СЕРЧИНФОРМ ДЛП

Руководство администратора

на 413 листах

2020

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин		Определение
Active Directory	–	служба каталогов корпорации Microsoft для операционных систем семейства Windows Server; предоставляет информацию об объектах, позволяет организовывать объекты, управлять доступом к ним, а также устанавливает правила безопасности
GET-запрос	–	метод запроса, который отправляется на сервер с помощью браузера открыто, через URL, адресную строку. Например, запрос поисковой системе Google.
IM-клиент	–	программа-клиент для обмена мгновенными сообщениями посредством сети Интернет
POST-запрос	–	метод запроса, передаваемые параметры которого скрыты от пользователя. В отличие от GET-запроса, позволяет передавать большие объемы данных.
Атрибутный поиск	–	поиск по атрибутам перехваченных документов (дата и время отправки сообщения, имя пользователя локальной сети, IP-/MAC-адрес рабочей станции, с которой осуществлялся перехват и т.п.)
База данных	–	база данных под управлением Microsoft SQL Server, содержащая перехваченные документы
Веб-сервер	–	служба SearchInform Rest API, устанавливаемая и запускаемая на сервере ReportCenter с целью обработки HTTP-запросов веб-браузеров и возвращения им HTTP-ответов (отображение запрашиваемых отчетов)
Веб-отчеты	–	отчеты, доступ и просмотр которых осуществляется посредством веб-интерфейса
Домен	–	иерархическая структура сети, в которой компьютеры имеют разные права
Журналирование	–	функция почтового сервера, позволяющая хранить копии сообщений в центральном почтовом ящике для различных целей, включая архивацию почты
Защита информации	–	деятельность по предотвращению утечки конфиденциальной информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Индекс	–	структура, используемая для быстрого поиска по содержимому перехваченных документов
Индексация рабочих станций	–	операция, позволяющая отслеживать появление, копирование, перемещение и удаление конфиденциальной информации на рабочих станциях сети
Инцидент	–	факт нарушения настроенных политик безопасности, зафиксированный компонентом AlertCenter
Информационная безопасность	–	состояние защищенности информационной среды предприятия, обеспечивающее его функционирование и развитие в интересах его персонала
Карантин	–	хранилище заблокированных исходящих почтовых сообщений, нарушающих политики безопасности. По решению администратора безопасности заблокированные сообщения могут быть впоследствии отправлены указанному адресату.
Консоль администрирования	–	графический интерфейс, предназначенный для управления сервером
Контроллер домена	–	сервер, контролирующий область компьютерной сети (домен)
Критерий поиска	–	поисковый запрос, настроенный на обнаружение определенной информации, например, поиск по ключевому слову, фразе, значению атрибута
Парсинг	–	процесс разбора трафика на составляющие (атрибуты и их значения) с помощью анализаторов
Политика безопасности	–	настроенный набор поисковых запросов (критериев поиска), выявляющих факты нарушения данной политики
Программный продукт	–	программное обеспечение как результат человеческой деятельности, выставленный на рынке массового покупателя в качестве товара и имеющий ненулевую потребительную стоимость
Рабочая группа	–	организация локальной сети, в которой все компьютеры являются равноправными
Регулярное выражение	–	формальный язык поиска и осуществления манипуляций с подстроками в тексте, основанный на использовании метасимволов
Сервер баз данных	–	сервер Microsoft SQL, служащий для управления базами данных компонентов Серчинформ ДЛП

Система	–	автоматизированная система защиты информации
Текстовый поиск	–	поиск по ключевым словам и выражениям с учетом морфологии и синонимов
Фразовый поиск	–	частный случай текстового поиска, при котором можно зафиксировать порядок следования слов и выражений запроса
Поиск похожих	–	поиск текстовых документов, похожих по содержанию. В ходе поиска похожих, запрашиваемый текст сопоставляется каждому документу индекса. Документы, похожие по содержанию на запрос, фильтруются по степени сходства или «релевантности»
Цифровые отпечатки	–	способ идентификации данных на основании сформированного набора эталонных документов (образцов)

СОКРАЩЕНИЯ

Сокращение		*Расшифровка*
АРМ	–	Автоматизированное Рабочее Место
ИБ	–	Информационная Безопасность
ИРС	–	Индексация Рабочих Станций
ИС	–	Информационные Системы
ЛВС	–	Локальная Вычислительная Сеть
ОС	–	Операционная Система
ПО	–	Программное Обеспечение
РС	–	Рабочая Станция
СТП	–	Служба Технической Поддержки

1 ВВЕДЕНИЕ

Настоящее руководство содержит сведения по установке и первоначальной настройке системы «Серчинформ ДЛП».

1.1 Назначение системы

Программное решение Серчинформ ДЛП предназначено для выявления и предотвращения утечек конфиденциальной информации и персональных данных в ЛВС организаций, а также контроля данных, уходящих в Интернет.

1.2 Возможности Системы

Серчинформ ДЛП позволяет выявлять утечки конфиденциальной информации и персональных данных через электронную почту; ICQ; голосовые и текстовые сообщения Skype, Lync, Telegram, WhatsApp и Viber; посты на форумах или комментарии в блогах; документы облачных сервисов; внешние устройства (USB/CD); FTP; файл-серверы; ноутбуки, в том числе отключенные от корпоративной сети; документы, отправляемые на печать; а также появление конфиденциальной информации на компьютерах пользователей. Ответственные сотрудники оперативно оповещаются о нарушениях политики безопасности. Расширенные поисковые возможности позволяют эффективно защищать конфиденциальные данные при минимальных трудозатратах на анализ информационных потоков. Кроме того, служба профилирования позволяет построить профиль пользователя на основании генерируемого им цифрового контента – электронной корреспонденции, чатов в личных и корпоративных мессенджерах, таких как Viber, Telegram, WhatsApp, Lync, Skype, популярные соцсети и IM-клиенты.

1.3 Требования к численности и квалификации персонала Системы

Для обслуживания системы является достаточным наличие 2 администраторов.

Администраторы должны пройти обучение у сотрудников компании-разработчика программного обеспечения или у авторизованного им провайдера услуг. Также подготовка администраторов системы проводится во время опытной эксплуатации системы сотрудниками компании-разработчика.

В Таблица 1 представлен ролевой состав, функции и требования к квалификации персонала, осуществляющего сопровождение системы.

Таблица 1 – Требования к функциям и квалификации персонала Системы

Роль	**Функции**	**Уровень квалификации**
Администратор Системы (программного обеспечения)	Модернизация, настройка и мониторинг работоспособности Системы. Установка, модернизация, настройка и мониторинг работоспособности системного и базового ПО. Установка, настройка и мониторинг прикладного ПО. Управление базами данных. Ведение учетных записей пользователей Системы.	Профильное высшее образование. Сертификаты компании-производителя Системы
Администратор аппаратного обеспечения[1]	Сопровождение аппаратного обеспечения	Стандартные требования Компании
Сетевой администратор[2]	Сопровождение сетевых коммуникаций	Стандартные требования Компании
Инженер технической поддержки[3]	Установка и настройка всех компонентов Системы. Сопровождение при неполадках компонентов Серчинформ ДЛП	Стандартные требования Компании. Знания инструкций по установке Системы
Сотрудник службы безопасности	Поиск (отслеживание) конфиденциальной информации в общем потоке контролируемого документооборота: – формализация анализа текстовых документов посредством настройки списка поисковых запросов; – настройка расписания проверок; – предварительный просмотр документа, идентифицированного как конфиденциальный, и принятие решения о целесообразности дальнейшей проверки.	Стандартные требования Компании. Знания инструкции аудитора Системы

[1] Администратор аппаратного обеспечения предоставляется Заказчиком.
[2] Сетевой администратор предоставляется Заказчиком.
[3] Инженер технической поддержки предоставляется Исполнителем.

1.4 Режимы функционирования Системы

Основной режим функционирования Системы – автоматизированный, под управлением администратора Системы.

Система обеспечивает возможность работы в следующих режимах:

- *штатный режим* (непрерывная круглосуточная работа);
- *сервисный режим* (для проведения обслуживания, реконфигурации и модернизации компонентов Системы);
- *автономный режим* (в случае отсутствия связи между компонентами Системы или с внешними сетями, для доступа к конфигурационной и архивной информации).

1.4.1 Штатный режим работы

Выбранные модули Системы обеспечивают непрерывную и круглосуточную работу, с учетом перерывов, необходимых для технического обслуживания и профилактики, за исключением технологических окон, определяемых Администратором Системы для проведения обновления или модернизации Системы. В основном режиме работы модули Системы обеспечивают выполнение возложенных на них функций в полном объеме.

Возникновение сбоев в работе Системы (кратковременных неисправностей, устранение которых не требует участия квалифицированного персонала и ощутимых временных затрат) не приводит к переводу Системы в автономный режим или в сервисный режим.

При возникновении отказа (неисправность, устранение которой требует проведения ремонтных или аварийно-восстановительных работ) Система переходит в автономный режим.

Персонал, занимающийся обслуживанием Системы, ведет постоянный процесс диагностирования работы модулей Системы с целью своевременного выявления отказов или сбоев в работе Системы. Список компонентов Системы, способы их диагностики, описание возможных отказов и действий по устранению этих отказов приведены в Таблица 2. При выходе из строя компонентов серверного ПО Системы, Система должна быть восстановлена силами обслуживающего персонала в течение одного часа.

Таблица 2 – Способы диагностики компонентов Системы, возможные отказы и действия по их устранению

Компонент	**Способы диагностики**	**Отказ**	**Влияние отказа на работу Системы**	**Устранение отказа**
Компоненты Windows на сервере Системы	– Журнал событий Windows – Уведомления по эл. почте	Нарушение работы ОС	Частичная остановка функций сбора, индексации и анализа перехваченных данных. Прекращение доступа к средствам диагностики и управления Системой.	Восстановление работы ОС
СУБД Microsoft SQL Server, содержащая настройки Системы и перехваченные данные	– Журнал событий СУБД – Журнал событий DataCenter – Уведомления по электронной почте	Нарушение целостности БД	Остановка сервиса сбора, индексации и анализа данных перехвата, потеря данных перехвата	Восстановление СУБД из резервной копии. Переустановка ПО без восстановления данных.
Консоли управления компонентами Системы	– Журнал событий ОС – Визуальный контроль	Нарушение работы ПО	Прекращение доступа к одному из средств диагностики и управления Системой	Переустановка ПО
Серверные компоненты Системы	Журнал событий DataCenter Уведомления по электронной почте	Нарушение работы одной или нескольких служб Системы на одном из серверов	Частичная остановка служб сбора, индексации и анализа перехваченных данных	Восстановление ОС сервера из резервной копии. Восстановление настроек программного компонента из резервной копии.

Компонент	Способы диагностики	Отказ	Влияние отказа на работу Системы	Устранение отказа
Агент Системы на РС пользователей и серверах	Консоль EndpointController	Нарушение работы ПО	Остановка службы сбора данных для РС или сервера	Переустановка ПО

1.4.2 Сервисный режим работы

Перевод Системы в сервисный режим производится при необходимости проведения мероприятий по техническому обслуживанию, требующих временного останова одного или нескольких модулей Системы.

В сервисном режиме Система может не выполнять часть возложенных на нее функций.

Перечень мероприятий по техническому обслуживанию, требующих останова системы, частота и порядок проведения таких мероприятий определяются эксплуатационной документацией на применяемые в составе Системы модули.

1.4.3 Автономный режим работы

Переход Системы в автономный режим происходит при возникновении отказа одного или нескольких модулей Системы. Список компонентов Системы, способы их диагностики, описание возможных отказов и действий по устранению этих отказов приведены в Таблица 2.

1.5 Перечень эксплуатационной документации

Перечень эксплуатационных документов, с которыми необходимо ознакомиться:

- Серчинформ ДЛП. «Руководство администратора»;
- Серчинформ ДЛП. «Руководство пользователя».

2 ОБЩИЕ СВЕДЕНИЯ

2.1 Назначение Системы

Серчинформ ДЛП предназначен для выявления и предотвращения утечек конфиденциальной информации и персональных данных в локальных вычислительных сетях (далее – ЛВС) организаций.

Система позволяет:

- контролировать входящий и исходящий почтовый трафик на уровне рабочих станций (далее – РС) и/или сетевых протоколов (SMTP, POP3, NNTP, IMAP, MAPI, Web mail);
- блокировать на уровне РС исходящий SMTP-трафик для отдельных пользователей;
- интегрироваться с распространенными почтовыми и прокси-серверами;
- контролировать сообщения и файлы, переданные с помощью различных IM-клиентов (ICQ/QIP, Mail.ru Agent, Jabber, Google Hangouts, MS Lync, Viber, Telegram, WhatsApp), а также переписку в популярных социальных сетях (Facebook, LinkedIn, В Контакте, Мой Мир@Mail.ru, Одноклассники, Google+, Мамба, Imo, Meebo);
- контролировать трафик Skype: сеансы текстовой и голосовой связи, файлы и SMS-сообщения;
- контролировать и ограничивать доступ пользователей или групп пользователей к устройствам (дисководам, CD/DVD-приводам, сменным накопителям, жестким дискам, мобильным устройствам типа iPod) и портов ввода-вывода (USB, FireWire, COM, LPT, IrDA);
- хранить для каждого пользователя точную копию данных, переданных на внешние устройства (теневое копирование);
- протоколировать все действия пользователей с файлами, расположенными в общих сетевых папках и/или файловых серверах;
- контролировать отправку документов на печать;
- перехватывать GET-/POST-запросы и файлы, передаваемые по HTTP(S)-протоколу;
- контролировать FTP-трафик;
- контролировать данные облачных сервисов (Evernote, SkyDrive, OneDrive, Office 365, Google Drive, Dropbox, Yandex Disk, MailRuCloud, SharePoint, ICloud, DropMeFiles, Amazon S3, OwnCloud, Pcloud, OziBox, MediaFire, OpenDrive, 4shared, Box, Syncplicity, CloudMe, MiMedia);
- фиксировать нажатия клавиш пользователями;
- осуществлять звукозапись разговоров пользователей;

- перехватывать информацию, отображаемую на мониторах РС;
- контролировать изменения файлов на РС, серверах, сетевых ресурсах;
- отслеживать посредством веб-камеры личность пользователя, авторизовавшегося в системе, наличие пользователя на рабочем месте, а также его действия в течение рабочего дня;
- контролировать активность пользователей в запускаемых ими приложениях;
- собирать документы, хранящиеся на жестких дисках станций ЛВС, индексировать и просматривать данные документы (поддерживается около 100 файловых форматов);
- контролировать действия сотрудников службы ИБ в консолях компонентов Серчинформ ДЛП;
- контролировать данные, отправляемые с ноутбука, когда сотрудник находится вне корпоративной сети;
- однозначно идентифицировать пользователя, отправившего информацию, благодаря интеграции с доменной структурой Windows;
- исключать из перехвата трафика отдельных пользователей, пользующихся доверием;
- фильтровать перехваченную информацию и сохранять в базу данных лишь те данные, которые представляют интерес;
- управлять всеми возможными функциями агента с АРМ сотрудника службы безопасности с помощью консоли управления;
- разграничить права доступа к перехваченной информации;
- контролировать работу компонентов Серчинформ ДЛП и условий, необходимых для их корректной работы;
- автоматизировать управление индексами и базами данных компонентов Системы;
- анализировать передаваемые и принимаемые данные согласно настроенным политикам безопасности и уведомлять сотрудников службы безопасности о фактах их нарушения по электронной почте;
- собирать статистику и составлять отчеты по активности пользователей и инцидентам, связанным с нарушениями политик безопасности;
- создавать психологические профили пользователей на основании генерируемого им цифрового контента – электронной корреспонденции, чатов в личных и корпоративных мессенджерах, таких как Viber, Telegram, WhatsApp, Lync, Skype, популярные соцсети и IM-клиенты.

2.2 Архитектура Системы

Серчинформ ДЛП базируется на клиент-серверной архитектуре.

Серверные компоненты Серчинформ EndpointController и Серчинформ NetworkController представляют собой платформы, на которых работают модули перехвата данных. Компонент Серчинформ EndpointController осуществляет перехват данных на уровне PC пользователей с помощью специально устанавливаемых агентов, в то время как сервер Серчинформ NetworkController осуществляет перехват данных на уровне сетевых шлюзов методом зеркалирования трафика.

Каждый модуль перехвата выступает в роли анализатора трафика и контролирует свои каналы передачи данных. Для текущей версии системы предусмотрены следующие модули перехвата:

- модуль перехвата MailController;
- модуль перехвата IMController;
- модуль перехвата SkypeController;
- модуль перехвата HTTPController;
- модуль перехвата FTPController;
- модуль перехвата CloudController;
- модуль перехвата DeviceController;
- модуль перехвата PrintController;
- модуль перехвата ProgramController;
- модуль перехвата MonitorController;
- модуль перехвата CameraController;
- модуль перехвата MicrophoneController;
- модуль перехвата KeyLogger;
- модуль перехвата FileController;
- модуль перехвата FileAuditor;
- модуль перехвата Индексация рабочих станций.

Сервер индексации Search Server индексирует документы, перехваченные посредством зеркалирования трафика на сетевых шлюзах либо с помощью установленных на PC агентов, и обеспечивает поддержание индекса в постоянно актуальном состоянии.

Сервер Серчинформ AlertCenter обеспечивает проверку индексов по настроенным политикам безопасности на предмет их нарушения.

Сервер Серчинформ DataCenter предназначен для разграничения прав сотрудников службы безопасности, мониторинга состояния компонентов Системы и управления всеми базами данных и индексами, созданными этими компонентами. В своем составе имеет сервер Серчинформ ReportCenter, который, в свою очередь, получает статистику по перехваченным документам и инцидентам, и записывает ее в собственную базу данных.

Консоли серверных компонентов Серчинформ EndpointController, Серчинформ NetworkController и Search Server позволяют управлять процессами настройки перехвата и индексирования данных.

В качестве клиентской части выступают:

- клиентское приложение Серчинформ AnalyticConsole, предназначенное для работы с индексами и базами данных, содержащими перехваченную информацию, обработки статистических данных и формирования по ним отчетов, работы с психологическими портретами пользователей;
- клиентское приложение Серчинформ AlertCenter, предоставляющее возможность создания и настройки политик безопасности (набора правил, в соответствии с которыми фиксируются инциденты) и просмотра нарушений для текущего набора правил проверки;
- клиентское приложение Серчинформ DataCenter, предназначенное для управления индексами, базами данных и службами компонентов Системы.

2.3 Контролируемые протоколы

Система контролирует следующие протоколы и веб-приложения:

- SMTP – сетевой протокол, предназначенный для передачи электронной почты в сетях TCP / IP. Также поддерживается Extended SMTP (ESMTP). Поддерживаются незащищенные и защищенные (SSL/TSL) соединения;
- POP3 – интернет-протокол прикладного уровня, используемый клиентами электронной почты для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению. Поддерживаются незащищенные и защищенные (SSL/TSL) соединения;
- NNTP – сетевой протокол распространения, запрашивания, размещения и получения групп новостей при взаимодействии между сервером групп новостей и клиентом;
- IMAP (в том числе IMAP Compressed) – протокол прикладного уровня для доступа к электронной почте, предоставляющий пользователю обширные возможности для работы с почтовыми ящиками, находящимися на центральном сервере;
- MAPI (в том числе RPC over HTTP) – программный интерфейс, позволяющий приложениям работать с различными системами передачи электронных сообщений. Позволяет получать, читать, создавать, отправлять сообщения, присоединять к ним файлы, получать доступ к присоединенным файлам и т.д.;
- FTP (протокол передачи файлов) – стандартный протокол для передачи файлов с одного компьютера на другой через сеть Internet. Поддерживаются

активный и пассивный режимы FTP-соединений. Также поддерживается FTPS (FTP + SSL);

- HTTP (протокол передачи гипертекста) – протокол прикладного уровня для распределенных и объединенных информационных систем. Также поддерживается HTTPS (SSL + HTTP);
- Social Networks – контроль сайтов социальных сетей. Поддерживаются следующие сайты социальных сетей: Facebook, LinkedIn, Odnoklassniki, Vkontakte, Мой Мир@Mail.Ru, Google+, Mamba, Imo, Meebo;
- Cloud – контроль данных облачных сервисов. Модуль позволяет отслеживать следующие облачные хранилища данных: Evernote, Skydrive (включая Office 365), Google Drive, Dropbox, Yandex Disk, MailRuCloud, SharePoint, ICloud, DropMeFiles, Amazon S3, OwnCloud, Pcloud, OziBox, MediaFire, OpenDrive, 4shared, Box, Syncplicity, CloudMe, MiMedia;
- Web Mail – контроль почтовых веб-служб:
    - Exchange Web Services – исходящая и входящая почта;
    - Kerio Outlook Connect – исходящая и входящая почта;
    - Outlook Web App и Outlook Web App light – исходящая и входящая почта;
    - Zimbra Web Client – исходящая и входящая почта;
    - исходящая и входящая корреспонденция с почтовых веб-серверов: Gmail, Hotmail, mail.ru, tut.by, open.by, freemail.ru, yandex.ru, rambler.ru и других. Поддерживаются незащищенные и защищенные (SSL) соединения;
- Skype – популярная бесплатная программа видео- и аудиообщения в режиме реального времени;
- ICQ/QIP – открытый сетевой протокол OSCAR, обеспечивает обмен сообщениями в реальном времени. Поддерживаются незащищенные и защищенные (SSL) соединения;
- XMPP – основанный на XML, открытый протокол для мгновенного обмена сообщениями. Поддерживаются незащищенные и защищенные (SSL) соединения;
- Mail.ru Agent – программа для быстрого обмена сообщениями через Интернет, разработанная компанией Mail.ru;
- SIP – протокол передачи данных, описывающий способ установления и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным содержимым (видео- и аудиоконференция, мгновенные сообщения);

- Viber, Telegram, WhatsApp – кроссплатформенные приложения для бесплатных сообщений, файлов и звонков, которые интегрируются в адресную книгу и авторизуют по номеру телефона.

Перехват шифрованного SSL-/TSL-трафика возможен с помощью агентов Серчинформ EndpointController либо путем зеркалирования (в случае, когда в сети установлен прокси-сервер, способный производить мониторинг шифрованного трафика).

2.3.1 Контроль других каналов передачи данных

Агенты Серчинформ EndpointController позволяют также:

- осуществлять перехват данных, отправленных на печать;
- контролировать доступ пользователей к внешним устройствам (CD/DVD-приводы, съемные накопители USB и FireWire, USB-устройствам WiFi и Bluetooth) и портам (USB, Firewire, COM, LPT, IRDA, Windows Mobile, Palm), а также осуществлять теневое копирование всех сохраняемых на внешние устройства данных в специальное файловое хранилище;
- протоколировать файлы, статически хранящиеся, создаваемые, изменяемые на PC пользователей;
- перехватывать информацию, отображаемую на одном или нескольких мониторах PC, включая список запущенных процессов, а также предоставляют возможность просмотра активности экрана одного или нескольких пользователей в режиме реального времени;
- фиксировать активность пользователей и запускаемых ими приложений в течение рабочего дня;
- осуществлять звукозапись разговоров пользователей, находящихся как внутри офиса, так и за его пределами (в командировках);
- фиксировать нажатия клавиш пользователями (включая системные клавиши) и контролировать содержимое буфера обмена.

3 ОБЯЗАННОСТИ И ЗАДАЧИ АДМИНИСТРАТОРА

В круг типовых задач администратора относительно системы входят:

- выбор, установка и конфигурирование рекомендуемого Разработчиком аппаратного и программного обеспечения;
- настройка локальной сети и обеспечение ее оптимального функционирования;
- установка и настройка СУБД MS SQL Server, резервное копирование баз данных, сохранение резервных копий; восстановление баз данных; архивирование информации;
- создание и поддержание в актуальном состоянии пользовательских учётных записей, наделение их достаточными правами;
- настройка прокси- и почтовых серверов, свитча с функцией зеркалирования;
- конфигурирование сетевых протоколов и портов;
- развертывание и настройка Серчинформ ДЛП [4];
- установка и настройка антивирусного ПО и файерволов;
- планирование и проведение работ по расширению сетевой структуры предприятия;
- обеспечение необходимого качества функционирования серверов;
- устранение неполадок в системе собственными силами, а в случае невозможности, с помощью СТП компании-разработчика;
- ответственность за информационную безопасность в компании;
- документирование всех произведенных действий.

В организациях с большим штатом сотрудников вышеупомянутые обязанности могут делиться между несколькими администраторами безопасности, например, могут быть отдельные администраторы баз данных, администраторы сети и администраторы почтовых серверов.

[4] Установка и первоначальная настройка компонентов Серчинформ ДЛП может быть также произведена инженером СТП компании-разработчика.

4 ПОДГОТОВКА К УСТАНОВКЕ

4.1 Системные требования

Компоненты Серчинформ ДЛП могут работать под управлением ОС семейства Windows, обозначенных в Таблица 3.

Таблица 3 – Поддерживаемые операционные системы

Компоненты	XP x32/x64	7 x32/x64	8, 8.1 x32/x64	10 x32/x64	2003 x32/x64	2008 R1 x32/x64	2008 R2	2012, 2012 R2	2016	2019
Search Server							+	+	+	+
Сервер DataCenter							+	+	+	+
Сервер EndpointController							+	+	+	+
Сервер NetworkController							+	+	+	+
Сервер AlertCenter							+	+	+	+
Сервер ReportCenter							+	+	+	+
Серчинформ AnalyticConsole		+	+	+			+	+	+	+
Клиент AlertCenter		+	+	+	+	+	+	+	+	+
Агенты EndpointController [5]	+	+	+	+	+	+	+	+	+	+

Агенты EndpointController могут работать под управлением операционных систем семейства Linux[6], которые приведены в Таблица 4.

[5] С 01.01.2020 развитие функционала для агентов, работающих на операционной системе Windows XP и Windows Server 2003, прекращено. Возможность работы агента в данных операционных системах сохранена, но с функционалом, актуальным на конец 2019 года.

[6] Контролируются следующие протоколы: HTTP/HTTPS, SMTP, POP3, IMAP, Web mail, IM (XMPP, HTTPIM), FTP, Cloud, Device.

Таблица 4 – Системные требования к ОС Linux для работы агента EndpointController

ОС	Поддерживаемые версии	Поддерживаемые ядра
Astra Linux	1.4 x64 (сборки «Смоленск» и «Орёл»)	Special Edition (Смоленск) – 3.16.0
CentOS	7.3 x64	3.10.0
	7.6 x64 [7]	3.10.0 (DeviceController – 3.10.0-957)
GosLinux	6.4 x64	3.10.0
ROSA Linux	6.8 x64	4.9.20
Ubuntu [8]	16.04 x32/x64	• x32 – 4.4.0 и 4.15.0 (DeviceController – 4.4.0-135, 4.4.0-140, 4.15.0-29, 4.15.0-39) • x64 – 4.4.0 и 4.15.0 (DeviceController – 4.4.0-122, 4.4.0-135, 4.4.0-140, 4.15.0-29, 4.15.0-32, 4.15.0-36, 4.15.0-39)
	17.04 x32/x64	• x32 – 4.10.0 (DeviceController – 4.10.0-42) • x64 – 4.10.0 (DeviceController – 4.10.0-19)
	18.04 x64	4.15.0 (DeviceController – 4.15.0-29, 4.15.0-32, 4.15.0-36, 4.15.0-39)

Перед установкой агента EndpointController на PC убедитесь, что конфигурация данной PC достаточна для его корректной работы. При наличии на PC большого количества установленного стороннего софта, который также занимает оперативную память, компания-разработчик не дает гарантий качества и скорости функционирования PC с минимальной конфигурацией.

Минимальные требования к PC с работающим агентом приведены в Таблица 5.

Таблица 5 – Минимальные требования к PC с работающим агентом EndpointController

Позиция/требование	Значение
Процессор	1-ядерный частотой 2 ГГц
Оперативная память	1 ГБ
Винчестер	250 ГБ
Сетевая карта	100 Мбит/с
Операционная система	Windows Server 2019, Server 2016, 10 x32/x64, 8/8.1 x32/x64, Server 2012/2012 R2, 7 x32/x64, Server 2008 R2, Server 2008 R1 x32/x64, Server 2003 x32/x64

[7] Возможность блокировки USB-устройств и сетевых ресурсов.

[8] Возможность блокировки USB-устройств и сетевых ресурсов.

При необходимости установки модуля «Индексация Рабочих Станций», для индексации 200 рабочих станций, необходим выделенный сервер, по своим характеристикам не хуже приведенных в Таблица 6.

Таблица 6 – Рекомендуемые требования к серверу индексации Search Server с модулем «Индексация Рабочих Станций»

Позиция/требование	**Значение**
Процессор	4-ядерный частотой 2,4 ГГц
Оперативная память	16 ГБ
Винчестер	1 ТБ RAID
Сетевая карта	1 ГБ/с
Операционная система	MS Windows Server 2008 R2

Для закрытия бóльшего количества компьютеров, число серверов увеличивается линейно.

Типовая конфигурация сервера компонентов Серчинформ ДЛП, достаточная для проведения тестирования не более чем на 50 PC, приведена в Таблица 7.

Таблица 7 – Минимальная конфигурация для проведения тестирования Серчинформ ДЛП (до 50 рабочих станций)

Позиция/требование	**Значение**
Процессор	2-ядерный частотой 2,0 ГГц
Оперативная память	8 ГБ
Винчестер	1 ТБ
Сетевая карта	2 x 1 ГБ/с
Операционная система	MS Windows Server 2008 R2
СУБД	MS SQL Server 2008 R2

Данная конфигурация рекомендована только для проведения базового тестирования функциональных возможностей Серчинформ ДЛП (получения понятия идеологии работы, получения впечатления об интерфейсе, просмотра информации «на выходе»).

Для проведения полноценного тестирования в условиях сетевой инфраструктуры используйте конфигурации, предложенные в Таблице 6 – Таблице 11.

Таблица 8 – Минимальные конфигурации двух серверов для коммерческого использования и тестирования Серчинформ ДЛП (до 100 рабочих станций)

Сервер 1 (NetworkController, DataCenter agent)	
Позиция/требование	Значение
Процессор	2-ядерный частотой 2,0 ГГц
Оперативная память	4 ГБ
Винчестер	500 ГБ (желательно RAID)

Сетевая карта	2 x 1 ГБ/с
Операционная система	MS Windows Server 2008 R2
Сервер 2 (Search Server, EndpointController, DeviceController, AlertCenter, ReportCenter, DataCenter Server, MS SQL Server)	
Позиция/требование	**Значение**
Процессор	4-ядерный частотой 2,4 ГГц
Оперативная память	8 ГБ
Винчестер	500 ГБ RAID
Сетевая карта	1 ГБ/с
Операционная система	MS Windows Server 2008 R2
СУБД	MS SQL Server 2008 R2 Standard/Enterprise Edition

Таблица 9 – Минимальная конфигурация одного сервера для коммерческого использования и тестирования Серчинформ ДЛП (до 100 рабочих станций)

Сервер 1 (все компоненты Серчинформ ДЛП)	
Позиция/требование	**Значение**
Процессор	2 x 4-ядерных частотой 2,4 ГГц
Оперативная память	12 ГБ
Винчестер	1 ТБ RAID
Сетевая карта	2 x 1 ГБ/с
Операционная система	MS Windows Server 2008 R2
СУБД	MS SQL Server 2008 R2 Standard/Enterprise Edition

Таблица 10 – Минимальные конфигурации двух серверов для коммерческого использования и тестирования Серчинформ ДЛП (100-300 рабочих станций)

Сервер 1 (NetworkController, DataCenter agent)	
Позиция/требование	**Значение**
Процессор	4-ядерный частотой 2,4 ГГц
Оперативная память	4 ГБ
Винчестер	1 ТБ (желательно RAID)
Сетевая карта	2 x 1 ГБ/с
Операционная система	MS Windows Server 2008 R2
Сервер 2 (Search Server, EndpointController, DeviceController, AlertCenter, ReportCenter, DataCenter Server, MS SQL Server)	
Позиция/требование	**Значение**
Процессор	4-ядерный частотой 2,4 ГГц
Оперативная память	12 ГБ
Винчестер	1 ТБ RAID
Сетевая карта	1 ГБ/с
Операционная система	MS Windows Server 2008 R2
СУБД	MS SQL Server 2008 R2 Standard/Enterprise Edition

Таблица 11 – Минимальная конфигурация одного сервера для коммерческого использования и тестирования Серчинформ ДЛП (100-300 рабочих станций)

Сервер 1 (все компоненты Серчинформ ДЛП)	
Позиция/требование	**Значение**
Процессор	2 x 4-ядерных частотой 2,4 ГГц
Оперативная память	16 ГБ
Винчестер	2 ТБ RAID
Сетевая карта	2 x 1 ГБ/с
Операционная система	MS Windows Server 2008 R2
СУБД	MS SQL Server 2008 R2 Standard/Enterprise Edition

Таблица 12 – Минимальные конфигурации трех серверов для коммерческого использования и тестирования Серчинформ ДЛП (300-1000 рабочих станций)

Сервер 1 (NetworkController, DataCenter agent)	
Позиция/требование	**Значение**
Процессор	4-ядерный частотой 2,4 ГГц
Оперативная память	8 ГБ
Винчестер	1 ТБ (желательно RAID)
Сетевая карта	2 x 1 ГБ/с
Операционная система	MS Windows Server 2008 R2
Сервер 2 (Search Server, EndpointController, DataCenter Server)	
Позиция/требование	**Значение**
Процессор	4-ядерный частотой 2,4 ГГц
Оперативная память	16 ГБ
Винчестер	1 ТБ RAID
Сетевая карта	1 ГБ/с
Операционная система	MS Windows Server 2008 R2
Сервер 3 (DeviceController, AlertCenter, ReportCenter, DataCenter agent, MS SQL Server)	
Позиция/требование	**Значение**
Процессор	4-ядерный частотой 2,4 ГГц
Оперативная память	16 ГБ
Винчестер	1 ТБ RAID
Сетевая карта	1 ГБ/с
Операционная система	MS Windows Server 2008 R2
СУБД	MS SQL Server 2008 R2 Standard/Enterprise Edition

Таблица 13 – Минимальная конфигурация одного сервера для коммерческого использования и тестирования Серчинформ ДЛП (300-1000 рабочих станций)

Позиция/требование	**Значение**
Процессор	2 × 4-ядерных частотой 2,4 ГГц
Оперативная память	24 ГБ
Винчестер	2 ТБ RAID
Сетевая карта	2 x 1 ГБ/с

Позиция/требование	Значение
Операционная система	MS Windows Server 2008 R2
СУБД	MS SQL Server 2008 R2 Standard/Enterprise Edition

Минимальные системные требования к PC сотрудника службы безопасности, управляющего политиками безопасности, получающего и просматривающего информацию по инцидентам и осуществляющего генерирование отчетов, приведены в Таблица 14.

Таблица 14 – Минимальные требования к конфигурации рабочей станции сотрудника службы безопасности

Позиция/требование	Значение
Процессор	1 ГГц
Оперативная память	1 ГБ
Винчестер	2 ГБ свободного пространства
Сетевая карта	100 Мбит/с
Операционная система	Windows Server 2019, 2016, 2012/2012 R2, 2008 R2, 2008 x32/x64, 2003 x32/x64 Windows 10 x32/x64, 8/8.1 x32/x64, 7 x32/x64

4.2 Порты, используемые клиентами и агентами

В процессе работы компонентов Серчинформ ДЛП используются следующие порты:

- Для работы агентов EndpointController по умолчанию используется порт 8999, однако его можно заменить на любой другой.
- Для работы режимов LiveView, LiveSound и LiveCam, на рабочих станциях с установленными агентами должны быть открыты TCP порты 18999, 18998 и 18997, соответственно (номера портов, заданные по умолчанию, можно изменить в настройках).
- Все клиентские приложения при подключении к индексам используют порты 8953.
- DataCenter Server и DataCenter agent используют по умолчанию порт 9094/9096.
- Для модуля интеграции NetworkController с ISA/TMG по умолчанию установлен порт 1344, однако его можно заменить на любой другой.
- Для установки агентов EndpointController требуются открытые порты: TCP – 135, 139, 445; UDP – 137, 138 (инициируются со стороны сервера).
- Для инициирования со стороны агента достаточно открытия HTTP-порта EndpointController (обычно 8999) и TCP 139, 445.
- Для работы классификатора сайтов ReportCenter должен быть открыт HTTP(S)-порт 443.

Native SQL Client по умолчанию использует порт 1433, однако его можно заменить на любой другой.

4.3 Требования к учетным записям и правам

4.3.1 Учетная запись для запуска служб сервера NetworkController

Требуются следующие права и возможности:

- Права локального администратора на сервере NetworkController.
- Доступ к серверу баз данных NetworkController.
- Полные права доступа к БД NetworkController (создание баз данных/таблиц/…; чтение/запись/…).
- Доступ к журналам безопасности всех контроллеров доменов, к которым подключаются пользователи (контроллеры доменов должны быть доступны с сервера NetworkController).
- Права на чтение журналов безопасности всех контроллеров доменов, к которым подключаются пользователи. По умолчанию данными правами обладают члены группы Администраторы контроллера домена.

Для работы с административной консолью учетной записи нужны следующие права и возможности:

- Права локального администратора на сервере NetworkController.
- Доступ к серверу БД NetworkController.
- Полные права доступа к БД NetworkController (создание баз данных/таблиц/…; чтение/запись/…).

Для работы с клиентскими приложениями учетной записи требуются следующие права:

- Доступ к БД NetworkController;
- Доступ к серверу индексации Search Server (TCP/IP, порт 8953).

Прочие требования:

- Журналирование операций успешных логинов на всех контроллерах доменов, к которым подключаются пользователи, а также хранение этих записей в журнале как минимум в течение 72 часов.
- При интеграции по ICAP должны быть открыты соответствующие порты на сервере NetworkController, и он должен быть доступен с прокси-сервера. По умолчанию, это порт 1344 (ICAP Port Server), однако в настройках может быть задан другой порт.

4.3.2 Учетная запись для запуска служб сервера EndpointController

Необходимы следующие права и возможности:

- Право входа в систему в качестве службы (эти права должны быть заданы на уровне доменных политик, если они перекрывают локальные).
- Права локального администратора на сервере EndpointController.
- Права полного доступа к диспетчеру управления службами рабочих станций (Service Control Manager работает как RPC-сервер).
- Права полного доступа к удаленному реестру рабочих станций.
- Доступ к серверу БД EndpointController.
- Полные права доступа к БД EndpointController (создание баз данных/ таблиц/…; чтение/запись/…).

Для работы с административной консолью учетной записи нужны следующие права и возможности:

- Права локального администратора на компьютере, на котором запускается консоль.
- Доступ к серверу БД EndpointController.
- Полные права доступа к БД EndpointController (создание баз данных/ таблиц/…; чтение/запись/…).
- Доступ к серверу DataCenter (TCP/IP, порт 9094).

Для работы с клиентскими приложениями учетной записи требуются следующие права:

- Доступ к БД EndpointController.
- Доступ к серверу индексации Search Server (TCP/IP, порт 8953).

Прочие требования:

- Агенты на клиентских компьютерах должны иметь доступ к серверу EndpointController по протоколам HTTP/HTTPS под учетной записью LocalSystem (т.к. агент выполняется в качестве службы).
- Агенты на клиентских компьютерах должны иметь доступ к сетевым ресурсам общего доступа сервера EndpointController под учетной записью LocalSystem (т.к. установка агента выполняется из службы, которую на агентский компьютер устанавливает сервер).
- Сервер EndpointController должен иметь доступ к клиентским компьютерам по протоколу RPC. Порты для RPC должны быть открыты, службы RPC запущены.
- Для работы режимов LiveView и LiveSound, на рабочих станциях с установленными агентами должны быть открыты TCP порты 18999 и 18998 соответственно (номера портов, заданные по умолчанию, можно изменить в настройках).

Выполняемые на PC процессы должны быть добавлены в исключения антивирусов и файерволов, чтобы обеспечить работоспособность последних. Перечень данных процессов приведен в Таблица 15.

Таблица 15 – Процессы, запускаемые на PC пользователя

Приложение	Примечания
SIFilterSvc.exe[9]	Агент. Выполняется как служба (SIFilterSvc) под LocalSystem. Передает данные на сервер по HTTP-протоколу (порт может меняться в настройках, по умолчанию - 80).
SIHost.exe (SIHost64.exe)	Агент сессии пользовательской консоли. Ведет перехват.
SIAMSUpdateSvc.exe	Модуль установки агентов. Выполняемый модуль находится на сервере и не копируется на рабочую станцию. В строку запуска сервиса SIAMSUpdateSvc прописывается сетевой путь на разделяемый ресурс сервера. На рабочей станции запускается под именем службы SIReminstaller и устанавливает либо удаляет агента в зависимости от заданных параметров.
SIFilterSvc_manager.exe	Модуль разбора перехваченных сетевых пакетов непосредственно на агентах, а не на сервере. Задействуется в случае активации опции «Парсить данные на агенте».
SIFiltersvc_search.exe	Модуль, используемый для анализа данных FileAuditor-ом. Позволяет выяснить соответствуют ли файлы настроенным правилам, после чего осуществить их перехват.

Выделяется три варианта установки агентов EndpointController:

1. **Сервер находится в том же домене, что и пользователи.**

   Установка сервера EndpointController производится в обычном порядке.

2. **Сервер находится в одном домене, пользователи – в другом.**

   Требования, предъявляемые к установке:

   - Настроить передачу зон DNS между доменами в обе стороны.
   - При синхронизации через Active Directory задать описание доменов на консоли администрирования EndpointController в «Настройках программы…» на вкладке «Домены», либо выбрать нужные из DataCenter.
   - Указать логин и пароль учетной записи для домена, которая имеет права локального администратора и право на вход в качестве службы в домене

[9] Название службы может быть переименовано в настройках EndpointController.

с контролируемыми PC (Консоль администрирования EndpointController: вкладка «Сетевое окружение» в левой части консоли → выбрать домен → вкладка «Настройки» → «Подключиться как..» в правой части консоли).

- Выбрать параметр «Смешанный режим» в консоли администрирования в «Настройках программы…» на вкладке «Настройки сервера» → «Установка агентов».

3. Сервер находится не в домене, пользователи – в домене.

Требования, предъявляемые к установке:

- Прописать в DNS домена сервер, на котором будет установлен EndpointController.
- Задать описание доменов на консоли администрирования EndpointController в «Настройках программы…» на вкладке «Настройки сервера» → «Синхронизация» → «Домены».
- Указать логин и пароль учетной записи для домена, которая имеет права локального администратора и вход в качестве службы в домене с контролируемыми компьютерами (Консоль администрирования EndpointController: вкладка «Сетевое окружение» в левой части консоли → выбрать домен → в правой части консоли вкладка «Настройки» → вкладка «Общее» → опция «Подключиться как»).
- Выбрать параметр «Смешанный режим» в консоли администрирования в «Настройках программы…» на вкладке «Настройки сервера» → «Установка агентов».

4.3.3 Учетная запись для запуска служб Search Server без модуля «Индексация Рабочих Станций»

Необходимы следующие права и возможности:

- Права локального администратора на сервере индексации Search Server.
- Право закрепления страниц в памяти (эти права должны быть заданы на уровне доменных политик, если они перекрывают локальные).
- Доступ к серверам БД источников данных.
- Права на чтение в БД источников данных.

Для работы с административной консолью учетной записи нужны все вышеперечисленные права, за исключением права входа в систему в качестве службы.

Для работы с клиентскими приложениями учетной записи требуются следующие права:

- Доступ к серверам БД источников данных.
- Доступ к серверу индексации Search Server (TCP/IP, порт 8953).

4.3.4 Учетная запись для запуска служб сервера AlertCenter

Нужны следующие права и возможности:

- Права локального администратора на сервере AlertCenter.
- Доступ к серверу БД AlertCenter.
- Полные права доступа к БД AlertCenter (создание баз данных/таблиц/…; чтение/запись/…). База должна быть установлена в режиме смешанной аутентификации пользователей.
- Доступ к серверу индексации Search Server (TCP/IP, порт 8953).

Для работы с административной консолью учетной записи нужны следующие права и возможности:

- Права локального администратора на компьютере, на котором запускается консоль.
- Доступ к серверу БД AlertCenter.
- Полные права доступа к БД AlertCenter (создание баз данных/таблиц/…; чтение/запись/…). База должна быть установлена в режиме смешанной аутентификации пользователей.
- Доступ к серверу индексации Search Server (TCP/IP, порт 8953).
- Доступ к серверу DataCenter (TCP/IP, порт 9094/9096).

Для работы с клиентскими приложениями учетной записи требуются следующие права:

- Доступ к серверу БД AlertCenter.
- Доступ к серверу индексации Search Server (TCP/IP, порт 8953).

4.3.5 Учетная запись для запуска служб сервера DataCenter

Нужны следующие права и возможности:

- Права локального администратора на сервере DataCenter.
- Доступ к серверу БД DataCenter.

Для работы с административной консолью учетной записи нужны следующие права и возможности:

- Права локального администратора на компьютере, на котором запускается консоль.
- Доступ к серверу БД DataCenter.
- Полные права доступа к БД DataCenter (создание баз данных/таблиц/…; чтение/запись/…; …).
- Доступ к серверу DataCenter (TCP/IP, порт 9094/9096).

Права, необходимые учетной записи для запуска агента DataCenter:

- Право входа в систему в качестве службы (эти права должны быть заданы на уровне доменных политик, если они не перекрывают локальные).
- Права локального администратора на компьютере с агентом DataCenter.

- Доступ к БД и индексам продуктов.
- Доступ к серверу DataCenter (TCP/IP, порт 9094/9096).
- Доступ к серверу индексации Search Server (TCP/IP, порт 8953).

Обычно агент DataCenter запускается от той же учетной записи, что и серверы контролируемых продуктов Серчинформ ДЛП.

4.3.6 Учетная запись для запуска служб сервера ReportCenter

Нужны следующие права и возможности:

- Права локального администратора на сервере ReportCenter.
- Доступ к серверу БД ReportCenter.
- Полные права доступа к БД ReportCenter (создание баз данных/таблиц/…; чтение/запись/…).

Для работы с административной консолью учетной записи нужны следующие права и возможности:

- Права локального администратора на компьютере, на котором запускается консоль.
- Доступ к серверу БД ReportCenter.
- Полные права доступа к БД ReportCenter (создание баз данных/таблиц/…; чтение/запись/…).
- Доступ к серверу DataCenter (TCP/IP, порт 9094/9096).

Для работы с клиентскими приложениями учетной записи требуются следующие права:

- Доступ к БД ReportCenter.

4.4 Установка и конфигурация СУБД Microsoft SQL Server

Для управления базой перехваченных документов в сети должен быть установлен сервер баз данных под управлением СУБД Microsoft SQL Server версий 2008R2 / 2012 / 2014 / 2016 / 2019.

СУБД должна поддерживать внутреннюю аутентификацию пользователей. Для этого СУБД должна быть установлена в режиме смешанной аутентификации пользователей (mixed mode).

При нехватке RAM рекомендуется ограничить объём памяти, потребляемой Microsoft SQL Server. Настройка производится в консоли MS SQL Server Management Studio (см. Рисунок 4.1).

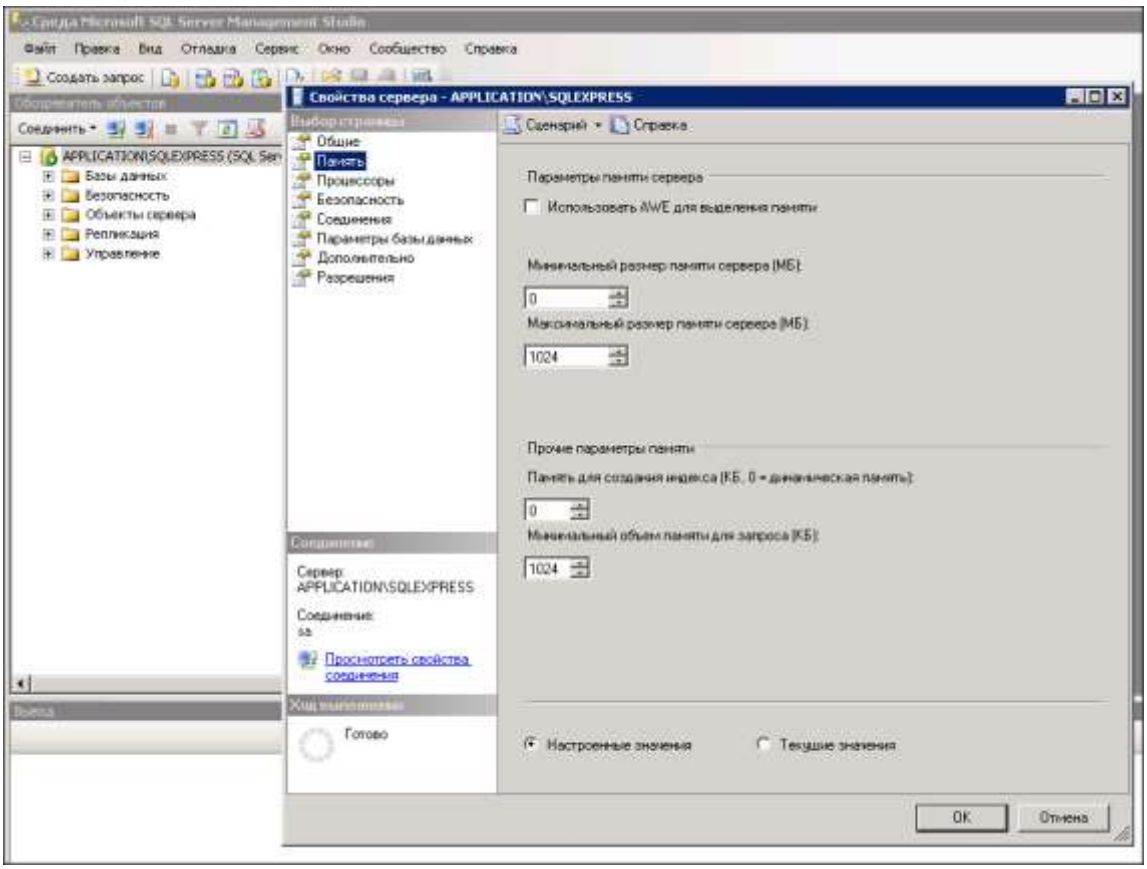


Рисунок 4.1

Помимо этого, на сервере SQL должна быть произведена настройка выбора простой модели восстановления для вновь создаваемых баз данных (см. Рисунок 4.2):

Базы данных → Системные базы данных → model → Свойства → Параметры.

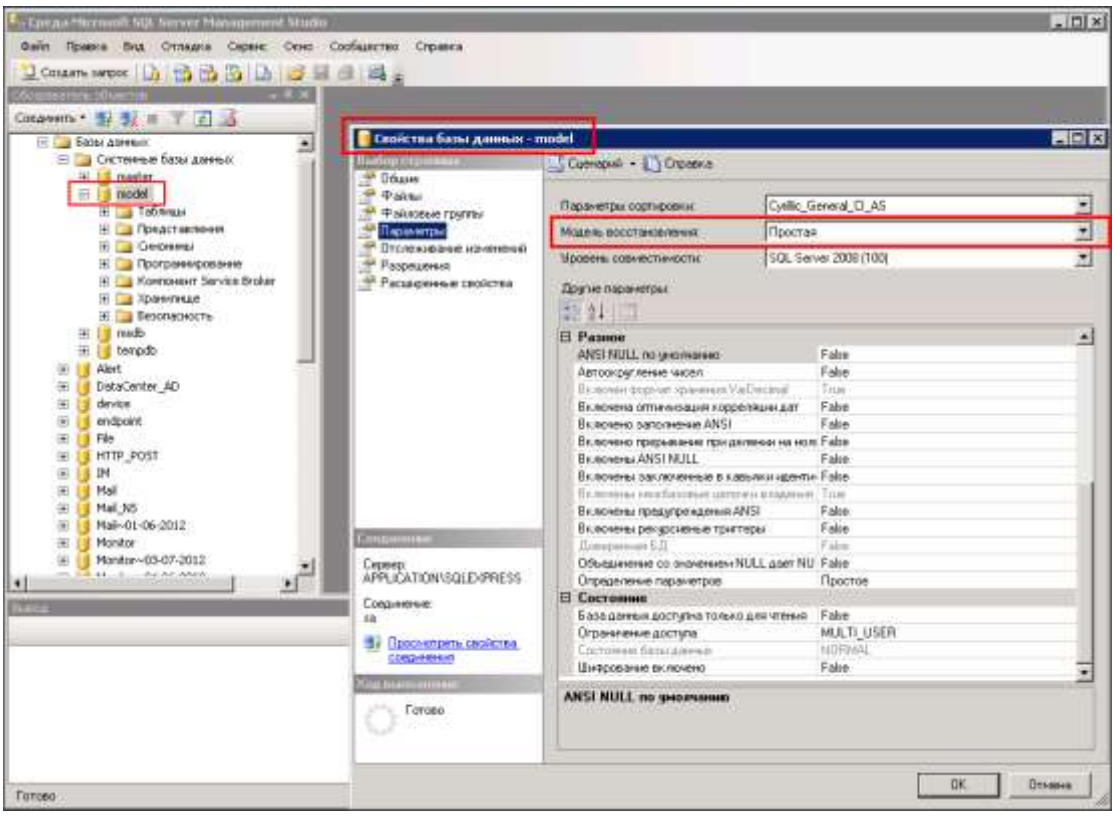


Рисунок 4.2

Также на сервере MS SQL для параметров сортировки должен быть задан CaseInsensitive Collation. В противном случае Серчинформ ДЛП не сможет корректно работать.

Пример. *Можно настроить Cyrillic_General_CI_AS, Latvian_CI_AI, любой с атрибутом CaseInsensitive (в названии Collation должен быть _CI). Важно, чтобы было именно _CI (caseinsensitive), а не _CS (casesensitive). Иначе (в случае _CS) даже названия таблиц латинскими символами считаются разными, если они отличаются только кейсом, например «T»<>«t».*

4.5 Настройка сетевых адаптеров сервера NetworkController

При использовании серверного приложения Серчинформ NetworkController на предварительном этапе необходимо обеспечить наличие на сервере как минимум двух сетевых адаптеров. Один будет использоваться для обычного приема и передачи данных, управления перехватом и хранения настроек Серчинформ ДЛП, второй – для зеркалирования сетевого трафика.

Для сетевого адаптера, используемого для зеркалирования сетевого трафика, необходимо отключить все функции, относящиеся к транспортному уровню, оставив только канальный уровень. Это связано с тем, что адаптер будет использоваться исключительно для забора передаваемых данных (см. Рисунок 4.3).

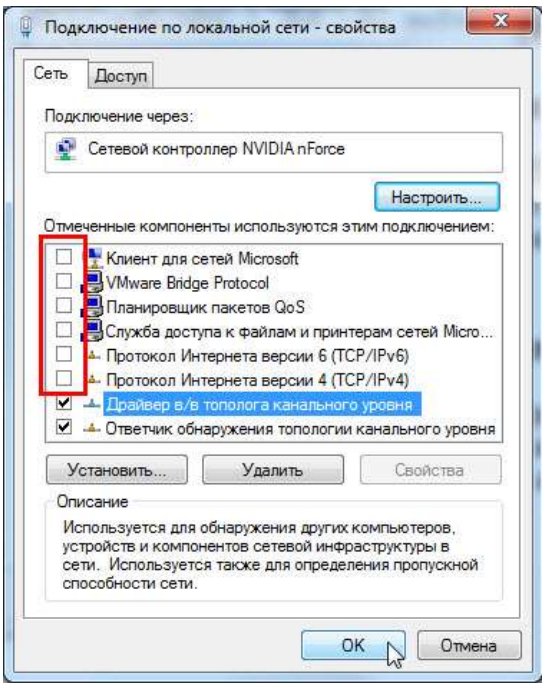


Рисунок 4.3

Для предотвращения потери пакетов в настройках сетевых карт опция «**Offload TCP segmentation**» и/или аналогичные ей параметры должны быть отключены (см. Рисунок 4.4).

Рисунок 4.4

Перечень «offload»-параметров может меняться в зависимости от производителя сетевой карты. В этом случае следует отключать все опции, в наименовании которых встречаются слова «offload» (разгрузка) и «segmentation».

В настройках некоторых сетевых адаптеров данное свойство может отсутствовать.

Вызовите свойства сетевого соединения из контекстного меню и щелкните кнопку «Настроить». Перейдите на вкладку «Дополнительно» для просмотра доступных свойств сетевого адаптера.

Для отключения параметра установите значение «Disable» или «None» (см. Рисунок 4.5).

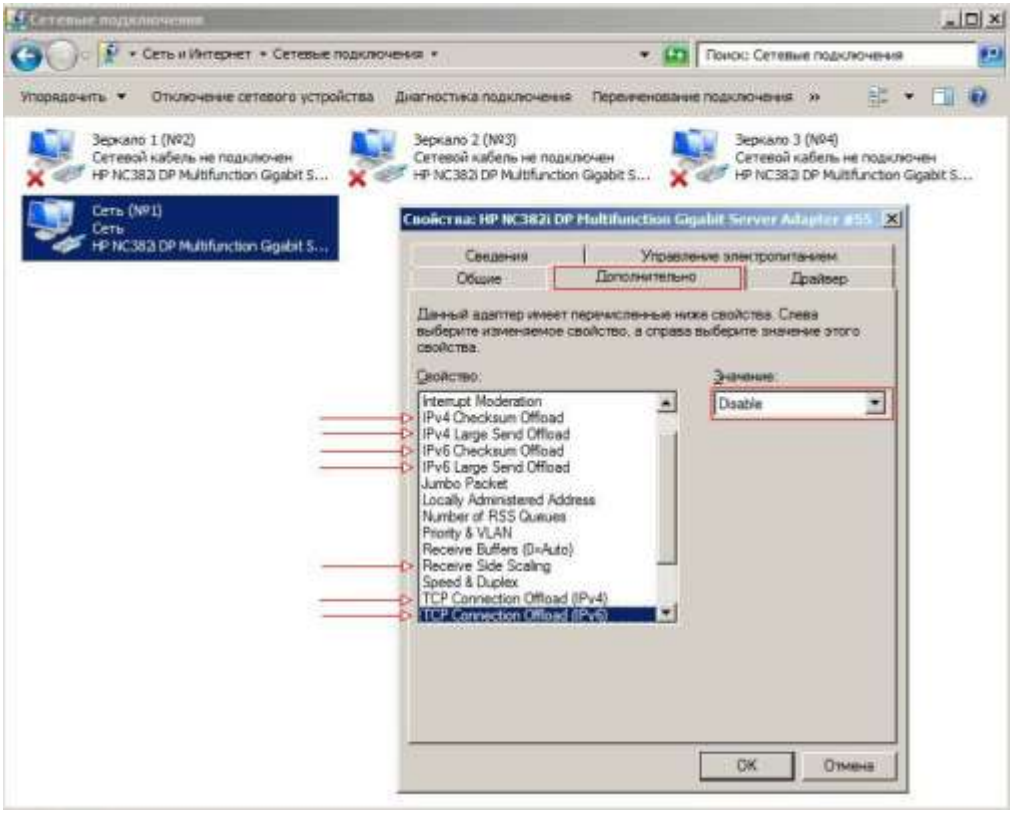


Рисунок 4.5

При наличии виртуальной сетевой карты необходимо отключать данные функции как на физической карте, так и на виртуальной.

Receive Side Scaling (RSS) – технология, которая равномерно распределяет нагрузку по обработке сетевых пакетов между ядрами процессора, позволяя оптимизировать производительность. Ее также рекомендуется отключать.

После произведенных настроек следует перезапустить сетевое соединение.

В настройках **VMware ESX/ESXi Server** данный параметр обозначен как «**LRO**» (Large Receive Offload). Соответственно, отключать нужно все опции, в наименовании которых встречается аббревиатура «LRO» (см. Рисунок 4.6).

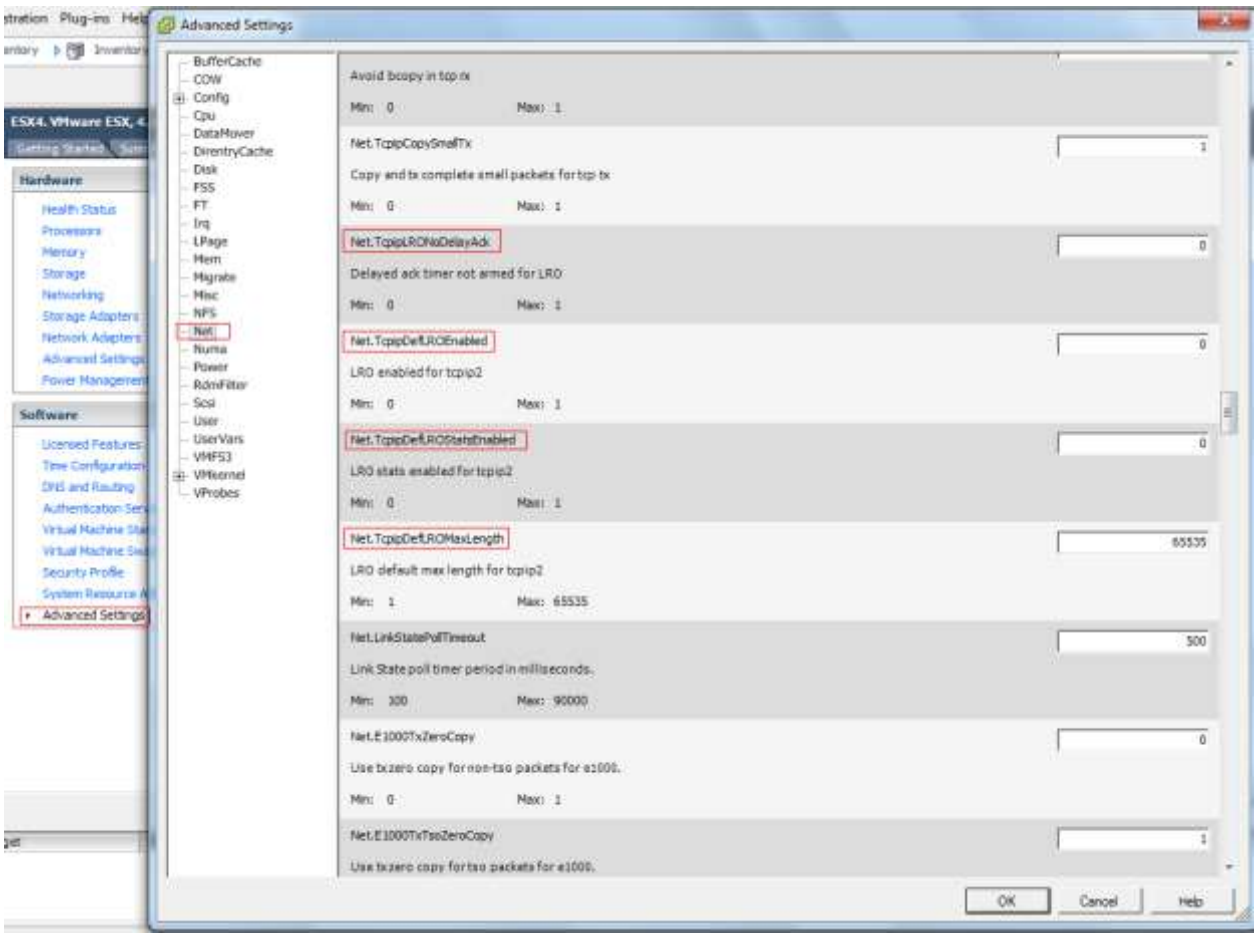


Рисунок 4.6

4.6 Создание учетной записи

Для установки и запуска компонентов «Серчинформ ДЛП» необходима учетная запись, обладающая определенными правами. Рекомендуется выделить учетную запись с правами администратора домена и добавить эту учётную запись в следующие групповые политики:

- Вход в качестве службы;
- Создание журналов безопасности;
- Управление аудитом и журналом безопасности.

4.6.1 Настройка прав входа в качестве службы

Настройка прав входа пользователей в качестве службы производится на контроллере домена.

Последовательность действий (для Windows Server 2012):

Меню (экран) «Пуск» → Администрирование (см. Рисунок 4.7)

Рисунок 4.7

Вызовите с помощью ярлыка консоль «Управление групповой политикой» (см. Рисунок 4.8).

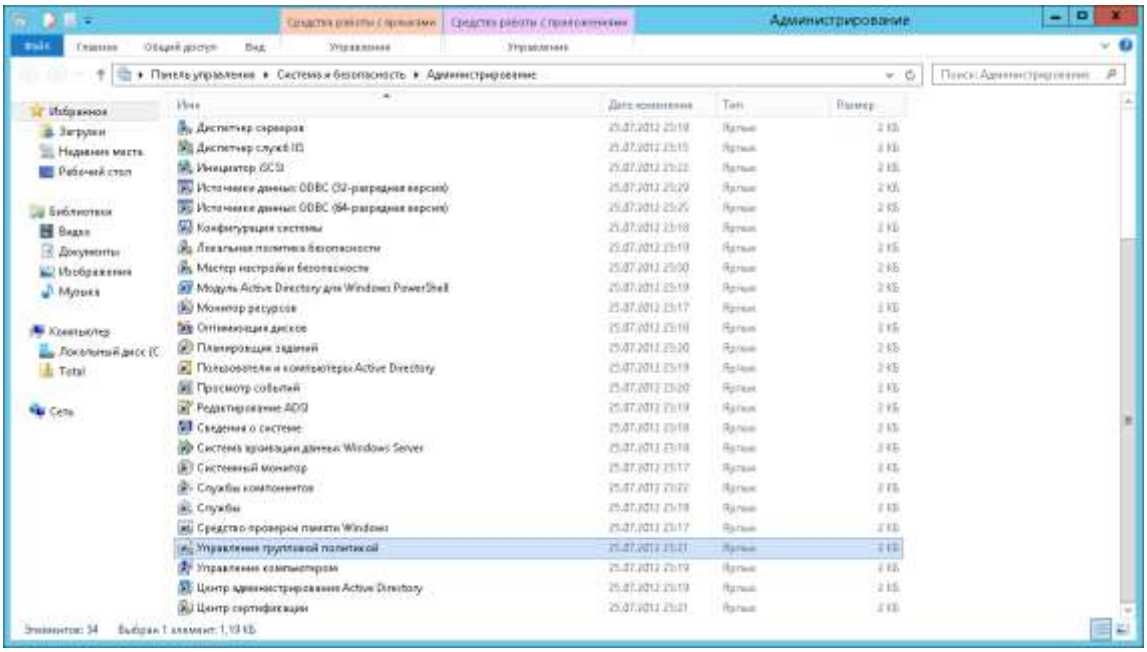


Рисунок 4.8

Двойным щелчком раскройте позицию «Лес» → «Домены». Разверните Ваш домен.

Перейдите в пункт «Default Domain Policy» и с помощью контекстного меню выберите команду «Изменить» (см. Рисунок 4.9).

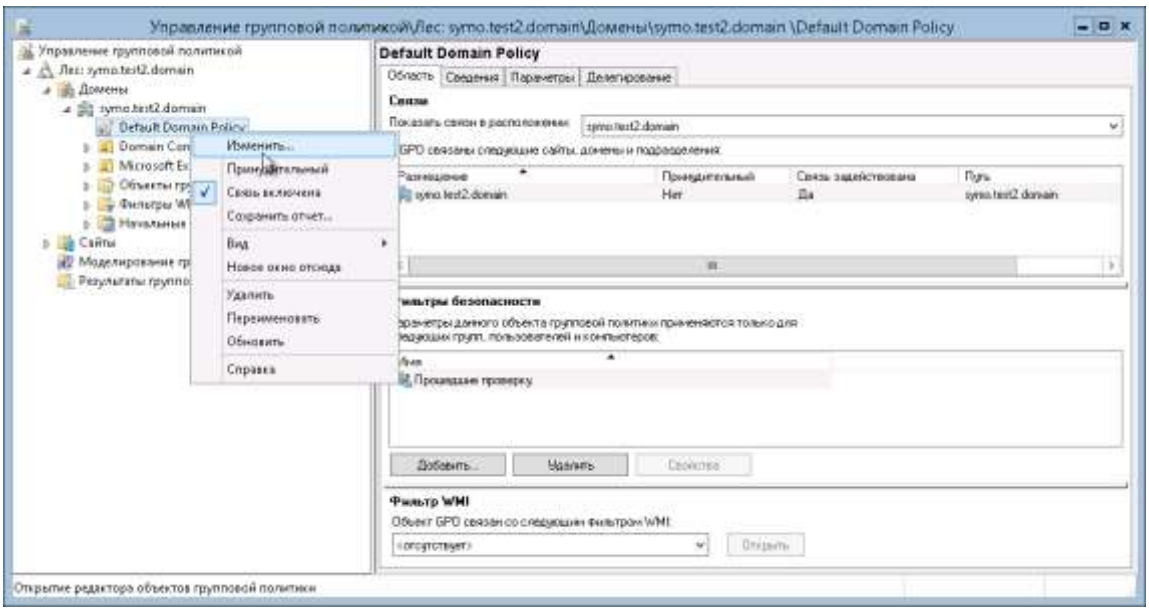


Рисунок 4.9

Разверните «Конфигурация компьютера» → «Политики» → «Конфигурация Windows» → «Параметры безопасности» → «Локальные политики».

Выберите пункт «Назначение прав пользователя» (см. Рисунок 4.10).

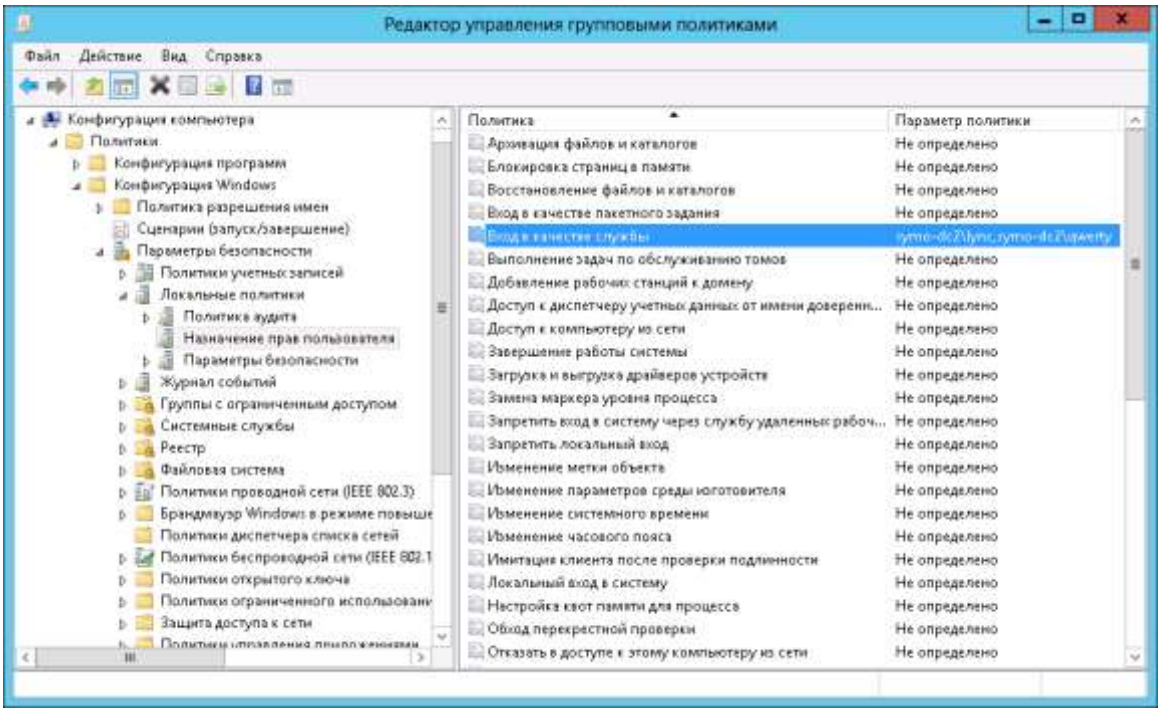


Рисунок 4.10

В правой панели выберите «Вход в качестве службы». Вызовите окно свойств с помощью контекстного меню, в котором необходимо указать учетную запись пользователя, наделяемую правом входа в качестве службы.

Последовательность действий (для Windows Server 2008):

Меню «Пуск» → Администрирование → Управление групповой политикой (см. Рисунок 4.11).

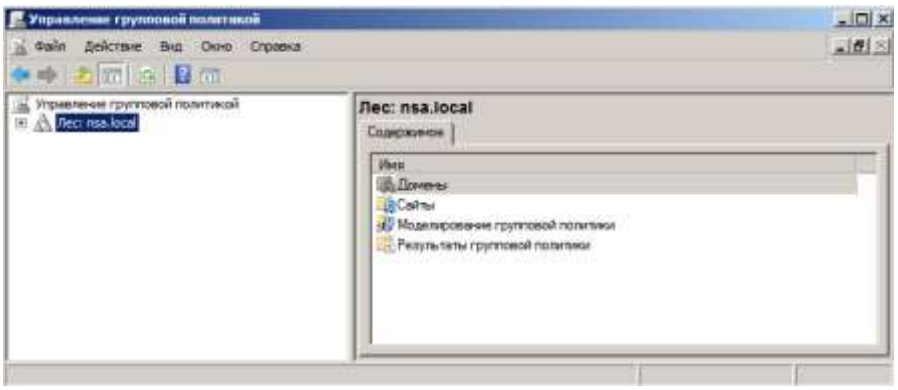


Рисунок 4.11

Двойным щелчком раскройте позицию «Лес» (см. Рисунок 4.12).

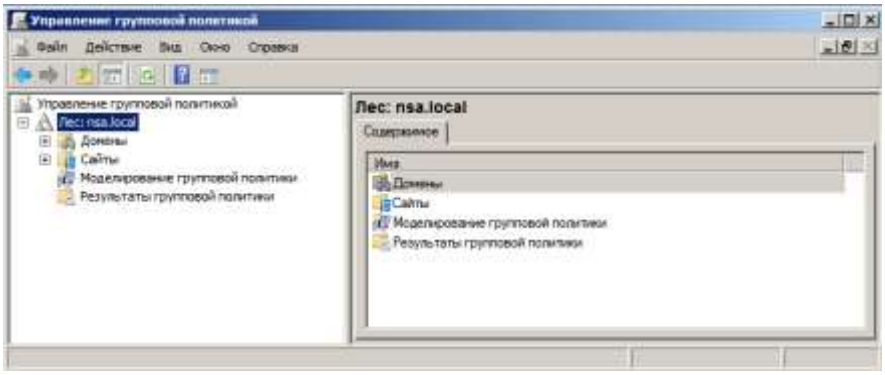


Рисунок 4.12

Перейдите в пункт Default Domain Policy и с помощью контекстного меню выберите команду «Изменить», как показывает Рисунок 4.13.

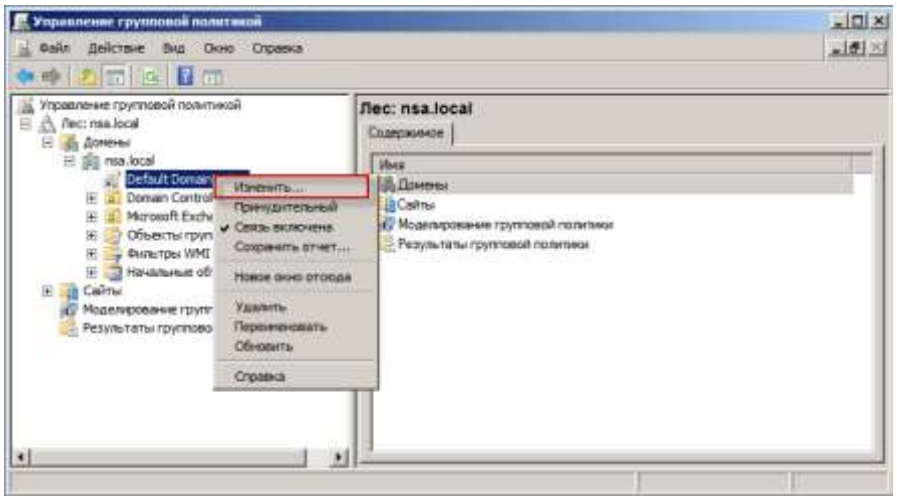


Рисунок 4.13

В открывшемся редакторе управления групповыми политиками перейдите в пункт «Назначение прав пользователя» и в правой панели щёлкните «Вход в качестве службы» (см. Рисунок 4.14).

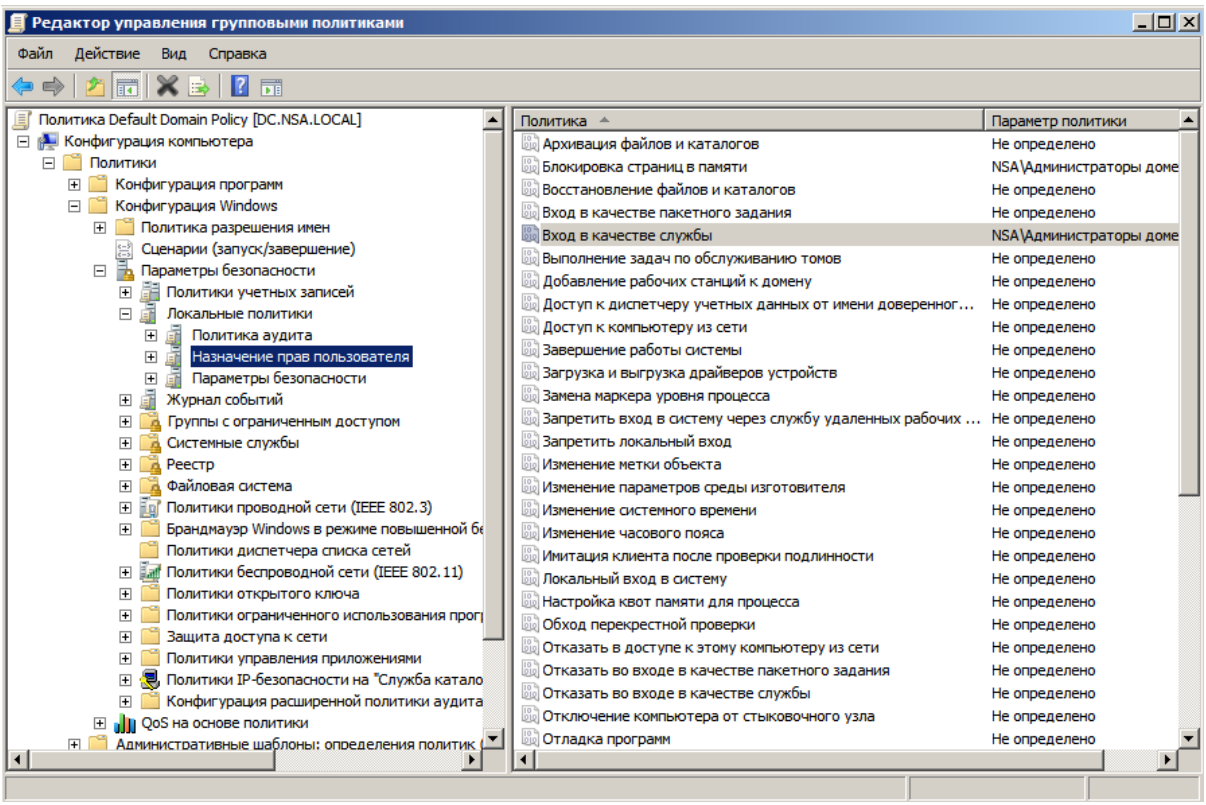


Рисунок 4.14

В открывшемся окне выберите пользователя или группу, которым необходимо предоставить право входа в качестве службы, и примените изменения.

Указанного пользователя необходимо также добавить в политику «Блокировка страниц в памяти», находящейся в том же разделе оснастки «Политика безопасности» (см. Рисунок 4.15). Добавление пользователя, под учётной записью которого работает сервер индексации, в данную политику необходимо для включения режима AWE, позволяющего хранить в памяти словарь уникальных слов. Включение режима AWE позволит значительно ускорить индексацию больших объёмов данных при установленной памяти 3 ГБ и выше.

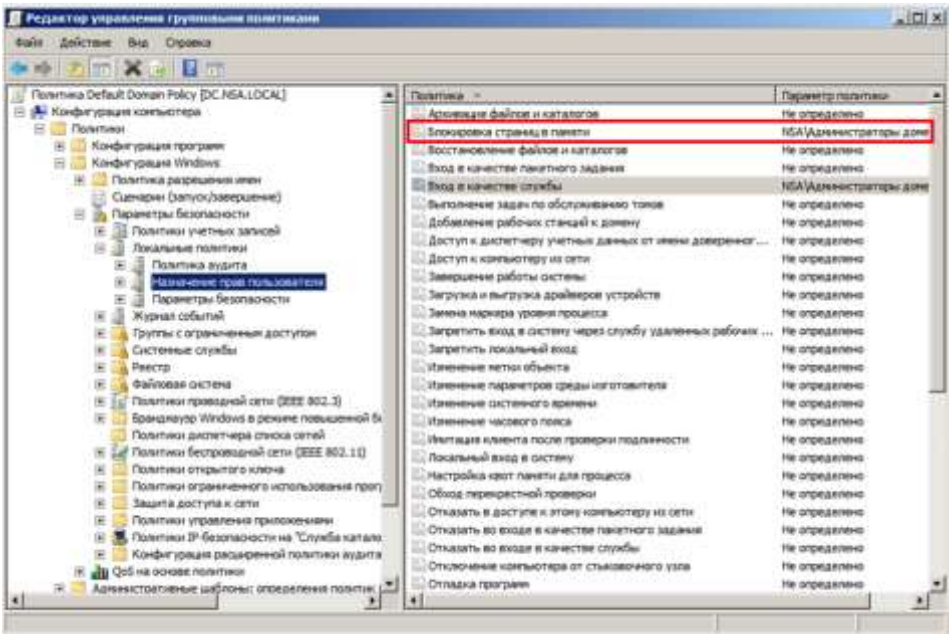


Рисунок 4.15

4.6.2 Назначение права чтения журнала безопасности

Последовательность действий для Windows Server 2008 R2:

Панель управления → Администрирование → Управление групповой политикой → Domain Controllers → Правый клик (Изменить) → Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Локальные политики → Назначение прав пользователя.

Добавьте пользователя в политику «Управление аудитом и журналом безопасности» (Manage auditing and security log) (см. Рисунок 4.16).

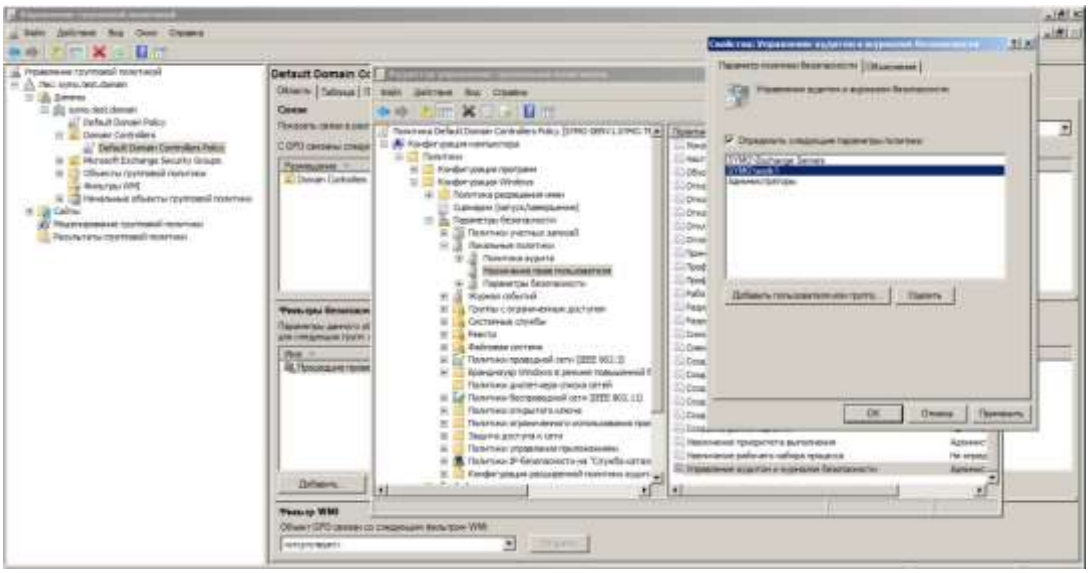


Рисунок 4.16

4.7 Отключение контроля учётных записей

Перед установкой компонентов Серчинформ ДЛП функция контроля учётных записей – UAC (User Account Control) – на сервере и клиентских рабочих станциях должна быть отключена.

Последовательность действий для Windows Server 2008:

1. Пуск → Панель управления → Учётные записи (User Accounts).
2. Щёлкните «Изменение параметров контроля учетных записей» (см. Рисунок 4.17).

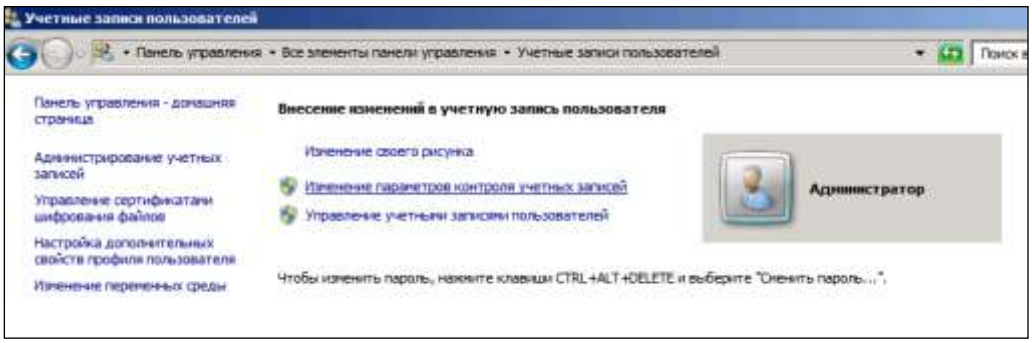


Рисунок 4.17

3. В настройке выдачи уведомлений о вносимых в компьютер изменениях опустите ползунок вниз до упора, как показано на Рисунок 4.18.

Рисунок 4.18

Контроль учётных записей будет отключен.

4.8 Поддержка русского языка в региональных настройках

Для выполнения поиска по русским текстам и корректного отображения кириллических символов системой на рабочих и серверных станциях должны быть настроены язык и региональные стандарты. При корректной настройке стандартов

система будет работать даже на нелокализованной под русский язык операционной системе.

Настройка стандартов для Windows Server 2008:

Настройки производятся в разделе «Язык и региональные стандарты» (Пуск → Панель управления).

а) Вкладка «Форматы». Выберите значение «Русский (Россия)» в качестве текущего формата (см. Рисунок 4.19).

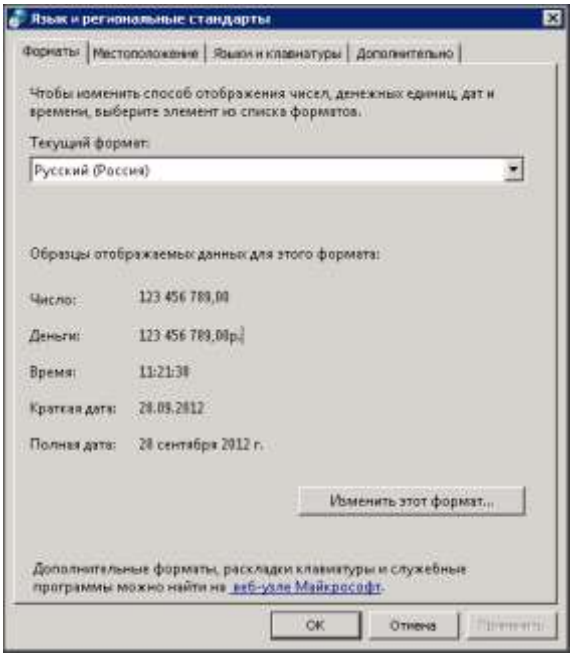


Рисунок 4.19

б) Вкладка «Местоположение». Выберите значение «Россия» в качестве текущего местоположения (см. Рисунок 4.20).

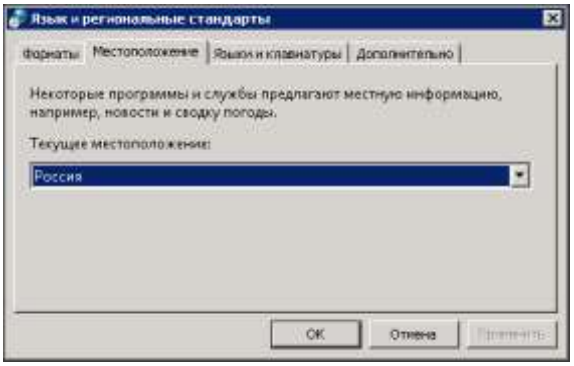


Рисунок 4.20

в) Вкладка «Языки и клавиатуры». Добавьте русский язык, если он отсутствует. Для этого в группе «Язык интерфейса» воспользуйтесь кнопкой «Установить или удалить язык…» и выберите язык (см. Рисунок 4.21).

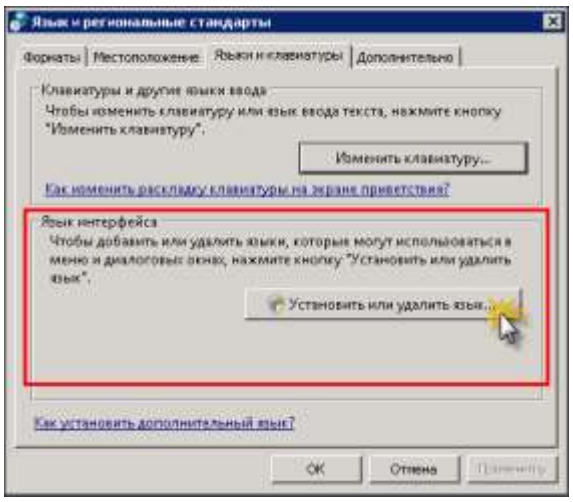


Рисунок 4.21

г) Вкладка «Дополнительно». В качестве текущего языка программ, не поддерживающих Юникод, должен стоять «Русский (Россия)» (см. Рисунок 4.22).

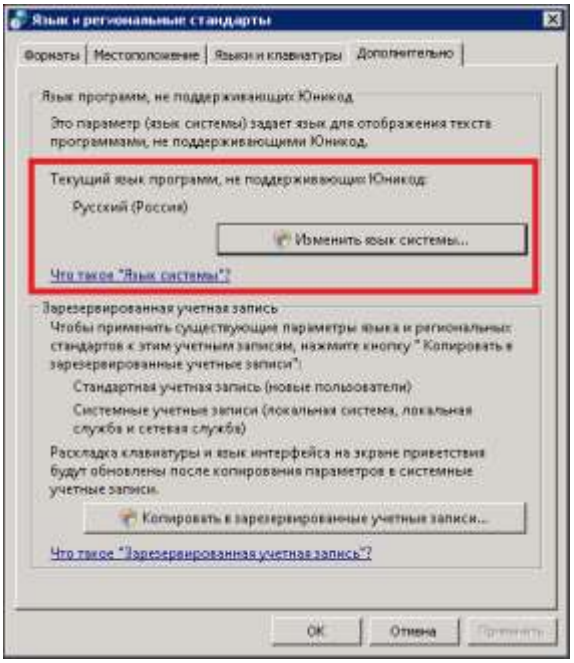


Рисунок 4.22

Если это не так, щёлкните по кнопке «Изменить язык системы…» и в открывшемся окне выберите значение «Русский (Россия)» (см. Рисунок 4.23).

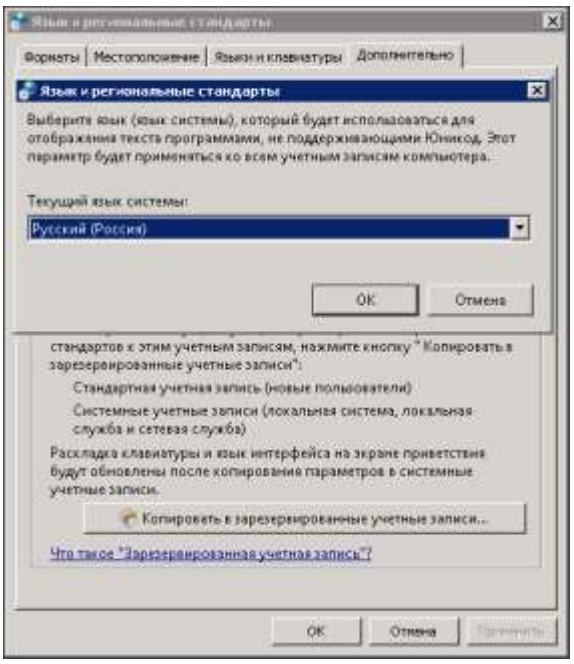


Рисунок 4.23

д) Вкладка «Дополнительно». Щёлкните по кнопке «Копировать в зарезервированные учетные записи…» и в открывшемся окне установите флажки «Стандартная учётная запись» и «Системные учётные записи» (см. Рисунок 4.24).

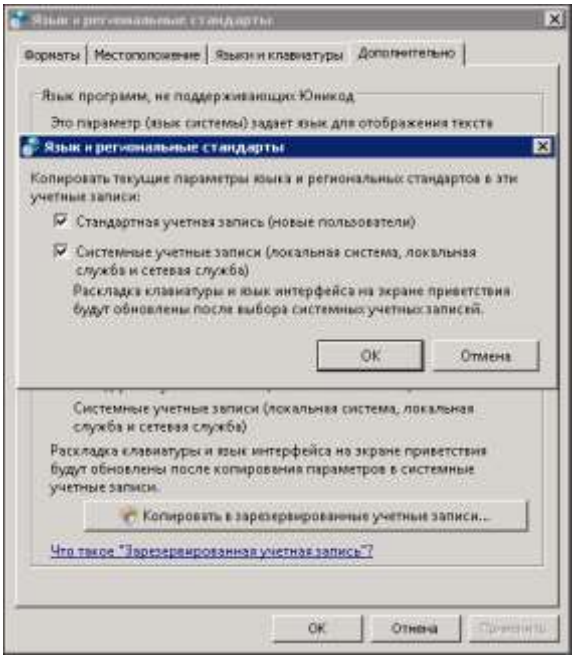


Рисунок 4.24

4.9 Настройка рабочих станций

Для установки агента на рабочие станции необходимо достижение двух условий:

1. Рабочая станция должна пинговаться;

2. На рабочей станции должна открываться системная шара admin$.

Если рабочие станции находятся в домене, все действия, производимые в консоли EndpointController, осуществляются по полному доменному имени. Соответственно проверки по пунктам 1 и 2 также должны производиться по полному имени рабочей станции.

4.9.1 Настройка брандмауэра Windows

Для достижения вышеприведенных условий в брандмауэре Windows должны быть либо отключены все профили, либо созданы два правила для входящих соединений:

1. Правило настраиваемого типа → Все программы → Тип протокола: ICMPv4;
2. Правило для порта → Протокол TCP, определенный локальный порт: 445.

4.9.2 Доступ к системным шарам на рабочей станции

Для доступа к системным шарам на рабочей станции должна быть запущена служба «Сервер».

В случае недоступности системной шары на компьютере, находящемся в составе рабочей группы, следует на этом компьютере в ветку реестра

`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]`

добавить

параметр `LocalAccountTokenFilterPolicy`,

тип: `DWORD`,

значение: `1`.

4.9.3 Службы

Для корректной установки агентов на рабочих станциях пользователей должны быть запущены следующие службы:

- Удаленный вызов процедур (RPC);
- Служба доступа к файлам и принтерам сетей Microsoft.

Для установки агентов индексации рабочих станций необходим также доступ к службе «Удаленный реестр».

Последовательность действий для Windows 7:

1) Меню «Пуск» → Панель управления → Система и безопасность → Администрирование → Службы.
2) Проверьте состояние служб «Удаленный вызов процедур (RPC)» и «Удаленный реестр» (см. Рисунок 4.25). Запустите их в случае необходимости.

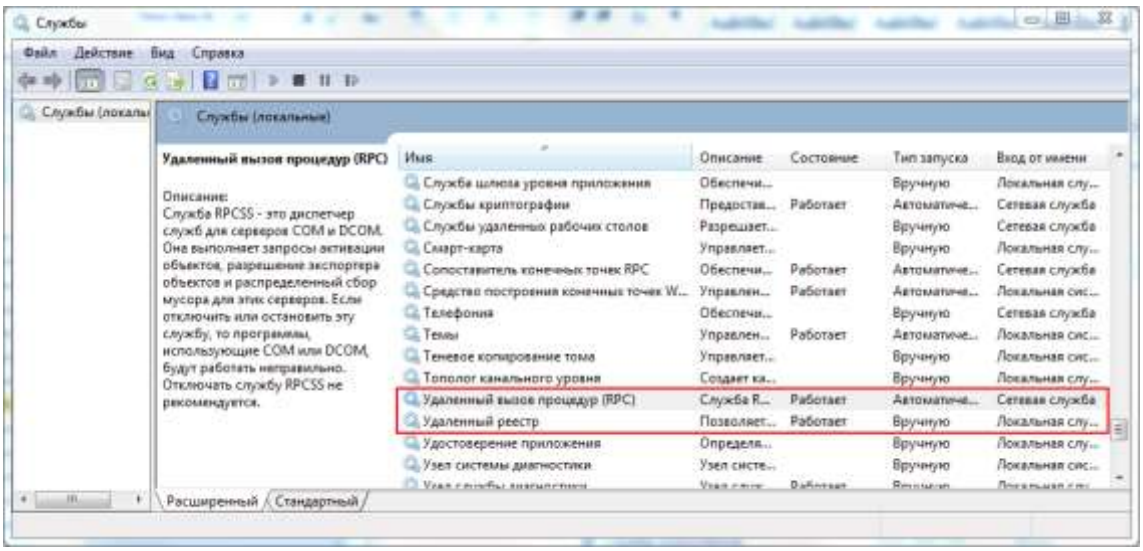


Рисунок 4.25

3) Меню «Пуск» → Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Подключение по локальной сети → Свойства.
4) Отметьте флажком «Служба доступа к файлам и принтерам сетей Microsoft» (см. Рисунок 4.26).

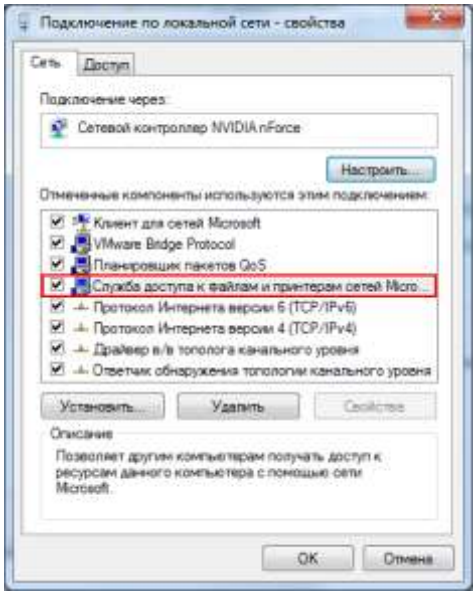


Рисунок 4.26

4.10 Размер индексов и баз данных

При разрастании индекса и базы данных замедляется доступ к данным, снижается скорость их обновления и повышается возможность ошибок. Использование нескольких индексов и баз данных среднего размера вместо одного источника данных большого размера позволит оптимизировать аналитическую обработку перехваченной информации.

Поэтому рекомендуется создавать новый индекс или базу данных по достижении любого из следующих параметров:

- размер индекса/базы данных – 8 Гигабайт;
- размер проиндексированного текста – 20 Гигабайт;
- количество проиндексированных документов – 10 миллионов;
- число уникальных слов – 10 миллионов.

5 РАЗВЁРТЫВАНИЕ СИСТЕМЫ

Развёртывание и настройку Серчинформ ДЛП производят:

- инженер службы технической поддержки компании-разработчика;
- Вы как специалист по информационной безопасности.

Инженер СТП проводит предварительную настройку функций перехвата документов пользователей и поиска по ним, а именно:

- устанавливает программное обеспечение;
- настраивает перехват данных;
- настраивает базы данных, в которых хранятся перехваченные документы;
- создает поисковые индексы;
- настраивает расписание и условия создания/удаления индексов и баз данных;
- проверяет функции перехвата пользовательских документов и поиска по ним.

Перед этим Вы должны подготовить для инженера площадку, соответствующую всем требованиям компании-разработчика (описаны в разделе 4).

Окончательную настройку Системы Вы обеспечиваете самостоятельно.

Установка компонентов Серчинформ ДЛП производится в следующем порядке:

1. Серчинформ DataCenter (включая Серчинформ ReportCenter);
2. Серчинформ Search Server;
3. Серчинформ EndpointController;
4. Серчинформ NetworkController;
5. Серчинформ AlertCenter;
6. Серчинформ AnalyticConsole.

5.1 Установка сервера и агентов Серчинформ DataCenter

Запустите дистрибутив и выберите язык, используемый в процессе установки (русский или английский) (см. Рисунок 5.1).

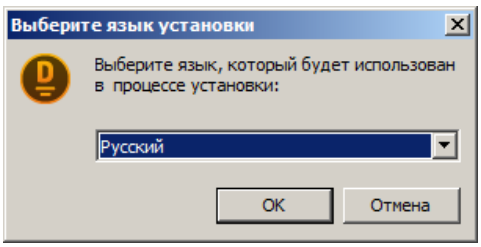


Рисунок 5.1

Нажмите «Далее» в приветственном окне Мастера установки (см. Рисунок 5.2).

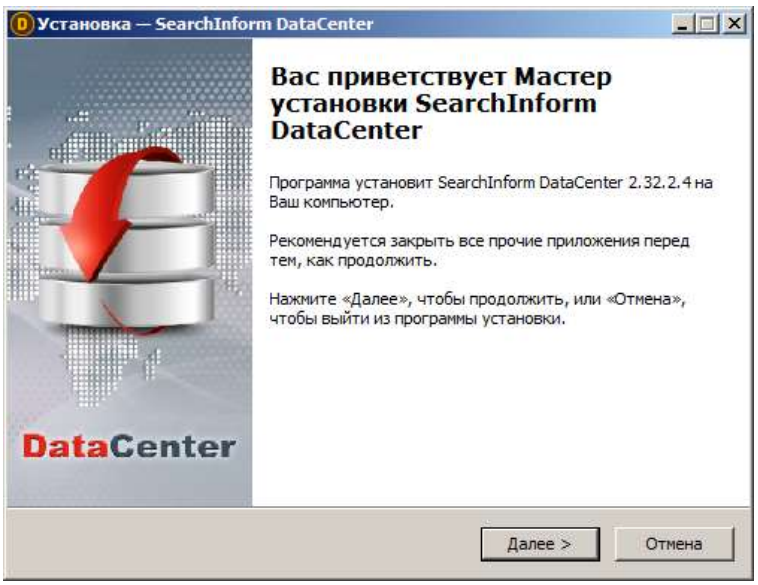


Рисунок 5.2

Примите условия лицензионного соглашения. Нажмите «Далее» (см. Рисунок 5.3).

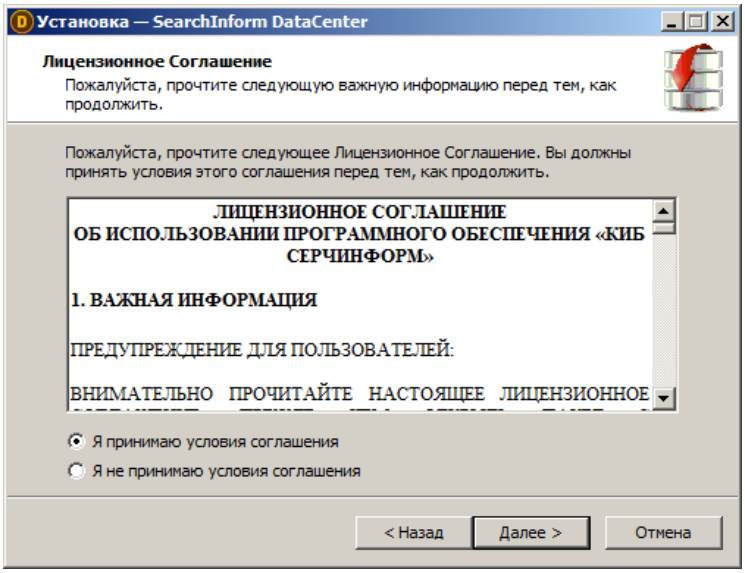


Рисунок 5.3

Выберите папку, в котоую будет произволиться установка приложения (см.Рисунок 5.4).

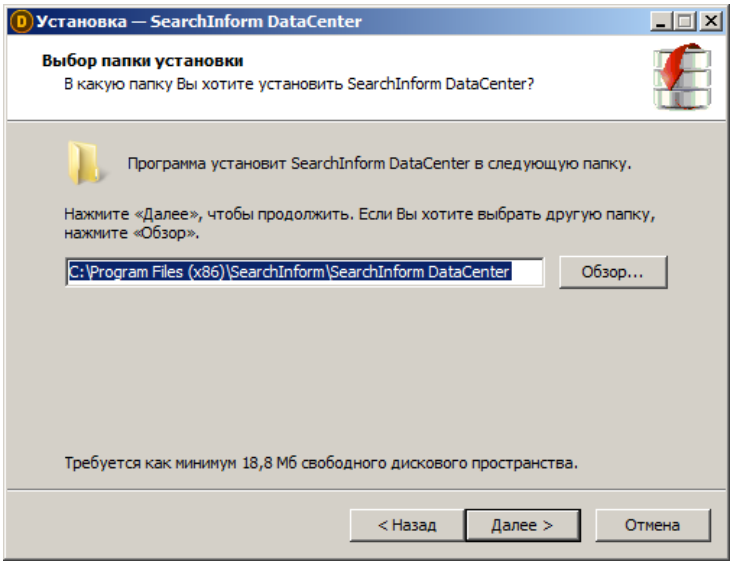


Рисунок 5.4

На следующем шаге выберите тип установки и устанавливаемые компоненты. Продукт DataCenter включает в себя следующие компоненты:

- сервер DataCenter;
- клиент DataCenter;
- агент DataCenter;
- сервер ReportCenter;
- сервер WebAnalytic;
- DataCenter API;
- DataCenter профайлинг[10].

Серверный и клиентский модуль устанавливаются на один компьютер. Агенты DataCenter устанавливаются на серверы компонентов Серчинформ ДЛП, которыми необходимо управлять.

Для установки используется один дистрибутив.

Возможные варианты установки DataCenter:

- *Серверная*. Устанавливается серверный и клиентский модуль. Установка серверной части без клиентской невозможна.
- *Агентская*. Агент устанавливается на сервер контролируемого компонента.
- *Полная*. Установка агента, серверного и клиентского модулей на один компьютер. Производится, если сервер DataCenter нужно установить совместно с контролируемыми компонентами.
- *DataCenter API.* Производится установка только API.

[10] Установка на сервер DataCenter службы компонента SearchInform ProfileCenter. Настройка серверной части доступна после установки в консоли DataCenter, просмотр профилей пользователей – в консоли аналитика.

- *ReportCenter.* Осуществляется установка компонентов, необходимых для работы сервера ReportCenter. Дополнительно может быть отмечен модуль интеграции со СКУД PERCo-S-20.
- *WebAnalytic.* Устанавливаются компоненты, необходимые для работы с отчетами ReportCenter посредством веб-интерфейса.
- *Выборочная*. Перечень устанавливаемых модулей определяется пользователем (см. Рисунок 5.5).

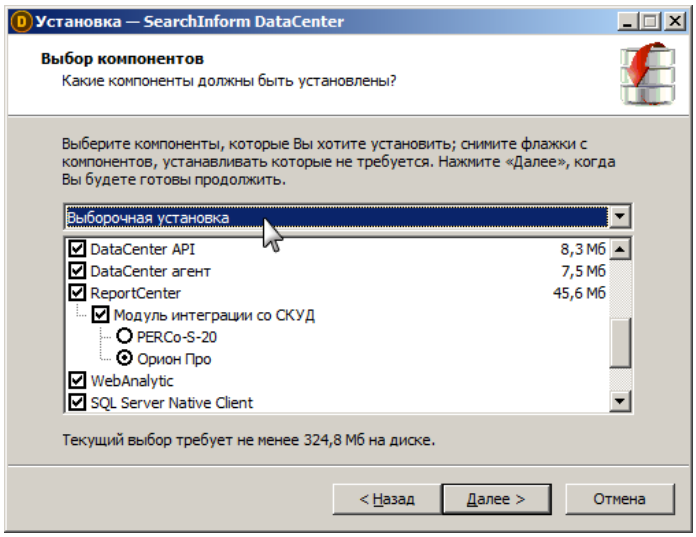


Рисунок 5.5

В случае отдельной установки агента укажите путь к серверу DataCenter (см. Рисунок 5.6). При совместной установке с сервером - укажите **localhost**.

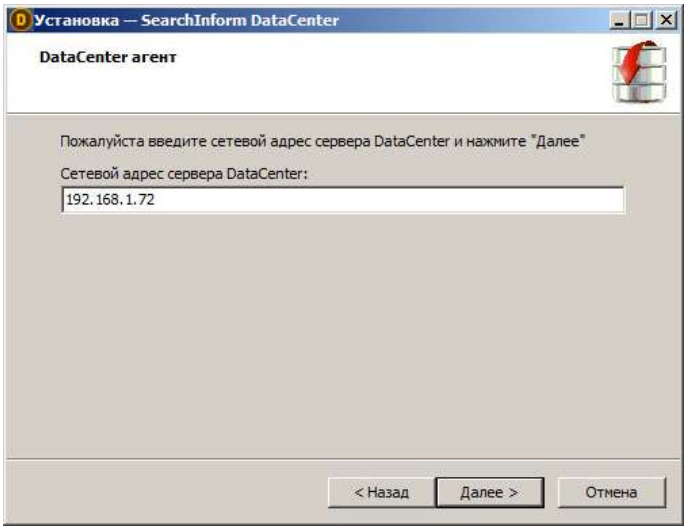


Рисунок 5.6

Создайте новую базу данных DataCenter или выберите уже существующую (см. Рисунок 5.7).

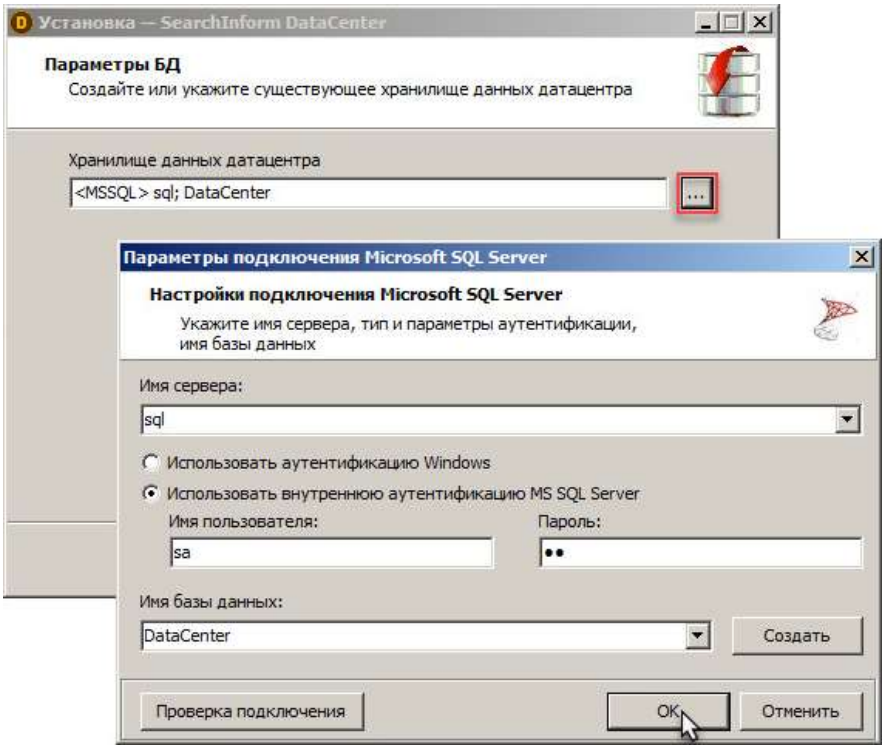


Рисунок 5.7

5.1.1 Ввод лицензии

Ввод лицензии возможен при условии, что сервер DataCenter остановлен.

Для лицензирования продукта щёлкните кнопку «Установленные лицензии» (см. Рисунок 5.8).

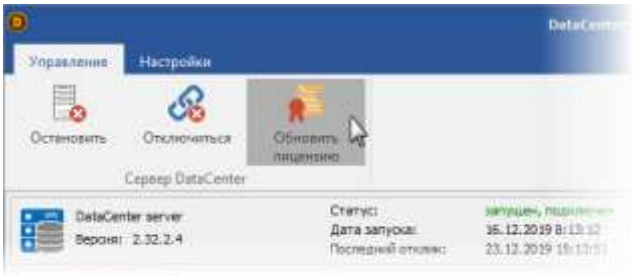


Рисунок 5.8

Будет открыто диалоговое окно «DataCenter ввод лицензии». Для получения лицензионного ключа обратитесь в службу технической поддержки компании-разработчика, указав Ваш идентификатор (выделен маркером, см. Рисунок 5.9). Идентификатор является уникальным для каждого компьютера.

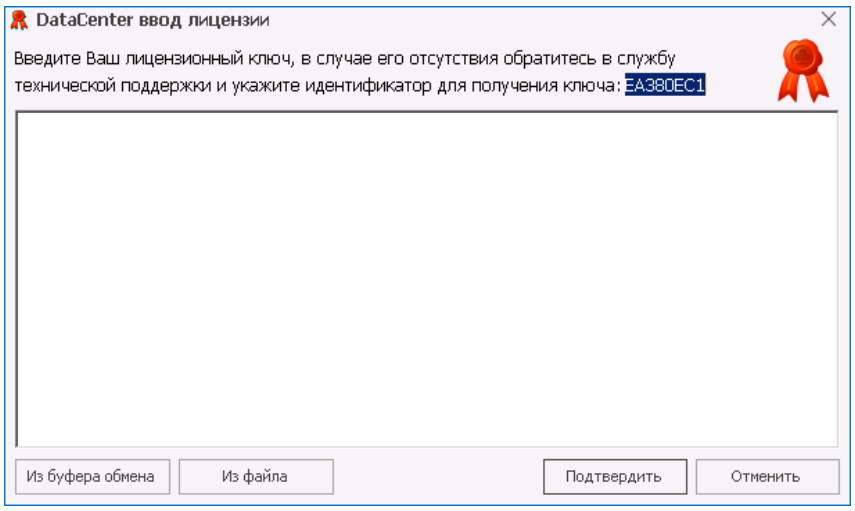


Рисунок 5.9

Вставьте полученный ключ в текстовое поле с помощью кнопки «Из буфера обмена»/«Из файла» (см. Рисунок 5.10).

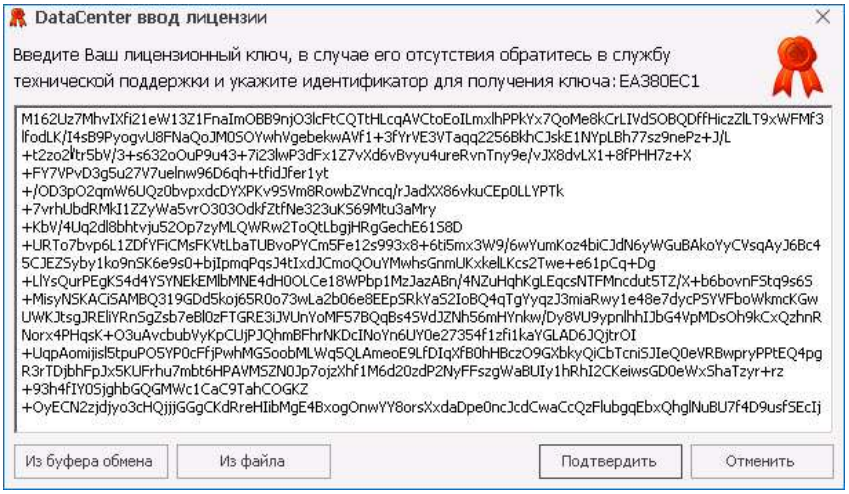


Рисунок 5.10

Для применения лицензии используется кнопка «Подтвердить», после чего будет отображено окно с перечнем установленных лицензий (см. Рисунок 5.11).

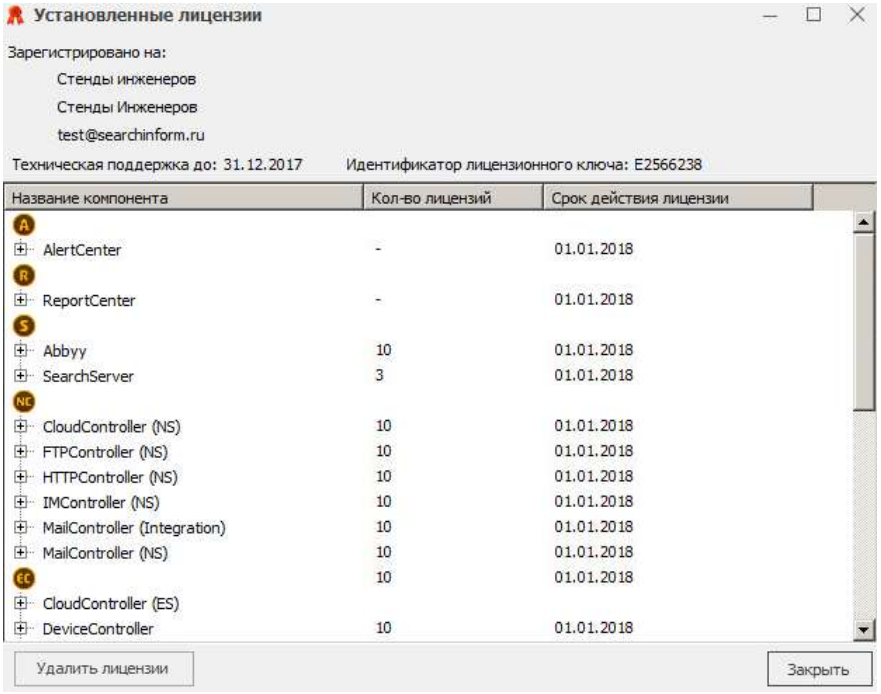


Рисунок 5.11

Для просмотра статистики и выдачи лицензий компонентам предназначена вкладка **Настройки** → **Используемые лицензии** (активна при запущенном сервере DataCenter) (см. Рисунок 5.12).

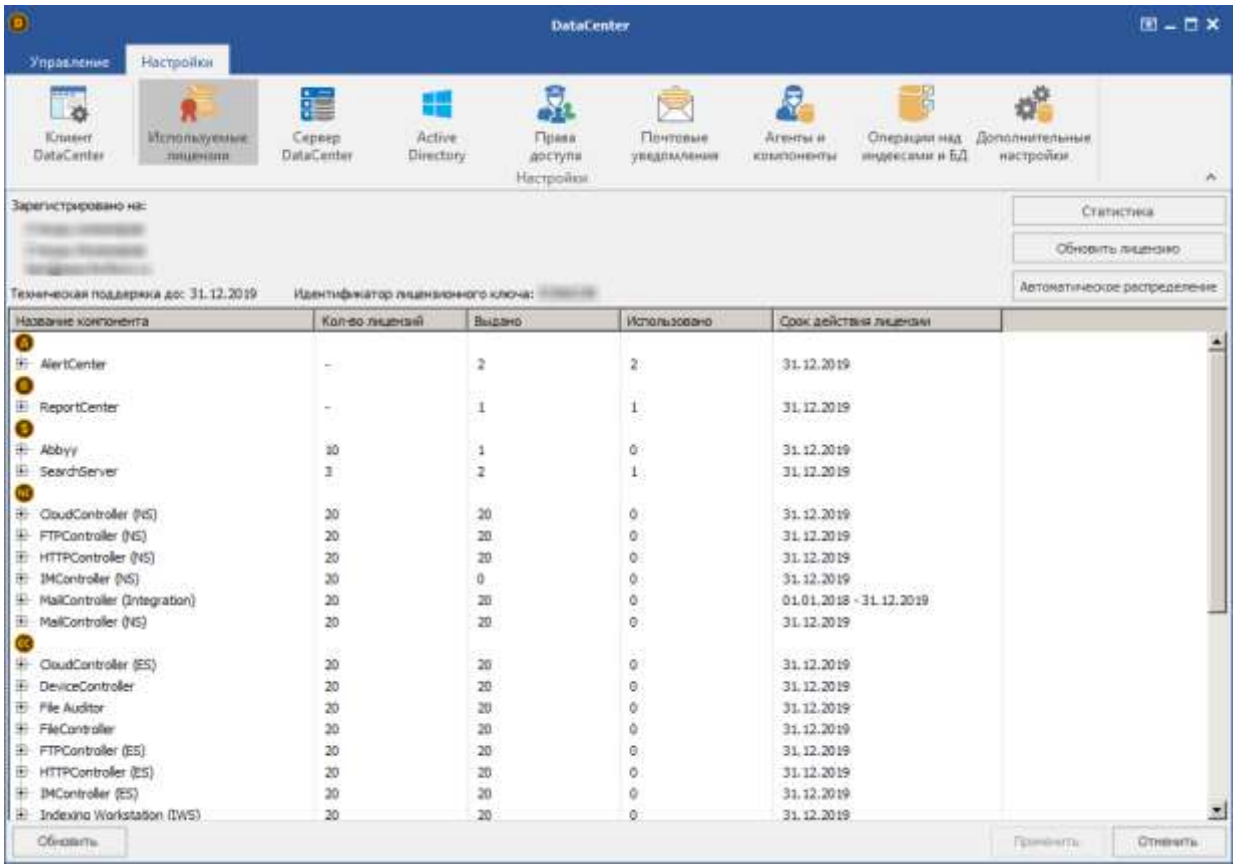


Рисунок 5.12

5.1.2 Лицензирование AlertCenter и ReportCenter

Для компонентов AlertCenter и ReportCenter в консоли DataCenter по умолчанию установлена автоматическая выдача лицензий и изменению не подлежит (окно выдачи лицензий не вызывается правой кнопкой мыши) (см. Рисунок 5.13).

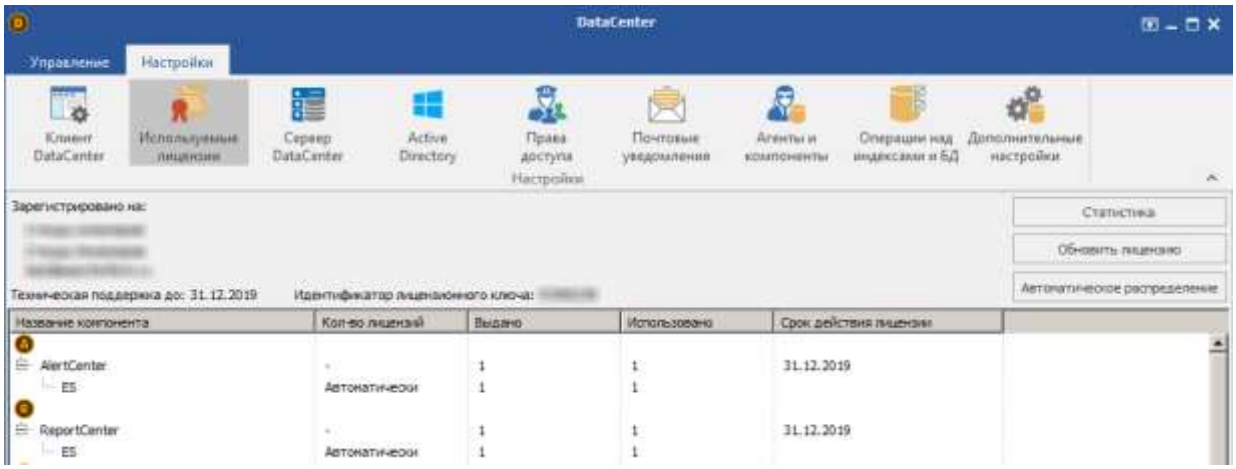


Рисунок 5.13

5.2 Установка сервера индексации Search Server

Перед началом установки убедитесь, что сервер функционирует под управлением одной из поддерживаемых ОС, обеспечено взаимодействие между компонентами системы и предоставлены достаточные права службе Search Server.

Выделяются следующие основные условия, необходимые для успешной установки Search Server в корпоративной сети компании:

а) Наличие установленного пакета FilterPacks от Microsoft для индексирования содержимого файлов определенных типов (docx, xlsx, pptx, vsd, …). Загрузка доступна по ссылке: http://www.microsoft.com/download/en/details.aspx?id=17062.
Обновления для пакета FilterPacks от Microsoft:
http://download.microsoft.com/download/6/7/8/6788CA38-7A25-4AFC-92D4-66E1C0160F57/filterpack2010sp1-kb2460041-x64-fullfile-ru-ru.exe
http://download.microsoft.com/download/E/E/9/EE96480F-1516-4A25-9950-5C682F89F963/filterpacksp2010-kb2687447-fullfile-x64-ru-ru.exe.
Устанавливаемые пакеты фильтров и обновления к ним должны соответствовать разрядности операционной системы.

б) Наличие установленного пакета iFilter от Adobe для индексирования содержимого файлов формата PDF. Загрузка доступна по ссылке:

http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Windows. Для каждой разрядности операционной системы должен иметься свой пакет.

Отсутствие вышеперечисленных пакетов на Search Server не нарушает его работоспособность. Но установка данных фильтров рекомендуется, поскольку они могут быть задействованы в случае, когда встроенная библиотека не отработала и вернула ошибку.

Установка серверного модуля Search Server производится на один выделенный под эти цели сервер.

Запустите дистрибутив Search Server.

Выберите вариант установки «Полная инсталляция» (см. Рисунок 5.14).

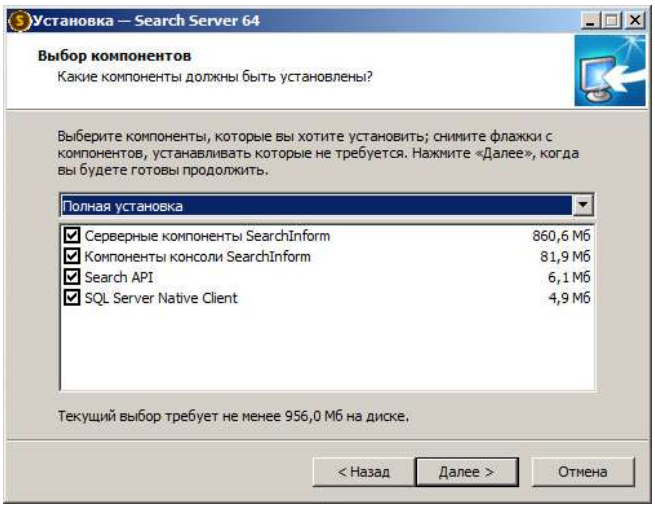


Рисунок 5.14

Настройте учётную запись, под которой будет работать сервис индексации (см. Рисунок 5.15).

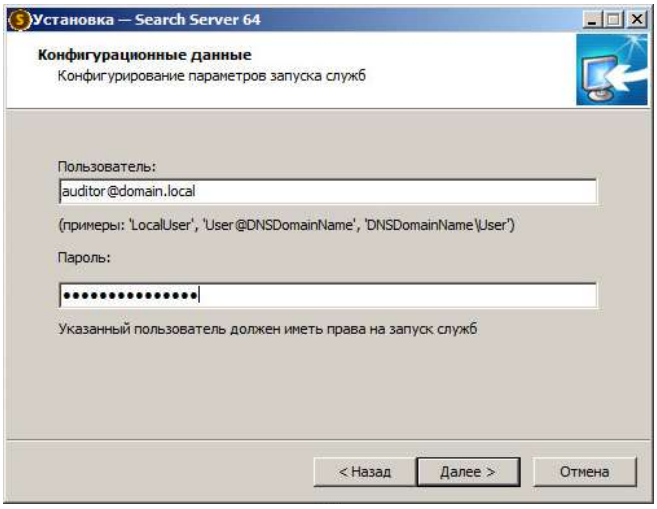


Рисунок 5.15

Выберите, для кого из пользователей будет создан ярлык на рабочем столе (см. Рисунок 5.16).

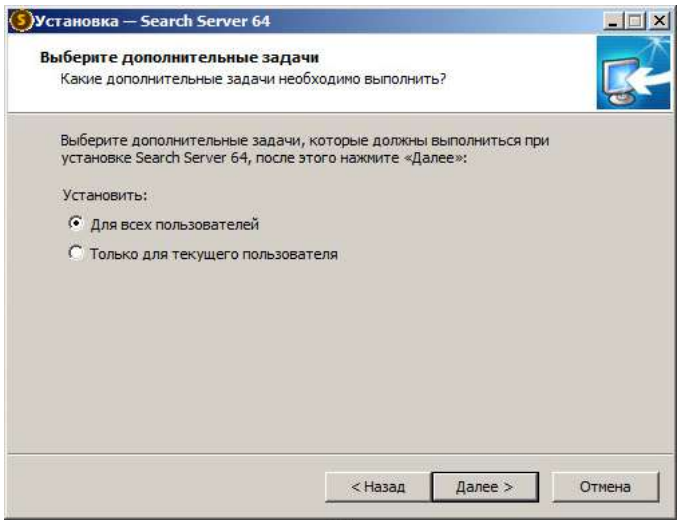


Рисунок 5.16

При просмотре окна «Всё готово к установке» убедитесь, что все параметры установки выбраны верно. Для внесения изменений воспользуйтесь кнопкой «Назад» (см. Рисунок 5.17).

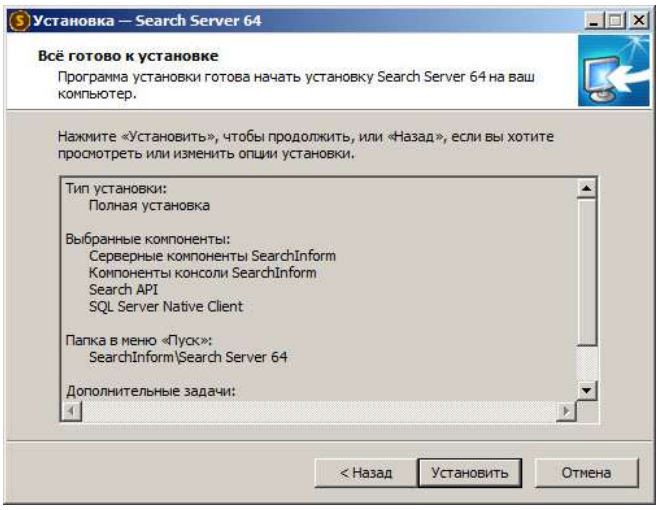


Рисунок 5.17

Щелкните кнопку «Установить» и дождитесь завершения операции. По завершении установки активируйте Search Server в DataCenter.

5.2.1 Активация сервера индексации

Запустите консоль DataCenter.

Перейдите на вкладку «Настройки» → «Используемые лицензии».

Разверните группу **SearchServer** в списке компонентов и вызовите из контекстного меню необходимого сервера команду «Изменить настройки» (см. Рисунок 5.18).

Рисунок 5.18

В настройках лицензий для Search Server необходимо разрешить выдачу лицензии (по умолчанию отключена, см. Рисунок 5.19).

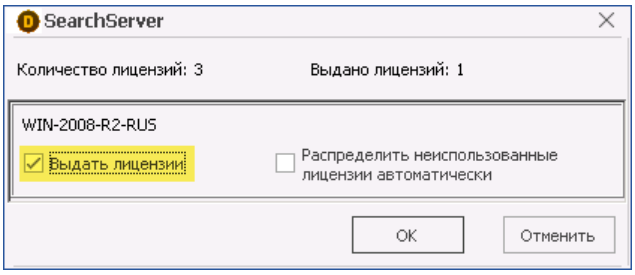


Рисунок 5.19

Если серверов Search Server в сети несколько, приобретенные лицензии могут быть распределены между ними автоматически при отметке соответствующего параметра.

Сохраните изменения кнопкой «Применить», расположенной в нижней части консоли DataCenter.

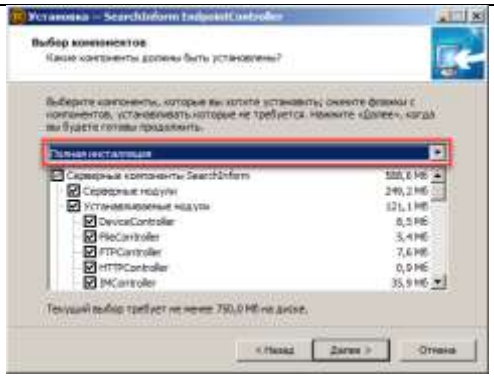
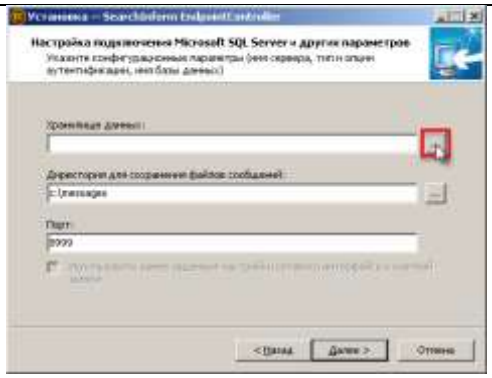
5.3 Установка сервера Серчинформ EndpointController

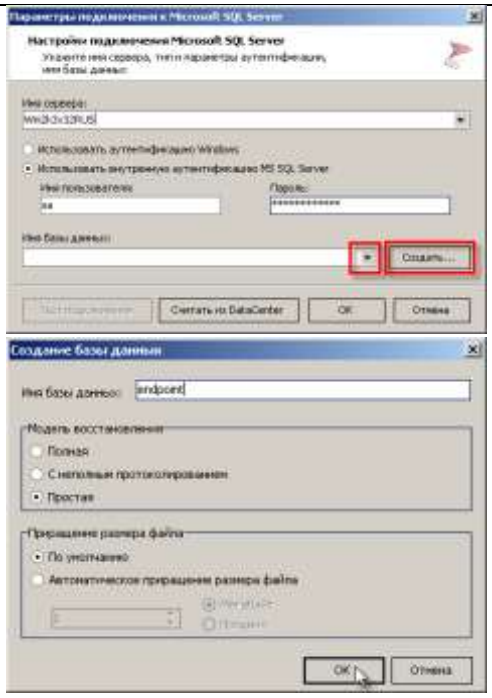
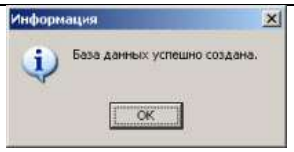
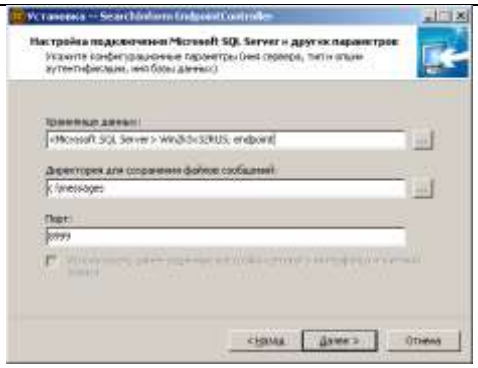
Запустите файл установки Серчинформ EndpointController.

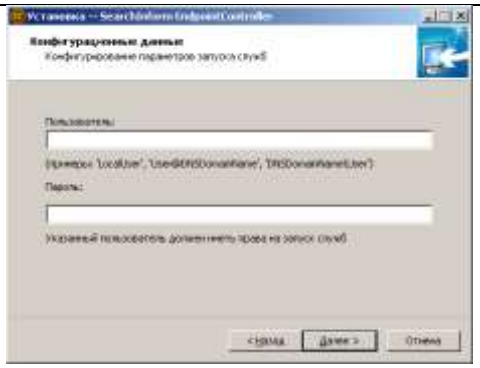
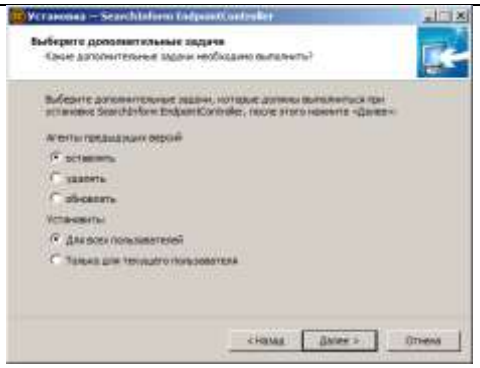
Произведите установку сервера EndpointController при помощи мастера, как это указано в Таблица 16.

Таблица 16 – Инструкция по установке сервера EndpointController

Страница мастера	Интерфейс (поле или свойство)	Действие или описание настроек
Выбор языка мастера	«Выберите язык»	«Русский»
Лицензионное соглашение	«Прочитайте лицензионное соглашение».	Ознакомьтесь с текстом и выберите «Я принимаю условия соглашения».
Папка установки	«Выбор папки установки»	Введите путь к папке на жестком диске вручную или воспользуйтесь кнопкой «Обзор» и выберите папку в обозревателе.

Страница мастера	Интерфейс (поле или свойство)	Действие или описание настроек
Выбор компонентов		Выберите «Полная инсталляция». В случае необходимости, отмените установку ненужных компонентов. При необходимости контроля рабочих станций на Linux дополнительно выберите «Модули поддержки Linux».
Задание хранилища настроек EndpointController, выбор папки для сообщений и указание порта		Чтобы задать БД, где будут храниться настройки сервера EndpointController, щёлкните кнопку справа от поля «Хранилище данных».
Подключение к СУБД Microsoft SQL Server		Ввод параметров для подключения сервера Microsoft SQL (имени сервера, при встроенной аутентификации дополнительно – имени пользователя и пароля) производится следующим образом: ВАРИАНТ 1 (если модуль DataCenter был предварительно настроен): Щелкните кнопку «Считать из DataCenter». Параметры «Имя сервера», «Имя пользователя» и «Пароль» будут автоматически сгенерированы из сервера DataCenter. ВАРИАНТ 2: Введите параметры подключения вручную (в поле «Имя сервера» можно вводить имя или IP-адрес сервера Microsoft SQL).

Страница мастера	Интерфейс (поле или свойство)	Действие или описание настроек
Привязка к базе данных при подключении к серверу Microsoft SQL Всплывающее окно – Создание базы данных		Из выпадающего списка выберите базу данных EndpointController. Для проверки подключения щёлкните «Тест подключения». В случае отсутствия нужной базы создайте новую базу: 1) Щёлкните кнопку «Создать». 2) В открывшемся окне «Создание базы данных» введите имя создаваемой базы данных. 3) Настройте параметры в группах «Модель восстановления» и «Приращение размера файла». 4) Подтвердите настройки нажатием «ОК».
Всплывающее сообщение		В случае успешного создания новой базы данных будет отображено подтверждающее сообщение.
Настройка хранилища настроек EndpointController, выбор папки для сообщений и указание порта		В поле «Хранилище данных» будет отображено местоположение хранилища с настройками сервера EndpointController. «Директория для сохранения файлов сообщений» – местоположение временного хранения перехваченных сообщений – можно оставить по умолчанию. «Порт» – оставьте по умолчанию. Если порт занят (отображается сообщение), измените на другой.
Отключение параметров работы сетевого интерфейса	Флажки: • TCP Offload, • Receive-side Scaling (RSS).	Оставьте настройки по умолчанию.

Страница мастера	Интерфейс (поле или свойство)	Действие или описание настроек
Выбор пользователя		Рекомендуется оставить поля пустыми, для того чтобы службы EndpointController работали от имени системной учётной записи. В случае, если для запуска служб необходима отдельная учётная запись, введите имя и пароль пользователя, который обладает следующими правами: • доступ к удалённому реестру; • удалённый доступ к службам (сервисам); • удалённый вызов процедур (RPC); • создание общих сетевых ресурсов (share folders); • вход в качестве службы. Рекомендуется использовать учётную запись с правами администратора домена.
Папка в меню «Пуск».	Выберите папку в меню «Пуск».	Выберите папку меню «Пуск», в которой будут созданы ярлыки.
Значки на рабочем столе	Создать значки на рабочем столе	Установка на ваш выбор.
Дополнительные задачи		«Агенты предыдущих версий». По умолчанию рекомендуется «Оставлять». «Установить» – «Для всех пользователей» / «Только для текущего пользователя» – на ваш выбор.
Завершение работы мастера	«Все готово к установке».	Отображается совокупность произведенных настроек для установки модуля. Щёлкните «Установить».

5.3.1 Лицензирование Серчинформ EndpointController

Запустите консоль Серчинформ DataCenter.

Перейдите на вкладку **Настройки** → **Используемые лицензии** (см. Рисунок 5.20).

Рисунок 5.20

Выберите в списке требуемый компонент платформы EndpointController. Вызовите из контекстного меню команду «Изменить настройки» (см. Рисунок 5.21).

Если для какого-либо продукта в консоли управления отключен перехват данных, он будет отмечен в списке символом «*».

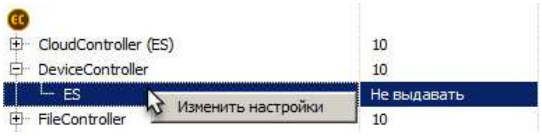


Рисунок 5.21

В настройках лицензий может быть указано количество выдаваемых лицензий для выбранного продукта. Количество выдаваемых продукту лицензий не может превышать количество свободных (см. Рисунок 5.22).

При выборе параметра «Распределить неиспользуемые лицензии автоматически» данному продукту будут выданы все лицензии, являющиеся на данный момент свободными. Если серверов EndpointController несколько, лицензии будут распределены между ними поровну.

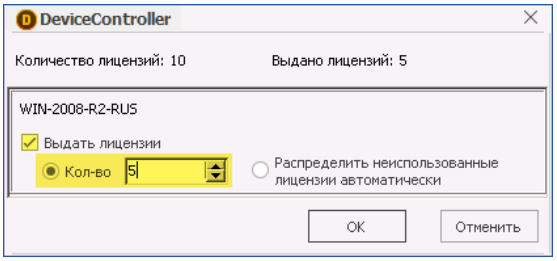


Рисунок 5.22

Сохраните изменения кнопкой «Применить», расположенной в нижней части консоли DataCenter.

Просмотр информации об используемых и превышенных лицензиях осуществляется в консоли EndpointController на вкладке «Лицензии» (см. Рисунок 5.23).

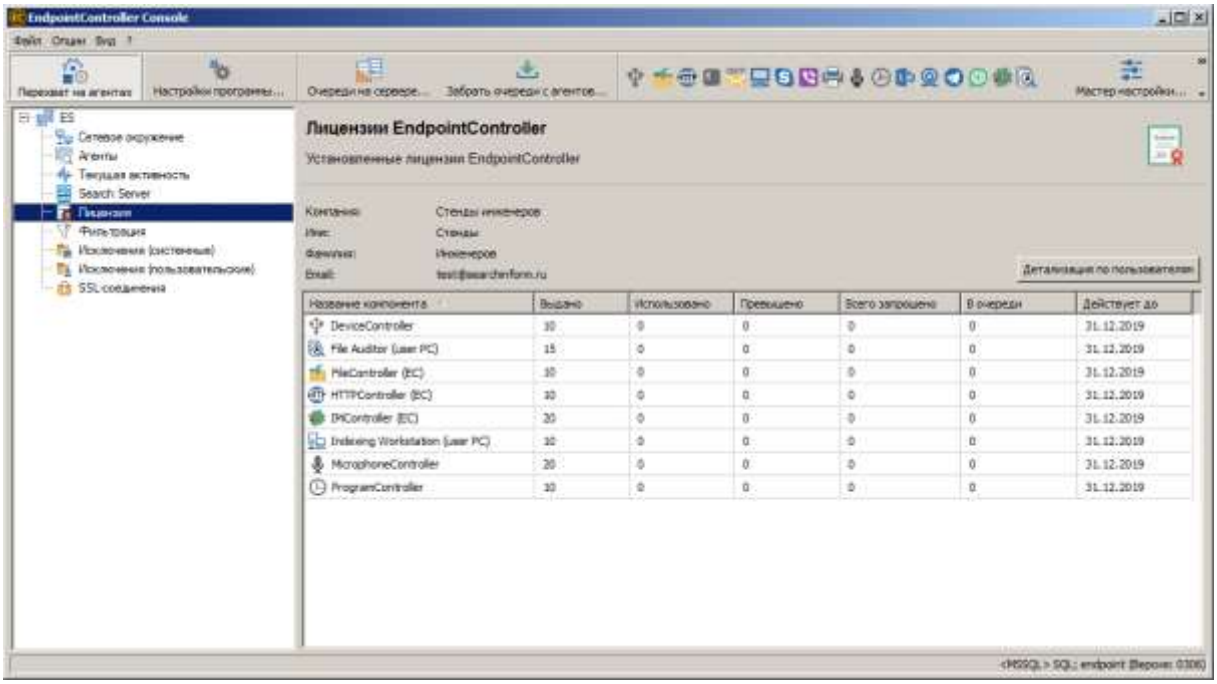


Рисунок 5.23

Для просмотра детальной информации о списывании лицензий воспользуйтесь кнопкой «Детализация по пользователям».

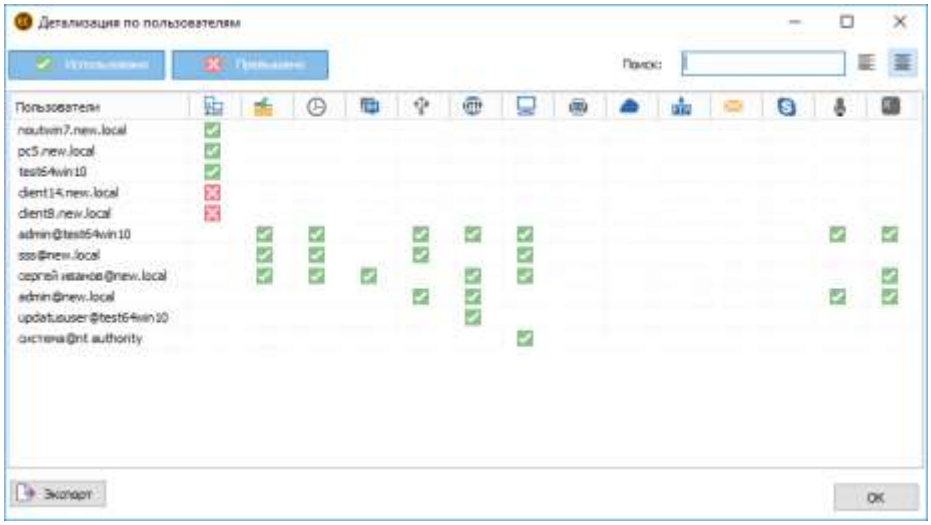


Рисунок 5.24

5.4 Установка сервера Серчинформ NetworkController

Запустите файл установки Серчинформ NetworkController.

Выберите язык установки: русский либо английский (см. Рисунок 5.25).

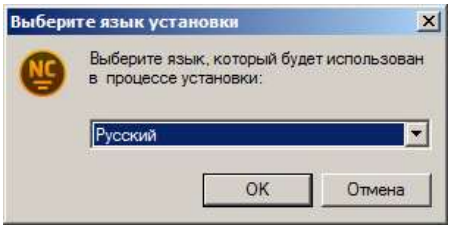


Рисунок 5.25

Ознакомьтесь с текстом лицензионного соглашения и выберите пункт «Я принимаю условия соглашения» (см. Рисунок 5.26). Щелкните кнопку «Далее».

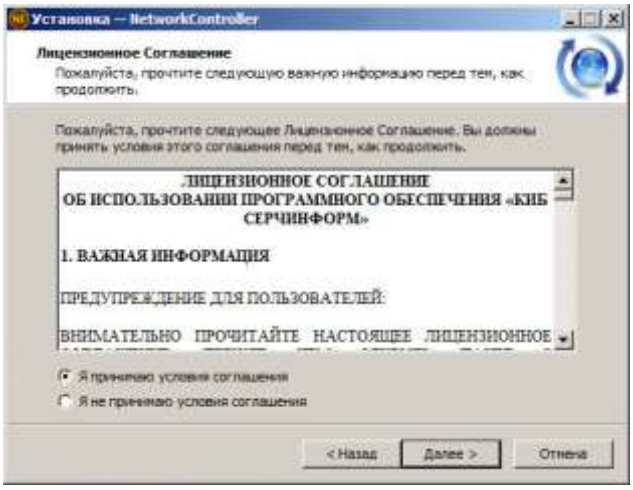


Рисунок 5.26

Укажите путь установки (см. Рисунок 5.27).

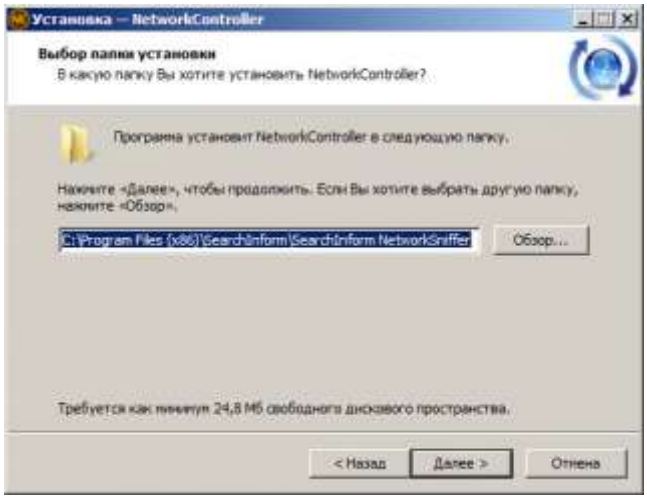


Рисунок 5.27

Выберите «серверную инсталляцию» NetworkController. Серверная инсталляция включает в себя модули анализаторов трафика, протоколов перехвата, модули подключения к базам данных и другое (см. Рисунок 5.28).

В группе «Анализатор трафика» выберите только требуемые модули.

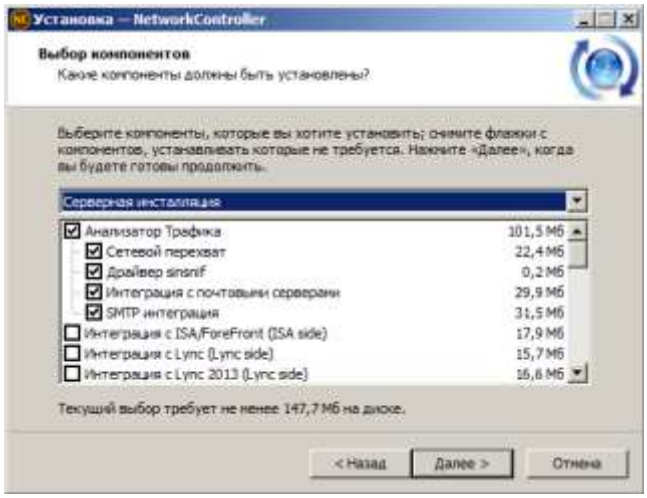


Рисунок 5.28

Выберите дополнительные задачи установки. Нажмите «Далее» (см. Рисунок 5.29).

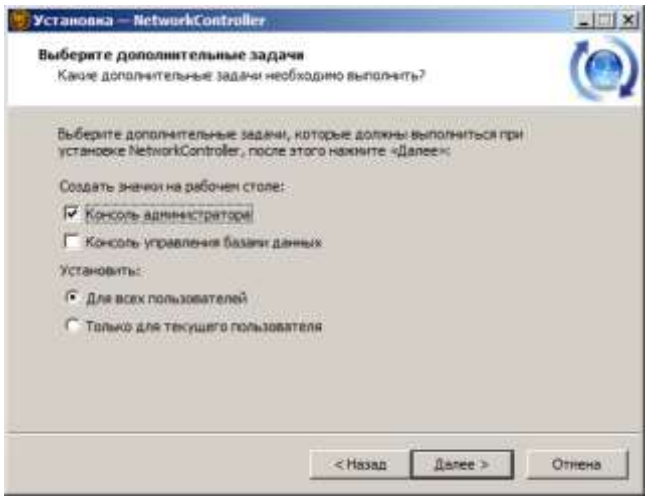


Рисунок 5.29

В следующем окне отобразится извещение мастера о готовности выбранных компонентов к установке (см. Рисунок 5.30). Щёлкните «Установить».

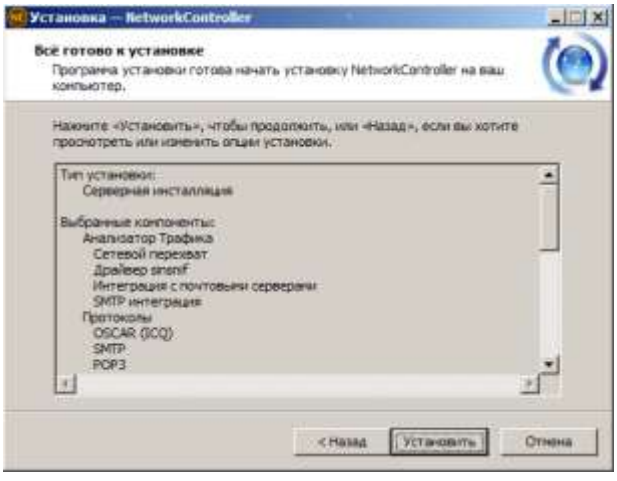


Рисунок 5.30

Для настройки NetworkController сразу после установки установите флажок напротив параметра «Запустить NetworkController Administrator Console» и щёлкните кнопку «Завершить» (см. Рисунок 5.31).

