

INFOWATCH

InfoWatch Traffic Monitor

Руководство пользователя

07/11/2019

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Введение 10
1.1 Аудитория 10
1.2 Комплект документов 10
1.3 Техническая поддержка пользователей 10
2 Обзор InfoWatch Traffic Monitor 12
2.1 Перехват объектов 14
2.2 Анализ объекта и вынесение решения по объекту 16
2.3 Ретроспективный анализ данных, решение пользователя по объекту 19
2.4 Транспортные режимы InfoWatch Traffic Monitor 19
2.5 Загрузка объекта в базу данных 20
2.6 Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов 21
2.7 Функции InfoWatch Device Monitor 22
2.7.1 Работа при загрузке операционной системы в безопасном режиме 23
3 Работа в консоли управления Traffic Monitor: общие принципы 25
3.1 Работа Системы до конфигурирования 26
3.2 Работа с конфигурацией Системы 27
3.3 Отображение актуальных данных в Консоли управления 29
4 Интерфейс Консоли управления Traffic Monitor 30
4.1 Раздел "Сводка" 32
4.1.1 Виджеты сводки 33
4.1.1.1 Динамика нарушений за период 34
4.1.1.2 Топ нарушителей 35
4.1.1.3 Количество нарушений за период 37
4.1.1.4 Подборка 37
4.1.1.5 Динамика статусов за период 38
4.1.1.6 Статистика по политикам 39
4.1.1.7 Статистика по объектам защиты 39
4.1.1.8 Статистика по каталогам объектов защиты 41
4.1.2 Выгрузка сводки 41
4.2 Раздел "События" 43
4.2.1 Запросы 44
4.2.1.1 Обычный режим создания запроса 46

4.2.1.2 Расширенный режим создания запроса ... 54
4.2.1.3 Поиск по тексту события ... 55
4.2.2 Объекты перехвата ... 57
4.2.2.1 Плитка события ... 59
4.2.2.2 Краткая форма просмотра событий ... 60
4.2.2.3 Детальная форма просмотра событий ... 63
4.2.3 Идентификация контактов в событии ... 65
4.3 Раздел "Отчеты" ... 66
4.3.1 Форма создания отчета ... 68
4.3.2 Виджеты отчетов ... 69
4.3.3 Запросы ... 71
4.4 Раздел "Технологии" ... 73
4.4.1 Категории и термины ... 74
4.4.1.1 Категории ... 74
4.4.1.2 Термины ... 75
4.4.2 Текстовые объекты ... 76
4.4.2.1 Шаблоны текстовых объектов ... 77
4.4.3 Эталонные документы ... 79
4.4.4 Бланки ... 80
4.4.5 Печати ... 82
4.4.6 Выгрузки из БД ... 83
4.4.6.1 Автоматически обновляемые выгрузки из БД ... 84
4.4.7 Графические объекты ... 86
4.5 Раздел "Объекты защиты" ... 87
4.5.1 Элементы технологий ... 88
4.5.2 Условия обнаружения ... 89
4.6 Раздел "Персоны" ... 92
4.6.1 Персоны ... 93
4.6.2 Компьютеры ... 95
4.6.3 Снимки экрана ... 96
4.7 Раздел "Политики" ... 96
4.7.1 Правила и форма их просмотра ... 98
4.7.1.1 Правило передачи ... 99
4.7.1.2 Правило копирования ... 101
4.7.1.3 Правило хранения ... 102
4.7.1.4 Правило работы в приложениях ... 103
4.7.1.5 Правило контроля персон ... 104
4.8 Раздел "Списки" ... 104
4.8.1 Теги ... 105
4.8.2 Веб-ресурсы ... 105
4.8.3 Статусы ... 106
4.8.4 Периметры ... 107

4.8.5 Файловые типы ... 108
4.9 Раздел "Управление" ... 109
4.10 Раздел "Краулер" ... 110
4.10.1 Сканер ... 112
4.10.2 Задача сканирования ... 113
5 Решение задач при работе в консоли Traffic Monitor ... 118
5.1 Типовые действия ... 118
5.1.1 Вход в Консоль управления ... 119
5.1.2 Применение конфигурации Системы ... 119
5.1.3 Редактирование элемента ... 120
5.1.4 Удаление элемента ... 120
5.1.5 Навигация по страницам ... 121
5.1.6 Изменение пароля пользователя ... 122
5.1.7 Выбор языка интерфейса ... 122
5.1.8 Вызов справки ... 122
5.1.9 Просмотр сведений о Системе ... 123
5.2 Работа с персонами и компьютерами ... 123
5.2.1 Создание группы персон и компьютеров ... 124
5.2.2 Создание персон и компьютеров ... 125
5.2.3 Настройка карточки персоны ... 126
5.2.3.1 Добавление контакта персоне ... 126
5.2.3.2 Добавление компьютера для персоны ... 128
5.2.3.3 Добавление персоны в группу ... 128
5.2.4 Настройка карточки компьютера ... 129
5.2.4.1 Добавление компьютеру контакта ... 129
5.2.4.2 Добавление персоны для компьютера ... 129
5.2.4.3 Добавление компьютера в группу ... 130
5.2.5 Добавление статуса персонам ... 130
5.2.6 Просмотр снимков экрана ... 131
5.3 Работа со справочниками ... 133
5.3.1 Работа с тегами ... 134
5.3.2 Работа с веб-ресурсами ... 134
5.3.3 Работа со статусами ... 136
5.3.4 Работа с периметрами ... 136
5.4 Работа с базой технологий ... 140
5.4.1 Определение конфиденциальной информации ... 141
5.4.1.1 Работа с категориями и терминами ... 143
5.4.1.2 Работа с текстовыми объектами ... 146
5.4.1.3 Работа с эталонными документами ... 148
5.4.1.4 Работа с бланками ... 150
5.4.1.5 Работа с печатями ... 153

5.4.1.6 Работа с выгрузками ... 154
5.4.2 Экспорт и импорт базы технологий ... 158
5.5 Работа с объектами защиты ... 160
5.5.1 Создание каталога объектов защиты ... 161
5.5.2 Создание объекта защиты ... 162
5.5.3 Добавление элементов технологий ... 163
5.5.4 Добавление условий обнаружения ... 165
5.5.5 Создание политики для объектов защиты и их каталогов ... 166
5.5.6 Импорт и экспорт объектов защиты ... 167
5.5.7 Активация и деактивация объектов защиты ... 168
5.6 Работа с подсистемой Краулер ... 169
5.6.1 Настройка сканера ... 169
5.6.2 Создание задачи ... 171
5.6.3 Очистка хеша ... 172
5.7 Работа с объектами перехвата ... 172
5.7.1 Просмотр сводки по нарушениям/нарушителям ... 173
5.7.1.1 Создание панели ... 174
5.7.1.2 Создание и настройка виджета ... 175
5.7.1.3 Создание выгрузки сводки ... 176
5.7.1.4 Просмотр выгрузки сводки ... 178
5.7.2 Просмотр событий ... 179
5.7.2.1 Создание запросов ... 179
5.7.2.2 Выбор полей просмотра событий ... 193
5.7.2.3 Просмотр краткой формы события ... 193
5.7.2.4 Просмотр детальной формы события ... 195
5.7.3 Вынесение решения по объекту ... 195
5.7.4 Добавление и удаление тега ... 196
5.7.5 Сохранение события (для SMTP-писем) ... 196
5.7.6 Выгрузка событий ... 197
5.7.7 Досылка события, находящегося в карантине ... 200
5.8 Настройка реакций Системы ... 201
5.8.1 Общие сведения о политиках ... 202
5.8.2 Предустановленные политики ... 210
5.8.2.1 Политики защиты конфиденциальных данных ... 210
5.8.2.2 Политика контроля персон ... 212
5.8.2.3 Политика, регулирующая передачу данных, защищенных паролем ... 212
5.8.2.4 Политики, контроллирующие посещение веб-ресурсов ... 213
5.8.2.5 Политика, исключающая из перехвата почтовые рассылки ... 215
5.8.3 Создание политики защиты данных ... 216
5.8.3.1 Примеры использования политики защиты данных ... 217
5.8.4 Создание политики защиты данных на агентах ... 221
5.8.5 Создание политики контроля персон ... 223

5.8.6 Создание правил ... 225
5.8.7 Определение действий Системы в случае нарушения правил ... 227
5.8.8 Настройка уведомлений в правилах ... 229
5.8.9 Определение действий Системы по умолчанию ... 230
5.8.10 Фильтрация списка политик ... 231
5.8.11 О политике защиты данных на агенте ... 232
5.8.12 О политике защиты данных ... 233
5.8.13 О политике контроля персон ... 234
5.9 Работа с отчетами ... 234
5.9.1 Создание и просмотр отчетов ... 235
5.9.1.1 Создание папки с отчетами ... 237
5.9.1.2 Создание отчета ... 238
5.9.1.3 Создание и настройка виджета ... 240
5.9.1.4 Просмотр готовых отчетов ... 242
5.9.2 Примеры использования отчетов ... 243
5.10 Управление Системой ... 248
5.10.1 Управление интеграцией с LDAP каталогами ... 248
5.10.1.1 Создание подключения к серверу ... 250
5.10.1.2 Редактирование подключения к серверу ... 251
5.10.1.3 Удаление подключения к серверу ... 251
5.10.1.4 Запуск синхронизации с сервером вручную ... 251
5.10.2 Управление пользователями Системы и их ролями ... 252
5.10.2.1 Пользователи ... 252
5.10.2.2 Роли ... 256
5.10.2.3 Области видимости ... 259
5.10.3 Управление лицензиями ... 262
5.10.3.1 Проверка валидности лицензии ... 263
5.10.3.2 Установка лицензии ... 263
5.10.3.3 Удаление лицензии ... 263
5.10.3.4 Запрос лицензии ... 264
5.10.4 Состояние системы ... 264
5.10.4.1 Настройка уведомлений ... 265
5.10.5 Управление службами ... 265
5.10.5.1 Запуск службы ... 265
5.10.5.2 Остановка службы ... 266
5.10.5.3 Перезапуск службы ... 266
5.10.5.4 Сохранение логов службы ... 267
5.10.6 Сбор диагностических данных ... 267
5.10.6.1 Сбор диагностических данных в обычном режиме ... 268
5.10.6.2 Сбор диагностических данных в расширенном режиме ... 268
5.10.7 Аудит действий пользователя ... 269
5.10.7.1 События аудита ... 269
5.10.7.2 Фильтрация по пользователю ... 270

5.10.7.3 Фильтрация по действию ... 271
5.10.7.4 Фильтрация по объекту ... 271
5.10.7.5 Фильтрация по дате ... 271
5.10.8 Контроль целостности ... 271
5.10.8.1 Ручная проверка целостности ... 271
5.10.8.2 Автоматическая проверка целостности ... 272
5.10.8.3 Принятие результата за эталонный ... 272
5.10.9 Плагины ... 272
5.10.9.1 Добавление плагина ... 275
5.10.9.2 Удаление плагина ... 275
5.10.9.3 Работа с токенами ... 276
5.10.10 Настройка подключения к почтовому серверу ... 277
5.10.11 Настройка уведомлений ... 278
5.10.11.1 Создание уведомления ... 279
5.10.11.2 Тестирование уведомления ... 281
5.10.11.3 Предустановленные уведомления ... 281

6 Работа в Консоли Управления Device Monitor ... 283

6.1 Начало работы с Консолью управления (DM) ... 283
6.1.1 Авторизация и соединение с сервером InfoWatch Device Monitor ... 283
6.1.2 Главное окно Консоли управления (DM) ... 284
6.1.2.1 Настройка элементов главного окна Консоли управления (DM) ... 286
6.1.3 Разделы Консоли управления (DM) ... 287

6.2 Управление учетными записями и ролями Консоли управления (DM) ... 287
6.2.1 Учетные записи пользователей Консоли управления (DM) ... 289
6.2.1.1 Добавление учетной записи Консоли управления (DM) ... 291
6.2.1.2 Редактирование учетной записи Консоли управления (DM) ... 294
6.2.1.3 Блокирование и разблокирование учетной записи Консоли управления (DM) ... 295
6.2.1.4 Удаление учетной записи Консоли управления (DM) ... 295
6.2.2 Роли пользователей Консоли управления (DM) ... 296
6.2.2.1 Добавление роли пользователя Консоли управления (DM) ... 297
6.2.2.2 Редактирование роли пользователя Консоли управления (DM) ... 300
6.2.2.3 Удаление роли пользователя Консоли управления (DM) ... 300
6.2.3 Аудит действий по управлению схемой безопасности в Консоли управления (DM) ... 301
6.2.3.1 Просмотр журнала аудита ... 301
6.2.3.2 Фильтрация записей в журнале аудита ... 304
6.2.3.3 Удаление записей из журнала аудита ... 308
6.2.3.4 Экспорт записей журнала аудита ... 308
6.2.3.5 Анализ журнала аудита в Microsoft Excel ... 309

6.3 Общие настройки Системы ... 309
6.3.1 Общие настройки работы Агентов ... 309
6.3.2 Контроль сетевых соединений ... 312

6.3.3 Контроль мессенджеров ... 315
6.3.4 Контроль сетевого трафика ... 316
6.3.4.1 Добавление серверов ... 318
6.3.5 Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor ... 320
6.3.6 Соединение с сервером LDAP и синхронизация с сервером Active Directory и Astra Linux Directory ... 323
6.3.7 Настройка уведомлений сотрудников о нарушении правил (DM) ... 326
6.3.8 Исключение приложений из перехвата ... 329
6.3.9 Контроль приложений и снимки экрана ... 332
6.3.10 Хранение событий ... 334
6.3.11 Синхронизация политик Traffic Monitor ... 335
6.3.12 Работа с Менеджером управления серверами ... 336
6.3.13 Остановка и запуск агента Device Monitor ... 337
6.3.13.1 Удаленная остановка/запуск агента ... 337
6.3.13.2 Локальная остановка/запуск агента ... 339
6.3.14 Контроль ввода с клавиатуры ... 339
6.4 Управление схемой безопасности ... 340
6.4.1 Организация схемы безопасности ... 341
6.4.1.1 Политики безопасности и правила (DM) ... 341
6.4.1.2 Сотрудники и группы сотрудников ... 343
6.4.1.3 Компьютеры и группы компьютеров ... 344
6.4.1.4 Загрузка схемы безопасности на контролируемые компьютеры ... 344
6.4.2 Общие действия при управлении схемой безопасности ... 345
6.4.2.1 Просмотр действующей версии схемы безопасности ... 345
6.4.2.2 Просмотр предыдущих версий схемы безопасности ... 346
6.4.2.3 Комментарии к схеме безопасности ... 347
6.4.2.4 Редактирование схемы безопасности ... 348
6.4.2.5 Обновление схемы безопасности ... 351
6.4.2.6 Экспорт/импорт конфигурации ... 351
6.4.3 Настройка схемы безопасности ... 352
6.4.3.1 Политики безопасности (DM) ... 353
6.4.3.2 Правила (DM) ... 358
6.4.3.3 Сотрудники ... 395
6.4.3.4 Компьютеры ... 404
6.4.3.5 Белые списки устройств ... 415
6.4.3.6 Категории сигнатур ... 423
6.4.3.7 Приложения ... 426
6.4.4 Временный доступ сотрудника к сети ... 432
6.4.5 Временный доступ сотрудника к устройствам ... 433
6.5 Просмотр событий DM ... 435
6.5.1 Фильтры событий ... 445
6.5.2 Удаление событий ... 447
6.6 Удаленная установка, обновление и удаление Агентов ... 448

6.6.1 Просмотр задач ... 449
6.6.2 Подготовка к первичной установке Агентов. Агент распространения ... 452
6.6.2.1 Включение административных разделяемых ресурсов ... 453
6.6.2.2 Настройки брандмауэра ... 453
6.6.3 Создание задачи первичного распространения ... 454
6.6.4 Создание задачи обновления ... 459
6.6.5 Создание задачи смены пароля деинсталляции ... 461
6.6.6 Создание задачи удаления ... 462
6.6.7 Запуск, остановка, редактирование и удаление задачи ... 463
6.6.8 Ошибки установки Агентов ... 464
6.6.9 Создание пакета установки ... 466
6.7 Дополнительные возможности ... 468
6.7.1 Фильтрация табличных данных ... 468
6.7.1.1 Фильтр по дате ... 468
6.7.1.2 Использование стандартных фильтров ... 469
6.7.1.3 Пользовательский фильтр ... 470
6.7.1.4 Редактирование фильтра ... 471
6.7.1.5 Отмена фильтра ... 472
6.7.2 Группирование и сортировка записей ... 473
6.7.3 Клавиши быстрого доступа ... 473
7 Лицензионная информация ... 477
7.1 Пользовательское лицензионное соглашение ... 477
7.2 Лицензии третьих сторон ... 479
8 Глоссарий ... 480

1 Введение

InfoWatch Traffic Monitor (далее Traffic Monitor или Система) – это распределенная многокомпонентная система, предназначенная для контроля различных видов трафика (SMTP, IMAP, POP3, HTTP, HTTPS, ICQ, NRPC). Кроме того, InfoWatch Traffic Monitor выполняет анализ данных, полученных от системы InfoWatch Device Monitor.

Веб-консоль управления (далее Консоль управления) является частью системы InfoWatch Traffic Monitor, позволяет управлять настройками и осуществлять мониторинг работы Системы.

Веб-консоль управления имеет интуитивно понятный интерфейс, поэтому настоящее руководство содержит только общую информацию и ряд наглядных примеров, которые дают возможность представить весь функционал Системы.

1.1 Аудитория

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

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Microsoft Windows.

1.2 Комплект документов

В комплект документации по InfoWatch Traffic Monitor входят:

- *«InfoWatch Traffic Monitor. Руководство по установке»*

Содержит описание порядка установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.

- «*InfoWatch Traffic Monitor. Руководство администратора*».

Содержит информацию по администрированию Системы (база данных, серверная часть).

- «*InfoWatch Traffic Monitor. Руководство пользователя*».

Содержит описание порядка работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, составление политик для обработки объектов).

- «*InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*».

Содержит пояснения к часто используемым конфигурационным файлам.

1.3 Техническая поддержка пользователей

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

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера.
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ.
Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/support.
Перед обращением в службу технической поддержки рекомендуется посетить раздел База знаний на нашем сайте: https://kb.infowatch.com/. Возможно, там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

2 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 (см. статью "Различия 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.

- Проверка файлов, находящихся в корпоративной сети (открытых сетевых папок, локальных дисков рабочих станций и файлового хранилища SharePoint 2007/2010/2013), с помощью подсистемы Crawler.
- 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 (версия для ПК). Также поддерживается перехват голосового трафика в Skype. Перехват перечисленных данных осуществляется системой InfoWatch Device Monitor.
- Анализ теневых копий файлов, перехваченных системой DeviceLock ЗАО «Смарт Лайн Инк» (версии 6.3 и выше).

- 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) и перехват трафика систем мгновенного обмена сообщениями.
Crawler	Проверка файлов, находящихся в корпоративной сети (открытых сетевых папок, локальных дисков рабочих станций и файлового хранилища SharePoint).
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

2.1 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 (версия для ПК), Facebook, 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 "Перехват трафика";
- Различия 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. • 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 (версия для ПК), Facebook, VK (ВКонтакте) от InfoWatch Device Monitor.
MS Lync	Система получает копию объектов от lW Lync Adapter, установленного на сервере MS Lync.
Файлы, расположенные в корпоративной сети	Система получает копии файлов от подсистемы Crawler.

Теневые копии файлов и задания на печать, полученные от InfoWatch Device Monitor	Система получает копию трафика. Блокирование действий пользователя (печать, доступ к устройствам) доступно только через InfoWatch Device Monitor.
Теневые копии файлов, полученные от DeviceLock	Система получает копию трафика. Блокирование действий пользователя (доступ к устройствам) доступно только через DeviceLock

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

2.2 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 и 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 Применения Политик	Модуль Интеграции с Active Directory, Domino Directory и Astra Linux Directory	Обеспечение первоначального импорта и периодической синхронизации структуры каталога Active Directory, Domino Directory и Astra Linux Directory 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.**
>
> Для документов MS Office 2007 и 2010 анализируются также метаданные, указанные в свойствах документа (вкладка **Подробно**, блок **Описание**).

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.

- 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.

2.3 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.

2.4 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
ICQ-сообщение	Нет	Да (только для копии трафика, полученной от Sniffer)
Сообщение Skype, Jabber, Telegram	Нет	Да
MS Lync	Нет	Да
Теневая копия файла	Нет	Да

2.5 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.

2.6 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.

2.7 Функции InfoWatch Device Monitor

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

Основные функции системы InfoWatch Device Monitor:

- мониторинг контролируемых рабочих станций в режиме реального времени, автоматическое создание снимков экрана (см. "Правило (DM) для ScreenShot Monitor");
- контроль доступа сотрудников к периферийным устройствам компьютерной системы (см. "Правило (DM) для Device Monitor");
- мониторинг печати на контролируемых компьютерах (см. "Правило (DM) для Print Monitor");
- контроль систем мгновенного обмена сообщениями: Skype, Telegram (версия для ПК), Facebook, VK (ВКонтакте), Jabber (протокол XMPP), протокол MMP (см. "Правило (DM) для IM Client Monitor");
- контроль трафика, передаваемого по протоколу FTP и FTPS (см. "Правило (DM) для FTP Monitor");
- контроль трафика, передаваемого по протоколу HTTP и HTTPS (см. "Правило (DM) для HTTP(S) Monitor");
- контроль передачи данных по сетевым соединениям вне корпоративной сети (см. "Правило (DM) для Network Monitor");
- контроль систем передачи почтовых сообщений (SMTP, IMAP, POP3, Outlook, HTTPS) (см. "Правило (DM) для Mail Monitor");
- контроль подключения с помощью Microsoft RDP или Citrix ICA (см. "Правило (DM) для Device Monitor");
- контроль файлов, копируемых с/на съемные устройства, сетевые ресурсы и ресурсы, подключенные через терминальную сессию (см. "Правило (DM) для File Monitor");
- контроль облачных хранилищ файлов (см. "Настройки правила для Cloud Storage Monitor");
- контроль снимков экрана (см. "Настройка правила для ScreenShot Control Monitor");
- контроль приложений (см. "Правило (DM) для Application Monitor");
- контроль доступа сотрудников к буферу обмена (см. "Правило (DM) для Clipboard Monitor");
- контроль ввода с клавиатуры (см. "Правило (DM) для Keyboard Monitor");
- сбор данных, полученных от контролируемых компьютеров;
- передача полученных данных в систему InfoWatch Traffic Monitor для анализа;
- настройка хранения событий (см. "Хранение событий").

Важно!

Для рабочих станций под управлением ОС Astra Linux доступны только следующие функции контроля:

- контроль систем передачи почтовых сообщений по протоколам SMTP, POP3, IMAP и HTTPS (см. "Правило (DM) для Mail Monitor");
- контроль файлов, копируемых с/на съемные устройства, сетевые ресурсы и ресурсы, подключенные через терминальную сессию(см. "Правило (DM) для File Monitor");
- контроль облачных хранилищ файлов (см. "Настройки правила для Cloud Storage Monitor");
- контроль трафика, передаваемого по протоколу FTP и FTPS (см. "Правило (DM) для FTP Monitor");
- мониторинг печати на контролируемых компьютерах (см. "Настройка правила для Print Monitor");
- контроль систем мгновенного обмена сообщениями: Facebook, VK (ВКонтакте), Jabber (протокол XMPP) (см. "Правило (DM) для IM Client Monitor");
- контроль трафика, передаваемого по протоколу HTTP и HTTPS (см. "Правило (DM) для HTTP(S) Monitor").

Примечание.

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

Мониторинг и контроль действий сотрудников выполняется на контролируемых компьютерах. На контролируемые компьютеры устанавливаются агентские модули Системы. В состав модуля входят перехватчики: **File Monitor**, **Print Monitor**, **Device Monitor**, **IM Client Monitor**, **FTP Monitor**, **HTTP(S) Monitor**, **Network Monitor**, **Mail Monitor**, **Application Monitor**, **Cloud Storage Monitor**, **ScreenShot Control Monitor**, **ScreenShot Monitor**, **Keyboard Monitor, Photo Monitor**. Подробнее о работе перехватчиков см. "Правила (DM)".

Примечание.

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

На агентах Device Monitor происходит анализ перехваченных данных, используя технологии детектирования:

- форматов файлов;
- текстовых объектов;
- терминов/баз контентной фильтрации (БКФ).

2.7.1 Работа при загрузке операционной системы в безопасном режиме

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

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

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

3 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*».

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)**.

3.1 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.

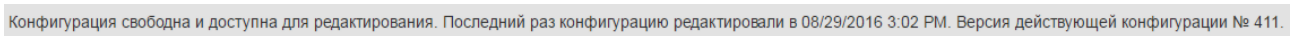
3.2 Работа с конфигурацией Системы

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"). 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.
- **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.

3.3 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.

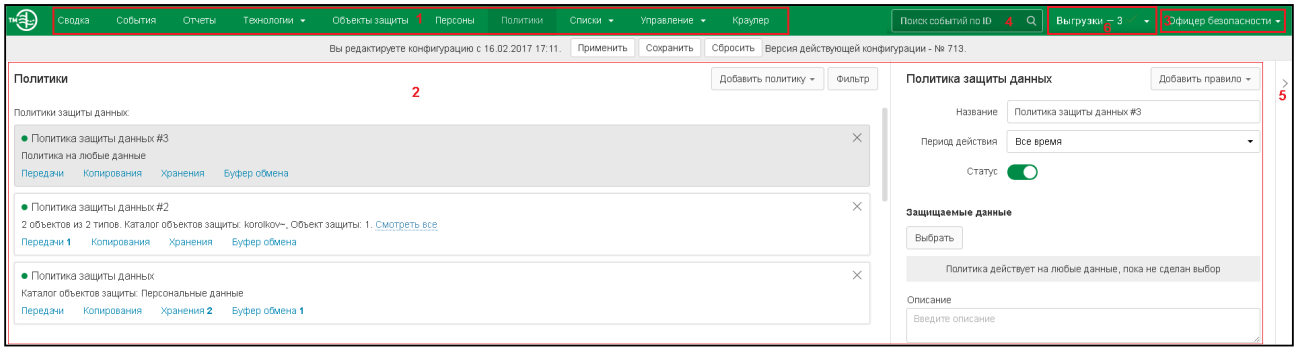
В любом из разделов Консоли управления вы также можете обновлять данные вручную. Для этого воспользуйтесь стандартным средством обновления страницы интернет-браузера (по умолчанию обновление выполняется при нажатии функциональной клавиши F5).

Примечание:

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

4 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
Списки	Раздел содержит редактируемые справочники тегов, ресурсов, статусов и периметров
Управление	Раздел позволяет выполнить первичную настройку Системы, просматривать события аудита и настраивать отправку уведомлений
Краулер	Раздел содержит средства для создания, редактирования и запуска задач для подсистемы Краулер

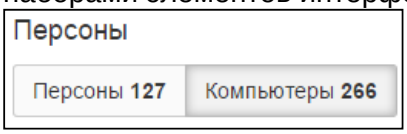
Переход к разделу происходит после нажатия на кнопку раздела.



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).

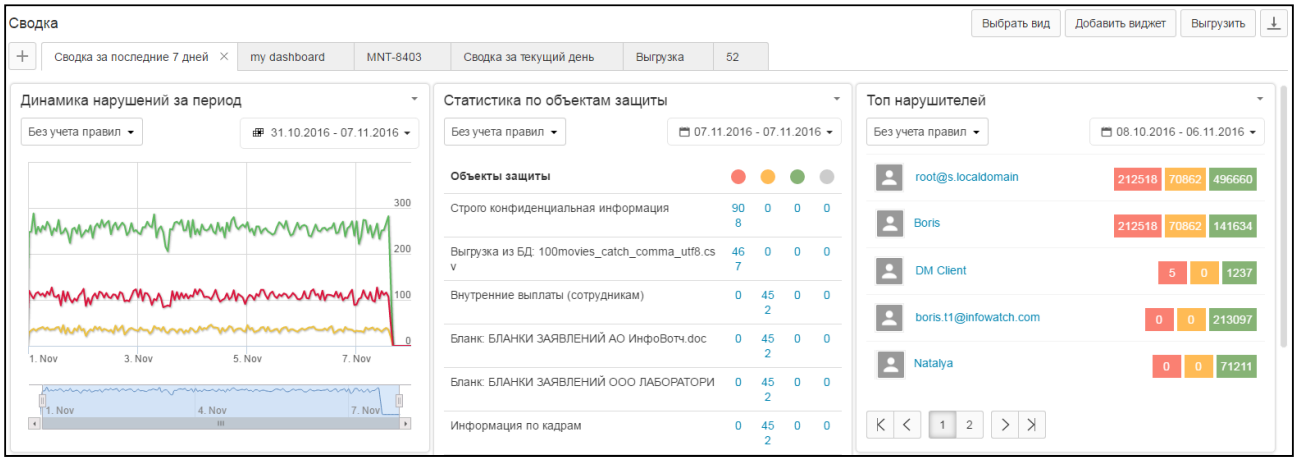
> **Примечание:**
>
> В тех случаях, когда запрашиваемые данные находятся в процессе загрузки, в Системе может отображаться символ вида  либо информационное сообщение.

4.1 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 .

Целевые 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").

4.1.1 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

Целевые 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.

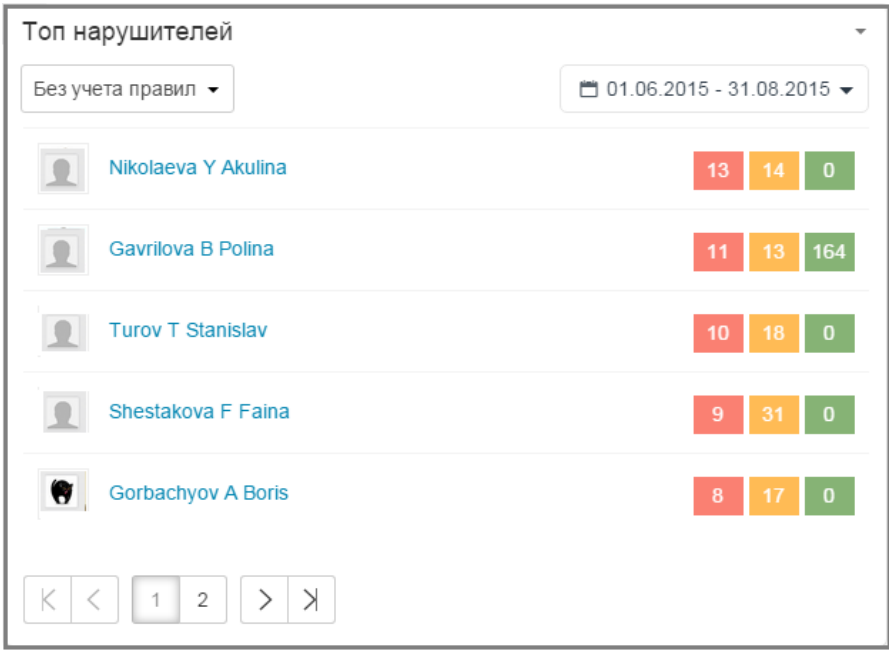
В верхнем левом углу виджета выберите, нарушения каких правил должны отображаться на виджете. Возможные значения: *Правила передачи*, *Правила копирования*, *Правила хранения*, *Без учета правил*.

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:

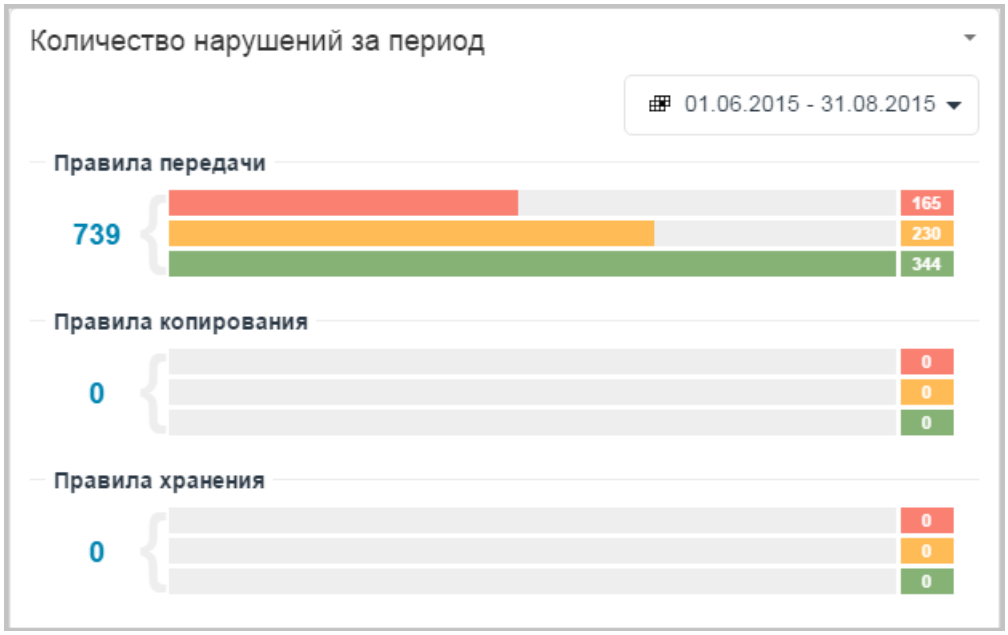
- **Название**;
- **Интервал обновления** данных на виджете;
- **Количество нарушителей**, по которым будет отображаться статистика;
- **Группы**, в которые могут входить нарушители. На виджете будет отображаться статистика по выбранным группам. Начните вводить название группы или нажмите и выберите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



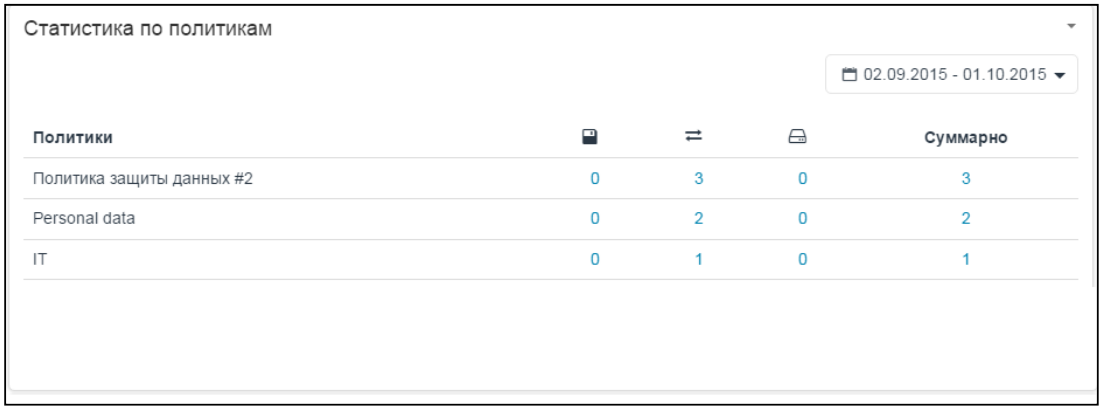
При нажатии на количество персон или компьютеров (выделено синим цветом), выполняется переход в раздел "Персоны" (к вкладке **Персоны** или **Компьютеры** соответственно), где будут показаны персоны (или компьютеры), удовлетворяющие заданным в виджете условиям.

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**.

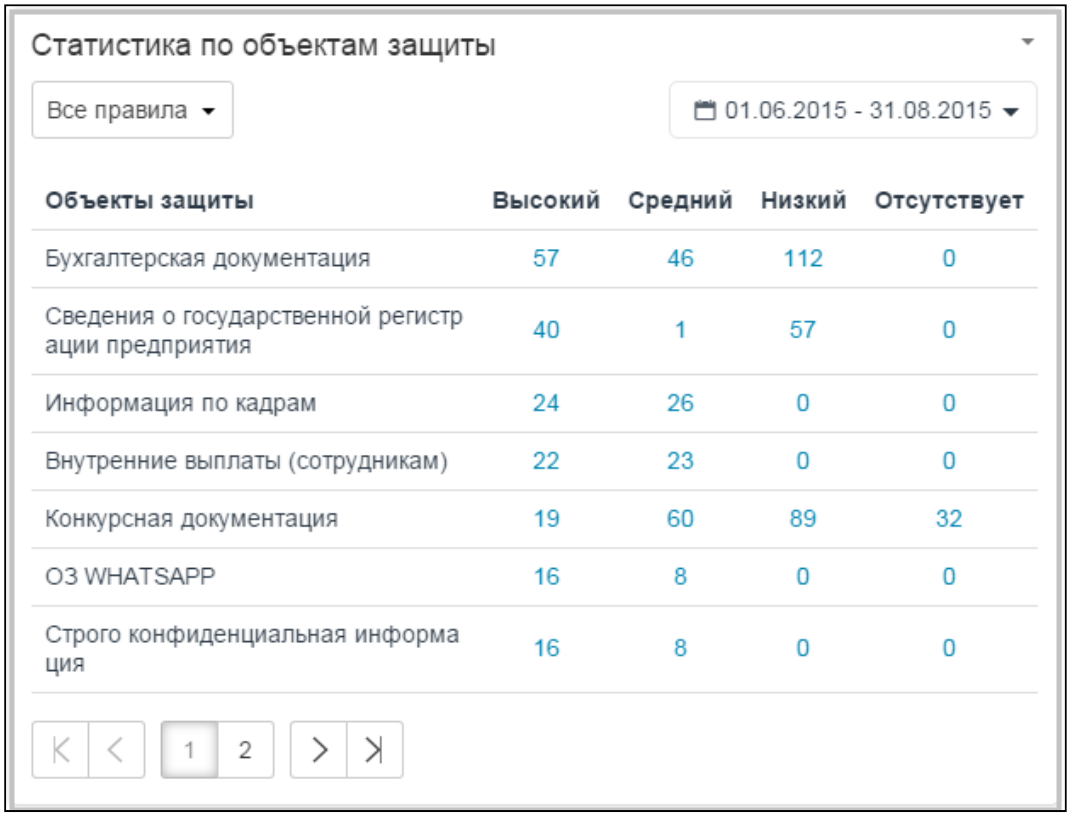
Для редактирования доступны следующие параметры:

- **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:

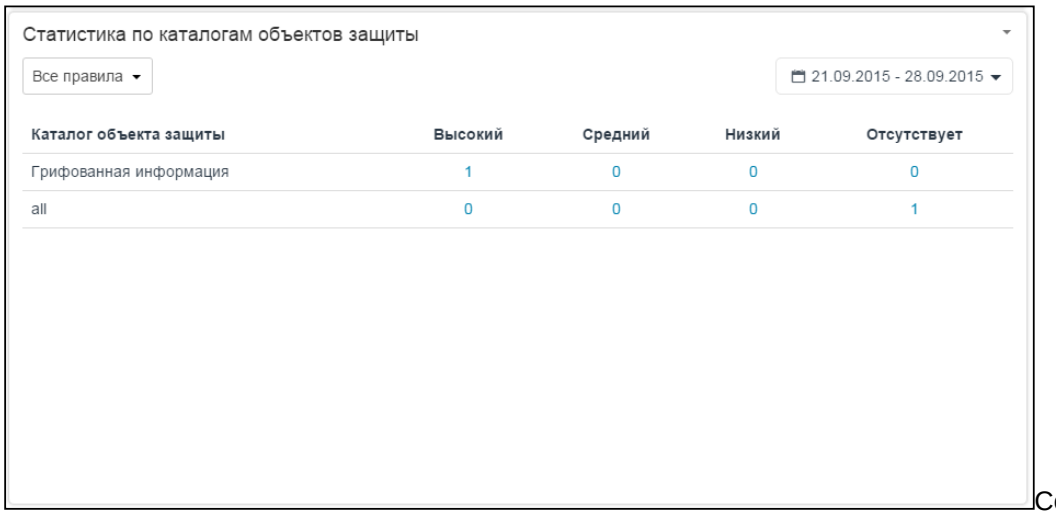
- **Название**;
- **Интервал обновления** данных на виджете;
- **Объект защиты** - объекты защиты, по которым будет отображаться статистика.

  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**.

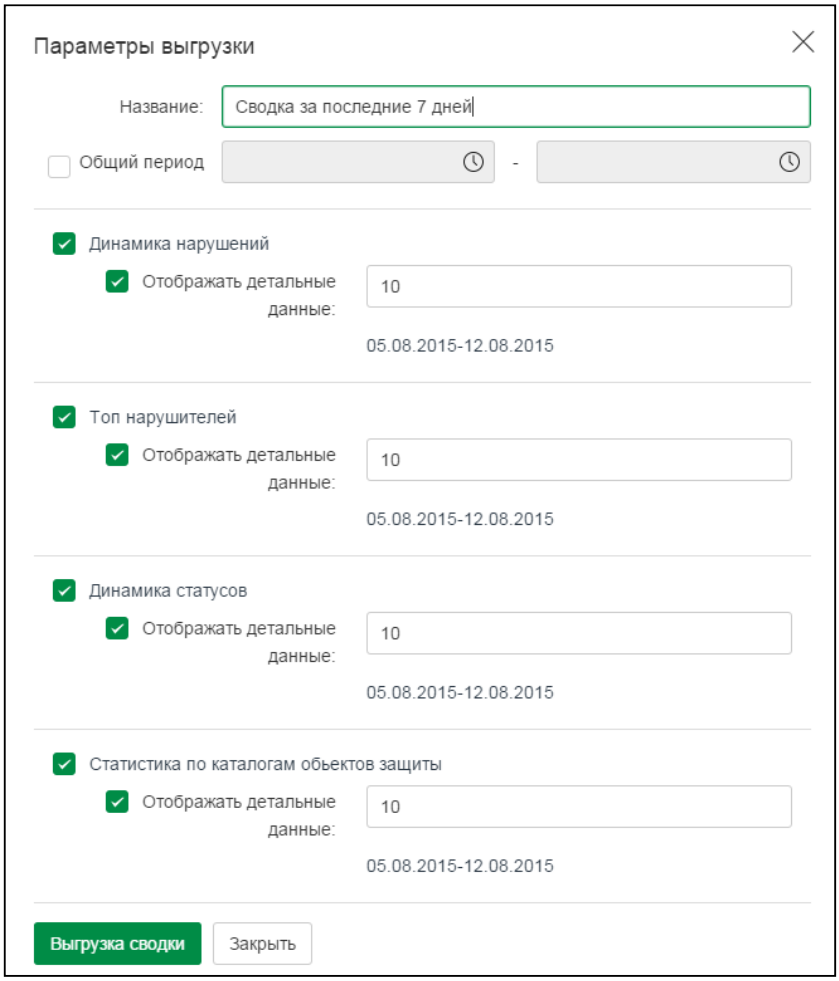
Для редактирования доступны следующие параметры:

- **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**.

4.1.2 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 опредяет, сколько персон 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.

Целевые действия пользователя:

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

4.2 Раздел "События"

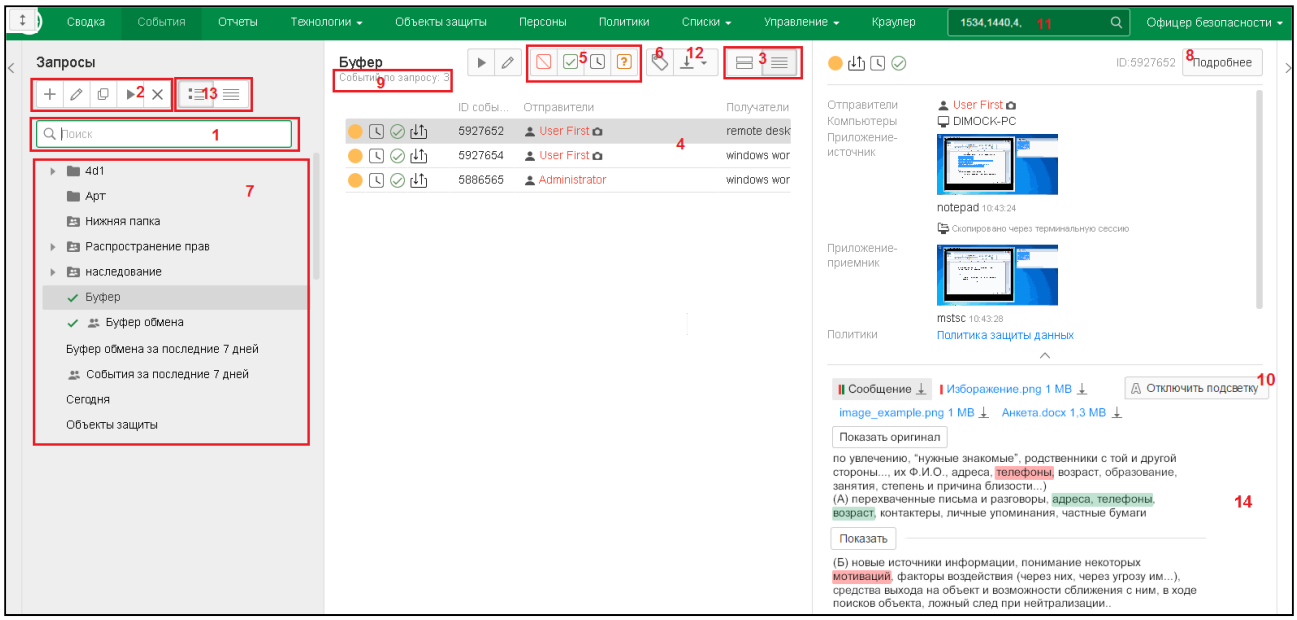
Справочная информация:
Событие - объект перехвата сетевого трафика.

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 скриншоте). Запросы могут создаваться как на верхнем уровне, так и внутри папок. Для работы с запросами и папками используются инструменты на панели (№2 на скриншоте). Вы можете выбрать режим отображения элементов в списке (№13 на скриншоте):

-  - 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 скриншоте) или создайте новый запрос с помощью кнопки  на панели инструментов (№2 на скриншоте).

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

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

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

> **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 скриншоте).

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

Вы можете выбрать способ отображения событий в списке (№3 на скриншоте):

-  - в виде плитки;
-  - в виде таблицы.

В правой части рабочей области отображается краткая форма просмотра выбранного события (№14 на скриншоте). 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 скриншоте).

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

Для выбранного события вы можете выполнить следующие действия:

- назначить событию вердикт (выберите нужный вердикт, используя кнопки на панели - №5 на скриншоте);
- назначить событию тег (№6 на скриншоте);
- выгрузить событие или сохранить отладочную информацию по событию (№12 на скриншоте).

Целевые действия пользователя:

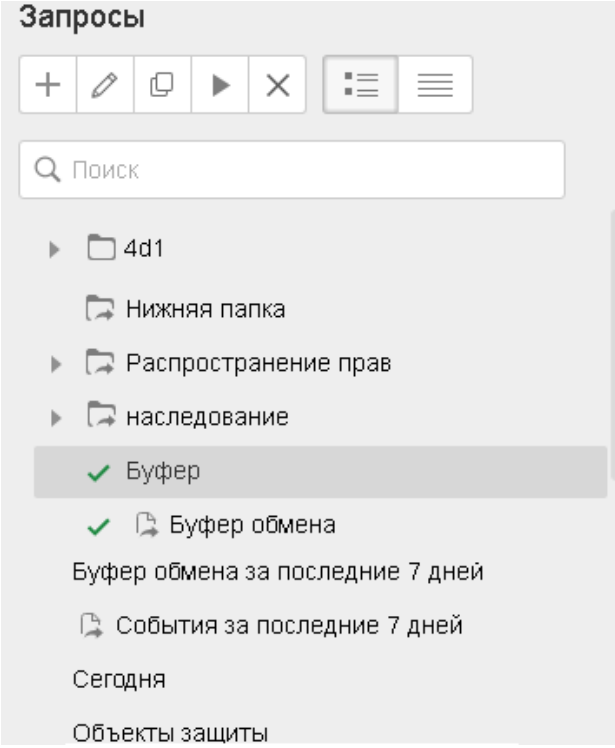
- фильтрация событий (см. "Создание запросов");
- просмотр информации по событию ("Просмотр краткой формы события" и "Просмотр детальной формы события");
- вынесение решения по событию (см. "Вынесение решения по объекту");
- добавление/удаление тега события (см. "Добавление/удаление тега");
- сохранение 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").

4.2.1 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.

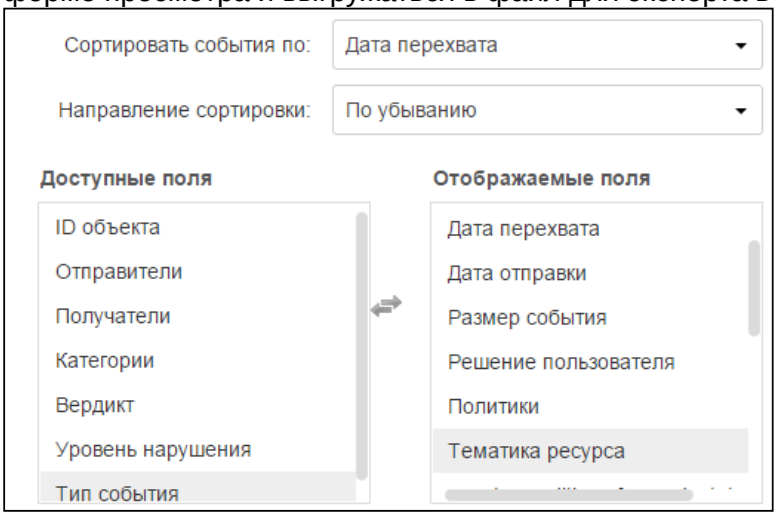
Если запрос в данный момент выполняется, рядом с его названием отображается значок . Для запросов, выполнение которых завершилось с ошибкой, отображается значок .

Чтобы создать новый запрос, нажмите на панели иструментов 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.
  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**).

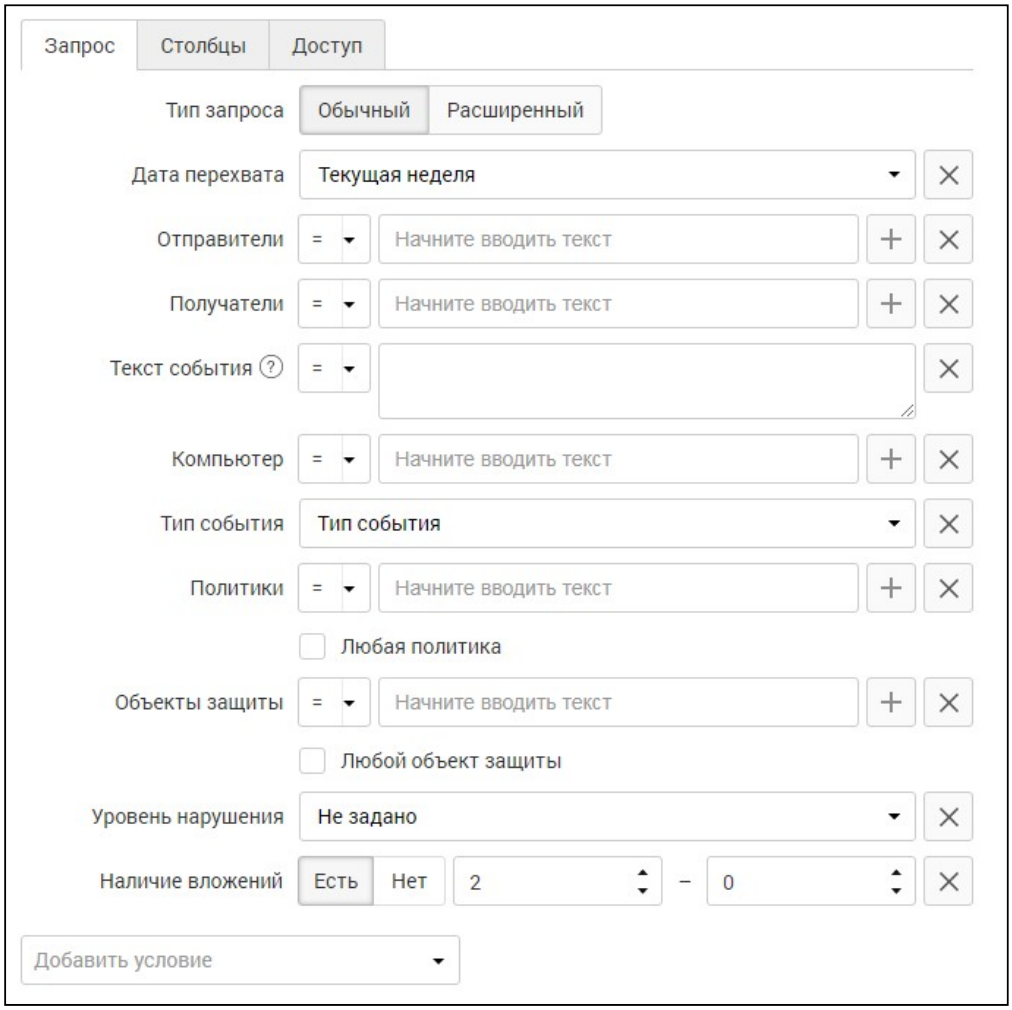
Целевые действия пользователя:

- 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:

Параметр	**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: • Буфер обмена: - Буфер обмена • Интернет-активность: - Веб-сообщение • Обмен файлами: - FTP - Съемные устройства - Облачное хранилище - Терминальная сессия - Сетевые ресурсы • Принтеры и МФУ: - Печать • Хранение файлов: - Краулер • Почта: - Почта на Клиенте - Почта в Браузере • Мессенджер: - Telegram - MS Lync - ICQ - XMPP - MMP - Skype
Перехватчик	Перехватчик, с помощью которого было получено событие. Возможные значения: • ICAP • DM • Adapter • SMTPD • Sniffer • PushAPI • Crawler

Протокол	Тип перехватываемого протокола. Возможные значения: • FTP • HTTP • HTTPS • IMAP • MAPI • MMP • NRPC • OSCAR • POP3 • SIP • Skype • SMTP/ ESMTP • Telegram • XMPP
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").
Мандатный уровень	Мандатный уровень конфиденциальности. Учитывается в Traffic Monitor, начиная с версии 6.10.10, на ОС Astra Linux.

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, vk.com).
Буфер обмена	
Приложение-источник	Приложение, из которого были скопированы данные

Приложение-приемник	Приложение, в которое были вставлены данные из буфера обмена
Политики	
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*.
Задачи Краулера	
Название задачи	Название задачи сканирования. 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.
Дата запуска задачи	Временной период, в который задача была запущена
Цель сканирования	Тип локации, на которой объект был найден. Возможные значения: • Разделяемые сетевые ресурсы • Локальные диски рабочих станций • Файловое хранилище SharePoint
Содержимое события	

Наличие 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.
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 вложения. Можно выбрать несколько значений из списка
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.
Дата создания файла	Дата создания вложенного файла
Дата модификации файла	Дата изменения вложенного файла
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 выполняет по всему содержимому события. Использование групповых символов ("*", "?") не допускается. При отрицании условия из результатов поиска будут исключены события, к 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.

Результаты анализа	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:** Если Система была обновлена до версии 6.9, то в результаты поиска могут не попасть системные текстовые объекты из событий, перехваченных до обновления.
Объекты защиты	Список сработавших объектов защиты. Вы можете выбрать как отдельные объекты защиты, так и каталоги.
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.

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;
- Теста события;
- Результаты анализа;
- Объекты защиты.

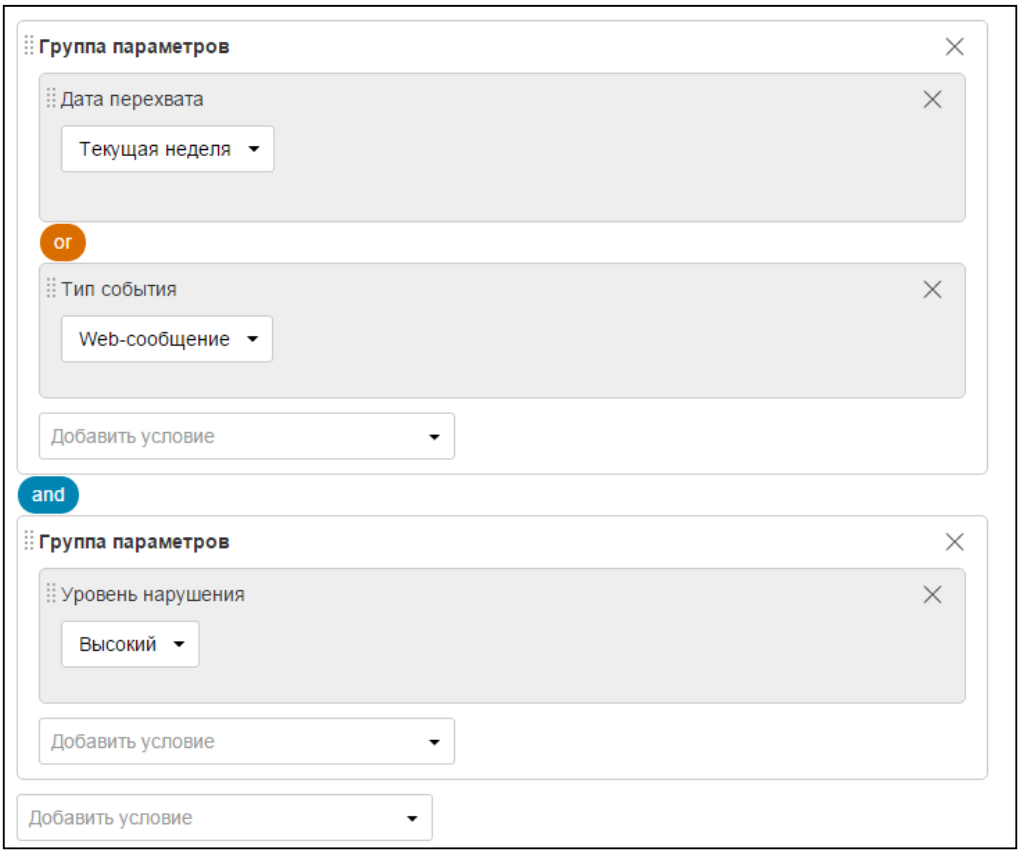
Если отрицание применяется к атрибуту с множественными значениями, то из результатов поиска будут исключены события, содержащие указанные значения. Например, если в качестве отправителей указаны адреса `user1@example.com` и `user2@example.com`, из результатов поиска будут исключены события, в которых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

Целевые 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.

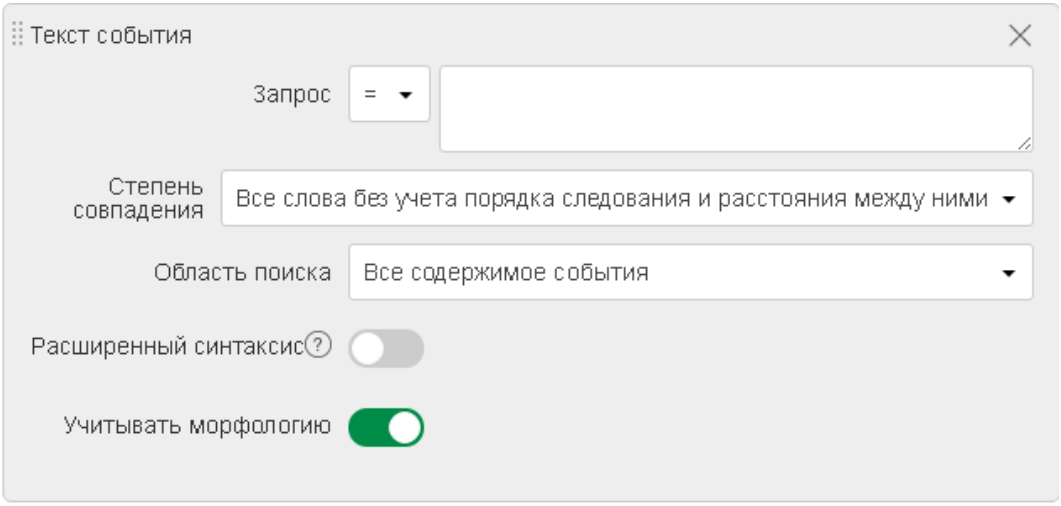
Также при создании запроса в расширенном режиме вы можете выполнить гибкую настройку условий поиска по тексту события.

Целевые 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 (если выбран параметр равенства =) или не должен (если к атрибуту применено отрицание ≠) содержаться в событии

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. 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 события. • **Текст сообщения** - поиск будет выполняться по тексту сообщения и теме письма. • **Тема письма** - поиск будет выполняться по теме письма. • **Вложение** - поиск будет выполняться по тексту вложений 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:** Опция **Учитывать морфологию** доступна, только если в настройках Базы данных включено построение морфологического индекса. Подробнее об этой настройке смотрите документ *«Руководство администратора».*

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.

Целевые действия пользователя:

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

4.2.2 Объекты перехвата

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

Информация о событии представлена в следующих видах:

- в плитке события (или записи о событии в таблице) отображается основная информация о событии;
- 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: •  - Буфер обмена (копирование и вставка данных через буфер обмена); •  - Интернет-активность (post-запросы к веб-ресурсам); •  - 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 (отправка или получение фотографий); •  - Электронная почта (отправка и получение данных через почту на клиенте и почту в браузере); •  - Мессенджер (отправка или получение сообщений через Skype, MS Lync, ICQ (OSCAR), XMPP, Telegram); •  - 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

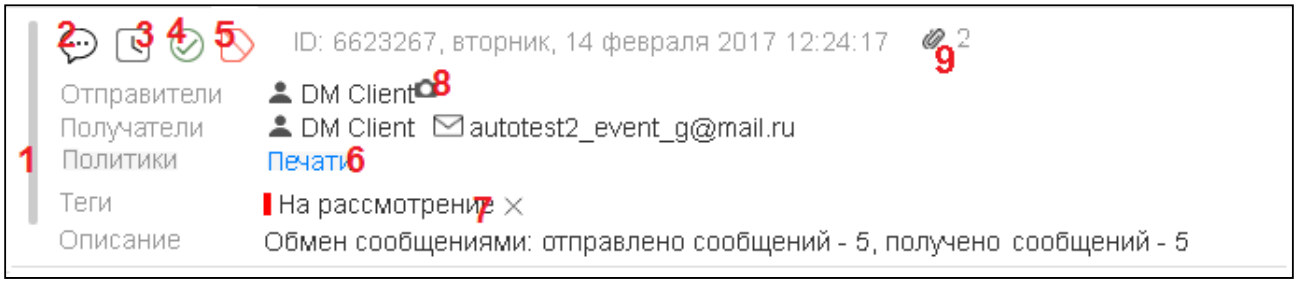
Теги	Список тегов, присвоенных данному объекту
Дата перехвата	Дата и время, когда трафик был перехвачен Системой
Дата вставки	Дата и время, когда данное событие было сохранено в БД
Размер	Размер события (в байтах)
Уровень нарушения	Характеристика нарушения, присвоенная событию. Возможные варианты: • *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;
- "Краткая форма просмотра событий" - о представлении общей информации о событии;
- "Детальная форма просмотра событий" - о представлении расширенной информации о событии.

Плитка события

При выборе события в списке отображается плитка события:



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)

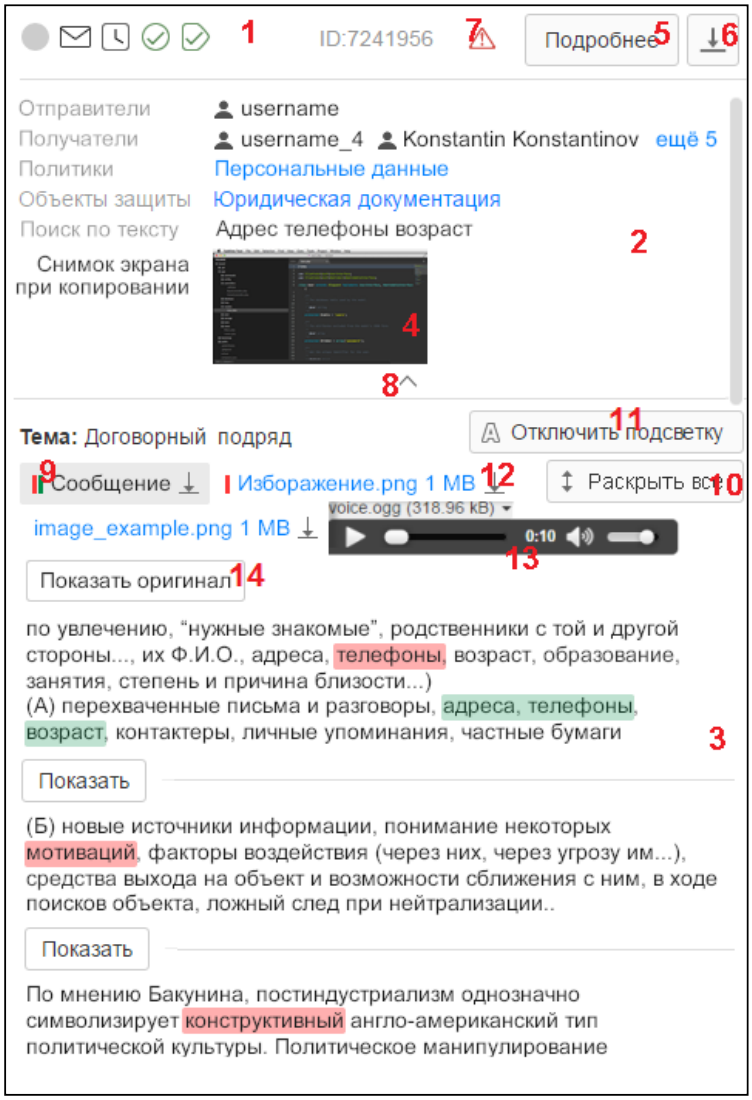
> **Примечание.**
>
> Набор отображаемых атрибутов зависит от типа события.

1. Цвет уровня нарушения. Возможные значения : *Высокий*, *Средний*, *Низкий*, *Отсутствует*.
2. Тип события. Возможные значения: *Краулер, Буфер обмена, Ввод с клавиатуры, Веб-сообщение, Facebook, ICQ, MS Lync, Mail.ru Агент, Skype, Telegram, XMPP, ВКонтакте, Почта на Клиенте, Почта в Браузере, FTP, Внешнее устройство, Облачное хранилище, Печать*.
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 вложении отображается индикатор с указанием количества вложений.

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

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), сработавших

политиках и объектах защиты.
Для событий буфера обмена может отображаться миниатюра снимка экрана (№ 4 на рисунке), если при копировании/вставке данных был создан снимок экрана.

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).

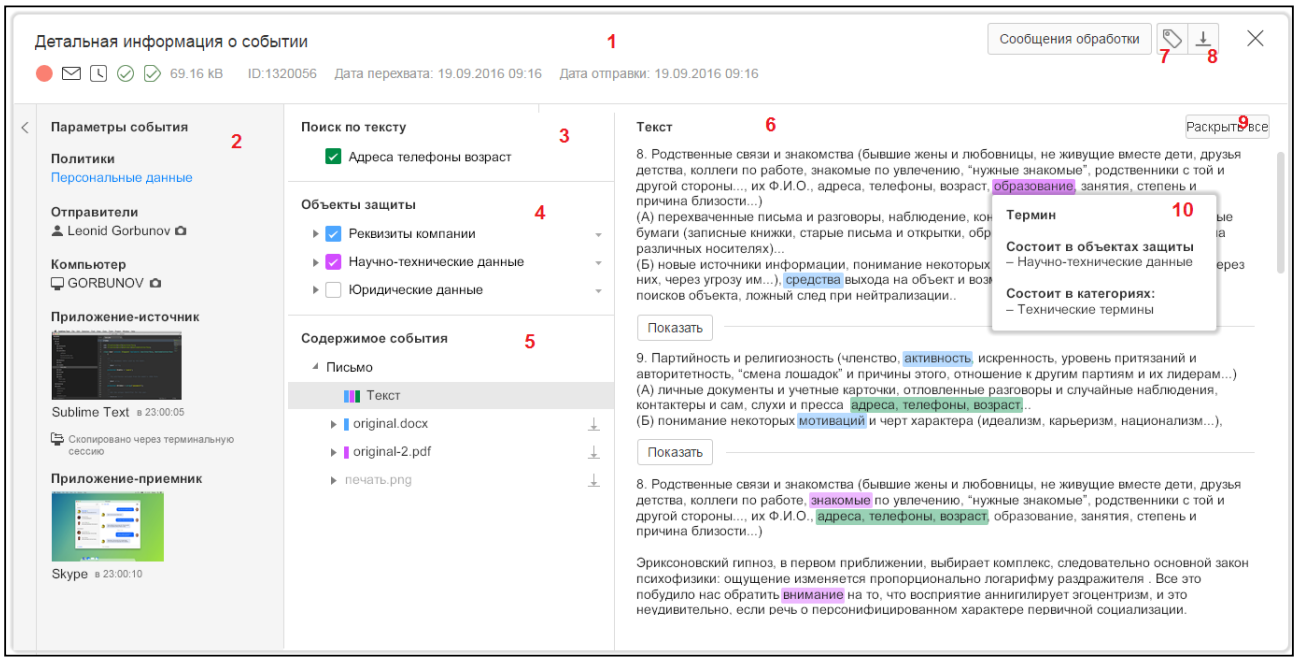
Чтобы сохранить вложение на компьютер, нажмите (№ 12 на рисунке) рядом с названием нужного вложения.

Целевые 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), объектах защиты, периметрах и т.д.
   Для событий буфера обмена может отображаться миниатюра снимка экрана, если при копировании/вставке данных был создан снимок экрана.
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.
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.
6. Область просмотра (№ 6 на рисунке). Позволяет просмотреть текст сообщения и текст, извлеченный из вложений.

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; при этом все сработавшие элементы технологий, относящиеся к данному объекту защиты, выделены тем же цветом;

  Примечание.

  Если часть текста относится сразу к нескольких элементам технологий, то такая часть текста выделяется серым цветом.

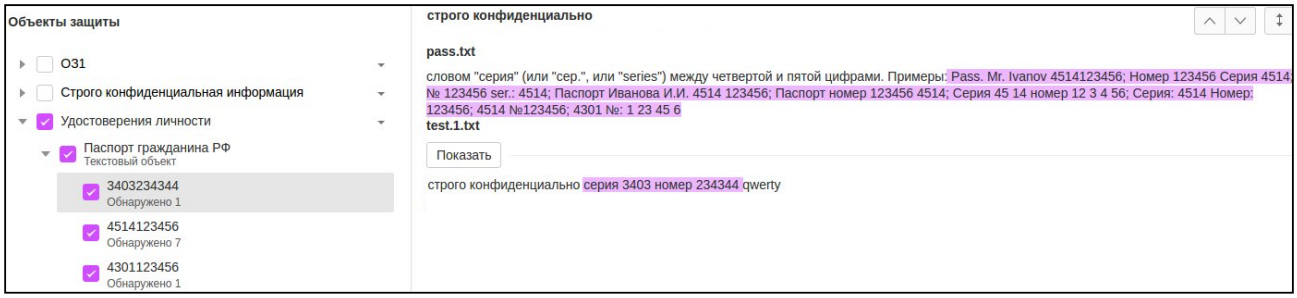
- результаты поиска по тексту события выделены зеленым цветом.

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:

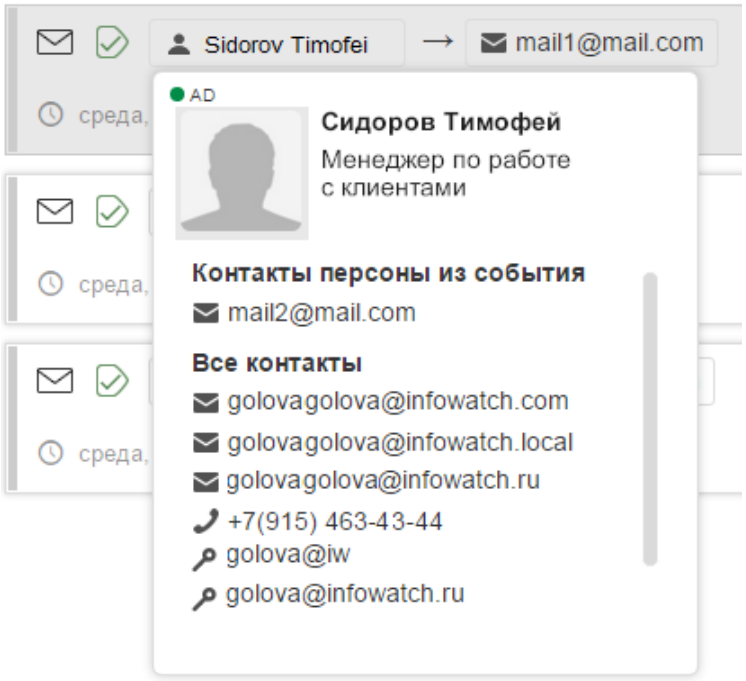
- для вложения `original.docx` - объект защиты *Реквизиты компании*;
- для вложения `original-2.pdf` - объект защиты *Научно-технические данные*;
- для текста события - объект защиты *Реквизиты компании*, объект защиты *Научно-технические данные*, а также найден искомый текст.

Целевые действия пользователя:

- Просмотр детальной формы события

4.2.3 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), 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:

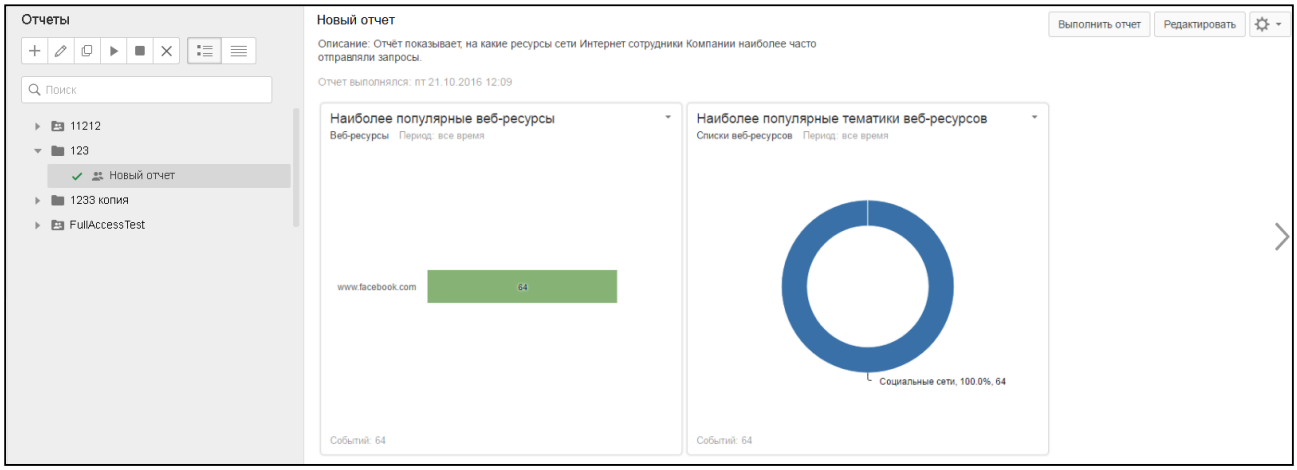
- odnoklassniki.ru
- gmail.com

4.3 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.

Целевые действия пользователя:

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

4.3.1 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**).

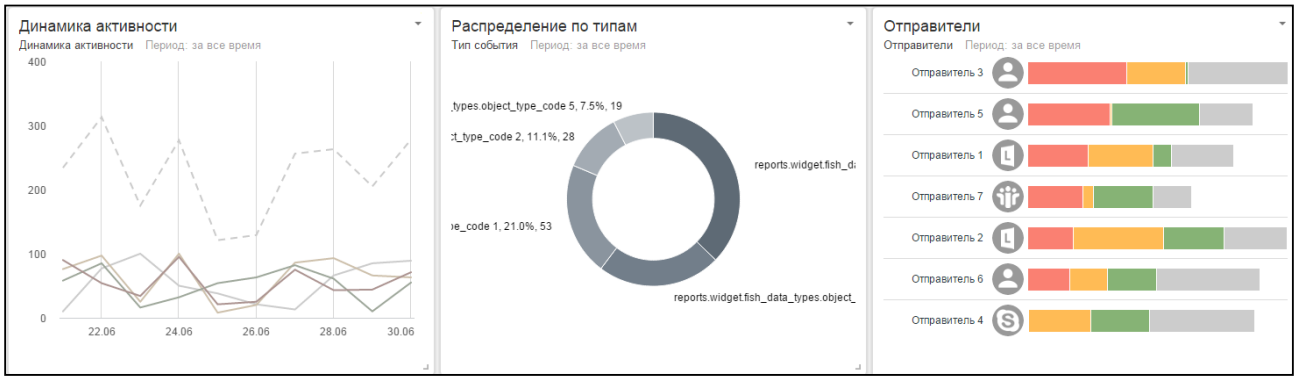
Целевые действия пользователя:

- Создание отчета

4.3.2 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
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").
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.

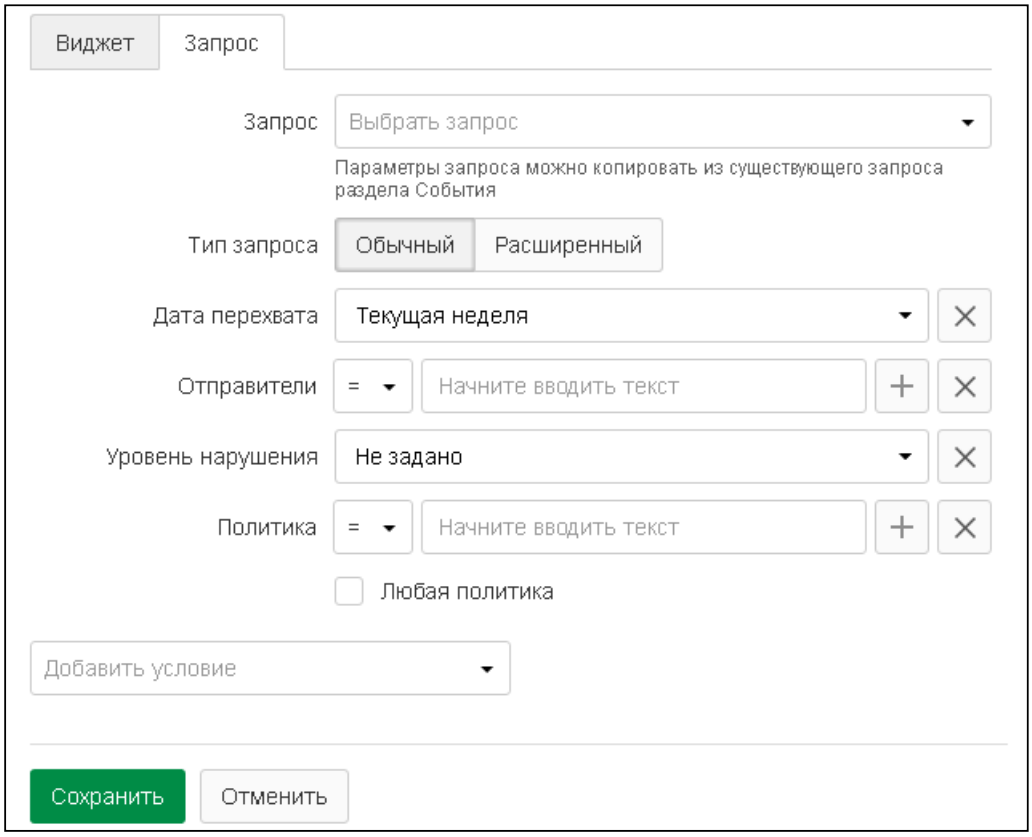
Целевые действия пользователя:

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

4.3.3 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".

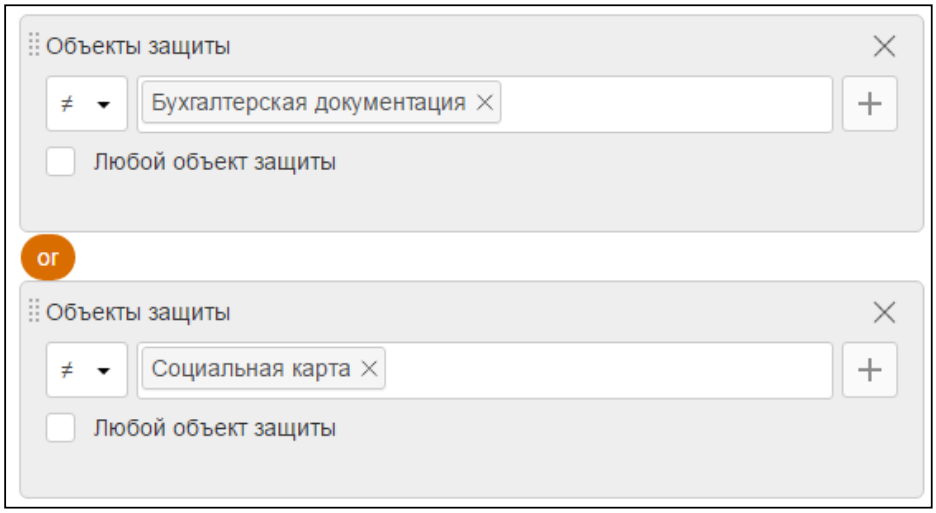
Для выбора режима используйте кнопки **Обычный** и **Расширенный** в поле **Тип запроса**.

Совет.

Если в процессе создания запроса в обычном режиме вы обнаружете, 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 нет ни одного из указанных элементов.



В данном примере событие не будет включено в отчет, если в нем присутствует объект защиты "Бухгалтерская документация" или "Социальная карта".

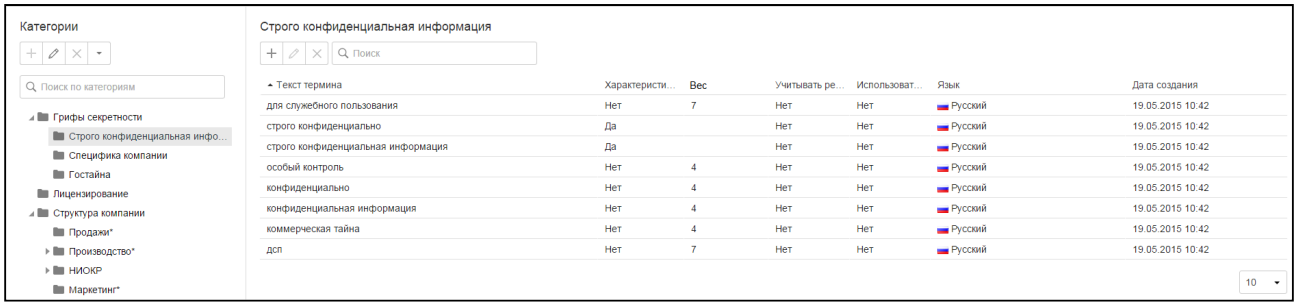
Целевые действия пользователя:

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

4.4 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, а также список предустановленных графических объектов.



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

Целевые действия пользователя:

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

4.4.1 Категории и термины

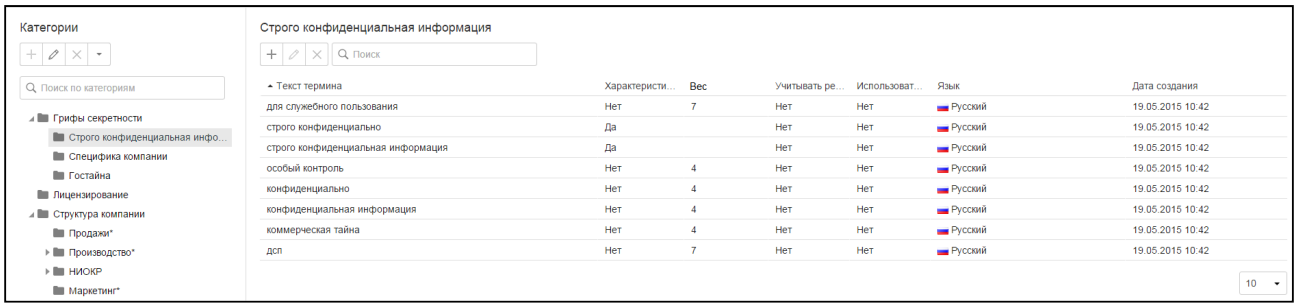
Справочная информация:

Категории и термины - это набор данных, 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 *Финансы* содержит финансовую терминологию (*платеж*, *инвесторы*, *цены* и пр.). Таким образом, наличие в тексте терминов "платеж", "инвесторы" или "цены" позволяет соотнести текст с категорией *Финансы*.

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.



Целевые 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, *Грифы секретности* или *Термины проекта*). Содержит либо перечень категорий (подкатегорий), либо перечень терминов, характерных для данной категории.

> **Примечание:**
>
> Предустановленные категории, помеченные знаком астериска (*), не содержат объектов и заполняются на этапе внедрения Системы или позже, в рамках кастомизации.

Для категории указывается ее название и при необходимости добавляется описание.

Для терминов, входящих в категорию, указываются следующие атрибуты:

- Вес - значение, указываемое по умолчанию для всех терминов категории в качестве атрибута **Вес**;
- Язык - язык терминов категории;

- Учитывать морфологию - при выборе данной настройки анализ выполняется с учетом всех морфологических форм термина;
- Учитывать регистр - при выборе данной настройки анализ выполняется с учетом регистра.

