



# **KEO DLP**

Версия 8.1.0

## **Руководство по установке и настройке**

2025

---

## Содержание

|                                                                              |     |
|------------------------------------------------------------------------------|-----|
| Перечень терминов и сокращений .....                                         | 10  |
| Использование стилей .....                                                   | 12  |
| 1. Введение .....                                                            | 13  |
| 1.1. Назначение документа .....                                              | 13  |
| 1.2. Аудитория .....                                                         | 13  |
| 2. О системе KEO DLP .....                                                   | 14  |
| 3. Условия эксплуатации .....                                                | 15  |
| 3.1. Требования к квалификации персонала .....                               | 15  |
| 3.2. Требования к АРМ администратора .....                                   | 15  |
| 3.2.1. Аппаратное обеспечение .....                                          | 15  |
| 3.2.2. Программное обеспечение .....                                         | 15  |
| 4. Планирование установки KEO DLP .....                                      | 17  |
| 4.1. Варианты установки .....                                                | 17  |
| 4.2. Режимы перехвата почтового потока .....                                 | 17  |
| 4.3. Выбор схемы развертывания .....                                         | 19  |
| 4.4. Рекомендации по размещению в сетевой инфраструктуре .....               | 19  |
| 4.5. Требования к серверам KEO DLP .....                                     | 26  |
| 4.5.1. Требования к одномашинной конфигурации .....                          | 27  |
| 4.5.2. Требования к распределенной конфигурации .....                        | 27  |
| 4.6. Требования к инфраструктуре .....                                       | 28  |
| 4.7. Необходимое ПО для установки .....                                      | 28  |
| 5. Установка ОС Debian .....                                                 | 29  |
| 6. Настройка системы и установка KEO DLP в интерфейсе командной строки ..... | 74  |
| 6.1. Настройка системы .....                                                 | 74  |
| 6.1.1. Настройка DNS .....                                                   | 74  |
| 6.1.2. Настройка файловой системы .....                                      | 74  |
| 6.1.3. Настройка синхронизации времени .....                                 | 75  |
| 6.2. Установка KEO DLP .....                                                 | 76  |
| 6.2.1. Установка в одномашинной конфигурации .....                           | 77  |
| 6.2.2. Установка в распределенной конфигурации .....                         | 78  |
| 6.3. Первый вход в систему .....                                             | 79  |
| 6.4. Загрузка лицензии .....                                                 | 81  |
| 6.4.1. Загрузка лицензии KEO DLP .....                                       | 81  |
| 6.4.2. Загрузка лицензий других продуктов .....                              | 86  |
| 7. Настройка KEO DLP для работы в активном режиме .....                      | 88  |
| 7.1. Настройка Exim4 .....                                                   | 88  |
| 7.2. Настройка профиля отправки .....                                        | 91  |
| 7.3. Создание правила политики фильтрации .....                              | 92  |
| 7.4. Настройка балансировщика .....                                          | 92  |
| 7.5. Настройка отправки сообщений при ошибках фильтрации .....               | 94  |
| 7.5.1. Настройка профиля отправки .....                                      | 94  |
| 7.5.2. Настройка отправки уведомлений о состоянии ресурсов системы .....     | 95  |
| 7.5.3. Создание правила политики фильтрации .....                            | 96  |
| 7.5.4. Активация отправки сообщений адресатам .....                          | 96  |
| 8. Первичная настройка KEO DLP .....                                         | 97  |
| 8.1. Настройка контроля целостности .....                                    | 97  |
| 8.2. Назначение ролей узлам .....                                            | 97  |
| 8.2.1. Назначение ролей с помощью GUI .....                                  | 98  |
| 8.2.2. Назначение ролей с помощью CLI .....                                  | 100 |
| 8.3. Создание и настройка БД архива PostgreSQL .....                         | 101 |

|                                                                                    |     |
|------------------------------------------------------------------------------------|-----|
| 8.3.1. Настройка схемы соединения с БД .....                                       | 101 |
| 8.3.2. Создание схемы БД .....                                                     | 102 |
| 8.4. Настройка БД для хранения событий и инцидентов ИБ .....                       | 104 |
| 8.5. Настройка сервера хранения медиаинформации .....                              | 107 |
| 8.6. Настройка синхронизации Досье .....                                           | 110 |
| 8.6.1. Синхронизация с FreeIPA .....                                               | 110 |
| 8.6.2. Синхронизация с ALD Pro .....                                               | 112 |
| 8.6.3. Синхронизация со службами каталогов без шифрования .....                    | 114 |
| 8.6.4. Синхронизация со службой LDAP с TLS .....                                   | 115 |
| 8.6.5. Синхронизация со сторонним Досье .....                                      | 117 |
| 8.6.6. Синхронизация с локальным источником .....                                  | 118 |
| 8.7. Настройка планировщика .....                                                  | 120 |
| 8.8. Настройка индексатора .....                                                   | 121 |
| 8.8.1. Общая настройка индексатора .....                                           | 121 |
| 8.8.2. Настройка индексации оперативных и исторических данных .....                | 125 |
| 8.9. Настройка файлового хранилища .....                                           | 126 |
| 8.10. Настройка перехвата файлов из МойОфис Документы Онлайн .....                 | 129 |
| 8.11. Настройка перехвата сообщений из Express .....                               | 130 |
| 8.12. Настройка перехвата сообщений из TrueConf Server .....                       | 132 |
| 8.13. Настройка перехвата сообщений из VK Teams .....                              | 134 |
| 8.14. Настройка перехвата сообщений из Cisco Webex Teams .....                     | 135 |
| 8.15. Настройка передачи информации в пользовательский сервер Zabbix .....         | 139 |
| 8.16. Настройка распознавания графических объектов .....                           | 140 |
| 8.17. Настройка распознавания речи .....                                           | 146 |
| 8.18. Настройка сервиса интеграции .....                                           | 147 |
| 8.18.1. Настройка взаимодействия по протоколу mTLS .....                           | 151 |
| 8.19. Выпуск сертификата организации для web-интерфейса .....                      | 157 |
| 8.20. Проверка работоспособности настроенного KEO DLP .....                        | 165 |
| 9. Работа модуля S/MIME .....                                                      | 170 |
| 9.1. Генерация ключей и сертификатов пользователей .....                           | 172 |
| 9.2. Настройка модуля S/MIME .....                                                 | 174 |
| 9.3. Настройка почтового клиента .....                                             | 175 |
| 9.3.1. Настройка Microsoft Outlook .....                                           | 175 |
| 9.3.2. Настройка Mozilla Thunderbird .....                                         | 181 |
| 10. Настройка системы подтверждения отправки сообщений .....                       | 191 |
| 10.1. Настройка аутентификации пользователей .....                                 | 191 |
| 10.1.1. Настройка LDAP-аутентификации пользователей .....                          | 191 |
| 10.2. Проверка работоспособности подсистемы подтверждения отправки сообщений ..... | 195 |
| 11. Установка модуля KEO DLP File Crawler .....                                    | 202 |
| 12. Установка модуля KEO DLP Traffic Analyzer .....                                | 204 |
| 13. Установка агентов .....                                                        | 205 |
| 14. Настройка антивируса .....                                                     | 206 |
| 14.1. Подключение Kaspersky .....                                                  | 206 |
| 14.2. Использование локального антивируса .....                                    | 206 |
| 15. Удаление KEO DLP .....                                                         | 208 |
| Приложение А. Настройка проверки пароля пользователя для подключения к БД ....     | 210 |
| Приложение В. Настройка подключения к БД под доменной учетной записью .....        | 213 |
| В.1. Создание доменной учетной записи для БД PostgreSQL .....                      | 213 |
| В.2. Настройка LDAPS-аутентификации .....                                          | 217 |
| В.3. Настройка SSL-подключения к БД PostgreSQL .....                               | 218 |
| В.3.1. Использование самоподписанных сертификатов .....                            | 218 |

|                                                                                            |     |
|--------------------------------------------------------------------------------------------|-----|
| В.3.2. Использование корпоративных сертификатов .....                                      | 220 |
| В.4. Настройка конфигурационного файла БД на использование SSL .....                       | 221 |
| Приложение С. Ответвление сообщений с почтовых серверов .....                              | 224 |
| С.1. Ответвление почтового потока с сервера Yandex .....                                   | 224 |
| С.1.1. Регистрация приложения .....                                                        | 224 |
| С.1.2. Добавление правил обработки писем .....                                             | 225 |
| С.1.3. Настройка KEO DLP File Crawler для сбора писем .....                                | 230 |
| С.1.4. Идентификация сообщений .....                                                       | 232 |
| С.2. Ответвление почтового потока с сервера «МойОфис Почта» .....                          | 232 |
| С.3. Ответвление почтового потока с сервера «МойОфис Mailion» .....                        | 234 |
| С.3.1. Пересылка скрытых копий сообщений (bcc) .....                                       | 234 |
| С.3.2. Пересылка всех исходящих сообщений .....                                            | 235 |
| С.3.3. Пересылка всех исходящих сообщений в зависимости от<br>отправителя .....            | 235 |
| С.4. Ответвление почтового потока с сервера Microsoft Exchange .....                       | 236 |
| С.4.1. Microsoft Exchange 2000 .....                                                       | 237 |
| С.4.2. Преобразование журнальных сообщений Exchange в оригинальные<br>SMTP-сообщения ..... | 237 |
| С.5. Ответвление почтового потока с сервера Exim .....                                     | 238 |
| С.6. Ответвление сообщений с сервера Microsoft Exchange 2003 .....                         | 239 |
| С.6.1. Общая последовательность действий .....                                             | 239 |
| С.6.2. Создание объекта типа «контакт» в Active Directory .....                            | 239 |
| С.6.3. Создание учетной записи пользователя .....                                          | 240 |
| С.6.4. Дополнительная настройка .....                                                      | 243 |
| С.6.5. Включение стандартного журналирования .....                                         | 246 |
| С.6.6. Включение ВСС-журналирования .....                                                  | 247 |
| С.6.7. Откат изменений .....                                                               | 248 |
| С.7. Ответвление сообщений с сервера Microsoft Exchange 2007 .....                         | 249 |
| С.7.1. Общая последовательность действий .....                                             | 250 |
| С.7.2. Создание объекта типа «контакт» в MS Exchange server 2007 .....                     | 251 |
| С.7.3. Настройка коннектора для пересылки сообщений на сервер<br>SMAP .....                | 252 |
| С.7.4. Включение журналирования .....                                                      | 252 |
| С.7.5. Проверка правильности работы журналирования .....                                   | 254 |
| С.8. Ответвление сообщений с сервера Microsoft Exchange 2013 .....                         | 255 |
| С.8.1. Общая последовательность действий .....                                             | 255 |
| С.8.2. Создание объекта типа «контакт» в MS Exchange server 2013 .....                     | 256 |
| С.8.3. Настройка коннектора для пересылки сообщений на сервер KEO<br>DLP .....             | 257 |
| С.8.4. Включение журналирования .....                                                      | 258 |
| Приложение D. Описание ролей и сервисов .....                                              | 260 |
| Приложение E. Описание файлового хранилища .....                                           | 267 |
| Е.1. Общая архитектура ФХ .....                                                            | 267 |
| Е.2. Запись данных в файловое хранилище и базу данных Cassandra .....                      | 269 |
| Е.3. Перемещение сообщений из локального ФХ в центральное .....                            | 269 |
| Е.4. Извлечение сообщения из файлового хранилища .....                                     | 270 |
| Приложение F. Создание БД архива на удаленном сервере .....                                | 272 |
| Лист контроля версий .....                                                                 | 274 |



---

## Список иллюстраций

|                                                                                                        |    |
|--------------------------------------------------------------------------------------------------------|----|
| 4.1. Схема подключения KEO DLP в пассивном режиме .....                                                | 17 |
| 4.2. Схема подключения одномашинной конфигурации KEO DLP в активном режиме .....                       | 18 |
| 4.3. Схема подключения распределенной конфигурации KEO DLP в активном режиме .....                     | 18 |
| 4.4. Схема подключения KEO DLP в гибридном режиме .....                                                | 19 |
| 4.5. Взаимодействие KEO DLP с внешними системами .....                                                 | 20 |
| 4.6. Взаимодействие KEO DLP Endpoint Agent с KEO DLP .....                                             | 21 |
| 5.1. Окно приветствия .....                                                                            | 29 |
| 5.2. Настройка клавиатуры .....                                                                        | 30 |
| 5.3. Выбор местоположения .....                                                                        | 31 |
| 5.4. Настройка раскладки клавиатуры .....                                                              | 32 |
| 5.5. Настройка сети .....                                                                              | 33 |
| 5.6. Окно настройки учетных записей: ввод пароля root .....                                            | 34 |
| 5.7. Окно настройки учетных записей: ввод имени учетной записи, которая используется вместо root ..... | 35 |
| 5.8. Ввод сокращенного имени учетной записи, которая используется вместо root .....                    | 36 |
| 5.9. Создание пароля для учетной записи, которая используется вместо root .....                        | 37 |
| 5.10. Окно Разметка дисков .....                                                                       | 39 |
| 5.11. Выбор области для разметки .....                                                                 | 40 |
| 5.12. Создание таблицы разделов .....                                                                  | 41 |
| 5.13. Выбор пространства для создания разделов .....                                                   | 42 |
| 5.14. Выбор варианта для создания раздела .....                                                        | 43 |
| 5.15. Задание размера раздела .....                                                                    | 44 |
| 5.16. Выбор типа раздела .....                                                                         | 45 |
| 5.17. Выбор местоположения раздела .....                                                               | 46 |
| 5.18. Параметры монтирования раздела .....                                                             | 47 |
| 5.19. Выбор типа раздела .....                                                                         | 48 |
| 5.20. Выбор варианта использования раздела .....                                                       | 49 |
| 5.21. Пункт настройки менеджера логических томов .....                                                 | 50 |
| 5.22. Создание группы томов для LVM .....                                                              | 51 |
| 5.23. Ввод имени группы томов .....                                                                    | 52 |
| 5.24. Выбор устройства для размещения группы томов .....                                               | 53 |
| 5.25. Задание имени логического тома root .....                                                        | 54 |
| 5.26. Выделение размера для логического тома root .....                                                | 55 |
| 5.27. Разметка дисков для master-узла .....                                                            | 56 |
| 5.28. Разметка дисков для slave-узла .....                                                             | 57 |
| 5.29. Настройки тома root .....                                                                        | 58 |
| 5.30. Выбор файловой системы .....                                                                     | 59 |
| 5.31. Выбор точки монтирования .....                                                                   | 60 |
| 5.32. Заполненные настройки тома root .....                                                            | 61 |
| 5.33. Заполненные настройки томов для master-узла .....                                                | 62 |
| 5.34. Заполненные настройки томов для slave-узла .....                                                 | 63 |
| 5.35. Предупреждение об отсутствии разделов для пространства подкачки .....                            | 64 |
| 5.36. Информация о разметке дисков .....                                                               | 65 |
| 5.37. Отказ от сканирования другого носителя .....                                                     | 66 |
| 5.38. Выбор местоположения зеркала архива Debian .....                                                 | 67 |
| 5.39. Выбор зеркала архива Debian .....                                                                | 68 |
| 5.40. Добавление информации о прокси-сервере .....                                                     | 69 |

---

|                                                                                                    |     |
|----------------------------------------------------------------------------------------------------|-----|
| 5.41. Выбор программного обеспечения .....                                                         | 70  |
| 5.42. Окно установки системного загрузчика GRUB .....                                              | 71  |
| 5.43. Выбор устройства установки загрузчика .....                                                  | 72  |
| 5.44. Завершение установки ОС Debian .....                                                         | 73  |
| 6.1. Окно авторизации при входе в систему .....                                                    | 80  |
| 6.2. Окно смены пароля .....                                                                       | 81  |
| 6.3. Уведомление об отсутствии лицензии .....                                                      | 82  |
| 6.4. Информация о лицензии KEO DLP .....                                                           | 83  |
| 7.1. Выбор типа почтовой конфигурации .....                                                        | 89  |
| 7.2. Ввод имени узла .....                                                                         | 89  |
| 7.3. Ввод loopback-адреса .....                                                                    | 89  |
| 7.4. Окно ввода локальных доменов .....                                                            | 89  |
| 7.5. Ввод доменов, для которых Exim будет ретранслировать сообщения .....                          | 89  |
| 7.6. Ввод IP-адреса и порта почтового сервера организации .....                                    | 90  |
| 7.7. Скрытие локального имени сервера .....                                                        | 90  |
| 7.8. Отключение поиска DNS при запуске .....                                                       | 90  |
| 7.9. Выбор метки доставки локальной почты .....                                                    | 90  |
| 7.10. Выбор разбиения конфигурации на маленькие файлы .....                                        | 90  |
| 7.11. Добавление профиля отправки .....                                                            | 91  |
| 7.12. Правило фильтрации для активного режима .....                                                | 92  |
| 7.13. Правило отправки при ошибках .....                                                           | 96  |
| 8.1. Назначение ролей .....                                                                        | 98  |
| 8.2. Разбиение на страницы .....                                                                   | 99  |
| 8.3. Поиск узлов .....                                                                             | 99  |
| 8.4. Кнопка принудительной синхронизации Досье .....                                               | 112 |
| 8.5. Кнопка принудительной синхронизации Досье .....                                               | 113 |
| 8.6. Кнопка принудительной синхронизации Досье .....                                               | 115 |
| 8.7. Кнопка принудительной синхронизации Досье .....                                               | 117 |
| 8.8. Создание графического шаблона .....                                                           | 142 |
| 8.9. Пример настройки графического шаблона .....                                                   | 143 |
| 8.10. Создание условия .....                                                                       | 144 |
| 8.11. Настройка условия .....                                                                      | 144 |
| 8.12. Создание набора правил .....                                                                 | 145 |
| 8.13. Настройка набора правил "Управление печатями" .....                                          | 145 |
| 8.14. Запрос Применить политику .....                                                              | 149 |
| 8.15. Результат выполнения запроса Применить политику .....                                        | 150 |
| 8.16. Просмотр сертификатов в настройках браузера Mozilla Firefox .....                            | 155 |
| 8.17. Добавление сертификата в формате PFX в хранилище сертификатов браузера Mozilla Firefox ..... | 155 |
| 8.18. Добавление сертификата в формате crt в хранилище сертификатов браузера Mozilla Firefox ..... | 156 |
| 8.19. Подтверждение выбора сертификата в сервисе интеграции KEO DLP .....                          | 156 |
| 8.20. Просмотр информации о соединении с сервисом интеграции KEO DLP .....                         | 157 |
| 8.21. Экран приветствия УЦ Windows .....                                                           | 160 |
| 8.22. Экран запроса сертификата .....                                                              | 160 |
| 8.23. Экран особого запроса сертификата .....                                                      | 161 |
| 8.24. Экран атрибутов сертификата .....                                                            | 162 |
| 8.25. Экран выдачи сертификата .....                                                               | 163 |
| 8.26. Экран приветствия УЦ Windows .....                                                           | 163 |
| 8.27. Раздел Поиск .....                                                                           | 166 |
| 8.28. Результат поиска .....                                                                       | 167 |
| 9.1. Настройка параметров S/MIME .....                                                             | 175 |

|                                                                                      |     |
|--------------------------------------------------------------------------------------|-----|
| 9.2. Окно Параметры Outlook .....                                                    | 175 |
| 9.3. Окно Центр управления безопасностью .....                                       | 176 |
| 9.4. Окно Импорт/экспорт цифрового удостоверения .....                               | 177 |
| 9.5. Файл сертификата в формате .p12 .....                                           | 178 |
| 9.6. Данные для импорта сертификата .....                                            | 179 |
| 9.7. Импорт нового закрытого ключа .....                                             | 180 |
| 9.8. Выбор уровня защиты .....                                                       | 180 |
| 9.9. Завершение импорта закрытого ключа .....                                        | 181 |
| 9.10. Просмотр параметров учетной записи .....                                       | 182 |
| 9.11. Окно Параметры учетной записи .....                                            | 183 |
| 9.12. Параметры настройки шифрования и работы с зашифрованными сообщениями .....     | 184 |
| 9.13. Окно Управление устройствами .....                                             | 185 |
| 9.14. Окно создания мастер-пароля .....                                              | 185 |
| 9.15. Окно менеджера сертификатов .....                                              | 186 |
| 9.16. Выбор файла сертификата .....                                                  | 186 |
| 9.17. Ввод мастер-пароля .....                                                       | 187 |
| 9.18. Ввод пароля для экспорта сертификата .....                                     | 187 |
| 9.19. Сообщение об успешном завершении операции .....                                | 188 |
| 9.20. Импортированный сертификат пользователя .....                                  | 188 |
| 9.21. Выбор сертификата для шифрования почтовых сообщений .....                      | 189 |
| 9.22. Выбор сертификата для шифрования почтовых сообщений .....                      | 189 |
| 9.23. Завершение настройки личных сертификатов .....                                 | 190 |
| 10.1. Настройки модуля подтверждения отправки сообщений .....                        | 193 |
| 10.2. Создание шаблона уведомления «Нарушение политики безопасности» .....           | 196 |
| 10.3. Заполнение полей шаблона уведомления «Нарушение политики безопасности» .....   | 197 |
| 10.4. Создание условия .....                                                         | 198 |
| 10.5. Настройка условия .....                                                        | 199 |
| 10.6. Создание набора правил «Уведомление пользователей» .....                       | 199 |
| 10.7. Настройка набора правил «Уведомление пользователей» .....                      | 200 |
| 10.8. Уведомление о нарушении политики безопасности .....                            | 200 |
| 10.9. Таблица с данными сообщений, ожидающих подтверждения отправки .....            | 201 |
| 11.1. Назначение узлу роли Краулер .....                                             | 202 |
| 11.2. Раздел "Краулер" .....                                                         | 203 |
| В.1. Настройка LDAP-аутентификации в pg_hba.conf .....                               | 215 |
| В.2. Проверка соединения с БД после смены пользователя .....                         | 216 |
| В.3. Пример заполнения секции # - SSL в конфигурационном файле postgresql.conf ..... | 222 |
| В.4. Пример вывода команды для проверки SSL-соединений с БД .....                    | 223 |
| С.1. Условие для поиска сообщений Yandex 360 .....                                   | 232 |
| С.2. Форма New Object > Contact .....                                                | 240 |
| С.3. Скрытие адреса пользователя в досье .....                                       | 241 |
| С.4. Свойства пользователя, вкладка Exchange General .....                           | 242 |
| С.5. Окно Delivery Options .....                                                     | 243 |
| С.6. Свойства виртуального сервера SMTP .....                                        | 244 |
| С.7. Создание коннектора. Вкладка Address .....                                      | 246 |
| С.8. Установка архивирования всех сообщений из хранилища .....                       | 247 |
| С.9. Редактирование реестра для включения BCC-журналирования .....                   | 248 |
| С.10. Перезапуск службы SMTP .....                                                   | 248 |
| С.11. Схема ответвления почтового потока .....                                       | 249 |
| С.12. Окно редактирования свойств контакта в MS Exchange 2007 .....                  | 251 |

---

|                                                                                    |     |
|------------------------------------------------------------------------------------|-----|
| С.13. Окно свойств почтовой базы Exchange .....                                    | 253 |
| С.14. Создание правила журналирования .....                                        | 254 |
| С.15. Центр администрирования Exchange .....                                       | 256 |
| С.16. Создание почтового контакта .....                                            | 257 |
| С.17. Консоль Exchange Management Shell .....                                      | 258 |
| С.18. Создание группы рассылки .....                                               | 259 |
| С.19. Создание правила журналирования .....                                        | 259 |
| Е.1. Общая схема организации распределенного файлового хранилища .....             | 268 |
| Е.2. Добавление записей в базу данных Cassandra .....                              | 269 |
| Е.3. Перемещение сообщений из локального в центральное файловое<br>хранилище ..... | 270 |
| Е.4. Извлечение сообщения из файлового хранилища .....                             | 271 |

---

## Список таблиц

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| 4.1. Описание портов, используемых по умолчанию .....                | 22  |
| 4.2. Требования к серверу KEO DLP .....                              | 27  |
| 4.3. Требования к оборудованию master-узла кластера KEO DLP .....    | 27  |
| 4.4. Требования к оборудованию slave-узлов кластера KEO DLP .....    | 27  |
| 6.1. Контрольный лист действий при одномашинной конфигурации .....   | 76  |
| 6.2. Контрольный лист действий при распределенной конфигурации ..... | 76  |
| 8.1. Таблица групп .....                                             | 118 |
| 8.2. Таблица персон .....                                            | 119 |

## Перечень терминов и сокращений

|                  |                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| АРМ              | Автоматизированное рабочее место                                                                                                                                                                                                                                                                                                                                                   |
| БД               | База данных                                                                                                                                                                                                                                                                                                                                                                        |
| ИБ               | Информационная безопасность                                                                                                                                                                                                                                                                                                                                                        |
| ИТ               | Исключаемый текст                                                                                                                                                                                                                                                                                                                                                                  |
| КА               | Контентный анализ                                                                                                                                                                                                                                                                                                                                                                  |
| МРД              | Мандатное управление доступом                                                                                                                                                                                                                                                                                                                                                      |
| ОЕ               | Организационная единица                                                                                                                                                                                                                                                                                                                                                            |
| ОС               | Операционная система                                                                                                                                                                                                                                                                                                                                                               |
| ПО               | Программное обеспечение                                                                                                                                                                                                                                                                                                                                                            |
| ПК               | Программный комплекс                                                                                                                                                                                                                                                                                                                                                               |
| СХД              | Система хранения данных                                                                                                                                                                                                                                                                                                                                                            |
| KEO DLP webProxy | Модуль контроля веб-трафика                                                                                                                                                                                                                                                                                                                                                        |
| СУБД             | Система управления базами данных                                                                                                                                                                                                                                                                                                                                                   |
| УЗ               | Учетная запись (пользователя)                                                                                                                                                                                                                                                                                                                                                      |
| УЦ               | Удостоверяющий центр                                                                                                                                                                                                                                                                                                                                                               |
| ФХ               | Файловое хранилище                                                                                                                                                                                                                                                                                                                                                                 |
| ЦП               | Центральный процессор – электронный блок либо интегральная схема, исполняющая машинные инструкции, главная часть аппаратного обеспечения компьютера или программируемого логического контроллера                                                                                                                                                                                   |
| ЭЦП              | Электронная цифровая подпись                                                                                                                                                                                                                                                                                                                                                       |
| AD               | Active Directory – служба каталогов для операционных систем семейства Windows. В каталоге хранятся сведения о различных объектах сетей, например, о компьютерах и учетных записях их пользователей. С помощью AD можно использовать групповые политики для единообразия настройки пользовательской рабочей среды и развертывания программного обеспечения на множестве компьютеров |
| CEF              | Common Event Format – общий формат события                                                                                                                                                                                                                                                                                                                                         |
| CLI              | Command Line Interface – интерфейс командной строки                                                                                                                                                                                                                                                                                                                                |
| CRL              | Certificate Revocation List – список отозванных сертификатов                                                                                                                                                                                                                                                                                                                       |
| DC               | Domain controller — контроллер домена                                                                                                                                                                                                                                                                                                                                              |
| DHCP             | Dynamic Host Configuration Protocol – протокол динамической настройки узла                                                                                                                                                                                                                                                                                                         |
| FQDN             | Fully Qualified Domain Name – полное имя домена (имя домена, не имеющее неоднозначностей в определении)                                                                                                                                                                                                                                                                            |
| GUI              | Graphical User Interface – графический интерфейс пользователя                                                                                                                                                                                                                                                                                                                      |
| MD               | Обозначение используется на рисунках и помечает элемент управления, отображаемый при наличии в системе модуля централизованного управления системой                                                                                                                                                                                                                                |
| MIME             | Multipurpose Internet Mail Extension – многоцелевое расширение Интернет-почты                                                                                                                                                                                                                                                                                                      |

---

|             |                                                                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PID         | Product Identifier – Идентификатор модели устройства                                                                                                                       |
| RFC         | Request for Comments – спецификации и стандарты, применяемые в Интернет                                                                                                    |
| SMB         | Server Message Block – сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия |
| SMTP        | Simple Mail Transfer Protocol – простой протокол передачи почты                                                                                                            |
| TNEF        | Transport Neutral Encapsulation Format – собственный формат вложений электронной почты, используемый Microsoft Outlook и Microsoft Exchange Server                         |
| TTS         | Transportable Tablespaces – транспортируемые (перемещаемые) табличные пространства                                                                                         |
| VID         | Vendor Identifier – Идентификатор производителя                                                                                                                            |
| Кластер     | Совокупность серверов KEO DLP, соединенных между собой управляющими связями.                                                                                               |
| master-узел | Управляющий (главный) сервер кластера KEO DLP, непосредственно связанный с каждым из остальных.                                                                            |
| slave-узел  | Любой узел кластера KEO DLP, не являющийся управляющим.                                                                                                                    |

---

## Использование стилей

|                                                 |                                   |
|-------------------------------------------------|-----------------------------------|
| Шрифт без форматирования                        | Основной текст                    |
| <b>Моноширинный шрифт</b>                       | Пользовательский ввод             |
| Рамка                                           | Программный вывод на экран        |
| <i>Курсивный шрифт</i>                          | Наименования документов           |
| <u>Полужирный подчеркнутый фиолетовый шрифт</u> | Внутренняя ссылка                 |
| <b>Полужирный шрифт</b>                         | Наименование элементов интерфейса |



---

# 1. Введение

## 1.1. Назначение документа

В настоящем руководстве описаны задачи, возникающие при развертывании ПК «KEO DLP» (далее – KEO DLP), а также способы и примеры их решения в ряде стандартных сценариев.

## 1.2. Аудитория

Документ предназначен для системных и сетевых администраторов, а также для сотрудников службы информационной безопасности компаний, внедряющих KEO DLP.

---

## 2. О системе KEO DLP

Программный комплекс «KEO DLP» – это система контроля корпоративных коммуникаций класса Data Leak Prevention (DLP), с помощью которой можно выявлять и блокировать несанкционированную передачу данных с компьютеров, а также определять признаки корпоративного мошенничества.

К основным функциональным возможностям KEO DLP относятся:

- контроль каналов утечки данных (электронной почты, социальных сетей, мессенджеров и т. п.);
- контроль использования сетевых ресурсов сотрудниками;
- отслеживание и ограничение движения потоков информации;
- отслеживание и блокирование сетевых коммуникаций сотрудников;
- сбор, анализ и хранение сообщений о фактах передачи информации (при этом обеспечивается анализ содержимого сообщений и документов; выявление документов определенной структуры и содержания; сравнение текстовых, графических и табличных документов с заранее заданными эталонными документами; распознавание в текстах сообщений определенных последовательностей – ИНН, номеров паспортов и т. д.);
- сбор, систематизация и хранение данных о сотрудниках (ведение досье на каждого сотрудника);
- сбор, систематизация и хранение данных о местонахождении материалов, содержащих конфиденциальную информацию, и о сотрудниках, имеющих доступ к ним;
- поддержка процессов работы сотрудников службы безопасности (создание и настройка правил передачи и хранения информации; мониторинг событий и инцидентов; отслеживание действий сотрудников; назначение сотрудников, ответственных за разбор инцидентов; получение статистических отчетов);
- поддержка проведения расследований инцидентов информационной и экономической безопасности (поиск данных, выявление рабочих и личных контактов сотрудников; предоставление данных для анализа сетевой активности каждого сотрудника; подсказка следующих шагов в процессе расследования);
- учет и контроль рабочего времени сотрудников;
- мониторинг и анализ особенностей поведения персон и ресурсов на основе данных об их информационных коммуникациях.

---

## 3. Условия эксплуатации

### 3.1. Требования к квалификации персонала

Квалификация системного администратора KEO DLP должна быть достаточной для выполнения задач по обслуживанию системы, обеспечивающих бесперебойное функционирование всех ее компонентов.

К задачам системного администратора KEO DLP относятся:

- настройка компонентов KEO DLP;
- мониторинг процессов системы;
- управление подсистемой архивирования;
- реагирование на служебные уведомления системы.

Требования к квалификации системного администратора KEO DLP:

- знания и навыки администрирования ОС Linux и СУБД PostgreSQL;
- понимание особенностей работы KEO DLP;
- понимание работы сетевых протоколов;
- базовые знания языка PL/SQL;
- знания в области безопасности ОС класса UNIX.

В своей работе системные администраторы KEO DLP должны использовать документацию по обслуживанию KEO DLP и документацию по ОС Linux и СУБД PostgreSQL.

### 3.2. Требования к АРМ администратора

#### 3.2.1. Аппаратное обеспечение

АРМ системного администратора KEO DLP должно быть оборудовано персональным компьютером с подключением к интернету. Минимально рекомендованные характеристики оборудования:

- Объем свободной оперативной памяти – не менее 4 ГБ после загрузки браузера.
- Разрешение экрана при работе с GUI от 1600x900.

АРМ системного администратора KEO DLP должно иметь терминальный доступ к master-узлу KEO DLP.

#### 3.2.2. Программное обеспечение

В состав ПО компьютера для АРМ системного администратора KEO DLP должен входить браузер. Гарантируется корректная работа GUI KEO DLP в браузерах Google Chrome, Mozilla Firefox, Yandex, Edge и Atom актуальных версий. В других браузерах работа GUI KEO DLP невозможна.

---

Для корректной работы GUI KEO DLP необходимо в настройках браузера разрешить выполнение **javascript** и сохранение файлов **cookies**. Кроме того, рекомендуется отключить сторонние расширения браузера, поскольку некоторые расширения могут негативно влиять на работу KEO DLP.

### **Внимание!**

*Рекомендуется использовать настройки размера шрифта и масштаба экрана по умолчанию, поскольку изменение этих настроек может привести к искажению дизайна и некорректной работе GUI KEO DLP.*

## 4. Планирование установки KEO DLP

### 4.1. Варианты установки

KEO DLP имеет три варианта установки:

- **Одномашинная конфигурация** – все функции KEO DLP выполняются одним физическим сервером.
- **Распределенная конфигурация** – функции KEO DLP выполняются несколькими серверами. Такая конфигурация позволяет равномерно распределять нагрузку между серверами и достигать таким образом большей производительности. Количество серверов может быть увеличено в любой момент эксплуатации KEO DLP без его остановки. Распределенная конфигурация (кластер) KEO DLP имеет топологию «звезда», то есть один из узлов (главный) непосредственно связан с каждым из остальных (подчиненные узлы).

В одномашинной конфигурации сервер KEO DLP является главным узлом. Здесь и далее главный узел будет называться master-узлом, а подчиненные – slave-узлами.

### 4.2. Режимы перехвата почтового потока

Перехват почтовых сообщений в KEO DLP осуществляется в одном из трех режимов:

- **Пассивный режим** – серверы KEO DLP не препятствуют ни передаче почтовых сообщений внутри корпоративной сети, ни почтовому потоку между корпоративной сетью и внешним миром. В этом режиме на почтовых серверах организации настраивается ответвление почтового потока на сервер (серверы) KEO DLP для дальнейшего анализа и хранения. Процедура настройки ответвления почтового потока подробно описана в разделе [Приложение С. Ответвление сообщений с почтовых серверов](#).

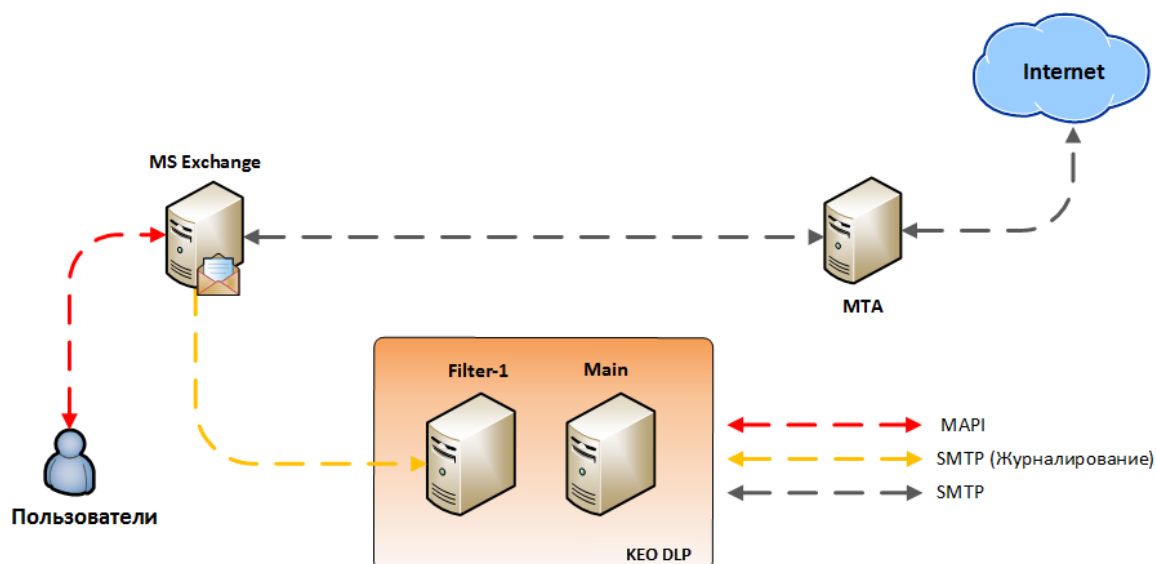


Рис. 4.1. Схема подключения KEO DLP в пассивном режиме

- **Активный режим** – серверы KEO DLP не препятствуют передаче почтовых сообщений внутри корпоративной сети, но создают барьер на пути почтового потока между кор-

поративной сетью и внешним миром. В этом режиме становится возможным активный контроль передачи почтовых сообщений в соответствии с заданными критериями вплоть до полной их блокировки. Активный режим требует включения сервера (серверов) KEO DLP в разрыв между почтовым сервером организации и почтовым шлюзом.

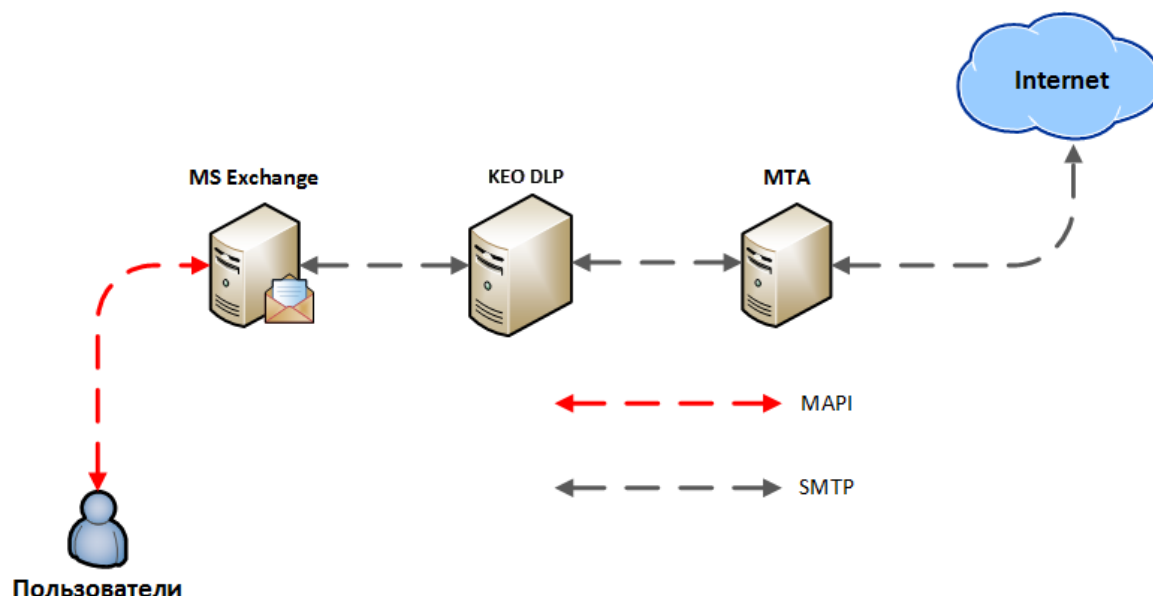


Рис. 4.2. Схема подключения одномашинной конфигурации KEO DLP в активном режиме

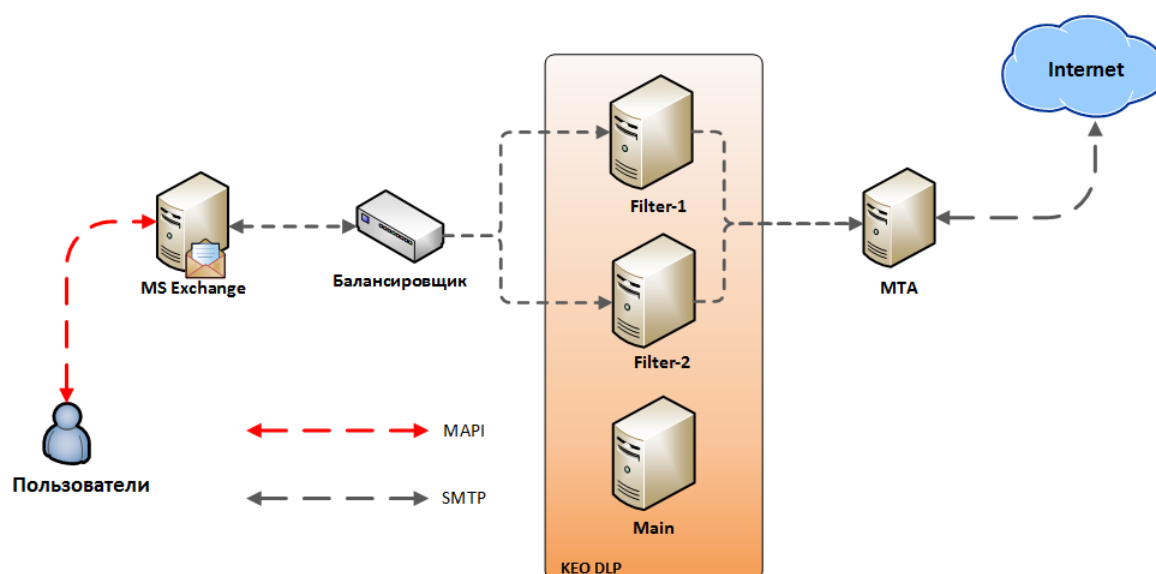


Рис. 4.3. Схема подключения распределенной конфигурации KEO DLP в активном режиме

Для работы распределенной конфигурации в активном режиме требуется наличие балансировщика нагрузки на серверы фильтрации. Функции балансировщика могут быть реализованы как с помощью специального аппаратного обеспечения, так и с помощью программных настроек почтового сервера организации.

- Гибридный режим – на пути почтового потока между корпоративной сетью и внешним миром создается барьер лишь для одного направления (например, исходящая почта), а другое направление контролируется в пассивном режиме. В гибридном режиме на-

личие балансировщика требуется только в случае, когда барьер на активно контролируемом направлении создан двумя или более серверами.

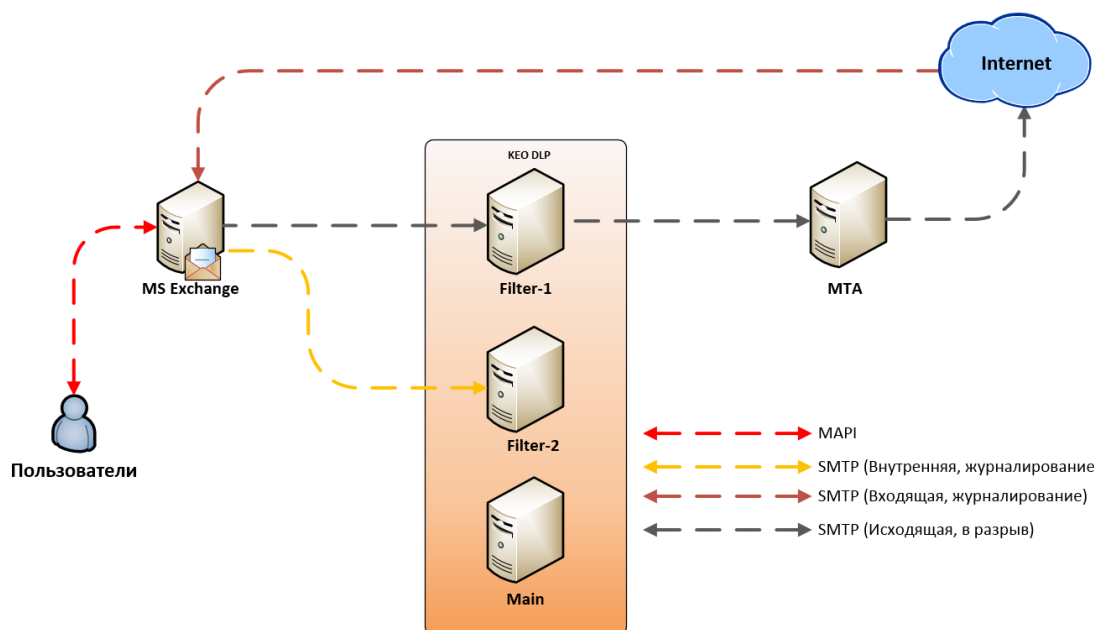


Рис. 4.4. Схема подключения KEO DLP в гибридном режиме

### 4.3. Выбор схемы развертывания

Не рекомендуется использовать одномашинную конфигурацию при большом объеме почтового трафика (более 10 ГБ в сутки), так как при этом возрастает риск аварийной остановки KEO DLP в случае сбоев при фильтрации почтовых сообщений. Следует использовать распределенную конфигурацию, в которой задачи фильтрации ложатся на slave-узлы, а master-узел освобожден от них. Если в организации существуют требования к отказоустойчивости, предполагающие безостановочную работу KEO DLP, рекомендуется использование двух или более slave-узлов в качестве почтовых фильтров, так как в этом случае аварийная остановка одного из них не приводит к прекращению фильтрации в целом.

Активный (гибридный) режим используется если существует необходимость контролировать передаваемые данные в реальном времени, например, если внутри корпоративной сети имеются высокочувствительные к разглашению сведения.

В любой конфигурации KEO DLP существует возможность горизонтального масштабирования. Кластер KEO DLP в любой момент может быть дополнен любым количеством серверов, при этом нет необходимости в остановке работающих узлов кластера.

### 4.4. Рекомендации по размещению в сетевой инфраструктуре

Настоятельно рекомендуется размещать кластер KEO DLP в отдельной подсети, в которую нет доступа из других корпоративных подсетей. Системные администраторы и администраторы безопасности должны иметь доступ к веб-интерфейсу master-узла по протоколу

HTTPS, системные администраторы должны дополнительно иметь доступ к master-узлу по протоколу SSH.

Схема верхнего уровня взаимодействия KEO DLP с внешними системами представлена на [Рис.4.5](#). Синим цветом обозначены сервисы KEO DLP, а белым – внешние сервисы корпоративной сети.

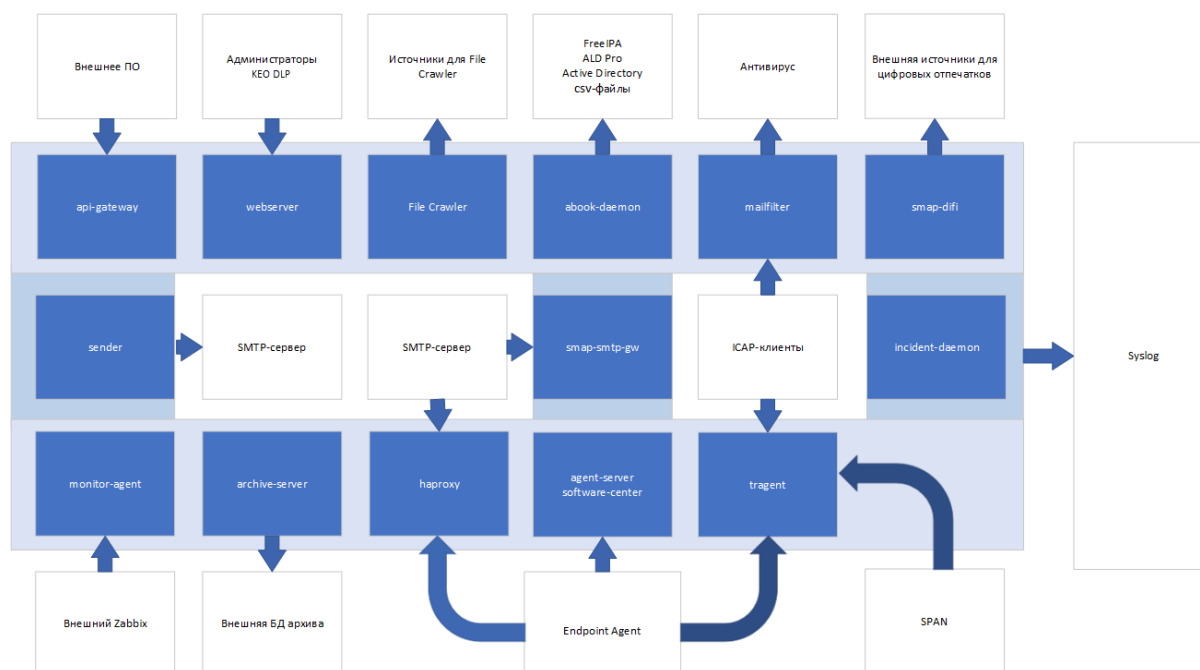


Рис. 4.5. Взаимодействие KEO DLP с внешними системами

Пример взаимодействия сервисов и утилит KEO DLP по обеспечению функционирования модуля KEO DLP Endpoint Agent представлен на [Рис.4.6](#).



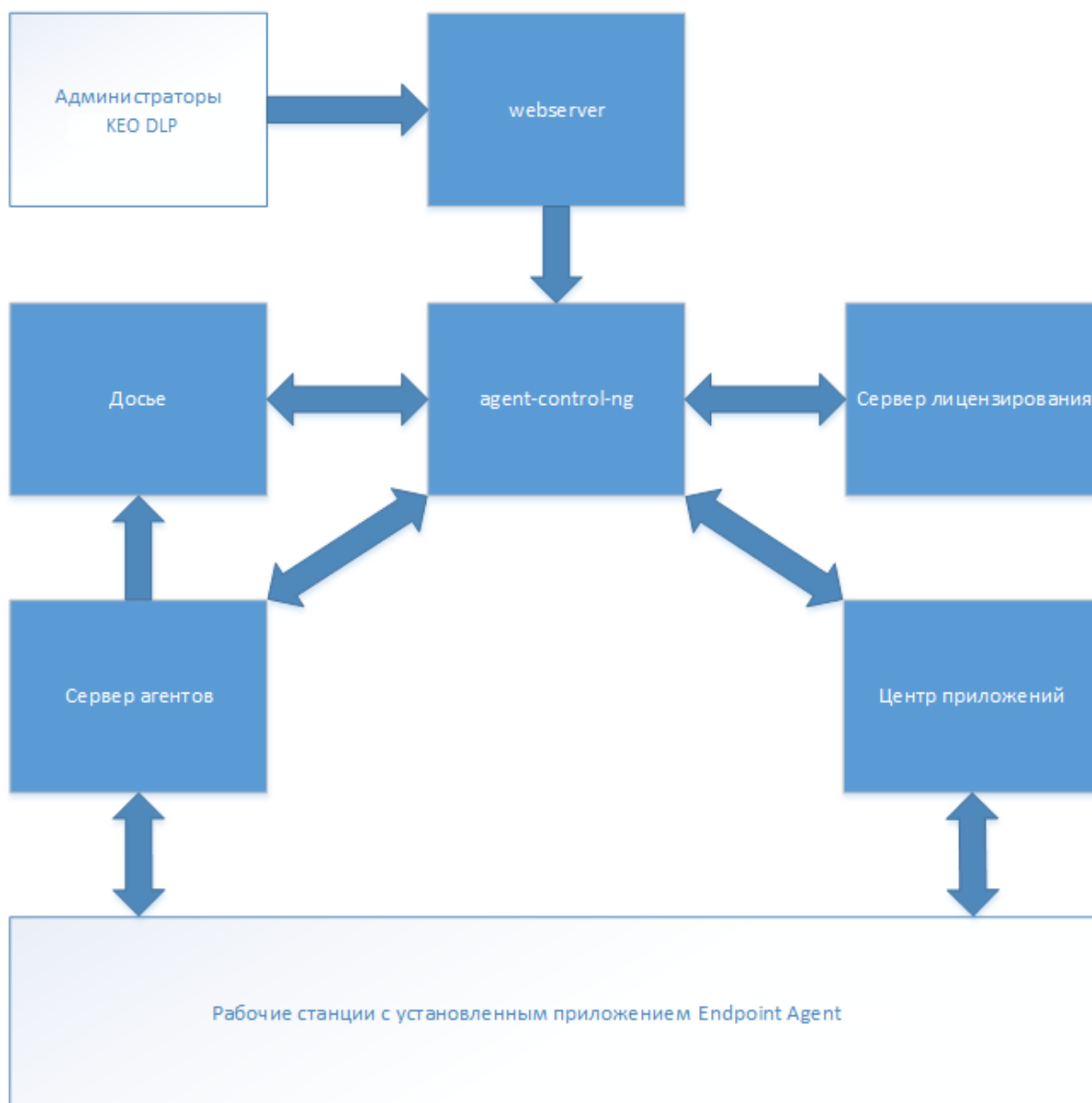


Рис. 4.6. Взаимодействие KEO DLP Endpoint Agent с KEO DLP

В [Табл.4.1](#) приведено описание взаимодействия сервисов и утилит KEO DLP с указанием портов, назначенных по умолчанию. Все сервисы используют протокол TCP.

### Внимание!

При обновлении с предыдущих версий используемые порты автоматически не меняются, даже если был установлен порт по умолчанию, и в новой версии он отличается от порта в старой. В этом случае следует обратиться к документации на изначально установленную версию.

Табл. 4.1. Описание портов, используемых по умолчанию

| Порт | Сервисы                                                                              |                                     | Описание                                                                                                                                                              |
|------|--------------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | откуда                                                                               | куда                                |                                                                                                                                                                       |
| 22   | APM администратора                                                                   | Узлы KEO DLP                        | Удаленное администрирование                                                                                                                                           |
| 22   | Узлы KEO DLP                                                                         | Узлы KEO DLP                        | Взаимодействие узлов KEO DLP между собой                                                                                                                              |
| 80   | monitor-httpd                                                                        | monitor-httpd                       | Веб-сервер подсистемы мониторинга                                                                                                                                     |
| 389  | abook-sync<br>abook-daemon<br>agent-control-ng<br>monitor-ng                         | Контроллеры домена,<br>серверы LDAP | Отображение данных пользователей и рабочих станций из домена Active Directory в системе KEO DLP                                                                       |
| 443  | APM администратора                                                                   | webserver                           | Организация точки входа в веб-интерфейс администратора                                                                                                                |
| 1010 | mailfilter                                                                           | HAProxy                             | Взаимодействие с внешним балансировщиком                                                                                                                              |
| 1025 | sender<br>Почтовый сервер                                                            | smap-smtp-gw                        | Ответвление почтового трафика в KEO DLP                                                                                                                               |
| 1344 | mailfilter<br>Прокси-серверы                                                         | Антивирус<br>tragent                | Прием запросов на поиск вирусов по протоколу ICAP от узла с ролью <b>Фильтр почтового потока</b><br><br>Прием запросов по протоколу ICAP от ICAP-прокси               |
| 2214 | ds-bus-rc                                                                            | Узлы KEO DLP                        | Распределенное управление кластером KEO DLP                                                                                                                           |
| 2266 | archive-server                                                                       | filestorage-ng                      | Извлечение сообщений из файлового хранилища                                                                                                                           |
| 2266 | abook-daemon                                                                         | filestorage-ng                      | Прикрепление сохраненных файлов к карточке персоны                                                                                                                    |
| 2266 | filestorage-ng                                                                       | filestorage-ng                      | Перенос сообщений из локального файлового хранилища в центральное файловоe хранилище                                                                                  |
| 2269 | webserver                                                                            | abook-daemon                        | Работа с Досье (просмотр и редактирование)                                                                                                                            |
| 2269 | agent-control-ng                                                                     | abook-daemon                        | Получение информации о пользователях для привязки к APM                                                                                                               |
| 2269 | agent-server                                                                         | abook-daemon                        | Получение информации об активности персон (контроль рабочего времени)                                                                                                 |
| 2269 | mailfilter<br>archive-server<br>crawler-ccc<br>report-server<br>abook-daemon (slave) | abook-daemon                        | Получение информации о персонах для использования в политике фильтрации. Перенос информации о персонах и группах в архив для использования в поиске и для индексации. |
| 2272 | webserver                                                                            | incident-daemon                     | Работа с инцидентами (просмотр и редактирование)                                                                                                                      |
| 2344 | mailfilter                                                                           | Антивирус                           | Прием запросов на поиск вирусов по протоколу ICAP от узла с ролью <b>Фильтр почтового потока</b>                                                                      |
| 3000 | archiver                                                                             | archive-server                      | Помещение сообщений в архив                                                                                                                                           |
| 3000 | webserver                                                                            | archive-server                      | Получение сообщений из архива                                                                                                                                         |

| Порт          | Сервисы                                                                                                          |                                        | Описание                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------|
|               | откуда                                                                                                           | куда                                   |                                                                                                                 |
| 3001          | webserver                                                                                                        | action-server                          | Выполнение действий над сообщениями                                                                             |
| 3002          | webserver<br>mailfilter                                                                                          | category-server                        | Проверка принадлежности текстов категориям (антиспам)                                                           |
| 3003          | agent-server<br>webserver                                                                                        | agent-media-server                     | Помещение медиаинформации в хранилище                                                                           |
| 3004          | webserver<br>mailfilter<br>crawler-ccc<br>agent-control-ng                                                       | license-server                         | Получение информации о лицензии                                                                                 |
| 3006 (master) | agent-server                                                                                                     | agent-control-ng                       | Передача данных об агентах серверу управления endpoint-серверами                                                |
| 3010          | tragent                                                                                                          | mailfilter                             | Прием сообщений от узла с ролью <b>Сервис перехвата и анализа сетевого трафика</b>                              |
| 3012          | agent-server                                                                                                     | media-processor-action-server          | Прием запросов от сервера агентов на создание задач по распознаванию текста медиаданных и выдача их результатов |
| 3030          | webserver                                                                                                        | uba-server                             | Подключение к сервису <b>uba-server</b> из веб-интерфейса                                                       |
| 3268          | abook-sync<br>abook-daemon<br>agent-control-ng<br>monitor-ng                                                     | Контроллеры домена, серверы LDAP       | Отображение данных пользователей и рабочих станций из домена Active Directory в системе KEO DLP                 |
| 3900          | webserver                                                                                                        | grafana                                | Прием соединений от сервера веб-интерфейса                                                                      |
| 4444          | agent                                                                                                            | agent-server                           | Сервер агентов                                                                                                  |
| 5434          | abook-sync<br>action-server<br>abook-daemon<br>webserver<br>report-server<br>agent-control-ng<br>software-center | database                               | Доступ сервисов к БД политики                                                                                   |
| 5439          | crawler-ccc<br>crawler-pccc<br>crawler-snapshot                                                                  | crawler-database                       | Доступ Crawler (Краулера) к БД PostgreSQL                                                                       |
| 5440          | action-server                                                                                                    | action-server-database                 | Доступ сервера действий к своей БД                                                                              |
| 5441          | software-center                                                                                                  | software-center-database               | Доступ Центра приложений к своей БД                                                                             |
| 5442          | media-processor-action-server                                                                                    | media-processor-action-server-database | Доступ сервера действий по обработке медиаданных к своей БД                                                     |
| 5443          | detective-server                                                                                                 | detective-database                     | Доступ сервиса <b>Расследование</b> к своей БД                                                                  |

| Порт | Сервисы                                       |                                               | Описание                                                                                                                                                     |
|------|-----------------------------------------------|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | откуда                                        | куда                                          |                                                                                                                                                              |
| 5445 | archive-server                                | Узел, на котором была создана схема БД архива | Доступ сервера архива к БД PostgreSQL                                                                                                                        |
| 5558 | webserver                                     | monitor-ng                                    | Проверка соединений, заданных в конфигурации                                                                                                                 |
| 7001 | skvt-cassandra<br>Все узлы кластера           | skvt-cassandra                                | Поиск информации на серверах Cassandra различных узлов системы. Для корректной работы Cassandra в кластере необходимо, чтобы этот порт был открыт в firewall |
| 7199 | skvt-cassandra<br>Все узлы кластера           | skvt-cassandra                                | Внутренний мониторинг при запуске диагностических утилит                                                                                                     |
| 7837 | archive-server                                | indexer-ng                                    | Уведомления о новых и измененных сообщениях в БД архива                                                                                                      |
| 7837 | webserver                                     | indexer-ng                                    | Получение информации о сообщениях в БД архива                                                                                                                |
| 8008 | webserver                                     | smarp-request-handler                         | Обработка запросов администратора безопасности                                                                                                               |
| 8080 | crawler-processor<br>crawler-scanner          | crawler-ccc                                   | Получение экземпляров задач от CCC сервиса                                                                                                                   |
| 8090 | crawler-ccc                                   | crawler-pccc                                  | Обмен информацией между CCC и PCCC                                                                                                                           |
| 8090 | webserver                                     | crawler-pccc                                  | Подключение к сервису PCCC из веб-интерфейса                                                                                                                 |
| 8123 | webserver                                     | clickhouse                                    | Прием запросов сервисом clickhouse из веб-интерфейса                                                                                                         |
| 8300 | webserver                                     | detective-server                              | Прием запросов сервисом <b>Расследование</b> из веб-интерфейса                                                                                               |
| 8445 | webserver-local                               | webserver                                     | Подключение локальных веб-серверов к основному                                                                                                               |
| 9000 | webserver                                     | report-server                                 | Получение информации об отчетах                                                                                                                              |
| 9001 | Узлы KEO DLP                                  | clickhouse                                    | Выборка данных из БД Clickhouse                                                                                                                              |
| 9042 | filestorage-ng                                | skvt-cassandra                                | Доступ к индексу ФХ                                                                                                                                          |
| 9090 | Сервер Cisco Webex                            | imcrawler                                     | Передача сообщений Webex на анализ в KEO DLP                                                                                                                 |
| 9160 | filestorage-ng                                | skvt-cassandra                                | Обмен информацией с узлами, входящими в кластер Cassandra                                                                                                    |
| 9200 | webserver                                     | opensearch                                    | Внешний поисковый индексатор. Принимает запросы от веб-интерфейса на поиск слов в БД поисковой машины OpenSearch (внешний индекс)                            |
| 9200 | action-server<br>archive-server               | opensearch                                    | Закладка новых индексов сообщений в OpenSearch                                                                                                               |
| 9201 | indexer-ng                                    | opensearch                                    | Управление кластером поисковой машины OpenSearch (внешний индекс)                                                                                            |
| 9201 | incident-daemon<br>webserver<br>report-server | opensearch                                    | Закладка новых индексов инцидентов в OpenSearch                                                                                                              |

| Порт  | Сервисы                                                                      |                  | Описание                                                                                                                                     |
|-------|------------------------------------------------------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|       | откуда                                                                       | куда             |                                                                                                                                              |
| 9301  | mailfilter<br>webserver                                                      | difi             | Взаимодействие с сервером проверки по алгоритму цифровых отпечатков в распределенной среде (при наличии соответствующего модуля)             |
| 9302  | mailfilter<br>webserver                                                      | idid             | Взаимодействие с сервером проверки по алгоритму цифровых идентификаторов (IDID) в распределенной среде (при наличии соответствующего модуля) |
| 9303  | mailfilter<br>webserver                                                      | god-server       | Взаимодействие с сервером распознавания графических объектов (god-server) в распределенной среде (при наличии соответствующего модуля)       |
| 9304  | action-server<br>webserver                                                   | stt-server       | Взаимодействие с сервисом распознавания речи (stt-server) в распределенной среде                                                             |
| 9400  | Агенты                                                                       | Центр приложений | Передача статуса агента                                                                                                                      |
| 9400  | agent-control-ng                                                             | Центр приложений | Управление задачами развертывания агентов                                                                                                    |
| 9401  | Сервер управления агентами                                                   | Центр приложений | Получение состояния Агентов от узла с ролью <b>Центр приложений</b>                                                                          |
| 9666  | crawler-scanner                                                              | crawler-snapshot | Взаимодействие с сервисом отпечатков для получения и отправки информации                                                                     |
| 9998  | mailfilter<br>webserver                                                      | smap-tikaserver  | Извлечение текстов, распаковка офисных документов, определение кодировок в распределенной среде                                              |
| 10050 | monitor-agent                                                                | monitor-server   | Прием сервером мониторинга информации о статистических показателях                                                                           |
| 10051 | monitor-agent                                                                | monitor-server   | Прием сервером мониторинга информации о статистических показателях                                                                           |
| 11344 | Прокси-серверы                                                               | tragent          | Прием запросов по протоколу ICAPS от ICAP-прокси                                                                                             |
| 16379 | mailfilter<br>archive-server<br>filestorage-ng<br>indexer-ng<br>smap-smtp-gw | smap-redis       | Хранение счетчиков                                                                                                                           |
| 33033 | Внешний клиент                                                               | api-gateway      | Передача запросов от внешнего клиента к сервису интеграции                                                                                   |
| 61616 | crawler-processor<br>crawler-scanner                                         | activemq         | Обмен данными между сканером и обработчиком<br><br>Хранение очередей                                                                         |

### Примечание

Если в конфигурации KEO DLP меняется какой-либо порт, необходимо поменять и разрешающее правило.

---

### Внимание!

- Порт 22 должен быть открыт на всех узлах KEO DLP – используется для доступа к CLI по протоколу SSH, а также для синхронизации конфигурации между узлами с использованием учетной записи **dozor**.
- Порт 443 должен быть открыт на master-узле, и на всех узлах, где предполагается использование локального веб-сервера – используется для доступа к GUI с помощью браузера.
- Порт 80 должен быть открыт на master-узле – используется для службы мониторинга.

---

### Внимание!

Ни один сторонний сервис на узлах кластера KEO DLP не должен использовать порт 8443 (зарезервирован для веб-сервера).

## 4.5. Требования к серверам KEO DLP

Ниже описаны требования, предъявляемые к оборудованию серверов KEO DLP в зависимости от выбранной схемы развертывания и статистики трафика внутри организации. Предполагается, что система хранения данных (СХД), содержащая БД архива почтовых сообщений, примонтирована к файловой системе master-узла. Под процессором понимается виртуальный процессор (технология Hyper-treading) при тактовой частоте физического процессора не ниже 2.1 ГГц. Срок хранения данных в архиве считается равным одному году. Требования к СХД прямо и линейно пропорциональны сроку хранения данных в архиве, остальные требования не зависят от него.

Рекомендуемые характеристики аппаратного обеспечения СХД:

- Количество операций ввода-вывода в секунду (IOPS) – не менее 2000. IOPS может быть увеличен за счет использования большего количества жестких дисков меньшей емкости при сохранении общего объема СХД.
- Технология виртуализации данных – RAID 10 или RAID 6.
- Интерфейс подключения жестких дисков – SAS. Скорость вращения шпинделя – 10к или выше.
- Для хранения индексов OpenSearch по возможности выделить диски SSD.

### Внимание!

Приведенные ниже значения рассчитаны на обеспечение работоспособности KEO DLP без использования модулей KEO DLP Traffic Analyzer, KEO DLP File Crawler, Endpoint Agent, UBA и модуля распознавания графических объектов. Для получения значений, достаточных для использования одного или нескольких из этих модулей, следует обратиться в службу технической поддержки поставщика ПО KEO DLP.

### 4.5.1. Требования к одномашинной конфигурации

Табл. 4.2. Требования к серверу KEO DLP

| СХД, ТБ/год   | Оперативная память, ГБ | Число процессоров (vCPU) | СУБД архива |
|---------------|------------------------|--------------------------|-------------|
| 1 ГБ в сутки  |                        |                          |             |
| 1             | 32                     | 8                        | PostgreSQL  |
| 5 ГБ в сутки  |                        |                          |             |
| 4             | 72                     | 20                       | PostgreSQL  |
| 10 ГБ в сутки |                        |                          |             |
| 7             | 80                     | 28                       | PostgreSQL  |

### 4.5.2. Требования к распределенной конфигурации

Требования, предъявляемые к master-узлу в распределенной конфигурации, не зависят от выбранного режима (активного или пассивного), то есть предполагается, что задачи фильтрации почтовых сообщений решаются исключительно slave-узлами. Требования к СХД являются суммарными по всему кластеру KEO DLP, а не отдельными для каждого узла. Требования с использованием символа + означают, что для фильтрации указанного объема суточного трафика настоятельно рекомендуется использование двух или более slave-узлов.

Табл. 4.3. Требования к оборудованию master-узла кластера KEO DLP

| СХД, ТБ/год   | Оперативная память, ГБ | Число процессоров (vCPU) | Дисковое пространство, ГБ |
|---------------|------------------------|--------------------------|---------------------------|
| 1 ГБ в сутки  |                        |                          |                           |
| 1             | 32                     | 8                        | 300                       |
| 5 ГБ в сутки  |                        |                          |                           |
| 4             | 40                     | 8                        | 300                       |
| 10 ГБ в сутки |                        |                          |                           |
| 7             | 40                     | 8                        | 300                       |
| 20 ГБ в сутки |                        |                          |                           |
| 14            | 64                     | 10                       | 300                       |
| 40 ГБ в сутки |                        |                          |                           |
| 30            | 96                     | 10                       | 300                       |

Табл. 4.4. Требования к оборудованию slave-узлов кластера KEO DLP

| Оперативная память, ГБ | Число процессоров (vCPU) | СУБД архива | Дисковое пространство, ГБ |
|------------------------|--------------------------|-------------|---------------------------|
| 1 ГБ в сутки           |                          |             |                           |
| 32                     | 8                        | PostgreSQL  | 300                       |
| 5 ГБ в сутки           |                          |             |                           |
| 32                     | 8                        | PostgreSQL  | 300                       |
| 10 ГБ в сутки          |                          |             |                           |
| 40                     | 20                       | PostgreSQL  | 300                       |
| 20 ГБ в сутки          |                          |             |                           |
| 40 + 40                | 16 + 16                  | PostgreSQL  | 300                       |

---

## 4.6. Требования к инфраструктуре

Для поддержания нормальной работоспособности KEO DLP, инфраструктура корпоративной сети должна соответствовать следующим требованиям:

- Наличие DNS-сервера и сервера точного времени.
- Сеть должна пропускать трафик между компонентами KEO DLP в соответствии с матрицей доступа (подробнее см. раздел [4.4](#)).
- Пропускная способность сетевых интерфейсов серверов системы не менее 100 Мбит/с.

## 4.7. Необходимое ПО для установки

Для установки KEO DLP необходимо наличие следующего ПО:

- дистрибутив ОС Debian версии 12.10;
- SSH-клиент;
- лицензия на KEO DLP.

Также необходимо наличие локальной копии дистрибутива ОС или наличие доступа к официальному репозиторию ОС.



---

## 5. Установка ОС Debian

Для установки ОС Debian необходимо запустить сервер с использованием установочного диска или USB-носителя «Debian 12» и выполнить следующие действия:

1. В окне приветствия оставить выбор параметров программы установки по умолчанию (**Graphical Install**) и нажать **Enter**.

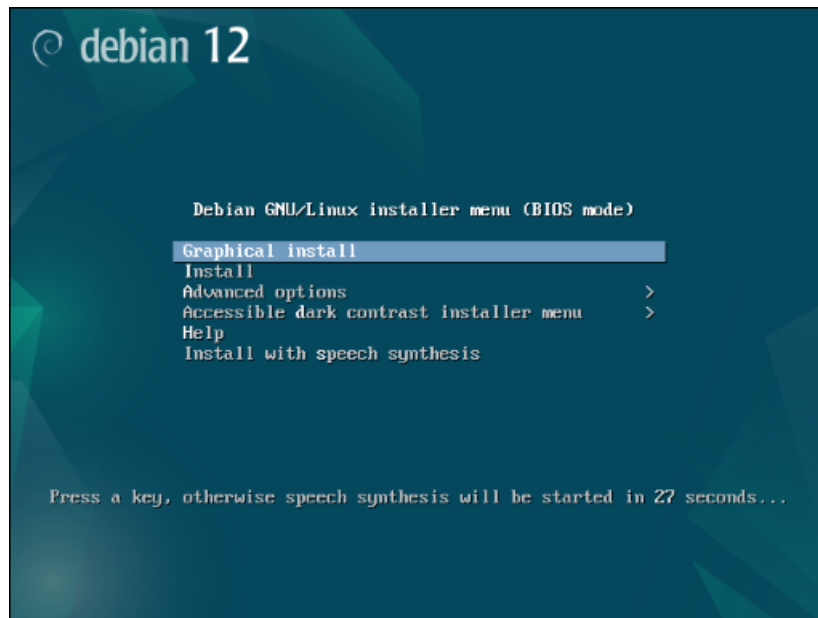


Рис. 5.1. Окно приветствия

2. На следующем шаге выбрать язык программы установки и нажать **Continue**.

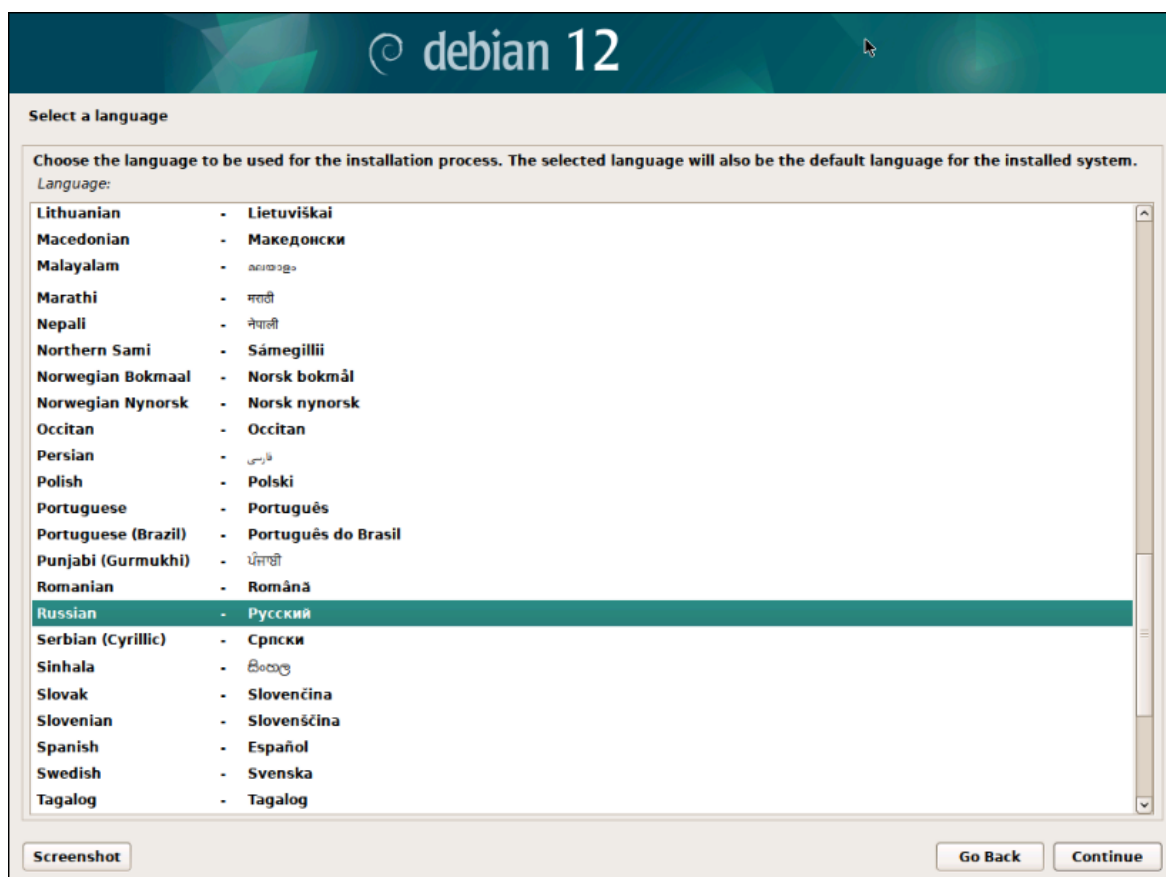


Рис. 5.2. Настройка клавиатуры

3. На следующем этапе выбрать местонахождение и нажать **Продолжить**.

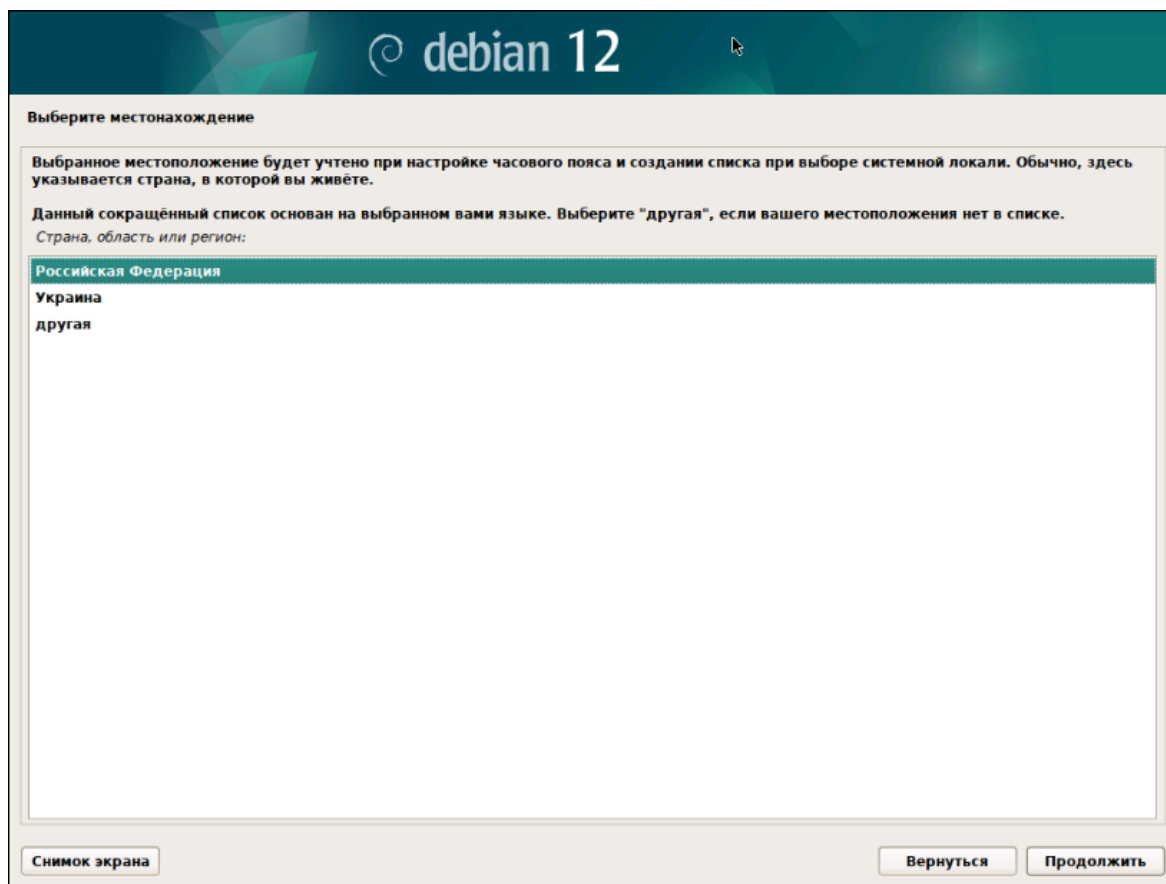


Рис. 5.3. Выбор местоположения

4. В окне **Настройка клавиатуры** выбрать удобный способ переключения раскладки ввода с клавиатуры и нажать **Продолжить**.

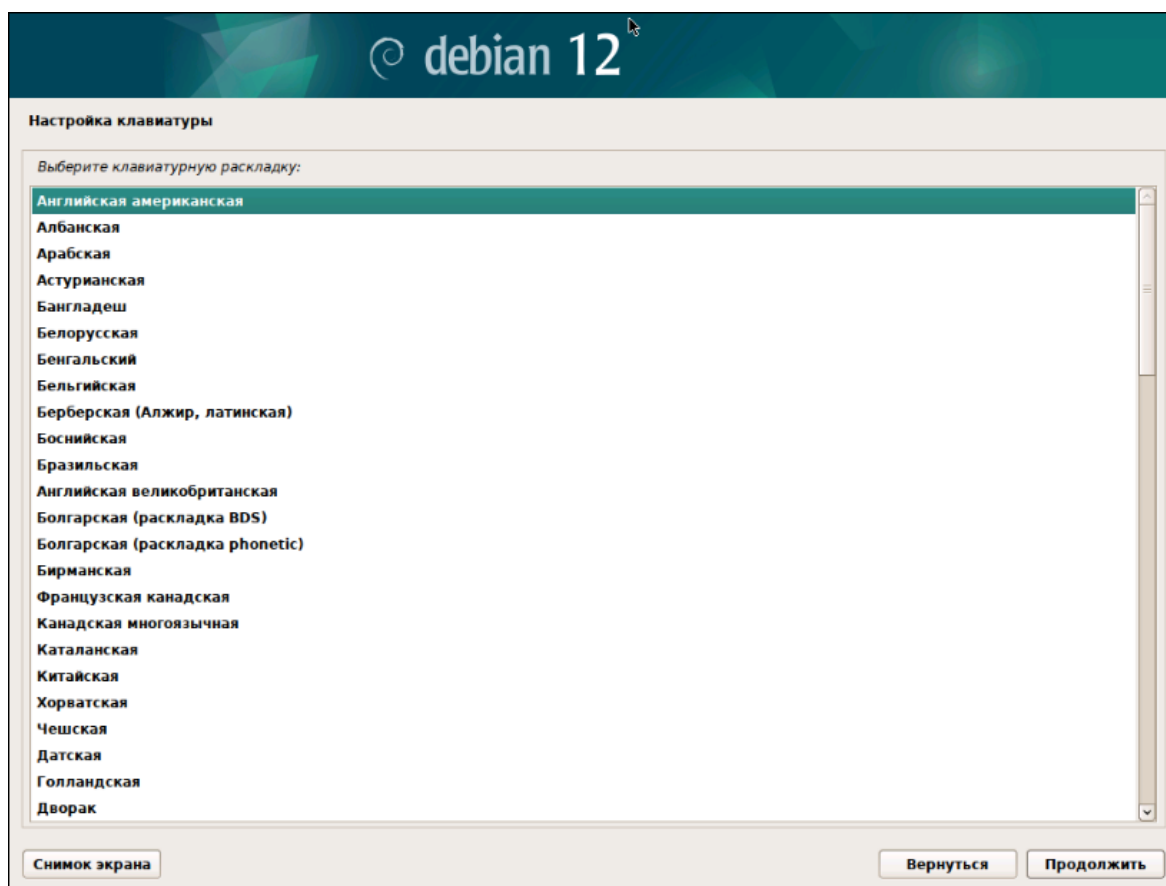


Рис. 5.4. Настройка раскладки клавиатуры

5. Дождаться загрузки компонентов программы установки. В появившемся окне **Настройка сети** указать краткое сетевое имя сервера (должно совпадать с прежним именем сервера).

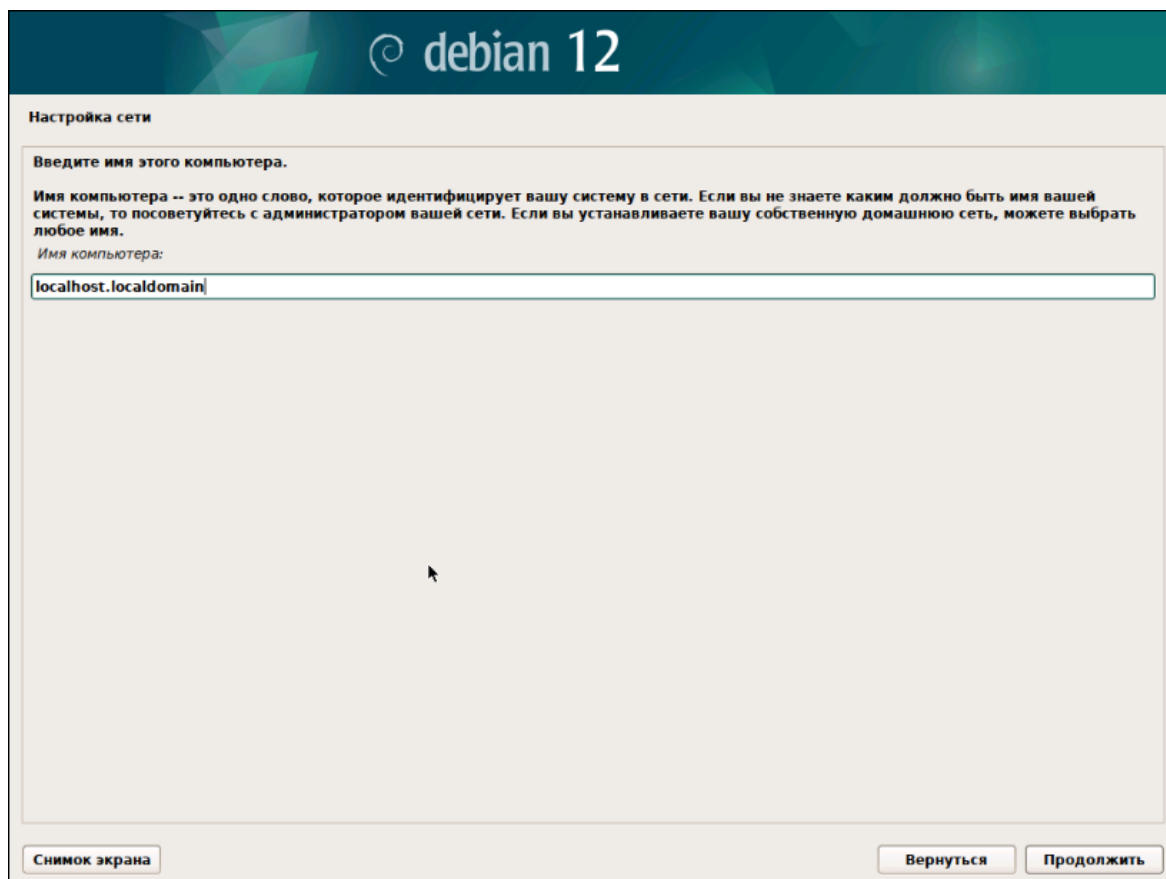


Рис. 5.5. Настройка сети

6. В окне **Настройка учетных записей пользователей и паролей** задать пароль супер-пользователя (**root**) и ввести его подтверждение. Нажать **Продолжить**.