Рисунок 5.31

5.4.1 Активация серверного модуля Серчинформ NetworkController

Запустите консоль Серчинформ DataCenter.

Перейдите на вкладку **Настройки** → **Используемые лицензии** (см. Рисунок 5.32).

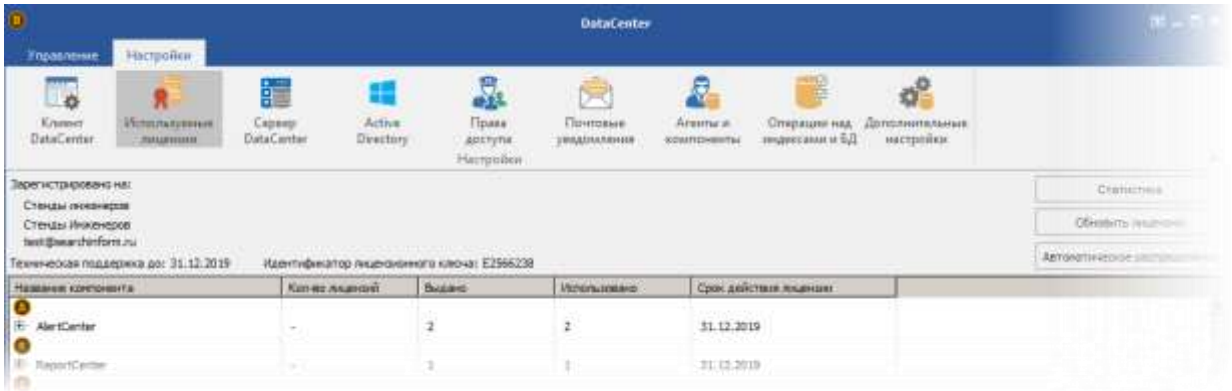


Рисунок 5.32

Выберите в списке требуемый компонент платформы NetworkController. Вызовите из контекстного меню команду «Изменить настройки».

Если для какого-либо продукта в консоли управления отключен перехват данных, он будет отмечен в списке символом «*» (см. Рисунок 5.33).

Рисунок 5.33

В окне настройки лицензий может быть указано количество выдаваемых лицензий для выбранного продукта. Количество выдаваемых продукту лицензий не может превышать количество свободных (см. Рисунок 5.34).

Рисунок 5.34

При выборе параметра «Распределить неиспользуемые лицензии автоматически» данному продукту будут выданы все лицензии, являющиеся на данных момент свободными. Если серверов NetworkController несколько, лицензии продукта будут распределены между серверами поровну.

Сохраните изменения кнопкой «Применить», расположенной в нижней части консоли DataCenter.

Просмотр параметров лицензии, периода ее действия, количества используемых и превышенных лицензий осуществляется в консоли Серчинформ NetworkController на вкладке «Лицензии» (см. Рисунок 5.35).

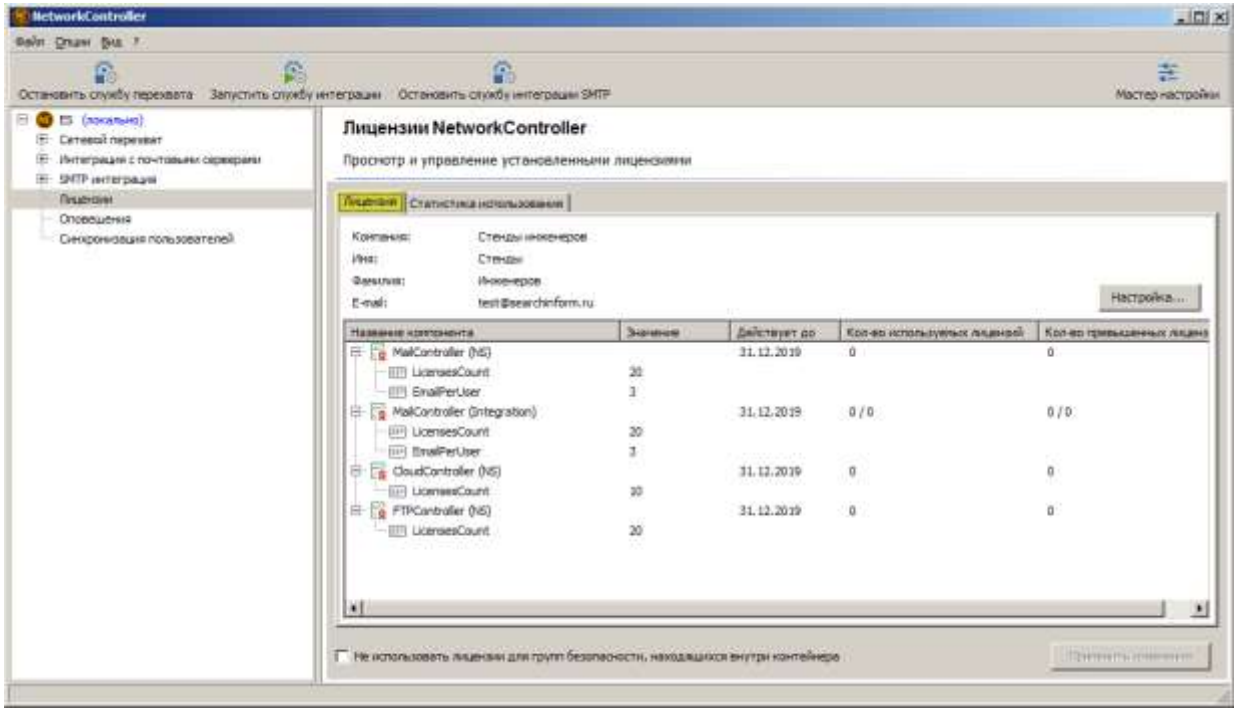


Рисунок 5.35

Статистика использования лицензий позволяет получить подробную информацию по использованным и недостающим лицензиям компонентов NetworkController (см. Рисунок 5.36).

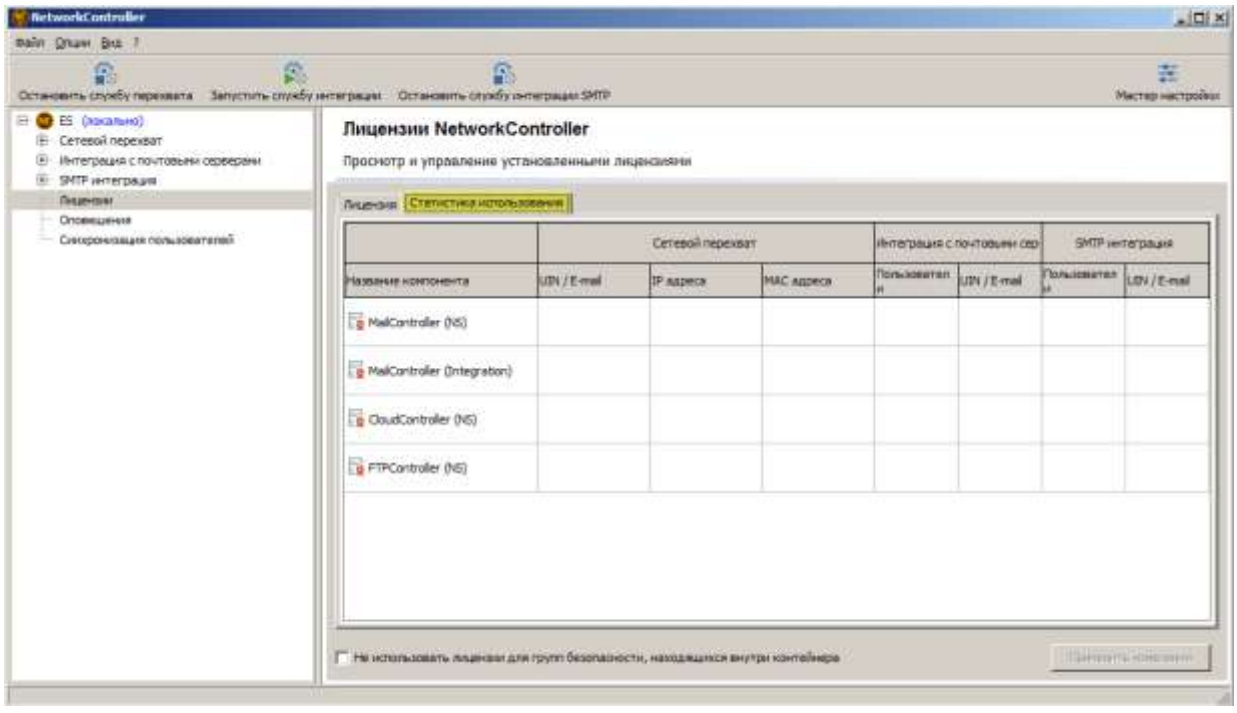


Рисунок 5.36

5.5 Установка аналитического модуля Серчинформ AlertCenter

Обычно серверная и клиентская части AlertCenter устанавливаются раздельно:

- Серверная часть AlertCenter устанавливается на сервер индексации Search Server или на отдельный сервер.
- Клиентская часть AlertCenter устанавливается на PC сотрудника службы информационной безопасности.

5.5.1 Установка серверной части AlertCenter

Запустите дистрибутив.

После выбора языка (русский), используемого в процессе установки, будет отображено окно приветствия мастера установки (см. Рисунок 5.37).

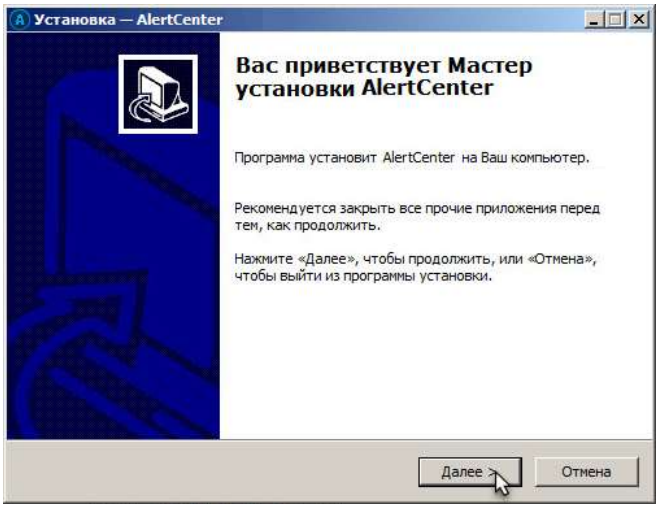


Рисунок 5.37

Ознакомьтесь с текстом лицензионного соглашения и выберите пункт «Я принимаю условия соглашения» (см. Рисунок 5.38). Щелкните кнопку «Далее».

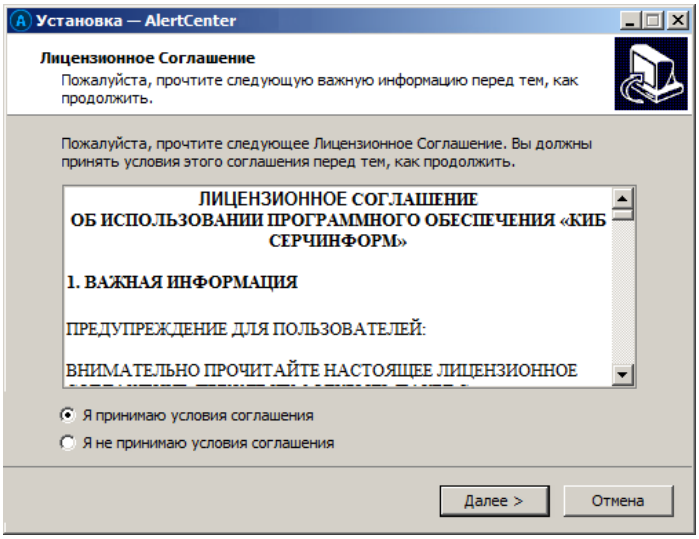


Рисунок 5.38

Выберите папку, в которую будет устанавливаться программа (см. Рисунок 5.39).

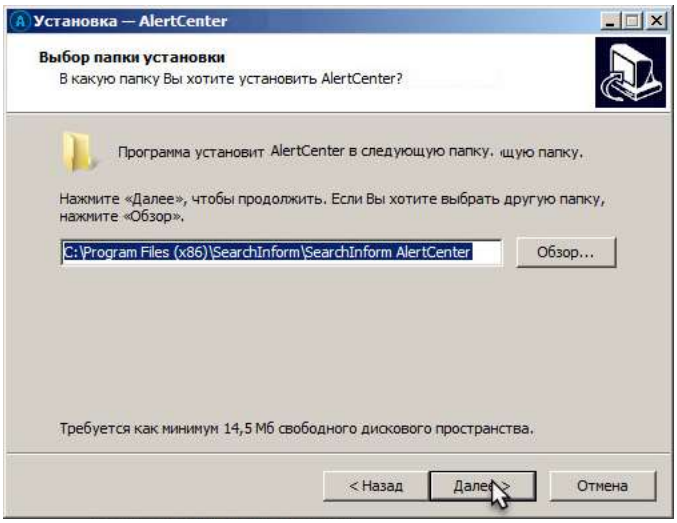


Рисунок 5.39

Выберите компоненты AlertCenter Server и SQL Server Native Client (см. Рисунок 5.40). **Без установленного компонента SQL Server Native Client система работать не будет!**

Если понадобится функция блокировки исходящей почты, установите флажок «AlertCenter Служба остановки почты».

Если понадобится функция экспорта в SIEM, установите флажок «AlertCenter Служба экспорта в SIEM».

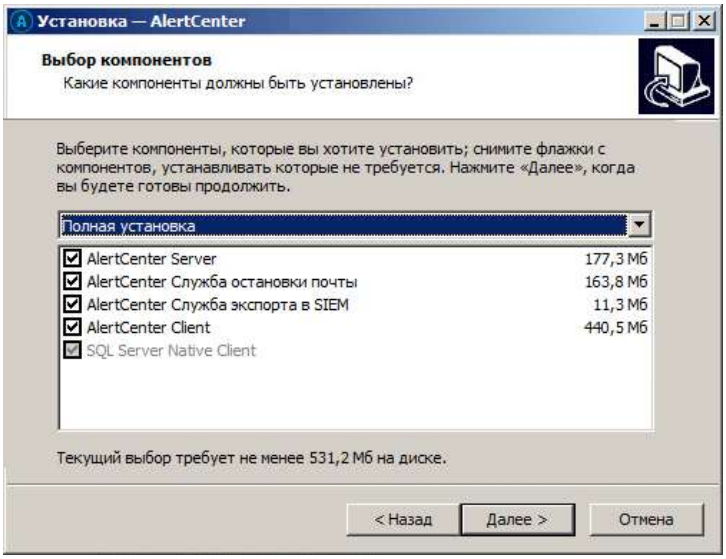


Рисунок 5.40

На следующем шаге создайте (а в случае обновления версии выберите/измените) базу данных AlertCenter, в которой будут храниться настройки сервера AlertCenter и журналы инцидентов. Для этого нажмите кнопку «Изменить настройки» (см. Рисунок 5.41).

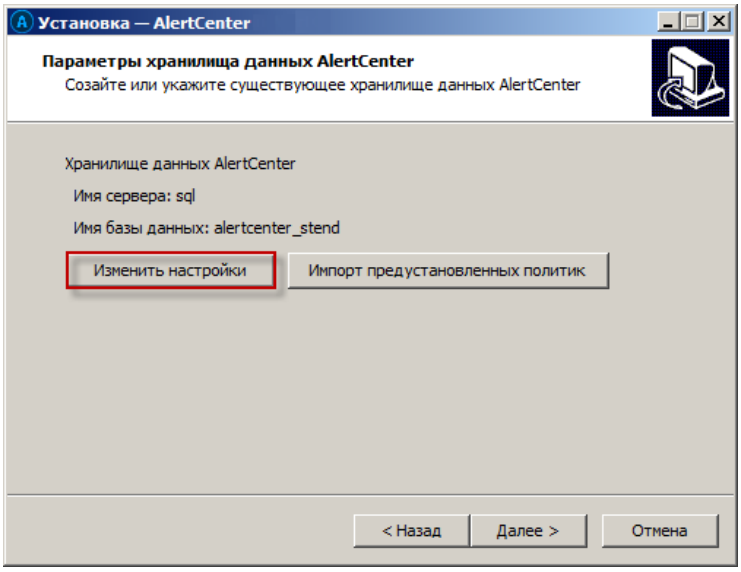


Рисунок 5.41

Выберите из выпадающего списка сервер, к которому необходимо подключиться:

- Если выбранный сервер присутствует в списке серверов DataCenter, то параметры подключения к нему можно получить, нажав кнопку «Считать из DC».
- Если выбранный сервер отсутствует в списке серверов DataCenter, то кнопка «Считать из DC» будет неактивна (см. Рисунок 5.42).

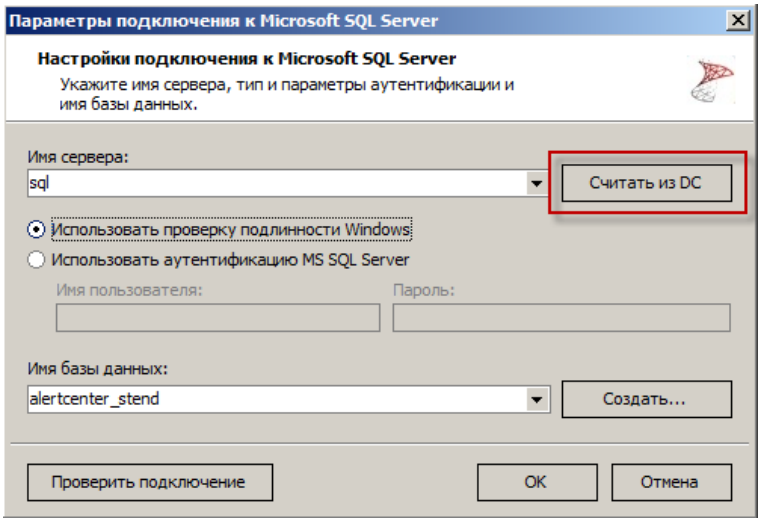


Рисунок 5.42

В выпадающем списке выберите существующую базу данных, к которой необходимо подключиться. Если база данных не создана, щёлкните кнопку «Создать». Введите имя новой базы данных и заполните поля, позволяющие указать пути к файлам создаваемой базы данных:

- Данные - путь к файлам создаваемой базы;

- Журнал - путь к журналу транзакций базы данных, в котором фиксируются все транзакции и производимые ими в базе изменения. При сбое системы этот журнал позволяет вернуть базу данных в согласованное состояние (см. Рисунок 5.43).

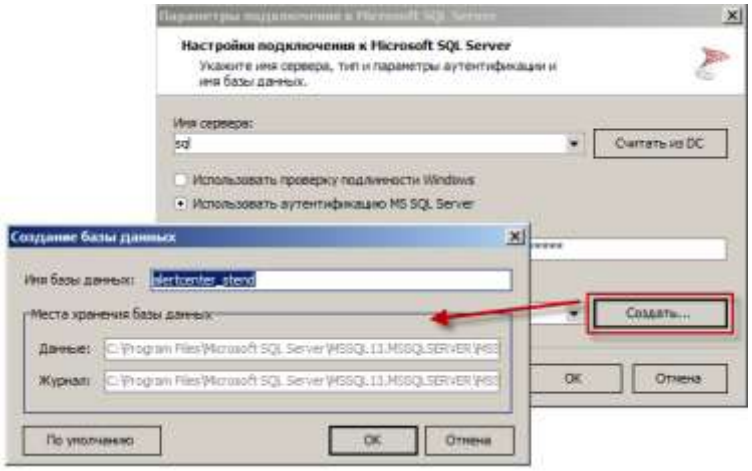


Рисунок 5.43

Проверка подключения к выбранной/созданной базе данных осуществляется нажатием кнопки «Проверить подключение». При успешном подключении появляется подтверждающее сообщение (см. Рисунок 5.44).

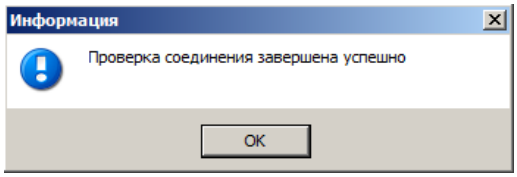


Рисунок 5.44

Сохраните настройки подключения, нажав «ОК».

При обновлении версии AlertCenter (или подключении к существующей базе данных) может оказаться, что версия выбранной базы данных устарела, и при попытке подключения к ней будет отображаться ошибка. В этом случае нужно произвести преобразование базы (см. Рисунок 5.45).

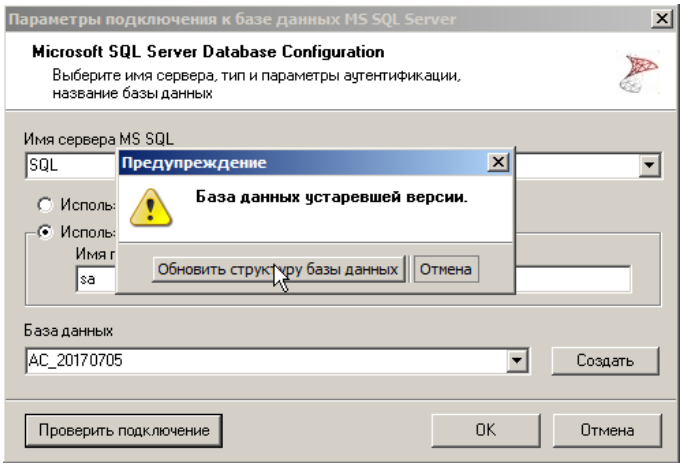


Рисунок 5.45

В некоторых случаях преобразование версии базы данных может занять довольно продолжительное время. Длительность операции зависит от объёма данных в базе, а также от объёма изменений структуры базы данных (насколько новая версия AlertCenter отличается от текущей).

Затем произведите импорт предустановленных политик безопасности для Вашей страны (см. Рисунок 5.46).

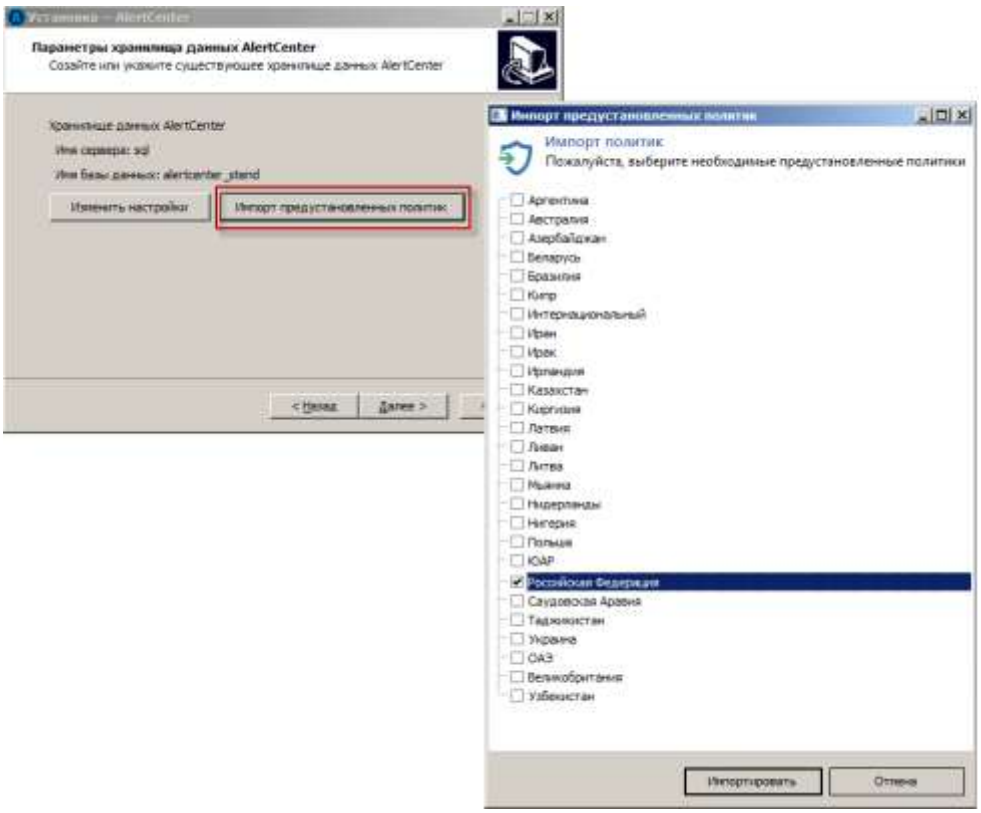


Рисунок 5.46

На следующем шаге (см. Рисунок 5.47) выберите учётную запись, от имени которой будут запущены службы AlertCenter.

- Если параметры доступа при установке новой версии поверх предыдущей не планируется изменять, оставьте настройку по умолчанию – **«с текущими настройками службы»**.
- Для запуска AlertCenter от имени системной учётной записи выберите опцию – **«с параметрами системной учетной записи»**. Данная опция не рекомендуется для постоянной работы с AlertCenter, она используется в служебных целях.
- Если необходимо расширить права доступа к индексам для других пользователей, то при установке AlertCenter укажите учётную запись, под которой будет работать сервер AlertCenter. Для этого выберите опцию **«с указанной учётной записью»** и введите имя и пароль пользователя, учётная запись которого будет иметь права доступа к индексам.

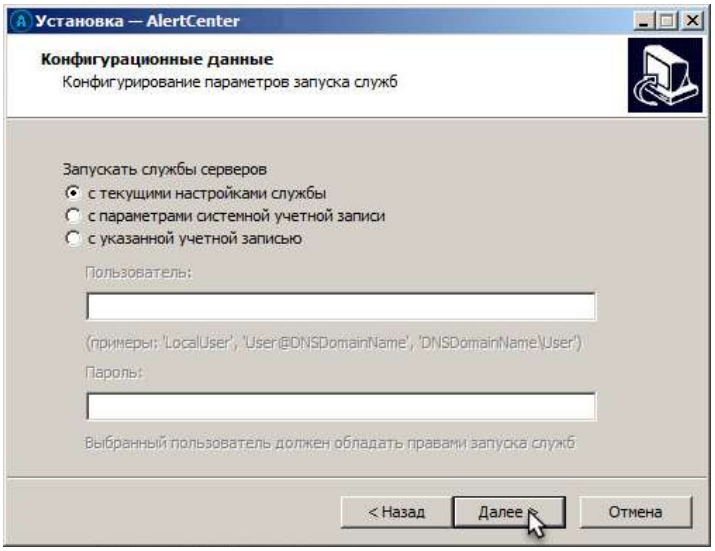


Рисунок 5.47

На следующем шаге установки AlertCenter выберите дополнительные задачи: создавать либо не создавать значок на Рабочем столе, установить модуль AlertCenter для всех пользователей или только для текущего пользователя (см. Рисунок 5.48).

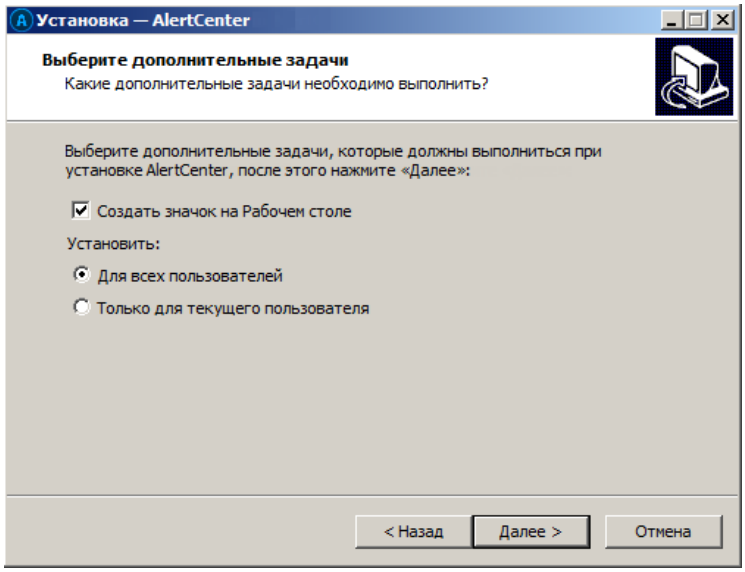


Рисунок 5.48

В окне «Все готово к установке» будет отображена совокупность заданных параметров для установки AlertCenter (см. Рисунок 5.49). Если параметры верны, щёлкните кнопку «Установить».

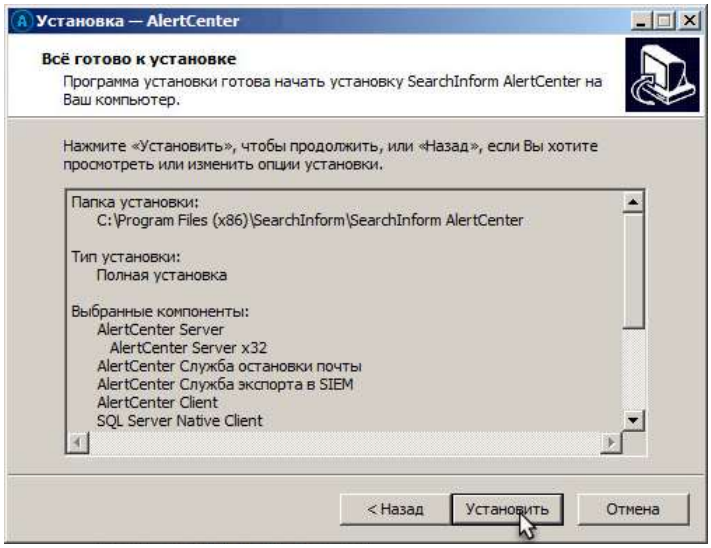


Рисунок 5.49

В открывшемся окне будет отображен прогресс установки AlertCenter, дождитесь его окончания и в завершающем окне мастера щёлкните «Завершить» (см. Рисунок 5.50).

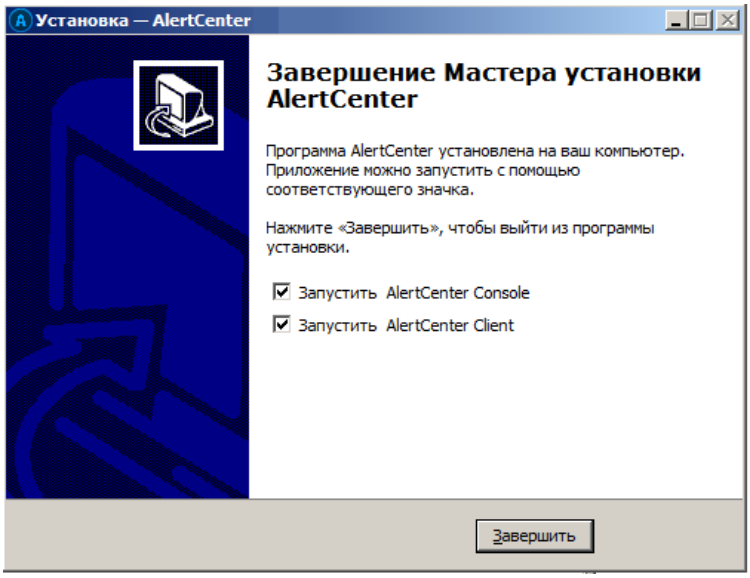


Рисунок 5.50

5.5.2 Установка клиентской части AlertCenter

Порядок установки клиентской части AlertCenter практически полностью совпадает с описанной выше процедурой установки серверной части AlertCenter.

На этапе выбора компонентов выберите тип инсталляции – «Клиентская установка» или компоненты AlertCenter Клиент, SQL Server Native Client (без установленного компонента SQL Server Native Client система работать не будет!). Службу остановки почты при установке клиента AlertCenter выбирать не нужно.

Если появится сообщение о необходимости преобразования базы данных, щёлкните кнопку «Преобразовать».

По завершении работы мастера установки на экране будет отображено окно авторизации, в котором укажите (права доступа к консоли настраиваются в DataCenter):

- имя DataCenter сервера - если AlertCenter и DataCenter установлены на одном компьютере, можно указать *localhost*.
- проверку подлинности - Windows (для доменных учетных записей) или SearchInform (используются внутренние пользователя DataCenter - для рабочих групп) (см. Рисунок 5.51).

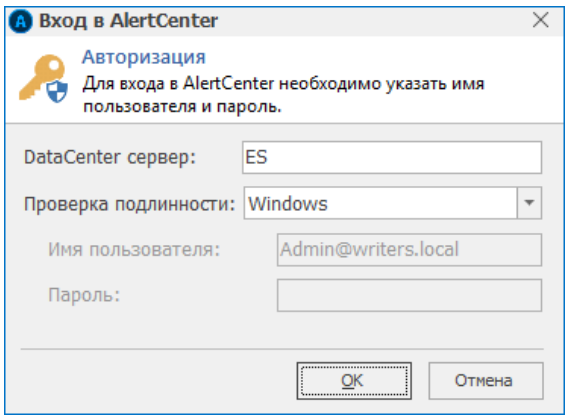


Рисунок 5.51

По завершении работы мастера установки на экране будет отображена консоль клиентской части AlertCenter (см. Рисунок 5.52).

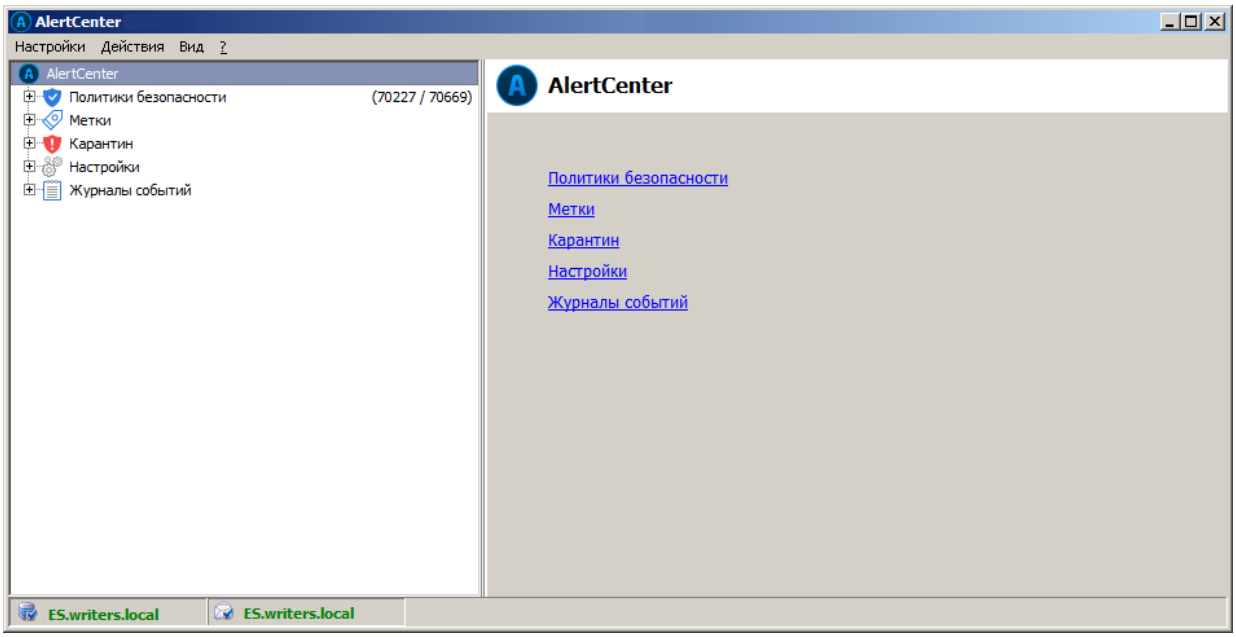


Рисунок 5.52

5.5.3 Активация модуля AlertCenter

Для компонента AlertCenter в консоли DataCenter по умолчанию установлена автоматическая выдача лицензий и изменению не подлежит (см. Рисунок 5.53).

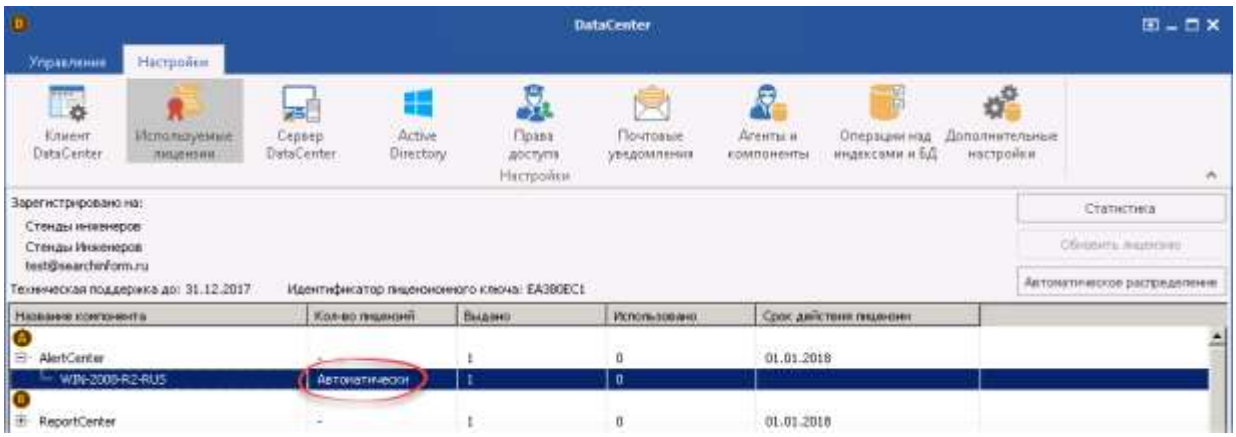


Рисунок 5.53

Просмотр установленных лицензий осуществляется в консоли настройки сервера AlertCenter (см. Рисунок 5.54).

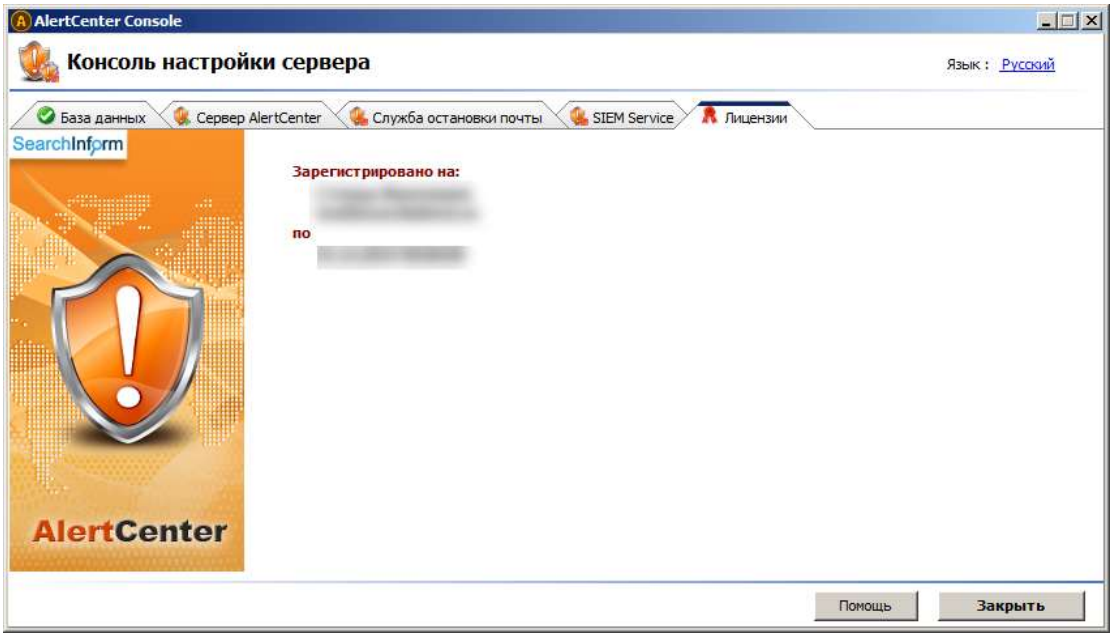


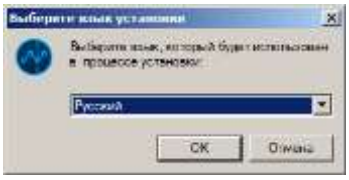
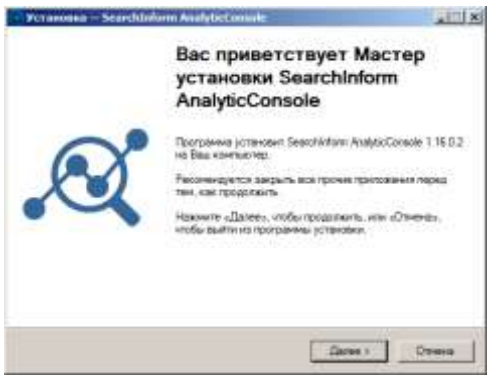
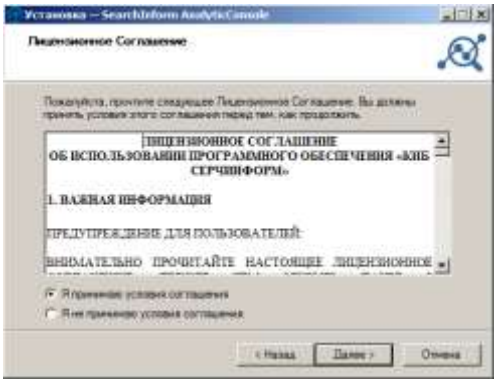
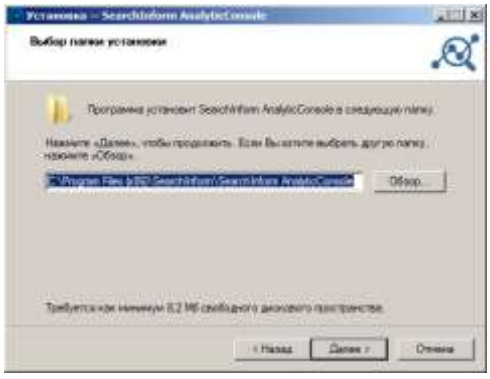
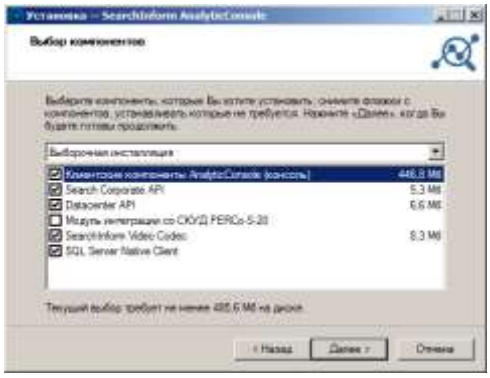
Рисунок 5.54

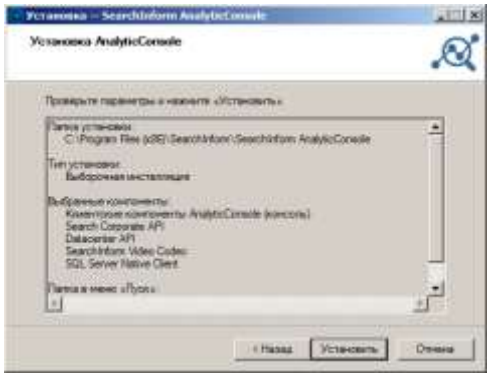
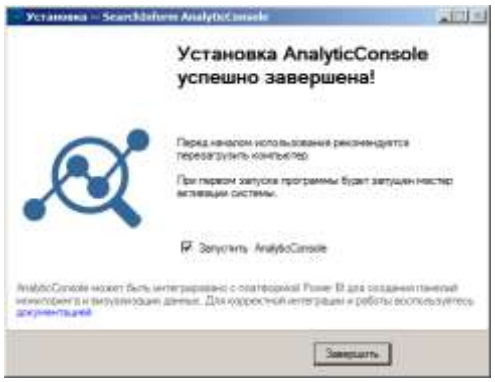
5.6 Установка Серчинформ AnalyticConsole

Установка клиентского модуля производится на PC сотрудника службы безопасности.

Запустите файл установки Серчинформ AnalyticConsole. Произведите установку приложения Серчинформ AnalyticConsole при помощи мастера, как это указано в Таблица 17.

Таблица 17 – Инструкция по установке Серчинформ AnalyticConsole

Страница мастера	Интерфейс (поле или элемент управления)	Действие или описание настроек
Выбор языка мастера		Выберите язык - «Русский».
Приветствие мастера		Щёлкните кнопку «Далее».
Лицензионное соглашение		Ознакомьтесь с текстом и выберите «Я принимаю условия соглашения».
Папка установки		Введите путь к папке на жестком диске вручную или воспользуйтесь кнопкой «Обзор» и выберите папку в обозревателе.
Выбор компонентов установки		Выберите необходимые для установки компоненты, щёлкните «Далее».

Страница мастера	Интерфейс (поле или элемент управления)	Действие или описание настроек
Проверка настроек установки		Отображается обобщенная картина произведенных настроек для установки приложения. Щелкните «Установить». *Если появится сообщение о запущенных процессах, остановите их через Диспетчер задач Windows, не прерывая работу мастера установки!*
Завершение работы мастера		Оставьте флажок установленным, если необходимо запустить приложение Серчинформ AnalyticConsole немедленно. Щёлкните «Завершить».

6 НАСТРОЙКА КОМПОНЕНТОВ СЕРЧИНФОРМ ДЛП

Каждый раз при вызове консоли какого-либо компонента Серчинформ ДЛП необходимо пройти процедуру авторизации (см. Рисунок 6.1).

Возможен вход с использованием доменной учетной записи Windows, от имени которой запущено приложение, либо под учетной записью пользователя, не состоящего в структуре домена. При выборе последней потребуется ввести логин и пароль внутреннего пользователя Серчинформ, который был предварительно создан в консоли DataCenter.

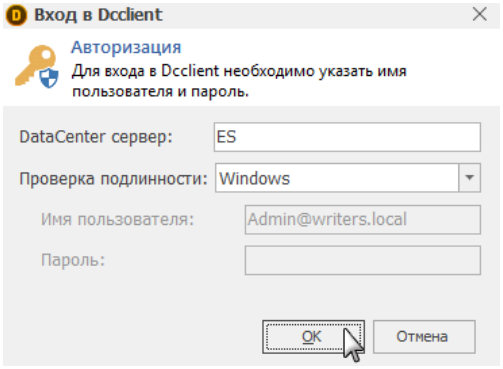


Рисунок 6.1

6.1 Настройка модуля администрирования Серчинформ DataCenter

Настройка DataCenter производится в следующем порядке:

1) запуск сервера;
2) настройка баз данных по умолчанию;
3) выбор доменов для синхронизации с Active Directory или добавление пользователей рабочих групп и пользователей SearchInform;
4) настройка параметров использования дискового пространства;
5) настройка почтовых уведомлений;
6) настройка правил создания и удаления индексов и баз данных;
7) настройка принудительного включения служб;
8) настройка параметров прокси-сервера;
9) настройка журналирования действий аудиторов;
10) настройка сервера профайлинга;
11) настройка сервера ReportCenter;
12) настройка сервера WebAnalytic.

Настройка прав сотрудников службы безопасности на просмотр данных того или иного пользователя осуществляется после завершения процесса синхронизации с Active Directory.

Настройка библиотеки цифровых отпечатков производится после установки компонента Search Server и его активации.

Настройке службы сбора данных должно предшествовать создание индексов в консоли сервера EndpointController/NetworkController.

Все операции по настройке производятся в консоли клиента DataCenter.

6.1.1 Запуск сервера

Для запуска сервера, щёлкните кнопку «Запустить», расположенную на вкладке «Управление». Имя кнопки изменится на «Остановить» (см. Рисунок 6.2).

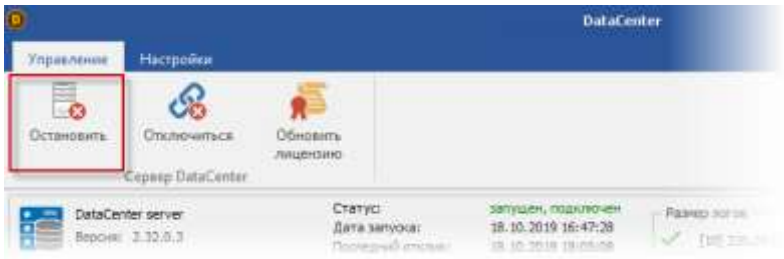


Рисунок 6.2

6.1.2 Синхронизация с Active Directory

Синхронизация с Active Directory запускается:

1. При добавлении домена в список синхронизации.
2. Согласно настройкам частоты синхронизации домена:
   - раз в сутки в определенное время,
   - круглосуточно через определенный интервал времени (минимальное значение – 30 минут).

Щёлкните кнопку «Active Directory», расположенную на вкладке «Настройки». Существует возможность добавить один или несколько доменов для синхронизации с Active Directory. Для добавления и удаления доменов предназначены кнопки  и  , соответственно.

Задайте имя домена, логин и пароль.

В случае, когда контроллеров домена несколько, можно задать подключение к конкретному из них. Для этого отметьте флажком параметр «Подключаться только к контроллеру домена» и задайте полное доменное имя или IP-адрес контроллера в текстовом поле.

Для добавления еще одного домена повторите вышеописанную процедуру.

Если добавляемый домен имеет большой размер, отключите кэширование с помощью параметра «Не использовать кэширование данных». В иных случаях отмечать данный параметр не рекомендуется, поскольку это снижает скорость чтения содержимого домена (см. Рисунок 6.3).

Рисунок 6.3

Также есть возможность указать количество неудачных попыток синхронизации сервера DataCenter с доменом Active Directory, по достижении которых DataCenter сгенерирует отправку почтового уведомления. Задайте значение параметра **«Уведомить после N неудачных попыток»** (см. Рисунок 6.4).

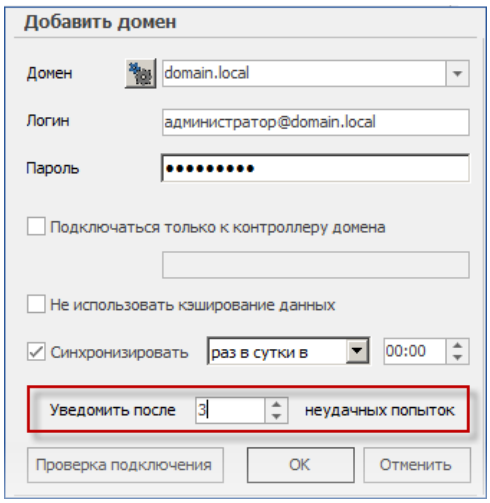


Рисунок 6.4

Когда число подряд идущих неудачных попыток синхронизации достигает заданного значения, то отправляется уведомление об ошибке. Затем уведомления

генерируются при каждой следующей неудачной попытке синхронизации. Счётчик неудачных попыток обнуляется после каждой удачной попытки синхронизации.

Внимание! *Отправка уведомлений осуществляется только в том случае, если параметры уведомлений настроены и активированы на вкладке «Почтовые уведомления» (см. Рисунок 6.5).*

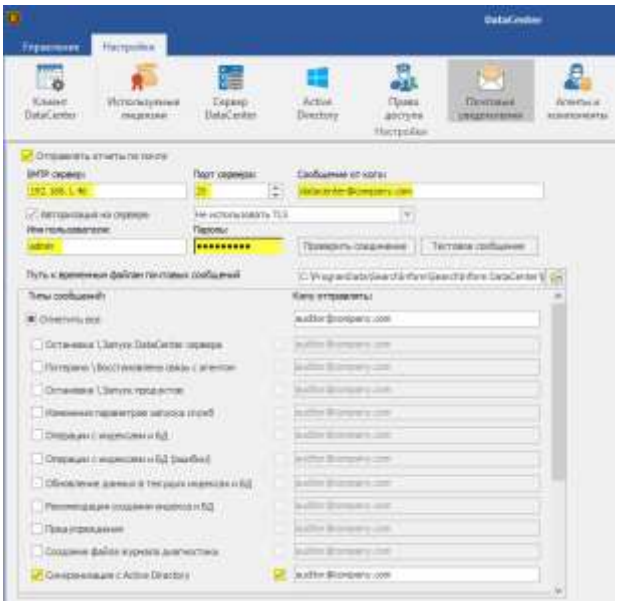


Рисунок 6.5

Щёлкните «ОК» для применения настроек.

Щёлкните по кнопке «Настроить подключение к БД» и создайте подключение к базе данных, в которой будут сохраняться данные указанных доменов, полученные в результате синхронизации DataCenter с Active Directory (см.Рисунок 6.6).

Рисунок 6.6

В окне «Параметры подключения Microsoft SQL Server» выберите СУБД (MS SQL и PostgreSQL), имя сервера и данные для авторизации при подключении к серверу баз данных. Если сервер баз данных был предварительно внесен в список баз данных по умолчанию, возможен импорт настроек подключения к указанному серверу по нажатию кнопки «Считать из DC».

После чего следует выбрать в выпадающем списке наименование базы данных, с которой будут синхронизированы домены. Если такая база данных не создана, кликните по кнопке «Создать».

Кнопка «Проверка подключения» проверяет корректность введенных настроек подключения к базе данных.

В нижней части вкладки «Active Directory» отображается список атрибутов Active Directory (см. Рисунок 6.7). Отмеченные флажками атрибуты DataCenter считывает и сохраняет в указанной БД.

В данной версии доступен только поиск по наименованиям в списке импортируемых в БД атрибутов.

Рисунок 6.7

6.1.2.1 Работа с пользователями рабочих групп

Если в структуре компьютерной сети присутствуют только рабочие группы либо параллельно с доменом необходима работа с пользователями рабочих групп, потребуется настройка списка таких пользователей и компьютеров вручную. В дальнейшем работа с ними ничем не отличается от работы с доменными пользователями, в частности, к ним могут быть применены настройки разграничения прав доступа.

Настройка списка осуществляется в правой части окна на вкладке «Active Directory». Предварительно должно быть настроено подключение к базе данных DataCenter (см. Рисунок 6.8).

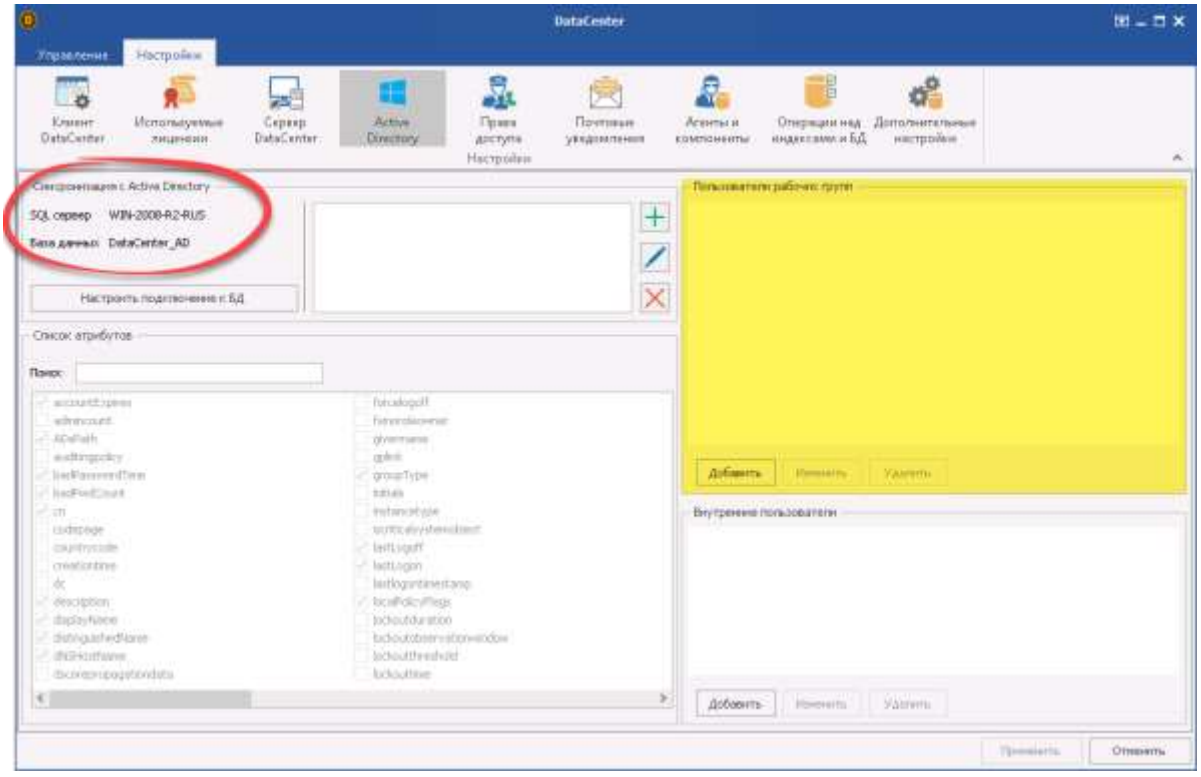


Рисунок 6.8

Нажмите кнопку «Добавить» и в открывшемся диалоговом окне «Добавить пользователя» укажите:

- Наименование компьютера рабочей группы;
- Учетную запись пользователя Windows на данном компьютере;
- Полное имя пользователя компьютера (см. Рисунок 6.9).

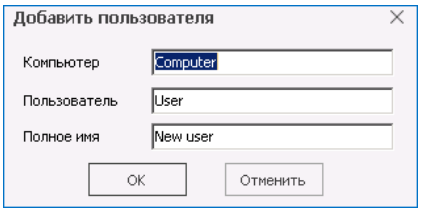


Рисунок 6.9

Щелкните кнопку «ОК» для отображения данных в консоли.

6.1.2.2 Создание учетных записей SearchInform

Для аудиторов безопасности, рабочие станции которых состоят в рабочей группе, возможно создание учетной записи SearchInform. В дальнейшем параметры таких учетных записей используются при входе в консоль DataCenter.

На вкладке «Active Directory» в блоке «Внутренние пользователи» нажмите кнопку «Добавить» и в появившемся диалоговом окне укажите (см. Рисунок 6.10):

- Полное имя аудитора службы безопасности;
- Учетная запись пользователя на данном компьютере;
- Пароль к учетной записи пользователя;
- Повтор заданного пароля.

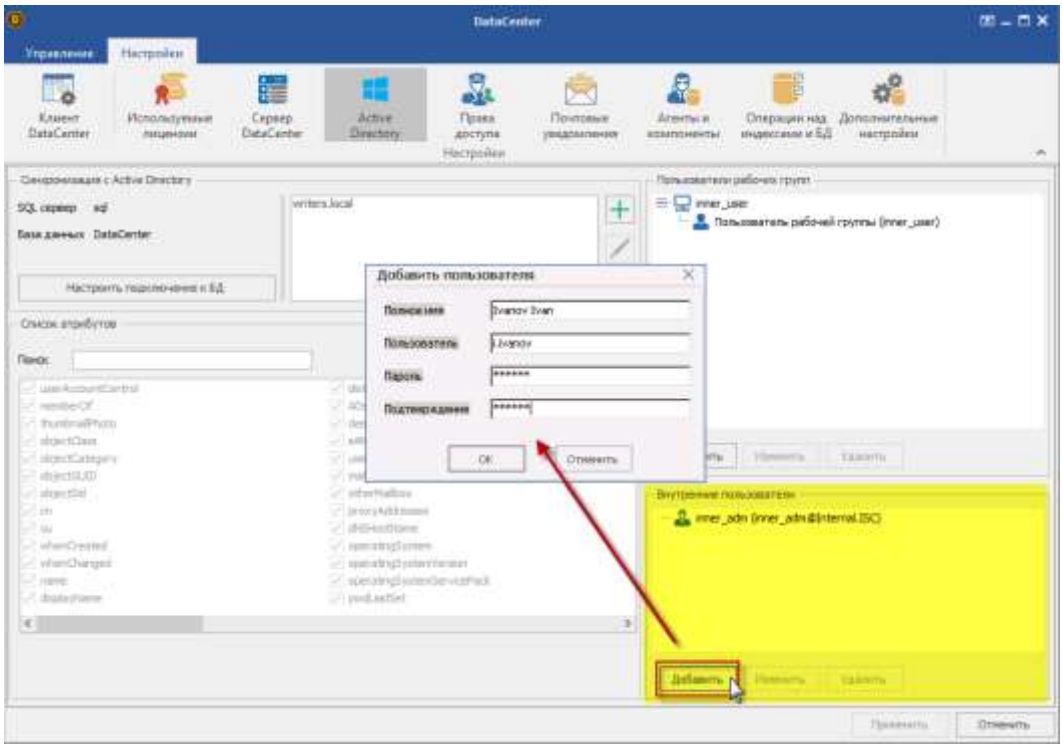


Рисунок 6.10

6.1.3 Настройка прав доступа

DataCenter позволяет создать список сотрудников службы безопасности и сформировать для каждого из них права на просмотр данных по тем или иным пользователям, группам пользователей и компьютерам. Под данными подразумеваются инциденты, зафиксированные компонентом Серчинформ AlertCenter, а также содержимое документов при просмотре в Серчинформ AnalyticConsole.

Перейдите на вкладку «Настройки» и щелкните кнопку «Права доступа».

Установите флажок «Включить ограничение прав доступа для просмотра результатов поиска и инцидентов».

6.1.3.1 Добавление аудиторов и назначение им ролей

В области «Аудиторы» с помощью кнопки «Добавить/Удалить» формируется список сотрудников службы безопасности (см. Рисунок 6.11).

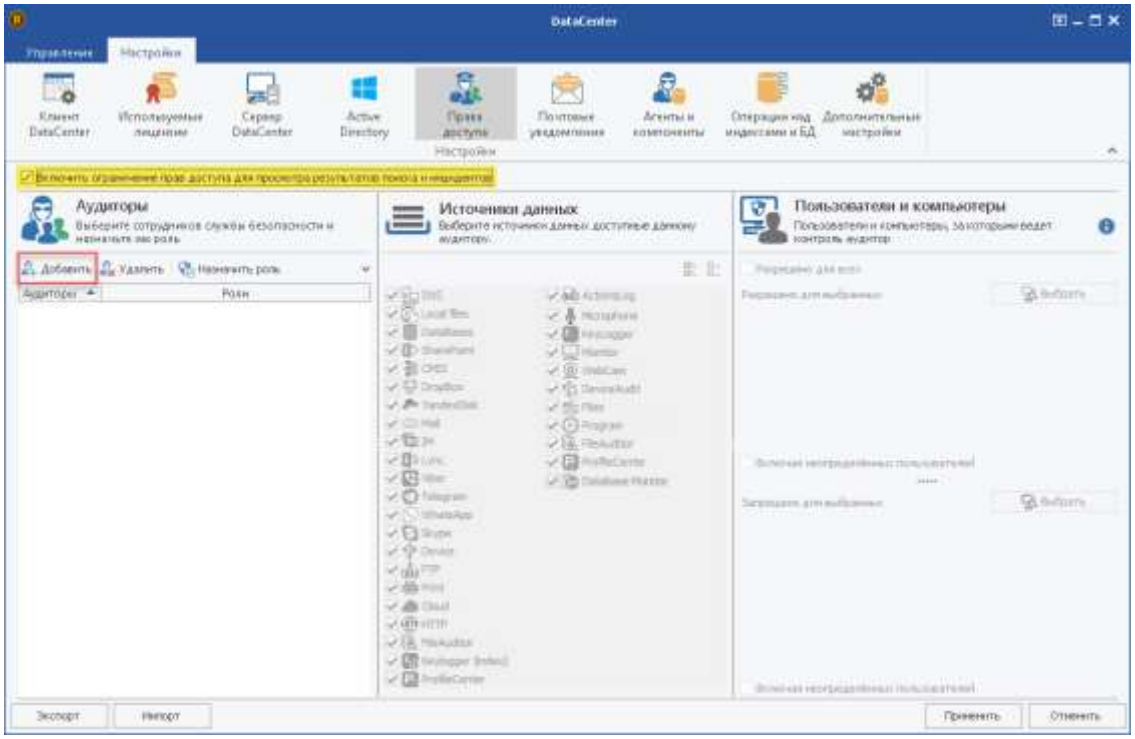


Рисунок 6.11

По умолчанию в системе предустановлены роли **Admin**, **Viewer, DirectReports**[11]. Каждому добавленному аудитору присваивается роль **Viewer**, которая, при необходимости, может быть изменена. Выбранных ролей может быть несколько (см. Рисунок 6.12).

Окно со списком доступных ролей может быть вызвано:

[11] Роль **DirectReports** назначается руководителям отделов. Она предоставляет доступ к просмотру Web-отчетов по подчиненным своего отдела.

- двойным кликом по имени аудитора,
- кликом по иконке,
- из контекстного меню.

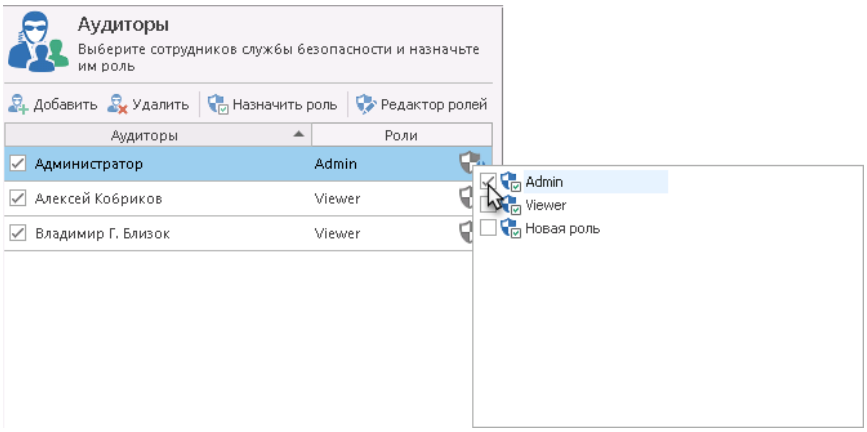


Рисунок 6.12

Если имеющихся по умолчанию ролей/прав недостаточно, воспользуйтесь редактором ролей.

6.1.3.2 Выбор источников данных

В области «Источники данных» отметьте флажками продукты, данные которых доступно мониторить выбранному сотруднику службы безопасности. Для руководителя отдела ИБ может быть разрешен просмотр журнала действий (**ActionsLog**) остальных сотрудников отдела (см. Рисунок 6.13).

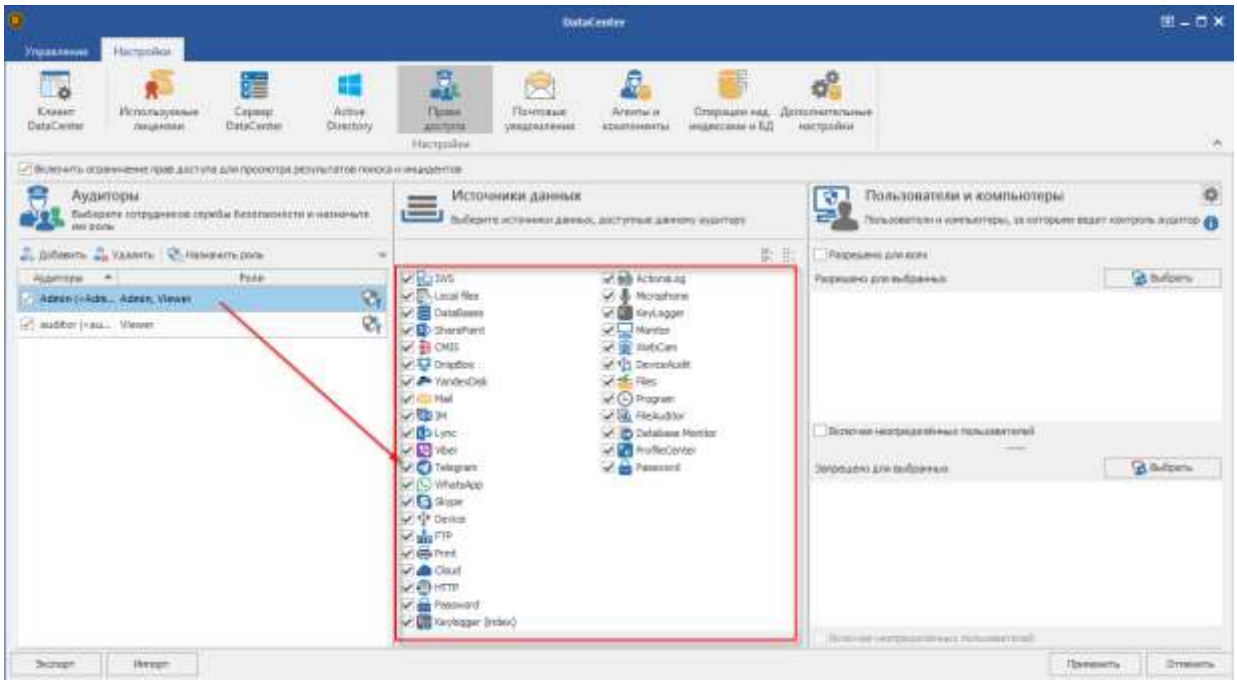


Рисунок 6.13

6.1.3.3 Настройка прав аудитора

По умолчанию, каждому аудитору разрешен просмотр данных по всем пользователям.

Настройте режим доступа для выбранного сотрудника службы безопасности:

- При установленном флажке **«Разрешено для всех»** аудитор имеет доступ к данным всех пользователей/компьютеров, кроме тех, что указаны в области **«Запрещено для выбранных»** (см. Рисунок 6.14).

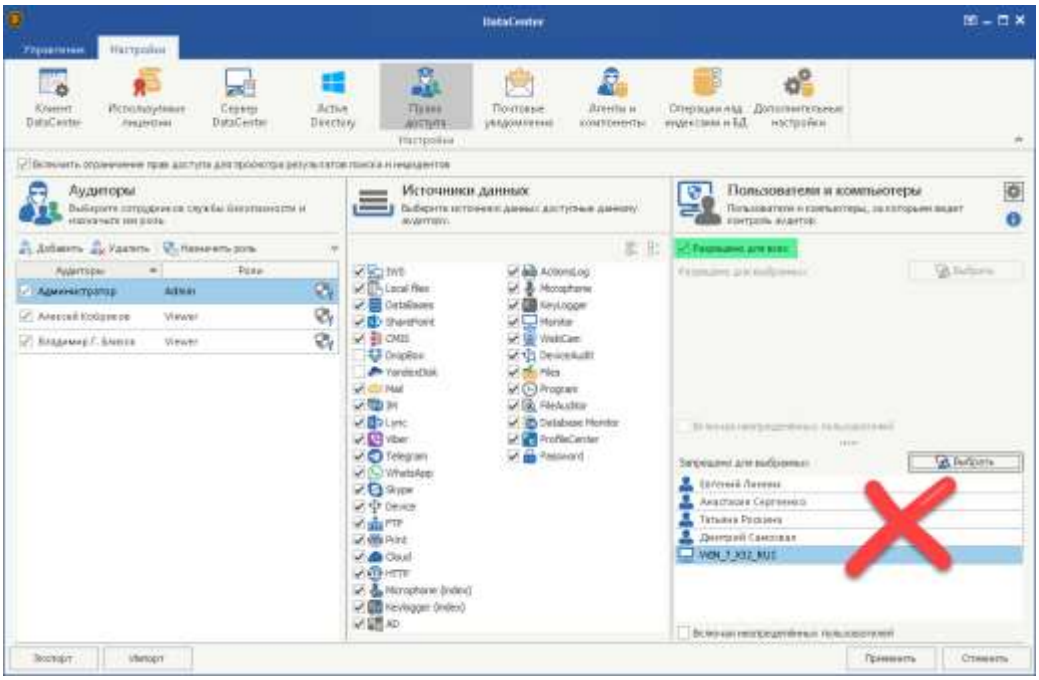


Рисунок 6.14

- При снятом флажке **«Разрешено для всех»** аудитор имеет доступ к данным только тех пользователей/компьютеров, которые будут выбраны из списка. Флажок «Включая неопределенных пользователей» предоставляет возможность просматривать документы пользователей, доменное имя которых системе не удалось определить и помечено как «unknown» (см. Рисунок 6.15).

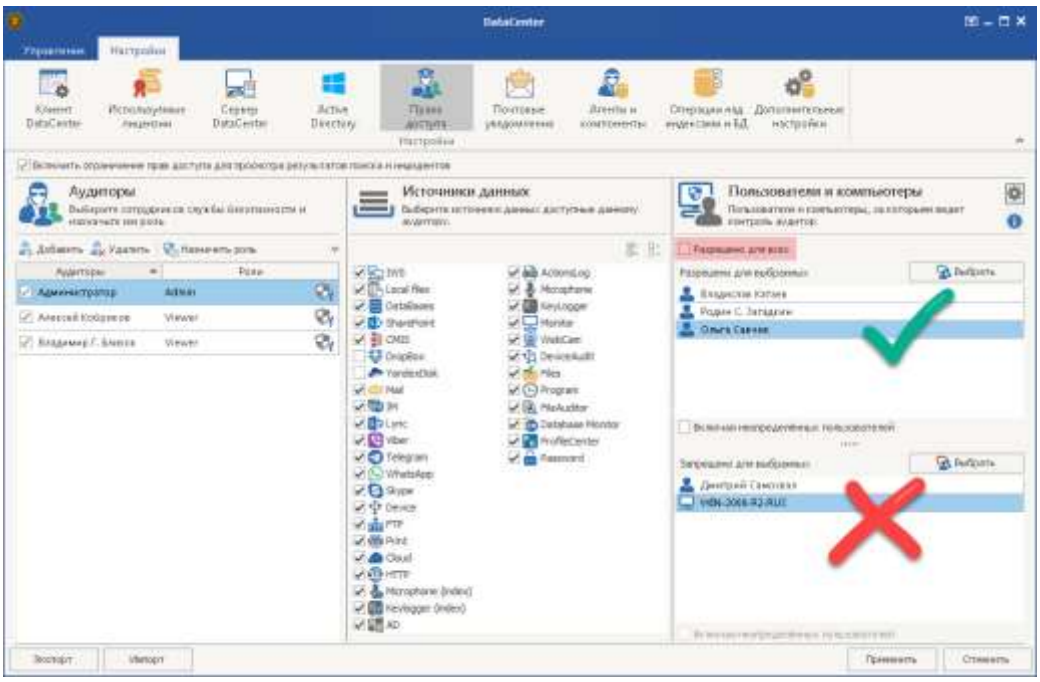


Рисунок 6.15

Для добавленных в список **имен компьютеров** ограничения будут применены только в отношении документов, проиндексированных на рабочих станциях пользователей, и отчетов по EndpointController, доступных в AnalyticConsole на вкладке «Отчеты» отчеты по установленному ПО, истории установки ПО, истории установки агентов на рабочие станции).

Доступны также дополнительные настройки по пользователям, вызываемые кликом по иконке  :

- Не добавлять в список пользователей из групп, находящихся внутри выбранных организационных подразделений (OU) Active Directory;
- Автоматически выдавать руководителям отделов права просмотра веб-отчетов ReportCenter по своим подчиненным и, в свою очередь, их подчиненным. Данный параметр работает в том случае, когда руководитель отсутствует в списке аудиторов. Право просмотра отчетов по собственным данным у него отсутствует (см. Рисунок 6.16).

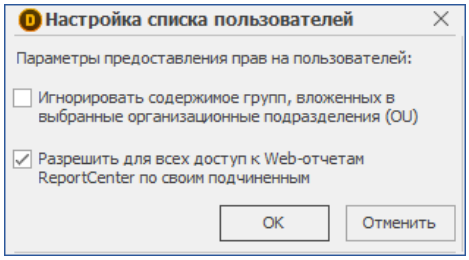


Рисунок 6.16

Сохраните изменения, щелкнув кнопку «Применить».

6.1.4 Настройка путей к архивам и параметров использования дискового пространства

Щелкните кнопку «Сервер DataCenter», расположенную на вкладке «Настройки».

Выберите уровень логирования работы сервера DataCenter.

Настройте параметры дискового пространства на серверах управляемых компонентов, при несоблюдении которых DataCenter будет оповещать аудитора (см. Рисунок 6.17). Настраиваемые условия:

- Свободное место на жестком диске ниже заданной величины (задается в ГБайтах или в процентах от общего объема). Данный критерий применяется по отношению ко всем доступным внутренним и внешним (USB HDD) накопителям.
- Объем файлов журналирования, журнала производительности и файлов сохраненного трафика превышает заданную величину (задается в ГБайтах).

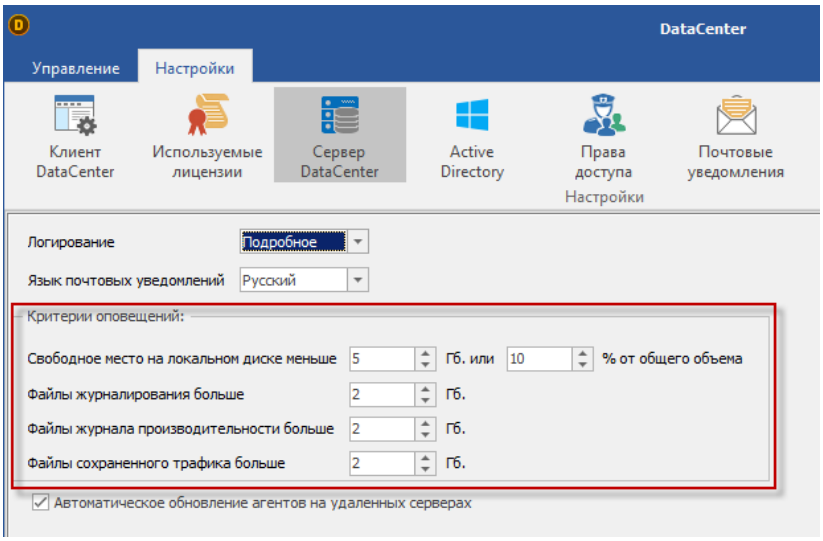


Рисунок 6.17

Для активации опции автоматического обновления агентов DataCenter[12], установленных на серверы управляемых компонентов Серчинформ ДЛП, отметьте соответствующий параметр флажком (по умолчанию флаг установлен).

Щёлкните кнопку «Применить» в нижней части окна.

6.1.5 Управление продуктами: принудительный и плановый запуск компонентов

Запуск компонентов может осуществляться в двух режимах:

1. Автоматический (принудительный запуск);

[12] Обновление возможно для агентов версии DataCenter не ниже 2.30.2.4.

2. Плановый (запуск по настроенному расписанию).

Щёлкните кнопку «Агенты и компоненты», расположенную на вкладке «Настройки». Разверните список установленных компонентов, щелкнув по иконке слева от имени сервера. Нажмите кнопку для настройки запуска служб продукта.

Для автоматического запуска служб выбранного компонента в появившемся окне установите ***флаг*** **«Запускать принудительно»** (см. Рисунок 6.18). Щелкните «Сохранить».

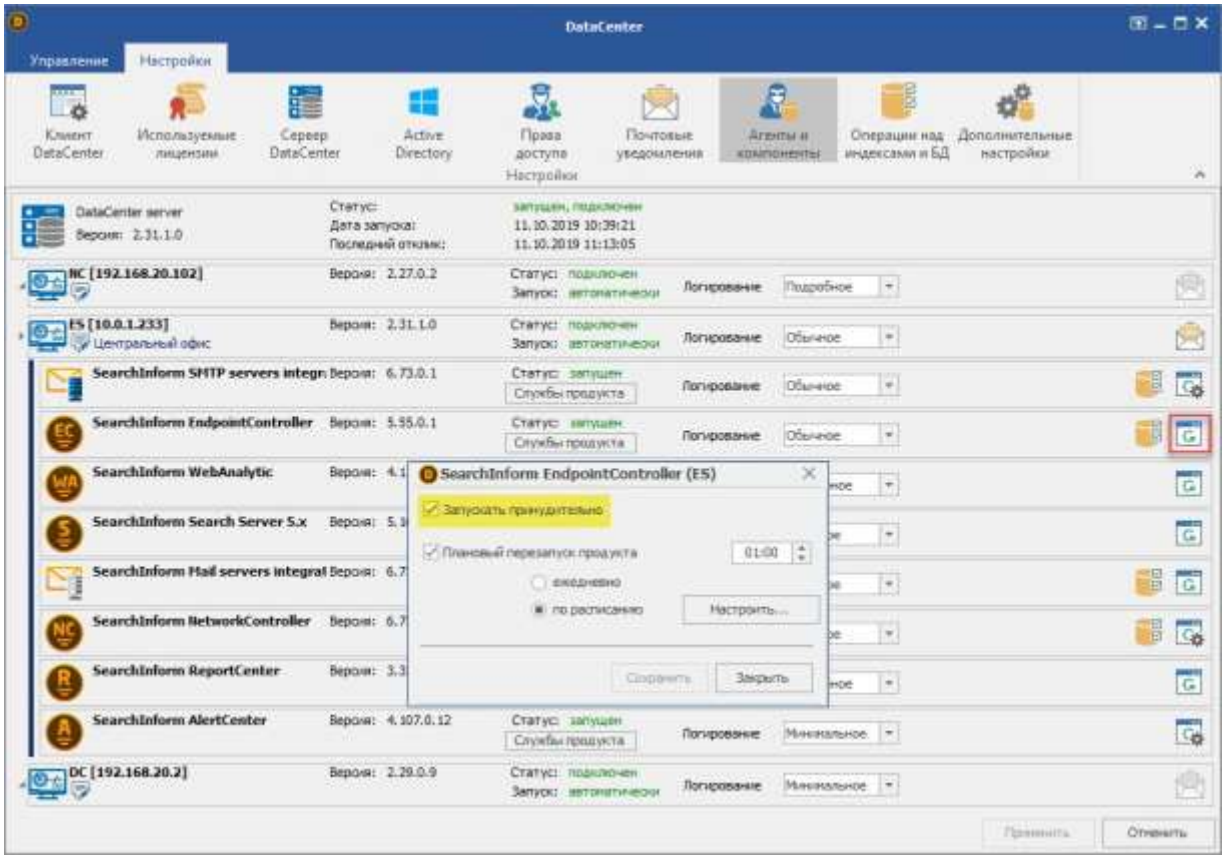


Рисунок 6.18

Если параметр «Запускать принудительно» не отмечен флажком, то на вкладке «Управление» будет активна кнопка «Запустить/Остановить» (в зависимости от статуса компонента) для запуска/остановки службы компонента вручную (см. Рисунок 6.19).

Рисунок 6.19

Для запуска служб продукта согласно расписанию, установите ***флаг «Плановый перезапуск продукта»*** и настройте условия перезапуска:

- ежедневно – для ежедневного перезапуска продукта в установленное время;

- по расписанию – для задания расписания нажмите кнопку «Настроить…» и в окне планировщика укажите даты, по которым необходимо запускать продукт (см. Рисунок 6.20).

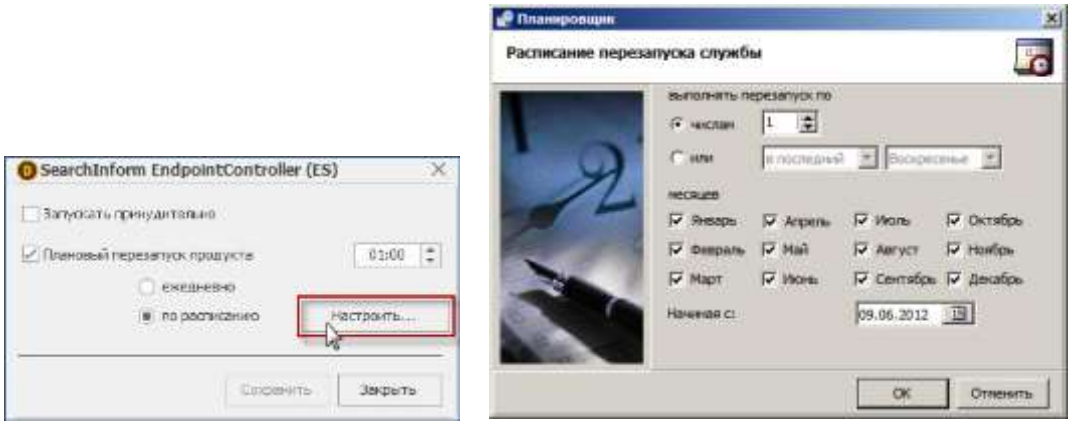


Рисунок 6.20

Щелкните «Сохранить».

После сохранения изменений иконка  примет вид  .

Примените настройки кнопкой «Применить».

6.1.6 Настройка правил создания и удаления индексов и баз данных

Все автоматические операции над индексами и базами данных будут осуществляться лишь в случае, когда активирован параметр «Запускать принудительно»[13] напротив соответствующего продукта (см. п. 6.1.5).

Щёлкните кнопку «Операции над индексами и БД», расположенную на вкладке «Настройки».

Установите флажок «Автоматически создавать индексы по достижении условий:» и настройте условия, по достижении которых создаются новые индексы (см. Рисунок 6.21). Для этого, отметьте флажками критерии, на которые будет распространяться операция. Доступные критерии:

- максимальный размер индекса (Гбайт);
- максимальный размер перехваченных документов (Гбайт);
- максимальный размер перехваченных документов в базе данных (Гбайт);
- максимальный размер текста перехваченных документов (Гбайт);
- максимальное число перехваченных документов (млн.);
- максимальное число записей в базе данных (млн.);
- максимальное число уникальных слов (млн.);

[13] Отметка флажком параметра «Запускать принудительно» активирует опцию «Автоматическое управление» продуктом.

- максимальный возраст индекса (дней).

Дополнительно установите время суток, в которое будет производиться операция. Для этого установите флажок «только в промежутке времени» и настройте удобное для операции время, например, нерабочие часы.

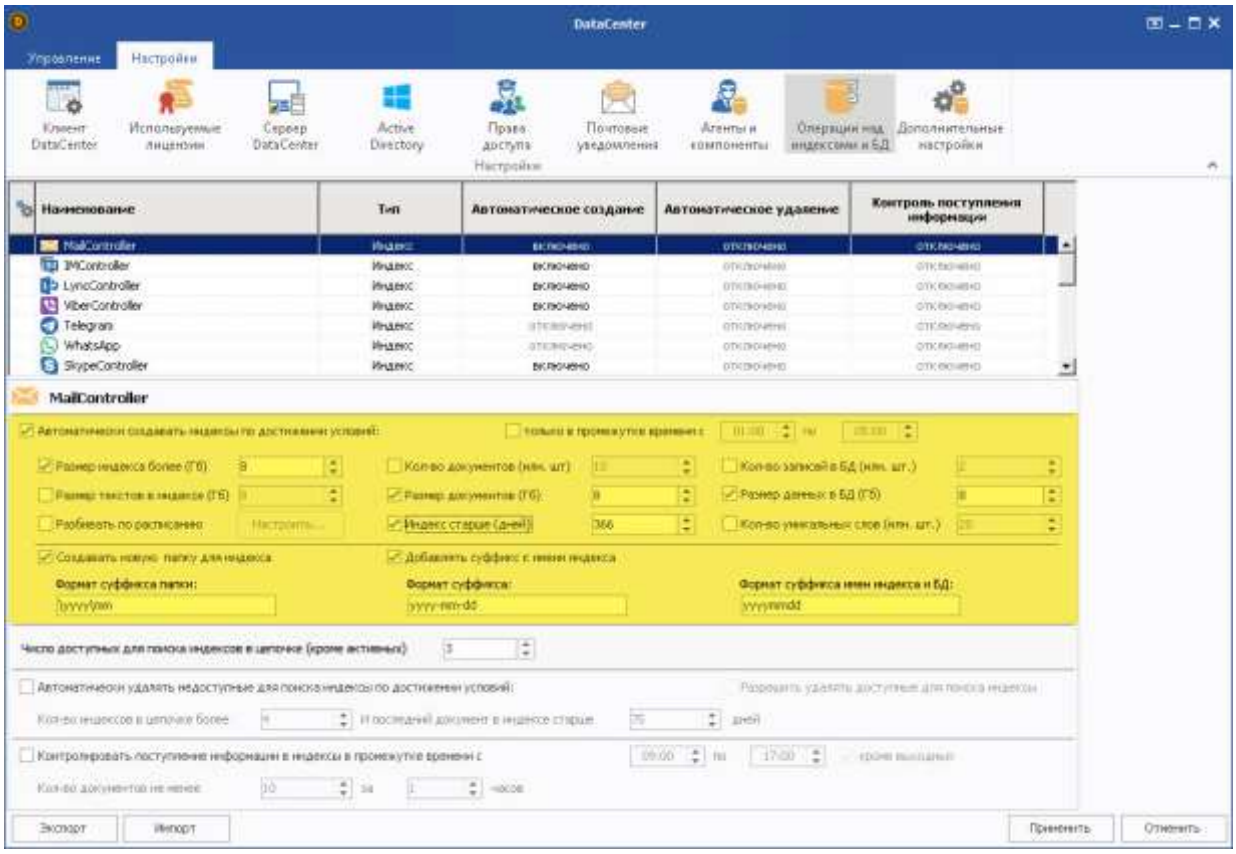


Рисунок 6.21

Другой возможный подход – создание индексов/БД по расписанию. Для этого установите флажок «Разбивать по расписанию» и щелкните кнопку «Настроить». Для формирования ежемесячного расписания, осуществите следующие настройки (см. Рисунок 6.22):

- «разбивать индексы по» - «числам», **1**;
- «месяцы» – выделите все;
- «Начиная с» – укажите дату первой операции.

Щёлкните «ОК».

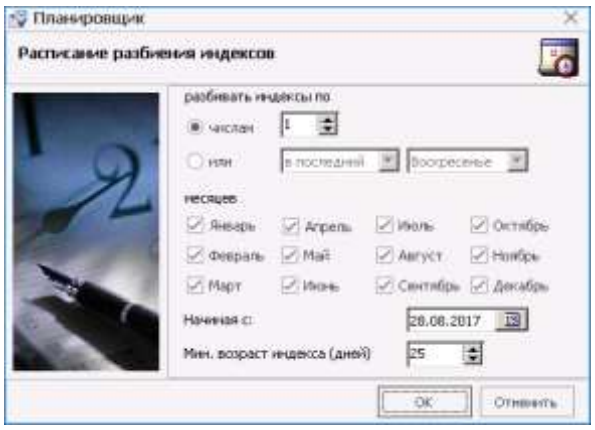


Рисунок 6.22

Укажите количество доступных для поиска индексов/БД в цепочке (кроме активных). Активные индексы/БД, в которые на данный момент сохраняются перехваченные документы, не учитываются.

Существует также возможность настроить условия, при наступлении которых недоступные для поиска индексы/БД будут автоматически удалены. Для этого активируйте параметр «Автоматически удалять недоступные для поиска индексы/БД по достижении условий». Задайте число индексов в цепочке, при превышении которого самый старый индекс может быть удален, и количество дней с момента индексации последнего документа в индексе (см. Рисунок 6.23).

Индекс/БД будет удален(а) только по достижении обоих условий одновременно.

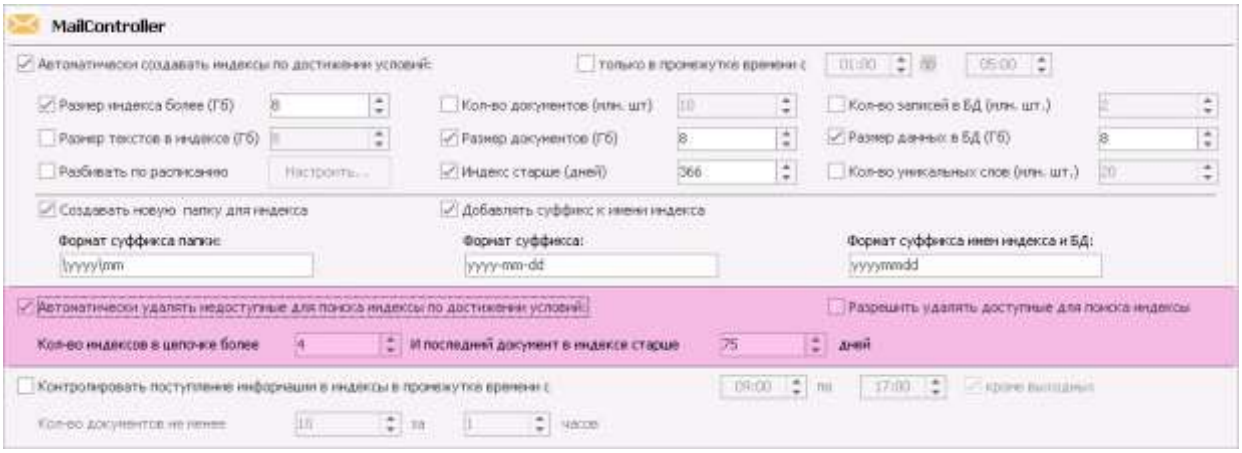


Рисунок 6.23

Для применения настроек удаления в том числе к индексам, доступным для поиска, установите флажок «Разрешить удалять доступные для поиска индексы». Активные и бонусные индексы не могут быть автоматически удалены.

Примените настройки, щелкнув кнопку «Применить».

6.1.6.1 Переопределение настроек автоматического управления индексами и БД

Серверов компонентов Серчинформ ДЛП в сети может быть установлено несколько, и разные серверы контролируют свои модули перехвата. Соответственно, для каждого сервера Серчинформ ДЛП могут быть заданы свои настройки управления индексами и базами данных продуктов.

Переопределение настроек серверов производится на вкладке «Агенты и компоненты». Разверните список компонентов сервера Серчинформ ДЛП и для требуемого компонента щелкните кнопку  (см. Рисунок 6.24).

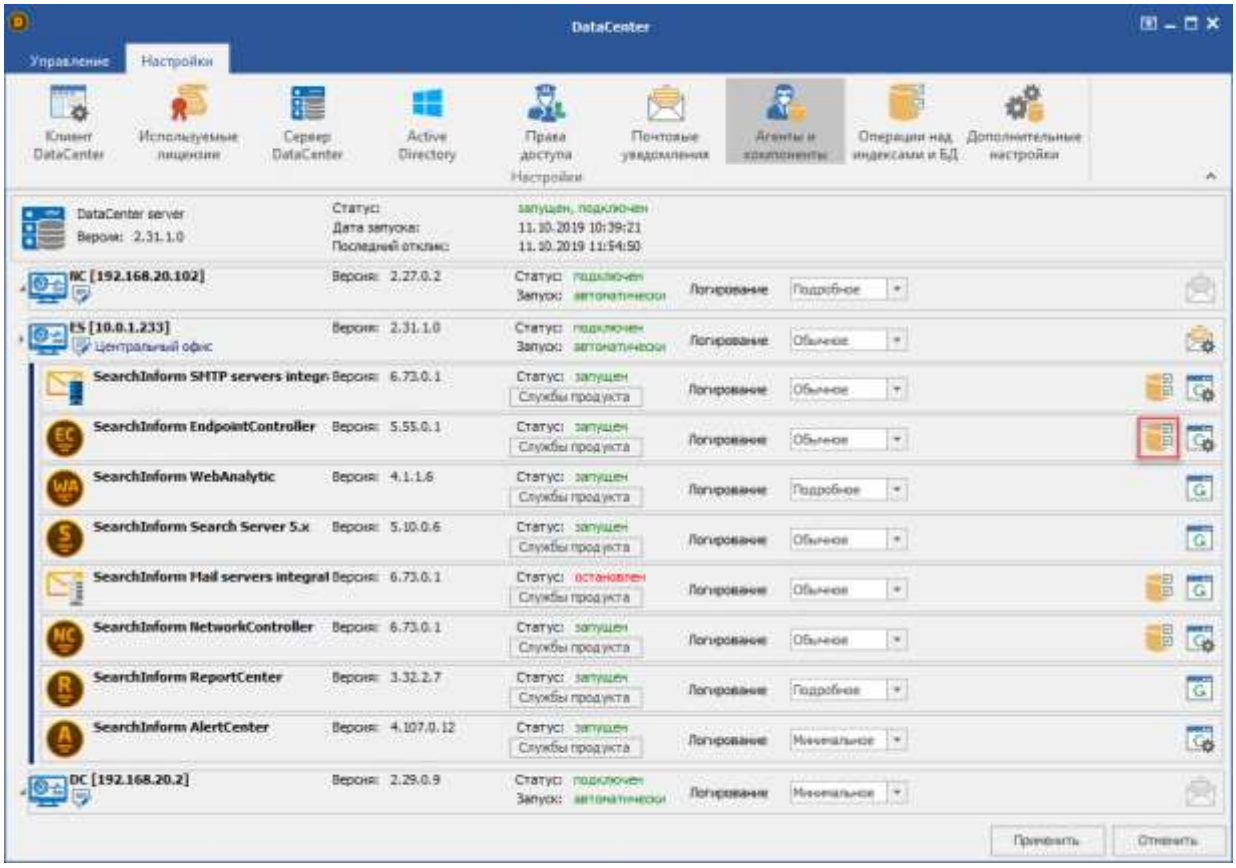


Рисунок 6.24

Переопределите настройки необходимых индексов/БД. Параметры, доступные в отобразившемся диалоговом окне, идентичны настройкам, описанным в п. 6.1.6 настоящего документа (см. Рисунок 6.25).

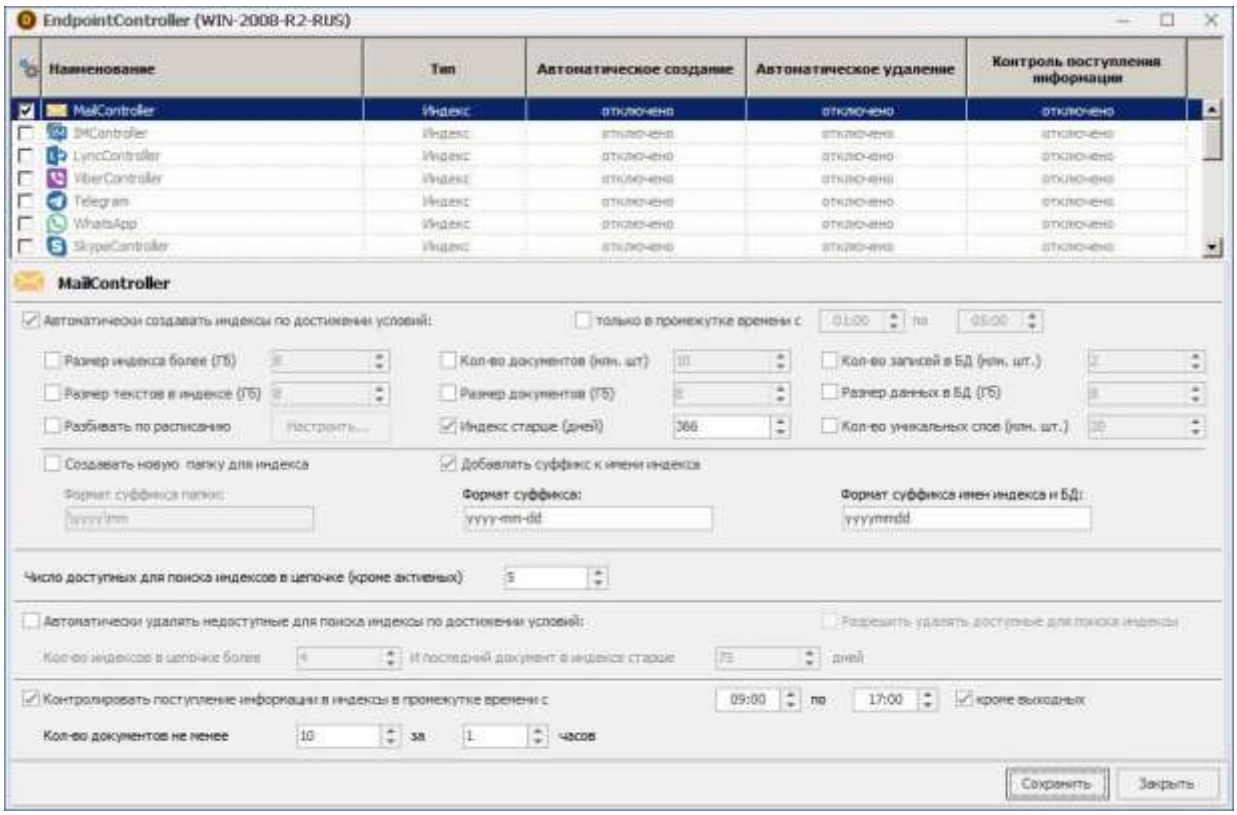


Рисунок 6.25

В рамках данного примера, сделанные настройки будут применены только к почтовым индексам компонента EndpointController, установленного на сервере WIN-2008-R2-RUS. Для остальных индексов электронной почты будут по-прежнему действовать глобальные настройки вкладки «Операции над индексами» (если они заданы).

6.1.7 Настройка почтовых уведомлений

Отправка почтовых уведомлений от продуктов Серчинформ ДЛП осуществляется через сервер DataCenter.

Для настройки параметров отправки уведомлений щёлкните кнопку **«Почтовые уведомления»**, расположенную на вкладке «Настройки».

Установите флаг «Отправлять отчеты по почте» и настройте параметры уведомлений (см. Рисунок 6.26):

- Отправитель уведомлений – адрес SMTP-сервера, SMTP-порт, адрес электронной почты. В случае необходимости, установите флажок «Авторизация на сервере» и введите имя и пароль учетной записи.
- Типы сообщений – отметить все.
- Кому отправлять – введите адрес в верхнее поле. Введенный адрес будет использован по умолчанию для всех уведомлений.

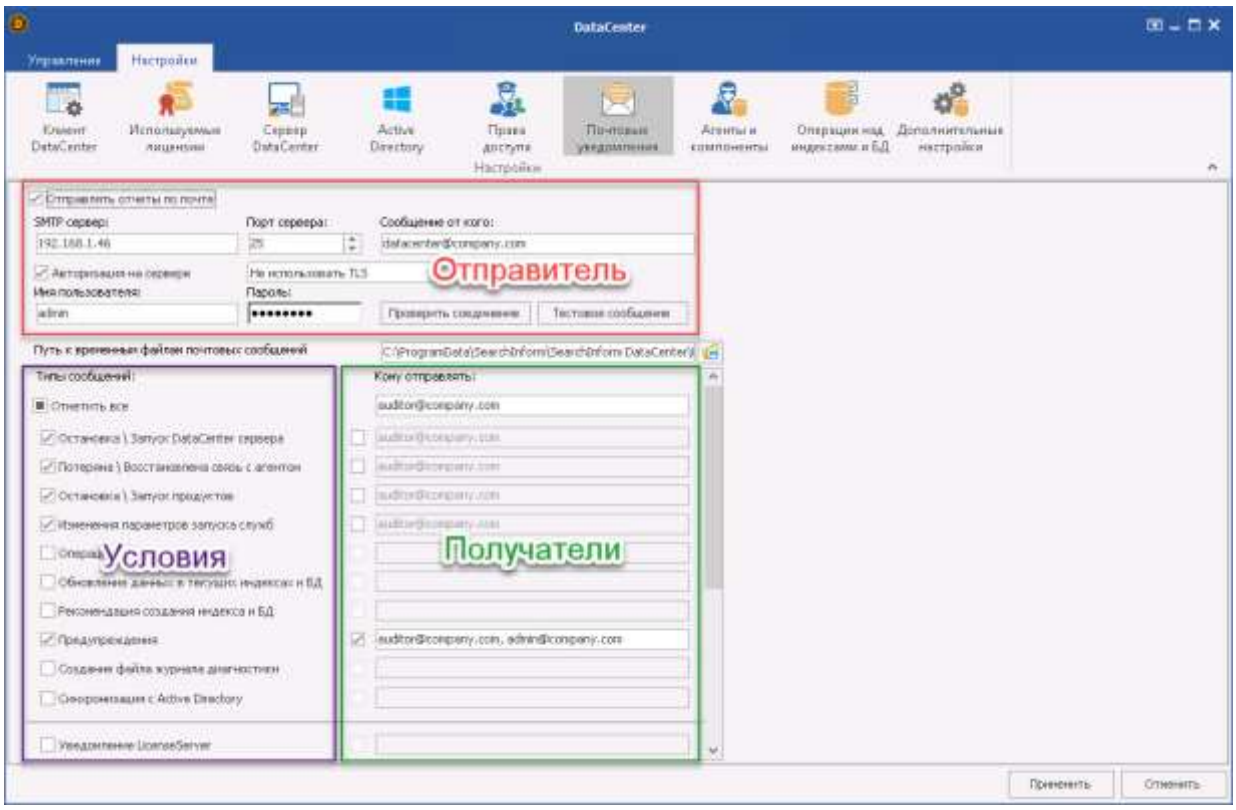


Рисунок 6.26

Щёлкните кнопку «Применить».

6.1.7.1 Отправка уведомлений службой MailService

Существует возможность отправления SMTP- уведомлений с помощью службы MailService, не используя при этом сервер DataCenter. На данный момент функционал актуален **только для продукта ProfileCenter**.

Для индивидуальной настройки отправки почтовых уведомлений через службу щёлкните кнопку «Агенты и компоненты» на вкладке «Настройки». Вызовите окно настроек SMTP-сервера, нажав кнопку  (см. Рисунок 6.27).

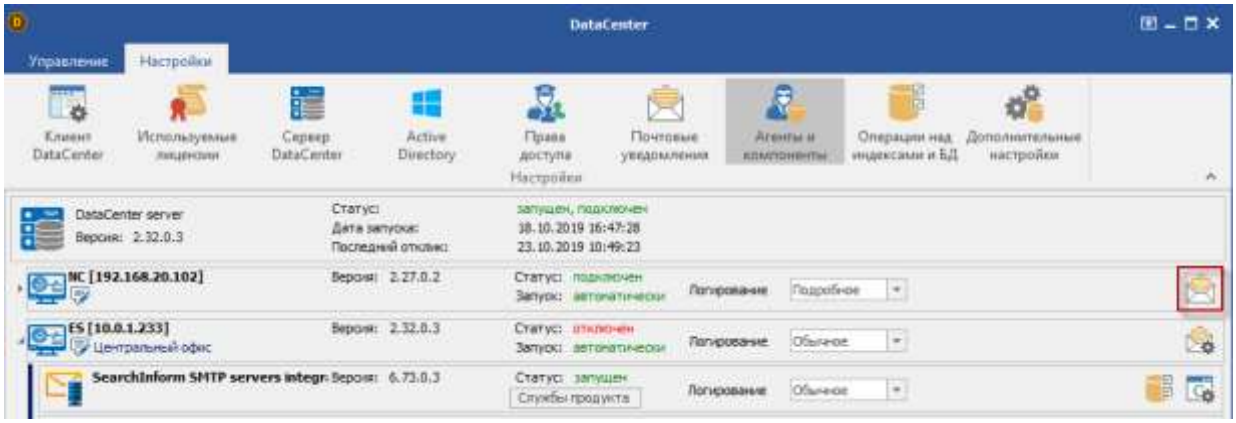


Рисунок 6.27

В появившемся окне установите флажок напротив параметра «Использовать следующие настройки для отправки почтовых уведомлений» и задайте настройки, отличные от тех, что были сформированы ранее на вкладке «Почтовые уведомления»:

- Имя или IP-адрес SMTP-сервера;
- Номер используемого сервером порта;
- Адрес отправителя уведомлений (см. Рисунок 6.28).

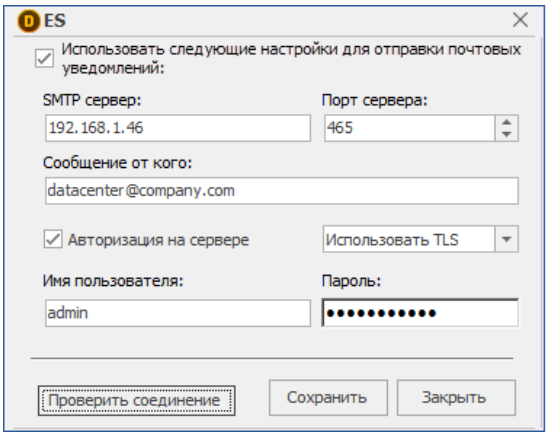


Рисунок 6.28

При необходимости авторизации на SMTP-сервере отметьте параметр «Авторизация на сервере», введите имя и пароль почтовой учетной записи.

Сохраните изменения. Затем нажмите кнопку «Применить» в нижней части окна.

6.1.8 Задание баз данных по умолчанию

DataCenter позволяет задать настройки для подключения к базам данных под управлением СУБД MS SQL и/или PostgreSQL.

Для установки настроек подключения перейдите на вкладку **«Настройки»** и щелкните кнопку **«Дополнительные настройки»**.

На вкладке **«Базы данных по умолчанию»** нажмите кнопку «Добавить» для добавления сервера баз данных в список.

Выберите тип сервера СУБД в выпадающем списке, после этого укажите имя сервера баз данных и задайте параметры подключения к серверу:

- Тип используемой для подключения учетной записи (Windows/внутренняя учетная запись);
- Имя пользователя и пароль (при выборе внутренней аутентификации SQL Server).

Проверить подключение к серверу можно нажатием кнопки «Проверка подключения». После этого щелкните кнопку «Добавить» (см. Рисунок 6.29).

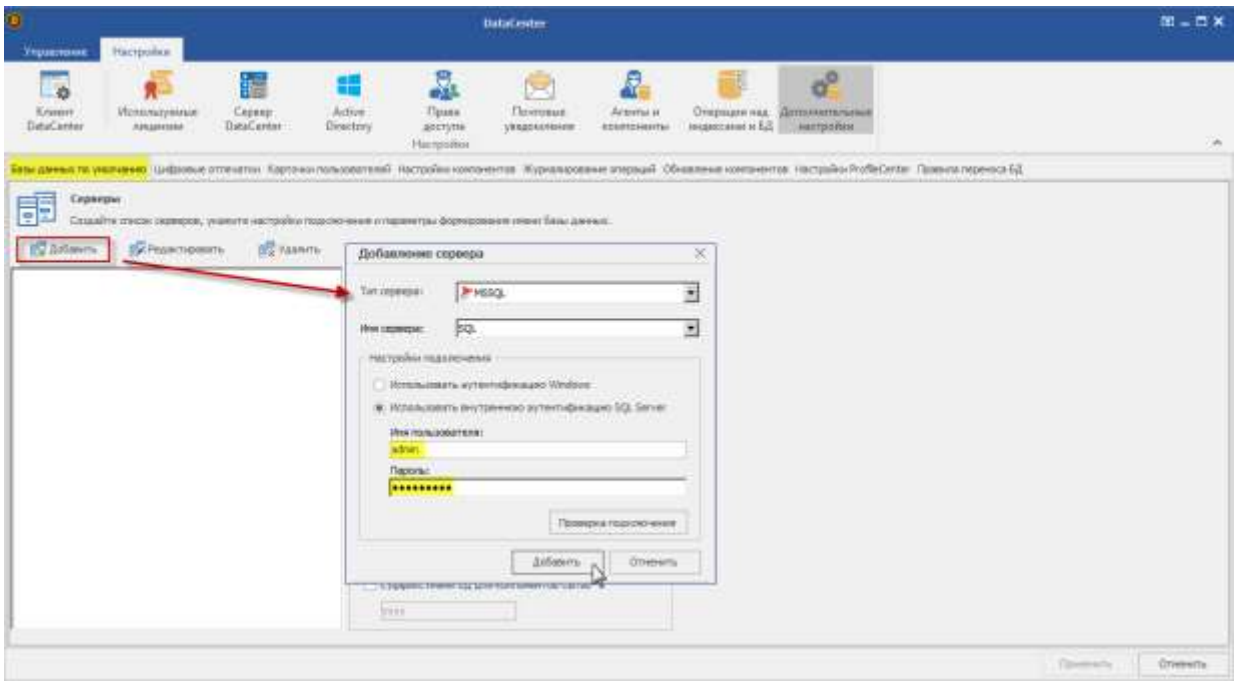


Рисунок 6.29

Добавленный сервер отобразится в списке слева.

Для редактирования параметров подключения к сереру используйте кнопку **«Редактировать»**, для удаления сервера из списка – кнопку **«Удалить»** (см. Рисунок 6.29).

Когда серверов в списке несколько, один из них может использоваться по умолчанию. Выделите сервер, примените из контекстное меню команду «Использовать по умолчанию». После этого сервер, назначенный сервером по умолчанию, обозначается маркером «*» (см. Рисунок 6.30).

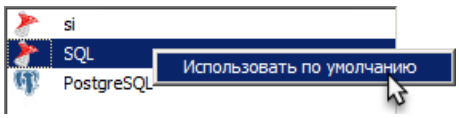


Рисунок 6.30

Справа от списка серверов в группе параметров созданного сервера «MS SQL» предложены параметры для генерирования имени создаваемой базы данных (см. Рисунок 6.31), а именно:

- возможность добавления указанного префикса перед наименованием создаваемой БД;
- определение идентификатора сервера, на котором установлен компонент (актуально, когда в системе установлено несколько серверов данного компонента);
- выбор суффикса, добавляемого к имени БД (в зависимости от компонента).

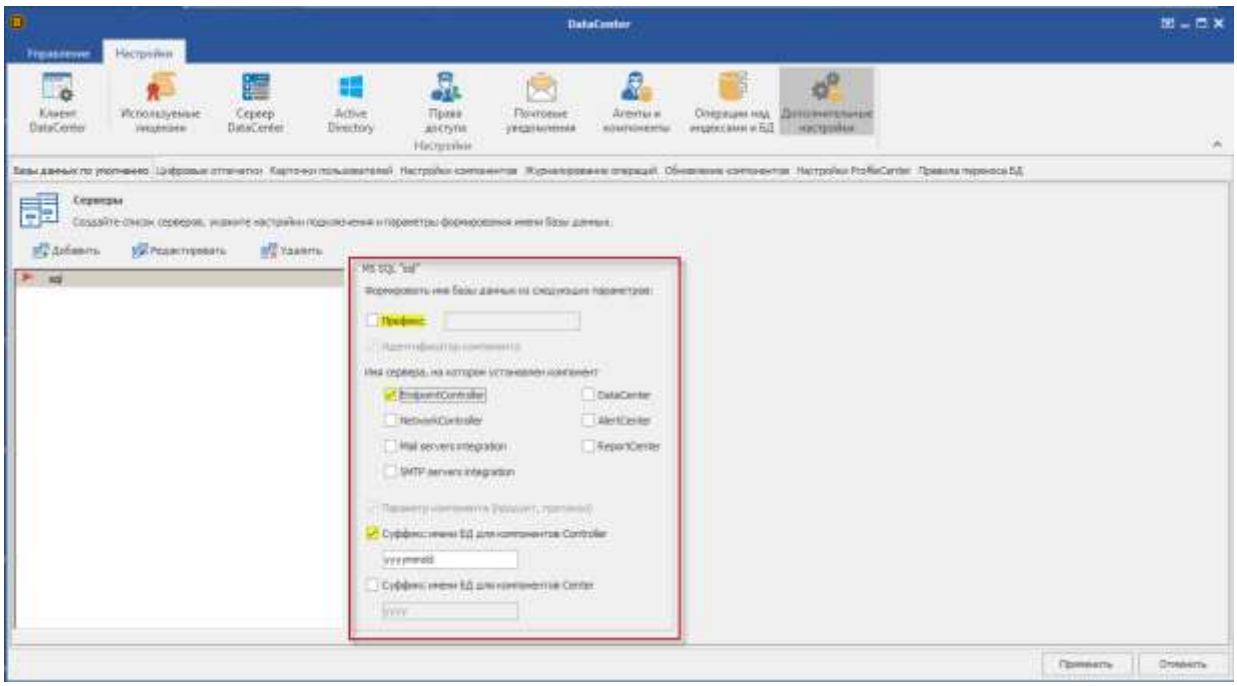


Рисунок 6.31

Конечный вариант имени БД можно отредактировать вручную.

Сохраните изменения, нажав кнопку «Применить».

6.1.9 Настройка библиотеки цифровых отпечатков

Для работы с цифровыми отпечатками необходимо создать каталог образцов документов (либо использовать уже имеющийся) в консоли клиента Серчинформ DataCenter.

Перейдите на вкладку **Настройки → Дополнительные настройки** и нажмите кнопку «Цифровые отпечатки». В текстовом поле введите путь к каталогу и щёлкните кнопку «Добавить» (см. Рисунок 6.32).

Рисунок 6.32

Указать нужный каталог также можно с помощью обозревателя, нажав  . В появившемся окне выерите папку и нажмите «ОК» (см. Рисунок 6.33).

Рисунок 6.33

Каталог образцов цифровых отпечатков будет отображён в списке. Для изменения выбранной папки предназначена кнопка «Заменить», для удаления – «Удалить». При необходимости, настройте расписание индексации цифровых отпечатков. *При использовании Search Server версии 5.x настройка расписания индексации не требуется!* (см. Рисунок 6.34).

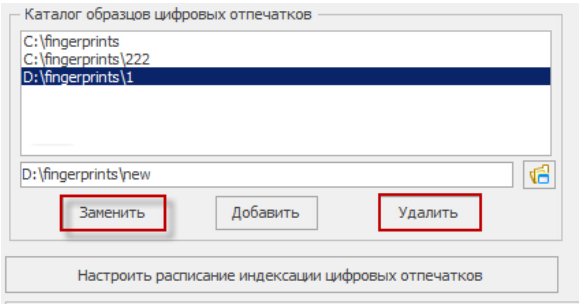


Рисунок 6.34

Установите флажок напротив сервера Search Server, который будет производить индексацию цифровых отпечатков. Щёлкните мышью по кнопке «Применить» в нижней части консоли (см. Рисунок 6.35).

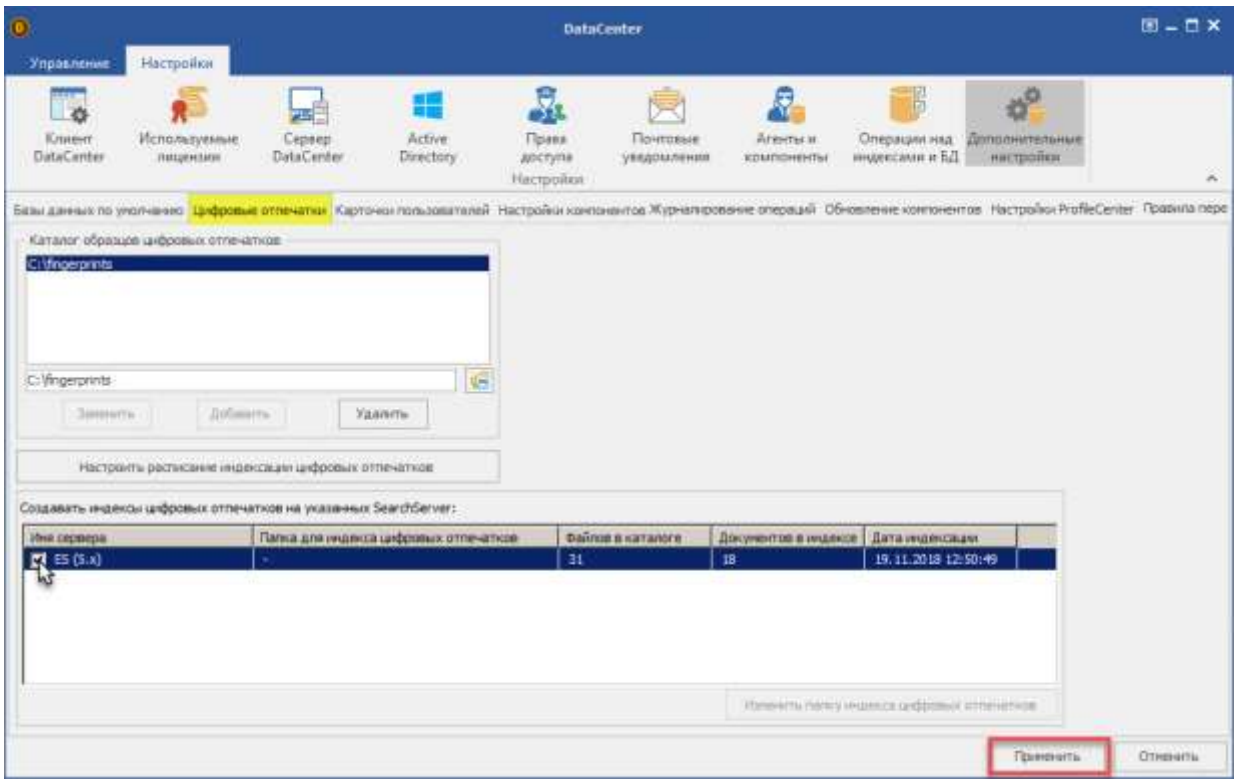


Рисунок 6.35

По истечении некоторого времени будет отображено количество файлов в каталоге образцов.

6.1.10 Настройка службы сбора данных

Служба сбора данных осуществляет извлечение из атрибутов документов выбранных индексов (почтовых, IM, Skype) контактных данных и привязку их к внутреннему пользователю компании или внешнему. Данные по внутренним пользователям извлекаются из базы данных DataCenter, которые, в свою очередь, были импортированы из Active Directory. В дальнейшем полученная информация используется для генерирования и отображения карточек пользователей в приложении Серчинформ AnalyticConsole.

Перейдите на вкладку **Настройки → Дополнительные настройки** и нажмите кнопку **«Карточки пользователей»**.

В блоке настроек «Расписание» укажите частоту загрузки пользователей из Active Directory и импорта данных из индексов (при необходимости, можно указать начальную дату для импортируемых индексов).

Выберите уровень логирования службы сбора данных.

Отметьте флажками индексы, из которых будет извлекаться информация. Если необходимо собирать данные всех индексов без исключения, установите флажок напротив параметра «Обрабатывать все доступные индексы (mail, skype, im, lync, viber, telegram, whatsapp)» (см. Рисунок 6.36).

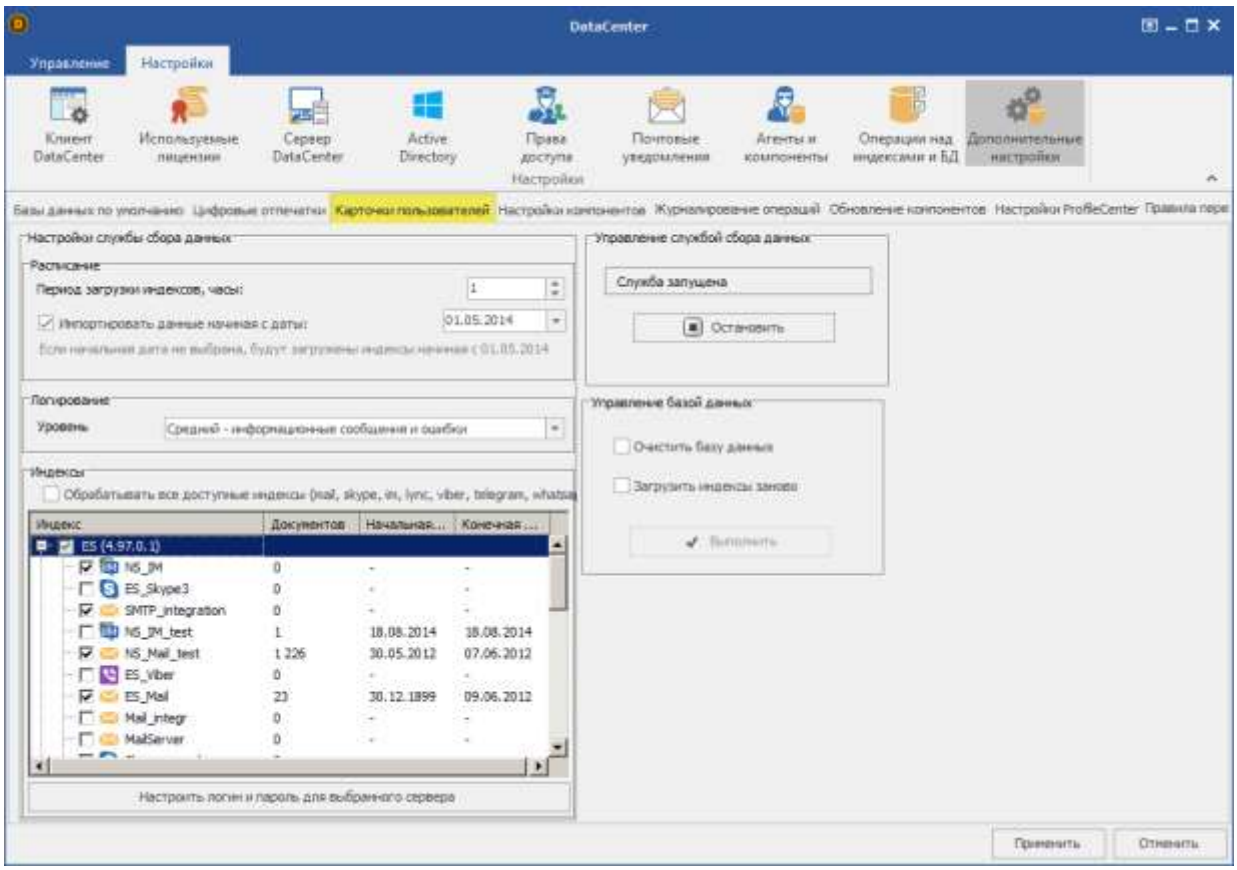


Рисунок 6.36

Управление службой сбора данных производится с помощью кнопок:

- **Остановить** – остановка работающей службы;
- **Запустить** – старт службы (если была отключена).

Управление базой данных производится с помощью следующих команд:

- **Очистить базу данных** – удаление извлеченной информации из базы данных DataCenter;
- **Загрузить индексы заново** – извлечение всех данных из индекса заново.

6.1.11 Настройка параметров прокси-сервера

При наличии в локальной сети прокси-сервера, укажите его параметры для корректной работы компонентов Серчинформ ДЛП.

Щелкните кнопку «Дополнительные настройки» на вкладке «Настройки».

Откройте вкладку «Настройки компонентов» (см. Рисунок 6.37).

Установите флажок «Использовать прокси» и укажите:

- IP-адрес либо полное имя прокси-сервера,
- номер используемого порта,
- имя пользователя и пароль (для прокси с авторизацией).

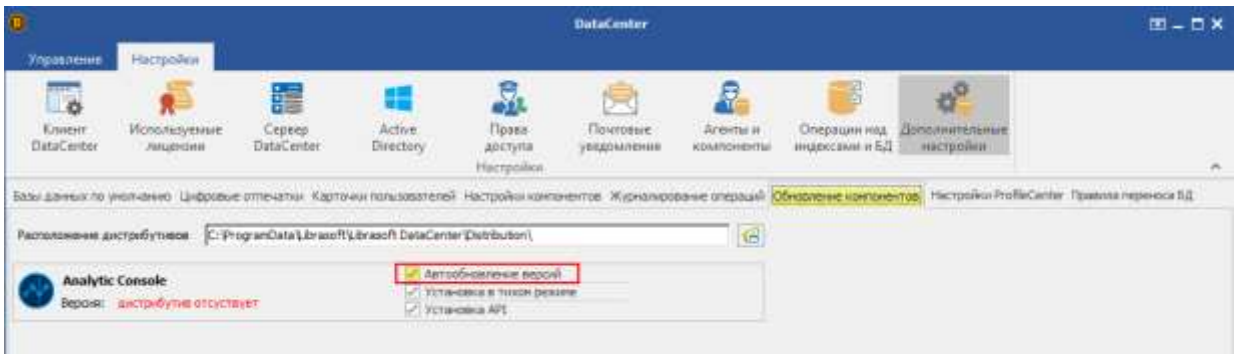


Рисунок 6.37

6.1.12 Отображение данных компании-разработчика в отчетах

Для скрытия/отображения данных компании-разработчика в отчетах WebAnalytic на вкладке **Настройки компонентов** задайте параметры:

- Имя компании (может отсутствовать или заменено именем Вашей компании);
- Иконка программного продукта (установите флаг для отображения иконки приложения, снимите флаг – для скрытия иконки приложения в отчетах);
- Логотип компании-разработчика (установите флаг для отображения логотипа, снимите флаг – для скрытия логотипа в отчетах) (см. Рисунок 6.38).

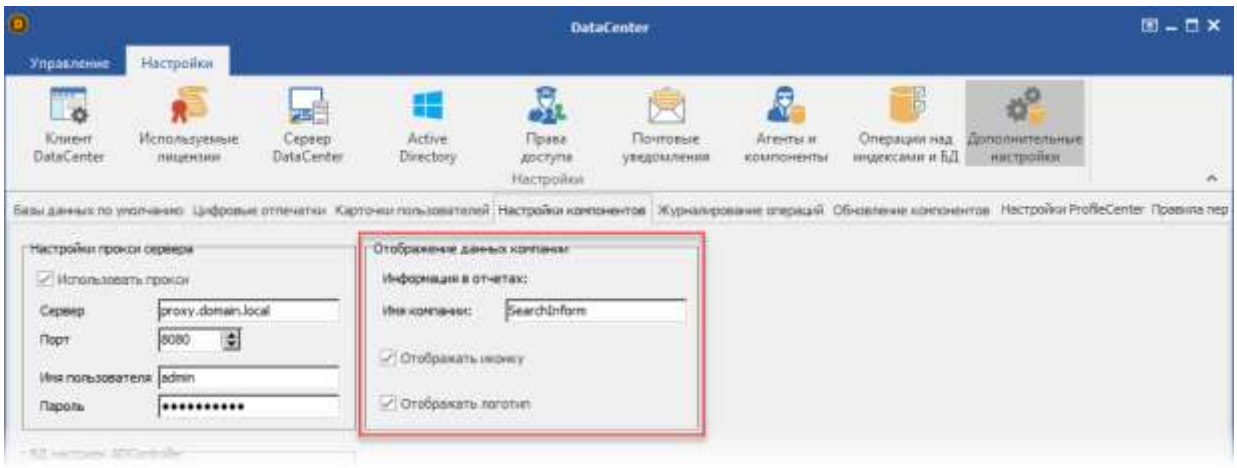


Рисунок 6.38

6.1.13 Настройка журналирования операций

Ведение журнала операций позволяет хранить историю действий сотрудников службы безопасности в консолях компонентов Серчинформ ДЛП. В базу данных попадают такие события, как добавление/изменение/удаление баз данных и индексов,

запуск поиска по источникам данных, добавление/удаление/изменение прав доступа, трансляция LiveView/LiveSound и др.

Перейдите на вкладку **Настройки → Дополнительные настройки** и щелкните вкладку **«Журналирование операций»** (см. Рисунок 6.39).

Установите флажок «Включить журналирование действий аудиторов в консолях продуктов» и настройте:

- подключение к базе данных, в которую будет вестись запись действий (см. Рисунок 6.39);
- язык журналирования операций;
- список консолей продуктов, действия в которых будут подвергаться журналированию.

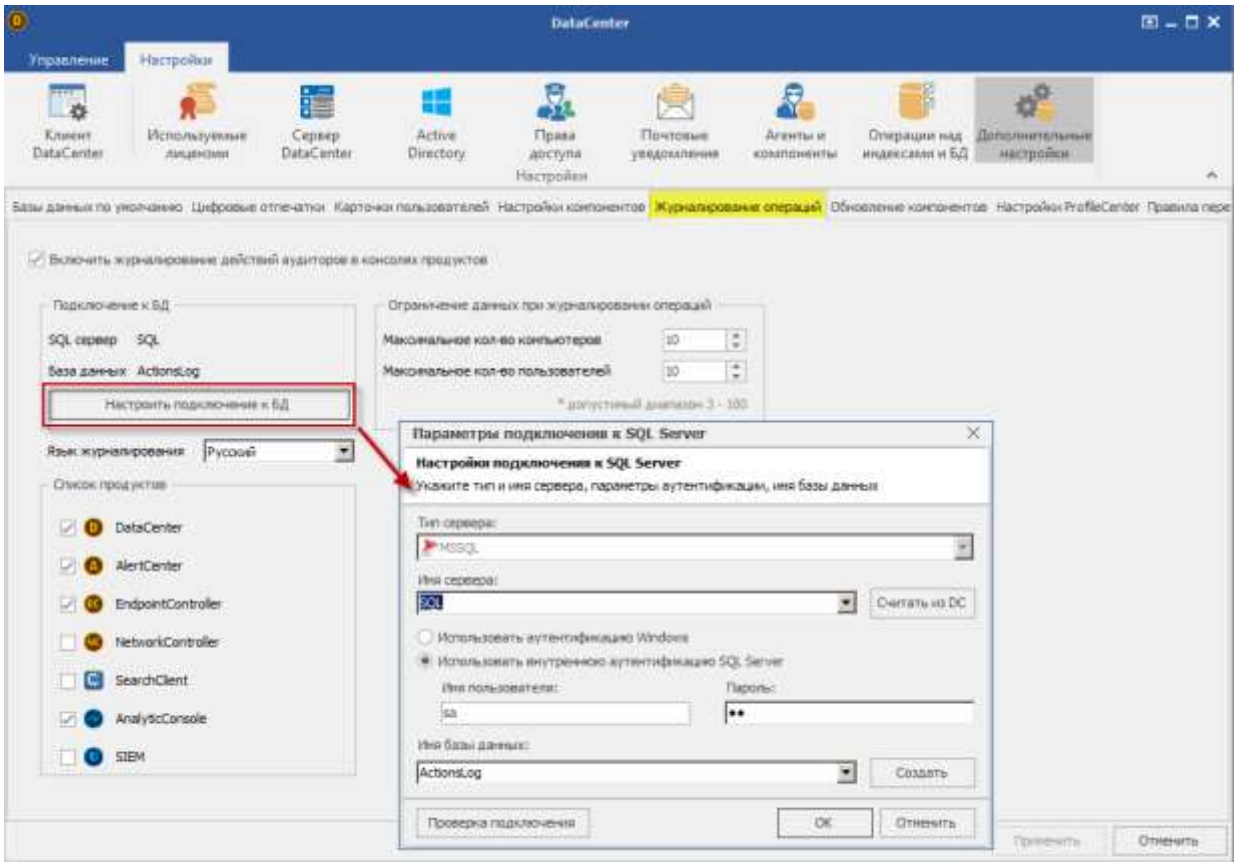


Рисунок 6.39

Установите также максимальное число компьютеров и пользователей, операции которых будут записаны в журнале.

Сохраните произведенные настройки, щелкнув кнопку «Применить».

6.1.14 Настройка автообновления компонентов

Автообновление позволяет добавить функционал новых версий продуктов при минимальном участии пользователя.

Перейдите на вкладку **Настройки** → **Дополнительные настройки** и щелкните вкладку **«Обновление компонентов».**

Укажите путь к папке, в которой располагаются дистрибутивы[14] новых версий. Папка может быть указана вручную в текстовом поле либо выбрана с помощью обозревателя нажатием кнопки .

Активируйте функционал автообновления, установив флажок напротив параметра **Автообновление версий.** Автообновление выполняется при наличии инсталлятора в заданной директории, в противном случае вместо в поле «Версия:» красным цветом выводится предупреждение об отсутствии дистрибутива. На текущий момент есть возможность настроить автоматическое обновление для AnalyticConsole[15] .

Флажок «Установка в тихом режиме» активирует установку новых версий данного приложения без взаимодействия польззователя с интерфейсом инсталлятора.

Флажок «Установка API» автоматически обновляет версию API при условии, что она установлена совместно с AnalyticConsole (см. Рисунок 6.40).

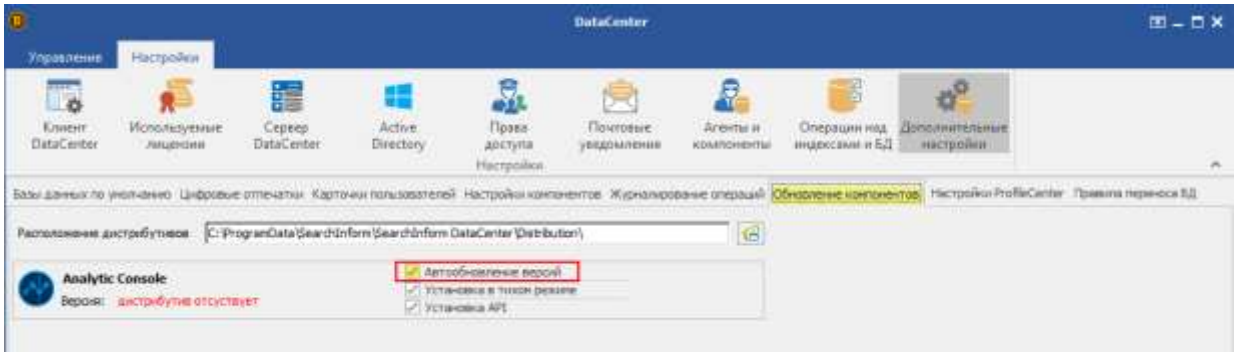


Рисунок 6.40

Сохраните произведенные настройки, щелкнув кнопку «Применить».

6.1.15 Настройка правил переноса баз данных

Для перемещения баз данных *MS SQL Server* в другие локальные хранилища в рамках одного сервера необходимо наличие установленной на сервере MS SQL **службы переноса баз данных**.

Настройка параметров переноса осуществляется на вкладке **Настройки** → **Дополнительные настройки** → **Правила переноса БД** (см. Рисунок 6.41).

[14] Дистрибутивы новых версий приложений могут быть загружены с официального сайта SearchInform или получены от инженера технической поддержки.

[15] Версия AnalyticConsole должна быть не ниже 1.24.0.13, версия DataCenter – не ниже 2.29.0.16.

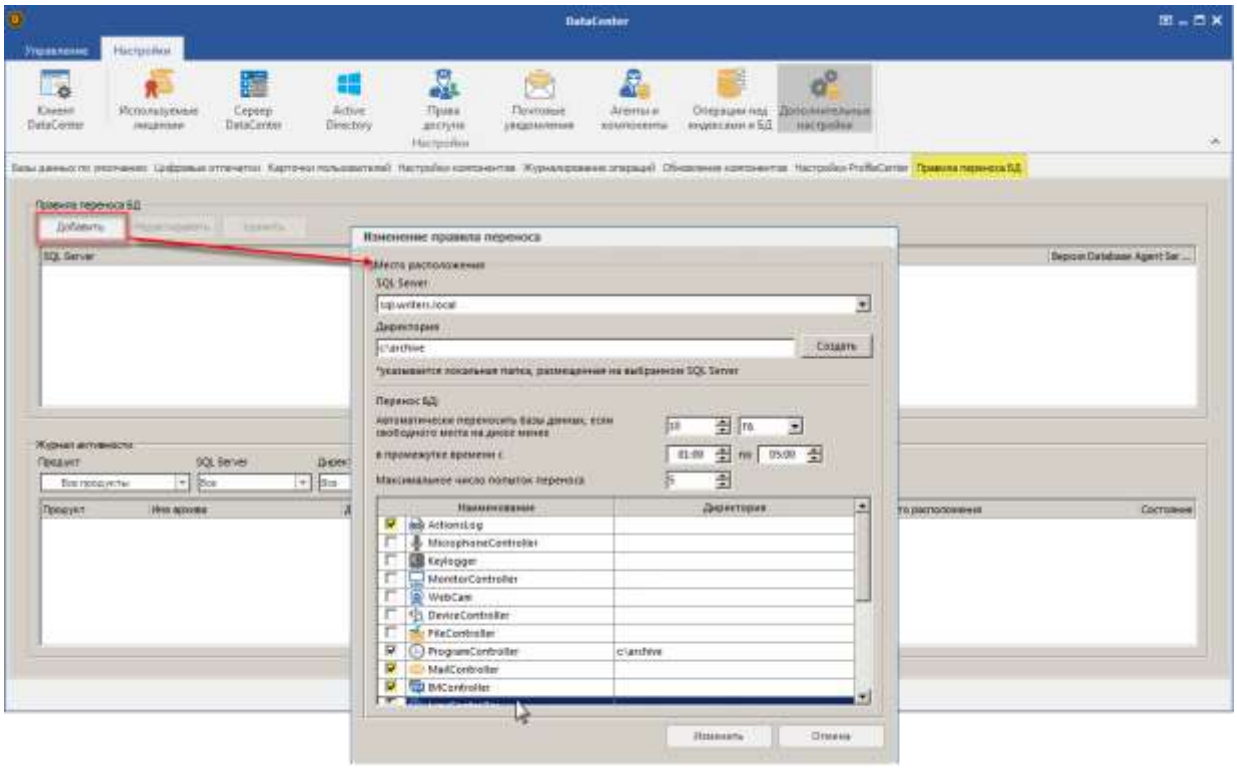


Рисунок 6.41

В появившемся окне укажите:

- Новое место хранения баз данных;
- Условия переноса баз данных;
- Продукт(ы), к базам данных которых будет применяться правило (только для баз продуктов, не имеющих индексов.

Перенос баз данных может осуществляться:

- в автоматическом режиме (с периодичностью 5 минут и согласно сформированным правилам),
- вручную (немедленный перенос БД настраивается отдельно для неактивных БД продуктов на вкладке «Управление» с помощью кнопки «Перенос БД») (см. Рисунок 6.42).

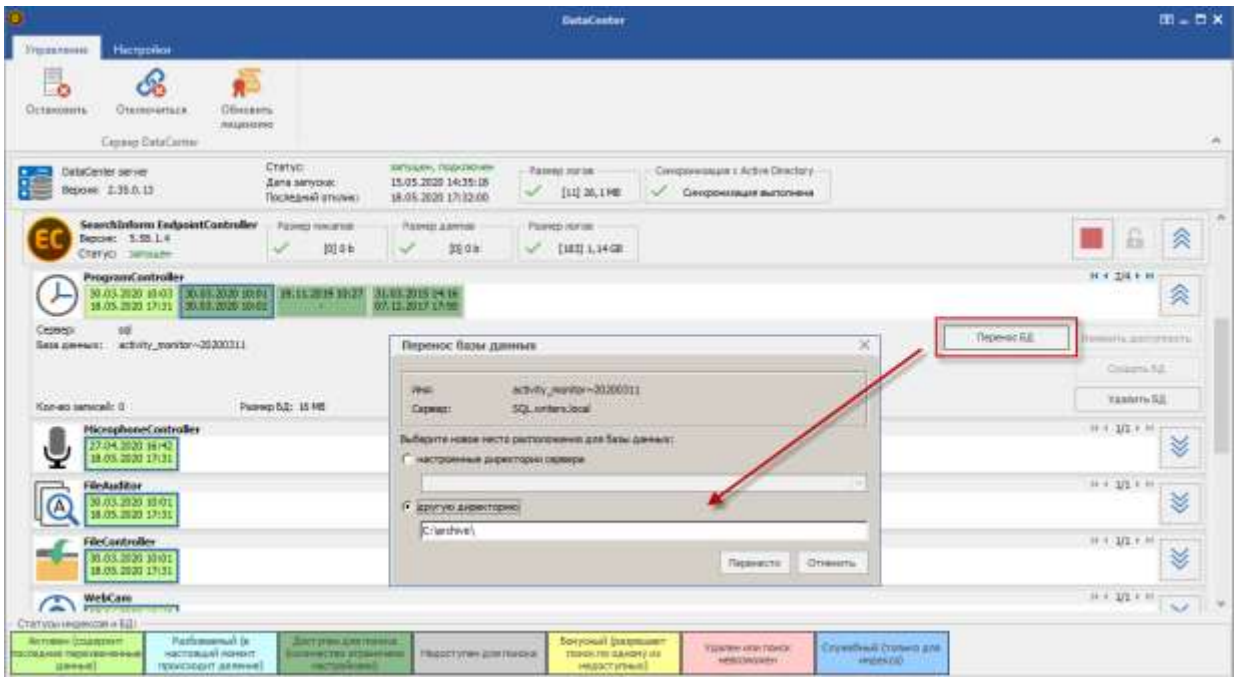


Рисунок 6.42

В нижней части вкладки «Правила переноса БД» расположен журнал операций архивирования БД и их статус, а также форма для фильтрации отображаемых операций (см. Рисунок 6.43).

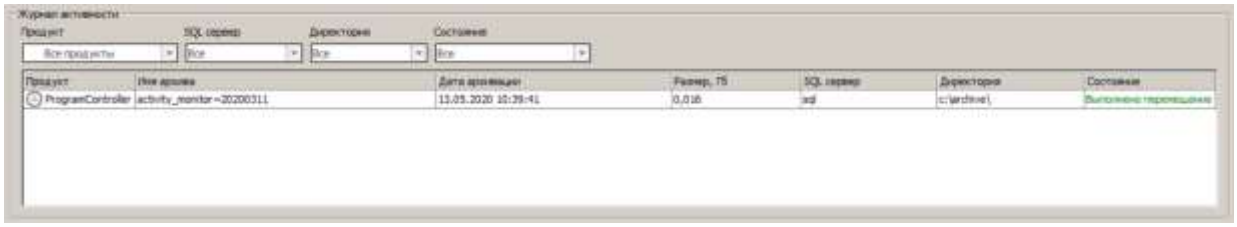


Рисунок 6.43

6.2 Настройка службы профилирования ProfileCenter

Профайлинг – совокупность методов, позволяющих дистанционно и без использования тестов проводить психологическую оценку личности, прогнозировать поведение, выявлять сильные и слабые стороны, заблаговременно выявлять риски человеческого фактора и снижать их значимость. Служба профилирования способна построить профиль пользователя на основании генерируемого им цифрового контента – электронной корреспонденции, чатов в личных и корпоративных мессенджерах, таких как Viber, Telegram, WhatsApp, Lync, Skype, популярные соцсети и IM-клиенты.

Настройки компонента ProfileCenter могут изменяться:

- в консоли DataCenter на вкладке **Настройки** → **Дополнительные настройки** → **Настройки ProfileCenter** (см. Рисунок 6.44),
- в файле конфигурации, расположенном по адресу **C:\ProgramData\SearchInform\SearchInform UserProfiler\UserProfiler.ini**.

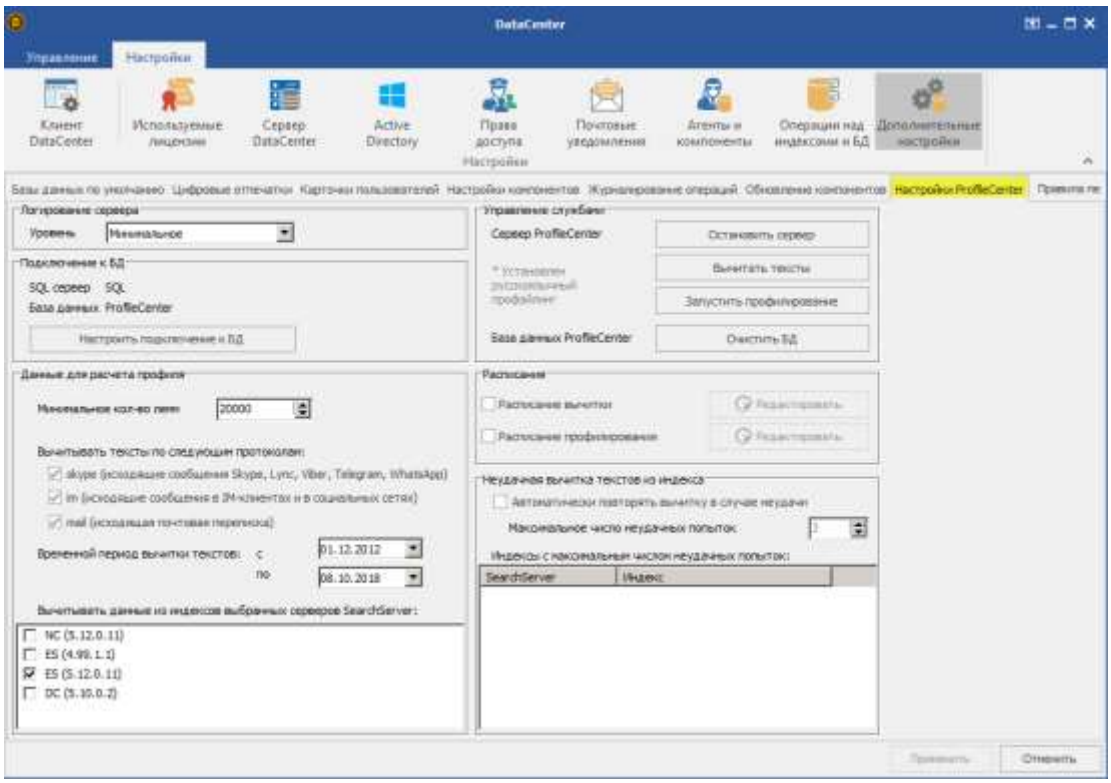


Рисунок 6.44

Параметры и их значения приведены в Таблица 18.

Таблица 18 – Настройки ProfileCenter

Наименование в консоли	**Наименование в файле UserProfiler.ini**	**Пояснение**	**Значение по умолчанию**
Логирование сервера		Уровень логирования событий службой ProfileCenter. Доступны уровни: Error, Info, Warning, Debug.	Минимальное
	port	Номер порта, на котором работает служба и отвечает на запросы	9443
Имя сервера Имя базы данных Имя пользователя	ConnectionString	Настройки подключения к базе данных ProfileCenter. В конфигурационном файле данная строка подключения закодирована Base64.	пусто
	TextStore	Директория для сохранения отладочной информации процесса профайлинга	пусто

Наименование в консоли	Наименование в файле UserProfiler.ini	Пояснение	Значение по умолчанию
	SavePreprocessed Texts	Включение сохранения анализируемых текстов в папку, указанную в параметре "TextStore"	0
	SaveMyStemResult	Активация сохранения аналитической информации в папку, указанную в параметре "TextStore"	0
Минимальное кол-во лемм	LemmasLimit	Число лемм, необходимое для составления профайла пользователя. При изменении значения необходимо произвести перерасчет результатов. *Не рекомендуется изменять значение ниже, чем установлено по умолчанию, поскольку это может исказить результаты расчета профайла. Чем выше число лемм, тем точнее результат!*	20000
Вычитывать тексты по следующим протоколам:	protocols	Отметка протоколов, по которым необходимо вычитывать тексты: • skype (исходящие сообщения в Skype, Lync, Viber, Telegram, WhatsApp), • im (исходящие сообщения в IM-клиентах и в социальных сетях), • mail (исходящая почтовая переписка). Для перечисления используется запятая.	skype,im,mail
Временной период вычитки текстов:	period	Период чтения данных. В конфигурационном файле может быть задан двумя способами: 1) Указать срок, за который необходимо произвести вычитку. *Примеры:* "6m" - означает, что профайл будет сформирован по данным последних 6 месяцев, начиная с текущей даты;	пусто

Наименование в консоли	Наименование в файле UserProfiler.ini	Пояснение	Значение по умолчанию
		"1y" - для построения профайла будут использоваться данные за 1 год, начиная с текущей даты. 2) Указать период в формате "[dd.mm.yyy]-[dd.mm.yyy]", при этом обязательно должна присутствовать хотя бы одна из дат и символ тире "-". *Примеры:* "01.01.2017-" - означает, что будут вычитываться тексты, начиная с 01.01.2017 по текущий момент; "-01.09.2017" - профайл будет сформирован по всем имеющимся данным до 1 сентября 2017 года. Для консоли доступен только 2-й способ.	
Вычитывать данные из индексов выбранных серверов SearchServer:	servers	Отметка серверов Search Server, из индексов которых будет осуществляться вычитка текстовых данных	пусто
Расписание вычитки		Включение/отключение расписания чтения текстов индексов	отключено
Расписание профилирования		Включение/отключение расписания расчета профилей пользователей	отключено
Автоматически повторять вычитку в случае неудачи	autoresumesync	Включение/отключение автоматических попыток вычитки текстов из индексов в случае неудачи (0 – отключено, 1 – включено).	0
Максимальное число неудачных попыток	maxerrorcount	Максимальное количество попыток, после которых вычитка из указанного индекса прекратится.	3

В файл **UserProfiler.ini** может быть добавлен параметр **usersfilter**, позволяющий задать пользователей, для которых не требуется расчет профилей (т.е. эти учетные записи будут исключаться).

Пример записи в файле конфигурации, вносимый в секцию [profiling]:

usersfilter=i.ivanov@company.com;p.petrov@company.com

Формат написания учетной записи должен полностью совпадать (не учитывая регистр). В качестве разделителя нескольких пользователей могут использоваться символы '**,**' или '**;**' .

Управление службой и БД ProfileCenter осуществляется с помощью кнопок:

- **Остановить сервер / Запустить сервер** - остановка службы *SearchInform DataCenter: userprofiler.*
- **Вычитать тексты** - выгрузка необходимой информации из индексов в базу данных ProfileCenter (при первом запуске либо после изменения списка серверов/протоколов).
- **Запустить профилирование** - запуск расчета профилей, в том числе перерасчет после изменения каких-либо значений (например, количества лемм).
- **Очистить БД** - очистка всех данных в базе данных ProfileCenter.

6.3 Настройка модуля генерирования отчетов Серчинформ ReportCenter и сервера WebAnalytic

Сервер ReportCenter получает статистику инцидентов из баз AlertCenter под управлением Microsoft SQL Server 2008 R2 или выше.

Сервер ReportCenter подключается к базам настроек EndpointController, откуда забирает статистику:

- по наименованиям установленного программного обеспечения на рабочих станциях и истории его установки;
- по фактам установки и удаления агентов с компьютеров.