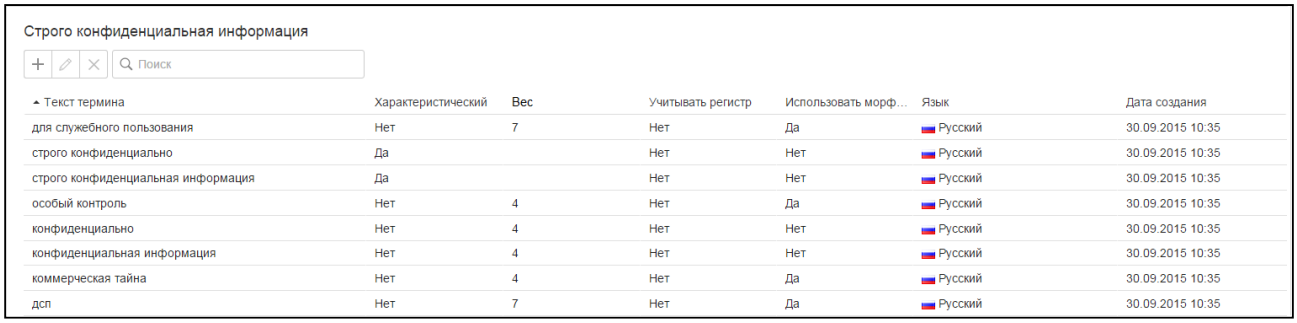
Для того чтобы категория детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

Целевые 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, нахождение которого в анализируемом тексте увеличивает степень соответствия этого текста категории, содержащей термин
Характеристический	Если данный атрибут включен, нахождение в трафике термина обязательно присваивает объекту категорию, содержащую термин
Вес	Показатель значимости термина
Учитывать регистр	Показатель учета регистра при анализе трафика
Учитывать морфологию	Показатель использования морфологии при анализе трафика
Язык	Язык термина

Примечание:

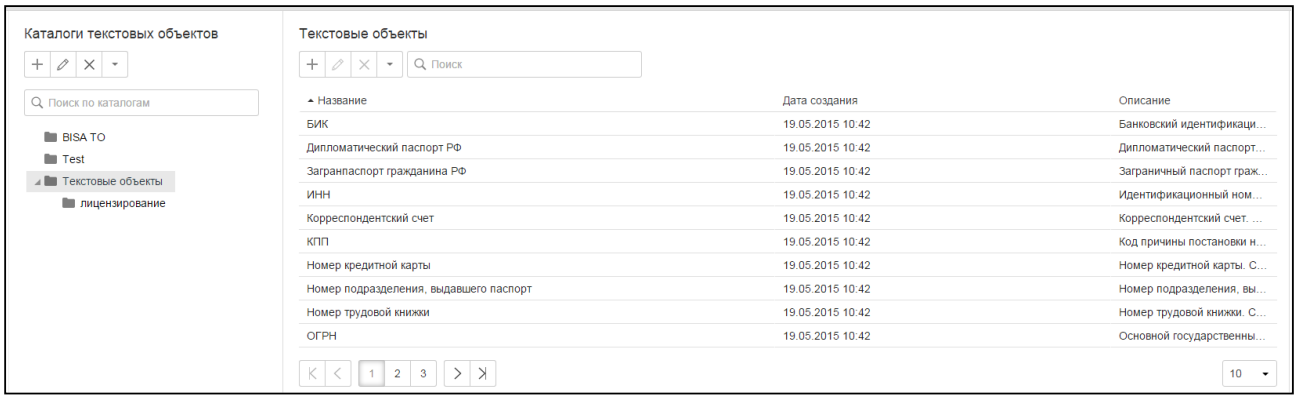
Настройки параметров **Учитывать регистр** и **Учитывать морфологию для термина** задаются по умолчанию при указании аналогичных параметров для категории. Параметры термина могут быть отредактированы и сохранены отдельно, но при изменении настроек регистра и морфологии для категории данные изменения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

Целевые действия пользователя:

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

4.4.2 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.

Целевые действия пользователя:

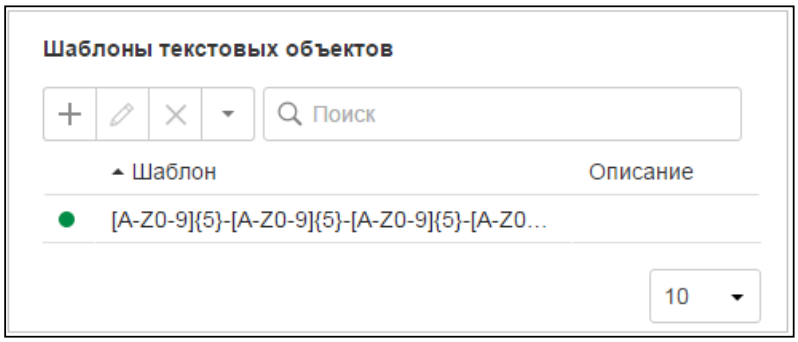
- создание текстовых объектов и их каталогов (см. "Работа с текстовыми объектами")
- добавление системных текстовых объектов в выбранный каталог (см. "Работа с текстовыми объектами")

- 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

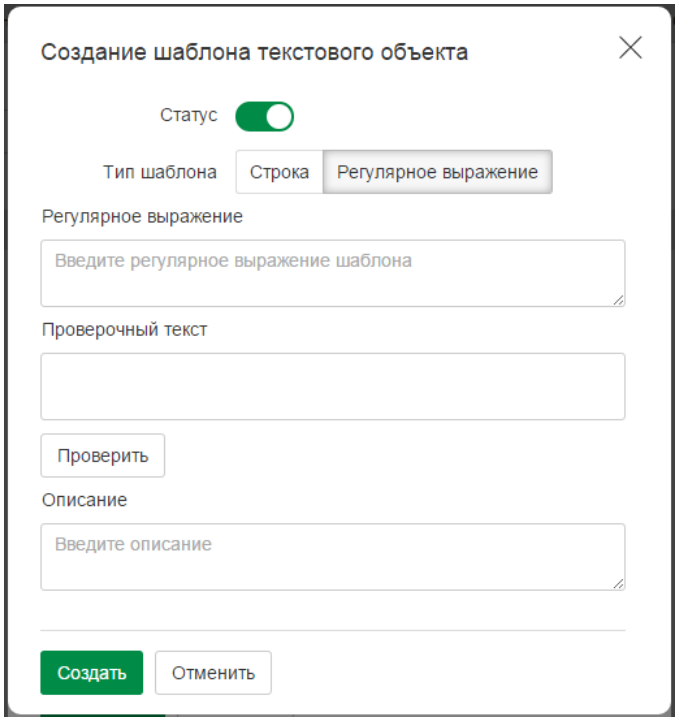
Справочная информация:
Шаблон текстового объекта - значение текстового объекта, заданное в виде точной последовательности символов либо с помощью регулярного выражения. С помощью шаблона для каждого текстового объекта может быть задано одно или несколько значений.

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 создании настраиваемого шаблона см. в интернет-статье "Элементы языка регулярных выражений".
Проверочный текст	Отображается, если выбран тип шаблона - *Регулярное выражение*. Пример текста для проверки нахождения регулярного выражения. Введите проверочный текст в поле и нажмите **Проверить**.
Описание	При необходимости добавьте описание шаблона

Целевые действия пользователя:

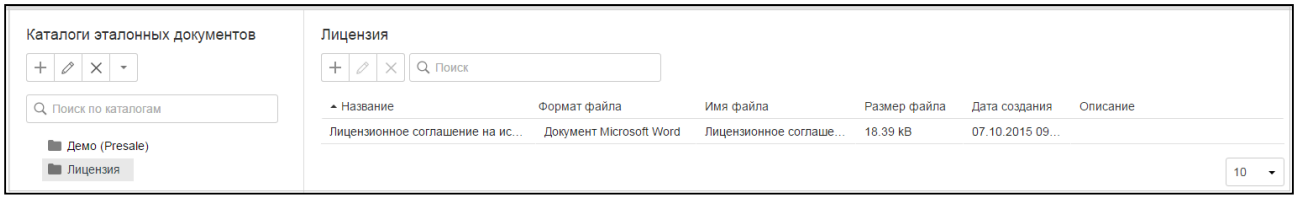
- Создание текстового объекта

4.4.3 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);

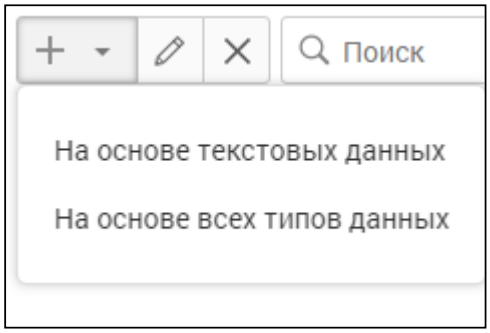
Эталонные документы создаются внутри каталогов. Для работы с каталогами эталонных документов (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части рабочей области.
В правой части рабочей области расположен список эталонных документов внутри выделенного 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.

Целевые 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")

4.4.4 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.

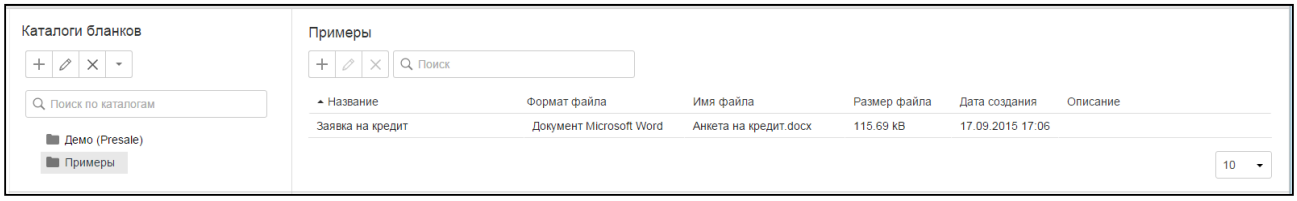
Для того чтобы бланк детектировался в перехваченных данных, его необходимо включить в объект защиты.

Важно!

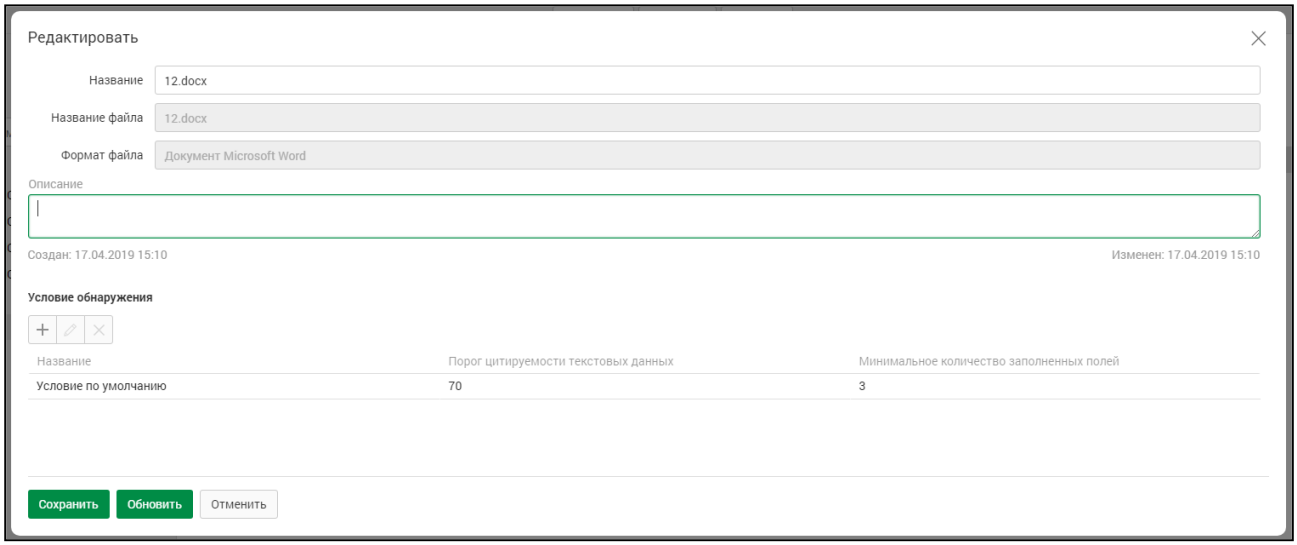
Для соотнесения объекта перехвата с бланком необходимо, чтобы выполнялись следующие условия:

- 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.



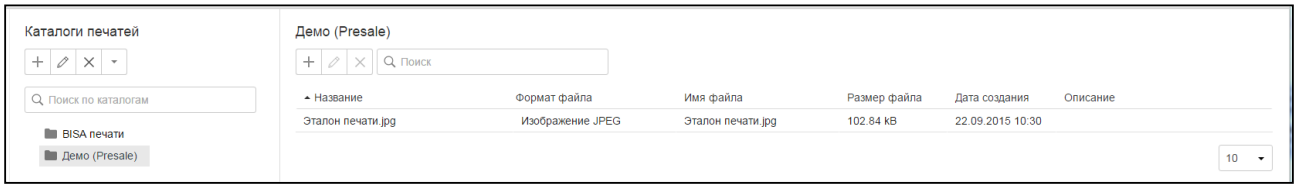
Целевые действия пользователя:

- 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")

4.4.5 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.

Целевые 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")

4.4.6 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:
>
> - размер файла - от 128 байт до 2 Гб;
> - 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);
> - размер выгрузки - не более 1 Гб, если используется База данных Postgre SQL.

Выгрузки создаются внутри каталогов. Для работы с каталогами выгрузок (создание, редактирование, 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 (добавление, редактирование, удаление, 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.



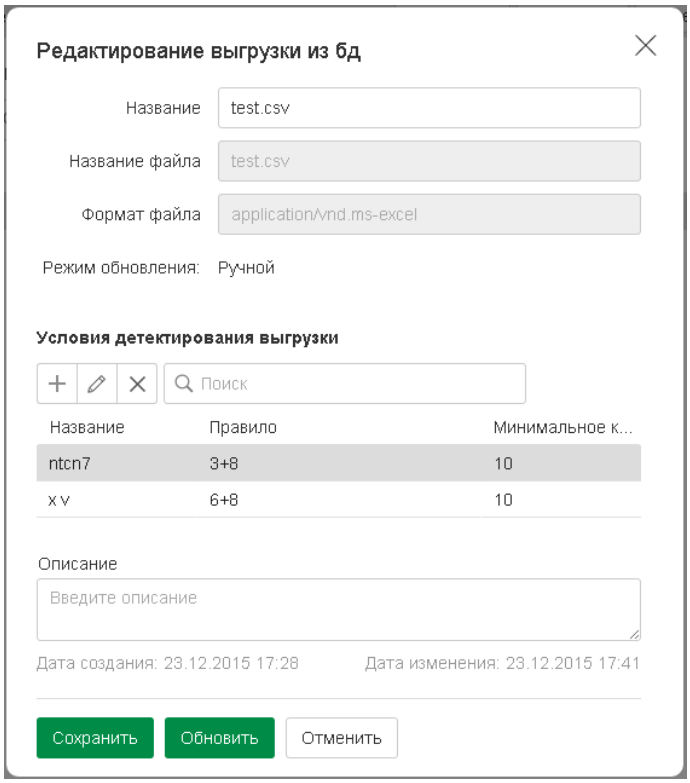
Предустановленный каталог **Автоматические выгрузки из БД** содержит выгрузки, полученные от внешней системы (подробнее см. "Автоматически обновляемые выгрузки из БД").

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 и минимальное количество непустых строк, требуемое для срабатывания выгрузки.

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



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

Целевые действия пользователя:

- создание выгрузок из БД и их каталогов (см. "Работа с эталонными выгрузками")
- обновление выгрузки (см. "Работа с эталонными 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.

Атрибуты автоматической выгрузки формируются на основе данных, переданных от внешней системы:

Параметр	Описание
Наименование	Название файла выгрузки в Системе
Источник обновления	Система - источник файла выгрузки
Комментарий к выгрузке	Сопроводительная информация
Условие срабатывания	Детектирование всех заполненных столбцов. Минимальное количество столбцов - `10` *Например:* При количестве столбцов `3`, условие будет иметь следующий вид: `1+2+3`, минимальное количество строк - `10`.

Вы также можете добавить выгрузки в каталог **Автоматические выгрузки из БД** вручную. Для выгрузок, добавленных вручную, обновление будет выполняться стандартным способом (см. "Работа с выгрузками").

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.

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.

> **Внимание!**
>
> При удалении выгрузки, созданной внешней системой, автоматическое обновление данной выгрузки будет недоступно.

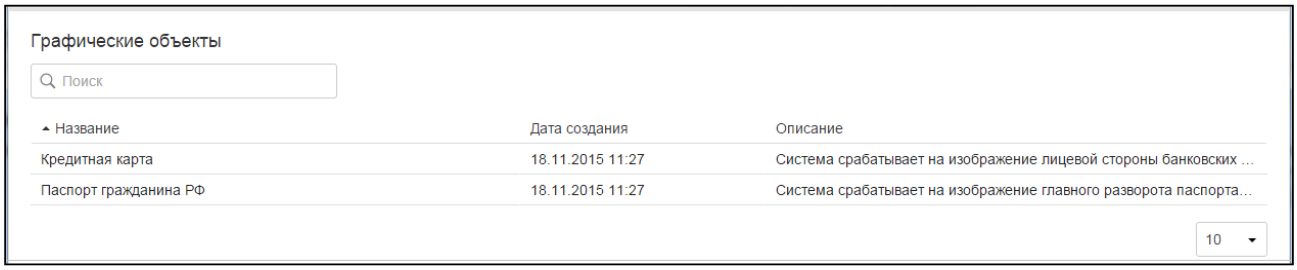
Для того чтобы автоматическая выгрузка детектировалась в перехваченных данных, ее необходимо включить в объект защиты.

4.4.7 Графические объекты

Справочная информация:

Графический объект - изображение, извлеченное из тела объекта и его вложений. Наличие в изображении определенных признаков позволяет отнести его к какому-либо классу предустановленных графических объектов.

Графические объекты используются при создании объектов защиты.



В Системе могут содержаться следующие предустановленные графические объекты (в соответствии с типом лицензии):

Название	Описание
Паспорт гражданина РФ	Изображение главного разворота паспорта гражданина РФ (стр. 2-3)
Кредитная карта	Изображение лицевой стороны банковских карт VISA, Visa Electron, MasterCard, Maestro, Мир

При необходимости набор графических объектов может быть расширен следующими видами изображений:

Название	Описание
Географические карты	Географическая карта или ее часть
Технические чертежи	Чертежи, представляющие собой набор черных линий на белом фоне

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)

Для того чтобы графический объект детектировался в перехваченных данных, его необходимо включить в объект защиты.В Системе используются только предустановленные графические объекты с заранее заданными атрибутами. Добавление, редактирование и удаление графических объектов недоступно.

Целевые действия пользователя:

- создание объекта защиты с использованием графических объектов (см. "Создание объекта защиты").

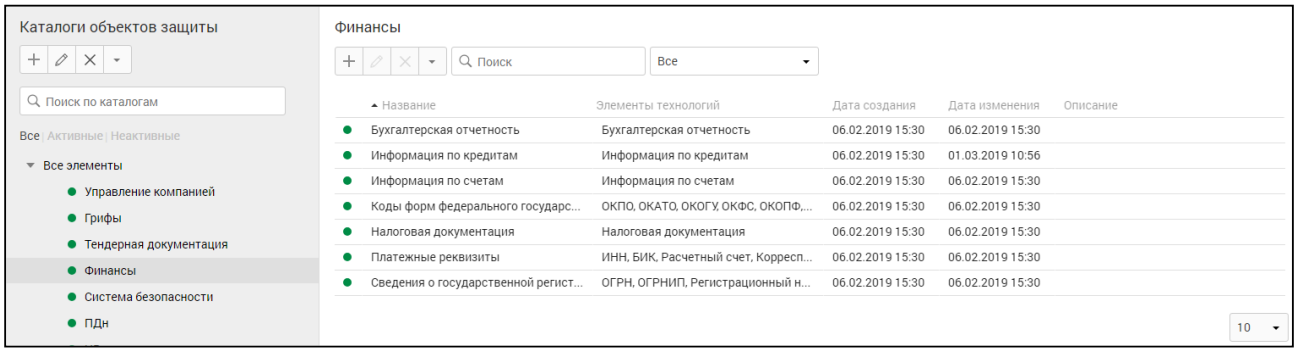
4.5 Раздел "Объекты защиты"

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.

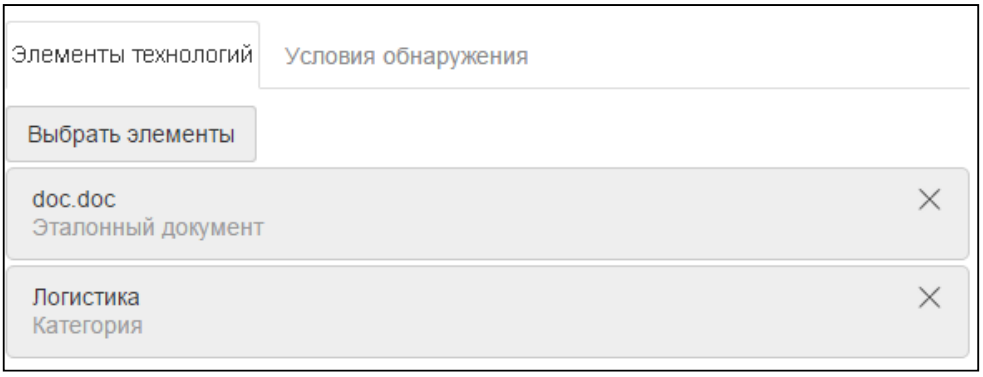
В режиме редактирования объекта защиты вы можете изменить список элементов технологий для выбранного объекта защиты и указать условия обнаружения.

Целевые 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

4.5.1 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).

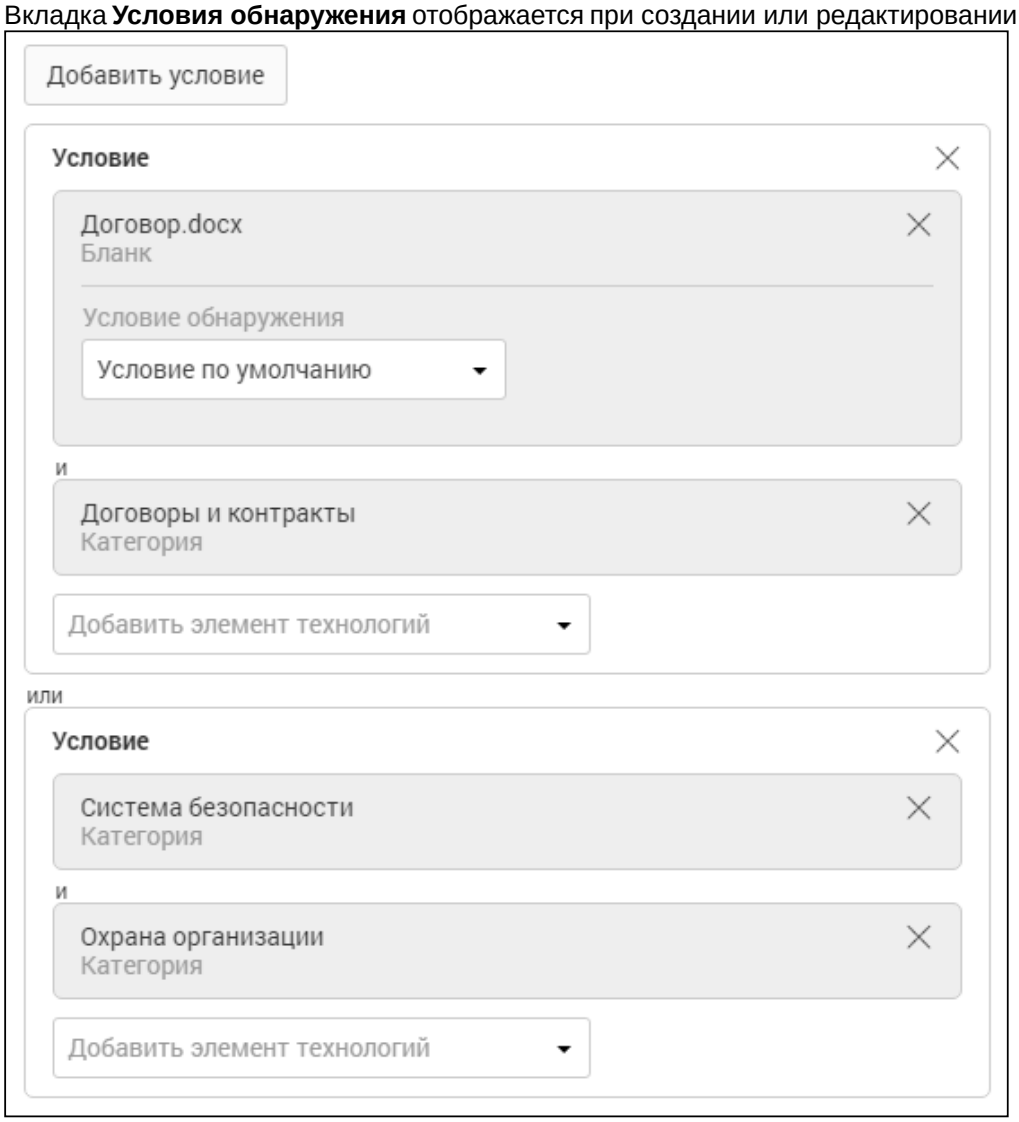
Условия детектирования добавленных элементов технологий указываются на вкладке **Условия обнаружения**.

Целевые действия пользователя:

- Добавление элементов технологий

4.5.2 Условия обнаружения

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



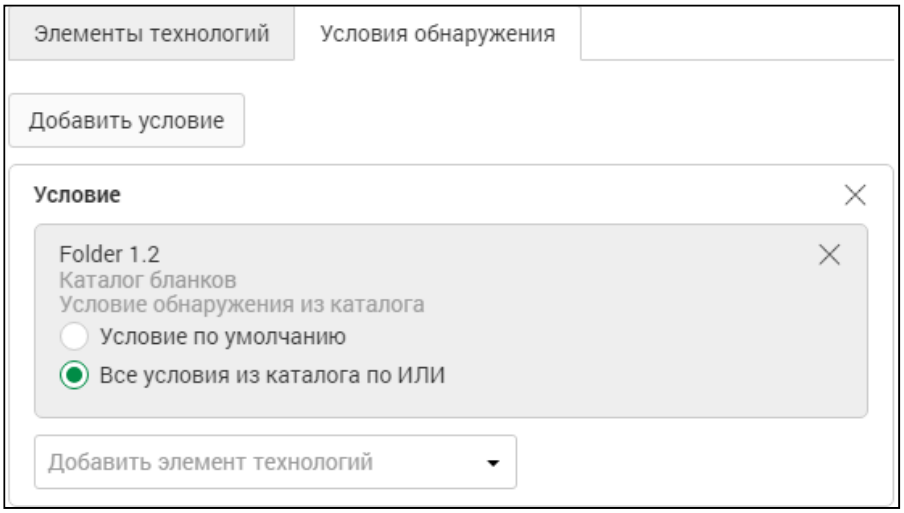
Вы можете указать условия обнаружения при создании объекта защиты, после того как требуемые элементы выбраны в окне добавления элементов технологий, или при переходе в режим редактирования ранее созданного объекта защиты.

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.

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, 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. 
Печать	Проверяется, содержит ли объект перехвата указанную печать
Графический объект	Проверяется, содержит ли объект перехвата указанный графический объект
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.

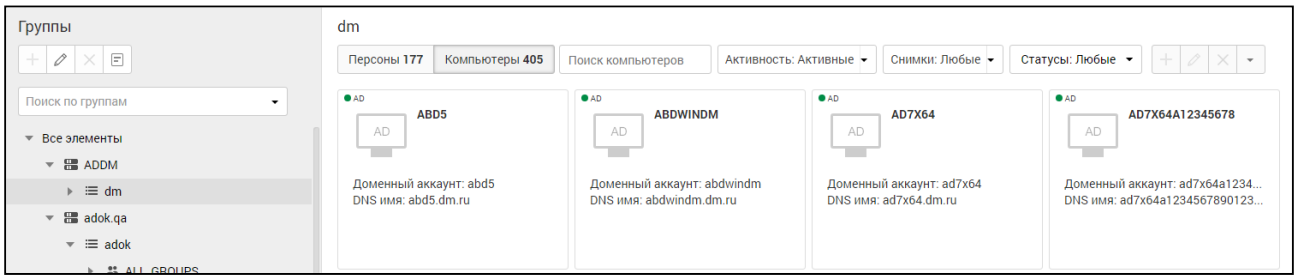
См. также: Элементы технологий

Целевые действия пользователя:

- Добавление условий обнаружения

4.6 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, Domino Directory, Astra Linux Directory, а также созданы средствами Traffic Monitor (см. "Создание группы персон и компьютеров").

Примечание.

Группы, для которых была выполнена синхронизация с Active Directory, отмечены значком .

Группы, для которых была выполнена синхронизация с Domino Directory, отмечены значком . Группы, для которых была выполнена синхронизация с Astra Linux Directory, отмечены значком .

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").

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 AD.

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:

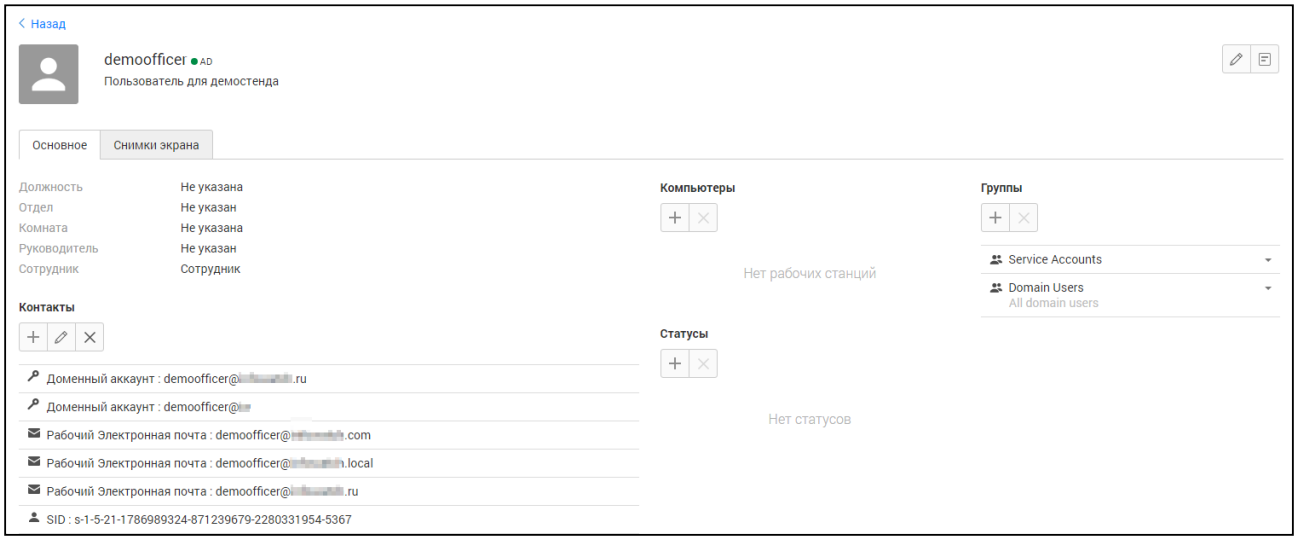
- Создание группы персон и компьютеров (см. "Создание группы персон и компьютеров")
- Создание персон и компьютеров (см. "Создание персон и компьютеров")
- Просмотр виджетов с информацией о персонах и компьютерах (см. "Просмотр сводки по персоне/компьютеру")
- Создание фильтра по персонам и компьютерам (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")

4.6.1 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 или Astra Linux Directory, отображается цветовой индикатор в левом верхнем углу фотографии профиля:
> - для активных сотрудников, в том числе с истекшим сроком действия учетной записи в AD/ALD;
> - для сотрудников, отключенных в AD/ALD.

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".

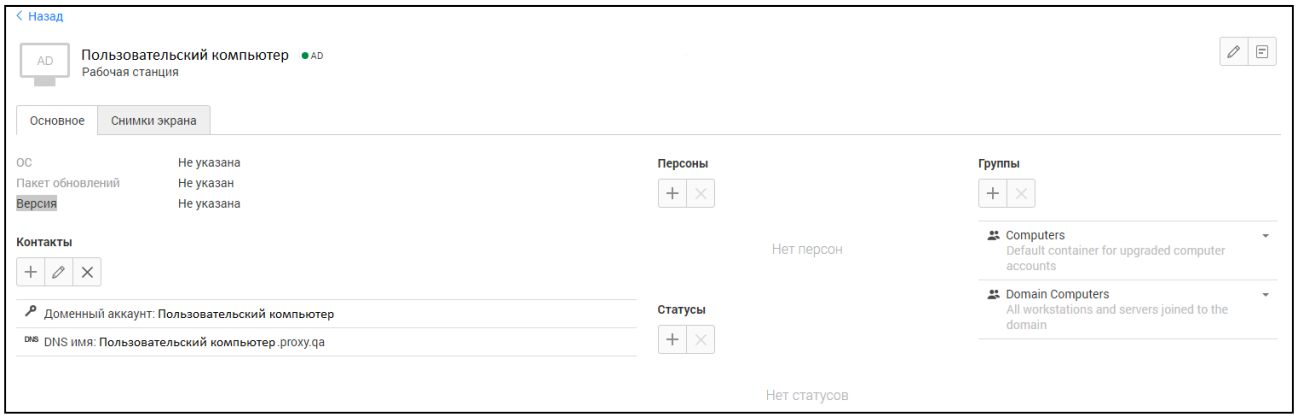
Целевые действия пользователя:

- Создание фильтра по персонам (см. "Создание запросов")
- Настройка карточки персоны ("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")

4.6.2 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".

Целевые 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")

4.6.3 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 отобрается 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**.

Целевые действия пользователя:

- Просмотр снимков экрана

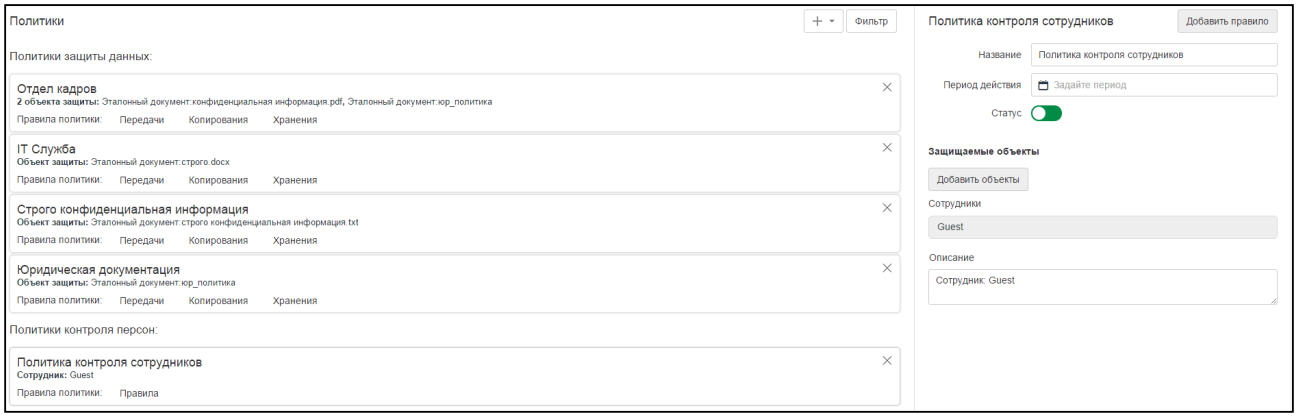
4.7 Раздел "Политики"

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.

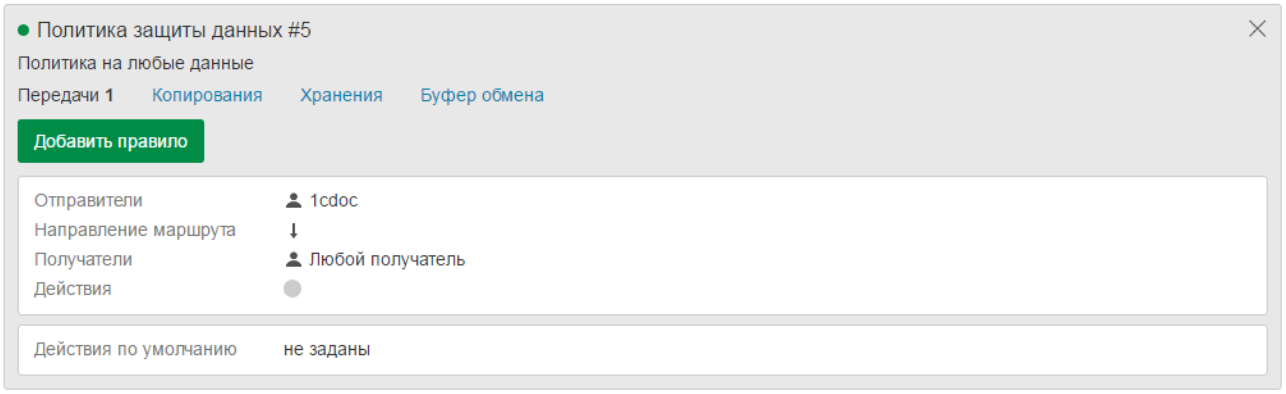
При нажатии кнопки **Фильтр** в правой части рабочей области отображается область **Настройка фильтра**, где вы можете отфильтровать политики по названию или объектам исследования.

Целевые 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")

4.7.1 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.

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

- Передачи данных
- Копирования данных

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;  - аккаунт Skype. Строка от 6 до 32 символов, должна начинаться с буквы; может содержать только латинские буквы, цифры и символы «.», «,», «-», «_»);  - 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;  - 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.

Целевые 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*
      - *Mail.Ru Агент*
      - *MS Lync*
      - *Skype*
      - *Telegram*
      - *XMPP*
      - *Facebook*
    - **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").

Целевые 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**;
- **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**.

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").

Целевые 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:
  - **Краулер**
- **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** - полное имя компьютера;
    - в поле **Введите путь** - путь к сетевому ресурсу в формате `<directory>\<subdirectory>` (путь указывается без использования групповых символов ? и *). Например: *share|123*
  - **Файловые хранилища**. Для добавления файлового хранилища SharePoint введите следующие значения в поля:
    - в поле **Введите источник** - IP-адрес или полное DNS-имя файлового хранилища;
    - в поле **Введите путь хранения** - путь к хранилищу в формате `<directory>` / `<subdirectory>` (путь указывается без использования групповых символов ? и *). Например: *Lib/Проектная документация*

  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").

Целевые 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.**
- **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 приложением-приемником является терминальная сессия. Если отмечена эта опция, выбор приложения-приемника вручную недоступен.
- **Приложение-источник** (только для типа события **Буфер обмена**) - приложение, копирование данных из которого приводит к срабатыванию правила;
- **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").

Целевые 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").

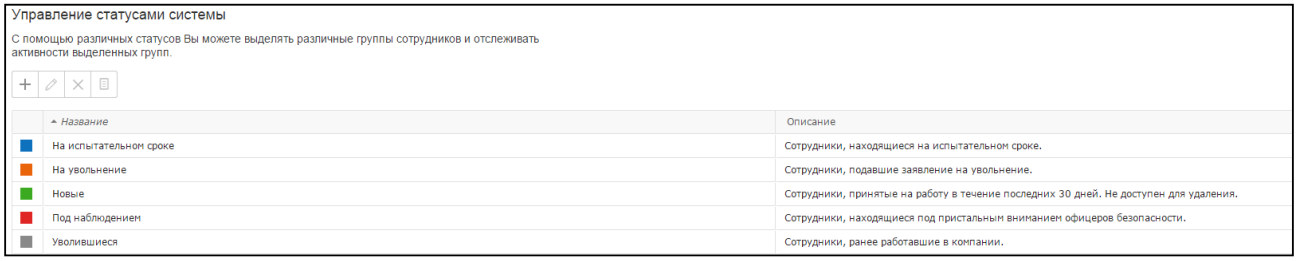
Целевые действия пользователя:

- Создание правил
- Настройка уведомлений в правилах

4.8 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
- Веб-ресурсы
- Статусы
- Периметры
- Файловые типы

Целевые 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 ("Создание политики защиты данных" и "Создание политики защиты данных на агентах")

4.8.1 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.

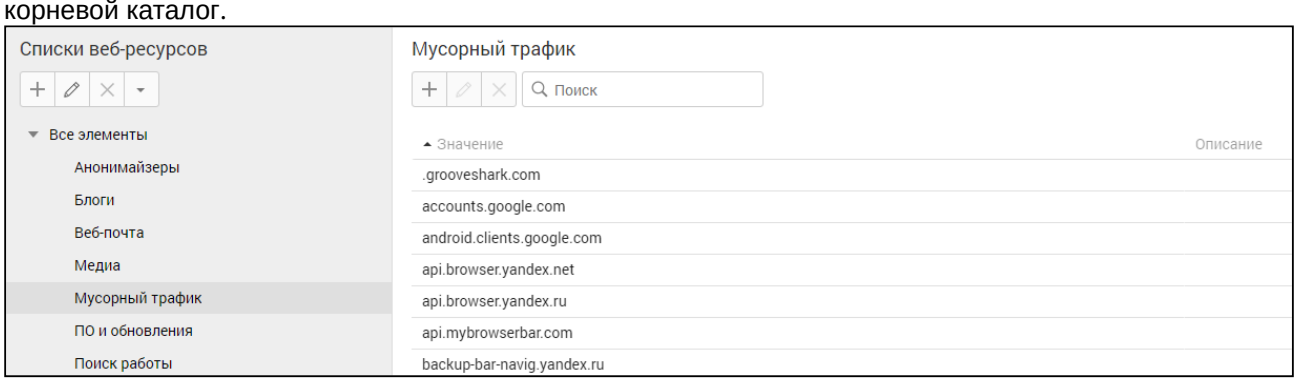
Целевые действия пользователя:

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

4.8.2 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) используются инструменты в левой части рабочей области.
В правой части рабочей области отображены веб-ресурсы внутри выделенного списка, а также инструменты для работы с веб-ресурсами (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. Чтобы осуществлять поиск 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

Целевые действия пользователя:

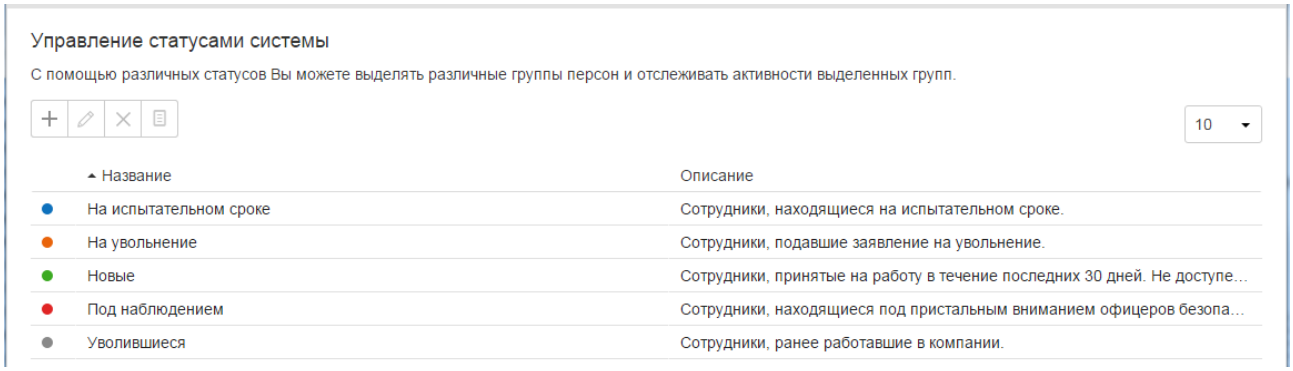
- Формирование списка веб-ресурсов (см. "Работа с веб-ресурсами")

4.8.3 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, Domino Directory или Astra Linux Directory;
- 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.

Целевые 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**)

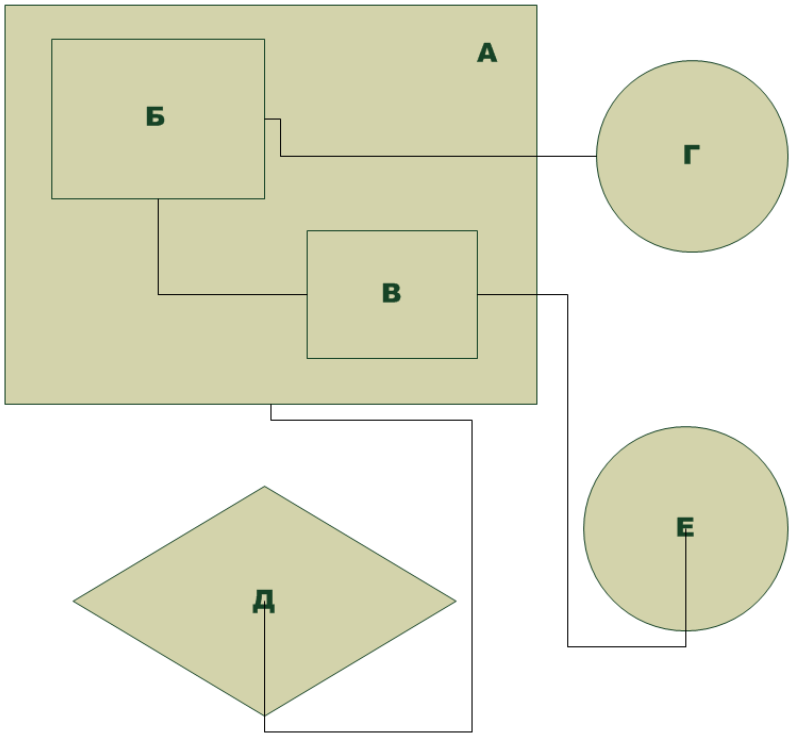
- При добавлении политики контроля персон - выбор в качестве объектов исследования персон с определенными статусами (см. "Создание политики контроля персон")

4.8.4 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").

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.

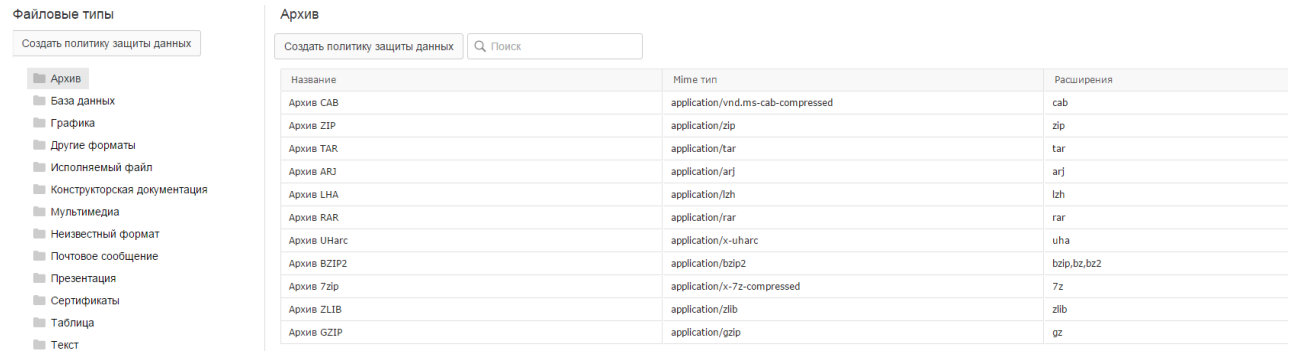
Целевые действия пользователя:

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

4.8.5 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 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.

Целевые действия пользователя:

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

4.9 Раздел "Управление"

Раздел **Управление** содержит следующие подразделы:

- LDAP-синхронизация
- Лицензии
- Управление доступом
- Состояние Системы
- Аудит
- Контроль целостности
- Службы
- Плагины
- Настройки подключения
- Почтовые уведомления

О работе в разделе см. "Управление Системой".

4.10 Раздел "Краулер"

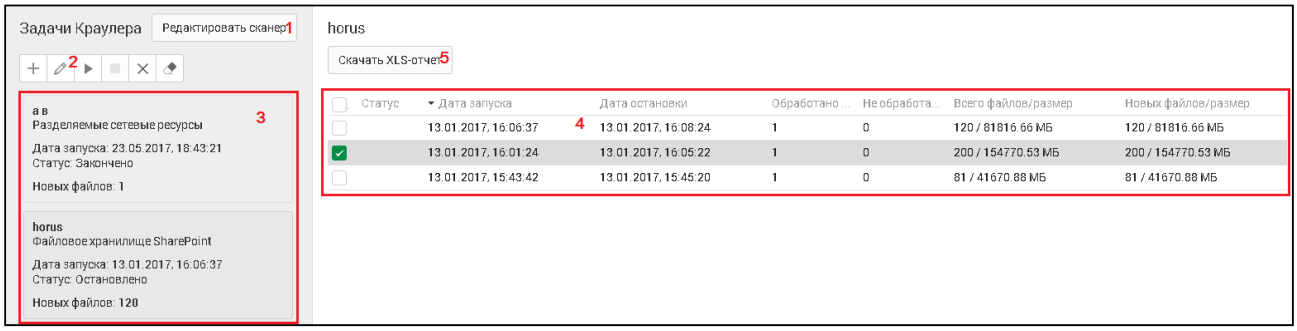
Справочная информация:
Подсистема ***Краулер*** системы InfoWatch Traffic Monitor позволяет выполнять проверку файлов в корпоративной сети на предмет нарушения корпоративных политик безопасности. Проверка файлов выполняется с помощью *сканера* - специального модуля, сканирующего места хранения информации (см. "Сканер").

Функции Краулера:

- Сканирование сетевых папок, открытых для удаленного доступа по протоколу SMB.
- Сканирование локальных дисков рабочих станций, работающих под управлением ОС Windows.
- Сканирование файлового хранилища SharePoint. Выполняет проверку документов, хранящихся в БД Microsoft SharePoint 2007/2010/2013. При этом рассматриваются только текущие версии файлов: история изменений не исследуется.
- Гибкая настройка задач сканирования с возможностью указать:
  - папки и сетевые узлы, на которых будет выполняться сканирование;
  - маски обрабатываемых файлов;
  - ограничения по размеру обрабатываемых файлов;
  - расписание выполнения задания (также возможен ручной запуск).
- Передача файлов для анализа на сервер InfoWatch Traffic Monitor. На сервер передаются только новые и измененные файлы, ранее обработанные файлы повторно не отправляются.
- Сохранение файлов согласно настройкам политики (по умолчанию сохраняются файлы, признанные потенциальным нарушением действующей политики безопасности)
- Результаты сканирования доступны в Консоли управления: вы можете просмотреть их с помощью запросов и в виде отчетов, в том числе предустановленных.

Краулер не выполняет удаления, перемещения, переименования, шифрования или каких-либо иных действий над файлами – даже в тех случаях, когда они признаны потенциальным нарушением. Происходит только информирование офицера безопасности об инциденте. Офицер безопасности может просмотреть в Консоли управления файлы, признанные потенциальным нарушением, и получить информацию об их расположении и пользователях, имеющих к ним доступ.

О разделе:
Раздел **Краулер** содержит список задач сканирования и средства для работы с задачами.



В левой части рабочей области расположены следующие элементы:

- кнопка **Редактировать сканер** (№1 на рисунке), с помощью которой вы можете настроить параметры используемого сканера (см. "Настройка сканера");

- панель инструментов для работы с задачами сканирования (№2 на рисунке);
- список задач сканирования (№3 на рисунке).

Для создания новой задачи используется кнопка на панели инструментов (см. "Создание задачи").

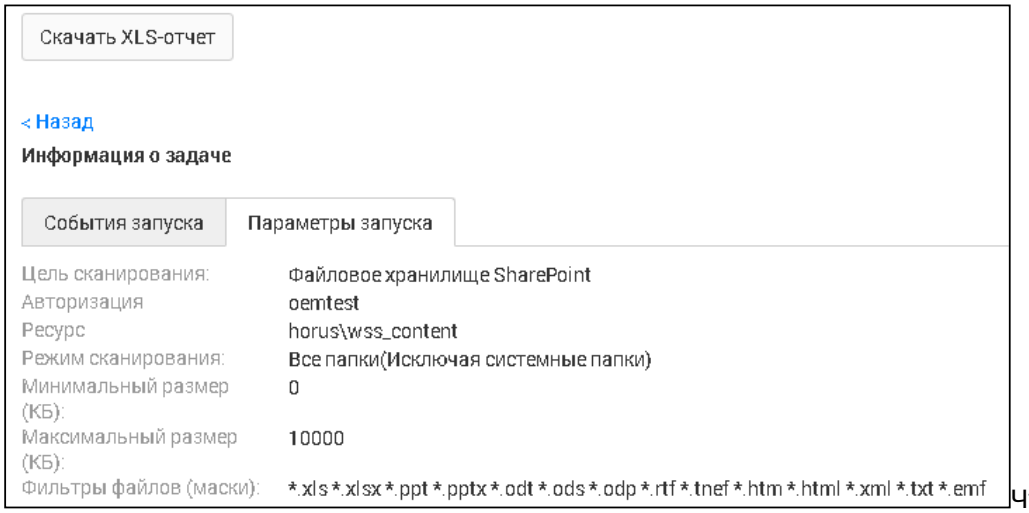
При выборе задачи в списке становятся доступны кнопки **Редактировать задачу**, **Запустить задачу**, **Удалить задачу** и **Очистить хеши задач**, а в правой части рабочей области отображается история запуска задачи (№4 на рисунке).

Если выполнение задачи запущено, вы можете остановить выполнение, нажав на панели инструментов.

В истории запуска задачи (№4 на рисунке) содержится краткая информация о запусках:

- Статус;
- Дата запуска и остановки задачи;
- Количество обработанных и необработанных компьютеров;
- Количество и размер обработанных файлов;
- Количество и размер новых файлов, обработанных за время выполнения задачи.

Чтобы просмотреть подробную информацию о выбранном запуске задачи, дважды щелкните по нужной строке в истории запуска. В правой части рабочей области отобразится информация о запуске. Информация представлена на следующих вкладках: **События запуска** и **Параметры запуска**.



Чтобы сохранить отчет в формате Excel для выбранной версии задачи, нажмите **Скачать XLS-отчет**.

Чтобы вернуться к истории запуска задачи, нажмите **<Назад**.

Вы также можете сохранить отчеты в формате Excel сразу для нескольких версий задачи. Для этого установите флажки напротив выбранных версий в истории запуска задачи и нажмите кнопку **Скачать XLS-отчет** (№5 на рисунке).

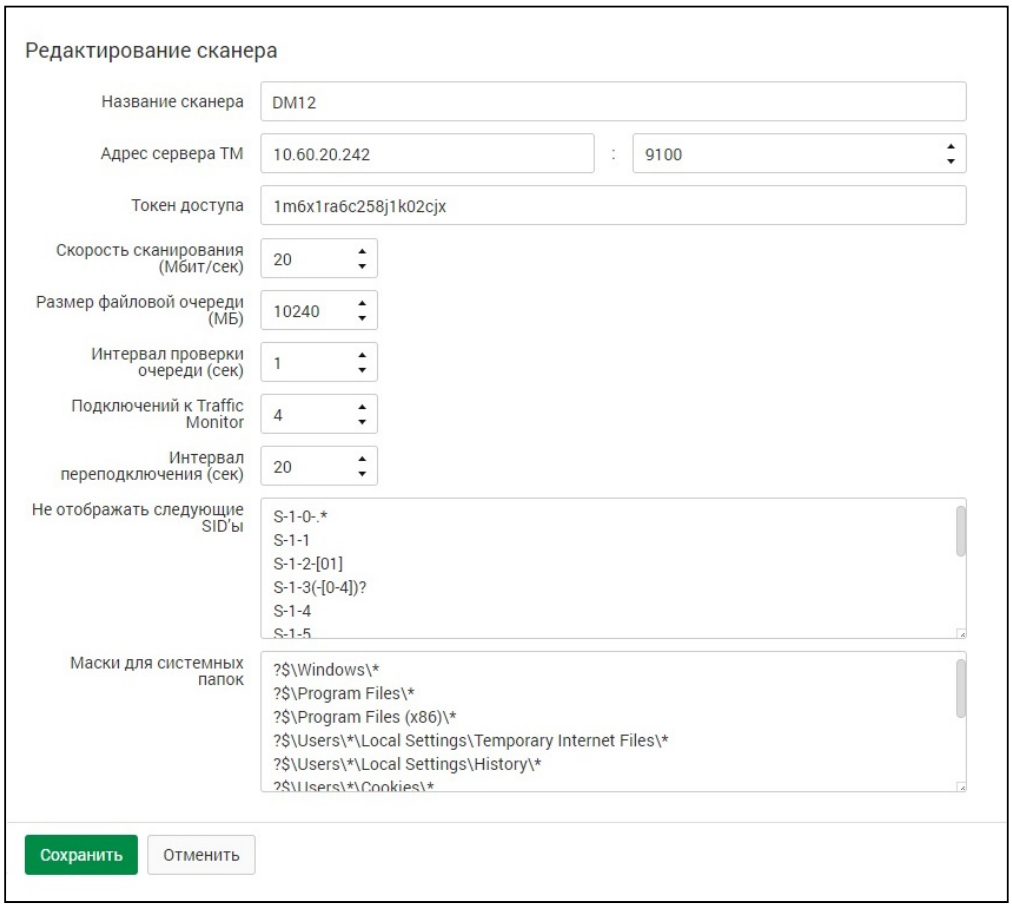
Целевые действия пользователя:

- Настройка сканера
- Создание задачи
- Очистка хешей

4.10.1 Сканер

Справочная информация:
Сканер - модуль подсистемы Краулер, выполняющий сканирование мест хранения информации (хранилище Microsoft SharePoint 2007/2010/2013, локальные диски рабочих станций, разделяемые сетевые ресурсы), определенных пользователем с помощью заданий на сканирование.

> **Примечание:**
>
> При сканировании хранилища SharePoint необходимо, чтобы Сканер находился с ним в одном домене.



Атрибуты сканера:

Параметр	Описание
Название сканера	Название сканера
Адрес сервера TM	IP-адрес сервера Traffic Monitor, где работает служба `iw_xapi`, и порт подключения службы

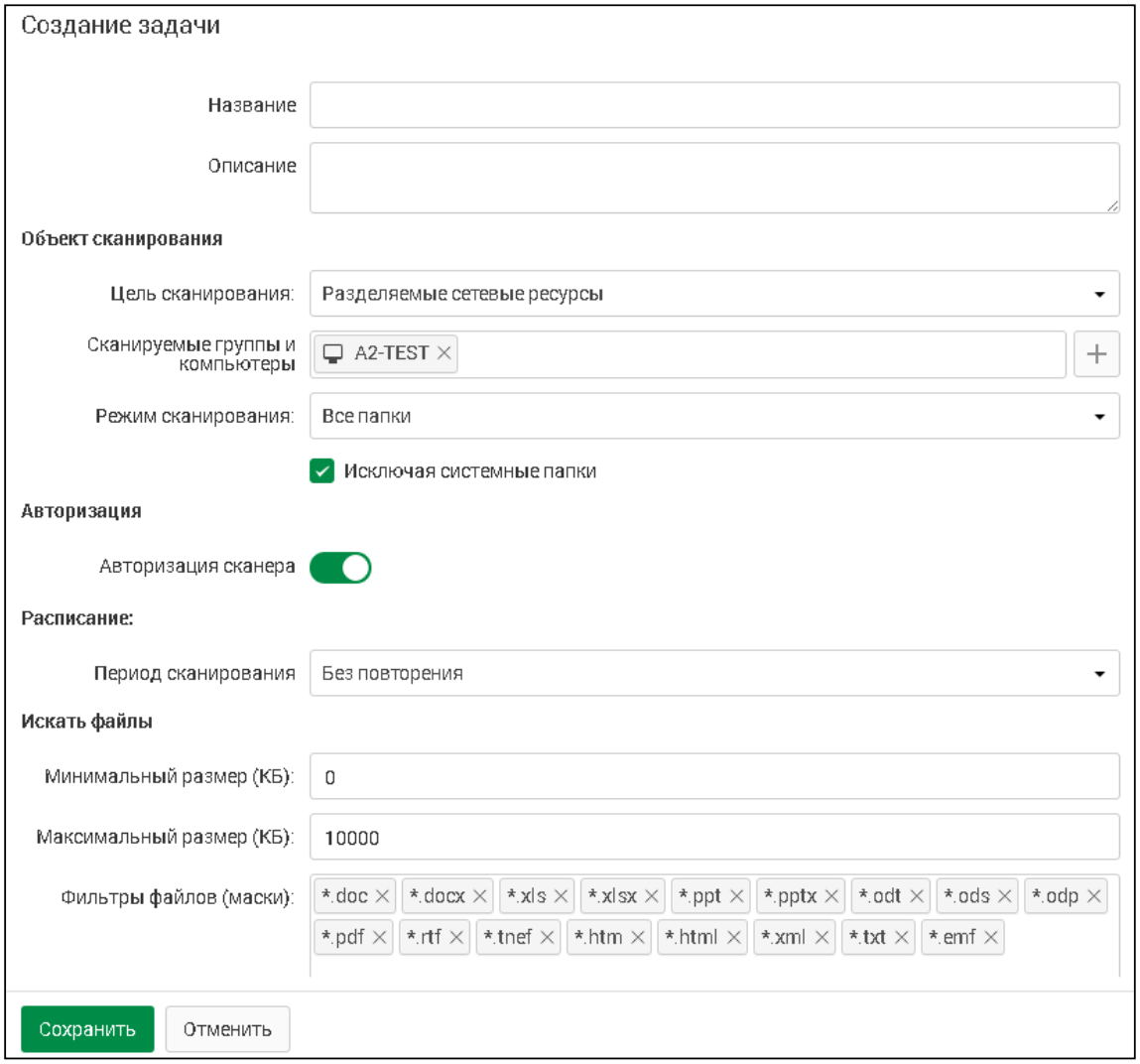
Токен доступа	Токен доступа на сервер Traffic Monitor для плагина службы Краулера
Скорость сканирования (Мбит/сек)	Максимальная скорость загрузки файлов с проверяемых ресурсов во временное хранилище, Мбит/с Позволяет снизить нагрузку на рабочую станцию, на которой производится сканирование
Размер файловой очереди (Мб)	Максимальный суммарный размер очереди, куда помещаются найденные файлы перед отправкой на сервер Traffic Monitor, Мбайт **Важно!** При достижении максимального суммарного размера задания останавливаются, и все файлы из этого буфера удаляются без отправки в Traffic Monitor.
Интервал проверки очереди (сек)	Интервал (в секундах), с которым сервер Краулер будет проверять наличие объектов в очереди для загрузки на сервер Traffic Monitor. Если в очереди есть хотя бы один объект, он будет передан на сервер Traffic Monitor
Подключений к Traffic Monitor	Максимальное количество одновременных подключений к серверу Traffic Monitor
Интервал переподключения (сек)	Интервал (в секундах), с которым сервер Краулер будет пытаться восстановить подключение к серверу Traffic Monitor в случае потери подключения
Не отображать следующие SID'ы	Позволяет настроить фильтр персон
Маски для системных папок	Маски папок, которые не будут сканироваться при работе сканера

Целевые действия пользователя:

- Настройка сканера

4.10.2 Задача сканирования

Справочная информация:
Задача сканирования - единичная или повторяющаяся операция проверки указанных мест хранения информации (хранилища Microsoft SharePoint 2007/2010/2013, локальные диски рабочих станций, разделяемые сетевые ресурсы) на наличие конфиденциальных данных (о том, как узазать конфиденциальные данные, см. "Определение конфиденциальной информации"). При создании новой или редактированнии ранее созданной задачи отображается диалоговое окно, в котором вы можете указать параметры задачи.



Параметры задачи:

Параметр	Описание
Название	Название задачи. Обязательный параметр
Описание	Описание задачи

Цель сканирования	Тип задачи сканирования: • **Разделяемые сетевые ресурсы** **Важно!** Краулер не предусматривает использование более одного домена Astra Linux для сканирования разделяемых сетевых ресурсов. • **Локальные диски рабочих станций** • **Файловое хранилище SharePoint** В зависимости от используемой версии SharePoint указываются следующие параметры: **Для SharePoint 2007 и 2010:** • **Версия SharePoint** - используемая версия SharePoint: 2007 или 2010; • **Адрес БД ресурса** - адрес сервера базы данных SharePoint. Например, sharepoint-test; • **Название БД ресурса** - имя экземпляра базы данных SharePoint. Например, wss_content. **Для SharePoint 2013:** • **Версия SharePoint** - используемая версия SharePoint: 2013; • **Адрес SharePoint сервера** - адрес сервера базы данных SharePoint, указывается с учетом протокола http:// или https://.
Сканируемые группы и компьютеры	Вы можете указать отдельные компьютеры, группы компьютеров и IP-адреса. Введите требуемые значения вручную либо нажмите +, чтобы выбрать значения из списка. Параметр является обязательным.

Режим сканирования	**Все папки** • в режиме **Разделяемые сетевые ресурсы** сканирует все доступные (открытые) папки • в режиме **Локальные диски рабочих станций** сканирует все папки на локальных дисках рабочей станции **Все папки, кроме** - сканирует все папки на рабочей станции с установленными исключениями **Только папки** - сканирует только папки, указанные пользователем **Примечание:** Если требуется сканировать в том числе системные папки, снимите флажок в поле **Исключить системные папки**. По умолчанию сканирование системных папок не выполняется. **Для написания пути сканирования используются следующие символы:** `*` - 0 или любое количество символов `?` - 0 или один любой символ `$` - символ, который используется Windows для указания скрытой папки **При сканировании разделяемого ресурса или хранилища SharePoint, можно использовать запросы типа:** `Docs*` - будет сканировать папку Docs и все подпапки при условии, что папка Docs находится в корневом каталоге хранилища или сетевого ресурса. **При сканирование локальных дисков и папок, можно использовать следующие запросы:** `C$\Docs\` - будет сканировать папку Docs `C$\Docs*` - будет сканировать папку Docs и все вложенные `*\Docs\` - будет сканировать папку Docs и все подпапки, вне зависимости от их расположения. `C:\Docs????\` - будет сканировать любую папку, которая имеет имя Docs с четырьмя дополнительными символами (Docs1234) на указанном диске **Важно!** В конце пути сканирования должен быть указан символ ***** либо ****.

Авторизация	Вы можете использовать авторизацию сканера (в этом случае сканирования будет выполняться под учетной записью, от имени которой запущен сканер) либо указать логин и пароль учетной записи вручную. По умолчанию используется авторизация сканера. **Важно!** При сканировании хранилища SharePoint должен быть указан пользователь сервера MS SQL, на котором расположена целевая БД **Важно!** Краулер использует доступ к контроллеру домена для получения информации о пользователе или группе по уникальному идентификатору (SID). Для обеспечения доступа учетная запись должна быть доменной и иметь права на чтение ресурса, который предполагается сканировать.
Период сканирования	Расписание, согласно которому производится сканирование **Важно!** Если выбран период **Ежемесячно**, то для запуска задания на сканирование необходимо, чтобы текущий месяц содержал дату, указанную в качестве значения параметра **День месяца**. Например, если выбрано значение 30, то в феврале сканирование запускаться не будет.
Минимальный размер (Кб)	Минимальный размер сканируемых файлов в килобайтах
Максимальный размер (Кб)	Максимальный размер сканируемых файлов в килобайтах
Фильтры файлов (маски)	Расширения сканируемых файлов. Обязательный параметр. Вы можете выбрать нужные расширения из раскрывающегося списка либо ввести значение вручную и нажать **Enter**. Чтобы удалить какое-либо значение, нажмите × рядом с выбранным расширением. **Примечание:** Если требуется сканировать все файлы, то в качестве значения укажите символ *.

Целевые действия пользователя:

- Создание задачи

5 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 подсистемой Краулер
- 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
- Раздел Краулер

5.1 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

5.1.1 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**.

5.1.2 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.

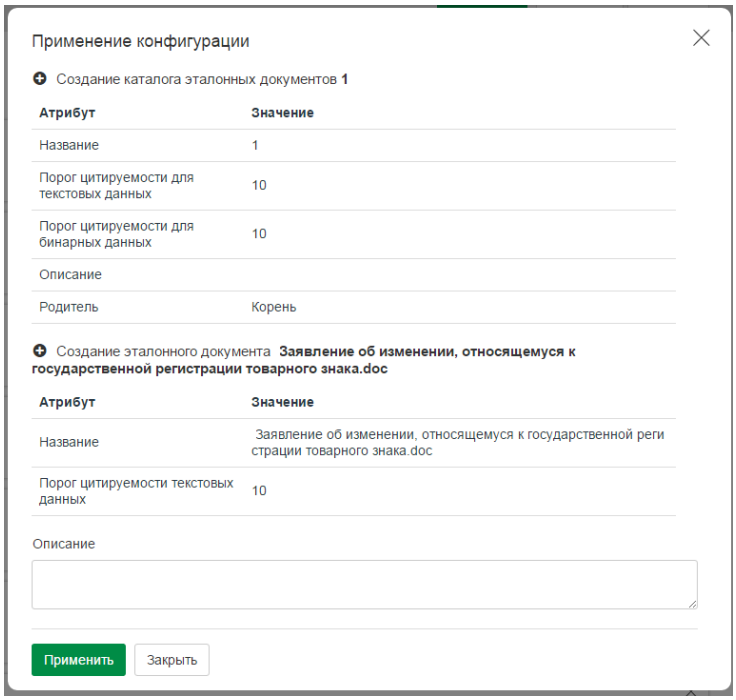
Решение:

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

   Откроется окно **Применение изменений конфигурации**, содержащее информацию о

внесенных изменениях:



2. При необходимости введите текст в поле **Описание**.
3. Нажмите **Применить**.

5.1.3 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**.

5.1.4 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**.

5.1.5 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".

5.1.6 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:
   - **Пароль**;
   - **Подтверждение пароля**.

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

3. Нажмите **Сохранить**.

5.1.7 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.

5.1.8 Вызов справки

Цель:
Получить справочную информацию о работе в Системе.
Решение:

1. В правом вехнем 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** - для перехода к онлайн-версии документации;

- **Офлайн** - 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.

5.1.9 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.

5.2 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. "Добавление статуса персонам").

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.

5.2.1 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.

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

Чтобы добавить группу Active Directory, Domino Directory или Astra Linux Directory в пользовательскую группу, выделите в списке групп нужную группу Active Directory, Domino Directory или Astra Linux Director 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, Domino Directory или Astra Linux Director, обновлялся автоматически, необходимо выполнить синхронизацию с LDAP-сервером.

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

Пример:

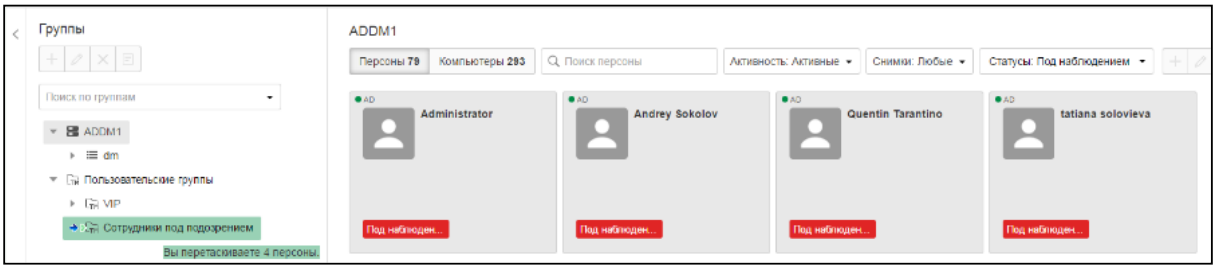
Требуется объединить сотрудников, находящихся под подозрением, в отдельную группу. Для этого:

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".

Дополнительные сведения:

Редактирование и удаление групп персон и компьютеров выполняются стандартным способом:

- Редактирование элемента
- Удаление элемента

5.2.2 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 щелчком левой кнопки мыши 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 добавить персону из контакта в событии:

1. Выберите непроидентифицированный контакт в событии щелчком мыши.
2. В открывшемся диалоговом окне выберите **Создать новую персону**.
3. Укажите параметры новой персоны и нажмите **Добавить.**

Дополнительные сведения:
Редактирование и удаление персон и компьютеров выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.2.3 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 целевую 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);
-  - 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);
-  - прочий Веб-аккаунт (строка от 1 символа).

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 щелчком мыши.
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 щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Персоны**.
4. Двойным щелчком левой кнопки мыши выделите целевую 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 щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Персоны**.
4. Двойным щелчком левой кнопки мыши выделите целевую 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 открывшемся окне подтверждения нажмите **Да**.

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

5.2.4 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 области щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Компьютеры.**
4. Двойным щелчком левой кнопки 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 щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Компьютеры.**

4. Двойным щелчком левой кнопки 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 щелчком левой кнопки мыши выделите требуемую группу.
3. В правой части рабочей области перейдите на вкладку **Компьютеры.**
4. Двойным щелчком левой кнопки 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.

5.2.5 Добавление статуса персонам

Цель:
Добавить статус персоне или компьютеру.

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** - чтобы добавить статус персоне;
- **Компьютеры** - чтобы добавить статус компьютеру.

4. Выделите целевую персону или целевой 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, Domino Directory или Astra Linux Directory статус *Новый* сохраняется в течение 30 дней с момента создания записей в Active Directory, Domino Directory или Astra Linux Directory соответственно).

См. также:

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

5.2.6 Просмотр снимков экрана

Предварительные настройки:

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

Если в вашей организации не используется Active Directory, 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, установленных на ОС Astra Linux, 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 или Astra Linux Directory для персон также можно указать доменный аккаунт.

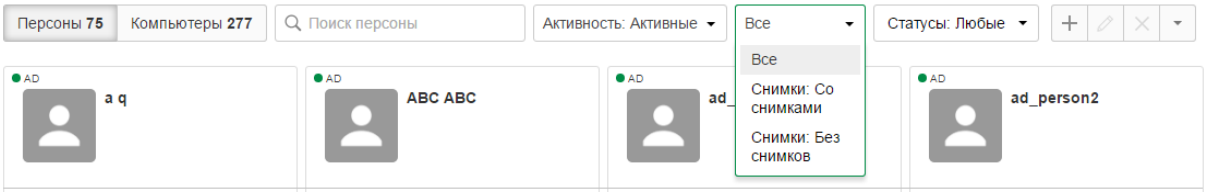
> **Важно!**
>
> Указанные шаги необходимо выполнить до создания правила Device Monitor (см. "Правило (DM) для ScreenShot Monitor") и распространения политики Device Monitor, содержащей данное правило, на рабочие станции. В противном случае снимки экрана не будут отображаться в Системе.

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 посмореть 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**.

5.3 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:

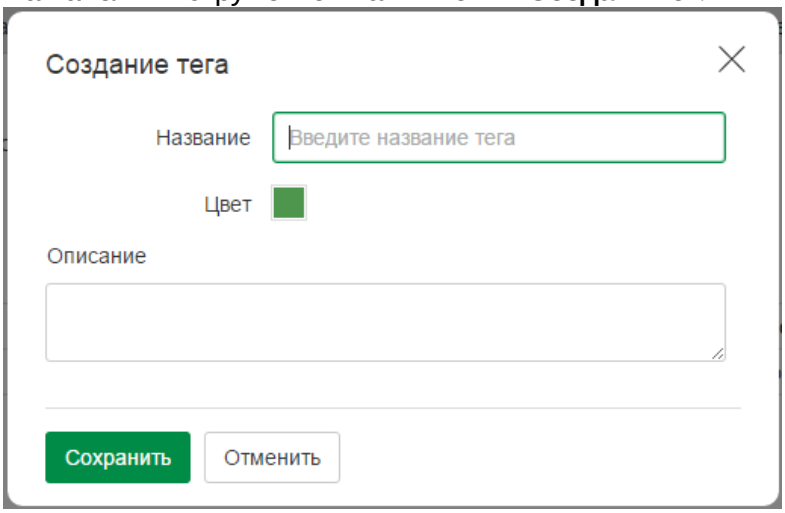
- "Раздел Списки" - о разделе, в котором ведется работа со списками

5.3.1 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.

Дополнительные сведения:
Редактирование и удаление тега выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

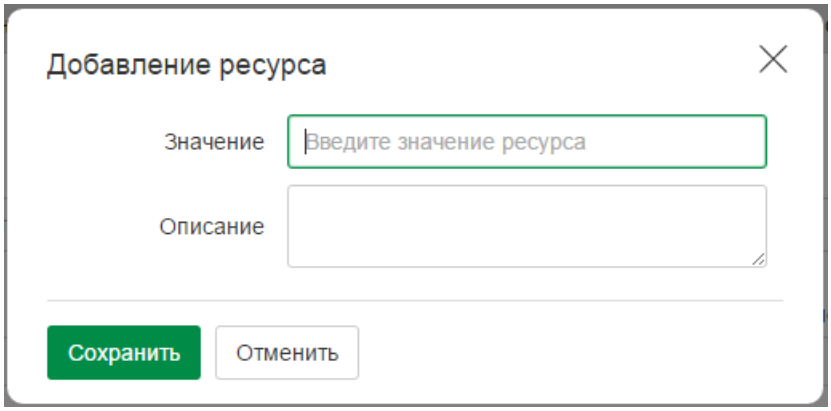
5.3.2 Работа с веб-ресурсами

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

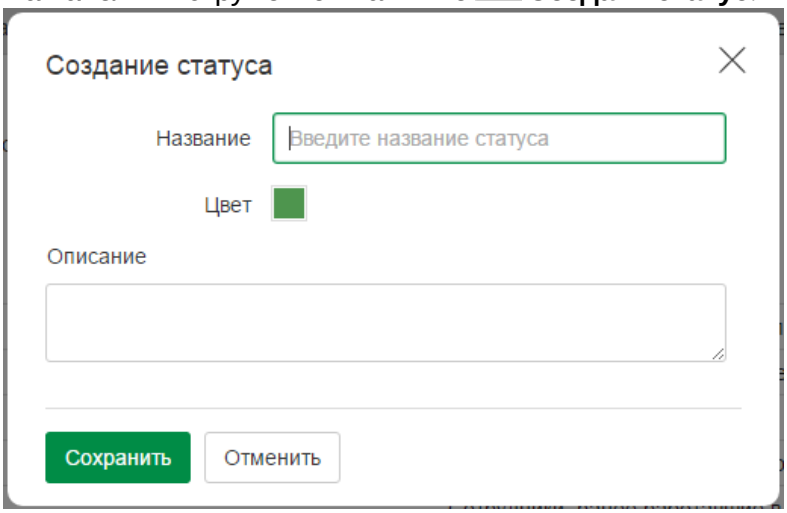
5.3.3 Работа со статусами

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 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").

Дополнительные сведения:

Редактирование и удаление статуса выполняются стандартным способом:

- Редактирование элемента
- Удаление элемента

5.3.4 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.

По умолчанию в Системе созданы следующие 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. *Цель 2* в данной статье).

Помимо предустановленных периметров, вы можете создать периметры вручную на основе следующих элементов:

- Адрес электронной почты
- Веб-ресурс
- Телефон
- Skype-контакт
- ICQ-контакт
- Домен
- Lotus-контакт
- Персона
- Группа персон

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

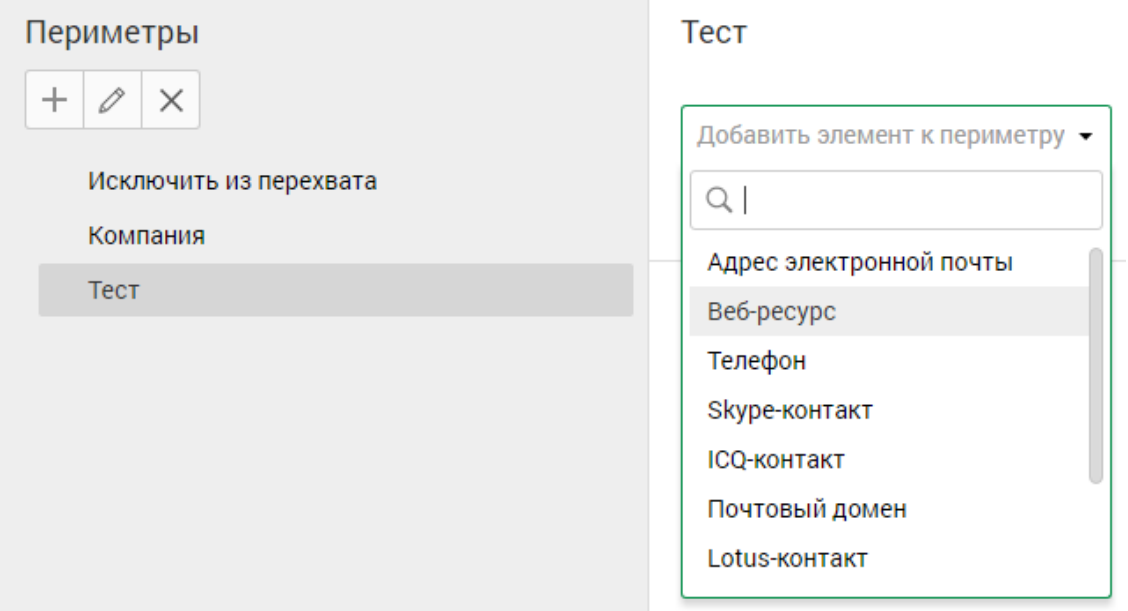
Цель:

1. Создать периметр.
2. Добавить элемент в периметр.

Решение:

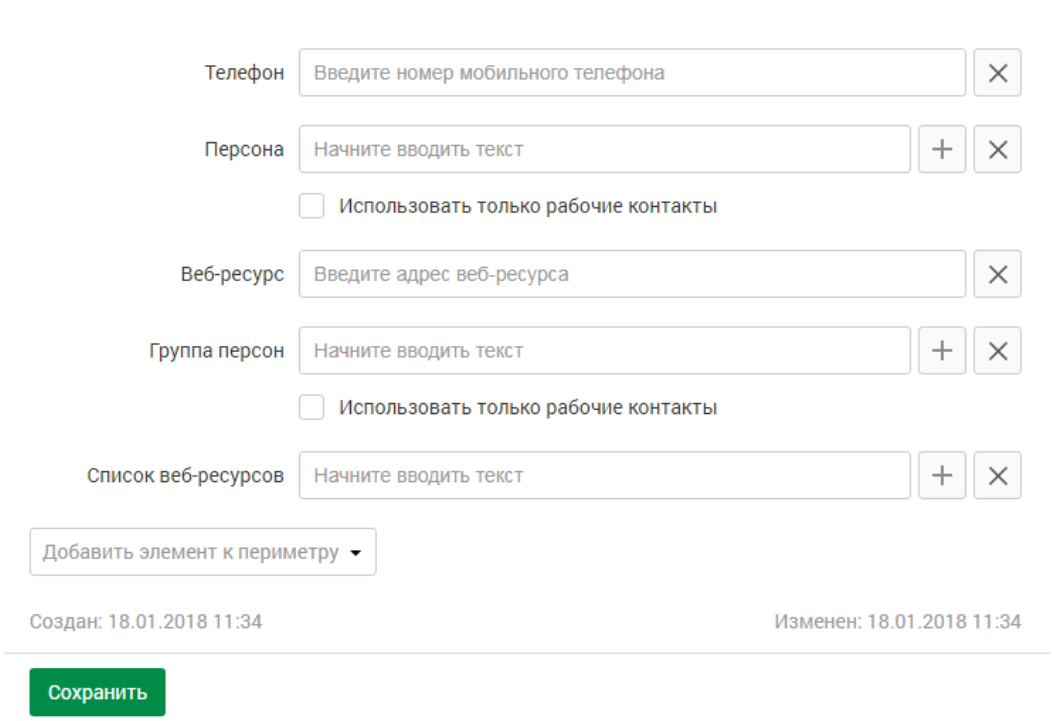
1. Создание периметра.
   a. Перейдите в раздел **Списки**, в подраздел **Периметры**.
   b. В левой части рабочей области нажмите + **Создать периметр**.
   c. В открывшемся диалоговом окне в поле **Название** укажите название добавляемого периметра.
   d. В поле **Описание** введите описание периметра (необязательно).
   e. Нажмите **Сохранить**.
2. Добавление элемента в периметр.
   a. Перейдите в раздел **Списки**, в подраздел **Периметры**.
   b. В левой части рабочей области щелчком левой кнопки мыши выделите нужный периметр.

c. В правой части рабочей области нажмите **Добавить элемент к периметру** и в раскрывающемся списке выберите требуемый тип элемента.



d. 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 целевым элементом. Нажмите **Добавить**.
   - Для *Адреса электронной почты*, *Веб-ресурса*, *Телефона*, *Skype*, *ICQ*, *Домена* и *Lotus-контакта* - введите название или значение в поле и

нажмите **Enter**.



Примечание:

Если указано доменное имя первого уровня, то домены вложенных уровней также будут включены в периметр. Например, при добавлении в периметр домена `domain.com`, домен вложенного уровня `basic.domain.com` тоже будет учитываться.

Примечание.

В качестве значения веб-ресурса может быть указано DNS-имя или IP-адрес (v4, v6) с типом контакта URL.

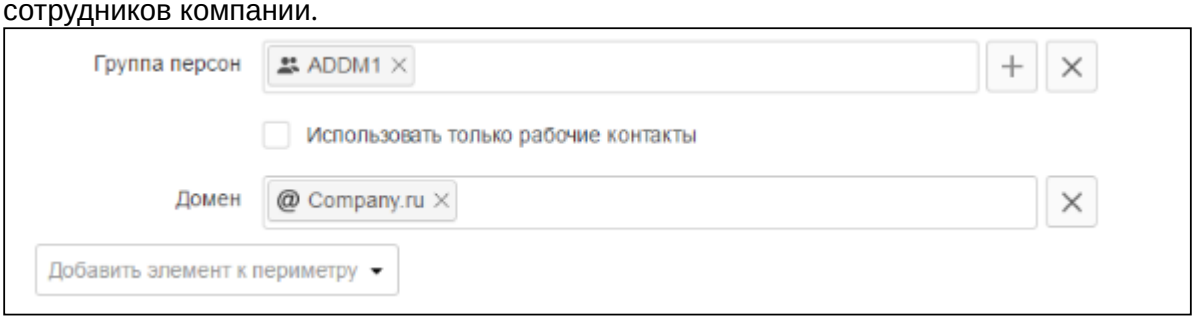
e. Введенные значения будут добавлены в список элементов. Чтобы удалить отдельный элемент из списка, нажмите × рядом с названием элемента. Чтобы удалить весь список элементов определенного типа, нажмите кнопку × напротив строки со списком элементов.



