

Диасофт Платформа

Traffic Monitor FD

Руководство пользователя

Traffic Monitor FD

Руководство пользователя

© 2016 Diasoft
Тел. +7 (495) 780-7575
http://www.diasoft-platform.ru
Дата редакции: 2016-07-22

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 10

1.1 Аудитория 10
1.2 Структура руководства 10
1.3 Техническая поддержка пользователей 11
1.4 Условные обозначения 11

2 ОБЗОР TRAFFIC MONITOR FD 12

2.1 Перехват исходящего трафика 13
2.2 Анализ объекта и вынесение решения по объекту 13
2.3 Ретроспективный анализ данных, решение пользователя по объекту 14
2.4 Загрузка объекта в базу данных 15

3 УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ 16

3.1 Схемы развертывания Системы и выбор типа установки 17
3.2 Аппаратные и программные требования 18
3.3 Установка Системы 18
3.4 Предустановленные серверные параметры 25
3.5 Настройка сервера 26
3.5.1 Настройка работы сервера TMFD в качестве Sniffer 27
3.5.2 Настройка сервера TMFD на прием копии трафика от Sniffer 28
3.5.3 Создание кластера TMFD 29
3.6 Настройка перехвата трафика 30
3.7 Автозапуск процессов 31
3.7.1 Проверка автозапуска процессов 31
3.7.2 Включение и выключение автозапуска процессов 32
3.8 Дополнительные настройки 33
3.8.1 Настройка OCR-экстракторов 33
3.8.2 Настройка отправки уведомлений пользователям и сотрудникам 34
3.8.3 Ограничение количества найденных событий 35
3.8.4 Настройка синхронизации времени 35
3.8.5 Конфигурирование работы Sphinx при распределенной установке 36
3.8.6 Настройка подсистемы мониторинга 36
3.8.6.1 Ручная настройка индикаторов 37
3.8.6.2 Настройка адреса сервера синхронизации времени для подсистемы мониторинга 37
3.8.6.3 Настройка порогов срабатывания для индикатора нагрузки 37
3.8.6.4 Настройка запуска служб 38
3.8.6.5 Настройка механизма уведомлений 38
3.8.6.5.1 Настройка отправки уведомлений о превышении порогового значения индикаторов 38
3.8.6.5.2 Настройка отправки писем-уведомлений с помощью Postfix 39
3.9 Лицензирование 40

4 АДМИНИСТРИРОВАНИЕ СИСТЕМЫ 41

4.1 Администрирование базы данных 41
4.1.1 Oracle 41
4.1.1.1 Проведение регламентных работ на сервере базы данных 41
4.1.1.2 Табличные пространства в базе данных TMFD 43
4.1.1.3 Управление ежедневными табличными пространствами 43
4.1.1.3.1 Настройка размещения файлов в файловой системе 43
4.1.1.3.2 Индексирование данных в ежедневных табличных пространствах 45
4.1.1.3.3 Архивирование ежедневных табличных пространств 47
4.1.1.3.3.1 Автоматическое архивирование ежедневных табличных пространств 47
4.1.1.3.3.2 Архивирование ежедневных табличных пространств вручную 48

4.1.1.3.4 Восстановление ежедневных табличных пространств 49
4.1.1.3.5 Удаление ежедневных табличных пространств 50
4.1.1.4 Резервное копирование базы данных 52
4.1.1.4.1 Создание резервной копии базы данных 52
4.1.1.4.1.1 Определение размера резервной копии 53
4.1.1.4.1.2 Проверка хранилища резервной копии 53
4.1.1.4.1.3 Создание папок для резервной копии 53
4.1.1.4.1.4 Создание вспомогательных файлов на Linux 54
4.1.1.4.1.5 Создание списка файлов, подлежащих резервному копированию 55
4.1.1.4.1.6 Остановка системы 56
4.1.1.4.1.7 Остановка БД Oracle 56
4.1.1.4.1.8 Копирование файлов БД в хранилище резервных копий 57
4.1.1.4.2 Восстановление базы данных из резервной копии 57
4.1.1.4.2.1 Восстановление на той же БД 57
4.1.1.4.2.2 Восстановление на новой БД 58
4.1.2 Postgre SQL 58
4.1.2.1 Табличные пространства в базе данных 59
4.1.2.2 Управление ежедневными табличными пространствами 59
4.1.2.2.1 Архивирование ежедневных табличных пространств 59
4.1.2.2.1.1 Автоматическое архивирование ежедневных табличных пространств 60
4.1.2.2.1.2 Архивирование ежедневных табличных пространств вручную 61
4.1.2.2.2 Восстановление ежедневных табличных пространств 62
4.1.2.2.3 Настройка размещения файлов в файловой системе 63
4.1.2.2.4 Удаление ежедневных табличных пространств 64
4.1.2.3 Резервное копирование базы данных 66
4.1.2.3.1 Создание резервной копии базы данных 66
4.1.2.3.1.1 Определение размера резервной копии 66
4.1.2.3.1.2 Проверка хранилища резервной копии 67
4.1.2.3.1.3 Создание каталов для резервной копии 67
4.1.2.3.1.4 Остановка системы 67
4.1.2.3.1.5 Остановка Postgre SQL 68
4.1.2.3.1.6 Копирование файлов БД в хранилище резервных копий 68
4.1.2.3.2 Восстановление базы данных из резервной копии 68
4.1.2.3.2.1 Восстановление на той же базе данных 68
4.1.2.3.2.2 Восстановление на новой базе данных 69
4.2 Администрирование серверной части TMFD 69
4.2.1 Процессы TMFD Server 70
4.2.1.1 Список процессов TMFD Server 70
4.2.1.2 Работа с процессами TMFD Server 73
4.2.2 Настройка конфигурационных файлов TMFD Server 75
4.2.2.1 Общие настраиваемые параметры конфигурационных файлов 75
4.2.2.1.1 Секция Logging 75
4.2.2.1.2 Секция Startup 76
4.2.2.1.3 Секция Nookdir 76
4.2.2.2 Специфичные настраиваемые параметры конфигурационных файлов 76
4.2.2.2.1 Конфигурационный файл serman_resolver.conf 77
4.2.2.2.2 Конфигурационный файл sniffer.conf 77
4.2.2.2.3 Конфигурационный файл proxy.conf 77
4.2.2.2.3.1 Секция Http 77
4.2.2.2.3.2 Секция Icq 80
4.2.2.2.3.3 Секция Smtp 80
4.2.2.2.4 Конфигурационный файл oracle.conf 80
4.2.2.2.5 Конфигурационный файл cas.conf 81
4.2.2.2.5.1 Секция Analysis 81
4.2.2.2.5.2 Секция Tableanalysis 81
4.2.2.2.5.3 Секция Thrift 81
4.2.2.2.6 Конфигурационный файл messed.conf 82
4.2.2.2.7 Конфигурационный файл capstack.conf 82
4.2.2.2.7.1 Секция UsedProcessors 82
4.2.2.2.7.2 Секция UsedSources 82
4.2.2.2.8 Конфигурационный файл indexer.conf 83

4.2.2.2.9 Конфигурационный файл web.conf 83
4.2.2.2.10 The analysis.conf configuration file 84
4.2.2.2.10.1 Секция Analysis 84
4.2.2.2.10.2 Секция Bookworm 84
4.2.2.2.11 Конфигурационный файл sample_compiler.conf 85
4.2.2.2.12 Конфигурационный файл serman.conf 85
4.2.2.2.12.1 Секция Serman 85
4.2.3 Настройка использования OCR 85
4.2.4 Настройка параметров обработки архивов вложений 86
4.2.4.1 Конфигурационный файл extractors.conf 86
4.2.4.2 Конфигурационный файл extractors.xml 86
4.2.5 Архивирование каталога очереди сообщений 88
4.2.6 Логирование работы Системы 88
4.2.7 Перемещение объектов между очередями (утилита iw_qtool) 89
4.2.8 Загрузка очередей объектов 90
4.2.9 Восстановление работоспособности системы в аварийных ситуациях 92
4.2.10 Настройка serman.conf при изменении адреса сервера БД 93
4.2.11 Настройка передачи информации в SIEM 93
4.2.11.1 Настройки на стороне SIEM 93
4.2.11.2 Настройки на стороне TMFD 94
4.2.11.2.1 Передача логов в SIEM 94
4.2.11.2.2 Управление логированием сессий пользователей БД TM 95
4.2.11.2.3 Управление пользователем siem 95
4.2.11.2.3.1 Создание пользователя siem 96
4.2.11.2.3.2 Смена пароля пользователя siem 96
4.2.11.2.3.3 Удаление пользователя siem 96
4.2.11.3 Типы логов, передаваемых в SIEM 97
4.2.12 Удаление временных файлов 97

5 ИСПОЛЬЗОВАНИЕ СИСТЕМЫ 99

5.1 Общие принципы работы с Консолью управления 99
5.1.1 Работа Системы до конфигурирования 100
5.1.2 Работа с конфигурацией Системы 100
5.1.3 Отображение актуальных данных в Консоли управления 102
5.2 Интерфейс Консоли управления 102
5.2.1 Раздел "Сводка" 105
5.2.1.1 Панели 107
5.2.1.2 Виджеты сводки 107
5.2.1.2.1 Динамика нарушений 108
5.2.1.2.2 Топ нарушителей 109
5.2.1.2.3 Количество нарушений за период 109
5.2.1.2.4 Подборка 110
5.2.1.2.5 Динамика статусов 111
5.2.1.2.6 Статистика по политикам 112
5.2.1.2.7 Статистика по объектам защиты 112
5.2.1.2.8 Статистика по каталогам объектов защиты 113
5.2.1.3 Выгрузка сводки 114
5.2.2 Раздел "События" 115
5.2.2.1 Запросы 117
5.2.2.1.1 Условие 118
5.2.2.1.2 Поля просмотра 121
5.2.2.1.3 Параметры доступа 122
5.2.2.1.4 Расширенный режим редактирования запроса 123
5.2.2.1.5 Поиск по тексту события 124
5.2.2.2 Объекты перехвата 126
5.2.2.2.1 Плитка события 127
5.2.2.2.2 Краткая форма просмотра событий 128
5.2.2.2.3 Детальная форма просмотра событий 130
5.2.2.3 Идентификация контактов в событии 131

5.2.3 Раздел "Отчеты" ... *132*
5.2.3.1 Виджеты отчетов ... 133
5.2.3.2 Запросы ... 136
5.2.3.3 История выполнения отчета ... 137
5.2.3.4 Окно создания отчета ... 137
5.2.3.5 Форма создания папки с отчетами ... 138
5.2.4 Раздел "Технологии" ... *139*
5.2.4.1 Выгрузки из БД ... 139
5.2.4.1.1 Автоматически обновляемые выгрузки из БД ... 142
5.2.5 Раздел "Объекты защиты" ... *143*
5.2.5.1 Каталоги объектов защиты ... 144
5.2.5.2 Объекты защиты ... 145
5.2.5.2.1 Элементы анализа ... 146
5.2.5.2.2 Условия обнаружения ... 146
5.2.5.2.3 Окно добавления элементов анализа ... 148
5.2.6 Раздел "Персоны" ... *148*
5.2.6.1 Группы персон и рабочих станций ... 150
5.2.6.2 Персоны ... 151
5.2.6.3 Рабочие станции ... 153
5.2.7 Раздел "Политики" ... *154*
5.2.7.1 Политики и форма их просмотра ... 155
5.2.7.2 Правила и форма их просмотра ... 156
5.2.7.2.1 Правило передачи ... 158
5.2.7.2.2 Правило контроля персон ... 159
5.2.7.3 Область "Настройка фильтра" ... 160
5.2.7.4 Окно добавления политики ... 161
5.2.8 Раздел "Списки" ... *161*
5.2.8.1 Теги ... 162
5.2.8.2 Список ресурсов ... 163
5.2.8.3 Статусы ... 163
5.2.8.4 Периметры ... 164
5.2.8.5 Список файлов ... 166
5.3 Типовые действия ... 167
5.3.1 Вход в Консоль управления и выход из нее ... *167*
5.3.2 Применение конфигурации Системы ... *168*
5.3.3 Редактирование элемента ... *169*
5.3.4 Удаление элемента ... *170*
5.3.5 Навигация по страницам ... *170*
5.3.6 Изменение пароля пользователя ... *171*
5.3.7 Выбор языка интерфейса ... *171*
5.3.8 Вызов справки ... *172*
5.3.9 Просмотр сведений о Системе ... *172*
5.4 Работа с персонами и рабочими станциями ... 172
5.4.1 Создание группы персон и рабочих станций ... *173*
5.4.2 Создание списка персон и рабочих станций ... *174*
5.4.3 Просмотр событий по персоне ... *175*
5.4.4 Просмотр сводки по персоне ... *175*
5.4.5 Добавление статуса персонам ... *176*
5.4.6 Добавление персоны в периметр ... *176*
5.4.7 Настройка карточки персоны ... *177*
5.4.7.1 Добавление персоне контакта ... 177
5.4.7.2 Добавление персоне рабочей станции ... 178
5.4.7.3 Добавление персоны в группу ... 179
5.4.8 Настройка карточки компьютера ... *180*
5.4.8.1 Добавление компьютеру контакта ... 180
5.4.8.2 Добавление компьютеру персоны ... 181
5.4.8.3 Добавление компьютера в группу ... 181
5.5 Работа со справочниками ... 182
5.5.1 Работа с тегами ... *183*

5.5.2 Работа со списками ресурсов ... 183
5.5.3 Работа со статусами ... 185
5.5.4 Работа с периметрами ... 185
5.6 Работа с базой технологий ... 188
5.6.1 Определение конфиденциальной информации ... 188
5.6.1.1 Работа с выгрузками ... 189
5.6.1.1.1 Условия детектирования выгрузки ... 190
5.6.2 Экспорт и импорт базы технологий ... 193
5.7 Работа с объектами защиты ... 194
5.7.1 Создание каталога объектов защиты ... 194
5.7.2 Создание объекта защиты ... 195
5.7.3 Добавление элементов анализа ... 196
5.7.4 Добавление условий обнаружения ... 197
5.7.5 Создание политики для объектов защиты и их каталогов ... 198
5.7.6 Импорт и экспорт объектов защиты ... 199
5.7.7 Активация и деактивация объектов защиты ... 200
5.8 Работа с объектами перехвата ... 201
5.8.1 Просмотр сводки по нарушениям/нарушителям ... 201
5.8.1.1 Создание панели ... 201
5.8.1.2 Создание виджета ... 202
5.8.1.3 Настройка виджета ... 203
5.8.2 Просмотр событий ... 203
5.8.2.1 Создание запросов ... 204
5.8.2.1.1 Создание запроса в стандартном режиме ... 205
5.8.2.1.2 Создание запроса в расширенном режиме ... 205
5.8.2.1.3 Использование расширенного синтаксиса ... 207
5.8.2.2 Выбор полей просмотра событий ... 208
5.8.2.3 Просмотр краткой формы события ... 209
5.8.2.4 Просмотр детальной формы события ... 209
5.8.3 Работа с выгрузками сводки ... 210
5.8.3.1 Создание выгрузки сводки ... 210
5.8.3.2 Просмотр выгрузки сводки ... 212
5.8.4 Вынесение решения по объекту ... 212
5.8.5 Добавление и удаление тега ... 213
5.8.6 Сохранение события (для SMTP-писем) ... 213
5.8.7 Выгрузка события ... 214
5.9 Настройка реакций Системы ... 215
5.9.1 Общие сведения о политиках ... 216
5.9.1.1 Разбиение события на суб-события ... 217
5.9.1.2 Разбиение правил на суб-правила ... 217
5.9.1.3 Определение приоритетного суб-правила ... 218
5.9.1.4 Порядок применения действий согласно отобранным приоритетным правилам ... 219
5.9.1.5 Пример: ... 219
5.9.2 Предустановленные политики ... 221
5.9.2.1 Политики защиты конфиденциальных данных ... 221
5.9.2.2 Политика контроля персон ... 222
5.9.2.2.1 Правила политики ... 222
5.9.2.3 Политика, регулирующая передачу данных, защищенных паролем ... 223
5.9.2.3.1 Правила политики ... 223
5.9.2.4 Политики, контроллирующие посещение веб-ресурсов ... 223
5.9.2.4.1 Нецелевое использование ресурсов ... 223
5.9.2.4.1.1 Правила политики ... 224
5.9.2.4.2 Нелояльные сотрудники ... 224
5.9.2.4.2.1 Правила политики ... 224
5.9.2.4.3 Скрытие действий сотрудников ... 224
5.9.2.4.3.1 Правила политики ... 225
5.9.2.4.4 Подозрительная активность ... 225
5.9.2.4.4.1 Правила политики ... 225
5.9.3 Создание политики защиты данных ... 226

5.9.4 Создание политики контроля персон ... 227
5.9.5 Редактирование политики ... 228
5.9.6 Создание правил ... 228
5.9.7 Редактирование правил ... 230
5.9.8 Определение действий Системы в случае нарушения правил ... 230
5.9.9 Определение действий Системы по умолчанию ... 231
5.9.10 Фильтрация списка политик ... 233
5.9.11 Отправка уведомлений о сработавшем правиле ... 233
5.10 РАБОТА С ОТЧЕТАМИ ... 234
5.10.1 Создание папки с отчетами ... 234
5.10.2 Создание отчета ... 235
5.10.3 Работа с виджетами отчетов ... 236
5.10.3.1 Создание и настройка виджета ... 237
5.10.4 Работа с готовыми отчетами ... 238
5.11 РАБОТА В РАЗДЕЛЕ АДМИНИСТРИРОВАНИЕ ... 239
5.11.1 Управление интеграцией с LDAP каталогами ... 239
5.11.1.1 Создание подключения к серверу ... 241
5.11.1.2 Редактирование подключения к серверу ... 241
5.11.1.3 Удаление подключения к серверу ... 241
5.11.1.4 Запуск синхронизации с сервером вручную ... 242
5.11.2 Управление пользователями Системы и их ролями ... 242
5.11.2.1 Пользователи ... 242
5.11.2.1.1 Создание учетной записи пользователя ... 243
5.11.2.1.2 Редактирование учетной записи пользователя ... 244
5.11.2.1.3 Удаление учетной записи пользователя ... 244
5.11.2.1.4 Изменение пароля учетной записи пользователя ... 244
5.11.2.1.5 Изменение статуса учетной записи пользователя ... 245
5.11.2.1.6 Импорт учетной записи пользователя ... 245
5.11.2.1.7 Задание пользователю роли ... 246
5.11.2.1.8 Задание пользователю области видимости ... 246
5.11.2.2 Роли ... 246
5.11.2.2.1 Создание роли ... 247
5.11.2.2.2 Редактирование роли ... 248
5.11.2.2.3 Удаление роли ... 248
5.11.2.3 Области видимости ... 248
5.11.2.3.1 Создание области видимости ... 249
5.11.2.3.2 Редактирование области видимости ... 251
5.11.2.3.3 Удаление области видимости ... 251
5.11.3 Управление лицензиями ... 252
5.11.3.1 Проверка валидности лицензии ... 253
5.11.3.2 Установка лицензии ... 253
5.11.3.3 Удаление лицензии ... 253
5.11.3.4 Запрос лицензии ... 254
5.11.4 Состояние системы ... 254
5.11.4.1 Настройка параметров отправки уведомлений ... 255
5.11.5 Управление службами ... 256
5.11.5.1 Запуск службы ... 256
5.11.5.2 Остановка службы ... 256
5.11.5.3 Перезапуск службы ... 257
5.11.5.4 Сохранение логов службы ... 257
5.11.6 Сбор диагностических данных ... 257
5.11.6.1 Сбор диагностических данных в обычном режиме ... 258
5.11.6.2 Сбор диагностических данных в расширенном режиме ... 259
5.11.7 Аудит действий пользователя ... 259
5.11.7.1 События аудита ... 260
5.11.7.1.1 Расширенная информация ... 260
5.11.7.2 Фильтрация по пользователю ... 261
5.11.7.3 Фильтрация по действию ... 261
5.11.7.4 Фильтрация по объекту ... 261

5.11.7.5 Фильтрация по дате 262
5.11.8 Контроль целостности 262
5.11.8.1 Ручная проверка целостности 262
5.11.8.2 Автоматическая проверка целостности 262
5.11.8.3 Принятие результата за эталонный 263
5.11.9 Плагины 263
5.11.9.1 Добавление плагина 265
5.11.9.2 Удаление плагина 265
5.11.9.3 Работа с токенами 265
5.11.9.3.1 Добавление токена 265
5.11.9.3.2 Удаление токена 266
6 ОБНОВЛЕНИЕ СИСТЕМЫ 267
6.1 Обновление пакетов RHEL и IWTM 267
6.2 Обновление схемы БД Oracle 269
6.3 Обновление схемы БД PostgreSQL 269
7 УДАЛЕНИЕ СИСТЕМЫ 271
7.1 Удаление схемы базы данных 271
8 ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ИМЕН И ПАРОЛЕЙ 273
9 ПРИЛОЖЕНИЕ В. ИНДИКАТОРЫ МОНИТОРИНГА 275
10 ПРИЛОЖЕНИЕ С. ЛИЦЕНЗИОННАЯ ИНФОРМАЦИЯ 279
10.1 Лицензии третьих сторон 279

1 ВВЕДЕНИЕ

Traffic Monitor FD (далее TMFD или Система) – это распределенная многокомпонентная система, предназначенная для контроля различных видов трафика (SMTP, HTTP, ICQ, NRPC). Кроме того, TMFD выполняет анализ данных, полученных от систем на платформе Диасофт.

В настоящем руководстве вы можете найти сведения по установке, настройке, использованию, обновлению и удалению Системы.

1.1 Аудитория

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

Руководство предназначено для специалистов, знакомых с основами работы в средах операционных систем Microsoft Windows и Linux, а также обладающих навыками администрирования СУБД Oracle и Postgre SQL.

1.2 Структура руководства

В настоящем руководстве вы можете найти следующую информацию:

- *Обзор TMFD*
  Общие сведения об TMFD (назначение, основные функции).
- *Установка Системы.*

  Содержит рекомендации по установке компонентов Системы и пошаговое описание установки.
- *Администрирование Системы*
  Описание шагов, выполняемых администратором для настройки Системы.
- *Использование Системы*
  Описание настроек Системы, выполняемых в Консоли управления.
- *Обновление Системы.*

  Содержит описание процедуры обновления Системы с использованием пакетов обновления, поставляемых на диске с дистрибутивом.
- *Удаление системы.*

  Приводятся сведения по удалению компонентов Системы.
- *Приложение А. Рекомендации по составлению имен и паролей.*

  Приводится набор правил для составления имен и паролей пользователей, даются рекомендации по составлению надежных паролей.

- *Приложение B. Индикаторы мониторинга.*

  Содержит значения индикаторов, используемых подсистемой мониторинга для проверки состояния компонентов Системы.

- *Приложение C. Лицензии на стороннее программное обеспечение.*

  Содержит информацию о лицензиях на стороннее программные компоненты, использованные в продукте.

1.3 Техническая поддержка пользователей

При возникновении общих вопросов вы можете обратиться в компанию «Диасофт» по адресу info@diasoft-platform.ru.

При возникновении проблем и вопросов, связанных с работой продукта, вы можете обратиться в службу технической поддержки по адресу support@diasoft-platform.ru.

1.4 Условные обозначения

Для наглядности в тексте документации используются различные стили оформления. Области применения стилей указаны в следующей таблице.

Стиль оформления	Область применения	Пример
Полужирный шрифт	Названия элементов графического пользовательского интерфейса (кнопки, команды меню и пр.), компоненты системы (при первом упоминании)	Для перемещения объектов из одной очереди в другую используется утилита **iw_qtool**
Курсив	При описании таблиц, в примерах, описаниях – названия и значения атрибутов объектов	База контентной фильтрации содержит термин *Договор*
`Шрифт Courier New`	Имена файлов, примеры текста программ; значения параметров конфигурационных файлов, примеры настройки	Проверка запуска TMFD Server осуществляется командой: `service iwtm status`

2 ОБЗОР TRAFFIC MONITOR FD

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

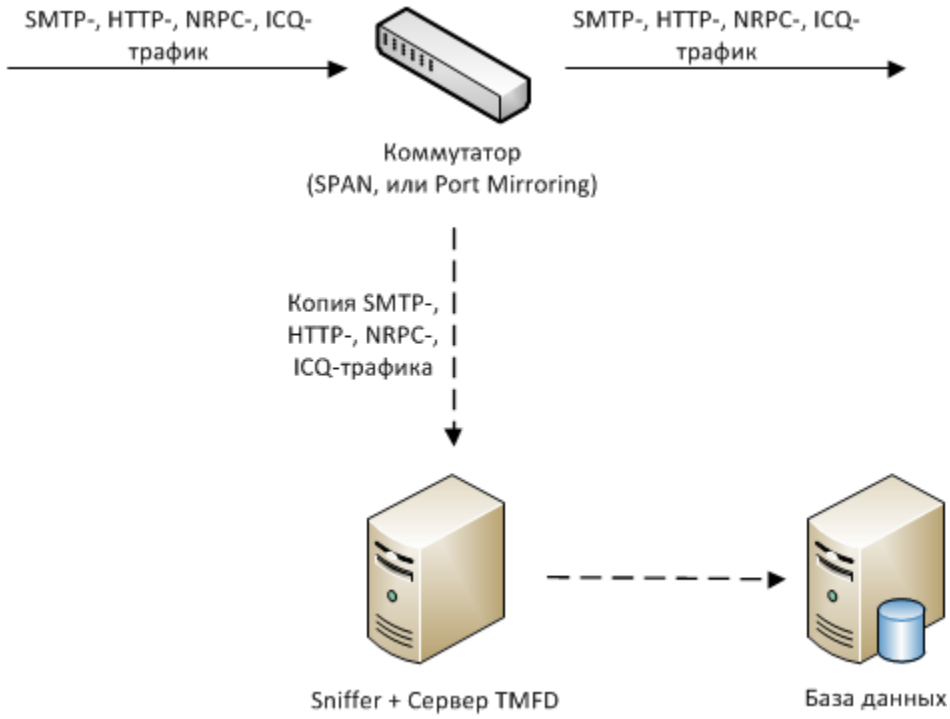
Система перехватывает исходящий трафик, передаваемый по протоколам SMTP, HTTP, OSCAR (ICQ), NRPC (IBM Notes). Далее происходит анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности. Примеры конфиденциальных данных TMFD получает из систем на платформе Diasoft с помощью коннектора TMFD Connector.

С помощью специально разработанного коннектора «Модуль Диасофт TM Connector» можно отправлять эталонные выгрузки из систем на базе Diasoft в TrafficMonitor FD. Сама эталонная выгрузка представляет собой записи таблицы базы данных, представленные в виде CSV- или TSV-файлов. Эталонные выгрузки, полученные таким образом из программных продуктов Diasoft с помощью модуля Диасофт TM Connector, обрабатываются на стороне TrafficMonitor FD и сохраняются в базе данных TrafficMonitor FD в скомпилированном (бинарном) виде, обеспечивая таким образом гибкую настройку политики безопасности и поддержание этой политики в актуальном состоянии в автоматическом режиме.

Информация о работе Системы на каждом этапе представлена в разделах:

- *Перехват исходящего трафика*
- *Анализ объекта и вынесение решения по объекту*
- *Ретроспективный анализ данных, решение пользователя по объекту*
- *Загрузка объекта в базу данных*

2.1 Перехват исходящего трафика



Трафик снимается с управляемого коммутатора по технологии SPAN Port, или Port Mirroring. Большое количество управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов или VLAN на отдельно взятый порт.
Настроенный порт коммутатора подключается к сетевому интерфейсу сервера TMFD. Интерфейс сервера переводится в «неразборчивый» (promiscuous) режим, что позволяет ему принимать все входящие пакеты. IP-адрес при подключении к сетевому интерфейсу не требуется.
Наиболее эффективным является зеркалирование внутреннего порта шлюза или внутреннего интерфейса прокси-сервера.

Данный способ позволяет безопасно анализировать трафик даже в изолированном сегменте сети. Система никак не может повлиять на анализируемый трафик, независимо от состояния сервера.

2.2 Анализ объекта и вынесение решения по объекту

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

Подсистема TMFD	**Модули подсистемы**	**Функции подсистемы/модуля**
Подсистема Обработки	Модуль Обработки SMTP-, HTTP-, ICQ-, NRPC-трафика	Извлечение из перехваченных объектов значимой информации и вложений, определение форматов вложений и передача извлеченных текстов в Подсистему Анализа.

Подсистема Анализа	Модуль детектирования выгрузок из БД	Поиск цитат из базы данных в тексте событий.
Подсистема Применения Политик	Модуль Интеграции с Active Directory и Domino Directory	Обеспечение первоначального импорта и периодической синхронизации структуры каталога Active Directory и Domino Directory со справочником персон и рабочих станций 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.
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.
   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.
   - **Назначить событию теги**. Теги, которые будут назначены событию в случае нарушения политики.
   - **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.

2.4 Загрузка объекта в базу данных

После того как объект проанализирован и по нему принято решение Системы, 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.

3 УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ

Примечание:

После установки Системы будет автоматически загружена пробная лицензия на технологии TMFD.

В данном разделе приведены инструкции для каждого из типов установки Системы.

О выборе типа установки см. "Схемы развертывания Системы и выбор типа установки".

Установка серверных компонентов системы TMFD выполняется с помощью программы-инсталлятора (**kickstart**).

В зависимости от целевого назначения сервера, будет различаться набор устанавливаемых компонентов:

Назначение сервера	**Ключ kickstart**	**Компоненты, устанавливаемые инсталлятором**
Все компоненты TMFD устанавливаются на один компьютер	**TMFDE All-in-one**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка и настройка СУБД Oracle или PostgreSQL • Установка схемы базы данных TMFD • Установка RPM пакетов сервера TMFD • Установка подсистемы мониторинга • Установка консоли управления
Установка сервера СУБД со схемой БД TMFD на отдельный компьютер	**TMFDE DB server**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка и настройка СУБД Oracle Enterprise или PostgreSQL • Установка схемы базы данных TMFD

Установка сервера TMFD на отдельный компьютер	**TMFDE Node server**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка RPM пакетов сервера TMFD • Установка подсистемы мониторинга • Установка консоли управления

Сведения о предустановленных учетных записях приведены в статье "Предустановленные серверные параметры".

После окончания установки серверных компонентов работа в консоли управления доступна через окно браузера, при этом требуется ввести URL-адрес:

- сервера TMFD – если выполнена совместная установка;
- основного сервера TMFD – если компоненты Системы установлены на разные компьютеры.

3.1 Схемы развертывания Системы и выбор типа установки

Система TMFD может устанавливаться совместно или распределенно.

В максимально развернутой конфигурации может выглядеть следующим образом:

- **Сервер TMFD**. Обеспечивает работу перехватчика, подсистемы анализа и подсистемы применения политик. В ряде случаев рекомендуется использовать несколько серверов TMFD: это позволяет обеспечивать более эффективную работу нагруженных процессов. При этом необходимо учитывать, что некоторые процессы должны быть запущены только на одном сервере (подробнее см. статью "Проверка автозапуска процессов" в Руководстве администратора).
- **База данных**. Сервер СУБД Oracle или PostgreSQL. На этом компьютере не рекомендуется устанавливать и запускать приложения (особенно серверные) или использовать его в качестве файл-сервера.
- **Консоль управления**. Веб-интерфейс управления Системой. Реализован в виде набора процессов, которые должны быть запущены только на одном сервере TMFD (подробнее см. статью "Проверка автозапуска процессов").

Существуют следующие типы установки:

4. Совместная – все компоненты Системы (с СУБД Oracle или PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов TMFD.
5. Сервер TMFD + База данных – сервер TMFD и СУБД Oracle или PostgreSQL устанавливаются на разные машины. Такая установка используется, если с учетом предполагаемой нагрузки сервисы TMFD и СУБД не смогут производительно работать на одной машине.

3.2 Аппаратные и программные требования

Требования к аппаратной конфигурации сервера для TMFD определяются на основании варианта установки, предполагаемой нагрузки на Систему и параметров сети, в которой происходит развертывание Системы. Поэтому спецификация оборудования для каждого случая рассчитывается отдельно.

Для сервера TMFD аппаратно-программные требования варьируются в очень большом диапазоне.

Также на количество и назначение серверов TMFD может влиять существенная разница в нагрузке на те или иные каналы перехвата.

Элемент TMFD		**Дисковая подсистема**	**Процессор**	**Оперативная память**	**Программные требования**	**Дополнительные требования**
Сервер TMFD	Менее 10 GB/день	SATA, 600 GB	2CPU 8xC + Hyper-threading (Intel® Xeon® Processor E5-2640 v3 - частота 2,6 Hz)	32 GB	Не предъявляются: программа-инсталлятор (kickstart) форматирует жесткий диск и устанавливает все необходимое программное обеспечение.	Для работы требуется правляемый коммутатор с поддержкой функции SPAN / Port Mirroring (рекомендованная модель - Cisco Catalyst 2960 Series) с портом, настроенным на режим TRx (BOTH - получение и передача в одном подключении). Сервер должен иметь сетевой интерфейс с назначенным IP-адресом.
	От 10 GB/день до 50 GB/день	SATA/SAS, RAID5, 6+ HDD	2SRVx2CPU 10xC	64 GB		
	Более 50 GB/день	SAS, полка	Рассчитывается по запросу	По 64 GB на каждый из серверов		
Сервер базы данных	Oracle	3,6 TB	2CPU 6xC, 2,6 Ghz	32 GB		Обеспечивает хранение трафика для 1-2 тыс. пользователей, сроком до 3 месяцев; без OCR
	PostgreSQL			24 GB		

Допустима установка Системы в виртуальную среду: например, VMware, MS Hyper-V или других систем виртуализации.

3.3 Установка Системы

Чтобы выполнить установку TMFD, выполните следующие действия:

1. Подключите диск с дистрибутивом: программа-инсталлятор (**kickstart**) запустится автоматически.



2. В окне приветствия выберите **TMFD Enterprise**, нажмите **Enter**.
3. В окне выбора базы данных укажите, какая СУБД должна быть установлена:
   - Oracle;
   - PostgreSQL.

   Нажмите **Enter**.
4. В окне выбора режима установки выберите один из следующих вариантов:
   - **TMFDE All-in-one: TM+DB server** – все компоненты Системы (с СУБД Oracle или PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов TMFD.
   - **TMFDE DB server** – установка базы данных вместе с выбранной СУБД на отдельный компьютер.

     Такая установка используется, если с учетом предполагаемой нагрузки сервисы TMFD и СУБД не смогут производительно работать на одном компьютере.

     Установка серверов должна производиться в следующем порядке:
     - Установка Базы данных (TMFDE DB server);
     - Установка Сервера TMFD (TMFDE Node server).

Важно!

Установка в другом порядке (сервер TMFD устанавливается раньше, чем База данных) не поддерживается.

Вы можете установить несколько серверов TMFD. При этом необходимо логически разделить их на основной и второстепенный (второстепенные). Основным сервером называется сервер, на котором будут запущены процессы, необходимые Системе в единственном экземпляре.

- **TMFDE Node server** – установка сервера TMFD на отдельный компьютер.

Нажмите **Enter**.



Важно!

После выбора режима установки на экран может быть выведено предупреждение «*The storage device below may contain data*». Чтобы очистить диск и начать установку, нажмите **Yes, discard any data**, оставив без изменений поле **Apply my choice to all devices with undetected partitions of file systems**.

5. Укажите настройки часового пояса для сервера (если системное время установлено по Гринвичу (UTC), установите флажок в поле **System clock uses UTC**), нажмите **Next**.

   Вы можете выбрать нужный город:

   - в раскрывающемся списке. Города отсортированы по принадлежности к той или иной части света: например, Москва входит в группу Европа;
   - на карте. Для навигации по карте используйте полосы прокрутки и инструменты изменения масштаба).

   Отметьте флажок в поле **System clock uses UTC**, если системное время установлено по Гринвичу (UTC).

   Нажмите **Next**.

6. Задайте пароль суперпользователя *root*, подтвердите его и нажмите **Next**. Рекомендации по составлению паролей приведены в разделе "Приложение А. Рекомендации по составлению имен и паролей".

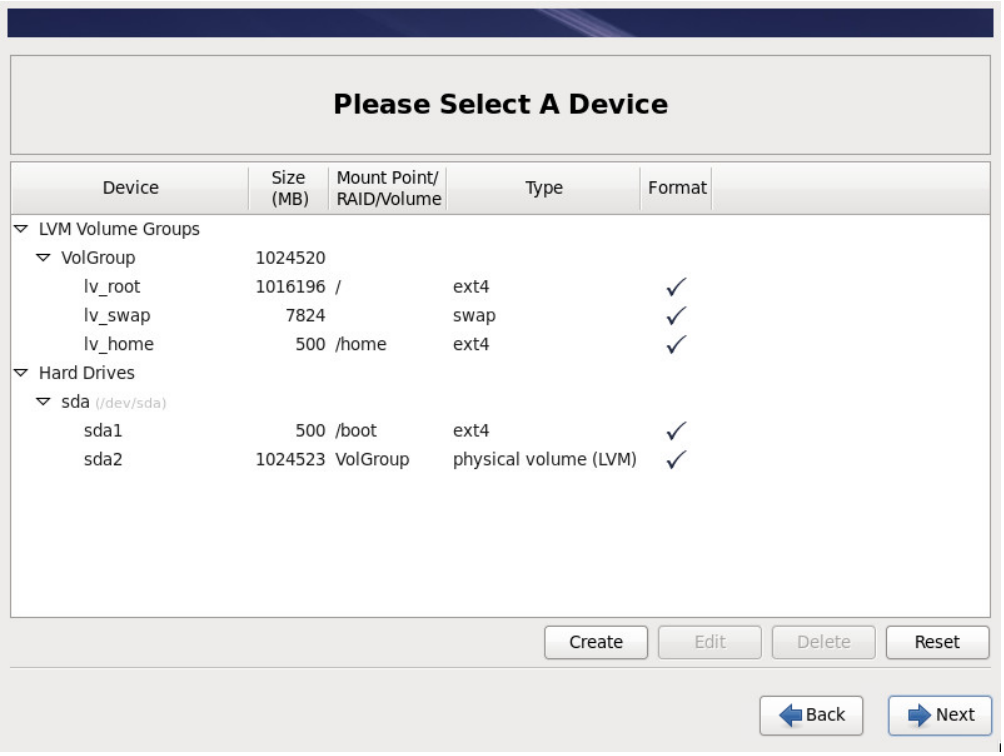
   Пользователь *root* – это суперпользователь в Системе.

   Если введенный пароль не соответствует правилам безопасности, на экране отобразится предупреждающее окно **Weak Password**. Используйте кнопки:

   - **Use anyway** – если вы хотите использовать введенный пароль без учета рекомендаций;

- **Cancel** – если вы хотите изменить введенный пароль.

7. Определите способ разбиения дискового пространства:
   - Выберите **Use All Space**.
   - Отметьте опцию **Review and modify partitioning layout**, расположенную внизу окна.
   - Нажмите **Next**.
   - В окне **Please Select A Device** выберите раздел **lv_home** и нажмите **Edit**.
   - В поле **Size (MB)** укажите **5000**. Нажмите **OK**.
   - В окне **Please Select A Device** выберите раздел **lv_root** и нажмите **Edit**.
   - В поле **Size (MB)** укажите все оставшееся свободное пространство (отображается под полем - **Max size is...**) . Нажмите **OK**.



   - Нажмите **Next**.

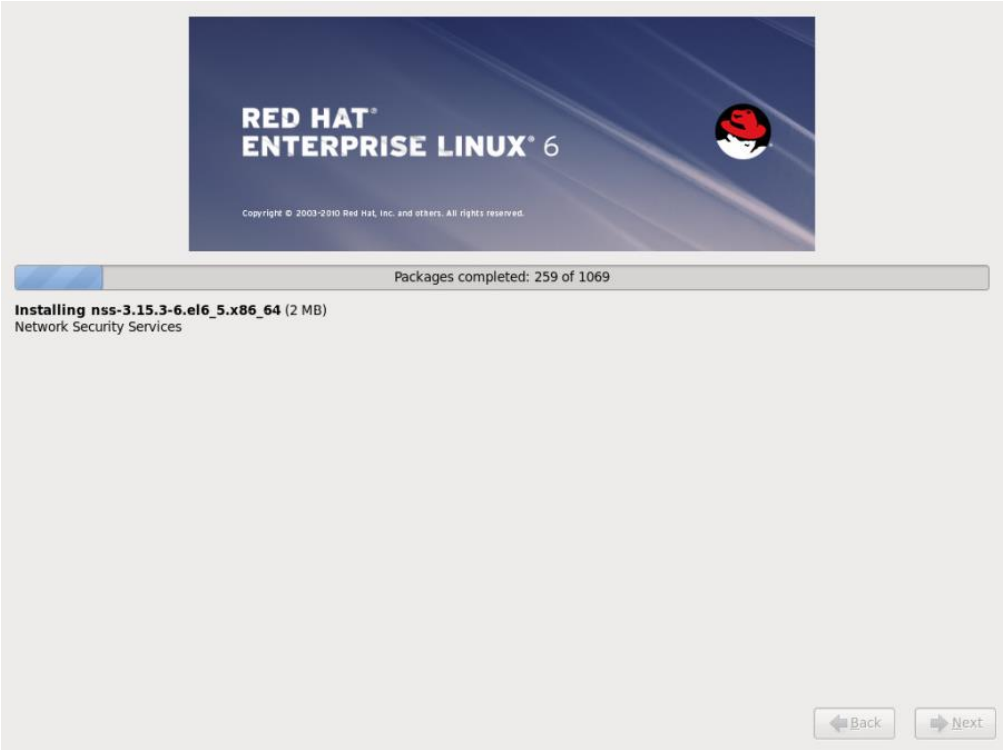
> **Примечание:**
>
> На экран может быть выведено окно **Format Warnings**, свидетельствующее о том, что требуется отформатировать разделы жесткого диска, которые будут использоваться для установки. Для продолжения установки нажмите **Format**.

Важно

По завершении установки Системы компоненты будут установлены в следующие директории:

- TMFD – в каталог `/opt/iw`;

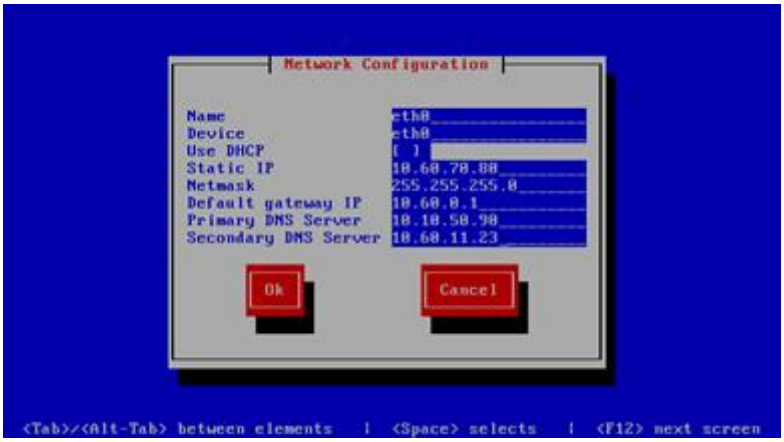
- БД – в каталоги `/u01` и `/u02`.
  Если сервер TMFD и БД устанавливаются по отдельности, то эти директории будут располагаться на разных серверах.



Начнется процесс разбиения диска, а затем – установки операционной системы. Прогресс выполнения обоих процессов будет отображаться на экране.
Это может занять некоторое время.

По окончании установки операционной системы выполнится перезагрузка, и будет предложено настроить сетевые параметры.

8. Для настройки параметров сетевой карты:
   - Выберите **Device configuration**, нажмите **Enter**.
   - Выберите сетевой интерфейс **eth0**, нажмите **Enter**.



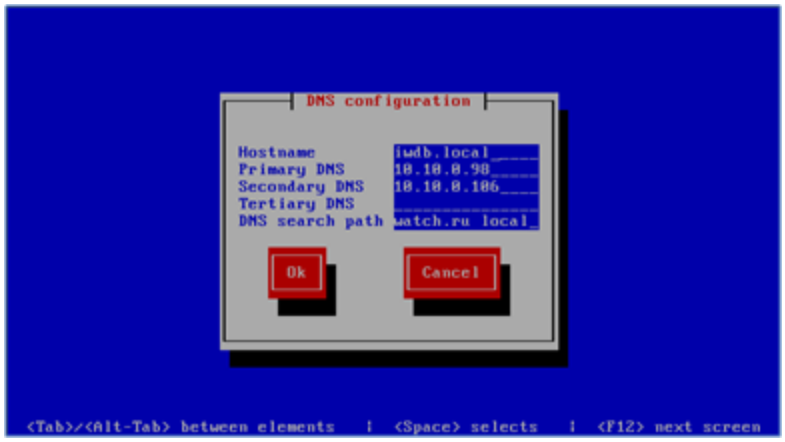
   - Если вы хотите, чтобы Система использовала сетевые настройки от DHCP сервера, переведите курсор в поле **Use DHCP** и нажмите пробел. В противном случае вручную

введите сетевые настройки сервера (статический IP-адрес машины и прочее). По завершении конфигурирования нажмите **OK**.

> **Важно!**
>
> При использовании настройки **Use DHCP** Система будет использовать только данные, полученные от указанных серверов DHCP. Данные, введенные в диалоге **DNS configuration** (см. далее) будут игнорироваться. Если вручную изменить файл `/etc/resolv.conf`, то его данные при следующей перезагрузке сервера будут заменены на полученные от сервера DHCP.

- Нажмите **Save**, чтобы сохранить сделанные настройки.

9. Для настройки DNS конфигурации выберите **DNS configuration** и укажите необходимые параметры сетевых настроек сервера. Затем нажмите **OK**.



> **Важно!**
>
> Если в окне **Network Configuration** был отмечен пункт **Use DHCP**, то вместо этих параметров будут использоваться полученные от указанных серверов DHCP.

10. Нажмите **Save&Quit**.
11. Проверьте указанные сетевые настройки. Если настройки некорректны, нажмите **N** на клавиатуре и укажите правильные параметры (см. предыдущие шаги). Если настройки корректны, нажмите **Y** на клавиатуре для подтверждения и нажмите **Enter**.
12. Настройте адрес сервера для синхронизации времени (NTP-server). Для этого установите знак астериска (*) в поле **DNS** и нажмите пробел, затем - **OK**.

    Вы можете выбрать одну из следующих опций настройки сервера для синхронизации времени (NTP-server):

    - **Default_GW** - шлюз, используемый компьютером по умолчанию;
    - **DNS** - контроллер домена: обычно используется в организациях в качестве сервера времени;
    - **Manual** - возможность вручную указать имя сервера или его IP-адрес.

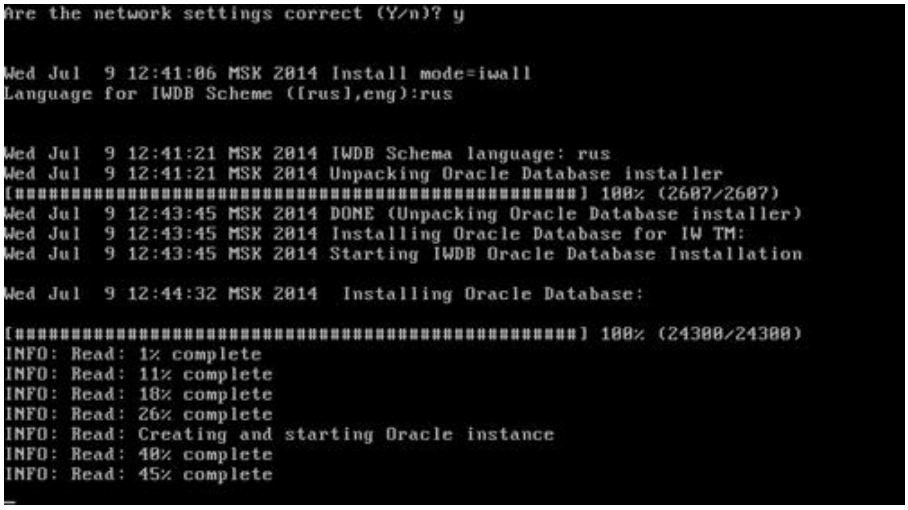
Примечание:

Если по каким-либо причинам указать NTP-сервер не удается, нажмите **Cancel** и выполните данную настройку позднее (подробнее о настройке NTP-сервера см. в документе «*TMFD. Руководство администратора*»).

13. Укажите язык интерфейса (для всех типов установки, кроме **TMFDE Node server**):
    - Выберите **Interface**, нажмите **Enter**.
    - Выберите требуемый язык, нажмите **OK**.
      На выбранном языке будет установлена консоль управления.
    - Нажмите **Accept**.
    - В открывшемся окне проверьте, что выбранные языки для предустановленных сущностей и для интерфейса указаны правильно, затем нажмите **Yes**.
14. Настройте параметры автоматического удаления событий из БД (для всех типов установки, кроме **TMFDE Node server**).
    Выберите одну из трех опций, затем нажмите **Select** :
    - **Events cleaning** – настраивает включение и выключение автоматического удаления событий двух типов (по умолчанию: отключено).
      Чтобы выбрать пункт, установите курсор в нужное поле и нажмите пробел до появления в поле значка астериска (*):
      - **Violation** – включить автоматическое удаление событий, которые являются нарушением
      - **Non-violation** – включить автоматическое удаление событий, которые не являются нарушением .
        Вы можете выбрать оба пункта, чтобы удалялись объекты как с нарушениями, так и без.

      Нажмите **Ok**.
    - **Violation** – настраивает периодичность автоматического удаления событий, которые являются нарушением (по умолчанию: 90 дней).
      Установите периодичность удаления в днях. Нажмите **Ok**.
    - **Non-violation** – настраивает периодичность автоматического удаления событий, которые не являются нарушением (по умолчанию: 45 дней).
      Установите периодичность удаления в днях. Нажмите **Ok**.
15. По завершению настроек нажмите **Save settings**.

Начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране.



Процесс может занять некоторое время.

В результате установки в системе будут созданы учетные записи, приведенные в статье "Предустановленные серверные параметры".

Имя сервера (hostname) будет иметь следующий формат:
`iwtm-xxxxxxxxxxxxxxxx.local`
где xxxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

Установка Веб-консоли управления происходит в автоматическом режиме с помощью программы-инсталлятора (**kickstart**). После окончания установки серверных компонентов работа в консоли управления доступна через окно браузера, при этом требуется ввести URL-адрес сервера TMFD.

3.4 Предустановленные серверные параметры

В результате установки серверной части Системы создается ряд сущностей, к которым впоследствии может потребоваться обращаться при дальнейшей настройке и эксплуатации Системы.

Имя сервера (hostname): **iwtm-xxxxxxxxxxxxxxxx.local**, где xxxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

Директории установки Системы (могут располагаться на разных серверах):

- сервер TMFD – **/opt/iw**
- БД – **/u01** и **/u02**

Параметры базы данных TMFD:

Параметр	**Oracle**	**PostgreSQL**
Порт подключения к БД	**1521**	**5433**
Имя базы данных / SID или service name	**iwtm**	**postgres**

Учетные записи:

Учетная запись	Имя	Пароль
Суперпользователь OS Linux (root)	**root**	Задается при установке
Пользователь Linux, от имени которого будут запускаться серверные процессы TMFD	**iwtm**	Без пароля
Oracle администратор	**sys**	xxXX1234
	system	xxXX1234
Владелец схемы базы данных	**iwtm**	xxXX1234
Пользователь Linux части СУБД, от имени которого перехваченные объекты будут загружаться в базу данных (и Oracle, и PostgreSQL)	**iwtm_linux**	xxXX1234
Пользователь, от имени которого веб-интерфейс будет взаимодействовать с БД	**iwtm_web**	xxXX1234
Веб-консоль управления: администратор пользователей	**administrator**	xxXX1234
Веб-консоль управления: офицер безопасности	**officer**	xxXX1234
Пользователь Linux, от имени которого будут запускаться серверные процессы БД **Важно!** Настоятельно рекомендуется сразу же по окончании установки сменить пароль этой учетной записи .	**oracle**	xxXX1234

Группа владельца инсталляции клиента СУБД Oracle, в состав которой включены пользователи iwtm, oracle – **oinstall**.

3.5 Настройка сервера

Возможно несколько вариантов развертывания:
Вариант 1. Перехват и анализ копии трафика выполняется на одном компьютере (ключ установки **TMFDE All-in-one**). Кластер не создается:

- Настройте сервер на работу в качестве Sniffer (см. "Настройка работы сервера TMFD в качестве Sniffer", вариант 2)
- Настройте параметры приема копии трафика от Sniffer (см. "Настройка работы сервера TMFD в качестве Sniffer").

Вариант 2. Перехват и анализ копии трафика выполняется на разных компьютерах, кластеризация не используется:

- На одном компьютере (ключ установки **TMFDE Node server**):
    - Настройте сервер на работу в качестве Sniffer (см. "Настройка работы сервера TMFD в качестве Sniffer", вариант 1).
- На другом компьютере (ключ установки **TMFDE All-in-one**):

- Настройте параметры приема копии трафика от Sniffer (см. "Настройка сервера TMFD на прием копии трафика от Sniffer").

Вариант 3. Перехват и анализ копии трафика выполняются на разных компьютерах. Для увеличения производительности создан кластер из двух экземпляров сервера TMFD:

- Установите и настройте сервер СУБД Oracle со схемой БД TMFD с использованием типа установки *База данных* (ключ установки **TMFDE All-in-one**).
- На компьютере, где будет работать Sniffer (ключ установки **TMFDE Node server**):
  - Настройте его на работу в качестве Sniffer (см. "Настройка работы сервера TMFD в качестве Sniffer", вариант 1).
- На компьютере, где будет работать экземпляр кластера TMFD (ключ установки **TMFDE Node server**):
  - Настройте параметры приема копии трафика от Sniffer (см. "Настройка сервера TMFD на прием копии трафика от Sniffer").
  - Укажите параметры кластеризации (см. "Создание кластера TMFD").

Повторите п.3, чтобы добавить в кластер еще один экземпляр сервера TMFD.

3.5.1 Настройка работы сервера TMFD в качестве Sniffer

Для того чтобы сервер TMFD работал в качестве Sniffer, следует выполнить ряд настроек конфигурационного файла:

- Остановите серверные процессы TMFD:
  `service iwtm stop`
- Настройте автозапуск процессов:
  - Вариант 1. Перехват и анализ трафика будет выполняться на разных компьютерах.Настраиваемый экземпляр сервера TMFD будет работать только как Sniffer (перехват трафика):
    - Включите автозапуск процесса **iw_sniffer**.
    - Отключите автозапуск других процессов:
      `service имя_процесса stop`
  - Вариант 2. Перехват и анализ копии трафика будет выполняться на одном компьютере. Сервер TMFD будет принимать копию трафика от коммутатора (функция Sniffer), анализировать полученные данные и загружать их в базу данных (функции сервера TMFD):
    - Включите автозапуск процессов **iw_sniffer, iw_loader, iw_updater, iw_warpd и iw_adlibitum**.
    - Отключите автозапуск других процессов:
      `service имя_процесса stop`
- В конфигурационном файле **proxy.conf**, расположенном в директории `/opt/iw/tm5/etc`, в секции Startup включите автозапуск для нужных перехватчиков трафика (настройка для SMTP,HTTP(S), ICQ-трафика:
  - `"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}` – включение всех перехватчиков;

- `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}` – включение перехватчика **iw_proxy_http**;
- `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}` – выключение всех перехватчиков.

- В файле **/opt/iw/tm5/etc/sniffer.conf**, в секции `Iscp`, задайте параметры перехвата трафика:
  - `ListenHost`. IP-адрес, на который нужно принимать входящие соединения.
  - `ListenPort`. Порт, через который нужно принимать входящие соединения
- Запустите процессы TMFD:
  `service iwtm start`

3.5.2 Настройка сервера TMFD на прием копии трафика от Sniffer

Настройка выполняется на компьютере с сервером TMFD. Настройка необходима также и в том случае, когда Sniffer и сервер TMFD установлены на одном компьютере.
Перейдите в директорию `/opt/iw/tm5/etc` и выполните настройки:

- В конфигурационном файле **sniffer.conf** укажите требуемые параметры в секции каждого из перехватчиков (секции `Http`, `Icq` и `Smtp`):

Параметр	**Пояснения**
`Interface`	Сетевой интерфейс, через который будут поступать данные от коммутатора
`OpenInSec (подсекция Timeouts)`	Время сохранения соединения (в сек) при отсутствии пакетов. Рекомендуемое значение – `600`
`LiveInSec (подсекция Timeouts)`	Время ожидания (сек), в течение которого соединение должно перейти в состояние *ESTABLISHED*. Если состояние не изменилось, то соединение автоматически прекращается. Рекомендуемое значение – 86400
`CloseInSec (подсекция Timeouts)`	Время сохранения соединения (в сек) при переходе в состояние *TIME_WAIT*. Рекомендуемое значение – `300`
`TailInSec (подсекция Timeouts)`	Время ожидания доставки отправленных пакетов (в сек) после прекращения соединения
`QueueMemorySizeInBytes`	Объем памяти (в байтах), используемой для приема пакетов. При высокой загруженности канала, можно увеличить значение. Диапазон значений: от 1 до 500 Мб. Рекомендуемое значение – `16777216`

- Убедитесь, что в конфигурационном файле **proxy.conf** для параметра `SkipNegotiate` указано значение `false`.
- Если необходимо перехватывать ICQ-трафик, передаваемый через прокси-сервер (поверх HTTP), то в конфигурационном файле **proxy.conf** установите `true` для параметра `IcqFilter`.

- В конфигурационном файле **proxy.conf**, в разделе `Iscp` секций `Smtp`, `Icq`, `Http` укажите значение параметров `Host` и `Port`.
  Например, для настройки взаимодействия с компьютером, имеющим IP-адрес 10.20.30.40 и порт **1234**, раздел `Iscp` для перехватчика ICQ будет выглядеть следующим образом:

```
"iscp": {
 "ListenArea": "icq",
 "Host": 10.20.30.40,
 "Port": 1234
 }
```

3.5.3 Создание кластера TMFD

При перехвате копии трафика через Sniffer для увеличения производительности Системы можно создавать кластеры серверов TMFD.

> **Важно!**
>
> Один кластер может содержать до двух экземпляров сервера TMFD. Не рекомендуется использовать более 3-х кластеров.
> При использовании кластера сетевое соединение между Sniffer и сервером TMFD должно обеспечивать скорость передачи, в два раза превышающую ту скорость, с которой трафик поступает на Sniffer.

