КАЗАНСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

ИНСТИТУТ ФИЗИКИ

Кафедра Радиофизики

П. А. Корчагин, Д. Е. Чикрин

МОНИТОРИНГ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Методические указания к выполнению лабораторной работы

Казань – 2019

УДК 681.322

Принято на заседании кафедры радиофизики

Протокол № 7 от 25марта 2019 года

Рецензент

кандидат физико-математических наук,

доцент кафедры радиоастрономии КФУ **Е. Ю. Зыков**

Корчагин П. А., Чикрин Д. Е.
Мониторинг утечек конфиденциальной информации. Методические указания к выполнению лабораторной работы / П. А. Корчагин, Д. Е. Чикрин Д. Е. – Казань: Казан. ун-т, 2014. – 68 с.

Методические указания рассчитаны на студентов старших курсов, обучающихся по направлению «Информационная безопасность» и содержат необходимые для выполнения лабораторной работы теоретические и справочные сведения.

Содержание

Лабораторная работа №2

Принципы использования программного комплекса SearchInform для мониторинга утечек конфиденциальной информации

Цель работы: освоить основные приемы использования программного комплекса SearchInform для перехвата и поиска утечек конфиденциальной информации.

Теоретические сведения

Существующая версия программного комплекса «Контур информационной безопасности SearchInform» предназначена для выявления утечек конфиденциальной информации при ее передаче посредством:

- электронной почты,
- службы обмена мгновенными сообщениями (ICQ, QIP),
- вэб-клиентов (передача данных по протоколу HTTP в социальные сети, форумы, блоги),
- ftp-клиентов,
- голосовых и текстовых сообщений Skype,
- записи на внешние устройства (Flash-носители, компакт-диски, внешние жесткие диски),
- печати на принтере.

Кроме этого, существует возможность выявления конфиденциальной информации на компьютерах пользователей, а также мониторинга изображений на дисплее пользователя.

Укрупненно выявление утечек разделяется на четыре этапа:

- перехват информации, передаваемой по контролируемым каналам,
- запись перехваченной информации в хранилище,
- поиск в информационном хранилище конфиденциальных данных,
- оповещение о найденных конфиденциальных данных.

Для перехвата передаваемых данных используются: MailSniffer, IMSniffer, HTTPSniffer, FTPSniffer, SkypeSniffer, PrintSniffer, сервер индексации рабочих станций, MonitorSniffer. Перехваченные данные записываются в базу данных MS SQL Server и подвергаются процедуре индексации, необходимость которой объясняется повышением скорости поиска. Собственно, поиск конфиденциальных данных осуществляется по индексам, которые представляют собой элементы, включающие в себя информацию о расположении и содержании перехваченных документов и список всех слов этих документов. Для индексации данных используется компонент DataCenter. Оповещение о найденных конфиденциальных данных, т.е. о выявленном факте утечки, реализуется с помощь компонента AlertCenter.

Отметим, что во многих организациях есть пользователи, документы которых должны быть исключены из перехвата. Для исключения перехвата следует использовать фильтры SearchInform EndpointSniffer Console и SearchInform NetworkSniffer Administrator Console. Фильтры по пользователям особенно актуальны для сервера NetworkSniffer, который управляет компонентами MailSniffer, IMSniffer и HTTPSniffer, т.к. перехват идет на уровне сетевых адаптеров и по умолчанию перехватываются документы всех пользователей. Фильтры по пользователям не настолько важны для компонентов SkypeSniffer, PrintSniffer и DeviceSniffer, т.к. информация перехватывается только агентами, установленными на целевые рабочие станции. Документы пользователей, исключенных из перехвата, не будут помещены в базы данных. Еще одной причиной ограничения пользователей, документы которых должны быть исключены из перехвата, может быть ограниченность приобретенной лицензии комплекса SearchInform. Например, если приобретена лицензия на 50 рабочих станций, а есть 60 пользователей электронной почты, то нужно настроить или ограничивающий фильтр на 10 пользователей, или разрешающий фильтр на 50 пользователей.

Есть общие правила работы фильтров. Если опция фильтрации включена, но список фильтров пуст, перехват будет осуществляться без ограничений по адресам. Чтобы пакет данных попал под правило ("запретить" или "разрешить" перехват), достаточно совпадения по одному атрибуту. Одновременно можно использовать или запрещающие фильтры, или разрешающие фильтры. При использовании запрещающих фильтров в базу данных будут передаваться все перехваченные пакеты, за исключением совпадений по фильтрам. При использовании разрешающих фильтров в базу данных будут переданы все перехваченные пакеты, совпадающие с фильтрами.

В консоли EndpointSniffer для запрещающей фильтрации должна быть включена опция "Исключить из перехвата трафика", а для разрешающей фильтрации должна быть включена опция "Включить в перехват трафика".

Если нужно сделать так, чтобы документы перехватывались и помещались в базу, но по ним не генерировались уведомления, следует настроить фильтры SearchInform AlertCenter Client.

Наиболее сложным этапом выявления утечки является поиск в перехваченных документах конфиденциальных данных. Реализация эффективного поиска требует комплексного применения различных приемов и методов, которые существенно зависят от содержания анализируемого документа и характера конфиденциальных данных.

С точки зрения эффективного поиска, анализируемые документы разделяются на формализованные (структурированные) и неформализованные (неструктурированные). Примерами структурированных документов являются финансовые отчеты, бизнес-планы, счета-фактуры, авансовые ведомости. К неструктурированным документам чаще всего относятся сообщения социальных сетей, форумов, ICQ, Skype. Очевидно, что выявить структурированный конфиденциальный документ проще всего на основании определения некоторых формальных атрибутов, кото-

рые присутствуют в подобных документах. Распознать неструктурированную конфиденциальную информацию сложнее. Для этого следует проанализировать смысл текста документа.

Поиск конфиденциальной информации осуществляется с помощью клиентов MailSniffer, IMSniffer, HTTPSniffer, PrintSniffer, DeviceSniffer, SkypeSniffer, SoftInform Search, а также компонента AlertCenter, которые обеспечивают:

1. Полнотекстовый поиск – поиск, по ключевым словам, и словосочетаниям в тексте перехваченных документов. При полнотекстовом поиске не учитывается порядок слов и их положение в документе.

2. Фразовый поиск – поиск, по ключевым словам, с учетом их положения друг относительно друга. Позволяет отсечь документы, в которых ключевые слова разбросаны по всему тексту.

3. Поиск похожих – поисковый запрос представляет собой целый текст, с которым сравнивается каждый перехваченный документ. Система вычисляет степень похожести (релевантность) для каждого перехваченного документа, если релевантность превышает заданный аудитором уровень, система генерирует оповещение для аудитора безопасности. При вычислении показателя релевантности учитывается множество факторов, в том числе процент общих слов, порядок слов запроса, размер запроса, размер искомого документа. Интеллектуальные возможности этого типа поиска позволяют отслеживать отсылку конфиденциальных документов даже в том случае, если они были предварительно отредактированы. В качестве поискового запроса используются как фрагменты документов, так и документы целиком, а результатом поиска являются документы, не только содержащие весь поисковый запрос, но и похожие на него по смыслу.

4. Поиск по техническим параметрам документа – имени пользователя, который его отправил, дате перехвата, методу передачи и т.д.

Кроме этого для обнаружения конфиденциальной информации, компонент AlertCenter имеет дополнительные возможности:

1. Использование синонимических рядов при полнотекстовом и фразовом поиске.

2. Расширенный поиск по техническим параметрам документа.

3. Поиск нераспознанных документов (документов из которых не удалось извлечь текст).

3. Сложные запросы – комбинирование нескольких простых запросов для текста, атрибутов и нераспознанных документов.

4. Запросы с регулярными выражениями – поиск критичной информации по одному или нескольким шаблонам заданного формата.

5. Запросы с цифровыми отпечатками – сравнение всех перехваченных документов с набором контрольных документов. Этот вид поиска предполагает определение группы конфиденциальных документов и снятие с них цифровых отпечатков, по которым в дальнейшем и будет осуществляться поиск. С помощью данного метода можно быстро выявлять в информационных потоках документы, содержащие большие фрагменты текста из документов, относящихся к конфиденциальным. Основным достоинством метода является высокая скорость работы, а к недостаткам можно отнести его неэффективность при внесении в документ значимых изменений и необходимость оперативного создания цифровых отпечатков всех новых документов для возможности их поиска.

При этом, компонент AlertCenter позволяет:

- Настраивать и хранить поисковые запросы, используемые для определения содержащих конфиденциальную информацию документов.

- Настраивать расписание, по которому происходит поиск конфиденциальных документов.

Таким образом, первоначально для выявления утечек конфиденциальной информации в программном комплексе SearchInform следует настроить:

1. Список пользователей, данные которых будут перехватываться системой;

2. Режим индексации перехваченных документов и режим использования индексов;

3. Список пользователей, по перехваченным данным которых будут генерироваться уведомления;

4. Параметры анализа индексов поисковыми клиентами и компонентом AlertCenter.

Примечание: подробная информация о настройках поиска содержится в руководстве аудитора безопасности системы SearchInform, а также в справке клиентов MailSniffer, IMSniffer, HTTPSniffer, PrintSniffer, DeviceSniffer, SkypeSniffer, SoftInform Search, компонента AlertCenter, а также консолей EndpointSniffer, DeviceSniffer, NetworkSniffer Administrator.

Ход выполнения работы

1. Подготовительные работы:

В соответствии с методическими указаниями лабораторной работы №1 запустить виртуальный компьютер с установленным программным комплексом SearchInform. В дальнейшем вся работа выполняется только на этом виртуальном компьютере.

2. Определение списка пользователей, данные которых будут перехватываться системой:

– С помощью ярлыка SearchInform AlertCenter Console в соответствии с рис. 1, 2 запустить сервер AlertCenter и закрыть окно консоли. При необходимости ввести пароль.

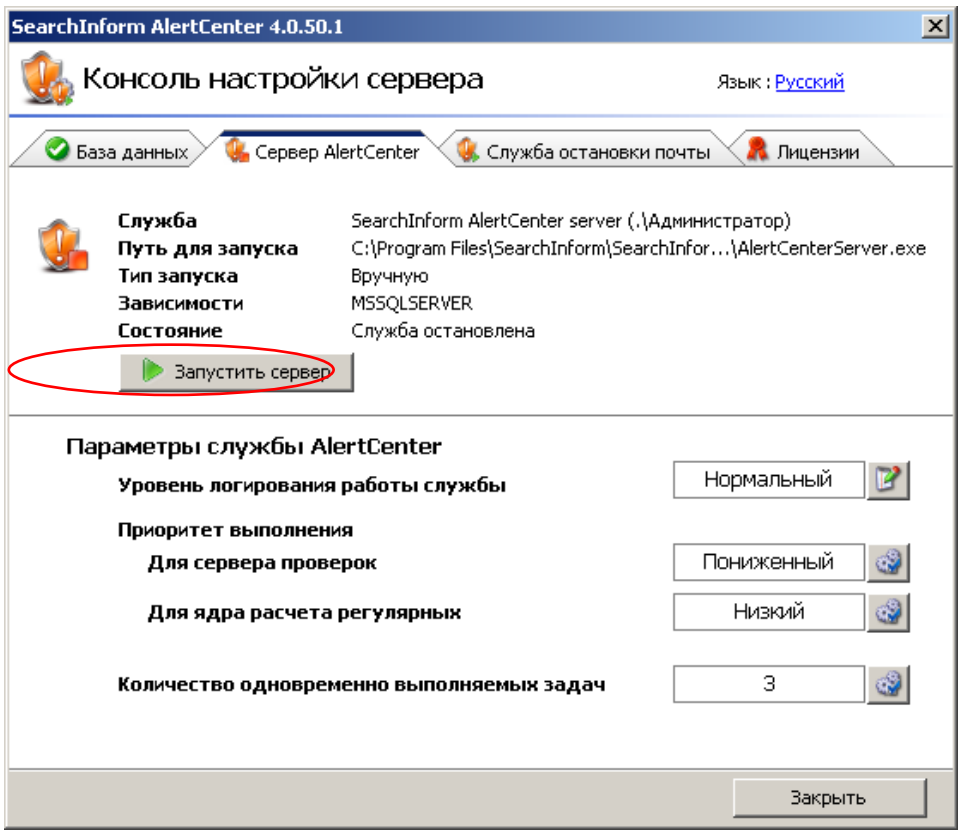

Рис. 1 Запуск сервера AlertCenter

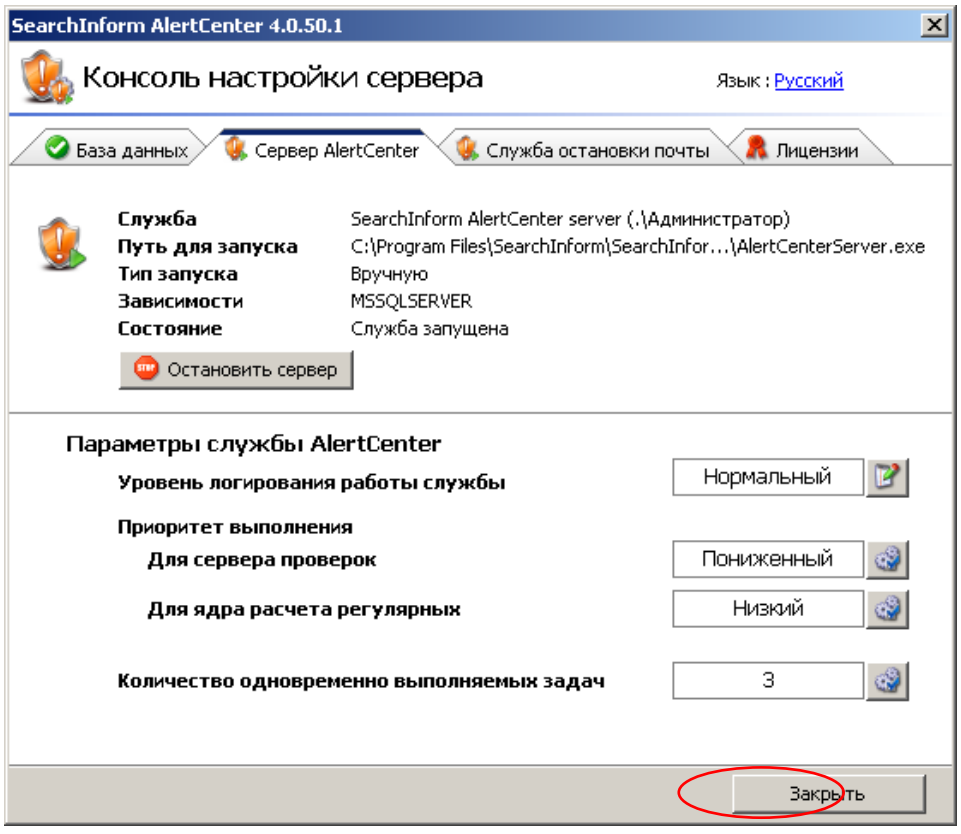

Рис. 2 Индикация функционирования сервера AlertCenter

– С помощью соответствующего ярлыка запустить SearchInform NetworkSniffer Administrator Console, окно которого показано на рис. 3. Отметим, что в процессе запуска может потребоваться ввод парольных данных, установленных в предыдущей лабораторной работе.

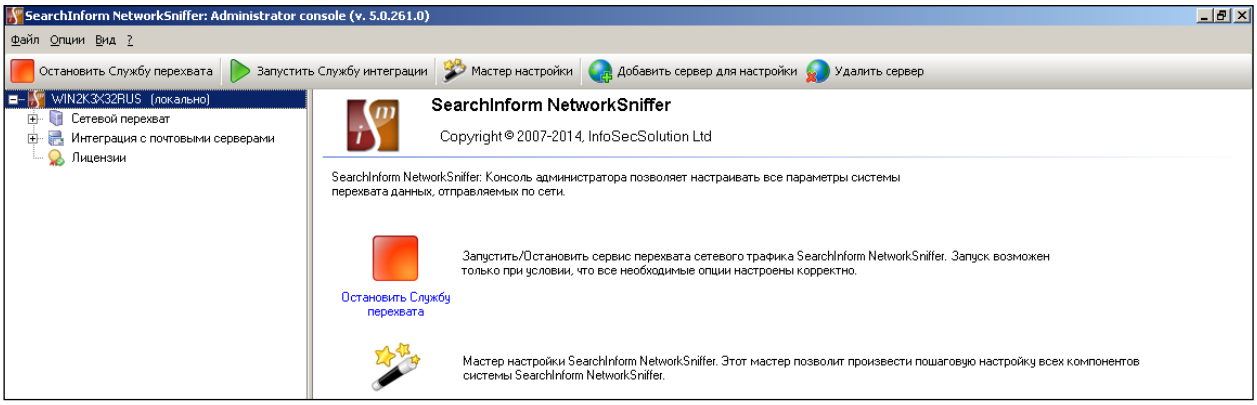

Рис. 3 SearchInform NetworkSniffer Administrator Console

– В соответствии с рис. 4-7 проведем редактирование фильтра перехвата информации. После редактирования будут перехватываться данные пользователей ivanov, bublik и konev для всех контролируемых протоколов.

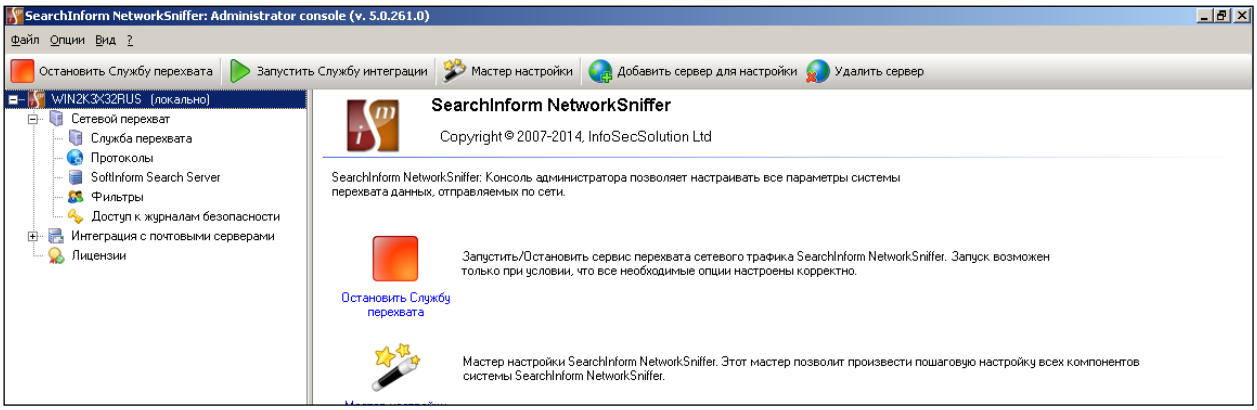

Рис.4 Открытие ветви «Сетевой перхват»

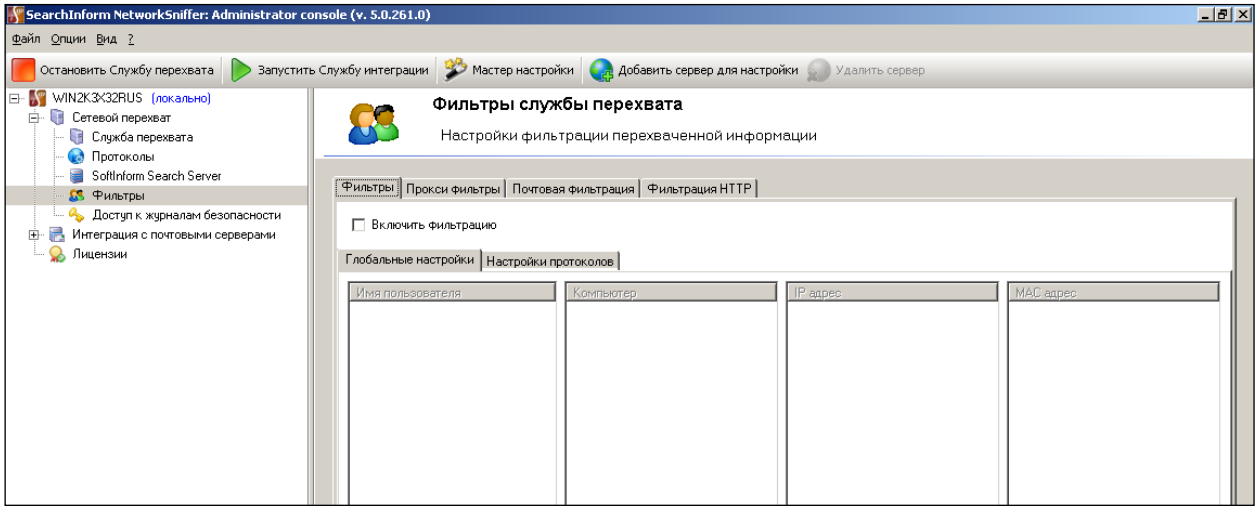

Рис.5 Переход в режим редактирования фильтров для всех контролируемых протоколов

– В соответствии с рис. 6-11 добавить фильтр, разрешающий перехват данных по пользователю ivanov для всех контролируемых протоколов.