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 считается легитимной. В этом случае:

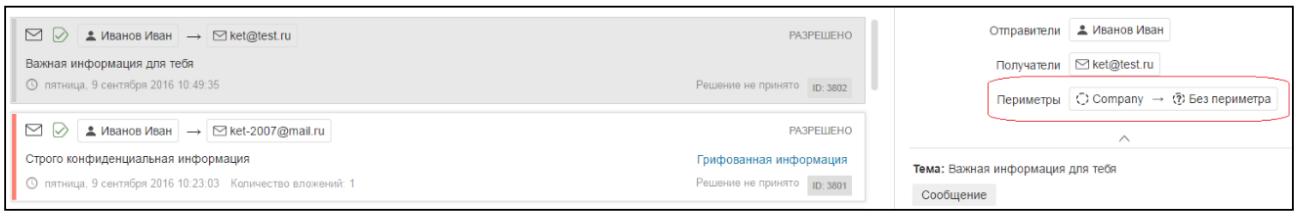
1. Создайте периметр *Компания* (если в Системе уже есть периметр *Компания*, пропустите этот шаг).
2. Добавьте в периметр почтовый домен `@company.ru` и группу персон AD, содержащую сотрудников компании.



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", вы можете быстро найти все события отправки данных за пределы компании.



Дополнительные сведения:

Редактирование и удаление периметра выполняются стандартными средствами:

- Редактирование элемента
- Удаление элемента

5.4 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 элементов базы технологий вы можете указать Системе, какая информация является конфиденциальной в рамках компании (т.е. разглашение какой информации является нарушением политики корпоративной безопасности). На основе базы технологий выполняется анализ действий персон, в результате которого выявляются нарушения политики корпоративной безопасности (например, отправка конфиденциального документа за пределы компании). *Базой*

технологий называется 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 на рабочем месте является 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

5.4.1 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** или **Выгрузки из БД**).

   > **Примечание.**
   >
   > Подраздел Графические объекты содержит только предустановленные элементы, для которых недоступны операции добавления, редактирования и удаления.

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 проч. 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
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	Изображение определенного типа, которое ищется в сетевом трафике. Графическими объектами могут быть изображения разворота паспорта или кредитной карты.	Все графические объекты в Системе являются предустановленными. Создание и редактирование графических объектов недоступно.

См. также:

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

Работа с категориями и терминами

Справочная информация:
Термины - набор данных, 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:

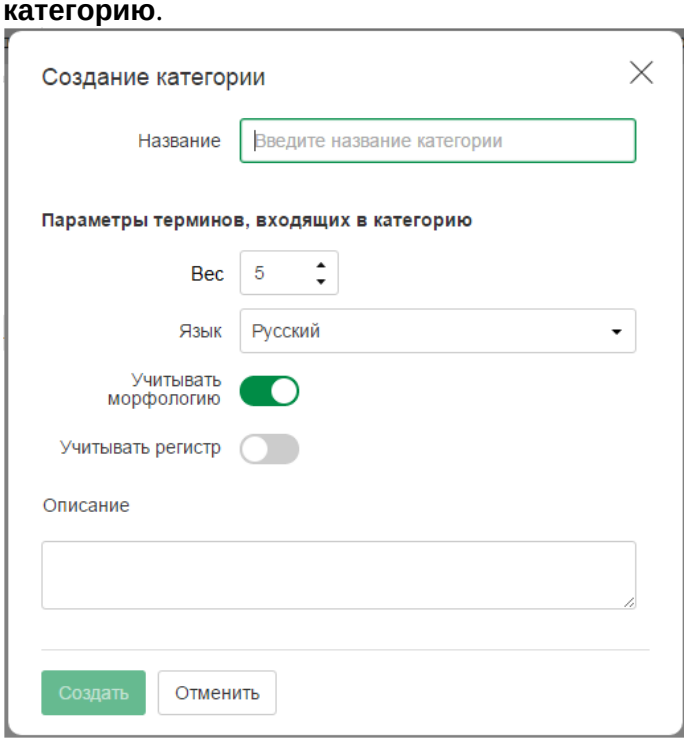
1. Создать категорию терминов.
2. Создать термин внутри категории.

Решение:

1. Создание категории.

a. Перейдите в раздел **Технологии**->**Категории и термины**.

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



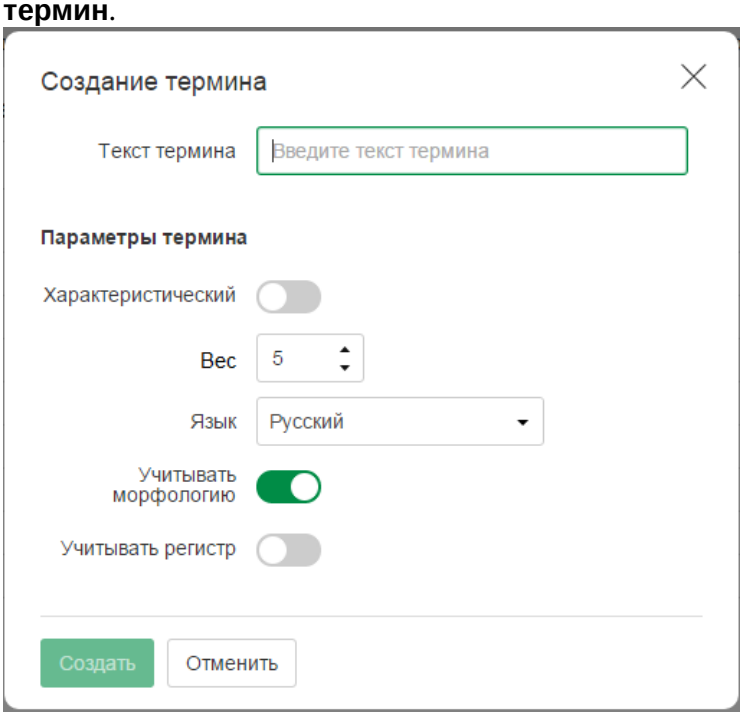
c. Укажите требуемые атрибуты для категории (см. "Категории").
d. Нажмите **Создать**.

2. Создание термина.

a. Перейдите в раздел **Технологии**->**Категории и термины**.
b. В левой части рабочей области щелчком левой кнопки мыши 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**.

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 целевую 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*.

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*.

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.

Дополнительные сведения:

Редактирование и удаление терминов выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

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. Создать каталог текстовых объектов

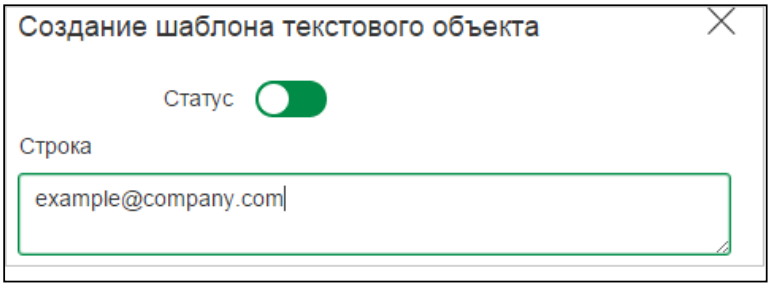
a. Перейдите в раздел **Технологии**->**Текстовые объекты**.
b. В левой части рабочей области на панели инструментов нажмите **Создать каталог текстовых объектов**.
c. В открывшемся окне введите название и описание каталога.
d. Нажмите **Сохранить**.

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**.

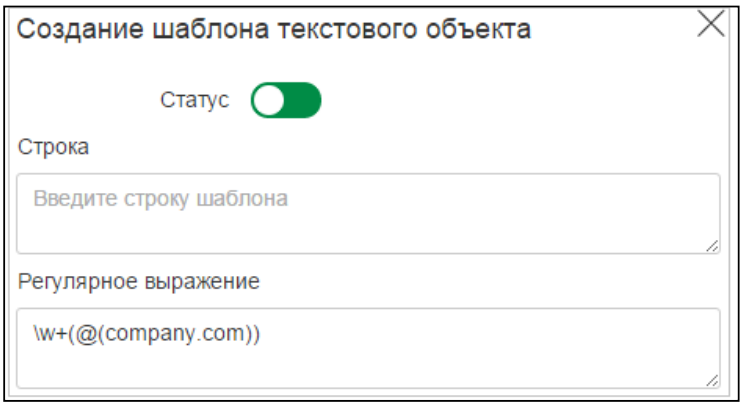
Пример 1:
Требуется, чтобы Система определяла наличие в трафике адреса электронной почты "example@company.com" и определяла его как текстовый объект EXAMPLE_MAIL. Для этого:

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:

В Системе используется стандартный язык регулярных выражений. Подробную информацию о регулярных выражениях Вы можете найти, например, в интернет-статье "Регулярные выражения, пособие для новичков".

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.

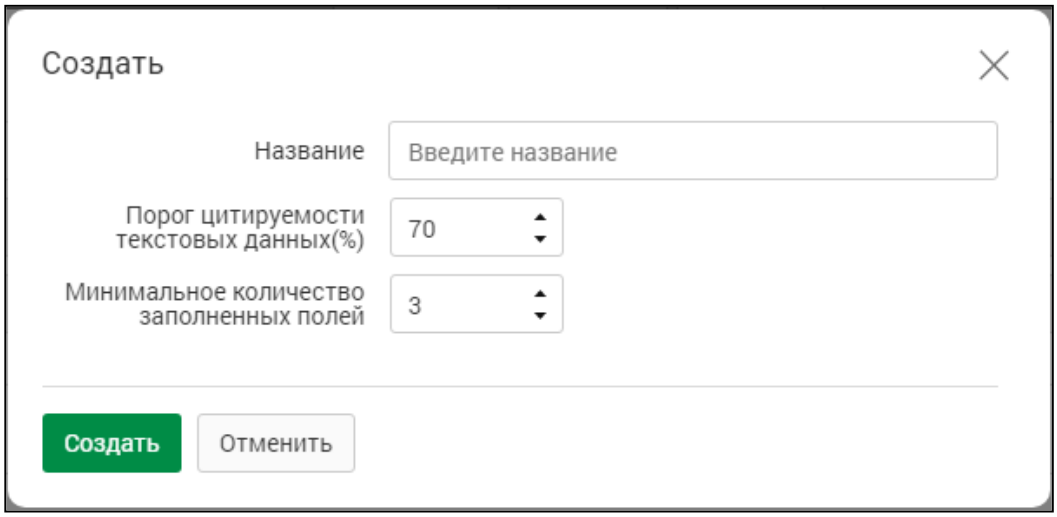
> **Примечание:**
>
> Если Системе не удалось загрузить файл бланка, в окне загрузки будет выведено сообщение об ошибке.

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.

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!**
>
> При использовании Postgre SQL размер выгрузки не должен превышать 1Гб.

e. После успешной загрузки файла:
   - нажмите **Настроить выгрузку из БД** - для настройки выгрузки;
   - закройте окно **Создание выгрузки из базы данных** - для выхода без дополнительных настроек.
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.

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.

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. **Условие обнаружения**.
6. Нажмите **Создать**.

Параметры условия обнаружения заполняются в соответствии со следующими рекомендациями:

Правило обнаружения.

Правило 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.

> **Примечание:**
>
> 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".

Список **Доступные столбцы в выборке** содержит столбцы, которые могут быть использованы для создания условия. Поле **Поиск** позволяет найти нужный столбец по его названию.

Логические отношения задаются с помощью символов:

1. "+" - конъюнкция ячеек (логическое "И");
2. "|" - дизъюнкция ячеек (логическое "ИЛИ");

> **Примечание.**
>
> Условие вида (1|3) должно указываться в скобках.

3. "()" - 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*.

4. "*" - 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 правила.

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).

Пример:
Требуется, чтобы Система помечала объект перехвата как НОМЕРА_ТЕЛЕФОНОВ при обнаружении в нем не менее 7 строк с заполненными столбцами 1 и 4 из таблицы со следующей структурой:

Фамилия	Имя	Отчество	Номер телефона
Иванов	Иван	Иванович	89441234347
Петров	Петр	Петрович	83531355424

Фамилия	Имя	Отчество	Номер телефона
Сидоров	Сидор	Сидорович	83544593406
Смирнов	Юрий	Борисович	83245446441
Кузнецов	Владимир	Андреевич	84534359243
Соколов	Михаил	Григорьевич	83544352925

Для этого:

1. Сохраните таблицу в формате CSV или TSV и загрузите созданный файл в Систему.
2. Настройте правила обработки столбцов таблицы:
   - в поле **Условие обнаружения** указывает **1+4**;
   - в поле **Минимальное количество строк** указывает **7**.
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

5.4.2 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 и импорт технологий не могут быть выполнены, если конфигурация Системы находится на редактировании. В этом 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** или **Выгрузки из БД**).
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** или **Выгрузки из БД**).
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** или **Выгрузки из БД**).

   > **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.

5.5 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. Таким образом вы можете настроить Систему на обнаружение 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
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

5.5.1 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.

5.5.2 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.

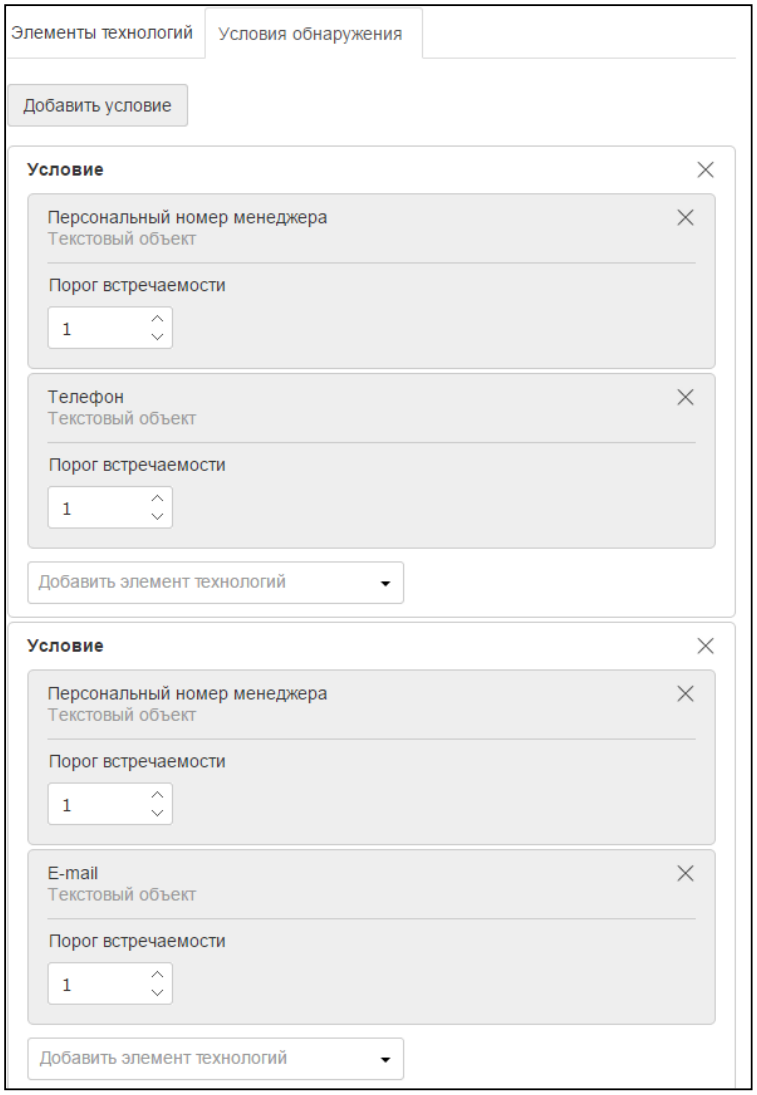
Пример:
Требуется создать объект защиты *"Персональные данные менеджера"*, который должен детектироваться в Системе при выполнении одного из следующих условий:

- 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:



Дополнительные сведения:
Редактирование и удаление объектов защиты выполняются стандартным способом:

- Редактирование элемента
- Удаление элемента

5.5.3 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.

5.5.4 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 одним из следующих способов:
   - 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.
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.

5.5.5 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 на агенте**.
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 на агенте**.
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.

5.5.6 Импорт и экспорт объектов защиты

Цель:

- экспортировать в файл структуру каталогов, содержащих объекты защиты и используемые в них элементы анализа;
- загружать из файла ранее созданную структуру каталогов, содержащих объекты защиты и используемые в них элементы анализа.

> **Примечание:**
>
> Экспорт и импорт объектов защиты не могут быть выполнены, если конфигурация Системы находится на редактировании. В этом 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 на кнопку 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 анализа. При экспорте сохраняется структура каталогов объектов защиты и элементов анализа.

Чтобы импортировать объекты защиты:

1. Перейдите в раздел **Объекты защиты**.
2. На панели инструментов в левой части рабочей области нажмите на кнопку 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:
   а) дочерние каталоги объектов защиты;
   б) объекты защиты.
2. Для объекта защиты будут добавлены следующие элементы, отсутствующие в Системе:
   а) элементы анализа;
   б) условия обнаружения.
3. Для условий обнаружения будут добавлены новые вложенные условия, включая параметры детектирования (для текстовых объектов, бланков и выгрузок из БД).

5.5.7 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.

5.6 Работа с подсистемой Краулер

Для чего требуется подсистема Краулер?

Подсистема Краулер позволяет проверять следующие места хранения файлов на наличие конфиденциальных данных:

- Разделяемые сетевые ресурсы
- Локальные диски рабочих станций
- Файловое хранилище SharePoint 2007/2010/2013

Работа с подсистемой Краулер включает следующие действия:

Действие	Описание
Настройка сканера	После того как администратор установит и настроит Систему, пользователь получит доступ к сканеру. Перед работой со сканером пользователь может выполнить его настройку
Создание задачи	Для сканирования ресурсов требуется создать задачу сканирования
Очистка хешей	Сброс сохраненных в Системе контрольных сумм

См. также:

- "Раздел Краулер" - о разделе, в котором ведется работа с подсистемой Краулер

5.6.1 Настройка сканера

Цель:
Настроить сканер подсистемы Краулер.

Решение:

1. Перейдите в раздел **Краулер**.
2. В левой части рабочей области нажмите кнопку **Редактировать сканер**.
3. В открывшемся окне измените требуемые атрибуты (см. "Сканер").
4. Нажмите **Сохранить** для сохранения сделанных изменений или **Отменить** для выхода из режима редактирования без сохранения изменений.

> **Примечание.**
>
> При редактировании сканера отображается сообщение о том, что данный сканер заблокирован. В это время задачи для сканера не выполняются.
>
> После выхода из режима редактирования отображается сообщение о том, что сканер разблокирован. Это означает, что задачи сканирования для данного сканера могут выполняться.

Дополнительная информация:
В значении атрибута **Не отображать следующие SID'ы** перечислены стандартные SID служебных записей. При необходимости, пользователь может добавить в этот список собственные SID и задать маски, используя регулярные выражения.

> **Важно!**
>
> Для корректного определения имен и SID пользователей Сканер Краулера должен находиться в одном домене со сканируемой рабочей станцией или хранилищем SharePoint.

Пример записи:
`S-1-5-21-.*-(498|502|517|527)`
Данная запись означает, что в Консоли управления не будет отображаться информация о том, что файл доступен учетным записям с любыми SID, начинающимися со строки "S-1-5-21-", имеющими в середине 0 или больше любых букв, цифр, и др. символов и оканчивающихся на "-498", или "-502", или "-517", или "-527".

Подходящие SID:
`S-1-5-21-12345-ABCDEF-498`
`S-1-5-21-527`

Неподходящие SID:
`1S-1-5-21-12345-ABCDEF-498` - начинается не с "S-1-5-21-"
`S-1-5-21-527` - начинается с "S-1-5-21-", но заканчивается на "527", а не на "-527"
`S-1-5-21-ABCDEF-100` - не заканчивается на "-498", или "-502", или "-517", или "-527".
`S-1-5-21-ABCDEF-502-` - не заканчивается на "-498", или "-502", или "-517", или "-527".
`S-1-6-21-ABCDEF-502` - начинается не с "S-1-5-21-".

> **Примечание:**
>
> Более подробно о формате языка регулярных выражений см. в интернет-статье "Элементы языка регулярных выражений".

5.6.2 Создание задачи

Цель:
Добавить задачу сканирования.

Решение:

1. Перейдите в раздел **Краулер**.
2. На панели инструментов нажмите  **Создать задачу**.
3. В открывшейся форме **Создание задачи** укажите требуемые параметры (см. "Задача сканирования").
4. Нажмите **Сохранить**.

Чтобы отредактировать ранее созданную задачу, выделите задачу в списке и нажмите  на панели инструментов.

Для удаления выбранной задачи нажмите .

Пример:
Требуется, чтобы Система присваивала тег *Печатная плата* объектам перехвата, созданным в результате обнаружения текстовых файлов формата TXT, которые содержат словосочетание "печатная плата" и хранятся в корпоративном файловом хранилище *SharePointRepo*, в БД *CorporateDataBase* (подразумевается, что файловое хранилище *SharePointRepo*, включающее БД *CorporateDataBase*, уже создано в организации). Для этого:

1. Создайте термин с текстом "печатная плата" (см. "Работа с категориями и терминами").
2. Создайте тег *Печатная плата* (см. "Работа с тегами").
3. Примените конфигурацию (см. "Применение конфигурации Системы").
4. Создайте задачу сканирования, выбрав в качестве цели сканирования *Файловое хранилище SharePoint* и указав атрибутам следующие значения:
   - атрибуту **Адрес БД ресурса** - значение *SharePointRepo*;
   - атрибуту **Название БД ресурса** - значение *CorporateDataBase*.
5. Создайте политику и добавьте правило хранения.
6. В правиле хранения укажите следующие значения атрибутов:
   - **Место хранения** - *Файловое хранилище*; атрибутам указываются следующие значения:
     - атрибуту **Введите источник** - значение *SharePointRepo*;
     - атрибуту **Введите путь хранения** - значение *CorporateDataBase*;
   - **Назначить событию теги** - тег *Печатная плата*.

Важно!

Во время выполнения задачи даже с использованием прав доменного администратора возможно появление ошибки доступа:

```
Ошибка получения каталогов для <адрес_каталога>: Access to the path
<адрес_каталога> is denied,
```

где `<адрес_каталога>` - абсолютный путь к каталогу проверки.
Такая ошибка может возникнуть, например, если владелец папки запретил к ней доступ.

5.6.3 Очистка хеша

Справочная информация:
Для оптимизации работы в подсистеме Краулер предусмотрено хранение **хешей** – контрольных сумм файлов. Если в ходе предыдущего запуска задачи сканирования был сохранен хеш какого-либо файла и при очередном запуске той же задачи хеш для этого файла не изменился, это означает, что данный файл не изменялся и его не нужно отправлять на обработку на сервер Traffic Monitor. Это позволяет уменьшить нагрузку на канал между подсистемой Краулер и сервером Traffic Monitor и на сам сервер Traffic Monitor, а также исключает дублирование идентичных событий при каждом запуске задачи.

Особенности хранения базы хешей:

- База хешей сохраняется отдельно для каждой задачи сканирования. То есть если какой-либо файл уже был обработан другой задачей, то при создании и запуске новой задачи файл будет обработан повторно.
- Хеш-суммы хранятся для файлов с учетом рабочих станций, на которых эти файлы были обнаружены. Таким образом, если один и тот же файл находится на нескольких рабочих станциях, он будет обрабатываться отдельно для каждой рабочей станции.

Рекомендуется выполнять периодическую очистку базы хешей: например, при изменении конфигурации Traffic Monitor. Так как изменение конфигурации включает изменение политики, списка терминов и т.п., то после изменения конфигурации решение о том, является ли перехваченный объект потенциальным нарушением, может приниматься Системой по другому алгоритму. В результате очистки базы хешей из задачи удалится информация о ранее обработанных файлах, и Краулер будет отправлять для анализа на сервер Traffic Monitor все файлы, соответствующие условиям задачи

Цель:
Очистить хеш.

Решение:

1. Перейдите в раздел **Краулер**.
2. Выделите нужную задачу в списке.
3. На панели инструментов нажмите  **Очистить хеши задачи**.

5.7 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
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
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

5.7.1 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").

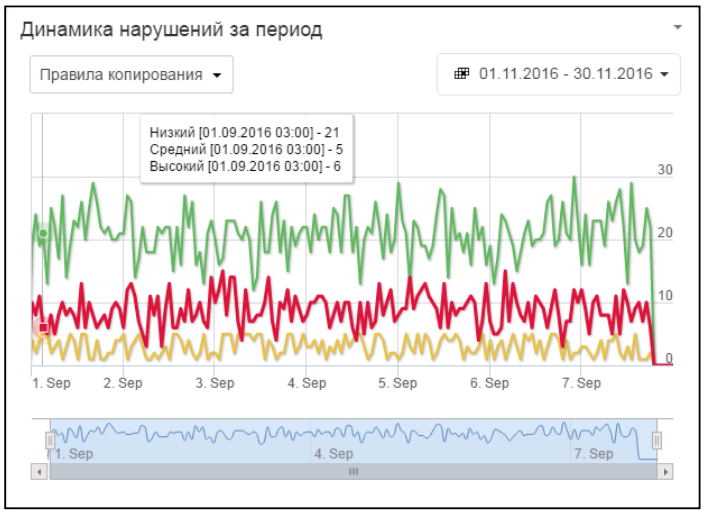
Все сформированные выгрузки сохраняются в Системе. Вы можете просмотреть требуемую выгрузку или удалить выгрузки, хранение которых не требуется (см. "Просмотр выгрузки сводки").

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:

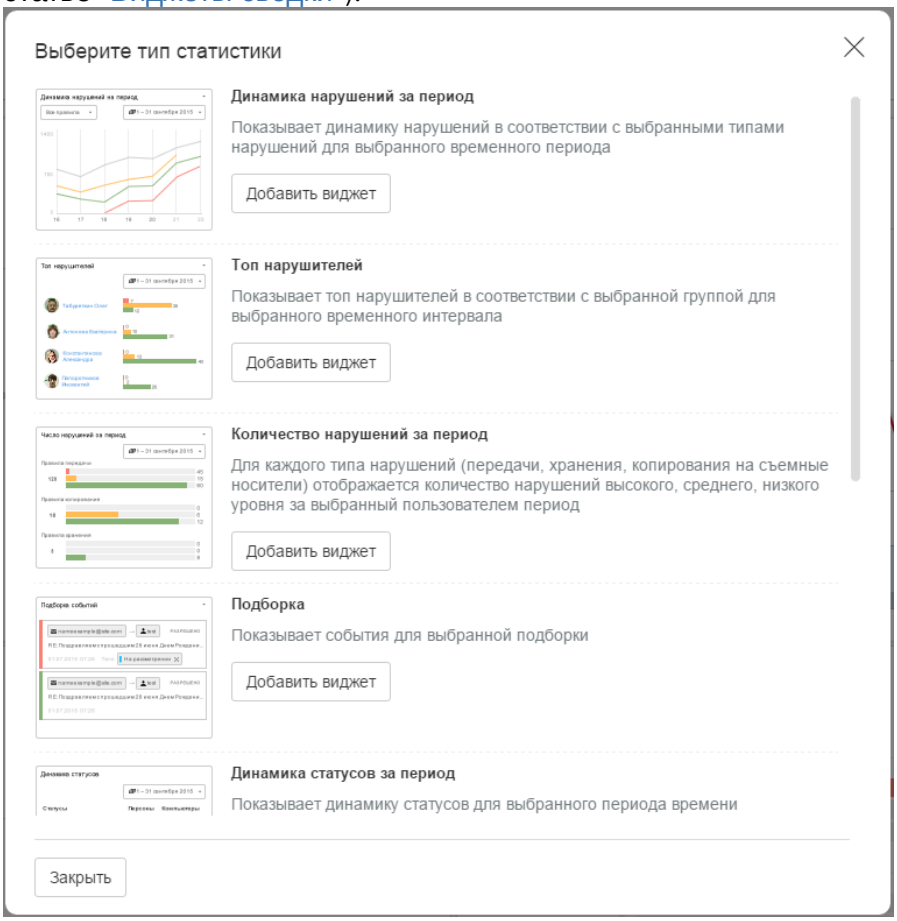
- Наполнение панели описано в статье "Создание и настройка виджета".
- Для удаления панели перейдите на панель, которую требуется удалить и нажмите на вкладке с названием панели. В окне подтверждения нажмите **Удалить**.

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 открывшемя 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**.

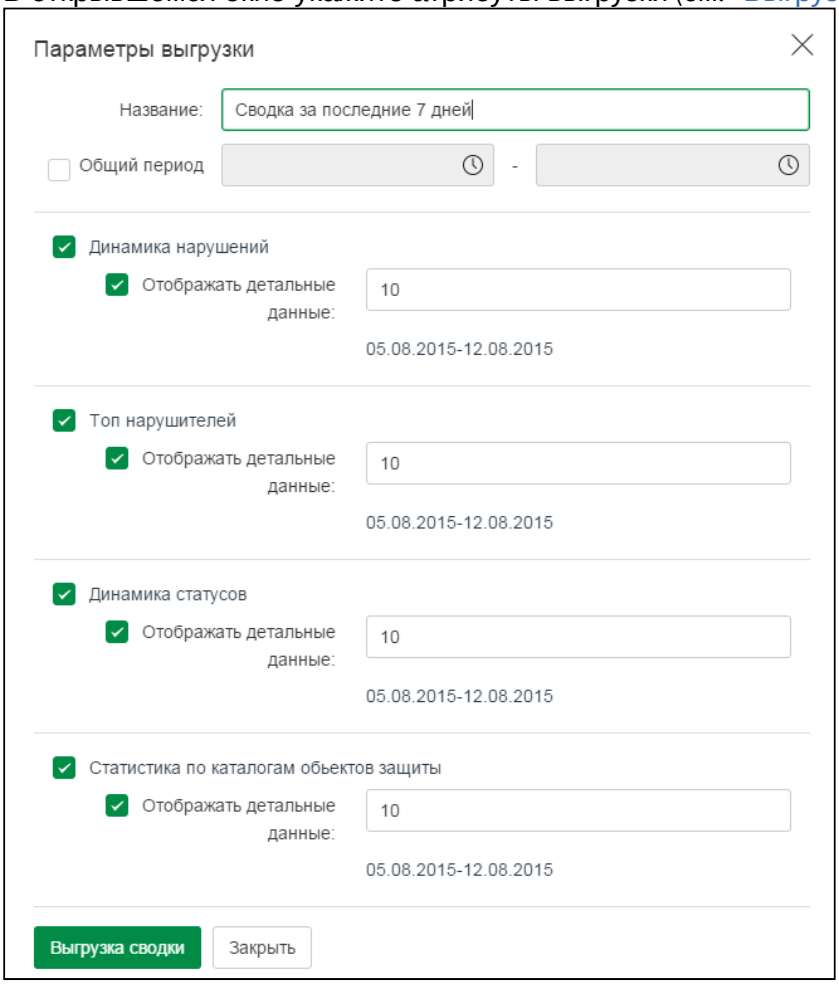
Создание выгрузки сводки

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).

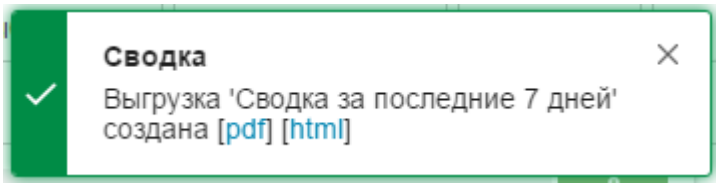
Примечание:

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.

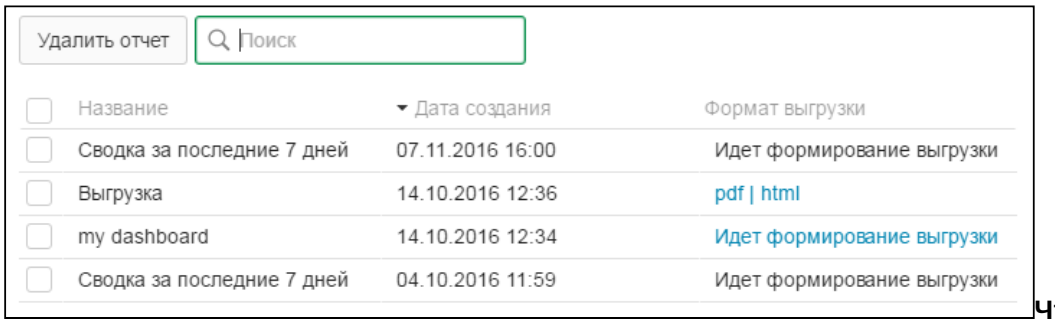


Нажмите на ссылку **pdf** или **html**, чтобы открыть выгрузку в новом окне браузера. Также вы можете сохранить, отправить или распечатать созданную выгрузку стандартными средствами вашего браузера и операционной системы. Все сгенерированные выгрузки сохраняются в Системе.

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:

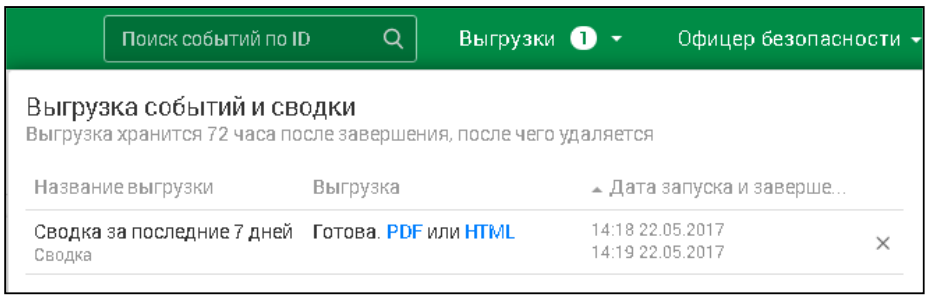
- **pdf** - если требуется отобразить выгрузку сводки в формате PDF;
- **html** - если требуется отобразить выгрузку сводки в формате HTML.

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.

5.7.2 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. 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 запрос:

1. Выделите запрос 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 запрос. Если у пользователя отсутствует полный доступ к папке, или выполняется копировании запроса 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 запросы, пользователю также требуется полный доступ к запросам, содержащимся в папке. Подробнее см. таблицу ниже.

Чтобы переместить запрос, выделите в списке нужный запрос и, удерживая левую клавишу мыши зажатой, переместите его в требуемое место, после чего отпустите зажатую клавишу мыши.

> **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 и выполнение 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 редактировании 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 (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.
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.

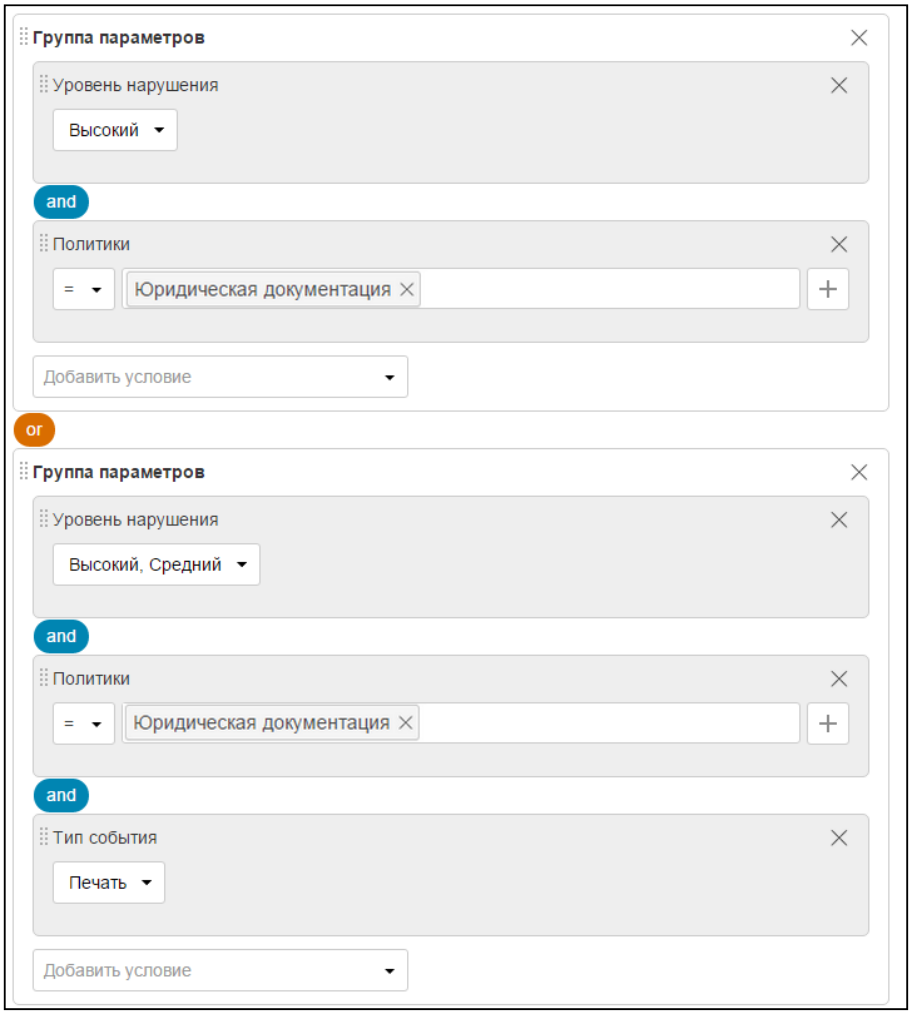
Пример 3:

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:

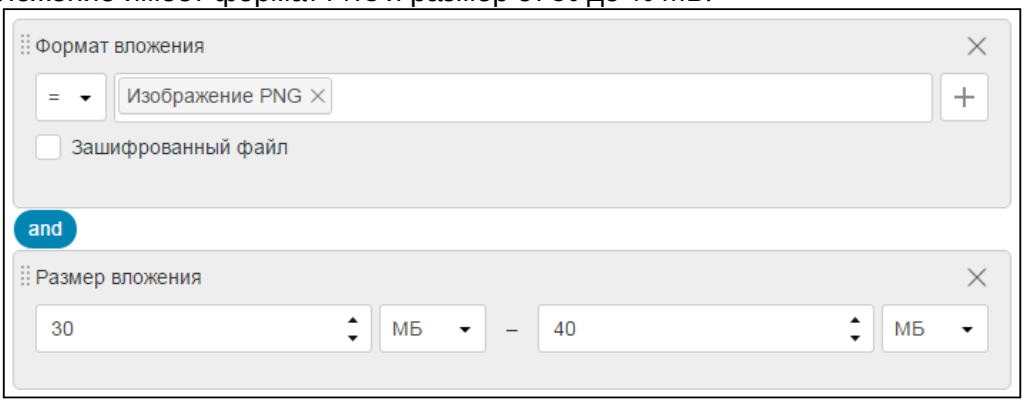
1. Создайте запрос в расширенном режиме и укажите его название.
2. Добавьте два элемента *Группа параметров*, связанных операцией дизъюнкции.
3. Внутри первой группы добавьте следующие атрибуты, связанные операцией конъюнкции:
    - **Уровень нарушения** - *Высокий*;
    - **Политика** - *Юридическая 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:

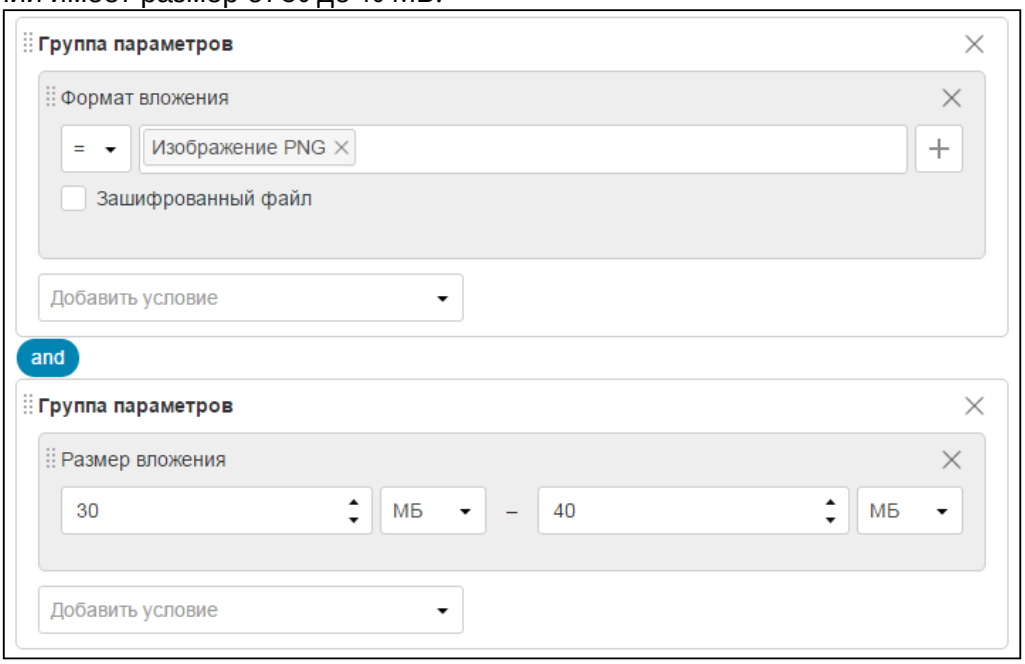
Если условия заданы для вложений объекта, то при наличии у объекта нескольких вложений условия будут применяться следующим образом:

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:

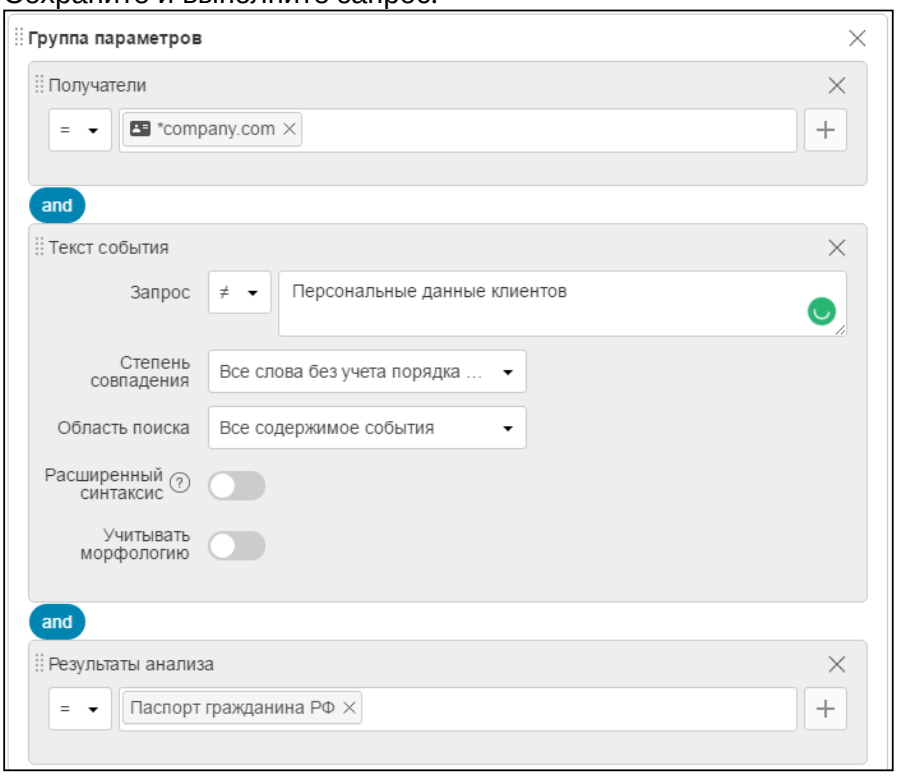
Требуется найти события:

- пересылаемые внутри компании;
- не содержащие слова *Персональные данные клиентов* в тексте события;
- 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:
   - `Получатели` - **company.com*;
   - `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;
   - `Область поиска` - *"Все содержимое события"*;
   - `Результаты анализа` - текстовый объект *"Паспорт гражданина РФ"*.

4. Сохраните и выполните запрос.



Пример 6:

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:

- не сработал ни один объект защиты;
- 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:

- не сработал ни один объект защиты;
- 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 плитке события (или в строке таблицы - в зависимости от выбранного стиля) отображаются все атрибуты события.

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 **Поля просмотра**.
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. Выделите плитку целевого 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, выделите с помощью мыши требуемое значение. Отобразится карточка выбранной персоны или выбранного компьютера.
   При просмотре карточки вы можете:
   a. Назначить статус персоне/компьютеру. Для этого нажмите ссылку Назначить статус, в открывшемся окне **Добавление статуса** выберите требуемые статусы и нажмите **Сохранить**.
   b. Просмотреть подробную информацию о персоне/компьютере в разделе "Персоны". Для этого нажмите ссылку Профиль персоны (для персоны) или Перейти к компьютеру (для компьютера).
   c. Просмотреть снимки экрана для персоны/компьютера (при наличии снимков экрана рядом с именем персоны отображается значок). Для этого нажмите ссылку 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 вблизи события. При нажатии на эту ссылку откроется вкладка **Снимки экрана**, где будет показан снимок экрана, время создание которого максимально близко к событию.

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 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 просморе 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

5.7.3 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 заблокированного события".

- **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.

См. также:

- "Ретроспективный анализ данных, решение пользователя по объекту" - о вынесении пользовательского решения.

5.7.4 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

5.7.5 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.

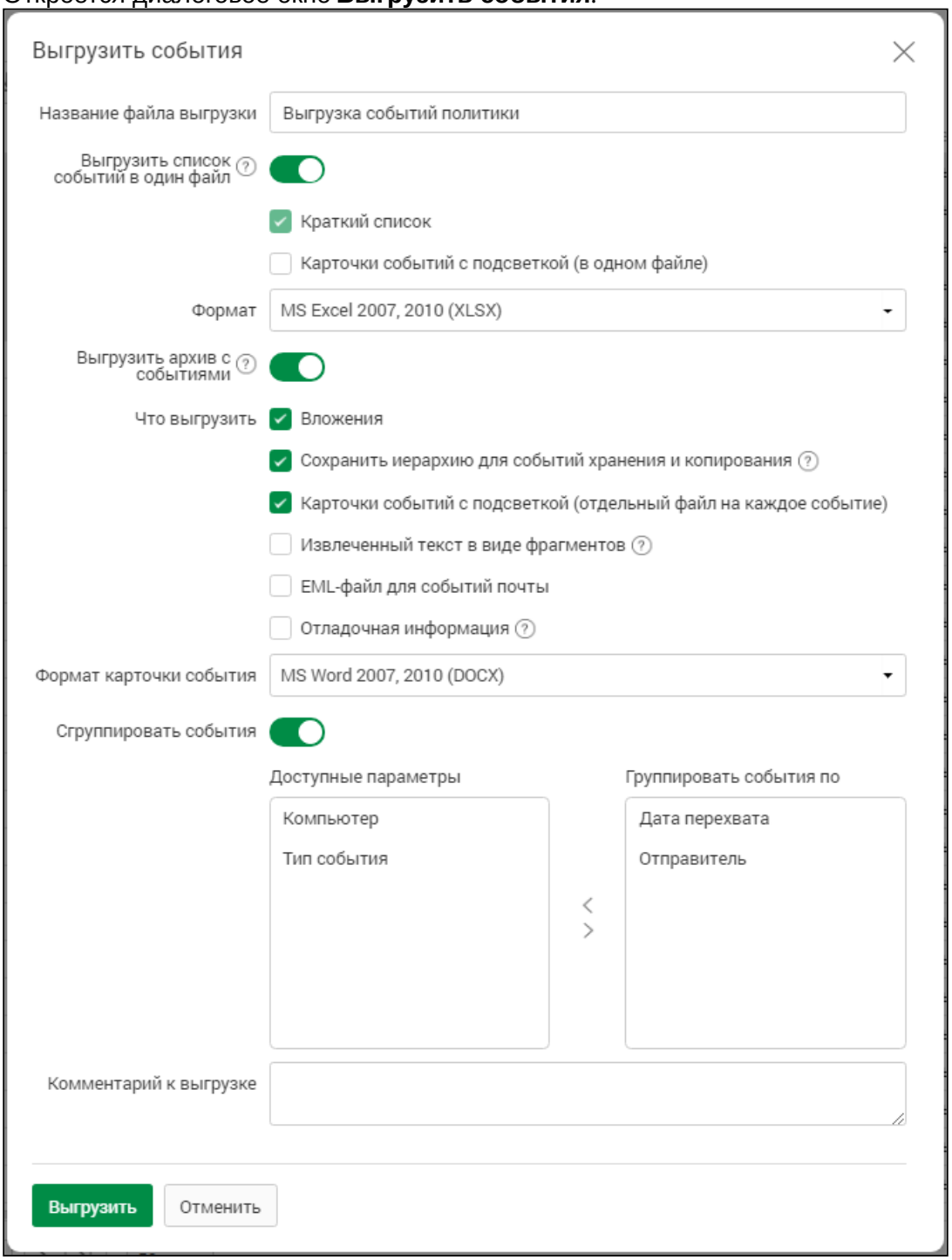
5.7.6 Выгрузка событий

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).

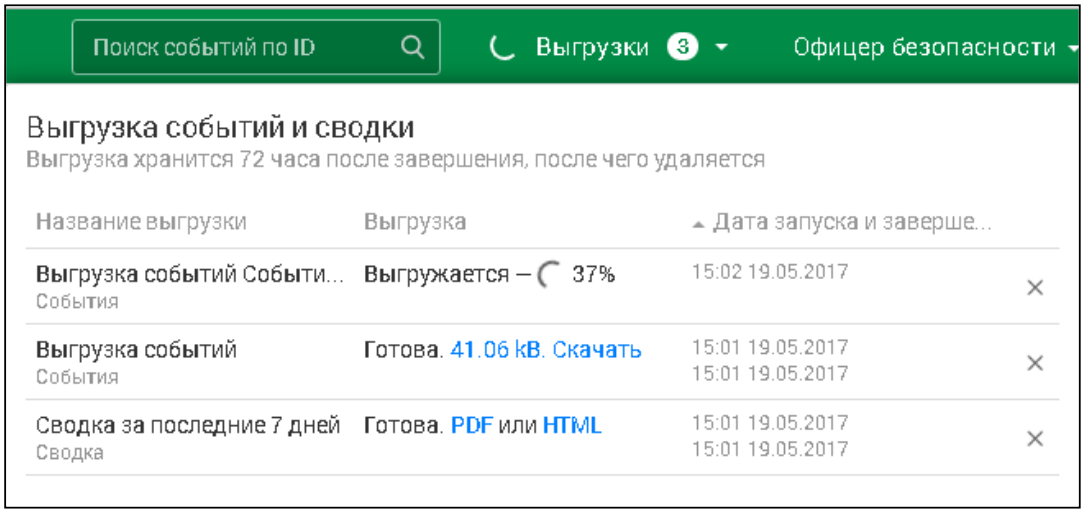
7. Если выбрана настройка **Выгрузить архив с событиями** или если выгрузка содержит только одно событие, укажите следующие настройки:
   - **Вложения** - будут выгружены исходные файлы вложений.
     Настройка по умолчанию отключена для экономии оперативной памяти системы;
   - **Сохранить иерархию для событий хранения и копирования** - отображается, если выбрана настройка **Вложения**. События, относящиеся к одному типу, будут сохраняться в папку "Внешнее устройство", "FTP" или "Краулер" 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.

5.7.7 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.

5.8 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 непосредственно на агентах Device Monitor. 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

5.8.1 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 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 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
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
Если не заполнен атрибут: ▪ Отправитель (для правил передачи и копирования) ▪ Получатель (для правил передачи) ▪ Персона (для правил буфера обмена) ▪ 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, буфера обмена) ▪ Время (для правил передачи, копирования, буфера обмена) ▪ Компьютер (для правил передачи, копирования, буфера обмена) ▪ Место хранения (для правил хранения) ▪ Терминальная сессия (для правил буфера обмена) ▪ Приложение-источник / Приложение-приемник (для правил буфера обмена) ▪ Ресурс (для правил копирования)	0	не применимо

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
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

5.8.2 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
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 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, контроллирующие посещение веб-ресурсов

По умолчанию в Системе установлены следующие политики защиты данных, контроллирующие посещение веб-ресурсов сотрудниками компании:

- Нецелевое использование ресурсов
- Нелояльные сотрудники
- Скрытые действия сотрудников
- Подозрительная активность

Нецелевое использование ресурсов

По умолчанию в Системе установлена политика, контроллирующая посещение развлекательных ресурсов сотрудниками компании.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Нецелевое использование ресурсов
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 группы "Медиа", "Блоги", "Развлечения", "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
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	Активная
Период действия	Не ограничен
Защищаемые данные	Любые данные

Правила политики

Правило передачи, контроллирующее 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, контроллирующая подозрительную активность сотрудников в интернете.

Предустановленная политика имеет следующие значения атрибутов:

Атрибут	Значение
Тип политики	Политика защиты данных
Название политики	Подозрительная активность
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Любые данные

Правила политики

Правило передачи, контроллирующее 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

Атрибут	Значение
Тип политики	Политика защиты данных
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.

5.8.3 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 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.

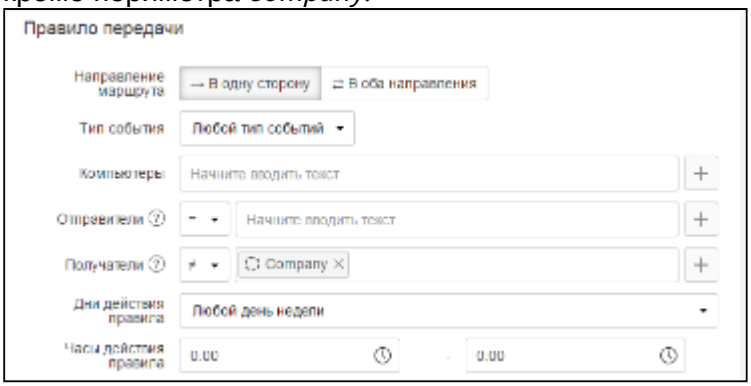
См. также: "Примеры использования политики защиты данных".

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.

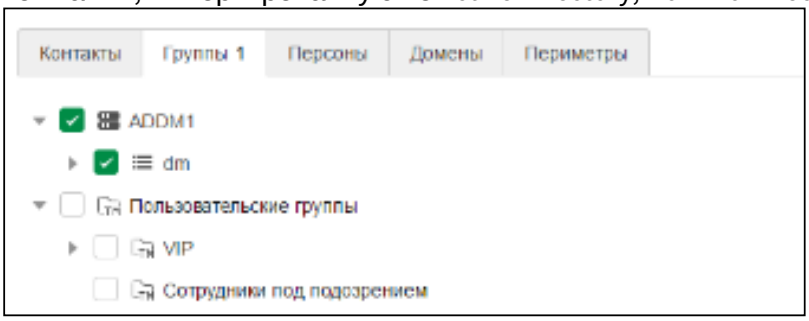
Пример 2:

Требуется выявить сотрудников, посещающих сайты по поиску работы. Для этого:

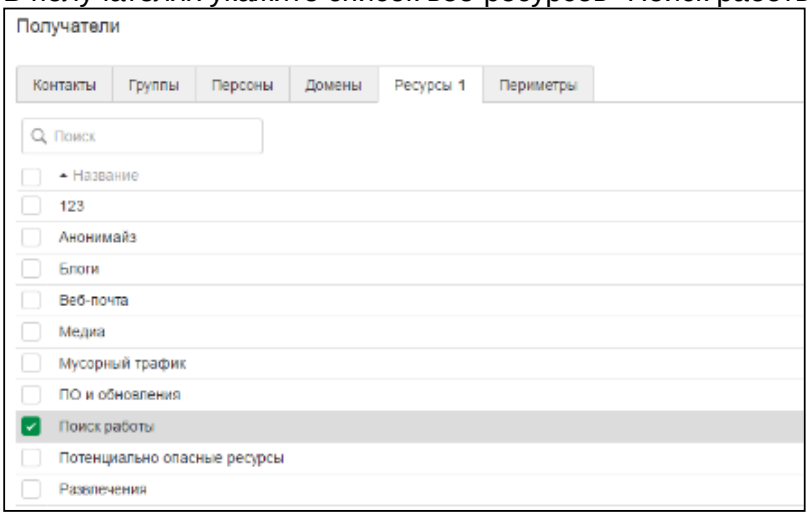
1. Создайте политику защиты данных "Выявление нелояльных сотрудников".

> **Совет.**
>
> Добавьте описание политики, чтобы легче идентифицировать ее в списке политик. Например, "Выявление сотрудников, отправляющих запросы на сайты по поиску работы".

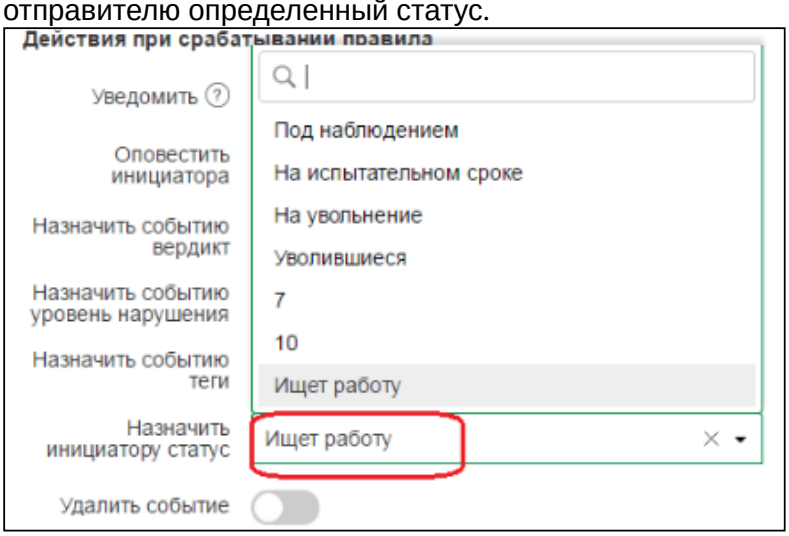
2. Добавьте правило передачи и укажите в качестве отправителей группу сотрудников компании, импортированную из Active Directory, Domino Directory или Astra Linux Directory.



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.

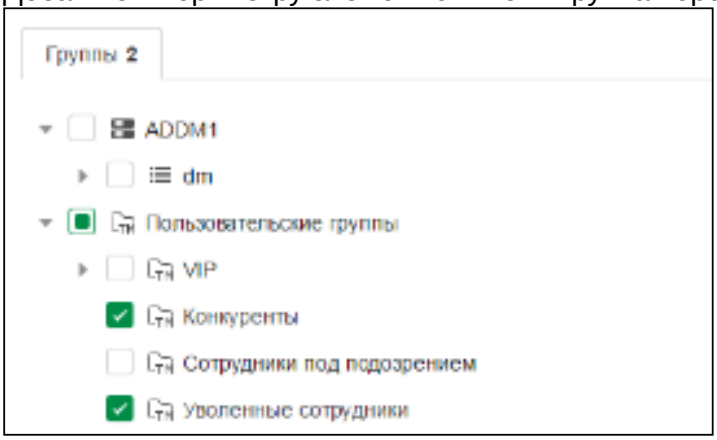
Выполните следующие шаги:

1. Создайте группу "Уволенные сотрудники" и наполните ее одним из следующих способов:
   - создайте карточки уволенных сотрудников вручную;
   - импортируйте персон из Active Directory, Domino Directory или Astra Linux Directory (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".

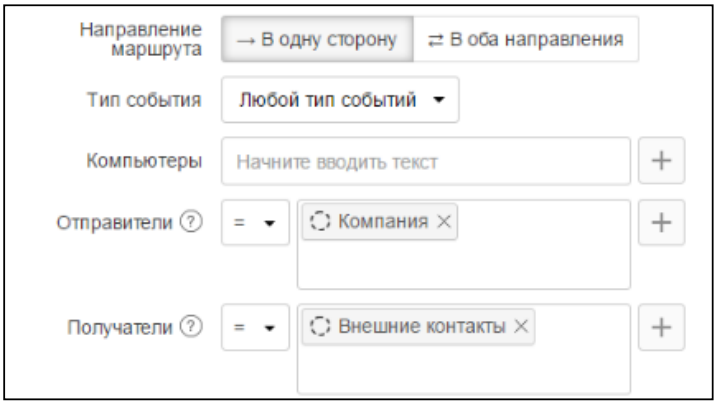
   Примечание.

   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".

5.8.4 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 ОС Astra Linux, 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.
   - **Каталоги объектов защиты**
     В выбранных каталогах будут использоваться только объекты защиты, созданные на основе категорий и текстовых объектов.
   - **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:

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 **Ресурс** 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*.

Подробнее об особенностях создания политики см. "Особенности задания правил в политиках защиты данных на агентах".

5.8.5 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.

5.8.6 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** и **Буфер обмена** - для политики защиты данных;
   - **Передача**, **Копирование** - 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 намжите **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*.

5.8.7 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. **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

5.8.8 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.

5.8.9 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.

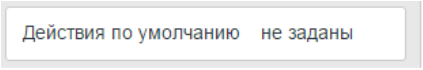
Цель:

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.*

5.8.10 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**.

5.8.11 О политике защиты данных на агенте

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 такие действия пользователя, как передача (Интернет-активность, Почта на Клиенте, Почта в Браузере) и копирование данных (FTP, облачные хранилища, внешние носители).

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 политики 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 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 и правило копирования.
Подробнее о правилах и их создании в статьях Правила и форма их просмотра, Правило передачи, Правило копирования.

5.8.12 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;
- Краулер (для сканирования хранимой информации);
- Буфер обмена.

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.

5.8.13 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.

5.9 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

5.9.1 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

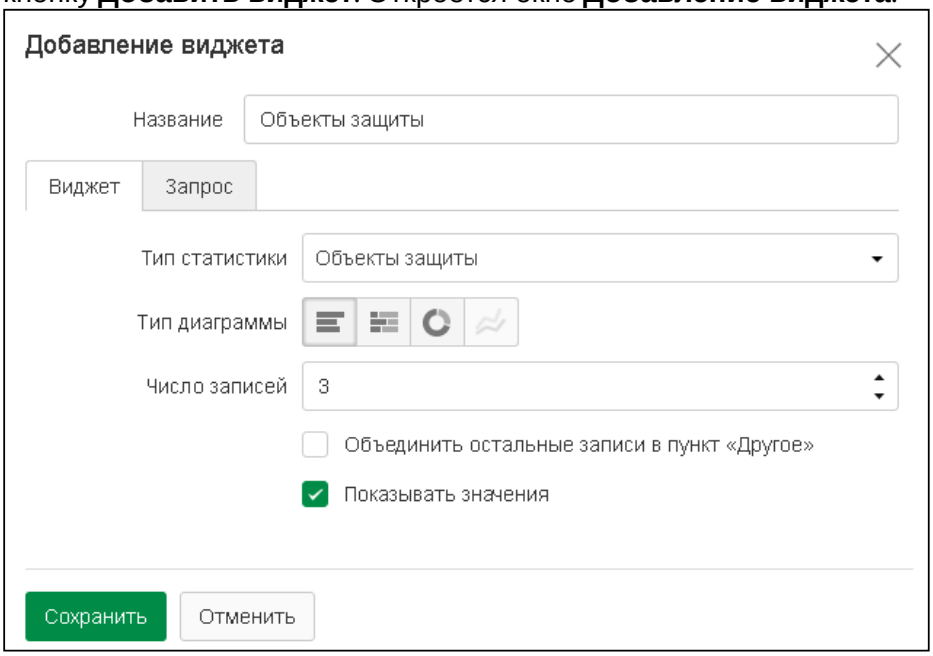
Цель:
Добавить в отчет виджет, на котором будет отображаться статистическая информация.

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.

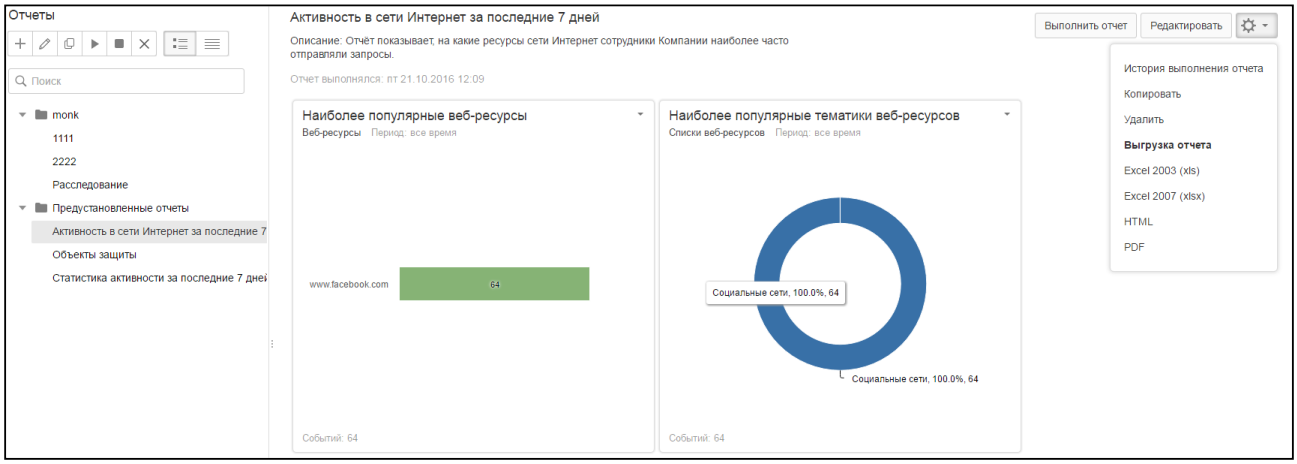
Дополнительные сведения:

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.



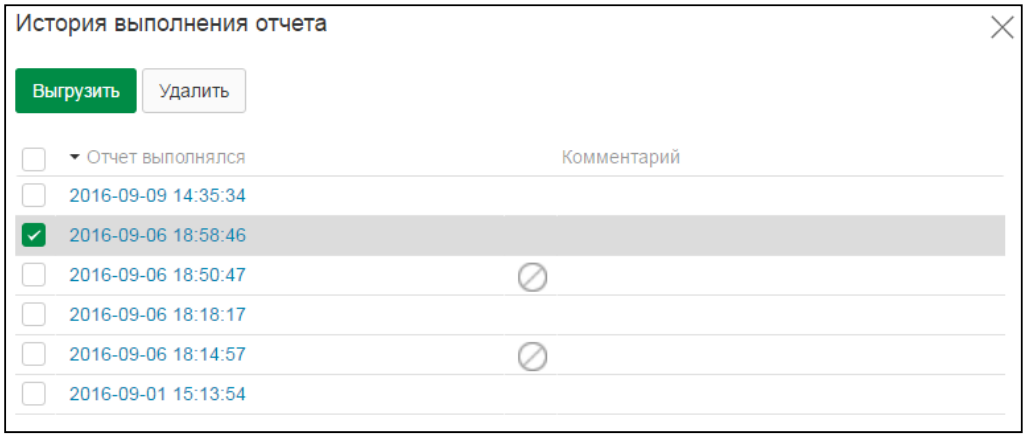
Если вы хотите посмотреть события, информация о которых отображается на виджете, в правом верхнем углу виджета нажмите ▾ и в раскрывающемся списке выберите **Перейти в события**. Будет выполнен переход к списку событий виджета в разделе "События".

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:

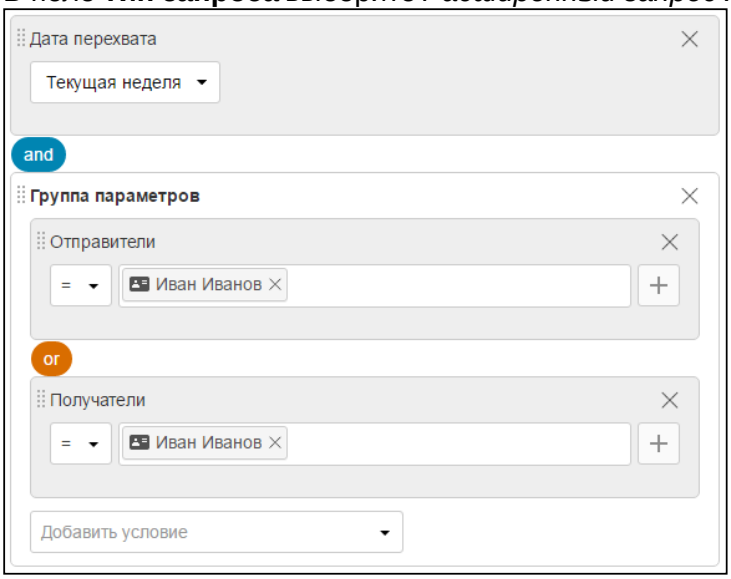
1. Установите флажки напротив версий, которые вы хотите сохранить в виде файла. Чтобы выбрать все строки сразу, установите флажок в поле заголовка.
2. Нажмите **Выгрузить** и в раскрывающемся списке выберите формат сохранения: Excel 2007, Excel 2003, HTML или PDF. Файл в выбранном формате будет сохранен на ваш компьютер.

5.9.2 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.

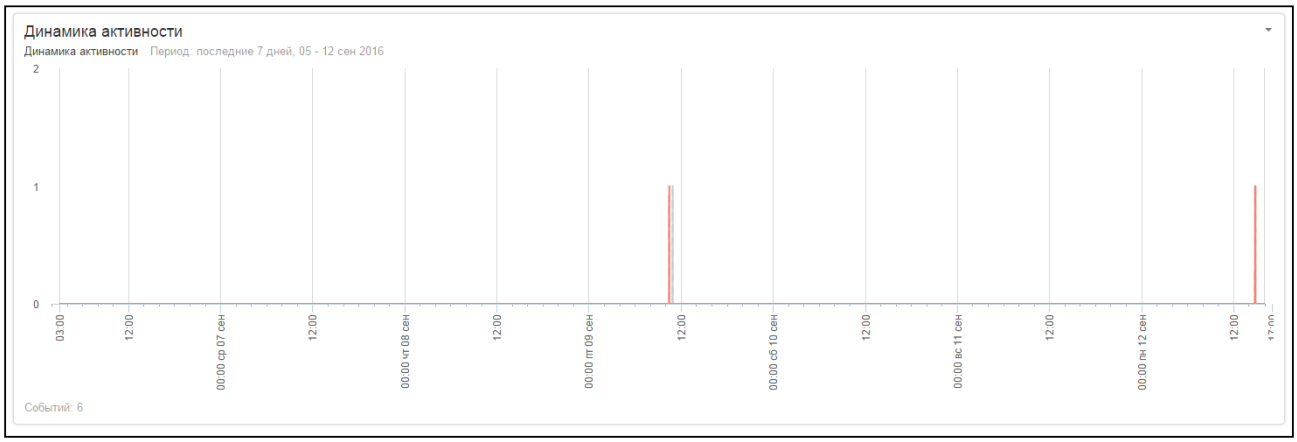
Этап 1. Получить информацию о динамике нарушений. Для этого:

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:



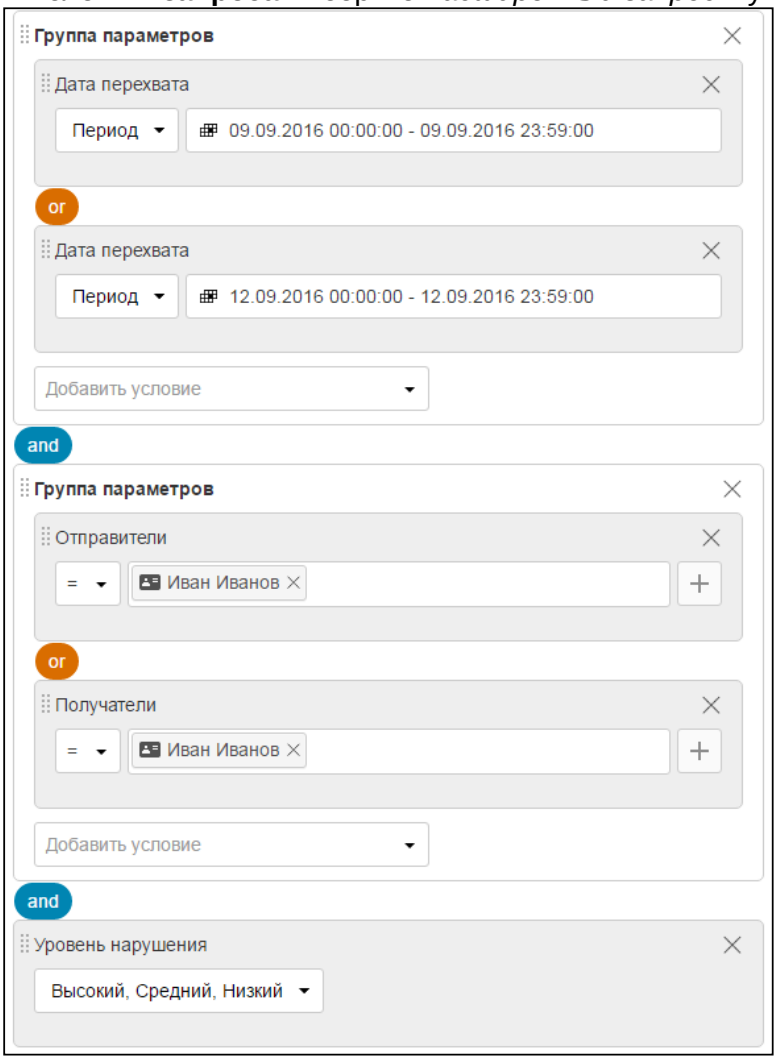
4. Сохраните и выполните отчет.

По полученному графику вы можете определить, что наибольшее количество нарушений сотрудник совершил 09.09 и 12.09.



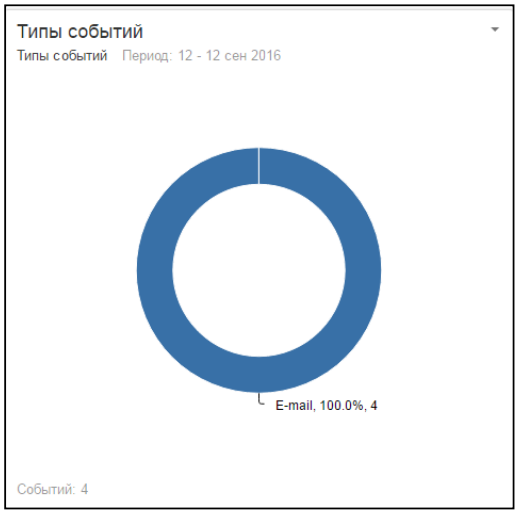
Этап 2. Определить, по каким каналам произошла утечка информации. Для этого:

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:



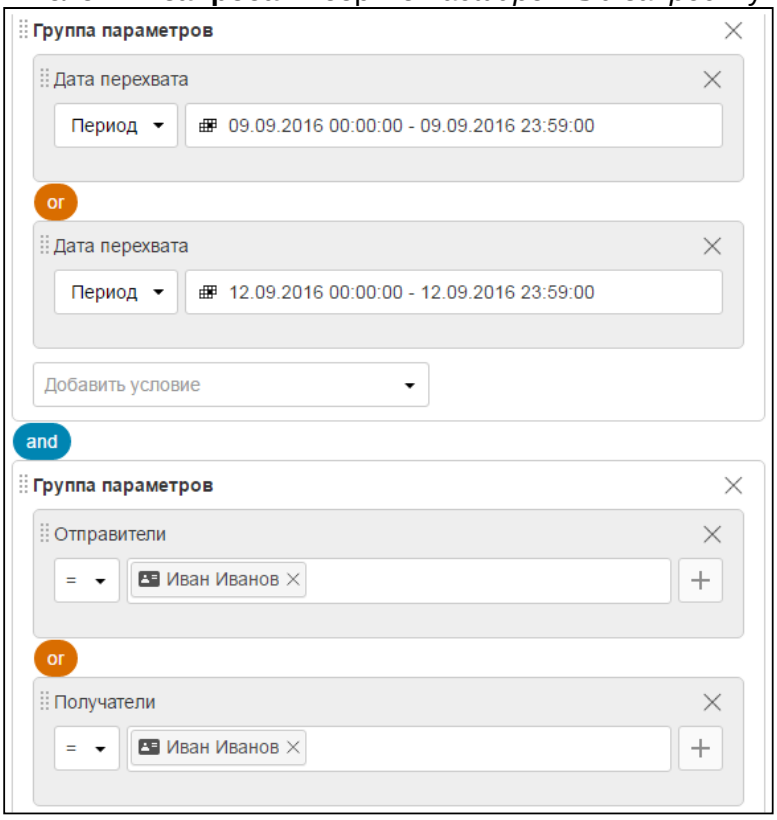
4. Сохраните и выполните отчет.

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:



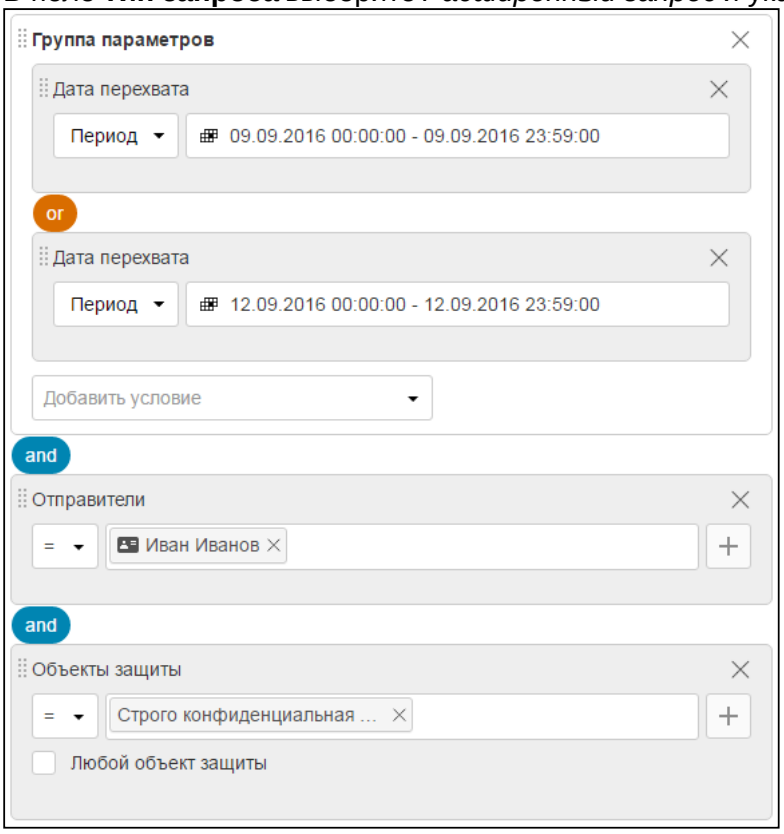
4. Сохраните и выполните отчет.

Из отчета вы можете определить, что сотрудник отправлял по почте документы, входящие в объект защиты "Строго конфиденциальная информация".



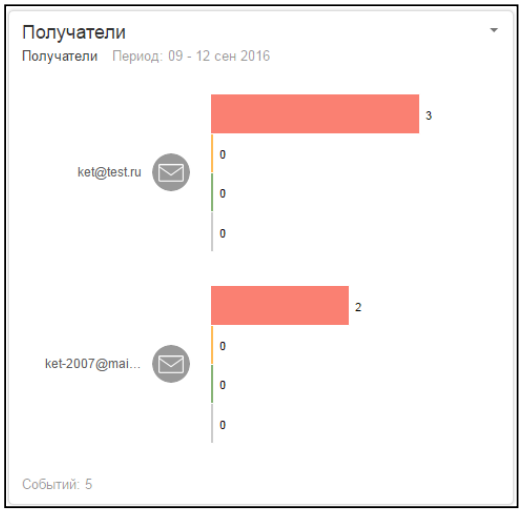
Этап 4. Определить, кому сотрудник Иван Иванов отправлял конфиденциальные данные. Для этого:

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.

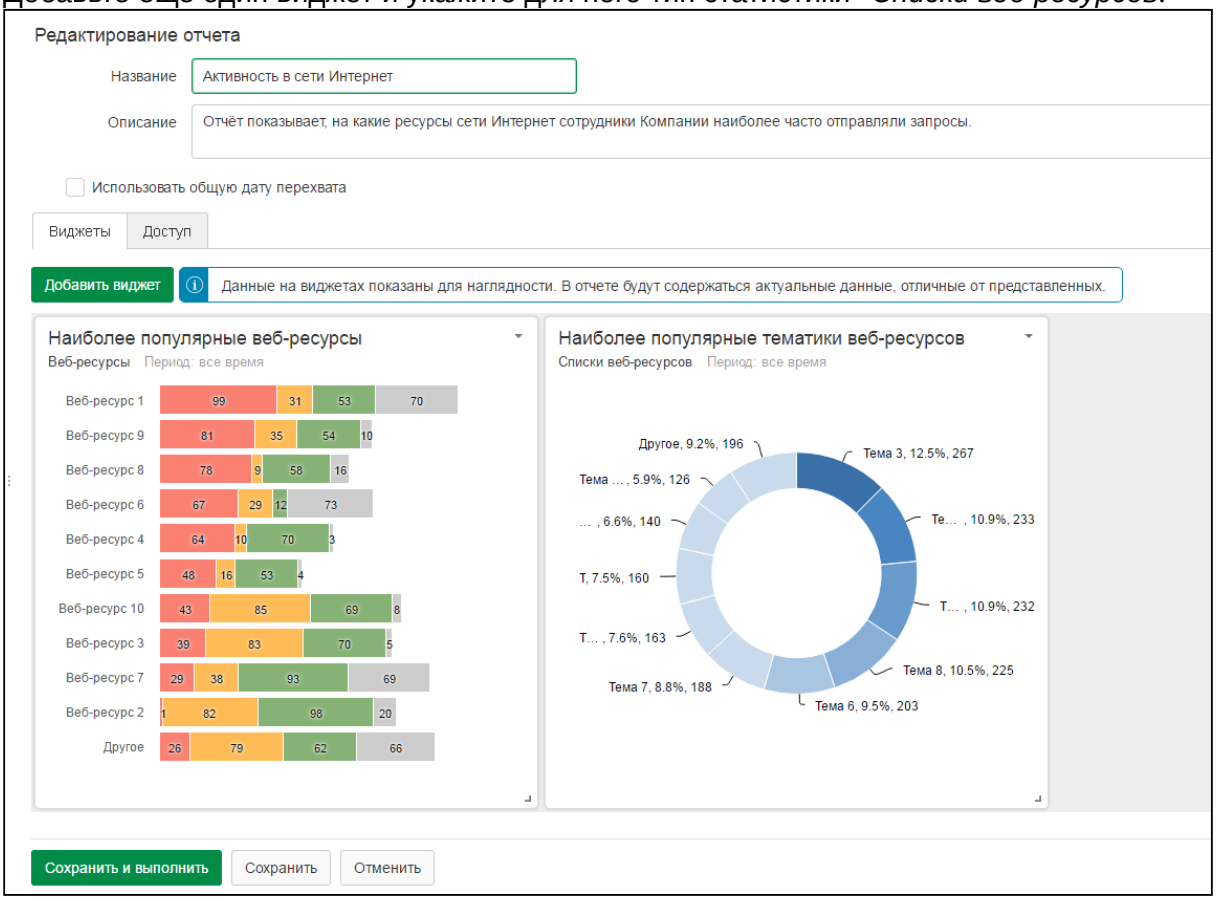
Из отчета вы можете определить, на какие email-адреса была отправлена конфиденциальная информация.



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.

5.10 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 пользователями Системы и их ролями
- Управление лицензиями
- Просмотр состояния Системы
- Управление службами
- Сбор диагностических данных
- Аудит действий пользователя
- Контроль целостности
- Добавление плагинов
- Настройка подключения к почтовому серверу
- Настройка уведомлений

5.10.1 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 сервера** 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:

Параметр	Описание
Название сервера	Идентификатор соединения, который используется в консоли управления
Тип сервера	Признак того, какой сервер используется – *Active Directory*, *Domino Directory* или *Astra Linux Directory*
Синхронизация	Признак того, что синхронизация выполняется по указанному расписанию

Период синхронизации	Тип периодичности выполнения синхронизации
Повторение	Время повторения синхронизации ***Например*** , при заданных значениях • *Период синхронизации* – ежеминутно; • *Повторение* – 60 минут, синхронизация будет выполняться каждые 60 минут.
LDAP-сервер	Сетевой идентификатор сервера, с LDAP каталогами которого производится синхронизация
Глобальный LDAP-порт	Порт для подключения глобального LDAP каталога. **Примечание:** данная настройка доступна только для Active Directory
LDAP-порт	Порт для подключения доменного каталога
Использовать глобальный каталог	Признак того, что для синхронизации используется глобальный LDAP каталог **Примечание:** данная настройка доступна только для Active Directory. **Важно!** При синхронизации с каталогом Windows 2008 R2 или Windows 2012, укажите значение параметра Не использовать.
LDAP-запрос	Домен (LDAP base), в котором ведется поиск данных AD. **Примечание:** данная настройка не обязательна для Domino Directory Для оптимизации поиска по AD Вы можете использовать отдельные уровни иерархии базы. ***Например*** , чтобы использовать в качестве базы поиска ветку Users, расположенную в домене компании, необходимо присвоить параметру **Атрибуты фильтрации** следующее значение: cn=users,dc=company,dc=com
Анонимный доступ	Признак того, что подключение к LDAP-серверу осуществляется от имени анонимного пользователя
Использовать протокол Kerberos	Признак того, что для аутентификации используется протокол Kerberos (протокол взаимной аутентификации клиента и сервера) **Примечание:** При синхронизации с ALD (Astra Linux Directory) рекомендуется активировать данный параметр.
Логин	Логин для доступа к серверу синхронизации
Пароль	Пароль для доступа к серверу синхронизации

Последняя синхронизация	Дата и время завершения последней синхронизации
Статус последней синхронизации	Результат последней синхронизации
Следующая синхронизация	Дата и время следующей синхронизации

Важно!

Чтобы в результате синхронизации с ALD были добавлены AUTH-контакты персон, необходимо в конфигурационном файле **adlibitum.conf** в параметре `DnsRootDefault` прописать значение домена ALD. После этого нужно перезапустить службу: `iwtm restart adlibitum`.

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.

Важно!

Для работы LDAPS (с шифрованием по SSL) через порт 389 требуется внести изменения в конфигурационном файле **/etc/openldap/ldap.conf.** Для этого добавьте в него следующую запись и сохраните изменения: `TLS_REQCERT never`. Без данной записи попытка синхронизации с AD будет отклонена.

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 (см. "Управление интеграцией с LDAP каталогами").
4. Нажмите **Проверить соединение**, чтобы выполнить контрольную проверку подключения к серверу.
5. Нажмите **Сохранить**.

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. "Управление интеграцией с LDAP каталогами").
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.

