварительно настроить синхронизацию с LDAP-сервером и добавить домен через закладку **Группы**.

Также для *Отправителя* и *Получателя* можно указать следующие параметры:

Параметр	Описание
Контакты	Укажите контакты отправителей/получателей трафика. Для этого в выпадающем списке слева выберите тип контакта: – аккаунт ICQ. Целое число от 10000 до 999999999999;

Параметр	Описание
	– аккаунт Skype. Строка от 6 до 32 символов, должна начинаться с буквы; может содержать только латинские буквы, цифры и символы «.», «,», «-», «_»); – контакт Azure AD (если установлен адаптер). Строка от 1 символа; – номер мобильного телефона. Строка от 3 символов, может содержать только цифры, пробел и символы "-","_", "( )","+","."); – номер стационарного телефона. Строка от 3 символов, может содержать только цифры, пробел и символы "-","_", "( )","+","."); – адрес электронной почты. Адрес в формате RFC; – аккаунт Telegram (строка от 1 символа); – аккаунт Facebook. Строка от 1 символа; – аккаунт WhatsApp. Строка от 1 символа; – адрес электронной почты Lotus. Строка от 3 символов при вводе данных в поле ввода или строка от 1 символа при вводе данных в окне **Отправители** (открывается при нажатии кнопки +); – идентификатор на Web-ресурсе. Строка от 3 символов при вводе данных в поле ввода или строка от 1 символа при вводе данных в окне **Отправители** (открывается при нажатии кнопки +)
Группы	Укажите группы, члены которых являются отправителями/получателями трафика
Персоны	Укажите персон, которые являются отправителями/получателями трафика
Домены	Укажите домены, члены которых являются отправителями/получателями трафика
Периметры	Укажите периметры, элементы которых являются отправителями/получателями трафика

Правила контроля персон регулируют действия выбранных персон, а также позволяют применить к этим персонам имеющиеся в Системе политики защиты данных и политики защиты данных на агентах.

Действия пользователя:

- Добавление правил в политику (см. "Создание правил")

Правило передачи

Для правила передачи указываются следующие атрибуты:

- **Направление маршрута**. Возможные значения:
  - **В одну сторону** – правило срабатывает только в случае передачи трафика от отправителя получателю;
  - **В оба направления** – правило срабатывает при передаче трафика от отправителя получателю и от получателя отправителю.
- **Тип события** – тип трафика, передача которого приводит к срабатыванию правила. Возможные значения:
  - **Интернет-активность**
    - Веб-сообщение
  - **Мессенджер** (только для политик защиты данных)
    - ICQ
    - MS Lync
    - Skype
    - Telegram
    - MS Teams (если установлен адаптер)
    - XMPP
    - Facebook
    - WhatsApp
    - Vkontakte
    - Kribrum
  - **Почта**
    - Почта на Клиенте
    - Почта в Браузере
- **Компьютеры** – компьютеры, с которых выполнялась передача данных;
- **Отправители** – список персон, компьютеров, доменов и периметров, передача трафика которыми приводит к срабатыванию правила;
- **Получатели** – список персон, компьютеров, доменов и периметров, получение трафика которыми приводит к срабатыванию правила;

> **Примечание.**
>
> Если в качестве защищаемых данных указан объект защиты на базе графического объекта и выбран тип события **Почта в Браузере**, то для срабатывания политики требуется не указывать персон в поле **Получатели**. Данное ограничение связано с тем, что в событиях веб-почты получателем вложения считается домен. Например, если письмо с вложением отправлено на адрес `user1@example.com`, то получателем вложения будет считаться домен `example.com`. Такие образом, если в качестве получателей указаны определенные персоны, то событие, содержащее во вложении графический объект, не попадет под действие политики.

- **Дни действия правила**
- **Часы действия правила**

> **Важно!**

Выбранные условия объединяются с помощью логического "И". Внутри одного условия значения объединяются следующим образом:

- с помощью логического "ИЛИ", если выбран параметр равенства атрибуту;
- с помощью логического "И", если к атрибуту применено отрицание.

В блоке **Действия при срабатывании правила** укажите требуемые действия (подробнее см. "Определение действий Системы в случае нарушения правил").

Действия пользователя:

- Создание правил
- Настройка уведомлений в правилах

Правило копирования

Для правила копирования указываются следующие атрибуты:

- **Направление маршрута**. Возможные значения:
  - **В одну сторону** – правило срабатывает только в случае передачи трафика от отправителя получателю;
  - **В оба направления** – правило срабатывает при передаче трафика от отправителя получателю и от получателя отправителю.
- **Тип события** – тип трафика, копирование которого приводит к срабатыванию правила. Возможные значения:
  - **Обмен файлами**
    - *Съемное устройство*
    - *FTP*
    - *Облачное хранилище*
    - *Сетевой ресурс*
    - *Терминальная сессия*
  - **Принтер и МФУ** (только для политики защиты данных)
    - *Печать*
- **Компьютеры**;

> **Примечание.**
>
> При указании домена правило будет срабатывать также для его поддоменов. Например, если указан домен `domain.com`, правило будет срабатывать также для домена `subdomain.domain.com`.

- **Отправители** – список персон, компьютеров, доменов и периметров, передача трафика которыми приводит к срабатыванию правила;
- **Приемник копирования**;

> **Важно!**
>
> Тип значения атрибута **Путь к файлу или адрес** для приемника копирования типа "Терминальная сессия" зависит от версии Traffic Monitor. Типы значений различаются для этого атрибута в событиях обмена файлами по терминальной сессии:

- **Для событий, созданных в Traffic Monitor версии ниже 7.5**: в атрибуте указывается имя скопированного файла, например: `file.txt`
- **Для событий, созданных в Traffic Monitor версии 7.5 и выше**: в атрибуте указывается IP-адрес устройства, с которого осуществлялось удаленное подключение к рабочей станции сотрудника и на которое был скопирован файл, например: `192.0.2.0`

Чтобы политики срабатывали корректно на события, созданные в Traffic Monitor версии 7.5 и выше, рекомендуется отредактировать существующие правила копирования в политиках. Существующие правила копирования необходимо отредактировать, если в них используется устаревший тип значения атрибута **Путь к файлу или адрес** для приемника копирования типа "Терминальная сессия". Если в правиле в этом атрибуте указано имя файла, то правило не будет корректно работать с новыми событиями, так как у новых событий в этом атрибуте указан IP-адрес.

- **Источник копирования**;

> **Примечание:**
>
> В зависимости от выбранного типа источника или приемника копирования у поля **Путь к файлу или адрес** могут быть особенности заполнения (см. Особенности заполнения поля "Путь к файлу или адрес").

- **Дни действия правила**;
- **Часы действия правила**.
- **Имя терминальной станции** – имя устройства, с которого было осуществлено удаленное подключение к рабочей станции сотрудника. Атрибут указывается для приемника копирования типа *Терминальная сессия* в событиях обмена файлами по терминальной сессии.

> **Примечание:**
>
> **Имя терминальной станции** является пользовательским атрибутом предустановленного плагина InfoWatch Device Monitor. Атрибут может быть использован только в правилах политик защиты данных. Атрибут недоступен в правилах политик защиты данных на агентах.

> **Важно!**
>
> Выбранные условия объединяются с помощью логического "И". Внутри одного условия значения объединяются следующим образом:
>
> - с помощью логического "ИЛИ", если выбран параметр равенства атрибуту;
> - с помощью логического "И", если к атрибуту применено отрицание.

> **Важно!**

Политика, в которой заданы источники или приемники копирования, в некоторых случаях может не срабатывать. Подробнее в статье "Ограничения на срабатывание политики защиты данных на агенте"

В блоке **Действия при срабатывании правила** укажите требуемые действия (подробнее см. "Определение действий Системы в случае нарушения правил").

Действия пользователя:

- Создание правил
- Настройка уведомлений в правилах

Правило хранения

Для правила хранения указываются следующие атрибуты:

- **Тип события** – тип трафика, хранение которого приводит к срабатыванию правила. Возможные значения:
  - **Data Discovery**
- **Место хранения** – список мест, хранение защищаемых данных в которых приводит к срабатыванию правила. Чтобы указать место хранения, нажмите  и в открывшемся диалоговом окне перейдите на нужную вкладку:
  - **Компьютеры**. На вкладке отображаются компьютеры, полученные при синхронизации с LDAP. Установите флажки напротив требуемых компьютеров;
  - **Сетевые ресурсы**. Для добавления сетевого ресурса введите следующие значения в поля:
  - В поле **Введите сетевой ресурс** – IP-адрес или полное DNS-имя хоста.
  - В поле **Введите путь** – путь на хосте. Форматы:
  - Для SMB-хостов: `share/folder`, где `share` – имя сетевого ресурса;
  - Для SSH-хостов: `/home/folder`;
  - Для SharePoint-хостов: `path/lib/folder`, где `path` – путь к сайту с библиотекой документов, `lib` – библиотека документов.

Примечание:

Условия на вкладке **Файловые хранилища** не используются для событий, полученных от Data Discovery.

После того как вы указали все требуемые места хранения, нажмите **Сохранить**.

- **Владельцы файла** – хранение защищаемых данных указанными персонами и группами, а также внутри указанных периметров приводит к срабатыванию правила;
- **Кому доступен файл** – доступность файла указанным персонам, группам персон, а также в пределах указанных периметров приводит к срабатыванию правила.

Важно!

Выбранные условия объединяются с помощью логического "И". Внутри одного условия значения объединяются следующим образом:

- с помощью логического "ИЛИ", если выбран параметр равенства атрибуту;
- с помощью логического "И", если к атрибуту применено отрицание.

В блоке **Действия при срабатывании правила** укажите требуемые действия (подробнее см. "Определение действий Системы в случае нарушения правил").

Действия пользователя:

- Создание правил
- Настройка уведомлений в правилах

Правило работы в приложениях

Для правила работы в приложениях указываются следующие атрибуты:

- **Тип события** – тип трафика, хранение которого приводит к срабатыванию правила. Возможные значения:
  - **Буфер обмена**;
  - **Ввод с клавиатуры**.

  Примечание:

  Для правила работы в приложениях, добавленного в политику защиты данных на агентах:

  - доступен только тип события **Буфер обмена**;
  - всегда активна опция **Только для терминальной сессии**;
  - отсутствует возможность исключения компьютеров.

- **Персоны** – список персон, групп и периметров, передача трафика которыми или за пределы которых приводит к срабатыванию правила;
- **Компьютеры** – список компьютеров, передача трафика которыми приводит к срабатыванию правила;
- **Приложения** (только для типа события **Ввод с клавиатуры**) – список приложений, работа в которых приводит к срабатыванию правила;
- **Только для терминальной сессии** (только для типа события **Буфер обмена**) – выберите эту опцию, если нужно контролировать только пересечение границы терминальной сессии, независимо от направления. Если отмечена эта опция, выбор приложений вручную недоступен.
- **Приложение-источник** (только для типа события **Буфер обмена**) – приложение, копирование данных из которого приводит к срабатыванию правила. Недоступно, если выбрана опция **Только для терминальной сессии**;
- **Приложение-приемник** (только для типа события **Буфер обмена**) – приложение, вставка данных в которое приводит к срабатыванию правила. Недоступно, если выбрана опция **Только для терминальной сессии**;
- **Дни действия правила**;
- **Часы действия правила**.

Важно!

Выбранные условия объединяются с помощью логического "И". Внутри одного условия значения объединяются следующим образом:

- с помощью логического "ИЛИ", если выбран параметр равенства атрибуту;
- с помощью логического "И", если к атрибуту применено отрицание.

В блоке **Действия при срабатывании правила** укажите требуемые действия (подробнее см. "Определение действий Системы в случае нарушения правил").

Действия пользователя:

- Создание правил
- Настройка уведомлений в правилах

Правило контроля персон

Для правила контроля персон указываются следующие атрибуты:

- **Уровень нарушения** – Система будет перехватывать события с заданным уровнем нарушения;
- **Связать с политикой** – укажите политики защиты данных и политики защиты данных на агентах, срабатывание которых будет инициировать срабатывание правила (если уровень нарушения соответствует значению поля **Перехватывать с уровнем нарушения**).

В блоке **Действия при срабатывании правила** укажите требуемые действия (подробнее см. "Определение действий Системы в случае нарушения правил").

Действия пользователя:

- Создание правил
- Настройка уведомлений в правилах

Правило файловых операций

Для правила файловых операций указываются следующие атрибуты:

- **Тип события** – действия с файлами, которые приводят к срабатыванию правила. Возможные значения:
  - **Запись файла;**
  - **Чтение файла.**
- **Персоны** – список персон, групп и периметров, выполнение операций которыми приводит к срабатыванию правила;
- **Компьютеры** – список компьютеров, операции с файлами на которых приводят к срабатыванию правила;
- **Приложения** – список приложений, действия в которых приводят к срабатыванию правила;
- **Дни действия правила**;
- **Часы действия правила**;
- **Адрес вкладки браузера** – адрес активной вкладки браузера. Дополнительный атрибут.

Важно!

Выбранные условия объединяются с помощью логического "И". Внутри одного условия значения объединяются следующим образом:

- с помощью логического "ИЛИ", если выбран параметр равенства атрибуту;
- с помощью логического "И", если к атрибуту применено отрицание.

В блоке **Действия при срабатывании правила** укажите требуемые действия (подробнее см. "Определение действий Системы в случае нарушения правил").

Важно!

Для работы правила файловых операций настройте в консоли Device Monitor правило для File Operations Monitor (см. "Правило для File Operations Monitor" в *"InfoWatch Device Monitor. Руководство пользователя"*).

Действия пользователя:

- Создание правил
- Настройка уведомлений в правилах

3.8 Раздел "Списки"

Справочная информация:
Списки – наборы однотипных данных, используемых при создании политик. Списки создаются средствами Консоли управления. Также Система содержит предустановленные списки.

О разделе:
Раздел содержит редактируемые справочники тегов, веб-ресурсов, статусов, периметров и нередактируемый список файлов.



Раздел **Списки**, список статусов

Раздел содержит следующие справочники:

- Теги
- Статусы
- Периметры
- Веб-ресурсы
- Файлы

Действия пользователя:

- Формирование списка тегов (см. "Работа с тегами")

- Формирование списка веб-ресурсов (см. "Работа с веб-ресурсами")
- Формирование списка статусов (см. "Работа со статусами")
- Формирование периметров (см. "Работа с периметрами")
- Включение файловых форматов в политику (см. "Создание политики защиты данных" и "Создание политики защиты данных на агентах")

3.8.1 Теги

Справочная информация:
Тег – метка, дающая краткую характеристику перехваченному объекту. Для каждого тега устанавливается цветовой маркер.

В Системе существуют следующие предустановленные теги:

- **На рассмотрение** – события, характеризующие подозрительную активность персон;
- **VIP** – события, инициированные руководством организации.

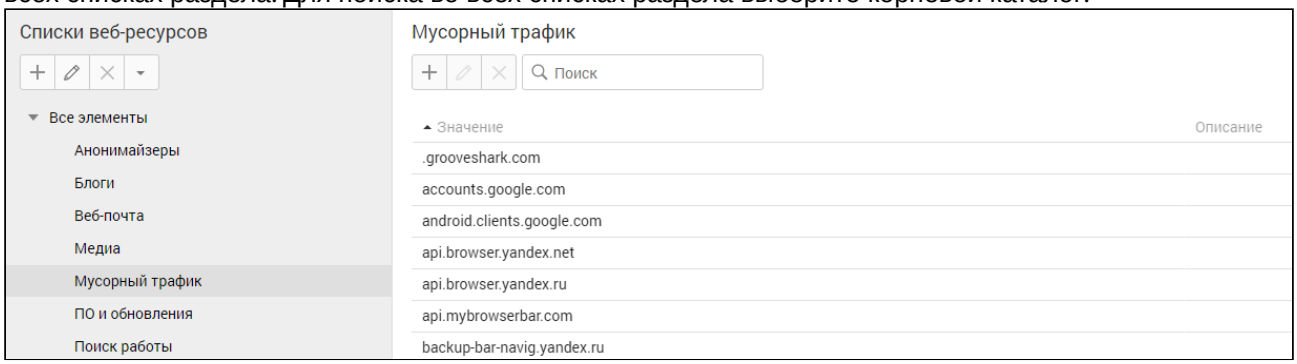
Действия пользователя:

- Формирование списка тегов (см. "Работа с тегами")

3.8.2 Веб-ресурсы

Справочная информация:
Веб-ресурсы – набор интернет-ресурсов, посещение которых детектируется Системой как нецелевое использование рабочего времени.

Веб-ресурсы добавляются в списки. Для работы со списками веб-ресурсов (создание, редактирование, удаление списка) используйте инструменты в левой части рабочей области.
В правой части рабочей области отображаются веб-ресурсы внутри выделенного списка, а также инструменты для работы с ними: добавление, редактирование, удаление, сквозной поиск по спискам. Сквозной поиск осуществляется по значению веб-ресурса и может вестись в выбранном списке и во всех списках раздела. Для поиска во всех списках раздела выберите корневой каталог.



В Системе содержатся следующие предустановленные списки веб-ресурсов:

- Анонимайзеры
- Блоги
- Веб-почта
- Медиа
- ПО и обновления
- Поиск работы

- Потенциально опасные ресурсы
- Развлечения
- Сайты агрессивной направленности
- Социальные сети
- Тематика для взрослых
- Файлообменники
- Финансы

Действия пользователя:

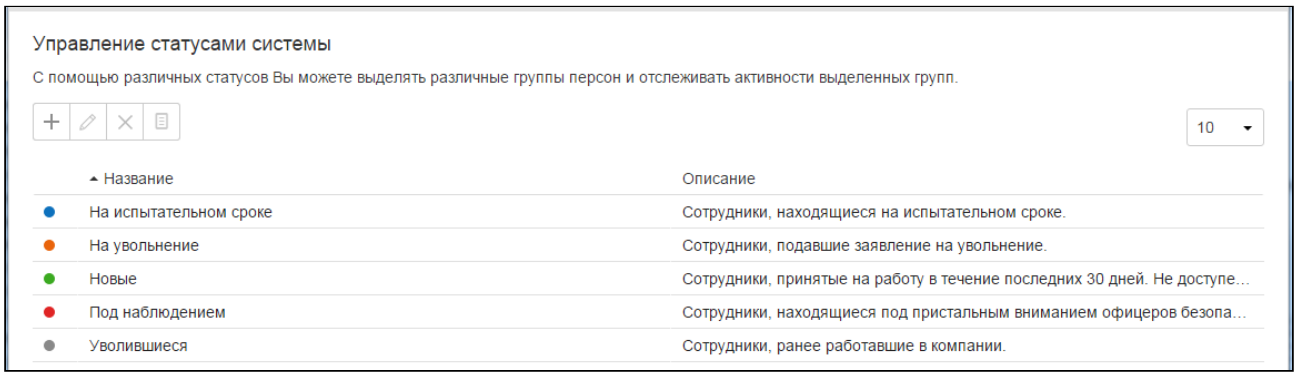
- Формирование списка веб-ресурсов (см. "Работа с веб-ресурсами")

3.8.3 Статусы

Справочная информация:
Статус персоны – метка, созданная одним из следующих способов:

- автоматически присвоена персоне в соответствии со статусом персоны или компьютера, импортированных из Active Directory, Samba DC, Domino Directory, Astra Linux Directory, FreeIPA и Astra Linux Directory Pro;
- вручную присвоена персоне офицером безопасности;
- автоматически назначена отправителю в результате срабатывания правила.

Для каждого статуса устанавливается цветовой индикатор.



Статусы *На испытательном сроке*, *На увольнение*, *Новый*, *Под наблюдением* и *Уволившиеся* являются предустановленными.

> **Примечание.**
>
> Статус *Новый* не доступен для удаления.

Действия пользователя:

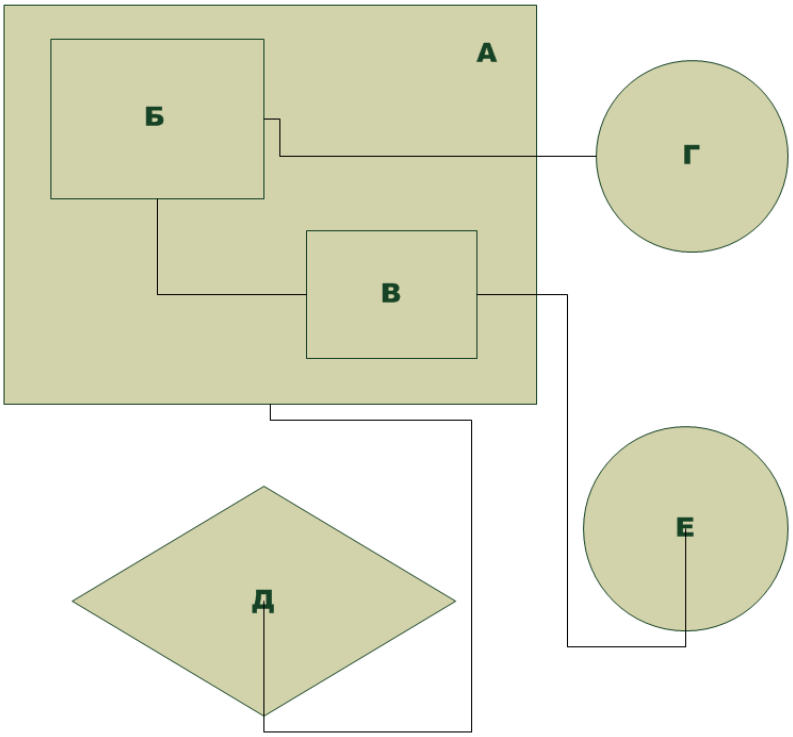
- Формирование списка статусов (см. "Работа со статусами")
- Ручное назначение статуса персоне или компьютеру для отслеживания активности, а также для визуального отличия (см. "Добавление статуса персоне")
- Автоматическое назначение статуса отправителю в случае срабатывания правила (см. "Правила и форма их просмотра", атрибут **Назначить отправителю статус**)
- При добавлении политики контроля персон – выбор в качестве объектов исследования персон с определенными статусами (см. "Создание политики контроля персон")

3.8.4 Периметры

Справочная информация:
Периметр – это контейнер, содержащий элементы инфраструктуры компании (сотрудников, домен и прочие) и контактные данные. Периметр используется для того, чтобы логически разделить организацию на структурные элементы и следить за трафиком каждого из таких элементов.

Например:

- Есть компания с инфраструктурой А, в которой есть подразделения Б и В;
- Подразделения Б и В взаимодействуют между собой;
- Компания взаимодействует с организациями Г, Д и Е.



Выделив в периметры все названные объекты (А, Б, В, Г, Д, Е), офицер безопасности может настроить контроль трафика:

- внутри компании – в пределах периметра А;
- внутри одного подразделения компании – в пределах периметра Б или периметра В;
- только между подразделениями компании – между периметрами Б и В;
- за пределами компании – между периметром А и одним из периметров Г, Д или Е;
- за пределами компании только для одного подразделения – между периметром Б или В и одним из периметров Г, Д или Е;

Важно!

Для более гибкой работы со структурными элементами рекомендуется выделять меньшие периметры в больших (в приведенном примере – периметры Б и В в периметре А). Периметры могут иметь общее содержимое, но нельзя помещать один периметр в другой и создавать иерархическую структуру.

В Системе содержатся следующие предустановленные периметры:

- ***Компания*** – используется для контроля данных, передаваемых за пределы компании;
- ***Исключить из перехвата*** – используется в предустановленной политике ***Исключение из перехвата*** (см. "Политика, исключающая из перехвата почтовые рассылки").

Предустановленные периметры не содержат элементов, их нужно добавить самостоятельно (см. "Работа с периметрами").

> **Примечание.**
>
> При добавлении в периметр персон или групп доступна функция **Использовать только рабочие контакты**. Вы можете использовать эту функцию, например, для того, чтобы отправка сотрудником сообщения с личного почтового ящика не считалась передачей данных за периметр.

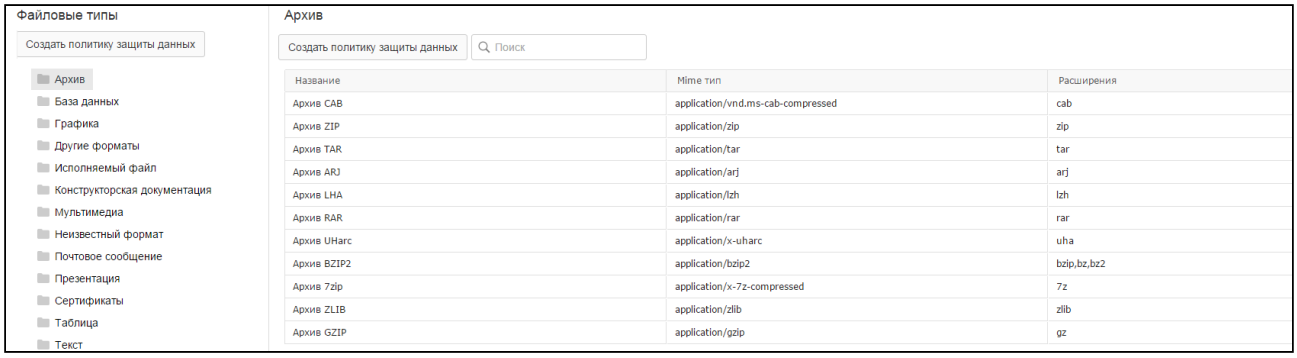
Действия пользователя:

- Формирование периметров (см. "Работа с периметрами")

3.8.5 Файловые типы

Справочная информация:

Файловые типы – набор типов файлов, которые детектируются в Системе.



Файлы различных форматов разделены на группы в зависимости от предметной области. Например, тип **Архив** содержит файлы с расширением ZIP, RAR и прочие.

В разделе содержатся следующие элементы:

Элемент	Назначение
Список файловых типов	Расположен в левой части рабочей области. Содержит набор предметных областей, в которых используются файлы одного или нескольких форматов
Список файловых форматов выбранного типа	Расположен в правой части рабочей области. Содержит список файловых форматов данного типа, которые детектируются в Системе. Представляет собой таблицу

Элемент	Назначение
	со следующими параметрами: **Название**, **Mime тип** и **Расширение**
Кнопка **Создать политику защиты данных**	Кнопка добавления новой политики для выбранного файлового типа или формата. Нажмите на кнопку и в раскрывающемся списке выберите требуемое действие: ▪ Создать политику защиты данных ▪ Создать политику на агенте Будет выполнен переход к разделу "Политики" на форму создания новой политики для выбранного файлового формата. **Примечание:** Для форматов, анализ которых не поддерживается в Device Monitor, пункт **Создать политику на агенте** не доступен
Поле сквозного поиска	Расположено в правой части рабочей области. Система осуществляет сквозной поиск форматов файлов по названию и расширению. Поиск может вестись в выбранном списке файловых типов и во всех списках раздела. Чтобы осуществлять поиск во всех списках раздела, выберите корневой каталог

Важно!

Список файловых типов определен Системой и недоступен для изменения.

Действия пользователя:

- Добавление файловых типов в политику (см. "Создание политики защиты данных" и "Создание политики защиты данных на агентах")

3.9 Раздел "Управление"

Раздел **Управление** содержит следующие подразделы:

- LDAP-синхронизация
- Лицензии
- Управление доступом
- Состояние Системы
- Аудит
- Контроль целостности
- Службы
- Плагины
- Почтовый сервер

- Почтовые уведомления

О работе в разделе см. "Управление Системой".

4 Решение задач при работе в консоли Traffic Monitor

Работа Офицера безопасности в Консоли управления сводится к следующим основным задачам:

- Работа с персонами и компьютерами
- Работа со справочниками
- Работа с базой технологий
- Работа с объектами защиты
- Работа с объектами перехвата
- Настройка реакций Системы
- Работа с отчетами
- Управление Системой

> **Примечание.**
>
> Часть настроек, доступных в разделе "Управление", выполняется администратором Системы.

Однотипные действия, выполняемые в рамках перечисленных задач, описаны в разделе "Типовые действия".

Об элементах интерфейса в разделах Консоли управления читайте:

- Раздел "Сводка"
- Раздел "События"
- Раздел "Отчеты"
- Раздел "Технологии"
- Раздел "Объекты защиты"
- Раздел "Персоны"
- Раздел "Политики"
- Раздел "Списки"
- Раздел "Управление"

4.1 Типовые действия

Для чего требуются типовые действия:
Для выполнения однотипных операций при работе в Консоли управления.

К типовым действиям относятся:

- Вход в Консоль управления
- Применение конфигурации Системы
- Редактирование элемента
- Удаление элемента
- Навигация по страницам
- Изменение пароля пользователя
- Выбор языка интерфейса
- Вызов справки
- Просмотр сведений о Системе

4.1.1 Вход в Консоль управления

Цель:

Войти в Консоль управления.

Решение:

Чтобы войти в Консоль управления:

1. Откройте интернет-браузер Google Chrome или Mozilla Firefox актуальной версии (если ни один из указанных браузеров не установлен, вы можете загрузить их, перейдя по одной из ссылок: Google Chrome или Mozilla Firefox).
2. Перейдите по адресу, выданному вам системным администратором. В окне браузера отобразится стартовая страница Консоли управления.
3. В поле **Логин** укажите имя пользователя.
4. В поле **Пароль** укажите пароль.

> **Примечание.**
>
> Логин и пароль вы можете получить у администратора InfoWatch Traffic Monitor.

5. Нажмите **Войти**.

Чтобы выйти из Консоли управления:

1. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления Traffic Monitor").
2. Выберите **Выйти**.

4.1.2 Применение конфигурации Системы

Справочная информация:
В конфигурацию Системы включено содержимое следующих разделов Консоли управления:

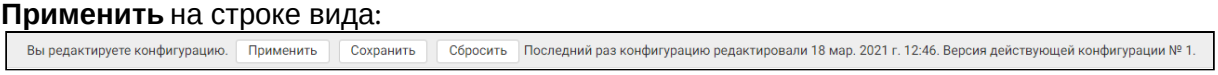
- Технологии
- Объекты защиты
- Персоны
- Политики
- Списки

По завершении редактирования элементов этих разделов необходимо применить сделанные изменения, чтобы они вступили в действие: то есть Система начала бы работать в соответствии с внесенными изменениями.

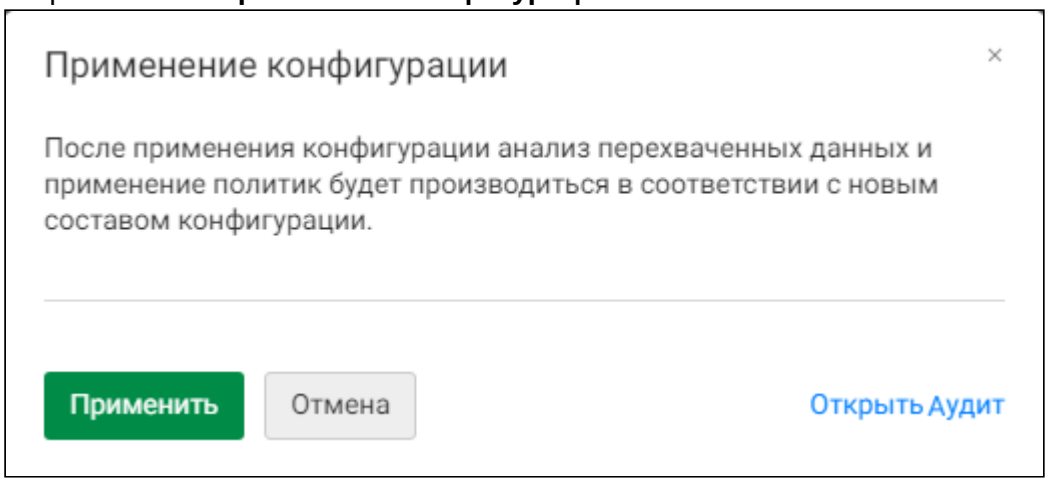
Цель:
Применить конфигурацию Системы.

Решение:

1. По окончании редактирования конфигурации в верхней части окна браузера нажмите **Применить** на строке вида:



Откроется окно **Применение конфигурации**:

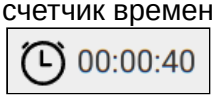


2. Чтобы просмотреть подробную информацию о внесенных изменениях, нажмите **Открыть Аудит**. Данное действие возможно при Применении, Сохранении, Сбросе конфигурации. При переходе в раздел Аудит, он открывается в новой вкладке браузера. События Применения и Сброса конфигурации в разделе Аудит выделяются цветом.



> **Примечание:**
>
> Опция **Открыть Аудит** доступна только Пользователю с правом просматривать раздел Аудит.

3. В окне **Применение конфигурации** нажмите **Применить**.
4. Дождитесь окончания применения конфигурации.
   Применение новой конфигурации может занять некоторое время. Длительность применения не превышает 3-х часов. В верхней части рабочей области отображается счетчик времени с начала применения конфигурации:



Вы можете отредактировать конфигурацию и применить ее, даже если другая конфигурация находится в процессе применения. В этом случае применение конфигурации будет прервано, начнется применение отредактированной конфигурации.

4.1.3 Редактирование элемента

Цель:
Изменить атрибуты ранее созданного элемента.

Решение:

1. Перейдите в целевой раздел.
2. При необходимости перейдите в целевой подраздел или на целевую вкладку.
3. Для редактирования целевого элемента выделите его в списке с помощью левой кнопки мыши (либо выберите элемент в раскрывающемся списке) и нажмите  **Редактировать**.
4. Введите требуемые атрибуты элемента (атрибуты всех элементов описаны в статье "Интерфейс Консоли управления").
5. Нажмите **Сохранить**.

4.1.4 Удаление элемента

Цель:
Удалить элемент.

Решение:

1. Перейдите в целевой раздел.
2. При необходимости перейдите в целевой подраздел или на целевую вкладку.
3. Для удаления целевого элемента щелчком левой кнопки мыши выделите его из списка (либо выберите в раскрывающемся списке).

> **Примечание:**
>
> Вы можете удалить несколько элементов списка, при выделении удерживая клавишу *Shift* или *Ctrl*.

4. Нажмите  **Удалить**.
5. В окне подтверждения удаления нажмите **Да**.

4.1.5 Навигация по страницам

Справочная информация:
Навигация по страницам может осуществляться только в многостраничном режиме просмотра элементов интерфейса.
Многостраничный режим просмотра используется для более эргономичного использования рабочей области и доступен, когда в окне браузера отображается панель навигации по страницам:



Панель навигации по страницам

Цель:
Перейти к требуемой странице в многостраничном режиме.

Решение:

1. Перейдите в целевой раздел.
2. При необходимости перейдите в целевой подраздел или на целевую вкладку.
3. В раскрывающемся списке, расположенном в правой части панели навигации, укажите, какое количество элементов должно отображаться на странице.
4. Для навигации по страницам используйте кнопки с номерами страниц, содержащих элементы. Вы также можете использовать кнопки:
   - **|<** - для перехода на первую страницу;
   - **<** - для перехода на предыдущую страницу;
   - **>** - для перехода на следующую страницу;
   - **>|** - для перехода на последнюю страницу.

> **Примечание:**
>
> При использовании сортировки списка кнопки навигации работают в соответствии с обновленным списком.
> Например, при сортировке списка, начинающегося на "А", кнопка **>|** переведет на страницу, содержащую элементы на "Я". Но при обратной сортировке кнопка **>|** переведет на страницу, содержащую элементы на "А".

4.1.6 Изменение пароля пользователя

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

Цель:
Изменить пароль пользователя.

Решение:

1. Нажмите на кнопку меню пользователя и выберите пункт **Сменить пароль**.
   На экран будет выведено диалоговое окно **Смена пароля**.
2. В открывшемся диалоговом окне введите пароль, который будет назначен учетной записи, в поля:
   - **Новый пароль**;
   - **Подтверждение пароля**.

   > **Примечание:**
   >
   > Подробные рекомендации по составлению паролей см. в документе «*Infowatch Traffic Monitor. Руководство администратора*».

3. Нажмите **Сохранить**.

4.1.7 Выбор языка интерфейса

Цель:
Изменить язык интерфейса Консоли управления.

Решение:

1. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления Traffic Monitor") и в блоке **Сменить язык** выберите требуемый язык.
2. В открывшемся диалоговом окне **Изменение языка** нажмите **Да**.

Вернуть русский язык можно аналогичным способом: с той разницей, что названия будут отображаться на выбранном языке интерфейса.

4.1.8 Вызов справки

Цель:
Получить справочную информацию о работе в Системе.

Решение:

1. В правом верхнем углу рабочей области нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления Traffic Monitor").
2. В выпадающем списке в блоке **Помощь** выберите нужный тип справки:
   - **Онлайн-справка** – для перехода к онлайн-версии документации;
   - **Офлайн-справка** – для перехода к офлайн-версии документации.

   В новой вкладке браузера отобразится руководство пользователя InfoWatch Traffic Monitor в выбранном формате.
3. Ознакомьтесь с информацией, после чего закройте вкладку стандартным способом.

4.1.9 Просмотр сведений о Системе

Цель:
Получить справочную информацию о Системе.

Решение:

1. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления Traffic Monitor") и выберите **О системе**.

   На экран будет выведено окно **О системе**, в котором будут отображаться сведения об используемой версии Системы.
2. Ознакомьтесь с информацией, после чего закройте окно стандартным способом.

4.2 Работа с персонами и компьютерами

Для чего требуются персоны и компьютеры:
Списки персон и компьютеров облегчают офицеру безопасности работу с перехваченными объектами. Это происходит за счет учета информации об отправителях, получателях и компьютерах, участвующих в передаче данных.

Важно!

Чтобы изменения, описанные в данном разделе, отразились на работе Системы, примените конфигурацию: см. "Работа с конфигурацией Системы" и "Применение конфигурации Системы".

Формирование списков персон и компьютеров включает следующие шаги:

1. Создание группы, в которую будут добавлены персоны и компьютеры (см. "Создание группы персон и компьютеров").
2. Наполнение созданной группы (см. "Создание персон и компьютеров").
3. Настройка карточек для добавленных персон и компьютеров (см. "Настройка карточки персоны" и "Настройка карточки компьютера").
4. Назначение статуса персоне или компьютеру (см. "Назначение статуса персонам и компьютерам").

Вы можете экспортировать группы, персон и компьютеры для переноса конфигурации на другой сервер. Также доступен импорт конфигурации, выгруженной с другого сервера (см. "Экспорт и импорт персон").

После того как вы сформировали группы персон и компьютеров, вы можете выполнить с ними следующие действия:

- добавить персону или группу персон в периметр (см. "Работа с периметрами");
- создать политику контроля персон для группы или отдельных персон (см. "Создание политики контроля персон");
- создать запрос для поиска событий по персоне или компьютеру (см. "Создание запросов");
- просмотреть сводку по персоне или компьютеру (см. "Просмотр сводки по нарушениям/нарушителям");
- просмотреть снимки экрана для персоны или компьютера (см. "Просмотр снимков экрана").

См. также:

- "Раздел Персоны" - о разделе, в котором формируются списки персон и компьютеров;
- "Периметры" - о разделе, в котором настраиваются периметры;
- "Раздел События" - о разделе, в котором создаются поисковые запросы;
- "Раздел Сводка" - о разделе, в котором отображается сводка по объектам перехвата.

4.2.1 Создание группы персон и компьютеров

Цель:
Создать группу персон и компьютеров.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области выберите  **Пользовательские группы**.
3. На панели инструментов в левой части рабочей области нажмите  **Создать группу**.

4. В открывшемся окне укажите название новой группы и при необходимости введите примечание.
   Также вы можете указать контакты группы. В качестве контактов могут выступать **Электронная почта** и **Электронная почта Lotus**.
5. Нажмите **Сохранить**.

> **Важно**
>
> При создании новой группы события для этой группы будут отображаться, начиная с момента применения конфигурации.

Для редактирования группы выберите нужную группу в списке и нажмите . Чтобы удалить группу, выберите ее в списке и нажмите .

Вы можете добавить в пользовательскую группу имеющиеся группы Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro и FreeIPA. В этом случае при добавлении/удалении пользователей в группе Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro или FreeIPA состав соответствующей пользовательской группы обновится автоматически.

Чтобы добавить группу Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro или FreeIPA в пользовательскую группу, выделите в списке групп нужную группу Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro или FreeIPA с помощью мыши и, удерживая левую клавишу мыши зажатой, перетащите выбранный элемент в требуемую пользовательскую группу.

В одну пользовательскую группу можно добавить группы из различных доменов. Таким же способом можно добавить в пользовательскую группу отдельных пользователей из домена.

> **Примечание**
>
> Для того чтобы состав пользовательских групп, содержащих группы Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro или FreeIPA, обновлялся автоматически, необходимо выполнить синхронизацию с LDAP-сервером.

Наполнение созданных групп описано в статье "Создание персон и компьютеров".

Пример:

Требуется объединить сотрудников, находящихся под подозрением, в отдельную группу. Для этого:

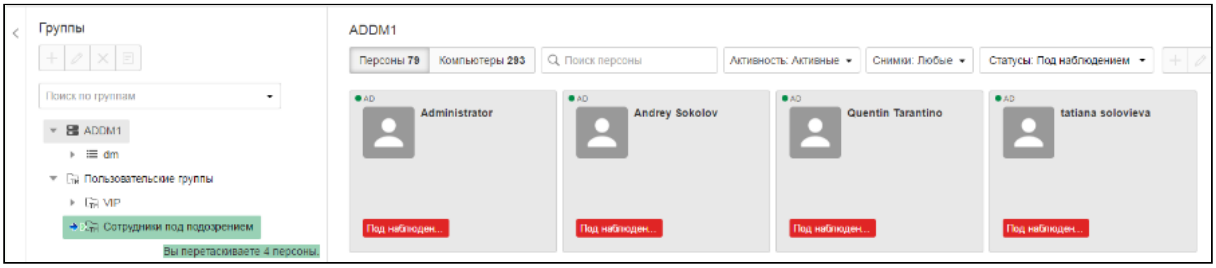
1. В узле  **Пользовательские группы** создайте группу "Сотрудники под подозрением".
2. С помощью поиска по персоне либо с помощью фильтров найдите сотрудников, которых требуется включить в группу.

   > **Совет**
   >
   > С помощью фильтров вы можете найти всех активных сотрудников, имеющих статус "Под наблюдением".

3. Добавьте найденных сотрудников в группу.

Совет

Вы можете выделить карточки требуемых сотрудников и перетащить их в группу с помощью мыши.



Вы можете использовать созданную группу "Сотрудники под подозрением" для оперативного мониторинга, создания правил контроля персон или поиска событий по сотрудникам, имеющим статус "Под наблюдением".

4.2.2 Создание персон и компьютеров

Справочная информация:
Вы можете наполнить группу персон и компьютеров одним из следующих способов:

- из LDAP-каталога – настраивается администратором Системы (см. документ «*Infowatch Traffic Monitor. Руководство администратора*»);
- средствами Traffic Monitor – формируется офицером безопасности, как описано в этой статье.

Цель:
Наполнить группу персон и компьютеров.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку:
   - **Персоны** – чтобы добавить персону;
   - **Компьютеры** – чтобы добавить компьютер.
4. На панели инструментов в правой части рабочей области нажмите  **Добавить**.
5. Укажите параметры новой персоны или компьютера (см. "Персоны" и "Компьютеры").
6. Нажмите **Сохранить**.

Чтобы отредактировать персону или компьютер, выберите нужный элемент в списке и нажмите .

Чтобы удалить персону или компьютер, выберите персону/компьютер в списке и нажмите .

Чтобы добавить персону из контакта в событии:

1. Выберите в событии контакт, который не был идентифицирован.
2. В открывшемся диалоговом окне выберите **Создать новую персону**.
3. Укажите параметры новой персоны и нажмите **Добавить**.

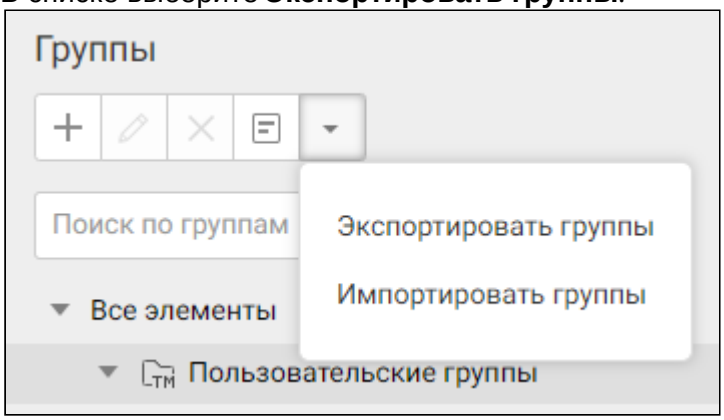
4.2.3 Экспорт и импорт персон

В Traffic Monitor также есть возможность **экспортировать** и **импортировать** группы персон. Это облегчает сохранение и перенос конфигурации на другой сервер.

Для экспорта убедитесь, что конфигурация Traffic Monitor не находится в процессе редактирования, а пользователю назначена привилегия **Импорт и экспорт организационной структуры**.
Экспортируются все группы, персоны и компьютеры.

Чтобы **экспортировать** из Traffic Monitor группы персон:

1. Перейдите в раздел **Персоны**.
2. Нажмите .
3. В списке выберите **Экспортировать группы**.



4. Система подготовит данные для экспорта, прогресс будет отображен в правом нижнем углу.
   В результате на компьютер будет сохранен zip-архив, содержащий xml-файл с описанием элементов конфигурации. В названии архива указана дата экспорта.
   Пример названия архива: `iwtm-group-20221213_141243.zip`.
   С помощью архива вы можете импортировать элементы конфигурации на другой сервер.

Для импорта групп персон необходимо сначала применить конфигурацию. Убедитесь, что конфигурация Traffic Monitor применена, а пользователю назначена привилегия **Импорт и экспорт организационной структуры**.

Чтобы **импортировать** группы персон в Traffic Monitor:

1. Перейдите в раздел **Персоны**.
2. Нажмите .
3. В списке выберите **Импортировать группы**.
4. В открывшемся окне укажите ранее экспортированный zip-архив, содержащий описание групп персон.
5. Дождитесь завершения импорта данных, прогресс будет отображен в правом нижнем углу.
6. Примените конфигурацию и обновите страницу, чтобы добавленные группы, персоны и компьютеры отобразились в консоли управления Traffic Monitor.

Особенности экспорта и импорта организационной структуры

Особенности экспорта:

- Экспортируется только примененная конфигурация.
- Экспортируются только сущности созданные или отредактированные в Traffic Monitor. Контакты и атрибуты экспортируются с привязкой к персоне.
  Пример: если персона была добавлена в Систему в результате LDAP-синхронизации, экспортированы будут только атрибуты и контакты, которые были добавлены или отредактированы в Traffic Monitor.
- Удаленные сущности не экспортируются.
- В Traffic Monitor 7.6 не экспортируются статусы персон и компьютеров.

Особенности импорта:

- При импорте сохраняется иерархия групп.
- Для импорта групп, персон или компьютеров, добавленных при LDAP-синхронизации, в Системе должна быть аналогичная сущность, иначе произойдет ошибка. Но остальной процесс импорта продолжится.
- Если у имеющейся в Системе и импортируемой сущностей совпадают имена, но отличаются идентификаторы (ID), сущность не будет импортирована.
- Если у имеющейся в Системе и импортируемой сущностей совпадают идентификаторы (ID), но отличаются имена, сущность будет импортирована.
- При совпадении имен и идентификаторов будут добавлены новые контакты и атрибуты, но если они уже присутствуют:
  - для сущностей, созданных при LDAD-синхронизации, имеющиеся контакты и атрибуты будут заменены на значения из файла.
  - для сущностей, созданных в Traffic Monitor, имеющиеся контакты и атрибуты останутся без изменений.

4.2.4 Настройка карточки персоны

Цель:

Наполнить данными карточку персоны.

Настройка карточки персоны состоит из следующих действий:

Действие	Описание
Добавление контакта персоне	Добавление контактных данных для созданной персоны
Добавление персоне компьютера	Добавить компьютер, связанный с персоной
Добавление персоны в группу	Добавление персоны в имеющуюся группу

Добавление контакта персоне

Цель:
Добавить или отредактировать контактные данные персоны.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.

3. В правой части рабочей области перейдите на вкладку **Персоны**.
4. Двойным щелчком левой кнопки мыши выделите нужную персону. Откроется карточка персоны.
5. На вкладке **Основное** в блоке **Контакты** нажмите .
6. В открывшейся форме **Добавление контакта** укажите требуемые параметры:
   - тип контакта: электронная почта, электронная почта Lotus, мобильный телефон, стационарный телефон, Skype, ICQ, Web-контакт, доменный аккаунт, профиль в социальных сетях и др.;
   - является ли контакт личным или рабочим;
   - значение (адрес или номер) контакта;
   - произвольное описание.
7. Нажмите **Сохранить**.

Примечание.

Значение контакта необходимо указывать в следующем формате:

-  – мобильный телефон (строка от 3 символов; может содержать только цифры, пробел, и символы: "-","_", "( )","+");
-  – стационарный телефон (строка от 3 символов; может содержать только цифры, пробел, и символы: "-","_", "( )","+");
-  – электронная почта (адрес в формате RFC);
-  – электронная почта Lotus (адрес в формате RFC);
-  – доменный аккаунт (адрес в формате RFC);
-  – контакт Skype (строка от 1 символа);
-  – аккаунт MS Teams, если установлен адаптер (строка от 1 символа);
-  – контакт ICQ (строка от 1 символа);
-  – профиль в социальной сети Facebook (строка от 1 символа);
-  – профиль в социальной сети ВКонтакте (строка от 1 символа);
-  – аккаунт Telegram (строка от 1 символа);
-  – аккаунт WhatsApp (строка от 1 символа);
-  – прочий веб-аккаунт (строка от 1 символа).

Мессенджеры WhatsApp и Telegram используют собственные форматы идентификаторов, для ассоциации персоны с перехватываемыми контактами мессенджеров рекомендуем использовать тип контакта Мобильный телефон.

Чтобы отредактировать ранее указанные контактные данные:

1. Выделите нужный контакт с помощью левой клавиши мыши и на панели инструментов нажмите .
2. Отредактируйте параметры контакта.
3. Нажмите **Сохранить**.

Чтобы добавить персоне новый контакт из события:

1. Выберите непроидентифицированный контакт в событии.

2. В открывшемся диалоговом окне выберите **Добавить контакт к персоне**.
3. Укажите персону из списка и нажмите **Сохранить**.
4. Нажмите **Да**, чтобы подтвердить добавление контакта.
5. В открывшемся диалоговом окне нажмите **Перейти к персоне**, чтобы убедиться в наличии нового контакта в карточке персоны.

Добавление компьютера для персоны

Цель:
Добавить персоне связанный компьютер.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Персоны**.
4. Двойным щелчком левой кнопки мыши выделите требуемую персону. Откроется карточка персоны.
5. На вкладке **Основное** в блоке **Компьютеры** нажмите .
6. В открывшемся окне **Добавить рабочую станцию** установите флажки в полях напротив требуемых компьютеров.
7. Нажмите **Сохранить**.

Добавление персоны в группу

Цель:
Добавить персону в имеющуюся группу.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Персоны**.
4. Двойным щелчком мыши выделите требуемую персону. Откроется карточка персоны.
5. На вкладке **Основное** в блоке **Группы** нажмите .
6. В открывшемся окне **Добавить группу** установите флажки напротив требуемых групп.
7. Нажмите **Сохранить**.

Если требуется удалить персону из текущей группы:

1. Выделите требуемую персону на вкладке **Персоны**.
2. На панели инструментов в правой части рабочей области нажмите  и в раскрывающемся списке нажмите **Удалить из группы**.
3. В окне подтверждения нажмите **Да**.

> **Важно!**
>
> Если персона состоит только в одной группе, то при выполнении этой команды персона будет удалена.

4.2.5 Настройка карточки компьютера

Цель:
Наполнить данными карточку компьютера.

Настройка карточки компьютера состоит из следующих действий:

Действие	Описание
Добавление компьютеру контакта	Добавление компьютеру контакта IP/DNS или доменного аккаунта
Добавление персоны для компьютера	Добавление персоны, связанной с данным компьютером
Добавление компьютера в группу	Добавление компьютера в имеющуюся группу

Добавление компьютеру контакта

Цель:
Указать для компьютера IP-адрес, DNS-имя или доменный аккаунт.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Компьютеры**.
4. Двойным щелчком мыши выделите требуемый компьютер. Откроется карточка компьютера.
5. На вкладке **Основное** в блоке **Контакты** нажмите .
6. В открывшейся форме **Добавление контакта** укажите требуемые параметры:
   - тип контакта: **IP**, **DNS** или **Доменный аккаунт**;
   - значение контакта: адрес IP, имя DNS или название доменного аккаунта;
   - произвольное описание.
7. Нажмите **Сохранить**.

Добавление персоны для компьютера

Цель:
Добавить персоне связанный компьютер.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Компьютеры.**
4. Двойным щелчком мыши выделите требуемый компьютер. Откроется карточка компьютера.
5. На вкладке **Основное** в блоке **Персоны** нажмите .

6. В открывшемся окне **Добавить персону** установите флажки напротив требуемых персон.
7. Нажмите **Сохранить**.

Для удаления добавленной персоны выделите ее в списке и нажмите .

Добавление компьютера в группу

Цель:
Добавить компьютер в имеющуюся группу.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Компьютеры**.
4. Двойным щелчком мыши выделите требуемый компьютер. Откроется карточка компьютера.
5. На вкладке **Основное** в блоке **Группы** нажмите .
6. В открывшемся окне **Добавить группу** установите флажки напротив требуемых групп.
7. Нажмите **Сохранить**.

Если требуется **удалить компьютер** из текущей группы:

1. Выделите требуемый компьютер на вкладке **Компьютеры**.
2. На панели инструментов в правой части рабочей области нажмите  и в раскрывающемся списке нажмите **Удалить из группы**.
3. В открывшемся окне подтверждения нажмите **Да**.

> **Важно!**
>
> Если компьютер состоит только в одной группе, то при выполнении этой команды он будет удален.

4.2.6 Назначение статуса персонам и компьютерам

Цель:
Назначить статус персоне или компьютеру.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку:
   - **Персоны** – чтобы назначить статус персоне;
   - **Компьютеры** – чтобы назначить статус компьютеру.
4. Выделите требуемую персону или компьютер.
5. На панели инструментов в правой части рабочей области нажмите  и в раскрывающемся списке выберите **Назначить статус**.