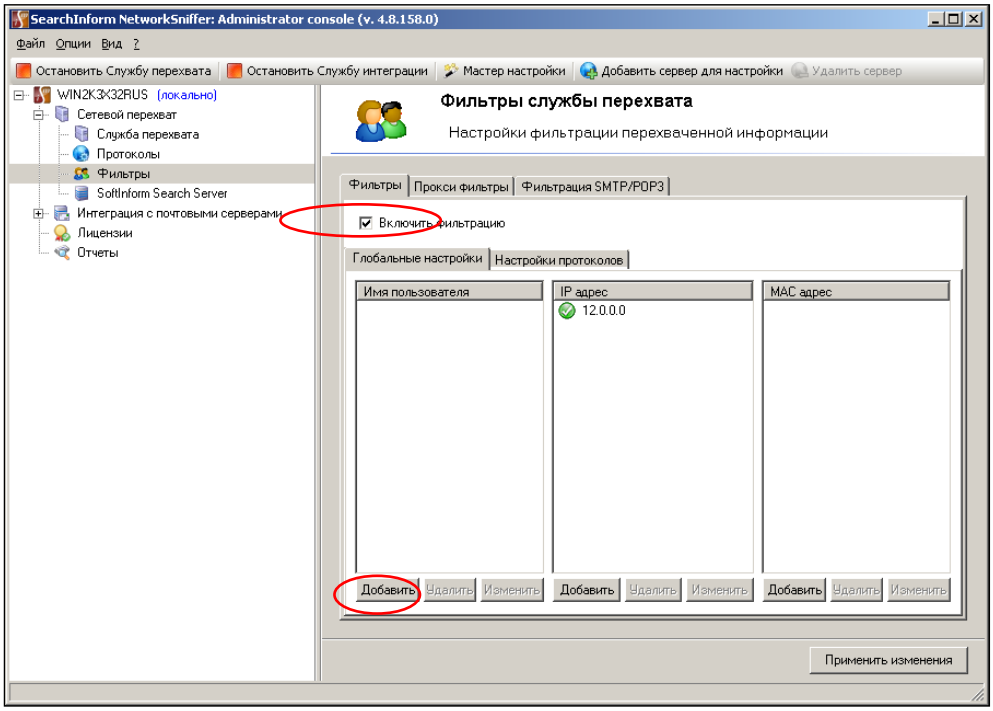

Рис.6 Вход в режим добавления фильтра для всех контролируемых протоколов

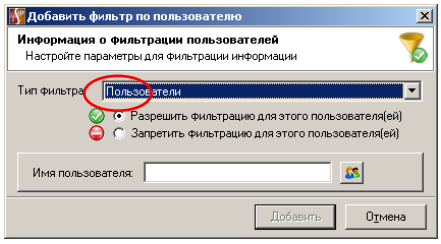

Рис.7 Вход в режим выбора пользователей для разрешающего фильтра

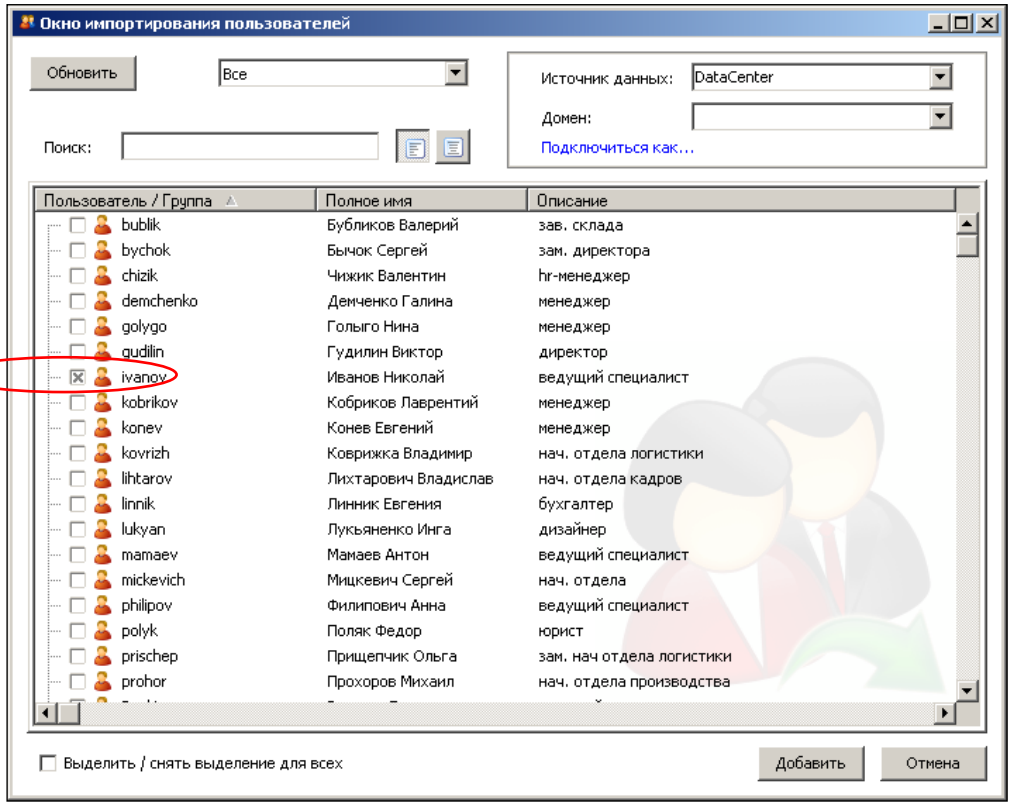

Рис.8 Окно выбора пользователей для фильтра

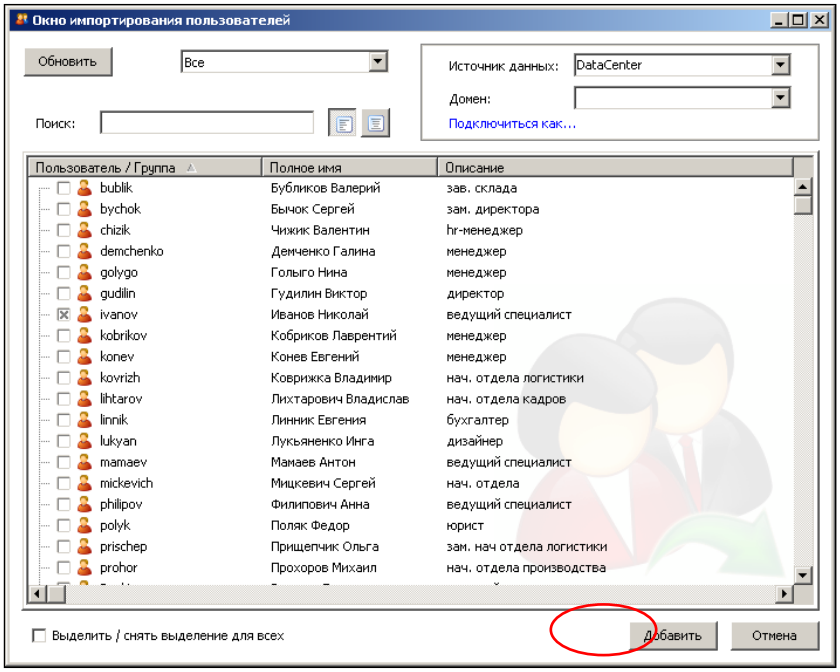

Рис.9 Подтверждение выбора пользователей для фильтрации

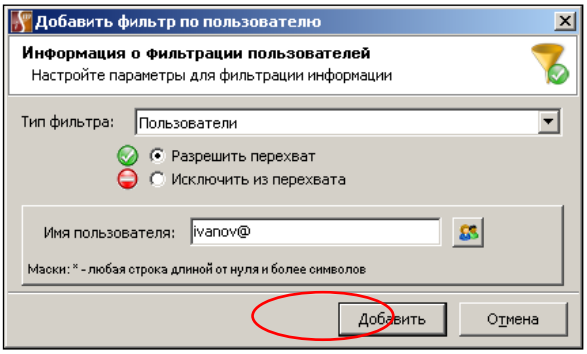

Рис.10 Подтверждение настройки фильтра

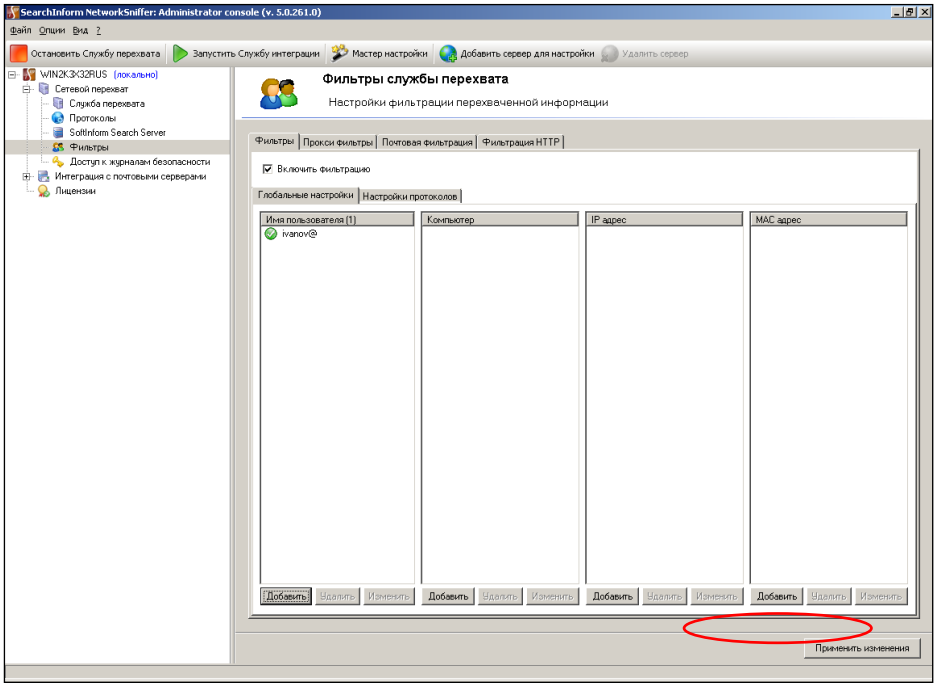

Рис.11 Индикация разрешающих фильтров по пользователям для всех контролируемых протоколов

– По аналогии с добавлением пользователя ivanov, добавить пользователей bublik и konev.

– В соответствии с рис. 12-13 удалить фильтр, разрешающий перехват данных пользователя konev для всех контролируемых протоколов.

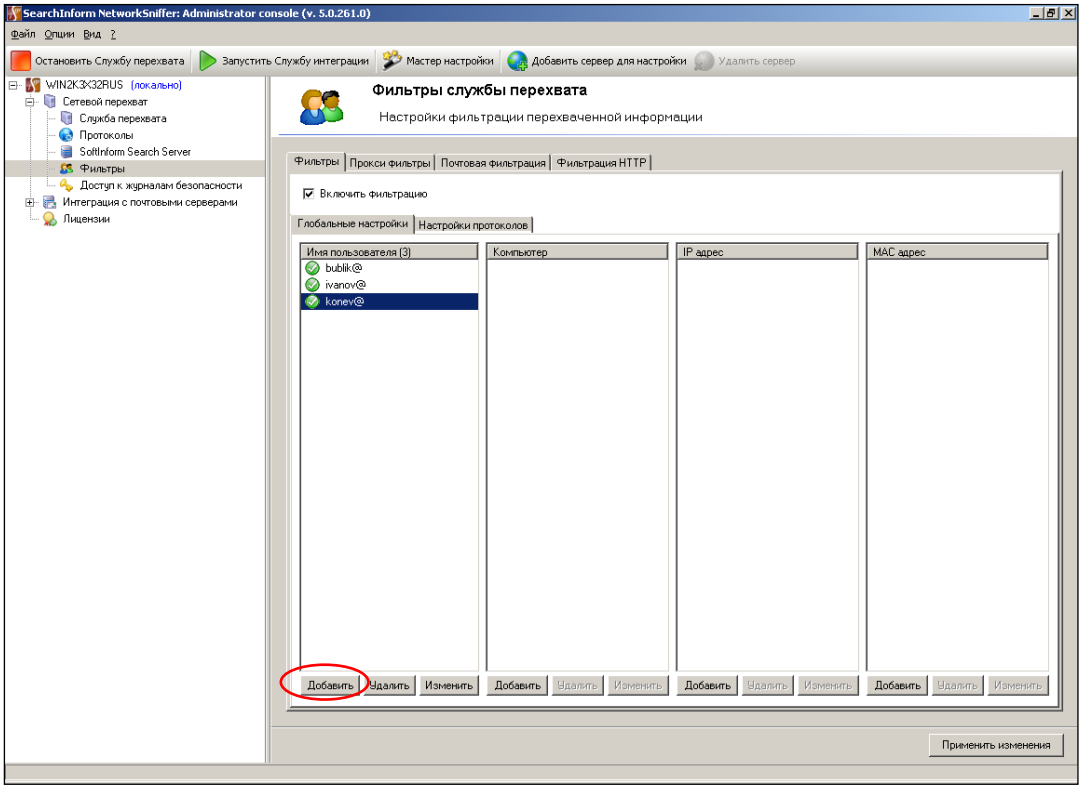

Рис.12 Удаление разрешающего фильтра по пользователю konev для всех контролируемых протоколов

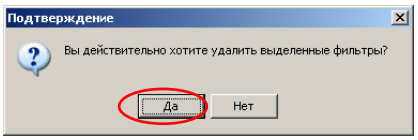

Рис.13 Подтверждение удаления фильтра

– В соответствии с рис. 14-20 настроить фильтрацию перехватываемых данных по сетевой маске и MAC- адресам для всех контролируемых протоколов. Отметим, что для входа в режим настройки фильтрации по сетевой маске необходимо нажать кнопку «Добавить» в разделе «IP-адрес», а для настройки фильтрации по MAC- адресам – в разделе «MAC-адрес».

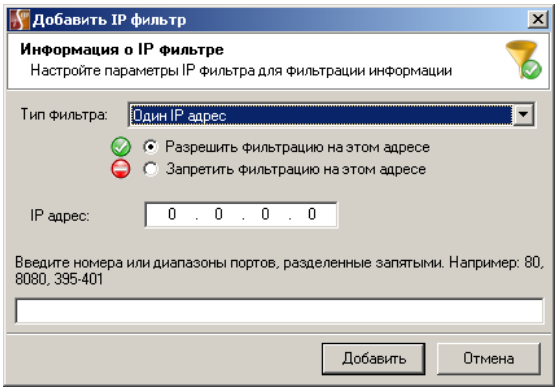

Рис.14 Первый этап добавления разрешающей фильтрации по параметрам сети

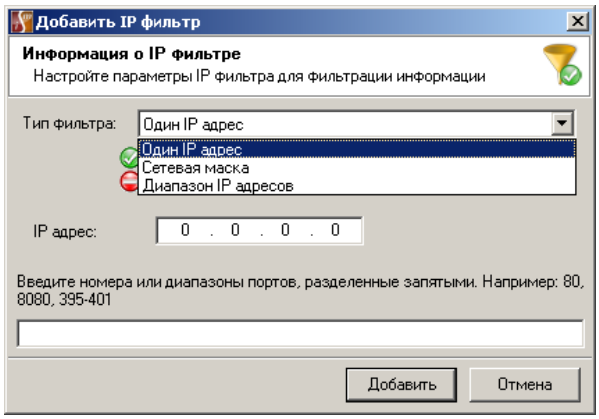

Рис.15 Выбор опции «Сетевая маска»

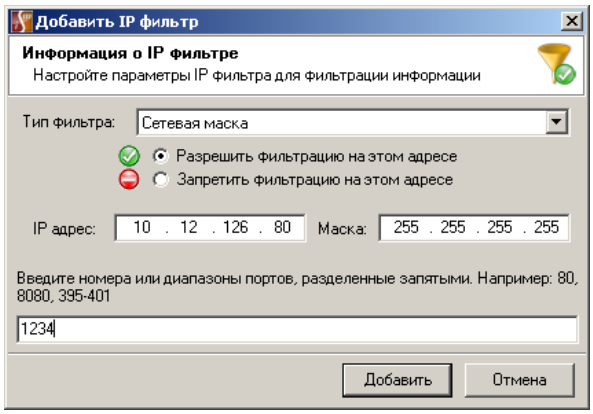

Рис.16 Указание сетевой маски и прослушиваемых портов

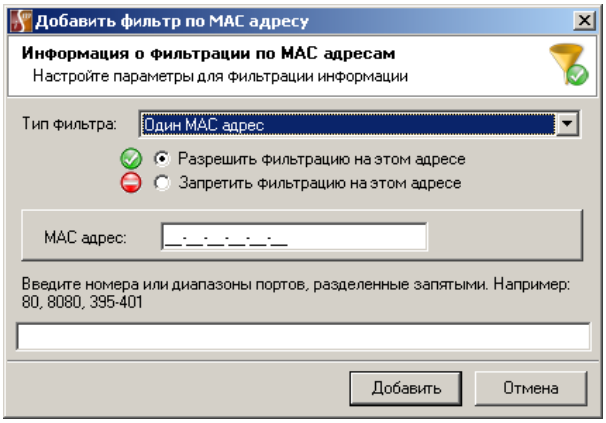

Рис.17 Первый этап добавления разрешающей фильтрации по MAC- адресам

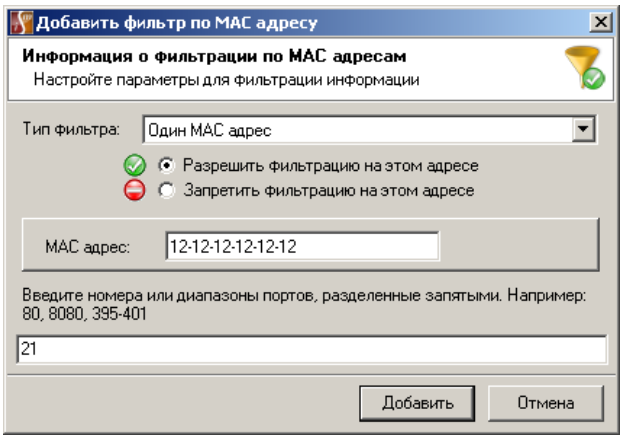

Рис.18 Указание MAC- адреса и прослушиваемых портов

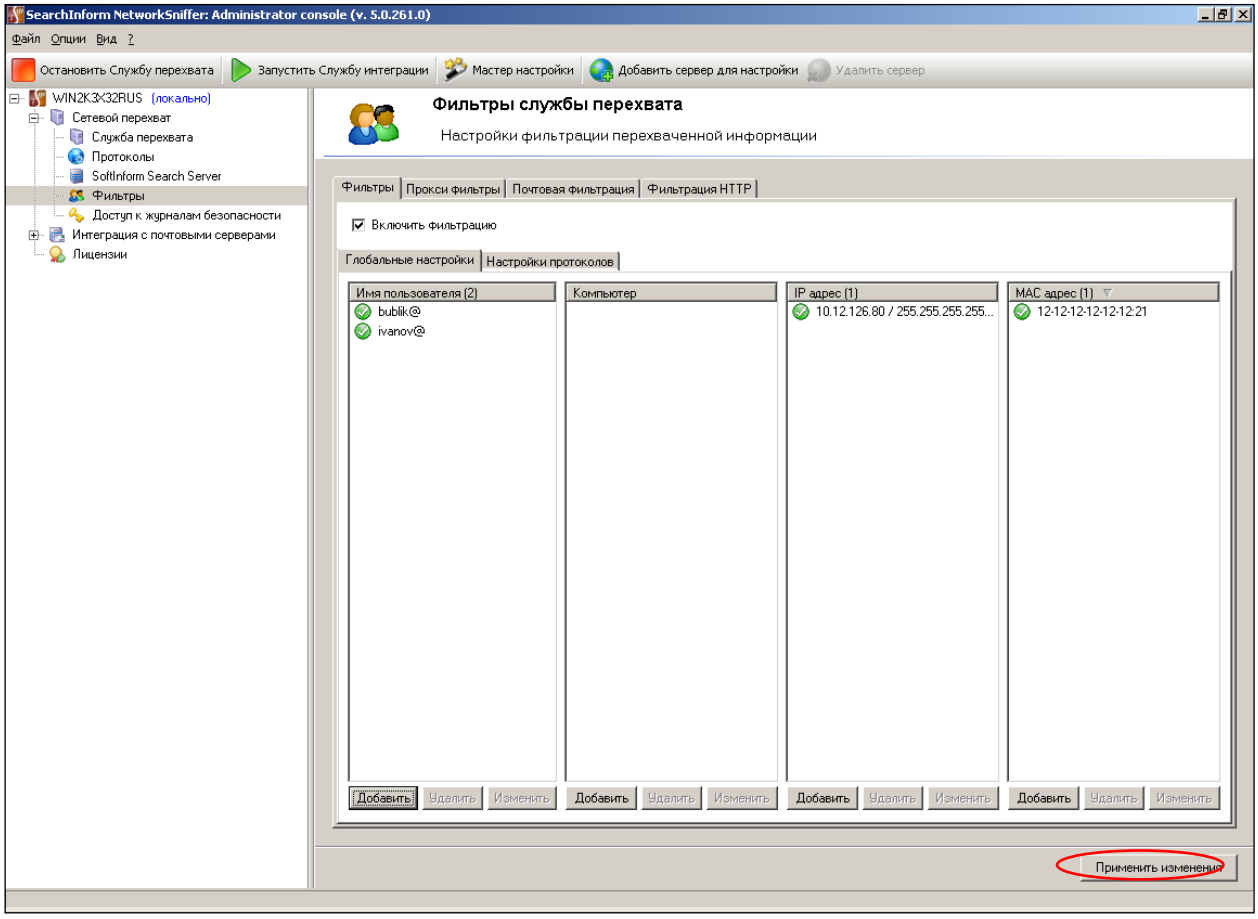

Рис.19Подтверждение добавления фильтров по IP-адресам и MAC- адресам для всех контролируемых протоколов

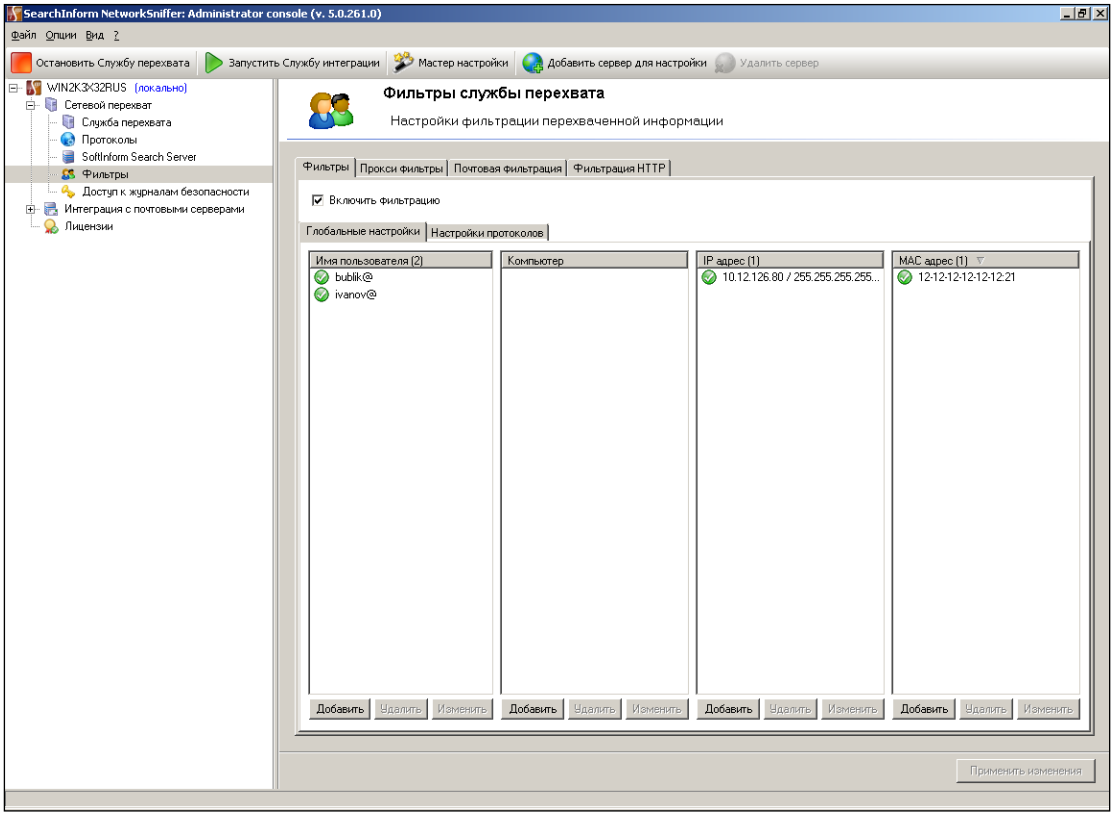

Рис.20 Индикация фильтров для всех контролируемых протоколов

– В соответствии с рис. 21 настроить фильтр, запрещающий перехват данных по протоколу HTTP для пользователя ivanov.

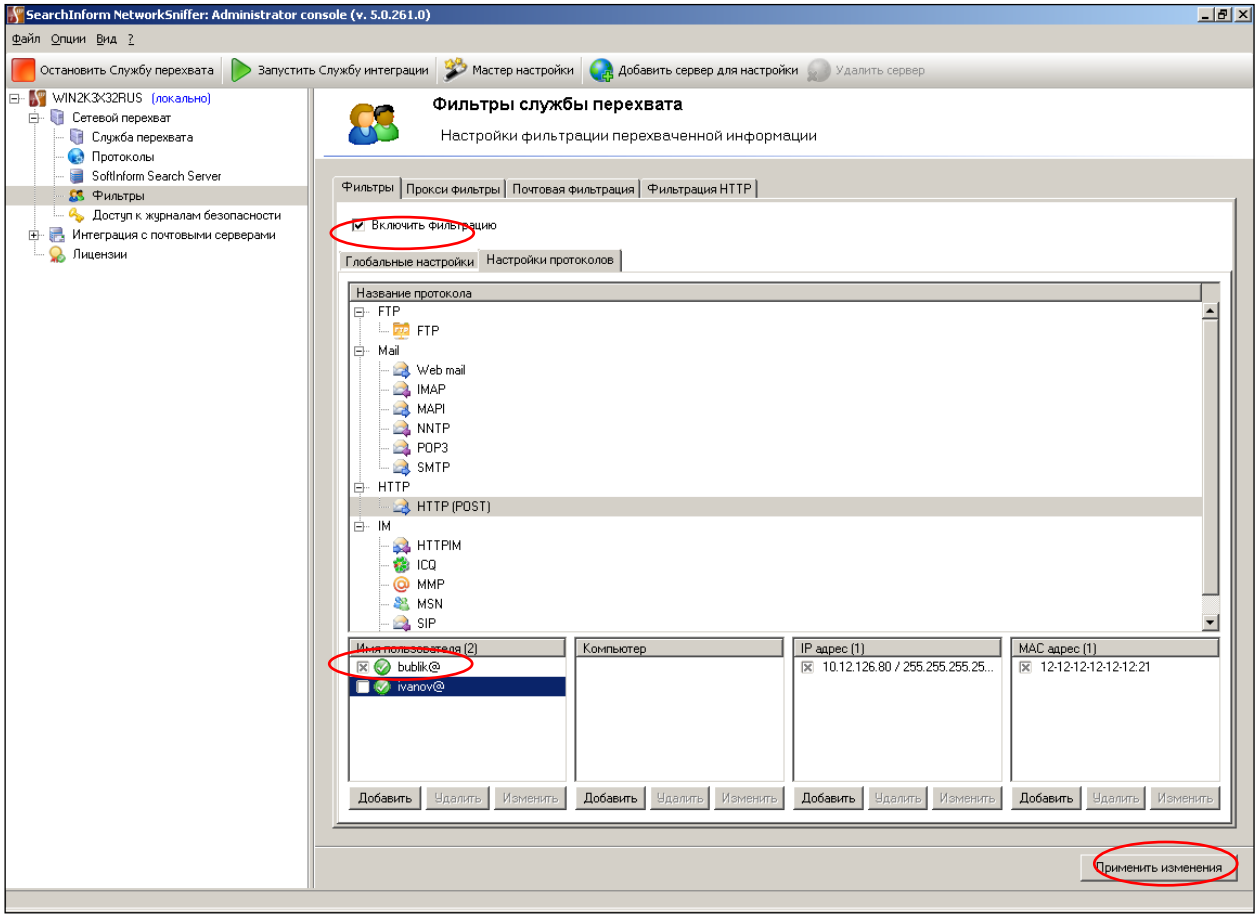

Рис.21 Отмена разрешающего фильтра по протоколу HTTP для пользователя ivanov

– В соответствии с рис. 22-26 настроить фильтр, разрешающий перехват данных по протоколу POP3 для пользователя polyk.