Чтобы создать кластер серверов TMFD, на каждом экземпляре сервера TMFD, который будет входить в кластер, в конфигурационном файле /opt/iw/tm5/etc задайте параметры кластеризации:

- Убедитесь, что в конфигурационном файле sniffer.conf секция `Usedareas` имеет следующий вид:
  ```
  "UsedAreas": [
  "capstack",
  "http",
  "icq",
  "smtp"
  ]
  ```
  По умолчанию данная настройка выполнена.
- В конфигурационном файле **proxy.conf**, в разделе `Iscp` секций `Smtp`, `Icq`, `Http` укажите значение параметров и `Host` и `Port`.
  Например,
  Для настройки взаимодействия с компьютером, имеющим IP-адрес 10.20.30.40 и порт **1234**, раздел Iscp для перехватчика ICQ будет выглядеть следующим образом:
  "iscp": {
  "ListenArea": "icq",
  "Host": 10.20.30.40,
  "Port": 1234
  }
- В конфигурационном файле **sniffer.conf** для каждой из секций `Smtp`, `Icq`, `Http` укажите значение параметра Balancer. Возможные значения:

- `Easy`. Для каждого нового TCP-соединения выбирается экземпляр TMFD Server с **iw_proxy**. Таким образом, поочередно задействуются все экземпляры сервера TMFD.
- `IpPref`. Распределение трафика между несколькими экземплярами сервера TMFD с **iw_proxy** выполняется на основании IP-адреса клиента. Это значит, что все данные с одинаковым IP-адресом клиента будут передаваться на один экземпляр сервера TMFD.

По умолчанию указан параметр `IpPref`.

Пример. Создание кластера из двух экземпляров сервера TMFD
Система перехватывает копию SMTP- и HTTP-трафика через Sniffer. Для повышения производительности при анализе трафика создается кластер из двух экземпляров сервера TMFD.

3.6 Настройка перехвата трафика

- Убедитесь, что в конфигурационном файле proxy.conf, расположенном в директории `/opt/iw/tm5/etc`, в секции Startup включен автозапуск перехватчикова трафика:
```
"Startup": {
"Enabled": true,
"smtp": true
"http": true
"icq": true
```
- Убедитесь, что включен автозапуск для процессов, участвующих в перехвате и обработке трафика: **iw_sniffer**, **iw_proxy_smtp**, **iw_messed**, **iw_warpd**, **iw_cas**, **iw_loader** (см. "Включение и выключение автозапуска процессов").
- Чтобы избежать дублирования перехваченных данных, отключите процесс **iw_smtpd**.
- Откройте на редактирование конфигурационный файл **capstack.conf**, расположенный в директории `/opt/iw/tm5/etc`.
- Убедитесь, что в секции Usedprocessors включен перехватчик NRPC-трафика:
```
"UsedProcessors": {
"nrpc": true,
```
- Убедитесь, что в секции Processors включена передача NRPC-трафика:
```
"processors": {
"nrpc": {
"TrackExternal": true,
"TrackInternal": true
},
```
- Убедитесь, что в секции Startup включен автозапуск:
```
"Startup": {
"Enabled": true
},
```
- Сохраните файл **capstack.conf**.
- Перезапустите процесс **capstack**:
```
service iwtm restart capstack
```

3.7 Автозапуск процессов

В этом разделе:

- Проверка автозапуска процессов;
- Включение и выключение автозапуска процессов.

Общая информация о работе с процессами изложена в разделе "Процессы TMFD Server".

3.7.1 Проверка автозапуска процессов

Важно!

Отключите автозапуск нелицензированных процессов, отвечающих за перехват трафика. Это позволит уменьшить количество сообщений в журнале протоколирования.

Автозапуск должен быть включен только для процессов, которые необходимы данному экземпляру сервера TMFD для корректной работы:

Процесс	**По умолчанию автозапуск включен**
iw_adlibitum	Да **Примечание:** Процесс должен работать только на основном сервере
iw_agent	Да
iw_agent_kicker	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью
iw_blackboard	Да
iw_blackboard_kicker	Да **Примечание:** Процесс должен работать только на основном сервере
iw_bookworm	Да
iw_capstack	Да
iw_cas	Да
iw_deliver	Да
iw_indexer	Да **Примечание:** Процесс должен работать только на основном сервере
iw_licensed	Да **Примечание:** Процесс должен работать только на основном сервере
iw_loader	Да

iw_luaengined	Да
iw_messed	Да
iw_notifier_kicker	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью
iw_proxy_http iw_proxy_icq iw_proxy_smtp	Да
iw_qmover_client	Нет
iw_qmover_server	Нет
iw_report_kicker	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью
iw_sample_compiler	Да
iw_selection_kicker	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью
iw_serman	Да
iw_sniffer	Да
iw_system_check	Да
iw_systemcheck_kicker	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью
iw_updater	Да
iw_warpd	Да
iw_whiteboard	Да
iw_xml2liro	Да

Примечение:

Чтобы удалить с сервера все **iw_*_kicker** процессы, удалите пакет **iwtm-webgui**:

```
rpm -e iwtm-webgui
```

3.7.2 Включение и выключение автозапуска процессов

Чтобы включить/отключить автозапуск процесса (пример приведен для службы iw_sniffer):

- Для корректной смены параметров остановите серверные процессы TMFD:
  `service iwtm stop`
- В файле `/opt/iw/tm5/etc/sniffer.conf` выполните настройки:
  Чтобы включить автозапуск для процесса, установите в блоке процесса:
  `"Startup" : {"Enabled" : true}`
  Чтобы отключить автозапуск для процесса, установите в блоке процесса:
  `"Startup" : {"Enabled" : false}`

> **Важно!**
>
> Для службы **iw_proxy** включение и выключение компонентов выполняется следующим образом:
>
> - `"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}` – включение всех модулей;
> - `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}` – включение модуля **iw_proxy_http**;
> - `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}` – выключение всех модулей.

- Запустите процессы TMFD:
  `service iwtm start`

3.8 Дополнительные настройки

После установки и настройки Системы, в зависимости от особенностей использования, могут потребоваться дополнительные настройки:

3.8.1 Настройка OCR-экстракторов

Распознавание текста из извлеченных изображений производится с использованием одного из двух OCR-экстракторов: Tesseract 3.0 и ABBYY FineReader Engine 9.5.
При установке с помощью программы-инсталлятора (**kickstart**) на серверную часть Системы устанавливаются оба OCR-экстрактора. По умолчанию на работу настроен Tesseract 3.0.

Функциональные ограничения экстракторов приведены в таблице ниже:

Функциональность	Tesseract 3.0	ABBYY FineReader Engine 9.5
Распознавание углов поворота изображения	-	0(+/-20) , 90(+/-20), 180(+/-20) и 270(+/-20) градусов
Распознавание цветного изображения	-	+
Коррекция изображения	-	+

Рекомендуемое разрешение изображения	300dpi для текста с размером шрифта от 10pt 400-600dpi для текста с размером шрифта 9pt и меньше	300dpi для текста с размером шрифта от 10pt 400-600dpi для текста с размером шрифта от 9pt и меньше

Чтобы настроить на работу экстрактор ABBYY FineReader Engine 9.5:

- Удалите символьную ссылку **/opt/iw/tm5/bin/iw_image2text**.
- Создайте символьную ссылку:
  `ln -s /opt/iw/tm5/bin/iw_image2text_fre /opt/iw/tm5/bin/iw_image2text`

Чтобы заменить используемый экстрактор ABBYY FineReader Engine 9.5 на Tesseract 3.0:

- Удалите символьную ссылку **/opt/iw/tm5/bin/iw_image2text**.
- Создайте символьную ссылку:
  `ln -s /opt/iw/tm5/bin/iw_image2text_ts /opt/iw/tm5/bin/iw_image2text`

3.8.2 Настройка отправки уведомлений пользователям и сотрудникам

Пользователь Консоли управления имеет возможность настроить отправку уведомлений из Системы пользователю или сотруднику. Уведомления отправляются в результате срабатывания тех или иных правил в политиках. Чтобы Система имела возможность отправлять уведомления, требуется:

- указать Системе электронный адрес, с которого будут отправляться уведомления – электронные сообщения пользователям или сотрудникам
- настроить отправку писем через Postfix.

Чтобы настроить электронный адрес для отправки уведомлений:

- Подключитесь к БД от имени владельца схемы.
- В таблице *SETTING*, для атрибута `NOTIFY_SENDER` укажите требуемый e-mail адрес отправителя.

Чтобы проверить, отправляются ли письма через Postfix,
Выполните команду:
`sendmail -v <employee@company.com> < <sample.log>`
где:

- `<employee@company.com>` - email-адрес пользователя, которому будет отправлено уведомление
- `<sample.log>` - текстовый файл, содержимое которого будет служить текстом письма (для проверки рекомендуется использовать простой текстовый файл размером до 1 МБ).

Если письма не отправляются, настройте отправку писем через Postfix.

Чтобы настроить отправку писем через Postfix:

- Откройте файл **/etc/postfix/main.cf**;
- В качестве значения параметра `relayhost` укажите требуемый почтовый сервер:
  `relayhost = <mail.company.ru>,`
  где `<mail.company.ru>` - требуемый почтовый сервер

Примечание:

Если в файле **/etc/postfix/main.cf** нет строки с параметром `relayhost`, добавьте такую строку.

- Перезапустите Postfix с помощью команды:
  `service postfix restart`
- Проверьте, выполняется ли отправка сообщений, с помощью команды:
  `sendmail -v <employee@company.com> < <sample.log>,`
  где:

- `<employee@company.com>` - email-адрес пользователя, которому будет отправлено уведомление
- `<sample.log>` - текстовый файл, содержимое которого будет служить текстом письма (для проверки рекомендуется использовать простой текстовый файл размером до 1 МБ).

3.8.3 Ограничение количества найденных событий

Вы можете указать ограничение для количества событий, которые будут выведены в Консоли управления в результате применения фильтра. Для этого в таблице *SETTING* Базы данных укажите требуемое значение для атрибута *query_stop_count*. По умолчанию задано ограничение 10 000.

3.8.4 Настройка синхронизации времени

- Установите системное время с помощью команды `date`. Например, для установки 11 сентября 2013 13:30 запустите команду со следующими параметрами:
  `date 09111330`
- Скопируйте системное время для настройки аппаратных часов с помощью команды:
  `hwclock --systohc`
- Проверьте, что системное и аппаратное время настроены корректно:
  `hwclock ; date`
- Время должно быть одинаковым, допустимы небольшие отклонения.
  Остановите службу ntpd:
  `service ntpd stop`
- Определите сервер синхронизации времени. Вы можете использовать любую службу точного времени, работающую по протоколу ntp и доступную из вашей сети: как сетевое оборудование, так и контроллеры домена Windows (сервер Active Directory).
  Чтобы проверить, поддерживает ли сервер NTP, воспользуйтесь командой ntpdate -q <IP> (где IP - адрес проверяемого сервера), например:

```
root@atl-iw:~# ntpdate -q 10.10.0.98
server 10.10.0.98, stratum 3, offset 9.196765, delay 0.04437
11 Sep 13:09:02 ntpdate[13819]: step time server 10.10.0.98 offset 9.196765 sec
root@atl-iw:~#
```

- Настройте синхронизацию, указав сервер NTP-синхронизации в файле /etc/ntp.conf. Для этого добавьте запись вида (укажите IP-адрес вашего NTP-сервера):
  `server 10.10.0.98`
- Запустите службу ntpd:
  `service ntpd start`
- Проверьте текущее состояние службы ntpd с помощью команды:
  `service ntpd status`
- Включите автоматическую синхронизацию времени:
  `chkconfig --level 345 ntpd on`

3.8.5 Конфигурирование работы Sphinx при распределенной установке

Полнотекстовый поиск по запросам в TMFD осуществляется посредством поискового механизма Sphinx. Служба **sphinx** устанавливается в режиме установки **All-in-one** или **TMFDE DB server**.

Распределенной установкой считается схема установки, когда TMFD и база данных установлены на разных серверах с ключами **TMFDE Node server** и **TMFDE DB server** соответственно.

При наличии второстепенных серверов, выполните следующие действия:

- На сервере **TMFDE Node server** в параметре `hostname` секции `search` конфигурационного файла **web.conf** укажите IP-адрес сервера, на котором запущена служба **sphinx** (сервер с базой данных);
- На сервере **TMFDE DB server** в конфигурационном файле **/opt/iw/tm5/etc/serman_resolver.conf** в параметре `Host` укажите `IP-адрес` основного сервера.

3.8.6 Настройка подсистемы мониторинга

Подсистема мониторинга выполняет следующие функции:

1. мониторинг работы всех серверов, входящих в состав решения TMFD (как физических, так и виртуальных);
2. мониторинг всех программных компонентов, входящих в состав решения (ОС, СУБД, БД, процессы и т.д.);
3. контроль значений индикаторов для каждого сервера и компонента. Под контролем подразумевается периодическое получение значения индикатора и сравнение значения индикатора с пороговым значением;
4. возможность включения и отключения мониторинга отдельных индикаторов и отдельных серверов;

Подсистема мониторинга автоматически устанавливается при установке серверных компонентов системы TMFD с помощью программы-инсталлятора (**kickstart**).

Если система TMFD установлена так, что все серверные компоненты расположены на одном компьютере (**All-in-one**) или сервер базы данных (**DB server**) установлен отдельно от сервера TMFD (**Node server**), диагностика серверов будет настроена автоматически.

Настройка подсистемы мониторинга включает следующие задачи:

1. Ручная настройка индикаторов;
2. Настройка адреса сервера синхронизации времени для подсистемы мониторинга;
3. Настройка порогов срабатывания для индикатора нагрузки;
4. Настройка запуска служб;
5. Настройка механизма уведомлений.

3.8.6.1 Ручная настройка индикаторов

Включение и выключение индикаторов производится в конфигурационных файлах директории `/etc/nagios/iwmon`:

1. iwmon-services-db-psql.cfg – настройка индикаторов для базы данных Postgre SQL;
2. iwmon-services-db.cfg – настройка индикаторов для базы данных Oracle;
3. iwmon-services-loadavg.cfg – настройка параметров нагрузки на серверы (индикатор Общая нагрузка системы);
4. iwmon-services.cfg – настройка основных индикаторов;
5. iwmon-services-queue.cfg – настройка индикаторов очередей;
6. iwmon-services-traffic.cfg – настройка индикатора трафика из подсетей.

Параметр `service_description` отображает назначение каждого индикатора.

Чтобы включить индикатор, измените значение параметра `register на 1.`

Чтобы выключить индикатор, измените значение параметра `register` на `0`.

Чтобы применить изменения, перезапустите процесс nagios:

```
nagios service restart
```

3.8.6.2 Настройка адреса сервера синхронизации времени для подсистемы мониторинга

Для корректной синхронизации времени, на всех серверах системы необходимо указать IP-адрес NTP-сервера. Вы можете использовать любую службу точного времени, работающую по протоколу NTP и доступную из вашей сети: как сетевое оборудование, так и контроллеры домена Windows.
Чтобы настроить синхронизацию времени на сервере:

- Откройте на редактирование файл **iwmon-services-ntp.cfg**.
- В значении параметра `check command` замените IP-адрес, заданный по умолчанию, на актуальный IP-адрес NTP-сервера (сервера синхронизации времени).

3.8.6.3 Настройка порогов срабатывания для индикатора нагрузки

В файле **/etc/nagios/iwmon/iwmon-services-loadavg.cfg** для индикатора (службы) `Current Load`, который проверяет значения для load average на сервере TMFD, уточните пороговые значения срабатывания, в зависимости от количества ядер на сервере TMFD.
Например, для 4-х ядерного процессора пороговые значения должны быть определены

следующим образом:
`iwmon_check_load!10.0,8.0,6.0!20.0,16.0,12.0`
Пороговые значения для другого количества ядер вычисляются пропорционально.

3.8.6.4 Настройка запуска служб

3.8.6.5 Настройка механизма уведомлений

Подсистема мониторинга позволяет отправлять уведомления по электронной почте для случаев, когда текущее значение индикатора превышает пороговое значение.
В разделе:

- Настройка отправки уведомлений о превышении порогового значения индикаторов; Настройка отправки писем-уведомлений с помощью Postfix.

3.8.6.5.1 Настройка отправки уведомлений о превышении порогового значения индикаторов

Чтобы настроить отправку почтовых уведомлений:

1. В конфигурационном файле **/etc/nagios/private/resource-notify-iw.cfg** в качестве значения параметра `$USER10$` укажите сервер Postfix, встроенный в систему TMFD, и используемый порт. Например:
   `$USER10$=localhost:25`
2. В конфигурационном **файле /etc/nagios/iwmon/iwmon-contacts.cfg** добавьте контакты, на которые будут отправляться уведомления. Для этого нужно для каждого контакта добавить секцию вида:

```
define contact{
        contact_name                    <название контакта>
        use                             generic-contact
        alias                           Recipient Notification
        service_notification_commands   iw-notify-service-by-email
        host_notification_commands      iw-notify-host-by-email
        email                           <адрес>
        register                        1
}
```

> **Примечание:**
>
> Также в этой секции можно указать дополнительные настройки отправки уведомлений, например, время отправки и события, при которых будут отправляться уведомления. Подробную информацию Вы можете найти в документации Nagios.

3. В этом же файле, в поле `members`, укажите названия контактов, на которые будут отсылаться уведомления. Контакты указываются через запятую:

```
define contactgroup{
        contactgroup_name           admins
        alias                       IW Nagios Notification Recipient
        members                     <название контакта>, <название контакта1>
}
```

4. Перезапустите Nagios, выполнив следующую команду:
   `service nagios restart`

Уведомления будут содержать следующую информацию:

1. Название индикатора;
2. Имя сервера, на котором контролируемый индикатор превысил пороговое значение;
3. IP адрес этого сервера;
4. Текущее состояние индикатора;
5. Дата и время превышения порогового значения индикатора;
6. Системное сообщение от источника.

Чтобы настроить отправку почтовых уведомлений для выбранных индикаторов:

1. Зайдите в каталог подсистемы Nagios:
   `cd /etc/nagios/iwmon`
2. Откройте файл iwmon-services.cfg:
   `nano /etc/nagios/iwmon/iwmon-services.cfg:`
3. Для того чтобы определить нужный индикатор, посмотрите поле `service_description`.
4. В секции индикатора измените параметр `notifications_enabled` на:
   a. 1 – если вы хотите включить отправку уведомлений
   b. 0 – если вы хотите выключить отправку уведомлений
5. Сохраните изменения.

> **Примечание:**
>
> В случае если в конфигурационном файле отсутствует параметр `notifications_enabled`, добавьте его вручную.

3.8.6.5.2 Настройка отправки писем-уведомлений с помощью Postfix

Если Система установлена так, что:

- отправка SMTP-писем выполняется с использованием Postfix

и

- подсистема мониторинга установлена на тот же сервер, что и Postfix,

то для корректной отправки писем с уведомлениями:

- В файле `/etc/postfix/transport` добавьте строчки вида:
  `example@example.com smtp:[mailserver]`
  где `example@example.com` - адрес, на который должны отправляться почтовые сообщения, а `mailserver` – имя почтового сервера компании.
  Для каждого адресата должна быть указана отдельная строчка.

- Выполните команду:

  `postmap /etc/postfix/transport`

- В файл /etc/postfix/main.cf добавьте параметр transport_maps:
  `transport_maps = hash:/etc/postfix/transport`
- Перезагрузите Postfix:
  `service postfix restart`

3.9 Лицензирование

Ознакомительная лицензия на перехватчики действует в течение 30 дней со дня сборки устанавливаемого дистрибутива TMFD и допускает использование не более чем 100 пользователями. Чтобы продолжить эксплуатацию Системы, установите коммерческую лицензию на перехватчики, которые Вы планируете использовать.
Чтобы продолжить эксплуатацию Системы по истечении ознакомительного срока, установите коммерческую лицензию на перехватчики, которые Вы планируете использовать. Для этого запросите файл коммерческого лицензионного ключа (см. "Запрос лицензии").
Коммерческий лицензионный ключ представляет собой файл формата LIC.
При установке и использовании лицензионного ключа нужно учитывать следующее:

- Если период действия ознакомительной лицензии истек, работа перехватчиков будет остановлена. Установите коммерческую лицензию или удалите Систему.
- Если требуется изменить настройки передачи трафика согласно новой схеме развертывания, замените лицензионный ключ с учетом новых перехватчиков.

При полной переустановке операционной системы или системы TMFD вам потребуется заново установить лицензию. Поэтому рекомендуется сохранить файл лицензионного ключа на каком-либо носителе информации.

4 АДМИНИСТРИРОВАНИЕ СИСТЕМЫ

После установки Системы выполняются следующие настройки, необходимые для штатного функционирования Системы:

- Администрирование базы данных
- Администрирование серверной части TMFD

4.1 Администрирование базы данных

Этот раздел содержит информацию по администрированию:

- Oracle
- Postgre SQL

4.1.1 Oracle

Раздел содержит инструкции по администрированию Oracle:

1. Проведение регламентных работ на сервере базы данных
2. Табличные пространства в базе данных TMFD
3. Управление ежедневными табличными пространствами
4. Резервное копирование базы данных

4.1.1.1 Проведение регламентных работ на сервере базы данных

Важно!

Категорически не рекомендуется выключать сервер БД кнопкой питания. В некоторых случаях это может привести к повреждению БД

При выполнении регламентных работ на сервере базы данных придерживайтесь такого порядка:

1. Закройте все окна браузера, отображающие Консоль управления. Убедитесь, что отсутствуют соединения со схемой БД TMFD из других программ. Если такие соединения есть, отключите их.
2. На сервере TMFD остановите процессы TM:
```
service iwtm stop
service php-fpm stop
service nginx stop
```

3. На сервере базы данных получите список заданий, запускающихся по расписанию. Для этого в sqlplus, из-под учетной записи владельца схемы выполните запрос:
```
select JOB_NAME, STATE
from user_scheduler_jobs u
where u.enabled = 'TRUE'
```
4. Выключите задания, выполнив сценарий:
```
BEGIN
dbms_scheduler.disable('JOB_1');
…
dbms_scheduler.disable('JOB_N');
COMMIT;
END;
/
```
где JOB_1… JOB_N – имена выключаемых заданий.
5. Убедитесь, что ни одно задание не выполняется. Для этого выполните запрос:
```
SELECT job_name
FROM user_scheduler_running_jobs
```
Будет выведен перечень запущенных заданий. Если какое-либо задание выполняется, Вы можете остановить его, выполнив сценарий:
```
BEGIN
dbms_scheduler.stop_job('имя_задания');
COMMIT;
END;
/
```
6. Выполните необходимые работы с базой данных.
7. По окончании необходимых работ, с сервера TMFD проверьте соединение с сервером базы данных:
```
sqlplus db_login/db_password@tns_name
```
Здесь db_login и db_password – имя и пароль владельца схемы базы данных, а tns_name – имя службы TNS.
Если проверка пройдена успешно, то в ответ на выполнение команды будет выведено приглашение SQL *Plus:
```
SQL>
```
8. Запустите процессы TMFD Server:
```
service iwtm start
service php-fpm start
service nginx start
```
9. Проверьте системный журнал на наличие ошибок. Путь к файлу журнала:
```
/var/log/messages
```
10. Если в системном журнале содержится информация об ошибках, то обратитесь в службу технической поддержки.
11. Включите выполнение ранее отключенных заданий:
```
BEGIN
dbms_scheduler.enable('JOB_1');
…
dbms_scheduler.enable('JOB_N');
COMMIT;
END;
/
```
где JOB_1… JOB_N – имена ранее остановленных заданий.

4.1.1.2 Табличные пространства в базе данных TMFD

В базе данных TMFD имеются два типа табличных пространств (ТП):

Тип табличного пространства	Назначение
Основное	Хранение настроек, которые нужны для анализа и обработки объектов (конфигурация, теги, цвета и пр.). Управление системой через Консоль управления (роли, учетные записи пользователей и др.)
Ежедневное	Хранение объектов, перехваченных в течение одних суток. Хранение информации о результатах анализа и обработки объектов. Состоит из двух табличных пространств: для хранения объектов со статусами *Нарушение* и *Нет нарушений*. Таким образом, достигается возможность раздельного архивирования, восстановления и удаления.

Все данные об объектах, перехваченных в определенный день, находятся в одном ежедневном ТП. Ежедневные ТП создаются каждые сутки с таким расчетом, чтобы в базе данных всегда были ТП для работы в ближайшие шесть суток, не включая текущие. Всем ежедневным ТП автоматически присваиваются имена:

- <*SchemaOwner*>*_YYYY_MM_DD_N* – табличное пространство за день, которое содержит объекты без нарушений.
- <*SchemaOwner*>*_YYYY_MM_DD_V* – табличное пространство за день, которое содержит объекты с нарушениями.

Параметры, предназначенные для управления сегментами данных, задаются при настройке схемы базы данных, но могут быть переопределены после создания схемы.

4.1.1.3 Управление ежедневными табличными пространствами

В этом разделе:

- Настройка размещения файлов в файловой системе;
- Индексирование данных в ежедневных табличных пространствах;
- Архивирование ежедневных табличных пространств;
- Восстановление ежедневных табличных пространств;
- Удаление ежедневных табличных пространств.

4.1.1.3.1 Настройка размещения файлов в файловой системе

Ежедневные табличные пространства могут храниться либо в одном каталоге, либо распределенно, в разных каталогах на разных дисках.
При установке системы с помощью поставляемого инсталлятора задается использование одного ежедневного табличного пространства, расположенного в `/u02/oradata/`.
Однако при больших нагрузках рекомендуется размещать ежедневные табличные пространства распределенно, на разных файловых системах (LUN-ах, физических дисках) для поочередного их использования. Например, если задано 3 файловых системы, то данные будут размещаться следующим образом:

Первый день – ежедневное табличное пространство создается в файловой системе 1.
Второй день – ежедневное табличное пространство создается в файловой системе 2.
Третий день – ежедневное табличное пространство создается в файловой системе 3.
Четвертый день – ежедневное табличное пространство создается в файловой системе 1.
…

Распределение файлов ежедневных ТП (количество и расположение) можно изменять с помощью следующих сценариев.

Пример сценария, изменяющего количество отдельных мест хранения ежедневных ТП:

```
BEGIN
pkg_part.set_df_path_cnt('4');
 COMMIT;
 END;
 /
```

> **Важно!**
>
> Изменив количество мест хранения ежедневных ТП, обязательно откорректируйте (добавьте/удалите) пути их расположения.

Пример сценария, изменяющего пути для расположения ежедневных ТП:

```
BEGIN
pkg_part.set_df_path('/test1/', 1);
pkg_part.set_df_path('/test2/', 2);
pkg_part.set_df_path('/test3/', 3);
pkg_part.set_df_path('/test4/', 4);
 COMMIT;
 END;
 /
```

> **Примечание:**
>
> Рекомендуется при указании пути в конце указывать символ «/».

Пример сценария просмотра содержимого ежедневных ТП:

```
select a.tbs_name, a.service_code, power(10, trunc(log(10, a.text_size))) || '-' ||
power(10, trunc(log(10, a.text_size)) + 1) size_range,
count(1) cnt, sum(a.text_size) text_size
from
(
select t.tbs_name, o.service_code,
 case
 when length(o.text) > 0 then length(o.text)
 else 1
 end text_size
from object o
inner join object_source os on os.object_id = o.object_id
inner join tbs_list t on o.tbs_id = t.tbs_id
) a
group by a.tbs_name, a.service_code, power(10, trunc(log(10, a.text_size))) || '-' ||
```

```
power(10, trunc(log(10, a.text_size)) + 1)
order by 1, 2, 3
```

Определение кодов сервиса указано в файле **services.xml**, который находится в каталоге `/opt/iw/tm5/etc/compendiums/`.

> **Примечание:**
>
> Чтобы получить результат анализа размеров перехваченных объектов в табличных пространствах вместе со служебной информацией БД, рекомендуется использовать SQLDeveloper.

4.1.1.3.2 Индексирование данных в ежедневных табличных пространствах

Контекстный поиск по тексту перехваченных объектов возможен при условии, что в базе данных регулярно выполняется индексация поступающих данных. По умолчанию задание на индексацию запускается каждые 20 минут.

Корректность работы задания на индексацию данных (отсутствие зависаний) можно проверить, выполнив следующий запрос от имени владельца схемы базы данных:

```
select t.REQ_START_DATE, t.actual_start_date, t.RUN_DURATION
from sys.user_scheduler_job_run_details t
where t.job_name='IWTM_SYNC_INDEXES' and t.LOG_DATE > sysdate - 3/24
```

По результатам запроса выводится информация о работе задания на индексацию данных за последние 3 часа. Если интервал индексации не менялся, то задание должно запускаться каждые 20 минут и выполняться менее чем за 20 минут. При сильной загрузке базы данных следует выполнять эту проверку периодически, с интервалами в несколько часов.

Изменение интервала индексации

> **Примечание:**
>
> Контекстный поиск по объектам, загруженным в базу данных, становится возможен только после того, как эти объекты будут проиндексированы. Это необходимо учитывать при изменении интервала между процедурами индексации.

Далее показано несколько примеров использования сценария.Чтобы изменить интервал индексации, запустите сценарий:

```
DECLARE
 v_start_date date;
 v_repeat_interval VARCHAR2(100);
 BEGIN
 v_start_date := SYSDATE;
 v_repeat_interval := 'FREQ=MINUTELY; INTERVAL=10';
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
 COMMIT;
 END;
```

```
/
```

где:

1. v_start_date – дата и время запуска задания. Указывается в любом из форматов даты, поддерживаемых СУБД Oracle.
2. v_repeat_interval – частота выполнения задания. Определяется параметрами:
    a. FREQ. Размерность частоты, с которой будет выполняться задание. Допустимы следующие значения: DAILY, WEEKLY, MONTHLY, HOURLY, MINUTELY.
    b. INTERVAL. Значение частоты с выбранной размерностью. Допустимы целые значения от 1 до 99.

Пример 1. Запуск индексации 1 раз в минуту

```
DECLARE
 v_start_date date;
 v_repeat_interval VARCHAR2(100);
 BEGIN
 v_start_date := SYSDATE;
 v_repeat_interval := 'FREQ=MINUTELY; INTERVAL=1';
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
 COMMIT;
 END;
 /
```

Пример 2. Запуск индексации 1 раз в 2 часа

```
DECLARE
 v_start_date DATE;
 v_repeat_interval VARCHAR2(100);
 BEGIN
 v_start_date := SYSDATE;
 v_repeat_interval := 'FREQ= HOURLY; INTERVAL=2';
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
 COMMIT;
 END;
 /
```

Пример 3. Запуск индексации ежесуточно в 00 ч 00 мин 00 с, начиная со следующего дня

```
DECLARE
 v_start_date DATE;
 v_repeat_interval VARCHAR2(100);
 BEGIN
 v_start_date := trunc(SYSDATE + 1);
 v_repeat_interval := 'FREQ= DAILY; INTERVAL=1';
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
 COMMIT;
 END;
 /
```

4.1.1.3.3 Архивирование ежедневных табличных пространств

Чтобы освободить пространство на жестком диске, Вы можете периодически архивировать устаревшие данные. Архив с данными рекомендуется размещать на внешних носителях информации. При необходимости эти данные могут быть восстановлены.

> **Важно!**
>
> Если в качестве интервала времени используются месяцы или годы, то рекомендуется в расчете использовать максимальное значение интервала. Для месяца – 31 день. Для года – 366 дней. Например, чтобы архивировать ежедневные ТП старше 4-х лет, в задании IWTM_ARCHIVE_TABLESPACES укажите интервал 366*4=1464 дня.

Архивирование может выполняться:

- Автоматически после истечения указанного периода;
- Вручную – для архивирования выбранного ЕТП.

4.1.1.3.3.1 АВТОМАТИЧЕСКОЕ АРХИВИРОВАНИЕ ЕЖЕДНЕВНЫХ ТАБЛИЧНЫХ ПРОСТРАНСТВ

Перед тем, как включить автоматическое архивирование, необходимо проверить, что каталог архивирования задан верно:

```
select value
from setting
where setting = 'archive_path'
```

Пользователь `oracle` должен являться владельцем каталога.

Если каталог установлен неправильно, установите его, выполнив следующую команду:

```
begin;
select sp_setting_set('archive_path', '/test/archive/');
commit;
```

Для автоматического архивирования табличных пространств (по умолчанию функция выключена) Вы можете использовать следующие сценарии (запускаются от имени владельца схемы данных):

1. Для ежедневного табличного пространства, хранящего объекты со статусом *Нарушение*:

```
begin
 sp_setting_set('violation_archive_enabled', 1);
 sp_setting_set('violation_archive_period', D);
 commit;
 end;
```

где:
1 – показатель того, что автоматическое архивирование включено (чтобы выключить, вместо 1 используйте значение 0);
D – количество дней, по истечении которого ежедневное табличное пространство будет архивироваться Системой.

1. Для ежедневного табличного пространства, хранящего объекты со статусом *Нет нарушений*:

```
begin
 sp_setting_set('noviolation_archive_enabled', 1);
 sp_setting_set('noviolation_archive_period', D);
 commit;
 end;
```

где:
1 – показатель того, что автоматическое архивирование включено (чтобы выключить, вместо 1 используйте значение 0);
D – количество дней, по истечении которого ежедневное табличное пространство будет архивироваться Системой.

4.1.1.3.3.2 АРХИВИРОВАНИЕ ЕЖЕДНЕВНЫХ ТАБЛИЧНЫХ ПРОСТРАНСТВ ВРУЧНУЮ

Архивирование ЕТП вручную производится в порядке, представленном ниже.

Выборка ежедневных табличных пространств и файлов данных

Список отключаемых табличных пространств можно получить, выполнив запросы к базе данных от имени владельца схемы базы данных. Запросы составляются в соответствии со стратегией архивирования, принятой в вашей организации. Например, для выборки ежедневных ТП, в которых хранятся объекты, перехваченные более 100 дней назад, можно применить следующий запрос:

```
SELECT t.tbs_id, t.tbs_name, t.part_date
FROM tbs_list t
WHERE t.part_date<trunc(SYSDATE) - 100 + 23 / 24 AND t.status IN (0, 3)
```

> **Важно!**
>
> Настоятельно рекомендуется для получения списка файлов использовать запрос, пример которого описывается далее в этом разделе. Это связано с тем, что список файлов данных, полученный другими способами, может оказаться неполным.

Для выборки файлов данных в этом случае создается следующий запрос:

```
SELECT f.file_name
FROM dba_data_files f
WHERE f.tablespace_name in
(
  SELECT t.tbs_name
  FROM tbs_list t
  WHERE t.part_date<trunc(SYSDATE) - 100 + 23 / 24 AND t.status IN (0, 3)
)
```

где `t.status IN (0, 3)` указывает на то, что для архивации выбраны табличные пространства со статусами *Чтение и запись* (код статуса 0) и *Только чтение* (код статуса 3).

Отключение ежедневных табличных пространств от базы данных

Важно!

Не отключайте ежедневные ТП во время работы заданий IWTM_ADD_PARTS, IWTM_DELETE_TABLESPACES и IWTM_ARCHIVE_TABLESPACES так как это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:
   `select pkg_part_archive_tablespace(N);`
   где `N` – это значение атрибута `tbs_id` целевого ТП из таблицы `tbs_list`.
   После выполнения этого сценария статус ежедневного ТП изменится на *Отключено от базы данных*.
2. Повторите вызов процедуры для каждого ежедневного ТП, которое нужно отключить.

Перенос файлов данных

Перенесите файлы данных, принадлежащие отключенным ежедневным ТП, на другой носитель информации.
Для получения списка отключенных табличных пространств используйте команду:
`select tbs_name from tbs_list where NOTE = 'Tablespace is offline'`
где `tbs_name` – имя табличного пространства.
`tbs_list` – имя таблицы.
Файлы данных хранятся в каталоге:
`select value from setting where setting = 'archive_path'`

4.1.1.3.4 Восстановление ежедневных табличных пространств

Важно!

Табличное пространство можно восстанавливать только в той схеме базы данных, в которой оно было отключено (даже если эта схема была обновлена). Восстановить табличное пространство после полной переустановки схемы базы данных невозможно.

Перемещение файлов данных

Для восстановления ежедневного ТП необходимо переместить файлы данных этого табличного пространства с внешнего носителя в каталог, путь к которому можно получить, выполнив запрос:

`select value from setting where setting = 'archive_path'`

Важно!

Убедитесь, что пользователь *oracle* имеет права на чтение и запись в том каталоге, куда будут перемещаться файлы данных.

Подключение ежедневного табличного пространства

Важно!

Не подключайте ежедневное ТП во время работы заданий IWTM_ADD_PARTS и IWTM_DELETE_TABLESPACES. Это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:
   ```
   begin
   pkg_part.restore_tablespace(N);
   end;
   ```
   где `N` – ID табличного пространства (указывается в tbs_list).
   После выполнения процедуры статус ежедневного ТП изменится на *Восстановлено*.
2. Повторите вызов процедуры для каждого ежедневного ТП, которое нужно подключить
   .

4.1.1.3.5 Удаление ежедневных табличных пространств

Если дальнейшее хранение данных не требуется, то Вы можете воспользоваться процедурой удаления ежедневных ТП (**IWTM_DELETE_TABLESPACES**). Данная процедура позволяет автоматически удалить все данные, хранящиеся в табличном пространстве, сегменты, табличное пространство и файлы данных.

Важно!

- Удаление табличных пространств – необратимая операция. После выполнения этой операции Вы не сможете восстановить удаленные данные.
- После удаления табличных пространств, которые отключены от базы данных (имеют статус *Offline*), остаются файлы данных. Чтобы освободить пространство на жестком диске, удалите эти файлы вручную.
- Процедура IWTM_DELETE_TABLESPACES не работает с теми табличными пространствами, которые были отключены/подключены вручную.

В результате выполнения этой процедуры удаляются все ежедневные ТП (и в т.ч. информация о заархивированных ежедневных ТП), которые удовлетворяют следующему условию:

Дата создания табличного пространства меньше или равна разнице между текущей датой и заданным интервалом времени для удаления табличного пространства.

Примечание:

Если заархивированное ежедневное ТП не подлежит восстановлению (т.к. информация о нем была удалена из базы данных), то Вы можете удалить файлы данных этого ежедневного ТП из архива.

На время удаления табличных пространств работа процессов **iw_deliverd**, **iw_loader**, **iw_updater** будет автоматически приостановлена. По завершении процедуры удаления, выполняется

автоматический перезапуск процессов. Рекомендуется запускать задание на удаление данных ежедневно. В противном случае количество удаляемых данных увеличится, что приведет к большим временным затратам на выполнение данной процедуры и, как следствие, к увеличению времени простоя сервера TMFD.

Важно!

Если в качестве интервала времени используются месяцы или годы, то рекомендуется в расчете использовать максимальное значение интервала. Для месяца – 31 день. Для года – 366 дней. Например, чтобы удалять ежедневные ТП старше 4-х лет, в задании IWTM_DELETE_TABLESPACES укажите интервал 366*4=1464 дня.

Определение интервала времени для удаления ежедневных ТП

Для автоматического удаления табличных пространств (по умолчанию функция выключена) вы можете использовать следующие сценарии (запускаются от имени владельца схемы данных):

1. Для ЕТП, хранящего объекты со статусом *Нарушение*:

```
begin
 sp_setting_set('violation_delete_enabled', 1);
 sp_setting_set('violation_delete_period', D);
 commit;
 end;
```

где:
`1` – показатель того, что автоматическое удаление включено (чтобы выключить, вместо 1 используйте значение 0);
`D` – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

1. Для ЕТП, хранящего объекты со статусом *Нет нарушений*:

```
begin
 sp_setting_set('noviolation_delete_enabled', 1);
 sp_setting_set('noviolation_delete_period', D);
 commit;
 end;
```

где:
`1` – показатель того, что автоматическое удаление включено (чтобы выключить, вместо 1 используйте значение 0);
`D` – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

Включение запуска процедуры по расписанию

По умолчанию автоматическое удаление ежедневных ТП отключено. Чтобы включить удаление всех ежедневных ТП согласно расписанию (ежедневно, в 01 ч. 00 мин. 00 с.), от имени владельца схемы базы данных выполните следующий сценарий:

```
BEGIN
 dbms_scheduler.enable('IWTM_DELETE_TABLESPACES');
 COMMIT;
 END;
 /
```

Чтобы отключить автоматическое выполнение процедуры по расписанию, выполните следующий сценарий:

```
BEGIN
 dbms_scheduler.disable('IWTM_DELETE_TABLESPACES');
 COMMIT;
 END;
 /
```

Ручной запуск процедуры

Если вам требуется немедленный запуск процедуры удаления ежедневных ТП (например, из-за нехватки места в файловой системе был изменен интервал удаления, но следующий запуск задания произойдет нескоро), от имени владельца схемы базы данных выполните следующий сценарий:

```
BEGIN
 dbms_scheduler.run_job('IWTM_DELETE_TABLESPACES');
 END;
 /
```

4.1.1.4 Резервное копирование базы данных

Для снижения рисков потери данных рекомендуется ежемесячно выполнять создание резервной копии (бэкапа) базы данных. Для хранения бэкапов рекомендуется использовать специально выделенные системы хранения.

Опытные администраторы промышленных баз данных Oracle могут выполнять резервное копирование на работающей БД (процедура «горячего бэкапа») с помощью программы RMAN, рекомендуемой компанией Oracle (см. документацию Oracle), предварительно переведя БД Oracle в режим ARCHIVELOG.

Для специалистов, не являющихся администраторами Oracle, то есть не располагающих стандартными методами создания резервной копии БД, рекомендуется описанная ниже процедура «холодного бэкапа», выполняемая на остановленной БД. Данная процедура также может применяться для переноса базы данных с одного сервера на другой.

Далее в разделе:

1. Создание резервной копии базы данных;
2. Восстановление базы данных из резервной копии.

4.1.1.4.1 Создание резервной копии базы данных

Процедура создания резервной копии (выполнения холодного бэкапа) осуществляется в следующем порядке:

1. Определение размера резервной копии;
2. Проверка хранилища резервной копии;
3. Создание папок для резервной копии;
4. Создание вспомогательных файлов на Linux;
5. Создание списка файлов, подлежащих резервному копированию;
6. Остановка системы;
7. Остановка БД Oracle;
8. Копирование файлов БД в хранилище резервных копий.

4.1.1.4.1.1 ОПРЕДЕЛЕНИЕ РАЗМЕРА РЕЗЕРВНОЙ КОПИИ

Чтобы определить размер базы данных:

1. На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
2. Откройте Oracle SQL*Plus и подключитесь как пользователь *sysdba*:
   `OS> sqlplus / as sysdba`
3. Если система была установлена с помощью программы-инсталлятора (kickstart), для удобства можете воспользоваться командой **wsqlplus**.

   > **Примечание:**
   >
   > Команда `wsqlplus` является алиасом команды `sqlplus`:
   > `alias wsqlplus='rlwrap -b "" -f ~/sql.dict sqlplus'`

   Дождитесь подключения – об этом будет свидетельствовать сообщение **Connected**.
4. Скопируйте (или введите) в командную строку и выполните следующий SQL запрос:
   ```
   SQL> SELECT ROUND(SUM(bytes)/1024/1024/1024,4) GB FROM ( SELECT SUM(bytes) bytes FROM dba_data_files union SELECT SUM(bytes) bytes FROM dba_temp_files union SELECT SUM(bytes) bytes FROM v$log);
   ```
5. Запишите получившийся размер базы данных.
6. Выйдите из Oracle SQL*Plus:
   `SQL> exit`

4.1.1.4.1.2 ПРОВЕРКА ХРАНИЛИЩА РЕЗЕРВНОЙ КОПИИ

Проверьте приемлемость выбранного хранилища резервной копии. Оно должно соответствовать следующим требованиям:

1. Размещаться на компьютере, отличном от того, где работает база данных.
2. Доступно с компьютеров, где работают сервера и базы данных, подлежащие резервному копированию.
3. На жестком диске больше свободного места, чем размер резервной копии:

Чтобы определить количество свободного места на жестком диске
от имени **root** выполните следующую команду:
`OS> df -h`
Убедитесь, что это число больше размера БД.

4.1.1.4.1.3 СОЗДАНИЕ ПАПОК ДЛЯ РЕЗЕРВНОЙ КОПИИ

> **Важно!**
>
> Директории файлов резервной копии должны находиться на компьютере, отличном от того, где расположена БД.

Чтобы создать структуру папок для бэкапа:

1. Войдите в систему от имени пользователя **root.**
2. Создайте директорию для хранения файлов резервной копии:
   `OS> mkdir /opt/IWTM_Backup_Files`
3. Создайте следующие поддиректории:
   ```
   OS> mkdir /opt/IWTM_Backup_Files/Oradata
   OS> mkdir /opt/IWTM_Backup_Files/IWTM
   OS> mkdir /opt/IWTM_Backup_Files/Recovery_Aid
   ```
4. Назначьте права на эти директории для пользователя **Oracle**:
   `OS> chmod 777 /opt/IWTM_Backup_Files/ -R`

4.1.1.4.1.4 СОЗДАНИЕ ВСПОМОГАТЕЛЬНЫХ ФАЙЛОВ НА LINUX

Для обеспечения возможности восстановления из резервной копии, помимо самих файлов данных, вам потребуются вспомогательные файлы: **trace**–файл контрольного файла и копия файла **init.ora**.
Trace–файл контрольного файла содержит имена и пути для всех файлов данных и дополнительных файлов данных, добавленных в БД. Также содержит файлы **redo log** и команды, которые можно использовать для восстановления структуры БД.
Файл **init.ora** содержит инициализационные параметры Oracle, в частности, имена и пути для контрольных файлов базы данных.
Чтобы создать `trace`**-файл для контрольного файла, spfile-файл и скопировать их:**

- На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
- Откройте Oracle SQL*Plus и подключитесь как пользователь **sysdba**:
  `OS> sqlplus / as sysdba`
  Если система была установлена с помощью kickstart, для удобства Вы можете использовать команду **wsqlplus**.

  Примечание:

  Команда `wsqlplus` является алиасом команды `sqlplus`:
  `alias wsqlplus='rlwrap -b "" -f ~/sql.dict sqlplus'`

  Дождитесь подключения – об успешном подключении будет свидетельствовать сообщение **Connected**.
- Скопируйте (или введите) в командную строку и выполните следующий SQL запрос**:**
  `SQL> alter database backup controlfile to trace;`
- Найдите путь к директории, в которой был создан trace-файл, выполнив команду:
  `SQL> show parameter user_dump;`
  В данной директории находятся файлы `trc` и `alert_iwtm.log` (alert_INSTANCE_NAME). В `log`-файле указано имя созданного `trace`-файла.
  Выйдите из Oracle SQL*Plus:
  `SQL> exit`
- Если система была установлена с помощью kickstart и были оставлены параметры по умолчанию, Вы можете проверить последние записи в файле журнала `alert_iwtm.log` с помощью команды:

```
OS> tail -f /u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log
```
Чтобы выйти из режима просмотра, нажмите CTRL+C

- Создайте копию файла параметров **spfile** (**pfile**):
```
OS> sqlplus / as sysdba
SQL> CREATE PFILE from SPFILE;
```
- Найдите путь к директории, в которой был создан `pfile`-файл. Для этого выполните команду:
```
SQL> show parameter PFILE
```
Будет возвращен путь к директории, в которой был создан `pfile` (по умолчанию `/u01/app/oracle/product/db_1/dbs/`).
В этой же директории находится файл initiwtm.ora, для которого нужно также создать резервную копию.
Выйдите из Oracle SQL*Plus:
```
SQL> exit
```
- Скопируйте файлы `trace` и `spfile` на компьютер с резервной копией, в ранее созданную поддиректорию **/opt/IWTM_Backup_Files/Recovery_Aid**.
- Вам нужно скопировать самые актуальные файлы. Чтобы найти файлы с самой поздней датой и временем изменения, выполните:
```
OS> ll
```
- Переименуйте файл так, чтобы впоследствии его можно было легко найти, например:
`controlfilebackupMMDDYY.trc`

4.1.1.4.1.5 СОЗДАНИЕ СПИСКА ФАЙЛОВ, ПОДЛЕЖАЩИХ РЕЗЕРВНОМУ КОПИРОВАНИЮ

Вы можете создать список файлов, подлежащих резервному копированию. Эти списки будут использоваться впоследствии.

- На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
- Откройте Oracle SQL*Plus и подключитесь как пользователь **sysdba**:
OS> sqlplus / as sysdba
Дождитесь подключения – об этом будет свидетельствовать сообщение **Connected**.
- Создайте список директорий и файлов, подлежащих резервному копированию. Это можно сделать с помощью следующих команд SQL:
```
SQL> SELECT file_name FROM dba_data_files UNION SELECT file_name FROM dba_temp_files
UNION SELECT name FROM v$controlfile union select member name from v$logfile;
```
В результате получится список приблизительно следующего вида:
```
/u01/app/oracle/fast_recovery_area/iwtm/control02.ctl
/u01/app/oracle/oradata/iwtm/control01.ctl
/u01/app/oracle/oradata/iwtm/redo01.log
/u01/app/oracle/oradata/iwtm/redo02.log
/u01/app/oracle/oradata/iwtm/redo03.log
/u01/app/oracle/oradata/iwtm/redo04.log
/u01/app/oracle/oradata/iwtm/redo05.log
/u01/app/oracle/oradata/iwtm/redo06.log
/u01/app/oracle/oradata/iwtm/redo07.log
/u01/app/oracle/oradata/iwtm/redo08.log
/u01/app/oracle/oradata/iwtm/redo09.log
/u01/app/oracle/oradata/iwtm/redo10.log
/u01/app/oracle/oradata/iwtm/redo11.log
```

```
/u01/app/oracle/oradata/iwtm/redo12.log
/u01/app/oracle/oradata/iwtm/redo13.log
/u01/app/oracle/oradata/iwtm/sysaux01.dbf
/u01/app/oracle/oradata/iwtm/system01.dbf
/u01/app/oracle/oradata/iwtm/temp01.dbf
/u01/app/oracle/oradata/iwtm/undotbs01.dbf
/u01/app/oracle/oradata/iwtm/users01.dbf
/u02/oradata/IWTM_2012_06_25_1.dbf
/u02/oradata/IWTM_2012_06_26_1.dbf
/u02/oradata/IWTM_2012_06_27_1.dbf
/u02/oradata/IWTM_2012_06_28_1.dbf
/u02/oradata/IWTM_2012_06_29_1.dbf
/u02/oradata/IWTM_2012_06_30_1.dbf
/u02/oradata/IWTM_2012_07_01_1.dbf
/u02/oradata/IWTM_2012_07_02_1.dbf
/u02/oradata/IWTM_2012_07_03_1.dbf
/u02/oradata/IWTM_2012_07_04_1.dbf
/u02/oradata/iwtm_1.dbf
```

- Выйдите из Oracle SQL*Plus:
  `SQL> exit`

4.1.1.4.1.6 ОСТАНОВКА СИСТЕМЫ

Остановка Системы является необязательным шагом, но рекомендуется для выполнения, если на сервере TMFD мало свободного места.

Чтобы остановить систему:

1. На компьютере, где работают процессы TMFD, зайдите в систему от имени пользователя **root**.
2. Остановите все запущенные процессы TMFD:
   `OS> service iwtm stop`
   По окончании процедуры резервного копирования сервисы можно запустить с помощью следующих команд:
   `OS> service iwtm start`

4.1.1.4.1.7 ОСТАНОВКА БД ORACLE

> **Важно!**
>
> Перед началом резервного копирования файлов базы данных обязательно нужно остановить БД ORACLE.

Чтобы остановить БД Oracle:

1. На компьютере, где работает база данных, зайдите в систему от имени пользователя oracle.
2. В командной строке введите:
   `OS> dbshut $ORACLE_HOME`
   По окончании процедуры резервного копирования сервисы можно запустить с помощью

следующей команды:
```
OS> dbstart $ORACLE_HOME
```

4.1.1.4.1.8 КОПИРОВАНИЕ ФАЙЛОВ БД В ХРАНИЛИЩЕ РЕЗЕРВНЫХ КОПИЙ

1. Убедитесь, что все сервисы Oracle остановлены. Если сервисы Oracle не остановлены, файлы резервной копии могут быть повреждены и оказаться непригодными для восстановления.
2. На компьютере, где установлена БД, скопируйте директории (со всем содержимым) с помощью ранее созданного списка директорий.
   Если система была установлена с помощью программы-инсталлятора (**kickstart**) и были оставлены параметры по умолчанию, то пути будут такими:
   скопируйте содержимое директории **/u01/app/oracle/oradata/iwtm/** - в директорию **/opt/IWTM_Backup_Files/IWTM**,
   а директорию **/u02/oradata/** - в директорию **/opt/IWTM_Backup_Files/Oradata**
3. С компьютера, где установлена БД, скопируйте файл **/u01/app/oracle/product/db_1/dbs/orapwiwtm** в директорию **/opt/IWTM_Backup_Files/Recovery_Aid** компьютера, где расположены файлы резервной копии.

4.1.1.4.2 Восстановление базы данных из резервной копии

С учетом причины падения вашей базы данных, выберите подходящую процедуру восстановления БД:

- Если БД была повреждена вследствие сбоя системы или ошибки пользователя, восстановите старую БД. Например, если случайно был удален важный файл, Вы можете восстановить БД до состояния, когда этот файл еще существовал: см. "Восстановление на той же БД".
- Если старая БД не может больше использоваться, создайте новую и восстановите данные на ней: см. "Восстановление на новой БД".

4.1.1.4.2.1 ВОССТАНОВЛЕНИЕ НА ТОЙ ЖЕ БД

Ниже описана процедура восстановления на БД, имеющую ту же структуру каталогов, как и та, с которой была создана резервная копия.

Чтобы восстановить БД с помощью создания новой БД:

1. Убедитесь в работоспособности БД. Проверьте существующую схему БД, сервер БД, где размещена эта схема, и компьютер, на котором работает сервер БД.
2. Установите БД Oracle согласно приведенной инструкции.
3. Выполните следующие шаги:
   a. Удалите все содержимое папок **/u02/oradata/** и **/u01/app/oracle/oradata/iwtm/**
   b. Скопируйте содержимое директории **/opt/IWTM_Backup_Files/Oradata/** в директорию **/u02/oradata/**
   c. Скопируйте содержимое директории **/opt/IWTM_Backup_Files/IWTM/** в директорию **/u01/app/oracle/oradata/iwtm/**
   d. Переименуйте файл **control01.ctl**, расположенный в директории **/opt/IWTM_Backup_Files/Oradata/**, в **control02.ctl** и скопируйте его в директорию **/u01/app/oracle/fast_recovery_area/iwtm/**

e. Проверьте права.

4. При необходимости, измените их:
```
OS> chown oracle:oinstall /u02/oradata –R
OS> chown oracle:oinstall /u01/app/oracle/oradata/iwtm/ -R
OS> chown oracle:oinstall /u01/app/oracle/fast_recovery_area/iwtm/ -R
```
5. Запустите БД
```
OS> dbstart $ORACLE_HOME
```

4.1.1.4.2.2 ВОССТАНОВЛЕНИЕ НА НОВОЙ БД

Если структура каталогов на новой БД отличается от структуры старой БД, выполните следующие шаги:

- В директории **/opt/IWTM_Backup_Files/Recovery_Aid** отредактируйте файл **initiwtm.ora** так, чтобы он соответствовал структуре каталогов новой БД.
- Скопируйте отредактированный файл **initiwtm.ora** в директорию **$ORACLE_HOME/dbs** на компьютер, где расположена новая БД.
- На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
- Откройте Oracle SQL*Plus и подключитесь как пользователь **sysdba**:
```
OS> sqlplus / as sysdba
```
- Сгенерируйте файл параметров
```
SQL> create spfile from pfile;
```
- Если нужно переименовать какие-либо файлы, воспользуйтесь следующим сценарием:
```
OS> sqlplus / as sysdba
SQL> startup mount
SQL> alter database rename file '/<path_to_proddb_files>/<filename1>' to
'/<path_to_clonedb_files>/<filename1>';
…
SQL> alter database rename file '/<path_to_proddb_files>/<filenameN>' to
'/<path_to_clonedb_files>/<filenameN>';
SQL> shutdown immediate
```
Здесь `path_to_proddb_files` – это путь к директории, где размещены файлы новой БД, в которой восстанавливается резервная копия, а `path_to_clonedb_files` - путь к директории, где размещены файлы резервной копии.

4.1.2 Postgre SQL

Чтобы подключиться к серверу БД из терминала сервера TMFD, используйте следующую команду:

```
psql postgre iwtm
```

Для подключения к БД с рабочих станций под управлением Windows, используйте программу pgAdmin.

Информация, необходимая для подключения содержится в конфигурационном файле **/opt/iw/tm5/csw/postgresql/database.conf**.

4.1.2.1 Табличные пространства в базе данных

В базе данных TMFD имеются два типа табличных пространств (ТП):

Тип табличного пространства	Назначение
Основное	Хранение настроек, которые нужны для анализа и обработки объектов (конфигурация, теги, цвета и пр.). Управление системой через Консоль управления (роли, учетные записи пользователей и др.)
Ежедневное	Хранение объектов, перехваченных в течение одних суток. Хранение информации о результатах анализа и обработки объектов. Состоит из двух табличных пространств: для хранения объектов со статусами *Нарушение* и *Нет нарушений*. Таким образом, достигается возможность раздельного архивирования, восстановления и удаления.

Все данные об объектах, перехваченных в определенный день, находятся в одном ежедневном ТП. Ежедневные ТП создаются каждые сутки с таким расчетом, чтобы в базе данных всегда были ТП для работы в ближайшие шесть суток, не включая текущие. Всем ежедневным ТП автоматически присваивается имя <*Schema Owner*>_*X*. Здесь

1. *Schema Owner*– владелец схемы базы данных.
2. *X* – номер ТП (tbs_id из таблицы tbs_list).

Параметры, предназначенные для управления сегментами данных, задаются при настройке схемы базы данных, но могут быть переопределены после создания схемы (см. "Управление ежедневными табличными пространствами").

4.1.2.2 Управление ежедневными табличными пространствами

В этом разделе:

- Архивирование ежедневных табличных пространств
- Восстановление ежедневных табличных пространств
- Настройка размещения файлов в файловой системе
- Удаление ежедневных табличных пространств

4.1.2.2.1 Архивирование ежедневных табличных пространств

Чтобы освободить пространство на жестком диске, Вы можете периодически архивировать устаревшие данные. Архив с данными рекомендуется размещать на внешних носителях информации. При необходимости эти данные могут быть восстановлены.

Важно!

Если в качестве интервала времени используются месяцы или годы, то рекомендуется в

расчете использовать максимальное значение интервала. Для месяца – 31 день. Для года – 366 дней. Например, чтобы архивировать ежедневные ТП старше 4-х лет, в задании <*SchemaOwner*>_iwtm_archive_tablespaces укажите интервал 366*4=1464 дня.

Архивирование может выполняться:

1. Автоматически после истечения указанного периода (см. "Автоматическое архивирование ежедневных табличных пространств");
2. Вручную – для архивирования выбранного ЕТП (см. "Архивирование ежедневных табличных пространств вручную").

4.1.2.2.1.1 АВТОМАТИЧЕСКОЕ АРХИВИРОВАНИЕ ЕЖЕДНЕВНЫХ ТАБЛИЧНЫХ ПРОСТРАНСТВ

Перед тем, как включить автоматическое архивирование, необходимо проверить, что каталог архивирования задан верно:

```
select value
from setting
where setting = 'archive_path'
```

Пользователь postgre должен являться владельцем каталога.