The screenshot shows the 'debian 12' logo at the top. Below it, the title is 'Настройка учётных записей пользователей и паролей'. The main text explains the importance of a strong root password. It includes instructions on password requirements and a warning about the consequences of a weak password. There are two password input fields, each with a 'Показывать вводимый пароль' checkbox. The first field is for the root password, and the second is for confirmation. At the bottom, there are buttons for 'Снимок экрана', 'Вернуться', and 'Продолжить'.

debian 12

Настройка учётных записей пользователей и паролей

Необходимо ввести пароль учётной записи суперпользователя (root), используемой для администрирования системы. Доступ к компьютеру с использованием этой учётной записи злонамеренных или низкоквалифицированных пользователей может привести к катастрофическим последствиям. Поэтому пароль суперпользователя не должен легко угадываться, подбираться по словарю, и он не должен быть связан с вашей личностью.

Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.

Пароль учётной записи суперпользователя не должен быть пустым, иначе она будет заблокирована, а настроенной в программе установки пользовательской учётной записи будет разрешено работать с правами суперпользователя через команду "sudo".

Во время ввода пароля вводимые символы не будут отображаться на экране.

Пароль суперпользователя:

••••••••

☐ Показывать вводимый пароль

Введите тот же самый пароль ещё раз, чтобы убедиться в правильности ввода.

Введите пароль ещё раз:

••••••••

☐ Показывать вводимый пароль

Снимок экрана

Вернуться

Продолжить

Рис. 5.6. Окно настройки учетных записей: ввод пароля root

7. Ввести полное имя учетной записи, которая используется вместо **root**. Нажать **Продолжить**.

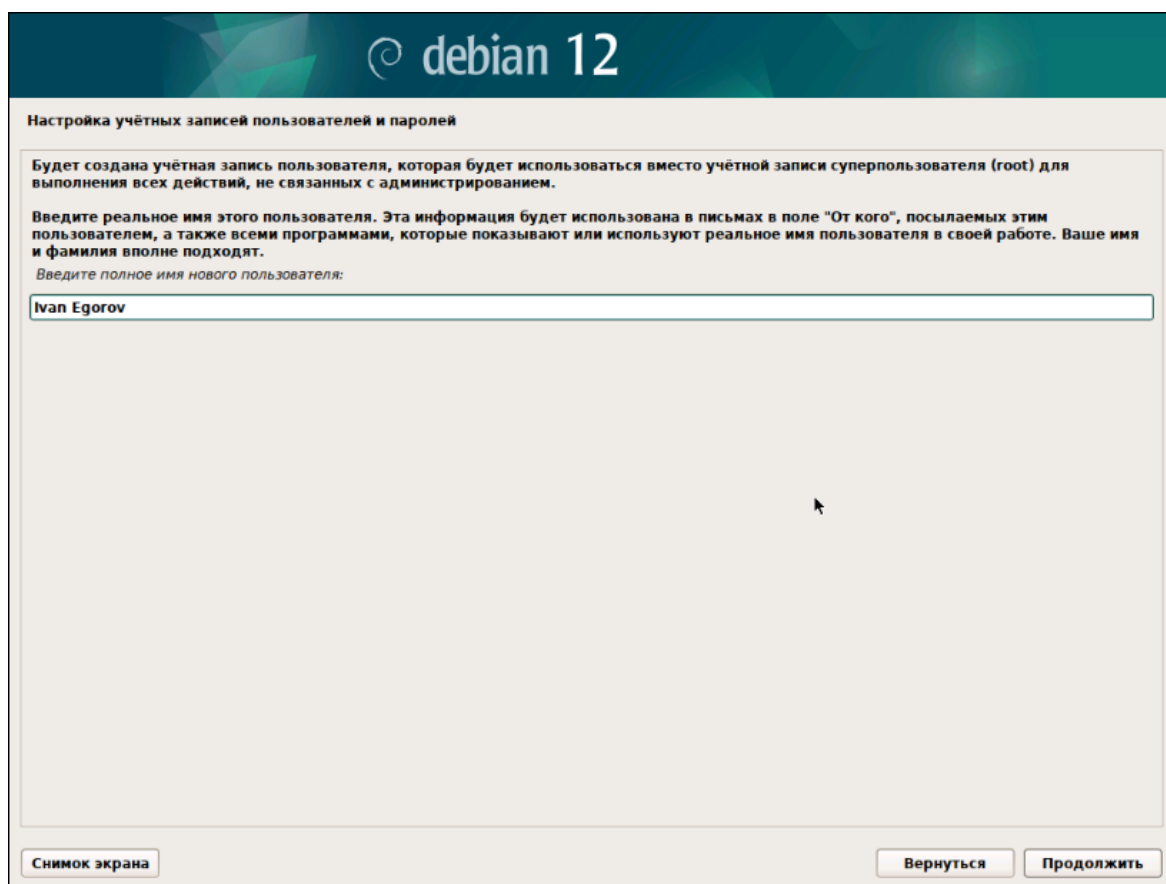


Рис. 5.7. Окно настройки учетных записей: ввод имени учетной записи, которая используется вместо root

8. Ввести сокращенное имя учетной записи, которая используется вместо **root**. Не следует использовать имя **dozor**, поскольку оно зарезервировано в KEO DLP. Нажать **Продолжить**.



Рис. 5.8. Ввод сокращенного имени учетной записи, которая используется вместо root

9. В появившемся окне задать пароль для созданной учетной записи и ввести его подтверждение. Нажать **Продолжить**.



debian 12

Настройка учётных записей пользователей и паролей

Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.  
Введите пароль для нового пользователя:

••••••

☐ Показывать вводимый пароль

Проверка правильности ввода осуществляется путём повторного ввода пароля и сравнения результатов.  
Введите пароль ещё раз:

••••••

☐ Показывать вводимый пароль

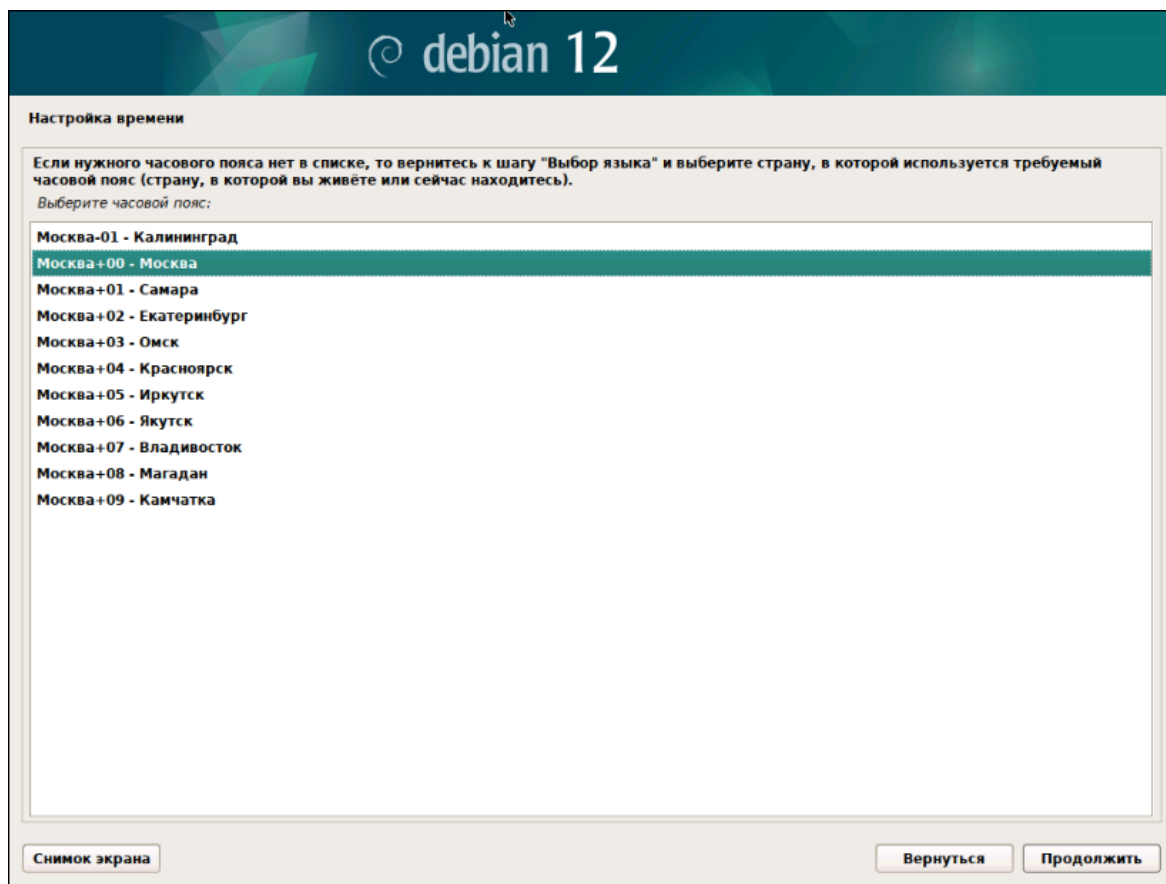
Снимок экрана

Вернуться

Продолжить

Рис. 5.9. Создание пароля для учетной записи, которая используется вместо root

10. В окне **Настройка времени** задать требуемый часовой пояс и нажать **Продолжить**.



11. В появившемся окне **Разметка дисков** выбрать метод разметки **Вручную** и нажать **Продолжить**.

### Внимание!

*При выборе любого другого метода разметки все данные на диске будут потеряны.*

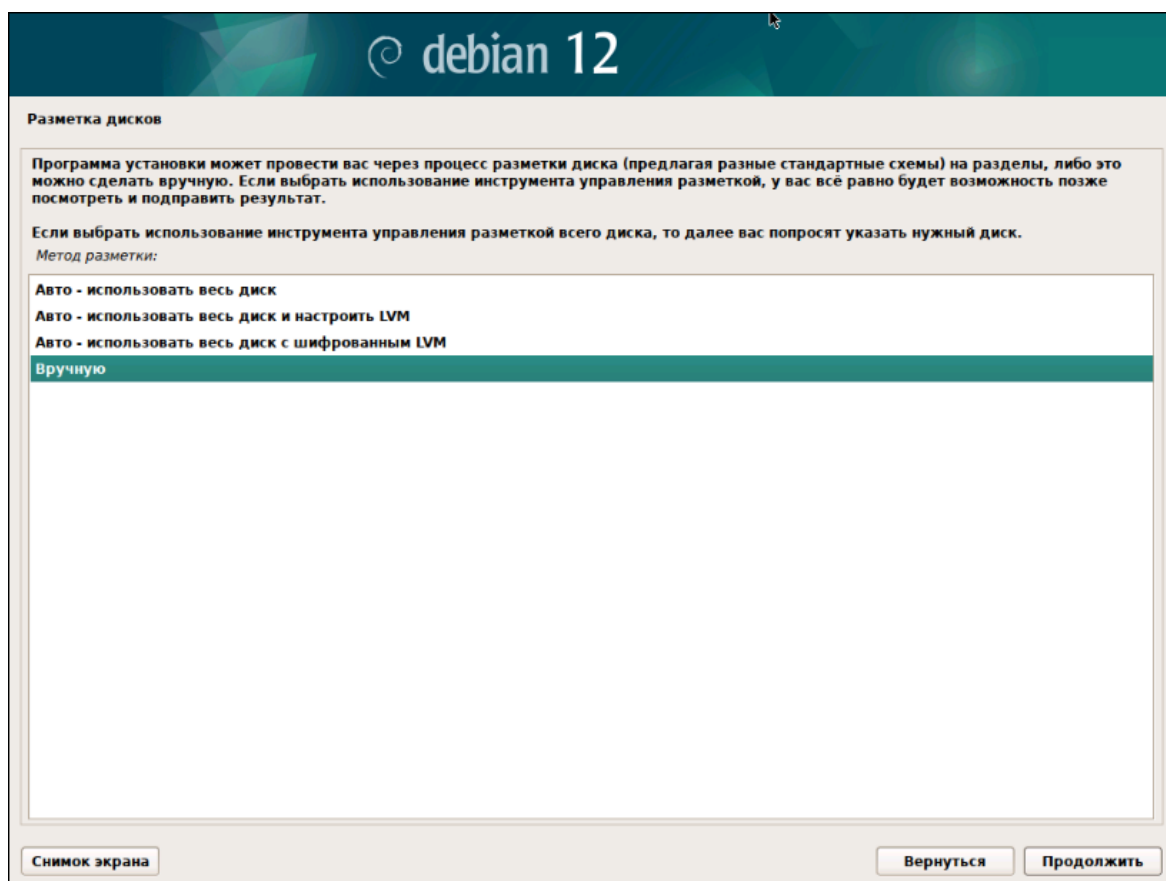


Рис. 5.10. Окно Разметка дисков

12. В появившемся окне выбрать область для разметки, например, как показано ниже. Нажать **Продолжить**.

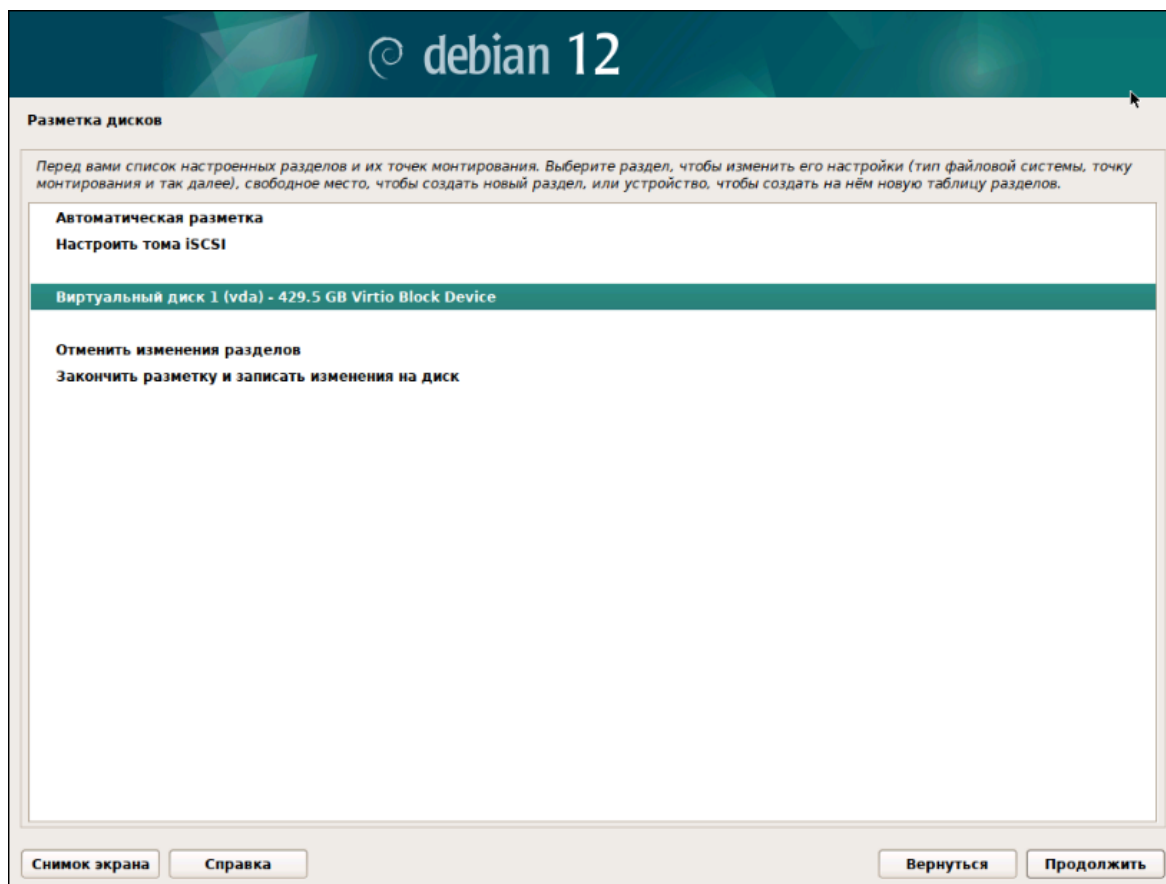


Рис. 5.11. Выбор области для разметки

13. В появившемся окне на запрос **Создать новую пустую таблицу разделов?** выбрать вариант **Да**. Нажать **Продолжить**.

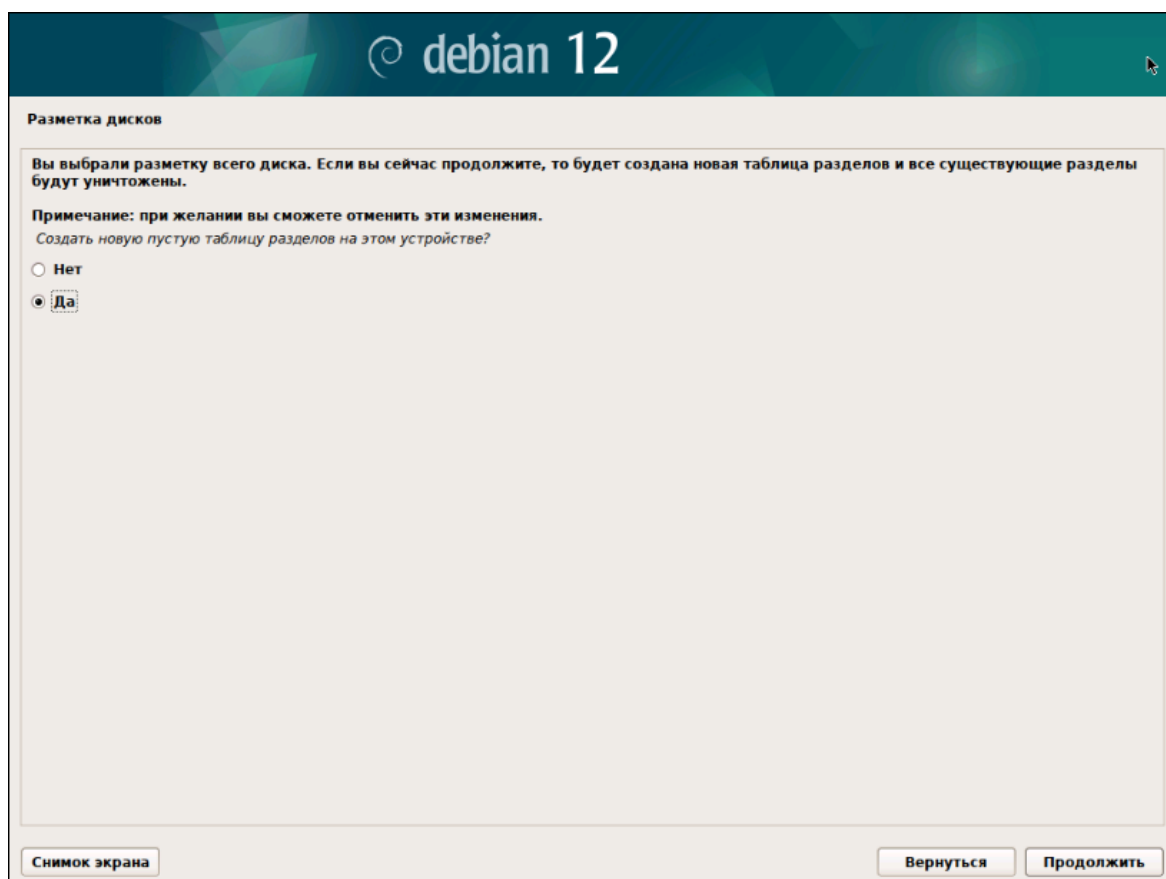


Рис. 5.12. Создание таблицы разделов

14. В появившемся окне выделить строку, помеченную как **СВОБОДНОЕ МЕСТО**, и нажать **Продолжить**.

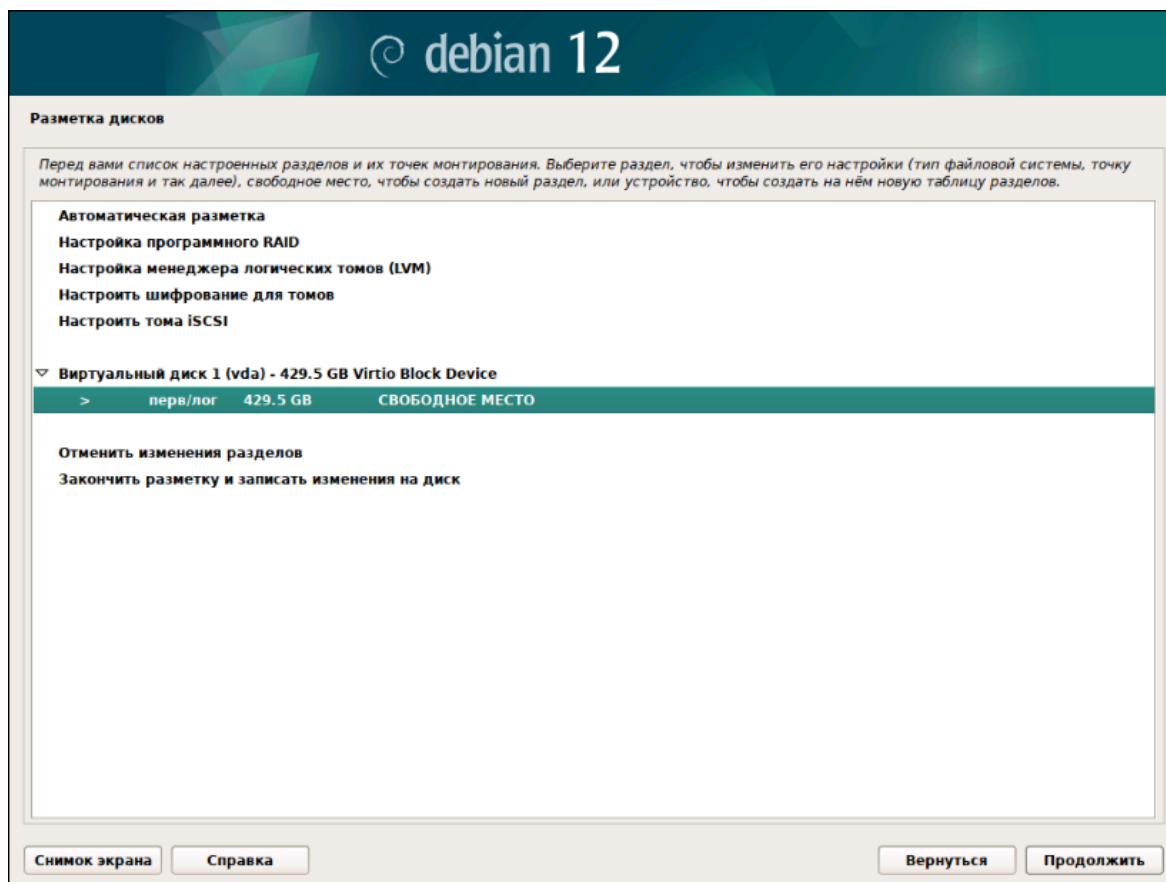


Рис. 5.13. Выбор пространства для создания разделов

15. В появившемся окне на запрос **Что делать со свободным пространством** выбрать вариант **Создать новый раздел**. Нажать **Продолжить**.

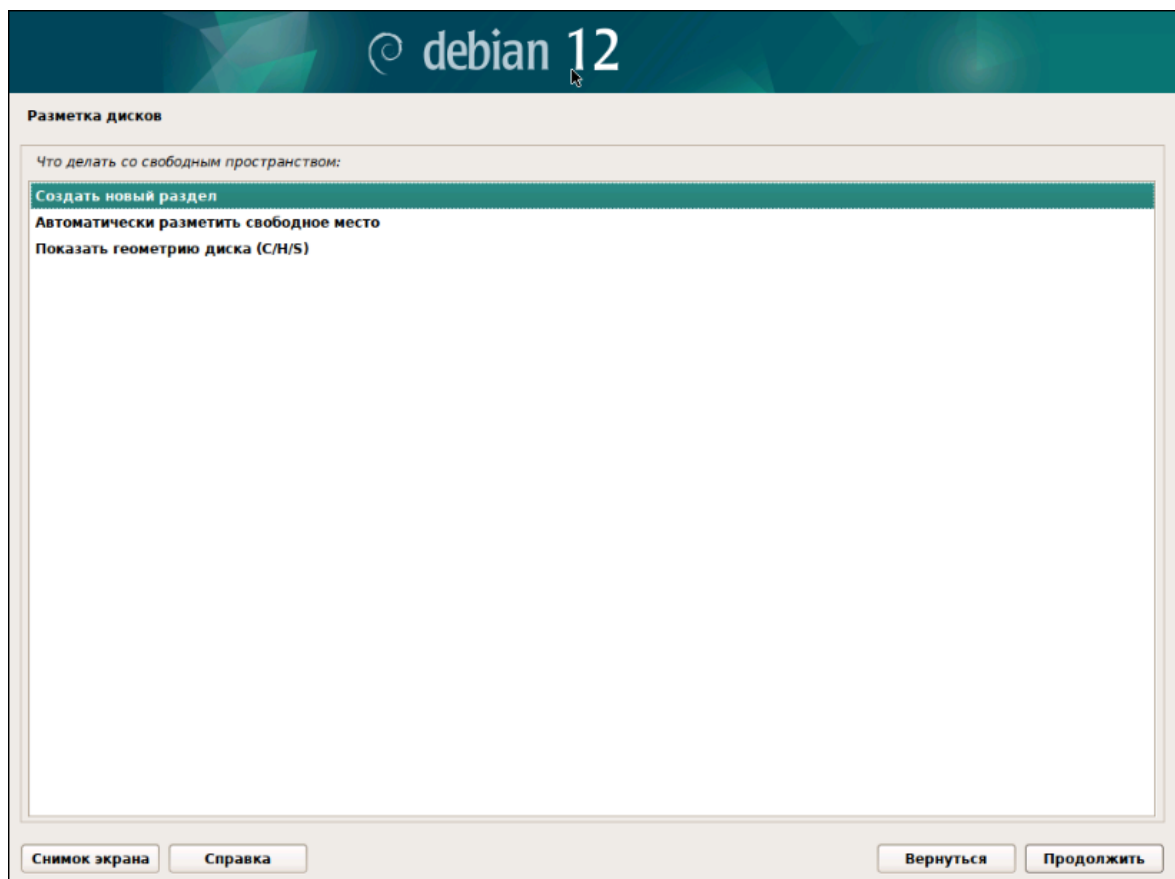


Рис. 5.14. Выбор варианта для создания раздела

16. В появившемся окне задать размер диска **1 GB**. Нажать **Продолжить**.

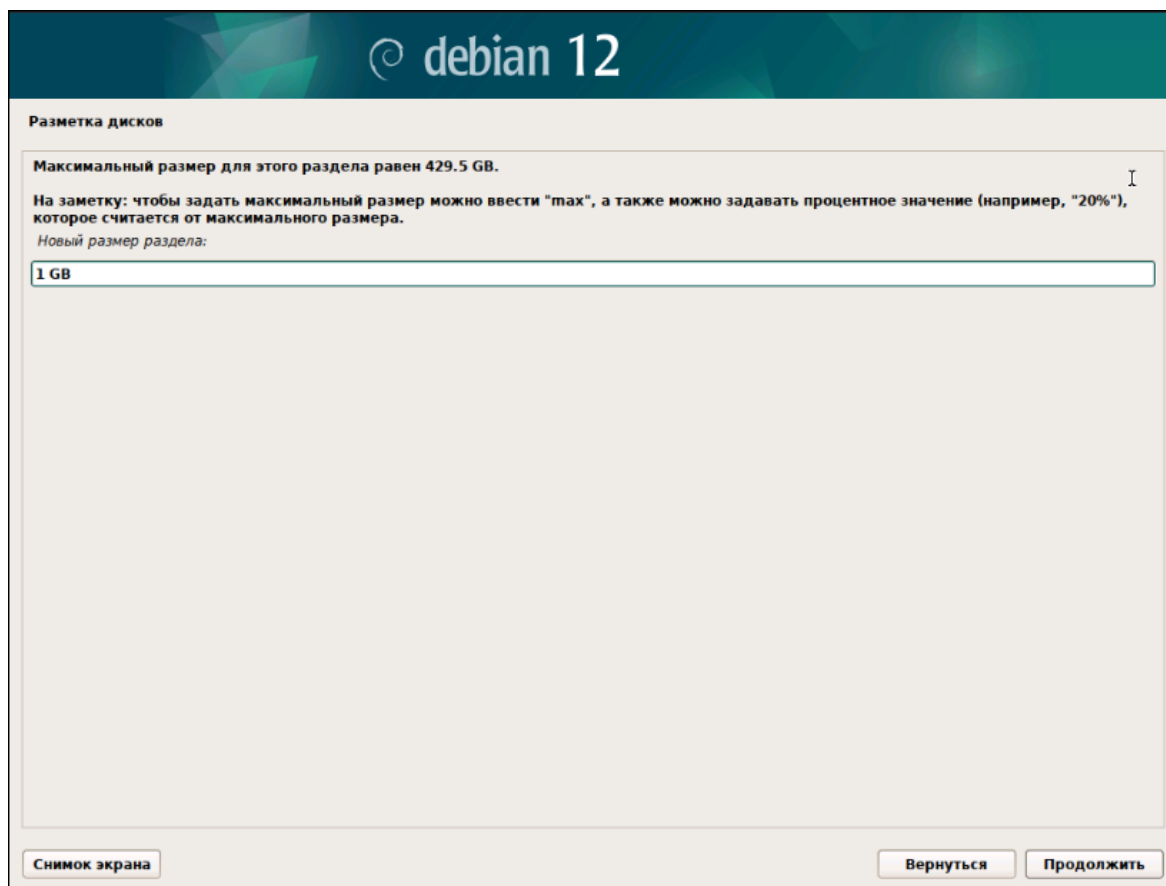


Рис. 5.15. Задание размера раздела

17. В появившемся окне выбрать тип раздела **Первичный**. Нажать **Продолжить**.



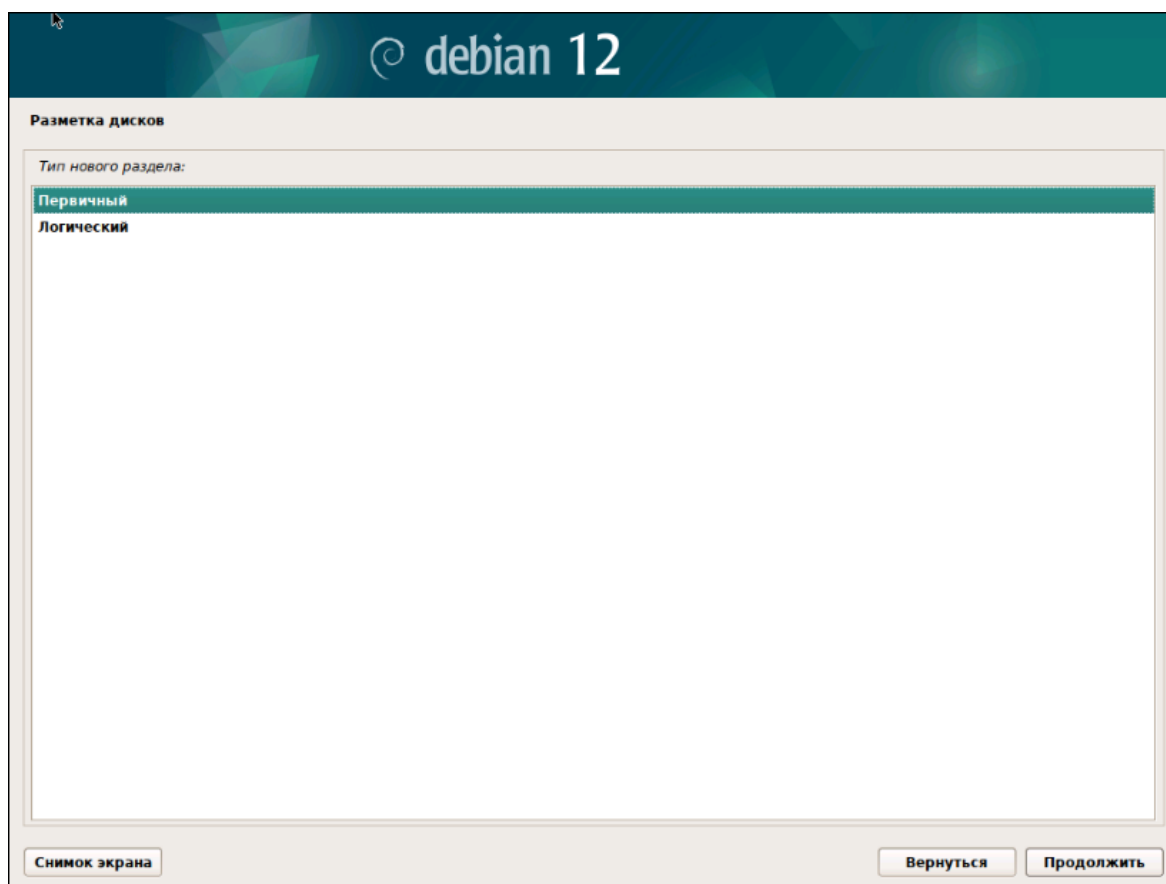


Рис. 5.16. Выбор типа раздела

18. В появившемся окне выбрать расположение раздела **Начало**. Нажать **Продолжить**.



Рис. 5.17. Выбор местоположения раздела

19. Выполнить двойной щелчок на строке **Точка монтирования** и в появившемся окне двойным щелчком выбрать вариант **/boot**. Выполнить двойной щелчок на строке **Метка 'загрузочный'** (так, чтобы было выбрано значение **вкл**). Нажать **Продолжить**.

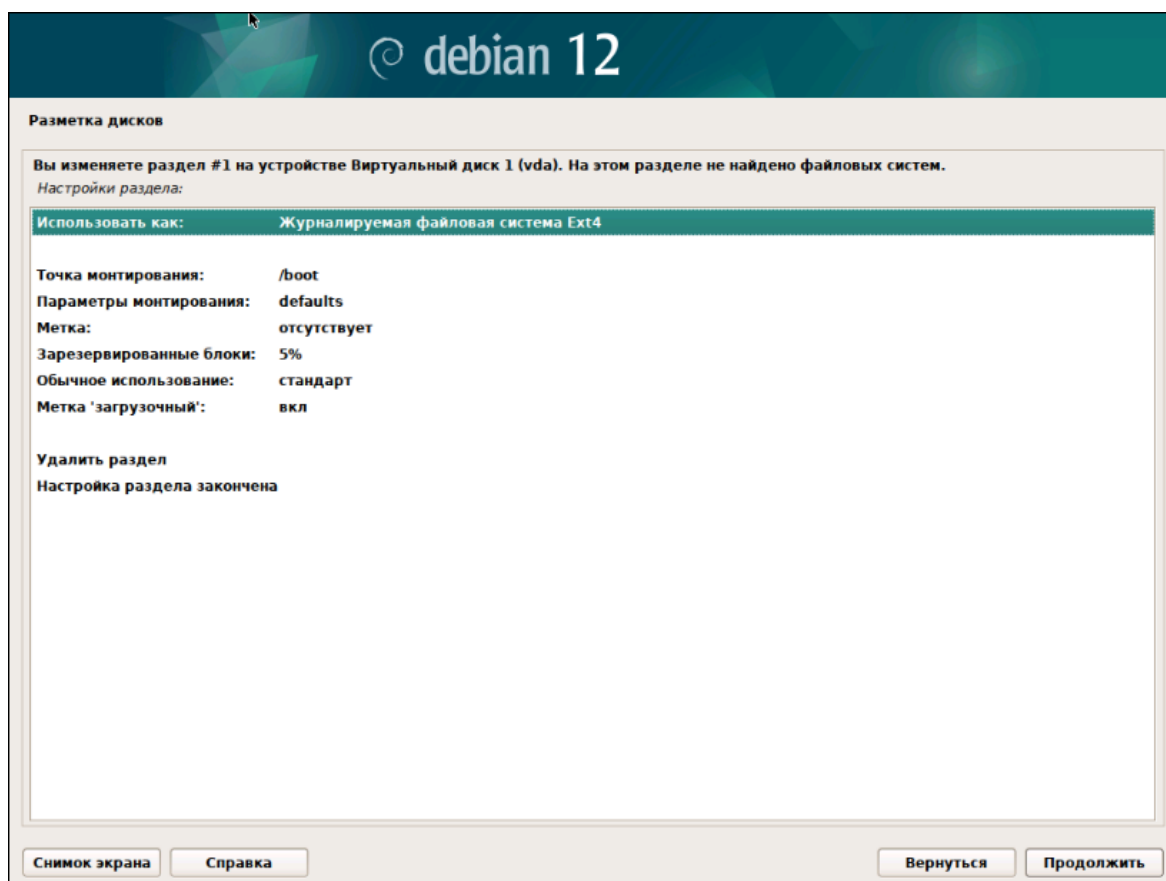


Рис. 5.18. Параметры монтирования раздела

20. Выделить строку **Настройка раздела закончена** и нажать **Продолжить**.
21. Создать новый раздел, выполнив шаги [14](#) и [15](#).
22. В появившемся окне выбора размера раздела оставить максимальное значение по умолчанию. Нажать **Продолжить**.
23. В появившемся окне выбрать тип раздела **Логический**. Нажать **Продолжить**.

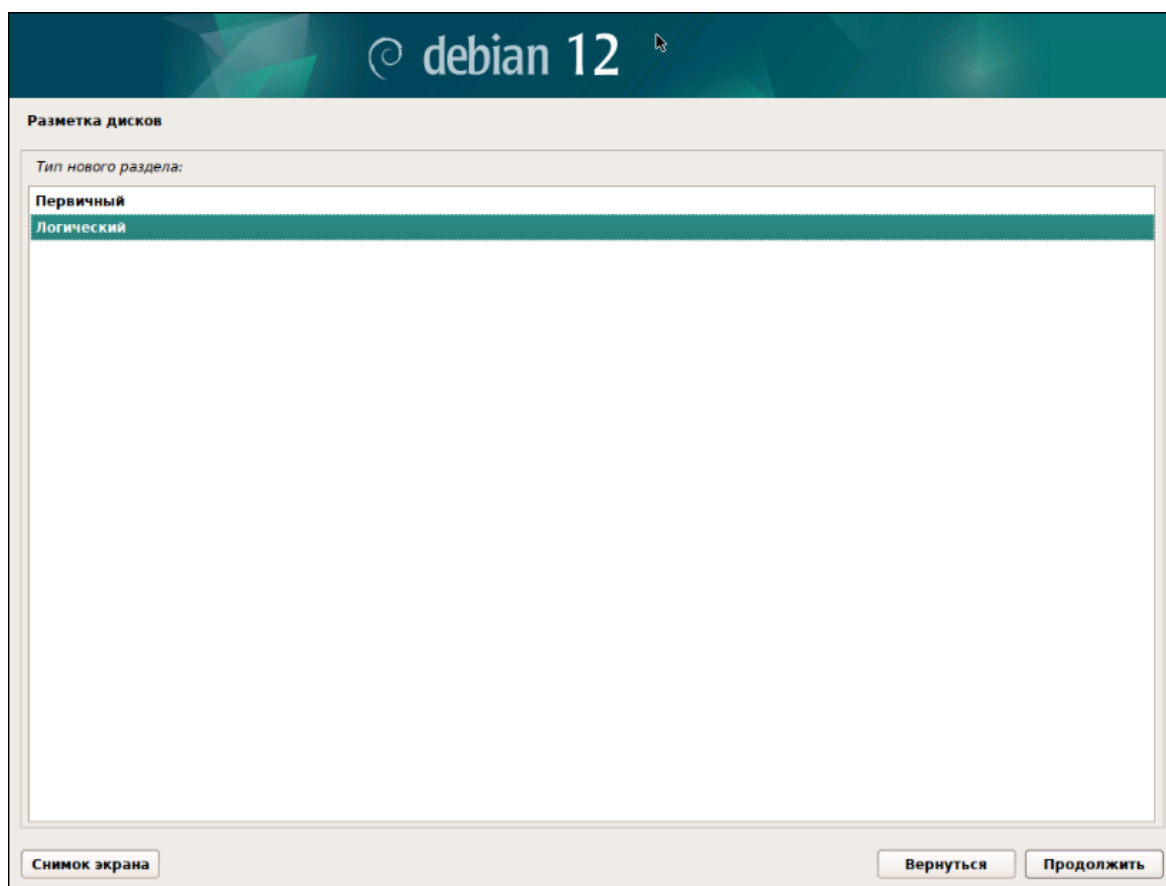


Рис. 5.19. Выбор типа раздела

24. В появившемся окне выполнить двойной щелчок на строке **Использовать как:** и выбрать вариант **физический том для LVM**, затем нажать **Продолжить**. Выделить строку **Настройка раздела закончена** и нажать **Продолжить**.

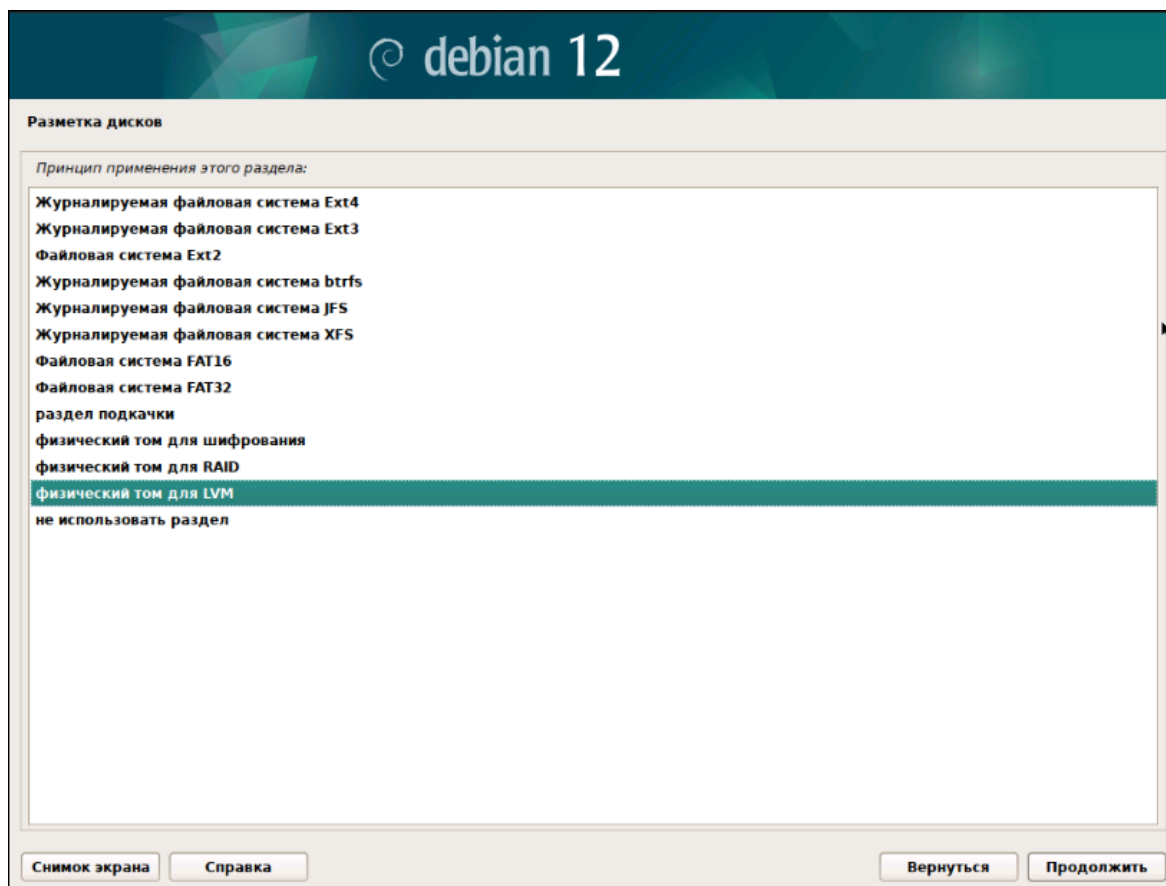


Рис. 5.20. Выбор варианта использования раздела

25. Выполнить двойной щелчок на строке **Настройка менеджера логических томов (LVM)** и в появившемся окне выбрать **Да**. Нажать **Продолжить**.

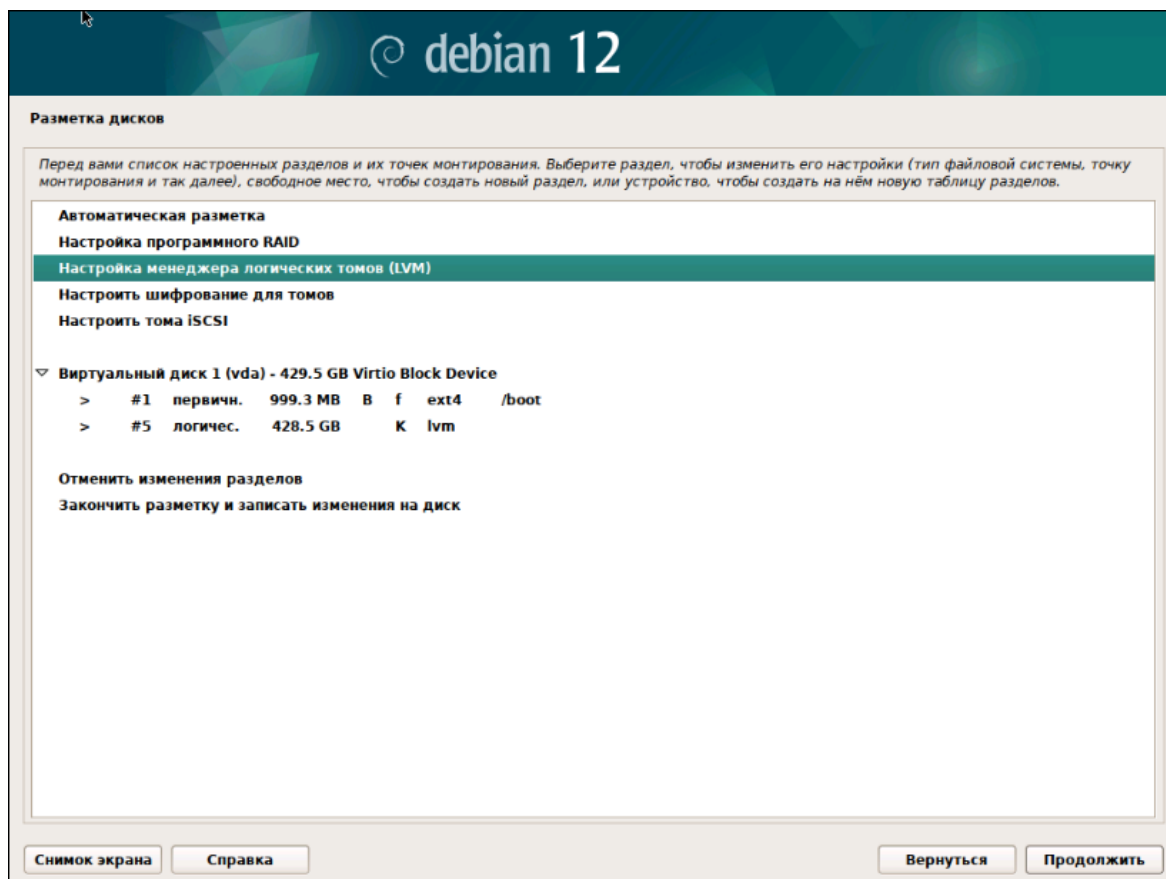


Рис. 5.21. Пункт настройки менеджера логических томов

26. В появившемся окне выбрать вариант **Создать группу томов**. Нажать **Продолжить**.

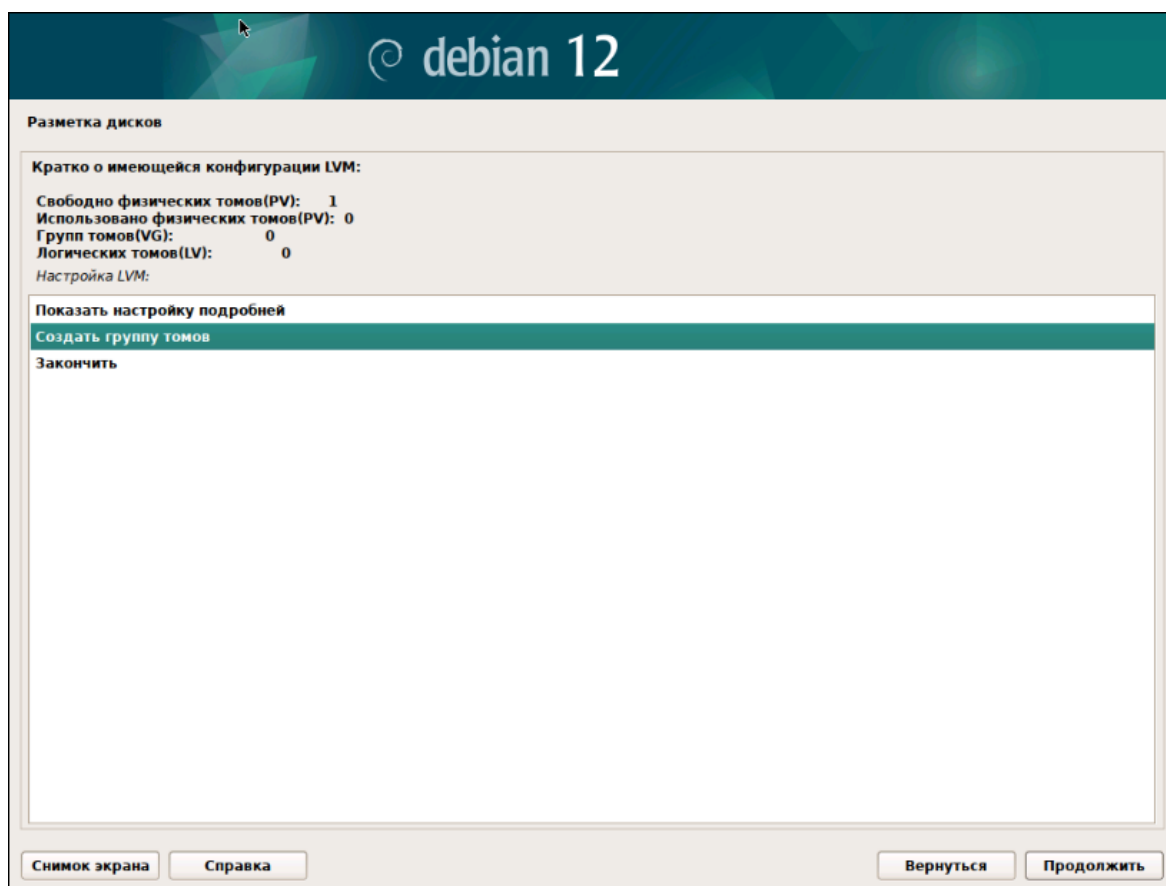


Рис. 5.22. Создание группы томов для LVM

27. В появившемся окне задать название для группы томов, например, **dozor**. Нажать **Продолжить**.

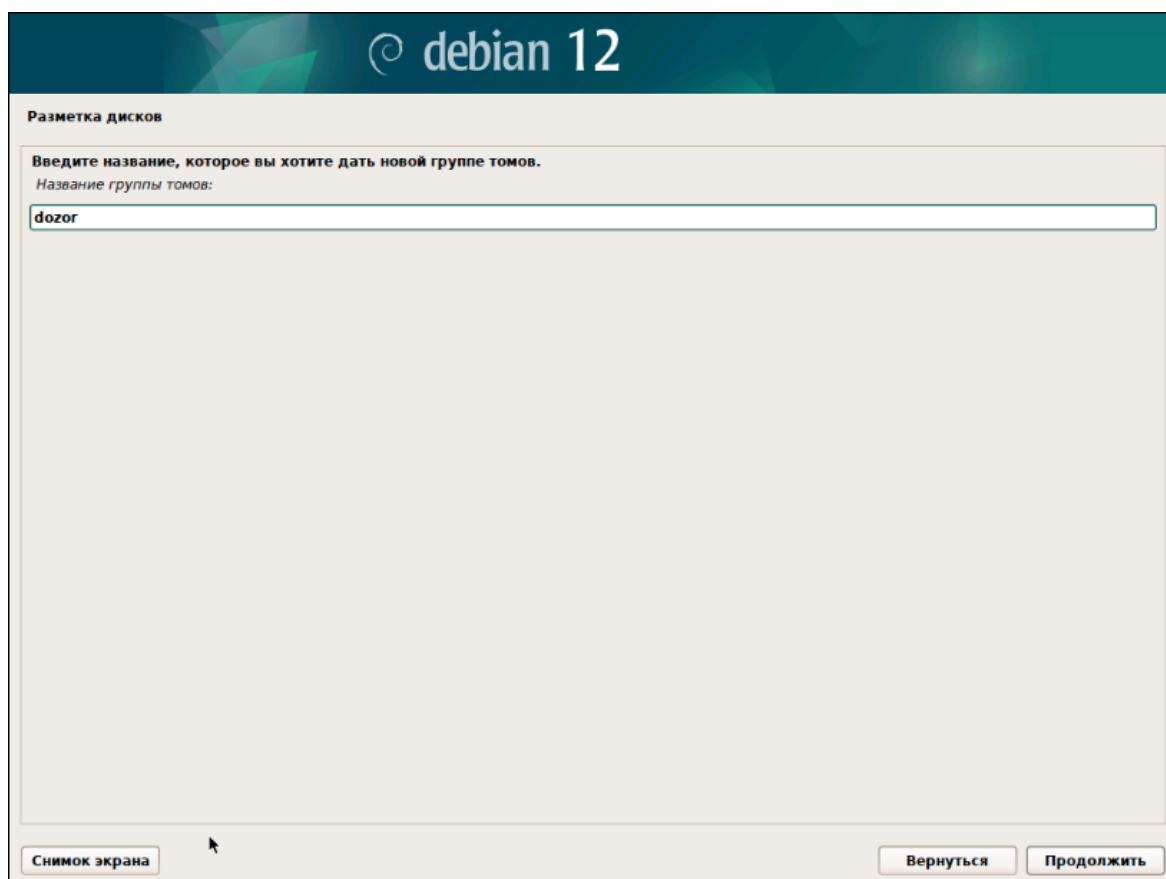


Рис. 5.23. Ввод имени группы томов

28. В появившемся окне выбрать раздел, созданный на шаге 21. Нажать **Продолжить**.



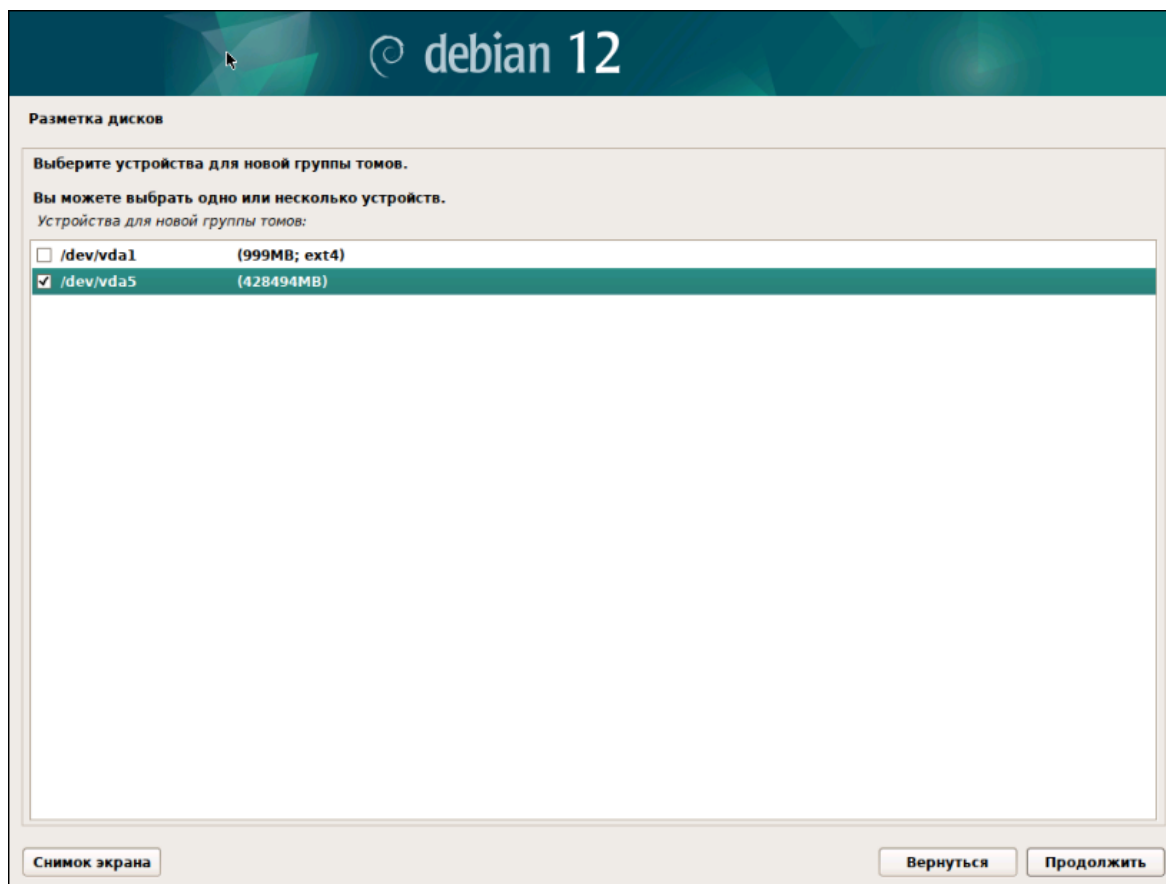


Рис. 5.24. Выбор устройства для размещения группы томов

29. В появившемся окне выбрать вариант **Создать логический том**, нажать **Продолжить** и выбрать группу томов, созданную на шаге [26](#). Нажать **Продолжить**.
30. В появившемся окне для нового логического тома задать имя **root**. Нажать **Продолжить**.

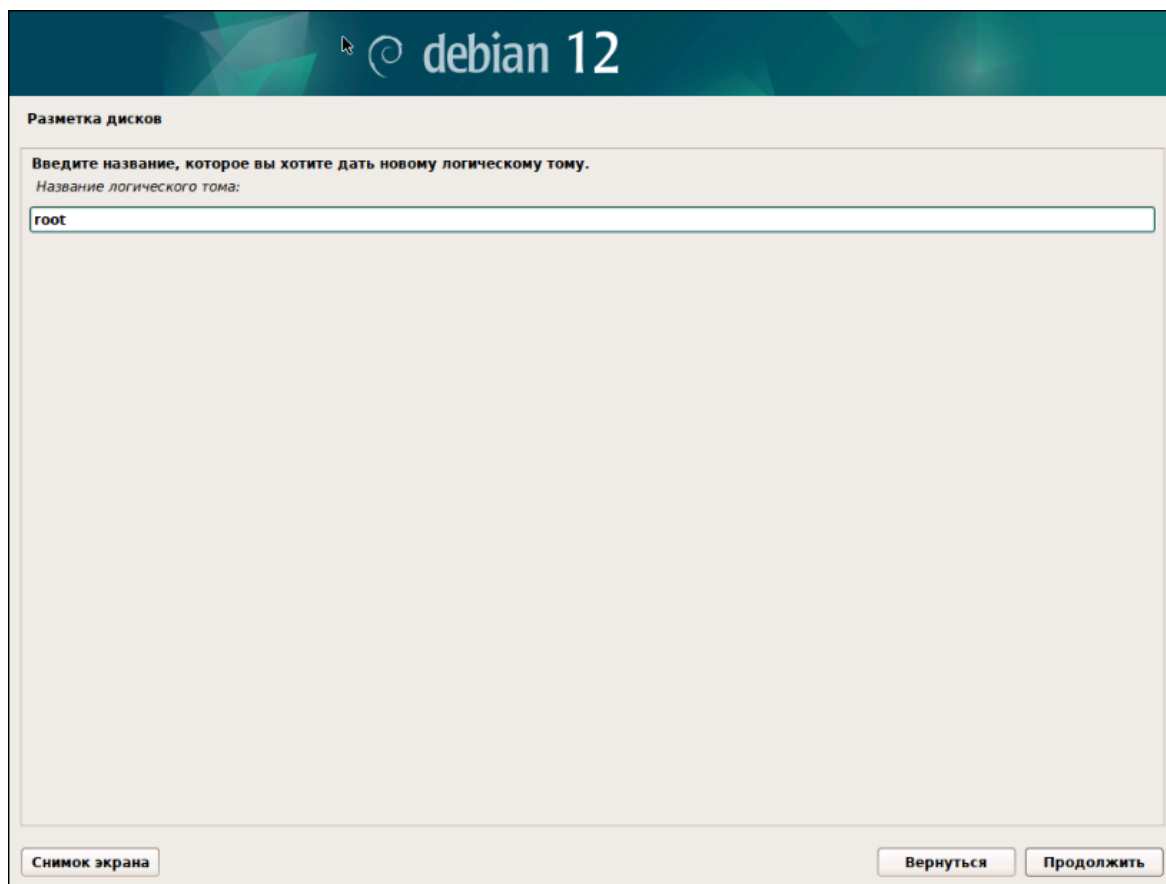


Рис. 5.25. Задание имени логического тома root

31. В следующем окне для нового логического тома задать размер **25G**. Нажать **Продолжить**.



Рис. 5.26. Выделение размера для логического тома root

32. Создать том с названием **var** и выделить для него 50 ГБ, выполняя действия шагов [29](#), [30](#) и [31](#).
33. Создать тома, выполняя действия шагов [29](#), [30](#) и [31](#), в зависимости от назначения узла:
  - При установке на master-узел – создать тома **data**, **storage** (опционально) и **opt**. Для тома **data** выделить дисковое пространство в соответствии с требованиями к размеру хранилища. Рекомендуется выделить не менее 100 ГБ дискового пространства. Для тома **storage** выделить пространство в соответствии с сайзингом. Примонтировать СХД к этому разделу (во время или после установки ОС). Для тома **opt** выделить все оставшееся дисковое пространство.

#### Внимание!

*Крайне желательно, чтобы объем пространства, выделенного для тома **opt**, составлял не менее 130 ГБ. Этот том в процессе эксплуатации KEO DLP активно наполняется данными, и исчерпание свободного места на нем приведет к аварийной остановке KEO DLP.*

- При установке на slave-узел – создать тома **opt** и **data**. Выделить для тома **opt** не менее 130 ГБ дискового пространства, а для тома **data** – все оставшееся дисковое пространство.

34. В появившемся окне **Настройка LVM** выбрать вариант **Закончить**. Нажать **Продолжить**.



Рис. 5.27. Разметка дисков для master-узла

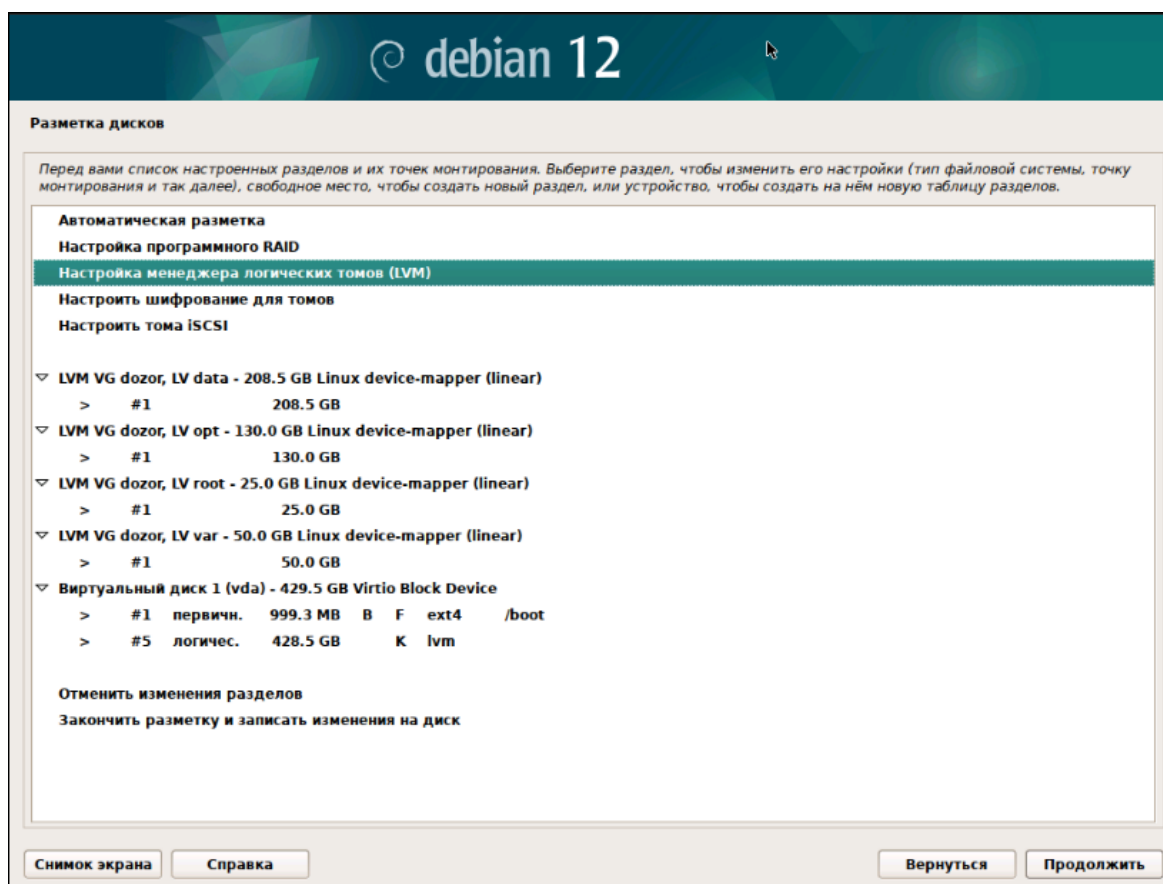


Рис. 5.28. Разметка дисков для slave-узла

35. Задать точки монтирования и файловые системы для созданных томов. Например, для тома **root** выделить строку:

```
> #1      25.0 GB
```

Нажать **Продолжить** (или выполнить двойной щелчок на этой строке). В появившемся окне выполнить двойной щелчок на строке **Использовать как: не использовать**. В появившемся окне выбрать строку **Журналируемая файловая система Ext4** и нажать **Продолжить**. В окне настроек тома выполнить двойной щелчок по строке **Точка монтирования** и выбрать точку монтирования **/ -- корневая файловая система**. В окне настроек тома выполнить двойной щелчок по строке **Настройка раздела закончена**.

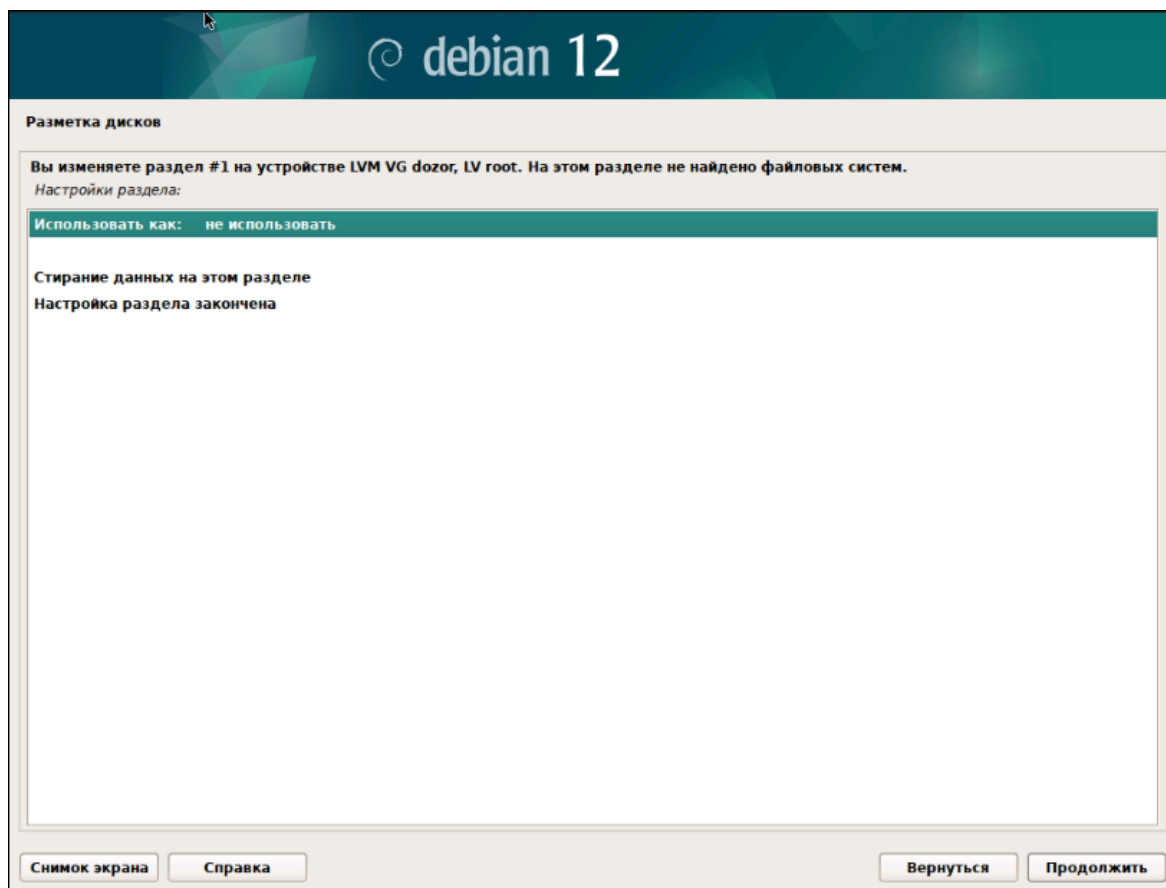


Рис. 5.29. Настройки тома root

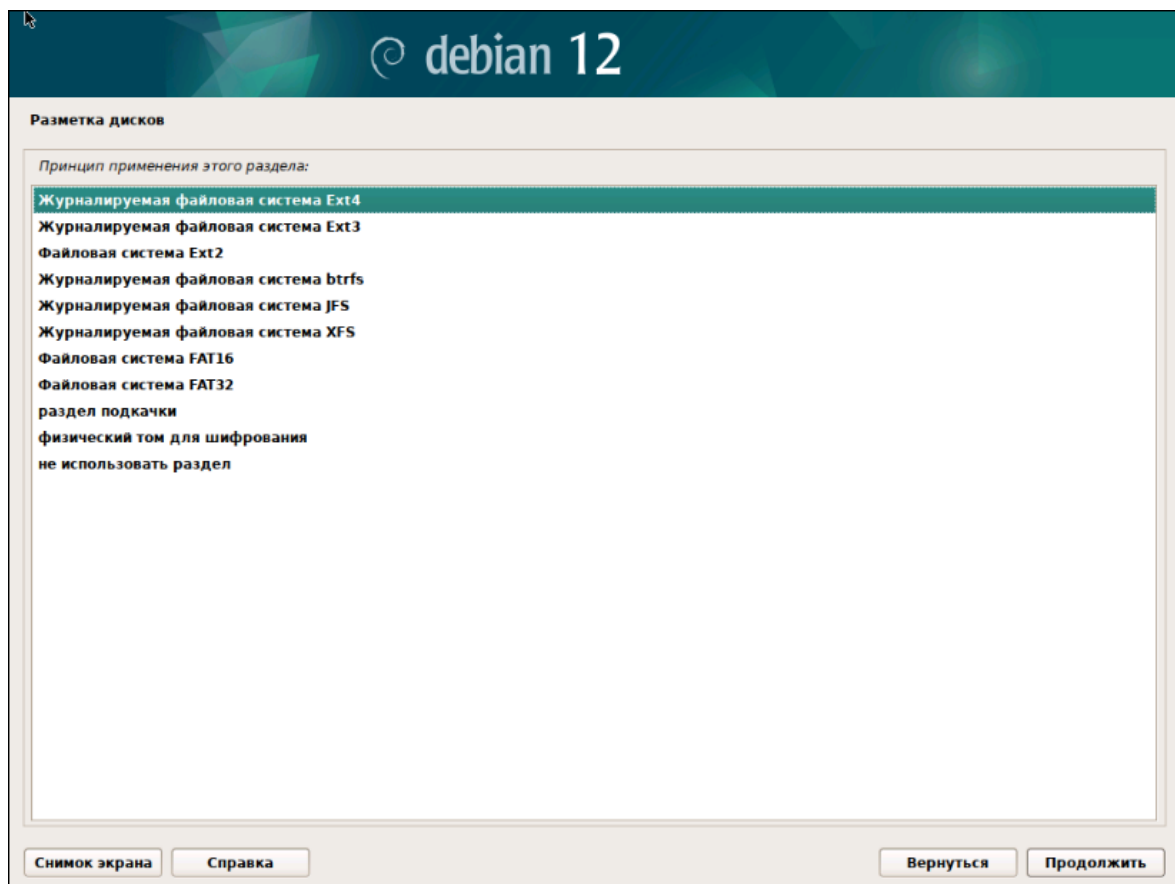


Рис. 5.30. Выбор файловой системы

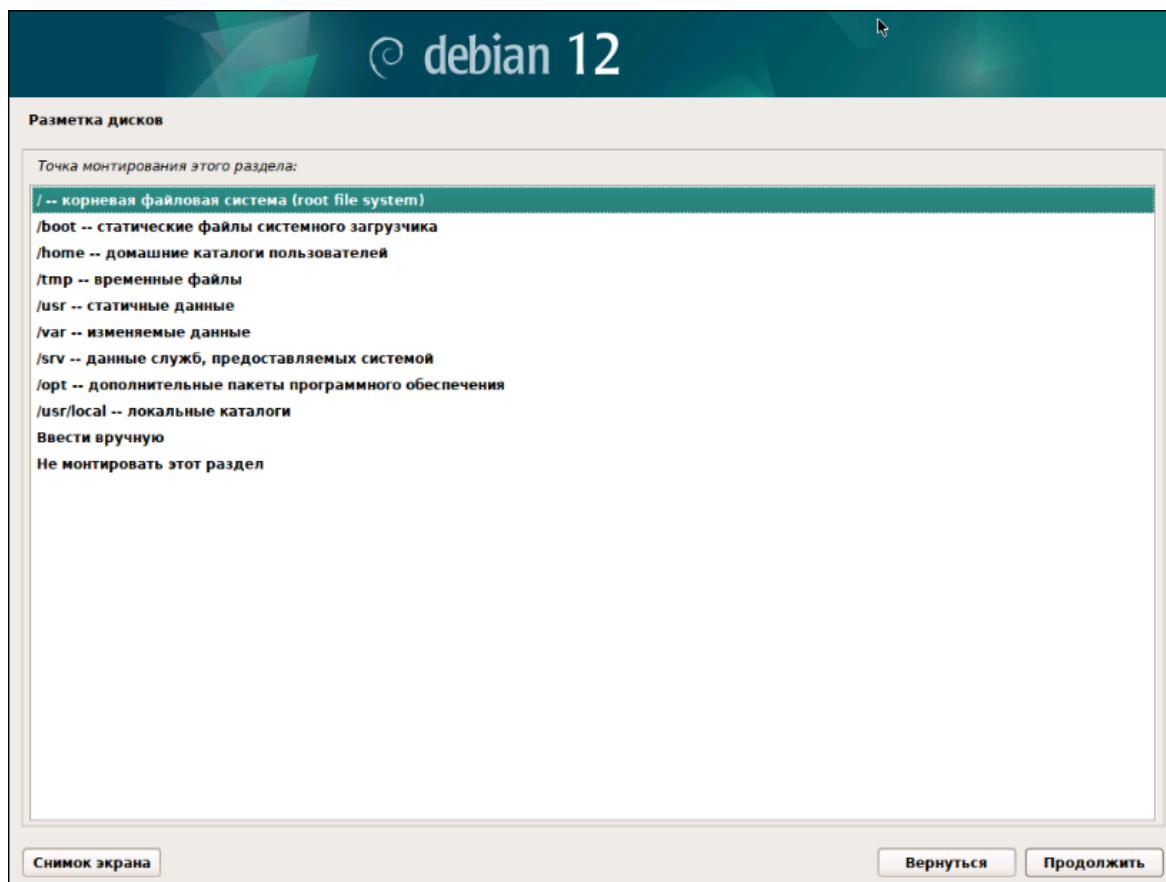


Рис. 5.31. Выбор точки монтирования



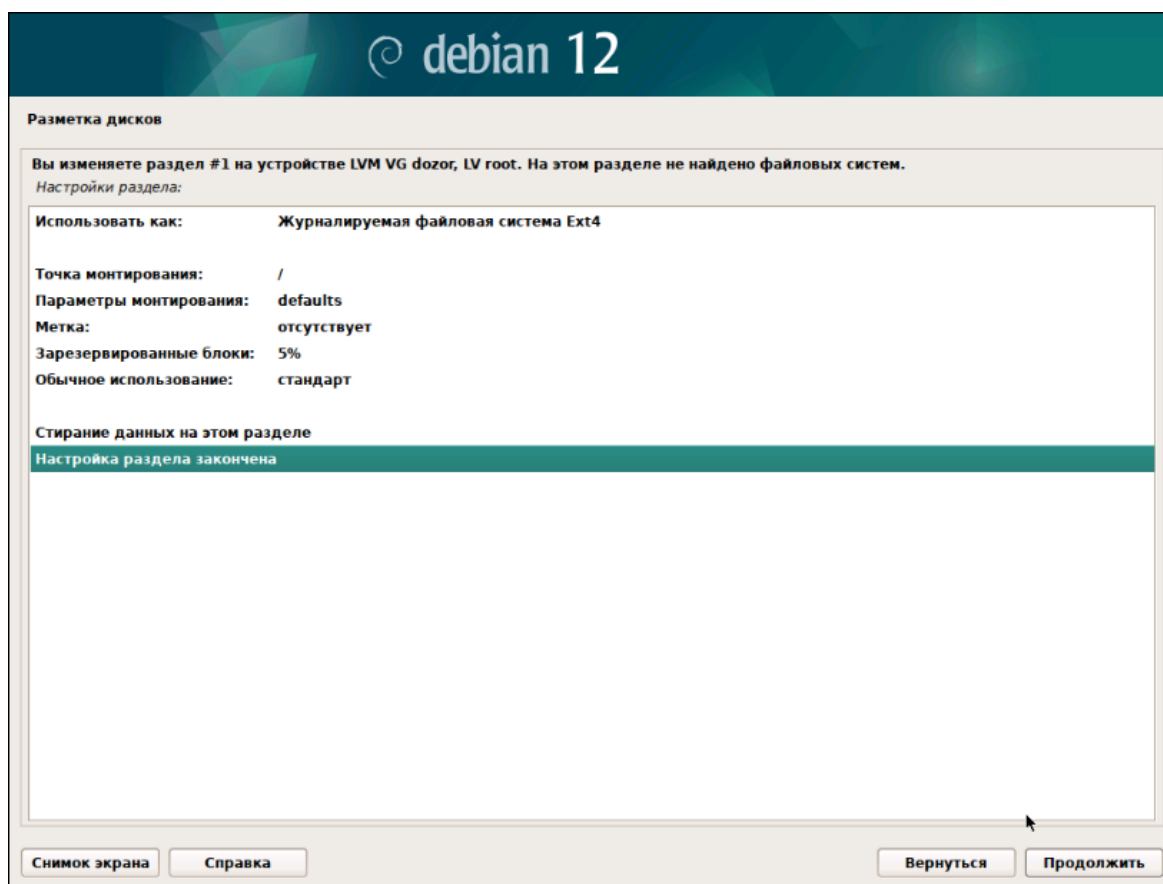


Рис. 5.32. Заполненные настройки тома root

36. Выполнить действия предыдущего шага, задавая следующие точки монтирования и файловые системы:

- **var** – /var, ext4
- **data** – /data, ext4 либо xfs (см. примечание)
- **storage** – /data/storage, xfs
- **opt** – /opt, ext4

При выборе точек монтирования для томов **data** и **storage** следует выбирать пункт **Ввести вручную**.

#### Внимание!

*Том, содержащий директорию /data/storage всегда должен иметь файловую систему **xfs**. Если эта директория содержится в отдельном томе **storage**, то он должен быть отформатирован под **xfs**, а том **data** – под **ext4**. Если отдельный том **storage** не создается, то весь том **data** должен быть отформатирован под **xfs**.*

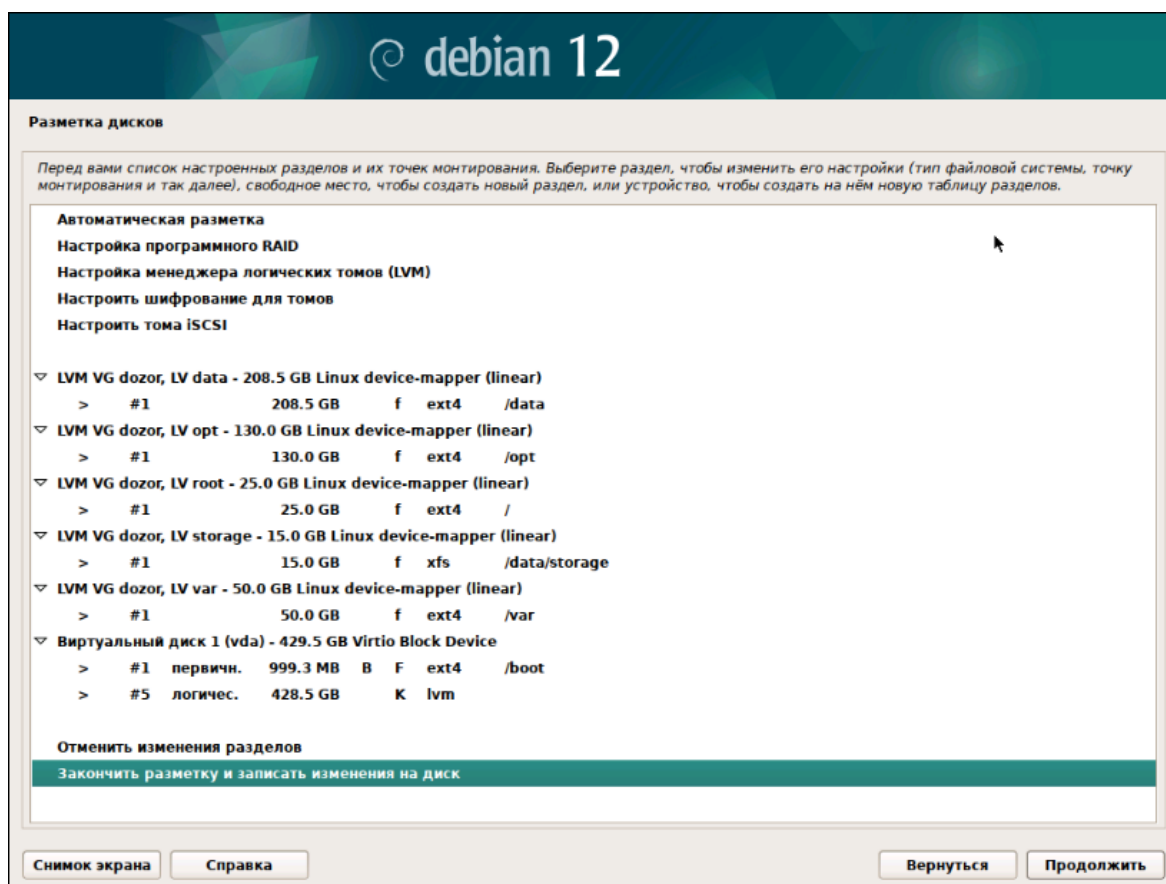


Рис. 5.33. Заполненные настройки томов для master-узла

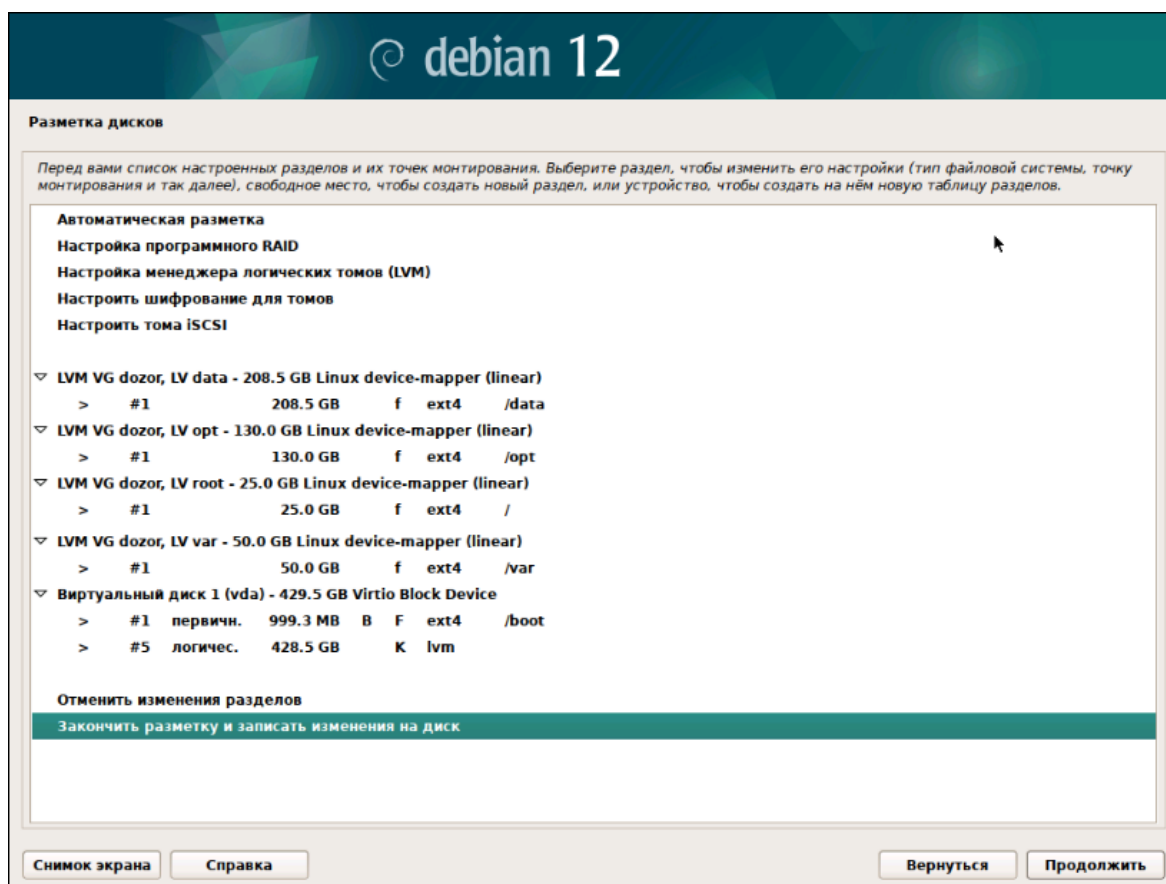


Рис. 5.34. Заполненные настройки томов для slave-узла

37. Выбрать строку **Закончить разметку и записать изменения на диск** и нажать **Продолжить**.
38. В появившемся окне будет отображено предупреждение об отсутствии разделов для пространства подкачки. Следует выбрать **Нет** и нажать **Продолжить**.