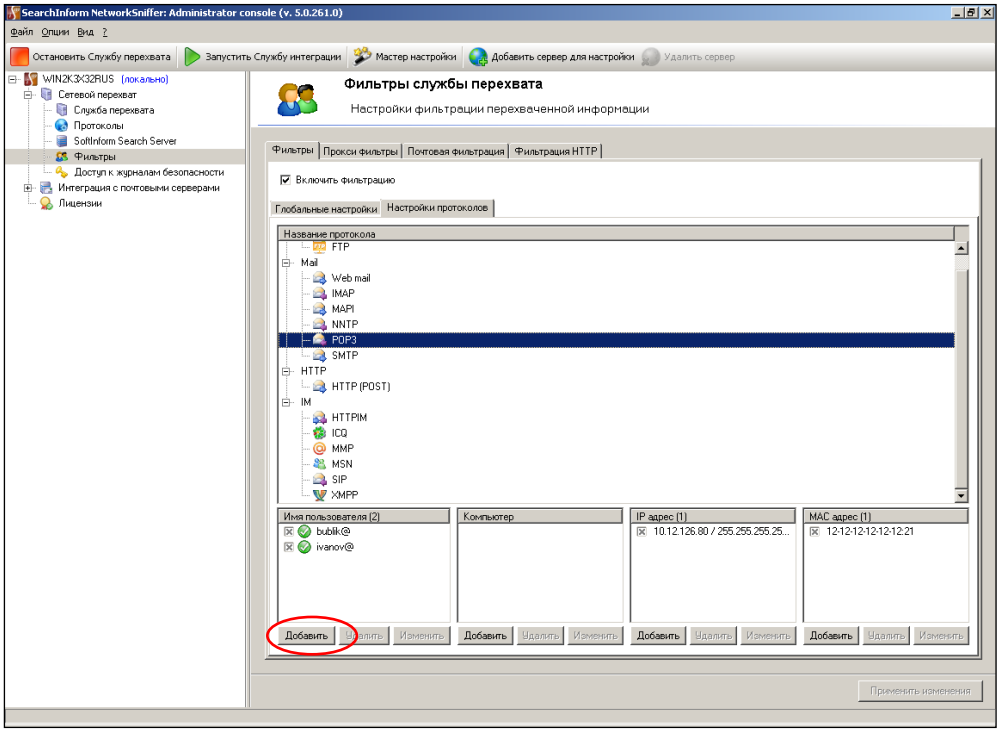

Рис.22 Вход в режим добавления нового фильтра пользователей по протоколу HTTP

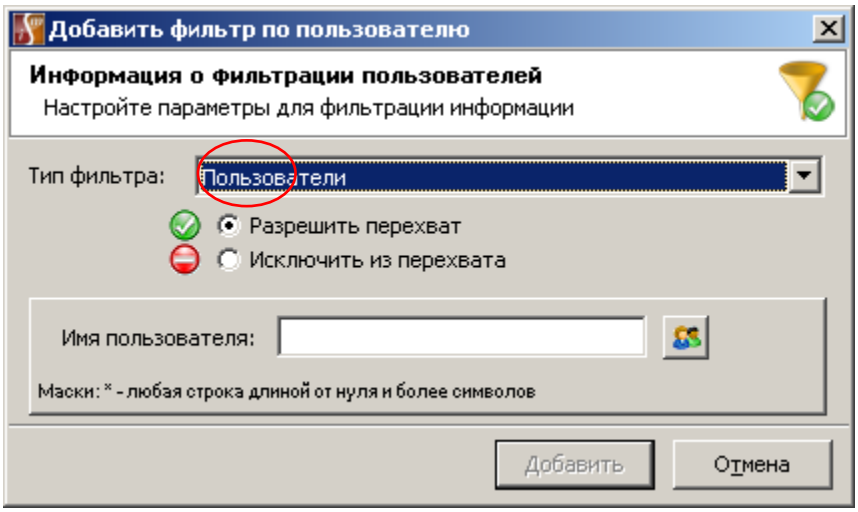

Рис.23 Вход в режим выбора пользователей

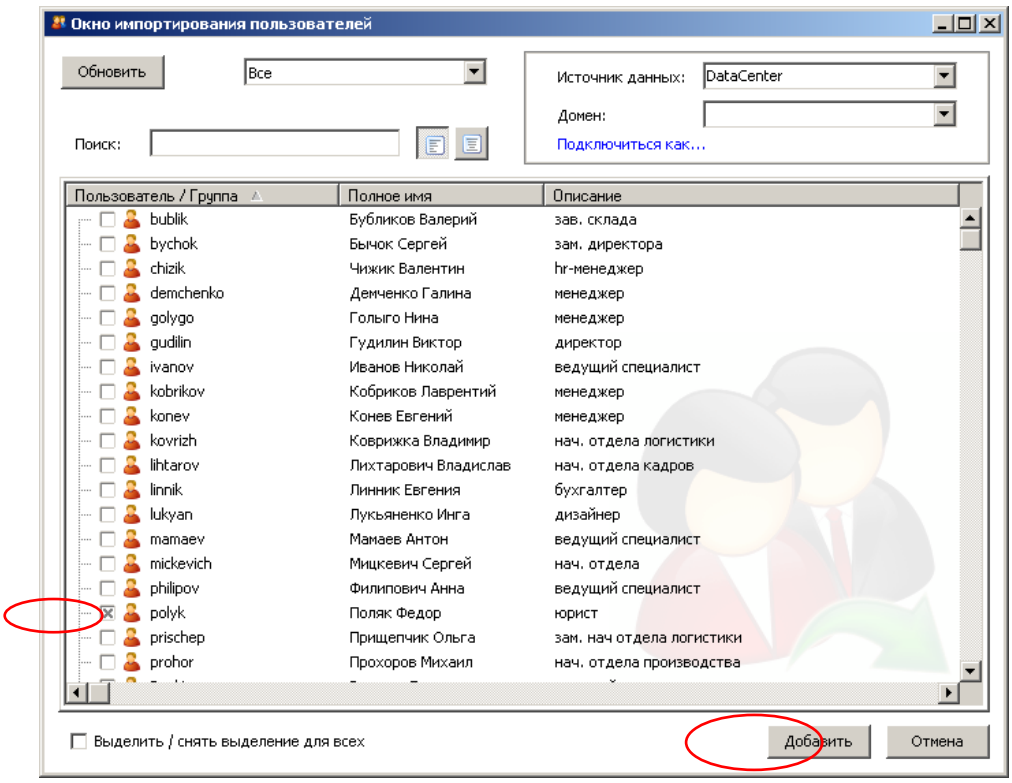

Рис.24 Выбор пользователя polyk

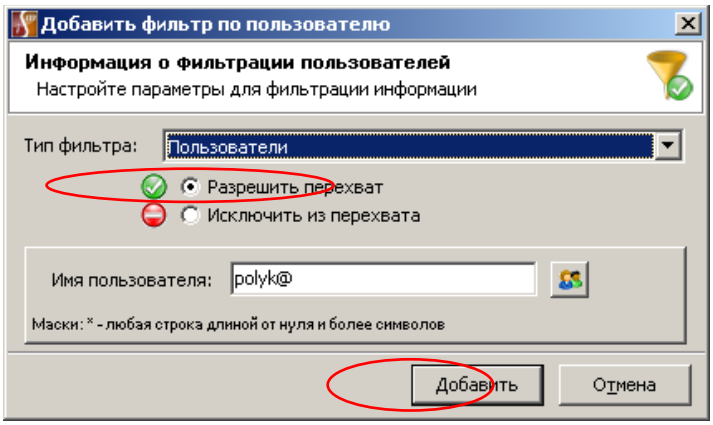

Рис.25 Выбор разрешающего фильтра

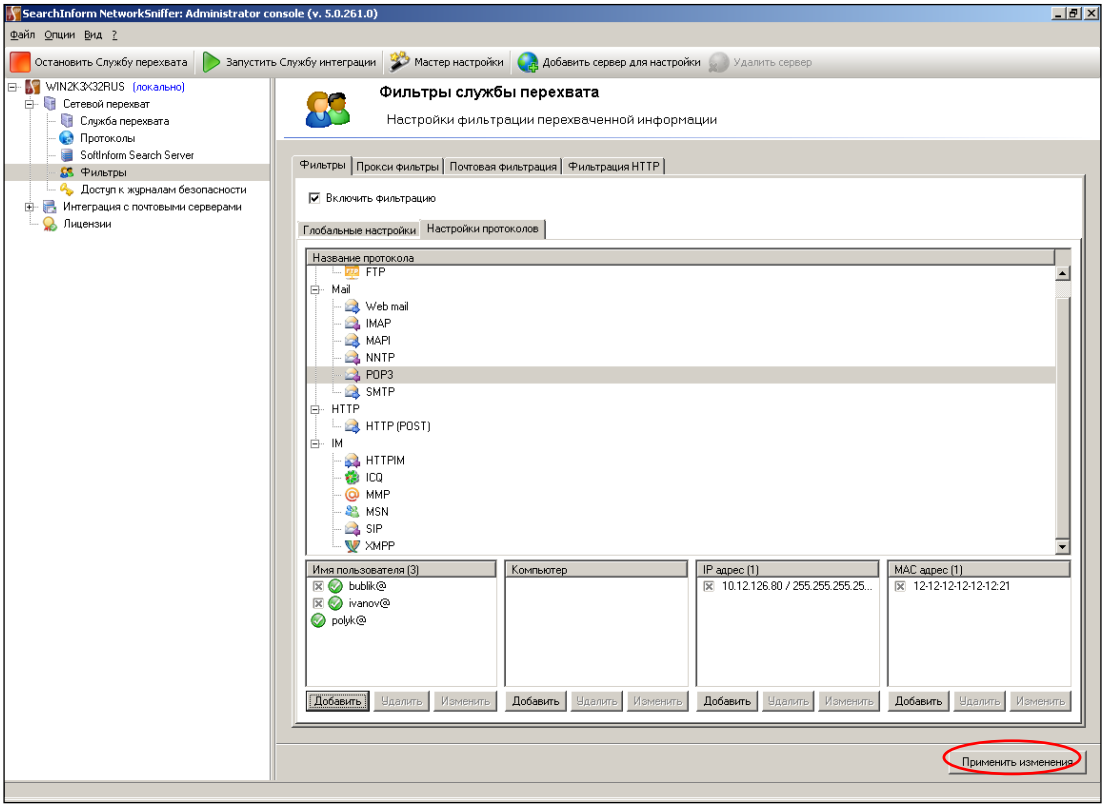

Рис.26 Подтверждение добавления нового разрешающего фильтра

– В соответствии с рис. 27-31 настроить прокси-фильтр.

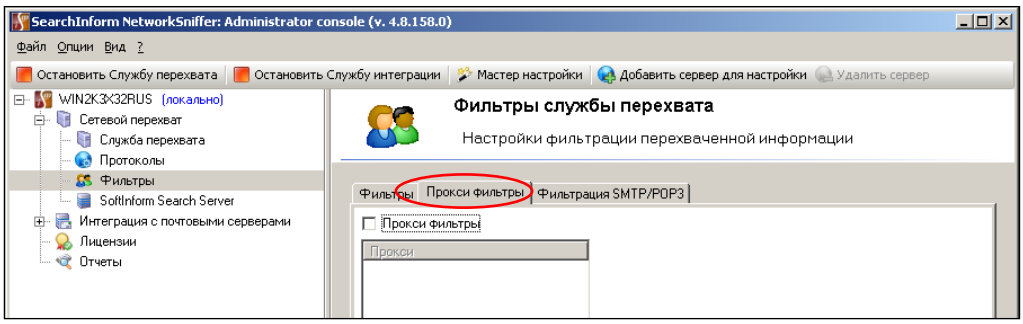

Рис.27 Переход к настройкам фильтрации по прокси-серверам

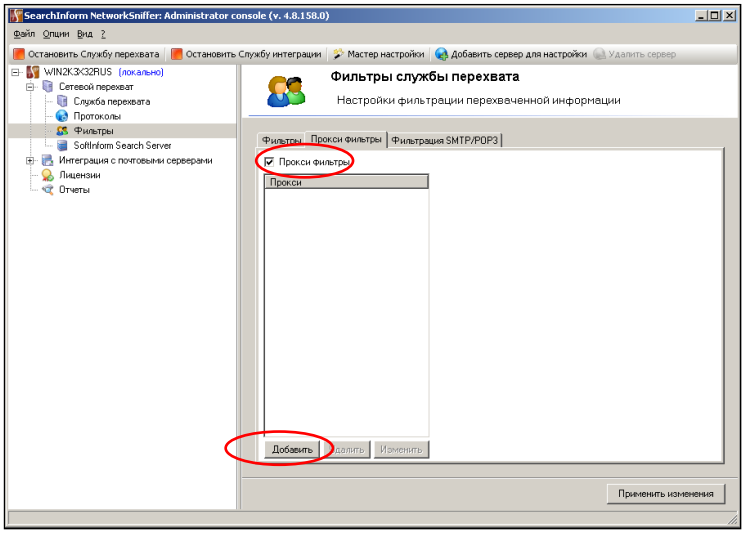

Рис.28 Первый этап добавление прокси фильтра

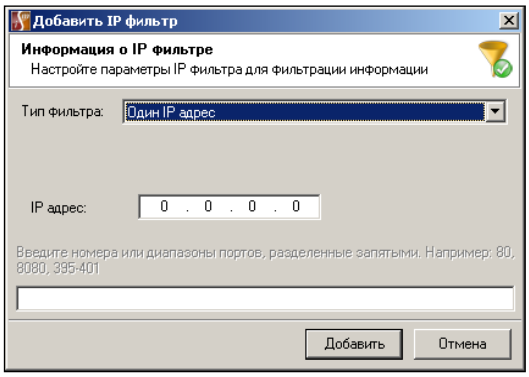

Рис.29 Окно ввода параметров прокси-сервера

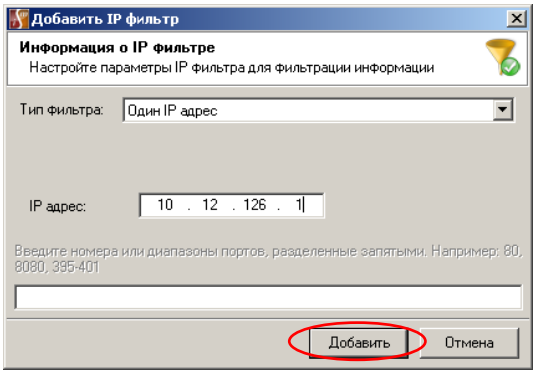

Рис.30 Добавление параметров прокси-сервера

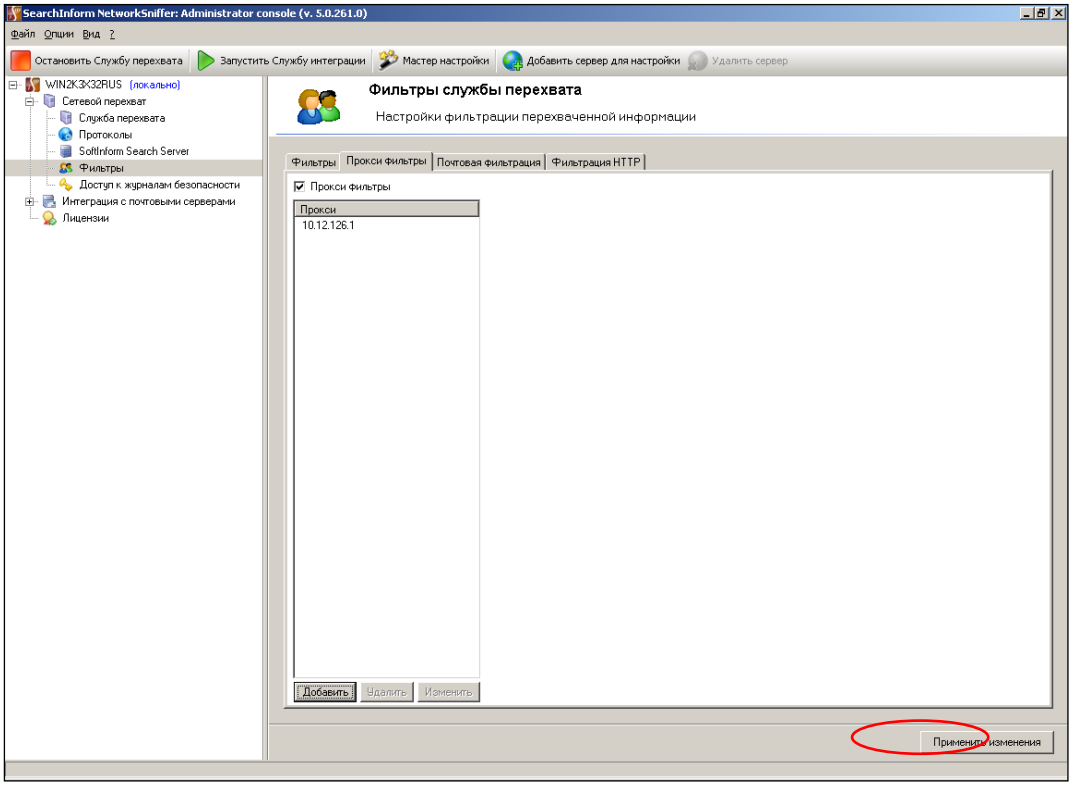

Рис.31 Подтверждение параметров прокси-сервера

– В соответствии с рис. 32-34 удалить прокси-фильтр.

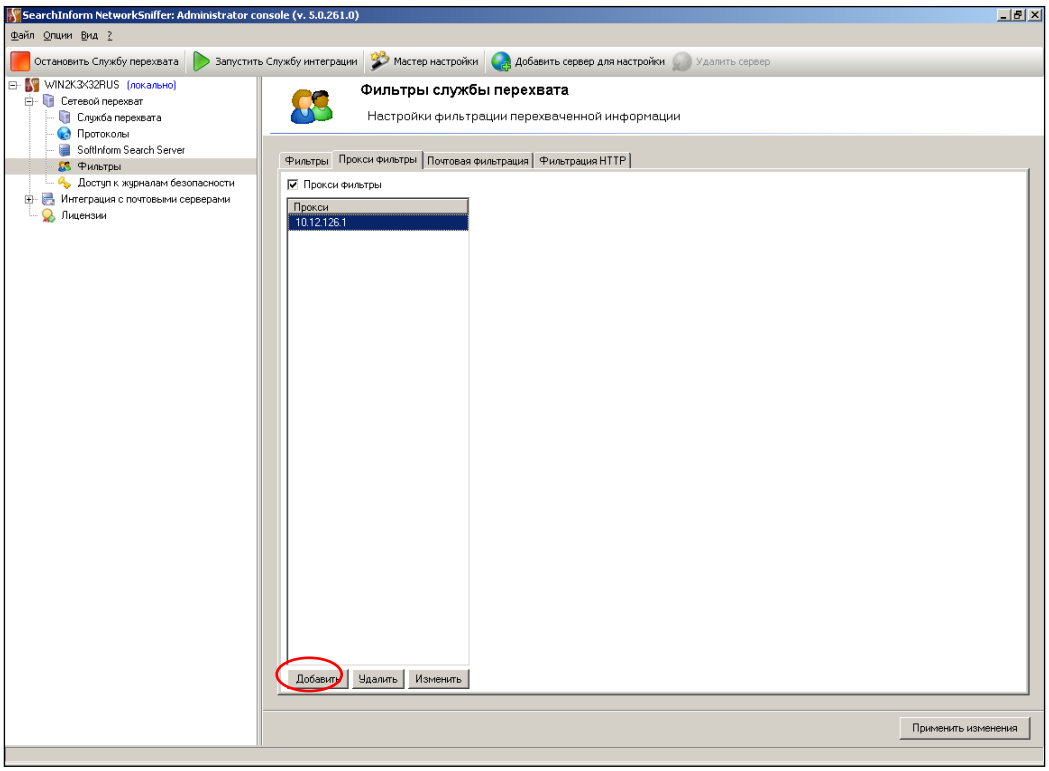

Рис.32Выбор прокси-фильтра для удаления

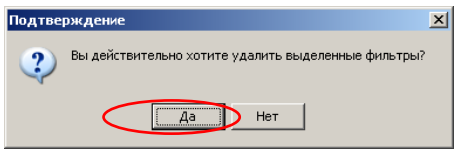

Рис.33 Подтверждение удаления фильтра

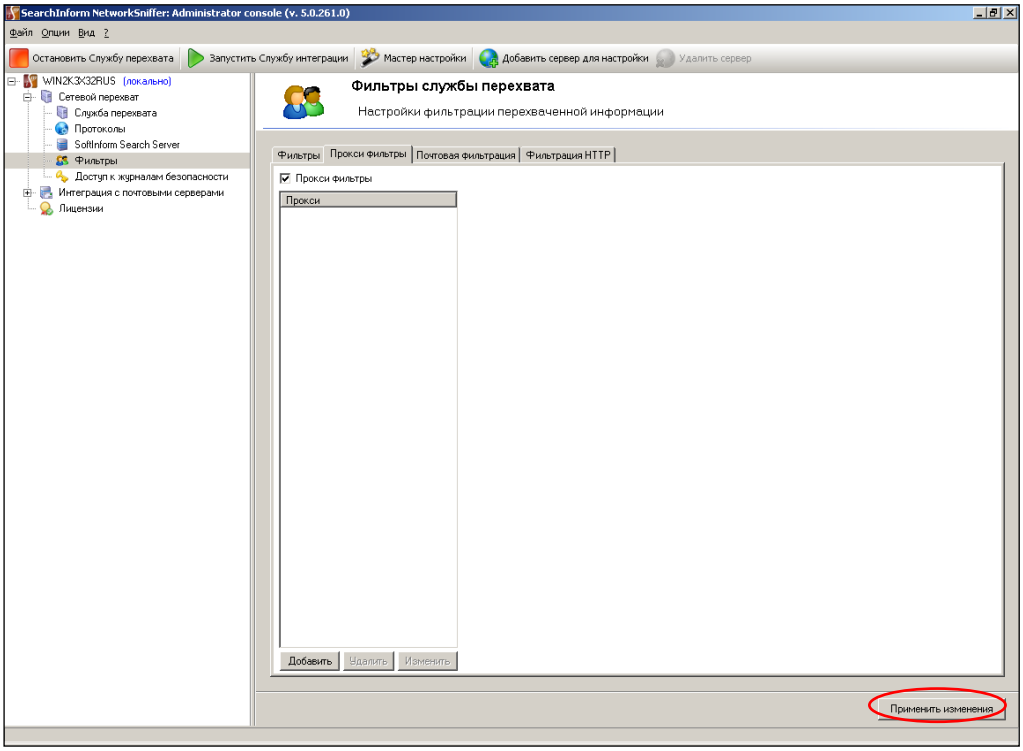

Рис.34 Подтверждение настроек по удалению фильтра

– В соответствии с рис. 34-38создать фильтр по почтовым адресам для сообщений больше 10000 байт.

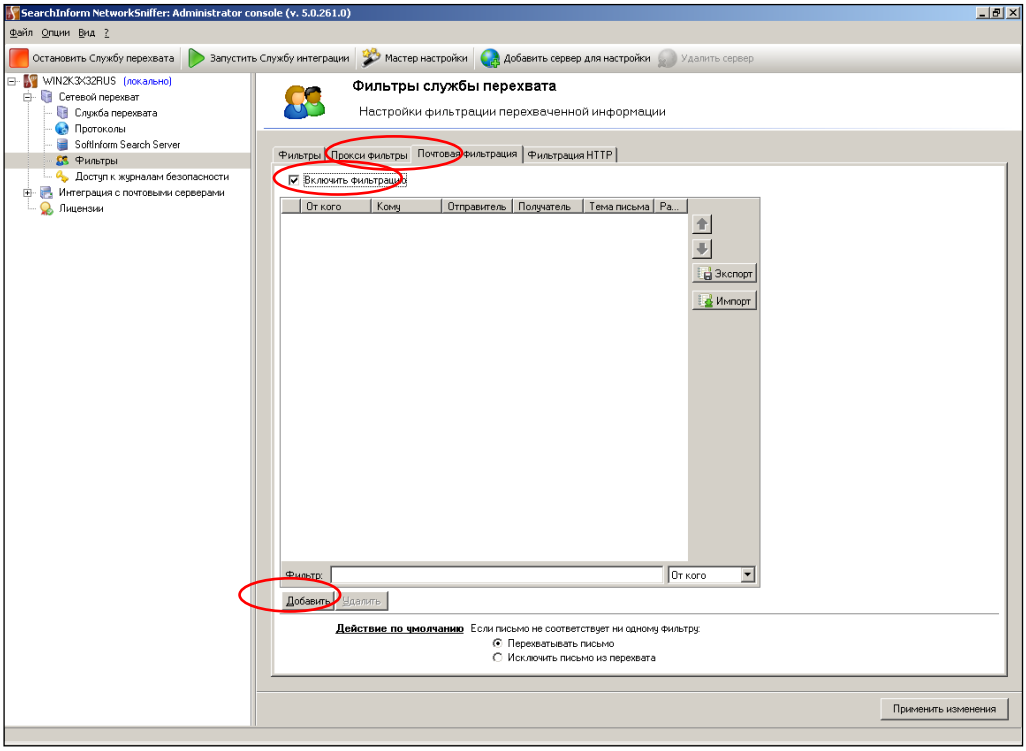

Рис.35 Вход в режим добавления фильтра по почтовым адресам

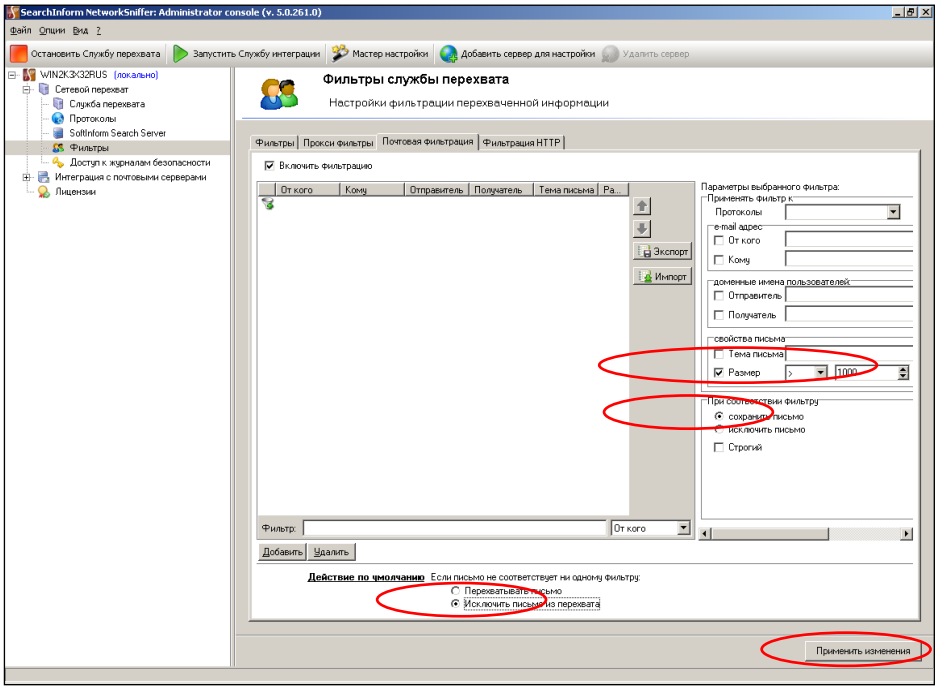

Рис.36 Установка размера сообщения

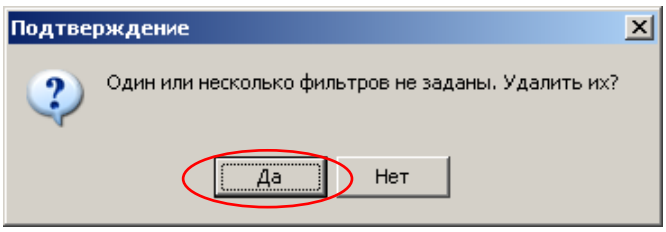

Рис.37 Окно подтверждения настройки

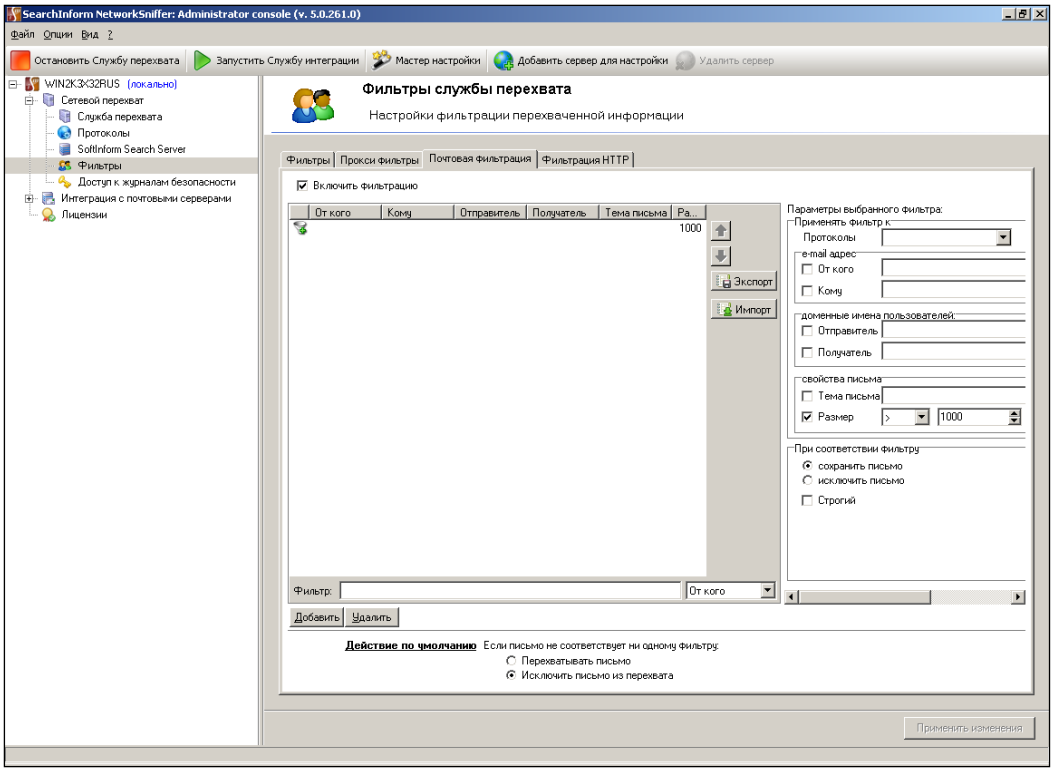

Рис.38 Индикация установленного фильтра по почтовым адресам

– В соответствии с рис. 39-45 указать соответствие пользователя 123 почтовому адресу 123@ukr.net.