Статистику по активности пользователей сервер ReportCenter получает из индексов модулей перехвата DeviceController, FTPController, HTTPController, CloudController, IMController, MailController, PrintController, SkypeController, LyncController, ViberController. Индексы хранятся на сервере индексации Search Server.

Для получения статистики активности пользователей и процессов в течение рабочего дня ReportCenter использует базы данных компонента ProgramController.

Настройка серверной части ReportCenter осуществляется в консоли DataCenter. Для вызова окна настроек перейдите на вкладку «Управление» и напротив продукта

ReportCenter щелкните кнопку  (доступна, когда служба сервера запущена) (см. Рисунок 6.45).

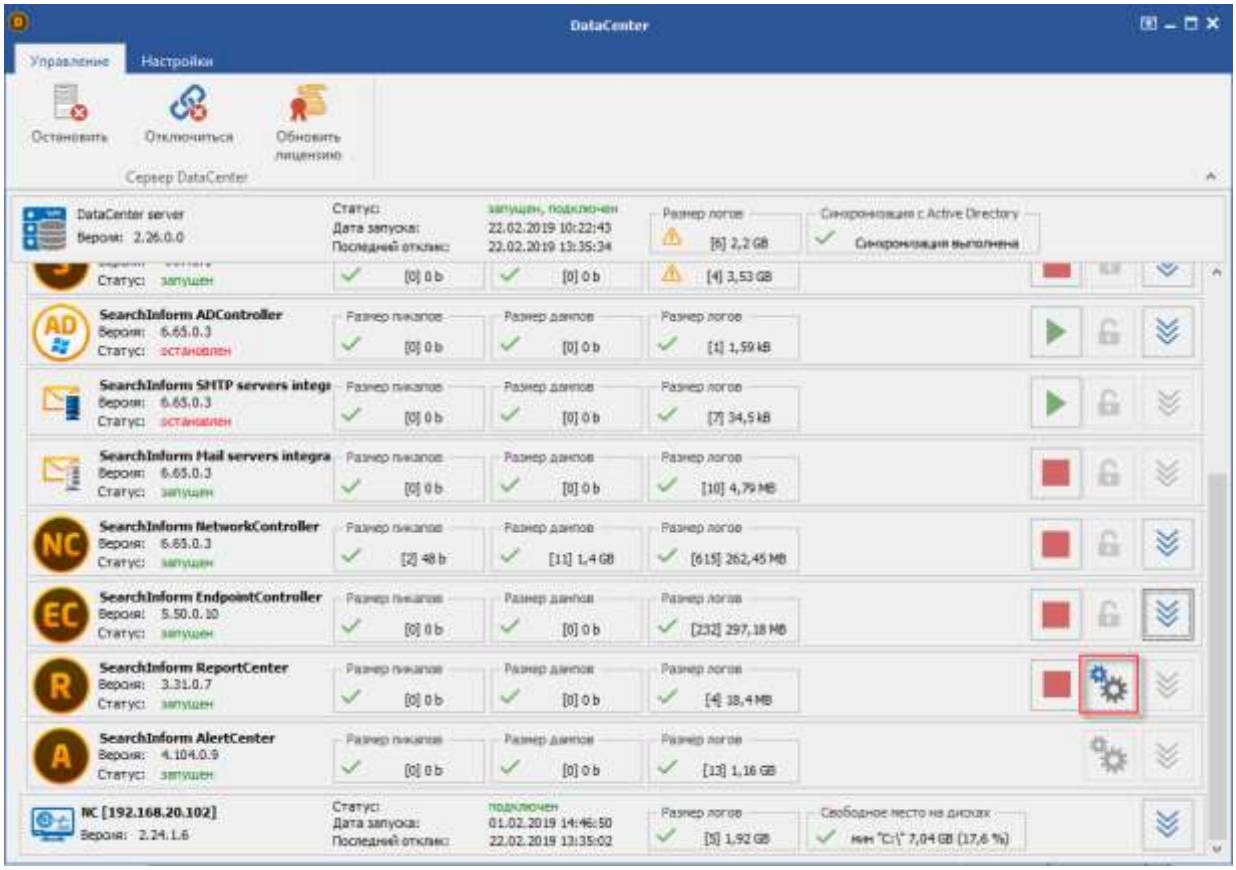


Рисунок 6.45

В появившемся окне возможно:

- конфигурирование подключения к базе данных ReportCenter,
- выбор уровня логирования сервера ReportCenter,
- настройка параметров синхронизации данных,
- конфигурирование параметров синхронизации со СКУД (см. Рисунок 6.46).

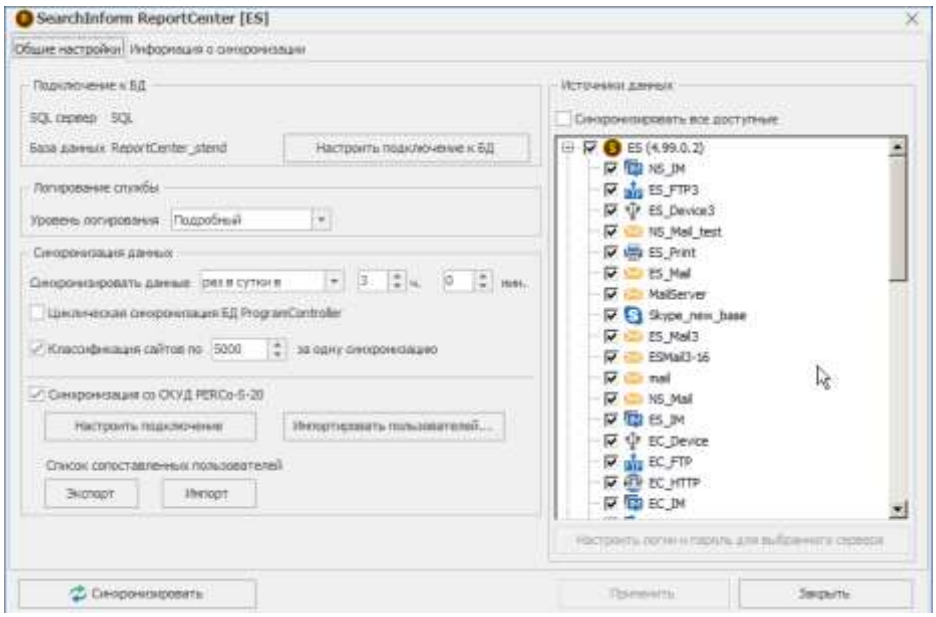


Рисунок 6.46

6.3.1 Подключение к базе данных ReportCenter

Для управления базой ReportCenter используется СУБД Microsoft SQL Server 2008 R2 и выше. В базе данных ReportCenter хранятся:

- импортированные данные:
  - для индексов перехваченных данных - число и общий объем перехваченных данных в привязке к пользователю, протоколу и дате;
  - для индексов компонентов IMController, MailController, SkypeController, LyncController, ViberController дополнительно - число и общий объем перехваченных данных в привязке к адресам, с которых отправлялись либо на которые получались сообщения;
  - для баз данных ProgramController - данные по активности пользователей и процессов в привязке к дате и пользователю;
  - для баз AlertCenter - список инцидентов в привязке к группам алертов, продуктам, запросам и пользователям;
  - для баз данных EndpointController - история установки ПО и история установки агентов EndpointController в привязке к имени компьютера и дате;
- структура службы каталогов Active Directory со списком пользователей, а также введенные вручную адресаты (AnalyticConsole позволяет присваивать и переназначать адресатам имена);
- результаты последней синхронизации данных (при синхронизации индексов обрабатываются только те документы, которые были проиндексированы после последней успешной синхронизации данного индекса);

- список зафиксированных агентами адресов (учетных записей) для компонентов MailController, IMController, SkypeController, LyncController, ViberController с привязкой к списку пользователей (данные сопоставляются с Active Directory и введенными вручную адресатами).

В области «Подключение к БД» щелкните кнопку «Настроить подключение к БД» (см. Рисунок 6.47.

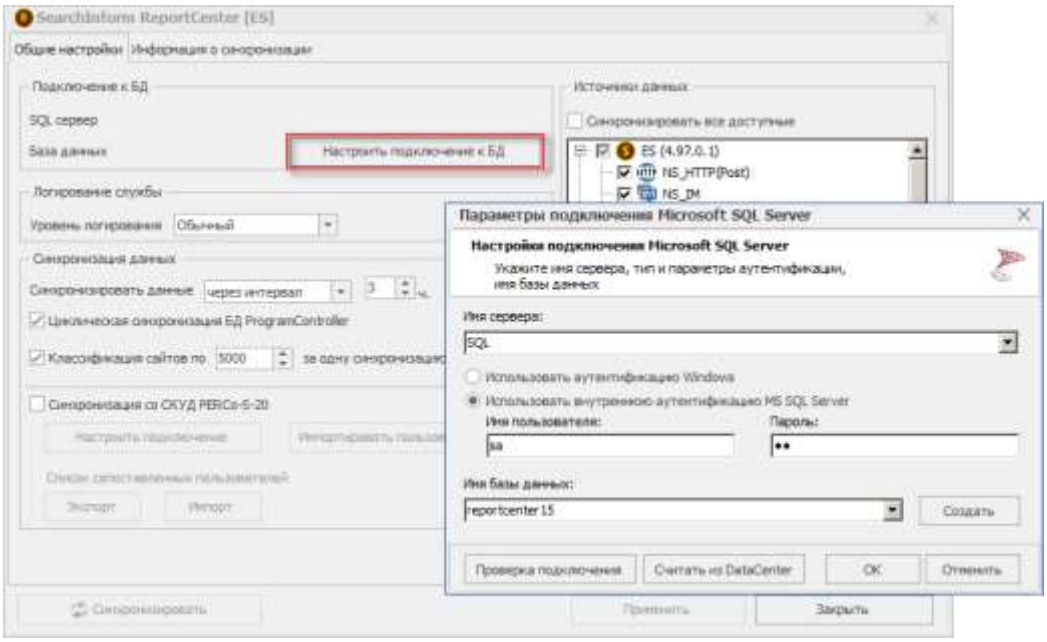


Рисунок 6.47

В окне параметров подключения введите имя или IP-адрес сервера Microsoft SQL, параметры авторизации на сервере, имя создаваемой базы данных и щелкните кнопку «Создать». Также можно импортировать настройки подключения, воспользовавшись кнопкой «Считать из DataCenter». Нажмите «ОК». В случае успешного создания базы данных отобразится окно с подтверждением.

6.3.2 Выбор уровня логирования сервера

Выберите требуемый уровень логирования для службы сервера ReportCenter. Предусмотрено четыре уровня логирования (см. Рисунок 6.48):

- Выключено - никакие данные не фиксируются.
- Минимальный - фиксируются только серьезные ошибки службы синхронизации и консоли управления сервером, повлекшие прерывание или аварийное завершение работы. Данный режим может быть включен при необходимости контроля работы сервера.
- Обычный - дополнительно фиксируется запуск внутренних функций программы.
- Детальный - дополнительно фиксируется запуск внутренних функций программы в более подробном виде (например, отражаются процессы

синхронизации со службой каталогов Active Directory). Данный режим рекомендуется включать только по запросу сотрудников службы технической поддержки в случае критических проблем с сервером.

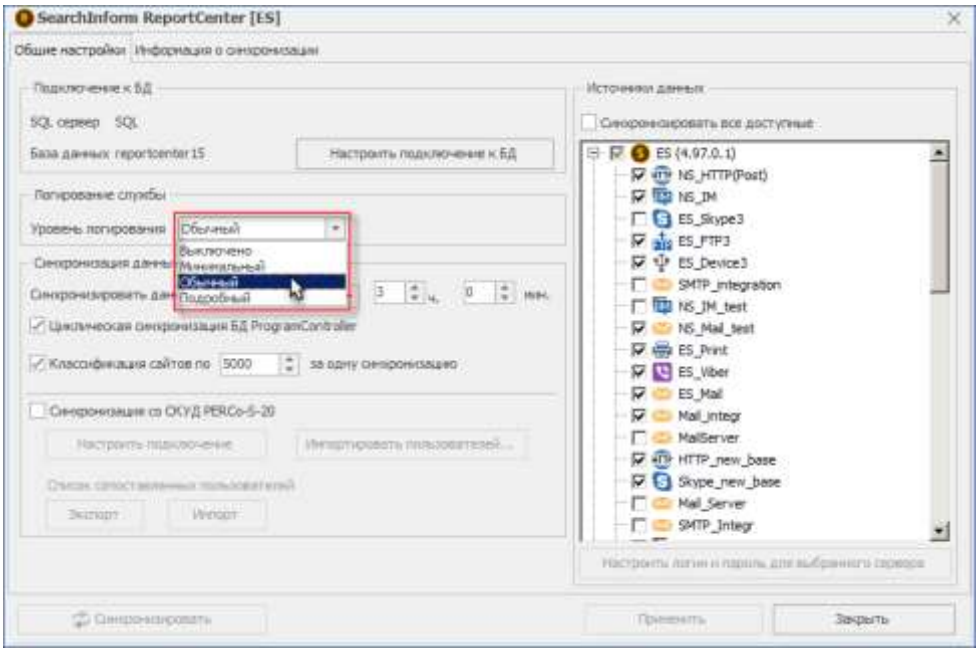


Рисунок 6.48

6.3.3 Настройка синхронизации данных

Синхронизация данных позволяет актуализировать данные в БД по статистике перехвата и инцидентам AlertCenter.

В группе настроек «Синхронизация данных» задайте расписание, согласно которому будет происходить актуализация статистики перехвата и инцидентов. При этом можно выбрать одну из двух схем расписания синхронизации:

- «через интервал» - синхронизация производится с интервалом, заданным в часах и минутах;
- «раз в сутки в» - синхронизация производится ежедневно в указанное время, начиная с момента применения настроек.

Установка флажка «Циклическая синхронизация БД ProgramController» активирует непрерывную синхронизацию БД ProgramController до тех пор, пока не завершится синхронизация баз данных и индексов остальных продуктов.

Для активации функционала классификатора веб-сайтов[16] установите флажок напротив параметра «Классификация сайтов» и настройте количество сайтов, единовременно передаваемых для синхронизации. Максимально возможное количество - 30.000. Запуск классификации для следующей порции веб-сайтов осуществляется после завершения очередной синхронизации (см. Рисунок 6.49).

[16] Для работы классификатора на сервере ReportCenter должен быть обеспечен доступ в сеть Интернет по HTTP(S)-порту 443 для подключения к https://wtm.searchinform.ru.

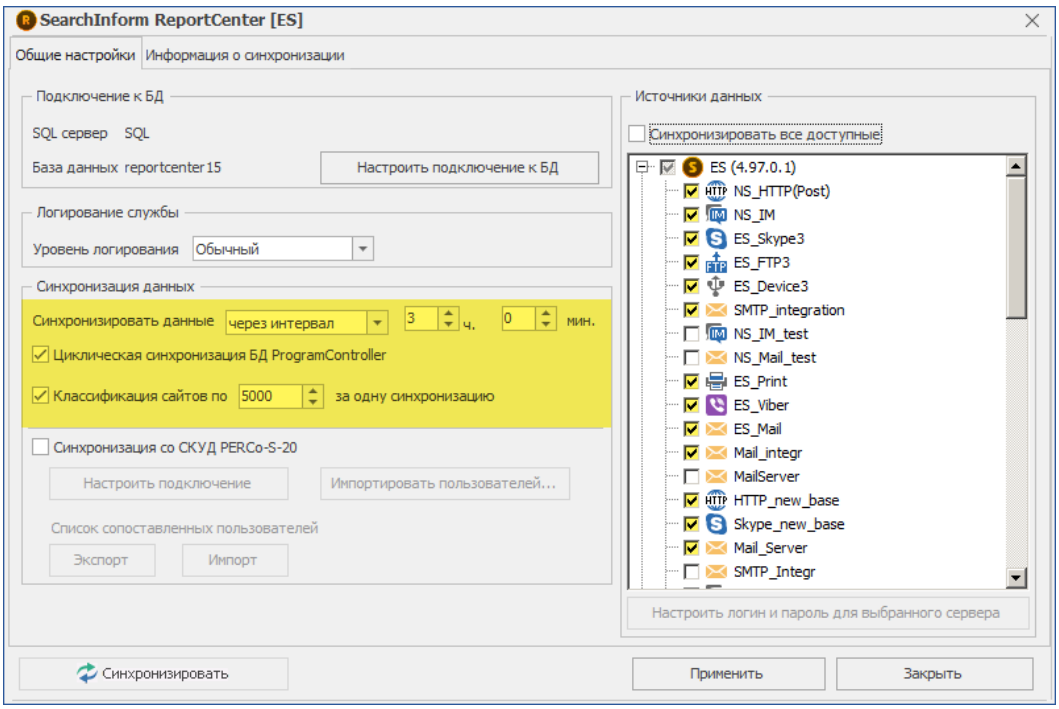


Рисунок 6.49

В правой части окна отметьте индексы и базы данных, синхронизацию с которыми необходимо произвести.

В некоторых случаях при подключении к цепочкам индексов может потребоваться аутентификация пользователя. Например, в случаях, когда для индекса настроены права доступа или когда Search Server находится не в домене.

Для аутентификации при подключении к индексам Search Server выделите сервер и щелкните кнопку «Настроить логин и пароль для выбранного сервера» (при выборе одной из цепочек индексов аутентификация все равно будет относиться ко всему серверу) (см. Рисунок 6.50).

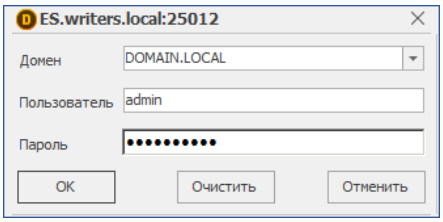


Рисунок 6.50

В открывшемся окне введите данные аутентификации:

- Домен (выбирается из выпадающего списка). Если сервер находится вне домена, необходимо вручную ввести его имя.
- Пользователь (вводится имя пользователя, обладающего правами доступа).
- Пароль (вводится пароль пользователя, обладающего правами доступа).

Щелкните кнопку «OK». Доступ к выбранному серверу со всеми цепочками индексов будет открыт.

Синхронизацию данных следует запускать только после создания базы данных ReportCenter и выбора источников данных для синхронизации. Синхронизация запускается согласно заданному расписанию либо принудительно, после нажатия кнопки «Синхронизировать» (название кнопки сменится на «Прервать синхронизацию», см. Рисунок 6.51).

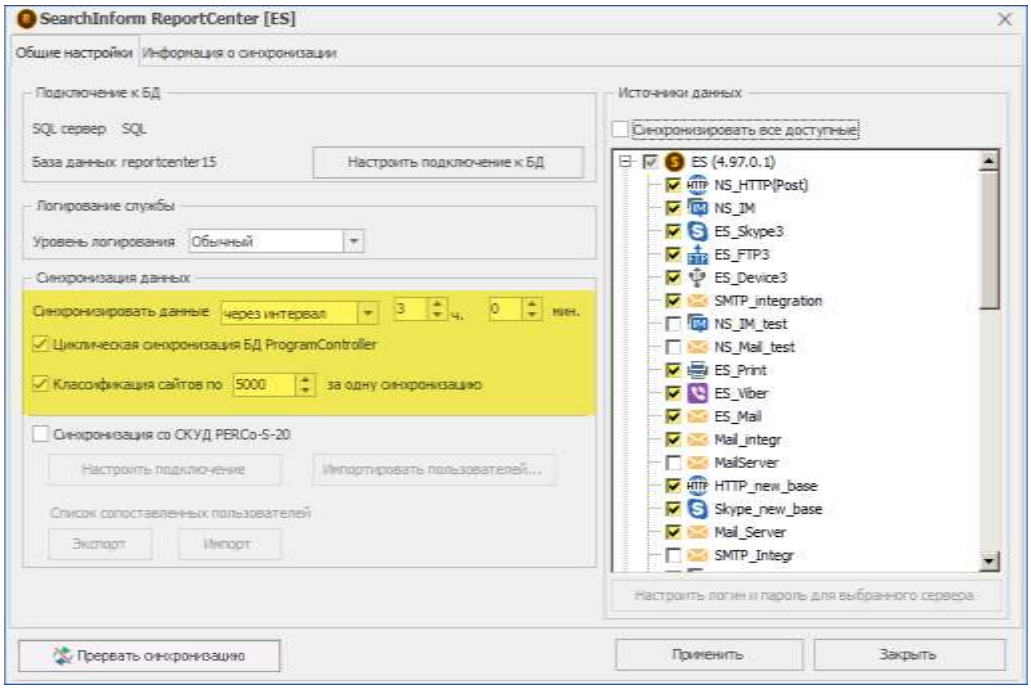


Рисунок 6.51

Статистика синхронизации источников данных отображается на вкладке «Информация о синхронизации» (см. Рисунок 6.52).

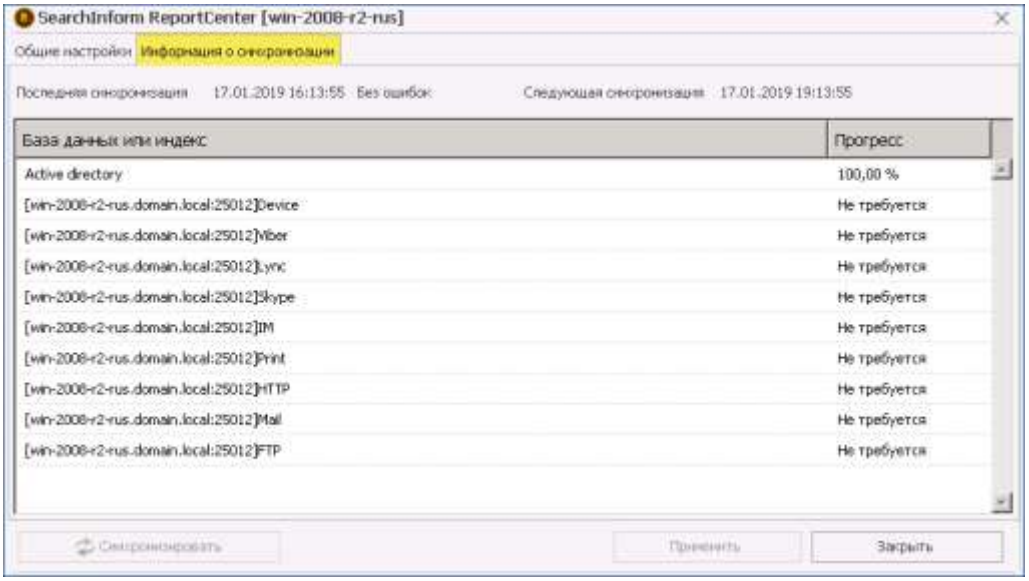


Рисунок 6.52

В результате процесса синхронизации пользователь получает одно из следующих уведомлений:

- «Ожидание» - подготовка к процессу синхронизации;
- «100 %» - синхронизация всех данных успешно завершена;
- «Не требуется» - после последней синхронизации не проиндексировано ни одного документа;
- «Индексация» - в текущий момент выполняется индексирование данных;
- «Прервано» - нажата кнопка «Остановить»;
- «Ошибка Search API» - не установлено или конфликт версий;
- «Ошибка сервера» - права доступа отсутствуют, выключен сервер, имеются неполадки в работе оборудования;
- «Ошибка индекса» - не удается подключиться к индексу;
- «Ошибка БД» - не удалось подключиться к БД серверного компонента;
- «Ошибка» - в процессе синхронизации произошла неустановленная ошибка.

6.3.4 Настройка синхронизации со СКУД

В данной версии ReportCenter доступна интеграция со следующими СКУД:

- PERCo-S-20 версии 3.9.6.0 и выше
- Орион Про версии 1.12 и выше.

Для использования в отчетах данных СКУД необходимо выбрать соответствующий модуль интеграции при установке DataCenter (см. Рисунок 6.53).

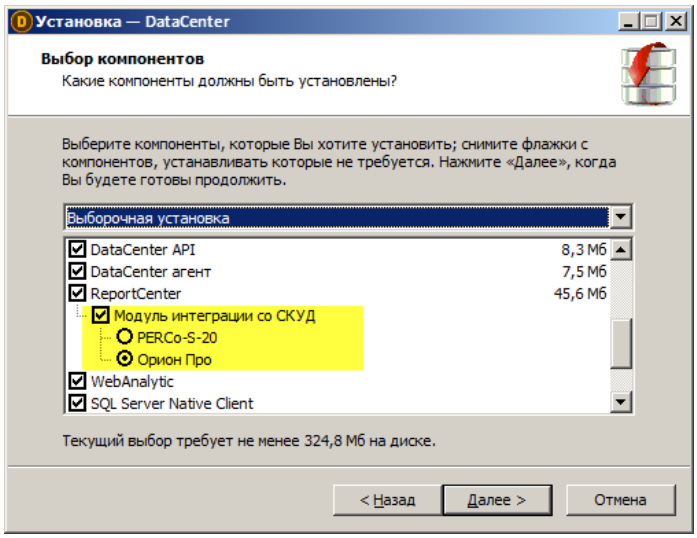


Рисунок 6.53

При настройке синхронизации в ReportCenter будут отображаться параметры той СКУД, которая была выбрана на этапе установки DataCenter.

Данные, полученные из базы данных СКУД, могут быть опционально отображены в AnalyticConsole в следующих отчетах:

- Опоздания сотрудников;
- Ранние уходы;

- Журнал рабочего времени;
- Посещения сотрудников;
- Табель рабочего времени.

6.3.4.1 Настройка синхронизации со СКУД PERCo-S-20

Активируйте настройки, отметив флажком параметр «Синхронизация со СКУД PERCo-S-20», и нажмите кнопку «Настроить подключение» (см. Рисунок 6.54).

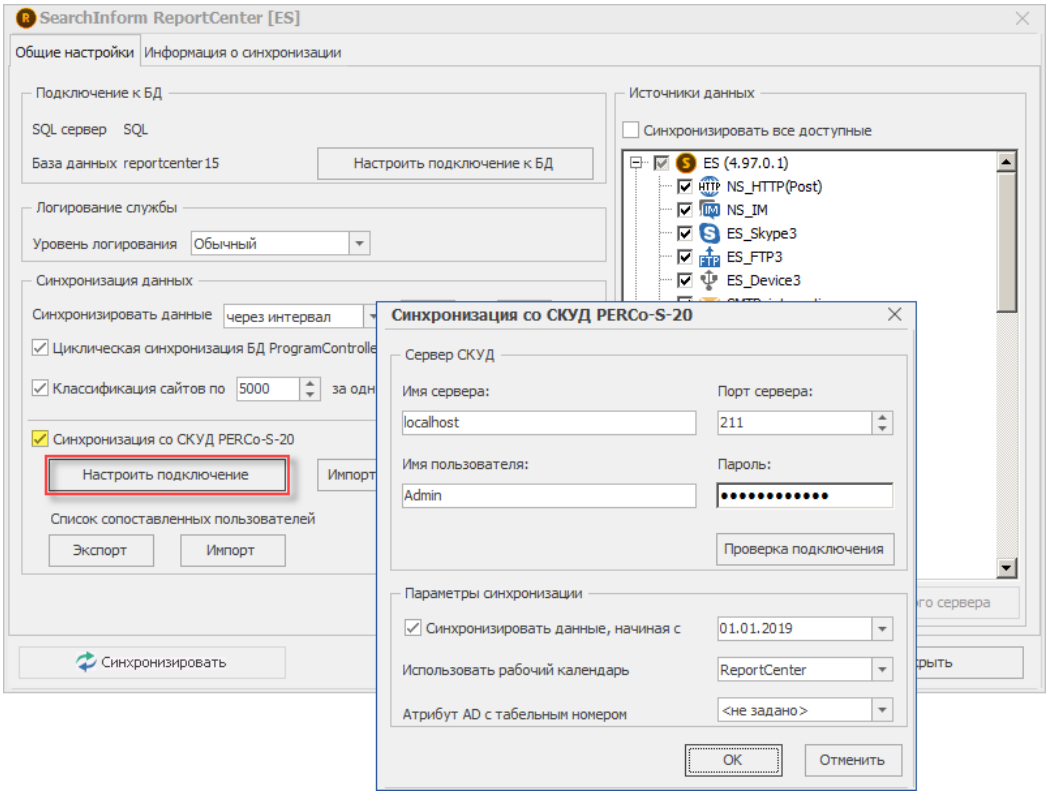


Рисунок 6.54

В появившемся окне настроек задайте:

- Имя или IP-адрес сервера СКУД;
- Номер порта, используемого для подключения (по умолчанию - 211);
- Параметры учетной записи, имеющей право подключения к СКУД.

Укажите начальную дату, с которой необходимо начать синхронизацию с данными СКУД. Если в дальнейшем будет выбрана более ранняя дата, полной пересинхронизации не понадобится, будут синхронизированы только недостающие данные. Сопоставленные ранее пользователи СКУД также не пострадают.

Выберите, какой график рабочей недели будет использоваться: настроенный в AnalyticConsole либо в консоли PERCo-S-20.

Каждому пользователю СКУД может быть присвоен табельный номер (при наличии такового). Для этого необходимо:

С помощью оболочки Windows PowerShell добавить в Active Directory для каждого пользователя атрибут **ExtensionAttributeN** (**N** - любое числовое значение) и его значение, соответствующее табельному номеру пользователя.

Пример:

```
import-module ActiveDirectory
set-ADUser -Identity User -Add @{extensionAttribute4="36"}
```

В консоли DataCenter на вкладке **Настройки → Active Directory** отметьте флажком **ExtensionAttributeN** в списке вычитываемых атрибутов.

В настройках синхронизации ReportCenter со СКУД в выпадающем списке **Атрибут AD с табельным номером** выберите наименование созданного атрибута.

Пользователи СКУД, предварительно экспортированные в Excel-файл, могут быть импортированы в базу данных ReportCenter для сопоставления с пользователями Active Directory. Для корректного импорта пользователей СКУД на компьютере необходимо наличие установленного Microsoft Excel.

В окне настроек ReportCenter нажмите кнопку «Импортировать пользователей...». В появившемся окне выберите файл со списком пользователей СКУД и нажмите кнопку «Начать импорт» (см. Рисунок 6.55).

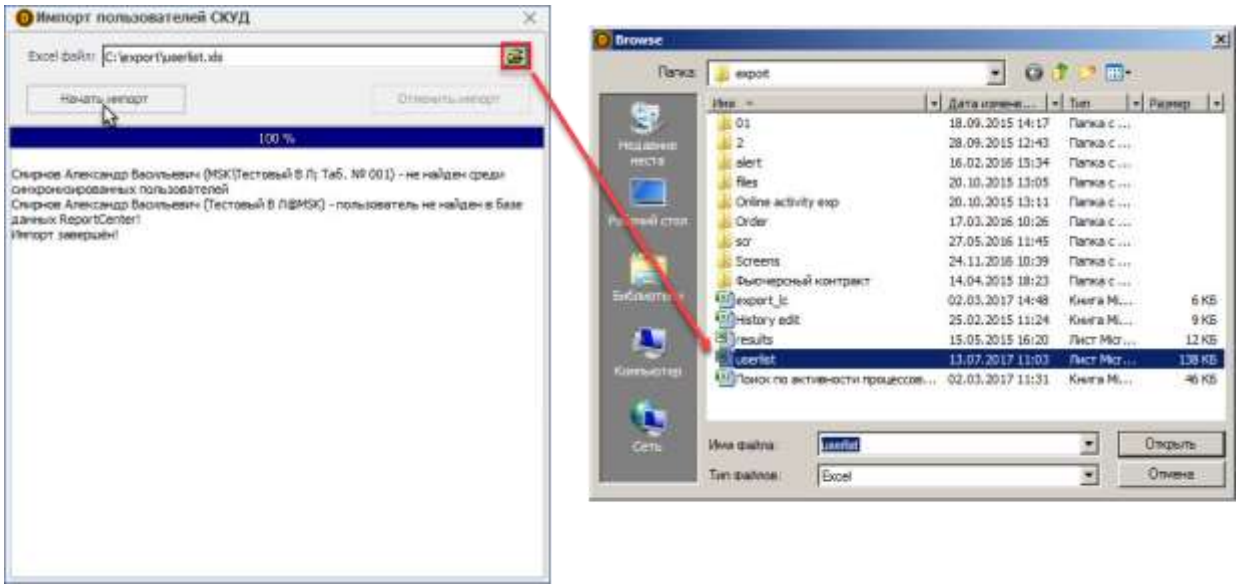


Рисунок 6.55

При возникновении ошибок в процессе импорта они будут выведены в лог. Помимо автоматического сопоставления, возможна привязка пользователей PERCo-S-20 к пользователям Active Directory вручную из AnalyticConsole.

Выгрузка/загрузка списка уже сопоставленных пользователей СКУД может осуществляться с помощью кнопок «Экспорт/Импорт» (см. Рисунок 6.56).

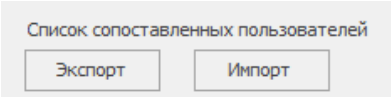


Рисунок 6.56

Сохраните произведенные настройки.

6.3.4.2 Настройка синхронизации со СКУД Орион Про

Активируйте настройки, отметив флажком параметр «**Синхронизация со СКУД Орион Про**», и нажмите кнопку «**Настроить подключение**».

В появившемся окне «Синхронизация со СКУД Орион Про» нажмите для добавления сервера СКУД и укажите:

- Тип используемого протокола: HTTP/HTTPS;
- Имя или IP-адрес сервера СКУД;
- Номер порта, используемого для подключения (по умолчанию - 8090).

Для проверки подключения к серверу используйте кнопку «Проверка подключения».

Нажмите «ОК» для сохранения настроек подключения.

Установите дату начала синхронизации с данными СКУД Орион Про. В случае переустановки даты на более раннюю, будут синхронизированы только недостающие данные (данные по сопоставленным ранее пользователям Орион Про также не пострадают).

Пользователи СКУД Орион Про могут быть автоматически сопоставлены с пользователями, импортированными из Active Directory, при условии полного совпадения имен таких пользователей (без учета пробелов). Для активации данного функционала установите флажок **Сопоставлять пользователей по имени** (по умолчанию флаг снят) (см. Рисунок 6.57).

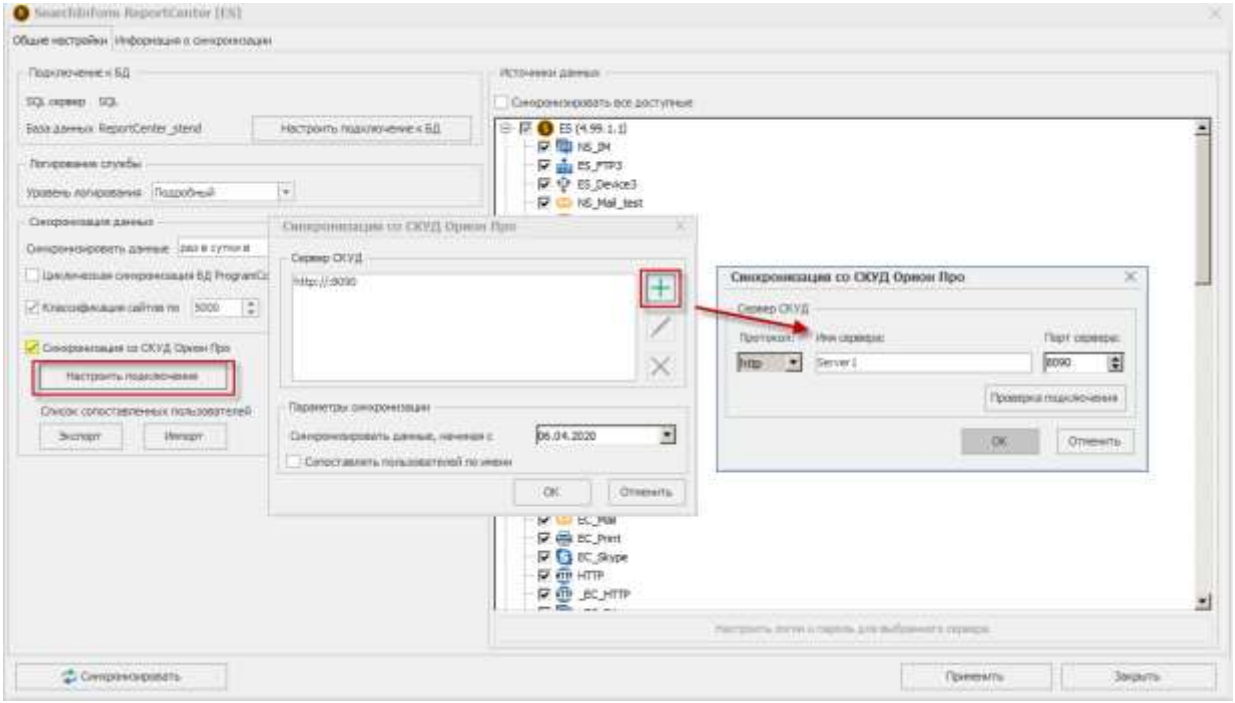


Рисунок 6.57

Помимо автоматического сопоставления, возможна привязка пользователей Орион Про к пользователям Active Directory вручную из AnalyticConsole.

Выгрузка/загрузка списка уже сопоставленных пользователей СКУД может осуществляться с помощью кнопок «Экспорт/Импорт» (см. Рисунок 6.58).

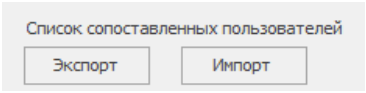


Рисунок 6.58

Сохраните произведенные настройки.

6.3.5 Настройка сервера веб-отчетов

Для вызова окна настроек сервера WebAnalytic на вкладке «Управление» напротив продукта щелкните кнопку  (доступна, когда служба сервера запущена. См.Рисунок 6.59).

Рисунок 6.59

Для работы и корректного отображения веб-отчетов в открывшемся окне настройте следующие параметры:

- **Уровень логирования** службы SearchInform REST API (минимальный или подробный);
- **Порт,** прослушиваемый веб-сервером (по умолчанию - 443);

- Опционально - **включение перенаправления** на защищенное HTTPS-соединение;
- Опционально - **использование протокола TLS для подключения к LDAP-серверу** (Active Directory);
- Опционально - явное **подключение к контроллеру домена**. В случае, когда контроллеров домена несколько, можно задать подключение к конкретному из них, указав полное доменное имя или IP-адрес контроллера в текстовом поле. Зачастую данная настройка используется в случае нахождения сервера Серчинформ ДЛП не в домене, а в рабочей группе;
- При необходимости, замените файл **SSL-сертификата** для использования вместо генерируемого по умолчанию либо **восстановите** исходный сертификат (сброс установленного в системе сертификата на самоподписанный сертификат по умолчанию reports.local);
- **Сетевые интерфейсы** - IP-адрес сервера, к которому будут подключаться пользователи веб-отчетов. На данном веб-сервере может быть несколько сетевых карт или несколько IP-адресов, назначенных одной сетевой карте (см. Рисунок 6.60).

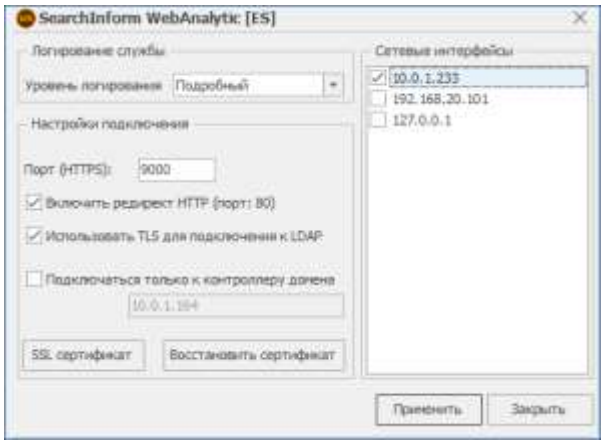


Рисунок 6.60

Сохраните произведенные настройки, щелкнув кнопку «Применить».

6.4 Настройка сервера индексации Search Server

Для входа в консоль сервера индексации Search Server выберите тип проверки подлинности (учетная запись Windows или SearchInform) и укажите имя пользователя и пароль. Нажмите «ОК».

Выберите сервер и запустите его, нажав кнопку  (см. Рисунок 6.61).

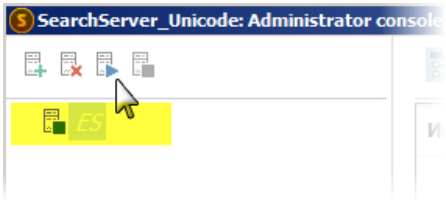


Рисунок 6.61

Создание индексов для перехваченных данных и расписание их обновления осуществляется в серверных консолях EndpointController и NetworkController.

В консоли Search Server может быть создан индекс данных, хранящихся в облачных хранилищах DropBox, YandexDisk, CMIS, OneDrive.

6.4.1 Создание индекса облачного хранилища

Для создания индекса выберите из контекстного меню команду «Создать индекс» (см. Рисунок 6.62).

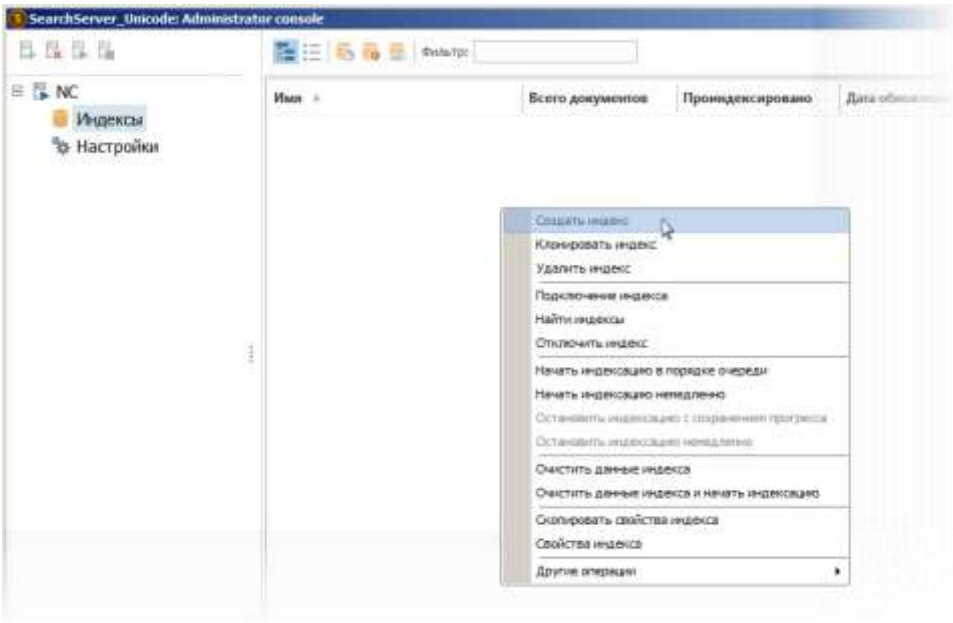


Рисунок 6.62

Задайте папку и имя нового индекса. Отметьте «Другое» в данных, подлежащих индексации (см. Рисунок 6.63).

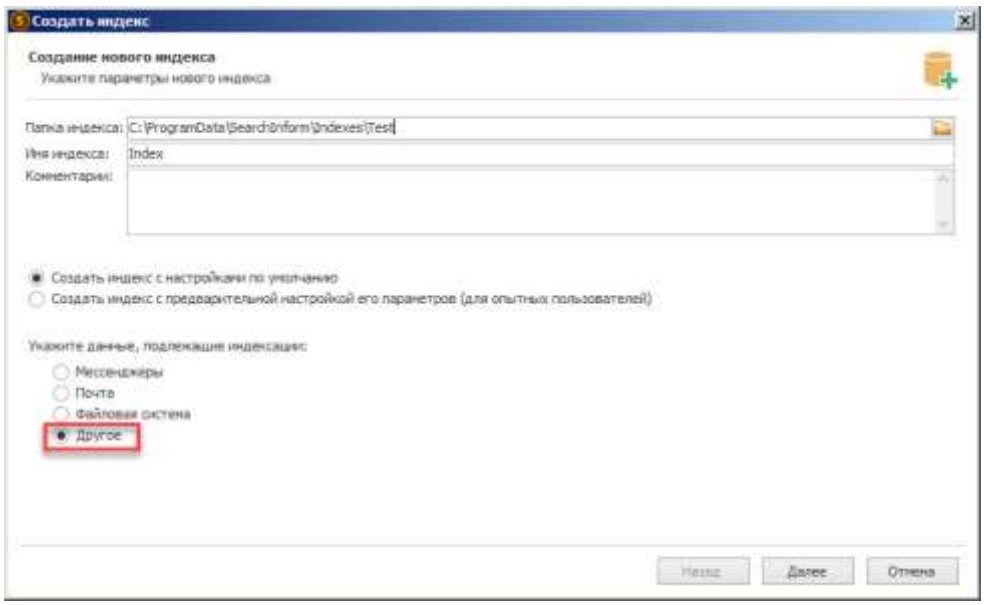


Рисунок 6.63

Выберите требуемый источник данных и настройте параметры подключения к облачному хранилищу, нажав кнопку «Конфигурация» (см. Рисунок 6.64).

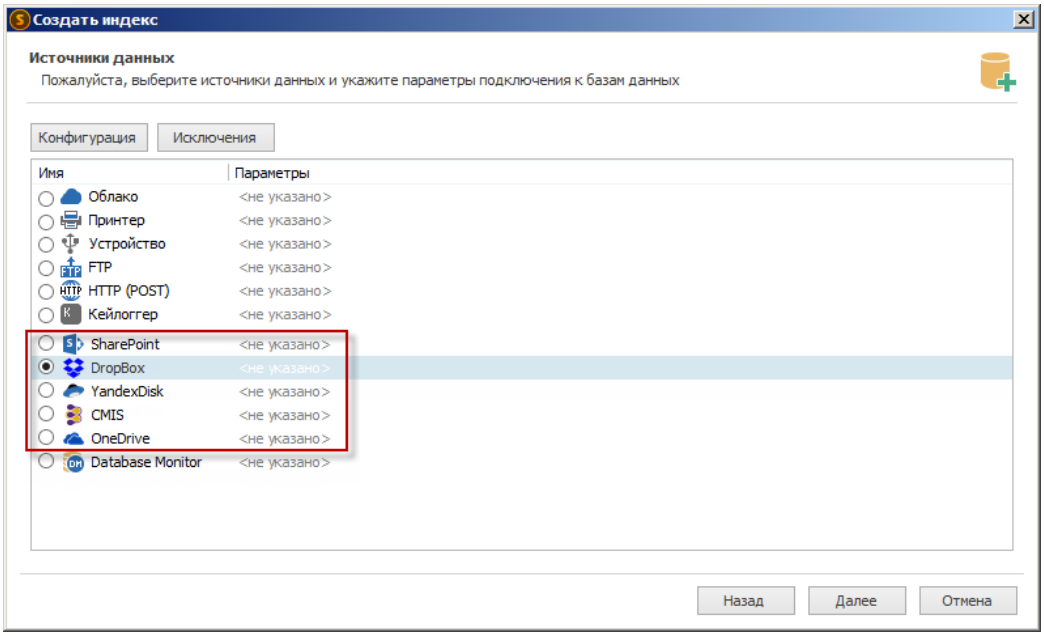


Рисунок 6.64

Для подключения к облачному хранилищу требуется Internet Explorer версии 11.0.9600.18893 или выше, а также должны быть включены активные сценарии!

Введите параметры учетной записи, используемой для входа в облачное хранилище (см. Рисунок 6.65). Нажмите кнопку «Войти».

Рисунок 6.65

После успешного подключения окно будет автоматически закрыто.

Настройте подключение к необходимым облачным сервисам. После чего в окне мастера отметьте флажком автоматический запуск индексации и щелкните кнопку «Завершить» (см. Рисунок 6.66).

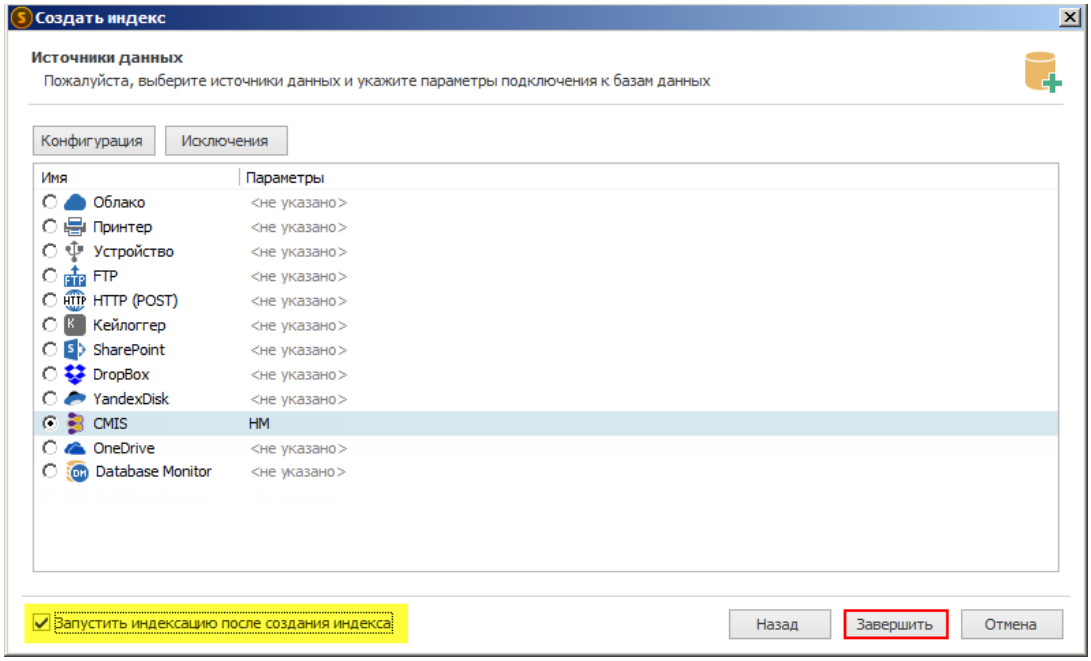


Рисунок 6.66

В консоли сервера появятся созданные индексы, которые тут же начнут обновляться (см. Рисунок 6.67).

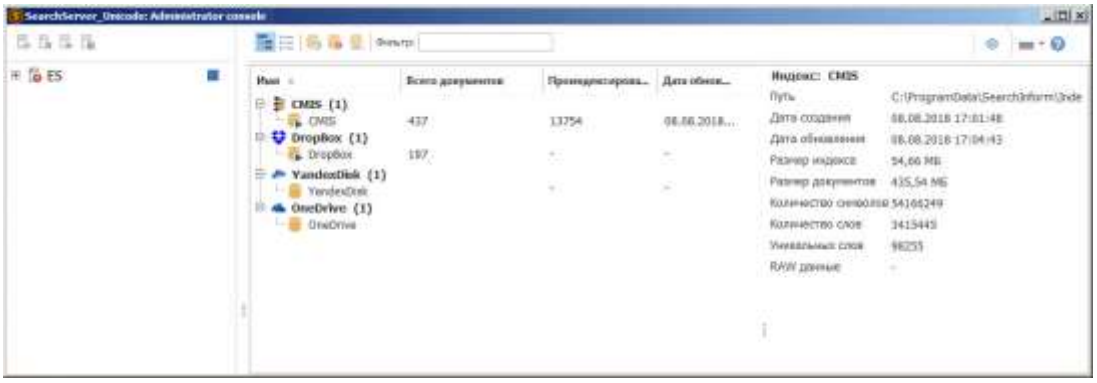


Рисунок 6.67

6.5 Настройка сервера EndpointController

6.5.1 Первоначальная настройка сервера EndpointController

Для входа в консоль администрирования серверного модуля EndpointController укажите имя сервера DataCenter (если EC и DC установлены на одном компьютере, можно указать *localhost*) и выберите проверку подлинности Windows (см. Рисунок 6.68).

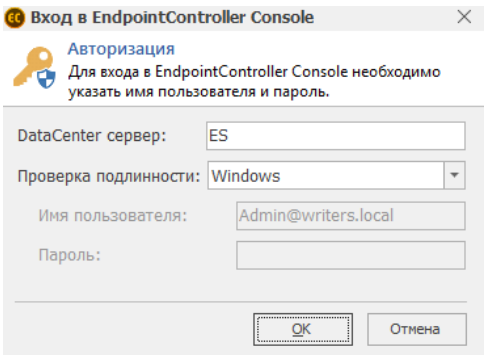


Рисунок 6.68

Для загрузки системных исключений щёлкните «Да» в появившемся окне (см. Рисунок 6.69).

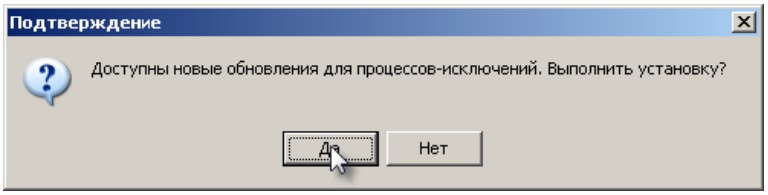


Рисунок 6.69

Будет открыта консоль администрирования EndpointController.

Мастер настройки откроется автоматически при первом запуске после установки. Либо воспользуйтесь одноименной кнопкой (см. Рисунок 6.70).

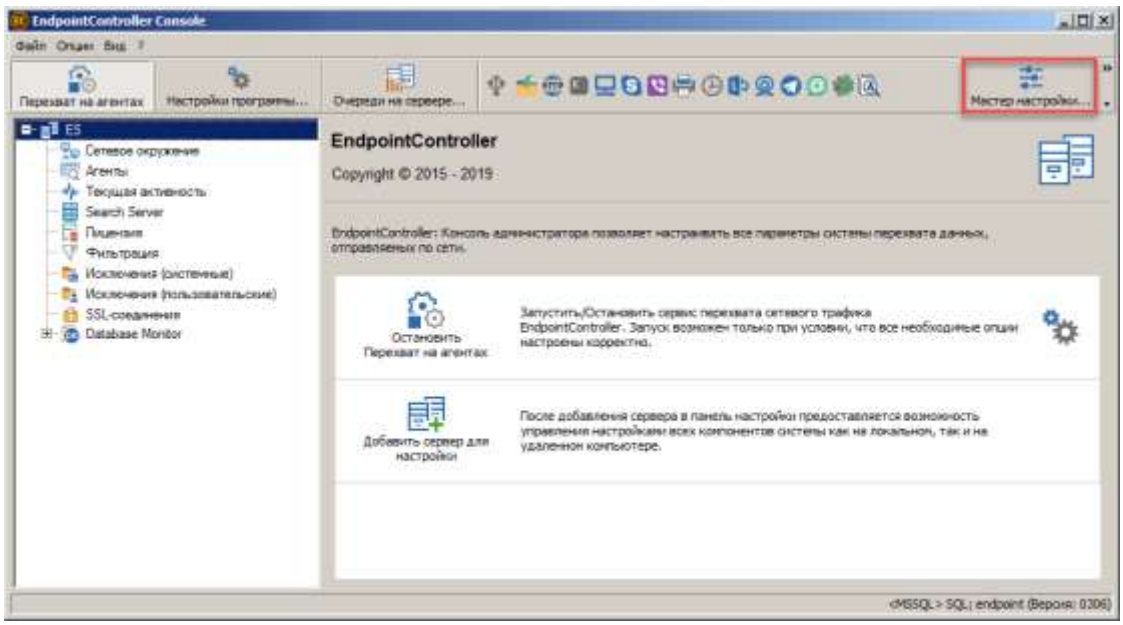
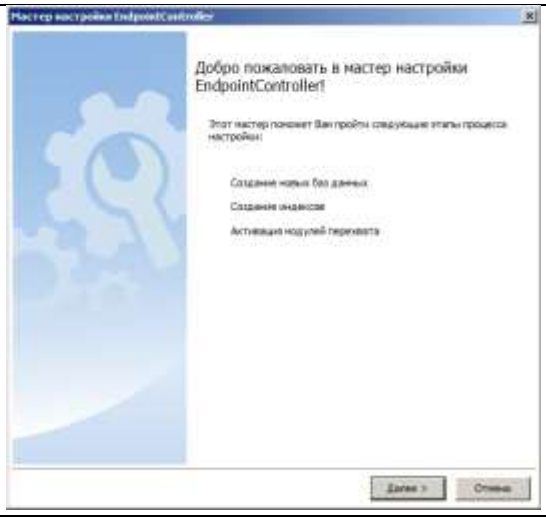
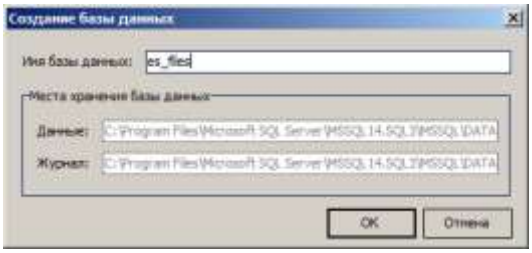


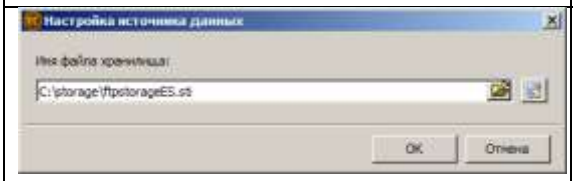
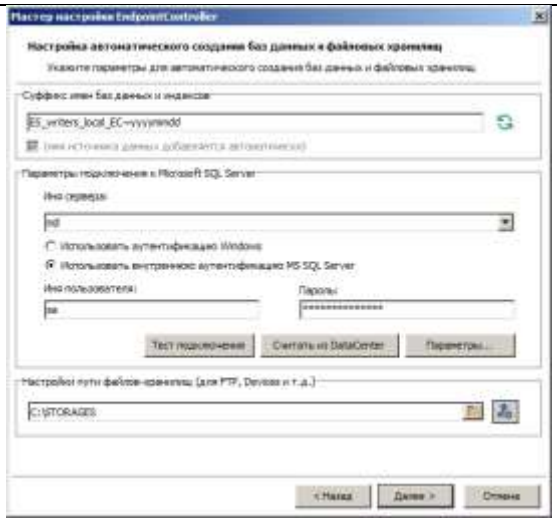
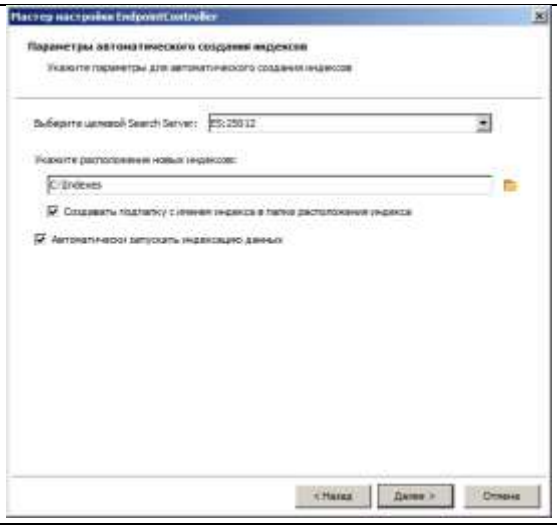
Рисунок 6.70

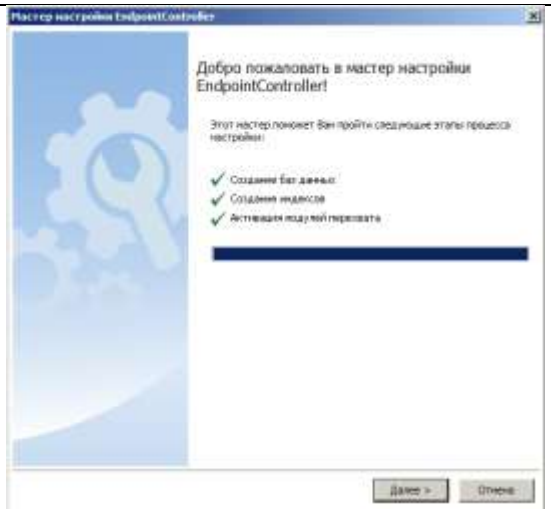
С помощью мастера настройки SearchInform EndpointController создайте требуемые базы данных, индексы (в примере индексы рассмотрены Device, Skype, Viber, остальные создаются по аналогии), и хранилища, как указано в Таблица 19.

Таблица 19 – Мастер настройки SearchInform EndpointController

Страница мастера	Интерфейс (поле или свойство)	Настройка
Начальная страница		Нажмите «Далее».

Страница мастера	Интерфейс (поле или свойство)	Настройка
Выбор источников для индексации		Отметьте источники данных, для которых необходимо создать индексы. Если «Текущее подключение» не задано, оно будет создано автоматически. При необходимости, можно настроить параметры подключения вручную: Двойной клик по области столбца «Текущее подключение» вызывает окно настройки подключения к базе данных, а для FTP и Device (хранилище) - подключения к хранилищам данных. EndpointController будет записывать сообщения, перехваченные по указанным протоколам, в подключенную БД (хранилище).
Подключение к источнику данных	 	Настройте подключение к базе данных. Выберите сервер Microsoft SQL или введите его имя / IP-адрес. Выберите тип аутентификации. При использовании встроенной в MS SQL Server аутентификации, выберите «Использовать внутреннюю аутентификацию MS SQL Server» и введите имя пользователя и пароль. При использовании унаследованной аутентификации Windows, выберите «Использовать аутентификацию Windows». Выберите существующую базу данных. При создании

Страница мастера	Интерфейс (поле или свойство)	Настройка
		новой базы данных, щелкните кнопку «Создать», задайте ее имя, а также при необходимости измените места хранения базы данных и журнала транзакций по умолчанию.
		Настройте подключение к хранилищу (для Device/FTP). В диалоговом окне «Настройка источника данных» вручную либо с помощью кнопки  выберите путь для хранения перехваченных данных. При создании нового каталога подтвердите запрос на его создание.
Параметры автоматичес-кого создания		Для всех не настроенных на предыдущем шаге источников данных параметры подключения будут созданы автоматически в соответствии с указанными параметрами. Настройте суффикс имен, параметры подключения к серверу БД, а также путь к папке, в которой будут созданы хранилища данных (только при выборе Device/FTP).
Расположение индексов		Укажите Search Server и папку, в которой индексы будут храниться. Рекомендуется, чтобы индексы и базы SQL Server для хранения перехваченных данных, располагались на разных дисках сервера. Если установлен флажок «Автоматически запускать индексацию», индексация

Страница мастера	Интерфейс (поле или свойство)	Настройка
		начинается сразу по щелчку кнопки «Финиш».
Завершение работы мастера		Нажмите кнопку «Завершить».

По завершении работы мастера будут созданы соответствующие источники данных для выбранных продуктов.

На вкладке «Планировщик» с помощью мастера создайте расписание обновления индекса (см. Рисунок 6.71).

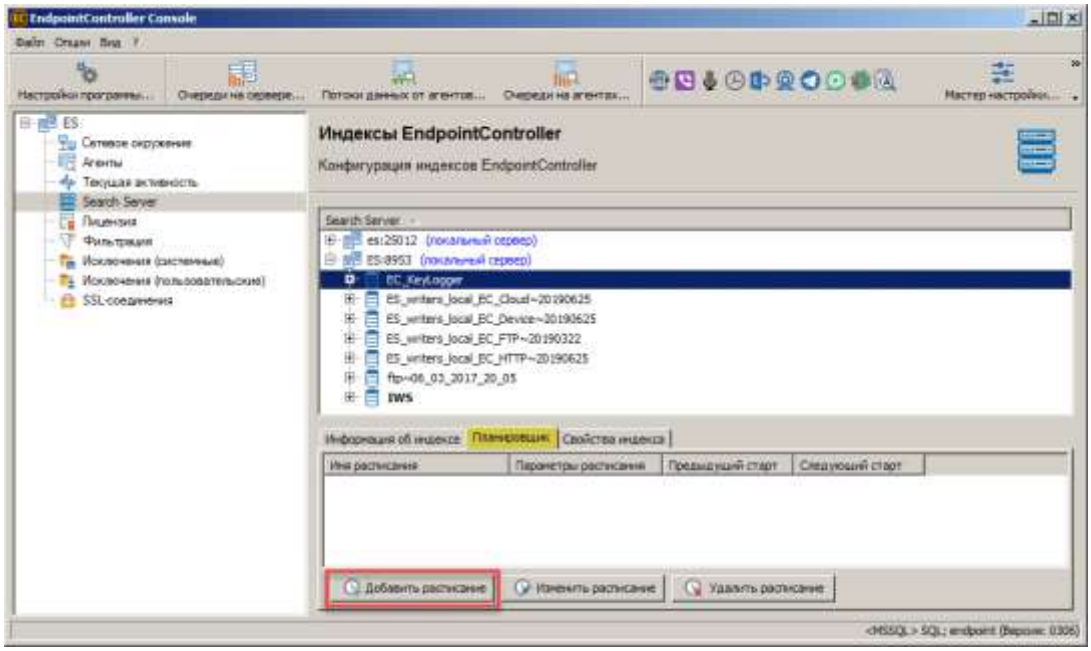


Рисунок 6.71

Задайте имя расписания и периодичность, с которой оно будет запускаться (см. Рисунок 6.72).

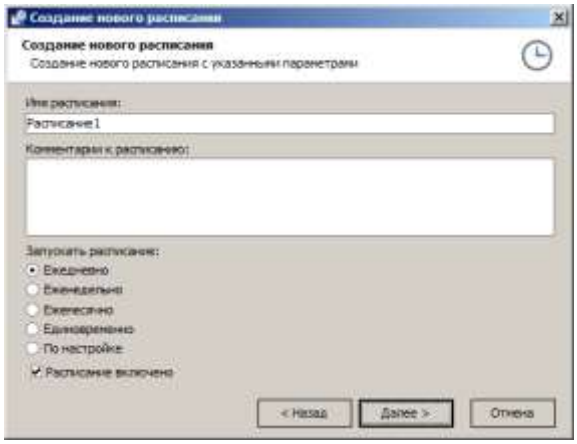


Рисунок 6.72

Настройте обновление индекса с интервалом 20 минут (см. Рисунок 6.73).

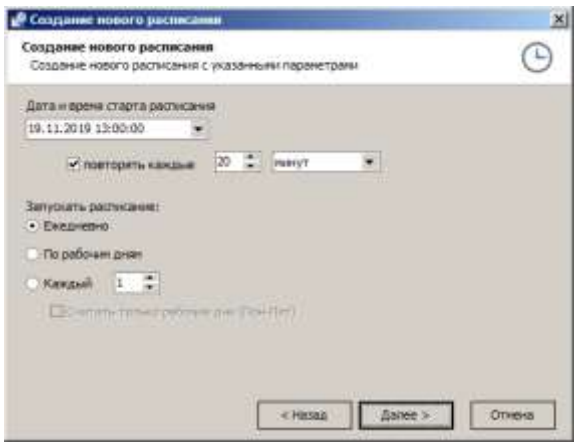


Рисунок 6.73

Созданное расписание отобразится во вкладке «Планировщик». Для изменения параметров расписания используйте кнопку «Изменить расписание» (см. Рисунок 6.74).

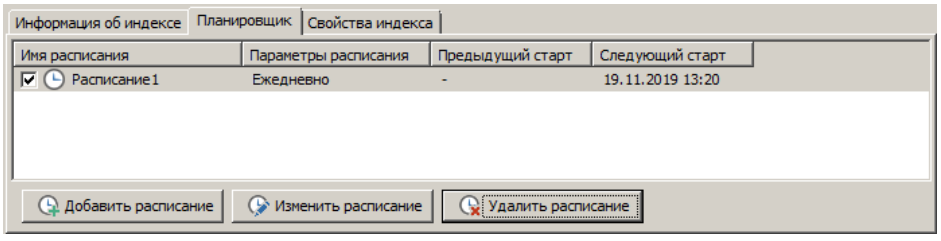


Рисунок 6.74

6.5.1.1 Настройка модуля перехвата FileAuditor

Модуль перехвата FileAuditor позволяет:

- производить сканирование файлов, хранящихся как на компьютерах пользователей, так и на серверах, и в сетевых папках;
- формировать дерево каталогов/файлов, а также перечень прав доступа к ним;

– контролировать операции с файлами (с помощью компонента FileController).

Сканирование ресурсов согласно настроенным правилам осуществляется:

- агентом;
- службой анализа данных на сервере.

Для модуля FileAuditor создаются база данных и хранилище, которые затем соответствующим образом настраиваются. **База данных** используется для хранения журнала аудита операций, производимых с файлами. **Файловое хранилище** – для хранения теневых копий файлов.

Порядок действий для подключения базы/хранилища[17] FileAuditor (если не было выполнено в п. 6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «FileAuditor» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.75).

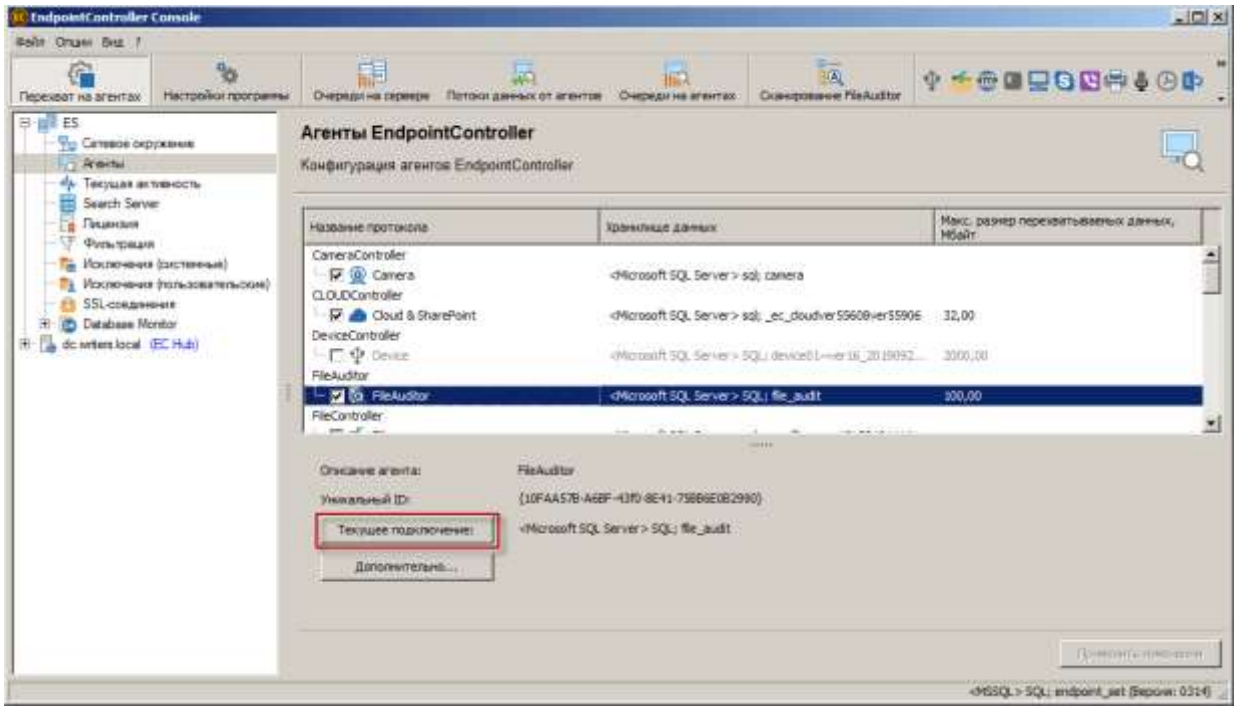


Рисунок 6.75

2. Настройте подключение к базе данных. Порядок действий для создания базы FileAuditor аналогичен вышеизложенному порядку создания базы данных FileController (см. Таблица 22). Порядок действий для создания хранилища FileAuditor аналогичен вышеописанному порядку создания хранилища FTPController (см. Таблица 23).

Управление агентом с подключенной базой производится на вкладке «Агенты» консоли администрирования. Выделите протокол FileAuditor и двойным щелчком

[17] Базы данных и хранилища не разбиваются.

откройте окно редактирования агента (другие варианты: щёлкните кнопку  на панели «Конфигурирование агентов» либо кнопку «Дополнительно») (см. Рисунок 6.76).

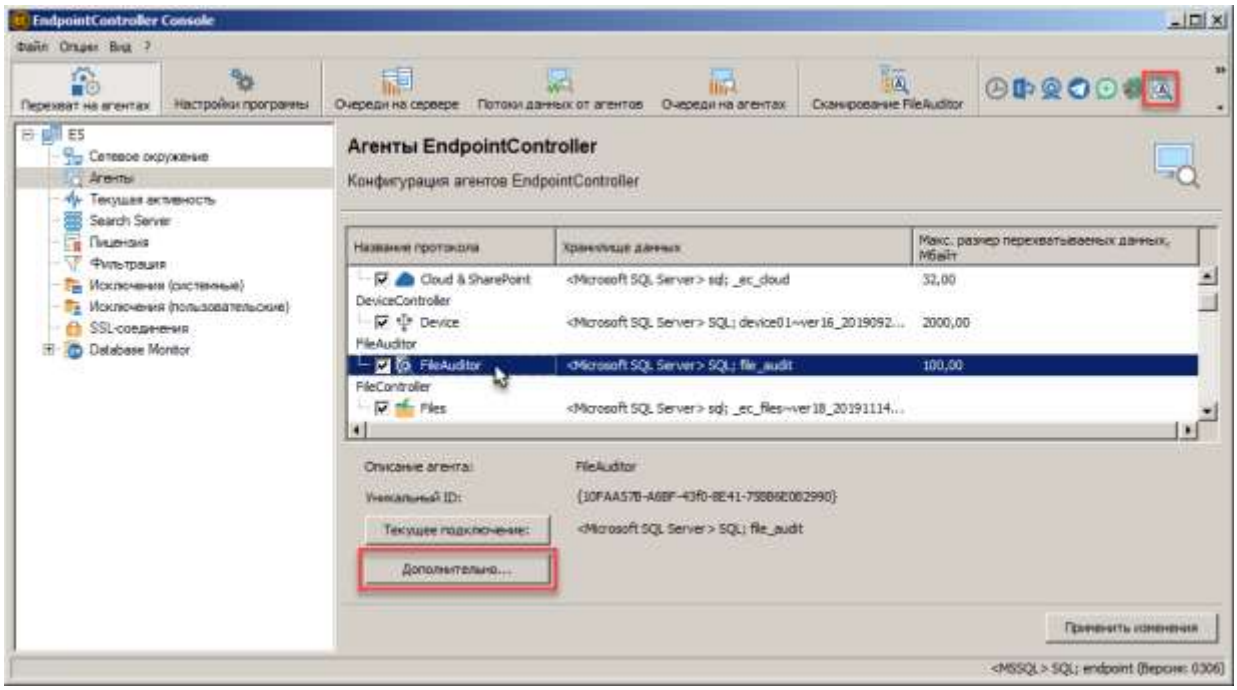


Рисунок 6.76

В открывшемся окне перейдите в узле «**Настройки**» на вкладку «**Хранилище данных**» и укажите следующие параметры:

- Путь к папке хранилища[18], в которой хранятся теневые копии файлов, подпавших под условия правил.
- Настройки подключения, используемые для подключения к указанному хранилищу (имя пользователя и пароль, наименование домена).
- Количество последних версий файлов для хранения (см. Рисунок 6.77).

[18] Путь к хранилищу должен быть указан обязательно, независимо от того, имеются настроенные правила аудита/теневого копирования или нет.

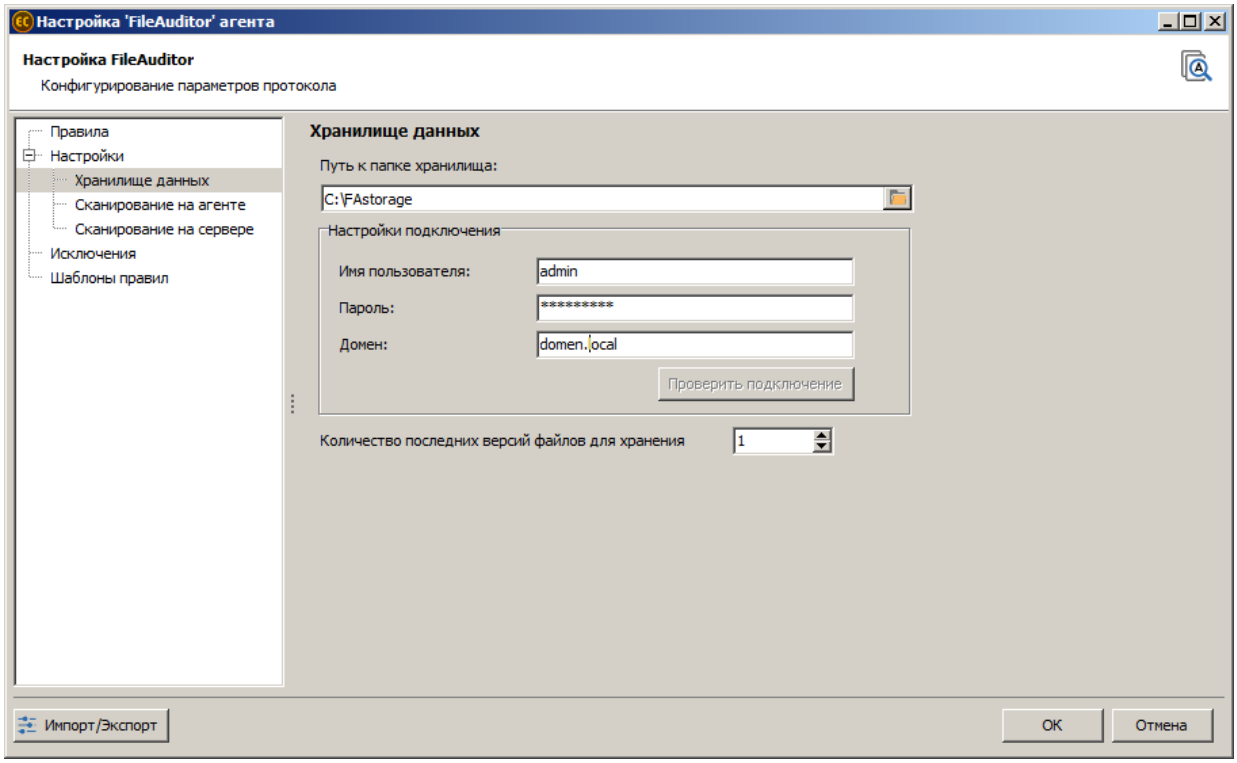


Рисунок 6.77

На вкладке «**Сканирование на агенте**»[19] укажите параметры, используемые при сканировании файлов с помощью агента (см. Рисунок 6.78).

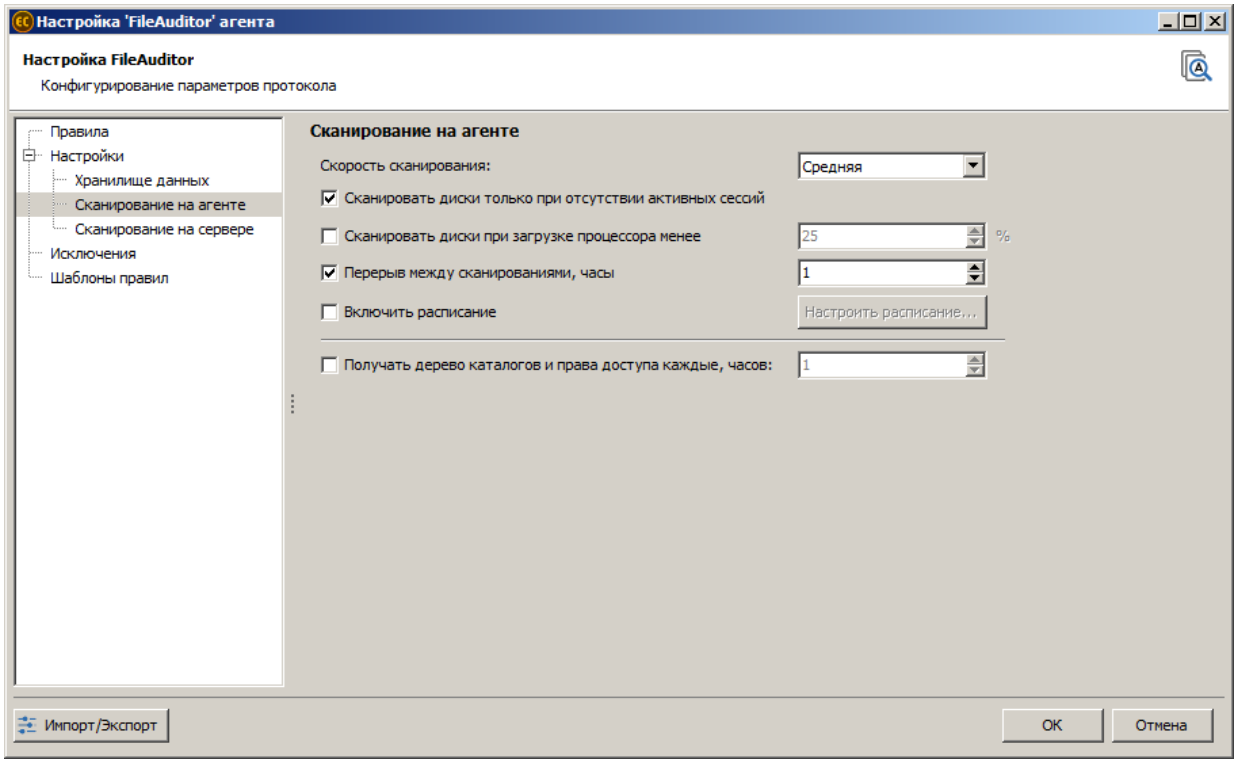


Рисунок 6.78

[19] Агент сканирует только диски файловой системы NTFS.

Таблица 20 содержит перечень параметров сканирования агентом.

Таблица 20 – Перечень параметров сканирования агентом FileAuditor

Настройка	Описание
Скорость сканирования	Высокая скорость сканирования может существенно повысить нагрузку на процессор/жесткий диск (особенно при поиске по типам файлов).
Сканировать диски только при отсутствии активных сессий	Фоновая проверка файлов будет запускаться только при отсутствии активных сессий на рабочей станции.
Сканировать диски при загрузке процессора менее…%	Фоновая проверка файлов будет запускаться при загрузке процессора ниже указанного значения.
Перерыв между сканированиями, часы	Включение/отключение периодической отправки агентом дерева папок и прав. При снятом флажке агент отправляет только те данные, которые соответствуют настроенным правилам сканирования.
Включить расписание	Включение/отключение расписания работы фонового сканирования файлов
Получать дерево каталогов и права доступа каждые, часов	Включение/отключение периодической отправки агентом дерева папок и прав. Если флажок снят, агентом будут отправлены только те данные, которые соответствуют настроенным правилам сканирования.

Кроме агента сканирование файловой системы может производиться **серверной службой FileAuditor.** Серверная служба подключается к папкам серверов, указанных в списке, для сканирования файлов с учетом настроенных правил и исключений.

Перейдите на вкладку **«Сканирование на сервере»** и установите флажок **Включить сканирование** для активации работы службы сканирования и доступа к ее настройкам.

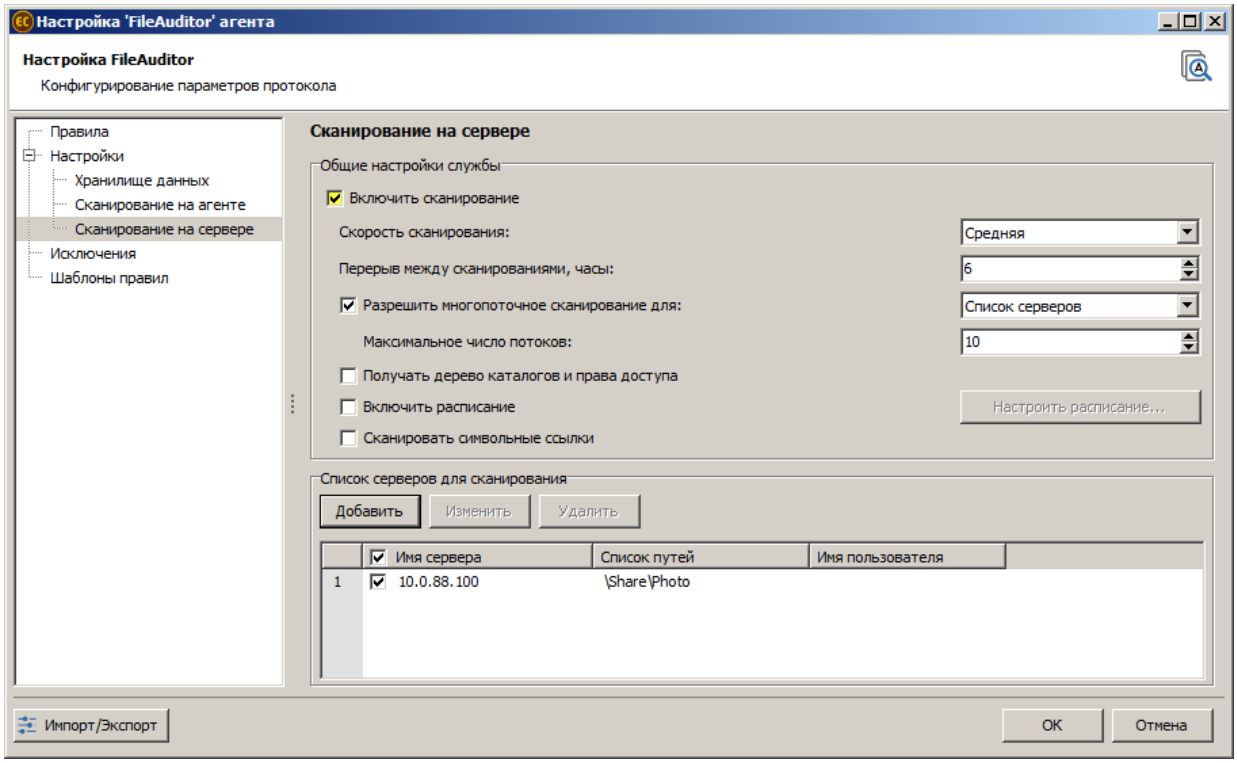
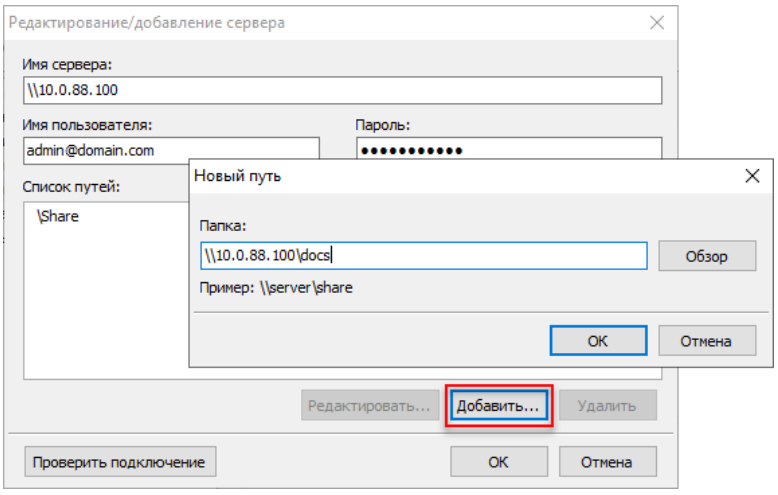


Рисунок 6.79

Таблица 21 содержит описание настроек службы сканирования на сервере.

Таблица 21 – Настройки службы сканирования на сервере

Настройка	Описание
Скорость сканирования	Высокая скорость сканирования может существенно повысить нагрузку на процессор/жесткий диск (особенно при поиске по типам файлов)
Перерыв между сканированиями, часы	Промежуток времени между операциями сканирования файлов, к которым было обращение. Минимальное значение - 1 час, максимальное - 168 часов. Если флажок снят, сканирование осуществляется раз в сутки.
Разрешить многопоточное сканирование для:	Включение/отключение сканирования в несколько потоков: • ***Списка серверов*** Сканирование серверов в списке будет осуществляться в количество потоков, заданное в параметре **Максимальное число потоков**. *Например, при значении «3» и пяти серверах в списке будут одновременно сканироваться три сервера, остальные два ожидают освобождения какого-либо из потоков.* • ***Каждого отдельного сервера*** При выборе данной опции значение параметра **Максимальное число потоков** будет распространяться на каждый сервер из списка. *Например, при значении "3" каждый сервер в списке*

Настройка	Описание
	будет сканироваться в три потока, а остальные сервера - дожидаться завершения сканирования вышестоящего в списке сервера.
Максимальное число потоков	Сканирование серверов в списке будет осуществляться в указанное количество потоков.
Получать дерево каталогов и права доступа	Включение/отключение ежедневной отправки агентом дерева папок и прав. Если флажок снят, агентом будут отправлены только те данные, которые соответствуют правилам сканирования.
Включить расписание	Включение/отключение расписания работы фоновой проверки файлов
Сканировать символьные ссылки	Включение/отключение сканирования директорий, переход к которым осуществляется по символьным ссылкам, расположенным на сервере
Список серверов для сканирования	Для добавления сервера в список нажмите кнопку **Добавить**. В появившемся окне задайте: • Имя или IP-адрес сканируемого сервера; • Параметры учетной записи, имеющей доступ к указанным директориям сервера; • Список путей, которые требуется сканировать. Папки, указываемые в качестве нового пути, не должны пересекаться с уже имеющимися в списке.  Нажмите **OK** для применения настроек.

Настройка правил сканирования

На вкладке **«Правила»** задаются параметры теневого копирования и аудита файлов. При добавлении нового правила указываются:

- объекты, которые подлежат сканированию или исключаются из него (папки, файлы, типы файлов);
- условия поиска, применяемые к заданным объектам (поиск по тексту/по атрибутам файлов/по регулярным выражениям/по словарю).

Для управления списком правил используются кнопки:

- **Добавить** – создание нового правила;
- **Создать по шаблону** – создание правила на основе шаблона (кнопка активна при наличии хотя бы одного настроенного шаблона на вкладке «Шаблоны правил»);
- **Изменить** – редактирование имеющегося в списке правила;
- **Удалить** – удаление правила из списка (см. Рисунок 6.80).

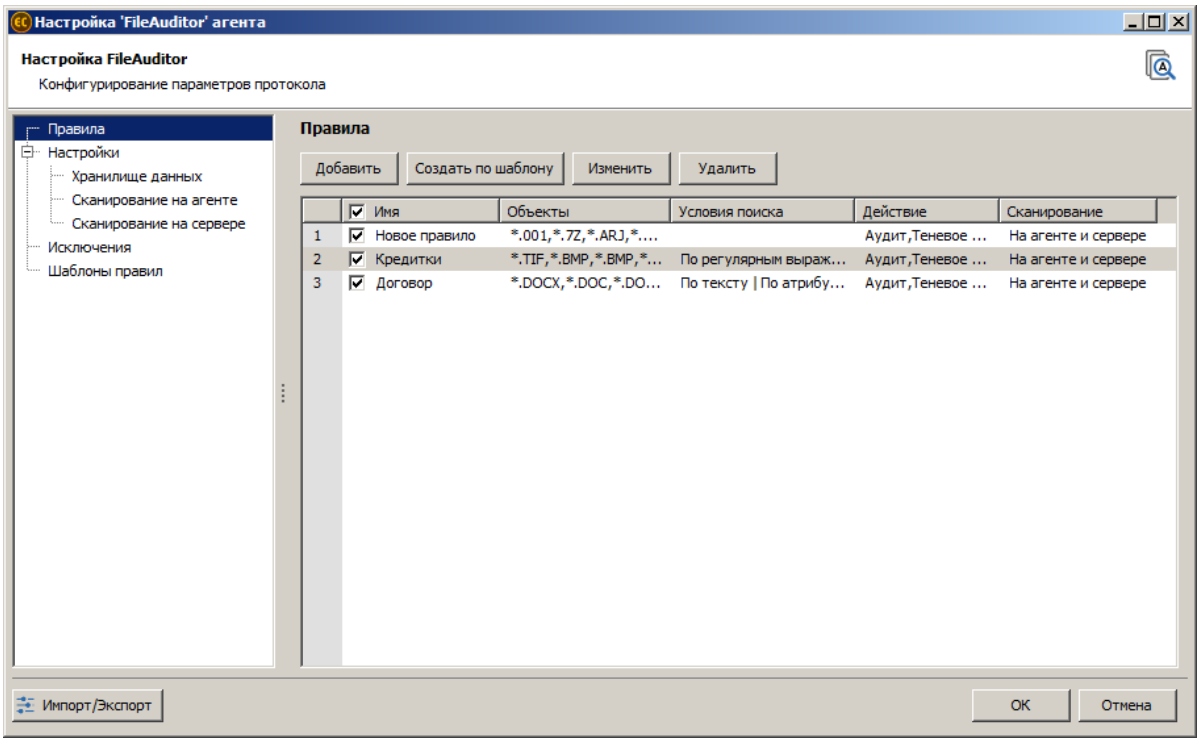


Рисунок 6.80

Щелкните кнопку **«Добавить»**. Появится диалоговое окно «Добавление нового правила». Введите имя правила и выберите действие, которое будет применяться к файлам при соответствии правилу:

- *Теневое копирование* - запись в хранилище файлов, обнаруженных в результате сканирования.
- *Аудит* - помещение в базу данных только информации о файлах, которые соответствуют правилам сканирования (без теневой копии самих файлов) (см. Рисунок 6.81).

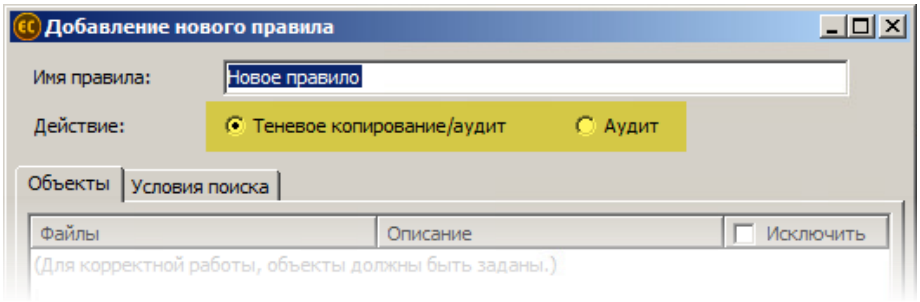


Рисунок 6.81

На вкладке **«Объекты»** настройте список файлов/типов файлов, которые необходимо контролировать. Для этого щелкните по стрелке рядом с кнопкой «Добавить» и выберите одну из опций:

- По имени... - для применения правила к типам файлов, когда тип файла определяется расширением, указанным в имени файла;
- По типу... - для применения правила к типам файлов, когда тип файла определяется выполняемым процессом (следует учитывать, что поиск по типу значительно повышает нагрузку на процессор/жесткий диск, особенно, если условиями поиск не ограничен - например, задан весь диск рабочей станции, а не конкретная директория);
- Папки - для применения правила к файлам, расположенным в указанной директории;
- (любой файл) - для применения правила к файлу любого формата (формат можно задать вручную) (см. Рисунок 6.82).

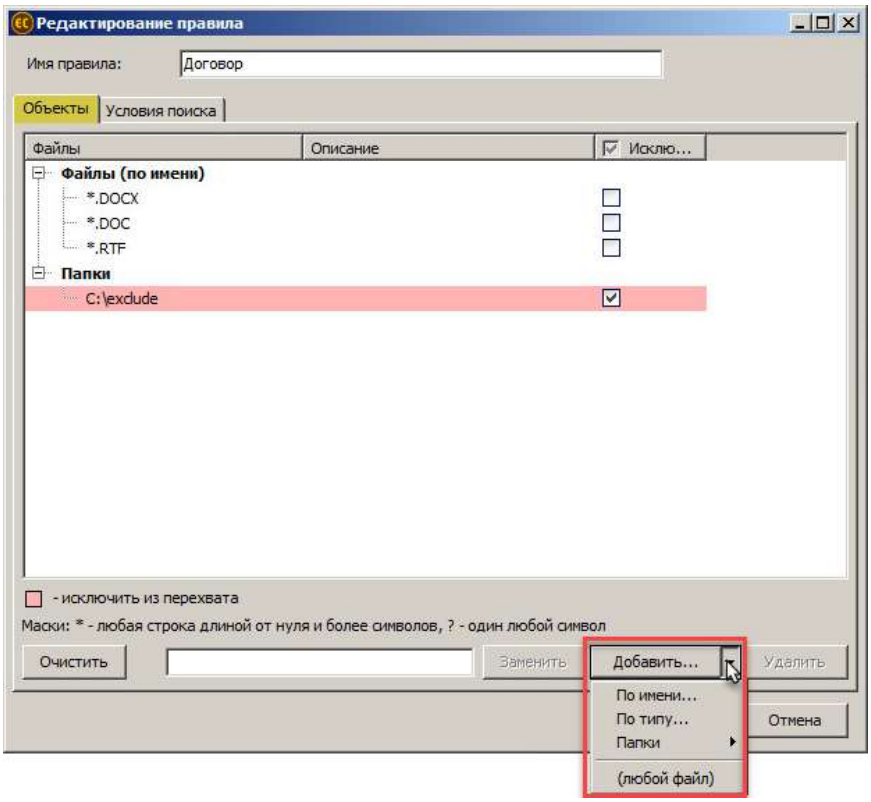


Рисунок 6.82

Файлы/папки внутри одной категории объединяются по логическому **ИЛИ** (на скриншоте выше: *.docx, *.doc, *.rtf), а сами категории между собой - по логическому **И** (на скриншоте выше: файлы (по имени), папки).

Для прекращения аудита какого-либо файла или папки они могут быть добавлены в исключения путем установки флажка в столбце «Исключить» напротив исключаемого файла/папки.

Внимание! *Не настраивайте исключения в отдельном правиле! Например, если в одном правиле настроить аудит файлов *.DOCX, а в другом - исключение контроля папки C:\exclude, исключение НЕ будет работать корректно.*

На вкладке **«Условия поиска»** настраиваются поисковые запросы, которые будут применены к указанным файлам. Запросы могут объединяться логическими **И** и **ИЛИ.** Для добавления нового запроса нажмите «Добавить»(см. Рисунок 6.83).

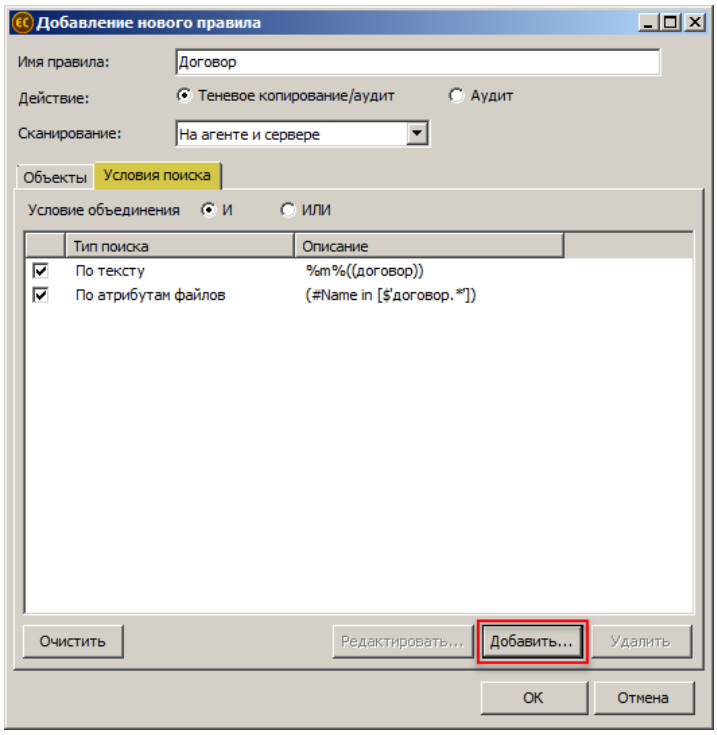


Рисунок 6.83

В открывшемся окне «Условия поиска»:

1. Выберите тип поиска.
2. Введите текст для поиска.
3. Укажите дополнительные параметры поиска, определяемые выбранным типом поиска (см. Рисунок 6.84).

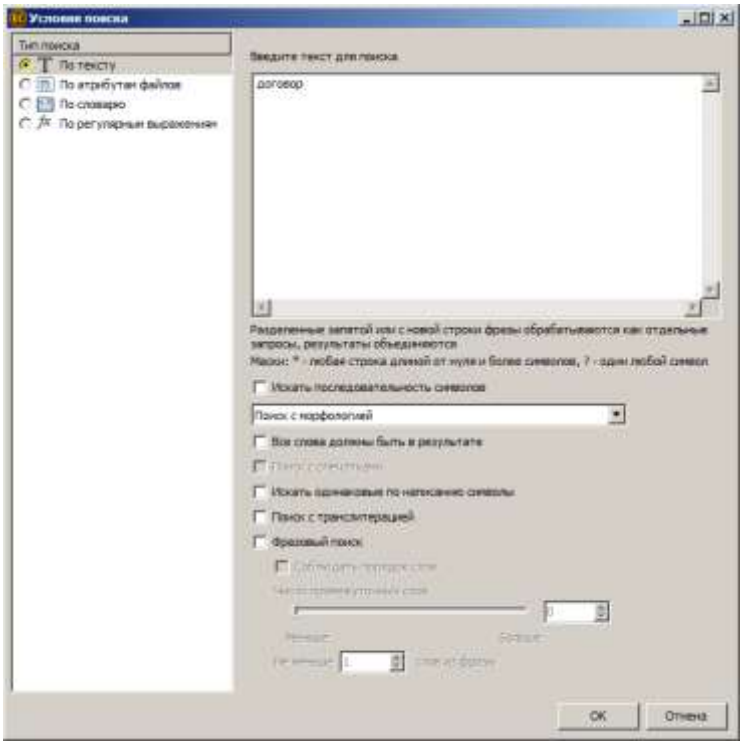


Рисунок 6.84

Настройка исключений

На вкладке «Исключения» укажите перечень файлов/папок и сетевых путей, которые необходимо исключить из сканирования. Присутствует как предустановленный список исключений, так и возможность задать собственные значения.

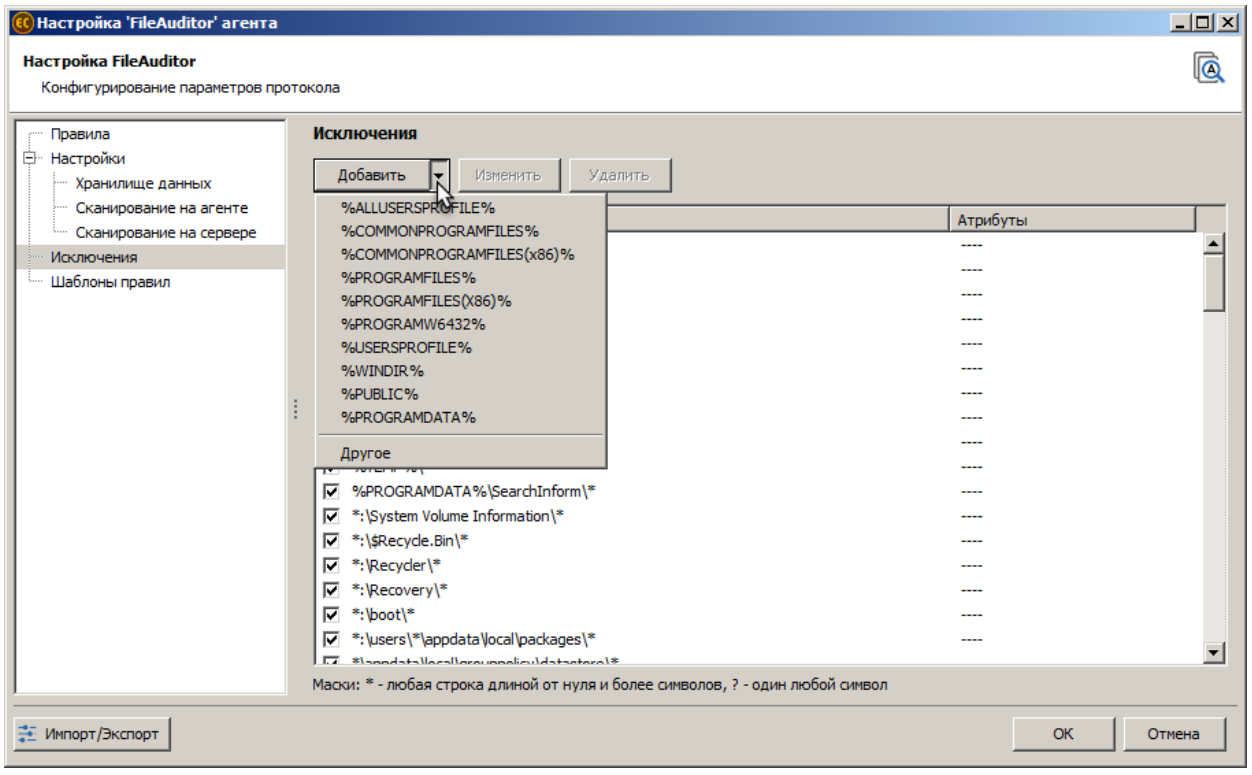


Рисунок 6.85

Настройка шаблонов правил

На вкладке «Шаблоны правил» осуществляется настройка шаблонов, которые могут быть в дальнейшем использованы при создании правил сканирования на вкладке «Правила». Настройка шаблона аналогична созданию типичного правила сканирования и осуществляется по нажатии кнопки «Добавить».

Также имеется список предустановленных шалонов[20] (см. Рисунок 6.86).

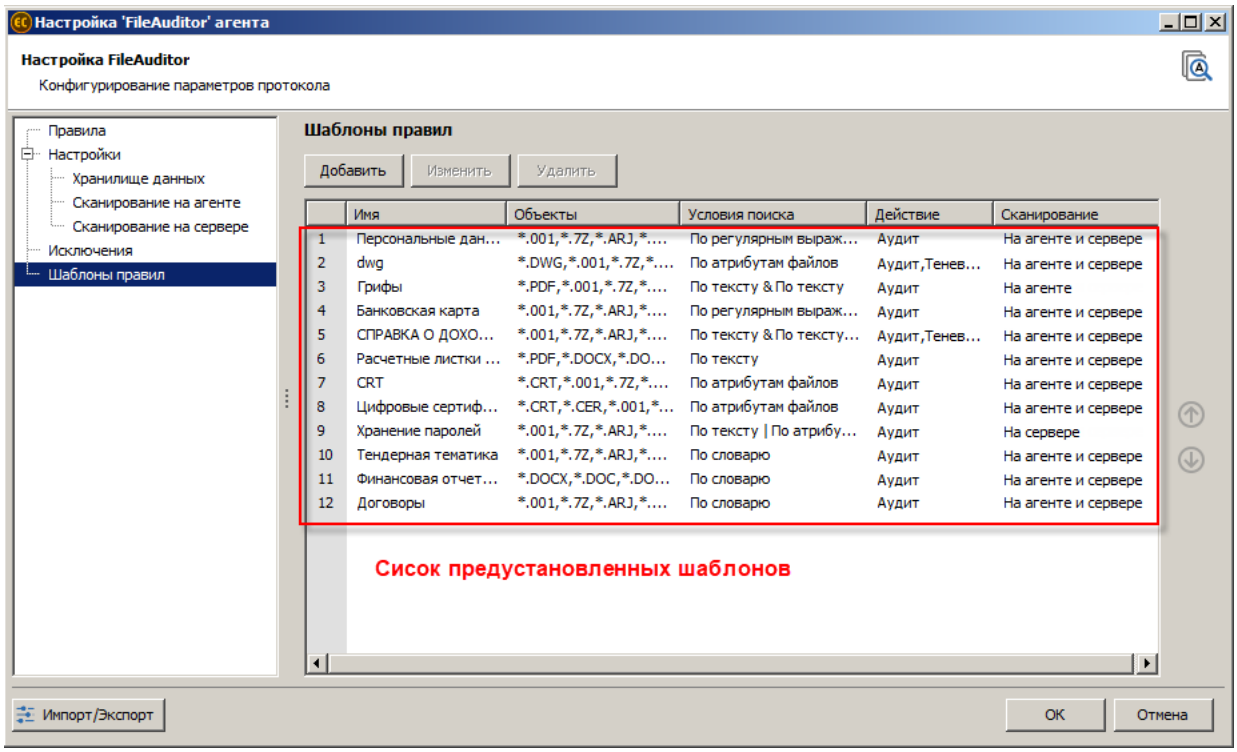


Рисунок 6.86

Чтобы произведенные настройки FileAuditor вступили в силу, нажмите «OK». После этого перейдите к настройке параметров контроля файловых операций (модуль FileController).

6.5.1.1.1 Настройка FileController

FileController является составной частью модуля перехвата FileAuditor и предназначен для контроля операций с файлами, хранящимися на серверах и в общих сетевых папках.

Для FileController создаются базы данных, которые затем соответствующим образом настраиваются. Базы данных FileController не привязываются к индексам.

Порядок действий для создания базы данных FileController (если не было выполнено в п. 6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке позицию «FileController» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.87).

[20] При необходимости шаблоны также могут быть импортированы из файла формата XML.

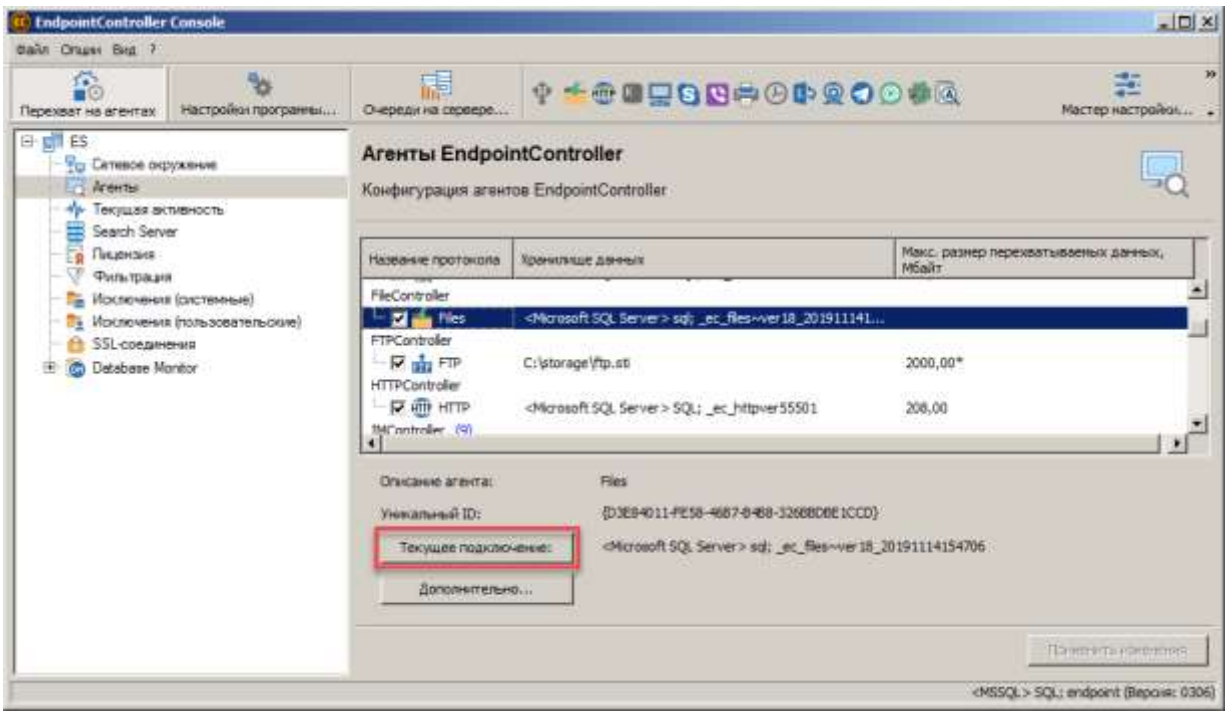
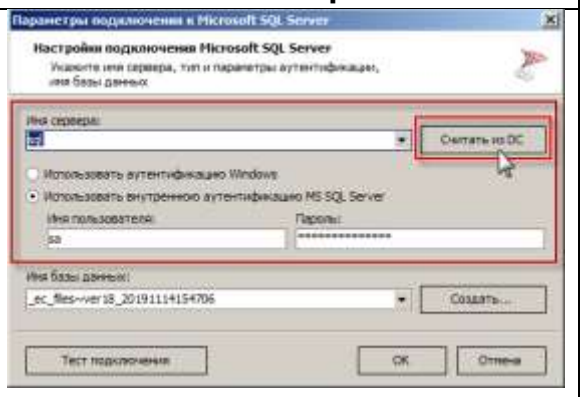
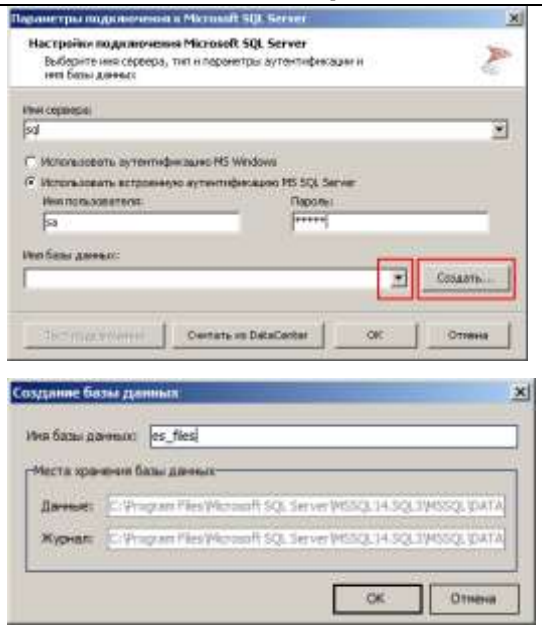
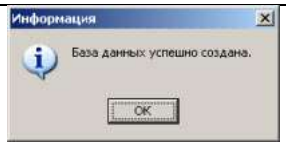


Рисунок 6.87

2. Настройте подключение к базе данных. Процесс подробно описан в Таблица 22.

Таблица 22 – Настройка подключения к базе данных

Действие	Снимок экрана
Введите параметры подключения вручную (в поле «Имя сервера» можно вводить имя или IP-адрес сервера Microsoft SQL). Если модуль DataCenter был предварительно настроен, щёлкните кнопку «Считать из DataCenter». Параметры «Имя сервера», «Имя пользователя» и «Пароль» будут автоматически считаны из сервера DataCenter.	

Действие	Снимок экрана
Из выпадающего списка выберите базу данных EndpointController. Для проверки подключения щелкните «Тест подключения». В случае отсутствия нужной базы создайте новую базу: 1) Щёлкните кнопку «Создать». 2) В открывшемся окне «Создание базы данных» введите имя создаваемой базы данных. 3) При необходимости измените места хранения базы данных и журнала транзакций по умолчанию. 4) Подтвердите настройки нажатием ОК.	
При успешном создании базы данных будет отображено окно с подтверждающим сообщением.	

Управление агентом с подключенной базой производится на вкладке «Агенты» консоли администрирования. Выделите протокол FileController и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку  на панели «Конфигурирование агентов:» либо кнопку «Дополнительно») (см. Рисунок 6.88).

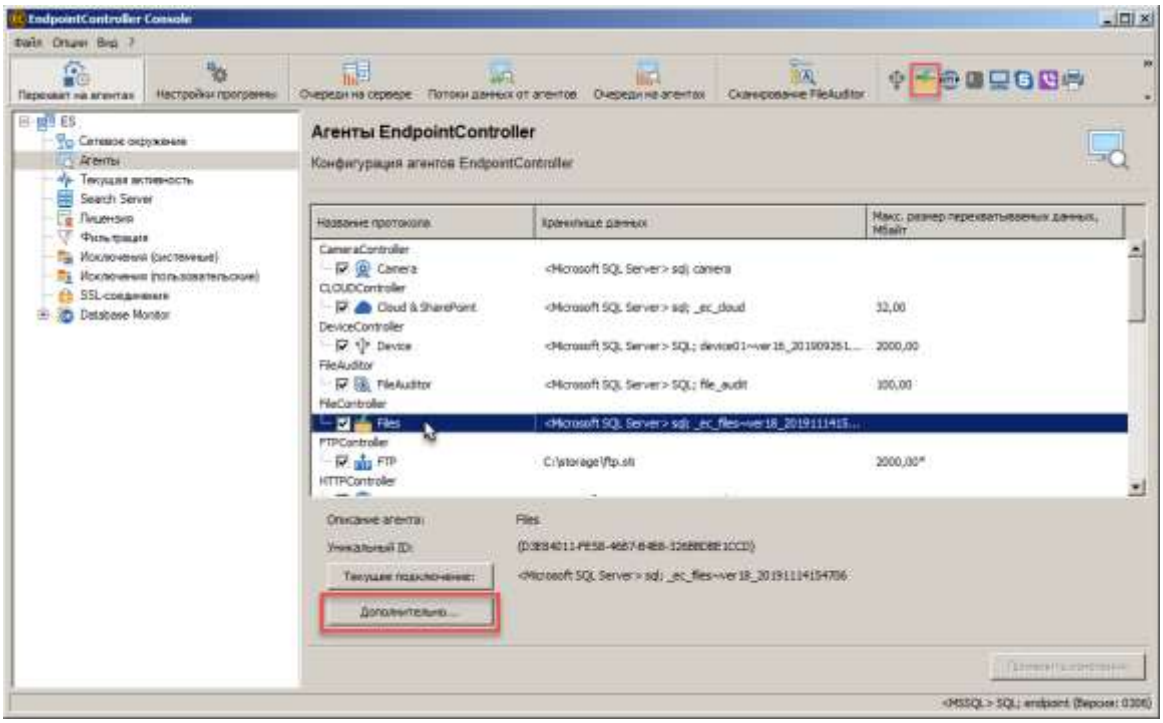


Рисунок 6.88

В диалоговом окне «Редактирование 'Files' агента» отображается настроенный перечень правил аудита (см. Рисунок 6.89). Для управления списком используются следующие кнопки:

- **Добавить** – создание нового правила аудита;
- **Редактировать** – изменение имеющегося в списке правила;
- **Удалить** – удаление правила из списка.

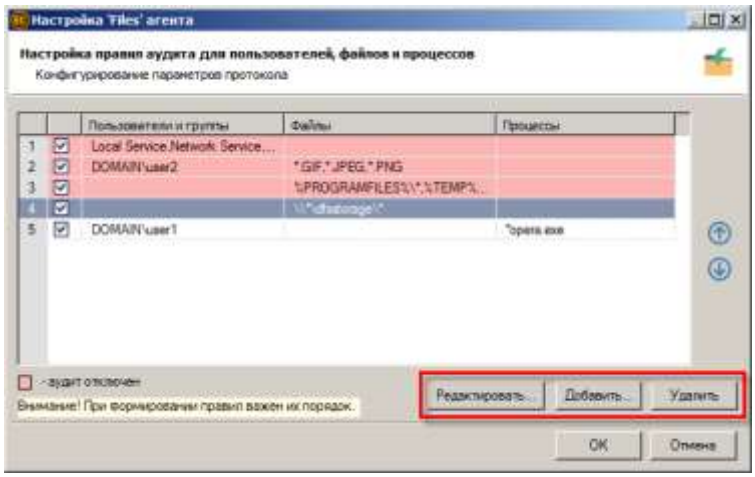


Рисунок 6.89

Щёлкните кнопку «Добавить».

В открывшемся окне добавления правила аудита произведите необходимые настройки параметров фильтрации, позволяющей включить в перехват или исключить из него отдельных пользователей, файлы и процессы (см. Рисунок 6.90).

Рисунок 6.90

В левой части окна определяется один или несколько пользователей, к которым будут применены одни и те же правила аудита, в левой части – перечень файлов и процессов, к которым будет применен аудит (см. Рисунок 6.91).

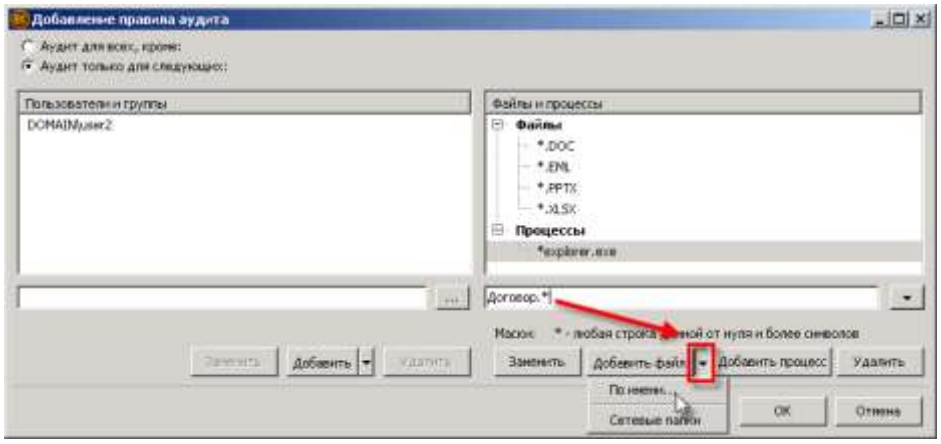


Рисунок 6.91

Рекомендуется добавить системных пользователей к числу исключаемых из аудита, чтобы не вести учет операций с файлами, совершаемых системой (см. Рисунок 6.92).

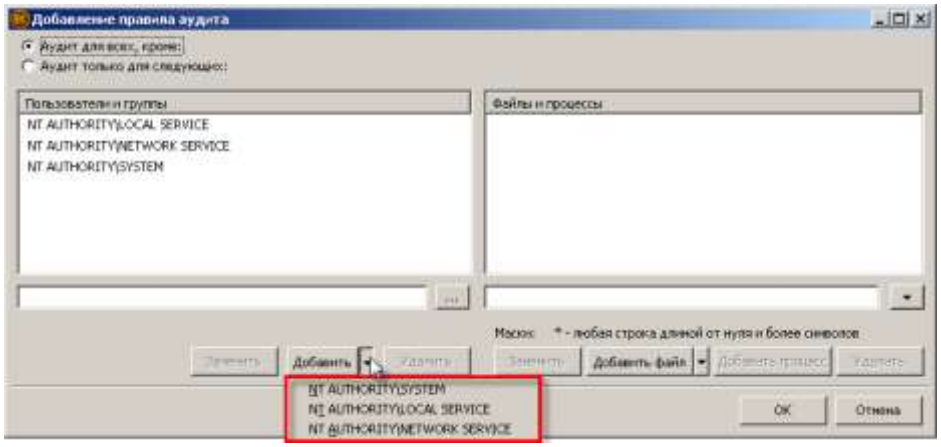


Рисунок 6.92

При работе в текстовом редакторе Microsoft Word автоматически создаются временные файлы с расширением .tmp. Для отключения аудита операций над такими временными данными отметьте флажком параметр «Отключить аудит операций с временными файлами MS Word» (см. Рисунок 6.93).

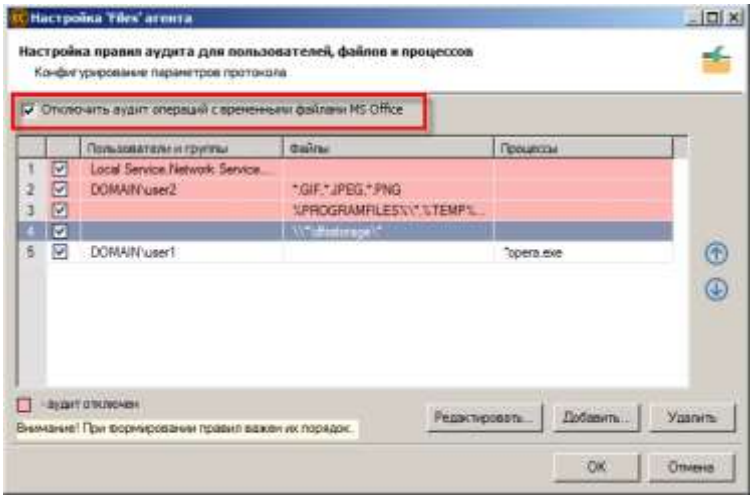


Рисунок 6.93

Для сохранения настроек в окнах добавления и редактирования правил нажмите OK, а затем щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведенные настройки агента FileController вступили в силу.

6.5.1.2 Настройка модуля перехвата FTPController

Модуль перехвата FTPConroller предназначен контролировать трафик, передаваемый через FTP/FTPS-соединение, и утечку «тяжелых» файлов (например, баз данных, ПО, проектной документации).

Для компонента FTPController должно быть создано файловое хранилище, которое затем привязывается к индексам.

Порядок действий для создания хранилища FTPController (если не было выполнено в п.6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «FTPController» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.94).

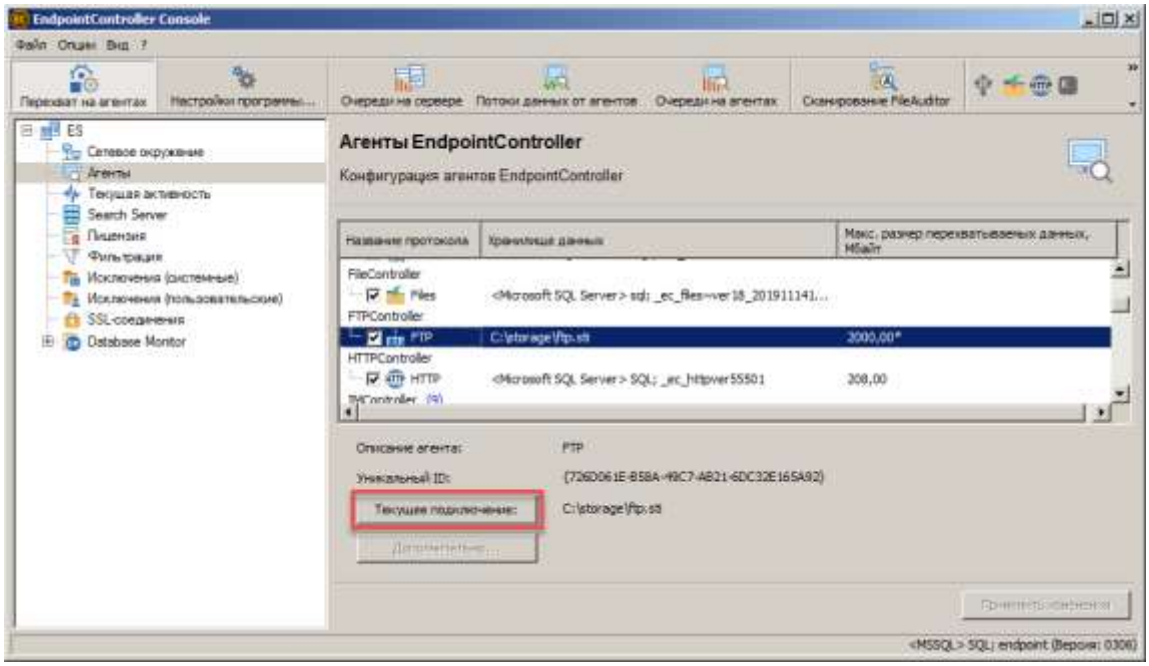


Рисунок 6.94

3. В открывшемся окне конфигурирования FTP задайте необходимые настройки, перечисленные в Таблица 23.

Таблица 23 – Настройки хранилища FTP

Настройка	Описание	Комментарий
Имя файла хранилища	Путь к файлу хранилища, в котором будут храниться перехваченные файлы.	Папка, в которой расположен файл хранилища, не должна совпадать с папкой временных файлов.
Путь к FTP файлам	Путь к папке, в которой будут храниться временные файлы.	

Остальные настройки в окне конфигурирования FTP оставьте по умолчанию, как показано на Рисунок 6.95.

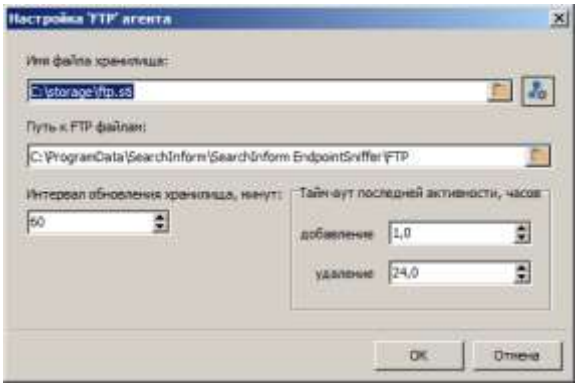


Рисунок 6.95

4. Нажмите «OK», а затем щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведенные настройки вступили в силу.

6.5.1.3 Настройка модуля перехвата DeviceController

Модуль перехвата DeviceController контролирует передачу данных на внешние устройства, подключаемые к рабочим станциям пользователей (USB, CD/DVD, камеры, сканеры, внешние диски и др.). Позволяет заблокировать доступ к устройствам/портам/папкам, а также запретить операции с файлами на устройствах.

Для компонента DeviceController создается файловое хранилище, которое затем соответствующим образом настраивается. Хранилище DeviceController должно быть привязано к индексам.

Помимо хранилища, для модуля перехвата DeviceController создается база данных для хранения журнала аудита внешних устройств. Журнал содержит данные об операциях, выполняемых на внешних устройствах.

Порядок действий для создания хранилища/базы DeviceController (если не было выполнено в п. 6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке позицию «DeviceController» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.96).

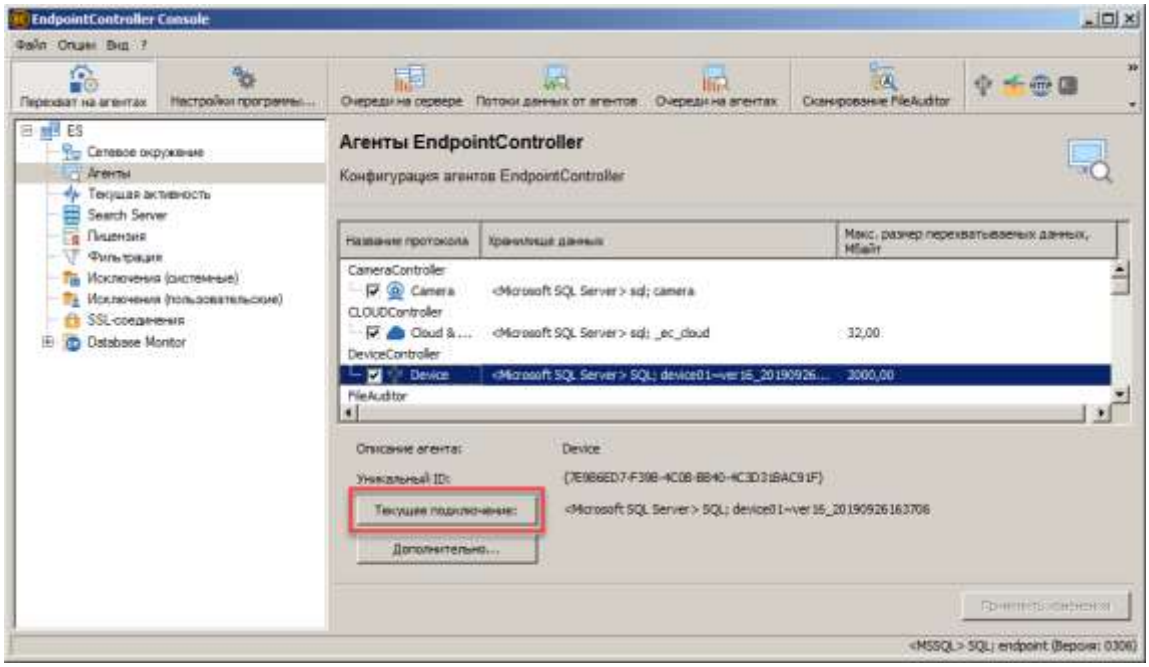


Рисунок 6.96

3. Настройте подключение к хранилищу или базе данных.

Порядок действий для создания базы DeviceController аналогичен порядку создания базы данных FileController, изложенному в Таблица 22.

Порядок действий для создания хранилища DeviceController аналогичен вышеописанному порядку создания хранилища FTPController (см.Таблица 23).

Управление агентом с подключенной базой производится на вкладке «Агенты» консоли администрирования. Выделите протокол DeviceController щёлкните кнопку  на панели «Конфигурирования агентов:» либо кнопку «Дополнительно») (см. Рисунок 6.97).

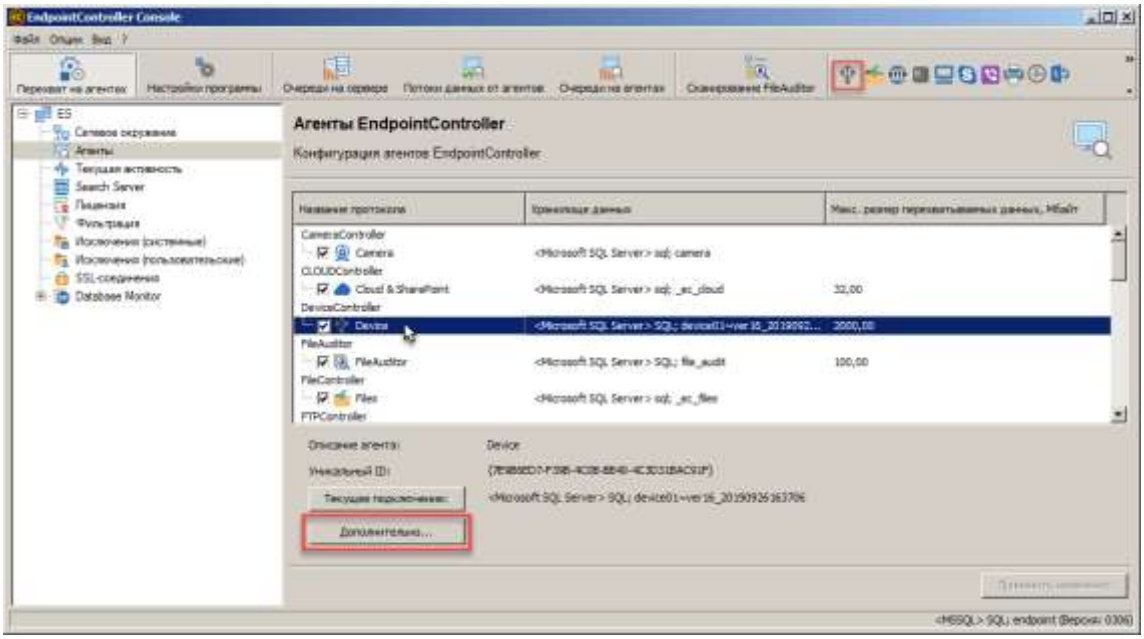


Рисунок 6.97

В открывшемся окне редактирования агента DeviceController на вкладке «Настройки» произведите следующие настройки:

- Задайте имя и местоположение хранилища для теневого копирования данных, перехваченных агентом DeviceController (файл будет иметь расширение .sti).
- Над списком внешних устройств установите флажок, если необходимо, чтобы системные пользователи исключались из аудита и теневого копирования.
- Выберите из списка тип внешнего устройства и задайте для него параметры доступа и аудита, воспользовавшись кнопкой «Редактировать» (см. Рисунок 6.98).

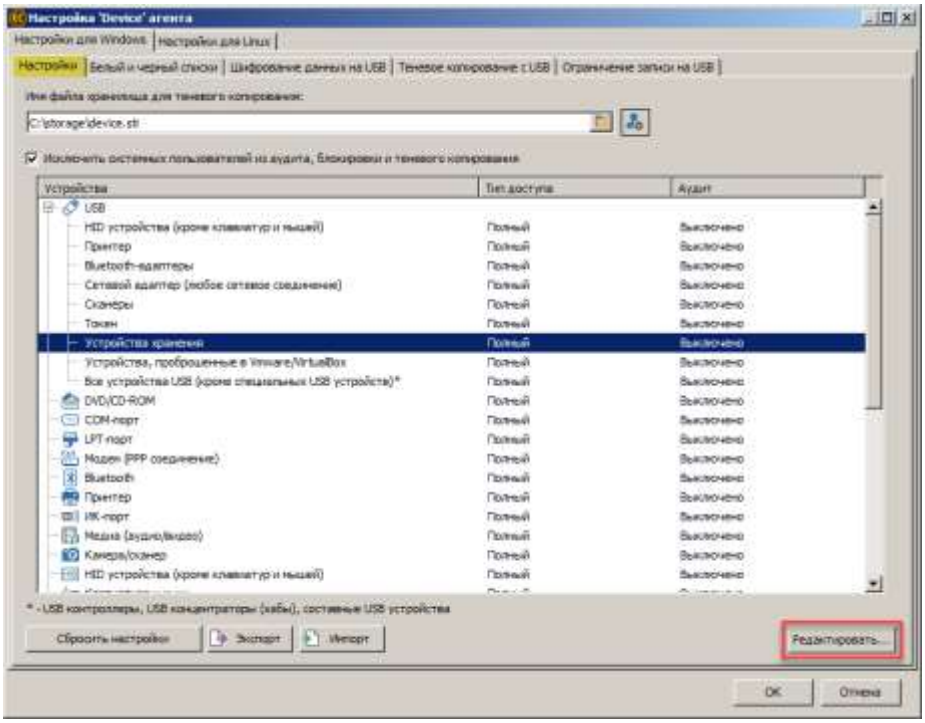


Рисунок 6.98

На вкладке «Белый список» настройте список внешних устройств, на которые действие агента DeviceController распространяться не будет.

Вкладка «Шифрование устройств хранения USB» позволяет задать пользователей/группу, записываемые данные которых будут зашифрованы, а также пользователей/группу, доступ к зашифрованным данным для которых будет либо разрешен, либо заблокирован.

Вкладка «Теневое копирование с USB» позволяет настроить правила теневого копирования данных с подключаемых usb-устройств.

Вкладка «Ограничение записи на USB» позволяет настроить ограничение записи данных на подключаемые usb-устройства по объему.

При выборе на этапе установки пункта «Модули поддержки Linux» также будут доступны настройки модуля DeviceController для рабочих станций на ОС Ubuntu (версии 16.04, 17.04, 18.04). На вкладке «Настройки для Linux» осуществляется управление доступом к подключаемым устройствам и сетевым ресурсам (см. Рисунок 6.99).

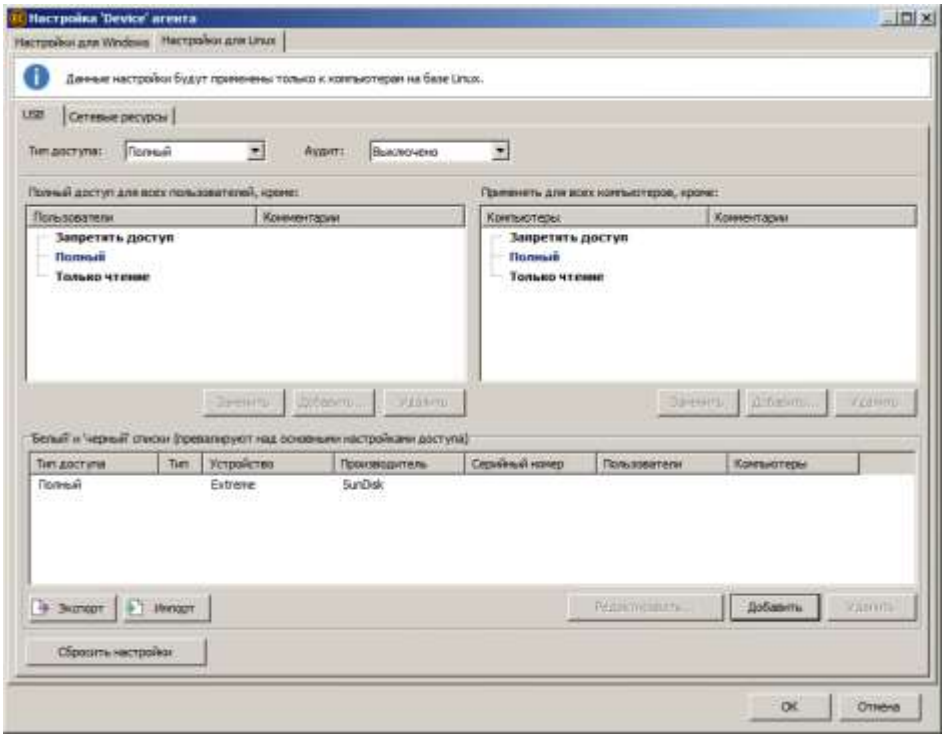


Рисунок 6.99

Для сохранения настроек в окне редактирования нажмите «OK», а затем щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведенные настройки агента DeviceController вступили в силу.

6.5.1.4 Настройка модуля перехвата HTTPController

Модуль перехвата HTTPController предназначен для перехвата POST- и GET-запросов, формируемых пользователями; позволяет перехватывать HTTP/HTTPS-трафик, переданный с помощью браузера, а также блокирует посещение запрещенных веб-ресурсов.

Для модуля HTTPController создается база данных, которая затем соответствующим образом настраивается. Базы данных HTTPController необходимо привязывать к индексам.

Порядок действий для создания базы HTTPController (если не было выполнено в п. 6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке позицию «HTTPController» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.100).

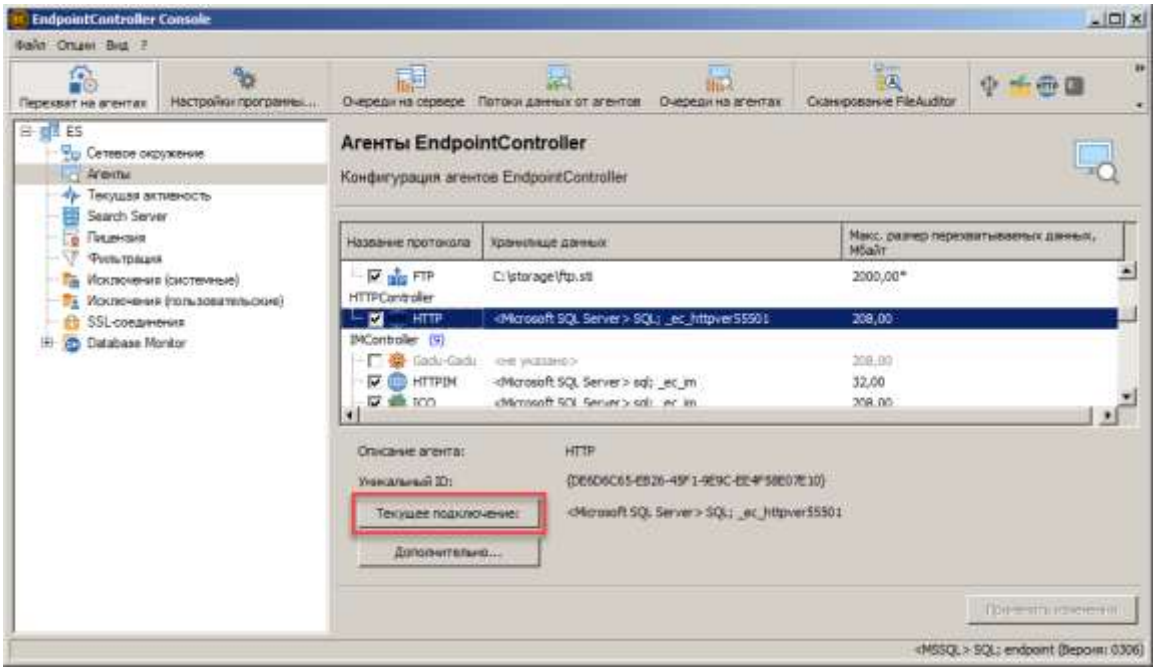


Рисунок 6.100

2. Настройте подключение к базе данных. Порядок действий для создания базы HTTPController аналогичен вышеизложенному порядку создания базы данных FileController (см. Таблица 22).

Управление агентом с подключенной базой производится на вкладке «Агенты» консоли администрирования. Выделите протокол HTTPController и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку  на панели «Конфигурирование агентов» или кнопку «Дополнительно») (см. Рисунок 6.101).

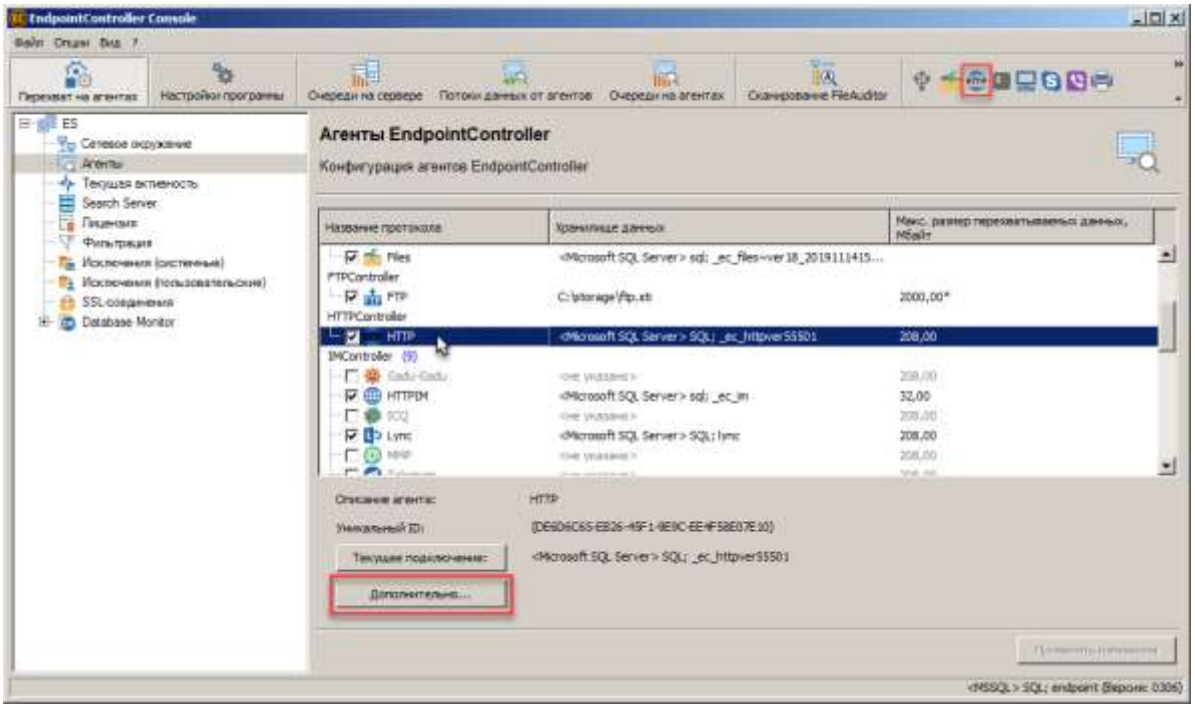


Рисунок 6.101

Окно редактирования агента HTTPController позволяет:

- производить настройку минимального размера перехватываемых данных (чекбокс «Включить перехват HTTP POST'ов» и поле «Минимальный размер тела POST-запроса»).
- указывать ресурсы, доступ к которым должен быть заблокирован (части окна «Адрес сайта» и «Правила»).

Для внесения ресурса в список заблокированных введите его название в поле «Адрес сайта» (используйте маску «*» для исключения ресурса вместе с поддоменами либо добавьте символ «/» перед именем ресурса для исключения конкретного домена) и выберите условие, которое будет применяться к сайту: блокировать/исключать из блокировки.

При необходимости укажите комментарий к сайту (введите в текстовом поле вручную либо выберите из списка уже добавленных). Нажмите кнопку «Добавить». (см. Рисунок 6.102).

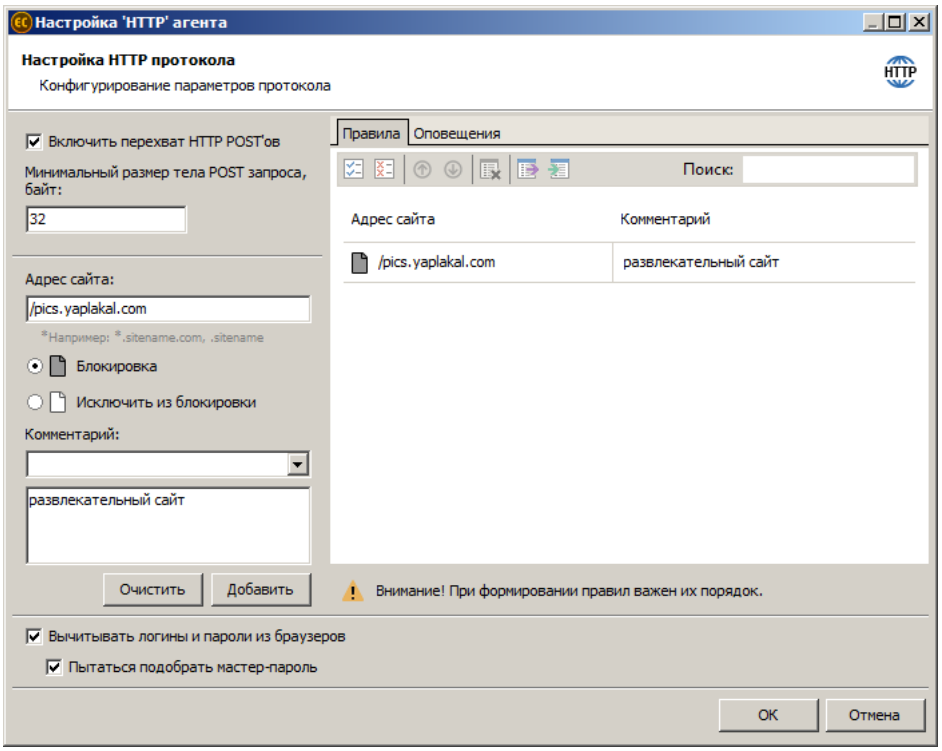


Рисунок 6.102

На вкладке «Правила» отображаются добавленные веб-ресурсы согласно сформированным правилам блокировки (*при формировании правил важно учитывать их порядок!*). Над списком сайтов расположены элементы управления:

- кнопка - выделить все/снять выделение для всех сайтов;
- кнопка - удаление выбранных сайтов из списка;
- кнопки и - управление порядком сайтов в списке;

- кнопка - экспорт списка сайтов в формат XML;
- кнопка - импорт списка сайтов из файлов формата XML или TXT;
- строка поиска/фильтрации сайтов.

Для редактирования выбранного ресурса нажмите , для удаления - .

Отметка параметра «Вычитывать логины и пароли из браузеров» активизирует функционал чтения сохраненных авторизационных данных пользователей из хранилища паролей браузеров Microsoft Edge, Opera, Internet Explorer, Mozilla Firefox, Google Chrome.

Доступ к хранилищу паролей в браузере Mozilla Firefox может блокироваться мастер-паролем. Для попытки подбора мастер-пароля из собственной базы данных паролей отметьте опцию «Пытаться подобрать мастер-пароль».

На вкладке «Оповещения» настройте действие, которое будет применено к пользователю при попытке открыть сайт, который был добавлен в список блокируемых:

- Не предпринимать никаких действий (только блокировать);
- Перенаправить пользователя на определенный веб-ресурс;
- Выводить пользователю указанное сообщение (см. Рисунок 6.103).

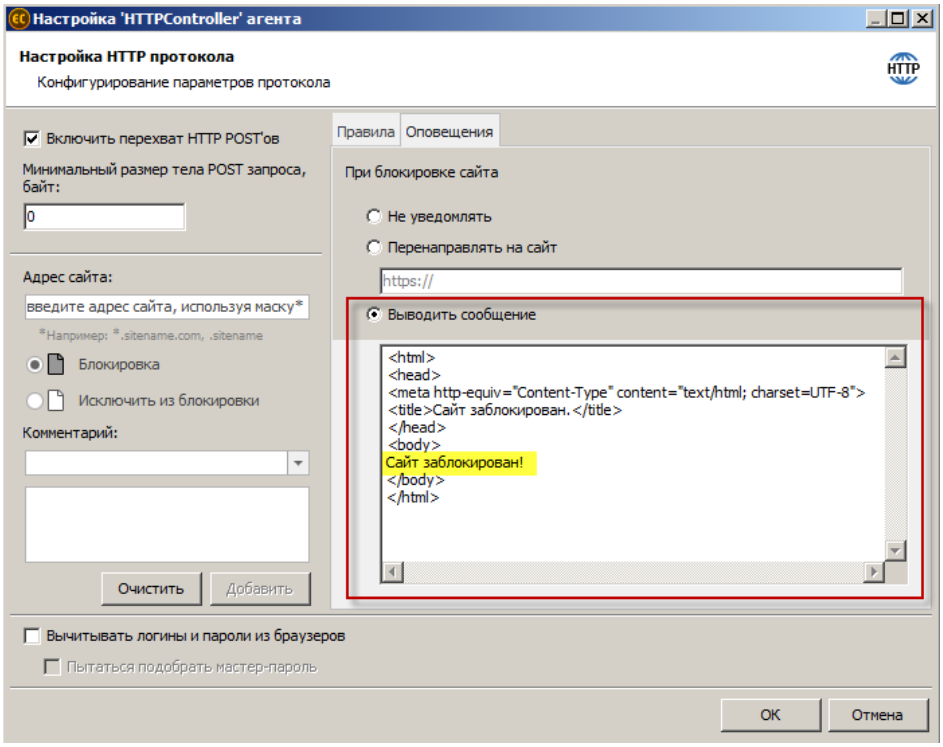


Рисунок 6.103

Для сохранения настроек нажмите «OK», а затем щёлкните кнопку «Применить изменения» в консоли администрирования EndpointController, чтобы произведённые настройки моуля перехвата HTTPController вступили в силу.