5.10.2 Управление пользователями Системы и их ролями

Для работы пользователя в Системе используются следующие сущности:

- *Пользователь* – учетная запись (см. "Пользователи");
- *Роль* – набор прав, которые могут быть присвоены 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

Параметр	Описание
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

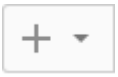
Чтобы изменить учетную запись:

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**.

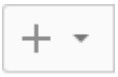
> **Примечание:**
>
> Вы можете изменить статус любой учетной записи, кроме **Administrator**.

Импорт учетной записи пользователя

Для удобства создания пользователей Вы можете импортировать учетные записи из Active Directory или Domino Directory.

> **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. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите .
5. Выберите из списка **Задать область видимости** (см. "Области видимости").
6. 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:

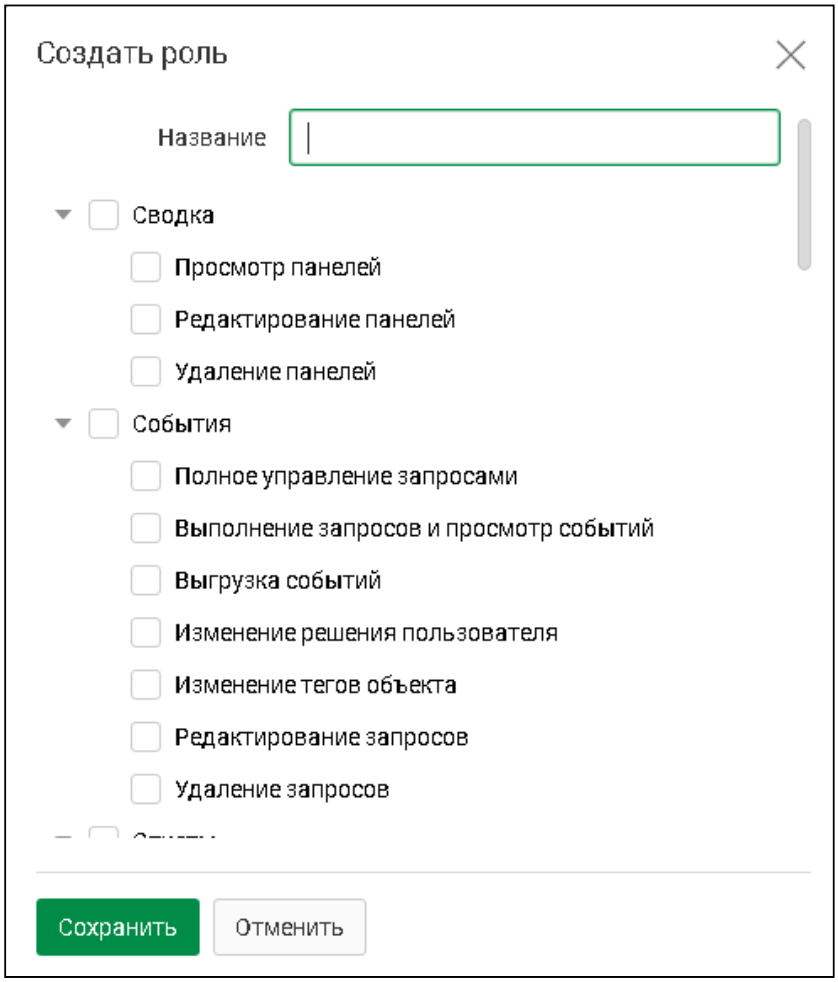
- Создание роли
- Редактирование роли
- Удаление роли

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 действий, которые требуется разрешить 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 действия, которые разрешены 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.

Например,

Пользователю officer 1 присвоена область видимости с Персоной: Иванов и Тегом: 1. Пользователь officer 1 сможет просматривать только события с участием персоны Иванов и помеченные тегом 1.

Примечание:

Для одного пользователя может быть задано несколько областей видимости.

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.

Раскрывающееся меню определяет количество областей видимости, отображаемых на странице.

Атрибуты области видимости приведены в таблице:

Параметр	**Описание**
Название	Имя области видимости
Описание	Примечание к области видимости

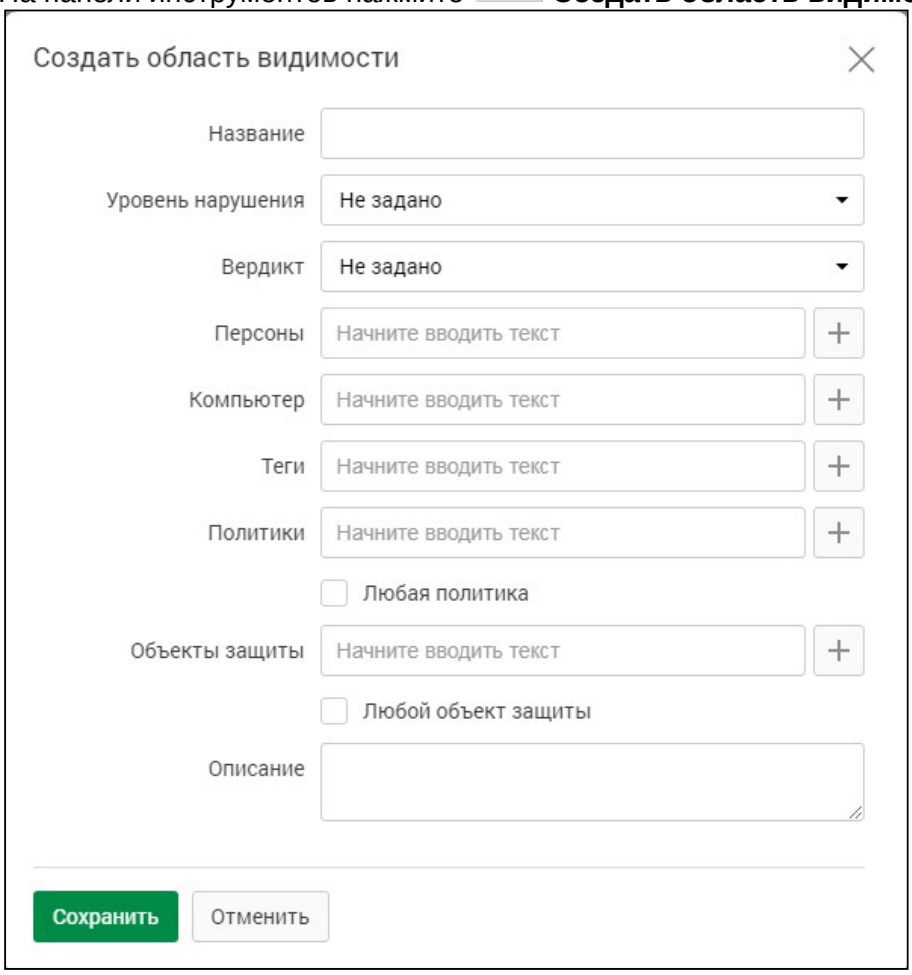
Вы можете выполнять следующие действия при управлении областями видимости:

- 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  **Создать область видимости**.

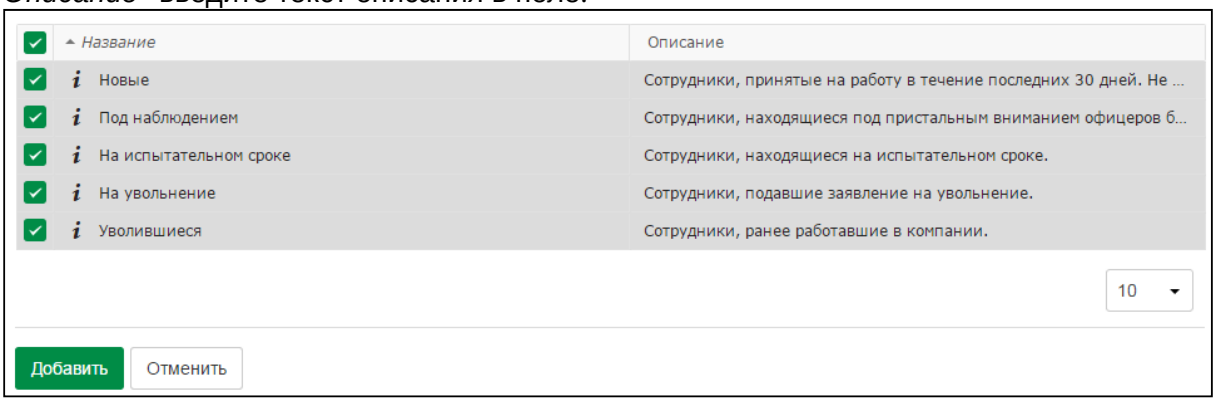


4. В открывшемся окне заполните требуемые поля следующим образом:

1. *Название* - введите название в поле.
2. *Уровень нарушения* - выберите из раскрывающегося списка.
3. *Вердикт* - выберите из раскрывающегося списка.
4. *Персоны* :
   введите первые символы наименования пользователя и выберите требуемое значение из выпадающего списка
   или

нажмите  и в появившемся окне, в списке пользователей, установите флажки требуемым пользователям. Нажмите **Добавить**.

5. *Компьютер* – аналогично пункту d.
6. *Теги* - аналогично пункту d.
7. *Политика* – аналогично пункту d.
8. *Объект защиты* – аналогично пункту d.
9. *Любой объект защиты* - выберите настройку.
10. *Описание* - введите текст описания в поле.



- Нажмите **Добавить**.

Редактирование области видимости

Чтобы изменить параметры области видимости:

1. Перейдите в раздел **Управление** -> **Управление доступом**.
2. Перейдите на вкладку **Области видимости**.
3. На панели инструментов нажмите  **Редактировать область видимости**.
4. В открывшемся окне измените параметры области видимости аналогично действиям по созданию области видимости (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  **Удалить область видимости**.

> **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**.

5.10.3 Управление лицензиями

Важно!

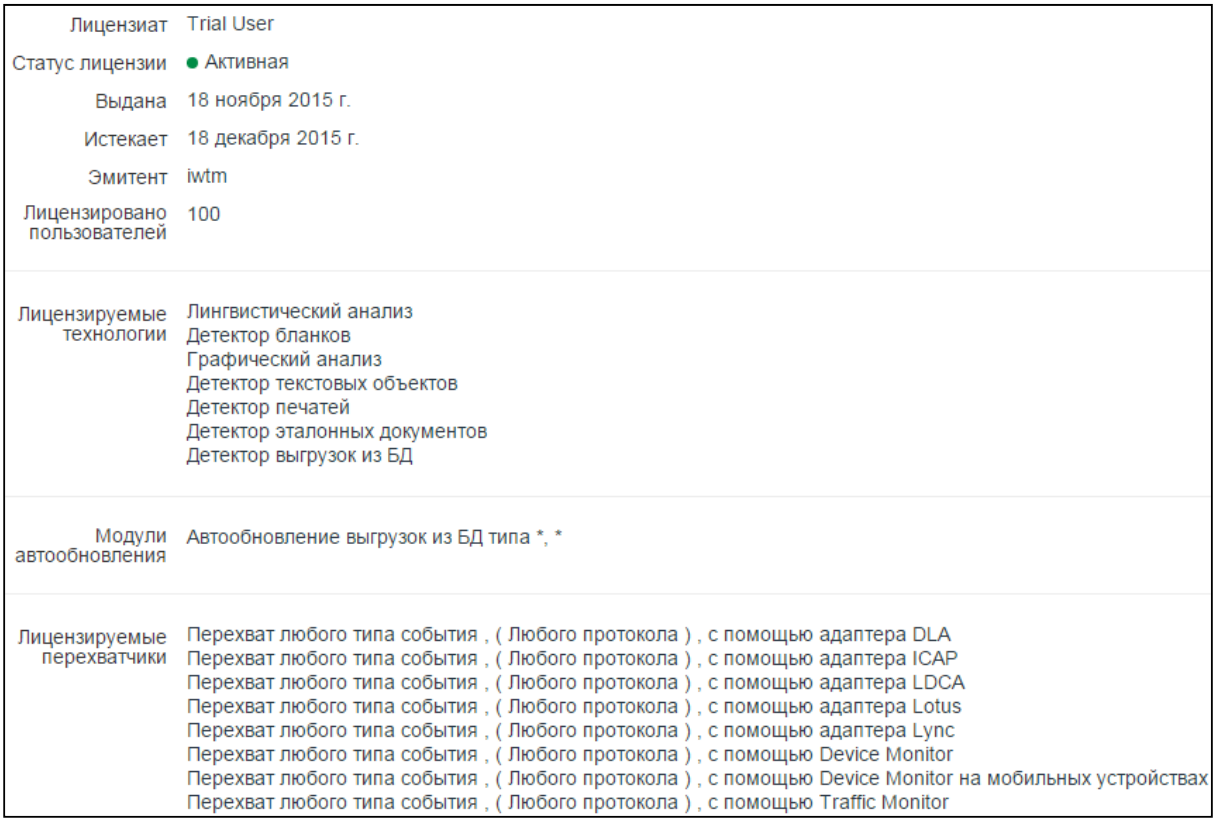
Описание лицензирования Системы приведено в документе "*InfoWatch Traffic Monitor. Руководство администратора*", статья "Лицензирование".

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.

5.10.4 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 кнопку **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**.

5.10.5 Управление службами

Администратору Системы предоставлена возможность управлять службами без использования командной строки Linux.

Доступны следующие действия со службами:

- Запуск службы
- Остановка службы
- Перезапуск службы
- Сохранение логов службы

Запуск службы

Чтобы запустить службу:

1. Перейдите в раздел **Управление - Службы**.
2. Установите флажок в поле службы, которую Вы хотите запустить.
3. Нажмите кнопку .

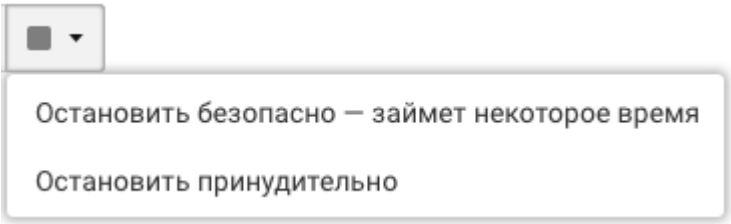
Примечание:

Чтобы запустить несколько служб, необходимо установить флажок напротив каждой из них.

Остановка службы

Чтобы остановить службу:

1. Перейдите в раздел **Управление - Службы**.
2. Установите флажок в поле службы, которую Вы хотите остановить.
3. Нажмите кнопку и выберите один из вариантов:



Остановить безопасно - Система дождется полного завершения работы службы и выполнит ее остановку без потери обрабатываемых в этот момент данных.
Остановить принудительно - быстрая остановка работы службы. Имеется возможность потери данных.

Примечание:

Чтобы остановить несколько служб, необходимо установить флажок напротив каждой из них.

Перезапуск службы

Чтобы перезапустить службу:

1. Перейдите в раздел **Управление - Службы**.
2. Установите флажок в поле службы, которую Вы хотите перезапустить.
3. Нажмите кнопку .

Примечание:

Чтобы перезапустить несколько служб, необходимо установить флажок напротив каждой из них.

Сохранение логов службы

Чтобы сохранить логи службы:

1. Перейдите в раздел **Управление - Службы**.
2. Нажмите **Сохранить** в колонке **Логи** напротив службы, логи которой Вы хотите сохранить.

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.

5.10.6 Сбор диагностических данных

Сбор диагностических данных выполняется в разделе **Управление - Службы.**

Режим сбора данных	Описание
Обычный	Информация о логах Системы, конфигурационная информация, данные о начальной установке
Расширенный	Информация о логах Системы, конфигурационная информация, данные о начальной установке, о ситуациях аварийного завершения процессов системы

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 скачать отчет по результатам последней диагностики:

1. Перейдите в раздел **Управление - Службы** .
2. Скачайте архив по ссылке **Доступен результат последнего сбора данных** в формате `dd-mm-yyyy_hh-mm-ss`.

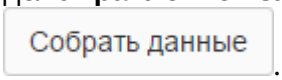
> **Важно!**
>
> В случае, если диагностика ранее не проводилась, скачивание результатов последней диагностики доступно не будет.

Диагностические данные могут быть собраны следующими способами:

- Сбор диагностических данных в обычном режиме
- Сбор диагностических данных в расширенном режиме

Сбор диагностических данных в обычном режиме

Чтобы собрать диагностическую информацию в обычном режиме:

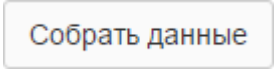
1. Перейдите в раздел **Управление - Службы**.
2. Нажмите кнопку 

.
3. Установите маркер в поле **Обычный**.
4. Нажмите кнопку 

.
5. Дождитесь завершения сборки диагностической информации.
6. Скачайте архив по ссылке **Доступен результат последнего сбора данных** в формате `dd-mm-yyyy_hh-mm-ss`.

Сбор диагностических данных в расширенном режиме

Чтобы собрать диагностическую информацию в расширенном режиме:

1. Перейдите в раздел **Управление - Службы**.
2. Нажмите кнопку 

.
3. Установите маркер в поле **Расширенный**.
4. Нажмите кнопку 

.
5. Дождитесь завершения сборки диагностической информации.

6. Скачайте архив по ссылке **Доступен результат последнего сбора данных** в формате `dd-mm-yyyy_hh-mm-ss`.

5.10.7 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 и выход из Системы;
- управление объектами, отвечающими за разграничение доступа (пользователи, роли, области видимости);
- действия пользователя с объектами Системы (запросы, отчеты, политики, элементы классификатора и т. д.).

> **Примечание:**
>
> Изменения элементов вследствие отмены конфигурации не фиксируются в событиях аудита. В данном случае будет создано только событие отмены конфигурации.

Чтобы задать период хранения событий аудита:

1. Перейдите в раздел **Управление - Аудит**;
2. В области **Период хранения событий аудита (дни)** укажите количество дней хранения событий аудита.

Работа с событиями аудита описана в следующих разделах:

- События аудита
- Фильтрация по пользователю
- Фильтрация по действию
- Фильтрация по объекту
- Фильтрация по дате

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:

Атрибут	Описание
Пользователь	Имя пользователя, осуществившего действие
Объект	Имя объекта, над которым осуществлялось действие
Действие	Тип действия, которое было произведено пользователем

Дата и время действия	Дата/время зарегистрированного действия пользователя
Расширенная информация	Дополнительная информация о событии аудита

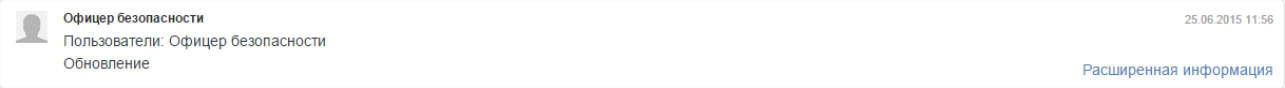
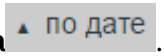


Рисунок 1. Плашка события аудита

Чтобы отсортировать события аудита по дате:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В левом верхнем углу нажмите **Сортировка** 

.

Расширенная информация

Расширенная информация будет отображена в зависимости от *Объекта* и *Действия* зарегистрированных в Системе.

Например, при выходе пользователя из Системы, параметры события аудита будут следующими:

- **DNS-имя** - имя компьютера, с которого происходит выход в Системы;
- **IP** - IP-адрес компьютера, с которого происходит выход в Системы;
- **Логин** - имя пользователя, который произвел выход из Системы.

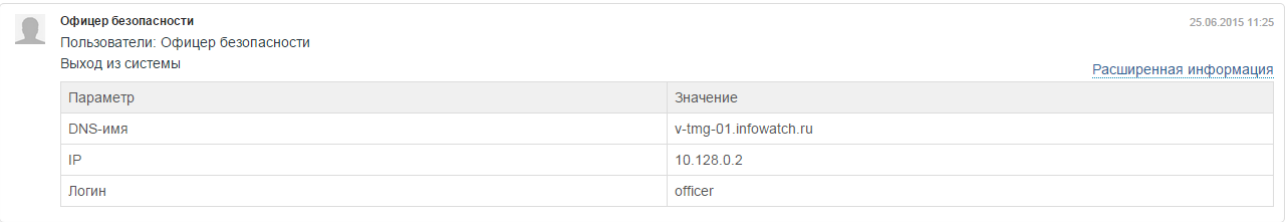


Рисунок 2. Расширенная информация

> **Важно!**
>
> Параметры события аудита могут варьироваться в зависимости от *Объекта* и *Действия*.

Чтобы посмотреть расширенную информацию о событии аудита:

1. Перейдите в раздел **Управление - Аудит**.
2. На плашке событий аудита нажмите **Расширенная информация**.

Фильтрация по пользователю

Чтобы отфильтровать события аудита по пользователю:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В области **Фильтры поиска** выберите имя пользователя из выпадающего списка **Пользователь** (см. "Управление пользователями Системы и их ролями").

Чтобы добавить дополнительные условия фильтрации, используйте параметры *Действие*, *Объект*, *Дата*.

Фильтрация по действию

Чтобы отфильтровать события по совершенному действию:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В области **Фильтры поиска** выберите действие из выпадающего списка **Действие**.

Чтобы добавить дополнительные условия фильтрации, используйте параметры *Пользователь*, *Объект*, *Дата*.

Фильтрация по объекту

Чтобы отфильтровать события по объекту:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В области **Фильтры поиска** выберите объект из выпадающего списка **Объект**.

Чтобы добавить дополнительные условия фильтрации, используйте параметры *Пользователь*, *Действие*, *Дата*.

Фильтрация по дате

Чтобы отфильтровать события по дате:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В области **Фильтры поиска** нажмите на поле **Дата**.
3. В календаре укажите даты начала и конца периода, за который будут показаны события аудита.
4. Нажмите **Применить**.
5. Чтобы отменить фильтрацию по дате, нажмите **Очистить**.

Чтобы добавить дополнительные условия фильтрации, используйте параметры *Пользователь*, *Действие*, *Объект*.

5.10.8 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**.

5.10.9 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**, **InfoWatch Crawler** 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 TM 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 TM, регистрируемых в рамках данного Плагина.
Описание	Да	Описание плагина.
Признак "Предустановленный"	Нет	Входит ли в состав Системы.
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 .

5.10.10 Настройка подключения к почтовому серверу

В разделе **Управление** -> **Подключение к почтовому серверу** вы можете указать SMTP-сервер, который будет использоваться для отправки уведомлений о сработавших правилах (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.
3. Если используется внешний сервер, укажите параметры сервера:
   - **Адрес SMTP-сервера**;
   - **Порт**;
   - **Логин** - необязательный параметр;
   - **Пароль** - необязательный параметр;
   - **Шифрование** - необязательный параметр. Если выбрано **Использовать**, то при подключении будет использоваться SSL-/TLS-шифрование и NTLM-аутентификация.

   После того как вы указали параметры подключения, нажмите **Проверить соединение**.
4. Нажмите **Сохранить**.

5.10.11 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, нарушевшего 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 полики 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 отпавку 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**.

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 подстветкой 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.

6 Работа в Консоли Управления Device Monitor

Консоль управления (DM) предназначена для решения следующих задач:

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

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

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

6.1 Начало работы с Консолью управления (DM)

Общие принципы работы с Консолью управления (DM) изложены в следующих подразделах:

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

6.1.1 Авторизация и соединение с сервером InfoWatch Device Monitor

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

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

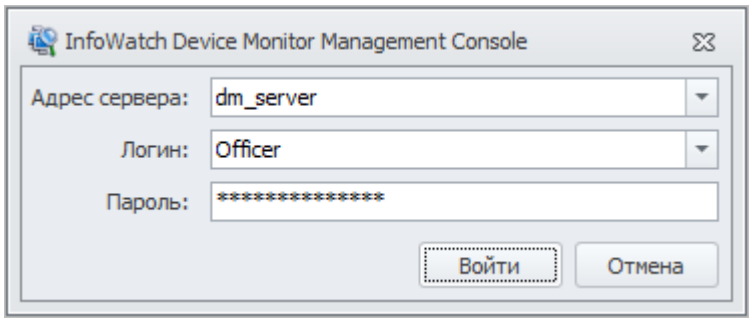
Чтобы начать работу с Консолью управления:

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

Успешное прохождение авторизации возможно только при выполнении следующих условий:

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

Данные для авторизации вводят в диалоговом окне подключения.



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

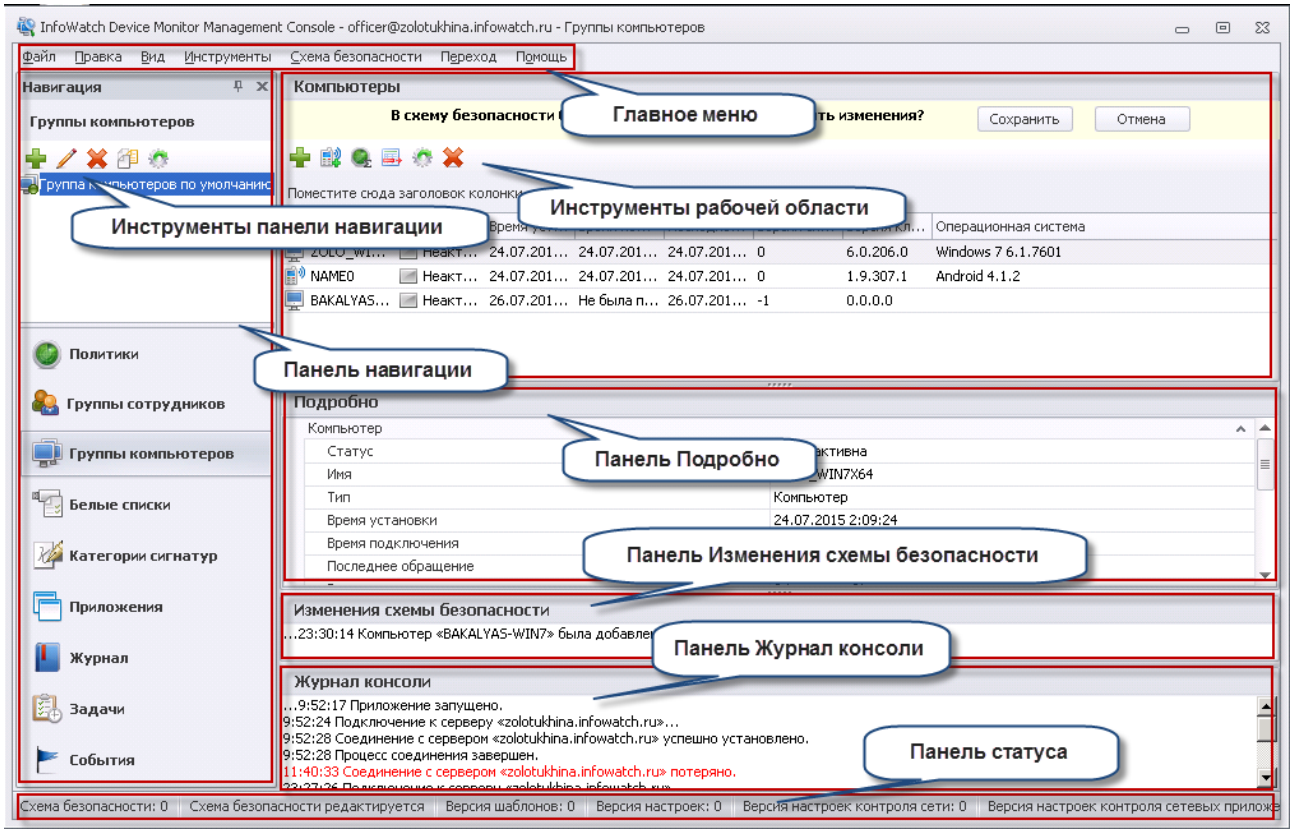
При первом запуске Консоли управления поля диалогового окна **Подключение** – пустые. В дальнейшем поля **Адрес сервера** и **Пользователь** будут заполнены данными, соответствующими последней попытке авторизации. Поле **Пароль** необходимо заполнять при каждой попытке авторизации.

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

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

6.1.2 Главное окно Консоли управления (DM)

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



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

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

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

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

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

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

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

Настройка элементов главного окна Консоли управления (DM)

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

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

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

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

Чтобы скрыть/отобразить панель инструментов или панель статуса, щелкните правой кнопки мыши в области панели инструментов или панели статуса. Затем в раскрывшемся контекстном меню отметьте те элементы, которые будут отображены на экране (по умолчанию выделена только панель статуса).

6.1.3 Разделы Консоли управления (DM)

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

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

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

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

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

6.2 Управление учетными записями и ролями Консоли управления (DM)

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

В Консоли управления (DM) используется один предустановленный пользователь - **Суперпользователь,** обладающий всеми правами при работе в Консоли. Он не предназначен для

повседневной работы с Системой, рекомендуется использовать исключительно для первоначальной настройки Консоли управления (DM), создания учетной записи для Администратора, а затем - только в аварийных условиях.

Для разграничения полномочий пользователей, работающих с Консолью управления (DM), используются роли. Есть возможность для одного пользователя задать разные роли на разные группы. Для каждой роли определен набор полномочий. Пользователь не может выполнять действия, которые выходят за рамки назначенной ему роли.
В Консоли управления (DM) используются следующие предустановленные роли:

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

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

Список доступных действий для предустановленных ролей:

Действия	Администратор	Офицер безопасности	Офицер безопасности группы
Просмотр журнала аудита		+	
Экспорт записей журнала аудита		+	
Удаление записей из журнала аудита			
Учетные записи пользователей Консоли управления (DM)	+	+	
Добавление, редактирование, удаление учетных записей пользователей Консоли управления	+		
Назначение/ удаление ролей для пользователей Консоли управления	+		
Блокировка/разблокировка учетных записей пользователей Консоли управления	+		
Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor		+	
Просмотр предыдущих версий схем безопасности		+	
Редактирование схемы безопасности		+	
Импорт/экспорт политик безопасности и правил		+	

Просмотр событий		+	
Удаленная установка, обновление и удаление Агентов Device Mionitor		+	
Временный доступ сотрудника к сети		+	
Временный доступ сотрудника к устройствам		+	
Создание группы			+
Просмотр и управление группами сотрудников, Просмотр и управление группами компьютеров, Просмотр событий группы			+
Просмотр белых списков, управление белыми списками			+
Управление агентами		+	+

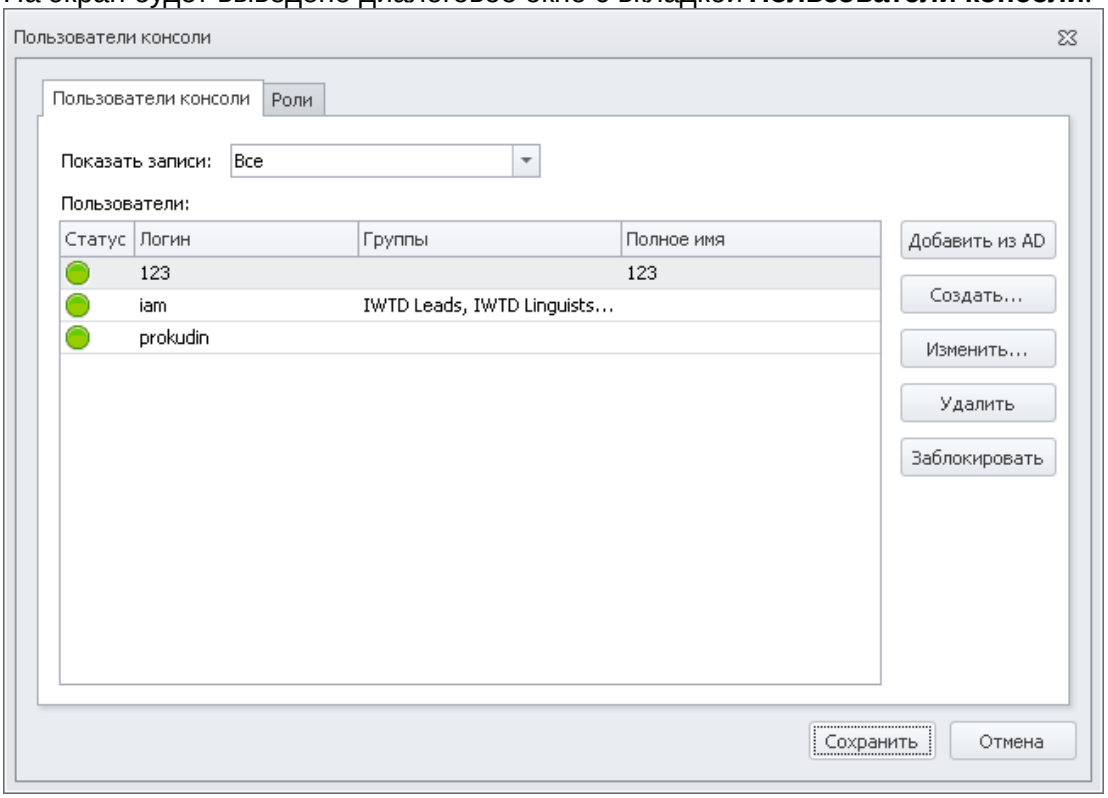
Более подробная информация об управлении учетными записями Консоли управления (DM) содержится в подразделах:

- Учетные записи пользователей Консоли управления (DM);
- Добавление учетной записи Консоли управления (DM);
- Блокирование и разблокирование учетной записи Консоли управления (DM);
- Редактирование учетной записи Консоли управления (DM);
- Удаление учетной записи Консоли управления (DM);
- Аудит действий по управлению схемой безопасности в Консоли управления (DM).

6.2.1 Учетные записи пользователей Консоли управления (DM)

Чтобы просмотреть информацию об учетных записях Консоли управления:

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



2. В верхней части данного окна расположено поле **Показать записи**. Из раскрывающегося списка в этом поле выберите тип отображаемых учетных записей:
   - **Все**. Все учетные записи, независимо от их статуса.
   - **Активные**. Список всех действующих учетных записей.
   - **Заблокированные**. Учетные записи, которые были заблокированы, но могут быть разблокированы (см. "Блокировка/разблокировка учетных записей пользователей Консоли управления (DM)").
   - **Удаленные**. Список учетных записей, которые были удалены и не подлежат восстановлению. Однако информация о действиях, которые эти пользователи выполнили, в Системе сохраняется.

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

Для учетной записи отображаются следующие элементы:

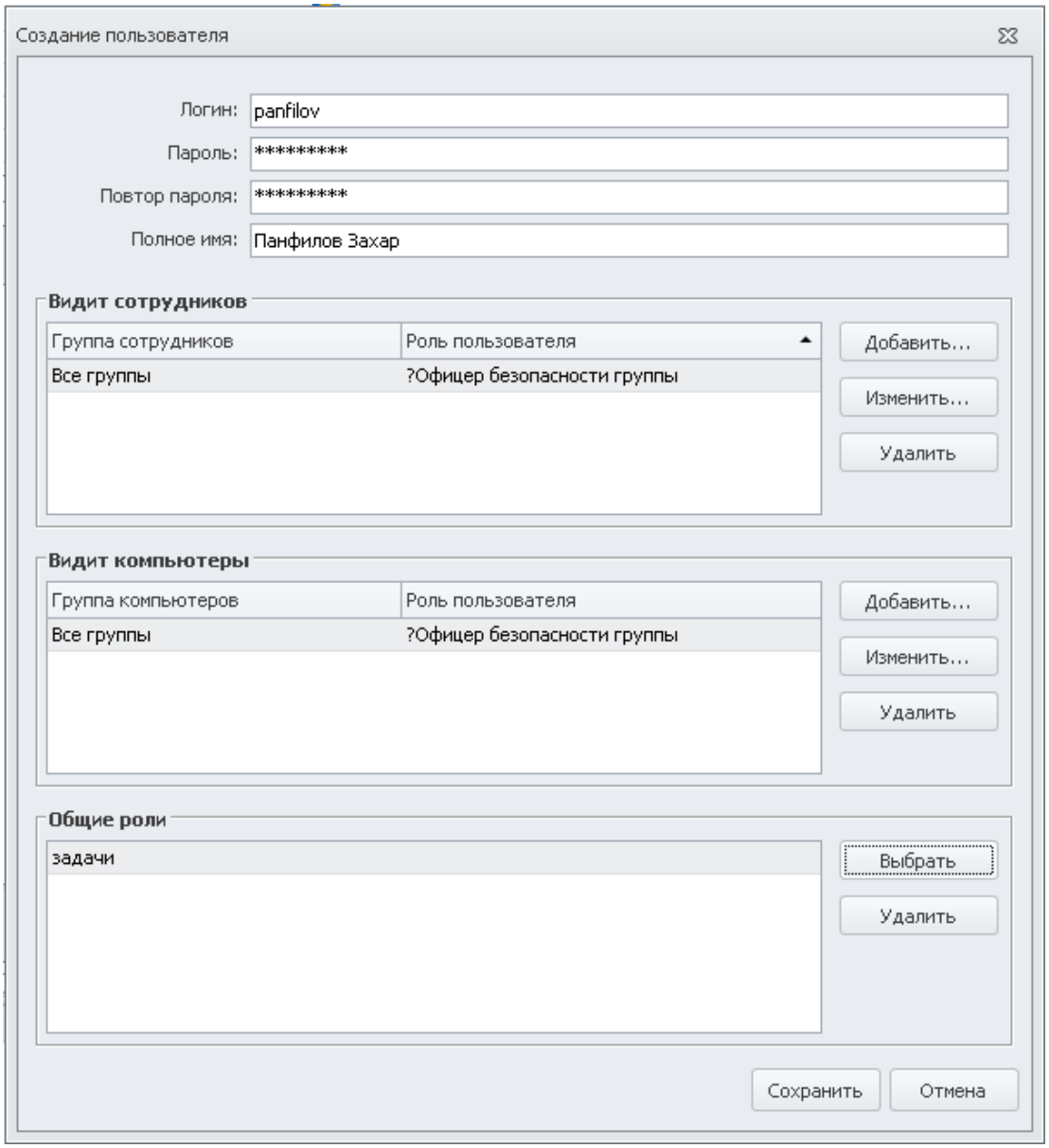
- **Статус**. Признак того, является ли учетная запись активной (), заблокированной () или удаленной ().
- **Логин**. Имя учетной записи.
- **Группы**.Группы, доступные пользователю.
- **Полное имя**. Фамилия, имя и отчество пользователя.

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

Добавление учетной записи Консоли управления (DM)

Чтобы добавить новую учетную запись Консоли управления:

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



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

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

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

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

Чтобы добавить пользователя из Active Directory или ALD:

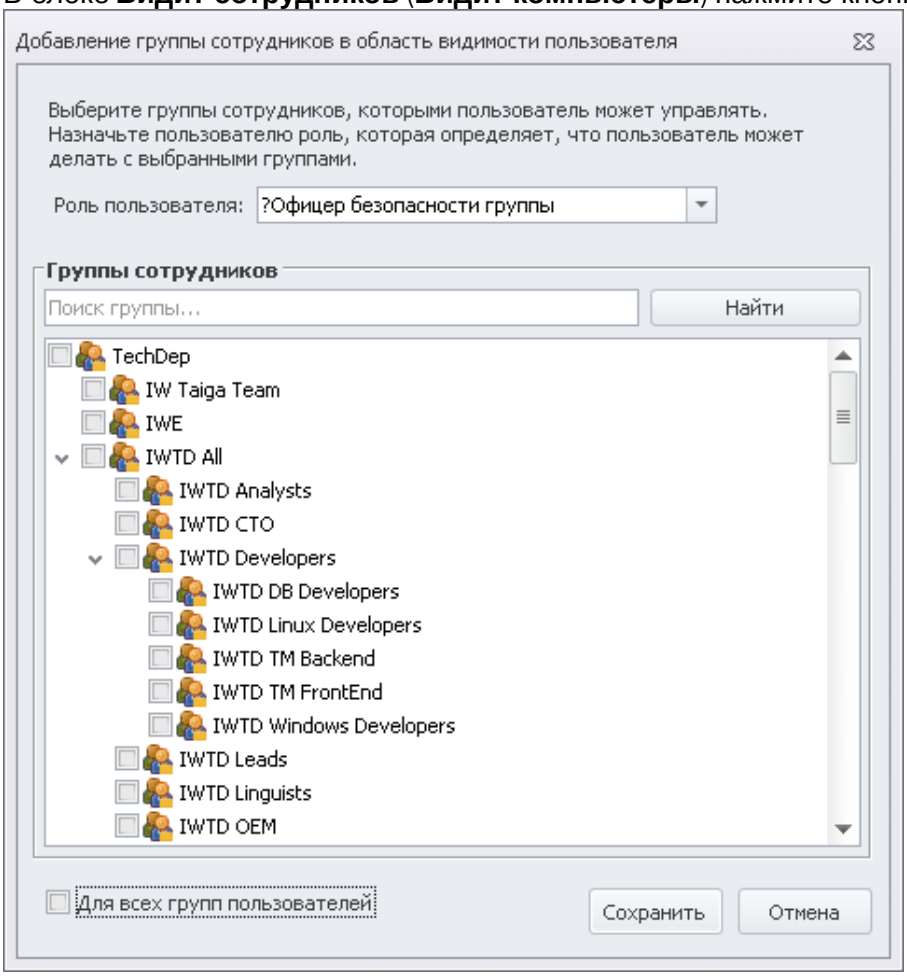
1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**.
2. Нажмите на кнопку **Добавить из AD**, расположенную в правой части диалогового окна на вкладке **Пользователи консоли**.
3. В открывшемся окне **Добавление пользователя из AD** выберите пользователя из группы (или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

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

Добавление роли пользователя на группы сотрудников (компьютеров)

Чтобы добавить группу сотрудников в область видимости пользователя:

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



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

Редактирование роли пользователя на группы сотрудников (компьютеров)

Чтобы изменить права доступа в область видимости пользователя:

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

3. Нажмите кнопку **Изменить.**
4. В открывшемся окне назначьте роль, определяющую действия пользователя на группу. Дальнейшие возможности по действиям с сотрудниками (компьютерами) будут осуществляться согласно привилегиям выбранной роли.
5. Нажмите **Сохранить**.

Чтобы снять роль с пользователя:

1. Перейдите в окно **Изменение пользователя.**
2. В блоке **Видит сотрудников** (**Видит компьютеры**) выберите нужную группу.
3. Нажмите кнопку **Удалить.**
4. Нажмите **Да** для подтверждения. Выбранная роль будет снята с пользователя.

Настройка общих ролей пользователя

Чтобы назначить общие роли пользователю:

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

Чтобы снять общие роли с пользователя:

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

Редактирование учетной записи Консоли управления (DM)

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

Чтобы отредактировать параметры учетной записи Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**. На экран будет выведено диалоговое окно **Пользователи консоли**.
2. На вкладке **Пользователи консоли** выберите строку с названием учетной записи, которую нужно отредактировать.
3. Нажмите на кнопку **Изменить**, расположенную в правой части данного окна, или дважды щелкните левой кнопкой мыши по выделенной строке.
4. В открывшемся диалоговом окне **Изменение пользователя** отредактируйте параметры учетной записи, описанные в разделе "Добавление учетной записи Консоли управления (DM)").

5. После того как все необходимые параметры будут настроены, нажмите на кнопку **Сохранить**.
6. Чтобы сделанные изменения окончательно вступили в силу, нажмите на кнопку **Сохранить** в диалоговом окне **Пользователи консоли**.

> **Важно!**
>
> Недоступно любое редактирование предустановленных пользователей, кроме изменения пароля.

Блокирование и разблокирование учетной записи Консоли управления (DM)

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

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

Чтобы заблокировать/разблокировать учетную запись Консоли управления:

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

Удаление учетной записи Консоли управления (DM)

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

> **Важно!**
>
> Учетные записи Суперпользователя и предустановленных пользователей не могут быть удалены.
> Удаленные учетные записи не могут быть восстановлены для повторного использования.

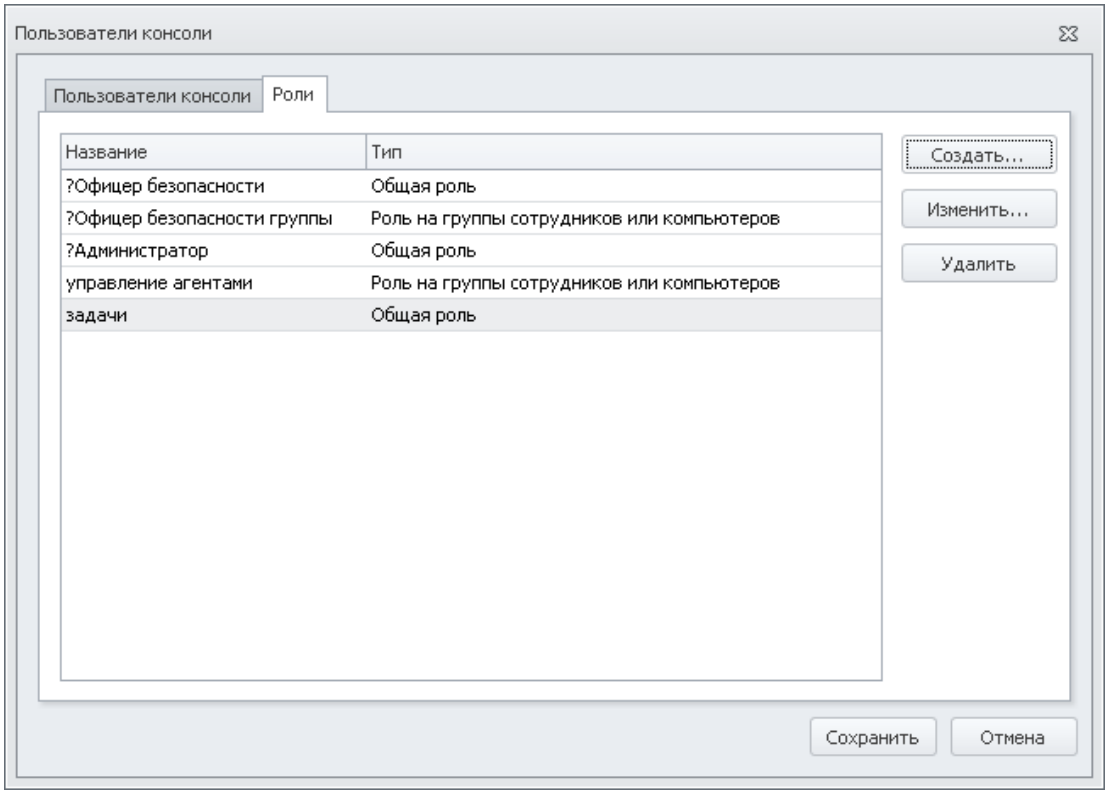
Чтобы удалить учетную запись Консоли управления:

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

6.2.2 Роли пользователей Консоли управления (DM)

Чтобы просмотреть информацию о ролях пользователей Консоли управления:

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



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

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

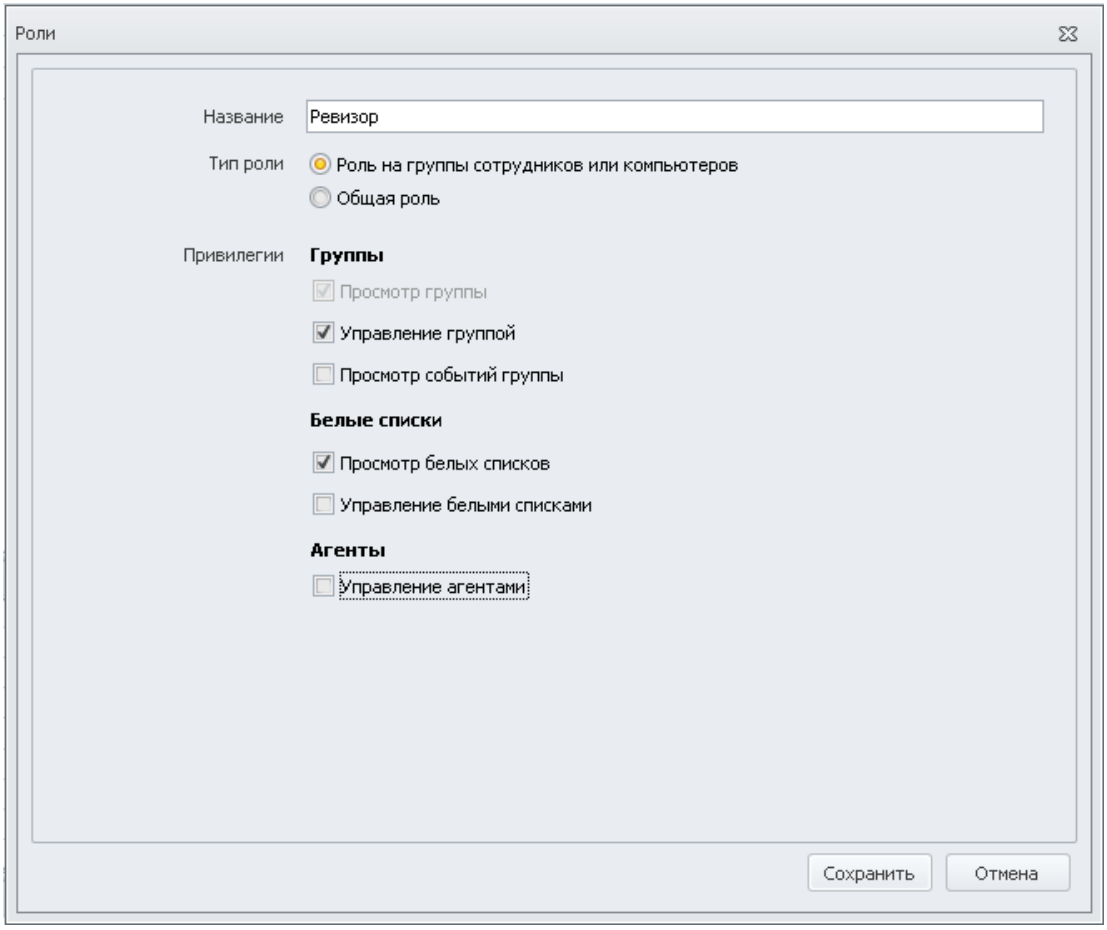
Подробное описание привилегий вы можете найти на странице "Добавление роли пользователя Консоли управления (DM)".

Добавление роли пользователя Консоли управления (DM)

Чтобы добавить новую роль пользователя Консоли управления:

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

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



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

Привилегии пользователей

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

- по отношению к конкретной группе компьютеров или сотрудников;
- по отношению к Системе в целом (общие привилегии).

Привилегии на группы сотрудников/компьютеров

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

Общие привилегии

Привилегия	Доступные действия
Политики	
Просмотр всех политик	Просмотр всех имеющихся в Системе политик, доступных на чтение или редактирование, и входящих в них правил
Управление всеми политиками	• Редактирование всех имеющихся в Системе политик (независимо от владельца и уровня доступа к политике) и входящих в них правил • Создание новой политики • Удаление политики (доступно только владельцу политики)
Управление доступными политиками	• Редактирование доступных пользователю политик (политик, для которых пользователь является владельцем, и политик, доступных на редактирование всем пользователям) • Создание новой политики • Удаление политики (доступно только владельцу)
Другие привилегии	
Просмотр журнала аудита	Доступ в раздел "Журнал"
Удаление записей журнала	Удаление записей из журнала аудита, очистка журнала аудита **Примечание:** при добавлении данной привилегии привилегия **Просмотр журнала аудита** добавляется автоматически.
Управление пользователями	▪ Просмотр пользователей и ролей консоли ▪ Создание пользователей и ролей консоли ▪ Редактирование пользователей и ролей консоли ▪ Удаление пользователей и ролей консоли
Создание групп	Создание новых групп компьютеров или сотрудников. Новая група автоматически добавляется в группы, доступные пользователю. На группу назначается предустановленная роль "Офицер безопасности группы". **Примечание:** при добавлении данной привилегии привилегия **Просмотр всех политик** добавляется автоматически.
Управление агентами на отдельных компьютерах	• Добавление компьютеров из сетевого окружения и через подключение к AD или ALD в задаче распространения агентов • Добавление компьютеров через импорт файла и по имени/IP в задаче распространения агентов • Создание пакета установки
Управление настройками	Управление глобальными настройками DM (кроме раздела "Интеграция с AD" в меню **Инструменты** -> **Настройки**)

Привилегия	Доступные действия
Синхронизация с AD	Настройка синхронизации рабочих станций и сотрудников с AD и ALD (раздел "Интеграция с AD" в меню **Инструменты** -> **Настройки**)
Импорт/экспорт конфигурации	Импорт и экспорт схемы безопасности и настроек **Важно!** Данная привилегия позволяет пользователю Консоли импортировать и экспортировать конфигурацию вне зависимости от наличия у него прав на импортируемые/экспортируемые объекты
Предоставление временного доступа	Предоставление по запросу сотрудника временного доступа к сети или устройствам

Редактирование роли пользователя Консоли управления (DM)

Важно!

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

Чтобы отредактировать параметры роли пользователя Консоли управления:

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

Важно!

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

Удаление роли пользователя Консоли управления (DM)

Чтобы удалить роль пользователя Консоли управления:

1. В главном меню выберите команду **Инструменты** > **Пользователи консоли и роли**. На экран будет выведено диалоговое окно **Пользователи консоли**.
2. На вкладке **Роли** выберите строку с названием роли, которую нужно удалить.

3. Нажмите на кнопку **Удалить**, расположенную в правой части данного окна.
4. В появившемся окне запроса нажмите на кнопку **ОК**, чтобы подтвердить удаление.

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

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

6.2.3 Аудит действий по управлению схемой безопасности в Консоли управления (DM)

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

Информация по работе с журналом аудита содержится в следующих подразделах:

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

Просмотр журнала аудита

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

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

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

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

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

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

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

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

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

Свойство	Описание
Транзакция (#)	Номер транзакции
Шаг	Порядковый номер элементарного действия, выполненного в рамках данной транзакции
Дата	Дата и время выполнения действия
Объект	Название объекта, над которым выполнялось действие
Действие	Тип действия
Селектор	Содержит информацию, позволяющую однозначно идентифицировать объект, над которым было выполнено действие. Расшифровка значений параметра Селектор приведена в разделе "Значения параметра Селектор".
Поле	Атрибут объекта, измененный в ходе выполнения действия
Старое значение	Значение атрибута до изменения
Новое значение	Новое значение атрибута
Пользователь	Имя учетной записи Консоли управления (DM), под которой выполнялась транзакция
Учетная запись Windows	Учетная запись, с данными которой пользователь авторизован в Windows
Компьютер	Название компьютера, на котором было выполнено действие
Порядковый номер	Порядковый номер, присвоенный этой записи, в базе данных

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

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

Пример:

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

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

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

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

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

Значения параметра Селектор

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

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

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

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

Пример 1:

В журнале аудита имеется следующая запись:

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

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

Расшифровка значения Селектора

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

Пример 2:

В журнале аудита имеется следующая запись:

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

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

Расшифровка значения Селектора

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

Пример 3:

В журнале аудита имеется следующая запись:

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

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

Расшифровка значения Селектора

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

Фильтрация записей в журнале аудита

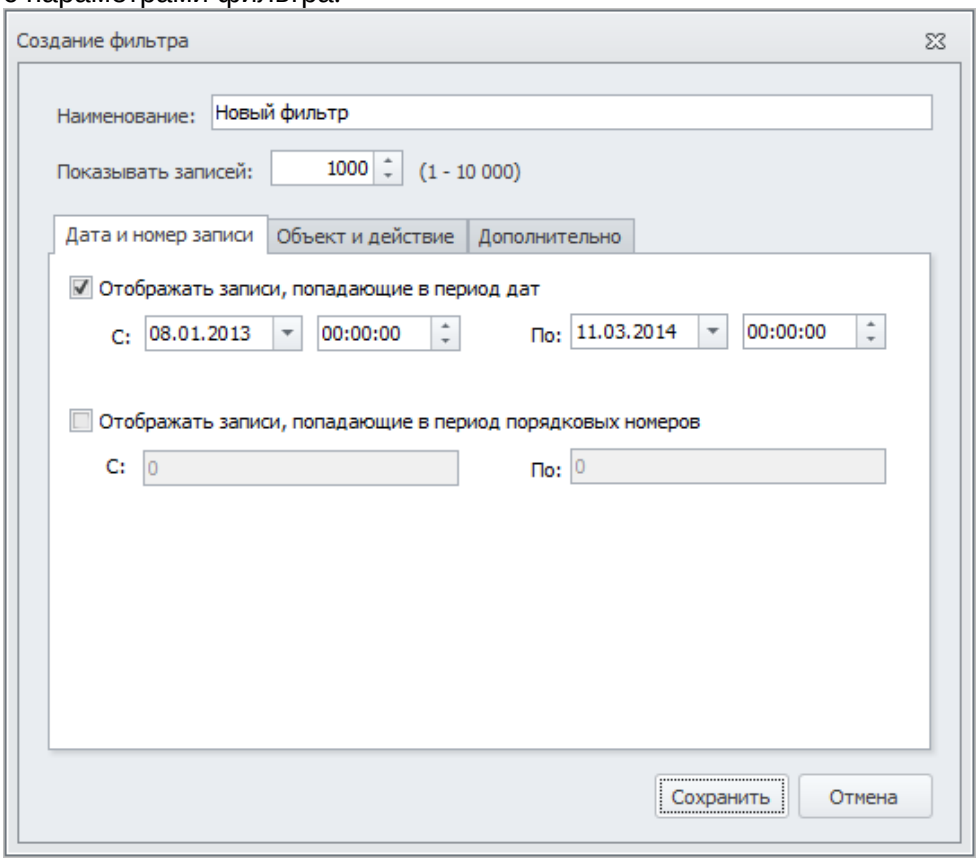
Для получения доступа к записям журнала аудита, удовлетворяющим определенным критериям, вы можете воспользоваться функциями фильтрации.

Чтобы создать фильтр или изменить существующий:

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

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

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



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

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

5. Нажмите **Сохранить**.

Чтобы удалить фильтр:

1. Перейдите к разделу **Журнал**.

2. В области **Журнал** на Панели навигации выберите название фильтра, который нужно удалить.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - щелкните правой кнопкой мыши и в контекстном меню выберите **Удалить**;
   - используйте сочетание клавиш **Ctrl+D**.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление фильтра.

Вкладка Дата и номер записи

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

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

Чтобы задать условия фильтрации по дате и времени:

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

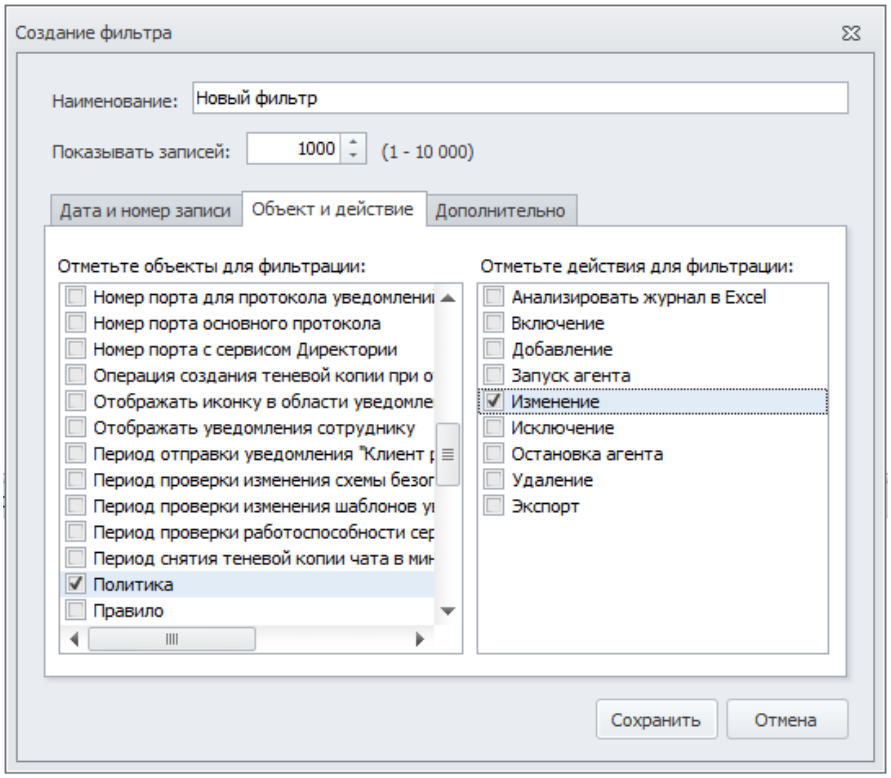
Чтобы задать условия фильтрации по порядковому номеру:

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

Вкладка Объект и действие

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

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



Чтобы задать условия фильтрации:

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

Вкладка Дополнительно

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

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

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

Примечание.

Значение дополнительного параметра фильтрации вводится без учета регистра символов.

Удаление записей из журнала аудита

Важно!

Удалять записи из журнала аудита может только Суперпользователь.

Чтобы удалить записи из журнала аудита:

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

   Важно!

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

3. Нажмите **ОК**.

Экспорт записей журнала аудита

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

Чтобы экспортировать записи журнала аудита:

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

После этого записи журнала аудита будут экспортированы в указанный файл.

Анализ журнала аудита в Microsoft Excel

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

Чтобы просмотреть записи журнала аудита в Microsoft Excel:

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

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

6.3 Общие настройки Системы

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

- Общие настройки работы Агентов
- Контроль сетевых соединений
- Контроль сетевого трафика
- Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor
- Соединение с сервером LDAP и синхронизация с сервером Active Directory и Astra Linux Directory
- Настройка уведомлений сотрудников о нарушении правил (DM)
- Исключение приложений из перехвата
- Контроль приложений и снимки экрана
- Хранение событий
- Работа с Менеджером управления серверами
- Остановка и запуск агента Device Monitor

Важно!

Измененные настройки вступят в силу на контролируемых компьютерах сразу же после того, как Агенты на каждом компьютере, получив уведомление от Сервера (при проверке работоспособности сервера, или при проверке изменения схемы безопасности, или при проверке изменения шаблонов уведомлений), выполнят обновление.

6.3.1 Общие настройки работы Агентов

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

Чтобы указать общие настройки работы Агентов Device Monitor:

1. В главном меню выберите команду **Инструменты** > **Настройки**.
2. На левой панели выберите **Общие**.
3. Измените необходимые параметры:

Параметр	Описание
Соединение	
Отправлять на сервер уведомления о работе Агента каждые	Периодичность, с которой Агент отправляет на сервер уведомления о своей работе, в секундах.
Проверять работоспособность сервера каждые	Периодичность, с которой Агент выполняет проверку доступности сервера, в секундах.
Проверять изменения схемы безопасности каждые	Если Агент работает в активном режиме (т.е. сам опрашивает Сервер об изменениях схемы безопасности), то проверка будет выполняться с указанной периодичностью, в секундах.
Проверять изменения шаблонов уведомлений для активных Агентов каждые	Если Агент работает в активном режиме (т.е. сам опрашивает Сервер об изменениях шаблонов уведомлений, то проверка будет выполняться с указанной периодичностью, в секундах. **Примечание**: Подробнее о настройке уведомлений см. "Настройка уведомлений сотрудников о нарушении правил (DM)".
Контроль дискового пространства на Агентах	
Минимальное свободное дисковое пространство на Агенте	Минимальный размер свободного пространства (в процентах) на контролируемом компьютере, при достижении которого, теневые копии не будут создаваться. Т.е. если при создании теневой копии свободного пространства на Агенте останется меньше чем указано, то копия создаваться не будет; частичной копии также не будет. Подробнее см. "Создание теневых копий и запрет операций при нехватке свободного места"

Если место под события на диске закончилось	На том диске контролируемого компьютера, куда выполняется установка Агента Device Monitor, выделяется место, достаточное для хранения информации о 30000 событий. Если Агент Device Monitor настолько долго не имел связи с сервером Device Monitor, что накопилось более 30000 событий, контролируемых правилами (DM), определенными для сотрудника/компьютера, то любые действия, контролируемые текущей политикой безопасности (DM), могут быть запрещены. Чтобы запретить, выберите **Запрещать операции**. Чтобы все действия могли неконтролируемо выполняться, выберите **Разрешать операции**.
Скорость отправки данных с Агента	
Ограничивать скорость отправки данных	При узком канале связи, во избежание его чрезмерной загрузки, вы можете регулировать скорость отправки теневых копий на сервер. Для этого отметьте настройку и укажите верхнюю границу скорости, Кбит/с, в поле **Максимальная скорость отправки данных**.
События	
Логировать события от перехватчика устройств и облачных хранилищ	Степень детализации при сохранении сведений о работе с внешними устройствами, получаемых перехватчиками Device Monitor и Cloud Storage Monitor: подробнее см. "Правило (DM) для Device Monitor", "Правило (DM) для Cloud Storage Monitor" и "Просмотр событий". Возможен один из следующих вариантов: - **Не логировать** - события не сохраняются; - **При отказе в доступе** - события создаются только при попытках нарушения политики безопасности (DM) - то есть при блокировании использования устройства, включая блокирование попыток превышения уровня доступа. Использование внешних устройств, не запрещенных политиками (DM), не фиксируется. - **Логировать всегда** - сохраняются сведения обо всех действиях (подключение/использование любых устройств, даже занесенных в белые списки)
Логировать соединения вне корпоративной сети	Степень детализации при сохранении сведений о передаче данных по сетевым соединениям, получаемых перехватчиком Network Monitor: подробнее см. "Правило (DM) для Network Monitor". Возможен один из следующих вариантов: - **Не логировать** - события не сохраняются; - **При отказе в доступе** - события создаются только при попытках нарушения политики безопасности (DM) - то есть при блокировании попыток соединения.
Поведение агента на компьютере	
Отображать уведомления сотруднику	Признак того, что при попытке сотрудника выполнить действие, запрещенное политикой безопасности (DM), ему будет отображаться предупреждающее уведомление. Подробнее см. "Настройка уведомлений сотрудников о нарушении правил (DM)"

Скрывать присутствие агента на компьютере	Признак того, что Система будет скрывать присутствие Агента на компьютерах. Если данная настройка не отмечена, в области уведомлений панели задач Windows на компьютере, где установлен Агент, будет отображаться значок . При нажатии на этот значок будет доступна информация о работе Агента, а также список контролируемых в данный момент устройств. **Важно!** Если на контролируемом компьютере включена антивирусная защита, то антивирус может выявлять работу Device Monitor: например, в списке процессов, запущенных на контролируемом компьютере или в списке программ, инициирующих контроль.
Ключ формирования кодов	
Обновить	Нажмите кнопку Обновить, чтобы Система сгенерировала новый ключ, используемый для формирования кодов снятия запрета доступа к сетевым соединениям или устройствам. Подробнее о кодах см. "Временный доступ сотрудника к сети" и "Временный доступ сотрудника к устройствам", параметры **Код запроса** и **Код подтверждения**. Частое обновление ключа не рекомендуется.

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

6.3.2 Контроль сетевых соединений

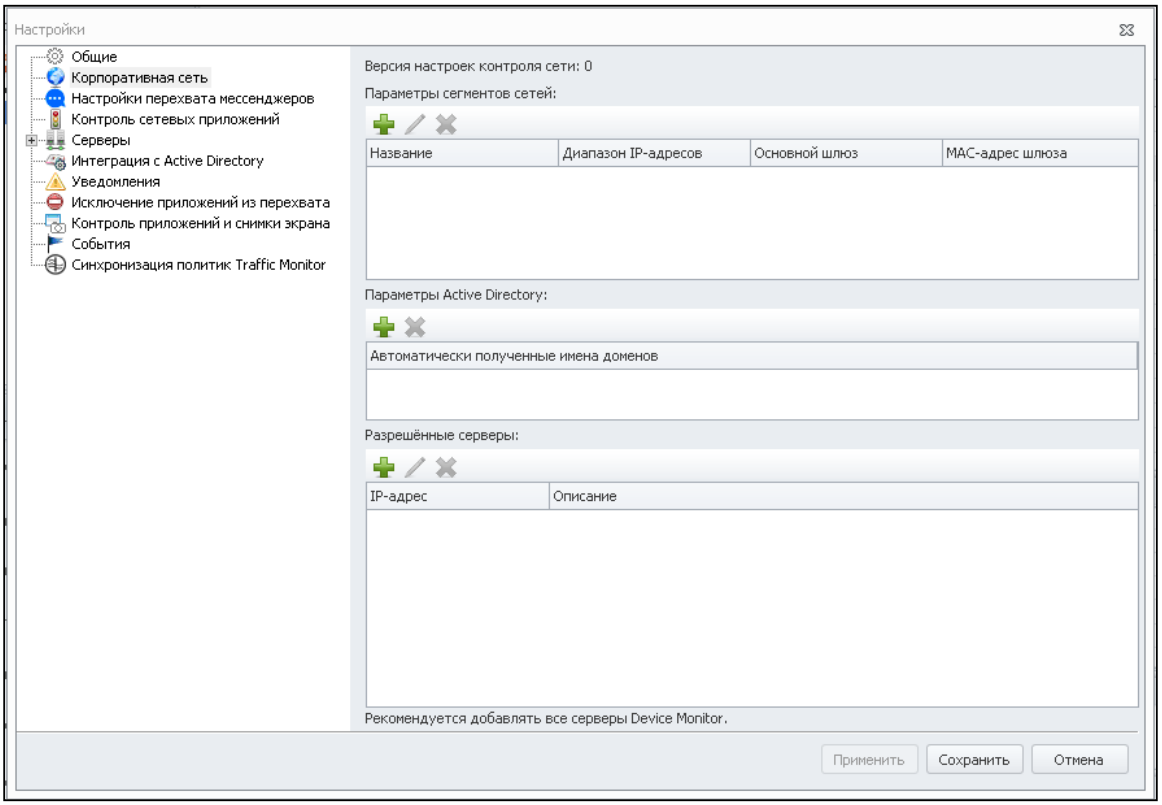
Для обеспечения контроля передачи данных по сетевым соединениям с помощью **Network Monitor** (о настройке правил (DM) для данного типа контроля см. "Правило (DM) для Network Monitor") необходимо задать параметры того, какие сегменты сети считаются корпоративной сетью, и какие внешние адреса разрешены.

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

Чтобы настроить параметры контроля сетевых соединений:

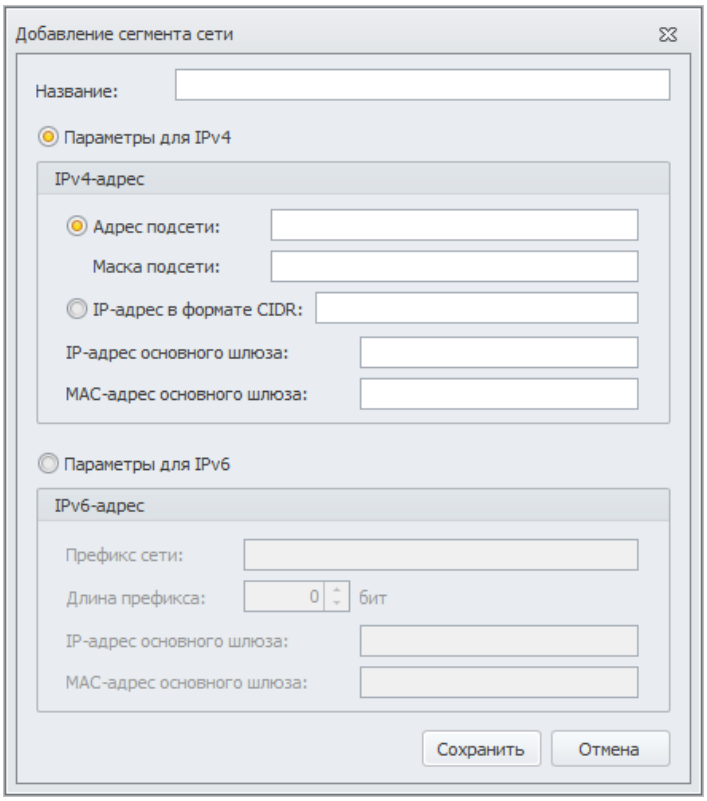
1. В главном меню выберите команду **Инструменты** > **Настройки**.

2. На левой панели выберите **Корпоративная сеть**.



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

сегмента сети.



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

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

Чтобы удалить сервер из списка разрешенных, выберите его, нажмите  (либо нажмите клавишу **Delete**), затем нажмите **Да** в окне подтверждения.

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

Определение наличия подключения к корпоративной сети для различных вариантов заполнения:

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

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

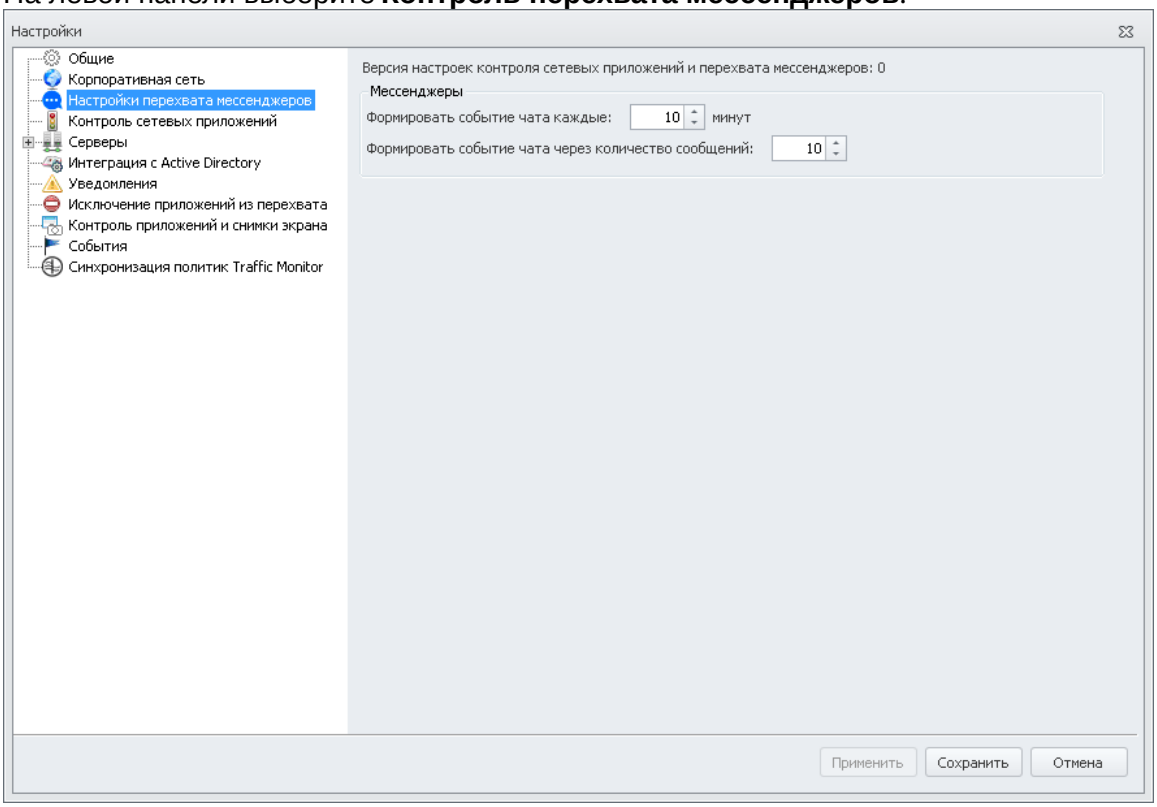
6.3.3 Контроль мессенджеров

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

Чтобы настроить параметры контроля мессенджеров:

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

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



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

6.3.4 Контроль сетевого трафика

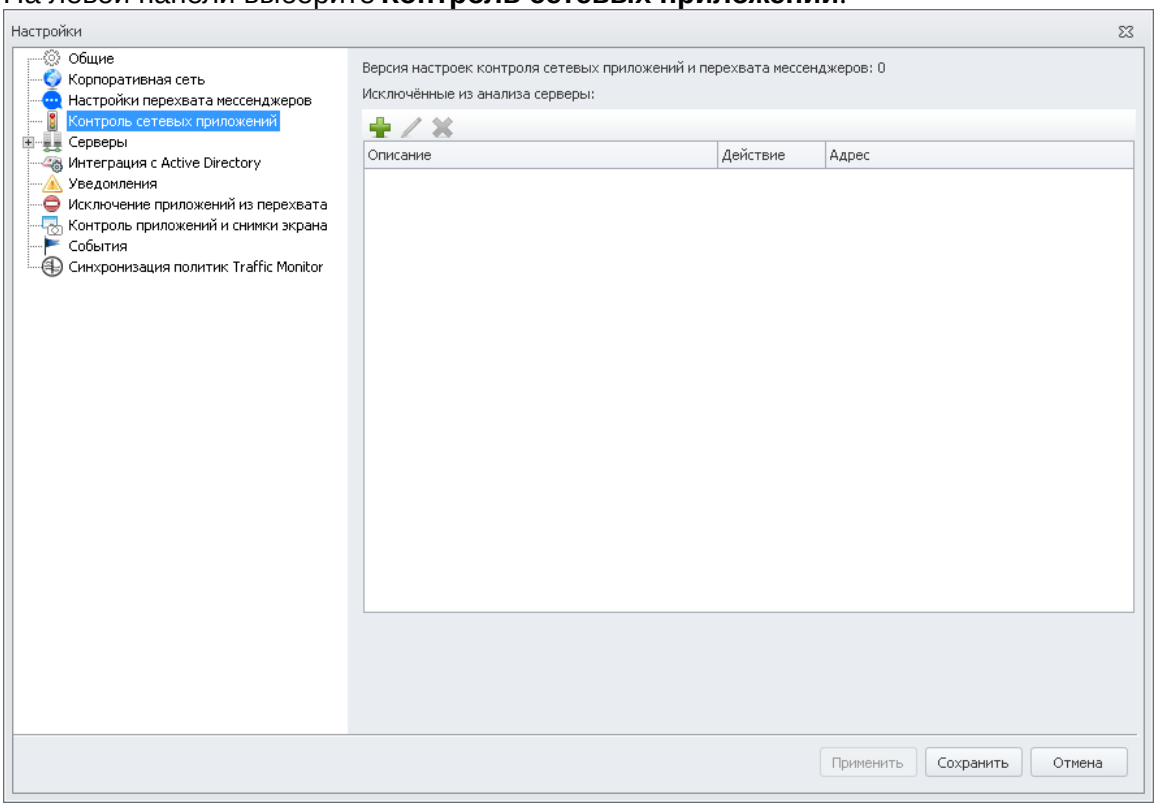
Для контроля сетевого трафика на Агенте Device Monitor реализован прозрачный прокси-сервер. На этот сервер перенаправляются все соединения, вне зависимости от используемого протокола. Далее Агент Device Monitor разбирает протокол и определяет, относится ли данный протокол к перехватываемым. Перехватываются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

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

Чтобы настроить параметры контроля сетевого трафика:

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

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



3. Вы можете задать перечень адресов серверов, при соединении с которыми контроль протоколов проводиться не будет (то есть трафик на данные серверы не будет перенаправляться на внутренний прокси-сервер) либо принудительно контролироваться (будет перенаправляться на внутренний прокси-сервер).

> **Примечание:**
>
> Разрешение внешних адресов может понадобиться, например, для обеспечения работы с внешними ресурсами и обновления установленных программ, например:
>
> - для автоматического обновления Firefox в списке разрешенных серверов должны присутствовать *.mozilla.com и *.mozilla.net;
> - для работы Filezilla - update.filezilla-project.org;
> - для работы Dropbox - *.dropbox.com;
> - для работы Yandex Disk:
>   - oauth.yandex.ru
>   - webdav.yandex.ru
>   - clck.yandex.ru
>   - push.xmpp.yandex.ru
>   - и т.п.

> **Примечание:**
>
> Для агентов, установленных на Astra Linux, из перехвата исключается только трафик, передаваемый на сервер через SSL-протокол.

Чтобы задать список разрешенных или запрещенных серверов:

a. В области **Исключенные из анализа серверы** нажмите .
b. В диалоговом окне **Добавить сервер в список исключенных из анализа** введите описание сервера. Подробнее о добавляемых адресах см. "Добавление серверов.
c. Выберите нужное действие: **Исключить из перехвата** или **Включить в перехват**.
d. Задайте DNS-имя или IP-адрес сервера и порт подключения.
e. Если необходимо, выберите **Диапазон адресов** и задайте интервал IP-адресов.

> **Примечание:**
>
> Дополнительно при исключении сервера из перехвата можно выбрать и ввести **Домен из MiM перехватчика,** трафик которого будет исключен из перехвата при SSL-соединении.

f. Нажмите **ОК**.
g. Повторите действия для других разрешенных адресов.
h. Чтобы изменить параметры сервера, выберите его в списке и нажмите .
i. Чтобы удалить сервер из списка разрешенных, выберите его, нажмите , затем нажмите **Да** в окне подтверждения удаления.

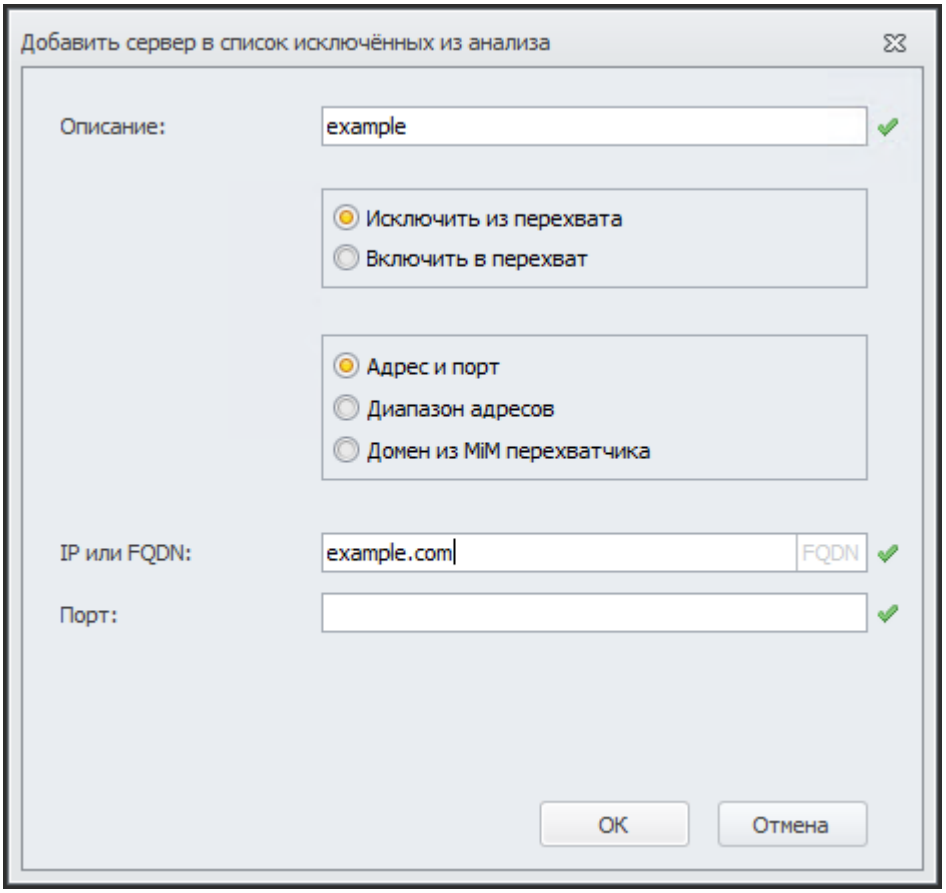
4. Чтобы внесенные изменения начали действовать, нажмите **Применить**.

Добавление серверов

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

Чтобы задать список разрешенных или запрещенных серверов:

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

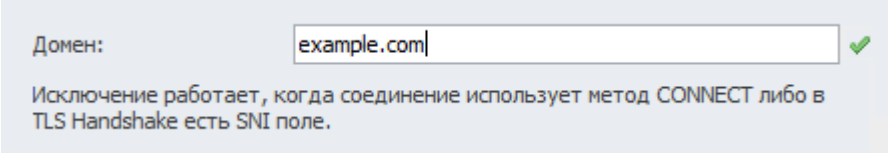


2. В диалоговом окне **Добавить сервер в список исключенных из анализа** введите описание сервера:
   - чтобы добавить отдельный порт сервера:
     a. Выберите нужное действие: **Исключить из перехвата** или **Включить в перехват**;
     b. Установите флажок в поле **Адрес и порт**;
     c. Укажите FQDN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

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

c. Укажите домен



3. Нажмите **ОК**.

В текстовом виде адрес IPv4 записывается как nnn.nnn.nnn.nnn, где nnn принимает значения от 0 до 255, а каждая буква n представляет десятичную цифру. Незначащие нули можно не указывать.
В текстовом виде адрес IPv6 записывается как xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, где каждая буква x - это шестнадцатеричная цифра, представляющая 4 бита. Незначащие нули можно не указывать**.**

> **Важно!**
>
> Включение в перехват имеет более высокий приоритет, чем исключение.
>
> Шаблонные исключения будут работать, только если агент подключается через прокси-сервер.
>
> Адрес 0.0.0.0 применяется только в сочетании с портом, так как является специальным адресом для исключения всех адресов с указанным портом.