Если каталог установлен неправильно, установите его, выполнив следующую команду:

```
begin;
select sp_setting_set('archive_path', '/test/archive/');
commit;
```

Для автоматического архивирования табличных пространств (по умолчанию функция выключена) Вы можете использовать следующие сценарии (запускаются от имени владельца схемы данных):

1. Для ежедневного табличного пространства, хранящего объекты со статусом *Нарушение*:
   ```
   begin;
   select sp_setting_set('violation_archive_enabled', '1');
   select sp_setting_set('violation_archive_period', 'D');
   commit;
   ```

1 – показатель того, что автоматическое архивирование включено (чтобы выключить, вместо 1 используйте значение 0);
D – количество дней, по истечении которого ежедневное табличное пространство будет архивироваться Системой.

- Для ежедневного табличного пространства, хранящего объекты со статусом *Нет нарушений*:
  ```
  begin;
  select sp_setting_set('noviolation_archive_enabled', '1');
  select sp_setting_set('noviolation_archive_period', 'D');
  commit;
  ```

где:
1 – показатель того, что автоматическое архивирование включено (чтобы выключить, вместо 1 используйте значение 0);

D – количество дней, по истечении которого ежедневное табличное пространство будет архивироваться Системой.

4.1.2.2.1.2 АРХИВИРОВАНИЕ ЕЖЕДНЕВНЫХ ТАБЛИЧНЫХ ПРОСТРАНСТВ ВРУЧНУЮ

Архивирование ЕТП вручную производится в порядке, представленном ниже.

Выборка ежедневных табличных пространств и файлов данных

Список отключаемых табличных пространств можно получить, выполнив запросы к базе данных от имени владельца схемы базы данных. Запросы составляются в соответствии со стратегией архивирования, принятой в вашей организации. Например, для выборки ежедневных ТП, в которых хранятся объекты, перехваченные более 100 дней назад, можно применить следующий запрос:

```
SELECT t.tbs_id, t.tbs_name, t.part_date
FROM tbs_list t
WHERE t.part_date <= date_trunc('day', current_date) - '100 days'::interval  AND t.status IN (0, 3)
```

> **Важно!**
>
> Настоятельно рекомендуется для получения списка файлов использовать запрос, пример которого описывается далее в этом разделе. Это связано с тем, что список файлов данных, полученный другими способами, может оказаться неполным.

Архивное табличное пространство расположено в отдельных каталогах.
Чтобы получить имена этих каталогов, выполните следующий запрос:

```
select s.value || t.tbs_name archive_path
from tbs_list t
inner join setting s on s.setting  = 'archive_path'
where t.part_date <= date_trunc('day', current_date) - '100 days'::interval  and t.status in (0, 3)
```

где `t.status IN (0, 3)` указывает на то, что для архивации выбраны табличные пространства со статусами *Чтение и запись* (код статуса `0`) и *Только чтение* (код статуса `3`).

Отключение ежедневных табличных пространств от базы данных

> **Важно!**
>
> Не отключайте ежедневные ТП во время работы заданий <*SchemaOwner*>_iwtm_add_parts, <*SchemaOwner*>_iwtm_delete_tablespaces, <*SchemaOwner*>_iwtm_archive_tablespaces так как это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:
   `select pkg_part_archive_tablespace(N);`
   где `N` – это значение атрибута `tbs_id` целевого ТП из таблицы `tbs_list`.
   После выполнения этого сценария статус ежедневного ТП изменится на *Отключено от базы данных*.
2. Повторите вызов процедуры для каждого ежедневного ТП, которое нужно отключить.

Перенос файлов данных

Перенесите каталоги с заархивированными табличными пространствами, принадлежащие отключенным ежедневным ТП, на другой носитель информации.
Для получения списка отключенных табличных пространств используйте команду:
`select tbs_name from tbs_list where NOTE = 'Tablespace is offline'`
где `tbs_name` – имя табличного пространства.
`tbs_list` – имя таблицы.
Файлы данных хранятся в каталоге:
`select value from setting where setting = 'archive_path'`

4.1.2.2.2 Восстановление ежедневных табличных пространств

Важно!

Табличное пространство можно восстанавливать только в той схеме базы данных, в которой оно было отключено (даже если эта схема была обновлена). Восстановить табличное пространство после полной переустановки схемы базы данных невозможно.

Перемещение файлов данных

Для восстановления ежедневного ТП необходимо переместить файлы данных этого табличного пространства с внешнего носителя в каталог, путь к которому можно получить, выполнив запрос:

```
select value from setting where setting = 'archive_path'
```

Важно!

Убедитесь, что пользователь *oracle* имеет права на чтение и запись в том каталоге, куда будут перемещаться файлы данных.

Подключение ежедневного табличного пространства

Важно!

Не подключайте ежедневное ТП во время работы заданий <*SchemaOwner*>_iwtm_add_parts, <*SchemaOwner*>_iwtm_delete_tablespaces и <*SchemaOwner*>_iwtm_archive_tablespaces. Это может привести к повреждению данных.

- От имени владельца схемы базы данных вызовите процедуру:
  `select pkg_part_restore_tablespace(N);`
  где `N` – ID табличного пространства (указывается в tbs_list).
  После выполнения процедуры статус ежедневного ТП изменится на *Восстановлено*.
- Повторите вызов процедуры для каждого ежедневного ТП, которое нужно подключить.

4.1.2.2.3 Настройка размещения файлов в файловой системе

Ежедневные табличные пространства могут храниться либо в одном каталоге, либо распределенно, в разных каталогах на разных дисках.
При установке системы с помощью поставляемого инсталлятора задается один путь для ежедневных табличных пространств - `/u01/iwtm_data/`.
Однако при больших нагрузках рекомендуется размещать ежедневные табличные пространства распределенно, на разных файловых системах (LUN-ах, физических дисках) для поочередного их использования. Например, если задано 3 файловых системы, то данные будут размещаться следующим образом:
Первый день – ежедневное табличное пространство создается в файловой системе 1.
Второй день – ежедневное табличное пространство создается в файловой системе 2.
Третий день – ежедневное табличное пространство создается в файловой системе 3.
Четвертый день – ежедневное табличное пространство создается в файловой системе 1.
…

Распределение файлов ежедневных ТП (количество и расположение) можно изменять с помощью следующих сценариев.
Пример сценария, изменяющего количество отдельных мест хранения ежедневных ТП:

```
begin;
select pkg_part_set_df_path_cnt('4');
commit;
```

> **Важно!**
>
> Изменив количество мест хранения ежедневных ТП, обязательно откорректируйте (добавьте/удалите) пути их расположения.

Пример сценария, изменяющего пути для расположения ежедневных ТП:

```
begin;
select pkg_part_set_df_path('/test1/', 1);
select pkg_part_set_df_path('/test2/', 2);
select pkg_part_set_df_path('/test3/', 3);
select pkg_part_set_df_path('/test4/', 4);
commit;
```

> **Примечание:**
>
> Рекомендуется при указании пути в конце указывать символ «/».

Пример сценария просмотра содержимого ежедневных ТП:

```
select a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) || '-' ||
power(10, trunc(log(10, a.binary_size + a.text_size)) + 1) size_range,
count(1) cnt, sum(a.binary_size) binary_size, sum(a.text_size) text_size
```

```
64
from
(
select date_trunc('day', o.capture_date) d, s.display_name code, o.object_id,
coalesce(length(os.source),0)+coalesce(length(os.context),0)+
coalesce(length(o.gui_xml),0)+coalesce(length(o.preview_data),0) binary_size,
coalesce(length(o.text), 0) text_size
from object o
inner join service s on o.service_code = s.service_id and s.language = 'eng'
inner join object_source os on os.object_id = o.object_id
where o.capture_date between to_date('05.05.2014', 'dd.mm.yyyy') and
to_date('14.05.2014', 'dd.mm.yyyy')
) a
group by a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) || '-' ||
  power(10, trunc(log(10, a.binary_size + a.text_size)) + 1)
order by 1, 2, 3
```

Примечание:

Чтобы получить результат анализа размеров перехваченных объектов в табличных пространствах вместе со служебной информацией БД, рекомендуется использовать pgAdmin.

4.1.2.2.4 Удаление ежедневных табличных пространств

Если дальнейшее хранение данных не требуется, то Вы можете воспользоваться процедурой удаления ежедневных ТП (<*SchemaOwner*>_iwtm_delete_tablespaces). Данная процедура позволяет автоматически удалить все данные, хранящиеся в табличном пространстве, сегменты, табличное пространство и файлы данных.

Важно!

1. Удаление табличных пространств – необратимая операция. После выполнения этой операции Вы не сможете восстановить удаленные данные.
2. После удаления табличных пространств, которые отключены от базы данных (имеют статус *Offline*), остаются файлы данных. Чтобы освободить пространство на жестком диске, удалите эти файлы вручную.
3. Процедура <*SchemaOwner*>_iwtm_delete_tablespaces не работает с теми табличными пространствами, которые были отключены/подключены вручную.

В результате выполнения этой процедуры удаляются все ежедневные ТП (и в т.ч. информация о заархивированных ежедневных ТП), которые удовлетворяют следующему условию:

Дата создания табличного пространства меньше или равна разнице между текущей датой и заданным интервалом времени для удаления табличного пространства.

Примечание:

Если заархивированное ежедневное ТП не подлежит восстановлению (т.к. информация о нем была удалена из базы данных), то Вы можете удалить файлы данных этого ежедневного ТП из архива.

На время удаления табличных пространств работа процессов **iw_deliverd**, **iw_loader**, **iw_updater** будет автоматически приостановлена. По завершении процедуры удаления, выполняется автоматический перезапуск процессов. Рекомендуется запускать задание на удаление данных ежедневно. В противном случае количество удаляемых данных увеличится, что приведет к большим временным затратам на выполнение данной процедуры и, как следствие, к увеличению времени простоя сервера TMFD.

Важно!

Если в качестве интервала времени используются месяцы или годы, то рекомендуется в расчете использовать максимальное значение интервала. Для месяца – 31 день. Для года – 366 дней. Например, чтобы удалять ежедневные ТП старше 4-х лет, в задании <*SchemaOwner*>_iwtm_delete_tablespaces укажите интервал 366*4=1464 дня.

Определение интервала времени для удаления ежедневных ТП
Для автоматического удаления табличных пространств (по умолчанию функция выключена) вы можете использовать следующие сценарии (запускаются от имени владельца схемы данных):

- Для ЕТП, хранящего объекты со статусом *Нарушение*:
```
begin;
select sp_setting_set('violation_delete_enabled', '1');
select sp_setting_set('violation_delete_period', 'D');
commit;
```

где:
`1` – показатель того, что автоматическое удаление включено (чтобы выключить, вместо 1 используйте значение 0);
`D` – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

- Для ЕТП, хранящего объекты со статусом *Нет нарушений*:
```
begin;
select sp_setting_set('noviolation_delete_enabled', '1');
select sp_setting_set('noviolation_delete_period', 'D');commit;
```

где:
`1` – показатель того, что автоматическое удаление включено (чтобы выключить, вместо 1 используйте значение 0);
`D` – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

Ручной запуск процедуры

Если вам требуется немедленный запуск процедуры удаления ежедневных ТП (например, из-за нехватки места в файловой системе был изменен интервал удаления, но следующий запуск задания произойдет нескоро), от имени владельца схемы базы данных выполните следующий сценарий:

```
select pkg_part_delete_tablespaces()
```

4.1.2.3 Резервное копирование базы данных

Для снижения рисков потери данных рекомендуется ежемесячно выполнять создание резервной копии (бэкапа) базы данных. Для хранения бэкапов рекомендуется использовать специально выделенные системы хранения.

Для специалистов, не являющихся администраторами Postgre, то есть не располагающих стандартными методами создания резервной копии БД, рекомендуется описанная ниже процедура «холодного бэкапа», выполняемая на остановленной БД. Данная процедура также может применяться для переноса базы данных с одного сервера на другой.

Далее в разделе:

1. Создание резервной копии базы данных*;*
2. Восстановление базы данных из резервной копии.

4.1.2.3.1 Создание резервной копии базы данных

Процедура создания резервной копии (выполнения холодного бэкапа) осуществляется в следующем порядке:

1. Определение размера резервной копии*;*
2. Проверка хранилища резервной копии*;*
3. Создание каталов для резервной копии*;*
4. Остановка системы*;*
5. Остановка Postgre SQL*;*
6. Копирование файлов БД в хранилище резервных копий*.*

4.1.2.3.1.1 ОПРЕДЕЛЕНИЕ РАЗМЕРА РЕЗЕРВНОЙ КОПИИ

Чтобы рассчитать размер будущего архива, необходимо узнать суммарный размер каталога с базой Postgre, каталога основного табличного пространства и ежедневных табличных пространств:

- Войдите в систему от имени пользователя **root**;
- Получите суммарный размер каталогов:
  ```
  du -sx -BM /u01/postgres/ /u01/iwtm_main/ /u01/iwtm_data/
  ```

4.1.2.3.1.2 ПРОВЕРКА ХРАНИЛИЩА РЕЗЕРВНОЙ КОПИИ

Проверьте приемлемость выбранного хранилища резервной копии. Оно должно соответствовать следующим требованиям:

- Размещаться на компьютере, отличном от того, где работает база данных.
- Доступно с компьютеров, где работают сервера и базы данных, подлежащие резервному копированию.
- На жестком диске больше свободного места, чем размер резервной копии:

Чтобы определить количество свободного места на жестком диске

от имени **root** выполните следующую команду:

```
OS>df -h
```

Убедитесь, что это число больше размера БД.

4.1.2.3.1.3 СОЗДАНИЕ КАТАЛОВ ДЛЯ РЕЗЕРВНОЙ КОПИИ

> **Внимание!**
>
> Директории файлов резервной копии должны находиться на компьютере, отличном от того, где расположена БД.

Чтобы создать структуру каталогов для бэкапа:

- Войдите в систему от имени пользователя **root**;
- Создайте директорию для хранения файлов резервной копии:
  ```
  mkdir /opt/IWTM_Backup_Files
  ```
- Создайте следующие поддиректории:
  ```
  mkdir /opt/IWTM_Backup_Files/Pgdata
  mkdir /opt/IWTM_Backup_Files/IWTM_main
  mkdir/opt/IWTM_Backup_Files/IWTM_data
  ```

4.1.2.3.1.4 ОСТАНОВКА СИСТЕМЫ

Остановка системы является необязательным шагом, но рекомендуется для выполнения, если на сервере мало свободного места.

Чтобы остановить систему:

1. На компьютере, где работают процессы PDP, зайдите в систему от имени пользователя **root**.
2. Остановите все запущенные процессы:
   ```
   service iwtm stop
   ```
   По окончании процедуры резервного копирования сервисы можно запустить с помощью следующих команд:
   ```
   service iwtm start
   ```

4.1.2.3.1.5 ОСТАНОВКА POSTGRE SQL

Важно!

Перед началом резервного копирования файлов базы данных обязательно нужно остановить БД Postgre SQL.

Чтобы остановить Postgre SQL БД:

- На компьютере, где работает база данных, зайдите в систему от имени пользователя **root**.
- В командной строке введите:
  ```
  service pgagent-9.4 stop
  service postrgesql-9.4 stop
  ```
  По окончании процедуры резервного копирования сервисы можно запустить с помощью следующей команды:
  ```
  service pgagent-9.4 start
  service postrgesql-9.4 start
  ```

4.1.2.3.1.6 КОПИРОВАНИЕ ФАЙЛОВ БД В ХРАНИЛИЩЕ РЕЗЕРВНЫХ КОПИЙ

- Убедитесь, что все сервисы Postgre SQL остановлены. Если сервисы Postgre SQL не остановлены, файлы резервной копии могут быть повреждены и оказаться непригодными для восстановления.
- На компьютере, где установлена БД, скопируйте директории (со всем содержимым) с помощью ранее созданного списка директорий.
  Если система была установлена с помощью программы-инсталлятора (kickstart) и были оставлены параметры по умолчанию, то пути будут такими:
  скопируйте содержимое директории **/u01/iwtm_main/** и **/u01/iwtm_data/** - в директории **/opt/IWTM_Backup_Files/IWTM_main** и **/opt/IWTM_Backup_Files/IWTM_data** соответственно, а директорию **/u01/postgres/** - в директорию **/opt/IWTM_Backup_Files/Pgdata**

4.1.2.3.2 Восстановление базы данных из резервной копии

С учетом причины падения вашей базы данных, выберите подходящую процедуру восстановления БД:

1. Если БД была повреждена вследствие сбоя системы или ошибки пользователя, восстановите старую БД. Например, если случайно был удален важный файл, Вы можете восстановить БД до состояния, когда этот файл еще существовал (см. "Восстановление на той же базе данных").
2. Если старая БД не может больше использоваться, создайте новую и восстановите данные на ней (см. "Восстановление на новой базе данных").

4.1.2.3.2.1 ВОССТАНОВЛЕНИЕ НА ТОЙ ЖЕ БАЗЕ ДАННЫХ

Ниже описана процедура восстановления на БД, имеющей ту же структуру каталогов, что и та, с которой была создана резервная копия.

Чтобы восстановить базу данных с помощью создания новой базы данных:

- Убедитесь в работоспособности БД. Проверьте существующую схему БД, сервер БД, где размещена эта схема, и компьютер, на котором работает сервер БД;
- Остановите сервисы Postgre SQL:
  `service pgagent-9.4 stopservice postrgesql-9.4 stop`
- Установите БД Postgre SQL согласно приведенной инструкции.
- Выполните следующие шаги:
  Удалите все содержимое каталогов **/u01/iwtm_main/**, **/u01/iwtm_data/** и **/u01/postgres/**
  Скопируйте содержимое директории **/opt/IWTM_Backup_Files/Pgdata** в директорию **/u01/postgres/**
  Скопируйте содержимое директории **/opt/IWTM_Backup_Files/IWTM_main/** в директорию **/u01/iwtm_main/**
  Скопируйте содержимое директории **/opt/IWTM_Backup_Files/IWTM_data/** в директорию **/u01/iwtm_data/**
- Проверьте права.
  При необходимости, измените их:`chown postgres /u01/iwtm_main/ –R`
  `chown postgres /u01/iwtm_data/ –R`
  `chown postgres /u01/postgres/ –R`
- Запустите базу данных:`service postrgesql-9.4 start`
  `service pgagent-9.4 start`

4.1.2.3.2.2 ВОССТАНОВЛЕНИЕ НА НОВОЙ БАЗЕ ДАННЫХ

При восстановлении Postgre SQL, необходимо копировать файлы БД в те же каталоги, в которых они были сохранены.

Чтобы восстановить БД, скопируйте каталоги, проверьте права и запустите сервисы БД (см. "Восстановление на той же базе данных").

4.2 Администрирование серверной части TMFD

В этой главе:

- Процессы TMFD Server*;*
- Настройка конфигурационных файлов TMFD Server*;*
- Настройка использования OCR*;*
- Настройка параметров обработки архивов вложений*;*
- Архивирование каталога очереди сообщений*;*
- Логирование работы Системы*;*
- Перемещение объектов между очередями (утилита iw_qtool)*;*
- Загрузка очередей объектов*;*

- Восстановление работоспособности системы в аварийных ситуациях.
- Настройка serman.conf при изменении адреса сервера БД
- Настройка передачи информации в SIEM
- Удаление временных файлов

4.2.1 Процессы TMFD Server

В этом разделе:

- Список процессов TMFD Server;
- Работа с процессами TMFD Server.

4.2.1.1 Список процессов TMFD Server

Работа Системы осуществляется посредством процессов: один и тот же процесс может быть запущен единовременно в нескольких экземплярах.

Имя процесса	**Описание процесса**	**Конфигурационный файл**
iw_adlibitum	Управляет процессами получения актуальных данных с сервера Active Directory.	/opt/iw/tm5/etc/adlibitum.conf
iw_agent	Требуется для управления конфигурацией Системы.	/opt/iw/tm5/etc/agent.conf
iw_agent_kicker	Вспомогательный процесс для модуля iw_agent.	/opt/iw/tm5/etc/agent_kicker.conf
iw_analysis	Забирает объекты из файловой очереди, в которую их кладет **iw_xapi**. По очереди отправляет на обработку процессами **iw_warpd**, **iw_cas**, **iw_pas**, **iw_luaengined**. Далее объекты складываются в файловую очередь для отправки в базу данных.	/opt/iw/tm5/etc/analysis.conf
iw_blackboard	Осуществляет взаимодействие применяемых политик и базы данных	/opt/iw/tm5/etc/blackboard.conf
iw_blackboard_kicker	Вспомогательный процесс для iw_blackboard	/opt/iw/tm5/etc/blackboard_kicker.conf
iw_bookworm	Выполняет роль справочника в Системе	/opt/iw/tm5/etc/bookworm.conf
iw_capstack	Выполняет обработку трафика, передаваемого по протоколам POP3 и IMAP	/opt/iw/tm5/etc/capstack.conf
iw_cas	Выполняет роль сервера контентного анализа. Процесс **iw_cas** принимает от подсистем перехвата текстовые запросы в формате plain-text для проведения контентного анализа. По окончании контентного анализа возвращает результат запроса подсистеме анализа и принятия решения.	/opt/iw/tm5/etc/cas.conf

iw_config_compiler	Переводит конфигурационный файл сервера контентного анализа в бинарный вид для возможности использования конфигурации в контентном анализе	/opt/iw/tm5/etc/config_compiler.conf
iw_deliver	Выполняет доставку писем. Отправляет SMTP-письма получателям в случае, если доставка письма разрешена из Management Console (только в нормальном и прозрачном транспортных режимах). Также этот процесс доставляет SMTP-письма, которые по той или иной причине (например, ввиду отсутствия связи с почтовым relay-сервером или почтовым клиентом) не смог доставить процесс **iw_messed**.	/opt/iw/tm5/etc/deliver.conf
iw_indexer	Служит для индексации текста объектов из БД. Получает доступ к базе данных для ее индексации и складывает индексы в файловое хранилище. При выполнении поискового запроса **sphinx** получает из файлового хранилища индексов id объектов.	/opt/iw/tm5/etc/indexer.conf
iw_licensed	Подсистема лицензирования. Производит мониторинг и обработку установленных в Системе лицензий.	/opt/iw/tm5/etc/licensed.conf
iw_luaengined	Процесс, обеспечивающий выполнение LUA-скрипта согласно действующей политике	/opt/iw/tm5/etc/luaengined.conf
iw_messed	Процесс обработки SMTP-писем. Извлекает данные из SMTP-, POP3- и IMAP-объектов. Затем извлеченные данные добавляются в полученный XML-контекст. Готовый XML-контекст, содержащий данные конверта и письма, передается подсистеме анализа и принятия решения для проверки. По окончании анализа **iw_messed** передает SMTP-письма, доставка которых разрешена, компоненту почтовой системы, ответственному за доставку почты (только в нормальном и прозрачном транспортном режиме). В случае интеграции с почтовым сервером Postfix, таким компонентом является Postfix. Если интеграция с Postfix отсутствует, то, в зависимости от настроек вашей почтовой системы, таким компонентом может быть корпоративный почтовый сервер или почтовый клиент. Кроме того, копия проверенного SMTP-письма передается процессу **iw_loader** для сохранения в базу данных.	/opt/iw/tm5/etc/messed.conf
iw_notifier_kicker	Вспомогательный процесс для отправки уведомлений из Системы.	/opt/iw/tm5/etc/notifier_kicker.conf
iw_pas	Получает результаты анализа **iw_cas**. Определяет наличие объекта защиты и добавляет объекту соответствующие атрибуты.	/opt/iw/tm5/etc/pas.conf

iw_proxy	Принимает копию трафика и передает ее модулю iw_messed, разбив на http-, icq- и smtp-трафик. Включает следующие процессы: 1. iw_proxy_http - процесс, принимающий копию HTTP-трафика. Принимает HTTP-запрос, формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа и принятия решения. По окончании анализа копия объекта передается процессу **iw_loader** для укладки в базу данных. 2. iw_proxy_icq - процесс, принимающий копию ICQ-трафика. Принимает ICQ-сообщение, формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа и принятия решения. По окончании анализа копия объекта передается процессу **iw_loader** для укладки в базу данных 3. iw_proxy_smtp - процесс, принимающий копию SMTP-трафика. Принимает SMTP-письмо, формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа и принятия решения. По окончании анализа копия объекта передается процессу **iw_loader** для укладки в базу данных.	/opt/iw/tm5/etc/proxy.conf
iw_qmover_client	Работает на TMFD Server, установленном в филиале. Отправляет перехваченные объекты в базу данных центрального офиса. Путь к файлу: /opt/iw/tm5/etc/qmover_client.conf	
iw_qmover_server	Работает на TMFD Server, установленном в центральном офисе. Принимает объекты, полученные от клиента, установленного в филиале. Передает объекты процессу **iw_loader** для сохранения в базу данных.	/opt/iw/tm5/etc/qmover_server.conf
iw_report_kicker	Вспомогательный процесс для создания отчетов.	/opt/iw/tm5/etc/report_kicker.conf
iw_sample_compiler	Процесс, создающий цифровые отпечатки из загруженных эталонных файлов	/opt/iw/tm5/etc/sample_compiler.conf
iw_selection_kicker	Вспомогательный процесс для работы с фильтрами (запросами).	/opt/iw/tm5/etc/selection_kicker.conf
iw_serman	Регистрирует и хранит регистрационную информацию сервисов, взаимодействующих с интерфейсом пользователя.	/opt/iw/tm5/etc/serman.conf

iw_sniffer	Процесс, перехватывающий трафик, который передается по протоколам SMTP, HTTP, ICQ, POP3 и IMAP.	/opt/iw/tm5/etc/sniffer.conf
iw_system_check	Процесс, занимающийся сбором данных от службы Nagios и предоставляющий полученные данные для выведения в Консоли управления.	/opt/iw/tm5/etc/system_check.conf
iw_updater	Процесс, загружающий конфигурацию из базы данных на TMFD Server.	/opt/iw/tm5/etc/updater.conf
iw_warpd	Управляет процессами извлечения данных из контейнеров, вложенных в перехваченные объекты.	/opt/iw/tm5/etc/warpd.conf
iw_whiteboard	Позволяет серверным процессам публиковать сообщения в интерфейсе пользователя.	/opt/iw/tm5/etc/whiteboard.conf
iw_xml2liro	Процесс, преобразовывающий xml-контекст, полученный из трафика, в бинарный формат liro.	/opt/iw/tm5/etc/xml2liro.conf

4.2.1.2 Работа с процессами TMFD Server

Все процессы TMFD Server (за исключением **iw_warpd**) запускаются от имени пользователя **iwtm**. Процесс **iw_warpd** запускается от имени пользователя **root**.

Пользователи создаются в процессе установки TMFD Server автоматически.

Примечание:

Имя пользователя прописывается в конфигурационных файлах процессов в параметре `User` секции `Permissions`.

Для стабильной работы Системы рекомендуется оставить значение этого параметра без изменений.

Во время работы состояние процессов TMFD Server проверяется сценарием **pguard**, который в ходе установки создается в директории `/opt/iw/tm5/bin`. Если по какой-либо причине один или несколько процессов TMFD Server были остановлены, сценарий **pguard** перезапускает эти процессы.
Управление работой процессов TMFD Server выполняется при помощи **iwtm**, находящегося в каталоге `/etc/rc.d/init.d`. Файл **iwtm** является сценарием автозапуска для уровней запуска (runlevel) 2, 3, 4, 5.

Примечание:

1. Для перехвата копии трафика через Sniffer (ICQ- HTTP-, SMTP-трафик) запускаются отдельные процессы **iw_proxy**.
2. Процессы **iw_qmover_server, iw_qmover_client** доступны, но для них по умолчанию выключен автозапуск. Каждый процесс запускается на соответствующей стороне (в

филиалах **iw_qmover_client,** в центральном офисе **iw_qmover_server**).

Ключи запуска для сценария **iwtm**:

Ключ запуска	**Назначение**
start	запуск процессов
stop	остановка процессов
restart	перезапуск процессов
reload	перезагрузка конфигурации
status	вывод на экран информации о состоянии процессов

Примеры команд

Действие	**Команда**
Перезапустить сервер контентного анализа	`service iwtm restart cas`
Проверить состояние процессов TMFD Server	`service iwtm status`
Проверить состояние сервера контентного анализа	`service iwtm status cas`

Важно!

В каталоге `/opt/iw/tm5/run` хранятся PID-файлы. При аварийном завершении работы необходимо перед запуском процессов стереть все PID-файлы.

Изменение параметров автозапуска процессов

Для каждого процесса, управляемого сценарием **iwtm** можно задать параметры автозапуска в конфигурационном файле.

Чтобы включить/отключить автозапуск процесса (пример приведен для службы iw_sniffer):

- Для корректной смены параметров остановите серверные процессы TMFD:
  `service iwtm stop`
- В файле `/opt/iw/tm5/etc/sniffer.conf`, выполните настройки:
  - Чтобы включить автозапуск для процесса, установите в блоке процесса:
    `"Startup" : {"Enabled" : true}`
  - Чтобы отключить автозапуск для процесса, установите в блоке процесса:
    `"Startup" : {"Enabled" : false}`
- Запустите процессы TMFD:
  `service iwtm start`

4.2.2 Настройка конфигурационных файлов TMFD Server

В данном разделе описаны настройки конфигурационных файлов Системы, которые вы можете изменять для отражения специфики работы Системы в вашей инфраструктуре. Файлы, не описанные в данном подразделе, изменять не рекомендуется.

Расположение конфигурационных файлов: `/opt/iw/tm5/etc`.

Названия конфигурационных файлов соответствуют названиям тех компонентов, для настройки которых они используются. Например, для конфигурирования компонента **iw_loader** используется конфигурационный файл **loader.conf**.

4.2.2.1 Общие настраиваемые параметры конфигурационных файлов

Для конфигурирования работы Системы используются файлы формата JSON. В разделе описаны наиболее используемые секции и параметры.

> **Важно!**
>
> Настоятельно не рекомендуется изменять параметры, описание которых в настоящем документе не приведено.

Общие настраиваемые параметры содержатся в следующих секциях конфигурационных файлов:

- Секция Logging;
- Секция Startup;
- Секция Nookdir.

4.2.2.1.1 Секция Logging

Параметр	Описание процесса и путь к файлу
`ActiveBackends`	Настройка вывода лог-файлов. Возможные варианты: 1. `Console` - вывод в консоль (если процесс запущен не как демон, иначе логи будут сохраняться в директорию `/dev/null`) 2. `Syslog` - вывод в системный лог (`/var/log/messages`) 3. `File` - вывод в отдельный файл (директория для создания файла указана в параметре `DefaultDirectory`) 4. `Whiteboard` - вывод логов в компонент **iw_whiteboard** (для последующей передачи информации в веб-консоль)
`DefaultDirectory`	Директория, содержащая лог-файлы
`Descriptions`	Описание формата для каждого типа логирования и специфичных настроек

`GlobalLevel`	Глобальный уровень логирования. Рекомендуемое значение при внедрении – *error*. Такая настройка позволит записывать в лог только сообщения уровня *error* и выше (*critical*). Значение по умолчанию - *warning*
`DisableLogging`	Возможность полного отключения логирования в компоненте

4.2.2.1.2 Секция Startup

В секции `Startup` включается (значение `true`) и выключается (значение `false`) автозапуск модуля.

Важно!

Для службы `iw_proxy` включение и выключение компонентов выполняется следующим образом:
`"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}`
– включение всех модулей;
`"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}`
– включение модуля **iw_proxy_http**;
`"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}`
– выключение всех модулей.

4.2.2.1.3 Секция Nookdir

В секции `Nookdir` указывается рабочий каталог модуля. По умолчанию – `/opt/iw/tm5`.

4.2.2.2 Специфичные настраиваемые параметры конфигурационных файлов

Для конфигурирования работы Системы используются файлы формата JSON.

Важно!

Настоятельно не рекомендуется изменять параметры, описание которых в настоящем документе не приведено.

В разделе описаны наиболее используемые секции и параметры следующих конфигурационных файлов:

- Конфигурационный файл serman_resolver.conf;
- Конфигурационный файл sniffer.conf;
- Конфигурационный файл proxy.conf;
- Конфигурационный файл oracle.conf;
- Конфигурационный файл cas.conf;
- Конфигурационный файл capstack.conf;

- Конфигурационный файл indexer.conf;
- Конфигурационный файл web.conf.

4.2.2.2.1 Конфигурационный файл serman_resolver.conf

В файле хранятся вспомогательные данные для работы модуля **iw_serman**: регистрационные данные компонентов, которые могут быть запрошены другими зарегистрированными сервисами.

Параметр	**Описание**
`Host`	IP-адрес, на котором работает служба **iw_serman**
`Password`	Пароль пользователя. Используется для подключения к Serman
`Port`	Порт для подключения к Serman
`Username`	Имя пользователя. Используется для подключения к Serman

4.2.2.2.2 Конфигурационный файл sniffer.conf

Если веб-консоль управления TMFD и компонент Sniffer установлены на одном компьютере, необходимо внести следующий фрагмент кода в секцию `Listenareas`, параметр `http`, подпараметр `Rules`:

```
{
 "HiPort": 80,
 "IP": "[Server_IP]",
 "LoPort": 80,
 "Mask": "0.0.0.0",
 "Policy": "DROP"
 }
```

где `[Server_IP]` – IP-адрес сервера, на котором установлена служба sniffer.

4.2.2.2.3 Конфигурационный файл proxy.conf

Конфигурационный файл **proxy.conf** содержит следующие секции, которые описывают обработку копий различного объектов, полученных от Sniffer:

1. Секция Http;
2. Секция Icq;
3. Секция Smtp.

4.2.2.2.3.1 СЕКЦИЯ HTTP

В секции `Http` заданы параметры, необходимые для обработки HTTP-запросов, а также ICQ-сообщений (при перехвате ICQ поверх HTTP), полученных от Sniffer:

Параметр	**Описание**

AuthContext	Отключает сохранение в очередь HTTP-запросов без аутентификации. Возможные значения: • 0 – производится сохранение запросов без аутентификации; • 1 – не сохраняются запросы с ответом прокси-сервера "*407*", • 2 – не сохраняются запросы с NTLM Type 1, либо без заголовка *Proxy-Authorization.* При этом значении значение параметра SkipNegotiate не имеет значения: Система работает так, как если бы он имел значение On. Значение по умолчанию 0
CharsetDetection	Метод определения кодировки текста. Значение по умолчанию 0. При этом кодировка определяется обычным методом. После извлечения в контекст, тексты некоторых POST-запросов могут отображаться некорректно. Для исправления проблемы можно установить значение 1
DataPoolSize	Максимальный объем выделенной памяти для обработки соединений, в Мб. Значение по умолчанию 1024
DecodeHttpContent	Включение распаковки содержимого запроса в случае наличия заголовка Content-Encoding со значением gzip, deflate или compress. Значение по умолчанию true
DefaultCodepage	Кодировка входящего ICQ-трафика. Значение по умолчанию cp1251
DialogBytesCount	Размер диалога (в байтах), по достижении которого ICQ-диалог (при перехвате ICQ поверх HTTP) сохраняется в файловую очередь. Значение по умолчанию 500
DialogTimeout	Временной интервал (в минутах), по истечении которого с момента перехвата последнего сообщения происходит сохранение ICQ-диалога (при перехвате ICQ поверх HTTP) в файловую очередь. Значение по умолчанию 5
ExtractHttpEntity	Включение процедуры извлечения текста из кодированного содержимого запроса с помощью внешних распаковщиков. Эта процедура применяется при сбоях внутренней процедуры декодирования с использованием zlib. Значение по умолчанию false
FakeFileTransferPort	Порт, с помощью перенаправления на который блокируются попытки передачи файлов. Значение по умолчанию 62225
FormatXmlContext	Форматирование XML. Используется для отладки. Значение по умолчанию false
HttpDumpPath	Путь к файлу дампа для HTTP-трафика.
IcqDumpPath	Путь к файлу дампа для ICQ-трафика.
IcqFilter	Возможность перехвата ICQ-сообщений (если установлено значение true), передаваемых через прокси-сервер (поверх HTTP). По умолчанию возможность включена
IcqIgnoreHosts	Отключение перехвата ICQ-сессий определенных хостов.
IcqKnownServers	Диапазоны IP для ICQ серверов при перехвате ICQ поверх HTTP. Несколько диапазонов перечисляются через запятую, например: "205.188.251.0/24:443, 64.12.30.0/24:443, 205.188.8.8:443"

IcqSessionTimeOut	Время неактивности ICQ-сессии, после которого перехват трафика прекращается в секундах. Значение по умолчанию 10800
LogAuth	Запись в лог информации о привязке логина пользователя к его POST-запросам. Значение по умолчанию false
LogBlock	Запись в системный журнал сообщений о блокировке перехваченных HTTP-запросов. Запись ведется, если установлено значение true. По умолчанию запись отключена – значение false
MaxMemoryBlock	Максимальный объем данных POST-запроса (в килобайтах), которые могут храниться в оперативной памяти. Блоки большего размера будут выгружаться во временные файлы. Значение по умолчанию 4096 Кб
MessageWindow	Количество сообщений диалога, по достижении которого ICQ-диалог (при перехвате ICQ поверх HTTP) сохраняется в файловую очередь. Значение по умолчанию 10
MinHeader	Минимальный объем текста (в байтах) для одного блока переменной в кодировке URL, который будет передан на сервер контентного анализа. Значение по умолчанию 10.
MinText	Минимальный размер текстового блока для отправки в iw_cas. Значение по умолчанию 0
OCR	Использование технологии OCR. Значение по умолчанию false
OnlyPost	Перехват только POST-запросов. Значение по умолчанию true
SetCp1251	Использование кодовой таблицы windows-1251 вместо mac-cyrillic при автоматическом определении кодировки текста в HTTP-запросе. Значение по умолчанию false. Если в вашей организации применяется программное обеспечение, использующее кодировку windows-1251, то рекомендуется включить этот параметр (значение true). Автоматическое определение кодовой таблицы в ряде случаев может происходить некорректно. В частности, при недостаточно большом объеме русскоязычного текста возможен выбор кодировки mac-cyrillic вместо windows-1251
SkipNegotiate	Отключает сохранение в очередь HTTP-запросов с NTLM Type 1 (необходимо для исключения дубликатов запросов). Значение по умолчанию false. При реализации схемы внедрения, когда перехват копии HTTP-трафика выполняется через Sniffer, должен принимать значение false.
SkipStat4XX	Отключает сохранение в очередь HTTP-запросов с ответом прокси-сервера вида "*4XX*", где *XX* – любые цифры. Значение по умолчанию false.
StatusCheck	Установка состояния доставки HTTP-запроса в зависимости от статус-кода, возвращенного веб- или прокси-сервером. Если установлено значение true, то анализ кода выполняется, что позволяет более точно показывать состояние доставки HTTP-запроса. Значение по умолчанию false
UnsafeMode	Режим, в котором при возникновении ошибки перехвата, работа процесса останавливается и создается дамп файл. Значение по умолчанию false
WCGAuthCache	Признак того, включена ли функция кэширования авторизационной информации, необходимая для интеграции с WebSense WSG. Чтобы включить кэширование, установите значение true. Значение по умолчанию false

WCGAuthTTL	Время кэширования авторизационной информации, если включен параметр WCGAuthCache, в секундах. Значение по умолчанию 900
ZimbraMail	Перехват почты Zimbra. Значение по умолчанию false

4.2.2.2.3.2 СЕКЦИЯ ICQ

В секции Icq заданы параметры, необходимые для обработки копий ICQ-сообщений, полученных от Sniffer:

Параметр	Описание
DefaultCodepage	Кодировка входящего ICQ-трафика. Значение по умолчанию cp1251
DialogBytesCount	Размер диалога (в байтах), по достижении которого ICQ-диалог сохраняется в файловую очередь. Значение по умолчанию 500
DialogTimeout	Интервал времени (в минутах), по истечению которого с момента перехвата последнего ICQ-сообщения необходимо сохранить диалог в файловую очередь. Значение по умолчанию 5
FakeFileTransferPort	Порт, с помощью перенаправления на который блокируются попытки передачи файлов. Значение по умолчанию 62225
FormatXmlContext	Форматирование XML. Используется для отладки. Значение по умолчанию false
MessageWindow	Количество сообщений диалога, по достижении которого ICQ-диалог сохраняется в файловую очередь. Значение по умолчанию 10
OCR	Использование технологии OCR. Значение по умолчанию false

4.2.2.2.3.3 СЕКЦИЯ SMTP

В секции Smtp задаются параметры, необходимые для обработки SMTP-сообщений, полученных от Sniffer:

Параметр	Описание
DumpMode	Регулирует количество данных, которое попадает в дамп. Значение по умолчанию false
DumpPath	Путь к файлу дампа. Значение по умолчанию dump.smtp
FormatXmlContext	Форматирование XML. Используется для отладки. Значение по умолчанию false
MaxMsgSize	Размер SMTP-сообщения (в байтах), при превышении которого сообщение не обрабатывается Системой. Значение по умолчанию – 52428800.
ReadBufferSize	Размер данных, получаемых от Sniffer за один раз. Значение по умолчанию 32768

4.2.2.2.4 Конфигурационный файл oracle.conf

Параметры соединения с сервером базы данных:

Параметр	Описание
ConnString	Строка соединения с сервером базы данных (псевдоним сервера из файла **tnsnames.ora**)
NLS_LANG	Кодировка, определяющая локализацию БД
ORACLE_HOME	Значение переменной окружения ORACLE_HOME
Password	Пароль учетной записи пользователя Linux части
Username	Имя учетной записи пользователя Linux части

4.2.2.2.5 Конфигурационный файл cas.conf

Конфигурационный файл **cas.conf** содержит следующие секции, описывающие настройки подсистемы контентного анализа:

- Секция Analysis;
- Секция Classifier;
- Секция Tableanalysis;
- Секция Thrift.

4.2.2.2.5.1 СЕКЦИЯ ANALYSIS

Включение (значение on) и выключение (значение off) технологии анализа

Параметр	Описание
TableAnalysis	Детектор выгрузок из БД

4.2.2.2.5.2 СЕКЦИЯ TABLEANALYSIS

Параметр	Описание
MinWords	Минимальное количество слов в файле эталонной выгрузки из БД, достаточное для детектирования эталонной выгрузки. В данное количество входят все названия полей и все содержащиеся в таблице данные. Требуется, чтобы слова были отделены друг от друга пробелом или иным отступом. **Например:** WinWords = 10. Будет работать – пустая таблица с 11 столбцами, в названии которых есть хотя бы одно слово; не будет работать – таблица, в которой 2 столбца с названиями из 2 слов для каждого и 1 строка, в каждой из ячеек которой по 1 слову. Значение по умолчанию – 10

4.2.2.2.5.3 СЕКЦИЯ THRIFT

Параметр	Описание
ServerPort	Порт, на котором сервер контентного анализа принимает входящие соединения. Значение по умолчанию – 9992

4.2.2.2.6 Конфигурационный файл messed.conf

Параметр	Описание
HeloDomain	Значение команды HELLO SMTP-диалога. Значение по умолчанию smtp.company.com
OCR	Значение по умолчанию – false
Relay	Полное доменное имя почтового relay-сервера, которому перенаправляется письмо, используется для идентификации внутри почтового протокола. Задается при установке.
RelayPort	Порт почтового relay-сервера, которому перенаправляется письмо. Задается при установке.
Timeout	Время, в течение которого предпринимаются попытки доставки SMTP-писем, в секундах. По истечении указанного времени письмо передается в базу данных. Значение по умолчанию 1200
WorkerThreads	Максимальное количество потоков для параллельного выполнения процесса **iw_messed**. Значение по умолчанию 8. Увеличение числа потоков повысит производительность процесса, но увеличит использование памяти

4.2.2.2.7 Конфигурационный файл capstack.conf

Конфигурационный файл **capstack.conf** описан в следующих разделах:

1. Секция UsedProcessors;
2. Секция UsedSources.

4.2.2.2.7.1 СЕКЦИЯ USEDPROCESSORS

В секции UsedProcesses задаются протоколы, которые будет разбирать **iw_capstack**. Процесс разбирает протокол и преобразовывает его в расширение. Далее трафик передается процессу **iw_messed** (см. "Конфигурационный файл messed.conf").

Параметр	Описание
imap4	Разбор imap4. Возможные значения: true, false. Значение по умолчанию: true
nrpc	Разбор nrpc. Возможные значения: true, false. Значение по умолчанию: false
pop3	Разбор pop3. Возможные значения: true, false. Значение по умолчанию: true

4.2.2.2.7.2 СЕКЦИЯ USEDSOURCES

В секции UsedSources задаются параметры источника данных для **iw_capstack**.

Параметр	Описание
iscp	Использование в качестве получения трафика от компонента **iw_sniffer**. Значение по умолчанию: true. Возможные значения true, false

4.2.2.2.8 Конфигурационный файл indexer.conf

В файле хранится конфигурация модуля индексации. Параметры индексации применяются к модулю **iw_indexer**.В секции `Indexer` заданы параметры работы модуля с Базой Данных и методы индексации:

Параметр	**Описание**
`ArchiveDir`	Путь к каталогу архивированных индексов. Значение по умолчанию: `sphinx_archive`
`BuildIndexByContent`	Расширенная индексация. Возможные значения: `true, false`. Значение по умолчанию: true
`FetchSize`	Количество объектов, запрашиваемых службой из БД для последующей индексации. Значение по умолчанию: `100`
`IndexExactWords`	Точное совпадение. Возможные значения: `true, false`. Значение по умолчанию: `false`
`ProcessSizeInBytes`	Максимальный размер объектов в цикл индексации. Значение по умолчанию: `67108864`
`TarPath`	Путь к утилите архивации. Значение по умолчанию: /bin/tar
`WaitTimeInSects`	Время ожидания между попытками получить объекты из БД

4.2.2.2.9 Конфигурационный файл web.conf

В файле хранятся параметры взаимодействия Консоли управления с другими компонентами системы. В секции `Search` заданы параметры взаимодействия Консоли управления с сервисом полнотекстового поиска:

Параметр	**Описание**
`driver`	Название движка полнотекстового поиска. Значение по умолчанию: `sphinx`
`hostname`	Адрес сервера с БД. Значение в случае использования типа установки All-in-one: `127.0.0.1`
`max_matches_common`	Максимальное количество возвращаемых результатов при первичном запросе. Значение по умолчанию: `100000`
`max_matches_maximum`	Максимальное количество возвращаемых результатов при вторичном запросе. Значение по умолчанию: `10000000`
`page_size`	Количество результатов, возвращаемых при однократном обращении к службе **sphinx**: `10000`
`port`	Порт, через который Консоль управления подсоединяется к службе sphinx. Значение по умолчанию: `9306`

4.2.2.2.10 The analysis.conf configuration file

Файл содержит вспомогательную информацию для модуля **iw_analysis**. Конфигурационный файл **analysis.conf** содержит следующие секции:

- Секция Analysis;
- Секция Bookworm.

4.2.2.2.10.1 СЕКЦИЯ ANALYSIS

Параметр	**Описание**
`CharsetDetection`	Метод определения кодировки текста. Значение по умолчанию `0`. При этом кодировка определяется обычным методом. После извлечения в контекст, тексты некоторых POST-запросов могут отображаться некорректно. Для исправления проблемы можно установить значение 1
`DecodeHttpContent`	Включение распаковки содержимого запроса в случае наличия заголовка Content-Encoding со значением gzip, deflate или compress. Значение по умолчанию `true`
`ExtractHttpEntity`	Включение процедуры извлечения текста из кодированного содержимого запроса с помощью внешних распаковщиков. Эта процедура применяется при сбоях внутренней процедуры декодирования с использованием zlib. Значение по умолчанию `false`
`MaxMemoryBlock`	Максимальный объем данных POST-запроса (в килобайтах), которые могут храниться в оперативной памяти. Блоки большего размера будут выгружаться во временные файлы. Значение по умолчанию `4096` Кб
`MaxReadBuf`	Ограничение для размера буфера. Значение по умолчанию 131072.
`MinHeader`	Минимальный объем текста (в байтах) для одного блока переменной в кодировке URL, который будет передан на сервер контентного анализа. Значение по умолчанию `10`.
`MinText`	Минимальный объем текста (в байтах), для которого будет проводиться контентный анализ. Значение по умолчанию `0` байт. Настройка данного параметра позволяет снизить нагрузку на сервер контентного анализа. Это может быть достигнуто путем отказа от контентного анализа текста, размер которого настолько мал, что не позволяет передавать значимые сообщения
`OnlyPost`	Перехват только POST-запросов. Значение по умолчанию `true`
`ZimbraMail`	Перехват почты Zimbra. Значение по умолчанию `false`
`OCR`	Включение OCR. Значение по умолчанию `false`
`TempDir`	Директория для хранения временных файлов. Значение по умолчанию tmp
`WorkThreads`	Количество обрабатывающих потоков. Значение по умолчанию 12

4.2.2.2.10.2 СЕКЦИЯ BOOKWORM

Параметр	**Описание**

ConnectTryCount	Количество попыток соединения. Значение по умолчанию 5
CacheDuration	Время валидности справочных данных, которые возвращает **iw_bookworm**. Значение по умолчанию 15

4.2.2.2.11 Конфигурационный файл sample_compiler.conf

Секция/Параметр	**Описание**
Bookworm	Секция определяет параметры работы с процессом **iw_bookworm**
DebugBreak	Отладочный параметр. Значение по умолчанию false
EnableOCR	Включение использования OCR. Значение по умолчанию false
Logging	см. статью "Секция Logging"
NookDir	см. статью "Секция Nookdir"
OutChunckSizeLimit	Максимальный размер чанка, в который возаращаются результаты компиляции. Значение по умолчанию 1048576
ResourceLimits	Различные ограничения системных ресурсов, которые может использовать программа
Stratup	см. статью "Секция Startup"
Technologies	Секция конфигурирования отдельных технологий
ThreadsCount	Количество потоков обработки. Значение по умолчанию 5
ThriftServers	Настройки трифт-сервера, через который **sample_compiler** получает задачи на компиляцию данных

4.2.2.2.12 Конфигурационный файл serman.conf

4.2.2.2.12.1 СЕКЦИЯ SERMAN

4.2.3 Настройка использования OCR

Настройка OCR производится в следующих конфигурационных файлах:

- **messed.conf** – требуется указать значение true параметру OCR, если нужно включить использование OCR для писем, проходящих через почтовый relay-сервер (см. "Конфигурационный файл messed.conf").
- **warpd.conf –** в секции Warp требуется указать параметру EnableOCR значение true.
- **proxy.conf –** в секции Http или Icq требуется указать параметру OCR значение true (см. "Конфигурационный файл proxy.conf")

4.2.4 Настройка параметров обработки архивов вложений

Обработка вложений настраивается в двух конфигурационных файлах: **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml** и **/opt/iw/tm5/etc/extractors.conf**.

В этом разделе:

1. *Конфигурационный файл extractors.conf*;

2. *Конфигурационный файл extractors.xml*.

4.2.4.1 Конфигурационный файл extractors.conf

Файл **/opt/iw/tm5/etc/extractors.conf** содержит локальные настройки экстракторов.

Параметр	**Описание и примеры настройки**
`Dreamcatcher`	Директория, в которой хранятся файлы, которые не удалось распаковать
`MaxRecursiveLevel`	Максимальный уровень вложенности файлов. Значение по умолчанию – `100`
`TempDir`	Временная директория для результатов распаковки. Значение по умолчанию – `tmp`

4.2.4.2 Конфигурационный файл extractors.xml

Файл **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml** содержит настройки справочника и базу сигнатур, с помощью которых определяется тип файлов при распаковке архивов и вложений.

Параметр	**Описание и примеры настройки**
`FilenameCharsets`	Если кодировка имени файла отличается от стандартной (ANSI, UTF), то файл будет обрабатываться как соответствующий кодировкам, указанным в данном параметре. Несколько значений перечисляются через запятую; Система будет последовательно пытаться обработать файл в перечисленных кодировках, пока не найдет похожую. Значения по умолчанию – `UTF-8,cp1251,cp866`
`MinFileSizeInBytes`	Минимальный размер файла (в байтах), подлежащего распаковке. Это ограничение позволяет увеличить производительность Системы, за счет отказа от распаковки небольших файлов. Значение по умолчанию – `10`
`MaxTextPlainSizeInKb`	Верхняя граница размера файла, сигнатура которого не определена. При превышении порогового значения файл автоматически считается бинарным и не отправляется на анализ в **iw_cas**. Значение по умолчанию – `25600`
`SpeedInKBs`	Предположительная скорость работы экстрактора, в Кб/с, в расчете на 1 ГГц частоты процессора. Значение по умолчанию – `100`
`TimeoutInSec`	Время ожидания (в секундах) до завершения обработки файла. Значение по умолчанию – `1800`
`UseLog`	Логирование экстрактора. Значение по умолчанию – false

Если общие значения параметров TimeoutInSec и MinFileSizeInBytes не подходят для каких-либо типов файлов, включите эти параметры в секции для нужных типов файлов с другими значениями.

Остальные секции содержат сигнатуры, при помощи которых детектируются типы файлов, находящиеся во вложениях и архивах. Секции имеют следующий набор параметров:

Параметр	**Описание и примеры настройки**
Extension	Расширение файла архива. Необязательный параметр, необходим для корректной работы некоторых архиваторов, которые требуют наличия правильного расширения входных файлов **Пример** Ext = arj
Name	Имя формата. Используется для точного определения имени формата при распаковке файла. Для определения/уточнения формата может включать также список имен: "defaultname, name1(code1), name2(code2)" В этом случае формат определяется на основании кода (*codeN*), присвоенного файлу при распаковке. Например, если распаковка завершается с кодом *code1*, то считается, что файл имеет формат *name1*. Список имен может также включать имя по умолчанию (*defaultname*), которое будет присваиваться в случаях, когда код не присвоен: **Пример 1 (одно имя формата)** text/xml **Пример 2 (список имен формата)** "application/arj, UNKNOWN(9), text/encrypted(4)" По умолчанию формат файла определяется как application/arj. Если формат архива не удается определить, ему присваивается имя UNKNOWN. Для зашифрованного архива используется имя форматаtext/encrypted
Signature	Сигнатура формата, которая представляет собой «образцовую» последовательность значений (байтов) с начальным смещением и масками. Эта последовательность необходима для однозначного определения формата файлов по их содержимому Сигнатура может включать до 16 триад вида: [OFFSET]:BYTE_VALUE/[MASK] Допускается также и строковая сигнатура, например, "BZh", для BZIP2. Эта сигнатура означает указанную последовательность байтов от смещения 0. Поиск строковых сигнатур выполняется без учета регистра символов. Параметр OFFSET является необязательным. Для первого байта этот параметр по умолчанию равен 0, для всех последующих – увеличивается на единицу. Смещение можно задать с символом «?» – поиск образца в первых N байтах файла. Например, для поиска образца в первых 500 байтах файла, нужно задать смещение '500?'. Параметр MASK, также является необязательным и равен 0xFF по умолчанию. **Пример** (сигнатура заголовка WAV-формата): Sign = "'RIFF', 0x8: 'WAVEfmt'" Начиная от смещения 0, расположена последовательность 'R', 'I', 'F', 'F', далее от смещения 8 должно следовать 'W', 'A', 'V', 'E', 'f', 'm', 't'
Comment	Комментарий с пояснениями. Например, указание используемой версии архиватора: Comment = "bzip2 v. 1.0.x"
Command	Строка команды для извлечения файлов. Например, Extract = "/usr/bin/bzip2 -f -dc ${SRC} > ${OUTDIR}/${SRC}" где ${OUTDIR} – каталог, в который будет распакован архив, а ${SRC} – имя файла, который нужно распаковать

ExcludeFromContext	Если параметр включен (On), то распаковка объекта выполняется, но информация об архиваторе не добавляется в XML-контекст объекта. Это позволяет не отображать в контексте объекта фиктивные контейнеры типа MS-TNEF. По умолчанию параметр отключен (Off)
CaseInsensitive	Учет регистра символов при обработке файла. Значение по умолчанию – false
CreateTags	Извлечение метаинформации из файла. Значение по умолчанию – true
Archive	Регламентирует вид извлеченной информации. При значении true - файлы. При значении false - данные.

4.2.5 Архивирование каталога очереди сообщений

При ошибках в очереди входящих SMTP-писем заархивируйте каталог очереди SMTP-писем и сохраните его для последующего анализа. Затем удалите каталог. Местоположение каталога очереди сообщений указано в конфигурационном файле **/opt/iw/tm5/etc/filequeues.conf**, в секции Smtppath.

4.2.6 Логирование работы Системы

Для удобства отслеживания работы процессов, подсистема протоколирования имеет шесть уровней:

Название уровня	**Описание**
fatal	Показывает ошибки, которые препятствуют дальнейшей работе процесса
error	Показывает сообщения об ошибках, которые не являются критическими для работоспособности процесса
warning	Выводит сведения о потенциально опасных ситуациях
info	Общая полезная информация о процессе (старт/стоп, применение конфигураций и т.д.)
debug	Выводит информацию, которая чаще всего используется для диагностики работы сервиса (IT, системные администраторы и т.д.)
trace	Чаще всего используется для отслеживания кода разработчиками

Настройка уровней протоколирования

Важно!

Следует учитывать, что изменение уровня протоколирования на более подробный может значительно снизить производительность Системы.

Конфигурационные файлы хранятся в директории `/opt/iw/tm5/etc`. По умолчанию все процессы имеют уровень протоколирования `warning`.

Чтобы изменить уровень протоколирования для процессов TMFD Server:

1. В конфигурационном файле нужного процесса, в секции `Logging` установите для параметра `GlobalLevel` необходимое значение.
2. Сохраните измененный файл.
3. После внесения изменений в системный журнал, перезапустите процесс:
   `service iwtm restart имя_службы`

Все логи процессов по умолчанию хранятся в каталоге `/var/log/infowatch`.

Для экстракторов, у которых нет отдельного конфигурационного файла, настройте уровень протоколирования в конфигурационном файле **/opt/iw/tm5/etc/extractors.conf**:

1. Откройте конфигурационный файл;
2. Для параметра `text-extractor` добавьте значение `–l <level>`
   Где <level> - уровень протоколирования.
   Например:

```
  },
        "docx": {
            "Command": [
                "bin/text-extractor –l error -t ooxml -i
${SRC} -d ${OUTDIR}"
```

Примечание:

Данный тип настройки протоколирования доступен для экстракторов следующих форматов: docx, html, msoffice_xml, msole, odp, odt, pptx, xlsx, xml.

4.2.7 Перемещение объектов между очередями (утилита iw_qtool)

Необходимость перемещения объектов из одной очереди в другую может возникнуть, когда объекты не загружаются в базу данных.
Для перемещения объектов из одной очереди в другую используется утилита **iw_qtool**. Порядок перемещения следующий. Наиболее старые объекты из очереди-источника перемещаются в начало очереди-приемника, таким образом, новые объекты будут перемещены в конец очереди-приемника. По окончании операции выводится количество перемещенных объектов.

Примечание:

Утилиту **iw_qtool** нужно запускать от имени пользователя **iwtm**. Для этого смените пользователя при помощи команды `su – iwtm` или выполните команду от имени пользователя напрямую при помощи команды `sudo -u iwtm <команда>`.