6.5.1.5 Настройка модуля перехвата CloudController & SharePoint

Модуль перехвата CloudController предназначен для контроля входящих и исходящих данных облачных сервисов. Модуль позволяет отслеживать данные популярных облачных хранилищ, таких как: Evernote, Skydrive (включая Office 365), Google Drive, Dropbox, Yandex Disk, MailRuCloud, SharePoint, ICloud, DropMeFiles, Amazon S3, OwnCloud, Pcloud, OziBox, MediaFire, OpenDrive, 4shared, Box, Syncplicity, CloudMe, MiMedia.

Для агента CloudController создается база данных, которая затем соответствующим образом настраивается. Базы данных CloudController необходимо привязывать к индексам.

Порядок действий для создания базы CloudController (если не было выполнено в п.6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «CLOUDController» и щёлкните кнопку «Текущее подключение» (см.Рисунок 6.104).

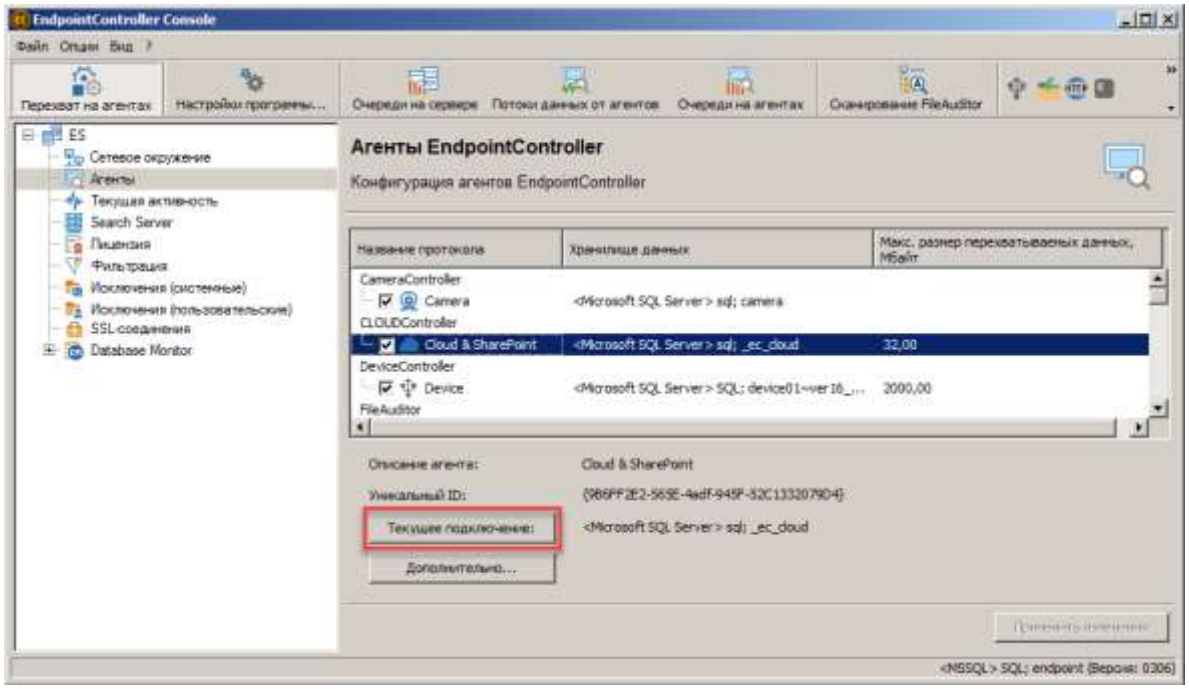


Рисунок 6.104

2. Настройте подключение к базе данных.

Порядок действий для создания базы CloudController & SharePoint аналогичен вышеизложенному порядку создания базы данных FileController (см. Таблица 22).

3. Для настройки модуля перехвата HTTPController с подключенной базой щёлкните кнопку «Дополнительно».

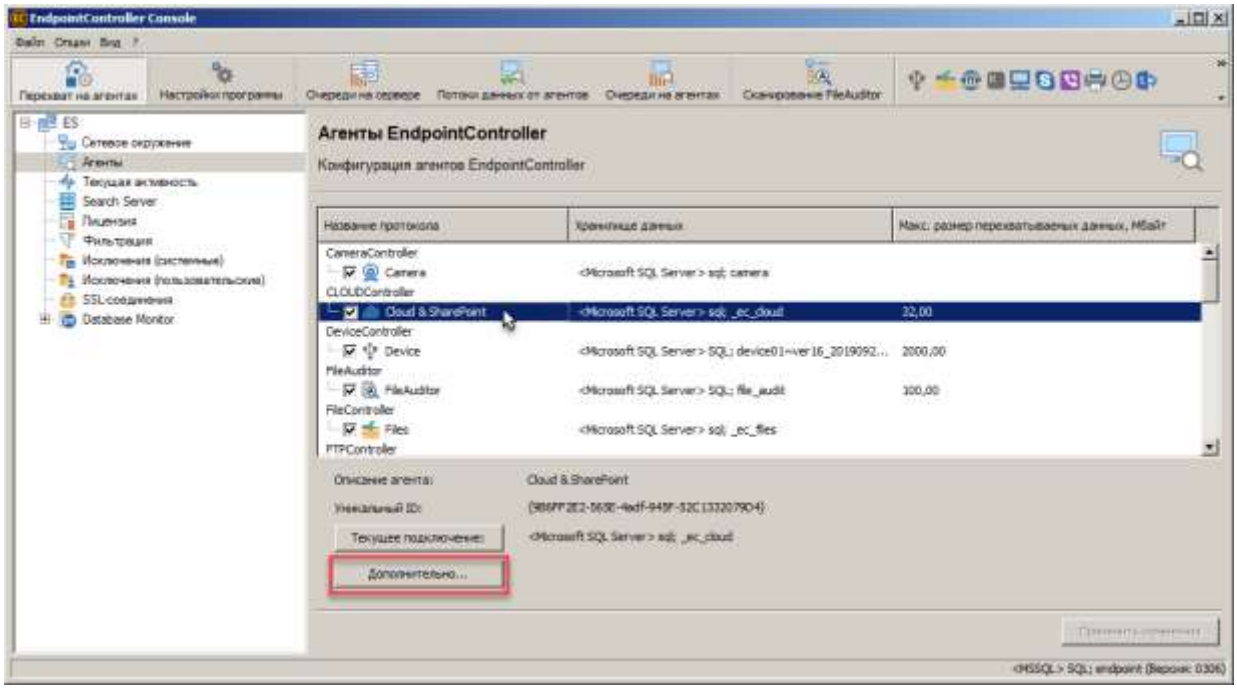


Рисунок 6.105

В открывшемся окне конфигурирования параметров протокола установите флажок «Сохранять повторно перехваченные файлы», если необходимо сохранять в базу данных повторно загружаемые файлы. Если флажок снят, работает режим дедупликации перехваченных файлов.

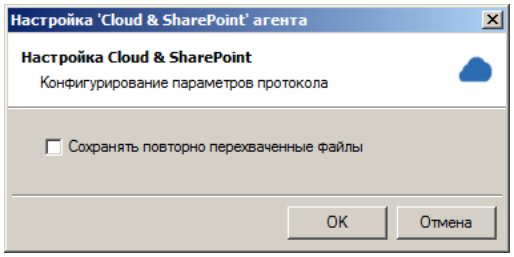


Рисунок 6.106

4. Щёлкните кнопку «Применить изменения» в консоли администрирования EndpointController, чтобы произведенные настройки модуля перехвата CloudController вступили в силу.

6.5.1.6 Настройка модуля перехвата IMController

Модуль перехвата IMController предназначен для контроля сервисов мгновенных сообщений, интернет-мессенджеров. В настоящей версии компонент IMController поддерживает перехват следующих протоколов:

- ICQ;
- MMP;
- XMPP;

- HTTPIM (социальные сети - Facebook, LinkedIn, В Контакте, Мой Мир@Mail.Ru, Одноклассники, Google+, Мамба.ru, Imo.im, Meebo.com, веб-версии Skype);
- Gadu-Gadu;
- WhatsApp;
- Lync;
- Viber;
- Telegram.

Настройка модуля IMController предусматривает задание дополнительных параметров для протоколов ICQ, MMP и HTTPIM.

Протоколы компонента IMController можно включать и отключать. Для включения или отключения протоколов установите или удалите соответствующие флажки. Включить можно только протоколы, привязанные к базам данных, поэтому каждый перехватываемый протокол должен быть привязан к базе данных.

Порядок действий по созданию базы IMController (если не было выполнено в п.6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «IMController» (для настройки базы данных сразу для всех протоколов) либо позицию протокола (для настройки отдельной базы данных для каждого протокола). Щёлкните кнопку «Текущее подключение» (см. Рисунок 6.107).

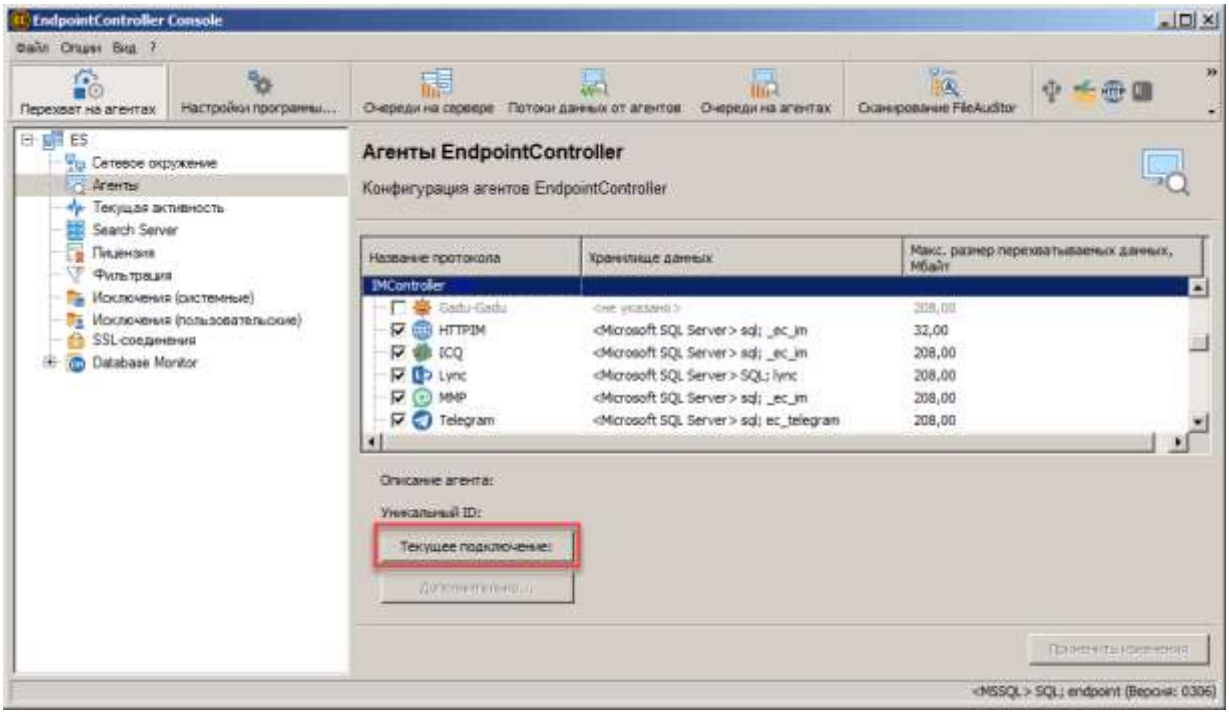


Рисунок 6.107

2. Настройте подключение к базе данных.

Порядок действий для создания базы IMController аналогичен выше изложенному порядку создания базы данных FileController (см. Таблица 22).

Управление дополнительными настройками протоколов ICQ/MMP производится на вкладке «Агенты» консоли администрирования. Выделите протокол ICQ/MMP щёлкните кнопку «Дополнительно» или кнопку / (см. Рисунок 6.108).

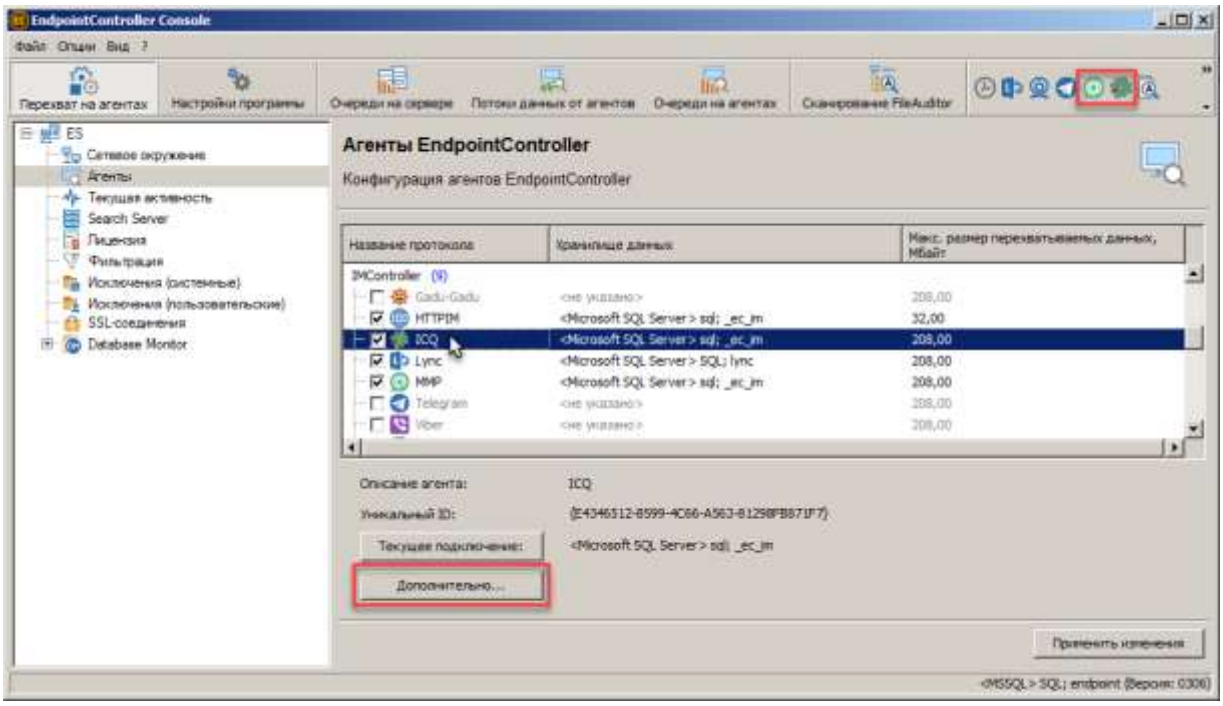


Рисунок 6.108

Окно редактирования протокола ICQ/MMP позволяет производить настройки фильтрации каналов данных и параметров голосовой связи (см. Рисунок 6.109, Рисунок 6.110).

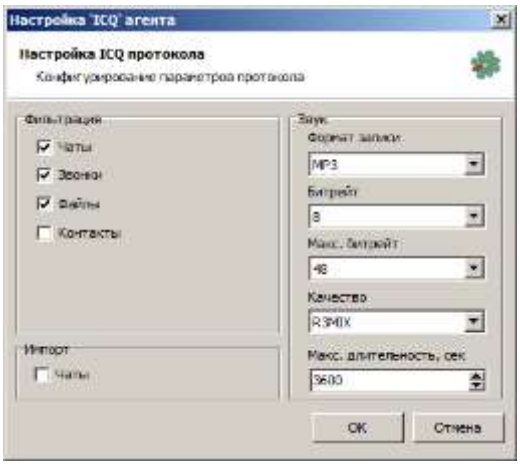


Рисунок 6.109

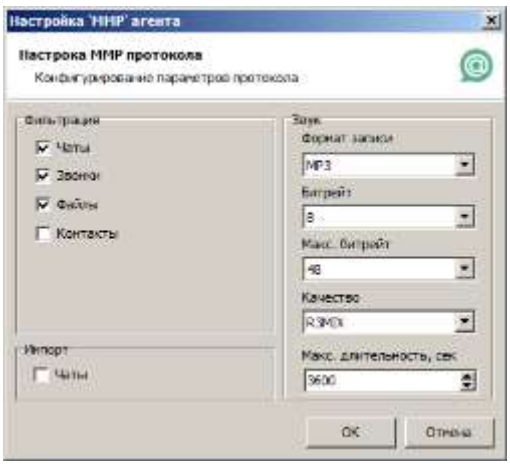


Рисунок 6.110

Таблица 17 содержит описание настроек агента ICQ/MMP.

Таблица 17 – Настройки агента ICQ/MMP

Настройка	Описание
«Фильтрация»	
Чаты	Установленный флажок включает перехват чатов.
Файлы	Установленный флажок включает захват файлов.
Звонки	Установленный флажок включает перехват сеансов голосовой связи.
Контакты	Установленный флажок включает захват списка контактов.
«Импорт»	
Чаты	Установленный флажок позволяет перехватывать историю сообщений в чатах.
«Звук»	
Формат записи	Задается формат записи: MP3 - формат со сжатием данных, или WAV - формат без сжатия.
Битрейт	Задается битрейт для записей в формате MP3. Минимальный – 8 кбит/с, максимально возможный – 320 кбит/с.
Макс. битрейт	Задается максимальный битрейт для записей в формате MP3.
Качество	Задается качество записываемого сеанса голосовой связи при использовании формата MP3. Данный параметр задает пресет кодека LAME, который выполняет сжатие полученных от микрофона данных (пресет — предварительно заданная схема настроек параметров). По умолчанию используется пресет R3MIX, который обеспечивает неплохой уровень качества при

Настройка	Описание
	достойной скорости сжатия и использует Variable Bit Rate (VBR) - технологию изменяющегося битрейта, при которой битрейт динамически изменяется кодером. Например, тишина кодируется с минимальным битрейтом.
Макс. длительность, сек	Задается максимальная длительность файла звукозаписи. При превышении установленной длительности запись сеанса голосовой связи будет разделена на части.

Для сохранения настроек в окне редактирования агента нажмите «OK», а затем щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведённые настройки вступили в силу.

6.5.1.6.1 Настройка протокола HTTP IM

На вкладке «Агенты» выделите протокол **HTTPIM** и вызовите окно настроек любым из перечисленных способов:

- двойным кликом курсора мыши по названию настраиваемого протокола;
- нажатием кнопки «Дополнительно...» для выбранного протокола.

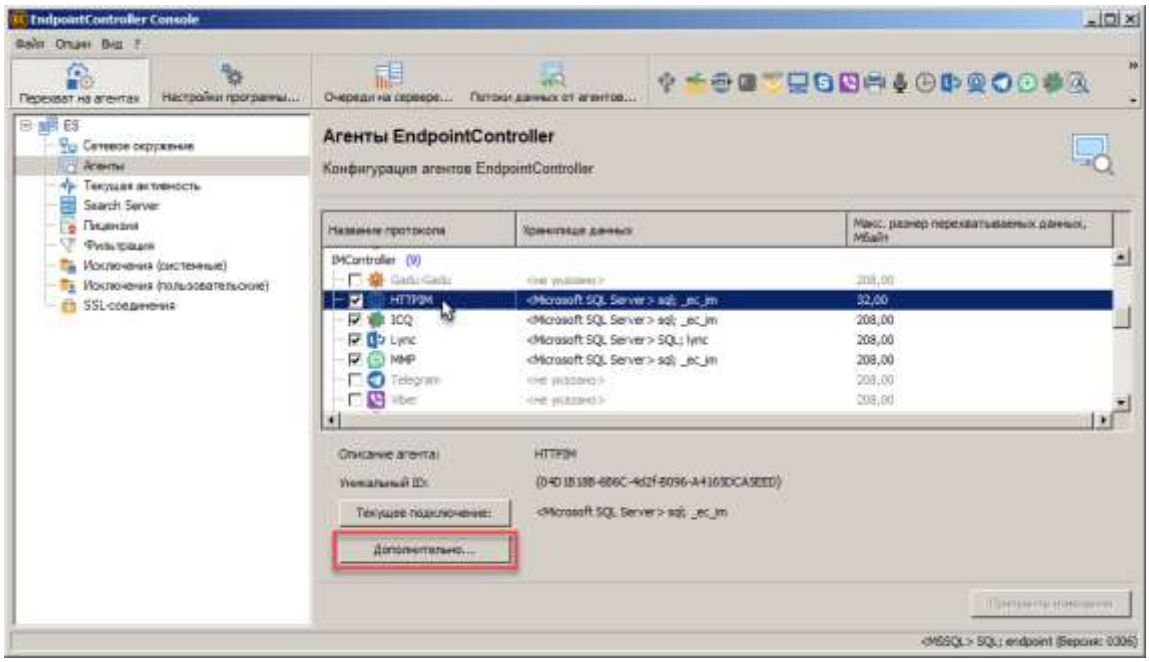


Рисунок 6.111

По умолчанию, перехват истории переписки в соцсетях активирован и осуществляется непрерывно при поступлении таких данных. Снятие флажка с параметра «Перехват истории исходящей переписки» позволяет исключить «подтягивание» из истории переписки исходящих сообщений пользователей с целью исключить дублирование информации в базе данных. Таким образом, при снятом

флажке история исходящих сообщений перехвачена не будет, только текущая переписка.

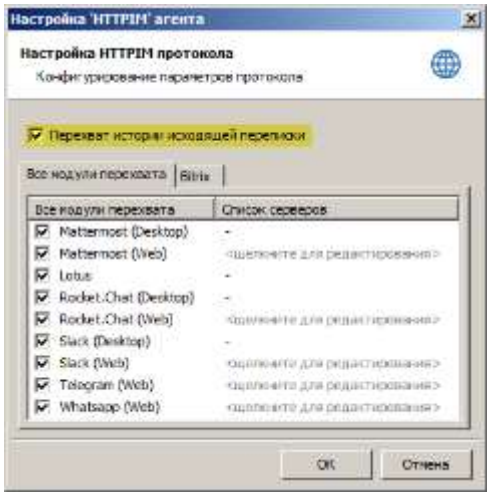


Рисунок 6.112

На вкладке «Все модули перехвата» приведен список веб-версий чатов, поддерживаемых протоколом HTTPIM.

Для активации модуля перехвата установите напротив него флажок. Щелкните напротив требуемого модуля в столбце «Список серверов» и в открывшемся окне редактора настройте список серверов, контролируемых данным модулем.

Если в процессе установки EndpointController были отмечены «Модули перехвата Bitrix24», в окне настроек протокола HTTPIM будет отображена вкладка «Bitrix». На вкладке расположен параметр «Перехват Bitrix24», отметка которого активирует перехват чатов Bitrix24.

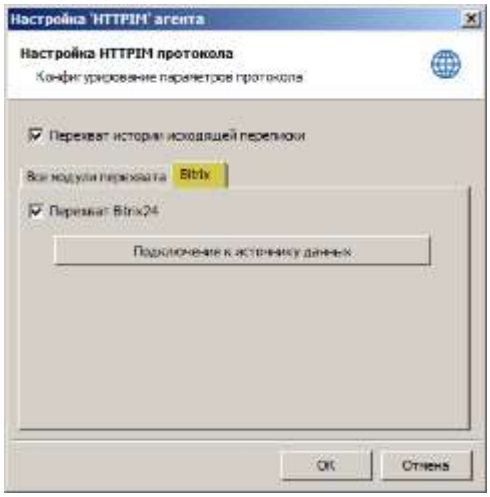


Рисунок 6.113

Щелкните кнопку «Подключение к источнику данных» и в появившемся окне укажите параметры подключения к базе данных Bitrix24. Для осуществления передачи трафика **должно быть разрешено подключение к базе данных на стороне сервера Bitrix24**.

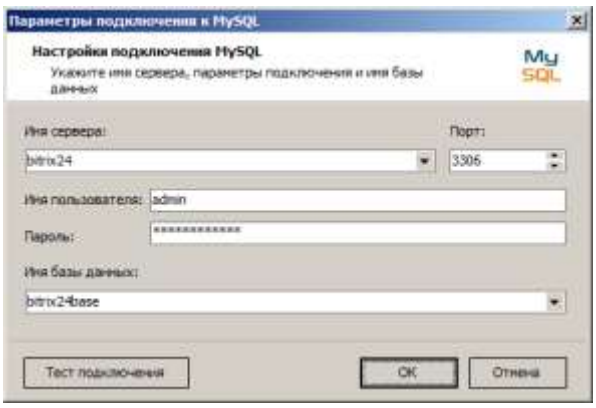


Рисунок 6.114

Для сохранения настроек в окне редактирования нажмите «OK», а затем щелкните кнопку «Применить изменения» в консоли EndpointController, чтобы произведенные настройки IMController вступили в силу.

6.5.1.6.2Настройка протокола Lync

Модуль перехвата IMController позволяет перехватывать и анализировать трафик Microsoft Lync 2010+ (Skype for Business, Microsoft Teams): сеансы текстовой и голосовой связи, контакты, переданные или полученные при помощи протокола Lync файлы.

Для настройки перехвата данных MS Lync с подключенной базой выделите протокол Lync и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку «Дополнительно» или иконку протокола  на панели «Конфигурирование агентов») (см. Рисунок 6.115).

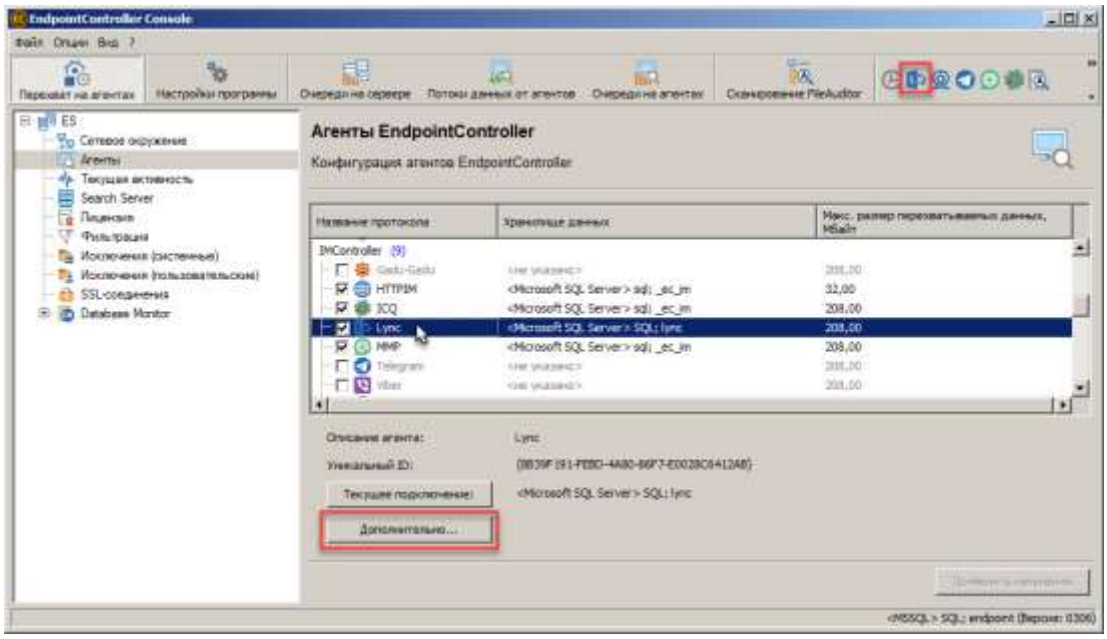


Рисунок 6.115

В открывшемся окне редактирования агента LyncController произведите необходимые настройки фильтрации каналов данных (чаты, звонки, файлы), максимального размера файла для обработки и параметров голосовой связи (формат записи, битрейт, максимальный битрейт, качество и максимальную длительность сеанса связи) (см. Рисунок 6.116).

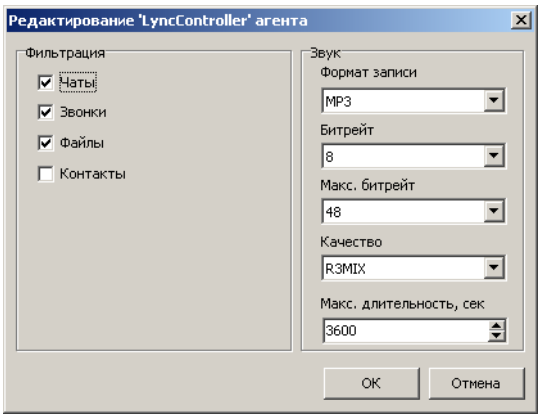


Рисунок 6.116

Таблица 18 содержит описание настроек агента LyncController.

Таблица 18 – Настройки агента LyncController

Настройка	**Описание**
«Фильтрация»	
Чаты	Установленный флажок включает перехват чатов.
Звонки	Установленный флажок включает перехват сеансов голосовой связи.
Файлы	Установленный флажок включает захват файлов, переданных через Lync.
Контакты	Установленный флажок включает перехват списков контактов Lync.
«Звук»	
Формат записи	Задается формат записи: MP3 – формат со сжатием данных, или WAV – формат без сжатия.
Битрейт	Задается битрейт для записей в формате MP3. Минимальный – 8 кбит/с, максимально возможный – 320 кбит/с.
Макс. битрейт	Задается максимальный битрейт для записей в формате MP3.

Настройка	Описание
Качество	Задается качество записываемого сеанса голосовой связи при использовании формата MP3. Данный параметр задает пресет кодека LAME, который выполняет сжатие полученных от микрофона данных (пресет — предварительно заданная схема настроек параметров). По умолчанию в LyncController используется пресет R3MIX, который обеспечивает неплохой уровень качества при достойной скорости сжатия и использует Variable Bit Rate (VBR) - технологию изменяющегося битрейта, при которой битрейт динамически изменяется кодером. Например, тишина кодируется с минимальным битрейтом.
Макс. длительность, сек	Задается максимальная длительность файла звукозаписи. При превышении установленной длительности запись сеанса голосовой связи будет разделена на части.

Для сохранения настроек в окне редактирования агента нажмите OK, а затем щелкните кнопку «Применить изменения» на консоли администрирования, чтобы произведенные настройки агента LyncController вступили в силу.

6.5.1.6.3Настройка протокола Viber

Модуль перехвата IMController позволяет перехватывать и анализировать трафик Viber Desktop: сеансы текстовой и голосовой связи, списки контактов, файлы, переданные при помощи протокола Viber.

Для настройки параметров перехвата данных Viber выделите протокол Viber и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку «Дополнительно» или иконку протокола  на панели «Конфигурирование агентов») (см. Рисунок 6.117).

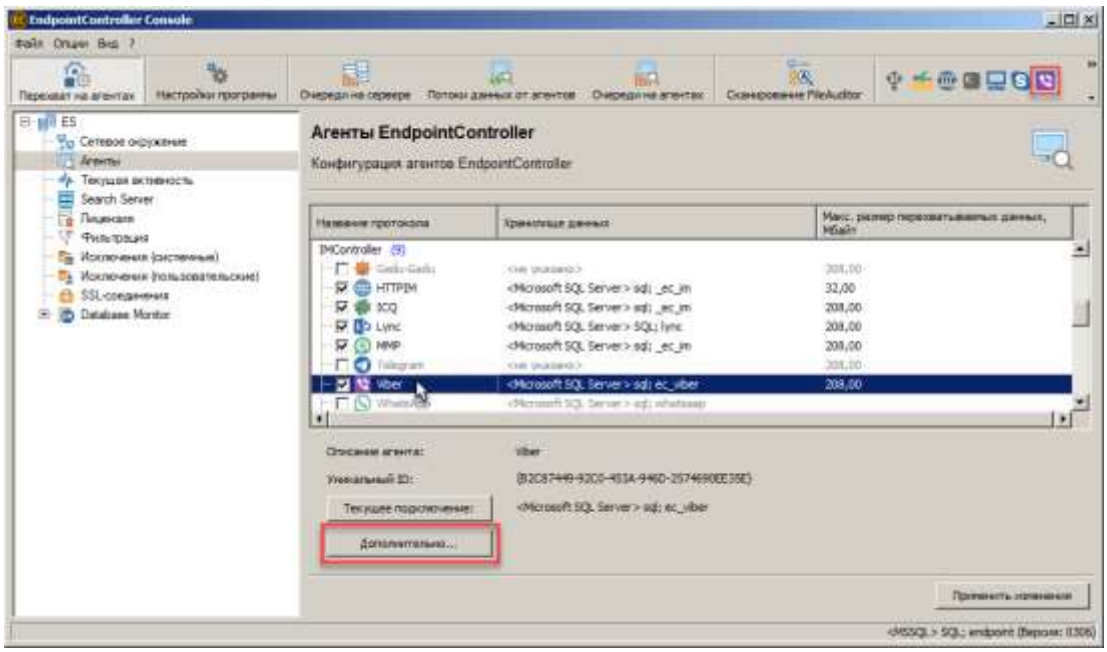


Рисунок 6.117

В окне редактирования агента ViberController произведите необходимые настройки фильтрации каналов данных (чаты, звонки, файлы, контакты), импорта, параметров голосовой связи (формат записи, битрейт, максимальный битрейт, качество и метод захвата, максимальную длительность сеанса связи) и пользователей Viber (см. Рисунок 6.118).

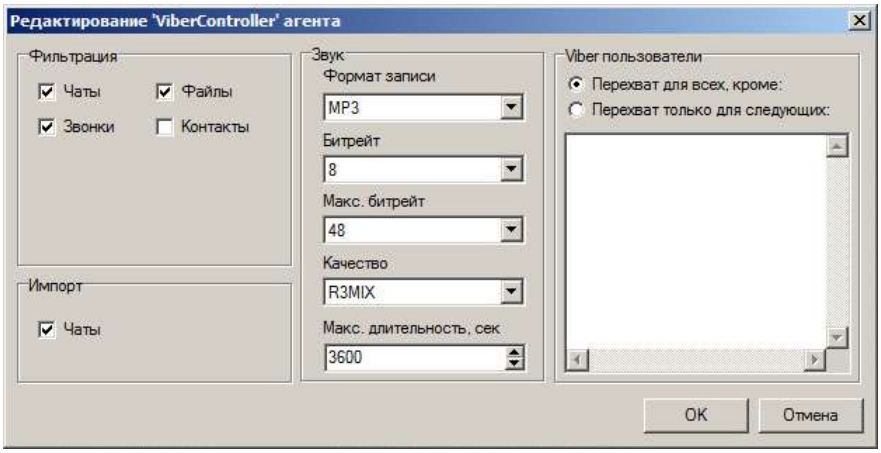


Рисунок 6.118

Таблица 19 содержит описание настроек агента ViberController.

Таблица 19 – Настройки агента ViberController

Настройка	Описание
«Фильтрация»	
Чаты	Установленный флажок включает перехват чатов.

Настройка	Описание
Файлы	Установленный флажок включает захват файлов, переданных через Viber.
Звонки	Установленный флажок включает перехват сеансов голосовой связи.
Контакты	Установленный флажок включает захват списка контактов из Viber.
«Импорт»	
Чаты	Установленный флажок позволяет перехватывать историю сообщений в чатах.
«Звук»	
Формат записи	Задается формат записи: MP3 - формат со сжатием данных, или WAV - формат без сжатия.
Битрейт	Задается битрейт для записей в формате MP3. Минимальный – 8 кбит/с, максимально возможный – 320 кбит/с.
Макс. битрейт	Задается максимальный битрейт для записей в формате MP3.
Качество	Задается качество записываемого сеанса голосовой связи при использовании формата MP3. Данный параметр задает пресет кодека LAME, который выполняет сжатие полученных от микрофона данных (пресет — предварительно заданная схема настроек параметров). По умолчанию в LyncController используется пресет R3MIX, который обеспечивает неплохой уровень качества при достойной скорости сжатия и использует Variable Bit Rate (VBR) - технологию изменяющегося битрейта, при которой битрейт динамически изменяется кодером. Например, тишина кодируется с минимальным битрейтом.
Макс. длительность, сек	Задается максимальная длительность файла звукозаписи. При превышении установленной длительности запись сеанса голосовой связи будет разделена на части.
«Viber пользователи»	
Перехват для всех, кроме:	Задаются мобильные номера пользователей Viber через запятую, которые будут исключены из перехвата.
Перехват только для следующих:	Задаются мобильные номера пользователей Viber через запятую, только для которых будет осуществляться перехват.

Для сохранения настроек в окне редактирования агента нажмите OK, а затем щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведенные настройки вступили в силу.

6.5.1.6.4Настройка протокола Telegram

Модуль перехвата IMController позволяет перехватывать и анализировать трафик Telegram Desktop: сеансы текстовой и голосовой связи, списки контактов, файлы, переданные при помощи протокола Telegram.

Для настройки параметров перехвата данных Telegram выделите протокол «Telegram» и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку «Дополнительно» или иконку протокола  на панели «Конфигурирование агентов») (см. Рисунок 6.119).

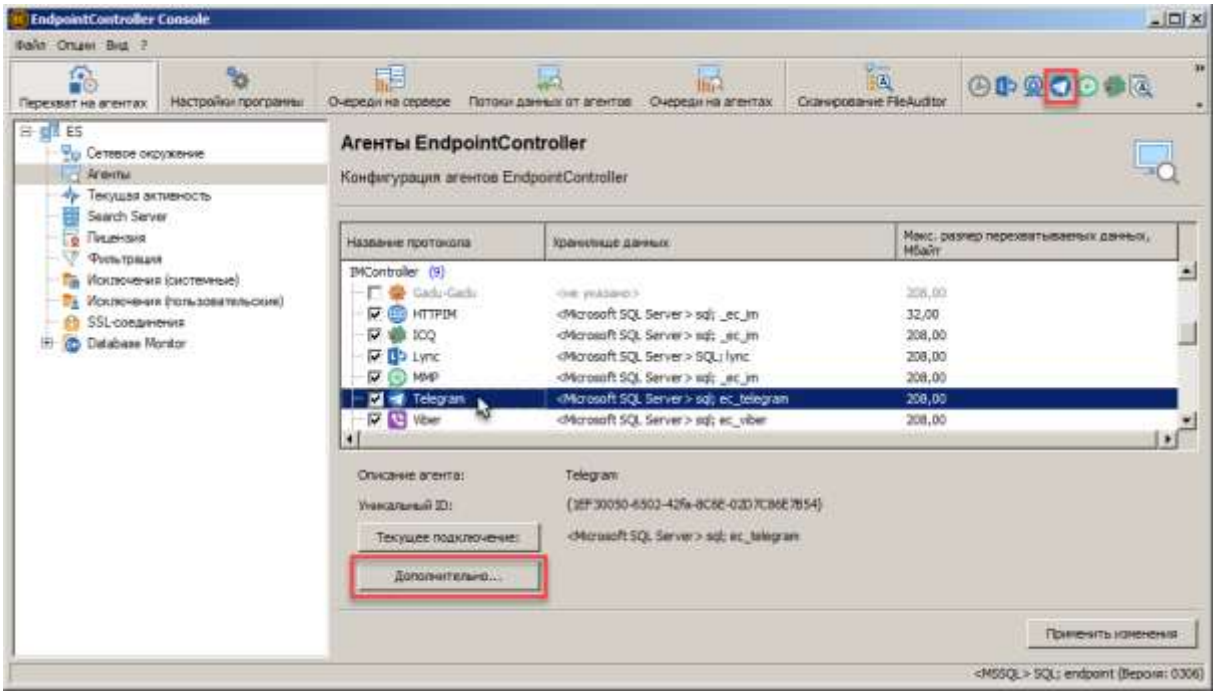


Рисунок 6.119

В открывшемся окне редактирования агента TelegramController произведите необходимые настройки фильтрации каналов данных (чаты, звонки, файлы, контакты) и параметров голосовой связи (битрейт, максимальный битрейт, качество и метод захвата, максимальную длительность сеанса связи) (см. Рисунок 6.120).

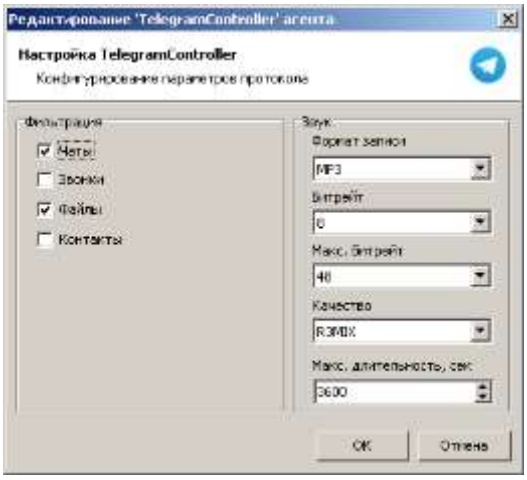


Рисунок 6.120

Таблица 24 содержит описание настроек перехвата данных Telegram.

Таблица 24 – Настройки агента TelegramController

Настройка	Описание
«Фильтрация»	
Чаты	Установленный флажок включает перехват чатов. Входящие тестовые сообщения от пабликов Telegram исключаются из перехвата.
Файлы	Установленный флажок включает захват файлов, переданных через Telegram.
Звонки	Установленный флажок включает перехват сеансов голосовой связи.
Контакты	Установленный флажок включает захват списка контактов из Telegram.
«Звук»	
Формат записи	Задается формат записи: MP3 - формат со сжатием данных, или WAV - формат без сжатия.
Битрейт	Задается битрейт для записей в формате MP3. Минимальный – 8 кбит/с, максимально возможный – 320 кбит/с.
Макс. битрейт	Задается максимальный битрейт для записей в формате MP3.
Качество	Задается качество записываемого сеанса голосовой связи в формате MP3. Данный параметр задает пресет кодека LAME, который выполняет сжатие полученных от микрофона данных (пресет — предварительно заданная схема настроек параметров). По умолчанию в TelegramController используется пресет R3MIX, который обеспечивает неплохой уровень качества при достойной скорости сжатия и использует Variable Bit Rate (VBR) -

	технологию изменяющегося битрейта, при которой битрейт динамически изменяется кодером. Например, тишина кодируется с минимальным битрейтом.
Макс. длительность, сек	Задается максимальная длительность файла звукозаписи. При превышении установленной длительности запись сеанса голосовой связи будет разделена на части.

Для сохранения настроек в окне редактирования агента нажмите «OK», а затем щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведённые настройки вступили в силу.

6.5.1.7 Настройка модуля перехвата KeyLogger

Модуль перехвата KeyLogger предназначен для фиксирования и сохранения в базу данных нажатий клавиш и их сочетаний в различных приложениях; позволяет контролировать содержимое, поступающее в буфер обмена и вставляемое из него.

Для компонента KeyLogger создаются базы данных, которые затем соответствующим образом настраиваются. Базы данных KeyLogger необходимо привязывать к индексам.

Не рекомендуется включать KeyLogger без предварительной настройки, т.к. в этом случае количество перехватываемых данных будет очень большим.

Порядок действий для создания базы KeyLogger (если не было выполнено в п.6.5.1.1):

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «KeyLogger» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.121).

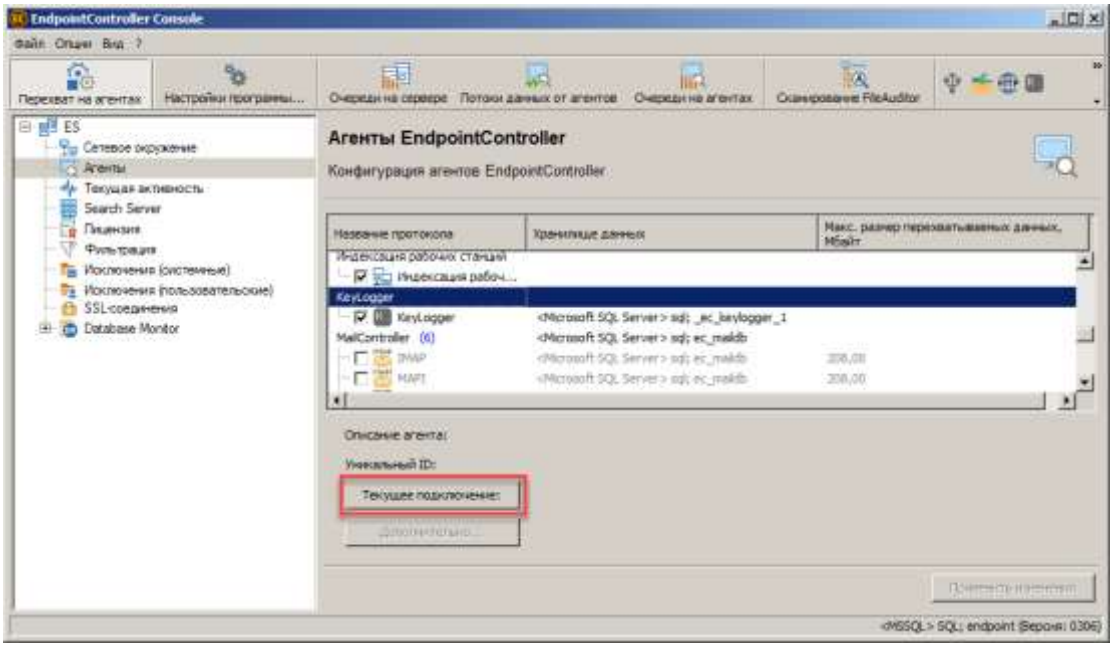


Рисунок 6.121

2. Настройте подключение к базе данных.

Порядок действий для создания базы KeyLogger аналогичен вышеизложенному порядку создания базы данных FileController (см.Таблица 22).

Управление агентом производится на вкладке «Агенты» консоли администрирования. Выделите протокол KeyLogger и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку  или кнопку «Дополнительно») (см. Рисунок 6.122).

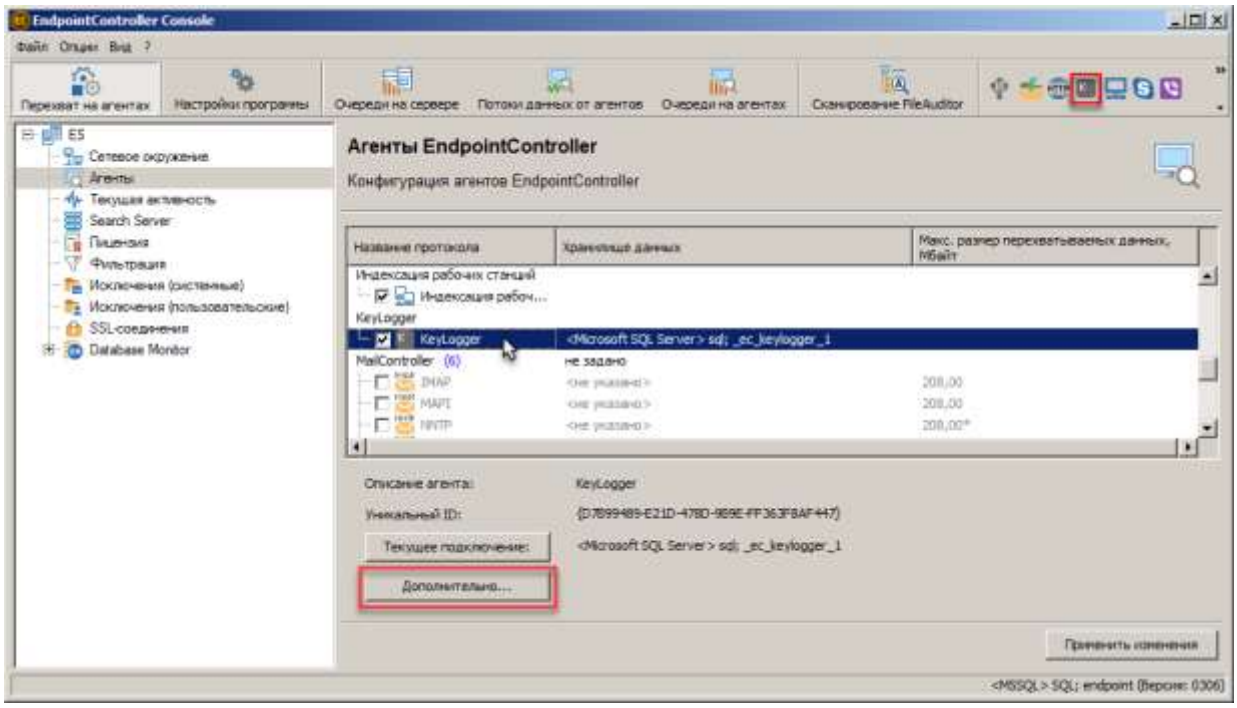


Рисунок 6.122

В открывшемся окне редактирования агента KeyLogger произведите необходимые настройки по применению перехвата нажатий клавиш к отдельным пользователям и запущенным процессам.

Отметьте флагом опцию для блокировки нажатий клавиши «PrintScreen» (см. Рисунок 6.123).

Рисунок 6.123

Снимите флажок «Перехват паролей», если не требуется перехват паролей, вводимых в системных окнах авторизации. По умолчанию перехват включен.

Выберите один из вариантов перехвата для KeyLogger (см. Рисунок 6.124):

- **Перехват только клавиш** – в перехват попадут все нажатия клавиш (включая системные);
- **Перехват только буфера обмена** – в перехват попадут помещаемые в буфер обмена данные, ограниченные параметром «Перехватывать первые N КБ буфера обмена»;
- **Перехват всего** – в перехват попадут и нажатия клавиш и помещаемые в буфер обмена данные. Перехват буфера обмена ограничен параметром «Перехватывать первые N КБ буфера обмена».

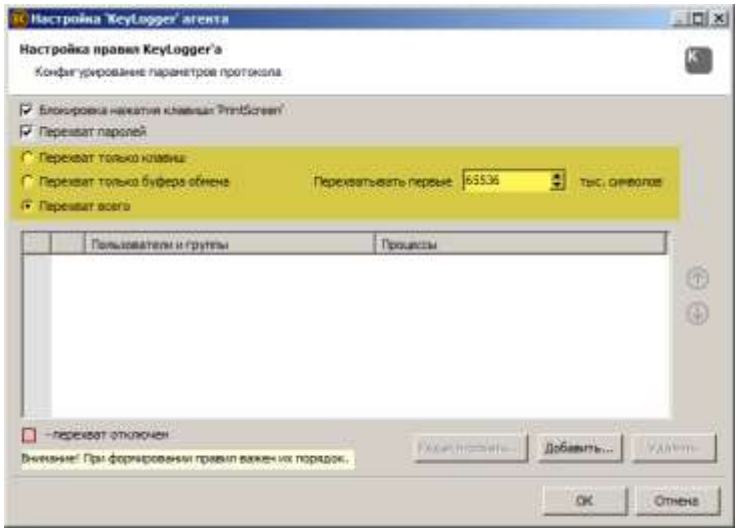


Рисунок 6.124

В диалоговом окне «Настройка 'KeyLogger' агента» отображается настроенный перечень правил перехвата. Для управления списком используются следующие кнопки (см. Рисунок 6.125):

- **Добавить** – создание нового правила логирования;
- **Редактировать** – изменение имеющегося в списке правила;
- **Удалить** – удаление правила из списка.

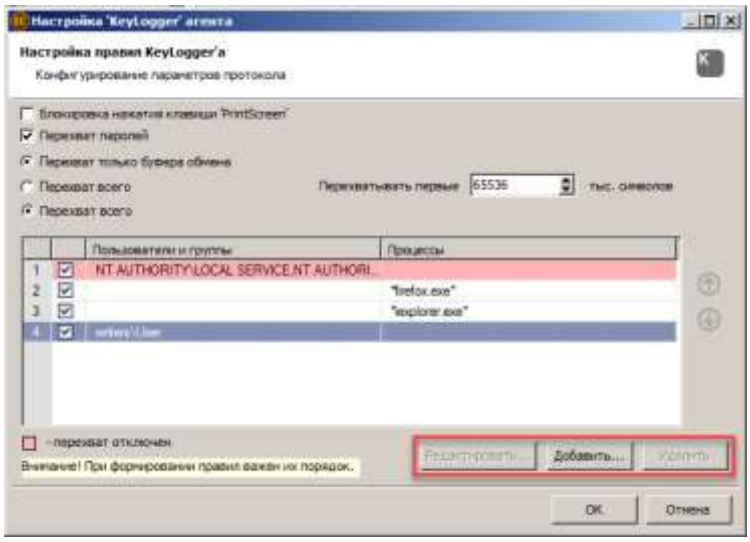


Рисунок 6.125

Щёлкните кнопку «Добавить».

В открывшемся окне добавления правила для KeyLogger'а произведите необходимые настройки параметров фильтрации, позволяющей включить в перехват или исключить из него отдельных пользователей, групп пользователей и процессы (см. Рисунок 6.126).

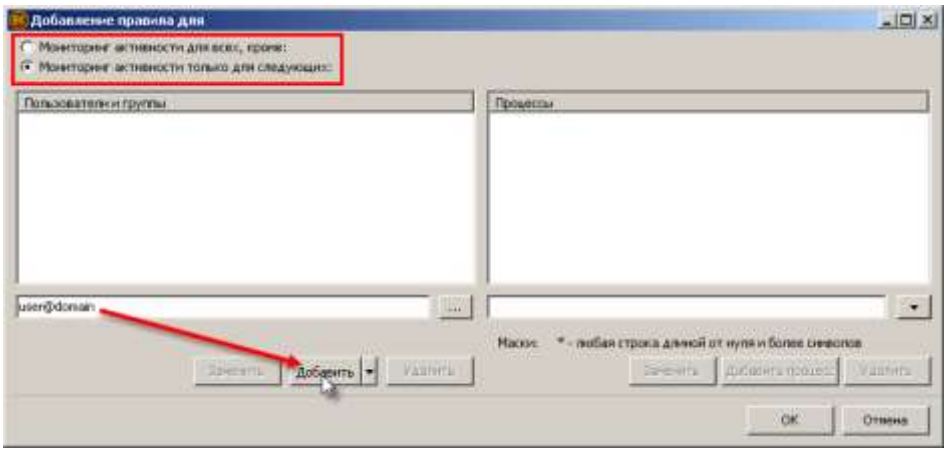


Рисунок 6.126

В левой части окна определяется один или несколько пользователей, в правой части – перечень процессов, к которым будут применены одни и те же правила фильтрации (см. Рисунок 6.127).

Рисунок 6.127

5. Для сохранения настроек нажмите **OK** в окнах редактирования правила и списка всех правил логирования, а затем щёлкните кнопку «Применить изменения» в консоли администрирования EndpointController, чтобы произведенные настройки модуля перехвата KeyLogger вступили в силу.

6.5.1.8 Настройка модуля перехвата MailController

Модуль перехвата MailController позволяет контролировать почтовый трафика как на уровне рабочих станций, так и на уровне сетевых протоколов.

В настоящей версии компонент MailController поддерживает перехват шести протоколов:

- IMAP;
- MAPI;
- NNTP;
- POP3;
- SMTP;
- Web mail[21].

Каждый перехватываемый протокол должен быть привязан к базе данных.

Серверный модуль EndpointController позволяет перехватывать помимо обычного почтового трафика зашифрованный SSL-трафик, переданный по электронной почте.

Сервер EndpointController позволяет включать/выключать режим остановки исходящих сообщений электронной почты, передаваемых по протоколу SMTP (а также

[21] Под названием **Web mail** объединено несколько протоколов веб-почты:

- EWS (Exchange Web Services) - исходящая и входящая почта;
- KOC (Kerio Outlook Connect) - исходящая и входящая почта;
- OWA (Outlook Web App и Outlook Web App Light) – исходящая и входящая почта;
- Zimbra Web Client – исходящая и входящая почта;
- Протоколы почтовых сервисов (gmail.com, mail.live.com, e.mail.ru, mail.yandex.ru и т.д.) – исходящая и входящая почта.

MAPI/IMAP при использовании плагина Outlook), с помещением блокированных сообщений в карантин, а также задавать параметры перехвата для веб-почты.

Базы данных протоколов MailController необходимо привязывать к индексу.

Порядок действий по созданию базы MailController (если не было выполнено в п. 6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «MailController». Щёлкните кнопку «Текущее подключение» (см. Рисунок 6.128).

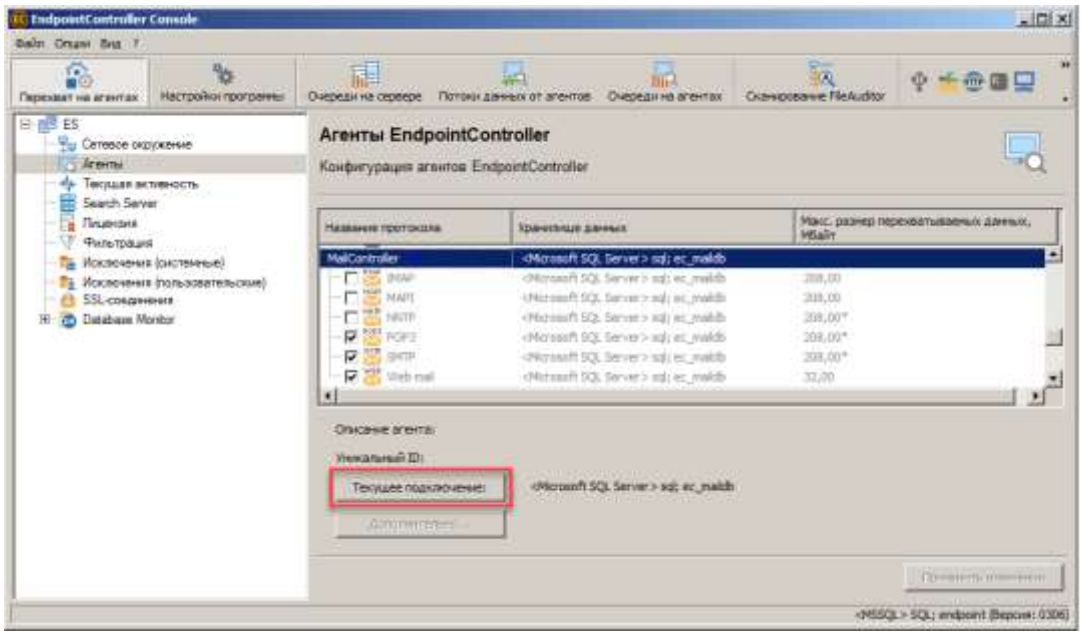


Рисунок 6.128

2. Настройте подключение к базе данных.

Порядок действий для создания базы MailController аналогичен вышеизложенному порядку создания базы данных FileController (см.Таблица 22).

Управление дополнительными настройками протоколов производится на вкладке «Агенты» консоли администрирования.

6.5.1.8.1 Настройка перехвата Web mail

На вкладке «Агенты» в списке агентов модуля перехвата MailController выделите протокол Web mail и двойным щелчком откройте окно редактирования агента (или щёлкните кнопку «Дополнительно» в нижней части окна) (см. Рисунок 6.129).

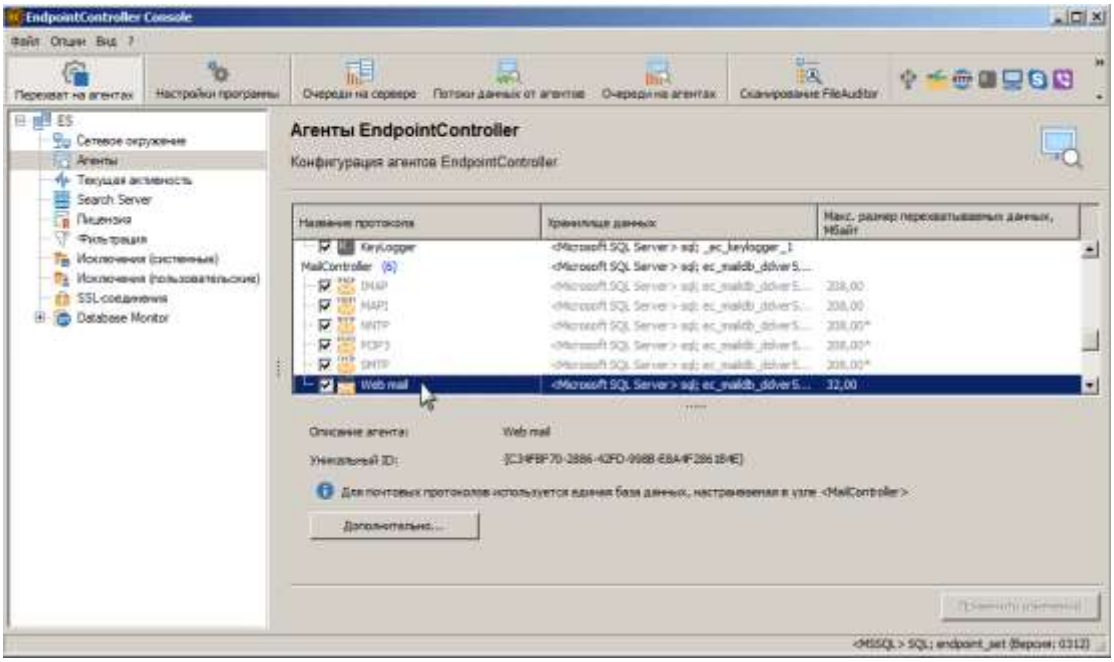


Рисунок 6.129

Отметьте флажком параметр «Перехват входящей почты», если при просмотре почтового ящика с помощью браузера, помимо исходящих электронных писем, требуется перехватывать также входящие данные (см. Рисунок 6.130).

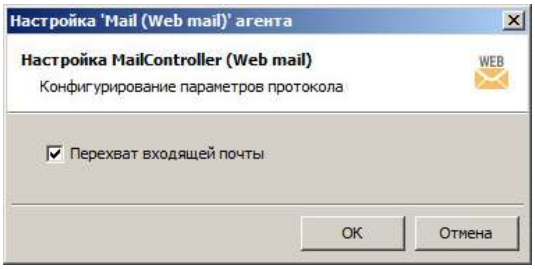


Рисунок 6.130

6.5.1.8.2 Настройка блокировки исходящих сообщений

Сервер EndpointController позволяет включать/выключать режим остановки исходящих сообщений электронной почты, передаваемых по протоколу SMTP (а также MAPI/IMAP при использовании плагина Outlook). Блокированные сообщения помещаются в карантин, откуда они могут быть разблокированы и отправлены по адресу назначения.

Для настройки режима остановки электронной почты используются консоли:

- EndpointController;
- клиента AlertCenter либо AnalyticConsole (в зависимости от используемой службы SMTP-карантина).

Остановка исходящих сообщений электронной почты должна быть первоначально проверена на компьютерах тестовой группы.

Перед включением режима остановки исходящих почтовых сообщений необходимо настроить политики карантина[22].

Включение режима остановки исходящих сообщений производится в консоли администрирования серверного модуля EndpointController. Последовательность действий:

1. Убедитесь, что политики карантина в AlertCenter/ AnalyticConsole настроены.
2. В настройках EndpointController перейдите на вкладку **SMTP-карантин** и отметьте метод получения SMTP-почты:
   - **посредством агента**, установленного на почтовом сервере (параметр «Блокировать SMTP на агентах);
   - **с использованием встроенной службы карантина** на сервере EndpointController, прослушивающей указанный порт (параметр «Служба получения почты для SMTP-карантина»).

При необходимости шифрования канала передачи писем карантина укажите также SSL-порт (при условии, что используемый клиент поддерживает шифрованные соединения). Параметры сертификата шифрования задаются в консоли EndpointController в меню *Настройки → Настройки сервера → Защита соединений* (см. Рисунок 6.131).

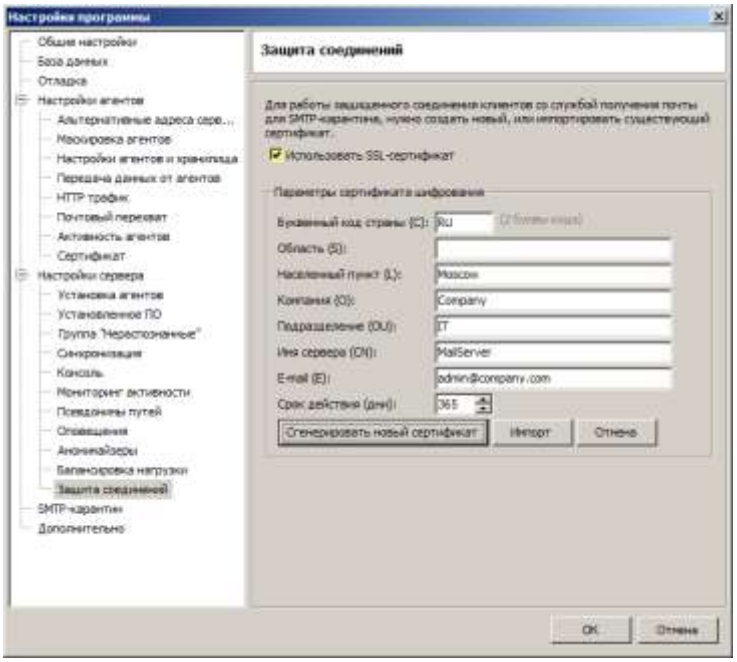


Рисунок 6.131

3. Выберите службу, используемую для обработки SMTP-почты. В зависимости от выбранной службы сообщения помещаются в базы разных продуктов (см. Рисунок 6.132).

[22] Порядок настройки политик карантина описан в справке используемого клиентского приложения.

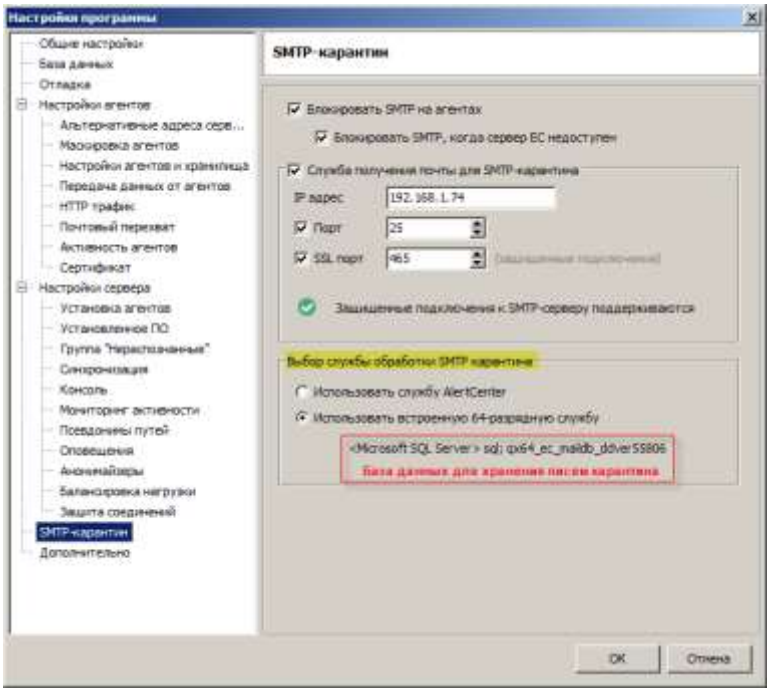


Рисунок 6.132

4. Нажмите «ОК», чтобы произведенные настройки вступили в силу. Удостоверьтесь, что остановка исходящей почты работает корректно.
5. При необходимости блокировки почтового трафика протоколов MAPI и IMAP включите также плагин интеграции Outlook в настройках программы на вкладке «Почтовый перехват» (см. Рисунок 6.133).

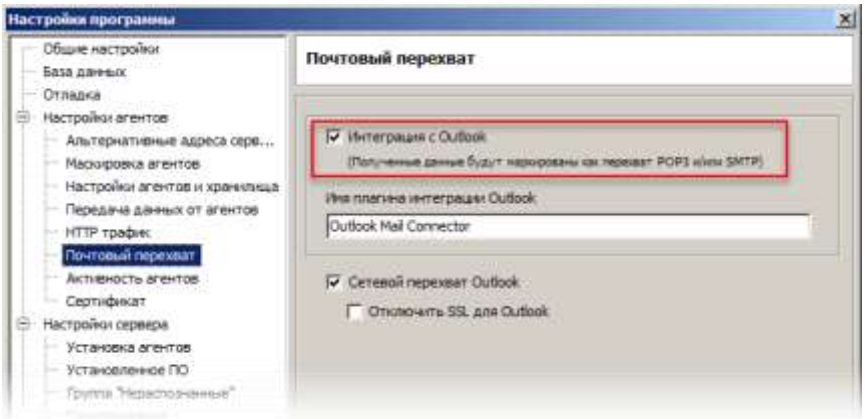


Рисунок 6.133

6.5.1.9 Настройка модуля перехвата MicrophoneController

Модуль перехвата MicrophoneController предназначен для контроля разговоров, ведущихся сотрудниками внутри офиса либо за его пределами (в командировках). Позволяет также прослушивать разговоры в режиме реального времени.

Аудиозапись голоса производится с помощью любого подключенного к рабочей станции микрофона (в наушниках, ноутбуке, веб-камере…).

Для компонента MicrophoneController создаются базы данных, которые затем соответствующим образом настраиваются. Базы данных MicrophoneController в общем случае не привязываются к индексам.

При использовании системы распознавания аудиофайлов базы данных MicrophoneController необходимо привязывать к индексам.

Порядок действий для создания базы MicrophoneController (если не было выполнено в п.6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке агентов пункт «MicrophoneController» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.134).

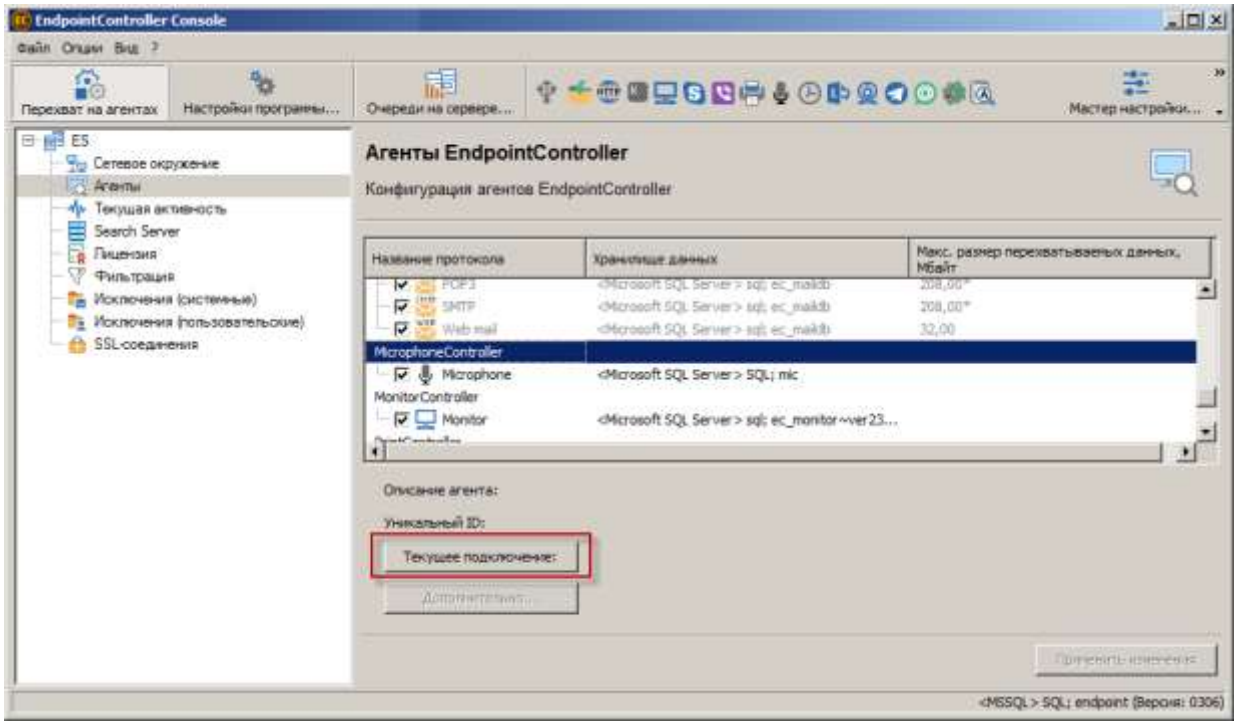


Рисунок 6.134

2. Настройте подключение к базе данных.

Порядок действий для создания базы MicrophoneController аналогичен вышеизложенному порядку создания базы данных FileController (см.Таблица 22).

Управление агентом производится на вкладке «Агенты» консоли администрирования. Выделите протокол Microphone и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку  на панели «Конфигурирование агентов» или кнопку «Дополнительно») (см. Рисунок 6.135).

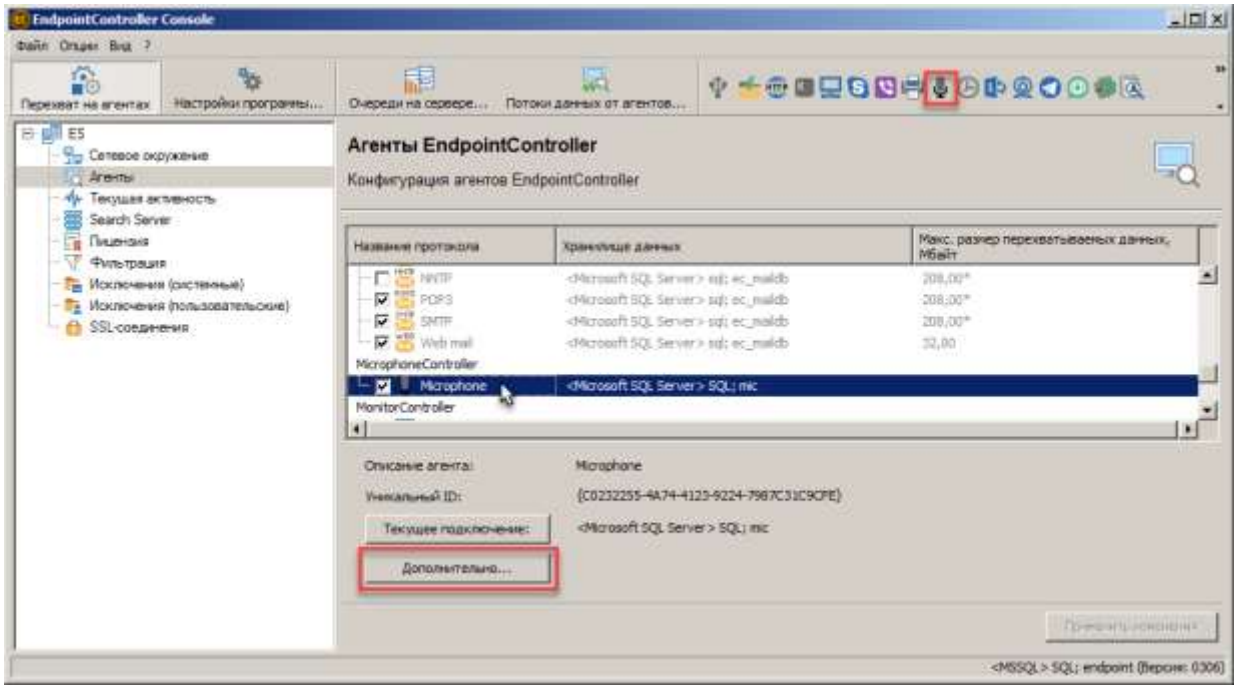


Рисунок 6.135

В открывшемся окне редактирования агента MicrophoneController произведите необходимые настройки.

Запись речи сотрудников может вестись как внутри офиса (вкладка «В офисе»), так и в случае нахождения сотрудника в командировке с корпоративным ноутбуком (вкладка «Вне офиса»). Настройки «Вне офиса» включаются автоматически при переходе агента в офлайн-режим. Параметры на обеих вкладках идентичны (см. Рисунок 6.136).

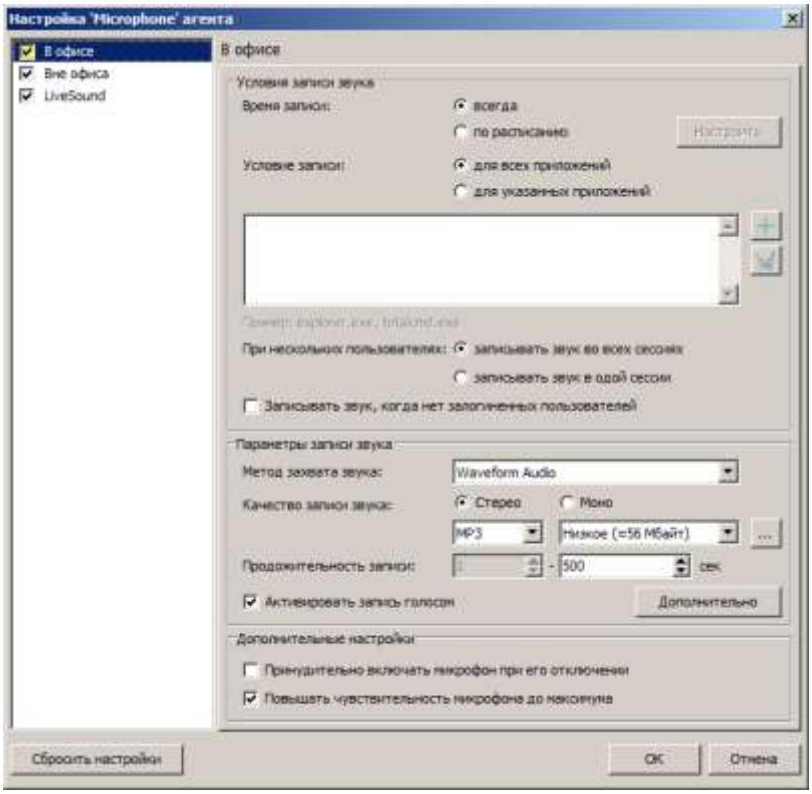


Рисунок 6.136

Не оставляйте настройки по умолчанию на вкладке «Вне офиса»! В случае, когда агент не обнаружил сервер управления, он накапливает данные локально на системном диске в ожидании доступности сервера EndpointController, которому можно передать перехваченные данные. Если агент настроен на перехват всего подряд, размер очереди на системном диске быстро достигает указанного объема, после чего производится циклическая запись, и наиболее старые данные затираются.

Для того чтобы настроить параметры звукозаписи разговоров пользователей, установите флаг нпрапротив режима, в котором будет осуществляться перехват: «В офисе»/«Вне офиса». Таблица 25 содержит описание настроек агента MicrophoneController.

Таблица 25 – Настройки агента MicrophoneController

Параметр (группа параметров)	**Значение**
Условия записи звука	
Время записи	• **всегда** - запись звука будет выполняться агентом непрерывно; • **по расписанию** - при выборе данной опции нажмите «Настроить» для задания параметров начала, окончания и дней недели, в которые будет выполняться запись звука.

Параметр (группа параметров)	Значение
Условие записи	• По умолчанию агент ведет запись **для всех приложений**, т.е. непрерывно; • При выборе опции **для указанных приложений** в текстовом поле необходимо указать или выбрать с помощью проводника перечень процессов приложений, при запуске которых будет активироваться запись. В этом случае запись звука будет вестись только с момента запуска приложения и до момента завершения его работы.
При нескольких пользователях	• По умолчанию запись звука осуществляется **для каждой сессии,** т.е. для всех пользователей одновременно • Отметьте опцию **записывать звук в одной сессии** для записи звука в одной пользовательской сессии
Записывать звук, когда нет залогиненных пользователей	Активируйте опцию для записи звука с рабочих станций, на которых ни один из пользователей не авторизовался в ОС.
Параметры записи звука	
Метод захвата звука	Выберите метод захвата звука: • Waveform Audio – используется по умолчанию; • Audio Client – используется, если есть проблемы с перехватом методом по умолчанию (используется иной метод определения активного микрофона, что может решить проблемы перехвата и даст возможность получать более высокие значения битрейта на устройствах, способных его обеспечить)
Качество записи звука	**Выберите качество записи:** • Моно - одноканальная запись звука (и, соответственно, его воспроизведение). • Стерео - двухканальная (и более) запись и трансляция звука. **Выберите формат записи звука**: • FLAC – фомат сжатия аудиоданных без потерь, • MP3 - формат сжатия данных с потерями, • WAV - формат без сжатия, • Opus – формат сжатия данных с потерями. **Выберите размер звукового файла**: воспользуйтесь кнопкой ... для просмотра размера файла зависимости от выбранного формата
Продолжительность записи	Ограничьте время записи файла, установив максимальную продолжительность аудиофайла (диапазон макс. границы 240-900 сек.). *Длительность файла НЕ всегда равна установленному максимальному значению. Частота разбиения файлов и их продолжительность зависят от используемого микрофона и настроек качества звука, т.е. чем быстрее буфер*

Параметр (группа параметров)	Значение	
	достигнет определенного объема (при высоком качестве это происходит быстрее), тем быстрее данные будут переданы на конвертацию и сохранены в базу данных, а буфер будет заполняться новыми данными. Такой алгоритм позволяет оптимизировать нагрузку на рабочую станцию и сеть.	
Активировать запись голосом	При снятом флажке агент перехватывает все без исключения окружающие звуки. При отметке данного параметра агент использует алгоритм Voice Activity Detection (VAD) для распознавания наличия звуков, попавших под указанный ниже диапазон улавливаемого сигнала. Звуки, не попавшие в этот диапазон, будут вырезаться из записи (к примеру, тишина или шумы). За счет этого, алгоритм VAD позволяет сократить объем обрабатываемой информации. Установленный флаг позволяет разблокировать кнопку **Дополнительно** для вызова окна настроек активации записи	
Кнопка «Дополнительно»	Уровень подавления шума, дБ	Установка значения параметра уровня подавления постороннего шума. Для получения записи наилучшего качества, данный параметр следует подбирать индивидуально для каждого микрофона. Допустимый диапазон от -5 до -45 дБ, где -45дБ соответствует максимальному уровню подавления шума.
	Определение голосовой активности (алгоритм VAD)	При установке данной опции агент использует алгоритм Voice Activity Detection (VAD) для распознавания наличия звуков, попавших под указанный ниже диапазон улавливаемого сигнала. Звуки, не попавшие в этот диапазон, будут вырезаться из записи (к примеру, тишина или шумы). За счет этого, алгоритм VAD позволяет сократить объем обрабатываемой информации. Границы уровня улавливаемого сигнала задаются параметрами **«Верхняя граница»** и **«Нижняя граница»**, которые отвечают за громкость звуков, при обнаружении которых будет производиться запись аудиофайла. Чем выше диапазон этих границ, тем с большей вероятностью в перехват попадет только речь, но вместе с тем также повышается вероятность «вырезки» из записи более тихих голосов. При этом, чем ниже данный диапазон, тем выше

Параметр (группа параметров)	Значение	
		чувствительность алгоритма и выше вероятность того, что фон может ошибочно интерпретироваться как голос. Рекомендуемый диапазон 50 - 67 %. Однако, в зависимости от эффективности перехвата на конкретном микрофоне, рекомендуется индивидуально настраивать значения верхней и/или нижней границ.
Дополнительные настройки		
Принудительно включать микрофон при его отключении	Установленный флаг позволяет включить микрофон, который был отключен на панели управления, при условии, что ранее данные с этого микрофона уже передавались на сервер.	
Повышать чувствительность микрофона до максимума	При установленном флаге MicrophoneController поднимает уровень чувствительности микрофона на рабочей станции. Включение данной опции может ухудшить качество записи.	
Режим «LiveSound» Активирует возможность удаленного подключения к рабочим станциям для прослушивания речи в реальном времени		
Порт	Номер порта для передачи данных режима LiveSound. Если указанный порт отличается от значения по умолчанию, то соответствующий номер должен быть задан также и в Серчинформ AnalyticConsole.	
Параметры авторизации	Не задано	При установке данной опции при запуске режима LiveSound из Серчинформ AnalyticConsole авторизация не запрашивается.
	Пароль	У для ограничения доступа к режиму LiveSound. Для получения доступа к режиму LiveSound в настройках Серчинформ AnalyticConsole нужно ввести пароль.
	Выбранные пользователи	Разрешить добавленным пользователям работать с LiveSound в Серчинформ AnalyticConsole.

Для сохранения настроек агента MicrophoneController в окне редактирования агента нажмите «OK».

Щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведённые настройки вступили в силу.

Также существует возможность в индивидуальных настройках агента MicrophoneController выбрать устройство, через которое будет осуществляться запись (см. Рисунок 6.137). Для этого:

1. Установите флаг справа от иконки модуля MicrophoneController и щелчком по разблокированной кнопке вызовите окно настроек агента.
2. В поле «Микрофон» выберите из выпадающего списка устройство, с которого необходимо пвести перехват. Если выбранное устройство будет недоступно (например, не подключено в данный момент), агент выберет микрофон автоматически.

   Неактивные микрофоны (те, что когда-либо использовались или подключались к рабочей станции пользователя) посвечены в списке серым цветом.

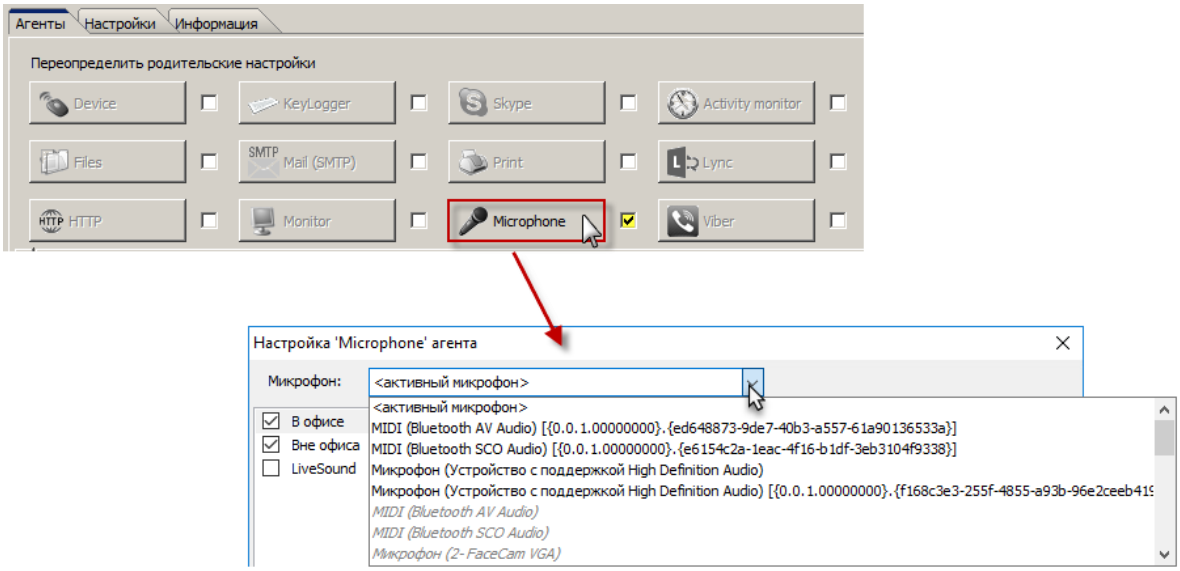


Рисунок 6.137

6.5.1.10 Настройка модуля перехвата MonitorController

Модуль перехвата MonitorController предназначен для фиксации снимков, видеозаписей с экранов мониторов сотрудников. Позволяет также просматривать содержимое информации, отображаемой на экранах, в режиме реального времени.

Для компонента MonitorController создаются базы данных. Базы данных MonitorController не привязываются к индексам.

Порядок действий для создания базы MonitorController (если не было выполнено в п.6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке агентов пункт «MonitorController» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.138).

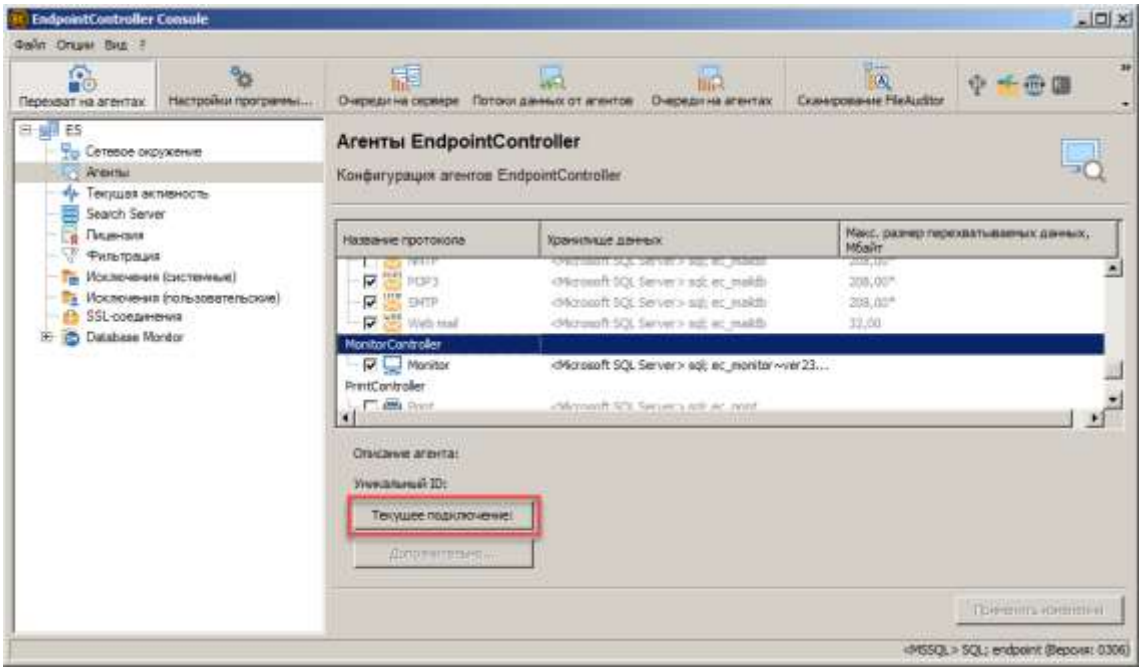


Рисунок 6.138

2. Настройте подключение к базе данных.

Порядок действий для создания базы MonitorController аналогичен вышеизложенному порядку создания базы данных FileController (см. Таблица 22).

Управление агентом производится на вкладке «Агенты» консоли администрирования. Выделите протокол MonitorController и двойным щелчком откройте окно редактирования агента (варианты: щёлкните иконку  на панели «Конфигурирование агентов» или кнопку «Дополнительно») (см. Рисунок 6.139).

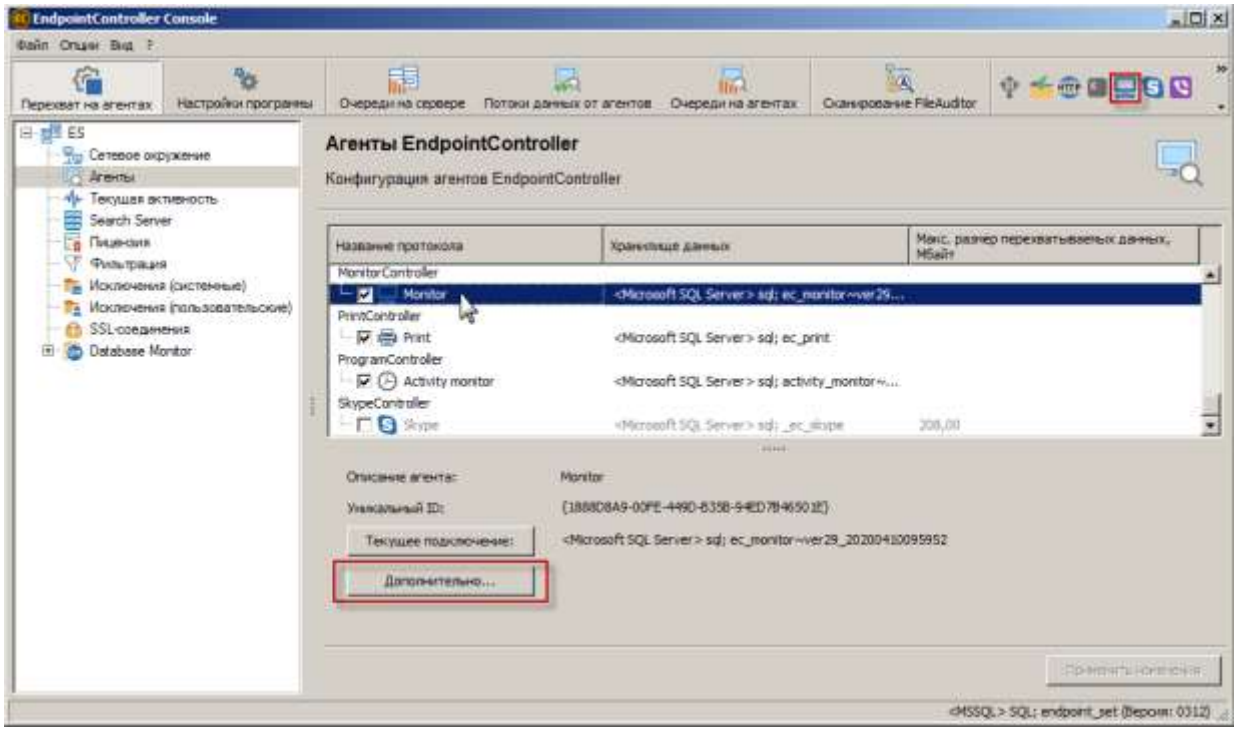


Рисунок 6.139

Установка флажка «Для всех» (см. Рисунок 6.140) позволяет производить настройки перехватываемого изображения, обработку масок процессов, расписание перехвата для всех пользователей, а также управлять перехватом мониторной активности в отношении URLs (единых указателей ресурсов) и масок процессов. Для переопределения перечисленных настроек для отдельных пользователей используется группа настроек «Для выбранных».

Установка флажка «LiveView» включает режим оперативного контроля активности экрана одного или нескольких пользователей (просмотр в режиме реального времени).

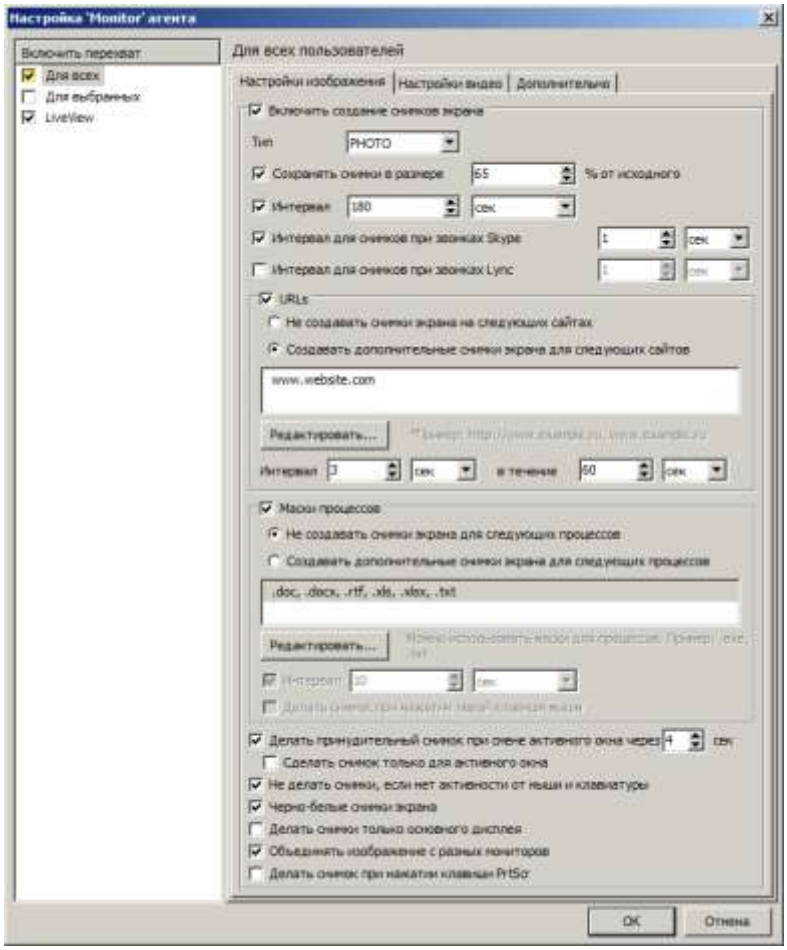


Рисунок 6.140

Таблица 22 содержит описание настроек изображений, видео и расписания **«Для всех» и «Для выбранных»** пользователей.

Таблица 26 – Описание настроек агента MonitorController в отношении всех пользователей

Настройка	Описание
Вкладка «Настройки изображения»	
Тип	Позволяет выбрать графический формат (PHOTO или PNG), в котором сохраняются перехваченные агентом снимки экрана. Формат PHOTO установлен по умолчанию и сохраняет изображения с цветопередачей 256 цветов (8 бит).
Качество (для типа PNG)	Задает число бит на пиксель. Возможны 4 значения: 1 бит (2 цвета), 4 бита (16 цветов), 8 бит (256 цветов) и 24 бита (полноцветное изображение). *Объем занимаемого снимками места в БД зависит от выбранного качества: чем выше количество бит, тем больше объем изображения. Например, объем 24-битных изображений может достигать порядка 1,5МБ, при этом объем 8-битных изображений будет порядка 200КБ.*

Настройка	Описание
Сохранять снимки в размере N% от исходного	Позволяет изменять размер сохраняемых снимков. Размер задается в процентах от исходного, значение по умолчанию - 65%.
Интервал	Позволяет задавать интервал (в секундах, минутах), через который будет происходить захват изображений экрана.
Интервал для снимков при звонках Skype	Позволяет задавать интервал (в секундах, минутах), через который будет происходить захват изображений звонков/видеоконференций Skype. *Для работы данной опции на целевом компьютере с агентом MonitorController должен быть также установлен агент SkypeController.*
Интервал для снимков при звонках Lync	Позволяет задавать интервал (в секундах, минутах), через который будет происходить захват изображений звонков/видеоконференций Lync. *Для работы данной опции на целевом компьютере с агентом MonitorController должен быть также установлен агент LyncController.*
URLs	Активация/деактивация списка веб-ресурсов, при посещении которых: • не будут создаваться скриншоты экрана либо • скриншоты будут создаваться с определенным **интервалом** (в секундах, минутах) **в течение** указанного времени (в секундах, минутах). Для открытия редактора списка веб-сайтов нажмите кнопку «Редактировать». *Указанные URLs должны быть открыты пользователем в браузере.*

Настройка	Описание
Маски процессов	Активация/деактивация списка масок процессов, при запуске которых: • не будут создаваться скриншоты экрана либо • скриншоты будут создаваться с определенным **интервалом** (в секундах, минутах) и/или **при каждом нажатии пользователем левой клавиши мыши** в указанных приложениях (*создание скриншотов по нажатию левой клавиши мыши требует, чтобы на контролируемом компьютере был также установлен модуль Keylogger).* Для открытия редактора списка масок процессов нажмите кнопку «Редактировать». *Скриншоты создаются применительно к приложениям, для которых прописаны маски процессов. При этом должно быть запущено хотя бы одно из указанных в списке приложений.*
Интервал для масок процессов	Позволяет задавать интервал (в секундах, минутах) захвата содержимого экрана применительно к указанным маскам процессов.
Делать снимок при нажатии левой клавиши мыши	При установленном флажке снимки будут производиться при нажатии левой клавиши мыши в указанных приложениях/процессах.
Поведение при смене активного окна	Установленный флажок включает режим принудительного захвата снимков экрана при смене пользователем активного окна: снятие изображения экрана будет происходить при каждом переходе пользователя в другое окно через заданное число секунд.
Сделать снимок только активного окна	При установленном флажке снимается только активное окно. При снятом - весь экран.
Не делать снимки, если нет активности от мыши и клавиатуры	Установленный флажок отменяет захват снимков экрана при отсутствии активности пользователя (бездействие мыши и клавиатуры) в течение 2 минут.
Делать снимки только основного дисплея	Если к компьютеру пользователя подключено несколько мониторов, то при установленном флаге снимки будут производиться только с основного дисплея.
Чёрно-белые снимки экрана	При установленном флажке снимки сохраняются в чёрно-белом варианте, вместо цветного изображения.
Объединять изображения с разных мониторов	При установленном флажке снимки с разных мониторов объединяются в одно изображение.

Настройка	Описание
Делать снимок при нажатии PrtScr	При установленном флажке снимается содержимое экрана в момент нажатия клавиши PrintScreen. *Для работы функционала должен быть включен модуль перехвата KeyLogger.*
Вкладка «Настройки видео»	
Включить создание видео	Установленный флажок включает видеозапись мониторной активности.
Оттенки серого	При установленном флажке видео сохраняется в оттенках серого цвета, вместо цветной видеозаписи.
Исключить фон	При установленном флажке не записывается фоновое изображение.
Сохранять видео в размере N% от исходного	Позволяет изменять размер сохраняемых видеозаписей. Размер задается в процентах от исходного, значение по умолчанию - 65%.
Не делать видео, если нет активности от мыши и клавиатуры	Установленный флажок отменяет запись видео с экрана при отсутствии активности пользователя (бездействие мыши и клавиатуры) в течение 2 минут.
Делать видео только основного дисплея	Если к компьютеру пользователя подключено несколько мониторов, то при установленном флаге запись видео будет производиться только с основного дисплея.
Объединять видео с разных мониторов	При установленном флажке видео с разных мониторов объединяется в один файл.
Дополнительные настройки	При установленном флажке доступна корректировка частоты кадров в секунду. Рекомендуемое значение - 10 к/с. При заданных рекомендуемых параметрах объем данных в базе данных в среднем составит 50-400 МБ (варьируется в зависимости от выполняемых пользователем действий) с одного компьютера за рабочий день.
Записывать видео для всех процессов и сайтов	Запись видео будет производиться при работе с любыми процессами и сайтами.
Записывать видео для процессов и сайтов, указанных ниже	Запись видео будет производиться ТОЛЬКО при работе с указанными процессами и/или сайтами.
URL	Позволяет задать URLs, при посещении которых будет происходить запись видео с экрана. Указанные URLs должны быть открыты в браузере.
Маски процессов	Позволяет задавать процессы, к которым применяются маски. Запись видео с экрана осуществляется применительно к приложениям, для которых прописаны маски процессов. При этом должно быть запущено хотя бы одно из указанных приложений.

Настройка	Описание
Вкладка «Дополнительно»	
Включение расписания	Установленный флажок включает перехват мониторной активности по заданному расписанию.
Поле расписания	Графическое задание расписания перехвата мониторной активности.

Таблица 27 содержит описание параметров вкладки **«Пользователи и группы»**. Вкладка доступна только «Для выбранных» и предназначена для настройки списка пользователей (групп), для которых действуют настройки перехвата, заданные «Для выбранных».

Таблица 27 – Описание настроек агента MonitorController в отношении выбранных пользователей

Настройка	Описание
Вкладка «Пользователи и группы»	
[поле просмотра]	Отображает список пользователей, к которым применяется перехват мониторной активности. Команда «Очистить» из контекстного меню полностью удаляет список пользователей.
[поле ввода]	Позволяет вводить имя пользователя или группы, к которым будет применяться захват снимков экрана.
Кнопка добавления пользователей […]	Открывает стандартное окно выбора пользователей. Отметьте флажками необходимых пользователей и нажмите «Добавить».
Кнопка «Заменить»	Позволяет заменить пользователя или группу, выбранную в списке, на пользователя или группу, введенного в поле ввода.
Кнопка «Добавить»	Позволяет добавить пользователя или группу, в отношении которых назначен перехват мониторной активности.
Кнопка «Удалить»	Позволяет удалить пользователя или группу, в отношении которых назначен перехват мониторной активности.

Таблица 28 содержит описание настроек режима LiveView.

Таблица 28 – Описание настроек режима LiveView

Настройка	Описание
Вкладка «Основные»	
Порт	Позволяет задавать номер порта, через который производится передача данных в режиме оперативного контроля. Если порт отличается от значения по умолчанию, то соответствующий номер должен быть задан и в AnalyticConsole.

Настройка	Описание
Частота кадров	Позволяет задавать частоту смены кадров в режиме реального времени. При повышении частоты смены кадров увеличивается нагрузка на процессор, что приводит к замедлению рабочих операций компьютера.
Качество	Задает число бит на пиксель. Возможны 4 значения: 1 бит (2 цвета), 4 бита (16 цветов), 8 бит (256 цветов) и 24 бита (полноцветное изображение).
Оттенки серого	При установленном флажке данные в режиме LiveView отображаются в оттенках серого цвета, вместо цветного изображения.
Вкладка «Авторизация»	
Не задано	Тип авторизации не задан.
Пароль	Ограничить доступ к режиму LiveView в можно задав пароль. Для разрешения работы в настройках AnalyticConsole нужно подтвердить пароль. В противном случае в окне просмотра экрана в режиме реального времени будет отображаться сообщение «Разрыв соединения (ошибка проверки подлинности)».
Выбранные пользователи	Учетные записи, от имени которых будет доступна работа в режиме LiveView в AnalyticConsole.

Для сохранения настроек MonitorController в окне редактирования агента нажмите «OK».

Щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведённые настройки вступили в силу.

6.5.1.11 Настройка модуля перехвата CameraController

Модуль перехвата CameraController предназначен для создания снимков и видеозаписей происходящего за компьютером (при наличии подключенной к нему либо встроенной веб-камеры).

Модуль CameraController предназначен для создания снимков и видеозаписей происходящего за компьютером (при наличии подключенной к нему либо встроенной веб-камеры).

Для компонента CameraController создаются базы данных, которые затем соответствующим образом настраиваются. Базы данных CameraController не привязываются к индексам.

Порядок действий для создания базы CameraController (если не было выполнено в п.6.5.1):

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «CameraController» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.141).

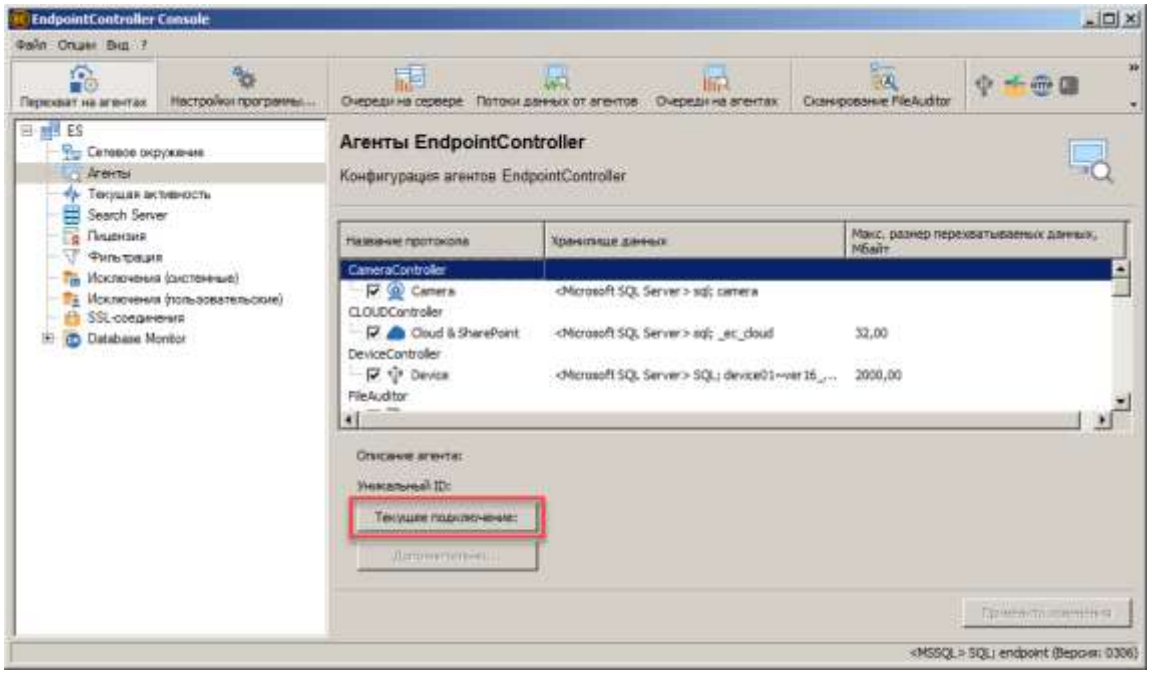


Рисунок 6.141

2. Настройте подключение к базе данных.

Порядок действий для создания базы CameraController аналогичен вышеизложенному порядку создания базы данных FileController (см.Таблица 22).

Управление агентом с подключенной базой производится на вкладке «Агенты» консоли администрирования. Выделите протокол CameraController и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку  на панели «Конфигурирование агентов» либо кнопку «Дополнительно») (см. Рисунок 6.142).

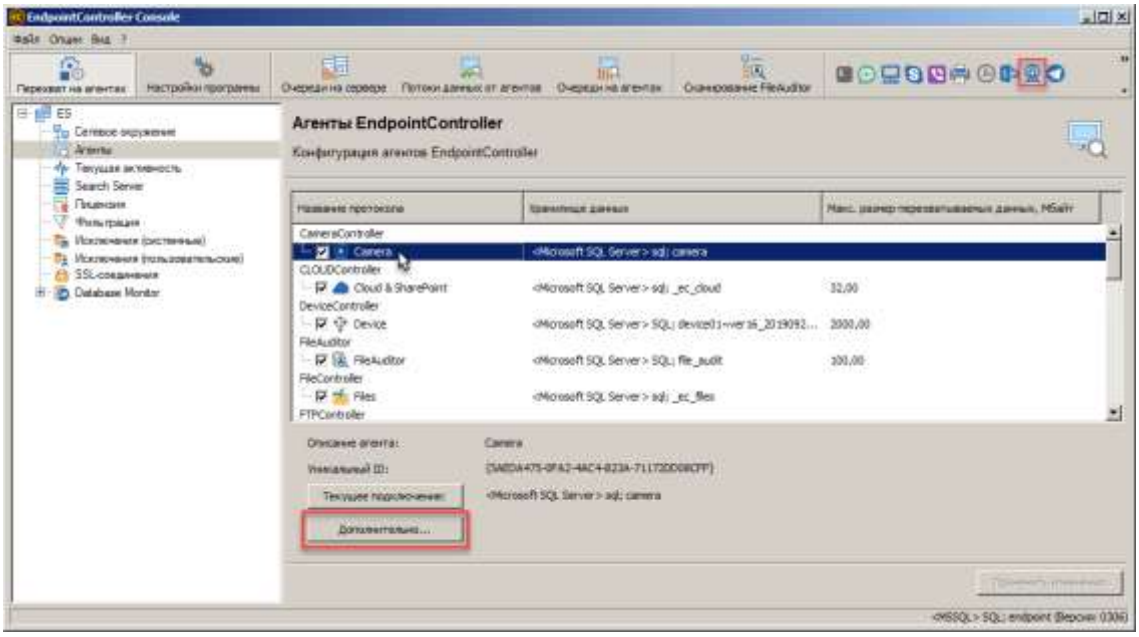


Рисунок 6.142

Установка флажка «Включить перехват» позволяет производить настройки перехватываемых изображений и видео, обработку масок процессов, а также управлять записью в отношении определенных URLs.

Установка флажка «LiveCam» включает режим оперативного слежения за пользователем в режиме реального времени.

Узел настроек «Включить перехват» содержит следующие вкладки:

- Настройки изображения (см. Рисунок 6.143)

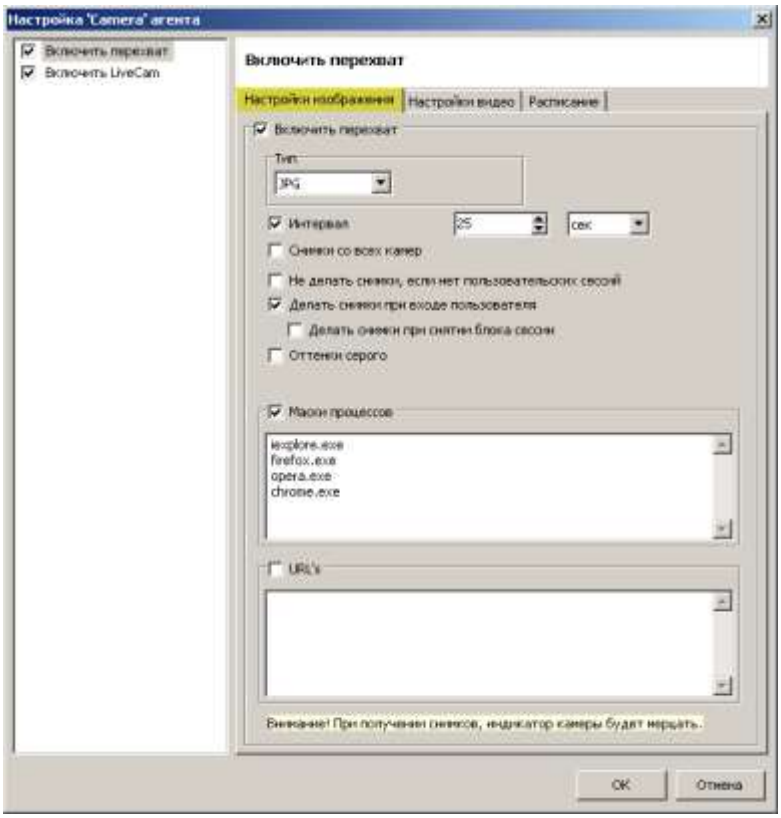


Рисунок 6.143

- Настройки видео (см. Рисунок 6.144)

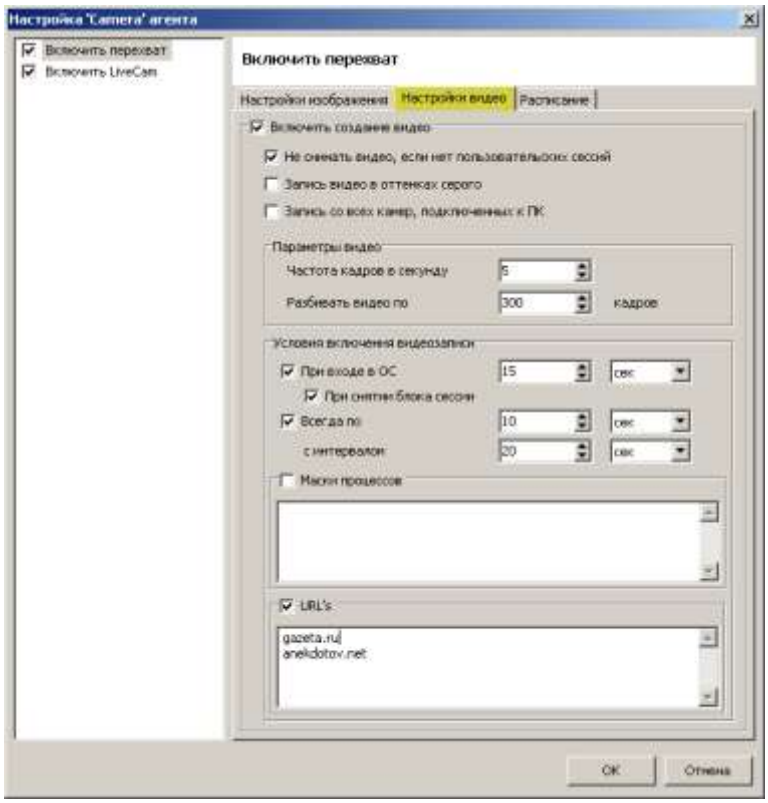


Рисунок 6.144

- Расписание (см.Рисунок 6.145)

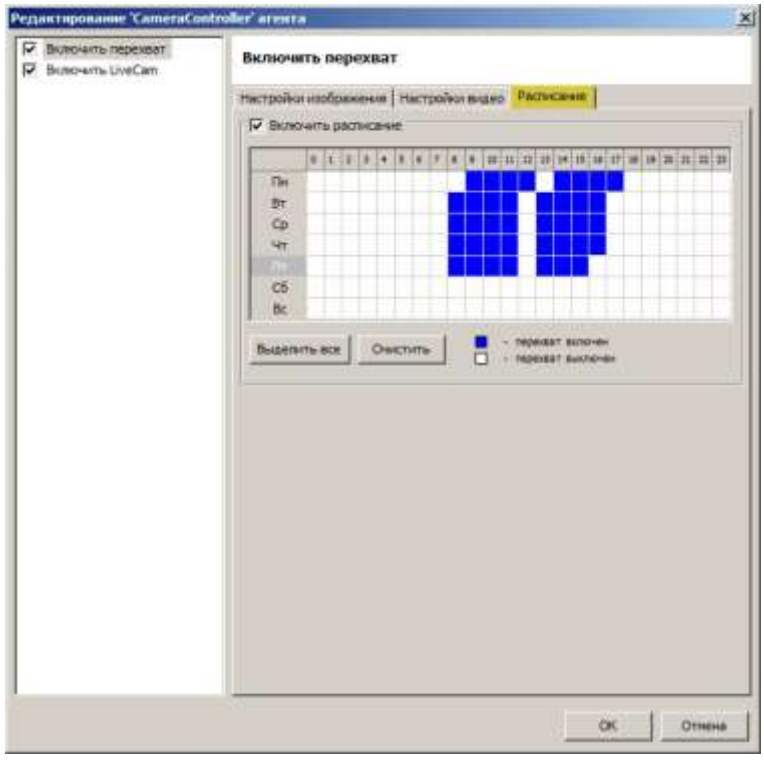


Рисунок 6.145

Таблица 29 содержит описание настроек перехвата агентом CameraController.

Таблица 29 – Описание настроек агента CameraController

Настройка	Описание
Вкладка «Настройки изображения»	
Включить создание снимков	Установленный флажок включает снятие камерой изображений.
Тип	Графический формат (JPG или PNG), в котором сохраняются созданные камерой снимки.
Качество (для типа PNG) [23]	Задает число бит на пиксель. Возможны 4 значения: 1 бит (2 цвета), 4 бита (16 цветов), 8 бит (256 цветов) и 24 бита (полноцветное изображение). *Объем занимаемого снимками места в БД зависит от выбранного качества: чем выше количество бит, тем больше объем изображения. Например, объем 24-битных изображений может достигать порядка 1,5МБ, при этом объем 8-битных изображений будет порядка 200КБ.*
Интервал	Позволяет задавать интервал (в секундах, минутах), через который будет происходить создание снимков.
Снимки со всех камер	Установленный флажок включает функционал создания снимков всеми доступными камерами.
Не делать снимки, если нет пользовательских сессий	Установленный флажок отменяет создание снимков экрана при отсутствии на компьютере пользовательских сессий.
Делать снимки при входе пользователя	Установленный флажок включает создание снимков при авторизации в системе.
При снятии блока сессии	Установленный флажок включает создание снимков при разблокировании сессии
Оттенки серого	При установленном флажке снимки сохраняются в чёрно-белом варианте, вместо цветного изображения
Маски процессов	Процессы, при запуске хотя бы одного из которых создаются снимки
URL's	Веб-ресурсы, при посещении которых создаются снимки
Вкладка «Настройки видео»	
Включить создание видео	Установленный флажок включает видеозапись происходящего за компьютером
Не снимать видео, если нет пользовательских сессий	Установленный флажок отменяет запись камерой видео при отсутствии на компьютере пользовательских сессий

[23] Следует учитывать, что на передачу и обработку пакетов данных затрачивается время, поэтому важно сбалансировать нагрузку с целью своевременного отображения свежих данных в AnalyticConsole. К примеру, если настройки записываемого видео максимальны, рекомендуется снизить требования к создаваемым снимкам. И наоборот - при максимальном качестве создаваемых снимков должны быть снижены требования к записываемому видео.

Настройка	Описание
Запись видео в оттенках серого	При установленном флажке видео сохраняется в оттенках серого цвета, вместо цветной видеозаписи
Запись со всех камер, подключенных к ПК	Установленный флажок включает функционал записи видео всеми доступными камерами
Параметры видео	
Частота кадров в секунду[24]	Количество сменяемых кадров за 1 секунду (минимум - 1, максимум - 10)
Разбивать видео по N кадров	Максимальное количество кадров в одном видеофрагменте (минимум - 100, максимум - 500)
Условия включения видеозаписи	
При входе в ОС	Длительность видеозаписей (в секундах, минутах), создаваемых в момент авторизации пользователей в системе
При снятии блока сессии	Установленный флажок включает запись видео при разблокировании сессии
Всегда по	Длительность видеофайлов (в секундах, минутах)
с интервалом	Интервал (в секундах, минутах), через который будет происходить запись видео
Маски процессов	Процессы, при запуске хотя бы одного из которых начинается видеозапись
URL's	Веб-ресурсы, при посещении которых начинается видеозапись
Вкладка «Расписание»	
Включение расписания	Установленный флажок включает создание снимков/видео по заданному расписанию.
Поле расписания	Графическое задание расписания создания снимков/видео.
Время	Задает начальное и конечное время, в течение которого будет производиться создание снимков/видео. Значение вводится вручную либо выбирается с помощью регулятора.
Дни недели	Задает дни недели, по которым будет производиться создание снимков/видео. Дни недели назначаются установлением флажка.

Таблица 30 содержит описание настроек режима LiveCam агента CameraController.

[24] Следует учитывать, что на передачу и обработку пакетов данных затрачивается время, поэтому важно сбалансировать нагрузку с целью своевременного отображения свежих данных в консоли Серчинформ AnalyticConsole. К примеру, если настройки записываемого видео максимальны, рекомендуется снизить требования к создаваемым снимкам. И наоборот - при максимальном качестве создаваемых снимков должны быть снижены требования к записываемому видео.

Таблица 30 – Описание настроек режима LiveCam

Настройка	Описание
Вкладка «Основные»	
Порт	Номер порта, через который производится передача данных в режиме оперативного контроля. Если порт отличается от значения по умолчанию, то соответствующий номер должен быть задан и в AnalyticConsole.
Частота кадров	Частота смены кадров в режиме реального времени.
Оттенки серого	При установленном флажке трансляция видео осуществляется в оттенках серого цвета вместо цветной.
Вкладка «Авторизация»	
Не задано	Тип авторизации не задан.
Пароль	Ограничить доступ к режиму LiveCam можно задав пароль. Для разрешения работы в настройках AnalyticConsole нужно подтвердить пароль. В противном случае в окне просмотра экрана в режиме реального времени будет отображаться сообщение «Разрыв соединения (ошибка проверки подлинности)».
Выбранные пользователи	Разрешить добавленным пользователям работать с LiveCam в AnalyticConsole.

Для сохранения настроек агента CameraController в окне редактирования агента нажмите «OK».

Щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведённые настройки вступили в силу.

6.5.1.12 Настройка модуля перехвата PrintController

Модуль перехвата PrintController предназначен для перехвата содержимого документов, поступающих на печать.

Для компонента PrintController создаются базы данных, которые затем соответствующим образом настраиваются. Базы данных PrintController необходимо привязывать к индексам.

Порядок действий для создания базы PrintController:

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «PrintController» и щёлкните кнопку «Текущее подключение».

2. Настройте подключение к базе данных (см. Рисунок 6.146).

Порядок действий для создания базы PrintController аналогичен вышеизложенному порядку создания базы данных FileController (см. Таблица 22).

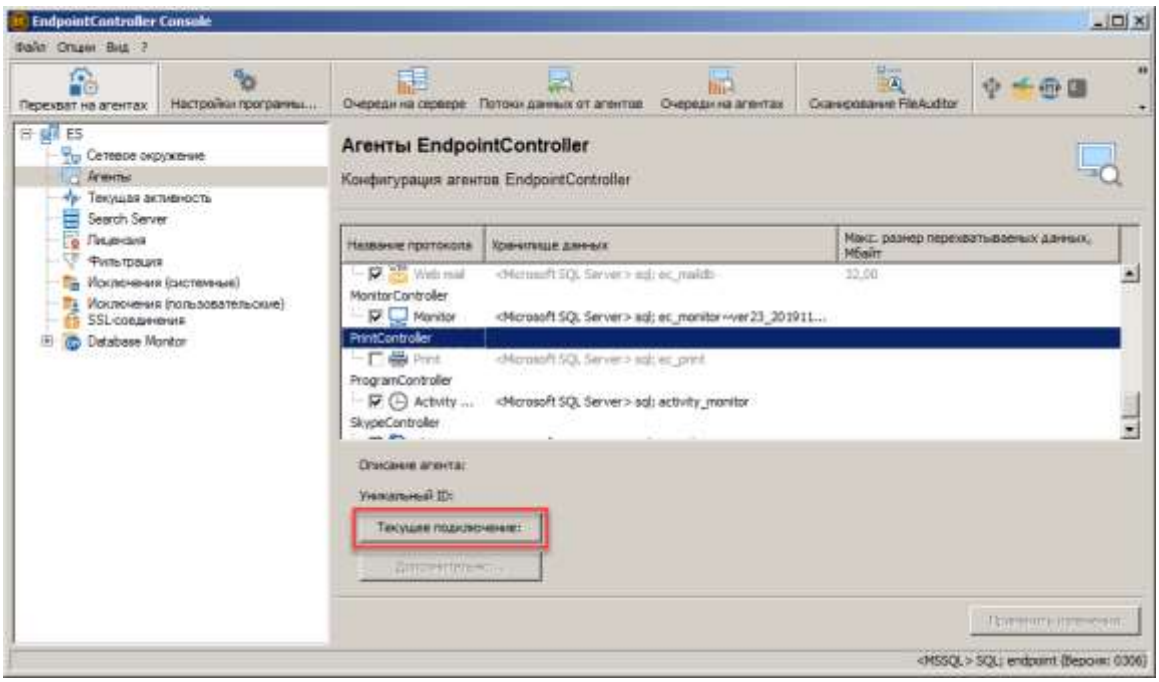


Рисунок 6.146

Для настройки агента PrintController с подключенной базой щёлкните дважды по названию протокола Print (варианты: щелкните кнопку на панели «Конфигурирование агентов» либо кнопку «Дополнительно» в нижней части окна).

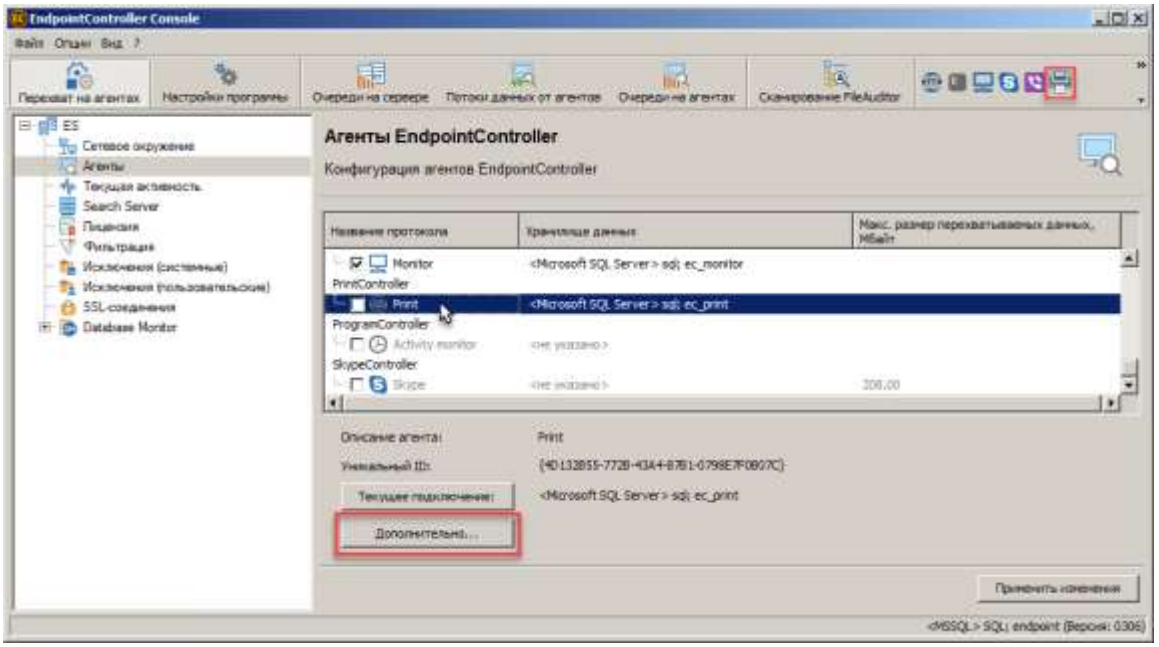


Рисунок 6.147

Окно редактирования агента PrintController позволяет:

- конфигурировать правила перехвата для отдельных принтеров в сети;
- задавать качество и DPI (dots per inch - количество точек на дюйм) перехватываемых изображений, используемое по умолчанию для всех принтеров.

Для создания нового правила перехвата нажмите кнопку «Добавить» (см. Рисунок 6.148Рисунок 6.150).

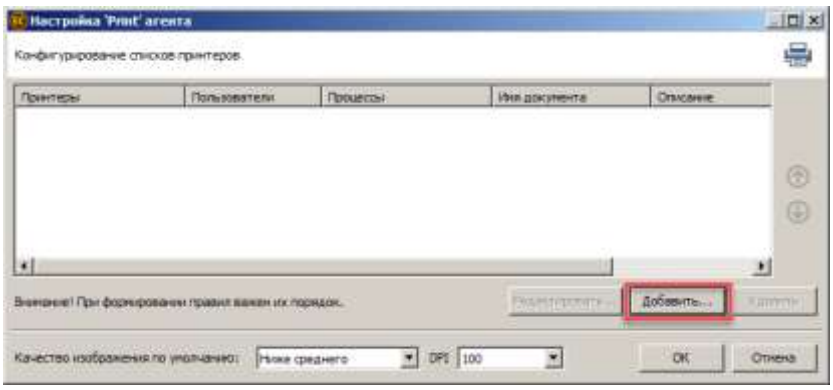


Рисунок 6.148

В открывшемся окне введите название принтера (для выбора всех принтеров введите «*») и выберите необходимое действие:

- **Исключить из перехвата**. Для принтеров из списка не перехватываются документы, отправленные на печать.
- **Блокировка Escape функций**. Для принтеров из списка блокируется печать через Escape функции.
- **Переопределение качества изображения.** Задание для указанного принтера индивидуальных параметров «Качество изображения» и «DPI» (см. Рисунок 6.149).

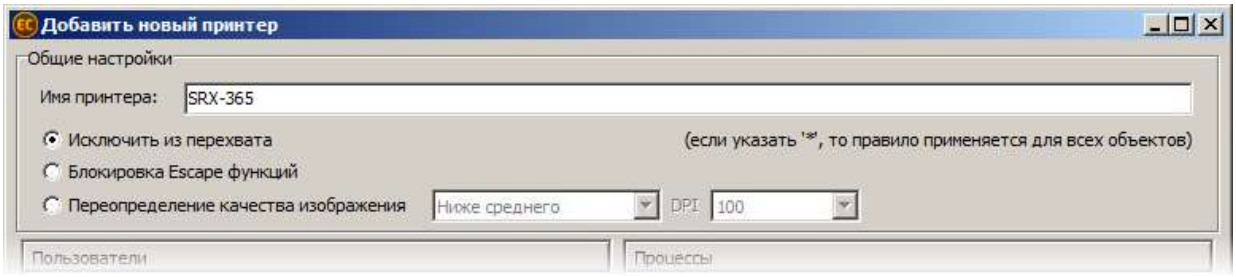


Рисунок 6.149

Для категории «Исключить из сетевого перехвата» пустое поле в строке «Имя» означает разрешить перехват для принтеров, которые подпадают под заданные ниже параметры.

Правило позволяет задатьследующие параметры:

- **Пользователи** (формат записи для добавления пользователей - **user@domain.local**, для добавления группы - **DOMAIN\group**);
- **Процессы** - названия процессов из которых произведена отправка документов на печать;
- **Описание и расположение** - соответствующие поля в свойствах принтера (в случае отсутствия данных свойств у принтера, оставьте поле пустым);

- **Имя документа** - название документа, который необходимо исключить из перехвата (в имени документа кроме метасимвола «*», заменяющего от нуля и более символов, допускается использование метасимвола «?», заменяющего один любой символ).

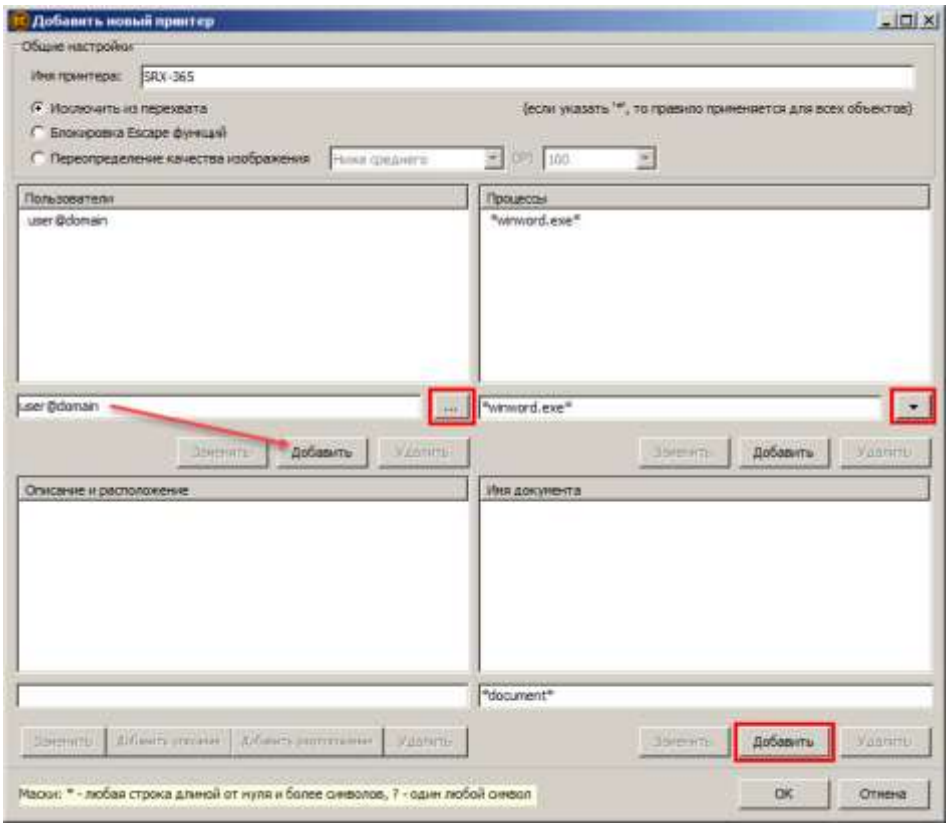


Рисунок 6.150

Для сохранения настроек PrintController в окне редактирования агента нажмите «OK».

Задайте качество перехватываемых изображений:

- Наилучшее - png;
- Высокое - jpeg (100%);
- Среднее - jpeg (90%);
- Ниже среднего (используется по умолчанию) - jpeg (75%);
- Низкое - jpeg (40%).

Также доступны следующие значения параметра «DPI» (dots per inch - количество точек на дюйм):

- 100 (используется по умолчанию);
- 300 - рекомендуется использовать для распознавания текста со шрифтом 10 и выше (*данные ABBYY);
- 600 - рекомендуется использовать для распознавания текста со шрифтом 9 и ниже (*данные ABBYY);

- Оригинал - оригинальное DPI принтера. *Если сохранить изображение в оригинальном разрешении не удается, то выполняются повторные попытки сохранения с уменьшением значения DPI в 2 раза (пока DPI не станет меньше 100)* (см.Рисунок 6.151).

Качество перехватываемых изображений по умолчанию можно переопределить для отдельного принтера. Чем выше качество и/или количество DPI, тем больше места будут занимать перехватываемые данные. Также следуют учитывать, что высокое значение DPI может существенно замедлить работу сервера/агента EndpointController.

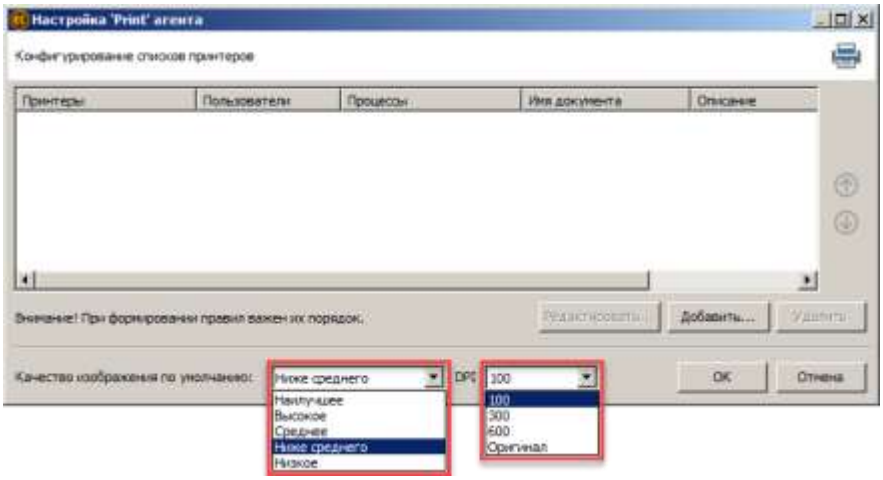


Рисунок 6.151

Щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведённые настройки вступили в силу.

6.5.1.13 Настройка модуля перехвата ProgramController

Модуль перехвата ProgramController предназначен для мониторинга активности запускаемых сотрудником приложений.

Для компонента ProgramController создаются базы данных, которые затем соответствующим образом настраиваются. Базы данных ProgramController не привязываются к индексам.

Порядок действий для создания базы ProgramController:

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «ProgramController» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.152).

2. Настройте подключение к базе данных.

Порядок действий для создания базы ProgramController аналогичен вышеизложенному порядку создания базы данных FileController (см. Таблица 22).

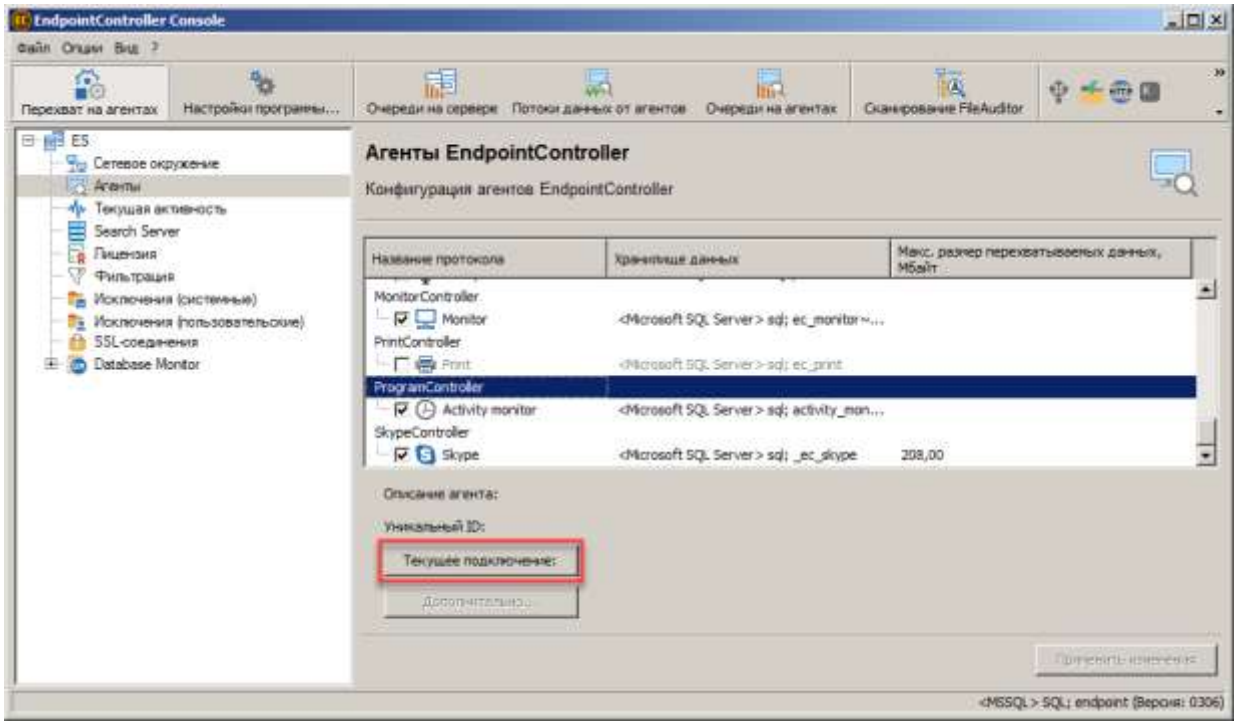


Рисунок 6.152

Управление агентом с подключенной базой производится на вкладке «Агенты» консоли администрирования. Выделите протокол «Activity monitor» и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку  на панели «Конфигурирование агентов» либо кнопку «Дополнительно») (см. Рисунок 6.153).

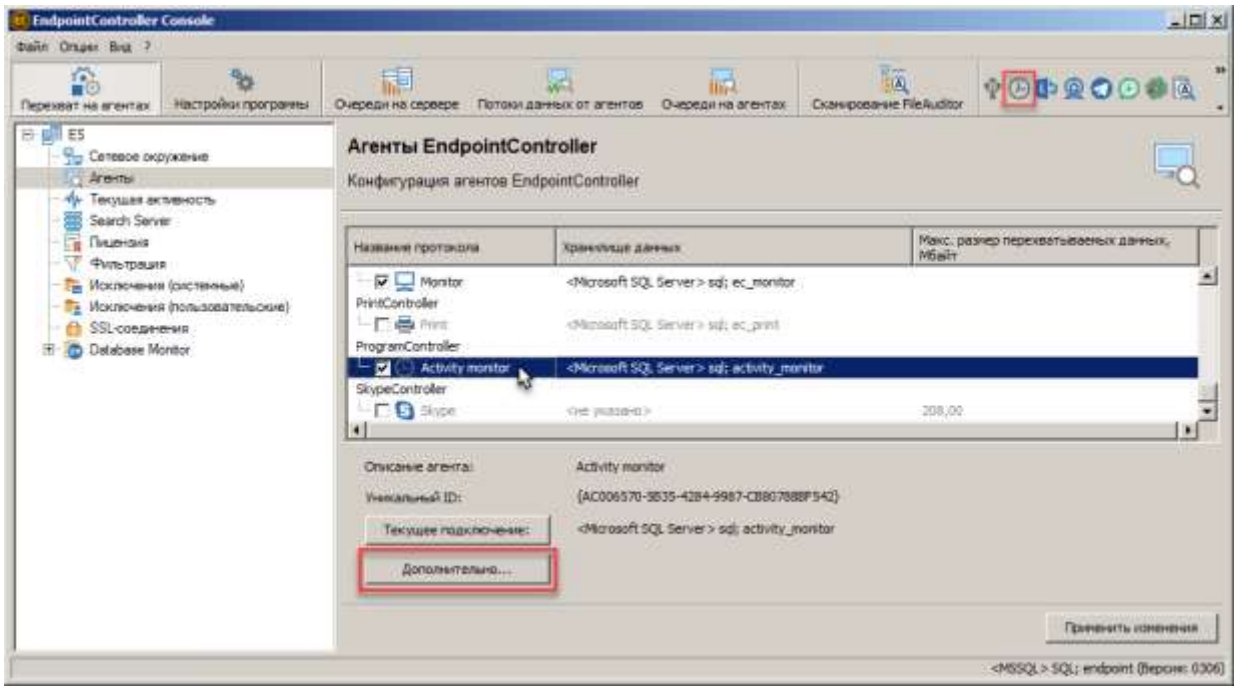


Рисунок 6.153

В диалоговом окне «Настройка 'Activity monitor' агента» отображается настроенный перечень правил мониторинга активности процессов. Для управления списком используются следующие кнопки:

- **Добавить** - создание нового правила;
- **Редактировать** - изменение имеющегося в списке правила;
- **Удалить** - удаление правила из списка (см. Рисунок 6.154).

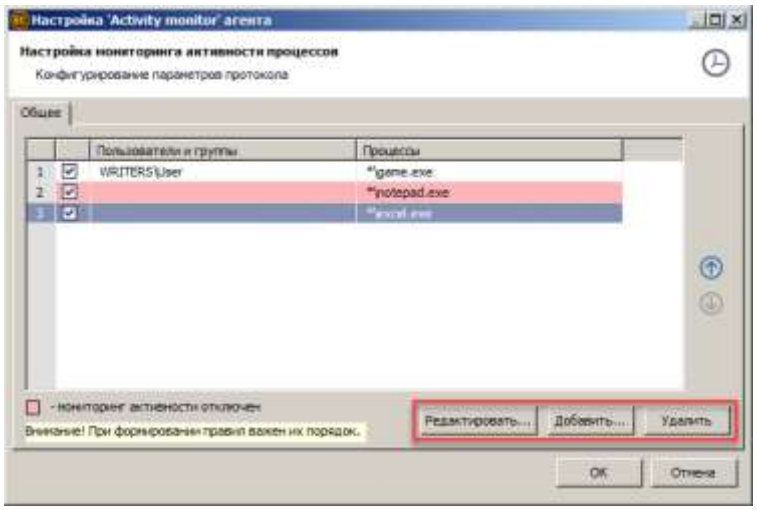


Рисунок 6.154

Щёлкните кнопку «Добавить». Появится диалоговое окно «Добавление правила для ProgramController».

Работа со списком пользователей, к которым применяется мониторинг активности либо которые исключаются из мониторинга, производится в левой части окна «Добавление правила для ProgramController» (см. Рисунок 6.155).

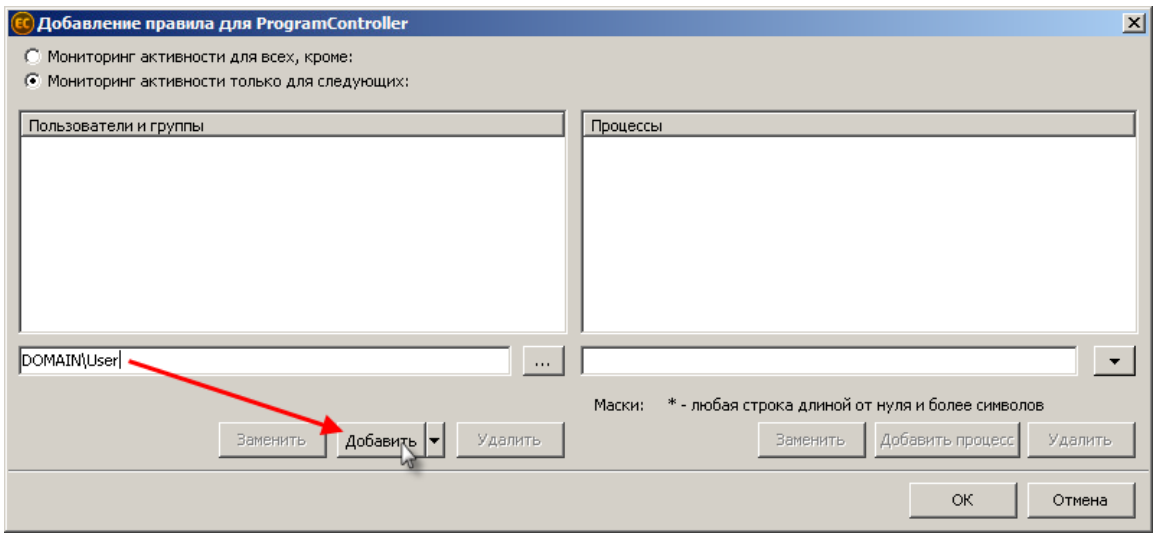


Рисунок 6.155

Работа со списком процессов, активность которых необходимо фиксировать, производится в правой части окна «Добавление правила для ProgramController» (см. Рисунок 6.156).

Для фиксирования активности в запущенных процессах должен быть выбран фильтр «Мониторинг активности только для следующих». Если выбран исключающий фильтр («Мониторинг активности для всех, кроме»), то для указанных процессов фиксирование активности производиться не будет (оно будет производиться при запуске всех остальных процессов).

Введите имя процесса в текстовое поле и щёлкните кнопку «Добавить процесс».

Рисунок 6.156

Для сохранения настроек в окне редактирования нажмите «OK», а затем нажмите кнопку «Применить изменения» в консоли администрирования.

6.5.1.14 Настройка модуля перехвата SkypeController

Модуль перехвата SkypeController используется для перехвата и анализа трафика Skype: сеансов текстовой и голосовой связи, файлов и SMS-сообщений, переданных при помощи Skype.

Для модуля SkypeController создается база данных, которая затем соответствующим образом настраивается. Базы данных SkypeController необходимо привязывать к индексам.

Порядок действий для создания базы SkypeController:

1. Перейдите на вкладку «Агенты», выделите в списке агентов позицию «SkypeController» и щёлкните кнопку «Текущее подключение» (см. Рисунок 6.157).

2. Настройте подключение к базе данных. Порядок действий для создания базы SkypeController аналогичен вышеизложенному порядку создания базы данных FileController (см. Таблица 22).

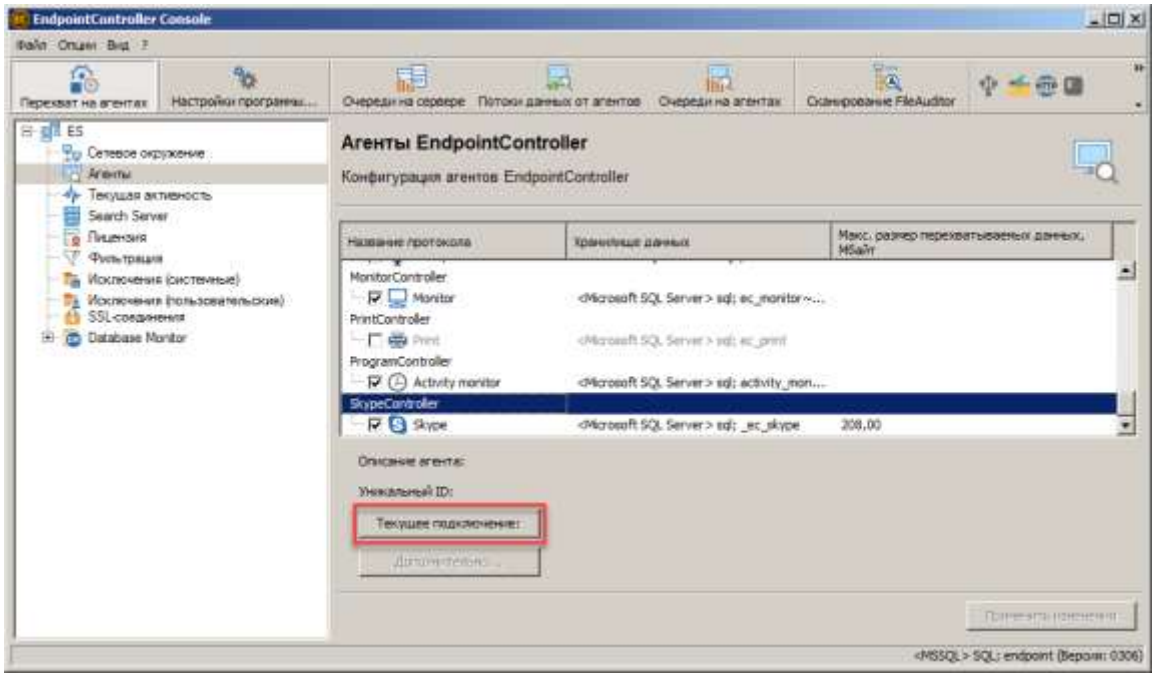


Рисунок 6.157

Управление агентом с подключенной базой производится на вкладке «Агенты» консоли администрирования. Выделите протокол SkypeController и двойным щелчком откройте окно редактирования агента (варианты: щёлкните кнопку на панели «Конфигурирование агентов» либо кнопку «Дополнительно» в нижней части окна) (см. Рисунок 6.158).

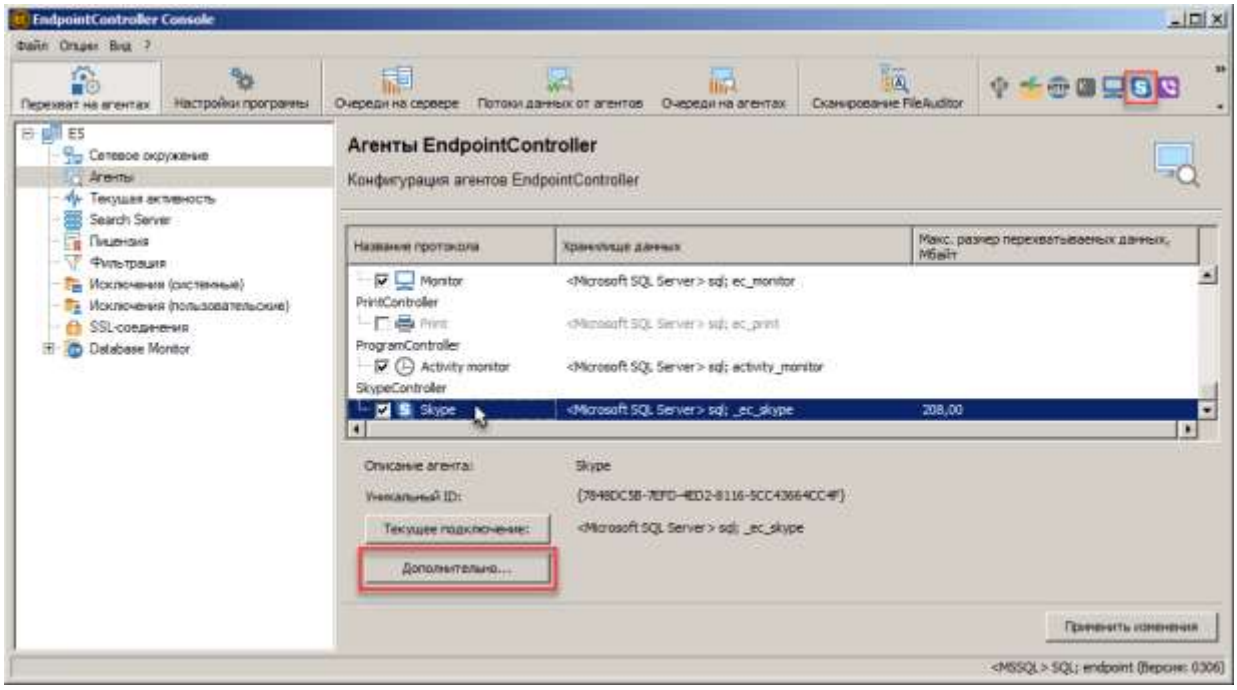


Рисунок 6.158

В открывшемся окне редактирования агента SkypeController произведите необходимые настройки фильтрации каналов данных (чаты, звонки, контакты, файлы,

SMS-сообщения), импорта (чаты, SMS-сообщения), параметров голосовой связи (формат записи, битрейт, максимальный битрейт, качество и метод захвата, максимальную длительность сеанса связи) и пользователей Skype (см. Рисунок 6.159).