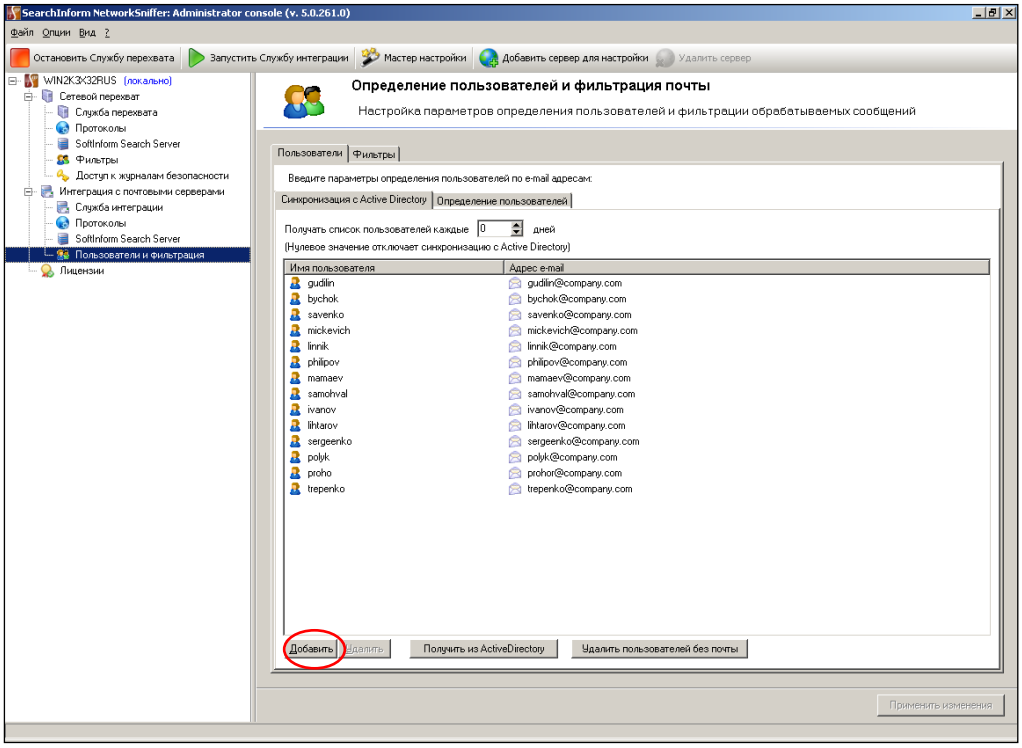

Рис.39 Добавление адреса

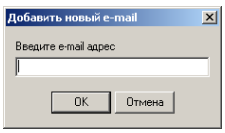

Рис.40 Ввод адреса

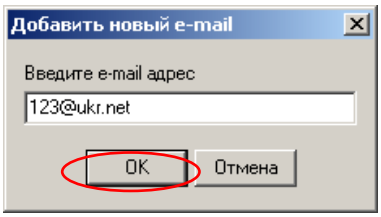

Рис.41 Подтверждение введенного адреса

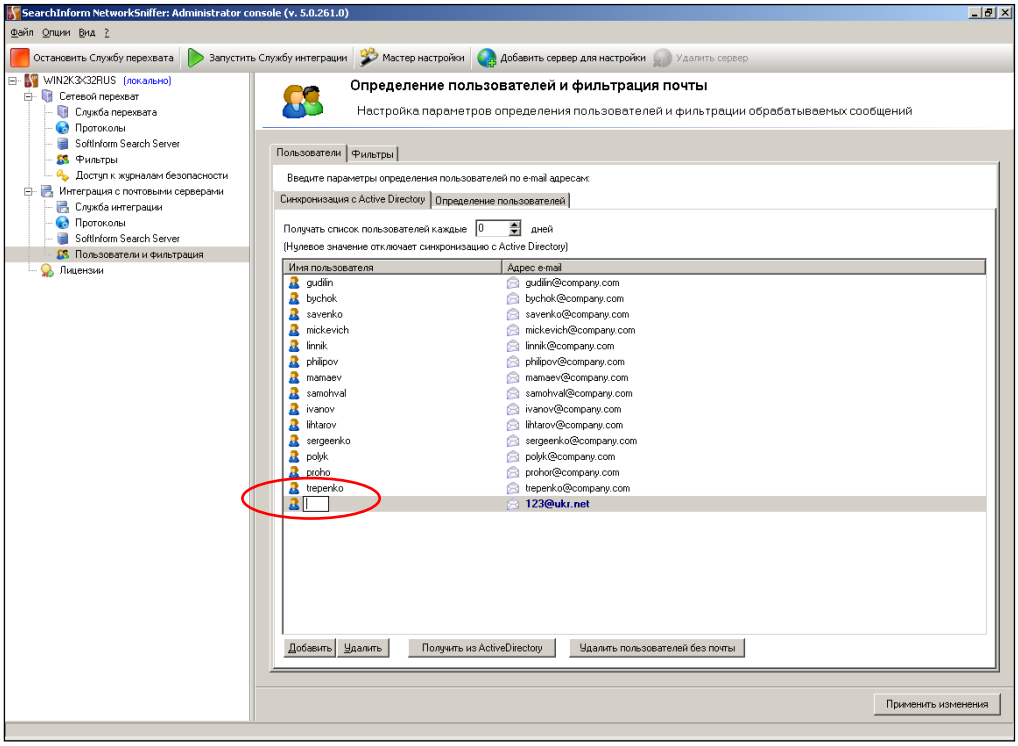

Рис.42Поле ввода имени пользователя

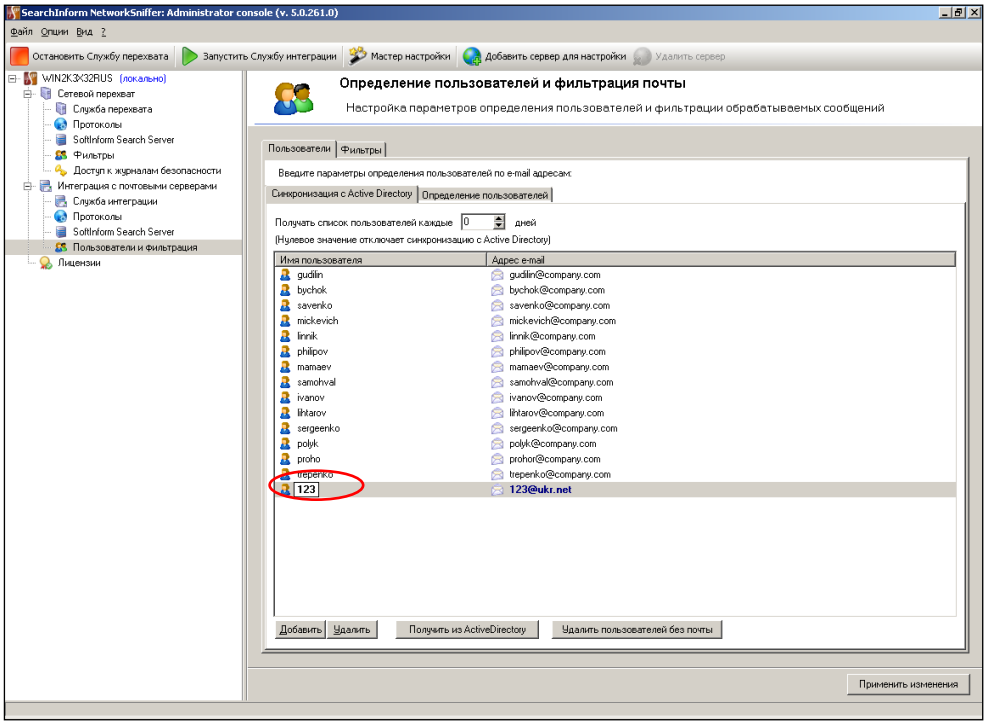

Рис.43 Ввод имени пользователя

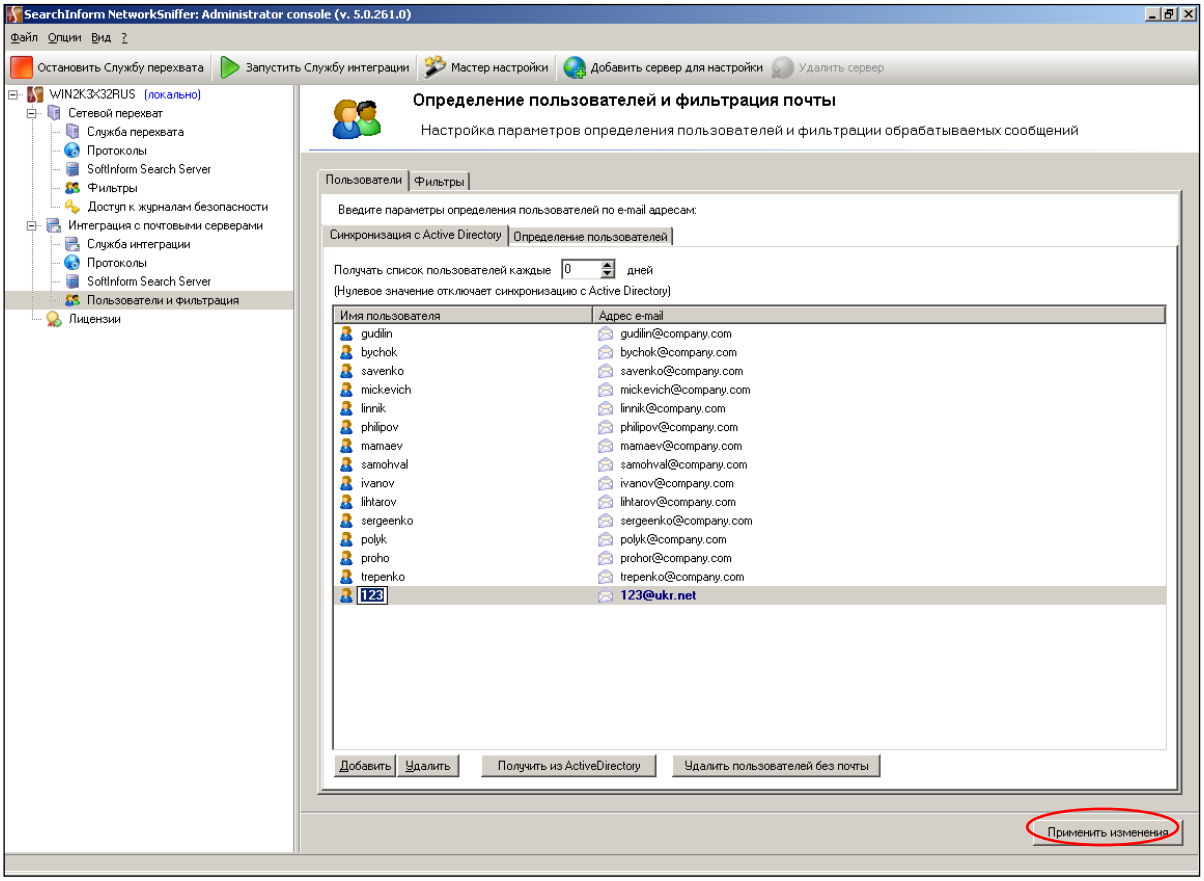

Рис.44 Подтверждение соответствия адреса пользователю

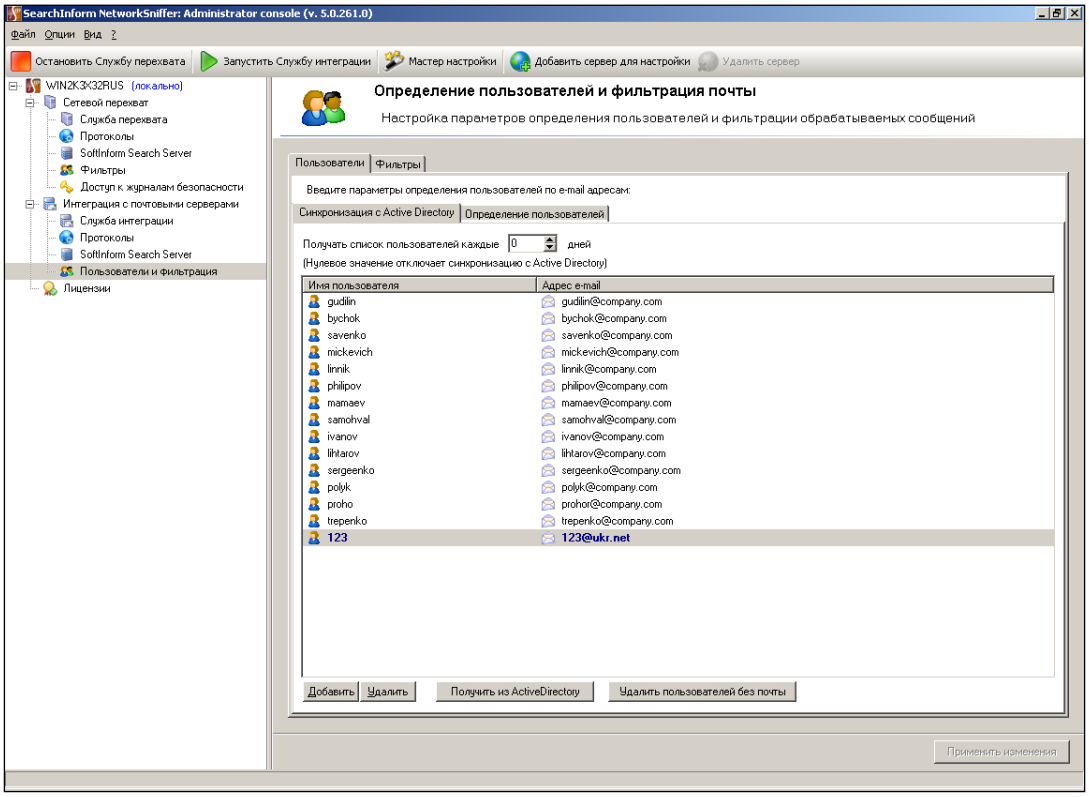

Рис.45 Индикация установленного соответствия

– В соответствии с рис. 46-49 создать список определения масок почтовых адресов пользователей.

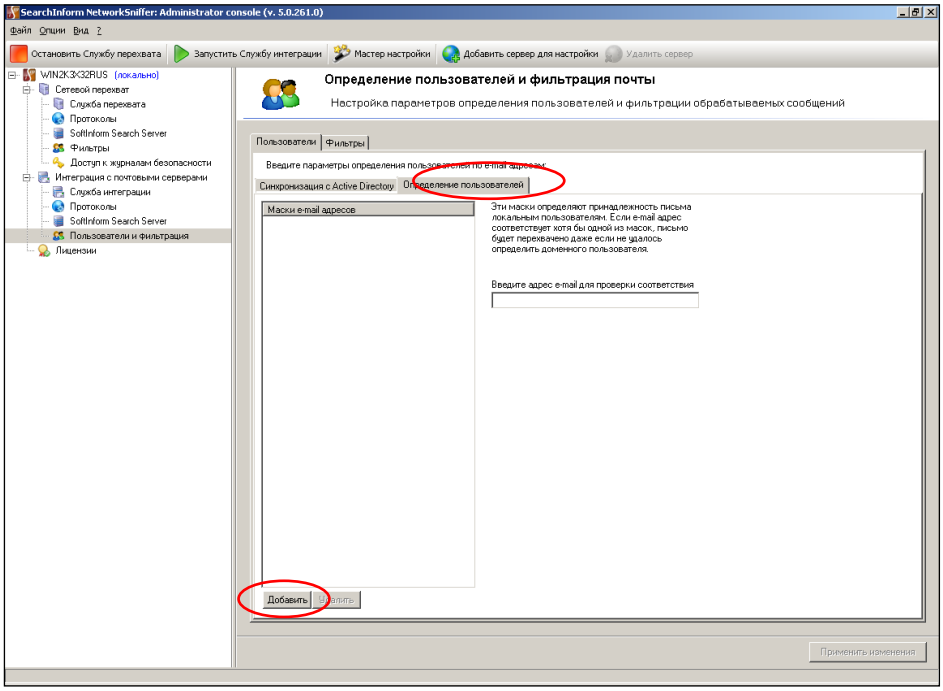

Рис.46 Добавление маски

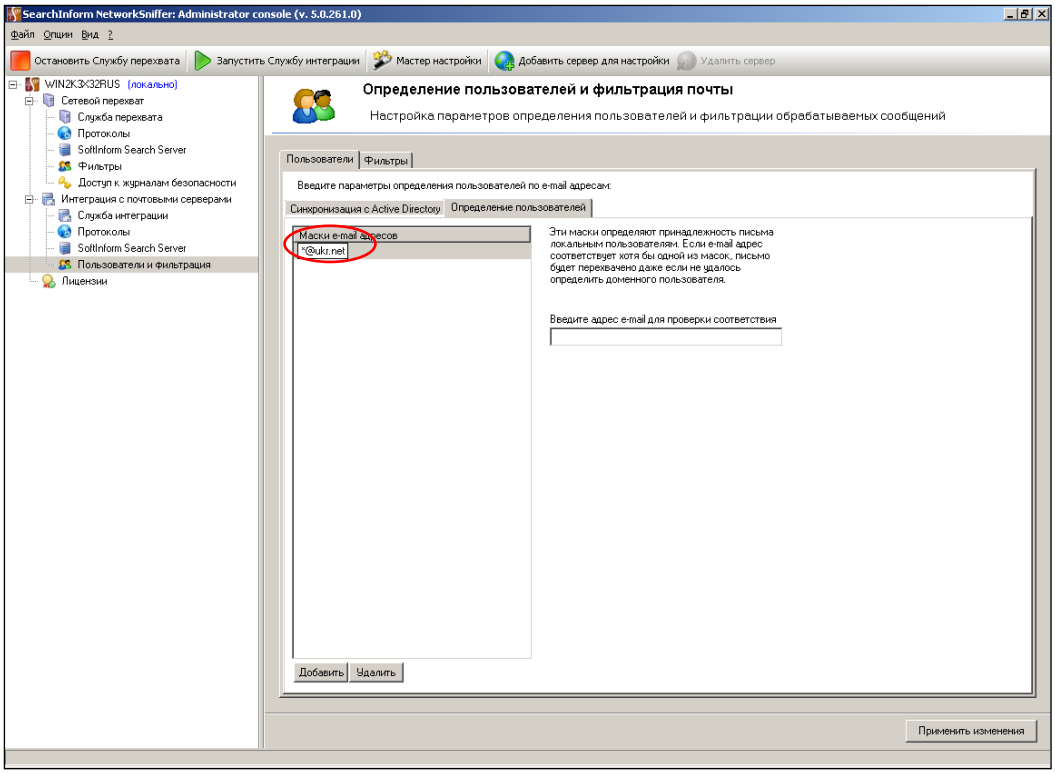

Рис.47 Ввод маски *@ukr.net

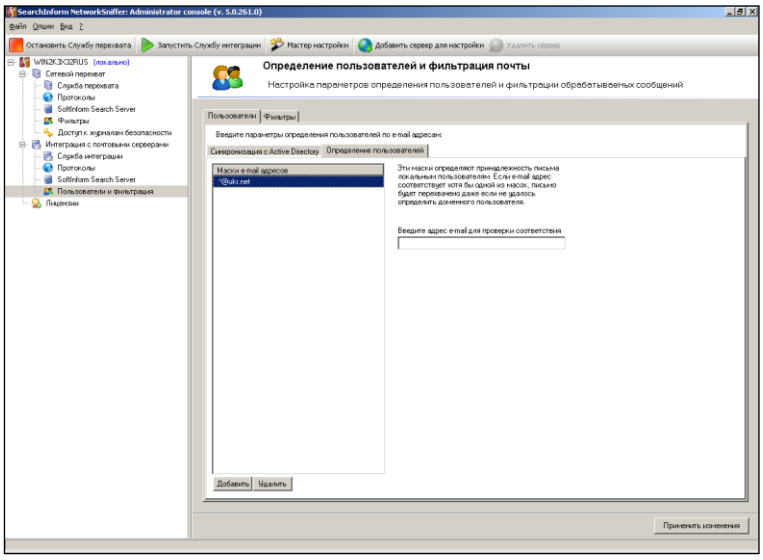

Рис.48 Индикация введенной маски

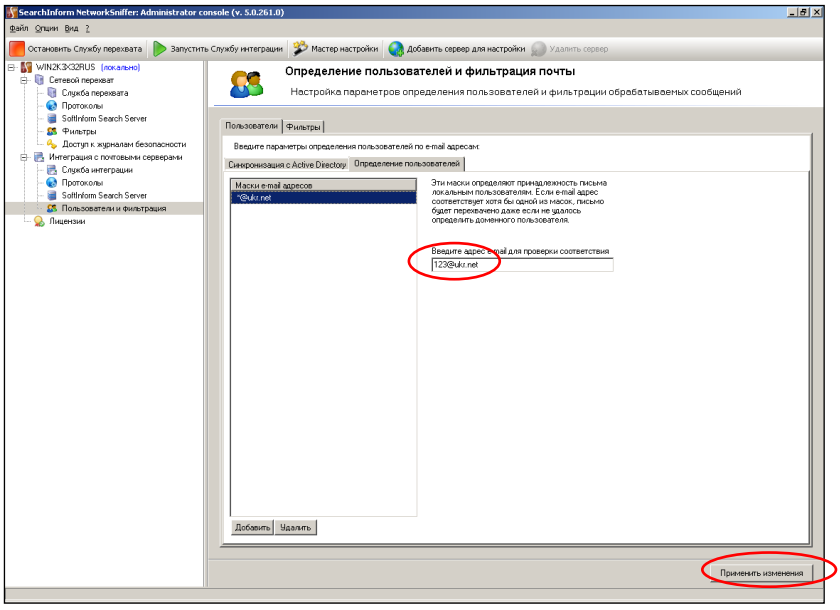

Рис.49 Проверка введенной маски и применение исправлений

– В соответствии с рис. 50-52 создать фильтр по почте пользователей, определив поиск наличия в теме письма слова «коррупция».

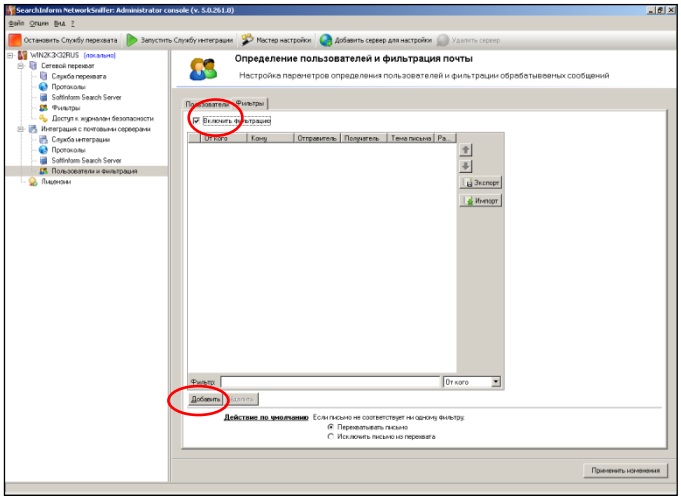

Рис.50 Переход к созданию фильтра

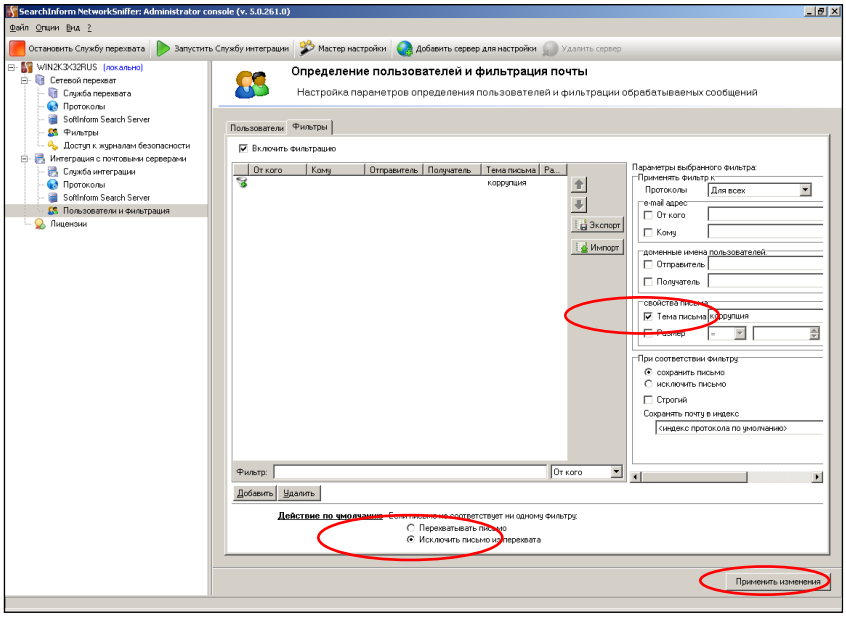

Рис.51 Определение параметров фильтра

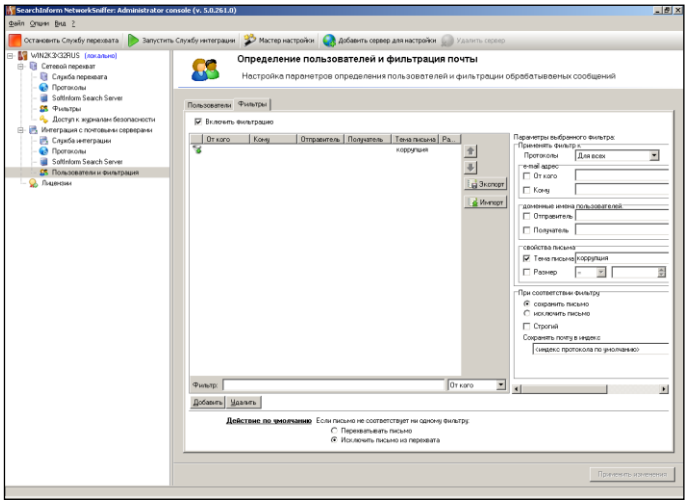

Рис.52 Индикация успешного создания фильтра

– В соответствии с рис. 53-54 создать фильтр по протоколу HTTP, определив поиск наличия в содержимом слова «взятка».