Команды для работы с утилитой **iw_qtool**:

Название команды	**Описание, синтаксис, примеры**

`stat`	Показывает количество объектов в очереди.
	Синтаксис:
	`iw_qtool stat имя_очереди`
	Пример (просмотр статистики по очереди объектов, загружаемых в базу данных):
	`/opt/iw/tm5/bin/iw_qtool stat /opt/iw/tm5/queue/db`

`move`	Перемещает объекты из одной очереди в другую.
	Внимание! В процессе перемещения объектов утилита создает временные файлы в текущем каталоге. Поэтому в данном случае рекомендуется запускать утилиту **iw_qtool** из каталога `/opt/iw/tm5`.
	Синтаксис:
	`iw_qtool move очередь_источник очередь_приемник [количество_объектов]`
	Параметры:
	• `очередь_источник` – полное имя очереди, из которой нужно переместить объекты. Если указанной очереди не существует, то работа утилиты завершится ошибкой;
	• `очередь_приемник` – полное имя очереди, в которую нужно переместить объекты. Если указанная очередь не существует, то она будет создана в процессе работы утилиты.
	• `количество_объектов` – ограничение на количество перемещаемых объектов (необязательный параметр). Если этот параметр не задан, то будут перемещены все объекты, находящиеся в очереди-источнике.
	Пример (перенос объектов из очереди errors в очередь db):
	`iw_qtool move /opt/iw/tm5/queue/errors /opt/iw/tm5/queue/db`

`put`	Помещает одиночный объект в очередь.
	Внимание! Для выполнения команды необходимо иметь права на запись в текущий каталог.
	Синтаксис:
	`iw_qtool put очередь_получатель xml_файл_объекта файл_объекта`
	Параметры:
	• `очередь_получатель` – полное имя очереди, в которую нужно поместить объект. Если указанной очереди не существует, то работа утилиты завершится ошибкой;
	• `xml_файл_объекта` – полное имя XML файла объекта. Если указанного файла не существует, то работа утилиты завершится ошибкой.
	• `файл_объекта` – полное имя файла с данными объекта. Если указанного файла не существует, то работа утилиты завершится ошибкой.
	Пример (помещение объекта в очередь db):
	`iw_qtool put /opt/iw/tm5/queue/db /home/iwtm/000000000.dat.xml /home/iwtm/000000000.dat`

4.2.8 Загрузка очередей объектов

Чтобы обеспечить загрузку имеющихся очередей объектов:

- Остановите процессы TMFD:
  `OS:root> service iwtm stop`
- Отключите автозапуск процессов **iw_proxy**, **iw_smtpd**, **iw_expressd** и **iw_icap** в конфигурационном файле каждого процесса:
  `"Startup" : {"Enabled" : false}`
- Запустите процессы TMFD
  `service iwtm start`
- Дождитесь, пока будут обработаны все объекты в файловой очереди.

> **Примечание:**
>
> По окончании процесса убедитесь, что перехватчики запущены, и включен автозапуск процессов.

TMFD имеет следующие очереди:

Путь к директории очереди	**Формат файлов в очереди**
`queue/blackboard`	`.dat`
`queue/blackboard_errors`	`.dat`
`queue/whiteboard`	`.dat`
`queue/errors`	`.xml & .dat`
`queue/xml2liro-errors`	`.xml & .dat`
`queue/db`	`.xml & .dat`
`queue/smtp`	`.xml & .dat`

Каждая из очередей содержит дополнительные технические очереди для отслеживания процесса обработки объектов:

a. `.db`

b. `.out`

c. `.in`

Например:
`queue/db/.out`

`queue/db/.in`

`queue/db/.db`

Для очереди `smtp` процесс обработки разделен на следующие этапы:

1. `queue/smtp/.in` – файл формируется в данной очереди в процессе получения объектов от Postfix модулем `smtpd`. Если объект по какой-то причине задерживается в этой очереди, необходимо проверить модули `smtpd` или `proxy_smtp`.
2. `queue/smtp/.db` – по окончании обработки файл перемещается из очереди `.in` в очередь `.db`.

3. queue/smtp/.out - в эту очередь объект перемещается следующим модулем в цепочке (в случае с очередью smtp - модулем messed).

Объекты в очередь помещаются посредством следующих модулей:

1. ВХОД – модуль, который помещает события в очередь.
2. ВЫХОД – модуль, который забирает события из очереди.

Имя очереди	**ВХОД**	**ВЫХОД**
queue/errors	все компоненты, если произошла ошибка обработки	нет
queue/xml2liro_loader	xml2liro	loader
queue/blackboard	luaengined	blackboard
queue/blackboard_errors	ошибка при обработке blackboard	нет
queue/whiteboard	luaengined	whiteboard
queue/rails_connector_errors	ошибки на вставке данных loader	нет
queue/xml2liro-errors	ошибки обработки xml2liro	нет

4.2.9 Восстановление работоспособности системы в аварийных ситуациях

При серьезных сбоях в работе серверов или сети восстановить работоспособность Системы можно, выполнив следующие действия:

1. Остановите процессы TMFD Server, выполнив команду:
   `service iwtm stop`
2. Переместите объекты из ошибочных очередей в обычные. Процедура выполняется при помощи утилиты iw_qtool.
3. По окончании работ проверьте соединение с СУБД Oracle, выполнив команду:
   `sqlplus db_login/db_password@tns_name`
   где `db_login` и `db_password` – имя и пароль владельца схемы базы данных, а `tns_name` – имя службы TNS.
   Если проверка пройдена успешно, то в ответ на выполнение указанной команды будет выведено приглашение SQL *Plus:
   `SQL>`
4. Запустите процессов TMFD Server, выполнив команду:
   `service iwtm start`

После запуска TMFD Server, проверьте системный журнал на наличие ошибок. Путь к файлу журнала:

`/var/log/messages`

Если в системном журнале содержится информация об ошибках, обратитесь в службу технической поддержки.

4.2.10 Настройка serman.conf при изменении адреса сервера БД

В случае изменения IP-адреса сервера базы данных, укажите новый адрес БД в параметре `DefaultInterface` секции `Serman` конфигурационного файла **serman.conf**.

4.2.11 Настройка передачи информации в SIEM

Интеграция TMFD с SIEM системами (ArcSight, Tivoli) происходит посредством встроенных возможностей программы. Настройка данного функционала возможна при помощи утилиты **setup**, которая доступна на сервере TMFD.

Под интеграцией подразумевается поступление в SIEM-систему консолидированной информации со всех установленных в компании заказчика компонент системы ТМ.

Информация из TMFD доступна для SIEM системы:

- Посредством табличного представления:
  - События, зарегистрированные в ТМ;
  - Аудит сессий пользователей консоли ТМ;
- Посредством rsyslog:
  - Вход/выход пользователей Linux-сервера ТМ;
  - События, зафиксированные в системном журнале Linux-сервера ТМ, включая информацию о входе/выходе пользователей Базы Данных Oracle или Postgre;
  - Состояние служб Linux-сервера TMFD или группы серверов.

В этом разделе:

1. *Настройки на стороне SIEM*
2. *Настройки на стороне TMFD*
3. *Типы логов, передаваемых в SIEM*

4.2.11.1 Настройки на стороне SIEM

Чтобы подготовить SIEM к получению данных от TMFD:

1. В SIEM укажите таблицы, из которых необходимо забирать информацию:
   a. `IWTM.ARC_VIEW_OBJECTS`
      События ТМ
   b. `IWTM.ARC_VIEW_AUDIT_LOG`
      Аудит пользователей ТМ
2. Создайте учетную запись SIEM для доступа к таблицам БД.
3. Настройте обработку данных, извлеченных из БД ТМ.

Важно!

При настройке интеграции могут понадобиться дополнительные модули от производителя SIEM системы, позволяющие SIEM системе работать с табличными представлениями. Например, для интеграции с HP ArcSight необходим модуль HP Flex Conector.

При подключении к БД TMFD используйте созданного пользователя **siem**. Искомые данные содержатся в таблице `IWTM.ARC_VIEW_OBJECTS`.

При подключении к БД TMFD используйте созданного пользователя **siem**. Искомые данные содержатся в таблице `IWTM.ARC_VIEW_AUDIT_LOG`.

4.2.11.2 Настройки на стороне TMFD

Чтобы настроить передачу консолидированной информации из ТМ:

1. Запустите меню утилиты **setup**.
2. Создайте учетную запись БД для SIEM (см. "Создание пользователя siem").
3. Настройте передачу информации из TMFD в SIEM (см. "Передача логов в SIEM");
4. Отрегулируйте настройку **Nagios** и компонент TMFD из меню;
5. Отрегулируйте настройки логирования аудита сессий пользователей БД ТМ.

4.2.11.2.1 Передача логов в SIEM

Чтобы настроить передачу записей из лог файлов Linux-сервера ТМ в SIEM:

- Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup.`
- Выберите опцию **IW Services configuration**.
- Выберите опцию **iwtm-siem**
- Выберите опцию **Log messages forwarding configuration**.
- Задайте параметры передачи логов:

Параметр	**Описание**
`Enable forwarding`	Включение/выключение пересылки логов в siem. (Возможные значения: `Yes/No`)
`Forwarding server`	IP-адрес или dns-имя сервера SIEM
`Forwarding server port`	Порт сервера SIEM, на котором работает **syslog**
`Forwarding protocol`	Протокол передачи данных в SIEM. (Возможные значения: `TCP/UDP`)
`Log messages severity`	Минимальный уровень лог-сообщений, пересылаемых на сервер SIEM. (Возможные значения: `Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug`)

`Size (MB)`	Допустимый размер очереди сообщений, требующих отправку в SIEM. (Значение по умолчанию: `500`)

- Нажмите **Ok**.

Важно!

В БД не логируется отключение от БД пользователей с правами администратора, соответственно в SIEM данная информация попадать не будет.

4.2.11.2.2 Управление логированием сессий пользователей БД ТМ

Включение и выключение логирования сессий пользователей БД ТМ в системный журнал ОС осуществляется через **rsyslog**.

Чтобы включить логирование сессий пользователей Базы Данных ТМ:

1. Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup.`
2. Выберите опцию **IW Services configuration**.
3. Выберите опцию **iwtm-siem**
4. Выберите опцию **DB audit logging management**.
5. Задайте параметры:

Параметр	**Значение**
`Enter login for DB administrative account`	Логин для учетной записи администратора Oracle/Postgre
`Enter password for DB administrative account`	Пароль для учетной записи администратора Oracle/Postgre

6. Нажмите **Check logging status**.
7. Если:
   - **DB audit logging to OS journal: OFF** - нажмите **Change logging status**, чтобы включить логирование.
   - **DB audit logging to OS journal: ON** - нажмите **Change logging status**, чтобы выключить логирование.

4.2.11.2.3 Управление пользователем siem

В данном разделе описывается создание, удаление и смена пароля для пользователя **siem**, от имени которого SIEM будет взаимодействовать с ТМ:

1. *Создание пользователя siem*
2. *Смена пароля пользователя siem*
3. *Удаление пользователя siem*

4.2.11.2.3.1 СОЗДАНИЕ ПОЛЬЗОВАТЕЛЯ SIEM

Чтобы создать пользователя siem:

1. Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup.`
2. Выберите опцию **IW Services configuration**.
3. Выберите опцию **iwtm-siem**
4. Выберите опцию **DB siem user**.
5. В появившемся меню выберите опцию **Create DB siem user**.
6. Задайте параметры:

Параметр	**Описание**
`Enter login for DB administrative account`	Логин для учетной записи администратора Oracle/Postgre
`Enter password for DB administrative account`	Пароль для учетной записи администратора Oracle/Postgre
`Enter password DB siem user`	Пароль для новой учетной записи siem

7. Нажмите **Create**.

4.2.11.2.3.2 СМЕНА ПАРОЛЯ ПОЛЬЗОВАТЕЛЯ SIEM

Чтобы сменить пароль пользователю siem:

1. Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup.`
2. Выберите опцию **IW Services configuration**.
3. Выберите опцию **iwtm-siem**.
4. Выберите опцию **DB siem user**.
5. Выберите опцию **Change password for DB siem user**.
6. Задайте параметры:

Параметр	**Описание**
`Enter login for DB administrative account`	Логин для учетной записи администратора Oracle/Postgre
`Enter password for DB administrative account`	Пароль для учетной записи администратора Oracle/Postgre
`Enter new password user siem`	Новый пароль для учетной записи **siem**

7. Нажмите **Change password**.

4.2.11.2.3.3 УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЯ SIEM

Чтобы удалить пользователя siem:

1. Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup.`

2. Выберите опцию **IW Services configuration**.
3. Выберите опцию **iwtm-siem**.
4. Выберите опцию **DB siem user**.
5. Выберите опцию **Delete DB siem user**.
6. Задайте параметры:

Параметр	**Описание**
`Enter login for DB administrative account`	Логин для учетной записи администратора Oracle/Postgre
`Enter password for DB administrative account`	Пароль для учетной записи администратора Oracle/Postgre

7. Нажмите **Delete**.

4.2.11.3 Типы логов, передаваемых в SIEM

Rsyslog формирует общий системный журнал и является протоколом, по которому логи передаются в SIEM.

Существует пять основных типов логов, которые передаются в SIEM:

1. Логи от процессов **iw_*** . Например:
   ```
   Mar 11 14:32:30 iw-VMware-4224da3ab iw_expressd: 5 (18485:0x00007f53001b97e0) [INFO
   ] : <Root> Runtime environment initialized. Starting...
   ```
2. Логи от скрипта **pguard**, который отслеживает состояние сервисов и перезапускает их в случае необходимости:
   ```
   Mar 11 14:32:26 iw-VMware-4224da3ab pguard: 148 (18256:0) [INFO] : expressd
   Terminating pid 18257 (signal 15)
   ```
3. Логи подключения и отключения от **БД Oracle**:
   ```
   Mar 11 14:28:20 iw-VMware-4224da3ab Oracle Audit[17786]: LENGTH : '153' ACTION :[7]
   'STARTUP' DATABASE USER:[1] '/' PRIVILEGE :[4] 'NONE' CLIENT USER:[4] 'root' CLIENT
   TERMINAL:[13] 'Not Available' STATUS:[1] '0' DBID:[0]
   ```
4. Логи входа и выхода **пользователей Linux**:
   ```
   Mar 11 14:32:02 iw-VMware-4224da3ab runuser: pam_unix(runuser:session): session opened
   for user iwtm by root(uid=0)
   ```
5. Логи **Nagios**:
   ```
   Feb 10 20:05:39 iw-VMware-4224289a4 nagios: SERVICE ALERT:
   IWTM;TM_DAEMONS_STATE;CRITICAL;SOFT;1;CRITICAL - updater(3)
   ```

4.2.12 Удаление временных файлов

Возможность удаления временных файлов реализована в продукте в виде сценария **clean_temporary_files.sh**.

Сценарий удаляет следующую информацию:

- Файлы из директории временных файлов операционной системы (директория `/opt/iw/tm5/tmp/`).

- Данные из директорий файловых очередей TMFD (директория `/opt/iw/tm5/queue/`).

Примечание:

Во время удаления временных файлов обработка поступающих в Систему событий будет остановлена. Данные обо всех необработанных на момент начала удаления событиях будут удалены.

Чтобы удалить временные файлы:

1. Запустите сценарий **clean_temporary_files.sh**:
   `/opt/iw/tm5/bin/clean_temporary_files.sh`
2. Согласитесь на удаление временных файлов:
   `yes`

5 ИСПОЛЬЗОВАНИЕ СИСТЕМЫ

5.1 Общие принципы работы с Консолью управления

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.

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 реакций Системы на действия персон, нарушающие корпоративную политику 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.

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)**.

5.1.1 Работа Системы до конфигурирования

Установленная Система, для которой еще не выполнялось конфигурирование, функционирует следующим образом:

- Осуществляет перехват трафика и проверку объектов перехвата на соответствие указанным в Системе выгрузкам из БД. В случае соответствия объекта перехвата какой-либо выгрузке из БД, Система присваивает объекту соответствующий атрибут.
- 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 рабочими станциями").
- 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.

5.1.2 Работа с конфигурацией Системы

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

Каждый объект, передаваемый в TMFD, 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.

Настройка конфигурации включает в себя:

- Составление базы элементов технологий (см. "Настройка базы технологий"):
    - выбор выгрузок из БД, подлежащих детектированию - *только при использовании технологии Детектирование выгрузок из БД (см. "Выгрузки из БД")*;
- Создание объектов защиты на основе элементов базы технологий *(см. "Объекты защиты")*.
- Составление справочников:
    - персон и рабочих станций *(см. "Работа с персонами и рабочими станциями")*;
    - тегов *(см. "Работа с тегами")*;
    - списков ресурсов *(см. "Работа со списками ресурсов")*;
    - статусов *(см. "Работа со статусами")*;
    - периметров *(см. "Работа с периметрами")*;
- Составление политик, в соответствии с которыми будет выполняться проверка объектов на сервере TMFD *(см. "Настройка реакций Системы")*

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

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

  Вы редактируете конфигурацию с 15.06.2015 15:54

- 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.
- **Отменить изменения** - конфигурация в Консоли управления будет соответствовать последней примененной на сервере конфигурации, и все сделанные изменения конфигурации удалятся. Для отмены изменений нажмите **Отменить** в появившемся окне списка изменений. В поле

Описание при необходимости укажите причину отмены конфигурации. 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.

5.1.3 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.

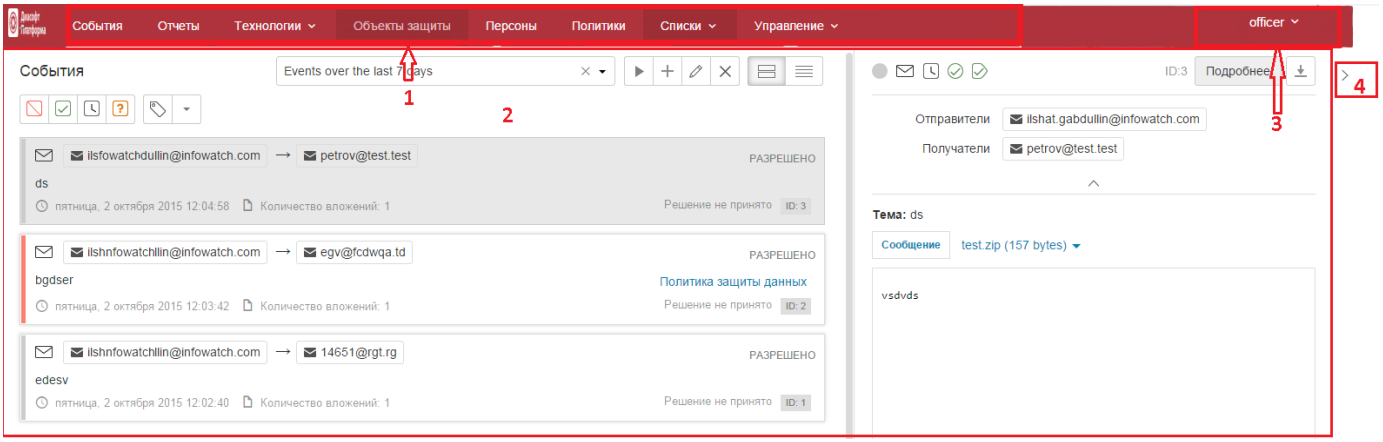
В любом из разделов Консоли управления вы также можете обновлять данные вручную. Для этого воспользуйтесь стандартным средством обновления страницы интернет-браузера (по умолчанию обновление выполняется при нажатии функциональной клавиши F5).

Примечание:

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

5.2 Интерфейс Консоли управления

Все окна Консоли управления TMFD имеют ряд общих элементов.



Элементы окна Консоли управления:

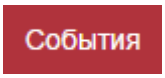
Номер на схеме	Элемент окна консоли	Назначение элемента
1	Панель Навигации	Отображение кнопок разделов. При нажатии на кнопку раздела выполняется переход к выбранному разделу Консоли управления.
2	Рабочая область	Отображение элементов выбранного раздела Консоли управления, работа с элементами выбранного 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 и выход из нее")
4	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.

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
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

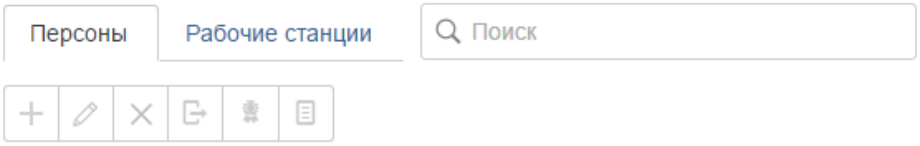
Переход к разделу происходит после нажатия на кнопку раздела.



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 **Рабочие станции**

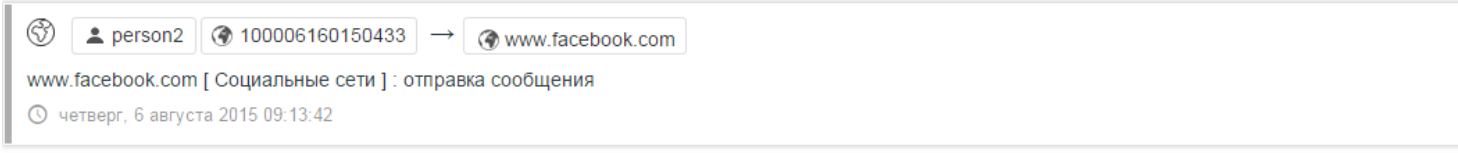
- **Панель** - область интерфейса, отображающая набор данных или содержащая набор элементов интерфейса, и отделенная от остальных областей.

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



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.



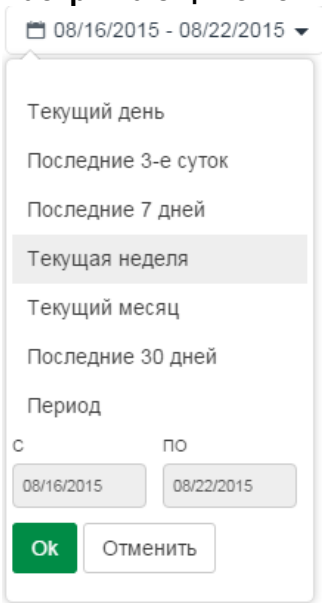
Раздел **События**, плитка события

- **Поле** - элемент для вывода строковых данных или для ввода данных с клавиатуры или из буфера обмена.



Поле **Поиск**

- **Раскрывающийся список** - отражает список элементов при нажатии.



Раздел **Сводка**, раскрывающийся список на виджете

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

Примечание:

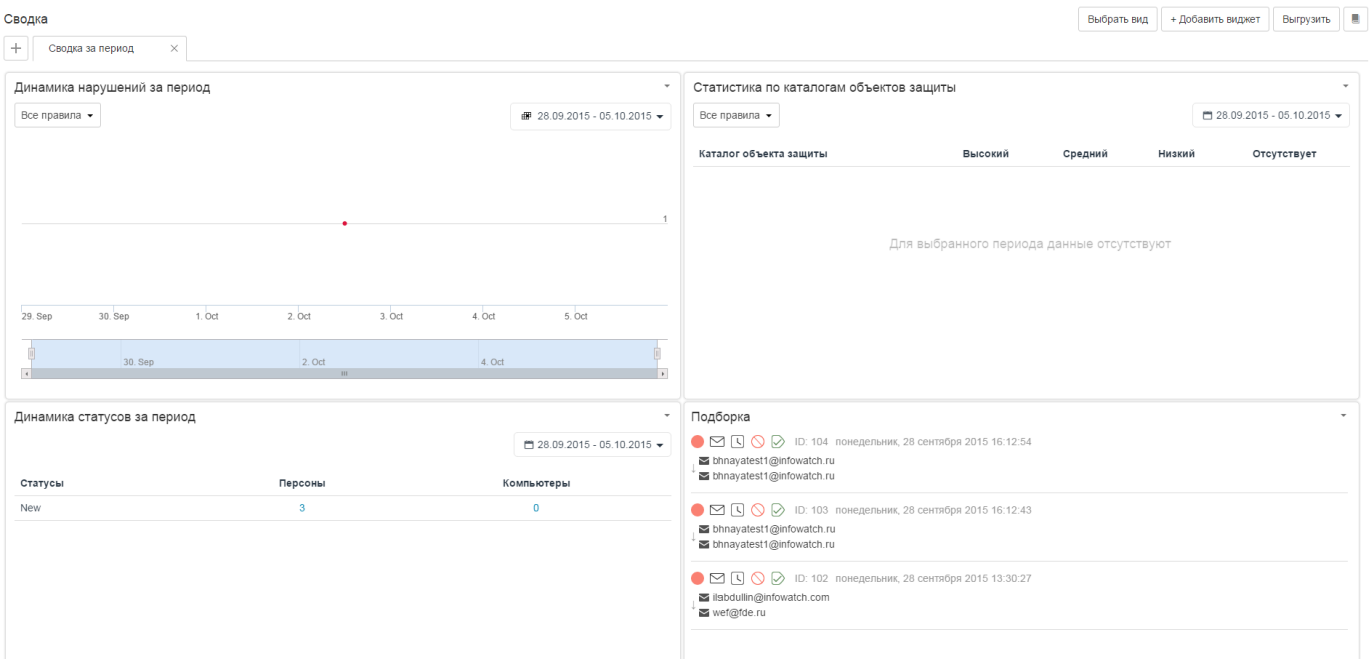
В тех случаях, когда запрашиваемые данные находятся в процессе загрузки, в Системе может отображаться символ вида либо информационное сообщение.

5.2.1 Раздел "Сводка"

О разделе:

Раздел содержит статистическую информацию о нарушениях/нарушителях.

Информация отображается на виджетах, которые располагаются на панелях (вкладках).



Раздел **Сводка**

В разделе содержатся следующие элементы:

Элемент	Назначение
Виджеты	Содержит информацию по нарушениям/нарушителям
Панели	Содержит виджеты
Кнопка **Добавить панель**	Добавление панели
Кнопка **Выбрать вид**	Позволяет выбрать способ разделения рабочей области, при котором панели будут отображаться в удобных пользователю пропорциях. Возможные варианты: - деление на 3 равные части; - деление в отношении 2:1; - деление на 2 равные части; - деление в отношении 1:2.
Кнопка **+Добавить виджет**	Добавление виджета
Кнопка **Выгрузить**	Выгрузка сводки о нарушениях/нарушителях (см. "Выгрузка сводки" - о параметрах выгрузки, и "Создание выгрузки" - о порядке действий, необходимых для формирования выгрузки)

Кнопка **Просмотреть список выгрузок**	Просмотр созданных выгрузок

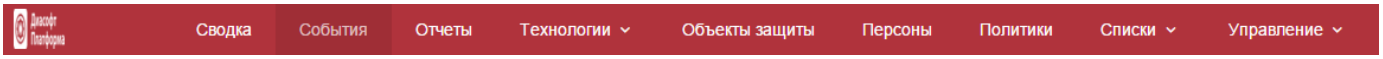
Целевые действия пользователя:

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

5.2.1.1 Панели

Рабочая область раздела **Сводка** содержит одну или несколько **панелей**: вкладок, где располагают виджеты, с помощью которых можно просматривать статистику по нарушениям и нарушителям.

Панели позволяют эргономично использовать рабочую область раздела **Сводка**.



Атрибуты панели описаны в таблице:

Параметр	Описание
Название	Наименование панели
Вид	Способ отображения данных на панели
Набор виджетов	Виджеты, закрепленные на панели

Целевые действия пользователя:

- создание и настройка панели для отображения информации о нарушениях/нарушителях (см. "Создание панели" и "Создание виджета")

5.2.1.2 Виджеты сводки

Рабочая область раздела **Сводка** содержит панели, предназначенные для отображения виджетов.

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	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 отображается количество нарушений высокого, среднего, низкого уровня за выбранный период времени

Подборка	События для выбранной подборки (по выбранному фильтру)
Динамика статусов	Динамика статусов за выбранный период времени
Статистика по политикам	Количество нарушений по политикам в разрезе правил передачи 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. "Настройка виджета")
- перемещение плиток виджетов (см. "Создание виджета")

5.2.1.2.1 Динамика нарушений

Виджет **Динамика нарушений** отображает количественные изменения по выбранным типам нарушений за выбранный период времени

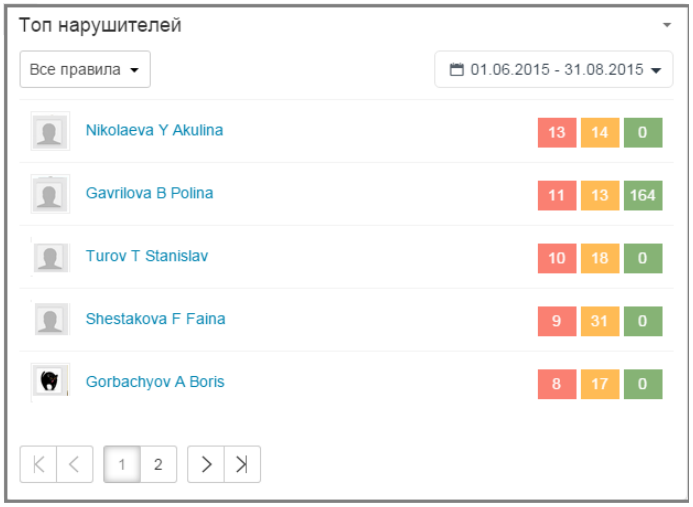


Параметры виджета:

Параметр	**Описание**
Название	Наименование виджета
Правила	Категория правил, нарушения которых отображаются на виджете
Интервал обновления	Периодичность обновления данных на виджете
Период	Временной промежуток, за который выводятся данные

5.2.1.2.2 Топ нарушителей

Виджет **Топ нарушителей** отображает список наиболее отличившихся нарушителей по выбранной группе за выбранный период времени

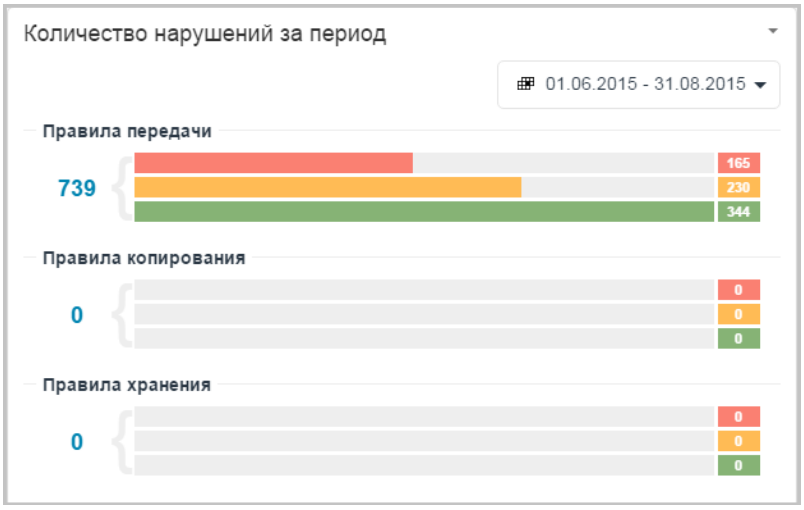


Атрибуты виджета описаны в таблице:

Параметр	Описание
Название	Наименование виджета
Правила	Категория правил, нарушения которых отображаются на виджете
Интервал обновления	Периодичность обновления данных на виджете
Период	Временной промежуток, за который выводятся данные
Кол-во нарушителей	Количество нарушителей, сводка по которым будет отображаться
Группы	Группы, сводка по которым будет отображаться
Статусы	Статусы, сводка по которым будет отображаться

5.2.1.2.3 Количество нарушений за период

Виджет **Количество нарушений за период** отображает количество нарушений высокого, среднего и низкого уровня для каждого из типа нарушений за выбранный пользователем период времени.



Атрибуты виджета описаны в таблице:

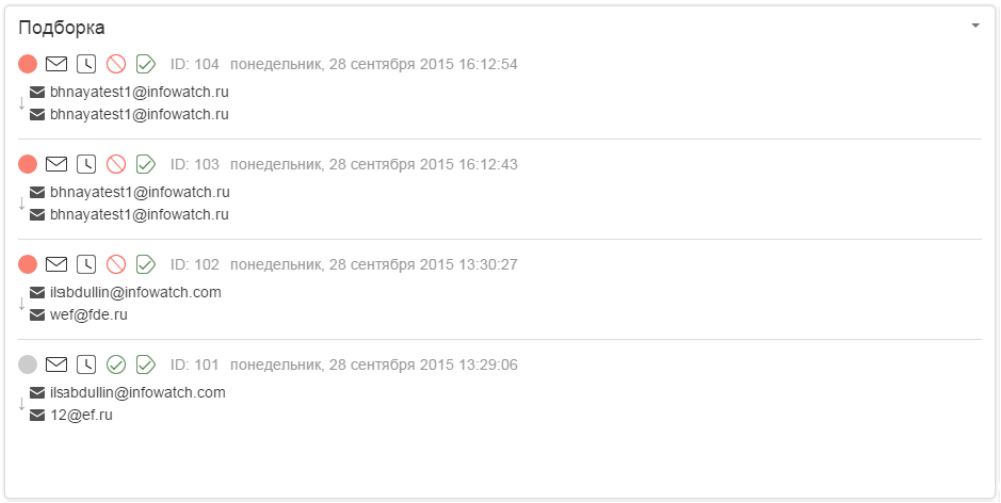
Параметр	Описание
Название	Наименование виджета
Интервал обновления	Периодичность обновления данных на виджете
Период	Временной промежуток, за который выводятся данные
Тип предоставления	Вид, в котором будут представлены данные

Примечание:

При нажатии на цифру количества нарушений (выделена синим цветом), выполняется переход в раздел **События** с отображением списка нарушений.

5.2.1.2.4 Подборка

Виджет **Подборка** отображает плитки событий для подборки по выбранному фильтру.



Атрибуты виджета описаны в таблице:

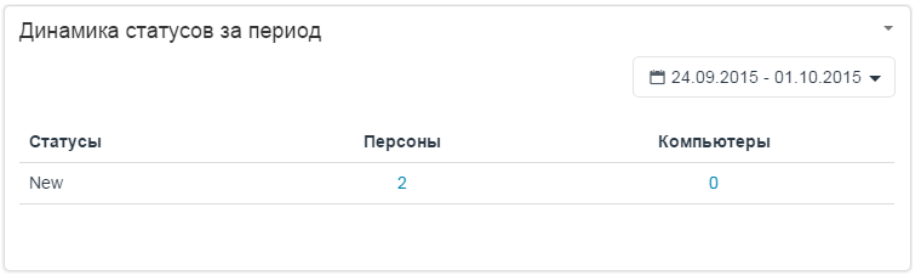
Параметр	Описание
Название	Наименование виджета
Интервал обновления	Периодичность обновления данных на виджете
Подборка	Название запроса, по которому будет осуществляться подборка (см. "Запросы")
Событий на странице	Количество событий, которое будет отображаться на странице

Примечание:

При нажатии на **ID** объекта (выделен синим цветом) выполняется переход в раздел **События**, к выбранному объекту.

5.2.1.2.5 Динамика статусов

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



Атрибуты виджета описаны в таблице:

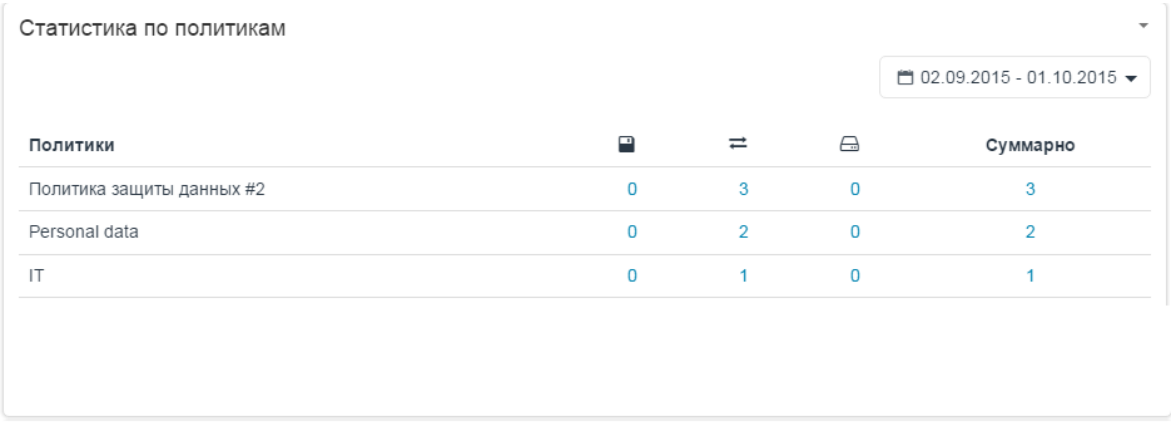
Параметр	Описание
Название	Наименование виджета
Интервал обновления	Периодичность обновления данных на виджете
Период	Временной промежуток, за который выводятся данные

Примечание:

При нажатии на количество персон или рабочих станций (выделено синим цветом), выполняется переход в раздел **Персоны**, к вкладке **Персоны** или **Рабочие станции** соответственно.

5.2.1.2.6 Статистика по политикам

Виджет **Статистика по политикам** отображает количество нарушений по политикам в разрезе активностей пользователя за выбранный период времени.



Атрибуты виджета описаны в таблице:

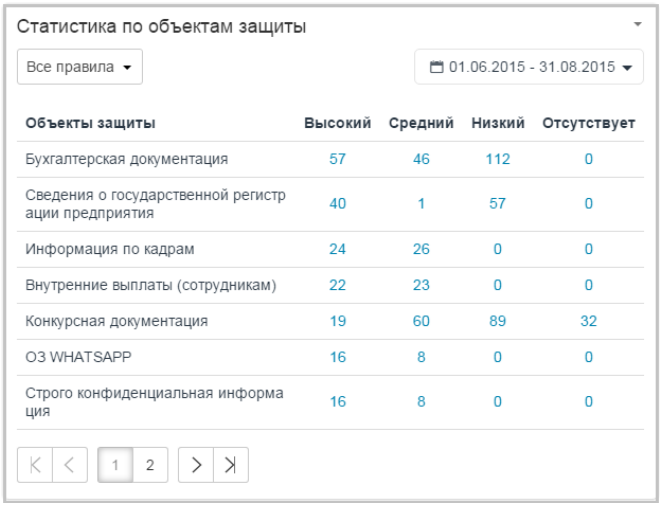
Параметр	Описание
Название	Наименование виджета
Интервал обновления	Периодичность обновления данных на виджете
Период	Временной промежуток, за который выводятся данные
Политики	Политики, сводка по которым будет отображаться

Примечание:

При нажатии на число нарушений политик (выделено синим цветом), выполняется переход в раздел **События**, где отображается список нарушений.

5.2.1.2.7 Статистика по объектам защиты

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



Атрибуты виджета

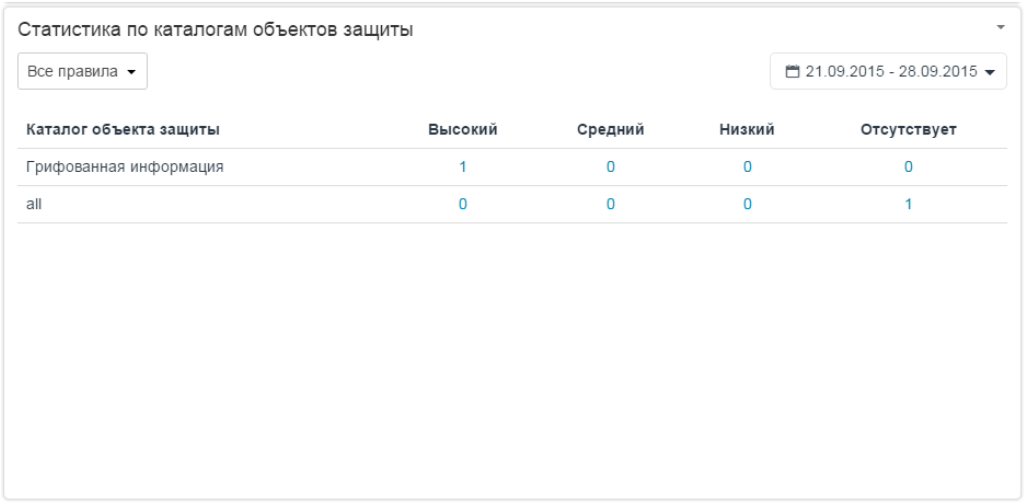
Параметр	Описание
Название	Наименование виджета
Правила	Категория правил, нарушения которых отображаются на виджете
Интервал обновления	Периодичность обновления данных на виджете
Период	Временной промежуток, за который выводятся данные
Объект защиты	Объекты защиты, сводка по которым будет отображаться
Каталог объекта защиты	Каталог, объекты защиты которого будут отображаться в сводке

Примечание:

При нажатии на число нарушений для каждого из объектов защиты (выделено синим цветом), выполняется переход в раздел **События**, где отображается список нарушений.

5.2.1.2.8 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.



Атрибуты виджета:

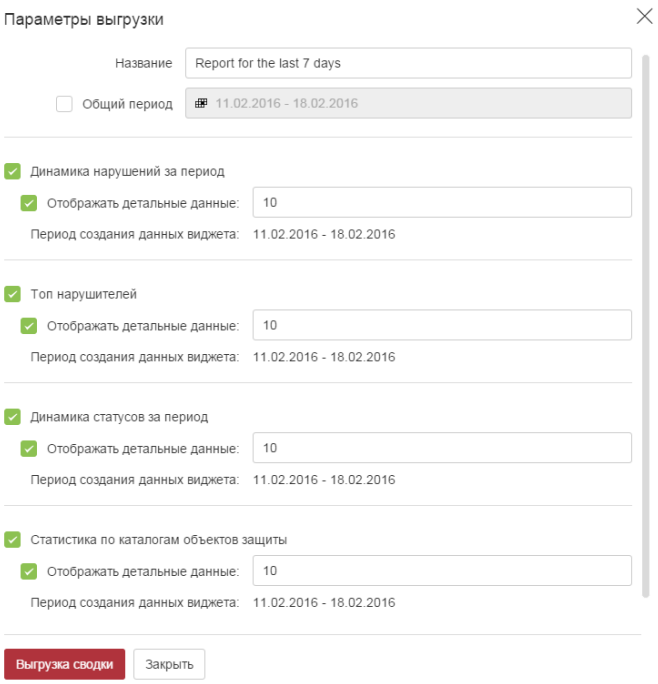
Параметр	Описание
Название	Наименование виджета
Правила	Категория правил, нарушения которых отображаются на виджете
Интервал обновления	Периодичность обновления данных на виджете
Период	Временной промежуток, за который выводятся данные
Каталог объектов защиты	Каталог объектов защиты, сводка по которому будет отображаться

Примечание:

При нажатии на число нарушений для каждого из каталогов объектов защиты (выделено синим цветом), выполняется переход в раздел **События**, где отображается список нарушений.

5.2.1.3 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.



Окно создания выгрузки

Атрибуты выгрузки:

Параметр	Описание
Название	Наименование выгрузки
Общий период	Период, за который будет сделана выгрузка. Укажите начальную и конечную дату для формирования выгрузки
Блок виджета	Показатель того, включены ли данные с виджета в выгрузку. По умолчанию выгрузка формируется для всех виджетов панели. Если Вы не хотите включать данные какого-либо виджета, снимите галочку напротив его названия.
Отображать детальные данные	Показатель того, будут ли в выгрузке отображаться конкретные объекты. Укажите количество объектов виджета, которые будут отображать в выгрузке. По умолчанию отображается 10 объектов.

Целевые действия пользователя:

- составление выгрузки сводки (см. "Работа с выгрузками").

5.2.2 Раздел "События"

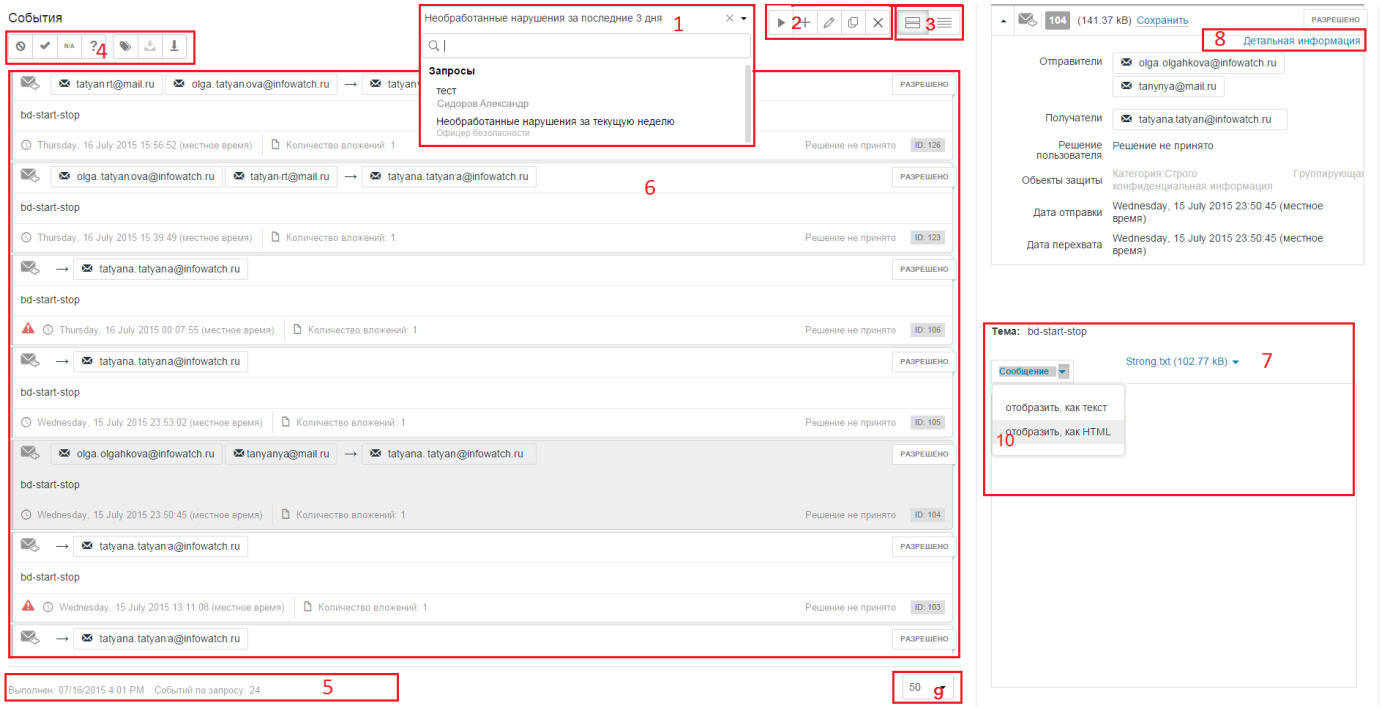
Справочная информация:
Событие - объект перехвата сетевого трафика.

События создаются Системой в результате перехвата трафика при:

- передаче данных сотрудниками другим людям;
- публикации данных в общедоступных источниках;

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 фильтрации.



В разделе содержатся следующие элементы:

Номер на схеме	Элемент	Назначение
1	Раскрывающийся список запросов	Содержит список доступных запросов, с помощью которых может быть произведена фильтрация объектов перехвата (см. "Запросы") **Примечание:** для каждого запроса в списке указано его название и пользователь, создавший запрос
2	Панель инструментов для работы с запросами	Набор инструментов для работы с запросами
3	Кнопки выбора стиля отображения событий	Переключение между способами отображения событий:  - отображение событий в виде плиток;  - отображение событий в виде таблицы.
4	Панель инструментов для событий	Набор инструментов для работы с событиями
5	Атрибуты события: время выполнения и количество найденных событий	Отображается дата выполнения запроса в формате MM/DD/YY, время выполнения и количество найденных событий

6	Список событий	Список объектов перехвата, найденных в результате выполнения запроса (см. "Объекты перехвата"). **Примечание:** О характеристиках плитки события см. "Плитка события"
7	Краткая форма просмотра события (см. "Краткая форма просмотра событий")	Набор наиболее часто используемых сведений о событии (см. "Краткая форма просмотра событий")
8	Детальная информация по событию (см. "Детальная форма просмотра событий")	Полный набор сведений о событии
9	Число отображаемых записей - раскрывающийся список	Позволяет выбрать количество событий, отображающихся на странице
10	Режим просмотра сообщения (только для писем, содержащих HTML-разметку)	Позволяет выбрать режим просмотра сообщения. Возможные значения: **отобразить как текст** - служит для отображения текста письма без форматирования. Позволяет увидеть скрытый текст (например, текст белого цвета или текст, содержащийся в названии картинки; **отобразить как HTML** - позволяет просмотреть картинки, таблицы и разметку текста.

Целевые действия пользователя:

- фильтрация событий (см. "Фильтрация событий");
- 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)");
- выгрузка событий (см. "Выгрузка события");
- просмотр контактов отправителей и получателей в событии (см. "Идентификация контактов в событии").

5.2.2.1 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 - это выборка объектов перехвата по заданным условиям.

Запрос содержит следующие элементы:

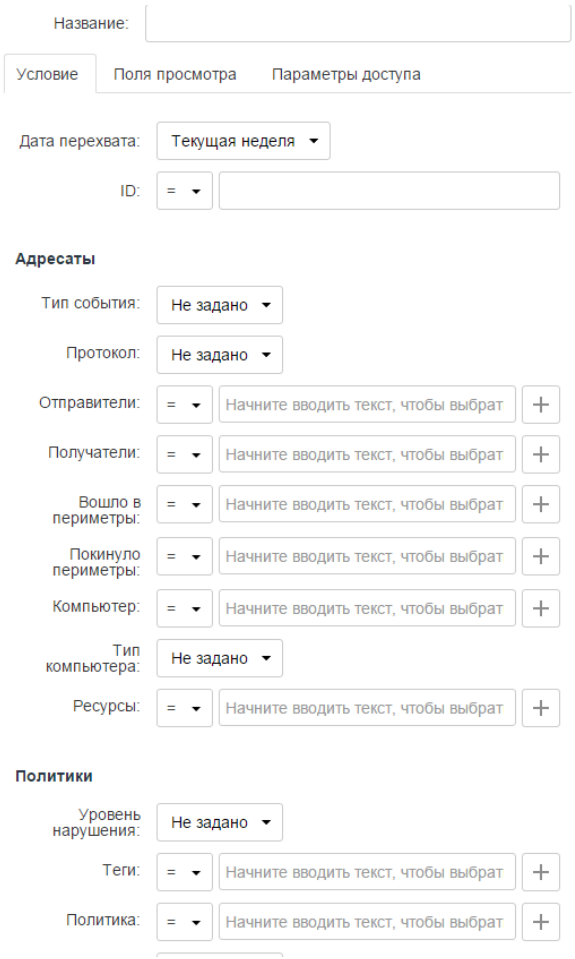
Элемент	**Назначение**
Условие	На этой вкладке вы можете указать условия, по которым будет производиться фильтрация

Поля просмотра	На этой вкладке вы можете выбрать, какие поля просмотра будут отображаться в записях событий
Параметры доступа	На этой вкладке вы можете настроить доступ только для владельца запроса
Режим создания запроса	Предусмотрено два режима создания запроса: обычный (позволяет выбрать нужные условия из списка) и расширенный (позволяет выполнить более гибкую настройку параметров поиска)

Целевые действия пользователя:

- настройка запроса (см. "Создание запросов");
- определение полей просмотра (см. "Выбор полей просмотра событий").

5.2.2.1.1 Условие



Раздел **События**, вкладка **Условие** для выбранного запроса

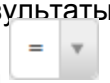
Атрибуты условия фильтрации:

Параметр	**Описание**

	Параметр равенства атрибуту
	Параметр отрицания атрибута
Дата перехвата	Дата, когда было создано событие. По умолчанию будут показаны события за текущую неделю.
ID объекта	Уникальный идентификатор события. Может быть указано несколько значений через запятую.
Тип события	Характеристика, указывающая на принадлежность события к тому или иному перехватчику.
Протокол	Протокол, по которому осуществляется передача трафика
Отправители	Список отправителей объекта
Получатели	Список получателей объекта
Вошло в периметры	Периметр, в котором находится получатель трафика
Покинуло периметры	Периметр, в котором находится отправитель трафика
Компьютер	Компьютер, с которого был отправлен объект
Тип компьютера	Тип компьютера, с которого был отправлен объект. Возможные значения: • компьютер • мобильное устройство • терминальный сервер
Ресурсы	Тип ресурса, на котором хранился объект
Уровень нарушения	Уровень нарушения политики корпоративной безопасности. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует*.
Теги	Теги, присвоенные объекту
Политика	Список политик, сработавших на объекте
Тип нарушения	Тип правила, которое было нарушено
Решение пользователя	Решение, принятое пользователем по объекту. Возможные значения: *Нарушение*, *Нет нарушения*, *Решение не принято*, *Требуется дополнительный анализ.*
Вердикт	Вердикт, вынесенный Системой по объекту. Возможные значения: *Разрешено*, *Заблокировано*, *Карантин*.
Имя задания	Имя задания на сканирование. **Примечание**. Вы можете указать имя задания с использованием групповых символов: "?" - вместо отдельного символа и "*" - вместо группы символов.

Дата запуска задания	Временной период, в который задача была запущена
Тип источника сканирования	Тип локации, на которой объект был найден. Возможные значения: • Разделяемые сетевые ресурсы • Локальные диски рабочих станций • Файловое хранилище SharePoint
Имя вложения	Название вложения, содержащегося в объекте. Указывается имя файла и его расширение. **Примечание**. Вы можете указать название с использованием групповых символов: "?" - вместо отдельного символа и "*" - вместо группы символов.
Формат вложения	Формат вложения. Можно выбрать несколько значений из списка.
Зашифрованный файл	Применяется ли к вложению шифрование
Путь к файлу	Источник файла
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
Любая технология анализа	Имеют ли значение сущности, под которые подпадает содержимое события
Объекты защиты	Список сработавших объектов защиты

При создании или редактировании условий возможно задать положительные и отрицательные параметры запроса:

- Чтобы результаты запроса включали требуемый атрибут, установите напротив него параметр равенства .
- Чтобы исключить требуемый атрибут из результатов запроса, установите напротив него параметр отрицания .

Настройка равенства или отрицания доступна для следующих атрибутов:

- ID объекта;
- Отправители;
- Получатели;
- Вошло в периметры;
- Покинуло периметры;
- Рабочая станция отправителя;
- Ресурсы;
- Теги;
- Политика;
- Имя вложения;
- Формат вложения;
- Теста события;
- Результаты анализа;
- Объекты защиты.

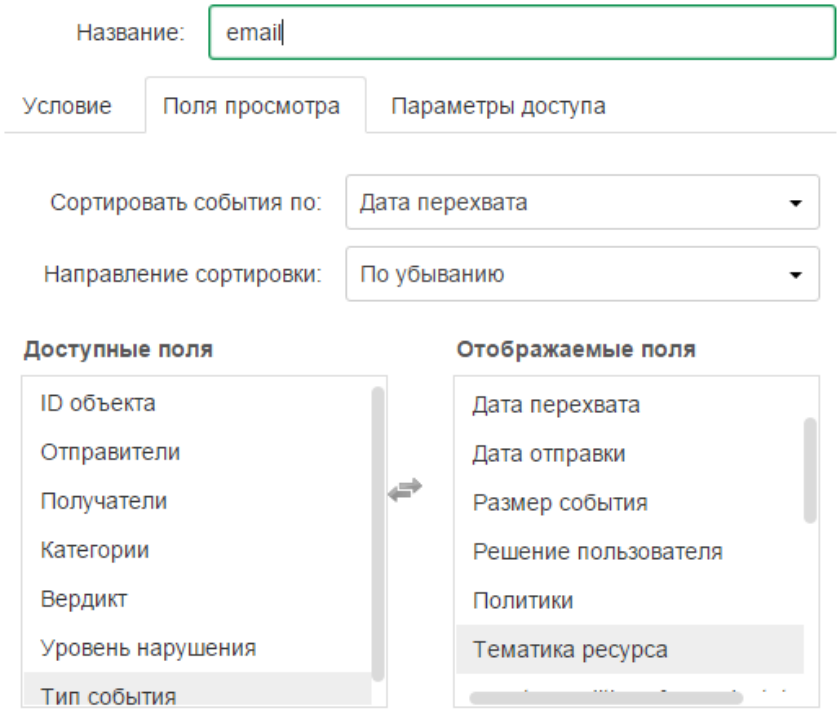
Если отрицание применяется к атрибуту с множественными значениями, то из результатов поиска будут исключены события, содержащие указанные значения. Например, если в качестве отправителей указаны адреса `user1@example.com` и `user2@example.com`, из результатов поиска будут исключены события, в которых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

Целевые действия пользователя:

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

5.2.2.1.2 Поля просмотра

На вкладке в левом поле представлен список доступных атрибутов события, а в правом - 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.

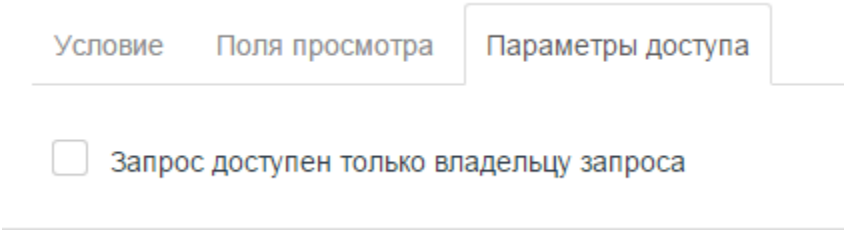


Раздел **События**, вкладка **Поля просмотра** для выбранного запроса

Целевые действия пользователя:

- Определение полей, которые будут отображаться в информации о событии (см. "Выбор полей просмотра событий")
- Выгрузка событий (см. "Выгрузка события")

5.2.2.1.3 Параметры доступа



Раздел **События**, вкладка **Параметры доступа** для выбранного запроса

Чтобы установить ограничение на просмотр и редактирование запроса другими пользователями:

1. Установите флажок в поле **Запрос доступен только владельцу запроса**.
2. Нажмите **Сохранить**.

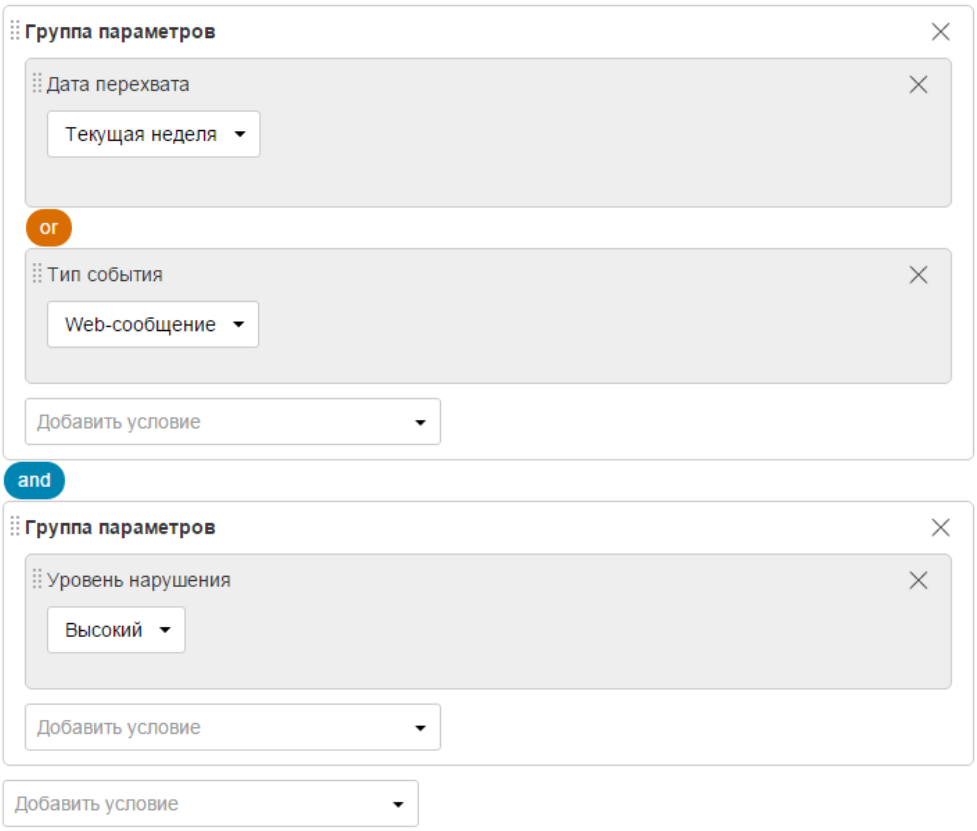
Чтобы открыть доступ на просмотр и редактирование запроса другими пользователями:

1. Снимите флажок в поле **Запрос доступен только владельцу запроса** (по умолчанию флажок установлен).