6. В открывшемся диалоговом окне укажите требуемый статус и при необходимости введите описание.
7. Нажмите **Сохранить**.

> **Примечание:**
>
> Статус *Новый* присваивается персоне или компьютеру в момент создания в Системе и сохраняется в течение 30 дней. В случае импорта персон и компьютеров из Active Directory, Samba DC, Domino Directory, Astra Linux Directory, FreeIPA или Astra Linux Directory Pro статус *Новый* сохраняется в течение 30 дней с момента создания записей в Active Directory, Samba DC, Domino Directory, FreeIPA или Astra Linux Directory Pro соответственно.

См. также:

- "Статусы" – о подразделе, в котором ведется работа со статусами персон и компьютеров

4.2.7 Просмотр снимков экрана

Предварительные настройки:

Для того чтобы снимки экрана отображались в карточках персон и компьютеров, должна быть выполнена синхронизация с Active Directory или Samba DC.

Если в вашей организации не используется Active Directory и Samba DC, либо из-за технических ограничений синхронизация невозможна, то для просмотра снимков экрана выполните следующие действия:

1. Создайте карточки персон и компьютеров, для которых вы хотите получать снимки экрана (см. "Создание персон и компьютеров").

   > **Примечание:**
   >
   > На рабочих станциях под управлением ОС Astra Linux или РЕД ОС снимки экрана создаваться не будут.

2. Для персон укажите доменный аккаунт (см. "Добавление контакта персоне").

   > **Примечание.**
   >
   > Доменный аккаунт указывается в формате *name@client*, где *name* – это имя пользователя, а *client* – имя компьютера.

3. Для компьютеров укажите NetBIOS-имя или имя устройства (см. "Добавление компьютеру контакта").

> **Примечание.**
>
> В случае синхронизации с Domino Directory, Astra Linux Directory, Astra Linux Directory Pro или FreeIPA для персон также можно указать доменный аккаунт.

Важно!

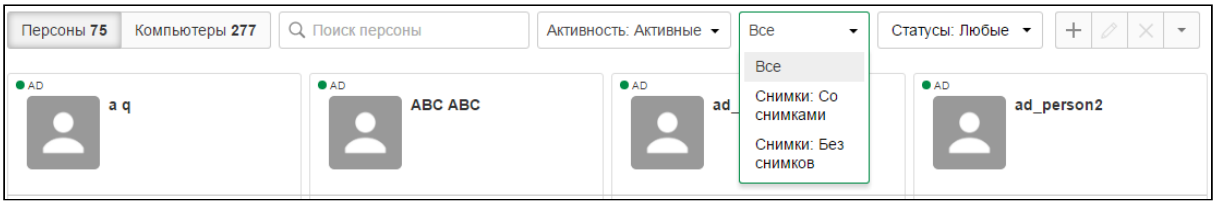
Указанные шаги необходимо выполнить до создания правила Device Monitor (см. "Правило (DM) для ScreenShot Monitor" в *"InfoWatch Device Monitor. Руководство пользователя"*) и распространения политики Device Monitor, содержащей данное правило, на рабочие станции. В противном случае снимки экрана не будут отображаться в Системе.

Цель:

Просмотреть перехваченные снимки экрана для персоны или компьютера.

Решение:

1. Перейдите в раздел **Персоны**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на требуемую вкладку: **Персоны** или **Компьютеры**. Отобразится список персон или компьютеров, входящих в выбранную группу.
4. Вы можете найти нужную персону или компьютер, воспользовавшись полем **Поиск** (поиск выполняется по имени персоны или IP-адресу компьютера).
   При наличии большого количества персон/компьютеров вы можете отфильтровать элементы по наличию снимков экрана: щелкните левой клавишей мыши по области фильтра и в раскрывающемся списке выберите **Снимки: Со снимками экрана**.



   В результате будут показаны персоны или компьютеры, удовлетворяющие условиям фильтрации.
5. Чтобы перейти к просмотру снимков экрана для выбранной персоны или выбранного компьютера, выполните одно из следующих действий:
   - выделите в списке персону или компьютер, на панели инструментов нажмите  и в раскрывающемся списке выберите **Показать снимки экрана**;
   - дважды щелкните левой клавишей мыши по персоне или компьютеру и в открывшейся карточке персоны/компьютера перейдите на вкладку **Снимки экрана**.

   Вкладка **Снимки экрана** содержит все снимки экрана, сделанные для данной персоны или данного компьютера.
6. Вы можете указать следующие критерии отображения снимков экрана:
   - **Приложение** – начните вводить название приложения и выберите нужное приложение из предложенных вариантов. Или нажмите  и в открывшемся окне установите флажки напротив выбранных приложений, после чего нажмите **Сохранить**.

> **Примечание.**
>
> При вводе название вручную вы можете использовать маску. Для этого введите символ * в начале или в конце строки для замены одного или нескольких символов.

- **Персона**/**Компьютер** – если вы просматриваете снимки экрана для персоны, вы можете отфильтровать снимки экрана по имени компьютера. Аналогичным образом, при просмотре снимков экрана для компьютера, вы можете указать персону, для которой требуется показать снимки экрана.
- **Дата** – укажите период, за который нужно показывать снимки экрана. По умолчанию снимки экрана выводятся за все время.

> **Примечание.**
>
> При выборе периода в календаре вы можете указать дату и время. Даты, для которых доступны снимки экрана, подсвечены синим цветом.

7. После того как вы указали требуемые критерии, нажмите **Применить**. Будут показаны снимки экрана, удовлетворяющие заданным критериям.
8. Чтобы посмотреть более подробную информацию по выбранному снимку экрана, щелкните по нему клавишей мыши. Будет показан снимок экрана и его атрибуты.
9. Вы можете увеличить или уменьшить масштаб снимка, скачать изображение на ваш компьютер, просмотреть предыдущий и следующий снимок (подробнее см. "Снимки экрана").
10. Чтобы закрыть окно просмотра, нажмите **X**.

4.3 Работа со справочниками

> **Важно!**
>
> Чтобы изменения, описанные в данном разделе, отразились на работе Системы, примените конфигурацию: см. "Работа с конфигурацией Системы" и "Применение конфигурации Системы".

Для чего требуются справочники:
Для группировки однотипных данных, используемых при создании политик.

Работа со справочниками состоит из следующих действий:

- Работа с тегами
- Работа с веб-ресурсами
- Работа со статусами
- Работа с периметрами

См. также:

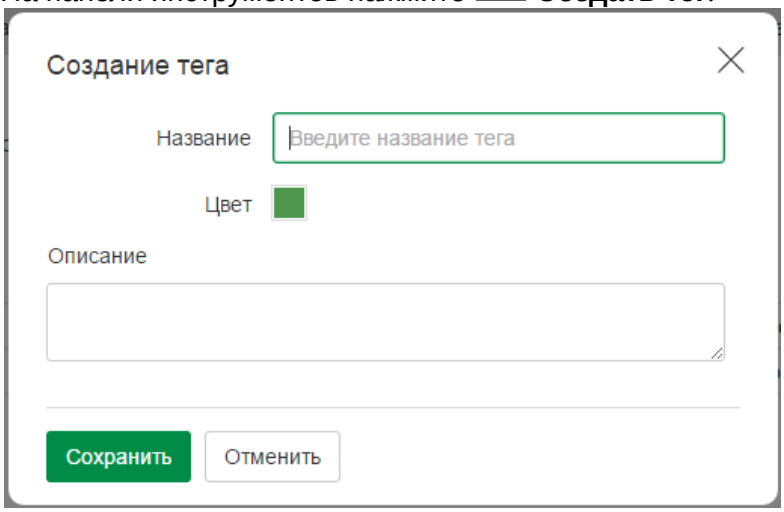
- "Раздел Списки" – о разделе, в котором ведется работа со списками

4.3.1 Работа с тегами

Цель:
Создать тег.

Решение:

1. Перейдите в раздел **Списки**, подраздел **Теги**.
2. На панели инструментов нажмите + **Создать тег**.



3. Укажите атрибуты добавляемого тега (см. "Теги").
4. Нажмите **Сохранить**.
5. При необходимости повторите добавление для наполнения справочника тегов.

Чтобы отредактировать тег, выделите его в списке и нажмите .

Если требуется удалить тег, выделите его в списке и нажмите .

4.3.2 Работа с веб-ресурсами

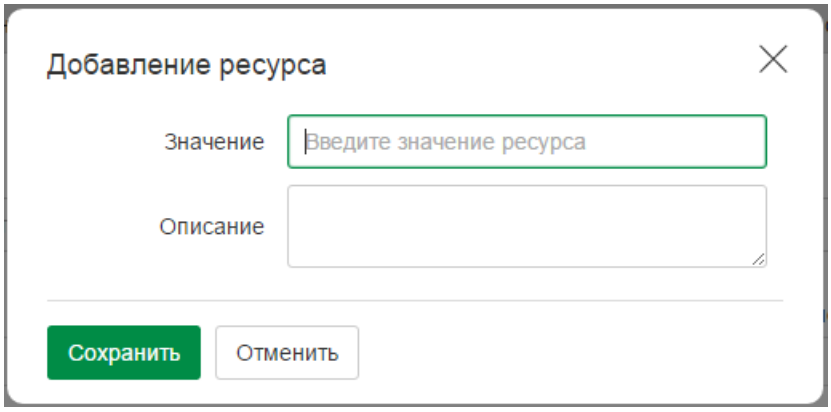
Цель:
Указать веб-ресурсы, посещение которых будет детектироваться Системой как нецелевое использование рабочего времени. Для этого требуется:

1. Создать список веб-ресурсов.
2. Добавить ресурсы в список.

Решение:

1. Создание группы ресурсов.
   a. Перейдите в раздел **Списки**, в подраздел **Веб-ресурсы**.
   b. В левой части рабочей области нажмите + **Создать список ресурсов**.
   c. В открывшемся окне введите название и описание списка ресурсов.
   d. Нажмите **Сохранить**.
2. Добавление ресурса.
   a. Перейдите в раздел **Списки**, в подраздел **Веб-ресурсы**.
   b. В левой части рабочей области щелчком левой кнопки мыши выделите требуемый список ресурсов.

c. В правой части рабочей области на панели инструментов ресурсов нажмите + **Создать ресурс**.



d. В открывшемся окне **Добавление ресурса** введите атрибуты ресурса:
   - в поле **Значение** - название ресурса в сети Интернет;
   - в поле **Описание** - комментарий к записи о ресурсе (необязательно).

e. Нажмите **Сохранить**.

Пример:

При вводе в поле **Значение** доменного имени EXAMPLE.COM будут добавлены также домены следующих уровней: LIBRARY.EXAMPLE.COM и т.д.

Важно!

По завершении редактирования списка веб-ресурсов требуется применить обновленную конфигурацию (см. "Применение конфигурации Системы").

Пример:

Если требуется, чтобы при посещении сотрудниками интернет-сайта EXAMPLE.COM Система помечала объект перехвата как *НЕЦЕЛЕВОЙ_САЙТ*:
Офицер безопасности создает группу ресурсов *НЕЦЕЛЕВОЙ_САЙТ*, а в созданной группе - ресурс *EXAMPLE.COM*.

Дополнительные сведения:

Редактирование и удаление веб-ресурсов и их групп выполняются стандартным способом:

- Редактирование элемента
- Удаление элемента

4.3.3 Работа со статусами

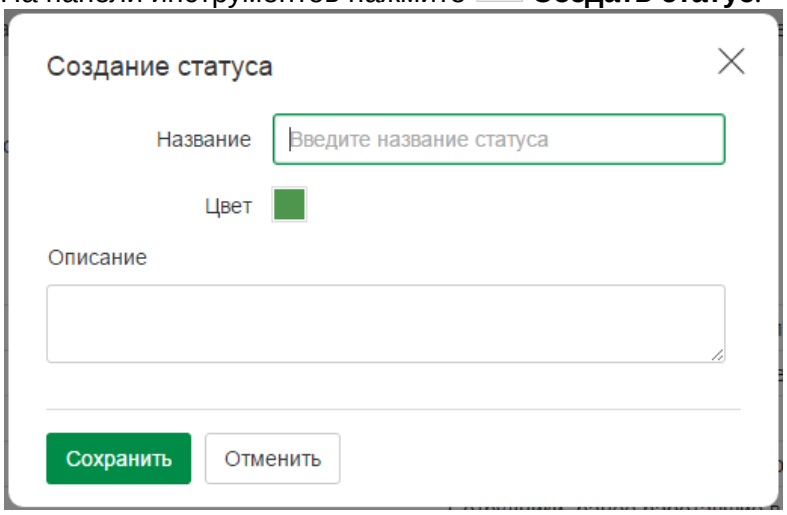
Цели:

1. Создать статус, характеризующий персону или компьютер.
2. Создать политику для контроля персон и компьютеров, объединенных общим статусом.

Чтобы создать новый статус:

1. Перейдите в раздел **Списки**, в подраздел **Статусы**.

2. На панели инструментов нажмите **Создать статус**.



3. Укажите атрибуты добавляемого статуса (см. "Статусы").
4. Нажмите **Сохранить**.

Чтобы отредактировать статус, выберите требуемый статус и нажмите .

Чтобы удалить статус, выберите требуемый статус и нажмите .

Чтобы создать политику контроля персон непосредственно из подраздела Статусы:

1. Перейдите в раздел **Списки**, в подраздел **Статусы**.
2. В списке статусов выделите требуемый статус.
3. На панели инструментов нажмите **Создать политику**.
   Откроется раздел **Политики**, в котором будет отображаться новая политика контроля персон для компьютеров и персон с указанным статусом (подробнее см. "Раздел Политики").

4.3.4 Работа с периметрами

Справочная информация:

Периметры позволяют логически разделить организацию на структурные единицы и отслеживать движение трафика. Периметры могут включать элементы различных типов: домены, группы персон и компьютеров, веб-ресурсы и т.д.

Периметры могут быть двух типов:

- Предустановленные (подробнее см. "Периметры")
- Созданные вручную на основе следующих элементов:
  - Персона
  - Группа персон
  - Веб-ресурсы
  - Контакты:
    - Адрес электронной почты
    - Телефон
    - Skype-контакт
    - ICQ-контакт

- Почтовый домен
- Lotus-контакт

> **Примечание:**
>
> Для выбора LDAP-домена в качестве элемента периметра необходимо предварительно настроить синхронизацию с LDAP-сервером и добавить домен через закладку **Группы**.

Цель:

1. Создать периметр.
2. Добавить элемент в периметр.
3. Экспортировать/импортировать периметр.

Решение:

Цель 1. Создание периметра. Чтобы создать периметр:

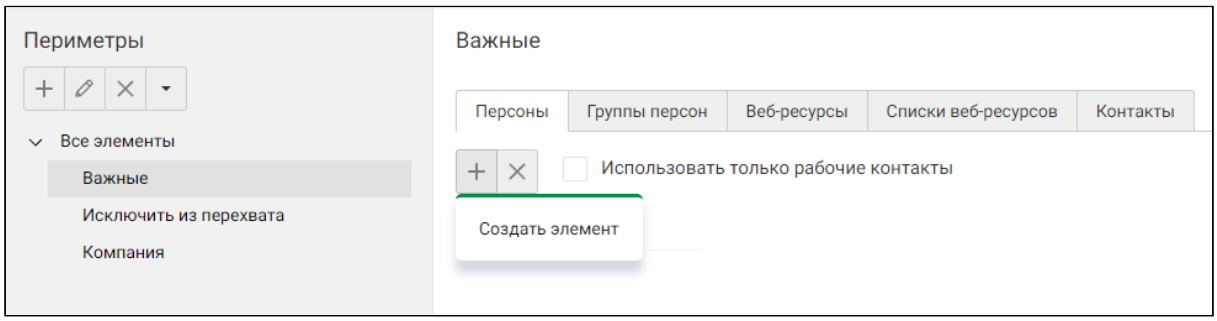
1. Перейдите в раздел **Списки**, в подраздел **Периметры**.
2. В левой части рабочей области нажмите  **Создать периметр**.
3. В открывшемся диалоговом окне в поле **Название** укажите название добавляемого периметра.
4. В поле **Описание** введите описание периметра (необязательно).
5. Нажмите **Сохранить**.

Чтобы отредактировать периметр, выберите нужный периметр и нажмите .

Чтобы удалить периметр, выберите нужный периметр и нажмите .

Цель 2. Добавление элемента в периметр. Чтобы добавить элемент в периметр:

1. Перейдите в раздел **Списки**, в подраздел **Периметры**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите нужный периметр.
3. В правой части рабочей области на одной или нескольких нужных вкладках *Персоны, Группы персон, Веб-ресурсы, Списки веб-ресурсов, Контакты* нажмите  **Создать элемент**.



4. В появившемся поле укажите один или несколько элементов одним из следующих способов:
   - Для *Персоны*, *Группы персон* или *Списка веб-ресурсов*:
     - начните вводить название элемента в поле и выберите требуемую запись из раскрывшегося списка;

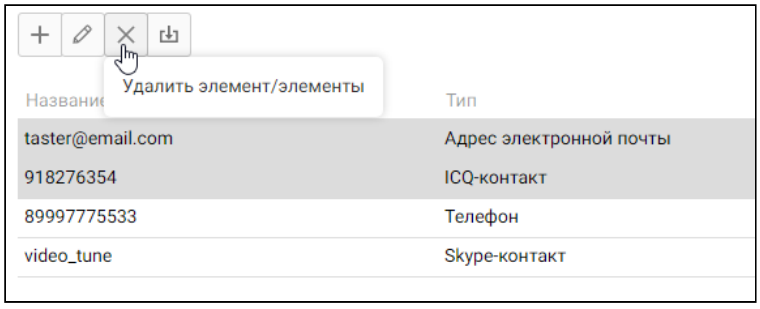
- нажмите  **Добавить** справа от поля и в открывшемся диалоговом окне установите флажок в поле с выбранным элементом. Для поиска нужного элемента воспользуйтесь строкой поиска;
- если требуется, установите флаг **Использовать только рабочие контакты**. Личные контактные данные персоны/группы использоваться в периметре не будут. Нажмите **Сохранить**.

> **Примечание.**
>
> После добавления в периметр персоны/группы персон можно перейти в ее карточку в разделе **Персоны**, нажав на имя персоны/группы персон.

- Для *Веб-ресурсов* и *Контактов* – введите название или значение в поле и нажмите **Enter**.
  - нажмите , введите название элемента и нажмите **Сохранить**. Для *Контакта* дополнительно укажите нужный из типов: *Адрес электронной почты, Почтовый домен, ICQ-контакт, Lotus-контакт, Телефон, Skype-контакт*;
  - нажмите  **Массовая загрузка элементов** и приложите csv-файл со списком элементов, дождитесь успешной загрузки и нажмите **Сохранить**.

> **Примечание:**
>
> CSV-файл должен представлять собой список с одним столбцом, без заголовка, где каждый email-адрес, почтовый домен или веб-ресурс располагается на новой строке.

5. Введенные значения будут добавлены в список элементов. Чтобы удалить отдельный или несколько элементов из списка, выделите их и нажмите  **Удалить элемент/элементы**.

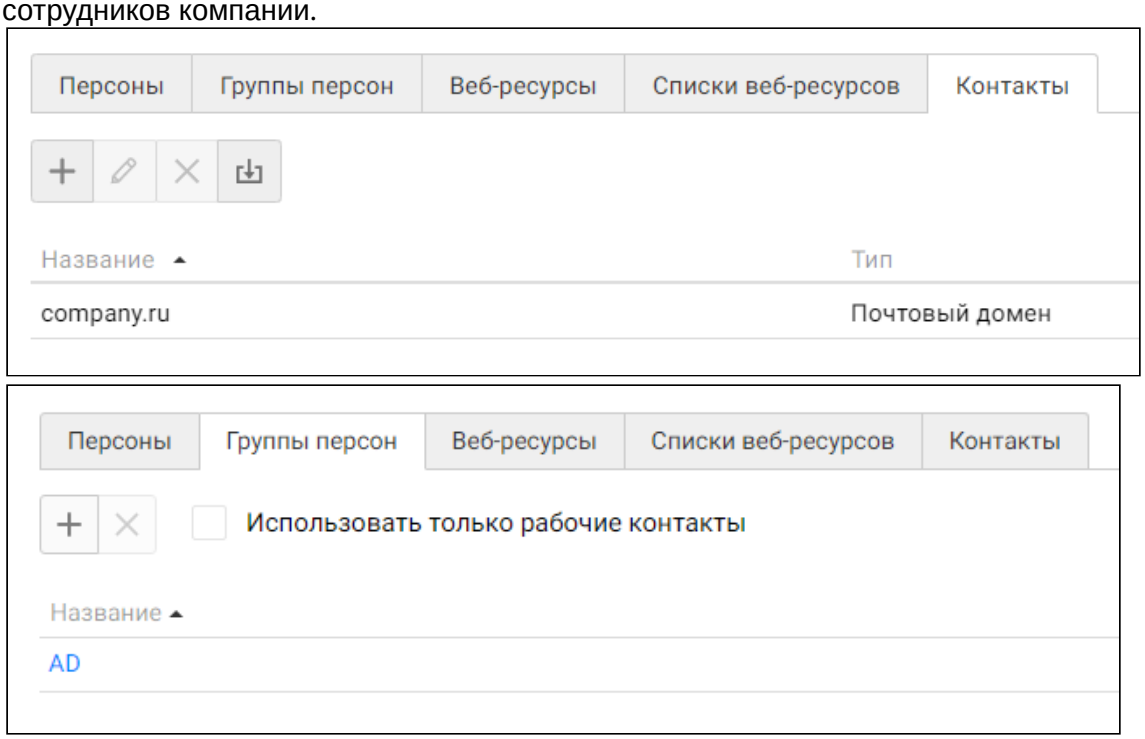


> **Важно!**
>
> Не рекомендуется создавать более 15 периметров с количеством элементов более 2000 в каждом их них.

Пример:

В компании используется корпоративная почта с выделенным доменом, для новых сотрудников почта генерируется автоматически по шаблону: `фамилия@ company.ru` . Требуется контролировать передачу конфиденциальной информации за пределы компании по электронной почте. При этом пересылка документов внутри компании разрешена. В этом случае:

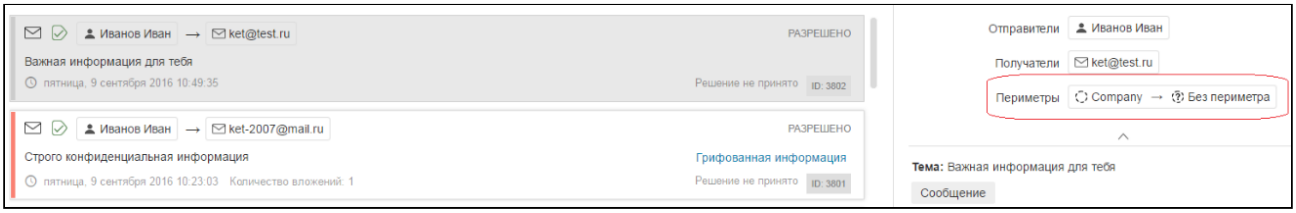
1. Создайте периметр *Компания* (если в Системе уже есть периметр *Компания*, пропустите этот шаг).
2. Добавьте в периметр почтовый домен `company.ru` и группу персон `AD` , содержащую сотрудников компании.



3. Сохраните периметр.

После этого отправка сообщений на личные почтовые адреса будет определяться Системой как выход информации за пределы компании.

Создав запрос в разделе **События** (подробнее см. "Создание запросов"), вы можете быстро найти все события отправки данных за пределы компании.



Цель 3. Экспорт и импорт периметров

В Traffic Monitor есть возможность **экспортировать** и **импортировать** периметры. Данная функциональность облегчает сохранение и перенос конфигурации на другой сервер.

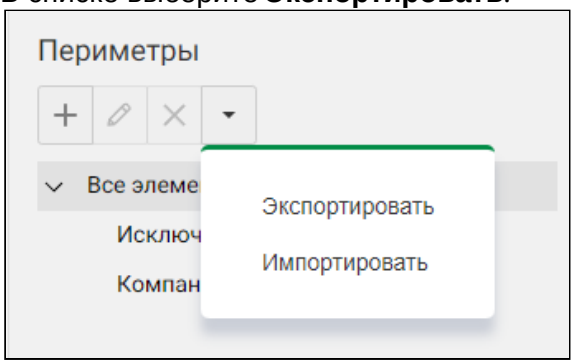
> **Важно!**

В текущей версии переносятся только элементы вкладок **Веб-ресурсы** и **Контакты**.

Для экспорта периметров убедитесь, что конфигурация Traffic Monitor не находится в процессе редактирования, а пользователю назначена привилегия **Импорт и экспорт периметров**. Экспортируются все периметры, а не только выбранный.

Чтобы **экспортировать** из Traffic Monitor периметры:

1. Перейдите в раздел **Списки**, в подраздел **Периметры**.
2. Нажмите .
3. В списке выберите **Экспортировать**.



4. Система подготовит периметры для экспорта, прогресс будет отображен в правом нижнем углу.
   В результате на компьютер будет сохранен zip-архив, содержащий xml-файл с описанием элементов конфигурации. В названии архива указана дата экспорта.
   Пример названия архива: `iwtm-perimeter-20220808_193432.zip`.
   С помощью архива вы можете импортировать элементы конфигурации на другой сервер.

Для импорта периметров необходимо сначала применить конфигурацию. Убедитесь, что конфигурация Traffic Monitor применена, а пользователю назначена привилегия **Импорт и экспорт периметров**.

Чтобы **импортировать** периметры в Traffic Monitor:

1. Перейдите в раздел **Списки**, в подраздел **Периметры**.
2. Нажмите .
3. В списке выберите **Импортировать**.
4. В открывшемся окне укажите ранее экспортированный zip-архив, содержащий описание периметров.
5. Дождитесь завершения импорта периметров, прогресс будет отображен в правом нижнем углу.
6. Примените конфигурацию и обновите страницу, чтобы добавленные периметры и элементы отобразились в консоли управления Traffic Monitor.

4.4 Работа с базой технологий

Важно!

Чтобы изменения, описанные в данном разделе, отразились на работе Системы, примените конфигурацию: см. "Работа с конфигурацией Системы" и "Применение конфигурации Системы".

Для чего требуется база технологий:
С помощью базы технологий вы можете указать Системе, какая информация является конфиденциальной в рамках компании. Разглашение этой информации будет считаться нарушением политики корпоративной безопасности. На основе базы технологий Система анализирует действия персон и выявляет нарушения политики корпоративной безопасности (например, отправку конфиденциального документа за пределы компании).

База технологий – это набор элементов (терминов, текстовых объектов, эталонных документов и пр.), используемых для анализа перехваченных данных.

Помимо базы технологий, при анализе действий персон также используется список ресурсов, который позволяет выявить нецелевое использование рабочего времени (например, просмотр развлекательных интернет-сайтов с рабочего компьютера). Подробнее об указании нецелевых ресурсов см. "Работа с веб-ресурсами".

Настройка анализа действий персон состоит из следующих действий:

1. Определение конфиденциальной информации – создание базы технологий.
2. Указание нецелевых ресурсов – создание списка ресурсов, посещение которых считается нецелевым использованием рабочего времени.
3. Создание объектов защиты на основе элементов, входящих в базу технологий.

После этого вы можете создать политику и указать Системе, каким образом следует реагировать на обнаружение в перехваченных данных объектов защиты или отправку запросов на ресурсы, включенные в список нецелевых (см. "Настройка реакций Системы").

См. также:

- "Раздел Технологии" – о разделе, в котором ведется работа с базой технологий
- "Веб-ресурсы" – о подразделе, в котором ведется работа со списком ресурсов
- "Раздел Объекты защиты" – о разделе, в котором ведется работа с объектами защиты

4.4.1 Определение конфиденциальной информации

Цель:

Добавить в базу технологий элементы, на основе которых Система будет определять наличие конфиденциальных данных в объектах перехвата.

Решение:

1. Перейдите в какой-либо подраздел раздела **Технологии**: **Категории и термины**, **Текстовые объекты**, **Эталонные документы**, **Бланки**, **Печати, Выгрузки из БД**, **Графические объекты** или **Автолингвист**.
2. Создайте новую категорию в подразделе **Категории и термины** или новый каталог в других подразделах.
3. Наполните созданную категорию (или созданный каталог) примерами конфиденциальных данных, наличие которых в трафике будет указывать Системе на нарушение политики безопасности.
4. При необходимости повторите шаги 2 и 3.

Важно!

По завершении настройки базы технологий требуется применить обновленную конфигурацию (см. "Применение конфигурации Системы").

Подробнее о работе с элементами технологий:

Название технологии	Описание технологии	Действие
Категории и термины	Набор терминов и их категорий. Термин – слово или словосочетание, нахождение которого в анализируемом тексте увеличивает степень соответствия этого текста той категории, к которой относится найденный термин	Создание терминов и их категорий
Текстовые объекты	Текстовая информация, извлеченная из тела объекта и его вложений. Не содержит элементов форматирования или разметки. Используется для решения задач анализа и поиска	Создание текстовых объектов
Эталонные документы	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	Работа с эталонными документами
Бланки	Бланк, версия которого ищется в сетевом трафике. Бланками могут служить различные анкеты, квитанции и прочее. Бланки хранятся в системе в виде цифровых отпечатков; текст недоступен для просмотра ни пользователям, ни администраторам Системы	Создание бланков
Печати	Изображение печати, которое ищется в сетевом трафике. Печатями могут быть изображения круглых оттисков, которые используются в организациях	Создание печатей

Название технологии	Описание технологии	Действие
Выгрузки из баз данных	Часть базы данных, цитаты из которой ищутся в анализируемом тексте. Выгрузками из БД могут быть списки заработных плат сотрудников, другие личные данные и прочее	Создание выгрузок из БД
Графические объекты	Обучение автоматического классификатора разным типам изображений, которые будут детектироваться в сетевом трафике. Графическими объектами могут быть изображения разворота паспорта, кредитной карты, географических карт, фото и др.	Работа с графическими объектами
Автолингвист	Обучение автоматического классификатора на типичных текстовых документах, которые будут детектироваться в сетевом трафике. Текстовыми документами могут быть различных текстовых форматов файлы, используемые в организации.	Работа С Автолингвистом

См. также:

- "Раздел Технологии" – о разделе, в котором ведется работа с базой технологий

Работа с категориями и терминами

Справочная информация:
Термины – набор слов и словосочетаний, необходимых для проведения лингвистического анализа. Все термины сгруппированы по *категориям*.
Категории служат для классификации возможных нарушений политики безопасности. Наличие в тексте термина, принадлежащего к определенной категории, позволяет соотнести текст с этой категорией.

Цели:

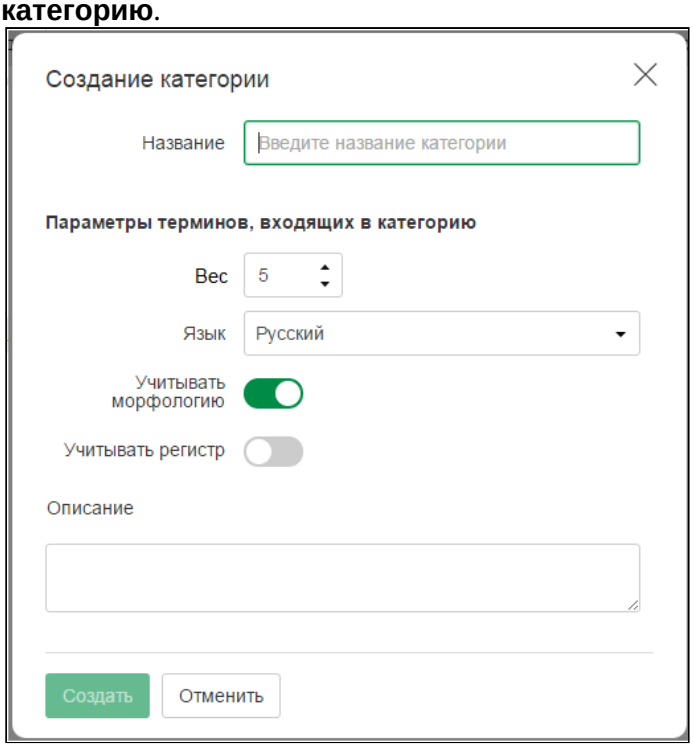
1. Создать категорию терминов.
2. Создать термин внутри категории.

Решение:

1. Создание категории.

a. Перейдите в раздел **Технологии** → **Категории и термины**.

b. В левой части рабочей области на панели инструментов нажмите  **Создать категорию**.



c. Укажите требуемые атрибуты для категории (см. "Категории").
d. Нажмите **Создать**.

Чтобы отредактировать категорию, выберите нужную категорию в списке и нажмите .

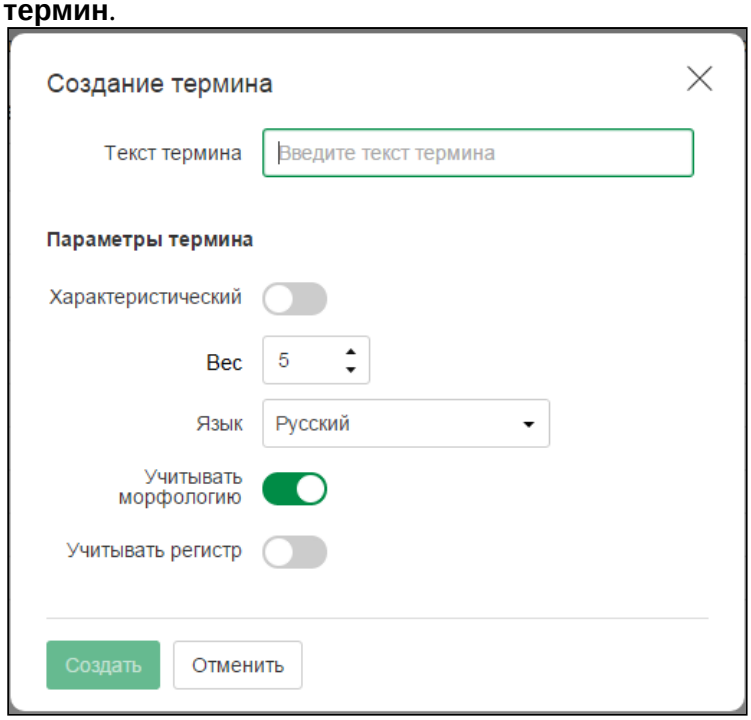
Если требуется удалить категорию, выберите нужную категорию и нажмите .

2. Создание термина.

a. Перейдите в раздел **Технологии → Категории и термины**.
b. В левой части рабочей области выделите требуемую категорию.

> **Примечание.**
>
> Для добавления терминов доступны только те категории, которые не включают других вложенных категорий.

c. На панели инструментов в правой части рабочей области нажмите  **Создать термин**.



d. Укажите требуемые атрибуты (см. "Термины").
e. Нажмите **Сохранить**.

> **Примечание:**
>
> При добавлении в категорию термины по умолчанию наследуют параметры категории. При создании или редактировании термина его параметры можно изменить.

Чтобы отредактировать термин, выберите нужный термин в списке и нажмите .

Если требуется удалить термин, выберите нужный термин и нажмите .

Пример 1:

Требуется, чтобы при наличии в трафике хотя бы одного словосочетания "Дата выдачи ИНН", Система помечала объект перехвата как *Дата выдачи ИНН*. Для этого:

1. Выберите нужную категорию.
2. Добавьте в нее термин *Дата выдачи ИНН*.
3. Включите настройку **Характеристический**.

При передаче данных, среди которых обнаруживается указанное словосочетание, Система присваивает объекту перехвата категорию *Дата выдачи ИНН*. Если настройка **Характеристический** выключена, то для присвоения категории событию необходимо, чтобы в событии встретилось минимум три разных весовых термина из категории.

Пример 2:
Требуется, чтобы при наличии в трафике фрагментов программного кода, Система помечала объект перехвата как утечку кода программы. Для этого:

1. Создайте категорию *Утечка кода программы*.

2. Добавьте в нее термины: *Procedure*, *Result*, *Create Sequence* с параметрами по умолчанию.

> **Примечание:**
>
> В случае, когда используются параметры по умолчанию, двух терминов может быть недостаточно для срабатывания категории. Рекомендуется указать минимум три термина.

В результате анализа переданных данных, среди которых обнаруживаются указанные термины, Система присваивает объекту перехвата категорию *Утечка кода программы*

> **Важно!**
>
> Объекту перехвата присваивается только категория, непосредственно содержащая сработавший элемент (термин, эталонный документ и др.).
> ***Например:***
> Категория А содержит категорию Б. Категория Б содержит термин В. Во время анализа события Система обнаружила в теле события наличие термина В.
> В этом случае объекту перехвата будут проставлены термин В и категория Б.

Работа с текстовыми объектами

Цели:

1. Создать каталог текстовых объектов.
2. Создать текстовый объект и указать его значение.
3. Добавить системный текстовый объект в выбранный каталог.

Решение:

1. Создание каталога текстовых объектов

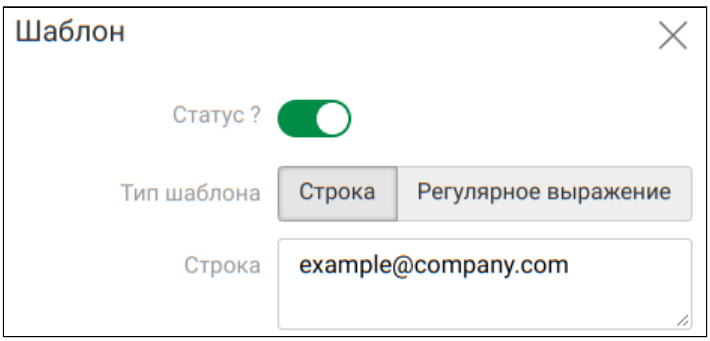
a. Перейдите в раздел **Технологии**->**Текстовые объекты**.
b. В левой части рабочей области на панели инструментов нажмите  **Создать каталог текстовых объектов**.
c. В открывшемся окне введите название и описание каталога.
d. Нажмите **Сохранить**.

2. Создание текстового объекта и указание его значения

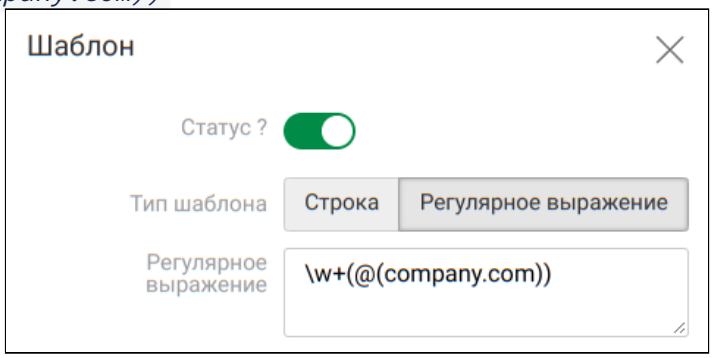
a. Перейдите в раздел **Технологии**->**Текстовые объекты**.
b. В левой части рабочей области щелчком левой кнопки мыши выделите каталог, внутри которого будет создан текстовый объект.
c. В правой части рабочей области на панели инструментов текстовых объектов нажмите  **Создать текстовый объект**.
d. Введите название и описание текстового объекта.
e. Нажмите **Создать**. Новый текстовый объект будет добавлен в список.
f. Выделите текстовый объект в списке и нажмите  **Редактировать**.
g. Создайте шаблон для текстового объекта и укажите его параметры (см. "Шаблоны текстовых объектов").

h. Нажмите **Сохранить**.

- ***Пример 1:***
  Требуется, чтобы Система определяла наличие в трафике адреса электронной почты "example@company.com" и определяла его как текстовый объект EXAMPLE_MAIL. Для этого:
  1. Создайте активный текстовый объект *EXAMPLE_MAIL* .
  2. Перейдите в режим редактирования объекта.
  3. Создайте для текстового объекта активный шаблон, указав в качестве значения строку `example@company.com`



- ***Пример 2:***
  Требуется, чтобы Система определяла наличие в трафике адреса электронной почты с доменом "company.com" и определяла его как текстовый объект *COMPANY_MAIL* . Для этого:
  1. Создайте активный текстовый объект *COMPANY_MAIL.*
  2. Перейдите в режим редактирования объекта.
  3. Создайте для текстового объекта активный шаблон, указав в качестве значения регулярное выражение:
     `\w+(@(company.com))`



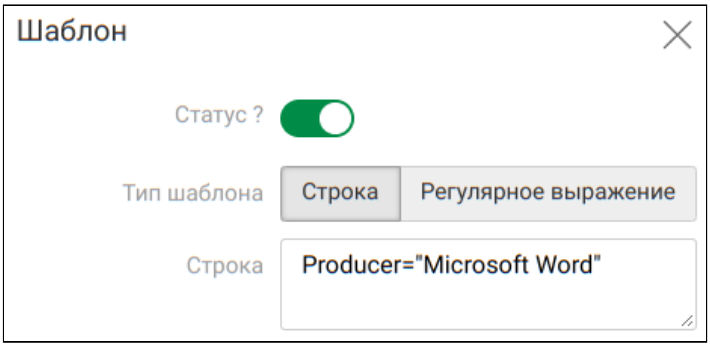
> **Примечание:**
>
> Подробнее о регулярных выражениях см. статьи Базы знаний: "Синтаксис регулярных выражений" и "Описание макросов для шаблонов текстовых объектов".

- ***Пример 3:***
  Требуется, чтобы агент Device Monitor блокировал передачу PDF-файла, если документ был преобразован в формат PDF с помощью Microsoft Word.

> **Примечание:**
>
> Агент Device Monitor извлекает из PDF-файла информацию о свойствах документа. Данные о свойствах добавляются в конец извлеченного из файла текста.
>
> **Подробнее об извлечении свойств PDF документов**
>
> Извлекаются названия и значения следующих свойств:
>
> - Author – автор документа;
> - Title – заголовок документа;
> - Subject – тема документа;
> - Keywords – ключевые слова документа;
> - Creator – приложение, в котором создан исходный документ;
> - Producer – приложение, в котором документ был сконвертирован в формат PDF.
>
> Данные о каждом свойстве добавляются в конец извлеченного из файла текста в формате: *название свойства="значение свойства"*. Данные о свойстве добавляются, если установлено значение свойства. Каждая запись добавляется с новой строки:
>
> ```
> Author="Ivanov Ivan"
> Creator="Microsoft Word"
> Keywords="договор; проект; бухгалтерия"
> Producer="Microsoft Word"
> Subject="Проект договора"
> Title="Проект договора N123"
> ```
>
> **Важно:** Если значение свойства Keywords было удалено, то запись с последним указанным значением Keywords все равно будет добавлена в конец извлеченного из PDF-файла текста.

Если в извлеченных данных о свойствах PDF-документа содержится строка *Producer="Microsoft Word"*, то Система должна определять ее как текстовый объект *PDF_PRODUCER*. Для этого:

1. Создайте активный текстовый объект *PDF_PRODUCER*.
2. Перейдите в режим редактирования объекта.
3. Создайте для текстового объекта активный шаблон, указав в качестве значения строку *Producer="Microsoft Word"* :



4. Добавьте текстовый объект PDF_PRODUCER в объект защиты и создайте политику защиты данных на агентах (подробнее см. "Создание объекта защиты" и "Создание политики защиты данных на агентах").

3. Добавление системного текстового объекта в каталог

a. Перейдите в раздел **Технологии** -> **Текстовые объекты**. В левой части рабочей области щелчком левой кнопки мыши выделите требуемую категорию.
b. В левой части рабочей области щелчком левой кнопки мыши выделите каталог, в который требуется добавить текстовый объект.
c. В правой части рабочей области на панели инструментов текстовых объектов нажмите  и в раскрывающемся списке выберите **Добавить системный текстовый объект**.
d. В открывшемся окне поставьте галочку напротив текстовых объектов, которые Вы хотите добавить.

> **Примечание:**
>
> Для поиска текстовых объектов в списке введите искомый текст в строку **Поиск**.

e. Нажмите **Добавить**.

Дополнительные сведения:
Редактирование и удаление текстовых объектов, их значений и каталогов выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

Работа с эталонными документами

Цели:

1. Создать каталог эталонных документов.
2. Создать эталонный документ внутри каталога.
3. Обновить эталонный документ.

Решение:

1. Создать каталог эталонных документов

a. Перейдите в раздел **Технологии**->**Эталонные документы**.

b. В левой части рабочей области на панели инструментов нажмите  **Создать каталог эталонных документов**.
c. В открывшемся окне укажите параметры нового каталога (см. "Эталонные документы").
d. Нажмите **Создать**.

2. Создать эталонный документ

a. Перейдите в раздел **Технологии**->**Эталонные документы**.
b. В левой части рабочей области щелчком левой кнопки мыши выделите каталог, внутри которого будет создан эталонный документ.
c. В правой части рабочей области на панели инструментов эталонных документов нажмите  **Добавить**.
d. В открывшемся диалоговом окне выберите тип данных, которые могут содержаться в документе: **Текстовые** или **Все типы** (могут содержать текст, изображения и бинарные данные).
e. Нажмите **Выбрать файлы** и в открывшемся окне укажите документ, с которого требуется снять цифровой отпечаток. Нажмите **Открыть**.

   Выберите для загрузки текстовый файл, изображение или архив в соответствии с типом данных, указанным на шаге d. При этом действуют следующие правила:
   - Если формат выбранного файла не поддерживается Системой, то цифровой отпечаток будет загружен как бинарные данные.
   - Если для загрузки выбран архив, то в качестве эталонных документов будут добавлены содержащиеся в архиве файлы.
f. После окончания загрузки эталонный документ будет добавлен в каталог. Все обязательные атрибуты присваиваются созданному эталонному документу по умолчанию.

> **Примечание:**
>
> Если Системе не удалось загрузить файл эталонного документа, в окне загрузки будет выведено сообщение об ошибке.

> **Важно!**
>
> Требования к размеру файла:
>
> - Максимальный размер бинарных данных - 128 МБ;
> - Максимальный размер текстовых данных - 30 МБ;
> - Минимальный размер бинарных или текстовых данных – 128 байт;
> - Минимальный размер plain text для текстовых данных - 10 символов;
> - Минимальный размер изображения - 100 пикселей по одной стороне;
> - Минимальный размер векторных данных - 300 КБ (около 800 примитивов), только формата DWG;
> - Допустимое соотношение сторон - не больше 5:1.

g. Для изменения указанных Системой атрибутов эталонного документа на панели инструментов нажмите  **Редактировать** и измените требуемые параметры (см. "Эталонные документы").

3. Обновить эталонный документ

a. Перейдите в раздел **Технологии**->**Эталонные документы**.
b. В левой части рабочей области выберите требуемый каталог.
c. В правой части рабочей области выделите в списке эталонный документ, который требуется обновить.
d. Нажмите **Редактировать**.
e. В открывшемся окне редактирования документа нажмите **Обновить**.
f. Нажмите **Выбрать файл**.
g. В открывшемся диалоговом окне укажите документ, который будет использоваться для обновления, и нажмите **Открыть**.
h. Начнется загрузка файла. После окончания загрузки эталонный документ будет дополнен новыми данными в соответствии с выбранным режимом обновления. Если Системе не удалось выполнить обновление, в окне загрузки будет выведено сообщение об ошибке.

> **Примечание.**
>
> При обновлении эталонного документа Система заменяет данные обновляемого документа на данные из файла обновления.

Пример 1:
Требуется, чтобы Система отслеживала передачу документа "Внутренний регламент компании" при наличии в трафике хотя бы 30% текста документа. Для этого:

1. Выберите каталог эталонных документов или создайте новый каталог.
2. Внутри выбранного каталога добавьте новый документ и укажите для него тип данных: **Текстовые** (так как документ не содержит изображения и графики).
3. Загрузите документ "Внутренний регламент компании" в качестве эталонного документа.
4. Укажите название эталонного документа, например, *ВНУТРЕННИЙ_РЕГЛАМЕНТ_КОМПАНИИ.*
5. Установите для атрибута **Порог цитируемости текстовых данных** значение **30**.

> **Примечание.**
>
> Порог цитируемости настраивается в зависимости от типа защищаемого документа. В примере выстален низкий порог цитируемости, так как документ состоит из большого числа страниц и может передаваться частями.

Пример 2:
Требуется, чтобы Система отслеживала передачу исполняемого файла "`Setup.exe`" при наличии в трафике хотя бы 10% бинарного содержимого файла "`Setup.exe`". Для этого:

1. Выберите каталог эталонных документов или создайте новый каталог.
2. Внутри выбранного каталога добавьте новый документ и укажите для него тип данных : **Все типы**.
3. Загрузите файл "`Setup.exe`" в качестве эталонного документа.
4. Укажите название эталонного документа, например, *SETUP_EXE.*
5. Установите для атрибута **Порог цитируемости бинарных данных** значение **10**.

Для того чтобы Система отслеживала наличие в трафике указанных эталонных документов, их нужно включить в объекты защиты.

Дополнительные сведения:
Редактирование и удаление эталонных документов и их каталогов выполняется стандартным способом:

- Редактирование элемента;
- Удаление элемента.

Работа с бланками

Цель:

1. Создать каталог бланков.
2. Создать бланк.
3. Создать условие обнаружения.
4. Обновить бланк.

Решение:

1. Создать каталог бланков

a. Перейдите в раздел **Технологии**->**Бланки**.
b. В левой части рабочей области на панели инструментов нажмите  **Создать каталог бланков**.
c. В открывшемся окне введите название и описание каталога.
d. Нажмите **Создать**.

2. Создать бланк

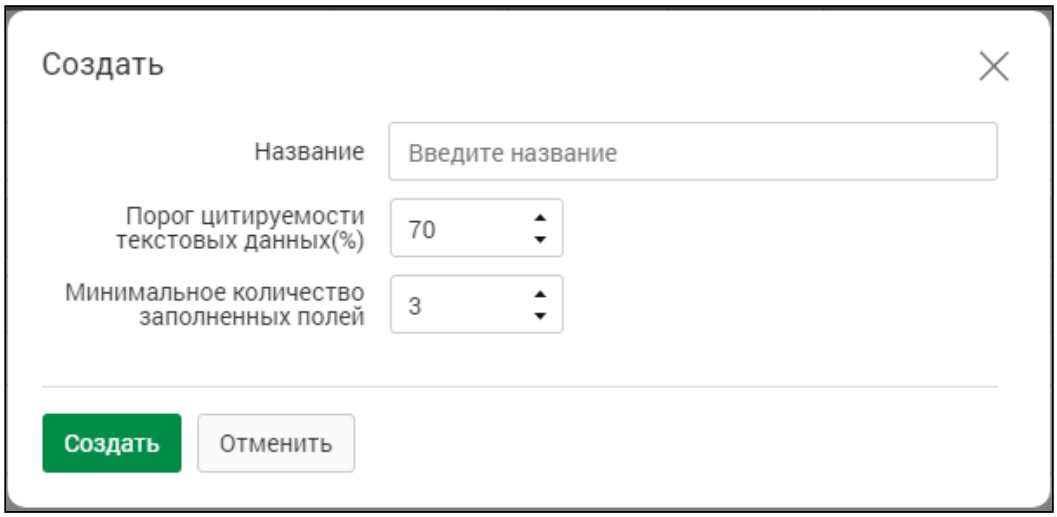
a. Перейдите в раздел **Технологии**->**Бланки**.
b. В левой части рабочей области щелчком левой кнопки мыши выделите каталог, внутри которого будет создана бланк.
c. В правой части рабочей области на панели инструментов форм нажмите  **Добавить**.
d. В открывшемся диалоговом окне укажите документ, который будет служить примером бланка, и нажмите **Открыть**. Вы можете загрузить документ в одном из следующих форматов: DOC, DOCX, DOT, DOTM, DOTX, XLS, XLSX, XLT, XLTM, XLTX, ODS, ODT, RTF, TXT, VSD, HTML, HTM, PDF, CHM.
e. После окончания загрузки бланк будет добавлен в каталог. Все обязательные атрибуты присваиваются созданному бланку по умолчанию.

> **Примечание:**
>
> Если Системе не удалось загрузить файл бланка, в окне загрузки будет выведено сообщение об ошибке.

f. Для изменения атрибутов бланка, заданных в Системе по умолчанию, на панели инструментов нажмите  **Редактировать** и измените требуемые атрибуты (см. "Бланки").

3. Создать условие обнаружения

a. Перейдите в раздел **Технологии**->**Бланки**.
b. В левой части рабочей области выберите требуемый каталог.
c. В правой части рабочей области выделите в списке бланк, к который требуется добавить условие обнаружения.
d. Нажмите **Редактировать**.
e. В левой части рабочей области нажмите **Создать**.
f. В открывшемся диалоговом окне введите название укажите параметры условия обнаружения:
   - Порог цитируемости текстовых данных.
   - Минимальное количество заполненных полей.



g. После ввода данных нажмите **Создать**.
h. Вы можете добавить несколько условий обнаружения бланка, для этого повторите действия e-g.

> **Примечание:**
>
> Рекомендуется создавать **не более 20** условий обнаружения для одного бланка.

i. Нажмите **Сохранить**.

4. Обновить бланк

a. Перейдите в раздел **Технологии**->**Бланки**.
b. В левой части рабочей области выберите требуемый каталог.
c. В правой части рабочей области выделите в списке бланк, который требуется обновить.
d. Нажмите **Редактировать**.
e. В открывшемся окне редактирования бланка нажмите **Обновить**.
f. Нажмите **Выбрать файл**.
g. В открывшемся диалоговом окне укажите файл, который будет использоваться для обновления, и нажмите **Открыть**. Начнется загрузка.
h. Данные бланка будут заменены данными из файла обновления.
Если Системе не удалось выполнить обновление, в окне загрузки будет выведено сообщение об ошибке.

Пример:

Требуется, чтобы при наличии в трафике фрагментов даже незаполненной анкеты "Анкета соискателя" Система помечала объект перехвата как *АНКЕТА_СОИСКАТЕЛЯ*. Для этого:

1. Создайте бланк *АНКЕТА_СОИСКАТЕЛЯ.*
2. Загрузите файл документа "Анкета соискателя" в качестве бланка.
3. Создайте для бланка условие обнаружения с **Минимальным количеством заполненных полей = 0**. Также допускается отредактировать условие по умолчанию, которое создается вместе с бланком.
4. Создайте новый объект защиты на основе бланка *АНКЕТА_СОИСКАТЕЛЯ* и выберите требуемое условие обнаружения.