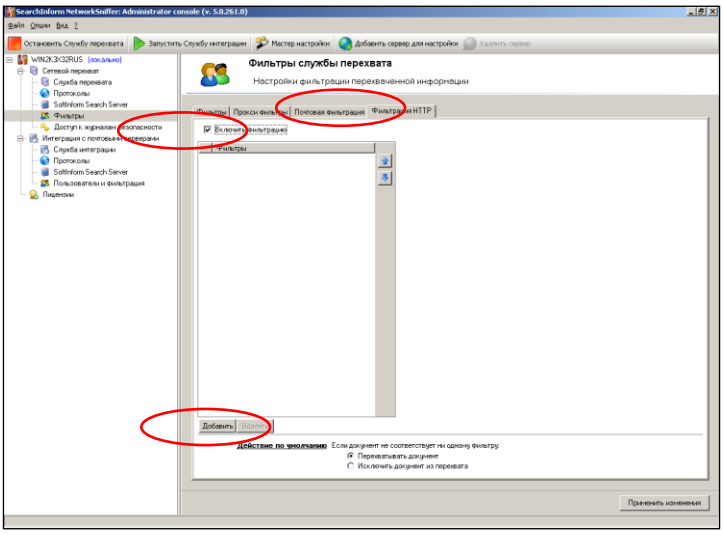

Рис.53 Переход к созданию фильтра

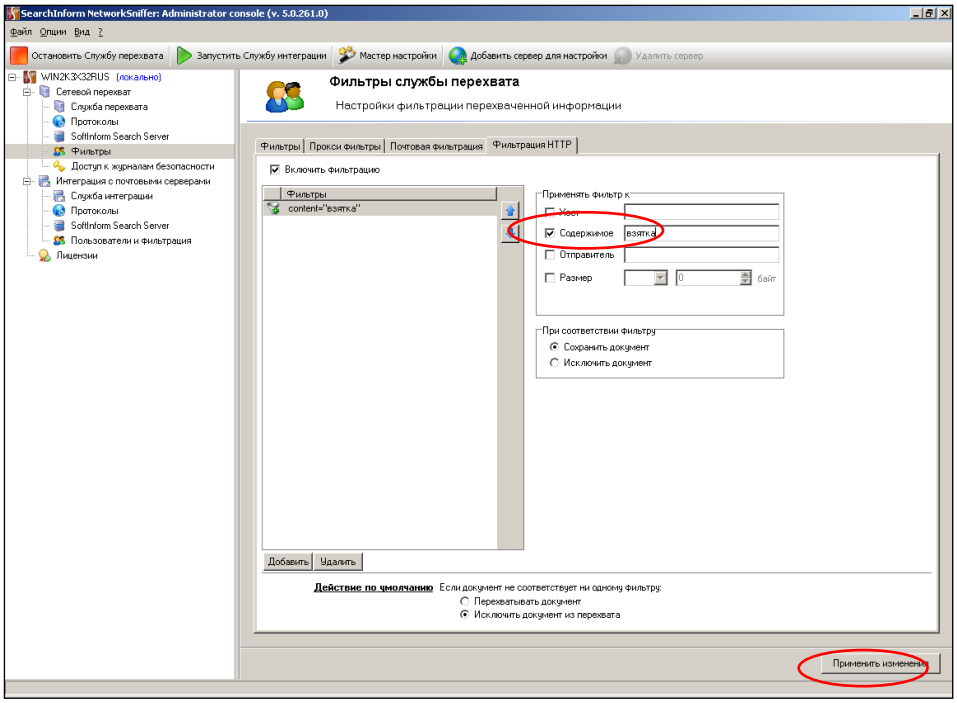

Рис.54Создание фильтра

– Закрыть окно консоли NetworkSniffer Administrator.

– Открыть окно консоли SearchInform EndpointSniffer.

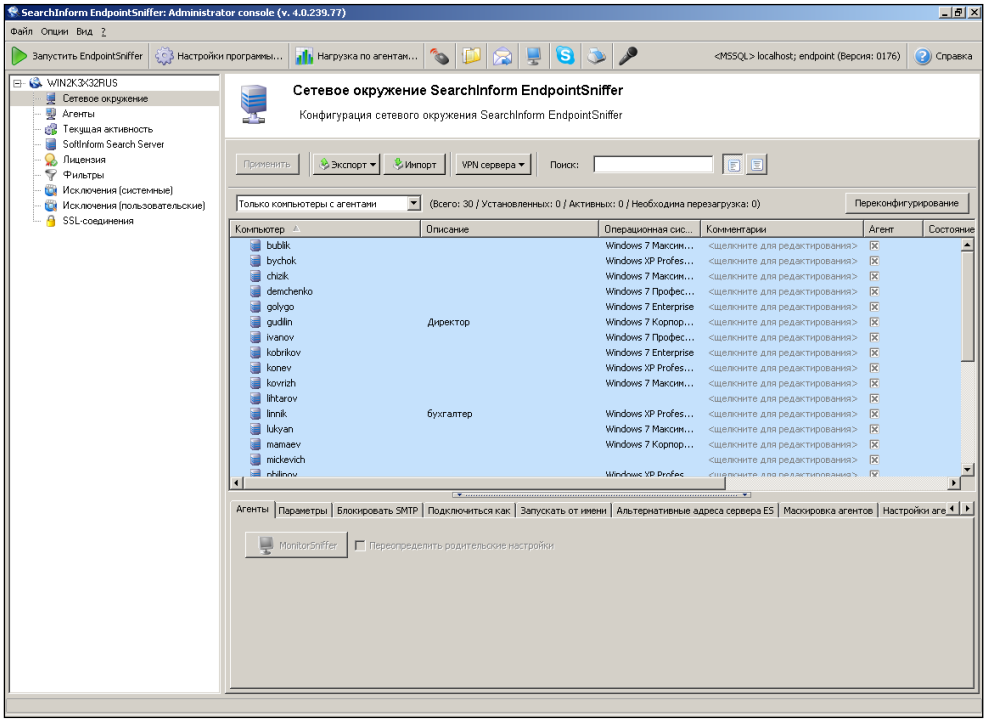

Рис.55 Окно SearchInform EndpointSniffer Console

– В соответствии с рис. 56-60 удалить из фильтрации по всем протоколам данные пользователя «Админ».

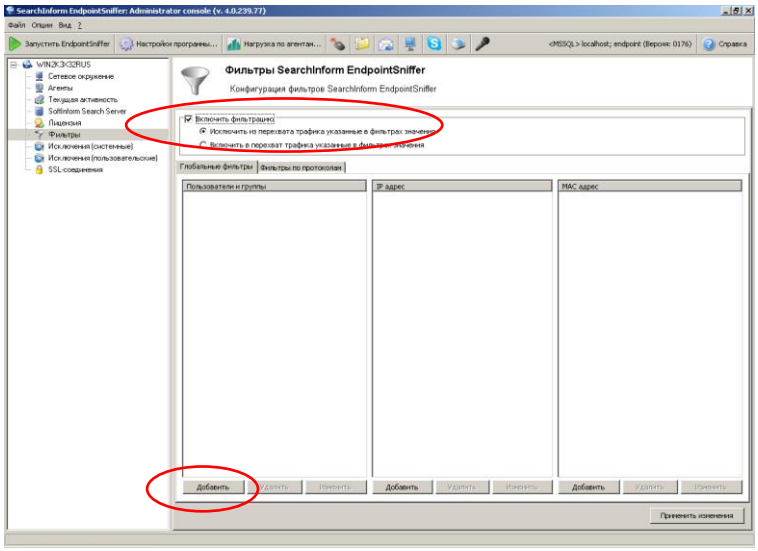

Рис.56 Добавление фильтра по всем протоколам

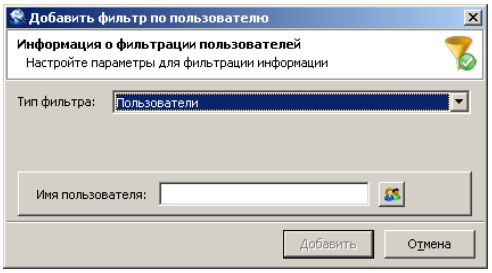

Рис.57Окно ввода имени пользователя

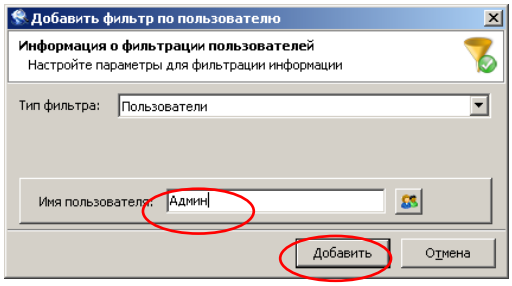

Рис.58 Ввод имени пользователя

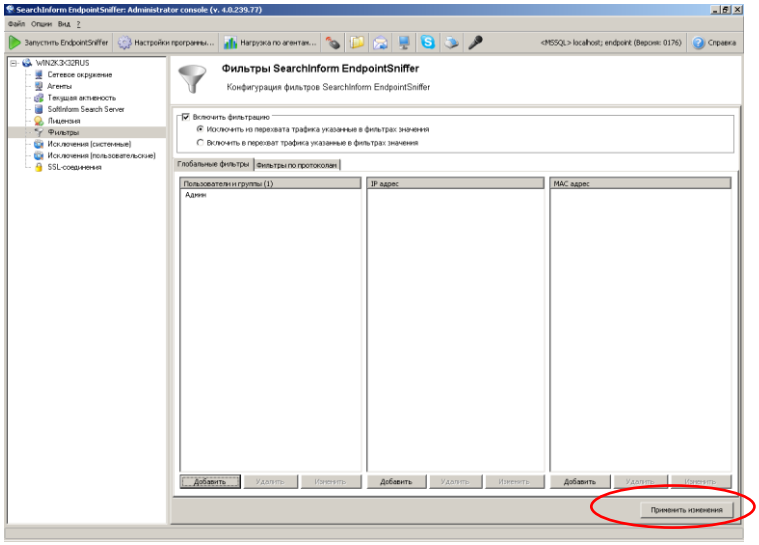

Рис.59 Подтверждение добавления фильтра по всем протоколам

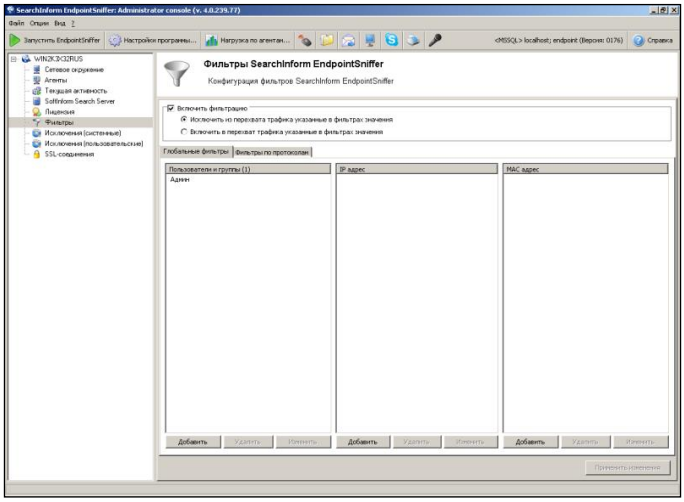

Рис.60 Индикация созданного фильтра по всем протоколам

– В соответствии с рис. 61-69 создать фильтр монитора группы пользователей «NT AUTHORITY\SYSTEM» и пользователя «ivanov». Фильтрация осуществляется с 10.00 до 23.00, кроме субботы и воскресенья.

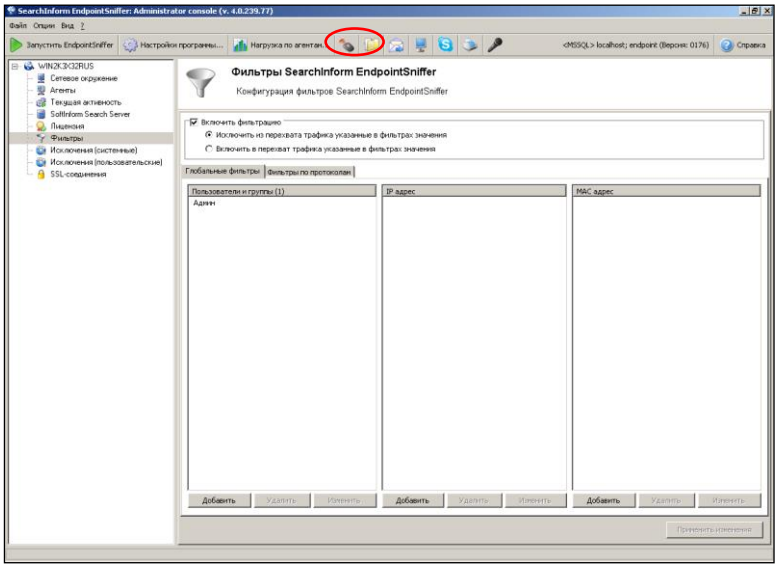

Рис.61 Переход в режим создания фильтра монитора

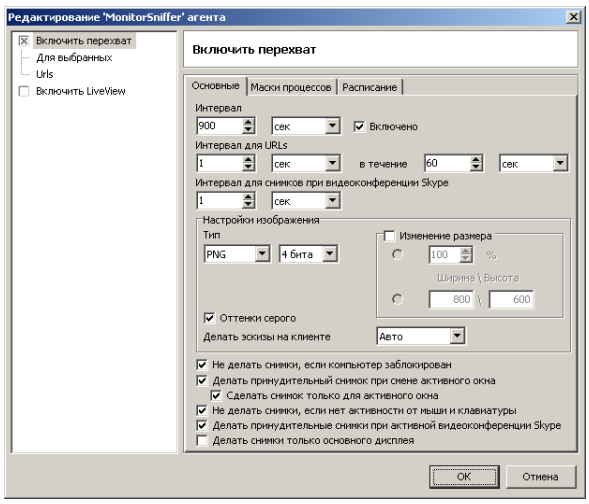

Рис.62 Окно создания фильтра монитора

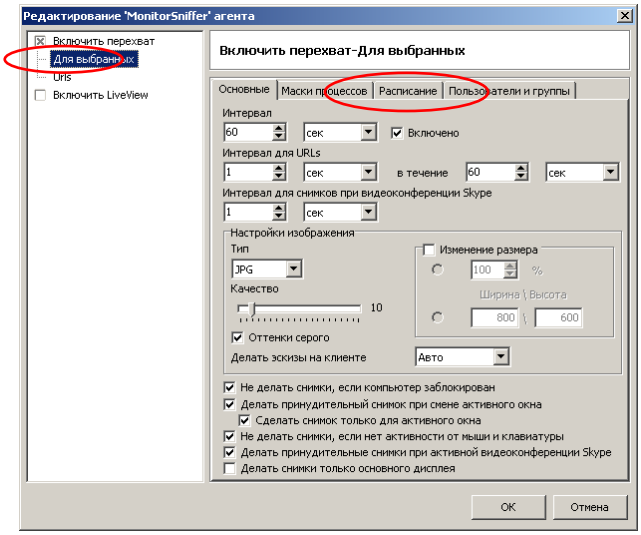

Рис.63 Переход в режим создания фильтра монитора для пользователей

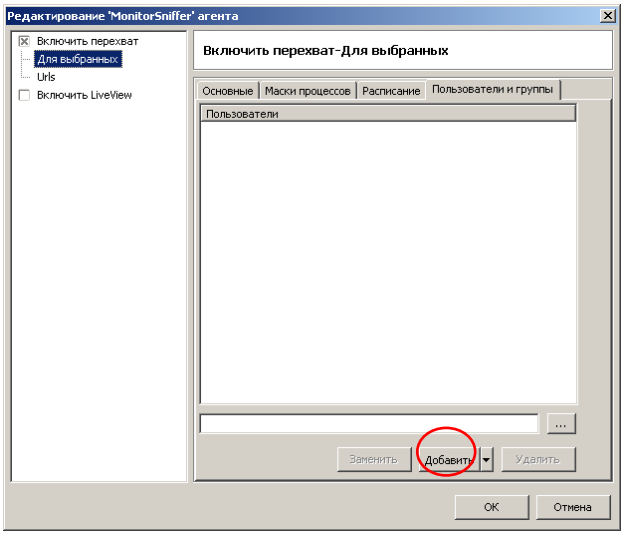

Рис.64 Окно настройки фильтра монитора пользователей

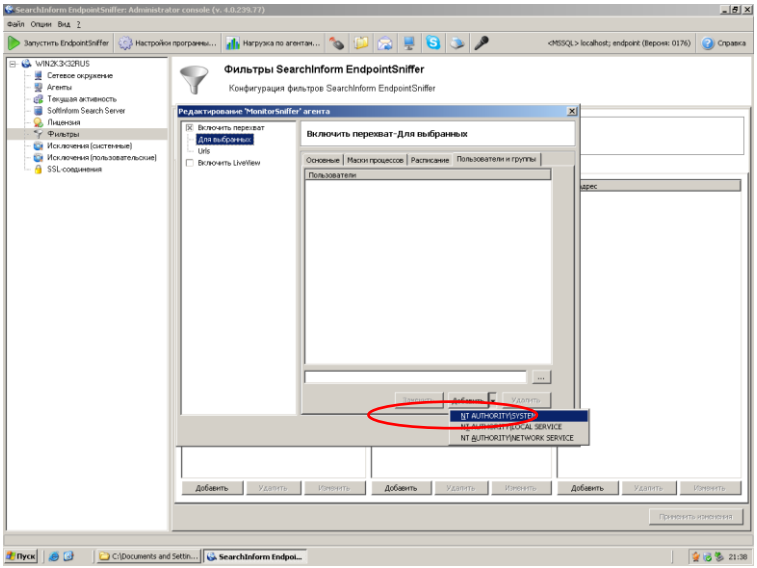

Рис.65 Выбор группы пользователей в фильтре монитора

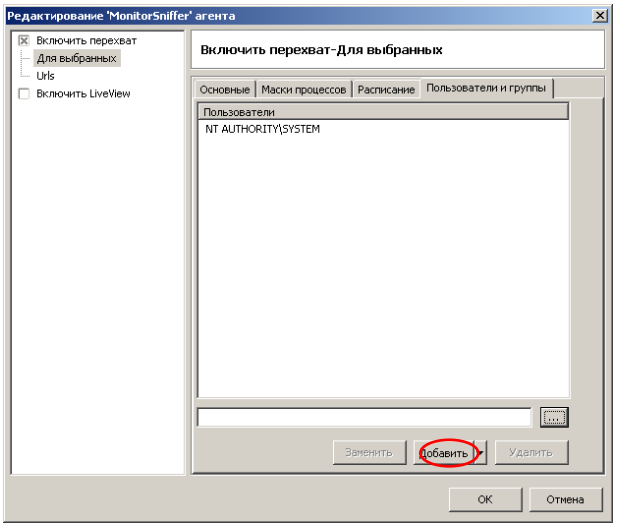

Рис.66 Переход в режим выбора имен пользователей для фильтра монитора

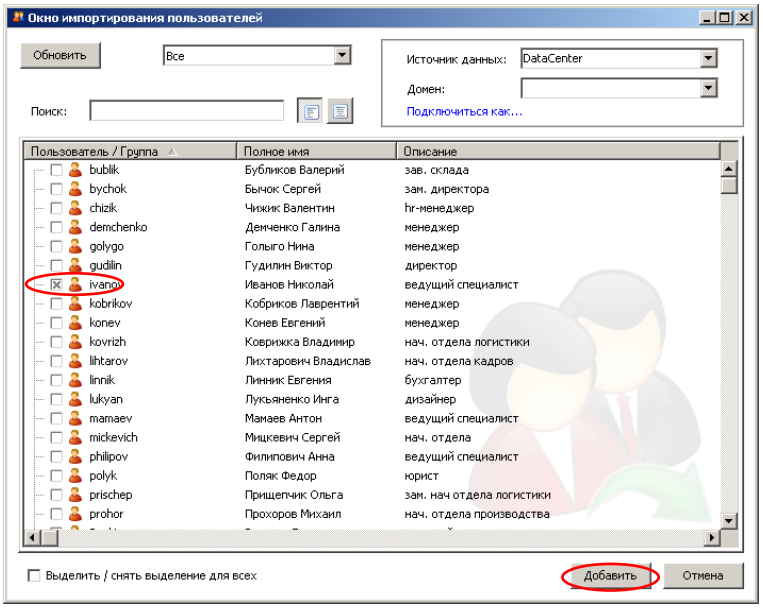

Рис.67 Задание имени пользователя для фильтра монитора

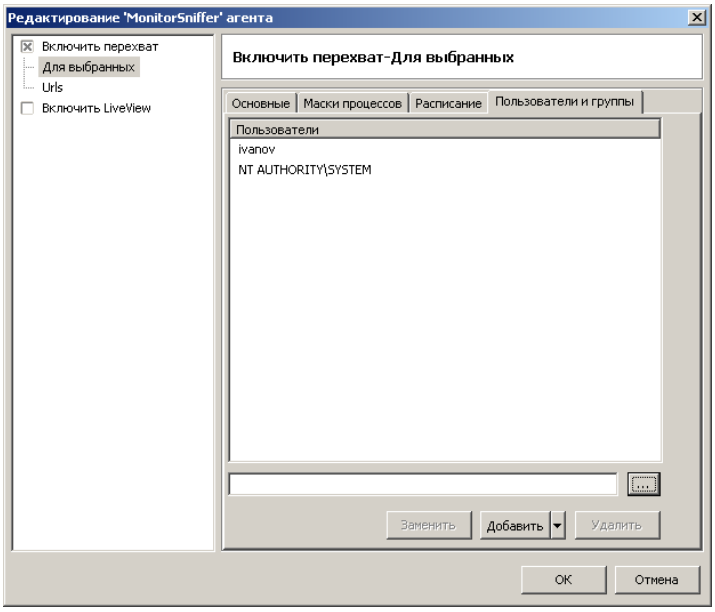

Рис.68 Индикация пользователей в фильтре монитора

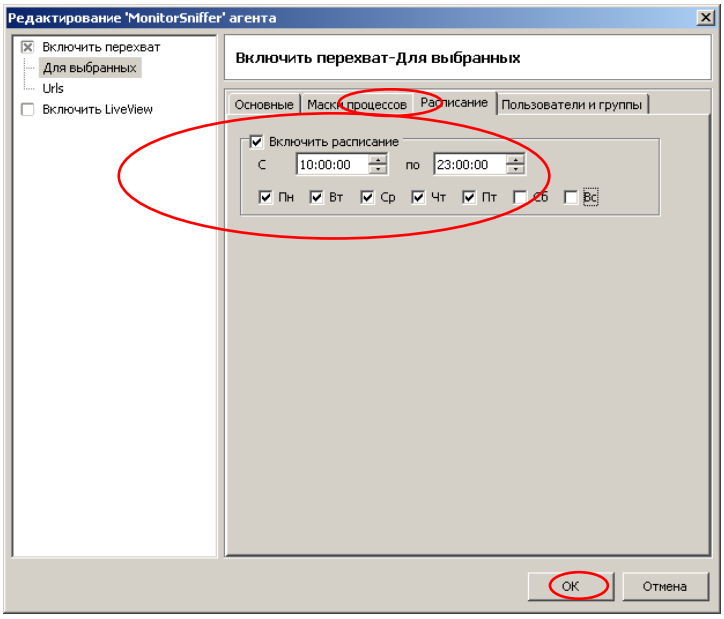

Рис.69 Создание расписания в фильтре монитора

– Закрыть окно консоли SearchInform EndpointSniffer.

– Открыть окно консоли NetworkSniffer Administrator.

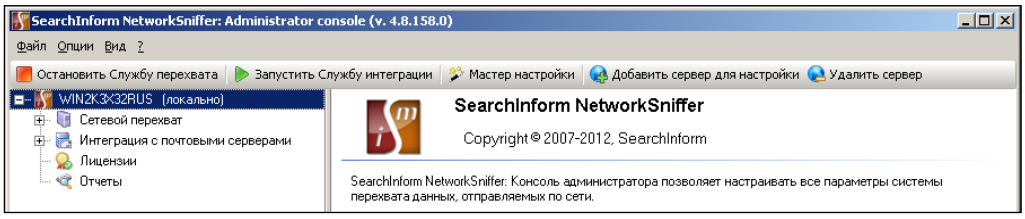

Рис.70 Окно консоли NetworkSniffer Administrator

– В соответствии с рис. 71-76 настроить расписание обновления индексов Network_POST. Предусматриваем обновление индексов через каждые 5 минут.