2. Нажмите **Сохранить**.

5.2.2.1.4 Расширенный режим редактирования запроса

Расширенный режим предназначен для более 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 фильтра на части;
-

– параметр равенства атрибуту. Индикатор того, что фильтрование событий будет учитывать наличие у события атрибутов, которым присвоен данный параметр;
- 

– параметр отрицания атрибута. Индикатор того, что в результатах поиска не будут отображены те события, для атрибутов которых выставлен данный параметр.

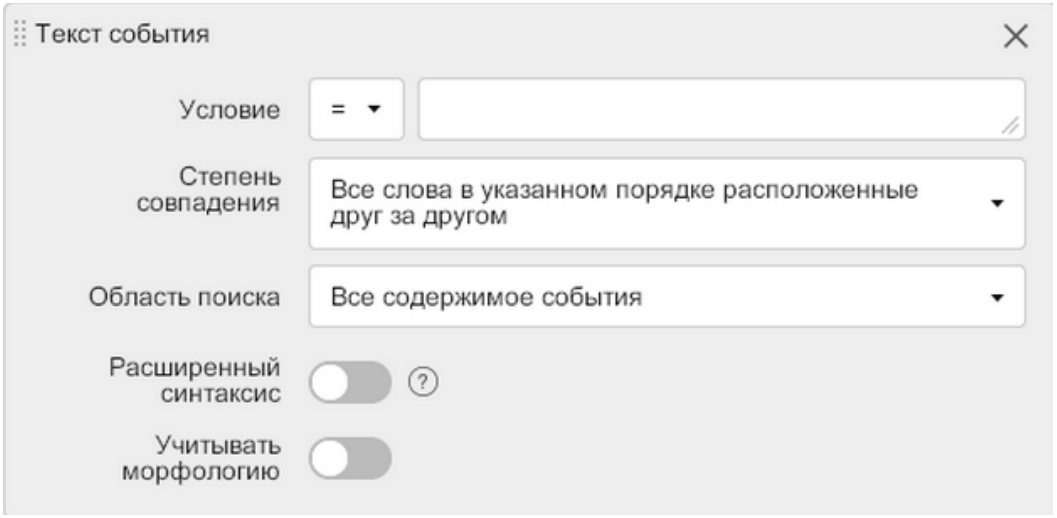
Также при создании запроса в расширенном режиме есть возможность гибкой настройки условий поиска по тексту события.

Целевые действия пользователя:

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

5.2.2.1.5 Поиск по тексту события

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



Параметры полнотекстового поиска:

Параметр	Описание
Условие	Параметр равенства атрибуту. Может принимать значения: = - индикатор того, что при фильтрации событий будет учитываться наличие атрибутов, которым присвоен данный параметр; ≠ - индикатор того, что из результатов поиска будут исключены события, для атрибутов которых выставлен данный параметр.

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".

Особенности задания условий для поиска:

- в качестве разделителя между словами используется пробел;
- регистр при поиске не учитывается;
- использование групповых символов ("*", "?") не допускается.

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").

5.2.2.2 Объекты перехвата

В списке событий отображаются события, удовлетворяющие условиям запроса.

Информация о событии представлена в следующих видах:

16. в плитке события (или записи о событии в таблице) отображается основная информация о событии;
17. в краткой форме просмотра события отображается наиболее часто требуемая информация;
18. в детальной форме просмотра события отображается наиболее полная информация об объекте перехвата.

Атрибуты объектов перехвата:

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
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
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)

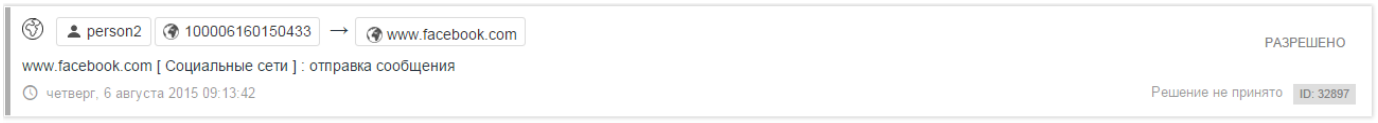
Уровень нарушения	Характеристика нарушения, присвоенная событию. Возможные варианты: • *Отсутствует* - обозначается на плитке серым (■) цветом; • *Высокий* - обозначается на плитке красным (■) цветом; • *Средний* - обозначается на плитке оранжевым (■) цветом; • *Низкий* - обозначается на плитке зеленым (■) цветом
Вердикт	Присвоенное в результате анализа Системой заключение по данному объекту. Возможные варианты: • *Разрешено* (пиктограмма) • *Заблокировано* (пиктограмма) • *Карантин* (пиктограмма)
Сервер перехвата	Имя сервера, которым был перехвачен объект.

См. также:

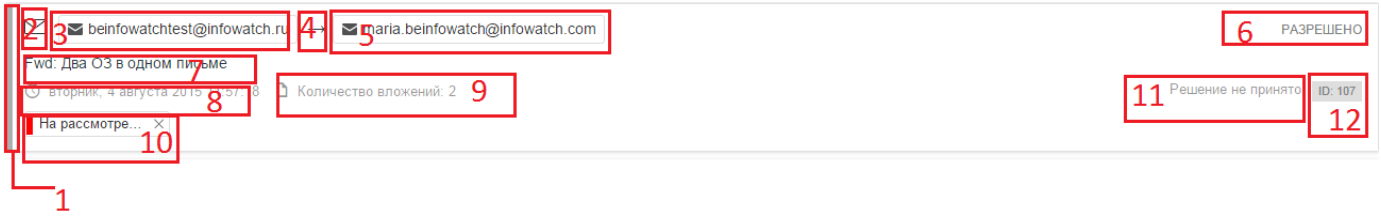
- "Плитка события" - о структуре элемента, выводящем информацию о событии по умолчанию.
- "Краткая форма просмотра событий" - о представлении общей информации о событии.
- "Детальная форма просмотра событий" - о представлении расширенной информации о событии.

5.2.2.2.1 Плитка события

Плитка события выглядит следующим образом:



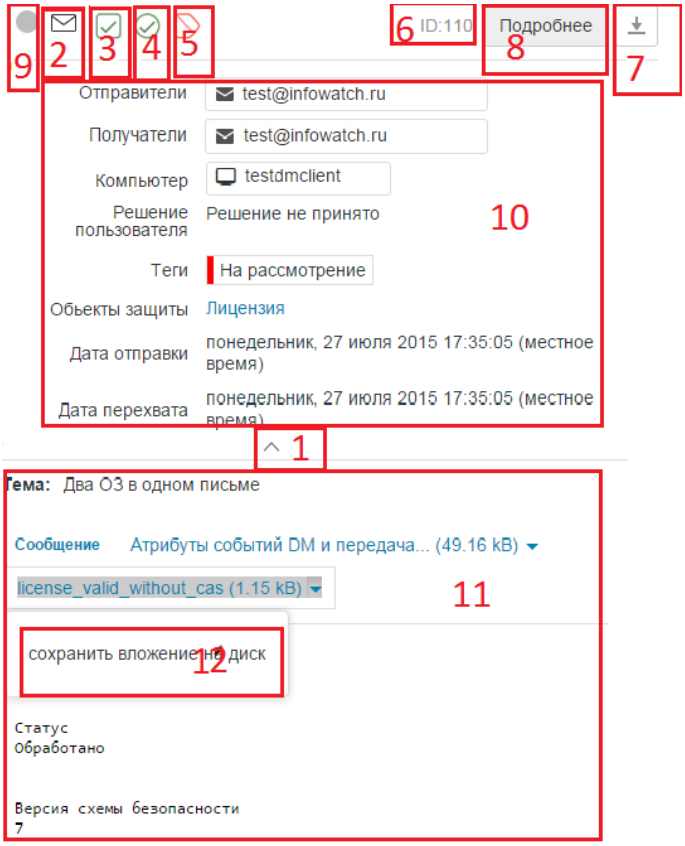
Плитка события состоит из следующих элементов:



где:
1 - Цвет уровня нарушения (возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует*)
2 - Тип события
3 - Отправитель (список отправителей)
4 - Направление трафика
5 - Получатель (список получателей)
6 - Вердикт (возможные значения: *Разрешено*, *Заблокировано*, *Карантин*)
7 - Превью события (краткая информация о причине возникновения события: в первом примере

это отправка сообщения в социальной сети, во втором - отправка письма)
8 - Дата и время создания события
9 - Индикатор вложений
10 - Присвоенные теги (см. "Теги")
11 - Решение пользователя (возможные значения: *Нарушение*, *Нет нарушения*, *Решение не принято*, *Требуется дополнительный анализ*)
12 - ID объекта

5.2.2.2.2 Краткая форма просмотра событий



Раздел **События**, краткая форма просмотра выбранного события

В краткой форме просмотра события отображаются следующие сущности:

№ на схеме	Сущность	Описание
1	Кнопка отображения/скрытия атрибутов события	Открывает или скрывает атрибуты события
2	Пиктограмма типа события	Отображает пиктограмму типа события
3	Решение пользователя	Отображает значение атрибута **Решение пользователя**. Возможные значения: *Нарушение*, *Нет нарушения*, *Решение не принято*, *Требуется дополнительный анализ*
4	Вердикт	Отображает значение атрибута **Вердикт**. Возможные значения: *Разрешено*, *Заблокировано*, *Карантин.*

5	Статус отправки	Отображает значение атрибута **Статус отправки**. Возможные значения: *Отправлено*, *Не отправлено*, *Ожидает отправки*.
6	ID объекта	Отображает значение атрибута **ID объекта**
7	Кнопка сохранения теневой копии	Кнопка, позволяющая сохранить событие на диск (см. "Сохранение события"). Отображается только для SMTP-писем.
8	Кнопка вызова детальной формы просмотра события	Открывает детальную форму просмотра события
9	Уровень нарушения	Отображает цветовое обозначение атрибута **Уровень нарушения**. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует.*
10	Атрибуты события	Извлеченные атрибуты объекта перехвата
11	Поле просмотра события и вложений	Отображает текст события и вложения
12	Команда **Сохранить вложение на диск**	Позволяет сохранить вложения на диск компьютера

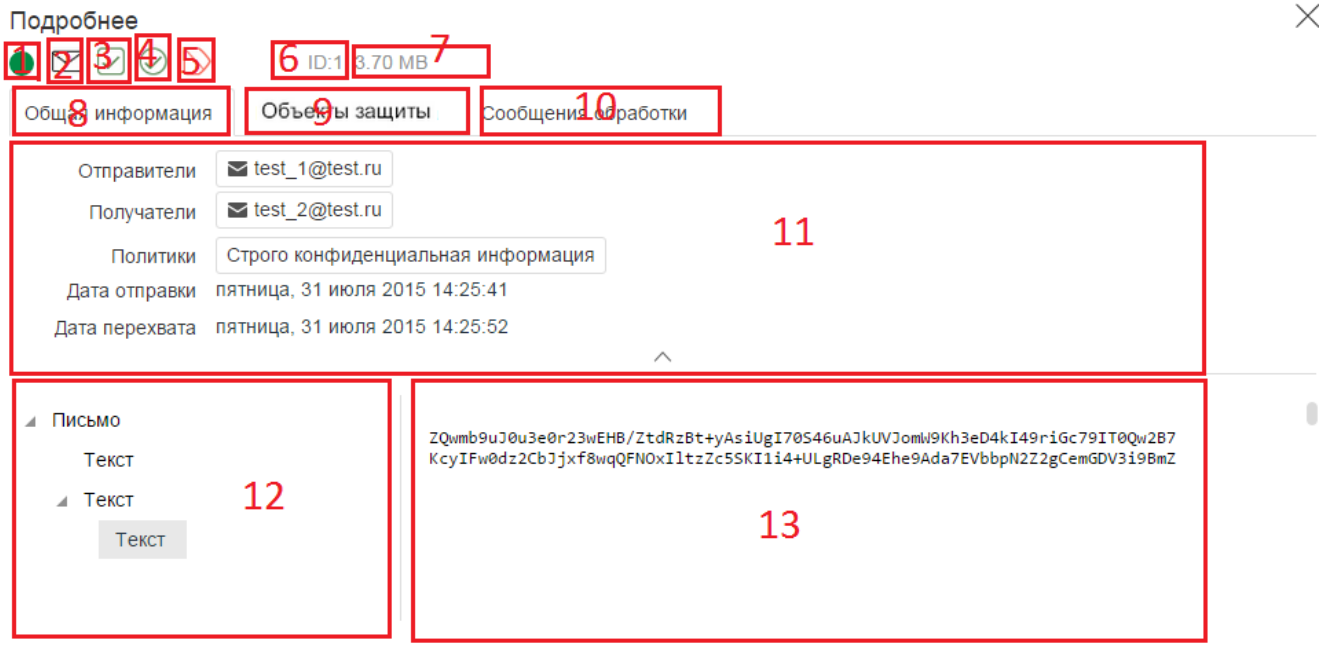
Примечание:

Набор объектов в краткой форме просмотра может различаться в зависимости от извлеченных атрибутов события.

Целевые действия пользователя:

- Ознакомление с общей информацией о событии (см. "Просмотр краткой формы события")

5.2.2.2.3 Детальная форма просмотра событий



Раздел **События**, детальная форма просмотра выбранного события, вкладка **Общая информация**

В детальной форме просмотра события содержатся следующие вкладки:

Вкладка	Назначение
Общая информация	Отображает общую информацию, представленную в краткой форме просмотра события
Объекты защиты	Отображает информацию о сработавших объектах защиты и входящих в них элементах анализа
Сообщения обработки	Отображает системные сообщения об этапах обработки объекта и возникших во время этого проблемах

В детальной форме просмотра события доступны следующие сущности:

№ на схеме	Сущность	Описание
1	Уровень нарушения	Отображает цветовое обозначение атрибута **Уровень нарушения**. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует.*
2	Тип события	Значение атрибута **Тип события**
3	Решение пользователя	Отображает значение атрибута **Решение пользователя**. Возможные значения: *Нарушение*, *Нет нарушения*, *Решение не принято*, *Требуется дополнительный анализ*.
4	Вердикт	Отображает значение атрибута **Вердикт**. Возможные значения: *Разрешено*, *Заблокировано*, *Карантин.*
5	Статус отправки	Отображает значение атрибута **Статус отправки**. Возможные значения: *Отправлено*, *Не отправлено*, *Ожидает отправки*.

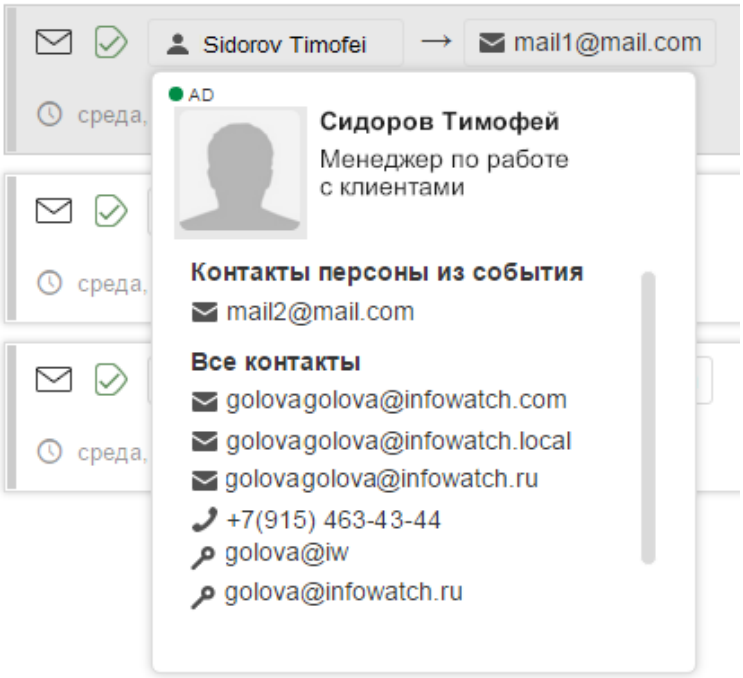
6	ID объекта	Значение атрибута **ID объекта**
7	Размер события	Значение атрибута **Размер события**
8	Вкладка **Общая информация**	Информация, представленная в краткой форме просмотра события
9	Вкладка **Объекты защиты**	Список сработавших объектов защиты и каталогов, в которых состояли данные объекты защиты на момент перехвата данных
10	Вкладка **Сообщения обработки**	Сообщения, возникшие при обработке объекта
11	Панель просмотра выбранной вкладки	Просмотр информации, в зависимости от выбранной вкладки (**Общая информация**, **Объекты защиты** или **Сообщения обработки**)
12	Панель с извлеченными атрибутами	Просмотр названий извлеченных из объекта атрибутов
13	Панель просмотра извлеченного атрибута	Просмотр извлеченных из объекта атрибутов

Целевые действия пользователя:

- Ознакомление с расширенной информацией о событии (см. "Просмотр детальной формы события")

5.2.2.3 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.



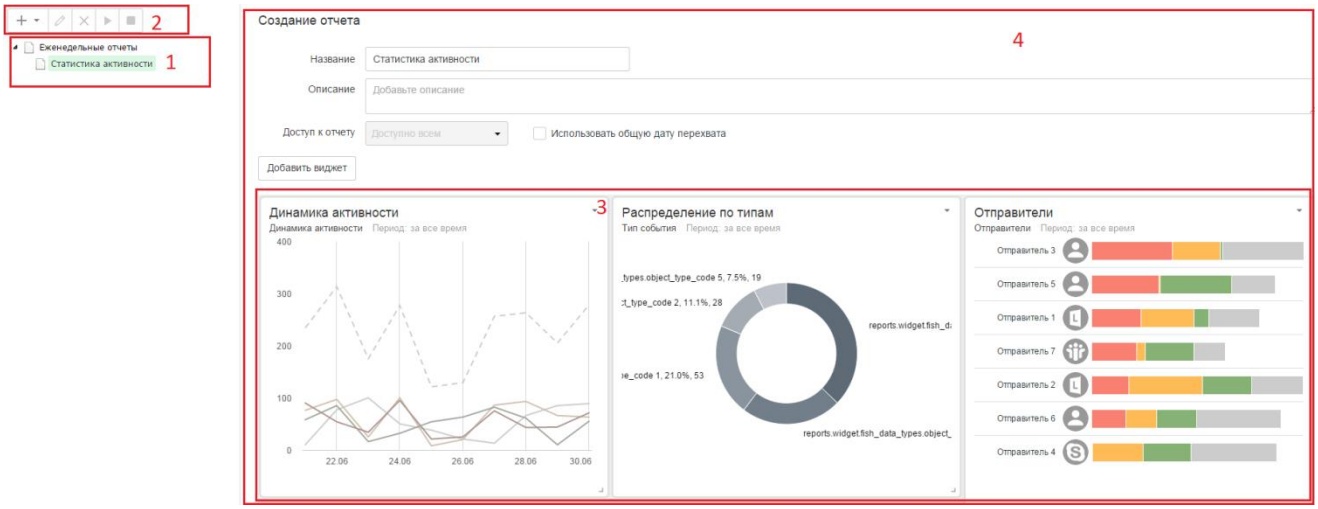
Если при обработке события Система определяет новые личные контакты персоны, найденные контакты автоматически добавляются в карточку персоны. Процесс автоматического добавление новых контактов имеющимся персонам называется ***пост-идентификацией***. В результате пост-идентификации в карточку персоны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

5.2.3 Раздел "Отчеты"

О разделе:

Раздел содержит выборку статистических данных о перехваченных объектах.

Статистическая информация отображается на виджетах в виде графиков и диаграмм. Каждый отчет может содержать один или несколько виджетов.



Раздел **Отчеты**

В разделе содержатся следующие элементы:

Номер на схеме	Элемент	Назначение
1	Раскрывающийся список папок с отчетами	Содержит список папок, в которых сгруппированных доступные отчеты
2	Панель инструментов для отчетов	Набор инструментов для работы с отчетами
3	Виджеты	Содержат графическое представление статистических данных о перехваченных объектах
4	Окно редактирования отчета	Содержит параметры отчета и добавленные виджеты

В папке **Предустановленные отчеты** содержатся следующие отчеты:

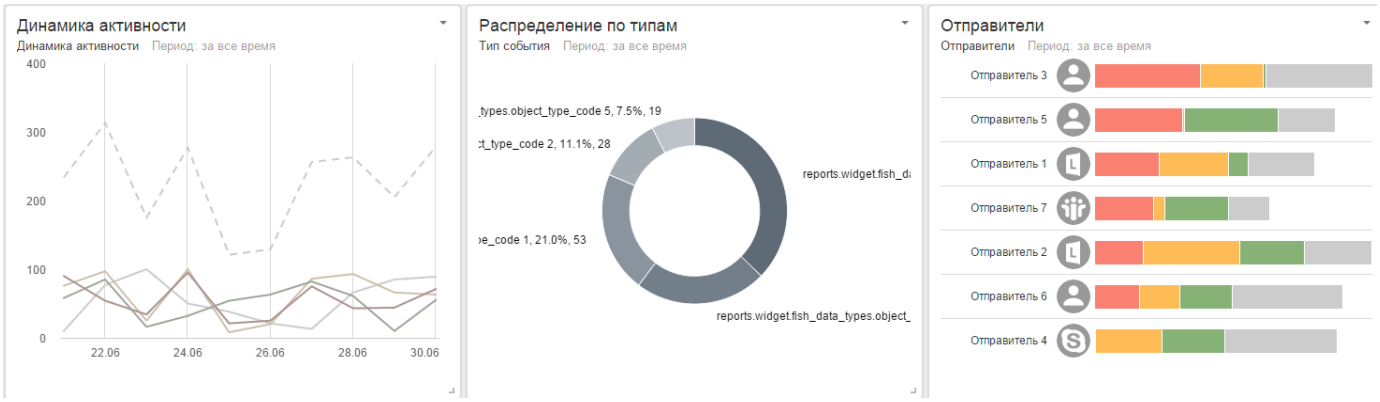
Отчет	Описание
Статистика активности за последние 7 дней	Показывает информацию о количестве перехваченных Системой событий, наиболее активных отправителях и получателях, а также о наиболее популярных контентных маршрутах отправителей-получателей
Активность в сети Интернет за последние 7 дней	Показывает, 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

Целевые действия пользователя:

- формирование отчета;
- настройка виджетов для отображения статистической информации;
- создание папки с отчетами;
- работа с готовыми отчетами.

5.2.3.1 Виджеты отчетов

В рабочей области раздела **Отчеты** отображаются виджеты.



Виджеты в разделе **Отчеты**

Виджеты предназначены для отображения статистической информации по перехваченным объектам за выбранный период времени.

Виджеты могут быть созданы для следующих данных:

Тип статистики	Описание
Тип события	Распределение количества событий по типам (почта, Skype, внешние устройства и т.д.)
Объекты защиты	Объекты защиты, наиболее часто встречающиеся в перехваченных Системой данных
Каталоги объектов защиты	Каталоги объектов защиты, наиболее часто встречающиеся в перехваченных Системой данных
Тематики сайтов	Тематики сайтов, на которые сотрудники отправляли наибольшее число запросов
Политики	Политики, наиболее часто применявшиеся к перехваченным данным
Динамика активности	Динамика количества событий, перехваченных Системой
Диалоги	Маршруты передачи сообщений (без учёта направления), для которых Системой зафиксировано наибольшее количество событий
Отправители	Отправители, для которых Системой зафиксировано наибольшее количество событий
Получатели	Получатели, для которых Системой зафиксировано наибольшее количество событий
Компьютеры	Компьютеры, для которых Системой зафиксировано наибольшее количество событий
Сайты	Сайты, на которые сотрудники отправляли наибольшее число запросов
Решения пользователей	Статистика решений, принятых офицером безопасности по событиям, перехваченным Системой

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 тип диаграммы "График". Для всех остальных типов статистики тип диаграммы "График" недоступен.

Параметры виджета для типа статистики "Динамика активности":

Параметр	Описание
Уровни нарушений	В виджет будут добавлены события с указанным уровнем нарушения. Поставьте галочки 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.
Число записей	Число записей, которые будут отображаться на виджете. Укажите значение от 1 до 100.
Объединить остальные записи в пункт "Другое"	Отметьте эту настройку, если Вы хотите, чтобы на виджет был добавлен элемент "Другое", объединяющий оставшиеся записи.
Показывать значения	Отметьте эту настройку, если Вы хотите, чтобы на виджете отображались количественные значения.
Показывать доли	Данная настройка доступна, если используется круговая диаграмма.

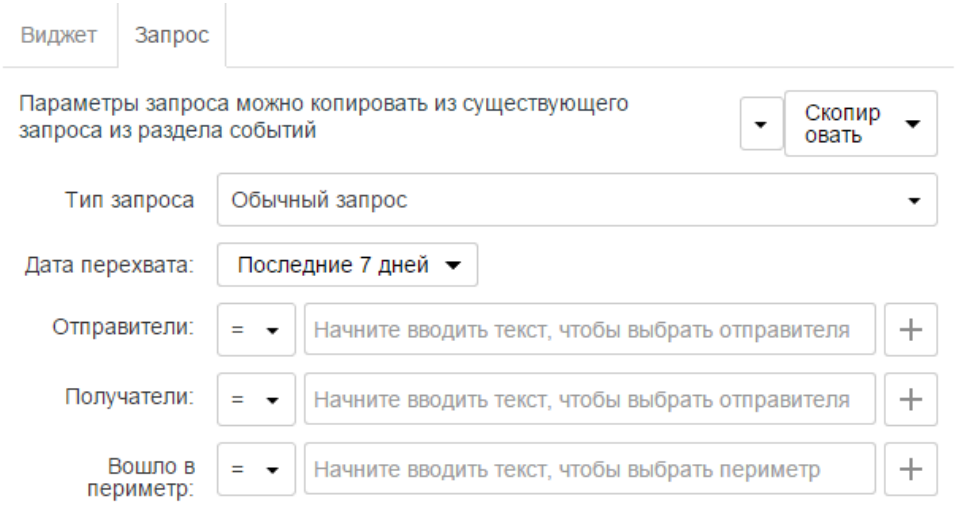
Целевые действия пользователя:

- настройка виджетов для отображения статистической информации (см. "Работа с виджетами отчетов")
- перемещение плиток виджетов (см. "Создание виджета")

5.2.3.2 Запросы

Запрос позволяет осуществить выборку объектов перехвата, которые будут отображаться на виджете.

Вы можете скопировать параметры запроса, добавленного в разделе **События**, либо создать новый запрос.



Вкладка **Запрос** в окне создания виджета

Запрос может быть создан в обычном либо в расширенном режиме.

В обычном режиме доступны следующие атрибуты:

Параметр	Описание
=	Параметр равенства атрибуту
≠	Параметр отрицания атрибута
Дата перехвата	Дата, когда было создано событие. По умолчанию будут показаны события за текущую неделю.
Отправители	Список отправителей объекта
Получатели	Список получателей объекта
Вошло в периметр	Периметр, в котором находится получатель трафика
Вышло из периметра	Периметр, в котором находится отправитель трафика

Рабочая станция	Рабочая станция, с которой был отправлен объект
Тип рабочей станции	Тип рабочей станции, с которой был отправлен объект. Возможные значение: компьютер или мобильное устройство
Ресурсы	Ресурс, на котором хранился объект

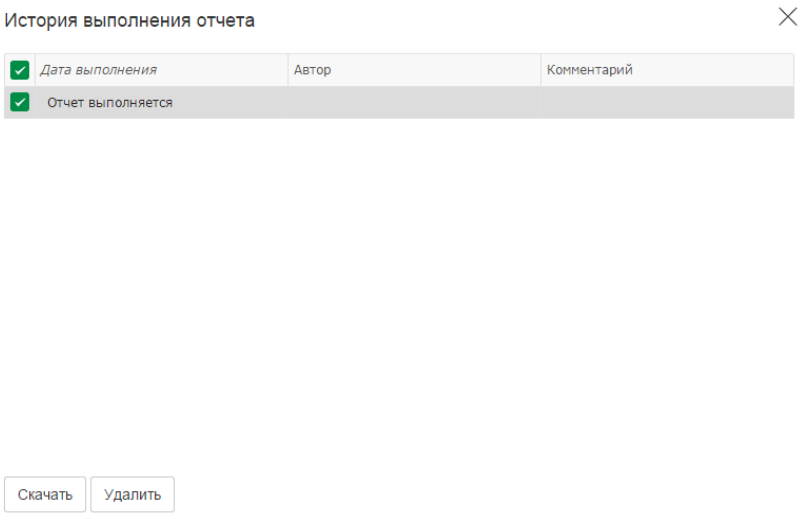
В расширенном режиме Вы можете выполнить более гибкую настройку условий поиска (подробнее см. "Расширенный режим").

Целевые действия пользователя:

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

5.2.3.3 История выполнения отчета

История выполнения отчета требуется для просмотра выполненных отчетов, удалении ненужных версий отчета и сохранения выбранных версий в файл.



Атрибуты истории выполнения отчета:

Параметр	Описание
Дата выполнения	Дата и время выполнения отчета
Автор	Пользователь, запустивший выполнение отчета
Комментарий	Комментарий к отчету, добавленный пользователем

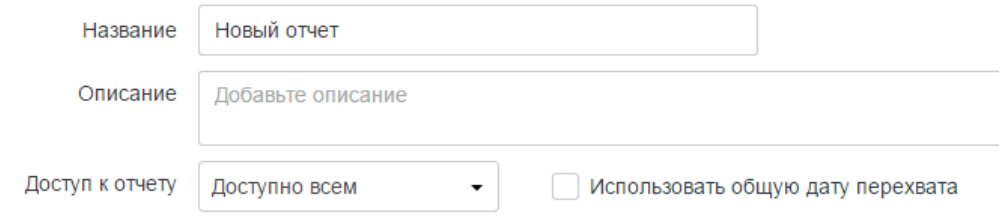
Целевые действия пользователя:

- просмотреть историю выполнения отчета, при необходимости удалить выбранные версии отчета или сохранить их в файл (подробнее см. "Работа с готовыми отчетами").

5.2.3.4 Окно создания отчета

В левой части рабочей области раздела **Отчеты** отображается список папок, содержащих отчеты.

Отчеты позволяют сформировать статистику на основе данных, хранящихся в Системе.



Атрибуты отчета:

Параметр	Описание
Название	Название отчета
Описание	Описание в произвольной форме
Доступ к отчету	Укажите, будет ли созданный отчет доступен всем пользователям либо только владельцу
Использовать общую дату перехвата	Установите флажок в этом поле, если Вы хотите, чтобы указанная дата перехвата использовалась для всех добавленных запросов. При выборе данной настройки появится выпадающий список, в котором Вы можете указать требуемый период.

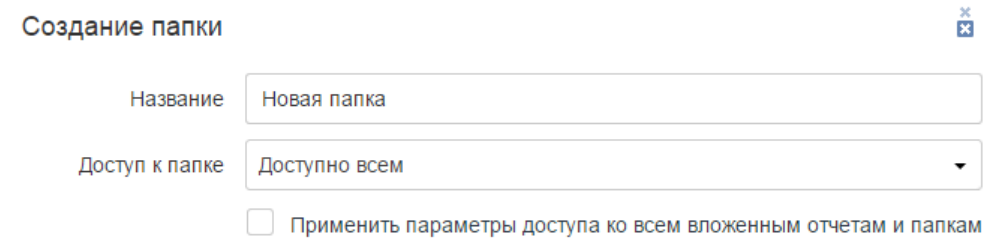
Целевые действия пользователя:

- Создание отчета

5.2.3.5 Форма создания папки с отчетами

В левой части рабочей области раздела **Отчеты** отображается список папок.

Папки позволяют группировать отчеты по какому-либо признаку, наследовать права доступа, а также копировать выбранную группу отчетов.



Атрибуты папки:

Параметр	Описание
Название	Название папки
Доступ к папке	Укажите, будет ли созданная папка доступна всем пользователям либо только владельцу
Применить параметры доступа ко всем вложенным отчетам и папкам	Установите флажок в этом поле, если Вы хотите, чтобы указанный режим доступа наследовался для вложенных папок и отчетов

Целевые действия пользователя:

- Создание папки с отчетами

5.2.4 Раздел "Технологии"

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

О разделе:
Раздел содержит редактируемые выгрузки из БД.

В разделе содержатся следующие элементы:

Элемент	Назначение
Вкладки с типами справочников: • Список выгрузок из БД	Содержат списки элементов и инструменты для выбранного справочника
Панель инструментов	Набор инструментов для работы с выбранным справочником
Панель навигации по страницам	Набор кнопок для просмотра страниц, содержащих записи (в случае, если не все записи помещаются на одной странице)
Регулятор количества записей	Раскрывающийся список, в котором устанавливается количество записей на странице

Целевые действия пользователя:

- Формирование списка выгрузок из БД (см. "Создание эталонных выгрузок из БД")

5.2.4.1 Выгрузки из БД

Справочная информация:
Эталонная выгрузка из БД - часть базы данных, цитаты из которой ищутся в анализируемом тексте. Эталонными выгрузками из БД могут быть списки заработных плат сотрудников, личные данные и прочее.

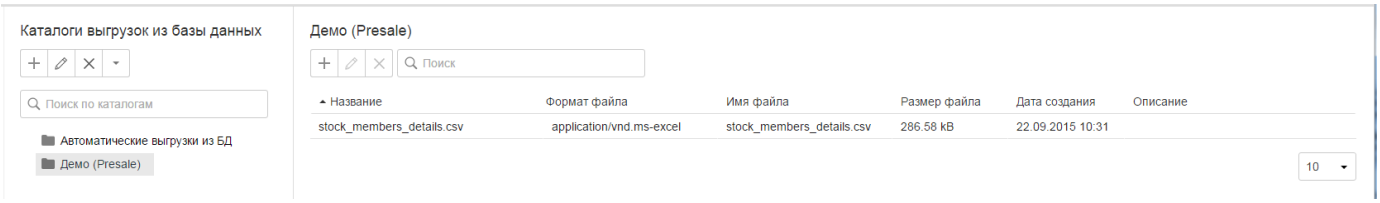
Важно!

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

- 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).

Эталонные выгрузки создаются внутри каталогов. Для работы с каталогами выгрузок (создание, редактирование, удаление каталога; поиск по каталогам) используются инструменты в левой части

рабочей области. Эталонные выгрузки, входящие в каталог, и инструменты для работы с выгрузками расположены в правой части рабочей области.



Предустановленный каталог **Автоматические выгрузки из БД** содержит эталонные 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.

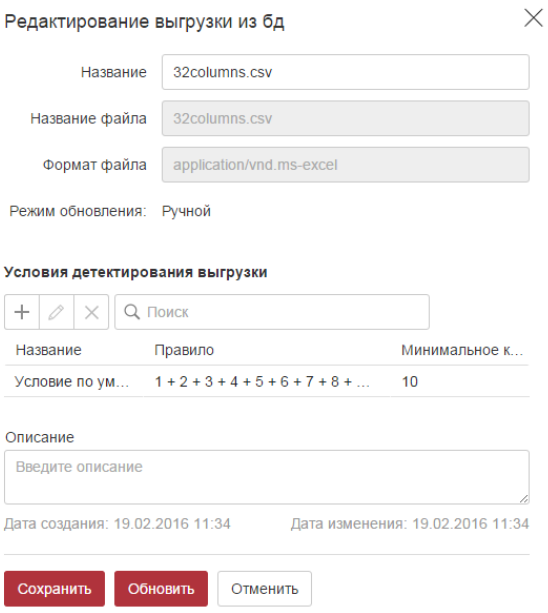
Добавление файла эталонной выгрузки в каталог выполняется с помощью кнопки  на панели инструментов в правой части рабочей области.

При загрузке файла эталонной 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.

Редактирование свойств добавленной эталонной выгрузки выполняется с помощью кнопки  на панели инструментов в правой части рабочей области. В открывшемся окне Вы можете просмотреть и при необходимости изменить атрибуты выбранной выгрузки.

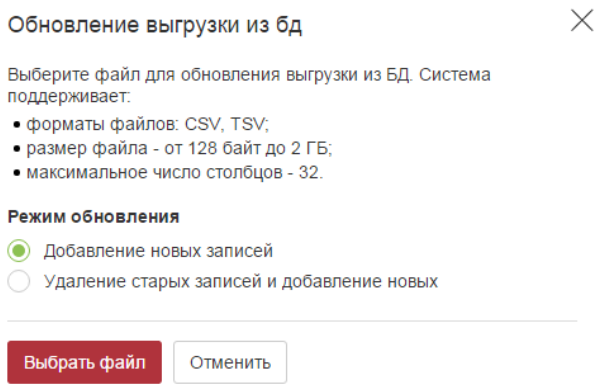


Атрибуты эталонной выгрузки из БД:

Параметр	Описание
Название	Наименование эталонной выгрузки
Название файла	Название файла, загруженного в качестве эталонной выгрузки из БД
Формат файла	Разновидность файла
Режим обновления	Возможные варианты: **Ручной** или **Автоматический**
Описание	Примечание в произвольной форме
Дата создания	Дата и время создания выгрузки
Дата изменения	Дата и время последнего изменения выгрузки. Данный атрибут отображается только при переходе в режим редактирования выгрузки
Условия детектирования выгрузки	Описание логических взаимоотношений между столбцами таблицы и минимальное количество непустых строк в таблице, требуемое для срабатывания эталонной выгрузки.

В области **Условия детектирования выгрузки** отображается панель инструментов для работы с условиями и список добавленных условий.

Переход в режим обновления эталонной выгрузки выполняется с помощью кнопки **Обновить** в окне редактирования выгрузки.



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

Целевые действия пользователя:

- создание эталонных выгрузок из БД и их каталогов (см. "Работа с эталонными выгрузками")
- обновление эталонной выгрузки (см. "Работа с эталонными выгрузками")
- добавление условий детектирования выгрузки (см. "Условия детектирования выгрузки")
- автоматическое обновление эталонной выгрузки (см. "Автоматическое создание и обновление эталонной выгрузки")
- добавление эталонных выгрузок в объекты защиты ("Создание объекта защиты")

5.2.4.1.1 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.

Эталонные выгрузки, созданные внешней системой, помещаются в предустановленный каталог **Автоматические выгрузки из БД**. Авторизация внешней системы в TMFD осуществляется с помощью плагина.

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 эталонные выгрузки в каталог **Автоматические выгрузки из БД** вручную с помощью кнопки  на панели инструментов в правой части рабочей области. Для эталонных выгрузок, добавленных вручную, обновление будет выполняться стандартным способом (см. "Создание эталонных выгрузок из БД").

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 эталонных 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 эталонной выгрузки, созданной внешней системой, автоматическое обновление данной выгрузки будет недоступно.

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

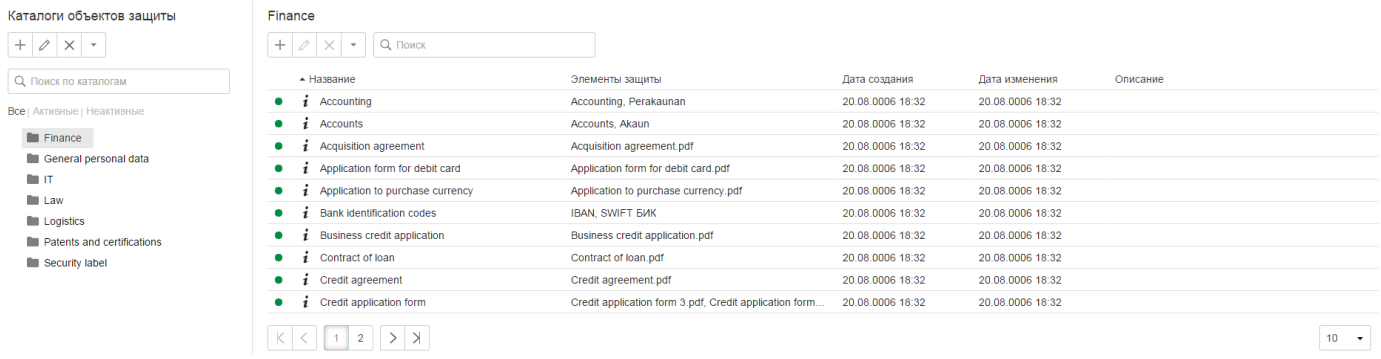
5.2.5 Раздел "Объекты защиты"

Справочная информация:

Объект защиты представляет собой совокупность элементов анализа содержимого событий. Объекты защиты используются для определения соответствия перехваченных данных определенным бизнес-документам.

О разделе:

Раздел содержит список событий (объектов перехвата) и средства для работы с ними.



В разделе содержатся следующие элементы:

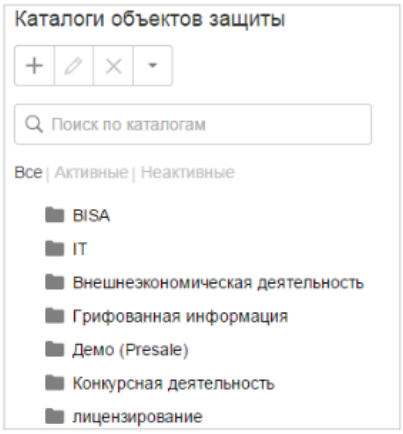
Элемент	Назначение

Каталоги объектов защиты	Список добавленных каталогов, содержащих объекты защиты. Расположен в левой части рабочей области
Объекты защиты	Список объектов защиты, содержащихся в выбранном каталоге. Отображается при выборе каталога
Панель инструментов	Набор инструментов для объектов защиты и их каталогов
Поле Поиск	Фильтрация объектов защиты
Панель навигации по страницам	Набор кнопок для просмотра страниц, содержащих записи (в случае, если не все записи помещаются на одной странице). Вы можете перейти к следующей или предыдущей странице, переместиться в начало или конце списка, либо перейти на страницу с выбранным номером.
Регулятор количества записей	Раскрывающийся список, в котором устанавливается количество записей на странице

Список каталогов содержит предустановленные каталоги объектов защиты. Для предустановленных объектов защиты указаны используемые элементы анализа и условия обнаружения.

5.2.5.1 Каталоги объектов защиты

В левой части рабочей области раздела **Объекты защиты** содержится список каталогов, панель инструментов для работы с каталогами и поле поиска по каталогам.



Атрибуты каталога объектов защиты:

Параметр	Описание
Название	Название каталога
Статус	Является ли каталог активным. Указанный статус будет применен ко всем вложенным дочерним каталогам и входящим в них объектам защиты.
Описание	Описание в произвольной форме
Дата создания	Дата и время создания каталога

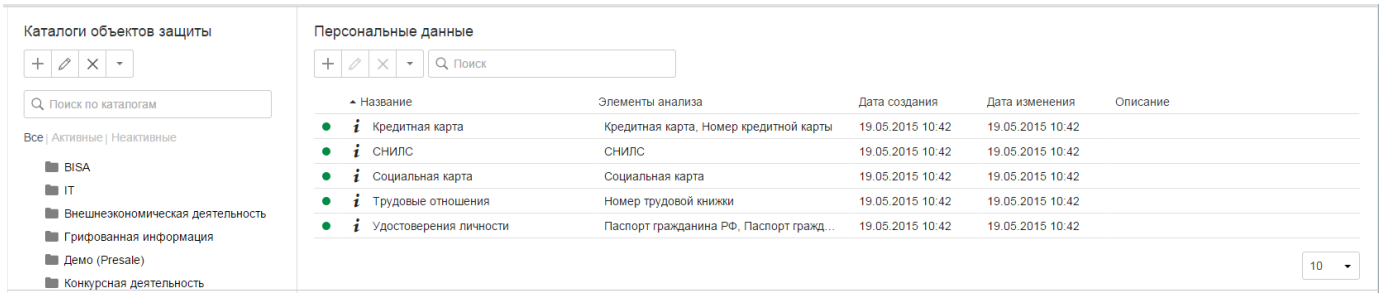
Дата изменения	Дата и время последнего изменения каталога

Целевые действия пользователя:

- Создание каталога объектов защиты
- Создание политики для каталога объектов защиты
- Импорт и экспорт объектов защиты

5.2.5.2 Объекты защиты

В правой части рабочей области отображаются объекты защиты для выбранного каталога, панель инструментов для работы с объектами защиты и поле поиска.



Параметры объекта защиты:

Параметр	Описание
Название	Название объекта защиты
Статус	Является ли объект защиты активным
Элементы анализа	Элементы анализа, входящие в объект защиты
Описание	Описание в произвольной форме
Дата создания	Дата и время создания объекта защиты
Дата изменения	Дата и время последнего редактирования объекта защиты

При создании нового объекта защиты (кнопка  на панели инструментов) отображается окно добавления элементов анализа.

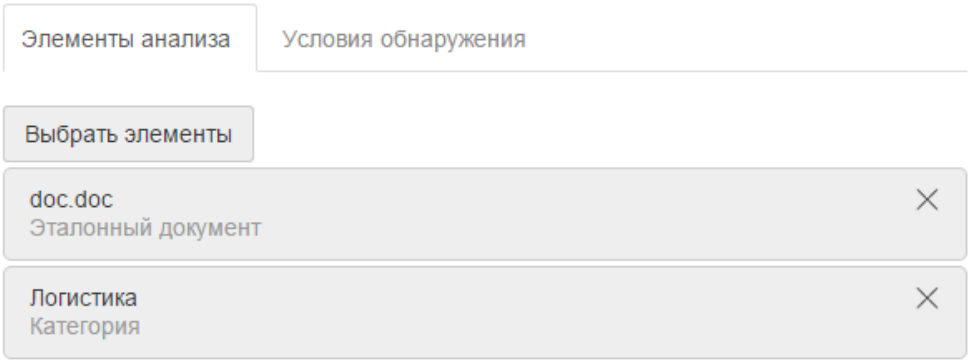
При нажатии на кнопку  на панели инструментов открывается окно редактирования выбранного объекта защиты, содержащее вкладки Элементы анализа и Условия обнаружения.

Целевые действия пользователя:

- Создание объекта защиты
- Добавление элементов анализа в объект защиты
- Создание политики для объекта защиты

5.2.5.2.1 Элементы анализа

Справочная информация:
Элементы анализа - элементы настройки технологий, на основе которых формируются объекты защиты (выгрузки из БД).



Раздел **Объекты защиты**, вкладка **Элементы анализа** при создании или редактировании объекта защиты

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

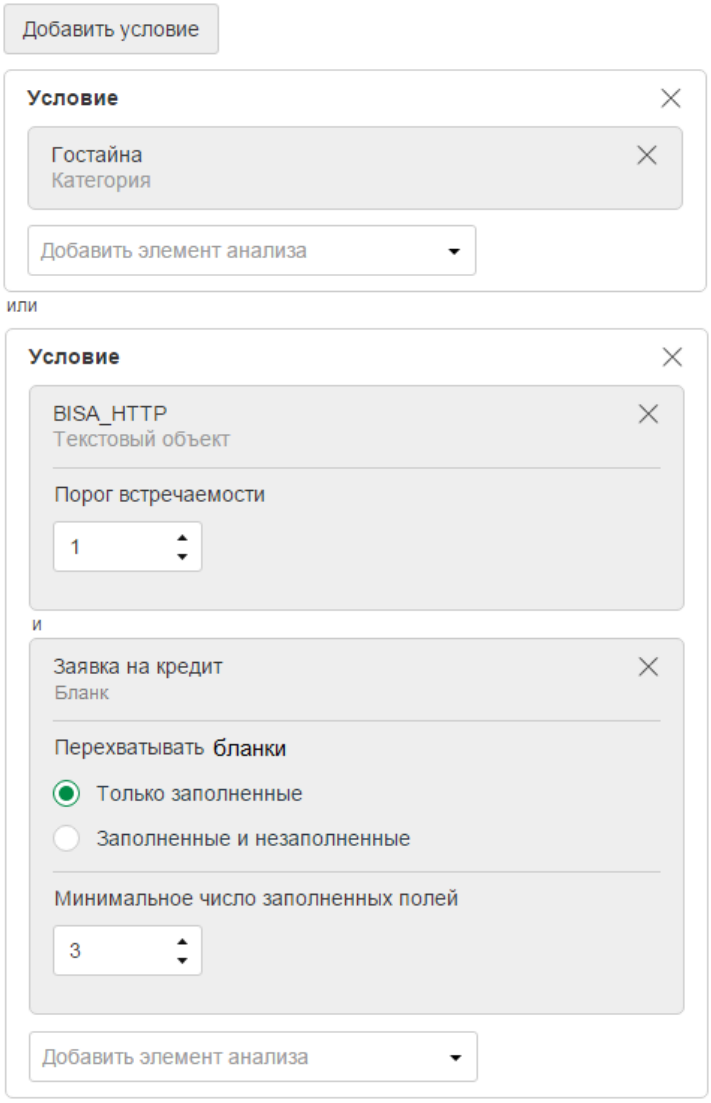
На вкладке **Элементы анализа** вы можете добавить дополнительные элементы в объект защиты (кнопка **Выбрать элементы**) или удалить элемент анализа (кнопка X в правом верхнем углу панели элемента).

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

Целевые действия пользователя:

- Добавление элементов анализа

5.2.5.2.2 Условия обнаружения



Вкладка **Условия обнаружения**, отображаемая при создании или редактировании объекта защиты

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

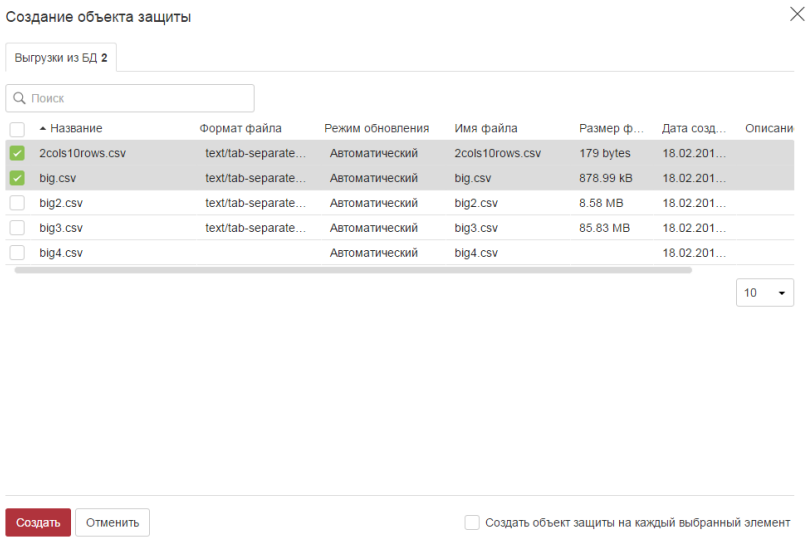
Условия обнаружения могут быть добавлены внутри одного блока и объединены с помощью операции конъюнкции (логическое "И"), либо добавлены в различные блоки, объединенные между собой с помощью операции дизъюнкции (логическое "ИЛИ").

См. также: Элементы анализа

Целевые действия пользователя:

- Добавление условий обнаружения

5.2.5.2.3 Окно добавления элементов анализа



Раздел **Объекты защиты**, окно добавления элементов анализа при создании или редактировании объекта защиты

Окно добавления элементов анализа отображается при создании нового объекта защиты либо при нажатии кнопки **Выбрать элементы** на вкладке **Элементы анализа**. Элементы в окне сгруппированы на вкладках. При нажатии на вкладку отображается список доступных элементов.

Окно добавления элементов анализа содержит следующие вкладки:

- *Выгрузка из базы данных* - список доступных выгрузок из базы данных.

Подробнее об элементах анализа см. "Определение конфиденциальной информации".

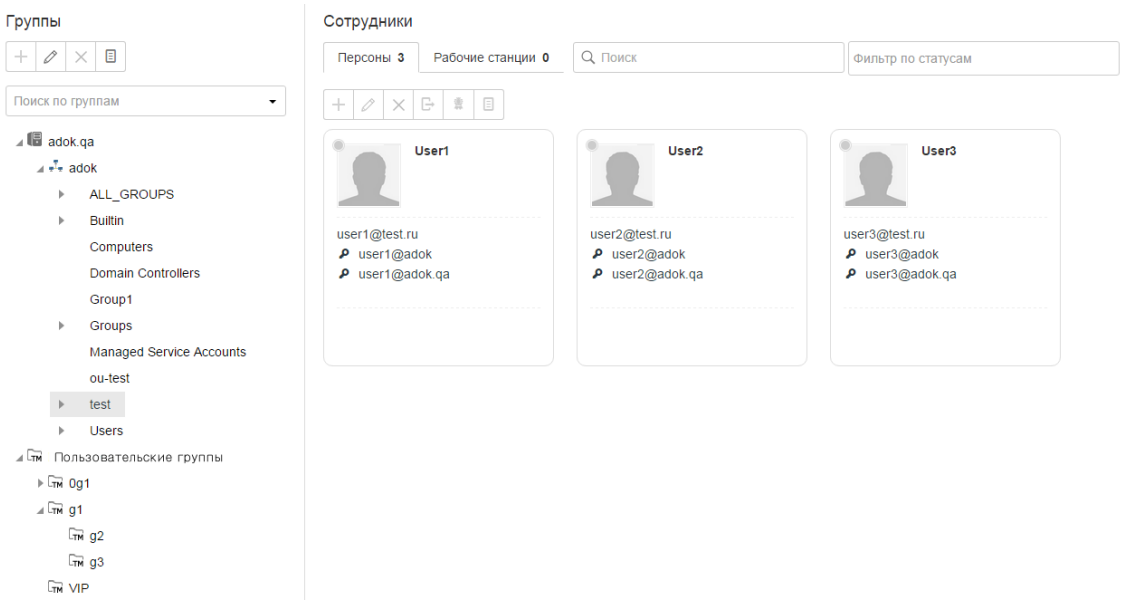
Примечание.

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

5.2.6 Раздел "Персоны"

Справочная информация:
Наличие списков персон и рабочих станций облегчает офицеру безопасности работу с перехваченными объектами. Это происходит за счет учета информации об отправителях и получателях (персонах), а также рабочих станциях с помощью специальных справочников.

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



Раздел **Персоны**

Важно!

При превышении допустимого в текущей лицензии количества персон, события от которых обрабатываются, в верхней части окна браузера отображается сообщение вида: **Внимание! Лицензионный порог кол-ва сотрудников, события от которых обрабатывает Система, превышен на 1.**

Данное сообщение имеет информационный характер и не влияет на работоспособность Системы.
Количество персон, события от которых обрабатываются в Системе, соответствует количеству персон, которые за последние 30 дней отправляли какой-либо тип трафика.
Допустимое в текущей лицензии количество персон отображается в сведениях о лицензии, в атрибуте **Лицензировано пользователей**.

В разделе содержатся следующие элементы:

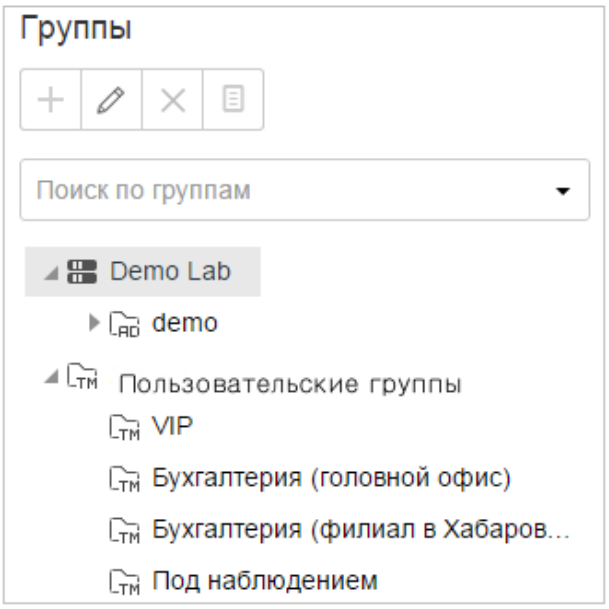
Элемент	Назначение
Группы персон/рабочих станций из Active Directory	Расположен в левой части рабочей области. Содержит структуру организации, полученную из Active Directory.
Группы персон/рабочих станций из Domino Directory	Расположен в левой части рабочей области. Содержит структуру организации, полученную из Domino Directory.
Группы персон/рабочих станций, созданные средствами TMFD	Расположен в левой части рабочей области. Содержит структуру организации, созданную средствами TMFD.
Вкладка **Персоны** для выбранной группы	Расположен в правой части рабочей области. Содержит список персон, входящих в выделенную группу.
Вкладка **Рабочие станции** для выбранной группы	Расположен в правой части рабочей области. Содержит список рабочих станций, входящих в выделенную группу.

Панели инструментов	Набор инструментов для групп, персон и рабочих станций
Поле **Поиск по группам**	Фильтрация групп персон и рабочих станций
Поле **Поиск**	Фильтрация персон и рабочих станций
Поле **Фильтр по статусам**	Фильтрация персон и рабочих станций по атрибуту **Статус**. Доступен только для групп персон и рабочих станций, полученных из Active Directory

Целевые действия пользователя:

- Создание группы персон и рабочих станций (см. "Создание группы персон и рабочих станций")
- Создание списка персон и рабочих станций (см. "Создание списка персон и рабочих станций")
- Просмотр виджетов с информацией о персонах и рабочих станциях (см. "Просмотр сводки по персоне/рабочей станции")
- Создание фильтра по персонам и рабочим станциям (см. "Просмотр событий по персоне/рабочей станции")
- Формирование политики для персон и рабочих станций (см. "Добавление персоны/рабочей станции в политику")
- Работа со статусами персон и рабочих станций (см. "Добавление статуса персоне/рабочей станции")
- Добавление персон и рабочих станций в периметры (см. "Добавление персоны/рабочей станции в периметр компании")

5.2.6.1 Группы персон и рабочих станций



Примечание:

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

.