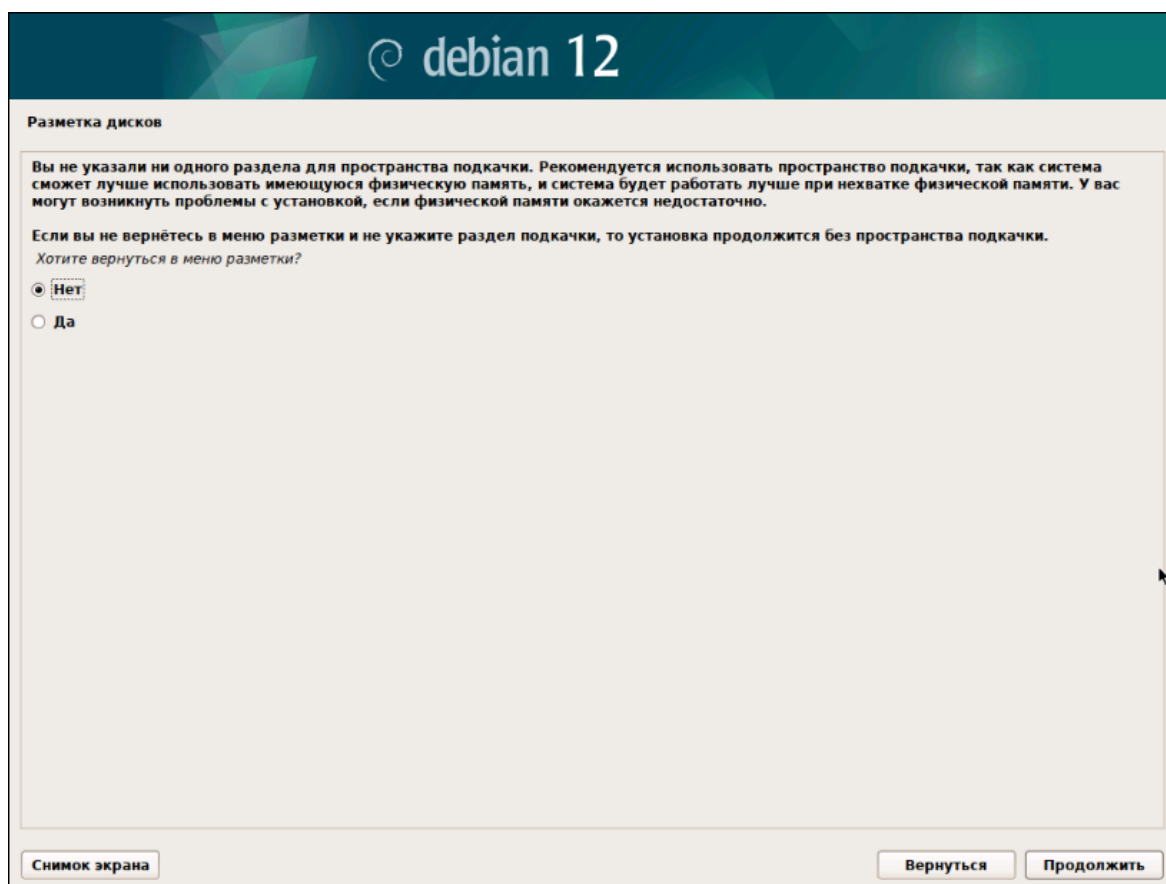


Рис. 5.35. Предупреждение об отсутствии разделов для пространства подкачки

39. В появившемся окне будет отображена информация о разметке дисков. Следует убедиться, что эта информация верна, выбрать **Да** и нажать **Продолжить**.

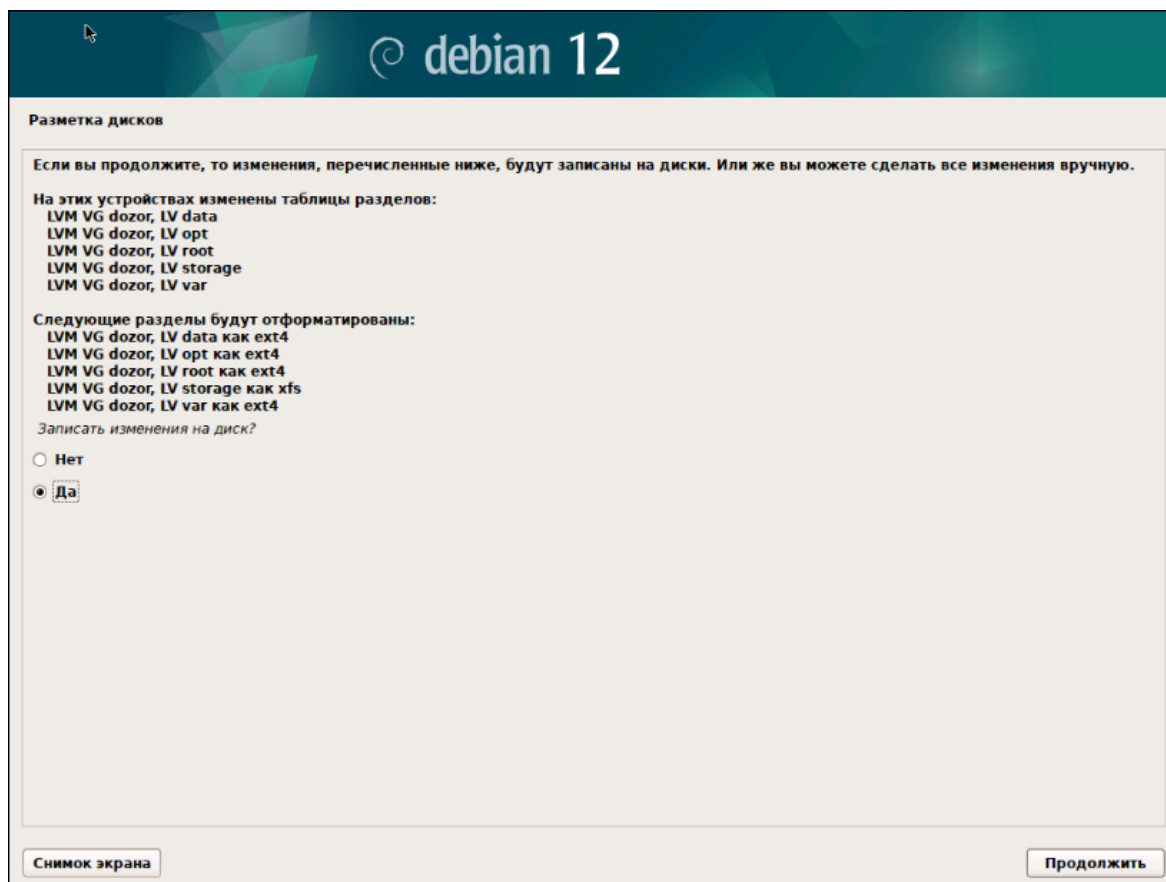


Рис. 5.36. Информация о разметке дисков

40. Дождаться установки базовой системы. На предложение просканировать следующий диск выбрать вариант **Нет**.



Рис. 5.37. Отказ от сканирования другого носителя

41. Выбрать любую страну, в которой будет расположено зеркало архива Debian. Нажать **Продолжить**.



Рис. 5.38. Выбор местоположения зеркала архива Debian

42. Выбрать зеркало архива Debian. Нажать **Продолжить**.

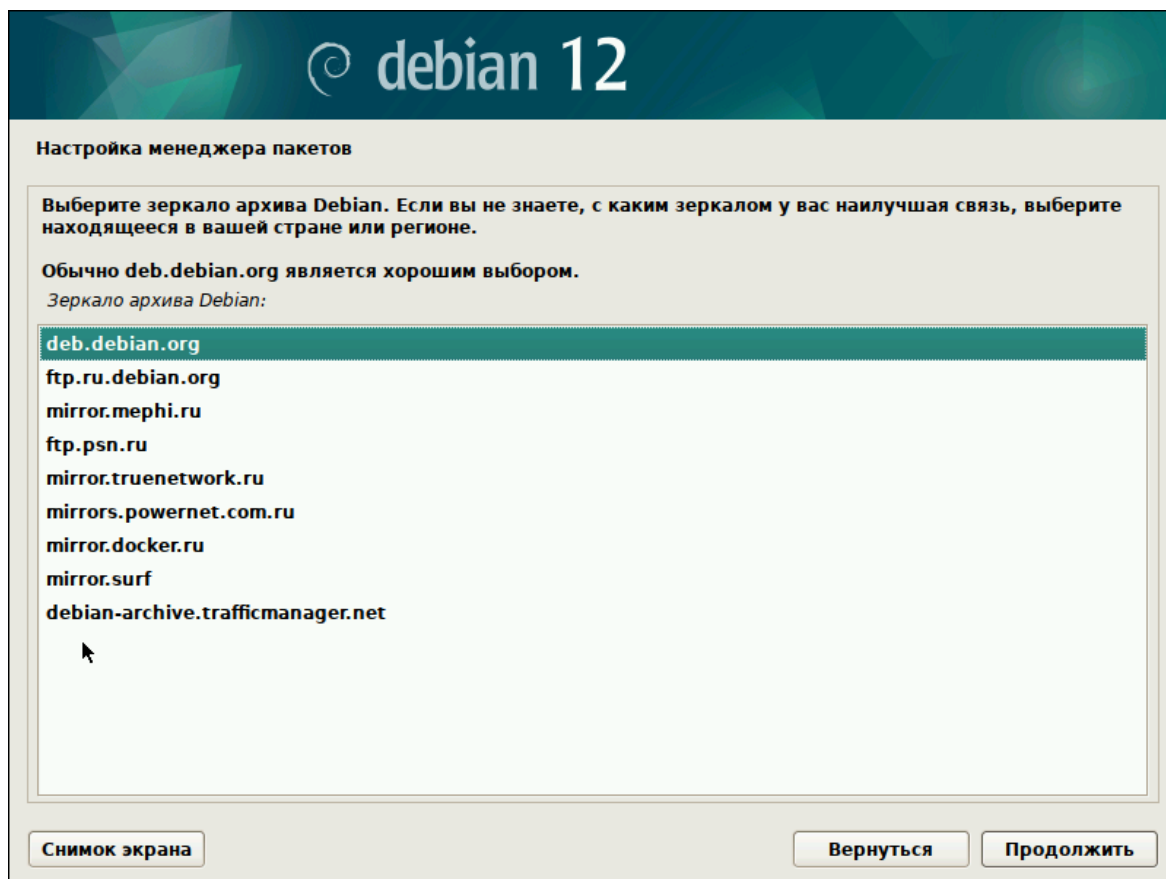


Рис. 5.39. Выбор зеркала архива Debian

43. Указать информацию о прокси-сервере. Если он не используется, оставить это поле пустым. Нажать **Продолжить**.



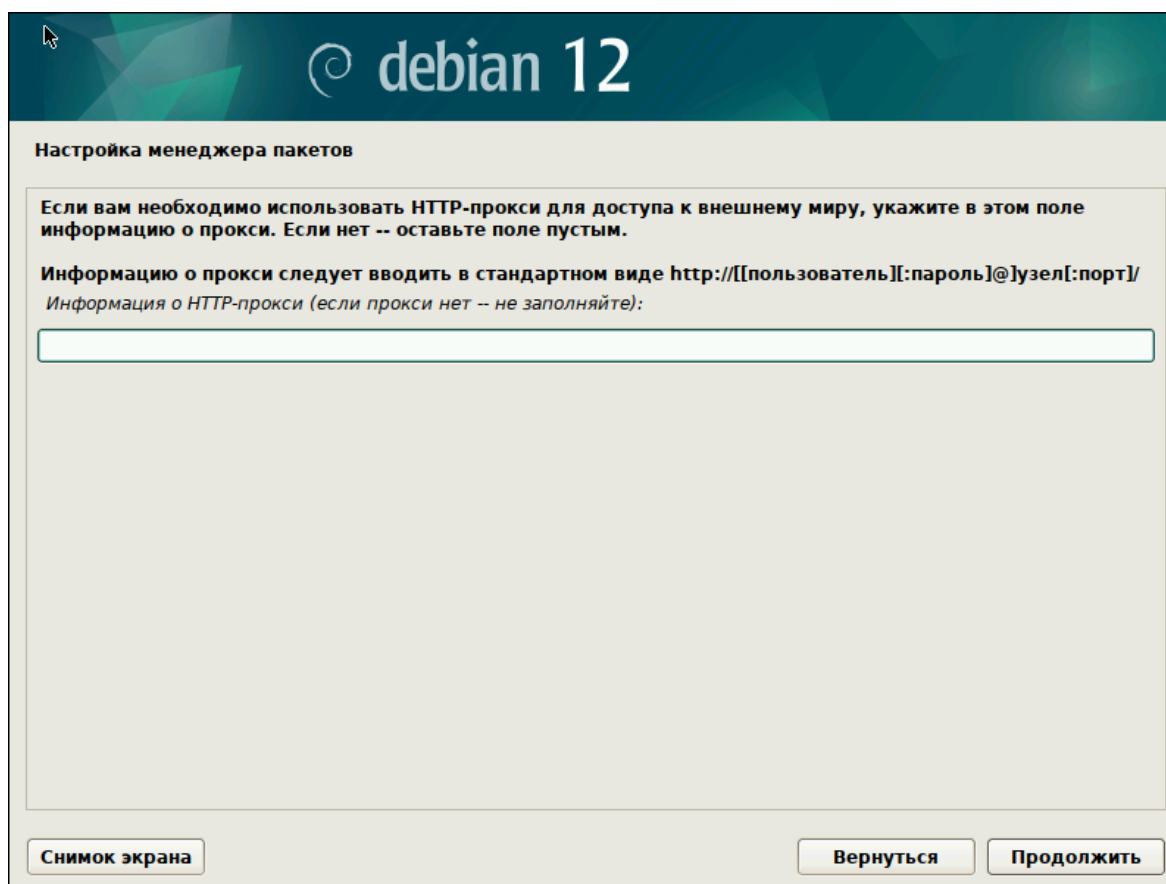


Рис. 5.40. Добавление информации о прокси-сервере

44. Пропустив вопрос об участии в опросе популярности пакетов, в появившемся окне **Выбор программного обеспечения** выбрать варианты **Стандартные системные утилиты** и **SSH-сервер**. Нажать **Продолжить**.

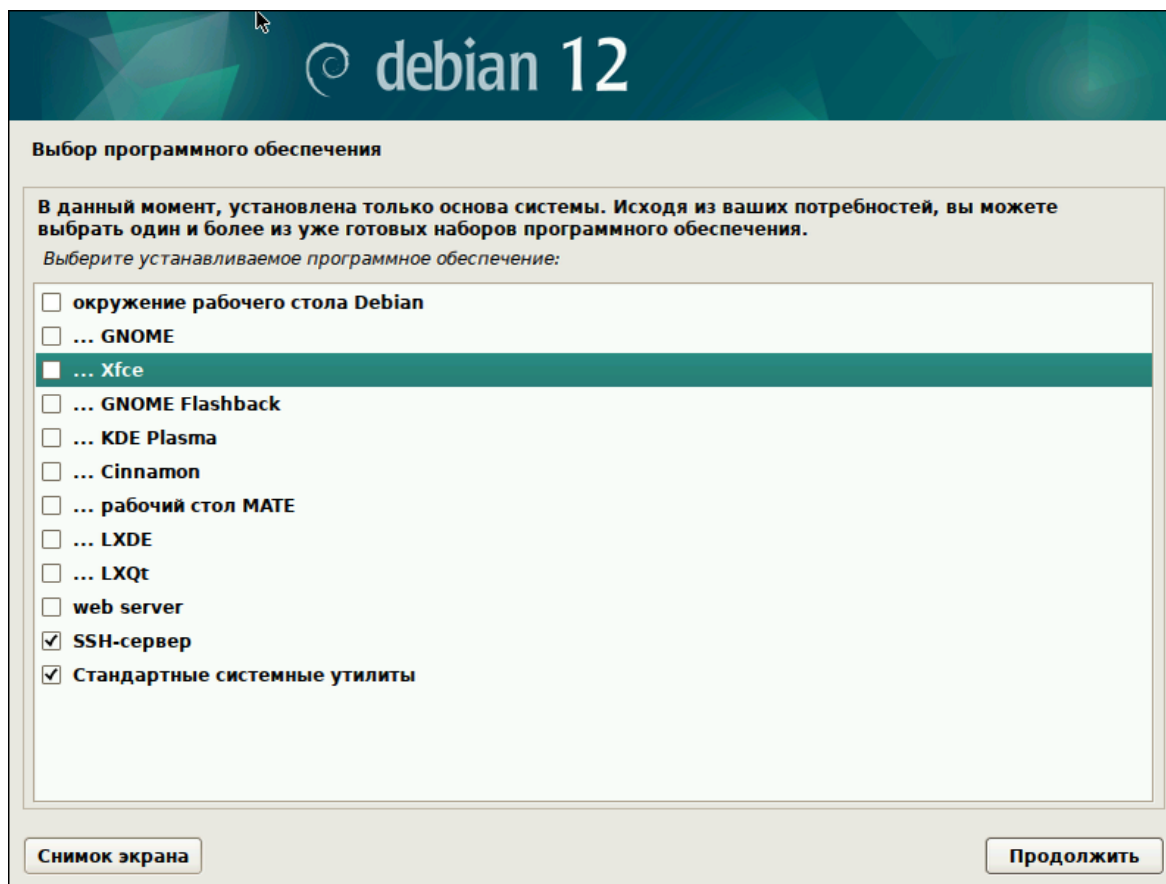


Рис. 5.41. Выбор программного обеспечения

45. Согласиться с установкой системного загрузчика GRUB. Нажать **Продолжить**.

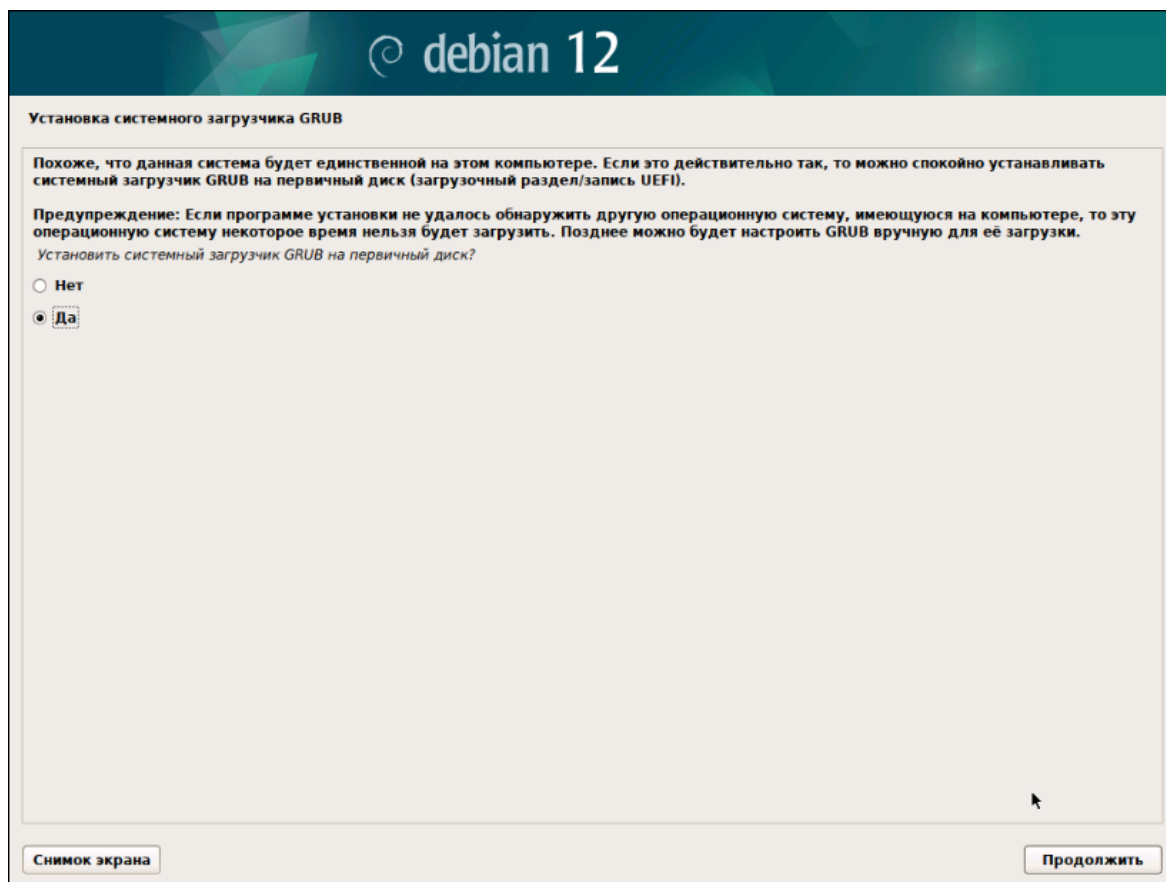


Рис. 5.42. Окно установки системного загрузчика GRUB

46. Выбрать устройство, на которое будет установлен загрузчик и нажать **Продолжить**.

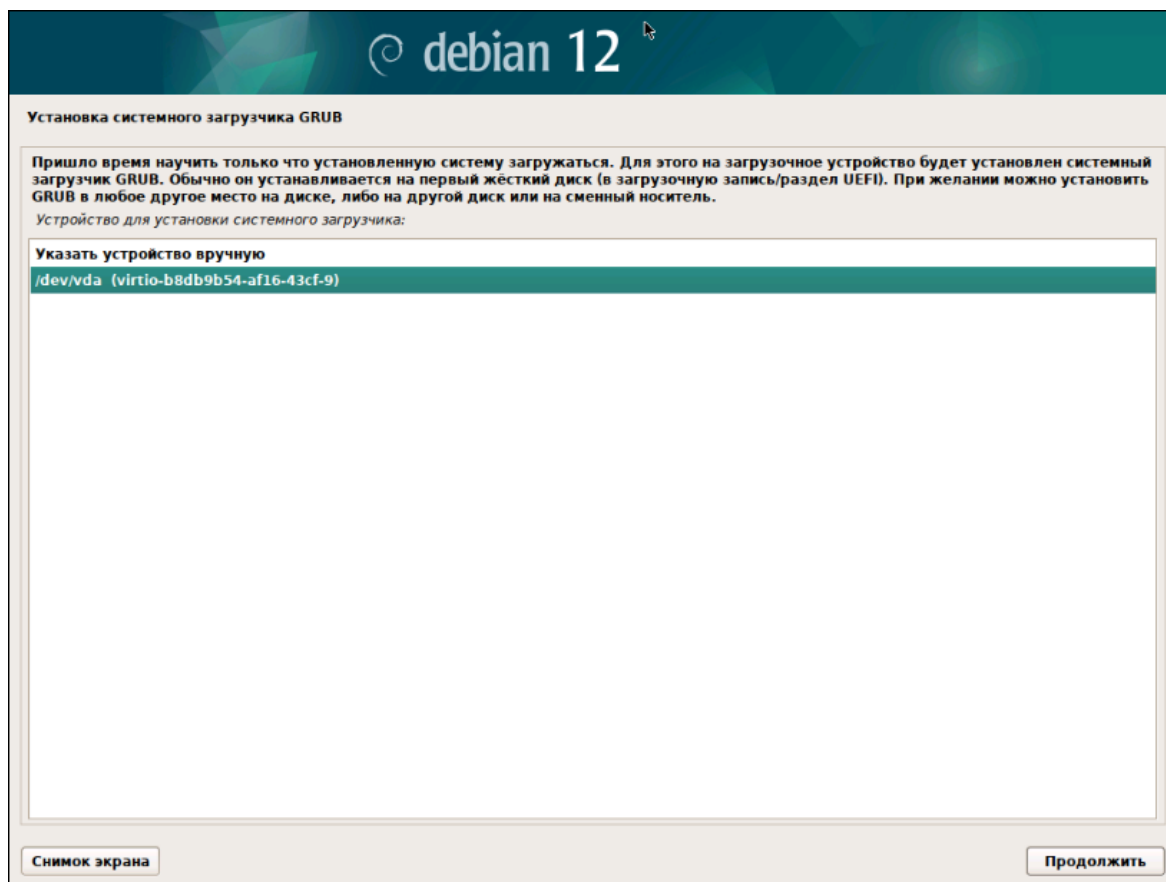


Рис. 5.43. Выбор устройства установки загрузчика

47. Дождаться завершения установки. По окончании установки нажать **Продолжить**.

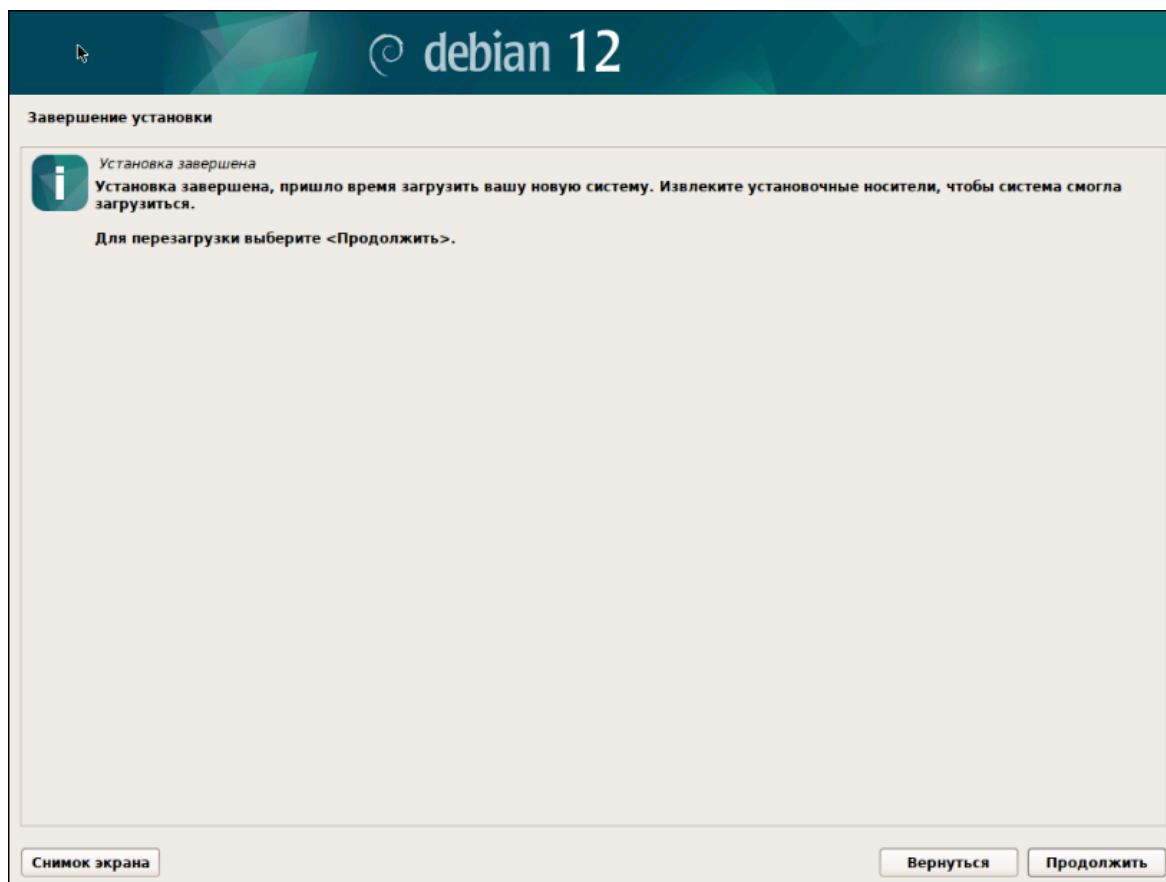


Рис. 5.44. Завершение установки ОС Debian

---

## 6. Настройка системы и установка KEO DLP в интерфейсе командной строки

### 6.1. Настройка системы

Приведенные в этом разделе процедуры предварительной настройки должны быть выполнены на всех серверах KEO DLP независимо от выбранной схемы развертывания.

#### Внимание!

*До завершения установки KEO DLP следует строго придерживаться описанных ниже процедур и не устанавливать какие-либо пакеты или обновления системы. Дистрибутив KEO DLP содержит все необходимые для работы пакеты, и в случае его установки на ОС с дополнительно установленными пакетами и/или обновлениями не гарантируется корректная работа KEO DLP.*

#### 6.1.1. Настройка DNS

Необходимо проверить содержимое следующих файлов настройки DNS на всех узлах KEO DLP:

- **/etc/hosts**
- **/etc/hostname**

Файл **/etc/hosts** должен содержать строки для всех узлов кластера KEO DLP, каждая из которых состоит из IP-адреса узла, его полного (FQDN) и краткого (домен нижнего уровня) доменного имени, например, так:

```
10.199.21.148 dozor7master.company.local dozor7master
10.199.21.149 dozor7filter1.company.local dozor7filter1
10.199.21.150 dozor7filter2.company.local dozor7filter2
```

После установки ОС файл **/etc/hosts** содержит следующую строку:

```
127.0.1.1 dozor73
```

Эту строку следует удалить или поместить под символ комментария (#).

IP-адрес и записи доменного имени должны быть разделены символом табуляции.

#### Внимание!

*При указании доменного имени узла нельзя использовать символ подчеркивания.*

Файл **/etc/hostname** должен содержать единственную строку, представляющую собой FQDN узла.

#### 6.1.2. Настройка файловой системы

При наличии внешней СХД необходимо примонтировать ее к разделу **/data** master-узла.

---

Следует убедиться, что раздел **/tmp** на master-узле примонтирован без использования опции **noexec**. Это можно сделать, выполнив команду:

```
# mount | grep /tmp | grep noexec
```

Вывод команды должен быть пустым. В противном случае следует поменять опцию монтирования для раздела **/tmp** и перемонтировать его. Для этого необходимо выполнить следующие действия:

1. Открыть для редактирования файл **/etc/fstab** и найти в нем строку, относящуюся к разделу **/tmp**.
2. Заменить в этой строке опцию **noexec** на **exec**. Сохранить и закрыть файл.
3. Перемонтировать раздел, выполнив команду:

```
# mount -o remount,exec /tmp
```

### 6.1.3. Настройка синхронизации времени

Синхронизация времени внутри кластера KEO DLP необходима для его корректной работы. В отсутствие контроллера домена или другого источника точного времени возникнут проблемы из-за разного времени в журналах и метках времени на данных, а также возможны проблемы с работой протокола HTTPS. Для синхронизации времени могут быть использованы один или несколько серверов точного времени, находящихся как в корпоративной сети, так и в сети Интернет.

Для настройки синхронизации времени необходимо на всех узлах KEO DLP выполнить следующие действия:

1. Найти нужную временную зону, выполнив следующую команду:

```
# timedatectl list-timezones
```

Для удобства поиска можно воспользоваться сортировкой, например:

```
# timedatectl list-timezones | grep Europe
```

2. Установить нужную временную зону, выполнив команду следующего вида:

```
# timedatectl set-timezone <timezone>
```

где **<timezone>** – значение, найденное в предыдущем шаге.

3. Во избежание расхождения настроек временной зоны в БД выполнить команду:

```
# DEBIAN_FRONTEND=noninteractive dpkg-reconfigure tzdata
```

4. Удостовериться в правильности настройки временной зоны, выполнив следующую команду:

```
# timedatectl
```

5. Открыть для редактирования файл **/etc/ntp.conf** и добавить в него одну или несколько строк следующего вида:

```
server <timeserver> iburst
```

где **<timeserver>** – FQDN или IP-адрес NTP-сервера (внешнего или принадлежащего организации). Параметр **iburst** является необязательным и служит для повышения точности синхронизации за счет увеличенного количества пакетов, отправляемых при обмене данными с NTP-сервером.

Наличие нескольких записей позволяет продолжать синхронизацию в случае отказа какого-либо из NTP-серверов. Серверы опрашиваются по очереди, в порядке их перечисления в файле **ntp.conf**.

6. Запустить службу NTP и добавить ее в автозагрузку, выполнив команды:

```
# systemctl start ntp
```

```
# systemctl enable ntp
```

Узнать список работающих используемых серверов точного времени можно выполнив следующую команду:

```
# ntpq -p
```

## 6.2. Установка KEO DLP

Процедура и порядок установки KEO DLP описаны ниже, а также в документе *Описание релиза*.

Табл. 6.1. Контрольный лист действий при одномашинной конфигурации

| № п/п | Наименование действия                | Ссылки на разделы                                                                                                                                                           | Обязательно    | Примечания                                                                         |
|-------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|------------------------------------------------------------------------------------|
| 1     | Установка пакетных файлов KEO DLP    | Раздел <a href="#">6.2.1</a> .<br>Документ <i>Описание релиза</i> .                                                                                                         | да             |                                                                                    |
| 2     | Вход в систему и загрузка лицензии   | Разделы <a href="#">6.3</a> и <a href="#">6.4</a> .                                                                                                                         | да             |                                                                                    |
| 3     | Назначение ролей узлам               | Раздел <a href="#">8.2</a> .                                                                                                                                                | да             |                                                                                    |
| 4     | Создание БД инцидентов               | Раздел <a href="#">8.4</a> .                                                                                                                                                | да             |                                                                                    |
| 5     | Создание БД хранения медиаинформации | Раздел <a href="#">8.5</a> .                                                                                                                                                | да             |                                                                                    |
| 6     | Создание БД архива                   | Раздел <a href="#">8.3</a> .                                                                                                                                                | см. примечание | Можно создать сколь угодно много БД архива (при желании можно не создавать вовсе). |
| 7     | Установка дополнительных модулей     | <ul style="list-style-type: none"><li>Модуль KEO DLP File Crawler – раздел <a href="#">11</a>.</li><li>Модуль KEO DLP Endpoint Agent – раздел <a href="#">13</a>.</li></ul> | нет            | При наличии соответствующих пунктов лицензии KEO DLP                               |

Табл. 6.2. Контрольный лист действий при распределенной конфигурации

| № п/п | Наименование действия             | Ссылки на разделы              | Обязательно | Примечания |
|-------|-----------------------------------|--------------------------------|-------------|------------|
| 1     | Установка пакетных файлов KEO DLP | Раздел <a href="#">6.2.2</a> . | да          |            |



| № п/п | Наименование действия                | Ссылки на разделы                                                                                                                                                              | Обязательно    | Примечания                                                                          |
|-------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------------------------------------------------------------------------|
|       |                                      | Документ <i>Описание релиза</i> .                                                                                                                                              |                |                                                                                     |
| 2     | Вход в систему и загрузка лицензии   | Разделы <a href="#">6.3</a> и <a href="#">6.4</a> .                                                                                                                            | да             |                                                                                     |
| 3     | Назначение ролей узлам               | Раздел <a href="#">8.2</a> .                                                                                                                                                   | да             |                                                                                     |
| 4     | Создание БД инцидентов               | Раздел <a href="#">8.4</a> .                                                                                                                                                   | да             |                                                                                     |
| 5     | Создание БД хранения медиаинформации | Раздел <a href="#">8.5</a> .                                                                                                                                                   | да             |                                                                                     |
| 6     | Создание БД архива                   | Раздел <a href="#">8.3</a> .                                                                                                                                                   | см. примечание | Можно создать сколь угодно много БД архива (при желании, можно не создавать вовсе). |
| 7     | Установка дополнительных модулей     | <ul style="list-style-type: none"> <li>Модуль KEO DLP File Crawler – раздел <a href="#">11</a>.</li> <li>Модуль KEO DLP Endpoint Agent – раздел <a href="#">13</a>.</li> </ul> | нет            | При наличии соответствующих пунктов лицензии KEO DLP                                |

Ниже описана установка только KEO DLP. Создание БД архива сообщений, БД событий и инцидентов ИБ и БД для хранения медиаинформации, описаны в разделах [8.3](#), [8.4](#) и [8.5](#) соответственно.

### 6.2.1. Установка в одномашинной конфигурации

Для установки KEO DLP следует выполнить следующие действия:

1. Скопировать полученный от производителя файл **dlp-dozor-8.1.0-73.debian-12.10.run** на сервер, на котором будет выполнена установка KEO DLP, например, в каталог **/var/tmp/**.

2. Проверить контрольную сумму загруженного файла, выполнив команды:

```
# cd /var/tmp/
```

```
# md5sum dlp-dozor-8.1.0-73.debian-12.10.run
```

Сопоставить полученное значение с контрольной суммой, приведенной в документе *Описание релиза*, раздел *Состав релиза*. При несовпадении значений прервать установку и связаться с производителем.

3. Проверить наличие пользователя **dozor** в системе, выполнив команду:

```
# cat /etc/passwd | grep dozor
```

При наличии в системе пользователя **dozor** следует его удалить, выполнив команду:

```
sudo deluser dozor
```

4. Для ОС Astra Linux изменить командную оболочку по умолчанию на **bash**, выполнив команду:

```
sudo dpkg-reconfigure dash
```

Выбрать вариант **Нет**.

- 
5. Открыть файлы **/etc/apt/sources.list** и **/etc/apt/sources.list.d/\*.list**, и проверить наличие в них репозиториев. При наличии репозиториев следует закомментировать все строки. Сохранить и закрыть файлы. После установки можно снова включить все нужные репозитории.

6. Запустить установку KEO DLP, выполнив команду:

```
~$ sudo ./dlp-dozor-8.1.0-73.debian-12.10.run -c
```

Во время установки система предложит задать пароль пользователя по умолчанию для БД Clickhouse. Этот пароль не используется во время эксплуатации KEO DLP, поэтому достаточно нажать **Ok**.

7. Назначить сервер master-узлом, выполнив следующую команду:

```
~$ sudo /opt/dozor/bin/set-role master main
```

8. Запустить KEO DLP, выполнив команды:

```
~$ sudo /opt/dozor/bin/shell
```

```
~$ dsctl boot
```

9. Перезагрузить ОС, выполнив команду:

```
~$ sudo init 6
```

После этого следует продолжить работу в GUI KEO DLP (см. раздел [6.3](#)).

### 6.2.2. Установка в распределенной конфигурации

Для установки KEO DLP следует выполнить на каждом сервере следующие действия:

1. Установить KEO DLP на все узлы согласно инструкциям раздела [6.2.1](#).

2. Запустить интерпретатор команд shell, выполнив команду:

```
~$ sudo /opt/dozor/bin/shell
```

3. Назначить один из серверов master-узлом, выполнив на нем следующую команду:

```
~$ sudo set-role master main
```

4. Запустить KEO DLP, выполнив следующую команду:

```
~$ sudo dsctl boot
```

5. Назначить все остальные серверы slave-узлами, выполнив на каждом из них команду следующего вида:

```
~$ sudo reg-slave <master-host> <name> <role-list>
```

где:

- **<master-host>** – FQDN master-узла.

- **<name>** – имя регистрируемого slave-узла. Это имя будет отображаться в GUI.

#### Примечание

*При указании имени узла нельзя использовать символ подчеркивания и верхний регистр текста.*

#### Внимание!

*В некоторых ситуациях (в основном, при клонировании виртуальных машин) могут возникать узлы с одинаковыми идентификаторами. Если узел с таким же именем и идентификатором, как и у вновь регистрируемого узла, уже присутствует в кластере KEO DLP, то вновь зарегистрированный узел заместит его в описании кластера. При совпадении идентификаторов и различии имен, идентификатор регистрируемого узла будет сгенерирован заново, и он будет корректно добавлен в кластер. Поэтому следует внимательно выбирать имя для регистрируемого узла.*

- **<role-list>** – список ролей, назначаемых узлу. Роли перечисляются через пробел. Описание ролей приведено в приложении [Приложение D, Описание ролей и сервисов](#).

Например, если имеется три сервера, один из которых является master-узлом, а на двух других требуется организовать фильтры почтового потока с именами **filter1** и **filter2**, то на каждом из этих двух узлов следует выполнить от имени пользователя **root** или **dozor** соответствующую команду следующего вида:

```
~$ sudo reg-slave <master-host> filter1 smtp-filter
```

```
~$ sudo reg-slave <master-host> filter2 smtp-filter
```

#### Внимание!

*Если при выполнении команды **reg-slave** возникла ошибка, следует проверить правильность написания команды и ее аргументов, исправить возможные ошибки и повторно выполнить команду.*

6. Запустить сервисы KEO DLP на всех slave-узлах, выполнив на каждом из них команду:

```
~$ sudo dsctl boot
```

После этого следует продолжить работу в GUI KEO DLP (см. раздел [6.3](#)).

## 6.3. Первый вход в систему

Для входа в GUI KEO DLP следует ввести в адресной строке браузера адрес **https://<доменное имя master-узла KEO DLP>** (либо можно использовать доменное имя другого узла которому назначена роль **Локальный веб-сервер**), и подтвердить включение сертификата безопасности. Появится окно авторизации (см. [Рис.6.1](#)):

---

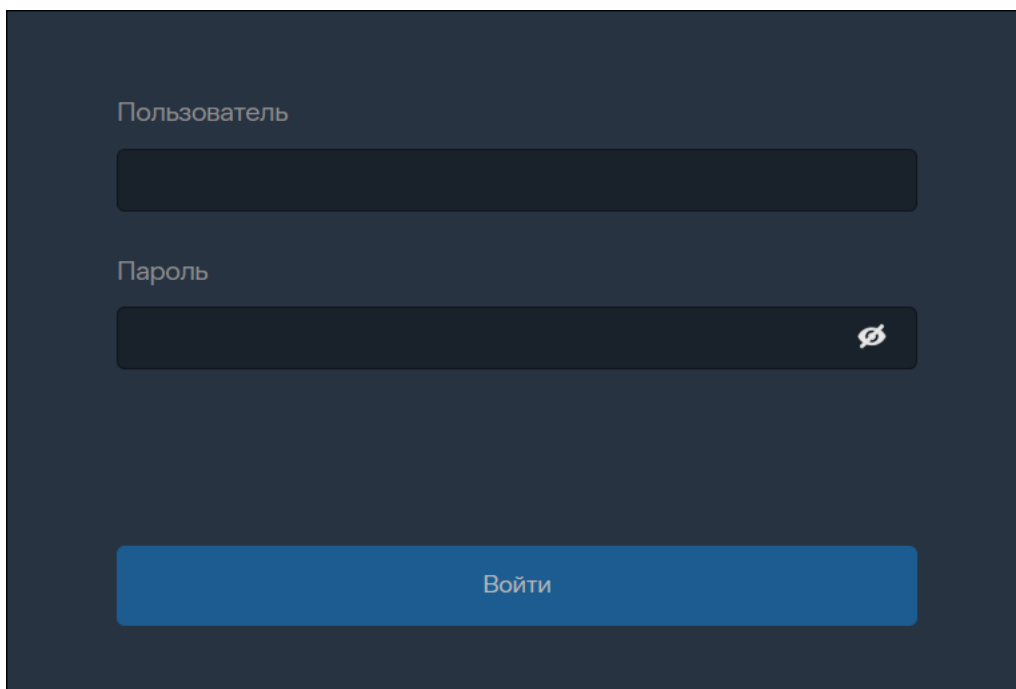


Рис. 6.1. Окно авторизации при входе в систему

В окне авторизации следует указать следующие имя и пароль по умолчанию: **superadmin/superadmin**. После первой авторизации система потребует изменить пароль по умолчанию (см. [Рис.6.2](#)). Следует изменить пароль, указав его дважды.

Рис. 6.2. Окно смены пароля

#### Внимание!

*Пароль должен содержать от 6 до 12 символов, а также отвечать критериям сложности. Требования к сложности пароля и метод ее вычисления приведены в документе Руководство системного Администратора, в приложении **Требования к паролям учетных записей пользователей**.*

## 6.4. Загрузка лицензии

### 6.4.1. Загрузка лицензии KEO DLP

После первоначальной смены пароля в верхней части экрана появится уведомление об отсутствии лицензии (см. [Рис.6.3](#)). Для получения файла лицензии следует скопировать указанный в уведомлении идентификатор инсталляции и отправить его в вендорскую службу поддержки KEO DLP.

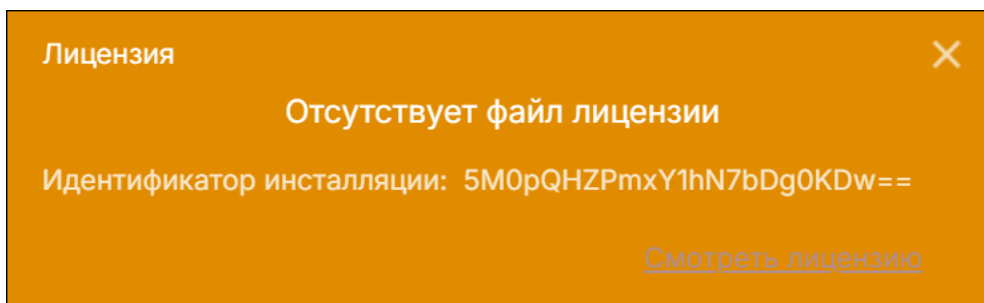


Рис. 6.3. Уведомление об отсутствии лицензии

Для загрузки лицензии следует нажать кнопку **Смотреть лицензию**, и в появившемся окне **Лицензия** нажать кнопку **Загрузить лицензию**. В открывшемся окне проводника указать путь к файлу с лицензией, после чего нажать кнопку **Открыть (Open)** и дождаться загрузки лицензии. При этом она автоматически сохранится в файле с именем **license.xml**.

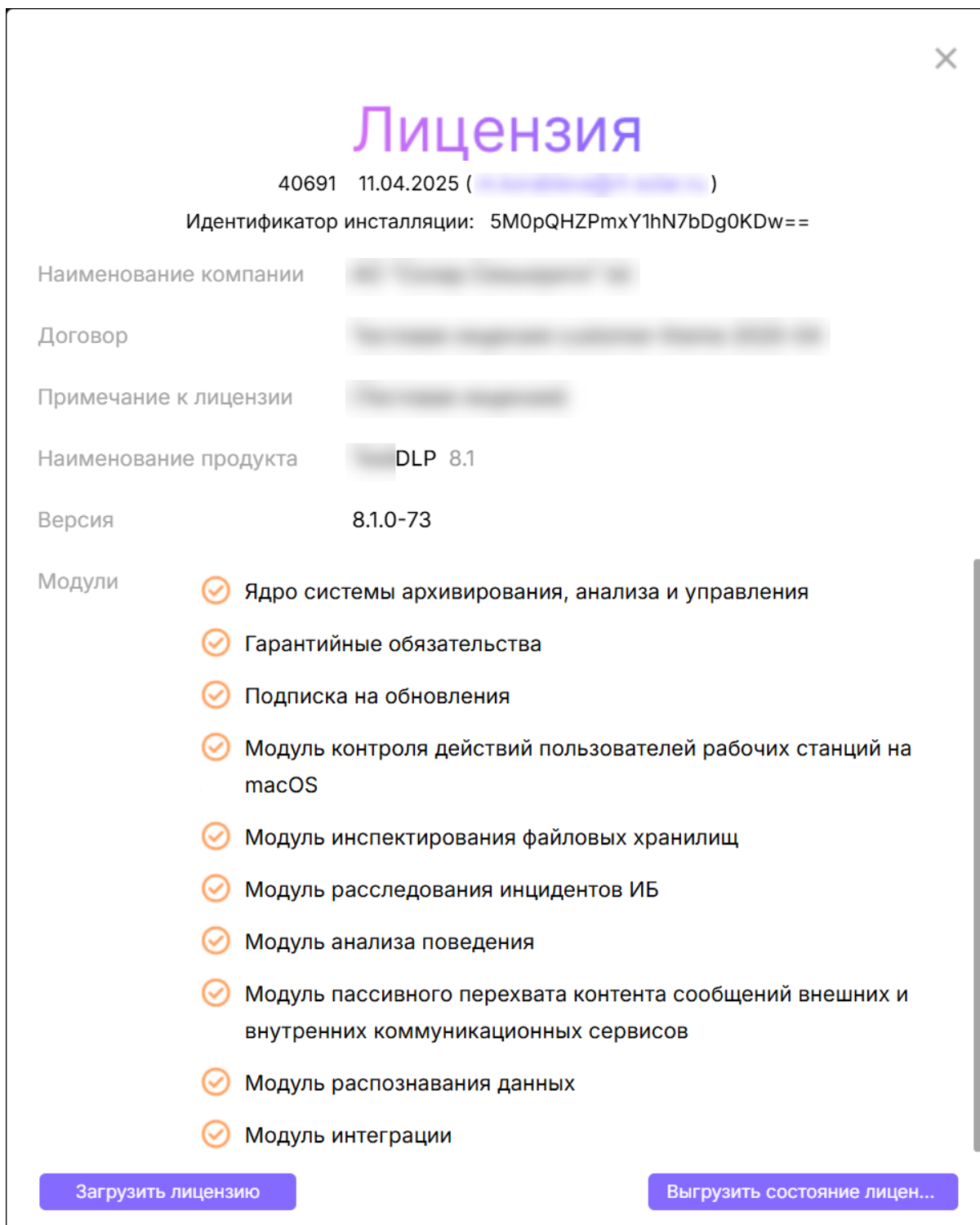


Рис. 6.4. Информация о лицензии KEO DLP

В лицензии применяются следующие условные обозначения:

-  – модуль доступен для использования.

-  – требуется внимание к модулю: до окончания разрешенного лицензией срока использования осталось менее 30 дней и/или количественное ограничение модуля превышено не более чем на 20%.
-  – модуль недоступен для использования: истек или не начался разрешенный лицензией срок использования или количественное ограничение модуля превышено более чем на 20%.

В лицензии также указаны версия и сборка продукта.

### Внимание!

*После замены лицензии с истекшим сроком действия необходимо перезапустить следующие процессы:*

- `agent-control-ng`
- `agent-server`
- `archiver-server`
- `mailfilter`
- `smap-smtp-gw`
- `crawler-ccc`
- `crawler-database`
- `crawler-pccc`
- `crawler-processor`
- `crawler-scanner`
- `crawler-snapshot`
- `smap-activemq`

Контроль состояния лицензии осуществляется сервисом **license-server**, входящим в роли **Сервер управления (master)** и **Сервер лицензирования подкластера (license-server)**. Сервис выполняет следующие функции:

- Периодическая проверка идентификатора инсталляции на соответствие указанному в лицензии (по умолчанию – каждые 30 минут).

В случае несоответствия идентификатора инсталляции, сформированного на основе характеристик аппаратной платформы master-узла, и идентификатора, указанного в лицензии, на экран выводится соответствующее уведомление, а функционирование KEO DLP прекращается.

- Периодический пересчет количества активных адресов электронной почты и сравнение его с количеством, указанным в лицензии (по умолчанию – раз в сутки).



---

В случае превышения разрешенного лицензией количества активных адресов электронной почты не более чем на 20% на экран выводится соответствующее уведомление, а ресурс **Количество активных адресов** принимает состояние WARNING (см. раздел *Мониторинг состояния ресурсов* документа *Руководство системного администратора*). В случае превышения разрешенного лицензией количества активных адресов электронной почты более чем на 20% на экран выводится соответствующее уведомление, а ресурс **Количество активных адресов** принимает состояние CRITICAL. Функционирование KEO DLP при этом не прекращается.

В случае территориально-распределенной инсталляции, при увеличении количества активных адресов электронной почты требуется расширение как основной лицензии, так и лицензии филиала, где было увеличено это количество.

Адрес электронной почты считается активным, если он принадлежит одному из доменов, указанных в лицензии в качестве внутренних, и является источником хотя бы одного сообщения в архиве за последние 30 дней.

- Периодический подсчет допустимого количества macOS-агентов и суммарного максимально допустимого количества агентов Windows и Linux, работающих в полнофункциональном режиме (т.е. перехватывающих данные).

В случае превышения разрешенного лицензией не процентного соотношения, а количества (для платформ macOS и Windows+Linux), или возникновения проблем с лицензией, агенты автоматически деактивируются (т.е. перестают перехватывать данные). При этом в историю состояний каждого такого агента записывается информация о том, что агент был деактивирован из-за проблем с лицензией.

Как только проблема с лицензией устраняется, агенты (все или часть – зависит от условий лицензии) активируются автоматически или администратором системы обратно. То, как происходит активация агентов – автоматически или вручную – зависит от ранее установленного значения параметра конфигурации Автоматическая активация агентов при наличии квоты в лицензии, который расположен в разделе GUI **Система > Конфигурация > Расширенные настройки > Настройка модулей перехвата > Агенты > Сервер управления агентами**. По умолчанию агенты активируются автоматически (флажок установлен). При отключении автоматической активации у администратора появляется возможность задавать, на каких рабочих станциях агенты должны перехватывать данные.

#### Примечание

*Сначала будут деактивированы/активированы те агенты, которые позже всех перешли в полнофункциональный режим работы.*

- Периодическая проверка сроков действия модулей.
- Периодическая отправка информации с серверов лицензирования подкластеров на сервер управления.

После загрузки лицензии на каждом узле появляется кэш лицензии. Сервис почтового фильтра (**mailfilter**) обновляет этот кэш раз в пять минут, делая запросы к сервису **license-server**. В случае недоступности сервиса **license-server** сервис почтового фильтра обращается к этому кэшу для проверки лицензионных ограничений. Для сервиса почтового

---

фильтра кэш лицензии остается действительным в течение 30 суток с момента последнего обновления. Если кэш лицензии становится недействителен, а сервис **license-server** остается недоступен – сервис почтового фильтра останавливает работу. При этом сервис почтового фильтра продолжает попытки обновить кэш лицензии раз в пять минут, и в случае успеха возобновляет работу.

Аналогичным образом сервер агентов (**agent-server**) делает запросы к сервису **license-server** и обновляет кэш лицензии раз в 10 минут. При неудачной попытке обновления кэша сервер агентов предпринимает новые попытки каждые две минуты. Если с момента последнего обновления кэша лицензии прошел час или более, то для сервера агентов кэш лицензии становится недействительным, и он деактивирует все зарегистрированные у себя полнофункциональные агенты. При этом сервер агентов продолжает попытки обновить кэш лицензии раз в две минуты, и в случае успеха активирует агенты вновь.

Постоянная лицензия KEO DLP всегда жестко привязана к конкретной аппаратной платформе (виртуальной или физической) master-узла KEO DLP. Для однозначной привязки используется идентификатор инсталляции, представляющий собой особым образом формируемый хэш, зависящий от некоторых уникальных характеристик аппаратного обеспечения master-узла. Идентификатор инсталляции формируется при первом запуске GUI KEO DLP и передается инженерами внедрения в вендорскую службу поддержки, которая на его основе выпускает активированную лицензию для постоянного использования. Изменение хотя бы одной из характеристик master-узла, от которых зависит идентификатор инсталляции, приводит к недействительности выпущенной лицензии и неработоспособности KEO DLP. При функционировании master-узла в виртуальной среде миграция виртуальной машины приводит к тем же последствиям. В этих случаях необходимо обратиться в вендорскую службу поддержки для повторного выпуска лицензии.

Помимо аппаратных характеристик, на идентификатор инсталляции также влияют значения, записанные в файлах с путями вида **/sys/devices/system/cpu/cpu<num>/online**, где **<num>** – номер ядра процессора. Изменение хотя бы одного из них приводит к изменению идентификатора инсталляции.

#### Примечание

*Идентификатор инсталляции не зависит от характеристик оперативной памяти и жестких дисков, то есть их замена не приводит к недействительности лицензии.*

### 6.4.2. Загрузка лицензий других продуктов

KEO DLP также позволяет хранить лицензии других продуктов, имеющие тот же формат. Например, продукт DCAP не имеет собственного сервера лицензий и вынужден использовать сервер лицензий KEO DLP. Загрузка лицензий других продуктов выполняется так же, как и загрузка лицензий KEO DLP. При загрузке с помощью GUI нескольких лицензий одного и того же продукта необходимо учитывать следующее:

- Новая лицензия KEO DLP всегда замещает имеющуюся;
- Новые лицензии других продуктов всегда замещают имеющуюся лицензию того же продукта.

---

В директории хранения файлов лицензии не рекомендуется хранить файлы, у которых совпадают комбинации идентификатора инсталляции и имени продукта. Такая ситуация может возникнуть при добавлении файла лицензии напрямую в репозиторий или при загрузке файла лицензии с помощью сервиса другого продукта (например, DCAP). В этом случае будет использоваться файл лицензии с наибольшим значением идентификатора лицензии (поле **license-id**), и только эта лицензия будет отображаться для продукта в GUI.

При просмотре лицензий других продуктов в GUI KEO DLP для них не будет отображаться список модулей, поскольку KEO DLP не обладает возможностью чтения соответствующих полей таких лицензий.

---

## 7. Настройка KEO DLP для работы в активном режиме

Для настройки активного режима системы необходимо следующее:

1. Настроить маршрутизацию почтового потока в корпоративной сети таким образом, чтобы не существовало маршрутов между почтовыми серверами организации и внешним почтовым шлюзом в обход серверов KEO DLP.
2. Настроить серверы фильтрации KEO DLP для корректного приема и пересылки почтовых сообщений.

Первая задача возлагается на системного (сетевого) администратора организации и решается им самостоятельно.

Для настройки серверов фильтрации KEO DLP для корректного приема и пересылки почтовых сообщений необходимо:

1. Настроить программу отправки **Exim4** (раздел [7.1](#)).
2. Создать профиль отправки (раздел [7.2](#)).
3. Настроить политику фильтрации (раздел [7.3](#)).
4. Настроить балансировщик нагрузки на серверы фильтрации (раздел [7.4](#)).
5. Настроить отправку сообщений при ошибках фильтрации (раздел [7.5](#)).

### 7.1. Настройка Exim4

Для настройки программы **Exim4** необходимо на всех узлах выполнить следующие действия:

1. Выполнить обновление списка пакетов ОС, выполнив следующую команду:

```
~$ sudo apt-get update
```

2. Установить программу **Exim4**, выполнив следующую команду:

```
~$ sudo apt-get install exim4
```

#### Примечание

Если необходимо использовать ACL и другие расширенные функции, следует установить **exim4-daemon-heavy** командой:

```
~$ sudo apt-get install exim4-daemon-heavy
```

3. Перейти к настройке **Exim4**, выполнив следующую команду:

```
~$ sudo dpkg-reconfigure exim4-config
```

4. В появившемся окне выбрать **Отправка почты через smarthost; прием по SMTP через fetchmail** и нажать **OK**.

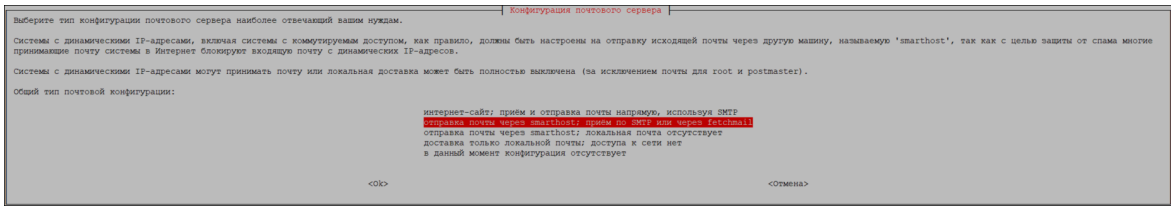


Рис. 7.1. Выбор типа почтовой конфигурации

5. В новом окне указать имя узла KEO DLP и нажать **ОК**.

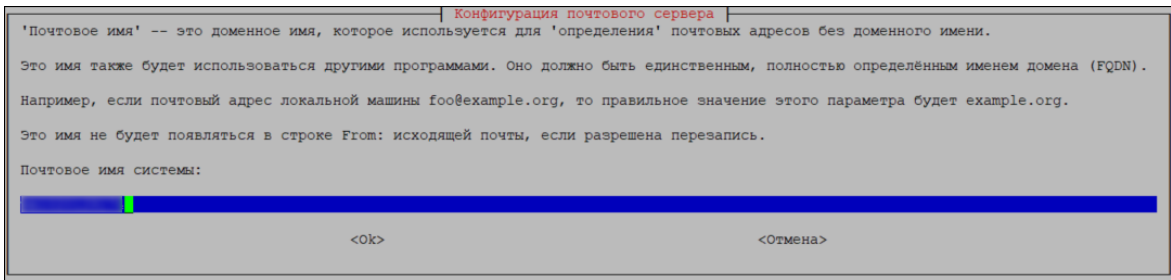


Рис. 7.2. Ввод имени узла

6. В открывшемся окне ввести 127.0.0.1 и нажать **ОК**.

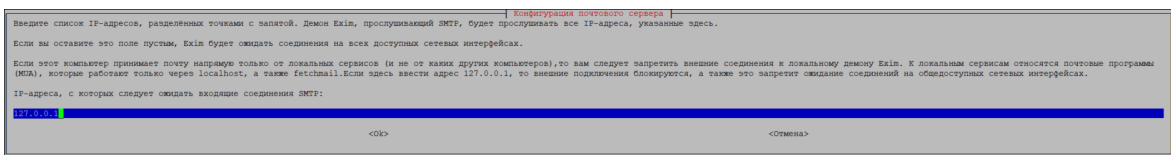


Рис. 7.3. Ввод loopback-адреса

7. В появившемся окне оставить строку пустой и нажать **ОК**.

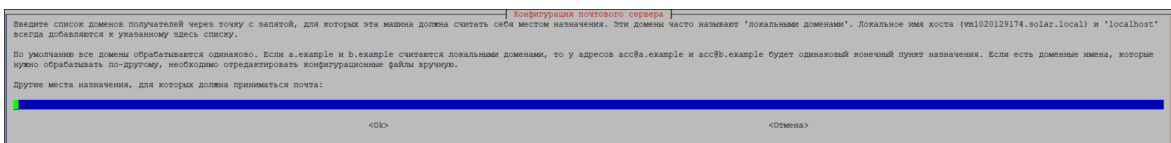


Рис. 7.4. Окно ввода локальных доменов

8. В открывшемся окне ввести символ \* и нажать **ОК**.

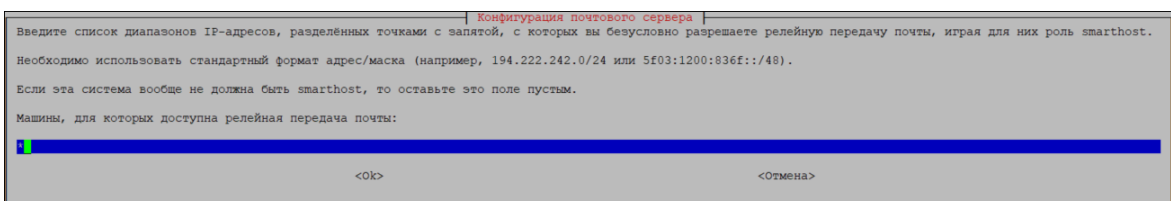


Рис. 7.5. Ввод доменов, для которых Exim будет ретранслировать сообщения

9. В появившемся окне ввести IP-адрес и порт почтового сервера организации и нажать **OK**.

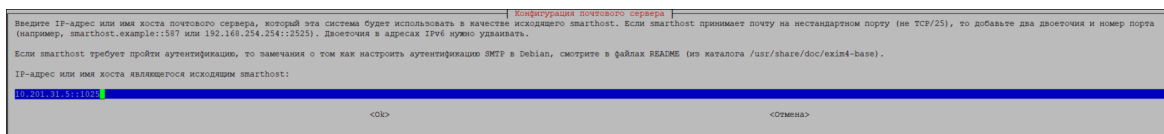


Рис. 7.6. Ввод IP-адреса и порта почтового сервера организации

10. В появившемся окне выбрать **Нет**.

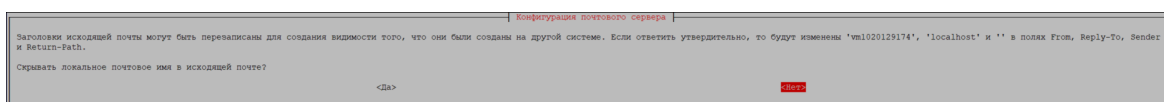


Рис. 7.7. Скрытие локального имени сервера

11. В появившемся окне выбрать **Нет**.

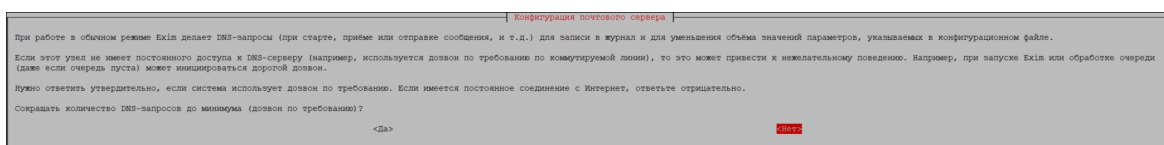


Рис. 7.8. Отключение поиска DNS при запуске

12. В новом окне выбрать **mbox формат в /var/mail/** и нажать **OK**.

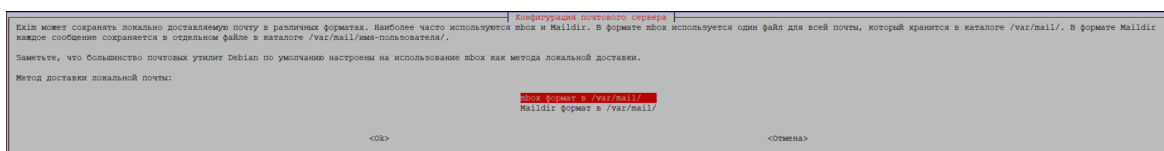


Рис. 7.9. Выбор метки доставки локальной почты

13. На вопрос о разделении файла конфигурации на маленькие ответить **Да**.

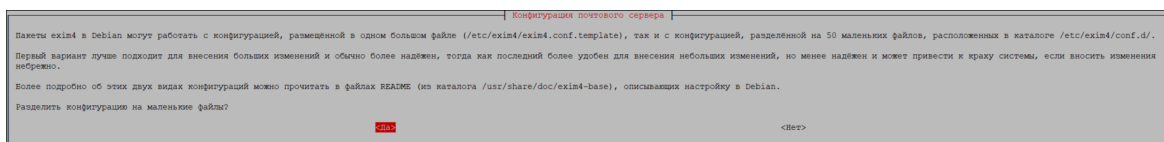


Рис. 7.10. Выбор разбиения конфигурации на маленькие файлы

14. Обновить конфигурацию **Exim4**, выполнив команду:

**~\$ sudo update-exim4.conf**

15. Перезапустить агент **Exim4**, выполнив команду:

~\$ sudo /etc/init.d/exim4 restart

## 7.2. Настройка профиля отправки

Для настройки профиля отправки необходимо выполнить следующие действия:

1. В GUI KEO DLP перейти в раздел **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Отправка** и в секции **Наборы параметров отправки сообщений** нажать **Добавить**.
2. Задать значения следующих параметров:
  - **Название набора параметров** – ввести название отвечающее реалиям набора, например: **Exim4**.
  - **Метод доставки** – **sendmail**.
  - **Путь к программе sendmail** – **/usr/sbin/exim4**.
3. Нажать **Сохранить, Применить**.
4. Перейти в раздел **Политика > Шаблоны и профили** и создать новый профиль отправки для **exim4**:

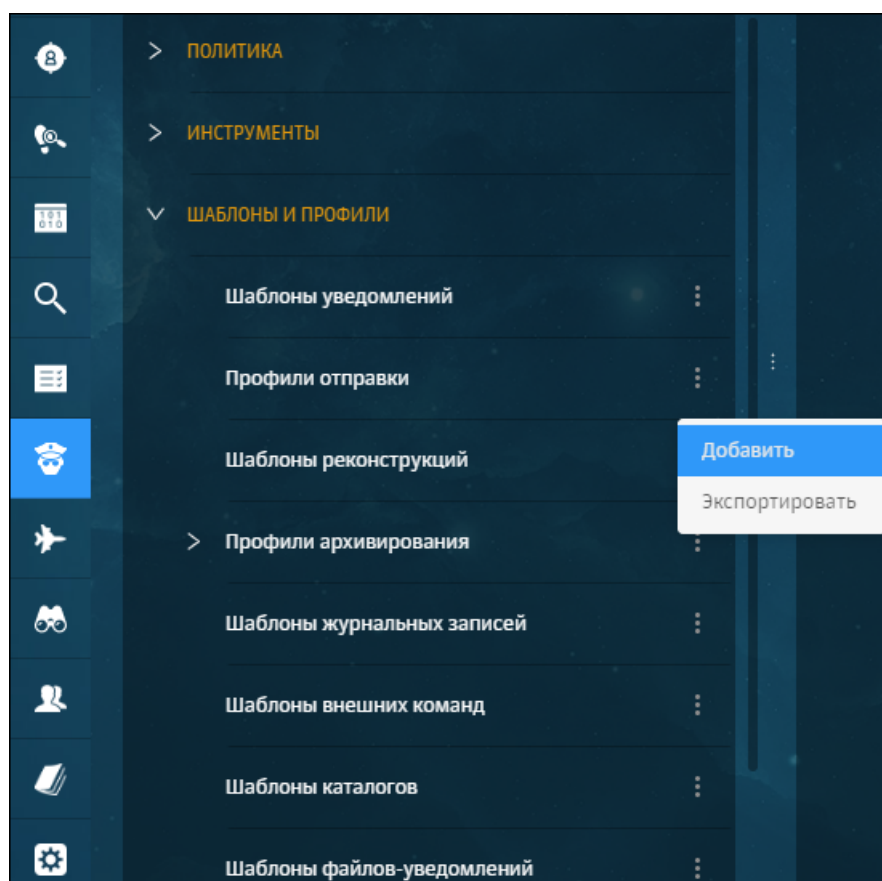


Рис. 7.11. Добавление профиля отправки

5. Ввести название профиля отправки, нажать **Сохранить** и задать значения следующих параметров:

- **Параметры отправки** – ввести название, выбранное для набора параметров в шаге 2.
- **Количество попыток отправки** – 1.
- **Действие по исчерпанию попыток** – Переместить сообщение в егг-спул.

6. Нажать **Сохранить, Применить политику**.

### 7.3. Создание правила политики фильтрации

После создания профиля отправки и настройки программы **Exim4** следует настроить головной набор правил политики фильтрации. Для этого необходимо выполнить следующие действия:

1. В GUI KEO DLP перейти в раздел **Политика > Политика > Наборы правил** и выбрать головной набор правил (отмеченный звездочкой).

#### Примечание

*Если головным является набор правил **Архивировать все сообщения** – следует создать новый набор правил и назначить его головным, поскольку набор правил **Архивировать все сообщения** является системным и не может быть изменен.*

2. Добавить правило следующего содержания:

- **Если** – Все сообщения
- **то** – Отправить
- **Профиль отправки** – указать созданный ранее профиль отправки.
- **Выполнить**

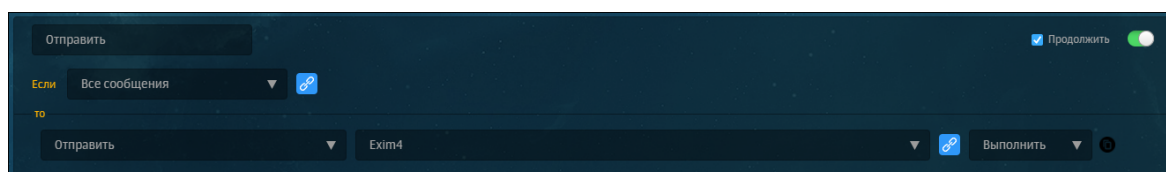


Рис. 7.12. Правило фильтрации для активного режима

3. Нажать **Сохранить, Применить политику**.

### 7.4. Настройка балансировщика

Кластер KEO DLP может использовать несколько серверов фильтрации. В этом случае для распределения трафика по серверам используют балансировщик.



---

Балансировщик управляет потоками данных (прозрачно и незаметно для клиентов) и позволяет увеличить производительность KEO DLP за счет параллельной обработки запросов на нескольких узлах кластера. Балансировщик контролирует работоспособность серверов фильтрации и автоматически отключает узлы от процесса обработки запросов в случае их недоступности.

Для настройки балансировщика HAProxy необходимо выполнить на master-узле следующие действия:

1. Перейти в раздел GUI **Система > Узлы и роли** и назначить одному из узлов роль **Балансировщик**.
2. Нажать кнопку **Применить**.
3. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Прием сообщений** и в секции **Балансировка трафика** нажать **Добавить**.
4. Задать значения следующих параметров:
  - **Название конфигурации балансировки** – ввести произвольное название.
  - **Порт для внешних соединений** – порт, на котором сервис балансировки трафика ожидает соединения (по умолчанию 1010).
  - **Время ожидания запроса от клиента (с)** – время ожидания запроса от клиента, выраженное в секундах (по умолчанию 10).

#### Примечание

*В качестве клиента выступают внешние системы, например SMTP/HTTP/ICAP-серверы.*

- **Время ожидания запроса от сервера (с)** – время ожидания запроса от серверов фильтрации, которые задаются в параметре **Узлы для балансировки**. Выражено в секундах (по умолчанию 10).
  - **Максимальное количество соединений** – максимальное количество соединений, которое принимает балансировщик от клиента (по умолчанию 1000).
  - **Метод балансировки** – алгоритм балансировки трафика (по умолчанию **roundrobin**).

При значении **roundrobin** нагрузка будет распределена равномерно в соответствии с весом каждого сервера фильтрации KEO DLP, если таковой указан ниже. При значении **leastconn** запросы будут передаваться серверу с наименьшим количеством подключений. При значении **source** сервер для соединения назначается на основании хэша IP-адреса отправителя запроса и весов серверов.
5. При необходимости, установить параметр **Узлы для балансировки** в значение **Указать вручную** и задать значения следующих параметров:
    - **Тип балансировки** – протокол, по которому распределяется нагрузка между узлами.

- **Узлы** – добавить одну или несколько записей резервных узлов, предназначенных для балансировки. Запросы от внешних систем будут перенаправляться на эти узлы при недоступности серверов фильтрации KEO DLP.

Запись резервного узла имеет следующие параметры:

- **Сетевой адрес** – FQDN или IP-адрес резервного узла.
- **Номер порта** – номер порта, на котором резервный узел будет ожидать соединения.
- **Вес балансировки** – коэффициент, помогающий балансировщику распределять нагрузку между серверами фильтрации. Узел с большим весом будет получать большее число запросов.

Пример: сервер с весовым коэффициентом 2 будет получать в 2 раза больше запросов, чем сервер с весом, равным 1.

Пример 2: имеется три сервера фильтрации А, В и С. Сервера А и В имеют вес, равный 1, а сервер С имеет весовой коэффициент 2. При недоступности сервера С нагрузка распределится равномерно между серверами А и В. При восстановлении своей работоспособности сервер С будет получать в 2 раза больше запросов, чем серверы А и В (каждый по отдельности).

6. Нажать **Сохранить** и **Применить**.

## 7.5. Настройка отправки сообщений при ошибках фильтрации

В KEO DLP можно настроить отправку сообщений адресатам при ошибках фильтрации. Например, сообщения, которые не успели распаковаться или обработаться политикой за отведенное время, будут доставлены получателям. В этом случае необходимо:

1. Создать профиль отправки.
2. Настроить отправку уведомлений системному администратору о состоянии ресурсов системы.
3. Настроить политику фильтрации.
4. Активировать отправку сообщений адресатам.

### 7.5.1. Настройка профиля отправки

Для настройки профиля отправки следует выполнить действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Отправка**.
2. В секции **Сервис отправки сообщений** задать значение параметра **Таймаут на сетевое взаимодействие при использовании SMTP** равным 600.
3. В секции **Наборы параметров отправки сообщений** нажать кнопку **Добавить**.
4. Задать значения следующих параметров:

- 
- **Название набора параметров** – ввести произвольное название.
  - **Метод доставки** – smtp.
5. В строке **Соединения SMTP** нажать кнопку **Добавить** и в появившемся поле задать значения следующих параметров:
- **Протокол SMTP сервера** – SMTP.
  - **SMTP сервер** – ввести FQDN или IP-адрес SMTP-сервера, на который будет выполнена отправка.
  - **SMTP порт** – 25.
6. Нажать **Сохранить, Применить**.
7. Перейти в раздел **Политика > Шаблоны и профили** и создать новый профиль отправки по протоколу SMTP.
8. Ввести название профиля отправки, нажать **Сохранить** и задать значения следующих параметров:
- **Параметры отправки** – ввести название, выбранное для набора параметров на шаге [4](#).
  - **Количество попыток отправки** – 1.
  - **Действие по исчерпанию попыток** – Переместить сообщение в err-спул.
9. Нажать **Сохранить, Применить политику**.

### 7.5.2. Настройка отправки уведомлений о состоянии ресурсов системы

После создания профиля отправки следует настроить отправки уведомлений системному администратору о состоянии ресурсов системы. Для этого следует выполнить действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование > Мониторинг**.
2. В секции **Сервер мониторинга** раскрыть список **Настройки оповещения**.
3. Раскрыть список **Адрес/порт SMTP-сервера** и задать значения следующих параметров:
  - **Сетевой адрес** – имя SMTP-сервера, заданное на шаге [4](#) раздела [7.5.1](#).
  - **Номер порта** – 1025.
4. Указать адреса получателей уведомлений в значениях параметров:
  - **Адреса для отправки уведомлений о проблемах чрезвычайной критичности**.
  - **Адреса для отправки уведомлений о проблемах высокой и средней критичности**.
  - **Адреса для отправки уведомлений о проблемах низкой критичности**.

---

5. Нажать **Сохранить, Применить**.

### 7.5.3. Создание правила политики фильтрации

После создания профиля отправки и настройки отправки уведомлений о состоянии ресурсов следует настроить головной набор правил политики фильтрации по инструкции в разделе [7.3](#).

### 7.5.4. Активация отправки сообщений адресатам

После настройки головного правила политики фильтрации следует активировать отправку сообщений адресатам при ошибках фильтрации. Для этого необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Политика > Политика > Наборы правил > Обработка ошибок**.
2. Отредактировать правило **Ошибки или таймаут обработки** таким образом, чтобы при срабатывании условия **Ошибки или таймаут обработки** выполнялось действие **Отправить** с использованием ранее настроенного профиля отправки.

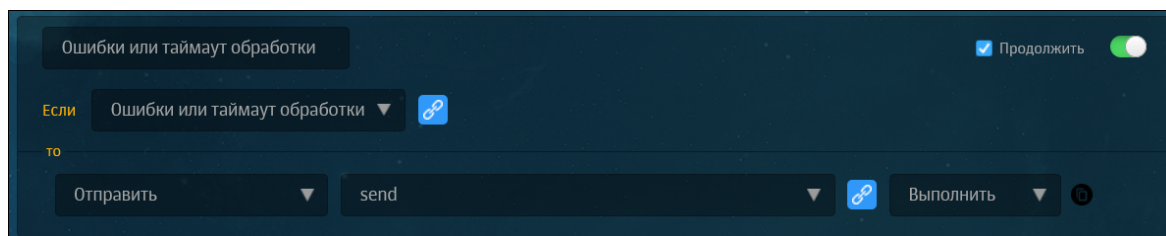


Рис. 7.13. Правило отправки при ошибках

3. Нажать **Сохранить, Применить политику**.

---

## 8. Первичная настройка KEO DLP

### 8.1. Настройка контроля целостности

Для контроля целостности используется скрипт **check\_dozor**, который при вызове пересчитывает контрольные суммы неизменяемых исполняемых файлов и сравнивает их с контрольными суммами, хранящимися в БД пакетного менеджера ОС. При несоответствии значений контрольных сумм хотя бы для одного проверяемого файла скрипт отправляет почтовое сообщение с результатами проверки по адресам, заданным в конфигурации. Сообщение с результатами проверки содержит следующую информацию:

- Сетевое имя узла, на котором было обнаружено несоответствие контрольных сумм.
- Данные об ОС.
- Дата и время выполнения проверки.
- Сводная таблица с результатами пересчета контрольных сумм по всем установочным пакетам KEO DLP.

Сообщение пересылается с помощью программы **Exim4**. Для этого на узлах KEO DLP должен быть установлен и настроен агент пересылки сообщений **Exim4**.

Для получения уведомлений о результатах регулярного контроля целостности необходимо выполнить следующие действия:

1. Перейти в GUI и открыть раздел **Система > Конфигурация > Основные настройки > Работа системы**, секцию настроек **Общие настройки системы**, развернуть список **Адреса получателей в системных сообщениях** и задать значения параметров:
  - **Имя почтового ящика** – задать имя почтового ящика (без домена), на который будет отправлено уведомление в случае аварийной остановки системы при несопадении контрольных сумм в результате проверки целостности.
  - **Имя почтового домена** – задать домен, в котором находится почтовый ящик, заданный в предыдущем параметре.
2. При необходимости, создать дополнительные записи с помощью кнопок **Копировать** или **Добавить** и повторить действия предыдущего шага.
3. Нажать **Сохранить, Применить**.

Механизм контроля целостности по умолчанию включен. Для отключения механизма контроля целостности необходимо создать файл **/opt/dozor/SKIP\_CHECK\_MODE**. Пока этот файл существует – никакие проверки целостности не будут выполняться ни в автоматическом режиме, ни в ручном.

### 8.2. Назначение ролей узлам

Набор функций, выполняемых каждым узлом кластера KEO DLP, определяется списком назначенных ему ролей. Каждая роль отражает конкретную прикладную задачу: прием и обработка почтовых сообщений, поиск по архиву сообщений, индексация событий и инцидентов ИБ, и другие. Для решения таких задач используются процессы KEO DLP. Список процессов, запускаемых на узле KEO DLP, определяется набором ролей, назна-

ченных этому узлу. Подробная информация о составе ролей приведена в [Приложение D. Описание ролей и сервисов](#).

### 8.2.1. Назначение ролей с помощью GUI

Для назначения ролей узлам используется вкладка **Система > Узлы и роли**, содержащая информацию о состоянии и ролях всех узлов кластера KEO DLP. Для назначения узлу какой-либо роли следует щелкнуть мышью в поле **Роли узла** и выбрать в раскрывающемся списке одну или несколько ролей для узла, а затем щелкнуть мышью на любой области за пределами списка. Для снятия с узла какой-либо роли следует нажать на крестик на плашке с названием этой роли.

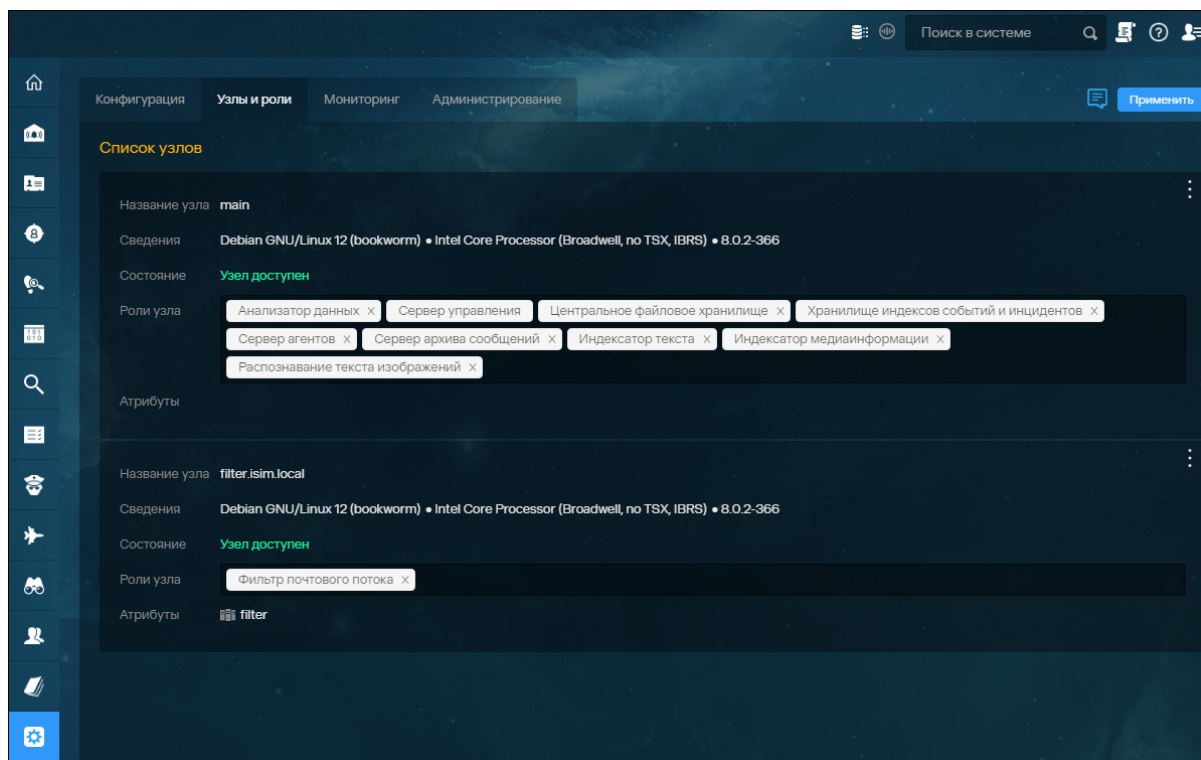


Рис. 8.1. Назначение ролей

Для отображения списка узлов используется пагинация, которая располагается в нижней части интерфейса. На одной странице может быть одновременно отображено не более пяти узлов (как при использовании модуля **Мультидозор**, так и без него).

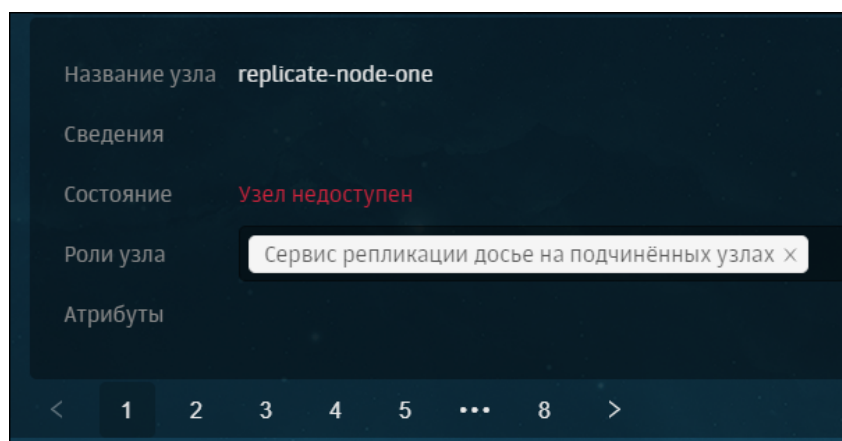


Рис. 8.2. Разбиение на страницы

Если в системе имеется более пяти узлов, в правой верхней части экрана отображается поле **Поиск по узлам**.