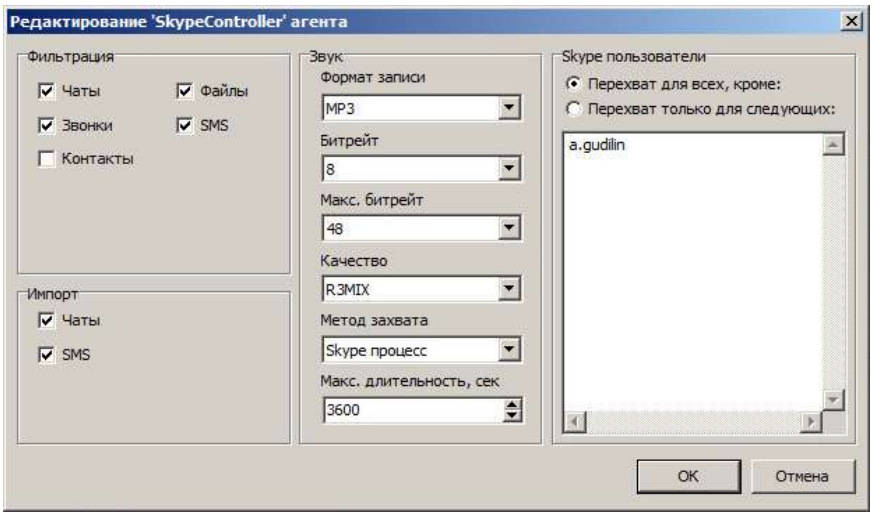


Рисунок 6.159

Таблица 31 содержит описание настроек агента SkypeController.

Таблица 31 – Описание настроек агента SkypeController

Настройка	Описание
«Фильтрация»	
Чаты	Установленный флажок включает перехват чатов.
Файлы	Установленный флажок включает захват файлов, переданных через Skype.
Звонки	Установленный флажок включает перехват сеансов голосовой связи.
SMS	Установленный флажок включает захват отправленных СМС-сообщений.
Контакты	Установленный флажок включает перехват списка контактов.
«Импорт»	
Чаты	Установленный флажок позволяет перехватывать историю сообщений в чатах.
SMS	Установленный флажок позволяет сохранять историю отправленных СМС-сообщений.
«Звук»	
Формат записи	Задается формат записи: MP3 - формат со сжатием данных, или WAV - формат без сжатия.
Битрейт	Задается битрейт для записей в формате MP3. Минимальный – 8 кбит/с, максимально возможный – 320 кбит/с.
Макс. битрейт	Задается максимальный битрейт для записей в формате MP3.

Настройка	Описание
Качество	Задается качество записываемого сеанса голосовой связи в формате MP3. Данный параметр задает пресет кодека LAME, который выполняет сжатие полученных от микрофона данных (пресет — предварительно заданная схема настроек параметров). По умолчанию в SkypeController используется пресет R3MIX, который обеспечивает неплохой уровень качества при достойной скорости сжатия и использует Variable Bit Rate (VBR) - технологию изменяющегося битрейта, при которой битрейт динамически изменяется кодером. Например, тишина кодируется с минимальным битрейтом.
Метод захвата	Задается метод захвата звука: • Skype процесс; • Звуковая плата (Windows Vista и выше).
Макс. длительность, сек	Задается максимальная длительность файла звукозаписи. При превышении установленной длительности запись сеанса голосовой связи будет разделена на части.
«Skype пользователи»	
Перехват для всех, кроме:	Через запятую задаются только те логины пользователей Skype, которые будут исключены из перехвата.
Перехват только для следующих:	Через запятую задаются только те логины пользователей Skype, для которых будет осуществляться перехват.

Для сохранения настроек в окне редактирования агента нажмите «OK», а затем щёлкните кнопку «Применить изменения» в консоли администрирования, чтобы произведённые настройки агента SkypeController вступили в силу.

6.5.1.15 Настройка модуля «Индексация рабочих станций»

Модуль перехвата «Индексация рабочих станций» (ИРС) позволяет отслеживать появление, копирование, пермодемещение и удаление документов с конфиденциальной информацией на рабочих станциях пользователей.

Управление агентом производится на вкладке «Агенты» консоли администрирования. Выделите протокол «Индексация рабочих станций» и двойным щелчком откройте окно редактирования агента либо используйте кнопку «Дополнительно» в нижней части окна (см. Рисунок 6.160).

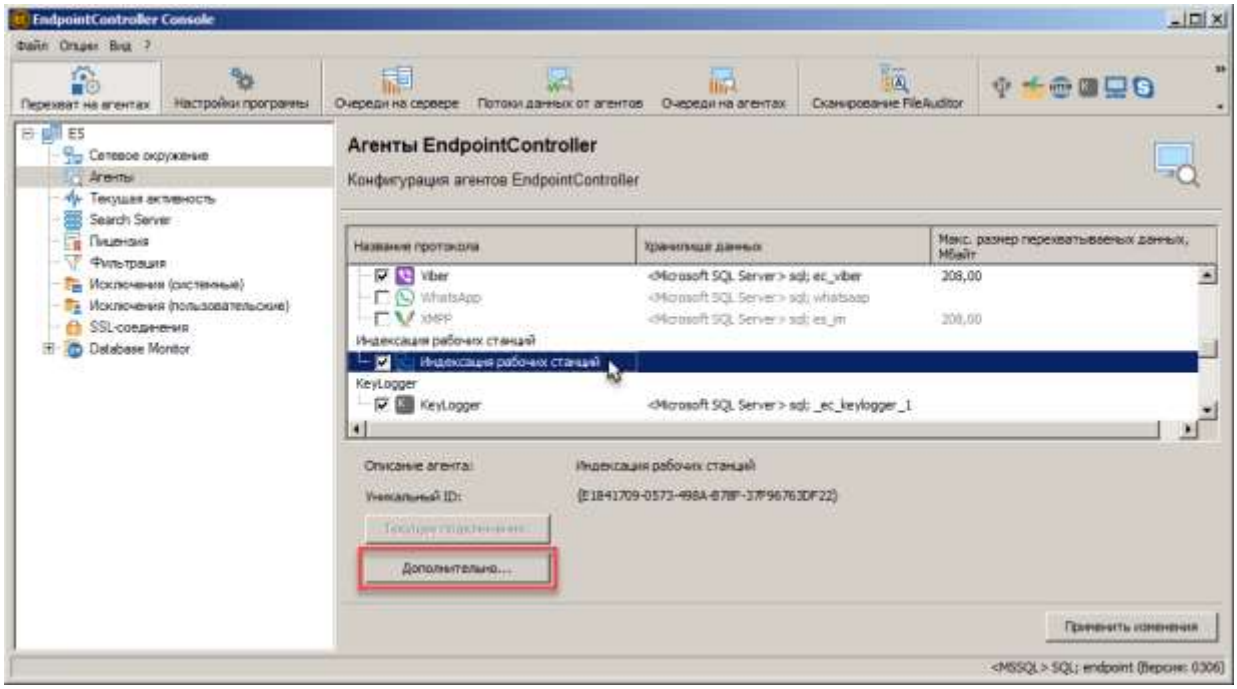


Рисунок 6.160

Окно настройки позволяет указать порт для передачи информации от агента серверу (см. Рисунок 6.161).

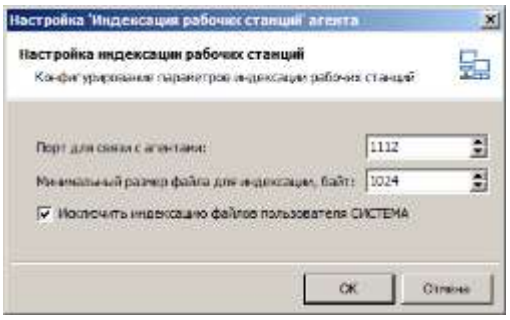


Рисунок 6.161

Настройка остальных параметров ИРС (контролируемые папки/диски, списки исключений, удаляемые файлы) производится на этапе создания индекса с помощью «Мастера настройки».

Выделите в списке протокол «Индексация рабочих станций» и нажмите «Далее» (см. Рисунок 6.162).

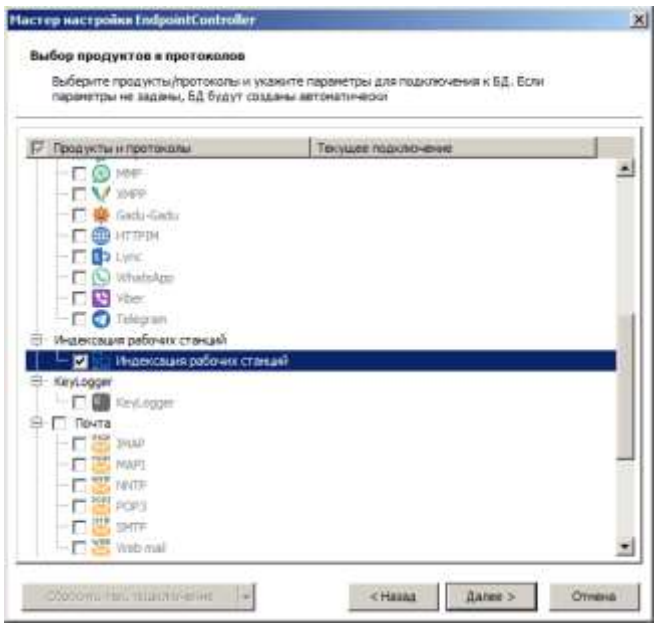


Рисунок 6.162

Для ИРС будет автоматически создан индекс.

Настройте формат префикса и/или суффикса, добавляемого к имени индекса. При необходимости, отметьте флажком опцию автоматического добавления имени источника данных. Нажмите «Далее» (Рисунок 6.163).

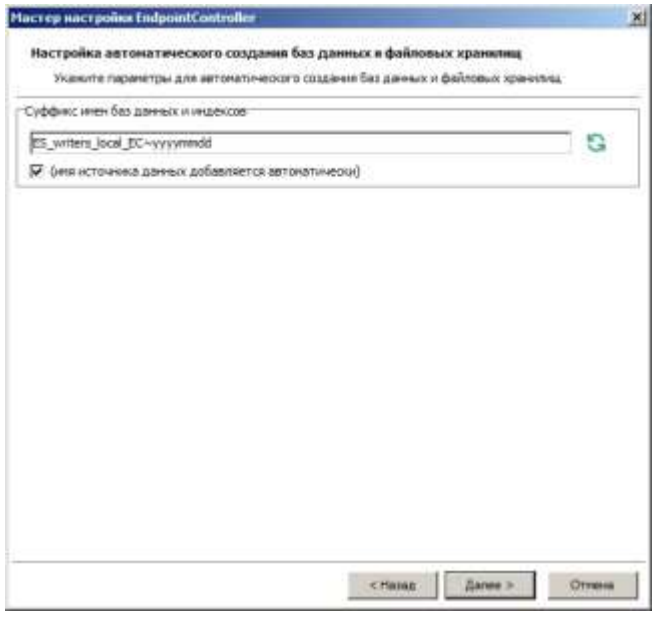


Рисунок 6.163

На этапе «Параметры автоматического создания индексов» нажмите кнопку «Выбрать компьютеры, диски...» для указания контролируемых модулем ИРС объектов (см. Рисунок 6.164). Нажмите «Далее».

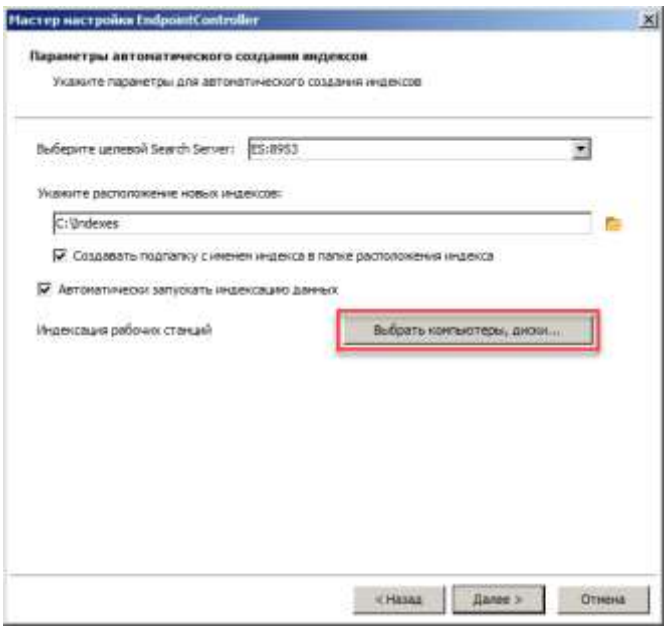


Рисунок 6.164

На вкладке «Сетевое окружение» выберите рабочие станции и директории, которые необходимо индексировать, а также укажите число потоков индексации (Параметр «Одновременно индексируемые компьютеры») (см. Рисунок 6.165).

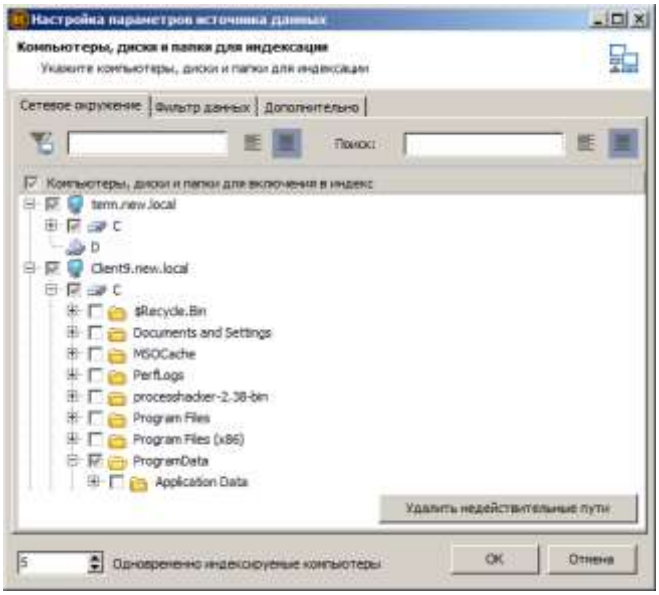


Рисунок 6.165

Для фильтрации списка компьютеров воспользуйтесь строкой рядом с иконкой . Для поиска файлов/папок среди отображаемых компьютеров введите искомое значение в строку «Поиск».

Кнопка «Удалить недействительные пути" отображается в случае, когда в раскрываемом дереве каталогов имеются удаленные папки (их имена имеют серый цвет). По нажатии кнопки такие папки будут удалены из списка.

На вкладке «Фильтр данных» выберите тип фильтра (разрешающий или запрещающий) и укажите расширения для файлов-исключений (см. Рисунок 6.166).

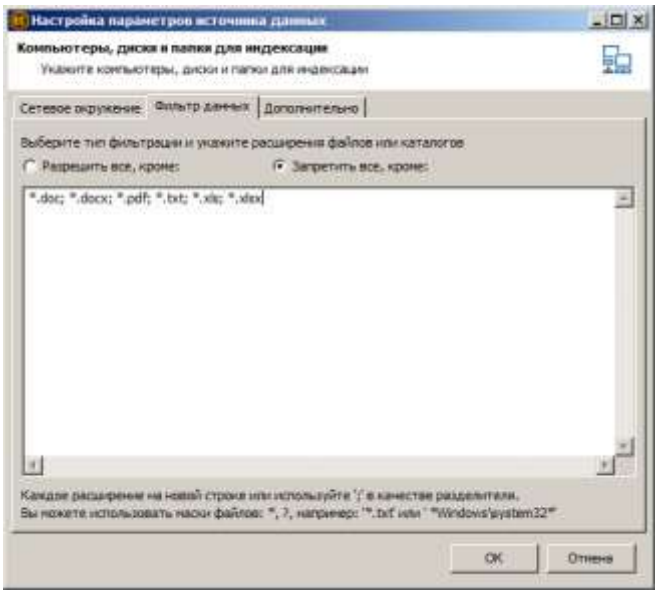


Рисунок 6.166

На вкладке «Дополнительно» установите флажок «Сохранить в индексе удаленные файлы, а также задайте срок хранения таких файлов.

Для сохранения в индексе файлов, форматы которых могут быть неизвестны детектору, установите флажок «Всегда сохранять в индексе файлы с расширениями:» и укажите типы таких расширений. Файлы данных форматов безусловно будут сохранены в индексе и в дальнейшем могут быть открыты в AnalyticConsole в ассоциированном формате либо сохранены на локальный диск (см. Рисунок 6.167).

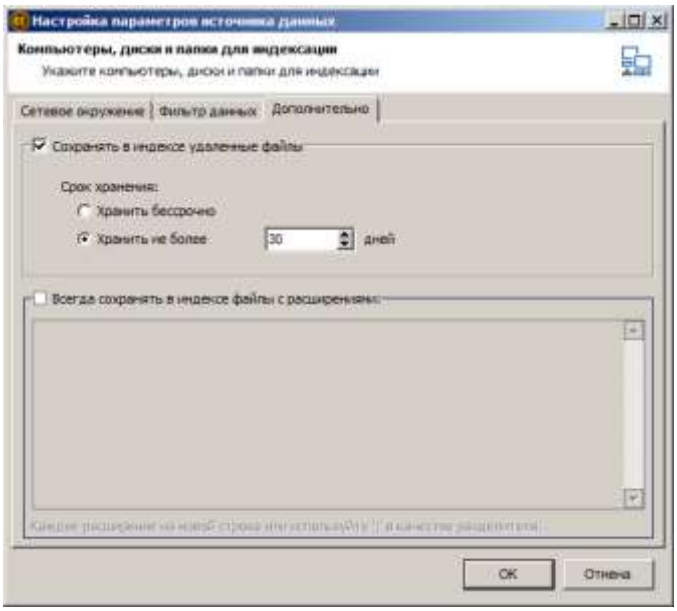


Рисунок 6.167

В окне мастера нажмите «Завершить» (см. Рисунок 6.168).

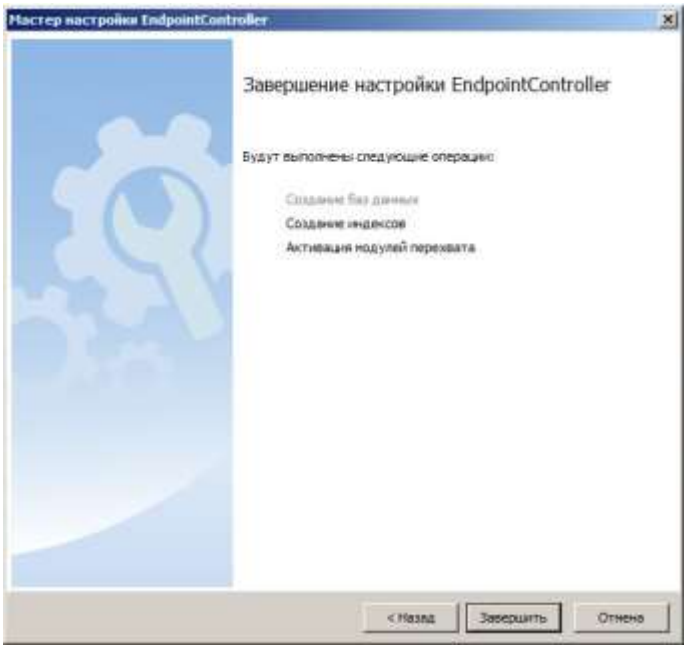


Рисунок 6.168

Индекс с соответствующими настройками будет создан.

6.5.2 Пуск сервера EndpointController

Серверный модуль запускается нажатием кнопки «Запустить перехват на агентах» на консоли администрирования (см. Рисунок 6.169). Нажатие данной кнопки включает службы Серчинформ EndpointController.

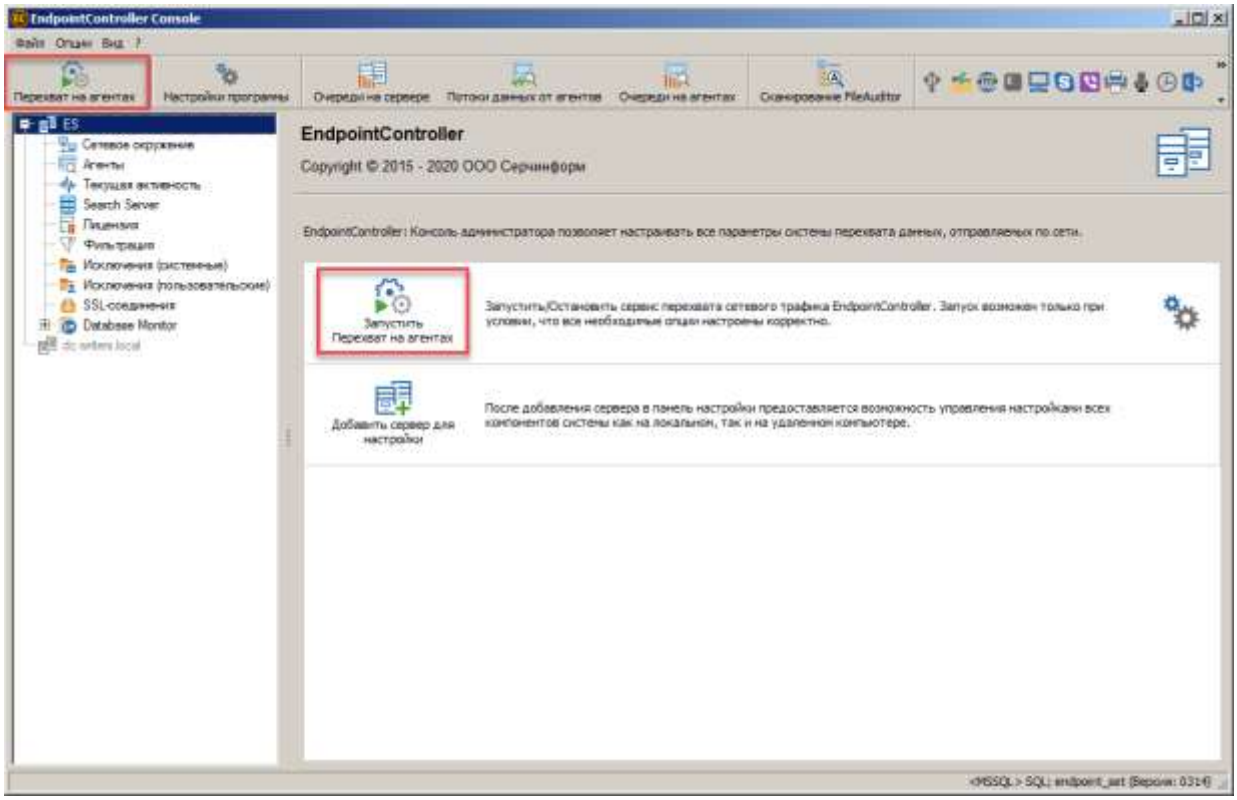


Рисунок 6.169

Для остановки службы используйте повторное нажатие кнопки (см. Рисунок 6.170).

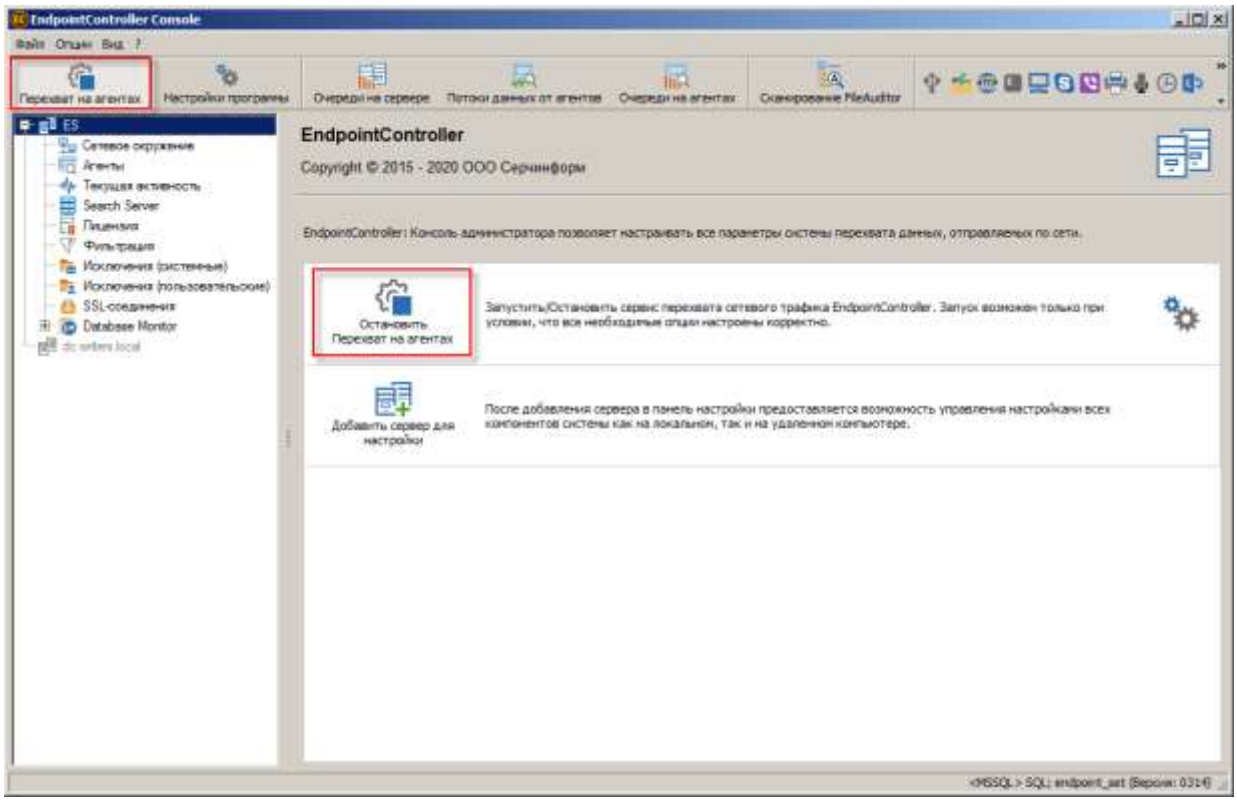


Рисунок 6.170

Окно настроек службы перехвата на агентах осуществляется в корневом узле нажатием кнопки  .

Настройки позволяют отрегулировать параметры службы EndpointController без обращения к оснастке «Службы»:

- тип запуска службы перехвата на агентах;
- учетную запись, под которой работает служба (см. Рисунок 6.171).

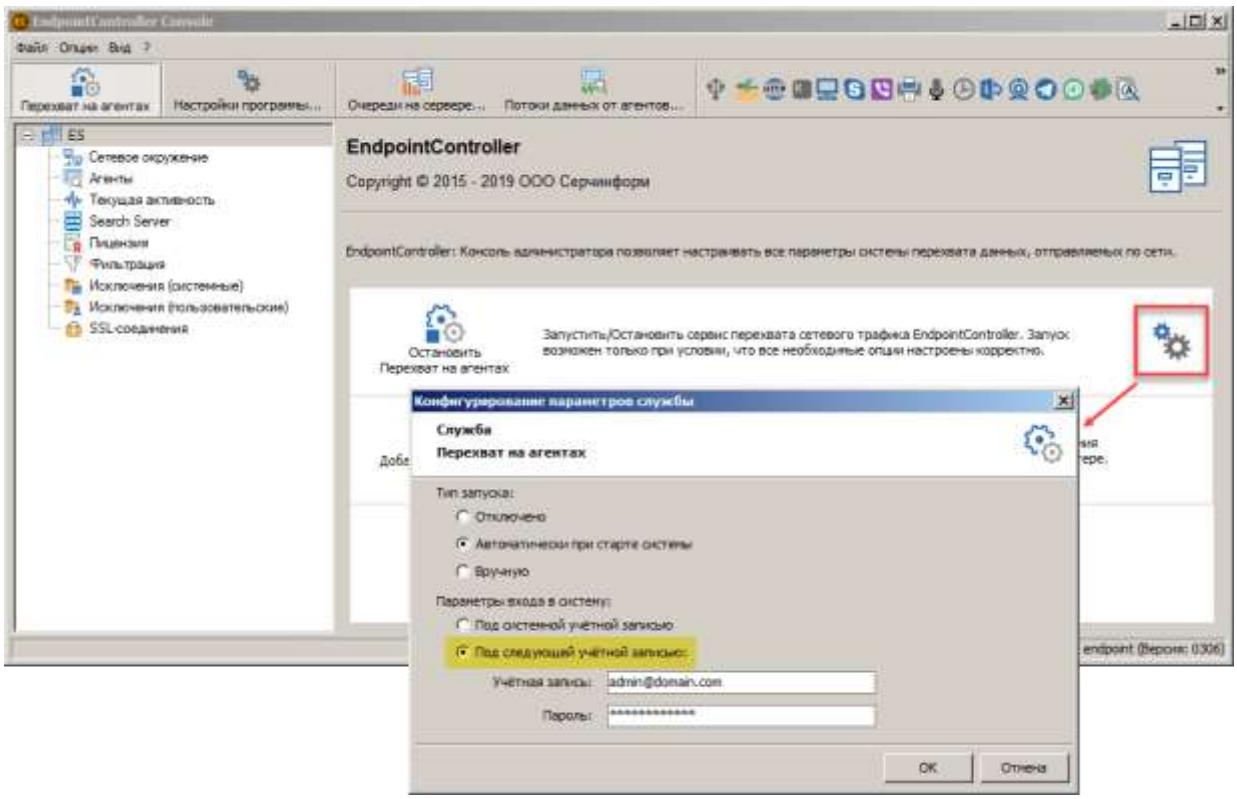


Рисунок 6.171

С настройками по умолчанию фильтрация данных не производится и в базу данных/хранилище записываются все перехваченные данные.

6.5.3 Работа с агентами

Агенты EndpointController устанавливаются на целевые компьютеры. В зависимости от того, какие типы данных агенты должны перехватывать, с помощью консоли EndpointController настраиваются модули перехвата данных, выбор которых производился на этапе установки компонентов сервера EndpointController.

Общая схема того, на какие целевые компьютеры устанавливаются агенты в привязке к модулям перехвата, приведено в Таблица 32.

Таблица 32 – Агенты и точки их установки

Тип данных	Модуль перехвата	Протоколы	Куда устанавливать
Внешние устройства	DeviceController	Device	Рабочие станции пользователей

Тип данных	Модуль перехвата	Протоколы	Куда устанавливать
Файлы и операции с файлами, хранящимися на компьютерах пользователей, серверах, общих сетевых ресурсах	FileAuditor (включая модуль FileController)	FileAuditor Files	1. Рабочие станции пользователей (поддерживаются десктопные и серверные ОС). 2. На файл-сервер, если файл-сервер работает под управлением ОС Windows. Если файл-сервер работает не под управлением ОС Windows, на рабочие станции пользователей
FTP-трафик	FTPController	FTP	Рабочие станции пользователей
HTTP-трафик	HTTPController	HTTP	Рабочие станции пользователей
Облачные сервисы	Cloud & SharePoint	CLOUD	Рабочие станции пользователей
Трафик сервисов мгновенных сообщений	IMController	Gadu-Gadu, ICQ, MMP, XMPP, HTTP IM, WhatsApp, Lync, Viber, Telegram	Рабочие станции пользователей
Вводимые с клавиатуры данные	KeyLogger	KeyLogger	Рабочие станции пользователей
Снимки и видеозаписи происходящего за компьютером	CameraController	Camera	Рабочие станции пользователей
Сообщения эл. почты	MailController	SMTP, POP3, NNTP, IMAP, MAPI, Web mail	Рабочие станции пользователей
Речь сотрудников	MicrophoneController	Microphone	Рабочие станции пользователей
Содержимое экранов	MonitorController	Monitor	Рабочие станции пользователей
Печать	PrintController	Print	Рабочие станции пользователей либо сервер печати
Данные об активности приложений	ProgramController	Activity monitor	Рабочие станции пользователей
Skype	SkypeController	Skype	Рабочие станции пользователей

Тип данных	Модуль перехвата	Протоколы	Куда устанавливать
Документы, хранящиеся на рабочих станциях пользователей	Индексация рабочих станций	Индексация рабочих станций	Рабочие станции пользователей

При работе в терминальных сессиях по RDP-соединению агенты устанавливаются не на рабочие станции, а на терминальные серверы.

Подключение/отключение агентов производится на вкладке «Сетевое окружение» консоли администрирования.

Агенты EndpointController можно устанавливать на включенные в домен компьютеры следующими способами:

- с помощью консоли администрирования EndpointController;
- средствами групповых политик;
- вручную (если не удается установить первыми двумя способами).

6.5.3.1 Установка агентов через консоль администрирования EndpointController

Перед установкой агентов на рабочие станции пользователей брандмауэр Windows на сервере EndpointController должен быть выключен либо в нём должны быть прописаны исключения на работу программы EndpointController.

Также необходимо удостовериться, что в настройках EndpointController (*Настройки программы → Установка агентов → Новые агенты*) флажок «Запретить установку новых агентов» снят. В противном случае агенты не смогут быть установлены.

Для просмотра списка рабочих станций и управления агентами, выделите узел «Сетевое окружение». Данный узел используется в следующих случаях:

а) Для управления агентами на компьютерах, включенных в домен.

б) Для управления агентами на компьютерах рабочих групп. Компьютеры рабочих групп должны быть добавлены в список вручную. Подробное описание в п. 6.5.3.3.

Варианты установки агентов:

Способ 1. Установите флажки в колонке «Агент» для целевых рабочих станций. Выберите необходимые модули перехвата данных. Для подтверждения настроек щёлкните «Применить». При установке агентов убедитесь, что из раскрывающегося списка не выбран пункт «Только компьютеры с агентами».

В течение некоторого времени будет происходить установка агентов и модулей перехвата. Активированные модули перехвата маркируются иконкой ☑.

Способ 2.

Выделите целевую рабочую станцию или группу, выберите из контекстного меню команду:

- **Инсталлировать → Агент -** для установки флажка в столбце «Агент»;
- **Инсталлировать → IMController** (или другой модуль перехвата) - для отметки соответствующего модуля перехвата;
- **Инсталлировать → Все –** для установки всех модулей перехвата.

Для подтверждения настроек щёлкните «Применить» (см. Рисунок 6.172).

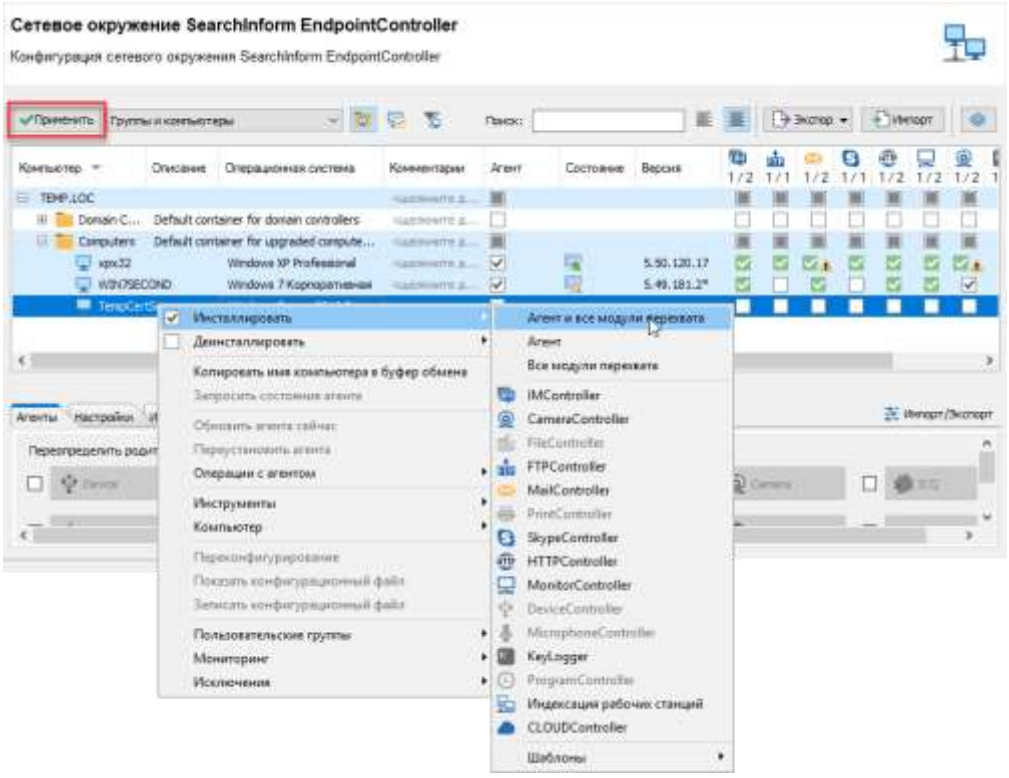


Рисунок 6.172

Иконка в столбце «Состояние» означает, что агент установлен и запущен (происходит перехват данных), иконка - установленный агент не запущен (перехват данных не происходит).

6.5.3.2 Установка агентов средствами групповых политик

Агенты EndpointController можно устанавливать средствами групповых политик. Для этого должен быть настроен сценарий принудительной установки агентов на рабочие станции пользователей.

Настройка политики агентов средствами групповых политик осуществляется на контроллере домена и производится однократно: настроенный контроллер домена больше не требует вмешательства. Позже необходимо лишь обновлять файлы инсталляционного пакета агента в сетевой папке.

Для установки агента средствами групповых политик EndpointController предоставляет возможность создания «установочного пакета», состоящего из:

- ESClient.exe;
- ESClientX64.exe;
- ESinstall.bat.

Используйте меню «Опции» → «Создание пакета для распространения агента через GPO...» для перехода к процедуре создания пакета (см. Рисунок 6.173).

Для работы опции необходимо, чтобы консоль администрирования была подключена к локальному серверу EC. При подключении консоли к удаленному серверу пункт меню «Создание пакета для распространения агента через GPO...» будет недоступен.

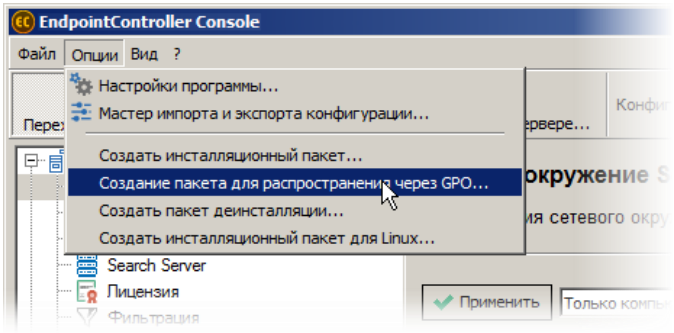


Рисунок 6.173

Открывшееся окно позволяет сформировать конфигурацию пакета для распространения с помощью групповых политик (см. Рисунок 6.174).

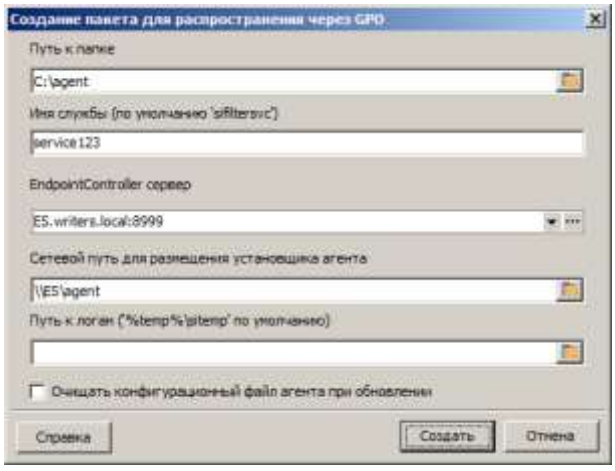


Рисунок 6.174

Задайте следующие параметры:

- В поле «Папка для сохранения» укажите или выберите каталог, куда будут сохранены файлы пакета.
- При необходимости задайте имя службы агента в одноимённом поле. Заданное имя службы должно совпадать с именем, указанным в настройках EndpointController. В противном случае агент будет автоматически

переустановлен с указанным в настройках именем. При пустом поле используется имя службы по умолчанию.

- Из выпадающего списка «EndpointController сервер» выберите необходимый сервер для установки агентом первоначального соединения и получения конфигурационного файла. Если необходимый сервер отсутствует в списке, добавьте его с помощью формы, вызываемой кнопкой ...
- В поле «Сетевой путь для размещения установщика агента» укажите или выберите сетевую папку, доступную с компьютеров, на которые будет производиться установка. Путь к установочным файлам не должен содержать кириллические символы и спецсимволы. В целях безопасности данная папка должна быть доступна с целевых компьютеров только для чтения.
- При необходимости измените путь к лог-файлам хода установки агента. Путь не должен содержать кириллические символы и спецсимволы.
- Установленный флаг «Оставлять конфигурационный файл при обновлении агента» позволяет оставить конфигурационный файл при обновлении, снятый - удалить.

По завершении всех настроек нажмите «Создать». Файлы будут сохранены в выбранной директории (см. Рисунок 6.175):

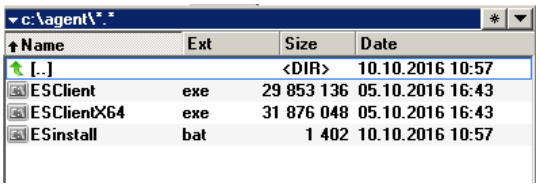


Рисунок 6.175

Поместите созданный пакет в сетевую папку, доступную с компьютеров, на которые будет производиться установка. Путь к установочным файлам не должен содержать кириллические символы. В целях безопасности данная сетевая папка должна быть доступна с целевых компьютеров только для чтения.

Создайте или измените политику принудительной установки агентов на контроллере домена соблюдая следующую последовательность действий:

1. Перейдите в оснастку «Active Directory - пользователи и компьютеры», создайте новое подразделение (Organization Unit) и переместите туда рабочие станции, на которые будет распространяться политика установки агентов (см. Рисунок 6.176).

Рисунок 6.176

2. Перейдите в оснастку «Управление групповой политикой» и привяжите новый объект групповой политики (ОГП) к созданному подразделению. Для этого щёлкните правой кнопкой мыши по подразделению и выберите команду «Создать ОГП в документе и связать его...». В поле «Имя» введите имя нового ОГП и нажмите кнопку «ОК» (см.Рисунок 6.177).

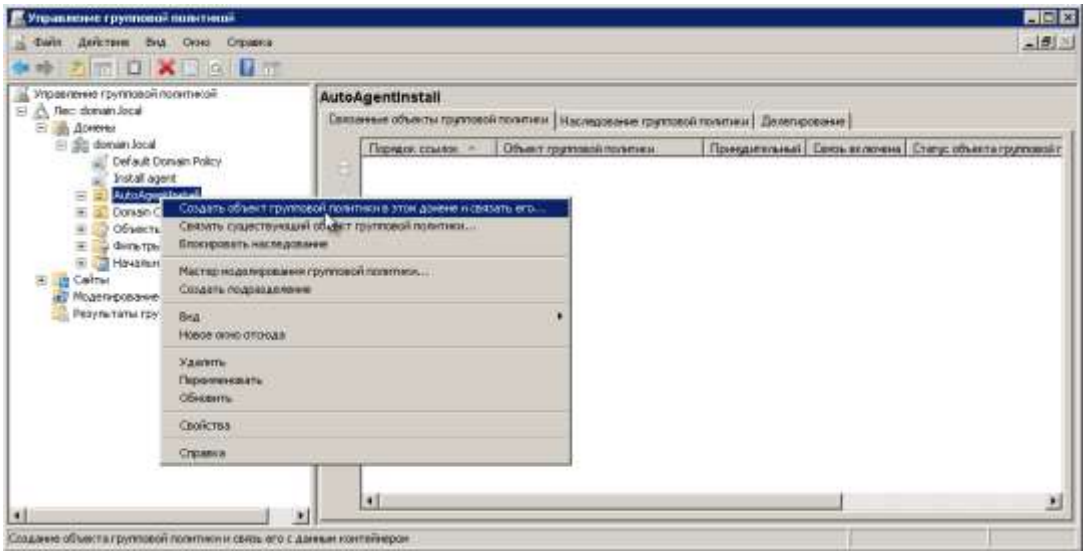


Рисунок 6.177

3. С помощью команды «Изменить» контекстного меню нового ОГП откройте оснастку «Редактор управления групповыми политиками» (см. Рисунок 6.178).

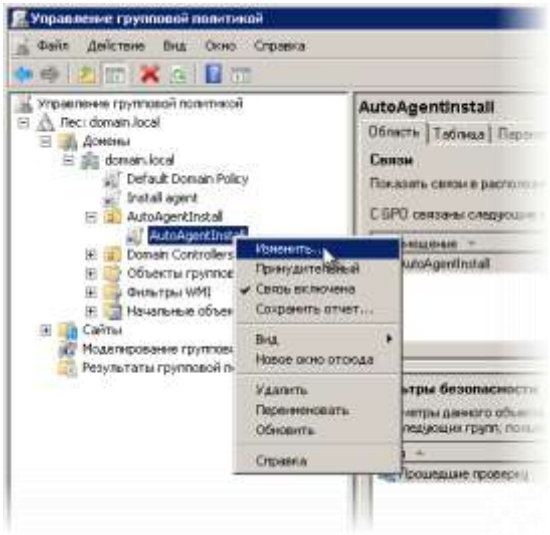


Рисунок 6.178

4. В оснастке «Редактор управления групповыми политиками» последовательно откройте «Конфигурация компьютера | Политики | Конфигурация Windows | Сценарии (запуск/завершение)». Откройте окно свойств сценария «Автозагрузка» (см. Рисунок 6.179).

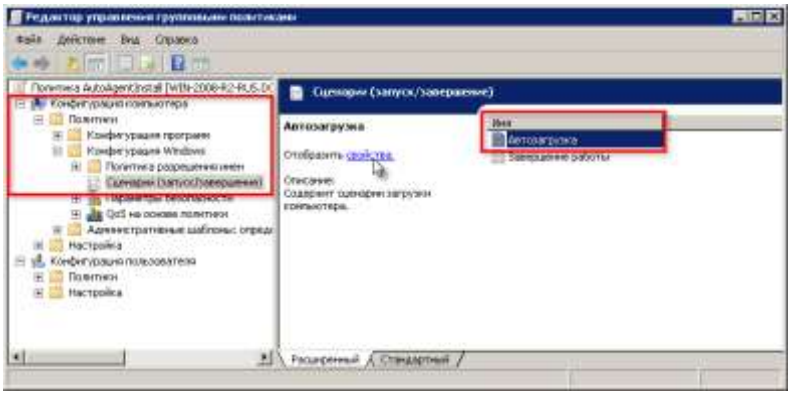


Рисунок 6.179

5. Щелкните кнопку «Добавить» (см.Рисунок 6.180).

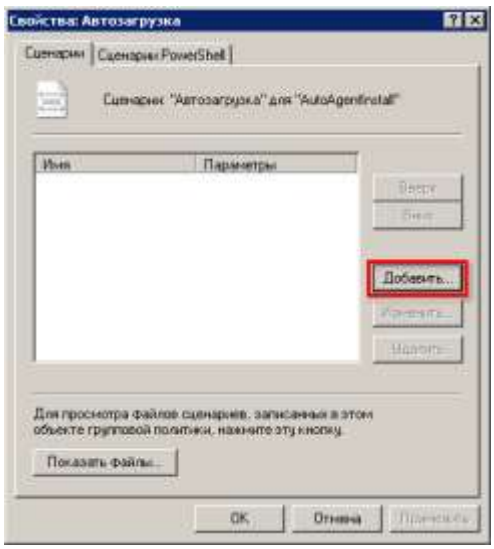


Рисунок 6.180

6. В поле «Имя сценария» укажите путь к файлу ESinstall.bat, расположенному в сетевой папке. Щёлкните «ОК», а затем подтвердите изменения в окне свойств сценария (см. Рисунок 6.181).

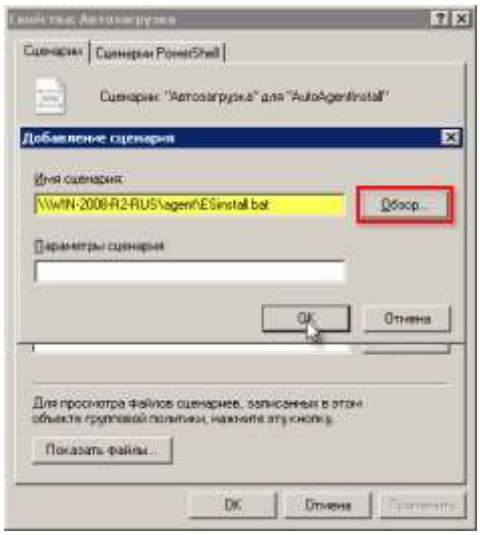


Рисунок 6.181

В целях отладки можно указать путь для сохранения лог-файла, содержащего ход выполнения сценария. Путь прописывается в параметрах сценария в следующем виде: **> path_to_log\file_name.log**. *Например, > %temp%\inst.log*.

7. Обновите политики. Для этого выполните команду **gpupdate /force** (см. Рисунок 6.182, Рисунок 6.183).

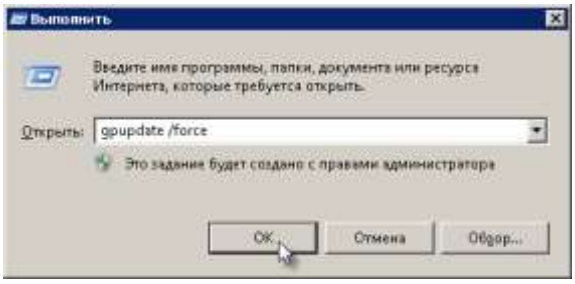


Рисунок 6.182

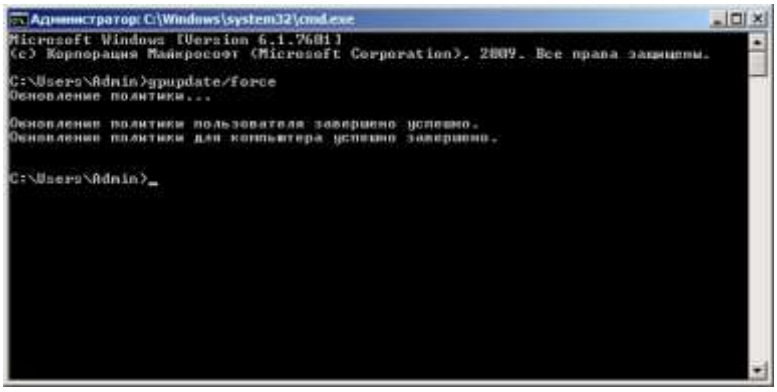


Рисунок 6.183

8. При перезагрузке целевого компьютера будет запущен скрипт установки агента. Для полноценной работы агента, после его установки требуется ещё одна перезагрузка целевой рабочей станции.

6.5.3.3 Установка агентов на компьютеры рабочих групп

Для установки агентов на компьютеры рабочих групп должны быть созданы следующие условия: учётная запись, под которой работает сервер EndpointController (имя и пароль пользователя), должна иметь права локального администратора на компьютерах рабочей группы, на которые планируется установка агентов EndpointController.

Установка производится в следующем порядке:

1) На каждом из целевых компьютеров рабочих групп создается учетная запись с правами локального администратора.
2) Создается список компьютеров рабочей группы, на которые устанавливаются агенты EndpointController.
3) Служба обработки данных (SIAMControlSvc.exe) перезапускается под созданной локальной учётной записью.
4) Список рабочих станций добавляется в консоль администрирования EndpointController.
5) Производится установка агентов.

Установка агентов на компьютеры рабочих групп производится под локальной учётной записью. Поэтому невозможно одновременное управление (установка,

удаление, обновление) агентами, установленными на компьютеры домена и рабочих групп.

6.5.3.3.1 Настройка локальных учётных записей

На сервере EndpointController и целевых компьютерах рабочей группы нужно создать одинаковые учётные записи с правами локального администратора, одним именем и паролем. Дополнительно к этому, учетная запись, созданная на сервере EndpointController должна иметь право входа в качестве службы (см. 6.5.3.3.2).

Откройте оснастку «Управление компьютером» и перейдите по пути «Служебные программы | Локальные пользователи | Пользователи». Воспользуйтесь меню «Действие | Новый пользователь» или выберите команду «Новый пользователь» в контекстном меню (см. Рисунок 6.184).

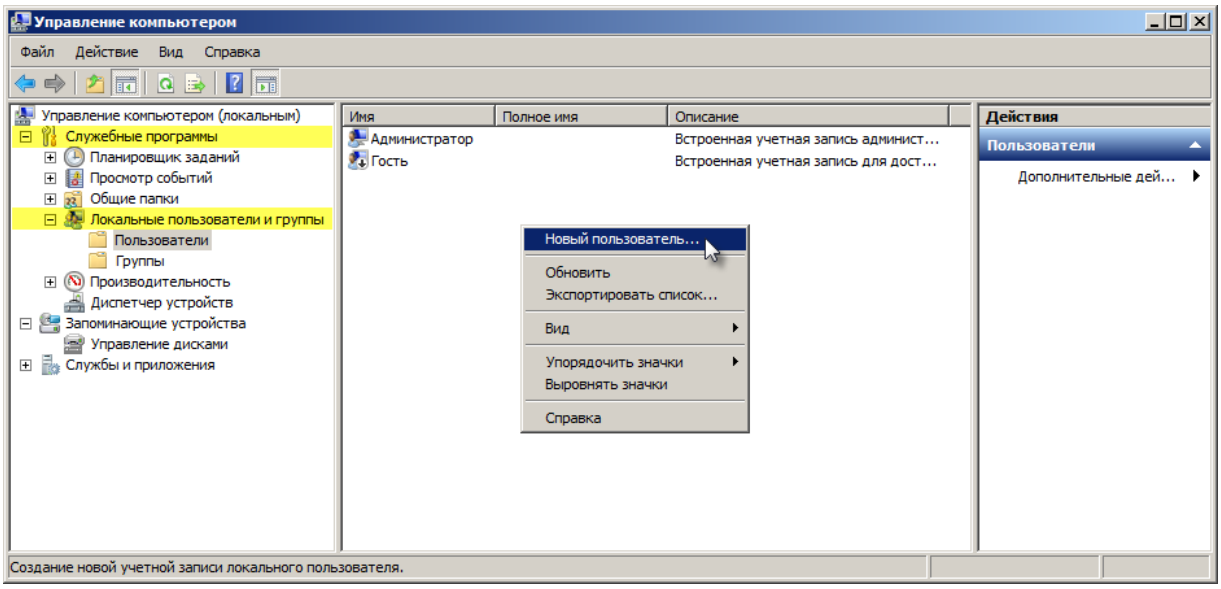


Рисунок 6.184

Для создания новой локальной учётной записи, введите имя пользователя, пароль и щёлкните кнопку «Создать» (см. Рисунок 6.185).

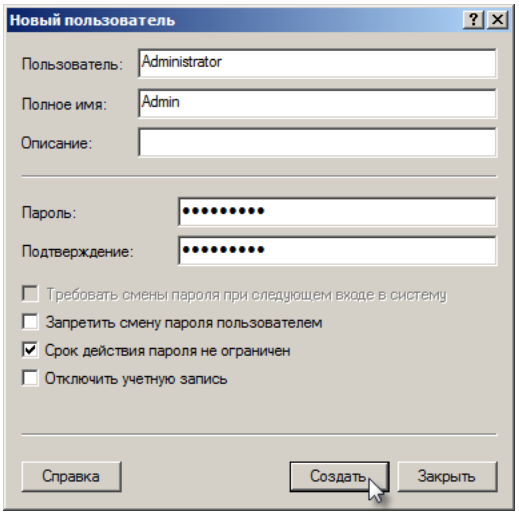


Рисунок 6.185

Перейдите в папку «Служебные программы | Локальные пользователи | Группы» и откройте свойства группы «Администраторы» (см. Рисунок 6.186).

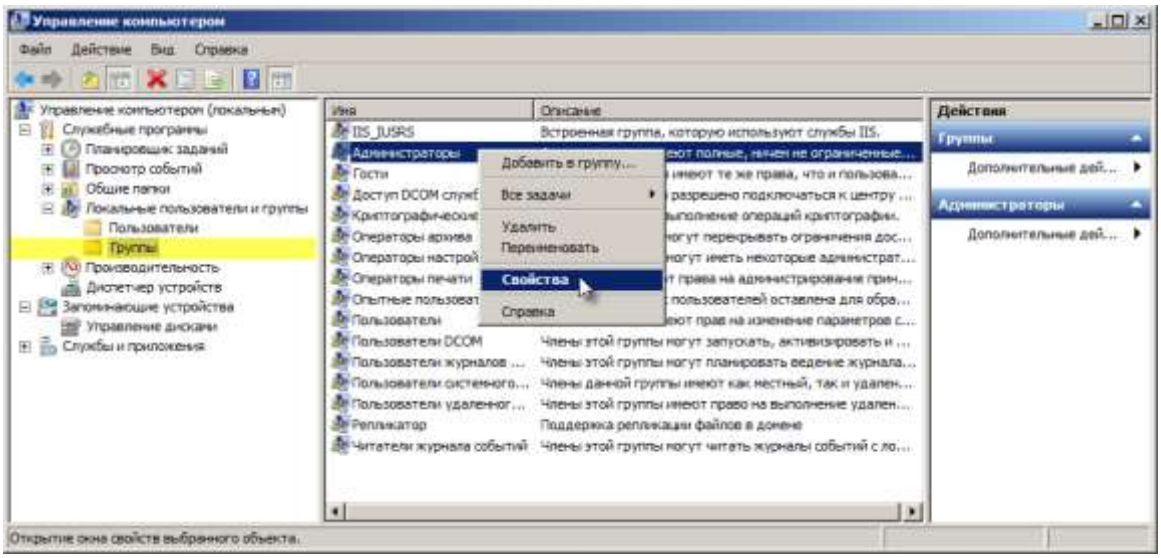


Рисунок 6.186

Добавьте созданного пользователя в список членов группы (см. Рисунок 6.187).

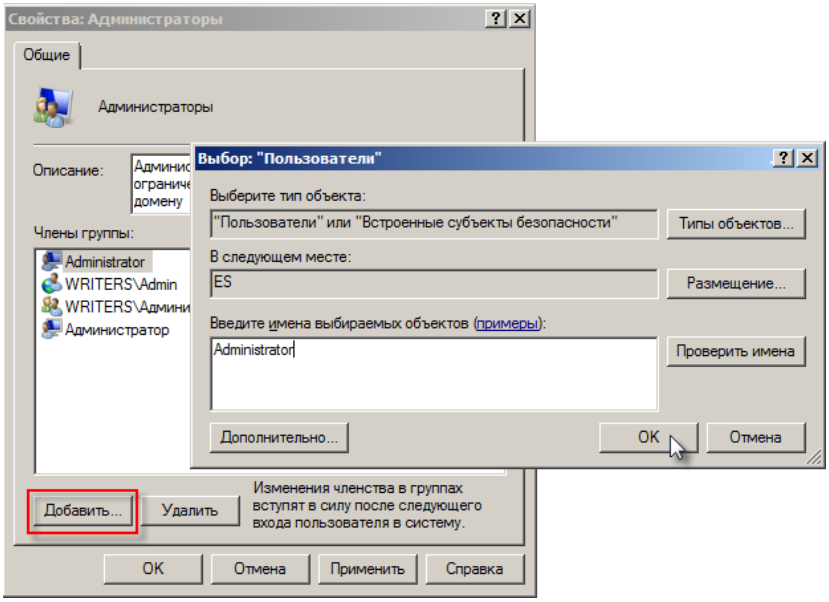


Рисунок 6.187

Данную операцию нужно повторить для остальных компьютеров рабочей группы, на которые планируется установить агенты.

6.5.3.3.2Настройка прав входа в качестве службы

Служба SearchInform EndpointController Agents Control должна работать под созданной учетной записью. Это значит, что созданная на сервере EndpointController локальная учетная запись должна иметь право входа в качестве службы.

Сочетанием клавиш Win+R вызовите окно «Выполнить», выполните команду secpol.msc. Будет открыта оснастка «Локальные политики безопасности».

Откройте свойства политики «Локальные политики | Назначение прав пользователя | Вход в качестве службы» (см. Рисунок 6.188).

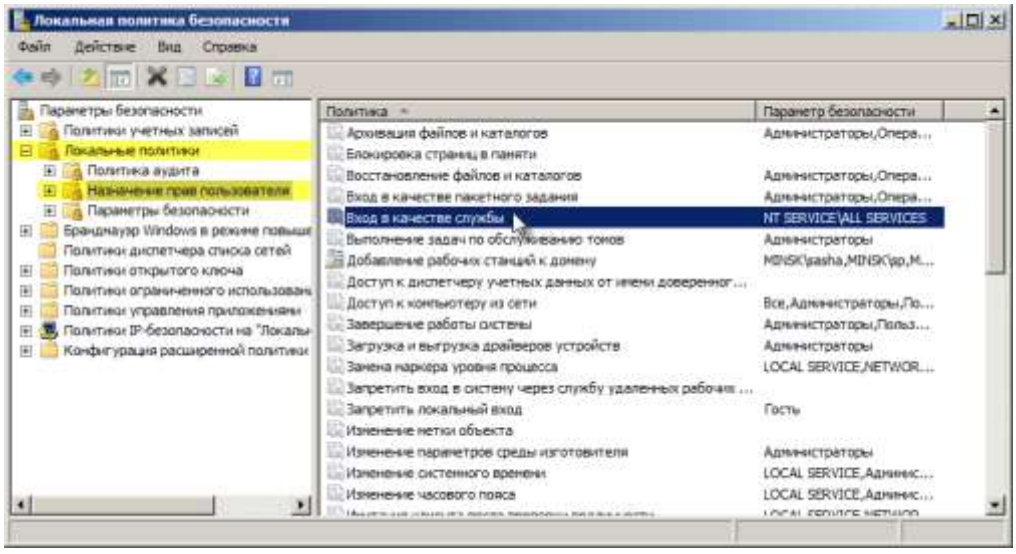


Рисунок 6.188

Добавьте созданного пользователя в политику и примените изменения (см. Рисунок 6.189).

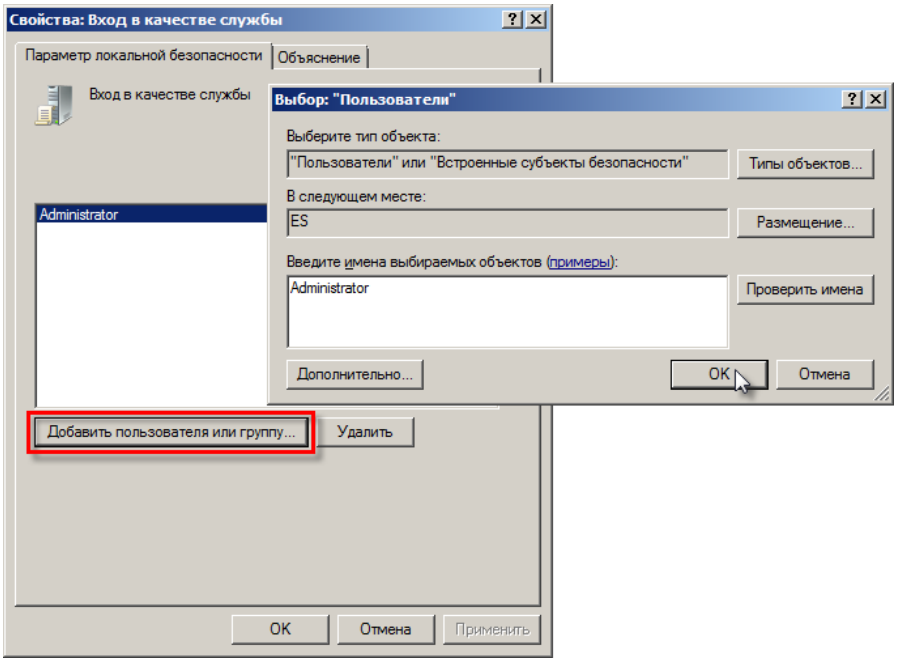


Рисунок 6.189

6.5.3.3.3Перезапуск службы

В большинстве случаев, служба SearchInform EndpointController Agents Control работает под доменной учетной записью. Для установки агентов на компьютеры рабочей группы, служба должна работать под ранее созданной учётной записью с правами локального администратора (см. 6.5.3.3.1). Данная учётная запись должна иметь право входа в качестве службы на сервере EndpointController.

Сочетанием клавиш Win+R вызовите окно «Выполнить», выполните команду services.msc. Будет открыта оснастка «Службы», отображающая список служб и их статус. Откройте свойства службы SearchInform EndpointController Agents Control на вкладке «Вход в систему» (см. Рисунок 6.190).

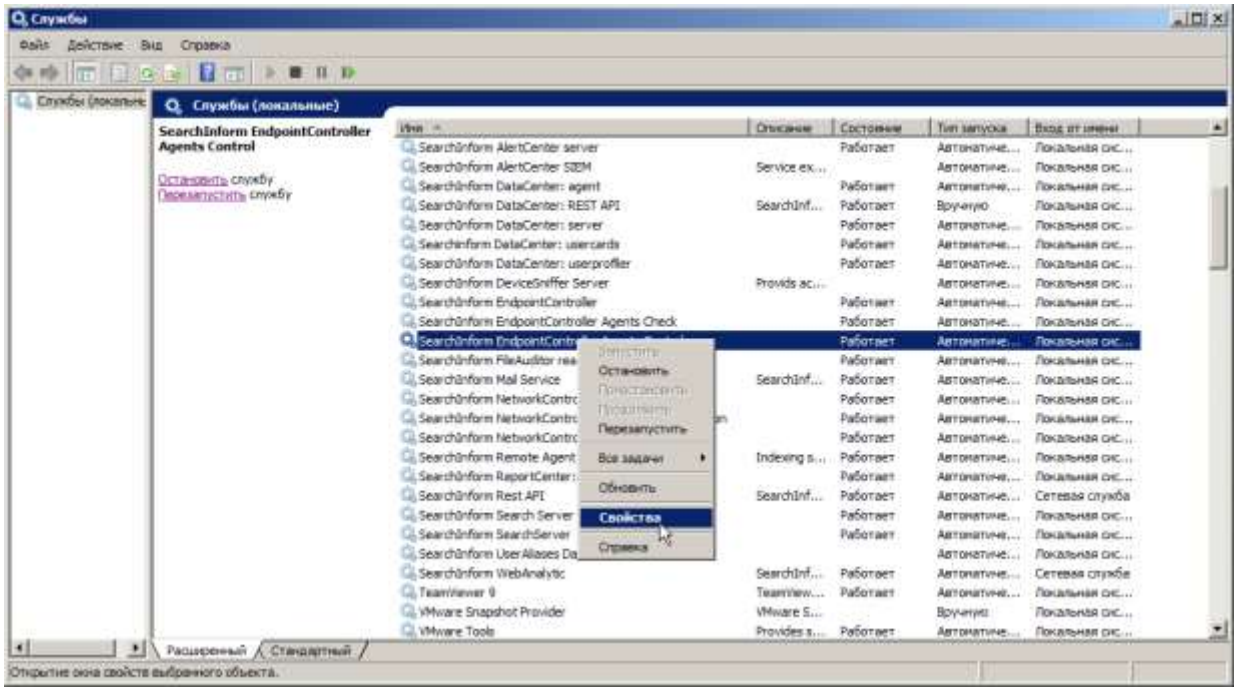


Рисунок 6.190

Выберите тип входа «С учетной записью», введите имя и пароль созданного локального пользователя (см.Рисунок 6.191).

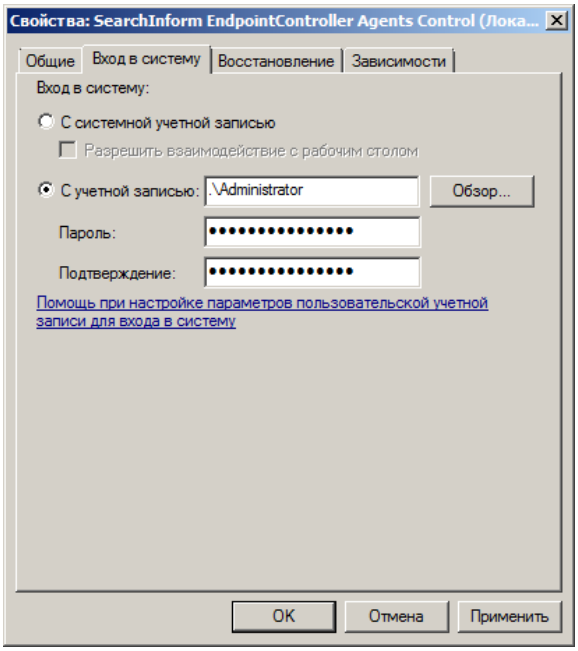


Рисунок 6.191

После этого, перезапустите службу SearchInform EndpointController Agents Control.

В случае невозможности переопределения учетной записи для службы управления агентами, в консоли EndpointController необходимо задать имя и пароль

созданного локального пользователя в свойствах подключения к каждой группе/компьютеру (см. Рисунок 6.192).

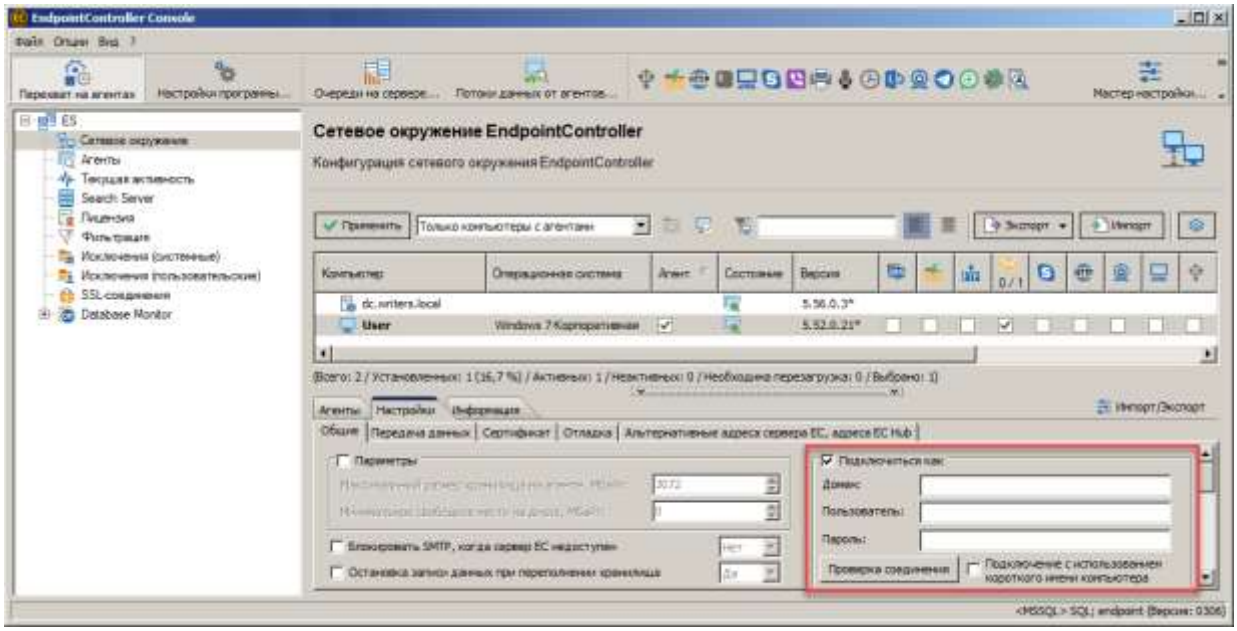
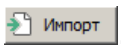


Рисунок 6.192

6.5.3.3.4Добавление списка рабочих станций и установка агентов

На вкладке «Сетевое окружение» щелкните кнопку 

.

Рабочие станции могут быть добавлены в список несколькими способами:

- Отметка флажками требуемых компьютеров и перенос в правую часть нажатием кнопки  ;
- Ввод вручную имен компьютеров в окне, вызываемом кнопкой  ;
- Добавление компьютеров из указанного файла.

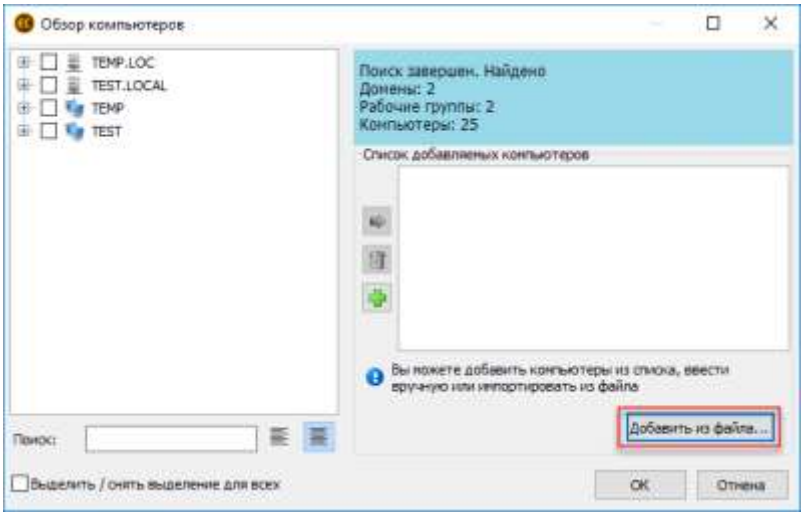


Рисунок 6.193

Введите имя группы, в которую будут добавлены компьютеры и щёлкните «ОК». (см. Рисунок 6.194).

Рисунок 6.194

Группа рабочих станций будет добавлена и отображена в окне просмотра (см. Рисунок 6.195).

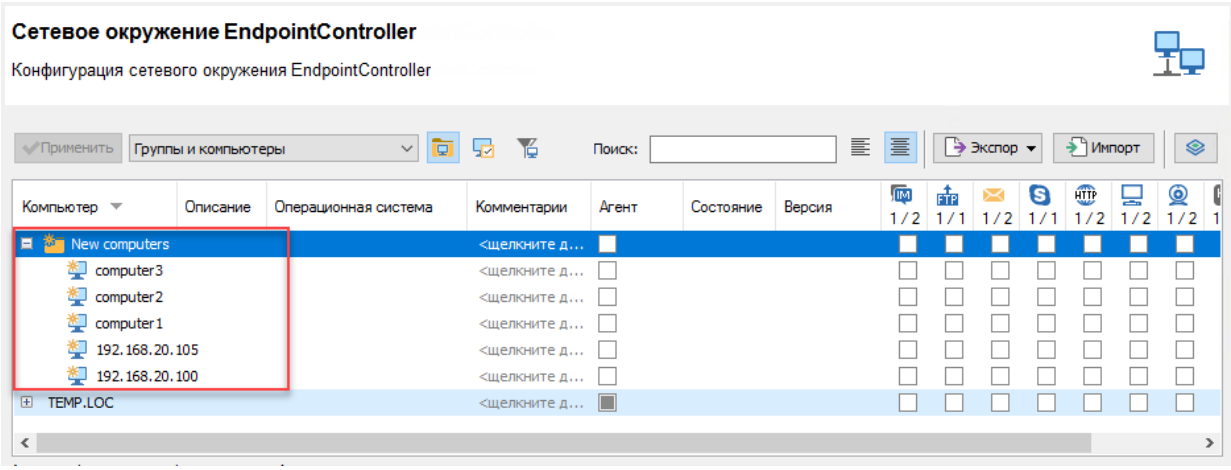


Рисунок 6.195

Установите агенты и модули перехвата на целевые компьютеры с помощью консоли EndpointController (см. 6.5.3.1).

После установки отобразится список установленных агентов и протоколов, сгруппированных по модулям перехвата (см. Рисунок 6.195). Установка может занять некоторое время (обычно в пределах нескольких минут). Время установки зависит от многих факторов, в том числе ширины канала, загруженности сети, мощности рабочей станции и сервера EndpointController, запущенных на рабочей станции приложений, установленных драйверов, наличия брандмауэров и т.д.

Если агентов не удалось установить с помощью консоли EndpointController, произведите установку вручную (см. 6.5.3.4).

6.5.3.4 Установка агентов вручную

Если агентов не удалось установить через консоль администрирования EndpointController или средствами групповых политик, произведите установку вручную.

Консоль EndpointController предоставляет возможность создания дистрибутива агента. Для этого воспользуйтесь командой «Создать инсталляционный пакет» в меню «Опции» (см. Рисунок 6.196).

Для работы опции необходимо, чтобы консоль администрирования была подключена к локальному серверу ЕС. При подключении консоли к удаленному серверу пункт меню «Создать инсталляционный пакет» будет недоступен.

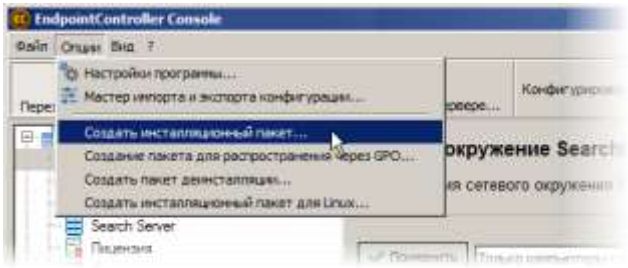


Рисунок 6.196

Выберите директорию для размещения создаваемых файлов (см. Рисунок 6.197).

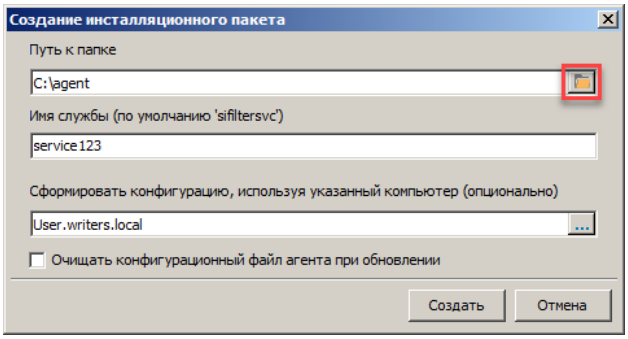


Рисунок 6.197

Задайте имя службы агента[25]. При пустом поле используется имя службы по умолчанию.

Установленный флаг «Очищать конфигурационный файл при обновлении агента» позволяет очистить конфигурационный файл при обновлении, снятый - оставить.

Параметр «Сформировать конфигурацию, используя указанный компьютер» позволяет создать дистрибутив агента с заданными настройками.

Выберите требуемый компьютер. Настройки 'нового' агента будут идентичны настройкам агента, установленного на выбранной рабочей станции (см. Рисунок 6.198).

[25] Заданное имя службы должно совпадать с именем, указанным в настройках EndpointController (**Настройки → Настройки агента → Маскировка агентов**). В противном случае агент будет автоматически переустановлен с указанным в настройках именем.

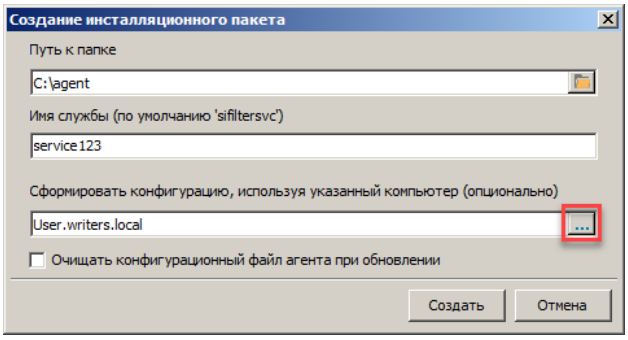


Рисунок 6.198

Отображаются только компьютеры с установленными агентами (см.Рисунок 6.199). По завершении всех настроек нажмите «ОК».

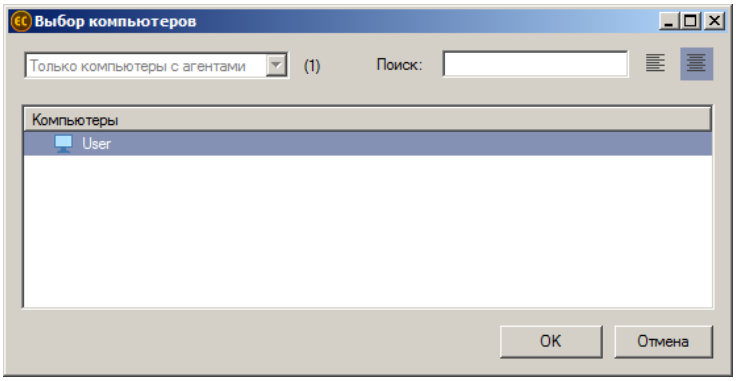


Рисунок 6.199

Инсталлятор будет сохранен в выбранной директории (см.Рисунок 6.200).

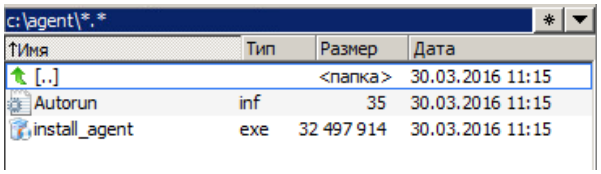


Рисунок 6.200

Скопируйте папку с файлами на целевую рабочую станцию. *Путь к установочным файлам не должен содержать кириллические символы!*

Запустите файл **install_agent.exe** на целевой рабочей станции. Запуск должен производиться пользователем с правами локального администратора (см.Рисунок 6.201).

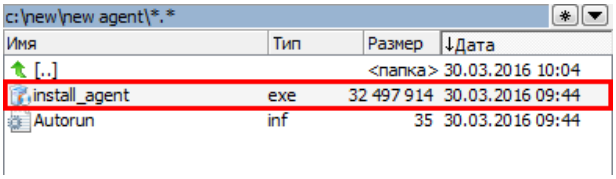


Рисунок 6.201

Ход установки записывается в файл **install.log**. Файл создается во временной папке операционной системы.

Установка может занять некоторое время. При успешной установке в логе будет записана информация вида «Установка завершена с состоянием: 0». В случае завершения установки с ошибкой – код ошибки (см.Рисунок 6.202).

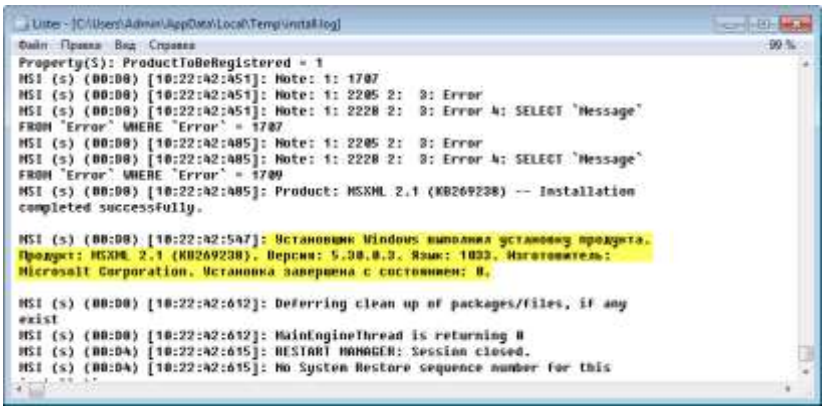


Рисунок 6.202

Если файл конфигурации агента не создавался, в консоли администрирования EndpointController напротив рабочей станции с установленным агентом отметьте флажками требуемые модули перехвата). Щелкните кнопку «Применить»(см. Рисунок 6.203).

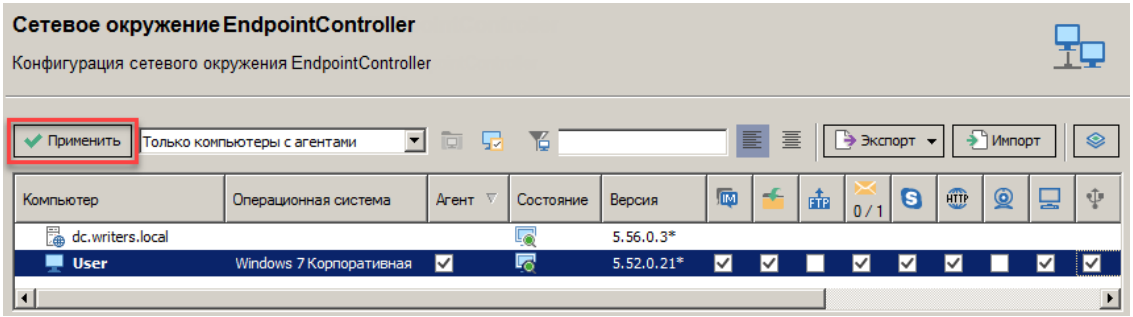


Рисунок 6.203

После установки агента перезагрузите целевую рабочую станцию.

Данный способ может быть применен для установки агентов как в домене, так и в рабочих группах.

6.5.3.4.1Установка агентов на Linux

EndpointController предоставляет возможность создания дистрибутива агента для установки на рабочие станции под управлением ОС семейства Linux. Перечень ОС Linux, на которые могут быть установлены агенты EndpointController, приведен в Таблица 4.

В текущей версии EndpointController агенты на поддерживаемых сборках ОС Linux не работают в «скрытом» режиме, следовательно, агент можно удалить, используя стандартные утилиты ОС.

Агент на базе Linux обеспечивает контроль следующих протоколов:

- HTTP/HTTPS;
- SMTP, POP3, IMAP, Web mail;
- IM (XMPP, HTTPIM);
- FTP;
- Cloud;
- Device[26].

6.5.3.4.1.1 Подготовка сервера EndpointController

1. Убедитесь, что между сервером EndpointController и рабочей станцией, на которую будет устанавливаться агент, есть прямое соединение, порт открыт и доступен.
2. Произведите настройки в окне «Настройки программы»:
   - В настройках консоли сервера укажите альтернативный IP-адрес сервера.
   - В «Настройках агента и хранилища» установите минимальное свободное место на диске, равное 0.
   - Для группы «Нераспознанные» установите значение «Принять данные».
   - На вкладке «Синхронизация» указан доступный сервер DataCenter, который также раздает лицензии модулям перехвата.

6.5.3.4.1.2 Создание инсталляционного пакета

Используйте меню «Опции» → «Создать инсталляционный пакет для Linux...» для перехода к процедуре создания (см. Рисунок 6.204).

Для работы опции необходимо, чтобы консоль администрирования была подключена к локальному серверу EC. При подключении консоли к удаленному серверу пункт меню «Создать инсталляционный пакет» будет недоступен.

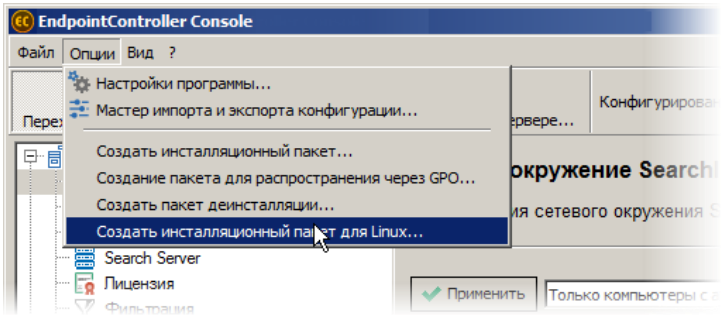


Рисунок 6.204

Укажите папку, в которую будут сохранены файлы.

[26] Только для Ubuntu 16.04, 17.04, 18.04 и CentOS 7.6.

Выберите версию сборки Linux, на которую будет устанавливаться агент, и ее разрядность.

Отметьте флажком инсталлятор агента в выбранной директории. Для Ubuntu доступен к выбору также модуль DeviceController, формируемый отдельным инсталлятором (при выборе учитывайте версию ядра ОС) (см. Рисунок 6.205).

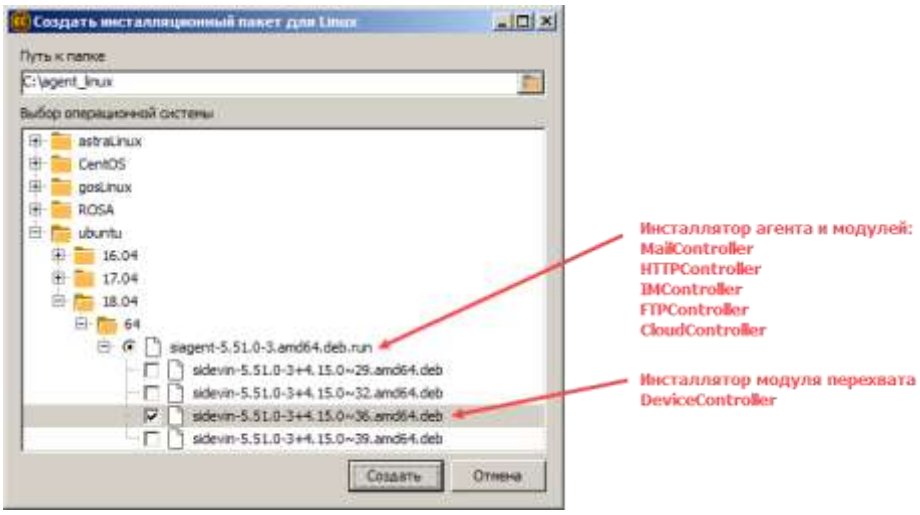


Рисунок 6.205

По завершении всех настроек нажмите «Создать».

Инсталлятор агента будет сохранен в указанной директории в виде пакета **siagent-5.31.198-x.x.deb.run**. В случае установки с модулем перехвата DeviceController дополнительно создается файл **sidevin-5.31.198-x.x.deb** (см. Рисунок 6.206).

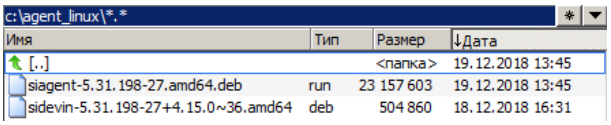


Рисунок 6.206

6.5.3.4.1.3 Установка агента на рабочую станцию

Для удобства работы в терминале рекомендуется предварительно установить утилиты mount.cifs и mc:

- ***sudo apt install mc***
- ***sudo apt install cifs.utils***

1. Перенесите дистрибутив(ы) на машину средствами Linux или используя внешний носитель.

2. Перейдите в каталог с дистрибутивом и установите пакет агента командой (в зависимости от выбранной ОС, расширение пакета может отличаться):

sudo ./siagent-5.31.198-x.x.deb.run (см. Рисунок 6.207).

Для установки модуля перехвата DeviceController используйте команду:

sudo dpkg -i sidevin-5.31.198-x.x.deb.

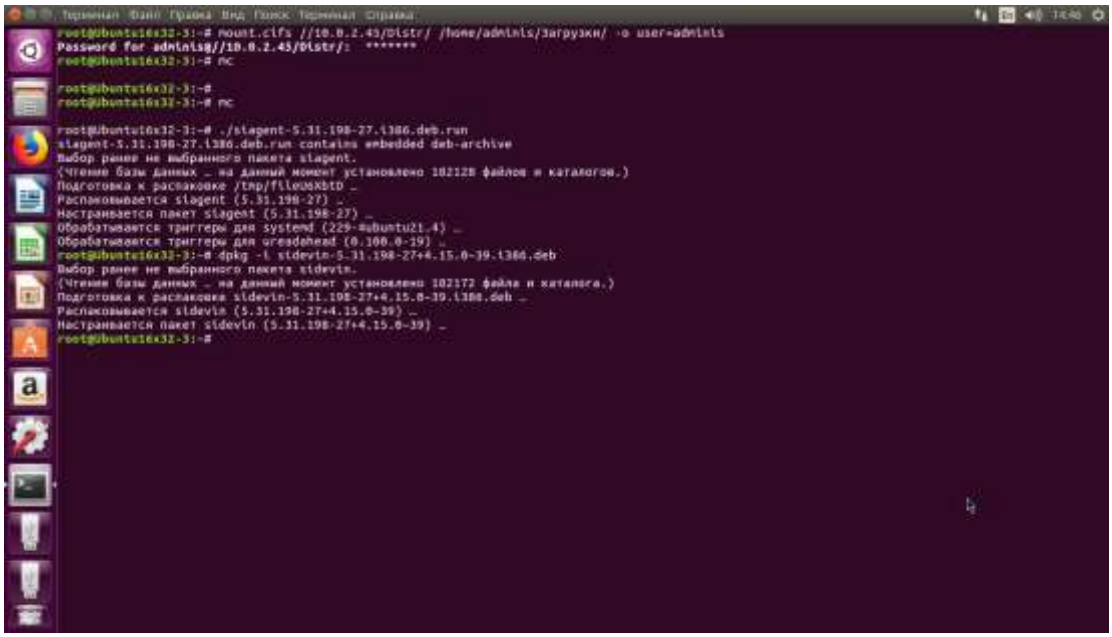


Рисунок 6.207

3. Перезагрузите рабочую станцию.

4. Проверьте статус службы командой **sudo service si status**. Если служба остановлена, запустите ее командой **sudo service si start** (см. Рисунок 6.208).

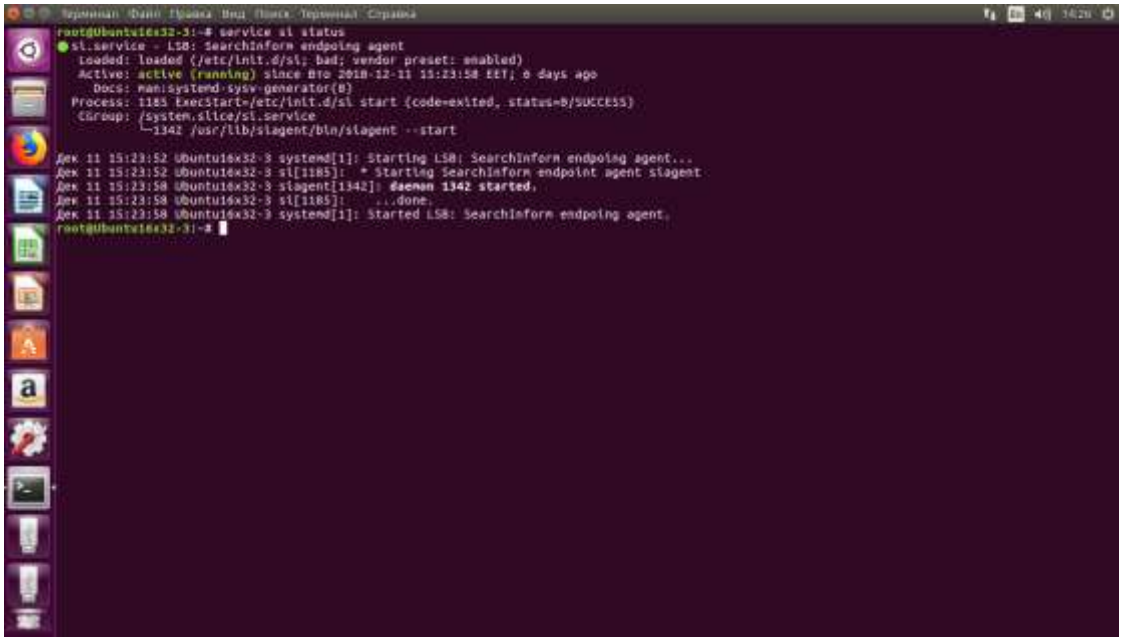


Рисунок 6.208

5. Дождитесь появления рабочей станции с агентом на вкладке «Сетевое окружение» консоли EndpointController.

6. Отметьте флажками требуемые модули перехвата и нажмите кнопку «Применить» (см. Рисунок 6.209).

- В случае установки пакета **siagent-5.31.198-x.x.deb.run** могут быть отмечены модули перехвата HTTPController, MailController, IMController, FTPController, CloudController.
- В случае установки пакета **sidevin-5.31.198-x.x.deb** может быть дополнительно активирован модуль перехвата DeviceController.

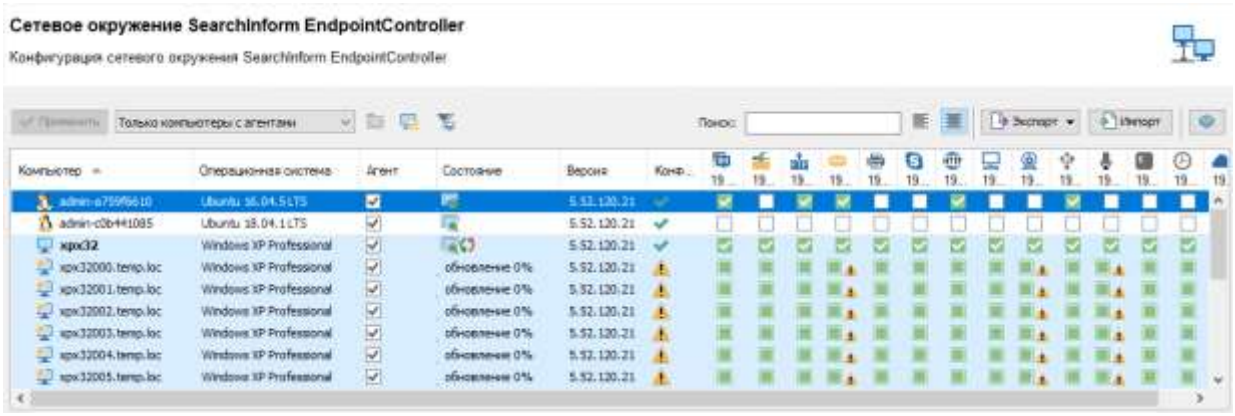


Рисунок 6.209

7. Дождитесь, пока агент получит конфигурацию.

6.5.3.4.1.4 Удаление агента на Linux

1. На рабочей станции с агентом Linux введите команду:

- для Ubuntu: sudo apt remove --purge siagent;
- для CentOS: sudo yum remove siagent;
- для других ОС на базе Linux последовательно введите команды (см. Рисунок 6.210):

  sudo service si stop

  sudo update-rc.d –f si remove

  sudo service si remove

  sudo dpkg -r sidevin

  sudo dpkg -r siagent

  sudo rm -fr /var/siagent/

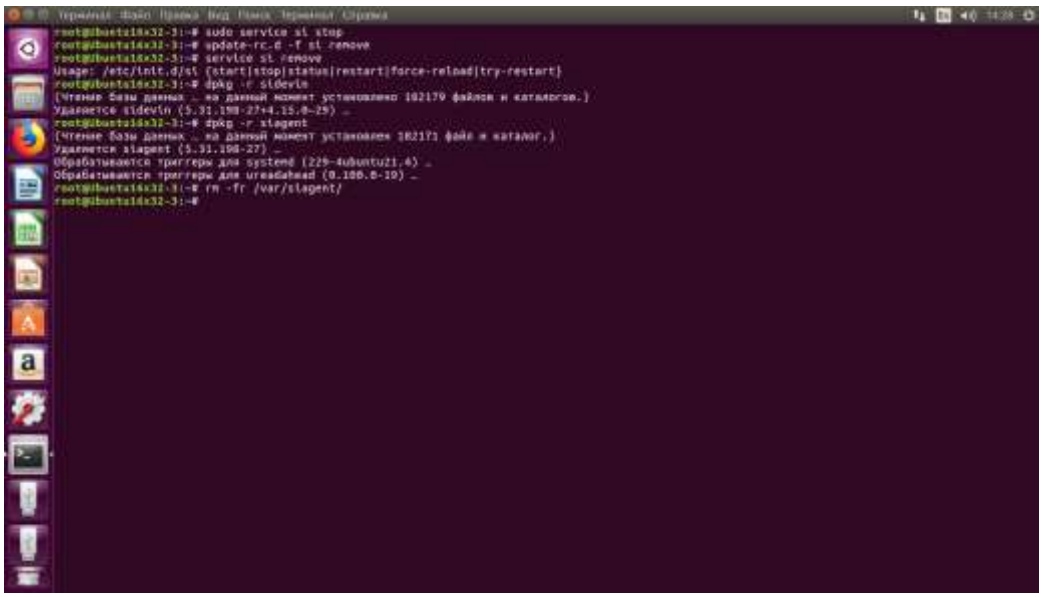


Рисунок 6.210

2. В консоли EndpointController на вкладке «Сетевое окружение» выберите рабочую станцию на базе Linux, с которой был удален агент. Вызовите контекстное меню и выберите команду «Удалить». Подтвердите удаление рабочей станции (см. Рисунок 6.211).

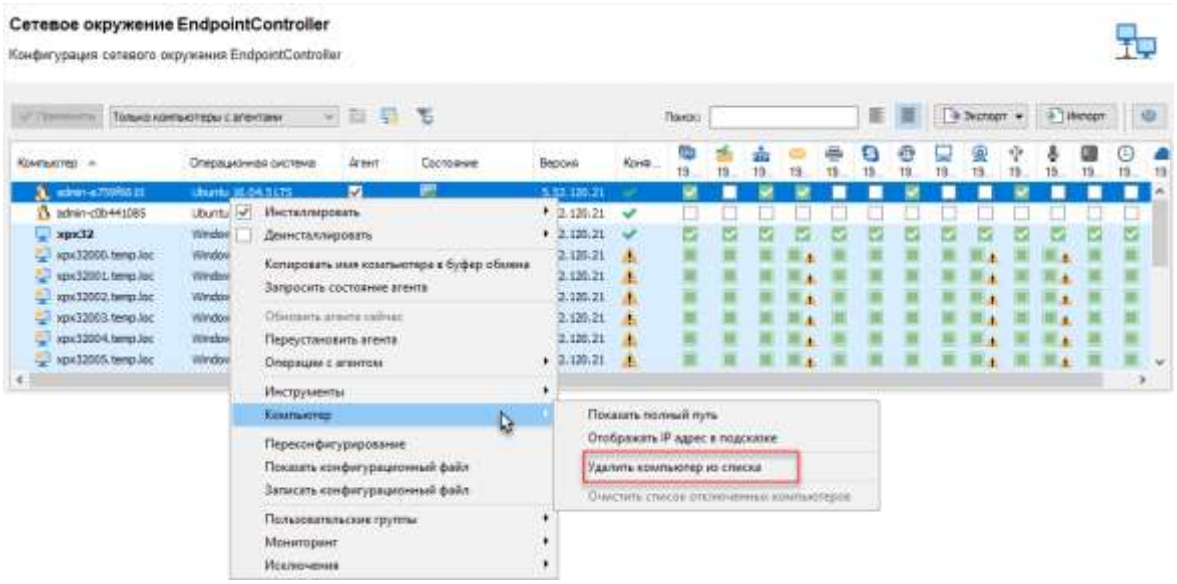


Рисунок 6.211

6.5.3.5 Удаление агентов и отключение модулей перехвата

Удалите флажок ☑ в колонке «Агенты» или воспользуйтесь командой «Деинсталлировать» из контекстного меню (см. Рисунок 6.212), после чего подтвердите удаление, щелкнув по кнопке «Применить».

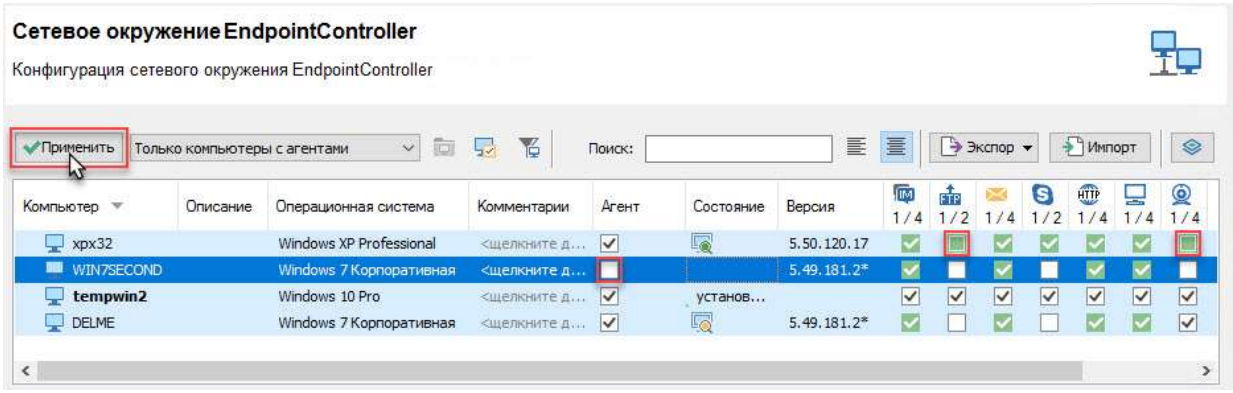


Рисунок 6.212

Также агентов можно удалить вручную при помощи созданного пакета деинсталляции.

Для отключения агентов на отдельных модулях перехвата удалите флажки ☑ в соответствующих колонках модулей перехвата[27], после чего щелкните кнопку «Применить».

6.5.3.1 Обновление агентов

Для обновления агента удалите существующий агент с рабочей станции, а затем - установите новый в соответствии с п. 6.5.3.4.1.2 – 6.5.3.4.1.3.

6.5.4 Особенности настройки фильтрации

Под фильтрацией трафика понимается ограничение перехвата документов по их атрибутам: пользователю домена, IP-адресу, MAC-адресу и другим.

Фильтрация используется в случаях, когда агенты действуют как на PC, которые необходимо подвергать мониторингу, так и на PC, которые нужно исключить из мониторинга. Если функционал фильтрации включен, но список фильтров пуст, перехват будет осуществляться без ограничений.

Предусмотрена возможность использования как запрещающих, так и разрешающих фильтров.

- При использовании запрещающих фильтров в базу данных будут передаваться все перехваченные пакеты, за исключением совпадений по фильтрам. Должна быть выбрана опция «Исключить из перехвата трафика указанные в фильтрах значения».
- При использовании разрешающих фильтров в базу данных будут переданы все перехваченные пакеты, совпадающие с фильтрами. Должна быть выбрана опция «Включить в перехват трафика указанные в фильтрах значения».

На вкладке «Глобальные фильтры» можно настроить фильтры для всех каналов передачи данных (см. Рисунок 6.213).

[27] Также можно воспользоваться командой «Деинсталлировать» из контекстного меню.

Для создания фильтров служат кнопки «Добавить» в блоках «Пользователи и группы», «IP-адрес», «MAC-адрес».

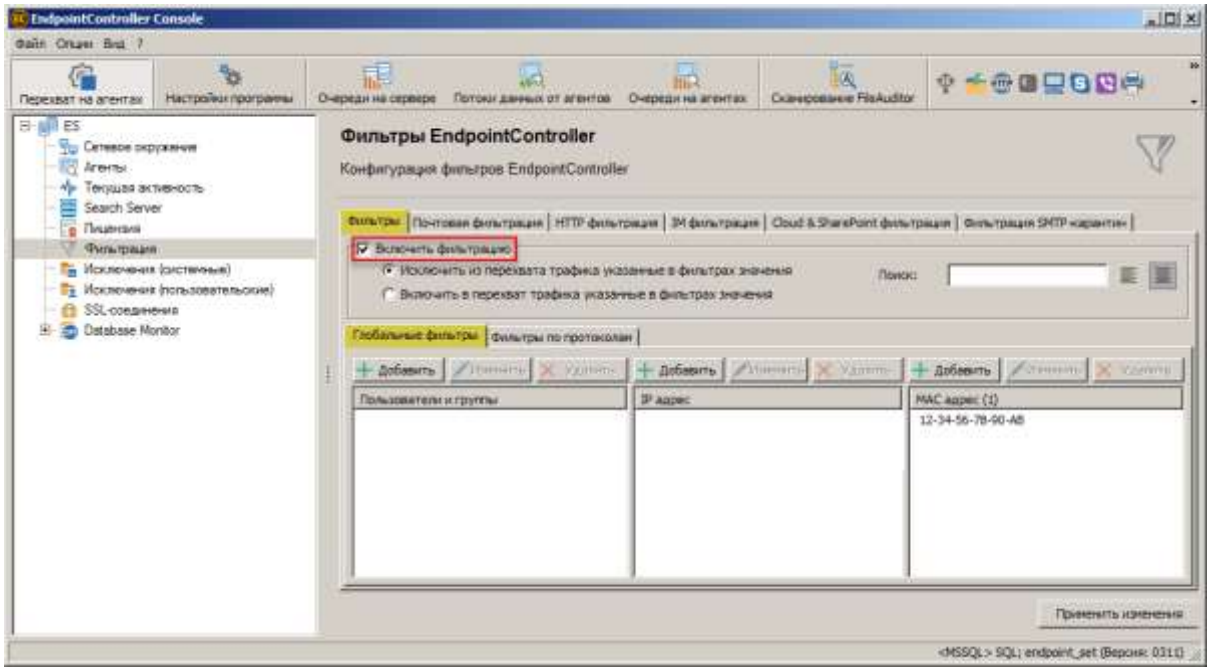


Рисунок 6.213

Добавьте необходимые фильтры. После этого они будут отображены в консоли EndpointController.

Для очистки списка фильтров используйте команду контекстного меню «Очистить». Действие распространяется только на тот столбец (Пользователи и группы/IP-адрес/MAC-адрес), из которого было вызвано контекстное меню (см. Рисунок 6.214).

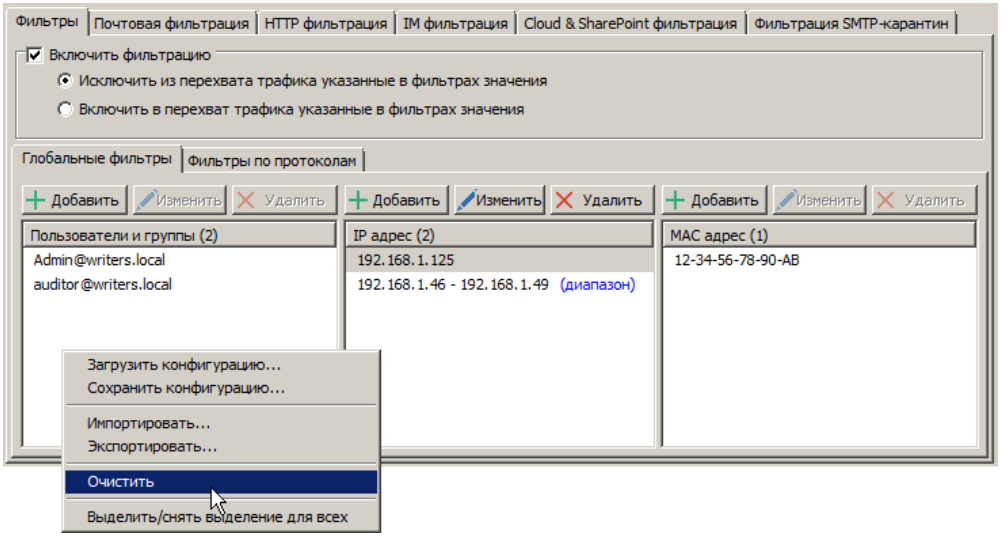


Рисунок 6.214

Примените изменения, нажав одноименную кнопку.

На вкладке «Фильтры по протоколам» настраиваются фильтры для отдельных протоколов передачи данных.

Для добавления фильтра выделите необходимый протокол и воспользуйтесь кнопкой «Добавить».

Добавленные фильтры будут отображены в консоли EndpointController. Наряду с фильтрами по протоколам в списке также отображаются глобальные фильтры - они маркируются полем с установленным флажком. Флажок может быть снят, в результате чего данный глобальный фильтр будет деактивирован (см. Рисунок 6.215).

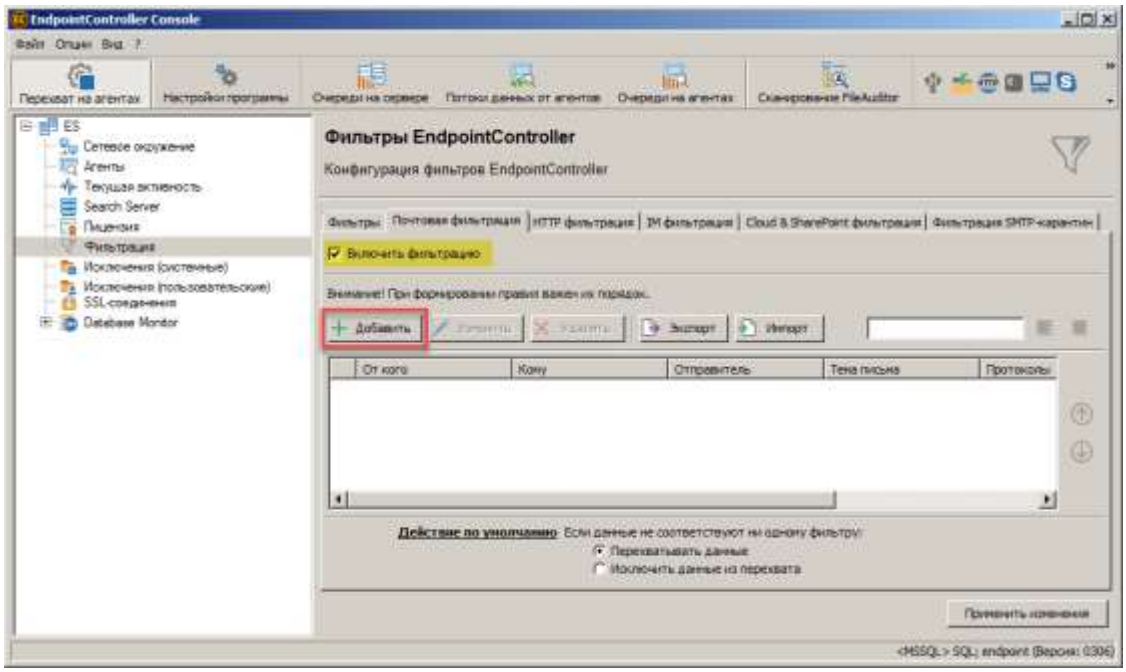


Рисунок 6.215

Очистка фильтров производится способом, аналогичным очистке глобальных фильтров, изложенным выше (см. Рисунок 6.216).

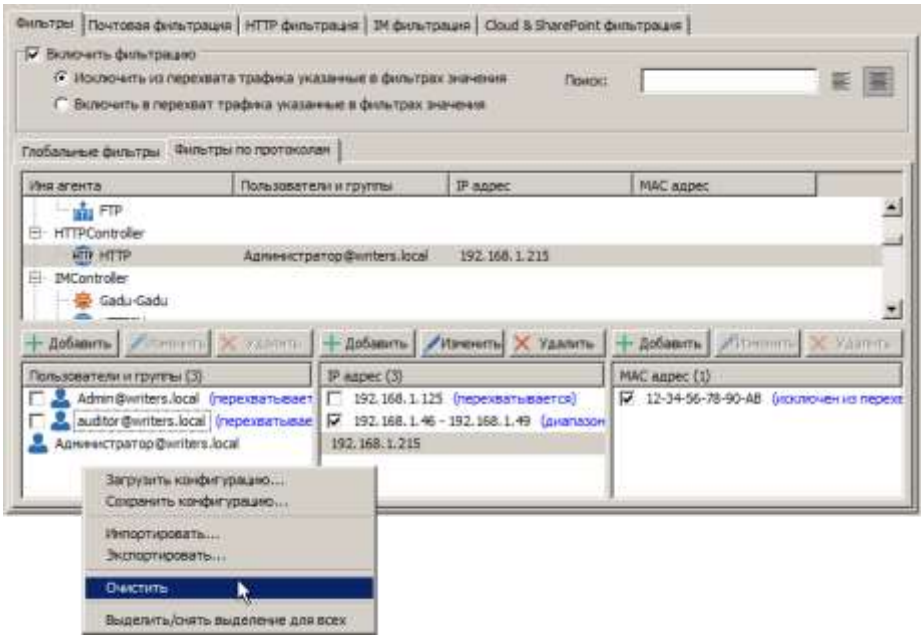


Рисунок 6.216

Из контекстного меню вызвываются команды «Экспортировать/Импортировать» фильтр (группы фильтров) из/в приложение, а также команды «Загрузить кофигурацию/Сохранить конфигурацию» фильтров.

6.5.4.1 Почтовая фильтрация

Фильтры применяются к сообщениям, передаваемым по почтовым протоколам.

Для настройки выделите в левой части окна консоли EndpointController узел «Фильтрация» и откройте вкладку «Почтовая фильтрация». Установите флажок «Включить фильтрацию» и нажмите кнопку «Добавить» (см. Рисунок 6.217).

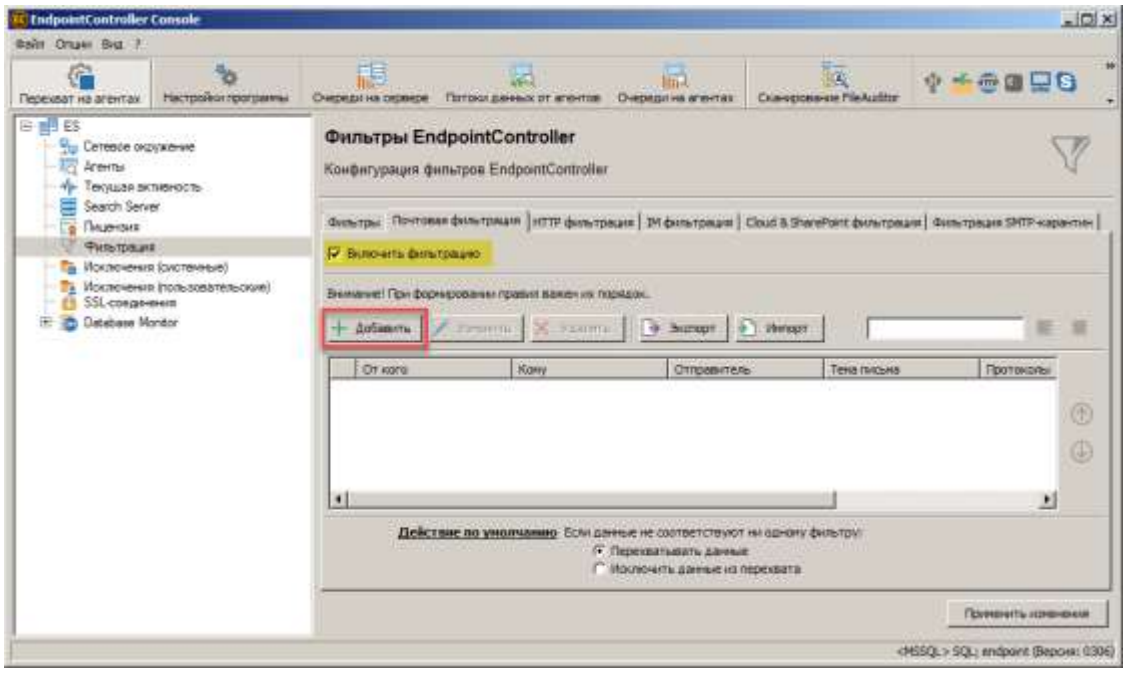


Рисунок 6.217

В открывшемся окне задайте параметры фильтра, заполнив поля: от кого/кому; отправитель; тема письма; размер; количество получателей; протоколы (см. Рисунок 6.218).

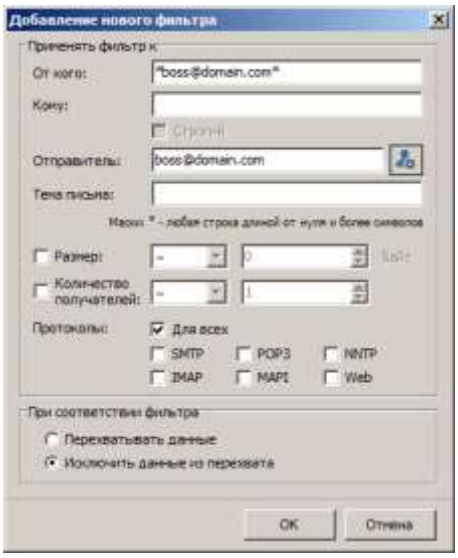


Рисунок 6.218

При указании доменных имен и адресов получателей/отправителей сообщений рекомендуется начинать и заканчивать запись маской с символом «*», подразумевающим любое количество и сочетание символов.

Также для получения списка пользователей можно воспользоваться кнопкой  и выбрать один из источников:

- DataCenter;
- Active Directory;
- NetBIOS.

Установите действие по умолчанию, если письмо не будет соответствовать ни одному из фильтров: либо «Перехватывать письмо», либо «Исключить письмо из перехвата».

Сохраните настройки, нажав «ОК».

Настроенные фильтры имеют приоритет и применяются последовательно в том порядке, в котором они заданы. Чем выше расположен фильтр, тем раньше он сработает. Для регулирования порядка фильтров воспользуйтесь направляющими стрелками (см. Рисунок 6.219).

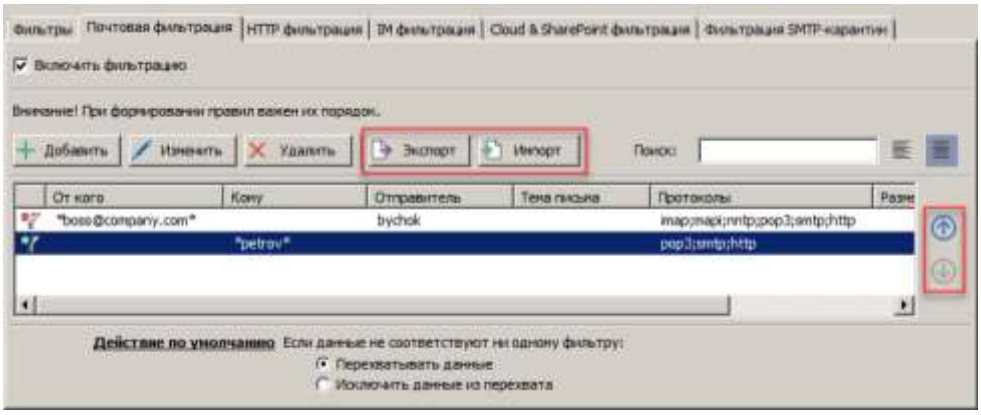


Рисунок 6.219

Фильтры могут быть экспортированы в указанный пользователем файл в формате XML. В свою очередь, сохраненный список фильтров может быть импортирован в приложение из указанного пользователем файла. Для управления используйте кнопки «Экспорт» и «Импорт».

По завершении всех настроек нажмите «Применить изменения».

6.5.4.2 HTTP-фильтрация

Фильтры применяются к GET-/POST-запросам, передаваемым по протоколу HTTP.

Для настройки фильтрации по протоколу HTTP выделите в левой части окна узел «Фильтрация» и откройте вкладку «HTTP фильтрация». Установите флажок «Включить фильтрацию» и нажмите кнопку «Добавить» (см. Рисунок 6.220).

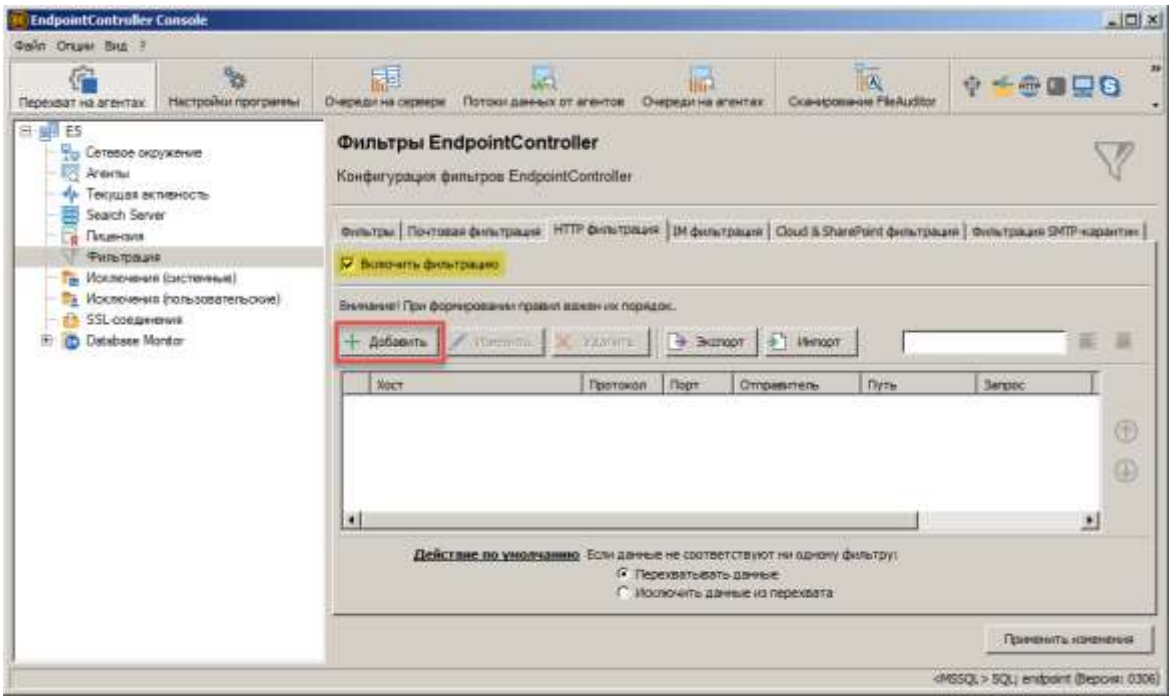


Рисунок 6.220

Укажите значения атрибутов документа, к которым будет применен фильтр, предварительно установив напротив него флажок:

- **Хост** - адрес ресурса в сети.
- **Отправитель** - полное доменное имя отправителя запроса (также получить список пользователей можно с помощью кнопки).

В имени хоста и отправителя допускается использование метасимвола «*», заменяющего от нуля и более символов.

Установите действие по умолчанию, если перехваченные данные не будут соответствовать ни одному из фильтров: либо «Перехватывать данные», либо «Исключить данные из перехвата» (см. Рисунок 6.221).

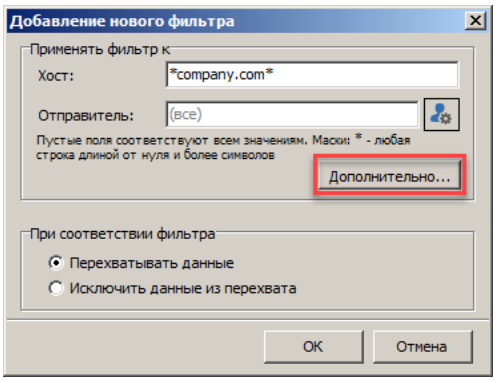


Рисунок 6.221

Щелкните «ОК» для создания фильтра или воспользуйтесь кнопкой «Дополнительно...» для детальной настройки фильтрации.

Укажите дополнительные значения атрибутов документа, по которым будет произведена фильтрация (см. Рисунок 6.222):

- **Протокол** – сетевой протокол (HTTP или HTTPS);
- **Порт** – порт хоста для подключения;
- **Путь** – уточняющая информация о месте нахождения ресурса;
- **Запрос** – строка запроса с передаваемыми на сервер параметрами. Разделитель запросов – символ «&»;
- **В любой части перехвата** – данные запроса, поиск по которым будет осуществлен как в адресной строке, так и в теле пакета (использование метасимвола «*» не допускается);
- **Размер (байт)** – размер запроса.

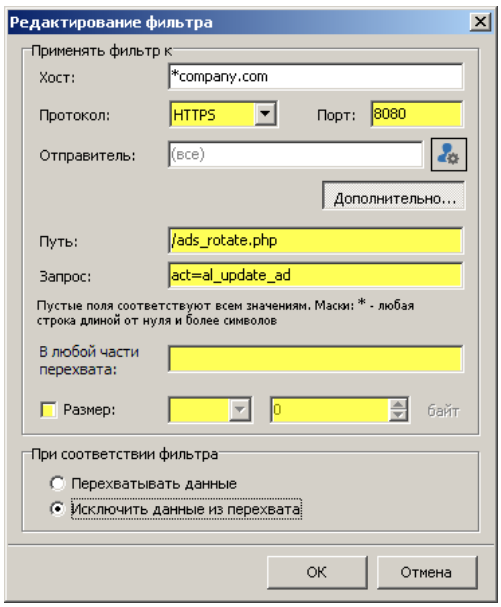


Рисунок 6.222

Для примера рассмотрим следующий URL-адрес:

https://www.company.com:8080/ads_rotate.php?act=al_update_ad, где:

https – протокол,

www.company.com – хост,

8080 – порт,

/ads_rotate.php – путь,

act=al_update_ad – запрос.

Установите действие по умолчанию, если перехваченные данные не будут соответствовать ни одному из фильтров: либо «Перехватывать данные», либо «Исключить данные из перехвата» (см. Рисунок 6.223).

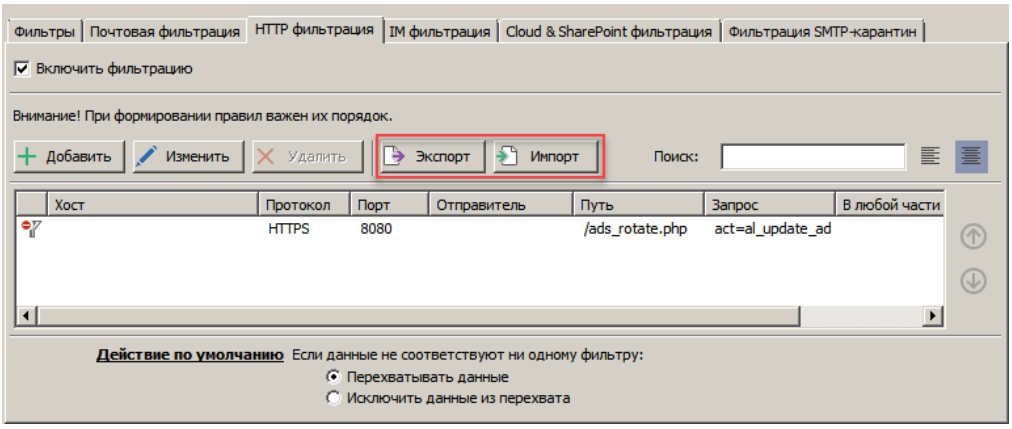


Рисунок 6.223

Фильтры могут быть экспортированы в указанный пользователем файл в формате XML. В свою очередь, сохраненный список фильтров может быть импортирован в приложение из указанного пользователем файла. Для управления используйте кнопки «Экспорт» и «Импорт».

По завершении всех настроек нажмите «Применить изменения».

6.5.4.3 IM-фильтрация

Фильтры работают для сообщений, передаваемых в социальных сетях (Facebook, LinkedIn, В Контакте, Мой Мир@Mail.Ru, Одноклассники, Google+, Мамба.ru, Imo.im, Meebo.com).

Для настройки фильтрации по протоколам IM выделите в левой части окна узел «Фильтрация» и откройте вкладку «IM фильтрация». Установите флажок «Включить фильтрацию» и нажмите кнопку «Добавить» (см. Рисунок 6.224).

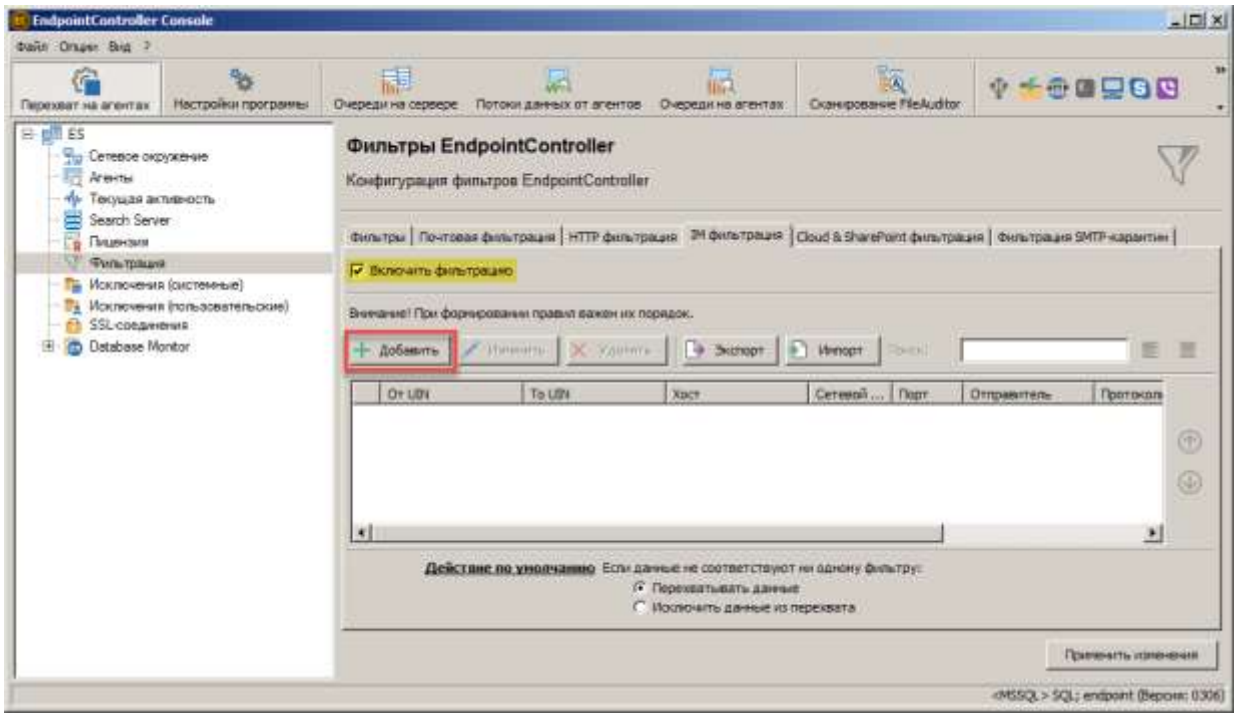


Рисунок 6.224

Укажите необходимые значения атрибутов документа, к которым будет применен фильтр:

- **От UIN/To UIN** - уникальный идентификатор отправителя и/или получателя.
- **Строгий** - при установленном флажке фильтр сработает, если условиям фильтра удовлетворяет хотя бы один UIN. При снятом флажке фильтр сработает только в том случае, когда под условие одного или нескольких фильтров попадут все UIN.
- **Хост** - адрес ресурса в сети (для протокола HTTP IM).
- **Сетевой протокол и Порт** - используемые для подключения протокол и номер порта (для HTTP IM).
- **Отправитель** - полное доменное имя отправителя запроса.

- **В любой части перехвата** – данные, поиск по которым осуществлен как в адресной строке, так и в теле пакета (использование метасимвола "*" не допускается).
- **Размер** - размер запроса.
- **Протоколы** - перечень протоколов, к которым может быть применен данный фильтр.

В имени хоста и отправителя допускается использование метасимвола «*», заменяющего от нуля и более символов.

В блоке «При соответствии фильтру» установите действие по умолчанию, применяемое к данным в случае соответствия фильтру: либо «Перехватывать данные» (производится запись в базу), либо «Исключить данные из перехвата» (не производится запись в базу) (см. Рисунок 6.225).

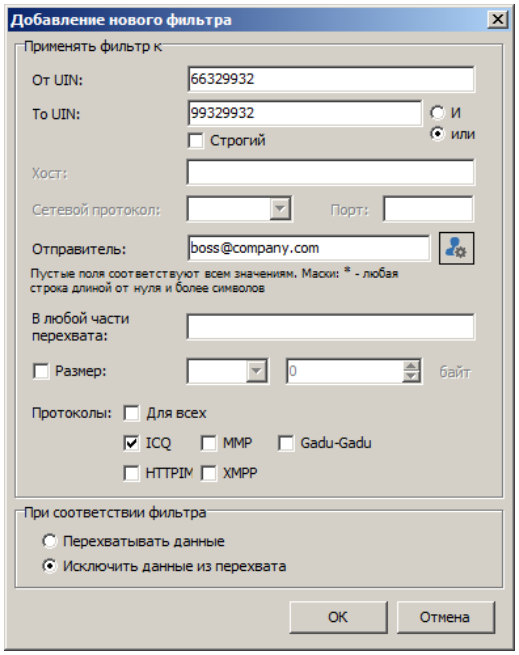


Рисунок 6.225

Щелкните «ОК», фильтр будет создан.

В окне консоли установите действие по умолчанию, если перехваченные данные не будут соответствовать ни одному из фильтров: либо «Перехватывать данные», либо «Исключить данные из перехвата» (см. Рисунок 6.226).

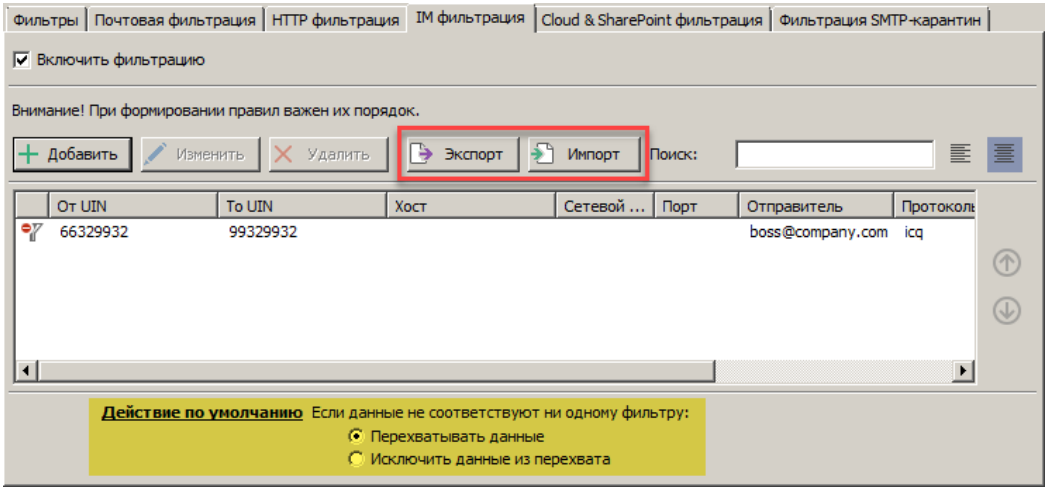


Рисунок 6.226

Фильтры могут быть экспортированы в указанный пользователем файл в формате XML. В свою очередь, сохраненный список фильтров может быть импортирован в приложение из указанного пользователем файла. Для управления используйте кнопки «Экспорт» и «Импорт».

По завершении настроек нажмите «Применить изменения» (см.Рисунок 6.226).

6.5.4.4 Cloud&SharePoint фильтрация

Фильтры работают для данных, передаваемых из/в облачные хранилища.

Для настройки фильтрации выделите в левой части окна узел «Фильтрация» и откройте вкладку «Cloud & SharePoint фильтрация». Установите флажок «Включить фильтрацию» и нажмите кнопку «Добавить» (см. Рисунок 6.227).

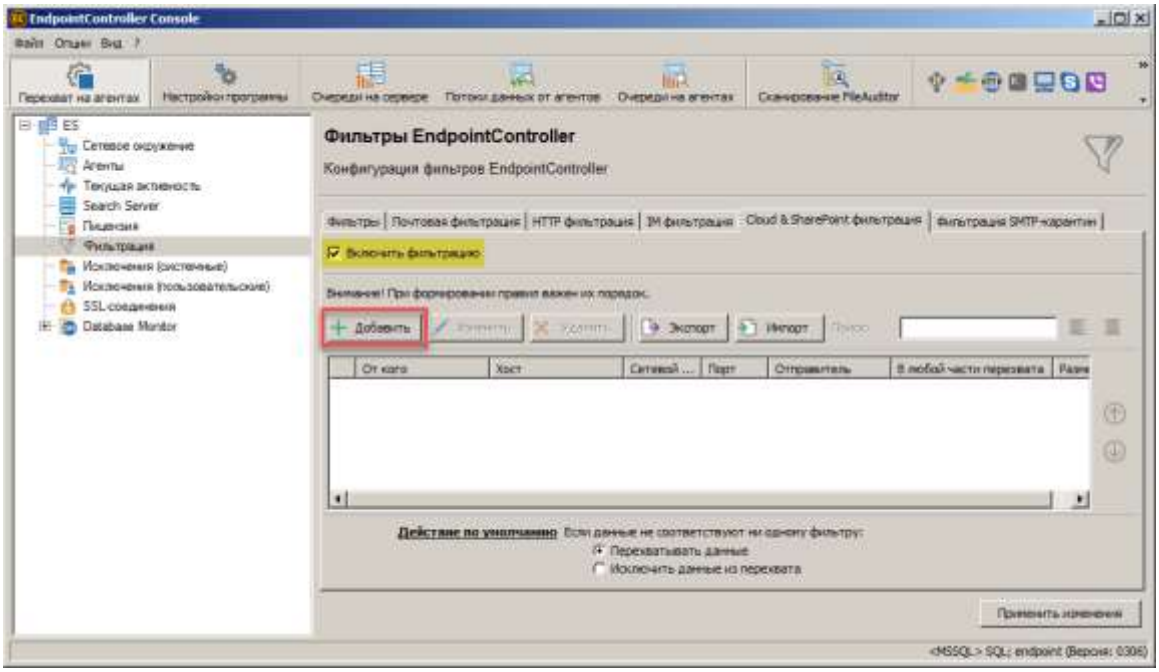


Рисунок 6.227

Укажите значения атрибутов документа, к которым будет применен фильтр (см. Рисунок 6.228):

- **Хост** – адрес ресурса в сети.
- **Отправитель** – полное доменное имя отправителя запроса.

В имени хоста и отправителя допускается использование метасимвола «*», заменяющего от нуля и более символов.

В блоке «При соответствии фильтру» установите действие по умолчанию, применяемое к данным в случае соответствия фильтру: либо «Перехватывать данные» (производится запись в базу), либо «Исключить данные из перехвата» (не производится запись в базу).

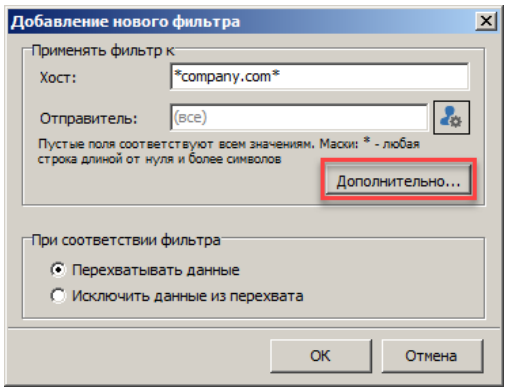


Рисунок 6.228

Щелкните «ОК» для создания фильтра или воспользуйтесь кнопкой «Дополнительно...» для детальной настройки фильтрации.

Укажите дополнительные значения атрибутов документа, по которым будет произведена фильтрация:

- **Сетевой протокол** – сетевой протокол (HTTP или HTTPS);
- **Порт** – порт хоста для подключения;
- **В любой части перехвата** – данные запроса, поиск по которым будет осуществлен как в адресной строке, так и в теле пакета (использование метасимвола «*» не допускается);
- **Размер** – размер запроса в байтах (см. Рисунок 6.229).

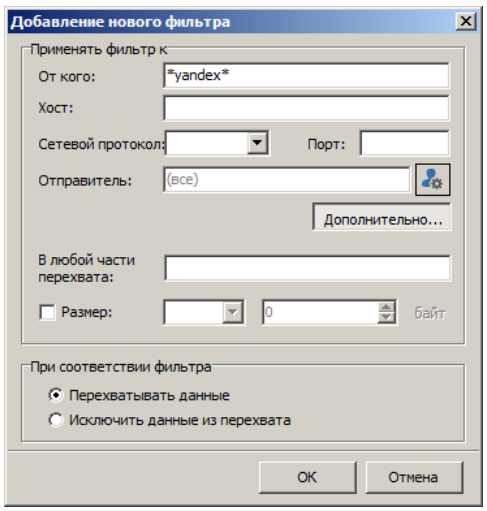


Рисунок 6.229

В окне консоли установите действие по умолчанию, если перехваченные данные не будут соответствовать ни одному из фильтров: либо «Перехватывать данные», либо «Исключить данные из перехвата» (см. Рисунок 6.230).

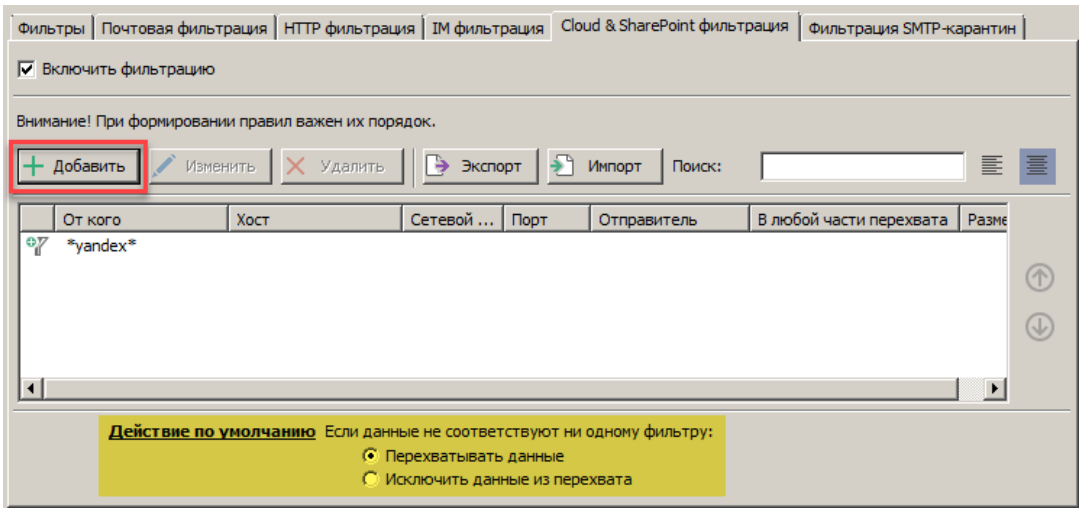


Рисунок 6.230

Фильтры могут быть экспортированы в указанный пользователем файл в формате XML. В свою очередь, сохраненный список фильтров может быть импортирован в приложение из указанного пользователем файла. Для управления используйте кнопки «Экспорт» и «Импорт».

По завершении всех настроек нажмите «Применить изменения».

6.5.4.5 Фильтрация писем карантина

Фильтры работают для сообщений, попавших под правило карантина, настроенное в AnalyticConsole.

Для настройки фильтра выделите в левой части окна узел «Фильтрация» и откройте вкладку «Фильтрация SMTP-карантин». Установите флажок «Включить фильтрацию» и нажмите кнопку «Добавить» (см. Рисунок 6.231).

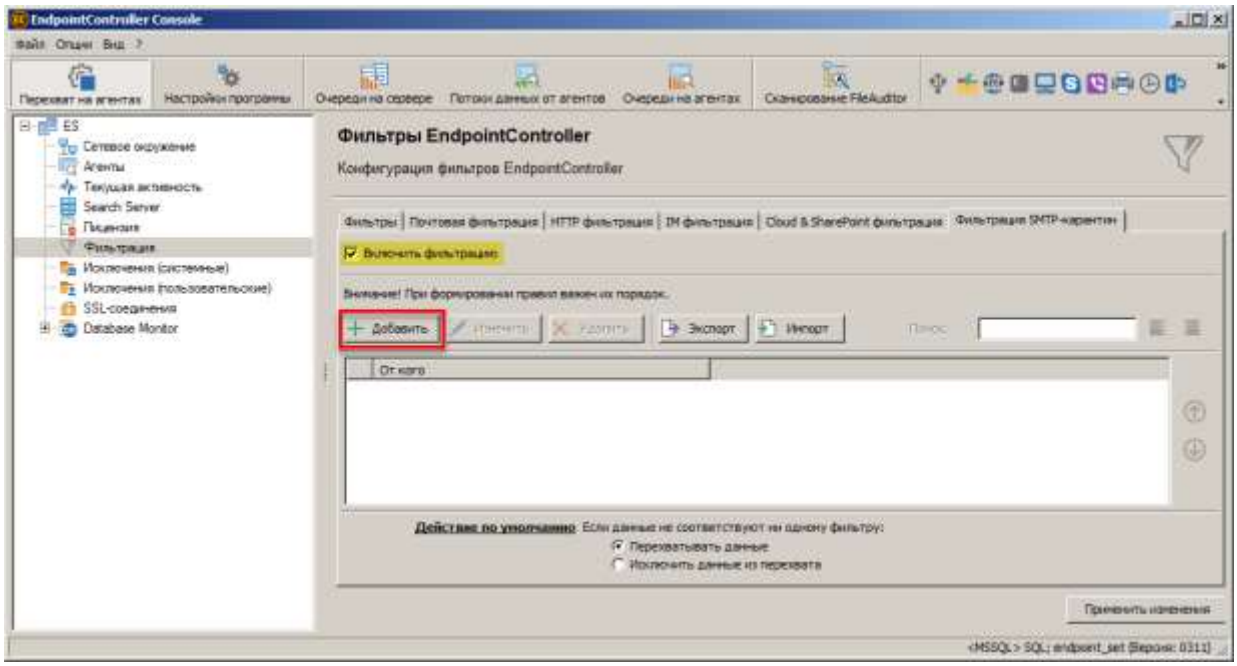


Рисунок 6.231

В открывшемся окне задайте электронный адрес отправителя письма. Рекомендуется указывать адреса пользователей с маской «*», подразумевающей любое количество и сочетание символов. Примеры масок:

- *ivan.ivanov@company.ru*
- *@company.ru*
- *ivan.*@company*
- *ivan.ivanov*
- *ivan*.

Выберите действие в области «При соответствии фильтру»: перехватывать письмо при его соответствии правилу карантина или исключить письмо из перехвата (см. Рисунок 6.232).

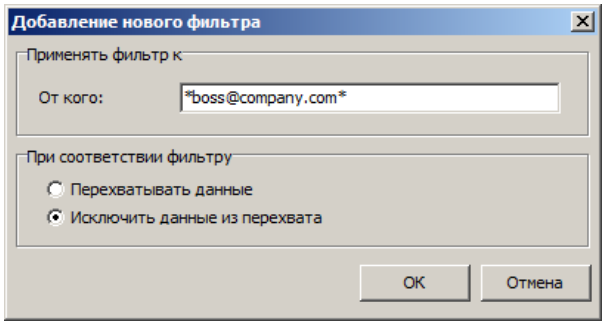


Рисунок 6.232

Завершите создание фильтра нажатием кнопки «ОК».

Фильтры карантина имеют приоритет и применяются последовательно в том порядке, в котором они заданы. Чем выше расположен фильтр, тем раньше он сработает. Управление порядком фильтров производится с помощью кнопок и (см. Рисунок 6.233).

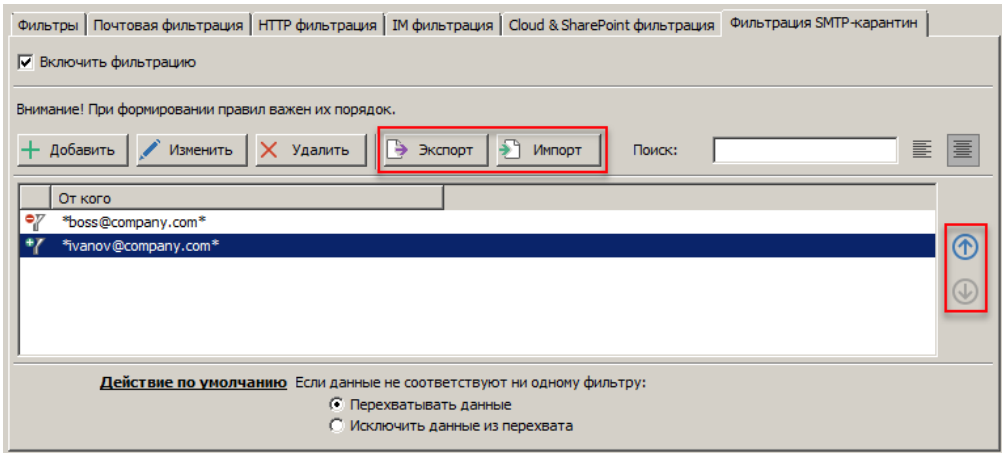


Рисунок 6.233

В окне консоли установите действие по умолчанию, если перехваченные данные не будут соответствовать ни одному из фильтров: либо «Перехватывать данные», либо «Исключить данные из перехвата».

Фильтры могут быть экспортированы в указанный пользователем файл в формате XML. В свою очередь, сохраненный список фильтров может быть импортирован в приложение из указанного пользователем файла. Для управления используйте кнопки «Экспорт» и «Импорт».

По завершении всех настроек нажмите «Применить изменения».