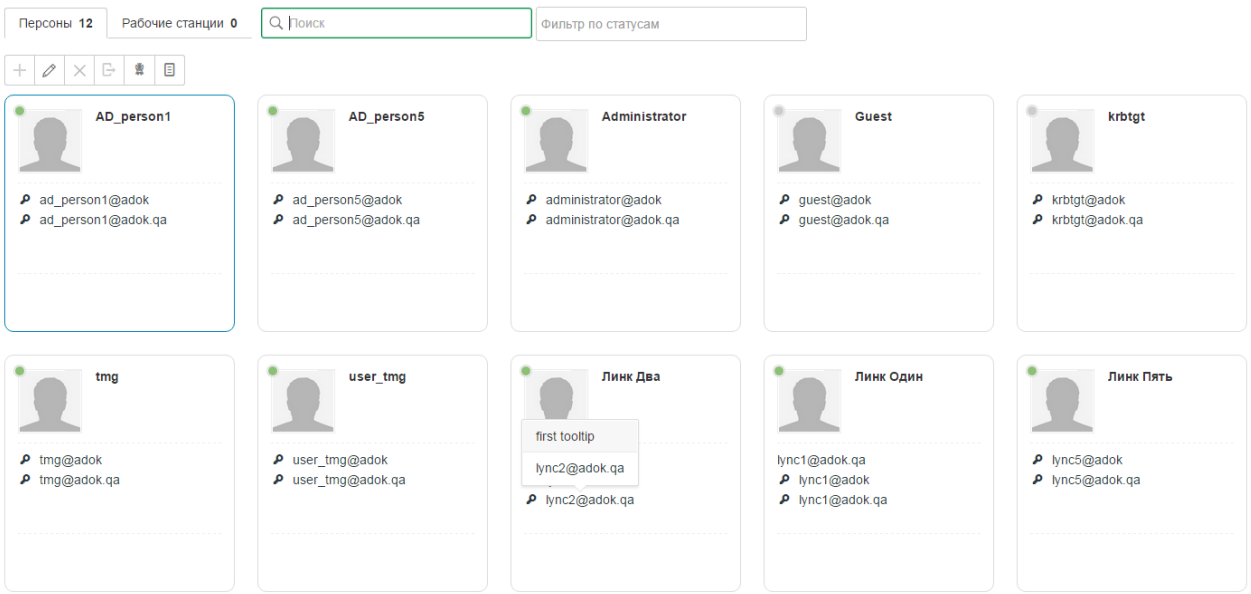
Атрибуты группы персон и рабочих станций:

Параметр	Описание
Имя	Наименование группы
Контакты	Контактные данные группы
Содержит группы	Список групп, входящих в данную группу
Входит в группы	Список групп, в которые входит данная группа
Примечание	Описание в произвольной форме

Целевые действия пользователя:

- Создание группы персон и рабочих станций

5.2.6.2 Персоны



Примечание:

Для персон, данные которых импортированы из Active Directory, отображается цветовой индикатор в левом верхнем углу фотографии профиля:

- для активных сотрудников;
- для сотрудников, отключенных в AD.

Атрибуты персоны:

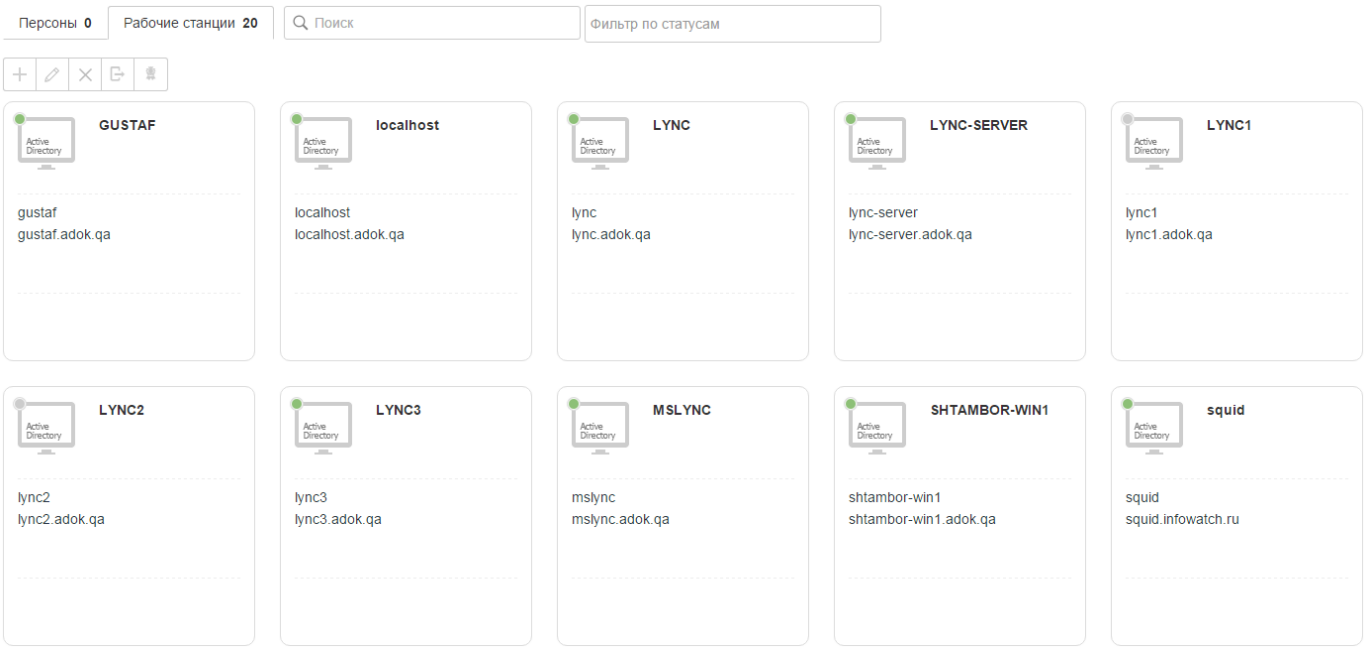
Параметр	Описание

Фамилия	Фамилия персоны
Имя	Имя персоны
Сотрудник/Не сотрудник	Индикатор того, является ли персона сотрудником компании
Должность	Должность персоны
Отдел	Отдел, в котором работает персона
Комната	Комната, в которой работает персона
Руководитель	Руководитель персоны
Примечание	Произвольное описание
Контакты	Контакты персоны (офицер безопасности может указать домашние или рабочие контакты, включая адрес электронной почты, номер телефона, логин Skype, ICQ или адрес сайта в Интернет)
Группы	Группы, в которые включена персона
Рабочие станции	Рабочие станции, привязанные к учетной записи персоны
Статусы	Статус, который присваивает персоне офицер безопасности
Фото	Фотография персоны

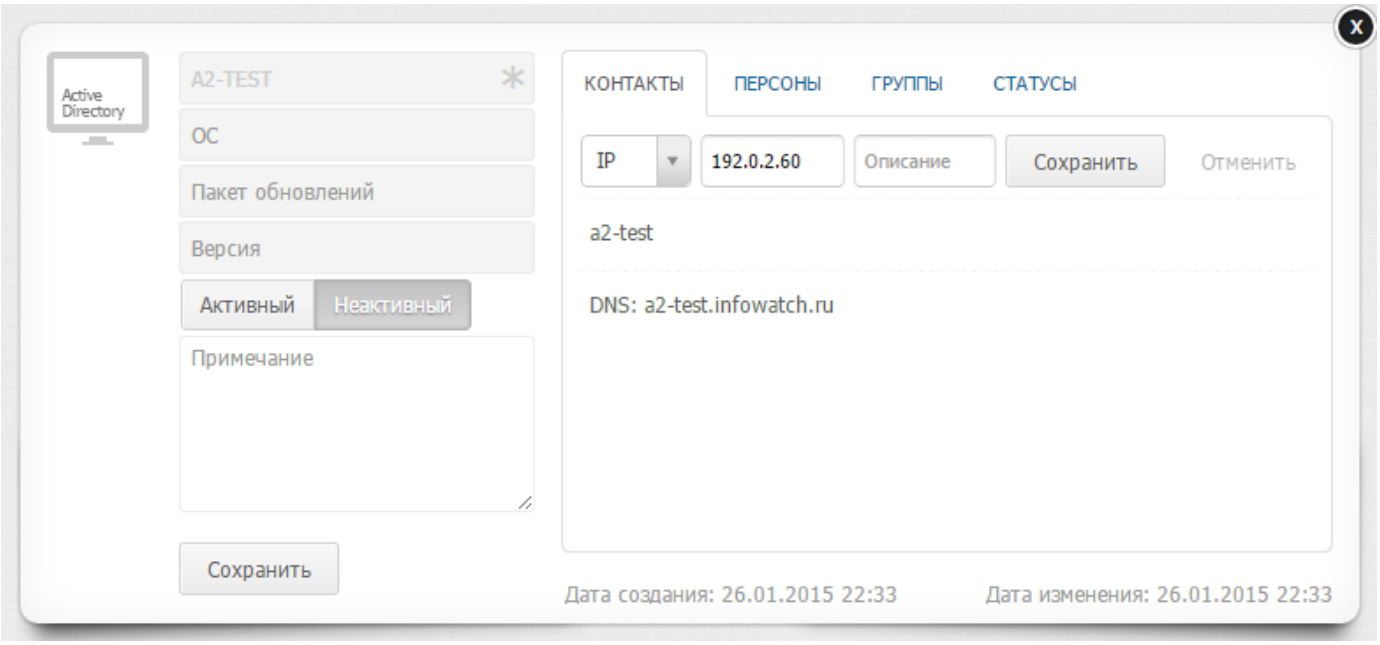
Целевые действия пользователя:

- Работа с группами персон (см. "Создание группы персон и рабочих станций")
- Просмотр виджетов с информацией о персонах (см. "Просмотр сводки по персоне/рабочей станции")
- Создание фильтра по персонам (см. "Просмотр событий по персоне/рабочей станции")
- Настройка карточки персоны ("Настройка карточки персоны")
- Формирование политики для персон (см. "Добавление персоны/рабочей станции в политику")
- Работа со статусами персон (см. "Добавление статуса персоне/рабочей станции")
- Добавлены персоны в периметр (см. "Добавление персоны/рабочей станции в периметр компании")

5.2.6.3 Рабочие станции



Пример списка рабочих станций



Пример диалога редактирования рабочей станции

Атрибуты рабочей станции:

Параметр	Описание
Имя	Наименование рабочей станции
Примечание	Произвольное описание

Контакты	Идентификатор рабочей станции в сети: • IP • DNS В первом из двух полей необходимо указать IP или DNS-имя (в зависимости от выбранной настройки). Во втором поле, если необходимо, оставьте свой комментарий.
Персоны	Персоны, к учетным записям которых привязана рабочая станция
Группы	Группы, включающие рабочую станцию
Статус	Статус, который офицер безопасности назначает рабочей станции

Целевые действия пользователя:

- Работа с группами рабочих станций (см. "Создание группы персон и рабочих станций")
- Работа с рабочими станциями (см. "Создание списка персон и рабочих станций")
- Просмотр виджетов с информацией о рабочих станциях (см. "Просмотр сводки по персоне/рабочей станции")
- Создание фильтра по рабочим станциям (см. "Просмотр событий по персоне/рабочей станции")
- Формирование политики для рабочих станций (см. "Добавление персоны/рабочей станции в политику")
- Работа со статусами рабочих станций (см. "Добавление статуса персоне/рабочей станции")
- Определение рабочих станций, входящих в периметры (см. "Добавление персоны/рабочей станции в периметр компании")

5.2.7 Раздел "Политики"

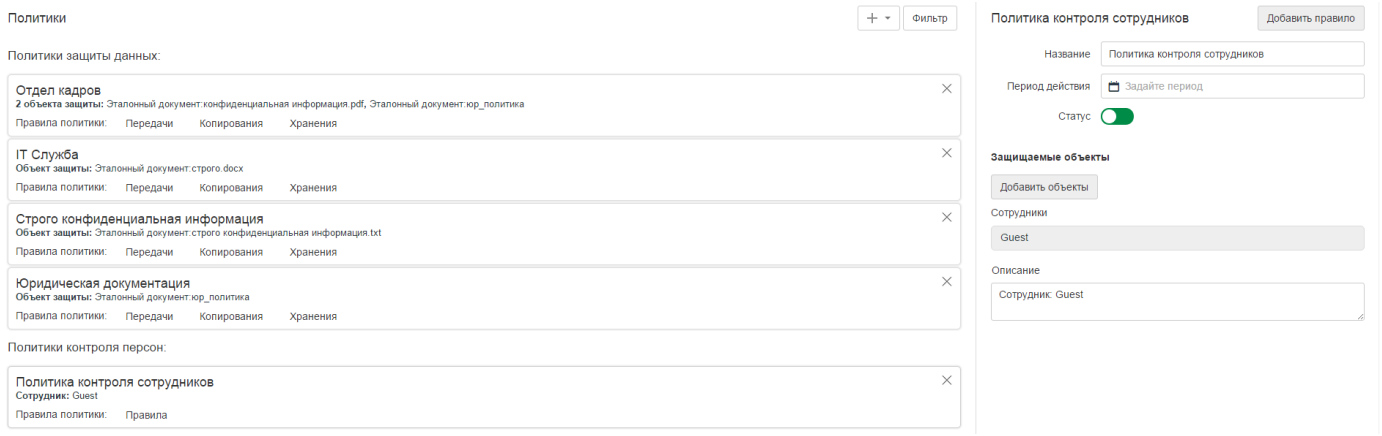
Справочная информация:
Политики - совокупность *правил*, в соответствии с которыми проводится анализ и обработка объектов перехвата. ***Правило*** состоит из набора условий, по которым выполняется проверка объекта, и действий, осуществляемых при выполнении или невыполнении заданных условий.

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 действий, которые выполняет Система в ответ на действия персон и рабочих станций.



В разделе содержатся следующие элементы:

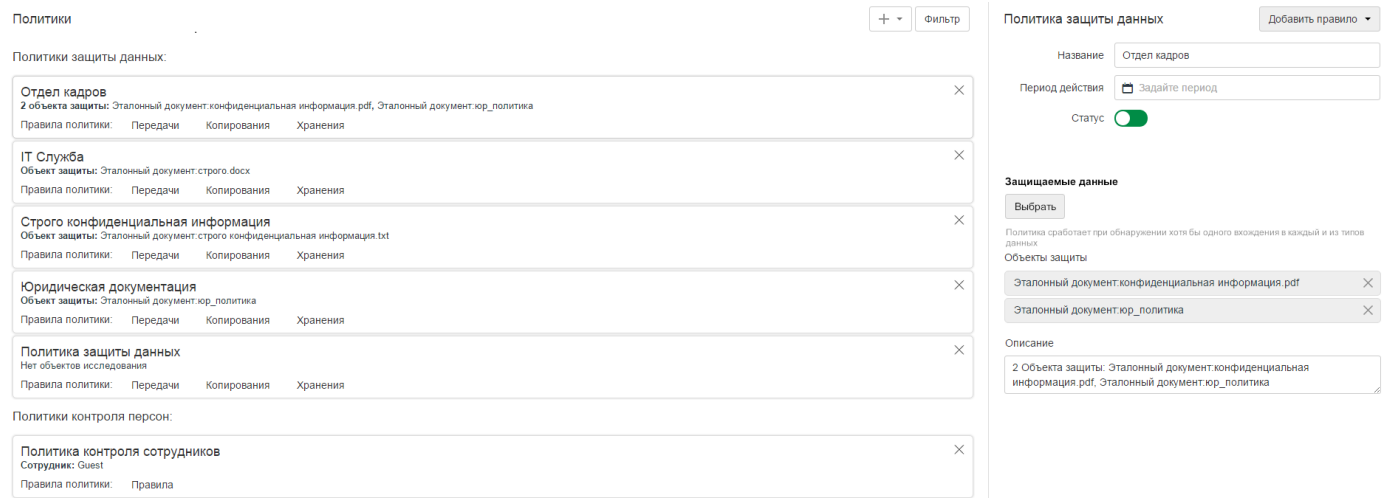
Элемент	Назначение
Список политик	Содержит доступные политики. Политики в списке разделены на две группы: политики защиты данных и политики контроля персон.
Форма просмотра политики	Содержит атрибуты выбранной политики
Форма просмотра правила	Позволяет настроить правило для выбранной политики
Кнопка **Фильтр**	Отображает область **Настройка фильтра**
Область **Настройка фильтра**	Позволяет отфильтровать политики по указанным атрибутам
Кнопка добавления политики 	Позволяет выбрать тип политики в раскрывающемся списке. Доступные значения: • Политика защиты данных • Политика контроля персон Для добавленной политики в правой части рабочей области отображается форма ее просмотра
Форма просмотра политики	Позволяет указать параметры созданной политики

Целевые действия пользователя:

- Добавление новой политики (см. "Создание политики")
- Изменение ранее созданной политики (см. "Редактирование политики")
- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")
- Фильтрация политик (см. "Фильтрация списка политик")

5.2.7.1 Политики и форма их просмотра

Форма просмотра политики отображается в правой части рабочей области при выборе политики в списке.



Атрибуты политик:

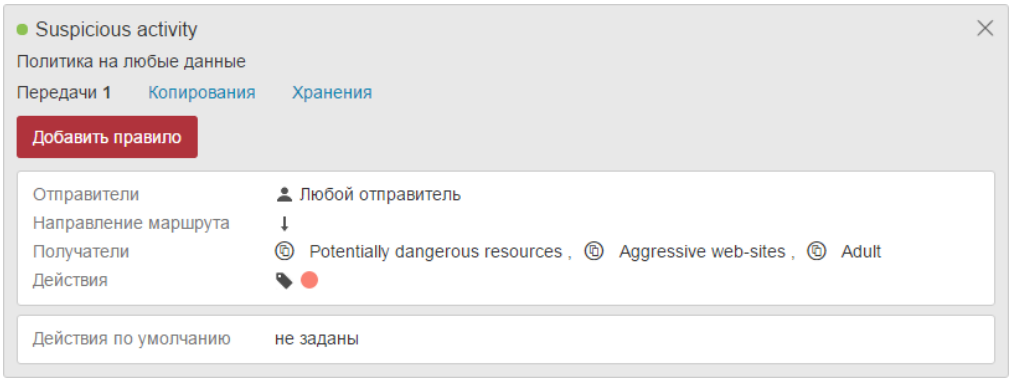
Параметр	Описание
Название	Наименование политики
Статус	Показатель того, активна ли политика в Системе
Период действия	Временной промежуток, в который действует политика
Защищаемые данные	Список объектов защиты, их каталогов и файловых форматов (для политики защиты данных) или список персон (для политики контроля персон), контролируемых политикой
Правила политики	Список действий, выполняемых Системой при срабатывании политики
Описание	Описание политики. Необязательный параметр.

Целевые действия пользователя:

- Добавление новой политики (см. "Создание политики")
- Изменение ранее созданной политики (см. "Редактирование политики")

5.2.7.2 Правила и форма их просмотра

Информация о правилах указывается в плитке политики, для которой они определены. 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 **политики защиты данных** существует один вид правил:

Правило	Описание
Правило передачи	Правило, регулирующее отправку и получение защищаемых данных

При создании правил передачи 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.

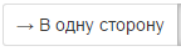
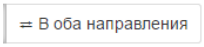
Правила контроля персон регулируют действия контролируемых персон, а также позволяют применить к выбранным персонам имеющиеся в Системе политики защиты данных.

Целевые действия пользователя:

- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")

5.2.7.2.1 Правило передачи

Атрибуты правила передачи:

Параметр	Описание
Направление маршрута	Направления могут быть двух типов:  - правило срабатывает при передаче трафика от отправителя получателю и от получателя отправителю;  - правило срабатывает только в случае передачи трафика от отправителя получателю
Тип события	Тип трафика, передача которого, при выполнении прочих настроек, приводит к срабатыванию правила. Возможные варианты: • Веб-сообщение • Email • Веб-почта • ICQ • XMPP • Mail.ru Агент • Jabber • Skype • MS Lync • Yahoo! • WhatsApp • SMS • Фотосъемка
Дни недели действия правила	Список дней недели, в которые правило будет срабатывать
Время действия правила в течение дня	Интервал времени в сутках, в который правило будет срабатывать
Компьютеры	Рабочие станции отправителя

Отправители	Список персон и рабочих станций, передача трафика которыми, при выполнении прочих настроек:  - приводит к срабатыванию правила  - не приводит к срабатыванию правила
Получатели	Список персон и рабочих станций, получение трафика которыми, при выполнении прочих настроек:  - приводит к срабатыванию правила  - не приводит к срабатыванию правила
Отправить уведомление	Список пользователей Консоли управления, которым будет отправлено уведомление в случае срабатывания правила **Примечание:** Если после создания правила пользователь или его e-mail будут удалены из Системы, то уведомление данному пользователю отправлено не будет.
Уведомить отправителя	Включите эту настройку, чтобы в случае срабатывания правила отправителям трафика было выслано уведомление. По умолчанию данная настройка отключена.
Назначить вердикт	Вердикт, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Разрешить*, *Заблокировать*, *Поместить на карантин.*
Назначить уровень нарушения	Уровень нарушения, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует.*
Теги	Список тегов, которые будут назначены объекту в случае срабатывания правила (см. "Теги")
Назначить персонам статус	Статус, который будет назначен отправителям в случае срабатывания правила (см. "Статусы")
Удалить событие	Если выбрана данная опция, то событие не будет сохранено в базу данных, а также не будут выполнены действия, заданные в правиле. По умолчанию данная настройка отключена.

Целевые действия пользователя:

- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")
- Добавление действий в политику (см. "Определение действий Системы в случае нарушения правил")

5.2.7.2.2 Правило контроля персон

Атрибуты правила контроля персон:

Параметр	Описание
Перехватывать с уровнем нарушения	Будет выполняться перехват событий с заданным уровнем нарушения

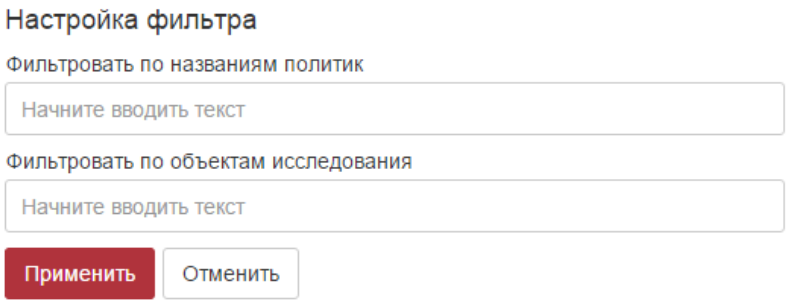
Связать с политикой	Политики защиты данных, срабатывание которых будет инициировать срабатывание правила (при условии, что уровень нарушения соответствует значению поля **Перехватывать с уровнем нарушения**)
Отправить уведомление	Список пользователей Консоли управления, которым будет отправлено уведомление в случае срабатывания правила **Примечание:** Если после создания правила пользователь или его e-mail будут удалены из Системы, то уведомление данному пользователю отправлено не будет.
Уведомить отправителя	Включите эту настройку, чтобы в случае срабатывания правила отправителям трафика было выслано уведомление. По умолчанию данная настройка отключена.
Назначить вердикт	Вердикт, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Разрешить*, *Заблокировать*, *Поместить на карантин.*
Назначить уровень нарушения	Уровень нарушения, который будет назначен объекту в случае срабатывания правила. Возможные значения: *Высокий*, *Средний*, *Низкий*, *Отсутствует.*
Теги	Список тегов, которые будут назначены объекту в случае срабатывания правила (см, "Теги")
Удалить событие	Если выбрана данная настройка, то событие не будет сохранено в базу данных, а также не будут выполнены действия, заданные в правиле. По умолчанию данная настройка отключена.

Целевые действия пользователя:

- Добавление правил в политику (см. "Создание правил")
- Изменение ранее созданных правил (см. "Редактирование правил")
- Добавление действий в политику (см. "Определение действий Системы в случае нарушения правил")

5.2.7.3 Область "Настройка фильтра"

Отображается при нажатии на кнопку **Фильтр** в разделе **Политики**.



Атрибуты фильтра:

Параметр	Описание
Фильтровать по названиям политик	Фильтрация выполняется с учетом указанных политик
Фильтровать по объектам	Фильтрация выполняется с учетом указанных защищаемых данных

Целевые действия пользователя:

- Фильтрация политик (см. "Фильтрация списка политик")

5.2.7.4 Окно добавления политики

Атрибуты политик описаны в статье "Политики и область их просмотра". При создании новой политики Вы можете указать защищаемые данные (для политики защиты данных) и контролируемых персон (для политики контроля персон).

Содержимое области добавления политики различается в зависимости от выбранного типа:

Тип политики	Описание области добавления политики
Политика защиты данных	При выборе новая политика добавляется в список политик защиты данных, а в правой части рабочей области отображается область просмотра политики. При нажатии на кнопку **Выбрать объекты** открывается диалоговое окно, в котором Вы можете указать защищаемые данные, входящие в одну из следующих категорий: • Каталог объектов защиты • Объекты защиты • Файловый формат
Политика контроля персон	При выборе открывается диалоговое окно, в котором требуется указать персон, действия которых будут контролироваться данной политикой. Вы можете выбрать отдельных персон, группу персон или персон, объединенных общим статусом.

Целевые действия пользователя:

- Добавление новой политики (см. "Создание политики защиты данных")

5.2.8 Раздел "Списки"

Справочная информация:
Списки - наборы однотипных данных, создаваемые средствами Консоли управления, или предустановленные, для использования при составлении политик.

О разделе:
Раздел содержит редактируемые справочники тегов, ресурсов, статусов, периметров и файлов.



Раздел **Списки**, вкладка **Статусы**

В разделе содержатся следующие элементы:

Элемент	Назначение

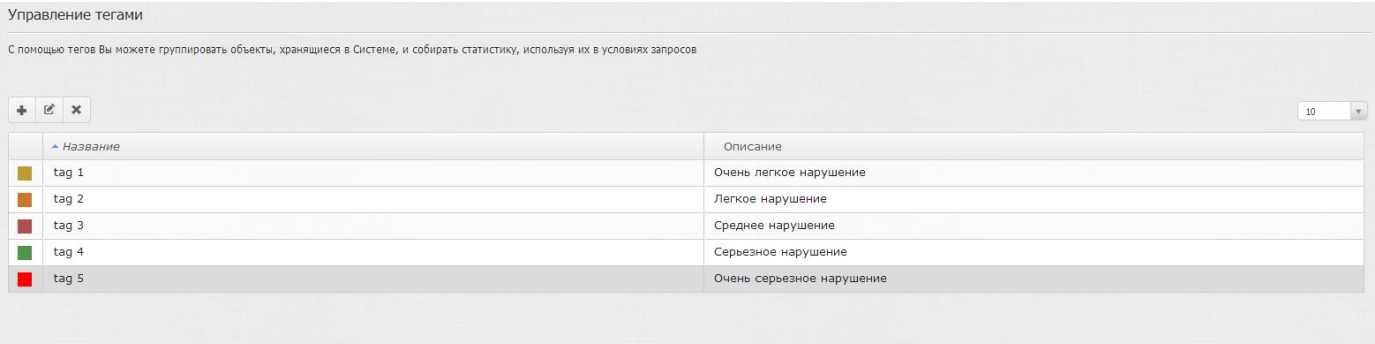
Вкладки различных типов справочников • Теги • Список ресурсов • Статусы • Периметры • Список файлов	Содержат списки элементов и инструменты для выбранного справочника
Список элементов или групп элементов для выбранного справочника	Открывается при выборе справочника. Содержит список элементов справочника или группу списков элементов справочника
Панель навигации по страницам	Набор кнопок для просмотра страниц, содержащих записи (в случае, если не все записи помещаются на одной странице)
Панель инструментов	Набор инструментов для справочников

Целевые действия пользователя:

- Формирование списка тегов (см. "Работа с тегами")
- Формирование списка ресурсов (см. "Работа со списком ресурсов")
- Формирование списка статусов (см. "Работа со статусами")
- Формирование периметров (см. "Работа с периметрами")

5.2.8.1 Теги

Справочная информация:
Тег - метка, дающая краткую характеристику перехваченному объекту.



Атрибуты тегов описаны в таблице:

Параметр	Описание
Цвет	Цветовой маркер, проставляемый вместе с тегом
Название	Наименование тега
Описание	Произвольное примечание

В системе существуют следующие предустановленные теги:

- **На рассмотрение** - события, характеризующие подозрительную активность персон.

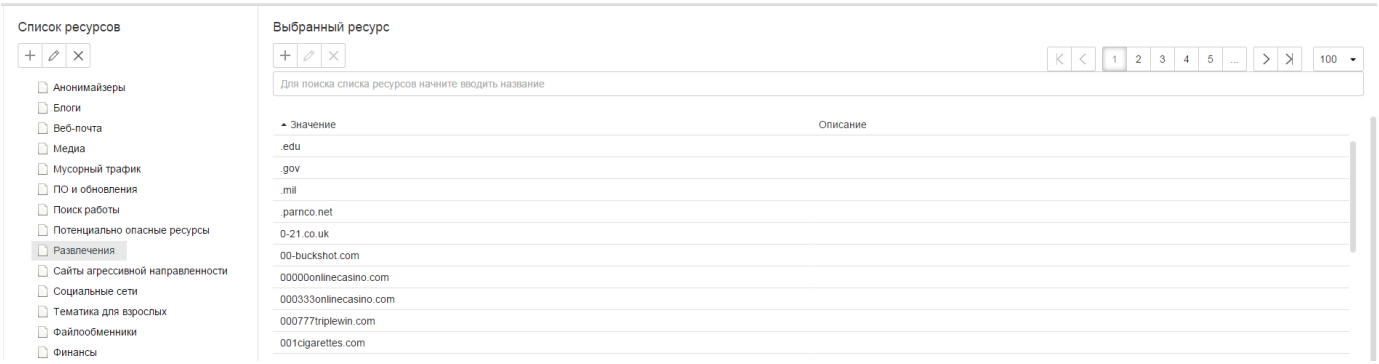
- **VIP** - события, инициированные руководством организации.

Целевые действия пользователя:

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

5.2.8.2 Список ресурсов

Справочная информация:
Список ресурсов - набор Интернет-ресурсов, посещение которых детектируется Системой как нецелевое использование рабочего времени.



Ресурсы организованы в списки в соответствии с их тематикой.

Атрибуты ресурсов описаны в таблице:

Параметр	Описание
Значение	Наименование ресурса в сети Интернет
Описание	Произвольное примечание

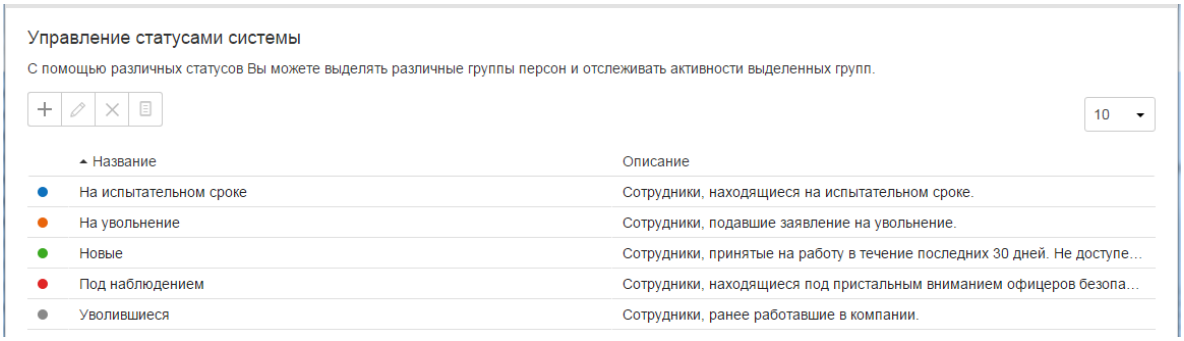
Целевые действия пользователя:

- Формирование списка ресурсов (см. "Работа со списком ресурсов")

5.2.8.3 Статусы

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

- автоматически присвоена персоне в соответствии со статусом персоны или рабочей станции, импортированных из Active Directory;
- вручную присвоена персоне офицером безопасности;
- автоматически назначена отправителю в результате срабатывания правила.



Атрибуты статусов персон описаны в таблице:

Параметр	Описание
Цвет	Цветовой маркер, проставляемый вместе со статусом
Название	Наименование статуса
Описание	Описание статуса. Необязательный параметр

Целевые действия пользователя:

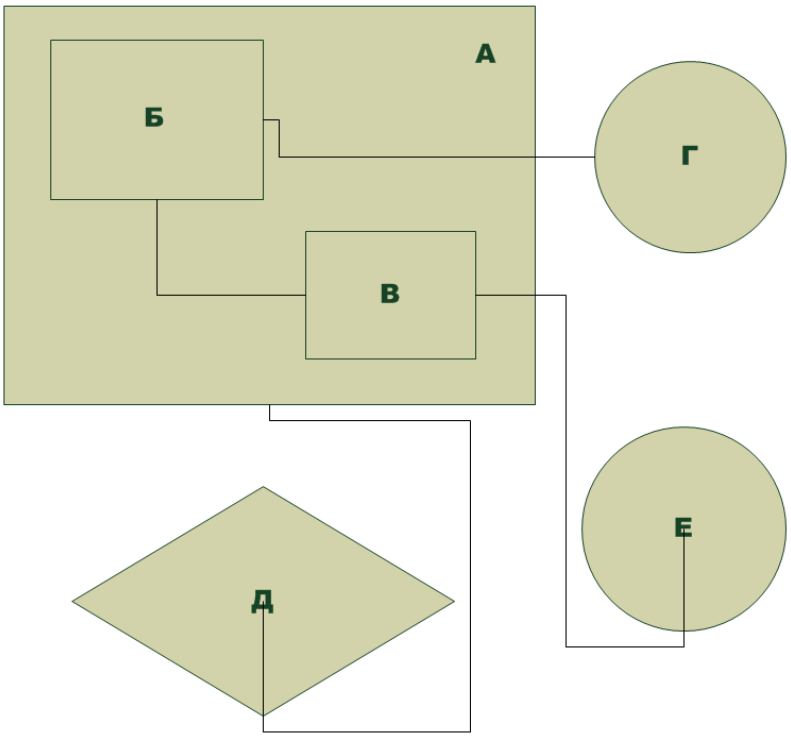
- Формирование списка статусов (см. "Работа со статусами");
- Ручное назначение статуса персоне или рабочей станции для отслеживания активности, а также для визуального отличия (см. "Добавление статуса персоне");
- Автоматическое назначение статуса отправителю в случае срабатывания правила (см. "Правила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

5.2.8.4 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;
- Компания взаимодействует с организациями Г, Д и Е.

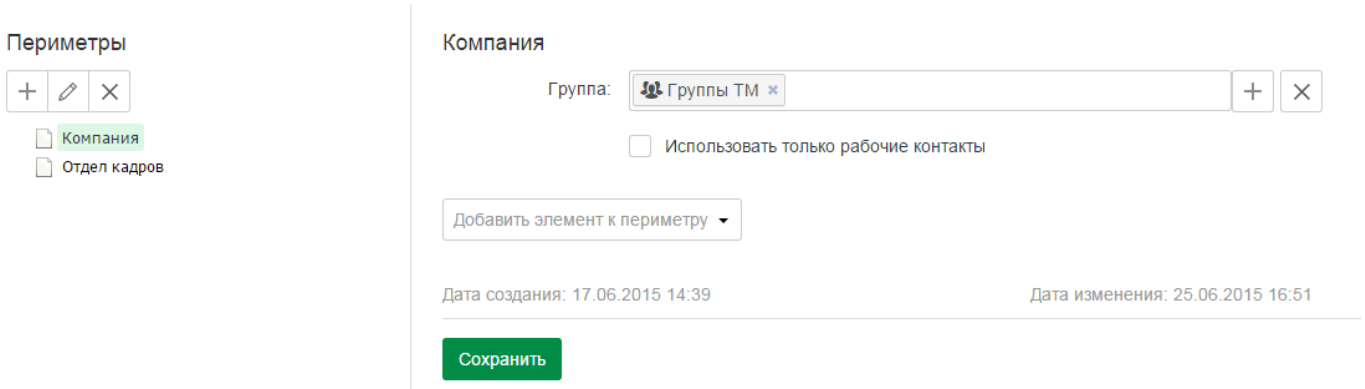


Выделив в периметры все названные объекты (А, Б, В, Г, Д, Е), офицер безопасности может настроить контроль трафика:

- внутри компании (в пределах периметра А);
- за пределами компании (между периметром А 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).



Атрибуты периметра:

Параметр	Описание
Название	Наименование периметра

Список элементов	Входящие в периметр элементы **Важно!** 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.
Дата создания	Дата и время создания периметра
Дата изменения	Дата и время последнего редактирования периметра

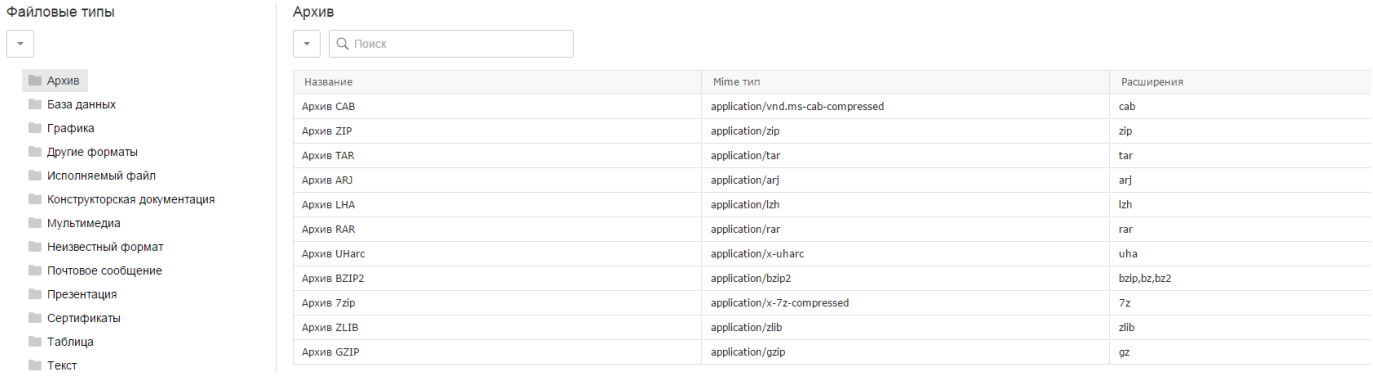
Целевые действия пользователя:

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

5.2.8.5 Список файлов

Справочная информация:

Список файлов - 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.

На вкладке содержатся следующие элементы:

Элемент	Назначение
Список типов файлов	Расположен в левой части рабочей области. Содержит набор предметных областей, в которых используются файлы одного или нескольких форматов.
Список форматов файлов выбранного типа	Расположен в правой части рабочей области. Содержит список атрибутов всех файлов данного типа, которые детектируются в Системе. Представляет собой таблицу, которая содержит в себе описание **Названия**, **Mime типа** и **Расширения**.
Кнопка **Создать политику**	Создание политики защиты данных, в качестве защищаемого объекта для которой указан выбранный формат файлов или тип файлов **Примечание:** После нажатия на кнопку открывается форма добавления новой политики в разделе **Политики**

Важно!

Списки файлов строго определены Системой и недоступны для изменения.

Целевые действия пользователя:

- Работа с политиками (см. "Создание политики защиты данных")

5.3 Типовые действия

Для чего требуются типовые действия:
Для выполнения однотипных операций во время использования Консоли управления.

К типовым действиям относятся следующие операции:

Операция	Описание
Вход в Консоль управления и выход из нее	Порядок авторизации в Консоли управления и порядок выхода из Консоли управления
Применение конфигурации Системы	Внесенные в конфигурацию Системы изменения вступают в силу с момента применения конфигурации
Редактирование элемента	Вы можете выполнять настройку сущностей, необходимых для конфигурирования Системы, отображения и обработки объектов перехвата
Удаление элемента	Вы можете удалять из интерфейса сущности, которые использовались для настройки конфигурации Системы, отображения и обработки объектов перехвата
Навигация по страницам	Вы можете просматривать большое количество элементов в многостраничном режиме: для перехода к определенной странице используются кнопки навигации
Изменение пароля пользователя	Порядок смены пароля для входа в Систему
Выбор языка интерфейса	Изменение языка интерфейса Консоли управления
Вызов справки	Обращение к справочной информации
Просмотр сведений о Системе	Вызов общей информации о Системе

5.3.1 Вход в Консоль управления и выход из нее

Цель:

1. Войти в Консоль управления.
2. Выйти из Консоли управления.

Решение:

1. **Чтобы войти в Консоль управления:**
    a. Откройте интернет-браузер Google Chrome версии 30 или выше (если указанный браузер не установлен, вы можете загрузить его, перейдя по ссылке).
    b. Перейдите по адресу, выданному Вам системным администратором. В окне браузера отобразится стартовая страница Консоли управления.
    c. В поле **Логин** укажите имя пользователя.
    d. В поле **Пароль** укажите пароль.
    Примечание:
    Логин и пароль Вы можете получить у администратора TMFD.
    e. Нажмите **Войти**.
2. **Чтобы выйти из Консоли управления:**
    a. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления").
    b. Выберите **Выйти**.

Чтобы войти в веб-консоль:

- Откройте интернет-браузер (рекомендуется использовать браузер Google Chrome. Если у Вас не установлен этот браузер, Вы можете загрузить его, перейдя по ссылке: http://www.google.com/intl/ru/chrome/browser/).
- В адресной строке введите адрес сервера TMFD.
- В поле **Логин** укажите имя пользователя.
- В поле **Пароль** укажите пароль.
- Нажмите **Войти**.

> **Важно!**
>
> Для обеспечения безопасности данных настоятельно рекомендуется по окончании работы с веб-консолью выполнить выход. Для этого в верхнем правом углу консоли нажмите **Выйти**.
> В Системе настроен автоматический выход из Консоли управления, если в течение 30 минут не выполнялось никаких действий.

5.3.2 Применение конфигурации Системы

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

- Технологии
- Объекты защиты

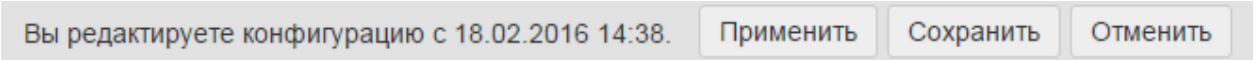
- Персоны
- Политики
- Списки

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

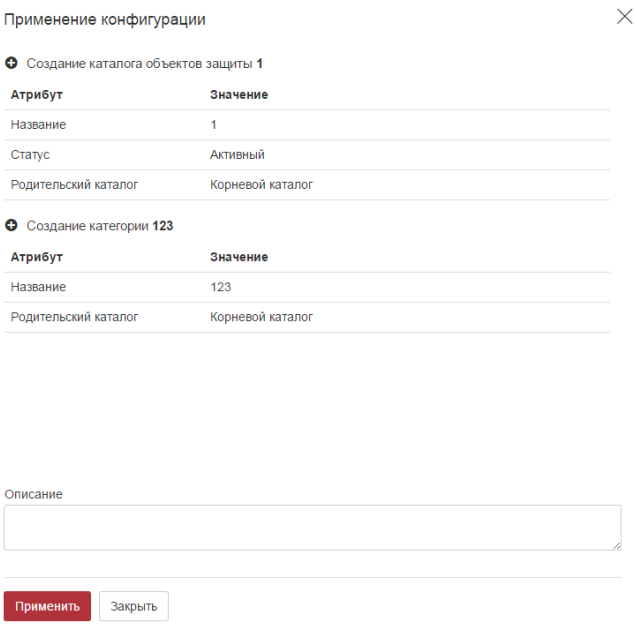
Цель:
Применить конфигурацию Системы.

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**.

5.3.3 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**.

5.3.4 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**.

5.3.5 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".

5.3.6 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**.
3. Нажмите **Сохранить**.

5.3.7 Выбор языка интерфейса

Цель:
Изменить язык интерфейса Консоли управления.

Решение:

1. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления") 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.

5.3.8 Вызов справки

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

1. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления") и выберите **Помощь**.
   В новой вкладке браузера отобразится руководство пользователя TMFD.
2. Ознакомьтесь с информацией, после чего закройте вкладку стандартным способом.

5.3.9 Просмотр сведений о Системе

Цель:
Получить справочную информацию о Системе.

Решение:

1. Нажмите на кнопку меню пользователя (см. "Интерфейс Консоли управления") 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.

5.4 Работа с персонами и рабочими станциями

Для чего требуется работа с персонами и рабочими станциями:
Наличие списков персон и рабочих станций облегчает офицеру безопасности работу с перехваченными объектами. Это происходит за счет учета информации об отправителях и получателях (персонах), а также рабочих станциях с помощью специальных справочников.

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

Работа с персонами и рабочими станциями состоит из следующих действий:

Действие	Описание
Создание группы персон и рабочих станций	Создание структурного элемента справочника
Создание списка персон и рабочих станций	Наполнение справочника
Просмотр сводки по персоне/рабочей станции	Настройка виджетов для отображения статистической информации по персоне/рабочей станции
Просмотр событий по персоне/рабочей станции	Просмотр объектов перехвата для требуемой персоны/рабочей станции
Добавление статуса персоне/рабочей станции	Выделение персоны/рабочей станции особым маркером для отслеживания активности, а также для визуального отличия
Добавление персоны/рабочей станции в периметр компании	Внесение персоны/рабочей станции в установленные списки компании
Настройка карточки персоны	Наполнение данными записи о персоне
Настройка карточки рабочей станции	Наполнение данными записи о рабочей станции

См. также:

- "Раздел Персоны" - о разделе, в котором ведется работа со списками персон и рабочих станций

5.4.1 Создание группы персон и рабочих станций

Цель:
Создать группу персон и рабочих станций.

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. Укажите атрибуты новой группы (см. "Группы персон и рабочих станций").
5. Нажмите **Да**.

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. В этом случае при добавлении/удалении пользователей в группе Active Directory состав соответствующей пользовательской группы обновится автоматически.

Чтобы добавить группу Active Directory в пользовательскую группу, выделите в списке групп нужную группу Active Directory 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 пользовательской группы, содержащих группы Active Directory, обновлялся автоматически, необходимо выполнить синхронизацию с LDAP-сервером.

О наполнении созданных групп смотрите "Создание списка персон и рабочих станций".

Дополнительные сведения:

Редактирование и удаление групп персон и рабочих станций выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.4.2 Создание списка персон и рабочих станций

Справочная информация:
Список персон и рабочих станций может наполняться двумя способами:

- из каталога Active Directory компании - настраивается администратором Системы;
- средствами TMFD - формируется офицером безопасности, как описано в этом подразделе.

Цель:
Наполнить группу персон и рабочих станций.

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;
    - **Рабочие станции** - чтобы добавить рабочую станцию.
4. На панели инструментов в правой части рабочей области нажмите + **Добавить**.
5. Укажите характеристики новой персоны или рабочей станции (см. "Персоны" и "Рабочие станции").
6. Нажмите **Сохранить**.

Дополнительные сведения:
Редактирование и удаление персон и рабочих станций выполняются стандартным способом:

- Редактирование элемента;

- Удаление элемента.

5.4.3 Просмотр событий по персоне

Цель:
Просматривать события по персоне или рабочей станции.

Решение:

1. Создайте запрос, указав в параметрах запроса целевую персону (подробнее см. "Создание запросов").
2. Выполните созданный запрос.

Аналогичным способом выполняется просмотр событий по рабочей станции.

Пример:
Если требуется, чтобы были показаны все объекты перехвата за текущую неделю, отправителем которых был *Иванов* (подразумевается, что персона *Иванов* создана в разделе **Персоны** до начала интересующего периода):

1. Офицер безопасности переходит в раздел **События** и создает запрос с названием *Иванов*, указав следующие значения:
    - атрибуту **Дата перехвата** - значение *Текущая неделя*;
    - атрибуту **Отправители** - значение *Иванов* (выбирает из списка ранее созданных персон).
2. Офицер безопасности сохраняет и выполняет созданный запрос.

В результате отобразится список, содержащий все найденные события.

5.4.4 Просмотр сводки по персоне

Цель:
Просматривать статистические данные по персоне или рабочей станции.

Решение:

1. Создать запрос, указав в параметрах запроса целевую персону (см. "Фильтрация событий").
2. Создайте виджет **Подборка**, указав в атрибуте **Подборка** ранее созданный запрос (см. "Создание виджета")

Аналогичным способом выполняется просмотр сводки по рабочей станции.

Пример:
Если требуется, чтобы были показаны все объекты перехвата за текущую неделю, отправителем трафика в которых был *Иванов* (подразумевается, что персона *Иванов* уже создана в разделе **Персоны**):

1. Офицер безопасности переходит в раздел **Сводка**
2. Офицер безопасности создает виджет с названием *Иванов*, причем атрибуту **Подборка** указывает ранее созданный запрос *Иванов* (см. "Просмотр событий по персоне").
3. Офицер безопасности сохраняет созданный виджет.

В разделе **Сводка** на виджете *Иванов* отображаются все требуемые события.

5.4.5 Добавление статуса персонам

Цель:
Добавить статус персоне или рабочей станции.

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;
    - **Рабочие станции** - чтобы добавить статус рабочей станции.
4. Выделите целевую персону или целевую рабочую станцию.
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 и рабочей станции в момент создания в Системе и сохраняется в течение 30 дней (в случае импорта персон и рабочих станций из Active Directory статус *Новый* сохраняется в течение 30 дней с момента создания записей в Active Directory).

См. также:

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

5.4.6 Добавление персоны в периметр

Цель:
Добавить персону или группу в существующий периметр.

Решение:

1. Перейдите в раздел **Списки**->**Периметры**.
2. Щелчком левой кнопки мыши выберите целевой периметр из списка периметров (см. "Периметры").
3. В правой части рабочей области нажмите **Добавить элемент к периметру** и в раскрывающемся списке выберите **Персона**.
4. В появившемся поле **Персона** укажите целевую персону одним из следующих способов:
    - начните вводить имя или фамилию и выберите из раскрывающемся списка необходимую запись;

- нажмите **Добавить**, в открывшемся диалоговом окне установите флажок в поле с целевой персоной (вы можете указать несколько персон) и нажмите **Сохранить**.

5. В области редактирования периметра нажмите **Сохранить**.

Аналогичным способом выполняется добавление в периметр группы персон.

Пример:

Если требуется, чтобы в периметр *Бухгалтерия* входила группа *Финансисты*:

Офицер безопасности выделяет периметр *Бухгалтерия* в списке периметров. Далее ОБ добавляет группу *Финансисты*:

1. нажимает **Добавить элемент к периметру**;
2. в раскрывающемся списке выбирает **Группа персон**;
3. в поле **Группа персон** указывает *Финансисты* и нажимает **Сохранить**.

См. также:

- "Периметры" - о подразделе, в котором ведется работа с периметрами.

5.4.7 Настройка карточки персоны

Цель:

Наполнить данными карточку персоны.

Настройка карточки персоны состоит из следующих действий:

Действие	Описание
Добавление персоне контакта	Добавление контактных данных для созданной персоны
Добавление персоне рабочей станции	Добавить рабочую станцию, связанную с персоной
Добавление персоны в группу	Добавление персоны в имеющуюся группу

5.4.7.1 Добавление персоне контакта

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** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевую запись;
   - щелчком левой кнопки мыши выделите целевую запись и на панели инструментов нажмите **Редактировать**.

Откроется форма редактирования карточки персоны.

4. В правой части формы редактирования карточки персон перейдите на вкладку **Контакты**.
5. Нажмите  **Добавить контакт** и укажите требуемые параметры:
   - тип контакта: электронная почта, электронная почта Lotus, мобильный телефон, стационарный телефон, Skype, ICQ, Web-контакт;
   - является ли контакт личным или рабочим;
   - значение (адрес или номер) контакта;
   - произвольное описание.
6. 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: "-","_", "( )","+");
-  - e-mail (адрес электронной почты в формате RFC);
-  - контакт Skype (строка от 1 символа);
-  - контакт ICQ (строка от 1 символа);
-  - WEB-идентификатор, например, профиль в социальной сети (строка от 1 символа);
-  - электронная почта Lotus (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**.

5.4.7.2 Добавление персоне рабочей станции

Цель:
Добавить персоне связанную рабочую станцию.

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** и выполните одно из следующих действий:
    - двойным щелчком левой кнопки мыши выделите целевую запись;
    - щелчком левой кнопки мыши выделите целевую запись и на панели инструментов нажмите **Редактировать**.

    Откроется форма редактирования карточки персоны.
4. В правой части формы редактирования карточки персоны перейдите на вкладку **Компьютеры**.
5. Нажмите **Добавить рабочую станцию**.
6. В открывшемся окне установите флажки в полях напротив требуемых рабочих станций и нажмите **Да**.
7. Нажмите **Сохранить**.

5.4.7.3 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** и выполните одно из следующих действий:
    - двойным щелчком левой кнопки мыши выделите целевую запись;
    - щелчком левой кнопки мыши выделите целевую запись и на панели инструментов в правой части рабочей области нажмите **Редактировать персону**.

    Откроется форма редактирования карточки персоны.
4. В правой части формы редактирования карточки персоны перейдите на вкладку **Группы**.
5. Нажмите **Добавить группу**.
6. В открывшемся окне установите флажок напротив требуемых группы и нажмите **Добавить**.
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 **Покинуть текущую группу**.
3. В открывшемся окне подтверждения нажмите **Да**.

Важно!

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

5.4.8 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

5.4.8.1 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** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевую рабочую станцию;
   - щелчком левой кнопки мыши выделите целевую рабочую станцию и на панели инструментов нажмите **Редактировать**.

   Откроется форма редактирования карточки компьютера.
4. В правой части формы редактирования карточки компьютера перейдите на вкладку **Контакты**.
5. Нажмите **Добавить контакт** и укажите требуемые параметры:
   - тип контакта: **IP**, **DNS** или **Доменный аккаунт**;
   - значение контакта: адрес IP, имя DNS или название доменного аккаунта;
   - произвольное описание.

6. Нажмите **Сохранить**.

5.4.8.2 Добавление компьютеру 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 **Компьютеры** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевой компьютер;
   - щелчком левой кнопки мыши выделите целевой компьютер и на панели инструментов нажмите **Редактировать**.

   Откроется форма редактирования карточки компьютера.
4. В правой части формы редактирования карточки компьютера перейдите на вкладку **Персоны**.
5. Нажмите **Добавить персону**.
6. В открывшемся окне установите флажки в полях напротив требуемых персон и нажмите **Сохранить**.
7. Нажмите **Сохранить** на форме редактирования.

Для удаления добавленной персоны выделите ее в списке и нажмите .

5.4.8.3 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** и выполните одно из следующих действий:
   - двойным щелчком левой кнопки мыши выделите целевой компьютер;
   - щелчком левой кнопки мыши выделите целевой компьютер и на панели инструментов нажмите

     Редактировать.

   Откроется форма редактирования карточки компьютера.

4. В правой части формы редактирования карточки рабочей станции перейдите на вкладку **Группы**.
5. Нажмите **Добавить группу**.
6. В открывшемся окне установите флажки в полях напротив требуемых групп и нажмите **Добавить**.
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 **Покинуть текущую группу**.
3. В открывшемся окне подтверждения нажмите **Да**.

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

5.5 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 требуется работа со справочниками:
Для того чтобы добавлять, редактировать или удалять справочники, используемые в Системе.

Работа со справочниками состоит из следующих действий:

Действие	Описание
Работа с тегами	Редактирование списка меток
Работа со списком ресурсов	Редактирование списка ресурсов.
Работа со статусами	Редактирование списка статусов
Работа с периметрами	Редактирование списка периметров

См. также:

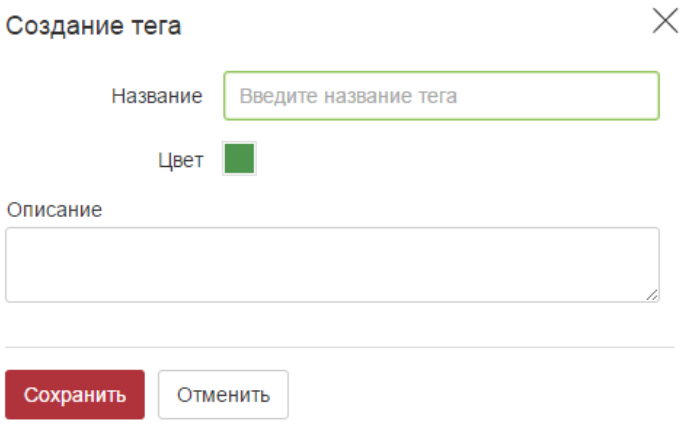
- "Раздел Списки" - о разделе, в котором ведется работа со списками

5.5.1 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.

5.5.2 Работа со списками ресурсов

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

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

Решение:

1. Создание группы ресурсов.
    a. Перейдите в раздел **Списки**, в подраздел **Ресурсы**.
    b. В левой части рабочей области нажмите
    +

Создание списка ресурсов.

c. В открывшемся окне введите название и описание списка ресурсов.

d. Нажмите **Сохранить**.

2. Добавление ресурса.

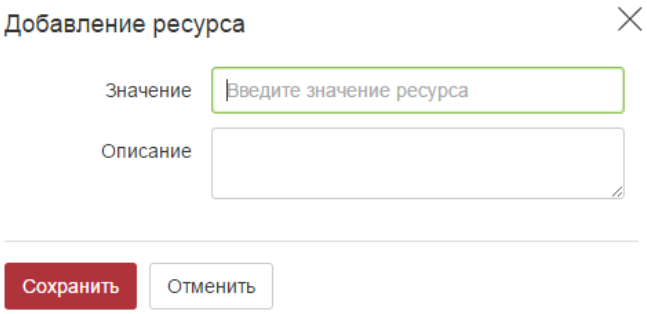
a. Перейдите в раздел **Списки**, в подраздел **Веб-ресурсы**.

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** - наименование ресурса в сети Интернет;
- в поле **Описание** - сопроводительный комментарий к записи о ресурсе (не обязательно).

e. Нажмите **Сохранить**.

Важно!

По завершении редактирования списка ресурсов требуется применить обновленную конфигурацию (см. "Работа с конфигурацией Системы").

Пример:

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

Дополнительные сведения:

- Редактирование и удаление ресурсов и их групп ресурсов выполняются стандартным способом:
  - Редактирование элемента;
  - Удаление элемента.

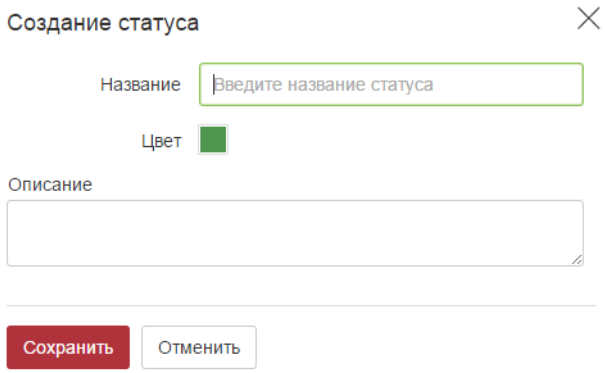
5.5.3 Работа со статусами

Цели:

1. Создать статус, характеризующий персону или рабочую станцию.
2. Создать политику контроля персон для персон, 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 персон с указанным статусом и форма ее просмотра (подробнее см. "Политики и форма их просмотра").

Дополнительные сведения:

Редактирование и удаление статуса выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.5.4 Работа с периметрами

Справочная информация:

Периметры позволяют логически разделить организацию на структурные элементы и отслеживать движение трафика.