Пример 1:

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

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

Пример 2:

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

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

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

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

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

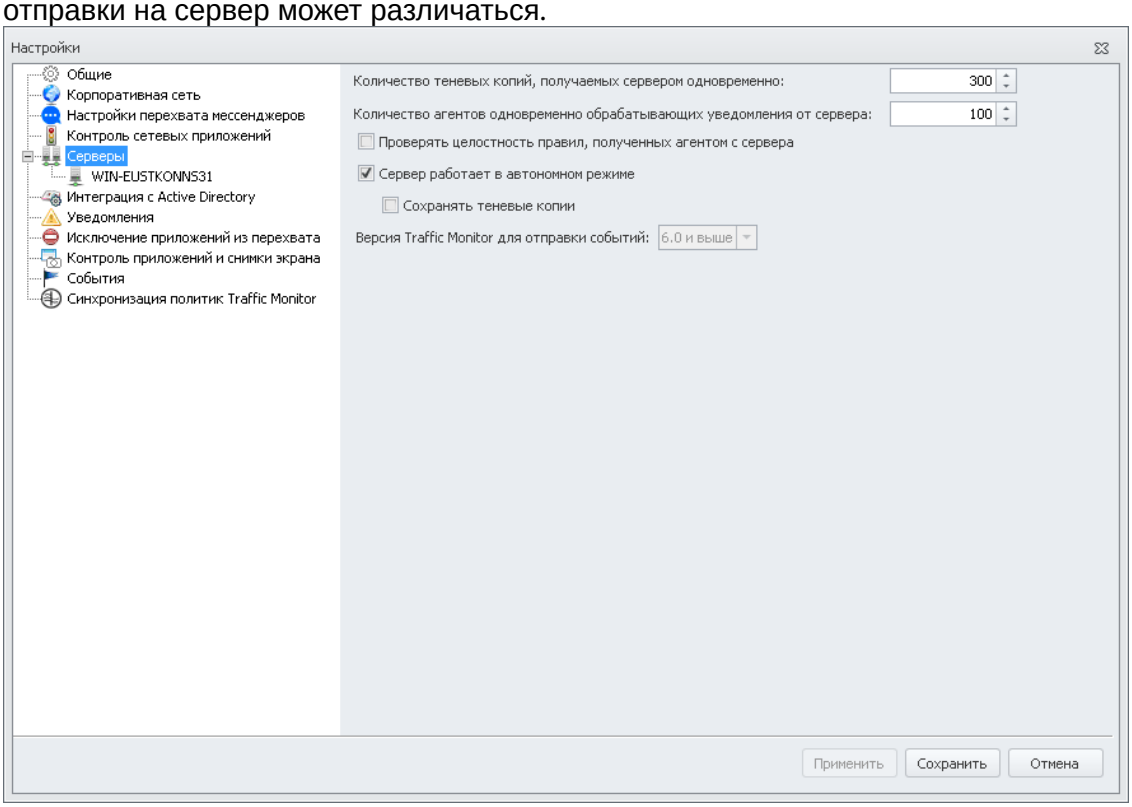
6.3.5 Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor

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

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

1. В главном меню Консоли управления (DM) выберите команду **Инструменты** > **Настройки**.
2. В узле **Серверы** определите следующие настройки:

- **Количество теневых копий, получаемых сервером одновременно** - определяет количество копий, которые могут поступить на сервер в один момент времени.
- **Количество агентов, одновременно обрабатывающих уведомления от сервера** - определяет количество агентов, которые могут получать уведомления (например, политику безопасности (DM)) от сервера в один момент времени.
- **Проверять целостность правил, полученных агентом с сервера** - проверяет, что схема безопасности, полученная с сервера, не повреждена.
- **Сервер работает в автономном режиме** - сервер работает без интеграции с Traffic Monitor.
    - **Сохранять теневые копии** - теневые копии сохраняются на локальном диске сервера по пути установки в папке `ShadowCopyTempDir`.
- **Версия Traffic Monitor для отправки событий** - текущая версия Traffic Monitor, с которой происходит интеграция. В зависимости от версии, формат событий для отправки на сервер может различаться.



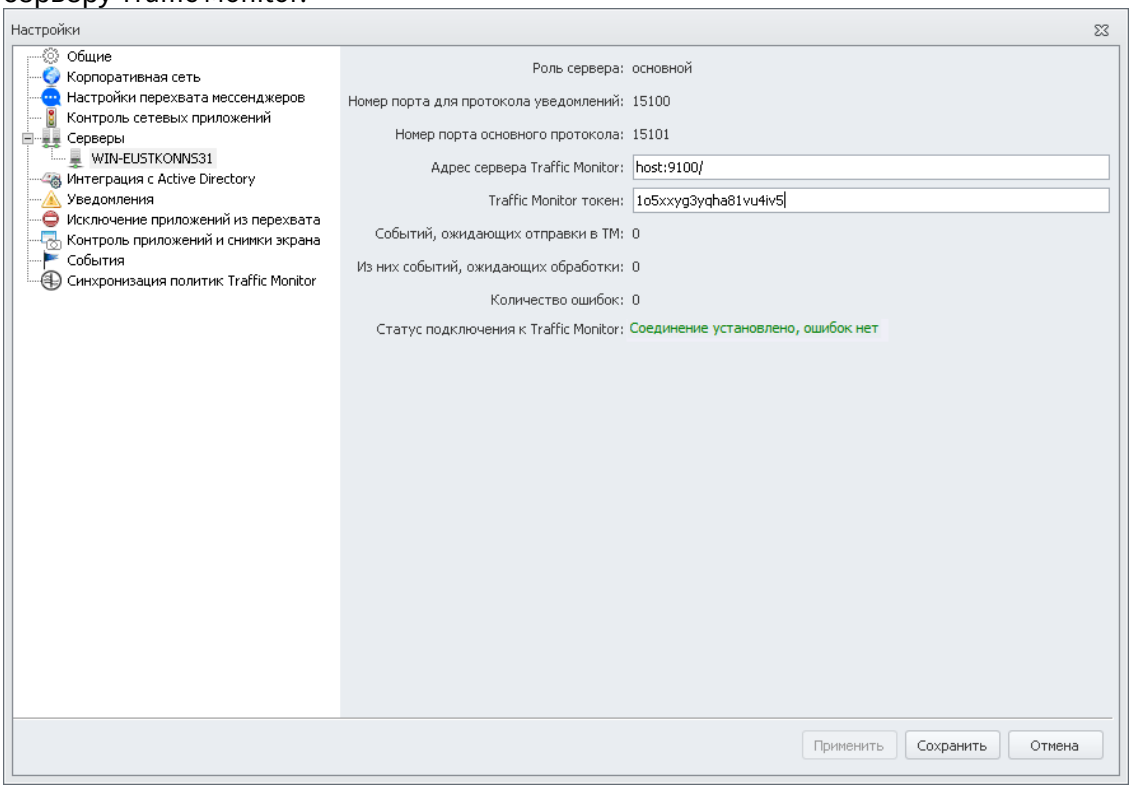
3. При выборе сервера подключения отображается информация по следующим параметрам соединения:
    - **Роль сервера** – роль сервера (*основной* или *вспомогательный*), назначенная при установке данного сервера (см. документ "*Traffic Monitor. Руководство по установке*", статья "Порядок установки серверной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

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

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

  Строка подключения должна быть заполнена в формате URI (Uniform Resource Identifier), формальный синтаксис которого описан в RFC 3986 http://tools.ietf.org/html/rfc3986.
  В качестве параметра `port` указывается порт сервера InfoWatch Traffic Monitor, через который будет о существляться доставка событий. По умолчанию, порт сервера InfoWatch Traffic Monitor - 9100.
- **Traffic Monitor токен** – токен для подключения к API. Необходимо указывать при работе с Traffic Monitor версии 6.0 и выше. Вы можете получить актуальный токен от администратора Traffic Monitor.
- **Событий, ожидающих отправки в ТМ** – общее количество событий для отправки в систему InfoWatch Traffic Monitor.
- **Из них событий, ожидающих обработки** – количество событий, ожидающих обработки перед отправкой в систему InfoWatch Traffic Monitor.
- **Количество ошибок** – количество событий, помещенных в отдельную очередь ошибок.

- **Статус подключения к Traffic Monitor** – информация о состоянии подключения к серверу Traffic Monitor.



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

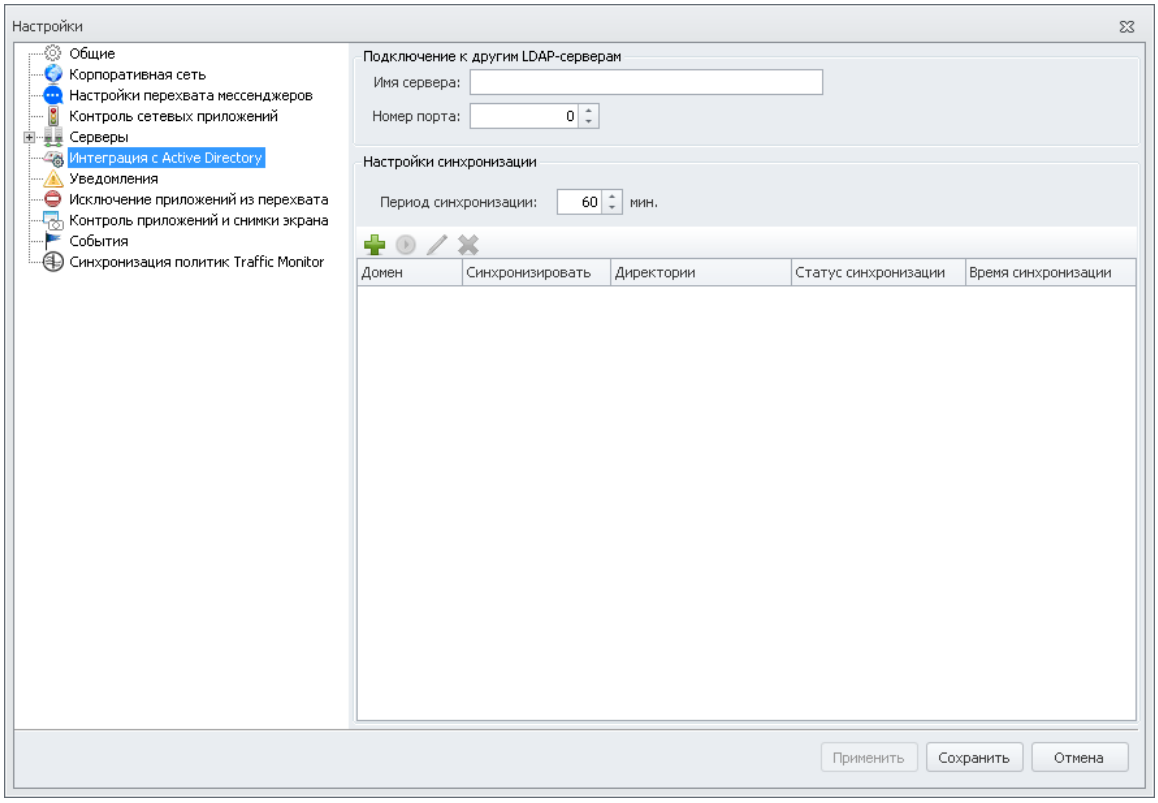
6.3.6 Соединение с сервером LDAP и синхронизация с сервером Active Directory и Astra Linux Directory

Настройка параметров соединения с сервером LDAP

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

Чтобы просмотреть и настроить параметры соединения с сервером LDAP:

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



Примечание:

Подключение к серверу LDAP осуществляется в анонимном режиме.

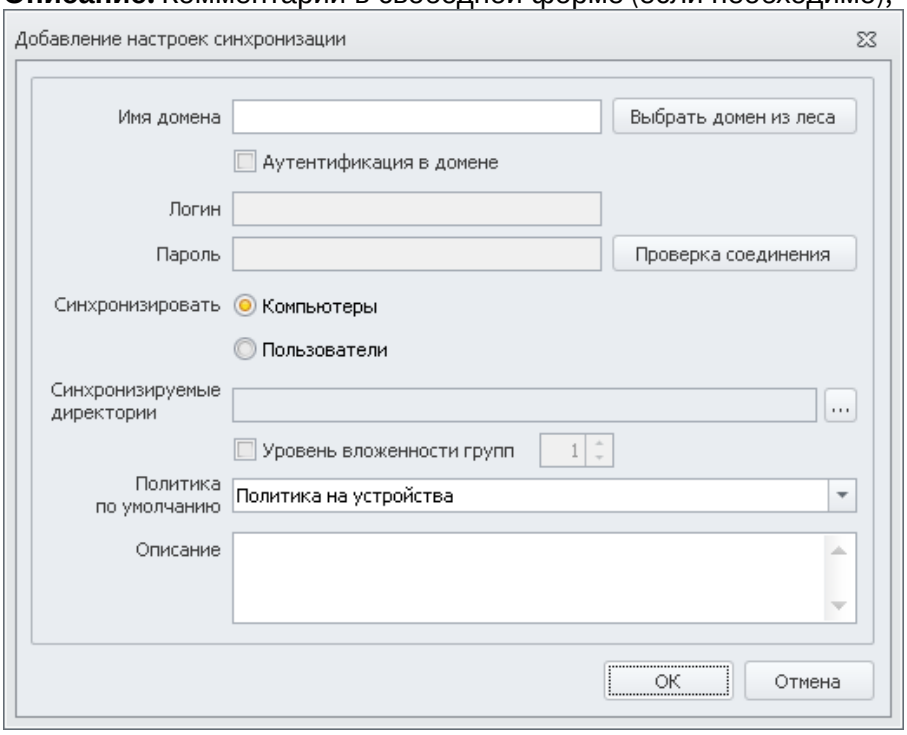
Добавление настроек синхронизации

Чтобы добавить настройку синхронизации с Active Directory или Astra Linux Directory:

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

- **Имя домена.** Имя домена, с которым должна производиться синхронизация (можно ввести вручную или выбрать из леса доменов);
- **Логин.** Для аутентификации в домене (если выбран флаг **Аутентификация в домене**);
- **Пароль.** Для аутентификации в домене (если выбран флаг **Аутентификация в домене**);
- **Синхронизировать.** Объекты синхронизации - **Компьютеры** или **Пользователи**;
- **Синхронизируемые директории.** Директории Active Directory или Astra Linux Directory, которые необходимо синхронизировать. Для этого:
    1. Нажмите .
    2. В дереве укажите директории для синхронизации.
    3. Нажмите **Выбрать.**
- **Уровень вложенности групп** (если необходимо)**.** Максимальный уровень вложенности равен 100;
- **Политика по умолчанию.** Политика, которая будет назначена на синхронизируемые группы после первой синхронизации;

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



- После выбора флага **Аутентификация в домене** (при вводе логина и пароля) нажмите **Проверка соединения** для проверки связи с доменом.
- Если соединение успешно установлено, нажмите **ОК**.
- Чтобы настройки вступили в силу, нажмите **Применить** в окне **Настройки.**

> **Примечание:**
>
> Поля **Имя домена** и **Синхронизируемые директории** являются обязательными.

Данные о настройках и результатах синхронизации представлены в сводной таблице в окне **Настройки**:

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

Время синхронизации	Дата и время последней синхронизации

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

Запуск/редактирование/отключение синхронизации

Чтобы запустить синхронизацию с Active Directory или Astra Linux Directory:

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

> **Примечание:**
>
> Синхронизация может запускаться автоматически через выбранный интервал времени. Для этого установите период синхронизации и нажмите **Применить**.

Чтобы отредактировать настройки синхронизации с Active Directory или Astra Linux Directory:

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

Чтобы отключить синхронизацию с Active Directory или Astra Linux Directory:

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

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

6.3.7 Настройка уведомлений сотрудников о нарушении правил (DM)

Если на контролируемом компьютере сотрудник пытается выполнить действие, запрещенное политикой безопасности (DM), отображается уведомление о запрете. Уведомления отображаются при следующих событиях:

- **Запрет доступа к устройству** – сработало правило Device Monitor, запрещающее чтение и запись на устройство (см. "Правило (DM) для Device Monitor").
- **Запрет записи на устройство** – сработало правило Device Monitor, запрещающее запись на устройство (см. "Правило (DM) для Device Monitor").

- **Запрет записи в открытую область** – сработало правило Device Monitor, запрещающее запись на незашифрованные флоппи-дисководы и съемные устройства (см. "Правило (DM) для Device Monitor").
- **Запрет копирования/печати файла, если места для событий недостаточно** – если Агент Device Monitor настолько долго не имел связи с сервером, что закончилось место, выделенное для хранения информации о событиях, контролируемых правилами (DM) (30000 событий), а в общих настройках для такого случая установлена настройка **Запрещена операция** (подробнее см. "Общие настройки работы Агентов"), то запрещаются любые операции, контролируемые текущей политикой безопасности (DM)
- **Запрет передачи данных по сетевым протоколам** – сработало правило (DM) Ftp Monitor, Mail Monitor или IM Client Monitor, запрещающее обмен данными по протоколу FTP/FTPS/SMTP/POP3/Outlook/XMPP/MMP/Skype/Telegram (см. "Правило (DM) для FTP Monitor", "Правило (DM) для Mail Monitor" и "Правило (DM) для IM Client Monitor").
- **Запрет вставки из буфера обмена при нехватке места для событий** – сработала опция «Если место под события закончилось, запрещать операцию», место под события закончилось и выполняется операция вставки из буфера обмена в какое-либо приложение.
- **Запрет доступа к буферу обмена в приложениях** – сработало правило (DM), запрещающее доступ к буферу обмена для приложения при попытке вставки/копирования данных в этом приложении.
- **Запрет печати в приложениях** – сработало правило (DM), запрещающее печать для приложения при попытке печати из этого приложения.
- **Запрет копирования файла при срабатывании политики защиты данных** – отображается при блокировании копирования файла в результате применения политики защиты данных (DM).
- **Запрет передачи данных по сетевым протоколам при срабатывании политики защиты данных** – отображается при блокировании передачи данных по почтовым протоколам, FTP, HTTP(S) в результате применения политики защиты данных (DM)
- **Запрет передачи данных по сетевым протоколам, если места для событий недостаточно** – если Агент Device Monitor настолько долго не имел связи с сервером, что закончилось место, выделенное для хранения информации о событиях, контролируемых правилами (DM) (30000 событий), а в общих настройках для такого случая установлена настройка **Запрещена операция** (подробнее см. "Общие настройки работы Агентов"), то запрещаются любые операции, контролируемые текущей политикой безопасности (DM).
- **Запрет сетевого подключения** – сработало правило (DM) Network Monitor, запрещающее передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами (см. "Правило (DM) для Network Monitor").
- **Запрет сетевого подключения и запрос временного сетевого подключения** – сработало правило (DM) Network Monitor, запрещающее передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами. При этом сотрудник может запросить временный доступ к внешним соединениям (см. "Правило (DM) для Network Monitor" и "Временный доступ сотрудника к сети").
- **Запрос временного доступа к устройству по телефону** – текст, отображаемый при выборе пользователем в интерфейсе Агента InfoWatch Device Monitor, вкладка **Список устройств**, команды **Запросить доступ** (см. "Временный доступ сотрудника к устройствам").

- **Запрос временного доступа к устройству по почте** – текст, отображаемый при выборе пользователем в интерфейсе Агента InfoWatch Device Monitor, вкладка **Список устройств,** команды **Запросить доступ** (см. "Временный доступ сотрудника к устройствам").
- **Запрет доступа к облачному хранилищу** – сработало правило (DM) Cloud Storage Monitor, контролирующее использование веб-клиентов облачных хранилищ (см. "Правило (DM) для Cloud Storage Monitor", настройка **Доступ запрещен**).
- **Запрет записи в облачное хранилище** – сработало правило (DM) Cloud Storage Monitor, контролирующее использование веб-клиентов облачных хранилищ (см. "Правило (DM) для Cloud Storage Monitor", настройка **Только скачивание**).
- **Запрет запуска приложения** – сработало правило (DM) Application Monitor, контролирующее доступ сотрудников к приложениям при помощи черных и белых списков (см. "Настропйка правила для Application Monitor").
- **Запрет снимка экрана** – сработало правило (DM) ScreenShot Control Monitor, контролирующее снятие снимков экрана (см. "Правило (DM) для ScreenShot Control Monitor").
- **Запрет вставки данных** - сработало правило (DM) Clipboard Monitor, контролирующее вставку данных из буфера обмена (см. "Правило (DM) для Clipboard Monitor").

Чтобы полностью отключить отображение уведомлений сотрудникам или включить его обратно:

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

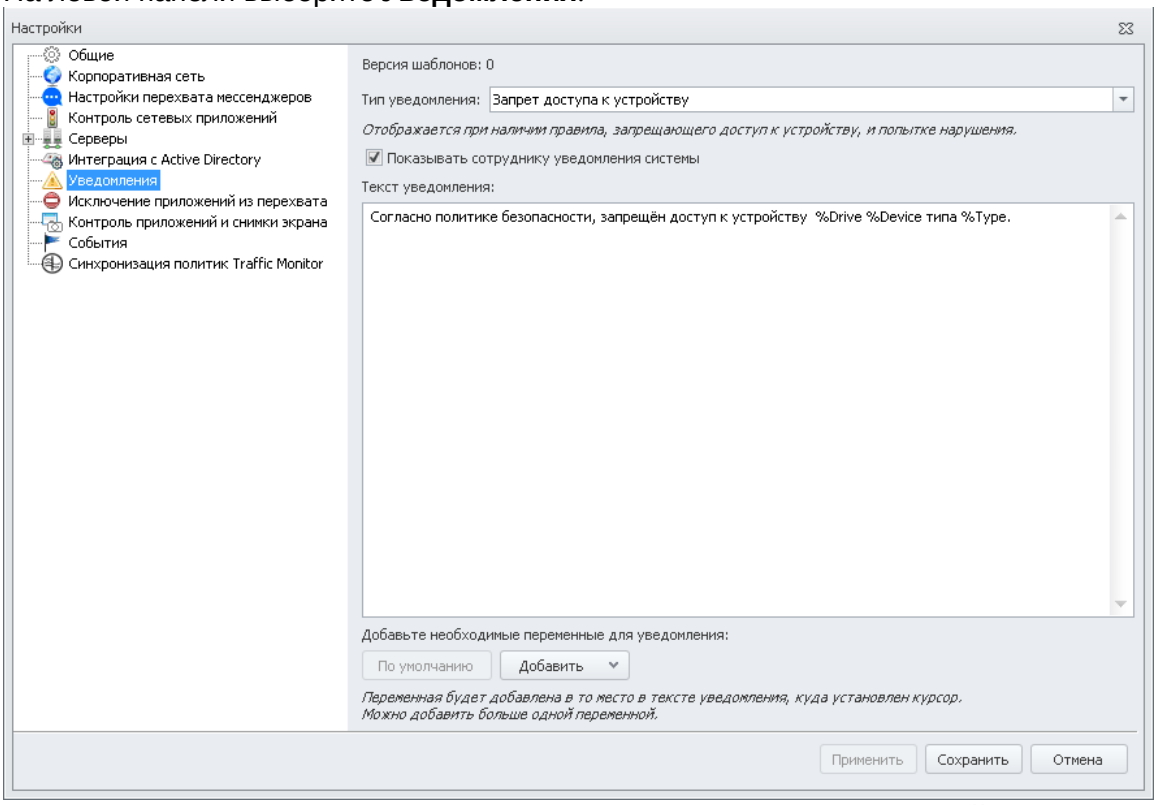
При необходимости, вы можете изменить текст уведомлений, а также отключить отображение любого типа уведомлений, или включить отображение обратно.

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

Чтобы изменить текст уведомлений или включить\отключить отдельные уведомления:

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

2. На левой панели выберите **Уведомления**.



3. Из раскрывающегося списка **Тип уведомления** выберите необходимый тип уведомлений.
4. Чтобы включить (отключить) отображение данного типа уведомлений, отметьте поле (снимите отметку с поля) **Показывать сотруднику уведомления системы**.
5. В поле ввода текста введите необходимый текст уведомления.
   В сообщении вы можете использовать переменные, которые при выводе сотруднику будут преобразовываться в актуальные данные: например, тип заблокированного устройства или IP-адрес разрешенного хоста. Для этого установите курсор в необходимое место текста уведомления, затем нажмите **Добавить** и в раскрывшемся списке выберите необходимую переменную.
   Чтобы отменить сделанные изменения и вернуть настройки по умолчанию, нажмите **По умолчанию**.
6. Нажмите **Применить**. При необходимости, измените настройки для других уведомлений, повторяя шаги 3-5.
7. После того, как сделаны все необходимые изменения, нажмите **Сохранить**.

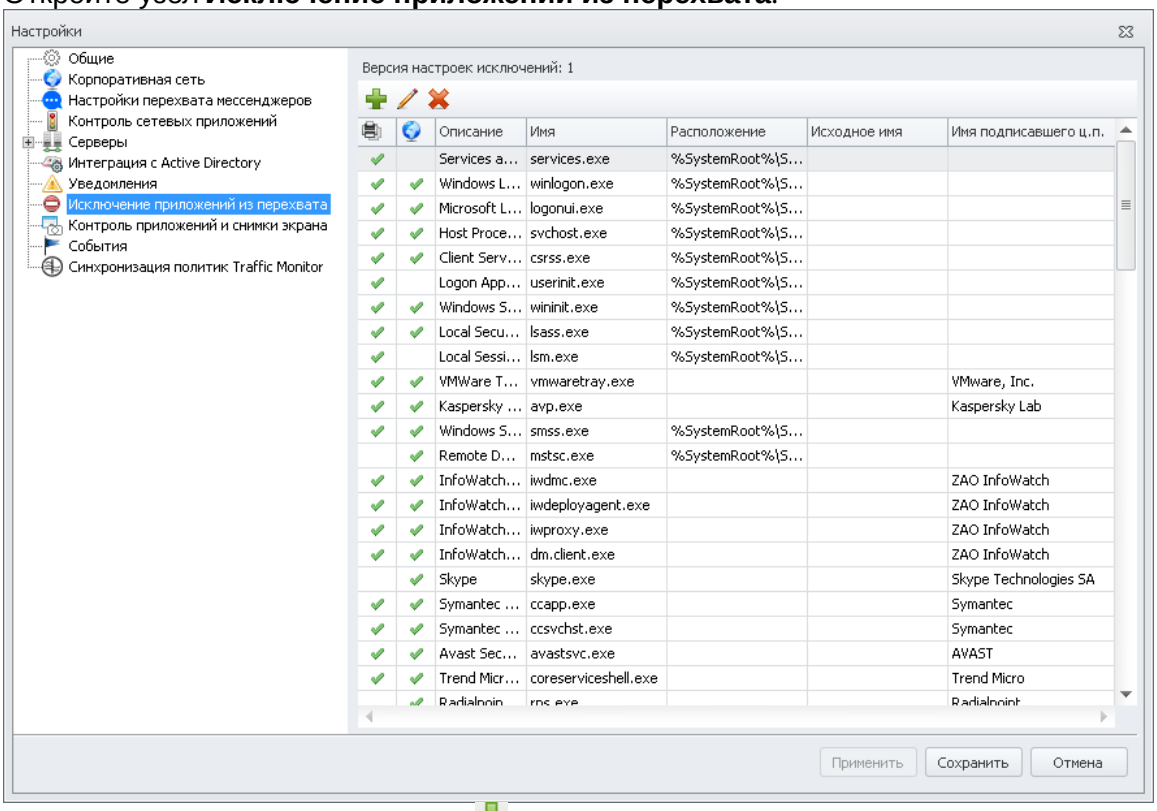
6.3.8 Исключение приложений из перехвата

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

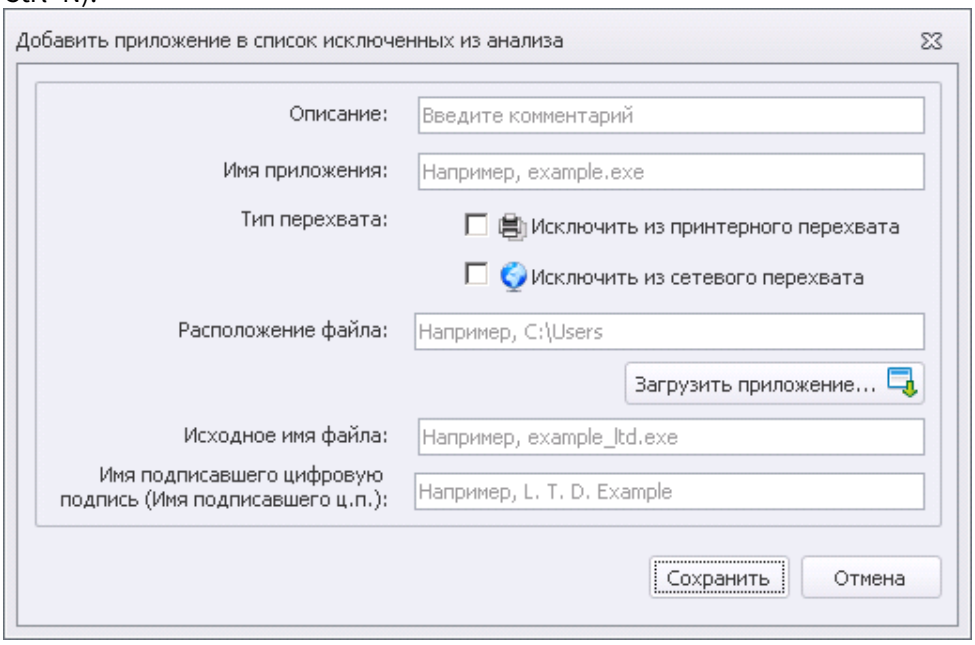
Чтобы просмотреть и настроить параметры исключения приложений из перехвата:

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

2. Откройте узел **Исключение приложений из перехвата**.



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



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

Примечание.

Вместо имени приложения можно ввести символ *. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути или имеющие указанную цифровую подпись (см. п. 7).

6. В поле **Тип перехвата** отметьте:
   - **Исключить из принтерного перехвата** - если требуется не создавать события и теневые копии при печати из данного приложения;
   - **Исключить из сетевого перехвата** - если требуется исключить сетевую активность приложения из перехвата (см. "Контроль сетевого трафика").

     Примечание.

     Должен быть выбран хотя бы один из типов перехвата.

7. Вы можете указать параметры файла приложения вручную либо автоматически:
   - Чтобы указать параметры файла приложения вручную:
     a. В поле **Расположение файла** укажите папку на Агенте, содержащую исполняемый файл приложения, либо папку верхнего уровня (возможно использование системных переменных). Заданная строка должна быть в начале пути к файлу. Например, если исключение задано в виде: «`*» + %ProgramFiles%\Citrix`, то из перехвата будут исключены все приложения в формате *.exe в папке Citrix, а также любой ее подпапке.
     b. В поле **Исходное имя файла** укажите название приложения (в контекстном меню исполняемого файла приложения выберите **Свойства**, вкладка **Подробно**, атрибут **Исходное имя файла**).
     c. В поле **Имя подписавшего цифровую подпись** (**Имя подписавшего ц.п.**) укажите значение из свойств исполняемого файла (в контекстном меню файла выберите **Свойства**, вкладка **Цифровые подписи**, атрибут **Имя подписавшего**). Можно указать имя целиком или часть имени. Например, если исключение задано в виде: «`*» + Kaspersky`, то из перехвата будут исключены все приложения, в цифровой подписи которых есть подстрока "Kaspersky".

     Примечание.

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

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

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

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

> **Примечание.**
>
> Программы со встроенной проверкой целостности (например, клиент SWIFT) или содержащие внутри себя антиотладочные методы необходимо добавлять в исключение из принтерного перехвата. В противном случае их запуск будет невозможен.

6.3.9 Контроль приложений и снимки экрана

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

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

О порядке формирования списков приложений см. "Приложения".

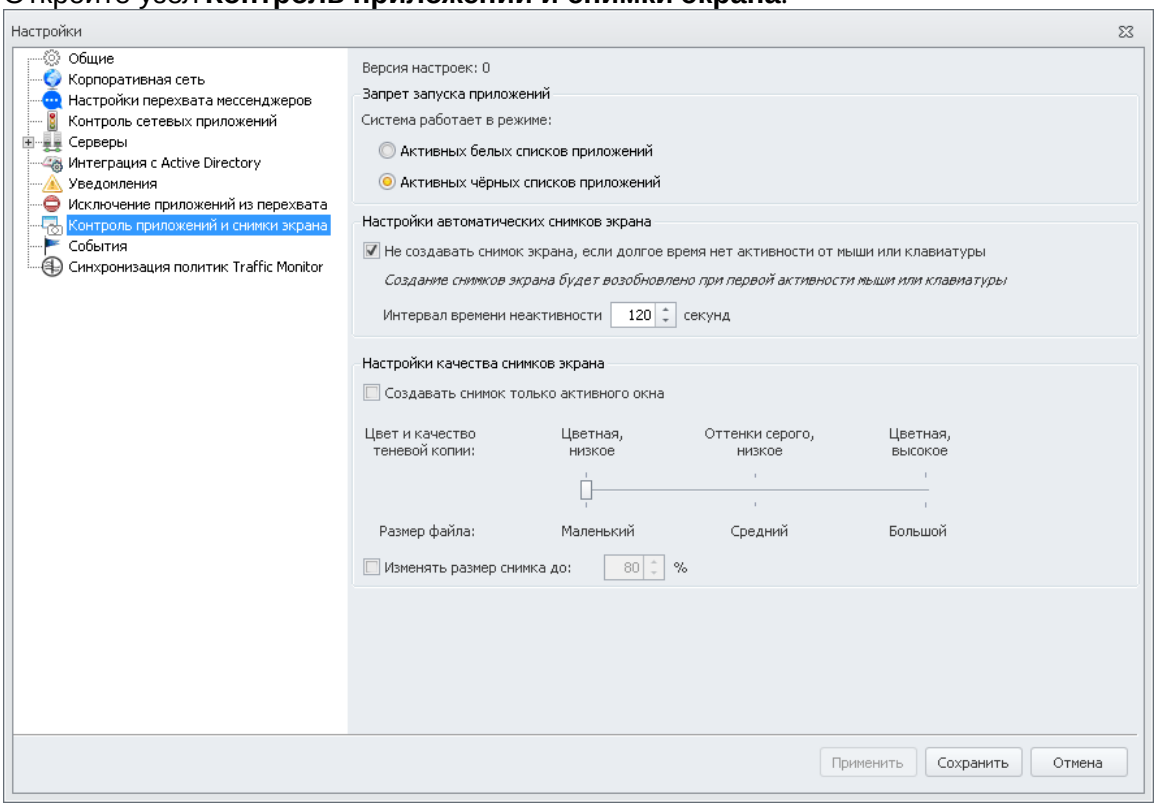
О порядке применения списков в правилах, регулирующих доступ к приложениям, см. "Правило (DM) для Application Monitor".

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

Чтобы выбрать режим работы Device Monitor с приложениями:

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

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



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

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

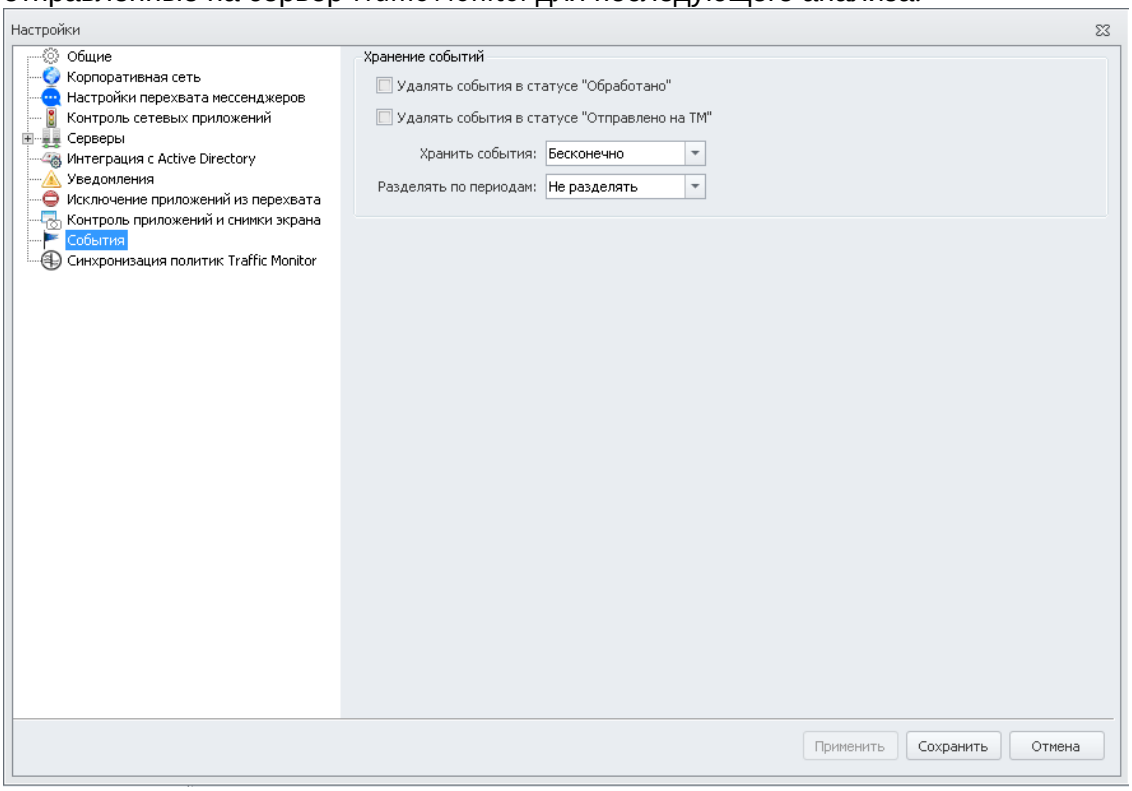
Новая версия настроек приложений и снимков экрана будет применена на контролируемых компьютерах после следующей их перезагрузки.

6.3.10 Хранение событий

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

Чтобы настроить хранение событий:

1. В главном меню выберите команду **Инструменты** > **Настройки**.
2. Откройте узел **События**.
3. Отметьте поля:
   - **Удалять события в статусе "Обработано"** - чтобы удалять отработанные события Device Monitor или события сервера, работающего в автономном режиме;
   - **Удалять события в статусе "Отправлено на ТМ"** - чтобы удалять события, отправленные на сервер Traffic Monitor для последующего анализа.



4. В раскрывающихся списках выберите:
   - **Хранить события** - для определения времени, которое событие будет находиться в базе данных и отображаться в консоли управления (DM), в том числе для событий со статусом **Ошибка отправки в ТМ** или **Нет лицензии**;
   - **Разделять по периодам** - разделение событий на блоки по времени создания для ускорения процессов обращения.

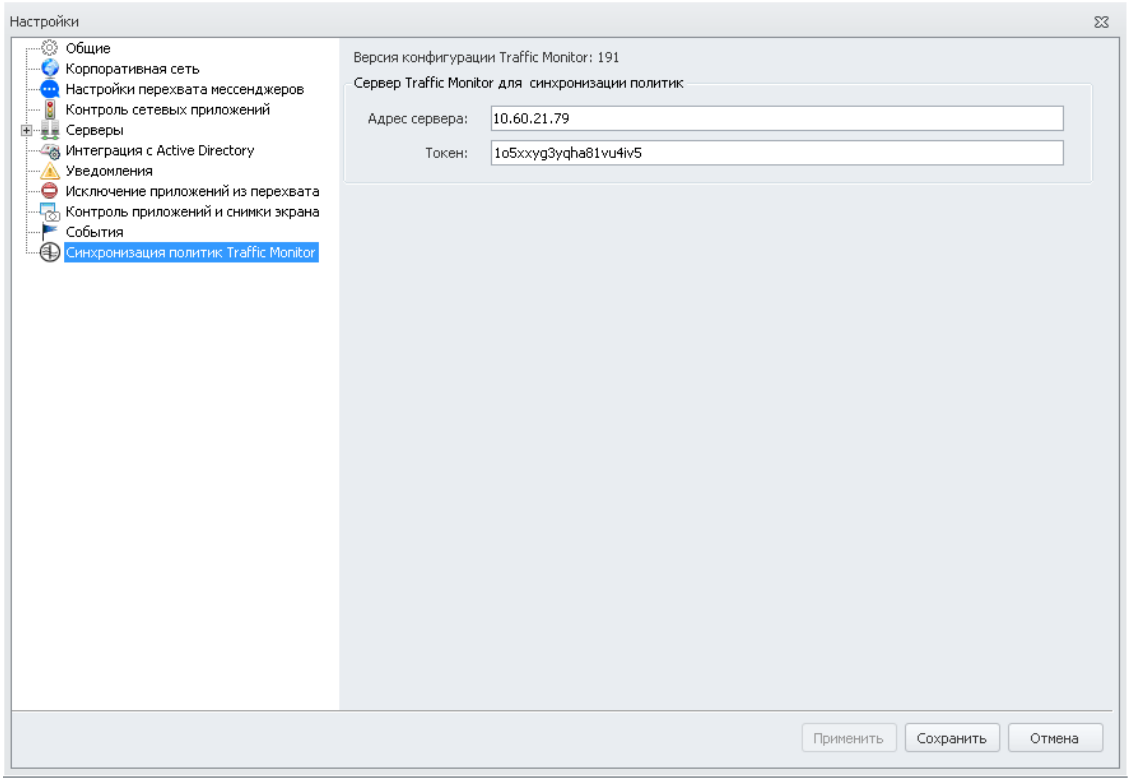
6.3.11 Синхронизация политик Traffic Monitor

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

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

Чтобы синхронизировать конфигурацию:

1. В главном меню Консоли (DM) управления выберите команду **Инструменты** > **Настройки**.
2. Откройте узел **Синхронизация политик Traffic Monitor**.
3. Убедитесь, что:
   a. адрес сервера (host) совпадает с установленными ранее настройками (см. "Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor").
   b. соединение устанавливается с сервером Traffic Monitor той же версии (см. "Особенности совместимости разных версий TM, DM и Агентов").



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

6.3.12 Работа с Менеджером управления серверами

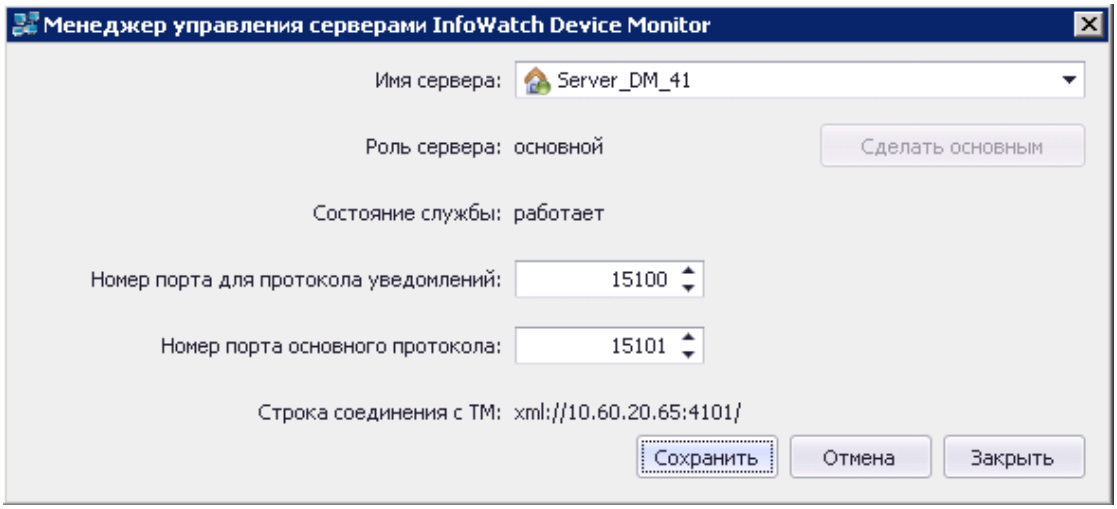
Для определения ролей и изменения некоторых настроек серверов, установленных в Системе, используется Менеджер управления серверами.

Важно!

Для работы утилиты "Менеджер управления серверами" требуется следующее:

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

Чтобы присвоить серверу роль Основной:

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

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

   Примечание.

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

4. Нажмите **Сохранить**.

5. Нажмите **Закрыть**.

Чтобы настроить порты сервера:

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

6.3.13 Остановка и запуск агента Device Monitor

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

Примечание.

Некоторые ограничения:

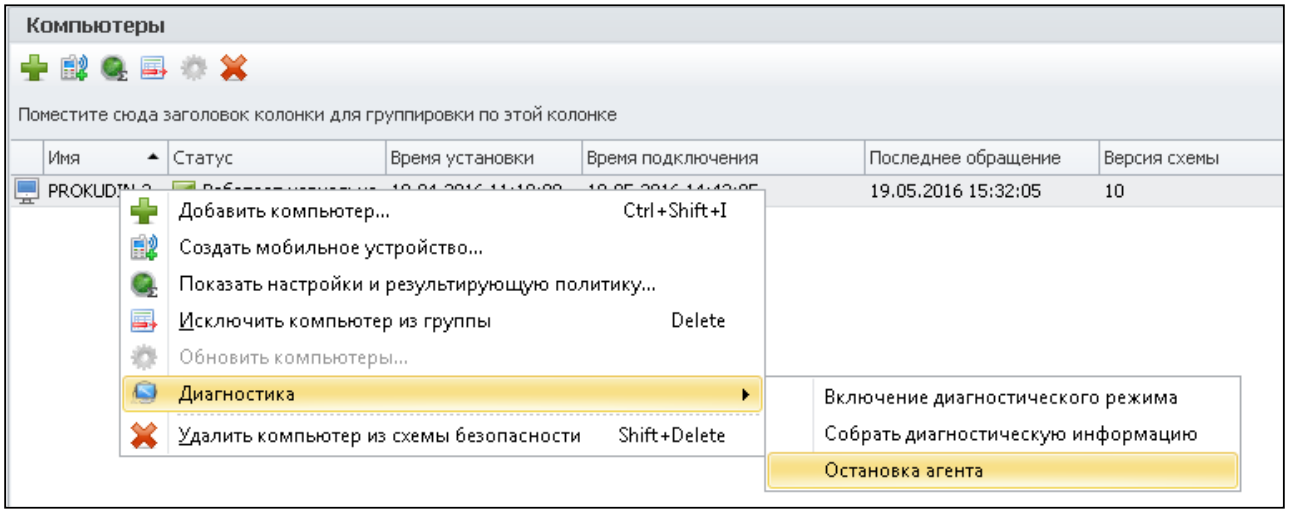
- При остановке агента DM модуль самозащиты агента не отключается.
- Во время сбора результатов логирования (логов) пункт контекстного меню **Диагностика** недоступен.
- Если остановленный агент был обновлен, то после завершения обновления он будет запущен.
- Если агент скрыт на рабочей станции, то он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

Важно!

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

Удаленная остановка/запуск агента

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



При выборе действия **Остановка агента** его работа будет приостановлена, а статус рабочей станции изменится на "Неактивна".

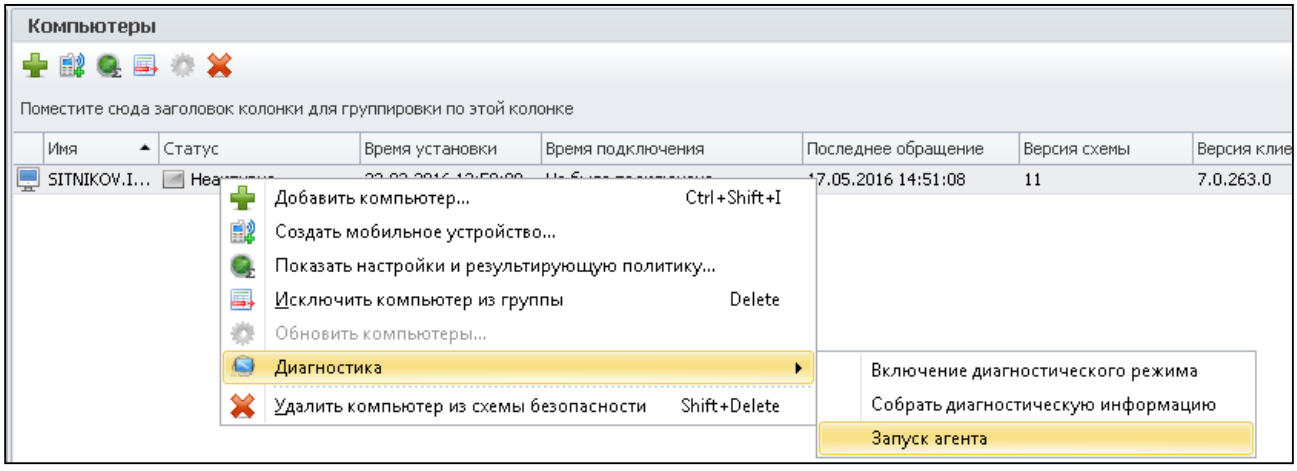
Примечание.

Остановленный агент доступен для обновления или удаления, но в процессе обновления/удаления агента остановка недоступна.
Если с агентом нет связи, то остановка/запуск недоступны.

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

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

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



При выборе действия **Запуск агента** его работа будет возобновлена, а статус рабочей станции изменится на "Работает нормально".

Локальная остановка/запуск агента

Локальная остановка/запуск агента осуществляется из командной строки Windows от имени администратора. Для этого необходимо запустить приложение **rmtdiag.exe**, указав полный путь к нему на рабочей станции (по умолчанию C:\Program Files\InfoWatch\DeviceMonitor\Client), с нужным параметром, Например:

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

> **Внимание!**
>
> Для остановки агента необходимо ввести пароль деинсталляции агента DM. Пароль вводится через пробел после ключа **/cld**. Для запуска агента пароль необязателен.
>
> Подробнее о пароле деинсталляции смотрите в статье "Создание задачи смены пароля деинсталляции".

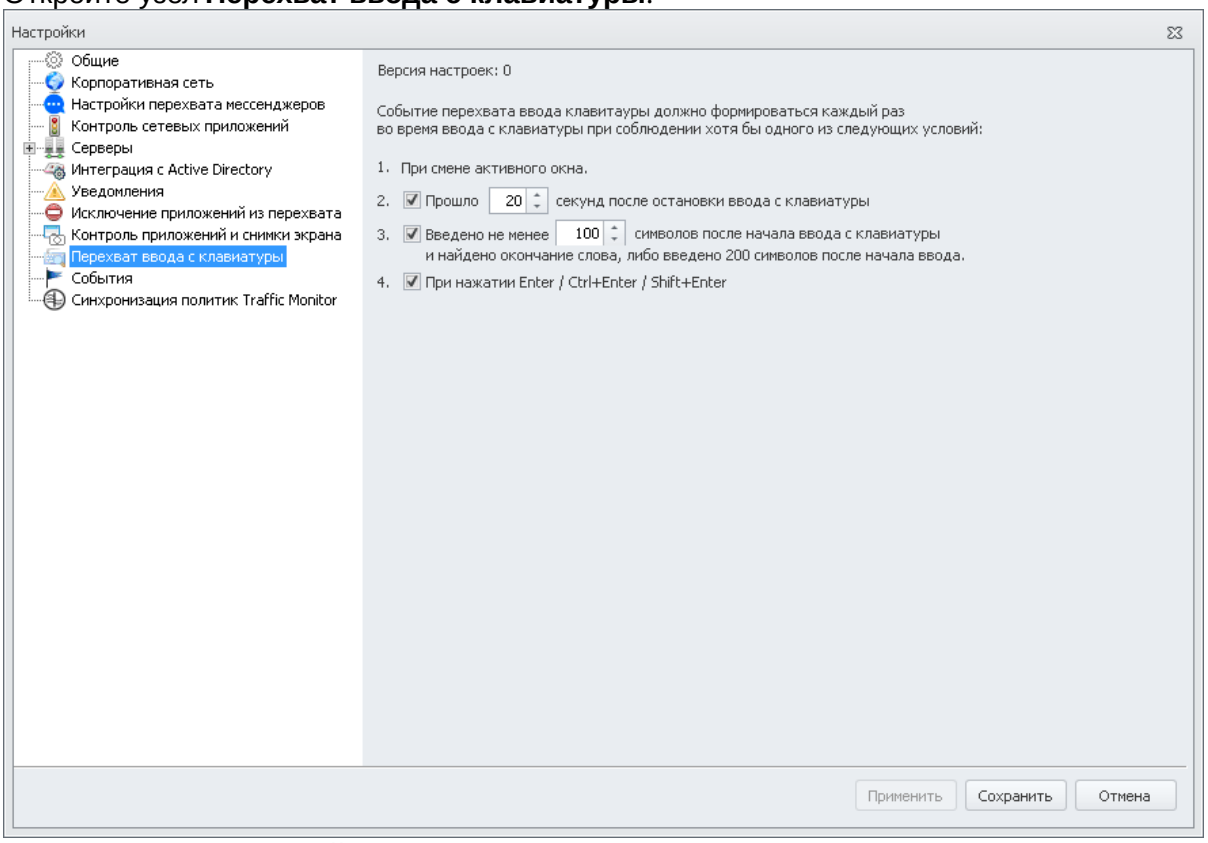
6.3.14 Контроль ввода с клавиатуры

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

Для этого:

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

2. Откройте узел **Перехват ввода с клавиатуры**.



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

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

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

6.4 Управление схемой безопасности

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

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

6.4.1 Организация схемы безопасности

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

В набор параметров схемы безопасности входят:

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

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

Остальные сущности Системы в схему безопасности не входят.

Схема безопасности может неоднократно редактироваться. Отредактированная схема безопасности будет сохранена как новая версия существующей схемы безопасности. Старые версии схемы безопасности при этом не удаляются, а хранятся в базе данных. При помощи Консоли управления (DM) вы можете просмотреть политики и содержащиеся в них правила любой версии схемы безопасности.

Далее в подразделе содержится следующая информация:

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

Политики безопасности и правила (DM)

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

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

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

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

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

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

> **Важно!**
>
> В случае многопользовательского доступа к рабочей станции и при невозможности определения инициатора процесса (события) правила перехвата для сотрудников учитываться не будут. Будут работать правила перехвата только для данной рабочей станции. В связи с этим необходима настройка правил перехвата не только для сотрудников, но и для рабочей станции, к которой возможен многопользовательский доступ.

Правила – это набор ограничений и условий, в соответствии с которыми осуществляется мониторинг операций, связанных с переносом файлов на съемные устройства и сетевые ресурсы, сетевой активностью и отправкой документов на печать, определяется уровень доступа к контролируемым периферийным устройствам. Для каждой политики безопасности (DM) создается свой набор правил (DM).

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

В InfoWatch Device Monitor существуют следующие типы правил:

- **Правило для Application Monitor**. Позволяет контролировать доступ сотрудников к приложениям при помощи черных и белых списков.
- **Правило для Clipboard Monitor**. Позволяет контролировать вставку данных из буфера обмена. Система позволяет запрещать вставку данных в приложения из списка либо все операции вставки данных в приложения терминальной сессии.
- **Правило для Cloud Storage Monitor**. Позволяет контролировать веб-клиенты облачных хранилищ.
- **Правило для Device Monitor**. Позволяет контролировать доступ сотрудников к выбранному типу периферийных устройств.
- **Правило для File Monitor**. Позволяет отслеживать следующие действия с файлами на съемных и сетевых ресурсах:

    - копирование файла на сетевые ресурсы с использованием UNC (например, *Server**SharedFolder**Folder**File*);
    - создание файла непосредственно на съемном устройстве;
    - копирование/перемещение файла на съемное устройство. В данном случае отслеживаются операции копирования/перемещения файла с контролируемого компьютера, другого съемного устройства или сетевых ресурсов.
- **Правило для FTP Monitor**. Позволяет контролировать обмен данными по протоколу FTP/FTPS. Система позволяет ограничивать или полностью запрещать использование FTP/FTPS протокола, а также создавать теневые копии передаваемых файлов.
- **Правило для HTTP(S) Monitor**. Позволяет контролировать обмен данными по протоколам HTTP и HTTPS. Система позволяет создавать теневые копии передаваемых файлов.
- **Правило для IM Client Monitor**. Позволяет контролировать доступ сотрудников к клиентам мгновенного обмена сообщениями и протоколам передачи данных: Skype, Telegram, XMPP, MMP, Facebook, Vkontakte. Система позволяет полностью запрещать использование приложения, либо только снимать копию чата (для Skype также возможно делать запись голосовых сообщений). Также возможно создавать теневые копии передаваемых файлов и сообщений.
- **Правило для Mail Monitor**. Позволяет контролировать отправку и получение электронной почты. Система позволяет полностью запрещать или разрешать использование почты почты, либо разрешать только получение почты, а также создавать теневые копии передаваемых файлов.
- **Правило для Network Monitor**. Позволяет запрещать передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами. Вы можете указать, какие сегменты сети считаются корпоративной сетью и какие внешние адреса разрешены.
- **Правило для Print Monitor**. Позволяет отслеживать действия, связанные с печатью документов на локальных и сетевых принтерах. Также возможно создавать теневую копию задания на печать.
- **Правило для ScreenShot Monitor**. Позволяет автоматически создавать снимки экрана на контролируемых компьютерах.
- **Правило для ScreenShot Control Monitor**. Позволяет осуществлять контроль снимков экрана со стороны агента.

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

Сотрудники и группы сотрудников

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

- Каждый сотрудник должен входить как минимум в одну группу сотрудников (группу «по умолчанию»). Это связано с тем, что политика безопасности (DM) не может быть назначена отдельному сотруднику.
  В группу «по умолчанию» входят учетные записи всех сотрудников, для которых не определены другие группы сотрудников (сотрудники, впервые зарегистрированные в Device Monitor; сотрудники, исключенные из всех прочих групп сотрудников).
  Исключить сотрудника из группы «по умолчанию» можно при условии, что учетная

запись сотрудника добавлена хотя бы в одну группу сотрудников, помимо группы «по умолчанию».

- После установки Системы группе сотрудников «по умолчанию» назначена *Политика теневого копирования*, содержащая следующие правила (DM):
  - **Теневое копирование документов**. Правило File Monitor, задающее создание теневых копий всех файлов, записываемых на съемные устройства и копируемых на сетевые ресурсы.
  - **Теневое копирование печати**. Правило Print Monitor, задающее создание теневых копий всех заданий на печать.
  - **Контроль Skype, Контроль Telegram, Контроль XMPP, Контроль MMP**. Правила IM Client Monitor, разрешающее использование соответствующих мессенджеров, но задающее создание теневых копий для всех сообщений и чатов, а также исходящих файлов.
  - **Контроль FTP**. Правило FTP Monitor, разрешающее использование протокола FTP/FTPS, но задающее создание теневых копий для всех файлов, отправляемых с использованием этого протокола.
  - **Контроль HTTPS**. Правило HTTP(S) Monitor, создающее событие для пост-запросов всегда, вне зависимости от их размера, если передача производится по зашифрованному каналу. Теневая копия создается, если размер запроса, передаваемого по зашифрованному каналу, находится в диапазоне от 40 байт до 40 Мбайт.
  - **Контроль системы передачи почтовых сообщений**. Правило Mail Monitor, разрешающее отправку и получение почты и задающее создание теневых копий для исходящих по зашифрованному каналу писем, если их размер не превышает 40 МБайт.

Компьютеры и группы компьютеров

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

> **Примечание:**
>
> В поле **Пользователь**, на вкладке **Группы компьютеров**, отображается имя пользователя, который последним заходил на компьютер.

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

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

Загрузка схемы безопасности на контролируемые компьютеры

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

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

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

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

6.4.2 Общие действия при управлении схемой безопасности

Информация по работе со схемой безопасности содержится в следующих подразделах:

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

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

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

Просмотр действующей версии схемы безопасности

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

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

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

Пиктограмма	Группа элементов
	Группа компьютеров «по умолчанию»
	Группа компьютеров
	Группа сотрудников «по умолчанию»
	Группа сотрудников
	Категория сигнатур «по умолчанию»
	Категория сигнатур

	Белый список устройств для сотрудника
	Белый список устройств для группы сотрудников
	Белый список устройств для компьютера
	Белый список устройств для группы компьютеров
	Фильтр в журнале аудита
	Политика безопасности

Чтобы просмотреть информацию по определенному разделу схемы безопасности:

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

Примечание.

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

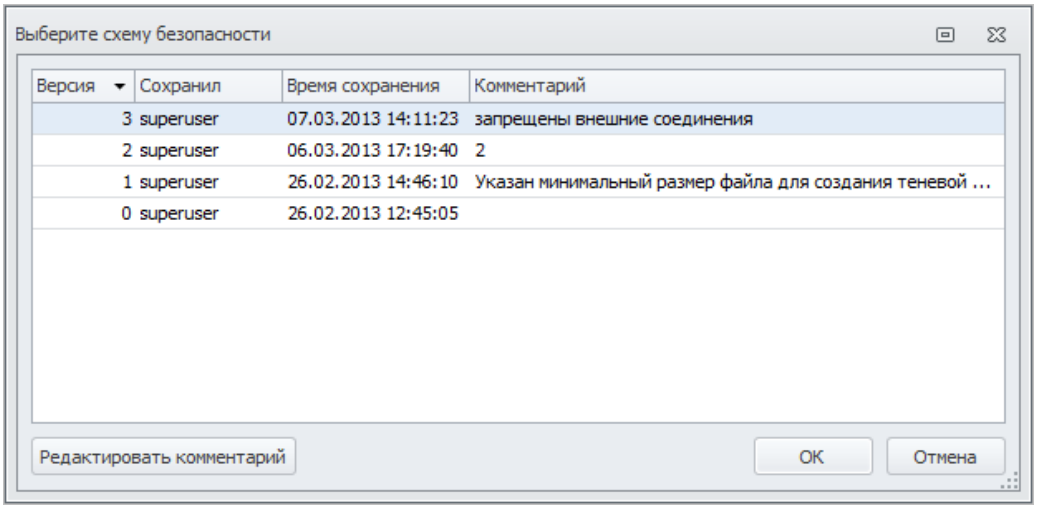
Просмотр предыдущих версий схемы безопасности

Примечание.

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

Чтобы просмотреть раннюю версию схемы безопасности:

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



По каждой версии выводится следующая информация:

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

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

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

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

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

Комментарии к схеме безопасности

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

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

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

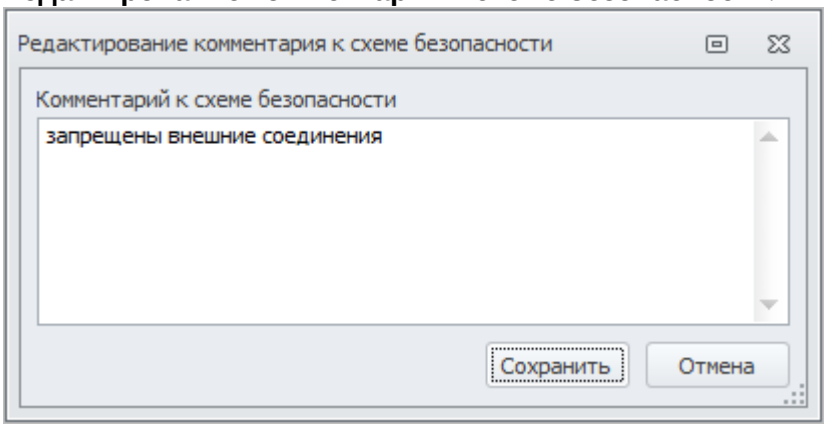
Примечание:

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

Чтобы добавить/отредактировать комментарий к схеме безопасности:

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

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



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

Редактирование схемы безопасности

Важно!

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

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

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

Чтобы отредактировать схему безопасности:

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

     Примечание:

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

2. Отредактируйте необходимые параметры схемы безопасности:
   - политики безопасности (см. "Политики безопасности (DM)");
   - группы компьютеров (см. "Компьютеры");
   - группы учетных записей сотрудников (см. "Сотрудники");
   - белые списки устройств (см "Белые списки")
   - категории сигнатур файлов (см. "Категории сигнатур").
3. После того как все необходимые изменения будут сделаны, сохраните схему безопасности. Для этого выполните одно из следующих действий:
   - в верхней строке рабочей области, где отображается сообщение "*В схему безопасности были внесены изменения...*" нажмите **Сохранить**;
   - в главном меню выберите команду **Схема безопасности** > **Сохранить**;
   - воспользуйтесь кнопкой **Сохранить**, расположенной на панели инструментов.
     В результате выполнения любого из этих действий все изменения будут сохранены, и схема безопасности будет выведена из режима редактирования.

Примечание:

Чтобы отменить внесенные изменения:

- в верхней строке рабочей области, где отображается сообщение "*В схему безопасности были внесены изменения...*" нажмите **Отмена**;

- в главном меню выберите команду **Схема безопасности** > **Отменить редактирование**;
- воспользуйтесь кнопкой **Отменить редактирование**, расположенной на панели инструментов.

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

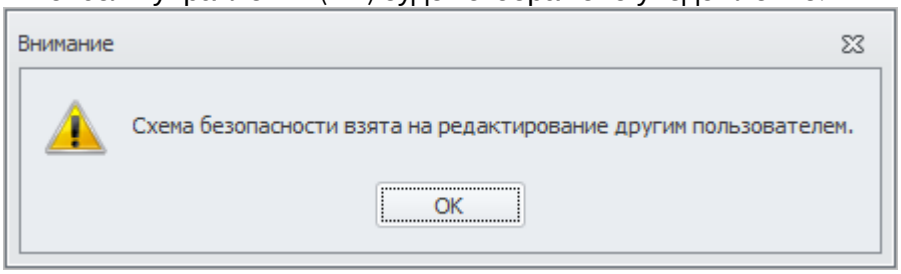
Ожидание окончания редактирования. Разблокирование схемы безопасности

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

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

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

1. В Консоли управления (DM) будет отображено уведомление.



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

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

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

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

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

Важно!

Разблокировать схему безопасности может только Суперпользователь.

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

При этом все несохраненные изменения схемы безопасности будут утеряны.

Обновление схемы безопасности

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

Необходимость в обновлении схемы безопасности может потребоваться в следующих случаях:

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

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

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

Экспорт/импорт конфигурации

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

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

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

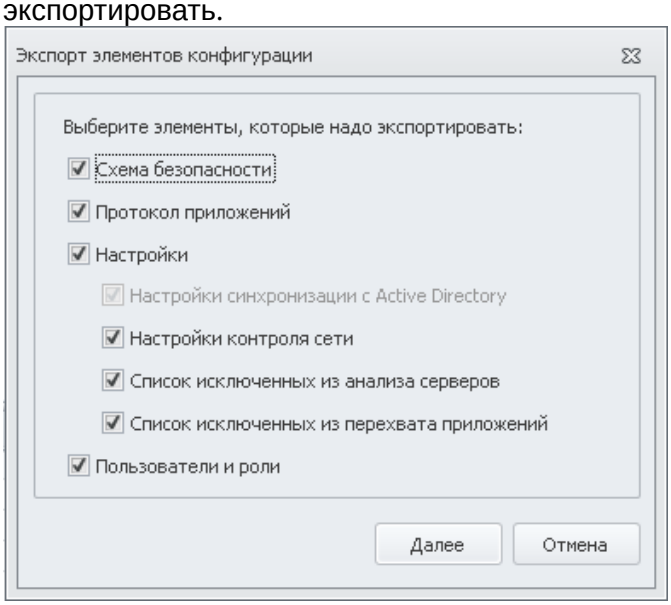
> **Важно!**
>
> В Систему версии 6.11 можно импортировать файл конфигурации только данной версии.

Впоследствии сохраненные настройки могут быть импортированы в новую схему безопасности.

Чтобы экспортировать конфигурацию Системы:

1. В главном меню выберите команду **Инструменты** > **Экспорт конфигурации**.

2. В открывшемся диалоговом окне отметьте элементы конфигурации, которые вы хотите экспортировать.

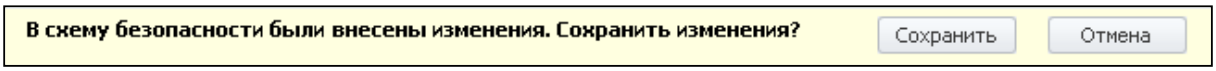


3. Нажмите **Далее**.
4. В окне сохранения файла задайте имя файла, в который будут экспортированы данные, и выберите каталог для его хранения. Нажмите **Сохранить**.

> **Важно!**
>
> Для корректной связки ролей и групп необходимо экспортировать роли и схему безопасности.

Чтобы импортировать схему безопасности:

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



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

6.4.3 Настройка схемы безопасности

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

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

При настройке конфигурационных параметров нужно придерживаться следующих принципов:

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

Особенности добавления компьютеров в схему безопасности

Добавление контролируемых компьютеров происходит одним из двух способов:

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

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

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

Особенности добавления учетных записей сотрудников в схему безопасности

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

Особенности добавления белых списков в схему безопасности

Перед созданием белого списка необходимо внести в базу устройств данные о включаемых в него моделях и экземплярах устройств. Затем нужно создать белый список для конкретного сотрудника / группы сотрудников / компьютера / группы компьютеров, и определить, какие устройства в него включены. Для этих сотрудников / компьютеров доступ к моделям и экземплярам устройств из белого списка разрешен, невзирая на назначенные политики (DM). По окончании периода действия записи в белом списке, доступ к устройству производится согласно назначенным политикам (DM).

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

- Политики безопасности (DM)
- Правила (DM)
- Сотрудники
- Компьютеры
- Белые списки
- Категории сигнатур
- Приложения
- Временный доступ сотрудника к сети
- Временный доступ сотрудника к устройствам

Политики безопасности (DM)

На агентах Device Monitor политики применяются в следующем порядке:

1. Запрещающие политики (DM).

2. Политики защиты данных на агентах, созданные в TM.
3. Политика теневого копирования (DM).

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

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

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

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

Информация по работе с политиками безопасности (DM) содержится в подразделах:

- Просмотр политик безопасности (DM)
- Создание и настройка политики безопасности (DM)
- Редактирование политики безопасности (DM)
- Удаление политики безопасности (DM)

Просмотр политик безопасности (DM)

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

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

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

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

Расширенная информация по каждому правилу (DM) выводится на панели **Подробно**.

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

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

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

Общие сведения:

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

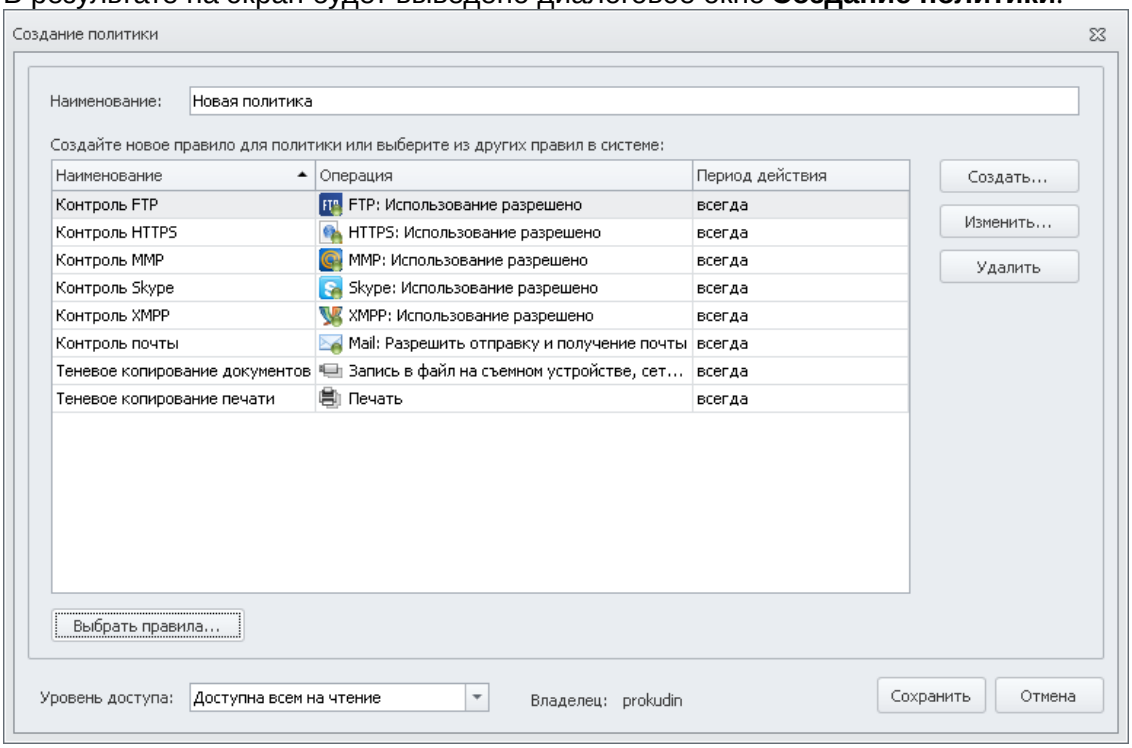
> **Примечание.**
>
> Информация по некоторым свойствам дублируется в рабочей области главного окна.

Создание и настройка политики безопасности (DM)

Чтобы создать и настроить политику безопасности:

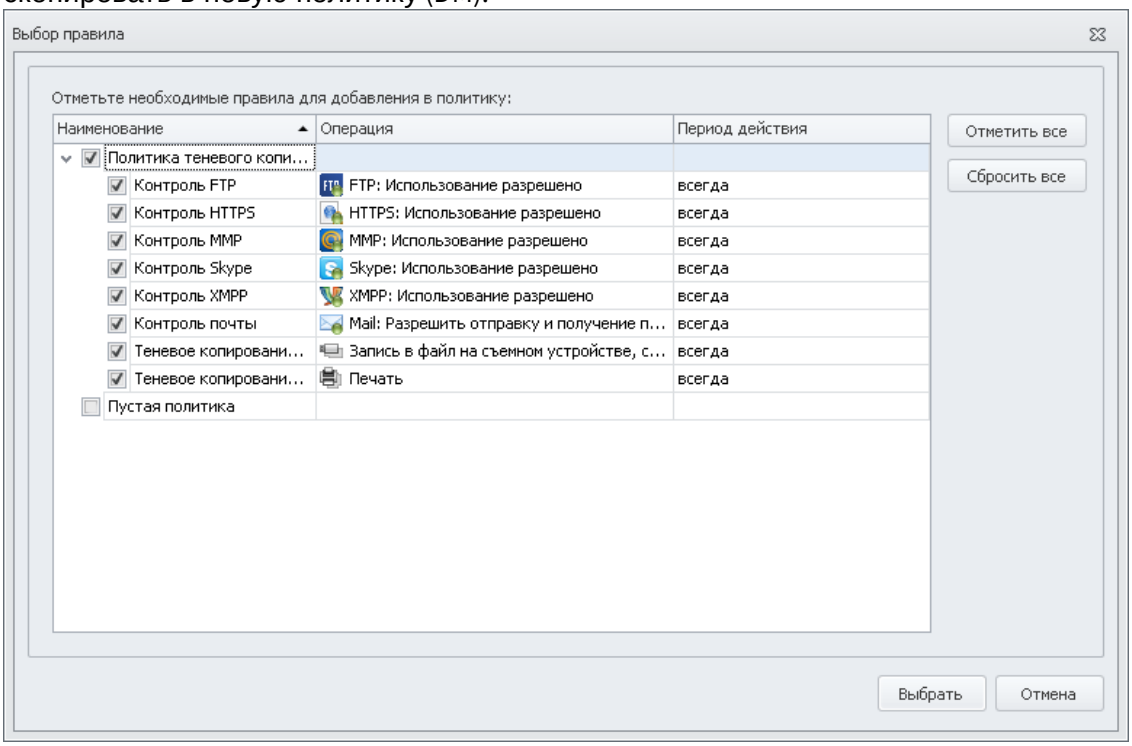
1. Перейдите к разделу **Политики**.
2. Выполните одно из следующих действий:
   - воспользуйтесь кнопкой **Создать политику**, расположенной в верхней части Панели навигации;
   - в главном меню выберите команду **Правка** > **Создание политики**;
   - на клавиатуре нажмите сочетание клавиш **Ctrl+N**.

   В результате на экран будет выведено диалоговое окно **Создание политики**.



3. В поле **Наименование политики** укажите название новой политики безопасности (DM).

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



     Вы можете также отметить целиком политику (DM) - в этом случае все правила (DM), в ней содержащиеся, будут скопированы в новую политику (DM).
     После того, как вы отметите все необходимые правила, нажмите **Выбрать**.
   - Чтобы создать новое правило (DM), нажмите **Создать** и задайте параметры правила как описано в одном из следующих разделов:
     - Правило (DM) для Application Monitor;
     - Правило (DM) для Cloud Storage Monitor;
     - Правило (DM) для Clipboard Monitor;
     - Правило (DM) для Device Monitor;
     - Правило (DM) для File Monitor;
     - Правило (DM) для FTP Monitor;
     - Правило (DM) для HTTP(S) Monitor;
     - Правило (DM) для IM Client Monitor;
     - Правило (DM) для Mail Monitor;
     - Правило (DM) для Network Monitor;
     - Правило (DM) для Print Monitor;
     - Настройка правила (DM) для ScreenShot Control Monitor;
     - Правило (DM) для ScreenShot Monitor.

     Вы также можете отредактировать или удалить правило (DM) из политики (DM), выбрав необходимое правило (DM) и нажав **Изменить** или **Удалить** соответственно.
5. В выпадающем списке **Уровень доступа** задайте права на чтение и редактирование политики.

6. После того, как вы определите все правила (DM), которые должны входить в политику (DM), и назначите права, нажмите **Сохранить**.

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

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

Редактирование политики безопасности (DM)

Чтобы отредактировать политику безопасности:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выберите название нужной политики безопасности (DM).
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить**;
   - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации;
   - на клавиатуре нажмите сочетание клавиш **Ctrl+E**;
   - дважды щелкните левой кнопкой мыши по названию выделенной политики безопасности (DM);
   - щелкните по названию политики правой кнопкой и в контекстном меню выберите **Изменить**.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно **Редактирование политики**.
4. Именование политики безопасности (DM) и определение правил (DM), входящих в нее, производится аналогично созданию политики (DM): см. "Создание и настройка политики безопасности (DM)", шаги 3-4.
5. Нажмите **Сохранить**.

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

Удаление политики безопасности (DM)

> **Важно!**
>
> Политику (DM), назначенную хотя бы одной группе сотрудников или группе компьютеров, невозможно удалить. Чтобы удалить политику (DM), убедитесь, что всем группам сотрудников

(см. "Просмотр сведений о сотрудниках и группах сотрудников") и компьютеров (см. "Просмотр сведений о компьютерах") не назначена удаляемая политика (DM).

Чтобы удалить политику безопасности:

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

Важно!

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

Правила (DM)

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

Информация по работе с правилами (DM) содержится в подразделах:

- Применение правил (DM);
- Создание правил (DM).

Применение правил (DM)

Событие считается удовлетворяющим правилу (DM), если оно соответствует всем параметрам, указанным в правиле.

Если событие соответствует нескольким правилам (DM) одновременно, то приоритет определяется следующим образом:

1. Правило (DM), исключающее из перехвата (опция **Исключить из перехвата** доступна для правила File Monitor), имеет наивысший приоритет.
2. Правило полного доступа (DM) имеет приоритет перед запрещающим, в то время как запрещающее правило имеет приоритет перед разрешающим только чтение и доступ на зашифрованные носители.
   Пример 1. Для Device Monitor правило (DM) *Использование разрешено* имеет приоритет над ограничением *Нет доступа*, которое в свою очередь имеет приоритет по сравнению с правилом (DM), разрешающим *Только чтение*, а оно, соответственно, более приоритетно чем правило (DM), где выбран *Полный доступ только к зашифрованным устройствам*.
   Пример 2. Если задано несколько правил HTTP(S) Monitor, то правило с включенной

опцией *Не перехватывать запросы на внутренние ресурсы* имеет больший приоритет, чем правило, для которого данная опция не выбрана.

3. Правило (DM), в котором отмечена опция **Создавать теневую копию**, имеет приоритет перед правилом без теневой копии.

См. также:

- Особенности применения правил для Device Monitor
- Создание теневых копий и запрет операций при нехватке свободного места

Особенности применения правил для Device Monitor

Доступ ко всем периферийным устройствам, контролируемым перехватчиком Device Monitor, определяется совокупностью правил (DM), назначенных каждому из этих устройств.

При определении прав доступа сотрудника к какому-либо устройству учитываются:

- правила (DM), распространяющиеся на группы сотрудников, в которые входит сотрудник;
- правила (DM), распространяющиеся на группы компьютеров, в состав которых включен компьютер, используемый для доступа к устройству;
- белые списки.

При установке Агента доступ к контролируемым устройствам по умолчанию разрешен. Поэтому каждая запрещенная операция для устройства должна быть задана явно в виде правила.

Каждый новый зарегистрированный компьютер попадает в группу компьютеров по умолчанию. Этой группе назначена *Политика на устройства* (DM), не содержащая ни одного правила (DM). Для сотрудников по умолчанию правила (DM) работы с устройствами не определены.

Таким образом, после установки доступ ко всем контролируемым устройствам по умолчанию разрешен.

Пример:

> Для группы компьютеров *A* задано правило (DM), запрещающее запись CD/DVD дисков. Сотрудник входит только в группу сотрудников *B*, для которой не определены правила (DM) работы с устройствами, а его компьютер входит в группу компьютеров *A*. Сотрудник пытается просмотреть содержимое компакт-диска на своем компьютере. В этом случае сотрудник не сможет просматривать содержимое диска и записывать новую информацию на диск.

Вы можете назначить с помощью Консоли управления (DM) несколько правил (DM), в том числе и в разных политиках (DM), с разным уровнем доступа на одно и то же устройство. В этом случае более приоритетным будет разрешающее правило (подробнее см. таблицу ниже).

Тип устройства	Доступ в порядке убывания приоритета
Все устройства, кроме CD/DVD, Floppy и съемных устройств хранения	1. Использование разрешено 2. Использование запрещено
CD/DVD	1. Использование разрешено 2. Нет доступа 3. Только чтение

Floppy и съемные устройства хранения	1. Использование разрешено 2. Нет доступа 3. Только чтение 4. Полный доступ только к зашифрованным устройствам

Пример:

> Для группы сотрудников *E* действует правило (DM), предоставляющее доступ к съемному устройству хранения только для чтения. Для группы сотрудников *F* действует правило (DM), разрешающее полный доступ только к зашифрованному съемному устройству хранения. Сотрудник *Иванов*, входящий в обе группы, сможет получить доступ к съемным устройствам только на чтение: причем как к зашифрованным, так и к незашифрованным, так как правило с меньшим приоритетом не учитывается.

Для некоторых типов устройств, контролируемых перехватчиком Device Monitor, правила могут пересекаться (см. таблицу ниже). Это нужно учитывать при настройке доступа к контролируемому устройству.

Правило (DM)	Пересекающиеся правила	Примечание
Флоппи-дисковод	Нет	
CD/DVD	Нет	
Параллельный порт (LPT)	Локальный принтер (LPT) Устройства работы с изображениями (LPT)	При запрете на использование LPT-порта взаимодействие с устройством, подключенным к этому порту, будет невозможно
Последовательный порт (COM)	Модем Локальный принтер (COM) Устройства работы с изображениями (COM)	Доступ к модему, подключенному через COM-порт, определяется только правилом использования COM-порта При запрете на использование COM-порта взаимодействие с устройством, подключенным к этому порту, будет невозможно
Съемное устройство хранения (устройства, подключаемые через интерфейсы USB, IEEE 1394)	FireWire (IEEE 1394)	При запрете на использование порта FireWire (IEEE 1394) взаимодействие с подключенным к порту устройством становится невозможным
Локальный принтер (подключаемый через интерфейс USB, IEEE 1394, SCSI и пр.)	FireWire (IEEE 1394) Последовательный порт (COM) Параллельный порт (LPT)	При запрете на использование порта FireWire (IEEE 1394), COM, LPT взаимодействие с подключенным к этому порту устройством становится невозможным

Устройства работы с изображениями (видеокамеры, сканеры)	FireWire (IEEE 1394) Последовательный порт (COM) Параллельный порт (LPT)	При запрете на использование FireWire (IEEE 1394), COM, LPT порта взаимодействие с устройством, подключенным к этому порту, будет невозможно
Bluetooth устройство	Нет	
IrDA устройство	Нет	
Другое USB устройство	Нет	
FireWire	Съемное устройство хранения (IEEE 1394) Локальный принтер (IEEE 1394) Устройства работы с изображениями (IEEE 1394)	При запрете на использование порта FireWire (IEEE 1394) взаимодействие с устройством, подключенным к этому порту, будет невозможно
Модем	Последовательный порт (COM)	Правила (DM), определяющие доступ к модему, не распространяются на модемы, подключаемые через COM-порт. Возможность доступа к модему, подключенному через COM-порт, определяется только правилами использования COM-порта
Считыватель смарт-карт (Smart Card Reader)	Нет	
Ленточный накопитель	Нет	
Многофункциональное устройство	Нет	
PCMCI устройство	Нет	
Сетевой адаптер USB	MTP совместимое устройство	Мобильный телефон при подключении к компьютеру может быть определен как MTP-устройство или как сетевой адаптер USB
Сетевой принтер	Нет	
КПК (карманные компьютеры под управлением операционных систем Windows Mobile и Palm OS)	Нет	

MTP совместимое устройство	Сетевой адаптер USB	Мобильный телефон при подключении к компьютеру может быть определен как MTP-устройство или как сетевой адаптер USB

Создание теневых копий и запрет операций при нехватке свободного места

Теневая копия файла, документа, сообщения или чата создается в случае, если выполнены следующие условия:

1. В правиле (DM), под действие которого попадает файл, установлена отметка о создании теневой копии, и размер файла входит в диапазон, указанный в правиле.
2. На контролируемом компьютере имеется больше свободного места, чем указано в значении параметра **Минимальное свободное пространство на агенте** (см. "Общие настройки работы Агентов"). Значение по умолчанию - 10%.
3. На контролируемом компьютере больше свободного места, чем необходимо для создания теневой копии.

Примечание:

Если в правиле (DM) задано создание теневой копии, но на компьютере осталось меньше свободного места, чем определено политикой (DM) или чем требуется для сохранения файла, то событие будет создано без теневой копии. Для таких событий в Консоли управления (DM) отображается состояние "*Ошибка создания копии*" (см. "Просмотр событий").

Важно!

Не создаются теневые копии печати размером более 512 Мб.

Помимо теневых копий, на компьютере временно (до установления соединения с сервером Device Monitor) сохраняется информация о событиях. Для этого на диске компьютера, где установлен Агент Device Monitor, выделяется место, достаточное для хранения информации о 30000 событиях (около 300 Мб).

Если:

- Агент Device Monitor долго не имел связи с сервером Device Monitor, в результате чего накопилось более 30000 событий, и
- в общих настройках работы Агентов для параметра **Если место под события на диске закончилось** установлено значение **Запрещать операции**,

то любые действия сотрудника, контролируемые текущей политикой безопасности (DM), будут запрещены.

Создание правил (DM)

Чтобы добавить в политику новое правило:

1. Перейдите к разделу **Политики**.
2. В области **Политики** на Панели навигации выберите политику безопасности (DM), в которую вы хотите добавить правило.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Создать правило**;

- воспользуйтесь кнопкой **Создать правило**, расположенной в верхней части области **Политики** ;
- в области **Правила** нажмите правой кнопкой мыши и из раскрывшегося списка выберите **Создать правило**;
- нажмите сочетание клавиш **Ctrl+Shift+N**.