6.5.5 Настройка исключений

Настройка исключений применяется с целью обеспечить совместности работы агентов EndpointController со стандартными системными процессами, а также для ограничения действия агентов на некоторые заслуживающие доверия программы (пользовательские приложения).

Рекомендуется исключать системные процессы при работе агентов с целью предотвращения возможных конфликтов при взаимодействии приложений (см. 2676.5.5.1).

Возможны случаи, когда при наличии запущенных агентов EndpointController пользовательские программные приложения (например, антивирусное ПО, банковские клиенты, компоненты сторонних DLP-систем, системы электронного документооборота) перестают функционировать.

При обнаружении некорректной работы приложений в системе с установленным агентом EndpointController конфликтующие приложения могут быть внесены в список исключений EndpointController (см. 6.5.5.2).

В свою очередь, процессы EndpointController могут быть добавлены в список исключений конфликтующих приложений. **При использовании EndpointController совместно с антивирусными программами настройка взаимных исключений является обязательной!**

В список исключений могут быть также внесены хосты, располагающие встроенной защитой от мониторинга передаваемых данных (см. п. 6.5.5.3).

Также с помощью исключений могут быть заданы глобальные разрешающие правила для определенных IP-адресов/портов (см. п. 6.5.5.5).

В отношении списков исключений могут применяться операции импорта и экспорта (см. 6.5.5.7).

Настройка и управление исключениями производится на вкладке «Исключения» в левой части консоли администрирования.

6.5.5.1 Исключение системных процессов

Стандартные системные процессы необходимо исключить из обработки агентами только путем импорта, т.к. исключения такого рода процессов не могут редактироваться. Рекомендуемый набор исключений можно загрузить с сайта разработчика и импортировать при запуске консоли EndpointController (см. Рисунок 6.234).

Если системные кнопоки «Экспорт»/«Импорт» не отображаются в консоли EndpointController, перейдите в Настройки программы в раздел «Дополнительно» и активируйте экспертный режим.

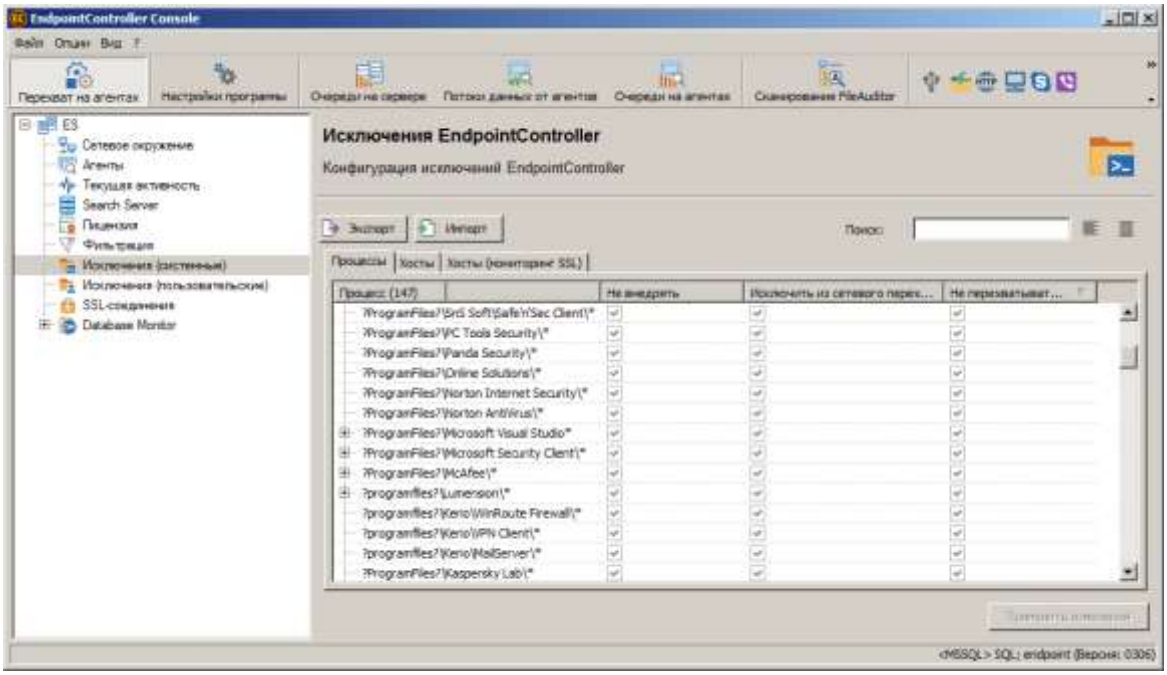


Рисунок 6.234

6.5.5.2 Исключение пользовательских приложений

Настройка исключения пользовательских приложений производится на вкладке «Процессы» панели просмотра исключений (см. Рисунок 6.235).

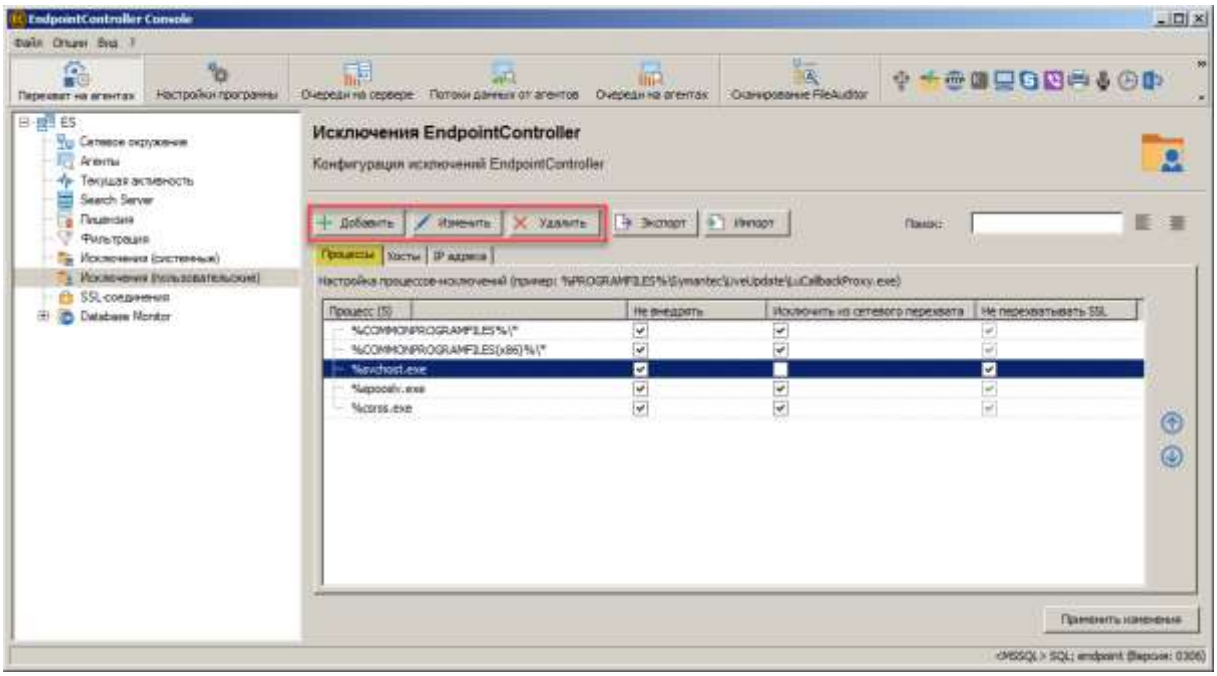


Рисунок 6.235

Управление списком исключений возможно с помощью кнопок «Добавить», «Изменить», «Удалить». Сортировка списка осуществляется кнопками-стрелками справа от списка процессов.

Для управления процессами исключений используйте флажки в следующих колонках:

- **Не внедрять** – запрет на вмешательство агентов EndpointController в работу выбранного приложения;
- **Исключить из сетевого перехвата** – исключение сетевого трафика выбранного приложения из обработки агентом;
- **Не перехватывать SSL** – исключение зашифрованного трафика выбранного приложения из обработки агентом (незашифрованный трафик перехватываться будет).

Установка флажка «Исключить из сетевого перехвата» автоматически деактивирует опцию «Не перехватывать SSL».

Для добавления процесса в список исключений нажмите «Добавить». В открывшемся окне укажите требуемые атрибуты процесса (см. Рисунок 6.236).

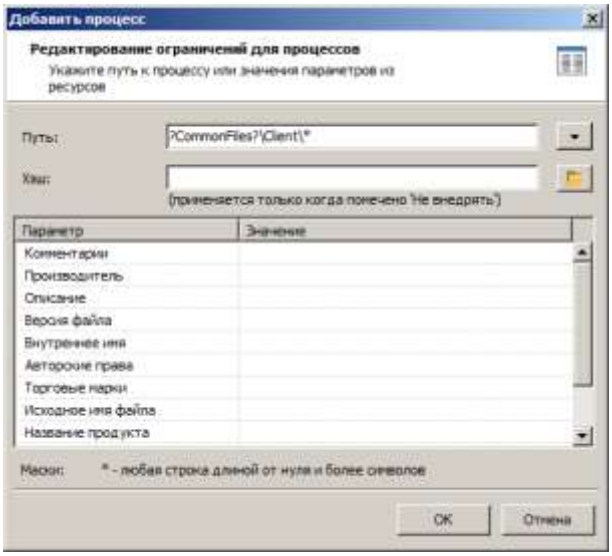


Рисунок 6.236

Символ маски (*) означает, что в роли значения параметра может выступать строка любой длины.

Указание пути к процессу и других параметров является опциональным. Указываемые параметры должны соответствовать значениям, которые прописаны в свойствах процесса. В случае, если хоть по одному параметру будет несоответствие – исключение не сработает.

При внесении исключений допускается вместо абсолютного пути указывать переменные среды окружения, например, %ProgramFiles%\SomeAppFolder*. Список наиболее часто используемых переменных открывается по щелчку по направляющей стрелке, расположенной справа от поля «Путь».

В нижней части списка переменных располагаются **пользовательские списки путей**[28] (см. Рисунок 6.237). Всплывающая подсказка по наведении указателя мыши на имя списка отображает пути, входящие в данный пользовательский список (как абсолютные, так и относительные – переменные среды).

[28] Пользовательские списки путей задаются в настройках EndpointController в разделе «Псевдонимы путей».

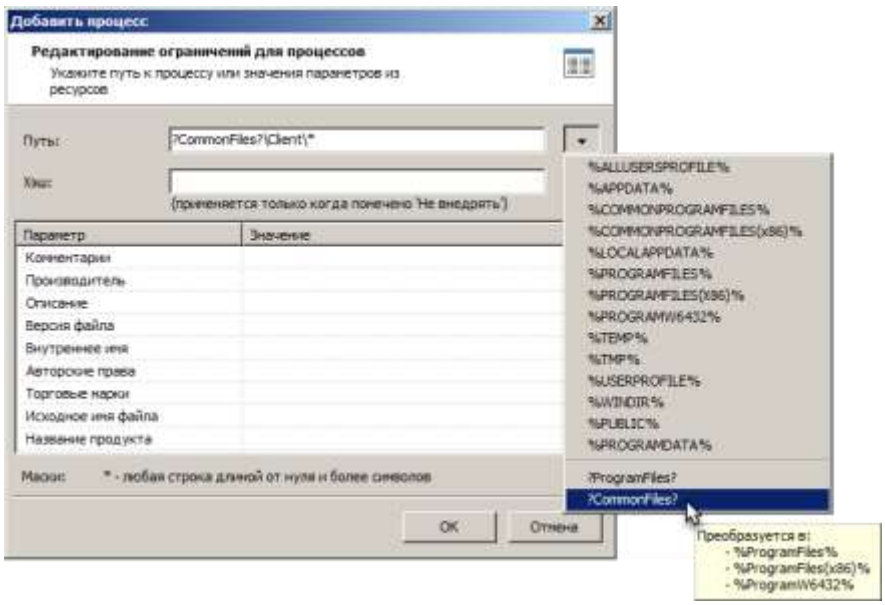


Рисунок 6.237

Для редактирования выделенного процесса воспользуйтесь кнопкой «Изменить».

Для удаления выделенного процесса воспользуйтесь кнопкой «Удалить». Если необходимо удалить сразу несколько процессов, используйте дополнительно кнопки SHIFT и CTRL.

Для того, чтобы произведенные настройки процессов-исключений вступили в силу, щёлкните кнопку «Применить изменения».

6.5.5.3 Исключение хостов

Включение хостов в список исключений позволяет управлять перехватом HTTP-трафика.

Хосты, внесенные в список исключений, игнорируются агентами EndpointController. Данная функция может применяться, к примеру, при интеграции Серчинформ ДЛП с системами корпоративного документооборота или клиентами интернет-банкинга, работающими по защищенному соединению и запрещающими контролировать свой трафик. Добавление подобных веб-ресурсов в список исключений позволяет избежать сбоев в работе системы безопасности, возникающих в результате конфликтов различных программных решений.

Настройка исключения пользовательских приложений производится на вкладке «Хосты» панели просмотра (см. Рисунок 6.238).

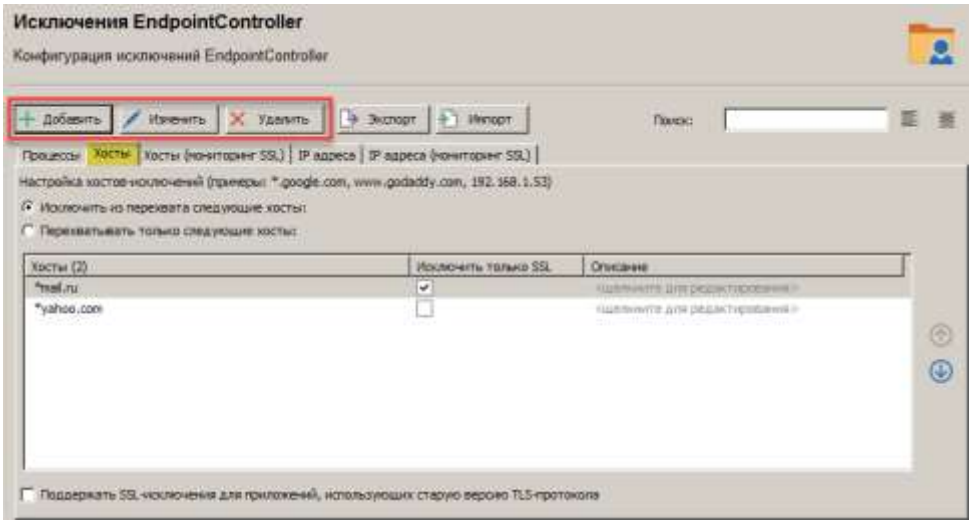


Рисунок 6.238

Трафик присутствующих в списке сайтов будет исключаться из перехвата в случае, если выбрана опция «Исключить из перехвата следующие хосты». Трафик сайта, указанного в колонке «Хосты», будет исключен из перехвата полностью (и обычный, и зашифрованный трафик), если в колонке «Исключить только SSL» для этого сайта снят флажок.

Для исключения только зашифрованного трафика выбранного хоста установите флажок в колонке «Исключить только SSL». В данном случае из перехвата будет исключен только зашифрованный трафик выбранного хоста, незашифрованный трафик перехватываться будет (см. Рисунок 6.239).

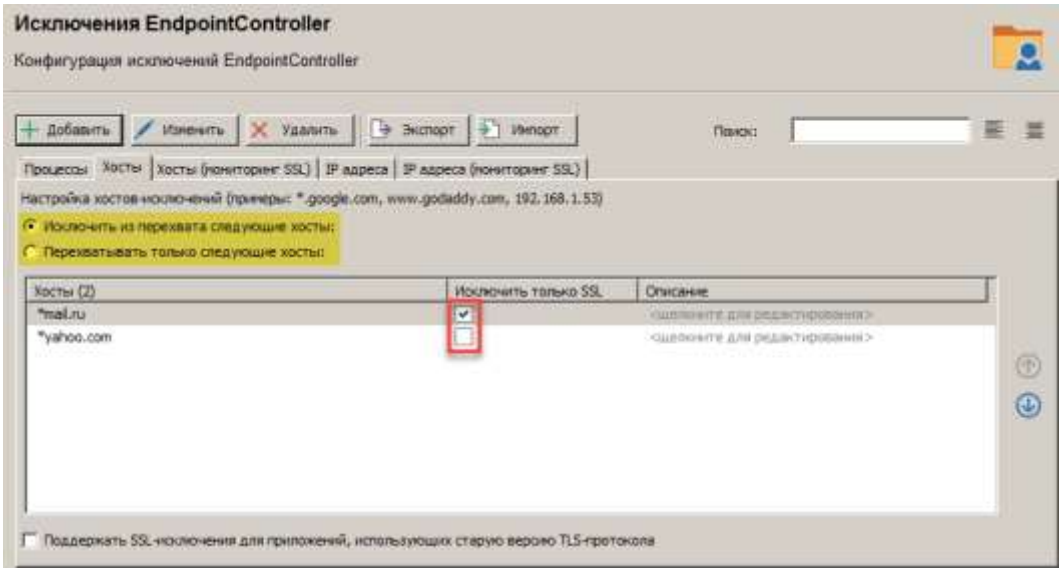


Рисунок 6.239

Чтобы добавить хост в список исключений, щёлкните кнопку «Добавить» и введите имя хоста (см. Рисунок 6.240).

Рисунок 6.240

Допускается ввод имени хоста или маски в URL, например, **mail.ru*.

Для редактирования имени хоста из списка исключений воспользуйтесь кнопкой «Изменить» (см. Рисунок 6.241).

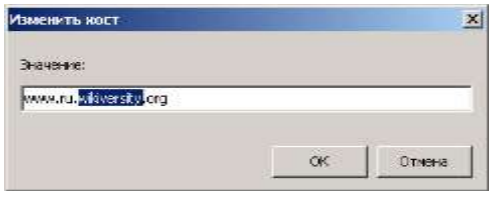


Рисунок 6.241

Для удаления выбранного сайта воспользуйтесь кнопкой «Удалить». Если необходимо удалить сразу несколько хостов, используйте дополнительно кнопки SHIFT и CTRL.

Для поддержки исключений при использовании старой версии TLS-протокола отметьте параметр «**Поддержать SSL-исключения для приложений, использующих старую версию TLS-протокола**». При снятом флажке должно учитываться условие полного совпадения имен хостов, указанных в исключениях и вводимых пользователем. Например, добавленный в исключения хост **hostname.com** не соответствует введенному хосту **www.hostname.com**, в связи с чем данное исключение при текущей записи может не отработать.

Для того чтобы произведенные настройки хостов вступили в силу, щёлкните кнопку «Применить изменения».

6.5.5.4 Мониторинг хостов с SSL

Для перехвата только шифрованного трафика с определенных хостов настраиваются исключения на вкладке «Хосты (мониторинг SSL)». Обычный трафик таких ресурсов игнорируется.

При попытке доступа к любому из хостов данного списка, агент EndpointController пытается осуществить безусловную подмену сертификата с целью дальнейшего перехвата SSL-трафика. В случае успешной подмены пользователь сможет работать с данным хостом, а SSL-трафик будет перехватываться агентом. Если попытка подмены сертификата окажется безуспешной, доступ к ресурсу пользователь не получит (см. Рисунок 6.242).

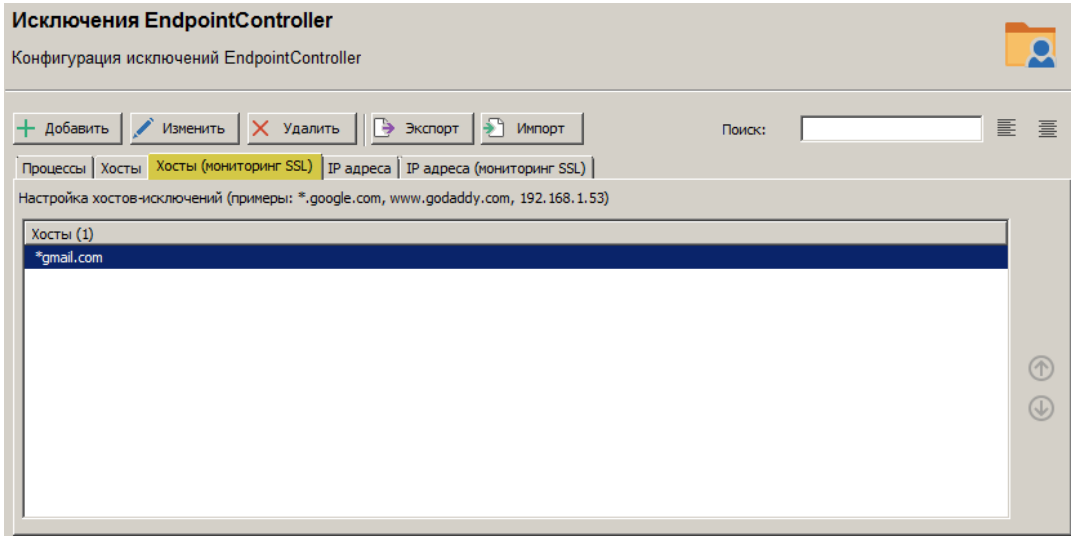


Рисунок 6.242

Для добавленных в исключения хостов проверка будет производиться независимо от успеха/неудачи предыдущей попытки перехвата защищённого трафика.

6.5.5.5 Исключение IP-адресов

С помощью исключений можно задать глобальные **разрешающие** правила для определённых IP-адресов/портов. Это значит, что агент не будет внедряться в обмен данными с указанными IP-адресами, а отправляемые данные в перехват не попадут.

При работе через прокси-сервер исключения по IP-адресам будут применяться только ко внутренним ресурсам. При обращении к сети Интернет соединение будет осуществляться через прокси-сервер, и передаваемые данные будут обрабатываться сетевым драйвером агента. Сетевой драйвер сопоставит IP-адрес получателя данных со списком внесенных исключений. Так как в этом случае получателем данных выступает прокси-сервер, агент не распознает внешний IP-адрес и будет внедряться в обмен данными.

Для предотвращения подобных ситуаций, исключения для внешних ресурсов необходимо вносить через хосты. В этом случае агент производит первичный разбор сетевого пакета, из которого получает информацию о внешнем адресе и, если этот адрес находится в исключениях, агент не внедряется в обмен данными с запрашиваемым адресом.

Настройка исключений по IP-адресам производится на вкладке «IP адреса» в правой части консоли при выбранной вкладке «Исключения (пользовательские)» (см. Рисунок 6.243).

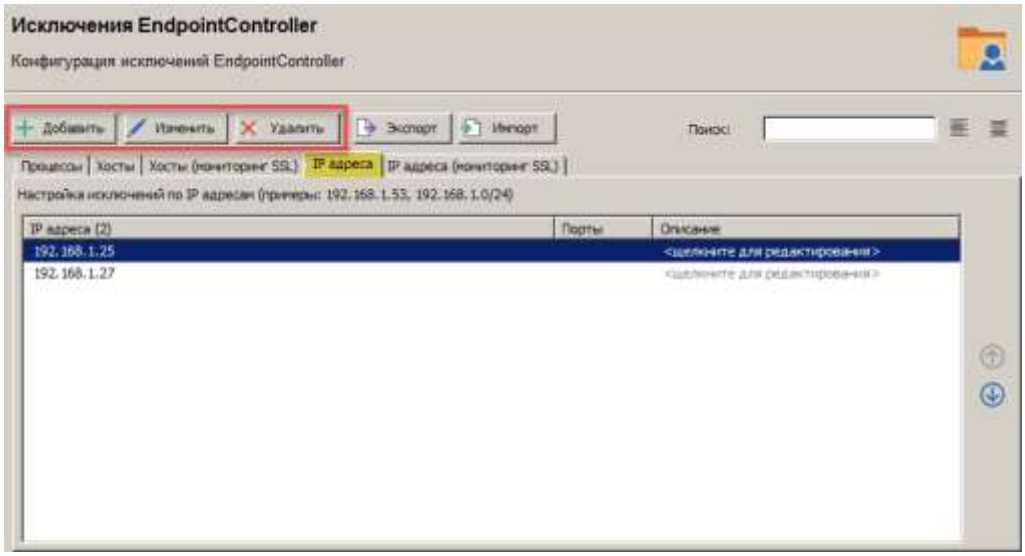


Рисунок 6.243

Можно задавать как IP-адреса, так и отдельные порты для заданных IP (см. Рисунок 6.244).

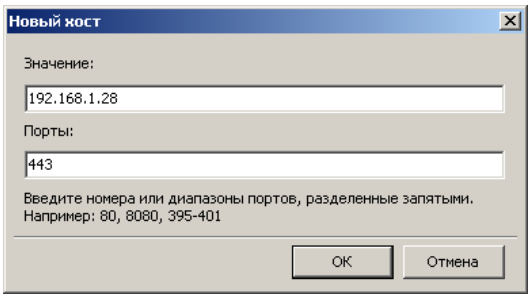


Рисунок 6.244

6.5.5.6 Исключение IP-адресов (мониторинг SSL)

На вкладке «IP адреса (мониторинг SSL)» осуществляется настройка совместимости с Outlook для определенных серверов MS Exchange.

Необходимость данной настройки связана с проблемой в Outlook при доступе по протоколам RPC over HTTP и MAPI: перекодирование SSL изменяет размер данных, из-за чего сервер в определенный момент обрывает соединение. Для устранения проблем с «зависанием» шифрованных RPC over HTTP соединений, добавьте для сервера Exchange SSL-фильтр с флагом совместимости с Outlook (см. Рисунок 6.245).

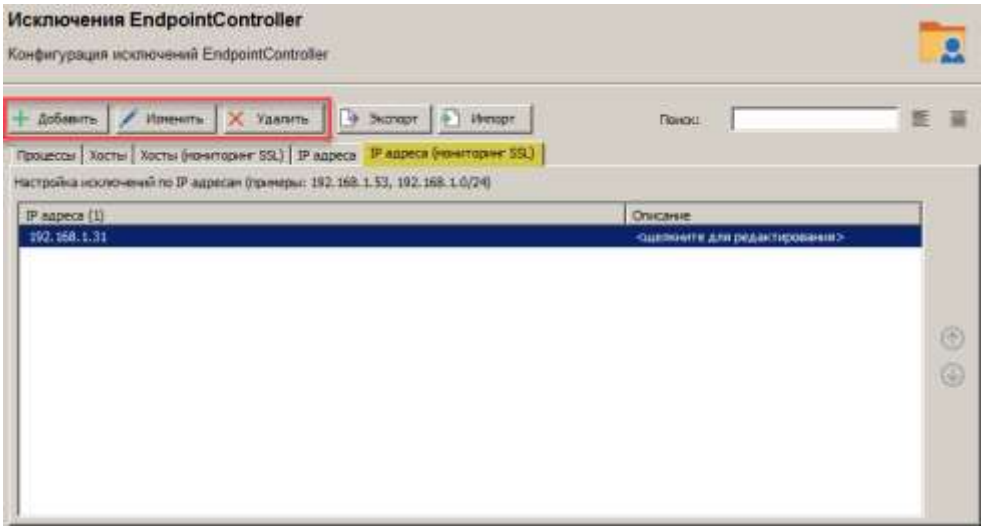


Рисунок 6.245

Для внесения IP-адреса в список исключений нажмите «Добавить» (см.Рисунок 6.246).

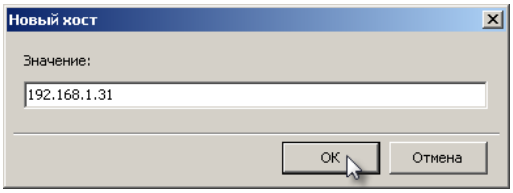


Рисунок 6.246

Для редактирования IP-адреса из списка исключений воспользуйтесь кнопкой «Изменить», для удаления - кнопкой «Удалить». Если необходимо удалить сразу несколько IP-адресов, используйте добавочные клавиши SHIFT и CTRL.

Для того, чтобы произведенные настройки исключений вступили в силу, щёлкните кнопку «Применить изменения».

6.5.5.7 Импорт и экспорт исключений

Списки исключений системных процессов, а также пользовательских приложений и хостов могут быть экспортированы в указанный пользователем файл в формате XML. В свою очередь, сохранённый список исключений может быть импортирован в приложение из указанного пользователем файла.

Для экспорта-импорта списка исключений используются кнопки «Экспорт» и «Импорт» (см. Рисунок 6.247).

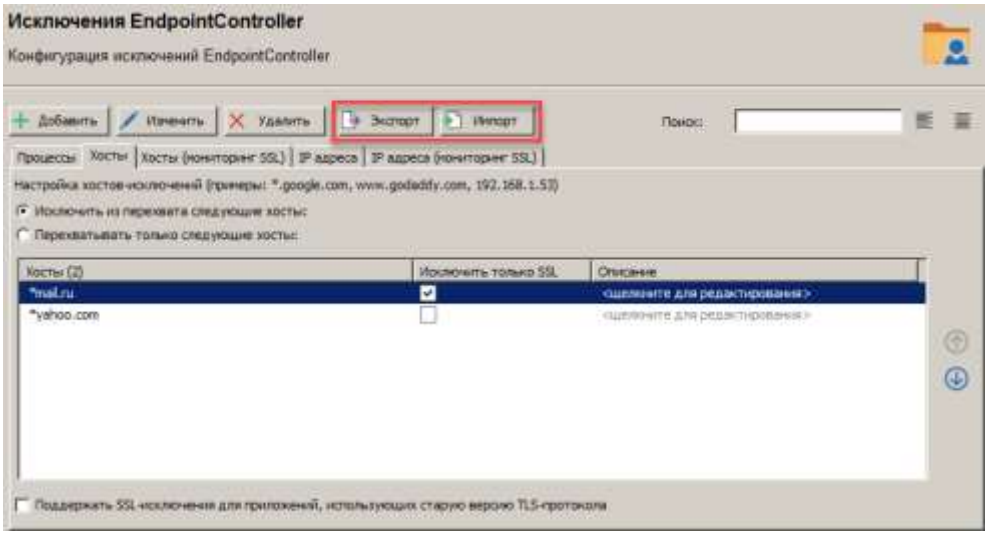


Рисунок 6.247

Кнопка «Экспорт» открывает стандартный диалог «Сохранить как», с помощью которого задается имя файла, содержащего список исключений, и выбирается путь к месту его хранения.

Кнопка «Импорт» открывает стандартный диалог «Открыть», с помощью которого выбирается сохранённый в каталоге файл со списком исключений.

6.5.6 Настройка антивирусных приложений

Для того чтобы совместная работа Серчинформ ДЛП и корпоративных антивирусных программ не приводила к взаимным конфликтам, необходимо внести установленные компоненты Серчинформ ДЛП в исключения используемого антивирусного ПО.

Перейдите в настройки антивируса и откройте раздел «Исключения». Пользуясь кнопкой открытия обозревателя, добавьте в список исключений необходимые файлы и папки (если данная опция поддерживается антивирусом). Подтвердите произведенные изменения щелчком по «OK» (см. Рисунок 6.248).

Если антивирус не поддерживает указание папок, а только файлов, для каждой перечисленной ниже папки необходимо указать все файлы, расположенные как в самой папке, так и во вложенных папках.

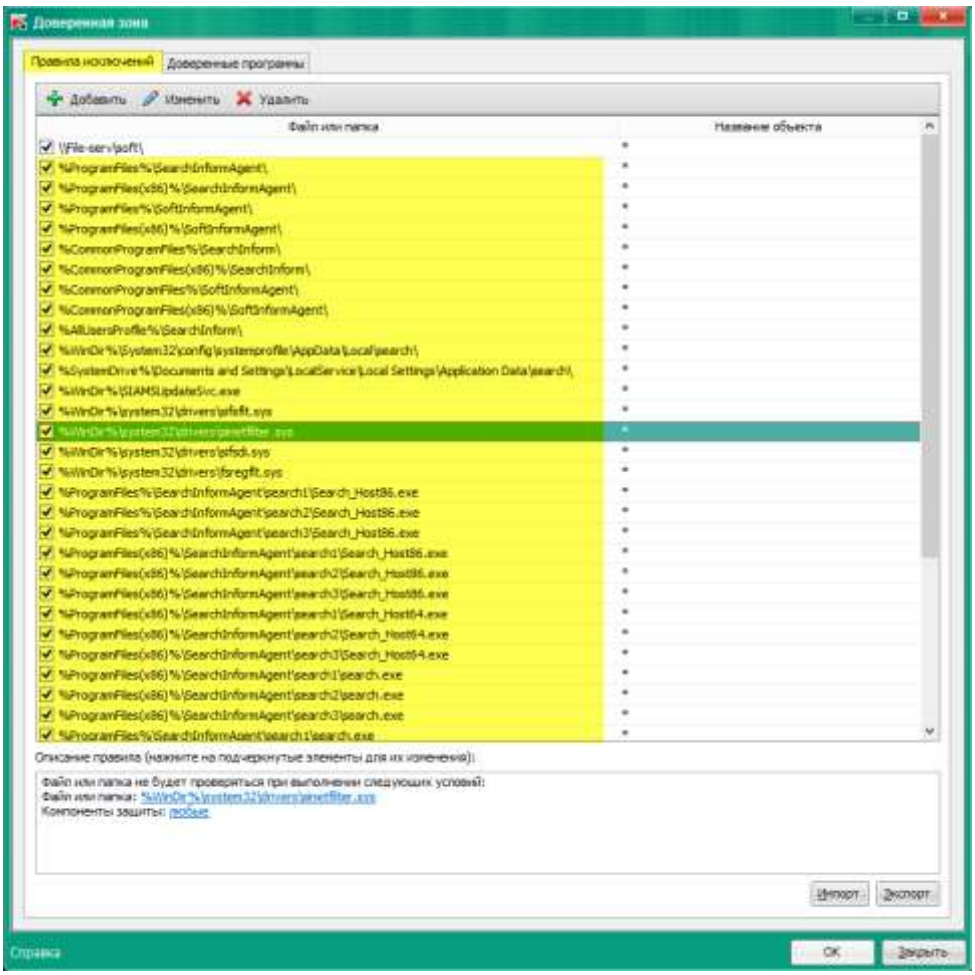


Рисунок 6.248

Исключения приведены для разных операционных систем и разных разрядностей. При внесении исключений рекомендуется использовать относительные пути если их поддерживает антивирус (`%ProgramFiles%`, `%SystemRoot%`, `%SystemDrive%` и т.д.).

Если антивирус не поддерживает указание путей через переменные окружения, необходимо вместо каждой переменной перечислить все папки в сети, куда может ссылаться данная переменная: например, если система встречается на `C:\` и `D:\`, то вместо каждого исключения вида `%WinDir%\*` необходимо добавить по два исключения: `C:\Windows\*` и `D:\Windows\*`.

6.5.6.1 Исключения для сервера

Папки, которые необходимо вносить в перечень исключений на сервере EndpointController:

`%ProgramFiles(x86)%\SearchInform\`

`%AllUsersProfile%\SearchInform\`

`*\messages\` – местоположение временного хранилища перехваченных сообщений

*\Storage\ – местоположение локального хранилища модулей DeviceController и FTPController.

6.5.6.2 Исключения для рабочих станций

Файлы и папки, которые необходимо вносить в перечень исключений[29]:

```
*\SIAMSUpdateSvc.exe
%TEMP%\ESClient.msi
%TEMP%\ESClient.exe
%TEMP%\ESClientX64.exe
*\Cleaner.exe
*\CleanerX64.exe
%TEMP%\Cleaner.exe
%TEMP%\CleanerX64.exe
%WinDir%\system32\drivers\sicore.sys
%WinDir%\system32\drivers\fsregflt.sys
%WinDir%\system32\drivers\sifsflt.sys
%WinDir%\system32\drivers\sinetfilter.sys
%WinDir%\system32\drivers\sifsdi.sys
%WinDir%\system32\drivers\sikbmohk.sys
%AllUsersProfile%\SearchInform\
%WinDir%\Installer\
```

Для 32-разрядных систем дополнительно необходимо внести следующие файлы и папки:

```
%WinDir%\system32\drivers\EsPsProtect32.sys
%WinDir%\system32\drivers\EsSiphLdr32.sys
%WinDir%\system32\drivers\silstipt32.sys
%ProgramFiles%\SearchInformAgent\SIFilterSvc1\SIFilterSvc.exe
%ProgramFiles%\SearchInformAgent\SIFilterSvc2\SIFilterSvc.exe
%ProgramFiles%\SearchInformAgent\SIFilterSvc3\SIFilterSvc.exe
%ProgramFiles%\SearchInformAgent\SIFilterSvc1\SIHost.exe
%ProgramFiles%\SearchInformAgent\SIFilterSvc2\SIHost.exe
%ProgramFiles%\SearchInformAgent\SIFilterSvc3\SIHost.exe
%ProgramFiles%\SearchInformAgent\SIFilterSvc1\SIFilterSvc_manager.exe
%ProgramFiles%\SearchInformAgent\SIFilterSvc2\SIFilterSvc_manager.exe
```

[29] Названия папок будут отличаться в случае переименования службы агента в консоли EndpointController.

%ProgramFiles%\SearchInformAgent\SIFilterSvc3\SIFilterSvc_manager.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc1\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc2\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc3\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles%\SearchInformAgent\

%ProgramFiles%\SearchInformAgent\SIFilterSvc1\DRIVERS\

%ProgramFiles%\SearchInformAgent\SIFilterSvc2\DRIVERS\

%ProgramFiles%\SearchInformAgent\SIFilterSvc3\DRIVERS\

%ProgramFiles%\SearchInformAgent\SIFilterSvc1\nss\

%ProgramFiles%\SearchInformAgent\SIFilterSvc2\nss\

%ProgramFiles%\SearchInformAgent\SIFilterSvc3\nss\

%CommonProgramFiles%\SearchInform\

%SystemDrive%\Documents and Settings\LocalService\Local Settings\Application Data\SIFilterSvc\

%WinDir%\System32\config\systemprofile\AppData\Local\SIFilterSvc\

Для 64-разрядных систем дополнительно необходимо внести следующие файлы и папки:

%WinDir%\system32\drivers\EsPsProtect64.sys

%WinDir%\system32\drivers\EsSiphLdr64.sys

%WinDir%\system32\drivers\silstipt64.sys

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\SIFilterSvc.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\SIFilterSvc.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\SIFilterSvc.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\SIHost.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\SIHost.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\SIHost.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\SIHost64.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\SIHost64.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\SIHost64.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\SIFilterSvc_manager.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\SIFilterSvc_manager.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\SIFilterSvc_manager.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles(x86)%\SearchInformAgent\

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\DRIVERS\

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\DRIVERS\

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\DRIVERS\

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\nss\

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\nss\

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\nss\

%CommonProgramFiles(x86)%\SearchInform\

%AllUsersProfile%\SearchInform\

%SystemDrive%\Documents and Settings\NetworkService\Local Settings\Application Data\SIFilterSvc\

%WinDir%\SysWOW64\config\systemprofile\AppData\Local\SIFilterSvc\

Для ПО Kaspersky дополнительно необходимо исключить из проверки и внести в список доверенных программ следующие файлы:

%ProgramFiles%\SearchInformAgent\SIFilterSvc1\SIHost.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc2\SIHost.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc3\SIHost.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\SIHost.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\SIHost.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\SIHost.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\SIHost64.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\SIHost64.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\SIHost64.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\sifiltersvc.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\sifiltersvc.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\sifiltersvc.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\SIFilterSvc_manager.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\SIFilterSvc_manager.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\SIFilterSvc_manager.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc1\sifiltersvc.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc2\sifiltersvc.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc3\sifiltersvc.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc1\SIFilterSvc_manager.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc2\SIFilterSvc_manager.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc3\SIFilterSvc_manager.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc1\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc2\AgentSearch\SIFiltersvc_search.exe

%ProgramFiles%\SearchInformAgent\SIFilterSvc3\AgentSearch\SIFiltersvc_search.exe

Для рабочих станций, на которых будет использоваться модуль CameraController, необходимо отключить опцию «Показывать уведомление, когда веб-камеру использует программа, которой это разрешено» (Настройка → Защита → Защита Веб-камеры).

Для Windows Defender рекомендуется распространять исключения через групповые политики (GPO). Также дополнительно необходимо исключить следующие папки:

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc1\

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc2\

%ProgramFiles(x86)%\SearchInformAgent\SIFilterSvc3

%ProgramFiles%\SearchInformAgent\SIFilterSvc1\

%ProgramFiles%\SearchInformAgent\SIFilterSvc2\

%ProgramFiles%\SearchInformAgent\SIFilterSvc3\

и процессы:

sifiltersvc.exe

sifiltersvc_manager.exe

sifiltersvc_search.exe

sihost.exe

sihost64.exe

6.5.6.3 Особенности настройки Symantec Endpoint Protection 12

Характерной чертой 12-й версии антивируса Symantec Endpoint Protection является запись всех происходящих в системе событий в журналы. К примеру, в **Журнале защиты от изменений** фиксируются все сведения о попытках изменить приложения Symantec на локальном компьютере (см. Рисунок 6.249). Функция защиты от изменений могла как заблокировать, так и зарегистрировать это в журнале.

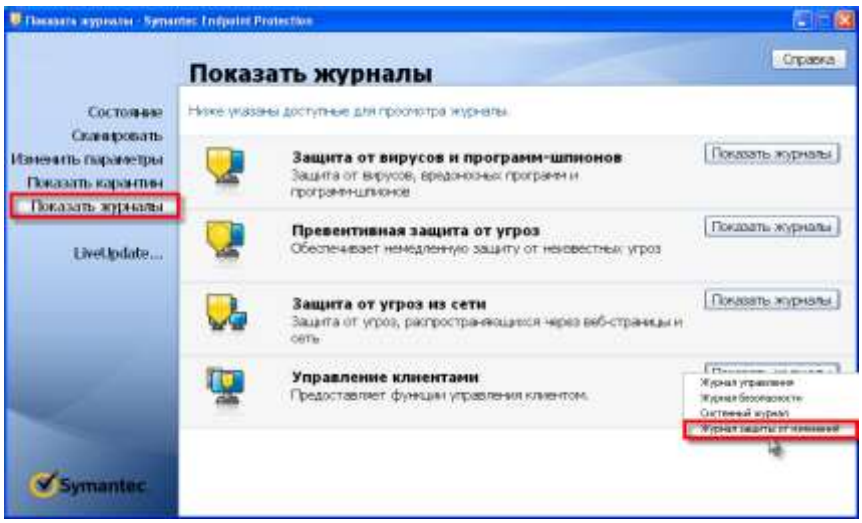


Рисунок 6.249

Просмотр журнала доступен обычному пользователю из консоли антивируса, где тот может видеть процессы, создающиеся при работе EndpointController (см. Рисунок 6.250).

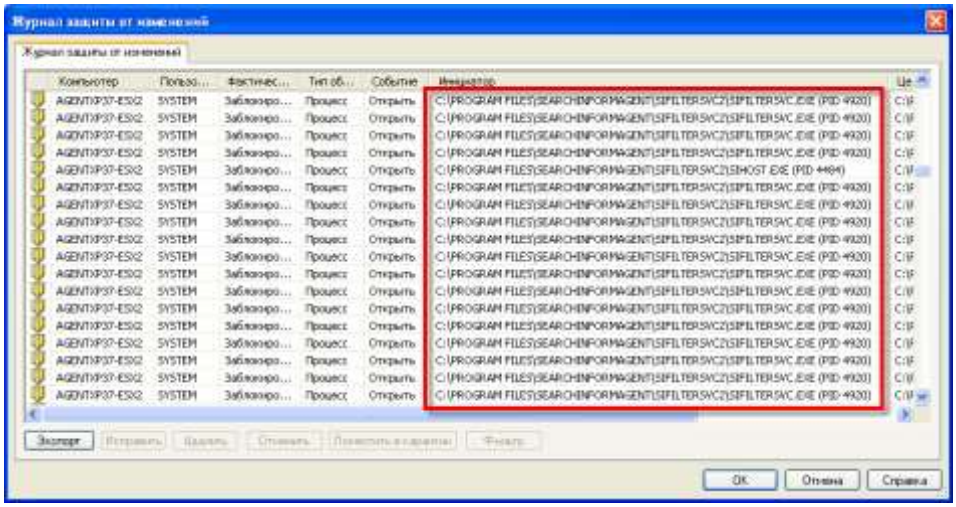


Рисунок 6.250

Существует несколько решений данной проблемы:

1. Отключить защиту программ Symantec от изменения или завершения. Порядок действий показан на Рисунок 6.251 и Рисунок 6.252.

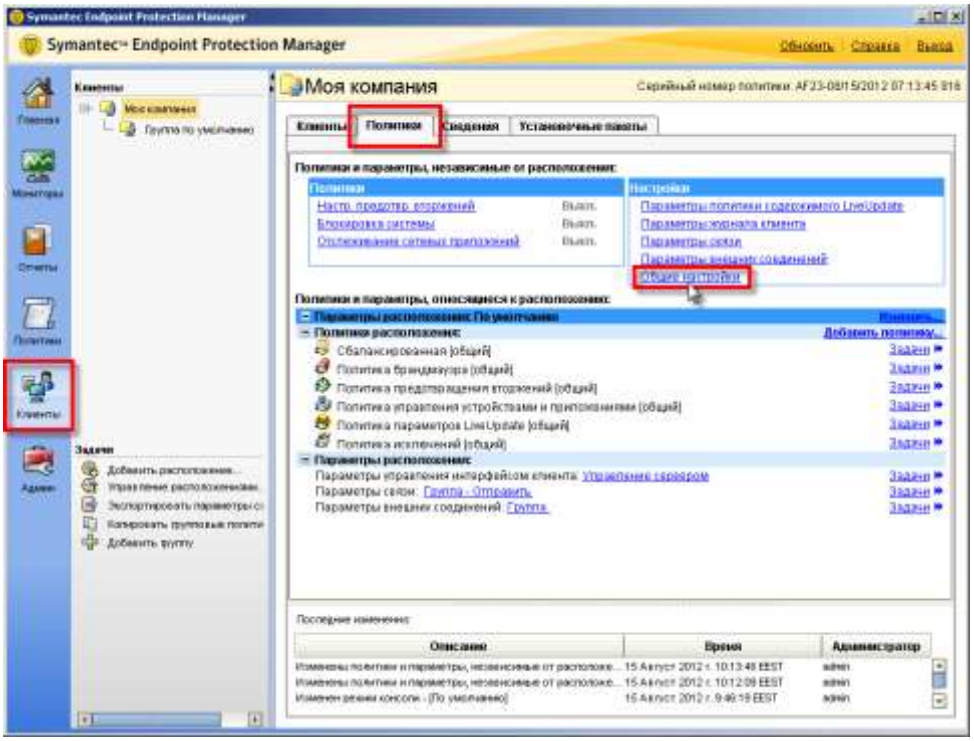


Рисунок 6.251

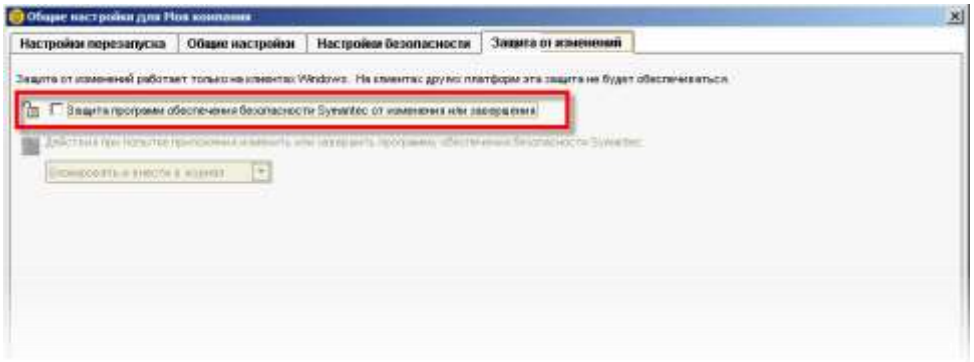


Рисунок 6.252

2. Отключить введение журнала (см. Рисунок 6.253).

Рисунок 6.253

3. Запретить пользователям просмотр журналов (см. Рисунок 6.254, Рисунок 6.255, Рисунок 6.256).

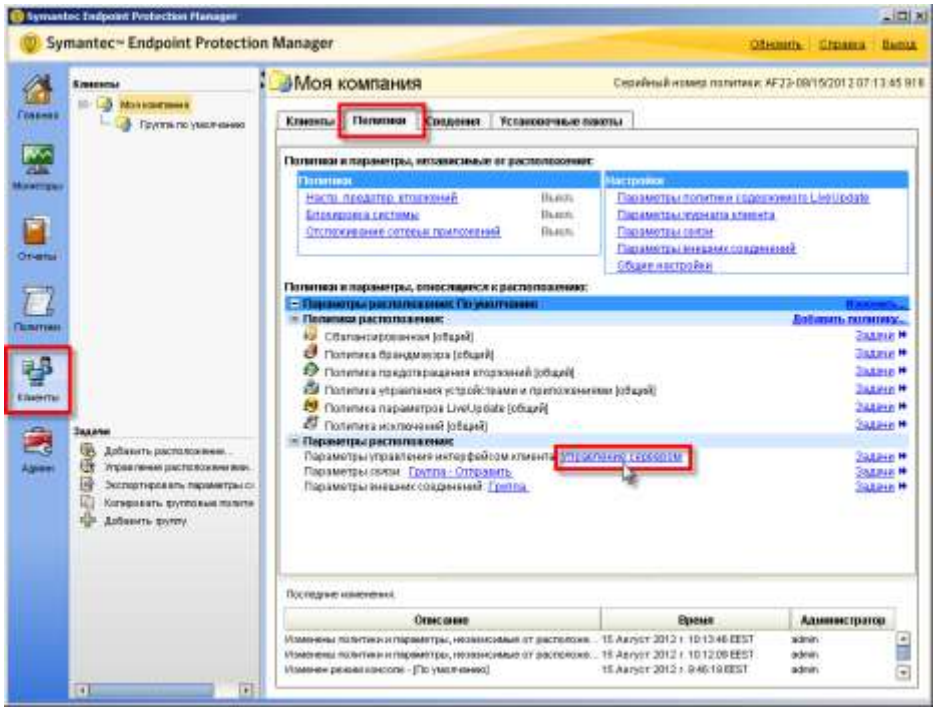


Рисунок 6.254

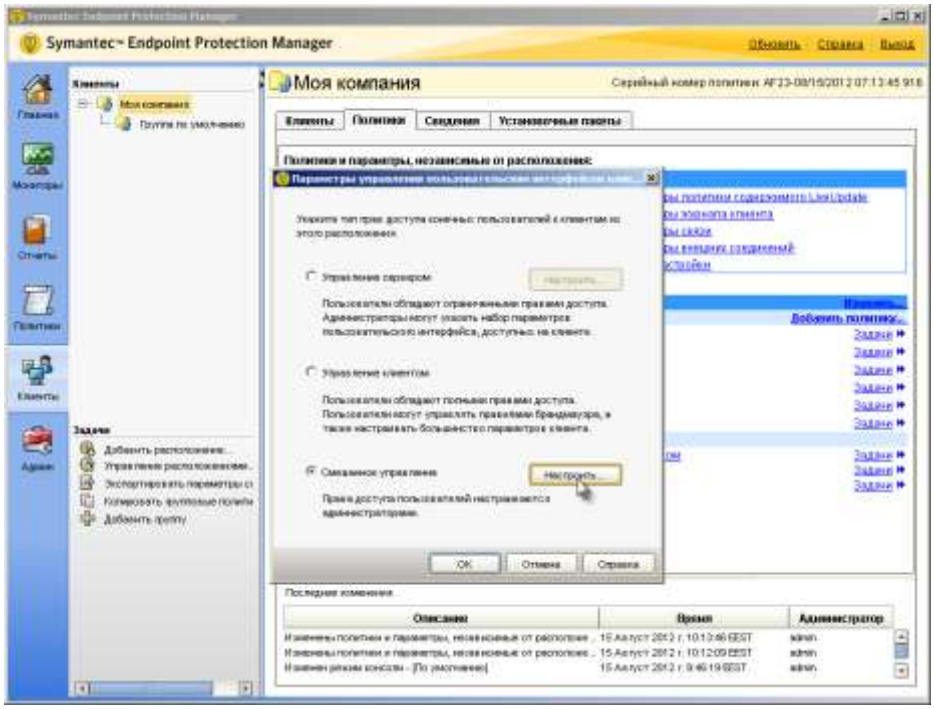


Рисунок 6.255

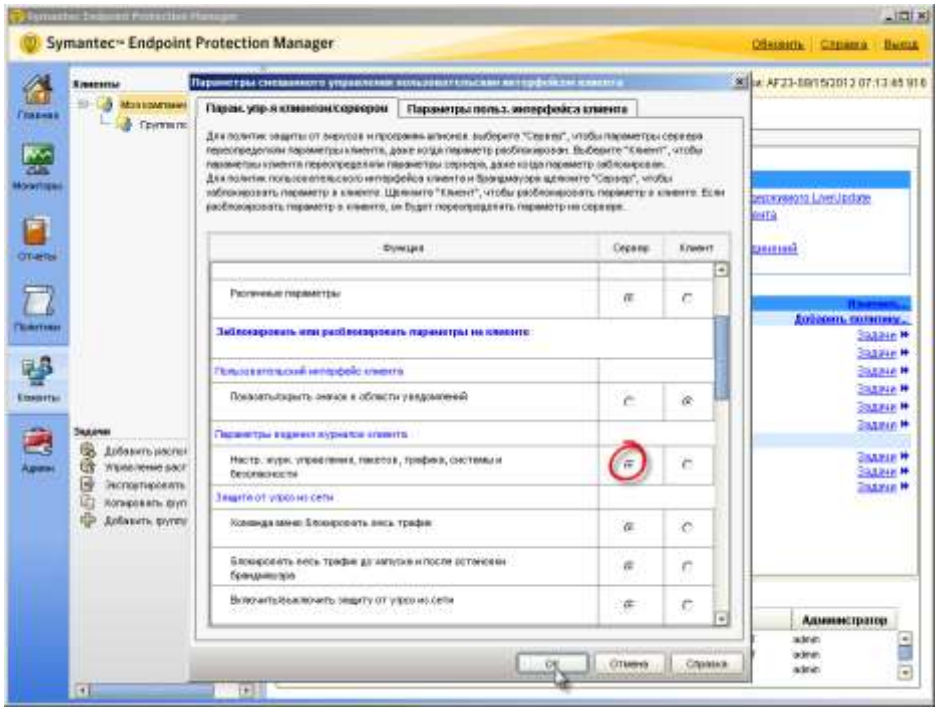


Рисунок 6.256

6.6 Настройка EndpointController Hub

Модуль EndpointController Hub предназначен для использования в территориально разделённых компаниях с филиалами, в каждом из которых небольшое количество рабочих станций и/или «узкий» канал связи с головным офисом.

Схема работы модуля следующая: данные перехватываются агентами и собираются на сервере EndpointController Hub. На сервере происходит фильтрация, обработка, сжатие и шифрование данных. Затем, в соответствии с заданным расписанием, перехваченная информация передается на основной сервер EndpointController для дальнейшей обработки.

С помощью консоли EndpointController можно производить подключение и удалённую настройку Hub-серверов. Управление осуществляется с помощью узла «Сетевое окружение».

В списке рабочих станций серверы EC Hub и компьютеры, контролируемые с помощью EC Hub, выделяются в отдельную группу под названием «EndpointController Hubs» (должен быть выбран тип отображения «Группы и компьютеры»). Серверы EC Hub обозначаются иконкой .

Для подключения EC Hub выберите необходимый сервер в списке компьютеров и щёлкните «Подключиться» в нижней части консоли (см. Рисунок 6.257).

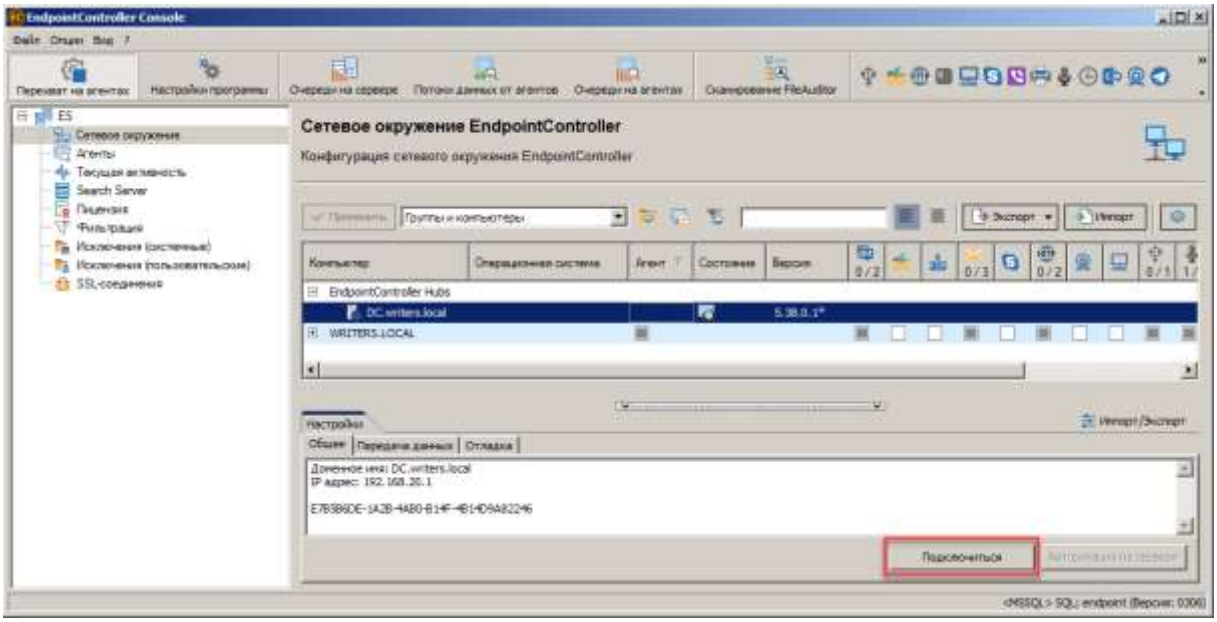


Рисунок 6.257

В результате подключения EC Hub должен появиться в списке серверов в левой части консоли (см. Рисунок 6.258).

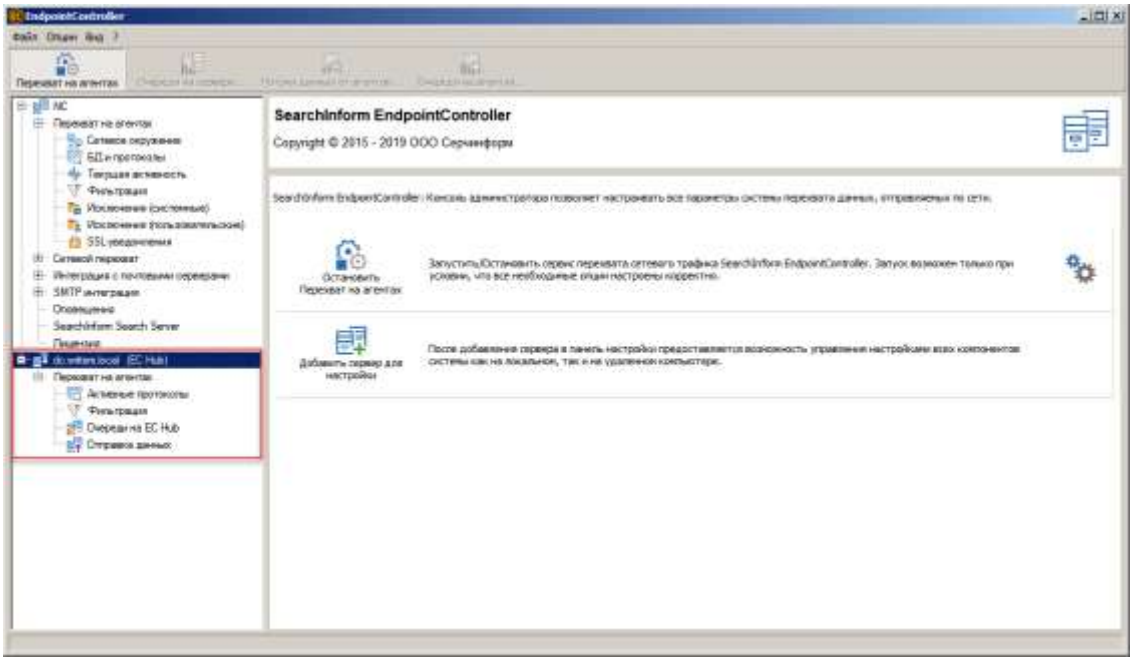


Рисунок 6.258

Настройка передачи перехваченных данных через сервер EC Hub осуществляется на вкладке «Сетевое окружение». Выберите в списке рабочих станций группу или компьютер и примените команду контекстного меню **Инструменты** → **Передавать перехват через EC Hub...** (см. Рисунок 6.259).

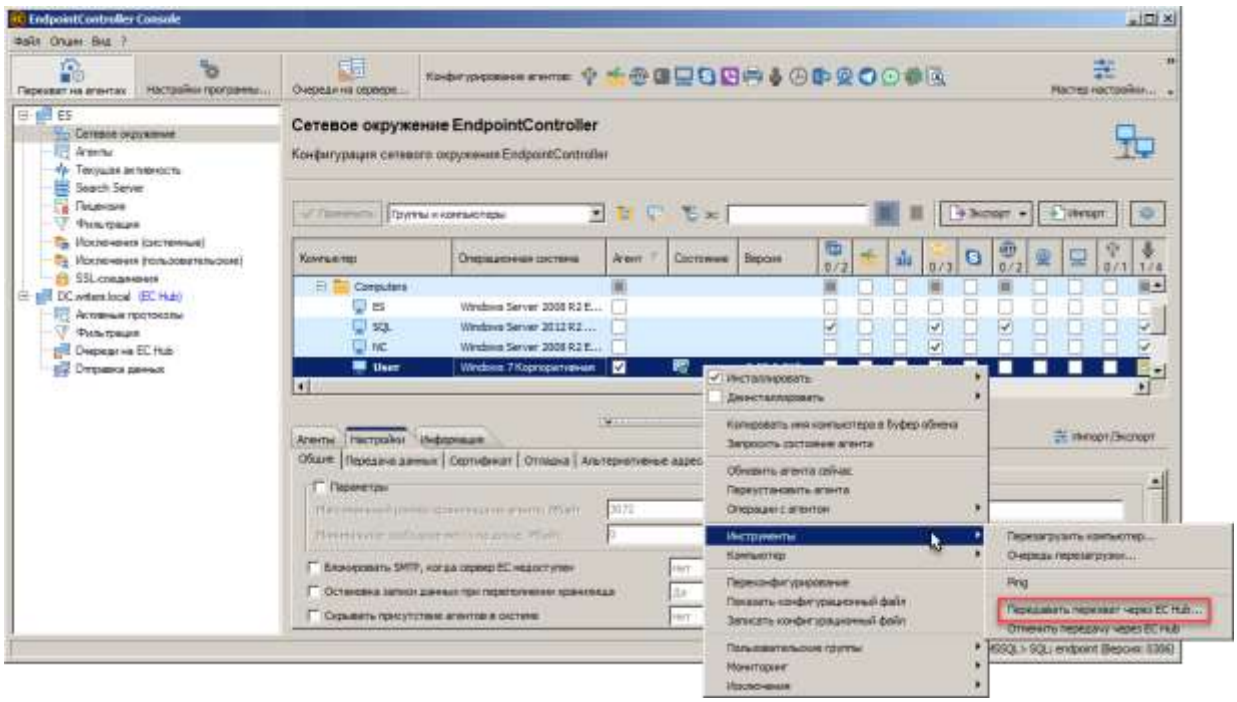


Рисунок 6.259

В открывшемся окне выберите необходимый сервер EC Hub и щёлкните «ОК» для применения настроек.

Указанный сервер EC Hub будет назначен приоритетным для выбранных рабочих станций. Щёлкните кнопку «Применить» в консоли для сохранения изменений (см. Рисунок 6.260).

Рисунок 6.260

Настройка параметров передачи данных с Hub-серверов на основной сервер EndpointController осуществляется на вкладке «Передача данных», расположенной в правой нижней части узла «Сетевое окружение».

Параметр «Широковещательная рассылка уведомлений агентам» позволяет рассылать агентам broadcast-уведомления, содержащие данные об адресе/порте Hub-

сервера. Агент, получивший такое уведомление, будет использовать адрес указанного сервера EndpointController Hub. С помощью выпадающего меню «Сетевой адрес рассылки» можно выбрать интерфейс, через который будут отправляться уведомления (см. Рисунок 6.261).

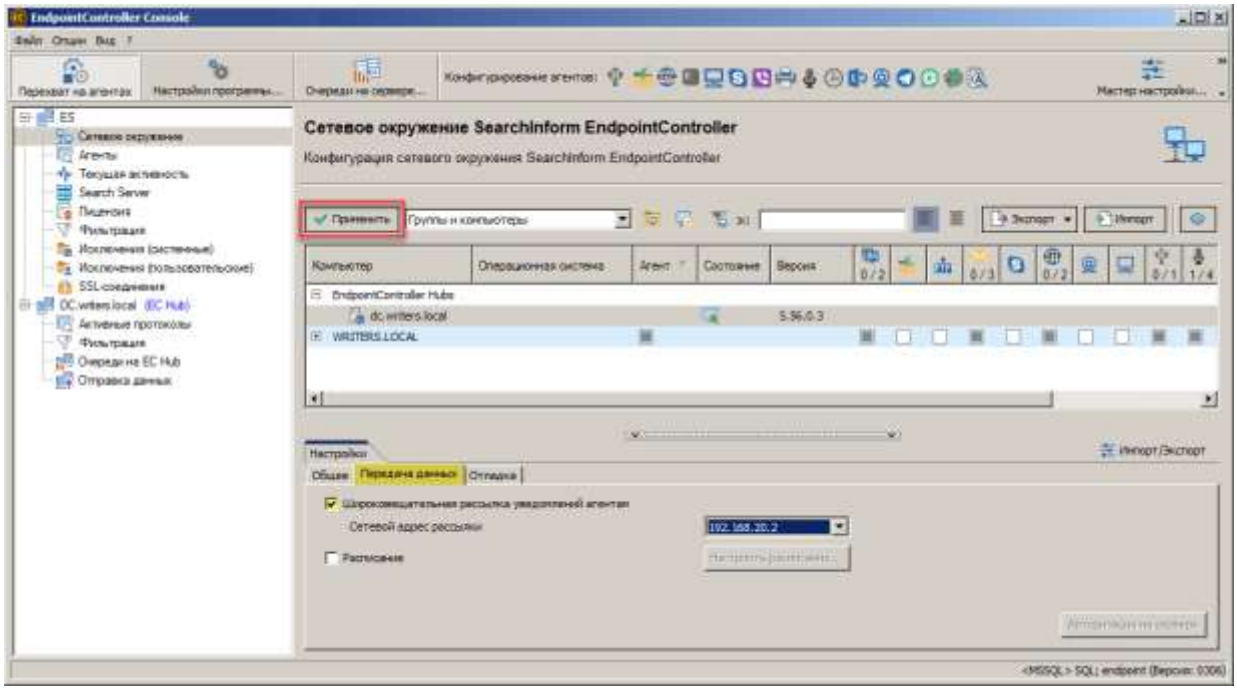


Рисунок 6.261

Для включения расписания передачи данных на сервер EndpointController отметьте флажком параметр «Расписание». Для задания параметров расписания щёлкните кнопку «Настроить расписание...» (см. Рисунок 6.262).

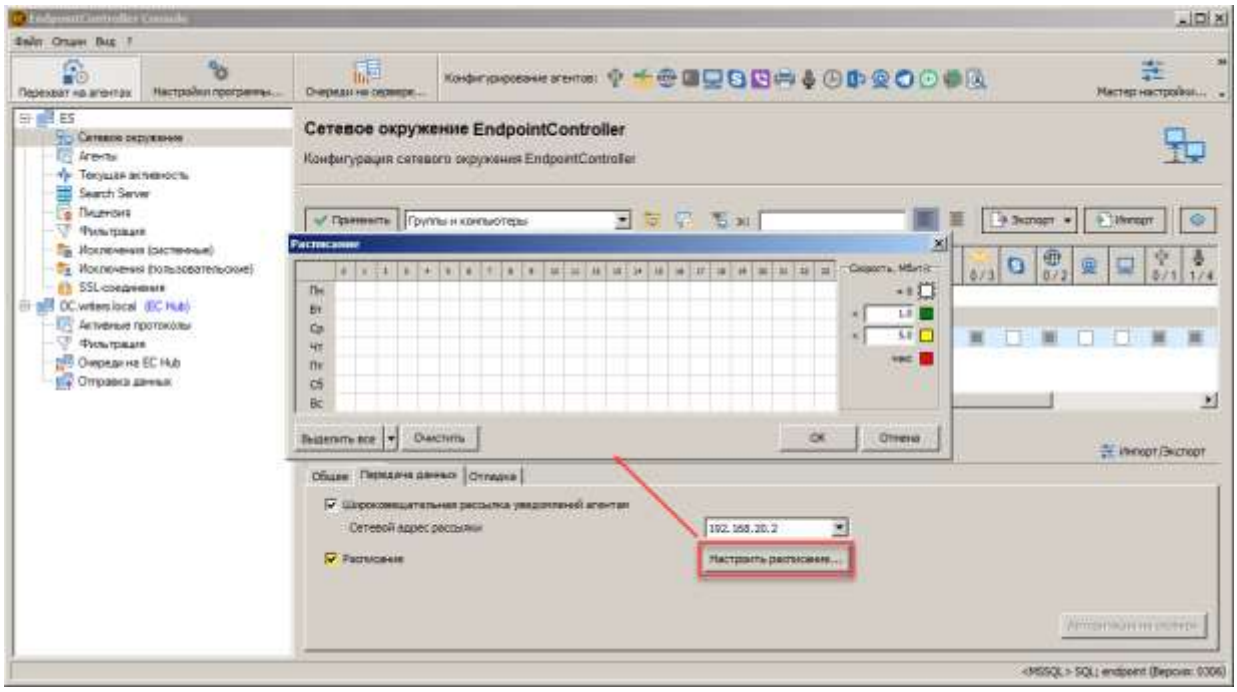


Рисунок 6.262

В открывшемся диалоговом окне задайте временной промежуток (начало, окончание, дни недели) и порог максимальной скорости передачи. Для двух цветовых меток возможно указать скорость вручную.

Соответствие цветов и порогов скорости приведено в легенде в правой части окна (см. Рисунок 6.263).

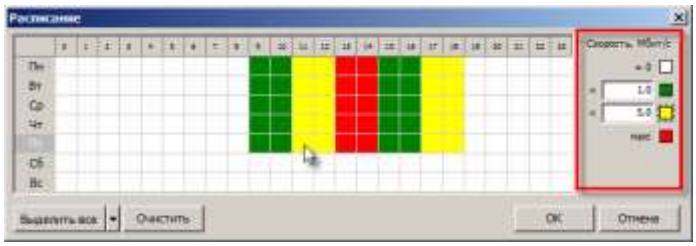


Рисунок 6.263

Выделение необходимых интервалов и выбор максимальной скорости передачи осуществляется с помощью мыши. Щёлкните по иконке необходимого цвета в правой части окна, а затем кликните по ячейке таблицы. Ячейка приобретет выбранный цвет.

После настройки расписания щёлкните «ОК».

Щёлкните «Применить» для сохранения заданных настроек передачи данных.

6.7 Установка и настройка модуля Database Monitor

Модуль Database Monitor позволяет контролировать запросы пользователей к базам данных и ответы на них (поддерживаемые СУБД: MS SQL Server, PostgreSQL Server).

Примечание! Для работы модуля Database Monitor на контролируемом SQL-сервере необходимо наличие установленной **службы SIDBMonitorSvc** и включенной службы Windows **«Удаленный реестр»**.

6.7.1 Установка Database Monitor

Служба прокси-сервера Database Monitor может быть установлена:

- ***на севере EndpointController*** в том случае, если на этом же сервере установлен контролируемый SQL-Server (см. п. 6.7.1.1).

- ***на отдельном сервере***, запросы и ответы которого необходимо контролировать. Такой вариант удобно использовать, если в сети имеется несколько контролируемых SQL-серверов, на каждый из которых необходимо установить прокси-сервер, или SQL-сервер установлен отдельно от сервера EndpointController (см. п. 6.7.1.2).

6.7.1.1 Установка Database Monitor совместно с EndpointController

Установка осуществляется из инсталляционного файла **SI_EndpointController_X.X.X.X.exe**[30].

На шаге выбора устанавливаемых компонентов отметьте пункт «Служба Database Monitor» и «Вкладка Database Monitor» (см. Рисунок 6.264).

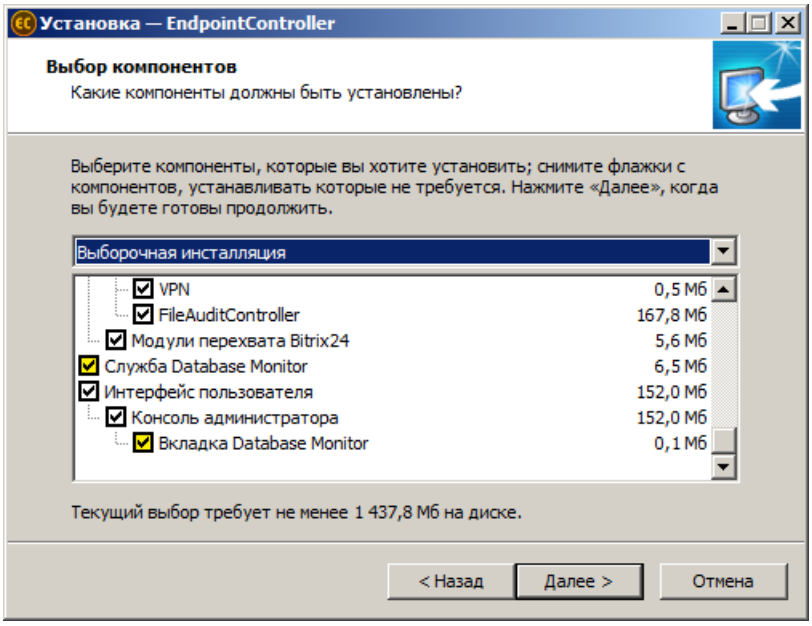


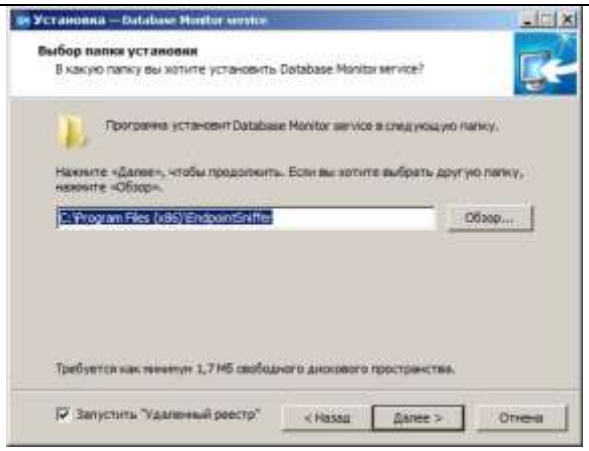
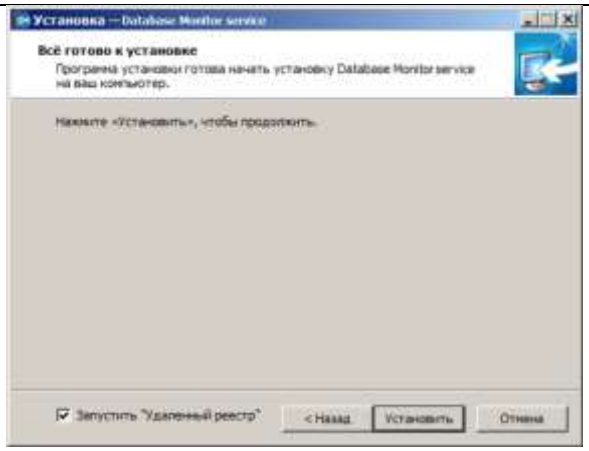
Рисунок 6.264

В конце процесса установки EndpointController автоматически будет запущен инсталлятор службы Database Monitor. Процесс установки службы Database Monitor представлен в Таблица 33.

Таблица 33 – Инструкция по установке службы Database Monitor

Страница мастера	**Интерфейс (поле или свойство)**	**Действие или описание настроек**
Выбор языка мастера	«Выберите язык»	«Русский»
Лицензионное соглашение	«Прочитайте лицензионное соглашение»	Ознакомьтесь с текстом и выберите «Я принимаю условия соглашения»

[30] Загрузить дистрибутив можно по ссылке, полученной от инженеров технической поддержки.

Страница мастера	Интерфейс (поле или свойство)	Действие или описание настроек
Папка установки		Введите путь к папке на жёстком диске вручную или воспользуйтесь кнопкой «Обзор» и выберите папку в обозревателе. Для работы службы Database Monitor необходим запуск службы «Удаленный реестр» (параметр должен быть отмечен флажком!).
Завершение работы Мастера		Отображается совокупность произведённых настроек для установки модуля. Щёлкните кнопку «Установить».

Примечание! *После установки служба запускается под системной учетной записью. Если Database Monitor и контролируемая СУБД расположены на разных серверах, и Database Monitor использует аутентификацию Windows, то для службы SIDBMonitorSvc необходимо указать учетную запись, обладающую:*

- *правами локального администратора,*
- *правом просмотра состояния сервера СУБД,*
- *правом подключения к СУБД,*
- *правом просмотра баз данных СУБД.*

6.7.1.2 Установка Database Monitor на отдельную машину

Установка осуществляется из отдельного дистрибутива самой службы **SI_DBMonitorSvc_X.X.X.X.exe**[31] (процесс установки службы Database Monitor представлен в Таблица 33).

[31] Загрузить дистрибутив можно по ссылке, полученной от инженеров технической поддержки.

6.7.2 Настройка модуля Database Monitor

Для работы службы Database Monitor необходимо настроить параметры подключения к прокси-серверу. Для этого перейдите на вкладку **Database Monitor → Настройки**.

Для добавления прокси-сервера в список нажмите кнопку «Добавить» (см. Рисунок 6.265).

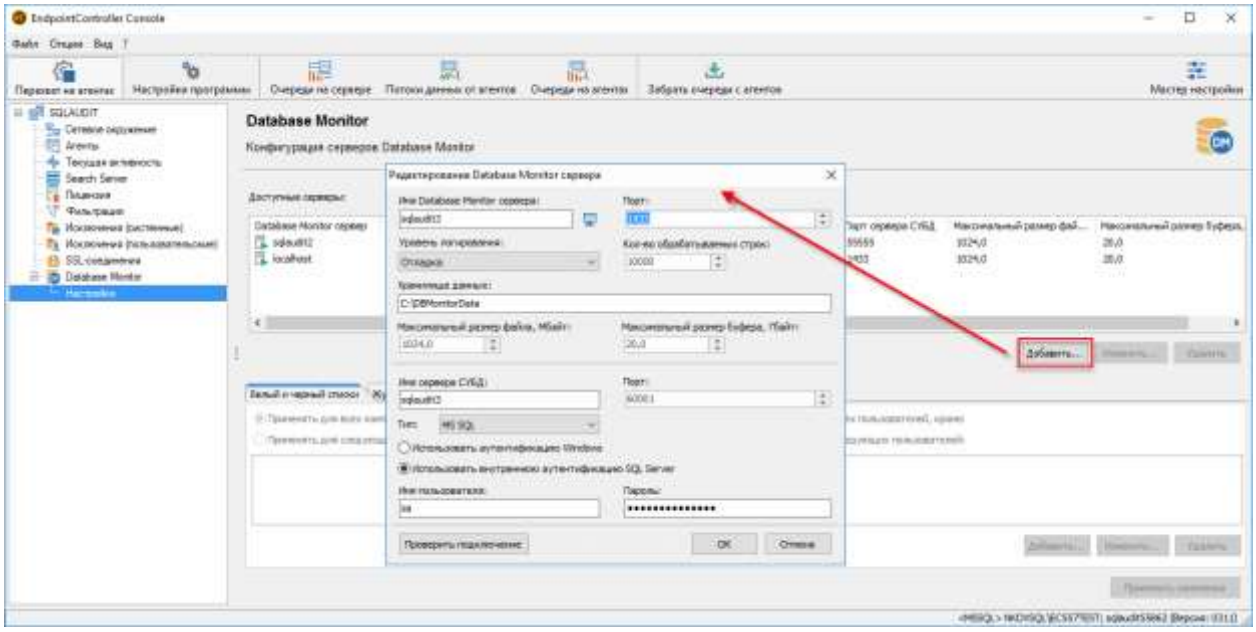


Рисунок 6.265

В появившемся окне «Редактирование сервера» настройте параметры подключения. Параметры и их значения приведены в Таблица 34.

Таблица 34 – Настройка параметров Database Monitor

Параметр	Значение
Параметры подключения к прокси-серверу	
Имя Database Monitor сервера	Наименование компьютера с установленной службой Database Monitor
Порт	Номер порта, используемый для подключения к прокси-серверу
Уровень логирования	В зависимости от выбранного уровня логирования меняется степень детализации содержимого лог-файлов. Доступные для выбора уровни логирования службой прокси-сервера: • Минимальный; • Нормальный, • Подробный, • Отладочный.
Кол-во обрабатываемых строк	Максимальное количество строк для запросов/ответов

Хранилище данных	Директория для хранения перехваченных запросов и ответов СУБД
Максимальный размер файла, Мбайт	Максимально допустимый размер файлов, в которые записываются перехваченные запросы
Максимальный размер буфера, Гбайт	Максимально допустимый размер хранилища перехваченных запросов. *Запись файлов в хранилище осуществляется циклически: при достижении максимального объема хранилища 'старые' файлы удаляются, и на их место записываются 'новые' файлы перехвата. При этом остается доступным поиск по удаленным файлам, если они были проиндексированы Search Server'ом.*
Параметры подключения к SQL-серверу	
Имя сервера СУБД	Наименование сервера баз данных, запросы и ответы которого необходимо контролировать
Порт	Номер порта контролируемого сервера СУБД
Использовать аутентификацию Windows	При аутентификации будут использоваться параметры учетной записи Windows
Использовать внутреннюю аутентификацию MS SQL Server	При аутентификации будут использоваться встроенные в MS SQL Server параметры (потребуется ввод Имени пользователя и Пароля)

Для проверки соединения используйте кнопку «Проверить подключение». При успешном подключении добавленный сервер появится в списке.

Статус состояния сервера отображается в столбце «Database Monitor сервер» соответствующей иконкой:

- запущен;
- остановлен;
- ошибки в работе сервера (например, отсутствует подключение к СУБД).

Для редактирования параметров подключения к прокси-серверу выделите его в списке доступных серверов и нажмите кнопку «Изменить», для удаления - кнопку «Удалить» (см. Рисунок 6.266).

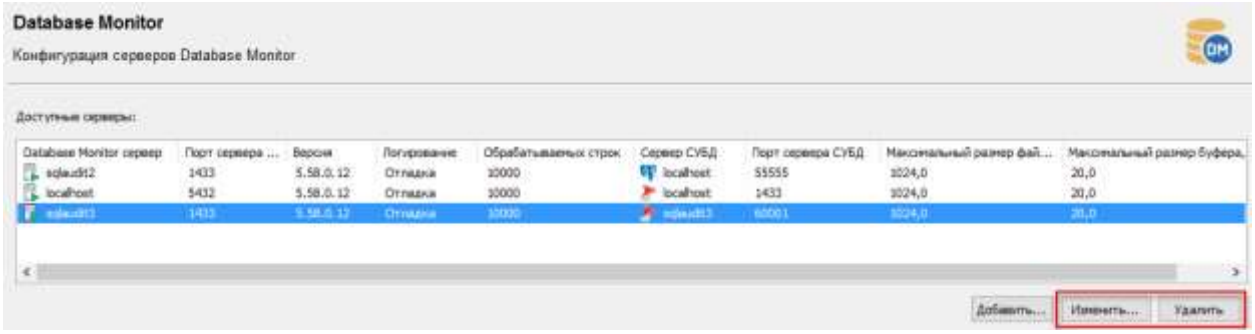


Рисунок 6.266

Запуск/остановка службы Database Monitor осуществляется с помощью команд контекстного меню (см. Рисунок 6.267).

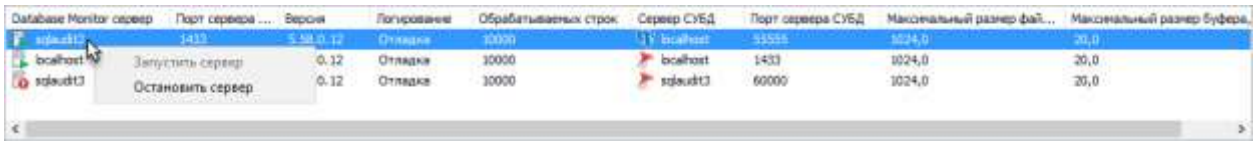


Рисунок 6.267

Для ограничения компьютеров/пользователей, контролируемых выбранным в списке сервером, настройте 'белый/черный' список, используя кнопку «Добавить»(см. Рисунок 6.268).

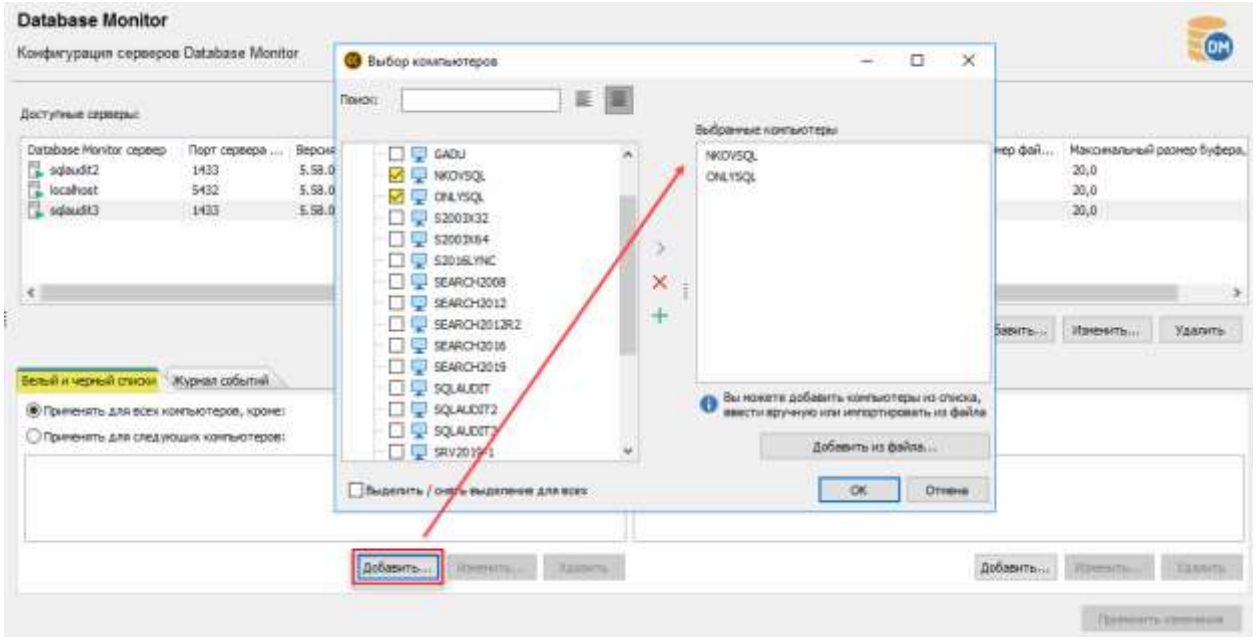


Рисунок 6.268

Для редактирования списка предназначена кнопка «Изменить», для удаления компьютеров/пользователей из списка - кнопка «Удалить».

Для сохранения настроек нажмите кнопку «Применить изменения».

После этого необходимо выбрать контролируемые базы данных (см. п. 6.7.3).

6.7.3 Выбор контролируемых баз данных

Для выбора баз данных, запросы к которым необходимо перехватывать, а также мониторинга их состояния перейдите в раздел **Database Monitor** и нажмите кнопку **«Выбрать БД»** (см. Рисунок 6.269).

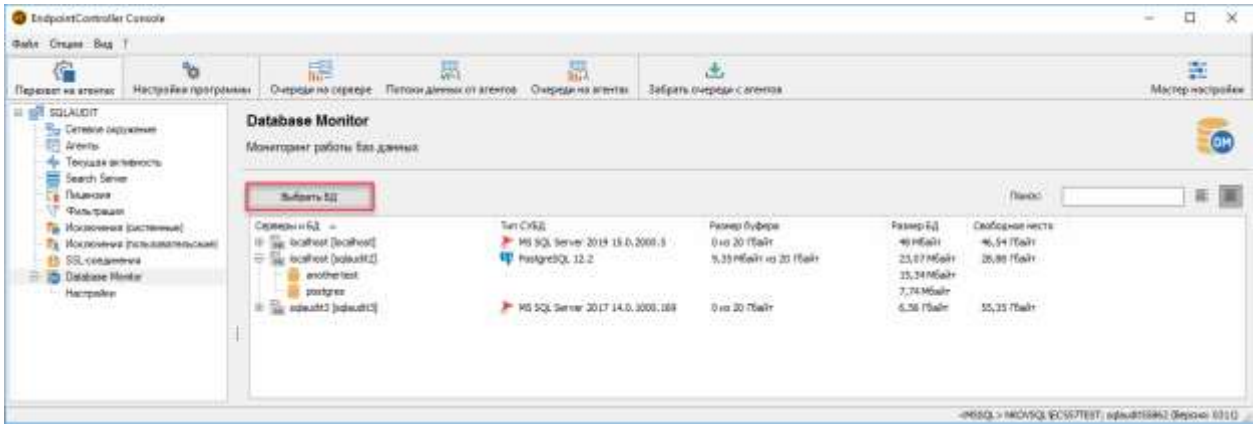


Рисунок 6.269

В появившемся окне отметьте флажками базы данных, запросы и ответы которых необходимо контролировать, и нажмите **ОК**. (см. Рисунок 6.270).

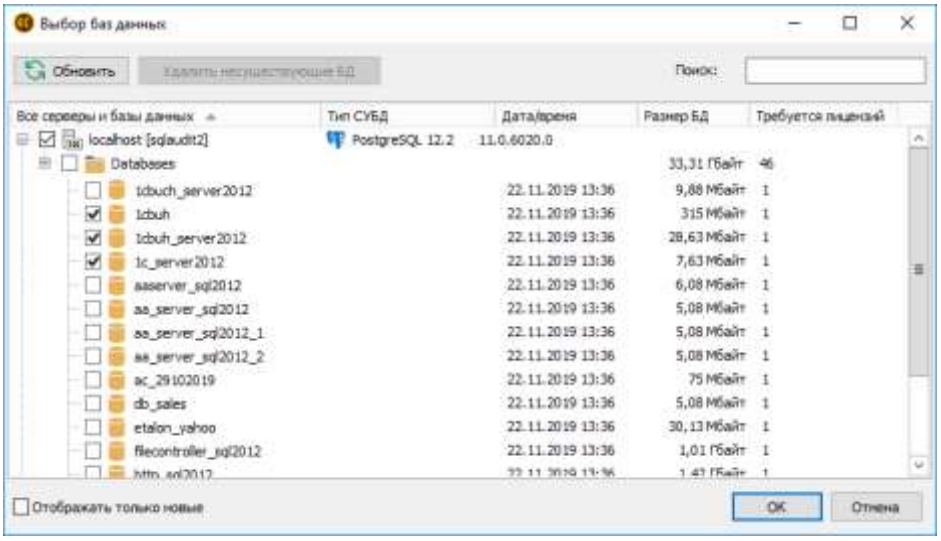


Рисунок 6.270

Выбранные БД будут отображены в списке.

Примечание! *При смене сервера СУБД или добавлении нового сервера Database Monitor, базы данных будут отображены в списке спустя непродолжительное время (до 200 секунд).*

Новые базы данных, создаваемые на контролируемых серверах, маркируются в списке словом *new!*. Щелчком по узлу разверните содержимое сервера для обнаружения новых баз данных (см. Рисунок 6.271).

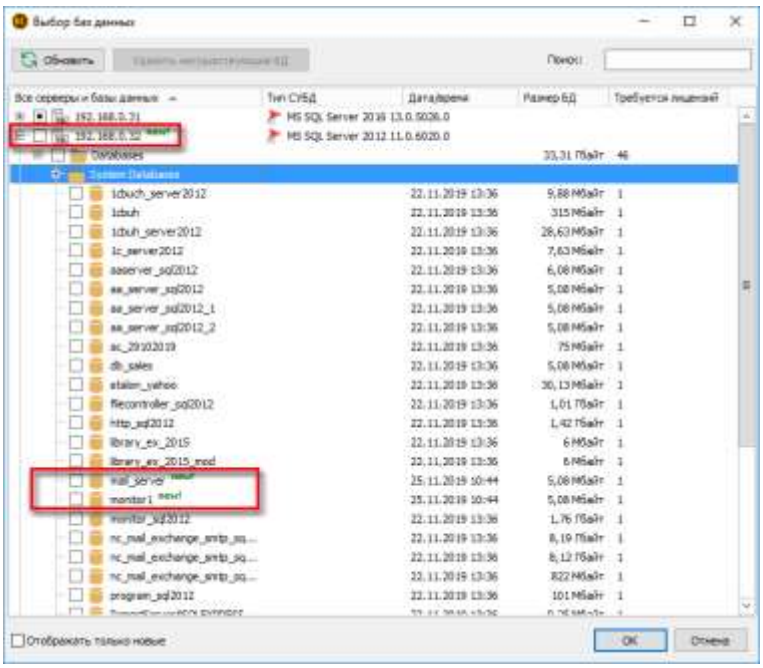


Рисунок 6.271

Для отображения в списке только новых баз данных установите флажок напротив параметра «Отображать только новые», расположенного в нижней части окна.

6.7.4 Настройка MS SQL Server для работы с Database Monitor

Для работы Database Monitor как службы-прокси, необходимо в настройках MS SQL Server изменить порт, через который будет передаваться трафик.

Для этого откройте MS SQL Server Configuration Manager, перейдите в раздел **Сетевая конфигурация SQL Server** → **Протоколы для MSSQLSERVER**, войдите в свойства протокола **TCP/IP** (см. Рисунок 6.272).

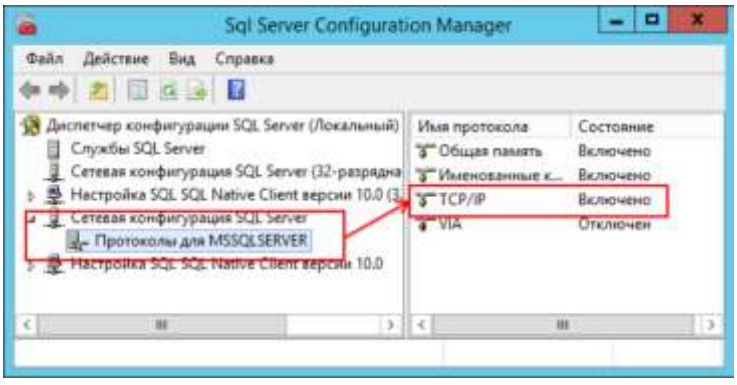


Рисунок 6.272

В свойствах TCP/IP перейдите на вкладку «IP-адреса» и укажите новый порт, на который будет настраиваться Database Monitor (см. Рисунок 6.273).

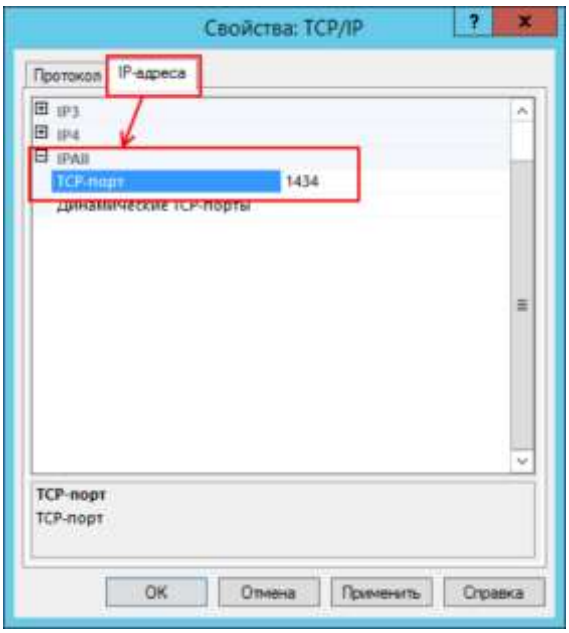


Рисунок 6.273

После применения изменений необходимо перегрузить службу MS SQL Server.

6.7.5 Настройка сервера PostgreSQL для работы с Database Monitor

Для изменения порта в установленной СУБД PostgreSQL отредактируйте файл **postgresql.conf**, расположенный в директории C:\Program Files\PostgreSQL\xx\data.

Измените значение строки **port = 5432**.

Сохраните изменения в файле конфигурации.

По завершении внесения изменений перезапустите службу сервера PostgreSQL.

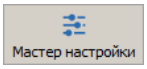
6.8 Настройка сервера Серчинформ NetworkController

Настройка NetworkController включает в себя следующие этапы:

- создание индексов, привязанных к базам данных/хранилищу;
- настройка фильтрации трафика;
- настройка механизма получения доменных имен.

Для быстрой настройки сервера NetworkController воспользуйтесь стандартным мастером.

Окно мастера быстрой настройки вызывается автоматически при первом запуске приложения, а также в случае отметки параметра «Отображать мастер настройки при запуске программы». Помимо этого, мастер может быть вызван вручную по нажатию

кнопки «Мастер настройки» 

в окне программы либо при помощи команды «Мастер настройки» в меню «Файл» (см. Рисунок 6.274).

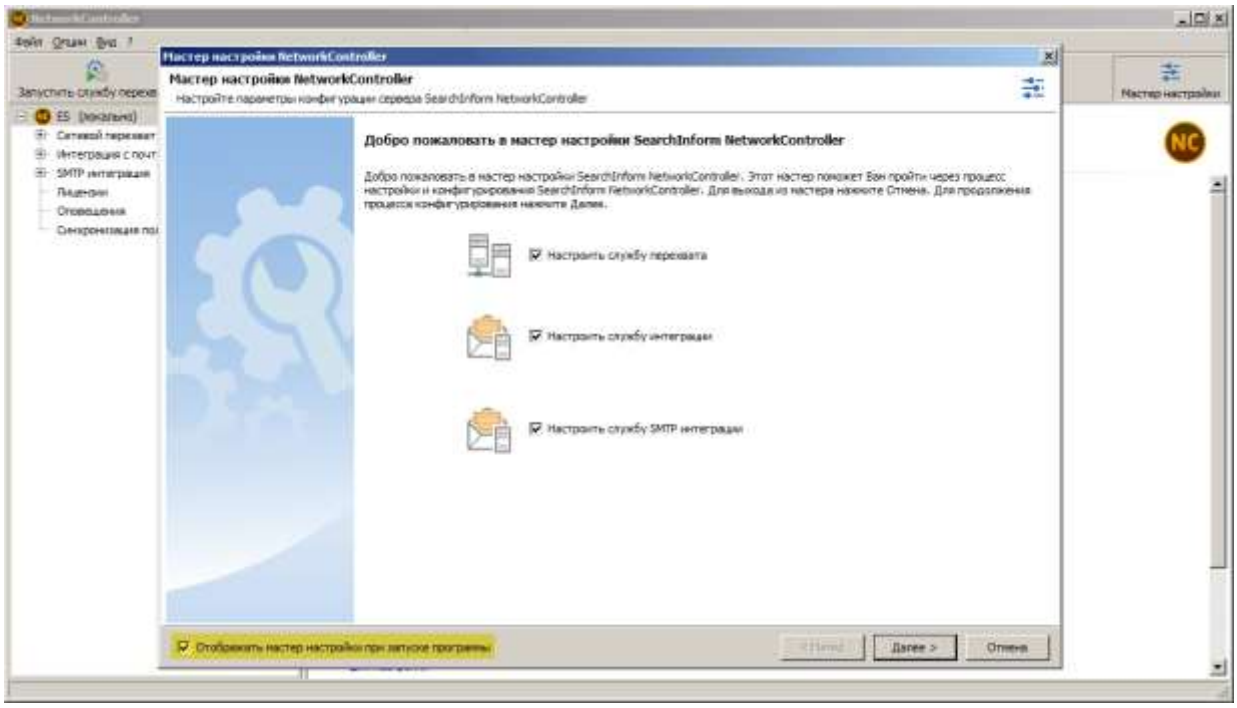
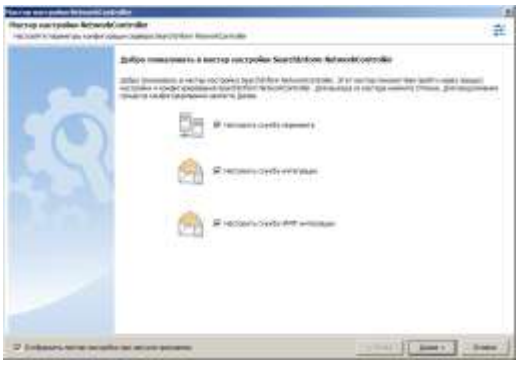
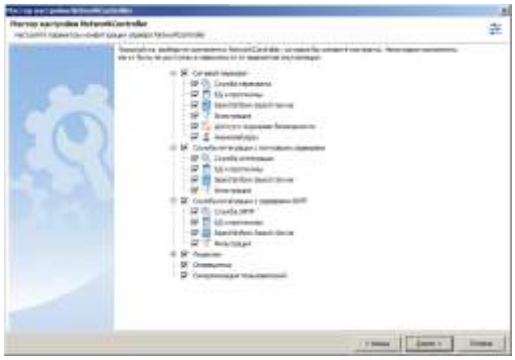


Рисунок 6.274

Шаги настройки NetworkController при помощи мастера описаны в Таблица 35.

Таблица 35 – Настройка NetworkController с помощью мастера

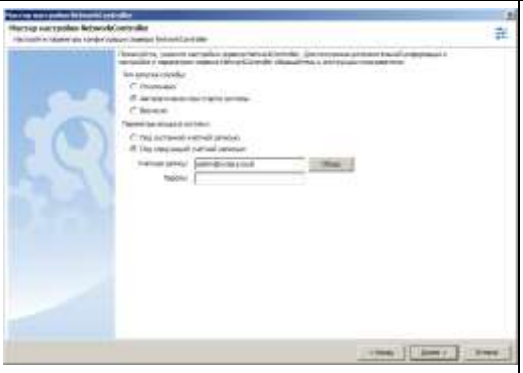
Страница мастера	Интерфейс	Настройка
Начальная страница		Для настройки перехвата на уровне сетевых шлюзов, установите флажок «**Настроить службу перехвата**». Для интеграции с почтовыми серверами (сбор сообщений напрямую с корпоративных почтовых серверов), установите флажок «**Настроить службу интеграции**». Для конфигурирования перехвата контейнеров с журналами от почтового сервера, установите флажок «**Настроить службу интеграции SMTP**». Для автоматического запуска мастера установки при открытии программы, установите флажок

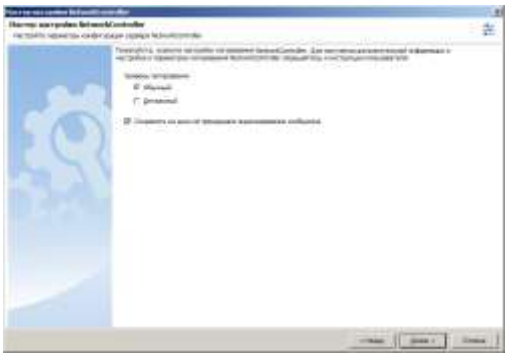
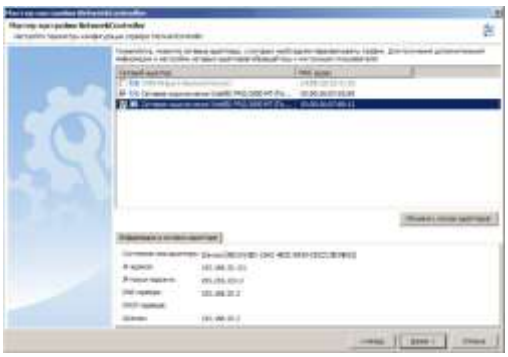
Страница мастера	Интерфейс	Настройка
		напротив параметра «**Отображать мастер настройки при запуске программы».**
Выбор компонентов		Выберите настраиваемые компоненты NetworkController. По умолчанию выбраны все позиции. При отмене выбора позиции, мастер пропустит страницы с набором соответствующих настроек.

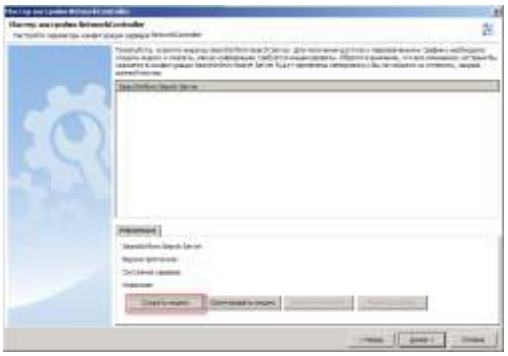
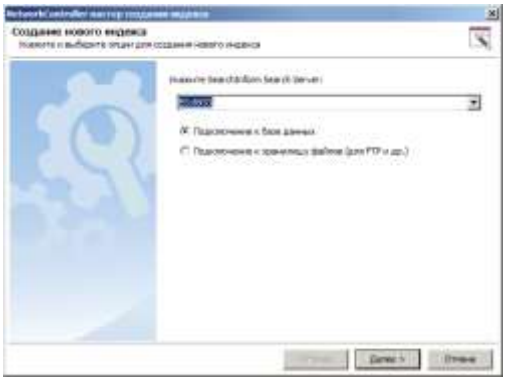
6.8.1 Настройка параметров сетевого перехвата при помощи мастера

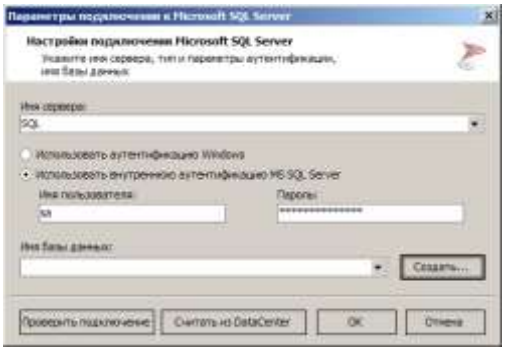
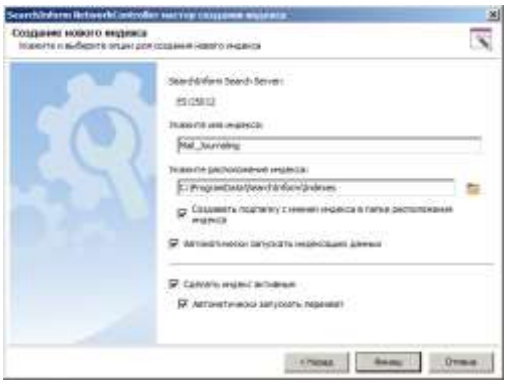
Сетевой перехват настраивается, если данные нужно получать путём перехвата на уровне сетевых шлюзов. Настройка параметров сетевого перехвата при помощи мастера производится в порядке, изложенном в Таблица 36.

Таблица 36 – Пошаговая настройка сетевого перехвата NetworkController при помощи мастера

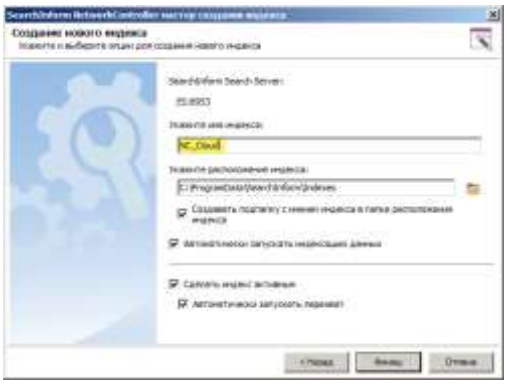
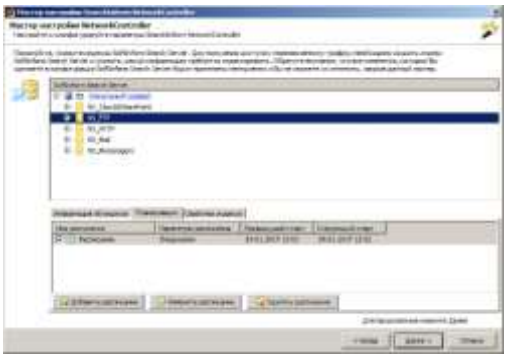
Страница мастера	Интерфейс	Настройка
Настройки запуска службы перехвата		Рекомендуется выбрать «**Тип запуска службы**»: «Автоматически при старте операционной системы». Настройте учетную запись, под которой будет работать служба сетевого перехвата **sinssvc.exe**: для этого введите имя и пароль доменного пользователя, облажающего правами входа в качестве службы и правами чтения журналов безопасности (системная учетная запись таких прав не имеет). Рекомендуемый формат доменного имени: **user@domain.local**.

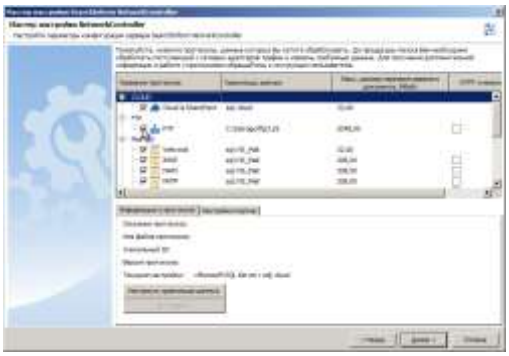
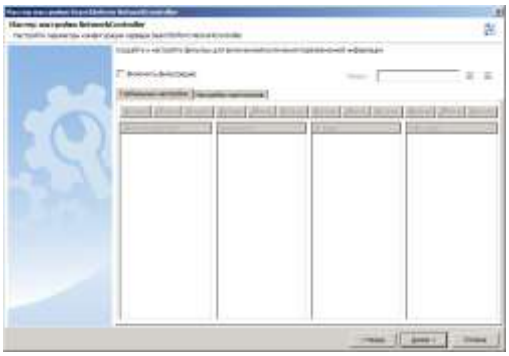
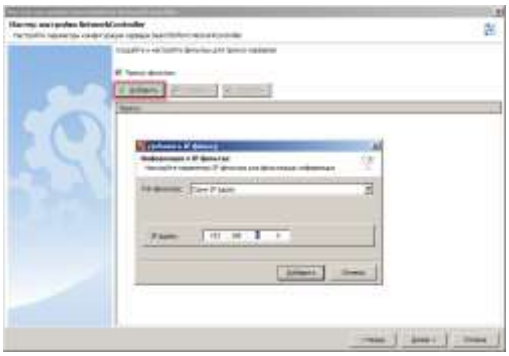
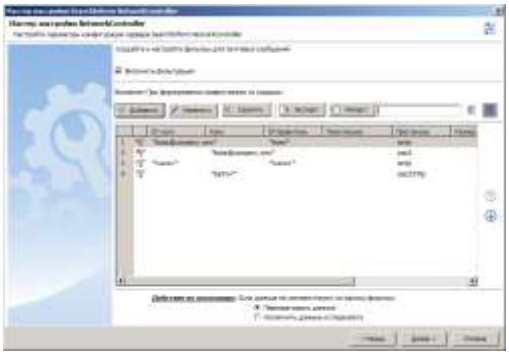
Страница мастера	Интерфейс	Настройка
Выбор уровня логирования		Укажите уровень логирования: • **Обычный** – фиксируются серьезные ошибки службы синхронизации и консоли управления сервером, повлекшие прерывание или аварийное завершение работы приложения; запуск внутренних функций программы; • **Детальный** – дополнительно фиксируется запуск внутренних функций программы в подробном виде. Рекомендуется включать данный режим только по запросу сотрудников службы технической поддержки в случае критических проблем с программным обеспечением.
Выбор сетевых адаптеров		Отметьте сетевые адаптеры, на которые поступает перенаправленный трафик. В свойствах выбранных сетевых карт должны быть отключены все offload-параметры с целью предотвращения потери пакетов. Подробнее… Зачастую в списке адаптеров сетевого перехвата присутствует WAN Miniport. Его следует использовать лишь в случае, когда NetworkController получает данные в режиме интеграции от сервера ISA/TMG. В этом случае флажком отмечается только WAN-порт, поскольку консоль требует, чтобы перехват был включен хотя бы на одном адаптере. С реальных сетевых карт флажки должны быть сняты. В остальных ситуациях перехват трафика с WAN-порта не требуется, поэтому можно снять с него флажок.

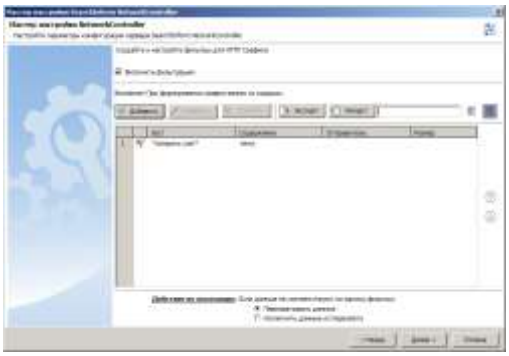
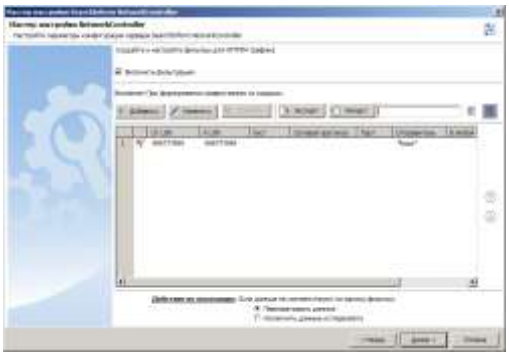
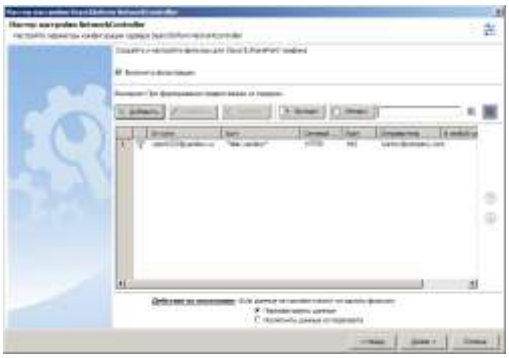
Страница мастера	Интерфейс	Настройка
Настройка ICAP		Для активации настроек интеграции сервера NetworkController с прокси-серверами, работающими по протоколу ICAP, установите флажок «ICAP». Укажите IP-адрес сервера NetworkController и номер ICAP-порта. При интеграции с прокси-серверами по протоколу ICAP становится возможной функция блокировки передачи данных по HTTP(S)-протоколу. Подробнее о блокировке…
Настройка индексов		Окно отображает список индексов и привязанные к ним протоколы. Для создания нового индекса щелкните кнопку «**Создать индекс**».
Настройка индексов:начальная страница создания индекса (1)		Введите имя или IP-адрес сервера индексации Search Server. Отметьте флажком, к чему настраивается подключение: к базе данных или хранилищу файлов.

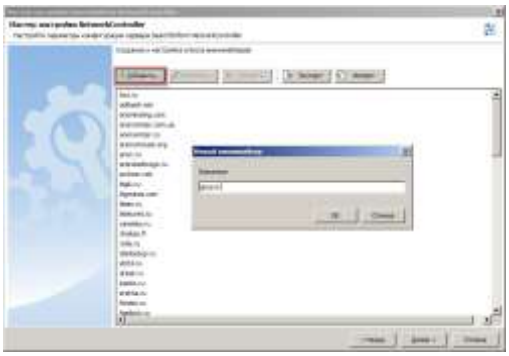
Страница мастера	Интерфейс	Настройка
Настройка индексов: подключение к серверу баз данных. Создание базы данных (2_A)	  	Настройте подключение к базе данных: введите имя или IP-адрес сервера баз данных, тип аутентификации (Windows или внутренняя MS SQL[32]), выберите базу данных из впадающего списка. Если нужной БД нет, щелкните кнопку «Создать». Введите имя создаваемой БД. Измените настройки по умолчанию, если требуется. Нажмите «ОК». Появится сообщение «**База данных успешно создана**».
Настройка индексов: подключение к базе данных: Привязка созданной БД к протоколам (3_A)	 	Отметьте протоколы, которые следует включить в индекс. При перехвате данных по указанным протоколам, NetworkController будет складывать сообщения в подключенную БД. Нажмите «Далее». Введите имя индекса и выберите директорию, по которой индекс будет храниться. Установите флажок «Автоматически запускать перехват».

[32] В случае использования внутренней аутентификации MS SQL введите имя и пароль пользователя.

Страница мастера	Интерфейс	Настройка
Настройка индексов: подключение к хранилищу файлов (2_Б)		При выборе «**Подключение к хранилищу файлов (для FTP и др.)**»: В диалоговом окне «Настройка источника данных» щелкните по кнопке и выберите/создайте директорию для хранения данных, переданных либо принятых по протоколу FTP. Путь и имя файла хранилища можно также задать вручную. При создании нового каталога подтвердите запрос на его создание.
Настройка индексов: подключение к хранилищу файлов: Привязка созданного хранилища к протоколам (3_Б)		Для привязки хранилища данных к FTP-протоколу доступен только протокол FTP. Отметьте его флажком и нажмите «Далее».
		Введите имя индекса, выберите папку на жестком диске сервера индексации. Выберите дополнительные настройки: • «Сделать индекс активным». • «Автоматически запускать перехват». Завершите работу мастера нажатием кнопки «Финиш».
Настройка расписания обновления индексов		Созданный индекс отображается в списке. Повторите операции (1) – (3) для создания остальных индексов. Требуемый результат: отображается список индексов с привязанными к ним протоколами. Дополнительно можно настроить интервал обновления индекса. Для этого выделите индекс, откройте вкладку «Планировщик» и воспользуйтесь стандартным мастером Windows.

Страница мастера	Интерфейс	Настройка
Включение протоколов		Если перехват уже запущен (шаг «**Привязка созданной БД (хранилища) к протоколам (2_А или 2_Б)**»), дополнительных действий не требуется. Если перехват не запущен, включите протоколы перехвата.
Фильтрация по пользова-тельским атрибутам		В окне задаются глобальные настройки фильтрации и индивидуальные для отдельных протоколов. Подробнее о фильтрации по атрибутам пользователя в п. 6.8.5.1.
Фильтры для прокси-серверов		Оставьте настройки по умолчанию. Фильтрацию удобнее настраивать после завершения работы мастера. Подробнее о прокси фильтрах в п. 6.8.5.2.1.
Фильтрация почтовых сообщений		Оставьте настройки по умолчанию. Фильтрацию удобнее настраивать после завершения работы мастера. Подробнее о фильтрации по атрибутам сообщений в п. 6.8.5.2.2.

Страница мастера	Интерфейс	Настройка
Фильтрация по HTTP		Оставьте настройки по умолчанию. Фильтрацию удобнее настраивать после завершения работы мастера. Подробнее о фильтрации по HTTP в п. 6.8.5.2.3.
Фильтрация по HTTP IM		Оставьте настройки по умолчанию. Фильтрацию удобнее настраивать после завершения работы мастера. Подробнее о фильтрации по HTTP в п. 6.8.5.2.4
Фильтрация Cloud & SharePoint		Оставьте настройки по умолчанию. Фильтрацию удобнее настраивать после завершения работы мастера. Подробнее о фильтрации по HTTP в п. 6.8.5.2.5
Добавление учетных записей для доступа к журналам безопас-ности		В домене может быть несколько контроллеров домена, проводящих аутентификацию пользователей и обеспечивающих политику безопасности домена. Каждый контроллер домена обслуживает только свой домен. Подключение к контролерам домена может производиться от разных учетных записей. Щелкните кнопку «**Добавить**», укажите контроллер домена, полное имя пользователя в формате **<domain\user>** или **<user@domain.local>** и пароль для доступа к журналам безопасности.

Страница мастера	Интерфейс	Настройка
		При наличии проблем с соответствием имен доменов, на одноименной вкладке укажите короткие и полные имена доменов.
Настройка анонимайзеров		Анонимайзеры позволяют перемещаться по любым сайтам, не выдавая истинного IP-адреса. Щелкните узел «**Анонимайзеры**» группы узлов «**Сетевой перехват**». Для добавления в список анонимайзера щелкните кнопку «**Добавить**» и в диалоговом окне «**Новый анонимайзер**» введите значение.

Следующие страницы мастера позволяют настроить параметры службы интеграции с почтовыми серверами.

6.8.2 Настройка параметров службы интеграции с почтовыми серверами при помощи мастера

Интеграция с почтовыми серверами производится в случае, если данные нужно получать напрямую с почтовых серверов, а только путём сетевого перехвата. Схема взаимодействия NetworkController с почтовыми серверами в режиме интеграции см. Рисунок 6.275.

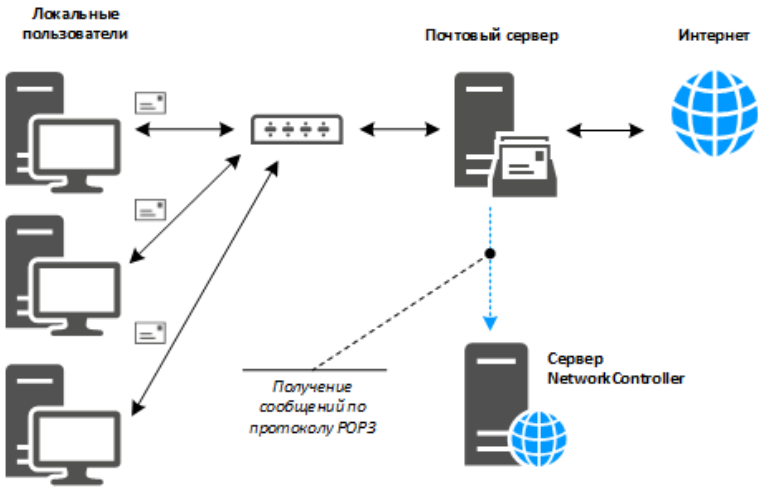


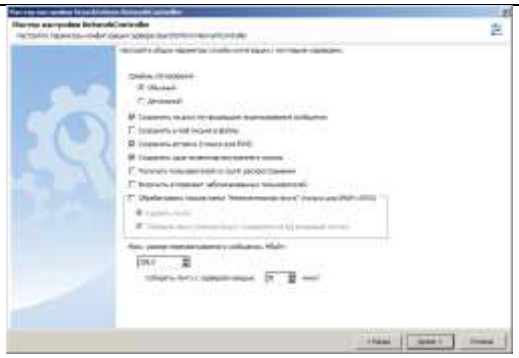
Рисунок 6.275

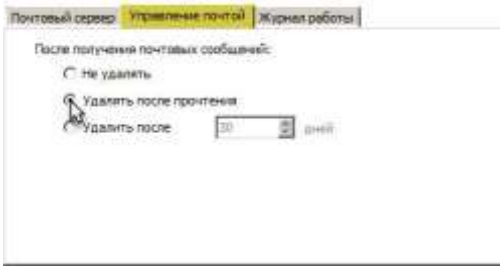
Перед интеграцией с почтовыми серверами должны быть созданы следующие условия:

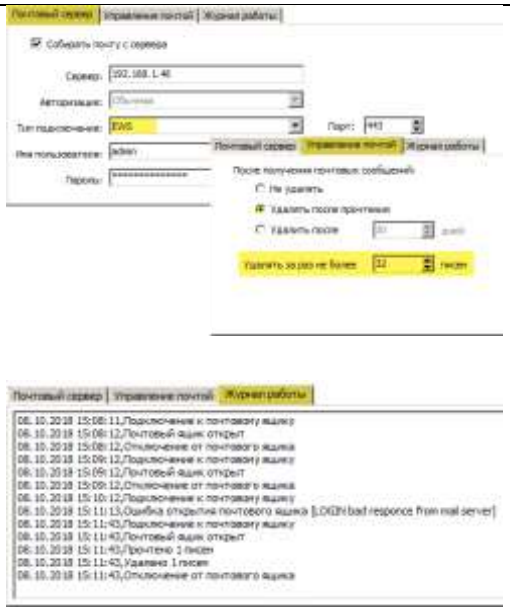
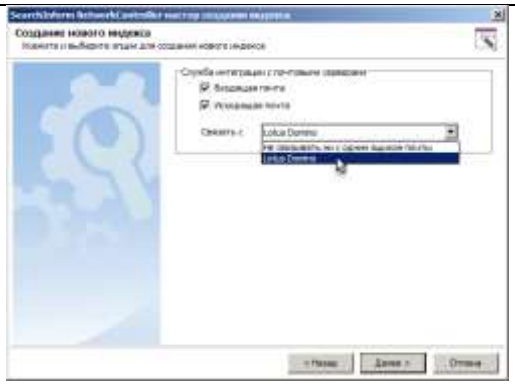
- Создан отдельный почтовый ящик, на который будут поступать почтовые сообщения.
- Настроена переадресация всех сообщений, обработанных почтовым сервером, на созданный почтовый ящик.
- Установлен компонент интеграции NetworkController с почтовыми серверами.

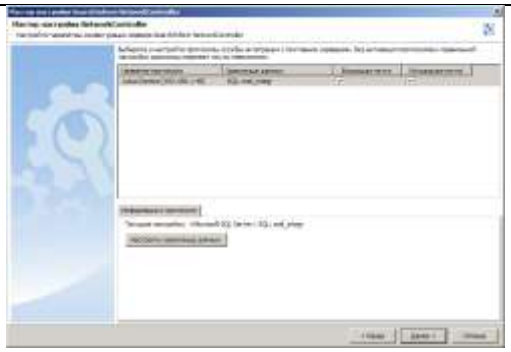
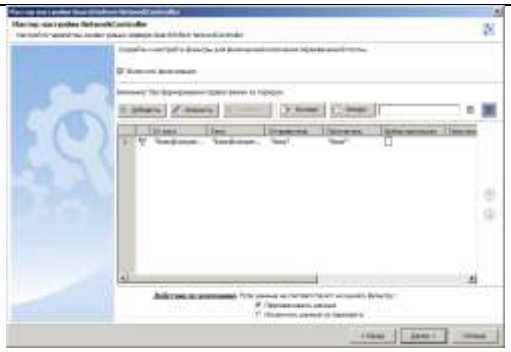
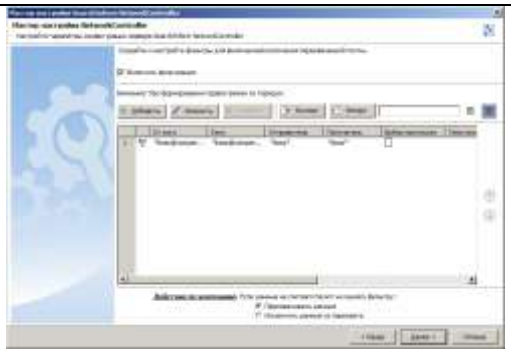
Настройка параметров интеграции с почтовыми серверами при помощи мастера производится в порядке, изложенном в Таблица 37.

Таблица 37 – Пошаговая настройка службы интеграции с почтовыми серверами при помощи мастера

Старинца мастера	**Интерфейс**	**Настройки**
Настройки параметров запуска службы интеграции с почтовыми серверами		Выберите: • Тип запуска – «Автоматически при старте» • Параметры входа в систему – «Под системной учётной записью». Системная учётная запись должна иметь право входа в качестве службы.
Настройка интервала сбора сообщений и уровня логирования		Выберите «Уровень логирования»: обычный/детальный. Для сохранения не прошедших лицензирование сообщений установите соответствующий флажок. При отметке флажком параметра «Сохранять e-mail письма в файлы» все почтовые сообщения будут экспортироваться во внешние файлы. Для сохранения в БД информации о встречах (протокол EWS), а также только одного экземпляра корпоративного письма (при дублировании) отметьте соответствующие параметры. Отметьте флажком параметр «Получать пользователей из групп распространения», если при перехвате письма от/к группе распространения необходимо вести подсчет только по тем пользователям группы, кто являлся участником почтовой

Старинца мастера	Интерфейс	Настройки
		переписки (исключая трату лицензии на саму группу). Отметьте параметр «Включить в перехват заблокированных пользователей» для перехвата писем заблокированных в домене пользователей (по таким пользователям также будут тратиться лицензии). Для обработки сообщений, попавших в папку "Нежелательная почта" установите флаг и выберите либо удаление писем, либо сохраненеие писем в базу данных с остальной входящей корреспонденцией (опция доступна только для протоколов IMAP и EWS). Укажите максимальный размер перехватываемого сообщения и интервал сбора почты с серверов: параметр «Собирать почту с серверов каждые». Минимальное рекомендуемое значение – 10 минут.
Выбор опрашиваемых почтовых серверов и настройка подключений к ним	 	Для добавления подключения, щёлкните кнопку «Добавить сервер» и введите требуемые настройки: • имя или IP-адрес почтового сервера; • тип авторизации - обычная, CRAM-MD5, NTLMv2 (для EWS); • тип подключения - POP3, POP3 TLS, POP3 STARTTLS, IMAP, IMAP STARTTLS, IMAP TLS, EWS; • имя пользователя; • пароль. На вкладке «Управление почтой» выберите действие относительно сообщений на почтовом сервере: • не удалять; • удалять после прочтения; • удалять после заданного периода (введите интервал в днях). При выборе типа подключения IMAP, IMAP STARTTLS, IMAP TLS или EWS на вкладке «Управление почтой» при удалении писем

Старинца мастера	Интерфейс	Настройки
		доступен также параметр «Удалять за раз не более ... писем», позволяющий задать количество одновременно удаляемых писем (от 32 до 2048). На вкладке «Журнал работы» доступна информация о действиях почтового сервера с указанием даты/времени и количества полученных писем.
Создание индексов интеграции, настройка их параметров и расписания обновления		Создайте требуемый индекс с помощью стандартного мастера. Для этого нажмите «Создать индекс». Настройте параметры создаваемого индекса. Требуемый результат - индекс отображается в списке. Дополнительно можно настроить расписание обновления индексов.
Создание индексов интеграции: настройка индексов интеграции: выбор направления перехватываемых сообщений		Укажите, с каким ящиком электронной почты будут связаны собранные данные.
Создание индексов интеграции:настройка индексов интеграции: выбор папки расположения индекса и имени индекса		Введите имя индекса и выберите директорию, по которой индекс будет храниться. Установите флажок «Автоматически запускать перехват».

Старинца мастера	Интерфейс	Настройки
Включение протоколов		Если протоколы интеграции с почтовыми серверами включены, оставьте настройки по умолчанию. Если нет – включите необходимые протоколы.
Фильтрация по атрибутам сообщений		Создайте фильтры для включения/ исключения перехваченной почты. Рекомендуется оставите настройки по умолчанию. Настройку удобнее производить вне мастера. Подробное описание в п. 6.8.5.2.2.
Фильтрация по атрибутам сообщений		Создайте фильтры для включения/исключения перехваченной почты. Рекомендуется оставите настройки по умолчанию. Настройку удобнее производить вне мастера. Подробное описание в п. 6.8.5.2.2.

Следующие страницы мастера позволяют настроить параметры службы SMTP-интеграции.

6.8.3 Настройка параметров SMTP-интеграции при помощи мастера

Исходя из необходимости соблюдения постоянно растущего количества регулятивных и нормативных требований, каждая организация должна хранить записи об обмене сообщениями при выполнении сотрудниками ежедневных деловых задач. Функция *журналирования* почтового севера позволяет хранить копии сообщений в центральном почтовом ящике для различных целей, включая архивацию почты.

Для перехвата отчётов журнала, помещённых в контейнеры, сервером NetworkController можно использовать две схемы.

Суть первой схемы: журналируемый трафик передается почтовым сервером по SMTP-протоколу другому почтовому серверу. Сервер NetworkController перехватывает

трафик, распознаёт в нём наличие контейнеров и извлекает из них сообщения со всеми необходимыми атрибутами (см. Рисунок 6.276).

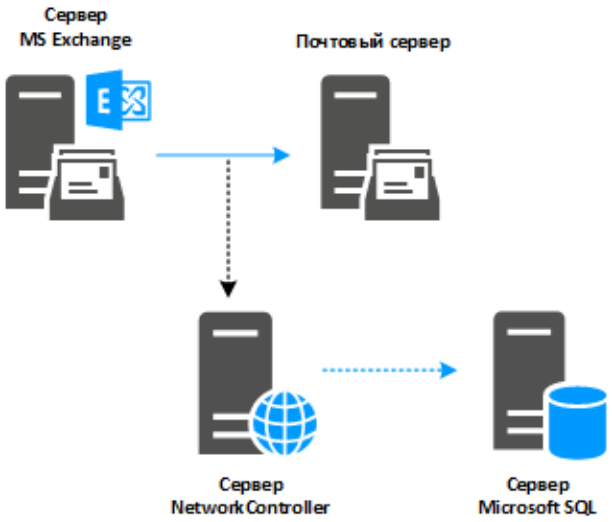


Рисунок 6.276

Второй вариант куда проще – настройка трафика журналирования непосредственно на сервер NetworkController. В такой схеме NetworkController выступает в роли SMTP-сервера, получающего пересылаемые контейнеры отчётов журнала, после чего обрабатывает их и помещает в базу данных (см. Рисунок 6.277).

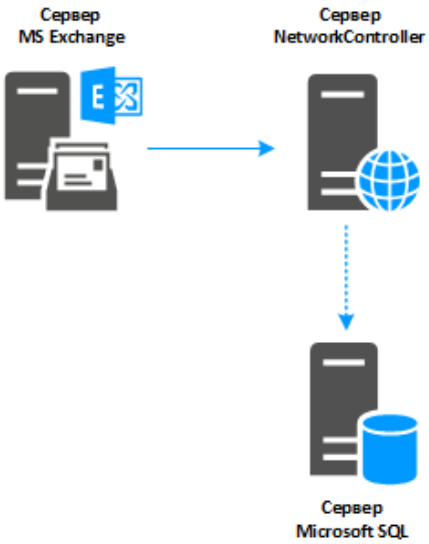
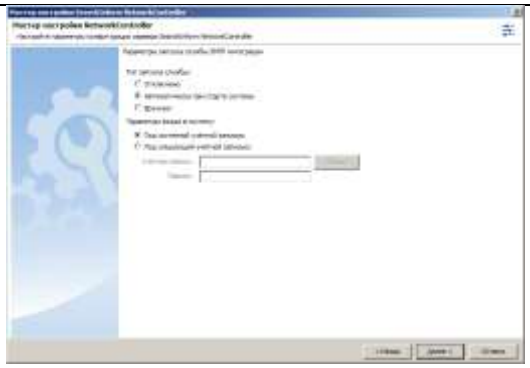
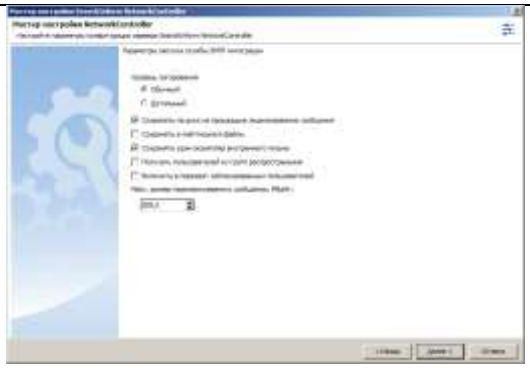
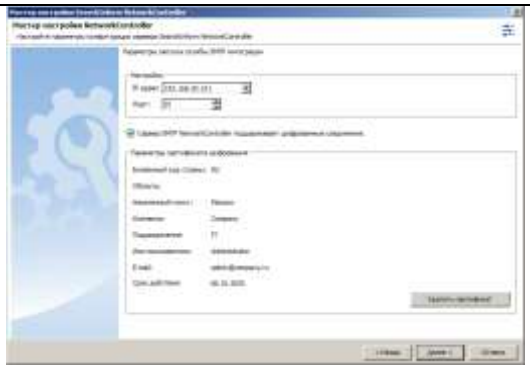
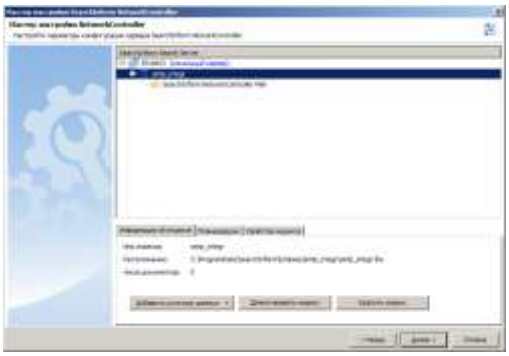
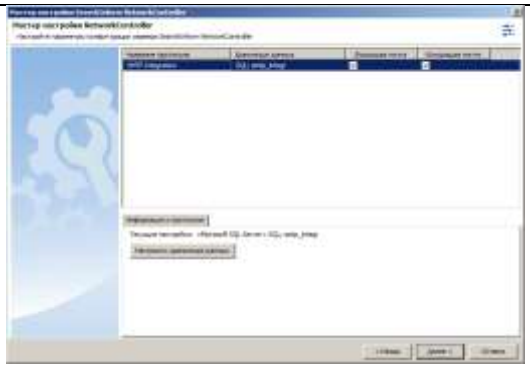


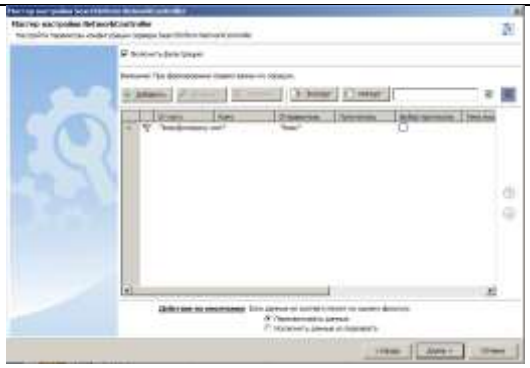
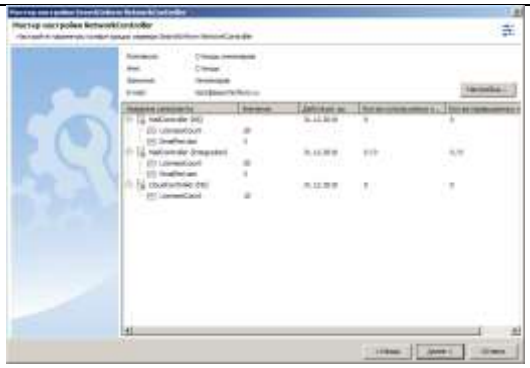
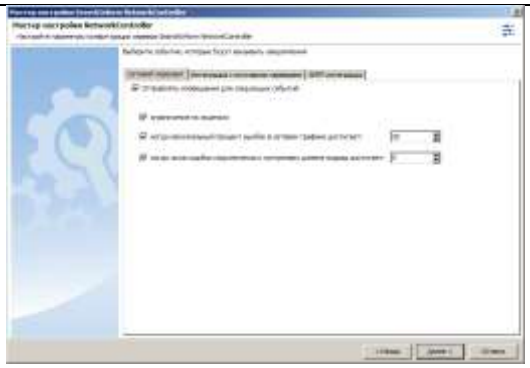
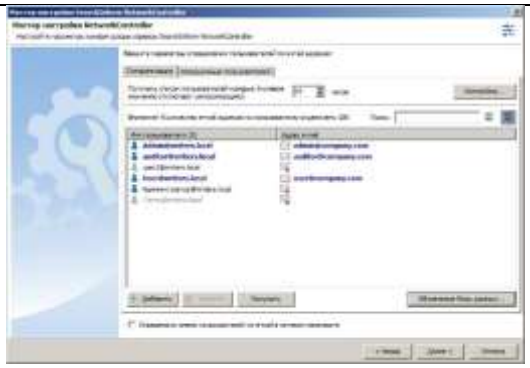
Рисунок 6.277

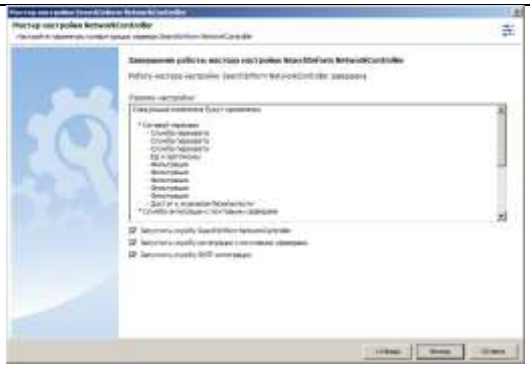
Настройка параметров SMTP-интеграции при помощи Мастера производится в порядке, изложенном в Таблица 38.

Таблица 38 – Пошаговая настройка службы SMTP-интеграции при помощи мастера

Страница мастера	Интерфейс	Настройка
Настройки запуска службы		«Тип запуска» - «Автоматически при старте операционной системы». Настройте учётную запись, под которой будет работать служба SMTP-интеграции. Требования к учётной записи: • возможность входа в качестве службы на сервере NetworkController; • право получения списка пользователей из каталога Active Directory. В большинстве случаев достаточно системной учётной записи.
Настройка уровня логирования		«Уровень логирования» – Обычный. Для сохранения на диск не прошедших лицензирование сообщений установите соответствующий флажок. При отметке параметра «Сохранять e-mail письма в файлы» все почтовые сообщения будут экспортироваться во внешние файлы. При дублировании одного и того же корпоративного письма (входящего и исходящего) возможно сохранение только одного из экземпляров. Отметьте флажком параметр «Получать пользователей из групп распространения», если при перехвате письма от/к группе распространения необходимо вести подсчет только по тем пользователям группы, кто являлся участником почтовой переписки (исключая трату лицензии на саму группу). Отметка параметра «Включить в перехват заблокированных пользователей» активирует перехват писем заблокированных в домене пользователей и, как следствие, по таким пользователям также будут использоваться лицензии.

Страница мастера	Интерфейс	Настройка
		Укажите максимальный размер перехватываемых данных.
Настройка параметров сервиса SMTP-интеграции		Укажите IP-адрес и номер SMTP-порта сервера NetworkController. При необходимости шифрования канала передачи журналов отчета, сгенерируйте сертификат.
Создание и настройка индексов (2)	 	Щёлкните кнопку «Создать индекс» для создания индексов с помощью мастера. Требуемый результат: созданный индекс отображается в списке. Дополнительно можно настроить интервал обновления индекса. Для этого выделите индекс, откройте вкладку «Планировщик» и воспользуйтесь стандартным мастером Windows.
Включение протоколов		Если протоколы интеграции с почтовыми серверами включены, оставьте настройки по умолчанию. Если нет – выберите протоколы и укажите имя созданной ранее базы данных.

Страница мастера	Интерфейс	Настройка
Настройка фильтров по атрибутам сообщений		Настройте фильтры для включения/исключения перехваченной почты. Подробное описание в п. 6.8.5.2.2.
Проверка лицензии		Проверьте наличие лицензии: для перевода сервера NetworkController из испытательного в лицензионный режим должна быть использована лицензия, ограниченная условиями лицензионного договора.
Конфигурирование оповещений		Настройте значения, по достижении которых сотруднику службы безопасности будет отправлено уведомление.
Настройки определения пользователей		На вкладке «Синхронизация» с помощью кнопки «Настройка» задайте способ синхронизации: из Active Directory либо из DataCenter. Для привязки адреса электронной почты к пользователю вручную используется кнопка «Добавить». (формат доменного имени: user@domain.local). Список пользователей и адресов можно считать из Active Directory по нажатию кнопки «Получить». Нажатие кнопки «Обновление базы данных...» вызывает окно настройки подключения к базам данных, содержащим данные почтовых протоколов. Подключение к заданной базе данных запускает процесс замены имен доменных пользователей "<unknown>" данными,

Страница мастера	Интерфейс	Настройка
	 	полученными в процессе синхронизации и/или введенными вручную. Для использования принципа сопоставления доменных имен пользователей электронным адресам при сетевом перехвате трафика, отметьте соответствующий параметр в нижней части окна. Настройка ***Привязок доменных пользователей к почтовым адресам и/или Масок адресов является обязательной!*** В случае их отсутствия ни одно из писем не будет перехвачено (независимо от условий дополнительных фильтров). На вкладке «Определение пользователей» настройте список масок по адресам электронной почты, согласно которым сообщениям, не попадающим под настроенные соответствия, будут присваиваться доменные имена. Поддерживаются маски «*», замещающие произвольный текст. Предусмотрена возможность проверки фильтров по образцам почтовых адресов.
Завершение работы мастера		Щелкните кнопку «Финиш».

6.8.4 Настройка интеграции с Microsoft Lync Server

На сервер NetworkController устанавливается протокол SIP (см. Рисунок 6.278).

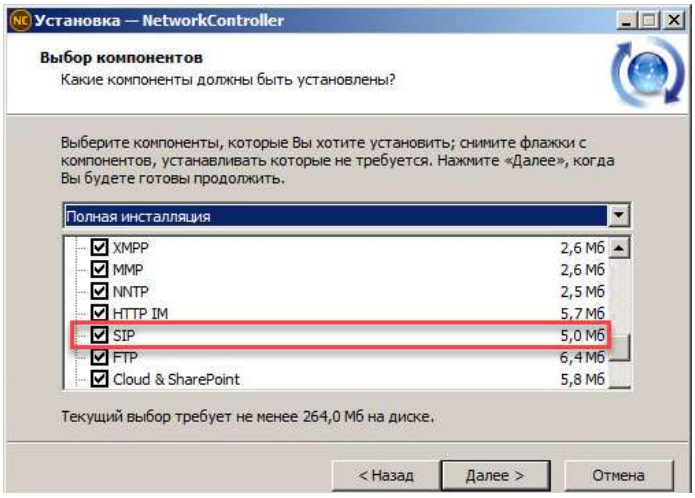


Рисунок 6.278

Для SIP-протокола должно быть настроено хранилище данных (см. Рисунок 6.279) и сняты ограничения по портам (см. Рисунок 6.280).

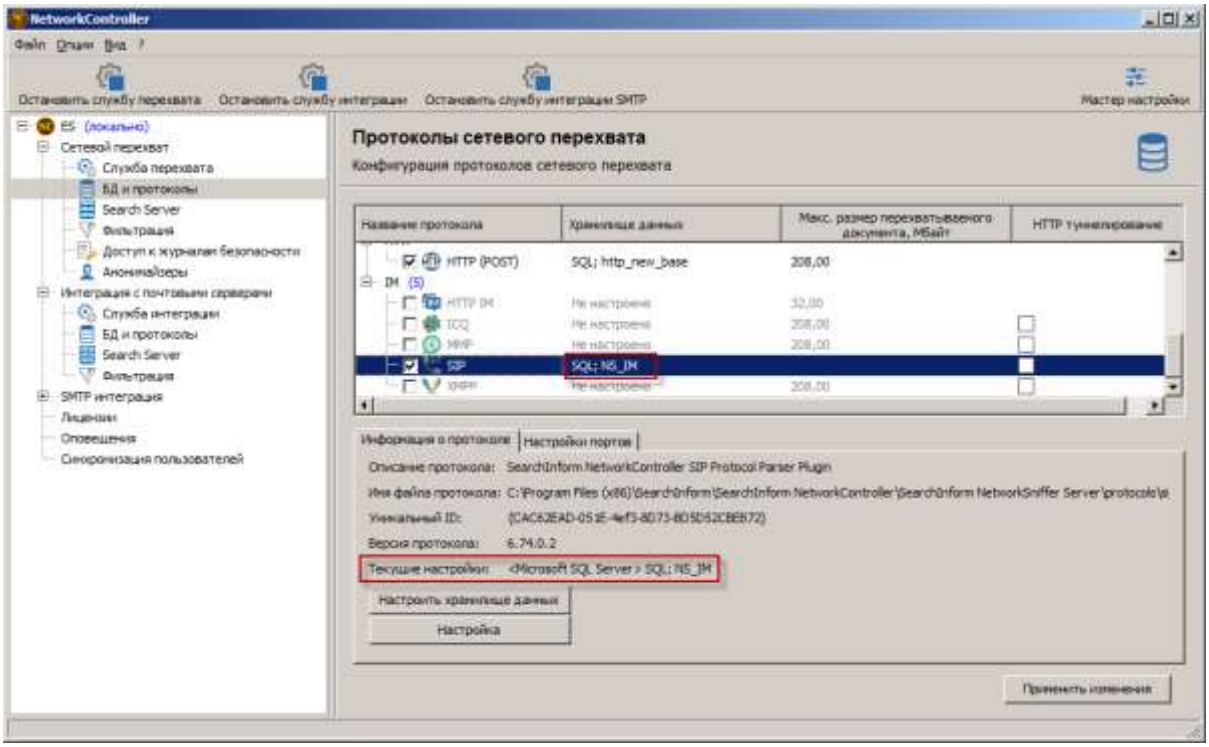


Рисунок 6.279

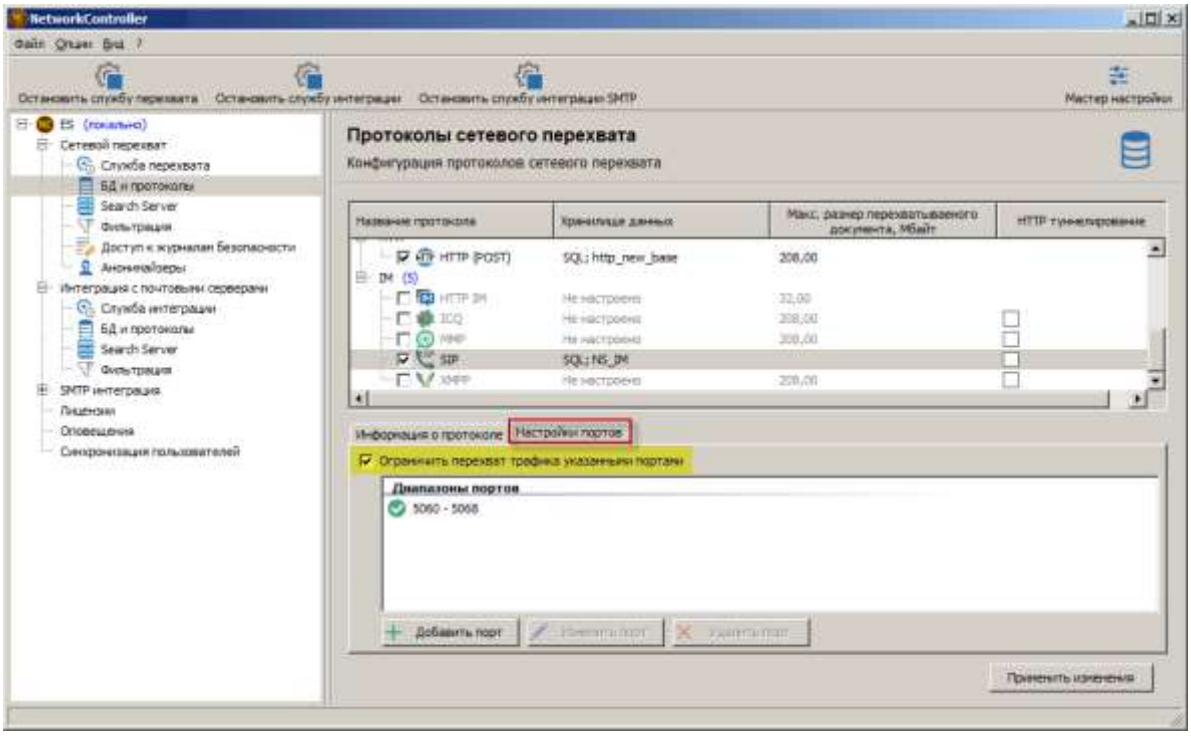


Рисунок 6.280

На этапе установки сервера NetworkController устанавливается модуль интеграции с Lync (см. Рисунок 6.281).

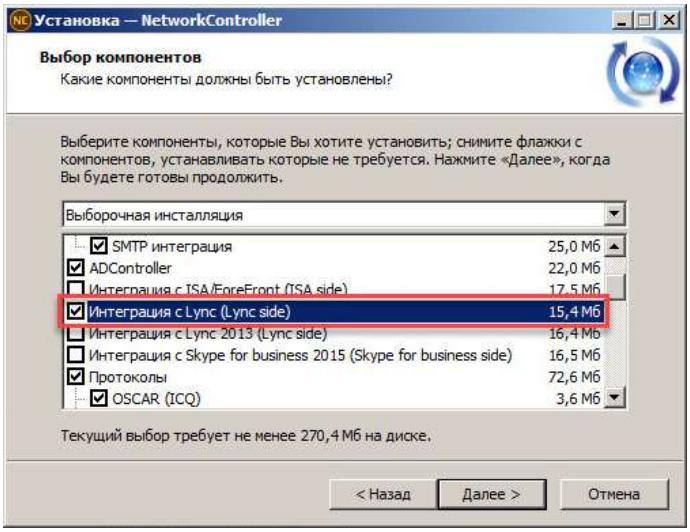


Рисунок 6.281

Для Microsoft Lync Server 2013 устанавливается модуль интеграции с Lync 2013 (см. Рисунок 6.282).