Дополнительные сведения:
Редактирование и удаление условий обнаружения, бланков и их каталогов выполняется стандартным способом:

- Редактирование элемента;
- Удаление элемента.

Работа с печатями

Цели:

1. Создать каталог печатей.
2. Создать печать.

Решение:

1. Создать каталог печатей

a. Перейдите в раздел **Технологии**->**Печати**.
b. В левой части рабочей области на панели инструментов нажмите + **Создать каталог печатей**.
c. В открывшемся окне укажите параметры нового каталога.
d. Нажмите **Создать**.

2. Создать печать

a. Перейдите в раздел **Технологии** ->**Печати**.
b. В левой части рабочей области рабочей области щелчком левой кнопки мыши выделите каталог, внутри которого будет создана печать.
c. В правой части рабочей области на панели инструментов печатей нажмите + **Добавить**.

> **Важно!**
>
> Загружаемый файл должен содержать только одно изображение печати.

d. В открывшемся диалоговом окне укажите документ, который будет служить примером печати, и нажмите **Открыть**.
e. После окончания загрузки печать будет добавлена в каталог. Все обязательные атрибуты присваиваются созданной печати по умолчанию.

> **Примечание:**
>
> Если Системе не удалось загрузить файл печати, в окне загрузки будет выведено сообщение об ошибке.

f. Для изменения указанных Системой атрибутов печати на панели инструментов нажмите  **Редактировать** и измените требуемые атрибуты.

> **Примечание:**
>
> О том, как правильно выбрать печать для загрузки в Систему, читайте на странице "Печати".

Пример:
Требуется обеспечить защиту юридических документов, заверенных печатью организации. Для этого:

1. Подготовьте файл с изображением печати вашей организации.
2. В разделе **Технологии**->**Печати** перейдите в требуемый каталог печатей либо создайте новый каталог.
3. Внутри выбранного каталога создайте новую печать и загрузите подготовленный файл с изображением печати вашей организации.

Для того чтобы добавленная печать детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

Дополнительные сведения:
Редактирование и удаление печатей и их каталогов выполняется стандартным способом:

- Редактирование элемента;
- Удаление элемента.

Работа с выгрузками

Цель:

1. Создать каталог выгрузок.
2. Создать выгрузку из БД.
3. Обновить выгрузку.
4. Переместить/копировать выгрузку.

Решение:

1. Создать каталог выгрузок

a. Перейдите в раздел **Технологии**->**Выгрузки из БД**.
b. В левой части рабочей области на панели инструментов нажмите  **Создать каталог выгрузок из БД**.
c. В открывшемся окне введите название и описание каталога.
d. Нажмите **Создать**.

2. Создать выгрузку

a. Перейдите в раздел **Технологии**->**Выгрузки из БД**.

b. В левой части рабочей области выделите группу, в которую требуется добавить выгрузку.
c. В правой части рабочей области на панели инструментов нажмите  **Добавить**.
d. В открывшемся диалоговом окне укажите требуемый файл для загрузки в формате CSV или TSV и нажмите **Открыть**.

> **Примечание.**
>
> При добавлении файла выгрузки выполняется его компиляция. Объем оперативной памяти, потребляемой при компиляции, можно приблизительно определить по следующей формуле:
>
> `Память(GB) = 0.05 * уникальных_слов (M) * ячеек (M)`, где M - миллион.
>
> Например, 10 миллионов ячеек могут поместиться в таблицу с 2 столбцами и 5 миллионами строк, либо в таблицу с 4 столбцами и 2,5 миллионами строк.

> **Важно!**
>
> Размер выгрузки не должен превышать 300 МБ.

e. После успешной загрузки файла выделите в списке добавленную выгрузку и нажмите .
f. Укажите требуемые атрибуты (см. "Выгрузки из БД" и "Условия обнаружения выгрузки").
g. Нажмите **Сохранить**.

3. Обновить выгрузку

1. Перейдите в раздел **Технологии**->**Выгрузки из БД**.
2. В левой части рабочей области выберите требуемый каталог.
3. В правой части рабочей области выделите в списке выгрузку, которую требуется обновить.
4. Нажмите  **Редактировать**.
5. В открывшемся окне редактирования выгрузки нажмите **Обновить**.
6. Укажите требуемый режим обновления: **Добавление новых записей** или **Удаление старых записей и добавление новых**.
7. Нажмите **Выбрать файл**.
8. В открывшемся диалоговом окне укажите файл, который будет использоваться для обновления, и нажмите **Открыть**. Начнется загрузка.
9. После окончания загрузки выгрузка из БД будет дополнена новыми данными в соответствии с выбранным режимом обновления. Если Системе не удалось выполнить обновление, в окне загрузки будет выведено сообщение об ошибке.

4. Переместить/копировать выгрузку

1. Перейдите в раздел **Технологии**->**Выгрузки из БД**.
2. В левой части рабочей области выберите каталог, в котором находится выгрузка.

3. Нажмите левой кнопкой мыши на  рядом с названием выгрузки, которую требуется переместить/копировать. Не отпуская кнопку, перетащите выгрузку на место того каталога, в который необходимо переместить/копировать выгрузку, после чего отпустите левую кнопку мыши.
4. В открывшемся окне нажмите **Переместить** или **Копировать**.
5. Выгрузка будет перемещена/скопирована в указанный каталог.

> **Примечание:**
>
> Если отредактировать или обновить оригинал выгрузки, то также будут изменены все копии этой выгрузки. Если отредактировать или обновить копию выгрузки, то также будет изменен оригинал и все копии этой выгрузки.

Дополнительные сведения:
Редактирование и удаление выгрузок из БД и их каталогов выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

Условия обнаружения выгрузки

Справочная информация:

Выполнение условий обнаружения позволяет соотнести объект перехвата с определенной выгрузкой.

При создании выгрузки создается условие обнаружения по умолчанию со следующими значениями параметров:

Параметр	Значение
Название условия	Условие по умолчанию
Условие обнаружения	1+2+...+n, где n – количество столбцов выгрузки
Минимальное количество строк	10 **Примечание**: Если в выгрузке содержится меньше 10 строк, то значение параметра будет равно количеству строк в выгрузке.
Тип поиска	Все слова из ячейки без учета порядка следования и расстояния между ними

Вы можете указать несколько (не более 20) условий обнаружения для выгрузки. В этом случае для отнесения объекта перехвата к данной выгрузке достаточно выполнения хотя бы одного из условий.

Цель:

Добавить условие обнаружения выгрузки.

Решение:

1. Перейдите в раздел **Технологии**->**Выгрузки из БД**.
2. В левой части рабочей области выберите требуемый каталог.
3. В правой части рабочей области выделите в списке требуемую выгрузку и нажмите  **Редактировать**.
   Откроется форма редактирования выгрузки.
4. На панели инструментов, расположенной под заголовком **Условие обнаружения**, нажмите  **Добавить**.
5. В открывшемся диалоговом окне укажите следующие параметры (подробное описание параметров смотрите ниже):
   a. **Название условия**;
   b. **Минимальное количество строк**;
   c. **Тип поиска**;
   d. **Условие обнаружения**.
6. Нажмите **Создать**.

Параметры условия обнаружения заполняются в соответствии со следующими рекомендациями:

Условие обнаружения:
Условие обнаружения содержит номера столбцов и логические отношения между ними. Если при анализе в объекте перехвата обнаружены данные из указанных ячеек с учетом заданных отношений, то данная строка считается сработавшей.

> **Важно!**
>
> Для исключения ложноположительных срабатываний в Системе используются стоп-слова: цифры, буквы и слова, нахождение которых в ячейках не приводит к срабатыванию этих ячеек. Полный список стоп-слов см. в статье Базы знаний InfoWatch "Список стоп-слов для выгрузок из баз данных".

Логические отношения задаются с помощью символов:

- "+" - конъюнкция ячеек (логическое "И");
- "|" - дизъюнкция ячеек (логическое "ИЛИ");

  > **Примечание.**
  >
  > Условие вида (1|3) должно указываться в скобках.

- "()" - группировка условий. Например, условие вида 1+(2|3) означает, что строка считается сработавшей, если в ней сработала первая ячейка, а также вторая или третья ячейка.
  Условие вида (1|3)+(5|4) означает, что строка считается сработавшей, если сработала первая или третья ячейка и пятая или четвертая ячейка.

  > **Важно!**

Символ "|" не может использоваться для разделения групп в скобках. То есть условие (1+8+11*)|(2+3*) должно быть представлено в виде двух отдельных условий: 1+8+11* и 2+3*.

- "*" - символ астериска позволяет учитывать также незаполненные ячейки. Например, условие вида 1+2* означает, что строка считается сработавшей, если в ней сработали первая и вторая ячейки, при этом вторая ячейка может быть незаполненной.

Важно!

Технология анализа не учитывает спецсимволы, поэтому, если столбец содержит адрес электронный почты, для уменьшения ложных срабатываний рекомендуется указать дополнительный столбец (например, ФИО).

Минимальное количество строк:
Минимальное количество строк, которое требуется обнаружить для срабатывания условия.

Например, если указано условие вида: 1+(2|3) и задано минимальное количество строк = 10, то для срабатывания условия необходимо, чтобы в анализируемом тексте содержалось не менее 10 различных строк, удовлетворяющих условию 1+(2|3).

Тип поиска:
Параметр определяет тип поиска цитат в анализируемом тексте. Доступные типы поиска:

- Все слова из ячейки без учета порядка следования и расстояния между ними
- Все слова из ячейки без учета порядка, но следующие друг за другом

Важно!

Если вы используете тип поиска **Все слова из ячейки без учета порядка, но следующие друг за другом**:

- Анализ текста будет прекращен, если выполнено условие для обнаружения выгрузки. В тексте события будут выделены только те фрагменты, которые были обнаружены до выполнения условия.
- Если в выгрузке есть ячейки с одинаковыми значениями, то эти ячейки могут сработать на один и тот же фрагмент текста.
- Скорость анализа текста может снизиться.

Пример:
Требуется, чтобы Система помечала объект перехвата как НОМЕРА_ТЕЛЕФОНОВ при обнаружении в нем не менее 5 строк с заполненными столбцами 1 и 3 из таблицы со следующей структурой:

ФИО	Город	Номер телефона
Иванов Иван Иванович	Москва	+0 (012) 345-67-89
Петров Петр Петрович	Владимир	+0 (012) 345-67-88
Сидоров Сидор Сидорович	Москва	+0 (012) 345-67-87

ФИО	Город	Номер телефона
Смирнов Юрий Борисович	Волгоград	+0 (012) 345-67-86
Кузнецов Владимир Андреевич	Самара	+0 (012) 345-67-85
Соколов Михаил Григорьевич	Москва	+0 (012) 345-67-84

При этом необходимо, чтобы слова из ячейки следовали в тексте строго друг за другом:

- текст вида "**Иванов** Петр Петрович, Петров **Иван Иванович**" не должен быть отмечен как содержащий слова из ячейки "**Иванов Иван Иванович**";
- текст вида "**+0 (012) 345**-00-00, +0 (000) 000-**67-89**" не должен быть отмечен как содержащий слова из ячейки "**+0 (012) 345-67-89**".

> **Примечение:**
>
> Словом считается любая последовательность букв или цифр.

Для этого:

1. Сохраните таблицу в формате CSV или TSV и загрузите созданный файл в Систему.
2. Настройте условие обнаружения:
   - в поле **Условие обнаружения** укажите **1+3**;
   - в поле **Минимальное количество строк** укажите **5**;
   - в поле **Тип поиска** выберите **Все слова из ячейки без учета порядка, но следующие друг за другом**.
3. Создайте объект защиты "НОМЕРА_ТЕЛЕФОНОВ" на основе созданной выгрузки из БД.

При передаче трафика, в котором обнаруживаются указанные колонки данных, в Системе срабатывает объект защиты *НОМЕРА_ТЕЛЕФОНОВ*.

Дополнительные сведения:
Редактирование и удаление условий обнаружения выгрузки выполняются стандартным способом:

- Редактирование элемента
- Удаление элемента

Работа с графическими объектами

Чтобы настроить автоматический классификатор графических объектов:

1. Создайте категорию графических объектов:
   a. Перейдите в раздел **Технологии**->**Графические объекты**.
   b. В левой части рабочей области на панели инструментов нажмите .
   c. В открывшемся окне укажите название и описание новой категории.
   d. Нажмите **Сохранить**.
2. Загрузите изображения:
   a. В левой части рабочей области щелчком левой кнопки мыши выделите категорию, в которую будет добавлено изображение.

b. В правой части рабочей области на панели инструментов нажмите .
c. В открывшемся окне выберите один или несколько файлов на диске и нажмите **Открыть**. Используйте файлы, из которых могут быть извлечены графические данные.
d. Убедитесь, что выбранный файл успешно добавлен в категорию. Статус процесса отображается на всплывающем окне справа.

3. Обучите классификатор:
a. Создайте хотя бы две категории, содержащие по одному или несколько изображений.
b. Нажмите  и дождитесь его окончания. Процесс может занять несколько минут. После завершения обучения некоторые категории могут содержать ошибки. В этом случае рекомендуется удалить все изображения в такой категории, добавить новые и заново провести обучение.
c. В верхней части рабочей области нажмите **Применить**.
d. В окне **Применение конфигурации** ознакомьтесь с новой конфигурацией и нажмите **Применить**. Новая конфигурация станет активной на сервере.

Примечание:

Для корректной работы технологии учитывайте рекомендации:

- Необходим большой размер коллекции изображений, разложенных по категориям, в каждой из которых должно быть не менее 50 изображений.
- Состав категории должен быть однороден: не помещайте в одну категорию изображения, относящиеся к разным категориям.
- Размеры разных категорий должны быть близкими по объему.
- Время обучения и производительность Системы зависит от количества загружаемых изображений.
- Минимальный допустимый размер изображения: 150 пикселей по одной стороне.
- Максимальное разрешение изображения: 10000x10000 пикселей.
- Максимальное соотношение сторон изображения: 8:1.
- Допустимые градусы поворота изображения только на: 90+-10, 180+-10, 270+-10 градусов.
- Форматы изображений для обучения: `bmp, gif, jpeg, jp2, pbm, pgm, png, ppm, ras, tiff`. При этом:
  - Если файл является незашифрованным архивом, то на основе каждого извлеченного файла будет создан отдельный документ. Все созданные документы будут помещены в категорию, выбранную при создании документа.
  - Если файл является зашифрованным архивом, документ не создается или создается с ошибкой.

Чтобы повысить точность детектирования документов из одной категории, обучите классификатор на ней и на других категориях. Изображения, вызвавшие ложно-положительные срабатывания и не относящиеся ни к одной из категорий, переместите в категорию *Снижение ЛПС.* Эта категория служит противовесом для всех созданных категорий, что также повышает качество работы технологии.

Чтобы проверить отдельные файлы на классификаторе, уже прошедшем обучение:

1. В левой части рабочей области нажмите  **Проверить**.
2. В окне нажмите **Начать новую проверку**.
3. Выберите на диске один или несколько файлов и нажмите **Открыть**. Не загружайте на проверку архивы.
4. Дождитесь окончания проверки и ознакомьтесь с результатами. Классификатор определит категории графических объектов, к которым относятся загруженные изображения. Вы можете добавить такие изображения в указанные категории и заново провести обучение классификатора.

> **Важно!**
>
> Проверка изображений на принадлежность тому или иному графическому объекту осуществляется только по доступным для редактирования графическим объектам. Подробнее о нередактируемых графических объектах см. "Графические объекты").

Если вас не устроили результаты обработки документов (например: для некоторых файлов не удалось определить категорию, не все нужные изображения детектируются классификатором или детектируются ошибочно), загрузите дополнительные файлы в категорию или удалите из категории ранее загруженные файлы, а затем заново обучите классификатор.

Работа с Автолингвистом

Чтобы классификатор корректно определял принадлежность документа тематическим категориям, его нужно настроить и обучить.

Чтобы настроить Автолингвист:

1. Создайте категорию Автолингвиста:
   a. Перейдите в раздел **Технологии** -> **Автолингвист**.
   b. В левой части рабочей области на панели инструментов нажмите .
   c. В открывшемся окне укажите название и описание новой категории.
   d. Нажмите **Создать**.
2. Загрузите типовые документы в категории:
   a. Перейдите в раздел **Технологии** -> **Автолингвист**.
   b. В левой части рабочей области щелчком левой кнопки мыши выделите категорию, в которую будет будет добавлен документ.

> **Примечание:**
>
> Можно загрузить файл любого формата из числа детектируемых форматов и извлекаемых данных в Системе. При этом есть ряд ограничений:
>
> - Если файл является незашифрованным архивом, то на основе каждого извлеченного файла создается отдельный документ. При этом документ на основе всего архива не создается. Все созданные документы помещаются в категорию, выбранную при создании документа.
>
> - Если файл является зашифрованным архивом, документ не создается или создается с ошибкой.

- Если файл является файлом типа *Контейнер*, создается один документ на основе этого файла.

c. В правой части рабочей области на панели инструментов нажмите .
d. В окне выберите один или несколько файлов и нажмите **Открыть**. Используйте документы, из которых могут быть извлечены текстовые данные.
e. Убедитесь, что выбранный файл успешно добавлен в категорию. Статус процесса отображается на всплывающем окне справа.

3. Обучите классификатор на новой коллекции:
   a. Создайте хотя бы две категории, содержащие один или несколько типовых документов.
   b. Нажмите  и дождитесь его окончания. Процесс может занять несколько минут. После завершения обучения некоторые категории могут содержать ошибки. В этом случае рекомендуется удалить все документы в такой категории, добавить новые и заново провести обучение. По итогам обучения выводятся показатели качества категорий и всей коллекции в процентах.
   c. В верхней части рабочей области нажмите **Применить**.
   d. В окне **Применение конфигурации** нажмите **Применить**. Новая конфигурация станет активной на сервере.

Примечание:

Количество документов и их содержимое влияют на качество обучения технологии. Чем больше документов схожей тематики в категории, тем точнее будет работа Автолингвиста.

Для корректной работы технологии учитывайте рекомендации:

- Для обучения классификатора необходимо как минимум две категории и как минимум по одному документу в каждой из них.
- Минимальный размер текста в документе - 5 слов, содержащих не менее трех символов.
- Время обучения и производительность Системы зависит от количества загружаемых документов и может занимать несколько минут.

Вы можете проверить работу обученного Автолингвиста. Для этого загрузите документ, чтобы классификатор отнес его к одной из категорий коллекции.

Чтобы проверить отдельные файлы в классификаторе, уже прошедшем обучение:

1. Нажмите **Проверить.**
2. В окне нажмите **Начать новую проверку**.
3. Выберите на диске один или несколько файлов и нажмите **Открыть**. Размер загружаемого на проверку файла может быть от 256 байт до 26 Мбайт.
4. Дождитесь окончания проверки и ознакомьтесь с результатами.
5. Примените новую конфигурацию. Классификатор определит категории текстовых объектов, к которым относятся загруженные документы. Вы можете добавить такие документы в указанные категории и заново провести обучение классификатора.

Если вас не устроили результаты обработки документов (например: для некоторых файлов не удалось определить категорию, не все нужные документы детектируются классификатором или детектируются

ошибочно), загрузите дополнительные файлы в категорию или удалите из категории ранее загруженные файлы, а затем заново обучите классификатор.

4.4.2 Экспорт и импорт базы технологий

Цель:

- сохранить архив, содержащий базу технологий, на жесткий диск компьютера;
- загрузить базу технологий, хранящуюся на компьютере в виде архива с расширением `.cfb`, для использования в Консоли управления InfoWatch Traffic Monitor.

> **Примечание:**
>
> Экспорт базы технологий не может быть выполнен, если конфигурация Системы находится на редактировании. Импорт базы технологий не может быть выполнен, если конфигурация Системы не применена. В противном случае будет выведено сообщение об ошибке.

Чтобы экспортировать базу технологий:

1. Перейдите в какой-либо подраздел раздела **Технологии** (**Категории и термины**, **Текстовые объекты**, **Эталонные документы**, **Бланки**, **Печати**, **Выгрузки из БД** или **Графические объекты**).
2. На панели инструментов в левой части рабочей области нажмите ▾ и в раскрывающемся списке выберите **Экспортировать**.
3. Начнется подготовка к экспорту базы технологий. После ее завершения на ваш компьютер будет загружен архив с расширением `.cfb`. Данный файл содержит следующие элементы:
   - категории и термины;
   - текстовые объекты, в том числе предустановленные;
   - эталонные документы;
   - бланки;
   - печати;
   - выгрузки из БД;
   - графические объекты.
4. Структура каталогов при экспорте сохраняется.

> **Важно!**
>
> В результате будет экспортирована вся база технологий, а не только выбранный подраздел.
>
> Экспортируется база технологий из последней примененной конфигурации (см. "Работа с конфигурацией Системы").

Чтобы импортировать базу технологий, хранящуюся на компьютере в виде архива с расширением `.cfb`:

1. Перейдите в какой-либо подраздел раздела **Технологии** (**Категории и термины**, **Текстовые объекты**, **Эталонные документы**, **Бланки**, **Печати**, **Выгрузки из БД** или **Графические объекты**).
2. На панели инструментов в левой части рабочей области нажмите ▾ и в раскрывающемся списке выберите **Импортировать**.
3. В открывшемся диалоговом окне **Открыть** укажите архив с расширением `.cfb`, который вы хотите загрузить.
4. Нажмите **Открыть** и дождитесь окончания загрузки данных в Систему.

> **Примечание:**
>
> Если название каталога в файле импорта совпадает с названием каталога в Системе, но различаются пути к каталогу, то каталог из файла импорта добавлен не будет.
> Если название каталога в файле импорта совпадает с названием каталога в Системе, и путь к каталогу также совпадает, то данные из файла импорта будут объединены с данными, содержащимися в Системе.

Особенности слияния данных при импорте:

1. Для каталогов будут добавлены следующие элементы, отсутствующие в Системе:
   а) дочерние каталоги;
   б) элементы технологий.
2. Для категории будут добавлены термины, отсутствующие в Системе.
3. Для текстового объекта будут добавлены шаблоны, отсутствующие в Системе.

   > **Примечание:**
   >
   > Имеющиеся в Системе верифицирующие функции будут заменены функциями из файла.

4. Для добавления в Систему отраслевых и кастомизированных БКФ необходимо использовать XML-файлы, совместимые с Системой InfoWatch Traffic Monitor. После импорта такого XML-файла соответствующие категории и термины будут автоматически добавлены в консоль управления Системы в раздел **Технологии** (**Категории и термины**, **Текстовые объекты**, **Эталонные документы**, **Бланки**, **Печати**, **Выгрузки из БД** или **Графические объекты**).

   > **Примечание:**
   >
   > В настоящее время отраслевые и кастомизированные БКФ для Системы InfoWatch Traffic Monitor уникальны и не могут быть импортированы в другие системы класса DLP.

5. Для выгрузки из БД будут добавлены представления выгрузки, если содержимое выгрузки в файле и в Системе не отличается.

Важно!

Выгрузки из БД, которые были созданы в Traffic Monitor версии ниже 7.4, считаются устаревшими. Устаревшие выгрузки отмечены в интерфейсе символом .

Для устаревшей выгрузки недоступно редактирование и обновление. Рекомендуется удалить устаревшую выгрузку и создать ее повторно.

4.5 Работа с объектами защиты

Важно!

Чтобы изменения, описанные в данном разделе, отразились на работе Системы, примените конфигурацию: см. "Работа с конфигурацией Системы" и "Применение конфигурации Системы".

Для чего требуются объекты защиты:

Использование объектов защиты позволяет анализировать перехваченные данные на предмет наличия в них сразу нескольких элементов анализа: например, эталонного документа, текстового объекта и выгрузки из базы данных. Также вы можете указать элементы, при обнаружении которых Система не будет детектировать объект защиты. Таким образом вы можете настроить Систему на обнаружение или игнорирование определенных бизнес-документов: например, паспорта транспортного средства или заявления о страховой выплате.

Работа с объектами защиты состоит из следующих действий:

Действие	Описание
Создание каталога объектов защиты	Создание каталога, в который будут добавлены объекты защиты
Создание объекта защиты	Создание объекта защиты и указание его параметров
Добавление элементов технологий	Добавление в объект защиты элементов анализа
Добавление условий обнаружения	Указание условий обнаружения для добавленных элементов анализа
Создание политики для объектов защиты и их каталогов	Создание политики защиты данных для выбранных объектов защиты и их каталогов
Импорт и экспорт объектов защиты	Импорт и экспорт структуры каталогов, содержащихся в них объектов и используемых элементов анализа

Действие	Описание
Активация и деактивация объектов защиты	Изменение статуса объектов защиты и их каталогов

См. также:

- "Раздел Объекты защиты" - о разделе, в котором ведется работа с объектами защиты

4.5.1 Создание каталога объектов защиты

Цель:
Создать каталог, в котором будут содержаться объекты защиты.

Решение:

1. Перейдите в раздел **Объекты защиты**.
2. На панели инструментов в левой части рабочей области нажмите  **Создать каталог объектов защиты**.

   > **Примечание:**
   >
   > Вы можете создать новый каталог объектов защиты внутри имеющегося каталога. Для этого выберите целевой каталог в списке.

3. В открывшемся диалоговом окне укажите атрибуты каталога.
4. Нажмите **Создать**.

Вы можете переместить выбранный каталог, используя перетаскивание. Для этого выделите каталог в списке и, удерживая левую клавишу мыши зажатой, переместите его в требуемое место в структуре каталогов, после чего отпустите зажатую клавишу мыши.

> **Примечание:**
>
> Перемещение каталога выполняется со всеми вложенными элементами: подкаталогами и объектами защиты. При перемещении каталога его статус меняется на статус каталога, в который выполняется перемещение.

Дополнительные сведения:

Редактирование и удаление каталога объектов защиты выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

4.5.2 Создание объекта защиты

Цель:
Создать объект защиты на основе имеющихся в Системе элементов технологий.

Решение:

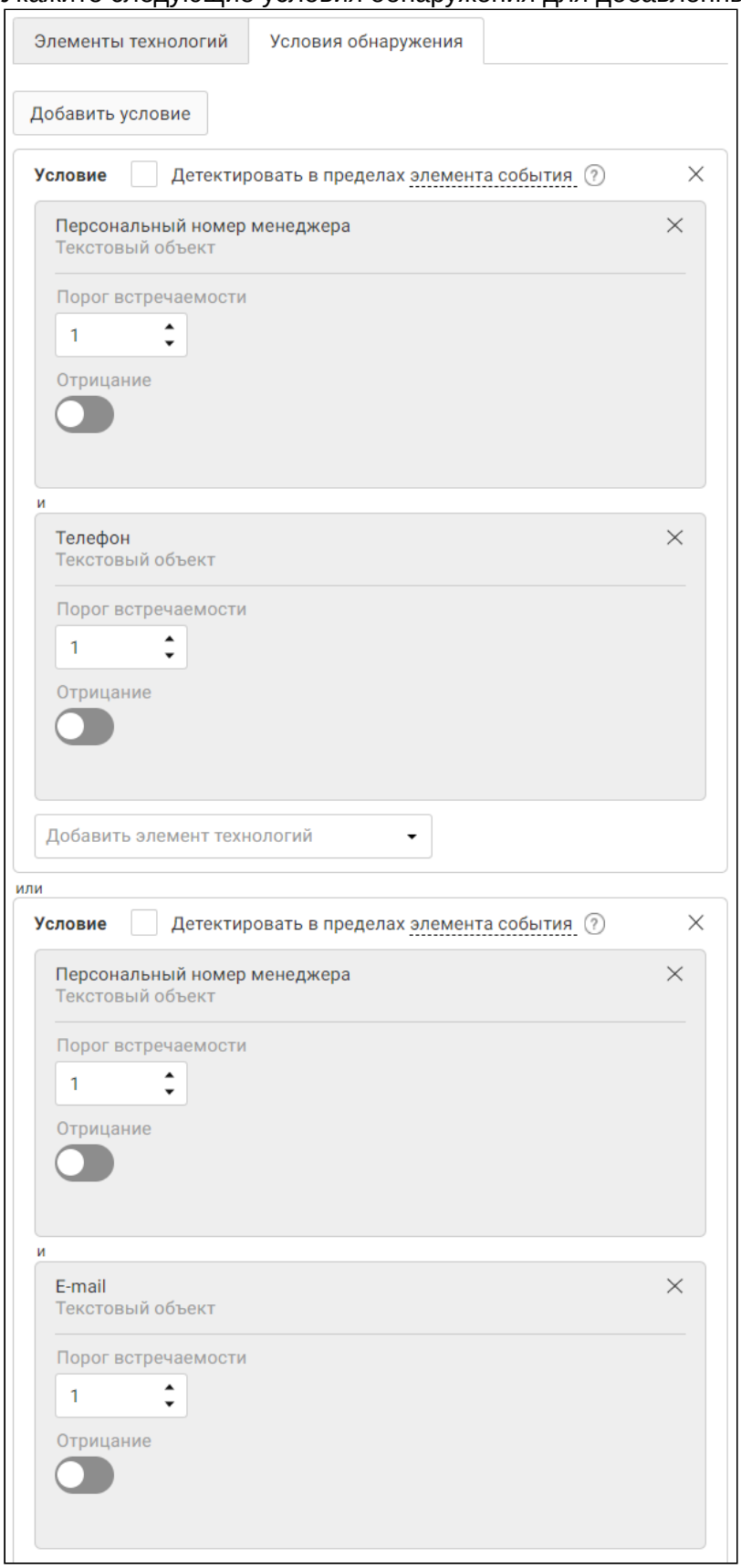
1. Перейдите в раздел **Объекты защиты**.
2. В левой части рабочей области выберите каталог, в который требуется добавить новый объект защиты, либо создайте новый каталог (см. "Создание каталогов объектов защиты").
3. На панели инструментов в правой части рабочей области нажмите  **Создать объект защиты**.
4. В открывшемся окне укажите элементы, на основе которых будет создан объект защиты (см. "Добавление элементов технологий").
5. Определите, должны ли выбранные элементы технологий входить в один объект защиты, либо для каждого элемента будет создан отдельный объект:
   - Если выбрана настройка **Создать объект защиты на каждый выбранный элемент**, будет создан набор объектов защиты для каждого выбранного элемента технологий. Атрибуты созданных объектов защиты формируются автоматически. Названия объектов формируются на основе названия технологии и названия элемента, например: "*Текстовый объект: Номер кредитной карты*".
   - Если настройка **Создать объект защиты на каждый выбранный элемент** не выбрана, то после нажатия **Создать** будет открыто дополнительное окно настроек параметров объекта защиты: см. шаг 7.
6. Нажмите **Создать**.
7. Если на шаге 5 настройка **Создать объект защиты на каждый выбранный элемент** не была выбрана, откроется окно **Создание объекта защиты**. В этом окне:
   a. Введите название объекта защиты.
   b. На вкладке **Элементы технологий**, содержащей выбранные элементы (см. "Элементы технологий"), вы можете добавить дополнительные элементы (для этого нажмите **Выбрать элементы**), а также удалить элементы из списка (нажмите на крестик в строке выбранного элемента).
   c. На вкладке **Условия обнаружения** укажите условия, при выполнении которых объекты защиты будут детектироваться в перехваченных данных (подробнее см. "Добавление условий обнаружения").
   d. При необходимости введите описание объекта защиты в поле **Описание**.
   e. Нажмите **Создать**.

В результате в выбранном каталоге будет создан объект защиты (или несколько, если выбрана настройка **Создать объект защиты на каждый выбранный элемент**).
Вы можете переместить созданный объект защиты в какой-либо другой каталог. Для этого выделите требуемый объект защиты и, удерживая левую клавишу мыши зажатой, переместите его в другой каталог, после чего отпустите зажатую клавишу мыши.

Пример 1:
Требуется создать объект защиты *"Персональные данные менеджера"*, который должен детектироваться в Системе при выполнении одного из следующих условий:
- объект перехвата содержит персональный номер менеджера и E-mail;
- объект перехвата содержит персональный номер менеджера и номер телефона.

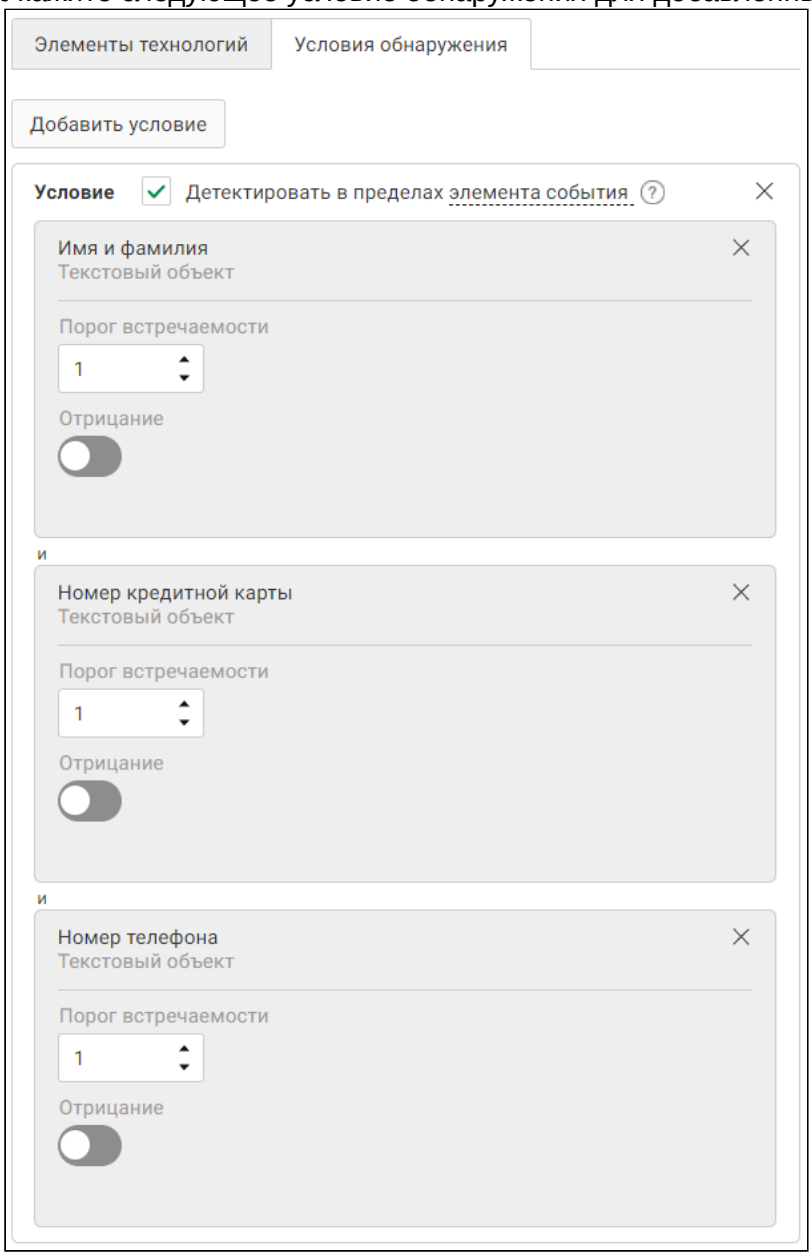
Для этого:
1. Создайте объект защиты и добавьте в него элементы технологий:
   - текстовый объект *"Персональный номер менеджера"*;
   - текстовый объект *"E-mail"*;
   - текстовый объект *"Телефон"*.

2. Укажите следующие условия обнаружения для добавленных элементов технологий:



Пример 2:
Требуется создать объект защиты, который должен детектироваться в Системе при выполнении следующего условия: объект перехвата в пределах одного элемента события содержит имя и фамилию, номер телефона и номер кредитной карты.
Для этого:

1. Создайте объект защиты и добавьте в него элементы технологий:
   - текстовый объект *"Имя и фамилия"*;
   - текстовый объект *"Номер телефона"*;
   - текстовый объект *"Номер кредитной карты"*.
2. Укажите следующее условие обнаружения для добавленных элементов технологий:



Обратите внимание, что для выполнения условия обязательно активировать функцию **Детектировать в пределах элемента события**. В этом случае объект защиты будет детектироваться Системой, если все защищаемые данные обнаружены в одном элементе, например в теле письма или в прилагаемом файле.

Пример 3:

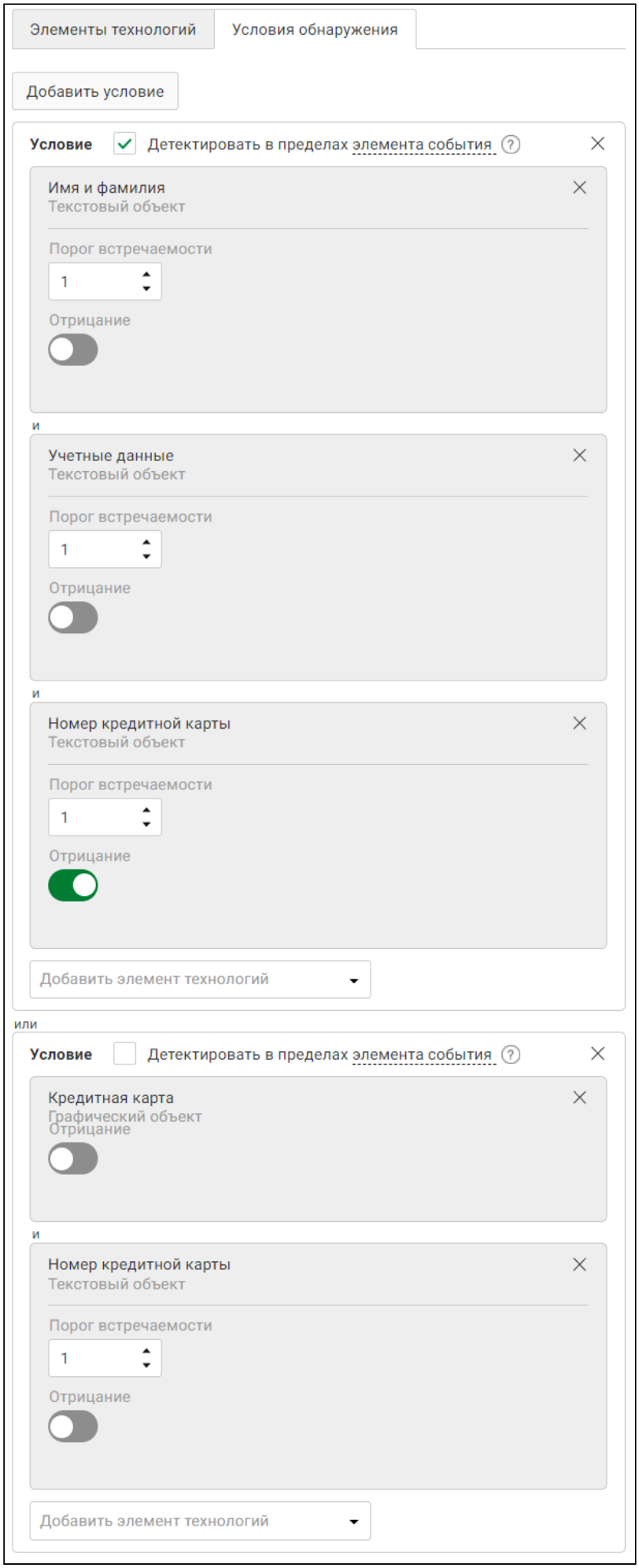
Требуется создать объект защиты, который должен детектироваться в Системе при выполнении одного из следующих условий:

- объект перехвата в пределах одного элемента события содержит имя и фамилию и учетные данные, но обязательно не содержит номер кредитной карты;
- объект перехвата содержит номер кредитной карты и ее изображение.

Для этого:

1. Создайте объект защиты и добавьте в него элементы технологий:
    - текстовый объект *"Имя и фамилия"*;
    - текстовый объект *"Учетные данные"*;
    - текстовый объект *"Номер кредитной карты"*;
    - графический объект "*Кредитная карта*".

2. Укажите следующие условия обнаружения для добавленных элементов технологий:


Элементы технологий
Условия обнаружения
Добавить условие
Условие
Детектировать в пределах элемента события
Имя и фамилия
Текстовый объект
Порог встречаемости
1
Отрицание
и
Учетные данные
Текстовый объект
Порог встречаемости
1
Отрицание
и
Номер кредитной карты
Текстовый объект
Порог встречаемости
1
Отрицание
Добавить элемент технологий
или
Условие
Детектировать в пределах элемента события
Кредитная карта
Графический объект
Отрицание
и
Номер кредитной карты
Текстовый объект
Порог встречаемости
1
Отрицание
Добавить элемент технологий

Обратите внимание, что для выполнения первого условия обязательно активировать функцию **Детектировать в пределах элемента события** и для элемента технологий, наличие которого отменяет детектирование, включить **Отрицание**.
В этом случае объект защиты будет детектироваться Системой по первому условию, только если в одном элементе события обнаружены все элементы технологий без отрицания, а элемент с отрицанием обязательно **отсутствует**.
Если в одном элементе события будут обнаружены все перечисленные текстовые объекты, объект защиты не будет детектирован Системой по первому условию. Но если в объекте перехвата также будет обнаружен и указанный графический объект, Система детектирует объект защиты по второму условию. Отрицание из первого условия не влияет, на детектирование по второму условию.

Пример 4:

В компании принято использовать во всех письмах следующее предупреждающее сообщение:

> КОНФИДЕНЦИАЛЬНО
>
> Это сообщение было отправлено с использованием корпоративной электронной почты, принадлежащей компании. Сообщение (включая любые вложения) содержит конфиденциальную информацию, предназначенную исключительно для лица, которому адресовано сообщение, и защищено законом об информации. Настоящим сообщается, что любое несанкционированное раскрытие, копирование или распространение информации, содержащейся в этом сообщении, а также любые несанкционированные действия, основанные на включенной информации, запрещены.

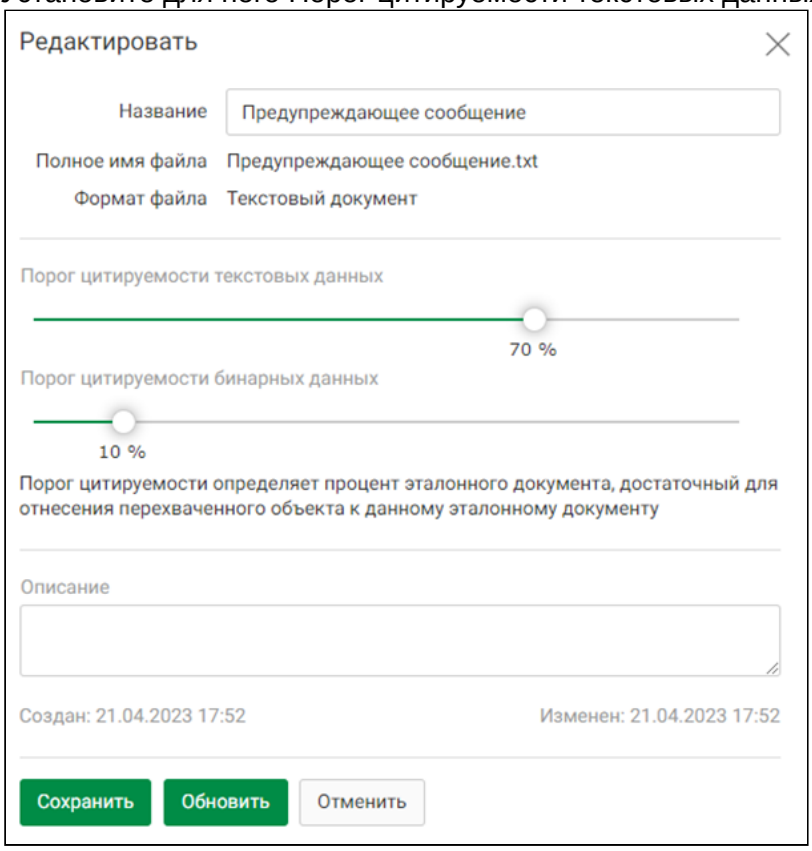
Требуется создать объект защиты для детектирования конфиденциальных документов.

В Traffic Monitor существует объект защиты "*Грифы конфиденциальности*", который детектирует любые документы/сообщения с грифами "Конфиденциально", "Строго конфиденциально", "Коммерческая тайна", "Для служебного доступа" и "ДСП". Если использовать его, то из-за наличия в предупреждающем сообщении слова «Конфиденциально» будет происходить множество ложноположительных срабатываний и искажение статистики.

Чтобы правильно настроить условия обнаружения объекта защиты в данном примере:

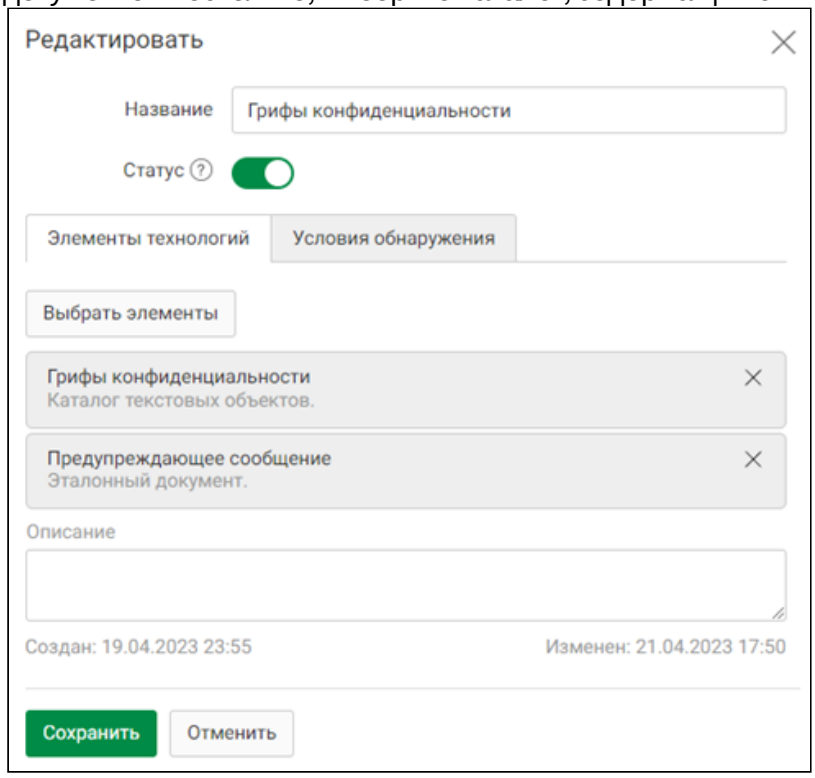
1. В разделе **Технологии** -> **Эталонные документы** создайте эталонный документ "*Предупреждающее сообщение*" на основе текстового файла, содержащего приведенное выше предупреждающее сообщение.

2. Установите для него Порог цитируемости текстовых данных от 70%.

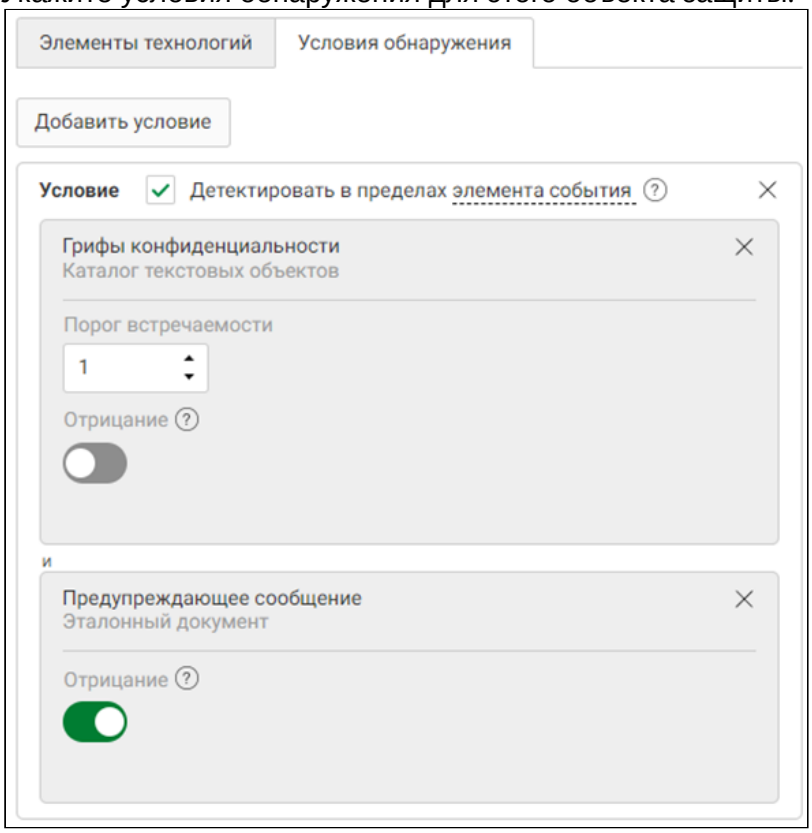


3. Создайте эталонный документ для каждого подобного предупреждающего сообщения или другого объекта, способного искажать статистику.
4. В разделе **Объекты защиты** выберите каталог «*Грифованная информация*».
5. В объект защиты "*Грифы конфиденциальности*" добавьте элемент технологий: эталонный документ "Предупреждающее сообщение". Если подобных эталонных

документов несколько, выберите каталог, содержащий эти эталонные документы.



6. Укажите условия обнаружения для этого объекта защиты:



При включении **Отрицания** у элемента технологий "Предупреждающее сообщение" будут детектироваться только те события, в которых есть грифы, но нет

предупреждающего сообщения. Таким образом, ложноположительные срабатывания не будут происходить.
Обратите внимание, что для данного условия обнаружения рекомендуется активировать функцию **Детектировать в пределах элемента события**, чтобы документ с грифом детектировался, когда он находится во вложении к письму с предупреждающим сообщением. Если не использовать эту функцию, то будет игнорироваться событие целиком.

Дополнительные сведения:
Редактирование и удаление объектов защиты выполняются стандартным способом, подробнее см.:

- Редактирование элемента
- Удаление элемента

4.5.3 Добавление элементов технологий

Цель:
Добавить элементы технологий в объект защиты.

Решение:

Вы можете добавить каталоги или отдельные элементы технологий при создании нового или редактировании ранее созданного объекта защиты (см. "Создание объекта защиты").

При создании нового объекта защиты:

1. В окне **Создание объекта защиты** перейдите на вкладку с требуемыми элементами.
2. Выберите в списке элементы или каталоги, которые вы хотите добавить.

> **Примечание.**
>
> При выборе категории на вкладке **Категория** будут также выбраны все имеющиеся у данной категории подкатегории. Если требуется добавить отдельные подкатегории, нажмите на кнопку раскрытия списка слева от названия категории и в раскрывшемся списке установите флажки в нужных полях.
>
> Это же правило действует при выборе каталогов и подкаталогов.
> Добавление каталогов в качестве элементов объекта защиты доступно для эталонных документов, печатей, текстовых объектов, бланков и выгрузок из БД.
> При добавлении каталога в объект защиты будут добавлены все элементы технологий, которые входят в него.
> Если после создания объекта защиты в задействованный каталог будут добавлены новые элементы технологий, то они также позволят детектировать объект защиты в перехваченном трафике.
> Если удалить элементы технологий из каталога, добавленного в объект защиты, детектирование по удаленным элементам прекратится.

3. Чтобы создать объект защиты на основе нескольких технологий или каталогов, повторяйте шаги 1-2, пока не будут добавлены все требуемые элементы.
4. Нажмите **Создать.**

> **Примечание.**
>
> Если выбрана настройка **Создать объект защиты на каждый выбранный элемент**, то для каждого элемента технологий будет создан отдельный объект защиты. Атрибуты объектов защиты будут заданы Системой по умолчанию.

При редактировании ранее созданного объекта защиты:

1. В окне **Редактирование объекта защиты** нажмите **Выбрать элементы**.
2. В открывшемся окне **Выбор элементов технологий** перейдите на вкладку с требуемыми элементами.
3. Отметьте в списке те элементы и каталоги, которые вы хотите добавить.

> **Примечание.**
>
> Если объект защиты включен в какую-либо политику защиты данных на агентах (см. "Создание политики защиты данных на агентах"), то в данный объект защиты можно добавить только категории и текстовые объекты.

4. Нажмите **Сохранить**.

Вы можете удалить ранее добавленные элементы или каталоги технологий. Для этого на вкладке **Элементы технологий** нажмите на крестик напротив требуемого элемента.

4.5.4 Добавление условий обнаружения

Справочная информация:

Объект защиты будет обнаружен в событии, если:

1. Объект защиты имеет статус - **Активный**.
2. В событии найдены элементы технологий, входящие в объект защиты, с учетом заданных условий обнаружения.

Каталог объектов защиты будет обнаружен в событии, если:

1. Каталог объектов защиты имеет статус - **Активный**.
2. В событии найден хотя бы один объект защиты, входящий в данный каталог.

> **Примечание.**
>
> Элементы технологий, для которых не указаны условия обнаружения, исключаются из состава объекта защиты при экспорте (см. "Импорт и экспорт объектов защиты").

Цель:

Добавить условия обнаружения для объекта защиты.

Решение:

Добавление условий обнаружения выполняется при создании объекта защиты после добавления выбранных элементов технологий (см. "Добавление элементов технологий").

Примечание.

Вы также можете добавить условия обнаружения при редактировании ранее созданного объекта защиты.

Чтобы добавить условия обнаружения для объекта защиты:

1. На вкладке **Условия обнаружения** в поле **Добавить элемент технологий** нажмите ▾ и в раскрывающемся списке выберите требуемый элемент.
2. Выбранный элемент будет добавлен в список условий. Для некоторых элементов технологий вы также можете указать дополнительные условия обнаружения (см. "Условия обнаружения").
3. Если объект защиты содержит несколько элементов технологий, добавьте условия обнаружения для остальных элементов:
   - Если требуется, чтобы условия были объединены с помощью операции конъюнкции (логическое "И"), добавьте условие, как описано на шаге 1.
     В этом случае все добавленные условия будут помещены в один блок **Условие** и объединены между собой с помощью операции конъюнкции.
   - Если требуется, чтобы условия (или группы условий) были объединены с помощью операции дизъюнкции (логическое "ИЛИ"), нажмите кнопку **Добавить условие**.
     Будет добавлен новый блок **Условие**, внутри которого вы можете добавить условия, как описано на шаге 1.
     В этом случае блоки **Условие** будут объединены между собой с помощью операции дизъюнкции, а условия внутри одного блока - с помощью операции конъюнкции.
   - Если требуется, чтобы Система детектировала объект защиты при выполнении всего условия только в пределах одного элемента события (тело письма, файл, переписка и тд.), активируйте функцию **Детектировать в пределах элемента события**.
   - Если требуется, чтобы Система **не** детектировала объект защиты при обнаружении указанного элемента технологии, включите этому элементу **Отрицание**.