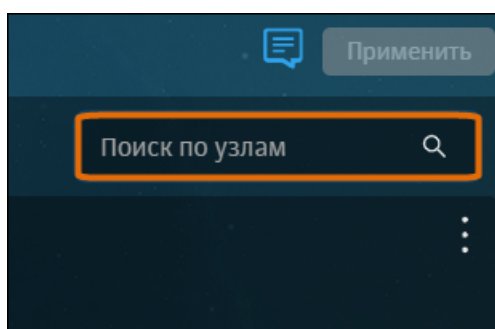


Рис. 8.3. Поиск узлов

Минимальный набор ролей для нормального функционирования KEO DLP:

- **Сервер управления** – роль будет назначена одному из узлов в процессе установки.
- **Хранилище индексов событий и инцидентов** – роль необходима для хранения индексов событий и инцидентов ИБ. Необходимо назначить эту роль master-узлу.
- **Индексатор текста** – роль необходима для индексирования сообщений в архиве и хранения индексов. При назначении этой роли узлам KEO DLP следует руководствоваться информацией из раздела [8.8](#).
- **Фильтр почтового потока** – роль необходима для фильтрации и отправки сообщений согласно заданной политике. Следует назначать эту роль высокопроизводительным серверам, по возможности – двум и более с использованием балансировщика нагрузки.
- **Мониторинг локального почтового шлюза** – роль необходима для того, чтобы система мониторинга могла отслеживать состояние сервиса почтового шлюза на тех узлах, где его функционирование необходимо. В большинстве случаев такие узлы имеют роли **Сервер управления**, **Балансировщик** и **Фильтр почтового потока** (особенно при реализации активного режима работы KEO DLP).

- **Центральное файловое хранилище** – роль необходима для хранения тел и текстовых частей сообщений архива, снимков экрана и вложений, отображаемых в большой карточке персоны.
- **Анализатор данных** – роль необходима для работы сервисов цифровых отпечатков, идентификаторов и извлечения текстов и метаданных из вложений.

### 8.2.2. Назначение ролей с помощью CLI

Для получения списка ролей и доступных узлов необходимо выполнить следующую команду:

```
~$ sudo /opt/dozor/bin/set-role
```

На экран будет выведена информация следующего вида:

Available roles:

- api-gateway
- master
- storage
  
- god-server
- cassandra
- analyzer
- traffic-agent
- abook-slave
- agent-server
- fsng-client
- fsng-storage
- text-indexer
- historic-text-indexer
- incident-indexer
- historic-incident-indexer
- local-incident-daemon
- opensearch
- smtp-filter
- action-server
- action-server-master
- category-server
- im-crawler
- crawler-x
- crawler-x-master
- uba-server
- time-control
- balancer
- software-center
- license-server
- indexer-only
- historic-indexer-only
- webserver-local
- mail-gw
- media-processor

Available nodes:

- 0f676af8-e25d-481e-a193-2aaecb2a2eed filter
- main main



---

Для назначения узлу какой-либо роли или списка ролей следует выполнить команду следующего вида:

**~\$ sudo /opt/dozor/bin/set-role <role-list> <name>**

где **<role-list>** – роли, перечисленные через пробел, а **<name>** – имя узла KEO DLP. Имена узлов перечислены в списке **Available nodes** при выполнении команды **set-role** (последнее значение в строке).

#### **Внимание!**

*При выполнении команды на master-узле следует убедиться, что среди назначаемых ролей есть **master**, а в качестве имени узла следует указать **main**.*

Для получения списка ролей, назначенных узлу, необходимо выполнить следующую команду:

**~\$ sudo /opt/dozor/bin/get-role**

Скрипт **get-role** имеет следующий формат:

**get-role [<node-name> | total | list]**

где **<node-name>** – имя узла, список ролей которого требуется получить. Команда **get-role** без аргументов выводит на экран список ролей текущего узла.

Команда

**get-role total**

выводит на экран списки ролей всех узлов кластера.

Команда

**get-role list**

выводит на экран список доступных ролей.

## **8.3. Создание и настройка БД архива PostgreSQL**

В KEO DLP может быть создано сколь угодно много БД архива сообщений (под управлением СУБД PostgreSQL). Для создания БД архива сообщений необходимо сначала настроить схему соединения с БД (раздел [8.3.1](#)), а затем создать схему БД (раздел [8.3.2](#)).

### **8.3.1. Настройка схемы соединения с БД**

Для настройки схемы соединения с БД PostgreSQL необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Доступ к данным** и в секции **Схемы соединений с БД** добавить новую запись с помощью кнопки **Добавить**.
2. Установить следующие значения параметров для новой записи:
  - **Имя схемы соединения с базой данных** – указать значение вида **db-conn-<n>**, где **<n>** – значение параметра **id** для этой записи (например, **db-conn-4**).

- **Включено** – установить флажок.
- **Настройки использования соединения с БД:**
  - **Использовать БД для поиска по архиву, Использовать БД для архивирования сообщений** – установить флажки.
  - **Использовать БД для архивирования по умолчанию** – установить флажок. Подробнее об использовании этого флажка см. документ *Руководство пользователя*, раздел *Профили архивирования*.
- **Тип базы данных** – оставить значение **pgsql**.
- **Настройки соединения с базой:**
  - **Сетевое имя сервера базы данных** – указать FQDN или IP-адрес узла, на котором предполагается размещение базы данных архива.
  - **Сетевой порт сервера базы данных** – указать порт, на котором БД архива будет ожидать соединения. Порт не должен быть занят никаким другим сервисом на данном узле (см. раздел [4.4](#)).
  - **Имя базы данных** – указать имя базы данных. К этому значению предъявляются те же требования, что и к именованию каталогов в ОС. Рекомендуется выбирать имя, отражающее назначение создаваемой БД (например, **archive-01**).
  - **Пользователь базы данных** – указать имя **dozor**.
  - **Пароль пользователя базы данных** – рекомендуется задать уникальный пароль для доступа к БД. Если оставить значение по умолчанию – доступ к БД будет осуществляться без пароля.
- **Использование секционирования** – установить значение **используется**, если требуется секционирование БД, и задать подчиненные параметры по усмотрению (описание параметров и подробная информация о секционировании в БД PostgreSQL приведены в документе *Руководство системного администратора*, раздел *Секционирование БД PostgreSQL*).

3. Нажать **Сохранить** и **Применить**.

### 8.3.2. Создание схемы БД

После настройки соединения необходимо создать схему БД, выполнив следующие действия:

1. Подключиться по протоколу SSH к узлу, указанному в параметре **Сетевое имя сервера базы данных** при настройке схемы соединения с БД.
2. Переключиться на работу от имени пользователя **dozor**, запустить интерпретатор команд shell и перейти в каталог **/opt/dozor/smap/schema/pgsql/**, выполнив следующие команды:

```
~$ sudo su - dozor
```

```
$ /opt/dozor/bin/shell
```

---

```
$ cd /opt/dozor/smap/schema/pgsql/
```

3. Создать схему БД с помощью скрипта **create-database.sh**, выполнив команду:

```
$ ./create-database.sh <path> -con <conn>
```

где **<path>** – каталог, в котором создается БД (например, **/data/base/smap-archive/**), а **<conn>** – имя схемы соединения с БД, определенное в настройках соединения (например, **db-conn-4**).

4. Переключиться на работу от имени пользователя **root** и запустить командную оболочку, выполнив команды:

```
$ exit
```

```
$ su - root
```

```
~$ /opt/dozor/bin/shell
```

5. Перейти в каталог **<path>** (**/data/base/smap-archive/** в данном примере) и отредактировать конфигурационный файл **pg\_hba.conf** таким образом, чтобы он содержал строки, определяющие доступ к узлу БД с других узлов кластера КЕО DLP. Пример таких строк в случае использования пароля для доступа к БД:

```
host all all <master-host> scram-sha-256
host all all <filter-host> scram-sha-256
```

где **<master-host>** – IP-адрес или FQDN master-узла, **<filter-host>** – IP-адрес или FQDN дополнительного узла фильтрации, например:

```
host all all master.dozor.local scram-sha-256
host all all filter1.dozor.local scram-sha-256
```

При использовании IP-адресов необходимо также использовать маску подсети, например:

```
host all all 192.168.100.2/32 scram-sha-256
host all all 192.168.100.3/32 scram-sha-256
```

Пример строк в случае отказа от использования пароля для доступа к БД (не рекомендуется):

```
host all all <master-host> trust
host all all <filter-host> trust
```

где **<master-host>** – IP-адрес или FQDN master-узла, **<filter-host>** – IP-адрес или FQDN дополнительного узла фильтрации, например:

```
host all all master.dozor.local trust
host all all filter1.dozor.local trust
```

При использовании IP-адресов необходимо также использовать маску подсети, например:

```
host all all 192.168.100.2/32 trust
host all all 192.168.100.3/32 trust
```

- 
- В этом же каталоге открыть конфигурационный файл **postgresql.conf** и найти строку с параметром **lc\_messages**. Строка должна выглядеть следующим образом:

```
lc_messages = 'C'
```

Если параметр имеет любое другое значение, следует заменить его на **'C'** (заглавная латинская буква C, заключенная в прямые апострофы). Сохранить и закрыть файл.

- После создания схемы БД PostgreSQL в каталоге **/opt/dozor/smap/schema/pgsql** создается скрипт **dozor-postgresql.service**, в котором записывается пользователь, от имени которого создана БД, а также каталог и порт, на котором работает БД. Необходимо скопировать скрипт **dozor-postgresql.service** в каталог **/etc/systemd/system/** и переименовать его, например в **archive.service**:

```
~$ sudo cp /opt/dozor/smap/schema/pgsql/dozor-postgresql.service  
/etc/systemd/system/archive.service
```

- От имени пользователя **root** выполнить следующие команды:

```
~$ sudo systemctl daemon-reload  
~$ sudo systemctl enable archive.service  
~$ sudo systemctl start archive.service
```

- Перезагрузить процессы KEO DLP, выполнив команду:

```
~$ sudo dsctl restart
```

Если при настройке соединения с БД для параметра **Использование секционирования** было задано значение **используется**, то необходимо настроить автоматическое создание секций с помощью планировщика **cron**. Для этого необходимо выполнить следующие действия:

- На master-узле открыть расписание планировщика (при запросе системы выбрать редактор **vim**):

```
~$ sudo crontab -u dozor -e
```

- Нажать клавишу **i** и добавить в расписание после комментария **### End: schedule of crontab entry ###** следующую строку:

```
0 0 * * * bash /opt/dozor/smap/schema/pgsql/shell/part-control -con <conn> > /dev/null 2>&1
```

где **<conn>** – имя схемы соединения с БД, определенное в настройках соединения (например, **db-conn-4**).

- Нажать клавишу **Esc**, ввести **:wq** и нажать **Enter**.

## 8.4. Настройка БД для хранения событий и инцидентов ИБ

Для хранения событий и инцидентов ИБ KEO DLP использует БД PostgreSQL. Для настройки БД событий и инцидентов ИБ необходимо выполнить следующие действия:

- Убедиться, что хотя бы одному узлу назначена роль **Хранилище индексов событий и инцидентов** (см. раздел [8.2](#)).

---

2. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > События и инциденты** и в секции **Настройки подключений к хранилищам инцидентов (PostgreSQL)** задать следующие значения параметров:

- **Имя схемы соединения с базой данных** – указать произвольное имя схемы соединения с создаваемой БД.
- **Подкластер** – оставить значение **Нет**, если БД создается для общих ресурсов, или установить значение **Да**, если БД создается для какого-либо подкластера. Во втором случае появляется параметр, в котором следует указать этот подкластер.

3. Раскрыть группу параметров **Настройки соединения с базой** и задать следующие значения параметров:

- **Сетевое имя сервера базы данных** – указать FQDN или IP-адрес узла, на котором предполагается размещение БД.
- **Сетевой порт сервера базы данных** – указать порт, на котором БД будет ожидать соединения. Порт не должен быть занят никаким другим сервисом на данном узле (см. раздел [4.4](#)).
- **Имя базы данных** – указать имя БД. К этому значению предъявляются те же требования, что и к именованию каталогов в ОС. Рекомендуется выбирать имя, отражающее назначение создаваемой БД (например, **dozor-event**).
- **Пользователь базы данных** – указать имя **dozor**.
- **Пароль пользователя базы данных** – задать пароль пользователя **dozor** для подключения к БД.

4. Нажать **Сохранить** и **Применить**.

5. Перейти в CLI на узле, на котором предполагается размещение БД событий и инцидентов (или на любом узле КЕО DLP, если БД предполагается разместить на внешнем сервере), переключиться на работу от имени пользователя **dozor**, выполнив команду:

```
~$ sudo su - dozor
```

6. Загрузить командную оболочку, выполнив команду:

```
$ /opt/dozor/bin/shell
```

7. Создать схему БД с помощью скрипта **create-database.sh**, выполнив команду:

```
$ /opt/dozor/smap/schema/pgsql/create-database.sh <db_path> <db_port> <db_name>  
<db_pass> <db_host> --empty-db
```

где:

- **<db\_path>** – путь к каталогу БД (например, **/data/base/incident/**).
- **<db\_port>** – номер порта, заданный в конфигурации (например, 5436).
- **<db\_name>** – имя БД, заданное в конфигурации (например, **dozor-event**).
- **<db\_pass>** – пароль для доступа к БД, заданный в конфигурации.

- **<db\_host>** – адрес узла для размещения БД, заданный в конфигурации (например, 127.0.0.1 или 10.31.10.12). Можно не указывать, если БД создается на текущем узле.

### Внимание!

Об успешном создании схемы БД свидетельствуют следующие строки в выводе команды:

```
Creating control script...
Control script "/opt/dozor/smap/schema/pgsql/dozor-postgresql" created.
Copy it to /etc/systemd/system/dozor-postgresql.service
And run: 'systemctl daemon-reload; systemctl enable dozor-postgresql.service;
systemctl start dozor-postgresql.service'
Stop database service ...
```

При наличии сообщений об ошибках в выводе команды следует удалить каталог базы данных (в данном примере – с помощью команды **\$ rm -rf /data/base/incident/**), и убедиться в правильности выполнения предыдущих шагов.

8. Завершить работу интерпретатора shell, выполнив команду:

```
$ exit
```

9. Настроить доступ к БД с других узлов кластера: перейти в каталог БД (в данном примере – **/data/base/incident**) и отредактировать конфигурационный файл **pg\_hba.conf** таким образом, чтобы он содержал строку следующего вида:

```
host all all <IP>/<mask> scram-sha-256
```

где **<IP>** – IP-адрес подсети, с узлов которой БД инцидентов будет принимать соединения, а **<mask>** – маска этой подсети, например:

```
host all all 10.31.0.0/16 scram-sha-256
```

10. Настроить БД на прослушивание сети на внешнем интерфейсе. Если при создании БД был указан внешний IP-адрес – то БД уже настроена. Если при создании БД был указан локальный адрес (или не указан вовсе) – в том же каталоге отредактировать конфигурационный файл **postgresql.conf** так, чтобы он содержал строку следующего вида:

```
listen_addresses = '<IP-interface>'
```

где **<IP-interface>** – IP-адрес сетевого интерфейса, который БД инцидентов будет использовать для приема соединений, например:

```
listen_addresses = '10.31.10.12'
```

11. Завершить работу от имени пользователя **dozor**, выполнив команду:

```
$ exit
```

12. После создания схемы БД PostgreSQL в каталоге **/opt/dozor/smap/schema/pgsql** создается скрипт **dozor-postgresql.service**, в котором записывается пользователь, от имени которого создана БД, а также каталог и порт, на котором работает БД. Необхо-

---

димо скопировать скрипт **dozor-postgresql.service** в каталог **/etc/systemd/system/** и переименовать его, например, в **event.service**:

```
~$ sudo cp /opt/dozor/smap/schema/pgsql/dozor-postgresql.service  
/etc/systemd/system/event.service
```

13. От имени пользователя **root** выполнить следующие команды:

```
~$ sudo systemctl daemon-reload  
~$ sudo systemctl enable event.service  
~$ sudo systemctl start event.service
```

14. Перезапустить сервис индексатора инцидентов, выполнив следующую команду:

```
~$ sudo dsctl restart incident-daemon
```

После этого БД событий и инцидентов должна начать свою работу. Чтобы в этом убедиться, необходимо открыть раздел **Система > Конфигурация > Расширенные настройки > События и инциденты** и в секции **Настройки подключений к хранилищам инцидентов (PostgreSQL)** нажать кнопку **Проверить**.

## 8.5. Настройка сервера хранения медиаинформации

Сервер хранения медиаинформации (далее – медиасервер) предназначен для хранения метаданных изображений (в том числе снимков экрана), звукозаписей и видеозаписей, присылаемых агентами. Письма, содержащие медиаинформацию от агентов, не обрабатываются фильтром почтового потока. После их обработки сервером агентов медиаинформация из таких писем сохраняется в ФХ, а метаданные – в заданной существующей БД PostgreSQL, где медиасервер создает отдельное табличное пространство с секционированием. Медиасервер самостоятельно создает новые секции и удаляет старые по истечении заданного срока хранения.

Для корректного отображения медиаинформации в интерфейсе КЕО DLP следует согласовать ротацию метаданных с ротацией медиаинформации. Для этого следует установить одинаковые значения для связанных параметров:

- снимки экрана:
  - Раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**, секция **Хранение медиаинформации**, параметр **Срок хранения снимков (д)**.
  - Раздел GUI **Система > Конфигурация > Основные настройки > Доступ к данным**, секция **Настройки файлового хранилища**, группа параметров **Настройка ротации**, список с параметром **Volume Group – agent-media**, параметр **Время жизни до ротации (д)**.
- аудиозаписи:
  - Раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**, секция **Хранение медиаинформации**, параметр **Срок хранения аудиозаписей (д)**.



- Раздел GUI Система > Конфигурация > Основные настройки > Доступ к данным, секция **Настройки файлового хранилища**, группа параметров **Настройка ротации**, список с параметром **Volume Group – audio**, параметр **Время жизни до ротации (д)**.
- записи экранов:
  - Раздел GUI Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > **Хранение**, секция **Хранение медиаинформации**, параметры **Срок хранения записей экрана (д)** и **Срок хранения списков процессов приложений (д)**.
  - Раздел GUI Система > Конфигурация > Основные настройки > Доступ к данным, секция **Настройки файлового хранилища**, группа параметров **Настройка ротации**, список с параметром **Volume Group – screen-video**, параметр **Время жизни до ротации (д)**.

Для хранения медиаинформации KEO DLP использует БД PostgreSQL. Для настройки БД для хранения медиаинформации необходимо выполнить следующие действия:

1. Перейти в раздел GUI Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > **Хранение** и в секции **Хранение медиаинформации** установить следующие значения параметров:

- **База данных (PostgreSQL) – Специальная БД.**
- **Сетевое имя сервера базы данных** – указать FQDN или IP-адрес узла, на котором предполагается размещение БД, используемой для хранения информации о задачах сервиса **agent-media-server**.
- **Сетевой порт сервера базы данных** – указать порт, на котором БД для хранения медиаинформации будет ожидать соединения. Порт не должен быть занят никаким другим сервисом на данном узле (см. раздел [4.4](#)).
- **Имя базы данных** – указать имя БД. К этому значению предъявляются те же требования, что и к именованию каталогов в ОС. Рекомендуется выбирать имя, отражающее назначение создаваемой БД (например, **dozor-media**).
- **Пользователь базы данных** – указать имя **dozor**.
- **Пароль пользователя базы данных** – задать пароль пользователя **dozor** для подключения к БД для хранения медиаинформации.

2. Нажать **Сохранить** и **Применить**.

3. Перейти в CLI на узле, на котором предполагается размещение БД для хранения медиаинформации (или на любом узле KEO DLP, если БД предполагается разместить на внешнем сервере) и переключиться на работу от имени пользователя **dozor**, выполнив команду:

```
~$ sudo su - dozor
```

4. Запустить командную оболочку, выполнив команду:

```
$ /opt/dozor/bin/shell
```



5. Создать схему БД с помощью скрипта **create-database.sh**, выполнив команду:

```
$ /opt/dozor/smap/schema/pgsql/create-database.sh <db_path> <db_port> <db_name>  
<db_pass> <db_host> --empty-db
```

где:

- **<db\_path>** – путь к каталогу БД (например, **/data/base/media/**).
- **<db\_port>** – номер порта, заданный в конфигурации (например, 5438).
- **<db\_name>** – имя БД, заданное в конфигурации (например, **dozor-media**).
- **<db\_pass>** – пароль для доступа к БД, заданный в конфигурации.
- **<db\_host>** – адрес узла для размещения БД, заданный в конфигурации (например, 127.0.0.1 или 10.31.10.12). Можно не указывать, если БД создается на текущем узле.

### Внимание!

Об успешном создании схемы БД свидетельствуют следующие строки в выводе команды:

```
Creating control script...  
Control script "/opt/dozor/smap/schema/pgsql/dozor-postgresql" created.  
Copy it to /etc/systemd/system/dozor-postgresql.service  
And run: 'systemctl daemon-reload; systemctl enable dozor-postgresql.service;  
systemctl start dozor-postgresql.service'  
Stop database service ...
```

При наличии сообщений об ошибках в выводе команды следует удалить каталог базы данных (в данном примере – с помощью команды **\$ rm -rf /data/base/media/**), и убедиться в правильности выполнения предыдущих шагов.

6. Завершить работу интерпретатора shell, выполнив команду:

```
$ exit
```

7. Настроить доступ к БД с других узлов кластера: перейти в каталог БД (в данном примере – **/data/base/media**) и отредактировать конфигурационный файл **pg\_hba.conf** таким образом, чтобы он содержал строку следующего вида:

```
host all all <IP>/<mask> scram-sha-256
```

где **<IP>** – IP-адрес подсети, с узлов которой БД для хранения медиаинформации будет принимать соединения, а **<mask>** – маска этой подсети, например:

```
host all all 10.31.0.0/16 scram-sha-256
```

8. Настроить БД на прослушивание сети на внешнем интерфейсе. Если при создании БД был указан внешний IP-адрес – то БД уже настроена. Если при создании БД был указан локальный адрес (или не указан вовсе) – в том же каталоге отредактировать конфигурационный файл **postgresql.conf** так, чтобы он содержал строку следующего вида:

```
listen_addresses = '<IP-interface>'
```

где **<IP-interface>** – IP-адрес сетевого интерфейса, который БД для хранения медиаинформации будет использовать для приема соединений, например:

```
listen_addresses = '10.31.10.12'
```

9. Завершить работу от имени пользователя **dozor**, выполнив команду:

```
$ exit
```

10. После создания схемы БД PostgreSQL в каталоге **/opt/dozor/smap/schema/pgsql** создается скрипт **dozor-postgresql.service**, в котором записывается пользователь, от имени которого создана БД, а также каталог и порт, на котором работает БД. Необходимо скопировать скрипт **dozor-postgresql.service** в каталог **/etc/systemd/system/** и переименовать его, например в **media.service**:

```
~$ sudo cp /opt/dozor/smap/schema/pgsql/dozor-postgresql.service  
/etc/systemd/system/media.service
```

11. От имени пользователя **root** выполнить следующие команды:

```
~$ sudo systemctl daemon-reload
```

```
~$ sudo systemctl enable media.service
```

```
~$ sudo systemctl start media.service
```

12. Перезапустить сервис хранения медиаинформации, выполнив следующую команду:

```
~$ sudo dsctl restart agent-media-server
```

После этого БД для хранения медиаинформации должна начать свою работу. Чтобы в этом убедиться, необходимо открыть раздел **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** и в секции **Хранение медиаинформации** нажать кнопку **Проверить**.

## 8.6. Настройка синхронизации Досье

### 8.6.1. Синхронизация с FreeIPA

Для настройки синхронизации данных Досье с существующей структурой каталогов 389 Directory Server необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Взаимодействие**, добавить новый источник (либо отредактировать шаблон **389 Directory Server Example**) в секции **Источники данных досье** и задать значения следующих параметров:
  - **Название источника** – указать произвольное название источника данных 389 Directory Server. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
  - **Синхронизация включена** – установить флажок.

- 
- **Параметры доступа к источнику данных – ldap.**
  - **DN пользователя** – DN учетной записи с правами чтения каталога 389 Directory Server.
  - **Пароль пользователя** – пароль учетной записи, указанной в предыдущем параметре. Пароль не должен содержать кириллицы, символов «\», «/», «{», «}», «[», «]», «(», «)» и пустых символов.
  - **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например – **ldap://ldap.organization.local:389**).
  - **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов AD организации.
  - **Атрибут, содержащий уникальный идентификатор записи (UUID) – nsUniqueId.**
  - **Атрибут, содержащий номер последнего изменения записи – entryUsn.**
  - **Атрибут RootDSE, содержащий идентификатор сервера – netscapemdsuffix.**
  - **Атрибут RootDSE, содержащий номер последнего изменения содержимого – lastusn.**
2. Раскрыть список **Список соответствий атрибутов** и при необходимости добавить и/или исправить соответствия между атрибутами 389 Directory Server и атрибутами досье.
  3. Нажать **Сохранить** и **Применить**.
  4. Выполнить принудительную синхронизацию Досье с источниками, нажав кнопку **Синхронизировать**:

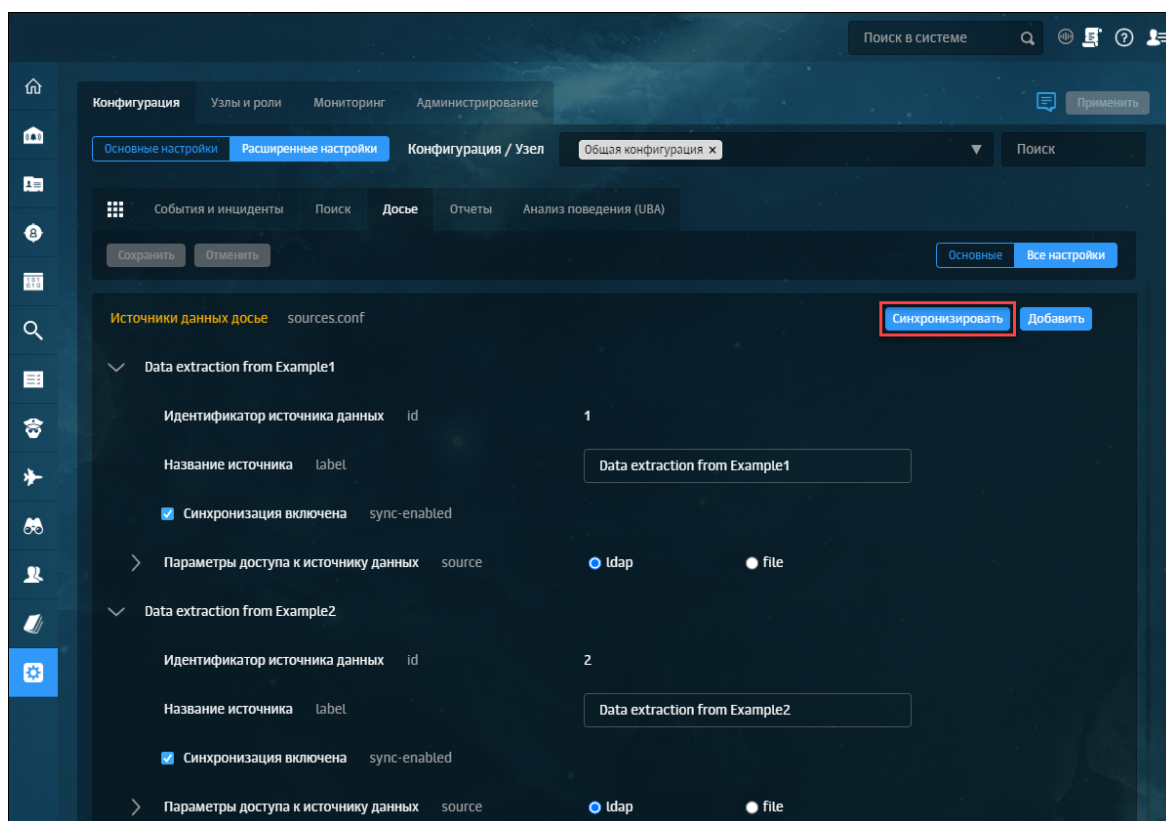


Рис. 8.4. Кнопка принудительной синхронизации Досье

5. Дождаться уведомления об успешности синхронизации.

### 8.6.2. Синхронизация с ALD Pro

KEO DLP имеет возможность синхронизировать данные Досье с ALD Pro версии 1.3.0. Для настройки синхронизации данных Досье с существующей структурой каталогов ALD Pro необходимо выполнить следующие действия:

1. Перейти в раздел GUI Система > Конфигурация > Основные настройки > Взаимодействие, добавить новый источник (либо отредактировать шаблон **ALD Pro**) в секции **Источники данных досье** и задать значения следующих параметров:

- **Название источника** – указать произвольное название источника данных ALD Pro. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
- **Синхронизация включена** – установить флажок.
- **Параметры доступа к источнику данных** – **ldap**.
- **DN пользователя** – DN учетной записи с правами чтения каталога ALD Pro.
- **Пароль пользователя** – пароль учетной записи, указанной в предыдущем параметре. Пароль не должен содержать кириллицы, символов «\», «/», «{», «}», «[», «]», «(», «)» и пустых символов.

- **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например – **ldap://ldap.organization.local:389**).
  - **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов ALD Pro организации.
  - **Атрибут, содержащий уникальный идентификатор записи (UUID)** – **nsUniqueid**.
  - **Атрибут, содержащий номер последнего изменения записи** – **entryUsn**.
  - **Атрибут RootDSE, содержащий идентификатор сервера** – **netscapemdsuffix**.
  - **Атрибут RootDSE, содержащий номер последнего изменения содержимого** – **lastusn**.
2. Раскрыть список **Список соответствий атрибутов** и при необходимости добавить и/или исправить соответствия между атрибутами ALD Pro и атрибутами досье.
  3. Нажать **Сохранить** и **Применить**.
  4. Выполнить принудительную синхронизацию Досье с источниками, нажав кнопку **Синхронизировать**:

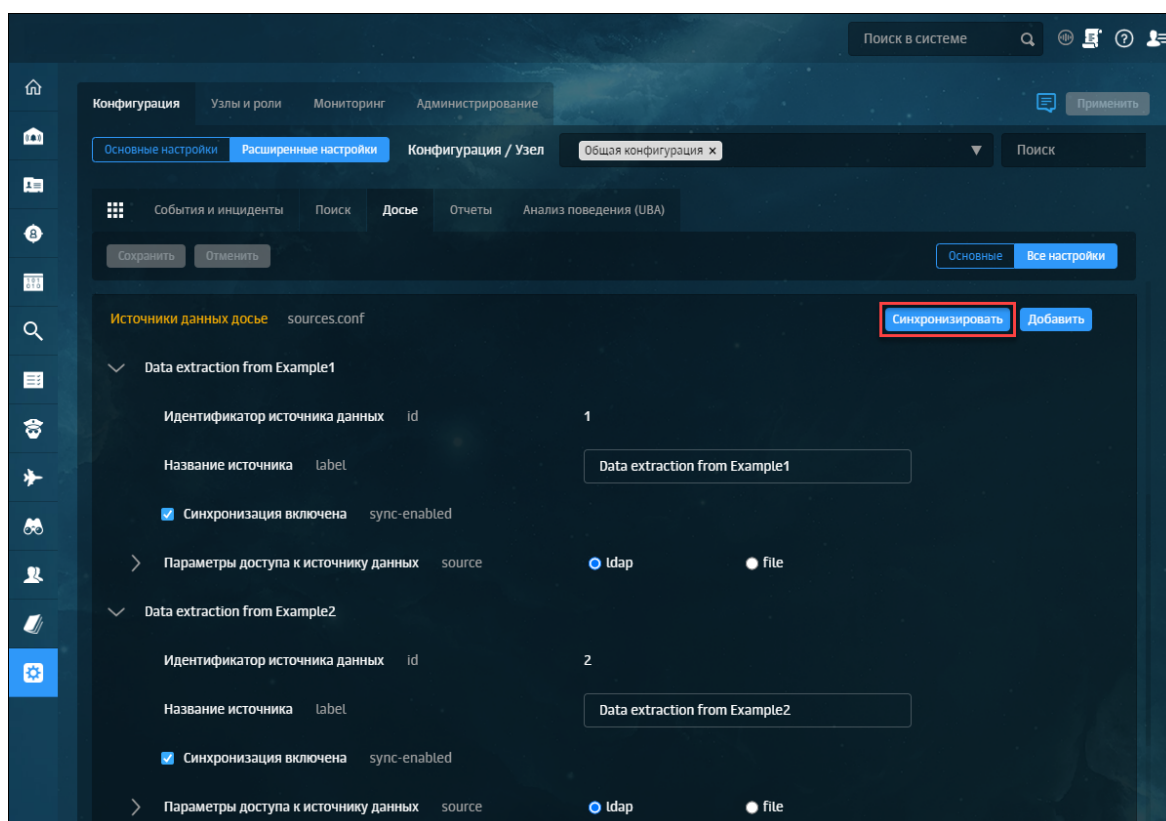


Рис. 8.5. Кнопка принудительной синхронизации Досье

5. Дождаться уведомления об успешности синхронизации.

---

### 8.6.3. Синхронизация со службами каталогов без шифрования

Для настройки синхронизации данных Досье с существующей структурой каталогов Active Directory без использования шифрования необходимо выполнить следующие действия:

1. Перейти в раздел GUI Система > Конфигурация > Основные настройки > **Взаимодействие**, добавить новый источник (либо отредактировать шаблон **AD example**) в секции **Источники данных досье** и задать значения следующих параметров:
  - **Название источника** – указать произвольное название источника данных AD. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
  - **Синхронизация включена** – установить флажок.
  - **Параметры доступа к источнику данных** – **ldap**.
  - **DN пользователя** – имя учетной записи с правами чтения каталога AD. Имя указывается вместе с доменом (например – **admin@organization.local**).
  - **Пароль пользователя** – пароль учетной записи, указанной в предыдущем параметре. Пароль не должен содержать кириллицы, символов «\», «/», «{», «}», «[», «]», «(», «)» и пустых символов.
  - **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например – **ldap://ldap.organization.local:389**).
  - **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов AD организации.
  - **Атрибут, содержащий уникальный идентификатор записи (UUID)** – **objectGuid**.
  - **Атрибут, содержащий номер последнего изменения записи** – **UsnChanged**.
  - **Атрибут RootDSE, содержащий идентификатор сервера** – **dnsHostname**.
  - **Атрибут RootDSE, содержащий номер последнего изменения содержимого** – **highestcommittedusn**.
2. Раскрыть список **Список соответствий атрибутов** и при необходимости добавить и/или исправить соответствия между атрибутами AD и атрибутами досье.
3. Нажать **Сохранить** и **Применить**.
4. Выполнить принудительную синхронизацию Досье с источниками, нажав кнопку **Синхронизировать**:



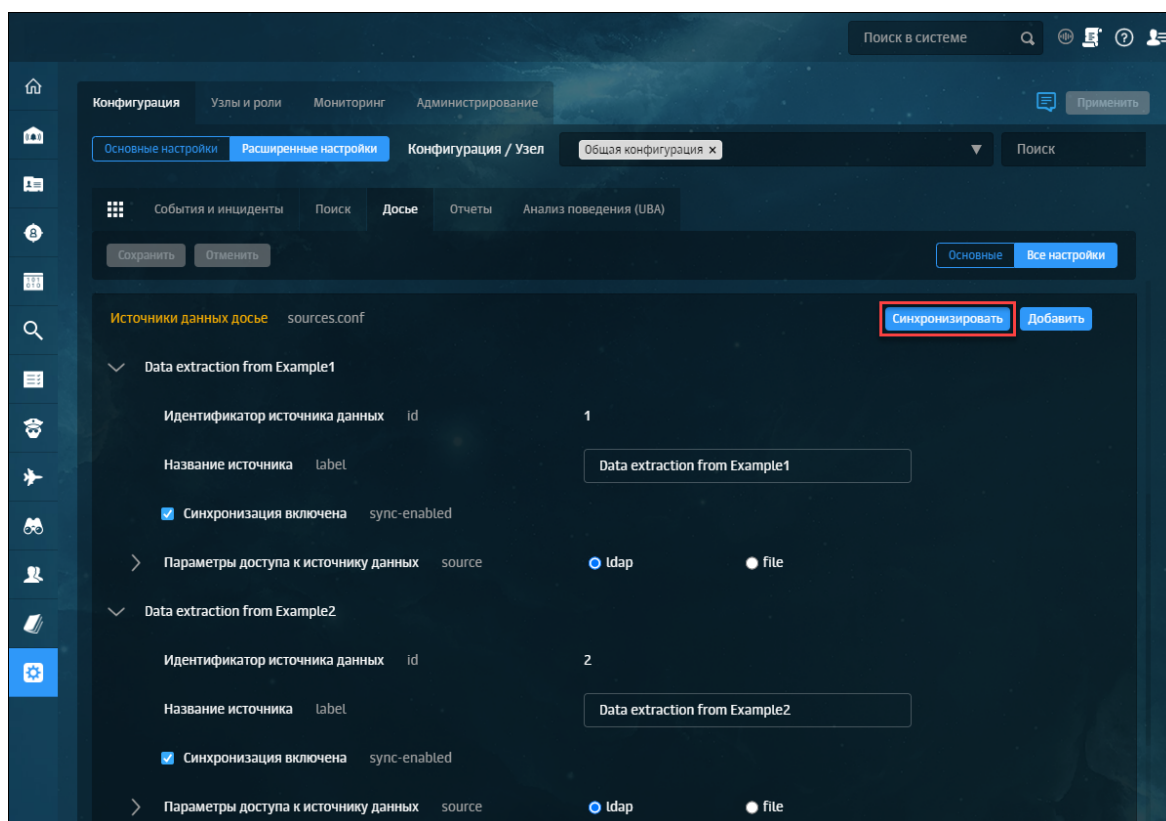


Рис. 8.6. Кнопка принудительной синхронизации Досье

5. Дождаться уведомления об успешности синхронизации.

#### 8.6.4. Синхронизация со службой LDAP с TLS

Установка сертификата организации на контроллере домена позволяет службе LDAP прослушивать и автоматически принимать подключения по протоколу TLS.

Для настройки синхронизации данных Досье с существующей структурой каталогов той или иной службы LDAP с использованием шифрования по протоколу TLS необходимо создать сертификат службы LDAPS, а затем импортировать его в KEO DLP. Поддерживаются версии TLS 1.2 и выше.

Для установки сертификата LDAPS в KEO DLP необходимо выполнить следующие действия (пример для Active Directory):

1. Выгрузить сертификат в формате PEM из LDAP-сервера организации, выполнив команду следующего вида:

```
# openssl s_client -connect <ip_ldap>:636 </dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /var/tmp/<name>.pem
```

где <ip\_ldap> – IP-адрес LDAP-сервера (FQDN недопустим), <name> – произвольное имя файла сертификата.

2. Проверить выгруженный сертификат, выполнив команду следующего вида:

```
# openssl x509 -in /var/tmp/<name>.pem -noout -text
```

- 
3. Создать хранилище и загрузить сертификат в него, выполнив команду следующего вида:

```
# keytool -import -v -trustcacerts -alias "<name_cert>" -file /var/tmp/<name>.pem -  
keystore /opt/dozor/etc/ldap.jks -deststoretype JKS
```

где **<name\_cert>** – имя сертификата (указывается в кавычках), **<name>** – имя файла сертификата. В процессе выполнения команды система предложит ввести новый пароль хранилища и подтвердить его, а также при добавлении сертификата в хранилище будет необходимо ввести **yes**.

4. Перезапустить сервис **monitor-ng**, выполнив команду:

```
# /opt/dozor/bin/dsctl restart monitor-ng
```

5. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Взаимодействие**, добавить новый источник (либо отредактировать имеющийся шаблон) в секции **Источники данных досье** и задать значения следующих параметров:

- **Название источника** – указать произвольное название источника данных AD. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
  - **Параметры доступа к источнику данных – ldap**.
  - **DN пользователя** – имя учетной записи с правами чтения каталога AD. Имя указывается вместе с доменом (например – **admin@organization.local**).
  - **Пароль пользователя** – пароль учетной записи, указанной в предыдущем параметре. Пароль не должен содержать кириллицы, символов «\», «/», «{», «}», «[», «]», «(», «)» и пустых символов.
  - **URL LDAP сервера** – FQDN LDAP-сервера организации с указанием протокола и порта (например – **ldaps://ldap.organization.local:636**). IP-адрес недопустим.
  - **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов AD организации.
6. Раскрыть список **Список соответствий атрибутов** и при необходимости добавить и/или исправить соответствия между атрибутами AD и атрибутами досье.
7. Нажать **Сохранить** и **Применить**.
8. Выполнить принудительную синхронизацию Досье с источниками, нажав кнопку **Синхронизировать**:



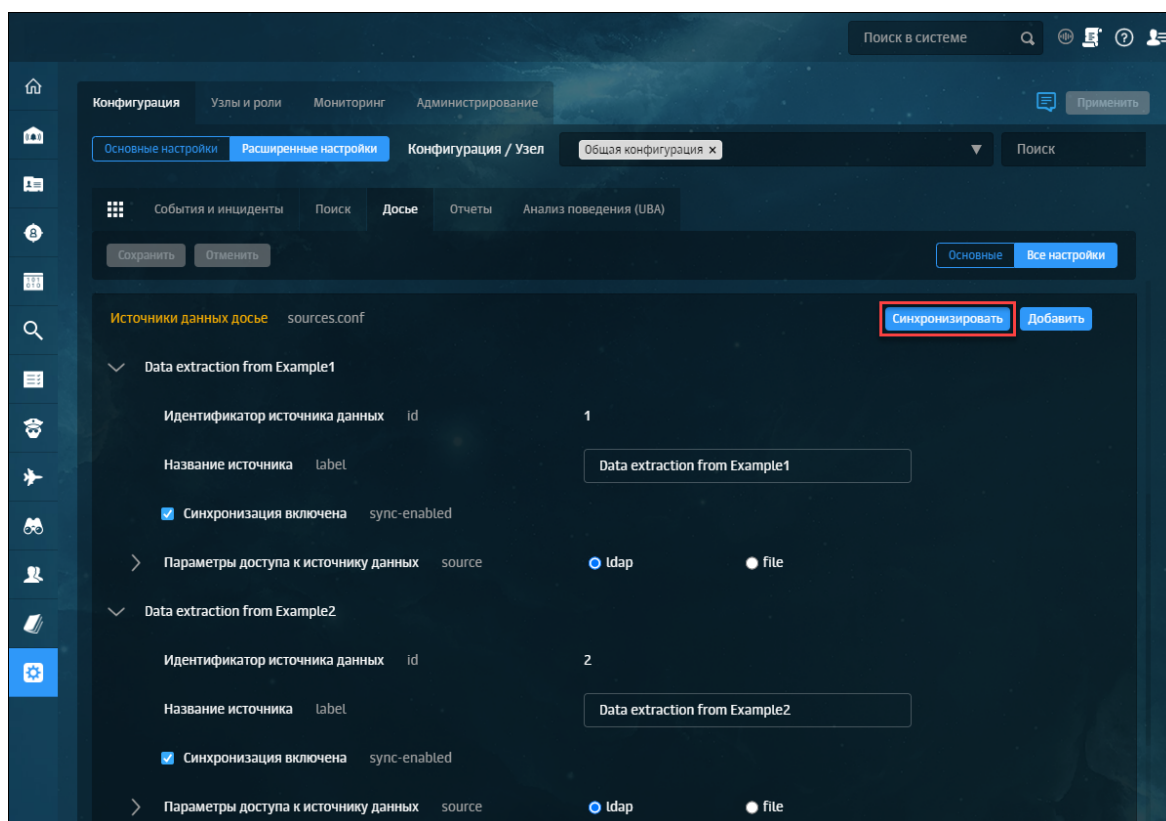


Рис. 8.7. Кнопка принудительной синхронизации Досье

9. Дождаться уведомления об успешности синхронизации.

### 8.6.5. Синхронизация со сторонним Досье

Досье KEO DLP может работать в подчиненном режиме, то есть использовать Досье другого кластера KEO DLP или KEO DLP webProxy. Для этого сторонний кластер должен иметь собственное хранилище Досье. В этом режиме локальный кластер KEO DLP подключается к Досье стороннего кластера и загружает в оперативную память локальную копию Досье. Все изменения, вносимые в Досье со стороны любого из кластеров, становятся доступными со стороны другого кластера. В подчиненном режиме нельзя подключиться к Досье кластера, также использующего подчиненный режим.

Для настройки синхронизации данных Досье KEO DLP с Досье KEO DLP webProxy или KEO DLP необходимо выполнить следующие действия:

1. На master-узле и всех slave-узлах, имеющих роль **Сервис репликации досье на подчиненных узлах (abook-slave)**, перейти в CLI и выполнить команду:

```
~$ sudo /opt/dozor/abook-daemon/bin/reg-abook-slave <host>
```

где **<host>** – FQDN master-узла кластера KEO DLP или KEO DLP webProxy, с Досье которого будет выполняться синхронизация. При выполнении команды система запросит пароль пользователя **root** на удаленном master-узле.

2. Перейти в GUI, выбрать раздел **Система > Конфигурация > Расширенные настройки > Досье**, и в секции **Сервис доступа к Досье** задать значения следующих параметров:

- **Режим работы сервера – Подчиненный.**
- **Сетевой адрес** – FQDN master-узла кластера KEO DLP или KEO DLP webProxy, с Досье которого будет выполняться синхронизация.
- **Номер порта** – порт, на котором сервис **abook-daemon** ожидает соединения по HTTPS (по умолчанию – 2269).

3. Нажать **Сохранить, Применить**.

4. Перезапустить сервис **abook-daemon** на локальном и удаленном master-узлах.

#### 8.6.6. Синхронизация с локальным источником

Досье KEO DLP может быть обновлено с помощью табличных файлов, содержащих данные организационно-штатной структуры (ОШС) для персон и групп. Такие файлы могут быть получены из внешних систем, и должны соответствовать следующим требованиям:

- Таблица персон и таблица групп сохранены каждая в отдельном файле.
- Файлы имеют формат CSV и кодировку UTF-8.
- Первая строка каждого файла содержит заголовки столбцов.
- Разделителем столбцов является точка с запятой.
- Разделителем элементов списка является запятая, все элементы в списке должны быть заключены в квадратные скобки, например: [группа1,группа2,группа3]
- Размер каждого файла не превышает 100 МБ.

Таблица групп должна содержать три столбца:

1. **id** – уникальный идентификатор группы.
2. **pid** – идентификатор родительской группы. Такой идентификатор должен существовать среди групп в столбце **id**, за единственным исключением, когда группа является корневой, и в этом случае не имеет никакой родительской группы (см. пример ниже).
3. **group** – название группы.

Пример таблицы групп:

Табл. 8.1. Таблица групп

| id   | pid | group                          |
|------|-----|--------------------------------|
| 1    |     | ПАО "Вектор"                   |
| 11   | 1   | Московский офис                |
| 12   | 11  | Совет директоров               |
| 13   | 11  | Аппарат генерального директора |
| 111  | 11  | Исполнительный аппарат         |
| 1111 | 111 | Пресс-служба                   |
| 1112 | 111 | АХО                            |

| id    | pid  | group               |
|-------|------|---------------------|
| 1113  | 111  | Секретариат         |
| 1114  | 111  | Коммерческая служба |
| 11141 | 1114 | Отдел маркетинга    |

Таблица персон обязательно должна содержать следующие столбцы:

- **id** – уникальный идентификатор персоны.
- **group-id** – идентификатор группы персоны.
- **fullname** – имя персоны.
- **title** – должность персоны.

Таблица персон также может иметь и другие столбцы, в зависимости от требований к полноте данных о персонах. Пример таблицы персон:

Табл. 8.2. Таблица персон

| id | group-id | fullname                         | title                      | email                  |
|----|----------|----------------------------------|----------------------------|------------------------|
| 1  | 13       | Иванов Иван Иванович             | Генеральный директор       | i.ivanov@vector.su     |
| 2  | 111      | Петров Петр Петрович             | Главный бухгалтер          | p.petrov@vector.su     |
| 3  | 111      | Егоров Егор Егорович             | PR-директор                | e.egorov@vector.su     |
| 5  | 21       | Кузнецова Анна Ивановна          | Офицер ИБ                  | a.kuznetsova@vector.su |
| 6  | 111      | Попова Елена Алексеевна          | Исполнительный директор    | e.popova@vector.su     |
| 78 | 11       | Смирнова Екатерина Александровна | Директор Московского офиса | e.smirnova@vector.su   |

Таблица персон должна удовлетворять следующим критериям:

- У каждой персоны должна быть указана должность.
- Идентификатор группы персон должен существовать в таблице групп.

Таблица персон может содержать столбец с изображениями (**image\_preview**). В ячейках такого столбца следует размещать текстовое base64-представление изображения, полученное из формата **.png**.

После создания файлов с таблицами групп и персон следует разместить их на файловой системе master-узла, а затем выполнить следующее:

1. Перейти в раздел GUI Система > Конфигурация > Расширенные настройки > Досье > Источники данных досье.
2. Нажать кнопку **Добавить** и для появившейся группы параметров задать значения:
  - **Название источника** – ввести произвольное значение.
  - **Параметры доступа к источнику данных** – **file**.

- **Каталог с данными ОШС** – ввести путь к файлам с таблицами групп и персон.
  - **Файл со списком групп** – ввести имя файла с таблицей групп.
  - **Файл со списком сотрудников** – ввести имя файла с таблицей персон.
3. Нажать **Сохранить**, **Применить**, затем **Синхронизировать**.
  4. Перейти в раздел **Досье** и проверить наличие новых данных о персонах и группах.

При синхронизации данных могут возникнуть ошибки импорта. Сведения об ошибках содержатся в файле `/data/spool/abook-daemon/org_structure/errors.log` и в разделе GUI **Досье > Организационная структура > Ошибки импорта данных**.

## 8.7. Настройка планировщика

Для выполнения заданий по расписанию используется планировщик **cron**. После установки KEO DLP расписание **cron** выглядит следующим образом:

- для пользователя **root**:

```
0 */12 * * * /opt/dozor/bin/check_dozor
```

- для пользователя **dozor**:

```
* * * * * accept-settings mode slave 2>&1 | logger -t dozor -i -p cron.warn
* * * * * accept-policy mode slave 2>&1 | logger -t dozor -i -p cron.warn
* * * * * counters-stat mode slave 2>&1 | logger -t dozor -i -p cron.warn
10 4 * * * dump-settings name daily password "" 2>&1 | logger -t dozor -i -p cron.warn
5 1 * * * send-vendor-report | logger -t dozor -i -p cron.warn
5 15 * * * gen-bug-report | logger -t dozor -i -p cron.warn
25 4 * * * do-logrotate || logger -t dozor "logrotate exited abnormally"
```

Данное расписание соответствует следующим заданиям:

- Вызов скрипта **accept-settings** на slave-узлах раз в минуту. Это задание предназначено для распространения конфигурации KEO DLP по slave-узлам.
- Вызов скрипта **accept-policy** на slave-узлах раз в минуту. Это задание предназначено для распространения политики фильтрации KEO DLP по slave-узлам.
- Вызов скрипта **counters-stat** на slave-узлах раз в минуту. Это задание предназначено для сбора метрик ОС и приложений.
- Вызов скрипта **dump-settings** на всех узлах раз в сутки. Это задание предназначено для сохранения репозитория настроек конфигурации в каталог `/data/backups/dozor/`.
- Вызов скрипта **send-vendor-report** на всех узлах раз в сутки. Это задание предназначено для отправки диагностических данных производителю.
- Вызов скрипта **gen-bug-report** на всех узлах раз в сутки. Это задание предназначено для создания отчета об ошибках.

- Вызов скрипта **do-logrotate** на всех узлах раз в сутки. Это задание предназначено для ротации журнальных файлов, находящихся в каталоге **/opt/dozor/var/log/** (журнальные файлы утилит).
- Вызов скрипта **check\_dozor** на всех узлах два раза в сутки (полдень и полночь). Это задание предназначено для подсчета контрольных сумм неизменяемых исполняемых файлов.

## 8.8. Настройка индексатора

### 8.8.1. Общая настройка индексатора

Для текстового поиска по досье, архиву сообщений и архиву событий ИБ используется поисковый движок OpenSearch.

Сервис **indexer-ng** выполняет индексацию сообщений в архиве. Данный сервис используется ролями **Индексатор текста** и **Вспомогательный сервис индексации текста**. Записи о сообщениях хранятся в таблице **message** БД архива. Версия сообщений определяется параметром **message\_version** таблицы. Значение по умолчанию равно 1. Оно увеличивается при изменении информации в сообщении (добавлении и удалении пометок, отправки уведомлений и т. д.).

Параметр **index\_version** задает версию сообщения, которую хранит сервис **indexer-ng**. При этом если значение **index\_version** равно 0, то сообщение ранее не индексировалось.

Работа индексатора заключается в преобразовании сообщений, хранящихся в БД архива, в документы OpenSearch. В случае изменения, архивирования и удаления сообщений сервис индексации данных получает уведомления от сервера архивации. Далее индексатор с заданной периодичностью сканирует БД архива и выполняет поиск сообщений, у которых различаются значения параметров **message\_version** и **index\_version**. Периодичность задается в параметре **Период плановой индексации (Ч)** (секция **Индексация сообщений в архиве**, раздел **GUI Конфигурации > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**) и по умолчанию равна одному часу. После этого выполняется синхронизация индексов на индексаторе, и обновляется значение параметра **index\_version**.

Сервис **indexer-ng** проверяет данные архива на наличие индексов. В случае их отсутствия индексатор текста выполняет сброс значения параметра **index\_version** таблицы **message**. Далее запускается индексация сообщений в БД архива.

#### Внимание!

*Следует учитывать, что во время выполнения обновления индексов сообщения могут пропадать из списков результатов быстрого поиска.*

#### Внимание!

*Настройка фоновой миграции устаревших индексов бесед, включаемая флажком **Включена для бесед**, может корректно работать только в комбинации с флажком **Включена для сообщений**.*

---

Работа OpenSearch обеспечивается сервисом **opensearch**. Этот сервис используется ролями **Индексатор текста**, **Хранилище индексов событий и инцидентов**, **Индексатор медиаинформации** и **Вспомогательный сервер OpenSearch**. В распределенной конфигурации KEO DLP OpenSearch может образовывать собственный кластер, то есть иметь распределенную конфигурацию, если его сервис запущен на нескольких узлах.

В зависимости от назначенной роли, узлы KEO DLP выполняют следующие задачи:

- **Индексатор текста** – создание и хранение индексов архива сообщений, поиск по архиву сообщений.
- **Вспомогательный сервис индексации текста** – создание индексов хранения сообщений без хранения.
- **Хранилище индексов событий и инцидентов** – создание и хранение индексов архива инцидентов, поиск по архиву инцидентов.
- **Индексатор медиаинформации** – создание и хранение индексов медиаинформации.
- **Вспомогательный сервер OpenSearch** – участие в кластере OpenSearch для решения некоторых служебных задач (см. ниже).

Если роль **Индексатор текста** назначена двум или более узлам, то они будут делить индексы между собой для равномерного использования ресурсов кластера (то же справедливо для ролей **Хранилище индексов событий и инцидентов** и **Индексатор медиаинформации**).

Роль **Вспомогательный сервер OpenSearch** предназначена для следующих целей:

- Выведение узла из кластера OpenSearch без потери данных. Если узел имеет роль **Индексатор текста** и/или **Хранилище индексов событий и инцидентов**, и требуется освободить его от этой роли без потери хранящихся на нем индексов, то необходимо выполнить следующие действия:

1. Назначить узлу роль **Вспомогательный сервер OpenSearch**.
2. Снять с узла роли **Индексатор текста** и/или **Хранилище индексов событий и инцидентов**.
3. Дождаться окончания переноса индексов на другие узлы кластера OpenSearch. Проверить наличие индексов на узле можно с помощью CLI, выполнив следующую команду:

```
indextool -i
```

Об окончании переноса свидетельствует значение **0** в столбце **Size**.

4. При необходимости, снять с узла роль **Вспомогательный сервер OpenSearch**.
- Исключение конфликтов внутри кластера OpenSearch. Некоторые внутренние решения (например, выбор ведущего узла) узлы OpenSearch принимают большинством. Если кластер состоит из двух узлов, и один из них по каким-либо причинам не отвечает на запросы (например, выключен или перегружен), то решение не может быть принято, поскольку оставшийся узел не составляет большинства из двух. Для исключения такой ситуации следует назначить роль **Вспомогательный сервер OpenSearch** еще одному



---

узлу. Сама по себе эта роль практически не создает дополнительной нагрузки на узел KEO DLP, поэтому ее можно назначить любому узлу, который имеет хотя бы минимальный резерв производительности.

Роль **Индикатор медиаинформации** необходимо назначить одному или нескольким узлам для полноценного использования инструмента **4D** в карточке персоны в разделе GUI **Досье**. При необходимости можно настроить OpenSearch в части индексации медиаинформации (см. ниже).

Настройку OpenSearch следует выполнять при следующих условиях:

- Узлу назначена роль **Вспомогательный сервер OpenSearch**.
- Требуется корректировка производительности сервиса **opensearch**.

Настройка OpenSearch производится в следующих секциях:

- **Сервис хранения и индексации событий и инцидентов** (раздел GUI Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > События и инциденты);
- **Сервис поиска и индексации OpenSearch** (раздел GUI Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск);
- **Производительность сервиса поиска и индексации OpenSearch** (раздел GUI Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск).
- **Настройки индексации медиаинформации** (раздел GUI Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение > Хранение медиаинформации).

Рекомендуемые значения параметров секций **Производительность сервиса поиска и индексации сообщений и инцидентов** (раздел GUI Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск) и **Сервис хранения и индексации событий и инцидентов** (раздел GUI Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > События и инциденты):

- **Количество shard-ов** – количество шардов базы данных индексов OpenSearch. Рекомендуемое значение параметра равно числу узлов в кластере OpenSearch (то есть по одному шарду на узел). Если на узлах кластера OpenSearch нет высоконагруженных сервисов и имеется запас производительности, допускается выделить по два шарда на узел; в этом случае, рекомендуемое значение параметра составит количество узлов в кластере OpenSearch, умноженное на 2. Максимальное значение рассчитывается исходя из того, что общее число шардов по всем индексам за требуемый срок хранения не должно превышать 500. Один шард содержит индексы за неделю. Таким образом, для расчета максимального значения необходимо разделить 500 на требуемый срок хранения, выраженный в неделях, и округлить вниз до целого. В качестве значения параметра следует указать меньшее из рекомендуемого и максимального значений.

Пример: имеется 5 узлов, их производительность достаточно высока, требуется хранить индексы за 52 недели (год). Рекомендуемое значение составляет 10 (по два шарда

---

на узел). Максимальное значение составляет 9 (целая часть результата деления 500 на 52). Тогда в качестве значения параметра следует указать 9.

Пример: имеется 2 узла, их производительность достаточно высока, требуется хранить индексы за 52 недели (год). Рекомендуемое значение составляет 4 (по два шарда на узел). Максимальное значение составляет 9 (целая часть результата деления 500 на 52). Тогда в качестве значения параметра следует указать 4.

- **Число копий** – количество копий индексов OpenSearch. Значение по умолчанию – 0, то есть все индексы хранятся в единственном экземпляре. Увеличивать это значение имеет смысл только в случае распределенной конфигурации кластера OpenSearch. Использование копий индексов OpenSearch позволяет повысить производительность работы OpenSearch, поскольку становится возможным параллельный доступ к индексам на разных узлах, но при этом кратно повышаются требования к объему физических носителей данных на узлах. Копии индексов всегда хранятся на разных узлах, то есть на одном узле не может быть двух и более копий одних и тех же индексов, поэтому максимальное значение этого параметра равняется числу узлов кластера OpenSearch, уменьшенному на единицу.
- **Периодичность обновления индекса (с)** – периодичность обновления индекса OpenSearch в секундах. Значение по умолчанию – 30, то есть индекс становится доступным для чтения и использования через тридцать секунд после его помещения в базу данных OpenSearch. Это значение нормально для штатной работы ПК KEO DLP, однако в отдельных сценариях (например, единовременная индексация базы данных с большими объемами данных) это может привести к значительному ухудшению производительности. В подобных случаях рекомендуется временно увеличивать это значение до окончания создания индекса.

Рекомендуемые значения параметров секции **Сервис поиска и индексации OpenSearch** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**):

- **Прекратить размещение новых индексов, если свободного места меньше (МБ)** – минимальный размер свободного места на файловой системе в мегабайтах, при котором происходит размещение новых индексов OpenSearch. Если свободного места на узле станет меньше указанного значения, OpenSearch на этом узле прекратит размещение новых индексов. Значение следует выбирать исходя из условий эксплуатации KEO DLP. Значение по умолчанию: 1024.
- **Переносить данных на другие узлы если свободного места меньше (МБ)** – максимальный размер свободного места на файловой системе узла кластера OpenSearch в мегабайтах, при котором происходит принудительный перенос данных на другие узлы. Если свободного места на узле станет меньше указанного значения, OpenSearch на этом узле будет пытаться переносить индексы на другие узлы кластера до тех пор, пока не будет освобожден указанный объем. Значение следует выбирать исходя из условий эксплуатации KEO DLP. Значение по умолчанию: 512.
- **Репликация с учетом размещения серверов в стойках** – при включении этого параметра копии индексов OpenSearch сохраняются на узлах с учетом их физического размещения в серверных стойках. На узлах, размещенных в одной стойке, совокупно будет находиться одна полная копия индексов или ее часть, без дублирования. Принадлежность узла к той или иной стойке следует указать во вкладке **Система > Узлы и роли**, открыв вспомогательное меню этого узла и выбрав пункт **Атрибуты**. Количе-



---

ство копий индексов OpenSearch не должно превышать количество стоек, содержащих узлы кластера OpenSearch.

Для остальных параметров рекомендуется оставить значения по умолчанию.

Рекомендуемые значения параметров секции **Производительность сервиса поиска и индексации сообщений и инцидентов** (раздел **GUI Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**):

- **Размер памяти (ГБ)** – объем оперативной памяти в гигабайтах, выделяемой для сервиса **opensearch** на каждом узле кластера OpenSearch. Значение по умолчанию: 4. Рекомендуется увеличить это значение на столько, сколько полных или неполных десятков миллионов сообщений содержится в архиве. Например, если в архиве содержится 35 миллионов сообщений, то в качестве значения параметра рекомендуется установить 8. Максимально допустимое значение – половина всей имеющейся оперативной памяти сервера, но не более 128 ГБ.

После установки значений параметров конфигурационных файлов необходимо нажать **Сохранить** на вкладках каждого из них, а затем нажать **Применить** на вкладке любого из них.

### 8.8.2. Настройка индексации оперативных и исторических данных

Для оптимизации работы с архивом сообщений и хранилищем событий и инцидентов ИБ используется механизм разделения данных на оперативные и исторические. При использовании этого механизма оперативными считаются данные не старше некоторого заданного значения в неделях, а историческими – все остальные. При неиспользовании этого механизма все данные считаются оперативными. Оперативные и исторические данные хранятся и индексируются разными сервисами на разных узлах.

#### Примечание

*Узел может хранить оперативные и исторические данные одного типа (сообщения архива или события и инциденты ИБ), но в этом случае теряется смысл их разделения.*

Для использования механизма оперативных и исторических данных необходимо выполнить следующие шаги:

1. Перейти в раздел **GUI Система > Узлы и роли** и назначить роль **Индексатор текста** тем узлам, на которых необходимо хранить и выполнять индексацию оперативных сообщений архива.
2. Назначить роль **Хранилище индексов событий и инцидентов** тем узлам, на которых необходимо хранить и выполнять индексацию оперативных событий и инцидентов ИБ.
3. Назначить роль **Индексатор исторических сообщений** тем узлам, на которых необходимо хранить и выполнять индексацию исторических сообщений архива.
4. Назначить роль **Хранилище индексов исторических событий и инцидентов** тем узлам, на которых необходимо хранить исторические события и инциденты ИБ.

- 
5. Назначить роль **Вспомогательный сервис индексации текста** тем узлам, на которых необходимо только выполнять индексацию оперативных сообщений архива, без хранения индексов.
  6. Назначить роль **Вспомогательный индексатор исторических сообщений** тем узлам, на которых необходимо только выполнять индексацию исторических сообщений архива, без хранения индексов.
  7. При необходимости, назначить некоторым узлам роль **Вспомогательный сервер OpenSearch** для исключения конфликтов внутри кластера OpenSearch, как описано в разделе [8.8.1](#).
  8. Перейти в раздел **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск** и в секции **Индексация сообщений в архиве** переключить параметр **Разделять оперативные и исторические данные** в значение **Разделять**. Для появившегося параметра **Период хранения в оперативном архиве** установить значение в неделях, которое будет определять максимальный возраст сообщения в архиве, после которого оно переходит из оперативных в исторические.
  9. Перейти в раздел **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > События и инциденты** и в секции **Сервис хранения и индексации событий и инцидентов** переключить параметр **Разделять оперативные и исторические данные** в значение **Разделять**. Для появившегося параметра **Период хранения в оперативном архиве** установить значение в неделях, которое будет определять максимальный возраст события или инцидента ИБ, после которого оно переходит из оперативных в исторические.
  10. Нажать **Сохранить** и **Применить**.

После этого индексаторы на узлах приступят к маркировке оперативных и исторических данных, а сервис OpenSearch начнет распределение индексов по заданным узлам. Пользоваться системой можно сразу же.

## 8.9. Настройка файлового хранилища

Создание схемы БД и настройка соответствующих соединений в конфигурации KEO DLP позволяет архивировать и хранить сообщения в БД архива. Помимо БД, сообщения можно хранить в файловой системе, для чего на одном или нескольких узлах организуется файловое хранилище (далее – ФХ). На одном или нескольких узлах необходимо настроить центральное ФХ, куда будут записываться данные с локальных ФХ, организованных на других узлах.

Архитектура ФХ подробно описана в приложении [Приложение Е. Описание файлового хранилища](#).

Использование ФХ по умолчанию включено. Необходимо либо выключить использование ФХ, либо назначить каким-либо узлам кластера роли, относящиеся к файловому хранилищу и затем настроить работу ФХ.

Для настройки ФХ необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Узлы и роли** и назначить роль **Центральное файловое хранилище** всем узлам, на которых предполагается производить долгосрочное

---

хранение и ротацию данных. Рекомендуется назначить эту роль узлу, к которому примонтирована СХД.

2. Назначить роль **Локальное файловое хранилище** всем узлам, на которых предполагается осуществлять временное хранение сообщений с последующим переносом в центральное ФХ. Рекомендуется назначить эту роль всем узлам с ролью **Фильтр почтового потока**.
3. Перейти в раздел **Система > Конфигурация > Расширенные настройки > Хранение** и в секции **Настройки файлового хранилища** задать значения следующих параметров:

- **Gzip-компрессия при размещении** – рекомендуется оставить включенным для экономии места на диске.
- **Вывод отладочной информации** – включить при необходимости диагностики ФХ.
- **Режим распределения по хранилищам при переносе** – выбрать алгоритм распределения данных по хранилищам при их переносе. Принимает значения: **Приоритет скорости** и **Равномерное распределение**. Значение по умолчанию: **Приоритет скорости**.

При выбранном значении **Приоритет скорости** данные переносятся в центральные ФХ с той скоростью, с которой они могут быть приняты. Более быстрый сервер забирает на себя больше данных. Неработающие узлы исключаются из переноса. Этот режим наиболее производительный, но может приводить к дисбалансу объемов хранения между хранилищами.

При выбранном значении **Равномерное распределение** на каждое центральное ФХ переносится одинаковое количество контейнеров. Медленный узел замедляет процесс переноса. Неработающий узел практически останавливает процесс переноса. Этот режим дает равномерное распределение данных по хранилищам, но скорость переноса фактически ограничена скоростью самого медленного узла.

Рекомендуется выбрать значение по умолчанию.

- **Разрешенные часы переноса данных из локального файлового хранилища в центральное:**
  - **Час начала (timezone сервера)** – час, начиная с которого будет выполняться перенос данных из локального ФХ в центральное.
  - **Час окончания (timezone сервера)** – последний час, в течение которого будет выполняться перенос. Например, если задано значение 17, то данные будут переноситься вплоть до момента 17:59:59.
- **Настройка переноса контейнеров** – нажать кнопку **Добавить** в строке параметра:
  - **Volume Group** – **vg-000000**
  - **Время жизни до переноса** – минимальное время нахождения данных в локальном ФХ до переноса. Значение по умолчанию **0 дн. 0 ч.** означает, что данные будут перенесены в центральное ФХ при первой же возможности.
- **Настройка ротации:**

- 
- **Volume Group – vg-000000**
  - **Время жизни до ротации** – период времени в днях, по истечении которого после помещения данных в центральное ФХ происходит их ротация (удаление или архивирование).
  - **Рекомендуемый размер файла архива (МБ)** – максимальный размер файла в мегабайтах, помещаемого в архив при ротации, если параметр **Режим ротации** имеет значение **Локальная файловая система** или **Внешний FTP сервер**.
  - **Критический объем свободного места (МБ)** – минимальный размер свободного пространства на узле центрального ФХ в мегабайтах. Если размер свободного пространства становится меньше этого значения, система производит внеочередную ротацию в момент 3:00:00 ближайших суток.
  - **Gzip компрессия архива** – Gzip-компрессия при сохранении данных в центральное ФХ. Включить, если это требуется.
  - **Режим ротации** – установить одно из следующих значений:
    - **Удалить, не архивировать** – данные при ротации будут удалены.
    - **Локальная файловая система** – данные при ротации будут отключены от ФХ и помещены в каталог, указанный в параметре **Путь**.
    - **Внешний FTP сервер** – данные при ротации будут отключены от ФХ и помещены заданный каталог на заданном FTP-сервере:
      - **Сетевой адрес** – адрес FTP-сервера организации.
      - **Номер порта** – порт, на котором FTP-сервер ожидает соединения.
      - **Режим FTP** – режим работы, на который настроен FTP-сервер (активный или пассивный).
      - **Пользователь** – имя пользователя для соединения с FTP-сервером.
      - **Пароль** – пароль этого пользователя.
      - **Путь на FTP-сервере** – путь к каталогу на FTP-сервер, в который будут сохраняться данные при ротации.
  - **Периодичность ротации** – выбрать **Ежедневно**, **Еженедельно** или **Ежемесячно**, после чего задать значения следующих параметров:
    - **День месяца**
    - **День недели**
    - **Час**
    - **Минута**
4. В секции **Тома файлового хранилища** задать значения следующих параметров:
- **Группа томов – vg-000000**

- **Идентификатор тома** – задать идентификатор тома. Рекомендуется выбирать значение с учетом возможного создания других томов.
- **Только для чтения** – включить, если требуется запретить запись данных в этот том.

#### **Внимание!**

*Ротация тома (если включена) выполняется независимо от значения этого параметра.*

- **Разрешить ротацию тома** – включить, если требуется ротация этого тома в соответствии с заданными на предыдущем шаге параметрами.
  - **Путь, по которому размещены данные** – путь к каталогу данных ФХ на файловой системе.
5. При необходимости, добавить новый том с помощью кнопки **Добавить** и повторить предыдущий шаг.
  6. Нажать **Сохранить** и **Применить**.

## **8.10. Настройка перехвата файлов из МойОфис Документы Онлайн**

В KEO DLP реализован перехват файлов из корпоративного облачного хранилища МойОфис Документы Онлайн версии 3.4. Для настройки перехвата необходимо выполнить следующие действия:

1. Перейти в GUI KEO DLP, раздел **Система > Расширенные настройки > Обработка сообщений** и открыть секцию **Сервис фильтрации сообщений**.
2. Раскрыть группу настроек **ICAP-интерфейс** и задать следующие значения:
  - **Включить ICAP-интерфейс** – установить флажок.
  - **Порт ICAP-интерфейса** – указать любой незанятый номер сетевого порта.
  - **Обрабатывать только указанные MIME-типы** – снять флажок.
3. В той же группе, в зависимости от возможностей по обработке ошибок снять или установить флажки для параметров:
  - **Не обрабатывать сообщения с пустым телом**
  - **Выдавать ответ с кодом 200/204 при ошибках обработки**
4. Убедиться, что в разделе GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений > Схемы преобразования** присутствует схема преобразования с идентификатором **dozor-file**.
5. Подключиться к серверу «Мой Офис» и настроить интеграцию с KEO DLP, руководствуясь соответствующей документацией.

## 8.11. Настройка перехвата сообщений из Express

В KEO DLP реализован перехват сообщений из корпоративного мессенджера Express. Для настройки перехвата необходимо выполнить следующие действия:

1. Обновить мессенджер Express до актуальной версии согласно официальной документации по ссылке [https://express.ms/admin\\_guide\\_update.pdf](https://express.ms/admin_guide_update.pdf).
2. Перейти в GUI KEO DLP, раздел **Система > Расширенные настройки > Обработка сообщений** и открыть секцию **Сервис фильтрации сообщений**.
3. Раскрыть группу настроек **ICAP-интерфейс** и задать следующие значения:
  - **Включить ICAP-интерфейс** – установить флажок.
  - **Порт ICAP-интерфейса** – указать любой незанятый номер сетевого порта.
  - **Обрабатывать только указанные MIME-типы** – снять флажок.
4. В той же группе, в зависимости от возможностей по обработке ошибок снять или установить флажки для параметров:
  - **Не обрабатывать сообщения с пустым телом**
  - **Выдавать ответ с кодом 200/204 при ошибках обработки**
5. Убедиться, что в разделе GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений > Схемы преобразования** присутствует схема преобразования с идентификатором **Express**.
6. Убедиться, что на серверах обработки сообщений Express существует файл схемы преобразования по пути **/opt/dozor/smap/mapping/express.edn**. В противном случае поместить файл в данный каталог и задать для него права на чтение. Содержимое файла должно быть следующим:

```
{
  ["x-dozor-mapping-schema" "Express"]
  [
    [:address-info :source] [:header "x-plain-authenticated-user" :extract #"\\.+\\.+" :as-login]
    [:address-info :source] [:header "x-plain-authenticated-user" :extract #"\\.+\\.+" :as-im]
    [:address-info :source] [:header "x-plain-authenticated-user" :extract #"^[1-9]+[0-9]*$" :as-im]
    [:address-info :destination] [:header "x-recipient-user-login" :as-list :extract #"\\.+\\.+" :as-login]
    [:address-info :destination] [:header "x-recipient-user-login" :as-list :extract #"\\.+\\.+" :as-im]
    [:address-info :destination] [:header "x-recipient-user-login" :as-list :extract #"^[1-9]+[0-9]*$" :as-im]

    :subject [:header "x-groups-channels-name"]
    :subject [:header "subject"]
    :headers [:header "x-application" :as-header "x-agent-application-name"]
    :headers [:header "x-groups-channels-id" :as-header "x-agent-chat-id"]
    :recv-date [:header "x-message-date" :or-now :as-date]
    :comp-date [:header "x-message-date" :or-now :as-date]
    :type [:const "endpoint/im"]
    :comm-channel [:const "im"]
    :filename [:header "x-file-name"]]
  ]
}
```

- 
7. Перезапустить сервис **mailfilter**, выполнив в CLI следующие команды:

```
# /opt/dozor/bin/shell  
  
# dsctl restart mailfilter
```

8. Перейти в CLI сервера Express и выполнить от имени пользователя **root** команды:

```
cd /opt/express  
  
mkdir -p dlps_keys/storage && chown -R 888:888 dlps_keys
```

9. Открыть файл настроек **/opt/express/settings** и добавить в него следующие строки:

```
dlps_enabled: true  
dlps_env_override:  
  DLPS_ICAP_CLIENT_HOST: <keo_dlp_ip>  
  DLPS_ICAP_CLIENT_PORT: <keo_dlp_port>  
dlps_icap_additional_headers:  
  client_ip: <express_ip>  
  server_ip: <dozor_ip>  
  network_segment: CTS  
  application: Express  
dlps_icap_client_host: <keo_dlp_ip>  
dlps_icap_client_port: <keo_dlp_port>
```

где:

- **<keo\_dlp\_ip>** – IP-адрес узла КЕО DLP с ролью **Фильтр почтового потока** или **Балансировщик** (см. раздел [7.4](#)). В этом файле настроек можно задать только один такой узел.
  - **<keo\_dlp\_port>** – порт, на котором этот узел ожидает соединения по протоколу ICAP (заданный на шаге [3](#)).
  - **<express\_ip>** – IP-адрес бэкенд-сервера Express.
10. Перезагрузить контейнеры Express, выполнив команды:
- ```
cd /opt/express  
  
dpl -d  
  
dpl --dc restart
```
- В каталоге **/opt/express/dlps\_keys** будет создан файл ключа с расширением **.key**.
11. Перейти в GUI сервера Express, перейдя по адресу <https://express.mydomain.ltd/dlps/>. При входе использовать имя пользователя **admin** и пароль **admin**. Настоятельно рекомендуется изменить пароль на более надежный.
12. Перейти в раздел **Общие** и установить флажки для следующих параметров:
- **DLPS**
  - **Отправлять события режима конфиденциальной переписки**



13. Перейти в раздел **Настройки** и установить флажки для следующих параметров:

- **Интеграция с KEO DLP**
- **Режим отладки интеграции с KEO DLP** (если требуется ведение журналов отладки на стороне Express)

14. Перейти в раздел GUI KEO DLP **Справочники > Приложения**, открыть вкладку **Справочник приложений** и нажать кнопку **Добавить приложение**. В появившемся окне **Добавить приложение** задать название **Express** и родительскую категорию **Общение > Мессенджеры и чаты**. Нажать **Сохранить**.

15. Выбрать в справочнике созданное приложение **Express** и добавить в список процессов значение **Express**.

## 8.12. Настройка перехвата сообщений из TrueConf Server

В KEO DLP реализован перехват сообщений из ПО для видеоконференцсвязи (ВКС) TrueConf Server версии 5.4.0 и выше. Для настройки перехвата необходимо выполнить следующие действия:

1. Перейти в GUI KEO DLP и открыть раздел **Система > Конфигурация > Расширенные настройки > Обработка сообщений**. Перейти в секцию **Сервис фильтрации сообщений**, раскрыть группу параметров **ICAP-интерфейс** и установить флажок **Включить ICAP-интерфейс**. Изменить порт по умолчанию, если это необходимо. Нажать **Сохранить**, **Применить**.
2. Убедиться, что в разделе GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений > Схемы преобразования** присутствует схема преобразования с идентификатором **TrueConf**.
3. Зайти на сервер **TrueConf** под учетной записью администратора. Выбрать раздел **Расширения > Интеграция с DLP**, активировать расширение, установив соответствующий флажок.
4. В секции **ICAP-сервер** задать следующие параметры подключения к KEO DLP:
  - **Хост** – IP-адрес узла KEO DLP с ролью **Фильтр почтового потока** без префикса **http: / https:**.
  - **Порт** – порт, на котором этот узел ожидает соединения по протоколу ICAP (заданный на шаге 1).
  - **Безопасное подключение** – **Не использовать**.

Нажать **Проверить соединение**. Если результат проверки отображается зеленым текстом, система доступна.

5. В секции ниже активировать проверку текстовых сообщений и настроить ICAP-запрос для отправки в KEO DLP. Пример:

```
REQMOD icap://%host:%port/icap/full ICAP/1.0
Host: %host
Allow: 204
```



```
Connection: keep-alive
Encapsulated: req-hdr=0, req-body=%body_offset

POST / HTTP/1.1
Host: %server_name
Date: %date
X-Dozor-Mapping-Schema: TrueConf
X-Dozor-Application: TrueConf
X-Client-IP: %src_ip
X-Dozor-Src-Im: %src
X-Dozor-Src-Domain-Login: %src_user
X-Dozor-Src-Login: %src_user_no_domain
X-Dozor-Dst-Im: %dst
X-Dozor-Dst-Domain-Login: %dst_user
X-Dozor-Dst-Login: %dst_user_no_domain
X-Dozor-Chat-Id: %chat_id
X-Dozor-Received-Date: %date
X-Dozor-Chat-Title: =?UTF-8?B?%chat_title_base64?=
Content-Type: application/octet-stream

%body_length
%body
```

### Примечание

*Текст запроса должен быть оформлен также, как и в примере: с переносами строк в нужных местах.*

Изменить действия с текстовым сообщением и время ожидания ответа от KEO DLP, если это необходимо.

6. В следующей секции активировать проверку файлов и настроить ICAP-запрос для отправки в KEO DLP. Пример:

```
REQMOD icap://%host:%port/icap/full ICAP/1.0
Host: %host
Allow: 204
Connection: keep-alive
Encapsulated: req-hdr=0, req-body=%body_offset

POST / HTTP/1.1
X-Dozor-Mapping-Schema: TrueConf
X-Dozor-Application: TrueConf
Host: %server_name
Date: %date
X-Client-IP: %src_ip
X-Dozor-Src-Im: %src
X-Dozor-Src-Domain-Login: %src_user
X-Dozor-Src-Login: %src_user_no_domain
X-Dozor-Dst-Im: %dst
X-Dozor-Dst-Domain-Login: %dst_user
X-Dozor-Dst-Login: %dst_user_no_domain
X-Dozor-Chat-Id: %chat_id
X-Dozor-Received-Date: %date
X-Dozor-Filename: =?UTF-8?B?%filename_base64?=-
```

```
X-Dozor-Chat-Title: =?UTF-8?B?%chat_title_base64?=
Content-Type: application/octet-stream

%body_length
%body
```

### Примечание

Текст запроса должен быть оформлен также, как и в примере: с переносами строк в нужных местах.

Изменить действия с файлом и время ожидания ответа от KEO DLP, если это необходимо.

7. Нажать кнопку **Применить**.

## 8.13. Настройка перехвата сообщений из VK Teams

В KEO DLP реализован перехват сообщений из корпоративного мессенджера VK Teams. Для настройки перехвата необходимо выполнить следующие действия:

1. Перейти в GUI KEO DLP и открыть раздел **Система > Конфигурация > Расширенные настройки > Обработка сообщений**. Перейти в секцию **Сервис фильтрации сообщений**, раскрыть группу параметров **ICAP-интерфейс** и установить флажок **Включить ICAP-интерфейс**. Изменить порт по умолчанию, если это необходимо. Нажать **Сохранить**, **Применить**.
2. Настроить синхронизацию Досье с тем же источником, который использует VK Teams. Настройка синхронизации Досье описана в разделе [8.6](#).
3. Настроить правила политики для обработки перехватов. Если не требуется обрабатывать перехваты типа **веб-запрос**, то их можно отфильтровать правилом политики по заголовку **Host** со значением **VkTeams**.
4. Перейти на сервер **VK Teams**, открыть конфигурационные файлы **/usr/local/etc/gbld-st-1.conf** и **/usr/local/etc/gbld-mchat-1.conf**, и добавить в каждый из них следующие строки (либо изменить значение **false** на **true**, если такие строки уже есть):

```
gbld.check_dlp true
gbld.check_dlp_sync true
```

5. Указать конечную точку сервера KEO DLP, выполнив команду:

```
etcdctl --endpoints=<host_etcd>:<port_etcd> put
/vars/services/plumber/development/public/service/DLP/ICAP/address
icap:VV<dozor_mailfilter>:<dozor_port>/icap/spool
```

где **<host\_etcd>:<port\_etcd>** – FQDN и порт сервера VK Teams, **<keo\_dlp\_mailfilter>:<keo\_dlp\_port>** – IP-адрес и порт узла KEO DLP с ролью **Фильтр почтового потока**. Пример:

```
etcdctl --endpoints=etcd.organization.local:2379 put  
/vars/services/plumber/development/public/service/DLP/ICAP/address  
icap:VV192.168.106.71:2344/icap/spool
```

6. Перезапустить сервис **plumber**, выполнив команду:

```
kubectl -n plumber scale deployment plumber --replicas=1
```

7. Перезапустить сервисы **gbld-st** и **gbld-mchat**, выполнив команду:

```
systemctl restart gbld-st-1 gbld-mchat-1
```

8. О т к р ы т ь к о н ф и г у р а ц и о н н ы й ф а й л **/usr/local/etc/go.files.icq.com/files.icq.com.config.yaml** и добавить в него следующие строки:

```
DLP:  
isActive: true  
syncSend: true  
resortClient:  
timeout: "3s"
```

9. Перезапустить сервис **gofiles\_httpd**, выполнив команду:

```
systemctl restart gofiles_httpd
```

## 8.14. Настройка перехвата сообщений из Cisco Webex Teams

В KEO DLP реализован перехват сообщений из корпоративного мессенджера Cisco Webex Teams с помощью официального API. Для настройки перехвата необходимо выполнить следующие действия:

1. Перейти по ссылке <https://developer.webex.com/my-apps/new/integration> и авторизоваться в системе под учетной записью с правами **Compliance Officer**.
2. На открывшейся странице в поле Redirect URI(s) указать адрес (IP или FQDN) и порт сервера KEO DLP, на котором будут выполняться перехваты сообщений. Пример: **https://filter.dozor.organization.com:9090**.

### Внимание!

*Номер порта 9090 не может быть изменен и должен быть разрешен пакетным фильтром.*

### Внимание!

*Выбранный сервер KEO DLP должен иметь роль **Фильтр почтового потока**.*

3. Включить следующие флажки:

- **spark:people\_read**

- 
- **spark-admin:people\_read**
  - **spark-compliance:events\_read**
  - **spark-compliance:rooms\_read**
  - **spark-compliance:messages\_read**
  - **spark-compliance:memberships\_read**
4. Заполнить остальные обязательные поля значениями по усмотрению или согласно реалиям организации.
  5. Нажать **Add Integration**.
  6. Сохранить значения полей **CLIENT\_ID** и **CLIENT\_SECRET** для будущего использования.
  7. Если на сервере KEO DLP, выбранном для выполнения перехватов, нет доступа к адресам **https://webexapis.com/** и **https://developer.webex.com/**, следует задать на этом сервере переменную окружения **https\_proxy**, выполнив в CLI команду следующего вида:

```
# export https_proxy=http://<proxy.host:port>/
```

где **<proxy.host:port>** – адрес (IP или FQDN) и порт прокси-сервера организации.

8. Запустить на этом сервере команду следующего вида:

```
# wereg.py -n <hostname> -i <CLIENT_ID> -s <CLIENT_SECRET> -t <path>
```

где **<hostname>** – адрес (IP или FQDN) этого сервера, **<CLIENT\_ID>** и **<CLIENT\_SECRET>** – соответствующие значения полей, сохраненные на шаге 6, **<path>** – произвольный путь к каталогу, в который будет записан файл **token.json** в результате выполнения команды (например, **/opt/dozor/share/im-crawler/token.json**).

### Внимание!

Файл **token.json** необходим для идентификации опрашивающего сервера KEO DLP на стороне серверов Webex. При отсутствии обращений серверов KEO DLP к серверам Webex с помощью этого файла в течение более 90 суток, файл становится недействительным. Для создания нового такого файла необходимо повторно выполнить этот шаг инструкции.

9. В результате выполнения команды на экран будет выведен URL, по которому нужно будет перейти с помощью браузера. Пример вывода:

```
Please point your browser to following url:
https://webexapis.com/v1/authorize?response_type=code&client_id=
C93071de24cda52557c925dc0341d2cb6e1c736579b4d58b93c94edb64eacf84b&
redirect_uri=https%3A%2F%2Fexample.organization.local%3A9090%2Fauth&scope=
spark-compliance%3Aevents_read%20spark-compliance%3Amessages_read%20
spark-compliance%3Arooms_read%20spark%3Apeople_read%20spark-admin%3A
people_read%20spark-compliance%3Amemberships_read%20spark%3Akms&state=
```

```
c8f61ebb8f484ee68df09754763416bc  
Waiting for request on https://example.organization.local:9090/auth
```

Следует перейти по первой, «длинной» ссылке.