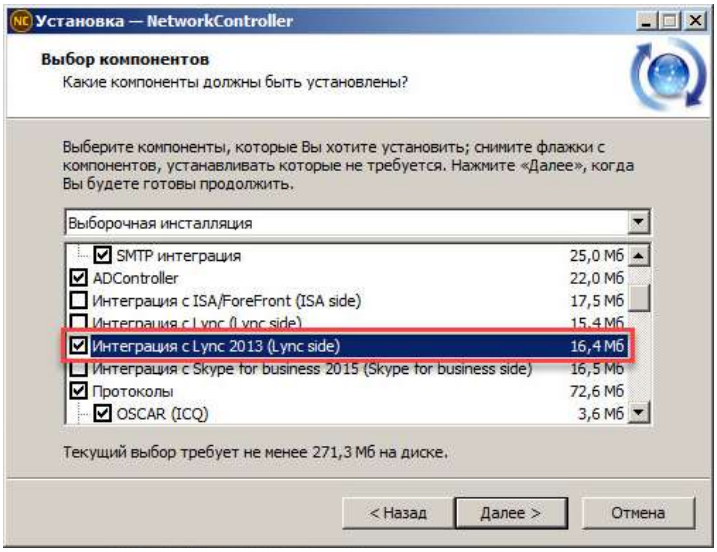


Рисунок 6.282

Для Skype for Business Server 2015 (Lync Server 2015) устанавливается модуль интеграции со Skype for Business.

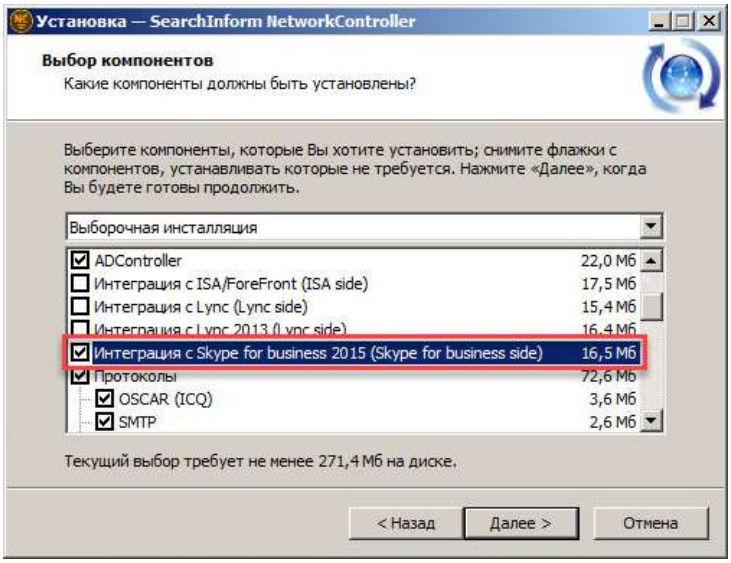


Рисунок 6.283

По завершении инсталляции выполните на сервере Lync следующие действия для **включения интеграции**:

1) Создайте доменную учётную запись и включите её в доменную группу «Администраторы домена» и в локальную группу «RTC Server Applications» на сервере Lync.

2) Установите для сервиса «SearchInform NetworkController Lync integration» запуск от созданной учётной записи.

3) Запустите «Lync Server Management Shell» и наберите команду

```
New-CsServerApplication -Identity
"service:registrar:lyncserver.lync.local/NsLync" -Uri
"http://www.microsoft.com/NsLync" -Critical $False -Enabled $True,
```

где lyncserver.lync.local – имя сервера Lync.

4) В файле sinssvc.xml (на сервере Lync и NetworkController) в параметре icapservices.transport.sock.server.ip укажите IP-адрес ICAP-сервера NetworkController, в параметре icapservices.transport.sock.server.port укажите порт ICAP-сервера NetworkController.

Для включения протоколирования данных, перехваченных модулем интеграции, необходимо на сервере Lync в ветке реестра

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SearchInform\SearchInform NetworkController

создать параметр LyncLogEnabled типа REG_DWORD и установить для него значение 1.

Для **отключения интеграции** с сервером Lync необходимо выполнить следующие действия:

1) Остановите сервис «SearchInform NetworkController Lync integration».

2) Установите для сервиса «SearchInform NetworkController Lync integration» тип запуска «Отключена».

3) Запустите «Lync Server Management Shell» и наберите команду

Remove-CsServerApplication -Identity "registrar:lyncserver.lync.local/NsLync",

где lyncserver.lync.local – имя сервера Lync.

6.8.5 Фильтрация сетевого трафика

Перехват информации производится на уровне сетевых адаптеров. По умолчанию весь FTP-трафик, трафик электронной почты, IM-клиентов и переданных при помощи POST-форм сообщений и файлов перехватывается и записывается в базы данных/хранилище.

Под фильтрацией понимается ограничение записи данных в базы/хранилище по формальным атрибутам.

Настройка фильтров производится в узле «Фильтрация» группы «Сетевой перехват».

Фильтрация сетевого трафика может понадобиться для следующих целей:

- Отмены записи информации, отправленной или полученной ответственными работниками. В данном случае используется фильтрация по пользовательским атрибутам.
- Ограничение записи информации и определение направления передачи информации в случае перехвата информации после прокси-сервера.

6.8.5.1 Фильтрация сетевого трафика по пользовательским атрибутам

Фильтрация трафика может потребоваться для отмены перехвата информации, переданной руководством и ответственными работниками организации.

Одновременно можно использовать или запрещающие, или разрешающие фильтры.

- При использовании запрещающих фильтров, в базу данных будут записаны все перехваченные данные, за исключением совпадений с настроенными условиями. При добавлении фильтра должна быть выбрана опция «Исключить из перехвата».
- При использовании разрешающих фильтров, в базу данных будут записаны только те перехваченные данные, которые подпадают под настроенные условия. При добавлении фильтра должна быть включена опция «Разрешить перехват».

В настройках сервера NetworkController можно создавать как общие фильтры для всех протоколов, так и частные фильтры для отдельных протоколов. Общие фильтры настраиваются на вкладке «Фильтры → Глобальные настройки», а фильтры протоколов – на вкладке «Фильтры → Настройки протоколов» (см. Рисунок 6.284).

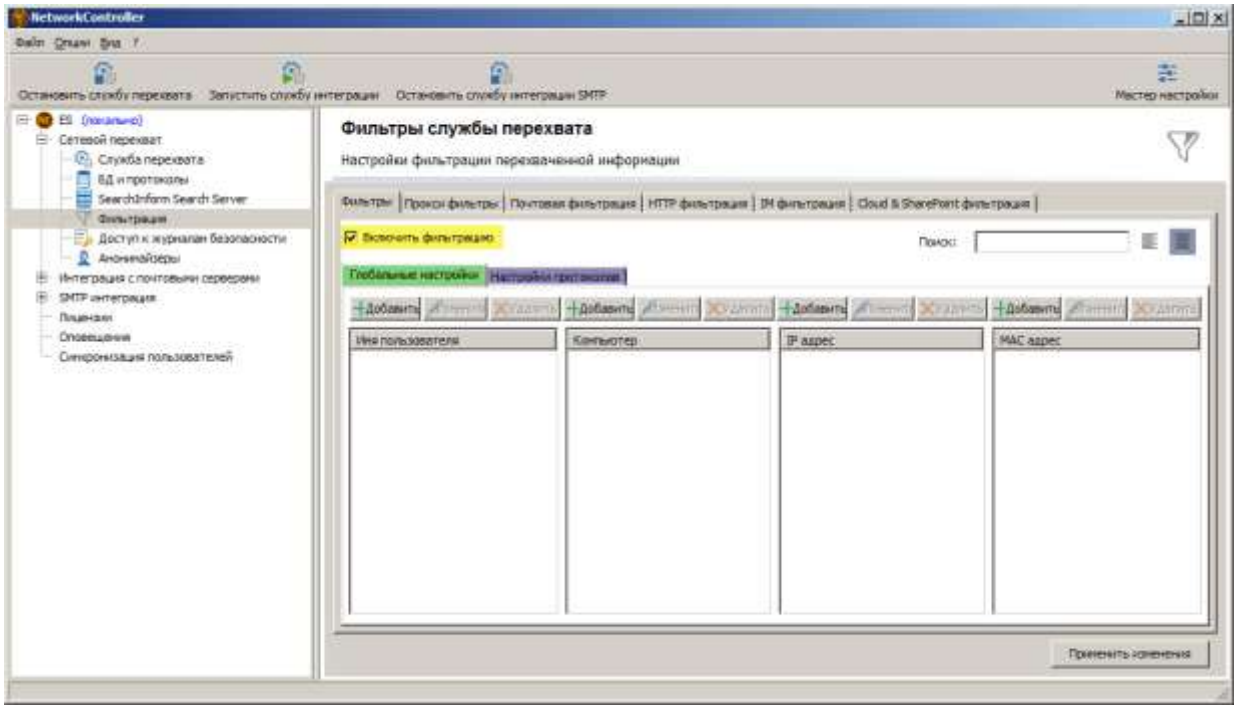


Рисунок 6.284

Глобальные фильтры применяются ко всем протоколам. Фильтры протоколов – только к отдельным протоколам. Для настройки такого фильтра на вкладке «Настройки протоколов» выделите протокол и нажмите кнопку «Добавить».

Глобальные настройки фильтрации можно отменить для отдельных протоколов. Для этого снимите соответствующий флажок (см. Рисунок 6.285).

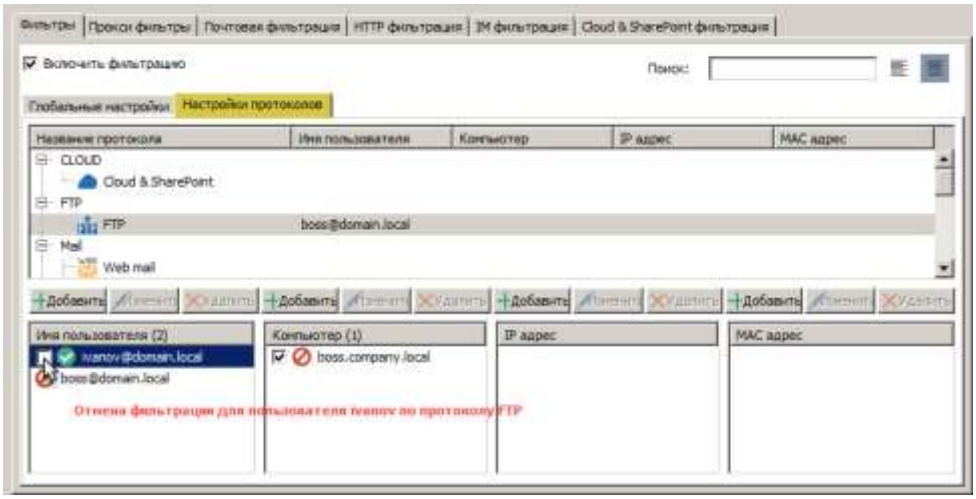


Рисунок 6.285

Для добавления фильтров, воспользуйтесь кнопками «Добавить» в каждой группе условий: имя пользоваателя домена / имя компьютера / IP-адреса пользователей / MAC-адреса пользователей. Для удаления или изменения фильтров используйте соответственно кнопки «Удалить», «Изменить» (см. Рисунок 6.286).

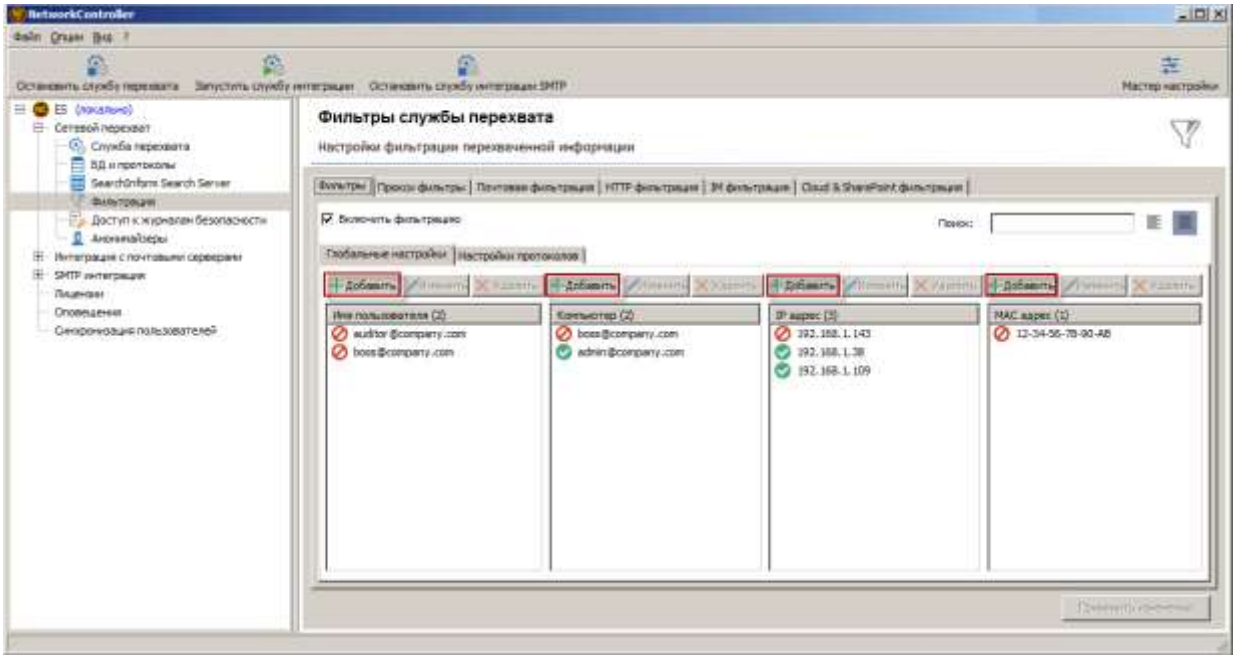


Рисунок 6.286

6.8.5.1.1Фильтрация по пользователям

Нажмите кнопку «Добавить» в группе фильтров «Имя пользователя».

В появившемся окне установите тип фильтра: разрешающий / запрещающий. Введите имена пользователей через запятую или воспользуйтесь кнопкой . В именах

пользователей разрешается использование метасимвола «*», который заменяет от нуля и более символов (см. Рисунок 6.287).

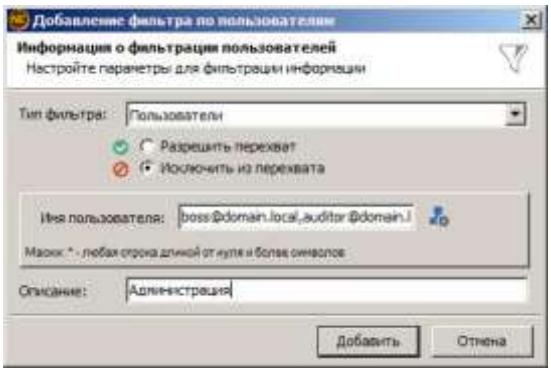


Рисунок 6.287

При необходимости добавьте описание фильтра и/или номер порта. После нажатия кнопки «Добавить» фильтр отобразится в консоли. Примените изменения.

6.8.5.1.2Фильтрация по компьютерам

Нажмите кнопку «Добавить» в группе фильтров «Компьютер».

В появившемся окне установите тип фильтра: разрешающий / запрещающий. Введите имя компьютера вручную или воспользуйтесь кнопкой . При указании имени компьютера разрешается использование метасимвола «*», который заменяет от нуля и более символов (см. Рисунок 6.288).

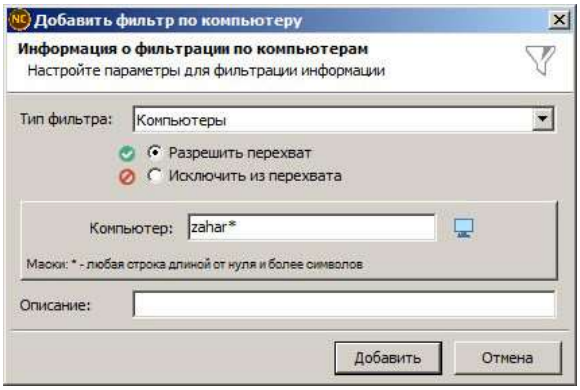


Рисунок 6.288

При необходимости добавьте описание фильтра и/или номер порта. После нажатия кнопки «Добавить» фильтр отобразится в консоли. Примените изменения.

6.8.5.1.3Фильтрация по IP-адресам

Нажмите кнопку «Добавить» в группе фильтров «IP-адрес».

В появившемся окне выберите один из доступных вариантов ввода адреса:

- один IP-адрес;
- сетевая маска (укаывается IP-адрес и маска);
- диапазон IP-адресов.

Установите тип фильтра: разрешающий / запрещающий (см. Рисунок 6.291).

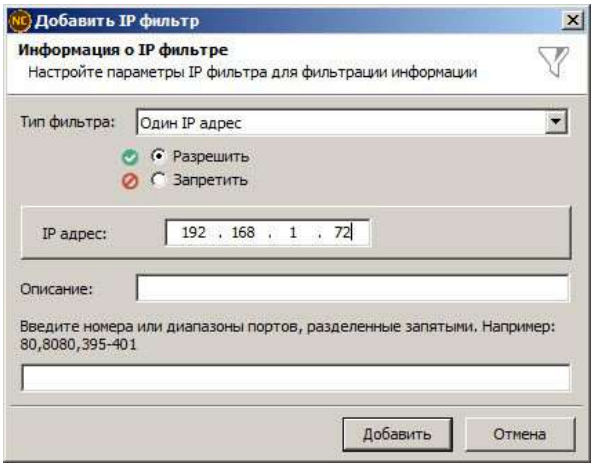


Рисунок 6.289

При необходимости добавьте описание фильтра и/или номер порта. После нажатия кнопки «Добавить» фильтр отобразится в консоли. Примените изменения.

6.8.5.1.4Фильтрация по MAC-адресам

Нажмите кнопку «Добавить» в группе фильтров «MAC-адрес».

В появившемся окне выберите из выпадающего списка значение «Один MAC-адрес» и установите тип фильтра: разрешающий / запрещающий. Введите значение адреса (см. Рисунок 6.290).

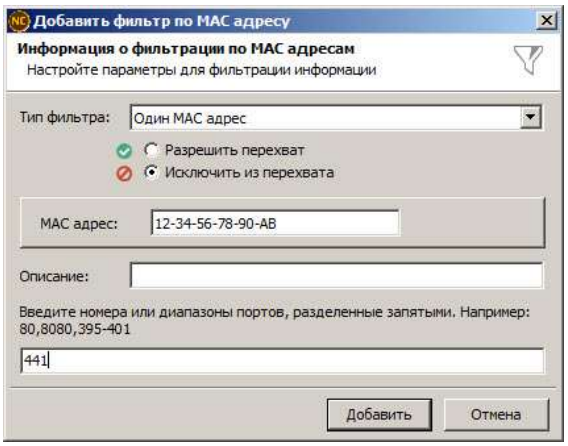


Рисунок 6.290

При необходимости добавьте через запятую номер порта / диапазона портов. После нажатия кнопки «Добавить» фильтр отобразится в консоли. Примените изменения.

6.8.5.2 Фильтрация сетевого трафика по SMTP-атрибутам и прокси-серверам

Фильтрацию трафика по SMTP-атрибутам и прокси-серверам нужно применять только при перехвате информации после прокси-сервера. В этом случае получателем и

отправителем сетевого пакета выступают прокси-сервер и удалённый сервер. В связи с этим возникают следующие затруднения:

- Сложно определить направление передачи данных (входящие или исходящие).
- Не определяются доменные имена пользователей, передавших данные, что ведет к невозможности фильтрации трафика.

Для решения этой задачи используются SMTP- и прокси-фильтры.

6.8.5.2.1Фильтрация по прокси-серверам

Для определения направления передачи данных используются прокси-фильтры. Для их настройки на вкладке «Прокси фильтры» установите флажок «Прокси фильтры» и, используя кнопку «Добавить», последовательно введите IP-адреса внутренних прокси-серверов (см. Рисунок 6.291).

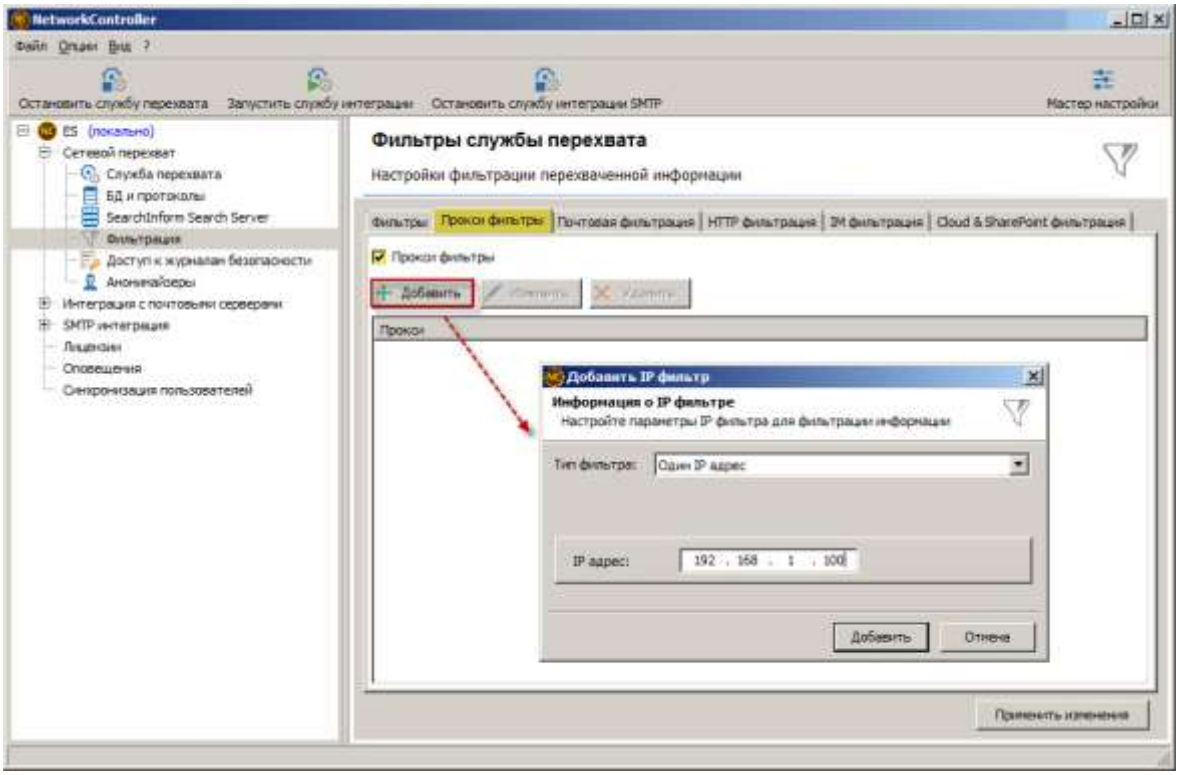


Рисунок 6.291

6.8.5.2.2Почтовая фильтрация

Для настройки фильтрации почтовых сообщений на вкладке «Почтовая фильтрация» установите флажок «Включить фильтрацию» и воспользуйтесь кнопкой «Добавить» для создания нового фильтра (см. Рисунок 6.292).

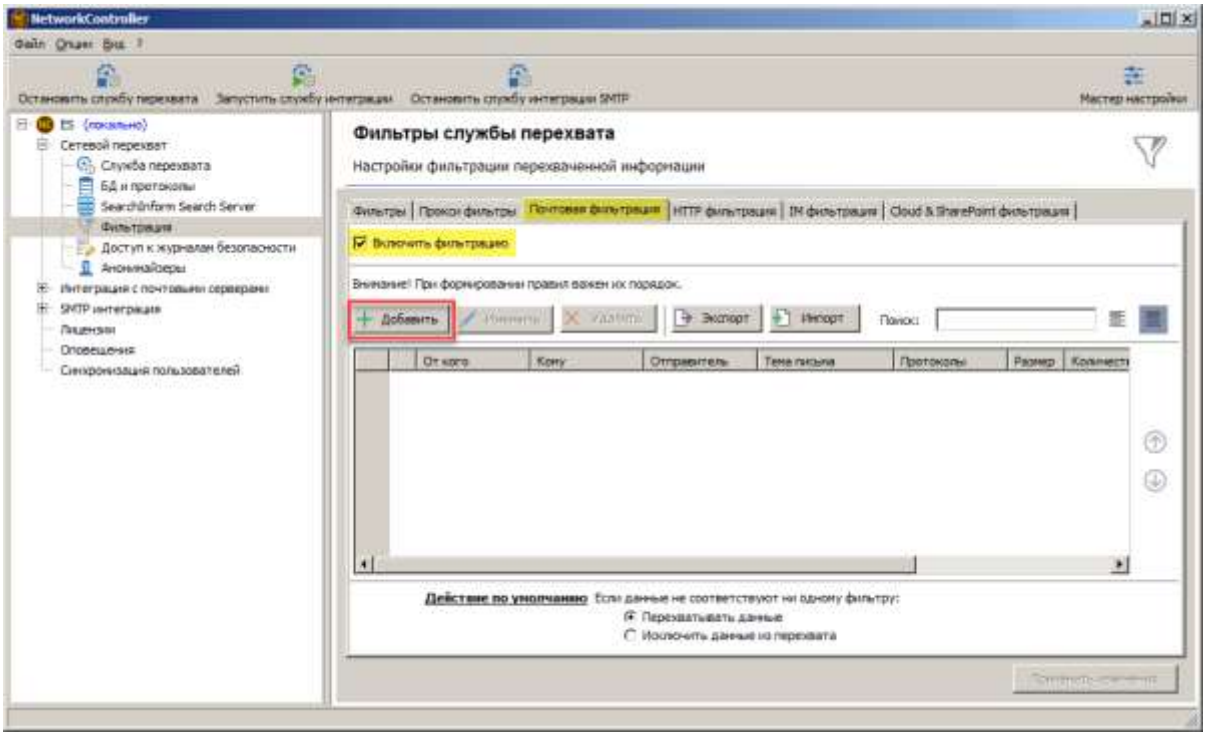


Рисунок 6.292

В окне добавления нового фильтра введите адреса получателей и отправителей сообщений в одном из форматов: ivan.ivanov@company.ru (простой почтовый адрес) или Иван Иванов <ivan.ivanov@company.ru> (полный почтовый адрес с именем пользователя). Каждый фильтр по почтовым адресам должен начинаться и заканчиваться на маску «*».

Примеры фильтров:

- *ivan.ivanov@company.ru*;
- *@company.ru*;
- *ivan.*@company*;
- *ivan.ivanov*;
- *Иван Иванов* (только для полного адреса с именем пользователя).

Для выбора доменных имен отправителей из списка, щелкните кнопку . В диалоговом окне «Окно импортирования пользователей» отметьте нужного пользователя и подтвердите выбор кнопкой «Добавить». В качестве отправителя и/или получателя также может быть выбрана группа или подразделение (см. Рисунок 6.293).

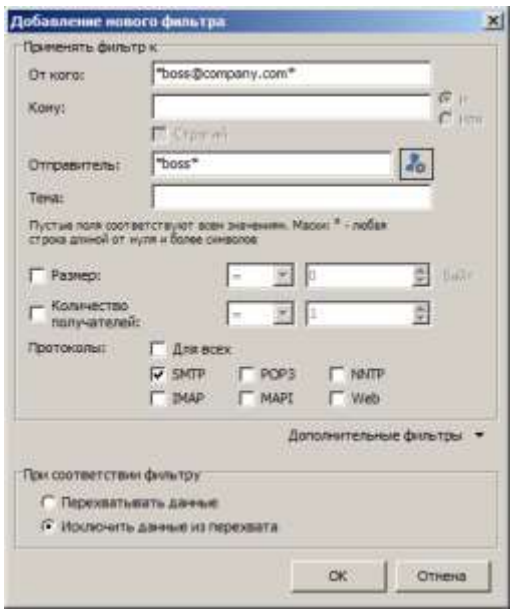


Рисунок 6.293

Блок «Дополнительные фильтры» разворачивается кликом по заголовку и предназначен для настройки значений служебных полей, которые необходимо исключить из перехвата. Несколько значений полей могут быть объединены логическими операторами И/ИЛИ (см. Рисунок 6.294).

Рисунок 6.294

Фильтрация может применяться как одновременно ко всем пакетам, переданным/полученным по протоколам POP3, SMTP, IMAP, MAPI, NNTP, Web mail, так и к отдельно выбранным протоколам (см. Рисунок 6.295).

Рисунок 6.295

Выберите тип фильтра:

- разрешающий – «Перехватывать данные» (сообщение сохраняется в базу данных)
- запрещающий – «Исключить данные из перехвата» (запись в базу данных не производится).

Фильтры имеют приоритет и применяются последовательно в том порядке, в котором они заданы. Чем выше расположен фильтр, тем раньше он сработает.

При отметке параметра «Строгий» данный фильтр сработает, если условиям фильтра удовлетворяет **хотя бы один** адресат. Он сохранит/не сохранит документ в базу и запретит обработку всех следующих за ним фильтров. При снятом флажке (нестрогий фильтр) запоминается сработавшее состояние и продолжается последовательная отработка остальных фильтров. Нестрогий фильтр сработает только в том случае, когда под условие одного или нескольких фильтров попадут **все** адресаты.

Кнопки «Экспорт»/«Импорт» позволяют сохранить/загрузить конфигурацию фильтров в нескольких форматах (.txt, .lst, .cvs).

Фильтры имеют приоритет и применяются последовательно в том порядке, в котором они заданы. Чем выше расположен фильтр, тем раньше он сработает. Управление порядком фильтров производится с помощью кнопок и .

6.8.5.2.3Фильтрация HTTP

Фильтры работают для GET-/POST-запросов, передаваемых по протоколу HTTP. HTTP-фильтры позволяют отсечь лишние данные, например, можно исключить из перехвата запросы к внутренним веб-системам или указать почтовые хосты, с которых не требуется перехват трафика.

Для их настройки на вкладке «Фильтрация HTTP» установите флажок «Включить фильтрацию» и, пользуясь кнопкой «Добавить», последовательно введите параметры фильтра (см. Рисунок 6.296).

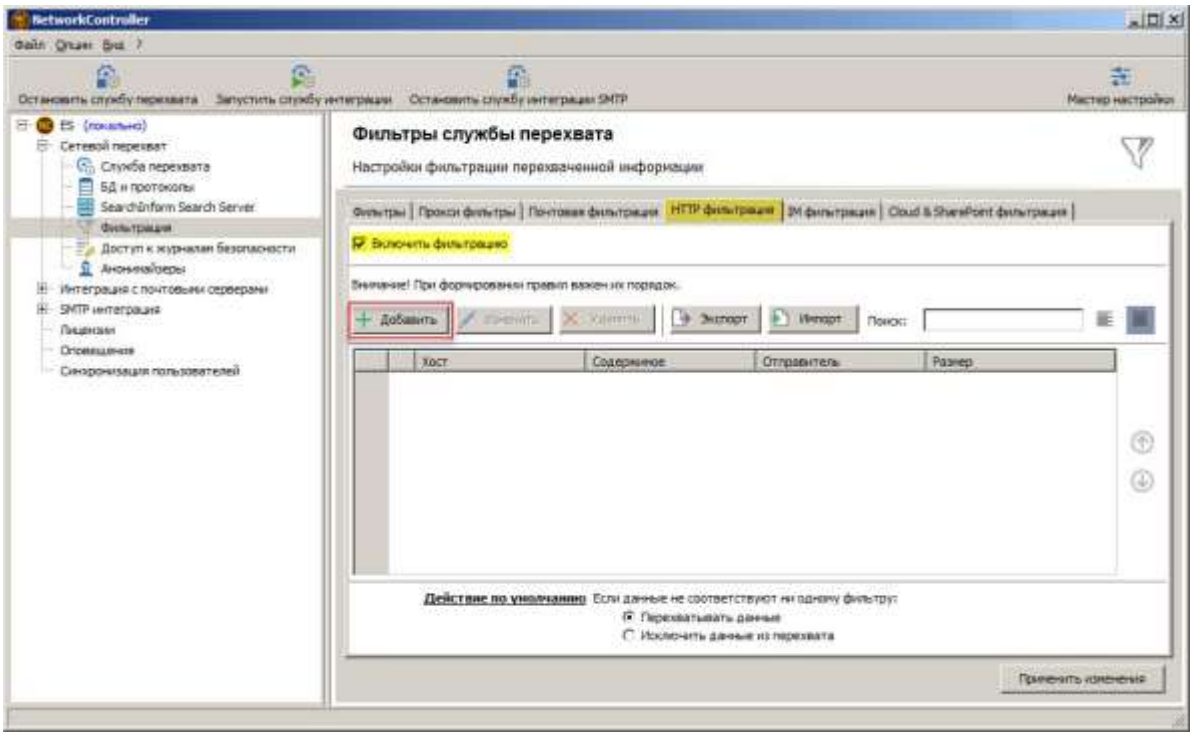


Рисунок 6.296

В открывшемся окне «Добавление нового фильтра» укажите значения параметров фильтра (см. Рисунок 6.297).

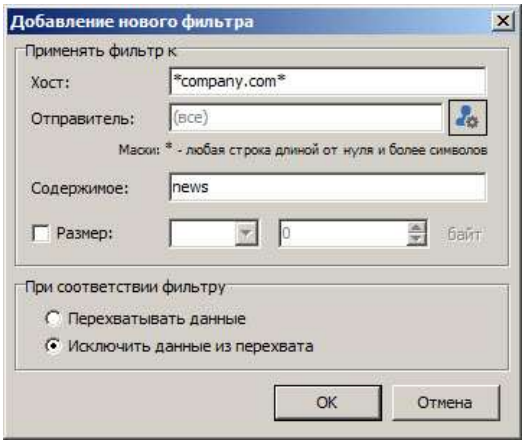


Рисунок 6.297

В полях «Хост» и «Отправитель» запроса допускается использование метасимвола «*».

Чтобы выбрать доменные имена отправителей из списка, щелкните кнопку . В диалоговом окне «Окно импортирования пользователей» отметьте нужного пользователя и подтвердите выбор кнопкой «Добавить». В качестве отправителя также может быть выбрана группа или подразделение (см.Рисунок 6.298).

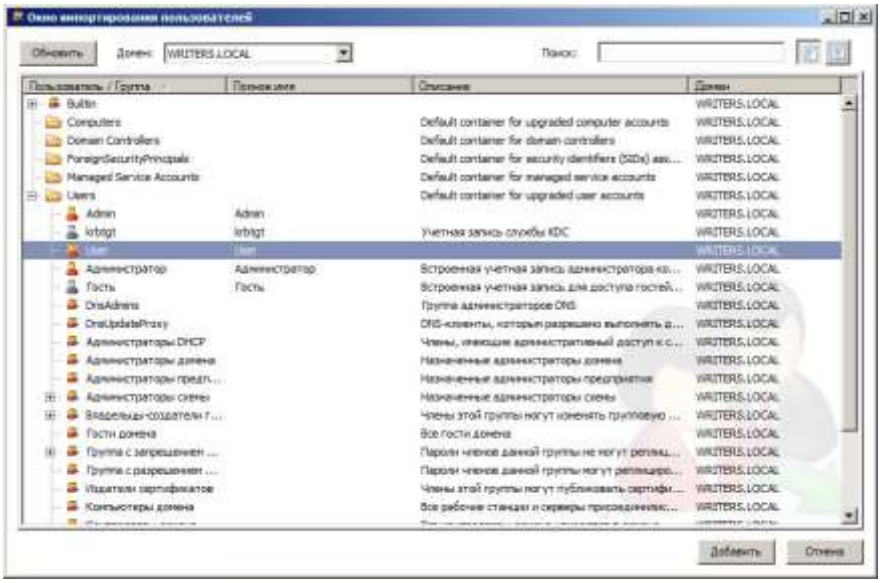


Рисунок 6.298

При добавлении HTTP-фильтра, выберите тип фильтра – запрещающий (запись в базу данных не производится) или разрешающий (сообщение записывается в базу данных) в зависимости от выбранной опции в группе «При соответствии фильтру»: сохранить данные или исключить их перехват (см. Рисунок 6.299).

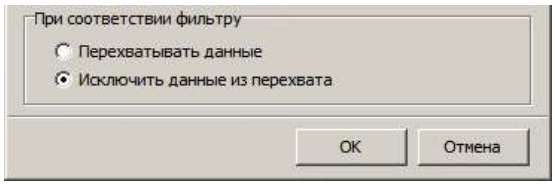


Рисунок 6.299

Установите действие по умолчанию, которое будет применяться, если перехваченные данные не будут соответствовать ни одному из либо «Перехватывать данные», либо «Исключить данные из перехвата» (см. Рисунок 6.300).

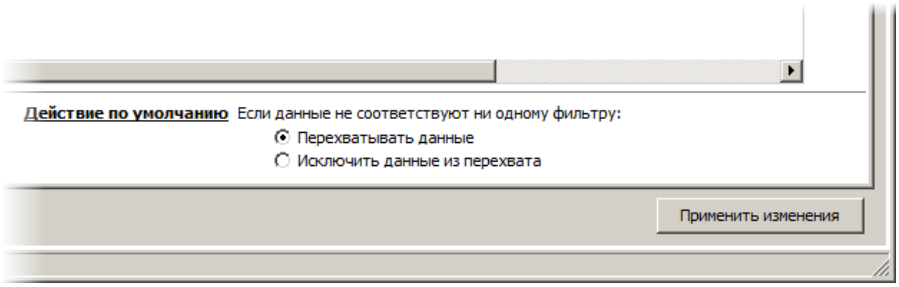


Рисунок 6.300

Фильтры имеют приоритет и применяются последовательно в том порядке, в котором они заданы. Чем выше расположен фильтр, тем раньше он сработает. Управление порядком фильтров производится с помощью кнопок  и  .

6.8.5.2.4Фильтрация HTTPIM

Фильтры работают для трафика, полученного по протоколу HTTPIM и позволяют отсечь лишние данные, например, можно исключить из перехвата переписку определенных пользователей.

Для их настройки на вкладке «IM фильтрация» установите флажок «Включить фильтрацию» и воспользуйтесь кнопкой «Добавить» для создания нового фильтра (см. Рисунок 6.301).

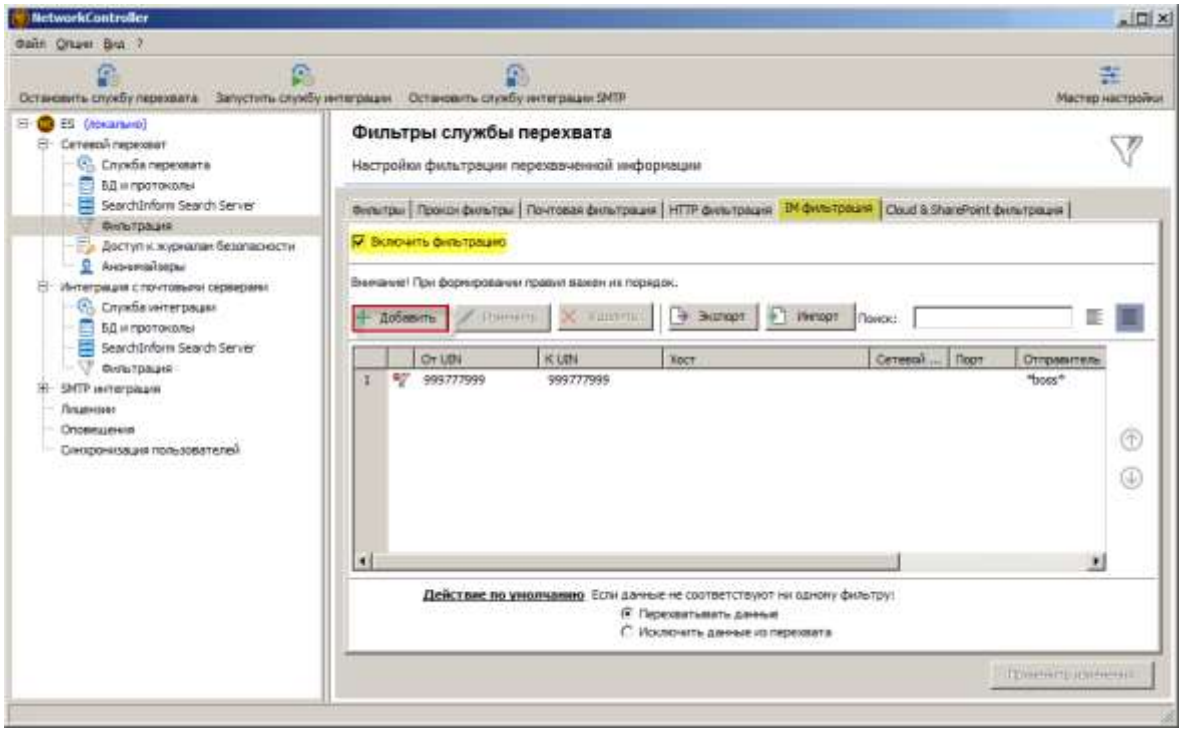


Рисунок 6.301

В появившемся окне укажите значения атрибутов документа, к которым будет применен фильтр:

- **От UIN / К UIN** - уникальный идентификатор отправителя/получателя;
- **Хост** - адрес ресурса в сети (при выборе протокола HTTP IM);
- **Сетевой протокол** и **Порт** - используемые протокол и номер порта (для HTTP IM);
- **Отправитель** - полное доменное имя отправителя запроса.

Для полей «Хост» и «Отправитель» допускается использование метасимвола «*****», заменяющего от нуля и более символов.

- **В любой части перехвата** - данные сообщения, поиск по которым осуществлен как в строке UIN, так и в теле пакета (использование метасимвола «*» не допускается).
- **Размер** - размер сообщения.
- **Протоколы** - список протоколов, к которым может быть применен данный фильтр.

Чтобы выбрать отправителя из списка, щелкните кнопку  (см.Рисунок 6.302).

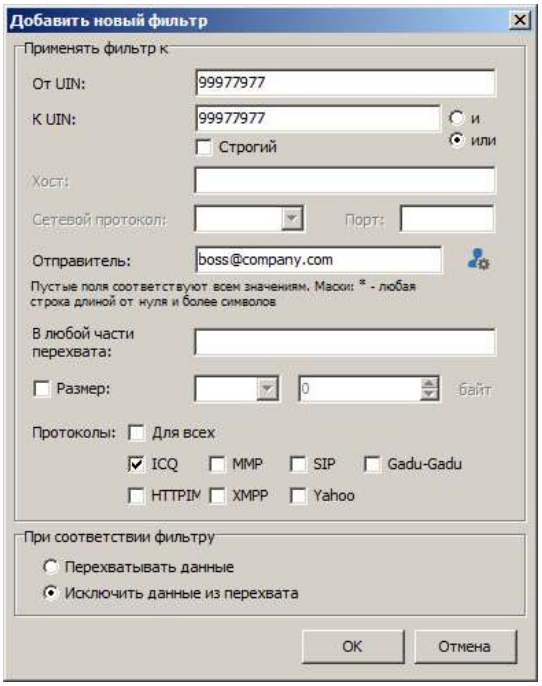


Рисунок 6.302

В диалоговом окне «Окно импортирования пользователей» отметьте нужного пользователя и подтвердите выбор кнопкой «Добавить». В качестве отправителя также может быть выбрана группа или подразделение (см.Рисунок 6.303).

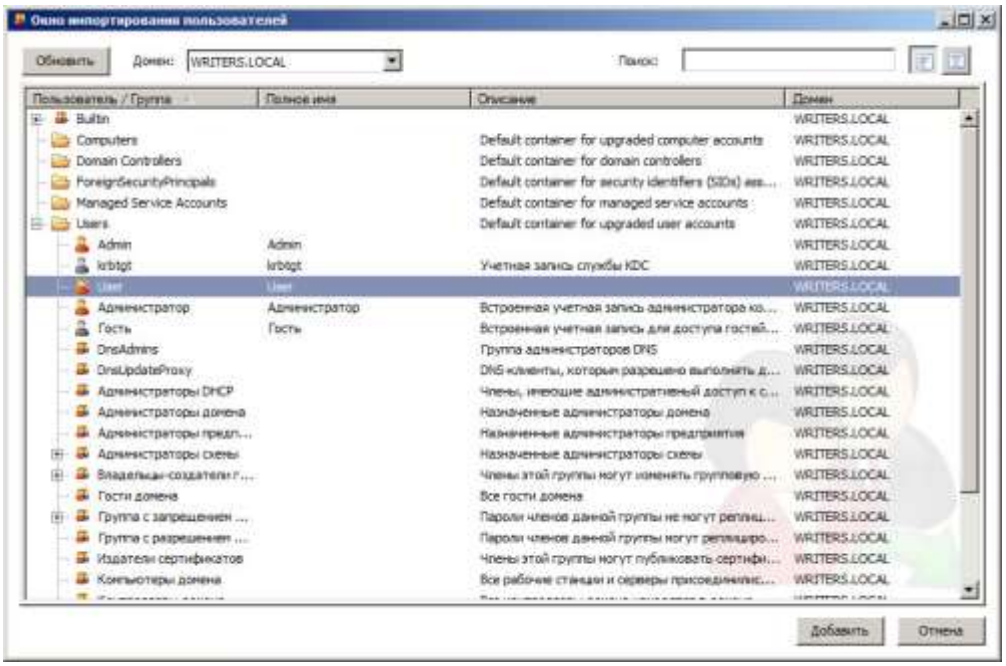


Рисунок 6.303

При добавлении HTTPIM-фильтра, выберите тип фильтра – запрещающий (запись в базу данных не производится) или разрешающий (сообщение записывается в базу данных).

Фильтры имеют приоритет и применяются последовательно в том порядке, в котором они заданы. Чем выше расположен фильтр, тем раньше он сработает. Управление порядком фильтров производится с помощью кнопок и .

6.8.5.2.5Фильтрация Cloud & SharePoint

Фильтры работают для данных облачных сервисов и SharePoint, позволяя отсечь лишние данные в перехвате.

Для их настройки на вкладке «Cloud & SharePoint фильтрация» установите флажок «Включить фильтрацию» и воспользуйтесь кнопкой «Добавить» для создания нового фильтра (см.Рисунок 6.304).

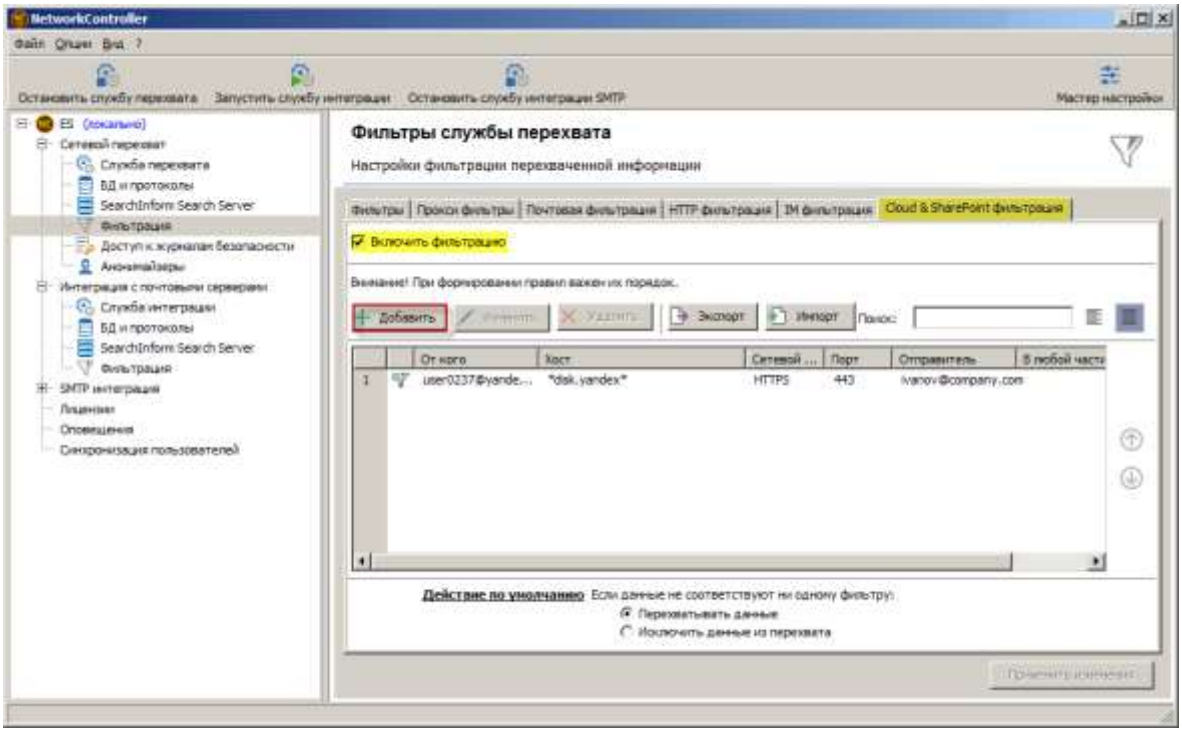


Рисунок 6.304

В появившемся окне укажите значения атрибутов документа, к которым будет применен фильтр:

- **От кого** - учетная запись пользователя ресурса (логин);
- **Хост** - адрес ресурса в сети;
- **Сетевой протокол** и **Порт** - используемые протокол и номер порта;
- **Отправитель** - полное доменное имя отправителя запроса. Чтобы выбрать отправителя из списка, щелкните кнопку . Также может быть выбрана группа или подразделение;
- **В любой части перехвата** - данные запроса, поиск по которым осуществлен как в адресной строке, так и в теле пакета (использование метасимвола «*» не допускается);
- **Размер** - размер запроса.

Рисунок 6.305

При добавлении фильтра выберите тип фильтра – запрещающий (запись в базу данных не производится) или разрешающий (сообщение записывается в базу данных).

Фильтры имеют приоритет и применяются последовательно в том порядке, в котором они заданы. Чем выше расположен фильтр, тем раньше он сработает. Управление порядком фильтров производится с помощью кнопок и .

6.8.6 Настройка механизма обработки доменных имен

Настройка политик производится на контроллере домена. Существует два варианта:

- настройка учетной записи сервиса перехвата (рекомендованный способ);
- запуск сервиса перехвата на компьютере, входящем в группу «Администраторы домена» (см. Рисунок 6.306).

Рисунок 6.306

6.8.6.1.1 Настройка учетной записи сервиса перехвата

Для настройки сервиса перехвата рекомендуется создать нового пользователя домена, обладающего правами чтения и управления журналами безопасности.

После создания нового пользователя откройте элемент «Политика безопасности контроллера домена» в папке «Администрирование».

Выберите «Параметры безопасности» / «Локальные политики» / «Назначение прав пользователя».

Добавьте созданного пользователя в политики «Создание журналов безопасности» / «Создание аудитов безопасности» (Generate security audits) и «Управление аудитом и журналом безопасности» (Manage auditing and security log) (см. Рисунок 6.307).

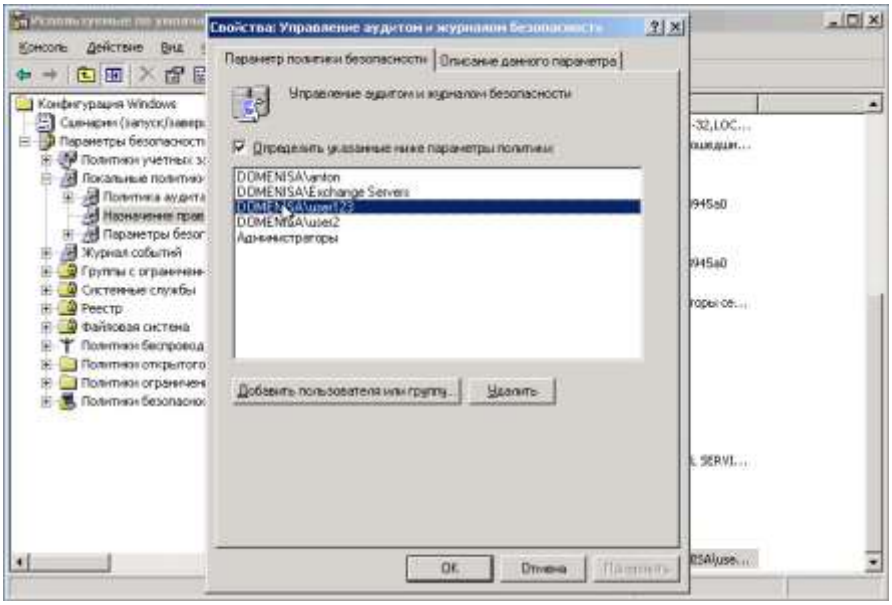


Рисунок 6.307

Необходимо, чтобы учетная запись пользователя обладала правом входа в качестве службы.

Настройка обладающих данным правом учетных записей производится в оснастке «Локальная политика» в разделе «Локальные политики» | «Назначение прав пользователя» | «Вход в качестве службы».

6.8.7 Особенности интеграции с Microsoft ISA/Forefront TMG

6.8.7.1 Устанавливаемые компоненты

На сервер Microsoft ISA/Forefront TMG устанавливается модуль интеграции NetworkController + ISA/Forefront и Search API.

Отдельно устанавливается сервер перехвата со стандартным набором компонентов NetworkController и Search API.

6.8.7.1.1 Сервер перехвата

На сервер перехвата устанавливается стандартный набор компонентов NetworkController и Search Server (см. Рисунок 6.308).

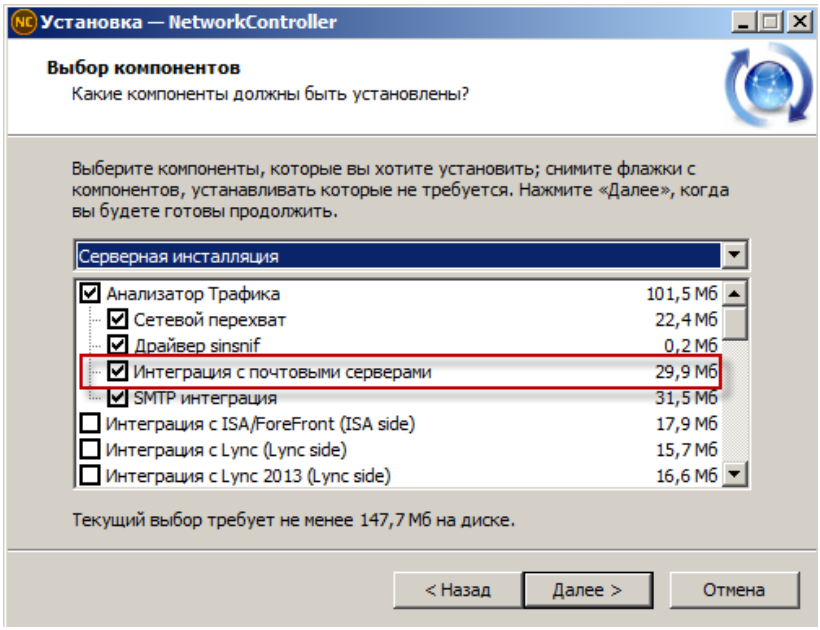


Рисунок 6.308

6.8.7.1.2 Сервер Microsoft ISA/Forefront TMG

Перед установкой модуля интеграции остановите сервер ISA/TMG!

Остановка и запуск сервера ISA/TMG производится под учётной записью администратора сервера при помощи команд **`net stop fwsrv`** и **`net start fwsrv`** (см. Рисунок 6.309).

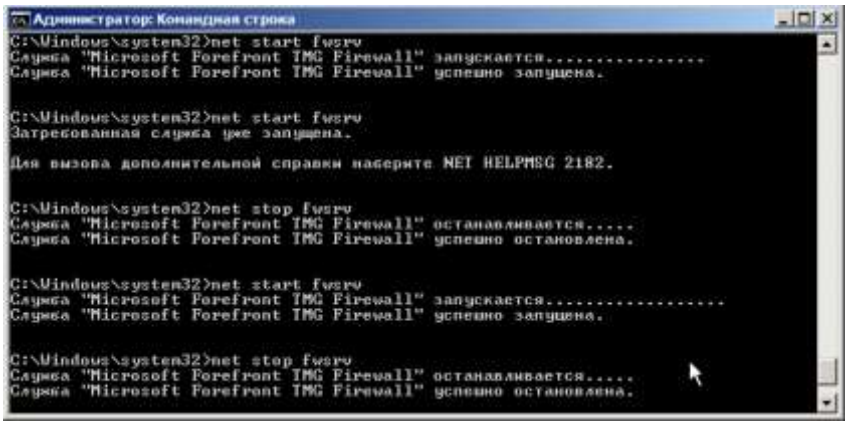


Рисунок 6.309

Убедитесь, что на ISA-сервере установлен пакет обновлений `vcredist_x86.exe` (`vcredist_x64.exe`). В случае отсутствия, загрузите данный пакет с сайта Microsoft (http://www.microsoft.com/downloads/ru-ru/details.aspx?FamilyID=c32f406a-f8fc-4164-b6eb-5328b8578f03) и установите.

Во избежание «падения» сетевых интерфейсов из-за высокой загруженности сети, на сервере ISA/TMG должна быть установлена самая свежая версия драйверов сетевой карты.

Выполните установку компонента интеграции NetworkController с ISA/Forefront. Вариант установки – «Модуль интеграции с ISA/Forefront» (см. Рисунок 6.310).

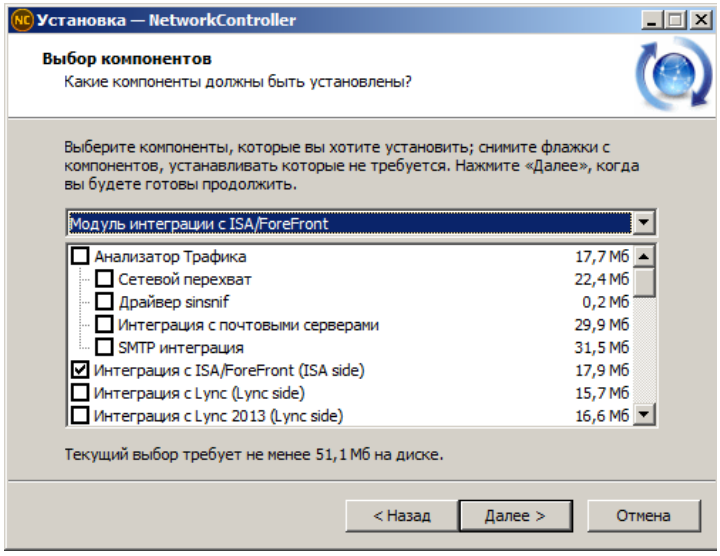


Рисунок 6.310

Также устанавливается компонент Search Corporate API (Рисунок 6.311).

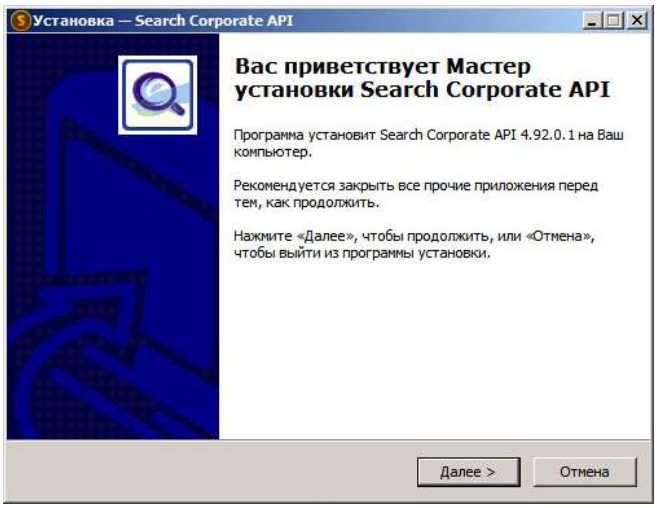


Рисунок 6.311

После установки запустите сервер ISA/TMG командой **`net start fwsrv`** (см. Рисунок 6.312).

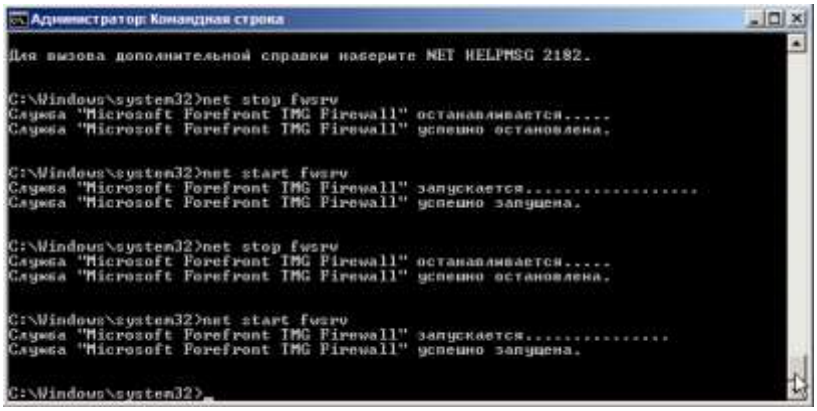


Рисунок 6.312

6.8.7.2 Проверка регистрации модуля интеграции ISA/TMG

В дереве консоли управления ISA/TMG щелкните узел «Система» (System).

В области вкладки «Фильтры приложений» (Application Filters) должен присутствовать плагин DataMonitor, означающий, что плагин успешно зарегистрирован (см. Рисунок 6.313). Также убедитесь, что на вкладке «Веб-фильтры» (Web Filters) присутствует плагин DataMonitorProxy.

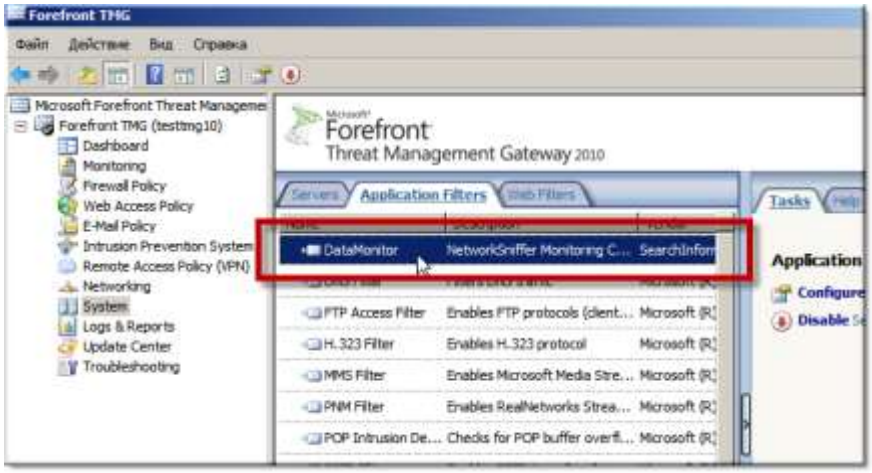


Рисунок 6.313

Если плагины отсутствуют, обновите список при помощи клавиши F5. Если плагины по-прежнему не отображаются в списке, удалите модуль интеграции NetworkController и произведите повторную установку с правами администратора компьютера.

6.8.7.3 Настройка обмена данными между серверами ISA/TMG и NetworkController

На сервере Microsoft ISA / Forefront TMG откройте файл **sinssvc.xml**, расположенный в папке **%ProgramFiles%\SearchInform\SearchInform NetworkController\SearchInform NetworkSniffer Server**, в которую установлен модуль интеграции NetworkController.

Произведите замену в файле следующих строк (см. Рисунок 6.314):

```
<icapservices>
     <enable>false</enable>
     <transport>
       <inuse>sock</inuse>
       <sock>
         <server>
           <ip>127.0.0.1</ip>
           <port>1344</port>
         </server>
       </sock>
     </transport>
     <preview_size>0</preview_size>
     <thread_num>128</thread_num>
     <filedebug>false</filedebug>
<max_reqmod_recv_size>33554432</max_reqmod_recv_size>
   </icapservices>
```

на

```
<icapservices>
  <enable>true</enable>          //включаем
  <transport>
    <inuse>sock</inuse>
    <sock>
      <server>
        <ip>192.168.X.X</ip>      //IP-адрес сервера NetwotkController
        <port>1344</port>
      </server>
    </sock>
  </transport>
  <preview_size>0</preview_size>
  <thread_num>128</thread_num>
  <filedebug>false</filedebug>
  <max_reqmod_recv_size>33554432</max_reqmod_recv_size>    // максимальный
размер
                                                          данных (в байтах),
                                                          которые может
                                                          принять NC по ICAP
                                                          (по умолч. – 32 Мб)
</icapservices>
```

При указании максимального размера необходимо учитывать тот факт, что данные могут отправляться в кодировке MIME, поэтому размер файла, передаваемого серверу NetworkController по протоколу ICAP, увеличивается на 33%. Таким образом, если данные будут отправлены не в кодировке MIME, а максимальный размер указан как «100000000», то NetworkController может перехватить также файл размером «130000000» байт.

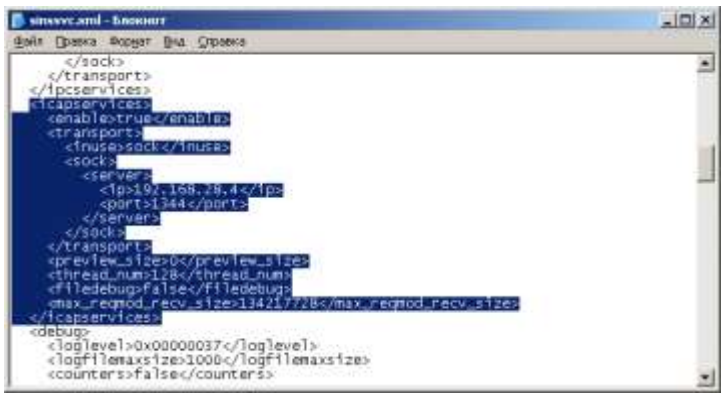


Рисунок 6.314

Сделайте аналогичные замены в файле `sinssvc.xml`, расположенном в той же директории на сервере NetworkController.

6.8.7.4 Создание определения протокола и его привязка к модулю интеграции

В дереве консоли управления ISA/TMG щелкните узел «Политика межсетевого экрана».

На вкладке «Инструментарий» (Toolbox) в области «Протоколы» (Protocols), нажмите кнопку «Создать» (New) и выберите «Протокол» (Protocol) (см. Рисунок 6.315).

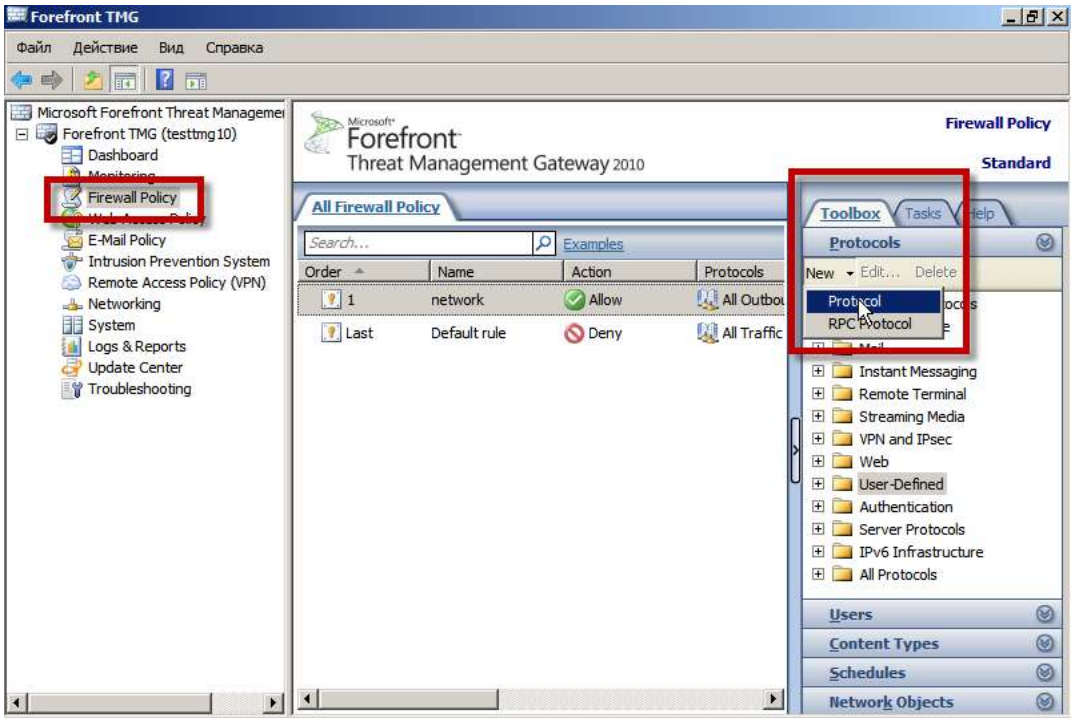
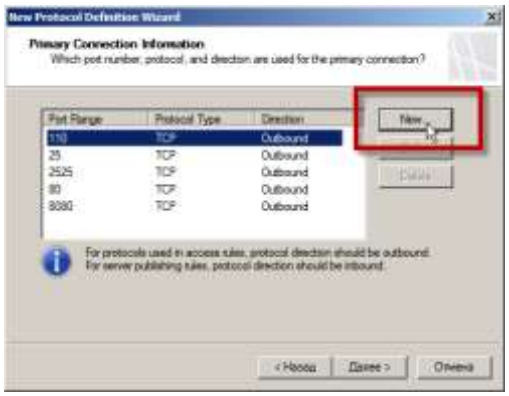
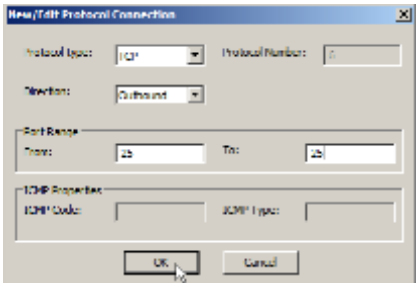


Рисунок 6.315

Произведите настройку с помощью мастера создания протокола, как указано в Таблица 39.

Таблица 39 – Привязка протокола к модулю интеграции

Страница мастера	Интерфейс (поле или свойство)	Настройка
Начальная страница	Имя определения протокола	Введите имя создаваемого определения протокола
Сведения о первичном соединении	Список добавляемых первичных соединений  Пример для протокола SMTP (порт 25):  	При помощи кнопки «Создать» (New) в определение нужно добавить все требуемые соединения. Настройки: • «Тип протокола» (Protocol type) – TCP; • «Направление» (Direction) – «исходящий» (outbound); • «Диапазон портов» (Port range) – выберите те порты, по которым необходимо отслеживать трафик. Для снижения нагрузки на серверы, рекомендуется использовать только те порты, которые используются для передачи данных по требуемым протоколам. **Внимание!** В созданный протокол не рекомендуется попадание трафика со следующих портов: • на котором работает HTTP-прокси (обычно 80 и 8080), • по которому передаются данные между ISA/TMG и NetworkController (обычно 1344), • по которому работает RDP (обычно 3389).
Сведения о дополнительном соединении	Вы хотите использовать дополнительные соединения?	«Нет» (по умолчанию).
Завершение работы мастера		Просмотрите параметры и щелкните кнопку «Готово» (OK).

Обновите консоль.

В раскрывающемся списке откройте созданное определение протокола, которое находится в папке «Пользовательские» (User-defined) (см. Рисунок 6.316).

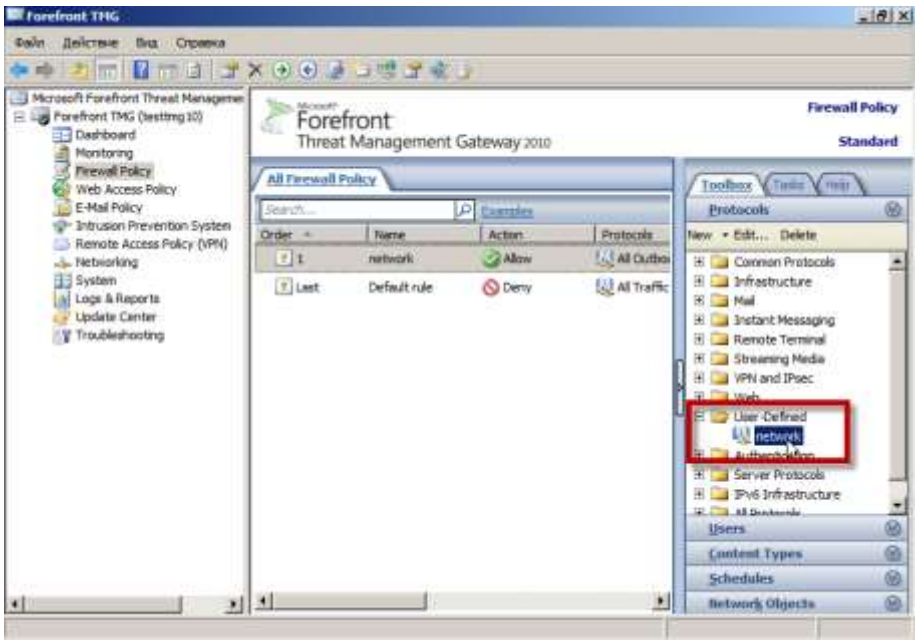


Рисунок 6.316

На вкладке «Параметры» (Parameters), установите флажок для созданного плагина DataMonitor и привяжите плагин к добавленным в определение протокола соединениям. Для привязки выделите соединение и установите флажок DataMonitor (см. Рисунок 6.317).

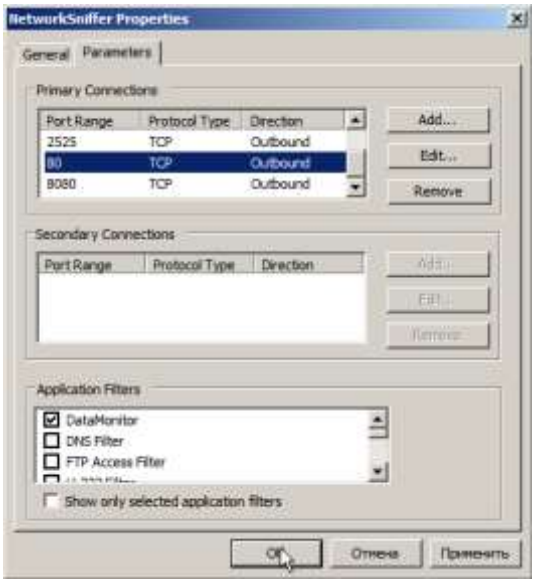


Рисунок 6.317

Перезапустите сервер ISA/TMG:

```
net stop fwsvr
net start fwsvr.
```

После запуска сервера ISA/TMG откройте диспетчер задач или другой менеджер процессов. Должен быть запущен процесс `svcisagate.exe` (см. Рисунок 6.318). Активный

процесс означает, что плагин забирает трафик и пытается передать его серверу NetworkController в соответствии с заданными настройками.

Рисунок 6.318

6.8.8 Особенности интеграции с прокси-серверами по протоколу ICAP

Сервер NetworkController способен интегрироваться с программными и аппаратными прокси-серверами, работающими по протоколу ICAP.

Для взаимодействия NetworkController с прокси-серверами, работающими по протоколу ICAP, должны быть соблюдены следующие условия:

1) Включен протокол ICAP.
2) Прокси-сервер должен быть настроен в качестве ICAP-клиента, сервер NetworkController – в качестве ICAP-сервера.

Механизм перехвата (см. Рисунок 6.319):

1. Пользователь передает данные.
2. Данные проходят через прокси-сервер.
3. Прокси-сервер (ICAP-клиент) передает данные по протоколу ICAP к серверу NetworkController (ICAP-сервер).
4. Сервер NetworkController записывает информацию в базу данных.

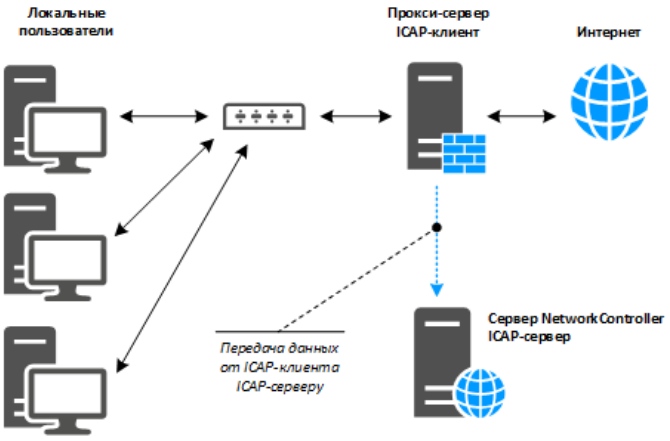


Рисунок 6.319

6.8.8.1 Предварительная настройка NetworkController

Произведите настройку сервера NetworkController.

Откройте файл конфигурации сервиса перехвата `sinssvc.xml`, расположенный в папке: `%ProgramFiles%\SearchInform\SearchInform NetworkController\SearchInform NetworkController Server\`.

Произведите следующие замены:

```
<icapservices>
    <enable>true</enable>            //включаем работу по протоколу ICAP
    <transport>
      <inuse>sock</inuse>
      <sock>
        <server>
          <ip>192.168.X.X</ip>       //IP-адрес сервера NetworkController
          <port>1344</port>
        </server>
      </sock>
    </transport>
    <preview_size>0</preview_size>
    <thread_num>128</thread_num>
    <filedebug>false</filedebug>
    <max_reqmod_recv_size>33554432</max_reqmod_recv_size> //максимальный размер
                                                          данных (в байтах),
                                                          которые может
                                                          принять
                                                          NetworkController
                                                          по ICAP(по умолч. –
                                                          32 Мб)
</icapservices>
```

При указании максимального размера необходимо учитывать тот факт, что данные могут отправляться в кодировке MIME, поэтому размер файла, передаваемого серверу NetworkController по протоколу ICAP, увеличивается на 33%. Таким образом,

если данные будут отправлены не в кодировке MIME, а максимальный размер указан как «100000000», то NetworkController может перехватить также файл размером «130000000» байт.

Перезапустите сервис перехвата.

6.8.9 Настройка прокси-серверов

На данный момент поддерживается интеграция со всеми прокси-серверами, которые поддерживают ICAP: достаточно популярным программным прокси-сервером SQUID, некоторыми аппаратными решениями, умеющими декодировать HTTPS и отдавать его по прооколу ICAP, например, Blue Coat ProxySG, Cisco IronPort (устройства управления IronPort M-серии и web-шлюзы IronPort S-серии).

6.8.9.1 Настройка Blue Coat ProxySG

Сервер NetworkController способен интегрироваться с устройствами Blue Coat ProxySG, используя безопасный протокол ICAP. Интеграция с ProxySG позволит серверу NetworkController перехватывать исходящий зашифрованный HTTPS-трафик. Порядок настройки ProxySG:

1. Настройте ICAP-сервис на ProxySG для исходящих соединений.
2. Создайте политику для исходящего трафика.

6.8.9.1.1 Настройка ICAP-сервиса для исходящих соединений

Откройте консоль управления Blue Coat ProxySG.

На вкладке Configuration (Настройка) откройте объект **External Services** | **ICAP** (Внешние сервисы | ICAP).

Щелкните кнопку **New** (Создать) и задайте имя ICAP-сервиса (см. Рисунок 6.320). Используйте легко идентифицируемое название, например, «NetworkController» или «DLP».

Рисунок 6.320

Настройте созданный ICAP-сервис:

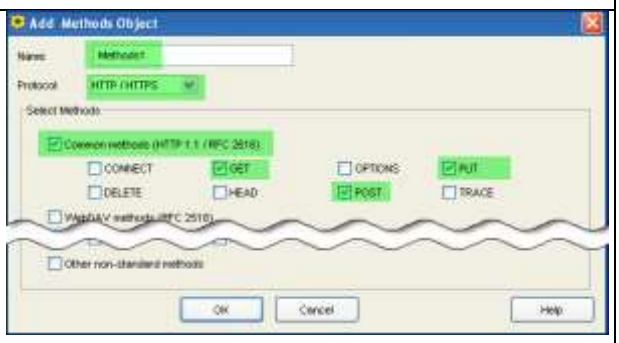
- Выберите созданный сервис и щелкните кнопку **Edit**.
- В качестве **Service URL** введите URL-адрес сервера NetworkController в следующем формате: `icap://<IP-адрес сервера NetworkController>`
- В области **ICAP v1.0 Options** выберите верную опцию поддерживаемого метода (**Method supported**) – **request modification** (Модификация исходящего запроса).
- Для автоматического получения настроек IS-TAG от сервера NetworkController, щелкните кнопку **Sense settings** (Считать настройки).
- Для подтверждения полученных настроек щелкните кнопку **OK**.

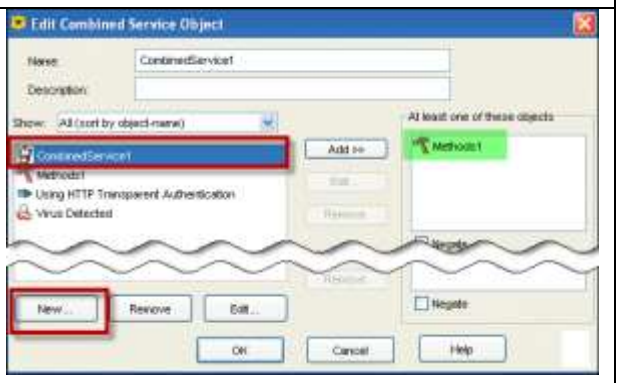
Перед закрытием окна производится автоматическая проверка состояния ICAP-службы. Если проверка статуса и получение настроек прошло успешно, считанные настройки сохраняются.

6.8.9.1.2Создание политики для исходящего трафика

Создайте фильтр веб-доступа (Web Access Layer) для созданного ICAP-сервиса. Для этого щелкните **Policy** (Политика) в верхней части окна и выберите **Web Access Layer**. Следуйте инструкциям из Таблица 37.

Таблица 37 – Создание сервис-объекта

Действие	Снимок экрана
Щелкните правой клавишей настройку **Setting** и выберите **Set** (Настроить). Будет открыто диалоговое окно **Set Service Object** (Настроить сервис-объект).	
Щелкните **New** и выберите **Protocol Methods** (Методы протоколов). Будет открыто диалоговое окно Add methods (Добавить методы).	
Введите имя создаваемого метода протокола (опционально). В выпадающем меню **Protocols** (Протоколы) выберите **HTTP/HTTPS.** Будут отображены параметры выбора HTTP/HTTPS методов. Установите флажок **Common methods** (Общие методы). После этого, установите флажки **GET, POST и PUT**. Щелкните OK для настройки HTTP/HTTPS-метода и закройте диалоговое окно.	

Действие	Снимок экрана
После настройки метода создайте сервис-объект. Для этого щелкните кнопку **New**, выберите **Combined Service Object** (Комбинированный сервис объект). Будет открыто диалоговое окно Add Combined Service Object (Добавить комбинированный сервис объект).	
Выберите созданный HTTP/HTTPS метод и щелкните кнопку **Add** (Добавить) для добавления в комбинированный сервис-объект. Будет открыто диалоговое окно Add Combined Service Object (Добавить комбинированный сервис-объект).	
Щелкните кнопку OK и закройте диалоговое окно. Щелкните кнопку OK. Комбинированный сервис-объект будет настроен в качестве фильтра веб-доступа.	

6.8.9.1.3Настройка действия

После настройки сервис-объекта настройте действие, применяемое для политики.

Щелкните правой клавишей мыши по настройке **Action** (Действие) и выберите **Set** (Настроить). Будет открыто диалоговое окно Set Action Object (Настроить действие объекта).

Щелкните кнопку **New** и выберите **Set ICAP Request Service** (Установить сервис ICAP для исходящего трафика). Будет открыто диалоговое окно «Add ICAP Request Service» («Добавить сервис ICAP для исходящего трафика»), отображенное на Рисунок 6.321.

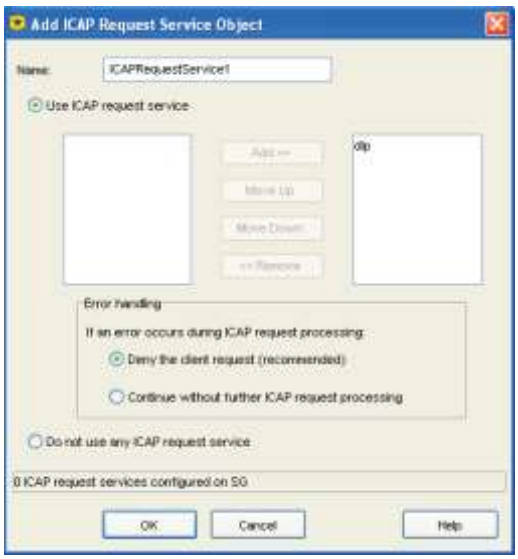


Рисунок 6.321

Введите имя создаваемого действия, привязанного к ICAP-сервису (опционально).

Выберите созданный ICAP-сервис и щелкните кнопку **Add** для его применения по отношению к объекту. Для создания объекта ICAP-сервиса щелкните кнопку «OK».

ICAP-сервер (NetworkController) и ICAP-клиент (Blue Coat) работают в тесной связке друг с другом. В случае обрыва связи между этими серверами, Blue Coat может отметать запросы пользователей, что чревато отсутствием связи с сетью Internet у пользователей. Во избежание таких последствий, в группе параметров **Error handling** (Обработка ошибок) установите флажок **Continue without further ICAP request processing** (Продолжить без дальнейшей обработки ICAP-запроса).

Для применения объекта ICAP-службы щелкните кнопку «OK». Закройте диалоговое окно.

6.8.9.2 Блокировка HTTP(S)-трафика

При интеграции с программными и аппаратными прокси-серверами, работающими по протоколу ICAP, становится доступной функция блокировки передачи данных по HTTP(S)-протоколу.

Для настройки взаимодействия NetworkController с прокси-серверами, работающими по протоколу ICAP необходимо произвести предварительную настройку на вкладке «ICAP» узла «Служба перехвата»:

1) Включите протокол ICAP, установив флажок «ICAP».
2) Укажите IP-адрес сервера NetworkController, который будет выступать в качестве ICAP-сервера. Прокси-сервер в данном случае должен быть настроен как ICAP-клиент.
3) Укажите прослушиваемый ICAP-сервером порт.

Сохраните настройки кнопкой «Применить изменения» (см. Рисунок 6.322).

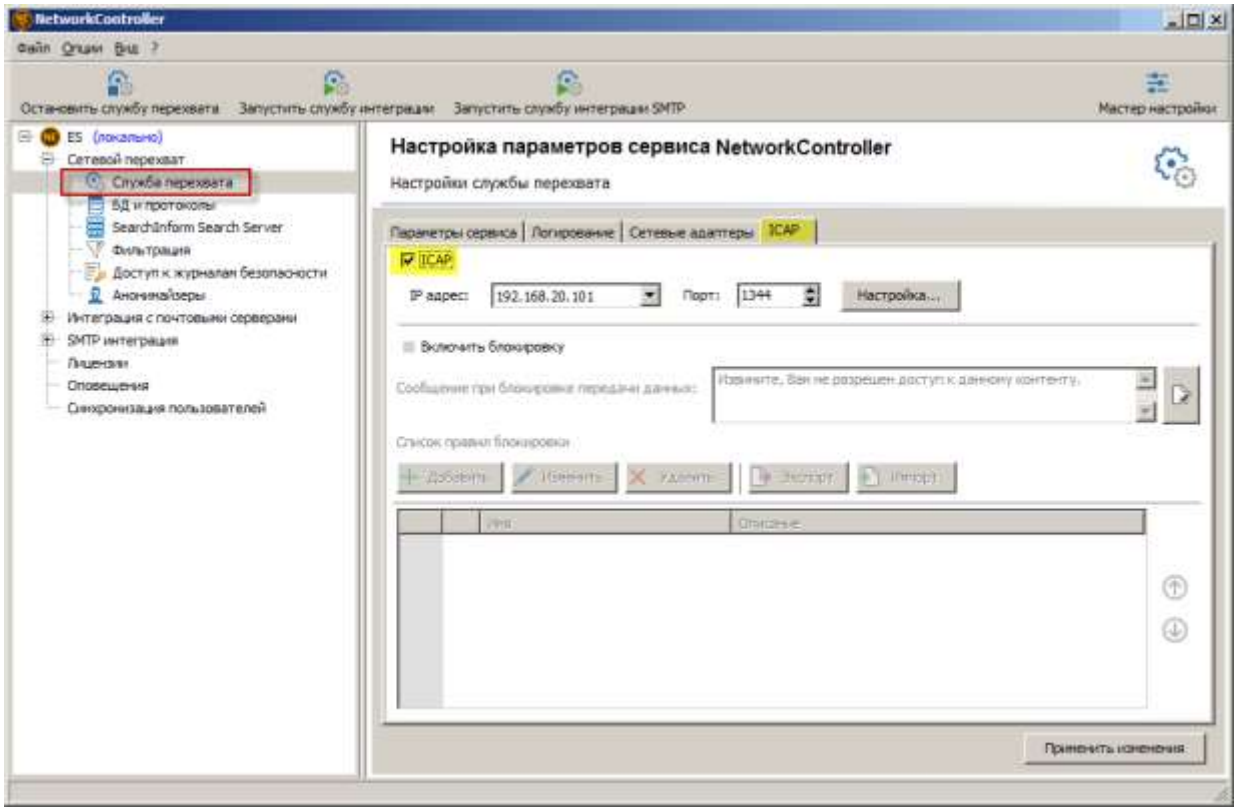


Рисунок 6.322

С помощью кнопки «Настройка...» открывается окно дополнительных параметров ICAP, в котором можно ограничить размер перехватываемых данных, количество одновременных подключений, а также настроить фильтрацию данных по MIME-типам (для RESPMOD) (см. Рисунок 6.323).

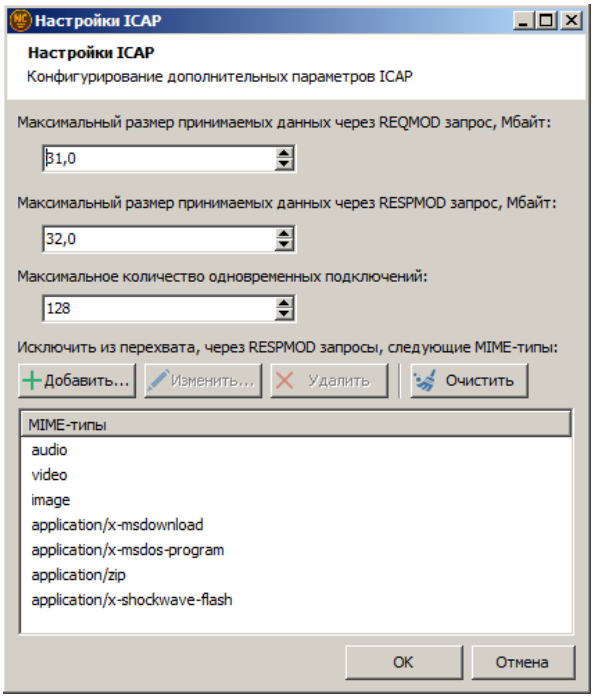


Рисунок 6.323

Для управления MIME-типами данных используйте кнопки «Добавить», «Редактировать», «Удалить», «Очистить». По завершении настроек нажмите «ОК».

Сохраните настройки ICAP нажатием кнопки «Применить изменения».

6.8.9.2.1 Настройка блокировки передачи данных

Для корректной работы функции блокировки HTTP(S)-трафика потребуется настройка определенных правил, на основании которых те или иные данные будут заблокированы либо разрешены к отправке.

Установите флажок «Включить блокировку» и нажмите кнопку «Добавить» для добавления нового правила (см. Рисунок 6.324).

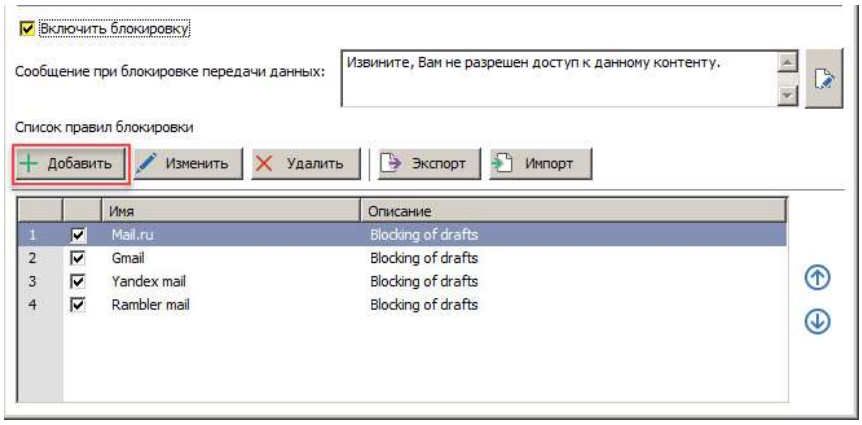


Рисунок 6.324

В окне «Добавление правила блокировки» задайте имя фильтра и (при необходимости) его описание. В области «Условия» нажмите кнопку «Добавить условие» либо щелкните по направляющей стрелке рядом с кнопкой и выберите сразу необходимый критерий (см. Рисунок 6.325).

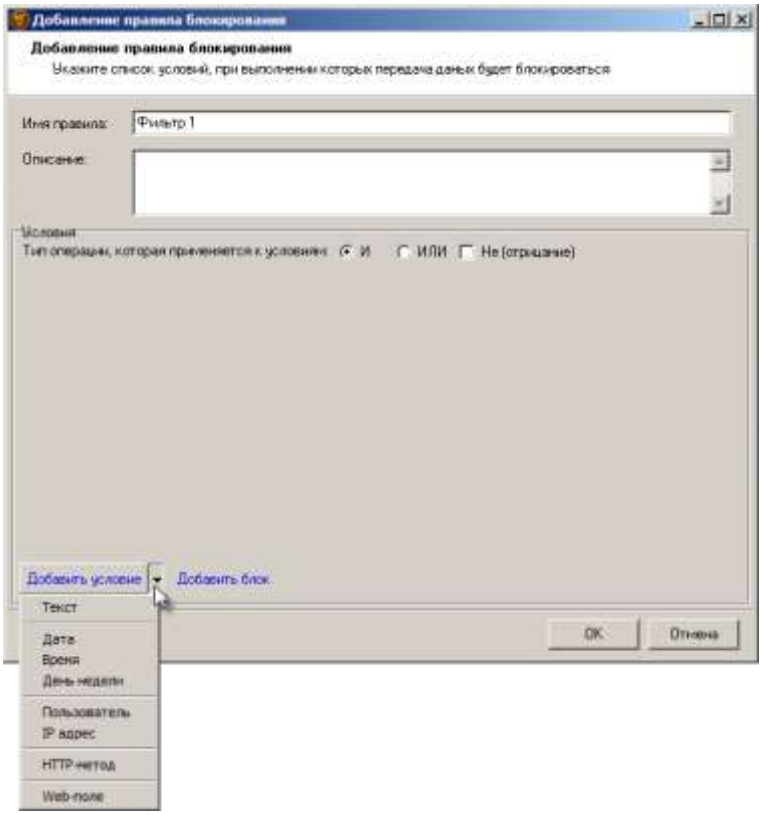


Рисунок 6.325

Сконфигурируйте значения выбранного критерия.

Значения критериев могут быть указаны вручную либо выбраны из списка.

При необходимости, добавьте остальные условия для текущего правила, воспользовавшись кнопкой «Добавить условие». Для удаления условия предназначена кнопка  (см. Рисунок 6.326).

Для добавления вложенного условия нажмите кнопку «Добавить блок», затем – «Добавить условие».

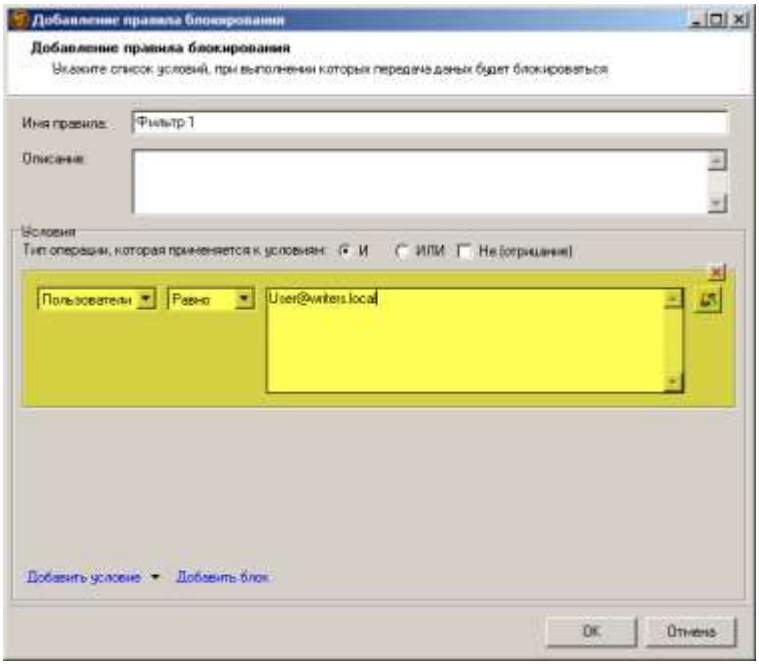


Рисунок 6.326

Условия могут взаимодействовать друг с другом согласно логическим операциям:

- логическое И (должны совпасть все условия одновременно),
- логическое ИЛИ (может совпасть хотя бы одно из условий),
- логическое НЕ (полное несоответствие ниженастроенному условию).

По окончании настройки правила блокировки, нажмите «ОК» для добавления его в консоль.

Настроенные правила применяются в том порядке, в котором они заданы. Чем выше расположено правило, тем раньше оно сработает. Управление порядком правил производится с помощью кнопок  и  (см.Рисунок 6.327).

Рисунок 6.327

Отредактируйте текстовое сообщение, которое будет выводиться пользователю при блокировке отправки. Редактор открывается в новом окне (см.Рисунок 6.328).

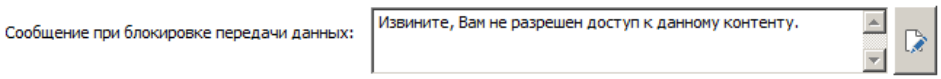


Рисунок 6.328

Для сохранения и загрузки списка фильтров предусмотрены кнопки «Экспорт» и «Импорт». Поддерживаются форматы .xml, .txt и .csv.

Для поиска по списку заданных фильтров укажите значение атрибута, по которому будет производиться поиск, в поле «Поиск», и определите, в какой части значений атрибутов искать введенный запрос.

6.8.10 Особенности интеграции с почтовыми серверами

Сервер NetworkController включает в себя службу интеграции (SILS.exe), предназначенную для получения сообщений напрямую с почтового сервера.

Функции службы:

- сбор сообщений с почтовых серверов;
- обработка полученных данных и запись в базу данных, которая может быть обработана поисковым движком.

Настройка производится в узле «Интеграция с почтовыми серверами». Предварительная настройка может быть произведена при помощи мастера (см. Таблица 37).

6.8.10.1 Устанавливаемые компоненты

Устанавливается «серверная инсталляция» NetworkController, включая компонент «Интеграция с почтовыми серверами» (см. Рисунок 6.329).

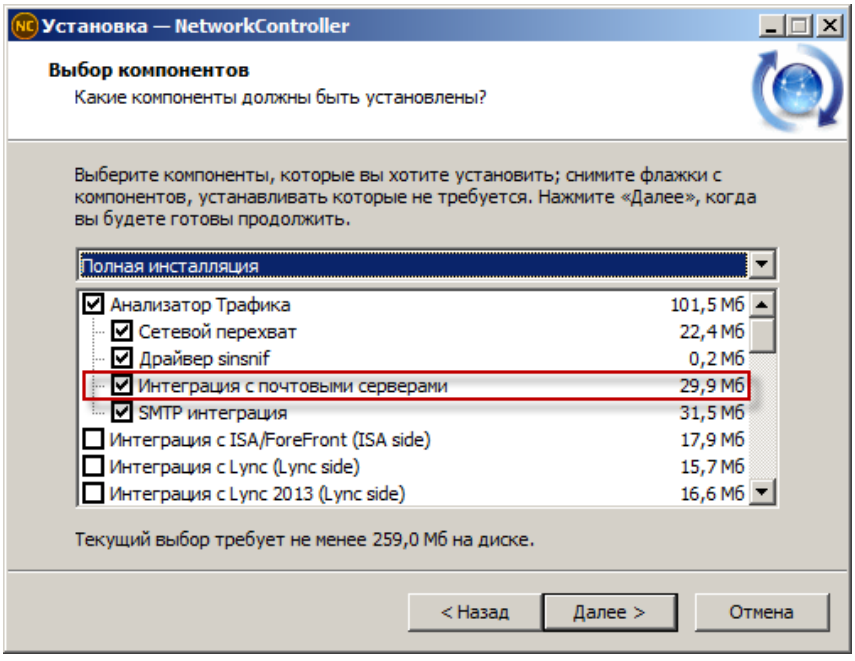


Рисунок 6.329

6.8.10.2 Фильтрация сообщений, собранных с почтовых серверов, и определение пользователей

Настройки фильтрации производятся после предварительной настройки службы интеграции с помощью мастера (см. Таблица 37).

6.8.10.3 Настройка соответствий «e-mail адрес – доменное имя»

Полученные от почтового сервера сообщения либо отчеты журнала проверяются по списку привязок доменных пользователей к почтовым адресам. Если найдено совпадение (по любому из адресов «От кого» или «Кому»), сообщение проверяется по атрибутным фильтрам (п. 6.8.10.5) и, в зависимости от результата проверки по атрибутам, записывается или не записывается в базу. Записанным в базы сообщениям присваивается доменное имя отправителя/получателя.

Получение списка доменных пользователей из Active Directory возможно двумя способами:

- в автоматическом режиме в процессе синхронизации с Active Directory с определенной частотой, указанной в параметре «Получать список пользователей каждые ... часов»;
- в ручном режиме, когда необходимо обновить список пользователей в настоящий момент, по нажатию кнопки «Получить» (см. Рисунок 6.330).

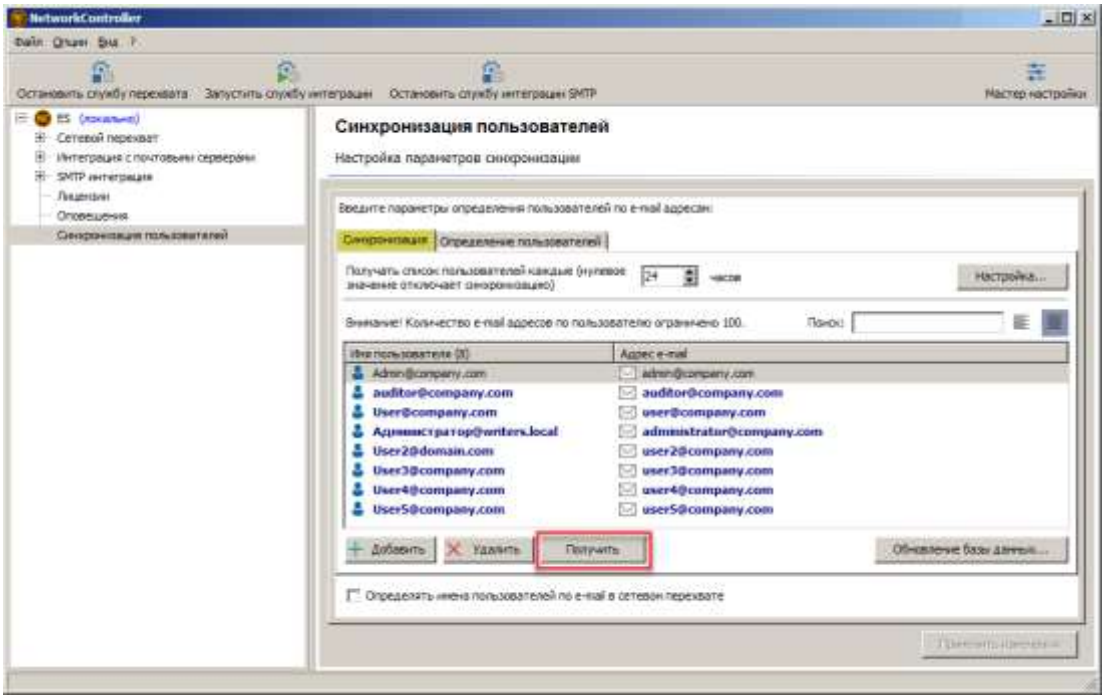


Рисунок 6.330

Для установки параметров синхронизации кликните кнопку «Настройка» (см. Рисунок 6.331).

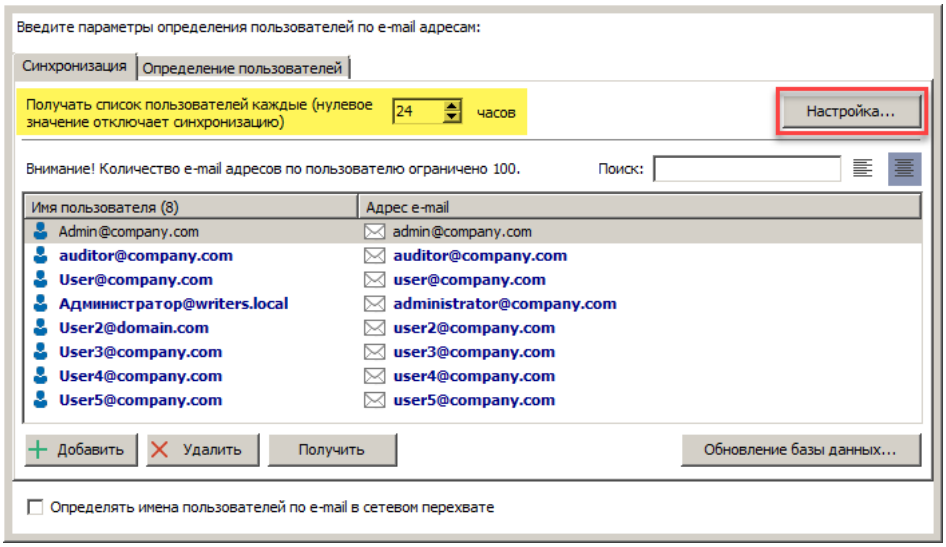


Рисунок 6.331

Список пользователей может быть получен:

- из базы данных DataCenter (может быть выбрано к чтению несколько доменов);
- из Active Directory (вычитке подлежит только текущий домен).

Для чтения базы данных DataCenter введите имя сервера DataCenter в поле «Сервер» вручную либо нажмите кнопку  и укажите его в появившемся окне (с возможностью проверки имени в Active Directory) (см.Рисунок 6.332).

Рисунок 6.332

Кнопка «Список доменов» открывает окно выбора доменов для синхронизации (см. Рисунок 6.333).

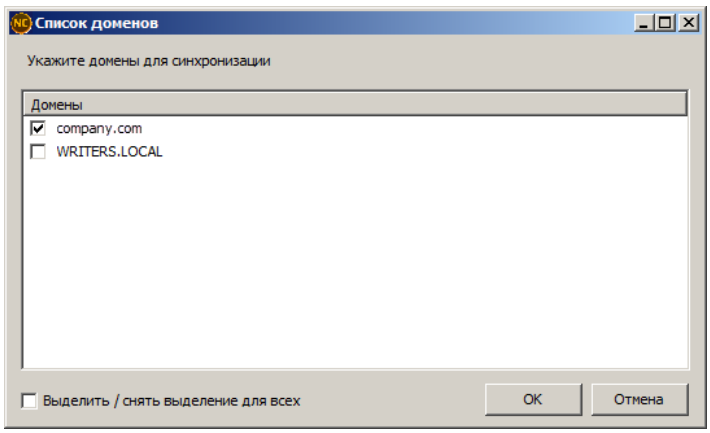


Рисунок 6.333

Выберите имя домена и нажмите «ОК».

Получение информации из Active Directory можно произвести вручную, нажав кнопку «Получить» (см. Рисунок 6.334).

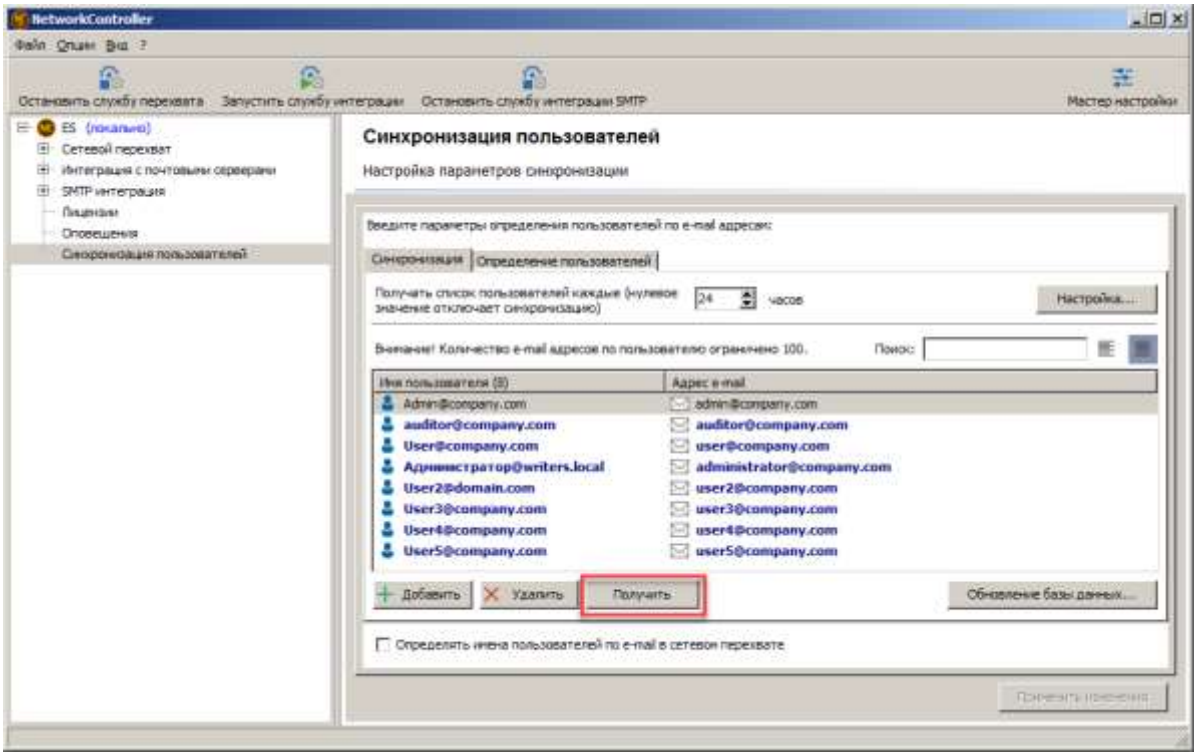


Рисунок 6.334

При отсутствии адресов электронной почты в доступных каталогах, привязку почтовых адресов к доменным пользователям можно настроить вручную. Для этого щёлкните кнопку «Добавить» и в появившемся диалоговом окне введите адрес электронной почты, щёлкните «ОК» (см. Рисунок 6.335).

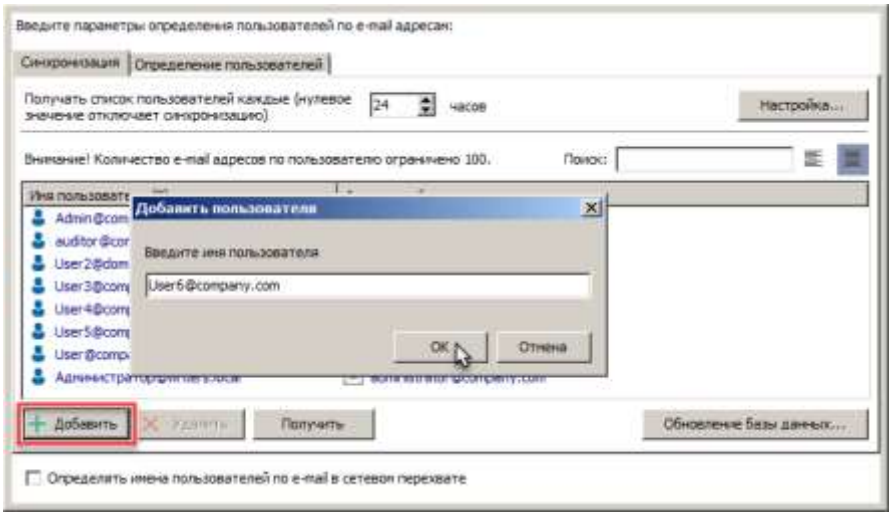


Рисунок 6.335

Затем задайте соответствующий пользователю электронный адрес (см. Рисунок 6.336).

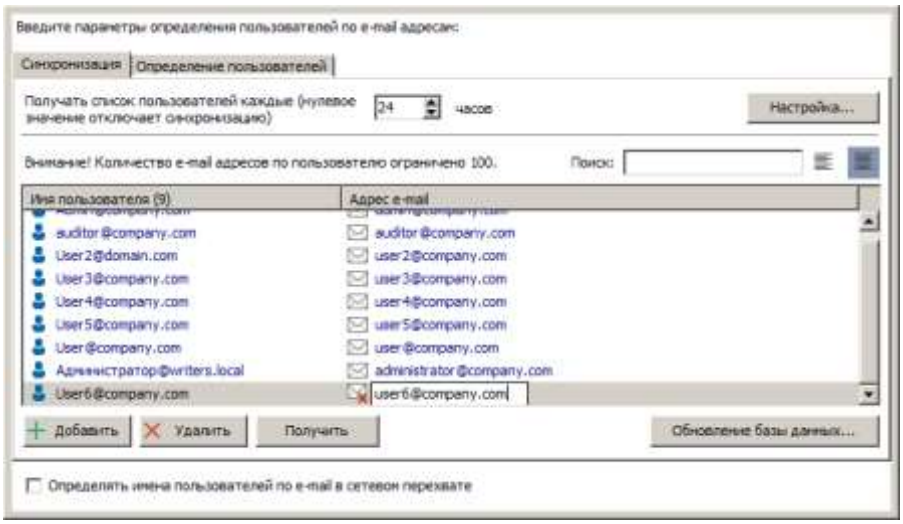


Рисунок 6.336

6.8.10.4 Фильтрация по маскам

Если сообщение не прошло проверку по соответствиям «e-mail адрес – доменное имя» (см. п. 6.8.10.3), то оно проверяется по маскам почтовых адресов «От кого» и «Кому». Сообщениям, прошедшим фильтрацию по маскам почтовых адресов, не присваивается значение доменного пользователя.

Обрабатываемые адреса получателей и отправителей сообщений могут иметь форматы: *petr.sidorov@company.ru* (простой почтовый адрес) или Петр Сидоров *<petr.sidorov@company.ru>* (полный почтовый адрес с именем пользователя). Поэтому рекомендуется, чтобы маски по почтовым адресам начинались и заканчивались символом «*».

Настройка фильтров по маскам производится на вкладке «Синхронизация пользователей | Определение пользователей». Нажмите «Добавить» и введите маску (см. Рисунок 6.337).

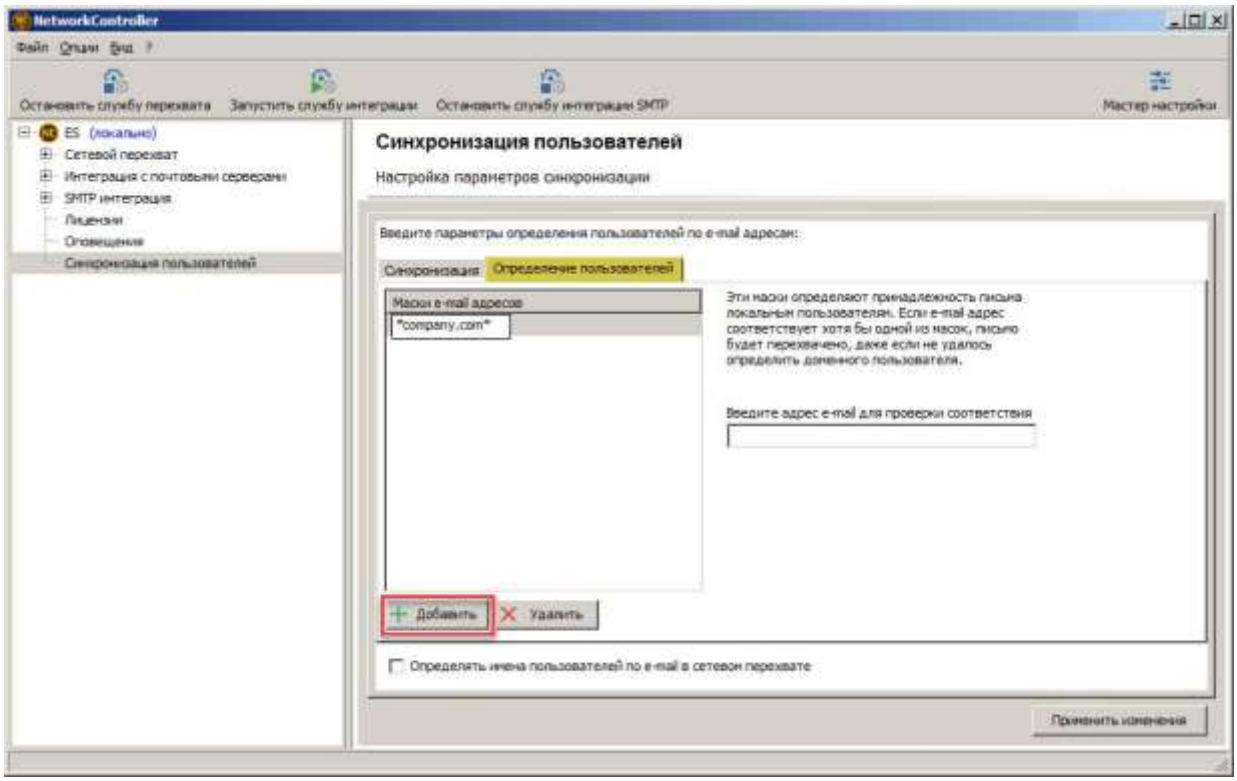


Рисунок 6.337

Для проверки корректности маски введите тестовый адрес электронной почты. Маски, удовлетворяющие введенному адресу, маркируются при помощи флажка (см. Рисунок 6.338).

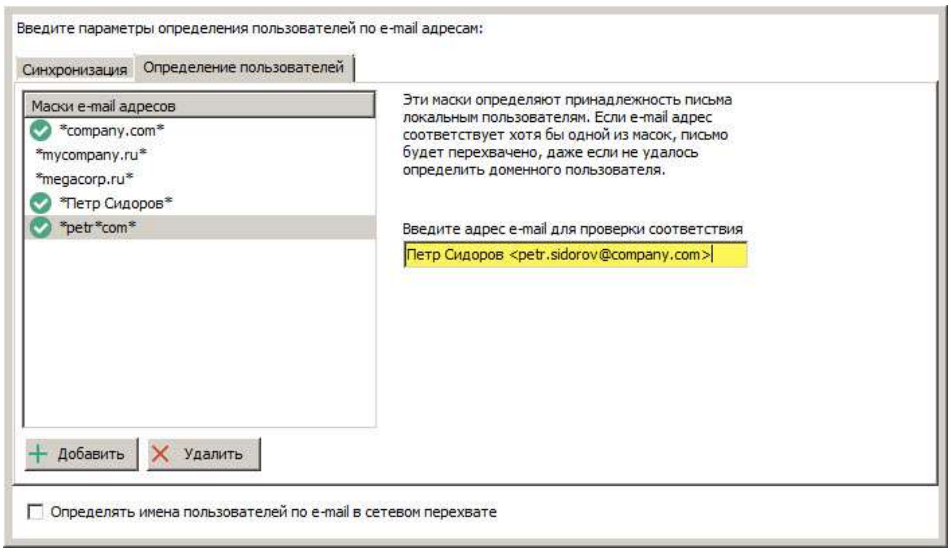


Рисунок 6.338

Для использования данного принципа определения доменных имен пользователей при сетевом перехвате трафика, отметьте флажком параметр «Определять имена пользователей по e-mail в сетевом перехвате».

После настройки фильтров по маскам адресов, примените изменения.

6.8.10.5 Фильтрация по атрибутам почтовых сообщений

Сообщения, прошедшие проверку по соответствиям «e-mail адрес – доменное имя» и по маскам адресов, проверяются по атрибутам сообщений. В зависимости от результата проверки по атрибутам, сообщения записываются или не записываются в базу. Правила фильтрации по атрибутам:

1) Условия бывают разрешающими и запрещающими. Если сообщение попадает под разрешающее правило, производится запись в базу. Если сообщение попадает под запрещающее условие, сообщение не записывается в базу.
2) Проверку можно производить по следующим атрибутам:
   - e-mail (поля «От кого», «Кому»);
   - доменные имена пользователей (поля «Отправитель», «Получатель»);
   - свойства письма (поля «Тема», «Размер»).
3) Фильтры имеют приоритет и проверяются последовательно в том порядке, в котором они заданы, до первого совпадения.
4) Строгий фильтр срабатывает (исключить/сохранить письмо), если условиям фильтра удовлетворяет хотя бы один заданный параметр (например, имя хотя бы одного адресата), и запрещает отработку следующих за ним фильтров.
   Нестрогий (обычный) фильтр сработает только в том случае, когда под условие одного или нескольких фильтров попадут все параметры (например, весь список адресатов). Фильтр запоминает сработавшее состояние и продолжает отработку следующих фильтров.
5) Если сообщение не подпадает ни под одно условие, выполняется действие по умолчанию.

Особенности фильтров по атрибутам:

- При настройке фильтров рекомендуется использовать маски с символом «*», замещающие произвольный текст.
- Управление списком фильтров производится при помощи кнопки «Добавить», «Изменить», «Удалить».
- Управление иерархией фильтров производится при помощи кнопок  и  .

Для создания и настройки фильтра выделите узел «Фильтрация» в группе «Интеграция с почтовыми серверами». Отметьте параметр «Включить фильтрацию» и щелкните кнопку «Добавить» (см. Рисунок 6.339).

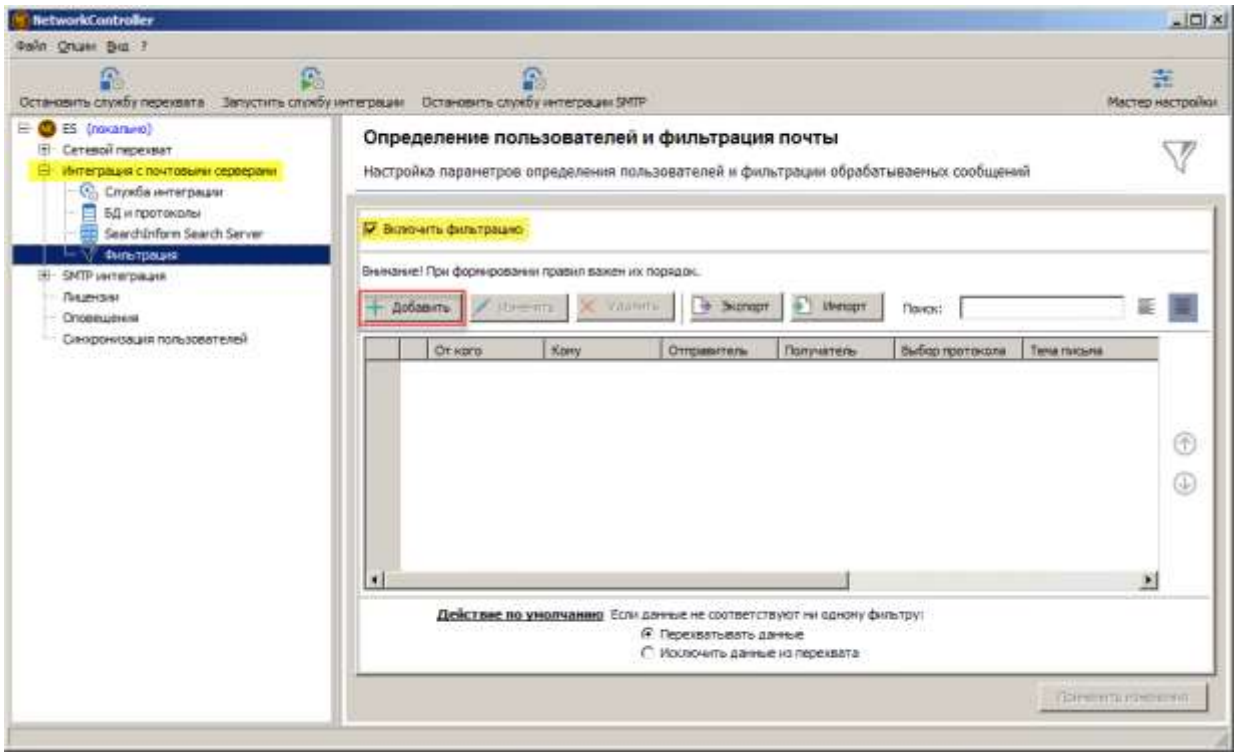


Рисунок 6.339

В появившемся окне фильтра настройте (см. Рисунок 6.340) атрибуты филтра:

- e-mail адрес (поля «От кого», «Кому»),
- доменное имя пользователя (определяется по привязкам почтовых адресов),
- тема письма,
- размер письма,
- количество получтелей.

Установленный флаг **«Строгий»** определяет сработку фильтра, если условиям фильтра удовлетворяет хотя бы один адресат. После чего остальные фильтры не обрабатываются. При снятом флажке (нестрогий фильтр) запоминается сработавшее состояние фильтра (запретить/разрешить) и последовательная работа остальных фильтров в списке продолжается. Нестрогий фильтр сработает только в том случае, когда под условие одного или нескольких фильтров попадут все адресаты.

Параметр «**Выбирать протокол по совпадению отправителя/получателя»** активируется для исключения дублирования в индексе одного и того же внутреннего письма (между двумя доменными пользователями). При настройках, показанных на Рисунок 6.340, письмо не попадет в SMTP и POP3 таблицы одновременно.

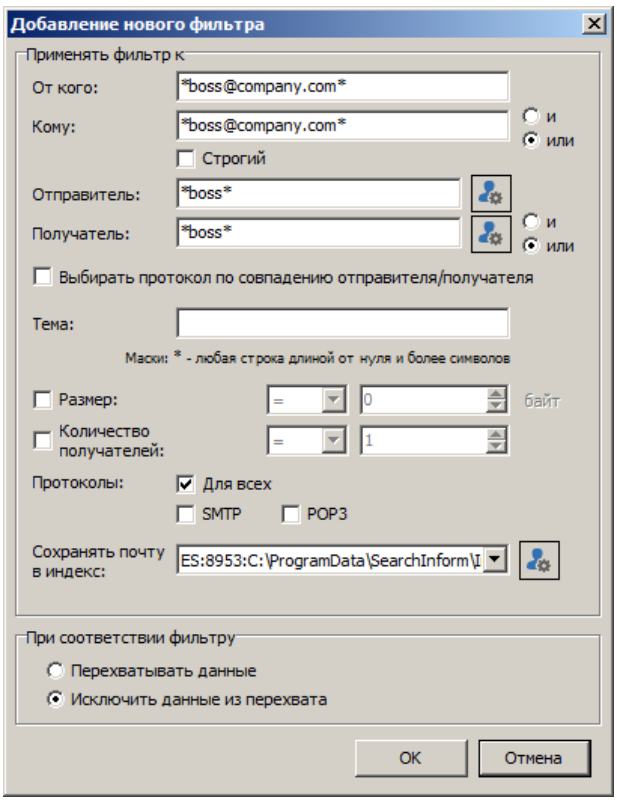


Рисунок 6.340

Параметр **«Сохранять почту в индекс»** позволяет выбрать индекс, в который будет помещаться текст почтовых сообщений. Если для входящей и исходящей почты будут настраиваться отдельные фильтры, то, соответственно, она будет сохраняться в разные индексы.

Также настройте действие по умолчанию, когда письмо не будет соответствовать ни одному фильтру (см.Рисунок 6.341).

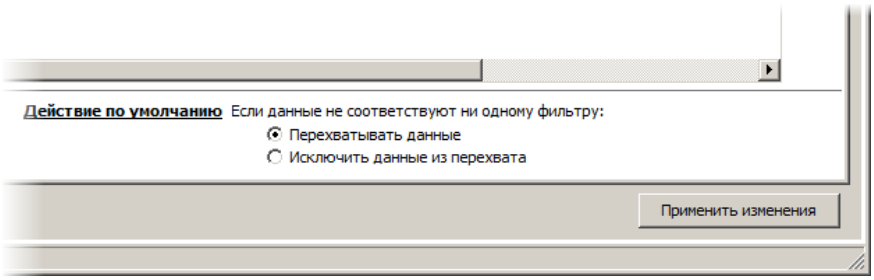


Рисунок 6.341

Примените заданные параметры, щелкнув по кнопке «Применить изменения».

Кнопки **«Экспорт/Импорт»** позволяют сохранить/загрузить конфигурацию фильтров в нескольких форматах: txt, lst, cvs (см. Рисунок 6.342).

Для поиска фильтра из имеющегося списка в поле **«Поиск»** введите название атрибута, по которому необходимо произвести поиск, и укажиет в какой части атрибута содержится искомый текст (кнопки  или ).

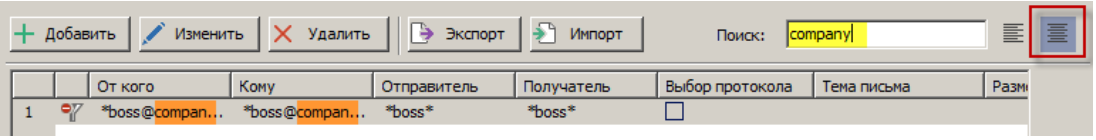


Рисунок 6.342

6.8.11 Одновременный перехват трафика и сбор сообщений с почтовых серверов

Если планируется совмещать перехват трафика и сбор сообщений с почтового сервера, существует возможность того, что одни и те же почтовые сообщения будут обработаны дважды – и службой перехвата, и службой интеграции.

Для того, чтобы сообщения, передаваемые внутренним почтовым сервером, обрабатывались только службой интеграции, произведите следующие операции: откройте узел «Фильтрация», перейдите на вкладку «Фильтры | Глобальные настройки», и настройте общий исключающий фильтр по IP- или MAC- адресу сервера NetworkController, как показано на Рисунок 6.343.

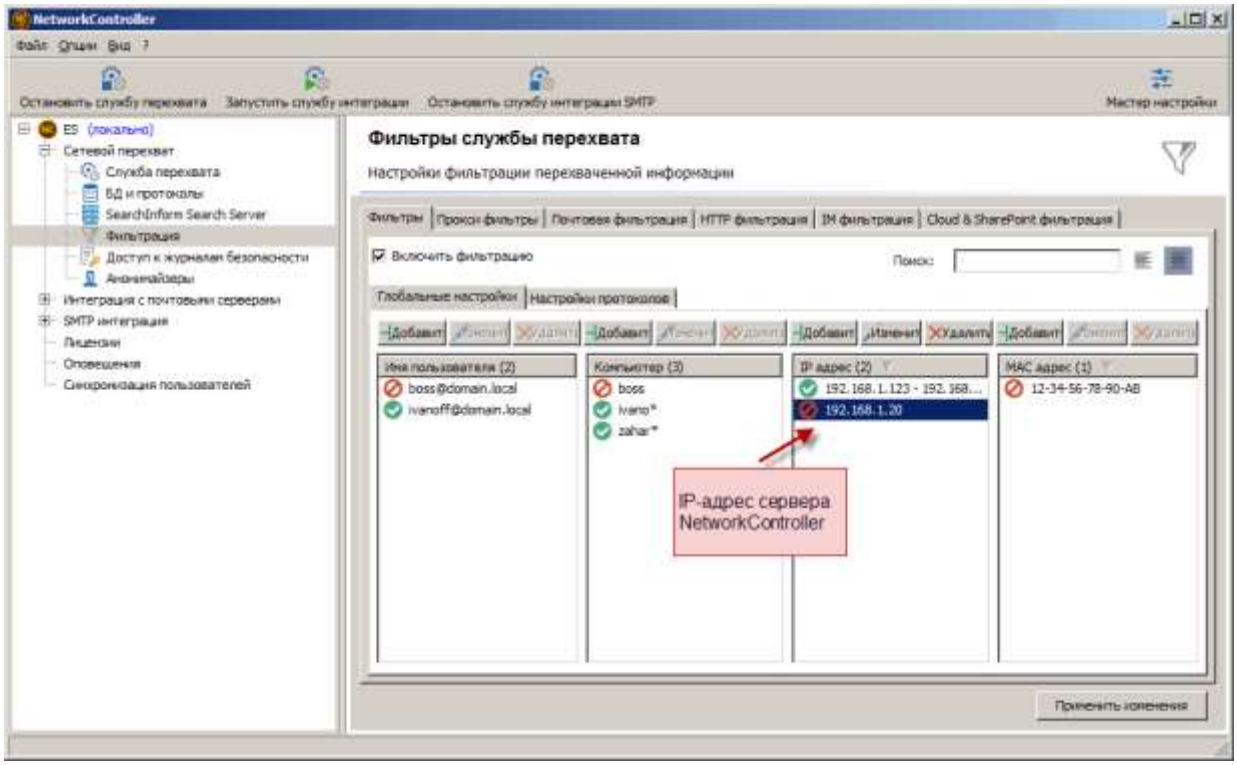


Рисунок 6.343

6.8.12 Настройка интеграции почтового сервера Lotus Domino с сервером NetworkController

Настройка сервера Lotus Domino производится с помощью пользовательского интерфейса IBM Lotus Domino Administrator.

1. На вкладке **People & Groups**(1) выберите директорию **People**(2). В правой части выберите операцию **Register...**(3).
2. При запросе введите пароль для доступа к *cert.id*, заданный при первоначальном конфигурировании сервера (см. Рисунок 6.344).

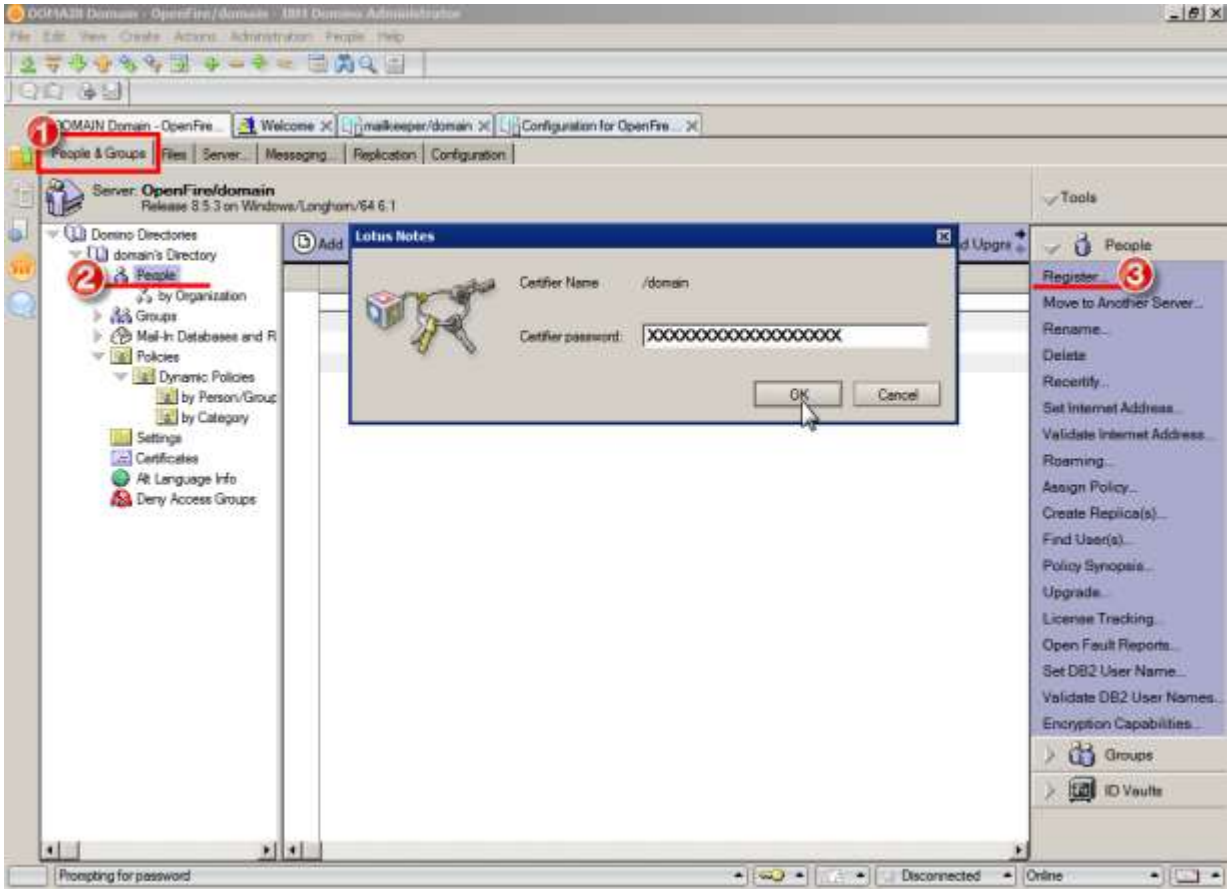


Рисунок 6.344

3. Создайте пользователя (см. Рисунок 6.345). Имя может содержать только латинские символы, исключая пробелы и спецсимволы. Введите имя нового пользователя в поле **Last name** и задайте пароль в поле **Password**.
   Щелкните кнопку **Register**(2), после чего нажмите **Done**(3).

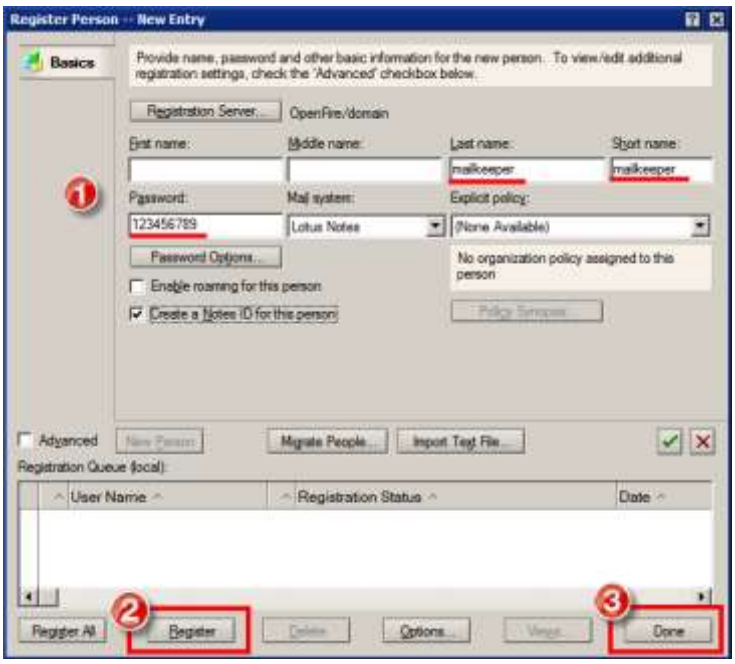


Рисунок 6.345

4. Выберите из списка созданного пользователя и нажмите **Edit Person** (см. Рисунок 6.346).

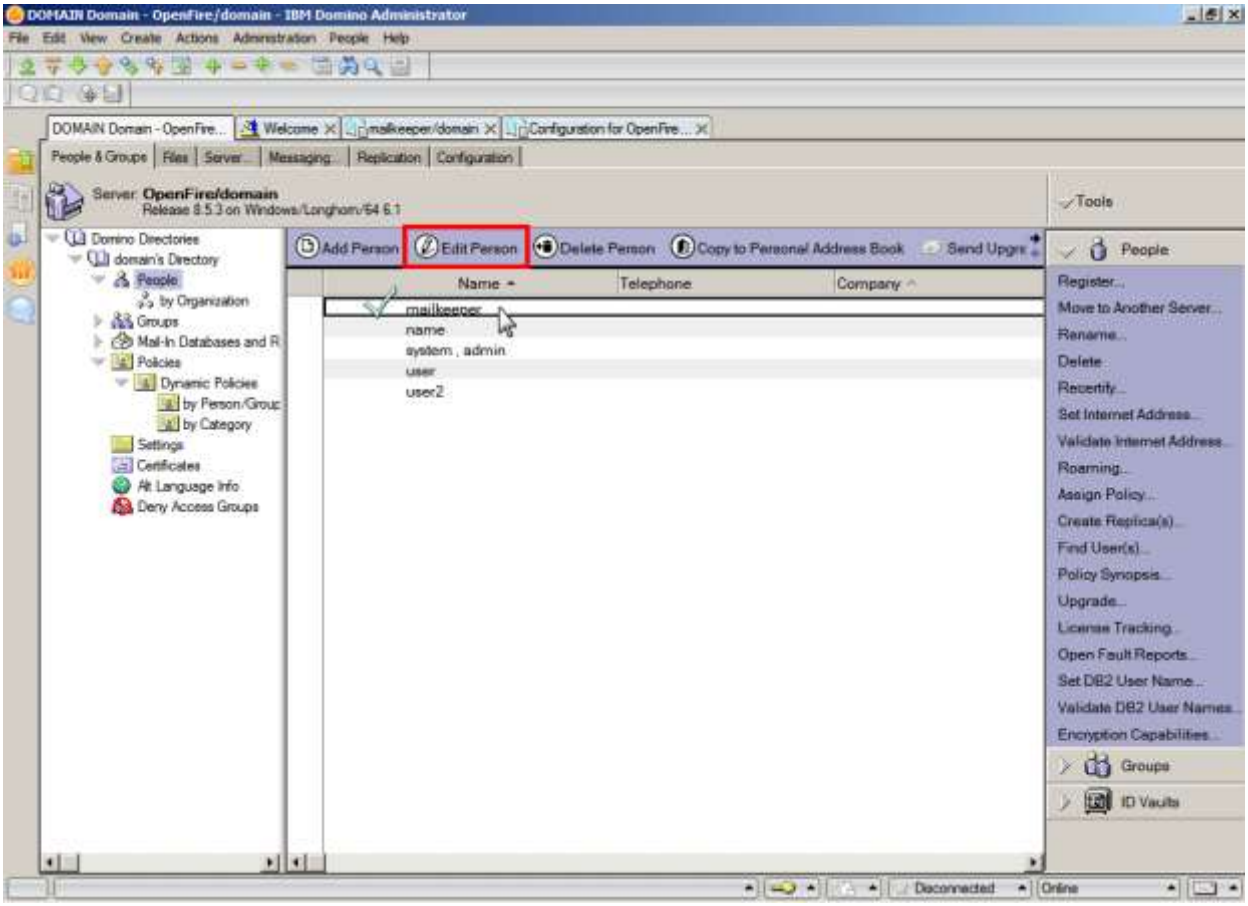


Рисунок 6.346

5. Укажите пароль (1) для доступа по POP3, протокол для загрузки писем (2) и интернет-адрес ящика (3) (см. Рисунок 6.347).

   Проверьте параметры и нажмите **Save & Close**(5).

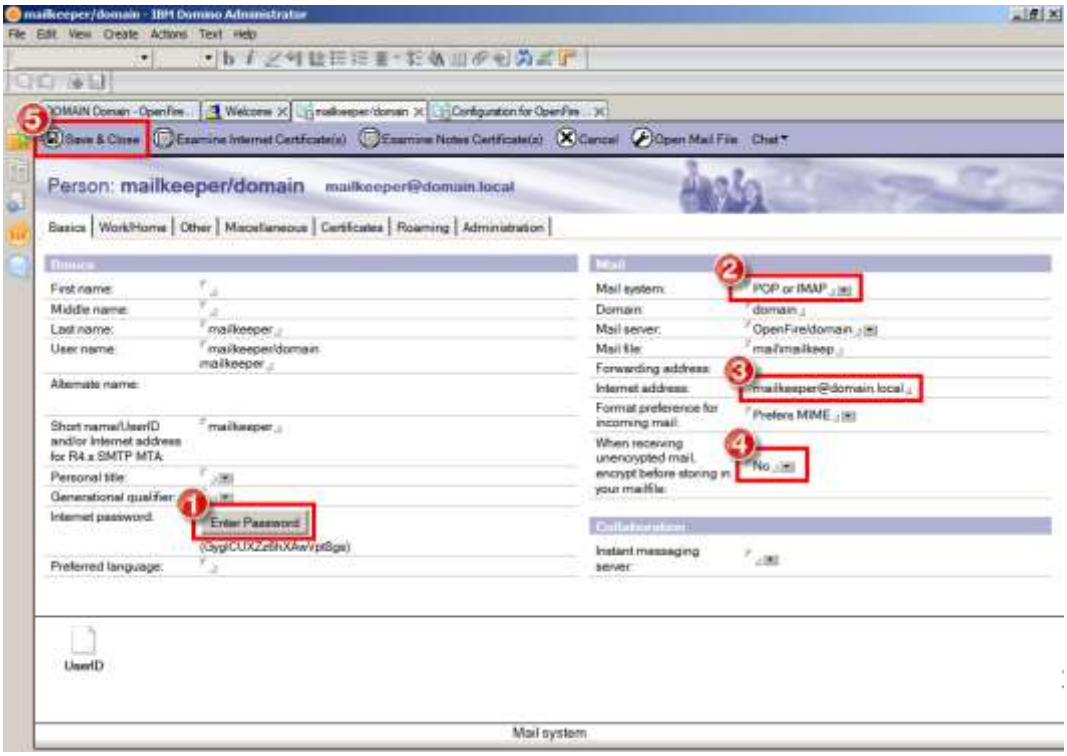


Рисунок 6.347

6. Проверьте, запущен ли сервер POP3 (см. Рисунок 6.348). Соответственно, должен быть включен протокол ***POP3*** сервера, известен ***порт*** (по умолчанию 110).

   Результат необходимо протестировать с помощью любого mail-клиента, например, TheBat! (ящик должен быть доступен для чтения клиентом).

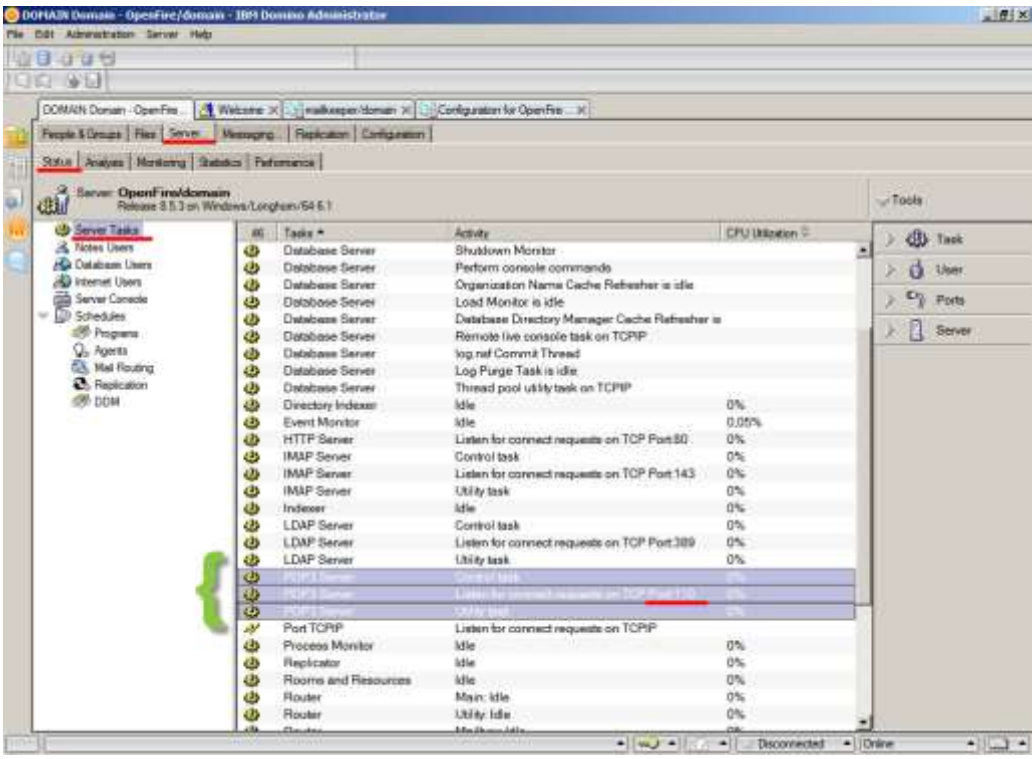


Рисунок 6.348

7. Настройте параметры журналирования для сохранения всех сообщений в базу пользователя ***mailkeeper*** (см. Рисунок 6.349).

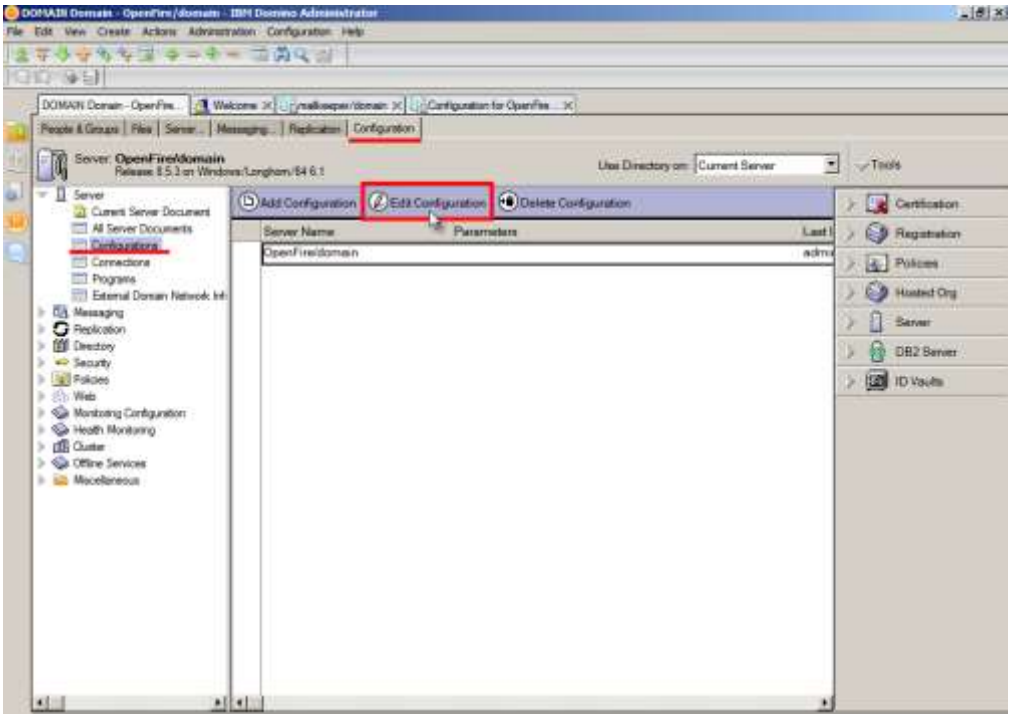


Рисунок 6.349

8. В качестве значения параметра **Field encryption exclusion list** внесите следующие данные: *Form; From; Principal; PostedDate; Body; Subject; SendTo;*

CopyTo; BlindCopyTo; InetSendTo; InetCopyTo; InetBlindCopyTo (см. Рисунок 6.350). Данные перечисленных полей будут сохраняться в базу данных.

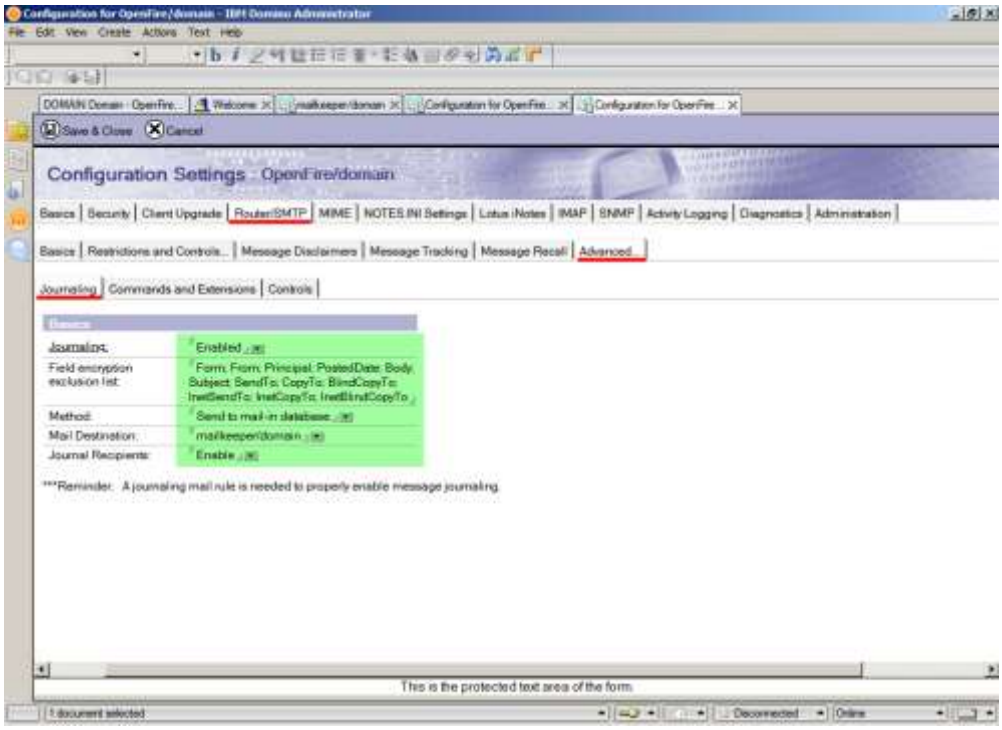


Рисунок 6.350

9. Настройте правило ***(Rule)*** для помещения всей почты в базу (см. Рисунок 6.351).