4. В открывшемся диалогом окне выберите тип правила и укажите остальные параметры правила (DM). Доступные типы правил:
   - Правило (DM) для Application Monitor
   - Правило (DM) для Clipboard Monitor
   - Правило (DM) для Cloud Storage Monitor
   - Правило (DM) для Device Monitor
   - Правило (DM) для File Monitor
   - Правило (DM) для FTP Monitor
   - Правило (DM) для HTTP(S) Monitor
   - Правило (DM) для IM Client Monitor
   - Правило (DM) для Mail Monitor
   - Правило (DM) для Network Monitor
   - Правило (DM) для Print Monitor
   - Правило (DM) для ScreenShot Control Monitor
   - Правило (DM) для ScreenShot Monitor
5. После того как вы указали все необходимые параметры, нажмите **Сохранить**.

Чтобы отредактировать правило:

1. В списке правил политики выберите правило, которое вы хотите изменить.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить правило**;
   - дважды щелкните левой кнопкой мыши по выделенной строке;
   - щелкните по выделенной строке правой кнопкой мыши и в контекстном меню выберите **Изменить правило**;
   - воспользуйтесь кнопкой **Изменить правило**, расположенной в верхней части области **Политики**;
   - на клавиатуре нажмите сочетание клавиш **Ctrl+Shift+E**.
3. В открывшемся диалогом окне внесите необходимые изменения, после чего нажмите **Сохранить**.

Чтобы удалить правило:

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

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

2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить правило**;
   - воспользуйтесь кнопкой **Удалить правило**, расположенной в верхней части области **Политики**;

- щелкните по строке правила правой клавишей мыши и в контекстном меню выберите **Удалить правило**;
- нажмите клавишу **Delete**.

3. В окне подтверждения нажмите **Да**.

Чтобы скопировать правило:

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

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

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

Важно!

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

Правило (DM) для Application Monitor

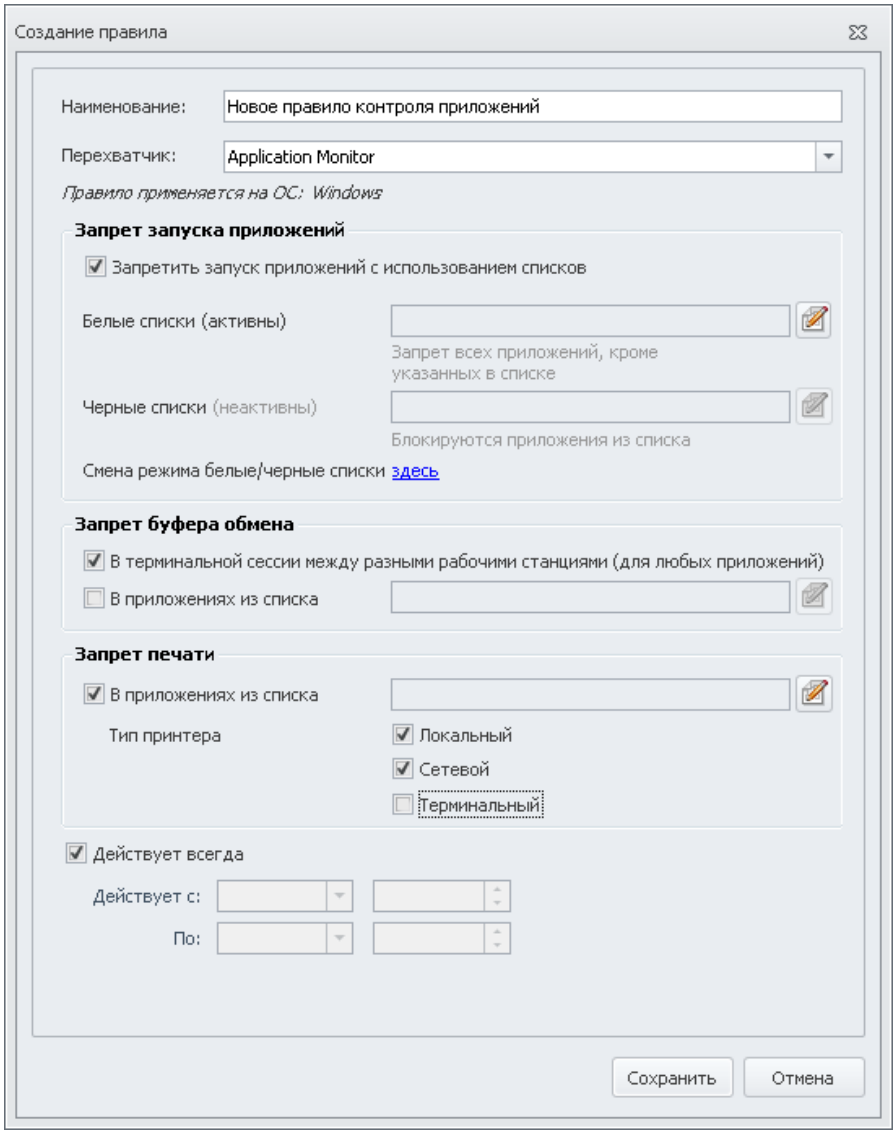
Через сторонние приложения, установленные на рабочей станции и не контролируемые InfoWatch Device Monitor, сотрудник может совершить действия, приводящие к утечке конфиденциальной информации.
Перехватчик Application Monitor позволяет контролировать доступ сотрудников к приложениям при помощи наложения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

- запуск приложений;
- буфер обмена;
- печать.

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

Примечание:

Правило применяется на компьютерах под управлением операционной системы MS Windows.

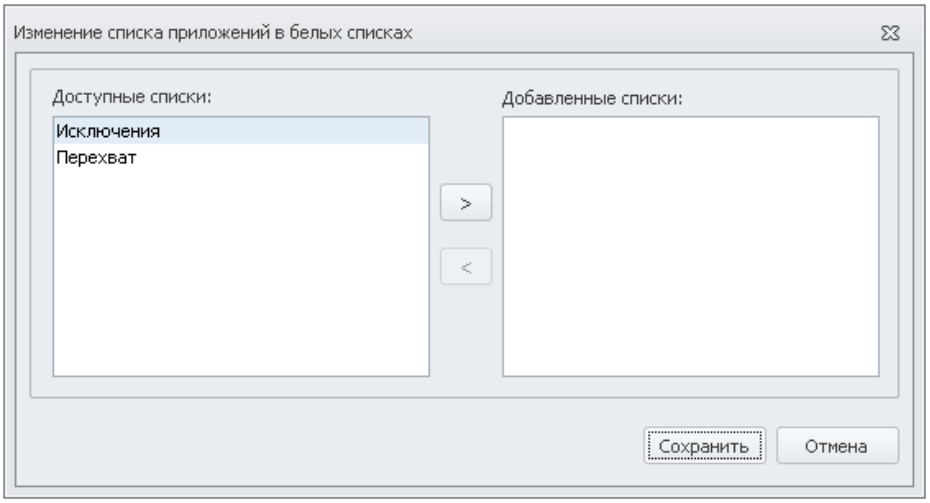


Чтобы настроить правило:

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

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

4. Добавьте белые или черные списки приложений нажатием кнопки .



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

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

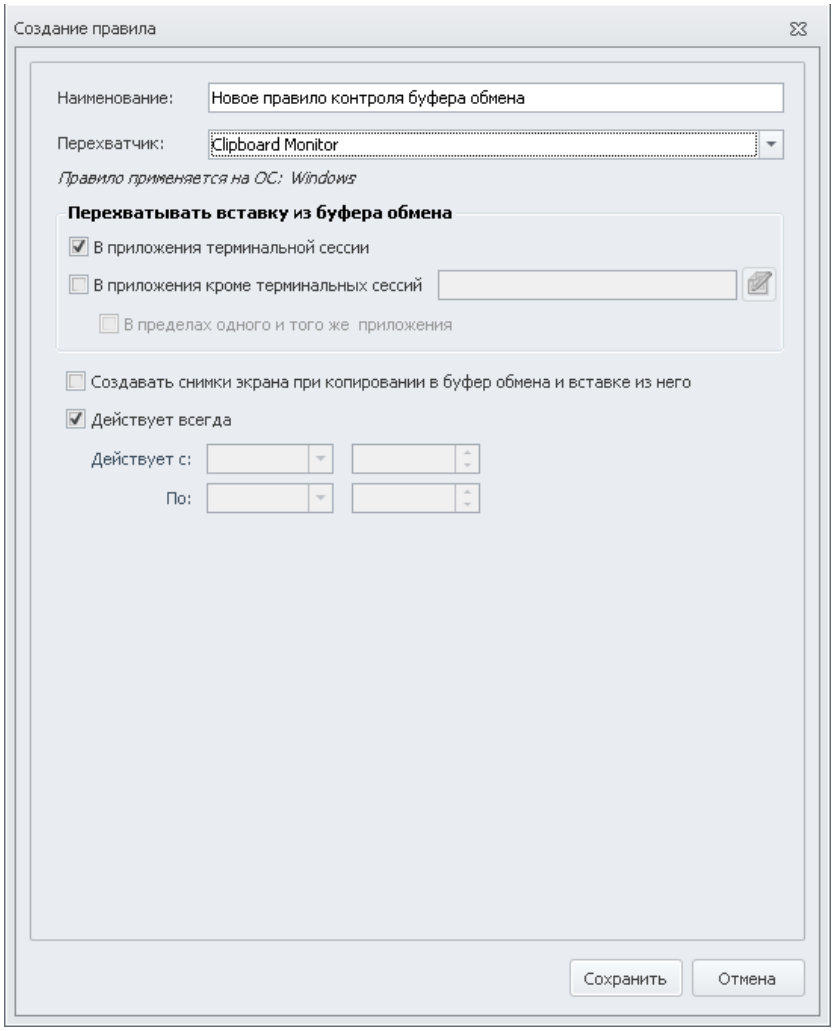
8. В блоке **Запрет печати** установите флажок напротив **В приложениях из списка,** чтобы включить запрет печати и укажите список приложений, печать из которых требуется запретить, а также тип принтера:
   - локальный;
   - сетевой;
   - терминальный.

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

Правило (DM) для Clipboard Monitor

Перехватчик Clipboard Monitor позволяет контролировать доступ сотрудников к буферу обмена.

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



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **Clipboard Monitor**.
3. В области **Перехватывать вставку из буфера обмена** определите, в каком случае правило (DM) будет действовать:
   - **В приложения терминальной сессии**. Если выбрана эта опция, то правило (DM) будет срабатывать при вставке данных в приложения терминальной сессии. При вставке данных внутри терминальной сессии правило срабатывать не будет.
   - **В приложения кроме терминальной сессии**. Выберите эту опцию, если правило (DM) должно действовать только в случае вставки данных в указанные

приложения, и выберите приложения с помощью кнопки : см. "Приложения".
Правило будет срабатывать также при вставке в указанные приложения данных, скопированных из терминальной сессии.
Если требуется, чтобы правило срабатывало также при вставки данных в приложение, из которого данные были скопированы, отметьте опцию **В пределах одного и того же приложения**.

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

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

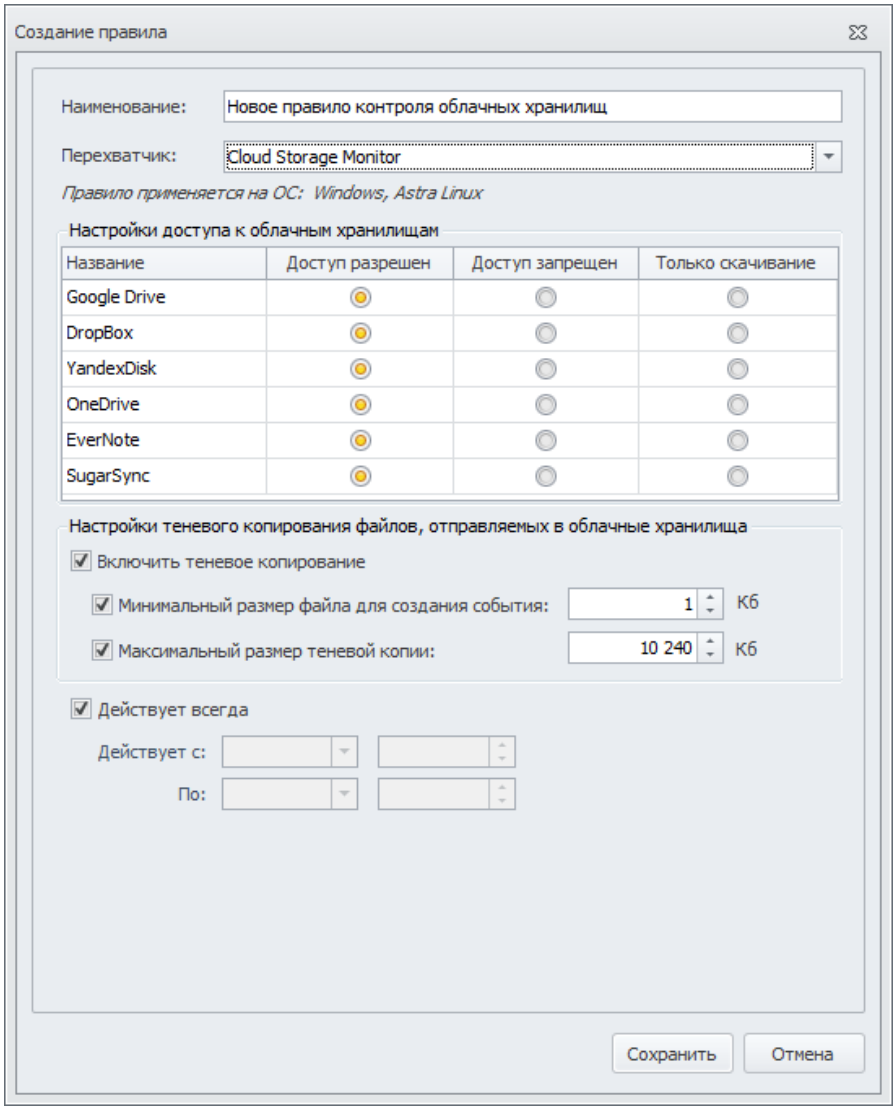
Правило (DM) для Cloud Storage Monitor

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

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

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

> **Примечание.**
>
> Правило применяется на компьютерах под управлением операционных систем MS Windows и Astra Linux.



Чтобы настроить правило:

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

> **Важно!**
>
> В случае если файл был когда-либо прежде загружен кем-либо на Yandex Disk и не был оттуда полностью удален (включая корзину), создание теневой копии данного файла невозможно.

Правило (DM) для Device Monitor

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

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

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

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

Примечание.

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

Мобильные устройства могут быть подключены к компьютеру:

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

Контроль подключения через MTP- и PTP-протокол осуществляется для телефонов на платформе Android, iOS, Windows Phone/10 Mobile; Blackberry 10. Полный список поддерживаемых устройств см. в документе "*InfoWatch Traffic Monitor. Руководство по установке*", в статье "Аппаратные и программные требования".

Фотокамера может быть подключена к компьютеру:

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

Важно!

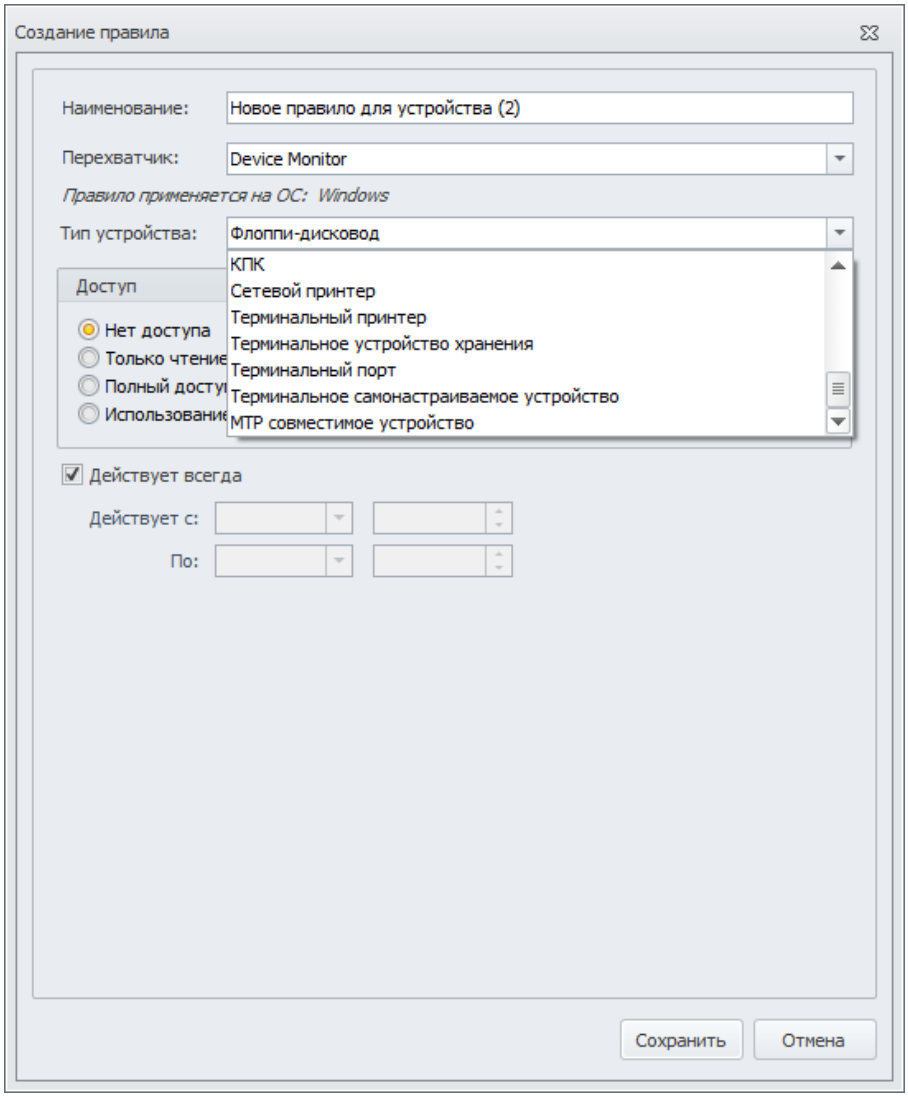
Копирование файлов на съемные устройства и MTP-устройства можно контролировать также с помощью правила File Monitor. При этом необходимо учитывать, что правило File Monitor позволяет отслеживать операции копирования, в то время как правило Device Monitor позволяет полностью запретить подобные операции.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

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

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

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

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



Чтобы настроить правило:

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

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

- разрешить полный доступ только к зашифрованным устройствам (только для типов **Флоппи-дисковод** и **Съемное устройство хранения**).
- полностью разрешить доступ к устройству;

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

Особенности применения правила на некоторых устройствах:

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

Правило (DM) для File Monitor

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

К съемным устройствам относятся:

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

Отслеживаются такие действия сотрудников, как:

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

Примечание.

Переименование файла на медиа-устройстве не отслеживается.

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

Важно!

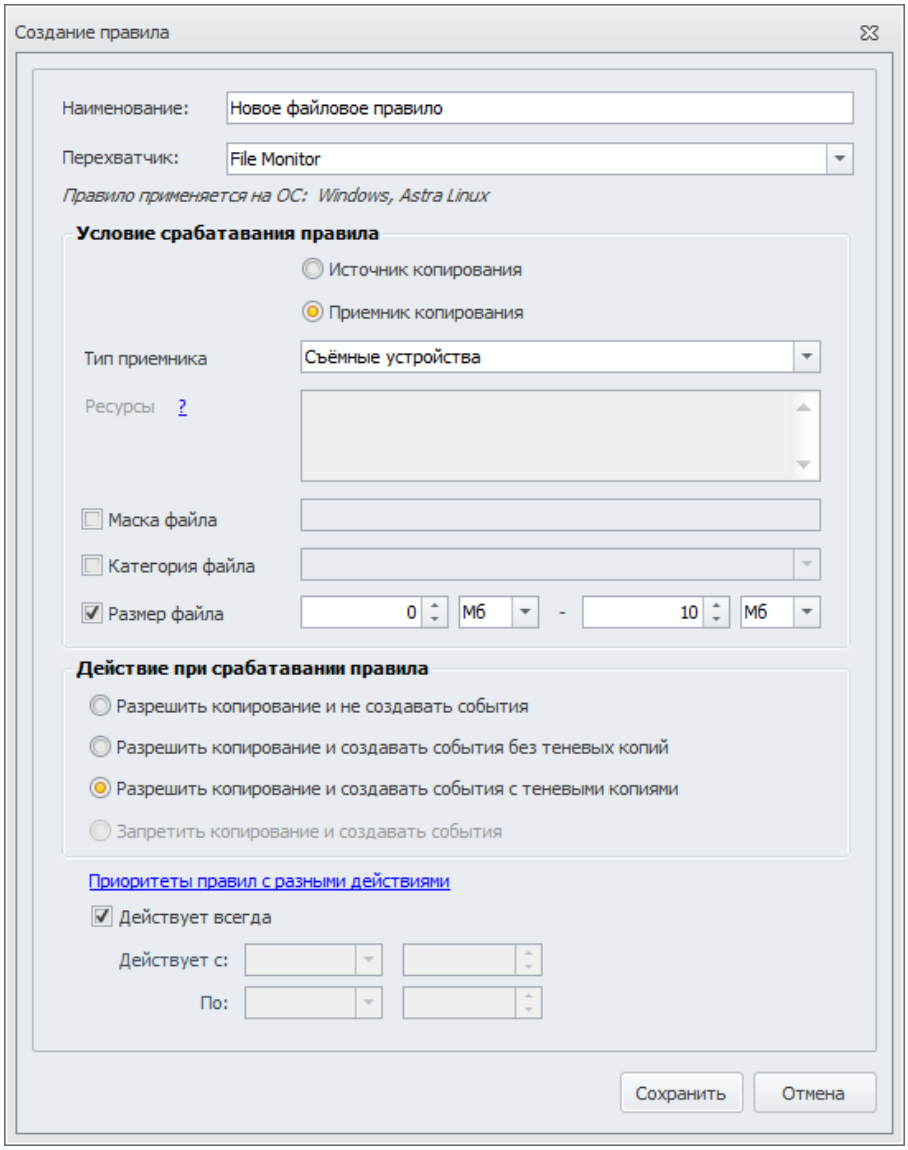
Правило применяется на компьютерах под управлением операционных систем MS Windows и Astra Linux.

На компьютерах под управлением Astra Linux не контролируются операции копирования/перемещения файлов на ресурсы, подключенные через терминальную сессию.

Важно!

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

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



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **File Monitor**.
3. Укажите **Условия срабатывания правила:**
   a. Задайте направление перехвата копирования: *Источник копирования* или *Приемник копирования*.
   b. Укажите тип источника: *Съемные устройства*, *Сетевые ресурсы* или *Терминальная сессия*.
   c. Если требуется, укажите Сетевые ресурсы, задав их адреса.
4. При необходимости вы можете ограничить набор контролируемых файлов, задав маску файла. Для этого отметьте поле **Маска файла** и укажите маску: можно использовать символы: «?» для замены одного символа или «*» для замены набора символов. Например, *.doc. Знак пробела интерпретируется как часть имени файла.

Важно!

Для одного правила (DM) может быть только одна маска. Если необходимо ввести несколько масок, следует создать по одному правилу (DM) на каждую из масок.

Примечание:

На компьютерах под управлением Astra Linux маски файлов не учитываются.

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

   Примечание:

   На компьютерах под управлением Astra Linux категории сигнатур не учитываются.

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

   Важно!

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

8. Определите период действия правила (DM). По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.

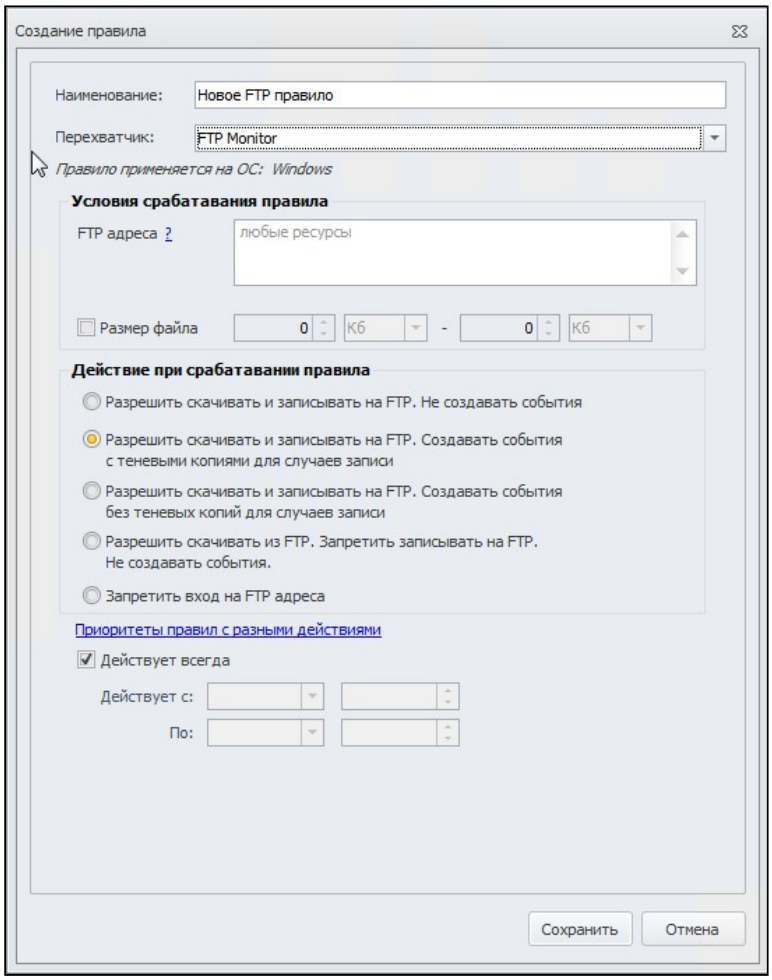
9. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Подробнее о работе правила см. "Особенности и ограничения перехвата при копировании файлов с/на съемные устройства, сетевые ресурсы, FTP".

Правило (DM) для FTP Monitor

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

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



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **FTP Monitor**.
3. В **Условиях срабатывания правила** укажите **адреса FTP.** Нажав на **?** (знак вопроса), вы узнаете правила заполнения данного поля. Вы также можете указать ограничения файла, установив галочку напротив **Размера файла** и обозначив диапазон значений. Этот параметр доступен только при создании событий с теневыми копиями отправляемых файлов и при создании события без теневых копий для случаев

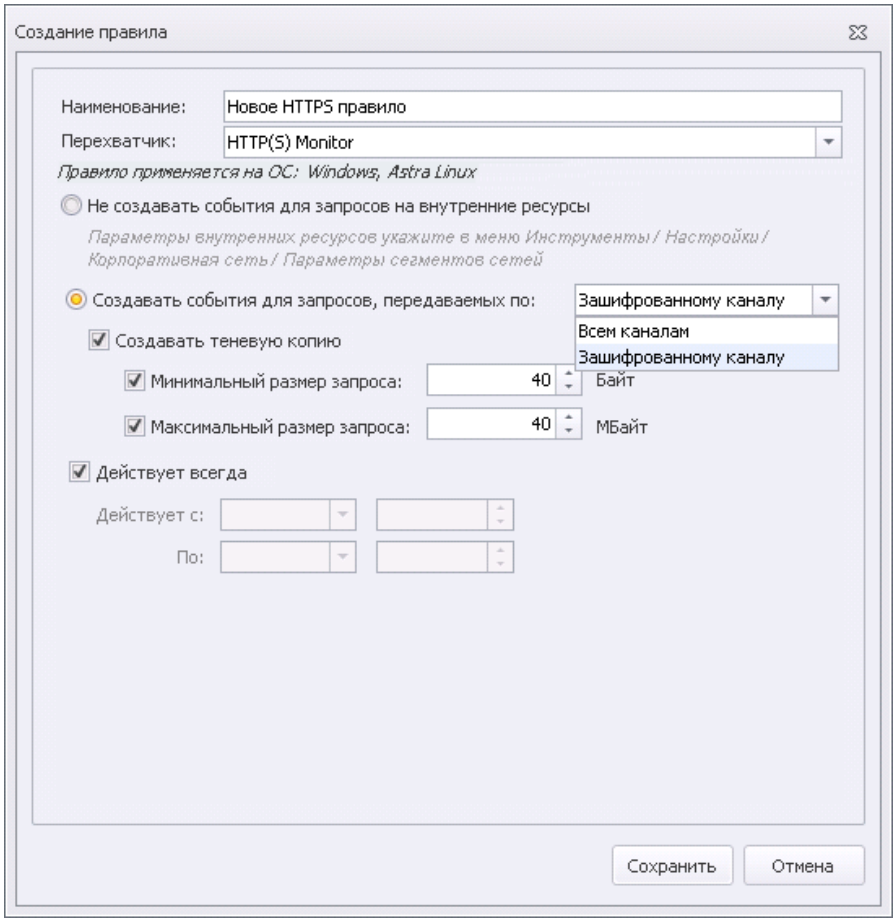
записи, если на компьютере осталось меньше свободного места, что определено политикой (DM) (см. "Создание теневых копий и запрет операций при нехватке свободного места").

4. Выберите степень контроля обмена данными по протоколу FTP:
   - **Разрешить скачивать и записывать на FTP. Не создавать события**
   - **Разрешить скачивать и записывать на FTP. Создавать события с теневыми копиями для случаев записи**
   - **Разрешить скачивать и записывать на FTP. Создавать события без теневых копий для случаев записи**
   - **Разрешить скачивать из FTP/ Запретить записывать на FTP. Не создавать события**
   - **Запретить вход на FTP адреса**
5. Настройте период действия правила (DM). По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
6. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Правило (DM) для HTTP(S) Monitor

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

> **Примечание.**
>
> Правило применяется на компьютерах под управлением операционных систем MS Windows и Astra Linux .



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик** выберите **HTTP(S) Monitor**.
3. Настройте параметры событий, создаваемых при перехвате трафика. Вы можете:
   - исключить перехват запросов на внутренние ресурсы. Отметьте поле **Не создавать события для запросов на внутренние ресурсы**, если вы хотите, чтобы все запросы, передаваемые внутри корпоративной сети не перехватывались. О том, как настроить сегменты сети, см. "Контроль сетевых соединений", группа **Параметры сегментов сетей**.

     Важно!

     Если выбрать этот режим, то создание теневой копии в данном правиле (DM) станет недоступно. Если вам необходимо, чтобы:
     - не создавались события для запросов на внутренние ресурсы, и при этом
     - теневая копия создавалась,

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

- настроить перехват данных только по шифрованным каналам, либо по всем каналам. Для этого отметьте **Создавать события для запросов, передаваемых по** и из раскрывающегося списка выберите:
  - **Всем каналам**
  - **Зашифрованному каналу**

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

  > **Важно!**
  >
  > Если на компьютере осталось меньше свободного места, чем определено политикой (DM) (см. "Создание теневых копий и запрет операций при нехватке свободного места"), то событие будет создано без теневой копии.

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

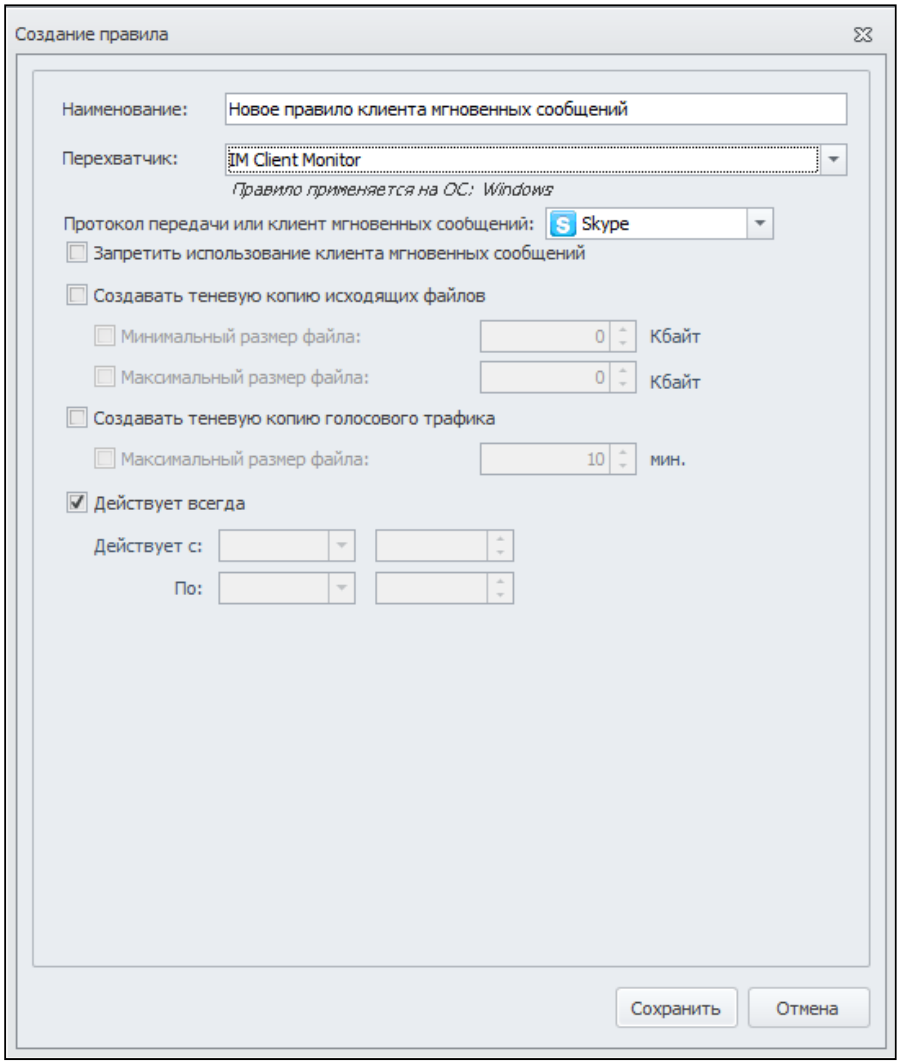
Особенности применения правила на компьютерах под управлением операционной системы Astra Linux:

1. Не перехватываются соединения по протоколу IPv6.
2. Запросы, относящиеся к веб-почте, перехватываются как обычные HTTP-запросы.
3. Правила с выбранной настройкой **Не создавать события для запросов на внутренние ресурсы** игнорируются.

Правило (DM) для IM Client Monitor

Перехватчик **IM Client Monitor** позволяет контролировать доступ сотрудников к системам мгновенного обмена сообщениями Skype, Telegram, Jabber (протокол XMPP), Facebook, VK (ВКонтакте), протокол MMP.

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



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **IM Client Monitor**.
3. В поле **Протокол передачи или клиент мгновенных сообщений** выберите тип мессенджера, контролируемого данным правилом (DM):
   - Skype - для контроля использования настольных приложений Skype версий 7 и 8, а также веб-версии Skype For Web;
   - XMPP - для контроля использования Jabber;
   - MMP - для контроля программ, использующих протокол MMP;
   - Telegram - для контроля использования Telegram
   - Facebook - для контроля использования Facebook
   - VK - для контроля использования VK (ВКонтакте).
4. Если требуется перехватывать голосовые сообщения в Skype, отметьте поле **Создавать теневую копию голосового трафика** и при необходимости укажите максимальный размер файла (звуковой файл будет сохранен в формате `*.ogg`):

- если поле **Максимальный размер файла** отмечено, то для разговоров, длительность которых превышает указанное значение, будет создано несколько отдельных событий с теневыми копиями.

5. Если вы хотите полностью запретить использование клиента данного типа, отметьте поле **Запретить использование клиента мгновенных сообщений** (недоступно для мессенджеров **Telegram, Facebook, VK**).

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

> **Важно!**
>
> Чтобы запретить использование Telegram, Facebook и VK, необходимо использовать правила (DM) Application Monitor: см. "Правило (DM) для Application Monitor".

6. Если вы хотите передавать в Traffic Monitor теневые копии пересылаемых файлов, отметьте поле **Создавать теневую копию исходящих файлов**. В этом случае вы также можете определить дополнительные параметры теневых копий:
   - **Минимальный размер файла**. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
   - **Максимальный размер файла**. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.
7. Если вы хотите передавать в Traffic Monitor теневые копии голосовых сообщений, отметьте поле **Создавать теневую копию голосового трафика** и укажите максимальную длительность звукового файла. Для этого в поле **Максимальный размер файла** установите нужное значение в минутах.
8. Определите период действия правила (DM). По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
9. После того как вы определите все необходимые параметры, нажмите **Сохранить**.

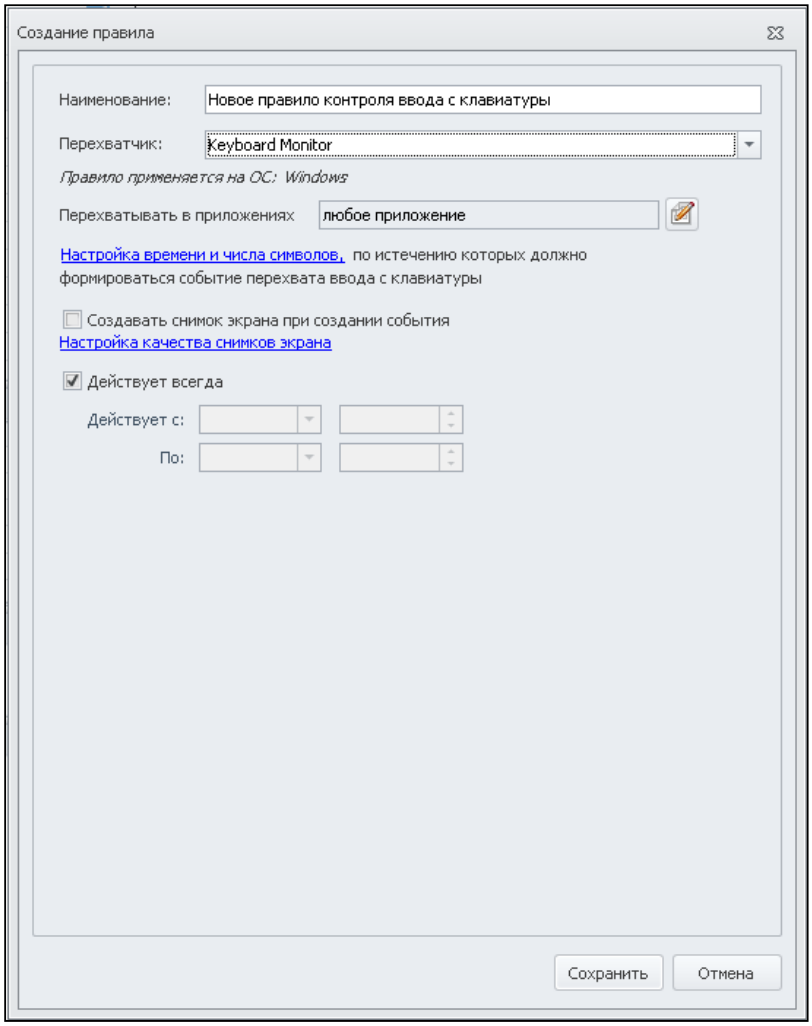
> **Важно!**
>
> Поля **Минимальный размер файла** и **Максимальный размер файла** учитываются только при создании теневой копии: если размер файла попадает в указанный диапазон, то событие будет содержать теневую копию; в противном случае событие будет сформировано без теневой копии. Также

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

Правило (DM) для Keyboard Monitor

Перехватчик **Keyboard Monitor** позволяет перехватывать ввод текста с клавиатуры на рабочих станциях. Далее сформированные из перехваченных данных события будут отправлены в TM для обработки и анализа.

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



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **Keyboard Monitor**.
3. В области **Перехватывать в приложениях** укажите:
   - Название приложения, где должно работать правило. Укажите приложения, где должно действовать правило (DM) , выберите их с помощью кнопки : см. "Приложения".
   - *Любое приложение* - в этом случае перехват ввода с клавиатуры будет осуществляться во всех приложениях.
4. Укажите (если требуется) более точные условия формирования события: см. "Контроль ввода с клавиатуры"
5. Укажите периодичность создания снимков экрана (в секундах). По умолчанию установлено значение 600 секунд. Также снимок экрана будет создаваться при смене активного окна.
6. Определите период действия правила (DM). По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
7. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Правило (DM) для Mail Monitor

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

Правило Mail Monitor обеспечивает контроль трафика, передаваемого с помощью SMTP, IMAP, POP3, HTTPS и Outlook.

Примечание.

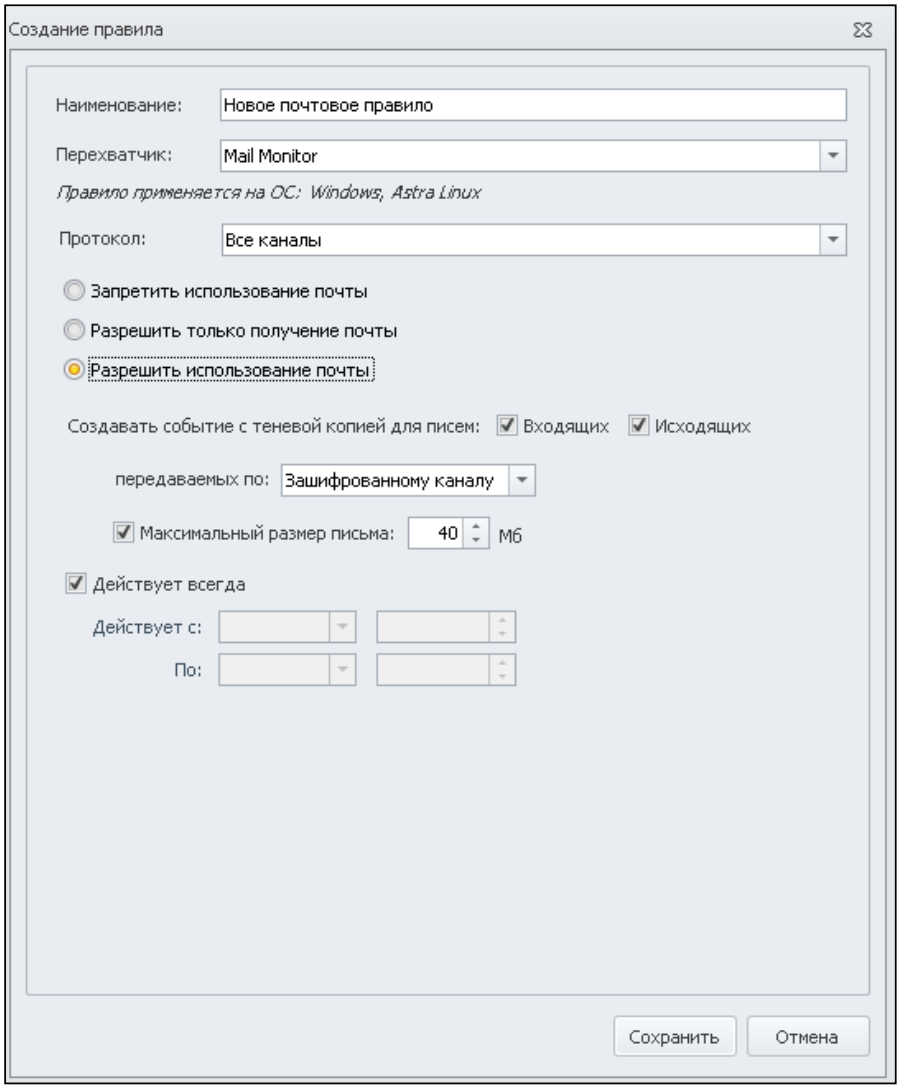
Для HTTPS контролируется отправка сообщений с помощью следующих сервисов:

- Gmail
- Yandex
- Mail.ru
- Yahoo
- Rambler
- Outlook.com

Важно!

Правило применяется на компьютерах под управлением операционных систем MS Windows и Astra Linux.

На компьютерах под управлением Astra Linux правило контролирует только протоколы SMTP, POP3, IMAP и HTTPS.



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **Mail Monitor**.
3. В поле **Протокол** выберите канал, который должен контролироваться правилом. Возможные значения:
   - **Все каналы**;
   - **SMTP** - только для исходящей почты;
   - **POP3** - только для входящей почты;
   - **Outlook** - как для входящей, так и для исходящей почты;
   - **IMAP** - только для входящей почты;
   - **HTTPS** - только для исходящей почты.
4. Выберите, какие действия с почтой должны быть доступны пользователю. Возможные значения:
   - **Запретить использование почты**;
   - **Разрешить только получение почты** - доступно только если в поле **Протокол** выбрано *Outlook* или *Все каналы*;
   - **Разрешить использование почты**.

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

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

Вы также можете определить дополнительные параметры создания теневых копий:

- В поле **передаваемых по** укажите, требуется ли создавать теневые копии для сообщений, передаваемых по всем каналам или только по зашифрованным.

> **Примечание.**
>
> Для протокола HTTPS значение **Всем каналам** недоступно.

- **Максимальный размер письма**. Если поле отмечено, то теневое копирование будет выполняться только для писем, размер которых меньше либо равен указанному.

> **Важно!**
>
> Если на компьютере осталось меньше свободного места, чем определено политикой (DM) (см. "Создание теневых копий и запрет операций при нехватке свободного места"), то письмо будет передано без создания теневой копии.

6. Настройте период действия правила (DM). По умолчанию выбрана настройка **Действует всегда**. Чтобы указать другой период действия, снимите отметку и в полях **Действует с** и **По** укажите требуемый период.
7. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

> **Важно!**
>
> Если действующее правило (DM) имеет атрибуты:
>
> - **Разрешить использование почты**;
> - **Создавать теневую копию для писем: Входящие и Исходящие, передаваемые по: Всем каналам**.

и в почтовой программе настроено хранение на сервере (например, в MS Outlook выбрано **Сохранять отправленные элементы в следующей папке на сервере** в окне **Настройки электронной почты Интернета** на вкладке **Отправленные**), то для каждого события отправки сообщения будет отображаться два объекта перехвата: одно с типом **Исходящее**, другое - **Входящее**. В зависимости от программы название опции может меняться.

Пример:

Чтобы перехват почты по протоколам IMAP, SMTP, POP3 работал на сетевом уровне:

1. Добавьте **Outlook** в исключения (см. "Исключение приложений из перехвата")
2. Создайте правила для перехвата по этим протоколам, как описано выше.
3. Удалите правило для протокола Outlook/MAPI.

Правило (DM) для Network Monitor

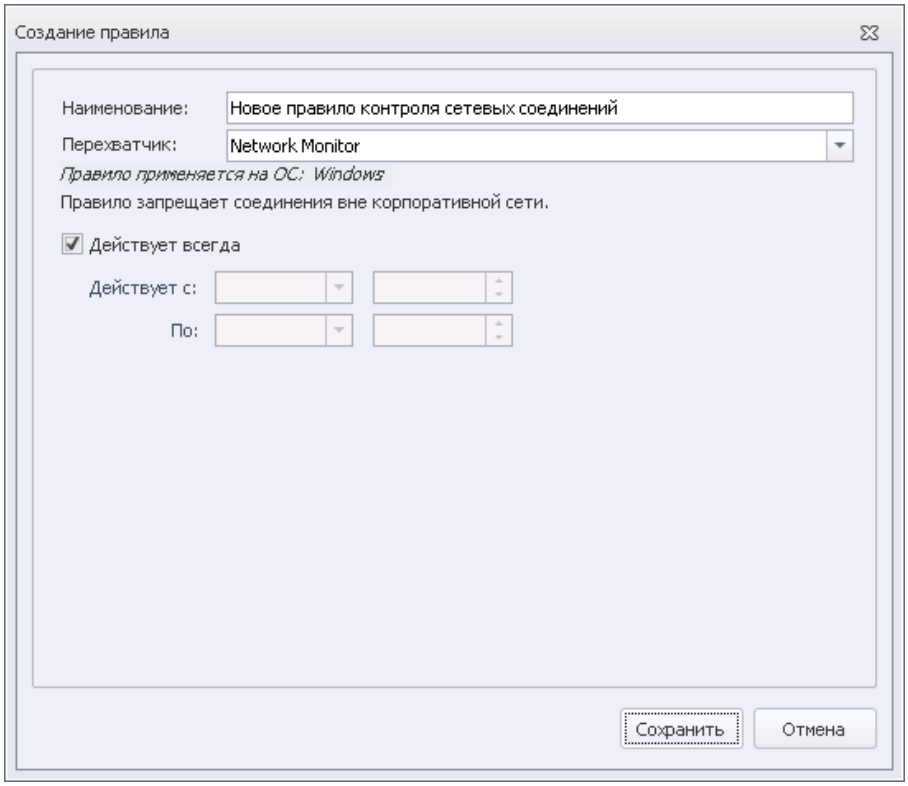
Перехватчик Network Monitor позволяет запрещать передачу данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами. Определение сегментов корпоративной сети и разрешенных внешних адресов выполняется, как описано в разделе "Контроль сетевых соединений".

Примечание.

Правило применяется на компьютерах под управлением операционной системы MS Windows.

Важно!

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

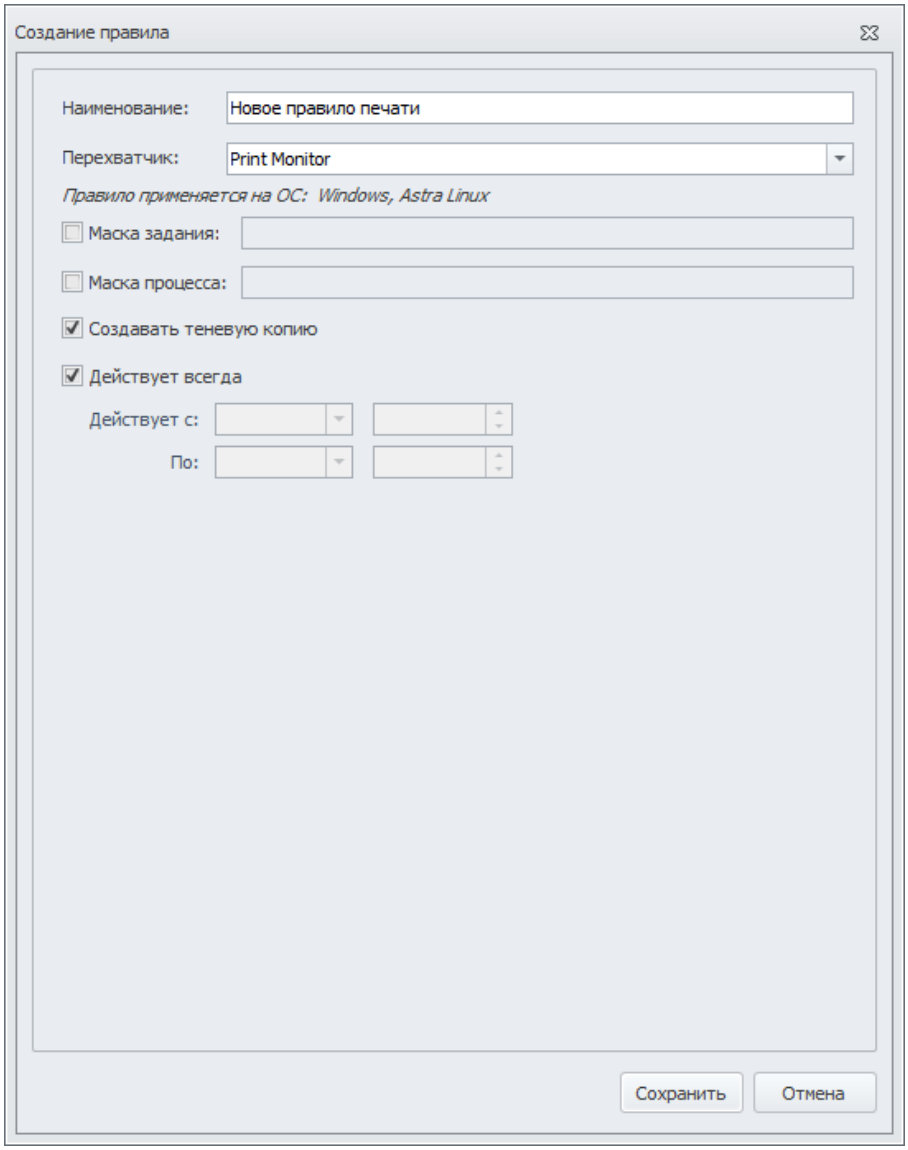


Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **Network Monitor**.
3. Настройте период действия правила (DM). По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
4. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Правило (DM) для Print Monitor

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



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **Print Monitor**.
3. При необходимости вы можете ограничить контролируемые задания на печать с помощью масок:
   - **Маска задания**. Использование маски для задания (документа), выводимого на печать. Если требуется указать маску задания, то отметьте данное поле и укажите маску задания.
     В маске задания можно использовать подстановочные символы: «?» для замены одного символа или «*» для замены набора символов. Знак пробела интерпретируется как часть имени задания.

> **Важно!**
>
> Наименование задания печати формируется приложением, из которого документ передается на печать. Поэтому наименование может представлять собой любую текстовую строку, в том числе вообще не связанную с типом и именем распечатываемого документа.

- **Маска процесса**. Использование маски для процесса, который выводит задание на печать. Если нужно задать маску процесса, отметьте данное поле и укажите маску процесса.
  Имя (полный путь) процесса будет получено для процесса, в контексте которого осуществляется рендеринг задания печати. В некоторых случаях (локальные LPT- и COM-принтеры) подсистема печати может осуществлять рендеринг в контексте службы Диспетчер очереди печати (Print Spooler). Путь к исполняемому файлу службы: `%SystemRoot%\system32\spoolsv.exe`.
  Для того чтобы имя процесса определялось корректно, необходимо в свойствах принтера установить параметр **Печатать прямо на принтер** (**Свойства принтера** > **Дополнительно**). Тогда обработка задания печати будет осуществляться в контексте приложения, из которого документ был отправлен на печать. Однако в этом случае печать будет происходить синхронно, т.е. работа с приложением будет невозможна до окончания печати.
  При задании маски процесса можно использовать подстановочные символы: «?» для замены одного символа или «*» для замены набора символов. Знак пробела интерпретируется как часть имени процесса.

4. Если вы хотите передавать на Traffic Monitor теневые копии печатаемых документов, отметьте поле **Создавать теневую копию**.

> **Важно!**
>
> Если на компьютере осталось меньше свободного места, чем определено политикой (DM) (см. "Создание теневых копий и запрет операций при нехватке свободного места"), то печать будет осуществляться без создания теневой копии.

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

Пример:
Для перехвата задания на печать файла с расширением `.txt` с помощью программы `notepad.exe`:

1. В строке Маска задания введите `*.txt*`
2. В строке Маска процесса введите `*nodepad.exe`

Важно!

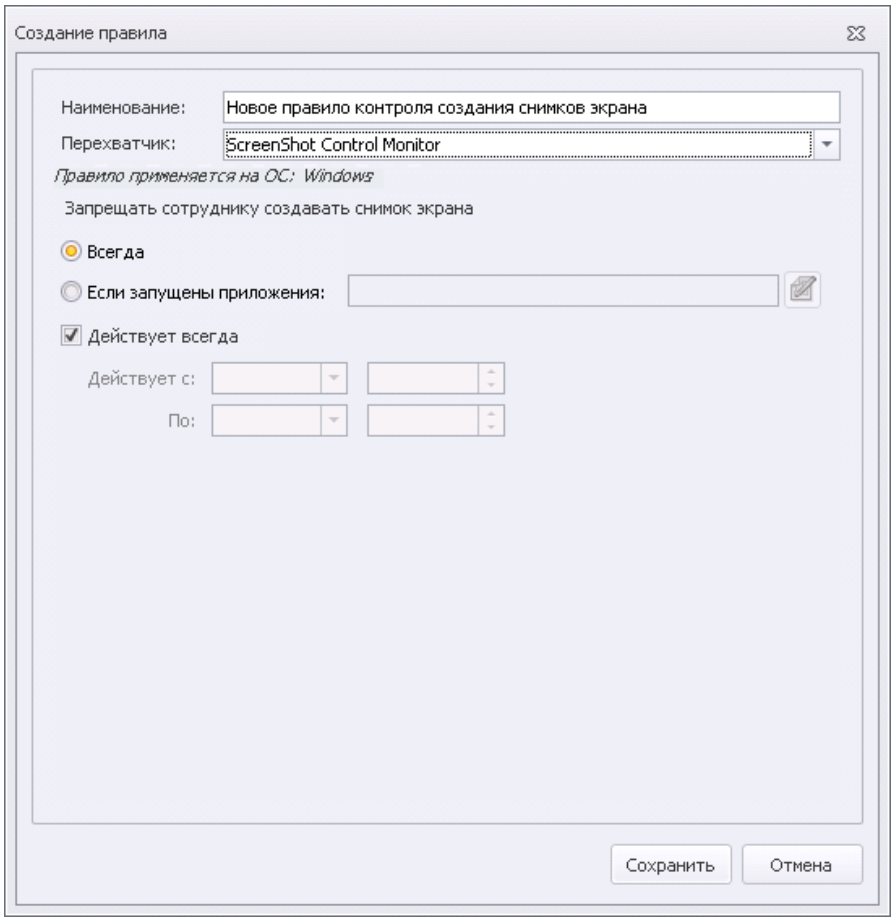
Задания на печать будут перехватываться при условии, что в операционной системе пользователя отображаются расширения файлов (в Параметрах папок снят флажок в поле **Скрывать расширения для зарегистрированных типов файлов**).

Правило (DM) для ScreenShot Control Monitor

Перехватчик **ScreenShot Control Monitor** позволяет осуществлять контроль снимков экрана со стороны агента.

Примечание.

Правило применяется на компьютерах под управлением операционной системы MS Windows.



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **ScreenShot Control Monitor**.
3. В области **Запрещать сотруднику создавать снимок экрана** определите, в каком случае накладывается запрет. Возможные значения:
   - **Всегда**;

- **Если запущены приложения**. Если выбрана эта опция, нажмите , чтобы указать приложения (см. "Приложения").

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

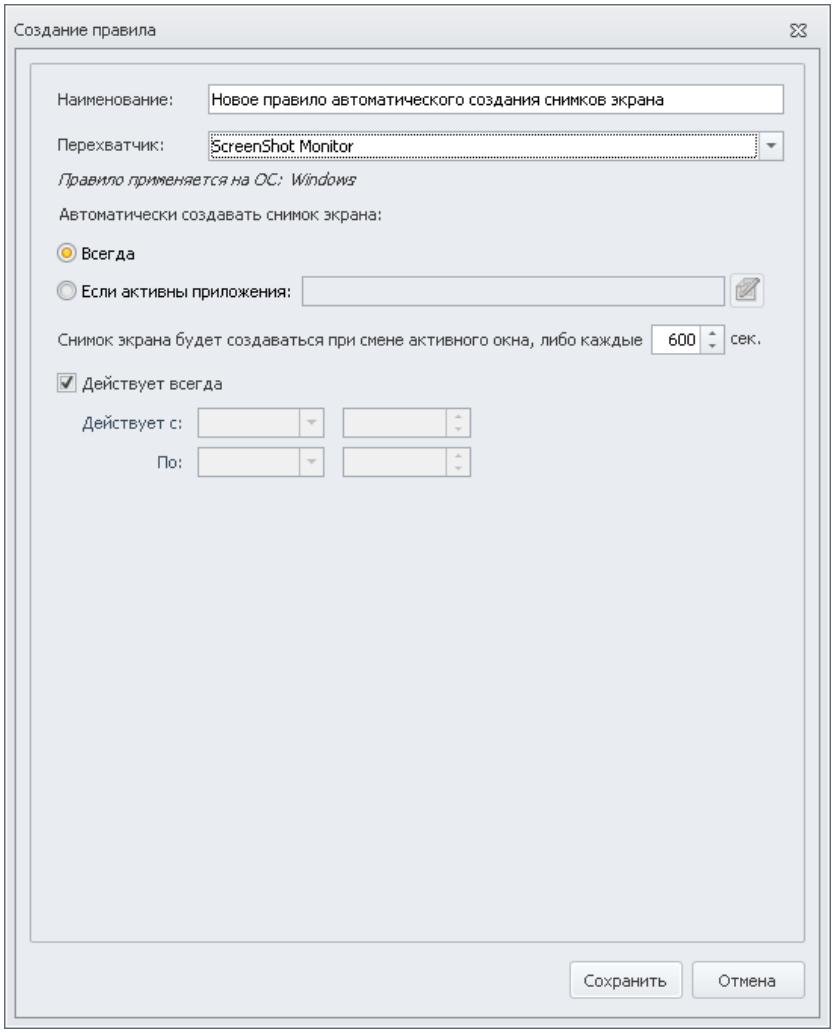
Правило (DM) для ScreenShot Monitor

Перехватчик **ScreenShot Monitor** позволяет автоматически создавать снимки экрана на контролируемых компьютерах.

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

> **Важно!**
>
> Параметр **Не создавать снимок экрана, если долгое время нет активности от мыши или клавиатуры**, определяющий работу правила (DM) в зависимости от активности на контролируемых компьютерах, настраивается вместе с общими настройками схемы безопасности: см. "Контроль приложений и снимки экрана".

> **Важно!**
>
> Создание снимков экрана при копировании данных в буфер обмена или вставке из буфера обмена настраивается в правиле Clipboard Monitor (см. "Правило (DM) для Clipboard Monitor").



Чтобы настроить правило:

1. Откройте окно создания правила (см. "Создание правил (DM)") и в поле **Наименование** укажите название правила.
2. В поле **Перехватчик**, выберите **ScreenShot Monitor**.
3. В области **Автоматически создавать снимок экрана** определите, в каком случае правило (DM) будет действовать. Возможные значения:
   - **Всегда**;
   - **Если активны приложения**. Отметьте, если правило (DM) должно действовать только в случае активности указанных приложений, и выберите приложения с помощью кнопки : см. "Приложения".
4. Укажите периодичность создания снимков экрана (в секундах). По умолчанию установлено значение 600 секунд. Также снимок экрана будет создаваться при смене активного окна.
5. Определите период действия правила (DM). По умолчанию выбрана настройка **Действует всегда**. Чтобы определить период, снимите отметку и в полях **Действует с** и **По** укажите даты и время.
6. После того, как вы определите все необходимые параметры, нажмите **Сохранить**.

Сотрудники

Основные принципы работы с сотрудниками (контролируемыми пользователями) и группами сотрудников описываются в разделе "Сотрудники и группы сотрудников".

Действующие политики безопасности (DM) могут быть назначены только группе сотрудников. Определение политики безопасности (DM) для отдельного сотрудника выполняется путем включения его учетной записи в ту или иную группу.

> **Важно!**
>
> На каждого сотрудника, помимо политики безопасности (DM), назначенной группе сотрудников, также действует и политика безопасности (DM), определенная для компьютера, на котором работает сотрудник. О порядке определения приоритетов при пересечении правил (DM) см. "Применение правил (DM)".

Чтобы перейти к разделу Консоли управления (DM), предназначенному для управления учетными записями сотрудников и группами сотрудников, воспользуйтесь кнопкой Группы сотрудников, расположенной на Панели навигации.

Информация по работе с сотрудниками и группами сотрудников содержится в подразделах:

- Просмотр сведений о сотрудниках и группах сотрудников
- Просмотр результирующих политик (DM) и белого списка для сотрудника
- Создание и редактирование группы сотрудников
- Удаление группы сотрудников
- Добавление учетной записи сотрудника в группу
- Редактирование учетной записи сотрудника
- Исключение учетной записи сотрудника из группы сотрудников
- Удаление учетной записи сотрудника из схемы безопасности

Просмотр сведений о сотрудниках и группах сотрудников

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

> **Примечание.**
>
> Для более удобного просмотра вы можете настроить отображение списка сотрудников, при помощи дополнительных функций (см. "Дополнительные возможности").

Чтобы просмотреть информацию по отдельной группе сотрудников, выберите название нужной группы в списке групп сотрудников.

Чтобы просмотреть информацию по всем сотрудникам, зарегистрированным в Системе, воспользуйтесь кнопкой **Показать всех сотрудников**, расположенной в верхней части Панели навигации.

Информация по учетным записям сотрудников представлена в виде табличного списка. Каждая строка списка соответствует одной учетной записи. В столбцах выводятся общие свойства учетных записей. Расширенная информация по свойствам учетной записи выводится на панели **Подробно**.

Чтобы просмотреть подробную информацию по свойствам отдельной учетной записи, выберите строку с названием нужной учетной записи.

В результате на панели Подробно будет отображена таблица свойств, в которой вы сможете просмотреть следующую информацию:

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

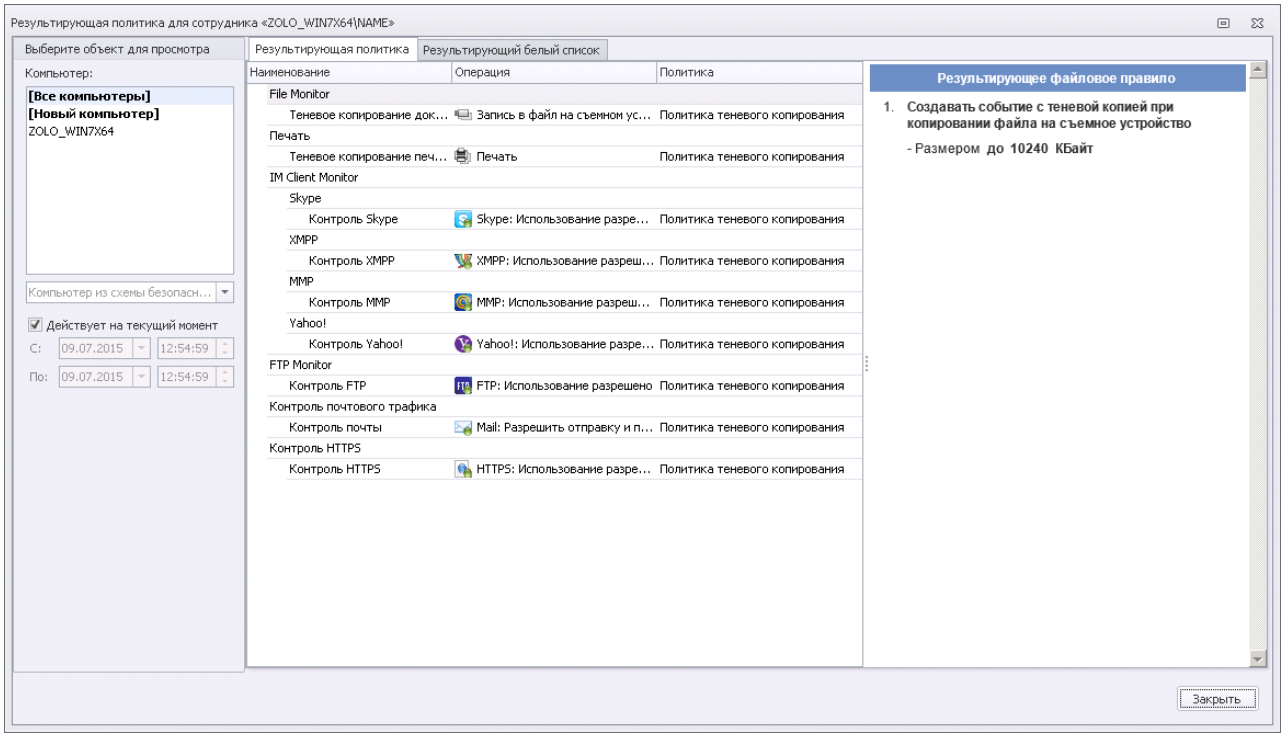
> **Примечание.**
>
> Часть свойств, выводимых на панели **Подробно**, дублируется в рабочей области главного окна.

Просмотр результирующих политик (DM) и белого списка для сотрудника

Чтобы посмотреть информацию о политике и белом списке, действующих для сотрудника:

1. В списке сотрудников выберите запись требуемого сотрудника.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Показать результирующую политику**.
   - на панели **Сотрудники** нажмите **Показать результирующую политику**.

В результате на экран будет выведено окно **Результирующая политика для сотрудника <имя сотрудника>**, где по умолчанию отображается результирующая политика (DM) для всех компьютеров выбранного сотрудника.



Основная область окна **Результирующая политика для сотрудника** содержит две вкладки:

- **Результирующая политика** - отображаются правила (DM), являющиеся результирующими для данного сотрудника. Результирующая политика (DM) складывается из правил (DM), настроенных по умолчанию, правил (DM), заданных для выбранного компьютера, и правил для выбранного сотрудника (см. "Особенности применения правил для Device Monitor"). Чтобы просмотреть подробную информацию по правилу (DM), выберите его из списка: на панели, находящейся справа, отобразится подробная информация о выбранном правиле (DM).
- **Результирующий белый список** - отображаются устройства, являющиеся разрешенными для данного сотрудника (см. "Белые списки"). Чтобы просмотреть подробную информацию об устройстве, выберите его из списка: на панели, находящейся справа, отобразится подробная информация о выбранном устройстве.

На панели **Компьютер** вы можете выбрать объект для просмотра:

- **Все компьютеры** - при выборе отображается результирующая политика\белый список для сотрудника, вне зависимости от того, на какой компьютер он выполнил вход.
- **Новый компьютер** - при выборе отображается результирующая политика пользователя на новом компьютере (которого еще нет в схеме безопасности).
- Чтобы просмотреть результирующую политику (DM) для выбранного пользователя на определенном компьютере:
  - из списка **Компьютер** выберите имя компьютера, на котором зарегистрирована выбранная учетная запись сотрудника

  или
- из раскрывающегося списка **Компьютер из схемы безопасности** выберите любую учетную запись компьютера, зарегистрированную в Системе (см. "Компьютеры").

Вы можете выбрать время, для которого будет показана результирующая политика\белый список:

- по умолчанию выбрана настройка **Действует на текущий момент** и отображаются текущие результирующие политика и белый список;
- чтобы просмотреть результирующие политику\белый список для выбранного сотрудника за интересующий вас период времени, снимите отметку с поля **Действует на текущий период** и укажите необходимый временной промежуток.

Создание и редактирование группы сотрудников

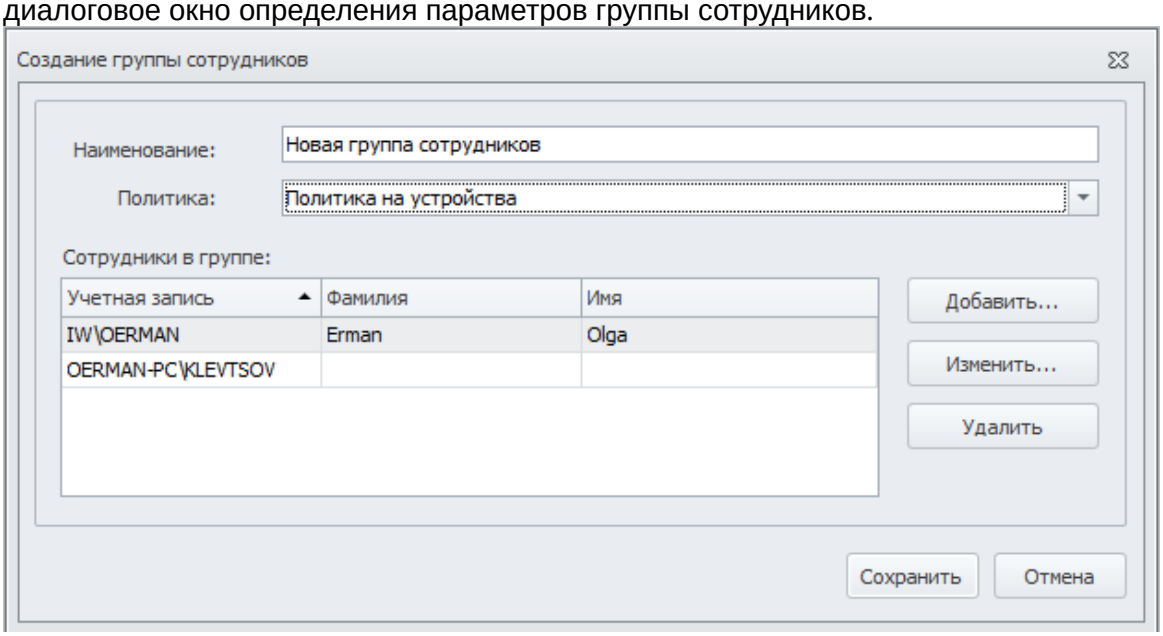
Чтобы добавить группу сотрудников:

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

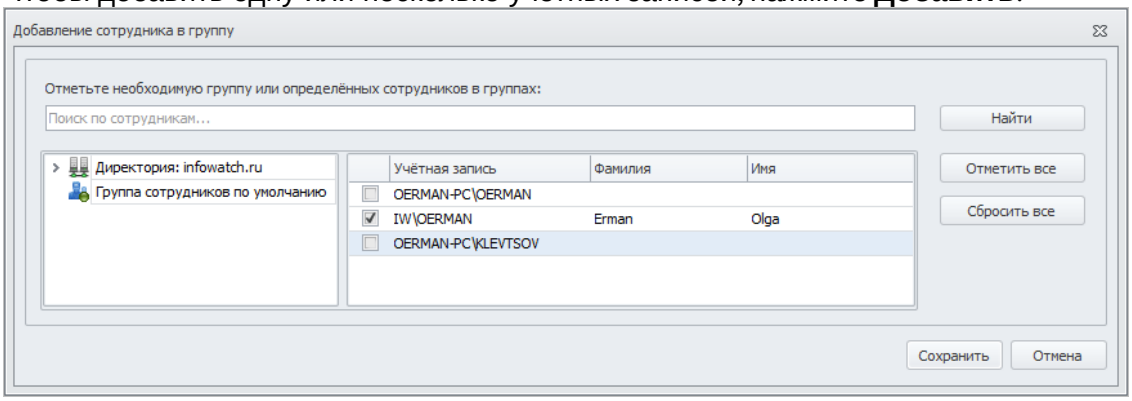
Действие	Шаги
Добавить группу сотрудников	• в главном меню выберите команду **Правка** > **Создать группу сотрудников**; • воспользуйтесь кнопкой **Создать группу сотрудников**, расположенной в верхней части Панели навигации.

Отредактировать группу сотрудников	a. В области Группы сотрудников на Панели навигации выберите название нужной группы сотрудников. b. Выполните одно из следующих действий: • в главном меню выберите команду **Правка** > **Изменить**; • воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации; • дважды щелкните левой кнопкой мыши по названию выделенной группы сотрудников.

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



3. Укажите следующие параметры:
   - **Наименование**. Название группы сотрудников.
   - **Политика**. Выберите из раскрывающегося списка политику безопасности (DM), которая будет назначена данной группе сотрудников.
4. Определите перечень сотрудников в группе:
   - Чтобы добавить одну или несколько учетных записей, нажмите **Добавить**.



В окне добавления сотрудников отображается список учетных записей, импортированных из службы каталогов (см. "Соединение с сервером LDAP и

синхронизация с сервером Active Directory и Astra Linux Directory"), а также уже зарегистрированных в системе (например, при установке Агента Device Monitor на компьютеры) и принадлежащих существующим группам сотрудников Device Monitor.
Чтобы добавить сотрудника, в левой области выберите необходимый узел в дереве групп, затем отметьте учетные записи, которые нужно добавить в редактируемую группу.
Чтобы отметить все учетные записи, принадлежащие выбранному узлу, нажмите **Отметить все**. Чтобы снять выделение, нажмите **Сбросить все**.
Вы также можете выполнить поиск учетной записи по всем доступным элементам. Для этого в верхней строке введите часть имени учетной записи и нажмите **Найти**.
После того, как все необходимые учетные записи выбраны, нажмите **Сохранить**, чтобы закрыть окно добавления сотрудников и вернуться к окну настройки параметров группы.
- Чтобы изменить параметры учетной записи, выберите ее в списке сотрудников, входящих в группу, и нажмите **Изменить**. О порядке редактирования учетной записи см. "Редактирование учетной записи сотрудника".
- Чтобы удалить запись из группы, выберите ее и нажмите **Удалить**.

5. Нажмите **Сохранить**.

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

Удаление группы сотрудников

Чтобы удалить группу сотрудников:

1. Перейдите к разделу **Группы сотрудников**.
2. Щелкните левой кнопкой мыши по названию нужной группы сотрудников.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - щелкните по выбранной группе правой кнопкой мыши и в контекстном меню выберите **Удалить**;
   - нажмите Ctrl+D.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление группы сотрудников.

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

Добавление учетной записи сотрудника в группу

В результате установки Агента InfoWatch Device Monitor на компьютер (см. "Traffic Monitor. Руководство по установке", статья "Установка Агента InfoWatch Device Monitor"), сведения обо всех пользователях, зарегистрированных на компьютере, автоматически добавляются в схему безопасности, в группу сотрудников "по умолчанию". Соответственно, на всех сотрудников, входящих в группу «по умолчанию», будет распространяться политика безопасности (DM), назначенная данной группе. В дальнейшем определение политик безопасности (DM) для сотрудника происходит путем включения его учетной записи в различные группы компьютеров.

Чтобы перенести сотрудника из одной группы в другую:

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

В результате учетная запись будет включена в выбранную группу.

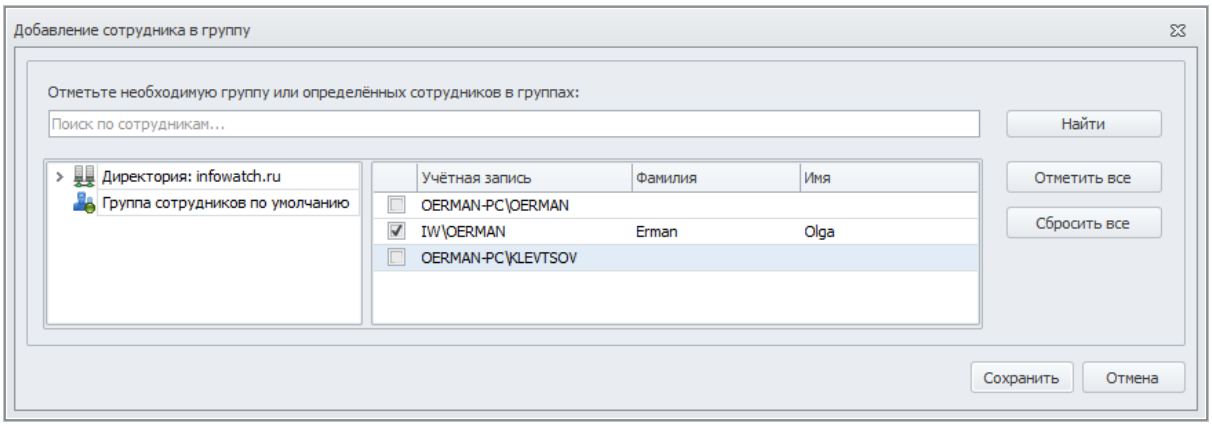
Вы также можете вручную импортировать в Систему информацию о сотруднике из службы каталогов (о настройке соединения см. "Соединение с сервером LDAP и синхронизация с сервером Active Directory и Astra Linux Directory"). Тогда после регистрации данного сотрудника на компьютере, где установлен Агент InfoWatch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

Чтобы добавить одну или несколько учетных записей, импортированных из службы каталогов или уже зарегистрированных в Системе, в группу сотрудников:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** на Панели навигации выберите название группы, в которую нужно добавить учетную запись сотрудника.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить сотрудника**;
   - воспользуйтесь кнопкой **Добавить сотрудника**, расположенной в верхней части области **Сотрудники**;
   - нажмите правой кнопкой мыши в рабочей области и из раскрывшегося контекстного меню выберите **Добавить сотрудника**.

   В результате на экран будет выведено диалоговое окно добавления сотрудников, где отображается список учетных записей, импортированных из службы каталогов (см. "Соединение с сервером LDAP и синхронизация с сервером Active Directory и Astra Linux Directory"), а также уже зарегистрированных в системе (например, при установке Агента Device Monitor на компьютеры) и принадлежащих существующим группам сотрудников

Device Monitor.



4. Чтобы добавить сотрудника, в левой области выберите необходимый узел в дереве групп, затем отметьте учетные записи, которые нужно добавить в редактируемую группу.
   Чтобы отметить все учетные записи, принадлежащие выбранному узлу, нажмите **Отметить все**. Чтобы снять выделение, нажмите **Сбросить все**.
   Вы также можете выполнить поиск учетной записи по всем доступным элементам. Для этого в верхней строке введите часть имени учетной записи и нажмите **Найти**.
5. После того, как вы выбрали все необходимые учетные записи, нажмите **Сохранить**, чтобы закрыть окно **Добавление сотрудника в группу** и вернуться в окно настройки параметров группы.
6. Нажмите **Сохранить**.

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

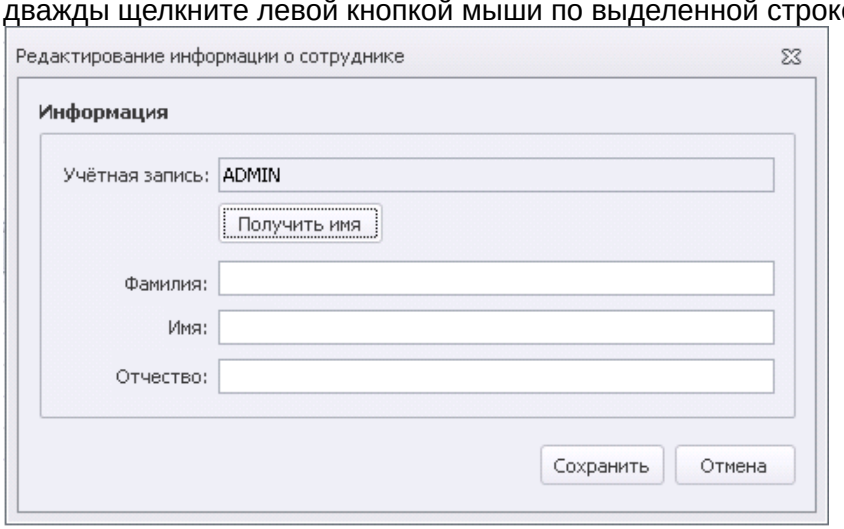
Редактирование учетной записи сотрудника

Параметры учетной записи сотрудника могут быть импортированы из службы каталогов или при установке Агента InfoWatch Device Monitor на компьютер, где этот сотрудник зарегистрирован. Если вы хотите дополнить полученные данные, то вы можете внести ФИО сотрудника, как описано ниже.

Чтобы отредактировать учетную запись сотрудника:

1. Перейдите к разделу **Группы сотрудников**.
2. В области **Группы сотрудников** на Панели навигации выберите название группы сотрудников, в которую входит нужная учетная запись.
3. Выберите строку с именем учетной записи, которую нужно отредактировать.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить** из нижней части раскрывающегося списка;
   - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части области Сотрудники;

- дважды щелкните левой кнопкой мыши по выделенной строке.



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

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

Исключение учетной записи сотрудника из группы сотрудников

Чтобы исключить учетную запись сотрудника из группы сотрудников:

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

> **Примечание:**
>
> Чтобы исключить несколько учетных записей из группы сотрудников, выберите строки с именами всех учетных записей сотрудников, которые нужно исключить из данной группы. Для выбора нескольких строк используйте клавиши Stift или Ctrl. Чтобы выделить все строки, нажмите Ctrl+A.

4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Исключить сотрудника из группы**;

- воспользуйтесь кнопкой **Исключить сотрудника из группы**, расположенной в верхней части области **Сотрудники**;
- щелкните по строке правой кнопкой мыши и в контекстном меню выберите **Исключить сотрудника из группы**;
- нажмите кнопку клавиатуры **Delete**.

После этого учетная запись сотрудника будет исключена из выбранной группы сотрудников.

> **Примечание:**
>
> Если учетная запись сотрудника входит только в одну группу сотрудников, то при исключении из группы такая учетная запись будет автоматически добавлена в группу сотрудников «по умолчанию».

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

Удаление учетной записи сотрудника из схемы безопасности

Чтобы удалить учетную запись сотрудника из схемы безопасности:

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

   > **Примечание:**
   >
   > Чтобы удалить несколько учетных записей из схемы безопасности, выберите строки с именами всех учетных записей, которые нужно удалить.

4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить сотрудника из схемы безопасности**;
   - воспользуйтесь кнопкой **Удалить сотрудника из схемы безопасности**, расположенной в верхней части области **Сотрудники**;
   - щелкните по строке правой кнопкой мыши и в контекстном меню выберите **Удалить сотрудника из схемы безопасности**;
   - нажмите сочетание клавиш клавиатуры **Shift+Delete**.
5. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление учетной записи.

Важно!

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

Компьютеры

Под компьютерами в системе InfoWatch Device Monitor понимаются контролируемые компьютеры, на которых установлены Агенты InfoWatch Device Monitor.

Основные принципы работы с компьютерами описываются в разделе "Компьютеры и группы компьютеров".

Действующие политики безопасности (DM) могут быть назначены только группе компьютеров. Определение политики безопасности (DM) для отдельного компьютера выполняется путем включения компьютера в ту или иную группу.

Важно!

На каждый компьютер, помимо политики безопасности (DM), назначенной группе компьютеров, также распространяется и политика безопасности (DM), определенная для сотрудника, который в данный момент авторизован на компьютере. О порядке определения приоритетов при пересечении правил (DM) см. "Применение правил (DM)".

Чтобы перейти к разделу Консоли управления (DM), предназначенному для управления компьютерами, воспользуйтесь кнопкой **Группы компьютеров**, расположенной на Панели навигации.

Информация по работе с контролируемыми компьютерами содержится в подразделах:

- Просмотр сведений о компьютерах;
- Просмотр результирующих политики и белого списка на компьютерах;
- Создание и редактирование группы компьютеров;
- Удаление группы компьютеров;
- Добавление компьютера в группу;
- Исключение компьютера из группы;
- Удаление компьютера из схемы безопасности;
- Обновление Агентов на контролируемых компьютерах;
- Диагностика рабочей станции.

Просмотр сведений о компьютерах

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

Примечание.

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

Чтобы просмотреть список компьютеров, входящих в группу, на панели **Группы компьютеров** выберите название нужной группы: перечень компьютеров, входящих в нее, отобразится в рабочей области.
Чтобы просмотреть список всех зарегистрированных компьютеров, воспользуйтесь кнопкой  **Показать все компьютеры**, расположенной в верхней части Панели навигации.

Информация по компьютерам представлена в виде табличного списка. В столбцах выводятся основные свойства компьютеров. Вы можете менять порядок столбцов, а также скрывать столбцы, отображать которые не требуется.