10. Проверить владельца файла **token.json**, выполнив команду следующего вида:

```
# ls -l <path>
```

Файлом должны владеть пользователь **dozor** и группа **dozor**. Если это не так, то сменить владельца файла **token.json**, выполнив команду следующего вида:

```
# chown dozor:dozor <path>
```

где **<path>** – путь, заданный в шаге 8 (например, **/opt/dozor/share/im-crawler/token.json**).

11. Перейти в GUI KEO DLP и открыть раздел **Система > Основные настройки > Работа системы**, пролистать до секции **Загрузка сообщений из корпоративных мессенджеров**. Задать значения следующих параметров:

- **Настройки прокси-сервера** – если для доступа к адресу **https://webexapis.com/** требуется соединение через прокси-сервер, то выбрать значение **Настройка прокси-сервера**, и в раскрывшемся списке задать значения параметров:
  - **Адрес прокси-сервера** – адрес (IP или FQDN) прокси-сервера, через который предполагается соединяться с узлом **webexapis.com**.
  - **Порт прокси-сервера** – номер порта, на котором этот прокси-сервер ожидает соединения.
  - **Логин для Basic-аутентификации на прокси-сервере** – имя учетной записи пользователя для авторизации на прокси-сервере.
  - **Пароль для Basic-аутентификации на прокси-сервере** – пароль этой учетной записи.
- **Файл с токеном доступа** – указать путь **<path>**, заданный в шаге 8.
- **Client ID** – указать значение **CLIENT\_ID**, сохраненное в шаге 6.
- **Client Secret** – указать значение **CLIENT\_SECRET**, сохраненное в шаге 6.

12. При необходимости, задать дополнительные параметры конфигурации. Для этого открыть раздел **Система > Расширенные настройки > Краулер**, пролистать до секции **Загрузка сообщений из корпоративных мессенджеров**, и задать значения следующих параметров:

- **Уровень журналирования** – выбрать требуемую степень подробностей журналируемых данных.
- **Время актуальности данных в кэше** – периодичность в секундах, с которой обновляется список участников беседы, для которой выполняется перехват сообщений. Значение по умолчанию – 3600 (один час).
- **Каталог для временных файлов** – задать каталог для временных файлов сервиса.

- **Максимальный размер загружаемых файлов** – максимальный размер файлов в мегабайтах, передаваемых в беседах, для которых будет выполняться загрузка и фильтрация по политике безопасности. KEO DLP не обрабатывает файлы размером более 500 МБ. Значение по умолчанию – 100.

#### Примечание

*Существует возможность ограничить максимальный размер передаваемых файлов на стороне мессенджера Webex и таким образом обеспечить загрузку и фильтрацию всех переданных в беседах файлов.*

- **Загружать историю сообщений за последние** – задать промежуток времени, за который требуется загрузить сообщения из истории. Возможные значения: **1 день, 5 дней, 10 дней, 30 дней, 60 дней, 90 дней, Все возможные**.
- **Сообщения и файлы** – выбрать один из двух вариантов:
  - **Только ранее не загруженные** – при загрузке истории сообщений будут учтены сообщения, уже имеющиеся в архиве, и повторно загружены не будут. Такой вариант подходит при увеличении выбранного периода истории.
  - **Все за выбранный период** – сообщения за выбранный период истории будут загружены независимо от того, были ли они помещены в архив ранее. Такой вариант можно применить при необходимости перефильтрации сообщений в архиве.
- **Интервал обновления** – периодичность в секундах, с которой KEO DLP опрашивает сервер Webex в ожидании новых сообщений.

#### Внимание!

*Производителем корпоративного мессенджера установлено ограничение на количество запросов в единицу времени, отправляемых на сервер Webex. При достижении предела сообщения перестают загружаться в KEO DLP. По умолчанию таймаут загрузки сообщений с сервера действует в течение минуты, при этом производитель может установить более длительный период. По истечении этого времени загрузка сообщений возобновляется.*

13. Нажать **Сохранить, Применить**.

14. Перейти в раздел **Система > Узлы и роли** и назначить выбранному узлу роль **Краулер: корпоративные мессенджеры**. Этот узел также должен иметь роль **Фильтр почтового потока**.

#### Внимание!

*Серверы Cisco Webex, от которых KEO DLP получает сообщения, испытывают переменную нагрузку в зависимости от времени суток, дня недели и других обстоятельств (в том числе непредсказуемых), вследствие чего время между возникновением сообщения в беседе и его попаданием в KEO DLP может составлять от нескольких минут до 24 часов.*

---

## 8.15. Настройка передачи информации в пользовательский сервер Zabbix

По умолчанию slave-узлы кластера KEO DLP принимают соединения от сервера мониторинга Zabbix, который функционирует на master-узле. Чтобы slave-узлы принимали соединения от пользовательского сервера, необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование > Мониторинг > Агенты мониторинга**.

2. Задать значения параметров:

- **Порт** – 10050.
- **Пользовательский сервер мониторинга (для пассивных проверок)** – пользовательские серверы мониторинга, используемые для пассивных проверок, т.е. упрощенных запросов. В качестве значения задается список перечисленных через запятую IP-адресов или имен узлов, допускается использование маски CIDR в формате **X.X.X.X/N**.

Примеры значений:

```
127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.domain
```

- **Пользовательский сервер мониторинга (для активных проверок)** – пользовательские серверы мониторинга, используемые для активных проверок, которые требуют более сложной обработки. В качестве значения задается список перечисленных через запятую пар **IP-адрес:порт** или **Имя узла: порт**. Не допускается использование пробелов. Если значение не указано, активные проверки отключены.
3. Для сбора дополнительной статистики по параметрам из каталога **/etc/zabbix/zabbix\_agentd.d/** установить флажок **Читать системную конфигурацию zabbix-agent (/etc/zabbix/zabbix\_agentd.d/)**.
4. Нажать **Сохранить** и **Применить**.

Чтобы получать статистику по показателям, проверка которых по умолчанию не предусмотрена в сервере мониторинга Zabbix, следует создать пользовательские параметры **Userparameter**.

### Примечание

*За рекомендациями относительно настройки **Userparameter** следует обращаться к руководству по Zabbix.*

### Примечание

*Созданные пользователем параметры **Userparameter** не будут работать, если конфигурационные файлы с их описанием отсутствуют в каталоге **/etc/zabbix/zabbix\_agentd.d**.*

---

При добавлении дублирующихся **Userparameter** пользовательский сервер Zabbix не будет работать.

---

## 8.16. Настройка распознавания графических объектов

Для корректного функционирования сервиса распознавания графических объектов необходимо, чтобы процессор поддерживал набор инструкций **avx**, **avx2** и **avx512**. Проверить наличие этой поддержки можно с помощью следующей команды:

**# grep avx /proc/cpuinfo**

Вывод команды должен быть непустым.

### Внимание!

Сервис **god-server** работает на серверах с поддержкой CPU/GPU и не работает на серверах с поддержкой QEMU. Изображения формата **JPEG2000** не обрабатываются.

Для настройки распознавания графических объектов необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Узлы и роли** и назначить одному из узлов роль **Распознавание графических объектов**.

### Внимание!

Настоятельно рекомендуется использовать сервер с графическими процессорами. Чем больше графических процессоров будет на сервере – тем производительнее будет сервис распознавания графических объектов. При отсутствии сервера с графическими процессорами следует выделить сервер с наибольшим количеством запаса производительности центрального процессора.

2. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Обработка сообщений**.
3. В секции **Сервис фильтрации сообщений** задать значение параметра **Таймаут при взаимодействии с сервером определения графических объектов** равным 30.
4. В секции **Сервис определения графических объектов** задать значения параметров:
  - **Локальный порт, на котором сервер будет принимать соединения** – 9303.
  - **Максимальное количество обработчиков, выполняющих распознавание** – количество экземпляров обработчика, одновременно выполняющих распознавание графических объектов. Для каждого экземпляра организуется очередь сообщений для обработки, максимальное количество сообщений в очереди – 100. Значение по умолчанию: 0 (количество экземпляров обработчика будет равно количеству ядер процессора).



- 
- **Количество GPU** – количество графических процессоров, используемых для распознавания графических объектов. Значение по умолчанию: 0 (будут использованы все графические процессоры сервера).
  - **Уровень журналирования** – включить при необходимости диагностики работы сервиса.
  - **Каталог для временных файлов** – оставить значение `/data/temp/god`.
  - **Настройки ограничений на параметры графических изображений** – настроить исходя из объема передаваемых данных.

#### **Внимание!**

*Максимальное ограничение на объем файлов изображений – 100 МБ, даже если задано значение выше или не задано вовсе.*

#### **Примечание**

*Подробное описание параметров конфигурации сервиса распознавания графических объектов приведено в документе *Руководство системного администратора*, приложение *Параметры конфигурации KEO DLP*.*

5. Перейти в раздел GUI **Политика > Инструменты > Графические шаблоны** и меню действий с этим разделом выбрать пункт **Добавить** ([Рис.8.8](#)).
6. В открывшемся окне ввести название шаблона (например, **Все печати**) и нажать кнопку **Сохранить** ([Рис.8.8](#)).

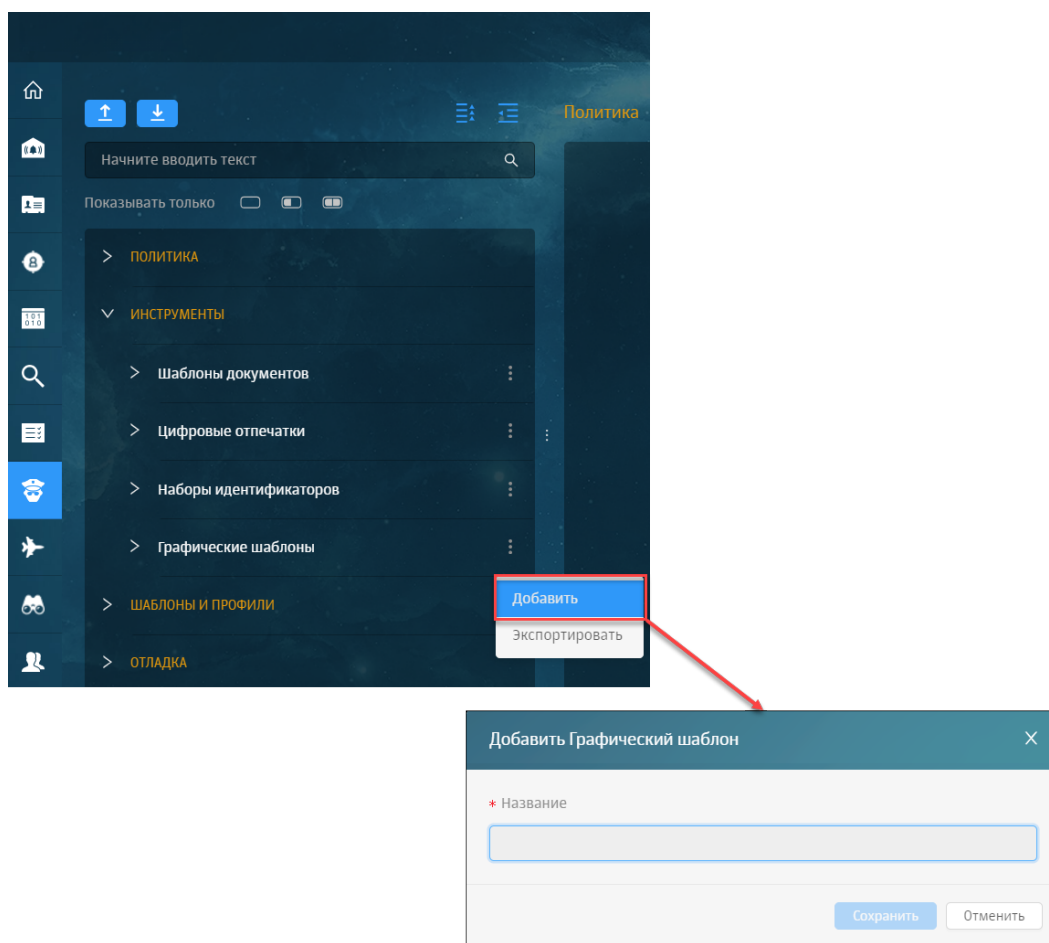


Рис. 8.8. Создание графического шаблона

7. В правой части экрана выбрать режим проверки, указать типы и минимальное количество объектов, необходимое для срабатывания условия политики ([Рис.8.9](#)). Нажать **Сохранить**.

Инструменты / Графические шаблоны / Все печати

Сохранить [v] [i] Применить политику

Режим проверки [v]

| Тип объекта                                                   | Минимальное количество |
|---------------------------------------------------------------|------------------------|
| <input type="checkbox"/> Круглая печать                       | 1                      |
| <input type="checkbox"/> Треугольная печать                   | 1                      |
| <input type="checkbox"/> Паспорт РФ                           | 1                      |
| <input type="checkbox"/> Банковская карта (лицевая сторона)   | 1                      |
| <input type="checkbox"/> Банковская карта (оборотная сторона) | 1                      |
| <input type="checkbox"/> Чертеж со штампом по ГОСТ            | 1                      |

Рис. 8.9. Пример настройки графического шаблона

- В меню действий с разделом GUI Политика > Политика > Условия выбрать пункт **Добавить** ([Рис.8.10](#)).
- В открывшемся окне ввести название условия (например, **Условие для печатей**) и нажать кнопку **Сохранить** ([Рис.8.10](#)).

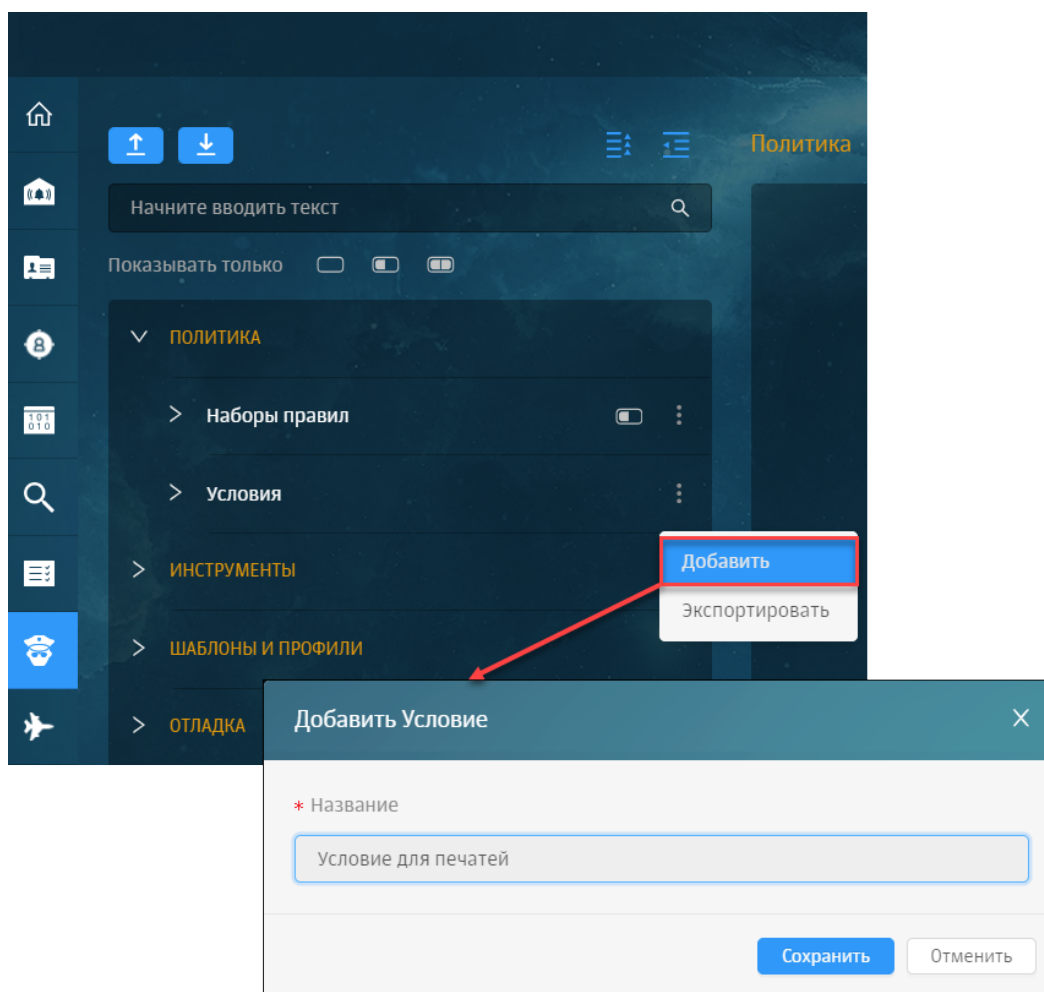


Рис. 8.10. Создание условия

10. В правой части экрана задать элементы условия ([Рис.8.11](#)), например:

- **Графический шаблон: Результат проверки**
- **Соответствует**
- **Все печати**

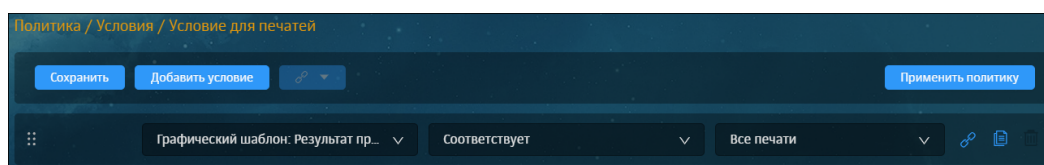


Рис. 8.11. Настройка условия

11. Нажать кнопку **Сохранить** ([Рис.8.11](#)).

12. В меню действий с разделом GUI **Политика > Политика > Наборы правил** выбрать пункт **Добавить** ([Рис.8.12](#)).

13. В открывшемся окне ввести название набора правил (например, **Правило для печатей**) и нажать кнопку **Сохранить** ([Рис.8.12](#)).

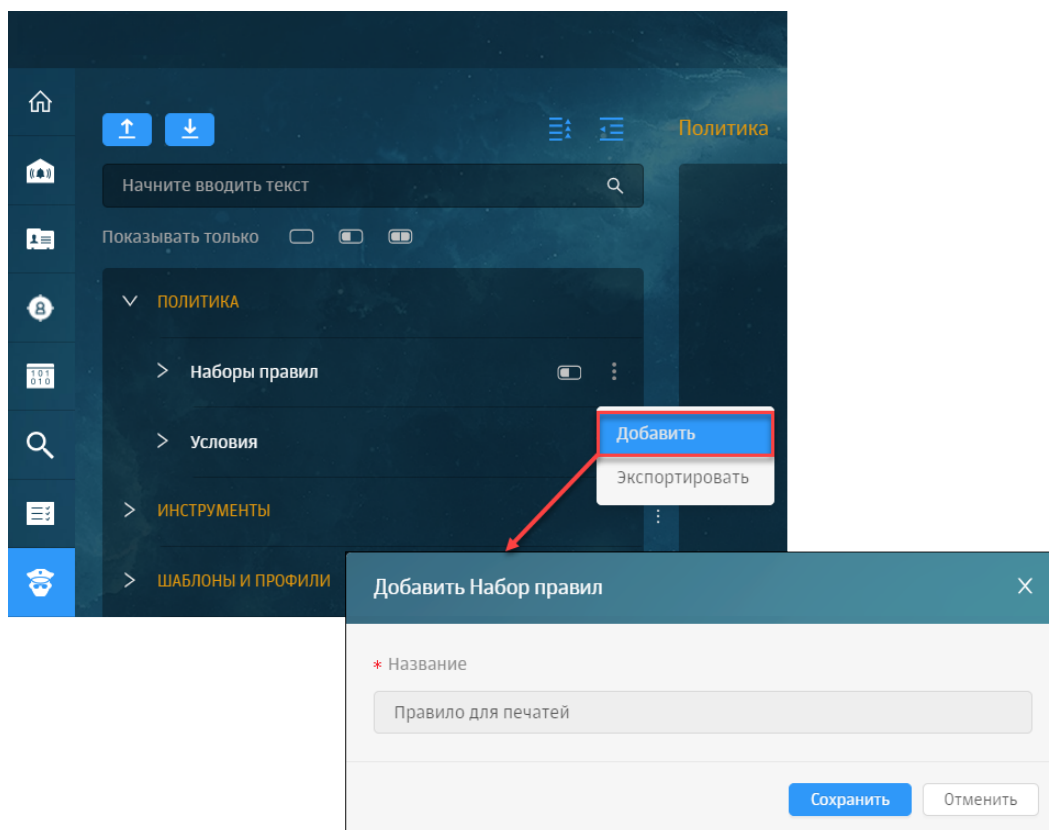


Рис. 8.12. Создание набора правил

14. В правой части экрана указать элементы правила ([Рис.8.13](#)):

- Название правила: **Правило для печатей**;
- Если: **Условие для печатей**;
- то: **Поместить в архив / Поместить в архив / Выполнить**.

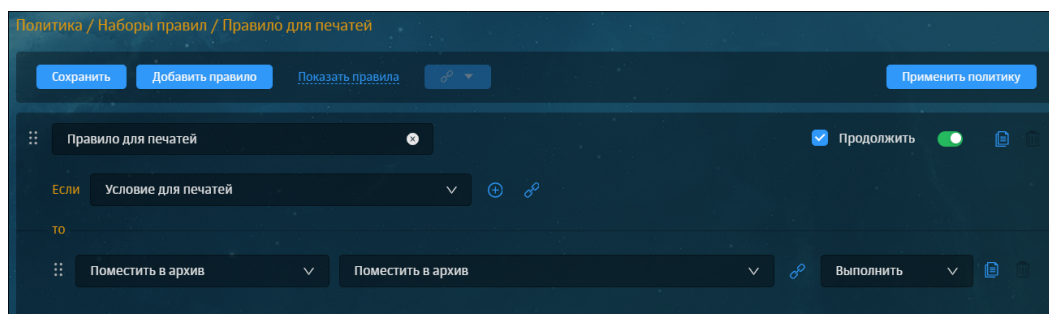


Рис. 8.13. Настройка набора правил "Управление печатями"

15. Нажать **Сохранить**, **Применить политику**.

---

## 8.17. Настройка распознавания речи

Для корректного функционирования сервиса распознавания речи необходимо, чтобы процессор поддерживал набор инструкций **avx**, **avx2** и **avx512**. Проверить наличие этой поддержки можно с помощью следующей команды:

```
# grep avx /proc/cpuinfo
```

Вывод команды должен быть непустым.

### Внимание!

Сервис **stt-server** работает на серверах с поддержкой CPU/GPU и не работает на серверах с поддержкой QEMU.

Для настройки распознавания речи необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Узлы и роли** и назначить одному из узлов роль **Распознавание речи**.

### Внимание!

Настоятельно рекомендуется использовать сервер с графическими процессорами. Чем больше графических процессоров будет на сервере – тем производительнее будет сервис распознавания речи. При отсутствии сервера с графическими процессорами следует выделить сервер с наибольшим количеством запаса производительности центрального процессора.

2. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Обработка сообщений**.
3. В секции **Сервис распознавания речи** задать значения параметров:
  - **Локальный порт**, на котором сервер будет принимать соединения – 9304.
  - **Максимальное количество обработчиков, выполняющих распознавание** – количество экземпляров обработчика, одновременно выполняющих распознавание речи. Для каждого экземпляра организуется очередь сообщений для обработки, максимальное количество сообщений в очереди – 100. Значение по умолчанию: 1.
  - **Количество GPU** – количество графических процессоров, используемых для распознавания речи. Значение по умолчанию: 0 (будут использованы все графические процессоры сервера).
  - **Уровень журналирования** – включить при необходимости диагностики работы сервиса.
  - **Каталог для временных файлов** – оставить значение **/data/temp/stt**.
4. Нажать **Сохранить**.

- 
5. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование системы > Общее** и в секции **Общие настройки системы** задать значение параметра **URL для формирования ссылок на систему**.

#### Примечание

*Подробное описание параметров конфигурации сервиса распознавания речи приведено в документе **Руководство системного администратора**, приложение **Параметры конфигурации KEO DLP**.*

6. Нажать **Сохранить** и **Применить**.

## 8.18. Настройка сервиса интеграции

В KEO DLP реализован сервис интеграции, предоставляющий единую точку входа для взаимодействия с внешним ПО. Текущая реализация позволяет внешнему ПО применять политику фильтрации, работать со списками слов, управлять событиями информационной безопасности, а также выполнять другие действия. В дальнейших релизах спектр возможностей будет расширяться.

Для работы сервиса интеграции требуется соответствующая лицензия.

Сервис интеграции является внутренним сервисом KEO DLP и пользуется доверенным доступом к данным. Сервис интеграции не связан с именами учетных записей KEO DLP и их паролями, поэтому настоятельно рекомендуется учитывать следующее:

- При использовании сервиса интеграции следует разрешить порт, назначенный этому сервису (по умолчанию – 33033) только тем узлам, которые будут участвовать во взаимодействии.
- При использовании сервиса интеграции следует использовать интеграционные ключи (см. ниже) во избежание несанкционированного доступа.
- Любой сервер KEO DLP, которому назначена роль **Сервер интеграции**, является точкой доступа. Не назначайте эту роль тем серверам, на которых не предполагается использовать функциональность сервиса интеграции.
- При использовании сервиса интеграции следует запретить выбранный сетевой порт (см. ниже) на всех узлах сетевой инфраструктуры организации, на которых не предполагается использование сервиса интеграции.

Для запуска сервиса интеграции необходимо назначить одному или нескольким узлам роль **Сервер интеграции**. После этого необходимо перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Вспомогательные сервисы** и в секции **Сервис интеграции** задать значения параметров:

- **Вывод отладочной информации** – включить, если требуется вывод отладочной информации о работе сервиса интеграции в его журнал.
- **Порт сервиса интеграции** – задать порт, на котором сервис интеграции будет ожидать соединения с внешним клиентом. Следует убедиться, что этот порт не закрыт никаким сетевым ПО. Значение по умолчанию: 33033.

- 
- **Использовать защищенное соединение** – рекомендуется оставить включенным. В этом случае сервис интеграции будет принимать запросы от внешнего клиента только в случае установки защищенного соединения по протоколу HTTPS.
  - **Таймаут взаимодействия с веб-сервером** – таймаут в секундах, в течение которого сервис интеграции ожидает ответа от веб-сервера на запрос, полученный от внешнего клиента. Если веб-сервер не успеет ответить за это время – сервис интеграции возвращает внешнему клиенту ошибку HTTP 502.
  - **Таймаут взаимодействия с сервером лицензирования** – таймаут в секундах, в течение которого сервис интеграции ожидает ответа от сервера лицензирования. Если сервис активен, то он запрашивает лицензию раз в час. Если сервис не получил лицензию и/или неактивен, то он запрашивает лицензию раз в пять минут. Неактивный сервис не принимает запросов от внешнего клиента.
  - **Интеграционные ключи** – при желании, добавить одну или несколько строк, содержащих произвольные последовательности символов. API сервиса интеграции будет ожидать одну из этих строк от внешнего клиента для его авторизации.

Также в секции JVM сервиса интеграции можно задать значения параметров:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса интеграции.
- **Снимать дампы памяти при критических ошибках** – включить, если требуется сохранение дампа памяти сервиса интеграции в случае ошибки исчерпания памяти.
- **Каталог для записи дампов памяти** – путь к каталогу для записи дампов памяти.

С описанием API можно ознакомиться в интерфейсе KEO DLP по адресу вида **https://api\_gateway\_FQDN:port/docs** либо **https://api\_gateway\_IP:port/docs**, где:

- **api\_gateway\_FQDN** – FQDN узла с ролью **Сервис интеграции**;
- **api\_gateway\_IP** – IP узла с ролью **Сервис интеграции**;
- **port** - порт, назначенный сервису интеграции (по умолчанию - 33033).

В этом же интерфейсе можно выполнять запросы к сервису интеграции в интерактивном режиме. Например, для применения политики следует раскрыть группу запросов **Политика**, раскрыть запрос **Применить политику**, нажать **Try it out** и нажать **Execute**.



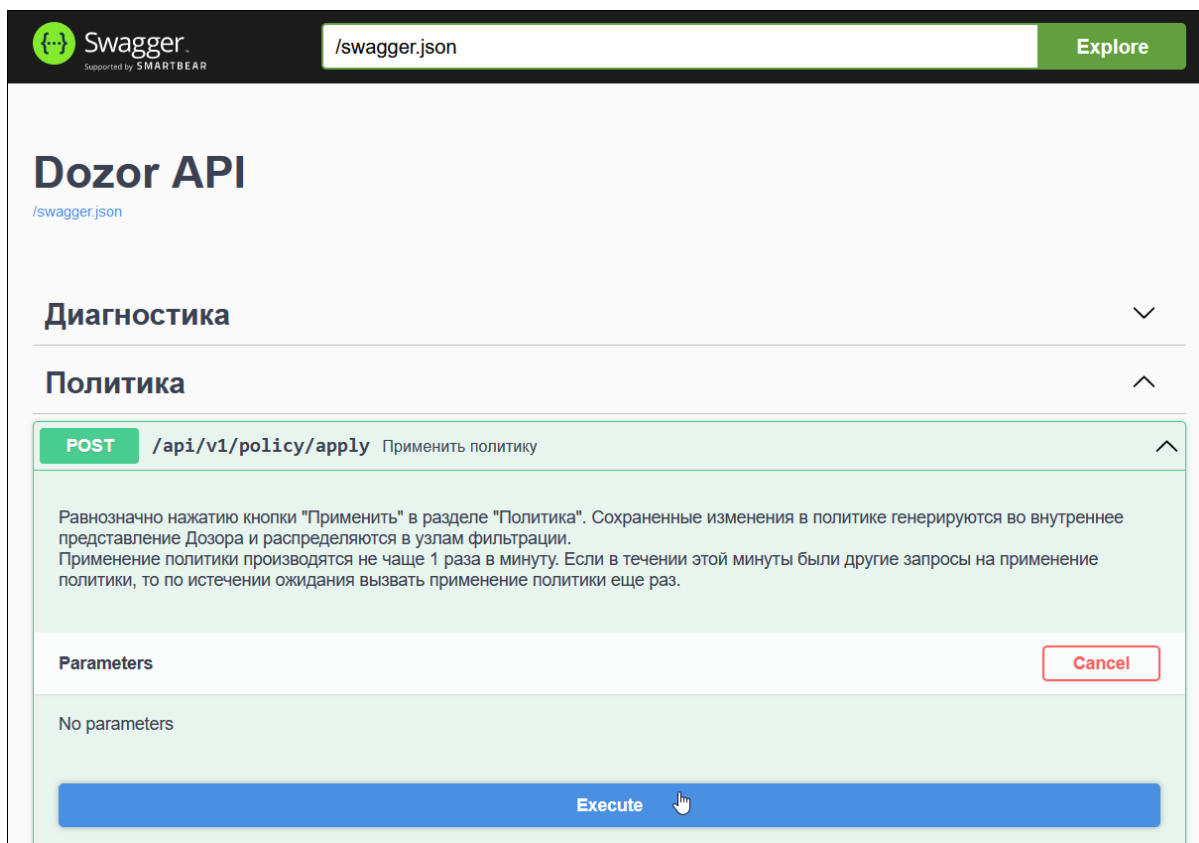


Рис. 8.14. Запрос Применить политику

После выполнения запроса на экран будет выведена следующая информация:

- **Curl** – текст запроса, с помощью которого можно выполнить этот же запрос из командной строки, используя утилиту **cURL**.
- **Request URL** – адрес, на который внешний клиент может отправить запрос с помощью каких-либо других средств.
- **Server response** – ответ сервера на отправленный запрос. Содержит стандартный код состояния HTTP и подробности:
  - **Response body** – тело ответа. Выводится, если предусмотрено синтаксисом ответа сервера на запрос.
  - **Response headers** – заголовки ответа.
- **Responses** – список кодов состояния HTTP и описаний всех возможных ответов сервера на запрос.

Responses
Response content type
application/json

Curl

```
curl -X 'POST' \
'https://10.201.28.136:33033/api/v1/policy/apply' \
-H 'accept: application/json' \
-d ''
```

Request URL

```
https://10.201.28.136:33033/api/v1/policy/apply
```

Server response

| Code | Details                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------|
| 202  | Response headers <pre>content-length: 0 date: Wed, 19 Jul 2023 14:43:59 GMT server: Jetty(9.4.51.v20230217)</pre> |

Responses

| Code | Description                                                                          |
|------|--------------------------------------------------------------------------------------|
| 202  | Команда на изменение принята. <div> Example Value   Model <pre>"string"</pre> </div> |

Рис. 8.15. Результат выполнения запроса Применить политику

Для авторизации внешнего клиента сервисом интеграции можно использовать интеграционный ключ. Настоятельно рекомендуется задать такие ключи – для этого следует задать в конфигурации один или несколько таких ключей, как описано выше, после чего сервис интеграции будет ожидать один из ключей в качестве значения заголовка **Authorization: apikey** каждого запроса со стороны внешнего клиента, например:

```
Authorization: apikey WKOHqszQNav+GGFhcYtwZnSvN7cy21LC
```

Ключ можно создать любым доступным способом: придумать самостоятельно или сгенерировать аппаратно, например, с помощью команды вида:

**openssl rand -base64 24**

Пример вывода команды:

```
WKOHqszQNav+GGFhcYtwZnSvN7cy21LC
```

К полученному результату можно добавить какую-либо осмысленную часть, например, название организации.

Если не задать интеграционные ключи, то любой клиент, находящийся в одной сети с соответствующим сервером KEO DLP, для которого открыт соответствующий сетевой порт, сможет получить доступ к API этого сервера и выполнить на нем любые доступные действия, в том числе вредоносные.

Сервис интеграции имеет ограничение на количество входящих запросов от внешних клиентов – 100 запросов в минуту. При превышении количества запросов сервис отдает

---

ответ с кодом **429 Too Many Requests**. Следует учитывать это ограничение при разработке внешнего клиента сервиса интеграции.

Подробная справка об использовании сервиса интеграции приведена в документе *Описание API универсального интеграционного модуля*.

### 8.18.1. Настройка взаимодействия по протоколу mTLS

По умолчанию внешний клиент и сервис интеграции KEO DLP взаимодействуют по протоколу защиты транспортного уровня (TLS), когда внешний клиент может, но не обязан передавать сертификат при каждом запросе к сервису интеграции. При необходимости можно настроить взаимодействие между ними по протоколу взаимной защиты транспортного уровня (mTLS) – расширению TLS, обязывающему внешнего клиента передавать сертификат при каждом запросе к сервису интеграции KEO DLP.

За выбор TLS либо mTLS отвечает параметр **client-auth**, принимающий значения:

- false – внешний клиент и сервис интеграции взаимодействуют по TLS;
- true – по mTLS.

Для настройки взаимодействия по протоколу mTLS необходимо выполнить следующие действия:

1. Запустить интерпретатор команд shell на master-узле, выполнив команду:

```
# /opt/dozor/bin/shell
```

2. Проверить текущее значение параметра **client-auth**, выполнив команду:

```
# get-config global /api-gateway/api-gateway.edn/client-auth
```

Пример вывода, когда параметр **client-auth** имеет значение **false**:

```
/api-gateway/api-gateway.edn/client-auth: #f
```

3. Включить принудительный режим mTLS, выполнив команду:

```
# set-config global /api-gateway/api-gateway.edn/client-auth #t
```

На экран будет выведено следующее сообщение:

```
Writing new values file /data/repos/dozor/config-base.git/values.json ...
[master 0f09a2b] set-config --path /api-gateway/api-gateway.edn/client-auth --value #t
Author: DOZOR <dozor@local>
1 file changed, 1 insertion(+), 1 deletion(-)
```

4. Проверить, что параметр установился корректно, выполнив команду:

```
# get-config global /api-gateway/api-gateway.edn/client-auth
```

Пример вывода команды:

```
/api-gateway/api-gateway.edn/client-auth: #t
```

- 
5. Перейти на узел с ролью **Сервис интеграции** и перезапустить сервис **api-gateway**, выполнив команду:

```
# /opt/dozor/bin/dsctl restart api-gateway
```

6. Перейти во временный каталог (например, **/var/tmp/**), выполнив команду:

```
# cd /var/tmp
```

7. Создать в текущем каталоге файл с именем **client.cnf** и записать в него следующие данные вида:

```
# client.cnf
[req]
default_bits      = 2048
default_md        = sha256
prompt           = no
distinguished_name = req_distinguished_name
req_extensions    = req_ext

[req_distinguished_name]
countryName       = KZ
stateOrProvinceName = Almaty
localityName      = Almaty
0.organizationName = Test Corp
organizationalUnitName = IT
commonName        = example.organization.local
emailAddress      = admin@test.corp

[req_ext]
subjectAltName = @alt_names

[alt_names]
IP.1 = 192.0.2.255
DNS.1 = example.organization.local
```

Выделенные жирным значения параметров следует заменить на актуальные значения в организации:

- **countryName** – двухбуквенный код страны.
- **stateOrProvinceName** – регион.
- **localityName** – город.
- **0.organizationName** – название организации.
- **organizationalUnitName** – название подразделения, департамента и т. д.
- **commonName** – FQDN узла с ролью **Сервис интеграции**.
- **emailAddress** – контактный адрес электронной почты организации.
- **IP.1** – IP-адрес узла с ролью **Сервис интеграции**.
- **DNS.1** – FQDN узла с ролью **Сервис интеграции**.

- 
8. Создать в текущем каталоге файл с именем **client\_cert\_ext.cnf** и записать в него следующие данные:

```
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection
```

9. Сгенерировать закрытый ключ с помощью команды:

```
# openssl genrsa -out client.key.pem 4096
```

В результате выполнения команды на экран будет выведено следующее сообщение::

```
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
```

10. Сгенерировать запрос на подпись сертификата, выполнив команду:

```
# openssl req -new -key client.key.pem -out client.csr
```

11. Сгенерировать клиентский сертификат, выполнив команду:

```
# openssl x509 -req -in client.csr \
-CA /opt/dozor/etc/ssl/ca.crt \
-CAkey /opt/dozor/etc/ssl/ca.key \
-out client.cert.pem \
-CAcreateserial \
-sha256 \
-extfile client_cert_ext.cnf
```

В результате выполнения команды на экране будет выведено сообщение:

```
Signature ok
subject=/C=KZ/ST=Almaty/L=Almaty/O=Test
Corp/OU=IT/CN=example.organization.local/emailAddress=admin@test.corp
Getting CA Private Key
```

12. Добавить корневой сертификат в доверенные, выполнив команды:

```
# apt-get install -y ca-certificates
```

```
# cp /opt/dozor/etc/ssl/ca.crt /usr/local/share/ca-certificates/ca.dozor.crt
```

---

## # update-ca-certificates

13. Проверить подключение к сервису интеграции, выполнив команду вида:

```
# curl -v --cert ./client.cert.pem --key ./client.key.pem \
'https://example.organization.local:33033/api/v1/status'
```

подставляя FQDN узла с ролью **Сервис интеграции** вместо **example.organization.local**.

В случае успешно установленного соединения на экран будет выведена следующая информация следующего вида:

```
# curl --cert ./client.cert.pem --key ./client.key.pem
'https://example.organization.local:33033/api/v1/status'

{"time":"2024-10-16T11:20:36.029Z","started":"2024-10-16T07:54:55.804Z","uptime":12340225,"message":""}
```

14. Сгенерировать сертификат в PFX-формате, выполнив команду:

```
# openssl pkcs12 -inkey client.key.pem -in client.cert.pem -export -out client.pfx
```

В ходе выполнения команды необходимо указать пароль для экспорта (например: **secret**) и подтвердить его:

```
Enter Export Password:
Verifying - Enter Export Password:
```

15. Перейти в используемом браузере в раздел настройки сертификатов:

### Примечание

*Далее для примера был использован браузер Mozilla Firefox.*

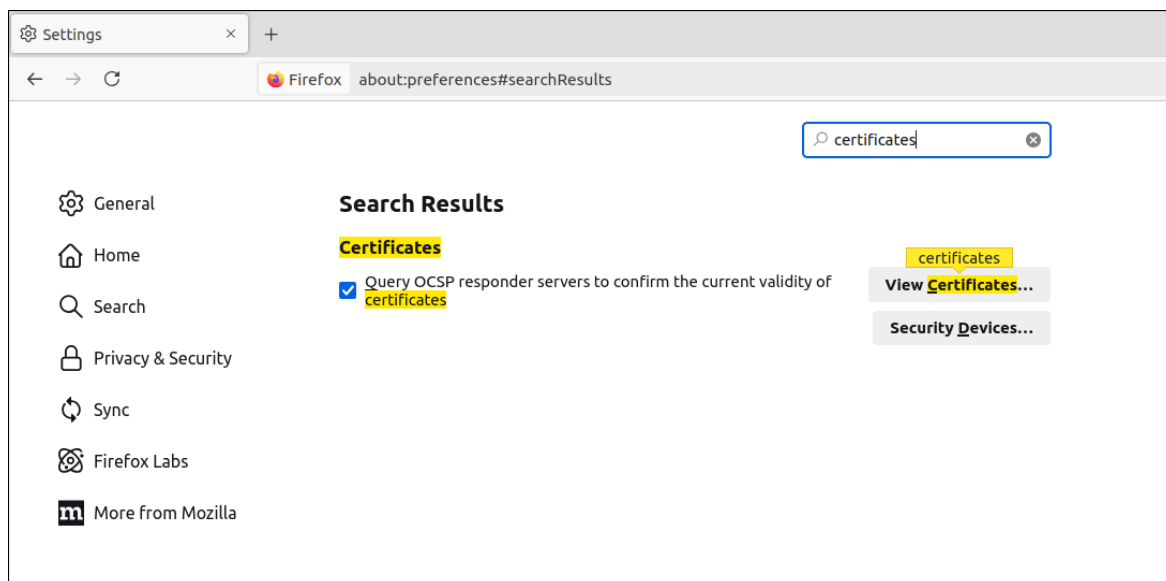


Рис. 8.16. Просмотр сертификатов в настройках браузера Mozilla Firefox

16. Импортировать созданный на шаге 14 файл **client.pfx** в хранилище сертификатов браузера, ввести пароль для экспорта:

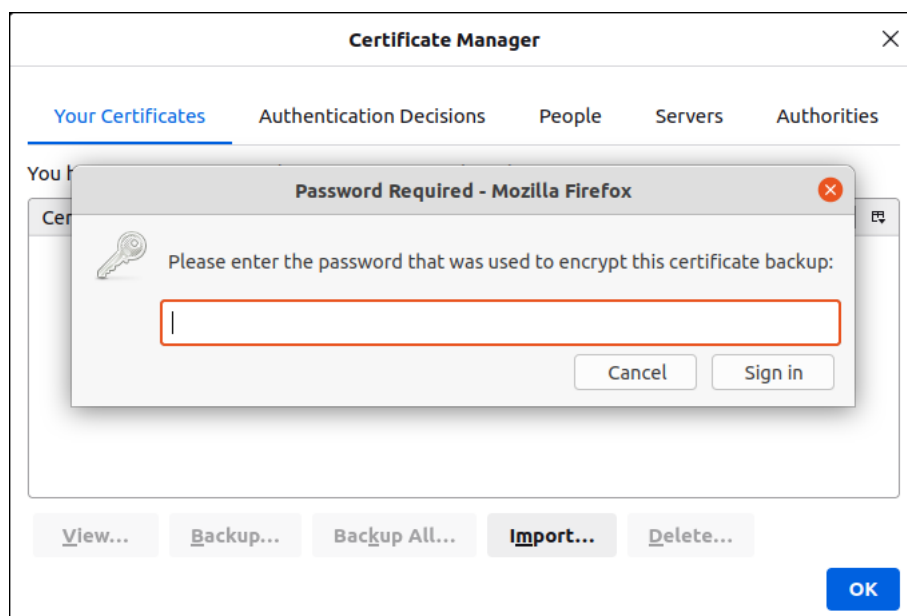


Рис. 8.17. Добавление сертификата в формате PFX в хранилище сертификатов браузера Mozilla Firefox

17. Импортировать файл **ca.crt** в хранилище сертификатов браузера:

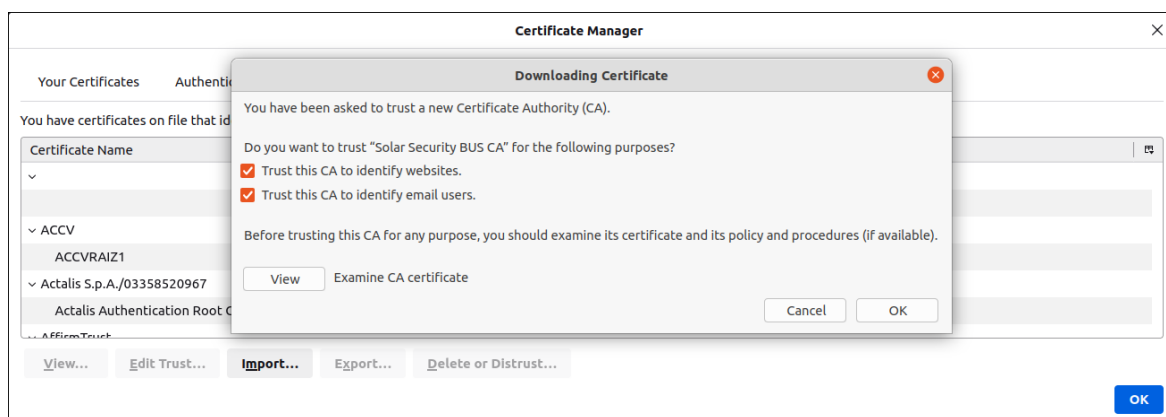


Рис. 8.18. Добавление сертификата в формате crt в хранилище сертификатов браузера Mozilla Firefox

18. Перейти в сервис интеграции по адресу вида **https://api\_gateway\_FQDN:port/docs** либо **https://api\_gateway\_IP:port/docs**, где:

- **api\_gateway\_FQDN** – FQDN узла с ролью **Сервис интеграции**;
- **api\_gateway\_IP** – IP узла с ролью **Сервис интеграции**;
- **port** – порт, назначенный сервису интеграции (по умолчанию - 33033).

и подтвердить выбор ранее добавленного сертификата для соединения с внешним клиентом:

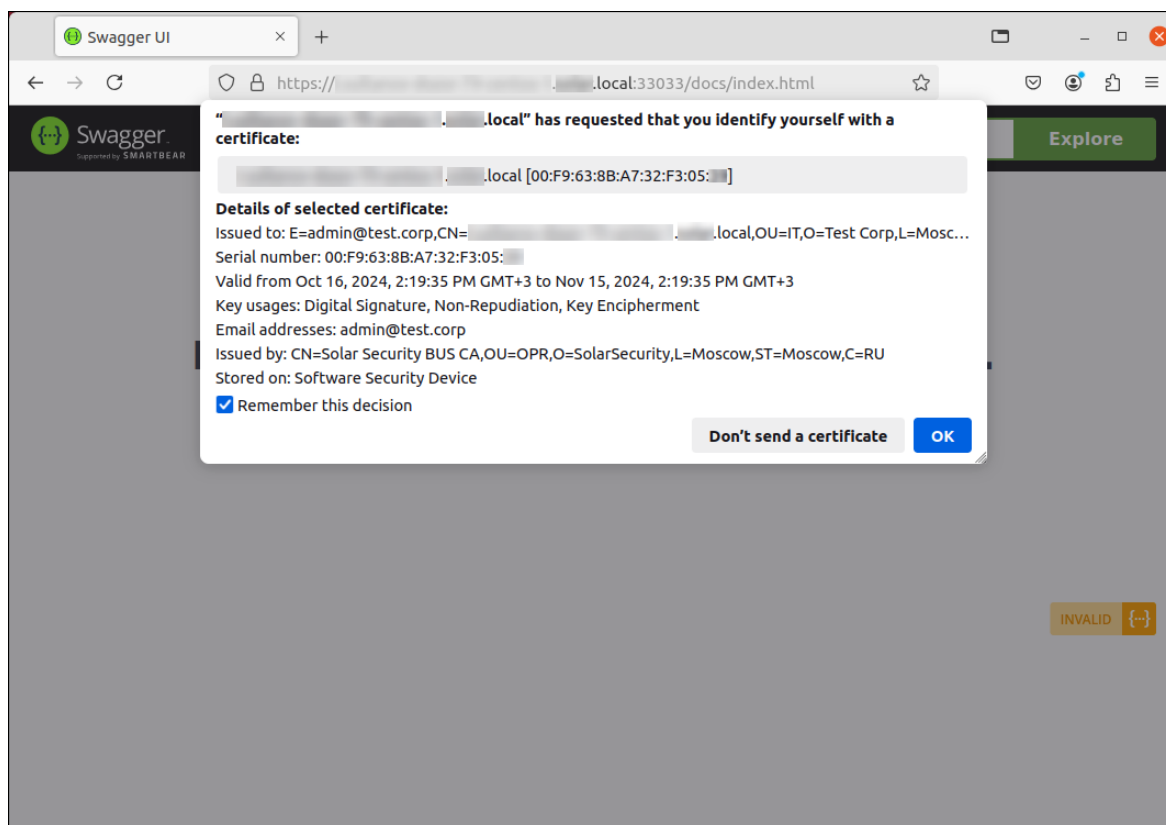


Рис. 8.19. Подтверждение выбора сертификата в сервисе интеграции KEO DLP



19. Просмотреть информацию о странице и убедиться, что установлено защищенное соединение:

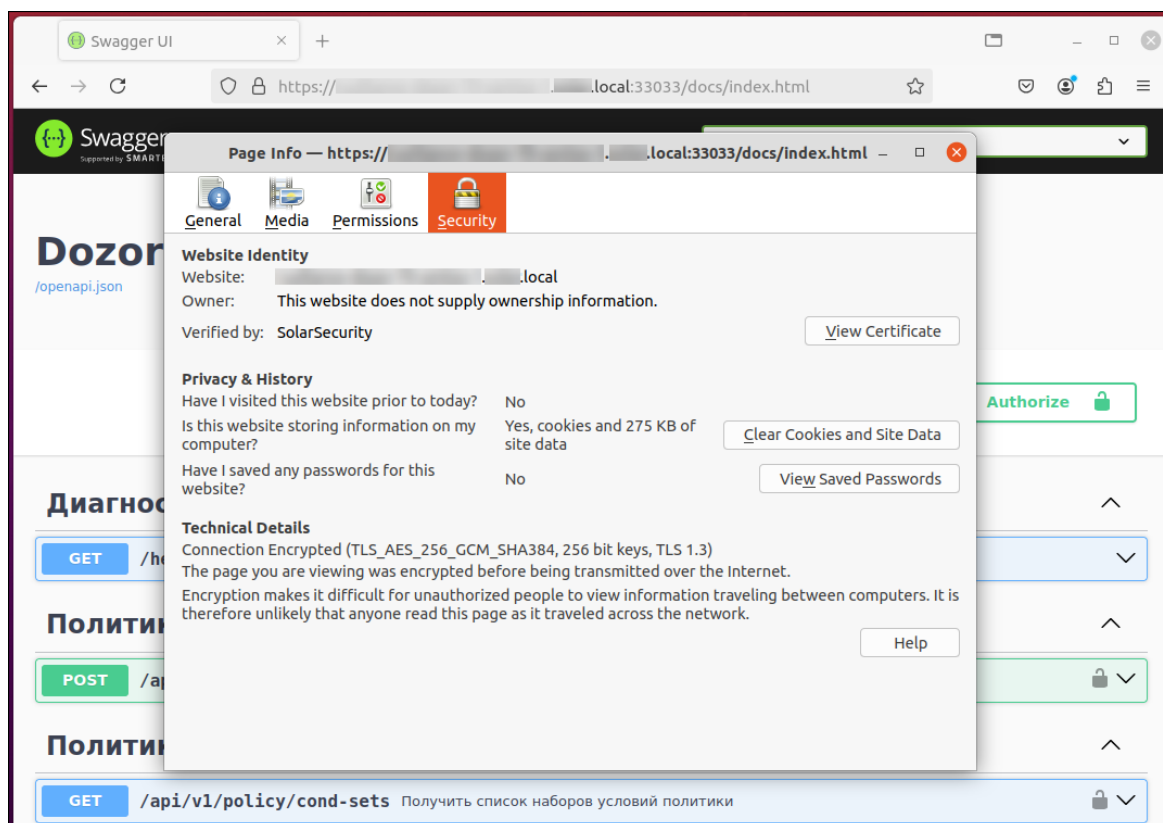


Рис. 8.20. Просмотр информации о соединении с сервисом интеграции KEO DLP

## 8.19. Выпуск сертификата организации для web-интерфейса

Если в организации имеется собственный УЦ, можно использовать его сертификат для установления соединения с GUI KEO DLP.

### Примечание

Если в организации имеется сертификат формата PFX, следует убедиться, что пароль для ключа вам известен. Для этого необходимо загрузить командную оболочку KEO DLP, а затем запросить информацию о сертификате, выполнив команды:

```
# sudo -i /opt/dozor/bin/shell
```

```
# openssl pkcs12 -in <cert.pfx> -info
```

где **<cert.pfx>** – имя сертификата с полным путем к нему. Во время выполнения команда запросит пароль для контейнера. После ввода пароля на экран будет выведена информация о контейнере. Затем будет запрошен пароль для ключа. При вводе правильного пароля для ключа на экран будет выведена информация о ключе. Если пароль неизвестен – следует либо запросить пароль у выпускающего подразделения организации, либо перевыпустить сертификат. Этот пароль должен содержать только буквы и/или цифры. После этого

следует конвертировать сертификат в формат JKS, выполнив команду в каталоге с этим сертификатом:

```
# keytool -importkeystore -srckeystore <cert.pfx> -srcstoretype pkcs12 -destkeystore WEB.jks -deststoretype JKS
```

Во время выполнения команда запросит установить пароль для нового контейнера. Следует установить пароль, совпадающий с паролем для ключа. После этого необходимо перейти к шагу [15](#).

Для выпуска сертификата организации необходимо выполнить следующие действия на master-узле KEO DLP:

1. Загрузить командную оболочку KEO DLP, выполнив команду:

```
~$ /opt/dozor/bin/shell
```

2. Открыть CLI и перейти во временный каталог (например, `/var/tmp/`), выполнив команду:

```
# cd /var/tmp
```

3. Перед тем как создавать сертификат пользователя, сгенерировать закрытый ключ для него. Для этого необходимо запустить программу openssl с указанием имени файла создаваемого ключа:

```
# openssl genrsa -out dz.key -aes256 2048
```

В результате работы на экран будет выведено следующее сообщение:

```
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for dz.key:
Verifying - Enter pass phrase for dz.key:
```

В ходе выполнения программы генерации на экран выводится приглашение ввести кодовое слово для создаваемого ключа – **Enter pass phrase for dz.key:**. Оно может состоять только из букв и/или цифр (специальные символы не допускаются). После чего необходимо дважды (второй раз для проверки) ввести с клавиатуры кодовое слово длиной не менее 4 символов (например: **123456**). Данное слово необходимо запомнить.

4. Создать в текущем каталоге файл с именем **openssl.cnf** и записать в него следующие данные:

```
[ req ]
req_extensions = v3_req
distinguished_name = req_distinguished_name
prompt=yes
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = KZ

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Almaty
```

```

localityName          = Locality Name (eg, city)
localityName_default  = Almaty

0.organizationName    = Organization Name (eg, company)
0.organizationName_default  = Organization

organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = Dept

commonName            = Common Name (eg, your name or your server's hostname)
commonName_default    = proxy.org.com

emailAddress          = Email Address
emailAddress_default   = support@org.com

[ v3_req ]
basicConstraints = critical, CA:true
#basicConstraints = CA:false
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.0 = proxy.org.com
IP.0 = 192.168.10.15

```

Выделенные жирным значения параметров следует заменить на актуальные значения в организации:

- **countryName\_default** – двухбуквенный код страны.
  - **stateOrProvinceName\_default** – регион.
  - **localityName\_default** – город.
  - **organizationName\_default** – название организации.
  - **organizationalUnitName\_default** – название подразделения, департамента и т. д.
  - **commonName\_default** – FQDN master-узла.
  - **emailAddress\_default** – контактный адрес электронной почты организации.
  - **DNS.0** – FQDN master-узла.
  - **IP.0** – IP-адрес master-узла.
5. Сгенерировать запрос на подпись сертификата, выполнив команду:
- ```
# openssl req -new -key dz.key -out name.csr -config openssl.cnf
```
- В процессе выполнения команды система потребует ввести кодовое слово, заданное на шаге [3](#).
6. Зайти на портал УЦ Windows и нажать **Request a certificate**.

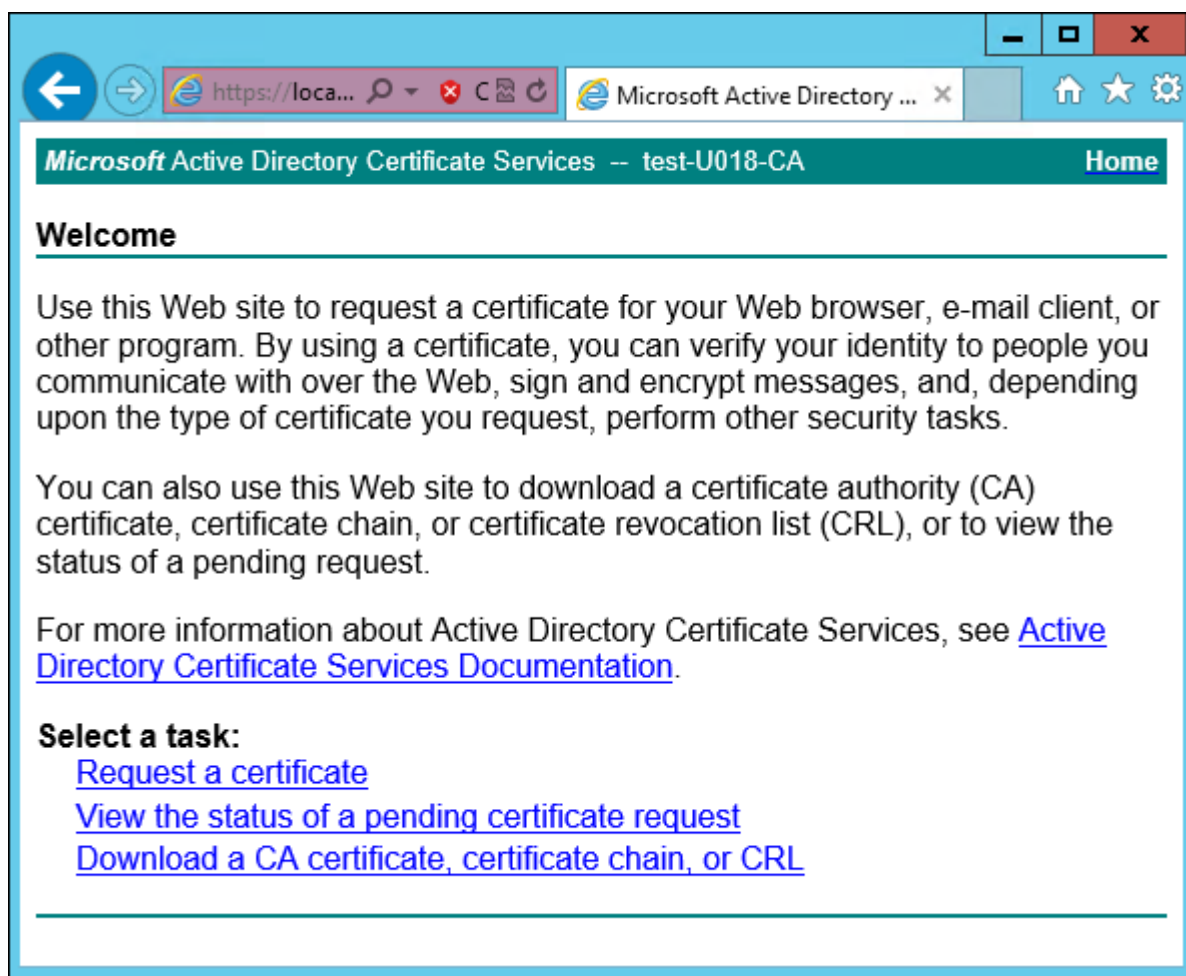


Рис. 8.21. Экран приветствия УЦ Windows

7. Нажать **advanced certificate request**.

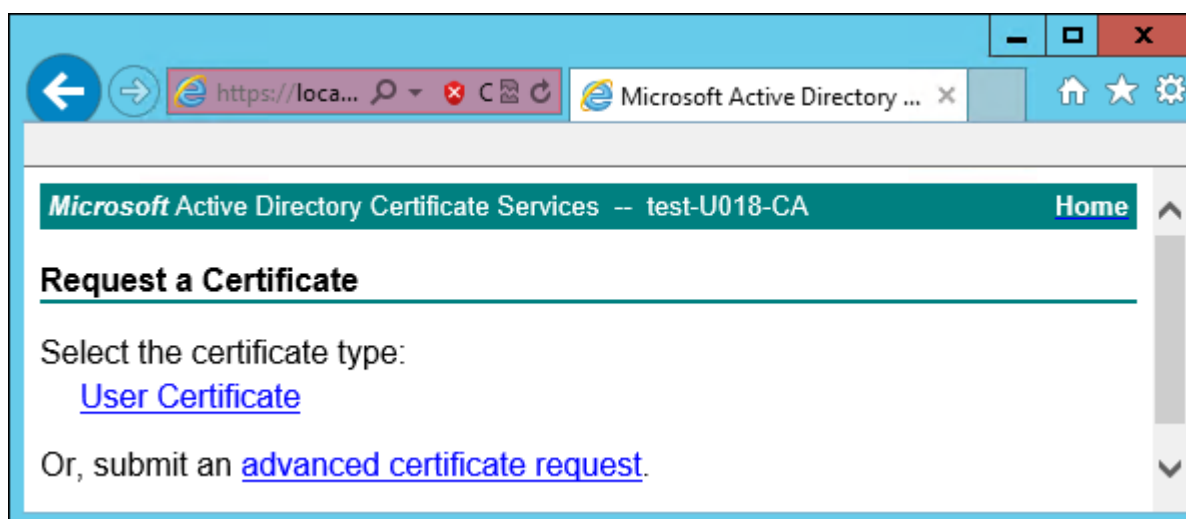


Рис. 8.22. Экран запроса сертификата

8. Нажать **Submit a certificate request by using....**

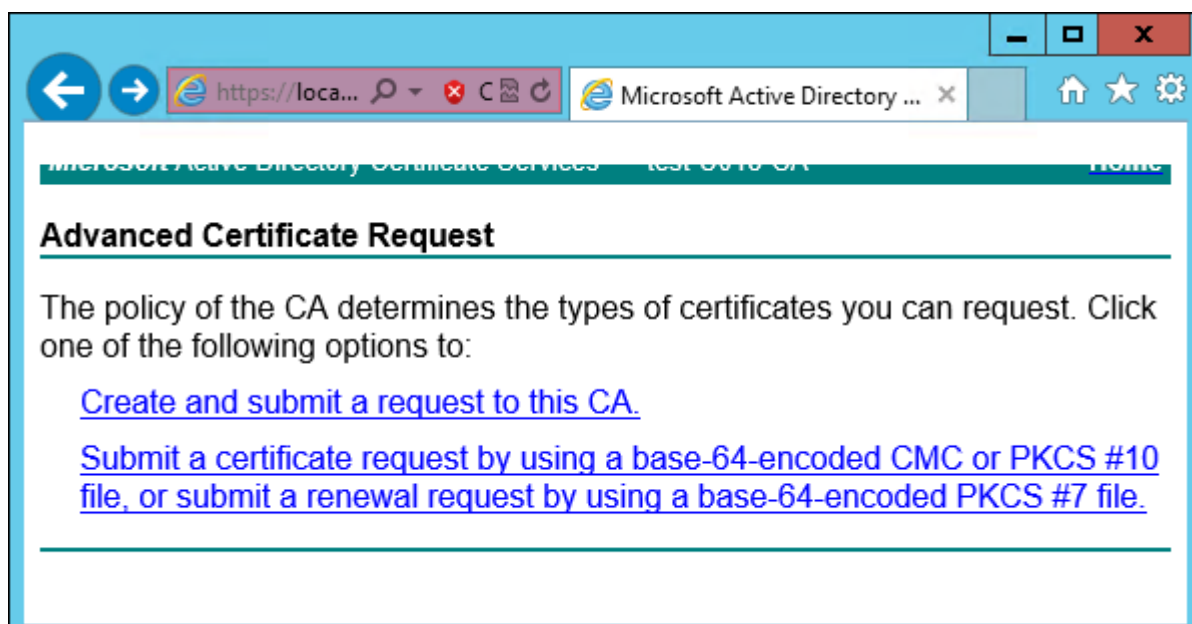


Рис. 8.23. Экран особого запроса сертификата

9. Выбрать шаблон сертификата **Веб-сервер** и вставить в поле **Base-64** содержимое файла, созданного на шаге **5**. Нажать **Выдать**.

Службы сертификации Active Directory (Microsoft) -- sns81-SNS81-AD-CA

### Выдача запроса на сертификат или на обновление сертификата

Чтобы выдать сохраненный запрос к ЦС, вставьте base-64-шифрованный поле "Сохраненный запрос".

**Сохраненный запрос:**

Base-64-шифрованный запрос сертификата (CMS или PKCS #10 или PKCS #7):

```

-----BEGIN CERTIFICATE REQUEST-----
MIIDIDCCAggCAQAwTELMakGA1UEBhMCU1UxCzAJ
DANNU0sxZzAVBgNVBAoMD1NvbGFyIFN1Y3VyaXR5
MBwGA1UEAwVZG96b3JtYXN0ZXIuc25zODEubGFil
AAOCAQ8AMIIBCgKCAQEA4wKJnJC2AoVPDQy34Pki
u+UFBN+nIe30Na3WLnfaU43Sr1+J/SGomYS1GESV:

```

**Шаблон сертификата:**

Веб-сервер

**Дополнительные атрибуты:**

Атрибуты:

Выдать >

Рис. 8.24. Экран атрибутов сертификата

10. Нажать **Download certificate**. Сохранить файл сертификата с именем **dz.cer** во временный каталог, выбранный на шаге 2.

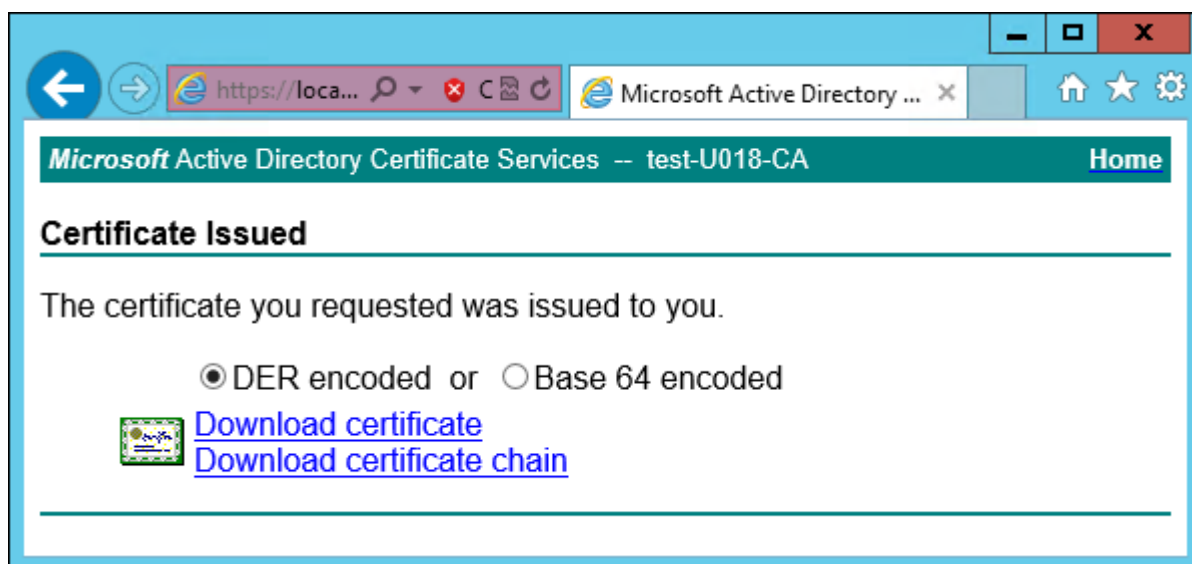


Рис. 8.25. Экран выдачи сертификата

11. Перейти на главную страницу портала УЦ и нажать **Download a CA certificate, certificate chain or CRL**. Сохранить сертификат УЦ с именем **ca.cer** в тот же каталог.

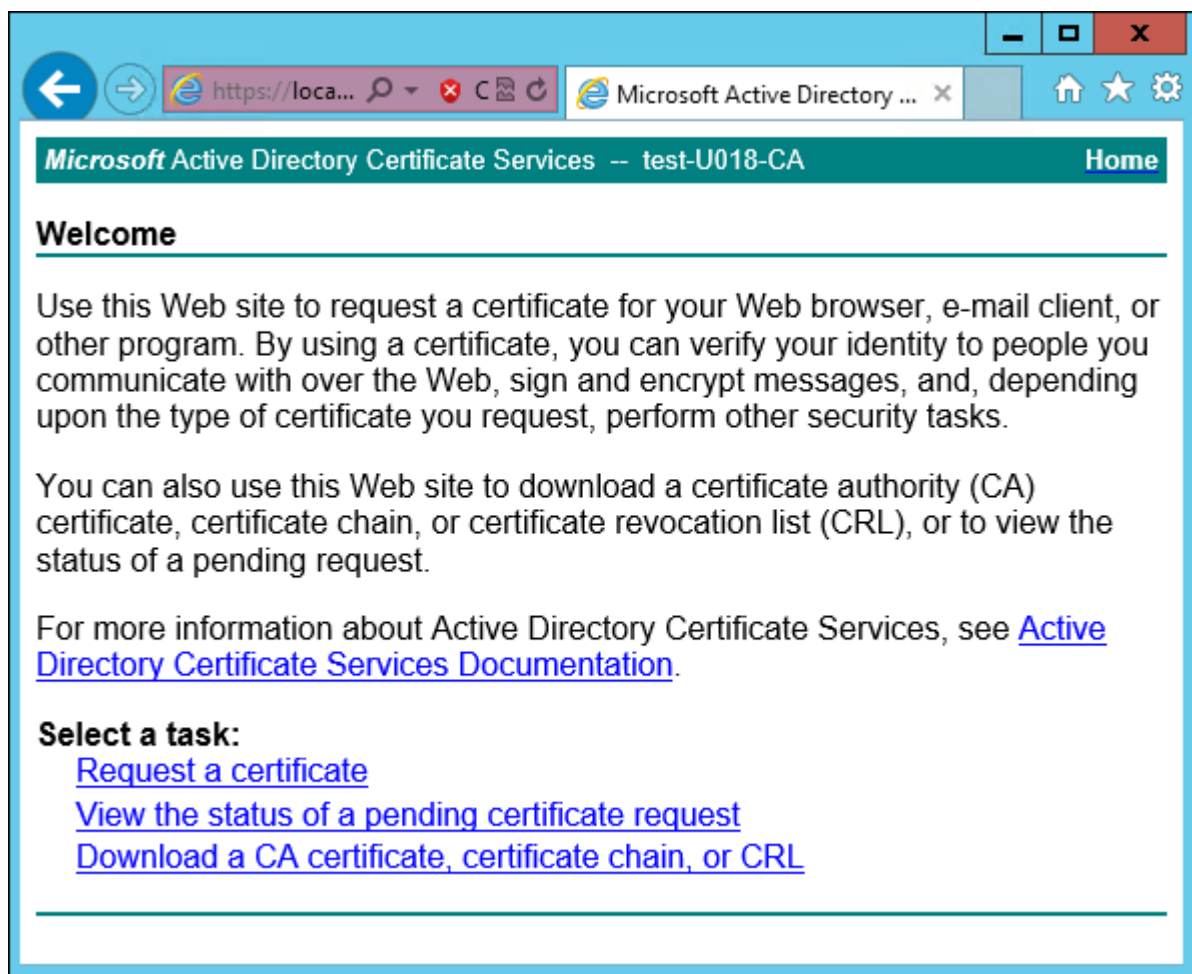


Рис. 8.26. Экран приветствия УЦ Windows

12. Вернуться в CLI KEO DLP, перейти в выбранный временный каталог и сконвертировать загруженные сертификаты в формат PEM, выполнив команды:

```
# openssl x509 -inform der -in dz.cer -out dz.pem
```

```
# openssl x509 -inform der -in ca.cer -out ca.pem
```

13. Объединить сертификаты и ключ в сертификат pkcs12, выполнив команду:

```
# openssl pkcs12 -export -out dz.p12 -inkey dz.key -in dz.pem -certfile ca.pem
```

В ходе выполнения команды будет предложено сначала ввести кодовое слово, заданное на шаге 3, а затем указать пароль для экспорта, например: **secret**, и подтвердить его:

```
Enter pass phrase for dz.key:
Enter Export Password:
Verifying - Enter Export Password:
```

14. Импортировать Java-хранилище сертификатов, выполнив команду вида:

```
# keytool -importkeystore -deststorepass <password> -destkeypass <password> -
destkeystore WEB.jks -srckeystore dz.p12 -srcstorepass <password>
```

где **<password>** – пароль для экспорта, указанный на предыдущем шаге.

15. Скопировать Java-хранилище в каталог KEO DLP, выполнив команду:

```
~$ sudo cp WEB.jks /opt/dozor/etc/ssl/
```

16. Сменить владельца хранилища, выполнив команду вида:

```
~$ sudo chown dozor:dozor /opt/dozor/etc/ssl/WEB.jks
```

17. Проверить, что сертификат находится в хранилище, выполнив команду вида:

```
# keytool -list -keystore /opt/dozor/etc/ssl/WEB.jks
```

О наличии сертификата в хранилище будет свидетельствовать вывод следующего вида:

```
1, Jul 10, 2020, PrivateKeyEntry,
Certificate fingerprint (SHA1): B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
```

18. Перейти в GUI, выбрать раздел **Система > Конфигурация > Расширенные настройки > Администрирование системы > Интерфейс**, перейти в секцию **Параметры сервера веб-интерфейса** и задать значения следующих параметров:

- Путь к хранилищу ключей и сертификатов – **/opt/dozor/etc/ssl/WEB.jks**
- Пароль к хранилищу ключей – **пароль**.

19. Перезапустить сервис **webserver**, выполнив в CLI следующие команды:



---

```
~$ sudo /opt/dozor/bin/shell
```

```
# dsctl restart webserver
```

## 8.20. Проверка работоспособности настроенного KEO DLP

Для проверки работоспособности архива сообщений установленного KEO DLP необходимо выполнить следующие действия:

1. Перезапустить на каждом из узлов процессы KEO DLP, выполнив от имени пользователя **root** следующую команду:

```
~$ sudo /opt/dozor/bin/dsctl restart
```

Следует дождаться завершения перезапуска процессов KEO DLP – об этом будет свидетельствовать возвращение приглашения командной строки.

2. Отправить тестовое сообщение на сервер KEO DLP. Ниже приведен листинг команд, выполняемых для отправки сообщения:

```
telnet 127.0.0.1 1025
```

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 Z-2 Firewall 2.6.17 SMTP proxy ready to service
```

```
helo localhost
```

```
250 Pleased to meet you, localhost
```

```
mail from: dlp@dlp.local
```

```
250 Sender OK
```

```
rcpt to: dlp@dlp.local
```

```
250 Recipient OK
```

```
data
```

```
354 OK enter mail, end with <CRLF>.<CRLF>
```

```
From: dlp@dlp.local
```

```
To: dlp@dlp.local
```

```
Subject: first letter
```

```
<Пустая строка>
```

```
Say hello to my little friend!
```

```
.
```

```
250 Message accepted for delivery (norm-d5d73742-fd4f-11df-8720-000c29e6dd7f)
```

quit

221 Closing connection  
Connection closed by foreign host.

### Примечание

*Команды и другой текст, вводимые пользователем с клавиатуры, выделены моноширинным шрифтом; ответы сервера и другая выводимая системой на экран информация подсвечены серым цветом.*

3. Запустить веб-интерфейс администратора KEO DLP, указав в адресной строке браузера адрес **https://<IP-адрес сервера ПК KEO DLP>**

Продолжить открытие веб-узла, проигнорировав предупреждение браузера об ошибке сертификата безопасности или недоверенном соединении, и принять предлагаемый сертификат.

4. Ввести в соответствующие поля имя учетной записи и пароль администратора.
5. Выбрать раздел **Поиск**. На экране отобразятся инструменты поиска (см. [Рис.8.27](#)).

Рис. 8.27. Раздел Поиск

6. Поле **Объект поиска** оставить в значении **Сообщения**, в поле **С текстом** ввести **Say hello my friend**, и нажать кнопку **Найти**.

На экране отобразится список результатов поиска с подсветкой совпадений (см. [Рис.8.28](#))

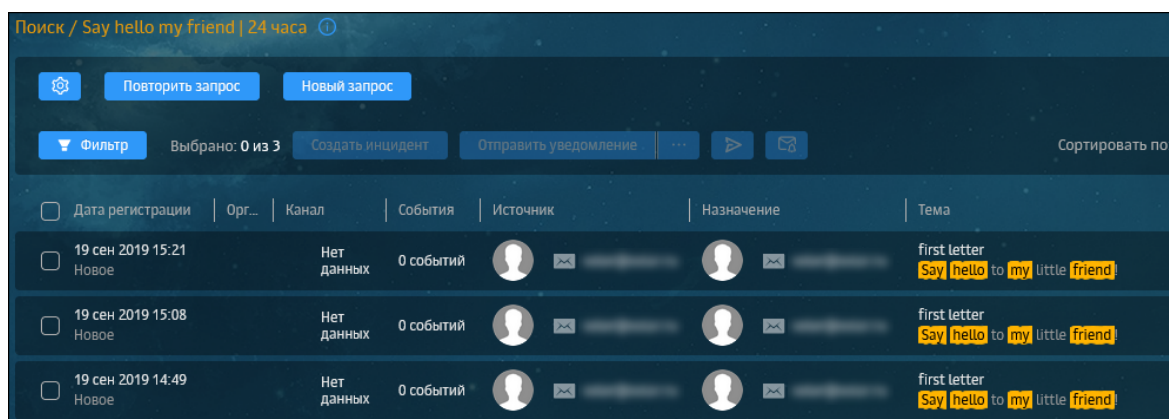


Рис. 8.28. Результат поиска

Для проверки работоспособности файлового хранилища установленного КЕО DLP необходимо выполнить следующие действия:

1. Проверить правильность настроек локальных ФХ и центрального ФХ.
2. Убедиться в том, что сервисы **filestorage-ng** и **skvt-cassandra**, обеспечивающие работу ФХ, находятся в состоянии **Запущен**.
3. Найти идентификатор контейнера отправленного письма (**vid**) в одном из журнальном файле архиватора (**archiver**), выполнив команду:

**sudo /opt/dozor/bin/seelog archiver**

На экране появится список следующего вида:

```
2015-12-11 11:47:50.233774500 support:info (8886) {f41c1342-ec81-11e3-b6e7-0050569900e4}
message f41c1342-ec81-11e3-b6e7-0050569900e4 archived successfully id=2.201406051147454239
time=4493 msec msg_size=6199 bytes
2015-12-11 11:47:52.450357500 support:info (6534) {f46cc40e-ec81-11e3-9e66-0050569900e4}
message f46cc40e-ec81-11e3-9e66-0050569900e4 archived successfully id=3.201406051147500332
time=1810 msec msg_size=7357 bytes
2015-12-11 11:47:52.581030500 support:info (12533) {f46f7be0-ec81-11e3-9e66-0050569900e4}
message f46f7be0-ec81-11e3-9e66-0050569900e4 archived successfully id=3.201406051147470345
time=5409 msec msg_size=6860 bytes
2015-12-11 11:47:55.316807500 support:info (8886) {f4238fbe-ec81-11e3-b6e7-0050569900e4}
message f4238fbe-ec81-11e3-b6e7-0050569900e4 archived successfully id=3.201406051147530364
time=1856 msec msg_size=5606 bytes
2015-12-11 11:47:59.487845500 support:info (6534) {f4937054-ec81-11e3-b387-0050569900e4}
message f4937054-ec81-11e3-b387-0050569900e4 archived successfully id=2.201406051147554240
time=3864 msec msg_size=134732 bytes
2015-12-11 11:47:59.748163500 support:info (12533) {f411273e-ec81-11e3-b6e7-0050569900e4}
message f411273e-ec81-11e3-b6e7-0050569900e4 archived successfully id=2.201406051147554241
time=4020 msec msg_size=2852 bytes
```

4. Выбрать из этого списка нужное письмо и соответствующий ему идентификатор контейнера **vid** (в фигурных скобках).
5. Создать конфигурационный файл командной оболочки языка запросов к Cassandra, выполнив команду:

---

```
# touch /var/tmp/cqlshrc
```

Записать в этот файл следующее содержимое:

```
[connection]
factory = cqlshlib.ssl.ssl_transport_factory

[ssl]
certfile = /opt/dozor/etc/ssl/ca.crt
userkey = /opt/dozor/etc/ssl/bus.key
usercert = /opt/dozor/etc/ssl/bus.pem
version = TLSv1_2
```

Сохранить и закрыть файл.

6. Подключиться к базе данных индексов ФХ следующей командой:

```
sudo /opt/dozor/cassandra/bin/cqlsh -k filestorage <hostname> --ssl --cqlsh
/var/tmp/cqlshrc
```

где **<hostname>** – имя узла, на котором размещено ФХ.

7. Ввести следующий запрос:

```
select url from vids where vid='vg-000000/<vid>';
```

где **<vid>** – идентификатор контейнера.

На экране появится результат вида:

```
url
-----
https://Dozor6:2266/_storage/main/2015/12/11/09/20/4abda222-9fe8-11e5-afb8-005056882665/
(1 rows)
```

8. Отключиться от базы данных командой **logout**. Перейти в каталог с контейнером командой вида:

```
cd /data/storage/vg-000000/fs-1/2015/12/11/09/20/<vid>/data/
```

где **/data/storage/vg-000000/fs-1/** – путь к файловому хранилищу, заданный в секции **Каталоги файлового хранилища** (раздел **GUI Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**). Вместо **2015/12/11/09/20/<vid>/** следует подставить соответствующую часть пути, полученного в предыдущем шаге.

9. Выполнить команду **ls -la**. В результате на экране появится информация следующего вида:

```
ds-mode@Dozor6
/data/storage/vg-000000/fs-1/2015/12/11/09/20/4abda222-9fe8-11e5-afb8-005056882665/data # ls
-la
итого 12
drwxr-xr-x 2 dozor dozor 4096 Dec 11 12:20 .
```

---

```
drwx----- 4 dozor dozor 4096 Dec 11 12:20 ..  
-rw-r--r-- 1 dozor dozor 196 Dec 11 12:20 body.gz
```

Последняя строка свидетельствует о том, что тело сообщения содержится в контейнере, и, следовательно, ФХ работает корректно.

---

## 9. Работа модуля S/MIME

Модуль **S/MIME** предназначен для шифрования и дешифрования сообщений и уведомлений, отправляемых и получаемых KEO DLP.

При хранении сертификатов в файлах поиск сертификата выполняется по имени файла в каталоге, указанном в значении параметра **Директория для ключей и сертификатов S/MIME** (секция **Хранилище ключей S/MIME** раздела **GUI Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений**). Имена файлов должны содержать email-адрес, например **<email@domain.com>-cert.pem**. Сертификаты должны иметь формат **PEM (BASE64)** с разделителями следующего вида:

```
-----BEGIN CERTIFICATE-----  
<Certificate_body>  
-----END CERTIFICATE-----
```

Различные сертификаты в файле размещены один за другим.

Для шифрования сообщений и уведомлений, отправляемых из KEO DLP, следует использовать в правилах фильтрации профиль отправки с установленным флажком **Зашифровать** (подробнее см. документ *Руководство пользователя*). При установленном флажке выполняется поиск сертификатов всех получателей уведомления. Если сертификаты для всех получателей найдены, то сообщение/уведомление шифруется открытыми ключами всех получателей. То есть в сообщении с уведомлением для каждого получателя содержится блок данных, который может быть расшифрован закрытым ключом данного получателя. После этого сообщение с уведомлением отправляется в соответствии с набором параметров отправки, который задан в профиле.

Если хотя бы для одного получателя сертификат не найден, действие зашифрованное уведомление не может быть отправлено. В таком случае генерируется ошибка, а сообщение перемещается в **err-spool**.

Для отправки зашифрованных уведомлений необходимо выполнить следующие действия:

1. Проверить, что указанный в параметре **Директория для ключей и сертификатов S/MIME** каталог с сертификатами пользователей существует (по умолчанию **/opt/dozor/etc/keystores**).

В противном случае необходимо создать каталог, выполнив команду от имени пользователя **dozor**:

```
~$ sudo mkdir /opt/dozor/etc/keystores
```

2. Сохранить и применить конфигурацию.
3. Скопировать файлы сертификатов в **/opt/dozor/etc/keystores**.
4. Перезапустить все процессы (раздел **GUI Система > Администрирование > Процессы**).
5. Создать профиль отправки (раздел **GUI Политика > Шаблоны и профили > Профили отправки**).

- 
6. Создать шаблон уведомлений (раздел GUI **Политика > Шаблоны и профили > Шаблоны уведомлений**).
  7. Создать условие (раздел GUI **Политика > Политика > Условия**), при котором необходимо отправлять зашифрованное уведомление.
  8. Создать правило фильтрации **Отправить зашифрованное уведомление** (раздел GUI **Политика > Политика > Наборы правил**) с созданными условием, шаблонами отправки и уведомлений. Сделать правило головным.
  9. Применить политику.

Расшифровка зашифрованного сообщения выполняется на этапе его распаковки. Дешифрование осуществляется распаковщиком соответствующего MIME-типа (**application/x-pkcs7-mime**). Такая схема обладает следующими особенностями:

- Единый механизм распаковки для всех типов данных (в том числе и для зашифрованных).
- Поддержка «ленивой» распаковки для шифрованных данных (дешифрование только при обращении к данным).
- Исходное сообщение не удаляется и не изменяется при дешифровании, можно осуществлять доставку исходного сообщения.
- В архиве сообщение доступно «как есть», можно осуществлять доставку из архива.
- В архиве доступны текстовые представления зашифрованных частей «открытым текстом», можно читать в архиве и осуществлять контекстный поиск.
- Из архива можно получить зашифрованные части в расшифрованном виде (дешифрование выполняется при извлечении из архива).

Для дешифрования требуются сертификаты и секретные ключи пользователей, а также файл с паролем от хранилища ключей.

При хранении закрытых ключей в файлах поиск осуществляется по имени файла в каталоге, указанном в конфигурации. Имена файлов должны иметь вид:

**<Email-адрес>-key.pem**

Например:

**user@host.example-key.pem.**

Ключи должны иметь формат **PEM (BASE64)** с разделителями:

**"-----BEGIN RSA PRIVATE KEY-----" и "-----END RSA PRIVATE KEY-----"**

Имя файла с паролем хранилища ключей должно иметь вид:

**<Email-адрес>.password**

Например:

**user@host.example.password**

---

Все закрытые ключи могут быть зашифрованы одним паролем. В этом случае в конфигурации указывается имя файла с общим паролем.

Подготовка к использованию возможности отправки и получения зашифрованных сообщений и уведомлений состоит из следующих этапов:

1. Генерация ключей и сертификатов пользователей (см. раздел [9.1](#)).
2. Настройка модуля **S/MIME** (см. раздел [9.2](#)).
3. Настройка почтового клиента (см. раздел [9.3](#)).

## 9.1. Генерация ключей и сертификатов пользователей

Сгенерировать ключи для шифрования почтовых сообщений можно с помощью программы **openssl**. Для этого необходимо выполнить следующие действия:

1. Создать каталог, в котором будут размещаться файлы ключей и сертификатов, например, **/home/ssl**. Для этого выполнить следующую команду от имени пользователя **dozor**:

```
$ mkdir /home/ssl
```

2. Перейти в созданный каталог, выполнив команду:

```
$ cd /home/ssl
```

3. Перед тем как создавать сертификат пользователя, сгенерировать закрытый ключ для него. Для этого необходимо запустить программу **openssl** с указанием имени файла создаваемого ключа. Действия выполнять от пользователя **dozor**. Формат команды для запуска следующий:

```
$ openssl genrsa -des3 -out <key_filename> 4096
```

где:

- **<key\_filename>** – имя создаваемого файла с расширением **.key**, например **cert.key**;
- **4096** – размер ключа в битах.

В результате выполнения команды на экран будет выведено сообщение следующего вида:

```
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for cert.key:
Verifying - Enter pass phrase for cert.key:
```

В ходе выполнения программы генерации на экран выводится приглашение ввести кодовое слово для создаваемого ключа – **Enter pass phrase for cert.key:**. После чего необходимо дважды (второй раз для проверки) ввести с клавиатуры кодовое слово длиной не менее 4 символов. Данное слово необходимо запомнить.



4. Создать csr-файл запроса на сертификат. Это файл нужен для проверки и идентификации. Для этого выполнить следующую команду от имени пользователя **dozor**:

```
$ openssl req -new -key cert.key -out cert.csr
```

После появления сообщения:

```
Enter pass phrase for cert.key:
```

необходимо ввести с клавиатуры кодовое слово, указанное на предыдущем шаге. После чего на экран будет выведено приглашение ввести информацию, которая будет включена в сертификат. Главное – указать почтовый адрес, для которого создается пара закрытый ключ – сертификат. Остальные параметры можно не указывать, для этого достаточно в каждой строчке ввести символ «.» (точка).

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
-----
```

```
Country Name (2 letter code) [AU]:.
```

```
State or Province Name (full name) [Some-State]:.
```

```
Locality Name (eg, city) []:.
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:.
```

```
Organizational Unit Name (eg, section) []:.
```

```
Common Name (e.g. server FQDN or YOUR name) []:
```

```
Email Address []:admin@example.com
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
```

```
A challenge password []:.
```

```
An optional company name []:.
```

5. Подписать созданный csr-файл созданным ранее ключом. Для этого выполнить следующую команду от имени пользователя **dozor**:

```
$ openssl x509 -req -days 365 -in cert.csr -signkey cert.key -out cert.crt
```

В результате выполнения команды будет проведена проверка подписи и на экран выведены данные о сертификате, указанные ранее, в частности адрес электронной почты, для которого он создается:

```
Signature ok
```

```
emailAddress=admin@example.com
```

```
Getting Private key
```

```
Enter pass phrase for cert.key:
```

В завершении потребуется ввести кодовое слово, заданное ранее.