     Примечание:

     В условии обнаружения обязательно должен быть хотя бы один элемент без отрицания.

     Если объект защиты добавлен в политику защиты данных на агентах, включение отрицания и детектирования в пределах одного элемента события недоступно.

4. Нажмите **Создать**, если вы находитесь в режиме создания объекта защиты, или **Сохранить**, если вы находитесь в режиме редактирования.

Дополнительные сведения:

Если вам требуется удалить условие, выполните одно из следующих действий:

- для удаления условия нажмите ✕ в правом верхнем углу панели с требуемых условием;

- для удаления блока, содержащего условия, нажмите × в правом верхнем углу блока.

4.5.5 Создание политики для объектов защиты и их каталогов

Цель:

Создать политику, где в качестве защищаемых данных будет выступать объекты защиты и их каталоги. Вы можете перейти к созданию политики непосредственно из раздела "Объекты защиты".

Чтобы создать политику для каталога объектов защиты:

1. Перейдите в раздел **Объекты защиты**.
2. В списке **Каталоги объектов защиты** в левой части рабочей области выберите требуемый каталог.
3. На панели инструментов в левой части рабочей области нажмите на кнопку ▾ и в раскрывающемся списке выберите один из пунктов:
   - **Создать политику защиты данных**
   - **Создать политику защиты данных на агентах**

   > **Примечание:**
   >
   > Для политик защиты данных на агентах в выбранных каталогах сработают только объекты защиты, в которых не включены отрицание и детектирование в пределах элемента события

4. В открывшейся форме создания политики укажите требуемые параметры (подробнее см. "Раздел Политики").
5. Нажмите **Сохранить**.

Созданная политика будет срабатывать при обнаружении хотя бы одного объекта защиты, входящего в выбранный каталог.

Чтобы создать политику для выбранных объектов защиты:

1. Перейдите в раздел **Объекты защиты**.
2. В списке **Каталоги объектов защиты** в левой части рабочей области выберите требуемый каталог.
3. В правой части рабочей области отобразится список объектов защиты, входящих в выбранный каталог. Выделите требуемый объект защиты с помощью мыши. Чтобы выделить несколько объектов, используйте клавиши Shift или Ctrl.
4. На панели инструментов в правой части рабочей области нажмите на кнопку ▾ и в раскрывающемся списке выберите один из пунктов:
   - **Создать политику защиты данных**
   - **Создать политику защиты данных на агентах**

   > **Примечание:**

Если в объекте защиты включено отрицание или детектирование в пределах элемента события, его невозможно добавить в политику защиты данных на агентах.

5. В открывшейся форме создания политики укажите требуемые параметры (подробнее см. "Раздел Политики").
6. Нажмите **Сохранить**.

Созданная политика будет срабатывать при обнаружении хотя бы одного из выбранных объектов защиты.

4.5.6 Импорт и экспорт объектов защиты

Цель:

- экспортировать в файл структуру каталогов, содержащих объекты защиты и используемые в них элементы технологий;
- загружать из файла ранее созданную структуру каталогов, содержащих объекты защиты и используемые в них элементы технологий.

Примечание:

Экспорт объектов защиты не может быть выполнен, если конфигурация Системы находится на редактировании. Импорт объектов защиты не может быть выполнен, если конфигурация Системы не применена. В противном случае будет выведено сообщение об ошибке.

Чтобы экспортировать объекты защиты:

1. Перейдите в раздел **Объекты защиты** и выберите каталог.
2. На панели инструментов в левой части рабочей области нажмите  и в раскрывающемся списке выберите пункт **Экспортировать**.
3. Начнется подготовка к загрузке, после чего архив будет сохранен на компьютере.

Сохраненный архив содержит xml-файлы, в которых хранится информация об объектах защиты и используемых в них элементах технологий. При экспорте сохраняется структура каталогов объектов защиты и элементов технологий.

Примечание:

Во время экспорта объектов защиты в условии их детектирования не сохраняется порядок элементов технологий. Поэтому при последующем импорте этих объектов защиты он может не соответствовать порядку элементов технологий, который существовал при экспорте.

Чтобы импортировать объекты защиты:

1. Перейдите в раздел **Объекты защиты**.
2. На панели инструментов в левой части рабочей области нажмите  и в раскрывающемся списке выберите пункт **Импортировать**.

3. В открывшемся окне выберите ранее экспортированный файл, который необходимо загрузить.
4. Дождитесь окончания загрузки объектов защиты в Систему.

> **Примечание:**
>
> Если название каталога в файле импорта совпадает с названием каталога в Системе, но различаются пути к каталогу, то каталог из файла импорта добавлен не будет. Если название каталога в файле импорта совпадает с названием каталога в Системе, и путь к каталогу также совпадает, то данные из файла импорта будут объединены с данными, содержащимися в Системе.

Особенности слияния данных при импорте:

1. Для каталога будут добавлены следующие элементы, отсутствующие в Системе:
   a. дочерние каталоги объектов защиты;
   b. объекты защиты.
2. Для объекта защиты будут добавлены следующие элементы, отсутствующие в Системе:
   a. элементы технологий;

> **Важно!**
>
> Выгрузки из БД, которые были созданы в Traffic Monitor версии ниже 7.4, считаются устаревшими. Устаревшие выгрузки отмечены в интерфейсе символом .
>
> Для устаревшей выгрузки недоступно редактирование и обновление. Рекомендуется удалить устаревшую выгрузку и создать ее повторно, после чего добавить созданную выгрузку в объект защиты.

   b. условия обнаружения.
3. Для условий обнаружения будут добавлены новые вложенные условия, включая параметры детектирования (для текстовых объектов, бланков и выгрузок из БД).

4.5.7 Активация и деактивация объектов защиты

По умолчанию все создаваемые объекты защиты и их каталоги имеют статус Активный (пиктограмма ). При необходимости вы можете деактивировать созданный каталог или отдельный объект защиты внутри каталога.

Чтобы деактивировать каталог объектов защиты:

1. На панели инструментов в левой части рабочей области нажмите  и в раскрывающемся списке выберите **Деактивировать**.
2. Статус каталога изменится на Неактивный (пиктограмма ).

Если вам требуется снова активировать деактивированный каталог, нажмите и в раскрывающемся списке выберите **Активировать**.

Чтобы деактивировать выбранный объект защиты:

1. В левой части рабочей области выберите требуемый каталог.
2. В правой части рабочей области щелчком левой кнопки мыши выделите в списке требуемый объект защиты.
3. На панели инструментов в правой части рабочей области нажмите и в раскрывающемся списке выберите **Деактивировать**.
4. Статус объекта защиты изменится на Неактивный (пиктограмма).

Если вам требуется снова активировать деактивированный объект защиты, нажмите и в раскрывающемся списке выберите **Активировать**.

> **Примечание:**
>
> Если объект защиты выбран в результате сквозного поиска по каталогам, изменить его статус при редактировании или кнопками **Активировать** и **Деактивировать** будет невозможно. Для изменения статуса объекта защиты выберите его в каталоге.
> Это ограничение связано с тем, что объект защиты может входить в разные каталоги, в том числе неактивные.

> **Важно!**
>
> Объекты защиты и их каталоги могут быть обнаружены в перехваченных данных только в том случае, если они активированы.

4.6 Работа с объектами перехвата

Для чего требуется работа с объектами перехвата?

- отслеживать статистику нарушений политики корпоративной безопасности;
- просматривать сведения по каждому объекту в отдельности;
- отображать объекты перехвата, удовлетворяющие определенным критериям.

Для ежедневного мониторинга, а также для оперативного получения статистики удобно использовать виджеты в разделе "Сводка".

Если требуется просмотреть большое количество событий за определенный период, вы можете создать запрос в разделе "События".

Работа с объектами перехвата включает следующие действия:

Действие	Описание
Просмотр сводки по нарушениям/ нарушителям	Просмотр статистической информации и подборок по событиям
Просмотр событий	Просмотр сведений по каждому объекту перехвата

Действие	Описание
Создание выгрузки сводки	Генерирование сводки по нарушениям/ нарушителям
Просмотр выгрузки сводки	Просмотр сформированных выгрузок
Вынесение решения по объекту	Решение по объекту, вынесенное пользователем
Добавление/удаление тега	Добавление тега объекту перехвата
Сохранение события (для SMTP-писем)	Сохранение объекта перехвата в формате EML на диск
Выгрузка событий	Сохранение информации о событиях на диск компьютера
Досылка события, находящегося в карантине	Отправление заблокированного сообщения адресату
Создание запросов	Фильтрация объектов перехвата по указанным критериям

См. также:

- Раздел "События" - о разделе, где выполняется поиск объектов перехвата по заданным критериям
- Раздел "Сводка" - о разделе, где можно просмотреть сводку по объектам перехвата

4.6.1 Просмотр сводки по нарушениям/нарушителям

Работа ведется в разделе **Сводка** (см. "Раздел Сводка")

Цель:
Просмотреть сводку по нарушениям/нарушителям.

Решение:

1. Перейдите в раздел **Сводка**.
2. Настройте панель, где будут расположены виджеты (см. "Создание панели").
3. Добавьте и настройте требуемый виджет (см. "Создание и настройка виджета").
4. Изучите сводку, представленную на виджете.

Вы можете выгрузить сводку в формате PDF или HTML (см. "Создание выгрузки сводки").

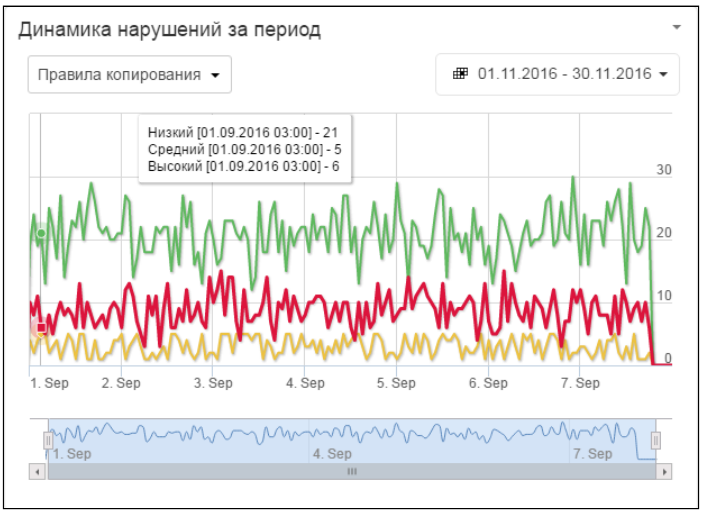
Все сформированные выгрузки сохраняются в Системе. Вы можете просмотреть требуемую выгрузку или удалить выгрузки, хранение которых не требуется (см. "Просмотр выгрузки сводки").

Пример 1:
Требуется отследить динамику копирования файлов, содержащих конфиденциальные данные (подробнее о действиях, относящихся к копированию данных, см. "Правило копирования").

Для этого:

1. Создайте панель или откройте ранее созданную панель.
2. Добавьте виджет "Динамика нарушений за период" (подробнее о настройке данного виджета см. "Динамика нарушений за период").
3. В правом верхнем углу виджета выберите период - *Текущий месяц*.
4. В левом верхнем углу виджета выберите в списке правил - *Правила копирования*.

В результате на виджете будут показаны графики, отображающие динамику нарушений правил копирования за текущий месяц.



Чтобы перейти к просмотру событий за определенный день и час, щелкните левой клавишей мыши по точке пересечения временной шкалы и кривой количества нарушений.

Пример 2:
Требуется показать все объекты перехвата за текущую неделю, отправителем или получателем трафика в которых был *Иванов Иван* (подразумевается, что персона *Иванов Иван* уже создана в разделе **Персоны**).

Для этого:

1. Создайте панель или откройте ранее созданную панель.
2. Добавьте виджет "Подборка" (подробнее о настройке данного виджета см. "Подборка").
3. Перейдите в режим редактирования виджета и укажите атрибуту **Подборка** ранее созданный запрос *Иванов* (см. пример 2 в статье "Примеры использования запросов").
4. Сохраните виджет.

Создание панели

Цель:
Создать панель, на которой будут располагаться виджеты.

Решение:

1. Перейдите в раздел "**Сводка**".
2. В левом верхнем углу рабочей области нажмите + **Добавить**.
3. Укажите название для новой панели.
4. Нажмите **Сохранить**.

Дополнительные сведения:

- Наполнение панели описано в статье "Создание и настройка виджета".

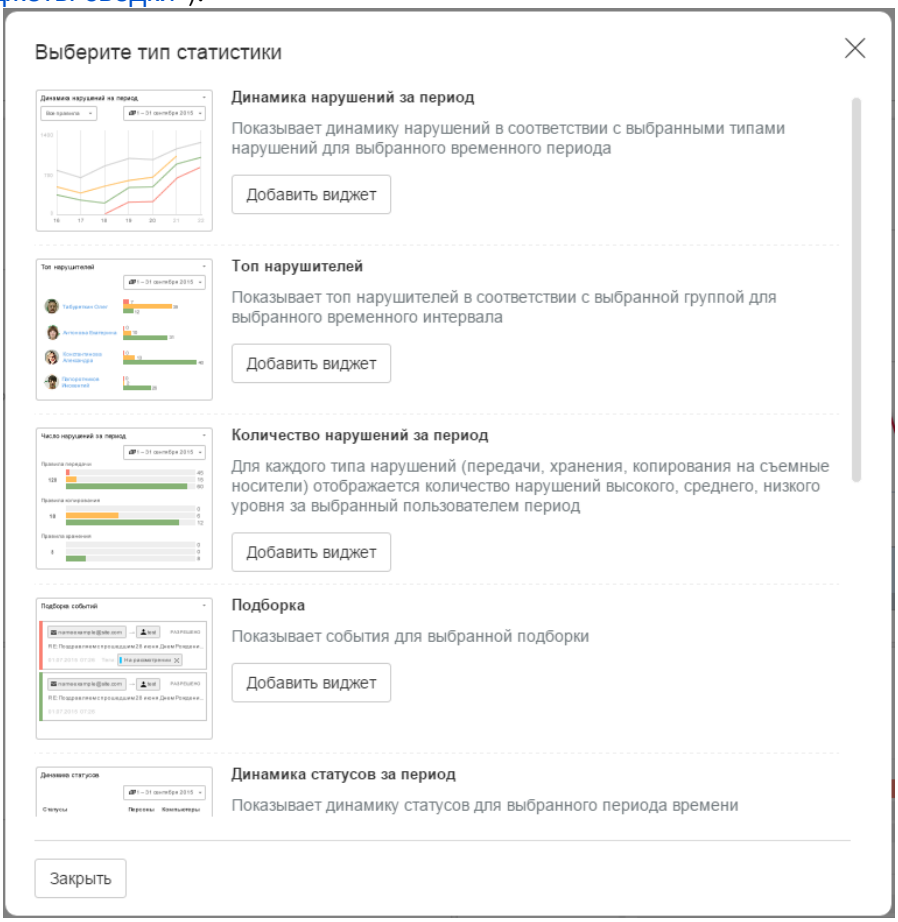
- Для удаления панели перейдите на панель, которую требуется удалить и нажмите на вкладке с названием панели. В окне подтверждения нажмите **Удалить**.

Создание и настройка виджета

Цель:
Создать виджет на панели сводки.

Решение:

1. Перейдите в раздел "**Сводка**".
2. Перейдите на панель, на которую требуется добавить виджет, или создайте новую панель (см. "Создание панели").
3. Нажмите **Добавить виджет**.
4. В открывшемся окне **Выберите тип статистики** выберите требуемый виджет и нажмите **Добавить виджет** под его описанием (подробнее о типах виджетов см. в статье "Виджеты сводки").



Примечание.

Вы можете добавить на панель несколько виджетов подряд. Для этого нажммите **Добавить виджет** под всеми виджетами, которые вы хотите добавить.

> **Совет**
>
> Вы можете добавить несколько виджетов одного типа, а затем настроить их на отображение различных типов данных: например, несколько виджетов с типом **Подборка** для отображения событий по результатам запросов (см. "Создание запросов").

5. Нажмите **Закрыть** или используйте кнопку ✕ в правом верхнем углу окна.
6. Настройте добавленные виджеты для отображения требуемых данных (параметры виджетов описаны в подразделе "Виджеты сводки").

Дополнительные сведения:

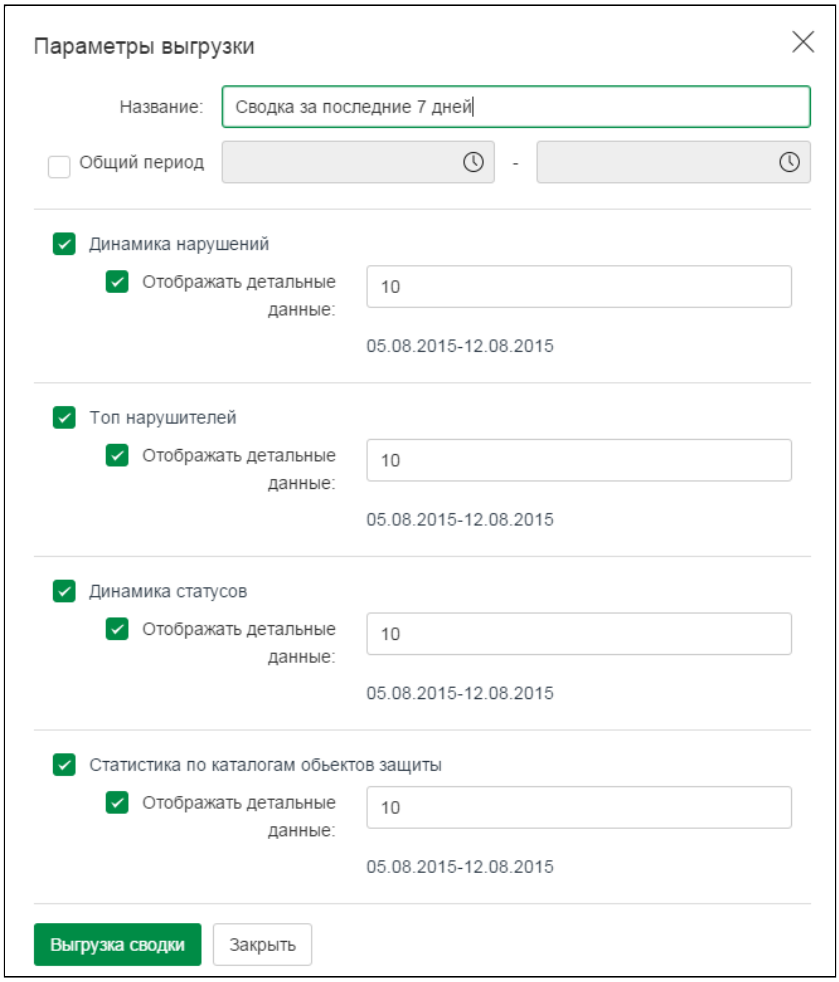
1. Вы можете перемещать плитки виджета, располагая их в удобном порядке. Для этого:
   a) Наведите указатель мыши на заголовок плитки, чтобы стандартный вид курсора изменился на вид курсора перемещения (четырехконечная стрелка).
   b) Зажмите левую клавишу мыши и, удерживая ее зажатой, перемещайте плитку по рабочей области, пока целевая позиция плитки не выделится пунктирной линией.
   c) Отпустите левую клавишу мыши.
2. Чтобы отредактировать виджет, в правом верхнем углу нажмите ▾ и в раскрывающемся списке выберите **Редактировать**. В открывшемся окне **Общие настройки виджета** измените требуемые параметры, после чего нажмите **Сохранить**.
3. Чтобы удалить виджет, в правом верхнем углу нажмите ▾ и в раскрывающемся списке выберите **Удалить**. В окне подтверждения нажмите **Да**.

Создание выгрузки сводки

Цель:
Создать выгрузку сводки по объектам перехвата.

Решение:

1. Перейдите в раздел "**Сводка**".
2. Перейдите на панель, для которой требуется сформировать выгрузку.
3. В правом верхнем углу рабочей области нажмите **Выгрузить**.
4. В открывшемся окне укажите атрибуты выгрузки (см. "Выгрузка сводки").



5. Убедитесь, что флажками отмечены все виджеты, данные которых вы хотите включить в выгрузку.
6. Если вы хотите вручную указать период, за который будет сформирована выгрузка, установите флажок в поле **Общий период** и введите начальную и конечную дату. Если данная настройка не выбрана, то для каждого виджета, включенного в отчет, выгрузка будет сформирована за период, указанный в настройках виджета.
7. Нажмите **Выгрузка сводки**.

В правом верхнем углу рабочей области будет отображаться информация о ходе генерации выгрузки.

После завершения генерации будет предложено открыть выгрузку в формате PDF или HTML.

Все созданные выгрузки сохраняются в Системе и доступны по нажатию кнопки **Посмотреть список выгрузок** в правом верхнем углу рабочей области. Подробнее см. "Просмотр выгрузок сводки".

Вы также можете просмотреть информацию о сформированных выгрузках из любого раздела Консоли управления, нажав на кнопку **Выгрузки** на панели навигации (см. "Интерфейс Консоли управления Traffic Monitor", №6 на скриншоте).

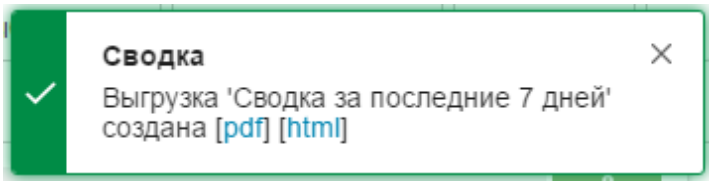
Примечание:

Если виджет, по которому была сформирована выгрузка, будет изменен либо удален с панели, то ранее созданная выгрузка изменена не будет.

Просмотр выгрузки сводки

Цель:
Изучить сформированную выгрузку сводки по объектам перехвата.

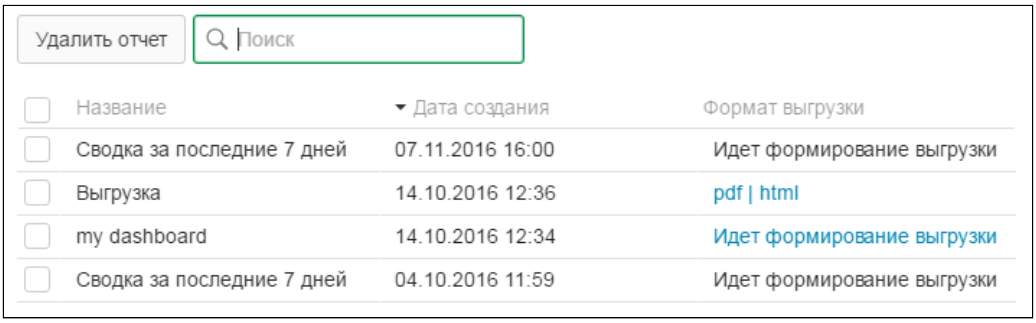
Решение:
По завершении генерации выгрузки в правом верхнем углу рабочей области отображается информационное сообщение с предложением открыть выгрузку в формате PDF или HTML.



Нажмите на ссылку **pdf** или **html**, чтобы открыть выгрузку в новом окне браузера. Также вы можете сохранить, отправить или распечатать созданную выгрузку стандартными средствами вашего браузера и операционной системы. Все сгенерированные выгрузки сохраняются в Системе.

Чтобы посмотреть список сгенерированных выгрузок, в правом верхнем углу рабочей области нажмите кнопку  **Посмотреть список выгрузок**. В открывшемся окне **Выгрузки** отображается информация о выгрузках.

> **Примечание.**
>
> Вы можете отсортировать выгрузки в списке по дате создания, а также воспользоваться полем **Поиск** для поиска нужной выгрузки по названию.



Чтобы просмотреть выбранную выгрузку, в столбце **Формат выгрузки** напротив требуемой выгрузки нажмите:

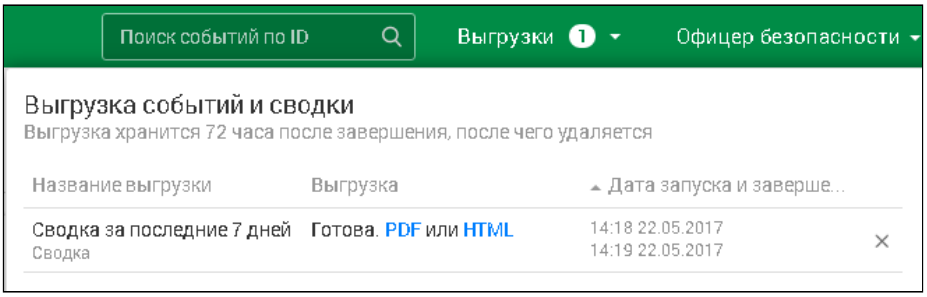
- **pdf** - если требуется отобразить выгрузку сводки в формате PDF;
- **html** - если требуется отобразить выгрузку сводки в формате HTML.

Откроется новая вкладка браузера, где будет показана выбранная выгрузка.

Чтобы удалить выбранные выгрузки:

1. Установите флажки напротив выгрузок, которые вы хотите удалить. Чтобы выбрать все строки сразу, установите флажок в заголовке.
2. Нажмите **Удалить отчет**.

Вы также можете просмотреть список выгрузок из любого раздела Консоли управления, нажав на кнопку **Выгрузки** на панели навигации.



В списке для каждой выгрузки отображается название, статус, дата запуска и завершения, а также ссылки PDF и HTML. Чтобы просмотреть выгрузку в новой вкладке браузера, нажмите на ссылку с выбранным форматом.

Чтобы удалить информацию о выгрузке из списка, нажмите ✕ в строке выбранной выгрузки.

4.6.2 Просмотр событий

Цель:
Просмотреть информацию по объекту перехвата.

Решение:

1. Перейдите в раздел **События** (см. "Раздел События").
2. Создайте и выполните запрос (см. "Создание запросов").

> **Примечание:**
>
> В списке отображаются последние 10 000 событий. События отсортированы по ID-номеру события в порядке убывания.

3. При необходимости измените список полей просмотра (см. "Выбор полей просмотра событий").
4. Просмотрите информацию в плитке события или в строке таблицы (см. п.3 на схеме в статье " Раздел События ").
5. Для получения дополнительно информации используйте краткую и детальную формы просмотра события.

Создание запросов

Цель:
Создать запрос для поиска нужных событий.

Решение:

1. Перейдите в раздел **События** (см. "Раздел События").
2. Если вы хотите создать запрос внутри папки, выберите нужную папку из списка или создайте новую папку (см. "Создание папки с запросами").
3. Создайте запрос в стандартном или расширенном режиме. Вы можете создать запрос внутри выбранной папки или на верхнем уровне.
4. Чтобы запустить выполнение запроса, выберите запрос в списке в левой части рабочей области и нажмите ▶ **Выполнить запрос** на панели инструментов (при создании запроса вы можете также использовать кнопку **Сохранить и выполнить**).

Вы также можете копировать или переместить ранее созданную папку или запрос.

Чтобы копировать папку и содержащиеся в ней запросы:

1. Выберите нужную папку в списке.
2. На панели инструментов в левой части рабочей области нажмите  **Копировать**.

Если выполняется копирование вложенной папки и у пользователя есть полный доступ к родительской папке, то копия будет в ту же папку, где расположена копируемая папка. Если у пользователя отсутствует полный доступ к родительской папке, или выполняется копировании папки верхнего уровня, то копия будет добавлена в корень дерева папок.

Чтобы копировать запрос:

1. Выберите запрос в списке.
2. На панели инструментов в левой части рабочей области нажмите  **Копировать**.

Если выполняется копирование внутри папки и у пользователя есть полный доступ к папке, то копия будет добавлена в ту же папку, где расположен копируемый запрос. Если у пользователя отсутствует полный доступ к папке, или выполняется копирование запроса верхнего уровня, то копия будет добавлена в корень дерева папок.

Чтобы переместить папку, выберите в списке нужную папку и, удерживая левую клавишу мыши зажатой, переместите ее в требуемое место.

> **Примечание:**
>
> Для перемещения папки пользователь должен иметь полный доступ как к перемещаемой папке, так и к папке, в которую выполняется перемещение. Если папка содержит запросы, пользователю также требуется полный доступ к запросам, содержащимся в папке. Подробнее см. таблицу ниже.

Чтобы переместить запрос, выберите в списке нужный запрос и, удерживая левую клавишу мыши зажатой, переместите его в требуемое место.

> **Примечание:**
>
> Для перемещения запроса пользователь должен иметь полный доступ как к запросу, так и к папке, в которую выполняется перемещение. Подробнее см. таблицу ниже.

В таблице ниже указано, какими правами должен обладать пользователь для выполения действий с запросами:

Действия в системе	**Права доступа**			
	Просмотр папки	Полный доступ к папке	Просмотр и выполнение запроса	Полный доступ к запросу
Просмотр папки	+	+	+	+

Редактирование атрибутов папки (название, описание, права доступа)		+		
Копирование папки	+	+	+	+
Создание нового элемента (запроса или подпапки) в папке запросов		+		
Перемещение пустой папки в другую папку		+		
Перемещение папки, содержащей хотя бы один запрос		+		
Удаление пустой папки		+		
Удаление папки, содержащей хотя бы один запрос		+		
Просмотр и выполнение запроса	+	+	+	+
Редактирование параметров запроса (в том числе, прав доступа)		+		+
Копирование запроса	+	+	+	+
Перемещение запроса в другую папку		+		+
Удаление запроса		+		+

Примечание.

Если в результате редактирования прав доступа запрос или папка оказываются недоступны ни одному пользователю Системы, то полный доступ к запросу/папке будет автоматически предоставлен текущему пользователю.

См. также:

- Создание папки с запросами
- Создание запроса в обычном режиме
- Создание запроса в расширенном режиме
- Примеры использования запросов

Создание папки с запросами

Цель:
Создать папку, в которой будут сгруппированы запросы.

Решение:

1. Перейдите в раздел **События**.
2. В списке папок и запросов в левой части рабочей области выберите, на каком уровне требуется создать папку. Вы можете создать папку верхнего уровня или подпапку внутри уже созданной папки с запросами.

> **Примечание:**
>
> Если у вас отсутсвуют права на создание элементов внутри выбранной папки, будет выведено сообщение. В этом случае необходимо создать папку в другом месте.

3. Нажмите  и в раскрывающемся списке выберите **Создать папку запросов**.
4. В открывшейся форме введите название папки.
5. Укажите, должны ли права доступа к папке наследоваться для вложенных подпапок и запросов. По умолчанию опция **Применить права для дочерних папок и запросов** не выбрана.

> **Примечание:**
>
> Если вы создаете подпапку внутри папки, для которой выбрана опция **Применить права для дочерних папок и запросов**, то действия, описанные на шаге 5-6, недоступны.

6. Укажите, кому доступна папка, и определите права доступа. Для этого:
   a. Найдите в списке требуемых пользователей.

> **Совет.**
>
> Для поиска нужных пользователей в списке воспользуйтесь полем **Поиск**.

   b. Напротив имен требуемых пользователей установите флажок в одном из полей:
      - **Просмотр и выполнение** - чтобы предоставить пользователю права на просмотр и копирование папки. Права доступа к запросам, содержащимся в папке, определяются при создании запроса;
      - **Полный доступ** - чтобы предоставить пользователю полный доступ к папке.

> **Примечание:**
>
> Чтобы предоставить доступ к папке всем пользователям Системы, установите флажок в поле с требуемым уровнем доступа напротив значения **Все пользователи**.

7. Нажмите **Сохранить**.

Редактирование папки выполняется с помощью кнопки  на панели инструментов.

Для удаления папки используйте кнопку  .

> **Примечание:**
>
> Для редактирования и удаления папки пользователю необходимо иметь полный доступ к папке. Если для выбранной папки вам разрешены только просмотр и выполнение, то вместо кнопки  будет отображаться кнопка , а кнопка  будет недоступна.

Создание запроса в обычном режиме

Цель:
Создать запрос для поиска событий, удовлетворяющих заданным условиям.

Решение:

1. Перейдите в раздел **События**.
2. В списке папок и запросов в левой части рабочей области выберите, на каком уровне требуется создать запрос. Вы можете создать запрос верхнего уровня или внутри выбранной папки.

   > **Примечание:**
   >
   > Если у вас отсутсвуют права на создание элементов внутри выбранной папки, будет выведено предупреждение. В этом случае необходимо создать запрос в другом месте.

3. На панели инструментов нажмите  и в раскрывающемся списке выберите **Создать обычный запрос**.
4. В открывшейся форме введите название запроса и при необходимости добавьте описание.
5. На вкладке **Запрос** отредактируйте параметры, которые будут использоваться в запросе. По умолчанию показаны наиболее часто используемые параметры. Для выбранных параметров укажите значения в полях ввода. Чтобы удалить параметры, которые не будут использоваться в запросе, нажмите  в правом углу выбранного элемента.
6. Чтобы добавить параметр, в раскрывающемся списке **Добавить условие** выберите требуемый параметр и его одно или несколько значений (полный список доступных параметров см. в статье "Обычный режим создания запроса").
7. На вкладке **Столбцы** выберите атрибуты, значения которых будут показаны для найденных событий.
8. На вкладке **Доступ** укажите, кому будет доступен запрос, и определите права доступа.

   > **Важно!**

Если запрос создается внутри папки, для которой выбрана настройка **Применить права для дочерних папок и запросов**, то права доступа к запросу будут соответствовать правам доступа, указанным для папки. Редактирование прав доступа к запросу в этом случае недоступно.

Чтобы указать права доступа к запросу:

a. Найдите в списке требуемых пользователей.

> **Совет.**
>
> Для поиска нужных пользователей в списке воспользуйтесь полем **Поиск**.

b. Напротив имен требуемых пользователей установите флажок в одном из полей:
   - **Просмотр и выполнение** - чтобы предоставить пользователю права на просмотр, копирование и выполнение запроса;
   - **Полный доступ** - чтобы предоставить пользователю полный доступ к запросу.

> **Примечание:**
>
> Чтобы предоставить доступ к папке всем пользователям Системы, установите флажок в поле с требуемым уровнем доступа напротив значения **Все пользователи**.

9. Нажмите:
   - **Сохранить** - чтобы сохранить запрос.
   - **Сохранить и выполнить** - чтобы сохранить и выполнить запрос.

> **Совет.**
>
> Если в процессе создания запроса вы обнаружите, что вам требуется более гибкая настройка параметров, воспользуйтесь расширенным режимом создания запроса. Для этого в поле **Тип запроса** нажмите **Расширенный**. Будет выполнен переход в расширенный режим создания запроса. При этом все введенные параметры запроса сохранятся.

Редактирование запроса выполняется с помощью кнопки  на панели инструментов.

Для удаления запроса используйте кнопку .

> **Примечание:**
>
> Для редактирования, удаления и перемещения запроса пользователю необходимо иметь полный доступ к запросу. Если для выбранного запроса вам разрешены только просмотр и выполнение, то вместо кнопки  будет отображаться кнопка , а кнопка  будет недоступна.

В статье "Примеры использования запросов" приведен пример создания поискового запроса в обычном режиме.

Создание запроса в расширенном режиме

Цель:
Выполнить гибкую настройку условий поиска событий.

Решение:

1. Перейдите в раздел **События**.
2. В списке папок и запросов в левой части рабочей области выберите, на каком уровне требуется создать запрос. Вы можете создать запрос верхнего уровня или выбрать папку, в которой будет создан запрос.

   > **Примечание:**
   >
   > Если у вас отсутсвуют права на создание элементов внутри выбранной папки, будет выведено предупреждение. В этом случае необходимо создать запрос в другом месте.

3. На панели инструментов нажмите + и в раскрывающемся списке выберите **Создать расширенный запрос**.
4. В открывшейся форме введите название запроса и при необходимости добавьте описание.
5. На вкладке **Запрос** отредактируйте параметры, которые будут использоваться в запросе. По умолчанию показаны наиболее часто используемые параметры. Для выбранных параметров укажите значения в полях ввода. Чтобы удалить параметры, которые не будут использоваться в запросе, нажмите × в правом углу выбранного элемента.
6. Чтобы добавить параметр, в раскрывающемся списке **Добавить условие** выберите требуемый параметр и введите одно или несколько значений.
7. По умолчанию все параметры связаны операцией конъюнкции (логическое "И"). Для изменения типа операции нажмите на пиктограмму and. При этом пиктограмма изменится на or, что соответствует операции дизъюнкции (логическое "ИЛИ").
8. Для отделения атрибутов, связанных операцией конъюнкции (логическое "И"), от атрибутов, связанных операцией дизъюнкции (логическое "ИЛИ"), используйте элемент **Группа параметров** (см. "Расширенный режим").
9. На вкладке **Поля просмотра** выберите атрибуты, значения которых будут показаны для найденных событий .
10. На вкладке **Доступ** укажите, кому будет доступен запрос, и определите права доступа.

    > **Важно!**
    >
    > Если запрос создается внутри папки, для которой выбрана настройка **Применить права для дочерних папок и запросов**, то права доступа к запросу будут соответствовать правам доступа, указанным для папки. Редактирование прав доступа к запросу в этом случае недоступно.

    Чтобы указать права доступа к запросу:

a. Найдите в списке требуемых пользователей.

> **Совет.**
>
> Для поиска нужных пользователей в списке воспользуйтесь полем **Поиск**.

b. Напротив имен требуемых пользователей установите флажок в одном из полей:
   - **Просмотр и выполнение** - чтобы предоставить пользователю права на просмотр, копирование и выполнение запроса;
   - **Полный доступ** - чтобы предоставить пользователю полный доступ к запросу.

> **Примечание:**
>
> Чтобы предоставить доступ к папке всем пользователям Системы, установите флажок в поле с требуемым уровнем доступа напротив значения **Все пользователи**.

11. Нажмите:
    - **Сохранить** - чтобы сохранить запрос.
    - **Сохранить и выполнить** - чтобы сохранить и выполнить запрос.

> **Примечание.**
>
> Если в процессе создания запроса вы захотите продолжить работу с запросом в обычном режиме, то в поле **Тип запроса** нажмите **Обычный**. Будет выполнен переход в обычный режим создания запроса. При этом все введенные параметры запроса сохранятся. Однако если заданные условия могут быть реализованы только в расширенном режиме, то переключение в обычный режим будет недоступно.

Редактирование запроса выполняется с помощью кнопки  на панели инструментов.

Для удаления запроса используйте кнопку  .

> **Примечание:**
>
> Для редактирования и удаления запроса пользователю необходимо иметь полный доступ к запросу. Если для выбранного запроса вам разрешены только просмотр и выполнение, то вместо  будет отображаться кнопка , а кнопка  будет недоступна.

В статье "Примеры использования запросов" приведены примеры создания запросов в расширенном режиме.

Использование расширенного синтаксиса

Цель:
Настроить поиск по тексту события с использованием расширенного синтаксиса.

Решение:

1. Перейдите в расширенный режим создания запроса.
2. На вкладке **Запрос**, в раскрывающемся списке **Добавить условие**, выберите параметр **Текст события**.
3. Включите настройку **Расширенный синтаксис**.
4. В поле **Запрос** введите искомый текст, используя логические операторы: "|", "-", "!", "( )" и другие.

   > **Примечание:**
   >
   > При включенной опции **Расширенный синтаксис** поиск спецсимволов может быть осуществлен при помощи экранирования. Экранирование символов выполняется с помощью символа '\', помещенного перед экранируемым символом.

5. Укажите остальные параметры запроса (подробнее см. "Создание запроса в расширенном режиме").
6. Нажмите **Сохранить**.

Подробную информацию о создании запросов с использованием логических операторов Вы можете найти в Интернет-статье о языке поисковых запросов Sphinx.

> **Примечание:**
>
> Обратите внимание, что область, в которой будет выполняться поиск, указывается в явном виде в поле **Область поиска** (см. "Поиск по тексту события"). Указывать область поиска с помощью операторов языка Sphinx не требуется.

Пример:

Если требуется, чтобы в тексте события:

- содержались слова *"персональные данные клиентов"* или *"личные данные клиентов"*;
- не содержалась фраза *"конфиденциальная информация"*,

Офицер безопасноти может создать следующий запрос, используя расширенный синтаксис:

```
(персональные| личные) данные клиентов -"конфиденциальная информация"
```

Примеры использования запросов

Пример 1:

Требуется посмотреть все почтовые сообщения за текущий день, которые отправляли сотрудники под наблюдением. Для этого:

1. Создайте запрос в обычном режиме и укажите его название.
2. Укажите следующие параметры запроса:
   - **Дата перехвата** - *Текущий день*;
   - **Тип события** - *Почта*.
3. В поле **Отправители** укажите группу "Сотрудники под подозрением" (пример создания такой группы описан в статье "Создание группы персон и компьютеров").
4. Сохраните и выполните запрос.

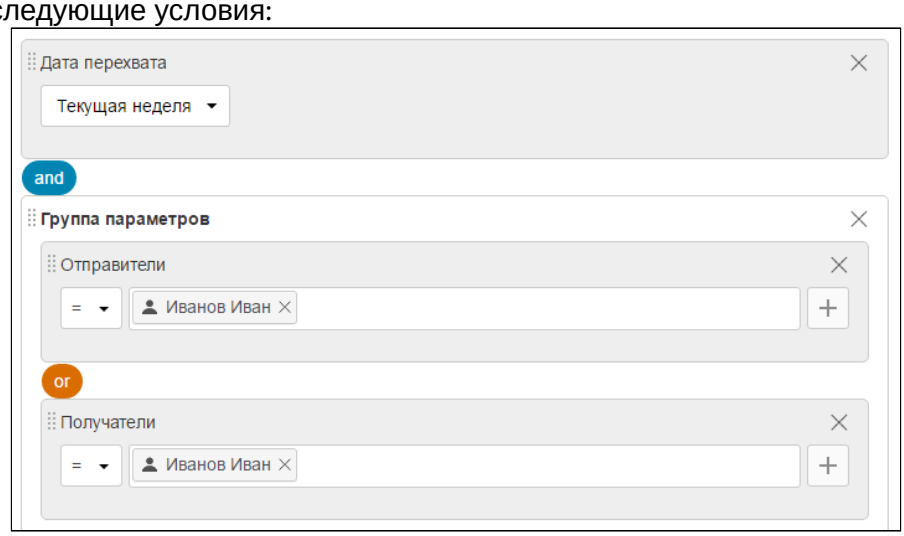
> **Совет**
>
> Если в вашей организации большой трафик и выполнение запроса занимает много времени, вы можете продолжить работу с другими задачами, пока запрос выполняется в фоновом режиме. Как только запрос будет выпонен, Система уведомит вас всплывающей подсказкой.

Пример 2:

Сотрудник Иванов Иван подозревается в нецелевом использовании служебной информации. Известно, что инцидент произошел в течение недели. Требуется найти события по персоне Иванов Иван для расследования инцидента.

Для этого:

1. Создайте запрос в расширенном режиме и укажите его название - *Иванов*.
2. Добавьте следующие условия:



3. Сохраните и выполните запрос.

Пример 3:

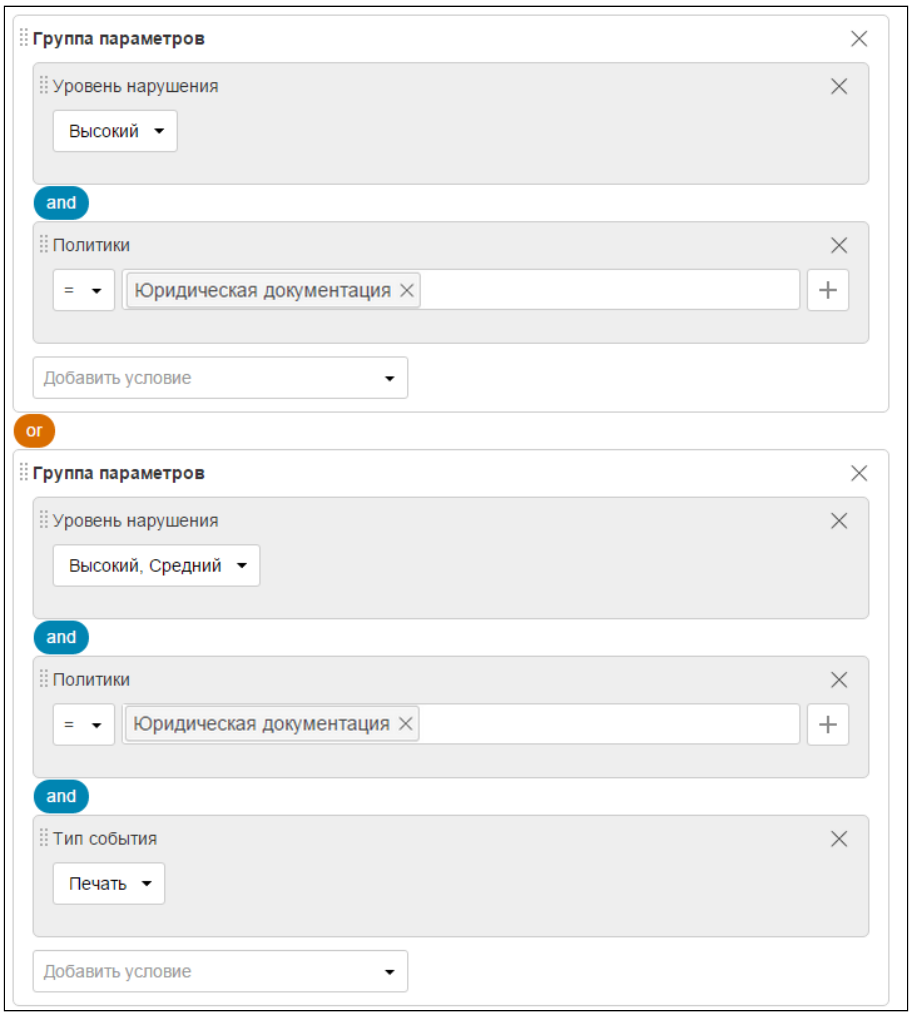
Требуется найти события:

- с уровнем нарушения *Высокий* и политикой *Юридическая документация*;
- с уровнями нарушения *Высокий* или *Средний*, политикой *Юридическая документация* и типом события *Печать*:

Для этого:

1. Создайте запрос в расширенном режиме и укажите его название.
2. Добавьте два элемента *Группа параметров*, связанных операцией дизъюнкции.
3. Внутри первой группы добавьте следующие атрибуты, связанные операцией конъюнкции:
    - **Уровень нарушения** - *Высокий*;
    - **Политика** - *Юридическая документация.*
4. Внутри второй группы добавьте следующие атрибуты, связанные операцией конъюнкции:
    - **Уровень нарушения** - *Высокий* и *Средний*;
    - **Политика** - *Юридическая документация*;
    - **Тип события** - *Печать.*

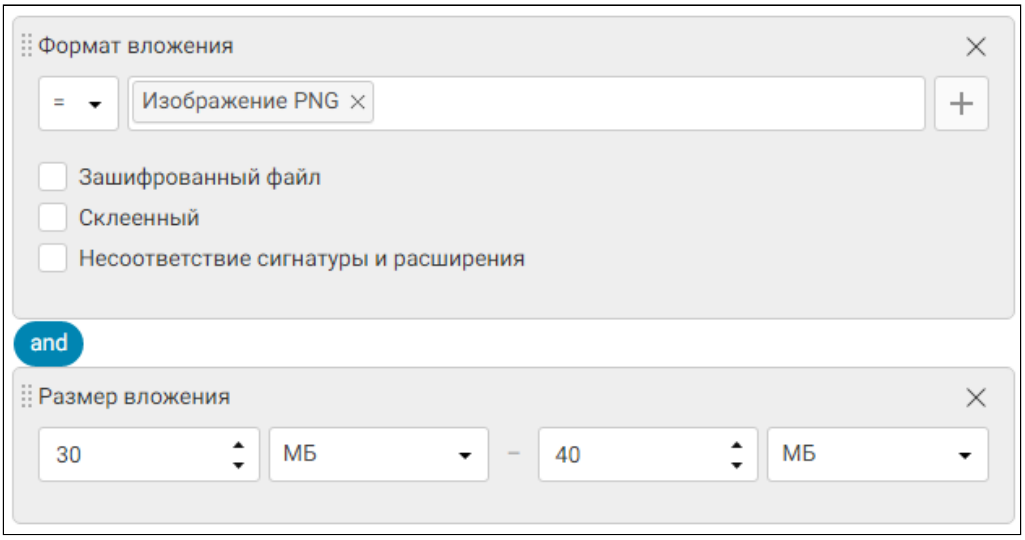
5. Сохраните и выполните запрос.



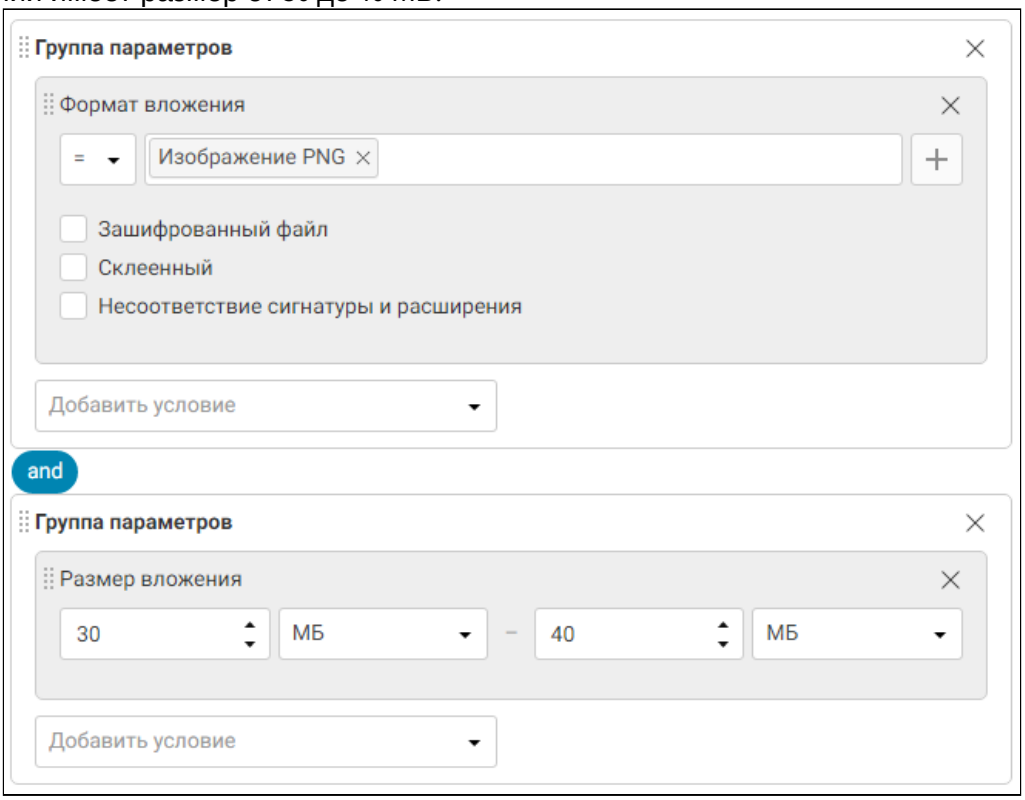
Пример 4:

Если условия заданы для вложений объекта, то при наличии у объекта нескольких вложений условия будут применяться следующим образом:

1. Если несколько условий объединены с помощью операции конъюнкции (логическое "И") внутри одной группы параметров, то после выполнения запроса будут показаны объекты, у которых хотя бы одно вложение удовлетворяет всем заданным условиям. В примере ниже при выполнении запроса будут показаны объекты, у которых хотя бы одно вложение имеет формат PNG и размер от 30 до 40 МБ.



2. Если каждое условие содержится в отдельной группе параметров и группы объединены между собой с помощью операции конъюнкции (логическое "И"), то после выполнения запроса будут показаны объекты, у которых каждое условие выполняется для какого-либо из вложений. В примере ниже при выполнении запроса будут показаны объекты, у которых хотя бы одно вложение имеет формат PNG и хотя бы одно из вложений имеет размер от 30 до 40 МБ.



Пример 5:

Требуется найти события с eml-вложениями.

Для этого:

1. Создайте запрос в любом режиме и укажите его название.
2. Добавьте элемент *Формат вложения*
3. Задайте ему значение "*Электронное письмо*"

4. Сохраните и выполните запрос.