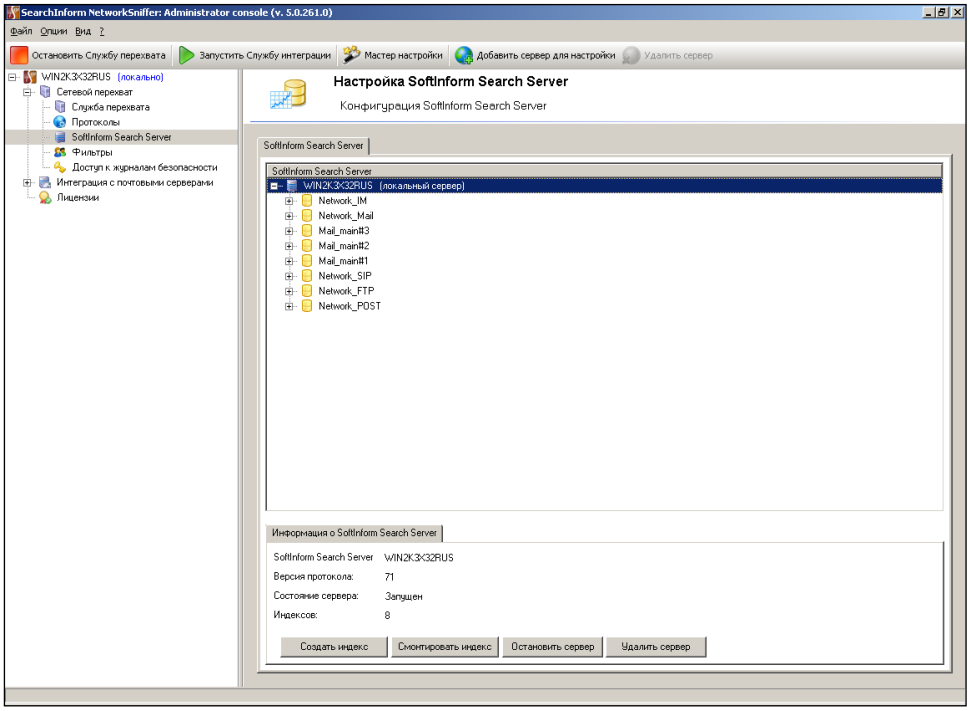

Рис.71 Окно редактирования параметров индексов

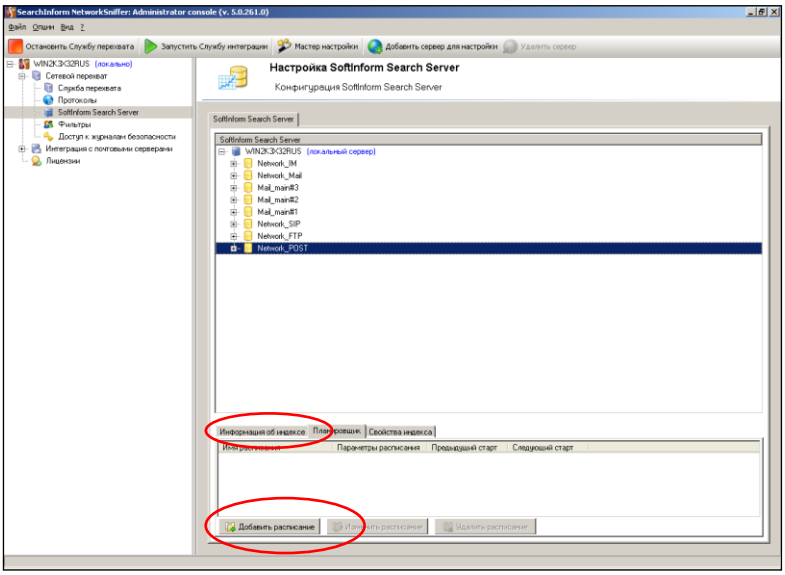

Рис.72 Добавление расписания для индекса Network_POST

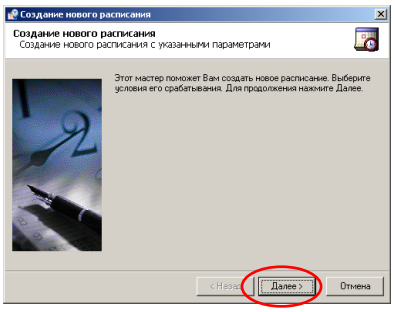

Рис.73 Первый этап создания расписания

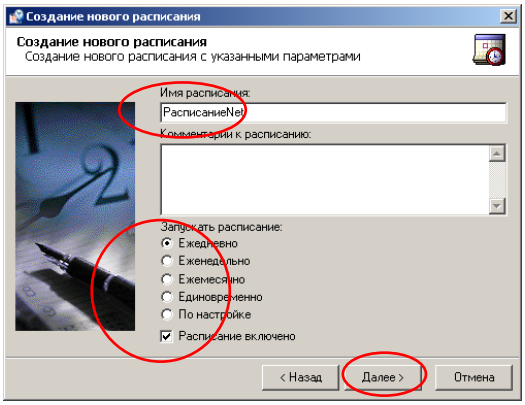

Рис.74 Второй этап создания расписания

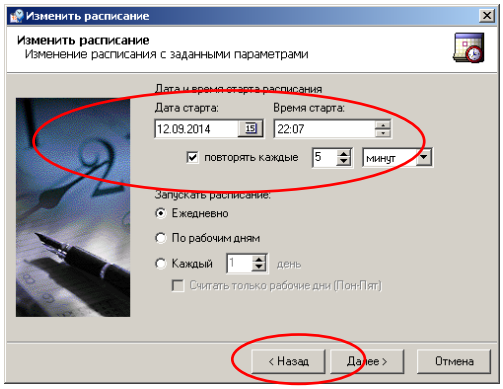

Рис.75 Третий этап создания расписания

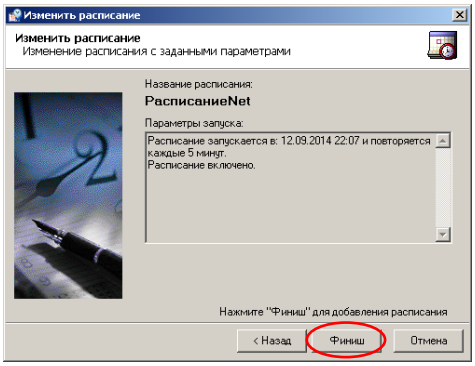

Рис.76 Заключительный этап создания расписания

– Закрыть окно NetworkSniffer Administrator Console.

– Открыть окно AlertCenter Client. В соответствии с рис. 77 открыть ветвь «Политика безопасности».

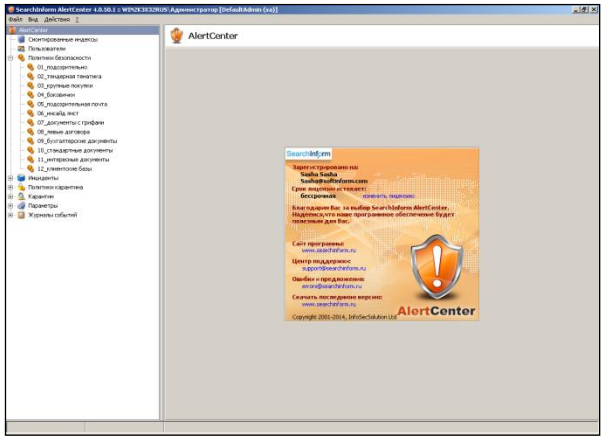

Рис.77 Ветвь «Политика безопасности»

– В соответствии с рис. 78-83 изменить параметры политики безопасности «05_подозрительная почта». Предусмотреть: использование индексов MailSniffer, отправку сообщений пользователю Admin, начало проверки индексов 10.12.2014, проверять индексы ежедневно, только по рабочим дням, через каждые 20 минут, исключить из проверки группу «Лояльные сотрудники».

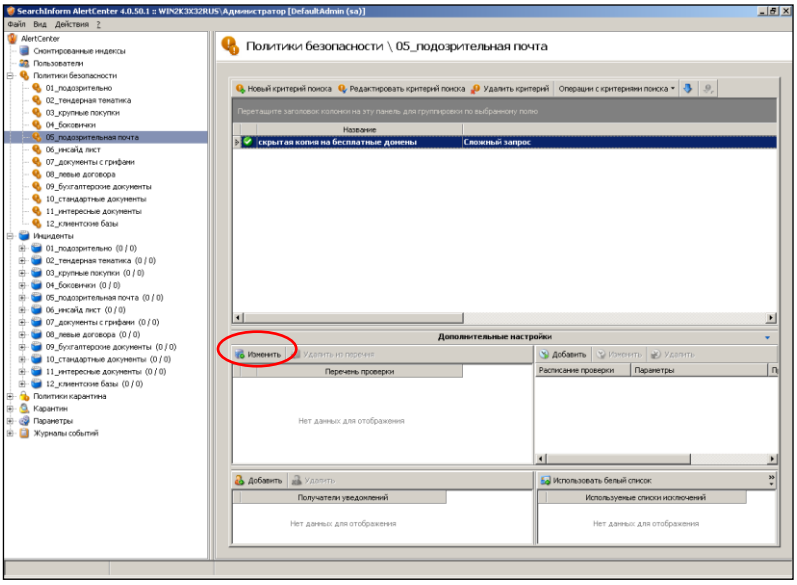

Рис.79 Переход к настройке используемых индексов

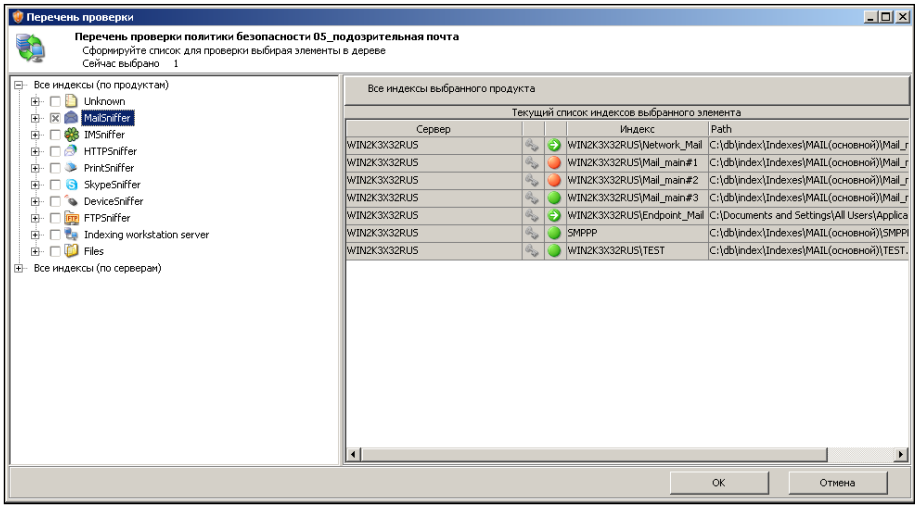

Рис.79 Выбор индексов

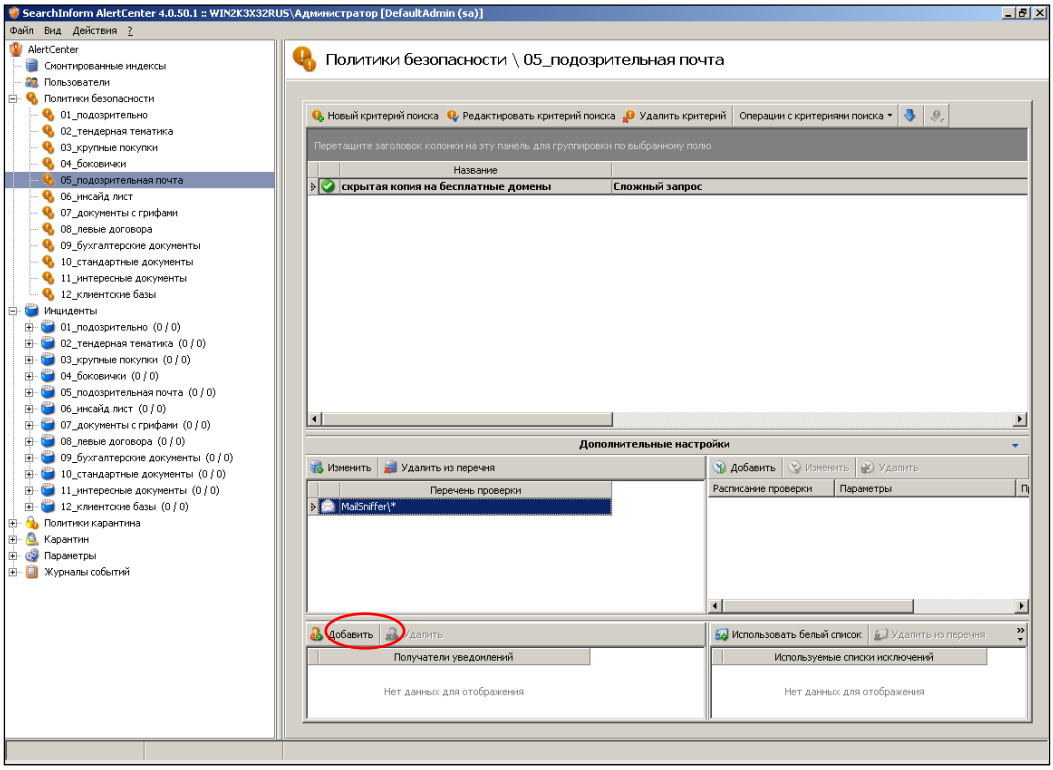

Рис.80 Переход к настройке получателей уведомлений

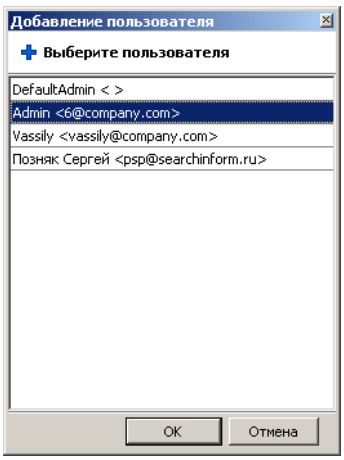

Рис.81 Выбор получателей уведомлений

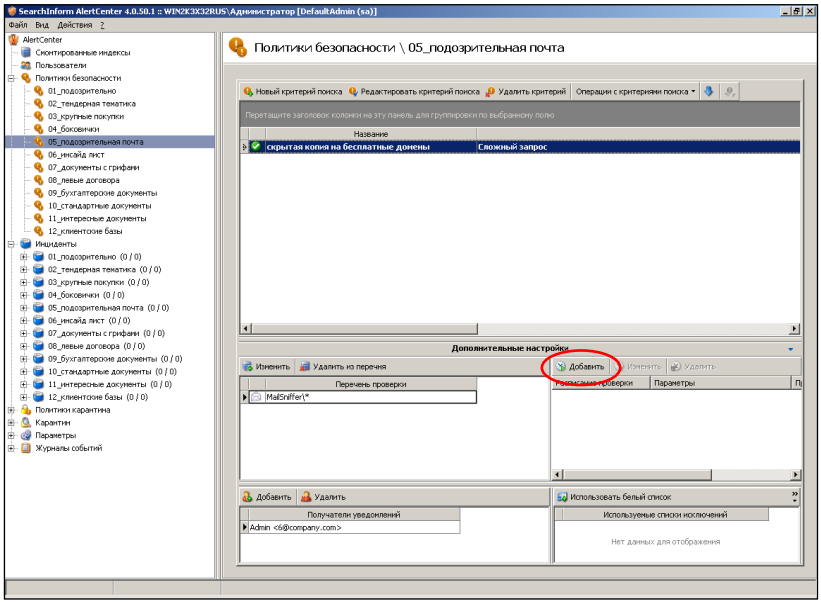

Рис.82 Переход к настройке расписания

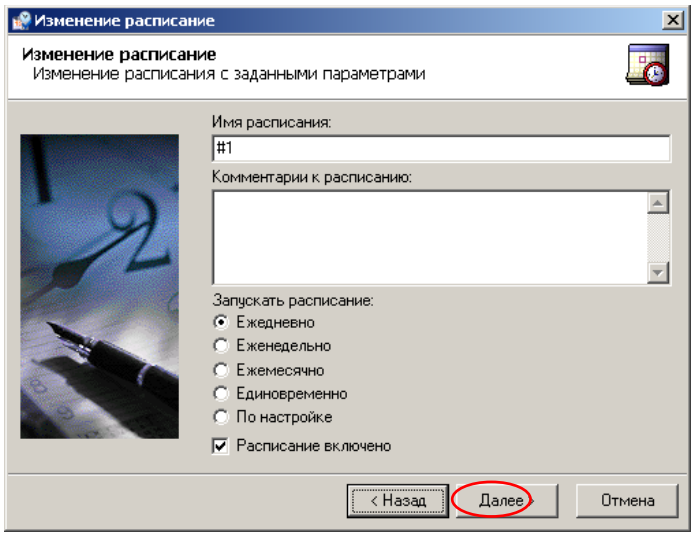

Рис.83 Первый этап создания расписания

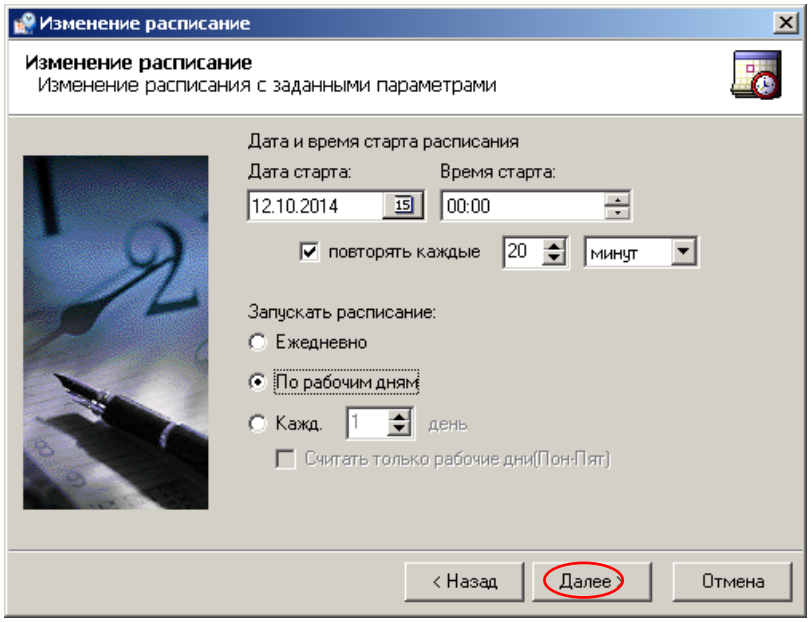

Рис.84 Второй этап создания расписания

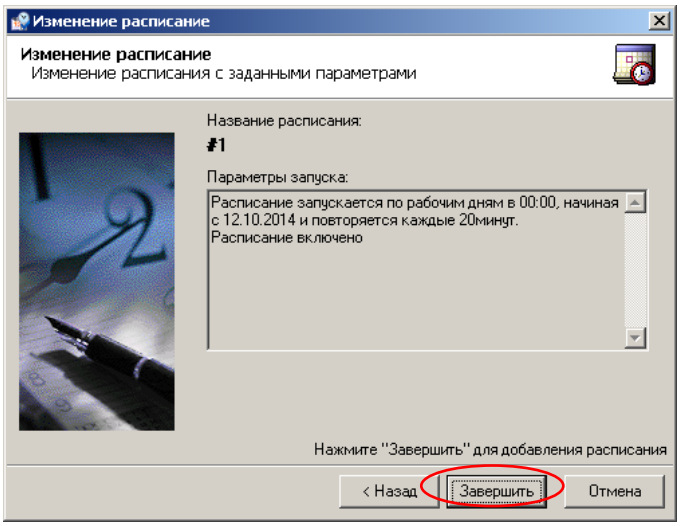

Рис.85 Третий этап создания расписания

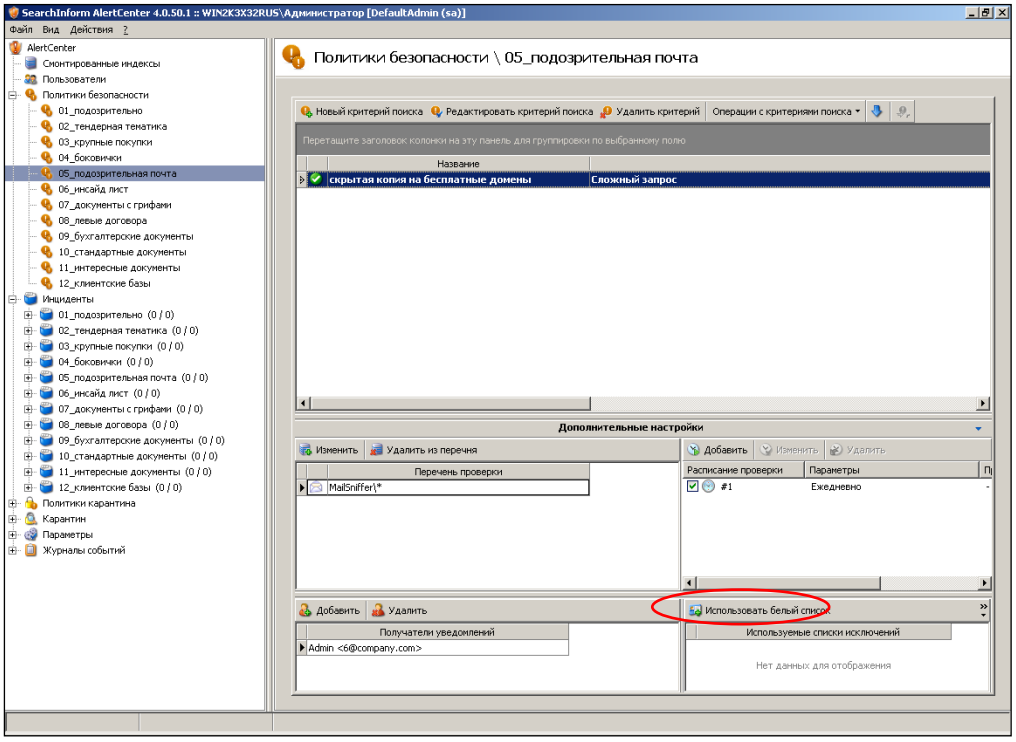

Рис.86 Переход к использованию «белых списков»

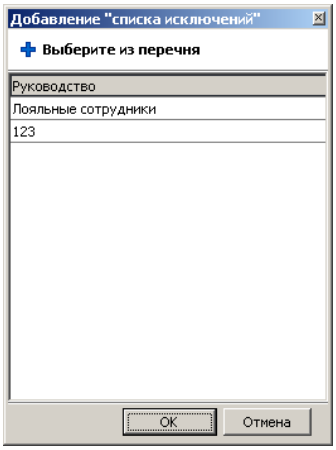

Рис.87 Перечень доступных «белых списков»

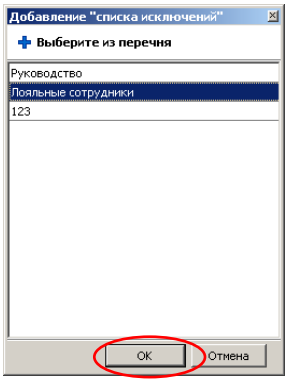

Рис.88 Выбор «белого списка»

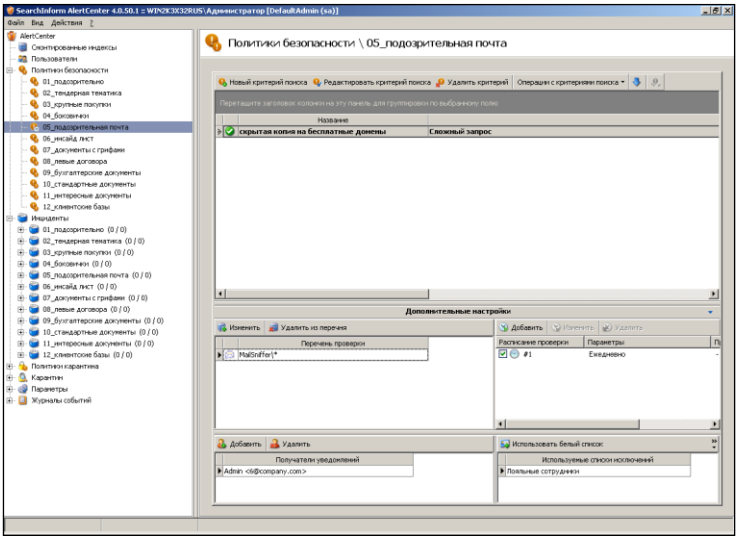

Рис.89 Индикация параметров политики безопасности «05_подозрительная почта»

– В соответствии с рис. 90 убедиться в наличии выявленных нарушений (инциндентов) политики «05_подозрительная почта».

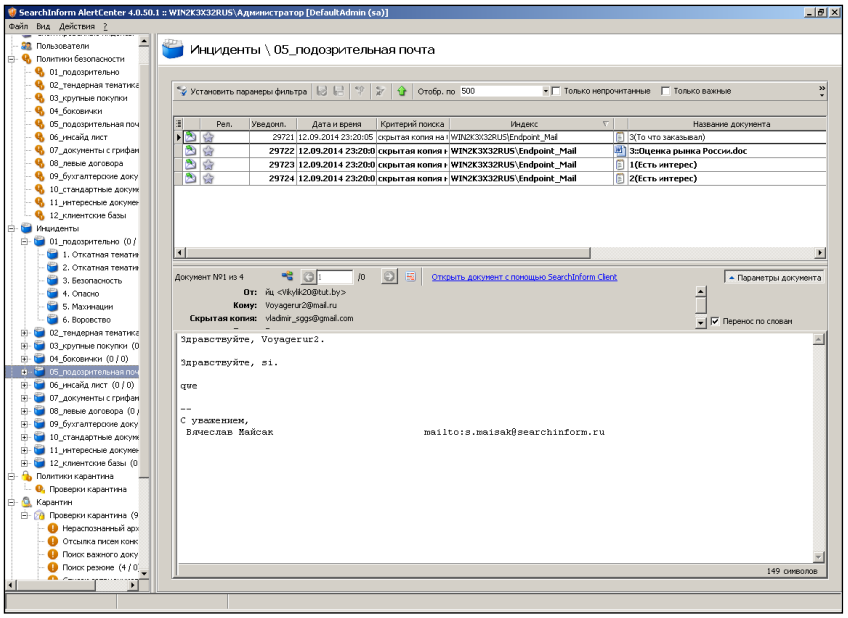

Рис.90 Просмотр выявленных нарушений политики «05_подозрительная почта»

– В соответствии с рис. 91-93 отредактировать белый список «Лояльных сотрудников». Добавить в него пользователя «link».