6. Сконвертировать полученный файл сертификата в формат **.p12**, пригодный для импорта в программу-почтовый клиент. Для этого выполнить следующую команду от имени пользователя **dozor**:

```
$ openssl pkcs12 -export -in cert.crt -inkey cert.key -name <name> -out cert.p12
```

где в качестве параметра **<name>** следует указать реальное имя пользователя (например, **admin**), для которого создается сертификат, чтобы в дальнейшем не возникло путаницы.

В ходе выполнения команды будет предложено сначала ввести кодовое слово, заданное ранее, а затем указать пароль для экспорта и подтвердить его.

```
Enter pass phrase for cert.key:  
Enter Export Password:  
Verifying - Enter Export Password:
```

Заданный пароль для экспорта необходимо запомнить, так как он используется для экспорта созданного сертификата в почтовую программу.

7. В результате выполнения указанных действий в созданном каталоге должно быть 4 файла с расширениями **.crt**, **.csr**, **.key**, **.p12**, наличие которых можно проверить, выполнив команду **ls** от имени пользователя **dozor**. Формат команды следующий:

```
$ ls -l
```

В результате выполнения команды на экран будет выведен список файлов в каталоге **/home/ssl**.

```
cert.crt  
cert.csr  
cert.key  
cert.p12
```

8. Файл с расширением **.p12** следует переименовать так, чтобы его имя имело вид **<email>.p12**, где **<email>** – электронный адрес пользователя, для которого был создан сертификат. Этот файл необходимо импортировать в почтовый клиент, чтобы было возможным с ее помощью открывать сообщения, зашифрованные сгенерированным ключом (подробнее см. [9.3](#)). Также его следует разместить в каталоге, указанном в параметре **Директория для ключей и сертификатов S/MIME** (см. [9.1](#)).
9. Если в системе используется несколько сертификатов, созданных по этой процедуре, и для них заданы неодинаковые пароли для экспорта, то для каждого файла с расширением **.p12** следует создать одноименный файл с расширением **.password**, записать в него пароль для экспорта в открытом виде, и разместить в том же каталоге.

#### Примечание

*Если один из паролей для экспорта повторяется чаще остальных – то можно указать его в параметре **Пароль по умолчанию для хранилищ ключей S/MIME** (см. [9.1](#)), и не создавать файл с расширением **.password**.*

## 9.2. Настройка модуля S/MIME

После генерации ключей и сертификатов пользователей переименованные файлы следует скопировать в каталог, определенный параметром конфигурации **Директория для ключей и сертификатов S/MIME** секции **Хранилище ключей S/MIME** (раздел **GUI Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации**

перехваченных данных и детектирования критичной информации > Обработка сообщений).

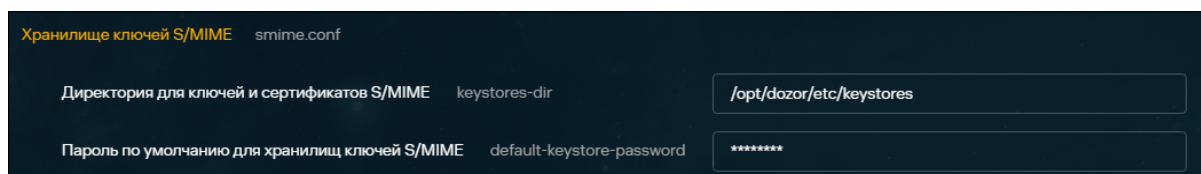


Рис. 9.1. Настройка параметров S/MIME

В значении параметра **Пароль по умолчанию для хранилищ ключей S/MIME** необходимо указать пароль, которым зашифрованы все закрытые ключи пользователей.

### 9.3. Настройка почтового клиента

В данном разделе описывается экспорт сгенерированного сертификата пользователя в программу - почтовый клиент и настройка почтового клиента для работы с зашифрованными почтовыми сообщениями. Такая настройка необходима, чтобы иметь возможность открывать зашифрованные уведомления, отправляемые из интерфейса KEO DLP. Приводится описание настройки для почтовых клиентов Microsoft Outlook и Mozilla Thunderbird.

#### 9.3.1. Настройка Microsoft Outlook

Для импорта ключа шифрования и настройки почтового клиента Microsoft Outlook на работу с зашифрованными сообщениями необходимо выполнить следующие действия:

1. Выбрать пункт меню **Файл > Параметры > Центр управления безопасностью** и нажать кнопку **Параметры центра управления безопасностью** (Рис.9.2).

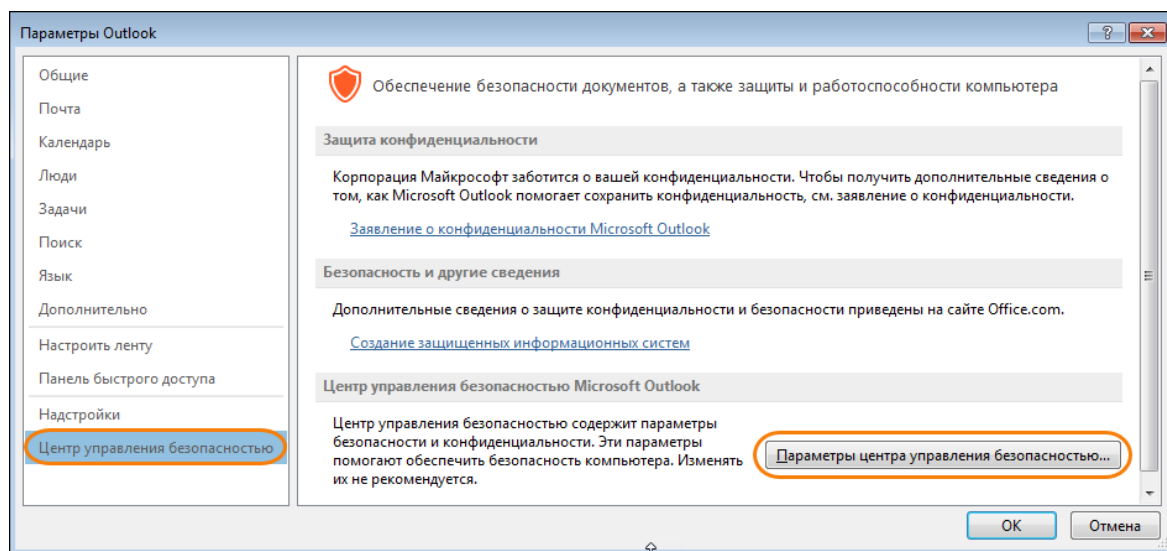


Рис. 9.2. Окно Параметры Outlook

2. В открывшемся окне в меню слева выбрать пункт **Защита электронной почты** (Рис.9.3):

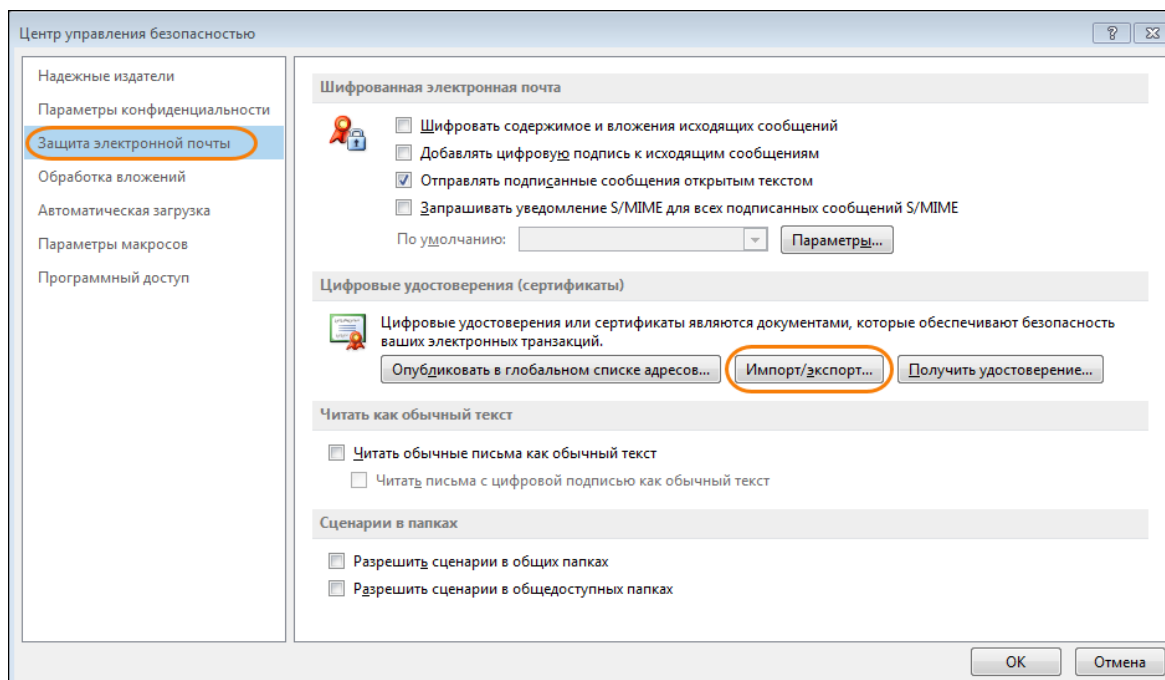


Рис. 9.3. Окно Центр управления безопасностью

3. В правой части окна в разделе **Цифровые удостоверения (сертификаты)** нажать кнопку **Импорт/экспорт** ([Рис.9.3](#)).
4. В открывшемся окне **Импорт/экспорт цифрового удостоверения** установить переключатель **Импортировать имеющееся цифровое удостоверение из файла** ([Рис.9.4](#)):

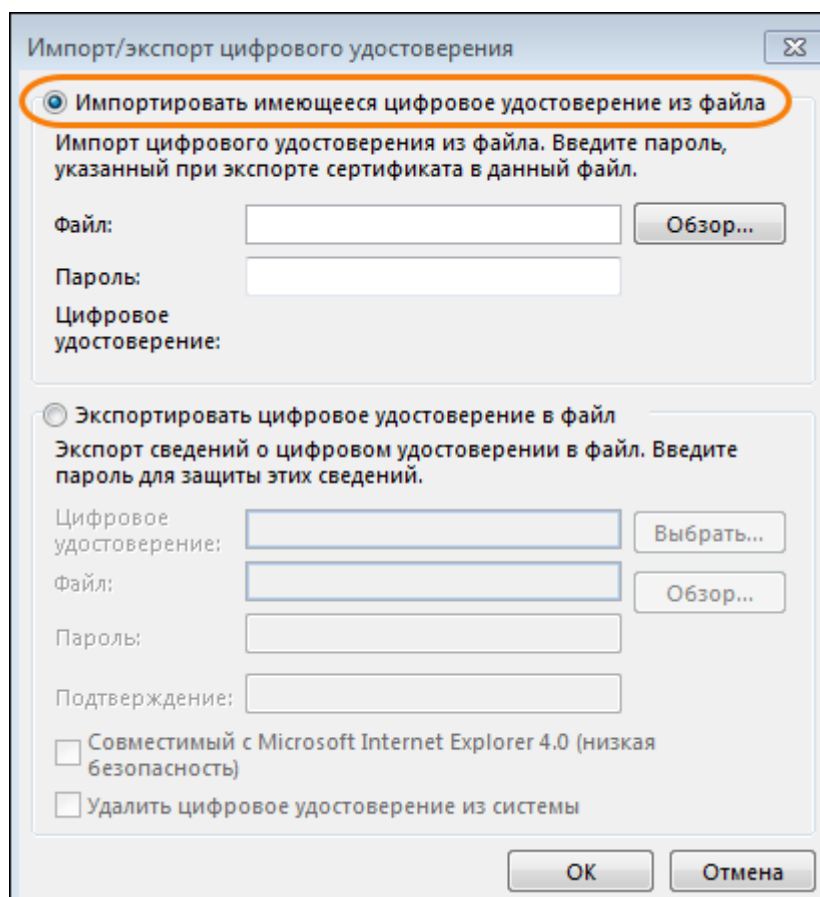


Рис. 9.4. Окно Импорт/экспорт цифрового удостоверения

5. Нажать кнопку **Обзор** и в открывшемся окне Проводника найти на жестком диске компьютера файл с сертификатом в формате **.p12**, созданный ранее и нажать кнопку **Открыть**:

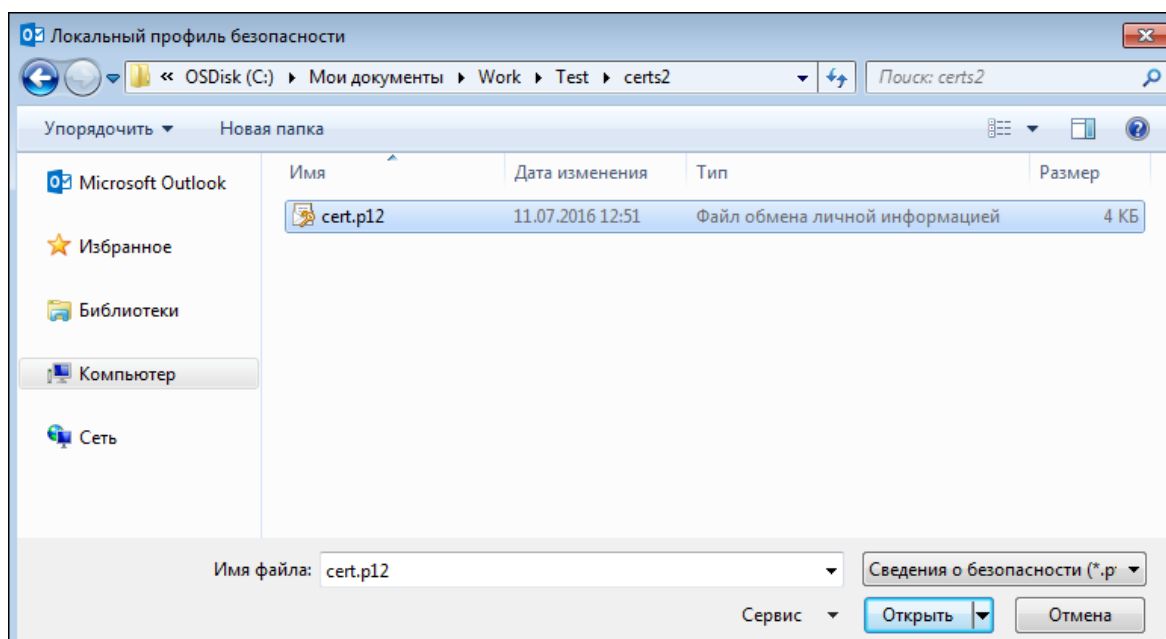


Рис. 9.5. Файл сертификата в формате .p12

6. В окне **Импорт/экспорт цифрового удостоверения** в поле **Файл** появится путь к указанному файлу (Рис.9.6). В поле **Пароль** необходимо ввести пароль для экспорта, указанный на шаге 6 в ходе генерации цифрового сертификата.

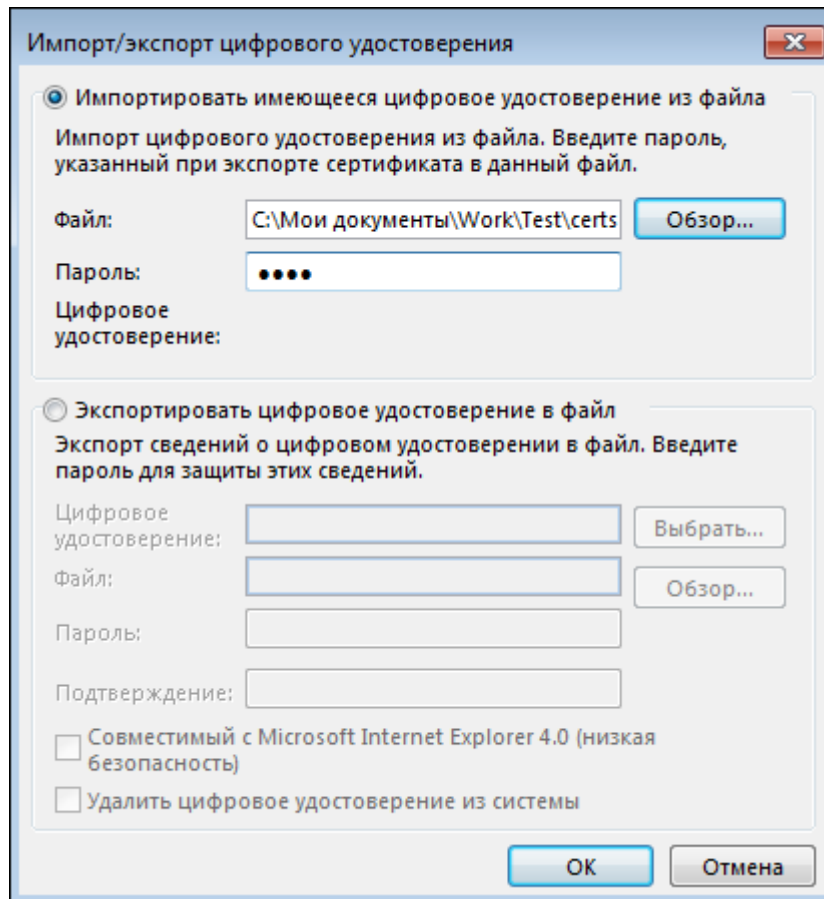


Рис. 9.6. Данные для импорта сертификата

7. Для завершения импорта сертификата нажать в окне **Импорт/экспорт цифрового удостоверения** кнопку **ОК**.
8. На экране появится окно **Импорт нового закрытого ключа обмена** ([Рис.9.7](#)) с сообщением о том, что будет установлен средний уровень безопасности и кнопкой **Уровень безопасности**, при нажатии на которую можно выбрать средний или высокий уровень безопасности. Чтобы завершить импорт закрытого ключа без изменения уровня безопасности, следует нажать кнопку **ОК**:

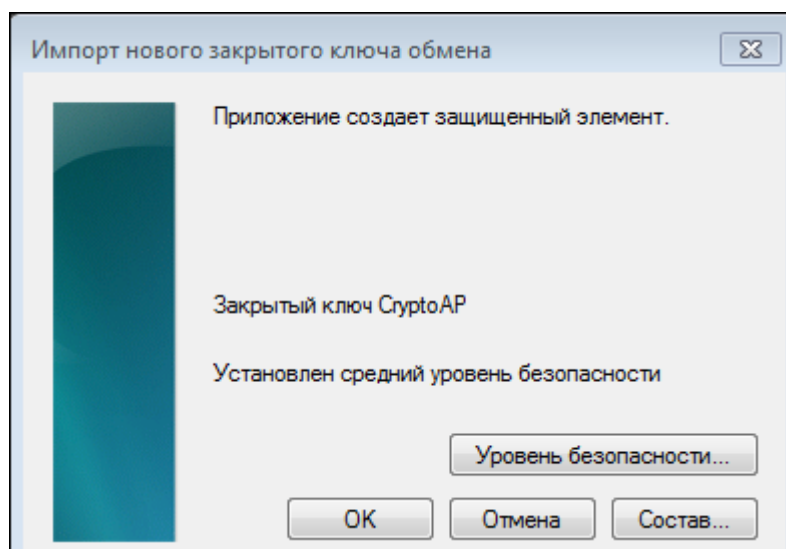


Рис. 9.7. Импорт нового закрытого ключа

9. При нажатии кнопки **Уровень безопасности** открывается окно, содержащее два переключателя для выбора уровня безопасности ([Рис.9.8](#)):

- **Средний** – при работе запрашивается только разрешение пользователя.
- **Высокий** – при работе запрашивается разрешение с паролем.

Для изменения уровня безопасности следует установить соответствующий переключатель и нажать кнопку **Далее**:

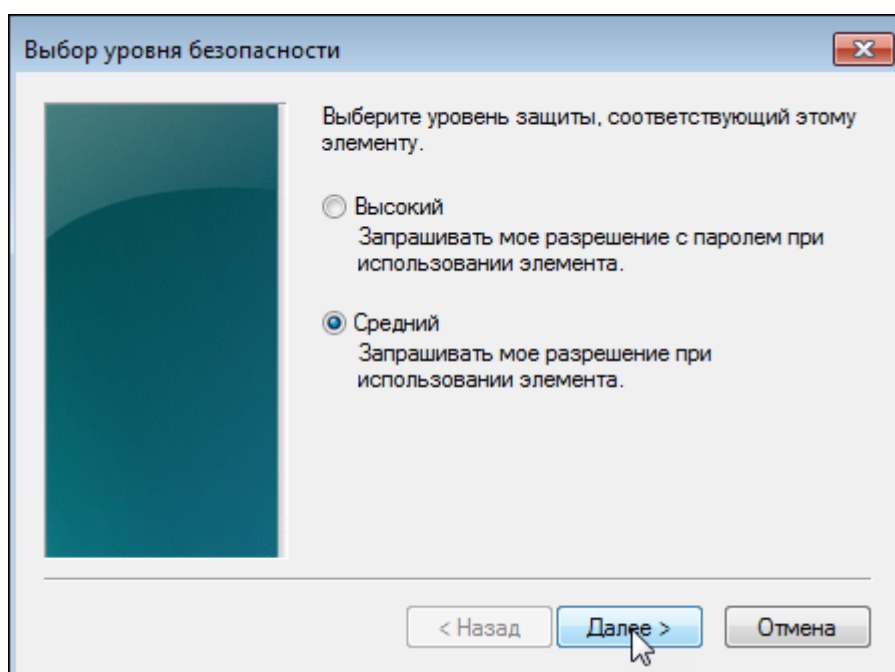


Рис. 9.8. Выбор уровня защиты



10. Откроется окно с сообщением об установке уровня безопасности ([Рис.9.9](#)). Для закрытия окна и завершения настройки Microsoft Outlook на работу с ключом шифрования следует нажать кнопку **Готово**:

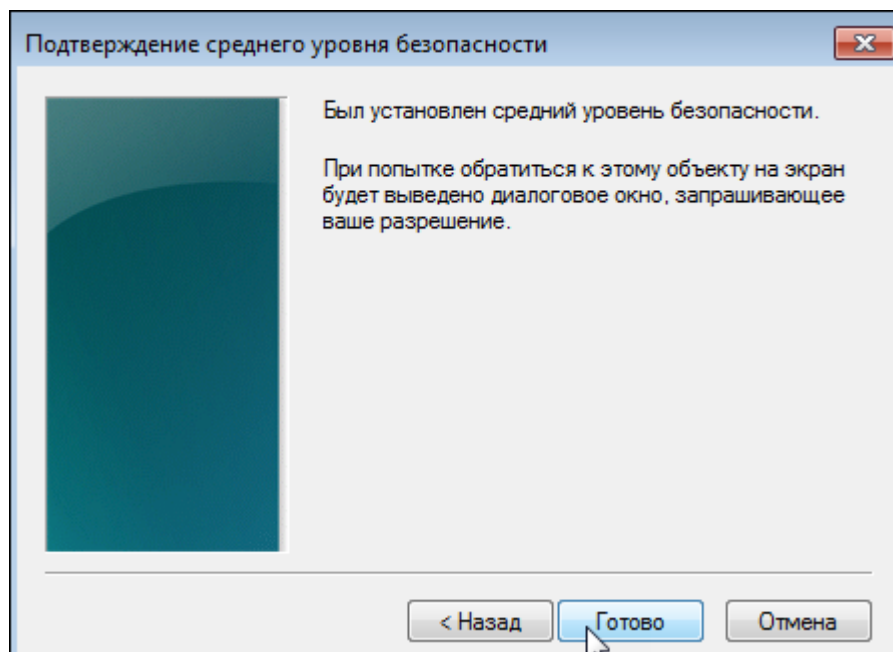


Рис. 9.9. Завершение импорта закрытого ключа

### 9.3.2. Настройка Mozilla Thunderbird

Для импорта ключа шифрования и настройки почтового клиента Mozilla Thunderbird на работу с зашифрованными сообщениями необходимо выполнить следующие действия:

1. Выбрать раздел **Учетные записи > Просмотр параметров этой учетной записи** ([Рис.9.10](#)).

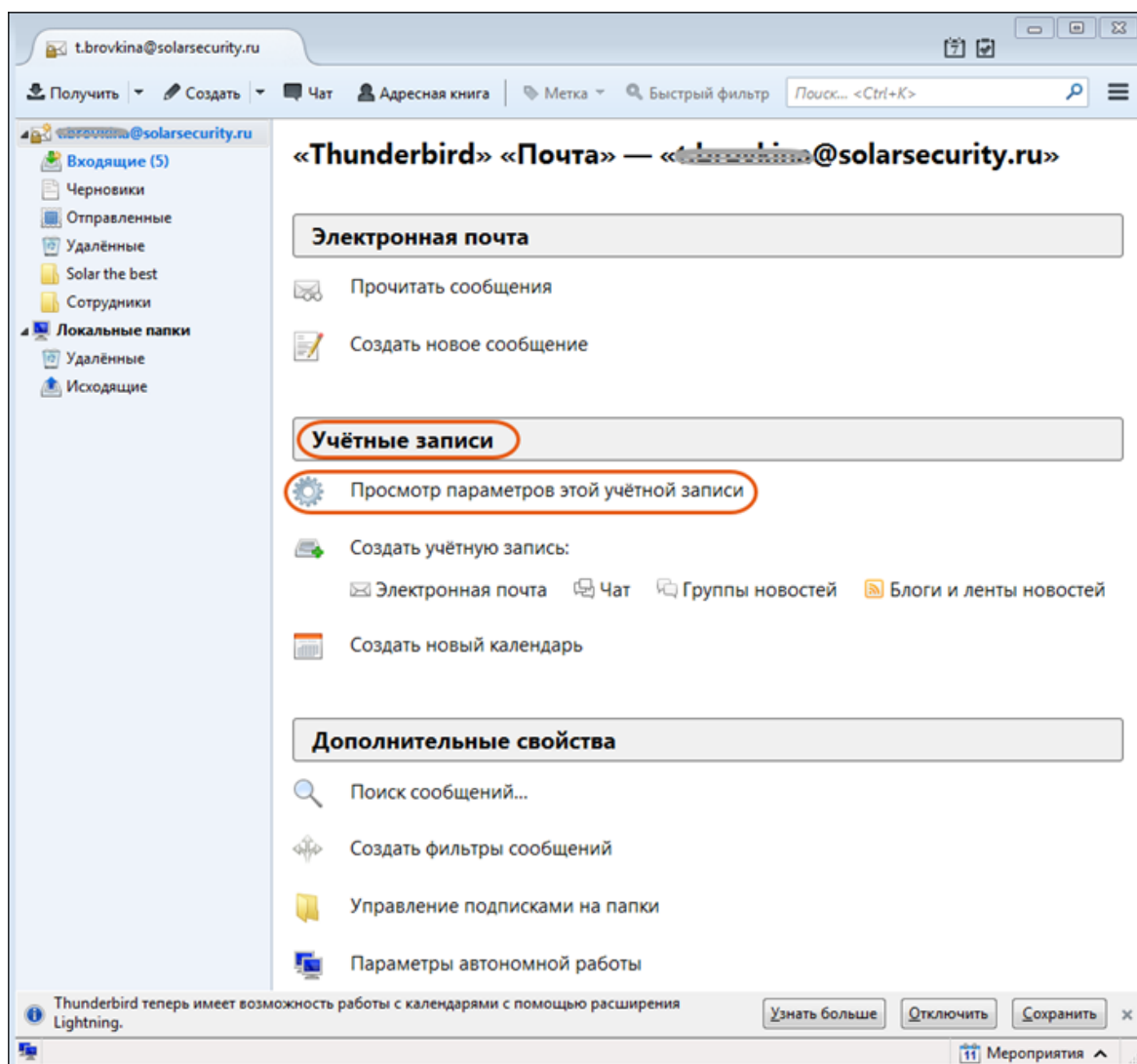


Рис. 9.10. Просмотр параметров учетной записи

2. В открывшемся окне **Параметры учетной записи** в списке параметров выбрать пункт **Защита** (Рис.9.11).

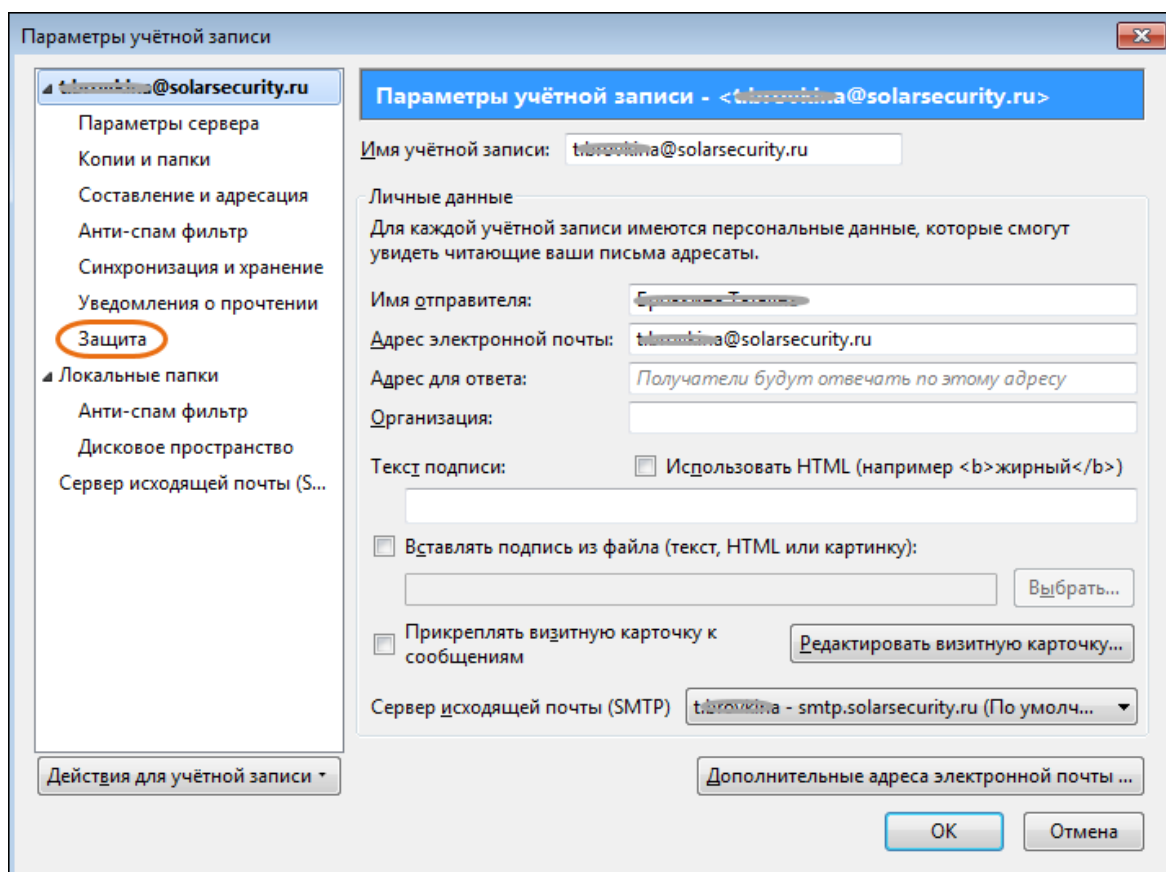


Рис. 9.11. Окно Параметры учетной записи

3. В правой части окна отобразятся параметры настройки шифрования и работы с зашифрованными сообщениями (Рис.9.12). Операция импорта сертификата должна быть подтверждена вводом мастер-пароля. Если он уже был создан ранее, то можно пропустить следующие шаги и переходить к пункту 6. Если мастер-пароль еще не создан, то необходимо в окне **Параметры учетной записи > Защита** нажать кнопку **Устройства защиты**.

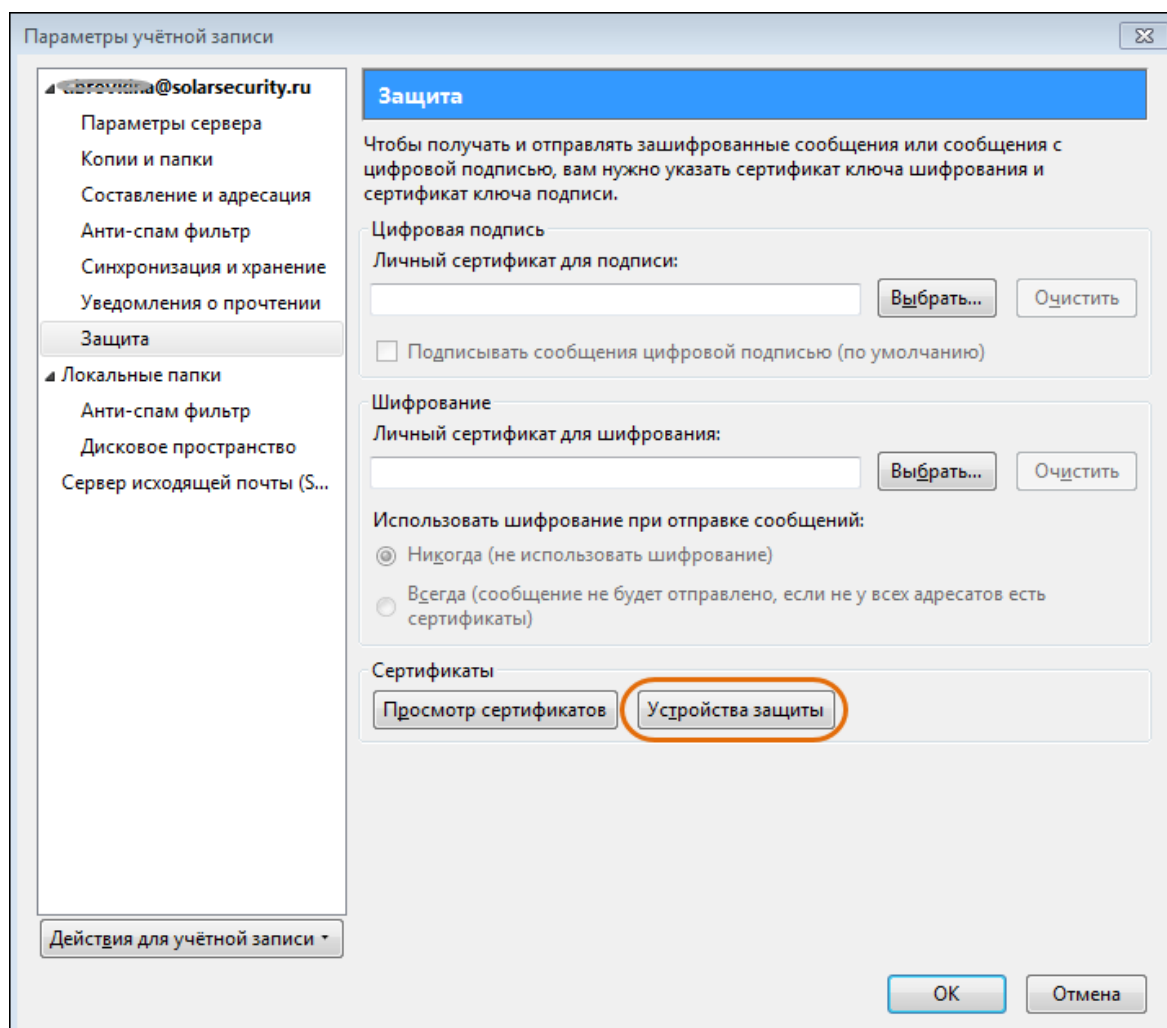


Рис. 9.12. Параметры настройки шифрования и работы с зашифрованными сообщениями

4. В открывшемся окне **Управление устройствами** в списке **Модули и устройства защиты** выбрать пункт **Модуль защиты** и нажать кнопку **Сменить пароль** ([Рис.9.13](#)):

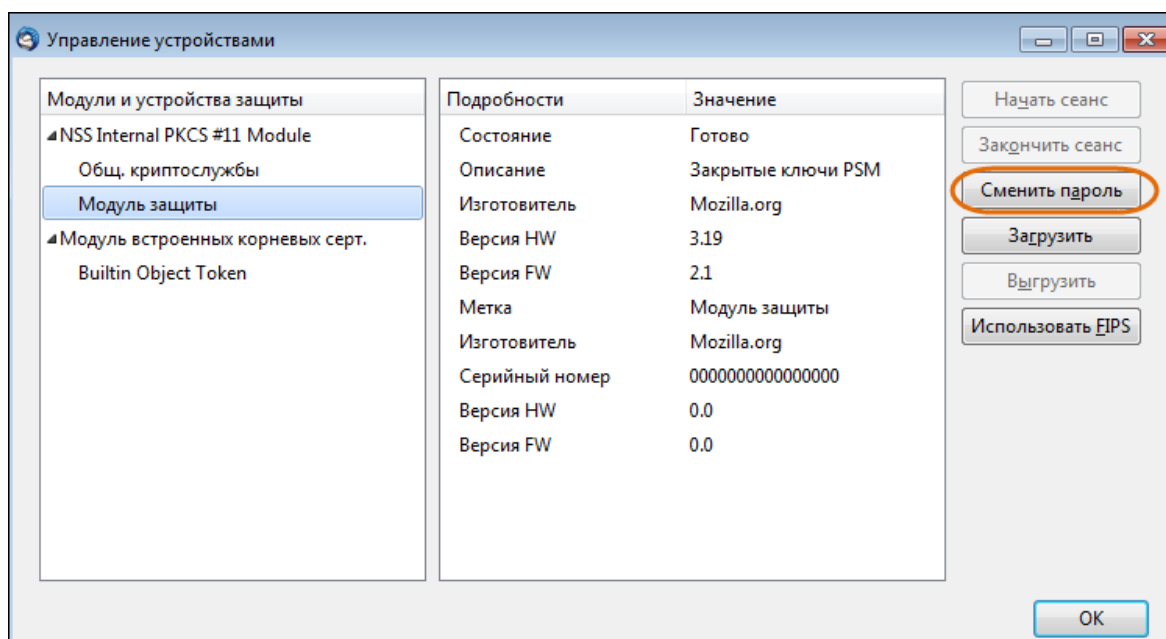


Рис. 9.13. Окно Управление устройствами

5. В открывшемся окне ([Рис.9.14](#)) следует ввести мастер-пароль (и подтвердить его, указав повторно) и нажать кнопку **ОК**:

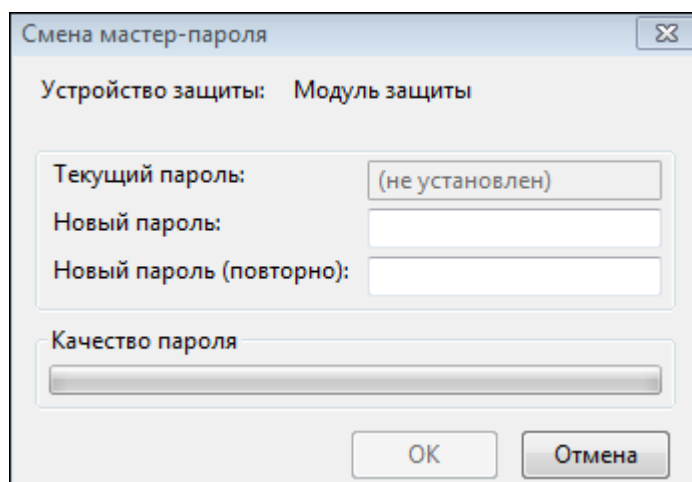


Рис. 9.14. Окно создания мастер-пароля

6. После того, как мастер-пароль создан, в окне **Параметры учетной записи** необходимо нажать кнопку **Просмотр сертификатов** ([Рис.9.12](#)). Откроется окно **Управление сертификатами** ([Рис.9.15](#)):

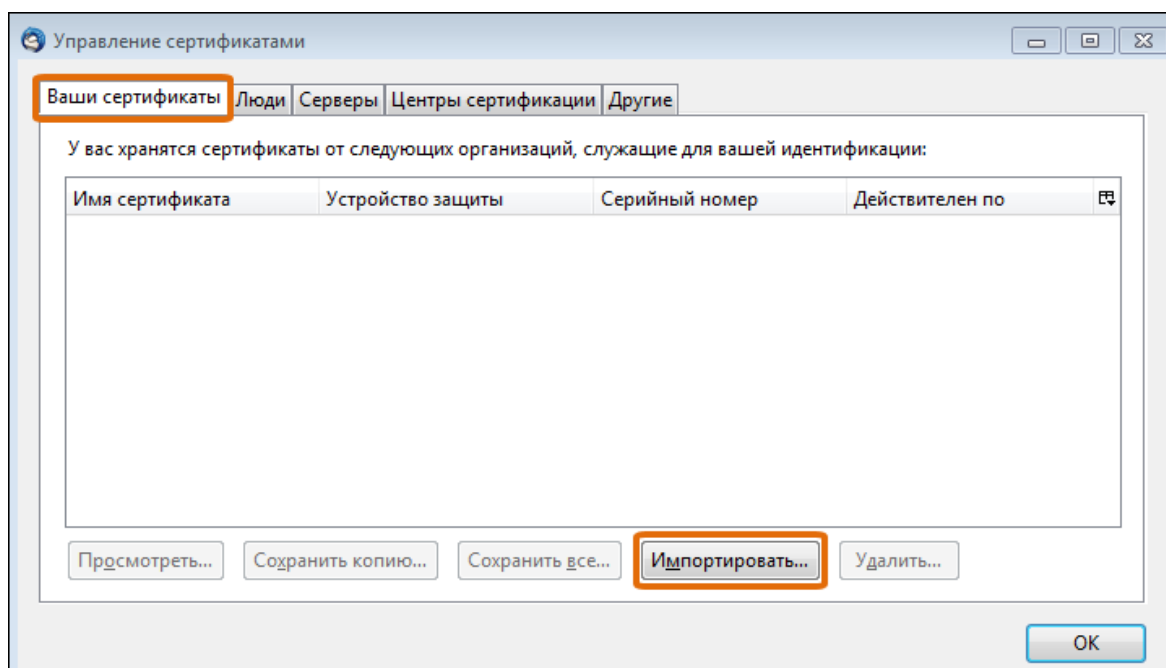


Рис. 9.15. Окно менеджера сертификатов

7. В окне **Управление сертификатами** перейти на вкладку **Ваши сертификаты**, нажать кнопку **Импортировать** и в открывшемся окне Проводника найти на жестком диске компьютера файл с сертификатом в формате **.p12**, созданный ранее. Выбрав файл, нажать кнопку **Открыть**:

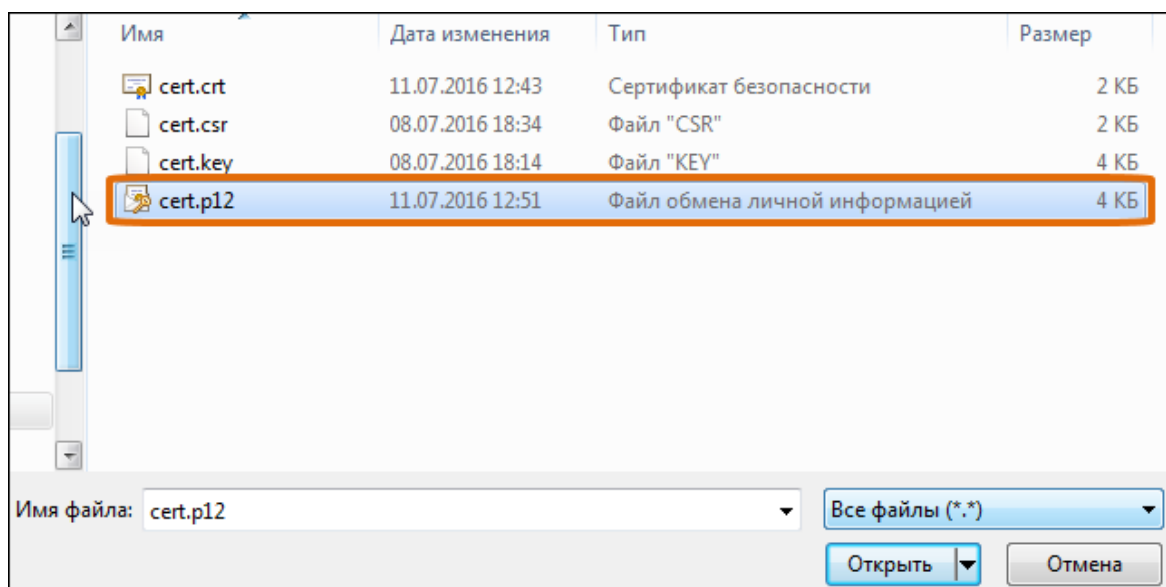


Рис. 9.16. Выбор файла сертификата

8. Для подтверждения импорта файла сертификата ввести мастер-пароль и нажать кнопку **ОК** (см. [Рис.9.17](#)):

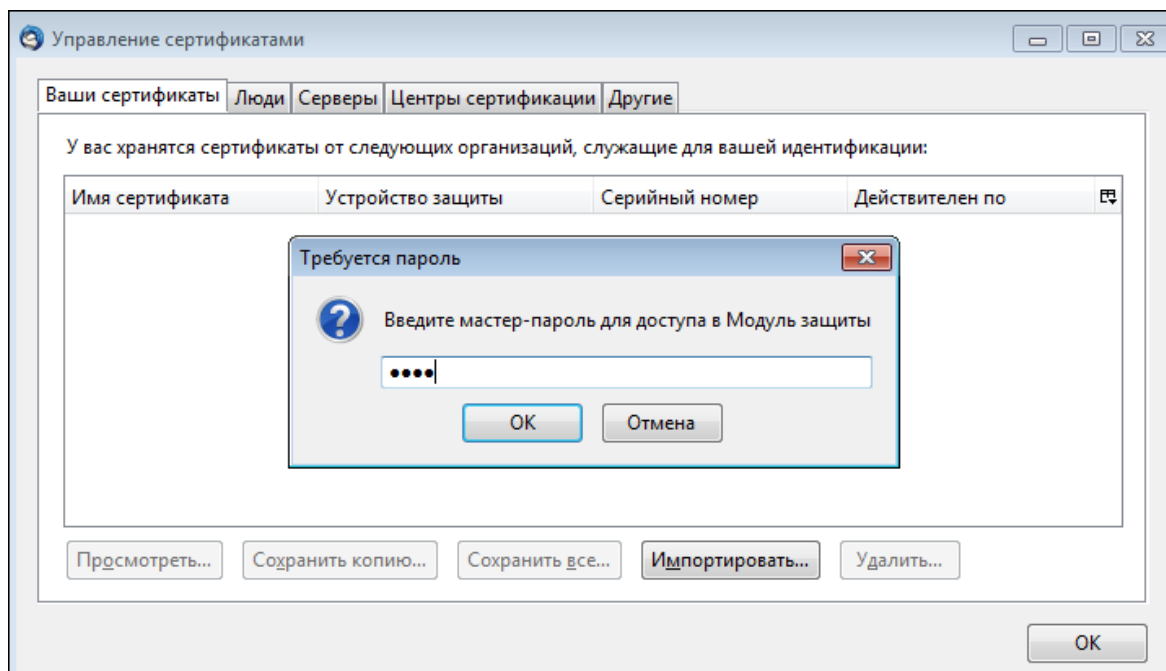


Рис. 9.17. Ввод мастер-пароля

9. Далее в окне **Ввод пароля** (см. [Рис.9.18](#)) указать пароль для экспорта, заданный на шаге 6 в процессе генерации сертификата. Нажать кнопку **ОК**:

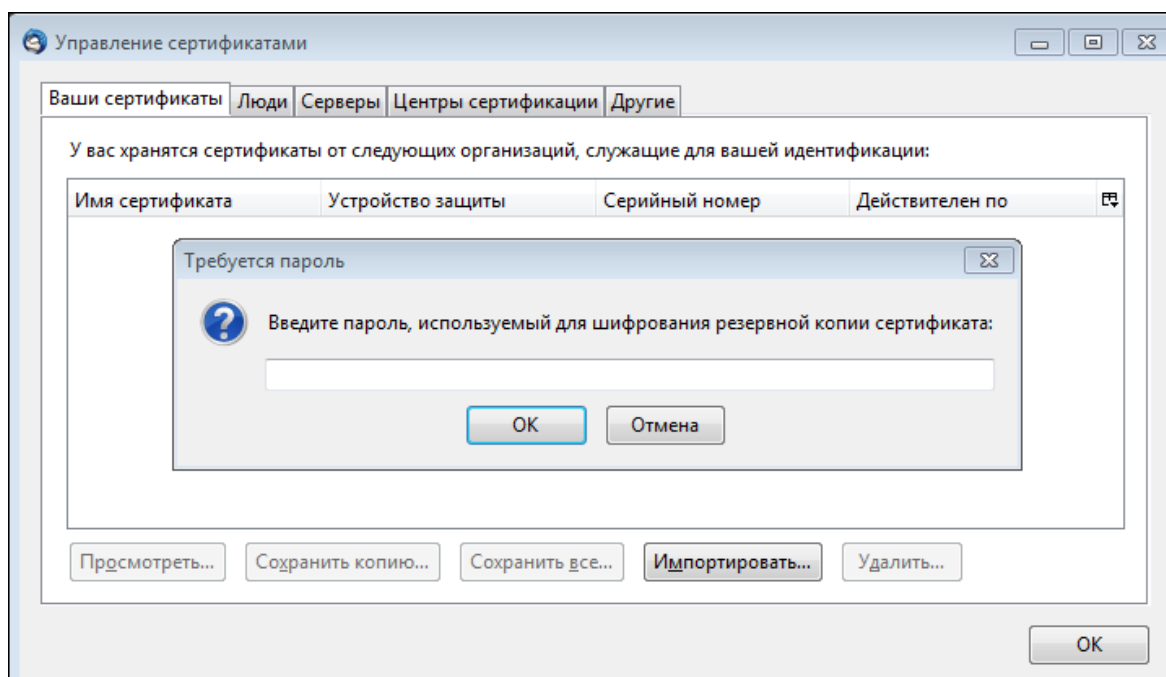


Рис. 9.18. Ввод пароля для экспорта сертификата

10. В открывшемся окне с сообщением об успешном завершении операции нажать кнопку **ОК**.

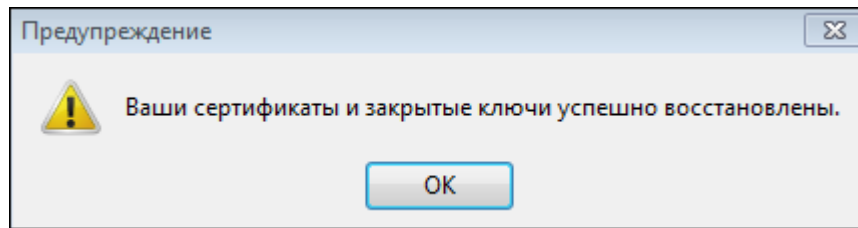


Рис. 9.19. Сообщение об успешном завершении операции

11. В окне **Управление сертификатами** будет добавлена запись с сертификатом пользователя (см. [Рис.9.20](#)). Нажать кнопку **ОК**:

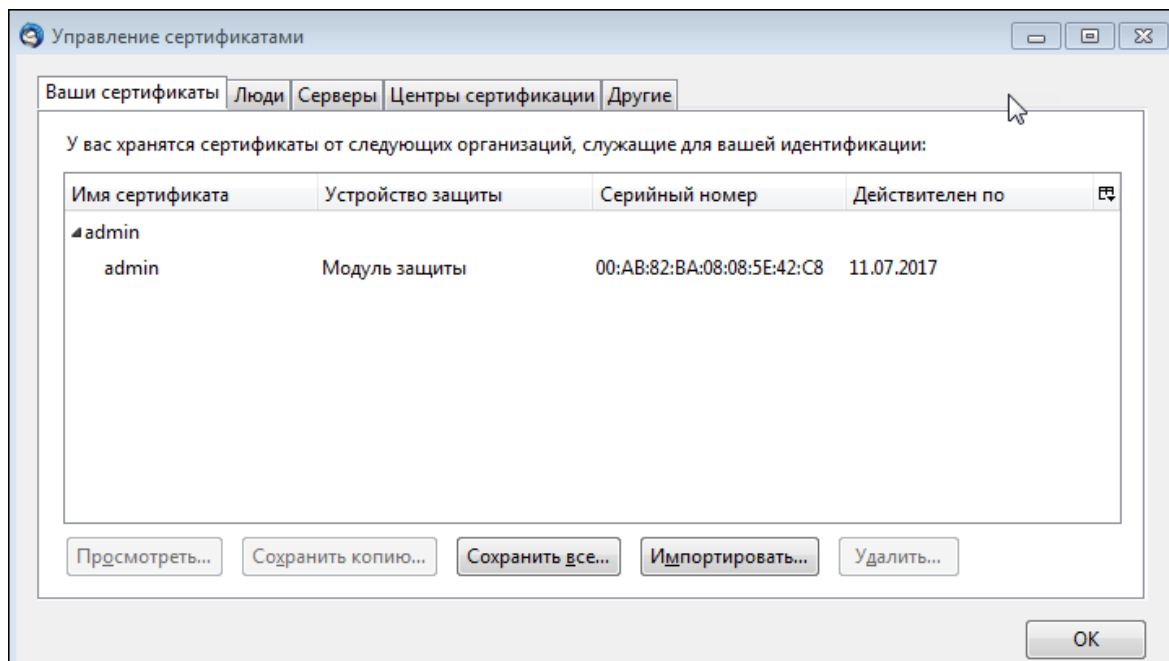


Рис. 9.20. Импортированный сертификат пользователя

12. В окне **Параметры учетной записи > Защита** (см. [Рис.9.11](#)) в разделе **Цифровая подпись** нажать кнопку **Выбрать**. В открывшемся окне **Выбор сертификата** ([Рис.9.21](#)) в раскрывающемся списке **Сертификат** выбрать импортированный ранее сертификат. В поле **Подробности о выбранном сертификате** необходимо проверить данные сертификата: главное, чтобы в качестве значения **Кому выдан** был указан правильный адрес электронной почты. Для подтверждения выбора сертификата нажать кнопку **ОК**:



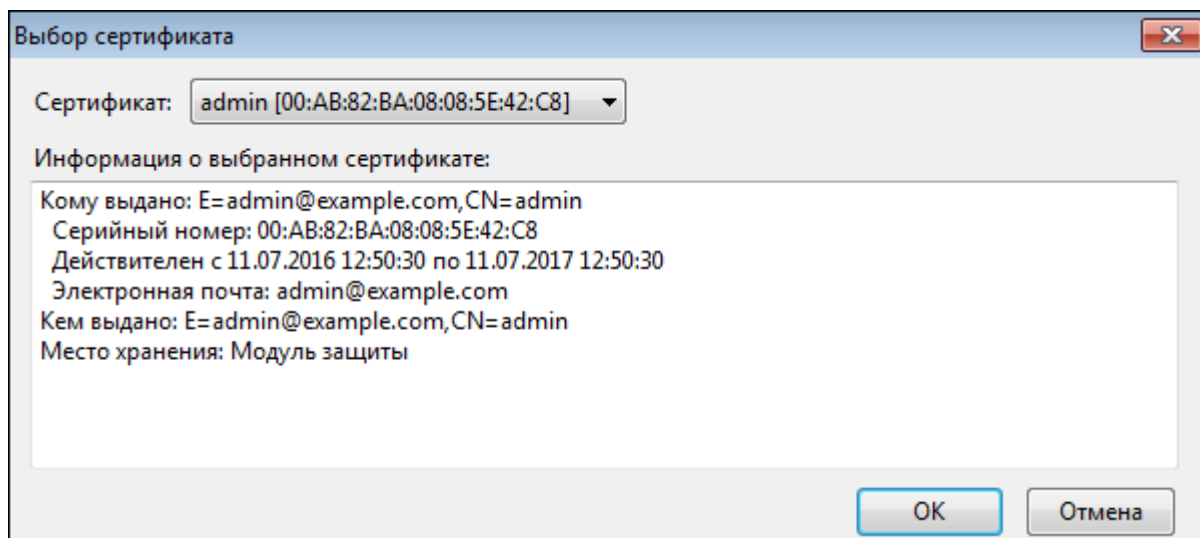


Рис. 9.21. Выбор сертификата для шифрования почтовых сообщений

13. В открывшемся окне с предложением использовать один и тот же сертификат как для шифрования, так и для расшифровки сообщений нажать кнопку **Да** (Рис.9.22).

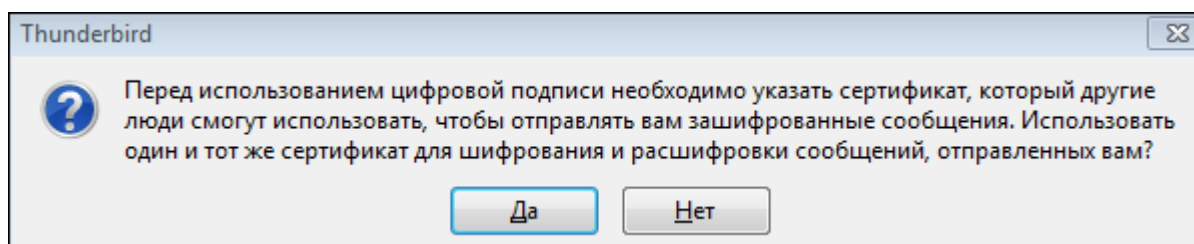


Рис. 9.22. Выбор сертификата для шифрования почтовых сообщений

14. В окне **Параметры учетной записи** будет указан выбранный сертификат для цифровой подписи и шифрования сообщений (Рис.9.23). Теперь появилась возможность получать сообщения, зашифрованные ключом, соответствующим импортированному сертификату. При этом для отправляемых сообщений шифрование по умолчанию не используется. При необходимости можно установить флажки, чтобы шифровать отправляемые сообщения или вставлять в сообщения цифровую подпись. Закройте окно **Параметры учетной записи**, нажав кнопку **ОК**:

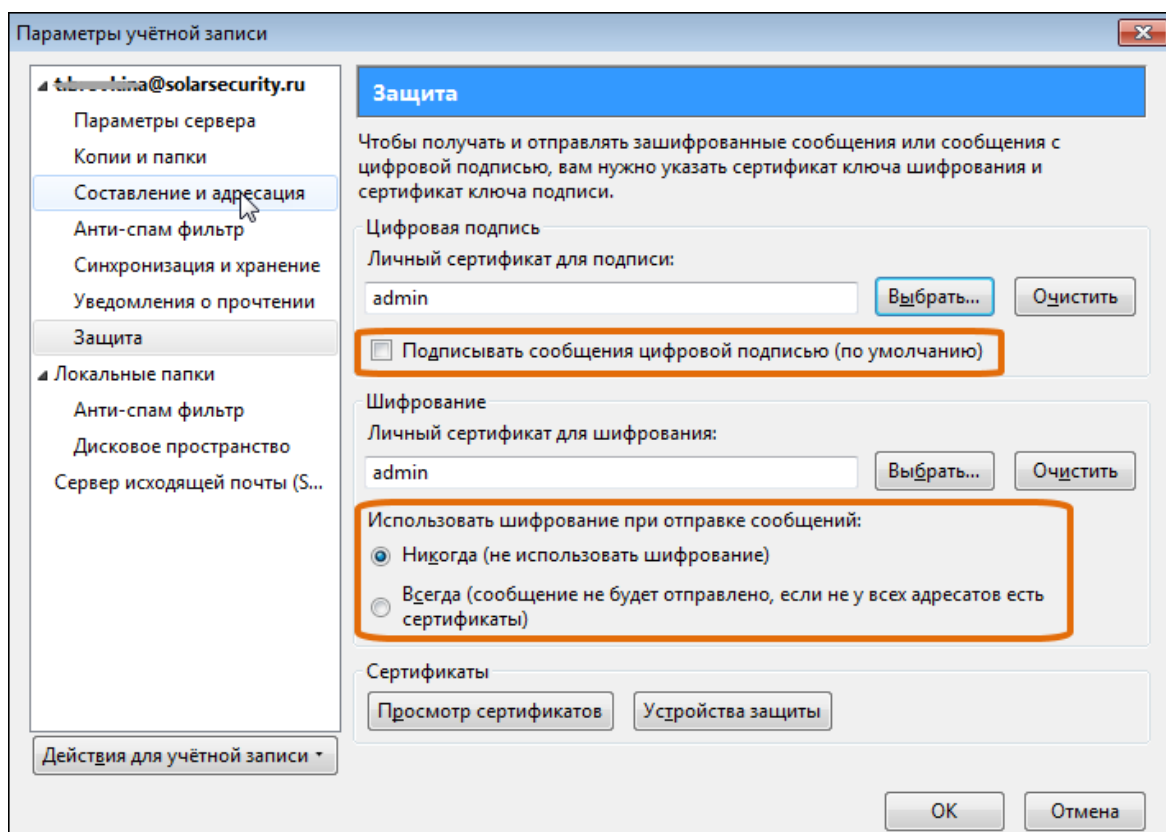


Рис. 9.23. Завершение настройки личных сертификатов

---

## 10. Настройка системы подтверждения отправки сообщений

Система подтверждения отправки сообщений дает возможность отправителю подтвердить или отменить отправку сообщения, задержанного на почтовом фильтре в соответствии с политикой безопасности KEO DLP.

Операции по подтверждению или отмене отправки сообщения регистрируются в журнальном файле **/opt/dozor/smap/log/confirm.log**. Также регистрируются попытки неавторизованного доступа к сообщениям.

Просмотр и подтверждение/отмена отправки сообщения разрешается пользователю, если почтовый ящик в SMTP-заголовке MAIL FROM совпадает с именем пользователя, а домен в SMTP-заголовке MAIL FROM совпадает со значением параметра **Локальный почтовый домен** в файле конфигурации.

Работоспособность системы не зависит от механизма аутентификации пользователя, так как на веб-сервере используется подключаемый модуль аутентификации, что позволяет подключать различные схемы аутентификации без модификации системы.

### 10.1. Настройка аутентификации пользователей

Система подтверждения отправки сообщений позволяет настроить аутентификацию пользователей через LDAP или PAM (Pluggable Authentication Modules, подключаемый модуль аутентификации). Рекомендуется использовать LDAP-аутентификацию.

#### 10.1.1. Настройка LDAP-аутентификации пользователей

В интерфейсе системы подтверждения отправки пользователю необходимо ввести имя учетной записи и пароль. Вид учетной записи зависит от используемой схемы LDAP. В общем случае он содержит имя пользователя и домен в виде **user@domain**. В случае использования AD имя учетной записи указывается пользователем в виде **netbios-domain\user** или **domain\user**. На основе учетной записи по определенным правилам строится **Bind DN**. В конфигурации **Bind DN** указывается в виде шаблона с подстановочными параметрами:

- **%l** – полное имя учетной записи пользователя: **user@domain**
- **%u** – имя пользователя: **user**
- **%d** – домен пользователя: **domain**
- **%c** – домен, разбитый на уровни. При этом для каждого уровня повторяется подстрока от предшествующей запятой до **%c**. То есть если домен имеет вид **xxx.yyy.com**, то **dc=%c** заменяется на **dc=xxx, dc=yyy, dc=ru**. Например, шаблон **cn=%l, dc=%c** для **user@example.organisation.com** заменяется на **cn=user@example.organisation.com, dc=example, dc=organisation, dc=ru**.

Примеры Bind DN: **AD, CGP: %l; OpenLDAP: uid=%u, dc=%c**.

Поиск учетной записи пользователя ведется по атрибуту, имя и значение для которого указываются в конфигурации. Например:

- для AD: имя **sAMAccountName**, значение **%u** или имя **userPrincipalName**, значение **%l**;
- для CGP: имя **uid**, значение **%u** или имя **mail**, значение **%l**.

Из найденной записи автоматически извлекаются все атрибуты, содержащие email-адреса (при этом таких атрибутов в записи может быть несколько и в каждом атрибуте может содержаться несколько адресов). Имея полный список email-адресов пользователя, можно получить список всех сообщений этого пользователя, ожидающих подтверждения отправки.

Для настройки LDAP-аутентификации пользователей необходимо перейти в раздел **GUI Система > Конфигурация > Расширенные настройки > Администрирование системы > Вспомогательные сервисы** и в секции **Модуль подтверждения отправки** определить значения следующих параметров ([Рис.10.1](#)) :

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Локальный почтовый домен</b>                        | Локальный почтовый домен.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Список Idap-Серверов</b><br><b>Idap://host:port</b> | Список LDAP-серверов (каждый сервер должен быть указан в формате <b>Idap://host:port</b> ). Могут быть указаны адреса основного и резервного (на случай недоступности основного) серверов. Адреса серверов указываются через пробел.                                                                                                                                                                                                                          |
| <b>Шаблон bind-dn</b>                                  | Шаблон bind-dn: строка, в которой последовательности <b>%l</b> , <b>%u</b> , <b>%d</b> заменяются на значения <b>user@domain</b> , <b>user</b> и <b>domain</b> соответственно.                                                                                                                                                                                                                                                                                |
| <b>Шаблон base-dn</b>                                  | Шаблон base-dn: строка, в которой последовательности <b>%l</b> , <b>%u</b> , <b>%d</b> заменяются на значения <b>user@domain</b> , <b>user</b> и <b>domain</b> соответственно.                                                                                                                                                                                                                                                                                |
| <b>Шаблон фильтра</b>                                  | Шаблон фильтра для поиска объектов в LDAP, из которых извлекаются данные о почтовых адресах.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Атрибуты с адресами</b>                             | Атрибуты записи, в которых содержатся email-адреса. Список атрибутов указывается через пробел. Например: <b>mail proxyAddresses</b> .                                                                                                                                                                                                                                                                                                                         |
| <b>Глубина поиска в LDAP</b>                           | Глубина поиска в LDAP.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Опции LDAP</b>                                      | Дополнительные опции LDAP. Например, версия протокола LDAP (рекомендуется указать <b>version=3</b> ).                                                                                                                                                                                                                                                                                                                                                         |
| <b>Таблица трансляции доменов NETBIOS</b>              | Таблица трансляции доменов NETBIOS (таблица соответствия имен доменов для AD). Указывается список пар через пробел. Например: <b>NETBIOS1=FQDN1 NETBIOS2=FQDN2</b> .                                                                                                                                                                                                                                                                                          |
| <b>Вывод отладочной информации</b>                     | <p>Включение отладочного режима журналирования сообщений системы подтверждения отправки. Если флажок <b>Вывод отладочной информации</b> снят, то в журнал записываются только сообщения о действиях пользователей и событиях, связанных с безопасностью. Например:</p> <pre> Message ... confirmed by user Message ... canEntryed by user Access to message ... denied for user Authentication for user ... failed User ... logged User ... logged out.</pre> |

Если флажок **Вывод отладочной информации** установлен, то, помимо сообщений о действиях пользователя и событиях, связанных с безопасностью, в журнал записываются сообщения о свойствах найденных объектов (к объектам относятся, например, списки адресов), параметрах сформированного запроса в LDAP и состоянии сессии. Формат этих сообщений может меняться в зависимости от версии KEO DLP.

**Почтовый домен для вывода в окне авторизации** Почтовый домен для вывода в окне авторизации.

### Примечание

В случае LDAP-аутентификации значение параметра **Локальный почтовый домен** (локальный почтовый домен, пользователям которого разрешено подтверждать отправку сообщений) не задается.

| Модуль подтверждения отправки                                   |                              | confirm.conf                                   |
|-----------------------------------------------------------------|------------------------------|------------------------------------------------|
| Локальный почтовый домен                                        | local-domain                 |                                                |
| Список ldap-Серверов                                            | ldap://host:port ldap-server | ldap://localhost:3268                          |
| Шаблон bind-dn                                                  | bind-dn-template             | %l                                             |
| Шаблон base-dn                                                  | base-dn-template             | dc=%c                                          |
| Шаблон фильтра                                                  | filter-template              | (userPrincipalName=%l)                         |
| Атрибуты с адресами                                             | mail-attributes              | mail proxyAddresses                            |
| Глубина поиска в LDAP                                           | ldap-scope                   | subtree                                        |
| Опции LDAP                                                      | ldap-options                 | version=3                                      |
| Таблица трансляции доменов NETBIOS                              | nbios-domains                | domain.local=domain subdomain.domain.local=... |
| <input checked="" type="checkbox"/> Вывод отладочной информации | enable-debug                 |                                                |
| Почтовый домен для вывода в окне авторизации                    | auth-domain                  | domain                                         |

Рис. 10.1. Настройки модуля подтверждения отправки сообщений

После изменения параметров конфигурации необходимо нажать кнопки **Сохранить** и **Применить**.

Далее приведены примеры настроек LDAP-аутентификации для различных случаев (приведенные примеры являются работоспособными для определенной конфигурации сети, оптимальная же настройка в каждом конкретном случае выполняется администратором в соответствии с сетевой инфраструктурой):

## 1. Домен LDAP

```
local-domain = ""  
auth-type = "ldap"  
ldap-server = "ldap://10.31.6.105:389"  
bind-dn-template = "cn=%u,dc=%c"  
base-dn-template = "dc=domain,dc=com"  
filter-template = "(cn=%u)"  
mail-attributes = "mail"  
ldap-scope = "subtree"  
ldap-options = "version=3"  
nbios-domains = "domain=domain.com"
```

В параметре **Список ldap-Серверов ldap://host:port** указывается IP адрес или имя узла, на котором развернут сервер LDAP.

## 2. Домен AD

```
local-domain = ""  
auth-type = "ldap"  
ldap-server = "ldap://10.31.7.16:389"  
bind-dn-template = "%l"  
base-dn-template = "dc=domain,dc=local"  
filter-template = "(userPrincipalName=%l)"  
mail-attributes = "mail proxyAddresses"  
ldap-scope = "subtree"  
ldap-options = "version=3"  
nbios-domains = "domain=domain.local"
```

В параметре **Список ldap-Серверов ldap://host:port** указывается IP адрес или имя узла, являющегося контроллером домена.

## 3. Домен AD с дочерним доменом

```
local-domain = ""  
auth-type = "ldap"  
ldap-server = "ldap://10.31.5.113:3268"  
bind-dn-template = "%l"  
base-dn-template = "dc=domain,dc=local"  
filter-template = "(userPrincipalName=%l)"  
mail-attributes = "mail proxyAddresses"  
ldap-scope = "subtree"  
ldap-options = "version=3"  
nbios-domains = "domain=domain.local subdomain.domain=subdomain.domain.local"
```

В параметре **Список ldap-Серверов ldap://host:port** указывается IP адрес или имя узла, на котором развернут глобальный каталог (включая порт глобального каталога – 3268).

## 4. Пример настроек для работы модуля подтверждения отправки с CommuniGatePro (CGP)

```
local-domain = ""  
auth-type = "ldap"  
ldap-server = "ldap://vm40.organisation.local:389"  
bind-dn-template = "%l"  
base-dn-template = "cn=%d"  
filter-template = "(uid=%u)"
```

```
mail-attributes = "mail"
ldap-scope = "subtree"
ldap-options = "version=3"
nbios-domains = "vm40=vm40.organisation.local"
```

В параметре **Список Idap-Серверов Idap://host:port** указывается IP адрес или имя узла, на котором развернут CommuniGatePro.

## 10.2. Проверка работоспособности подсистемы подтверждения отправки сообщений

Пример: необходимо выявлять случаи отправки сообщений, например, со словом **Приказ** в теме на адреса, которые не входят в группу легитимных получателей подобных сообщений.

Для выявления таких случаев следует:

1. Идентифицировать в потоке сообщений файлы, содержащие в теме слово **Приказ**.
2. Определить, входит ли получатель такого сообщения в группу легитимных получателей сообщений, содержащих приказы.
3. В том случае, если получатель сообщения, содержащего слово **Приказ** в теме сообщения, не входит в группу легитимных получателей, поместить это сообщение в архив с пометкой **Ожидается подтверждение отправки** и отправить автору сообщения уведомление (используя заранее созданный шаблон уведомления) о возможном нарушении политики безопасности с запросом на подтверждение отправки сообщения или на ее отмену.

Чтобы реализовать вышеуказанное, необходимо в интерфейсе KEO DLP выполнить следующие действия:

1. В меню действий с разделом GUI **Политика > Шаблоны и профили > Шаблоны уведомлений** выбрать пункт **Добавить** ([Рис.10.2](#)).
2. В открывшемся окне ввести название шаблона уведомления и нажать кнопку **Сохранить** ([Рис.10.2](#)).

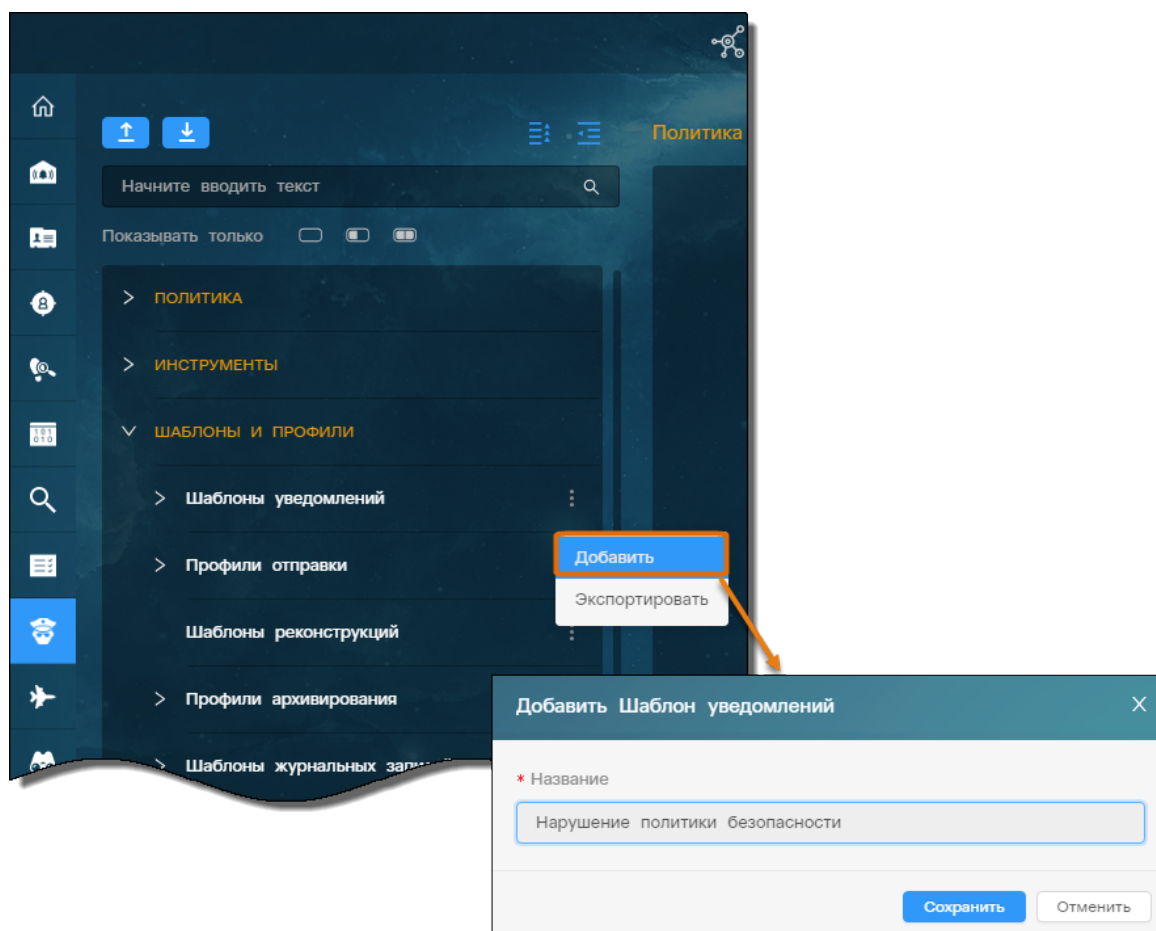


Рис. 10.2. Создание шаблона уведомления «Нарушение политики безопасности»

3. В правой части экрана ввести следующие значения полей ([Рис.10.3](#)):

- **От** – адрес администратора.
- **Кому** – адрес отправителя.
- **Тема** – например, **Нарушение политики безопасности**.
- **Название заголовка** – например, **subject**.
- **Значение заголовка** – например, **Приказ**.
- **Текст сообщения** – шаблон сообщения, в котором должна содержаться ссылка на интерфейс подтверждения отправки (URL интерфейса подтверждения).

4. Нажать кнопку **Сохранить**.



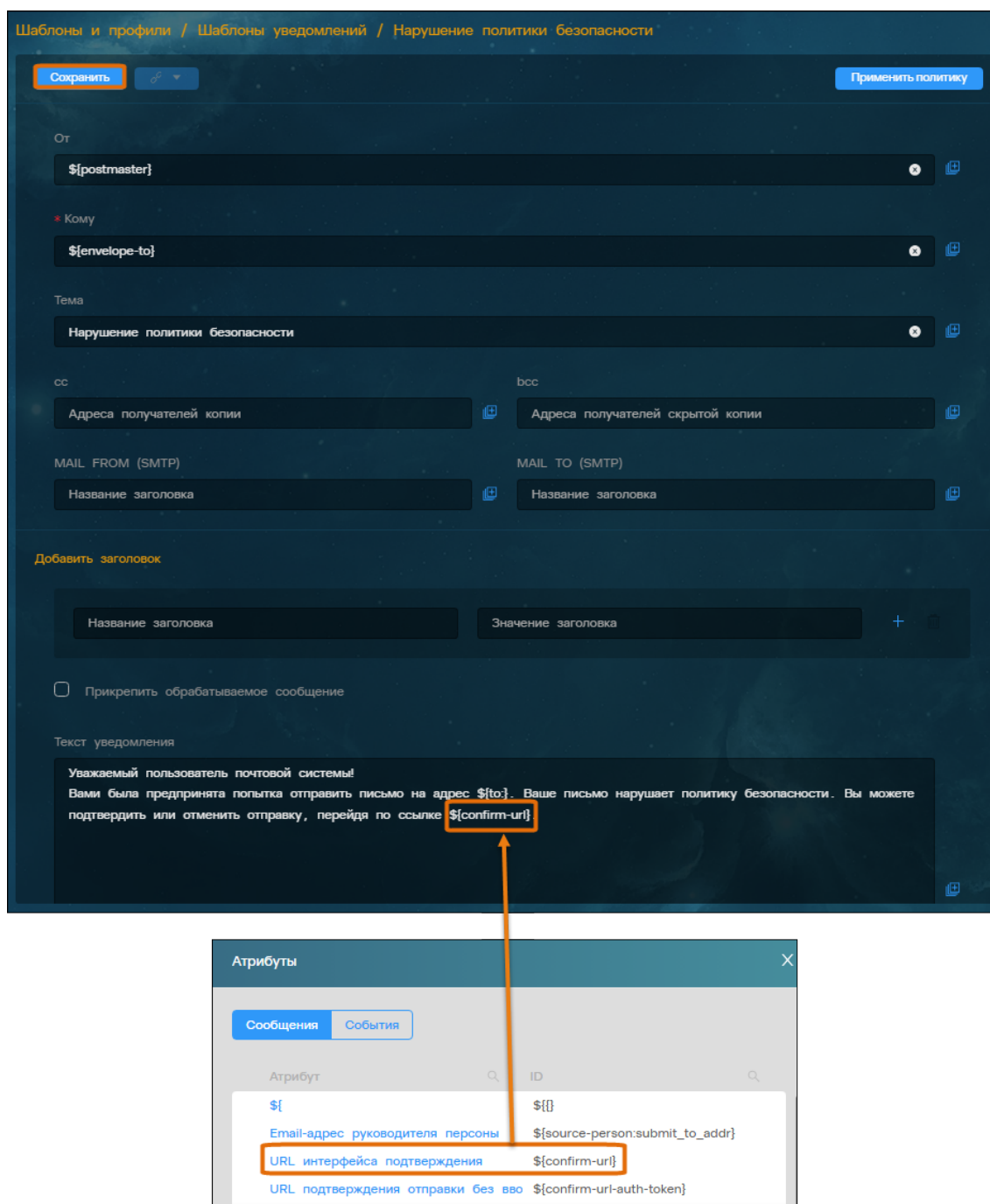


Рис. 10.3. Заполнение полей шаблона уведомления «Нарушение политики безопасности»

5. В меню действий с разделом GUI Политика > Политика > Условия выбрать пункт **Добавить** (Рис.10.4).
6. В открывшемся окне ввести название условия и нажать кнопку **Сохранить** (Рис.10.4).

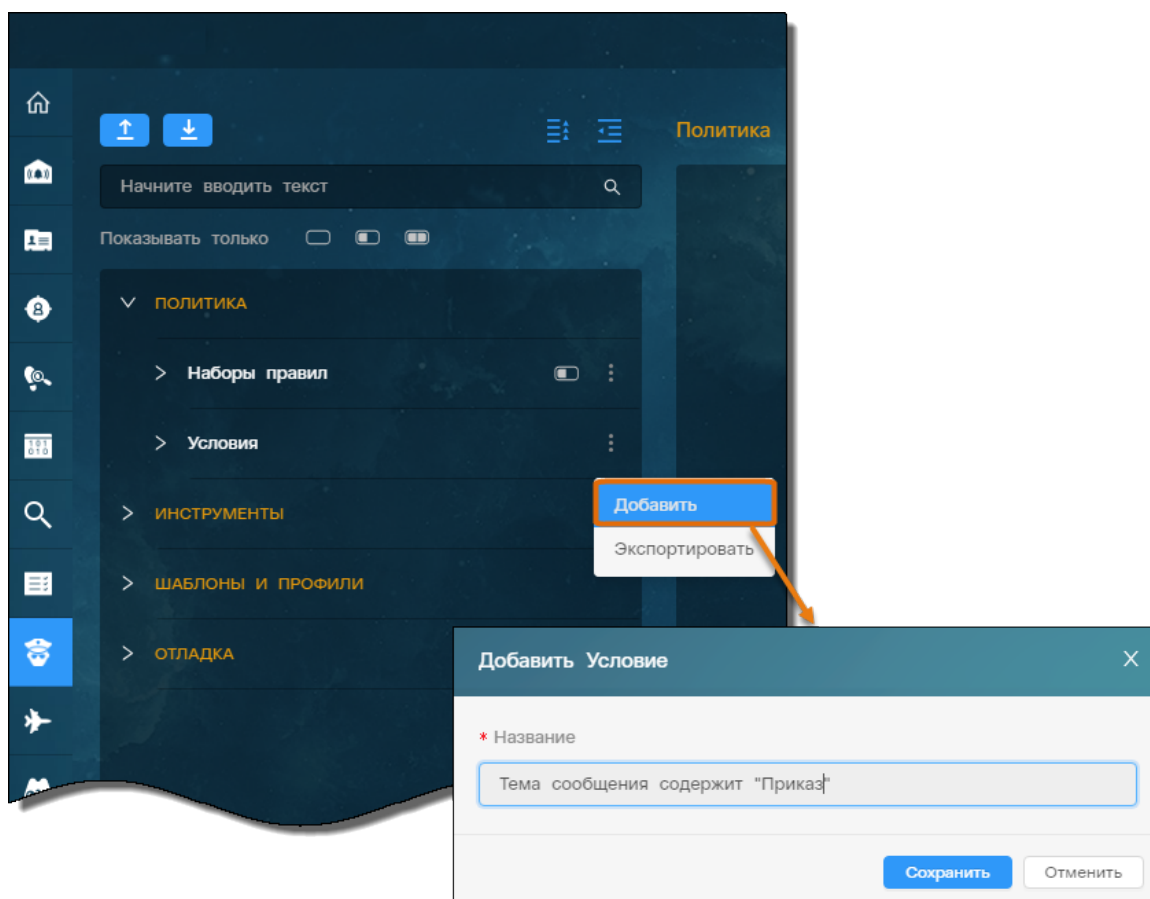


Рис. 10.4. Создание условия

7. В правой части экрана указать (выбрать из раскрывающихся списков) следующие элементы первого условия ([Рис.10.5](#)):
  - \*Заголовок
  - subject
  - Содержит
  - Приказ
8. Нажать кнопку **Добавить условие** и указать следующие элементы второго условия ([Рис.10.5](#)):
  - Получатель
  - Содержит
  - user2@company.com
9. Нажать кнопку **Сохранить** ([Рис.10.5](#)).