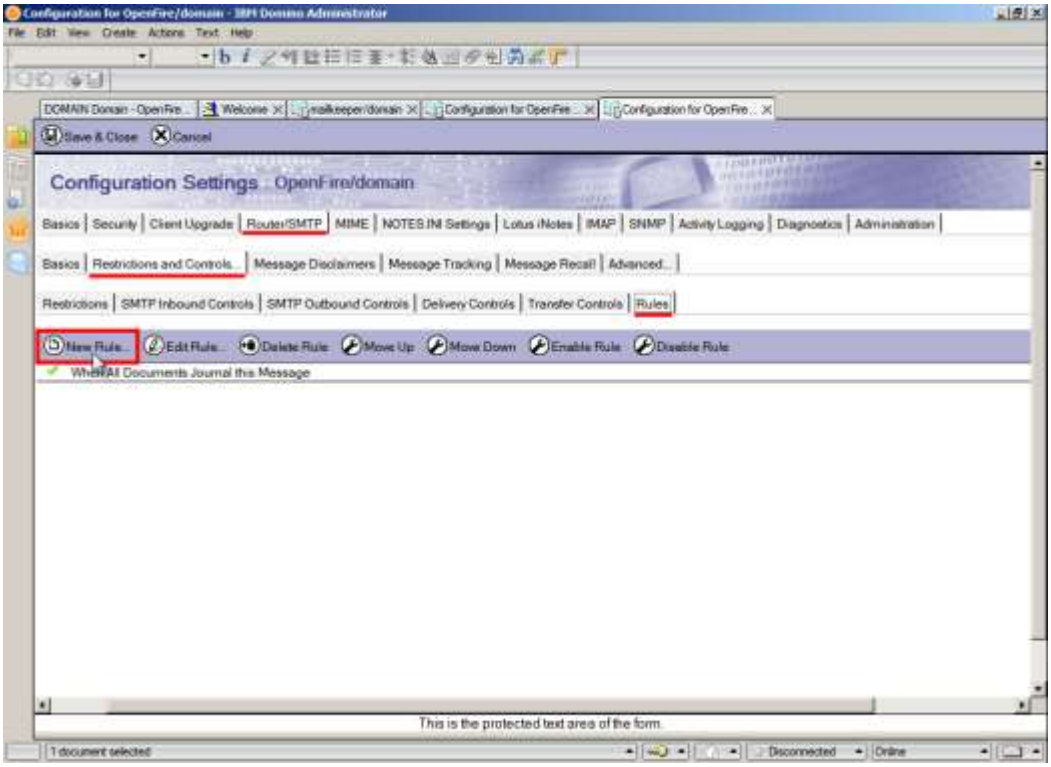


Рисунок 6.351

10. Проделайте операции, изображенные на Рисунок 6.352. Примените изменения, щелкнув «OK».

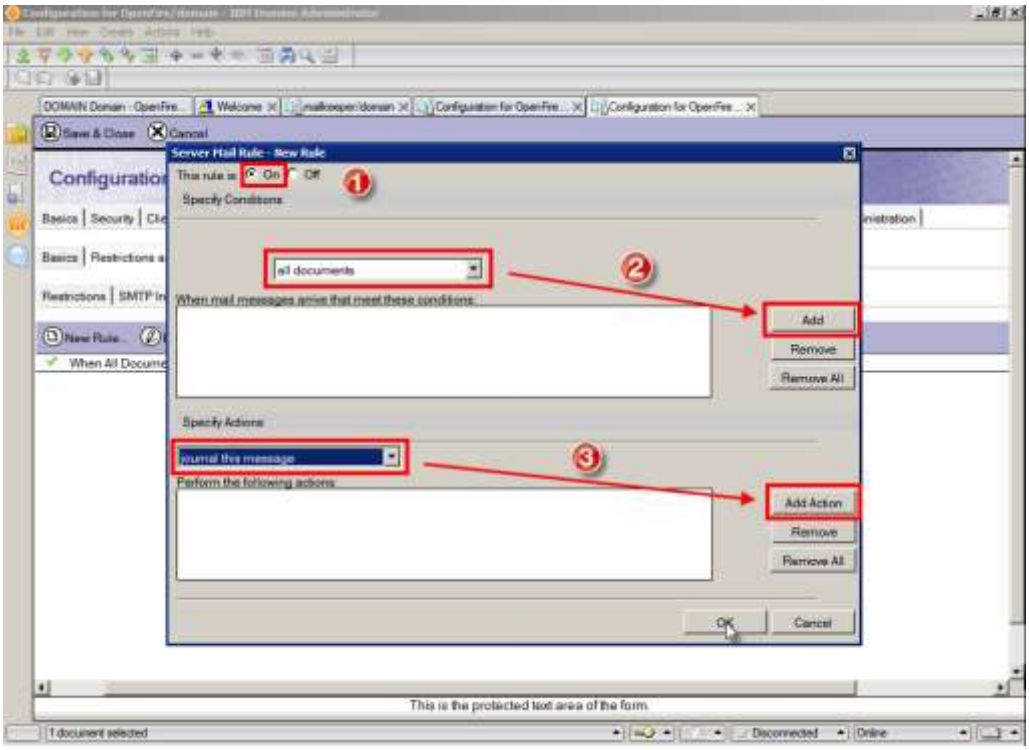


Рисунок 6.352

Настройка сервера NetworkController производится из консоли управления.

1. Настройте запуск от имени учётной записи с правами чтения из Active Directory и запуск служб. В большинстве случаев достаточно системной учётной записи.
2. Смените тип запуска на автоматический (см. Рисунок 6.353).

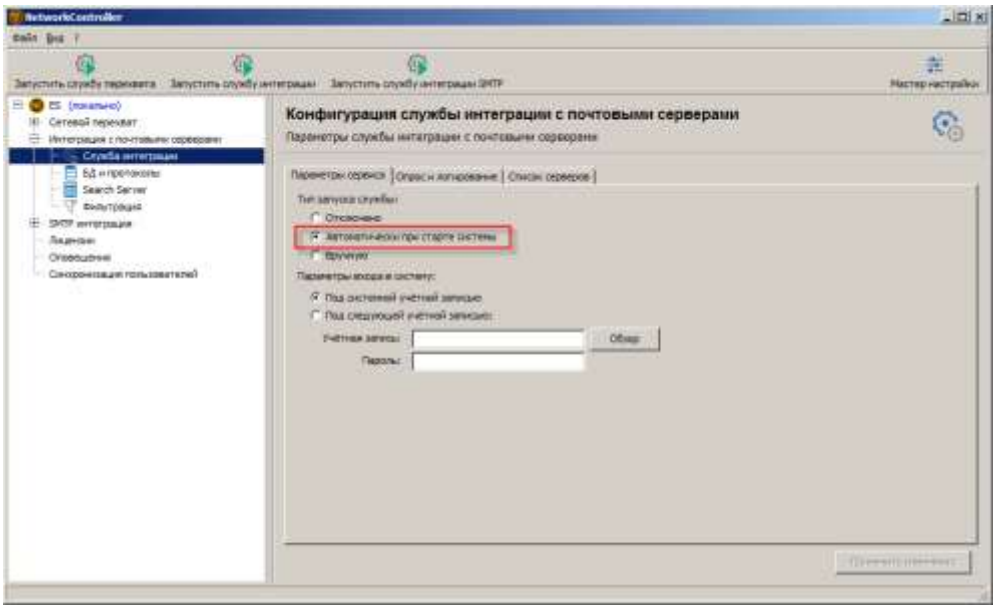


Рисунок 6.353

3. Создайте базу(ы) данных и индекс(ы).
4. Настройте NetworkController на сервер Lotus Domino: укажите *IP-адрес сервера*, *порт*, *вид авторизации*, *тип подключения*, а также *имя пользователя* и *пароль*, которые были заданы при создании пользователя в консоли IBM Lotus Domino Administrator.

   Уровень логирования при тестировании – *Подробный*.

   При включенной опции «Сохранять письма в файлы» вместе с логами в папку **EML** сохраняются перехваченные письма (см. Рисунок 6.354).

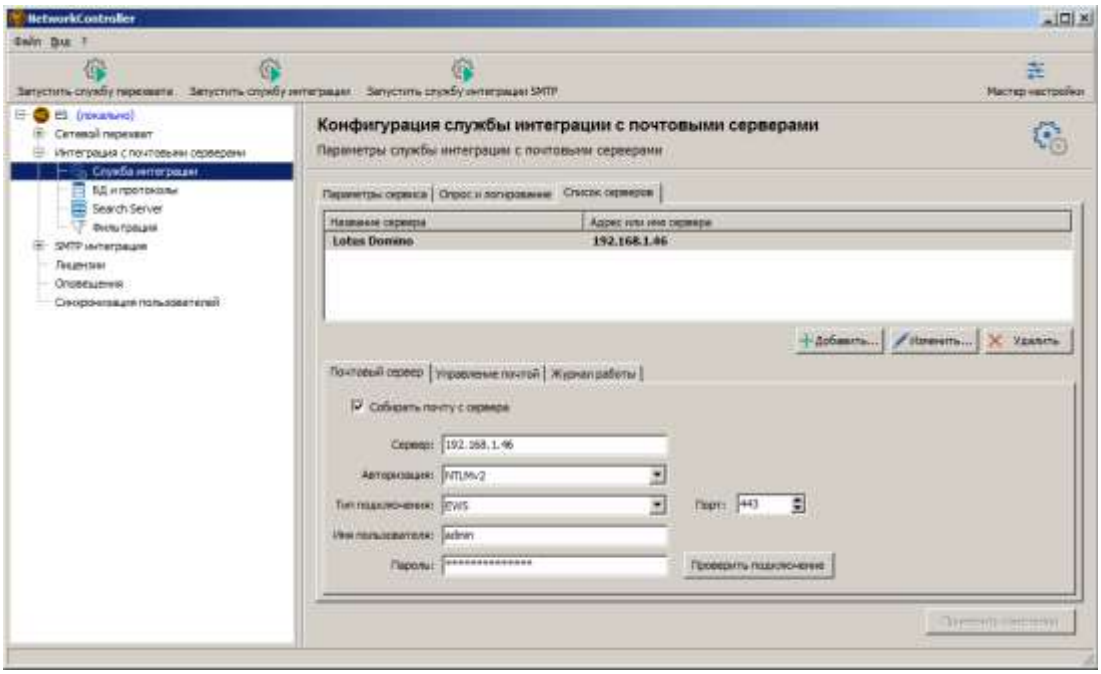


Рисунок 6.354

5. На вкладке **Управление почтой** выберите действие, которое будет производиться после получения почтовых сообщений из ящика ***mailkeeper***:
   - не удалять;
   - удалять после прочтения;
   - удалять после заданного периода (см. Рисунок 6.355).

Рисунок 6.355

Почтовый сервер в процессе своей работы ведет логирование действий с указанием даты/времени и количества полученных писем. Данная информация доступна на подвкладке «Журнал работы» (см. Рисунок 6.356).

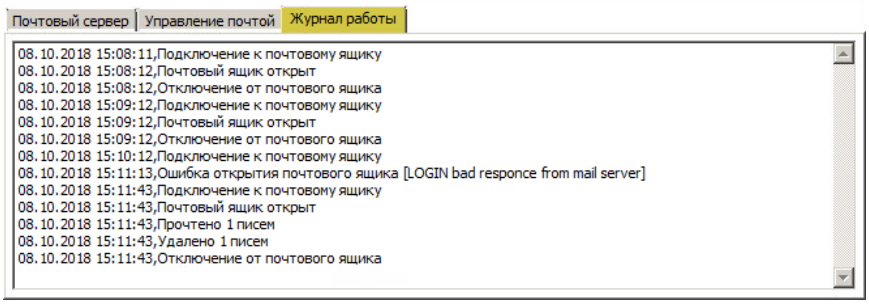


Рисунок 6.356

6. Настройте **Синхронизацию с Active Directory** и/или **Определение пользователей по маскам e-mail адресов** (см. п. 6.8.10.3 и 6.8.10.4).
   Настройка определения пользователей по e-mail адресам и/или их маскам **является обязательной**. В случае их отсутствия ни одно из писем не будет перехвачено!

Запустите Службу интеграции, проверьте работу, логирование, сохранение писем.

По умолчанию логи сохраняются в директории:

%allusersprofile%\SearchInform\SearchInform NetworkController\SearchInform Mail servers integration\.

6.9 Настройка аналитического модуля Серчинформ AlertCenter

Настройка AlertCenter предполагает последовательное выполнение следующих операций:

1. Подключение базы данных AlertCenter;
2. Запуск сервера AlertCenter;
3. Настройка списка индексов компонентов Серчинформ ДЛП;
4. Настройка отправки уведомлений по электронной почте.
5. Настройка экспорта данных в SIEM.

6.9.1 Подключение базы данных AlertCenter

Настройки сервера AlertCenter и журналы инцидентов хранятся в базе данных AlertCenter под управлением Microsoft SQL Server, к которой должны быть привязаны сервер и клиент AlertCenter.

На этапе установки сервера AlertCenter нужно создать базу данных. В консоли сервера AlertCenter на вкладке «База данных» будет отображена привязка к указанной базе данных (см. Рисунок 6.357).

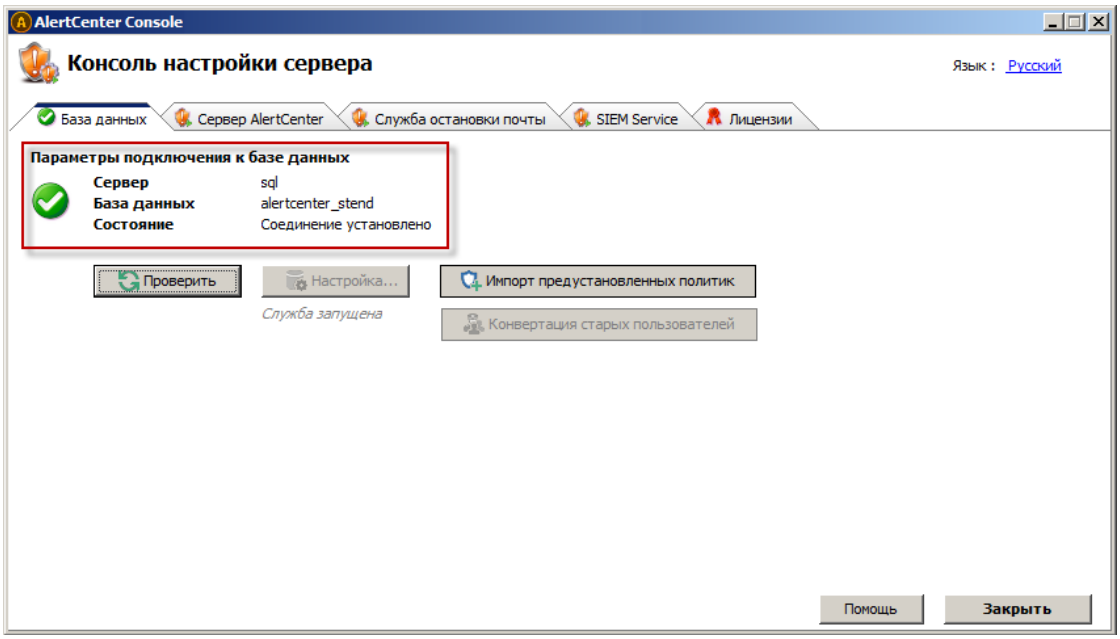


Рисунок 6.357

При необходимости изменения настроек подключения к базе данных, нажмите кнопку «Настройка» (кнопка активна только в случае, если **все службы** сервера AlertCenter ***остановлены.***

Остановка служб осуществляется на вкладках «Сервер Alert Center», «Служба остановки почты», «SIEM Service» (см. Рисунок 6.358).

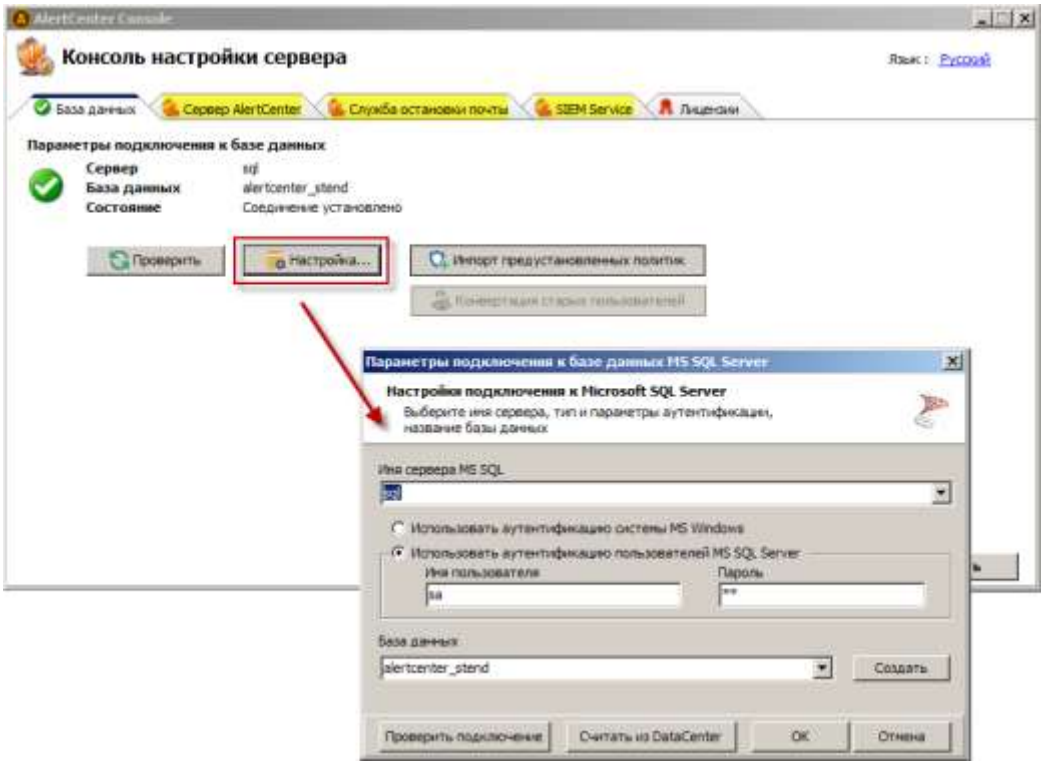


Рисунок 6.358

6.9.2 Запуск сервера AlertCenter

Далее запустите службу проверок AlertCenter на вкладке «Сервер AlertCenter», щелкнув кнопку «Запустить сервер» (см. Рисунок 6.359).

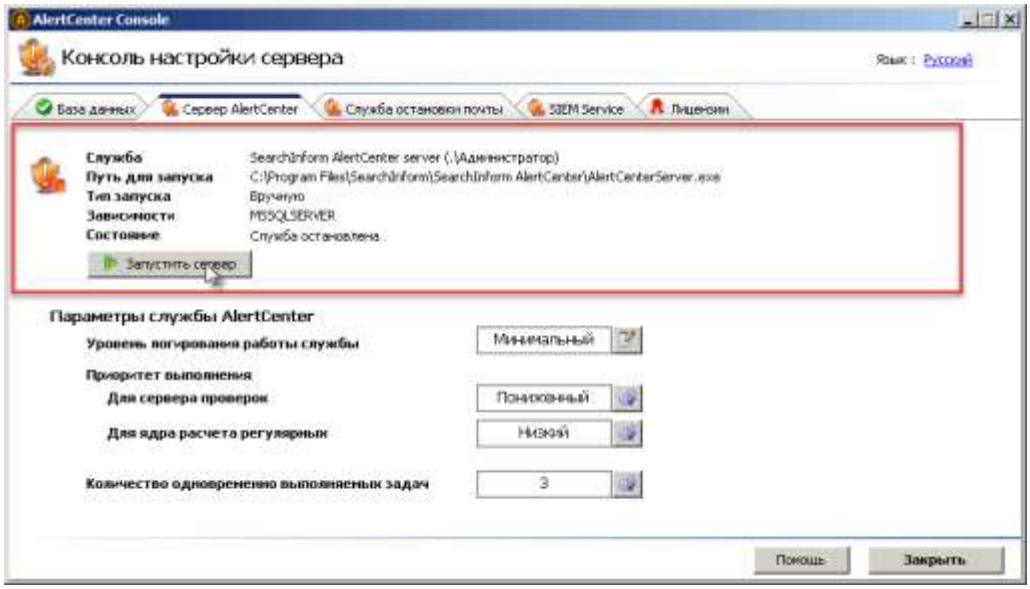


Рисунок 6.359

Настройте также параметры службы сервера AlertCenter: уровень логирования, приоритет выполнения задач, количество одновременно выполняемых задач.

6.9.3 Запуск службы остановки почты

Для использования службы остановки почты запустите сервер на вкладке «Служба остановки почты» и выберите уровень логирования работы службы: отключено, нормальный, отладочный, трассировочный (см. Рисунок 6.360).

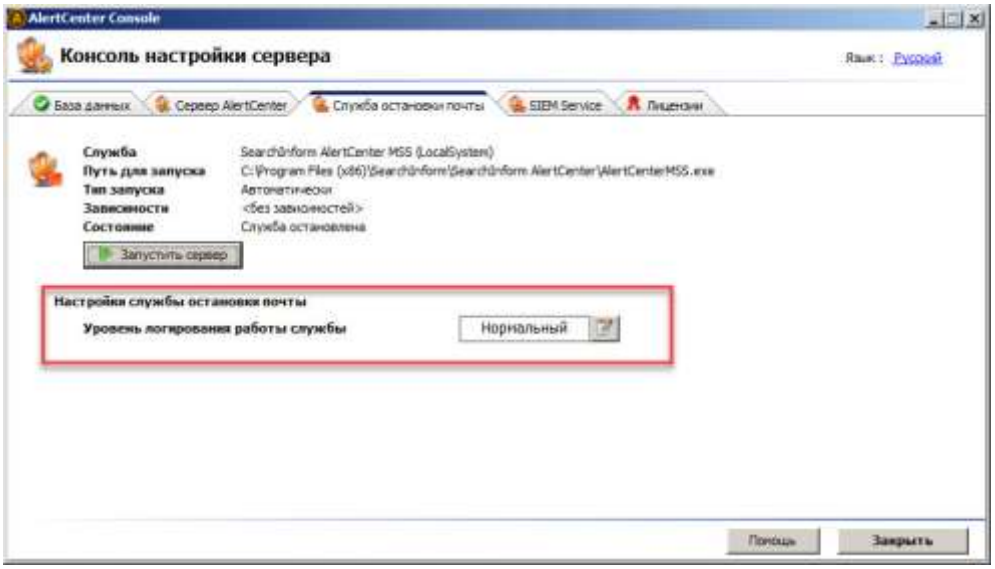


Рисунок 6.360

6.9.4 Настройка службы экспорта в SIEM

Служба AlertCenter SIEM позволяет экспортировать данные об инцидентах, а также сообщениях и изменениях (журнал событий в клиенте AlertCenter) в файл формата CEF или в SIEM-систему с помощью syslog.

Включение/выключение, а также настройка уровня логирования и приоритета службы выполняется в настройках серверной консоли AlertCenter (см. Рисунок 6.361).

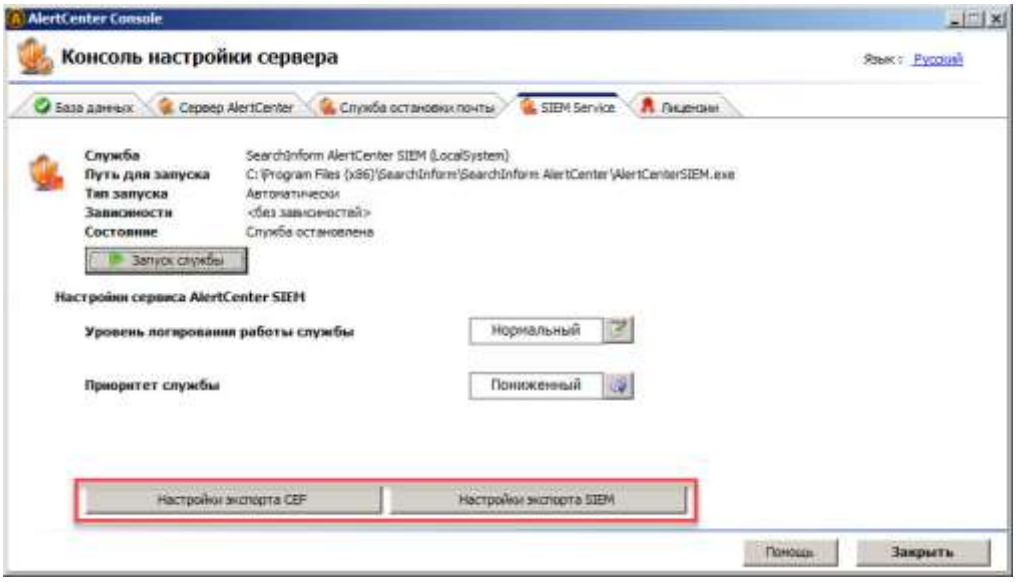


Рисунок 6.361

Переход к параметрам экспорта осуществляется посредством нажатия соответствующих кнопок:

- Настройки экспорта CEF;
- Настройки экспорта SIEM.

6.9.4.1 Настройки экспорта CEF

В окне настроек активируйте задачу экспорта, установив флажок в соответствующем чекбоксе (см. Рисунок 6.362). Задайте расписание частоты выполнения экспорта.

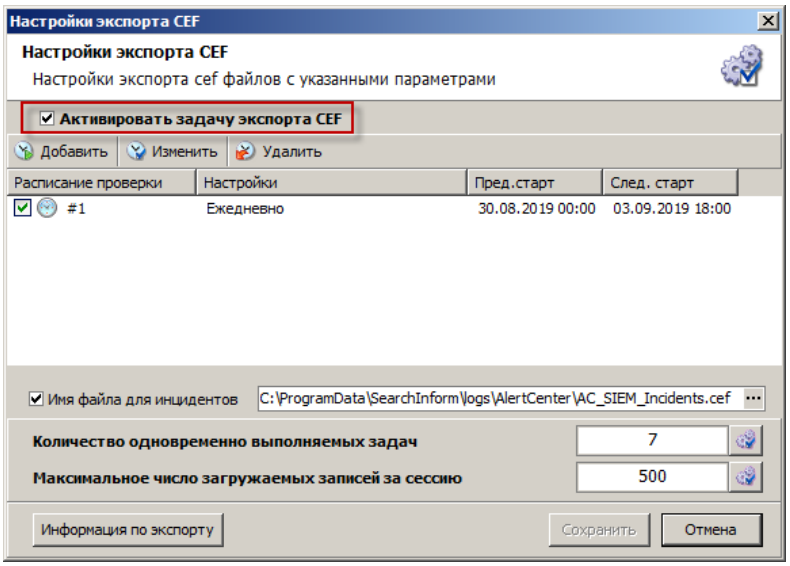


Рисунок 6.362

Отметьте флагом данные, которые необходимо экспортировать, и при необходимости измените путь к папке, в которую будет сохранен файл экспорта (см. Рисунок 6.363, Рисунок 6.364).

Рисунок 6.363

Рисунок 6.364

Для изменения параметров «Количество одновременно выполняемых задач» и «Максимальное число загружаемых записей за сессию» воспользуйтесь кнопкой «Изменить» (см. Рисунок 6.365).

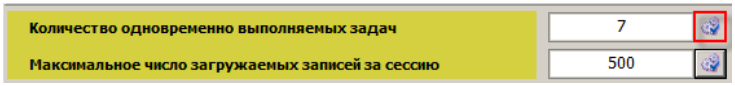


Рисунок 6.365

В открывшемся окне с помощью регулятора установите необходимое значение (см.Рисунок 6.366).

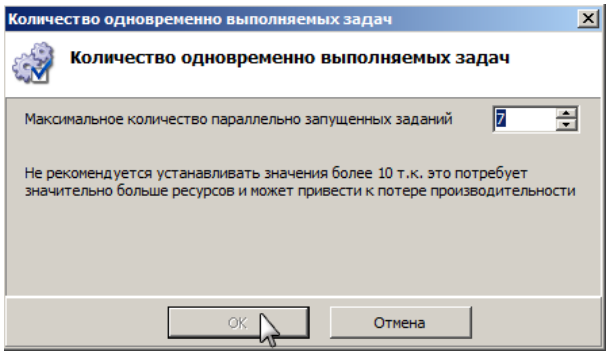


Рисунок 6.366

Для получения информации по экспортированным данным нажмите кнопку «Информация по экспорту». Откроется окно результатов (см. Рисунок 6.367).

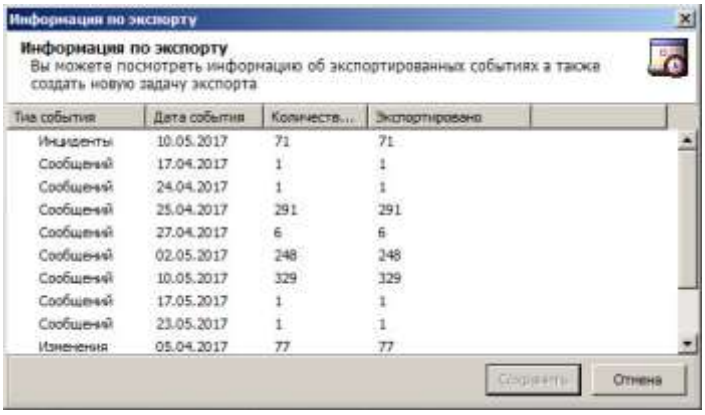


Рисунок 6.367

6.9.4.2 Настройки экспорта SIEM

В окне настроек активируйте задачу экспорта, установив флажок в соответствующем чекбоксе (см.Рисунок 6.368). Задайте расписание частоты выполнения экспорта.

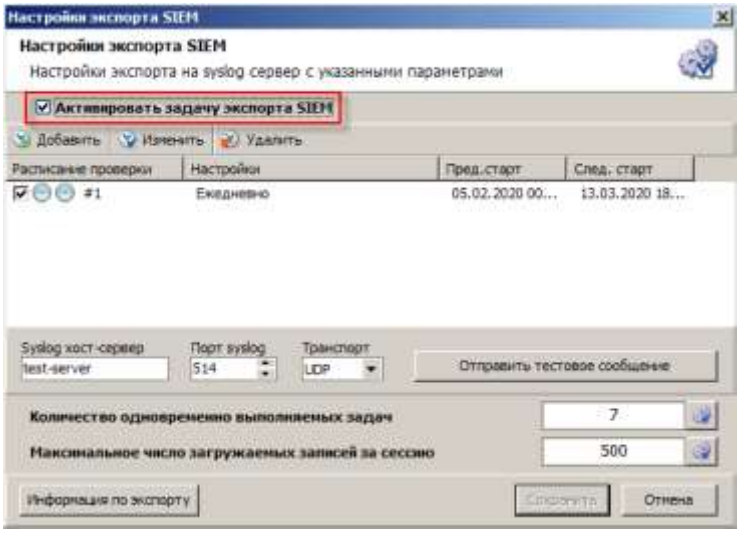


Рисунок 6.368

Укажите адрес syslog-сервера, порт, на который будет отправляться syslog, и транспортный протокол, с помощью которого осуществляется передача данных в систему SIEM. Для проверки доступа посредством отправки тестового сообщения нажмите одноименную кнопку.

Для изменения параметров «Количество одновременно выполняемых задач» и «Максимальное число загружаемых записей за сессию» воспользуйтесь кнопкой «Изменить» (см. Рисунок 6.369).

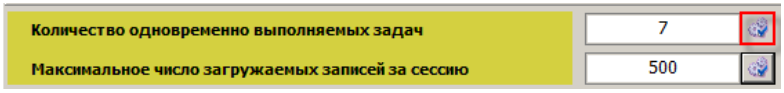


Рисунок 6.369

В открывшемся окне с помощью регулятора установите необходимое значение (см. Рисунок 6.370).

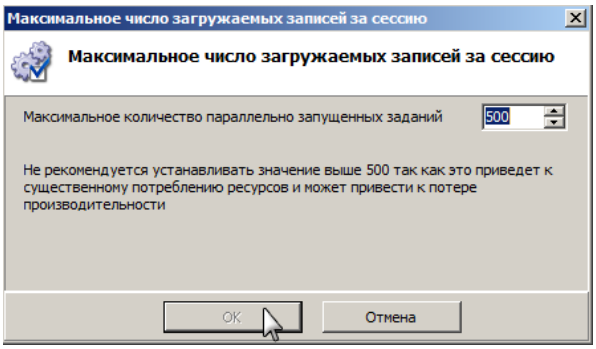


Рисунок 6.370

Для получения информации по экспортированным данным нажмите кнопку «Информация по экспорту». Откроется окно результатов (см. Рисунок 6.371).

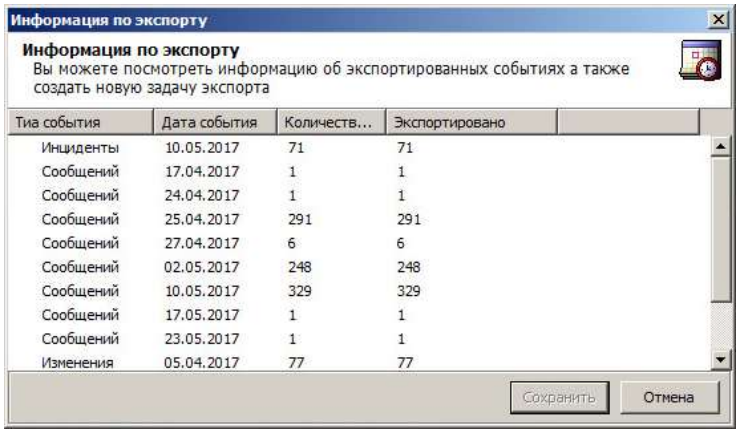


Рисунок 6.371

После этого серверную консоль AlertCenter можно закрыть. Дальнейшая настройка производится при помощи клиента AlertCenter.

6.9.5 Привязка клиента AlertCenter к базе данных

При первом вызове клиента AlertCenter может отображаться сообщение об отсутствии подключения к базе данных (см. Рисунок 6.372). Щелкните кнопку «Преобразовать».

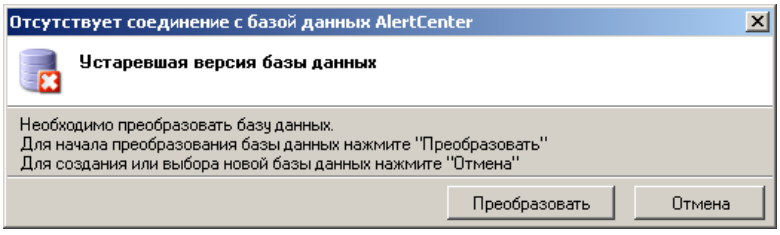


Рисунок 6.372

Введите имя сервера Microsoft SQL, настройте параметры доступа к серверу, выберите созданную базу данных и щелкните кнопку «ОК» (см. Рисунок 6.373).

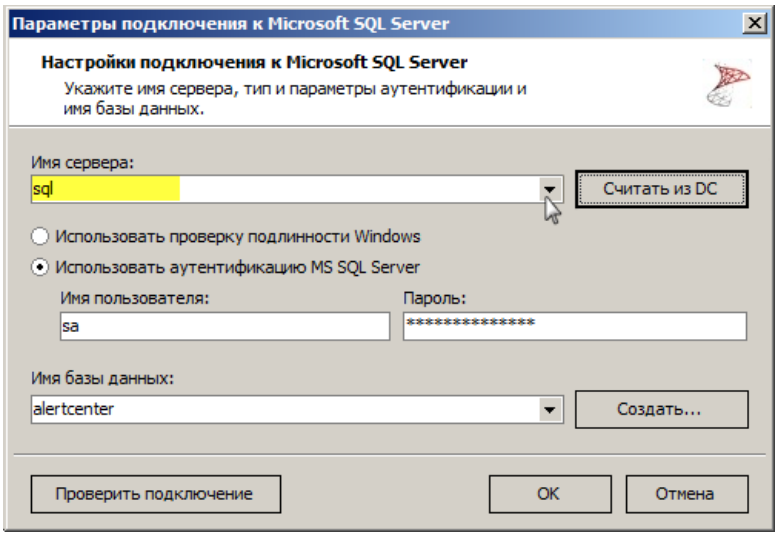


Рисунок 6.373

После удачного подключения к базе данных будет отображено окно клиента AlertCenter (см. Рисунок 6.374).

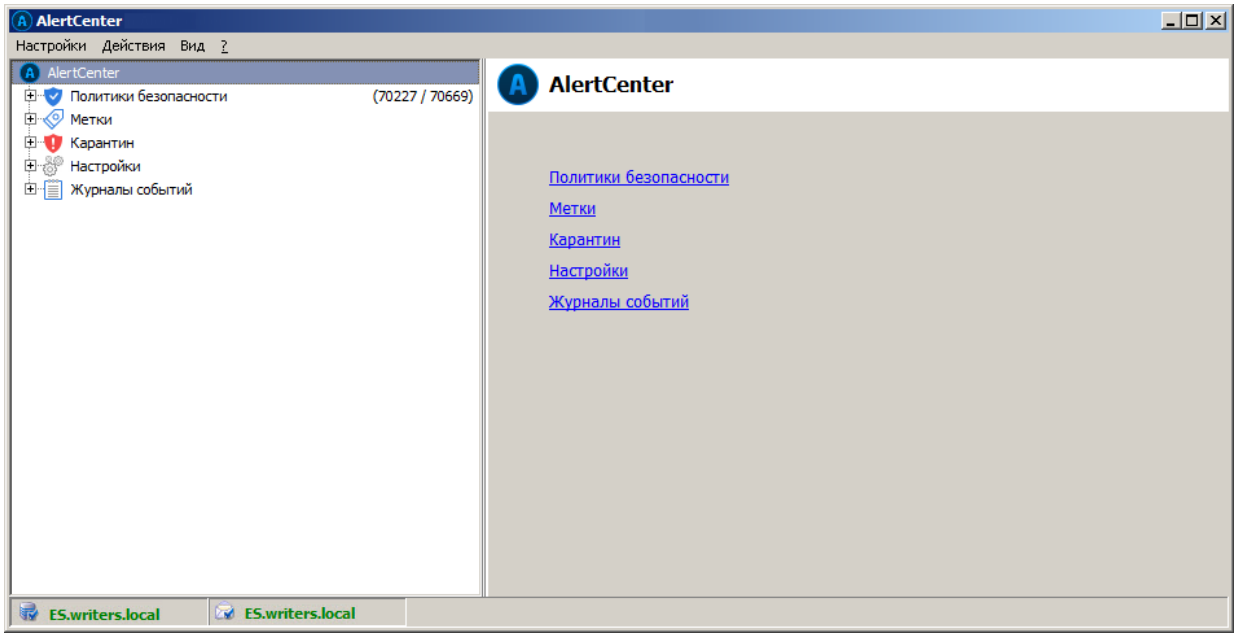


Рисунок 6.374

6.9.6 Настройка списка подключенных индексов

AlertCenter получает информацию об индексах и связях (сервера, продукты, цепочки), а также о базах данных из продукта DataCenter и кэширует ее в базе данных AlertCenter. Смонтированными считаются все индексы и базы данных, известные продукту DataCenter и имеющие статус доступных для поиска.

Для просмотра всех доступных для поиска индексов и баз данных выделите узел «Настройки» и перейдите на вкладку «Смонтированные индексы» (см. Рисунок 6.375).

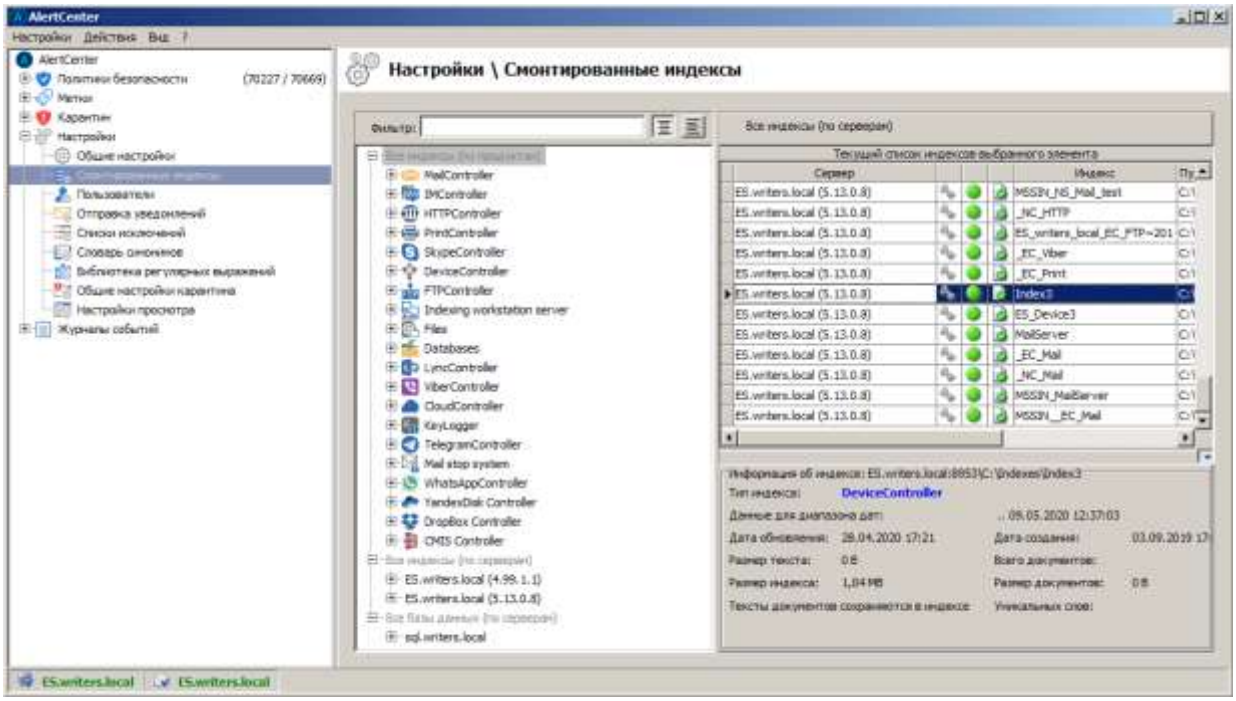


Рисунок 6.375

Смонтированные индексы могут быть сгруппированы по продуктам либо по серверам индексации Search Server.

- В группе «Все индексы (по продуктам)» содержатся цепочки и индексы сервера индексации Search Server, определенного продуктом DataCenter по умолчанию.
- Группа «Все индексы (по серверам)» содержит список серверов индексации Search Server. При раскрытии сервера, можно увидеть цепочки и список составляющих эти цепочки индексов, привязанных к данному серверу индексации.

Базы данных группируются по серверам индексации Search Server.

- В группе «Все базы данных (по серверам)» содержится список серверов индексации Search Server. При раскрытии сервера, можно увидеть список баз данных, привязанных к данному серверу индексации.

Если на сервере индексации Search Server выставлены дополнительные параметры авторизации, для доступа к индексу щелкните кнопку «Параметры авторизации» (либо выберите одноименную команду из контекстного меню), как показано на Рисунок 6.376.

Внимание: чтобы избежать ввода параметров авторизации каждый раз для доступа к отдельному индексу, достаточно один раз авторизоваться относительно самого сервера индексации. Для этого щелкните правой клавишей мыши по имени сервера и выберите из контекстного меню команду «Параметры доступа к серверу».

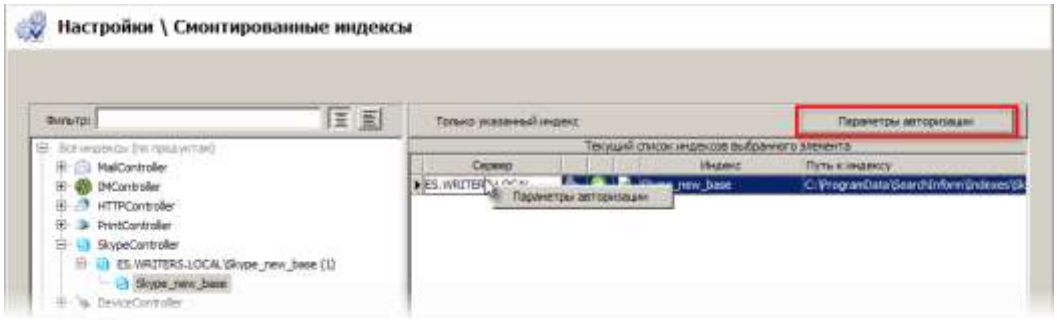


Рисунок 6.376

Введите имя пользователя, домен и пароль для подключения к серверу и щелкните «ОК» (см. Рисунок 6.377).

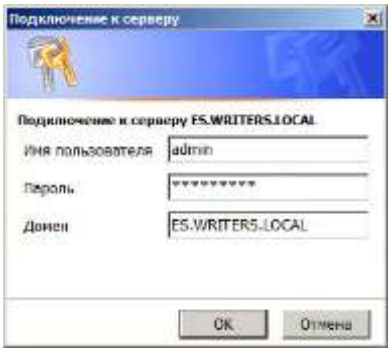


Рисунок 6.377

Индексы, подключенные с помощью дополнительных параметров авторизации, обозначаются в списке значком в виде желтого ключа (см. Рисунок 6.378).

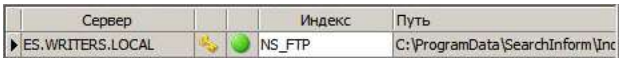


Рисунок 6.378

О статусе доступности индекса свидетельствует маркер, которым он обозначается в списке:

- индекс доступен для поиска;
- индекс не доступен для поиска;
- индекс активный, доступен для поиска.

Информация о сохранении текста документов в индексе отображается с помощью иконок:

- текст документов сохраняется в индексе;
- текст документов не сохраняется в индексе.

Ниже текущего списка индексов содержится краткая информация о выбранном индексе (дата создания, обновления индекса, его размер и т.д.) (см. Рисунок 6.379).

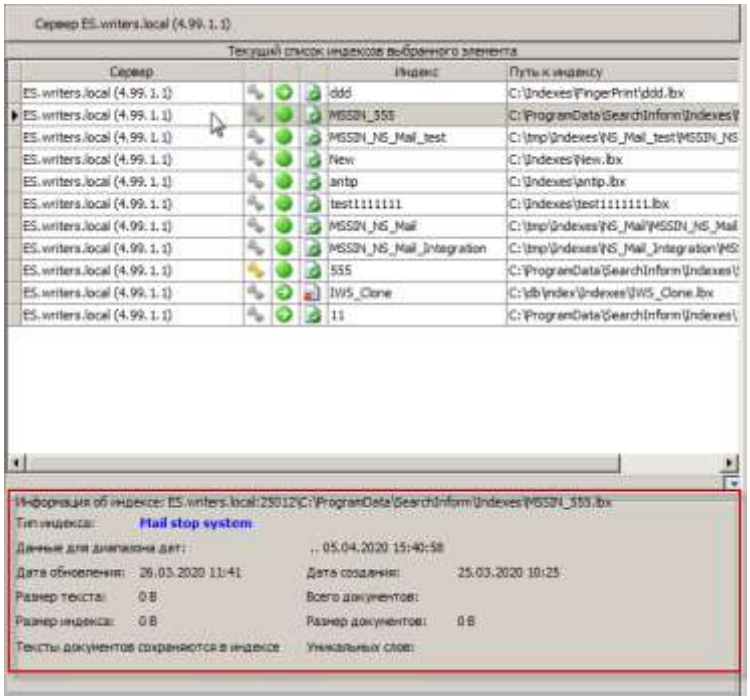


Рисунок 6.379

6.9.7 Настройка параметров отправки уведомлений по электронной почте

В случае срабатывания запроса на перехваченном документе AlertCenter может отправить сотруднику безопасности почтовое сообщение, содержащее ссылки на просмотр документа.

Для настройки параметров отправки уведомлений перейдите на вкладку «Отправка уведомлений» узла «Настройки.

Укажите настройки SMTP-сервера:

- Адрес сервера;
- SMTP-порт;
- Использовать TLS соединение - выберите один из предложенных вариантов: NoSSL, StartTLS, TLS;
- Имя пользователя;
- Пароль;
- Адрес отправителя.

Для установки дополнительных настроек щелкните кнопку «Настройка уведомлений» » (см. Рисунок 6.380).

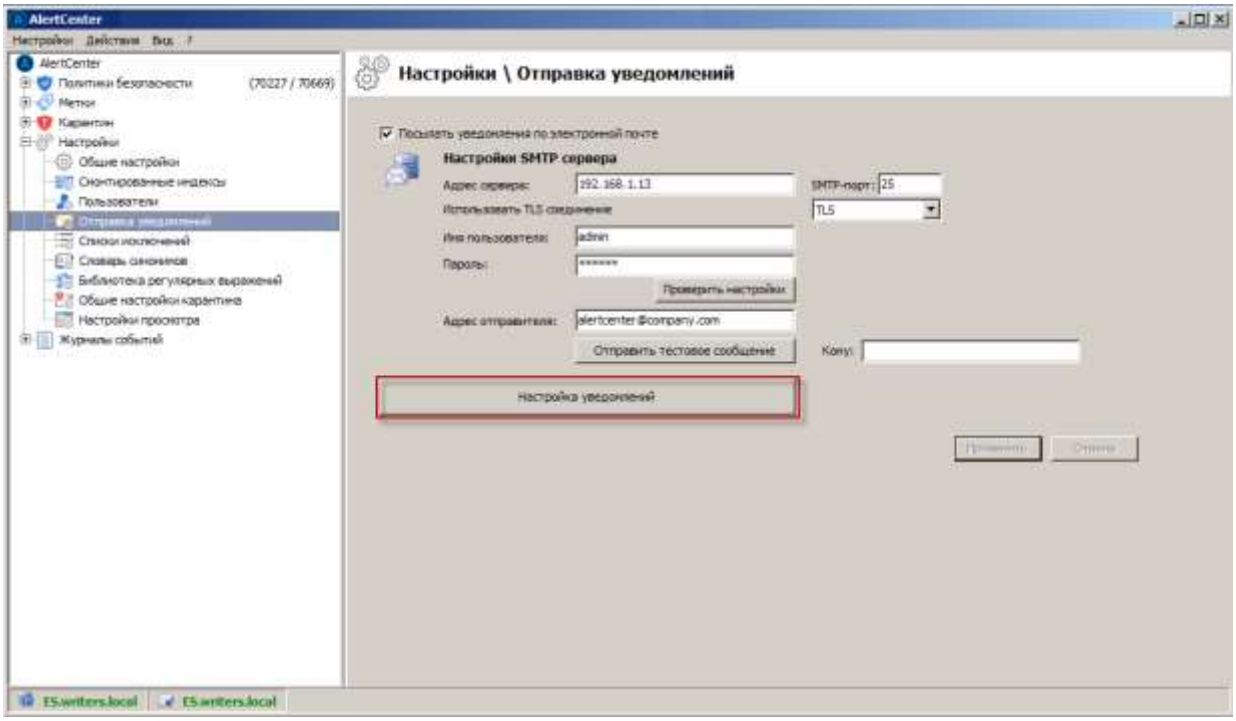


Рисунок 6.380

В открывшемся окне активируйте опцию «Посылать уведомления по электронной почте» и задайте параметры по умолчанию, которые будут применены ко всем политикам:

- **Тема письма.**
- **Язык уведомлений**: русский, английский, испанский.
- **Объединять уведомления в письма:** в одном сообщении будут объединены уведомления по всем зафиксированным инцидентам. Максимальный размер сообщения, а также количество инцидентов (вложенных документов) настраивается. По достижении указанных значений уведомления будут объединены по тому из параметров, максимальное значение которого было достигнуто первым.
- **Включать документ в письмо:** для включаемых в уведомление документов можно настроить максимальный размер в Кбайтах.
- **Уведомления в виде таблицы.**
- Выберите **поля,** информация которых будет отображаться в почтовом уведомлении. Для этого в строке параметра «Отображаемая информация» щёлкните по иконке  (см. Рисунок 6.381)**.**

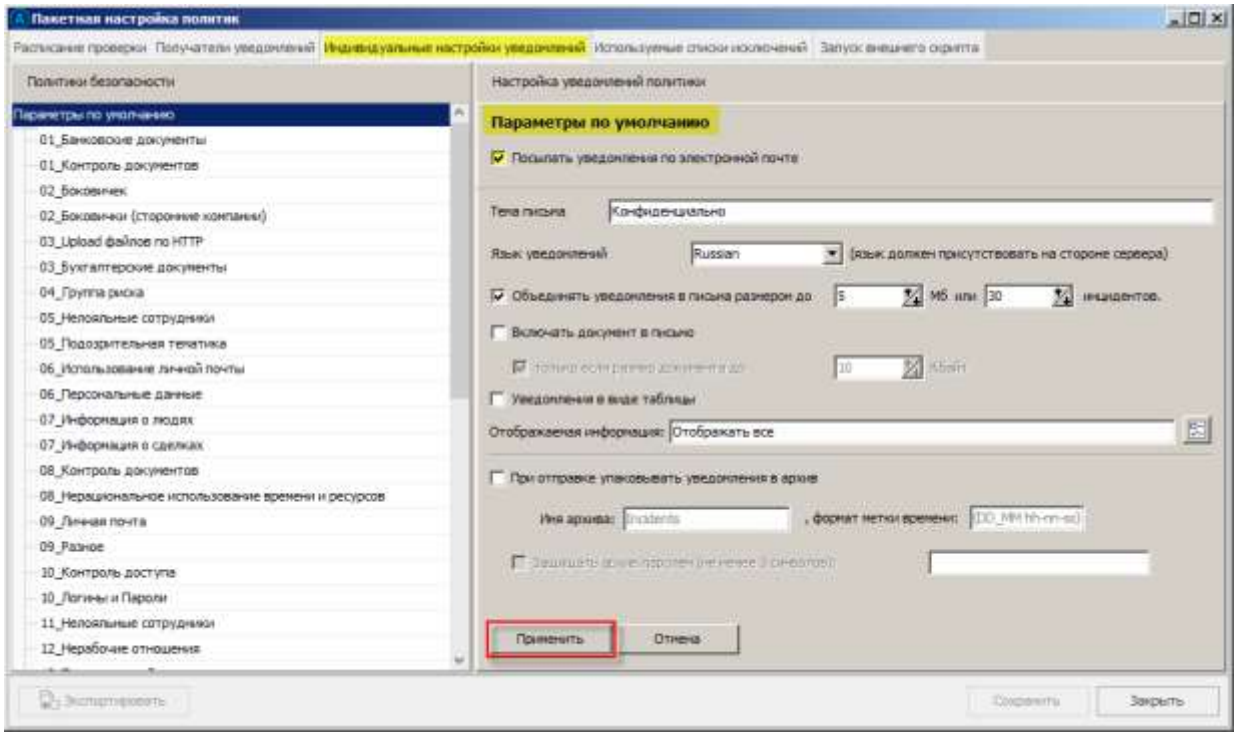


Рисунок 6.381

Настройте параметры защиты уведомлений:

- При отправке упаковывать уведомления в архив.
- Имя архива и формат метки времени.
- Защищать архив паролем.

Также можно задать индивидуальные настройки уведомлений для политик безопасности, позволяющие переопределить установленные по умолчанию настройки. Для этого выберие из списка слева политику, укажите индивидуальную тема письма и требуемые параметры отправки уведомлений.

Сохраните заданные настройки отправки уведомлений, щелкнув кнопку «Применить».

7 ОБНОВЛЕНИЕ ВЕРСИЙ КОМПОНЕНТОВ СЕРЧИНФОРМ ДЛП

Обновление версий компонентов Серчинформ ДЛП производится путем установки поверх существующей версии обновляемого продукта. Удаление старой версии не требуется.

Перед установкой новой версии остановите службу сервера обновляемого компонента, закройте консоль администрирования и клиентскую консоль. Если на сервере установлены и другие компоненты Серчинформ ДЛП, остановите все их службы и закройте все их окна!

При установке новой версии будут по умолчанию выбраны те же компоненты, что и при установке предыдущей версии ПО, и будут сохранены все существующие настройки, индексы и лицензия. Не изменяйте реестр операционной системы!

Дополнительную настройку сервера производить не требуется.

8 ПРОВЕРКА ПЕРЕХВАТА

Для проверки перехвата рекомендуется использовать предварительно подготовленный комплект документов в распространенных файловых форматах (.doc, .xls, .txt, .pdf и др.). Базовый комплект тестовых файлов может быть предоставлен компанией-разработчиком системы.

В качестве примера рассматривается перехват почтовых сообщений с вложенными файлами из комплекта контрольных документов.

Минимальный набор тестов для определения работоспособности должен подтвердить, что:

- сетевой трафик зеркалируется и/или перехватывается агентами;
- тестовые сообщения обрабатываются, размещаются в базы данных (хранилище) и индексируются;
- по сообщениям производится поиск;
- все атрибуты документов перехвачены и присвоены корректно (в частности, доменные имена отправителей и/или получателей).

8.1 Проверка работы перехвата методом зеркалирования трафика

Запустите Службу перехвата NetworkController. Если производится проверка работы с почтовыми серверами, запустите Службу интеграции (см. Рисунок 8.1).

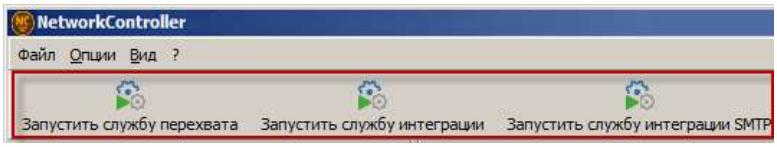


Рисунок 8.1

Выделите объект «Search Server» (в группе «Сетевой перехват» или «Интеграция с почтовыми серверами»). Убедитесь, что сервер индексации Search Server запущен (см. Рисунок 8.2).

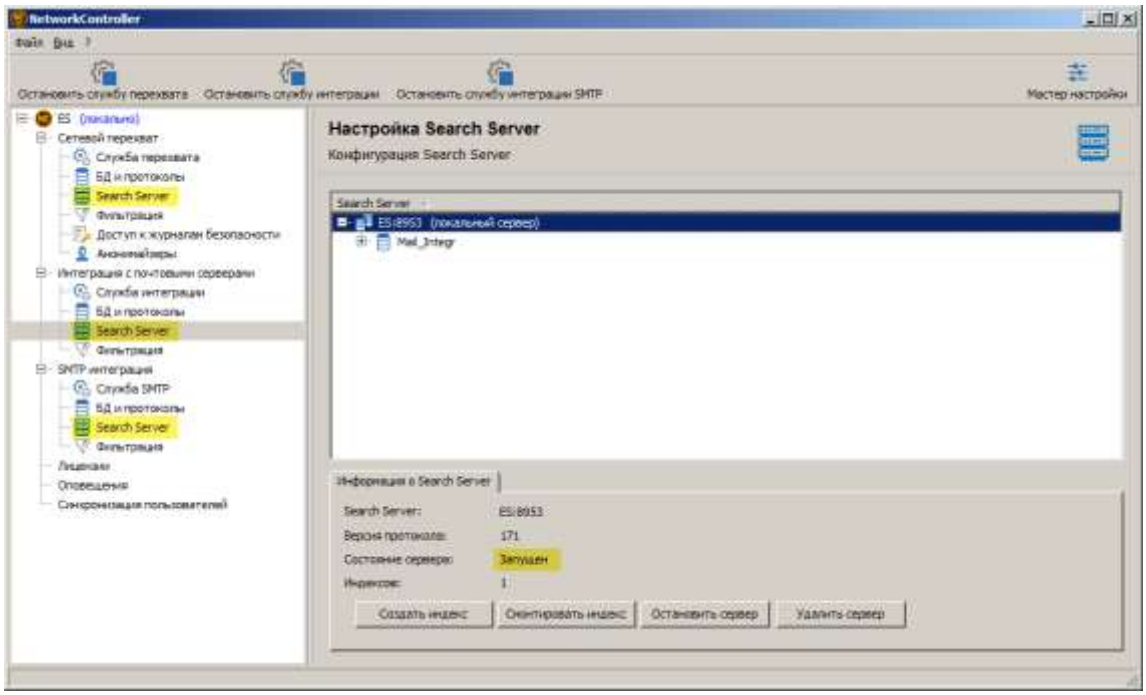


Рисунок 8.2

8.1.1 Проверка функций перехвата и индексации

В общем случае проверка функций перехвата и индексации сообщений производится в три этапа:

- передача информации;
- индексирование документов;
- проверка свойств индекса.

8.1.1.1 Передача информации

Под передачей информации в рамках текущего теста понимается:

- передача почтовых сообщений с вложенными файлами для проверки перехвата почты;
- отправка и получение сообщений ICQ для проверки перехвата сервисов мгновенных сообщений;
- отправка документов на файлообменный сервис rapidshare.com для проверки перехвата HTTP;
- отправка и загрузка файлов по FTP-соединению для проверки перехвата FTP;
- отправка и загрузка файлов из облачных хранилищ данных.

8.1.1.2 Передача почтовых сообщений

Отправьте несколько сообщений с произвольным текстом. Текст сообщений должен включать в себя легко распознаваемые слова (например, «инсайдер»).

Отправьте несколько тестовых сообщений с вложенными файлами из комплекта тестовых документов.

8.1.1.3 Передача ICQ-сообщений

Отправьте несколько тестовых сообщений, также содержащих легко распознаваемые слова.

Скопируйте текст одного из контрольных документов в буфер и отправьте в качестве сообщений. Повторите операцию для нескольких контрольных документов.

Также можно отправить несколько тестовых документов как файлы.

8.1.1.4 Передача файлов на сервис rapidshare.com

Загрузите несколько тестовых документов на файлообменный сервис rapidshare.com.

После этого удалите файлы с сервера.

8.1.1.5 Передача и загрузка файлов с помощью FTP-соединения

Загрузите несколько файлов на сервер FTP.

После этого скачайте данные файлы с FTP-сервера.

8.1.1.6 Передача и загрузка файлов из облачных хранилищ данных

Загрузите несколько тестовых документов на облачный сервис Яндекс Диск.

После этого скачайте файлы из облачного хранилища данных.

8.1.2 Индексирование документов и проверка свойств индекса

Обновите созданные индексы вручную и проверьте их свойства. Число документов должно совпасть с расчетным.

- Для почтовых сообщений число документов рассчитывается по формуле «число сообщений + число вложенных файлов».
- Для информации, переданной при помощи ICQ, число документов рассчитывается по формуле «число переписок + число файлов».
- Для файлов, переданных при помощи POST-форм, число документов рассчитывается по формуле «число сообщений + число файлов». Применительно к передаче файлов на сервер rapidshare.com – совпадет с числом переданных документов.
- Для переданных по FTP-протоколу файлов расчет документов производится по количеству принятых и переданных файлов.
- Для файлов, загруженных в облачные хранилища данных и скачанных из них, расчет документов производится по количеству принятых и переданных файлов.

Если сообщение отправлено от одного внутреннего пользователя другому, оно будет перехвачено дважды (исходящее и входящее). При использовании функционала почтовой и SMTP-интеграции для исключения дублирования одного и того же письма отметьте параметр «Сохранять один экземпляр внутреннего письма» (см. Рисунок 8.3). В базу будет сохранен один экземпляр отправленного письма – исходящий.

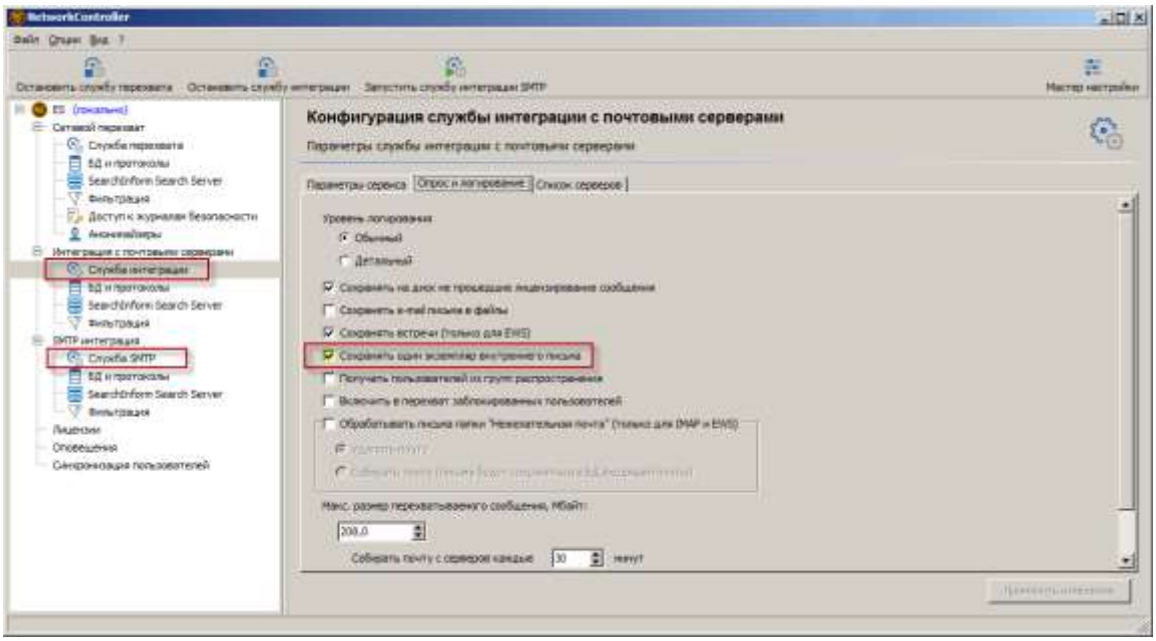


Рисунок 8.3

Чтобы начать обновление индекса, выделите его в списке и щелкните кнопку «Начать обновление» на вкладке «Свойства индекса» (см. Рисунок 8.4).

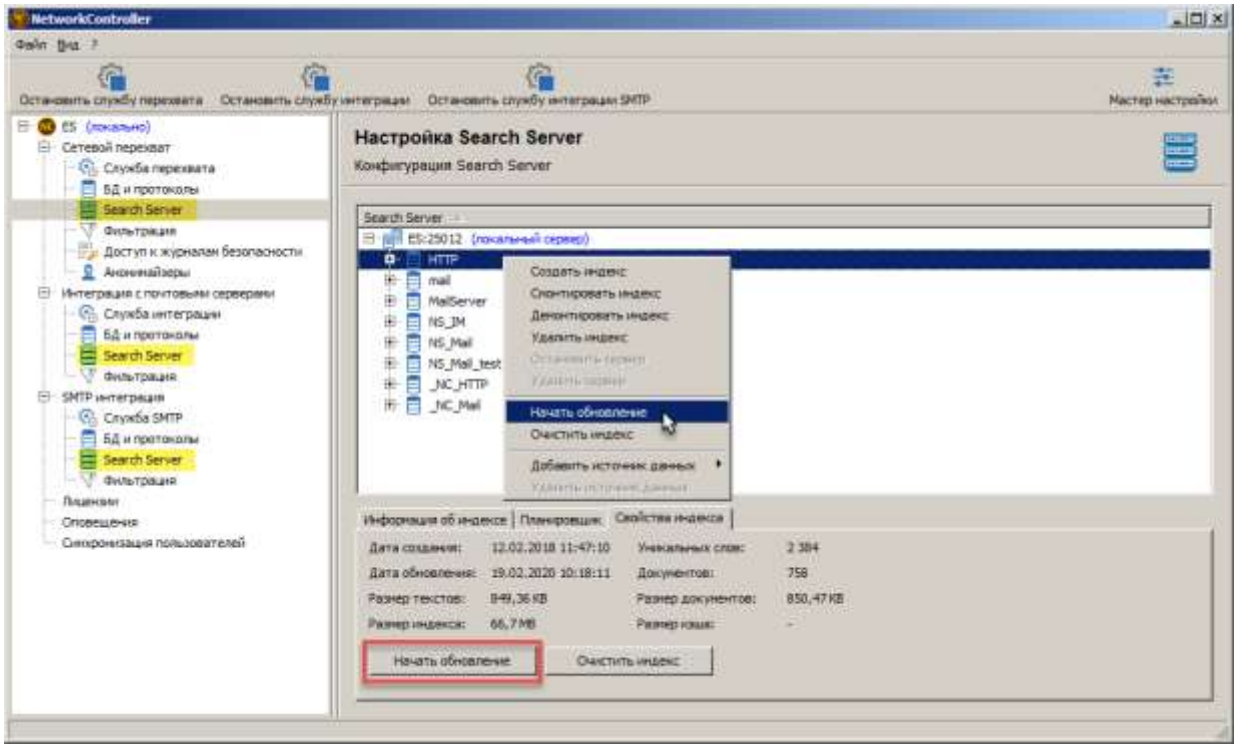


Рисунок 8.4

Откройте клиентское приложение AnalyticConsole, установленное на рабочее место аудитора безопасности, и на вкладке «Поиск» выберите источник данных «Почта».

Выполните запрос на отображение истории всех сообщений (см. Рисунок 8.5).

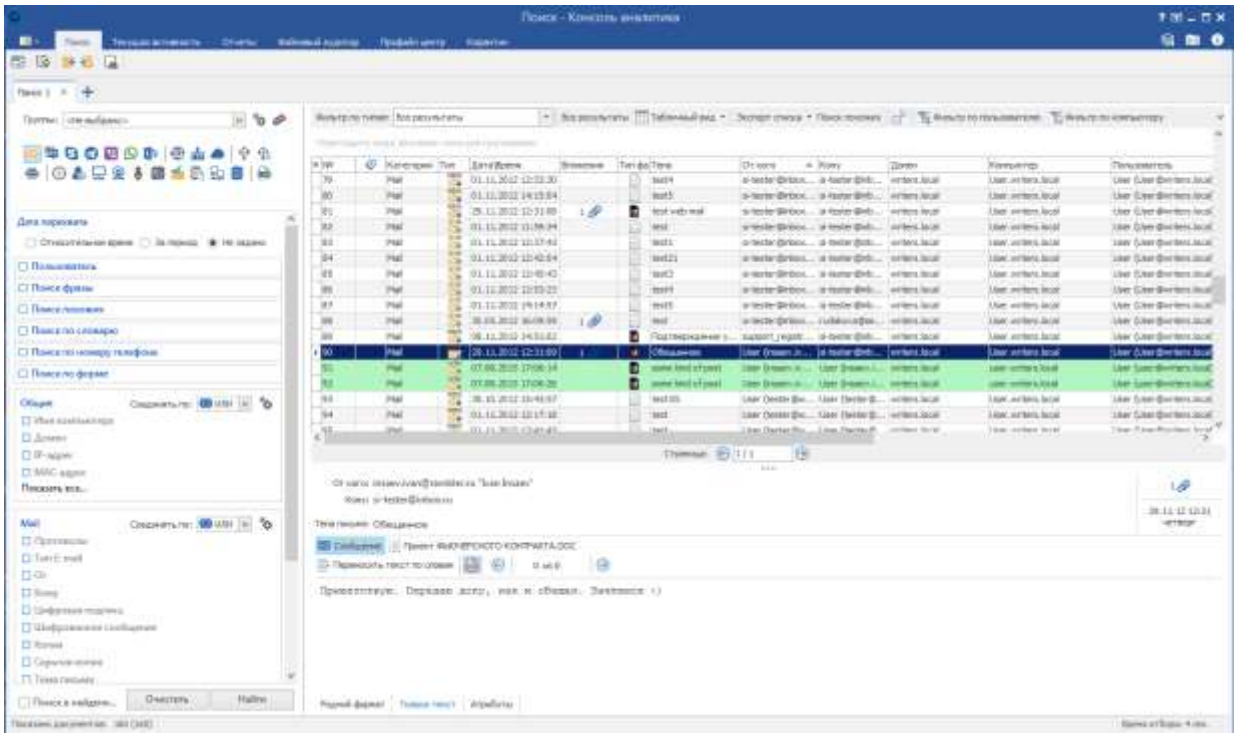


Рисунок 8.5

8.1.3 Проверка поиска по тексту документов

Скопируйте в буфер обмена текст одного из отправленных тестовых файлов, перейдите на вкладку поиска похожих, вставьте текст и произведите поиск. В данном примере обнаружено сообщение, отправленное по протоколу POP3 (см. Рисунок 8.6).

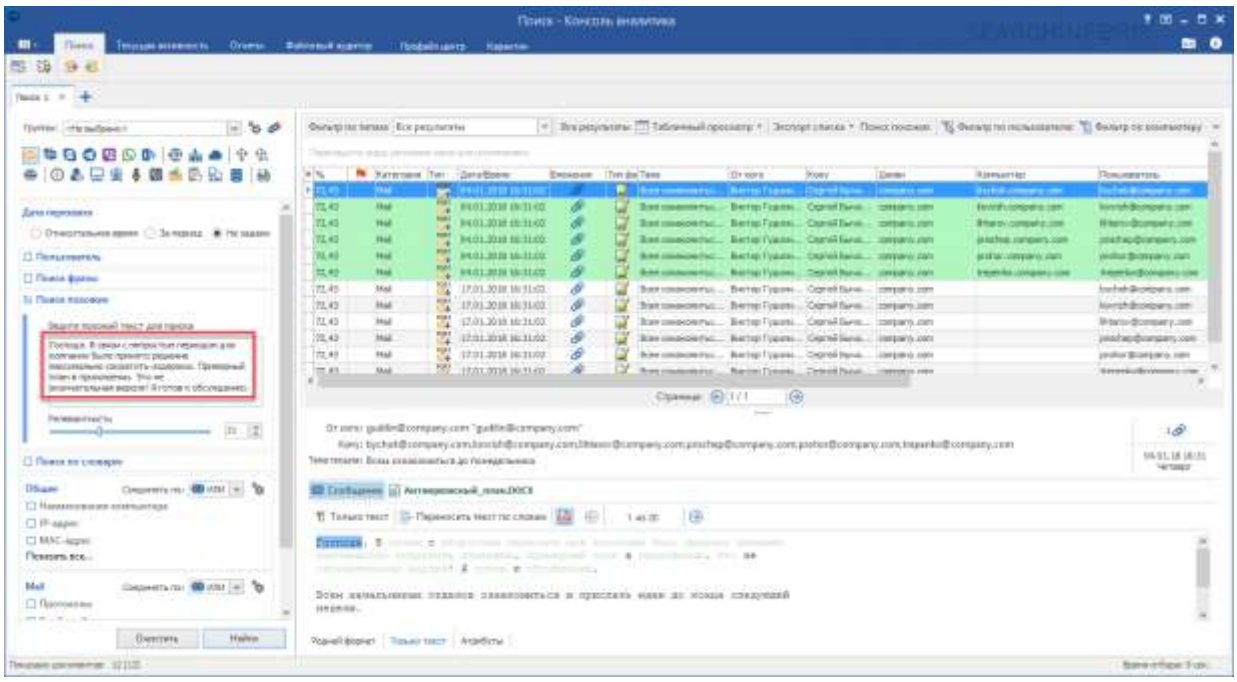


Рисунок 8.6

Искомый фрагмент текста обнаружен внутри прикрепленного к сообщению файла и был подсвечен.

8.1.4 Проверка поиска по доменным именам пользователей

В консоли AnalyticConsole откройте вкладку «Поиск». Установите флажок «Пользователь» и щелкните кнопку  (см. Рисунок 8.7).

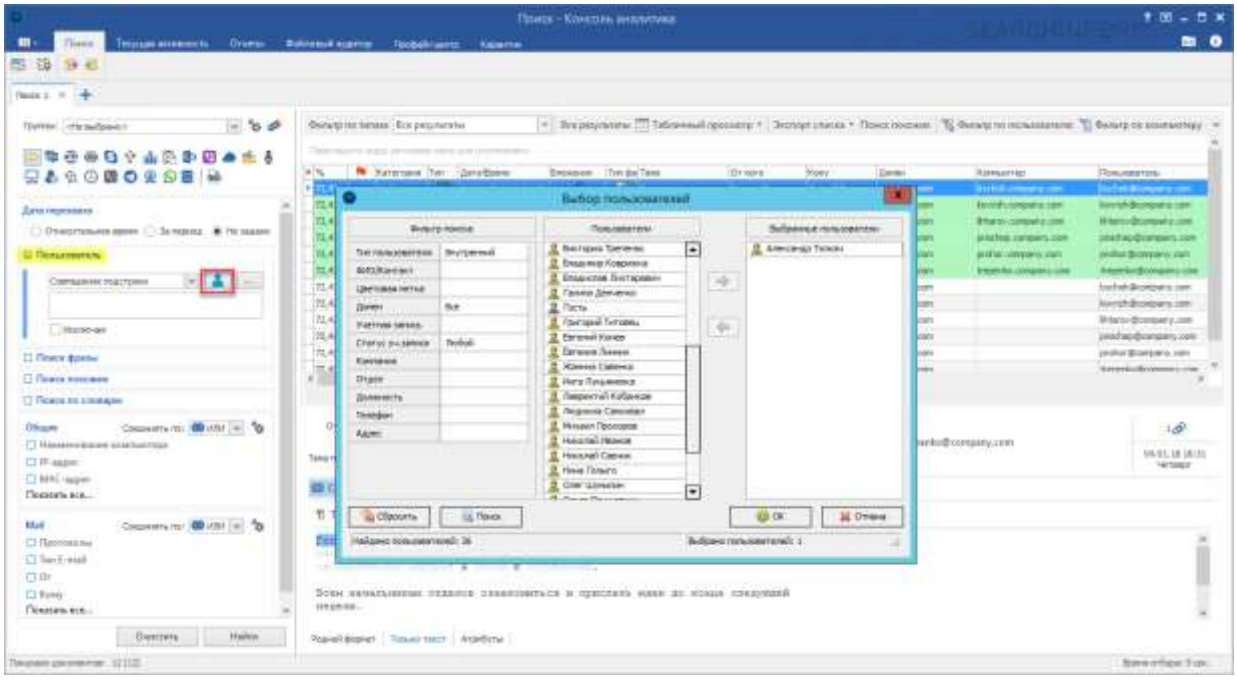


Рисунок 8.7

После добавления пользователей в консоль, произведите поиск. В выдаче клиента будут отображены все сообщения, полученные или отправленные выбранными пользователями домена (см. Рисунок 8.8).

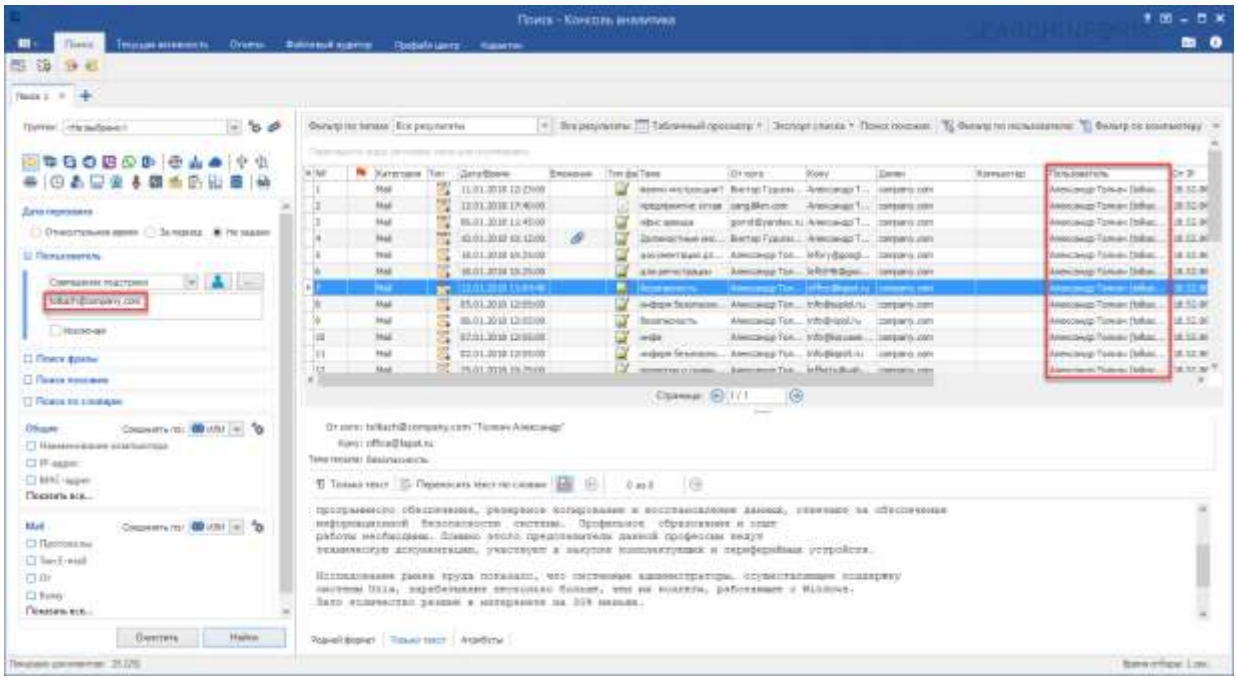


Рисунок 8.8

8.2 Проверка работы перехвата с помощью агентов EndpointController

В качестве тестового примера подробно рассматривается перехват сообщений и файлов, переданных при помощи инструментария Skype.

Проверка перехвата по остальным каналам производится аналогичным образом:

- Для внешних устройств – скопируйте несколько документов на USB-флеш-накопитель;
- Для перехвата операций с файлами – скопируйте несколько документов на жесткий диск, удалите их, пересчитайте количество выполненных операций;
- Для FTP – отправьте несколько файлов по FTP-соединению;
- Для HTTP – оставьте несколько записей в блогах либо на интернет-форумах;
- Для CLOUD – загрузите в облачное хранилище несколько файлов, затем скачайте их;
- Для сервисов мгновенных сообщений – отправьте несколько сообщений по ICQ с вложениями из комплекта тестовых файлов;
- Для электронной почты – отправьте несколько сообщений с вложениями из комплекта тестовых файлов;

- Для монитора – включите перехват содержимого монитора для выбранной рабочей станции на короткое время, задайте интервал перехвата (например, 1 минута), проверьте правильность перехваченных снимков экрана;
- Для печати – произведите печать нескольких документов из комплекта тестовых файлов (могут быть использованы физические или виртуальные принтеры);
- Для Viber – отправьте несколько сообщений и файлов по Viber Desktop.

8.2.1 Предварительная подготовка

Для проведения тестирования должны быть соблюдены следующие условия:

- Приобретены и распределены лицензии;
- На тестовые рабочие станции установлены агенты EndpointController с подключенными протоколами;
- Запущен сервер EndpointController (SIMHSvc);
- Запущена служба управления агентами (SIAMSControlSvc);
- Запущена служба контроля агентов (SIMHAgentCheck);
- Запущена служба индексирования (SearchServer);
- Настроены базы данных Microsoft SQL или FTP-хранилище, в которые записываются перехваченные данные;
- К базам данных привязаны протоколы;
- Созданы требуемые индексы;
- Настроено расписание обновления индексов;
- Настроена работа электронной почты с остановкой;
- Запущены сервисы обработки перехваченных данных;
- Установлены и настроены агенты.

8.2.2 Проверка функций перехвата

В качестве тестового примера подробно рассматривается перехват сообщений и файлов, переданных при помощи Skype.

Отправьте несколько тестовых сообщений и документов посредством Skype с произвольным текстом. Текст сообщений должен включать в себя легко распознаваемые слова (например, «контракт», «лицензия», «ведомость»).

Обновите индекс в консоли администрирования Серчинформ EndpointController (см. Рисунок 8.9).

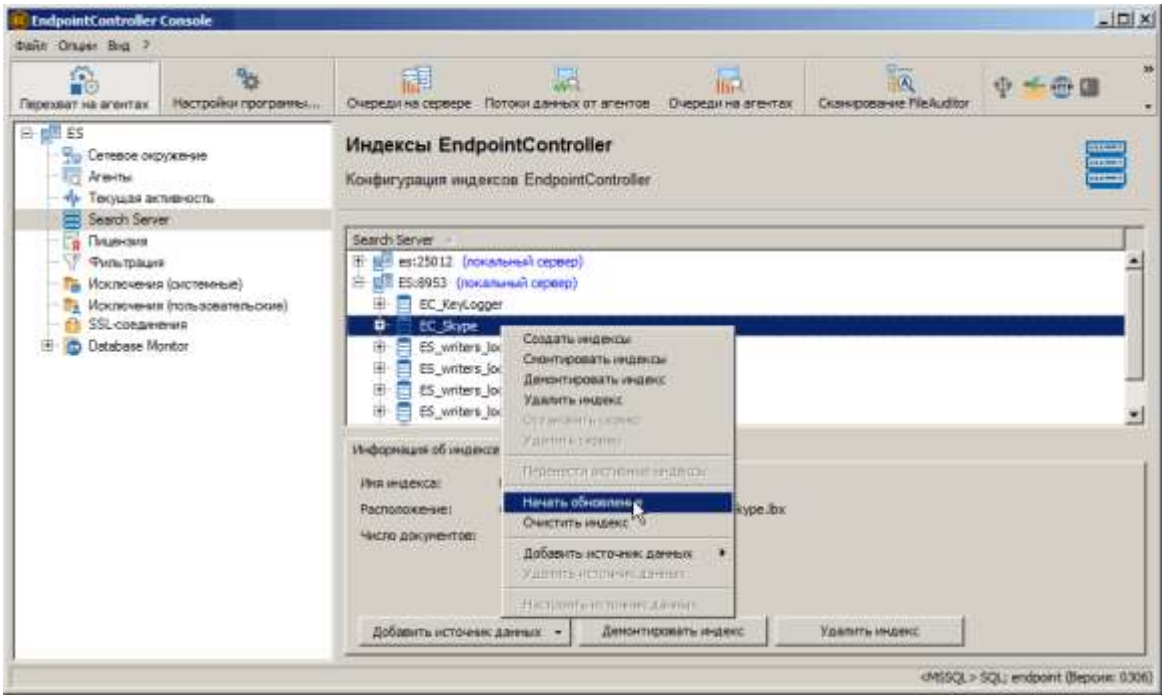


Рисунок 8.9

После обновления должно измениться число проиндексированных документов, которое должно совпасть со значением, рассчитанным по формуле «Число переписок + число файлов» (см. Рисунок 8.10).

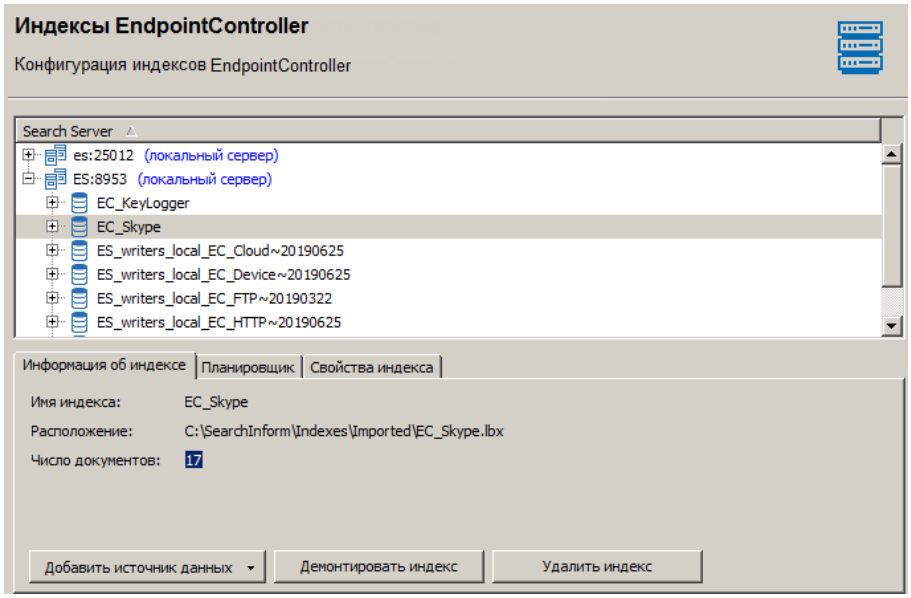


Рисунок 8.10

Откройте клиентское приложение AnalyticConsole, установленное на рабочее место аудитора безопасности, и выберите источник данных Skype.

Выполните запрос на отображение истории всех сообщений (см. Рисунок 8.11). Проверьте корректность отображения перехваченных документов.

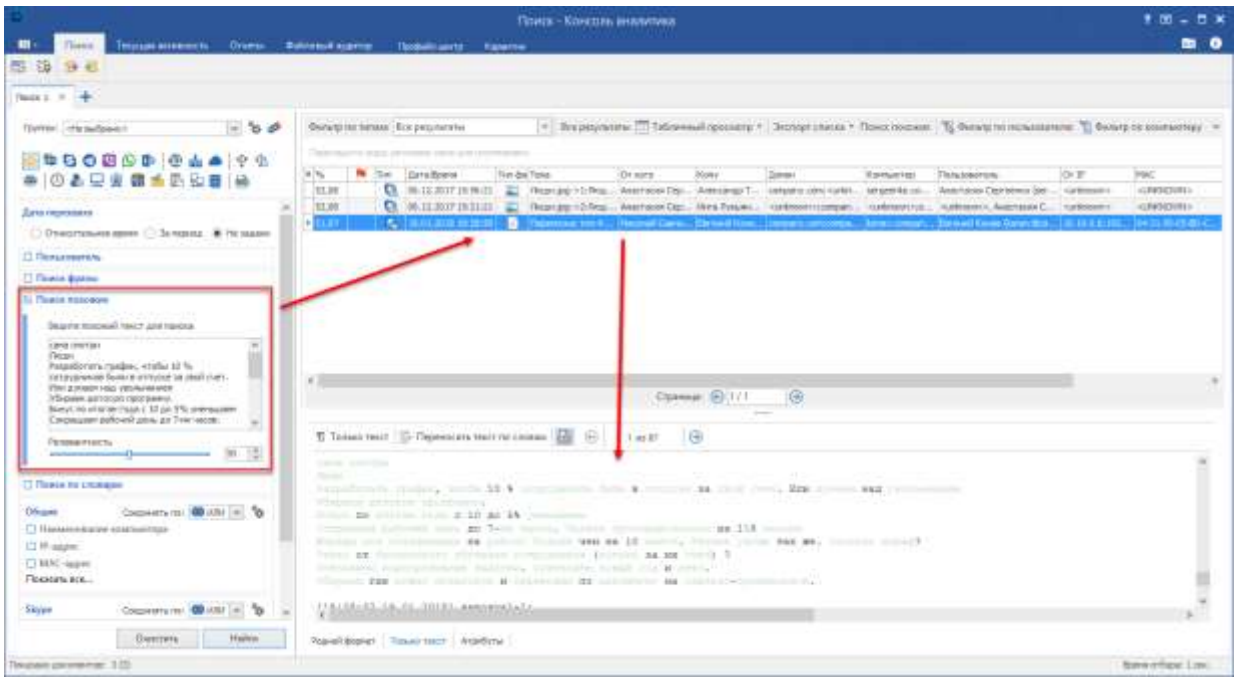


Рисунок 8.11

Проверка перехвата по остальным каналам производится аналогичным образом. Например, для перехвата почты отправьте несколько сообщений с вложениями из комплекта тестовых документов; для перехвата операций с файлами спокпируйте несколько документов на жесткий диск, удалите их, пересчитайте количество выполненных операций.

8.2.3 Проверка поиска по тексту документов

Выполните запрос для одного из тестовых сообщений Skype в клиентском приложении AnalyticConsole (см. Рисунок 8.12).

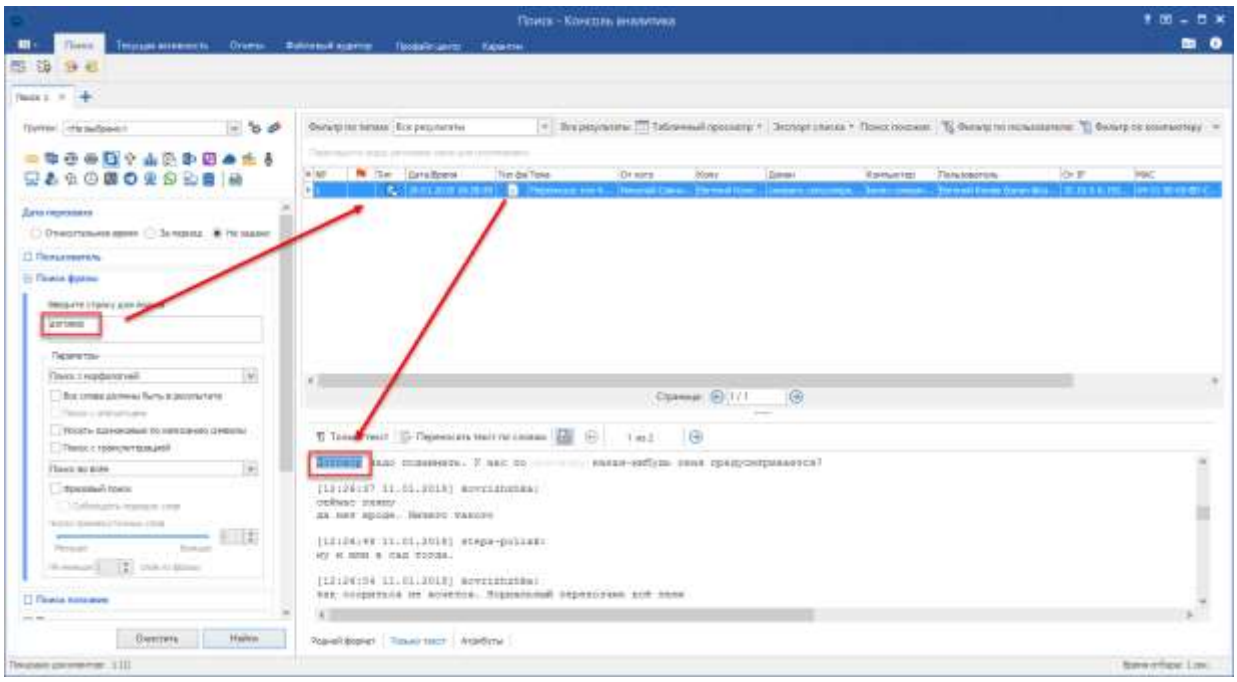


Рисунок 8.12

Для проверки поиска по перехваченным документам скопируйте в буфер обмена текст одного из отправленных сообщений (файлов), перейдите на вкладку поиска похожих, вставьте текст и произведите поиск (см. Рисунок 8.13).

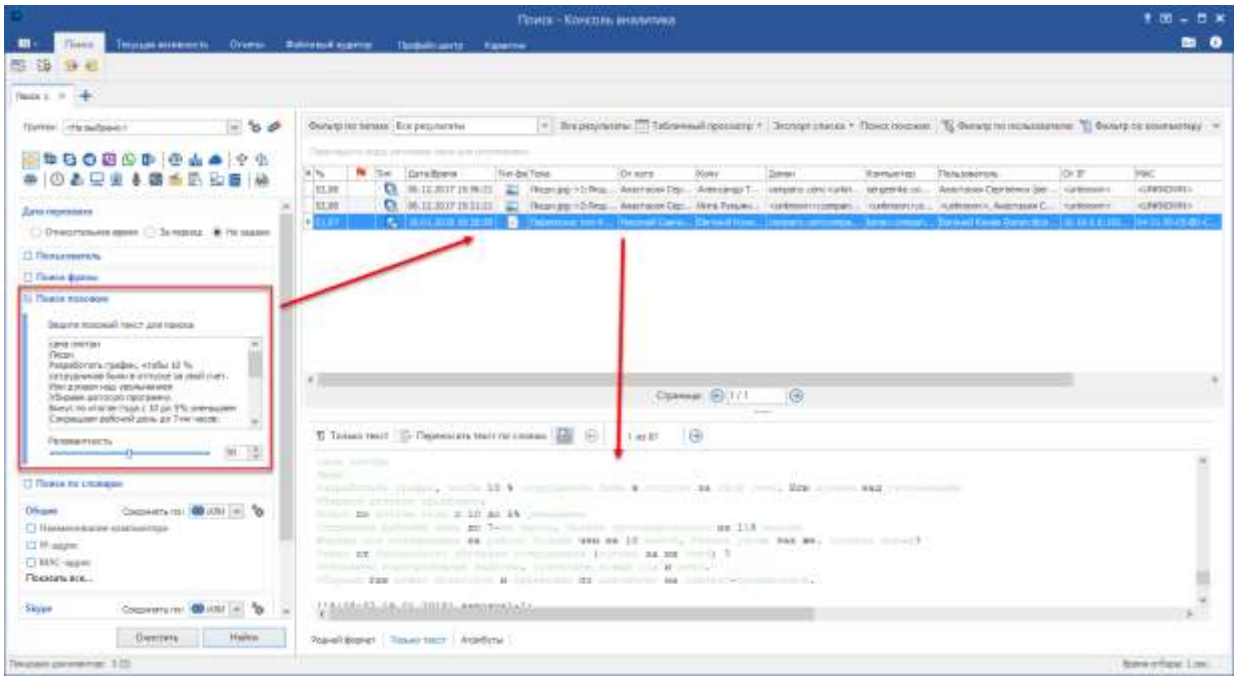


Рисунок 8.13

Документ можно открыть в сопоставленном приложении (см. Рисунок 8.14).

Рисунок 8.14

8.2.4 Проверка поиска по именам доменных пользователей

В консоли AnalyticConsole на вкладке «Поиск» установите флажок «Пользователь» и щелкните кнопку  . Выберите пользователей и щелкните кнопку «Ок». В поле ввода будет отображено имя выбранного пользователя.

Щелкните кнопку «Поиск». На панели результатов будут отображены все сообщения, полученные или отправленные выбранным доменным пользователем (см. Рисунок 8.15).

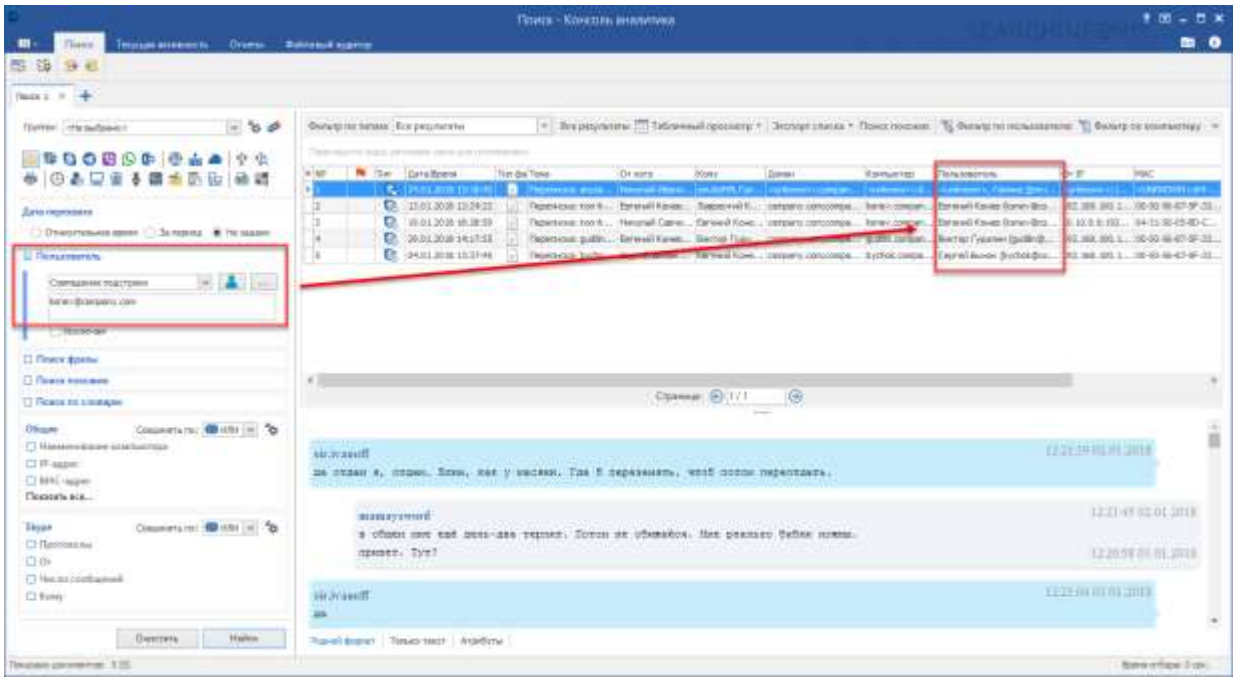


Рисунок 8.15

9 ПРОБЛЕМЫ В РАБОТЕ СИСТЕМЫ И СПОСОБЫ ИХ РЕШЕНИЯ

9.1 Проблемы в работе сервера NetworkController

9.1.1 Не отображаются имена пользователей

Симптом: Вместо доменных имен, в выдаче клиента отображено значение <Unknown>. Это означает, что не настроено или некорректно настроено взаимодействие системы с контроллером домена (см. Рисунок 9.1).

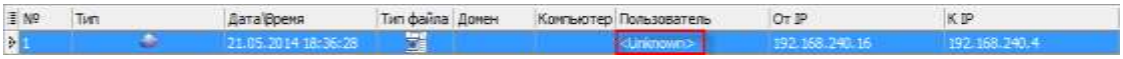


Рисунок 9.1

Возможные причины:

- недостаточные права сервиса перехвата;
- отключена индексация атрибутов документов;
- закрыты порты взаимодействия с контроллером домена.

9.1.1.1 Недостаточные права сервиса перехвата

Сервис перехвата должен быть запущен под учетной записью, включенной в доменные политики «Создание журналов безопасности» (Generate security audits) и «Управление аудитом и журналом безопасности» (Manage auditing and security log).

Процедура настройки подробно изложена в п. 6.8.6.

9.1.1.2 Закрыты порты взаимодействия с контроллером домена

Закрыты порты, используемые для подключения к журналу событий безопасности контроллера домена. Порты должны быть открыты.

NetworkController делает запрос, чтобы узнать имя контроллера домена. Это соединение происходит по протоколу CLDAP. Локальные порты этого соединения находятся в диапазоне 19**, удаленный порт (на контроллере домена) – 389. Данные порты, скорее всего, будут открыты по умолчанию, иначе компьютер не сможет войти в домен.

После того, как NetworkController получает имя контроллера домена, он подключается к журналу и начинает получать из него данные. Соединение происходит по протоколу SMB. Локальный порт соединения – 2002, удаленный порт (на контроллере домена) – 445.

9.1.2 Сообщения не перехватываются

Причина: Использование нестандартных портов.

По умолчанию NetworkController перехватывает трафик, ходящий по стандартным портам, перечисленным в Таблица 38.

Таблица 38 – Список используемых протоколами портов по умолчанию

Протоколы	Порты по умолчанию
Web mail	80
IMAP	143
MAPI	1118[33]
POP3	110
SMTP	25
NNTP (NNTPS)	119 (563)
HTTP POST	80
ICQ	443
MMP	2041
XMPP	5222
SIP	5060
HTTP IM	80
FTP	21

Решение: Для корректной работы перхвата проверьте, настроены ли нестандартные номера портов. Например, для передачи SMTP-трафика обычно используется порт 25, но может использоваться и порт 2525, а для протокола MAPI порты могут выбираться случайным образом, если на сервере Microsoft Exchange не задано жесткой привязки протокола к портам.

Для настройки привязок по портам, в группе «Сетевой перехват» выделите узел «Протоколы» и перейдите на вкладку «Настройки портов» (см. Рисунок 9.2).

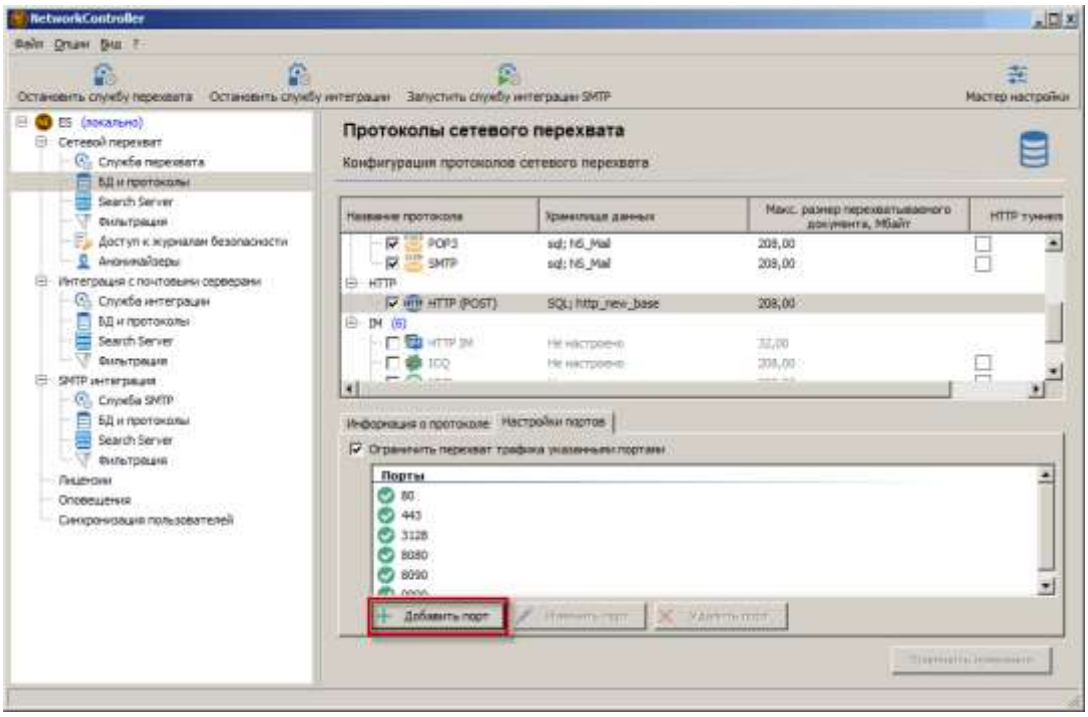


Рисунок 9.2

[33] Значение по умолчанию. Если на сервере Microsoft Exchange явным образом задан один порт, нужно прослушивать только его. Если явной привязки протокола MAPI к портам нет, нужно прослушивать весь доступный диапазон портов.

Фильтры по портам могут быть разрешающие или запрещающие. Фильтр может включать один порт (см. Рисунок 9.3) или диапазон портов (см. Рисунок 9.4).

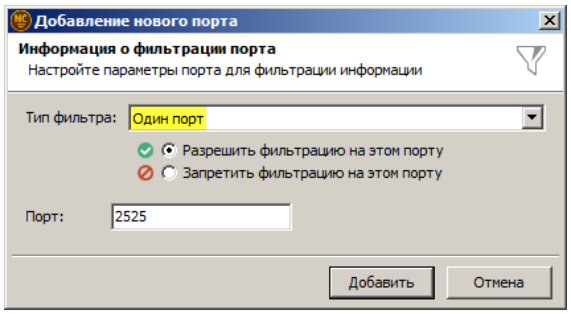


Рисунок 9.3

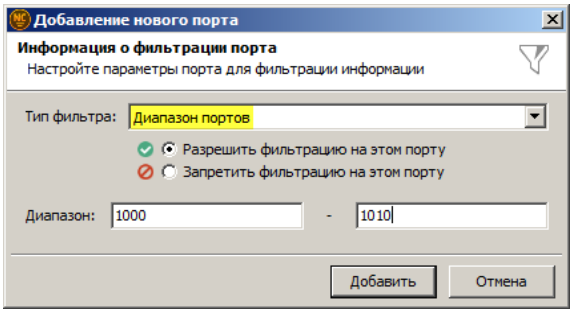


Рисунок 9.4

9.1.3 Неполный перехват данных

При подозрении на потерю пакетов рекомендуется:

- убедиться, что в настройках сетевых адаптеров отключены все «offload»-параметры);
- снять трафик с помощью программы-анализатора Wireshark и сравнить его с трафиком, перехваченным сервером NetworkController.

Wireshark – один из лучших анализаторов сетевого трафика, используемый сетевыми администраторами для выявления проблем в сети. Программа распространяется бесплатно и может быть загружена с www.wireshark.org.

Если настройки адаптеров соответствуют требованиям, а трафик Wireshark и NetworkController отличается количеством перехваченных документов, существует возможность смены библиотеки перехвата с Packet Sniffer SDK (pssdk.dll) на WinPcap (wpcap.dll). Однако данный механизм перехвата рекомендуется использовать лишь в крайнем случае, поскольку его работа существенно медленнее стандартного.

Для смены библиотеки перехвата откройте конфигурационный файл **sinssvc.xml**, расположенный по адресу: %ProgramFiles%\SearchInform\SearchInform NetworkController\SearchInform NetworkController Server\.

Внутри корневого тега `<sinssvc>` пропишите строку (см. Рисунок 9.5)**:**

<sniffer>wpcap</sniffer>.

Рисунок 9.5

Сохраните измененный файл.

9.1.4 Не запускается служба перехвата

Причина: Изменение доменных политик и отмена права входа в качестве службы для пользователя домена, под учетной записью которого запускается сервис NetworkController.

Решение: см. п. 4.6.1 «Настройка прав входа в качестве службы».

9.2 Проблемы в работе сервера EndpointController

9.2.1 Агенты не устанавливаются или не обновляются

Симптом 1: После выбора рабочих станций и нажатия кнопки «Применить» не отображаются маркеры «✔».

Симптом 2: Не происходит обновления версий агентов или версии агентов не отображаются (см. Рисунок 9.6).

Без установленных агентов перехват невозможен!

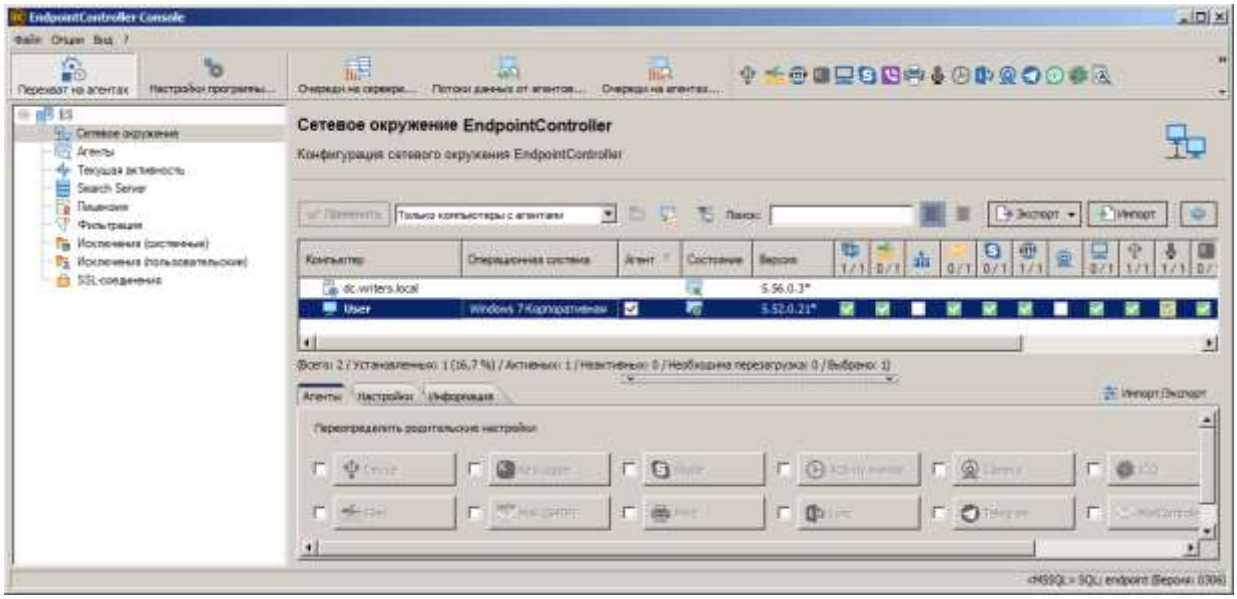


Рисунок 9.6

Журнал удачных и неудачных попыток установки агентов на рабочие станции пользователей можно просмотреть на вкладке «Текущая активность» (см. Рисунок 9.7).

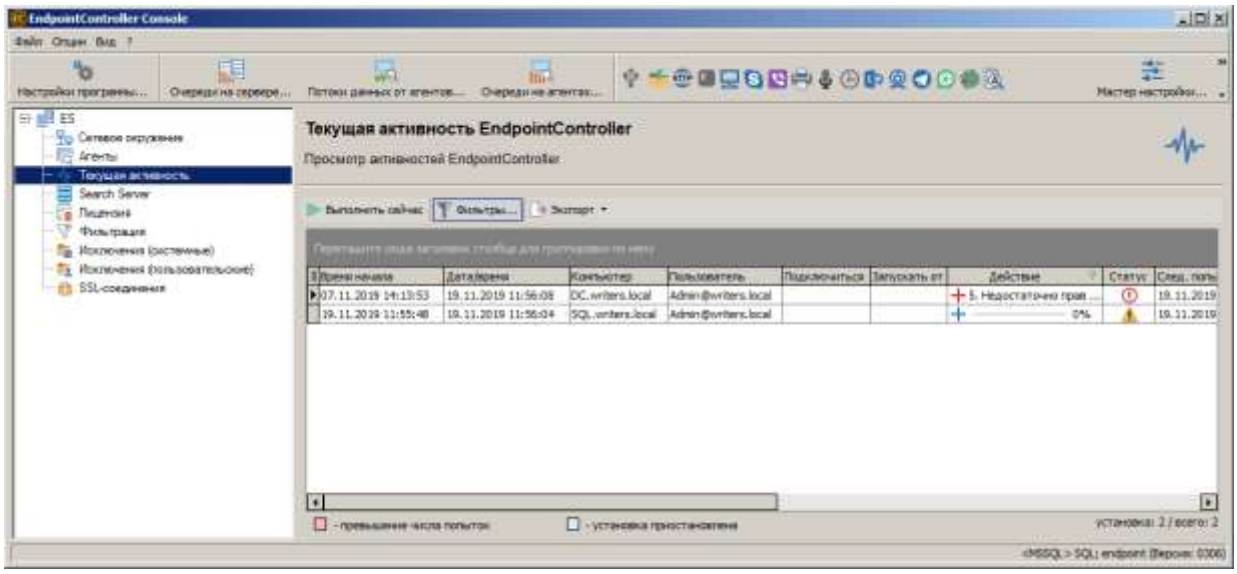


Рисунок 9.7

Журнал текущего состояния установок агентов включает в себя следующие параметры:

- **Время начала** – дата и время начала первой попытки установить/удалить/обновить агент на рабочей станции;
- **Дата/время** – дата и время начала текущей попытки установить/удалить/обновить агент на рабочую станцию;
- **Компьютер** – имя компьютера, на который устанавливался или был установлен агент;
- **Пользователь** – имя пользователя, инициировавшего активность;
- **Подключиться как** – учетная запись, от которой производится установка агента (при включенной опции «Подключаться как»);
- **Запускать от имени** – учетная запись, от которой производится запуск агента (при включенной опции «Запускать от имени»);
- **Действие** – значок, указывающий на действие, которое производится с агентом;
- **Статус** – значок, отображающий статус сообщения;
- **След. попытка** – дата и время следующей попытки установить/удалить/обновить агент;
- **Попыток** – число попыток, предпринятых для установки/удаления/обновления агента;
- **Сообщение** – пояснение о выполнении/невыполнении определенного действия над агентом;

- **Описание** – описание рабочей станции, заданное в Active Directory, либо на вкладке «Сетевое окружение»;
- **Комментарии** – пользовательский комментарий к определенной рабочей станции, задаваемый на вкладке «Сетевое окружение».

Возможные варианты действий, производимых с агентами:

- нет значка – действие не задано,
-  – добавление агента,
-  – удаление агента,
-  – обновление агента.

Возможные статусы сообщений:

- нет значка – статус не задан,
-  – сообщение,
-  – предупреждение,
-  – ошибка,
-  – обновление со стороны агента.

Возможные сочетания «проблема-решение»:

- агенты не устанавливаются – отмена запрета на установку;
- агенты не устанавливаются – установка вручную;
- агенты установлены, но не передают данные – запуск служб под другой учетной записью.

9.2.1.1 Агенты не устанавливаются – отмена запрета на установку

Симптом: Агенты не устанавливаются.

Причина: Новые агенты не будут устанавливаться, если в отношении их установки действует запретительный режим (по умолчанию действует разрешительный режим на установку агентов) (см. Рисунок 9.8).

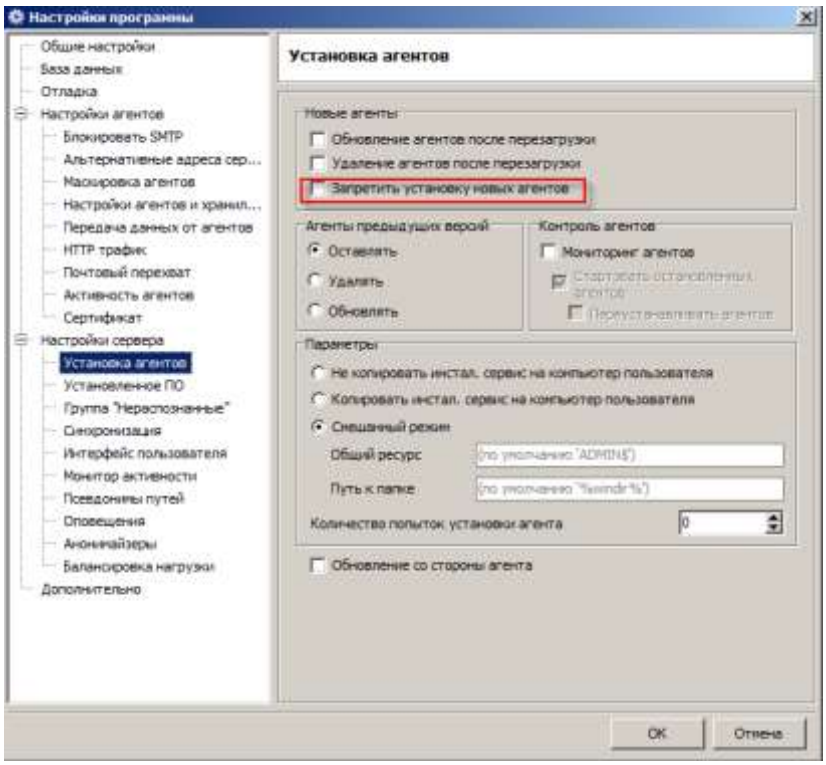


Рисунок 9.8

Решение: Перейдите в настройки EndpointController и выберите вкладку «Установка агентов». Снимите флажок «Запретить установку новых агентов» и щелкните «OK».

9.2.1.2 Агенты не устанавливаются – установка вручную

Симптом: Агенты не устанавливаются, протоколы не включаются.

Причина: Служба сервера EndpointController имеет недостаточно прав для установки агента, установке соединения мешает брандмауэр и др.

Решение: Установка агентов вручную.

Подробное описание решения проблемы приводится в пункте 6.5.3.4.

9.2.1.3 Агенты установлены, но не передают данные – запуск служб под другой учетной записью

Симптом 1: Агенты установлены, серверные службы работают, но индекс остается пустым при обновлении (проиндексировано 0 документов).

Симптом 2: Агенты установлены, службы работают, перехват был, но исчез, или не обновляются версии агентов.

Наиболее вероятная причина: Недостаточно прав у служб EndpointController (например, изменились доменные политики).

Решение: Настройте вход служб SIAMSControlSvc и SIMHSvc под учетной записью с правами администратора домена.

Сочетанием клавиш **Win+R** откройте окно «Выполнить», введите команду **services.msc**. Будет открыта оснастка «Службы», отображающая список служб и их

состояние. Сервер EndpointController использует службы SearchInform EndpointController Agents Control (SIAMSControlSvc.exe), SearchInform EndpointController Agents Check (SIMHAgentCheck.exe) и SearchInform EndpointController (SIMHSvc.exe) (см. Рисунок 9.9).

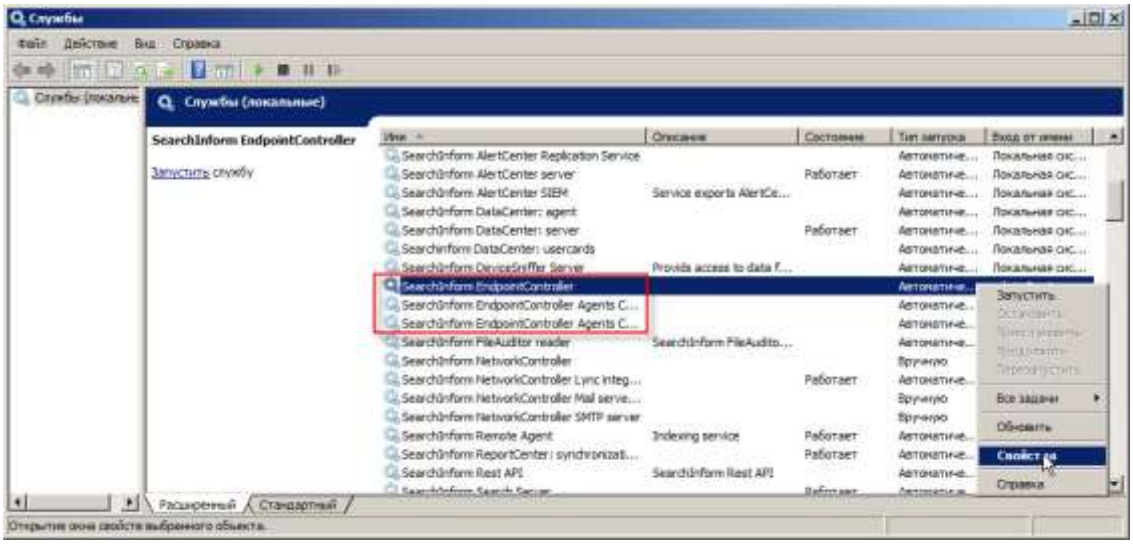


Рисунок 9.9

Откройте свойства служб на вкладке «Вход в систему». Выберите опцию «С учетной записью» и введите параметры учетной записи пользователя с правами администратора домена (см. Рисунок 9.10).

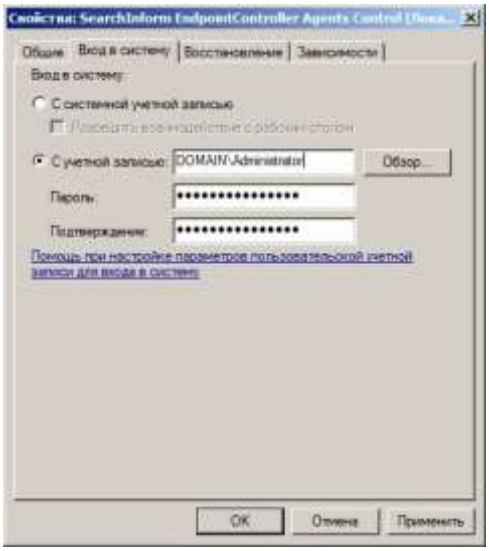


Рисунок 9.10

После изменения прав входа перезапустите службы.

9.2.2 Невозможно создать базу настроек EndpointController

Симптом: при создании новой базы данных EndpointController, где будут храниться настройки сервера, отображается сообщение об ошибке.

Причина: Неправильная конфигурация СУБД Microsoft SQL Server.

Microsoft SQL Server должен поддерживать внутреннюю аутентификацию пользователей. Для этого СУБД должна быть установлена в режиме смешанной аутентификации пользователей.

В общих свойствах сервера SQL в параметрах сортировки сервера должно быть выставлено значение "Cyrillic_General_CI_AS" (см. Рисунок 9.11).

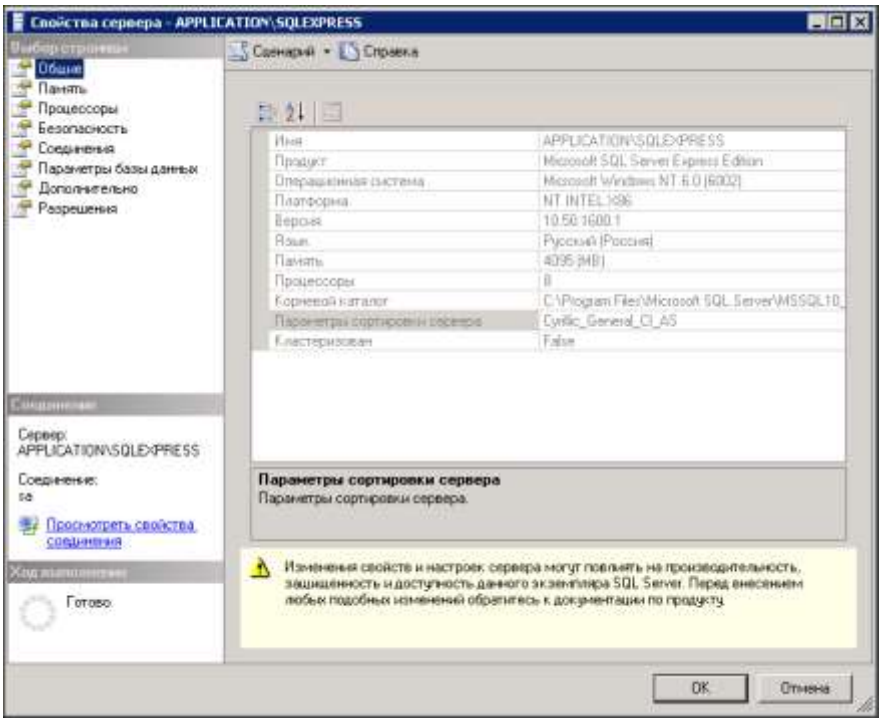


Рисунок 9.11

Решение: Зайдите на сервер SQL и выставить указанное значение параметра сортировки. После этого вернитесь к процедуре установки и настройки EndpointController.

9.3 Проблемы в работе сервера индексации Search Server

9.3.1 Невозможно выполнить индексацию

Симптом: При запуске индексации отображается сообщение о невозможности произвести индексацию.

Причина: Сохранение перехваченных по разным каналам коммуникации документов в одной базе данных.

Решение: Пересоздайте базу данных. Для каждого канала передачи данных создается отдельный индекс и соответственно – отдельная база данных. Сохранение перехваченных по разным каналам связи данных в одну базу приводит к сбоям в работе сервера индексации.

9.4 Проблемы в работе клиентского приложения

9.4.1 Нехватка памяти

Симптом: При нехватке памяти, клиент может отображать сообщение о динамической ошибке (run-time error).

Причина: Такая ошибка вызвана нехваткой памяти на построение списка документов.

Решение: Для разрешения проблемы уменьшите число документов в выдаче клиента.

Откройте настройки AnalyticConsole. На вкладке «Результаты поиска» ограничьте количество выдаваемых в консоли результатов поиска (см. Рисунок 9.12).

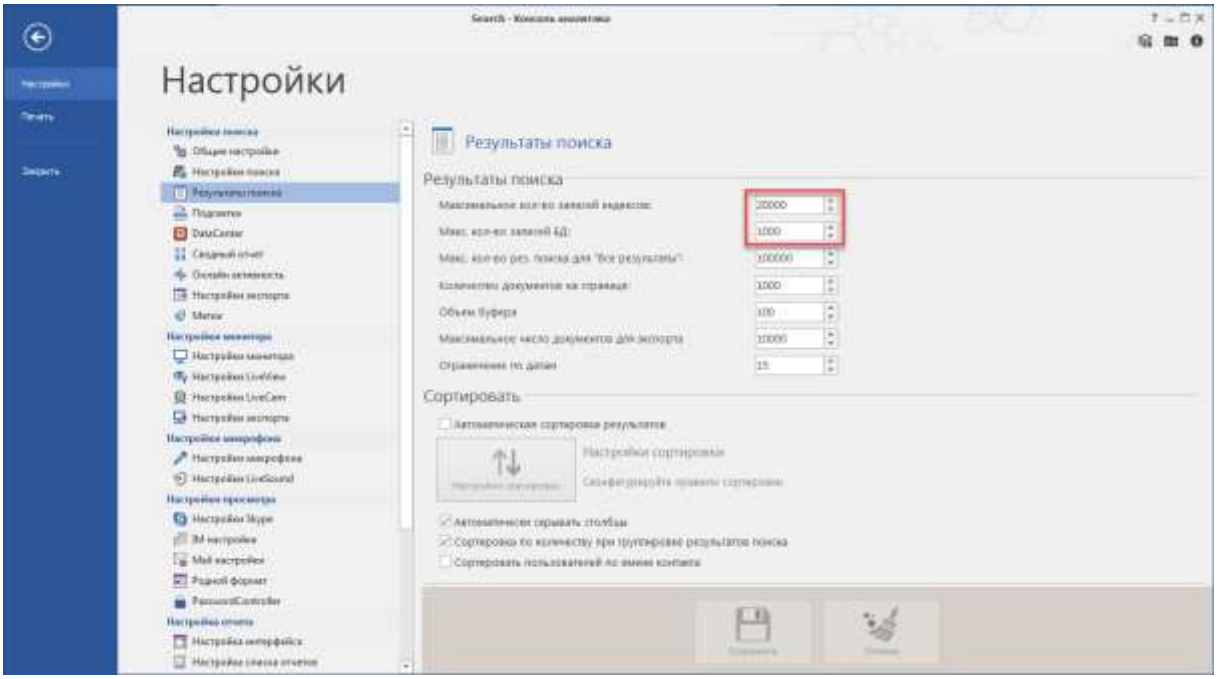


Рисунок 9.12

9.4.2 Проблемы с кодировкой при отображении сообщений в клиенте

Симптом: Клиент отображает сообщения в некорректной кодировке.

Решение: Выберите вручную верную кодировку из контекстного меню окна предпросмотра (см. Рисунок 9.13).

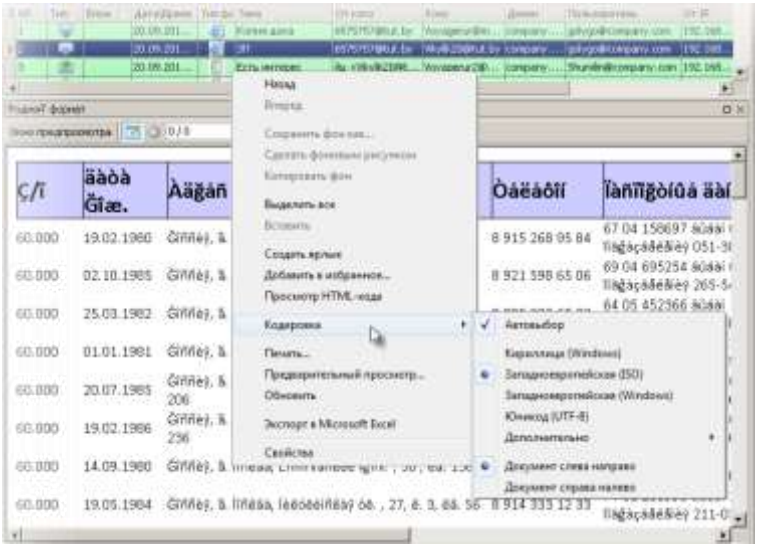


Рисунок 9.13

9.4.3 Переходы по отчетам не производятся

Симптом: В окне просмотра отчетов не производятся переходы, правая клавиша не вызывает контекстное меню.

Причина: Автопереходы и контекстное меню отключены в настройках клиента ReportCenter.

Решение: Установите флажки «Разрешить автопереходы …» и выберите опцию переходов по диаграммам «По правой кнопке мыши» (см. Рисунок 9.14).

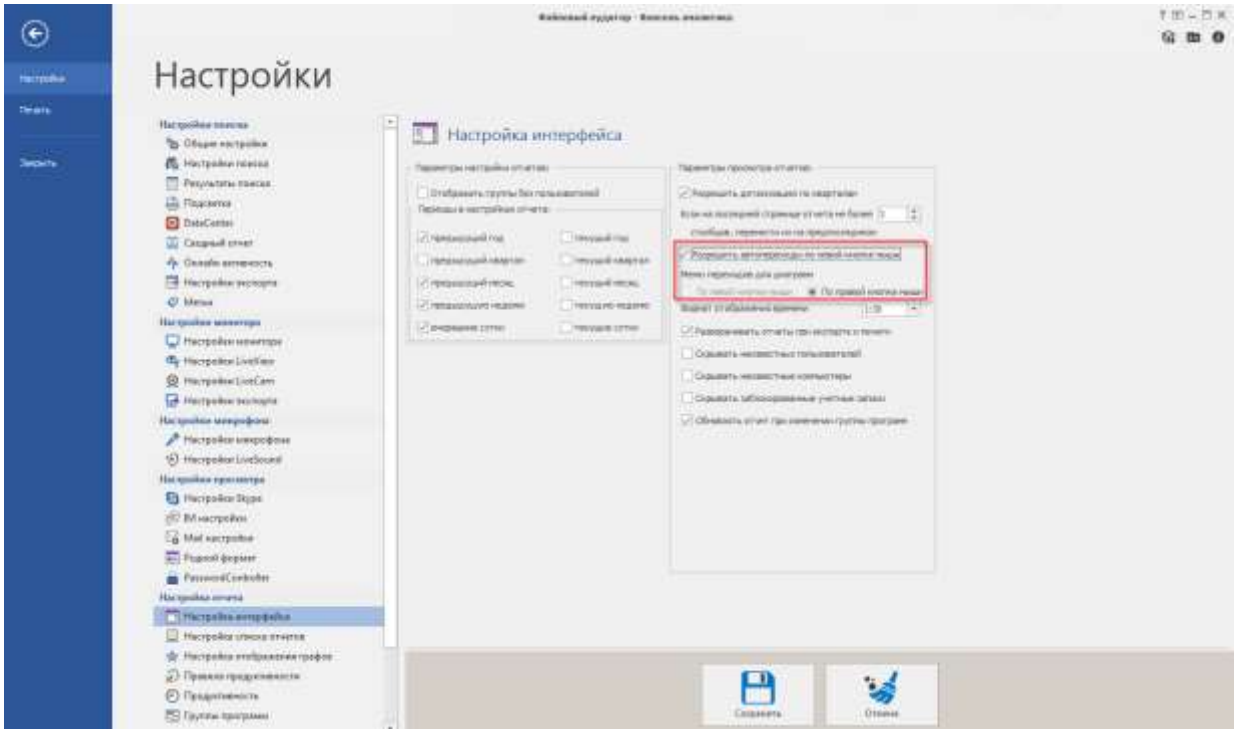


Рисунок 9.14

9.4.4 Отображаются пустые отчеты

Симптом: отображаются пустые отчеты.

Причина: Не подключены источники данных или сервер ReportCenter не синхронизирован с ними.

Решение: Подключите источники данных и/или произведите синхронизацию.

9.4.5 Статистика не обновляется

Симптом: статистика не обновляется.

Причина: Сервер и AnalyticConsole подключены к разным базам.

Решение: Произведите подключение сервера ReportCenter и AnalyticConsole к одной базе.

9.5 Проблемы в работе модуля администрирования DataCenter

9.5.1 Контролируемые компоненты не отображаются или отображаются некорректно

Симптом: Не отображаются серверы контролируемых компонентов, на которые были установлены агенты DataCenter (см. Рисунок 9.15).

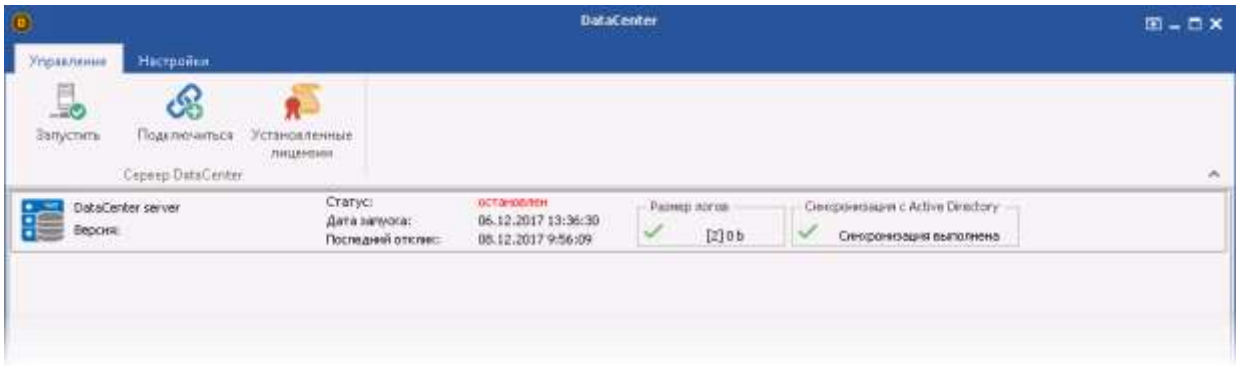


Рисунок 9.15

Причина: Задан неверный путь от агента к серверу DataCenter.

Решение: Произведите повторную установку агентов DataCenter. При этом укажите правильный путь к серверу DataCenter (см. Рисунок 9.16).

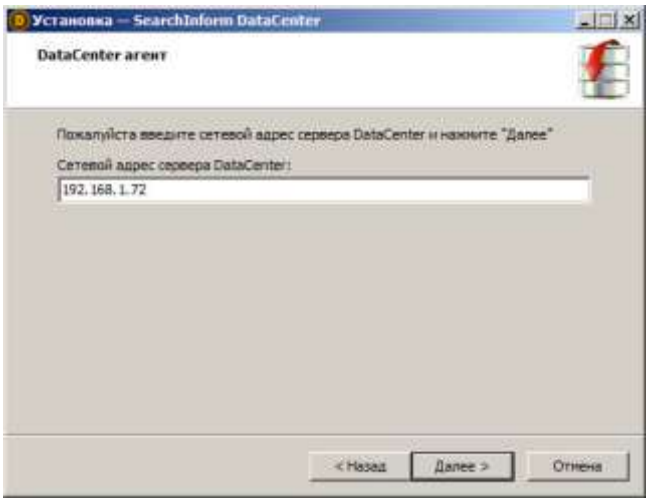


Рисунок 9.16

9.5.2 Уведомления не доставляются

Симптом: Настроена доставка уведомлений, но уведомления не доставляются.

Причина 1: Неправильные настройки подключения к серверу SMTP.

Причина 2: Неверный адрес получателя.

Причина 3: Неверный адрес отправителя.

Решение: Проверьте настройки подключения к SMTP-серверу.

Щелкните кнопку «Почтовые уведомления», расположенную на панели «Настройки». Нажмите кнопку «Проверить соединение» (см. Рисунок 9.17).

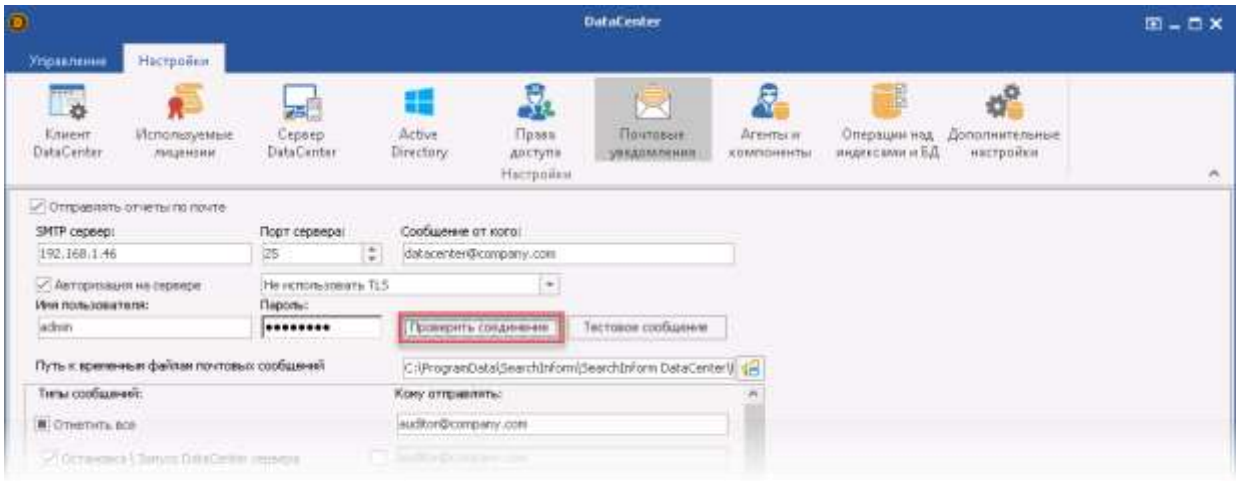


Рисунок 9.17

Будет отображено одно из следующих сообщений:

- «Не удалось установить соединение» - неверно указан SMTP-сервер, SMTP-порт или отправитель. Укажите верные настройки.
- «Не удалось пройти аутентификацию» - неверные настройки аутентификации. Установите флажок «Аутентификация на сервере», введите корректные имя учетной записи и пароль.

После настройки кликните кнопку «Проверить соединение. Если введены верные настройки, будет отображено сообщение «Соединение успешно установлено!».

Для отправки тестового сообщения на электронный адрес аудитора безопасности используется кнопка «Тестовое сообщение».

Если проблема заключалась в неверном адресе отправителя или получателя, очистите папку «MailTemp\», расположенную в папке с логами DataCenter (см. Рисунок 9.18).

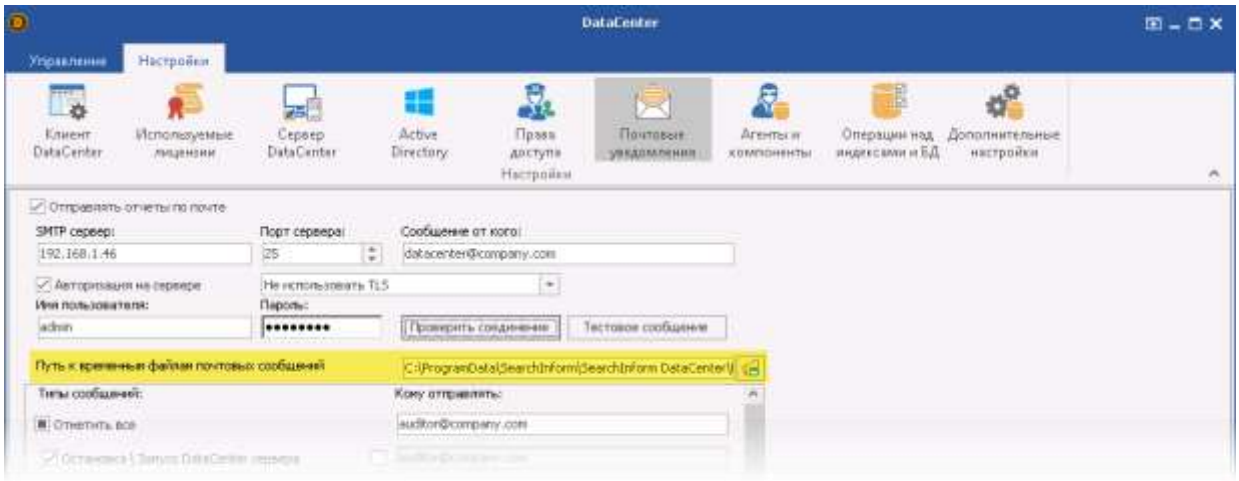


Рисунок 9.18

9.5.3 Сервер в списке выделен красным цветом

Выделение имени сервера красным цветом свидетельствует о наличии проблем в работе его компонентов. Например, если не запущен какой-либо из установленных на сервере продуктов или отсутствует доступ к базе перехвата, или возникли ошибки при разбиении индексов и БД. Для обнаружения источника ошибки разверните список компонентов сервера, имя которого подсвечено красным, нажав . Компонент с критической ошибкой также выделен в списке красным цветом (см. Рисунок 9.19).

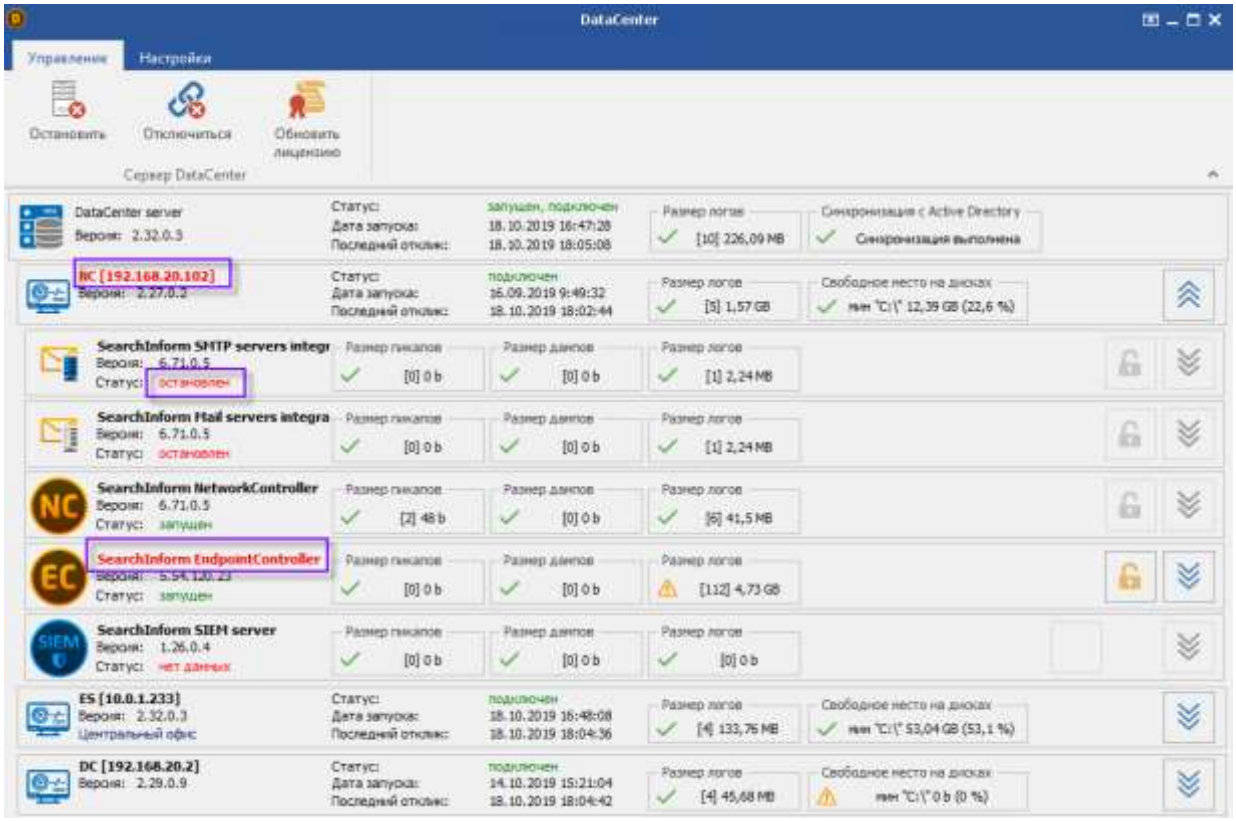


Рисунок 9.19

Симптом: Имя сервера выделено в списке красным цветом.

Причина 1: Ошибки при разбиении индекса или БД компонентов сервера.

Решение 1: Проверьте, не «загорелась» ли напротив компонента иконка (Рисунок 9.20).

Рисунок 9.20

Данное обстоятельство означает, что произошла блокировка автоматических действий по продукту, требующая выяснения и устранения причины. При этом индексация данных будет происходить в штатном режиме, а автоматическое разбиение,

удаление, принудительные запуск и перезапуск по данному модулю происходить не будут.

После устранения причины, вызвавшей неполадку, щелкните по иконке , чтобы деактивировать блокировку. Значок приобретет монохромные цвета.

Если других ошибок нет, красный цвет названия компонента сменится обычным.

Причина 2: Доступ к базе данных отсутствует.

Решение 2: Наведите курсор мыши на компонент, подсвеченный красным цветом, и дождитесь отображения всплывающего окна, отображающего информацию по корректности доступа к индексам и БД (см. Рисунок 9.21).

Шаблон отображаемой сводки следующий:

протокол [<СУБД> полное_доменное_имя_компьютера; имя_БД]: статус

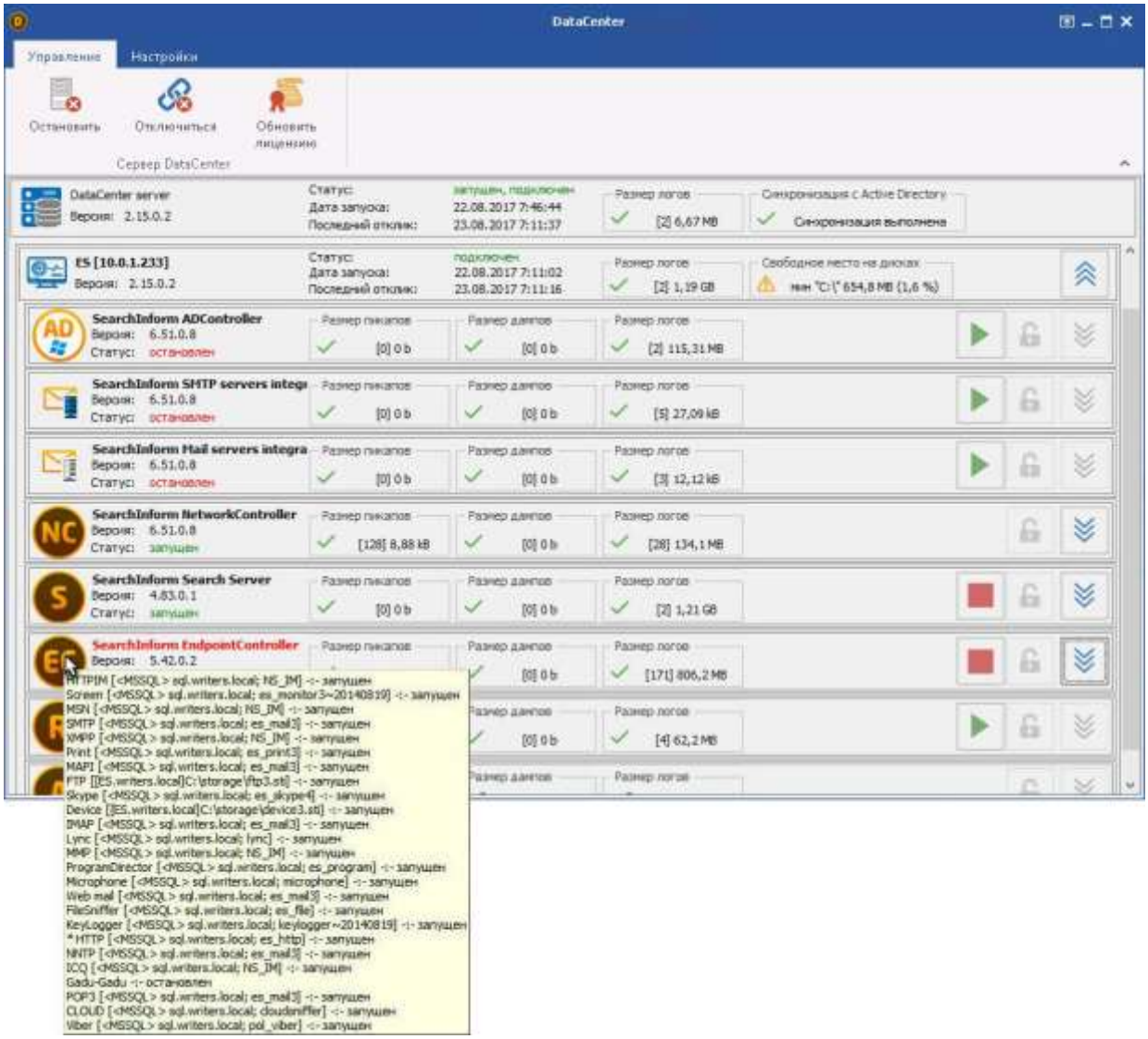


Рисунок 9.21

Обратите внимание на протоколы, перед которыми стоит символ «*****», отображающийся при *незаданных настройках БД*, *отсутствии индекса*, настроенного на данную БД по указанному протоколу, а также при *отключенном перехвате данных*.

Если Вы видите статус «*нет доступа*», это означает, что доступ к базе данных этого протокола отсутствует (база данных удалена, изменены настройки подключения к базе данных и пр.).

Если других ошибок нет, красный цвет названия компонента сменится обычным.

9.5.4 Не отображается онлайн активность пользователей в WebAnalytic

Симптом: В WebAnalytic не отображается отчет по онлайн активности пользователей.

Причина: Отсутствие у пользователя SQL-сервера прав на подключение Linked Server.

Решение: Для пользователя SQL-сервера, который будет просматривать данный отчет, добавьте права доступа с помощью запроса:

```
USE master;
GRANT ALTER ANY LINKED SERVER TO <UserName>;
GO

USE master;
GRANT ALTER ANY LOGIN TO <UserName>;
GO
```

10 ИСТОЧНИКИ РАЗРАБОТКИ

Документы, на основании которых разработан данный документ, а также на основании которых должно производиться выполнение работ:

1. РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов.
2. ГОСТ 2.503-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Правила внесения изменений.
3. ГОСТ 2.105-95 Общие требования к текстовым документам.
4. Федеральный закон от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5.