Табличный список содержит следующие основные сведения:

- **Имя**. Доменное имя рабочей станции.
- **Статус**. Состояние контролируемого компьютера и Агента. Данный параметр может принимать одно из следующих значений:
  -  **Работает нормально**. Контролируемый компьютер включен, Агент запущен.
  -  **Неактивен**. Контролируемый компьютер выключен либо долгое время недоступен. Этот же статус отображается после удаления Агента с контролируемого компьютера.
- **Время установки**. Дата и время первого обращения Агента, установленного на компьютере, к Серверу.
- **Время подключения**. Дата и время запуска Агента на компьютере.
- **Последнее обращение**. Дата и время последнего обращения Агента, установленного на компьютере, к Серверу.
- **Версия схемы**. Номер версии схемы безопасности, загруженной на Агент.
- **Версия Агента**. Номер версии Агента, установленного на компьютере.
- **Операционная система**. Версия операционной системы.
- **Комментарий.** Поле ввода текста комментария.
- **IP-адрес.** IP-адрес рабочей станции.
- **Пользователь.** Имя пользователя, заходившего на рабочую станцию последним.

> **Примечание**
>
> Комментарий рабочей станции сохраняется немедленно при редактировании, не изменяя версии схемы безопасности. При этом необходимо учитывать следующие ограничения:
>
> - при изменении комментария существующей рабочей станции он записывается в БД немедленно даже при редактировании схемы безопасности;
> - при изменении комментария только что добавленной рабочей станции он будет сохранен только при сохранении схемы безопасности.

Расширенная информация по свойствам компьютера выводится на панели **Подробно**.

Чтобы просмотреть свойства отдельного компьютера, в рабочей области главного окна выберите строку с описанием нужного компьютера.

На панели **Подробно** будет отображена таблица свойств, в которой содержатся дополнительные (к указанным выше) сведения по выбранному компьютеру:

- **Версия настроек**. Версия общих настроек политики безопасности (DM) (см. "Общие настройки политики безопасности").
- **Версия шаблонов**. Версия шаблонов уведомлений, которые могут быть показаны пользователю.

- **Версия настроек контроля сети**. Версия настроек контроля передачи данных по сетевым соединениям с помощью Network Monitor (см. "Контроль сетевых соединений").
- **Версия настроек контроля сетевых приложений**. Версия настроек контроля сетевого трафика, передаваемого по протоколам XMPP, MMP, FTP, FTPS, SMTP/S/MIME/Outlook/POP3, HTTPS (см. "Контроль сетевого трафика").
- **Версия настроек исключений**. Версия настроек исключения приложений из перехвата (см. "Исключение приложений из перехвата"). В скобках указывается номер последней примененной версии.
- **Версия конфигурации ТМ**. Последняя версия конфигурации Traffic Monitor, доставленная на данную рабочую станцию.
- **Свободное место на дисках компьютера**. Размер свободного места на дисках, куда сохраняются теневые копии (в т.ч. в процентах).

Важно!

Если на компьютере осталось меньше свободного места, чем определено политикой (DM) (см. "Создание теневых копий и запрет операций при нехватке свободного места"), то теневые копии сохраняться не будут.

Примечание.

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

Каждый зарегистрированный компьютер автоматически добавляется в группу компьютеров «по умолчанию». При этом компьютеру назначается политика безопасности (DM), определенная для группы компьютеров «по умолчанию».
В процессе работы вы можете выполнять следующие действия:

- управлять группами компьютеров:
  - добавлять группы компьютеров;
  - редактировать параметры групп компьютеров;
  - удалять группы компьютеров.
- управлять компьютерами:
  - добавлять информацию о компьютерах в группу компьютеров и тем самым определять политику безопасности;
  - исключать компьютеры из группы компьютеров;
  - удалять компьютеры из схемы безопасности;
  - обновлять Агенты на контролируемых компьютерах.

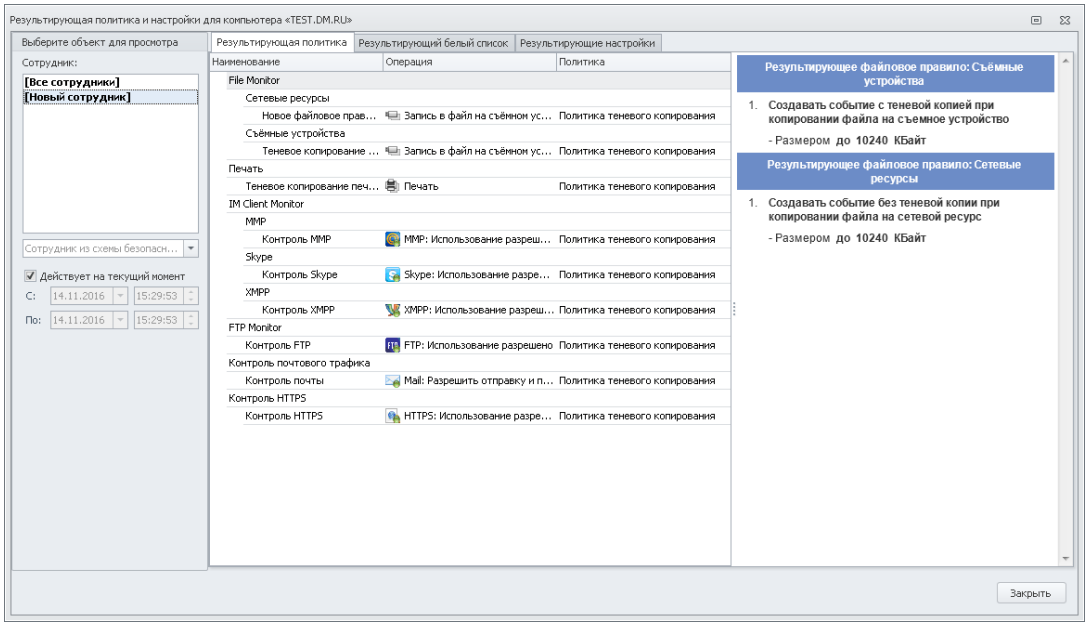
Просмотр результирующих настроек, политик (DM) и белого списка на компьютере

Чтобы посмотреть информацию о настройках, политике (DM) и белом списке, действующих на компьютере:

1. В списке компьютеров выберите название нужного.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Показать настройки и результирующую политику**.

- на панели Компьютеры нажмите **Показать настройки и результирующую политику**.

В результате на экран будет выведено окно **Результирующая политика и настройки для компьютера: <имя компьютера>**, где по умолчанию отображается результирующая политика (DM) для всех сотрудников на выбранном компьютере.



Основная область окна **Результирующая политика и настройки для компьютера** содержит три вкладки:

- **Результирующая политика** - отображаются правила (DM), являющиеся результирующими на компьютере. Результирующая политика (DM) складывается из правил (DM), настроенных по умолчанию, правил (DM), заданных для данного компьютера, и правил (DM) для сотрудников этого компьютера (см. "Особенности применения правил для Device Monitor"). Чтобы просмотреть подробную информацию по правилу (DM), выберите его из списка: на панели, находящейся справа, отобразится подробная информация о выбранном правиле (DM).
- **Результирующий белый список** - отображаются устройства, являющиеся разрешенными для компьютера (см. "Белые списки"). Чтобы просмотреть подробную информацию об устройстве, выберите его из списка: на панели, находящейся справа, отобразится подробная информация о выбранном устройстве.
- **Результирующие настройки** - отображаются настройки Скорости отправки данных с агента и Контроля дискового пространства на агентах, являющиеся результирующими на компьютере. Результирующие настройки складываются из настроек по умолчанию и настроек для группы компьютеров, в которую входит выбранный компьютер (см. "Общие настройки работы агентов" и "Создание и редактирование группы компьютеров").

На панели **Сотрудник** вы можете выбрать объект для просмотра:

- **Все сотрудники** - при выборе отображается результирующая политика\белый список\настройки для всех сотрудников, вне зависимости от того, кто выполнил вход на выбранный компьютер.

- **Новый сотрудник** - при выборе отображается результирующая политика\белый список\настройки на выбранном компьютере для нового сотрудника (которого еще нет в схеме безопасности).
- Чтобы просмотреть результирующую политику\белый список\настройки для определенного пользователя:
  - из списка **Сотрудник** выберите имя учетной записи, зарегистрированной на выбранном компьютере
    или
  - из раскрывающегося списка **Сотрудник** из схемы безопасности выберите любую учетную запись, зарегистрированную в Системе (см. "Сотрудники").

Вы можете выбрать время, для которого будет показана результирующая политика\белый список\настройки:

- по умолчанию выбрана настройка **Действует на текущий момент** и отображаются текущие результирующие политика\белый список\настройки;
- чтобы просмотреть результирующие политику\белый список\настройки за интересующий вас период времени, снимите отметку с поля **Действует на текущий период** и укажите необходимый временной промежуток.

Создание и редактирование группы компьютеров

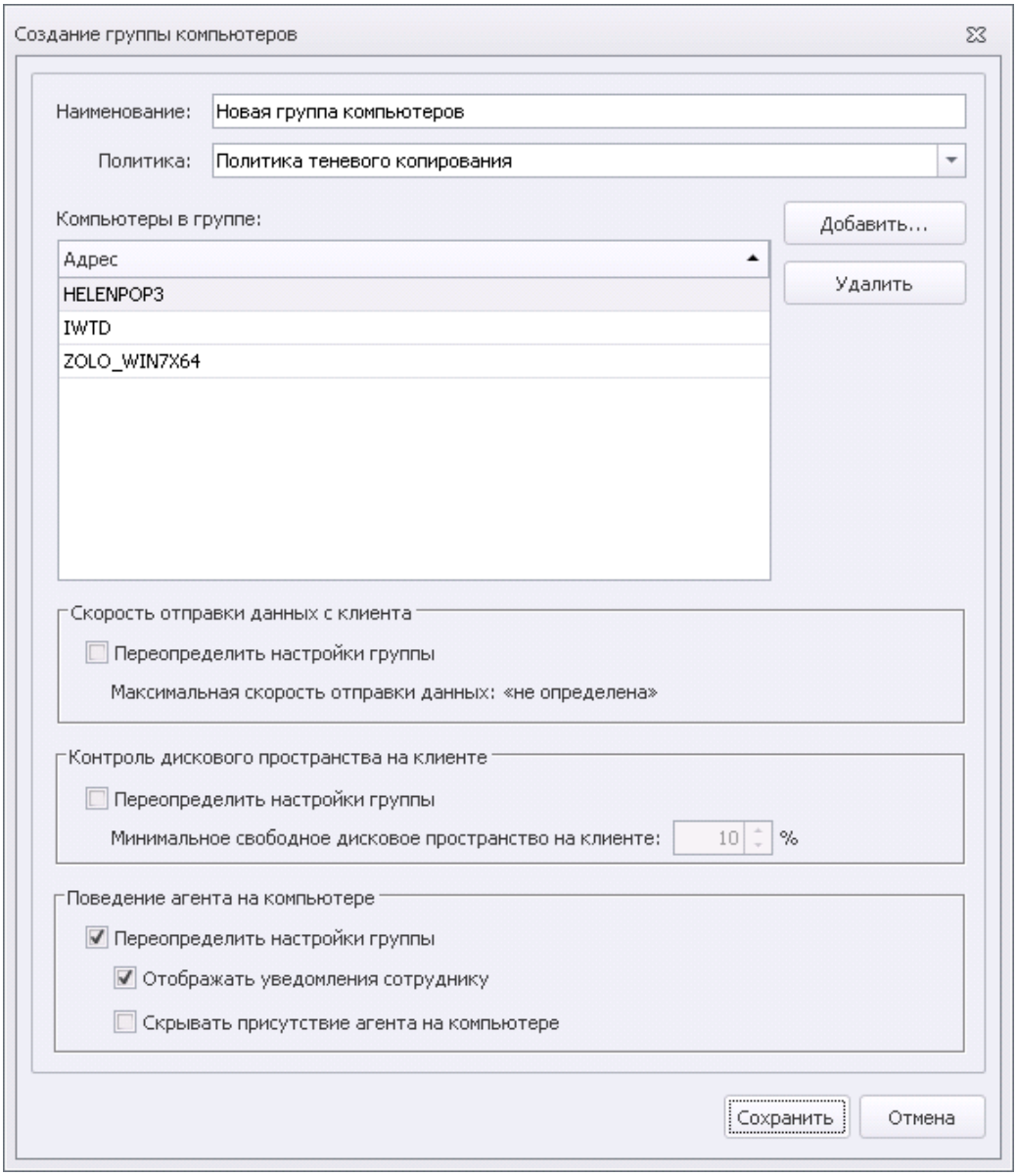
> **Важно!**
>
> Когда регистрируется новый компьютер, информация о нем автоматически добавляется в схему безопасности (в группу компьютеров «по умолчанию»).

Чтобы добавить группу компьютеров:

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

Действие	Шаги
Добавить группу компьютеров	- в главном меню выберите команду **Правка** > **Создать группу компьютеров**; - воспользуйтесь кнопкой **Создать группу компьютеров**, расположенной в верхней части Панели навигации.
Отредактировать группу компьютеров	a. В области **Группы компьютеров** на Панели навигации выберите название нужной группы компьютеров. b. Выполните одно из следующих действий: - в главном меню выберите команду **Правка** > **Изменить** - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации; - дважды щелкните левой кнопкой мыши по названию выделенной группы компьютеров.

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



3. Укажите следующие параметры:
   - **Наименование**.
   - **Политика**. Выберите из раскрывающегося списка политику безопасности (DM), которая будет назначена данной группе компьютеров.
4. Определите перечень компьютеров в группе:

- Чтобы добавить один или несколько компьютеров, нажмите **Добавить**. В открывшемся окне вы можете выбрать компьютеры:
  - из директории;
  - из сетевого окружения Microsoft Windows Network;
  - из числа ранее зарегистрированных в системе (например, в результате ручной установки Агента Device Monitor) и уже принадлежащих существующим группам Device Monitor.

  В левой области выберите необходимый узел в дереве групп, затем отметьте компьютеры, которые нужно добавить в редактируемую группу.
  Вы также можете выполнить поиск компьютера по директории. Для этого в верхней строке введите часть имени компьютера и нажмите **Найти**.
  После того, как все необходимые компьютеры выбраны, нажмите Сохранить, чтобы закрыть окно добавления и вернуться к окну настройки параметров группы.
- Чтобы удалить компьютер из группы, выберите его и нажмите **Удалить**.

5. Вы можете назначить для компьютеров, входящих в группу, собственную максимальную скорость отправки данных с Агента (об общих значениях см. "Общие настройки работы Агентов", параметр **Ограничивать скорость отправки данны**х). Для этого:
   a. в области **Скорость отправки данных с агента** выберите настройку Переопределить настройки группы;
   b. в поле **Максимальная скорость отправки данных** укажите необходимое значение, в Кбит/с.

   По умолчанию настройка не выбрана.
6. Вы можете назначить для компьютеров, входящих в группу, другое значение минимального размера свободного пространства на контролируемом компьютере, при достижении которого теневые копии не будут создаваться (об общих значениях см. "Общие настройки работы Агентов", параметр **Минимальное свободное пространство на агенте**). Для этого:
   a. в области **Контроль дискового пространства на агенте** выберите настройку **Переопределить настройки группы**;
   b. в поле **Минимальное свободное дисковое пространство на агенте** укажите необходимое значение, в процентах.

   По умолчанию настройка не выбрана.
7. Вы можете назначить для компьютеров, входящих в группу, другой режим сокрытия Агента на контролируемом компьютере (об общих значениях см. "Общие настройки работы Агентов", группа параметров **Поведение Агента на компьютере**). Для этого:
   a. в области **Поведение Агента на компьютере** выберите настройку **Переопределить настройки группы**;
   b. определите, должны ли быть отмечены настройки **Отображать уведомления сотруднику** и **Скрывать присутствие агента на компьютере**.

   По умолчанию настройка не выбрана.
8. Нажмите **Сохранить**.

Важно!

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

Удаление группы компьютеров

Чтобы удалить группу компьютеров:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - щелкните по названию выделенной группы правой кнопкой мыши и в контекстном меню выберите **Удалить**;
   - нажмите Ctrl+D.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление группы.

   Важно!

   В группе компьютеров, которую вы удаляете, могут быть компьютеры, не включенные в другие группы. Такие компьютеры при удалении единственной группы, в которую они были включены, будут автоматически добавлены в группу компьютеров «по умолчанию».

5. Нажмите на кнопку **ОК**.

Важно!

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

Добавление компьютера в группу

При установке Агента InfoWatch Device Monitor на компьютер (см. "Traffic Monitor. Руководство по установке", статья "Установка Агента InfoWatch Device Monitor"), в Системе автоматически создается запись о компьютере. Эта запись добавляется в группу "по умолчанию". Соответственно, на все компьютеры, входящие в группу «по умолчанию», будет распространяться политика безопасности (DM), назначенная данной группе. В дальнейшем определение политик безопасности (DM) для компьютера происходит путем его включения в различные группы компьютеров.

Чтобы скопировать компьютер из одной группы в другую:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы, в состав которой входит нужный компьютер.
3. В области **Компьютеры** выберите строку с именем компьютера, который нужно добавить в другую группу. Щелкните левой кнопкой мыши по выделенной строке и, не отпуская кнопку, перетащите компьютер в область **Группы компьютеров** на Панели навигации. Подведите курсор мыши к названию той группы, куда нужно добавить компьютер. После того как слева от названия выбранной группы появится желтая стрелка, отпустите левую кнопку мыши.

В результате компьютер будет включен в выбранную группу.

Вы также можете вручную добавить в Систему информацию о рабочей станции, на которой еще не установлен Агент InfoWatch Device Monitor. Информация о рабочей станции импортируется из службы каталогов (о настройке соединения см. "Соединение с сервером LDAP и синхронизация с сервером Active Directory и Astra Linux Directory") или из сетевого окружения. Тогда после установки Агента InfoWatch Device Monitor на такую рабочую станцию (см. "Создание задачи первичного распространения"), на нее будет распространяться политика (DM) той группы, в которую она была добавлена.

> **Важно!**
>
> Настоятельно не рекомендуется добавлять компьютеры с одинаковыми именами. В системе InfoWatch Device Monitor такие компьютеры будут зарегистрированы как один и, соответственно, на них будет распространяться одна политика (DM), будет вестись единая регистрация событий и т.д.

Чтобы добавить компьютер в группу:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы. После этого в рабочей области главного окна будет выведен список всех компьютеров, уже входящих в группу.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить компьютер**;
   - воспользуйтесь кнопкой **Добавить компьютер**, расположенной в верхней части области Компьютеры;
   - нажмите правой кнопкой мыши в рабочей области и из раскрывшегося контекстного меню выберите **Добавить компьютер**.

   В открывшемся диалоговом окне вы можете выбрать компьютеры:
   - из директории;
   - из сетевого окружения Microsoft Windows Network;
   - из дерева ALD;
   - из числа ранее зарегистрированных в Системе.
4. Отметьте необходимые компьютеры или группы компьютеров. Свернутые группы отмечены пиктограммой ; развернутые - . Чтобы развернуть или свернуть группу, дважды нажмите на ней левой кнопкой мыши.
   Вы также можете указать имя компьютера в строке внизу диалогового окна. При перечислении нескольких имен разделяйте их точкой с запятой.
5. Нажмите **Сохранить**.

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

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

Исключение компьютера из группы

Включение компьютера в определенную группу компьютеров влечет за собой назначение этому компьютеру политик безопасности (DM) выбранной группы. Поэтому если вам понадобится отменить действие какой-либо политики безопасности (DM) на компьютер, исключите его из группы, которой назначена эта политика безопасности (DM).

> **Примечание.**
>
> Если компьютер входит только в одну группу, то при исключении он будет автоматически добавлен в группу компьютеров «по умолчанию».

Чтобы исключить компьютер из группы компьютеров:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы, куда входит нужный компьютер. После этого в рабочей области главного окна будет выведен список всех компьютеров, включенных в выбранную группу.
3. Выберите строку с именем компьютера, которого нужно исключить из группы компьютеров.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Исключить компьютер из группы**;
   - воспользуйтесь кнопкой **Исключить компьютер из группы**, расположенной в верхней части области **Компьютеры**;
   - щелкните по компьютеру правой кнопкой мыши и в контекстном меню выберите **Исключить компьютер из группы**;
   - нажмите кнопку клавиатуры **Delete**.

После этого компьютер будет исключен из группы.

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

Удаление компьютера из схемы безопасности

Компьютер может быть выведен из списка зарегистрированных (например, эксплуатация рабочей станции прекращена). Сведения о таком компьютере не будут удалены, но, так как Агент на ней отключен, то компьютеру присваивается статус **Неактивен**.

Если сохранение информации о неактивном компьютере не требуется, то вы можете удалить запись о нем.

Чтобы удалить компьютер из схемы безопасности:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы компьютеров, в которую входит нужный компьютер.
3. В рабочей области главного окна выберите строку с названием неактивного компьютера, который нужно удалить.
4. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить компьютер из схемы безопасности**;
   - воспользуйтесь кнопкой **Удалить компьютер из схемы безопасности**, расположенной в верхней части области Компьютеры;
   - щелкните правой кнопкой на строке необходимого компьютера и из раскрывшегося списка выберите **Удалить компьютер из схемы безопасности**;
   - нажмите сочетание клавиш клавиатуры **Shift+Delete**.
5. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление.

В результате сведения о компьютере будут удалены из всех групп, в которые входил данный компьютер.

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

Обновление Агентов на контролируемых компьютерах

Для контролируемых компьютеров доступно упрощенное создание задачи обновления Агентов Device Monitor (подробнее об этом типе задач см. "Удаленная установка, обновление и удаление Агентов" и "Создание задачи обновления").

Чтобы обновить Агенты Device Monitor на всех контролируемых компьютерах, входящих в группу:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы.
3. Воспользуйтесь кнопкой **Обновить все компьютеры**, расположенной в верхней части Панели навигации.

Чтобы обновить Агенты Device Monitor выбранных контролируемых компьютерах:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название необходимой группы компьютеров.
3. В области **Компьютеры** выберите строку с именем одного или нескольких контролируемых компьютеров. Для выбора нескольких компьютеров отмечайте их, зажав клавишу **Shift** или **Ctrl**.

4. Воспользуйтесь кнопкой **Обновить компьютеры**, расположенной в верхней части области **Компьютеры**.

В результате выполнения любого из этих действий будет создана и автоматически запущена задача обновления для выбранных компьютеров.

Диагностика рабочей станции

Система предоставляет возможность удаленного сбора диагностических данных с рабочих станций.

Чтобы запустить сбор диагностической информации на рабочей станции:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы, в которую входит необходимая рабочая станция.
3. В списке компьютеров нажмите правой кнопкой мыши на название нужной рабочей станции и из раскрывшегося контекстного меню выберите команду **Диагностика** > **Включение диагностического режима**.

Чтобы остановить сбор диагностической информации на рабочей станции:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы, в которую входит необходимая рабочая станция.
3. В списке компьютеров нажмите правой кнопкой мыши на название нужной рабочей станции и из раскрывшегося контекстного меню выберите команду **Диагностика** > **Выключение диагностического режима**.

Чтобы получить архив файлов со всеми имеющимися диагностическими данными:

1. Перейдите к разделу **Группы компьютеров**.
2. В области **Группы компьютеров** на Панели навигации выберите название группы, в которую входит необходимая рабочая станция.
3. В списке компьютеров нажмите правой кнопкой мыши на название нужной рабочей станции и из раскрывшегося контекстного меню выберите команду **Диагностика** > **Собрать диагностическую информацию**.
4. В окне **Выберите путь сохранения архива с диагностической информацией** укажите папку и имя файла архива.
5. В открывшемся окне с уведомлением об успешном сборе нажмите **ОК.**

Белые списки устройств

Для управления списками устройств, доступ к которым безусловно разрешен (сотруднику, группе сотрудников, компьютеру или группе компьютеров), предназначен раздел **Белые списки**. Чтобы перейти к этому разделу, воспользуйтесь кнопкой **Белые списки**, расположенной на Панели навигации.

Информация по работе с белыми списками содержится в подразделах:

- Просмотр сведений о белых списках
- Добавление белого списка
- Установка периода действия записи
- Редактирование белого списка
- Удаление белого списка

Вы можете просмотреть информацию о действующих белых списках как описано в разделах "Просмотр результирующих политик (DM) и белого списка для сотрудника" и "Просмотр результирующих настроек, политик (DM) и белого списка на компьютере".

Просмотр сведений о белых списках

В области Белые списки на Панели навигации выводится перечень белых списков. В рабочей области главного окна отображается список устройств (моделей и экземпляров), входящих в состав выделенного белого списка.

> **Примечание.**
>
> Вы можете выполнять поиск в перечне белых списков, вводя наименование списка в строке поиска, находящейся под перечнем в Панели навигации.
>
> Для выбранного белого списка можно настроить его отображение при помощи дополнительных функций (см. "Дополнительные возможности").

Чтобы просмотреть информацию по отдельному белому списку, выберите название нужного белого списка группы в перечне белых списков.

Информация по белым спискам представлена в виде списка устройств, сгруппированного по их типам. Каждая строка списка соответствует одной модели или экземпляру устройства. В столбцах выводятся общие свойства устройств. Расширенная информация по свойствам устройства выводится на панели **Подробно**.

Чтобы просмотреть подробную информацию по свойствам отдельного устройства, выберите строку с названием нужной модели или экземпляра устройства.

В результате на панели **Подробно** будет отображена таблица свойств, в которой вы сможете просмотреть следующую информацию:

- **Идентификатор экземпляра или модели устройства**. Код модели (VID – Vendor ID) или серийного номера экземпляра (PID – Product ID) устройства.
- **Описание устройства**.
- **Тип устройств**.
- **Категория**. Модель или экземпляр.
- **Период действия**. Дата и время начала и окончания периода, в течение которого доступ к данному устройству безусловно разрешен.
- **Обнаружено на компьютере**. Имя компьютера, на котором обнаружено устройство.
- **Добавлено в базу данных**. Дата добавления информации об устройстве в базу данных (см. "Добавление устройства в базу").

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

Добавление белого списка

Действие белого списка распространяется на определенный (назначенный) объект: сотрудника, группу сотрудников, компьютер или группу компьютеров.

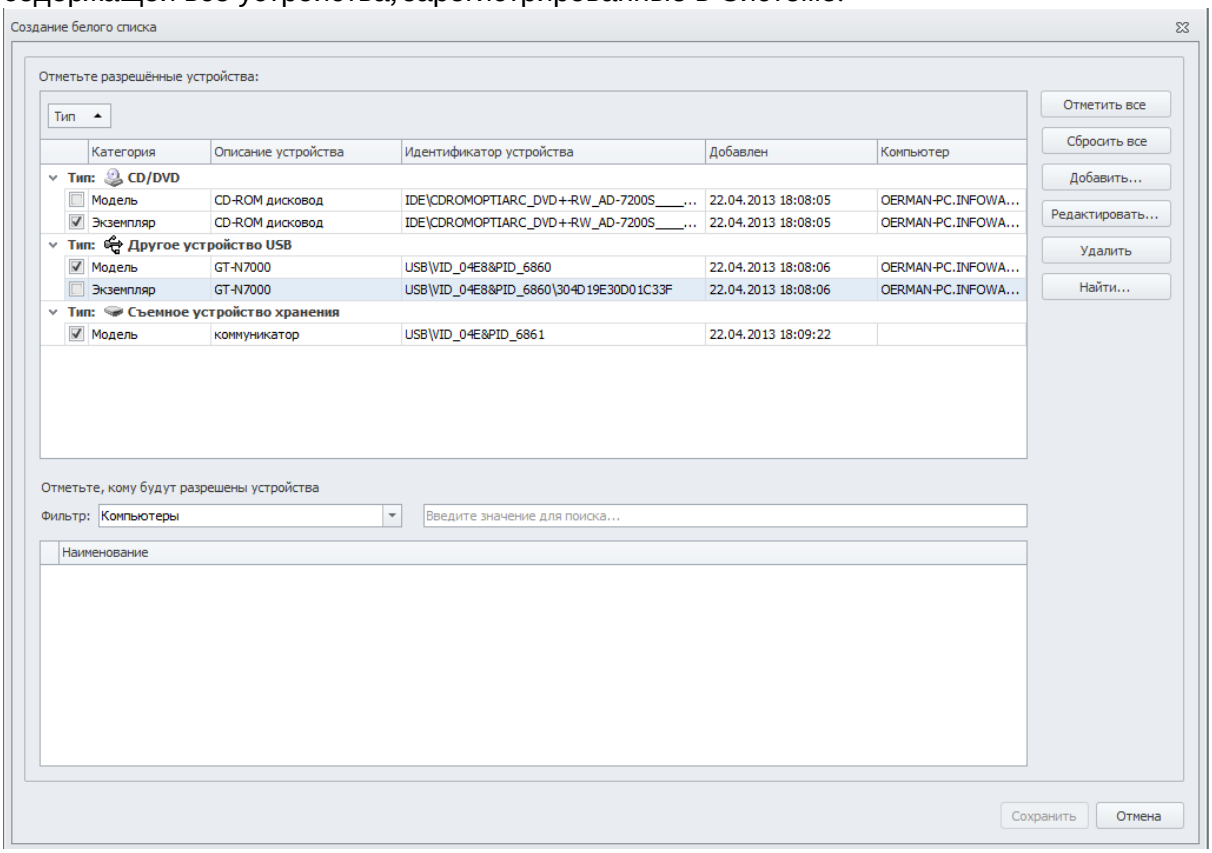
Важно!

Одному объекту назначения (сотруднику, группе сотрудников, компьютеру или группе компьютеров) может быть назначен только один белый список.

Чтобы добавить белый список:

1. Перейдите к разделу **Белые списки**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Создать белый список**;
   - воспользуйтесь кнопкой **Создать белый список**, расположенной в верхней части Панели навигации;
   - щелкните в области **Белые списки** правой кнопкой мыши и в контекстном меню выберите **Создать белый список**;
   - нажмите Ctrl+N.

   На экран будет выведено диалоговое окно **Создание белого списка** с таблицей, содержащей все устройства, зарегистрированные в Системе.



3. В таблице отметьте модели и экземпляры, доступ к которым должен быть безусловно разрешен.

Важно!

Информация о том, как изменять список зарегистрированных моделей и экземпляров устройств, содержится в следующих разделах:
- Добавление записи об устройстве
- Удаление записи об устройстве

4. В области **Отметьте, кому будут разрешены устройства** выберите фильтр: на кого будет распространяться действие белого списка:
   - сотрудники
   - группы сотрудников
   - компьютеры
   - группы компьютеров

   Внизу отобразится перечень записей, соответствующих выбранному фильтру.
   Вы также можете воспользоваться строкой поиска, введя искомое имя или его часть.
5. Выберите сотрудника / группу сотрудников / компьютер / группу компьютеров, на которые должно распространяться действие белого списка.
6. Нажмите **Сохранить**.

Добавление записи об устройстве

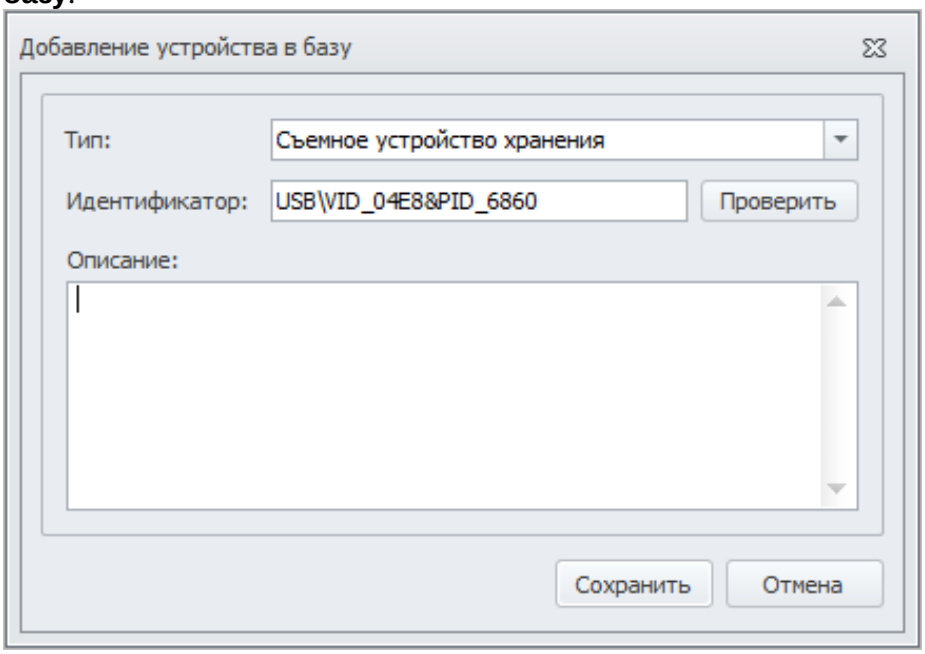
Вы можете включать в белые списки только те модели и экземпляры устройства, информация о которых была предварительно зарегистрирована в системе. Добавить информацию об устройстве вы можете одним из двух способов:

- вручную, если вы знаете идентификатор этого устройства;
- с помощью поиска, если это устройство подключено к контролируемому компьютеру.

Чтобы добавить запись об устройстве вручную:

1. Откройте диалоговое окно **Создание белого списка** (см. "Добавление белого списка").
2. Нажмите кнопку **Добавить**, расположенную в правой части окна.
   В результате на экран будет выведено диалоговое окно **Добавление устройства в**

базу.



3. Укажите параметры устройства:
   - из раскрывающегося списка **Тип** выберите тип устройства;
   - в поле **Идентификатор** введите код экземпляра или модели устройства;

> **Примечание.**
>
> Чтобы узнать код устройства, подключите это устройство и с помощью стандартных средств Windows (например, Диспетчер устройств) просмотрите свойства этого устройства. Код экземпляра устройства отображается на вкладке **Сведения**.
> Код экземпляра устройства имеет вид XXX\YYY\ZZZ, где XXX – тип устройства (обычно - наименование шины, к которой подключено устройство, например, USB, IDE или ACPI), YYY - строка, характеризующая модель устройства (Vendor ID), а ZZZ – строка, характеризующая данный экземпляр устройства (Product ID).
> Код модели устройства имеет вид XXX\YYY, где XXX – тип устройства, а YYY - строка, характеризующая модель (VID).

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

> **Важно!**
>
> При использовании кода экземпляра следует учитывать, что некоторые устройства не имеют уникального идентификатора: идентификатор может

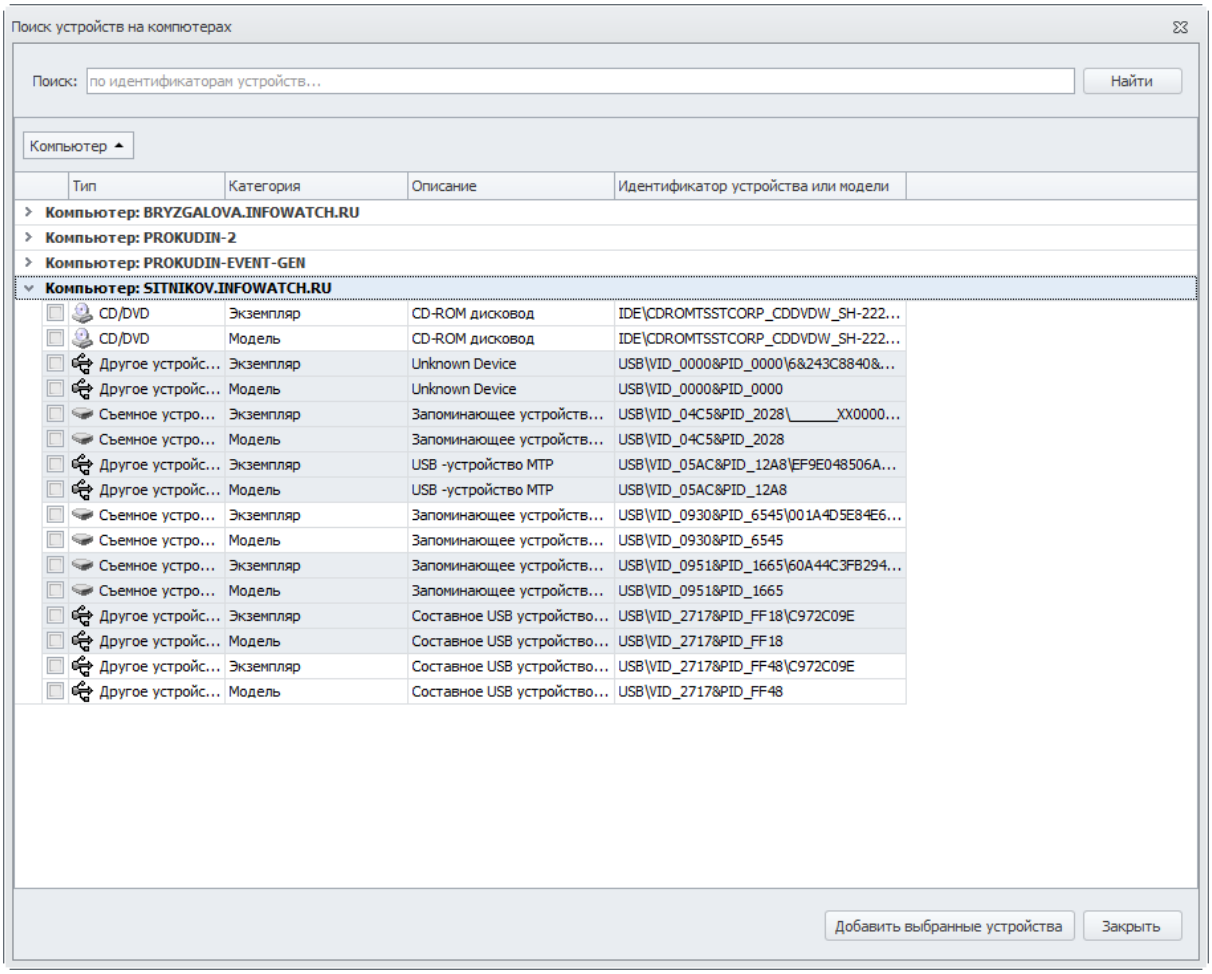
изменяться динамически и отличаться даже при подключении к разным портам одной рабочей станции.
В таких случаях рекомендуется использовать код модели устройства.

- в поле **Описание** введите описание устройства.

4. Нажмите **Сохранить**.

Чтобы добавить запись с помощью поиска устройств, подключавшихся к компьютерам:

1. Откройте диалоговое окно Создание белого списка (см. "Добавление белого списка").
2. Нажмите кнопку **Найти**, расположенную в правой части окна.
   В результате на экран будет выведено диалоговое окно **Поиск устройств на компьютерах**.



3. В списке контролируемых компьютеров выберите необходимый одним из следующих способов:
   - нажмите кнопку , соответствующую необходимому компьютеру;
   - дважды щелкните левой кнопкой мыши на названии компьютера.

   Раскроется список всех устройств, которые подключались к выбранному компьютеру за все время работы Агента Device Monitor на нем.

> **Примечание:**
>
> Следует обратить внимание на то, что подключенные к компьютеру устройства подсвечены в списке белым цветовым фоном, в то время как отключенные выделены серым.

4. Отметьте устройства, информацию о которых вы хотите добавить.
5. Нажмите **Добавить выбранные устройства**.

Удаление записи об устройстве

Чтобы удалить запись о зарегистрированном устройстве из Системы:

1. Откройте диалоговое окно **Создание белого списка** (см. "Добавление белого списка").
2. Выполните одно из следующих действий:
   - в таблице с зарегистрированными устройствами щелкните правой кнопкой мыши по выбранному экземпляру или модели устройства и в контекстном меню выберите **Удалить устройство**.
   - нажмите Ctrl+D.
3. В открывшемся окне подтверждения нажмите **Да**.

Установка периода действия записи

Для каждого экземпляра или модели устройства, внесенного в белый список, разрешение на его использование отображается в виде отдельной записи. По умолчанию эта запись (разрешение) действует в течение практически бесконечного периода времени (с 01.01.1753 по 31.12.9999). Вы можете установить ограничение по времени действия безусловного разрешения на работу с этим устройством. До и после указанного периода работа с устройством будет подчиняться общим правилам работы с устройствами данного типа.

Чтобы установить период действия записи в белом списке:

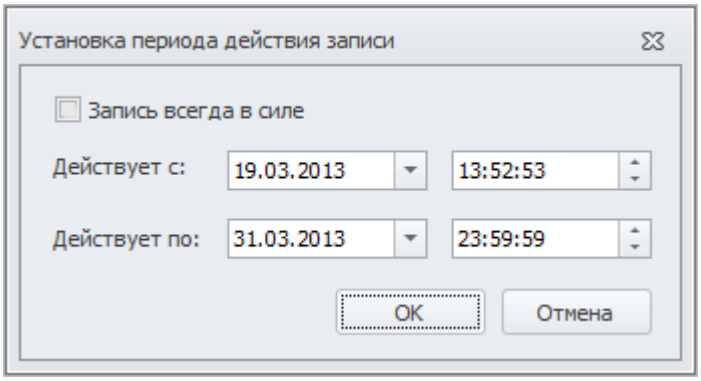
1. Перейдите к разделу **Белые списки**.
2. В области **Белые списки** на Панели навигации выберите название белого списка, куда входит нужная запись.
3. Если записи в белом списке сгруппированы (например, по типу устройств), разверните группу (см. "Группирование записей").

> **Примечание.**
>
> Если установить период действия для всей группы, то изменение вступит в силу только для первой записи в группе.

4. Выделите строку с записью об экземпляре или модели устройства, которому нужно установить период действия, и выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить запись**;
   - воспользуйтесь кнопкой **Изменить запись**, расположенной в верхней части области **Разрешенные устройства**;

- дважды щелкните левой кнопкой мыши по названию выделенной записи;
- щелкните по строке правой кнопкой мыши, затем в раскрывшемся контекстном меню выберите пункт **Изменить запись**;
- нажмите Ctrl+Shift+E.

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



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

Редактирование белого списка

Чтобы отредактировать параметры белого списка:

1. Перейдите к разделу **Белые списки**.
2. В области **Белые списки** на Панели навигации выберите название белого списка.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить**;
   - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации;
   - дважды щелкните левой кнопкой мыши по названию выделенного белого списка;
   - щелкните по названию выделенного белого списка правой кнопкой мыши и в контекстном меню выберите **Изменить**;
   - нажмите Ctrl+E.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно **Редактирование белого списка <Имя списка>**. Содержание этого окна аналогично окну **Создание белого списка**, но область **Отметьте**, кому будут разрешены устройства недоступна для изменения.
4. При необходимости, добавьте или удалите устройства в перечне зарегистрированных в Системе (см. "Добавление устройства в базу" и "Удаление устройства из базы").
   Вы также можете изменить описание ранее зарегистрированного устройства: для этого выберите устройство в перечне и нажмите кнопку **Редактировать**, расположенную в правой части окна. В открывшемся окне отредактируйте текст описания и нажмите **Сохранить**.
5. В таблице с зарегистрированными устройствами отметьте или снимите отметки, чтобы изменить список моделей и экземпляров устройств, включенных в белый список.
6. Нажмите **Сохранить**.

Важно!

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

Удаление белого списка

Чтобы удалить белый список:

1. Перейдите к разделу **Белые списки**.
2. Щелкните левой кнопкой мыши по названию нужного белого списка.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - щелкните по названию выделенного белого списка правой кнопкой мыши и в контекстном меню выберите **Удалить**;
   - нажмите Ctrl+D.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление белого списка.

Важно!

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

Категории сигнатур

Правила (DM) File Monitor можно настроить таким образом, что под правило (DM) будут подпадать только файлы, обладающие структурой, характерной для определенного формата файлов. Для этого в системе InfoWatch Device Monitor предусмотрено определение формата файла по **сигнатуре**.

В разделе Категории сигнатур определен список сигнатур, которые может распознавать Система. Для удобства использования сигнатуры сгруппированы по **категориям**.

Чтобы просмотреть имеющиеся сигнатуры:

1. Перейдите к разделу **Категории сигнатур**, воспользовавшись кнопкой, расположенной на Панели навигации. Вы также можете использовать команду меню **Переход** > **Категории сигнатур** или сочетание клавиш Ctrl+5.
   В области **Категории сигнатур** на Панели навигации будет выведен перечень **категорий**, по которым сгруппированы сигнатуры.
2. Выберите категорию сигнатур из перечня.
   В рабочей области главного окна будет отображен перечень сигнатур, входящих в состав выделенной категории.

Важно!

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

Вы можете:

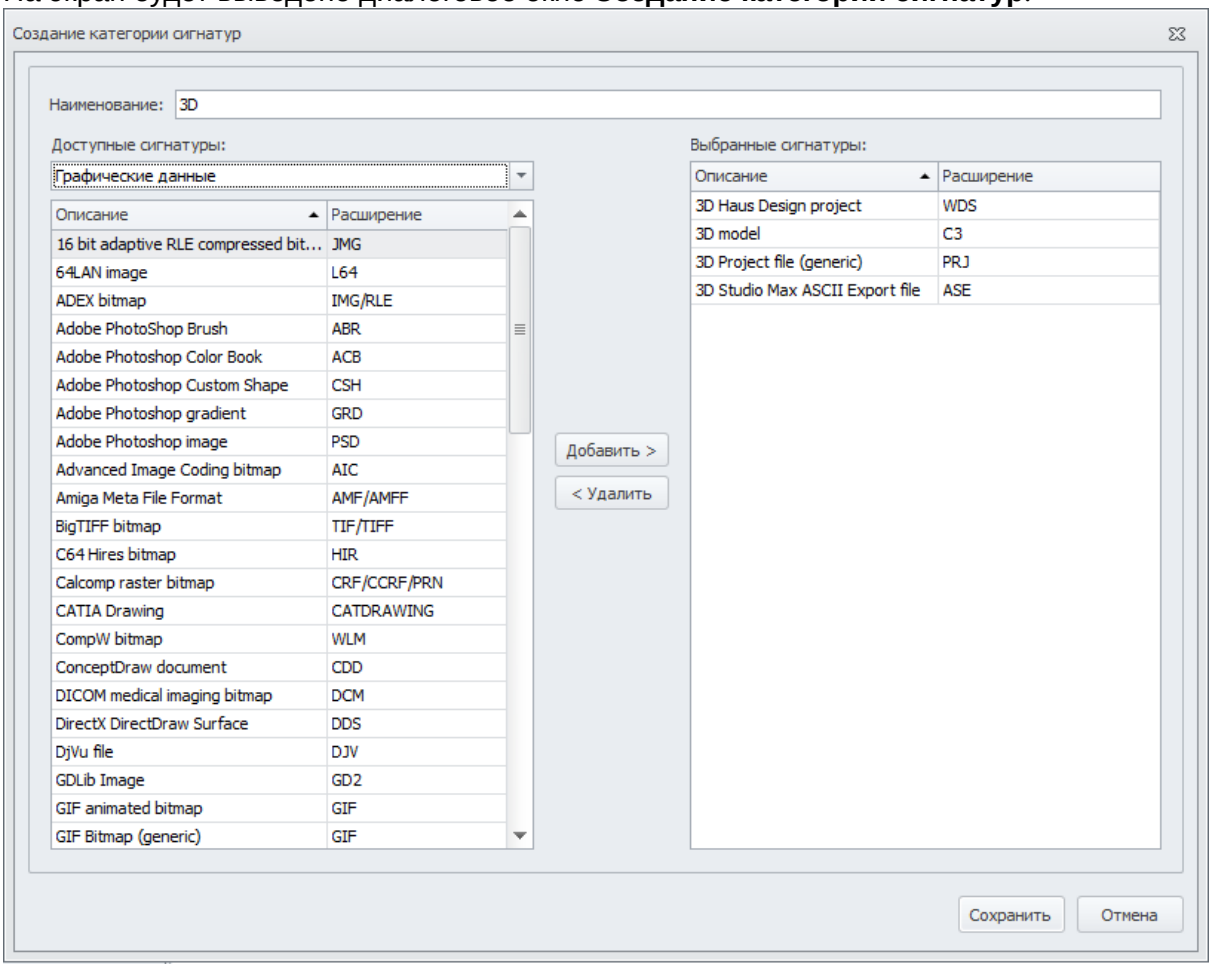
- создавать категории сигнатур;
- наполнять созданные категории, копируя в них сигнатуры из числа предустановленных;
- удалять созданные категории сигнатур, если они не используются ни в одном правиле.

Создание категории сигнатур

Чтобы добавить категорию сигнатур:

1. Перейдите к разделу **Категории сигнатур**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Создать категорию сигнатур**;
   - воспользуйтесь кнопкой **Создать категорию сигнатур**, расположенной в верхней части Панели навигации;
   - щелкните правой кнопкой мыши в области **Категории сигнатур** и в контекстном меню выберите **Создать категорию сигнатур**;
   - нажмите Ctrl+N.

   На экран будет выведено диалоговое окно **Создание категории сигнатур**.



3. В поле **Наименование** введите название создаваемой категории.
4. На панели **Доступные сигнатуры** вы можете выбрать из раскрывающегося списка одну из предустановленных категорий сигнатур. По умолчанию отображаются все предустановленные сигнатуры.
5. На левой панели выберите сигнатуры, которые вы хотите включить в новую категорию. Чтобы выделить несколько сигнатур сразу, используйте клавиши **Ctrl** и **Shift**. Чтобы перенести выбранные сигнатуры в новую категорию, нажмите **Добавить**. Чтобы удалить сигнатуры из списка вносимых в новую категорию, выберите их на правой панели **Выбранные сигнатуры** и нажмите **Удалить**.
6. Нажмите **Сохранить**.

Изменение категории сигнатур

После того, как вы создали категорию сигнатур (см. "Создание категории сигнатур"), вы можете наполнить ее одним из следующих способов:

1. Перейдите в режим редактирования сигнатуры и определите список сигнатур, как описано в разделе "Создание категории сигнатур". Для перехода в режим редактирования выбранной категории выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить**;
   - нажмите кнопку **Изменить** в верхней части Панели навигации;
   - дважды щелкните левой кнопкой мыши по названию выделенной категории;
   - щелкните по по названию выделенной категории правой кнопкой мыши и в контекстном меню выберите **Изменить**;
   - нажмите Ctrl+E.
2. Копировать сигнатуры из других категорий непосредственно в рабочей области Консоли (DM).

Чтобы скопировать сигнатуру из одной категории в другую:

1. Перейдите к разделу **Категории сигнатур**.
2. В области **Категории сигнатур** на Панели навигации выберите название предустановленной категории, которая содержит сигнатуру, которую нужно скопировать.
3. В рабочей области главного окна выберите строку с названием сигнатуры, которую нужно скопировать. Вы можете выделить несколько сигнатур сразу, используя клавиши **Ctrl** и **Shift**.
4. Щелкните левой кнопки мыши по выделенной строке и, не отпуская кнопку, перетащите курсор в область **Категории сигнатур** на Панели навигации. Подведите курсор мыши к названию созданной ранее категории, куда нужно добавить сигнатуры. После того как слева от названия выбранной категории появится желтая стрелка, отпустите левую кнопку мыши.

В результате сигнатура будет скопирована в выбранную категорию.

Чтобы исключить сигнатуру из категории, выберите эту сигнатуру и выполните одно из следующих действий:

- нажмите кнопку **Исключить сигнатуру из категории**, расположенную вверху области **Сигнатуры**;
- щелкните правой кнопкой мыши и в раскрывшемся меню выберите **Исключить сигнатуру из категории**;
- нажмите клавишу **Delete**.

Удаление категории сигнатур

Важно!

Удалению не подлежат:

- категории сигнатур, используемые в каком-либо правиле (DM) File Monitor;
- предустановленные категории сигнатур.

Чтобы удалить категорию сигнатур:

1. Перейдите к разделу **Категории сигнатур**.
2. Щелкните левой кнопкой мыши по названию нужной категории сигнатур.
3. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Удалить**;
   - воспользуйтесь кнопкой **Удалить**, расположенной в верхней части Панели навигации;
   - щелкните по по названию выделенной категории правой кнопкой мыши и в контекстном меню выберите **Удалить**;
   - нажмите Ctrl+D.
4. В появившемся окне запроса нажмите на кнопку **Да**, чтобы подтвердить удаление категории сигнатур.

Важно!

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

Приложения

После установки Агента InfoWatch Device Monitor на рабочую станцию и перезагрузки этого компьютера Система автоматически начинает получать информацию о приложениях, запускаемых на контролируемых рабочих станциях.

Информация обо всех запусках и установках формирует *протокол приложений*.

Важно!

Протокол приложений исключает приложения, которые являются критичными для работы компьютера. Это необходимо для того, чтобы офицер безопасности не мог запретить приложение, без которого компьютер перестанет функционировать в штатном режиме.

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

В этом разделе Панель навигации разделена на две группы элементов: **Списки приложений** и **Протокол приложений**:

- Группа элементов **Списки приложений** содержит списки, используемые для контроля доступа сотрудников к приложениям:
  - запрет запуска приложений в режиме черных и белых списков: подробнее см. "Правило (DM) для Application Monitor";
  - запрет создания снимков экрана сотрудником: подробнее см. "Правило (DM) для ScreenShot Control Monitor";
  - автоматическое создание снимков экранов Системой: подробнее см. "Правило (DM) для ScreenShot Monitor".
- Группа элементов **Протокол приложений** позволяет создавать фильтры для просмотра информации обо всех приложениях, запускаемых на контролируемых рабочих станциях. Отсюда можно добавлять приложения в списки.

Информация о работе с протоколами и списками приложений содержится в подразделах:

- Создание и изменение списка приложений
- Создание и изменение фильтра приложений
- Добавление приложения в список автоматически
- Добавление приложения в список вручную
- Экспорт протокола приложений

Создание и изменение списка приложений

Для управления черными и белыми списками, Система поддерживает функционал создания списков приложений из **Протокола приложений** (см. "Протокол приложений").

Списки используются для разрешения или запрещения запуска определенных приложений на компьютерах.

Чтобы создать пустой список приложений:

1. Перейдите к разделу **Приложения**.
2. На Панели навигации установите курсор в группе элементов **Списки приложений** и выполните одно из следующих действий:
   - в меню группы элементов **Списки приложений** нажмите **Создать список приложений**;
   - в главном меню выберите команду **Правка** > **Создать список приложений**;
   - нажмите правой кнопкой мыши в группе элементов **Списки приложений** и из раскрывшегося списка выберите **Создать список приложений**;
   - нажмите Ctrl+N.
3. В поле **Наименование списка** введите название для списка.
4. Нажмите **Сохранить**.

О наполнении списков, а также о создании списков из протокола приложений см. "Добавление приложения в список автоматически" и "Добавление приложения в список вручную".

Чтобы выбрать приложение из списка:

1. Перейдите к разделу **Приложения**.
2. Установите курсор в группе элементов **Списки приложений**.
3. Нажмите кнопку на панели **Список приложений**.
4. Выберите приложение из списка/списков и нажмите **Добавить приложение в список**.
5. Из раскрывающегося списка выберите **Добавить автоматически** или **Выбрать вручную**.

Чтобы отредактировать приложение в списке:

1. На панели **Список приложений** нажмите  либо щелкните по приложению правой кнопкой мыши и в контекстном меню выберите **Изменить**.
2. Здесь вы можете настроить параметры, которые будут использованы для фильтрации приложений (см. "Добавление приложения в список вручную")

Чтобы удалить приложение из списка:

1. На панели **Список приложений** нажмите  либо щелкните по приложению правой кнопкой мыши и в контекстном меню выберите **Удалить**.
2. Нажмите **Да**, чтобы удалить приложение из схемы безопасности.

Создание и изменение фильтра приложений

Фильтры позволяют настроить формирование протокола приложений (см. "Приложения") так, что будет отображаться информация только о приложениях, соответствующих выбранным вами условиям.

Важно!

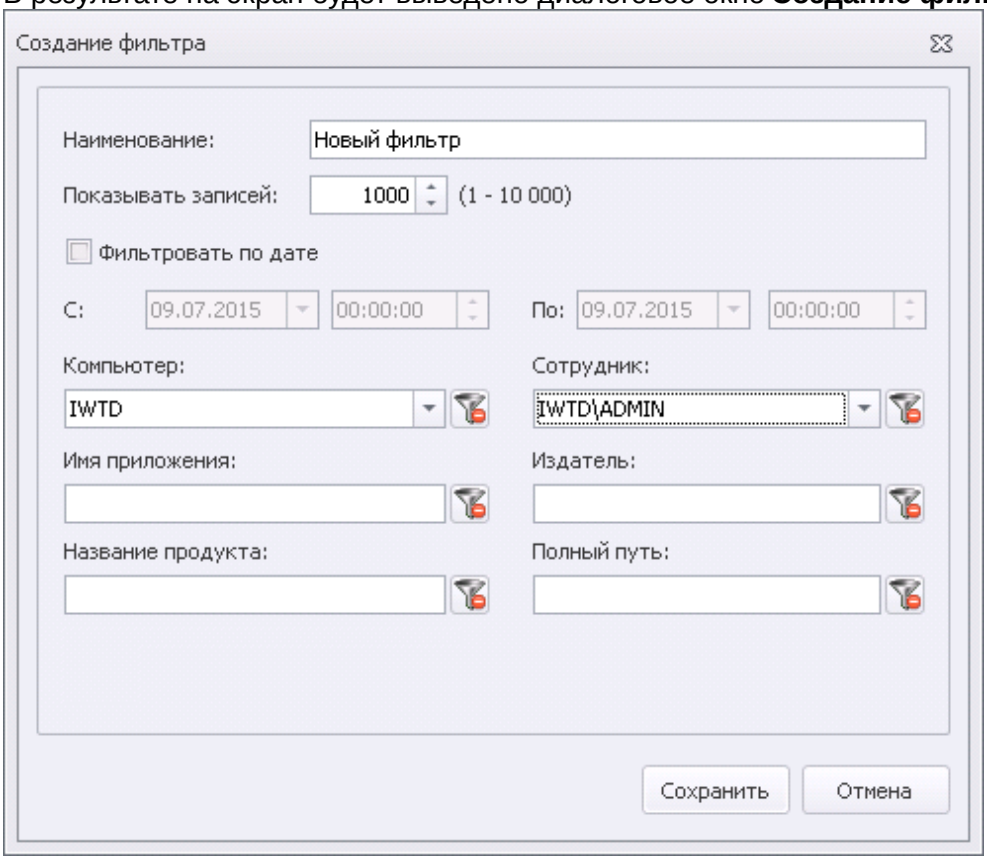
Предустановленный фильтр **За сегодня** показывает только приложения, запущенные в конкретный выбранный день впервые с момента установки Агента на компьютер.

Приложения, запущенные сразу после установки Агента, будут показаны в фильтре **Все**.

Чтобы создать новый фильтр:

1. Перейдите к разделу **Приложения**.
2. На Панели навигации установите курсор в группе элементов **Протокол приложений** и выполните одно из следующих действий:
   - в меню группы элементов **Протокол приложений** нажмите **Создать фильтр**;
   - в главном меню выберите команду **Правка** > **Создать фильтр**;
   - нажмите правой кнопкой мыши в группе элементов **Протокол приложений** и из раскрывшегося списка выберите **Создать фильтр**.

В результате на экран будет выведено диалоговое окно **Создание фильтра**.



3. В поле **Наименование** введите название фильтра.
4. В поле **Показывать записей** укажите количество записей, которые должно отображаться в **Протоколе приложений**.
5. Для фильтрации приложений по дате отметьте поле **Фильтровать по дате** и укажите продолжительность отображаемого периода в полях **С** и **По**.
6. При необходимости, определите дополнительные условия фильтрации:
   - В поле **Компьютер** выберите компьютер, протокол приложений с которого вы хотите просматривать;
   - В поле **Сотрудник** выберите учетную запись сотрудника, запускающего приложения;
   - В поле **Имя приложения** введите название файла приложения;
   - В поле **Издатель** укажите издателя программного обеспечения;
   - В поле **Название продукта** введите его название;
   - В поле **Полный путь** укажите расположение приложения;

   Для удаления ненужного условия фильтрации нажмите в строке этого условия.
7. Нажмите **Сохранить**.

Чтобы изменить фильтр, воспользуйтесь кнопкой в разделе **Протокол приложений** на Панели навигации, в контекстном меню или нажмите сочетание клавиш **Ctrl+E**.

Чтобы удалить фильтр:

1. Воспользуйтесь кнопкой в разделе **Протокол приложений** на Панели навигации, в контекстном меню или нажмите сочетание клавиш **Ctrl+D**.
2. Нажмите **Да**, чтобы подтвердить удаление.

Добавление приложения в список автоматически

Система позволяет наполнять списки приложений автоматически, на основании данных из протокола приложений.

Чтобы добавить одно или несколько приложений в список автоматически:

1. Перейдите к разделу **Приложения**.
2. На Панели навигации, в группе элементов **Протокол приложений**, выберите необходимый фильтр.
3. На панели **Протокол приложений** выберите одну или несколько записей. Для выбора нескольких записей отмечайте их курсором, зажав клавишу **Shift** или **Ctrl**.
4. Выполните одно из следующих действий:
   - на панели Протокол приложений нажмите **Добавить приложение в список автоматически**;
   - в главном меню выберите команду **Правка** > **Добавить приложение в список автоматически**;
   - нажмите правой кнопкой мыши на панели **Протокол приложений** и из раскрывшегося списка выберите **Добавить приложение в список автоматически**.
5. В появившемся окне:
   - выберите существующий список

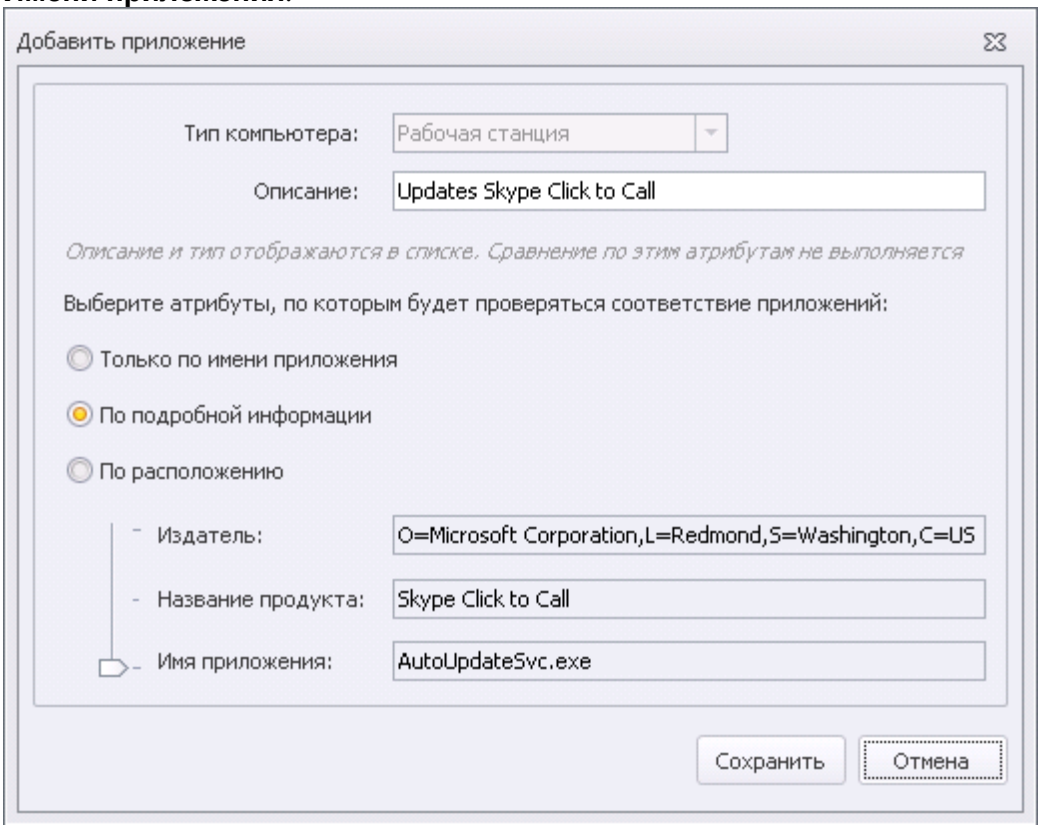
   или
6. нажмите **Создать новый**, в открывшемся окне, в поле **Наименование списка**, введите название для списка и нажмите **Сохранить**.
7. Нажмите **Выбрать**.
8. В окне, информирующем об успешном добавлении приложений, нажмите **ОК**.

Добавление приложения в список вручную

Чтобы добавить приложение в список вручную:

1. Перейдите к разделу **Приложения**.
2. На Панели навигации, в группе элементов **Протокол приложений**, выберите необходимый фильтр.
3. На панели **Протокол приложений** выберите одну или несколько записей. Для выбора нескольких записей отмечайте их курсором, зажав клавишу **Shift** или **Ctrl**.
4. Выполните одно из следующих действий:
   - на панели **Протокол приложений** нажмите **Добавить приложение в список вручную**;
   - в главном меню выберите команду **Правка** > **Добавить приложение в список вручную**;
   - нажмите правой кнопкой мыши на панели Протокол приложений и из раскрывшегося списка выберите **Добавить приложение в список вручную**.
5. В окне **Добавить приложение** вы можете настроить параметры, по которым будет проверяться соответствие приложения:
   - **Только по имени приложения**
     В поле **Имя приложения** введите полное исходное имя запускаемого файла.

- **По подробной информации**
  Фильтрация приложений по уточняющей информации в порядке уточнения **Издатель**, **Название продукта**, **Имя приложения**.
- **По расположению**
  Фильтрация приложений по уточняющей информации от **Расположения** до **Имени приложения**.



6. Нажмите **Сохранить**.
7. Если вы выбрали несколько записей приложений, повторите шаги 5 и 6 для остальных записей.
8. В окне, информирующем об успешном добавлении приложений, нажмите **OK**.

Экспорт протокола приложений

Чтобы экспортировать протокол приложений:

1. Перейдите в раздел **Приложения** на панели навигации.
2. На панели навигации, в группе элементов **Протокол приложений** выберите необходимый протокол.
3. В меню группы **Протокол приложений** нажмите **Экспортировать протокол приложений** либо используйте меню **Правка**>**Экспортировать протокол приложений**.
4. Укажите директорию и имя файла экспорта и нажмите **Сохранить**.
   Протокол будет сохранен в формате **.xls**.

6.4.4 Временный доступ сотрудника к сети

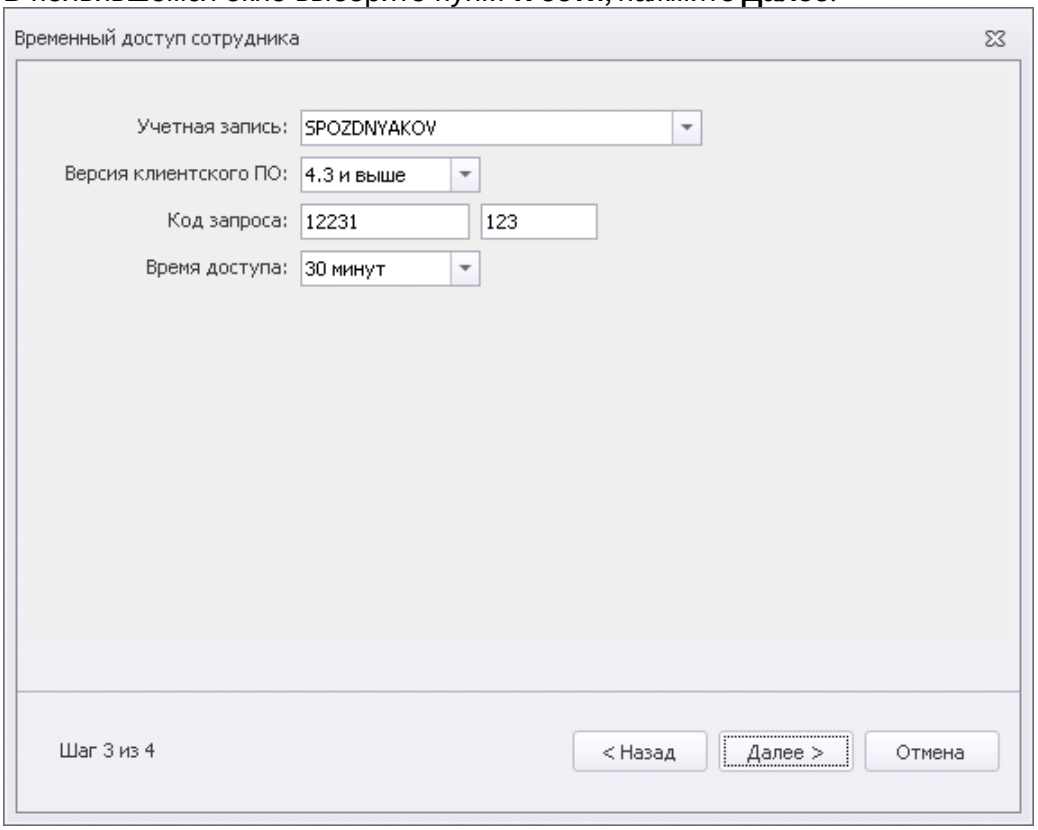
Сотрудник, для которого действует правило (DM), запрещающее соединения вне корпоративной сети (см. "Контроль сетевых соединений" и "Правило (DM) для Network Monitor"), может из меню Агента InfoWatch Device Monitor, команда Контроль сети, запросить временный доступ к внешним соединениям.

> **Важно!**
>
> Возможность запросить доступ есть у сотрудника только в том случае, если для уведомлений сотрудника не действует настройка **Скрывать присутствие агента на компьютере** (подробнее см. "Общие настройки работы Агентов").
> О том, как настроить текст, отображаемый сотруднику, см. "Настройка уведомлений сотрудников о нарушении правил (DM)", тип уведомления **Запрет сетевого подключения, детализированное**.

Получив код запроса, сотрудник должен передать его офицеру безопасности.

Чтобы предоставить сотруднику временный доступ к внешним соединениям:

1. В главном меню выберите команду **Инструменты** > **Временный доступ сотрудника**.
2. В появившемся окне выберите **Продиктован по телефону (цифровой код запроса)**, нажмите **Далее**.
3. В появившемся окне выберите пункт **К сети**, нажмите **Далее**.



4. Из раскрывающегося списка **Учетная запись** выберите запись сотрудника, которому требуется предоставить временный доступ.
5. Из раскрывающегося списка **Версия клиентского ПО** выберите номер версии приложения Device Monitor Agent, установленной на компьютере сотрудника.

6. В поле **Код запроса** введите код, переданный сотрудником.
7. Из раскрывающегося списка **Время доступа** выберите временной промежуток, на который предоставляется доступ.
8. Нажмите **Далее**.
   В поле **Код подтверждения** появится код, который нужно передать сотруднику для того, чтобы он смог получить требуемый доступ.
9. Нажмите **Готово**.

6.4.5 Временный доступ сотрудника к устройствам

Сотрудник, для которого действует правило (DM), запрещающее использование устройств (см. "Правило (DM) для Device Monitor"), может в интерфейсе Агента InfoWatch Device Monitor, вкладка Список устройств, запросить временный доступ к устройствам.

> **Важно!**
>
> Возможность запросить доступ есть у сотрудника только в том случае, если для уведомлений сотрудника не действует настройка **Скрывать присутствие агента на компьютере** (подробнее см. "Общие настройки работы Агентов").
> О том, как настроить текст, отображаемый сотруднику, см. "Настройка уведомлений сотрудников о нарушении правил (DM)", тип уведомления **Запрет доступа к устройству**.

Получив код запроса, сотрудник должен передать его офицеру безопасности.

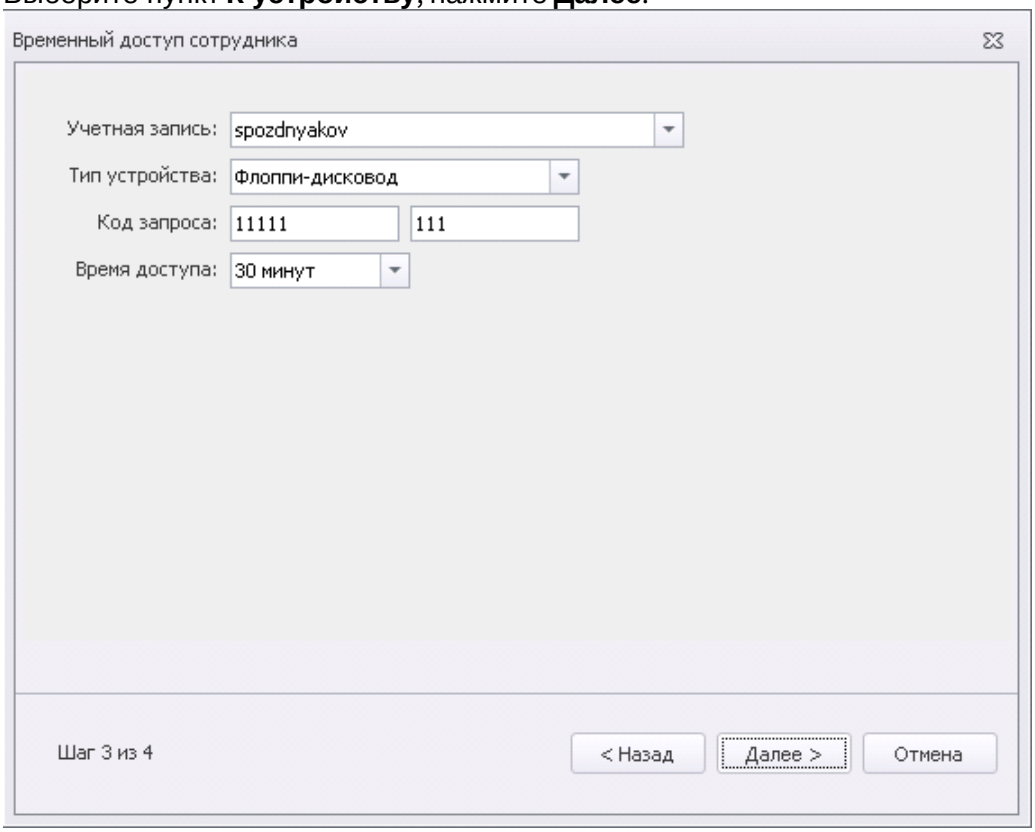
В зависимости от ситуации, вы можете использовать один из двух варианта взаимодействия с сотрудником:

- по телефону;
- по электронной почте.

Чтобы предоставить временный доступ к устройствам сотруднику, обратившемуся по телефону:

1. В главном меню выберите команду **Инструменты** > **Временный доступ сотрудника**.
2. В появившемся окне выберите пункт **Продиктован по телефону**, нажмите **Далее**.

3. Выберите пункт **К устройству**, нажмите **Далее**.

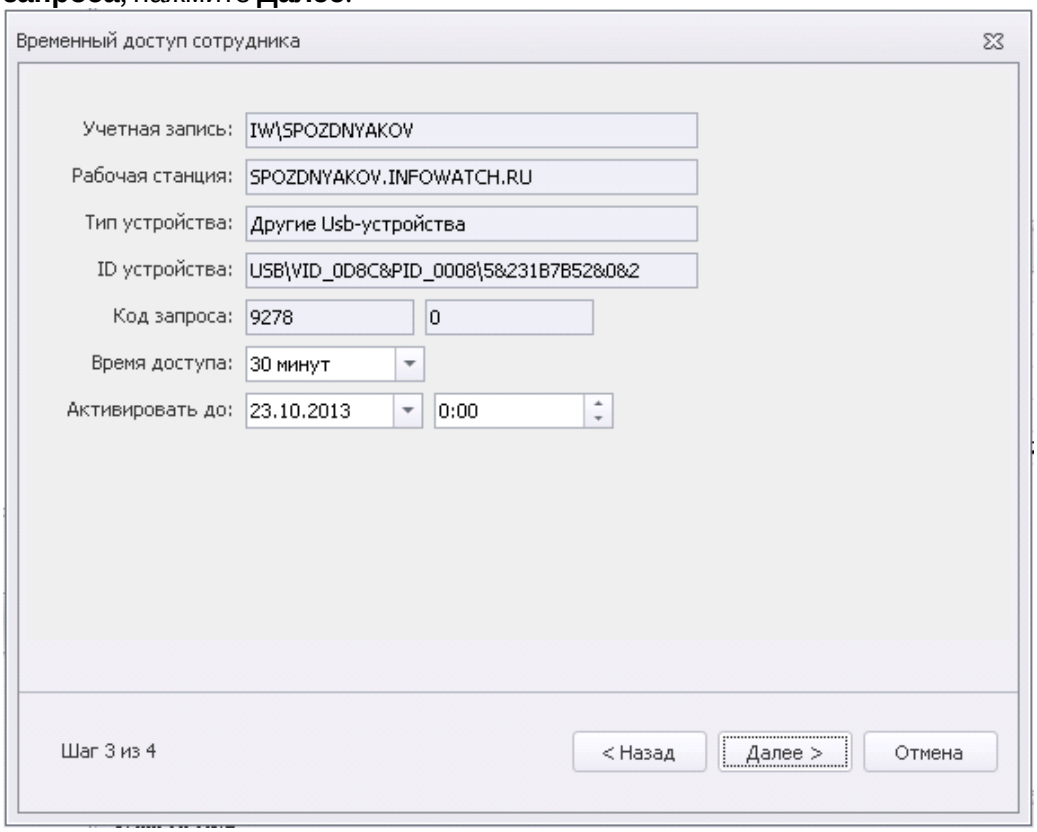


4. Из раскрывающегося списка **Учетная запись** выберите запись сотрудника, которому требуется предоставить временный доступ.
5. Из раскрывающегося списка **Тип устройства** выберите требуемый тип устройств.
6. В поле **Код запроса** введите код, переданный сотрудником.
7. Из раскрывающегося списка **Время доступа** выберите временной промежуток, на который предоставляется доступ.
8. Нажмите **Далее**.
   В поле **Код подтверждения** появится код, который нужно передать сотруднику для того, чтобы он смог получить требуемый доступ.
9. Нажмите **Готово**.

Чтобы предоставить временный доступ к устройствам сотруднику, обратившемуся по электронной почте:

1. В главном меню выберите команду **Инструменты** > **Временный доступ сотрудника**.
2. В появившемся окне выберите пункт **Получен через электронную почту или другие средства связи**, нажмите **Далее**.

3. Введите полученный по электронной почте текст запроса в поле **Введите текст запроса**, нажмите **Далее**.



4. Из раскрывающегося списка **Время доступа** выберите временной промежуток, на который предоставляется доступ.
5. Из группы раскрывающихся списков **Активировать до** выберите временной промежуток, в который сотрудник сможет активировать свой доступ к устройству (после активации доступ будет предоставлен на время, указанное в пункте **Время доступа**).
6. Нажмите **Далее**.
   В поле **Скопируйте в буфер обмена текст ответа** появится код, который нужно передать сотруднику для того, чтобы он смог получить требуемый доступ.
7. Нажмите **Готово**.

6.5 Просмотр событий DM

Данные, полученные в процессе работы агентов InfoWatch Device Monitor на контролируемых компьютерах, фиксируются в виде **событий** и передаются на сервера Device Monitor вместе с данными теневого копирования. События (в отличие от теневых копий) сохраняются в базе данных InfoWatch Device Monitor и доступны для просмотра в Консоли управления (DM).

Уровень логирования сведений (сохранять всю информацию о попытках доступа; сохранять только нарушения политик (DM) или не сохранять вообще) вы можете определить в общих настройках схемы безопасности: подробнее см. "Общие настройки работы Агентов".

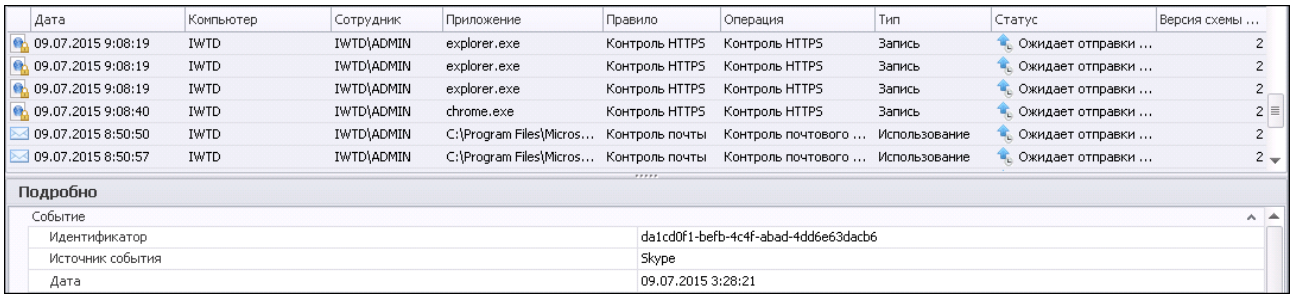
В разделе **События** вы можете просмотреть информацию о событиях. Для перехода к разделу нажмите кнопку **События** на Панели навигации.

Чтобы просмотреть события, выберите нужные фильтр в списке.

Вы можете выбрать один из предустановленных фильтров или создать новый фильтр, как описано в статье "Фильтры событий". Предустановленные фильтры:

- **За последние 4 часа**
- **За сегодня**

Сведения о событиях отображаются в виде таблицы. Расширенная информация по свойствам каждой записи выводится на панели **Подробно**.