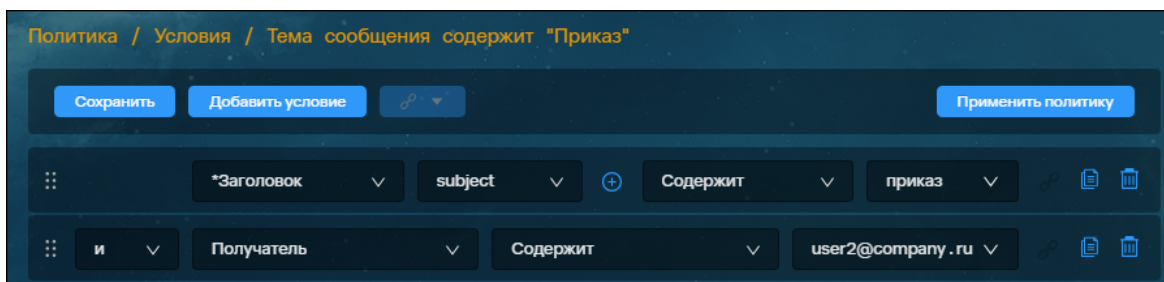


Рис. 10.5. Настройка условия

10. В меню действий с разделом GUI **Политика > Политика > Наборы правил** выбрать пункт **Добавить** (Рис.10.6).
11. В открывшемся окне ввести название набора правил (например, **Уведомление пользователей**) и нажать кнопку **Сохранить** (Рис.10.6).

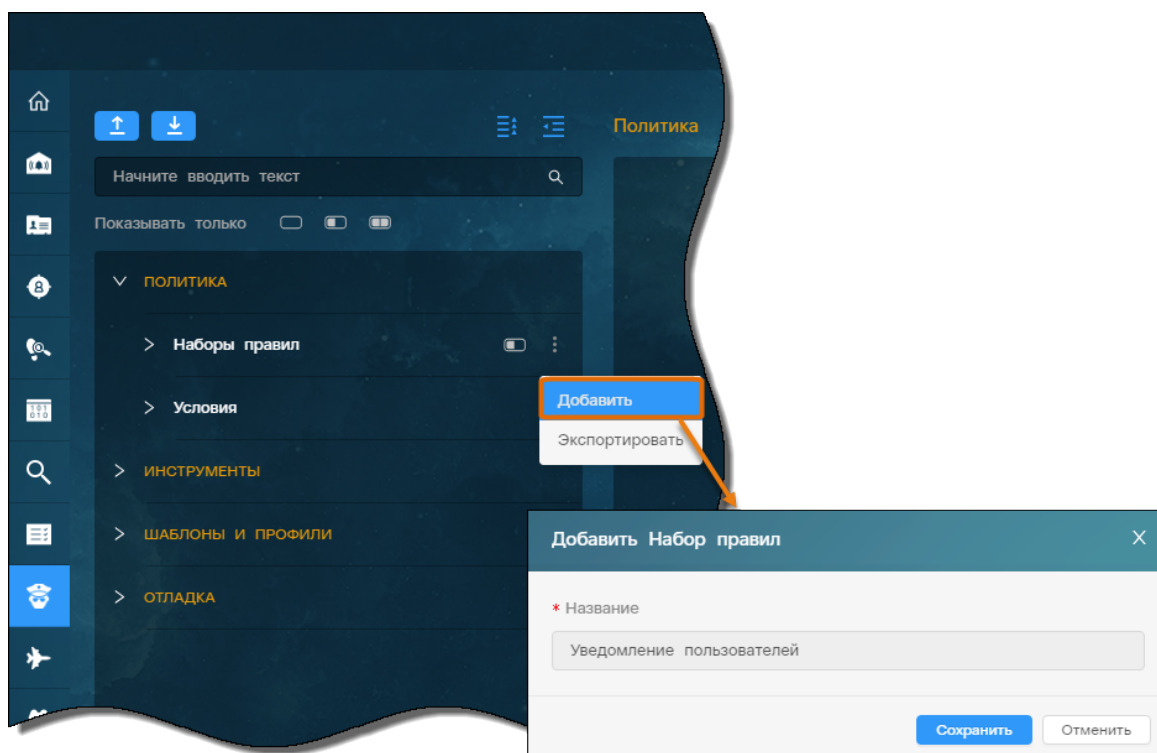


Рис. 10.6. Создание набора правил «Уведомление пользователей»

12. В правой части экрана указать элементы правила (Рис.10.7):
    - Название правила: **Уведомление пользователей**
    - Если: **Тема сообщения содержит «Приказ»**
    - то: **Отправить с подтверждением / Профиль1 / Выполнить**
- и**

Отправить уведомление / Нарушение политики безопасности / Профиль1 / Выполнить

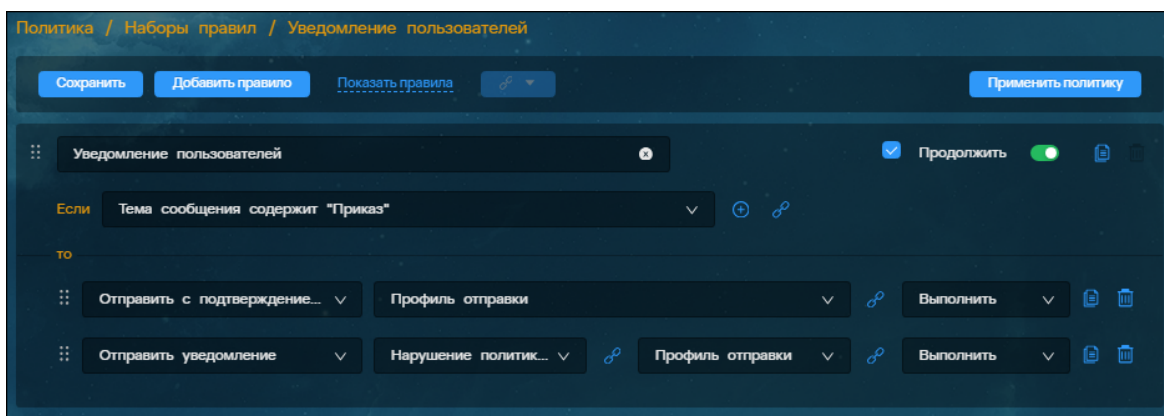


Рис. 10.7. Настройка набора правил «Уведомление пользователей»

13. Нажать кнопки **Сохранить** и **Применить политику**.
14. Отправить через KEO DLP на соответствующий адрес несколько сообщений с указанием слова **Приказ** в теме каждого сообщения. После отправки каждого сообщения на адрес, с которого отправлялись сообщения, должно прийти уведомление о нарушении политики безопасности, шаблон которого был сформирован ранее. Уведомление имеет следующий вид ([Рис.10.8](#)):

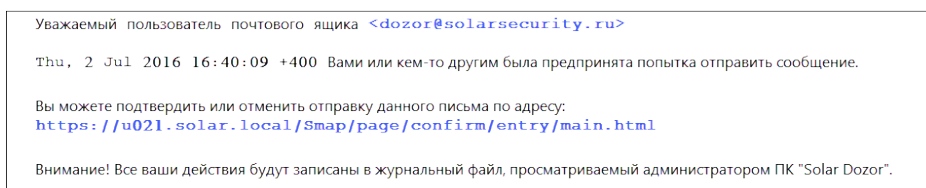


Рис. 10.8. Уведомление о нарушении политики безопасности

15. Перейти по ссылке, указанной в уведомлении, в появившемся диалоговом окне аутентификации ввести имя пользователя и пароль своей учетной записи в БД, используемой РАМ. После входа в интерфейс подтверждения отправки сообщений на экране появится таблица с данными о сообщениях, ожидающих подтверждения отправки ([Рис.10.9](#)).

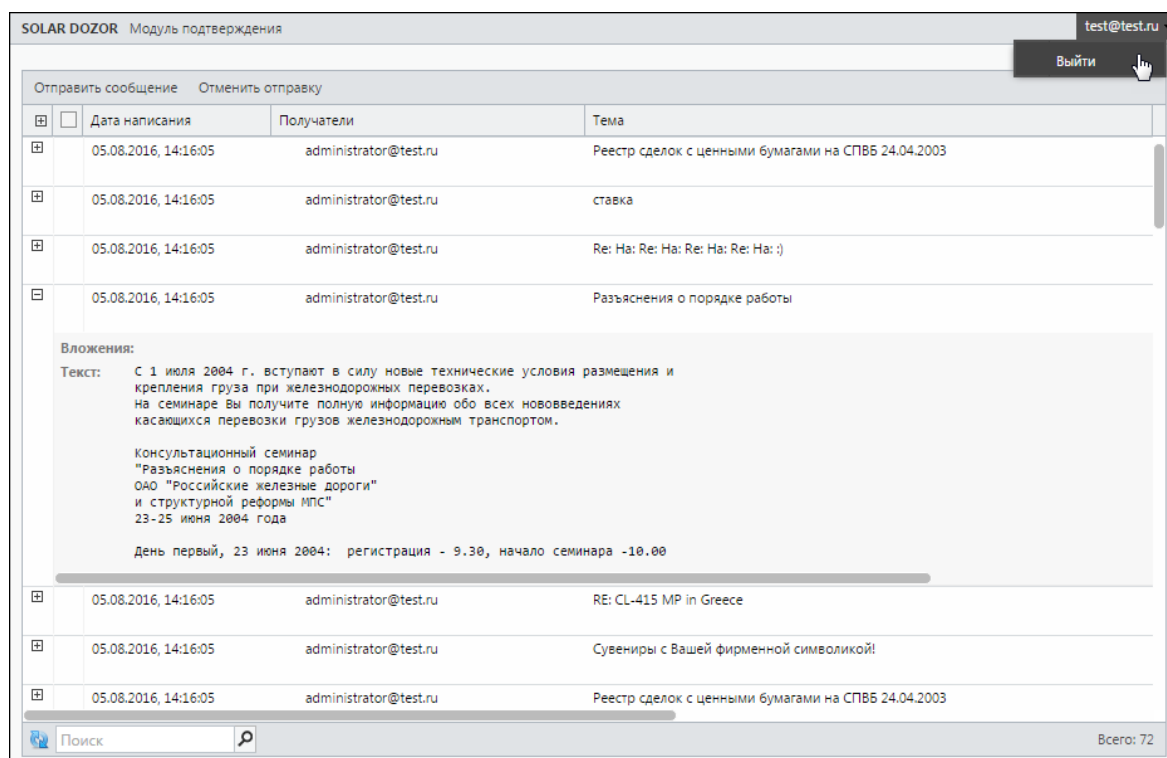


Рис. 10.9. Таблица с данными сообщений, ожидающих подтверждения отправки

16. Выбрать несколько сообщений, установив флажок в соответствующих строках таблицы, и выполнить действие **Отправить сообщение** или **Отменить отправку**. Убедиться, что данные сообщений, к которым были применены эти действия, не отображаются в таблице.
17. Выйти из интерфейса подтверждения отправки.
18. В разделе **Поиск** выполнить запрос на просмотр всех сообщений. Убедиться, что в архиве находятся сообщения с пометками, соответствующими действиям **Отправка сообщения подтверждена** и **Отправка сообщения отменена**, которые были выполнены над этими сообщениями.

## 11. Установка модуля KEO DLP File Crawler

Модуль KEO DLP File Crawler устанавливается в процессе установки KEO DLP.

После установки необходимо назначить роль **Сервер управления Краулером** одному узлу, роль **Краулер: файловые ресурсы и IMAP** всем узлам, на которых планируется использование Краулера и роль **Краулер: корпоративные мессенджеры** всем узлам, которые планируется использовать для выполнения загрузки сообщений пользователей в корпоративных мессенджерах. Для этого следует открыть в GUI KEO DLP раздел **Система**, перейти на вкладку **Узлы и роли** и выбрать соответствующий пункт в списке для нужных узлов.

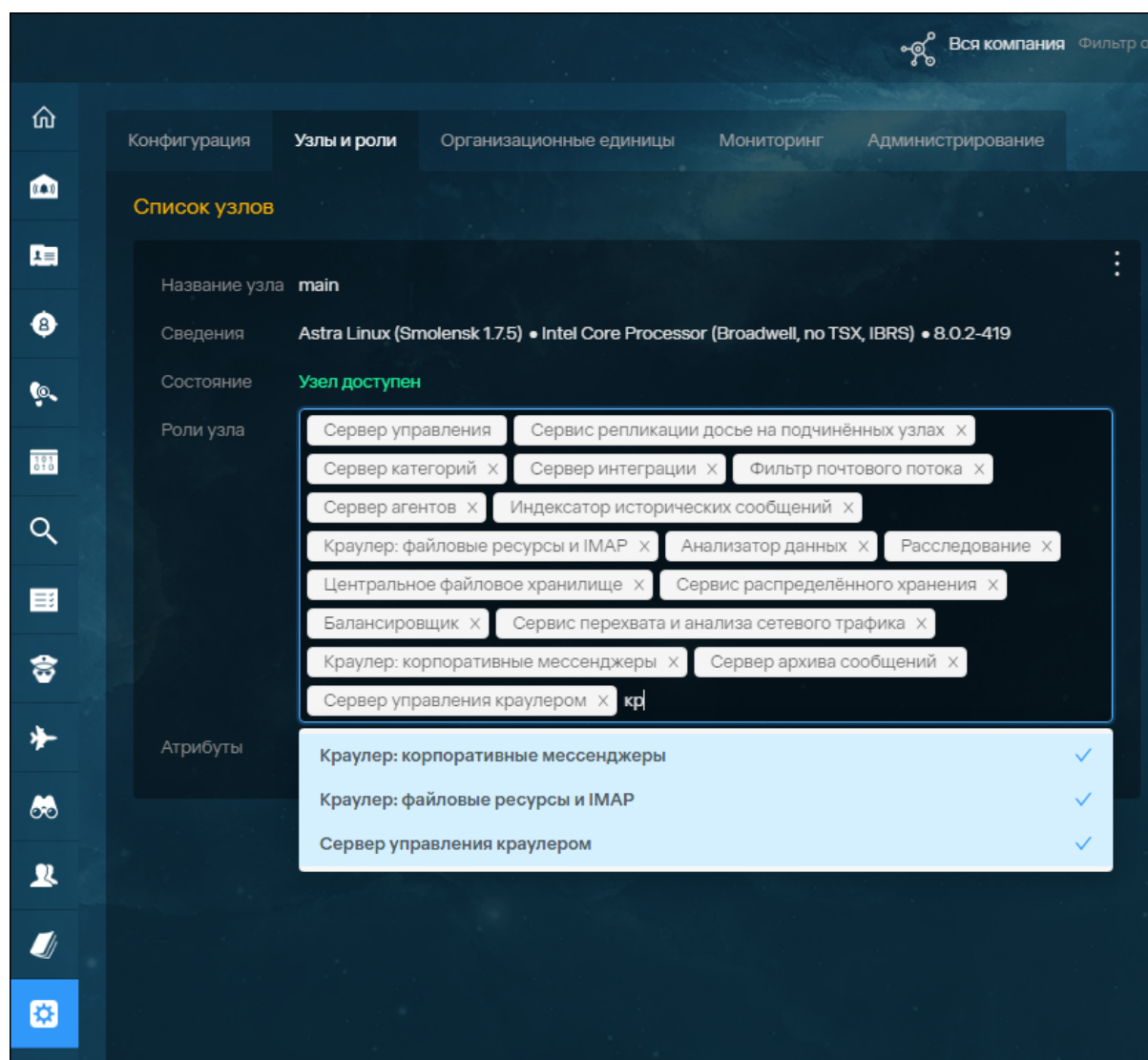


Рис. 11.1. Назначение узлу роли Краулер

После назначения узлу роли **Сервер управления Краулером** следует явно указать IP-адреса узлов кластера KEO DLP с ролью **Фильтр почтового потока**. Для этого следует выполнить действия:

1. Перейти в раздел настроек **Система > Конфигурация > Расширенные настройки > Настройка модулей перехвата > Краулер**.

2. В секции **Сервис обработки данных краулером** переключить параметр **Настройки mailfilter** в значение **Задать вручную**.

3. Раскрыть список **Настройки mailfilter** и задать значения следующих параметров:

- **Хост** – тип адреса (IP или FQDN) узла с ролью **Фильтр почтового потока**, ожидающего соединения. В зависимости от выбранного значения появляется подчиненный параметр **IP-адрес** или **Сетевой адрес**, в котором нужно указать соответствующее значение.
- **Порт** – порт, на котором узел с ролью **Фильтр почтового потока** ожидает соединения.

4. Нажать **Сохранить, Применить**.

Управление модулем осуществляется с помощью разделов **Краулер > Задачи** и **Краулер > Карта сети** ([Рис.11.2](#)).

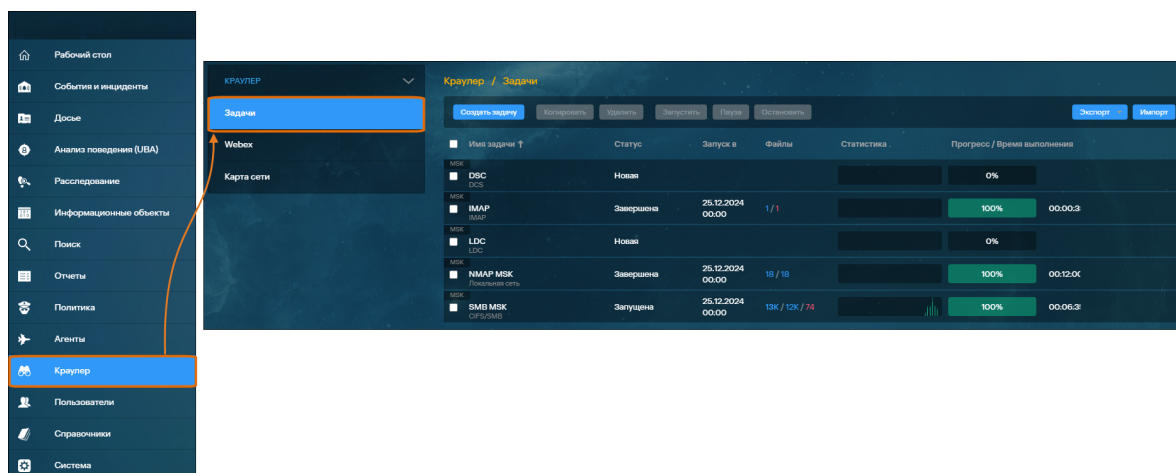


Рис. 11.2. Раздел "Краулер"

Описание работы с модулем приведено в документе *Руководство по работе с модулем «KEO DLP File Crawler»*.



---

## 12. Установка модуля KEO DLP Traffic Analyzer

Дистрибутив KEO DLP Traffic Analyzer поставляется в составе дистрибутива KEO DLP, и его установка выполняется в процессе установки KEO DLP.

Дальнейшую настройку следует выполнять согласно документу *Модуль перехвата и анализа сетевого трафика «KEO DLP Traffic Analyzer»*. *Руководство системного администратора*. После окончания настройки модуля следует перейти в GUI KEO DLP и в разделе **Система > Узлы и роли** выбрать роль **Сервер перехвата и анализа сетевого трафика**.



---

## 13. Установка агентов

Процедура установки и настройки агентов подробно описана в следующих документах:

- Модуль «KEO DLP Endpoint Agent». Руководство по установке, обновлению и удалению.
- Модуль «KEO DLP Endpoint Agent». Руководство администратора.

---

## 14. Настройка антивируса

В КЕО DLP имеется возможность использования антивируса, функционирующего на внешнем ICAP-сервере. Внешний антивирус используется для обнаружения и устранения вирусов, передаваемых по электронной почте и совершающих действия, результатом которых является частичная или полная потеря данных, остановка работы сотрудников, сбои в работе электронной почты и ПО, используемого в компании.

В ряде случаев исполняемый вредоносный или другой тип вложения сообщений может быть умышленно или случайно обфусцирован (замаскирован) под простой текст. КЕО DLP не учитывает всех возможных вариантов обфускации содержимого, поэтому для определения вредоносного содержимого рекомендуется использовать внешний антивирус.

### 14.1. Подключение Kaspersky

Для подключения внешнего антивируса Kaspersky необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Обработка сообщений** и в секции **Сервис фильтрации сообщений** в группе **Проверка сообщений с помощью антивируса** задать следующие параметры:
  - **Включить проверку с помощью антивируса** – установить флажок.
  - **Действие Антивируса** – **Сканировать**.
  - **Имя хоста** – IP-адрес ICAP-сервера антивируса Kaspersky.
  - **URL** – `/av/respmo`
  - **Порт** – 1344
2. Нажать **Сохранить** и **Применить**.
3. Перейти в CLI сервера антивируса Kaspersky, открыть для редактирования файл конфигурации `/etc/opt/kaspersky/kav4proxy.conf` и задать значения следующих параметров:
  - **AnswerMode=complete**
  - **SendAVScanResult=true**
  - **Timeout=60**
4. Сохранить и закрыть файл. Выполнить следующую команду:  
**~\$ sudo systemctl restart kav4proxy.service**

### 14.2. Использование локального антивируса

В КЕО DLP имеется возможность использования антивируса, установленного на одном из серверов кластера. Использование такой возможности **настоятельно не рекомендуется** ввиду непредсказуемых рисков и отрицательного влияния на производительность системы, однако не запрещается. При установке и настройке локального антивируса придерживайтесь следующих рекомендаций:

- 
- Внести в исключения контроля антивирусом все каталоги с файлами, имеющими отношение к работе KEO DLP, по умолчанию следующие:

- /data
- /opt/dozor
- /var/log/journal
- /tmp

Более тонкая настройка исключений высылается по запросу в службу технической поддержки.

### **Внимание!**

*Антивирусная проверка каталогов с полученными сообщениями приводит к значительному замедлению работы фильтрации из-за многократных повторных проверок сохраняемых данных (тел сообщений и извлеченных данных) и блокировки доступа к файлам.*

- Отключить контроль сетевых соединений и веб-трафика кластера KEO DLP и межкомпонентного взаимодействия ПО KEO DLP для модулей антивирусного ПО, выполняющих функции защиты от сетевых угроз.
- С осторожностью использовать модуль анализа поведения (**KESL Behavior\_Detection** и аналогичные ему). При нарушениях работы сервисов KEO DLP рекомендуется отключить использование такого модуля.

Не рекомендуется разворачивать серверные компоненты других средств защиты информации на серверах KEO DLP. Невыполнение рекомендаций может привести к значительному снижению производительности системы вплоть до полной ее остановки, нарушениям работоспособности и потере данных.

---

## 15. Удаление KEO DLP

Для удаления KEO DLP необходимо выполнить на всех узлах кластера следующие действия:

1. Загрузить командную оболочку KEO DLP, выполнив команду:

```
~$ sudo /opt/dozor/bin/shell
```

2. Остановить процессы KEO DLP, выполнив команду:

```
~$ dsctl down
```

3. Удалить схемы всех БД, кроме БД с политикой, выполнив команды (только на тех узлах, где эти схемы были созданы):

```
~$ systemctl stop dozor-data.service
```

```
~$ systemctl stop dozor-event.service
```

```
~$ rm -rf <db_schema_path>
```

где **<db\_schema\_path>** – путь к каталогу со схемой БД, как он был указан при создании этой схемы (см. разделы [8.3](#) и [8.4](#))

4. Удалить пакеты KEO DLP, выполнив команды:

```
~$ apt-get remove dlp-dozor
```

```
~$ apt-get autoremove
```

5. Удалить пакеты **traffic-agent**, выполнив команды:

```
~$ apt purge dlp-pfring
```

```
~$ apt autoremove
```

6. Удалить каталог установки KEO DLP, выполнив команду:

```
~$ rm -rf /opt/dozor
```

7. Удалить каталоги данных, выполнив команды:

```
~$ rm -rf /data/archive
```

```
~$ rm -rf /data/backups
```

```
~$ rm -rf /data/base
```

```
~$ rm -rf /data/index
```

```
~$ rm -rf /data/repos
```

```
~$ rm -rf /data/spool
```

```
~$ rm -rf /data/temp
```

---

```
~$ rm -f /etc/apt/dlp-*.list.template /etc/apt/sources.list.d/dlp-*.list
```

```
~$ rm -rf /etc/systemd/system/dozor-postgresql-*.service
```

```
~$ rm -rf /opt/iadmin
```

8. Выйти из командной оболочки KEO DLP, выполнив команду:

```
~$ exit
```

---

## Приложение А. Настройка проверки пароля пользователя для подключения к БД

Для повышения уровня безопасности можно включить принудительный ввод пароля пользователя **dozor** при подключении к следующим БД, используемым в KEO DLP:

- БД политики фильтрации.
- БД событий и инцидентов ИБ.
- БД модуля KEO DLP File Crawler.
- БД архива сообщений под управлением СУБД PostgreSQL.

Для этого необходимо выполнить следующие действия:

1. Подключиться по протоколу SSH к узлу, на котором функционирует выбранная БД:

- БД политики фильтрации – master-узел.
- БД событий и инцидентов ИБ, БД архива сообщений под управлением СУБД PostgreSQL – тот узел, на котором была создана схема этой БД. Это значение указано в параметре **Сетевое имя сервера базы данных** в разделе GUI **Система > Конфигурация > Основные настройки > Доступ к данным** в секции **Схемы соединений с БД** для соответствующей записи схемы соединения.
- БД модуля KEO DLP File Crawler – все узлы, которым назначены роли **Сервер управления Краулером** и/или **Краулер: файловые ресурсы и IMAP**.

2. Подключиться к БД, выполнив следующую команду:

```
# psql -U dozor -h localhost -p <port>
```

где **<port>** – порт, на котором БД ожидает соединения:

- БД политики фильтрации – 5434.
- БД модуля KEO DLP File Crawler – порт по умолчанию 5439. Актуальное значение указано в параметре **Порт для сервиса БД Краулера** в разделе GUI **Система > Конфигурация > Расширенные настройки > Краулер** в секции **Подключение к БД File Crawler**.
- БД событий и инцидентов ИБ, БД архива сообщений под управлением СУБД PostgreSQL – значение порта указано в параметре **Сетевой порт сервера базы данных** в разделе GUI **Конфигурации > Основные настройки > Доступ к данным** в секции **Схемы соединений с БД** для соответствующей записи схемы соединения.

3. Задать новый пароль пользователя БД, выполнив команду:

```
# alter user dozor with password '<password>';
```

где **<password>** – новый пароль пользователя БД, например:

```
# alter user dozor with password 'q1';
```

4. Перейти в каталог БД:

- БД политики фильтрации – **/data/base/dozor/pgsql**
- БД модуля KEO DLP File Crawler – **/data/base/crawler/pgsql/**
- БД событий и инцидентов ИБ, БД архива сообщений под управлением СУБД PostgreSQL – путь к каталогу можно узнать, выполнив команду:

**# ps ax | grep <port>**

где **<port>** – порт, на котором выбранная БД ожидает соединения. В результате выполнения команды на экран будет выведена информация следующего вида:

```
# ps ax | grep 5435
10440 ?      S    3:25 /usr/pgsql-9.6/bin/postmaster -p 5435 -D /data/base/smap-archive
31078 pts/0  S+   0:00 grep 5435
```

Путь **/data/base/smap-archive** в данном примере является путем к каталогу БД.

5. Открыть файл **pg\_hba.conf** для редактирования и найти строки следующего вида:

```
# IPv4 local connections:
host    all         all         <IP>/<mask>      trust
```

Убедиться, что в качестве значений **<IP>/<mask>** установлены правильные значения доверенной подсети и маски. Заменить слово **trust** на **password**, сохранить и закрыть файл.

6. Задать пароль пользователя БД в параметрах конфигурации KEO DLP:

- БД политики, БД событий и инцидентов ИБ, БД архива сообщений под управлением СУБД PostgreSQL – параметр **Пароль пользователя базы данных** в разделе **GUI Система > Конфигурация > Основные настройки > Доступ к данным** в секции **Схемы соединений с БД** для соответствующей записи схемы соединения.
- БД модуля KEO DLP File Crawler – параметр **Пароль пользователя БД с метазаданиями**, раздел **GUI Конфигурации > Расширенные настройки > Краулер**, секции:
  - Центр управления File Crawler;
  - Прокси центра управления File Crawler;
  - Сервис отпечатков File Crawler.

7. Если приведенные выше шаги выполнялись для БД событий и инцидентов ИБ или БД архива сообщений под управлением СУБД PostgreSQL, перезапустить БД, выполнив команду следующего вида:

**~\$ sudo systemctl restart <db-script-name>.service**

где **<db-script-name>** – имя скрипта автозапуска БД, который был создан при создании схемы этой БД. Если имя этого скрипта по каким-либо причинам не может быть установлено, следует выполнить следующие команды:

---

```
~$ sudo su - dozor
```

```
$ pg_ctl stop -D /data/base/<db-name>
```

```
$ pg_ctl start -D /data/base/<db-name>
```

где **<db-name>** – имя каталога БД (например, в шаге 4 – **smap-archive**).

8. Перезагрузить процессы KEO DLP, выполнив следующую команду:

```
~$ sudo /opt/dozor/bin/dsctl restart
```



---

## Приложение В. Настройка подключения к БД под доменной учетной записью

Если в организации используются доменные учетные записи, то от их имени можно подключаться к БД КЕО DLP. Настройка подключения приведена на примере БД архива и состоит из следующих этапов:

1. Создание и настройка доменной учетной записи для БД PostgreSQL (раздел [В.1](#));
2. Настройка LDAPS-аутентификации (опционально) (раздел [В.2](#));
3. Настройка SSL-подключения к БД PostgreSQL (раздел [В.3](#));
4. Настройка конфигурационного файла БД PostgreSQL для использования SSL-подключений (раздел [В.4](#));

### В.1. Создание доменной учетной записи для БД PostgreSQL

Создание и настройка доменной учетной записи для БД PostgreSQL выполняется следующим образом:

1. Создать и настроить БД архива PostgreSQL по инструкции из раздела [8.3](#).
2. В AD организации создать учетную запись пользователя.
3. Подключиться по протоколу SSH к узлу, на котором функционирует данная БД. Адрес узла указан в параметре **Сетевое имя сервера базы данных** в разделе GUI **Система > Конфигурация > Основные настройки > Доступ к данным > Схемы соединений с БД** для соответствующей схемы соединения в секции **Тип базы данных > Настройки соединения с базой**.
4. Переключиться на работу от имени пользователя **dozor**, выполнив команду:

```
# su - dozor
```

5. Подключиться к БД архива сообщений под управлением СУБД PostgreSQL, выполнив команду:

```
$ psql -h <host> -p <port> -d <db_name>
```

где:

- **<host>** – параметр **Сетевое имя сервера базы данных**;
- **<port>** – параметр **Сетевой порт сервера базы данных**;
- **<db\_name>** – параметр **Имя базы данных**.

из соответствующего раздела GUI (см. шаг [3](#)).

6. Создать учетную запись пользователя СУБД PostgreSQL, выполнив команду:

```
$ CREATE USER "<ad_user>";
```

где **<ad\_user>** – имя УЗ пользователя СУБД PostgreSQL, совпадающее с именем пользователя AD, созданным на шаге 2.

7. Назначить созданную на предыдущем шаге учетную запись владельцем данной БД и подтвердить полномочия суперпользователя, выполнив команды:

```
$ ALTER DATABASE <db_name> OWNER to "<ad_user>";
```

```
$ ALTER ROLE "<ad_user>" WITH SUPERUSER INHERIT CREATEROLE CREATEDB;
```

```
$ \q
```

#### Внимание!

*В PostgreSQL двойные кавычки являются частью имени объектов, но в самом имени объекта не отображаются. Если в имени объекта есть точка и/или нижнее подчеркивание, то использование двойных кавычек строго обязательно.*

#### Примечание

*Пользователь **dozor** сохраняет права суперпользователя. При необходимости возврата к пользователю **dozor** нужно снова назначить его владельцем данной БД.*

#### Примечание

*Если требуется удаление пользователя, то необходимо выполнить следующие действия:*

- a. Назначить владельцем БД другого пользователя, выполнив команду:

```
$ ALTER DATABASE <db_name> OWNER to "dozor";
```

- b. Удалить созданного пользователя, выполнив команду:

```
$ DROP USER "<ad_user>";
```

#### Примечание

*Для УЗ также можно задать описание, если это требуется, выполнив команду вида:*

```
$ COMMENT ON ROLE <ad_user> is 'Текст комментария одной строкой';
```

*Проверить описание УЗ можно при помощи команды:*

```
$ \du+
```

8. Перейти в каталог БД архива сообщений. Путь к каталогу можно узнать, выполнив команду:

```
$ ps ax | grep <port>
```

подставляя значение **<port>** из шага 5.

В выводе команды будет содержаться путь к каталогу с исполняемыми файлами PostgreSQL. Например:

```
$ ps ax | grep 5445
15444 ? S 0:00 /usr/pgsql-11/bin/postmaster -p 5445 -D /data/base/archive
```

Путь **/data/base/archive** в данном примере является путем к каталогу БД.

9. Открыть конфигурационный файл **pg\_hba.conf** для редактирования и в секции **# IPv4 local connections:** найти строки следующего вида:

```
host all all <IP>/<mask> trust
```

Заменить слово **trust** на **ldap** и настроить LDAP-аутентификацию. Сохранить и закрыть файл.

Пример:

```
host all all <IP>/<mask> ldap ldapserver="GALAXY-DC.GALAXY.local"
ldapport="389" ldaprefix="galaxy\" ldapsuffix="" ldapscheme="ldap"
```

### Примечание

Если БД вынесена на отдельный сервер, и к ней настраивается подключение других узлов, необходимо добавить аналогичные записи для этих серверов вида:

```
host all all <IP_узел1>/<mask_узел1> ldap ldapserver="GALAXY-DC.GALAXY.local" ldapport="389"
ldaprefix="galaxy\" ldapsuffix="" ldapscheme="ldap"
host all all <IP_узел2>/<mask_узел2> ldap ldapserver="GALAXY-DC.GALAXY.local" ldapport="389"
ldaprefix="galaxy\" ldapsuffix="" ldapscheme="ldap"
host all all <IP_узел3>/<mask_узел3> ldap ldapserver="GALAXY-DC.GALAXY.local" ldapport="389"
ldaprefix="galaxy\" ldapsuffix="" ldapscheme="ldap"
```

Остальные строки в конфигурационном файле можно закомментировать.

Пример содержания файла **pg\_hba.conf** после выполненных настроек:

```
# TYPE DATABASE USER ADDRESS METHOD
# "local" is for Unix domain socket connections only
#local all all trust
# IPv4 local connections:
#host all all .241/32 trust
#host all all .253/32 ldap ldapserver="GALAXY-DC.GALAXY.local" ldapport="389" ldaprefix="galaxy\" ldapsuffix="" ldapscheme="ldap"
#host all all .232/32 ldap ldapserver="GALAXY-DC.GALAXY.local" ldapport="389" ldaprefix="galaxy\" ldapsuffix="" ldapscheme="ldap"
# IPv6 local connections:
#host all all ::1/128 trust
# Allow replication connections from localhost, by a user with the
# replication privilege.
#local replication all trust
#host replication all .241/32 trust
#host replication all ::1/128 trust
```

Рис. В.1. Настройка LDAP-аутентификации в **pg\_hba.conf**

Сохранить и закрыть файл.

10. Переключиться на работу от имени пользователя **root** и перезапустить сервис БД архива сообщений, выполнив команды:

**\$ exit**

**\$ su - root**

**# systemctl restart <db\_service\_name>**

где **<db\_service\_name>** – имя сервиса БД архива сообщений, которое можно определить следующим образом:

- a. Узнать pid сервиса БД в системе, выполнив с соответствующей подстановкой команду вида:

**# ss -anp4 | grep <db\_port> | grep -i listen**

На экран будет выведена информация следующего вида:

```
tcp LISTEN 0 224 198.51.100.50:5445 0*:* users:(("postgres",pid=1080,fd=3))
```

В данном примере значением pid является 1080.

- b. По полученному на предыдущем шаге значению pid узнать имя сервиса БД, выполнив с соответствующей подстановкой команду вида:

**# systemctl status <pid> | head -n1**

На экран будет выведена информация следующего вида:

```
● dozor-postgresql.service - KEO DLP Archive database server
```

В данном примере именем сервиса БД является dozor-postgresql.service.

11. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Доступ к данным > Схемы соединений с БД** и для соответствующей схемы соединения в секции **Тип базы данных > Настройки соединения с базой** изменить значение параметра **Пользователь базы данных** на имя, заданное на шаге 2 и ввести пароль к УЗ в строке **Пароль пользователя базы данных**.
12. Проверить подключение к БД, нажав кнопку **Проверить**. При успешном завершении проверки архивирования сообщений нажать **Сохранить** и **Применить**.

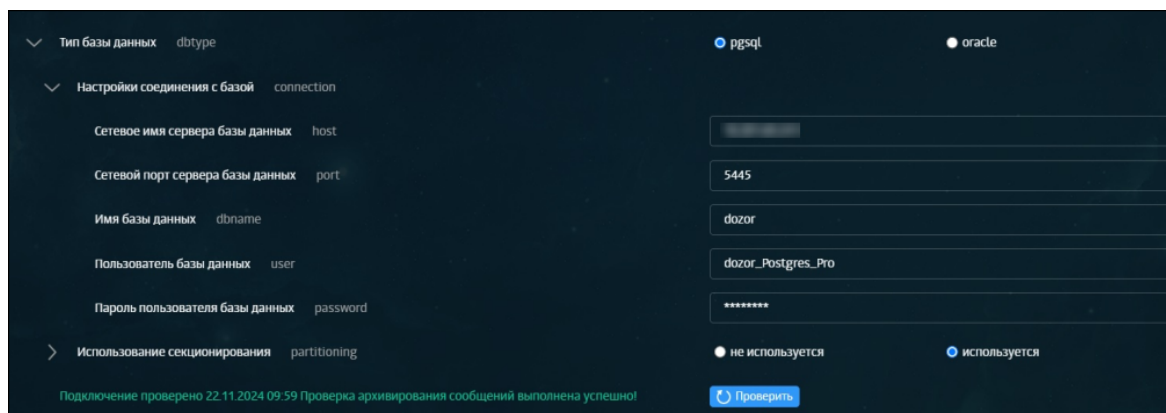


Рис. В.2. Проверка соединения с БД после смены пользователя

## Внимание!

Если проверка соединения с БД завершается с ошибкой, то необходимо перейти в интерфейс командной строки и выполнить следующие команды:

- a. Подключиться к БД от имени доменного пользователя с помощью команды:

```
# psql -h <host> -p <port> -U <ad_user> -d <db_name>
```

подставляя значения из шагов [5](#), [6](#).

Если при подключении возникает ошибка:

```
error obtaining mac configuration for user
```

то необходимо открыть для редактирования конфигурационный файл **postgresql.conf** в каталоге, путь к которому был найден на шаге [8](#), и изменить значение параметра **ac\_ignore\_maclabel** с **false** на **true**:

```
ac_ignore_maclabel = true
```

Сохранить и закрыть файл.

- b. Перезапустить сервис БД, выполнив команду:

```
# systemctl restart <db_service_name>
```

подставляя значение, найденное на шаге [10](#).

## В.2. Настройка LDAPS-аутентификации

При необходимости использования LDAPS-аутентификации следует настроить ее в интерфейсе командной строки узла с БД PostgreSQL:

1. Только для Astra Linux: проверить наличие пакета **ldap-utils**, выполнив команду:

```
# apt list --installed | grep ldap-utils
```

Если он отсутствует, установить его, выполнив команду:

```
# apt update
```

```
# apt install ldap-utils
```

2. Выгрузить сертификат в формате PEM из LDAP-сервера организации, выполнив команду вида:

```
# openssl s_client -connect <ip_ldap>:636 </dev/null | sed -ne '/-BEGIN CERTIFICATE\|/END CERTIFICATE-/p' > /var/tmp/<cert_name>.pem
```

где **<ip\_ldap>** – IP-адрес LDAP-сервера (FQDN недопустим), **<cert\_name>** – произвольное имя файла сертификата.

3. Проверить выгруженный сертификат, выполнив команду вида:

```
# openssl x509 -in /var/tmp/<cert_name>.pem -noout -text
```

4. Переместить выгруженный сертификат в каталог `/etc/ssl/certs/`, выполнив команду вида:

```
# mv /var/tmp/<cert_name>.pem /etc/ssl/certs/
```

5. Проверить права PEM-файла сертификата, выполнив команду:

```
# ls -la /etc/ssl/certs/<cert_name>.pem
```

Убедиться, что в первом столбце указано значение `-rw-r--r--`, в третьем и четвертом – `root`.

6. Отредактировать конфигурационный файл `Idap.conf`, расположенный в каталоге `/etc/ldap/`, так, чтобы он содержал строки следующего вида:

```
BASE dc=galaxy,dc=local
URL ldaps://galaxy-dc.galaxy.local:636
TLS_CACERT /etc/ssl/certs/<cert_name>.pem
```

Заменить значения на актуальные. Сохранить и закрыть файл.

#### Внимание!

Если сертификат не проходит проверку, то необходимо в том же файле закомментировать параметр `TLS_CACERT` и добавить параметр `TLS_REQCERT` для отключения проверки:

```
BASE dc=galaxy,dc=local
URL ldaps://galaxy-dc.galaxy.local:636
#TLS_CACERT /etc/ssl/certs/<cert_name>.pem
TLS_REQCERT never
```

Параметр `TLS_REQCERT { never | allow | try | demand }` указывает, каким образом клиент будет обрабатывать получение (или неполучение) сертификата сервера. При значении `never` клиент не будет запрашивать сертификат сервера, но если он его получит, то проигнорирует и продолжит соединение.

7. Выполнить шаги [8-12](#) из предыдущего раздела.

## В.3. Настройка SSL-подключения к БД PostgreSQL

Для настройки SSL-подключения к БД PostgreSQL возможно использование самоподписанных сертификатов (раздел [В.3.1](#)) либо корпоративных сертификатов (раздел [В.3.2](#)).

### В.3.1. Использование самоподписанных сертификатов

Для установления SSL-соединения с БД PostgreSQL можно воспользоваться самоподписанными сертификатами. Для их выпуска необходимо выполнить следующие действия:

1. Подключиться по протоколу SSH к узлу, на котором функционирует БД PostgreSQL.
2. Переключиться на пользователя `dozor` и перейти в каталог БД для создания сертификатов (определение пути до каталога БД описано в шаге [8](#)), выполнив команды:

```
# su - dozor
```

---

```
$ cd /data/base/archive/
```

3. Сгенерировать закрытый ключ для сертификата с указанием имени файла создаваемого ключа, выполнив команду:

```
$ openssl genrsa -aes128 2048 > <key_name>.key
```

В ходе выполнения команды на экран выводится приглашение ввести на клавиатуре кодовое слово для создаваемого ключа – **Enter pass phrase for <key\_name>.key:**. Оно может состоять только из букв и/или цифр (специальные символы не допускаются) и должно быть длиной не менее 4 символов. Потребуется ввести его дважды.

4. После задания кодового слова, необходимо удалить его для корректного запуска БД, выполнив команду:

```
$ openssl rsa -in <key_name>.key -out <key_name>.key
```

5. Задать права для созданного ключа, выполнив команду:

```
$ chmod 600 <key_name>.key
```

6. Сгенерировать серверный сертификат, выполнив команду:

```
$ openssl req -new -key <key_name>.key -days 365 -out <cert_name>.crt -x509
```

На экран будет выведено приглашение ввести информацию, которая будет включена в сертификат. Обязательны для заполнения следующие параметры:

- **Country Name** – двухбуквенный код страны;
- **Locality Name** – город;
- **Organization Name** – наименование организации;
- **Common Name** – FQDN-адрес узла, на котором функционирует БД.

Остальные параметры можно не указывать, для этого достаточно в каждой строке ввести символ «.» (точка):

- **State or Province Name** – регион;
- **Organizational Unit Name** – название подразделения, департамента и т.д.

7. Задать права для созданного сертификата, выполнив команду:

```
$ chmod 644 <cert_name>.crt
```

8. Создать пользовательский сертификат (trusted root certificate) путем копирования ранее созданного серверного сертификата, выполнив команду:

```
$ cp <cert_name>.crt <root_cert_name>.crt
```

9. Задать права для созданного на предыдущем шаге пользовательского сертификата, выполнив команду:

```
$ chmod 644 <root_cert_name>.crt
```

10. Назначить владельцем сертификатов и закрытого ключа пользователя dozor, выполнив команды:

```
$ chown dozor:dozor /data/base/archive/<root_cert_name>.crt
```

```
$ chown dozor:dozor /data/base/archive/<cert_name>.crt
```

```
$ chown dozor:dozor /data/base/archive/<key_name>.key
```

Проверить права с помощью команды **ls -la** и убедиться, что в первом столбце указаны следующие значения:

- для **<root\_cert\_name>** – **-rw-r--r--**;
- для **<cert\_name>** – **-rw-r--r--**;
- для **<key\_name>** – **-r-----**.

В третьем и четвертом столбцах для всех файлов должно быть указано значение **dozor**.

### В.3.2. Использование корпоративных сертификатов

Для установления SSL-соединения с БД PostgreSQL можно воспользоваться корпоративными сертификатами, для чего необходимо выполнить следующие действия:

1. Подключиться по протоколу SSH к узлу, на котором функционирует БД PostgreSQL.
2. Переключиться на пользователя dozor, выполнив команду:

```
# su - dozor
```

3. Запросить у организации-владельца сертификатов серверный и пользовательский сертификаты, а также закрытый ключ.

#### Примечание

Если полученные файлы представлены в PFX-формате, то необходимо извлечь из них сертификат и закрытый ключ. Для извлечения сертификата следует выполнить команду:

```
$ openssl pkcs12 -in <pfx_filename>.pfx -clcerts -nokeys -out <cert_name>.crt
```

При выполнении команды понадобится ввести пароль, которым защищен PFX-контейнер.

Для извлечения закрытого ключа следует выполнить команду:

```
$ openssl pkcs12 -in <pfx_filename>.pfx -nocerts -out <key_name>.key
```

При выполнении команды будет запрошен пароль, которым защищён PFX-контейнер. После его ввода будет предложено ввести новое кодовое слово (PEM pass phrase), которым будут зашифрованы данные закрытого ключа при выгрузке.

После задания кодового слова, необходимо удалить его для корректного запуска БД, выполнив команду:



```
$ openssl rsa -in <key_name>.key -out <key_name>.key
```

Сертификат и закрытый ключ будут извлечены в тот же каталог, в котором находится PFX-файл.

4. Задать права для созданного ключа, выполнив команду:

```
$ chmod 600 <key_name>.key
```

5. Задать права для серверного сертификата, выполнив команду:

```
$ chmod 644 <cert_name>.crt
```

6. Задать права для пользовательского сертификата, выполнив команду:

```
$ chmod 644 <root_cert_name>.crt
```

7. Назначить владельцем сертификатов и закрытого ключа пользователя dozor, выполнив команды:

```
$ chown dozor:dozor /data/base/archive/<root_cert_name>.crt
```

```
$ chown dozor:dozor /data/base/archive/<cert_name>.crt
```

```
$ chown dozor:dozor /data/base/archive/<key_name>.key
```

Проверить права с помощью команды **ls -la** и убедиться, что в первом столбце указаны следующие значения:

- для **<root\_cert\_name>** – **-rw-r--r--**;
- для **<cert\_name>** – **-rw-r--r--**;
- для **<key\_name>** – **-r-----**.

В третьем и четвертом столбцах для всех файлов должно быть указано значение **dozor**.

## B.4. Настройка конфигурационного файла БД на использование SSL

Для настройки необходимо выполнить в интерфейсе командной строки узла, на котором функционирует БД PostgreSQL, следующие действия:

1. Открыть для редактирования конфигурационный файл **postgresql.conf**, расположенный в каталоге БД, и записать в секцию **# - SSL** - следующие параметры:

```
ssl = on
ssl_ca_file = '<root_cert_name>.crt'
ssl_cert_file = '<cert_name>.crt'
ssl_crl_file = ''
ssl_key_file = '<key_name>.key'
ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL' # allowed SSL ciphers
ssl_prefer_server_ciphers = on
```

```
# - SSL -

ssl = on
ssl_ca_file = 'NN-Root-CA.crt'
ssl_cert_file = 'NN-Postgre.crt'
ssl_crl_file = ''
#ssl_crl_dir = ''
ssl_key_file = 'NN-Postgre1.key'
ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL' # allowed SSL ciphers
ssl_prefer_server_ciphers = on
#ssl_ecdh_curve = 'prime256v1'
#ssl_min_protocol_version = 'TLSv1.2'
#ssl_max_protocol_version = ''
#ssl_dh_params_file = ''
#ssl_passphrase_command = ''
#ssl_passphrase_command_supports_reload = off
```

Рис. В.3. Пример заполнения секции # - SSL в конфигурационном файле postgresql.conf

Сохранить и закрыть файл.

- В том же каталоге открыть для редактирования конфигурационный файл **pg\_hba.conf** и в секции **IPv4 local connections** заменить **host** на **hostssl**:

```
hostssl all all <IP_1>/<mask_1> ldap ldapserver="GALAXY-DC.GALAXY.local" ldapport="636"
ldaprefix="galaxy\" ldapsuffix="" ldapscheme="ldaps"
hostssl all all <IP_2>/<mask_2> ldap ldapserver="GALAXY-DC.GALAXY.local" ldapport="636"
ldaprefix="galaxy\" ldapsuffix="" ldapscheme="ldaps"
hostssl all all <IP_3>/<mask_3> ldap ldapserver="GALAXY-DC.GALAXY.local" ldapport="636"
ldaprefix="galaxy\" ldapsuffix="" ldapscheme="ldaps"
```

Сохранить и закрыть файл.

- Перезапустить сервис БД, выполнив команду:

```
# systemctl restart <db_service_name>
```

подставляя название сервиса, определенное на шаге [10](#).

- Перейти в раздел GUI Система > Конфигурация > Основные настройки > Доступ к данным > Схемы соединений с БД и для соответствующей схемы соединения в секции Тип базы данных > Настройки соединения с базой проверить подключение к БД, нажав кнопку Проверить.

- Перейти в CLI узла с данной БД и проверить подключение других узлов кластера к ней с помощью команды:

```
# psql -h <host> -p <port> -U <ad_user> -d <db_name>
```

подставляя значения из шагов [5](#), [6](#).

После ввода пароля доменной учетной записи при успешном подключении отобразится строка следующего вида:

sql (11.21 (Debian 1:11.21-astra.se6+ci1))  
 SSL-соединение (протокол: TLSv1.3, шифр: TLS\_AES\_256\_GCM\_SHA384, бит: 256, сжатие: выкл.)  
 Введите "help", чтобы получить справку

6. Выполнить запрос для проверки SSL-соединений с БД при помощи одной из команд:

```
# SELECT * FROM pg_stat_activity JOIN pg_stat_ssl USING(pid);
```

```
# SELECT * FROM pg_stat_ssl WHERE pid = pg_backend_pid();
```

| pid   | datid | datname | usesysid | username           | query_start                                   | application_name             | client_addr   | client_hostname | client_port | backend_start              | state      | backend_type | ssl | version | wait_event             | wait_event_type | cipher | backend_pid |
|-------|-------|---------|----------|--------------------|-----------------------------------------------|------------------------------|---------------|-----------------|-------------|----------------------------|------------|--------------|-----|---------|------------------------|-----------------|--------|-------------|
| 17497 |       |         |          |                    |                                               |                              |               |                 |             | 2024-12-04 15:03:57.972158 |            |              |     |         |                        |                 |        |             |
| +03   |       |         |          |                    |                                               |                              |               |                 |             |                            |            |              |     |         |                        |                 |        |             |
|       |       |         |          |                    |                                               | autovacuum launcher          |               |                 |             |                            | Activity   |              | f   |         | AutoVacuumMain         |                 |        |             |
| 17499 |       |         | 10       | dozor              |                                               |                              |               |                 |             | 2024-12-04 15:03:57.973112 |            |              |     |         |                        |                 |        |             |
| +03   |       |         |          |                    |                                               | logical replication launcher |               |                 |             |                            | Activity   |              | f   |         | LogicalLauncherMain    |                 |        |             |
| 27037 | 16384 | dozor   | 18127    | dozor_Postgres_Pro | indexer-ng                                    |                              | 192.168.1.241 |                 |             | 2024-12-16 09:27:48.269993 |            |              |     |         |                        |                 |        |             |
| +03   |       |         |          |                    | 2024-12-16 09:27:48.30586+03                  |                              | 192.168.1.241 |                 |             |                            | ClientRead |              | t   | TLSv1.3 | TLS_AES_256_GCM_SHA384 |                 | 2      |             |
| 56    | f     |         |          |                    | SET application_name = 'indexer-ng'           |                              |               |                 |             |                            |            |              |     |         |                        |                 |        |             |
| 26772 | 16384 | dozor   | 18127    | dozor_Postgres_Pro | indexer-ng                                    |                              | 192.168.1.241 |                 |             | 2024-12-16 09:26:36.406602 |            |              |     |         |                        |                 |        |             |
| +03   |       |         |          |                    | 2024-12-16 09:26:36.452978+03                 |                              | 192.168.1.241 |                 |             |                            | ClientRead |              | t   | TLSv1.3 | TLS_AES_256_GCM_SHA384 |                 | 2      |             |
| 56    | f     |         |          |                    | SET application_name = 'indexer-ng'           |                              |               |                 |             |                            |            |              |     |         |                        |                 |        |             |
| 28476 | 16384 | dozor   | 18127    | dozor_Postgres_Pro | indexer-ng                                    |                              | 192.168.1.241 |                 |             | 2024-12-16 09:33:02.235242 |            |              |     |         |                        |                 |        |             |
| +03   |       |         |          |                    | 2024-12-16 09:33:02.28295+03                  |                              | 192.168.1.241 |                 |             |                            | ClientRead |              | t   | TLSv1.3 | TLS_AES_256_GCM_SHA384 |                 | 2      |             |
| 56    | f     |         |          |                    | SET application_name = 'indexer-ng'           |                              |               |                 |             |                            |            |              |     |         |                        |                 |        |             |
| 21580 | 16384 | dozor   | 18127    | dozor_Postgres_Pro | indexer-ng                                    |                              | 192.168.1.241 |                 |             | 2024-12-16 09:05:48.314485 |            |              |     |         |                        |                 |        |             |
| +03   |       |         |          |                    | 2024-12-16 09:05:48.356762+03                 |                              | 192.168.1.241 |                 |             |                            | ClientRead |              | t   | TLSv1.3 | TLS_AES_256_GCM_SHA384 |                 | 2      |             |
| 56    | f     |         |          |                    | SET application_name = 'indexer-ng'           |                              |               |                 |             |                            |            |              |     |         |                        |                 |        |             |
| 18177 | 16384 | dozor   | 18127    | dozor_Postgres_Pro | PostgreSQL JDBC Driver                        |                              | 192.168.1.241 |                 |             | 2024-12-04 15:04:17.826714 |            |              |     |         |                        |                 |        |             |
| +03   |       |         |          |                    | 2024-12-04 15:04:22.928641+03                 |                              | 192.168.1.241 |                 |             |                            | ClientRead |              | t   | TLSv1.3 | TLS_AES_256_GCM_SHA384 |                 | 2      |             |
| 56    | f     |         |          |                    | SELECT value FROM app_options WHERE key = \$1 |                              |               |                 |             |                            |            |              |     |         |                        |                 |        |             |
| 27019 | 16384 | dozor   | 18127    | dozor_Postgres_Pro | indexer-ng                                    |                              | 192.168.1.241 |                 |             | 2024-12-16 09:27:39.617674 |            |              |     |         |                        |                 |        |             |
| +03   |       |         |          |                    | 2024-12-16 09:27:39.680897+03                 |                              | 192.168.1.241 |                 |             |                            | ClientRead |              | t   | TLSv1.3 | TLS_AES_256_GCM_SHA384 |                 | 2      |             |
| 56    | f     |         |          |                    | SET application_name = 'indexer-ng'           |                              |               |                 |             |                            |            |              |     |         |                        |                 |        |             |
| 27744 | 16384 | dozor   | 18127    | dozor_Postgres_Pro | indexer-ng                                    |                              | 192.168.1.241 |                 |             | 2024-12-16 09:30:10.003019 |            |              |     |         |                        |                 |        |             |
| +03   |       |         |          |                    | 2024-12-16 09:30:10.043338+03                 |                              | 192.168.1.241 |                 |             |                            | ClientRead |              | t   | TLSv1.3 | TLS_AES_256_GCM_SHA384 |                 | 2      |             |
| :     |       |         |          |                    |                                               |                              |               |                 |             |                            |            |              |     |         |                        |                 |        |             |

Рис. В.4. Пример вывода команды для проверки SSL-соединений с БД

---

## Приложение С. Ответвление сообщений с почтовых серверов

Схемы подключения при работе в пассивном режиме зависят от используемого почтового сервера (MTA). Блокировка сообщений при ответвлении невозможна, поскольку обработка по политике ИБ ведется только для копий сообщений. Ниже описаны способы ответвления почтового потока для наиболее распространенных почтовых серверов.

### С.1. Ответвление почтового потока с сервера Yandex

Для настройки ответвления почтового потока с сервера Yandex 360 необходимо выполнить следующие действия:

1. Зарегистрировать приложение в сервисе Яндекс OAuth (раздел [С.1.1](#));
2. Добавить правила обработки писем (раздел [С.1.2](#));
3. Настроить KEO DLP File Crawler для сбора писем (раздел [С.1.3](#)).

#### С.1.1. Регистрация приложения

Для создания и регистрации приложения в сервисе Яндекс OAuth необходимо выполнить следующие действия:

1. Для создания приложения с особыми правами доступа перейти по ссылке <https://oauth.yandex.ru/client/new/>, и заполнить название приложения в открывшейся форме.
2. В разделе **Платформы приложения** выбрать **Веб-сервисы**, и в появившемся поле **Redirect URL** ввести [https://oauth.yandex.ru/verification\\_code](https://oauth.yandex.ru/verification_code) или нажать **Подставить URL для отладки** во всплывающем окне.
3. В разделе **Доступ к данным** добавить особые права доступа для работы с правилами:
  - **ya360\_admin:mail\_write\_routing\_rules** – управление правилами обработки почты для домена (просмотр и изменение);
  - **ya360\_admin:mail\_read\_routing\_rules** – чтение правил обработки почты для домена (просмотр).
4. Скопировать и сохранить для дальнейшего использования данные из поля **ClientID**. Пример: **26d2d876b59445b6a97d2a4cf4b47eb8**.

#### Примечание

*Этот идентификатор становится недействительным через один год.*

5. Получить отладочный токен, перейдя по ссылке вида [https://oauth.yandex.ru/authorize?response\\_type=token&client\\_id=<ClientID>](https://oauth.yandex.ru/authorize?response_type=token&client_id=<ClientID>), где **<ClientID>** – идентификатор, полученный в предыдущем шаге. В ответе будет содержаться отладочный токен, например:

---

y0\_AgAAAABwZwdkAAqE8wAAAADtEOEqyCSm4UqQQ\_2fQKVnGwdeEmtJF-A.

При возникновении затруднений следует обратиться к документации по адресу <https://yandex.ru/dev/id/doc/ru/register-client>.

### С.1.2. Добавление правил обработки писем

Для создания правил обработки писем необходим идентификатор организации. Его можно узнать, перейдя по адресу <https://admin.yandex.ru> и открыв вкладку **Профиль организации** (поле ID). Пример идентификатора: 7949520.

URL для запросов чтения и записи правил обработки писем имеет следующий вид:

**`https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules`**

где **<id>** – идентификатор организации.

Для чтения и записи правил обработки писем используется утилита командной строки **curl**.

#### Внимание!

*Из-за технических ограничений невозможна пересылка скрытых копий сообщений (bcc).*

#### С.1.2.1. Чтение правил

Для вывода на экран текущих правил обработки писем в формате JSON следует выполнить команду следующего вида:

**`curl -H "Authorization: OAuth <oauth_token>" -v -k \`**  
**`https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules`**

где **<oauth\_token>** – отладочный токен, полученный в разделе [С.1.1](#), **<id>** – идентификатор организации.

Для записи в файл текущих правил обработки писем в формате JSON следует выполнить команду следующего вида:

`curl -H "Authorization: OAuth <oauth_token>" -v -k \`  
`https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules \`  
`-o <output_filename>`

где **<oauth\_token>** – отладочный токен, полученный в разделе [С.1.1](#), **<id>** – идентификатор организации, **<output\_filename>** – имя файла для записи правил.

#### С.1.2.2. Запись правил

#### Внимание!

*При выполнении любой команды записи правил все текущие правила для данной организации будут перезаписаны правилами, указанными в этой команде. Если необходимо обновить текущие правила – следует их получить как показано в предыдущем разделе, объединить*

---

*с новыми правилами и записать. Для удобства рекомендуется использовать запись правил из файла.*

---

Пример команды для записи правила пересылки входящих писем на заданный адрес в формате JSON из командной строки:

```
curl -H "Authorization: OAuth <oauth_token>" -v -k -X PUT \
https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules \
-d '{
  "rules": [
    {
      "terminal": false,
      "condition": {},
      "actions": [
        {
          "data": {
            "email": "dlp@organization.com"
          },
          "action": "forward"
        }
      ],
      "scope": {
        "direction": "inbound"
      }
    }
  ]
}'
```

где **<oauth\_token>** – отладочный токен, полученный в разделе [C.1.1](#), **<id>** – идентификатор организации, **dlp@organization.com** – почтовый адрес для приема пересылаемых писем.

Пример команды для записи правила в формате JSON из файла:

```
curl -H "Authorization: OAuth <oauth_token>" -g -i -v -k -X PUT \
https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules \
--databinary @input.json
```

где **<oauth\_token>** – отладочный токен, полученный в разделе [C.1.1](#), **<id>** – идентификатор организации, **input.json** – имя файла, содержащего правило.

Пример правила пересылки входящих и исходящих писем на заданный адрес в формате JSON для использования в командах записи:

```
{
  "rules": [
    {
      "terminal": false,
      "condition": {},
      "actions": [
        {
          "data": {
            "email": "dlp@organization.com"
          },
          "action": "forward"
        }
      ]
    }
  ]
}
```

```

    }
  ],
  "scope": {
    "direction": "inbound"
  }
},
{
  "terminal": false,
  "condition": {},
  "actions": [
    {
      "data": {
        "email": "dlp@organization.com"
      },
      "action": "forward"
    }
  ],
  "scope": {
    "direction": "outbound"
  }
}
}

```

Пример правила пересылки входящих и исходящих писем одного пользователя на заданный адрес в формате JSON для использования в командах записи:

```

{
  "rules": [
    {
      "scope": {
        "direction": "outbound"
      },
      "actions": [
        {
          "data": {
            "email": "dlp@organisation.com"
          },
          "action": "forward"
        }
      ],
      "terminal": false,
      "condition": {
        "$or": [
          {
            "from": {
              "$eq": "a.petrov@organisation.com"
            }
          },
          {
            "to": {
              "$eq": "a.petrov@organisation.com"
            }
          }
        ]
      }
    },
    {
      "scope": {
        "direction": "inbound"
      }
    }
  ]
}

```

```

},
"terminal": false,
"actions": [
  {
    "data": {
      "email": "dlp@organisation.com"
    },
    "action": "forward"
  }
],
"condition": {
  "$or": [
    {
      "from": {
        "$eq": "a.petrov@organisation.com"
      }
    },
    {
      "to": {
        "$eq": "a.petrov@organisation.com"
      }
    }
  ]
}
}
]
}

```

Пример правила пересылки входящих и исходящих писем двух пользователей на заданный адрес в формате JSON для использования в командах записи:

```

{
  "rules": [
    {
      "scope": {
        "direction": "outbound"
      },
      "actions": [
        {
          "data": {
            "email": "dlp@organisation.com"
          },
          "action": "forward"
        }
      ],
      "terminal": false,
      "condition": {
        "$or": [
          {
            "from": {
              "$eq": "a.petrov@organisation.com"
            }
          },
          {
            "to": {
              "$eq": "a.petrov@organisation.com"
            }
          }
        ]
      }
    }
  ]
}

```



```

    ],
  },
  {
    "scope": {
      "direction": "inbound"
    },
    "terminal": false,
    "actions": [
      {
        "data": {
          "email": "dlp@organisation.com"
        },
        "action": "forward"
      }
    ],
    "condition": {
      "$or": [
        {
          "from": {
            "$eq": "a.petrov@organisation.com"
          }
        },
        {
          "to": {
            "$eq": "a.petrov@organisation.com"
          }
        }
      ]
    }
  },
  {
    "scope": {
      "direction": "outbound"
    },
    "actions": [
      {
        "data": {
          "email": "dlp@organisation.com"
        },
        "action": "forward"
      }
    ],
    "terminal": false,
    "condition": {
      "$or": [
        {
          "from": {
            "$eq": "n.serov@organisation.com"
          }
        },
        {
          "to": {
            "$eq": "n.serov@organisation.com"
          }
        }
      ]
    }
  }
],
},

```

```

},
{
  "scope": {
    "direction": "inbound"
  },
  "terminal": false,
  "actions": [
    {
      "data": {
        "email": "dlp@organisation.com"
      },
      "action": "forward"
    }
  ],
  "condition": {
    "$or": [
      {
        "from": {
          "$eq": "n.serov@organisation.com"
        }
      },
      {
        "to": {
          "$eq": "n.serov@organisation.com"
        }
      }
    ]
  }
}
]
}
}

```

### С.1.3. Настройка KEO DLP File Crawler для сбора писем

Для настройки сбора писем в KEO DLP следует настроить доступ к почтовому ящику, на который выполняется пересылка писем, и создать соответствующую задачу в KEO DLP File Crawler.

#### С.1.3.1. Настройка доступа к почтовому ящику

Для настройки доступа к почтовому ящику необходимо выполнить следующие действия:

1. Перейти на адрес <https://mail.yandex.ru> и выполнить вход с учетной записью почтового ящика, на который выполняется пересылка писем (в данном примере – dlp@organization.com).
2. Перейти в раздел **Настройки > Все настройки > Почтовые программы** и установить флажки:
  - **С сервера imap.yandex.ru по протоколу IMAP**
  - **Пароли приложений и OAuth-токены**
3. Сохранить настройки.

4. Перейти в раздел **Настройки > Все настройки > Безопасность** и нажать на ссылку **Пароли приложений**. В открывшемся разделе **Создать пароль приложения** выбрать данные, к которым необходимо предоставить доступ (тип приложения).
5. Ввести название пароля, с которым он будет отображаться в списке. В качестве названия можно указать название приложения, для которого создается пароль. Нажать **Далее**.
6. В новом окне на экран будет выведен пароль приложения. Следует сохранить этот пароль для дальнейшего использования.

#### **Внимание!**

*Созданный пароль можно увидеть только один раз. Если пароль был утрачен – следует удалить его и создать заново.*

#### **Примечание**

*Для начала работы пароля требуется некоторое время: Яндекс предупреждает о 2–3 часах, хотя обычно это занимает несколько минут.*

### **С.1.3.2. Настройка задачи в KEO DLP File Crawler**

Для настройки задачи в KEO DLP File Crawler для сбора писем следует создать задачу со следующими параметрами:

- **Почтовый сервер** – `imap.yandex.ru`
- **Порт** – `993`
- **Использовать SSL-соединение** – включить
- **Почтовый ящик** – указать почтовый ящик, для которого выполнялась настройка (в данном примере – `dlp@organization.com`)
- **Пароль** – пароль, созданный в предыдущем разделе
- **Входящие и Письма с вложениями** – включить
- **Уведомлять при завершении задачи с ошибками** – рекомендуется включить

Также рекомендуется самостоятельно отслеживать результаты работы задачи в разделе **Результат**. После успешной проверки выполнения задачи следует настроить расписание для нее.

### **С.1.3.3. Возможные проблемы**

При пересылке на единый адрес (в данном примере – `dlp@organization.com`) письма могут попадать в папку **Спам**. Следует вручную указать, что рассылки с данного адреса не являются спамом.

### С.1.4. Идентификация сообщений

Для поиска сообщений Yandex 360 политикой фильтрации следует использовать два условия, объединенных логическим оператором **И**:

- **Заголовок x-dar-host Совпадает с imap.yandex.ru**
- **Тип сообщения Равно exchange**

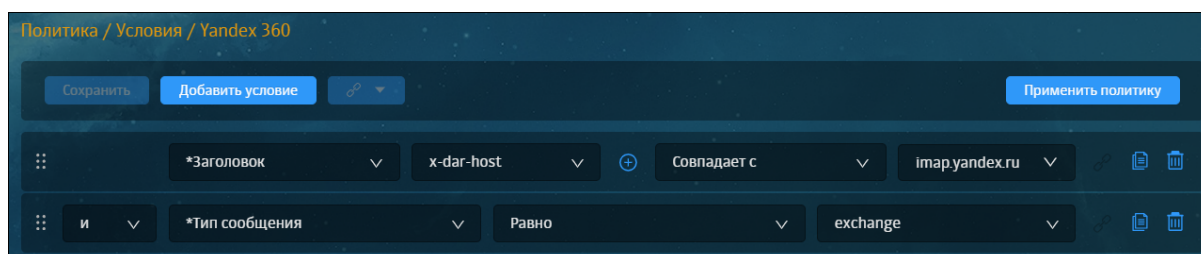


Рис. С.1. Условие для поиска сообщений Yandex 360

## С.2. Ответвление почтового потока с сервера «МойОфис Почта»

Для настройки ответвления почтового потока с сервера «МойОфис Почта» необходимо выполнить на этом сервере следующие действия:

1. Создать резервную копию конфигурационного файла **/opt/poseidon/postfix/main.cf**, выполнив команды:

```
cd /opt/poseidon/postfix
```

```
cp main.cf main.cf.bak
```

2. Открыть для редактирования файл **main.cf** и добавить в него следующие строки:

```
always_bcc = <m_address>  
transport_maps = lmdb:/etc/postfix/transport_map
```

где **<m\_address>** – почтовый адрес для отправки скрытых копий в KEO DLP, например: **dozor@dozor.organisation.local**. Сохранить и закрыть файл.

3. Создать файл **/opt/poseidon/postfix/transport\_map**, выполнив команду:

```
touch /opt/poseidon/postfix/transport_map
```

4. Открыть созданный файл и записать в него содержимое следующего вида:

```
<m_address> smtp:[<filter_address>]:<filter_port>
```

где:

- **<m\_address>** – почтовый адрес для отправки скрытых копий в KEO DLP;
- **<filter\_address>** – адрес сервера KEO DLP, имеющего роль **Фильтр почтового потока**;
- **<filter\_port>** – номер порта, на котором этот сервер ожидает входящие сообщения.

---

Пример:

```
dozor@dozor.organisation.local smtp:[10.201.31.2]:1025
```

5. Создать файл **/usr/local/bin/postfix\_to\_dozor\_fix.sh**, выполнив команду:

```
touch /usr/local/bin/postfix_to_dozor_fix.sh
```

6. Открыть созданный файл и записать в него следующее содержимое:

```
#!/bin/bash

docker service update psn-mail_postfix --force --with-registry-auth
container_id=$(docker ps | grep postfix | awk '{print $1}')

echo "Container_id is $container_id"
docker cp /opt/poseidon/postfix/transport_map $container_id:/etc/postfix/
docker exec -it $container_id postmap -v /etc/postfix/transport_map
```

Сохранить и закрыть файл.

7. Создать файл **/usr/local/bin/postfix\_to\_dozor\_fix\_cron.sh**, выполнив команду:

```
touch /usr/local/bin/postfix_to_dozor_fix_cron.sh
```

8. Открыть созданный файл и записать в него следующее содержимое:

```
#!/bin/bash

container_id=$(docker ps | grep postfix | awk '{print $1}')
docker cp /opt/poseidon/postfix/transport_map $container_id:/etc/postfix/
docker exec -it $container_id postmap -v /etc/postfix/transport_map
```

Сохранить и закрыть файл.

9. Назначить права на выполнение для скриптов **postfix\_to\_dozor\_fix.sh** и **postfix\_to\_dozor\_fix\_cron.sh**, выполнив команды:

```
chmod +x /usr/local/bin/postfix_to_dozor_fix.sh
```

```
chmod +x /usr/local/bin/postfix_to_dozor_fix_cron.sh
```

10. Открыть расписание планировщика, выполнив команду:

```
crontab -e
```

11. Добавить в расписание следующие строки:

```
@reboot root /usr/local/bin/postfix_to_dozor_fix_cron.sh
*/1 * * * * root /usr/local/bin/postfix_to_dozor_fix_cron.sh
```

12. Перезапустить службу планировщика, выполнив команду:

```
systemctl restart crond.service
```

---

## С.3. Ответвление почтового потока с сервера «МойОфис Mailion»

### С.3.1. Пересылка скрытых копий сообщений (bcc)

Для настройки пересылки скрытых копий сообщений (bcc) с сервера «МойОфис Mailion» необходимо выполнить на этом сервере следующие действия:

1. Создать резервную копию конфигурационного файла **/srv/docker/postfix/conf/main.cf**, выполнив команды:

```
cd /srv/docker/postfix/conf
```

```
cp main.cf main.cf.bak
```

2. Открыть для редактирования файл **main.cf** и добавить в него следующие строки:

```
always_bcc = <m_address>
transport_maps = hash:/etc/postfix/transport_map
```

где **<m\_address>** – почтовый адрес для отправки скрытых копий в КЕО DLP, например: **dozor@dozor.organisation.local**. Сохранить и закрыть файл.

3. Создать файл **/srv/docker/postfix/conf/transport\_map**, выполнив команду:

```
touch /srv/docker/postfix/conf/transport_map
```

4. Открыть созданный файл и записать в него содержимое следующего вида:

```
<m_address> smtp:[<filter_address>]:<filter_port>
```

где:

- **<m\_address>** – почтовый адрес для отправки скрытых копий в КЕО DLP;
- **<filter\_address>** – адрес сервера КЕО DLP, имеющего роль **Фильтр почтового потока**;
- **<filter\_port>** – номер порта, на котором этот сервер ожидает входящие сообщения.

Пример:

```
dozor@dozor.organisation.local smtp:[10.201.31.2]:1025
```

5. Создать файл **/usr/local/bin/transport\_map\_update.sh**, выполнив команду:

```
touch /usr/local/bin/transport_map_update.sh
```

6. Открыть созданный файл и записать в него следующее содержимое:

```
#!/bin/bash

mapfile=/etc/postfix/transport_map
container_id=$(docker ps | grep postfix: | awk '{print $1}')
docker exec -it $container_id postmap hash:$mapfile
docker restart postfix
```

---

Сохранить и закрыть файл.

7. Назначить права на выполнение для скрипта **transport\_map\_update.sh**, выполнив команду:

```
chmod +x /usr/local/bin/transport_map_update.sh
```

8. Запустить скрипт **transport\_map\_update.sh**, выполнив команду:

```
/usr/local/bin/transport_map_update.sh
```

### С.3.2. Пересылка всех исходящих сообщений

Для настройки пересылки всех исходящих сообщений с сервера «МойОфис Mailion» необходимо выполнить на этом сервере следующие действия:

1. Создать резервную копию конфигурационного файла **/srv/docker/postfix/conf/main.cf**, выполнив команды:

```
cd /srv/docker/postfix/conf
```

```
cp main.cf main.cf.bak
```

2. Открыть для редактирования файл **main.cf** и добавить в него следующие строки:

```
relayhost = <filter_address>:<filter_port>
```

где:

- **<filter\_address>** – адрес сервера КЕО DLP, имеющего роль **Фильтр почтового потока**;
- **<filter\_port>** – номер порта, на котором этот сервер ожидает входящие сообщения.

Пример:

```
relayhost = dozor-filter1.isim.local:1025
```

Сохранить и закрыть файл.

3. Перезапустить контейнер с почтовым сервером, выполнив команду:

```
docker restart postfix
```

### С.3.3. Пересылка всех исходящих сообщений в зависимости от отправителя

Для настройки пересылки всех исходящих сообщений с определенного домена сервера «МойОфис Mailion» необходимо выполнить на этом сервере следующие действия:

1. Создать резервную копию конфигурационного файла **/srv/docker/postfix/conf/main.cf**, выполнив команды:

```
cd /srv/docker/postfix/conf
```

```
cp main.cf main.cf.bak
```

2. Открыть для редактирования файл **main.cf** и добавить в него следующие строки:

---

```
sender_dependent_default_transport_maps = hash:/etc/postfix/relayhost_map
```

Сохранить и закрыть файл.

3. Создать файл **/srv/docker/postfix/conf/relayhost\_map**, выполнив команду:

```
touch /srv/docker/postfix/conf/relayhost_map
```

4. Открыть созданный файл и записать в него содержимое следующего вида:

```
<mailion_domain> smtp:[<filter_address>]:<filter_port>
```

где:

- **<mailion\_domain>** – домен, принадлежащий почтовому серверу Mailion;
- **<filter\_address>** – адрес сервера KEO DLP, имеющего роль **Фильтр почтового потока**;
- **<filter\_port>** – номер порта, на котором этот сервер ожидает входящие сообщения.

Пример:

```
@mailion.example.net smtp:[10.201.31.2]:1025
```

5. Создать файл **/usr/local/bin/relayhost\_map\_update.sh**, выполнив команду:

```
touch /usr/local/bin/relayhost_map_update.sh
```

6. Открыть созданный файл и записать в него следующее содержимое:

```
#!/bin/bash

mapfile=/etc/postfix/relayhost_map
container_id=$(docker ps | grep postfix: | awk '{print $1}')
docker exec -it $container_id postmap hash:$mapfile
docker restart postfix
```

Сохранить и закрыть файл.

7. Назначить права на выполнение для скрипта **relayhost\_map\_update.sh**, выполнив команду:

```
chmod +x /usr/local/bin/relayhost_map_update.sh
```

8. Запустить скрипт **relayhost\_map\_update.sh**, выполнив команду:

```
/usr/local/bin/relayhost_map_update.sh
```

## C.4. Ответвление почтового потока с сервера Microsoft Exchange

Действия по ответвлению почтового потока с сервера Microsoft Exchange отличаются для Microsoft Exchange разных версий. Описание процесса ответвления для версии Microsoft Exchange 2000 приведено ниже. Руководства по ответвлению почтовых потоков для версий Microsoft Exchange 2003 и 2007 приведены в приложениях [C.6](#) и [C.7](#). В доку-



ментации по Microsoft Exchange для процесса ответвления почтового потока используется термин «журналирование».

### Внимание!

*При использовании данного метода пропадает оригинальное значение заголовка **mail from**, которое заменяется значением, указанным при настройке ответвления.*

## C.4.1. Microsoft Exchange 2000

Для включения журналирования необходимо выполнить следующие действия:<sup>1</sup>

1. Создать новую учетную запись пользователя в **Active Directory Users and Computers**. При создании необходимо снять флажок **Create Exchange Mailbox**.
2. После создания пользователя в свойствах объекта пользователя (вызывается щелчком правой кнопкой мыши) следует выбрать пункт **Exchange Tasks** и в появившемся окне выбрать пункт **Establish E-mail Address**. Затем в открывшемся окне нужно ввести произвольный адрес пользователя на компьютере, где установлен KEO DLP (например, `dozor@server.domain`, где `server.domain` – имя сервера, на котором установлен KEO DLP).
3. В **Exchange System Manager** перейти на вкладку **Servers**.
4. Выбрать **Storage Group**, щелкнуть правой кнопкой мыши на списке хранилищ и выбрать пункт **Properties**.
5. На вкладке **General** выбрать пункт **Archive all messages sent or received by mailboxes on this store** и нажать кнопку **Browse** для выбора записи, на которую будут пересылаться скопированные сообщения (т.е. учетной записи получателя, созданного на первом шаге).

Эти действия необходимо проделать для каждого из хранилищ.

## C.4.2. Преобразование журнальных сообщений Exchange в оригинальные SMTP-сообщения

При обработке журнальных сообщений, поступающих от сервера Exchange, KEO DLP может преобразовать их в оригинальные SMTP-сообщения. Соответствующие модули поставляются в составе стандартной конфигурации. Модули встраиваются в точку разбора файлов в спуле и позволяют обрабатывать смешанный поток сообщений (журнальные и не журнальные сообщения в одном входящем потоке), при этом можно применять разные политики обработки к сообщениям журнальной подсистемы и обычным сообщениям. То есть включение обработки журнальных сообщений не влияет на обработку обычных сообщений.

Модуль поддержки Exchange отвечает за обработку журнальных сообщений с серверов Exchange любых версий. Возможность распознавания сообщений **Exchange** определяется параметром **Определять тип сообщений Exchange** в секции **Сервис фильтрации сообщений** (раздел **GUI Система > Конфигурация > Основные настройки > Работа системы**). Журнальные сообщения определяются по наличию любого из заголовков:

<sup>1</sup> По материалам Microsoft.com

- "X-MS-Exchange-Organization-Journal-Report"
- "X-MS-Journal-Report"
- "X-MS-Exchange-Organization-Processed-By-Journaling"

а также двух вложенных частей типа **text/plain** и **message/rfc2822**.

Адреса действительных отправителя и получателей сообщения определяются в ходе разбора полей журналирования (добавляемых сервером Exchange) в части сообщения **text/plain**. Текст оригинального сообщения берется из части типа **message/rfc2822**.

Модуль поддержки Exchange 2003 определяет обработку журнальных сообщений с сервера Exchange 2003, отличных по своей структуре. Для таких сообщений, полученных с адресов, определенных параметром **Значения RCPT TO для журнальных сообщений Exchange 2003** (раздел GUI Система > Конфигурация > Основные настройки > Работа системы, секция **Сервис фильтрации сообщений**), адреса отправителя и получателей определяются не в ходе разбора полей журналирования, а из заголовков самого сообщения: **Sender** или **From** – для отправителя, **To**, **CC** и **Bcc** – для получателей.

#### Примечание

*Параметром **Значения RCPT TO для журнальных сообщений Exchange 2003** определяются почтовые адреса - коннекторы, соответствующие специальным учетным записям на сервере Exchange 2003, которые обеспечивают пересылку журнальных сообщений с сервера Exchange на сервер KEO DLP. Поэтому эти адреса не соответствуют реальным адресам отправителей и получателей из оригинальных сообщений. Для таких сообщений и осуществляется подстановка адресов из заголовков оригинального сообщения. Подробнее см. приложение [С.6](#).*

На сообщения типа Email, полученные в результате преобразования журнальных сообщений Exchange, ставится соответствующая пометка: **«Преобразовано из журнала Exchange»** – в случае, если сообщение было обработано модулем разбора Exchange, или **«Преобразовано из журнала Exchange: Exchange 2003»** в случае, если сообщение было обработано модулем разбора Exchange 2003.

## С.5. Ответвление почтового потока с сервера Exim

В зависимости от версии Exim настройки файла конфигурации несколько различаются. Для Exim версии 3.x необходимо в начало раздела **ROUTERS CONFIGURATION** конфигурационного файла вписать следующие строки (в примере предполагается, что сервер, на котором установлен KEO DLP, имеет имя **dozor.example.com**):

```
smaphost1:
driver = domainlist
transport = remote_SMTP
route_list = "*" dozor.example.com bydns_a"
unseen
```

Для Exim версии 4.x строки будут следующими:

```
smaphost1:
driver = manualroute
transport = remote_SMTP
```

```
route_list = "*" dozor.example.com"
unseen
```

## С.6. Ответвление сообщений с сервера Microsoft Exchange 2003

### С.6.1. Общая последовательность действий

Для журналирования сообщений с сервера Microsoft Exchange 2003 необходимо выполнить следующие действия:

1. Создать объект типа «контакт» в службе Active Directory. В качестве почтового адреса для данного объекта указать почтовый адрес, для которого в доменной части прописать DNS-имя сервера, где функционирует KEO DLP.
2. Создать учетную запись пользователя, имеющего почтовый адрес на сервере Exchange, с которого будет осуществляться ответвление почтового потока. Весь почтовый поток будет дублироваться в почтовом ящике этого пользователя и далее пересылаться на сервер, где функционирует KEO DLP.
3. Провести дополнительную настройку, если KEO DLP работает не через стандартный SMTP-порт (25).
4. Включить стандартное журналирование на сервере Exchange, с которого будет происходить ответвление почтового потока на KEO DLP.
5. Включить BCC-журналирование на сервере Exchange, с которого будет происходить ответвление почтового потока на KEO DLP.

### С.6.2. Создание объекта типа «контакт» в Active Directory

В Active Directory требуется создать объект типа «contact». Для этого необходимо выполнить следующие действия:

1. Открыть консоль управления **Microsoft Management Console**, перейти к оснастке **Active Directory Users and Computers**, щелкнуть правой кнопкой мыши и в контекстном меню выбрать пункт **New > Contact**.
2. В открывшемся диалоговом окне создания нового контакта заполнить формы ввода, указав значения **First Name** и **Last Name**. Например, в поле **First Name** ввести значение «**To**», а в поле **Last Name** значение «**KEO DLP**». Нажать кнопку **Next**.
3. В следующем открывшемся окне создания нового контакта нажать кнопку **Modify**.
4. В окне **New E-mail Address** установить флажок **SMTP Address** и нажать кнопку **OK**.
5. В окне **Internet Address Properties** перейти на вкладку **General** и ввести почтовый адрес **copyforarchive@<DNS-имя сервера KEO DLP>**. Нажать кнопку **Next**.