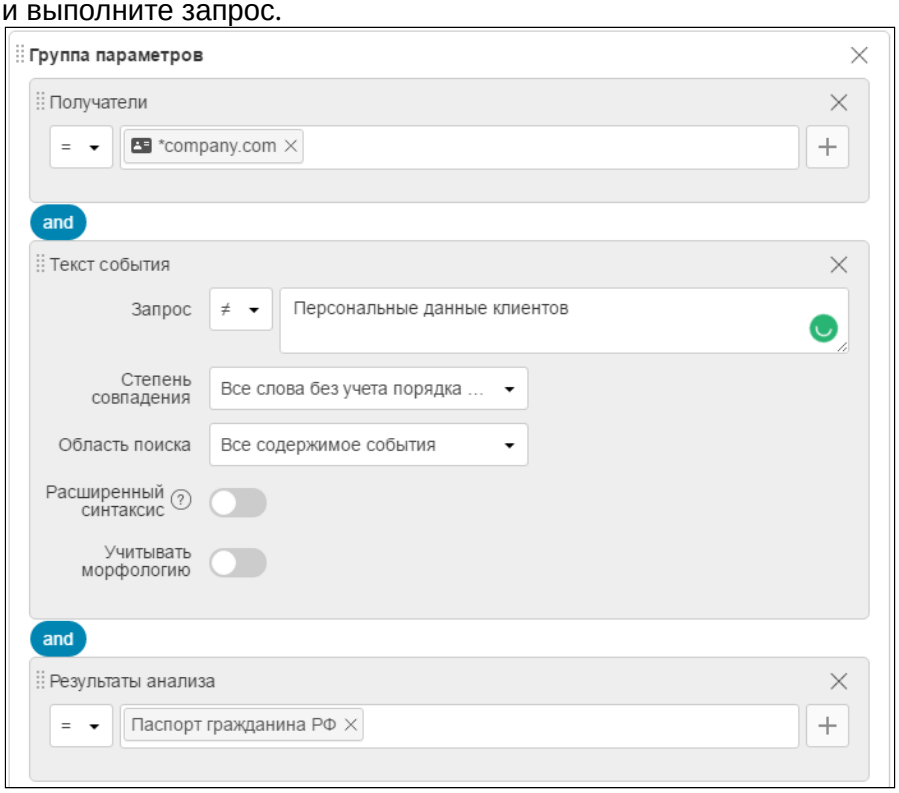
Пример 6:

Требуется найти события:

1. пересылаемые внутри компании;
2. не содержащие слова *Персональные данные клиентов* в тексте события;
3. содержащие номера паспортов:

Для этого:

1. Создайте запрос в расширенном режиме и укажите его название.
2. Добавьте элемент *Группа параметров*.
3. Внутри группы параметров укажите следующие атрибуты, связанные операцией конъюнкции:
   a. `Получатели` - **company.com*;
   b. `Текст события` - *"Персональные данные клиентов"*, при этом выбрана степень совпадения *Все слова без учета порядка следования и расстояния между ними*, и к атрибуту применено отрицание;
   c. `Область поиска` - *"Все содержимое события"*;
   d. `Результаты анализа` - текстовый объект *"Паспорт гражданина РФ"*.
4. Сохраните и выполните запрос.



Пример 7:

Требуется найти события, в которых не содержится текстовый объект "Паспорт гражданина РФ".

Для этого:

1. Создайте запрос и укажите его название.
2. Добавьте элемент *Технологии*.
3. В качестве значения выберите текстовый объект "*Паспорт гражданина РФ*" и примените к атрибуту отрицание.

4. Сохраните и выполните запрос.



В результате будут найдены события, в которых:

1. не сработал ни один объект защиты;
2. в сработавших объектах защиты не содержится текстовый объект "*Паспорт гражданина РФ*".

Если дополнительно указать серию и номер паспорта (серия 4505 номер 123456), то будут найдены события, в которых:

1. не сработал ни один объект защиты;
2. в сработавших объектах защиты не содержится тектовый объект "*Паспорт гражданина РФ*" со значением "серия 4505 номер 123456".

Выбор полей просмотра событий

Справочная информация:
По умолчанию в строке таблицы отображаются все атрибуты события.

> **Примечание:**
>
> По умолчанию агрегирующий столбец **Атрибуты приемника** не отображается в таблице и находится в списке **Доступные поля**.

Цель:
Выбрать отображаемые атрибуты объектов перехвата.

Решение:

1. Перейдите в раздел **События**.
2. Выполните одно из следующих действий:
   - отредактируйте уже созданный запрос. Для этого нажмите **Редактировать запрос**;
   - создайте новый запрос.

   > **Примечание:**
   >
   > Доступны два способа создания запроса: в стандартном режиме и в расширенном режиме .

3. В правой части рабочей области перейдите на вкладку **Столбцы**.
4. Перенесите все целевые атрибуты в правое поле, а все нецелевые - в левое:
   - Щелчком левой кнопки мыши выделите запись в левом поле, чтобы перенести ее в правое поле;

- Щелчком левой кнопки мыши выделите запись в правом поле, чтобы перенести ее в левое поле.

5. Нажмите:
   - **Сохранить** - чтобы сохранить изменения;
   - **Сохранить и выполнить** - чтобы сохранить изменения и выполнить фильтрацию с учетом заданных параметров запроса.

Просмотр краткой формы события

Цель:
Просмотреть краткую информацию по объекту перехвата.

Решение:

1. Перейдите в раздел **События**.
2. Создайте запрос либо запустите выполнение ранее созданного запроса (см. "Создание запросов").
3. Нажмите на плитку события в списке (или строку события в таблице событий).
4. Просмотрите краткую информацию о событии в правой части рабочей области. В верхней части формы отображаются параметры события, в нижней части - содержимое события.

> **Примечание:**
>
> Вы можете настроить отображение данных в области просмотра содержимого события. По умолчанию содержимое события отображается в виде фрагментов, в которых подсвечены вхождения сработавших объектов защиты и результаты поиска по тексту события.

5. Чтобы просмотреть данные отправителя, получателя или компьютера, нажмите на требуемое значение. Отобразится карточка выбранной персоны или выбранного компьютера.
   При просмотре карточки вы можете:
   a. Назначить статус персоне/компьютеру. Для этого нажмите **Назначить статус**, в открывшемся окне выберите требуемые статусы и нажмите **Сохранить**.
   b. Просмотреть подробную информацию о персоне/компьютере в разделе "Персоны". Для этого нажмите **Профиль персоны** (для персоны) или **Перейти к компьютеру** (для компьютера).
   c. Просмотреть снимки экрана для персоны/компьютера (если снимки экрана в наличии, рядом с именем персоны отображается значок ). Для этого нажмите **Снимки экрана**. Откроется вкладка **Снимки экрана** для выбранной персоны или выбранного компьютера.

> **Примечание:**

При наличии снимков экрана, сделанных в течение часа до и после события, для персон отображается ссылка **Снимки экрана в момент события**. Если нажать на эту ссылку, снимки экрана, время создания которых максимально близко к событию, будут показаны в полноэкранном режиме просмотра.

6. Чтобы просмотреть информацию о сработавшей политике в разделе "Политики", нажмите на название политики.
7. Если событие содержит вложения, вы можете сохранить их на ваш компьютер. Для этого рядом с названием нужного вложения нажмите .
8. Для перехода к детальной форме просмотра события нажмите **Подробнее** в правом верхнем углу формы.

См. также:

- "Краткая форма просмотра события" - о форме просмотра общей информации о событии
- "Просмотр детальной формы события" - о просмотре подробной информации о событии
- "Просмотр снимков экрана" - о просмотре снимков экрана для персоны или компьютера

Просмотр детальной формы события

Цель:
Просмотреть детальную информацию по объекту перехвата.

Решение:

1. Перейдите в раздел **События**.
2. Создайте запрос либо запустите выполнение ранее созданного запроса (см. "Создание запросов").
3. Выделите плитку целевого события в списке (или строку события в таблице событий). В правой части рабочей области отобразится краткая форма просмотра события.
4. Для перехода к детальной форме просмотра нажмите **Подробнее**.
5. В открывшемся окне **Детальная информация о событии** просмотрите интересующую вас информацию. Информация о событии представлена в областях **Параметры события**, **Поиск по тексту**, **Объекты защиты** и **Содержимое события** (см. "Детальная форма просмотра событий").

   Примечание.

   Вы можете настроить отображение данных в области просмотра. По умолчанию содержимое событие отображается в виде фрагментов, в которых подсвечены вхождения сработавших объектов защиты и результаты поиска по тексту события.

6. При просмотре параметров события вы можете получить дополнительную информацию о персонах, компьютерах и политиках, участвующих в событии (см. "Просмотр краткой формы события", п. 5 и 6).
7. Для закрытия детальной формы просмотра нажмите  в правом верхнем углу окна.

См. также:

- "Детальная форма просмотра события" - о форме просмотра подробной информации о событии
- "Просмотр краткой формы события" - о просмотре общей информации о событии

4.6.3 Вынесение решения по объекту

Цель:
Вынести решение, является ли объект нарушением.

Решение:

1. Перейдите в раздел **События**.
2. Щелчком левой кнопки мыши выделите нужное событие в списке.
3. На панели инструментов в левой части рабочей области нажмите:
   - **Нарушение** - для событий, нарушающих политику корпоративной безопасности. При этом, если для события был назначен вердикт *Поместить на карантин*, то значение вердикта изменится на *Заблокировано*.
   - **Нет нарушения** - для событий, не являющихся нарушением политики корпоративной безопасности. При этом, если для события был назначен вердикт *Поместить на карантин*, то значение вердикта изменится на *Разрешено*.

     Важно!

     Если используется режим *Блокировка*, то SMTP-письма, перемещенные Системой в карантин, в результате принятия этого решения будут отправлены получателю, а отправитель письма получит уведомление. Подробнее см. "Досылка события, находящегося в карантине".

   - **Решение не принято** - если на данный момент пользователь не принял решение, нарушает ли событие политику корпоративной безопасности.
   - **Требуется дополнительная обработка** - если для принятия решения требуются дополнительные действия.

Пример

Офицер безопасности оценивает событие без нарушения, приходит к выводу, что в некоторых из них есть нарушения и выносит решение *Нарушение*. В БД такие события перемещаются в табличное пространство за день (ETП), которое содержит объекты с нарушениями. Эти данные могут пригодиться в будущем для проведения расследования. События хранятся в таком ETП дольше, чем в ETП с событиями без нарушений. Этот период можно установить вручную (подробнее см. документ "Traffic Monitor. Руководство администратора", раздел "Управление ежедневными табличными пространствами").

См. также:

- "Ретроспективный анализ данных, решение пользователя по объекту" - о вынесении пользовательского решения.

4.6.4 Добавление и удаление тега

Цель:
Добавить тег объекту перехвата.

Решение:

1. Перейдите в раздел **События**.
2. Щелчком левой кнопки мыши выделите целевое событие.
3. На панели инструментов для событий нажмите  **Установить тег**.
4. В открывшемся окне выберите требуемый тег, установив для него флажок.
5. Нажмите **Сохранить**.

Для удаления тега нажмите на крестик рядом с названием тега в плитке события.

См. также:

- "Теги" - об интерфейсе раздела Консоли управления, в котором ведется работа с тегами
- "Работа с тегами" - о порядке наполнения справочника тегов

4.6.5 Сохранение события (для SMTP-писем)

Цель:
Сохранить объект перехвата (SMTP-письмо).

Решение:

1. Перейдите в раздел **События**.
2. Щелчком левой кнопки мыши выделите целевое событие.
3. В краткой форме просмотра события, расположенной в правой части рабочей области, нажмите .
   Начнется скачивание файла. После окончания загрузки вы можете открыть файл события и просмотреть его содержимое.

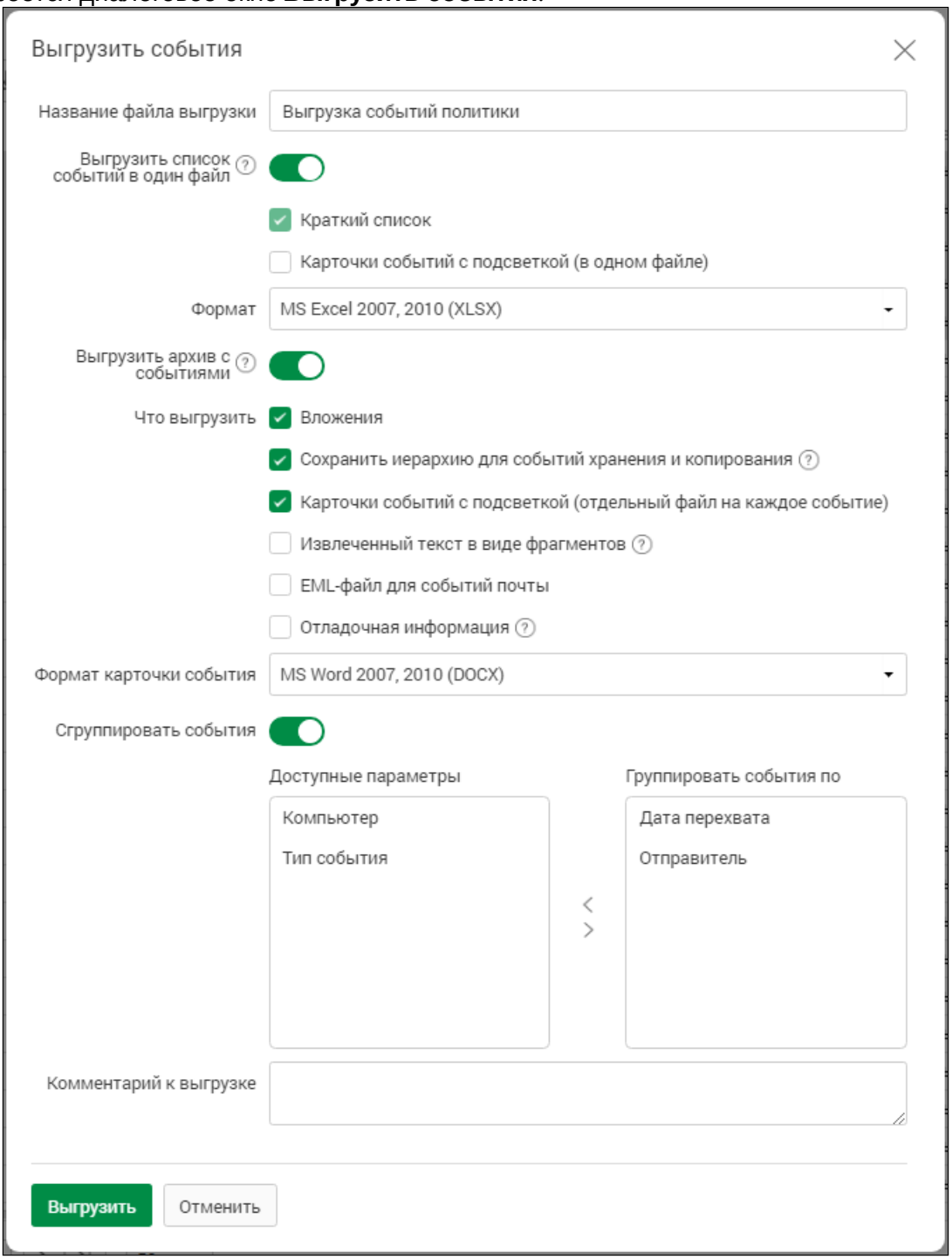
4.6.6 Выгрузка событий

Цель:
Сохранить информацию о событиях на диск компьютера.

Решение:

1. Зайдите в раздел **События**.
2. Выберите в списке запрос и выполните его либо создайте новый запрос (см. "Создание запросов").
3. Выделите в списке событие, которое вы хотите выгрузить. Чтобы выделить несколько событий, используйте клавиши **Shift** или **Ctrl**.

4. На панели инструментов нажмите  и раскрывшемся списке выберите **Выгрузить события** или **Выгрузить все события**.
   Откроется диалоговое окно **Выгрузить события**.



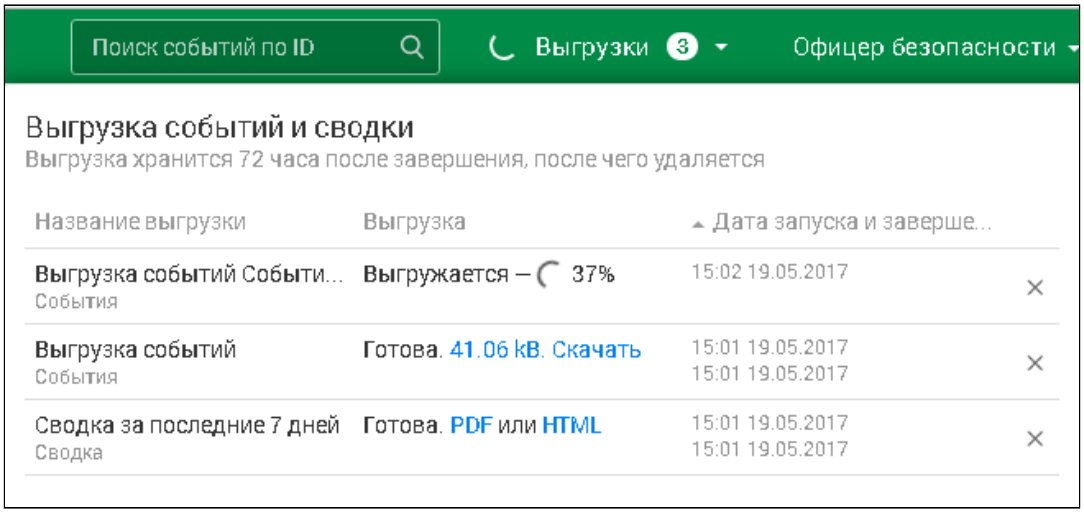
5. Если выбрано более одного события, укажите, в каком виде нужно выгрузить события (если выгружается только одно событие, перейдите к шагу 7).
   Вы можете выбрать один или оба варианта:
   - **Выгрузить список событий в один файл** - будет создан один файл, содержащий информацию по всем выгружаемым событиям;

- **Выгрузить архив с событиями** - будет создан архив, содержащий отдельные папки для каждого события.

6. Если выбрана настройка **Выгрузить список событий в один файл**:
   a. Укажите, в каком виде требуется создать список. Вы можете выбрать один или оба варианта:
      - **Краткий список** - для каждого события будет выгружен список основных параметров;
      - **Карточка события с подсветкой** - для каждого события будет выгружен список параметров события, а также текст события и текст, извлеченный из вложений, с подсветкой сработавших объектов защиты.
   b. Выберите формат выгрузки. Доступны следующие форматы:
      - MS Excel 2007, 2010 (XLSX) - недоступно, если выбран вид **Карточка события с подсветкой**;
      - MS Excel 2003 (XLS) - недоступно, если выбран вид **Карточка события с подсветкой**;
      - MS Word 2007, 2010 (DOCX);
      - Adobe Acrobat (PDF) - выгрузка ограничена 100 событий.
7. Если выбрана настройка **Выгрузить архив с событиями** или если выгрузка содержит только одно событие, укажите следующие настройки:
   - **Вложения** - будут выгружены исходные файлы вложений. Настройка по умолчанию отключена для экономии оперативной памяти системы;
   - **Сохранить иерархию для событий хранения и копирования** - отображается, если выбрана настройка **Вложения**. События, относящиеся к одному типу, будут сохраняться в папку "Внешнее устройство", "FTP" или "Data Discovery" в зависимости от типа события;
   - **Карточка события с подстветкой** - для события будет создан файл в формате DOCX, содержащий список параметров события, а также текст события и текст, извлеченный из вложений, с подсветкой сработавших объектов защиты;
   - **Извлеченный текст в виде фрагментов** - отображается, если выбрана настройка **Карточка события с подстветкой**. Текст, извлеченный из вложений, будет выгружен в виде фрагментов, содержащих сработавшие объекты защиты;
   - **EML-файл для событий почты** - будет выгружен EML-файл вида [ID события]_[Тема письма];
   - **Отладочная информация** - для каждого выгружаемого события в архив будет добавлена отладочная информация.
8. Если выбрана настройка **Выгрузить архив с событиями**, вы можете указать дополнительные настройки:
   - **Сгруппировать события** - выберите эту настройку, если требуется сгруппировать события в архиве, и добавьте требуемые параметры из поля **Доступные параметры** в поле **Группировать события по**. События могут быть сгруппированы по следующим параметрам: *Компьютер, Тип события, Дата перехвата, Отправитель.*
   - **Комментарий к выгрузке** - добавленный комментарий будет выгружен в корневую папку в формате DOCX.
9. После того как вы указали все необходимые параметры, нажмите **Создать**.

По завершении операции в правом верхнем углу появится уведомление. Чтобы просмотреть выгрузку, нажмите **Скачать** и сохраните данные на диске компьютера.

Вы можете получить информацию о ходе генерации выгрузки, нажав кнопку **Выгрузки** на панели навигации.



Для каждой выгрузки отображается ее название, статус, дата и время запуска. Для готовых выгрузок отображается также размер созданной выгрузки, дата и время завершения генерации и ссылка **Скачать**, позволяющая сохранить файл на компьютер.

Для выгрузок в процессе формирования отображается процент выполнения. Если вы хотите отменить генерацию выгрузки (например, если процесс занимает длительное время), нажмите ✕ в строке выбранной выгрузки. Создание выгрузки будет отменено.

Помимо выгрузок событий, в списке также отображается информация о созданных выгрузках сводки (см. "Просмотр выгрузки сводки").

Кнопка **Выгрузки** доступна из любого раздела Консоли управления.

4.6.7 Досылка события, находящегося в карантине

Справочная информация:
Если персона отправила SMTP-письмо, признанное потенциальным нарушением политики безопасности и перемещенное Системой в карантин (в Системе для SMTP-трафика применяется транспортный режим *Блокировка*), офицер безопасности может затем пересмотреть решение Системы и разрешить отправку письма. В этом случае будет выполнена досылка письма, а отправитель письма получит уведомление.

Цель:
Выполнить досылку письма, помещенного Системой в карантин.

Решение:

> **Важно!**
>
> Досылка письма возможна только для событий, имеющих вердикт *Карантин*. События с вердиктом *Заблокировано* дослать невозможно.

1. Перейдите в раздел **События**.
2. Щелчком левой кнопки мыши выделите целевое событие.
3. На панели инструментов в левой части рабочей области нажмите **Нет нарушения**.

См. также:

- "Ретроспективный анализ данных, решение пользователя по объекту" - о вынесении пользовательского решения;
- "Вынесение решения по объекту" - о действиях офицера безопасности по принятию возможных решений по объекту.

4.7 Настройка реакций Системы

Важно!

Чтобы изменения, описанные в данном разделе, отразились на работе Системы, примените конфигурацию: см. "Работа с конфигурацией Системы" и "Применение конфигурации Системы".

Справочная информация:
Реакции Системы - это действия, выполняемые Системой при обнаружении нарушений политики корпоративной безопасности. Эти действия задаются в правилах при создании политик защиты данных и политик контроля персон (см. "Раздел Политики"). Также в Системе имеются предустановленные политики (см. "Предустановленные политики").
В процессе работы Системы может возникнуть ситуация, когда подсистема анализа и принятия решений не может использовать политику: например, политика не создана или была удалена, при выполнении политики произошла ошибка. В этом случае объектам не назначается никаких атрибутов, а в детальной форме просмотра событий, в окне **Сообщения обработки**, отображаются сообщения о возникших в процессе обработки ошибках (см. "Детальная форма просмотра событий").

Для чего требуется настройка реакций Системы:
Для того чтобы при нарушении корпоративной политики безопасности (например, отправка конфиденциального документа за пределы компании) и нецелевом использовании рабочего времени (например, просмотр развлекательных интернет-сайтов с рабочего компьютера) Система:

- отправляла уведомления нарушителям, информировала офицера безопасности и других заинтересованных лиц;
- назначала вердикт объекту перехвата;
- присваивала объекту перехвата уровень нарушения, теги и статусы.

Настройка реакций Системы включает:

Действие	Описание
Создание политик защиты данных	Политика защиты данных представляет собой набор правил передачи, копирования, хранения и буфера обмена. Позволяет указать данные, действия с которыми могут приводить к срабатыванию правил политики.
Создание политик защиты данных на агентах	Политика защиты данных на агентах представляет собой набор правил передачи и копирования, применяющих непостредственно на агентах Device Monitor.

Действие	Описание
	Позволяет указать данные, действия с которыми могут приводить к срабатыванию правил политики.
Создание политик контроля персон	Позволяет указать список контролируемых персон, действия которых могут приводить к срабатыванию правил политики.
Создание правил	Определение, что является нарушением правила политики, и какие действия необходимо выполнить в случае нарушения
Настройка уведомлений в правилах	При срабатывании правила Система отправляет уведомление указанным получателям

Примечание.

При наличии большого числа политик в Консоли управления вы можете отфильтровать список политик по заданным критериям (подробнее см. "Фильтрация списка политик").

См. также:

- "Раздел Политики" - о разделе, в котором ведется работа с политиками

4.7.1 Общие сведения о политиках

В этом разделе описано применение настроенных политик Системы (т.е. совокупностей правил, в соответствии с которыми проводится анализ и обработка объектов) к событиям (объектам перехвата сетевого трафика).

Политики в Системе делятся на три группы:

- Политики защиты данных - позволяют настроить правила передачи, копирования, хранения и буфера обмена, имеют возможность работать с пользовательскими атрибутами.
- Политики защиты данных на агентах - позволяют настроить правила передачи и копирования, которые будут применяться непосредственно на агентах Device Monitor.
- Политики контроля персон - позволяют настроить правила для отслеживания действия отдельных персон и их групп.

Система применяет политики к событиям в следующем порядке:

1. Событие по очереди проверяется на соответствие всем активным политикам защиты данных на агентах.
2. Если политика сработала на событии, рассматриваются суб-события.
3. Для каждого суб-события отбираются правила, которым они соответствуют (которые срабатывают на данное суб-событие).
4. Правила, которые сработали, разделяются на суб-правила.

5. Из суб-правил, соответствующих событию, выбираются самые приоритетные.
6. К объекту перехвата применяются действия, заданные в сработавших суб-правилах самого высокого приоритета.
7. Если остались суб-события, которым не соответствует ни одно правило, выполняются действия по умолчанию (в случае, если они указаны для данного типа правил).

После этого шаги 2-7 повторяются для всех активных политик защиты данных и затем - для всех активных политик контроля персон.

Подробнее о процессах, происходящих при этом:

1. Разбиение события на суб-события
2. Разбиение правил на суб-правила и выбор подходящих суб-правил
3. Определение приоритетного суб-правила
4. Порядок применения действий согласно отобранным приоритетным правилам

Также в статье приведен пример применения политики.

1. Разбиение события на суб-события

В процессе обработки события Система разбивает событие на суб-события:

1. Для событий, относящихся к правилам передачи: по паре ключей "Отправитель" - "Получатель".
2. Для событий, относящихся к правилам копирования: по ключу "Отправитель".
3. Для событий, относящихся к правилам буфера обмена: по ключу "Персоны".
4. Для событий, относящихся к правилам хранения: по паре ключей "Владелец файла" - "Кому доступен файл".

Если какой-либо ключ получил несколько значений (например, несколько получателей SMTP-письма), то Система рассматривает это событие как совокупность нескольких суб-событий с уникальными значениями ключей.
Например, если перехваченное событие имеет следующие атрибуты:

Отправитель	Получатель	Тип события	Время
Персона: Иванов, Персона: Петров	Персона: Сидоров, Персона: Петров, Персона: Иванов	Skype	09:23

то оно подразделяется на следующие суб-события:

Отправитель	Получатель	Тип события	Время
Персона: Иванов	Персона: Сидоров	Skype	09:23
Персона: Иванов	Персона: Петров	Skype	09:23
Персона: Иванов	Персона: Иванов	Skype	09:23
Персона: Петров	Персона: Сидоров	Skype	09:23
Персона: Петров	Персона: Петров	Skype	09:23
Персона: Петров	Персона: Иванов	Skype	09:23

2. Разбиение правил на суб-правила и выбор подходящих суб-правил

Каждое правило действующей политики разбивается на суб-правила по следующим ключам:

1. Для правил передачи: по паре ключей "Отправитель" - "Получатель".

> **Примечание.**
>
> Если параметр **Направление маршрута** имеет значение "В обе стороны", то будет добавлена пара ключей: "Получатель" - "Отправитель".

2. Для правил копирования: по ключу "Отправитель".
3. Для правил буфера обмена: по ключу "Персоны".
4. Для правил хранения: по паре ключей "Владелец файла" - "Кому доступен файл".

Например, правила:

Отправитель	Направление	Получатель	Тип события	Время	Реакция
Группа: Юристы, Персона: Иванов, Персона: Петров	->	Группа: Маркетинг, Персона: Сидоров	Почта на Клиенте	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Группа: Логистики	->	Группа: Продаж, Группа: Доставки	Skype	10:00-19:00	Уведомить: Петрова, Уровень нарушения: Средний
Группа: Финансисты	-> <-	Группа: Юристы, Группа: Продаж			Уведомить: Белова, Уровень нарушения: Высокий

будут разбиты на следующие суб-правила:

Отправитель	Направление	Получатель	Тип события	Время	Реакция
Группа: Юристы	->	Группа: Маркетинг	Почта на Клиенте	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Группа: Юристы	->	Персона: Сидоров	Почта на Клиенте	08:00-20:00	Уведомить: Викторова, Уровень

Отправитель	Направление	Получатель	Тип события	Время	Реакция
					нарушения: Низкий
Персона: Иванов	->	Группа: Маркетинг	Почта на Клиенте	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Иванов	->	Персона: Сидоров	Почта на Клиенте	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Петров	->	Группа: Маркетинг	Почта на Клиенте	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Петров	->	Персона: Сидоров	Почта на Клиенте	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Группа: Логистики	->	Группа: Продаж	Skype	10:00-19:00	Уведомить: Петрова, Уровень нарушения: Средний
Группа: Логистики	->	Группа: Доставки	Skype	10:00-19:00	Уведомить: Петрова, Уровень нарушения: Средний
Группа: Финансисты	->	Группа: Юристы			Уведомить: Белова, Уровень нарушения: Высокий
Группа: Финансисты	->	Группа: Продаж			Уведомить: Белова, Уровень

Отправитель	Направление	Получатель	Тип события	Время	Реакция
					нарушения: Высокий
Группа: Юристы	->	Группа: Финансисты			Уведомить: Белова, Уровень нарушения: Высокий
Группа: Продаж	->	Группа: Финансисты			Уведомить: Белова, Уровень нарушения: Высокий

Далее для каждого суб-события отбираются подходящие ему по условиям суб-правила (подробнее об атрибутах правил см. "Правило передачи", "Правило копирования", "Правило хранения" и "Правило работы в приложениях").

3. Определение приоритетного суб-правила

Из суб-правил, соответствующих суб-событию, выбирается суб-правило, имеющее наибольший вес. Вес суб-правила определяется суммой весов совпавших условий в соответствии с таблицей:

Отправитель/Получатель	Вес (при включении атрибута)	Вес (при отрицании атрибута)
Контакт	10000	3
Персона	5000	7
Группа	2500	15
Домен	1250	35
URL	600	75
Список ресурсов	300	150
Периметр (для политик защиты данных)	Минимальный вес элемента, входящего в периметр	Максимальный вес элемента, входящего в периметр
Периметр (для политик защиты данных на агенте)	300	150
ID устройства	50	25

Отправитель/Получатель	Вес (при включении атрибута)	Вес (при отрицании атрибута)
Адрес облачного хранилища	50	не применимо
Адрес и путь к файлу	20	10
Имя устройства	10	5
Тип источника/приемника	1	не применимо
Место хранения	1,25	0,25
Компьютер	1,25	не применимо
Приложение-источник / Приложение-приемник	0,415	0,1
Терминальная сессия = Включено	0,83	не применимо
День недели	0,15	не применимо
Время (часы действия правила)	0,15	не применимо
Тип события	0,1	не применимо
Пользовательский атрибут	1	0,5
Если не заполнен атрибут: ▪ Отправитель (для правил передачи и копирования) ▪ Получатель (для правил передачи) ▪ Персона (для правил работы в приложениях, файловых операций) ▪ Владелец файла/кому доступен файл (для правил хранения)	1	не применимо
Если не заполнен атрибут: ▪ Тип события (для всех правил) ▪ День недели (для правил передачи, копирования, работы в приложениях)	0	не применимо

Отправитель/Получатель	Вес (при включении атрибута)	Вес (при отрицании атрибута)
▪ Время (для правил передачи, копирования, работы в приложениях) ▪ Компьютер (для правил передачи, копирования, работы в приложениях, файловых операций) ▪ Место хранения (для правил хранения) ▪ Терминальная сессия (для правил работы в приложениях) ▪ Приложение-источник / Прил ожение-приемник (для правил работы в приложениях, файловых операций) ▪ Источник копирования / Приемник копирования (для правил копирования) ▪ Пользовательский атрибут		

Например, правило с условием на пересылку от любого отправителя - определенному контакту (10000 + 1=10001) является более приоритетным, чем правило с условием на пересылку от определенной персоны - группе персон (5000 + 2500 = 7500).
Если для одного суб-события есть более одного суб-правила, имеющих одинаковый вес, то отбираются несколько самых приоритетных правил с одинаковым приоритетом.
Если суб-событию не соответствует ни одно правило, то выполняются действия по умолчанию (см. "Определение действий Системы по умолчанию").

4. Порядок применения действий согласно отобранным приоритетным правилам

Система назначает реакцию, выполняя действия из отобранных приоритетных правил, в следующем порядке:

1. Если выбрана настройка **Удалить событие**, то указанные в правиле действия не выполняются и событие не сохраняется в базу данных.
2. Событию назначается вердикт с наиболее высоким приоритетом из указанных в отобранных правилах. Вердикты имеют следующие приоритеты:
   - вердикт **Заблокировать** - приоритет 2;
   - вердикт **Поместить на карантин** - приоритет 1;
   - вердикт **Разрешить** - приоритет 0.

> **Примечание:**
>
> Вердикт, назначенный событию в результате применения политики защиты данных на агентах, не заменяется на вердикт, указанных в правилах политики защиты данных и политики контроля персон.

Вердикт, назначенный событию в результате применения политики защиты данных, не заменяется на вердикт, указанных в правилах политики контроля персон.

3. Событию назначается наиболее высокий уровень нарушения из указанных в отобранных правилах.
4. К тегам события добавляются теги, указанные в отобранных правилах.
5. Для проиденфицированных отправителей к имеющимся статусам добавляются статусы, указанные в отобранных правилах.
6. Уведомляются персоны, указанные в отобранных правилах.

Пример:

Пусть в Системе заданы две политики:

Политика №1					
Каталог объектов защиты: Бухгалтерия					
Номер правила	Отправитель	Получатель	Время	**Тип события**	Реакция
1.1	Группа: Отдел продаж	Группа: Отдел Бухгалтерия	08:00 – 20:00	Почта на Клиенте	Нарушение: Отсутствует
1.2	Иванов	Группа: Отдел Бухгалтерия		Почта на Клиенте	Нарушение: Отсутствует
1.3	Иванов	<> Периметр: Компании			Нарушение: Средние
1.4	По умолчанию:				Нарушение: Высокое
Политика №2					
Каталог объектов защиты: Договорная					
Номер правила	Отправитель	Получатель	Время	**Тип события**	Реакция
2.1	Группа: Отдел продаж	<> Периметр: Компании	08:00 – 20:00	Почта на Клиенте	Нарушение: Отсутствует
2.2	Иванов	<> Периметр: Компании		Почта на Клиенте	Нарушение: Отсутствует

Политика №2					
Каталог объектов защиты: Договорная					
Номер правила	Отправитель	Получатель	Время	**Тип события**	Реакция
2.3	По умолчанию:				Нарушение: Отсутствует

Пусть Иванов входит в группу "*Отдел Продаж*". Петров входит в группу "*Отдел Бухгалтерия*". E-mail `sidorov@mail.com` находится за периметром компании.
Пусть есть событие:

Данные	Отправитель	Получатель	Время	**Тип события**
Группа объектов защиты: Бухгалтерия, Договорная	Иванов	Петров, sidorov@mail.com	19:00	Почта на Клиенте

Это событие состоит из двух суб-событий, различающихся парами "отправитель-получатель": "Иванов->Петров" и "Иванов->sidorov@mail.com".

1. Проверка на соответствие политике №1.

Событие соответствует политике №1, так как в событии содержится *Группа объектов защиты - Бухгалтерия*.
Рассматривается суб-событие "Иванов->Петров":

Отправитель	Получатель	Время	**Тип события**
Иванов	Петров	19:00	Почта на Клиенте

Этому суб-событию соответствует два суб-правила: №1.1 и 1.2. Из них более приоритетным является суб-правило №1.2. Следовательно, отбирается правило №1.2
Рассматривается суб-событие "Иванов->sidorov@mail.com":

Отправитель	Получатель	Время	**Тип события**
Иванов	sidorov@mail.com	19:00	Почта на Клиенте

Этому суб-событию соответствует только суб-правило №1.3. Следовательно, отбирается правило №1.3

2. Проверка на соответствие политике №2.

Событие соответствует политике №2, так как в событии содержится *Группа объектов защиты - Договорная*
Рассматривается суб-событие "Иванов->Петров":

Отправитель	Получатель	Время	**Тип события**
Иванов	Петров	19:00	Почта на Клиенте

Этому суб-событию соответствует только суб-правило №2.3. Следовательно, отбирается правило №2.3
Рассматривается суб-событие "Иванов->sidorov@mail.com":

Отправитель	Получатель	Время	**Тип события**
Иванов	sidorov@mail.com	19:00	Почта на Клиенте

Этому суб-событию соответствует два суб-правила: №2.1 и 2.2. Из них более приоритетным является суб-правило №2.2. Следовательно, отбирается правило №2.2

3. Применяются отобранные действия: №1.2, №1.3, № 2.3, №2.2

4.7.2 Предустановленные политики

В Системе предустановлены следующие политики:

- Политики защиты конфиденциальных данных
- Политика контроля персон
- Политика, регулирующая передачу данных, защищенных паролем
- Политика, контролирующая посещение веб-ресурсов сотрудниками компании
- Политика, исключающая из перехвата почтовые рассылки

> **Примечание.**
>
> При удалении схемы БД (см. "*Infowatch Traffic Monitor. Руководство по установке*", статья "Удаление схемы базы данных") из Системы также удаляются политики, в том числе предустановленные.
>
> Для повторного распространения предустановленных политик выполните следующие действия:
>
> 1. Создайте файл **/opt/iw/tm5/www/backend/protected/runtime/first_run** от имени пользователя **iwtm**;
> 2. Перезапустите процесс **iw_kicker**:
>
> ```
> iwtm restart kicker
> ```
>
> Остальные политики требуется создать повторно (см. "Создание политики защиты данных", "Создание политики защиты данных на агентах" и "Создание политики контроля персон").

Политики защиты конфиденциальных данных

По умолчанию в Системе создается по одной политике защиты данных для каждого предустановленного каталога объектов защиты (список предустановленных каталогов приведен в статье "Раздел "Объекты защиты"):

Предустановленные политики имеют следующие значения атрибутов:

Атрибут	**Значение**
Название политики	<Название каталога объектов защиты>
Статус	Активная
Период действия	Не ограничен

Атрибут	Значение
Защищаемые данные	Каталог <Название каталога объектов защиты>

где <Название каталога объектов защиты> - название того каталога, для которого создается политика.

Каждая политика содержит следующие правила:

Правила передачи

1. *Правило, регулирующее передачу конфиденциальных данных за периметр компании*.
   Если персона передает трафик любого типа за периметр компании в любой из дней недели,
   То Система выполнит следующие действия:
   - установит значение *Разрешено* атрибуту события *Вердикт*;
   - установит одно из значений атрибуту события *Уровень нарушения*:
     - *Высокий* - для каталогов объектов защиты*:* Грифованная информация, Персональные данные;
     - *Низкий* - для каталогов объектов защиты: Юридическая информация, Отдел кадров, IT-служба, Внешнеэкономическая деятельность;
     - *Средний* - для всех остальных каталогов объектов защиты;
   - установит значение *Не назначать* атрибуту персоны-отправителя *Статус*.
2. *Правило, регулирующее передачу конфиденциальных данных руководством компании*.
   Если персон из группы VIP передает трафик любого типа любому получателю в любой из дней недели,
   То Система выполнит следующие действия:
   - установит значение *Разрешено* атрибуту события *Вердикт*;
   - установит значение *Отсутствует* атрибуту события *Уровень нарушения*;
   - установит событию тег *VIP*.

Правила копирования

Правило, регулирующее копирование конфиденциальной информации на съемные устройства.

Если персона копирует конфиденциальные данные на съемное устройство (в том числе через терминальную сессию), облачные хранилища, а также используя протокол FTP, в любой из дней недели,
То Система выполнит следующие действия:

- установит одно из значений атрибуту события *Уровень нарушения*:
  - *Высокий - для* каталогов объектов защиты*:* Грифованная информация, Персональные данные;
  - *Низкий* - для каталогов объектов защиты: Юридическая информация, Отдел кадров, IT-служба, Внешнеэкономическая деятельность;
  - *Средний* - для всех остальных каталогов объектов защиты;
- установит значение *Не назначать* атрибуту персоны-отправителя *Статус.*

Правила хранения

Правило, регулирующее хранение конфиденциальной информации. Добавляется только для политик, где в качестве защищаемых данных указан каталог объектов защиты "Грифованная информация" или "Персональные данные".

Если персона хранит защищаемые данные в любом месте,
То Система выполнит следующие действия по умолчанию:

- установит значение *Высокий* атрибута события *Уровень нарушения;*

- установит значение *Не назначать* атрибуту персоны-владельца *Статус.*

Политика контроля персон

По умолчанию в Системе установлена политика контроля персон, имеющая следующие значения атрибутов:

Атрибут	Значение
Название политики	Персоны под наблюдением
Статус	Активная
Период действия	Не ограничен
Статусы	Под наблюдением

Правила политики

Правило, регулирующее передачу данных персоной, имеющей статус Под наблюдением.

Если персона, имеющая статус *Под наблюдением*, передает трафик любого типа любому получателю,
То Система установит:

- значение *Разрешить* атрибуту события *Вердикт;*
- значение *На рассмотрение* атрибуту события *Тэг*.

Политика, регулирующая передачу данных, защищенных паролем

По умолчанию в Системе установлена политика, регулирующая передачу данных, защищенных паролем.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Данные, защищенные паролем
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Зашифрованные файлы всех файловых форматов

Правила политики

Правило, регулирующее передачу данных, защищенных паролем, за периметр компании.

Если персона передает трафик любого типа за периметр компании в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;

- установит значение *Средний* атрибуту события *Уровень нарушения*;
- установит событию тег *На рассмотрение*.

Политики, контролирующие посещение веб-ресурсов

По умолчанию в Системе установлены следующие политики защиты данных, контроллирующие посещение веб-ресурсов сотрудниками компании:

- Социальные сети
- Нелояльные сотрудники
- Скрытые действия сотрудников
- Подозрительная активность

Социальные сети

По умолчанию в Системе установлена политика, контролирующая посещение развлекательных ресурсов сотрудниками компании.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Социальные сети
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Любые данные

Правила политики

Правило передачи, контролирующее отправку запросов на развлекательные ресурсы.

Если персона отправляет запрос на веб-ресурс, входящий в группу "Социальные сети" (подробнее см. "Веб-ресурсы") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Низкий* атрибуту события *Уровень нарушения.*

Нелояльные сотрудники

По умолчанию в Системе установлена политика, предназначенная для отслеживания действий нелояльных сотрудников.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных

Атрибут	Значение
Название политики	Нелояльные сотрудники
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Любые данные

Правила политики

Правило передачи, контроллирующее отправку запросов на сайты, связанные с поиском работы.

Если персона отправляет запрос на веб-ресурс, входящий в группу "Поиск работы" (подробнее см. "Веб-ресурсы") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Низкий* атрибуту события *Уровень нарушения.*

Скрытие действий сотрудников

По умолчанию в Системе установлена политика, позволяющая отслеживать скрытие сотрудниками своих действий и попытки обойти ограничения доступа к веб-ресурсам.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Скрытие действий сотрудников
Статус	Неактивная
Период действия	Не ограничен
Защищаемые данные	Любые данные

Правила политики

Правило передачи, контролирующее отправку запросов на веб-анонимайзеры.

Если персона отправляет запрос на веб-ресурс, входящий в группы "Анонимайзеры" (подробнее см. "Веб-ресурсы") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Низкий* атрибуту события *Уровень нарушения.*

Подозрительная активность

По умолчанию в Системе установлена политика, контролирующая подозрительную активность сотрудников в интернете.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Подозрительная активность
Статус	Неактивная
Период действия	Не ограничен
Защищаемые данные	Любые данные

Правила политики

Правило передачи, контролирующее отправку запросов на потенциально опасные ресурсы.

Если персона отправляет запрос на веб-ресурс, входящий в группы "Потенциально опасные ресурсы", "Сайты агрессивной направленности", "Тематика для взрослых" (подробнее см. "Веб-ресурсы") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Низкий* атрибуту события *Уровень нарушения;*
- установит событию тег *На рассмотрение*.

Политика, исключающая из перехвата почтовые рассылки

В Системе установлена политика, позволяющая исключить из перехвата почтовые рассылки.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Исключить из перехвата
Статус	Отключена
Период действия	Не ограничен
Защищаемые данные	Любые данные

Правила политики

Правило, регулирующее передачу данных персонами, входящими в периметр Исключить из перехвата

Если персона, находящаяся в периметре *Исключить из перехвата* (см. "Периметры"), отправляет данные любому получателю в любой день недели,
То Система удаляет это событие.

4.7.3 Создание политики защиты данных

Цель:
Создать политику, определяющую реакцию Системы на действия с данными.

Решение:

1. Перейдите в раздел **Политики**.
2. В верхней части рабочей области нажмите **Добавить политику** и в раскрывающемся списке выберите **Политика защиты данных**.
   Новая политика будет добавлена в группу **Политики защиты данных**, а в правой части рабочей области отобразится форма добавления политики.
3. Укажите атрибуты политики:
   - Название;
   - Описание;
   - Статус;
   - Период действия.

   > **Важно!**
   >
   > При заполнении атрибута **Период действия** учитывайте возможную разницу часовых поясов между филиалами вашей организации. Временем перехвата события считается локальное время на сервере, выполняющем перехват. В случае, если локальное время перехвата события не попадает в указанный интервал, то политика к данному событию применяться не будет.

4. Чтобы добавить в политику защищаемые данные, нажмите кнопку **Выбрать**.

   > **Примечание.**
   >
   > Если защищаемые данные не выбраны, созданная политика будет применяться к любым данным.

5. В открывшемся окне установите флажки напротив элементов, которые вы хотите добавить. Защищаемые данные могут включать объекты защиты, их каталоги, а также файловые форматы. Для файловых форматов вы можете дополнительно указать размер (в байтах), а также следующие признаки:
   - зашифрованные;
   - склеенные;
   - несоответствие сигнатуры и расширения файла.

Важно!

Если для политики указаны защищаемые данные нескольких типов, то для срабатывания правил политики (см. "Правила и форма их просмотра") необходимо, чтобы для события были обнаружены нарушения хотя бы по одному объекту каждого из указанных типов.
Например, если в качестве защищаемых данных указаны каталог объектов защиты, несколько файловых форматов и несколько признаков, то для срабатывания политики необходимо, чтобы в перехваченных данных содержался как минимум один объект защиты из указанного каталога, хотя бы один из указанных файловых форматов и все указанные признаки.

6. После того как вы выбрали защищаемые данные, нажмите **Сохранить**.
7. Добавьте в политику правила (см. "Создание правил").
8. Чтобы сохранить новую политику, на форме создания политики нажмите **Сохранить**.

Чтобы отредактировать политику:

1. Выделите нужную политику в списке.
2. На форме в правой части рабочей области отредактируйте требуемые параметры.
3. Чтобы изменить список защищаемых данных, в блоке **Защищаемые данные** нажмите **Выбрать** и отредактируйте список, после чего нажмите **Сохранить**.
4. Нажмите **Сохранить** на форме редактирования политики.

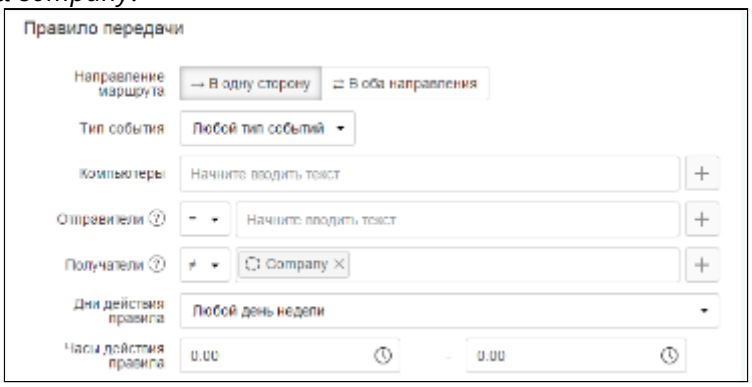
Чтобы удалить политику, нажмите ✖ в правом верхнем углу плитки политики и в открывшемся окне подтвердите удаление.

См. также: "Примеры использования политики защиты данных".

Примеры использования политики защиты данных

Пример 1:
Требуется контролировать передачу устава компании за пределы компании, в том числе отправку документа по электронной почте и копирование на съемные носители. Для этого:

1. Создайте политику защиты данных "Защита передачи устава организации".
2. В качестве защищаемых данных укажите объект защиты "Устав организации".
3. Добавьте правило передачи, контролирующее передачу данных любым получателям, кроме периметра *Company*.



4. Укажите действия при срабатывании правила (например, назначить событию низкий уровень нарушения).

5. Если требуется дополнительно контролировать сотрудников под наблюдением, добавьте еще одно правило передачи и укажите в качестве отправителей группу "Сотрудники под подозрением" (см. "Создание группы персон и компьютеров").
6. Укажите действия при срабатывании правила (например, назначить событию средний уровень нарушения и тег *На рассмотрение*).
7. Для контроля копирования документа на съемный носитель добавьте в политику правило копирования.

Теперь при отправке сообщения, в теле или вложении которого содержится информация, относящаяся к объекту защиты "Устав организации" за пределы периметра "*Company*", а также при копировании файла с информацией по данному объекту защиты на съемный носитель Система будет определять нарушение политики защиты данных.

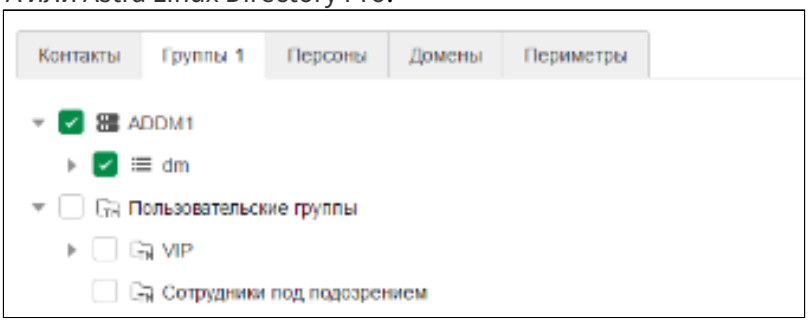
Пример 2:

Требуется выявить сотрудников, посещающих сайты по поиску работы. Для этого:

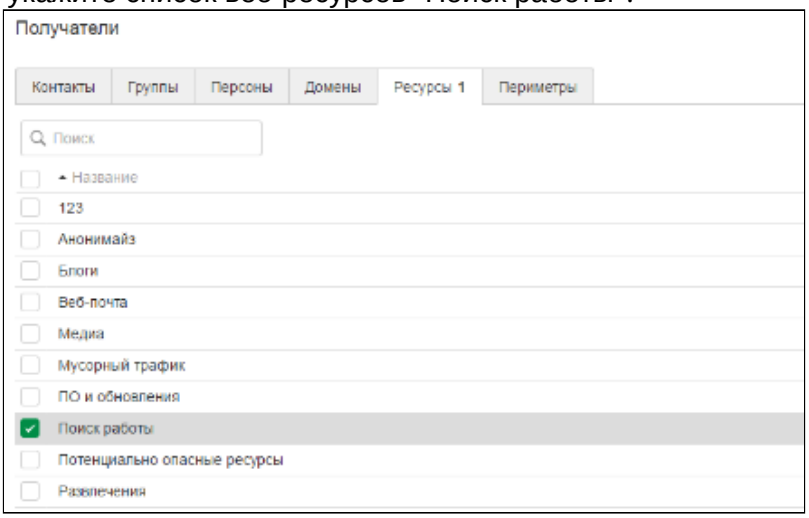
1. Создайте политику защиты данных "Выявление нелояльных сотрудников".

> **Совет.**
>
> Добавьте описание политики, чтобы легче идентифицировать ее в списке политик. Например, "Выявление сотрудников, отправляющих запросы на сайты по поиску работы".

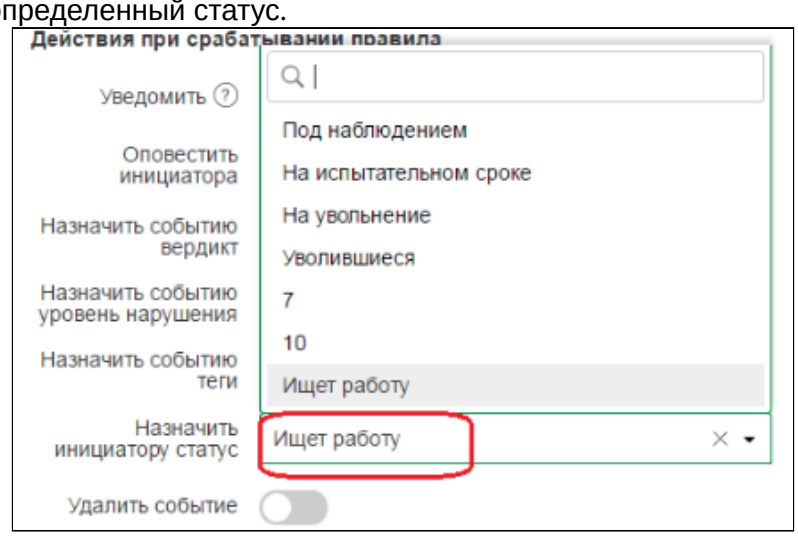
2. Добавьте правило передачи и укажите в качестве отправителей группу сотрудников компании, импортированную из Active Directory, Samba DC, Domino Directory, Astra Linux Directory, FreeIPA или Astra Linux Directory Pro.



3. В получателях укажите список веб-ресурсов "Поиск работы".



4. Укажите действия при срабатывании правила. Например, вы можете назначать отправителю определенный статус.



5. Сохраните правило и примените изменения конфигурации.

Теперь при отправке запроса на сайт по поиску работы, Система будет назначать отправителю статус "Ищет работу".

При необходимости вы сможете найти все такие события, создав запрос и указав один из следующих параметров поиска:

- политика "Выявление нелояльных сотрудников";
- отправители со статусом "Ищет работу".

Пример 3:
Требуется выявлять сотрудников, которые общаются с нежелательными адресатами - уволенными сотрудниками, конкурентами и т.д.

Для этого нужно создать периметр, в который будут входить уволенные сотрудники, конкуренты и т.д., после чего создать политику защиты данных, контролирующую передачу данных в данный периметр.

> **Примечание.**
>
> Вы можете добавить отдельные контакты персон или создать пользовательские группы, например, "Уволенные сотрудники" и "Конкуренты". Далее в примере рассматривается создание периметра на основе пользовательских групп.