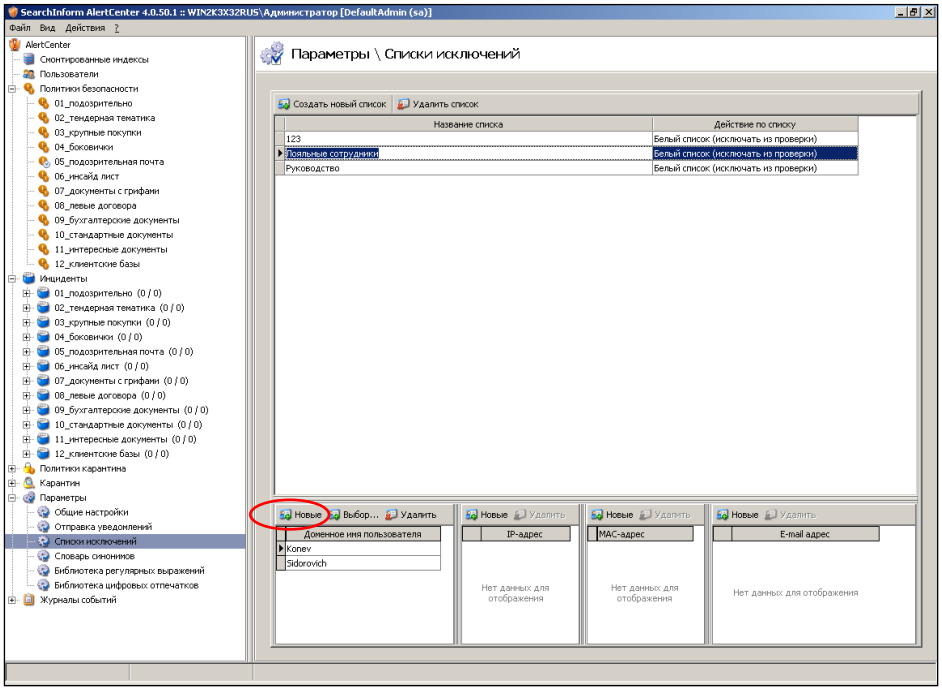

Рис.91 Вход в режим добавления нового пользователя

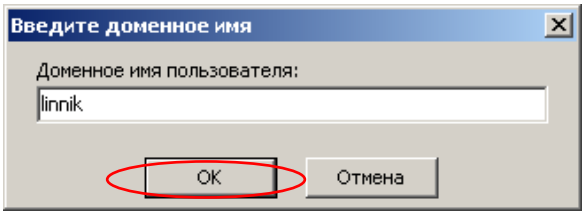

Рис.92 Ввод имени пользователя

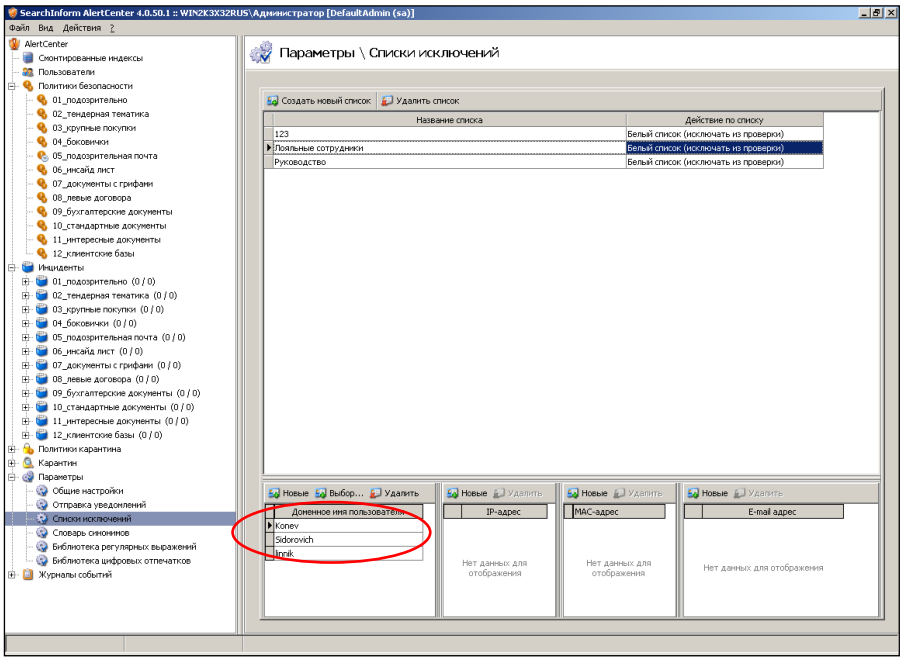

Рис.93 Индикация пользователей в белом списке «Лояльные сотрудники»

– В соответствии с рис. 94-98 создать белый список «Мой список». Добавить в него пользователя «Администратор».

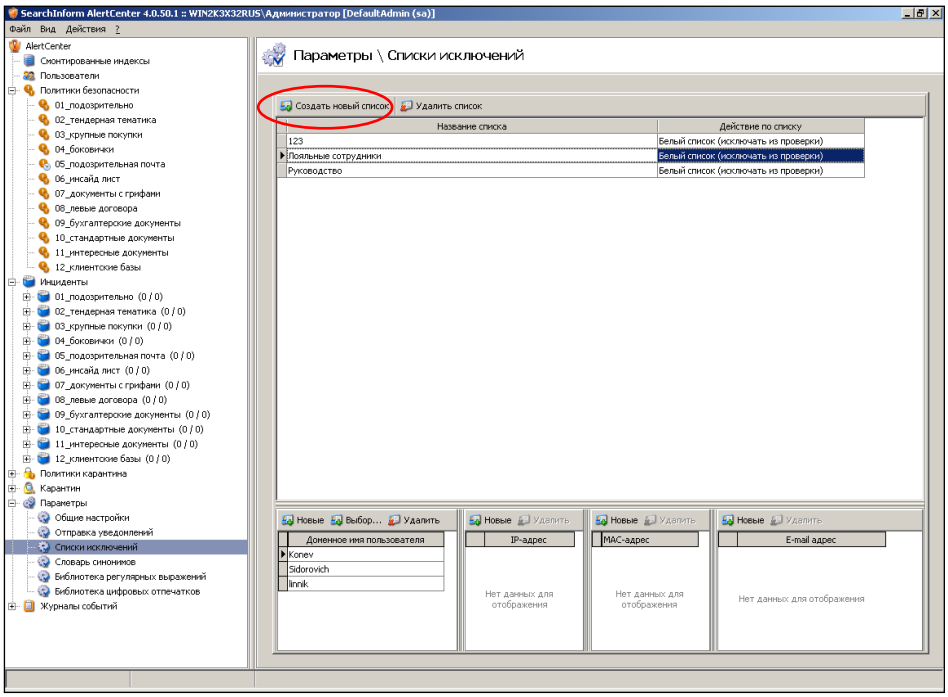

Рис. 94 Первый этап создания нового белого списка

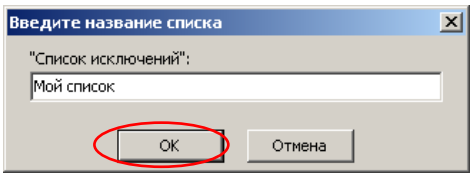

Рис.95 Указание имени списка

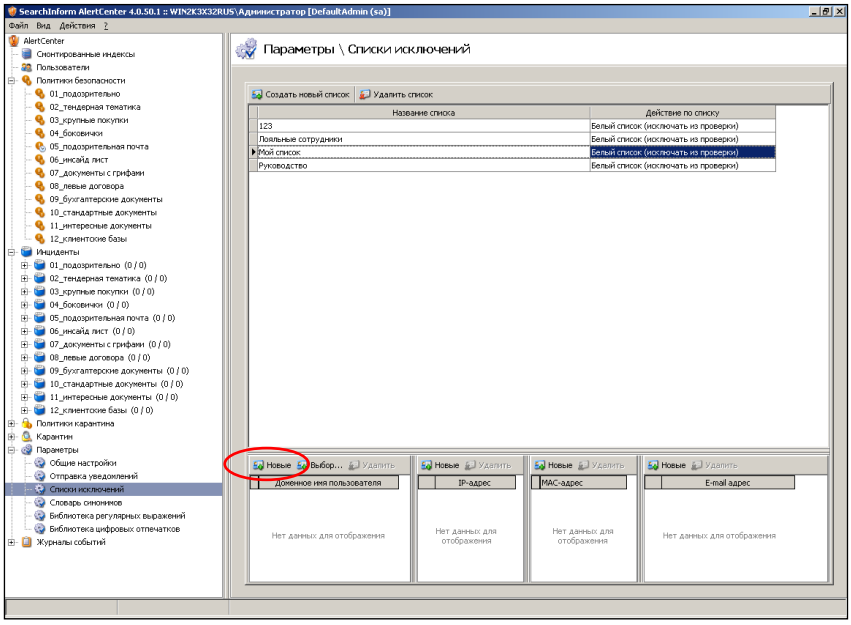

Рис.96 Первый этап добавления нового пользователя в список

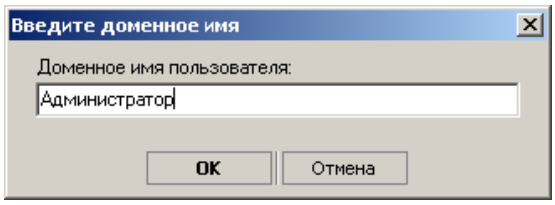

Рис.97 Указание имени добавляемого пользователя

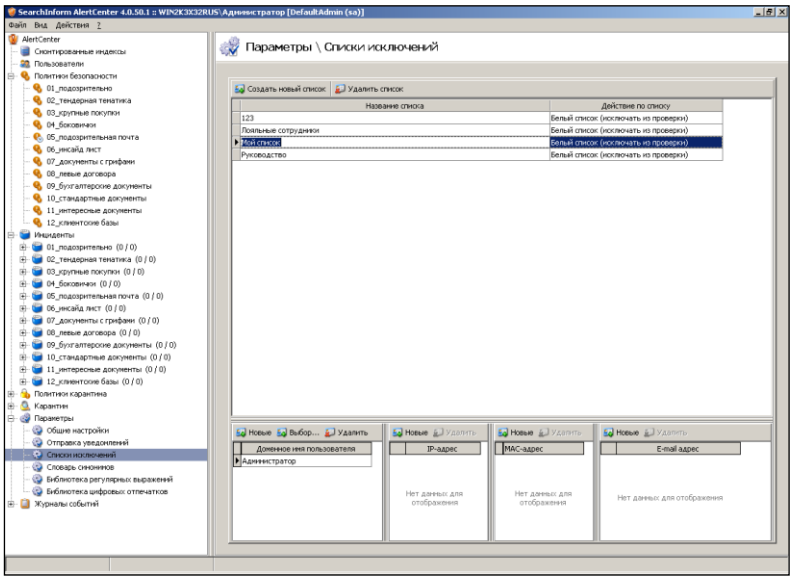

Рис.98 Индикация параметров созданного списка «Мой список»

– В соответствии с рис. 99-104 создать новую политику безопасности с названием «Тест1».

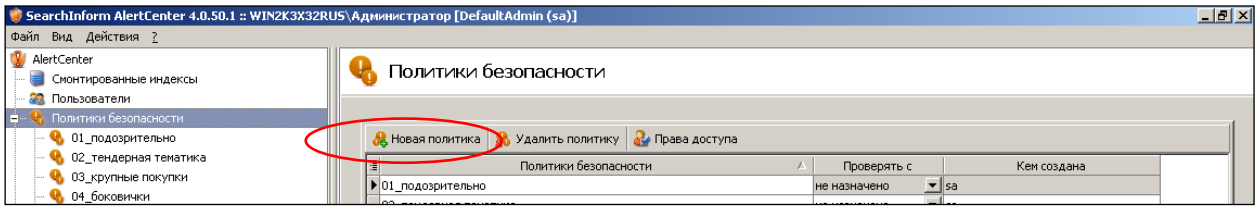

Рис.99 Вход в режим создания новой политики

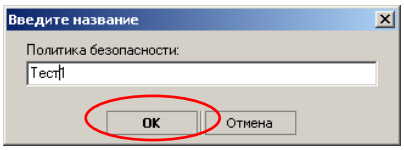

Рис.100 Указание имени политики

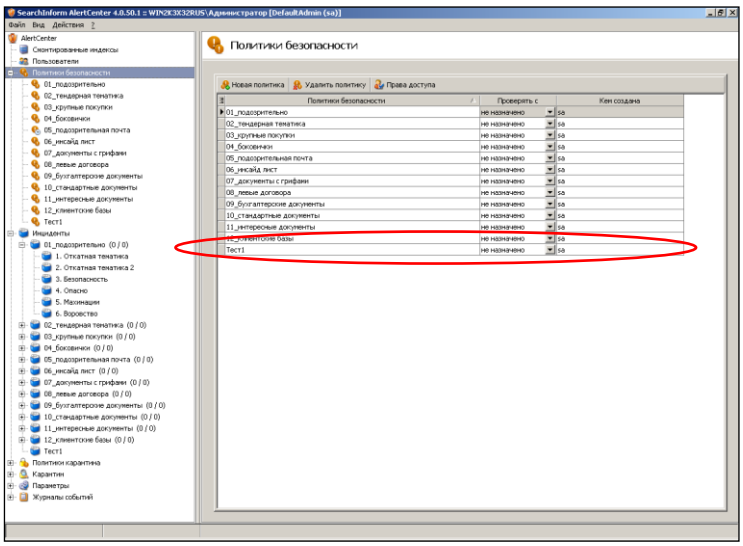

Рис.101 Индикация созданной политики

– В соответствии с рис. 102-106 добавить в политику «Тест1» поиск, по ключевым словам, и поиск по атрибутам перехваченных данных.

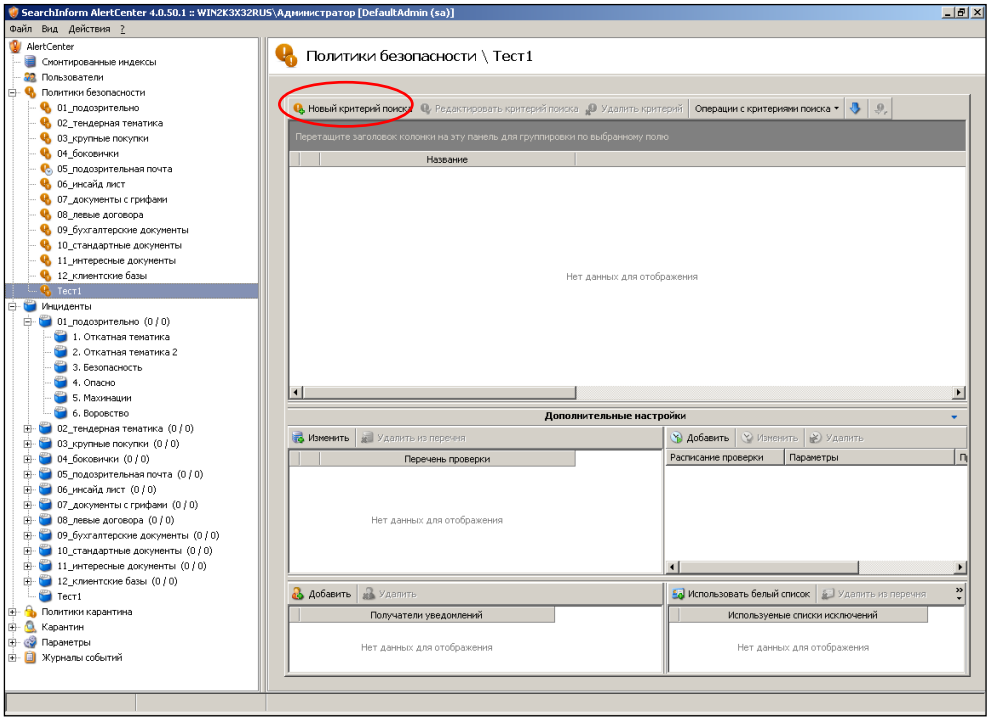

Рис.102 Вход в режим создания критериев поиска

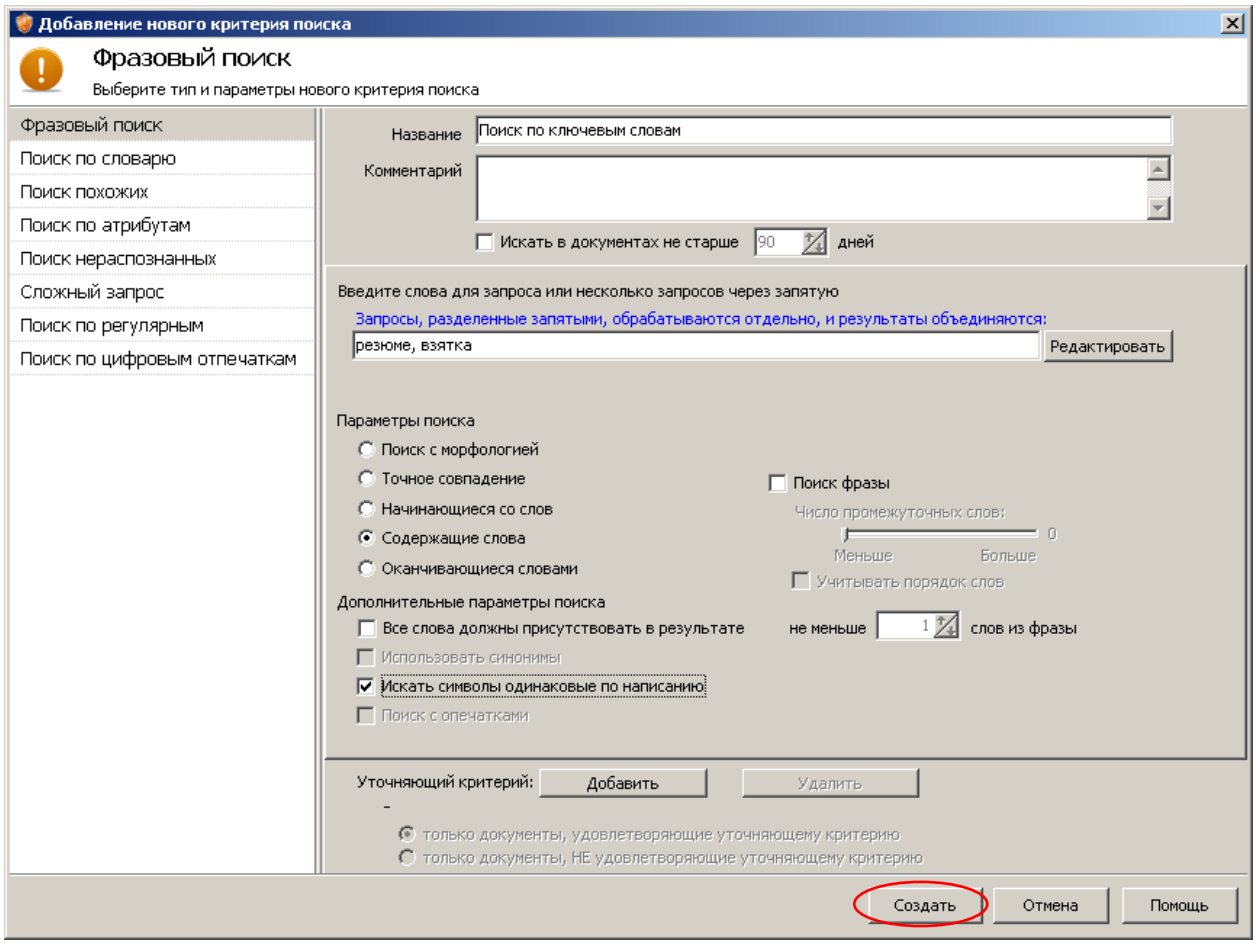

Рис.103 Указание параметров поиска по ключевыпм словам

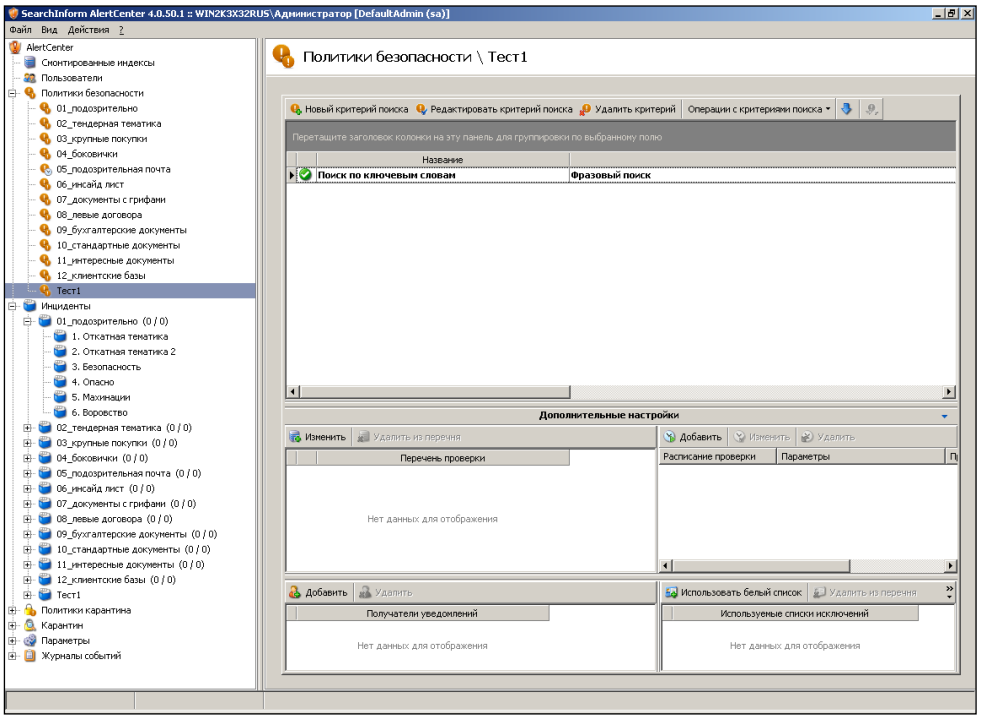

Рис.104 Индикация созданного запроса фразового поиска

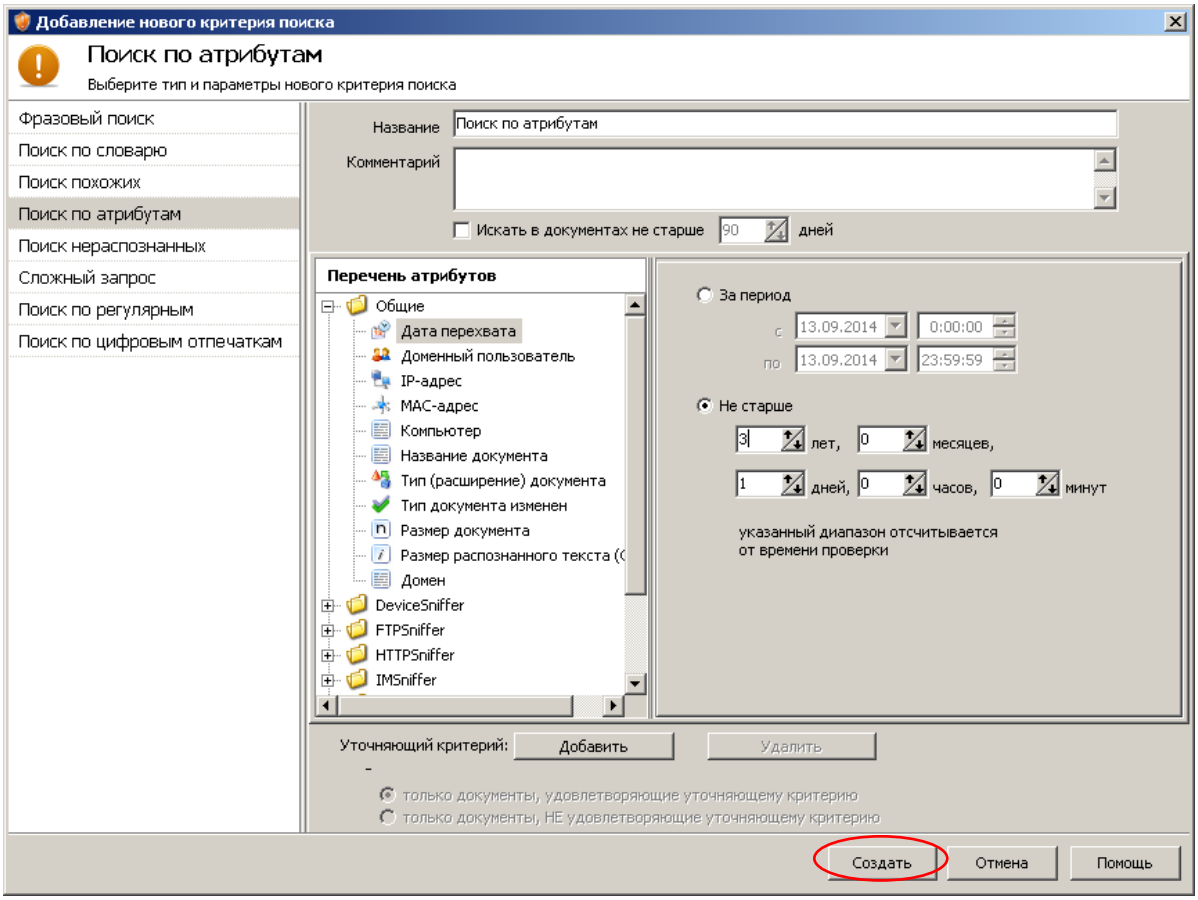

Рис.105 Указание параметров поиска по атрибутам

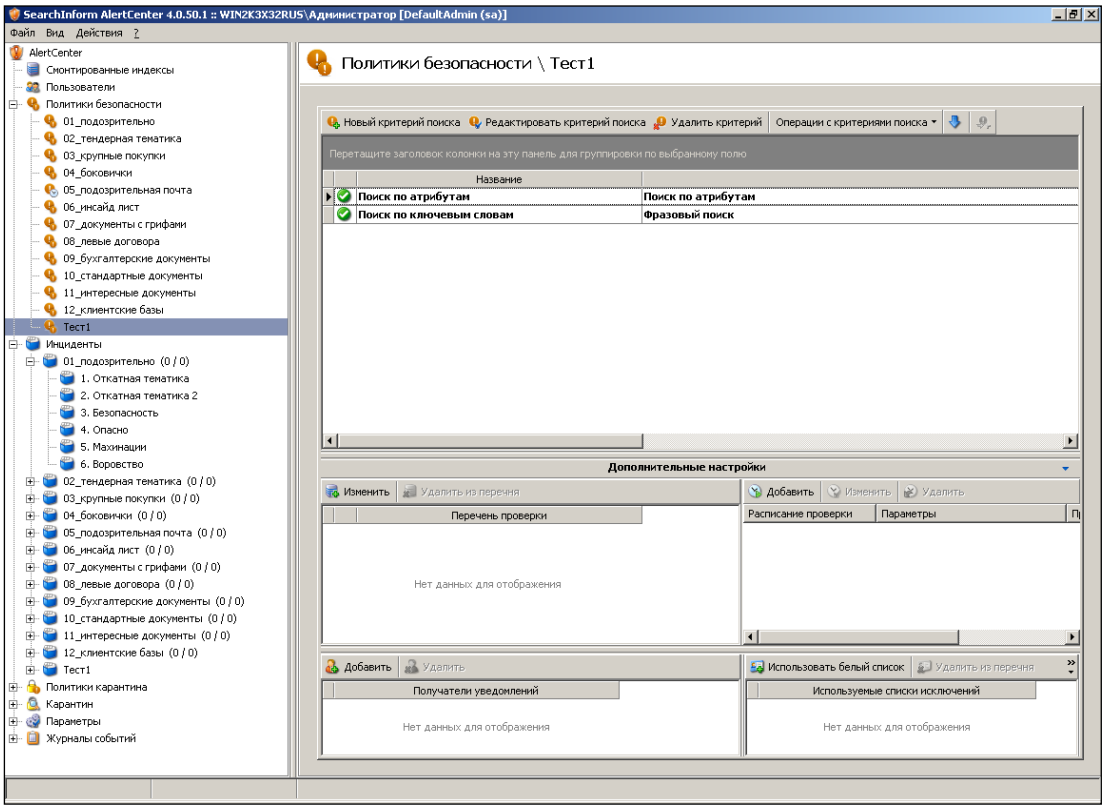

Рис.106 Индикация созданных поисковых запросов

– В соответствии с рис. 107-117 следует добавить в политику «Тест1» список проверяемых индексов, расписание проверки индексов, список получателей уведомлений о нарушениях и белый список пользователей.