#### Внимание!

*Почтовый адрес обязательно должен начинаться с copyforarchive@.*

В результате описанных действий на экране должна отобразиться форма **New Object > Contact** следующего вида (см. [Рис.С.2](#)). Для завершения создания нового контакта следует нажать кнопку **Next** и далее кнопку **Finish**:

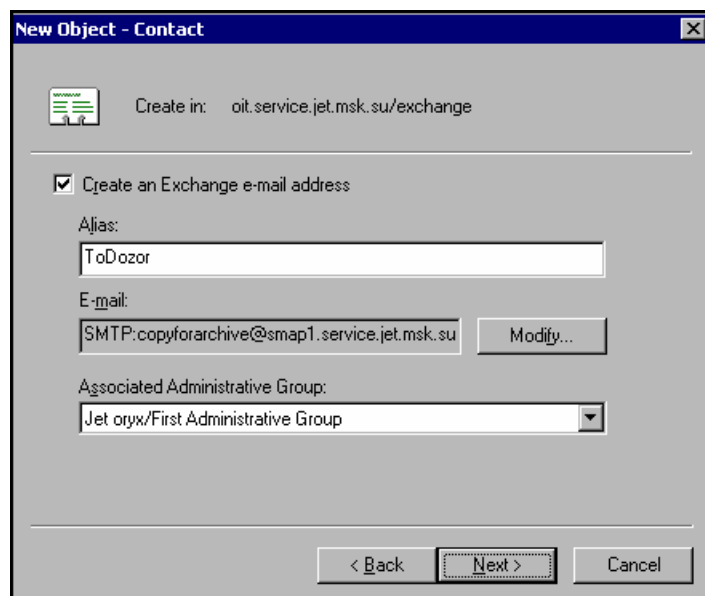


Рис. С.2. Форма New Object > Contact

### С.6.3. Создание учетной записи пользователя

Далее требуется создать учетную запись нового пользователя, на почтовый адрес которого будут отправляться архивные сообщения. Для этого необходимо выполнить следующие действия:

1. В Active Directory создать объект типа **user** с любым именем (например, **user1**) с почтовым адресом на сервере Exchange. С этого адреса будет происходить ответвление почтового потока.
2. После создания пользователя **user1** необходимо скрыть его почтовый адрес в досье. Для этого следует открыть окно **Properties** для пользователя **user1**, перейти на вкладку **Exchange Advanced**, где установить флажок **Hide from Exchange Address lists** (см. [Рис.С.3](#)):

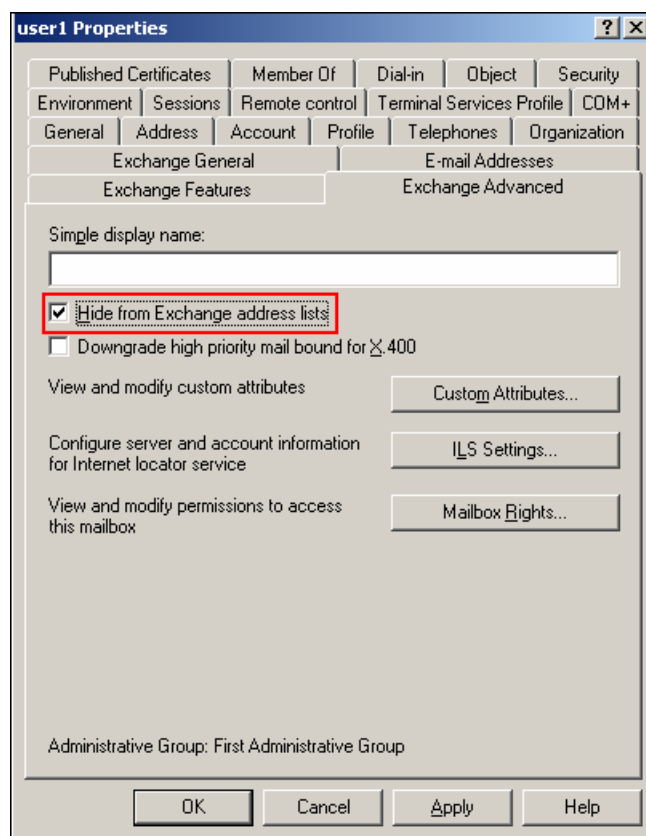


Рис. С.3. Соккрытие адреса пользователя в досье

### Примечание

Если в свойствах пользователя не отображается вкладка **Exchange Advanced**, то нужно выбрать пункт меню **View** в консоли **Active Directory Users and Computers** и установить параметр **Advanced Features**.

3. Далее необходимо настроить пересылку всей почты с ящика пользователя **user1** на созданный ранее контакт. Для этого следует перейти на вкладку **Exchange General** в окне свойств пользователя и нажать кнопку **Delivery Options** (см. [Рис.С.4](#)):

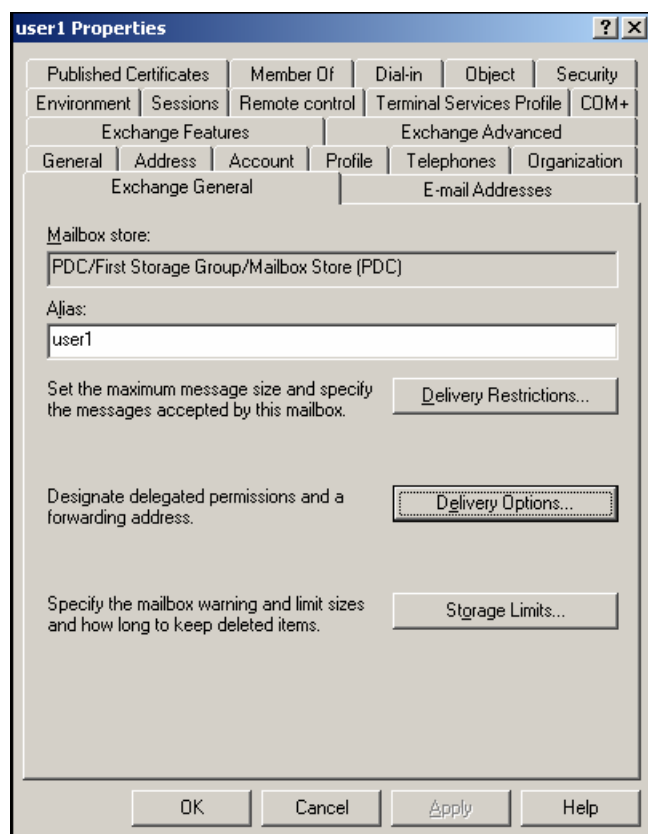


Рис. С.4. Свойства пользователя, вкладка Exchange General

4. В открывшемся окне **Delivery Options** для параметра **Forwarding Address** установить значение **Forward to** и нажать кнопку **Modify** (см. [Рис.С.5](#)). В появившемся окне необходимо ввести имя созданного контакта и нажать кнопку **OK**:

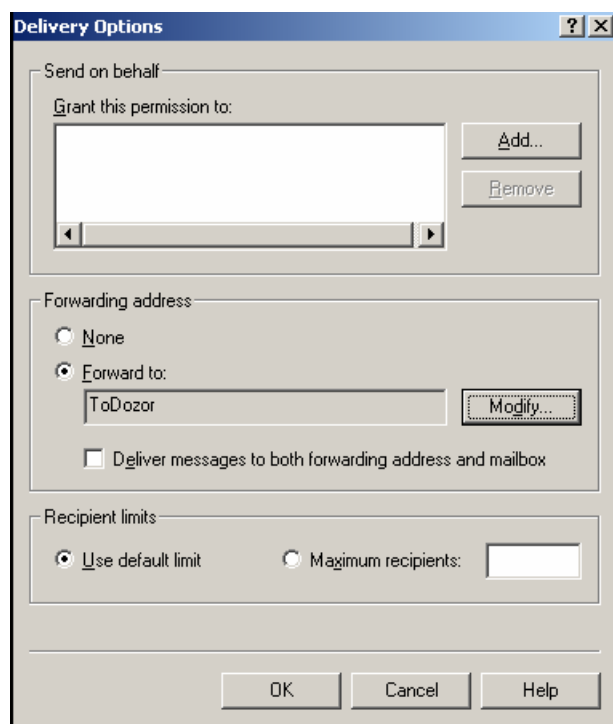


Рис. С.5. Окно Delivery Options

5. В окне **Delivery Options** нажать кнопку **OK**. Создание учетной записи пользователя завершено.

#### С.6.4. Дополнительная настройка

##### Примечание

*Если KEO DLP работает в режиме архивирования сообщений типа Email, то в этом случае важно знать, какой порт использует процесс **SMTP\_GW**. Если **SMTP\_GW** использует 25 порт, то SMTP-коннектор в Microsoft Exchange создавать не нужно. Важно только, чтобы был правильно настроен DNS, и Exchange-сервер отправлял сообщения на сервер, где функционирует KEO DLP. Если процесс **SMTP\_GW** использует порт, отличный от 25, то необходимо произвести дополнительную настройку сервера Exchange.*

Если процесс **SMTP\_GW** использует нестандартный порт (отличный от 25), то для настройки сервера Exchange необходимо выполнить следующие действия:

- Создать второй **SMTP Virtual Server**.
- Создать два SMTP-коннектора, один из которых будет доставлять почту в обычном режиме через **Default SMTP Virtual Server**, а второй через **KEO DLP SMTP Virtual Server** будет пересылать на KEO DLP все архивные сообщения.

Для создания **SMTP Virtual Server** необходимо выполнить следующие действия:

1. Открыть оснастку **Exchange System Manager** и в раскрывающемся дереве слева выбрать пункт **Servers > Name Exchange > Protocols > SMTP**, щелкнув на нем правой

кнопкой мыши. В открывшемся контекстном меню необходимо выбрать пункт **New SMTP Virtual Server**.

2. Указать для нового SMTP-сервера имя **KEO DLP**.
3. Щелкнуть правой кнопкой мыши на имени сервера **KEO DLP** и в контекстном меню выбрать пункт **Properties**.
4. В окне свойств сервера перейти на вкладку **Delivery** (см. [Рис.С.6](#)) и нажать кнопку **Outbound connections**:

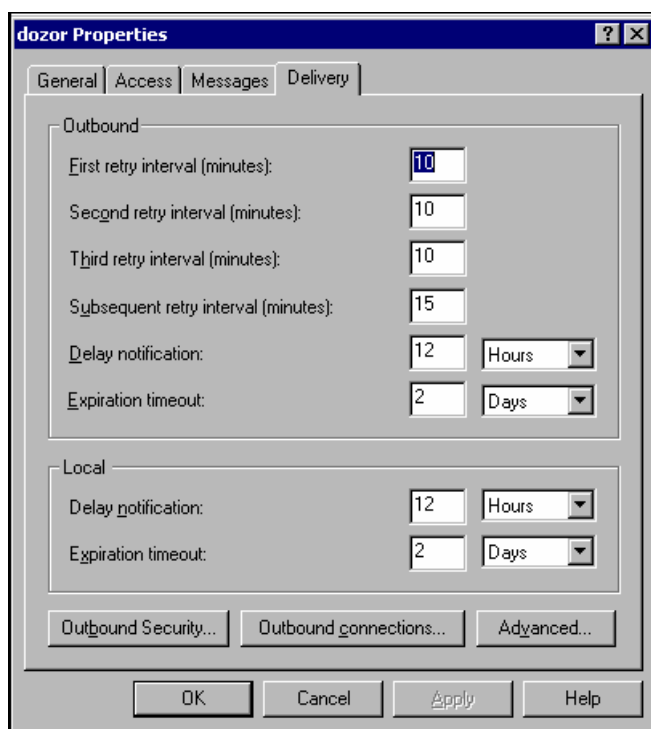


Рис. С.6. Свойства виртуального сервера SMTP

5. В открывшемся окне в поле **TCP port** необходимо ввести номер порта, по которому работает процесс **SMTP\_GW** в KEO DLP, например 1025.
6. Для завершения создания **SMTP Virtual Server** необходимо нажать кнопку **OK** во всех окнах.

Для создания коннектора для работы через **Default SMTP Virtual Server** необходимо выполнить следующие действия:

1. Открыть оснастку **Exchange System Manager > Connectors** (либо **Exchange System Manager > Routing Groups > First Routing Group > Connectors** – в зависимости от настройки Exchange).
2. Создать новый SMTP-коннектор. На вкладке **General** ввести название для созданного коннектора и установить флажок **Use DNS to route to each address space on this connector** (если Exchange сам производит рассылку поступающей из внешних источников почты).



- 
3. На той же вкладке **General** в разделе **Local bridgeheads** необходимо добавить сервер **Default SMTP virtual server**.
  4. Перейти на вкладку **Address Space** и добавить адресное пространство типа SMTP с почтовым доменом, в качестве которого выступает сервер KEO DLP. Для этого на вкладке **Address Space** нажать кнопку **Add** и в открывшемся окне ввести в поле **E-mail domain** символ «\*», в поле **Cost** ввести значение **1**.

Для создания коннектора для работы через **KEO DLP SMTP Virtual Server** необходимо выполнить следующие действия:

1. Открыть оснастку **Exchange System Manager > Connectors** (либо **Exchange System Manager > Routing Groups > First Routing Group > Connectors** - в зависимости от настройки Exchange).
2. Создать новый SMTP-коннектор. На вкладке **General** ввести название коннектора, установить переключатель **Forward all mail through this connector to the following smart hosts** и ввести DNS-имя сервера, где функционирует KEO DLP.
3. На той же вкладке **General** в разделе **Local bridgeheads** добавить сервер **KEO DLP SMTP virtual server**.
4. На вкладке **Address Space** указать в поле **Type** значение **Other**, а затем в открывшемся окне ввести следующие значения (см. [Рис.С.7](#)):
  - в поле **Type** ввести **SMTP**;
  - в поле **Cost** ввести **1**;
  - в поле **Address** ввести почтовый адрес **copyforarchive@<DNS-имя сервера KEO DLP>**.
5. Для завершения создания **KEO DLP SMTP Virtual Server** нажать кнопку **OK** во всех окнах:

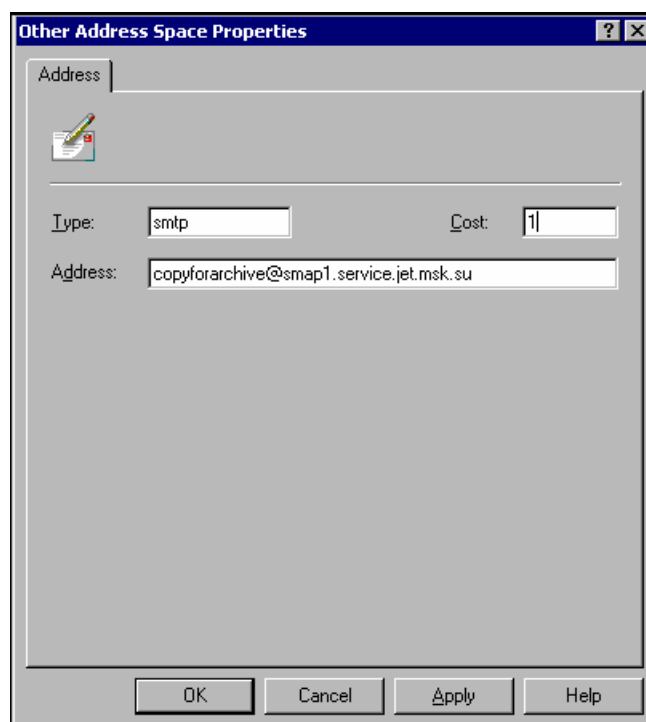


Рис. С.7. Создание коннектора. Вкладка Address

### С.6.5. Включение стандартного журналирования

Если изначально использовался режим расширенного журналирования, то его можно отключить, для чего используется специальная программа настройки журналирования **Exejcfg**, доступная для загрузки с официального сайта компании Microsoft. Для отключения режима расширенного журналирования необходимо в командной строке Windows выполнить команду:

**Exejcfg.exe -d**

где:

- **Exejcfg.exe** – исполняемый файл программы настройки журналирования;
- **-d** – параметр, означающий отключение режима расширенного журналирования.

После этого необходимо включить стандартное журналирование, выполнив следующие действия:

1. Открыть оснастку **Exchange System Manager**, щелкнуть правой кнопкой мыши в области того хранилища (**Information Store**), применительно к которому требуется включить стандартное журналирование, и в появившемся контекстном меню выбрать пункт **Properties**.
2. В открывшемся окне свойств хранилища перейти на вкладку **General** и установить флажок **Archive all messages sent or received by mailboxes on this store** (см. [Рис.С.8](#)):

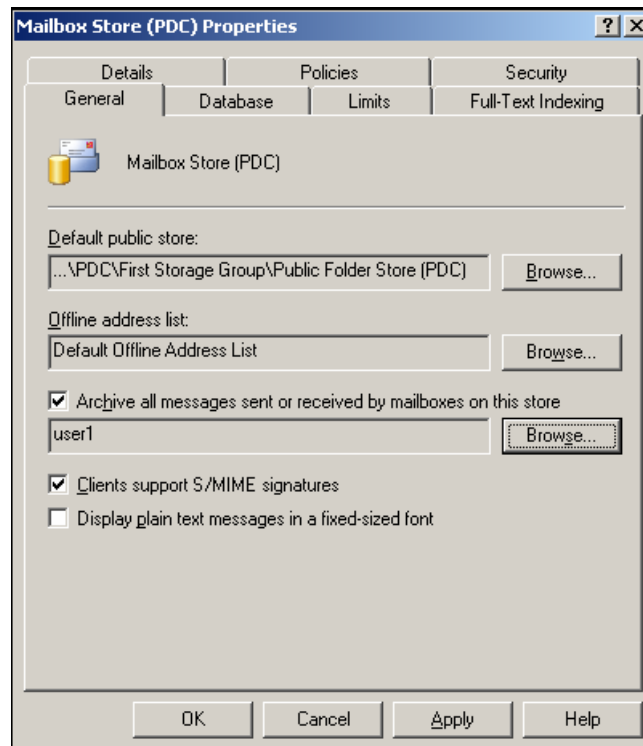


Рис. С.8. Установка архивирования всех сообщений из хранилища

3. Нажать кнопку **Browse** рядом с данным флажком и в открывшемся окне выбрать созданную ранее учетную запись пользователя **user1** (см. [С.6.3](#)). Нажать кнопку **OK**.

### С.6.6. Включение BCC-журналирования

Для включения журналирования BCC необходимо выполнить следующие действия:

1. Запустить редактор реестра. Для этого открыть пункт меню **Пуск > Выполнить**. И в командной строке выполнить команду запуска реестра. Формат команды для запуска следующий:

**regedit**

2. В открывшемся окне реестра найти ключ **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeTransport\Parameters**. Для данного ключа создать новый параметр типа **D\_WORD** с именем **JournalBCC** и присвоить этому параметру значение **1** (см. [Рис.С.9](#)). После чего закрыть редактор реестра:

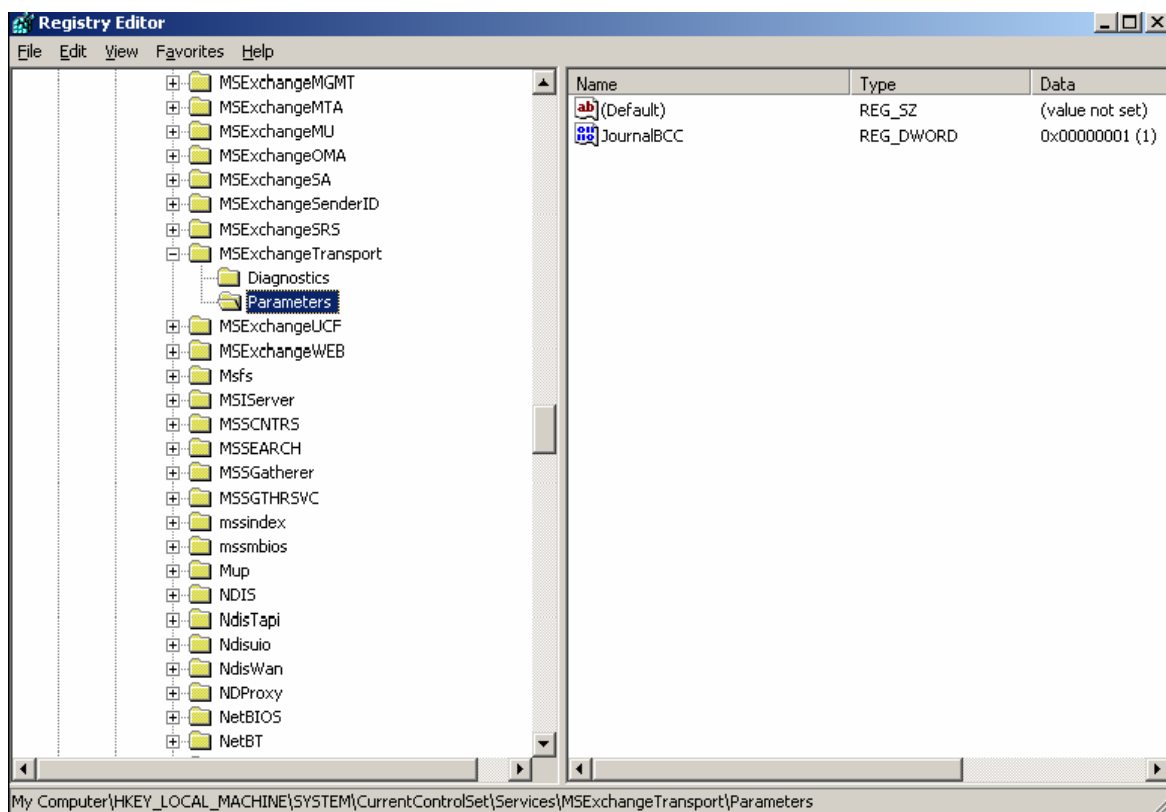


Рис. С.9. Редактирование реестра для включения ВСС-журналирования

3. Запустить оснастку **Services**, в которой перезапустить службу SMTP, выполнив соответствующую команду контекстного меню (см. [Рис.С.10](#)):

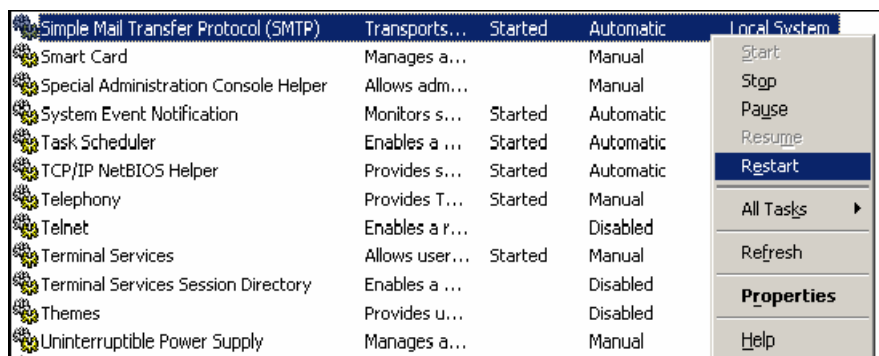


Рис. С.10. Перезапуск службы SMTP

### С.6.7. Откат изменений

Под начальным состоянием понимается отсутствие на сервере Exchange какого-либо ответвления почтового потока на сервер KEO DLP. Для отката изменений и возврата к начальному состоянию необходимо выполнить следующие действия:

1. Удалить созданный ключ реестра (см. [С.6.6](#) , пункт 1 списка действий).

2. Деактивировать стандартное журналирование путем снятия флажка **Archive all messages sent or received by mailboxes on this store** в свойствах выбранного хранилища **Information Store** (см. [C.6.5](#), пункт 2 списка действий).
3. Перезапустить службу SMTP (см. [C.6.6](#), пункт 3 списка действий).

## C.7. Ответвление сообщений с сервера Microsoft Exchange 2007

На рисунке ниже (см. [Рис.С.11](#)) показана типовая схема ответвления почтового потока с использованием журналирования Exchange 2007. Все сообщения, отправляемые и принимаемые пользователями, обрабатываются сервером - транспортировщиком почтовых сообщений. На каждом таком сервере функционирует специальный агент, который осуществляет журналирование почтовых сообщений согласно заданной политике журналирования.

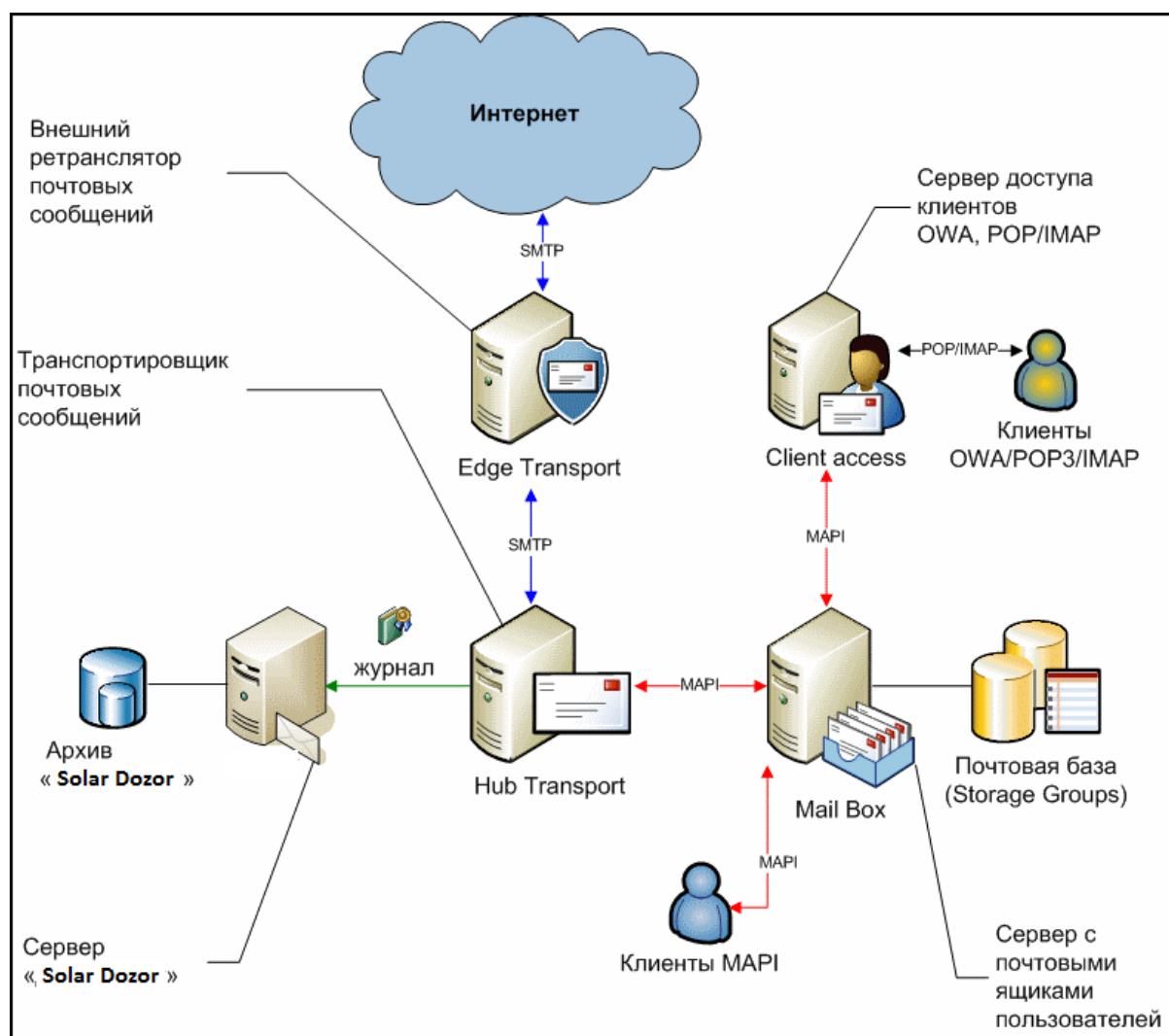


Рис. С.11. Схема ответвления почтового потока

В Microsoft Exchange Server 2007 используется два типа журналирования:

1. Стандартное журналирование. Обеспечивает журналирование всех почтовых сообщений, отправленных и принятых пользователями с учетными записями на определенном

---

почтовом хранилище. Данный тип журналирования аналогичен журналированию, используемому в MS Exchange Server 2000/2003.

2. **Расширенное журналирование.** Обеспечивает использование правил журналирования, которые могут быть настроены для обеспечения потребностей организации.

При использовании расширенного журналирования в среде Exchange 2007 объектами журналирования могут являться:

- **Внутренняя переписка (Internal).** В данную категорию входят сообщения, в которых получатель и отправитель являются пользователями, принадлежащими одной организации Exchange и имеющими учетные записи в домене Active Directory, в котором развернута данная организация Exchange.
- **Внешняя переписка (External).** В данную категорию входят сообщения, в которых получатель или отправитель являются внешними пользователями по отношению к организации Exchange.
- **Общая переписка (Global).** В данную категорию входят все почтовые сообщения как внешних пользователей, так и пользователей, находящихся в организации Exchange.
- **Почтовый ящик, Группа или Все пользователи.** Правила расширенного журналирования могут применяться к одному почтовому ящику, одной или нескольким группам, ко всем пользователям организации.

Процесс журналирования подразумевает своей конечной целью отправку журнала на сторонний SMTP-адрес (приемник журнальных данных). Под журналом понимается почтовое сообщение, содержащее служебную информацию и оригинал исходного сообщения. В качестве стороннего SMTP-адреса могут использоваться следующие объекты:

- организация Exchange;
- сторонний почтовый сервис.

В данном случае приемником журнальных данных является сервер KEO DLP, осуществляющий архивирование поступающего почтового потока. В независимости от типа приемника журнальных данных в домене Active Directory должен присутствовать объект получателя для этих журнальных данных. Объектом может являться конкретный почтовый ящик Exchange 2007, контакт или список рассылки.

Для отправки журнальных данных на сервер KEO DLP объектом получателя является контакт Active Directory, в котором прописан почтовый адрес с доменной частью, для которой настроен соответствующий коннектор Exchange. Данный коннектор осуществляет маршрутизацию почтовых сообщений, содержащих журнальные данные, на сервер KEO DLP.

### **С.7.1. Общая последовательность действий**

Для журналирования почтовых сообщений с сервера Microsoft Exchange 2007 необходимо выполнить следующие действия:

1. Создать объект типа «контакт» в Active Directory. В качестве почтового адреса для данного объекта указать почтовый адрес, для которого в доменной части прописать DNS-имя сервера, где функционирует KEO DLP.

2. Настроить коннектор для пересылки сообщений, содержащих журнальные данные, на сервер KEO DLP.
3. Включить журналирования для групп хранения (Storage Groups), почтовые сообщения которых необходимо журналировать.
4. Проверить корректность работы механизма ответвления.

### С.7.2. Создание объекта типа «контакт» в MS Exchange server 2007

Для создания объекта типа «контакт» необходимо выполнить следующие действия:

1. Открыть оснастку **Exchange Management Console**. Открыть раскрывающийся список **Настройка получателей (Recipient Configuration)**, в котором выбрать пункт **Почтовые контакты (Mail Contact)**. Выбрать пункт меню **Действия (Action) > Новый Почтовый Контакт (New Mail Contact)**.
2. В открывшемся окне редактирования свойств контакта (см. [Рис.С.12](#)) в списке слева выбрать пункт **Новый контакт (New Mail contact)** и в полях ввода **First name**, **Name**, **Alias** ввести **KEO DLP**. В поле ввода **External e-mail address**: указать почтовый ящик в формате **keodlp@<полное DNS имя сервера KEO DLP>**. Нажать кнопку **Далее (Next)**:

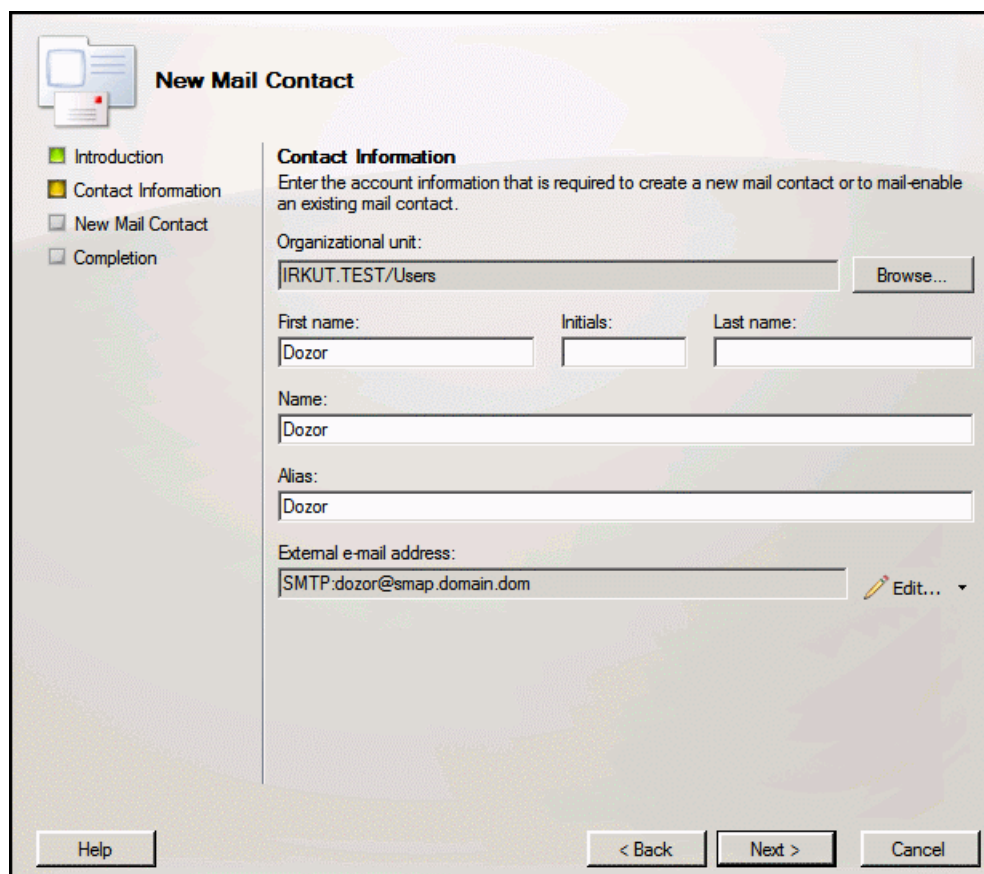


Рис. С.12. Окно редактирования свойств контакта в MS Exchange 2007

3. Далее для завершения создания нового контакта нажать кнопку **ОК** во всех окнах.



### С.7.3. Настройка коннектора для пересылки сообщений на сервер SMAP

Для настройки коннектора необходимо выполнить соответствующую команду в окне консоли **Exchange Management Shell**. Для запуска **Exchange Management Shell** следует открыть пункт меню **Пуск > Программы > Microsoft Exchange Server 2007 > Exchange Management Shell**. Откроется окно консоли для выполнения команд. Формат команды для выполнения настройки коннектора:

```
New-SendConnector -Name KEO DLP -AddressSpaces smap.keodlp.dom -SmartHosts 192.168.11.136 -Port 1025 -SourceTransportServers cas1.irkut.test,cas2.irkut.test
```

где:

- **Name** – формальное имя коннектора;
- **AddressSpaces** – полное DNS-имя сервера SMAP;
- **SmartHosts** – ip-адрес сервера SMAP;
- **Port** – порт, на котором сервер SMAP ожидает приема почтовых сообщений;
- **SourceTransportServers** – серверы Exchange с ролью Hub Transport.

В результате в окне консоли должны отобразиться данные следующего вида:

| Identity | AddressSpaces            | Enabled |
|----------|--------------------------|---------|
| -----    | -----                    | -----   |
| KEO DLP  | {smtp:smap.keodlp.dom;1} | True:   |

### С.7.4. Включение журналирования

#### Стандартное журналирование

На данном этапе необходимо указать группы хранения, которые будут использоваться для журналирования. Для этого необходимо выполнить следующие действия:

1. Запустить оснастку **Exchange Management Console**, выполнив команду **Пуск > Программы > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. В дереве элементов в левой части окна выбрать пункт **Server Configuration > Mailbox**. При работе с этим пунктом меню основное окно **Exchange Management Console** разделено на две области, верхнюю и нижнюю. В верхней области представлена таблица со списком созданных кластеров Exchange. В нижней области показаны характеристики выбранного кластера.
3. В верхней области необходимо выбрать мышью соответствующий кластер Exchange. В нижней области следует перейти на вкладку **Database Management** и выбрать нужную группу хранения, а в ней - нужную базу данных. Щелкнув правой кнопкой мыши на имя базы данных, выбрать в контекстном меню пункт **Properties**.
4. В окне **Properties** с параметрами выбранной базы данных следует перейти на вкладку **General** (см. [Рис.С.13](#)) и установить флажок **Journal Recipient**. После чего нажать кнопку **Browse** и в открывшемся окне выбора контактов **Select Recipient** выбрать созданный контакт **KEO DLP**:



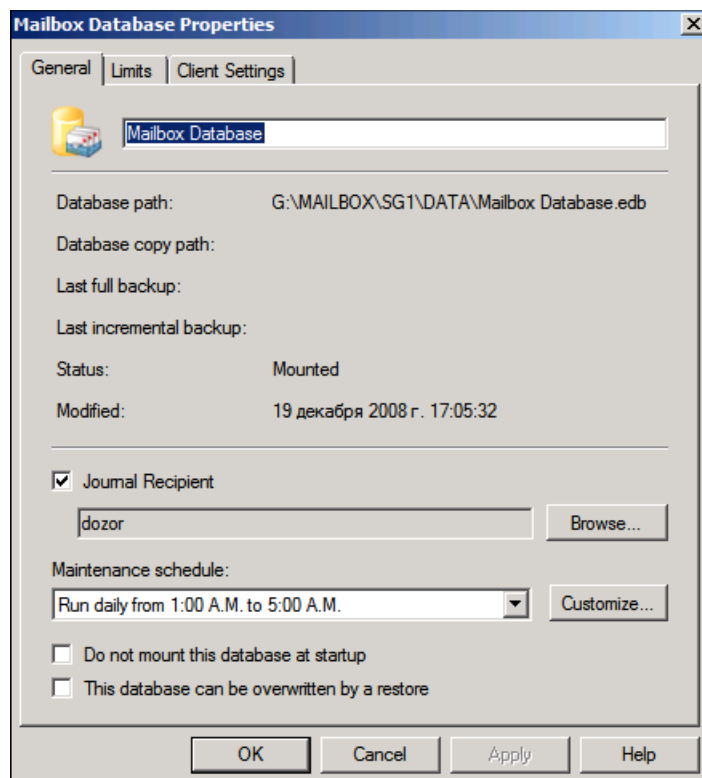


Рис. С.13. Окно свойств почтовой базы Exchange

5. Для завершения настройки журналирования необходимо нажать кнопку **ОК** в окне свойств базы данных.

### Расширенное журналирование

Для включения расширенного журналирования необходимо создать правило журналирования. Для этого следует выполнить следующие действия:

1. Запустить оснастку **Exchange Management Console**, выполнив команду **Пуск > Программы > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. В дереве элементов в левой части окна выбрать пункт **Organization Configuration > Hub Transport** и перейти на вкладку **Journalling** в правой части окна.
3. В столбце действий **Actions** в правой части окна выбрать пункт **New Journal Rule** для создания нового правила журналирования. В открывшемся окне в поле **Rule Name** необходимо ввести имя для нового правила – **KEO DLP**, и установить для параметра **Scope** значение **Global -all messages**. В этом же окне необходимо установить флажок **Enable Rule**. Для завершения создания правила необходимо нажать кнопку **New**.
4. В таблице **Hub Transport** в окне **Exchange Management Console** должна появиться новая запись с именем **KEO DLP**. Если дважды щелкнуть мышью на строку с записью **KEO DLP** откроется окно со свойствами созданного правила журналирования (см. [Рис.С.14](#)):

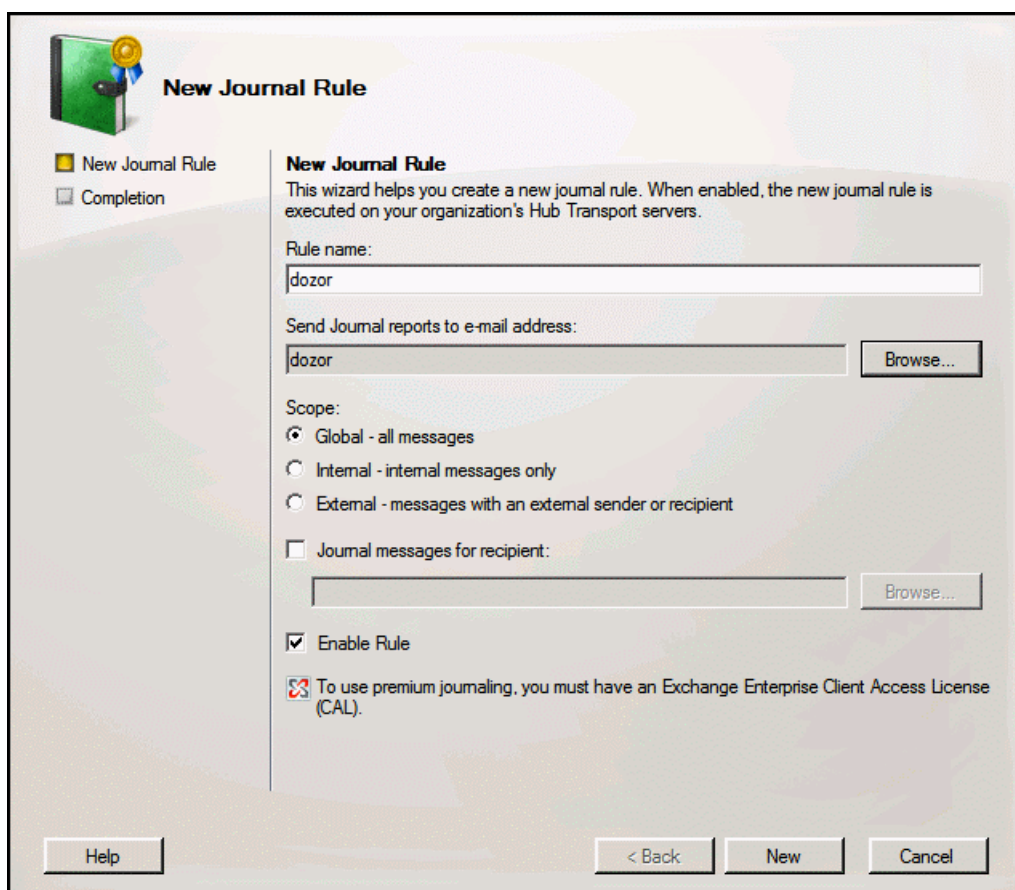


Рис. С.14. Создание правила журналирования

### С.7.5. Проверка правильности работы журналирования

Для проверки правильности работы журналирования необходимо отправить тестовое сообщение на тестовый почтовый адрес в Exchange и проверить путь прохождения сообщения при помощи журнальных файлов утилиты **Exchange Message Tracking Tool**, входящей в состав ПО Microsoft Exchange 2007.

До начала просмотра журнальных файлов необходимо убедиться, что включен режим отслеживания сообщений. Для этого необходимо выполнить соответствующую команду, используя **Exchange Management Shell** (Пуск > Программы > **Microsoft Exchange Server 2007 > Exchange Management Shell**). Формат команды для выполнения проверки следующий:

**Get-MailboxServer SERVERNAME | fl \*messagetracking\***

где **SERVERNAME** – имя кластера Exchange.

В результате в окне консоли должны отобразиться данные следующего вида:

```
MessageTrackingLogEnabled      :True
MessageTrackingLogMaxAge       :30.00:00:00
MessageTrackingLogMaxDirectorySize :250MB
MessageTrackingLogMaxFileSize  :10MB
MessageTrackingLogPatch        :C:\Program Files\Microsoft\Exchange
```

```
Server\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled :True
```

Значение переменной **MessageTrackingLogEnabled** должно быть **True**, а в переменной **MessageTrackingLogPath** должен быть указан путь к журнальным файлам утилиты. Если это не так, необходимо включить режим отслеживания сообщений. Для этого следует выполнить соответствующую команду в окне **Exchange Management Shell**.

Формат команды для включения режима отслеживания сообщений:

**Set-TransportServer SERVERNAME -MessageTrackingLogEnabled \$true**

где **SERVERNAME** – имя сервера Exchange (или нескольких серверов, перечисленных через запятую), выполняющего роль **Hub Transport**.

Далее необходимо отправить тестовое сообщение с одного внутреннего почтового адреса Exchange на другой внутренний адрес. После отправки сообщения необходимо открыть файл, указанный в переменной **MessageTrackingLogPath** (см. листинг выполнения команды **Get-MailboxServer** выше) и убедиться, что в этом файле присутствуют строки (выделены полужирным шрифтом), свидетельствующие об отправке журнальных файлов на сервер SMAP:

```
#Software: Microsoft Exchange Server
#Version: 8.0.0.0
#Log-type: Message Tracking Log
#Date: 2008-12-19T14:59:22.558Z
#Fields: date-time,client-ip, client-hostname, server-ip, server-hostname, source-context, connector-id,
source, event-id, internal-message-id, message-id, recipient-address, recipient-status, total-bytes,
recipient-count, related-recipient-address, reference, message-subject, sender-address, return-path,
message-info
2008-12-19T14:59:22.558Z, fe80::5c1a:d1de:8b91:5d24,
irkutbox.IRKUT.TEST,::1,CAS2,,,STOREDRIVER, RECEIVE, 4, <
F1926216EC7B4F48A45E9225AF49A4376466401764@IRKUTBOX.IRKUT.TEST>, ivanov@irkut.test;
test@irkut.test; Administrator@irkut.test,,7684,3,,,FW: test message for
dozor,Administrator@irkut.test,Administrator@irkut.test,04I:
2008-12-19T14:59:23.777Z,,,CAS2, Journaling,,AGENT, RECEIVE, 5,
<16bd3f92-f763-486d-ba61-55492d4b8f20@journal.report.generator>, dozor@domain.dom;
dozor@irkut.test,,9066,2,,4,FW: test message for dozor,
MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@IRKUT.TEST, <>,
2008-12-19T14:59:23.855Z,,,CAS2,,,ROUTING, RESOLVE,
5,<16bd3f92-f763-486d-ba61-55492d4b8f20@journal.report.generator>, dozor@domain.dom,,9066,
1, dozor@irkut.test,,FW: test message for dozor,
MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@IRKUT.TEST,<>,
```

После этого необходимо убедиться, что отправленное сообщение попало в архив KEO DLP.

## С.8. Ответвление сообщений с сервера Microsoft Exchange 2013

### С.8.1. Общая последовательность действий

Для журналирования почтовых сообщений с сервера Microsoft Exchange 2013 необходимо выполнить следующие действия:

1. Создать объект типа «контакт» в Active Directory. В качестве почтового адреса для данного объекта указать адрес, для которого в доменной части прописать имя сервера, на котором функционирует «KEO DLP».
2. Настроить коннектор для пересылки сообщений, содержащих журнальные данные, на сервер «KEO DLP».
3. Включить журналирование на сервере Exchange, с которого будет происходить ответвление почтового потока на KEO DLP.

### С.8.2. Создание объекта типа «контакт» в MS Exchange server 2013

Для создания объекта типа «контакт» необходимо выполнить следующие действия:

1. Открыть сетевую консоль **Центр администрирования Exchange**.
2. Перейти в раздел **Получатели > Контакты**. Создать новый почтовый контакт (см. [Рис.С.15](#)):

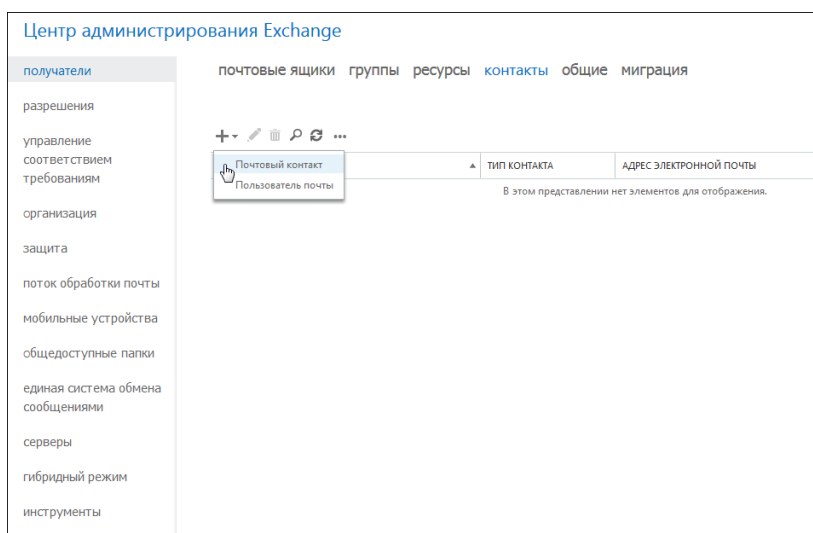


Рис. С.15. Центр администрирования Exchange

3. В открывшемся диалоговом окне создания нового контакта заполнить формы ввода, указав значения **Отображаемое имя**, **Имя**, **Псевдоним**, **Внешний почтовый ящик**. (см. [Рис.С.16](#)):

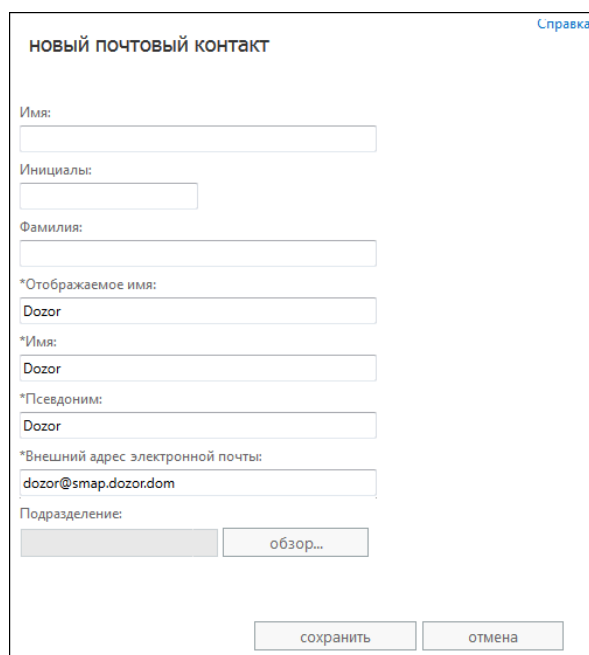


Рис. С.16. Создание почтового контакта

4. Для завершения создания нового контакта нажать кнопку **Сохранить**.

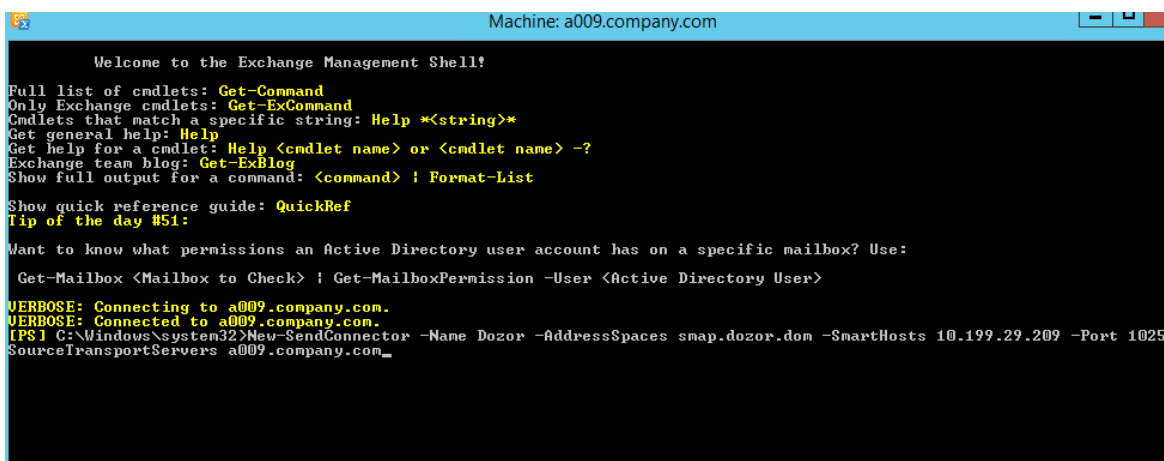
### С.8.3. Настройка коннектора для пересылки сообщений на сервер KEO DLP

Для настройки коннектора необходимо выполнить соответствующую команду в окне консоли **Exchange Management Shell**. Для запуска **Exchange Management Shell** следует открыть пункт меню **Пуск > Программы > Microsoft Exchange Server 2013 > Exchange Management Shell**. Откроется окно консоли для выполнения команд. Формат команды для выполнения настройки коннектора:

**New-SendConnector -Name KEO DLP -AddressSpaces smap.keodlp.dom -SmartHosts 10.199.29.209 -Port 1025 -SourceTransportServers a009.company.com.**

где:

- **Name** – формальное имя коннектора;
- **AddressSpaces** – доменное имя сервера KEO DLP;
- **SmartHosts** – ip-адрес сервера KEO DLP;
- **Port** – порт, на котором сервер KEO DLP ожидает приема почтовых сообщений;
- **SourceTransportServers** – сервер Exchange с ролью Hub Transport (если серверов несколько, их следует указывать через запятую).



```
Machine: a009.company.com

Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExchangeCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Exchange team blog: Get-ExchangeBlog
Show full output for a command: <command> | Format-List

Show quick reference guide: QuickRef
Tip of the day #51:

Want to know what permissions an Active Directory user account has on a specific mailbox? Use:
Get-Mailbox <Mailbox to Check> | Get-MailboxPermission -User <Active Directory User>

VERBOSE: Connecting to a009.company.com.
VERBOSE: Connected to a009.company.com.
[PS] C:\Windows\system32>New-SendConnector -Name Dozor -AddressSpaces smap.dozor.dom -SmartHosts 10.199.29.209 -Port 1025 -SourceTransportServers a009.company.com
```

Рис. С.17. Консоль Exchange Management Shell

В результате в окне консоли должны отобразиться данные следующего вида:

| Identity | AddressSpaces            | Enabled |
|----------|--------------------------|---------|
| KEO DLP  | {smtp:smap.keodlp.dom;1} | True    |

#### С.8.4. Включение журналирования

Чтобы включить журналирование, следует создать правило журналирования. Для этого необходимо выполнить следующие действия:

1. Открыть сетевую консоль **Центр администрирования Exchange**.
2. Перейти в раздел **Получатели > Группы**. Нажать кнопку **Создать+ > Группа рассылки**.

В открывшемся диалоговом окне создания группы заполнить формы ввода, указав значения **Отображаемое имя**, **Псевдоним**, **Владельцы** (см. [Рис.С.18](#)).

Рис. С.18. Создание группы рассылки

3. Для завершения создания новой группы нажать кнопку **Сохранить**
4. Перейти в раздел **Управление соответствием требованиям > Правила журнала**. Нажать кнопку **Добавить+**. В меню **Правило журнала** заполнить требуемые поля и нажать кнопку **Сохранить** (см. [Рис.С.19](#)).

Рис. С.19. Создание правила журналирования

---

## Приложение D. Описание ролей и сервисов

Ниже перечислены возможные роли узлов кластера KEO DLP. Для каждой роли указано ее назначение и состав сервисов, обеспечивающих ее функционирование. Имена ролей указаны как они отображаются в GUI (раздел **Система > Узлы и роли**), а в скобках приведены имена ролей как они отображаются в CLI (скрипты **set-role**, **get-role** и **reg-slave**).

- Сервисы, которые по умолчанию запущены на всех узлах независимо от роли, обеспечивающие полноценное функционирование кластера KEO DLP:
  - ds-bus-rc – сервис распределенного управления.
  - monitor-ng – сервис валидации параметров конфигурации.
  - smap-diag – виртуальный сервис регулярной отправки диагностических отчетов.
  - smap-settings – виртуальный сервис хранения общих для кластера настроек.
  - sender – сервис отправки почтовых сообщений.
  - internal-connectors – виртуальный внутренний сервис хранения метаинформации сервисов узла.
  - smap-redis – сервис хранения счетчиков, очередей сообщений для обработки и очередей действий над сообщениями.
  - monitor-agent – сервис мониторинга на узле.
- **Сервер управления (master)** – единая точка управления. Такую роль может иметь только один узел кластера. На узле с этой ролью запускается **Сервер архива сообщений** (см. ниже), веб-сервер для доступа к GUI, а также генерируется политика фильтрации, распространяемая на все остальные узлы кластера. Роль использует следующие сервисы:
  - database – сервис СУБД настроек, политики и Досье.
  - action-server-database – база данных сервера действий.
  - agent-control-ng – сервис управления модулем KEO DLP Endpoint Agent при помощи GUI.
  - software-center – Центр приложений.
  - software-center-database – БД Центра приложений.
  - smap-agents – виртуальный сервис хранения настроек Агентов.
  - smap-address-book – виртуальный сервис, используемый скриптом **abook-sync**.
  - incident-daemon – сервис управления событиями и инцидентами информационной безопасности.
  - report-server – сервис построения отчетов.



- 
- smap-difi – сервис цифровых отпечатков.
  - abook-daemon – сервис доступа к Досье.
  - agent-media-server – сервис хранения медиаинформации, поступающей от агентов KEO DLP Endpoint Agent.
  - license-server – сервис лицензирования.
  - grafana – сервис построения графиков и диаграмм.
  - monitor-server – сервис сбора данных мониторинга.
  - monitor-httpd – сервис HTTP-интерфейса к системе мониторинга Zabbix. Обеспечивает работу пользовательского интерфейса мониторинга.
  - archive-server – сервис доступа к сообщениям в архиве.
  - action-server – сервис выполнения действий над сообщениями в архиве.
  - webserver – сервис веб-сервера для доступа к GUI.
  - smap-request-handler – сервис обработчика запросов из GUI.
  - **Сервер архива сообщений (storage)** – роль, назначаемая slave-узлам для снижения нагрузки на master-узел при архивировании сообщений. Роль использует следующий сервис:
    - archive-server – сервис доступа к сообщениям в архиве.
  - **Сервис распределенного хранения (cassandra)** – участие узла кластера KEO DLP в кластере Cassandra. Назначение этой роли позволяет повысить производительность кластера Cassandra. Роль использует следующий сервис:
    - skvt-cassandra – сервис хранения индексов ФХ и кэша сервиса распознавания текстов изображений
  - **Анализатор данных (analyzer)** – извлечение и анализ данных из тел сообщений и приложений к сообщениям файлов. Роль использует следующие сервисы:
    - smap-difi – сервис работы с цифровыми отпечатками.
    - smap-idid – сервис контроля идентификаторов.
    - smap-tikaserver – сервис извлечения текстовых данных и определения кодировки.
  - **Сервер интеграции (api-gateway)** – прием запросов к сервисам KEO DLP от внешних клиентов. Роль использует следующий сервис:
    - api-gateway – сервис интеграции.
  - **Сервис перехвата и анализа сетевого трафика (traffic-agent)** – перехват, фильтрация сетевого трафика и пересылка его на почтовый фильтр. Роль использует следующий сервис:
    - tragent – сервис перехвата, анализа и пересылки сетевого трафика.

- **Сервис репликации досье на подчиненных узлах (abook-slave)** – дублирование части данных Досье. Роль предназначена для повышения отказоустойчивости в ситуациях, когда связь с master-узлом (и хранящимся на нем Досье) временно отсутствует. Роль использует следующий сервис:
  - abook-daemon – сервис хранения и управления данными Досье.
- **Сервер агентов (agent-server)** – управление ПО KEO DLP Endpoint Agent, установленным на рабочих станциях пользователей. Узлы обмениваются данными с Агентами по протоколу HTTPS и отправляют собранные данные на серверы фильтрации и медиаинформации. Роль использует следующий сервис:
  - agent-server – сервис взаимодействия с Агентами.
- **Центральное файловое хранилище (fsng-storage)** – долговременное хранение и ротация тел сообщений на файловой системе узла. Роль использует следующие сервисы:
  - filestorage-ng – сервис файлового хранилища.
  - skvt-cassandra – сервис хранения индексов файлового хранилища.
- **Локальное файловое хранилище (fsng-client)** – кратковременное хранение тел сообщений на файловой системе перед отправкой их в центральное файловое хранилище. Роль использует следующие сервисы:
  - filestorage-ng – сервис файлового хранилища.
  - skvt-cassandra – сервис хранения индексов файлового хранилища.

#### Примечание

*Назначение одному узлу ролей **Центральное файловое хранилище** и **Локальное файловое хранилище** эквивалентно назначению ему роли **Центральное файловое хранилище**.*

- **Индексатор текста (text-indexer)** – индексирование сообщений в оперативном архиве для полнотекстового поиска. Роль использует следующие сервисы:
  - indexer-ng – сервис индексации сообщений в архиве.
  - opensearch – сервис текстовой индексации и поиска на основе OpenSearch.
- **Вспомогательный сервис индексации текста (indexer-only)** – индексирование сообщений в оперативном архиве. Роль использует следующий сервис:
  - indexer-ng – сервис индексации сообщений в архиве.
- **Хранилище индексов событий и инцидентов (incident-indexer)** – хранение индексов оперативных событий и инцидентов информационной безопасности. Роль использует следующий сервис:
  - opensearch – сервис текстовой индексации и поиска на основе OpenSearch.

- 
- **Сервер управления событиями и инцидентами подкластера (local-incident-daemon)** – управление событиями и инцидентами ИБ в подкластере. Роль использует следующий сервис:
    - incident-daemon – сервис управления событиями и инцидентами информационной безопасности.
  - **Индексатор медиаинформации (media-indexer)** – индексирование медиаинформации. Роль использует следующий сервис:
    - opensearch – сервис текстовой индексации и поиска на основе OpenSearch.
  - **Вспомогательный сервер OpenSearch (opensearch)** – осуществляет индексацию оперативных сообщений и инцидентов ИБ. Роль использует следующий сервис:
    - opensearch – сервис текстовой индексации и поиска на основе OpenSearch.
  - **Хранилище индексов исторических событий и инцидентов (historic-incident-indexer)** – хранение исторических событий и инцидентов информационной безопасности. Роль использует следующий сервис:
    - opensearch – сервис текстовой индексации и поиска на основе OpenSearch.
  - **Индексатор исторических сообщений (historic-text-indexer)** – индексирование сообщений в историческом архиве для полнотекстового поиска. Роль использует следующие сервисы:
    - indexer-ng – сервис индексации сообщений в архиве.
    - opensearch – сервис текстовой индексации и поиска на основе OpenSearch.
  - **Вспомогательный индексатор исторических сообщений (historic-indexer-only)** – индексирование сообщений в историческом архиве. Роль использует следующий сервис:
    - indexer-ng – сервис индексации сообщений в архиве.
  - **Фильтр почтового потока (smtp-filter)** – прием, фильтрация и архивирование сообщений. Роль использует следующие сервисы:
    - smap-smtp-gw – сервис приема почтовых сообщений.
    - mailfilter – сервис обработки почтовых сообщений согласно политике фильтрации.
    - archiver – сервис архивирования почтовых сообщений.
    - smap-tikaserver – сервис извлечения текстовых данных и определения кодировки.
    - smap-address-book – виртуальный сервис, используемый скриптом **abook-sync**.
  - **Балансировщик (balancer)** – распределение трафика по серверам фильтрации КЕО DLP. Роль использует следующий сервис:
    - haproxy – сервис балансировщика HAProxy.

- **Вспомогательный сервер действий (action-server)** – работа с сообщениями в архиве: экспорт, удаление и отправка сообщений, добавление и удаление пометок, отправка уведомлений, перефильтрация сообщений. Роль использует следующий сервис:
  - action-server – сервис выполнения действий над сообщениями в архиве.
  - action-server-database – БД сервера действий.

#### **Внимание!**

*Роль **Вспомогательный сервер действий** не может быть назначена одному узлу вместе с ролями **Сервер действий подкластера** и **Сервер управления**.*

- **Сервер действий подкластера (action-server-master)** – работа с сообщениями в архиве: экспорт, удаление и отправка сообщений, добавление и удаление пометок, отправка уведомлений, перефильтрация сообщений. Роль использует следующие сервисы:
  - action-server – сервис выполнения действий над сообщениями в архиве.
  - action-server-database – БД сервера действий.

#### **Внимание!**

*Роль может быть назначена только узлу в подкластере. Роль **Сервер действий подкластера** не может быть назначена одному узлу вместе с ролями **Вспомогательный сервер действий** и **Сервер управления**.*

- **Сервер лицензирования подкластера (license-server)** – сервер лицензирования. Роль может быть назначена только узлу в подкластере. Роль использует следующий сервис:
  - license-server – сервер лицензирования.
- **Локальный веб-сервер (webserver-local)** – веб-сервер подкластера в территориально-распределенном режиме работы. Роль использует следующий сервис:
  - webserver-local – сервис GUI в подкластере.

#### **Внимание!**

*Узлу с ролью **Локальный веб-сервер** необходимо предварительно назначить одну или несколько из следующих ролей:*

- **Индикатор текста**
- **Хранилище индексов событий и инцидентов**
- **Вспомогательный сервер OpenSearch**

- 
- **Сервер категорий (category-server)** – категоризация текстов вложений. Роль использует следующий сервис:
    - category-server – сервис категоризации.
  - **Расследование (detective)** – работа с модулем **Расследование**, предназначенным для проведения внутренних расследований инцидентов ИБ. Роль может быть назначена только одному узлу на общих ресурсах. Для назначения роли требуется наличие файлового хранилища на общих ресурсах (роли **Центральное файловое хранилище** или **Локальное файловое хранилище**). Роль использует следующие сервисы:
    - detective-server – сервис **Расследование**.
    - detective-database – БД сервиса **Расследование**.
  - **Сервер управления Краулером (crawler-x-master)** – управление экземплярами краулера. Роль использует следующие сервисы:
    - crawler-рссс – сервис координации между экземплярами краулера и веб-интерфейсом, сбор данных с экземпляров краулера.
    - crawler-database – сервис базы данных краулера.
  - **Краулер: файловые ресурсы и IMAP (crawler-x)** – экземпляр краулера. Роль использует следующие сервисы:
    - crawler-ссс – сервис сбора статистики, телеметрии, журналов, управления заданиями, расписанием, передача информации на ProхуССС.
    - crawler-database – сервис базы данных краулера.
    - smar-activemq – сервис управления очередью метазаданий.
    - crawler-snapshot – сервис, предоставляющий информацию о просканированных ранее объектах по запросу.
    - crawler-processor – сервис обработки результатов сканирования: применение политики к файлам, осуществление заданных действий над файлами.
    - crawler-scanner – сервис сканирования файловых данных.
  - **Краулер: корпоративные мессенджеры (im-crawler)** – загрузка сообщений пользователей в корпоративных мессенджерах через официальный API. Роль использует следующий сервис:
    - im-crawler – сервис загрузки сообщений пользователей в корпоративных мессенджерах через официальный API.
  - **Распознавание графических объектов (god-server)** – идентификация определенных графических объектов в файлах изображений (сканах), например, печатей или разворотов паспорта. Роль использует следующий сервис:
    - god-server – сервис распознавания графических объектов, доступный для обращений клиентов. Выполняет обработку запросов, проверку и применение настроек распознавания, выполняет распознавание графических объектов.

- 
- **Распознавание речи (stt-server)** – распознавание речевой информации из записей с микрофона в текст. Роль использует следующий сервис:

- stt-server – сервис распознавания речи.

#### **Внимание!**

*Роль **Распознавание речи** не может быть назначена одному узлу вместе с ролью **Распознавание графических объектов**.*

- **Контроль рабочего времени (time-control)** – сбор информации об активности пользователей. Роль необходима для работы раздела **Рабочее время** (при отсутствии в кластере КЕО DLP узла с ролью **Анализ поведения (UBA)**, см. ниже). Роль использует следующие сервисы:

- clickhouse – сервис БД ClickHouse для хранения статистических данных.

- **Анализ поведения (UBA) (uba-server)** – сервер анализа поведения пользователей. Эта роль может быть только одна в кластере КЕО DLP и необходима для работы раздела **Поведение и аномалии** в большой карточке персоны. Роль также позволяет работать с разделом **Рабочее время**. Роль использует следующие сервисы:

- uba-server – сервис сбора данных о поведении пользователей.
- indexer-ng – сервис индексации сообщений в архиве.
- clickhouse – сервис БД ClickHouse для хранения статистических данных.

- **Мониторинг локального почтового шлюза (mail-gw)** – при наличии роли на узле включается мониторинг почтовых серверов Exim4, указанных в наборах параметров отправки. Роль не содержит собственных сервисов.

- **Центр приложений (software-center)** – сервис удаленного управления Агентами на станциях с ОС Windows. Роль использует следующий сервис:

- software-center – Центр приложений.
- software-center-database – БД Центра приложений.

#### **Внимание!**

*Роль может быть назначена только узлу в подкластере. Не допускается назначение роли двум и более узлам в одном подкластере.*

---

## Приложение Е. Описание файлового хранилища

### Е.1. Общая архитектура ФХ

В ФХ помещаются контейнеры, содержащие тела сообщений или медиаданные (аудио-записи, видеозаписи, снимки экрана рабочего стола АРМ сотрудников и снимки демонстрируемого контента через средства ВКС), а атрибуты сообщений хранятся в БД архива. При выполнении запросов к архиву определяется местоположение сообщения в ФХ по его идентификатору, и тело сообщения извлекается из контейнера. Размещение тел сообщений на жестком диске, а не в БД, дает возможность хранить их в архивированном виде и таким образом уменьшить объем используемого дискового пространства.

Если используется распределенная конфигурация КЕО DLP, то можно настроить ФХ на нескольких узлах и создать распределенное ФХ. Для этого следует распределить роли **Центральное файловое хранилище** и **Локальное файловое хранилище** между узлами. Узлы с ролью **Фильтр почтового потока** обрабатывают поступающий поток сообщений и помещают информацию о структуре сообщений, проставленных пометках и прочее – в БД архива, а тела сообщений – в один из экземпляров ФХ:

- При наличии ФХ на локальном узле – в него;
- При отсутствии или недоступности ФХ на локальном узле – в любое доступное ФХ на других узлах.

Сообщения с узлов с ролью **Локальное файловое хранилище** перемещаются на узлы с ролью **Центральное файловое хранилище**. Локальные хранилища предназначены для быстрой обработки поступающего потока сообщений и их временного хранения, а центральное хранилище предназначено для постоянного хранения тел сообщений. Общая схема организации распределенного ФХ показана на рисунке [Рис.Е.1](#).

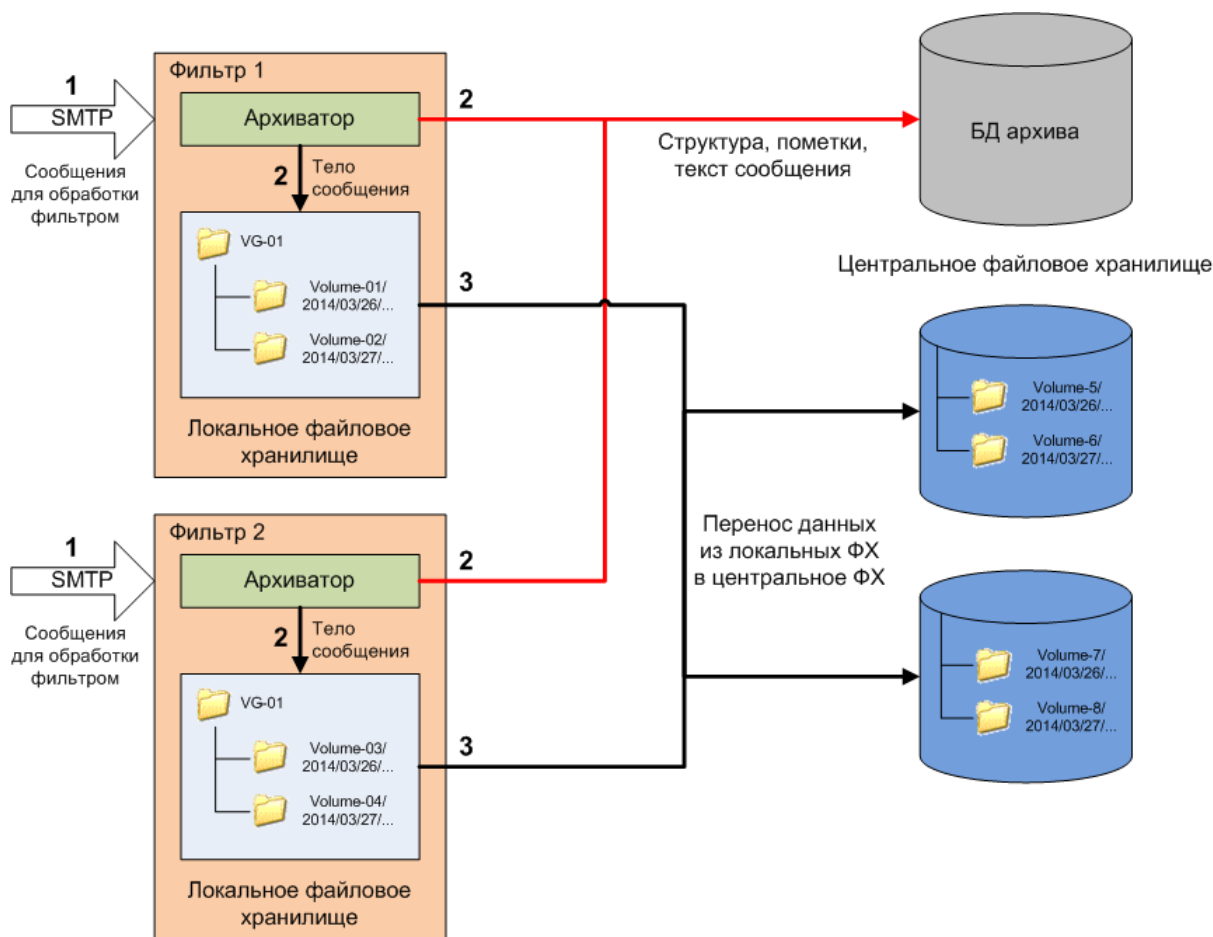


Рис. Е.1. Общая схема организации распределенного файлового хранилища

ФХ имеет структуру каталогов следующего вида:

**<path>/<год>/<месяц>/<число>/<час>/<минута>.**

Каталоги иерархически организованы по времени (в зависимости от времени получения сообщений – эта информация хранится в метаданных сообщения). Здесь **<path>** – каталог с данными ФХ, который указан в настройках конфигурации.

На более низких уровнях вложенности располагаются контейнеры с объектами. Каждый контейнер в своем корневом каталоге содержит файл манифеста, в котором описывается содержимое контейнера в виде xml-структуры. Манифест описывает состояние контейнера с данными, тип данных (сообщение ПК, файл, другое), формат хранения (сжатый файл, дубликат и т. д.). Каждый такой контейнер имеет идентификатор vID, а также области данных и служебных данных. В подкаталоге **vid/data** хранится тело сообщения (файл **body** или **body.gz**, если включено сжатие).

Работа ФХ обеспечивается следующими сервисами:

- **filestorage-ng** – сообщает о наличии объектов в индексе ФХ. По запросу с идентификатором vID объекта проверяет наличие соответствующей записи в индексе БД **Cassandra** и возвращает URL объекта в ФХ, либо возвращает сообщение об ошибке, если объекта с указанным vID нет в индексе. Также используется для размещения в центральном ФХ контейнеров, сформированных на других узлах ФХ. Кроме того, выполняет функции web-сервера, который принимает по протоколу HTTPS запросы от



веб-интерфейса с URL контейнера с телом сообщения в ФХ, и передает тело сообщения на веб-интерфейс.

- **skvt-cassandra** – сервис управления распределенной БД индекса ФХ, в которой хранятся записи обо всех сообщениях, помещенных в ФХ. Такая запись содержит информацию, позволяющую сопоставить идентификатор vID сообщения и каталог ФХ с телом сообщения.

#### Примечание

БД индексов ФХ построена на основе продукта *APACHE CASSANDRA*, поэтому здесь далее БД индексов ФХ будет называться **Cassandra**.

## Е.2. Запись данных в файловое хранилище и базу данных Cassandra

Информация о размещении тела сообщения в ФХ записывается в **Cassandra**. В этой БД хранятся записи с данными о vID-идентификаторах сообщений и их расположении в иерархии каталогов ФХ. Зная идентификатор vID сообщения, можно получить ссылку на каталог с телом сообщения, обратившись к БД **Cassandra**.

Схема добавления записей в БД **Cassandra** показана на рисунке [Рис.Е.2](#).

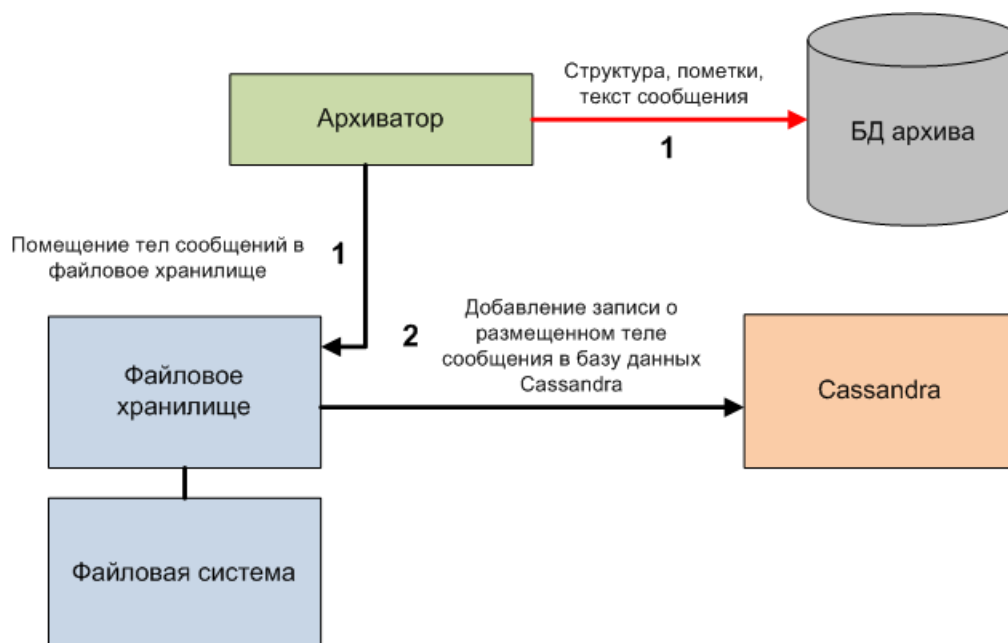


Рис. Е.2. Добавление записей в базу данных Cassandra

## Е.3. Перемещение сообщений из локального ФХ в центральное

Локальное ФХ служит для временного хранения тел сообщений, прошедших фильтрацию. Центральное ФХ предназначено для долговременного хранения сообщений, поступающих со всех узлов фильтрации. Для этого периодически, через настроенные промежутки времени, выполняется перенос накопленных данных из локальных ФХ в центральное.

Схема и порядок перемещения сообщений из локального ФХ в центральное показана на рисунке [Рис.Е.3](#).



Рис. Е.3. Перемещение сообщений из локального в центральное файловое хранилище

Перемещение контейнеров из локального ФХ в центральное осуществляется сервисом **filestorage-ng**, который размещает полученные из локального ФХ контейнеры с данными в центральном ФХ и добавляет записи о размещении контейнеров в базу данных **Cassandra**, после чего удаляет переданные контейнеры из локального ФХ, а затем удаляет соответствующую запись из БД **Cassandra**.

#### Е.4. Извлечение сообщения из файлового хранилища

При обработке запроса на поиск сообщения в архиве, поступившего с АРМ администратора, происходит поиск этого сообщения в БД архива. Если выясняется, что тело сообщения хранится в ФХ, то БД архива возвращает vID искомого сообщения, после чего происходит обращение к сервису **filestorage-ng** для продолжения поиска сообщения сначала в БД **Cassandra**, а затем в ФХ.

Сервис **filestorage-ng** обращается к любому доступному узлу **Cassandra** для поиска информации о сообщении. Для этого передается идентификатор сообщения vID (см. [Рис.Е.4](#)).

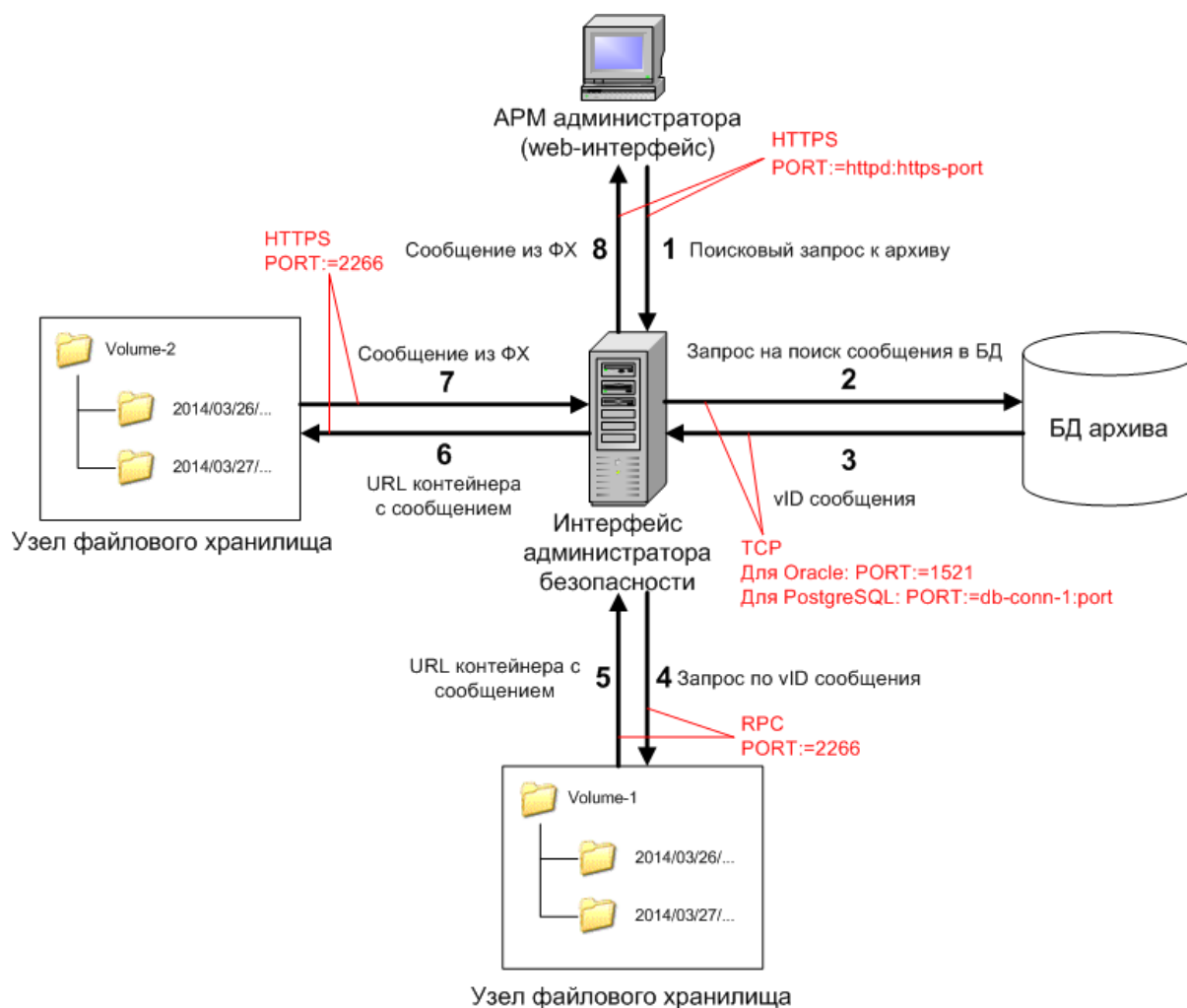


Рис. Е.4. Извлечение сообщения из файлового хранилища

Если запись о сообщении не найдена, то **Cassandra** возвращает ошибку **Not found**. Если в **Cassandra** имеется запись с нужным vID, то сервису **filestorage-ng** возвращается URL контейнера с искомым сообщением. Сервис **filestorage-ng** передает эти данные веб-серверу.

После получения URL контейнера с телом сообщения выполняется запрос на получение файла, хранящегося по указанному URL, к сервису **filestorage-ng** на том узле, где было найдено сообщение. Сервис извлекает файл с телом сообщения и отправляет его веб-серверу. После этого веб-сервер формирует HTML-страницу с результатами поиска для просмотра найденного сообщения.

---

## Приложение F. Создание БД архива на удаленном сервере

Для создания БД архива на удаленном сервере следует выполнить действия:

1. Настроить схему соединения с БД архива на master-узле по инструкции в разделе [8.3.1](#).

2. Создать схему БД архива по инструкции в разделе [8.3.2](#).

3. Подключиться к БД, выполнив следующую команду:

```
# psql -U dozor -h localhost -p <port>
```

где **<port>** – порт, на котором БД ожидает соединения.

4. Проверить версию сервера БД PostgreSQL на master-узле. Для этого ввести следующий запрос:

```
select version();
```

Пример вывода команды:

```
PostgreSQL 11.3 on x86_64-pc-linux-gnu, compiled by gcc (GCC) 4.8.5 20150623 (Red Hat 4.8.5-36),  
64-bit  
(1 строка)
```

В данном примере сервер БД PostgreSQL имеет версию 11.3.

5. Подключиться к удаленному серверу по протоколу SSH.
6. Установить СУБД PostgreSQL версии, полученной на шаге [4](#).
7. Создать группу и учетную запись пользователя **dozor**, выполнив следующие команды:

```
~$ sudo groupadd dozor
```

```
~$ sudo useradd dozor
```

8. Назначить пользователю права на исполнение, выполнив команду:

```
~$ sudo chown dozor:dozor /data/ -R
```

9. Переключиться на пользователя **postgres**, выполнив команду:

```
sudo su - postgres
```

10. Создать учетную запись пользователя СУБД PostgreSQL. Для этого выполнить команду:

```
createuser --interactive
```

При появлении информации:

Введите имя новой роли:

ввести **dozor** и далее подтвердить полномочия суперпользователя, нажав клавишу **y**.

- 
11. Переключиться на пользователя **root**, выполнив команды:

```
$ exit
```

```
$ sudo su - root
```

12. Создать каталог, в котором будут размещаться файлы БД, например, **/data/base/remote**. Для этого выполнить команду:

```
# mkdir -p /data/base/remote
```

13. Скопировать БД архива на удаленный сервер, выполнив команду:

```
rsync -avze ssh --progress --human-readable <master>:<path> /data/base/remote
```

где **<master>** – IP-адрес или FQDN master-узла, а **<path>** – каталог, в котором была создана БД (например, **/data/base/smap-archive/**).

14. Проверить наличие файлов БД архива. Для этого выполнить команду:

```
# ls -la /data/base/remote
```

Убедиться, что в выводе присутствует **dozor dozor**.

15. Запустить БД, выполнив команду:

```
# su dozor -c "pg_ctl -D /data/base/remote start"
```

16. Перейти в раздел GUI Система > Конфигурация > Основные настройки > Доступ к данным > Схемы соединений с БД.

17. В настройках соединения с БД изменить значение параметра **Сетевое имя сервера базы данных** на IP-адрес или FQDN удаленного сервера.

18. Проверить подключение к БД, нажав кнопку **Проверить**.

19. Нажать **Сохранить** и **Применить**.

---

## Лист контроля версий

03/09/2025-15:11