Выполните следующие шаги:

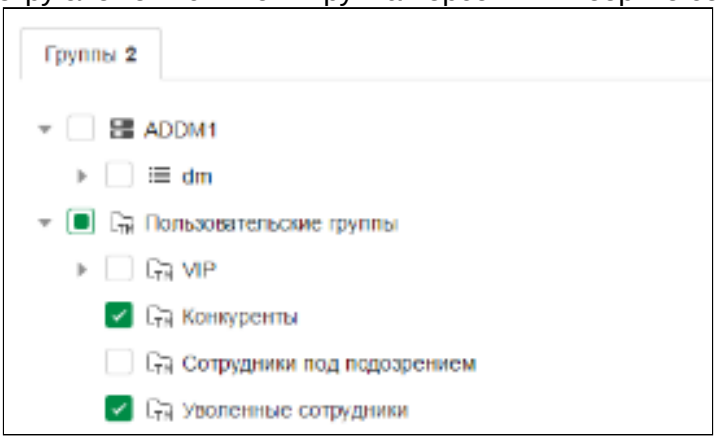
1. Создайте группу "Уволенные сотрудники" и наполните ее одним из следующих способов:
   - создайте карточки уволенных сотрудников вручную;
   - импортируйте персон из Active Directory, Samba DC, Domino Directory, Astra Linux Directory, FreeIPA или Astra Linux Directory Pro (если карточки персон не удаляются из службы каталогов при увольнении).
2. Создайте группу "Конкуренты" и наполните ее одним из следующих способов:
   - создайте в группе отдельную карточку для каждой персоны, например, Иван Петров из компании "Новая компания";

- создайте по одной карточке на каждую компанию-конкурента и добавьте в нее контакты сотрудников компании.

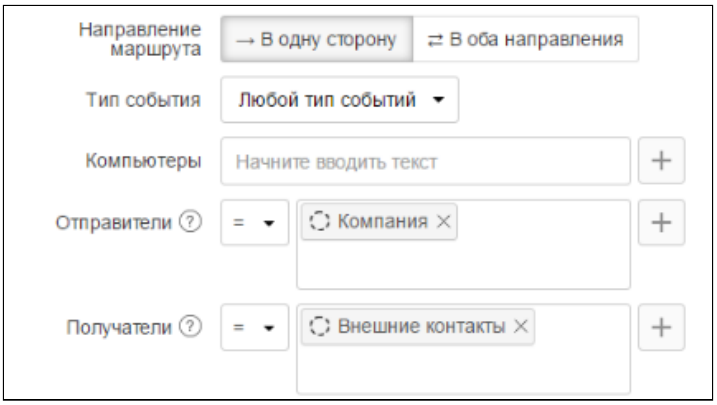
3. При необходимости создайте группы для других нежелательных адресатов.
4. Создайте периметр, который будет включать созданные группы, например, периметр "Внешние контакты".

> **Примечание.**
>
> При необходимости вы можете создать несколько периметров.

5. Добавьте к периметру элемент с типом "Группа персон" и выберите созданные группы.



6. Создайте политику "Выявление нежелательных адресатов" и добавьте в нее правило передачи.



7. Укажите действия при срабатывании правила, например, назначить событию средний уровень нарушения.
8. Примените конфигурацию, чтобы настроенная политика начала действовать.

Теперь в случае отправки письма на адреса уволенных сотрудников или конкурентов Система будет определять нарушение данной политики.

При необходимости вы сможете найти все такие события, создав запрос и указав в параметрах поиска политику "Выявление нежелательных адресатов".

4.7.4 Создание политики защиты данных на агентах

Цель:

Создать политику, определяющую реакцию Системы на действия с данными и применяющуюся непосредственно на агентах Device Monitor. Такая политика позволяет оперативно предотвращать утечки данных на компьютерах, где установлен агент Device Monitor.

> **Примечание:**
>
> На Агентах Device Monitor, установленных на рабочих станциях под управлением ОС Astra Linux или РЕД ОС, политики защиты данных на агентах не поддерживаются.

Решение:

1. Перейдите в раздел **Политики**.
2. В верхней части рабочей области нажмите **Добавить политику** и в раскрывающемся списке выберите **Политика защиты данных на агентах**.
   Новая политика будет добавлена в группу **Политики защиты данных на агентах**, а в правой части рабочей области отобразится форма добавления политики.
3. Укажите атрибуты политики:
   - Название;
   - Описание;
   - Статус;
   - Период действия.

   > **Важно!**
   >
   > При заполнении атрибута **Период действия** учитывайте возможную разницу часовых поясов между филиалами вашей организации. Временем перехвата события считается локальное время на агенте Device Monitor, где осуществляется перехват. В случае, если локальное время перехвата события не попадает в указанный интервал, то политика к данному событию применяться не будет.

4. Чтобы добавить в политику защищаемые данные, нажмите кнопку **Выбрать**.

   > **Примечание.**
   >
   > Если защищаемые данные не выбраны, созданная политика будет применяться к любым данным.

5. В открывшемся окне **Выбор защищаемых данных** установите флажки напротив требуемых значений. Защищаемые данные могут включать:
   - **Объекты защиты**
     Для выбора доступны объекты защиты, в составе которых есть только категории и текстовые объекты, и в которых не включено отрицание или детектирование в пределах элемента события.
   - **Каталоги объектов защиты**
     В выбранных каталогах будут использоваться только объекты защиты, созданные на основе категорий и текстовых объектов, и в которых не включено отрицание или детектирование в пределах элемента события.
   - **Файловые форматы**
     Для файловых форматов вы можете дополнительно установить ограничение на

размер файла (в байтах), а также указать, должна ли политика срабатывать для всех файлов либо в соответствии со следующими признаками файлов:

- зашифрованные;
- несоответствие сигнатуры и расширения файла.
  Если выбран признак **Зашифрованные**, политика срабатывает в случае, когда файл зашифрован или не удается определить формат данных.

> **Важно!**
>
> Если для политики указаны защищаемые данные нескольких типов, то для срабатывания правил политики (см. "Правила и форма их просмотра") необходимо, чтобы для события были обнаружены нарушения хотя бы по одному объекту каждого из указанных типов.
>
> Например, если в качестве защищаемых данных указаны каталог объектов защиты и несколько файловых форматов, то для срабатывания политики необходимо, чтобы в перехваченных данных содержался как минимум один объект защиты из указанного каталога и хотя бы один из указанных файловых форматов.

6. После того как вы выбрали защищаемые данные, нажмите **Сохранить**.
7. Добавьте в политику правила (см. "Создание правил").
8. Чтобы сохранить новую политику, на форме создания политики нажмите **Сохранить**.

Чтобы отредактировать политику:

1. Выделите нужную политику в списке.
2. На форме в правой части рабочей области отредактируйте требуемые параметры.
3. Чтобы изменить список защищаемых данных, в блоке **Защищаемые данные** нажмите **Выбрать** и отредактируйте список, после чего нажмите **Сохранить**.
4. Нажмите **Сохранить** на форме редактирования политики.

Чтобы удалить политику, нажмите ✖ в правом верхнем углу плитки политики и в открывшемся окне подтвердите удаление.

Пример 1:

Требуется, чтобы в случае загрузки данных в облачные хранилища Система назначала событию вердикт *Заблокировать* и уровень нарушения *Средний*. Для этого:

1. Создайте политику защиты данных на агентах.
2. Добавьте правило копирования (см. "Создание правил").
3. В атрибутах правила (см. "Правило копирования") укажите атрибуту **Тип события** значение *Облачное хранилище*.
4. В поле **Приемник копирования** укажите облачные хранилища, загрузка данных на которые должна блокироваться.
5. В блоке **Действия при срабатывании правила** присвойте атрибутам следующие значения:
   - атрибуту **Назначить событию вердикт** - значение Заблокировать;
   - атрибуту **Назначить событию уровень нарушения** - значение *Средний*.

Пример 2:

Требуется блокировать передачу данных через терминальную сессию с использованием буфера обмена, отправлять уведомление офицеру безопасности и назначать нарушителю статус "Под наблюдением". Для этого:

1. Создайте политику защиты данных на агентах.

2. При создании политики укажите защищаемые данные, обнаружив которые Система будет блокировать передачу.
3. Добавьте правило работы в приложениях (см. "Создание правил").
4. В атрибутах правила (см. "Правило работы в приложениях") укажите **Персон** и **Компьютеры**, на которых должна распространяться политика, а также дни и часы действия правила.
5. В блоке **Действия при срабатывании правила** присвойте атрибутам следующие значения:
   a. **Отправить почтовое уведомление** - укажите шаблон уведомления. Например, предустановленный шаблон **Уведомление офицеру безопасности**.
   b. **Назначить событию вердикт** - значение Заблокировать;
   c. **Назначить отправителю статус** - выберите предустановленный статус **Под наблюдением**.

   После применения конфигурации созданная политика будет отправлена через сервер Device Monitor на Агенты. Если в передаваемых через терминальную сессию текстовых данных будут обнаружены защищаемые данные, действие будет заблокировано, а буфер обмена очищен. Также будет создано соответствующее событие, офицер безопасности получит уведомление, а нарушителю в Системе будет назначен статус "Под наблюдением".

Подробнее об особенностях создания политики см. "Особенности задания правил в политиках защиты данных на агентах".

4.7.5 Создание политики контроля персон

Цель:
Создать политику, определяющую реакцию Системы на действия определенных персон. Политика распространяется только на действия отправителей трафика.

Решение:

1. Перейдите в раздел **Политики**.
2. В верхней части рабочей области нажмите **Добавить политику** и в раскрывающемся списке выберите **Политика контроля персон**.
3. В открывшемся окне установите флажки напротив элементов, которые вы хотите добавить, и нажмите **Сохранить**. В качестве объектов исследования могут выступать:
   - отдельные персоны (сотрудники или компьютеры);
   - группы персон и компьютеров;
   - персоны и компьютеры, объединенные одним статусом.

   > **Примечание.**
   >
   > Если выбраны элементы различных типов (например, персоны и статусы), то политика сработает при обнаружении хотя бы одного элемента каждого типа.

4. Новая политика будет добавлена в группу **Политики контроля персон**, а в правой части рабочей области отобразится форма просмотра политики.
5. На форме просмотра политики заполните необходимые поля (см. "Раздел Политики") и нажмите **Сохранить**.

> **Важно!**
>
> При заполнении атрибута **Период действия** учитывайте возможную разницу часовых поясов между филиалами вашей организации. Временем перехвата события считается локальное время на сервере, выполняющем перехват. В случае, если локальное время перехвата события не попадает в указанный интервал, то политика к данному событию применяться не будет.

Чтобы отредактировать политику:

1. Выделите нужную политику в списке.
2. На форме в правой части рабочей области отредактируйте требуемые параметры.
3. Чтобы изменить список контролируемых персон, в блоке **Контролируемые персоны** нажмите **Выбрать** и отредактируйте список, после чего нажмите **Сохранить**.
4. Нажмите **Сохранить** на форме редактирования политики.

Чтобы удалить политику, нажмите в правом верхнем углу плитки политики и в открывшемся окне подтвердите удаление.

Вы также можете добавлять политики контроля персон непосредственно из разделов **Персоны** (см. "Раздел Персоны") и **Статусы** (см. "Статусы").

Чтобы добавить политику для группы персон и компьютеров:

1. Перейдите в раздел **Персоны**.
2. Выделите нужную группу в списке.
3. На панели инструментов в левой части рабочей области нажмите .

Чтобы добавить политику для выбранных персон или компьютеров:

1. Перейдите в раздел **Персоны**.
2. Выделите нужную персону или компьютер. Для выбора нескольких элементов воспользуйтесь клавишами Shift или Ctrl.
3. На панели инструментов в правой части рабочей области нажмите и в раскрывающемся списке выберите **Создать политику**.

Чтобы добавить политику для выбранного статуса:

1. Перейдите в раздел **Списки**->**Статусы**.
2. Выберите в списке требуемый статус.
3. На панели инструментов нажмите .

Пример:
Требуется контролировать персону *Иванов* (подразумевается, что персона Иванов уже создана в разделе **Персоны**) таким образом, чтобы объекту перехвата с уровнем нарушения *Высокий*, отправителем которого является Иванов, назначался вердикт *Разрешить*, при этом персоне присваивался статус *Под наблюдением*, и на почтовый ящик *example@company.com* отправлялось уведомление об инциденте. Для этого:

1. Перейдите в раздел **Политики** и создайте политику контроля персон с названием *Иванов*.
2. Создайте правило для политики *Иванов*, при этом атрибутам должны быть присвоены следующие значения:
   - атрибуту **Перехватывать с уровнем нарушения** - значение *Высокий*;

- атрибуту **Отправить уведомление** - значение *example@company.com* (подробнее см. "Настройка уведомлений в правилах");
- атрибуту **Назначить событию вердикт** - значение *Разрешить*;
- атрибуту **Назначить отправителю статус** - значение *Под наблюдением*.

3. Сохраните политику.

4.7.6 Создание правил

Справочная информация:

Каждая политика может содержать одно или несколько правил.

Если политика срабатывает на объекте перехвата, то в зависимости от количества сработавших правил Система выполняет следующие действия:

- Если срабатывает одно правило, Система выполняет действия, указанные для этого правила.
- Если срабатывают несколько правил, и
  - действия сработавших правил противоречат друг другу - Система выбирает из противоречащих действий самое приоритетное и выполняет его (о приоритетах правил см. "Общие сведения о политиках");
  - действия сработавших правил не противоречат друг другу - Система выполняет все действия, не противоречащие другим.
- Если ни одно правило не срабатывает, но в политике заданы действия по умолчанию, Система выполняет указанные действия (см. "Определение действий Системы по умолчанию").

> **Примечание:**
>
> Если на объекте перехвата срабатывают несколько политик, каждая из которых содержит правила, Система выбирает из противоречащих действий наиболее приоритетное и выполняет его (о порядке выбора приоритетов см. "Общие сведения о политиках"). Действия, не противоречащие другим, выполняются в полном объеме.

Цель:
Указать действия, приводящие к срабатыванию правила, и определить реакцию Системы на эти действия.

Решение:

1. Перейдите в раздел **Политики**.
2. Выделите требуемую политику в списке или создайте новую политику (см. "Создание политики защиты данных", "Создание политики защиты данных на агентах", "Создание политики контроля персон").
3. Добавьте правило одним из следующих способов:
   - на вкладке с выбранной группой правил нажмите **Добавить правило**.
   - в правом верхнем углу формы нажмите **Добавить правило** и в выпадающем списке выберите требуемый тип правила.
4. Настройте правило, используя форму в правой части рабочей области (см. "Правила и форма их просмотра").
5. В блоке **Действия при срабатывании правила** укажите, какие действия должна выполнить Система в случае срабатывания правила (описание действий см. в статье "Определение действий Системы в случае нарушения правил").

6. Нажмите **Сохранить**.

Чтобы отредактировать правило:

1. Выделите требуемую политику в списке.
2. В плитке политики выберите требуемую группу правил. Правила сгруппированы на вкладках:
   - **Передача**, **Копирование**, **Хранение**, **Работа в приложениях** и **Файловые операции** - для политики защиты данных;
   - **Передача**, **Копирование**, **Работа в приложениях** - для политики защиты данных на агенте;
   - **Правила** - для политики контроля персон.
3. В плитке политики отобразится список правил выбранной группы. Щелчком левой кнопки мыши выделите нужное правило в списке.
4. В правой части рабочей области откроется форма редактирования правила. Измените необходимые поля и нажмите **Сохранить**.

Чтобы удалить правило, нажмите ✕ в правом верхнем углу плитки правила и в открывшемся окне подтвердите удаление.

Пример:

Требуется, чтобы в случае передачи файлов, составляющих объект защиты *Строго конфиденциальная информация*, по субботам и воскресеньям, Система присваивала событию тег *Отправка конфиденциальной информации в выходные* и назначала уровень нарушения *Средний*. Для этого:

1. Создайте тег *Отправка конфиденциальной информации в выходные* (см. "Работа с тегами").
2. Создайте политику защиты данных для объекта защиты *Строго конфиденциальная информация* (см. "Создание политики защиты данных").
3. Добавьте правило передачи, присвоив атрибуту **Дни недели действия** значения *Суббота* и *Воскресенье;*
4. В блоке **Действия при срабатывании правила** присвойте атрибутам следующие значения:
   - атрибуту **Назначить событию уровень нарушения** - значение *Средний*;
   - атрибуту **Теги** - значение *Отправка конфиденциальной информации в выходные*.

4.7.7 Определение действий Системы в случае нарушения правил

Справочная информация:
Для каждой политики вы можете указать действия, выполняемые Системой в случае нарушения правил. Для этого необходимо выбрать действия в блоке **Действия при срабатывании правила** при создании или редактировании правила (см. "Создание правил").

Доступные действия определяются типом правила:

Действие	Политики защиты данных				Политики защиты данных на агентах		Политики контроля персон
	Правило передачи	Правило копирования	Правило хранения	Правило буфера обмена	Правило передачи	Правило копирования	Правило контроля персон
Отправить уведомление	Доступно	Доступно	Доступно	Доступно	Доступно	Доступно	Доступно
Назначить событию вердикт	Доступно	Не доступно	Не доступно	Не доступно	Доступно	Доступно	Доступно
Назначить событию уровень нарушения	Доступно	Доступно	Доступно	Доступно	Доступно	Доступно	Доступно
Назначить событию теги	Доступно	Доступно	Доступно	Доступно	Доступно	Доступно	Доступно
Назначить отправителю статус	Доступно	Доступно	Доступно	Доступно	Доступно	Доступно	Доступно
Удалить событие	Доступно	Доступно	Доступно	Доступно	Не доступно	Не доступно	Доступно

Подробное описание действий:

Действие	Описание
Отправить уведомление	Позволяет указать, какие уведомления должны быть отправлены в случае срабатывания правила. Чтобы настроить отправку уведомлений, нажмите + рядом с полем. В открывшемся диалоговом окне выберите уведомление из списка или создайте новое уведомление. Подробнее см. "Настройка уведомлений в правилах". Выбранный шаблон уведомления должен соотвествовать указанному в правиле вердикту.

Действие	Описание
	Примечание: Если после создания правила персона или ее e-mail будут удалены из Системы (о работе с учетными записями см. *"InfoWatch Traffic Monitor. Руководство администратора"*, раздел "Пользователи"), то уведомление данной персоне отправлено не будет.
Назначить событию вердикт	Событию будет назначен вердикт - предварительное решение Системы о возможном нарушении политики безопасности. Возможные значения: • **Разрешить** - объект не является потенциальным нарушением и может быть доставлен получателям. • **Заблокировать** - объект является потенциальным нарушением. В режиме "Блокировка" доставка такого объекта блокируется. • **Поместить на карантин** (для политики защиты данных на агентах данный вердикт не доступен) - требуется решения пользователя, является ли объект нарушением. В режиме "Блокировка" доставка такого объекта откладывается до вынесения решения пользователем. В зависимости от решения пользователя значение вердикта изменится либо на **Разрешено** (в этом случае выполняется доставка), либо на **Заблокировано** (подробнее см. "Вынесение решения по объекту"). Досылка сообщений возможна только для SMTP-писем при работе Системы "в разрыв" - см. документ "*Infowatch Traffic Monitor. Руководство по установке и настройке*".
Назначить событию уровень нарушения	Событию будет назначен уровень нарушения. Возможные значения: **Высокий**, **Средний**, **Низкий**, **Отсутствует**.
Назначить событию теги	Событию будут назначены указанные теги, например, **На рассмотрение**. Подробнее см. "Теги".
Назначить отправителю статус	Нарушителям политики безопасности будет присвоен указанный статус, например, **Под наблюдением**. Подробнее см. "Статусы".
Удалить событие	Событие не будет сохранено в базу данных, а также не будут выполнены действия, указанные в правиле.

См. также:

- Создание правил
- Настройка уведомлений в правилах

4.7.8 Настройка уведомлений в правилах

При создании или редактировании правила вы можете указать, кому должны быть отправлены уведомления в случае срабатывания правила.

Для этого:

1. В области **Действия при срабатывании правила**, в поле **Отправить уведомление** нажмите .
2. В открывшемся диалоговом окне **Выбор почтовых уведомлений** отметьте поля напротив выбранных уведомлений. Вы можете выбрать несколько уведомлений для отправки различным получателям.

   > **Примечание.**
   >
   > Если в Системе отсутствуют уведомления, будет выведено сообщение. Вы можете перейти к созданию уведомления, нажав **Создать уведомление** в окне сообщения.

3. Если в списке отсутствует подходящее уведомление, вы можете создать новое уведомление. Для этого нажмите **Создать новое** в левом верхнем углу окна.

   > **Примечание.**
   >
   > Чтобы отредактировать уведомление из списка, щелкните по названию уведомление левой клавишей мыши.

   > **Примечание.**
   >
   > Вы также можете создавать и редактировать уведомления в разделе **Управление** -> **Уведомления** (см. "Настройка уведомлений").

4. На форме создания/редактирования уведомления укажите параметры уведомления, как описано в статье "Создание уведомления".
5. Для возврата к списку уведомлений нажмите **К выбору уведомлений** в левом верхнем углу формы.
6. После того как вы выбрали все требуемые уведомления, нажмите **Сохранить**.

   > **Важно!**
   >
   > Вердикт, указанный в уведомлении, должен совпадать с вердиктом, указанным в правиле. В противном случае уведомление не будет отправлено.

4.7.9 Определение действий Системы по умолчанию

Справочная информация:
Если после применения политики остаются суб-события, которым не соответствует ни одно правило, Система выполняет действия по умолчанию (о разбиении событий на суб-события см. "Общие сведения о политиках"). Действия по умолчанию определяются пользователем.

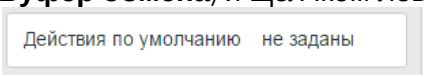
> **Примечание.**
>
> Если действие по умолчанию не заданы, и для объекта перехвата не сработало ни одно из правил, то политика также не сработает на данном объекте перехвата.

Цель:

Определить, как должна отреагировать Система при наличии в событии суб-события, которому не соответствует ни одно правило политики.

> **Примечание.**
>
> Возможность указать действия по умолчанию предусмотрена только для политик защиты данных и политик защиты данных на агентах.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите целевую политику.
3. В плитке политики выберите целевую вкладку (**Передача**, **Копирование**, **Хранение** или **Буфер обмена**) и щелчком левой кнопкой мыши выделите нижнюю часть плитки:
   

4. В правой части рабочей области, в единственном блоке **Действия при срабатывании правила**, укажите необходимые действия (см. "Правила и форма их просмотра") и нажмите **Сохранить**.

Дополнительная информация:

Для типов события *Веб-сообщение* и *Почта в Браузере* может возникать ситуация, когда происходит ложное срабатывание правила по умолчанию. Такая ситуация может возникнуть, если:

В Системе создано правило, регулирующее передачу данных от персоны А к персоне В. Если персона А отправляет данные персоне В через веб-сайт, в Системе создается событие, которое разбивается на два суб-события:

Отправитель	Получатель	Протокол
Персона А	Персона В	HTTP
Персона А	Домен веб-сайта	HTTP

Так как маршрут **Персона А**->**Домен веб-сайта** не описан в правилах политики, выполняются действия по умолчанию.

Чтобы избежать ложного срабатывания правила по умолчанию для типов события *Веб-сообщение* и *Почта в Браузере*, вы можете выполнить одно из следующих действий:

- добавить в правило передачи домен веб-сайта или список веб-сайтов, через которые может осуществляться передача данных;
- не указывать действия по умолчанию.

Пример:

Требуется, чтобы в случае копирования файлов, составляющих объект защиты *Гостайна*, при отсутствии сработавших правил копирования Система по умолчанию присваивала карточке копирующей персоны статус *Под наблюдение*м:
Для этого:

1. Создайте политику защиты данных для объекта защиты *Гостайна* (см. "Создание политики защиты данных").
2. Перейдите к выбору действий по умолчанию.
3. В единственном блоке **Действия при срабатывании правила** укажите атрибуту **Назначить персонам статус** значение *Под наблюдением.*

4.7.10 Фильтрация списка политик

Цель:
Отфильтровать список политик в случае большого числа политик в списке.

Решение:

1. Перейдите в раздел **Политики**.
2. В верхней части рабочей области нажмите **Фильтр**.
3. В области **Настройка фильтра** укажите критерии фильтрации в одном из полей или в обоих полях:
   - **Фильтровать по названиям политик** - начните вводить текст и выберите название требуемой политики (возможно выбрать несколько политик, повторяя данное действие);
   - **Фильтровать по объектам исследования** - начните вводить текст и выберите название требуемого объекта (возможно выбрать несколько объектов, повторяя данное действие).
     Для политик защиты данных и политик защиты данных на агентах вы можете указать следующие объекты исследования:
     - каталог объектов защиты;
     - объект защиты;
     - файловый формат.

     Для политик контроля персон вы можете указать следующие объекты исследования:
     - персона;
     - группа персон;
     - статус.
4. Нажмите **Применить**.

4.7.11 О политике защиты данных на агентах

Для чего нужна политика:

Из всех политик данная применяется в первую очередь и только непосредственно на агентах DM. На стороне ТМ политика не применяется.
Данная политика является инструментом Офицера Безопасности, предназначенным для контроля деятельности на рабочих станциях и предотвращения выхода конфиденциальных данных за периметр компании.
Политика накладывает ограничения на следующие действия пользователя:

- передача данных:
  - исходящие письма по протоколам SMTP, MAPI на почтовом Клиенте;
  - исходящие письма по Веб-почте в браузере;
  - Интернет-активность (HTTP(S)-запросы);
- копирование данных:
  - с и на съемные устройства, сетевые ресурсы, приложения, подключенные через терминальную сессию;
  - на FTP, медиа-устройства (по протоколу MTP), облачные хранилища;
- работа в приложениях (копирование текста с помощью буфер обмена через терминальную сессию).

Механизм работы политики следующий:

1. Для контроля трафика на рабочих станциях пользователей ОБ создает и настраивает в консоли ТМ политику защиты данных на агенте, которая, в свою очередь, автоматически распространяется на рабочие станции.
2. Пользователь совершает нелегитимные действия (например, передает данные, содержащие корпоративную тайну, через почту в браузере) со своей рабочей станции.
3. Агент DM на рабочей станции пользователя анализирует передаваемую информацию.
4. В случае срабатывания политики (т.е. нарушения заведенных правил), агент DM выполняет действие, предусмотренное политикой (например, блокировка действия пользователя при назначении вердикта "Заблокировать" в правиле), и отправляет в ТМ событие с результатами анализа, а пользователю выдается сообщение (если это настроено) «Согласно политике безопасности, запрещена передача данных … в связи с обнаружением в передаваемых данных признаков конфиденциальной информации». Запущенные пользователем процесс или действие остаются неосуществленными.
5. ТМ принимает событие, обрабатывает и анализирует его.
6. ОБ видит в консоли ТМ перехваченное событие с результатами анализа, полученными как на агенте DM, так и после обработки на сервере ТМ.
7. ОБ анализирует полученную информацию и применяет меры.

Необходимый минимум действий ОБ для заведения политики:

- Завести правила перехвата данных.
- Выбрать защищаемые данные. Это могут быть:
  - содержащие текстовые объекты, категории и термины объекты защиты и каталоги объектов защиты;
  - файловые форматы.
    Если проигнорировать этот пункт, то политика будет распространяться на действия с любыми данными.
- Указать период действия политики (это может быть временной отрезок или бессрочно).

Правила, доступные для заведения: правило передачи, правило копирования, правило работы в приложениях.
Подробнее о правилах и их создании в статьях Правила и форма их просмотра, Правило передачи, Правило копирования, Правило работы в приложениях.

4.7.12 О политике защиты данных

Для чего нужна политика:

Политика применяется во вторую очередь (после политики защиты данных на агенте) на стороне ТМ и способна отслеживать больший набор каналов утечки информации, а именно:

- Мессенджеры;
- Снимки экрана, печать;
- Хранение файлов;
- Файловые операции;
- Буфер обмена;
- Ввод с клавиатуры.

Механизм работы политики следующий:

1. ОБ создает и настраивает в консоли ТМ политику защиты для широкого контроля защиты данных. Контролю подлежат каналы, указанные выше.
2. Пользователь совершает действия (например, отправляет отправляет на печать файл, содержащий конфиденциальные данные).
3. ТМ анализирует передаваемую информацию.
4. В случае срабатывания политики (т.е. нарушения заведенных правил), создается событие для ОБ. Отправленное сообщение уходит адресату (при этом на сервере ТМ создается его теневая копия) либо передача блокируется (при назначении вердикта "Заблокировать" в правиле). Создается событие для ОБ.
5. ОБ видит в консоли ТМ перехваченное событие с результатами анализа после обработки на сервере ТМ.
6. ОБ анализирует полученную информацию и применяет меры.

Необходимый минимум действий ОБ для заведения политики:

- Завести правила перехвата данных.
- Выбрать защищаемые данные. Это могут быть любые комбинации объектов защиты, каталогов объектов защиты, файловых форматов. Если проигнорировать этот пункт, то политика будет распространяться на действия с любыми данными.
- Указать период действия политики (это может быть временной отрезок или бессрочно).

Правила, доступные для заведения: правило передачи, правило копирования, правило хранения и правило буфера обмена.
Подробнее о правилах и их создании в статьях Правила и форма их просмотра, Правило передачи, Правило копирования, Правило хранения, Правило работы в приложениях, Правило файловых операций.

4.7.13 О политике контроля персон

Для чего нужна политика:

Возможны ситуации, когда ОБ необходимо отследить нарушения по конкретному сотруднику организации и проконтролировать его рабочий процесс.

Для этого удобно применять политику данного вида.
При срабатывании политики ОБ получат проанализированные данные о нарушении.

Механизм работы политики следующий:

1. ОБ создает и настраивает в консоли ТМ политику контроля персон, указав при этом объект наблюдения (контролируемую персону).
2. Все действия пользователя, попадающие под действие политики, отправляются в ТМ.
3. ТМ анализирует полученную информацию.
4. В случае срабатывания правила контроля персон создается событие для ОБ.
5. ОБ видит в консоли ТМ перехваченное событие с результатами анализа после обработки на сервере ТМ и применяет меры.

Необходимый минимум действий ОБ для заведения политики:

- Завести правило контроля персон.
- Указать минимум одну позицию из категорий: Персоны, Группы, Статусы.

> **Примечание:**
>
> Политика срабатывает только для инициаторов событий. На получателей трафика политика не распространяется.

Подробнее о правиле контроля персон в статье Правило контроля персон.

4.8 Работа с отчетами

Для чего требуются отчеты:

Отчеты используются для мониторинга и расследования инцидентов и позволяют получить наглядную статистическую информацию по интересующим вас параметрам.

Использование отчетов удобно в тех случаях, когда требуется выполнить гибкую настройку параметров, в то время как виджеты в разделе "Сводка" содержат меньше условий и используются для оперативного получения статистических данных.

Инструменты в разделе "Отчеты" также позволяют сформировать печатную отчетность по результатам расследования или мониторинга.

Работа с отчетами заключается в создании отчетов, отображающих статистику по выбранным параметрам, и анализе их результатов (см. "Создание и просмотр отчетов"). Подробнее о выполняемых при этом действиях см. статьи:

- Создание папки с отчетами
- Создание отчета
- Создание виджета
- Просмотр готовых отчетов

В статье "Примеры использования отчетов" приведены примеры использования отчетов для мониторинга активности пользователей и для расследования инцидентов.

См. также:

- "Раздел "Отчеты"" - о разделе, в котором ведется работа с отчетами

4.8.1 Создание и просмотр отчетов

Цель:
Создать отчет для просмотра статистической информации по объектам перехвата.

Решение:

1. Перейдите в раздел **Отчеты** (см. "Раздел "Отчеты"").
2. Если вы хотите создать отчет внутри папки, выберите нужную папку из списка или создайте новую папку (см. "Создание папки с отчетами").
3. Создайте отчет внутри выбранной папки или на верхнем уровне (см. "Создание отчета").
4. Добавьте в отчет требуемые виджеты (см. "Создание и настройка виджета").
5. Чтобы запустить выполнение отчета, выберите отчет в списке в левой части рабочей области и нажмите  на панели инструментов или кнопку **Выполнить отчет** на форме просмотра отчета (при создании отчета вы можете также использовать кнопку **Сохранить и выполнить**).
6. Чтобы просмотреть результаты ранее выполнявшегося отчета, выбрети отчет в списке в левой части рабочей области. Также вы можете посмотреть результаты выполнения отчета за различные даты и сохранить выбранную версию отчета на ваш компьютер (подробнее см. "Просмотр готовых отчетов").

При необходимости вы можете копировать или переместить ранее созданную папку или отчет.

Чтобы копировать папку и содержащиеся в ней отчеты:

1. Выделите нужную папку в списке с помощью мыши.
2. На панели инструментов в левой части рабочей области нажмите  **Копировать**.

Если выполняется копирование вложенной папки и у пользователя есть полный доступ к родительской папке, то копия будет в ту же папку, где расположена копируемая папка. Если у пользователя отсутствует полный доступ к родительской папке, или выполняется копировании папки верхнего уровня, то копия будет добавлена в корень дерева папок.

Чтобы копировать отчет:

1. Выделите отчет в списке с помощью мыши.
2. На панели инструментов в левой части рабочей области нажмите  **Копировать**.

Если выполняется копирование внутри папки и у пользователя есть полный доступ к папке, то копия будет в ту же папку, где расположен копируемый отчет. Если у пользователя отсутствует полный доступ к папке, или выполняется копировании отчета верхнего уровня, то копия будет добавлена в корень дерева папок.

Чтобы переместить папку, выделите в списке нужную папку и, удерживая левую клавишу мыши зажатой, переместите ее в требуемое место, после чего отпустите зажатую клавишу мыши.

> **Примечание.**
>
> Для перемещения папки пользователь должен иметь полный доступ как к перемещаемой папке, так и к папке, в которую выполняется перемещение. Если папка содержит отчеты, пользователю также требуется полный доступ к отчетам, содержащимся в папке. Подробнее см. таблицу ниже.

Чтобы переместить отчет, выделите в списке нужный отчет и, удерживая левую клавишу мыши зажатой, переместите его в требуемое место, после чего отпустите зажатую клавишу мыши.

> **Примечание.**
>
> Для перемещения отчета пользователь должен иметь полный доступ как к отчету, так и к папке, в которую выполняется перемещение. Подробнее см. таблицу ниже.

В таблице ниже указано, какими правами должен обладать пользователь для выполения действий с отчетами:

Действия в системе	**Права доступа**			
	Просмотр и выполнение папки	Полный доступ к папке	Просмотр и выполнение отчета	Полный доступ к отчету
Просмотр папки	+			
Редактирование атрибутов папки (название, описание, права доступа)	+	+		
Копирование папки	+			
Создание нового элемента (отчета или подпапки) в папке отчетов	+	+		
Перемещение пустой папки в другую папку	+	+		
Перемещение папки, содержащей хотя бы один отчет	+	+	+	+
Удаление пустой папки	+	+		
Удаление папки, содержащей хотя бы один отчет	+	+	+	+
Просмотр и выполнение отчета	+		+	
Редактирование параметров отчета (в том числе, прав доступа)	+		+	+

Копирование отчета	+		+	
Перемещение отчета в другую папку	+		+	+
Удаление отчета	+		+	+

См. также:

- Создание папки с отчетами
- Создание отчета
- Примеры использования отчетов

Создание папки с отчетами

Цель:

Создать папку, в которой будут сгруппированы отчеты, объединенные общей тематикой.

Решение:

1. Перейдите в раздел **Отчеты**.
2. В списке папок и отчетов в левой части рабочей области выберите, на каком уровне требуется создать папку. Вы можете создать папку верхнего уровня или подпапку внутри уже созданной папки с отчетами.

   > **Примечание.**
   >
   > Если у вас отсутсвуют права на создание элементов внутри выбранной папки, будет выведено сообщение. В этом случае необходимо создать папку в другом месте.

3. Нажмите + и в раскрывающемся списке выберите **Создать папку**.
4. В открывшейся форме введите название папки.
5. Укажите, должны ли права доступа к папке наследоваться для вложенных подпапок и отчетов. По умолчанию опция **Применить права для дочерних папок и отчетов** не выбрана.

   > **Примечание.**
   >
   > Если вы создаете подпапку внутри папки, для которой выбрана опция **Применить права для дочерних папок и отчетов**, то действия, описанные на шаге 5-6, недоступны.

6. Укажите, кому доступна папка, и определите права доступа. Для этого:
   a. Найдите в списке требуемых пользователей.

   > **Совет.**
   >
   > Для поиска нужных пользователей в списке воспользуйтесь полем **Поиск**.

b. Напротив имен требуемых пользователей установите флажок в одном из полей:
   - **Просмотр и выполнение** - чтобы предоставить пользователю права на просмотр и копирование папки. Права доступа к отчетам, содержащимся в папке, определяются при создании отчета;
   - **Полный доступ** - чтобы предоставить пользователю полный доступ к папке.

> **Примечание.**
>
> Чтобы предоставить доступ к папке всем пользователям Системы, установите флажок в поле с требуемым уровнем доступа напротив значения **Все пользователи**.

7. Нажмите **Сохранить папку**.

Редактирование папки выполняется с помощью кнопки  на панели инструментов.

Для удаления папки используйте кнопку  .

> **Примечание.**
>
> Для редактирования и удаления папки пользователю необходимо иметь полный доступ к папке. Если для выбранной папки вам разрешены только просмотр и выполнение, то вместо кнопки  будет отображаться кнопка  , а кнопка  будет недоступна.

Создание отчета

Цель:
Создать отчет, содержащий статистические данные по объектам перехвата.

Решение:

1. Перейдите в раздел **Отчеты**.
2. В списке папок и отчетов в левой части рабочей области выберите, на каком уровне требуется создать отчет. Вы можете создать отчет верхнего уровня или внутри выбранной папки.

> **Примечание.**
>
> Если у вас отсутсвуют права на создание элементов внутри выбранной папки, будет выведено предупреждение. В этом случае необходимо создать отчет в другом месте.

3. На панели инструментов нажмите  и в раскрывающемся списке выберите **Создать отчет**.
4. В открывшейся форме создания отчета укажите требуемые параметры (подробнее см. "Форма создания отчета").
5. На вкладке **Виджеты** нажмите **Добавить виджет**.
6. В открывшемся окне **Добавление виджета** укажите параметры виджета (подробнее см. "Создание и настройка виджета") и нажмите **Сохранить**.

7. При необходимости продолжите добавлять виджеты, как описано на шаге 6. После того как вы добавили все необходимые виджеты, закройте окно **Добавление виджета**, нажав ✕ в правом вехнем углу.
8. Перейдите на вкладку **Доступ**, чтобы указать, кому будет доступен запрос и определить права доступа.

   > **Важно!**
   >
   > Если отчет создается внутри папки, для которой выбрана настройка **Применить права для дочерних папок и отчетов**, то права доступа к отчету будут соответствовать правам доступа, указанным для папки. Редактирование прав доступа к отчету в этом случае недоступно.

   Чтобы указать права доступа к отчету:
   a. Найдите в списке требуемых пользователей.

      > **Совет.**
      >
      > Для поиска нужных пользователей в списке воспользуйтесь полем **Поиск**.

   b. Напротив имен требуемых пользователей установите флажок в одном из полей:
      - **Просмотр и выполнение** - чтобы предоставить пользователю права на просмотр, копирование и выполнение отчета;
      - **Полный доступ** - чтобы предоставить пользователю полный доступ к отчету.

   > **Примечание.**
   >
   > Чтобы предоставить доступ к папке всем пользователям Консоли, установите флажок в поле с требуемым уровнем доступа напротив значения **Все пользователи**.

9. Нажмите:
   - **Сохранить** - чтобы сохранить отчет.
   - **Сохранить и выполнить** - чтобы сохранить и выполнить отчет.

Редактирование отчета выполняется с помощью кнопки  на панели инструментов.

Для удаления отчета используйте кнопку ✕ .

> **Примечание.**
>
> Для редактирования, удаления и перемещения отчета пользователю необходимо иметь полный доступ к отчету. Если для выбранного отчетса вам разрешены только просмотр и выполнение, то вместо кнопки  будет отображаться кнопка , а кнопка ✕ будет недоступна.

Создание и настройка виджета

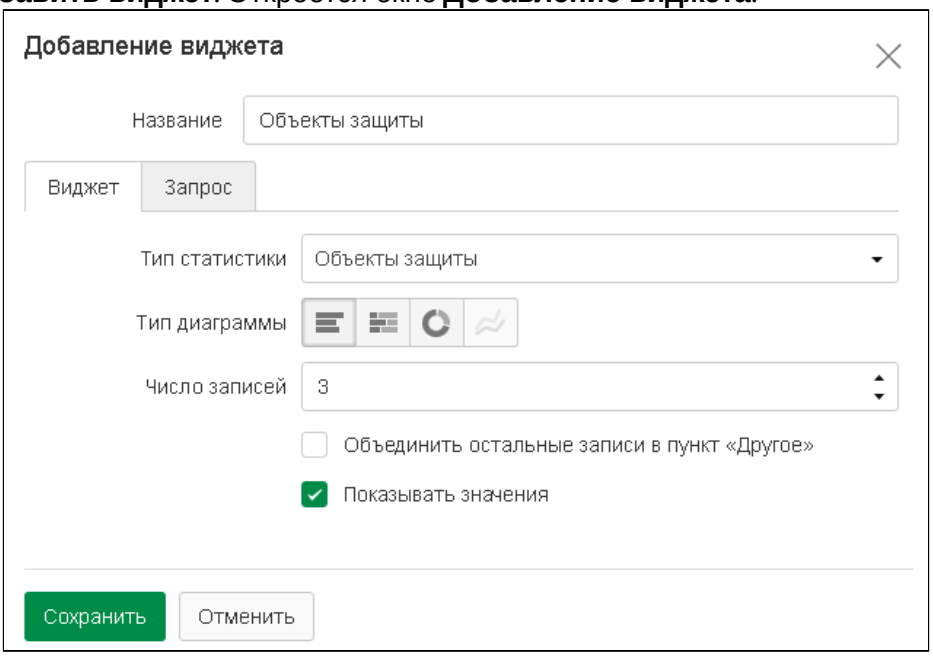
Цель:
Добавить в отчет виджет, на котором будет отображаться статистическая информация.

Решение:

1. Перейдите в раздел **Отчеты**.
2. В левой части рабочей области выберите отчет, в который требуется добавить виджет, или создайте новый отчет (подробнее см. "Создание отчета").

> **Примечание.**
>
> Чтобы добавить виджет в ранее созданный отчет, перейдите в режим редактирования отчета.

3. В открывшейся форме создания/редактирования отчета на вкладке **Виджеты** нажмите кнопку **Добавить виджет**. Откроется окно **Добавление виджета**.



4. Заполните требуемые поля:
   a. В поле **Название** введите название виджета.
   b. На вкладке **Виджет** выберите тип статистики. Остальные настройки (тип диаграммы, число записей, период группировки и т.д.) доступны в зависимости от выбранного типа статистики (подробнее о типах статистики см. статью "Виджеты").
   c. На вкладке **Запрос** укажите параметры, на основе которых будет выполняться фильтрация событий (подробнее о доступных параметрах см. "Запросы").
5. Нажмите **Сохранить виджет**.

Вы можете дублировать созданный виджет в какой-либо другой отчет. Для этого:

1. Перейдите в режим редактирования отчета, содержащего нужный виджет.
2. В правом верхнем углу требуемого виджета нажмите ▾ и в раскрывающемся списке выберите **Дублировать**.

3. В списке отчетов в левой части рабочей области выберите отчет, в который требуется дублировать виджет.

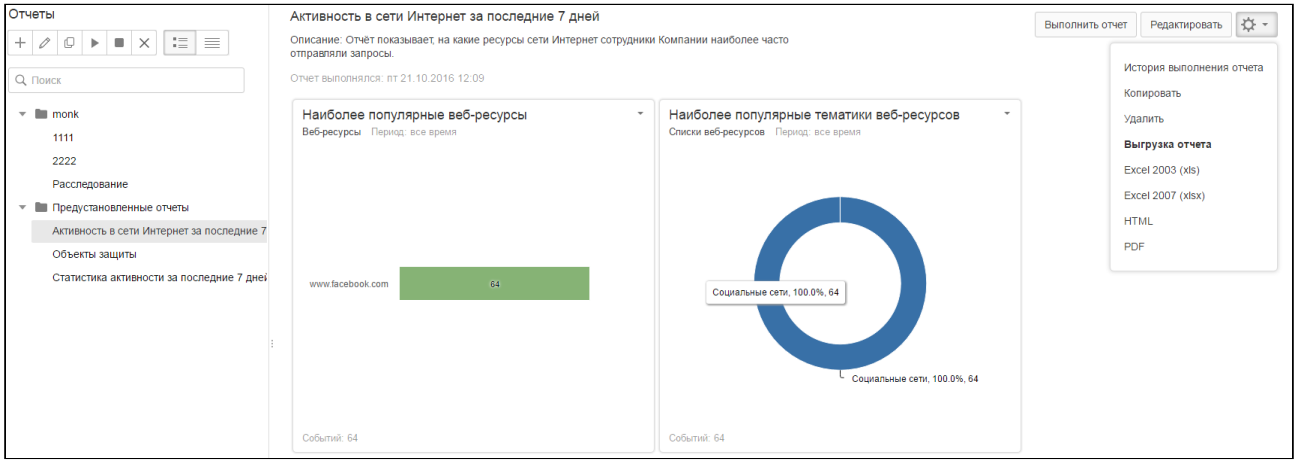
Дополнительные сведения:

Редактирование и удаление виджета выполняются следующим способом:

- Для редактирования виджета перейдите в режим редактирования отчета, в правом верхнем углу требуемого виджета нажмите и в раскрывающемся списке выберите **Редактировать**.
- Для удаления виджета перейдите в режим редактирования отчета, в правом верхнем углу требуемого виджета нажмите и в раскрывающемся списке выберите **Удалить**.

Просмотр готовых отчетов

Чтобы посмотреть последнюю выполненную версию отчета, выберите нужный отчет в списке. В правой части рабочей области будут показаны виджеты для выбранного отчета. Дата и время выполнения отчета отображаются над виджетами.



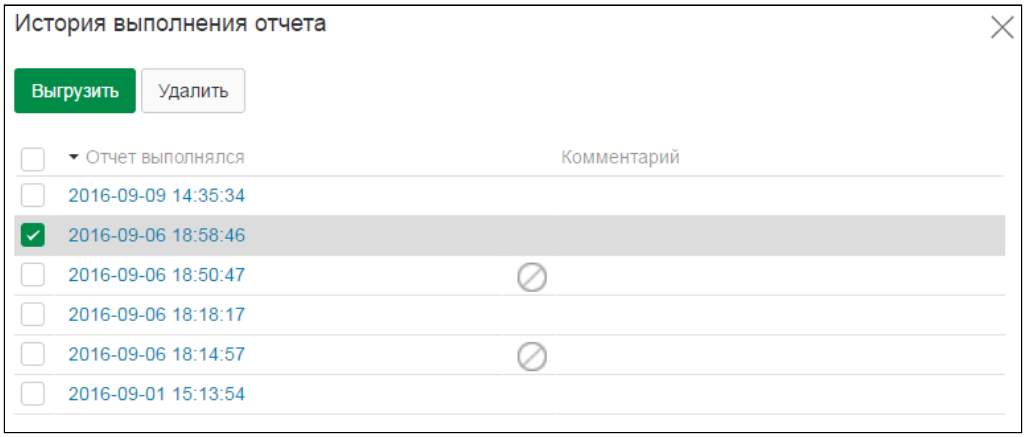
Если вы хотите посмотреть события, информация о которых отображается на виджете, в правом верхнем углу виджета нажмите и в раскрывающемся списке выберите **Перейти в события**. Будет выполнен переход к списку событий виджета в разделе "События".

Вы можете сохранить отчет в виде файла в одном из следующих форматов:

- Excel 2003
- Excel 2007
- HTML
- PDF

Чтобы выгрузить отчет, в правом верхнем углу нажмите кнопку и в раскрывающемся списке под заголовком **Выгрузка отчета** выберите требуемый формат. Отчет в указанном формате будет сохранен на ваш компьютер.

Чтобы посмотреть версии отчета за другие даты, откройте историю выполнения отчета. Для этого в правом верхнем углу нажмите кнопку и в раскрывающемся списке выберите **История выполнения отчета**. В открывшемся диалоговом окне вы можете просмотреть данные о выполнении отчета.



Для каждой версии отчета отображается дата и время выполнения, а также поле, где вы можете добавить комментарий к выбранной версии отчета (для добавления комментария дважды щелкните левой клавишей мыши в поле напротив выбранной версии).

Если выполнение отчета было отменено, то напротив версии отчета отображается пиктограмма .

Вы можете посмотреть требуемые версии отчета, удалить ненужные версии и сохранить выбранные версии отчета в файл.

Чтобы посмотреть версию отчета, щелкните по строке с датой и временем выполнения. Будут показаны виджеты для выбранной версии отчета.

Чтобы удалить выбранные версии отчета:

1. Установите флажки напротив версий, которые вы хотите удалить. Чтобы выбрать все строки сразу, установите флажок в заголовке.
2. Нажмите **Удалить**.

Чтобы выгрузить выбранные версии отчета:

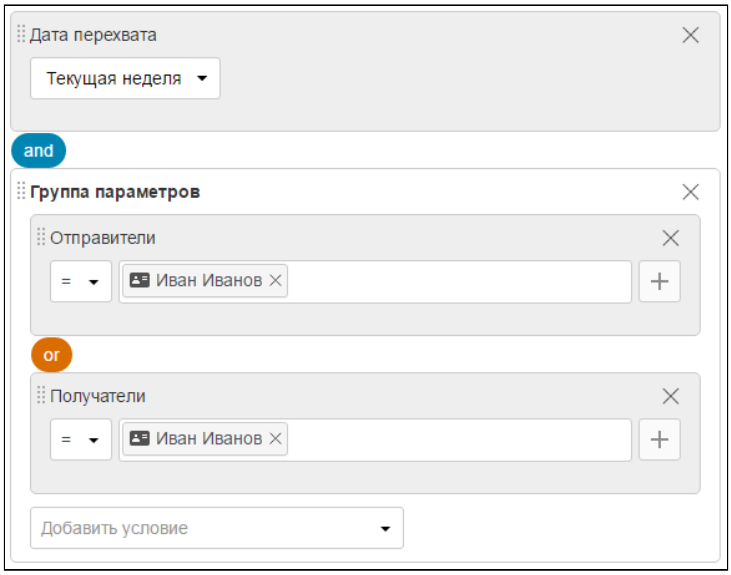
1. Установите флажки напротив версий, которые вы хотите сохранить в виде файла. Чтобы выбрать все строки сразу, установите флажок в поле заголовка.
2. Нажмите **Выгрузить** и в раскрывающемся списке выберите формат сохранения: Excel 2007, Excel 2003, HTML или PDF. Файл в выбранном формате будет сохранен на ваш компьютер.

4.8.2 Примеры использования отчетов

Пример 1:
Сотрудник Иван Иванов попал в список наиболее активных нарушителей за неделю (статистика по наиболее активным нарушителям отображается на виджете сводки "Топ нарушителей"). Требуется провести расследование и получить подробную информацию о деятельности данного сотрудника. Расследование можно провести в несколько этапов.

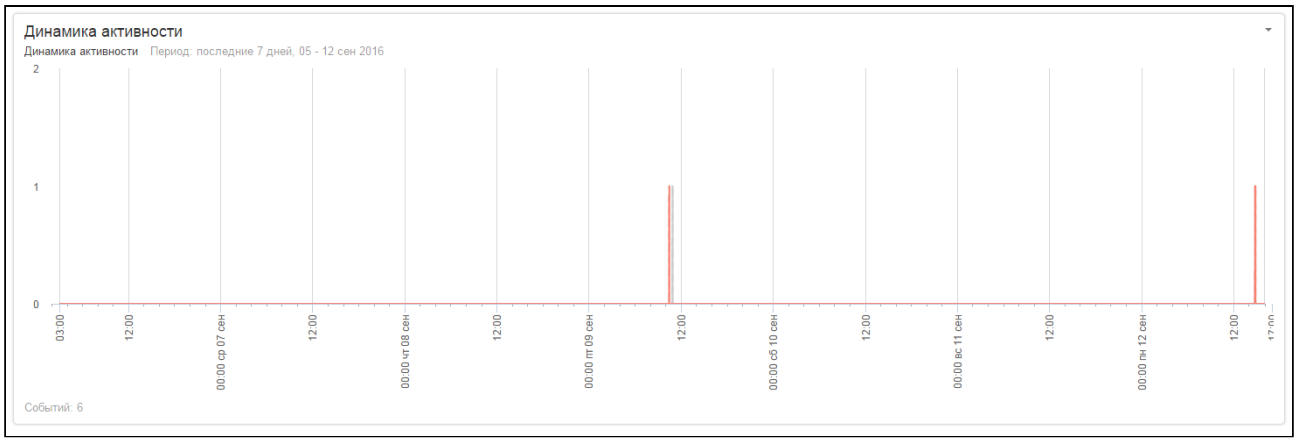
Этап 1. Получить информацию о динамике нарушений. Для этого:

1. Создайте отчет и добавьте в него виджет "Динамика активности".
2. Перейдите на вкладку **Запрос** виджета.
3. В поле **Тип запроса** выберите *Расширенный запрос* и укажите следующие условия:



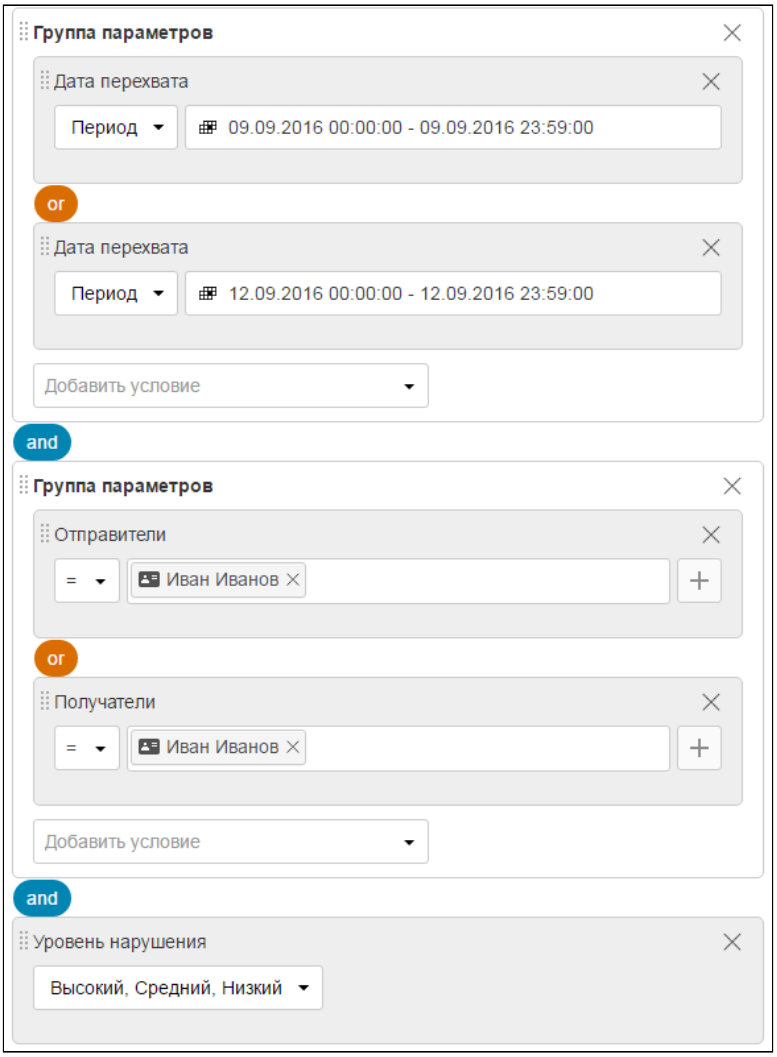
4. Сохраните и выполните отчет.