Имя атрибута	Описание	Возможные значения
Общие атрибуты		
Идентификатор	Уникальный номер, присваиваемый событию в Системе	
Источник события	Тип события в зависимости от перехватчика	▪ **Файловое** – File Monitor; ▪ **От устройств** – Device Monitor; ▪ **Принтер** – Print Monitor; ▪ **Skype, XMPP, MMP, Telegram** – IM Client Monitor; ▪ **FTP/FTPS** – FTP Monitor; ▪ **HTTP/HTTPS** – HTTP(S) Monitor; ▪ **Cloud Storage** - Cloud Storage Monitor; ▪ **Сетевое** – Network Monitor; ▪ **Электронная почта** – Mail Monitor; ▪ **Системное** - событие об окончании места на диске для сохранения теневой копии. *Такое событие не передается в систему Traffic Monitor.*
Дата	Дата и время (в часах и минутах) фиксации события на компьютере. На сервере Device Monitor событие сохраняется в UTC, а в Консоли управления (DM) отображается соответственно локальному времени того компьютера, где работает Консоль (DM)	
Имя компьютера	Имя компьютера, где зафиксировано событие	

Операция	Описание действия или попытки действия, выполненного сотрудником	
Сервер	Имя сервера InfoWatch Device Monitor, на который агент передал информацию о событии	
Приложение	Имя исполняемого файла и/или наименование процесса, выполняющего действие, если его удалось определить	
Тип	Тип события в зависимости от выполненного действия	▪ **Запись** – размещение или изменение данных (включая изменение имени файла) на внешнем устройстве; пересылка файла средствами мессенджера; отправка задания на печать на принтер; пересылка данных по протоколу FTP/FTPS; загрузка данных в облачное хранилище. ▪ **Использование** – подключение внешнего устройства, для которого отдельно не контролируются операции чтения/записи; отправка сообщений через мессенджер; ▪ **Нарушение** – нарушение сотрудником работы перехватчика IM Client; ▪ **Предупреждение** – запрет сотрудником или отсутствие согласия сотрудника на использование плагина IM Client, если этого требует политика безопасности (DM). ▪ **Запрет использования** – попытка передачи данных по запрещенному каналу.
Статус	Состояние обработки события на сервере и его отправки на сервер Traffic Monitor	▪ **Новое** ▪ **Ожидает обработки** ▪ **Обработано** ▪ **Нет лицензии** ▪ **Ожидает отправки в ТМ** ▪ **Ошибка отправки в ТМ** ▪ **Отправлено в ТМ** **Примечание:** В случае работы сервера в автономном режиме статус событий может быть только **Обработано**

Версия схемы безопасности	Номер версии схемы безопасности, используемой на компьютере в момент фиксации события	
Вердикт операции	Признак разрешения контролируемого действия. Для событий с источником *От устройств* (сработало правило **Device Monitor**) также возможна блокировка действия.	▪ **Операция разрешена** ▪ **Запрет** – только для событий от устройств ▪ **Запрет копирования незащищенных данных** – только для событий от устройств ▪ **Разрешено (В белом списке)** – для событий от устройств, состоящих в белом списке
Сотрудник	Наименование домена (наименование компьютера вне домена) и логин пользователя, в сессии которого фиксировалось событие, или ссылка на операционную систему, если событие зафиксировано вне сессий пользователей	
Правило (DM)	Название правила (DM) политики (DM), в соответствии с которым контролируется событие	
Для событий с источником Файловое, От устройств, Принтер, FTP/FTPS, HTTP/HTTPS, Cloud Storage, Сетевое, Системное		
Терминальный Клиент	Имя терминального клиента, если определено	
Сетевой адрес терминального клиента	IP терминального клиента, если определено	
Для событий с источником Файловое		
Назначение	Полное имя целевого файла	
Размер файла	Размер целевого файла	

Состояние	Результат теневого копирования перемещаемых данных	▪ **копия не создавалась** – правило не требует создания теневой копии ▪ **копия создана** – теневая копия успешно создана ▪ **закончилось свободное место на диске** – при нехватке свободного места на агенте ▪ **ошибка создания копии** – при возникновении ошибки создания копии
Описание устройства	Идентификатор экземпляра или модели устройства, на которое записывался файл	
Для событий с источником *От устройств*		
Тип устройств	Поддерживаемый перечень типов устройств см. "Функции InfoWatch Device Monitor"	
Идентификатор экземпляра или модели устройства	Идентификатор модели (VID) и серийный номер (PID) применяемого внешнего устройства или принтера, используемого в операции	
Описание устройства	Описание используемого устройства, полученное от операционной системы на компьютере, где установлен Агент	
Для событий с источником Skype, XMPP, MMP, Telegram		
Имя пользователя клиента мгновенных сообщений	UIN пользователя, авторизованного в мессенджере на компьютере	

Состояние	Результат теневого копирования	▪ **копия не создавалась** – правило (DM) не требует создания теневой копии ▪ **копия создана** – теневая копия успешно создана ▪ **закончилось свободное место на диске** – на агенте нет свободного дискового пространства ▪ **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки
Список отправителей	UIN пользователей мессенджера, отправивших сообщение/файл в диалоге мессенджера	
Список получателей	UIN пользователей мессенджера, получивших сообщение/файл в диалоге мессенджера	
Имя файла	Полное имя пересылаемого файла	
Размер файла	Размер пересылаемого файла	
Теневая копия	Результат теневого копирования файла, чата или сообщения	▪ **Нет** – теневая копия не создавалась ▪ **Да** – теневая копия успешно создана
Для событий с источником *От принтера*		
Документ	Полное имя файла, отправленного на печать	
Принтер	Сетевое имя принтера, на который было отправлено задание на печать	

Статус печати	Результат теневого копирования задания на печать	1. Теневая копия задания на печать создана успешно. Задание содержало графические и текстовые данные; 2. Теневую копию задания на печать не удалось создать. Задание не содержало графических и текстовых данных; 3. Ошибка при создании теневой копии задания на печать; 4. Теневую копию не нужно было создавать 5. Теневая копия задания на печать создана частично. Графические данные обработаны полностью. Текстовые данные обработаны частично. 6. Теневая копия задания на печать создана частично. Графические данные обработаны частично. Текстовые данные обработаны полностью. 7. Теневая копия задания на печать создана успешно. Задание содержало только текстовые данные; 8. Теневая копия задания на печать создана успешно. Задание содержало только графические данные; 9. Теневая копия задания на печать создана частично. Графические данные обработаны частично. Задание не содержало текстовых данных. 10. Теневая копия задания на печать создана частично. Задание не содержало графических данных. Текстовые данные обработаны частично.
Состояние	Результат теневого копирования задания на печать	▪ **копия не создавалась** – правило (DM) не требует создания теневой копии ▪ **копия создана** – теневая копия успешно создана ▪ **закончилось свободное место на диске** – на агенте нет свободного дискового пространства ▪ **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки
Для событий с источником *FTP/FTPS*		

Состояние	Результат теневого копирования перемещаемых данных	▪ **копия не создавалась** – правило (DM) не требует создания теневой копии ▪ **копия создана** – теневая копия успешно создана ▪ **закончилось свободное место на диске** – на агенте нет свободного дискового пространства ▪ **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки
Отправитель	Имя, под которым сотрудник авторизован на FTP сервере	
FTP сервер	Имя или IP адрес FTP сервера	**Примечание:** При использовании FTP через proxy-сервер данное поле может содержать адрес proxy-сервера, а не адрес используемого FTP-сервера.
Относительный путь	Директория на FTP сервере, куда осуществляется передача файла	
Имя файла	Полное имя пересылаемого файла	
Фактический размер файла	Размер переданного файла по результату передачи	
Заявленный размер файла	Размер передаваемого файла по данным приложения, выполняющего передачу на FTP сервер (например, браузера)	
Начальная позиция	При передаче файла по частям, это - позиция, с которой начата передача этой части.	
Теневая копия	Результат теневого копирования файла	▪ **Нет** – теневая копия не создавалась ▪ **Да** – теневая копия успешно создана
Для событий с источником *HTTP/HTTPS*		

Состояние	Результат теневого копирования данных	▪ **копия не создавалась** – правило (DM) не требует создания теневой копии ▪ **копия создана** – теневая копия успешно создана ▪ **закончилось свободное место на диске** – на агенте нет свободного дискового пространства ▪ **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки
DNS получателя	Сетевое имя компьютера, на который был отправлен запрос	
IP получателя	IP-адрес компьютера, на который был отправлен запрос	
Размер запроса	Размер отправленного запроса в КБ	
Правило	Название правила политики (DM), в соответствии с которым контролируется событие	
Для событий с источником *Cloud Storage*		
Название облачного хранилища	Название облачного хранилища, в которое выполняется загрузка данных	• Google Drive • DropBox • YandexDisk • SkyDrive • EverNote • SugarSync
Имя файла	Целевое имя файла	
Размер файла	Размер файла (в байтах), отправляемого в облачное хранилище	
Для событий с источником *Терминальная сессия*		
Путь	Короткое имя копируемого файла	
Имя устройства	Имя устройства, если определено	

ID устройства	ID устройства, если определено	
Для событий с источником *Электронная почта*		
Состояние	Результат теневого копирования данных	▪ **копия не создавалась** – правило не требует создания теневой копии ▪ **копия создана** – теневая копия успешно создана ▪ **закончилось свободное место на диске** – на агенте нет свободного дискового пространства ▪ **ошибка создания копии** – теневая копия не создалась из-за какой-либо ошибки
Список отправителей	Адрес электронной почты отправителя письма	
Список получателей	Список адресов, на которые было отправлено письмо	**Примечание:** Для событий с большим количеством получателей необходимо иметь в виду, что при просмотре события через Консоль Device Monitor данное поле не отображает более 1024 символов. Однако если для события настроено создание теневой копии, то в результате передачи события в Traffic Monitor поле Получатели будет отображать полный список получателей (ограничение в 4000 байт).
Правило	Название правила политики (DM), в соответствии с которым контролируется событие	
Для событий с сетевым источником		
Время отмены блокировки доступа	Для операции *Временная отмена блокировки доступа* - начало периода временного доступа. см. "Временный доступ сотрудника к сети".	
Время возобновления блокировки доступа	Для операции *Временная отмена блокировки доступа* - конец периода временного доступа. см. "Временный доступ сотрудника к сети".	

Сервер соединения	Для операции *Соединение запрещено* - адрес или имя сервера, доступ к которому запрещен	
Порт	Для операции *Соединение запрещено* - номер порта, доступ к которому запрещен	

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

6.5.1 Фильтры событий

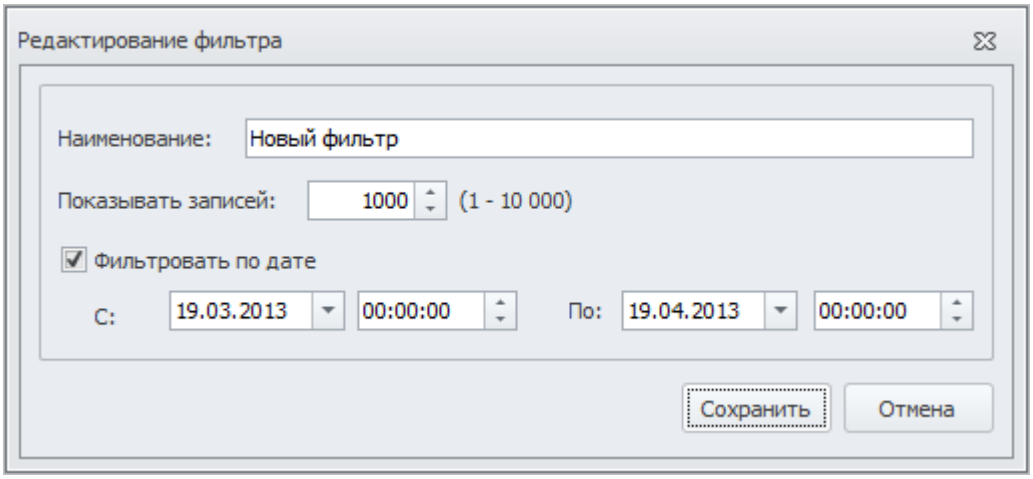
Помимо предустановленных фильтров вы можете создавать собственные фильтры для просмотра информации о событиях.

Чтобы добавить или отредактировать фильтр:

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

Действие	Шаги
Создание фильтра	- в главном меню выберите команду **Правка** > **Создать фильтр**; - воспользуйтесь кнопкой **Создать фильтр**, расположенной в верхней части Панели навигации.
Редактирование фильтра	1. В области **События** на Панели навигации выберите название фильтра, который нужно отредактировать. 2. Выполните одно из следующих действий: - в главном меню выберите команду **Правка** > **Изменить**; - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации; - дважды щелкните левой кнопкой мыши по названию выделенного фильтра; - щелкните по названию выделенного фильтра правой кнопкой мыши и в контекстном меню выберите **Изменить**; - нажмите Ctrl+E.

После выполнения любого из этих действий на экран будет выведено диалоговое окно определения параметров фильтра.



3. В диалоговом окне **Редактирование фильтра** укажите параметры фильтра:
   - **Наименование**.
   - **Показывать записей**. Ограничение на количество записей, которые могут быть выведены в рабочей области Консоли управления (DM) (значение по умолчанию 1000 записей).
   - Чтобы задать условия фильтрации по дате, отметьте поле **Фильтровать по дате** и укажите начало и окончание интересующего вас периода в полях **С** и **По** соответственно. Дату задают в левом поле, время – в правом.

     > **Примечание.**
     >
     > Для предустановленных фильтров параметры **Наименование** и **Фильтровать по дате** изменять нельзя.

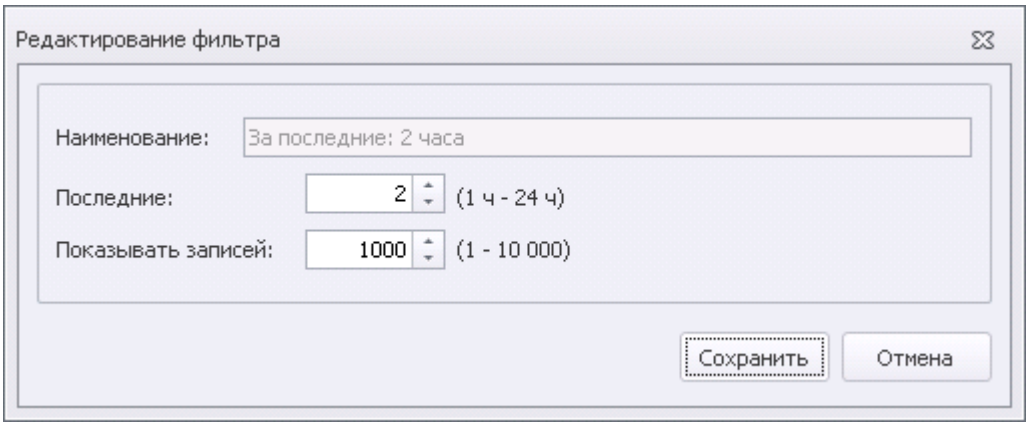
4. Нажмите **Сохранить**.

Предустановленный фильтр **За последние 4 часа** имеет другой интерфейс редактирования и позволяет создавать фильтры, отображающие события за последние несколько часов.

Чтобы отредактировать предустановленный фильтр так, чтобы отображались события за указанное количество часов:

1. В области **События** на Панели навигации выберите фильтр **За последние 4 часа**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Изменить**;
   - воспользуйтесь кнопкой **Изменить**, расположенной в верхней части Панели навигации;
   - дважды щелкните левой кнопкой мыши по названию фильтра;
   - щелкните по названию фильтра правой кнопкой мыши и в контекстном меню выберите **Изменить**;

- нажмите Ctrl+E.



3. В диалоговом окне **Редактирование фильтра** укажите параметры фильтра:
   - **Последние**. Укажите количество часов, записи за которые должны быть выведены в рабочей области Консоли управления (DM).
   - **Показывать записей**. Ограничение на количество записей, которые могут быть выведены (значение по умолчанию 1000 записей).
4. Нажмите **Сохранить**.

6.5.2 Удаление событий

Информация об уже обработанных событиях (статус **Обработано, Отправлено в TM, Ошибка отправки в TM, Нет лицензии**) может быть удалена.

Вы можете удалить события:

- за указанный период времени;
- все, соответствующие выбранному фильтру.

Чтобы удалить из журнала аудита информацию обо всех событиях за период:

1. Перейдите к разделу **События**.
2. Выполните одно из следующих действий:
   - воспользуйтесь кнопкой **Удалить события**, расположенной на Панели навигации;
   - в главном меню выберите команду **Правка** > **Удалить события**;
   - нажмите Ctrl + Shift + D;
3. В открывшемся диалоговом окне **Удаление событий из базы данных** укажите необходимый диапазон дат, информация за который должна быть удалена.
4. Нажмите **Удалить**.

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

Чтобы удалить из журнала аудита информацию о событиях, соответствующих выбранному фильтру:

1. Перейдите к разделу **События**.
2. В списке фильтров выберите название нужного фильтра.
3. Выполните одно из следующих действий:
   - воспользуйтесь кнопкой **Удалить события фильтра**, расположенной в верхней части раздела События;

- в главном меню выберите команду **Правка** > **Удалить события фильтра**;
- выберите пункт **Удалить события фильтра** в контекстном меню фильтра;
- Нажмите Shift + Delete.

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

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

6.6 Удаленная установка, обновление и удаление Агентов

Установка, обновление и удаление Агентов InfoWatch Device Monitor на рабочие станции может выполняться централизованно средствами Консоли управления InfoWatch Device Monitor. Для этого предусмотрен механизм задач. Задачи позволяют запускать процессы установки, обновления и удаления агентского ПО, смены пароля деинсталляции, а также наблюдать за состоянием выполнения этих процессов.

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

- Рабочие станции, на которые производится установка, должны удовлетворять необходимым аппаратным и программным требованиям (см. документ "*Traffic Monitor. Руководство по установке*", статья "Требования к аппаратному и программному обеспечению Агента InfoWatch Device Monitor").
- На момент установки Агента проактивная антивирусная защита на рабочих станциях должна быть отключена (только для Агентов, установленных на ОС Windows).
- Сервер Device Monitor и рабочие станции должны распознавать доменные имена друг друга.
- На рабочих станциях, где установлен межсетевой экран (firewall), отличный от стандартного брандмауэра Windows, этот межсетевой экран должен быть отключен, или в нем должно присутствовать разрешение на работу любых сетевых соединений для следующих компонент Device Monitor: *IWDeployAgent.exe*, *iwdmc.exe*, *DM.Client.exe*, *IWProxy.exe*, *rmtlogctr.exe* (только для Агентов, установленных на ОС Windows).

> **Примечание.**
>
> Для установки Агента на Windows 7 зайдите в **Панель управления** -> **Центр управления сетями и общим доступом** -> **Изменить дополнительные параметры общего доступа** и выберите опцию **Включить общий доступ к файлам и принтерам**. После этого Агент распространения сможет быть скопирован на рабочую станцию. Брандмауэр будет настроен автоматически.

Чтобы перейти к разделу Консоли управления (DM), предназначенному для работы с задачами, воспользуйтесь кнопкой **Задачи**, расположенной на Панели навигации.
Информация по управлению задачами содержится в подразделах:

- Просмотр задач
- Подготовка к первичной установке Агентов
- Создание задачи первичного распространения
- Создание задачи обновления
- Создание задачи смены пароля деинсталяции
- Создание задачи удаления

- Запуск, остановка, редактирование и удаление задачи
- Ошибки установки Агентов

Вы также можете осуществлять установку и обновление Агента с помощью средств распространения программного обеспечения (например, в Microsoft Active Directory посредством механизма групповых политик (DM)). Подробное описание такой установки см. в документе "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Установка Агента с помощью средств распространения программного обеспечения". Для этого удобно использовать пакет установки, созданный, как описано в разделе "Создание пакета установки".

6.6.1 Просмотр задач

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

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

Параметр	Описание
Наименование	Имя задачи, указанное при ее создании
Описание	Описание задачи, указанное при ее создании
Тип	Один из следующих типов задач: • первичное распространение; • смена пароля; • обновление; • удаление.
Статус	Текущее состояние задачи. Возможные значения: • создана; • запущена; • остановлена; • выполнена.
Период повторного запуска, мин	Время (в минутах), по истечении которого будет повторно запущена задача распространения для рабочих станций, к которым при предыдущем запуске не было доступа. Данное время начинает отсчитываться после завершения обработки последней станции из списка при предыдущем запуске задач. Если запуск завершился с ошибкой, то повторный запуск производиться не будет.
Количество попыток повторного запуска	Максимальное количество попыток перезапустить задачу распространения на рабочей станции.
Для задач первичного распространения	

Отображать сотруднику уведомления о работе агентского модуля	Признак того, что при попытке сотрудника выполнить действие, запрещенное политикой безопасности (DM), ему будет отображаться предупреждающее уведомление. Подробнее см. "Общие настройки политики безопасности (DM)", "Создание инсталляционного комплекта" и "Настройка уведомлений сотрудников о нарушении правил (DM)"
Скрывать присутствие агента на рабочей станции	Признак того, что Система будет скрывать присутствие Агента на рабочих станциях. Иначе в области уведомлений панели задач Windows на компьютере, где установлен Агент, будет отображаться пиктограмма . При нажатии на этот значок доступна информация о работе Агента, а также список контролируемых в данный момент устройств. **Внимание!** Если на контролируемом компьютере включена антивирусная защита, то антивирус может выявлять работу Device Monitor: например, в списке процессов, запущенных на контролируемом компьютере или в списке программ, инициирующих контроль.
Устанавливать компонент перехвата сетевого трафика	Признак того, что на компьютер будет установлен компонент `iw_proxy`.
Устанавливать компонент контроля сетевых соединений	Признак того, что на компьютер будет установлен перехватчик Network Monitor.
Пароль для деинсталляции	Признак того, задан ли пароль, запрашиваемый у сотрудника при попытке удалить Агент Device Monitor.
Proxy Root Issuer DN	Уникальное имя для сертификата proxy-сервера Device Monitor (Issuer Distinguished name)
Для задач первичного распространения и обновления	
Директория для установки	Папка на рабочих станциях, куда будет устанавливаться Агент Device Monitor.
Имя пользователя для установки	Имя пользователя, от имени которого выполняется запущенная задача на рабочих станциях.
Продолжительность ожидания перезагрузки, часов	Время, в течение которого будет ожидаться перезагрузка рабочей станции (в часах); если за указанное время рабочая станция не будет перезагружена, Система приступит к уведомлению сотрудника (если параметры уведомления заданы), а затем - к принудительной перезагрузке операционной системы.

Продолжительность уведомлений о перезагрузке компьютера	Время, в течение которого сотруднику будут отображаться сообщения о необходимости перезагрузки компьютера, в часах.
Частота уведомлений о перезагрузке компьютера, мин	Промежуток времени, с которым будут повторяться сообщения о необходимости перезагрузки компьютера, в минутах.
Сообщения о перезагрузке	Текст, отображаемый сотруднику в сообщении о необходимости перезагрузки.
Показать предупреждение перед принудительной перезагрузкой	Признак того, будет ли показано окно о принудительной перезагрузке компьютера (сотруднику даются 5 минут на завершение своих операций) или перезагрузка будет осуществлена принудительно.
Пароль для деинсталляции	Признак того, задан ли пароль, запрашиваемый у сотрудника при попытке удалить Агент Device Monitor

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

Параметр	Описание
Имя	IP-адрес или доменное имя рабочей станции
Статус выполнения задачи	Текущее состояние задачи для данной станции. Возможные значения: ▪ **Не выполняется** ▪ **Подготовка** ▪ **В процессе** ▪ **Ожидание перезагрузки** (только для задач установки и обновления) ▪ **Ошибка** (подробнее см. "Ошибки установки Агентов") ▪ **Нет доступа** ▪ **Выполнена**
Версия агента	Версия Агента, установленного в настоящий момент на рабочей станции
Операционная система	Операционная система, установленная на рабочей станции
Разрядность операционной системы	Разрядность операционной системы на рабочей станции

Количество подключений	Количество сделанных попыток подключения к недоступной рабочей станции
Время последнего обращения	Дата и время последнего подключения к рабочей станции

6.6.2 Подготовка к первичной установке Агентов. Агент распространения

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

Для того чтобы удаленная установка Агента средствами InfoWatch Device Monitor была произведена корректно, рабочие станции, на которые производится установка, должны удовлетворять необходимым аппаратным и программным требованиям: см. "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Требования к аппаратному и программному обеспечению Агента InfoWatch Device Monitor".

Также для рабочих станций, установленных на ОС Windows должны выполняться следующие условия:

- Проактивная антивирусная защита на рабочих станциях должна быть отключена.
- На рабочих станциях, где установлен межсетевой экран (firewall), отличный от стандартного брандмауэра Windows, этот межсетевой экран:
  - должен быть отключен
    или
  - в нем должно присутствовать разрешение на работу Агента распространения InfoWatch Device Monitor
    или
  - в брандмауэре должен быть открыт порт **15505** (порт по умолчанию, по которому агент распространения ждет соединения) для входящих соединений, если он не был изменен в настройках сервера (см. "*Traffic Monitor. Руководства администратора*", статья "Раздел <applicationSettings>", параметр **CommunicationPort**).

> **Важно!**
>
> Для рабочих станций управлением на ОС Astra Linux должны выполняться следующие условия:
>
> - должны быть установлены средства удаленного доступа **SSH**.
> Если SSH не был установлен во время установки ОС Astra Linux, его можно установить, выполнив в консоли сервера команду:
> `sudo apt-get install ssh`
> Для запуска сервиса используйте команду:
> `service ssh start`
> - пользователь, от имени которого будет произведена установка Агента, должен на целевой рабочей станции обладать правами на установку пакетов и регистрацию служб (root-правами).
> По умолчанию `ssh` запрещает подключаться через пользователя `root`.

Дополнительные требования зависят от способа распространения:

Способ 1:

Административными средствами распространить на целевые рабочие станции установочный пакет Агента распространения Setup.DeployAgent.msi, входящий в поставляемый дистрибутив.

Способ 2:

Для рабочих станций под упралением ОС Windows, выполнить действия, необходимые для передачи Агента распространения через административные разделяемые ресурсы:

- Межсетевые экраны (firewall) на рабочих станциях должны быть либо отключены, либо в них заданы необходимые разрешения: см. "Настройки брандмауэра".
- Необходимо определить параметры сетевого доступа к разделяемым ресурсам: см. "Включение административных разделяемых ресурсов".

Если все необходимые требования соблюдены, вы можете переходить к созданию, а затем - к запуску задачи первичного распространения.

Включение административных разделяемых ресурсов

Для передачи Агента распространения InfoWatch Device Monitor на целевые рабочие станции под управлением ОС Windows через административные разделяемые ресурсы необходимо выполнение требования:

На рабочих станциях должны быть включены административные разделяемые ресурсы вида `\\computername\admin$` (в Windows Vista, Windows 7, Windows 8 и Windows 10 они по умолчанию отключены). Для этого:

1. Убедитесь, что включен общий доступ к файлам и принтерам. В Панели управления откройте **Центр управления сетями и общим доступом** -> **Изменить дополнительные параметры общего доступа**. В нужном профиле включите общий доступ к файлам и принтерам.
2. В реестре, в ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`, добавьте параметр **DWORD (32-bit)** с названием **LocalAccountTokenFilterPolicy**. Установите для него значение **1**.

> **Примечание.**
>
> После того как вы добавили параметр в реестре, необходимо заново выполнить вход в Систему.

Настройки брандмауэра

Требования к настройкам брандмауера:

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

NetBIOS Session Service	TCP	139
SMB	TCP	445

Для быстроты определения доступности рабочей станции требуется разрешить протокол ICMP.

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

6.6.3 Создание задачи первичного распространения

Важно!

Если на компьютере с ОС Astra Linux 1.6 установлен Агент InfoWatch Device Monitor версии ниже 6.11, для установки Агента **обязательно** выполните следующие действия:

1. Удалите Агент InfoWatch Device Monitor;
2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 2 (20190222SE16) (см. официальную инструкцию);
3. Установите Агент InfoWatch Device Monitor 6.11.

Первичное распространение (установка средствами Консоли Управления) Агентов InfoWatch Device Monitor выполняется с помощью **агентов установки**. Агент установки - это исполняемый файл. В ходе выполнения задачи он передается на рабочие станции и автоматически запускается, получая с сервера актуальную версию Агента.

Важно!

Если учетная запись, от имени которой запущен Сервер, не имеет прав администратора на всех рабочих станциях, где будет производиться установка, то для первичного распространения Агентов Device Monitor потребуется ввод имени и пароля учетной записи, обладающей правами администратора на:

- всех целевых рабочих станциях;
- компьютере, где работает Консоль управления (DM);
- компьютере, где работает сервер Device Monitor.

Если у используемой учетной записи истекает пароль учетной записи Windows (предупреждение о необходимости смены пароля отображается в WIndows за 3 дня до истечения пароля), то задача первичного распространения, запущенная от имени этого пользователя, не сможет быть выполнена.

Если ввод имени и пароля администратора невозможен, вы можете создать собственный установочный комплект Агентов InfoWatch Device Monitor (см. "*InfoWatch Traffic Monitor. Руководство по установке* ", статья "Создание пакета установки") и установить его другими способами (см. "*InfoWatch Traffic Monitor. Руководство по установке*", статьи "Локальная установка Агента" и "Установка Агента с помощью средств распространения программного обеспечения").

Важно!

Если на рабочей станции установлено программное обеспечение Kaspersky Internet Security, то для установки Агента InfoWatch Device Monitor необходимо отключить самозащиту Kaspersky Internet Security.

О том, как выключить самозащиту, см. интернет-статью "Как включить/выключить самозащиту Kaspersky Internet Security".

Чтобы создать задачу первичного распространения Агента InfoWatch Device Monitor:

1. Перейдите к разделу **Задачи**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить задачу**;
   - нажмите **Добавить задачу** в верхней части раздела **Задачи**.

   Откроется диалоговое окно **Мастера создания задачи**.
3. Выберите **Задача первичного распространения** (для установки агента на компьютеры с ОС Windows) или **Задача первичного распространения (Linux)** (для установки агента на компьютеры с ОС Astra Linux), введите имя задачи и ее описание, затем нажмите **Далее**.
4. Создайте список компьютеров, на которые необходимо установить Агент Device Monitor. Чтобы добавить компьютер (или несколько компьютеров):
   a. Нажмите **Добавить**. В открывшемся окне вы можете выбрать компьютеры:
      - из директории;
      - из сетевого окружения Microsoft Windows Network;
      - из дерева ALD;
      - из числа ранее зарегистрированных в Системе (например, в результате ручной установки Агента Device Monitor) и уже принадлежащих существующим группам Device Monitor (узел **Группы компьютеров DM**).

   b. Выберите необходимые компьютеры или группы компьютеров. Свернутые группы отмечены пиктограммой ; развернутые - . Чтобы развернуть или свернуть группу, нажмите на или дважды нажмите на названии группы левой кнопкой мыши.
   Вы также можете указать имена или IP-адреса компьютеров следующими способами:
      - вручную в строке, расположенной внизу диалогового окна. При перечислении используйте точку с запятой;
      - нажать **Импорт** и загрузить текстовый файл, где перечислены IP-адреса или DNS-имена компьютеров: каждая запись должна начинаться с новой строки; пустых строк быть не должно.

   c. После того, как вы выберете компьютеры, нажмите **ОК**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи отобразится список выбранных компьютеров.
   Чтобы удалить компьютер из списка, выберите его имя и нажмите **Удалить**.
   Когда вы полностью определите список компьютеров, нажмите **Далее.**
5. Мастер создания задачи отобразит сервера, которые на данный момент зарегистрированы в Системе.
   Вы также можете изменить директорию на компьютерах, куда будет устанавливаться Агент (по умолчанию – `%Program Files%\Infowatch\DeviceMonitor\Client`).

Важно!

Путь к каталогу может содержать следующие символы: 0-9,a-z,A-Z, ":", ".", "_", "-", "\", " ". При наличии в пути других символов, установка Агента будет некорректной.

Нажмите **Далее**.

6. Мастер создания задачи отобразит уникальное имя для сертификата proxy-сервера Device Monitor (Issuer Distinguished name, Proxy Root Issuer DN). При необходимости вы можете изменить его параметры; при этом имя должно соответствовать стандарту X.509, обязательно содержать поле CN (Common Name), поля внутри имени должны быть разделены запятой.
   Нажмите **Далее**.
7. Определите настройки работы Агента:
   - Чтобы защитить Агент от удаления сотрудником, укажите пароль, который будет запрашиваться при попытке удалить Агент Device Monitor, и подтвердите его.
   - **Скрывать присутствие агента на компьютере до получения конфигурации с сервера DM** – признак того, что Система будет скрывать присутствие Агента на рабочих станциях до установки связи с сервером DM.

     Важно!

     Неуведомление об использовании перехватчика может входить в конфликт с действующим законодательством вашей страны.

     Важно!

     Настройки скрытия/оповещения используются на Агенте до первого обращения к серверу. После обращения к серверу будут действовать настройки той группы компьютеров, к которой принадлежит данный компьютер.

     Важно!

     Если на контролируемом компьютере включена антивирусная защита, то антивирус может выявлять работу Device Monitor: например, в списке процессов, запущенных на контролируемом компьютере или в списке программ, инициирующих контроль.

     если данная настройка не отмечена, в области уведомлений панели задач Windows на компьютере, где установлен Агент, будет отображаться пиктограмма

. При нажатии на этот значок доступна информация о работе Агента, а также список контролируемых в данный момент устройств.

- **Устанавливать компонент перехвата сетевого трафика** - если настройка отмечена, на компьютер будет установлен компонент **iw_proxy**.
- **Устанавливать компонент контроля сетевых соединений** - если настройка отмечена, на компьютер будет установлен перехватчик **Network Monitor**.

> **Важно!**
>
> Не рекомендуется устанавливать компонент контроля периметра сети в образ, который впоследствии будет являться базовым для инфраструктуры VDI под управлением Citrix Provisioning Services, т.к. это приведет к нарушению данной технологии и негативно повлияет на работоспособность всей схемы.

- Определите параметры перезапуска задачи: они будут использованы, если первый запуск по каким-либо причинам не произошел; если запуск завершился с ошибкой, то повторный запуск производиться не будет. Укажите количество попыток и время между попытками, в минутах.
- Чтобы выполнение задачи началось немедленно после ее сохранения, отметьте настройку **Запустить задачу сразу после сохранения**.
- Укажите параметры учетной записи, от имени которой будет запущена задача. Эта учетная запись должна обладать правами администратора на всех компьютерах, где будет производиться установка.

> **Важно!**
>
> Пароль учетной записи, от имени которой производится запуск задачи, в Системе не сохраняется.
> Если по окончании создания задачи она не будет запущена немедленно, то при последующем запуске этой задачи из Консоли управления (DM) потребуется ввод пароля.
> Если у используемой учетной записи истекает пароль учетной записи Windows (предупреждение о необходимости смены пароля отображается в WIndows за 3 дня до истечения пароля), то задача первичного распространения, запущенная от имени этого пользователя, не сможет быть выполнена.

По окончании настройки нажмите **Далее**.

8. Определите параметры перезагрузки компьютера.

> **Примечание.**
>
> Если на предыдущем шаге была выбрана настройка **Скрывать присутствие агента на компьютере до получения конфигурации с сервера DM**, то данные настройки будут недоступны.

Возможные значения:

- **Ожидать перезагрузки без уведомления сотрудника**. Агент может:
  - начать уведомление сотрудника сразу (параметр *Не ожидать*),
  - начать уведомление сотрудника через указанное время (параметр *Ожидать* - требуется указать время до начала уведомлений),
  - не уведомлять сотрудника вообще (параметр *Ожидать бесконечно*).
- **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки**. После завершения ожидания перезагрузки в "молчаливом" режиме (см. настройку **Ожидать перезагрузки без уведомления сотрудника**), или сразу же после завершения процесса установки, Агент Device Monitor начнет уведомлять сотрудника о необходимости перезагрузки:
  - в течение указанного времени (параметр *Уведомлять в течение*);
  - постоянно (параметр *Уведомлять бесконечно*);
  - не уведомлять сотрудника вообще (параметр *Не уведомлять*).

  При необходимости, измените длительность и частоту напоминаний и укажите текст сообщения, которое будет отображаться в напоминании о необходимости перезагрузки. Сообщение может содержать не более 255 символов.
- **Показать предупреждение перед принудительной перезагрузкой**. если параметр отмечен, то сотруднику будет показано окно о принудительной перезагрузке компьютера и дано 5 минут на завершение своих операций. После этого перезагрузка будет осуществлена принудительно. если параметр не отмечен, то принудительная перезагрузка (если она вообще должна производиться согласно сделанным настройкам) будет произведена неожиданно для сотрудника.

  > **Важно!**
  >
  > Принудительная перезагрузка будет произведена, если ни параметр **Ожидать перезагрузки без уведомления сотрудника**, ни параметр **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки** не установлены, либо период ожидания завершен, а сотрудник так и не перезагрузил компьютер.

По окончании настройки нажмите **Далее**.

9. Просмотрите сводку информации о задаче. если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). если все указано верно, нажмите **Готово**.

6.6.4 Создание задачи обновления

Важно!

При обновлении DM до версии 6.7 необходимо обновлять агенты с помощью задач первичного распространения (см. статью "Создание задачи первичного распространения"), иначе могут возникать ошибки. При обновлении до всех других версий используется процедура, описанная в данной статье.

Если на компьютере с ОС Astra Linux 1.6 установлен Агент InfoWatch Device Monitor версии ниже 6.11, для обновления Агента **обязательно** выполните следующие действия:

1. Удалите Агент InfoWatch Device Monitor;
2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 2 (20190222SE16) (см. официальную инструкцию);
3. Установите Агент InfoWatch Device Monitor 6.11.

Агенты InfoWatch Device Monitor необходимо обновить после обновления серверной части InfoWatch Device Monitor: подробнее см. "*InfoWatch Traffic Monitor. Руководство по установке*", раздел "Обновление серверной части InfoWatch Device Monitor".

Примечание.

Помимо описанного ниже способа, вы можете использовать функцию автоматического создания задачи обновления для выбранных компьютеров, как описано в разделе "Обновление Агентов на контролируемых рабочих станциях" (см. документ "*InfoWatch Traffic Monitor. Руководство по установке*").

Чтобы создать задачу обновления Агентов InfoWatch Device Monitor, перейдите к к разделу **Задачи** и выполните одно из следующих действий:

- в главном меню выберите команду **Правка** > **Добавить задачу**;
- нажмите **Добавить задачу** в верхней части раздела **Задачи**.

В открывшемся диалоговом окне **Мастер создания задачи** выполните следующие шаги:

1. Выберите **Задача обновления** (для обновления компьютеров с ОС Windows) или **Задача обновления (Linux)** (для обновления компьютеров с ОС Astra Linux), введите имя задачи и ее описание, затем нажмите **Далее**.
2. Создайте список компьютеров, на которых необходимо обновить Агент Device Monitor. Чтобы добавить компьютер (или несколько компьютеров):
   a. Нажмите **Добавить**. В открывшемся диалоговом окне **Выбор компьютеров**, в узле **Группы компьютеров DM**, отобразится перечень компьютеров, на которые установлен Агент Device Monitor, версия которого не соответствует версии Сервера Device Monitor, но которые могут быть автоматически обновлены (версия агентского ПО должна быть 4.0.651 и выше).
   b. Выберите необходимые компьютеры или группы компьютеров. Свернутые группы отмечены пиктограммой ; развернутые - . Чтобы развернуть или свернуть группу, нажмите на или дважды нажмите на названии группы левой кнопкой мыши. Вы также можете использовать строку поиска **Фильтр по названию компьютера**. Чтобы начать поиск компьютера, нажмите **Найти**.

c. После того как вы укажете добавляемые компьютеры, нажмите **ОК**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи отобразятся выбранные компьютеры.

Чтобы удалить компьютер из списка, выберите его имя и нажмите **Удалить**.
После того, как вы полностью определите список компьютеров, нажмите **Далее**.

3. Укажите параметры перезагрузки компьютеров:
   - **Ожидать перезагрузки без уведомления сотрудника**. Агент может:
     - Уведомить сотрудника сразу (параметр *Не ожидать*),
     - Уведомить сотрудника через указанное время (параметр *Ожидать* - требуется указать время до начала уведомлений),
     - Не уведомлять сотрудника (параметр *Ожидать бесконечно*).
   - **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки**. После завершения ожидания перезагрузки в "молчаливом" режиме (см. настройку **Ожидать перезагрузки без уведомления сотрудника**) или сразу же после завершения процесса установки Агент Device Monitor начнет уведомлять сотрудника о необходимости перезагрузки в течение указанного времени (параметр *Уведомлять в течение*) или постоянно (параметр *Уведомлять бесконечно*), либо не будет уведомлять (параметр *Не уведомлять*). При необходимости, измените длительность и частоту напоминаний и укажите текст сообщения, которое будет отображаться в напоминании о необходимости перезагрузки. Сообщение может содержать не более 255 символов.
   - **Показать предупреждение перед принудительной перезагрузкой** - признак того, будет ли показано окно о принудительной перезагрузке компьютера (сотруднику дается 5 минут на завершение операций) или перезагрузка будет осуществлена принудительно.

> **Важно!**
>
> Если на рабочей станции включена настройка **Скрывать присутствие агента на рабочей станции**, то уведомления отображаться не будут.

4. Укажите **Параметры перезапуска задачи**: они будут использованы, если первый запуск по каким-либо причинам не произошел. Если запуск завершился с ошибкой, то повторный запуск производиться не будет. Укажите количество попыток и время между попытками (в минутах).
   При необходимости отметьте поле **Запустить задачу сразу после сохранения**: задача будет запущена сразу же после ее сохранения.
   Нажмите **Далее**.
5. Просмотрите сводку информации о задаче. Если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). Если все указано верно, нажмите **Готово**.

Важно!

Если на компьютере используется программное обеспечение Kaspersky Internet Security, то для обновления Агентов InfoWatch Device Monitor необходимо отключить самозащиту Kaspersky Internet Security.
О том, как выключить самозащиту, см. интернет-статью "Как включить/выключить самозащиту Kaspersky Internet Security".

6.6.5 Создание задачи смены пароля деинсталляции

Чтобы создать задачу смены пароля, требуемого у сотрудника при попытке удалить Агента InfoWatch Device Monitor:

1. Перейдите к разделу **Задачи**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить задачу**;
   - воспользуйтесь кнопкой **Добавить задачу**, расположенной в верхней части раздела Задачи.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно Мастера создания задачи.
3. На шаге 1 выберите **Задача смены пароля деинсталляции**, введите имя задачи и ее описание, затем нажмите **Далее**.
4. На шаге 2 создайте список компьютеров, на которых необходимо сменить пароль деинсталляции. Чтобы добавить компьютер (или несколько компьютеров):
   a. Нажмите **Добавить**. В открывшемся диалоговом окне **Выбор компьютеров**, в узле **Группы компьютеров DM**, отобразится перечень компьютеров, на которые установлен Агент Device Monitor. Вы также можете использовать строку поиска **Фильтр по названию компьютера**. Чтобы найти компьютер, нажмите **Найти**.
   b. Выберите необходимые компьютеры или группы компьютеров, отмечая их. Свернутые группы отмечены пиктограммой ; развернутые - . Для того, чтобы развернуть или свернуть группу, дважды нажмите на ней левой кнопкой мыши.
   c. После того, как вы укажете компьютеры, нажмите **Выбрать**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи будет отображен перечень выбранных компьютеров.

   Чтобы удалить компьютер из списка, выберите ее имя и нажмите **Удалить**.
   После того, как вы полностью определите список компьютеров, нажмите **Далее**.
5. На шаге 3 укажите:
   - **Пароль**, который будет запрашиваться у сотрудника при попытке удалить Агент Device Monitor. Подтвердите пароль.
   - **Параметры перезапуска задачи**: они будут использованы, если первый запуск по каким-либо причинам не произошел; если запуск завершился с ошибкой, то повторный запуск производиться не будет. Укажите количество попыток и время между попытками, в минутах.
   - При необходимости, отметьте поле **Запустить задачу немедленно**: задача будет запущена сразу же после ее сохранения.

   Нажмите **Далее**.

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

6.6.6 Создание задачи удаления

Чтобы создать задачу централизованного удаления Агентов InfoWatch Device Monitor:

1. Перейдите к разделу **Задачи**.
2. Выполните одно из следующих действий:
   - в главном меню выберите команду **Правка** > **Добавить задачу**;
   - воспользуйтесь кнопкой **Добавить задачу**, расположенной в верхней части раздела **Задачи**.

   В результате выполнения любого из этих действий на экран будет выведено диалоговое окно **Мастера создания задачи**.
3. На шаге 1 выберите **Задача удаления продукта** (для удаления агента с компьютеров с ОС Windows) или **Задача удаления продукта (Linux)** (для удаления агента с компьютеров с ОС Astra Linux), введите имя задачи и ее описание, затем нажмите **Далее**.
4. На шаге 2 создайте список компьютеров, с которых необходимо удалить Агент Device Monitor. Чтобы добавить компьютер (или несколько компьютеров):
   a. Нажмите **Добавить**. В открывшемся диалоговом окне **Выбор компьютеров**, в узле **Группы компьютеров DM**, отобразится перечень компьютеров, на которые установлен Агент Device Monitor. Также вы можете использовтаь строку поиска **Фильтр по названию компьютера**. Чтобы начать поиск компьютера, нажмите **Найти**.
   b. Выберите необходимые компьютеры или группы компьютеров. Свернутые группы отмечены пиктограммой ; развернутые - . Для того, чтобы развернуть или свернуть группу, дважды нажмите на ней левой кнопкой мыши.
   Вы также можете перечислить имена или IP-адреса компьютеров:
      - вручную, в строке внизу диалогового окна; при перечислении используйте точку с запятой;
      - нажать **Импорт** и загрузить текстовый файл, где перечислены IP-адреса или DNS-имена компьютеров: каждая запись должна начинаться с новой строки; пустых строк быть не должно.

   c. После того, как вы укажете добавляемые компьютеры, нажмите **Выбрать**. Диалоговое окно **Выбор компьютеров** будет закрыто, а в окне мастера создания задачи отобразятся выбранные компьютеры.

   Чтобы удалить компьютер из списка, выберите его имя и нажмите **Удалить**.
   После того, как вы полностью определите список компьютеров, нажмите **Далее**.
5. На шаге 3 определите параметры перезапуска задачи: они будут использованы, если первый запуск по каким-либо причинам не произошел; если запуск завершился с ошибкой, то повторный запуск производиться не будет. Укажите количество попыток и время между попытками, в минутах.
   Чтобы начать выполнение созданной задачи сразу же после ее сохранения, отметьте поле **Запустить задачу немедленно**.
   Нажмите **Далее**.

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

> **Важно!**
>
> В случае наличия на компьютере программного обеспечения Kaspersky Internet Security для удаления Агентов InfoWatch Device Monitor необходимо отключить самозащиту Kaspersky Internet Security.
> Чтобы выключить самозащиту см. интернет-статью "Как включить/выключить самозащиту Kaspersky Internet Security"

6.6.7 Запуск, остановка, редактирование и удаление задачи

если при создании задачи вы выбрали настройку **Запустить задачу сразу после сохранения**, то задача начнет выполняться немедленно после ее создания. В противном случае вам будет необходимо выполнить запуск задачи вручную. Также это может потребоваться в том случае, если по каким-либо причинам вам потребовалось остановить задачу, и необходимо запустить ее вновь.

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

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

> **Важно!**
>
> При запуске задач распространения/обновления/удаления агентов на Astra Linux запрашивается логин и пароль для авторизации на рабочих станциях. При этом пользователь, логин и пароль которого указывается при запуске, должен находиться в списке `sudo users` на указанных в задаче рабочих станциях.

Действие	Шаги
Запуск задачи	▪ в главном меню выберите команду **Правка** > **Выполнить**; ▪ воспользуйтесь кнопкой **Выполнить**, расположенной в верхней части панели Задачи; ▪ щелкните по задаче правой кнопкой мыши и в контекстном меню выберите **Выполнить**.
Остановка задачи	▪ в главном меню выберите команду **Правка** > **Остановить**; ▪ воспользуйтесь кнопкой **Остановить**, расположенной верхней части панели Задачи; ▪ щелкните по задаче правой кнопкой мыши и в контекстном меню выберите **Остановить**.

Изменение списка компьютеров в задаче	▪ воспользуйтесь кнопками  **Добавить компьютер в задачу** или  **Исключить компьютер из задачи**, расположенными в верхней части рабочей области; ▪ щелкните правой кнопкой на строке необходимого компьютера и выберите **Добавить компьютер в задачу** или  **Исключить компьютер из задачи**; ▪ нажмите Ctrl+Shift+N для добавления компьютера в задачу или Delete для исключения компьютера из задачи. **Внимание!** Удалить рабочую станцию с запущенной, но незавершенной задачей, нельзя.
Редактирование задачи	▪ в главном меню выберите команду **Правка** > **Редактировать задачу**; ▪ воспользуйтесь кнопкой  **Редактировать задачу**, расположенной верхней части панели навигации; ▪ щелкните правой кнопкой на названии задачи и выберите  **Редактировать задачу**; ▪ дважды щелкните по задаче левой кнопкой мыши; ▪ нажмите Ctrl+E. Определите новые параметры задачи, как это делается при ее создании (см. "Создание задачи первичного распространения", "Создание задачи обновления", "Создание задачи смены пароля деинсталляции", "Создание задачи удаления")
Удаление задачи	▪ в главном меню выберите команду **Правка** > **Удалить задачу**; ▪ воспользуйтесь кнопкой  **Удалить задачу**, расположенной верхней части панели навигации; ▪ щелкните правой кнопкой на названии задачи и выберите  **Удалить задачу**; ▪ нажмите Ctrl+D. **Внимание!** Удалить задачу, где есть компьютеры с запущенной, но незавершенной задачей, нельзя.
Просмотр журнала ошибок для компьютера	▪ воспользуйтесь кнопкой  **Журнал ошибок**, расположенной в верхней части рабочей области; ▪ щелкните правой кнопкой на строке необходимого компьютера и выберите пункт **Журнал ошибок**; ▪ нажмите Ctrl+L.

6.6.8 Ошибки установки Агентов

В процессе выполнения задач на удаленную установку Агентов InfoWatch Device Monitor на рабочие станции возможно возникновение проблем установки. На это будет указывать значение параметра **Статус выполнения задачи** в перечне задач: см. "Просмотр задач".

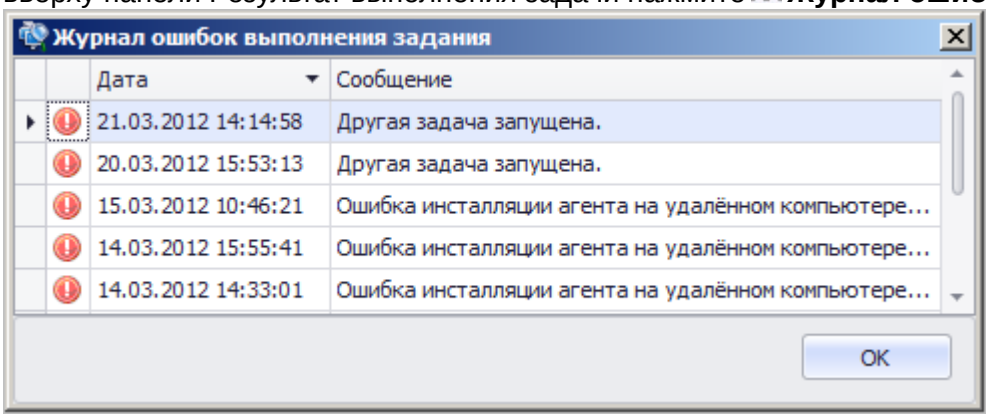
Чтобы просмотреть ошибки, возникавшие при выполнении задачи:

1. Перейдите к разделу **Задачи**.

2. На панели **Задачи** выберите задачу, ошибки выполнения которой необходимо просмотреть.
3. В столбце **Статус выполнения задачи** выберите значение фильтра Ошибка (о работе с фильтрами см. "Использование стандартных фильтров").

> **Примечание:**
>
> Статус **Нет доступа** свидетельствует о том, что рабочая станция недоступна (выключена или отключена от сети).

4. В строке рабочей станции, на которой возникла ошибка, выполните одно из следующих действий:
   - нажмите правой кнопкой мыши и в контекстном меню выберите **Журнал ошибок**;
   - дважды щелкните левой кнопкой мыши на строке необходимой рабочей станции;
   - вверху панели Результат выполнения задачи нажмите **Журнал ошибок**.



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

Подробную информацию о причинах ошибки вы можете получить из ее описания, кода ошибки или журнала, отображаемого в окне с описанием ошибки. В частности, ошибки могут быть обусловлены следующими причинами:

- рабочая станция недоступна (выключена или отключена от сети);
- другая задача или пользователь блокирует процесс установки или необходимую перезагрузку компьютера (типичное описание - "Другая задача запущена");
- на целевой рабочей станции запрещено использование административных ресурсов;
- учетная запись, используемая для установки, имеет недостаточно прав на целевой рабочей станции.

Если все условия, необходимые для выполнения удаленной установки Агента, перечисленные в разделе "Подготовка к установке" выполнены, и исключена блокировка выполнения задачи пользователем, но, тем не менее, ошибку устранить не удается, вы можете обратиться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com, приложив к письму описание ошибки и содержимое лога.

6.6.9 Создание пакета установки

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

- Папка на системном диске рабочих станций, куда будет устанавливаться Агент – `%Program Files%\Infowatch\DeviceMonitor\Client`.
- Пароль деинсталляции – отсутствует.
- После установки Агент Device Monitor начинает уведомлять сотрудника о необходимости перезагрузки компьютера с сообщением. Текст сообщения - "*Необходимо как можно скорее перезагрузить компьютер*". Уведомления отображаются бесконечно, с интервалом в 10 минут.

Для того чтобы изменить эти настройки, вы можете создать собственный инсталляционный комплект.

Чтобы создать пакет для установки Агента InfoWatch Device Monitor:

1. В главном меню выберите команду **Инструменты** > **Создать пакет установки**.
   На экран будет выведено диалоговое окно Мастера создания пакета установки.
2. На шаге **Отметьте сервера DM и каталог установки** отображаются сервера InfoWatch Device Monitor, которые на данный момент зарегистрированы в Системе. Они будут использоваться Агентом для первоначальной установки.
   При необходимости, измените директорию на рабочих станциях, куда будет устанавливаться Агент. Укажите локальную или сетевую директорию, куда будет сохранен готовый набор инсталляционных пакетов.
   Нажмите **Далее**.
3. Мастер создания задачи отобразит уникальное имя для сертификата proxy-сервера Device Monitor (Issuer Distinguished name, Proxy Root Issuer DN). При необходимости вы можете изменить его параметры; при этом имя должно соответствовать стандарту X.509, содержать поле CN (Common Name), поля внутри имени должны быть разделены запятой. Нажмите **Далее**.
4. На шаге **Укажите параметры перезагрузки** определите следующие параметры:
   - **Ожидать перезагрузки без уведомления сотрудника**. Агент может:
     - Начать уведомление сотрудника сразу (параметр *Не ожидать*),
     - Начать уведомление сотрудника через указанное время (параметр *Ожидать* - требуется указать время до начала уведомлений),
     - Не уведомлять сотрудника вообще (параметр *Ожидать бесконечно*).
   - **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки**. После завершения ожидания перезагрузки в "молчаливом" режиме (см. настройку **Ожидать перезагрузки без уведомления сотрудника**), или сразу же после завершения процесса установки, Агент Device Monitor начнет уведомлять сотрудника о необходимости перезагрузки в течение указанного времени (параметр *Уведомлять в течение*) или постоянно (параметр *Уведомлять бесконечно*), либо не будет уведомлять (параметр *Не уведомлять*). При необходимости, измените длительность и частоту напоминаний и укажите текст сообщения, которое будет отображаться в напоминании о необходимости перезагрузки. Сообщение может содержать не более 255 символов.
   - **Показать предупреждение перед принудительной перезагрузкой** - признак того, отобразит ли Агент уведомление окно о принудительной перезагрузке компьютера и даст ли сотруднику 5 минут на завершение своих операций. если

опция не выбрана, то принудительная перезагрузка (если она предусмотрена другими настройками) будет осуществлена неожиданно для сотрудника.

> **Важно!**
>
> Предупреждение перед принудительной перезагрузкой возникает, если ни параметр **Ожидать перезагрузки без уведомления сотрудника**, ни параметр **Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки** не установлены, или период действия их завершен, и сотрудник не перезагрузил компьютер.

Нажмите **Далее**.

5. Определите настройки работы Агента до первого подключения к Серверу:
   - Чтобы защитить Агента от удаления сотрудником, укажите пароль, который будет запрашиваться при попытке удалить Агент Device Monitor, и подтвердите его.
   - **Отображать сотруднику уведомления о работе клиентского модуля** – признак того, что при попытке сотрудника выполнить действие, запрещенное политикой безопасности (DM), ему будет отображаться предупреждающее уведомление. Подробнее см. "Настройка уведомлений сотрудника о нарушении правил"
   - **Скрывать присутствие агента на рабочей станции** – признак того, что Система будет скрывать присутствие Агента на рабочих станциях.

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

     > **Важно!**
     >
     > Если на контролируемом компьютере включена антивирусная защита, то антивирус может выявлять работу Device Monitor: например, в списке процессов, запущенных на контролируемом компьютере или в списке программ, инициирующих контроль.

     > **Важно!**
     >
     > Уведомление о перезагрузке компьютера не будет отображаться, если включено "скрывать присутствие агента на компьютере".

     Если данная настройка не отмечена, в области уведомлений панели задач

Windows на компьютере, где установлен Агент, будет отображаться пиктограмма . При нажатии на нее доступна информация о работе Агента, а также список контролируемых в данный момент устройств.

- **Устанавливать компонент перехвата сетевого трафика** - устанавливает на рабочую станцию компонент **iw_proxy**.
- **Устанавливать компонент контроля сетевых соединений** - устанавливает на рабочую станцию перехватчик **Network Monitor**.

> **Важно!**
>
> На сервер с Citrix Provisioning Services нельзя устанавливать компонент контроля сетевых соединений: это может привести к серьезным проблемам в работе сервера.

Нажмите **Далее**.

6. Просмотрите сводку информации о пакете установки. если какие-либо параметры требуется изменить, вы можете вернуться к настройкам (кнопка **Назад**). если все указано верно, нажмите **Готово**.

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

6.7 Дополнительные возможности

Для более удобной работы с Консолью управления (DM) вы можете воспользоваться функциями фильтрации, группировки и сортировки данных, выводящихся в таблицах.
Также некоторые функции системы доступны для выполнения с помощью клавиш быстрого доступа.

6.7.1 Фильтрация табличных данных

Информация в таблицах может быть отфильтрована по одному или нескольким признакам с помощью фильтров различной степени сложности. После применения фильтра в таблице отображаются только те записи, которые удовлетворяют заданным условиям фильтрации.

Работа с фильтрами описана в следующих подразделах:

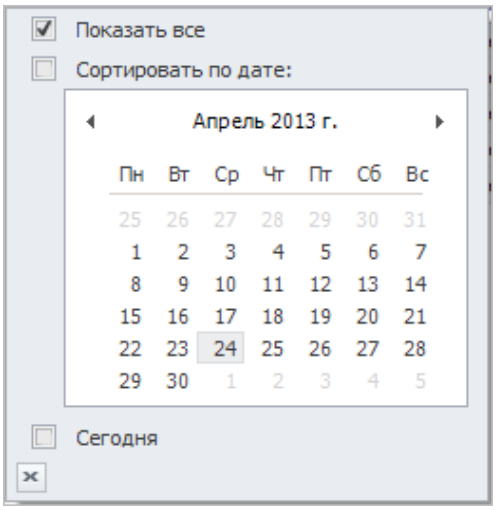
- Фильтр по дате
- Использование стандартных фильтров
- Пользовательский фильтр
- Редактирование фильтра
- Отмена фильтра

Фильтр по дате

Если в таблице отображается характеристика какого-либо временного параметра (например, дата и время установки Агента, время записи в журнал Консоли (DM), время последнего обращения к рабочей станции, дата зарегистрированного события и т.п.), то вы можете отфильтровать записи по этому столбцу, выбрав необходимую дату или период.

Чтобы просмотреть записи, относящиеся к определенной дате или периоду времени:

1. В строке заголовков столбцов таблицы подведите курсор мыши к атрибуту, характеризующему время/дату.
2. Нажмите на кнопку , расположенную справа от названия столбца.



3. В раскрывшейся форме выберите один из следующих фильтров:
   - **Показать все** – отметьте поле, чтобы отобразились записи независимо от их даты.
   - **Сортировать по дате** – в календаре выберите необходимую дату.
     Чтобы выбрать временной период, выберите его, не отпуская левую кнопку мыши.
     Чтобы перейти от отображения дат месяца к отображению месяцев или лет, нажмите на названии месяца/года левой кнопкой мыши.
     Чтобы перейти на месяц вперед или назад, пользуйтесь стрелками.
   - **Сегодня**; **Вчера**; **На прошлой неделе**; **Ранее на этой неделе**; **Ранее в этом году** – состав полей зависит от значений в столбце: например, если записей за текущую дату нет, то поле **Сегодня** будет отсутствовать. Отметьте это поле, чтобы отобразились только те записи, дата которых находится в описанном диапазоне.
4. Чтобы применить выбранный фильтр и закрыть форму, нажмите либо щелкните левой клавишей мыши по пространству за пределами формы.

Использование стандартных фильтров

Чтобы отфильтровать записи по одному атрибуту:

1. В строке заголовков столбцов таблицы подведите курсор мыши к заголовку того столбца, название которого соответствует нужному атрибуту.
2. Чтобы раскрыть список фильтров, нажмите на кнопку , расположенную справа от названия столбца.
3. В раскрывшемся списке выберите один из следующих фильтров:
   - **Пустые**. Отображение записей, в которых выбранный атрибут имеет значение `<Is Null>` (пустое поле).
   - **Непустые**. Отображение записей, в которых выбранный атрибут имеет значение `<Is Not Null>` (т.е. в поле содержится любое значение атрибута).
   - `<значение атрибута>`. Отображение записей, в которых выбранный атрибут имеет указанное значение.

Примечание.

Выбрав пункт **Условие** из списка фильтров, вы сможете настроить собственные условия фильтрации (подробнее см. "Пользовательский фильтр").

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

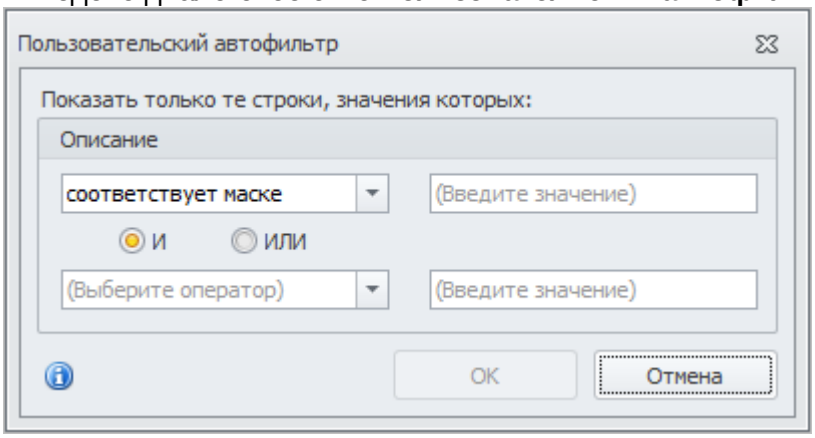
Чтобы отфильтровать записи по нескольким атрибутам, повторите процедуру создания простого фильтра для всех атрибутов, по которым будет производиться фильтрация.

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

Пользовательский фильтр

Чтобы задать собственные условия фильтрации:

1. В строке заголовков столбцов таблицы подведите курсор мыши к заголовку того столбца, название которого соответствует нужному атрибуту.
2. Раскройте список фильтров, нажав на кнопку, расположенную справа от названия столбца.
3. В раскрывшемся списке выберите пункт **Условие**. После этого на экран будет выведено диалоговое окно **Пользовательский автофильтр**.



4. В данном окне задайте условия фильтрации:
   - Выберите ограничение условия из раскрывающегося списка в верхнем левом поле.

     Примечание.

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

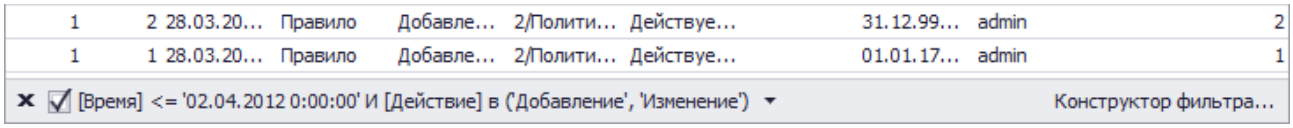
   - В верхнем правом поле укажите значение условия.

- Если необходимо задайте дополнительное условие, для чего выберите нужный логический оператор и укажите второе условие в нижней строке.

> **Примечание.**
>
> Логический оператор **И** выбирают, если нужно отфильтровать записи, удовлетворяющие и первому, и второму условию одновременно. Выбор логического оператора **ИЛИ** указывает на то, что будут отфильтрованы записи, удовлетворяющие хотя бы одному из заданных условий.

5. Нажмите **ОК**, чтобы применить фильтр.

После применения фильтра в таблице будут отображены только те записи, которые соответствуют заданным условиям фильтрации. В нижней части того окна, в котором используется фильтр, отобразится строка с условиями фильтрации.



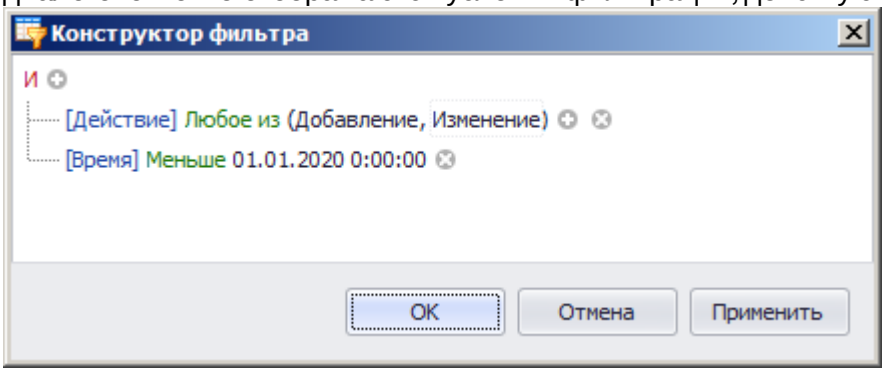
Чтобы отменить действие фильтра и просмотреть все записи таблицы, снимите отметку в строке фильтра. Чтобы применить фильтр вновь, установите отметку.

Чтобы повторно использовать фильтр, щелкните левой кнопкой мыши по строке фильтра и выберите нужный фильтр из раскрывшегося списка последних применявшихся фильтров. Пользовательские фильтры сохраняются до тех пор, пока не будет закрыто окно, в котором применялся данный фильтр.

Редактирование фильтра

Чтобы отредактировать действующий фильтр:

1. В строке с условиями фильтрации нажмите **Конструктор фильтра**. В открывшемся диалоговом окне отображаются условия фильтрации, действующие в текущий момент.



2. Отредактируйте условия фильтрации. При этом можно выполнять следующие действия:

Действие	Шаги
Изменить атрибут, значение атрибута или оператор	a. Щелкните левой кнопкой мыши по названию атрибута/значения атрибута/оператора b. В меню выберите необходимое значение
Добавить простое условие	Нажмите на кнопку справа от логического оператора или Выберите команду **Добавить условие** в меню логического оператора
Удалить условие	Нажмите на кнопку в конце строки условия
Добавить группу условий	a. Щелкните левой кнопкой мыши по названию логического оператора b. В меню выберите **Добавить группу**
Удалить группу условий	a. Щелкните левой кнопкой мыши по названию группы условий оператора b. В меню выберите **Удалить группу**
Удалить все условия	Выберите команду **Очистить все** в меню логического оператора

3. Нажмите **Применить**, чтобы применить фильтр и просмотреть результаты фильтрации, не закрывая окна **Конструктор фильтров**.
4. Нажмите **ОК**.

Отмена фильтра

Чтобы отменить назначенный фильтр, выполните одно из следующих действий:

- Щелкните левой кнопкой мыши по заголовку столбца, к которому был применен фильтр, и в раскрывшемся списке фильтров выберите пункт **Все**.
  Если был задан составной фильтр, повторите данную операцию для каждого условия, которое нужно отменить.
- Снимите отметку в левой части строки с условиями фильтрации.
- Нажмите на кнопку , расположенную в левой части строки с условиями фильтрации. После этого строка с условиями фильтрации будет закрыта.

6.7.2 Группирование и сортировка записей

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

Чтобы сгруппировать записи по какому-либо атрибуту, в строке заголовков столбцов таблицы щелкните левой кнопкой мыши по заголовку столбца, название которого соответствует нужному атрибуту, и не отпуская кнопку, перетащите заголовок столбца на панель группы. Название атрибута, по которому производилось группирование записей, будет отображено на панели группы.

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

> **Примечание.**
>
> Порядок группирования записей можно изменить, меняя местами заголовки столбцов в схеме группы. Первым в группировании участвует столбец, заголовок которого расположен слева на верхнем уровне схемы группы.

Сгруппированные записи отображаются в свернутом виде. Чтобы просмотреть информацию по отдельной записи, нажмите на кнопку , расположенную слева от записи, которую нужно просмотреть в развернутом виде. Чтобы свернуть запись, нажмите на кнопку , расположенную слева от записи.

Вы можете отменить группирование по одному или нескольким атрибутам, удаляя столбцы из схемы группы.

Чтобы отменить группирование записей по какому-либо атрибуту:

1. На панели группы щелкните левой кнопкой мыши по заголовку столбца, который вы хотите удалить из схемы группы, и, не отпуская кнопку, перетащите его в строку заголовков таблицы. Местоположение столбца при этом будет указываться прямоугольной рамкой.
2. Перемещайте заголовок столбца вдоль строки заголовков, чтобы выбрать нужное положение, и затем отпустите левую кнопку мыши. В результате столбец будет перемещен на указанное место.
   Вы также можете переместить заголовок столбца на свободное пространство. В этом случае заголовок вернется на место, которое он занимал до группирования.

При помощи функции сортировки вы можете настроить отображение записей в порядке либо возрастания, либо убывания значений какого-либо атрибута таблицы.

Чтобы изменить порядок сортировки значений атрибута в столбце, подведите курсор мыши к заголовку того столбца, по которому нужно выполнить сортировку. Когда нужный заголовок будет выделен, щелкните левой кнопкой мыши. В результате все записи таблицы будут отсортированы по возрастанию/убыванию значений выбранного атрибута.

Чтобы вернуть прежний порядок сортировки, щелкните по выделенному заголовку еще раз.

6.7.3 Клавиши быстрого доступа

В следующей таблице перечислены клавиши и сочетания клавиш, используемые для быстрого доступа к различным функциям Системы.

Название функции	Клавиши быстрого доступа
Соединение с Сервером	
Подключение к Серверу	F4
Выход из Консоли	Alt+F4
Настройка элементов главного окна	
Скрытие/отображение Панели навигации	Ctrl+Shift+1
Скрытие/отображение панели Подробно	Ctrl+Shift+2
Скрытие/отображение панели Журнал консоли	Ctrl+Shift+3
Разделы Консоли управления	
Переход к разделу Политики	Ctrl+1
Переход к разделу Группы сотрудников	Ctrl+2
Переход к разделу Группы компьютеров	Ctrl+3
Переход к разделу Белые списки	Ctrl+4
Переход к разделу Категории сигнатур	Ctrl+5
Переход к разделу Приложения	Ctrl+6
Переход к разделу Журнал	Ctrl+7
Переход к разделу Задачи	Ctrl+8
Переход к разделу События	Ctrl+9
Работа со схемой безопасности (общее)	
Переход к режиму редактирования схемы безопасности	F11
Сохранение схемы безопасности	F12
Отмена сохранения схемы безопасности	Shift+F11
Разблокировка схемы безопасности (только Суперпользователь)	Ctrl+Shift+U
Обновление схемы безопасности	F5
Переход к последней версии схемы безопасности (при просмотре одной из предыдущих версий)	F9
Работа с политиками безопасности	
Создание политики безопасности	Ctrl+N

Редактирование политики безопасности	Ctrl+E
Удаление политики безопасности	Ctrl+D
Работа с правилами	
Создание правила	Ctrl+Shift+N
Редактирование правила	Ctrl+Shift+E
Удаление правила	Delete
Работа с группами сотрудников	
Создание группы сотрудников	Ctrl+N
Редактирование группы сотрудников	Ctrl+E
Удаление группы сотрудников	Ctrl+D
Работа с учетными записями сотрудников	
Добавление учетной записи сотрудника в группу	Ctrl+Shift+N
Редактирование учетной записи сотрудника	Ctrl+Shift+E
Исключение сотрудника из группы	Delete
Удаление сотрудника из схемы безопасности	Shift+Delete
Работа с группами компьютеров	
Создание группы компьютеров	Ctrl+N
Редактирование группы компьютеров	Ctrl+E
Удаление группы компьютеров	Ctrl+D
Работа с контролируемыми компьютерами	
Добавление компьютера	Ctrl+Shift+I
Исключение компьютера из группы	Delete
Удаление компьютера из схемы безопасности	Shift+Delete
Работа с белыми списками	
Создание белого списка	Ctrl+N
Редактирование белого списка	Ctrl+E
Удаление белого списка	Ctrl+D
Редактирование записи в белом списке	Ctrl+Shift+E

Работа с сигнатурами	
Создание категории сигнатур	Ctrl+N
Редактирование категории сигнатур	Ctrl+E
Удаление категории сигнатур	Ctrl+D
Исключение сигнатуры из категории	Delete
Настройка фильтров для Журнала аудита и просмотра событий	
Создание фильтра	Ctrl+N
Редактирование фильтра	Ctrl+E
Удаление фильтра	Ctrl+D
Работа с задачами удаленной установки и обновления Агентов	
Создание задачи	Ctrl+N
Редактирование задачи	Ctrl+E
Удаление задачи	Ctrl+D
Добавление компьютера в выбранную задачу	Ctrl+Shift+N
Исключение компьютера из выбранной задачи	Delete
Просмотр журнала ошибок для выбранного компьютера выбранной задачи	Ctrl+L

7 Лицензионная информация

Лицензионная информация для Системы приведена в разделе "Пользовательское лицензионное соглашение".

7.1 Пользовательское лицензионное соглашение

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями лицензионного соглашения перед началом работы с программным обеспечением.
Нажатие Вами кнопки подтверждения согласия в окне с текстом лицензионного соглашения при установке программного обеспечения или использование устанавливаемого программного обеспечения означает Ваше безоговорочное согласие с условиями настоящего лицензионного соглашения. Если Вы не согласны с условиями настоящего лицензионного соглашения, Вы должны прервать установку и/или использование программного обеспечения.

1. Предоставление лицензии

1.1. Вам предоставляется неисключительная лицензия на использование программного обеспечения (далее — ПО) (Правообладатель прав на ПО — АО «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. Если Вы используете ПО разных версий или версии ПО для разных языков, если Вы получили ПО на нескольких носителях, если Вы иным способом получили несколько копий ПО или получили ПО в составе пакета другого программного обеспечения, то общее число используемых вами лицензий, не должно превышать их количества определенного Договором между Вами и Вашим лицензиаром;

1.4. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Такая копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.

1.5. 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, за исключением случаев, предусмотренных законодательством РФ.

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. Правообладатель имеет право заблокировать лицензионный ключ в случае нарушения Вами условий настоящего Соглашения и Договора, заключенного между Вами и Вашим лицензиаром.

2.6. За нарушение интеллектуальных прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством.

2.7. Вы не вправе использовать ПО для любых целей или способом, ограниченным или запрещенным применимым законодательством. Вы самостоятельно несете ответственность за неправомерное использование ПО.

2.8. 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 и отказ от предоставления гарантий

3.1. Правообладатель гарантирует работу ПО в соответствии с описанием, изложенным в Документации к ПО.

3.2. Вы соглашаетесь с тем, что никакое ПО не свободно от ошибок и Вам рекомендуется регулярно создавать резервные копии своих файлов.

3.3. Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Документации к ПО, а также в случае нарушения пользователем условий настоящего Соглашения и Договора, заключенного между Вами и Вашим лицензиаром.

3.4. За исключением устанавливаемой в настоящем пункте ограниченной гарантии, ПО поставляется «как есть». Правообладатель не дает никаких гарантий и не несет никакой ответственности перед Вами в случае любых изменений в программном обеспечении третьих лиц, произошедшее после установки/внедрения ПО и повлекшее потерю функциональности ПО (включая, но не ограничиваясь, изменением протокола передачи данных, формата хранения данных, логике работы стороннего программного обеспечения, обновлением программного обеспечения, которое перестает поддерживать работу с ПО). Правообладатель не дает никаких гарантий, условий, представлений или положений (выражаемых в явной или в подразумеваемой форме) на все, включая без ограничений нарушения прав третьих лиц, коммерческое качество, интеграцию или пригодность для определенных целей. Пользователь соглашается с тем, что он несет ответственность за выбор ПО для достижения нужных результатов, за установку и использование ПО, а также за результаты, полученные с его помощью.

4. Ограничение и пределы ответственности Правообладателя

Правообладатель не несет ответственности за какие-либо убытки, ущерб, независимо от причин его возникновения (включая, но не ограничиваясь этим, особый, случайный или косвенный ущерб, убытки связанные с недополученной прибылью, прерыванием коммерческой или производственной деятельности, утратой деловой информации, небрежностью, или какие-либо иные убытки), возникшие вследствие использования или невозможности использования ПО. Основанием ответственности Правообладателя будет вина, при этом убытки будут ограничиваться только доказанным в судебном порядке реальным ущербом.

5. Права на интеллектуальную собственность

5.1. 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.

5.2. Вы соглашаетесь с тем, что исходный код, лицензионный ключ для ПО являются собственностью Правообладателя.

5.3. Вы не можете удалять или изменять уведомления об авторских правах или другие проприетарные уведомления на любой копии ПО.

6. Права на информацию, доступ к которой получен Вами в рамках осуществления настоящего Соглашения

6.1. Вы соглашаетесь с тем, что Вам не принадлежат никакие права на любую информацию, не являющуюся объектом интеллектуальной собственности в соответствии с разделом 6, доступ к которой получен Вами в рамках осуществления настоящего Соглашения.

6.2. К указанной информации, включая, но не ограничиваясь, относятся системы, методы работы, другая информация.

6.3. 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.

7. 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

8. Контактная информация Правообладателя АО «ИнфоВотч»

Тел./факс: +7(495)229-00-22

Коммерческий департамент: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru

7.2 Лицензии третьих сторон

При создании Системы были использованы разработки третьих сторон, распространяемые на условиях лицензии MIT (http://www.opensource.org/licenses/mit-license.html):

- Lua – http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

Также использовалось программное обеспечение:

- распространяемое на условиях лицензий BSD (http://www.opensource.org/licenses/bsd-license.php):
    - Stringencoders – http://code.google.com/p/stringencoders/
- распространяемое на условиях GNU GENERAL PUBLIC LICENSE (http://www.gnu.org/licenses/gpl-2.0.html):
    - Pdftotext – http://www.foolabs.com/xpdf/
    - Tnef – http://sourceforge.net/projects/tnef/
    - Unzip – http://www.info-zip.org/UnZip.html
    - libcole.so – arturo@directmail.org; andy.scriven@research.natpower.co.uk
    - libhtmltree.so – pauljlucas@mac.com

8 Глоссарий

Термин	Определение
"В разрыв"	Схема развертывания IW TM, при которой возможно блокирование исходящих из периметра почтовых сообщений с последующей досылкой. При этом сервер IW TM используется в качестве relay-сервера.
Active Directory	LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT
AJAX	Asynchronous Javascript and XML (асинхронный JavaScript и XML) - подход к построению интерактивных пользовательских интерфейсов веб-приложений, заключающийся в «фоновом» обмене данными браузера с веб-сервером
CLI	Command Line Interface - интерфейс командной строки
DeviceLock	Средство защиты информации от утечек (DLP), осуществляющее контроль и протоколирование доступа пользователей к устройствам, портам ввода-вывода и сетевым протоколам
DeviceLock Adapter	Перехватчик IW DM, обеспечивающий интеграцию с системой DeviceLock, выполняющей перехват теневых копий файлов, переносимых на съемные устройства. См. также: IW DM, Теневая копия файла, Перехватчик
Domino directory	IBM Lotus Domino Directory - это директория с информацией о пользователях, серверах и группах. Domino Directory - это инструмент, используемый для администрирования системы Domino.
FTP	File Transfer Protocol (протокол передачи файлов) - сетевой протокол, предназначенный для передачи файлов по TCP-сетям
GTalk	Google Talk — программное обеспечения для мгновенного обмена сообщениями, разработанное компанией Google
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста) - протокол прикладного уровня передачи данных в виде текстовых сообщений. См. также: HTTPS, HTTP(S) Monitor
HTTPS	HyperText Transfer Protocol Secure (защищенный протокол передачи гипертекста) - расширение протокола HTTP, поддерживающее шифрование. См. также: HTTP, HTTP(S) Monitor
HTTP-запрос	Запрос, удовлетворяющий требованиям протокола HTTP (POST-запрос, GET-запрос и т. д.). См. также: HTTP, Событие
ICAP	Internet Content Adaptation Protocol - протокол, позволяющий контролировать входящий и исходящий HTTP-трафик. Предоставляет возможность модификации содержимого HTTP-запросов.
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
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)
Skype	Служба, обеспечивающая текстовую, голосовую и видеосвязь через Интернет

SMB	Server Message Block - сетевой протокол для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SMTP	Simple Mail Transfer Protocol (простой протокол передачи почты) - сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
S/MIME	Secure/Multipurpose Internet Mail Extensions - стандарт для шифрования и подписи в электронной почте с помощью открытого ключа.
SMTP-письмо	Письмо, удовлетворяющее требованиям протокола SMTP. См. также: SMTP, Событие
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
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
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
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 DM (импортированные из Domino Directory) и Группы TM (созданные средствами IW TM). См. также: Персона, Компьютер, Контакт
Заголовки	Вспомогательные данные, размещаемые в начале блока хранимых или передаваемых данных. Используются для формирования в Системе сущности события и определения значений атрибутов этого события. См. также: Событие, Атрибуты события
Задача	См. Задача сканирования
Задача сканирования	Операция (единоразовая или повторяющаяся по расписанию) проверки целевых мест хранения информации (хранилище Microsoft SharePoint 2007/2010/2013, локальные диски рабочих станций, разделяемые сетевые ресурсы) на предмет наличия в них файлов, содержащих элементы технологий. См. также: Краулер, Сканер, Элемент технологий

Защищаемые данные	Набор объектов защиты, их каталогов и файловых форматов, обнаружение которых в событии позволяет характеризовать это событие как подпадающее под ту политику защиты данных, в которой этот набор определен. См. также: Объект защиты, Файловый формат, Политика защиты данных
Инициатор, также: Инициатор события	Персона, чьи действия привели к созданию события в Системе
Интерфейс пользователя	Совокупность средств и методов, при помощи которых пользователь взаимодействует с системой.
Канал перехвата данных	Среда перехвата данных, состоящая из технических средств перехвата данных, средств программного обеспечения и протоколов передачи данных. В системе поддерживаются следующие каналы перехвата данных: электронная почта (SMTP, IMAP и POP3), веб (HTTP, HTTPS), сервисы мгновенных сообщений (Jabber, ICQ и Skype), теневые копии файлов, события подключения/отключения рабочих станций, задания на печать.
Категории и термины	Технология, выявляющая в тексте события наличие слов и выражений из базы терминов и относящая событие к категории, к которой принадлежат найденные термины. Ранее: Классификатор, БКФ. См. также: Событие, Термин, Категория, Технологии, Объект защиты
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

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
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
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 тд. Политика может быть назначена только группе (сотрудников или компьютеров). См. также: Правило (DM)
Политика контроля персон	Политика для оперативного добавления правил контроля персон, групп персон или персон с указанным статусом. См. также: Политика, Правило контроля персон, Персона, Статус персоны
Пользователь	Пользователь системы Traffic Monitor - администратор, офицер безопасности и др. См. также: Администратор, Офицер безопасности, Персона
Пользователь Консоли управления	Пользователь, в задачи которого входит выполнение различных функций по управлению Системой. Каждому пользователю назначается роль в соответствии с требованиями корпоративной политики безопасности.

Порог встречаемости	Количество текстовых объектов, найденных в событии, достаточное для обнаружения объекта защиты, в котором определен данный порог встречаемости. См. также: Событие, Текстовые объекты, Объект защиты
Порог цитируемости	Процент эталонного документа, найденный в событии в виде цитат, достаточный для отнесения события к этому эталонному документу. См. также: Событие, Эталонный документ, Цитата
Правило	Сущность, определяющая действия Системы в ответ на те или иные действия персон с защищаемыми объектами. Правило состоит из набора условий, по которым ведется проверка событий, и действий, осуществляемых при выполнении или невыполнении заданных условий. См. также: Событие, Политика, Защищаемый объект, Правило контроля персон, Правило копирования, Правило передачи, Правило хранения
Правило (DM)	Набор ограничений и условий, в соответствии с которыми осуществляется мониторинг операций по созданию файлов на съемных устройствах, сетевой активности, печати документов на принтере; определяется уровень доступа к контролируемым периферийным устройствам. С каждым перехватчиком сопоставлен отдельный тип правила. Правило действует в пределах той политики безопасности, в которую входит это правило. См. также: Политика (DM)
Правило контроля персон	Правило, назначающее атрибуты событию с указанным уровнем нарушения, и в котором среди отправителей или получателей есть персоны, указанные в политике, куда входит это правило. Позволяет переназначать статус 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, Краулер
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 политка 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
Сканер	Служба Краулера, выполняющая проверку файлов, находящихся в корпоративной сети, на предмет нарушения корпоративной политики безопасности. См. также: Краулер, Корпоративная политика безопасности
Событие	Объекты перехвата трафика (SMTP-, IMAP-, POP3-письма, HTTP-запросы, ICQ-сообщения, Skype-сообщения), теневые копии файлов и задания на печать. Создаются Системой в результате обмена данных между сотрудниками организации и другими людьми, включая публикацию в общедоступных источниках, копирование на внешние устройства и печать.
Состояние доставки	Атрибут события, определяющий возможность доставки события получателям после анализа. Если доставка события была разрешена, то значение атрибута отражает состояние доставки (выполнена/не выполнена). См. также: Атрибуты события
Списки	Списки однотипных данных, создаваемые средствами консоли управления, для использования при составлении политик. См. также: Конфигурация, Политика
Справочники персон, рабочих станций и групп	Данные о пользователях, рабочих станциях, а также группах персон и рабочих станций, импортированные из Active Directory, а также созданные средствами консоли управления. Используются для удобства работы с информацией о событиях
Статус	Характеристика персон и компьютеров, позволяющая разделять их по группам для удобства анализа и отслеживания активности, а также отображать в сводке и в отчетах с особой цветовой индикацией. См. также: Персоны, Компьютеры, Сводка, Отчет

Стоп-слово	Цифры, буквы и слова, нахождение которых в ячейках не приводит к срабатыванию этих ячеек. Стоп-слова используются для исключения ложноположительных срабатываний.
Тег	Текстовая метка, дающая краткую характеристику событию. См. также: Атрибуты события
Текст события	Текстовая информация, извлеченная из тела события и его вложений. Не содержит элементов форматирования или разметки. Используется для решения задач анализа и поиска. См. также: Событие, Тело события
Текстовые объекты	Технология, соотносящая данные из текста событий, с заданными шаблонами (например, с правилами формирования номеров банковских карт). См. также: Технологии, Событие, Элемент технологий, Шаблон текстового объекта
Теневая копия документа	Копия документа, отправленного на печать с контролируемого компьютера. См. также: InfoWatch Device Monitor
Теневая копия файла	Копия файла, записываемого на съемное устройство. Создается только при успешном завершении операции сохранения файла на съемное устройство. См. также: InfoWatch Device Monitor
Термин	Один из набора слов и словосочетаний, в совокупности определяющих предметную область. См. также: Категория
Технологии	Набор инструментов анализа, выполняющих поиск заданных элементов в контексте событий и добавляющие событию атрибуты, характеризующие это событие. См. также: Элемент технологий, Контекст события, Категории, Термины, Эталонные документы, Бланки, Выгрузки из БД, Текстовые объекты, Графические объекты
Транспортный режим	Атрибут события, определяющий степень контроля доставки событий получателям. В сочетании с атрибутом "Вердикт" определяет возможность дальнейшей транспортировки события. См. также: Событие, Атрибуты события, Вердикт, Режим копии, Нормальный транспортный режим, Состояние доставки
Уведомление	Сообщение, отправляемое в случае срабатывания политики на событии. Отправляется средствами Консоли управления для уведомления пользователей Консоли управления, сотрудников или третьих лиц. Содержит краткую информацию о перехваченных событиях и сопроводительное сообщение. См. также: Политика, Событие
Уровень нарушения	Атрибут события, с помощью цветовой метки указывающий на степень угрозы для корпоративной политики безопасности. См. также: Событие, Атрибуты события, Нарушение
Учет регистра	Параметр термина: при учете регистра в анализируемом тексте будет выполняться поиск только тех словоформ, в которых есть полное соответствие с заглавными и строчными буквами, заданными в термине. См. также: Термин
Цитата	Отрывок эталонного документа, найденный в тексте события. См. также: Эталонный документ

Цитируемость	Показатель того, насколько полно эталонный документ присутствует в тексте анализируемого документа. См. также: Эталонный документ, Цитата
Цифровой отпечаток	Способ хранения эталонного документа в базе данных в виде набора цитат. См. также: Эталонный документ, Цитата
Шаблон текстового объекта	Унифицированное описание всех возможных текстовых объектов с типичной структурой: номера паспортов, кредитных карт, телефонные номера, код медицинского диагноза и т.д. См. также: Текстовые объекты
Элемент технологий	Составляющая настройки технологий, входящих в состав Системы. Пример конфиденциальных данных. К элементам технологий относятся: категории и термины, эталонные документы, бланки, выгрузки, текстовые объекты и графические объекты. См. также: Технологии, Категории, Термины, Эталонные документы, Бланки, Выгрузки из БД, Текстовые объекты, Графические объекты, Объект защиты.
Эталонная контрольная сумма	В отличие от текущей контрольной суммы, фиксирует образцовое состояние файлов Системы. См. также: Контроль целостности
Эталонные документы	Технология поиска цитат из конфиденциальных документов: например, образцы текстов приказов, финансовых отчетов, договоров и др. Эталонные документы хранятся в системе в виде цифровых отпечатков, текст недоступен для просмотра ни пользователям, ни администраторам Системы. См. также: Технологии, Элемент технологий, Цифровой отпечаток, Цитата