По умолчанию в Системе создан периметр компании (название периметра может варьироваться). Для того чтобы к объектам перехвата применялись действия, указанные в предустановленных политиках, требуется добавить элементы в указанный периметр (см. Цель 2 в данной статье).

Примечание:

При создании периметра 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 + **Создание периметра**.
    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 целевой периметр из списка периметров.
    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 *Тематики ресурса*:
            - 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*, *Web-ресурса*, *Телефона*, *Skype*, *ICQ*, *Домена* и *Lotus-контакта* - введите название (например, для *Web-ресурса*) или значение (например, для *IP-адреса*) в поле и нажмите **Enter** на клавиатуре.

> **Важно!**
>
> Для включения домена в периметр необходимо использовать его полное имя. Если указано доменное имя первого уровня, то домены вложенных уровней не будут включены в периметр. Например, при добавлении в периметр домена `domain.com`, домен вложенного уровня `basic.domain.com` не будет учитываться.

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



Пример:

1. Если требуется создать периметр *Бухгалтерия*:
   Офицер безопасности добавляет новый периметр и присваивает ему название *Бухгалтерия*.
2. Если требуется, чтобы в периметр *Бухгалтерия* входила группа *Финансисты* (включая все контактные данные всех персон, входящих в указанную группу), а также сотрудник Василий Сидоров (подразумевается, что *Василий Сидоров* уже создан в разделе **Персоны**), не входящий в группу *Финансисты*:
   Офицер безопасности выделяет периметр *Бухгалтерия* в списке периметров. Далее офицер безопасности:
   - добавляет группу *Финансисты*:
     - нажимает **Добавить элемент к периметру**;
     - в раскрывающемся списке выбирает **Группа персон**;
     - в поле **Группа персон** указывает *Финансисты*;
   - добавляет персону *Василий Сидоров*:
     - нажимает **Добавить элемент к периметру**;
     - в раскрывающемся списке выбирает **Персона**;
     - в поле **Персона** указывает *Василий Сидоров*.

Дополнительные сведения:

- Редактирование периметра выполняется стандартным способом (см. "Редактирование элемента").
- Удаление периметра выполняется стандартным способом (см. "Удаление элемента").

5.6 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 (выгрузок из БД), 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 со списками ресурсов".

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 отправке запросов на ресурсы, включенные в список нецелевых (см. "Настройка реакций Системы").

См. также:

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

5.6.1 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 подраздел **Выгрузки из БД** раздела **Технологии**.
2. Создайте новый каталог.
3. Наполните 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
Выгрузки из баз данных	Часть базы данных, цитаты из которой ищутся в анализируемом тексте. Эталонными выгрузками из БД могут быть списки заработных плат сотрудников, другие личные данные и прочее	Создание эталонных выгрузок из БД

См. также:

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

5.6.1.1 Работа с выгрузками

Цель:

1. Создать каталог выгрузок из БД.
2. Создать выгрузку из БД.
3. Обновить выгрузку из БД.

Решение:

1. Создать каталог выгрузок из БД

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 из БД

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**.

e. После успешной загрузки файла:

- нажмите **Настроить выгрузку из БД** - для настройки эталонной выгрузки;
- закройте окно **Создание выгрузки из базы данных** - для выхода без дополнительных настроек.

f. Укажите требуемые атрибуты (см. "Выгрузки из БД" и "Условия детектирования выгрузки").

g. Нажмите **Сохранить**.

3. Обновить выгрузку из БД

a. Перейдите в раздел **Технологии**->**Выгрузки из БД**.

b. В левой части рабочей области выберите требуемый каталог.

c. В правой части рабочей области выделите в списке эталонную выгрузку, которую требуется обновить.

d. Нажмите  **Редактировать**.

e. В открывшемся окне редактирования выгрузки нажмите **Обновить**.

f. Укажите требуемый режим обновления: **Добавление новых записей** или **Удаление старых записей и добавление новых**.

g. Нажмите **Выбрать файл**.

h. В открывшемся диалоговом окне укажите файл, который будет использоваться для обновления, и нажмите **Открыть**. Начнется загрузка.

i. После окончания загрузки эталонная 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.

5.6.1.1.1 Условия детектирования выгрузки

Справочная информация:

Выполнение условий детектирования позволяет соотнести объект перехвата с определенной эталонной выгрузкой.

Вы можете указать несколько (не более 20) условий детектирования для эталонной выгрузки. В этом случае для отнесения объекта перехвата к данной выгрузке достаточно выполнения хотя бы одного из условий.

Цель:

Добавить условие детектирования 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 эталонную выгрузку и нажмите **Редактировать**.
   Откроется форма редактирования выгрузки.
4. На панели инструментов, расположенной под заголовком **Условия детектирования выгрузки**, нажмите **Добавить**.
5. В открывшемся диалоговом окне укажите следующие параметры (подробное описание параметров смотрите ниже):
   a. **Название условия**;
   b. **Минимальное количество строк**;
   c. **Правило детектирования**.
6. Нажмите **Создать**.

Параметры условия детектирования заполняются в соответствии со следующими рекомендациями:

Правило детектирования.

Правило детектирование 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.

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:

7. "+" - конъюнкция ячеек (логическое "И");
8. "|" - дизъюнкция ячеек (логическое "ИЛИ");

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

9. "()" - 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 четвёртая 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*.

10. "*" - символ астериска позволяет учитывать также незаполненные ячейки. Например, условие вида 1+2* означает, что строка считается сработавшей, если в ней сработала первая и вторая ячейка, 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:
Если 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
Сидоров	Сидор	Сидорович	83544593406
Смирнов	Юрий	Борисович	83245446441
Кузнецов	Владимир	Андреевич	84534359243
Соколов	Михаил	Григорьевич	83544352925

3. Офицер безопасности сохраняет таблицу в формате CSV или TSV и загружает созданный файл в Систему;
4. выполняет настройку правила обработки столбцов таблицы:
    - в поле **Правило детектирования** указывает **1+4**;
    - в поле **Минимальное количество строк** указывает **7**.
5. создает 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 детектирования выгрузки выполняются стандартным способом:

- Редактирование элемента
- Удаление элемента

5.6.2 Экспорт и импорт базы технологий

Цель:

- сохранить XML-документ, содержащий базу технологий, на жесткий диск компьютера;
- загрузить базу технологий, хранящуюся на компьютере в виде XML-документа, для использования в Консоли управления TMFD.

> **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:

3. Перейдите в какой-либо подраздел **Выгрузки из БД** раздела **Технологии**.
4. На панели инструментов в левой части рабочей области нажмите ▾ и в раскрывающемся списке выберите **Экспортировать**.
5. В открывшемся диалоговом окне **Сохранить как** укажите место на диске, куда будет сохранен xml-файл.
6. Нажмите **Сохранить**. Xml-файл будет сохранен на Ваш компьютер. Данный файл содержит следующие выгрузки из БД.

   Структура каталогов при экспорте сохраняется.

> **Важно!**
>
> Экспортируется база технологий из последней примененной конфигурации (см. "Работа с конфигурацией Системы").

Чтобы импортировать базу технологий, хранящуюся на компьютере в виде XML-документа:

4. Перейдите в какой-либо подраздел **Выгрузки из БД** раздела **Технологии**.
5. На панели инструментов в левой части рабочей области нажмите ▾ и в раскрывающемся списке выберите **Импортировать** .
6. В открывшемся диалоговом окне **Открыть** укажите xml-файл, который Вы хотите загрузить.
7. Нажмите **Открыть** и дождитесь окончание 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.

   Примечание:

   Имеющиеся в Системе верифицирующие функции будут заменены функциями из файла.

2. Для выгрузки из БД будут добавлены представления эталонной выгрузки, если содержимое выгрузки в файле и в Системе не отличается.

5.7 Работа с объектами защиты

Для чего требуются объекты защиты:

Использование объектов защиты позволяет анализировать перехваченные данные на предмет наличия в них элементов анализа: выгрузок из БД. Таким образом вы можете настроить Систему на детектирование 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 анализа	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

5.7.1 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 (см. "Каталоги объектов защиты").
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.

5.7.2 Создание объекта защиты

Цель:
Создать объект защиты на основе имеющихся в Системе элементов анализа.

Решение:

5. Перейдите в раздел **Объекты защиты**.
6. В левой части рабочей области выберите каталог, в который требуется добавить новый объект защиты, либо создайте новый каталог (см. "Создание каталогов объектов защиты").
7. На панели инструментов в правой части рабочей области нажмите + **Создать объект защиты**.
8. В открывшемся окне отметьте элементы, на основе которых будет создан объект защиты (см. "Добавление элементов анализа").
9. Определите, должны ли выбранные элементы анализа 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 анализа. Атрибуты созданных объектов защиты будут сформированы автоматически (см. "Объекты защиты"). Названия объектов будут сформированы из технологии элемента и названия элемента.
- 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.

10. Нажмите **Создать**.
11. 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 анализа**, содержащей выбранные элементы (см. "Элементы анализа"), 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 произвольный текст 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.

Дополнительные сведения:

Редактирование и удаление объектов защиты выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.7.3 Добавление элементов анализа

Цель:
Добавить элементы анализа в объект защиты.

Решение:

3. Перейдите в режим создания или редактирования объекта защиты (подробнее см. "Создание объекта защиты"). Если Вы находитесь в режиме редактирования объекта защиты, нажмите на кнопку **Выбрать элементы**.
4. В открывшемся окне добавления элементов анализа перейдите на нужную вкладку (см. "Окно добавления элементов анализа").
5. В списке элементов анализа отметьте элементы, которые вы хотите добавить.
6. Нажмите **Создать**, если вы находитесь в режиме создания объекта защиты, или **Добавить**, если Вы находитесь в режиме редактирования.

Примечание.

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

Для удаления элемента анализа нажмите на крестик напротив требуемого элемента.

5.7.4 Добавление условий обнаружения

Справочная информация:

Объект защиты будет обнаружен в событии, если:

3. Объект защиты имеет статус - **Активный**.
4. В событии найдены элементы анализа, входящие в объект защиты, с учетом указанных условий обнаружения.

Каталог объектов защиты будет обнаружен в событии, если:

4. Каталог объектов защиты имеет статус - **Активный**.
5. В событии найден хотя бы один объект защиты, входящий в данный каталог.

Цель:

Добавить условия обнаружения для объекта защиты.

Решение:

3. Перейдите в режим редактирования объекта защиты, на вкладку **Условия обнаружения**.

Примечание.

Условия обнаружения можно указать также при создании объекта защиты (см. "Создание объекта защиты", шаг 7c).

4. В поле **Добавить элемент анализа** нажмите на стрелочку и в раскрывающемся списке выберите требуемый элемент.
   Выбранный элемент будет добавлен в список условий. Для некоторых элементов анализа вы также можете указать дополнительные условия обнаружения (см. "Условия обнаружения").
5. Если объект защиты содержит несколько элементов анализа, 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 2.
     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 2.

В этом случае все блоки **Условие** будут объединены между собой с помощью операции дизъюнкции, а условия внутри одного блока - с помощью операции конъюнкции.

6. Нажмите **Сохранить**, если вы находитесь в режиме редактирования, или **Создать**, если вы находитесь в режиме создания объекта защиты.

Дополнительные сведения:

Удаление условий выполняется следующим способом:

- для удаления условия нажмите на крестик в правом верхнем углу панели с требуемых условием;
- для удаления блока, содержащего условия, нажмите на крестик в правом верхнем углу блока.

5.7.5 Создание политики для объектов защиты и их каталогов

Цель:

Создать политику защиты данных, настроенную на обнаружение объектов защиты, 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 пункт **Создать политику**.
4. В открывшемся окне создания политики защиты данных укажите требуемые параметры (подробнее см. "Политики и форма их просмотра").
5. Нажмите **Сохранить**.

Созданная политика защиты данных 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 пункт **Создать политику**.
5. В открывшемся окне создания политики защиты данных укажите требуемые параметры (подробнее см. "Политики и форма их просмотра").

6. Нажмите **Сохранить**.

Созданная политика защиты данных будет срабатывать при обнаружении хотя бы одного из выбранных объектов защиты.

5.7.6 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:

2. Перейдите в раздел **Объекты защиты**.
3. На панели инструментов в левой части рабочей области нажмите на кнопку и в раскрывающемся списке выберите пункт **Экспортировать**.
4. В открывшемся окне укажите, куда требуется сохранить созданный архив.

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:

4. Перейдите в раздел **Объекты защиты**.
5. На панели инструментов в левой части рабочей области нажмите на кнопку и в раскрывающемся списке выберите пункт **Импортировать**.
6. В открывшемся окне выберите ранее экспортированный файл, который необходимо загрузить.
7. 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:

3. Для каталога будут добавлены следующие элементы, отсутствующие в Системе:
   а) дочерние каталоги объектов защиты;
   б) объекты защиты.
4. Для объекта защиты будут добавлены следующие элементы, отсутствующие в Системе:
   а) элементы анализа;
   б) условия обнаружения.
5. Для условий обнаружения будут добавлены новые вложенные условия, включая параметры детектирования.

5.7.7 Активация и деактивация объектов защиты

По умолчанию все создаваемые объекты защиты и их каталоги имеют статус Активный (пиктограмма  для объектов защиты и  - для каталогов). При необходимости вы можете деактивировать созданный каталог или отдельный объект защиты внутри каталога.

Чтобы деактивировать каталог объектов защиты:

5. На панели инструментов в левой части рабочей области нажмите и в раскрывающемся списке выберите **Деактивировать каталог объектов защиты**.
6. Статус каталога изменится на Неактивный (пиктограмма).

Если вам требуется снова активировать деактивированный каталог, нажмите и в раскрывающемся списке выберите **Активировать каталог объектов защиты**.

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 объект защиты**.
4. Статус объекта защиты изменится на Неактивный (пиктограмма ).

Если вам требуется снова активировать деактивированный объект защиты, нажмите и в раскрывающемся списке выберите **Активировать объект защиты**.

Важно!

Объекты защиты и их каталоги могут быть обнаружены в перехваченных данных только в том случае, если они активированы.

5.8 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.

Работа с объектами перехвата состоит из следующих действий:

Действие	Описание
Просмотр сводки по нарушениям/нарушителям	Просмотр статистической информации и подборок по событиям
Просмотр событий	Просмотр сведений по каждому объекту перехвата
Работа с выгрузками	Генерирование сводки по нарушениям/нарушителям
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
Создание запросов	Фильтрация объектов перехвата по указанным критериям

См. также:

- "Раздел События" - о разделе, в котором ведется работа с объектами перехвата

5.8.1 Просмотр сводки по нарушениям/нарушителям

Работа ведется в разделе **Сводка** (см. "Раздел Сводка")

Цель:
Просмотреть сводку по нарушениям/нарушителям.

Решение:

4. Перейдите в раздел **Сводка**.
5. Настройте панель инструментов (см. "Создание панели").
6. Добавьте и настройте требуемый виджет (см. "Создание виджета" и "Настройка виджета").
7. Изучите сводку, представленную на виджете.

5.8.1.1 Создание панели

Цель:
Создать панель, на которой будут располагаться виджеты.

Решение:

8. Перейдите в раздел **Сводка**.
9. В левой части рабочей области нажмите + **Добавить**.
10. Укажите название для новой панели.
11. Нажмите **Сохранить**.

Дополнительные сведения:

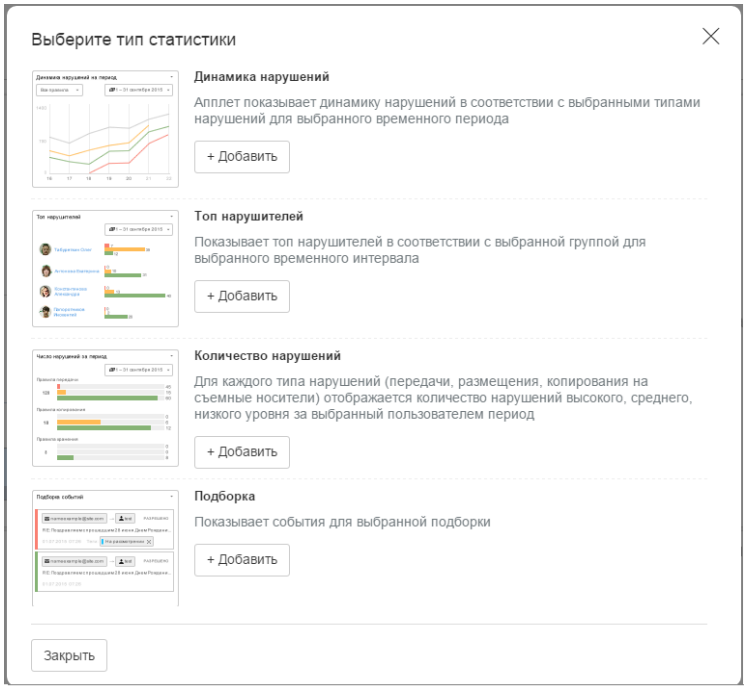
- Наполнение панели описано в статье "Создание виджета".
- Для удаления панели нажмите × на вкладке с названием панели.

5.8.1.2 Создание виджета

Цель:
Создать виджет на панели сводки.

Решение:

8. Перейдите в раздел **Сводка**.
9. Перейдите на панель, на которую требуется добавить виджет.
10. Нажмите **+Добавить виджет**.
11. В открывшемся окне **Выберите тип статистики** выберите требуемый виджет и нажмите **Добавить**.



Подробное о типах виджетов см. в статье "Виджеты".
Вы можете добавить на панель несколько виджетов подряд. Для этого продолжайте нажимать **Добавить**: после каждого нажатия на панель будет добавляться выбранный виджет.
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 (о создании запросов см. статьи "Создание запроса в стандартном режиме" и "Создание запроса в расширенном режиме").

12. Нажмите **Закрыть** или стандартную кнопку закрытия в правом верхнем углу окна.

13. Настройте виджет на отображение требуемых данных: см. "Настройка виджета".

Дополнительные сведения:

8. Вы можете перемещать плитки виджетов, 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 кнопку мыши.
9. Удаление виджета выполняется стандартным способом (см. "Удаление элемента") с той разницей, что вместо кнопки **Удалить**, расположенной на панели инструментов, используется кнопка **Удалить**, расположенная в правом верхнем углу целевого виджета.

5.8.1.3 Настройка виджета

Цель:
Настроить виджет.

Решение:

1. Перейдите в раздел **Сводка**.
2. Перейдите на требуемую панель.
3. При помощи элементов интерфейса, расположенных на виджете, настройте его: например, выберите тип правил из раскрывающегося списка, или укажите интересующий вас период времени, и т.п.
4. Для расширенной настройки виджета нажмите кнопку . Укажите необходимые значения параметров виджета (см. "Виджеты").
5. По окончании настройки нажмите **Сохранить**.

5.8.2 Просмотр событий

Цель:
Просмотреть информацию по объекту перехвата.

Решение:

6. Перейдите в раздел **События** (см. "Раздел События").
7. Примените фильтрацию событий, создав и выполнив запрос (см. "Создание запросов").

Примечание:

В списке отображаются последние 10 000 событий. События отсортированы по ID-номеру события в порядке убывания.

8. Если требуется, измените список полей просмотра событий (см. "Выбор полей просмотра событий").
9. Просмотрите информацию по событию в плитке события или в строке таблицы (см. п.3 на схеме в статье "Раздел События ").
10. При необходимости используйте краткую и детальную формы просмотра события.

5.8.2.1 Создание запросов

Цель:
Создать запрос, позволяющий отфильтровать объекты перехвата.

Решение:

3. Перейдите в раздел **События** (см. "Раздел События").
4. Выберите запрос из раскрывающегося списка запросов в верхней строке левой части рабочей области или создайте новый.

Примечание:

Доступны два способа создания запроса: в стандартном режиме и в расширенном режиме.

5. Примените запрос по событиям, нажав **Выполнить запрос** (при создании запроса вы можете также использовать кнопку **Сохранить и выполнить**).

Примечание:

Чтобы скрыть результаты выполнения запроса, справа от названия запроса в списке запросов нажмите кнопку .

См. также:

- "Создание запроса в стандартном режиме" - о создании стандартного запроса
- "Создание запроса в расширенном режиме" - о создании расширенного запроса

5.8.2.1.1 Создание запроса в стандартном режиме

Цель:
Создать фильтр объектов перехвата в стандартном режиме.

Решение:

1. Перейдите в раздел **События**.
2. На панели инструментов в верхней строке левой части рабочей области нажмите + **Добавить запрос**.
3. Выберите **Обычный запрос** в раскрывающемся списке. В правой части рабочей области появится форма создания запроса.
4. В поле **Название** укажите название запроса.
5. На вкладке **Условие** заполните поля, по которым будет осуществляться фильтрация (см. "Условие").
6. На вкладке **Поля просмотра** выберите атрибуты, значения которых будут показаны для событий, прошедших фильтрацию (см. "Поля просмотра").
7. Если Вы хотите открыть доступ на просмотр и редактирование запроса другими пользователями, то на вкладке **Параметры доступа** снимите флажок в поле **Запрос доступен только владельцу запроса** (по умолчанию флажок установлен).
8. Для выполнения более гибкой настройки фильтра Вы можете воспользоваться Расширенным режимом.
9. Нажмите:
    a. **Сохранить** - чтобы сохранить фильтр.
    b. **Сохранить и выполнить** - чтобы сохранить и применить фильтр.

Пример:
Если требуется, чтобы Система отображала события с уровнем нарушения *Высокий* и присвоенной политикой *Юридическая документация*:
ОБ создает фильтр в стандартном режиме и указывает атрибуту **Уровень нарушения** значение *Высокий*, а атрибуту **Политика** - значение *Юридическая документация*.

Дополнительные сведения:
Редактирование и удаление фильтра выполняются стандартным способом:

- Редактирование элемента;
- Удаление элемента.

5.8.2.1.2 Создание запроса в расширенном режиме

Цель:
Создать запрос в расширенном режиме.

Решение:

1. Перейдите в раздел **События**.
2. На панели инструментов, в верхней строке левой части рабочей области, нажмите + **Добавить запрос**.
3. В раскрывающемся списке выберите **Расширенный запрос**. Откроется окно создания запроса.

4. В поле **Название** укажите название запроса.
5. На вкладке **Условие**, в раскрывающемся списке **Добавить условие**, выберите параметры, по которым будет осуществляться поиск.
6. По умолчанию добавленные атрибуты связаны операцией конъюнкции (логическое "И"). Для изменения типа операции левой кнопкой мыши нажмите на пиктограмму and. При этом пиктограмма изменится на or, что соответствует операции дизъюнкции (логическое "ИЛИ").
7. Для отделения атрибутов, связанных операцией конъюнкции (логическое "И"), от атрибутов, связанных операцией дизъюнкции (логическое "ИЛИ"), используйте элемент **Группа параметров** (см. "Расширенный режим").
8. На вкладке **Поля просмотра**, выберите атрибуты, значения которых будут показаны для событий, удовлетворяющих условиям запроса (см. "Поля просмотра").
9. Если Вы хотите открыть доступ на просмотр и редактирование запроса другими пользователями, то на вкладке **Параметры доступа** снимите флажок в поле **Запрос доступен только владельцу запроса** (по умолчанию флажок установлен).
10. Нажмите **Сохранить**.

Пример 1:

Если требуется, чтобы Система отображала события:

- с уровнем нарушения *Высокий* и присвоенной политикой *Юридическая документация*;
- с уровнями нарушения *Высокий* и *Средний*, с присвоенной политикой *Юридическая документация*:

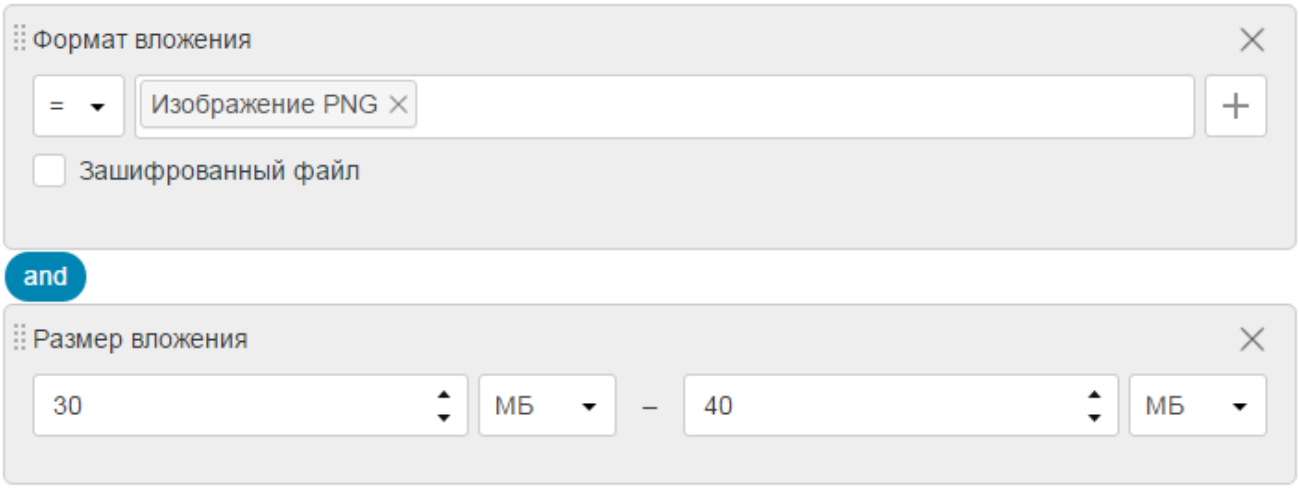
Офицер безопасности создает запрос в расширенном режиме и в качестве атрибутов указывает две группы параметров, связанных операцией дизъюнкции (см. рисунок ниже):

- В первой группе параметров блоке содержатся атрибуты со значениями:
  - **Уровень нарушения** - *Высокий*;
  - **Политика** - *Юридическая документация*;
- Во второй группе содержатся атрибуты со значениями:
  - **Уровень нарушения** - *Высокий* и *Средний*;
  - **Политика** - *Юридическая документация*;
- Атрибуты внутри групп связаны операцией конъюнкции.

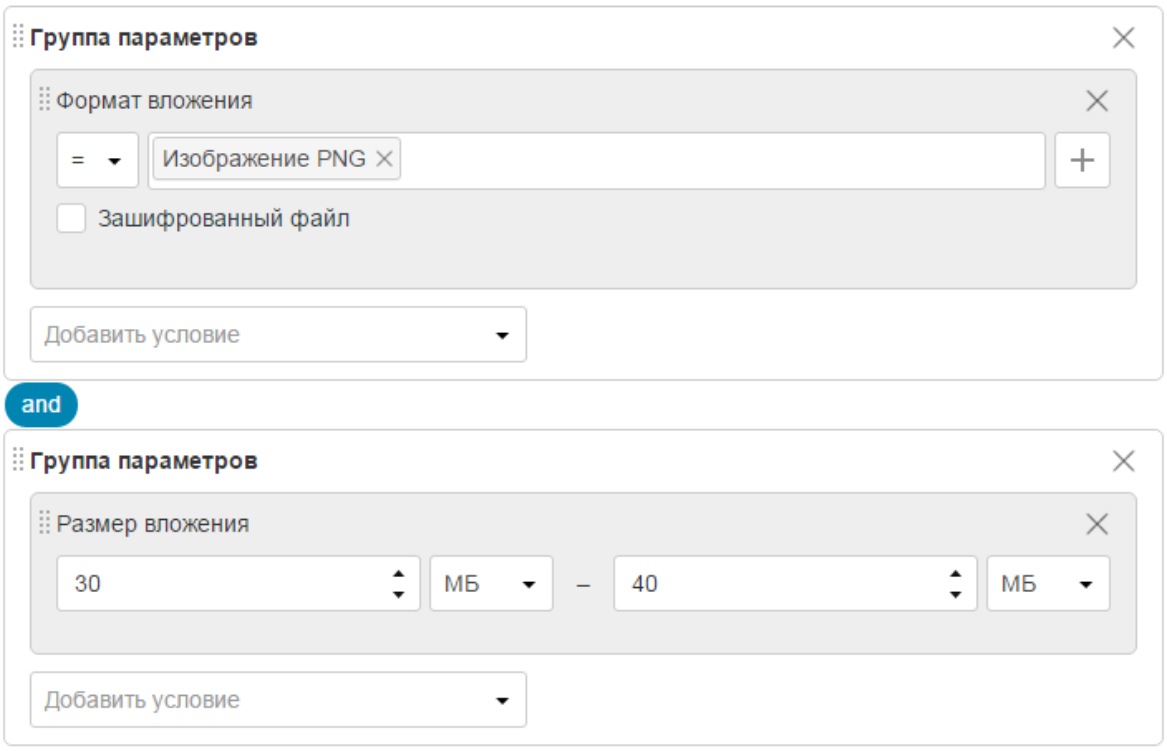
Пример 2:

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.



5.8.2.1.3 Использование расширенного синтаксиса

Цель:
Настроить поиск по тексту события с использованием расширенного синтаксиса.

Решение:

1. Перейдите в расширенный режим создания запроса.
2. На вкладке **Условие**, в раскрывающемся списке **Добавить условие**, выберите параметр **Текст события**.
3. Включите настройку **Расширенный синтаксис**.
4. В поле **Условие** введите искомый текст, используя логические операторы: "|", "-", "!", "( )" и другие.
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"
```

5.8.2.2 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 (см. "Поля просмотра"):
    - 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.

5.8.2.3 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. "Фильтрация событий").
3. Выделите плитку целевого события в списке (или строку события в таблице событий).
4. Нажмите кнопку ⌄ в правой части рабочей области для открытия краткой информации о событии. Чтобы скрыть информацию о событии, используйте кнопку ⌃.
5. Просмотрите краткую информацию о событии в правой части рабочей области.

См. также:

- "Краткая форма просмотра события" - о форме просмотра общей информации о событии
- "Просмотр детальной формы события" - о просмотре расширенной информации о событии

5.8.2.4 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 открытия детальной формы просмотра нажмите **Подробнее** в верхней строке правой части рабочей области.
5. В открывшемся окне просмотрите детальную информацию о событии:
    - вкладка **Общая информация** отображает атрибуты события (например, **Отправители**, **Получатели**, **Теги**, **Политики**, **Дата отправки**, **Дата перехвата**);
    - вкладка **Объекты защиты** отображает объекты защиты, обнаруженные в событии; сработавшие технологии, входящие в эти объекты защиты; и каталоги, в которых состояли объекты защиты на момент перехвата;
    - вкладка **Сообщения обработки** отображает ошибки, возникшие в процессе обработки события.
6. Для просмотра информации на вкладках нажмите значок . Чтобы скрыть панель информации, нажмите .
7. Для закрытия детальной формы просмотра используйте кнопку **Закрыть** или стандартную кнопку закрытия в правом верхнем углу окна.

См. также:

- "Детальная форма просмотра события" - о форме просмотра расширенной информации о событии
- "Просмотр краткой формы события" - о просмотре общей информации о событии

5.8.3 Работа с выгрузками сводки

Цель:
Создавать и просматривать выгрузки сводки.

Решение:
Решение состоит из следующих действий:

Действие	Описание
Создание выгрузки сводки	Формирование выгрузки сводки по панели
Просмотр выгрузки сводки	Просмотр файлов, содержащих сгенерированную выгрузку - в форматах PDF или HTML

См. также:

- "Выгрузка сводки" - о разделе, в котором ведется работа с выгрузками

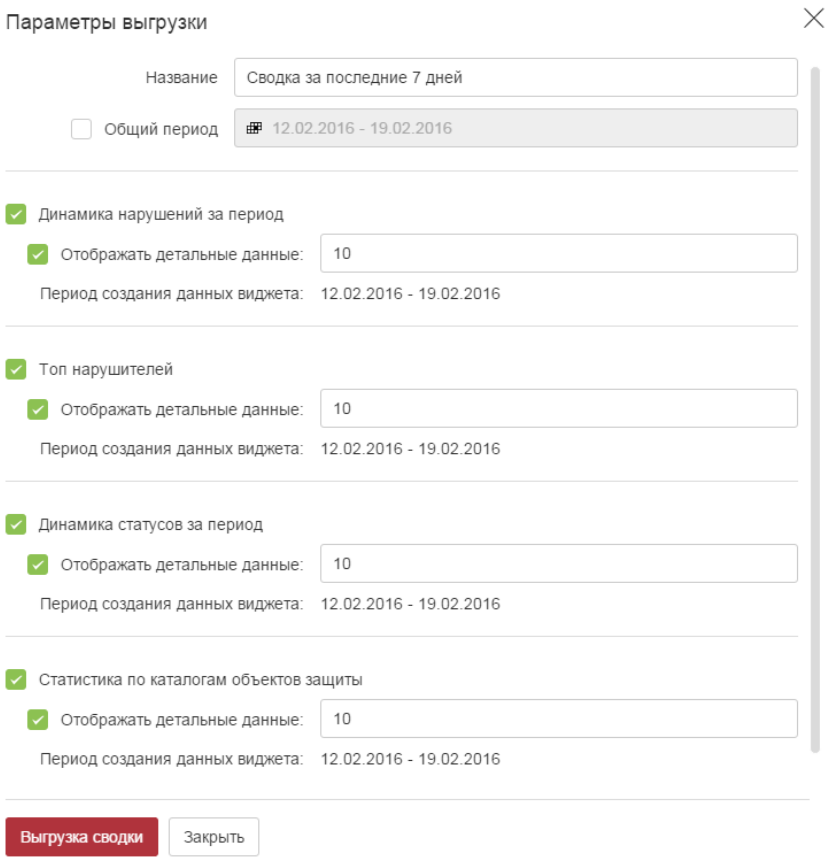
5.8.3.1 Создание выгрузки сводки

Цель:
Создать выгрузку сводки по объектам перехвата.

Решение:

1. Перейдите в раздел **Сводка**.

2. Нажмите кнопку **Выгрузка сводки** в правом верхнем углу рабочей области.
3. В открывшемся окне укажите атрибуты выгрузки (см. "Выгрузка сводки").



Окно создания выгрузки

4. Убедитесь, что флажками отмечены все виджеты, данные которых Вы хотите включить в выгрузку.
5. Установите флажок в поле **Общий период**, если Вы хотите вручную указать период, за который будет сформирована выгрузка, и введите начальную и конечную дату. Если флажок в поле **Общий период** не установлен, выгрузка будет сформирована за период, указанный в поле **Период генерации данных виджета** для виджетов, включенных в отчет.
6. 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 **Просмотреть список выгрузок** в правом верхнем углу рабочей области. Подробнее см. "Просмотр выгрузок сводки".

Примечание:

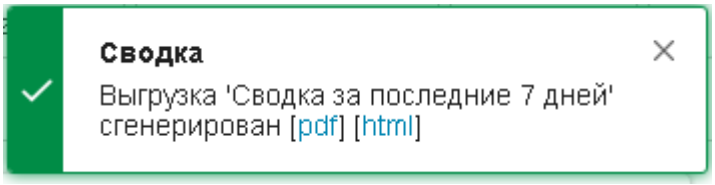
Если виджет, по которому была сформирована выгрузка, будет изменен либо удален с

панели, то уже готовая выгрузка изменена не будет.

5.8.3.2 Просмотр выгрузки сводки

Цель:
Просмотреть созданную 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 и доступны по нажатию кнопки **Просмотреть список выгрузок**.

Чтобы просмотреть список:

1. Перейдите в раздел **Сводка**.
2. Нажмите кнопку  **Просмотреть список выгрузок**.
3. В открывшемся окне, в строке требуемой выгрузки, нажмите:
   - **pdf** - если требуется вывести выгрузку сводки в формате PDF;
   - **html** - если требуется вывести выгрузку сводки в формате HTML.
4. На экран в новой вкладке браузера будет выведена созданная выгрузка.

5.8.4 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*.

- **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.

5.8.5 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

5.8.6 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 .

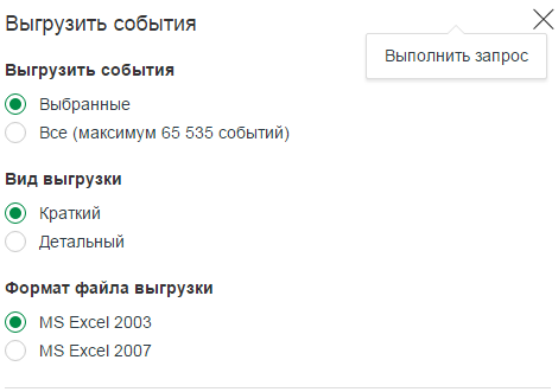
Начнется скачивание файла. После окончания загрузки вы можете открыть файл события и просмотреть его содержимое.

5.8.7 Выгрузка события

Цель:
Сохранить информацию о событиях на диск компьютера.

Решение:

1. Зайдите в раздел **События**.
2. Нажмите на значок табличной формы просмотра .
3. Выполните запрос для получения объектов.
4. Выделите в списке событие, которое вы хотите выгрузить. Чтобы выделить несколько событий, используйте клавиши Shift или Ctrl.
   Если вы хотите сформировать выгрузку для всех имеющихся событий, пропустите этот пункт.
5. На панели инструментов нажмите  и в раскрывшемся списке выберите **Выгрузить события**.
   Откроется диалоговое окно **Выгрузка событий**.



6. Убедитесь, что для параметра **Выгрузить события** установлено верное значение: **Выбранные**, если вы хотите выгрузить отдельные события, или **Все**, если вы хотите сформировать выгрузку для всех найденных событий.
7. Укажите остальные параметры выгрузки: вид (Краткий или Детальный) и формат файла выгрузки (MS Excel 2003 или MS Excel 2007).
8. Нажмите **Выгрузить**.

По завершении операции в правом верхнем углу будет отображено уведомление. Чтобы открыть новый или существующий файл выгрузки, нажмите **скачать**.

5.9 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. "Политики по умолчанию").
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, на вкладке **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 выполняла:

- отправку уведомлений нарушителям и информирование пользователей Консоли управления;
- назначение вердикта объекту перехвата;
- присвоение объекту перехвата уровня нарушения, тегов и статуса.

Настройка реакций Системы состоит из следующих действий:

Действие	Описание
Создание политики защиты данных	Политика защиты данных представляет собой набор правил передачи, контроля и хранения. Позволяет указать данные, действия с которыми могут приводить к срабатыванию правил политики.
Создание политики контроля персон	Позволяет указать список контролируемых персон, действия которых могут приводить к срабатыванию правил политики.
Создание правила	Определение, что является нарушением правила политики, и какие действия необходимо выполнить в случае нарушения
Отправка уведомлений о сработавшем правиле	При срабатывании правила Система отправляет уведомление указанным пользователям Консоли

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

5.9.1 Общие сведения о политиках

В этом разделе описан порядок применения 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 две группы:

1. Политики защиты данных - позволяют настроить правила передачи для защищаемых данных.
2. Политики контроля персон - позволяют отслеживать действия отдельных персон и их групп.

К перехваченным объектам сначала применяются все активные политики защиты данных, затем - активные политики контроля персон.

Система применяет политики к событиям в следующем порядке:

1. **Событие по очереди проверяется на соответствие всем активным политикам (вначале - политикам защиты данных, затем - политикам контроля персон)**
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)**

Подробнее о процессах, происходящих при этом:

- Разбиение события на суб-события
- Разбиение правил на суб-правила
- Определение приоритетного суб-правила
- Порядок применения действий согласно отобранным приоритетным правилам
- Пример применения политики

5.9.1.1 Разбиение события на суб-события

В результате обработки события Система присваивает ему ряд атрибутов (см. "Анализ объекта и вынесение решения по объекту"). Если какой-либо атрибут события получил несколько значений (например, несколько получателей SMTP-письма, или соответствие текста POST-запроса нескольким категориям и т.п.), то Система рассматривает это событие как совокупность нескольких суб-событий с уникальными значениями атрибутов.
Например, если перехваченное событие имеет следующие атрибуты:

Отправитель	**Получатель**	**Протокол**	**Время**
Персона: Иванов, Персона: Петров	Персона: Сидоров, Персона: Петров, Персона: Иванов	Skype	09:23

то оно подразделяется на следующие суб-события:

Отправитель	**Получатель**	**Протокол**	**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

5.9.1.2 Разбиение правил на суб-правила

При применении правил действующей политики также применяется разбиение правил на суб-правила для выявления суб-правил с наивысшим приоритетом.
Для этого из всех правил политики отбираются правила, которые соответствуют перехваченному событию по атрибутам: ***Отправитель***, ***Получатель***, ***Протокол***, например:

Отправитель	**Направление**	**Получатель**	**Протокол**	**Время**	**Реакция**
Группа: Юристы, Персона: Иванов, Персона: Петров	->	Группа: Маркетинг, Персона: Сидоров	SMTP	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

Далее производится разбиение на суб-правила по каждой паре отправителя-получателя, при этом при двусторонней передаче данных (например, сессия сообщений в чате) производится разбиение с унификацией направления отправки:

Отправитель	Направление	Получатель	Протокол	Время	Реакция
Группа: Юристы	->	Группа: Маркетинг	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Группа: Юристы	->	Персона: Сидоров	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Иванов	->	Группа: Маркетинг	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Иванов	->	Персона: Сидоров	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Петров	->	Группа: Маркетинг	SMTP	08:00-20:00	Уведомить: Викторова, Уровень нарушения: Низкий
Персона: Петров	->	Персона: Сидоров	SMTP	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

5.9.1.3 Определение приоритетного суб-правила

Приоритет правила определяется исходя из (в порядке убывания):

1. Приоритетной пары отправитель-получатель;
2. Наличия в правиле условия по времени и протоколу;
3. Наличия в правиле условия по времени;
4. Наличия в правиле условия по протоколу.

Приоритетной парой отправитель-получатель считается та, которая имеет наибольшее суммарное количество баллов отправителя и получателя:

Отправитель/Получатель	Количество баллов
Контакт	10000

Персона	5000
Группа	2500
Домен	1250
URL	600
Список ресурсов	300
Отрицание Список ресурсов	150
Отрицание URL	75
Отрицание Домен	35
Отрицание Группа	15
Отрицание Персона	7
Отрицание Контакт	3
Любой	1

Например, правило с условием на пересылку от любого отправителя - определённому контакту (10000 + 1=10001) является более приоритетным, чем правило с условием на пересылку от определённой персоны - группе персон (5000 + 2500 = 7500).
Если количество баллов за отправителя-получателя у двух или более правил равно, то учитывается наличие в правиле условий на время и/или протокол. Если и в этом отношении правила равны, 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").

5.9.1.4 Порядок применения действий согласно отобранным приоритетным правилам

Система назначает реакцию, выполняя действия из отобранных приоритетных правил, в следующем порядке:

1. Уведомляются все персоны, указанные в отобранных правилах
2. Назначаются все статусы, указанные в отобранных правилах
3. Событию присваивается наибольший уровень нарушения, указанный в отобранных правилах
4. Событие удаляется, если удаление указано хотя бы в одном правиле
5. Если хотя бы одно правило блокирует пересылку, пересылка блокируется
6. Событию присваиваются все теги, указанные в отобранных правилах

5.9.1.5 Пример:

Пусть в Системе заданы две политики:

Политика №1					
Каталог объектов защиты: Бухгалтерия					
Номер правила	Отправитель	Получатель	Время	**Протокол**	Реакция
1.1	Группа: Отдел продаж	Группа: Отдел Бухгалтерия	08:00 – 20:00	SMTP	Нарушение: Отсутствует
1.2	Иванов	Группа: Отдел Бухгалтерия		SMTP	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	**Протокол**	Реакция
2.1	Группа: Отдел продаж	<> Периметр: Компании	08:00 – 20:00	SMTP	Нарушение: Отсутствует
2.2	Иванов	<> Периметр: Компании		SMTP	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	**Протокол**
Группа объектов защиты: Бухгалтерия, Договорная	Иванов	Петров, sidorov@mail.com	19:00	SMTP

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	**Протокол**
Иванов	Петров	19:00	SMTP

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	**Протокол**
Иванов	sidorov@mail.com	19:00	SMTP

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	**Протокол**
Иванов	Петров	19:00	SMTP

Этому суб-событию соответствует только суб-правило №2.3. Следовательно, отбирается правило №2.3
Рассматривается суб-событие "Иванов->sidorov@mail.com":

Отправитель	Получатель	Время	**Протокол**
Иванов	sidorov@mail.com	19:00	SMTP

Этому суб-событию соответствует два суб-правила: №2.1 и 2.2. Из них более приоритетным является суб-правило №1.2. Следовательно, отбирается правило №2.2

3. Применяются отобранные действия: №1.2, №1.3, № 2.3, №2.2

5.9.2 Предустановленные политики

В Системе предустановлены следующие политики:

- Политики защиты конфиденциальных данных
- Политика контроля персон
- Политика, регулирующая передачу данных, защищенных паролем
- Политика, контроллирующая посещение веб-ресурсов сотрудниками компании

5.9.2.1 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 значение *Высокий* атрибуту события *Уровень нарушения*;
   - установит значение *Под наблюдением* 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*.

5.9.2.2 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

5.9.2.2.1 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 *Поместить на карантин* атрибуту события *Вердикт*.

5.9.2.3 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
Название политики	Данные, защищенные паролем
Статус	Активная
Период действия	Не ограничен
Защищаемые данные	Зашифрованные файлы всех файловых форматов

5.9.2.3.1 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 *Высокий* атрибуту события *Уровень нарушения*;
- установит событию тег *На рассмотрение*.

5.9.2.4 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

5.9.2.4.1 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

5.9.2.4.1.1 ПРАВИЛА ПОЛИТИКИ

Правило передачи, контроллирующее отправку запросов на развлекательные ресурсы.

Если персона отправляет запрос на веб-ресурс, входящий в группы "Медиа", "Блоги", "Развлечения", "Социальные сети" (подробнее см. "Список ресурсов") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Низкий* атрибуту события *Уровень нарушения.*

5.9.2.4.2 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

5.9.2.4.2.1 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. "Список ресурсов") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Средний* атрибуту события *Уровень нарушения.*

5.9.2.4.3 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

5.9.2.4.3.1 ПРАВИЛА ПОЛИТИКИ

Правило передачи, контроллирующее отправку запросов на веб-анонимайзеры.

Если персона отправляет запрос на веб-ресурс, входящий в группы "Анонимайзеры" (подробнее см. "Список ресурсов") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Средний* атрибуту события *Уровень нарушения.*

5.9.2.4.4 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

5.9.2.4.4.1 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. "Список ресурсов") в любой из дней недели,
То Система выполнит следующие действия:

- установит значение *Разрешено* атрибуту события *Вердикт*;
- установит значение *Высокий* атрибуту события *Уровень нарушения;*
- установит событию тег *На рассмотрение*.

5.9.3 Создание политики защиты данных

Цель:
Создать политику, определяющую реакцию Системы на действия с данными.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области нажмите  и в раскрывающемся списке выберите **Политика защиты данных**.
3. Новая политика будет добавлена в группу **Политики защиты данных**, а в правой части рабочей области отобразится форма добавления политики.
4. Чтобы добавить в политику защищаемые данные, нажмите кнопку **Выбрать**.
   Если защищаемые данные не выбраны, будет создана политика на любые данные.
5. В открывшемся окне установите флажки напротив элементов, которые Вы хотите добавить, и нажмите **Добавить**. В качестве защищаемых данных могут выступать объекты защиты, их каталоги, а также файловые форматы.

> **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 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. В правой части рабочей области заполните необходимые поля (см. "Политики и форма их просмотра") и нажмите **Сохранить**.

Пример 1:
Если требуется, чтобы Система реагировала на действия с данными, входящими в объект защиты *Гостайна*:
Офицер безопасности добавляет политику защиты данных и указывает в качестве защищаемых данных объект защиты *Гостайна*.

Пример 2:
Если требуется, чтобы Система реагировала на отправку любых данных на указанный ресурс:

Офицер безопасности добавляет политику защиты данных, указывает тип ресурса и уровень нарушения и не добавляет объекты исследования.

Дополнительные сведения:

- Редактирование политики описано в статье "Редактирование политики".
- Удаление политики происходит в результате нажатия кнопки , расположенной в правом верхнем углу плитки политики, и подтверждения удаления в открывшемся окне.

5.9.4 Создание политики контроля персон

Цель:
Создать политику, определяющую реакцию Системы на действия определенных персон.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области нажмите  и в раскрывающемся списке выберите **Политика контроля персон**.
3. В открывшемся окне установите флажки напротив элементов, которые Вы хотите добавить, и нажмите **Создать**. В качестве объектов исследования могут выступать:
   - отдельные персоны (сотрудники или рабочие станции);
   - группы персон и рабочих станций;
   - персоны и рабочие станции, объединенные одним статусом.

   Примечание.

   Политика сработает при обнаружении хотя бы одного объекта из каждой группы.
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. "Политики и форма их просмотра") и нажмите **Сохранить**.

Вы также можете добавить политику для выбранной персоны, рабочей станции или группы непосредственно из раздела **Персоны**.
Для этого:

1. Перейдите в раздел **Персоны**.
2. Выделите нужную персону, рабочую станцию или группу.
3. На панели инструментов в правой части рабочей области нажмите  и в раскрывающемся списке выберите **Создать политику**.

Пример:
Если требуется осуществлять контроль персоны *Иванов* (подразумевается, что персона Иванов уже создана в разделе **Персоны**) таким образом, чтобы объекту перехвата с уровнем нарушения *Высокий*, отправителем или получателем является данная персона, назначался вердикт *Разрешить*, при этом персоне присваивался статус *Под наблюдением*, и на почтовый ящик *example@company.com* отправлялось уведомление об инциденте:

Офицер безопасности переходит в раздел **Политики** и создает политику контроля персон с названием *Иванов*.

Далее Офицер безопасности создает 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. "Отправка уведомления о сработавшем правиле");
- атрибуту **Назначить событию вердикт** - значение *Разрешить*;

- атрибуту **Назначить отправителю статус** - значение *Под наблюдением*.

Дополнительные сведения:

- Редактирование политики описано в статье "Редактирование политики".
- Удаление политики происходит в результате нажатия кнопки ×, расположенной в правом верхнем углу плитки политики, и подтверждения удаления в открывшемся окне.

5.9.5 Редактирование политики

Цель:
Изменить атрибуты созданной политики.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите целевую политику.
3. В правой части рабочей области заполните необходимые поля (см. "Политики и форма их просмотра"), нажмите **Сохранить**.

> **Примечание:**
>
> Для внесения изменений в список защищаемых данных в блоке **Защищаемые данные** нажмите **Выбрать** и отредактируйте список.

5.9.6 Создание правил

Справочная информация:
Для каждой **политики защиты данных** вы можете настроить одно или несколько правил передачи объекта.

Если политика срабатывает на объекте перехвата, возможны следующие варианты, в зависимости от количества сработавших правил:

- 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 порядке выбора приоритетов 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, либо правила не заданы, Система выполняет действия, заданные для этого правила по умолчанию (см. "Определение действий Системы по умолчанию").

Для каждой **политики контроля персон** вы можете настроить правила перехвата событий с указанным уровнем нарушения. Вы также можете связать правило с имеющими в Системе политиками защиты данных.

Примечание:

Если на объекте перехвата срабатывают несколько политик, каждая из которых имеет 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:
Определить, какие действия с защищаемыми данными необходимо произвести, чтобы вызвать реакцию Системы, и как Система должна отреагировать на эти действия.

Решение:

1. Перейдите в раздел **Политики**.
2. Добавьте правило одним из следующих способов:
    - Щелчком левой кнопки мыши выделите целевую политику защиты данных, в левой части плитки политики выберите вкладку (**Передача**) и нажмите **Добавить правило**.
    - Щелчком левой кнопки мыши выделите целевую политику защиты данных, а затем в правой части рабочей области, нажмите **Добавить правило**, и в выпадающем списке выберите требуемое правило.
3. Настройте правило, используя форму в правой части рабочей области (см. "Правила и форма их просмотра").
4. В блоке **Действия при срабатывании правила** на форме просмотра правила укажите, какие действия должна выполнить Система в случае срабатывания правила.

Пример:

Если 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*: Офицер безопасности выполняет следующие действия:

1. создает тег *Отправка конфиденциальной информации в выходные* (см. "Работа с тегами");
2. создает политику защиты данных для объекта защиты *Строго конфиденциальная информация* (см. "Создание политики защиты данных");
3. создает правило передачи, присвоив атрибуту **Дни недели действия** значения *Суббота* и *Воскресенье;*
4. в блоке **Действия при срабатывании правила** присваивает атрибутам следующие значения:
    - атрибуту **Назначить событию уровень нарушения** - значение *Средний*;
    - атрибуту **Теги** - значение *Отправка конфиденциальной информации в выходные*.

Дополнительные сведения:

- Редактирование правил описано в статье "Редактирование правил".
- Удаление правила происходит после нажатия кнопки ×, расположенной в правом верхнем углу плитки правила, и подтверждения удаления в открывшемся окне.

5.9.7 Редактирование правил

Цель:
Отредактировать ранее созданное правило.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите целевую политику.
3. В плитке политики выберите группу правил **Передачи** для политики защиты данных или вкладка **Правила** для политики контроля персон).
4. В плитке политике отобразится список правил выбранной группы. Щелчком левой кнопки мыши выделите нужное правило в списке.
5. В правой части рабочей области откроется форма редактирования правила. Измените необходимые поля (см. "Правила и форма их просмотра") и нажмите **Сохранить**.

5.9.8 Определение действий Системы в случае нарушения правил

Справочная информация:
Для каждой политики вы можете указать действия, выполняемые Системой в случае нарушения правил.

Доступные действия определяются типом правила:

Действие	**Политики защиты данных**	**Политики контроля персон**
	Правило передачи	**Правило контроля персон**
Отправить уведомление пользователям	Доступно	Доступно
Уведомить нарушителя	Доступно только для типа событий "Электронная почта"	Не доступно
Назначить событию вердикт	Доступно	Доступно
Назначить событию уровень нарушения	Доступно	Доступно
Назначить событию теги	Доступно	Доступно
Назначить отправителю статус	Доступно	Доступно
Удалить событие	Доступно	Доступно

Подробное описание действий:

Действие	Описание
Отправить уведомление пользователям	Указанным пользователям Консоли будет отправлено уведомление по электронной почте. В списке можно указать пользователей или их email-адреса.
Уведомить нарушителя	Отправителю перехваченного электронного письма будет выслано уведомление
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. • **Поместить на карантин** - требуется решения пользователя, является ли объект нарушением.
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.

Цель:

Определить, как должна отреагировать Система в случае нарушения правил политики.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите нужную политику.
3. В плитке политики нажмите на ссылку с группой правил **Передачи** для политики защиты данных или **Правила** для политики контроля персон.
4. Щелчком левой кнопки мыши выделите нужное правило из списка правил или нажмите **Добавить правило** для создания нового правила (см. "Создание правил").
5. В правой части рабочей области, в блоке **Действия**, укажите, какие действие должна выполнить Система в случае срабатывания правила.
6. Нажмите **Сохранить**.

См. также:

- "Редактирование правил" - об изменении созданных правил

5.9.9 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 не сработало ни одно из правил, то политика защиты данных также не сработает на объекте перехвата.

Цель:

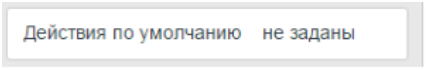
Определить, как должна отреагировать Система при наличии в событии суб-события, которому не соответствует ни одно правило политики.

Примечание.

Возможность указать действия по умолчанию предусмотрена только для политики защиты данных.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите целевую политику.
3. В плитке политики выберите вкладку **Передача**, в зависимости от требуемой задачи, и щелчком левой кнопкой мыши выделите нижнюю часть плитки:



4. В правой части рабочей области измените необходимые поля в единственном блоке **Действия** (см. "Правила и форма их просмотра") и нажмите **Сохранить**.

Дополнительная информация:

Для типов события Web-сообщение и Web-почта 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 Web-сайт, в Системе создается событие, которое разбивается на два суб-события:

Отправитель	Получатель	Протокол
Персона А	Персона В	HTTP
Персона А	Домен Web-сайта	HTTP

Так как маршрут **Персона А**->**Домен Web-сайта** не описан в правилах политики, выполняются действия по умолчанию.

Чтобы избежать ложного срабатывания правила по умолчанию для типов события Web-сообщение и Web-почта, вы можете:

- добавить в правило передачи домен Web-сайта или список Web-сайтов, через которые может осуществляться передача данных;
- не указывать действия по умолчанию.

5.9.10 Фильтрация списка политик

Цель:
Отфильтровать список политик в случае большого числа политик в списке.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области нажмите **Фильтр**.
3. 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).
4. Нажмите **Применить**.

5.9.11 Отправка уведомлений о сработавшем правиле

Цель:
Настроить автоматическое уведомление пользователей Системы о сработавшем правиле.

> **Важно!**
>
> Для отправки уведомлений можно использовать только email-адрес. При выборе из существующих контактов пользуйтесь записями только тех пользователей, у которых указан email-адрес.

Решение:

1. Перейдите в раздел **Политики**.
2. В левой части рабочей области щелчком левой кнопки мыши выделите целевую политику.
3. В плитке политике выберите вкладку **Передача** и левой кнопкой мыши выделите целевое правило из списка правил.
4. В плитке политики отобразится список правил выбранной группы. Щелчком левой кнопки мыши выделите нужное правило в списке.
5. В правой части рабочей области в поле **Отправить уведомление** укажите контакт пользователя Консоли управления. Для этого начните вводить контактные данные и выберите из раскрывающегося списка необходимую запись.

Примечание.

Если после создания правила пользователь или его e-mail будут удалены из Системы, то уведомление данному пользователю отправлено не будет.

5.10 Работа с отчетами

Для чего требуется работа с отчетами:

В отличие от краткой статистической информации, представленной в разделе "Сводка", отчеты позволяют выполнить более гибкую настройку параметров статистики и наглядно продемонстрировать результаты работы Системы за указанный период времени.

Работа с отчетами состоит из следующих действий:

Действие	Описание
Создание папки с отчетами	Создание папки, в которой будут храниться отчеты
Создание отчета	Формирование отчета со статистической информацией
Работа с виджетами	Указание параметров поиска и способа графического отображения данных в отчете
Работа с готовыми отчетами	Просмотр истории выполнения отчета с возможностью удалить ненужные версии отчета или сохранить данные отчета в файл

См. также:

- "Раздел Отчеты" - о разделе, в котором ведется работа с отчетами

5.10.1 Создание папки с отчетами

Цель:
Создать папку, в которой будут сгруппированы отчеты, объединенные общей тематикой.

Решение:

1. Перейдите в раздел **Отчеты**.
2. На панели инструментов в левой части рабочей области нажмите  и в раскрывающемся списке выберите **Создать папку**.
3. В открывшейся окне создания отчета укажите требуемые параметры (подробнее см. "Форма создания папки с отчетами").
4. Нажмите **Сохранить папку**.

Вы можете изменить расположение папки, используя перетаскивание. Для этого выделите в списке нужную папку и, удерживая левую клавишу мыши зажатой, переместите ее в требуемое место, после чего отпустите зажатую клавишу мыши.

Вы также можете скопировать ранее созданную папку и содержащиеся в ней отчеты. Для этого:

1. Выделите нужную папку в списке с помощью мыши.
2. В открывшейся форме просмотра свойств папки нажмите **Скопировать**.
3. В открывшемся диалоговом окне укажите, куда требуется вставить скопированную папку.

Важно!

При копировании или перемещении в папку, для которой выставлена настройка **Применить параметры доступа ко всем вложенным отчетам и папкам**, указанные параметры доступа будут применены ко всем копируемым или перемещаемым папкам и содержащимся в них отчетам.

Дополнительные сведения:

Редактирование и удаление отчета выполняются стандартным способом:

- редактирование папки выполняется стандартным способом (см. "Редактирование элемента"). Помимо кнопки , расположенной на панели инструментов, Вы можете использовать кнопку **Редактировать**, расположенную в правой части рабочей области;
- удаление папки выполняется стандартным способом (см. "Удаление элемента"). Помимо кнопки , расположенной на панели инструментов, Вы можете использовать кнопку **Удалить**, расположенную в правой части рабочей области.

5.10.2 Создание отчета

Цель:
Создать отчет, содержащий статистические данные по объектам перехвата.

Решение:

1. Перейдите в раздел **Отчеты**.
2. В левой части рабочей области выберите папку, в которой требуется создать отчет, либо создайте новую папку (подробнее см. "Создание папки с отчетами").
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. Нажмите **Добавить виджет**.
6. В открывшемся окне **Создание виджета** укажите параметры виджета (подробнее см. "Работа с виджетами отчетов").
7. Нажмите:
    a. **Сохранить** - чтобы сохранить отчет.
    b. **Сохранить и выполнить** - чтобы сохранить и выполнить отчет.

Вы можете изменить расположение отчета, переместив его с помощью мыши. Для этого выделите в списке нужный отчет и, удерживая левую клавишу мыши зажатой, перетащите его в требуемое место, после чего отпустите зажатую клавишу.

Вы также можете скопировать ранее созданный отчет. Для этого:

1. Выделите нужный отчет в списке с помощью мыши.
2. В правой части рабочей области нажмите на кнопку  и в раскрывающемся списке нажмите **Скопировать**.
3. В открывшемся диалоговом окне укажите, куда требуется вставить скопированный отчет.

Важно!

При копировании или перемещении в папку, для которой выставлена настройка **Применить параметры доступа ко всем вложенным отчетам и папкам**, указанные параметры доступа будут применены к копируемому или перемещаемому отчету.

Дополнительные сведения:

Редактирование и удаление отчета выполняются стандартным способом:

- Редактирование отчета выполняется стандартным способом (см. "Редактирование элемента"). Помимо кнопки , расположенной на панели инструментов, Вы можете использовать кнопку **Редактировать** в левой части рабочей области;
- Удаление отчета выполняется стандартным способом (см. "Удаление элемента"). Помимо кнопки , расположенной на панели инструментов, Вы можете использовать удалить отчет, нажав на кнопку  в правой части рабочей области и выбрав команду **Удалить**.

5.10.3 Работа с виджетами отчетов

Работа с виджетами состоит из следующих действий:

Действие	Описание
Создание и настройка виджета	Чтобы указать способ отображения статистических данных и условия фильтрации, требуется создать и настроить виджет
Редактирование виджета	Для редактирования виджета перейдите в режим редактирования отчета, в правом верхнем углу требуемого виджета нажмите  и в раскрывающемся списке выберите **Редактировать**.

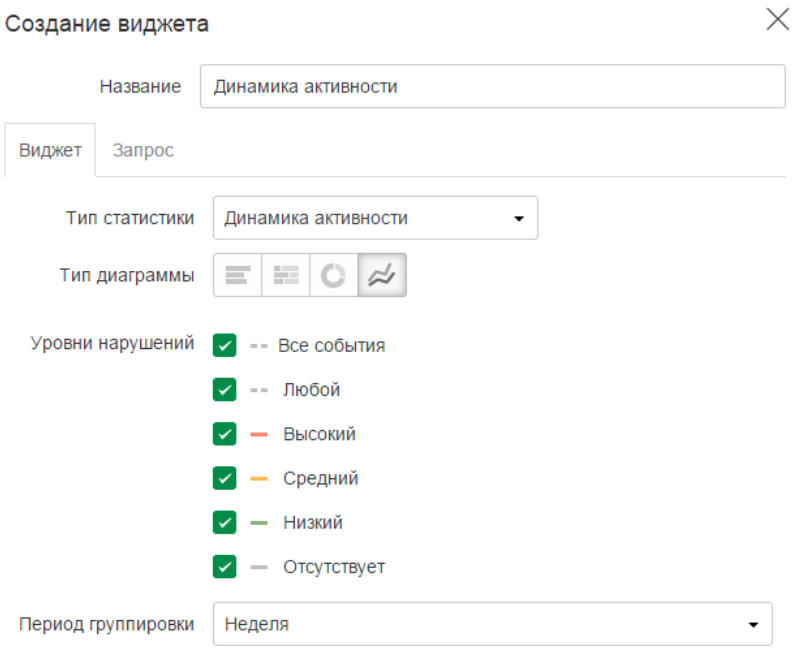
Дублирование виджета	Для дублирования виджета перейдите в режим редактирования отчета, в правом верхнем углу требуемого виджета нажмите ▾ и в раскрывающемся списке выберите **Дублировать**. В списке отчетов в левой части рабочей области выберите отчет, в который требуется дублировать виджет.
Удаление виджета	Для удаления виджета перейдите в режим редактирования отчета, в правом верхнем углу требуемого виджета нажмите ▾ и в раскрывающемся списке выберите **Удалить**.

5.10.3.1 Создание и настройка виджета

Цель:
Создать виджет для выбранного отчета и настроить его параметры.

Решение:

1. Перейдите в раздел **Отчеты**.
2. Выберите требуемый отчет и перейдите в режим редактирования либо создайте новый отчет (подробнее см. "Создание отчета").
3. В правой части рабочей области нажмите кнопку **Добавить виджет**. Откроется окно **Создание 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. статью "Запросы"). Чтобы

скопировать параметры из запроса, созданного в разделе События, нажмите Скопировать и в раскрывающемся списке выберите требуемый запрос.

5. Нажмите **Сохранить виджет**.

5.10.4 Работа с готовыми отчетами

Работа с готовыми отчетами состоит из следующих действий:

- просмотр истории выполнения отчета;
- просмотр выбранной версии отчета;
- удаление выбранных записей;
- выгрузка отчета в файл.

Для просмотра данных о выполнении отчета:

1. Перейдите в раздел **Отчеты**.
2. В правой части рабочей области нажмите кнопку и в раскрывающемся списке выберите **История выполнения отчета**. В открывшемся диалоговом окне вы можете просмотреть данные о выполнении отчета (подробнее см. "История выполнения отчета").
3. Чтобы добавить комментарий к отчету, дважды щелкните левой клавишей мыши в поле **Комментарий** напротив требуемой версии отчета и введите текст.

Для просмотра и редактирования выбранной версии отчета:

1. Чтобы открыть отчет за определенную дату, щелкните по требуемой дате выполнения левой клавишей мыши. Откроется список виджетов, отображающих результат выполнения отчета за выбранную дату.
2. Если вы хотите настроить представление виджета, содержащегося в отчете, нажмите на кнопку в верхнем правом углу выбранного виджета и в раскрывающемся списке выберите **Настроить представление**.
3. Если вы хотите перейти к событиям виджета, нажмите на кнопку в верхнем правом углу выбранного виджета и в раскрывающемся списке выберите **Перейти в события**.

Для удаления выбранных версий отчета:

1. Выберите версии отчета, которые вы хотите удалить. Для этого установите флажки в нужных строках. Чтобы выбрать все строки сразу, установите флажок в заголовке.
2. Нажмите **Удалить**.

Для выгрузки отчета:

1. Выберите версии отчета, которые Вы хотите сохранить в файл. Для этого установите флажки в нужных строках. Чтобы выбрать все строки сразу, установите флажок в заголовке.
2. Нажмите **Выгрузить** и в раскрывающемся списке укажите требуемый формат сохранения. Вы можете сохранить отчет в одном из следующих форматов: Excel 2007, HTML, PDF или JSON. Файл в указанном формате будет сохранен на ваш компьютер.

Примечание:

Чтобы выгрузить текущую версию отчета, нажмите кнопку  в правом верхнем углу рабочей области и в раскрывающемся списке выберите формат, в котором требуется сохранить выгрузку. Файл в указанном формате будет сохранен на ваш компьютер.

5.11 Работа в разделе Администрирование

Ряд действий по настройке Системы может выполняться администратором упрощенно, с помощью веб-интерфейса управления (веб-консоли), доступного из браузера любой рабочей станции локальной сети.
Основные действия администратора по управлению Системой с помощью веб-консоли описаны в следующих разделах:

- Управление интеграцией с LDAP каталогами;
- Управление пользователями Системы и их ролями;
- Управление лицензиями;
- Состояние системы;
- Управление службами;
- Сбор диагностических данных;
- Аудит действий пользователя;
- Контроль целостности;
- Плагины;

5.11.1 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* или *Domino 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
Глобальный каталог	Признак того, что для синхронизации используется глобальный LDAP каталог **Примечание:** данная настройка доступна только для Active Directory
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: `OU=Users,dc=company,dc=com`
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

Настройка интеграции с LDAP каталогами описана в разделах:

3. *Создание подключения к серверу;*
4. *Редактирование подключения к серверу;*

5. *Удаление подключения к серверу;*
6. *Запуск синхронизации с сервером вручную.*

5.11.1.1 Создание подключения к серверу

Чтобы создать подключение к серверу:

3. Перейдите в раздел **Управление -> LDAP Синхронизация**.
4. На панели инструментов нажмите  **Создать**.
5. Укажите параметры для нового подключения.
6. Нажмите **Проверить соединение**, чтобы выполнить контрольную проверку подключения к серверу.
7. Нажмите **Сохранить**.

5.11.1.2 Редактирование подключения к серверу

Чтобы отредактировать подключение к серверу:

2. Перейдите в раздел **Управление -> LDAP Синхронизация**.
3. Щелчком левой кнопки мыши выберите требуемый сервер.
4. На панели инструментов нажмите **Редактировать**.
5. Измените параметры подключения.
6. Нажмите **Проверить соединение**, чтобы выполнить контрольную проверку подключения к серверу.
7. Нажмите **Сохранить**.

5.11.1.3 Удаление подключения к серверу

Чтобы удалить существующее подключение к серверу, выполните следующие шаги:

2. Перейдите в раздел **Управление -> LDAP Синхронизация**.
3. Щелчком левой кнопки мыши выберите требуемый сервер.
4. 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**.

5. В появившемся окне нажмите **Да**.

5.11.1.4 Запуск синхронизации с сервером вручную

Чтобы запустить синхронизацию с сервером вручную, выполните следующие шаги:

4. Перейдите в раздел **Управление -> LDAP Синхронизация**.
5. Щелчком левой кнопки мыши выберите требуемый сервер.
6. На панели инструментов нажмите **Запустить синхронизацию**.

Информация о результатах синхронизации будет показана в строках *Дата последней синхронизации* и *Статус последней синхронизации*.

Примечание:

Если для подключения в качестве атрибута *Период синхронизации* выбраны значения Каждые N минут, Каждые N часов, Ежедневно или Еженедельно, автоматическая синхронизация будет выполняться с указанной периодичностью после последнего ручного запуска.

5.11.2 Управление пользователями Системы и их ролями

Для работы пользователя в Системе используются следующие сущности:

- *Пользователь* – учетная запись;
- *Роль* – набор прав, которые могут быть присвоены Пользователю;
- *Область видимости* – группа конкретных атрибутов объектов перехвата, к которым могут иметь доступ только указанные пользователи.

5.11.2.1 Пользователи

Настройка списка пользователей Системы выполняется в разделе **Управление -> Управление доступом**, на вкладке **Пользователи**.
В рабочей области расположен список пользователей Системы, панель инструментов и раскрывающееся меню.
В списке пользователей отображаются пользователи Системы.
Панель инструментов содержит набор инструментов для работы с пользователями.
Раскрывающееся меню определяет количество пользователей, отображаемых на странице.
Атрибуты учетной записи приведены в таблице:

Параметр	**Описание**
Логин	Имя учетной записи пользователя
Полное имя	ФИО пользователя
Email	Адрес электронной почты пользователя

Роли	Список ролей пользователя
Области видимости	Список областей видимости пользователя
Описание	Примечание к учетной записи
Статус	Признак того, является ли учетная запись пользователя активной или выключенной

Вы можете выполнять следующие действия при управлении пользователями:

1. Создание учетной записи пользователя*;*
2. Редактирование учетной записи пользователя*;*
3. Удаление учетной записи пользователя*;*
4. Изменение пароля учетной записи пользователя*;*
5. Изменение статуса учетной записи пользователя*;*
6. Импорт учетной записи пользователя*;*
7. Задание пользователю роли*;*
8. Задание пользователю области видимости*.*

5.11.2.1.1 Создание учетной записи пользователя

Чтобы создать учетную запись:

6. Перейдите в раздел **Управление -> Управление доступом**.
7. Перейдите на вкладку **Пользователи**.
8. На панели инструментов нажмите  **Создать пользователя**.
9. 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
Язык интерфейса	Язык, который будет присвоен интерфейсу выбранной учетной записи
Пароль	Пароль учетной записи **Примечание:** О правилах создания имен и паролей для пользователей читайте в "Приложение А. Рекомендации по составлению имен и паролей".
Подтверждение пароля	Пароль учетной записи
Email	Адрес электронной почты пользователя
Полное имя	ФИО пользователя
Описание	Примечание к учетной записи

10. Нажмите **Сохранить**.

5.11.2.1.2 Редактирование учетной записи пользователя

Чтобы изменить параметры существующей учетной записи:

5. Перейдите в раздел **Управление -> Управление доступом**.
6. Перейдите на вкладку **Пользователи**.
7. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
8. На панели инструментов нажмите **Редактировать пользователя**.
9. В открывшемся окне измените параметры учетной записи.
10. Нажмите **Сохранить**.

5.11.2.1.3 Удаление учетной записи пользователя

Чтобы удалить учетную запись:

- Перейдите в раздел **Управление -> Управление доступом**.
- Перейдите на вкладку **Пользователи**.
- В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
- 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**.

- В появившемся окне нажмите **Да**.

5.11.2.1.4 Изменение пароля учетной записи пользователя

Чтобы изменить учетную запись:

- Перейдите в раздел **Управление -> Управление доступом**.
- Перейдите на вкладку **Пользователи**.
- В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
- На панели инструментов нажмите  **Сменить пароль**.
- В открывшемся окне введите новый пароль в полях **Пароль** и **Подтверждение пароля**.

Примечание:

О правилах создания имен и паролей для пользователей читайте в "Приложение А. Рекомендации по составлению имен и паролей".

- Нажмите **Сохранить**.

5.11.2.1.5 Изменение статуса учетной записи пользователя

Чтобы изменить статус учетной записи:

3. Перейдите в раздел **Управление -> Управление доступом**.
4. Перейдите на вкладку **Пользователи**.
5. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
6. На панели инструментов нажмите  **Активировать пользователя/**  **Деактивировать пользователя**.

Примечание:

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

5.11.2.1.6 Импорт учетной записи пользователя

Для удобства создания пользователей Вы можете импортировать учетные записи из Active Directory или Domino Directory.
Чтобы импортировать учетную запись:

- Перейдите в раздел **Управление -> Управление доступом**.
- Перейдите на вкладку **Пользователи**.
- На панели инструментов нажмите  **Добавить пользователя из LDAP**.
- 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**.

- Установите флажок для требуемых пользователей.
- Нажмите **Сохранить**.

5.11.2.1.7 Задание пользователю роли

Чтобы задать пользователю роль:

- Перейдите в раздел **Управление -> Управление доступом**.
- Перейдите на вкладку **Пользователи**.
- В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
- На панели инструментов нажмите  **Задать роль**.
- В открывшемся окне установите флажок для требуемых ролей.
- Нажмите **Добавить**.

5.11.2.1.8 Задание пользователю области видимости

Чтобы задать пользователю область видимости:

- Перейдите в раздел **Управление -> Управление доступом**.
- Перейдите на вкладку **Пользователи**.
- В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
- На панели инструментов нажмите  **Задать область видимости**.
- В открывшемся окне установите флажок для требуемых областей видимости.
- Нажмите **Добавить**.

5.11.2.2 Роли

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:

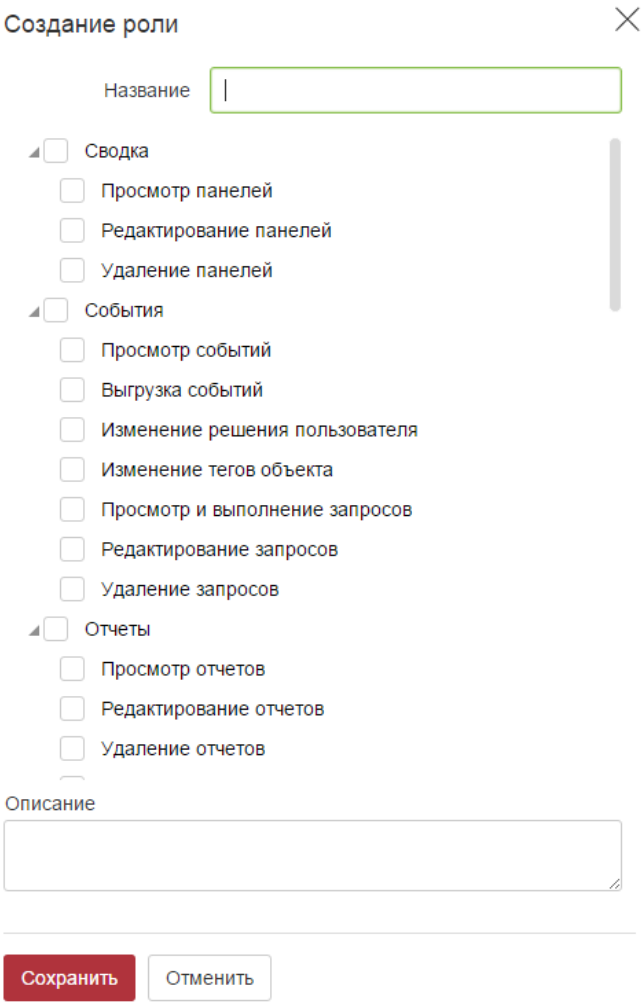
- Создание роли;
- Редактирование роли;
- Удаление роли.

5.11.2.2.1 Создание роли

Чтобы создать новую роль, выполните следующие действия:

- Перейдите в раздел **Управление -> Управление доступом**.
- Перейдите на вкладку **Роли**.
- На панели инструментов нажмите  **Создать роль**.
- В открывшемся окне установите флажки на те действия, которые требуется разрешить выбранной роли.

> **Примечание:**
>
> Чтобы развернуть или свернуть список, нажмите кнопки ▶ или ◢ соответственно.



Создание роли

- Нажмите **Сохранить**.

5.11.2.2.2 Редактирование роли

Чтобы изменить параметры существующей роли, выполните следующие действия:

3. Перейдите в раздел **Управление -> Управление доступом**.
4. Перейдите на вкладку **Роли**.
5. В списке ролей щелчком левой кнопки мыши выберите требуемую роль.
6. На панели инструментов нажмите **Редактировать роль**.
7. В открывшемся окне установите флажки на те действия, которые разрешены для выбранной роли.

> **Примечание:**
>
> Чтобы развернуть или свернуть список, нажмите кнопки ▶ или ◢ соответственно.

8. Нажмите **Сохранить**.

5.11.2.2.3 Удаление роли

Чтобы удалить роль:

- Перейдите в раздел **Управление -> Управление доступом**.
- Перейдите на вкладку **Роли**.
- В списке ролей щелчком левой кнопки мыши выберите требуемую роль.
- Нажмите  **Удалить роль**.

> **Примечание:**
>
> Чтобы удалить несколько ролей сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить роль**.

- В появившемся окне нажмите **Да**.

> **Примечание:**
>
> Вы можете изменить любую роль, кроме роли **Администратор** и **Офицер безопасности**.

5.11.2.3 Области видимости

Область видимости – это набор атрибутов объектов перехвата: объекты с такими атрибутами будут доступны только определенным пользователям.

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

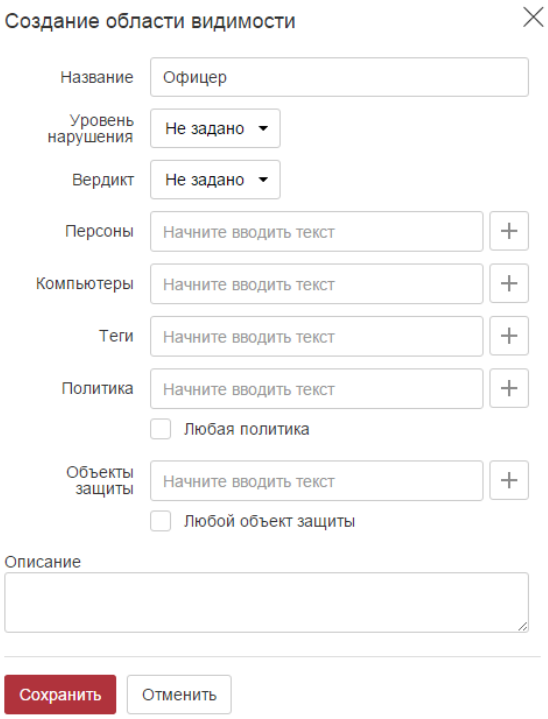
Вы можете выполнять следующие действия при управлении областями видимости:

- Создание области видимости;
- Редактирование области видимости;
- Удаление области видимости.

5.11.2.3.1 Создание области видимости

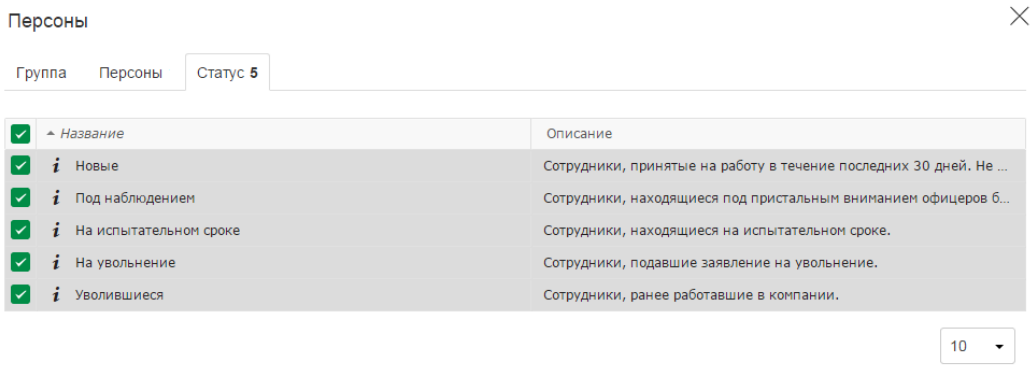
Чтобы создать область видимости:

- Перейдите в раздел **Управление -> Управление доступом** .
- Перейдите на вкладку **Области видимости**.
- На панели инструментов нажмите  **Создать область видимости**.



Создание области видимости

- В открывшемся окне заполните требуемые поля следующим образом:
  a. *Название* - введите название в поле.
  b. *Уровень нарушения* - выберите из раскрывающегося списка.
  c. *Вердикт* - выберите из раскрывающегося списка.
  d. *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**.
  e. *Компьютер* – аналогично пункту d.
  f. *Теги* - аналогично пункту d.
  g. *Политика* – аналогично пункту d.
  h. *Объект защиты* – аналогично пункту d.
  i. *Любой объект защиты* - выберите настройку.
  j. *Описание* - введите текст описания в поле.



Добавление отправителей в область видимости

- Нажмите **Добавить.**

5.11.2.3.2 Редактирование области видимости

Чтобы изменить параметры области видимости:

- Перейдите в раздел **Управление -> Управление доступом**.
- Перейдите на вкладку **Области видимости**.
- На панели инструментов нажмите **Редактировать область видимости**.
- В открывшемся окне измените параметры области видимости аналогично действиям по созданию области видимости.
- Нажмите **Сохранить**.

5.11.2.3.3 Удаление области видимости

Чтобы удалить область видимости:

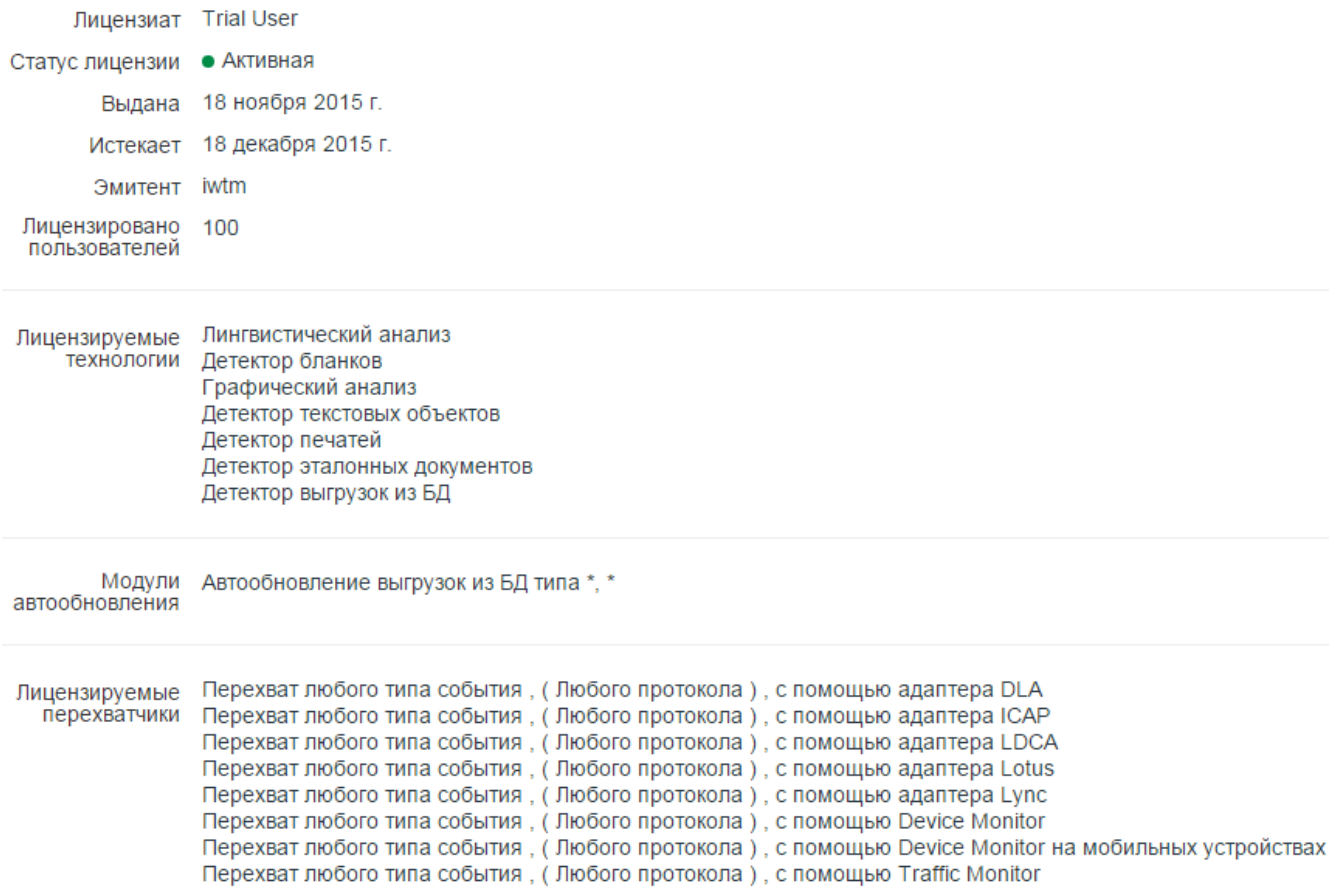
7. Перейдите в раздел **Управление -> Управление доступом**.
8. Перейдите на вкладку **Области видимости**.
9. На панели инструментов нажмите  **Удалить область видимости**.

> **Примечание:**
>
> Чтобы удалить несколько областей видимости сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить**.

10. В появившемся окне нажмите **Да**.

5.11.3 Управление лицензиями

В левой части рабочей области Консоли управления расположены список лицензий и панель управления лицензиями.Работа с лицензиями ведется в Консоли управления, в разделе **Управление –> Лицензии**:



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.

5.11.3.1 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:

4. Перейдите в раздел **Управление -> Лицензии**.
5. Убедитесь, что значение поля **Истекает** содержит дату, которая еще не наступила.
6. Убедитесь, что значение поля **Лицензиат** соответствует значению параметра Licensee конфигурационного файла **license.conf**, расположенного в директории `/opt/iw/tm5/etc`.

5.11.3.2 Установка лицензии

Чтобы установить лицензионный ключ:

8. Перейдите в раздел **Управление -> Лицензии**.
9. На панели инструментов нажмите  **Добавить лицензию**.
10. В открывшемся окне нажмите **Загрузить**.
11. 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.
12. Нажмите **Добавить**.
13. 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.

5.11.3.3 Удаление лицензии

Чтобы удалить лицензионный ключ:

- В списке лицензий выделите целевую лицензию.
- 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**.

- В открывшемся окне нажмите **Да**.

5.11.3.4 Запрос лицензии

Чтобы отправить запрос на получение лицензии:

8. Перейдите в раздел **Управление - Лицензии**;
9. В правом верхнем углу нажмите кнопку **Получить лицензию**.
10. Отправьте автоматически сформированное письмо, при необходимости указав дополнительную информацию в теле письма.

5.11.4 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: 0.21, 0.15, 0.19
●	Количество активных пользователей	USERS OK - 3 users currently logged in
●	Состояние локального почтового сервера	SMTP OK - 0.013 sec. response time
●	Отклонение системного времени	NTP OK: Offset -0.01090276241 secs
●	Ошибки в Alert-логе.	OK - no errors found in log
●	Размер Alert-лога базы данных.	OK - size of PostgresSQL system log is 9047 bytes
●	Состояние базы данных PostgreSQL.	OK - database postgres (0.003083 sec.)
●	Доступность сервера	PING OK - Packet loss = 0%, RTA = 0.06 ms
●	Свободное место в корневой партиции	DISK OK - free space: / 96362 MB (71% inode=98%):
●	Состояние службы синхронизации времени	OK - ntpd (pid 2491) is running...
●	Состояние службы Syslog	OK - 'rsyslogd' is running
●	Доступность сервера по SSH	SSH OK - OpenSSH_5.3 (protocol 2.0)
●	Использование файла подкачки	SWAP OK - 77% free (6145 MB out of 8015 MB)
●	Очередь обработки действий, указанных в примененных к событиям политиках.	OK - Blackboard queue: 0 item(s), 0.000 MBytes
●	Количество ошибок обработки действий из применённых к событиям политик.	OK - Blackboard-errors queue: 0 item(s), 0.000 MBytes
●	Наличие дампов памяти	OK
●	Состояние компонентов Системы	OK
●	Количество ошибок индексации событий службой INDEXER.	OK - index_error queue: 0 item(s)
●	TM_PG_INDEXER_QUEUE	OK - index_queue queue: 0 item(s)
●	Очередь загрузки в хранилище	OK - DB queue: 0 item(s), 0.000 MBytes
●	Очередь ошибок обработки	OK - Errors queue: 0 item(s), 0.000 MBytes
●	Очередь обработки почтового трафика	OK - SMTP queue: 0 item(s), 0.000 MBytes
●	Количество ошибок обработки событий службами IW_LOADER и IW_XML2LIRO	OK - XML2LIRO-errors queue: 0 item(s), 0.000 MBytes
●	Количество запущенных процессов	PROCS OK: 283 processes with STATE = RSZDT
●	Свободное место в партиции /var	DISK OK - free space: / 96361 MB (71% inode=98%):

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.
- **Подробнее** – 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:

4. 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
5. каждые 10 минут – для параметров:
    a. Доступность сервера по SSH/SSH availability
    b. Состояние базы данных/Database Status
    c. Статус службы доступа к базе данных/Oracle TNS Status
6. каждые 360 минут – для параметра Отклонение системного времени/NTP time deviation
7. каждые 30 минут – для всех остальных параметров

Если требуется обновить показатели вручную, нажмите  **Обновить статус**.

5.11.4.1 Настройка параметров отправки уведомлений

Чтобы настроить параметры уведомлений о состоянии системы:

- Перейдите в раздел **Управление** - **Состояние системы**;
- Нажмите кнопку  **Параметры сервера мониторинга**;
- Установите флажок в поле **Разрешить уведомления**.
- Укажите значения для следующих параметров:

Параметр	**Описание**
Почтовый сервер	IP-адрес или DNS-имя почтового сервера, который будет использоваться для отправки уведомлений. Должен быть указан сервер, поддерживающий отправку писем без SMTP-аутентификации.
Порт почтового сервера	Порт почтового сервера. Значение по умолчанию: 25
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: TMFD

Получатели	Почтовый адрес получателя/получателей. Значение по умолчанию: `nagios@localhost`

- Нажмите *Отправить тестовое сообщение*, чтобы проверить работоспособность указанных настроек.
- Нажмите **Сохранить**.

5.11.5 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

5.11.5.1 Запуск службы

Чтобы запустить службу:

8. Перейдите в раздел **Управление - Службы**.
9. Установите флажок в поле службы, которую Вы хотите запустить.
10. Нажмите кнопку .
11. Выберите опцию **Запустить**.

> **Примечание:**
>
> Чтобы запустить несколько служб, необходимо установить флажок напротив каждой из них.

5.11.5.2 Остановка службы

Чтобы остановить службу:

- Перейдите в раздел **Управление - Службы**.
- Установите флажок в поле службы, которую Вы хотите остановить.
- Нажмите кнопку .
- Выберите опцию **Остановить**.

Примечание:

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

5.11.5.3 Перезапуск службы

Чтобы перезапустить службу:

- Перейдите в раздел **Управление - Службы**.
- Установите флажок в поле службы, которую Вы хотите перезапустить.
- Нажмите кнопку .
- Выберите опцию **Перезапустить**.

Примечание:

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

5.11.5.4 Сохранение логов службы

Чтобы сохранить логи службы:

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

5.11.6 Сбор диагностических данных

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

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/nagios/nagios.log /root/iwsetup-install-logs/* /opt/distr/infowatch/appl-auto-update/appl_updater.log /home/oracle/addm/logs/* /u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log /var/log/nagios/status.dat
Конфигурационная информация	/opt/iw/tm5/etc/*.conf /opt/iw/tm5/etc/scripts/*.lua /opt/iw/tm5/etc/config/vademecums/*.info /opt/iw/tm5/etc/config/vademecums/vademecum.list /etc/nagios/* /etc/nagios/objects/*
Логи и скрипты начальной установки системы	/root/iw*

Чтобы скачать отчет по результатам последней диагностики:

- Перейдите в раздел **Управление - Сбор диагностических данных**.
- Нажмите на ссылку **Результаты последней диагностики доступны** в формате dd-mm-yyyy_hh-mm-ss.
- Откройте архив.

Важно!

В случае, если диагностика ранее не проводилась, скачивание результатов последней диагностики доступно не будет.

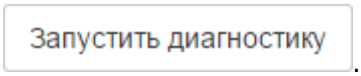
Диагностические данные могут быть собраны следующими способами:

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

5.11.6.1 Сбор диагностических данных в обычном режиме

Чтобы собрать диагностическую информацию в обычном режиме:

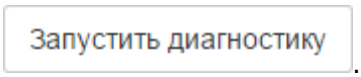
- Перейдите в раздел **Управление - Сбор диагностических данных**.
- Установите маркер в поле **Обычный**.

- Нажмите кнопку 

.
- Дождитесь завершения сборка диагностической информации.
- В сплывающем окне нажмите **Загрузить**.

5.11.6.2 Сбор диагностических данных в расширенном режиме

Чтобы собрать диагностическую информацию в расширенном режиме:

4. Перейдите в раздел **Управление - Сбор диагностических данных**.
5. Установите маркер в поле **Расширенный**.
6. Нажмите кнопку 

.
7. Дождитесь завершения сборка диагностической информации.
8. В сплывающем окне нажмите **Загрузить**.

5.11.7 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, отчёты, 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:

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

Работа с событиями аудита описана в следующих разделах:

- События аудита

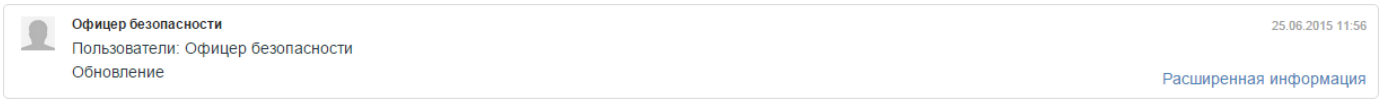
- Фильтрация по пользователю
- Фильтрация по действию
- Фильтрация по объекту
- Фильтрация по дате

5.11.7.1 События аудита

Область События аудита находится в разделе **Управление - Аудит**.

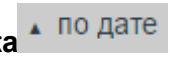
Область **События аудита** показывает результаты **Фильтров поиска** и представляет из себя список событий аудита в виде плашек со следующими атрибутами:

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



Плашка события аудита

Чтобы отсортировать события аудита по дате:

6. Перейдите в раздел **Управление** - **Аудит**;
7. В левом верхнем углу нажмите **Сортировка** 

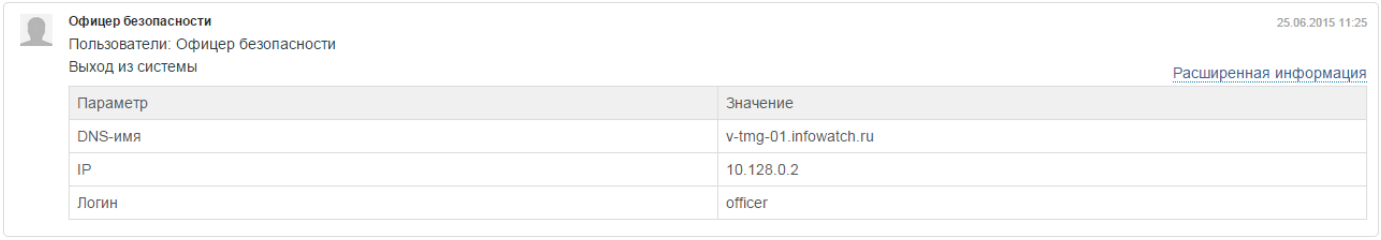
.

5.11.7.1.1 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.



Расширенная информация

Важно!

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

Чтобы посмотреть расширенную информацию о событии аудита:

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

5.11.7.2 Фильтрация по пользователю

Чтобы отфильтровать события аудита по пользователю:

3. Перейдите в раздел **Управление** - **Аудит**;
4. В области **Фильтры поиска** выберите имя пользователя из раскрывающегося меню.

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

5.11.7.3 Фильтрация по действию

Чтобы отфильтровать события по совершенному действию:

3. Перейдите в раздел **Управление** - **Аудит**;
4. В области **Фильтры поиска** выберите действие из раскрывающегося меню.

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

5.11.7.4 Фильтрация по объекту

Чтобы отфильтровать события по объекту:

2. Перейдите в раздел **Управление** - **Аудит**;
3. В области **Фильтры поиска** выберите объект из раскрывающегося меню.

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

5.11.7.5 Фильтрация по дате

Чтобы отфильтровать события по дате:

- Перейдите в раздел **Управление** - **Аудит**;
- В области **Фильтры поиска** нажмите на поле *Выбрать период.*
- В календаре укажите даты начала и конца периода, за который будут показаны события аудита.
- Нажмите **Применить**.

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

5.11.8 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.

5.11.8.1 Ручная проверка целостности

Чтобы проверить целостность системных файлов:

- Перейдите в раздел **Управление** - **Контроль целостности**;
- 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.

5.11.8.2 Автоматическая проверка целостности

Чтобы настроить автоматическую проверку целостности системных файлов:

- Перейдите в раздел **Управление** - **Контроль целостности**;
- В центральной части рабочей области включите настройку **Автоматическая проверка**.
- В поле **Проверять ежедневно в** установите время проверки целостности при помощи стрелок **вверх** и **вниз**.
- Нажмите **Сохранить**.

5.11.8.3 Принятие результата за эталонный

Чтобы принять результат проверки целостности как эталонный:

- Перейдите в раздел **Управление** - **Контроль целостности**;
- В центральной части рабочей области нажмите **Принять результат как эталонный**.

5.11.9 Плагины

Система использует плагины для подключения дополнительных перехватчиков. Расширение позволяет принимать события от внешних перехватчиков, а также автоматически обновлять эталонные выгрузки.

Любые Push API/Public API коннекторы внешних систем, должны быть зарегистрированы в TM 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 (необязательно);
- 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.

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	Название плагина
Описание	Нет	Описание плагина
Признак "Предустановленный"	Нет	Входит ли в состав Системы
Регистрируемые типы событий, контакты и протоколы	Нет	Содержит следующие данные: 1. Тип регистрируемых событий с указанием типа сервиса, к которому он относится; 2. Протоколы; 3. Действия; 4. Код типа перехватчика для плагинов TMFD; 5. Локализации наименований типов событий минимум на одном языке; 6. Типы регистрируемых контактов и их локализация минимум на одном языке; 7. 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	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.

В разделе **Плагины** можно осуществлять следующие действия:

- Добавление плагина;

- Удаление плагина;
- Работа с токенами.

5.11.9.1 Добавление плагина

Чтобы добавить плагин:

4. Перейдите в раздел **Управление - Плагины**;
5. В области **Плагины** нажмите .
6. Нажмите **Добавить**.
7. Просмотрите описание плагина и нажмите **Установить**.

> **Примечание:**
> Чтобы обновить плагин, добавьте его обновленную версию.

5.11.9.2 Удаление плагина

Чтобы удалить плагин:

- Перейдите в раздел **Управление - Плагины**;
- В области **Плагины** нажмите .
- Нажмите **Да**, чтобы подтвердить удаление.

5.11.9.3 Работа с токенами

Токен предназначен для авторизации внешней Системы, использующей Push API/Public API. После добавления плагина, токен генерируется автоматически.

Система предоставляет возможность следующих действий с токенами:

- Добавление токена;
- Удаление токена.

5.11.9.3.1 Добавление токена

Чтобы добавить токен:

3. Перейдите в раздел **Управление - Плагины**;
4. Выберите плагин в области **Плагины**;
5. Перейдите в закладку **Токены**;
6. Нажмите .

5.11.9.3.2 Удаление токена

Чтобы удалить токен:

2. Перейдите в раздел **Управление - Плагины**;
3. Выберите плагин в области **Плагины**;
4. Перейдите в закладку **Токены**;
5. Нажмите .

6 ОБНОВЛЕНИЕ СИСТЕМЫ

Чтобы обновить Систему, установленную совместно:

- Обновите пакеты RHEL и IWTM (см. "Обновление пакетов RHEL и IWTM").
- Обновите схему БД для Oracle (см. "Обновление схемы БД Oracle") или PostgreSQL (см. "Обновление схемы БД PostgreSQL").
- Перезагрузите сервер.

Чтобы обновить Систему для распределенного типа установки:

- На сервере TMFD и БД обновите пакеты RHEL и IWTM (см. "Обновление пакетов RHEL и IWTM").
- На сервере БД обновите схему БД для Oracle (см. "Обновление схемы БД Oracle") или PostgreSQL (см. "Обновление схемы БД PostgreSQL").
- Перезагрузите сервер БД.
- Перезагрузите сервер ТМ.

Перед началом обновления проверьте наличие файла `/opt/iwks_mode` и соответствие типа установки, указанного в файле, с фактическим типом установки.

Если файл отсутствует или в нем указана некорректная версия установки, создайте файл и укажите корректный параметр.

6.1 Обновление пакетов RHEL и IWTM

Для обновления Системы требуется подключения дистрибутивного диска **kickstart**. Необходимые для обновления пакеты устанавливаются на сервер с указанного диска.

- В произвольном разделе жесткого диска компьютера создайте директорию и смонтируйте CD-диск:
  `mkdir /mnt/rhel-dvd && mount /dev/cdrom /mnt/rhel-dvd`
- В директории `/etc/yum.repos.d` создайте файл **rhel-dvd.repo** (этот файл потребуется для указания пути к файлам обновления).
- Откройте файл **rhel-dvd.repo** для редактирования и вставьте в следующий текст:

```
[rhel-dvd]
 name=Red Hat Enterprise Linux $releasever - $basearch - DVD
 baseurl=file:///mnt/rhel-dvd/
 enabled=1
 gpgcheck=0

[rhel-dvd-iwtm]
 name=Red Hat Enterprise Linux $releasever - $basearch - DVD
 baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/Linux
 enabled=1
 gpgcheck=0
```

- Сохраните измененный файл **rhel-dvd.repo**.
- Очистите кэш менеджера пакетов:
  `yum clean all`
- Удалите пакет `iwtm-tmcap`:

  `rpm -e --nodeps iwtm-tmcap`

> **Важно!**
>
> Если не удалить пакет, то в процессе обновления может быть удален модуль ядра tmcap.ko, что потребует переустановку `iwtm-tmcap`.
>
> При обновлении сервера базы данных удаление `iwtm-tmcap` не требуется.

- Установите `kernel-headers` используемой версии ядра:

  `yum install kernel-headers`

> **Примечание:**
>
> Если после установки Системы не вносились изменения в kernel-headers, пропустите этот шаг.

- Установите пакет `iwtm-tmcap`:

  `yum install iwtm-tmcap`
- Запустите процесс обновления пакетов:
  `yum update`

- Проверьте наличие новых версий конфигурационных файлов с расширением **conf.rpmnew** в каталоге `/opt/iw/tm5/etc/`**.**
  - Если подобные файлы есть, приведите их в соответствие со старыми конфигурационными файлами.
- Проверьте наличие новых версий конфигурационных файлов Nagios с расширением **cfg.rpmnew** в каталоге `/etc/nagios/iwmon`**.**
  - Если подобные файлы есть, приведите их в соответствие со старыми конфигурационными файлами.
- Если в предыдущей версии вносились изменения в конфигурационный файл **config_manager.conf**, то необходимо скопировать настройки из секции Serman файла **config_manager.conf.rpmsave** в секцию `Serman` файла **agent.conf**. Оба файла расположены в директории `/opt/iw/tm5/etc`.

6.2 Обновление схемы БД Oracle

- Подключитесь к БД от имени владельца схемы:
  ```
  su - oracle
  sqlplus
  ```

  Примечание

  Логин владельца схемы по умолчанию: `iwtm` .

- Отключите пользователей от базы данных.
- Остановите службы, которые могут иметь доступ к БД, для последующего ее обновления:
  ```
  service iwtm stop
  service php-fpm stop
  service nagios stop
  ```
- Убедитесь, что конфигурационный файл **database.conf**, расположенный в директории `/opt/iw/tm5/csw/oracle`, обновился корректно, и в нем указана актуальная версия схемы.
- Перейдите в директорию `/opt/iw/tm5/csw/oracle`:

  ```
  cd /opt/iw/tm5/csw/oracle
  ```
- Запустите обновление БД при помощи сценария (скрипта):
  ```
  ./update.sh
  ```
- Запустите остановленные службы:
  ```
  service iwtm start
  service php-fpm start
  service nagios start
  ```
- Примените конфигурацию в Консоли управления TMFD.

6.3 Обновление схемы БД PostgreSQL

- Подключитесь к БД от имени владельца схемы:
  ```
  su postgres
  psql -p 5433
  ```

  Примечание

  Логин владельца схемы по умолчанию: `iwtm` .

- Отключите пользователей от базы данных.
- Остановите службы, которые могут иметь доступ к БД, для последующего ее обновления:
  ```
  service iwtm stop
  service php-fpm stop
  service nagios stop
  ```

- Убедитесь, что конфигурационный файл **database.conf**, расположенный в директории `/opt/iw/tm5/csw/postgres`, обновился корректно, и в нем указана актуальная версия схемы.
- Перейдите в директорию `/opt/iw/tm5/csw/postgres`:

  ```
  cd /opt/iw/tm5/csw/postgres
  ```

- Запустите обновление БД при помощи сценария (скрипта):
  `./update.sh`
- Запустите остановленные службы:
  ```
  service iwtm start
  service php-fpm start
  service nagios start
  ```
- Примените конфигурацию в Консоли управления TMFD.

7 УДАЛЕНИЕ СИСТЕМЫ

Удаление Системы подразумевает удаление всех пакетов Системы, а также удаление используемой схемы базы данных. Для полного удаления операционной системы и СУБД вы можете, например, выполнить форматирование используемых разделов стандартными средствами.

7. О порядке удаления схемы БД (как Oracle, так и PostrgreSQL) см. "Удаление схемы базы данных".
8. Чтобы удалить отдельный пакет, выполните команду:

```
rpm -e имя_пакета
```

9. Все серверные компоненты TMFD выполняются при помощи следующей команды:

```
yum remove `rpm -qa | grep iwtm`
```

По окончании удаления Сервера TMFD верните внешнюю инфраструктуру, настроенную на TMFD, в исходное состояние:

6. если выполнялась интеграция с почтовым relay-сервером - убедитесь, что параметры Postfix возвращены в исходное состояние;
7. если Система выполняла перехват и фильтрацию SMTP-трафика - настройте доставку SMTP-писем через корпоративный почтовый сервер, минуя TMFD.

После удаления на компьютере остаются только:

- операционная система;
- конфигурационные файлы, в которые были внесены изменения (измененным файлам присваивается суффикс **.rpmsave** - например, **detector.conf.rpmsave**; файлы, которые не изменялись, будут удалены);
- очередь объектов;
- файл лицензии;
- учетная запись пользователя – владельца TMFD, и группа, в состав которой входил этот пользователь.

7.1 Удаление схемы базы данных

Данная инструкция актуальна для СУБД Oracle и PostrgreSQL.

Важно

Не удаляйте схему базы данных, от которой для архивирования были отключены ежедневные табличные пространства. Иначе Вы не сможете восстановить данные из этих

табличных пространств.

7. **Проверка сервера СУБД Oracle**

   Убедитесь, что:

   a. версия установленной схемы базы данных соответствует версии программного пакета, используемого для ее удаления;

   b. запущен сервер СУБД;

   c. в конфигурационном файле **database.conf** корректно указаны имя и пароль учетной записи, обладающей правами SYSDBA (значения параметров `sysdba` и `sysdba_password`).

8. **Остановка TrafficMonitor**

   a. Остановить все процессы TMFD:
   `service iwtm stop`

   b. Закрыть все экземпляры консоли управления;

   c. Остановить веб-сервис:
   service php-fpm stop

   d. Прекратить все соединения с удаляемой схемой базы данных, осуществляемые из других программ.

9. **Запуск удаления схемы**

   - Перейдите в директорию
   `/opt/iw/tm5/csw/oracle` или `/opt/iw/tm5/csw/postgres`
   - Выполните скрипт:
   ./uninstall.sh

8 ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ИМЕН И ПАРОЛЕЙ

Требования к именам пользователей

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

Требования к паролям пользователей

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

«#», «$» или «_».
Может начинаться только с буквы.

10. Пароль чувствителен к регистру символов.

Рекомендации по составлению надежных паролей

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

Общие рекомендации
Не рекомендуется начинать имена и пароли пользователей с последовательностей: SYS_ и ORA_.
В составе имени и пароля пользователя не рекомендуется использовать зарезервированные слова СУБД Oracle:

ACCESS	DELETE	INTERSECT	OPTION	SUCCESSFUL
ADD	DESC	INTO	OR	SYNONYM
ALL	DISTINCT	IS	ORDER	SYSDATE
ALTER	DROP	LEVEL	PCTFREE	TABLE
AND	ELSE	LIKE	PRIOR	THEN
ANY	EXCLUSIVE	LOCK	PRIVILEGES	TO
AS	EXISTS	LONG	PUBLIC	TRIGGER

ASC	FILE	MAXEXTENTS	RAW	UID
AUDITBETWEEN	FLOAT	MINUS	RENAME	UNION
BY	FOR	MLSLABEL	RESOURCE	UNIQUE
CHAR	FROM	MODE	REVOKE	UPDATE
CHECK	GRANT	MODIFY	ROW	USER
CLUSTER	GROUP	NOAUDIT	ROWID	VALIDATE
COLUMN	HAVING	NOCOMPRESS	ROWNUM	VALUES
COMMENT	IDENTIFIED	NOT	ROWS	VARCHAR
COMPRESS	IMMEDIATE	NOWAIT	SELECT	VARCHAR2
CONNECT	IN	NULL	SESSION	VIEW
CREATE	INCREMENT	NUMBER	SET	WHENEVER
CURRENT	INDEX	OF	SHARE	WHERE
DATE	INITIAL	OFFLINE	SIZE	WITH
DECIMAL	INSERT	ON	SMALLINT	
DEFAULT	INTEGER	ONLINE	START	

9 ПРИЛОЖЕНИЕ В. ИНДИКАТОРЫ МОНИТОРИНГА

В приведенной ниже таблице перечислены все индикаторы, используемые подсистемой мониторинга для проверки состояния компонентов Системы. Под проверкой подразумевается периодическое получение значения индикатора и сравнение значения индикатора с пороговым значением.

Важно!

Если производились изменения конфигурационных файлов, то пороговые значения и период проверки могут отличаться от указанных.

Если все индикаторы указывают на критические значения, это может свидетельствовать о физической недоступности проверяемых серверов. Проверьте их работоспособность.

Управление сервисами (например, проверка статуса) выполняется из-под учетной записи root.

Название индикатора	**Проверка**	**Значения**	**Период опроса**
Общая нагрузка системы	Загрузка серверов IW-Linux-servers, TMcap-servers, DB-servers за последние 15, 5, 1 минут	🔴 – хотя бы одна цифра превышает соответствующее значение 20.0,16.0,12.0 за 15, 5, 1 🟡 – хотя бы одна цифра превышает соответствующее значение 10.0,8.0,6.0 за 15, 5, 1 🟢 – ни одна цифра не превышает соответствующее значение 10.0,8.0,6.0 за 15, 5, 1	30 мин.
Количество активных пользователей	Количество пользователей, зарегистрированных на хосте	🔴 – > 50 пользователей 🟡 – от 20 до 50 🟢 – < 20 пользователей	30 мин.
Доступность сервера Postfix	Доступность Postfix сервера	🔴 – не доступен 🟢 – доступен	30 мин.

Отклонение системного времени	Лаг времени на серверах Системы и сервере NTP **Примечание:** Данная ошибка возникает, если Системе не удалось установить соединение с NTP-серверами или в конфигурации Системы не указано ни одного NTP-сервера, появится сообщение об ошибке "can't create socket connection". Убедитесь, что в конфигурационных файлах ntp.conf и iwmon-services-ntp.cfg указан один и тот же корректный NTP-сервер.	– > 40 секунд – от 20 до 40 секунд – < 20 секунд	360 мин.
Ошибки в журнале предупреждений БД	Наличие ошибок в журнале предупреждений БД	– есть ошибки – нет ошибок	5 мин.
Размер журнала предупреждений БД	Проверяет размер журнала предупреждений: • Для СУБД Oracle Alert Log • Для СУБД PostgreSQL System Log	– > 100 Мб – от 50 до 100 Мб – < 50 Мб	5 мин.
Состояние базы данных	Состояние указанного экземпляра базы данных Oracle или PostgreSQL (в зависимости от используемой в системе СУБД).	– ok – <> ok	10 мин.
Свободное место в основном каталоге БД	Свободное место на партиции хранения основной информации (По умолчанию: `/u01`)	– < 10 000 Мб – от 10000 до 20 000 Мб – > 20 000 Мб	30 мин.
Доступность сервера	Доступность Linux серверов	– > 500 мл с – от 100 до 500 мл с – < 100 мл с	5 мин.
Свободное место в корне вой партиции	Наличие свободного места в корневой файловой системе	– < 10 000 Мб – от 10 000 МБ до 20 000 Мб – > 20 000 Мб	30 мин.
Состояние службы синхронизации времени	Доступность службы синхронизации времени	– NTP сервер доступен – NTP сервер не доступен	30 мин.
Состояние сервиса syslog	Проверяет, запущен или нет сервис syslog	– не запущен – запущен	30 мин.
Доступность сервера по SSH	Проверяет наличие ssh-сервиса на заданной группе серверов	– >= 10 секунд – < 10 секунд	10 мин.

Использование файла подкачки	Наличие свободного места в swap (виртуальная память)	🔴 – свободно < 10% 🟡 – свободно от 10 % до 20% 🟢 – свободно > 20%	5 мин.
Очередь обработки действий от примененных политик	Очередь обработки действий, указанных в примененных к событиям политиках	🔴 – > 1000 объектов 🟡 – от 200 до 1000 объектов 🟢< 200 объектов	30 мин.
Очередь ошибок обработки действий примененных политик	Количество ошибок обработки действий из применённых к событиям политик	🔴 – > 50 объектов 🟡 – от 1 до 50 объектов 🟢 = 0	30 мин.
Наличие дампов памяти	Работоспособность служб	🟢 – нет дампов 🔴 – есть дамп	30 мин.
Состояние компонентов Системы	Проверяет статусы служб системы	🔴 – хотя бы один сервис не запущен 🟢 – все сервисы запущены	30 мин.
Количество ошибок индексации	Количество ошибок индексации событий процессом **iw_indexer**	🔴 – > 50 🟡 – от 1 до 50 🟢 – 0	30 мин.
Очередь индексации	Очередь объектов на индексацию в Sphinx для полнотекстового поиска	🔴 – > 10000 🟡 – от 1000 до 10000 🟢 – < 1000	30 мин.
Очередь загрузки в хранилище	Скорость загрузки событий в базу данных (скорость обработки службой IW_LOADER объектов, которые помещает в очередь служба IW_XML2LIRO). Количество объектов в очереди	🔴 – > 10000 объектов 🟡 – от 1000 до 10000 объектов 🟢 – < 1000 объектов	30 мин.
Очередь ошибок в работе сервисов **iw_xml2liro** и **iw_loader**	Количество ошибок обработки событий службами IW_LOADER и IW_XML2LIRO	🔴 – > 50 объектов 🟡 – от 1 до 50 объектов 🟢 = 0	30 мин.
Количество запущенных процессов	Проверяет количество запущенных процессов	🔴 – > 600 процессов 🟡 – от 450 до 600 процессов 🟢 – < 450 процессов	30 мин.
Свободное место в партиции /var	Наличие свободного места в файловой системе `/var`	🔴 – < 10 000 Мб 🟡 – от 10 000 Мб до 20 000 Мб 🟢 – > 20 000 Мб	30 мин.

Свободное место в каталоге событий БД	Свободное место на партициях хранения событий. (По умолчанию: `/u02`)	– < 7% – от 7 до 15% – > 15%	30 мин.
Статус службы доступа к базе данных	Состояние службы доступа к базе данных. **Примечание:** Индикатор включен и отображаться в списке, только если в Системе используется СУБД Oracle	– TNS listener не запущен – TNS listener запущен	10 мин.
Наличие патчей БД	Наличие установленных патчей Oracle (17402822, 12919564), необходимых для корректной работы Системы **Примечание:** Индикатор включен и отображаться в списке, только если в Системе используется СУБД Oracle	– не установлен – установлен	30 мин.
Наличие ошибок в журнале базы данных	Проверяет syslog базы данных на наличие ошибок для схемы iwtm	– нет ошибок – есть ошибки	30 мин.

10 ПРИЛОЖЕНИЕ С. ЛИЦЕНЗИОННАЯ ИНФОРМАЦИЯ

10.1 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