По полученному графику вы можете определить, что наибольшее количество нарушений сотрудник совершил 09.09 и 12.09.



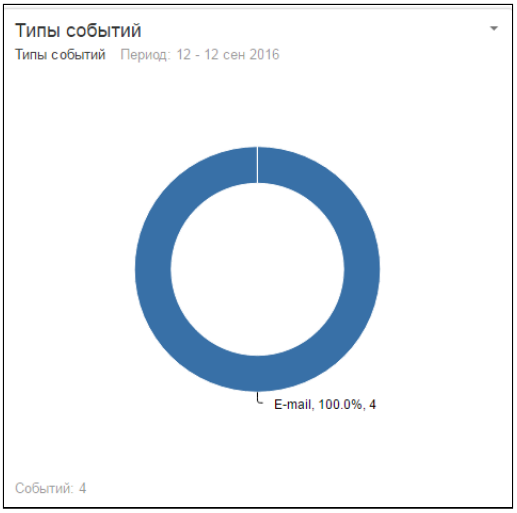
Этап 2. Определить, по каким каналам произошла утечка информации. Для этого:

1. Добавьте в созданный отчет виджет "Типы событий".
2. Перейдите на вкладку **Запрос** виджета.
3. В поле **Тип запроса** выберите *Расширенный запрос* и укажите следующие условия:



4. Сохраните и выполните отчет.

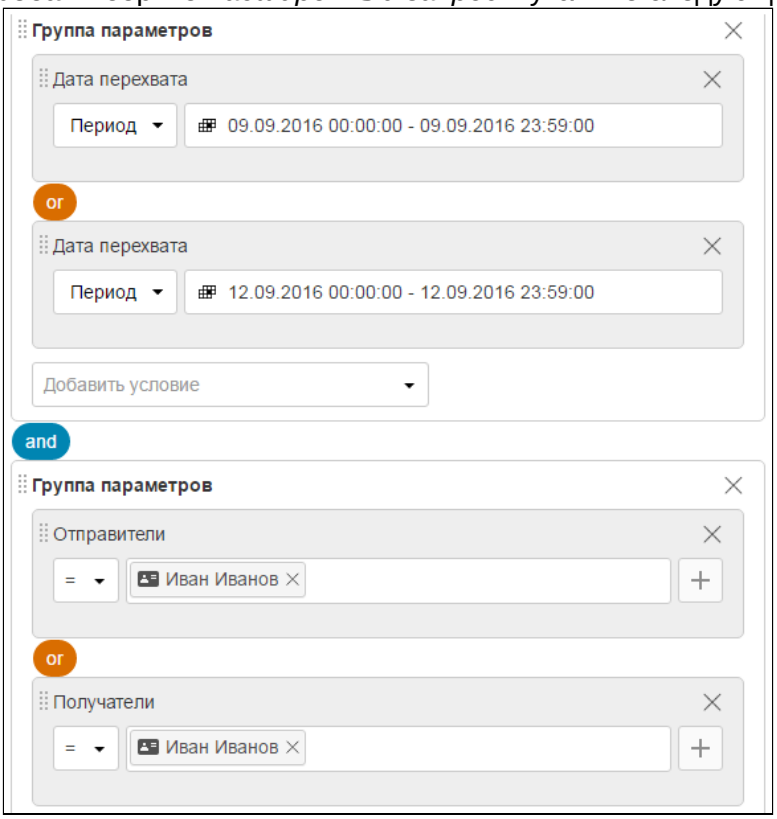
Из отчета вы можете определить, что нарушения были связаны с пересылкой данных по почте.



Этап 3. Определить, какие объекты защиты передаваны. Для этого:

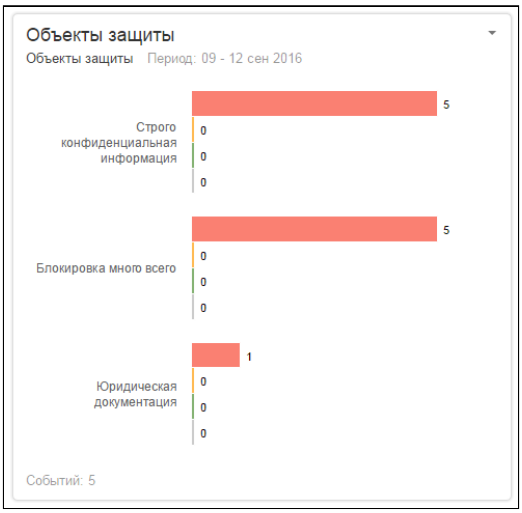
1. Добавьте в созданный отчет виджет "Объекты защиты".
2. Перейдите на вкладку **Запрос** виджета.

3. В поле **Тип запроса** выберите *Расширенный запрос* и укажите следующие условия:



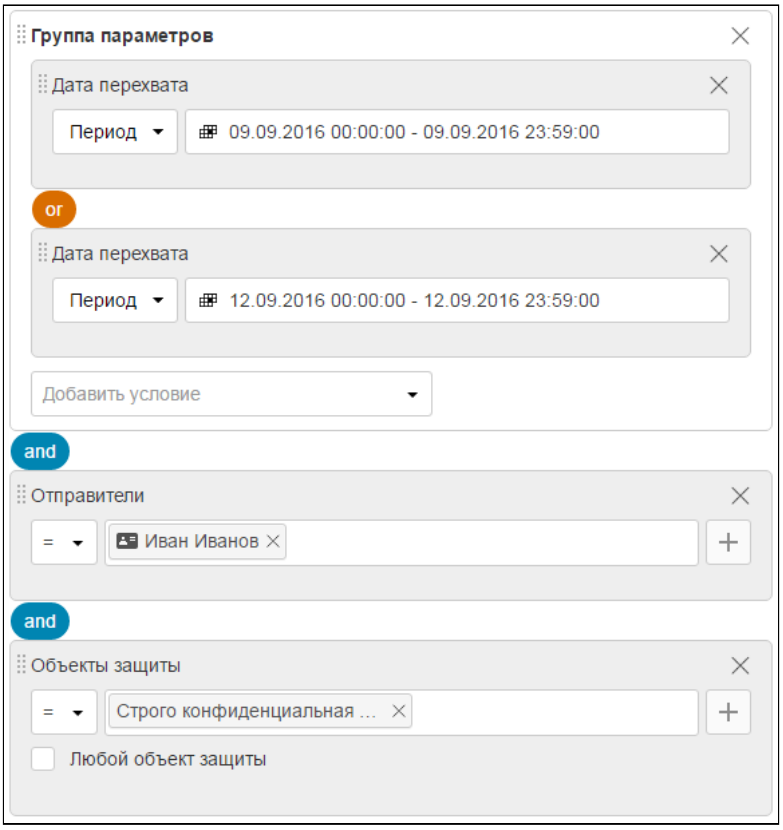
4. Сохраните и выполните отчет.

Из отчета вы можете определить, что сотрудник отправлял по почте документы, входящие в объект защиты "Строго конфиденциальная информация".



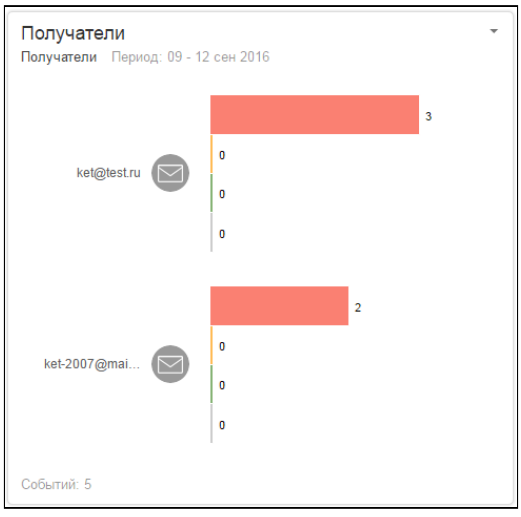
Этап 4. Определить, кому сотрудник Иван Иванов отправлял конфиденциальные данные. Для этого:

1. Добавьте в созданный отчет виджет "Получатели".
2. Перейдите на вкладку **Запрос** виджета.
3. В поле **Тип запроса** выберите *Расширенный запрос* и укажите следующие условия:



4. Сохраните и выполните отчет.

Из отчета вы можете определить, на какие email-адреса была отправлена конфиденциальная информация.

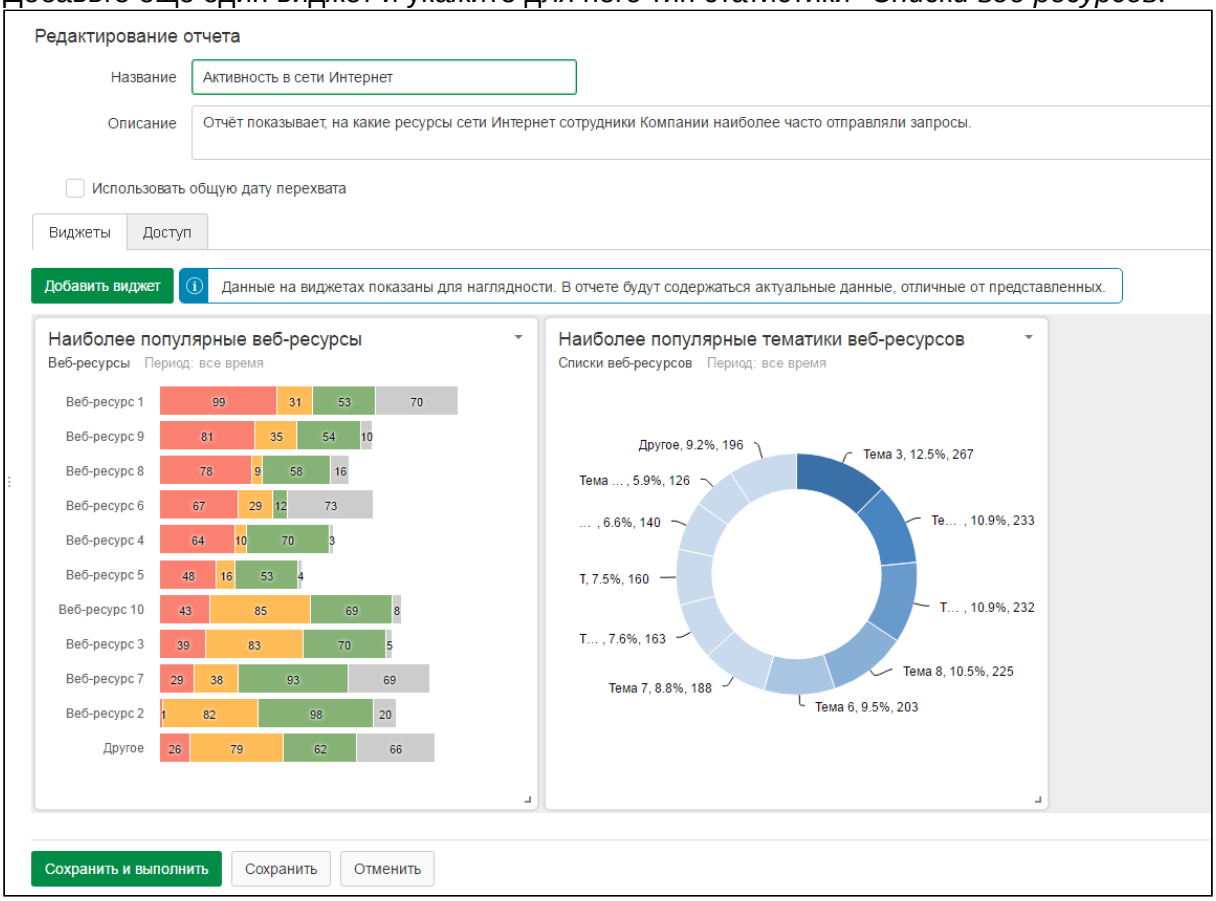


В результате проведения расследования было выяснено, когда, по каким каналам и каким получателям нарушитель передал конфиденциальные данные. Теперь вы можете быстро найти нужные события, создав запрос и указав в нем уже известные вам параметры (см. "Создание запросов"). В найденных событиях вы сможете посмотреть, что именно передавал нарушитель.

Пример 2:
Требуется отследить динамику посещаемости веб-ресурсов и наиболее популярные тематики. Для этого:

1. Создайте отчет "Активность в сети Интернет".
2. Добавьте виджет и укажите для него тип статистики - *Веб-ресурсы*.

3. Добавьте еще один виджет и укажите для него тип статистики - *Списки веб-ресурсов*.



4. На вкладке **Запрос** для каждого виджета выберите требуемый период и при необходимости укажите дополнительные параметры.
5. Сохраните и выполните отчет.

4.9 Управление Системой

Работа в разделе ведется администратором Системы, за исключением подразделов "Аудит" и "Уведомления", работа в которых ведется офицером безопасности.

Управление Системой включает следующие действия:

- Управление интеграцией с LDAP каталогами
- Управление лицензиями
- Управление пользователями Системы и их ролями
- Просмотр состояния Системы
- Сбор диагностических данных, сохранение логов служб
- Добавление плагинов
- Аудит действий пользователя
- Контроль целостности
- Настройка подключения к почтовому серверу
- Настройка уведомлений

4.9.1 Управление интеграцией с LDAP каталогами

Настройка синхронизации с LDAP каталогами выполняется в разделе **Управление** -> **LDAP-Синхронизация**.

> **Важно!**
>
> Если для интернет-браузера установлено расширение Adblock Plus, отключите его для обеспечения корректной работы в этом разделе веб-консоли.

В левой части рабочей области **LDAP-серверы** расположена панель инструментов.
Список серверов, синхронизация с LDAP-каталогами которых настроена, отображается под панелью инструментов.
Панель инструментов содержит набор инструментов для работы с подключениями.
В центральной части рабочей области отображаются параметры выбранного подключения, статус и расписание синхронизации.

Настройка интеграции с LDAP-каталогами описана в разделах:

- Создание подключения к серверу
- Редактирование подключения к серверу
- Удаление подключения к серверу
- Запуск синхронизации с сервером вручную

Создание подключения к серверу

Чтобы создать подключение к серверу:

1. Перейдите в раздел **Управление > LDAP-Синхронизация**.
2. На панели инструментов нажмите  **Создать**.
3. Укажите параметры для нового подключения:

Параметр	Описание
Общие параметры	
Имя сервера	Название соединения, которое используется в консоли управления. **Важно!** Изменение названия сервера между моментами последней синхронизации и обновления Системы не допускается
Тип сервера	Признак того, какой сервер используется – *Active Directory*, *Samba DC*, *Domino Directory, Astra Linux Directory, Astrra Linux Directory Pro/FreeIPA*
Синхронизация	• *Ручная* - синхронизация запускается пользователем в ручном режиме

Параметр	Описание
	• *Автоматическая* - синхронизация выполняется по указанному расписанию **Важно!** Рекомендуется устанавливать частоту автоматической синхронизации с сервером Domino Directory не менее 10 мин. Ручной запуск синхронизации не рекомендуется выполнять чаще, чем один раз в 10 мин.
Период синхронизации	Частота выполнения синхронизации: • *Ежеминутно* • *Ежечасно* • *Ежедневно* • *Еженедельно*
Выполнять каждые ... Выполнять в ...	Время повторения синхронизации, если выбрана *Автоматическая синхронизация* ***Например***, при заданных значениях: • *Период синхронизации* – `ежеминутно`; • *Выполнять каждые* – 60 `минут`, синхронизация будет выполняться каждые 60 минут.
Настройка соединения	
LDAP-сервер	IP-адрес сервера, с LDAP-каталогами которого производится синхронизация
Тип соединения	Выбор типа соединения с AD, Samba DC, DD, ALD или ALD Pro/FreeIPA, которое будет установлено: • Незащищенное соединение (LDAP); • Защищенное соединение по протоколу LDAP + StartTLS; • Защищенное соединение по протоколу LDAPS (SSL), **Важно!** Соединение без сертификатов небезопасно**.** При установке любого защищенного соединения дополнительно можно загрузить файл с сертификатом в формате .pfx **Важно!** Если загружаемый файл содержит несколько клиентских сертификатов, то Система будет работать с первым клиентским сертификатом и его закрытым ключом. Для корректной работы необходимо формировать файл с одним клиентским сертификатом. **Примечание.** Для Samba DC использование незащищенного соединения не поддерживается.

Параметр	Описание
	Важно! Синхронизация с использованием защищенного соединения поддерживается только для Active Directory и Samba DC. Для Samba DC можно выбрать только защищенное соединение про протоколу LDAP + StartTLS.
Сертификат сервера	Загрузка файла сертификата в pem-формате. **Примечание.** Для Samba DC данная настройка недоступна.
Клиентский сертификат	Загрузка файла сертификата в pem-формате. При использовании клиентского сертификата необходимо дополнительно загрузить файл с закрытым ключом клиентского сертификата. **Примечание.** Для Samba DC данная настройка недоступна.
Закрытый ключ клиентского сертификата	Загрузка файла с ключом в pem-формате. **Примечание.** Подробнее см. "Получение клиентского сертификата и сертификата сервера". **Примечание.** Для Samba DC данная настройка недоступна.
Использовать протокол Kerberos	Признак того, что для аутентификации используется протокол взаимной аутентификации клиента и сервера Kerberos. Подробнее см. "Особенности подключения и синхронизации по LDAPS с использованием протокола Kerberos"**Примечание:** При синхронизации с ALD (Astra Linux Directory) рекомендуется активировать данный параметр .**Важно!** Включать это признак стоит только отдельно от признака **Использовать клиентский сертификат для аутентификации.** Они являются взаимоисключающими, и при одновременном включении соединение работать не будет.
Глобальный LDAP-порт	Порт для подключения глобального LDAP-каталога. **Примечание:** данная настройка доступна только для Active Directory и Samba DC
LDAP-порт	Порт для подключения доменного каталога
Использовать глобальный каталог	Признак использования глобального каталога **Примечание:** данная настройка доступна только для Active Directory и Samba DC

Параметр	Описание

LDAP-запрос	**Примечание:** данная настройка обязательна только для Active Directory и Samba DC.
	Атрибуты фильтрации, являющиеся полным путем к указанному каталогу. При этом может быть указан только один каталог в организационной структуре Active Directory, Samba DC, Domino Directory, Astra Linux Directory или Astra Linux Directory Pro/FreeIPA.
	
	Для оптимизации поиска вы можете использовать отдельные уровни иерархии базы:
	
	`C- countryName`
	`O- organizationName`
	`OU- organizationalUnitName`
	`DC- domainComponent`
	`CN- commonName`
	
	Пример для AD, Samba DC, ALD, ALD Pro и FreeIPA: чтобы использовать в качестве базы поиска ветку `Users`, расположенную в домене компании, необходимо ввести:
	`cn=users,dc=company,dc=com`
	
	Пример для DD: запрос может содержать одно или несколько значений:
	`o=company,ou=department,ou=group`
	
	Важно! Для корректной работы частичной синхронизации с использованием LDAP-запроса необходимо сначала синхронизироваться со всем LDAP-каталогом (`dc=company,dc=ru`), а после этого выполнить синхронизацию с использованием более узкого LDAP-запроса. При этом для обновления информации о группах/персонах/компьютерах для этой синхронизации необходимо заново провести полную синхронизацию со всем LDAP-каталогом, а затем частичную с использованием LDAP-запроса.

Использовать клиентский сертификат для аутентификации	Признак использования клиентского сертификата для защищенных типов соединений вместо ввода пароля. **Важно!** Включать это признак можно только отдельно от признака **Использовать протокол Kerberos.** Они являются взаимоисключающими, и при одновременном включении соединение работать не будет.
Анонимный доступ	Признак того, что подключение к LDAP-серверу осуществляется от имени анонимного пользователя. **Примечание.** Для Astra Linux Directory Pro и FreeIPA данная настройка недоступна.

Параметр	Описание
Логин	Логин для доступа к серверу синхронизации
Пароль	Пароль учетной записи для доступа к серверу синхронизации

4. Нажмите **Проверить соединение**, чтобы выполнить контрольную проверку подключения к серверу.
5. Нажмите **Сохранить**.

> **Примечание.**
>
> Начиная с версии Traffic Monitor 7.5, заполнять значения полей `DnsRootDefault` и `NetbiosNameDefault` в конфигурационном файле **adlibitum.conf** не требуется. AUTH-контакты персон будут добавлены автоматически при синхронизации с ALD, ALD Pro или FreeIPA. Значения данных параметров, указанные в предыдущих версиях Traffic Monitor, будут проигнорированы.

> **Важно!**
>
> При синхронизации с ALD рекомендуется активировать параметр **Использовать протокол Kerberos** в настройках LDAP-сервера. Если этот параметр отключен, синхронизация с ALD будет работать только при включении параметра **Анонимный доступ**. При этом не будет возможности аутентификации пользователя, импортированного из ALD.

Поддержка шифрованного соединения

Передача данных по защищенному соединению для синхронизации с серверами LDAP возможна при выборе типов соединений:

- LDAP с функцией StartTLS, позволяющей установить защищенное соединение поверх существующего незащищенного по портам 389 или 3268 при использовании глобального каталога. При этом синхронизация с AD и Samba DC возможна как с использованием протокола Kerberos, так и анонимного доступа.
- LDAPS, при котором передача данных с осуществляется сразу по защищенному каналу: по портам 636 или 3269 при использовании глобального каталога.

Редактирование подключения к серверу

Чтобы отредактировать подключение к серверу:

1. Перейдите в раздел **Управление -> LDAP-Синхронизация**.
2. Щелчком левой кнопки мыши выберите требуемый сервер.
3. На панели инструментов нажмите  **Редактировать**.
4. Измените параметры подключения (см. "Создание подключения к серверу").

5. Нажмите **Проверить соединение**, чтобы выполнить контрольную проверку подключения к серверу.
6. Нажмите **Сохранить**.

Удаление подключения к серверу

Чтобы удалить существующее подключение к серверу, выполните следующие шаги:

1. Перейдите в раздел **Управление > LDAP-Синхронизация**.
2. Щелчком левой кнопки мыши выберите требуемый сервер.
3. На панели инструментов нажмите  **Удалить**.

> **Примечание:**
>
> Чтобы удалить несколько подключений сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить**.

4. В появившемся окне нажмите **Да**.

Запуск синхронизации с сервером вручную

Чтобы запустить синхронизацию с сервером вручную, выполните следующие шаги:

1. Перейдите в раздел **Управление -> LDAP-Синхронизация**.
2. Щелчком левой кнопки мыши выберите требуемый сервер.
3. На панели инструментов нажмите  **Запустить синхронизацию**.

Информация о результатах синхронизации будет показана в строках *Последняя синхронизация, Статус синхронизации и Следующая синхронизация*.

> **Примечание:**
>
> Если для подключения в качестве атрибута ***Период синхронизации*** выбраны значения *Ежеминутно*, *Ежечасно*, *Ежедневно* или *Еженедельно*, автоматическая синхронизация будет выполняться с указанной периодичностью после последнего ручного запуска.

> **Важно!**
>
> Синхронизация будет производиться по времени часового пояса сервера Traffic Monitor. Если консоль управления расположена в другом часовом поясе, то при задании времени синхронизации необходимо сделать поправку на разницу во времени между часовыми поясами сервера и консоли управления.

Необходимо проверить соединение с LDAP-серверами после обновления с более ранних версий. Для этого:

1. Щелчком левой кнопки мыши выберите требуемый сервер.
2. Нажмите **Проверить соединение.**

Информация о результатах проверки будет показана в сообщении. В случае ошибки настройте параметры подключения.

4.9.2 Управление пользователями Системы и их ролями

Для работы пользователя в Системе используются следующие сущности:

- *Пользователь* – учетная запись (см. "Пользователи");
- *Роль* – набор привилегий, которые могут быть выданы пользователю (см. "Задание пользователю роли");
- *Область видимости* – группа конкретных атрибутов объектов перехвата, к которым могут иметь доступ только указанные пользователи (см. "Области видимости").

Пользователи

Настройка списка пользователей Системы выполняется в разделе **Управление -> Управление доступом**, на вкладке **Пользователи**.
В рабочей области расположен список пользователей Системы, панель инструментов и раскрывающееся меню.
В списке пользователей отображаются пользователи Системы.
Панель инструментов содержит набор инструментов для работы с пользователями.
Раскрывающееся меню определяет количество пользователей, отображаемых на странице.
Атрибуты учетной записи приведены в таблице:

Параметр	**Описание**
Логин	Имя учетной записи пользователя
Полное имя	ФИО пользователя
Email	Адрес электронной почты пользователя
Роли	Список ролей пользователя
Области видимости	Список областей видимости пользователя
Описание	Примечание к учетной записи
Статус	Признак того, является ли учетная запись пользователя активной или выключенной

Вы можете выполнять следующие действия при управлении пользователями:

- Создание учетной записи пользователя
- Редактирование учетной записи пользователя
- Удаление учетной записи пользователя
- Изменение пароля учетной записи пользователя
- Изменение статуса учетной записи пользователя
- Импорт учетной записи пользователя
- Задание пользователю роли

- Задание пользователю области видимости

Создание учетной записи пользователя

Чтобы создать учетную запись:

1. Перейдите в раздел **Управление** -> **Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. На панели инструментов нажмите **Создать пользователя**.
4. В открывшемся окне укажите параметры учетной записи:

Параметр	Описание
Логин	Имя учетной записи пользователя
Статус	Признак того, является ли учетная запись пользователя активной или выключенной
Пароль	Пароль учетной записи
Подтверждение пароля	Пароль учетной записи
E-mail	Адрес электронной почты пользователя
Полное имя	ФИО пользователя
Описание	Примечание к учетной записи

5. Нажмите **Сохранить**.

Редактирование учетной записи пользователя

Чтобы изменить параметры существующей учетной записи:

1. Перейдите в раздел **Управление** -> **Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите **Редактировать пользователя**.
5. В открывшемся окне измените параметры учетной записи (см. "Пользователи").
6. Нажмите **Сохранить**.

Удаление учетной записи пользователя

Чтобы удалить учетную запись:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.

4. На панели инструментов нажмите  **Удалить пользователя**.

> **Примечание:**
>
> Чтобы удалить несколько учетных записей сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить пользователя**.

5. В появившемся окне нажмите **Да**.

Изменение пароля учетной записи пользователя

Чтобы изменить учетную запись:

1. Перейдите в раздел **Управление** -> **Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите **Сменить пароль**.
5. В открывшемся окне введите новый пароль в полях **Пароль** и **Подтверждение пароля**.
6. Нажмите **Сохранить**.

Изменение статуса учетной записи пользователя

Чтобы изменить статус учетной записи:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите  и выберите **Активировать пользователя** или **Деактивировать пользователя**.

> **Примечание:**
>
> Вы можете изменить статус любой учетной записи, кроме **Administrator**.

Импорт учетной записи пользователя

Для удобства создания пользователей вы можете импортировать учетные записи из Active Directory, Samba DC, Domino Directory, Astra Linux Directory, Astra Linux Directory Pro или FreeIPA.

> **Важно!**
>
> Если в вашем браузере используется расширение AdBlock, то перед импортом учетных записей необходимо отключить данное расширение, так как оно блокирует импорт.

Чтобы импортировать учетную запись:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. На панели инструментов нажмите **Добавить пользователя из LDAP**.
4. В открывшемся окне укажите LDAP-сервер, на котором хранится требуемая учетная запись пользователя.

   > **Примечание.**
   >
   > Для удобства поиска учетной записи введите часть названия учетной записи в поле **Строка поиска** и нажмите **Поиск**.

5. Установите флажок для требуемых пользователей.
6. Нажмите **Сохранить**.

Задание пользователю роли

Чтобы задать пользователю роль:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите .
5. В списке выберите **Задать роль** (см. "Роли").
6. Нажмите **Сохранить**.

Задание пользователю области видимости

Чтобы задать пользователю область видимости:

1. Перейдите в раздел **Управление** -> **Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. Щелчком левой кнопки мыши выберите нужную учетную запись в списке пользователей.
4. Установите пользователю область видимости из списка **Области видимости** (см. "Области видимости"). Пользователю станут доступны события и снимки экрана, удовлетворяющие критериям тех областей видимости, которые ему назначены. При этом:
   a. если пользователю не задана ни одна область видимости, то для него будут недоступны все события перехвата и все снимки экрана и доступны все группы персон;
   b. если пользователю назначено несколько областей видимости, то их критерии будут объединены логическим ИЛИ.
   c. чтобы предоставить пользователю доступ ко всем событиям с любыми критериями, назначьте область видимости **Полный доступ**.
5. Нажмите **Сохранить**.

Роли

Для контроля избыточности доступа к настройкам системы, политик разных структурных отделов, объектов перехвата и прочей важной информации, в InfoWatch Traffic Monitor предусмотрена ролевая система разграничения прав доступа с областью видимости.

Назначение ролей пользователям описано в статье "Задание пользователю роли".

Изначально в системе присутствуют две предустановленные роли и два предустановленных пользователя – роли **Администратор** и **Офицер безопасности**, которые назначены, соответственно, пользователям Administrator и Officer.

Роль **Администратор** предоставляет возможность проводить первичную настройку системы (Управление пользователями, ролями, областями видимости, лицензиями и синхронизацией с LDAP-каталогами).

Роль **Офицер безопасности** обладает всеми правами, кроме первичной настройки.

Настройка списка ролей выполняется в разделе **Управление** -> **Управление доступом**, на вкладке **Роли**.
В рабочей области расположен список ролей, панель инструментов и раскрывающееся меню.
Атрибуты роли приведены в таблице:

Параметр	**Описание**
Название	Имя роли
Пользователи	ФИО пользователя
Описание	Примечание к роли

Вы можете выполнять следующие действия при управлении ролями:

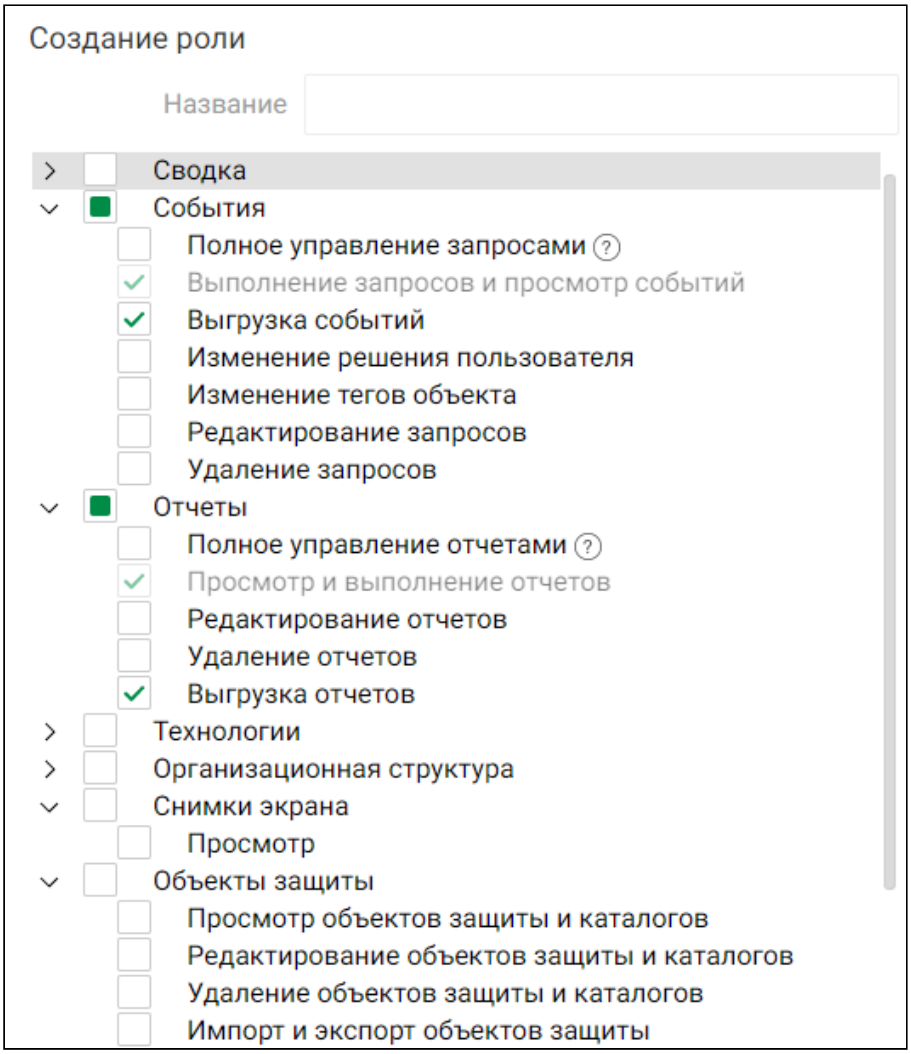
- Создание роли
- Редактирование роли
- Удаление роли

Создание роли

Чтобы создать новую роль, выполните следующие действия:

1. Перейдите в раздел **Управление** -> **Управление доступом**.
2. Перейдите на вкладку **Роли**.
3. На панели инструментов нажмите  **Создать роль**.
4. В открывшемся окне установите флажки напротив привилегий, которые требуется задать в выбранной роли.

> **Примечание.**
>
> Чтобы развернуть или свернуть список, нажмите кнопки  или соответственно.



Примечание:

Привилегии **Просмотр ролей** и **Просмотр областей видимости** доступны по умолчанию при назначении **Ролей** и **Областей видимости**.

5. Нажмите **Сохранить**.

Редактирование роли

Чтобы изменить параметры существующей роли, выполните следующие действия:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Роли**.
3. В списке ролей щелчком левой кнопки мыши выберите требуемую роль.
4. На панели инструментов нажмите **Редактировать роль**.
5. В открывшемся окне установите флажки на те привилегии, которые надо включить, или снимите флажки у тех привилегий, которые надо выключить для выбранной роли.

> **Примечание:**
>
> Чтобы развернуть или свернуть список, нажмите кнопки ▶ или ◢ соответственно.

> **Примечание:**
>
> Привилегии **Просмотр ролей** и **Просмотр областей видимости** доступны по умолчанию при назначении **Ролей** и **Областей видимости**.

6. Нажмите **Сохранить**.

Удаление роли

Чтобы удалить роль:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Роли**.
3. В списке ролей щелчком левой кнопки мыши выберите требуемую роль.
4. Нажмите  **Удалить роль**.

> **Примечание:**
>
> Чтобы удалить несколько ролей сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить роль**.

5. В появившемся окне нажмите **Да**.

> **Примечание:**
>
> Вы можете изменить любую роль, кроме роли **Администратор** и **Офицер безопасности**.

Области видимости

Области видимости позволяют осуществлять дополнительный контроль доступа к перехваченным объектам. Область видимости создается из атрибутов объектов перехвата. Пользователю будут видны только те события, атрибуты которых совпадают с атрибутами, заданными в области видимости. Для одного пользователя может быть задано несколько областей видимости.

> **Пример:**
>
> Пользователю officer присвоена область видимости с Персоной: *Иванов* и Тегом: *1*. Пользователь officer сможет просматривать только события с участием персоны *Иванов* и помеченные тегом *1*.

Назначение областей видимости пользователям описано в статье "Задание пользователю области видимости".

Настройка списка областей видимости выполняется в разделе **Управление** -> **Управление доступом** на вкладке **Области видимости**.

В рабочей области расположен список областей видимости, панель инструментов и раскрывающееся меню.

В списке областей видимости отображаются области видимости пользователей Системы.

Панель инструментов содержит набор инструментов для работы с областями видимости:

-  - создать новую область видимости. чтобы отредактировать область видимости, щелкните на ней указателем мыши.
-  - удалить ранее созданную область видимости. Предустановленную область видимости удалить невозможно.

Раскрывающееся меню определяет количество областей видимости, отображаемых на странице.

Информация об области видимости включает в себя ее название и краткое описание.

Вы можете выполнять следующие действия при управлении областями видимости:

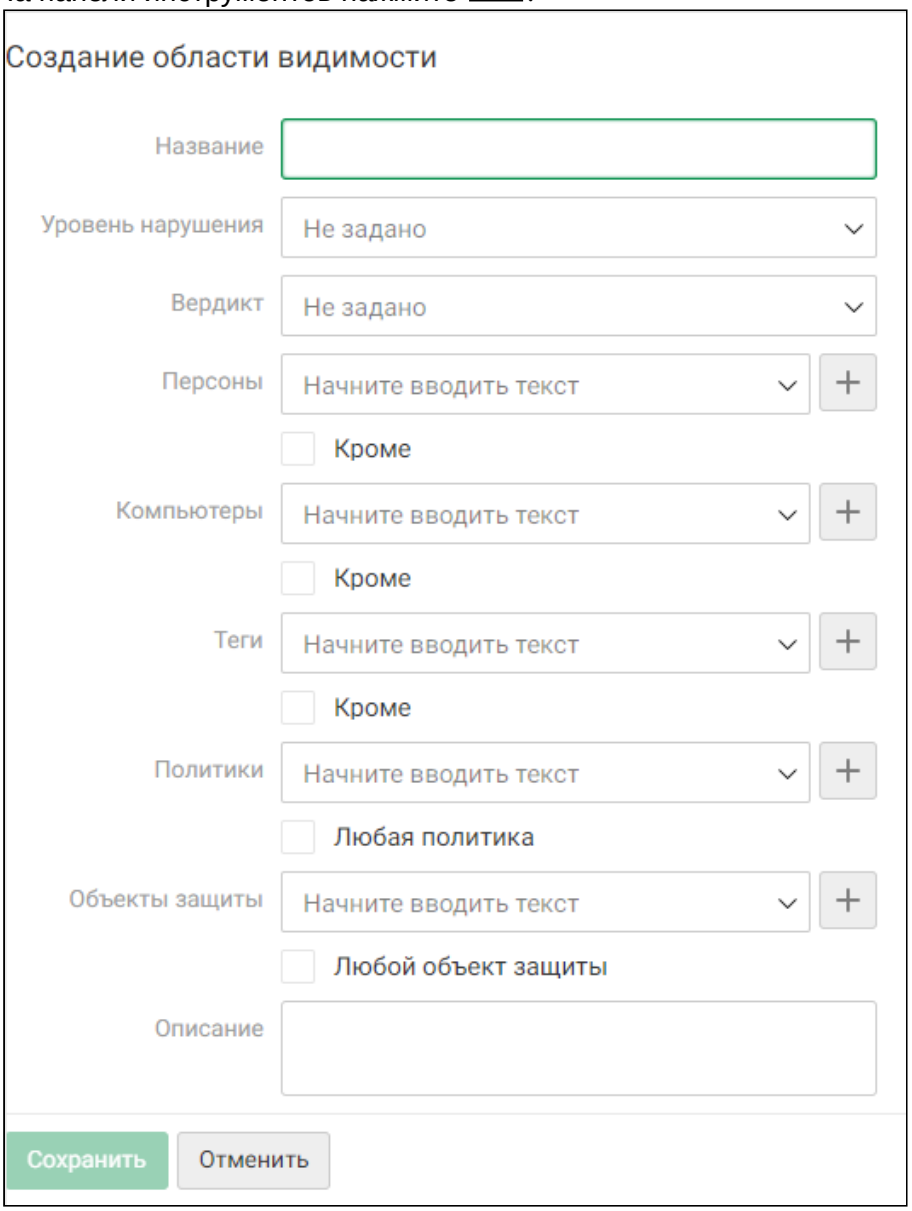
- Создание области видимости
- Редактирование области видимости
- Удаление области видимости

Создание области видимости

Чтобы создать область видимости:

1. Перейдите в раздел **Управление** -> **Управление доступом** .
2. Перейдите на вкладку **Области видимости**.

3. На панели инструментов нажмите [+].



4. В открывшемся окне заполните требуемые поля следующим образом:

1. *Название* – введите имя области видимости.
2. *Уровень нарушения* – выберите из раскрывающегося списка.
3. *Вердикт* – выберите из раскрывающегося списка.
4. *Персоны* – на выбор:
    a. введите первые символы имени пользователя, группы или статуса и выберите требуемое значение из выпадающего списка
    или
    b. нажмите [+] и в появившемся окне установите нужные флажки на вкладках **Персоны**, **Группы**, **Статусы**. Нажмите **Добавить**.
5. *Компьютер* – аналогично пункту d.
6. *Теги* – на выбор:
    a. введите первые символы названия тега или

b. нажмите  и в появившемся окне установите нужные флажки в списке тегов. Нажмите **Добавить**.

Чтобы исключить в результатах отбора событий и снимков экрана некоторые персоны, компьютеры или теги, установите флажок **Кроме** и заполните появившееся поле, как описано в предыдущем подпункте. Если в одной области видимости выбраны взаимоисключающие правила, то все события для данного пользователю будут недоступны.

7. *Политика* – аналогично пункту f.
8. *Объект защиты* – аналогично пункту f.
9. *Описание* – введите текст краткого описания.

> **Примечание:**
>
> Атрибуты событий, снимков экрана и персон, указанные в пунктах b-h, будут объединены логическим И, а вводимые значения в составе атрибута – логическим ИЛИ.

- Нажмите **Сохранить**.

> **Пример**
>
> Если в любом поле области видимости не выбрано ни одного значения, то при фильтрации событий оно учтено не будет. Таким образом, если не выбрано ни одной персоны, то пользователю будут доступны события всех персон.

Редактирование области видимости

Чтобы изменить параметры области видимости:

1. Перейдите в раздел **Управление** -> **Управление доступом**.
2. Перейдите на вкладку **Области видимости**.
3. Выберите нужную область видимости щелчком левой кнопки мыши.
4. В открывшейся области измените параметры области видимости аналогично действиям по ее созданию (см. "Создание области видимости").
5. Нажмите **Сохранить**.

Удаление области видимости

Чтобы удалить область видимости:

1. Перейдите в раздел **Управление** -> **Управление доступом**.
2. Перейдите на вкладку **Области видимости**.
3. На панели инструментов нажмите .

> **Примечание:**

Чтобы удалить несколько областей видимости сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить**.

4. В появившемся окне нажмите **Да**. При этом область видимости будет удалена у всех персон, к которым привязана.

4.9.3 Управление лицензиями

Важно!

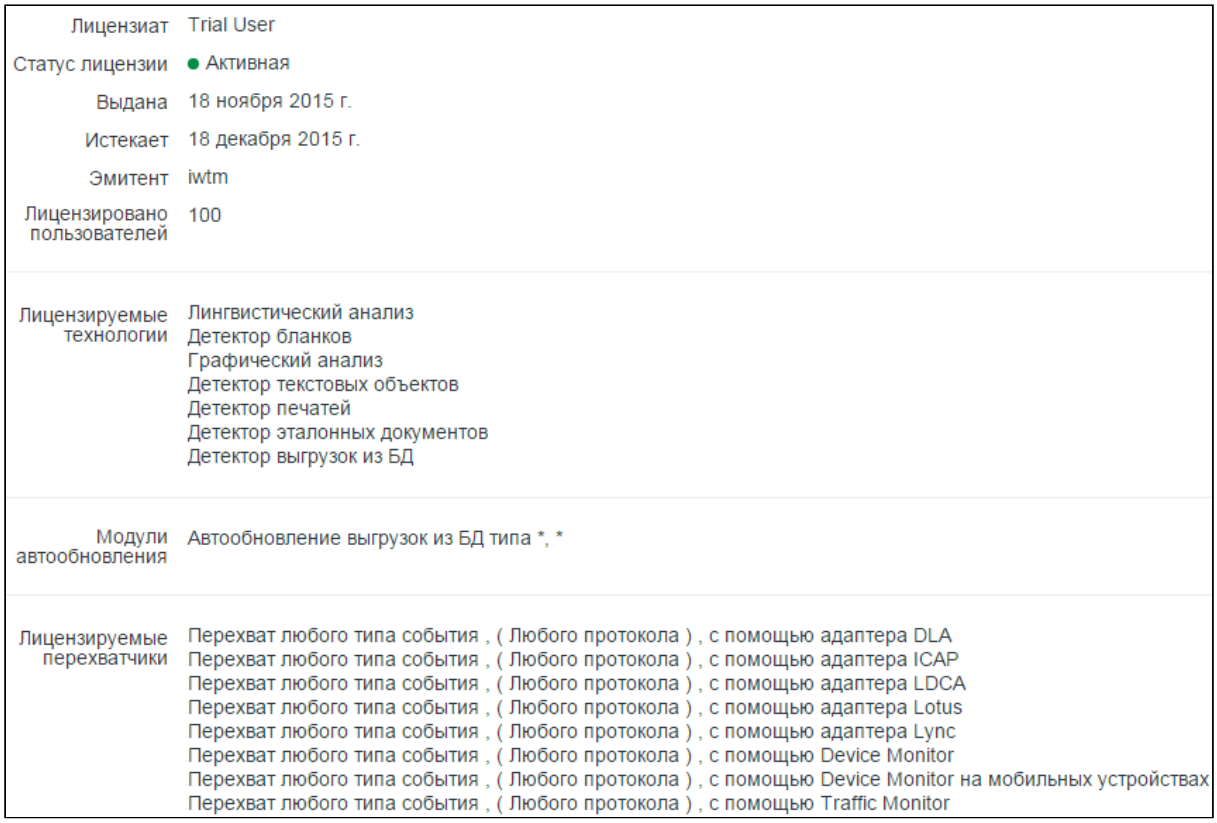
Описание лицензирования Системы приведено в документе "*InfoWatch Traffic Monitor. Руководство администратора*", статья "Лицензирование".

Работа с лицензиями ведется в Консоли управления, в разделе **Управление** –> **Лицензии**:

- в левой части рабочей области Консоли управления расположены список лицензий и панель управления лицензиями.
- в центральной части рабочей области отображается информация о выбранной в списке лицензии.

Примечание:

Редактирование лицензии недоступно. Есть возможность только загрузить новую или удалить ранее созданную лицензию.



Доступны следующие действия с лицензиями:

- Установка лицензии
- Удаление лицензии
- Запрос лицензии

Проверка валидности лицензии

Сведения о лицензируемых технологиях и перехватчиках, а также о статусе, сроке истечения и количестве лицензированных пользователей приведены в правой части рабочей области раздела **Управление –> Лицензии**.

Чтобы проверить валидность лицензии:

1. Перейдите в раздел **Управление -> Лицензии**.
2. Убедитесь, что значение поля **Истекает** содержит дату, которая еще не наступила.
3. Убедитесь, что значение поля **Лицензиат** соответствует значению параметра Licensee конфигурационного файла **license.conf**, расположенного в директории `/opt/iw/tm5/etc`.

Установка лицензии

Чтобы установить лицензионный ключ:

1. Перейдите в раздел **Управление -> Лицензии**.
2. На панели инструментов нажмите  **Добавить лицензию**.
3. В открывшемся окне нажмите **Загрузить**.

4. В открывшемся диалоговом окне выберите полученный по запросу файл **licence.lic** и нажмите **Открыть**.
   В открывшемся окне **Добавление лицензии** отобразятся сведения о лицензии и лицензируемых технологиях и перехватчиках.
5. Нажмите **Добавить**.
6. В открывшемся диалоговом окне нажмите **Да**.

Страница браузера перезагрузится, и новая лицензия будет добавлена в список установленных лицензий. Старую лицензию Вы можете оставить или удалить.

Удаление лицензии

Чтобы удалить лицензионный ключ:

1. В списке лицензий выделите целевую лицензию.
2. На панели инструментов нажмите  **Удалить**.

   > **Примечание:**
   >
   > Чтобы удалить несколько лицензий сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите  **Удалить**.

3. В открывшемся окне нажмите **Да**.

Запрос лицензии

Чтобы отправить запрос на получение лицензии:

1. Перейдите в раздел **Управление - Лицензии**.
2. В правом верхнем углу нажмите кнопку **Запросить лицензию**.
3. Отправьте автоматически сформированное письмо, при необходимости указав дополнительную информацию в теле письма.

4.9.4 Состояние системы

Просмотр состояний каждого из серверов, на которых развернута Система, ведется в Консоли управления, в разделе **Управление -> Состояние системы**.
Список индикаторов представлен в виде таблицы для каждого из используемых в Системе серверов:

	Параметр	Детальные данные
🟢	Общая нагрузка Системы	OK - load average: 0.01, 0.05, 0.05
🟢	Количество активных пользователей	USERS OK - 4 users currently logged in
🟢	Наличие ошибок в журнале БД	OK - no errors
🟢	Доступность встроенного агента передачи почты (Postfix или Exim)	SMTP OK - 0.002 sec. response time
🟢	Отклонение системного времени	NTP OK: Offset -0.0113941431 secs
🟢	Ошибки в журнале предупреждений БД	OK - no errors found in log
🟡	Размер журнала предупреждений БД	WARNING - size of PostgresSQL system log is 50265440 [gre…
🟢	Состояние базы данных PostgreSQL	OK - database postgres (0 sec.)
🟢	Свободное место в основном каталоге БД	DISK OK - free space: / 75525 MB (82% inode=97%):
🟢	Свободное место в каталоге событий БД	DISK OK - free space: / 75525 MB (82% inode=97%):
🟢	Доступность сервера	PING OK - Packet loss = 0%, RTA = 0.06 ms
🟢	Свободное место в корневой партиции	DISK OK - free space: / 75525 MB (82% inode=97%):
🟢	Состояние службы синхронизации времени	OK - NTP server is running.
🟢	Состояние службы syslog	OK - 'rsyslogd' is running
🟢	Доступность сервера по SSH	SSH OK - OpenSSH_6.0p1 Debian-4+deb7u3 (protocol 2.0)
🟢	Использование файла подкачки	SWAP OK - 100% free (4157 MB out of 4189 MB)

Для каждого индикатора отображается следующая информация:

- **Статус** – текущее значение индикатора:
  - 🔴 – CRITICAL, значение проверяемого параметра превышает критический порог;
  - 🟡 – WARNING, значение проверяемого параметра находится в зоне предупреждения (если такая предусмотрена);
  - 🟢 – OK, значение параметра находится в норме.
- **Параметр** – название индикатора.
- **Детальные данные** – подробная информация о результатах проверки.

> **Важно!**
>
> Если значение индикатора получить не удалось, то считается, что текущее значение индикатора превышает пороговое значение.

Показатели обновляются с периодичностью:

- каждые 5 минут – для параметров:
  - Ошибки в журнале предупреждений БД/DB Alert Log Errors
  - Использование файла подкачки/Swap usage
  - Размер журнала предупреждений БД/DB Alert log Size
- каждые 10 минут – для параметров:
  - Доступность сервера по SSH/SSH availability
  - Состояние базы данных/Database Status
- каждые 360 минут – для параметра Отклонение системного времени/NTP time deviation
- каждые 30 минут – для всех остальных параметров

Если требуется обновить показатели вручную, нажмите **Обновить**.

Настройка уведомлений

Чтобы настроить параметры отправки уведомлений о состоянии системы:

1. Перейдите в раздел **Управление** – **Состояние системы**.
2. Нажмите **Настроить уведомления**.
3. Включить опцию **Разрешить уведомления**.
4. Укажите значения для следующих параметров:

Параметр	Описание
Почтовый префикс	Почтовый префикс используется для удобства сортировки почтовых сообщений из разных систем мониторинга. Введенное значение будет добавлено к началу строки поля «Тема» отправляемых почтовых сообщений. Значение по умолчанию: `IWTM`
Получатели	Почтовый адрес получателя/получателей. Значение по умолчанию: `nagios@localhost`

5. Нажмите *Отправить тестовое сообщение*, чтобы проверить корректность введенных настроек.
6. Нажмите **Сохранить**.

Уведомления будут содержать следующую информацию:

- Название индикатора;
- Имя сервера, на котором контролируемый индикатор превысил пороговое значение;
- IP-адрес этого сервера;
- Текущее состояние индикатора;
- Дата и время превышения порогового значения индикатора;
- Системное сообщение от источника.

Важно!

Уведомления мониторинга будут отправлены только, если используется внешний почтовый сервер, на котором настроен метод аутентификации PLAIN.

4.9.5 Сбор диагностических данных, сохранение логов служб

Сбор диагностических данных и сохранение логов служб выполняются в разделе **Управление -> Службы.**

Режим сбора данных	Описание
Обычный	Сбор логов Системы, конфигурационной информации и данных о начальной установке

Режим сбора данных	Описание
Расширенный	Сбор детальной отладочной информации, включая информацию об ошибках, о содержимом рабочей памяти процессов и ситуациях их аварийного завершения

Диагностическая информация будет собрана из следующих источников:

Тип данных	Путь к файлам

Логи	`/var/log/infowatch/*.log`
	`/var/log/nagios3/nagios.log`
	`/var/log/iwtm-*.log`
	`/var/log/infowatch/install/*`
	`/var/log/infowatch/update/*`
	`/u01/postgres/pg_log/* -` Если установлена СУБД PostgreSQL

Конфигурационная информация	`/opt/iw/tm5/etc/*.conf`
	`/opt/iw/tm5/etc/scripts/*.lua`
	`/opt/iw/tm5/etc/config/lua/vademecums/*.info`
	`/opt/iw/tm5/etc/config/lua/vademecums/vademecum.list`
	`/etc/nagios3/*`

Логи и скрипты начальной установки системы	`/root/iw*`

Чтобы собрать диагностическую информацию и скачать отчет:

1. Перейдите в раздел **Управление -> Службы**.
2. Выберите нужный сервер Traffic Monitor в левой области.
3. Нажмите **Собрать данные**.
4. Выберите режим, установив маркер в одном из полей: *Обычный* или *Расширенный*.
5. Нажмите **Запустить**.
6. Дождитесь завершения сборки диагностической информации.
7. Скачайте архив отчет по результатам последней диагностики по ссылке **Доступен результат последнего сбора данных** в формате `diagnostic_report_dd-mm-yyyy_hh-mm-ss.`

Важно!

В случае, если диагностика ранее не проводилась, скачивание результатов последней диагностики доступно не будет.

Чтобы сохранить логи службы:

1. Выберите нужный сервер Traffic Monitor в левой области.
2. Нажмите **Сохранить** в колонке **Логи** напротив одной или нескольких запущенных служб, логи которой необходимо сохранить. Сохранить логи остановленной службы невозможно.

Примечание:

При работе в среде ОС Microsoft Windows возможно появление пустого архива с логами работы службы. В этом случае необходимо установить архиватор *UnZip* (for Windows) и распаковать архив через него.

4.9.6 Аудит действий пользователя

Система предоставляет возможность отслеживать действия пользователя в Консоли управления.

Просмотр событий аудита и фильтры поиска по событиям выполняются в разделе **Управление - Аудит**.

Система фиксирует и отображает в разделе **События аудита** следующую информацию:

- вход в Систему, выход из Системы, переход из другого продукта InfoWatch, временная блокировка авторизации;
- управление объектами, отвечающими за разграничение доступа (пользователи, роли, области видимости);
- действия пользователя по настройке периметров;
- действия пользователя с организационной структурой (персоны, группы, компьютеры);
- действия пользователя с объектами Системы (запросы, отчеты, почтовые уведомления, политики, правила, элементы технологий и т.д.);
- изменение конфигурации Системы (создание, редактирование, отмена);
- изменение объектов Системы внешними системами.

Важно!

Не фиксируются в событиях аудита:

- Изменения элементов вследствие отмены конфигурации. В данном случае будет создано только событие отмены конфигурации;
- Создание групп, персон или компьютеров в процессе синхронизации с LDAP-сервером, а также старые их значения при внесении изменений пользователем;
- Любые изменения виджета отчета, кроме смены названия.

Не будут изменены зарегистрированные в ранних версиях Системы события аудита для действий с правилами политик, персонами, группами и компьютерами после обновления на текущую версию.

Работа с событиями аудита описана в следующих разделах:

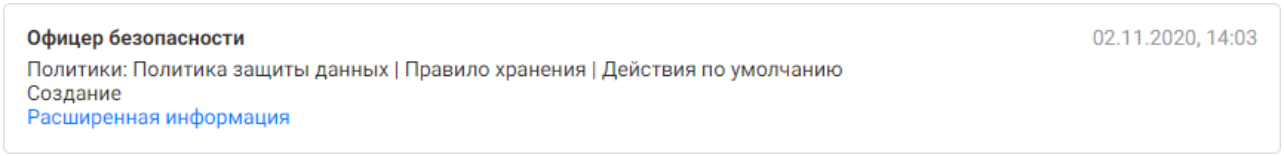
- События аудита
- Расширенная информация о событиях аудита
- Фильтрация и поиск событий аудита

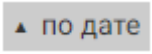
События аудита

Область События аудита находится в разделе **Управление - Аудит**.

Область **События аудита** показывает результаты **Фильтров поиска** и представляет из себя список событий аудита в виде плашек со следующими атрибутами:

- Имя пользователя, осуществившего действие;
- Имя объекта, над которым осуществлялось действие;
- Тип действия, которое было произведено пользователем;
- Дата и время зарегистрированного действия пользователя;
- Расширенная информация о событии аудита.



Чтобы отсортировать события аудита по дате создания, нажмите 

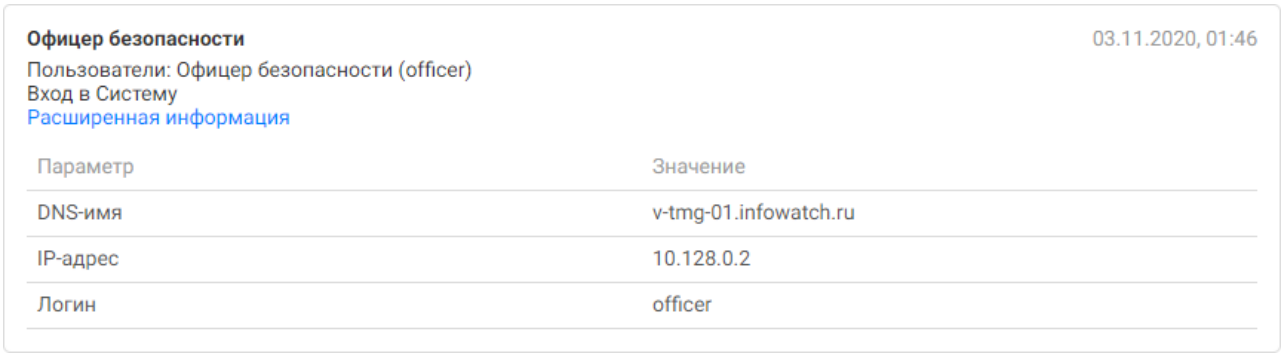
в левом верхнем углу.

Расширенная информация

Событие аудита может содержать дополнительную информацию: перечень измененных параметров, их старые и новые значения, дата внесения изменений. Чтобы ознакомиться с этими данными, нажмите **Расширенная информация** на интересующей плашке.

Например, при входе пользователя в Систему параметры события будут следующими:

- DNS-имя компьютера, с которого произошел вход в Систему;
- IP-адрес компьютера, с которого произошел вход в Систему;
- Имя пользователя, который произвел вход в Систему.



Важно!

Данные события аудита могут варьироваться в зависимости от *Объекта* и *Действия*.

Фильтрация и поиск

Для отображения нужных событий аудита можно воспользоваться полнотекстовым поиском или фильтрами в области **Фильтры поиска** раздела **События аудита**:

1. Введите полное имя интересующего объекта, содержащее хотя бы три буквы, в строке поиска. Допускается ввести первые три буквы имени, а затем использовать символ * для поиска длинных словоформ.
2. Если необходимо, выберите имя пользователя из выпадающего списка атрибутов **Пользователь** (см. "Управление пользователями Системы и их ролями").
3. Если необходимо, выберите действие пользователя из выпадающего списка атрибутов **Действие**.
4. Если необходимо, выберите объект в Системе из выпадающего списка атрибутов **Объект**.
5. Если необходимо, выберите атрибут **Дата** и далее:
    a. **Все время**, если нужен список событий, созданных за все время
    или
    b. **Период**, затем укажите даты начала и конца периода, за который будут показаны события аудита, и нажмите **Применить**.

Допускается использовать и строку поиска, и несколько или все атрибуты фильтра одновременно. При этом стоит учитывать, что найденные события аудита будут удовлетворять каждому установленному значению атрибутов и запросу в поисковой строке.

Для рационального использования свободного места в Базе данных можно установить **Период хранения событий аудита (дни)**, по прошествии которого события будут удалены.

> **Важно!**
>
> У событий аудита и событий Traffic Monitor может быть установлен разный срок хранения. Поэтому, если у событий аудита этот срок больше, то могут быть события аудита без событий Traffic Monitor, так как последние могут быть уже удалены.

4.9.7 Контроль целостности

Контроль целостности предназначен для отслеживания состояния системных файлов. Первичные эталонные суммы формируются Системой автоматически.

Контроль целостности системных файлов описан в следующих разделах:

- Ручная проверка целостности
- Автоматическая проверка целостности
- Принятие результата за эталонный

Ручная проверка целостности

Чтобы проверить целостность системных файлов:

1. Перейдите в раздел **Управление** - **Контроль целостности**;
2. В центральной части рабочей области нажмите **Проверить целостность**.

Примечание:

В процессе проверки целостности будет отображаться сообщение **Выполняется проверка целостности**. По окончании проверки будет выведено сообщение с датой и временем последней проверки.

Автоматическая проверка целостности

Чтобы настроить автоматическую проверку целостности системных файлов:

1. Перейдите в раздел **Управление** - **Контроль целостности**;
2. В центральной части рабочей области включите настройку **Автоматическая проверка**.
3. В поле **Проверять ежедневно в** установите время проверки целостности при помощи стрелок **вверх** и **вниз**.
4. Нажмите **Сохранить**.

Принятие результата за эталонный

Чтобы принять результат проверки целостности как эталонный:

1. Перейдите в раздел **Управление** - **Контроль целостности**;
2. В центральной части рабочей области нажмите **Принять результат как эталонный**.

4.9.8 Плагины

Система использует плагины для подключения дополнительных перехватчиков. Расширение позволяет принимать события от внешних перехватчиков, добавлять пользовательские атрибуты событий, автоматически обновлять эталонные выгрузки, а также предоставлять данные внешним системам.

Любые Push API/Public API коннекторы внешних систем, должны быть зарегистрированы в ТМ путем добавления нового плагина.

Плагин представляет собой архив в формате .zip. В состав архива входят:

- папка **licenses**, содержащая файлы лицензий;
- папка **icon**, содержащая файлы с используемыми пиктограммами для регистрируемых контактов и типов событий;
- файл **manifest.json**, содержащий информацию о плагине. Для плагинов, используемых для получения событий, и плагинов, используемых для обновления эталонных выгрузок, состав файла будет различаться.

Примечание:

Имена файлов, входящих в плагин должны содержать только символы латинского алфавита и/или цифры.

Папки **licenses** и **icon** не являются обязательными. Файлы лицензий и файлы с используемыми пиктограммами могут находиться в корне.

Предустановленные плагины **InfoWatch Device Monitor**, **InfoWatch Sample documents Autoupdate Adapter** будут отображаться в консоли Traffic Monitor, только если в Системе установлена действующая лицензия (см. "Управление лицензиями").

Для внешних систем – источников событий файл **manifest.json** должен содержать следующую информацию:

Название	Является обязательным	Описание
Версия	Да	Версия плагина
Идентификатор компании-разработчика	Да	Соответствует названию компании в лицензии
Используемые предустановленные типы событий, контакты и протоколы	Нет	Список предустановленных в Системе типов событий и протоколов, которые перехватываются с помощью данного плагина
Название	Да	Уникальное название плагина
Описание	Нет	Описание плагина
Признак "Предустановленный"	Нет	Входит ли в состав Системы
Регистрируемые типы событий, контакты и протоколы	Нет	Содержит следующие данные: • Тип регистрируемых событий с указанием типа сервиса, к которому он относится; • Протоколы; • Действия; • Код типа перехватчика для плагинов InfoWatch; • Локализации наименований типов событий минимум на одном языке; • Типы регистрируемых контактов и их локализация минимум на одном языке; • Файлы с иконками регистрируемых контактов и типов событий.
Уникальный идентификатор	Да	Уникальный 128-битный идентификатор (UUID) плагина

Для внешних систем – источников эталонных выгрузок файл **manifest.json** должен содержать следующую информацию:

Название	**Является обязательным**	**Описание**
Версия	Да	Версия плагина
Идентификатор компании-разработчика	Да	Соответствует названию компании в лицензии
Название	Да	Уникальное название плагина
Обновляемые типы данных	Да	Список эталонных выгрузок, которые обновляются с помощью данного плагина, с указанием систем-источников данных.
Описание	Да	Описание плагина.
Признак "Предустановленный"	Нет	Входит ли в состав Системы.
Уникальный идентификатор	Да	Уникальный 128-битный идентификатор (UUID) плагина.

Для внешних систем – приемников данных из ТМ файл **manifest.json** должен содержать следующую информацию:

Название	**Является обязательным**	**Описание**
Версия	Да	Версия плагина
Идентификатор компании-разработчика	Да	Соответствует названию компании в лицензии
Название	Да	Уникальное название плагина
Системы-приемники данных	Да	Список идентификаторов систем-приемников данных из ТМ, регистрируемых в рамках данного Плагина.
Описание	Да	Описание плагина.
Признак "Предустановленный"	Нет	Входит ли в состав Системы.

Название	Является обязательным	Описание
Уникальный идентификатор	Да	Уникальный 128-битный идентификатор (UUID) плагина.

В разделе **Плагины** можно осуществлять следующие действия:

- Добавление плагина
- Удаление плагина
- Работа с токенами

Важно!

Плагины и токены удаляются из Системы при удалении схемы БД (см. "Infowatch Traffic Monitor. Руководство по установке", статья "Удаление схемы базы данных"). Для восстановления плагина Device Monitor:

1. Создайте файл **/opt/iw/tm5/www/backend/protected/runtime/first_run** от имени пользователя **iwtm**;
2. Перезапустите процесс **iw_kicker**:
   ```
   iwtm restart kicker
   ```

Остальные плагины необходимо добавить вручную (см. "Добавление плагина").

Добавление плагина

Чтобы добавить плагин:

1. Перейдите в раздел **Управление - Плагины**;
2. В области **Плагины** нажмите .
3. Нажмите **Добавить**.
4. Просмотрите описание плагина и нажмите **Установить**.

Примечание:

Чтобы обновить плагин, добавьте его обновленную версию.

Удаление плагина

Чтобы удалить плагин:

1. Перейдите в раздел **Управление - Плагины**;
2. В области **Плагины** нажмите .
3. Нажмите **Да**, чтобы подтвердить удаление.

Важно!

Предустановленные плагины удалить нельзя.

Работа с токенами

Токен предназначен для авторизации внешней Системы, использующей Push API (передача в ТМ событий от сторонних перехватчиков) и Public API (загрузка в ТМ эталонных выгрузок из БД и доступ к данным ТМ для сторонних систем). После добавления плагина токен генерируется автоматически (см. "Добавление плагина").

Токен для InfoWatch Device Monitor создается автоматически и доступен в разделе **Управление** -> **Плагины** -> **Токены** Консоли управления.

Система предоставляет возможность следующих действий с токенами:

- Добавление токена
- Редактирование данных токена
- Обновление значения токена
- Копирование токена
- Удаление токена

Добавление токена

Чтобы добавить токен:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите .

Примечание:

Значение токена генерируется автоматически при создании токена и не может быть задано пользователем.

Редактирование данных токена

Чтобы изменить данные токена:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. По двойному нажатию левой кнопкой мыши в графе *Имя* или *Описание* введите нужную информацию.

Обновление значения токена

Если токен скомпрометирован или появилась вероятность его утечки третьим лицам, нужно сгенерировать значение токена заново.

Чтобы обновить значение токена:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите .

Копирование токена

Чтобы скопировать значение токена в буфер обмена:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите .

Удаление токена

Чтобы удалить токен:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите .

4.9.9 Настройка подключения к почтовому серверу

В разделе **Управление** -> **Почтовый сервер** вы можете указать SMTP-сервер, который будет использоваться для отправки уведомлений о сработавших правилах, политиках (см. "Настройка уведомлений") и о состоянии Системы (см. "Состояние системы").

Чтобы настроить подключение:

1. В поле **Почтовый адрес отправителя** укажите адрес, который будет использоваться для отправки уведомлений.
2. Выберите тип сервера. Возможные значения:
   - **Встроенный в Traffic Monitor** – выберите эту опцию, если вы используете локальный почтовый сервер Traffic Monitor с анонимным доступом (Posfix или Exim);
   - **Внешний** – выберите эту опцию, если используется внешний сервер. Например, если в вашей организации не разрешается отправка писем на сторонние сервера без авторизации. При использовании внешнего почтового сервера, на котором настроен метод аутентификации, отличный от PLAIN (например NTLM), почтовые уведомления мониторинга отправляться не будут.
3. Если используется внешний сервер, укажите параметры сервера:
   - **Адрес SMTP-сервера**;

- **Порт**;
- **Логин** – необязательный параметр;
- **Пароль** – необязательный параметр;
- **Шифрование** - при выборе режима с шифрованием соединение происходит по протоколу STARTTLS с NTLM-аутентификацией. Чтобы получать уведомления от системы мониторинга Nagios, выберите режим без шифрования.

4. После того, как вы указали параметры подключения, нажмите **Проверить соединение**.
5. Нажмите **Сохранить**.

4.9.10 Настройка уведомлений

В разделе **Управление** -> **Почтовые уведомления** вы можете настроить шаблоны писем, которые будут отправляться в случае нарушения политики безопасности.

Уведомления могут быть отправлены:

- **Сотруднику**, нарушившему политику безопасности. В случае срабатывания правила сотрудник будет проинформирован, что его действия нарушают политику информационной безопасности. Также при работе Системы "в разрыв" сотрудник своевременно получит информацию, если:
  - письмо заблокировано или задержано в карантине до рассмотрения офицером безопасности;
  - принято решение по задержанному в карантине письму (заблокировать или дослать адресату).
- **Офицеру безопасности**. Получение уведомлений об инцидентах по электронной почте позволяет офицеру безопасности оперативно реагировать на важные инциденты.
- **Другим заинтересованным лицам**, например, руководителю сотрудника, нарушившего политику безопасности.

Чтобы создать новое уведомление, нажмите  на панели инструментов в левой части рабочей области (см. "Создание уведомления"). Добавленные уведомления используются при создании правил политики: в области **Действия при срабатывании правила**, в поле **Отправить почтовое уведомление** нажмите  и выберите нужное уведомление (подробнее см. "Создание правил")

> **Примечание.**
>
> При необходимости вы можете создать или отредактировать уведомление при настройке правила в разделе **Политики**. Копирование и удаление уведомлений доступно только из раздела **Почтовые уведомления**.

При создании/редактировании уведомления вы можете протестировать получившийся шаблон (см. "Тестирование уведомления").

Чтобы скопировать ранее созданное уведомление, выберите уведомление в списке и нажмите  на панели инструментов. Копия уведомления будет добавлена в список.

Для удаления выбранного уведомления используйте кнопку  на панели инструментов.

Примечание.

При этом уведомление будет удалено также из всех политик, в которых оно используется.

Помимо уведомлений, созданных пользователем, в Системе также содержатся предустановленные уведомления (см. "Предустановленные уведомления").

Создание уведомления

Цель:
Создать уведомление для отправки в случае нарушения правил.

Решение:

1. Перейдите в раздел **Управление** ->**Почтовые уведомления**.
2. На панели инструментов в левой части рабочей области нажмите +.
3. В открывшейся форме укажите название уведомления.
4. Выберите получателей уведомления. Возможные варианты:
   - **Отправитель** - отметьте это поле, чтобы создать шаблон для отправки инициатору события;
   - **Произвольные получатели** - отметьте это поле и нажмите +, чтобы добавить получателей. В открывшемся окне перейдите на нужную вкладку:
     - На вкладках **Персоны** и **Пользователи консоли** выберите нужные значения из списка. Вы можете отсортировать значения в списке по имени персоны/пользователя.
     - На вкладке **Электронная почта** вы можете ввести email-адреса получателей, не входящих в список персон и офицеров безопасности.
     - На вкладке **Руководитель отправителя** включите переключатель, если требуется отправлять уведомление руководителю инициатора события.

   После того как вы указали всех требуемых получателей, нажмите **Сохранить**.
5. В области **Шаблон письма для разных вердиктов** перейдите на вкладку с вердиктом, для которого вы хотите создать шаблон. Доступны следующие вкладки:
   - **Разрешено** - в правиле выставлен вердикт *Разрешено*, однако требуется предупредить сотрудника о том, что его действия нарушают политику безопасности;
   - **Заблокировано** - событие заблокировано системой Traffic Monitor при работе "в разрыв" либо агентом Device Monitor в результате применения политики защиты данных на агенте;
   - **Карантин** - SMTP-письмо было задержано системой Traffic Monitor и ожидает решения офицера безопасности (только при работе Системы "в разрыв");
   - **Разблокировано после карантина** - офицер безопасности изменил вердикт события с *Карантин* на *Разрешено*, и SMTP-письмо передано на внешний сервер для досылки получателям (только при работе Системы "в разрыв").
   - **Заблокировано после карантина** - офицер безопасности изменил вердикт события с *Карантин* на *Заблокировано* и заблокировал отправку SMTP-письма (только при работе Системы "в разрыв").
6. Чтобы создать шаблон для выбранного вердикта, включите переключатель **Отправлять** на выбранной вкладке.

7. В открывшейся форме укажите элементы, которые будут входить в тему и тело письма. По умолчанию для темы и тела письма отображается поля ввода, в которых вы можете ввести требуемый текст.
8. Чтобы добавить элемент к теме или телу письма, нажмите **+Добавить** в области **Тема письма** или **Тело письма** соответственно и выберите требуемый элемент из раскрывающегося списка. Доступны следующие элементы:
    - **ID события** - при добавлении в тело письма вы можете также добавить ссылку на событие в Консоли управления;
    - **Отправители** и **Получатели** - из раскрывающегося списка выберите, какие данные отправителей и получателей следует включать в тему или тело письма. По умолчанию добавляется имя и контакт из события;
    - **Политики**, сработавшие в событии. При добавлении в тело письма вы можете указать, какую информацию о политиках нужно добавить: название политики, описание или оба параметра;
    - **Вложения** - из раскрывающегося списка выберите, какая информация о вложениях должна быть включена в тему или тело письма. По умолчанию добавляются имя и размер файла.
    - **Компьютер отправителя**;
    - **Дата перехвата**;
    - **Тип события**;
    - **Вердикт**;
    - **Уровень нарушения**;
    - **Объекты защиты**, сработавшие в событии;
    - **Тема письма**, отправленного сотрудником;
    - **Приложение-источник и приложение-приемник**;
    - **Путь к файлу**;
    - **Имя задания на печать**;
    - **Ресурс**;
    - **Периметры**;
    - **Дата отправки**;
    - **Имя терминальной сессии**;
    - **Адрес вкладки браузера**.

    Чтобы удалить элемент, нажмите × в правом верхнем углу выбранного элемента.
9. Если вы хотите, чтобы письмо содержало также карточку события, включите переключатель **Прикрепить карточку события**. К письму будет прикреплен файл, содержащий текст события и текст, извлеченный из вложений, с подсветкой сработавших объектов защиты.

    > **Важно!**
    >
    > Уведомление с карточкой события будет отправлено всем лицам, указанным в поле **Произвольные получатели**. Вам необходимо самостоятельно отслеживать, чтобы отправка подробной информации о событии на сторонние email-адреса не привела к утечке конфиденциальных данных.

10. Выберите формат карточки: **Microsoft Word** или **PDF**.
11. Укажите, в каком виде текст события с подсветкой должен быть включен в карточку. Возможные значения:

- **В виде фрагментов** - текст события будет выгружен в виде фрагментов, содержащих сработавшие объекты защиты;
- **Весь текст** - будет выгружен весь текст события.

12. После того как вы указали все требуемые параметры, нажмите **Сохранить**.

> **Примечание.**
>
> В процессе создания уведомления вы можете протестировать полученный шаблон (см. "Тестирование уведомления").

Тестирование уведомления

При создании или редактировании уведомления вы можете протестировать полученный шаблон. Для этого:

1. В нижней части рабочей области нажмите **Отправить тестовое письмо**.
2. В открывшемся диалоговом окне укажите:
   - **ID события** - введите идентификатор события, существующего в Системе;
   - **Получатель** - укажите email-адрес, на который нужно отправить тестовое письмо.
3. Нажмите **Отправить уведомление**.

На указанный адрес будет отправлено тестовое письмо с уведомлением, созданное по вашему шаблону.

Предустановленные уведомления

В Системе содержатся следующие предустановленные уведомления:

1. *Уведомление нарушителю*. Содержит шаблоны для отправки инициатору события в случае, если событие:
   - разрешено;
   - заблокировано;
   - помещено на карантин;
   - разблокировано после карантина;
   - заблокировано после карантина.

   Уведомление включает сообщение о текущем состоянии события, а также информацию об отправителях, получателях, дате и времени перехвата, ресурсе и вложениях.
2. *Уведомление офицеру безопасности*. Содержит шаблоны для отправки офицеру безопасности в случае, если событие:
   - разрешено;
   - заблокировано;
   - помещено на карантин.

   В теме письма содержится информация о наличии инцидента, уровне нарушения и вердикте. Тело письма включает следующие данные:
   - ID события;
   - дата и время перехвата;
   - тип события;
   - уровень нарушения;
   - вердикт;

- сработавшие политики;
- сработавшие объекты защиты;
- компьютер отправителя;
- отправители;
- получатели;
- ресурс;
- тема письма;
- вложения.

5 Лицензионная информация

Лицензионная информация для Системы приведена в разделе "Пользовательское лицензионное соглашение".

5.1 Пользовательское лицензионное соглашение

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями пользовательского соглашения перед началом работы с программным обеспечением.
Использование устанавливаемого программного обеспечения означает Ваше безоговорочное согласие с условиями настоящего пользовательского соглашения. Если Вы не согласны с условиями настоящего пользовательского соглашения, Вы должны прервать установку и/или использование программного обеспечения.

1. Предоставление лицензии

1.1. Вам предоставляется неисключительная лицензия на использование программного обеспечения (далее — ПО) (Правообладатель прав на ПО — ООО «Лаборатория ИнфоВотч») в рамках функциональности, описанной в Документации к ПО (Руководство Пользователя, Руководство Администратора, Руководство по Установке), при условии соблюдения Вами всех технических требований, описанных в Документации к ПО, а также всех ограничений и условий использования ПО, указанных в настоящем Соглашении и Договоре, заключенном между Вами и Вашим лицензиаром.

1.2. 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 ознакомительного периода. Любое использование ПО для других целей или по завершении ознакомительного периода запрещено.

1.3. 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.

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

2. Ограничения

2.1. Вы не вправе декомпилировать, дизассемблировать, модифицировать или выполнять производные работы, основанные на ПО, целиком или частично.

2.2. Вам запрещается передавать право на использование ПО третьим лицам.

2.3. Запрещается передавать и предоставлять доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения и Договора, заключенного между Вами и Вашим лицензиаром. Лицензионный ключ является конфиденциальной информацией. Правообладатель оставляет за собой право использовать средства для проверки подлинности установленного у Вас лицензионного ключа.

2.4. Запрещается сдавать ПО в аренду, прокат или во временное пользование, а также разглашать результаты стендовых испытаний ПО.

2.5. Запрещается использовать ПО в противоречащих законодательству целях.

2.6. Правообладатель имеет право заблокировать лицензионный ключ в случае нарушения Вами условий настоящего Соглашения и Договора, заключенного между Вами и Вашим лицензиаром.

2.7. За нарушение интеллектуальных прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством.

2.8. Вы не вправе использовать ПО для любых целей или способом, ограниченным или запрещенным применимым законодательством. Вы самостоятельно несете ответственность за неправомерное использование ПО.

2.9. В случае нарушения Вами какого-либо из условий данного Соглашения или Договора, заключенного между Вами и Вашим лицензиаром, Правообладатель или Ваш лицензиар вправе прервать действие лицензии на использование ПО в любое время без уведомления Вас и без возмещения стоимости ПО или его части.

3. Ограниченная гарантия

3.1. Правообладатель гарантирует работу ПО в соответствии с описанием, изложенным в Документации к ПО. Однако все Ваши требования относительно работоспособности ПО Вы можете предъявлять только к своему лицензиару в рамках заключенного между вами лицензионного договора.

3.2. Вы соглашаетесь с тем, что никакое ПО не свободно от ошибок и Вам рекомендуется регулярно создавать резервные копии своих файлов.

4. Права на интеллектуальную собственность

4.1. Вы соглашаетесь с тем, что исключительные права на любые объекты интеллектуальной собственности, воплощенные в ПО и /или любой предоставленной Вам документации, принадлежат Правообладателю. Ничто в данном Соглашении не предоставляет Вам никаких прав на указанные объекты интеллектуальной собственности иные, чем предоставленные Вам по Договору, заключенному между Вами и Вашим лицензиаром.

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

4.3. Вы не можете удалять или изменять уведомления об авторских правах или другие проприетарные уведомления на любой копии ПО.

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

5.1. Вы соглашаетесь с тем, что Вам не принадлежат никакие права на любую информацию, доступ к которой получен Вами в рамках осуществления настоящего Соглашения.

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

5.3. Указанная выше информация будет использоваться Вами только в целях осуществления предоставленных Вам по договору прав на ПО без права использования указанной информации в собственных интересах и за пределами Договора, заключенного между Вами и Вашим лицензиаром.

6. Вы проинформированы о том, что ПО содержит открытое программное обеспечение, распространяемое под определенными лицензиями, с которыми Вы можете ознакомиться в файле licenses.inf, распространяемом с ПО в составе дистрибутива. Каждый из предоставляемых дистрибутивов ПО содержит файл licenses.inf, соответствующий составу конкретного дистрибутива.

7. Уведомление о сборе информации об использовании ПО

7.1. Вы настоящим уведомляетесь о том, что при включении в ПО функции сбора статистики использования, в ПО осуществляется сбор и запись информации:

а) об аппаратном обеспечении, об операционной системе устройства, на котором установлено и эксплуатируется ПО, а также иная техническая информация, содержащая сведения об использовании аппаратных средств, нагрузке на аппаратные средства и быстродействии ПО;
б) об активности пользователя – анонимизированные (без указания сведений о самом пользователе или информации введенной пользователем) данные о действиях конечного пользователя в пользовательском интерфейсе ПО.

7.2. Правообладатель вправе использовать указанные данные в целях анализа особенностей эксплуатации ПО и особенностей использования ПО конечным пользователем для принятия решений о развития функциональности и улучшения эксплуатационных характеристик ПО.

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

8. Контактная информация Правообладателя ООО «Лаборатория ИнфоВотч»

Тел./факс: +7(495)229-00-22

Коммерческий департамент: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru

6 Глоссарий

Термин	Определение
"В разрыв"	Схема развертывания IW TM, при которой возможно блокирование исходящих из периметра почтовых сообщений с последующей досылкой. При этом сервер IW TM используется в качестве relay-сервера.
Active Directory	LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT
AJAX	Asynchronous Javascript and XML (асинхронный JavaScript и XML) - подход к построению интерактивных пользовательских интерфейсов веб-приложений, заключающийся в «фоновом» обмене данными браузера с веб-сервером
Astra Linux Directory Pro	Программный комплекс на базе ОС Astra Linux, предназначенный для централизованного управления объектами организаций различного масштаба
CLI	Command Line Interface - интерфейс командной строки
Domino directory	IBM Lotus Domino Directory - это директория с информацией о пользователях, серверах и группах. Domino Directory - это инструмент, используемый для администрирования системы Domino.
FreeIPA	Open-source-набор компонентов для централизованного управления пользователями, их группами, хостами, аутентификацией и авторизацией в Linux-системах
FTP	File Transfer Protocol (протокол передачи файлов) - сетевой протокол, предназначенный для передачи файлов по TCP-сетям
GTalk	Google Talk — программное обеспечения для мгновенного обмена сообщениями, разработанное компанией Google
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста) - протокол прикладного уровня передачи данных в виде текстовых сообщений. См. также: HTTPS, HTTP(S) Monitor
HTTPS	HyperText Transfer Protocol Secure (защищенный протокол передачи гипертекста) - расширение протокола HTTP, поддерживающее шифрование. См. также: HTTP, HTTP(S) Monitor

Термин	Определение
HTTP-запрос	Запрос, удовлетворяющий требованиям протокола HTTP (POST-запрос, GET-запрос и т. д.). См. также: HTTP, Событие
ICAP	Internet Content Adaptation Protocol - протокол, позволяющий контролировать входящий и исходящий HTTP-трафик. Предоставляет возможность модификации содержимого HTTP-запросов.
ICQ	Служба мгновенного обмена сообщениями в сети Интернет. Использует протокол OSCAR.
ICQ-сообщение	Сообщение, передаваемое по протоколу ICQ-OSCAR. См. также: Событие
IMAP	Internet Message Access Protocol Version 4 (протокол доступа к электронной почте Интернета) - сетевой протокол для доступа к электронной почте.
InfoWatch Device Monitor	IW DM: программный комплекс, предназначенный для контроля доступа сотрудников к периферийным устройствам и сетевым ресурсам, мониторинга операций (копирование данных на съемные носители и сетевые хранилища, отправка данных на печать, сетевая активность, использование приложений) и перехвата трафика систем мгновенного обмена сообщениями (Skype, Gtalk и Jabber) и т.п.
InfoWatch Traffic Monitor	IW TM: программный комплекс, предназначенный для осуществления контроля различных видов трафика (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) и теневых копий данных, копируемых на съемные носители и отправляемых на печать.
IW Lync Adapter	Перехватчик событий обмена данными через сервера MS Lync, установленные в инфраструктуре компании.
Jabber	Система для быстрого обмена сообщениями и информацией о присутствии на основе открытого протокола XMPP
LAN	Local Area Network - локальная вычислительная сеть
Lotus Adapter	Перехватчик, который устанавливается на почтовом сервере IBM Lotus для перенаправления писем для анализа при помощи IW TM. См. также: Перехватчик

Термин	Определение
Lotus Domino	Почтовый сервер компании IBM, сообщения которого перехватываются при помощи Lotus Adapter.
MAPI	Messaging Application Programming Interface - программный интерфейс, позволяющий приложениям работать с различными системами передачи электронных сообщений
MS Lync	Универсальный клиент Microsoft для общения и обмена информацией
MTProto	Криптографический протокол, используемый в системе обмена сообщениями для шифрования переписки пользователей
POP3	Post Office Protocol Version 3 (протокол почтового отделения) - сетевой протокол, используемый для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению
POST-запрос	Метод запроса POST предназначен для запроса, при котором веб-сервер принимает данные, заключенные в тело сообщения, для хранения. Он часто используется для загрузки файла или представления заполненной веб-формы
Relay-сервер	Сервер, выполняющий получение/пересылку электронной почты.
RPC	Класс технологий, позволяющих компьютерным программам вызывать функции или процедуры в другом адресном пространстве (как правило, на удаленных компьютерах)
Samba DC	Свободная программная реализация сетевого протокола SMB. Предоставляет службы файлов и печати для различных клиентов Microsoft Windows
Skype	Служба, обеспечивающая текстовую, голосовую и видеосвязь через Интернет
SMB	Server Message Block - сетевой протокол для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SMTP	Simple Mail Transfer Protocol (простой протокол передачи почты) - сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP

Термин	Определение
S/MIME	Secure/Multipurpose Internet Mail Extensions - стандарт для шифрования и подписи в электронной почте с помощью открытого ключа.
SMTP-письмо	Письмо, удовлетворяющее требованиям протокола SMTP. См. также: SMTP, Событие
SPAN	Switched Port Analyzer - технология зеркального копирования трафика с одного порта на другой
SPAN-копия	Разновидность транспортного режима Копия. Передача трафика в этом режиме осуществляется через коммутатор CISCO. Копия трафика передается для анализа на сервер Traffic Monitor. См. также: SPAN
SSL	Secure Sockets Layer (уровень защищенных сокетов) - криптографический сетевой протокол, обеспечивающий защищенный обмен данными
Telegram	Мессенджер, позволяющий пересылать текстовые сообщения, изображения, аудио- и видео-файлы (использует протокол MTProto).
WAN	Wide Area Network - глобальная компьютерная сеть
WhatsApp	Мессенджер, позволяющий пересылать текстовые сообщения, изображения, аудио- и видео-файлы (использует собственный протокол).
XMPP	Extensible Messaging and Presence Protocol - сетевой протокол, обеспечивающий мгновенный обмен сообщениями и информацией о присутствии
Агент Consul	Участник кластера Consul. Может быть как сервером, так и клиентом
Администратор	Предустановленная роль и учетная запись консоли управления, имеющая права на управление другими учетными записями и их правами. Также Администратор - пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. также: Роль пользователя, Офицер безопасности, Пользователь
Активная политика	Политика, действующий в конфигурации, загруженной на хост. См. также: Политика, Хост

Термин	Определение
Анализ события	Процедура обработки атрибутов, вложенных файлов и текста перехваченных событий и назначения событию дополнительных атрибутов. См. также: Политика, Атрибуты события, Событие
Атрибуты события	Структурированные данные, извлеченные из перехваченных событий и назначенные по результатам их обработки. См. также: Событие, Политика, Вердикт, Решение, Транспортный режим
Аудит	Контроль действий, выполняемых пользователями Консоли управления: создание и управление схемой безопасности, администрирование Системы. См. также: Журнал аудита, Учетные записи Консоли управления
База данных	Совокупность данных, хранимых в соответствии с используемой схемой данных. Хранит всю информацию, необходимую для работы Системы.
Бланки	Технология поиска заполненных бланков, форм например, анкет, квитанций и т.п. Бланки хранятся в системе в виде, недоступном для просмотра ни пользователям, ни администраторам Системы. См. также: Технологии, Элемент технологий
Вердикт	Атрибут события, содержащий заключение о наличии или отсутствии нарушений в анализируемом событии. В сочетании с атрибутом Транспортный режим определяет возможность дальнейшей транспортировки события. См. также: Транспортный режим, Состояние доставки, Атрибуты события, Событие
Версия конфигурации	Фиксированное состояние конфигурации, используемое для контроля изменений в настройках анализа событий. Версия конфигурации фиксируется в момент ее загрузки на хост, и может быть активной (используемой в настоящий момент), редактируемой (последняя версия с текущими изменениями) или сохраненной (имеющей изменения и доступной для редактирования пользователями). См. также: Конфигурация
Вес термина	Степень того, насколько данный термин характеризует категорию; целое число в диапазоне от 1 до 10. Если термин имеет высокий вес (значимость), то при его обнаружении в объекте существует большая вероятность того, что данный объект может быть отнесен к категории, содержащей данный термин. См. также: Термин

Термин	Определение
Виджет	Элемент интерфейса в виде обособленной области, выводящий заданную статистическую информацию о нарушениях и нарушителях. См. также: Консоль управления, Нарушение, Нарушитель
Вложение	Файл, приложенный к перехваченному событию, любой степени вложенности. См. также: Событие
Выгрузки из БД	Технология поиска цитат из базы данных. Выгрузками из БД могут быть списки заработных плат сотрудников, другие личные данные и т.п. См. также: Технологии
Графические объекты	Технология поиска изображений (например, изображений паспорта или банковской карты) в тексте и вложениях перехваченных событий. См. также: Технологии, Событие, Объект защиты
Группа персон и компьютеров	Группа, объединяющая информацию о компьютерах организации, сотрудниках организации, а также внешних контактах. Группы делятся на Группы AD (импортированные из Active Directory), Группы Samba DC (импортированные из Samba DC), Группы DM (импортированные из Domino Directory), Группы ALD (импортированные из Astra Linux Directory), Группы ALD Pro (импортированные из Astra Linux Directory Pro), Группы FreeIPA (импортированные из FreeIPa) и Группы TM (созданные средствами IW TM). См. также: Персона, Компьютер, Контакт
Заголовки	Вспомогательные данные, размещаемые в начале блока хранимых или передаваемых данных. Используются для формирования в Системе сущности события и определения значений атрибутов этого события. См. также: Событие, Атрибуты события
Защищаемые данные	Набор объектов защиты, их каталогов и файловых форматов, обнаружение которых в событии позволяет характеризовать это событие как подпадающее под ту политику защиты данных, в которой этот набор определен. См. также: Объект защиты, Файловый формат, Политика защиты данных
Инициатор, также: Инициатор события	Персона, чьи действия привели к созданию события в Системе
Интерфейс пользователя	Совокупность средств и методов, при помощи которых пользователь взаимодействует с системой.

Термин	Определение
Канал перехвата данных	Среда перехвата данных, состоящая из технических средств перехвата данных, средств программного обеспечения и протоколов передачи данных. В системе поддерживаются следующие каналы перехвата данных: электронная почта (SMTP, IMAP и POP3), веб (HTTP, HTTPS), сервисы мгновенных сообщений (Jabber, ICQ и Skype), теневые копии файлов, события подключения/отключения рабочих станций, задания на печать.
Категории и термины	Технология, выявляющая в тексте события наличие слов и выражений из базы терминов и относящая событие к категории, к которой принадлежат найденные термины. Ранее: Классификатор, БКФ. См. также: Событие, Термин, Категория, Технологии, Объект защиты
Категория	Именованная группа терминов, характеризующих определенную тематику. Если Система обнаруживает какой-либо из терминов категории в тексте перехваченного события, то она относит событие к этой категории. См. также: Термин
Компьютер	В терминах Системы под компьютером подразумевается контролируемая рабочая станция или терминальное устройство. См. также: Рабочая станция, Терминальное устройство
Консоль управления	Графический интерфейс пользователя. Предназначен для управления системой Traffic Monitor (администрирование Системы, настройка конфигурации, анализ событий и т. п.).
Консоль управления (DM)	Компонент графического пользовательского интерфейса. Предназначен для управления системой InfoWatch Device Monitor (настройка схемы безопасности, администрирование Системы и пр.).
Контекст события	Внутреннее представление перехваченного события в Системе. XML данные (атрибуты, текст), извлеченные из события и его вложений. После обработки с помощью технологий к контексту добавляются результаты анализа и информация о решении по событию. См. также: Событие, Технологии, Решение
Контролируемые персоны	Набор персон, групп персон и статусов персон, обнаружение которых в событии позволяет характеризовать это событие как подпадающее под ту политику контроля персон, в которой этот набор определен. См. также: Персоны, Группа персон, Статус персоны, Политика контроля персон

Термин	Определение
Конфигурация	Набор настроек, необходимых для проверки событий а также для мониторинга и анализа данных. См. также: Событие, Технологии, Списки, Политика
Корпоративная политика безопасности	Принятая в компании совокупность технических, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, регламентирующих все вопросы обеспечения безопасности информации
Лицензия	Право на использование Системы. Получается при приобретении Системы и определяет допустимое количество пользователей, используемые технологии и перехватчики и т.п. Также см.: Технологии, Перехватчики
Маска	Шаблон поиска — метод описания поискового запроса с использованием метасимволов. Маски используют для поиска файлов и папок
Мобильное устройство	Тип компьютера: смартфон или планшетный компьютер с установленной ОС семейства Android, Windows Phone или iOS. См. также: Компьютер
Монитор	См. Перехватчик
Морфология	Параметр термина: при использовании морфологии поиск по тексту будет осуществляться с учетом всех форм этого термина. См. также: Термин
Нарушение	Значение атрибута «Решение», означающее, что зарегистрировано нарушение корпоративной политики безопасности. См. также: Решение, Корпоративная политика безопасности
Нормальный транспортный режим	Режим, в котором выполняется анализ и фильтрация проходящего трафика. В этом режиме возможна блокировка запрещенного Системой трафика. См. также: Транспортный режим, "В разрыв"
Область видимости	Способ разделения перехваченных событий для ограничения доступа к ним пользователей консоли управления. События, удовлетворяющие критериям вхождения в какую-либо область видимости, будут видны только тем пользователям, которые имеют доступ к этой области видимости (при условии, что пользователь имеет привилегии на просмотр и/или работу с объектами). См. также: Событие, Привилегия

Термин	Определение
Объект защиты	Набор элементов технологий, обнаружение которых в событии позволяет отнести это событие к определенному типу бизнес-документов (каталогу объектов защиты). Объекты защиты используются при определении политик защиты данных. См. также: Элемент технологий, Политика защиты данных.
Основание вердикта	Атрибут события, описывающий причину, по которой событию был присвоен вердикт. См. также: Атрибуты события, Вердикт
Отчет	Выборка, обеспечивающая наглядное отображение статистических данных о событиях. См. также: Консоль управления, Событие
Офицер безопасности	Основной пользователь Консоли управления. Также - предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в системе, за исключением административных. См. также: Консоль управления, Пользователь, Роль пользователя, Привилегия, Администратор
Перехват данных	Процесс получения, разбора, рубрикации и преобразования данных (или их копии) в контекст. Осуществляется перехват данных, передаваемых по протоколам SMTP, IMAP, POP3, HTTP, HTTPS, ICQ/OSCAR, Skype, IXP, XMPP, MMP, FTP. См. также: Перехватчик, Контекст события
Периметр	Контейнер, содержащий элементы инфраструктуры компании (персоны, компьютеры, домен и прочие) и контактные данные. Используется для того, чтобы логически разделить организацию на структурные элементы и следить за трафиком каждого из таких элементов. См. также: Группа персон и компьютеров
Персона	Учетная запись сотрудника организации или внешнего контакта, содержащаяся в справочнике Системы и позволяющая обрабатывать данные, принадлежащие этой учетной записи, как единое целое, а также отображать события, относящиеся к ней, в удобном для пользователя виде. См. также: Группа персон и компьютеров
Плагин	Расширение, позволяющее Системе осуществлять прием событий предустановленных или новых типов от внешних перехватчиков, автоматическое обновление эталонных выгрузок данными от внешних систем (таких как SAP или 1С), предоставление сторонним системам данных об объектах ТМ

Термин	Определение
Политика	Совокупность правил, в соответствии с которыми проводится анализ и обработка событий. См. также: Политика, Активная политика, Правило
Политика (DM)	Совокупность правил, при помощи которых осуществляется мониторинг операций по созданию файлов на съемных устройствах, сетевой активности, печати документов на принтере; определяется уровень доступа к контролируемым периферийным устройствам и т. д. Политика может быть назначена только группе (сотрудников или компьютеров). См. также: Правило (DM)
Политика контроля персон	Политика для оперативного добавления правил контроля персон, групп персон или персон с указанным статусом. См. также: Политика, Правило контроля персон, Персона, Статус персоны
Пользователь	Пользователь системы Traffic Monitor - администратор, офицер безопасности и др. См. также: Администратор, Офицер безопасности, Персона
Пользователь Консоли управления	Пользователь, в задачи которого входит выполнение различных функций по управлению Системой. Каждому пользователю назначается роль в соответствии с требованиями корпоративной политики безопасности.
Порог встречаемости	Количество текстовых объектов, найденных в событии, достаточное для обнаружения объекта защиты, в котором определен данный порог встречаемости. См. также: Событие, Текстовые объекты, Объект защиты
Порог цитируемости	Процент эталонного документа, найденный в событии в виде цитат, достаточный для отнесения события к этому эталонному документу. См. также: Событие, Эталонный документ, Цитата
Правило	Сущность, определяющая действия Системы в ответ на те или иные действия персон с защищаемыми объектами. Правило состоит из набора условий, по которым ведется проверка событий, и действий, осуществляемых при выполнении или невыполнении заданных условий. См. также: Событие, Политика, Защищаемый объект, Правило контроля персон, Правило копирования, Правило передачи, Правило хранения
Правило (DM)	Набор ограничений и условий, в соответствии с которыми осуществляется мониторинг операций по созданию файлов на съемных устройствах, сетевой активности, печати документов на принтере; определяется уровень доступа к контролируемым периферийным устройствам. С

Термин	Определение
	каждым перехватчиком сопоставлен отдельный тип правила. Правило действует в пределах той политики безопасности, в которую входит это правило. См. также: Политика (DM)
Правило контроля персон	Правило, назначающее атрибуты событию с указанным уровнем нарушения, и в котором среди отправителей или получателей есть персоны, указанные в политике, куда входит это правило. Позволяет переназначать статус персонам и отправлять уведомления. См. также: Правило, Атрибуты события, Персона, Уровень нарушения, Статус персоны, Уведомление, Политика контроля персон
Правило копирования	Правило, регулирующее копирование или печать защищаемых данных. См. также: Правило, Защищаемые данные, Политика защиты данных
Правило передачи	Правило, регулирующее отправку и получение защищаемых данных. См. также: Правило, Защищаемые данные, Политика защиты данных
Правило хранения	Правило, регулирующее хранение защищаемых данных. См. также: Правило, Защищаемые данные, Политика защиты данных
Привилегия	Сущность, определяющая возможность пользователя выполнять какое-либо действие (набор действий) при работе с системой
Прокси-сервер	Служба, позволяющая выполнять косвенные запросы к другим сетевым службам. Прокси передает все запросы программ абонента в сеть, и, получив ответ, отправляет его обратно абоненту.
Рабочая станция	Тип компьютера: десктоп или ноутбук с ОС семейства Windows, Linux или Mac. См. также: Компьютер
Режим копии	Один из транспортных режимов системы IW TM. В этом режиме реальный трафик не проходит через Систему. Анализу подвергается копия трафика. В данном режиме невозможна фильтрация трафика средствами Системы. См. также: Транспортный режим
Решение	Заключение офицера безопасности о том, является ли событие нарушением корпоративной политики безопасности. Может принимать значения «Решение не принято», «Нарушение» и «Нет нарушений». См. также: Офицер безопасности, Корпоративная политика

Термин	Определение
	безопасности, Событие, Атрибуты события, Нарушение, Политика, Вердикт
Роль пользователя	Совокупность привилегий, определяющих набор действий, которые пользователь может выполнять при работе с системой. См. также: Администратор, Офицер безопасности, Консоль управления, Привилегия
Сводка	Раздел Консоли управления, отображающий статистическую информацию по нарушениям и нарушителям на виджетах. См. также: Консоль управления, Виджет, Нарушение
Сигнатура файла	Целочисленная константа, используемая для однозначной идентификации файлов определенного типа
Событие	Объекты перехвата трафика (SMTP-, IMAP-, POP3-письма, HTTP-запросы, ICQ-сообщения, Skype-сообщения), теневые копии файлов и задания на печать. Создаются Системой в результате обмена данных между сотрудниками организации и другими людьми, включая публикацию в общедоступных источниках, копирование на внешние устройства и печать.
Состояние доставки	Атрибут события, определяющий возможность доставки события получателям после анализа. Если доставка события была разрешена, то значение атрибута отражает состояние доставки (выполнена/не выполнена). См. также: Атрибуты события
Списки	Списки однотипных данных, создаваемые средствами консоли управления, для использования при составлении политик. См. также: Конфигурация, Политика
Справочники персон, рабочих станций и групп	Данные о пользователях, рабочих станциях, а также группах персон и рабочих станций, импортированные из Active Directory, Samba DC, Domino Directory, Astra Linux Directory или Astra Linux Directory Pro/Free IPA, а также созданные средствами консоли управления. Используются для удобства работы с информацией о событиях
Статус	Характеристика персон и компьютеров, позволяющая разделять их по группам для удобства анализа и отслеживания активности, а также отображать в сводке и в отчетах с особой цветовой индикацией. См. также: Персоны, Компьютеры, Сводка, Отчет
Стоп-слово	Цифры, буквы и слова, нахождение которых в ячейках не приводит к срабатыванию этих ячеек. Стоп-слова

Термин	Определение
	используются для исключения ложноположительных срабатываний.
Тег	Текстовая метка, дающая краткую характеристику событию. См. также: Атрибуты события
Текст события	Текстовая информация, извлеченная из тела события и его вложений. Не содержит элементов форматирования или разметки. Используется для решения задач анализа и поиска. См. также: Событие, Тело события
Текстовые объекты	Технология, соотносящая данные из текста событий, с заданными шаблонами (например, с правилами формирования номеров банковских карт). См. также: Технологии, Событие, Элемент технологий, Шаблон текстового объекта
Теневая копия документа	Копия документа, отправленного на печать с контролируемого компьютера. См. также: InfoWatch Device Monitor
Теневая копия файла	Копия файла, записываемого на съемное устройство. Создается только при успешном завершении операции сохранения файла на съемное устройство. См. также: InfoWatch Device Monitor
Термин	Один из набора слов и словосочетаний, в совокупности определяющих предметную область. См. также: Категория
Технологии	Набор инструментов анализа, выполняющих поиск заданных элементов в контексте событий и добавляющие событию атрибуты, характеризующие это событие. См. также: Элемент технологий, Контекст события, Категории, Термины, Эталонные документы, Бланки, Выгрузки из БД, Текстовые объекты, Графические объекты
Транспортный режим	Атрибут события, определяющий степень контроля доставки событий получателям. В сочетании с атрибутом "Вердикт" определяет возможность дальнейшей транспортировки события. См. также: Событие, Атрибуты события, Вердикт, Режим копии, Нормальный транспортный режим, Состояние доставки
Уведомление	Сообщение, отправляемое в случае срабатывания политики на событии. Отправляется средствами Консоли управления для уведомления пользователей Консоли управления, сотрудников или третьих лиц. Содержит краткую информацию о перехваченных событиях и

Термин	Определение
	сопроводительное сообщение. См. также: Политика, Событие
Уровень нарушения	Атрибут события, с помощью цветовой метки указывающий на степень угрозы для корпоративной политики безопасности. См. также: Событие, Атрибуты события, Нарушение
Учет регистра	Параметр термина: при учете регистра в анализируемом тексте будет выполняться поиск только тех словоформ, в которых есть полное соответствие с заглавными и строчными буквами, заданными в термине. См. также: Термин
Цитата	Отрывок эталонного документа, найденный в тексте события. См. также: Эталонный документ
Цитируемость	Показатель того, насколько полно эталонный документ присутствует в тексте анализируемого документа. См. также: Эталонный документ, Цитата
Цифровой отпечаток	Способ хранения эталонного документа в базе данных в виде набора цитат. См. также: Эталонный документ, Цитата
Шаблон текстового объекта	Унифицированное описание всех возможных текстовых объектов с типичной структурой: номера паспортов, кредитных карт, телефонные номера, код медицинского диагноза и т.д. См. также: Текстовые объекты
Элемент технологий	Составляющая настройки технологий, входящих в состав Системы. Пример конфиденциальных данных. К элементам технологий относятся: категории и термины, эталонные документы, бланки, выгрузки, текстовые объекты и графические объекты. См. также: Технологии, Категории, Термины, Эталонные документы, Бланки, Выгрузки из БД, Текстовые объекты, Графические объекты, Объект защиты.
Эталонная контрольная сумма	В отличие от текущей контрольной суммы, фиксирует образцовое состояние файлов Системы. См. также: Контроль целостности
Эталонные документы	Технология поиска цитат из конфиденциальных документов: например, образцы текстов приказов, финансовых отчетов, договоров и др. Эталонные документы хранятся в системе в виде цифровых отпечатков, текст недоступен для просмотра ни пользователям, ни администраторам Системы. См. также:

Термин	Определение
	Технологии, Элемент технологий, Цифровой отпечаток, Цитата