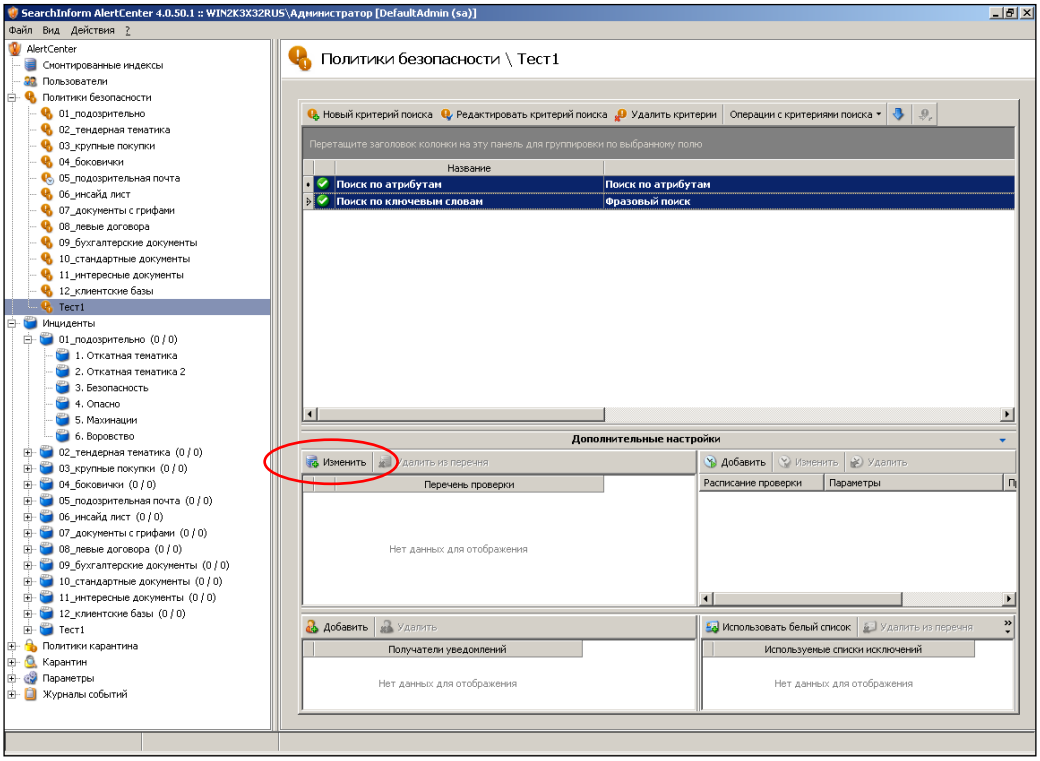

Рис.107 Вход в режим добавления индексов

(для выделения нескольких критериев поиска используйте клавиши Ctrl и Shift)

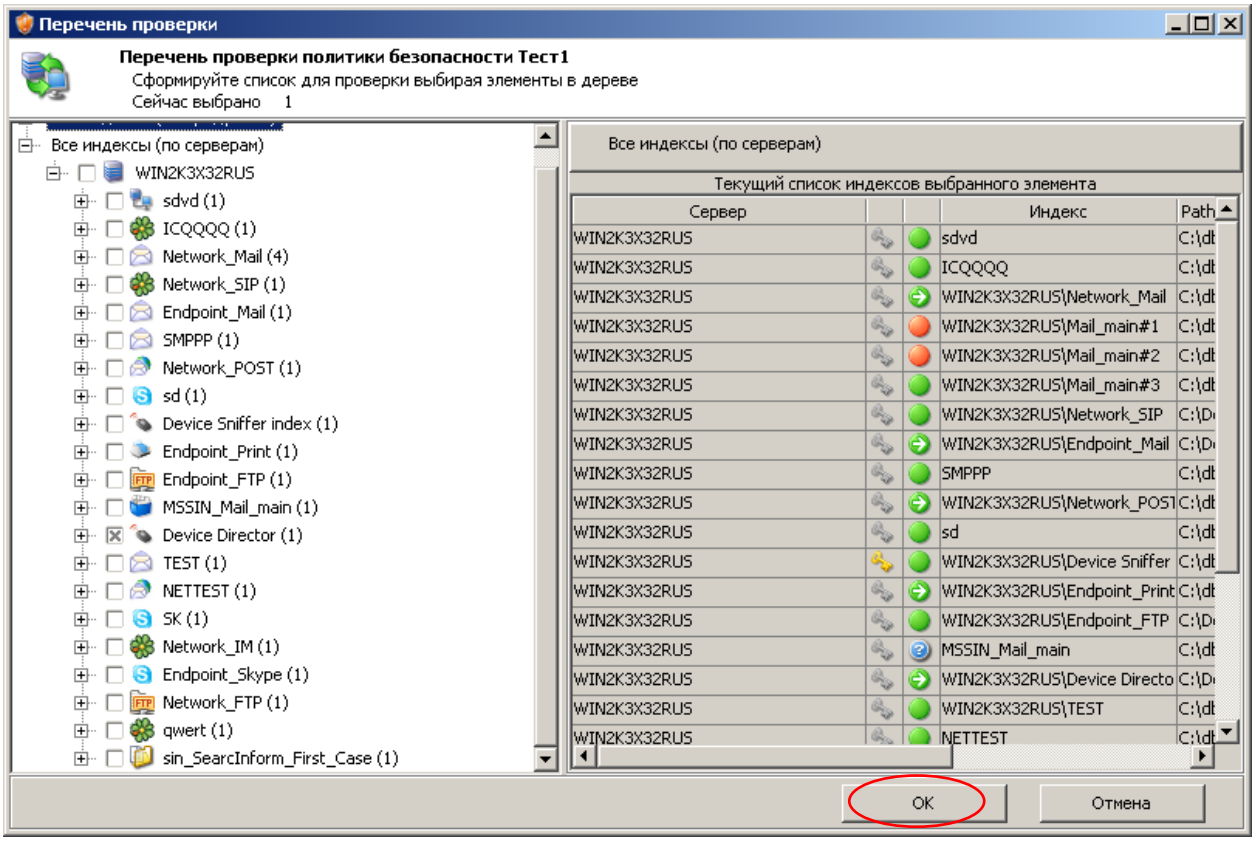

Рис.108Окно добавления имен индексов

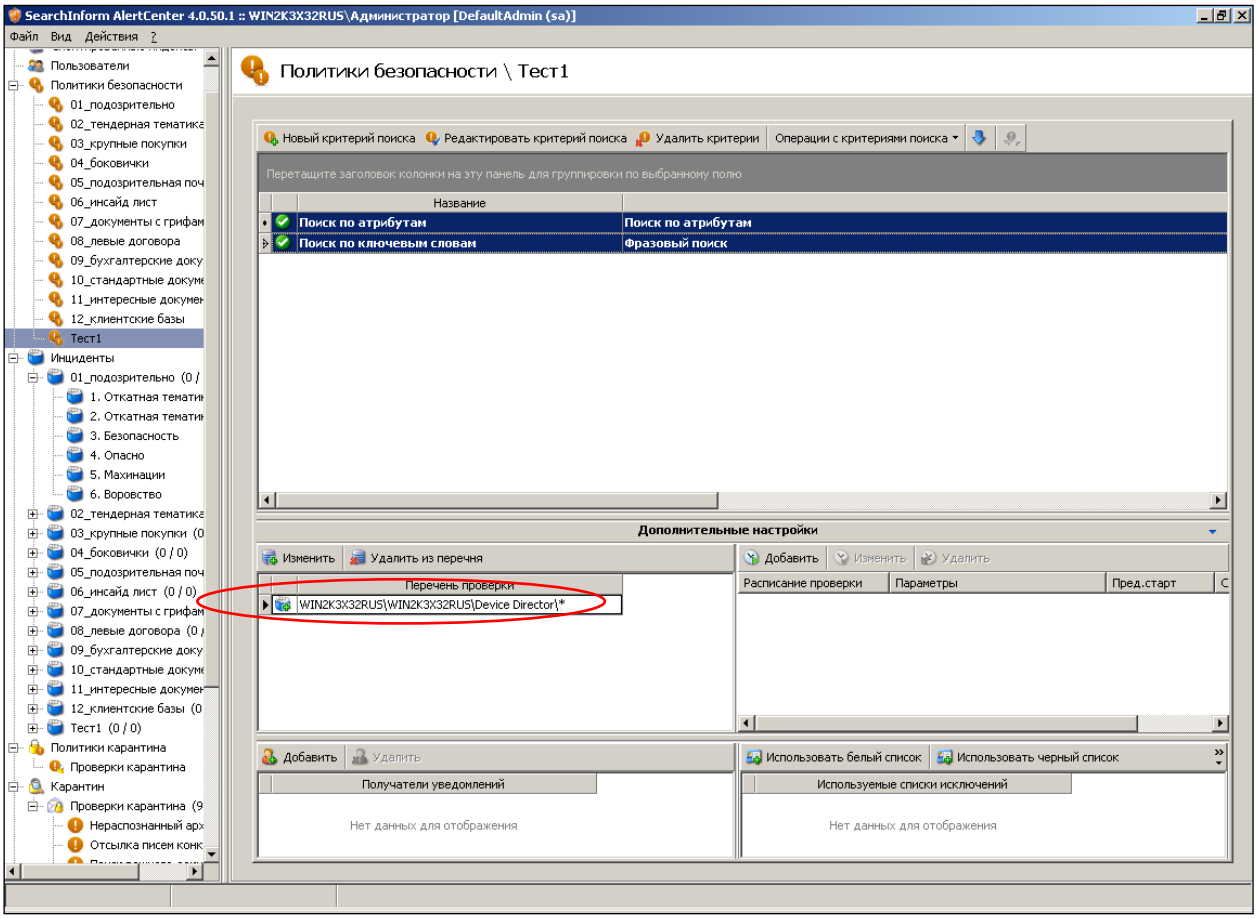

Рис.109 Индикация выбранных индексов

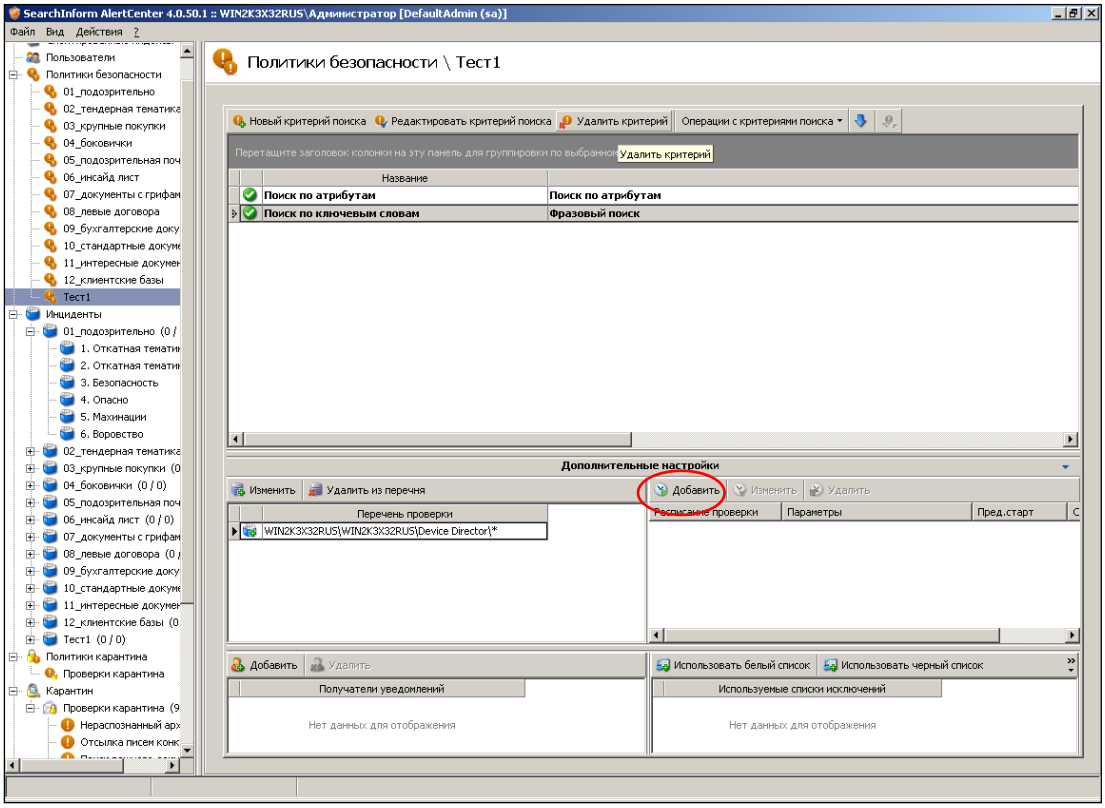

Рис.110 Добавление нового расписания проверок индексов

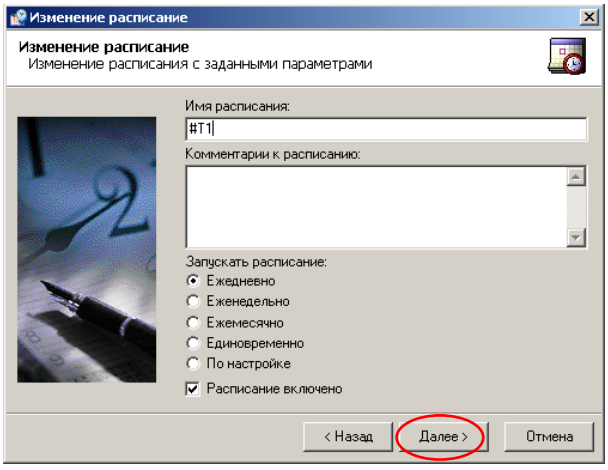

Рис.111 Первый этап формирования расписания проверок индексов

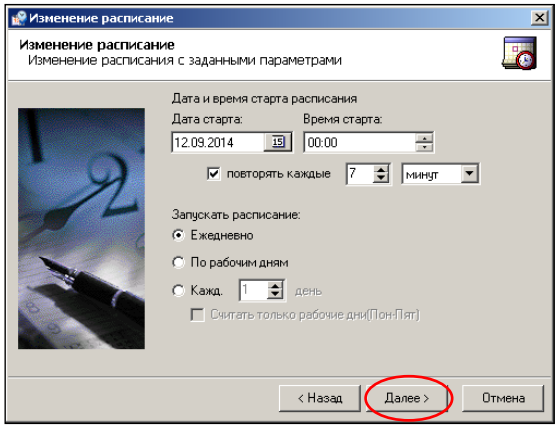

Рис.112Второй этап формирования расписания проверок индексов (частота проверки – 7 мин)

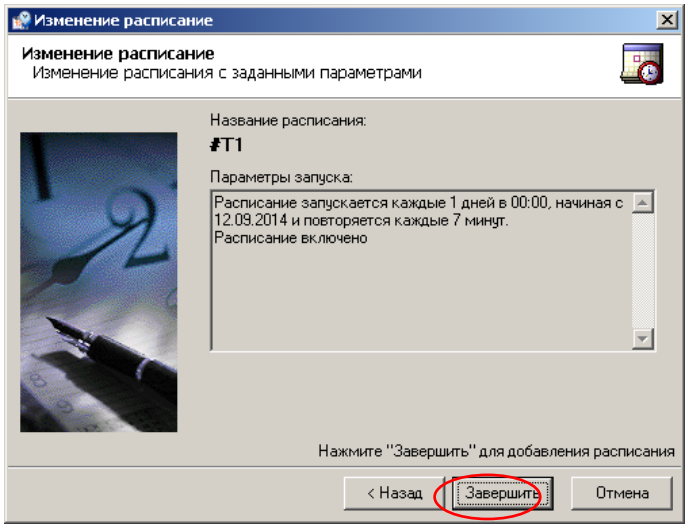

Рис.113 Заключительный этап формирования расписания проверок индексов

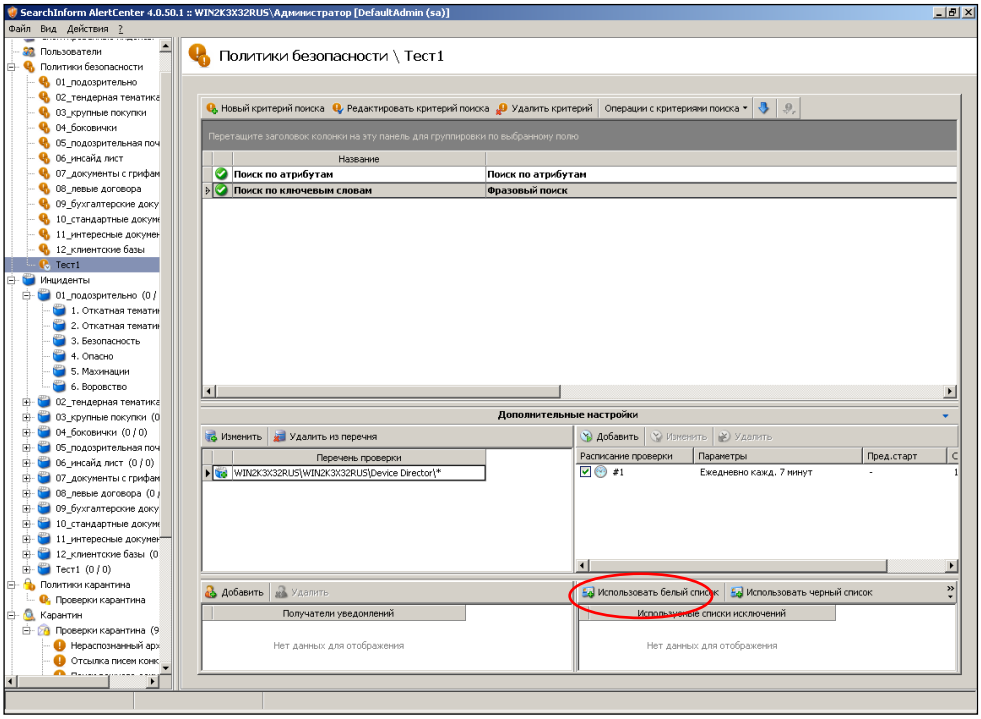

Рис.114 Первый этап добавления белого списка в политику «Тест1»

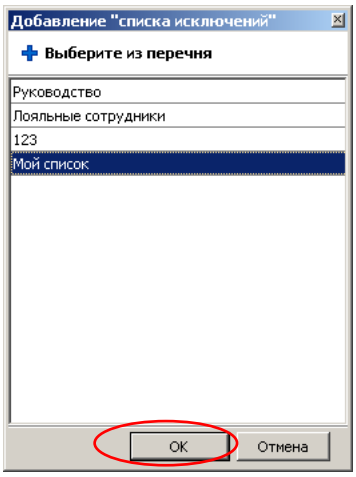

Рис.115 Второй этап добавления белого списка «Мой список» в политику «Тест1»

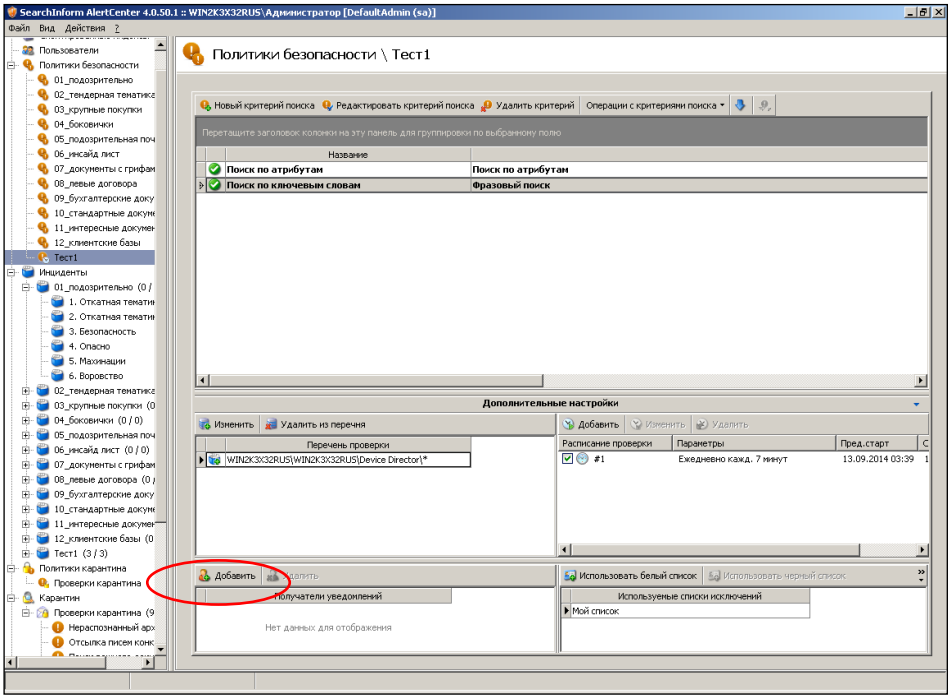

Рис.116 Первый этап формирования списка получателей уведомлений о нарушениях политики безопасности «Тест1»

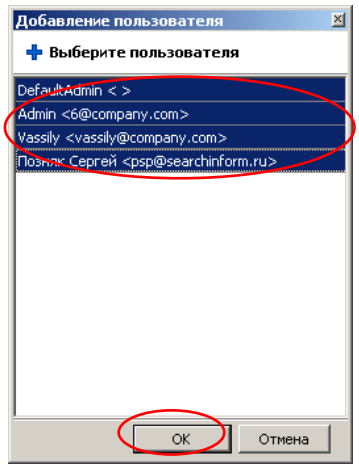

Рис.117 Выбор имен получателей

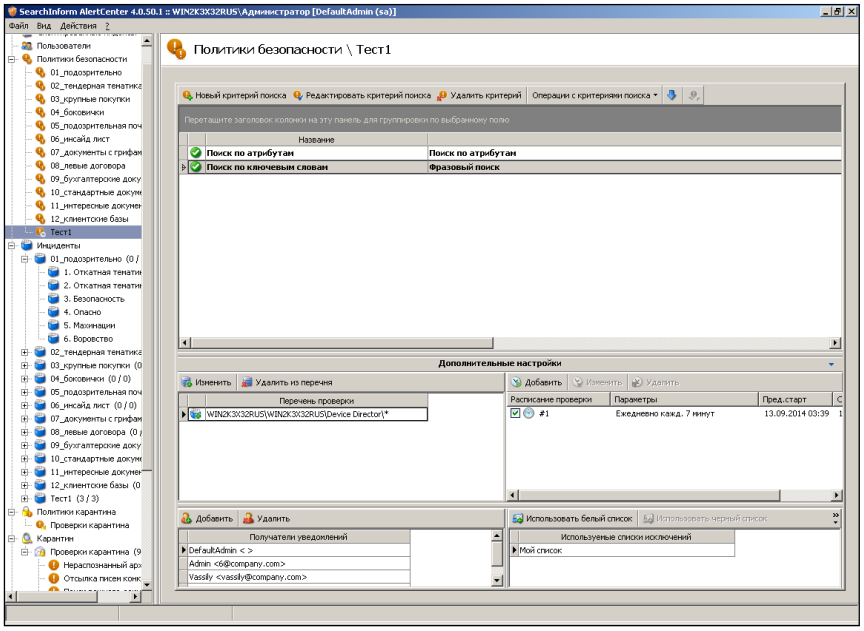

Рис.118 Отображение параметров политии безопасности «Тест1»

– В соответствии с рис. 119 просмотреть инциденты, связанные с нарушением политики безопасности «Тест1». Проверку произвести через 7 минут после окончания формирования политики, или в соответствии с рис. 120 запустить проверку принудительно.

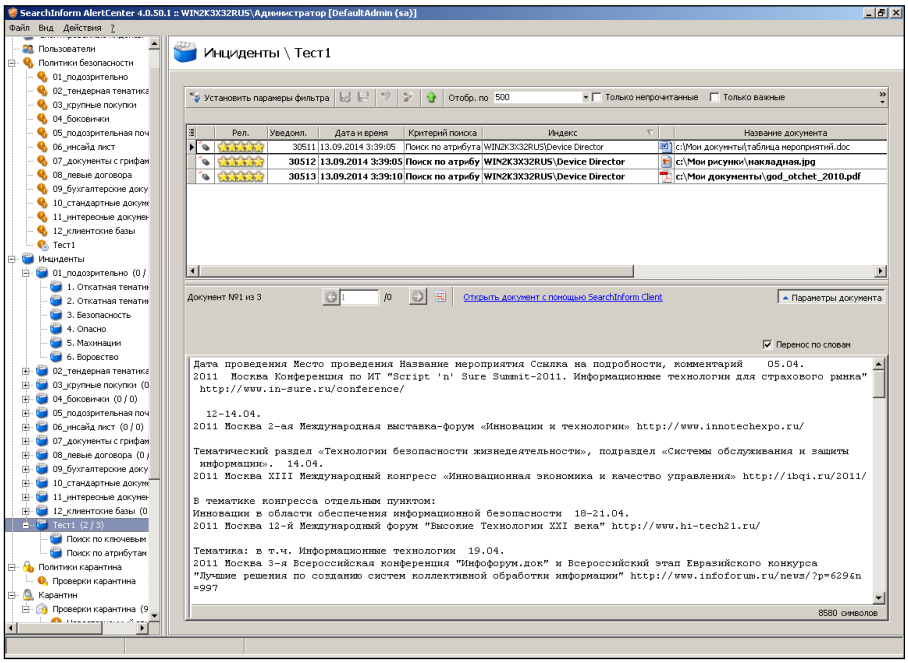

Рис.119 Проверка выявленных нарушений

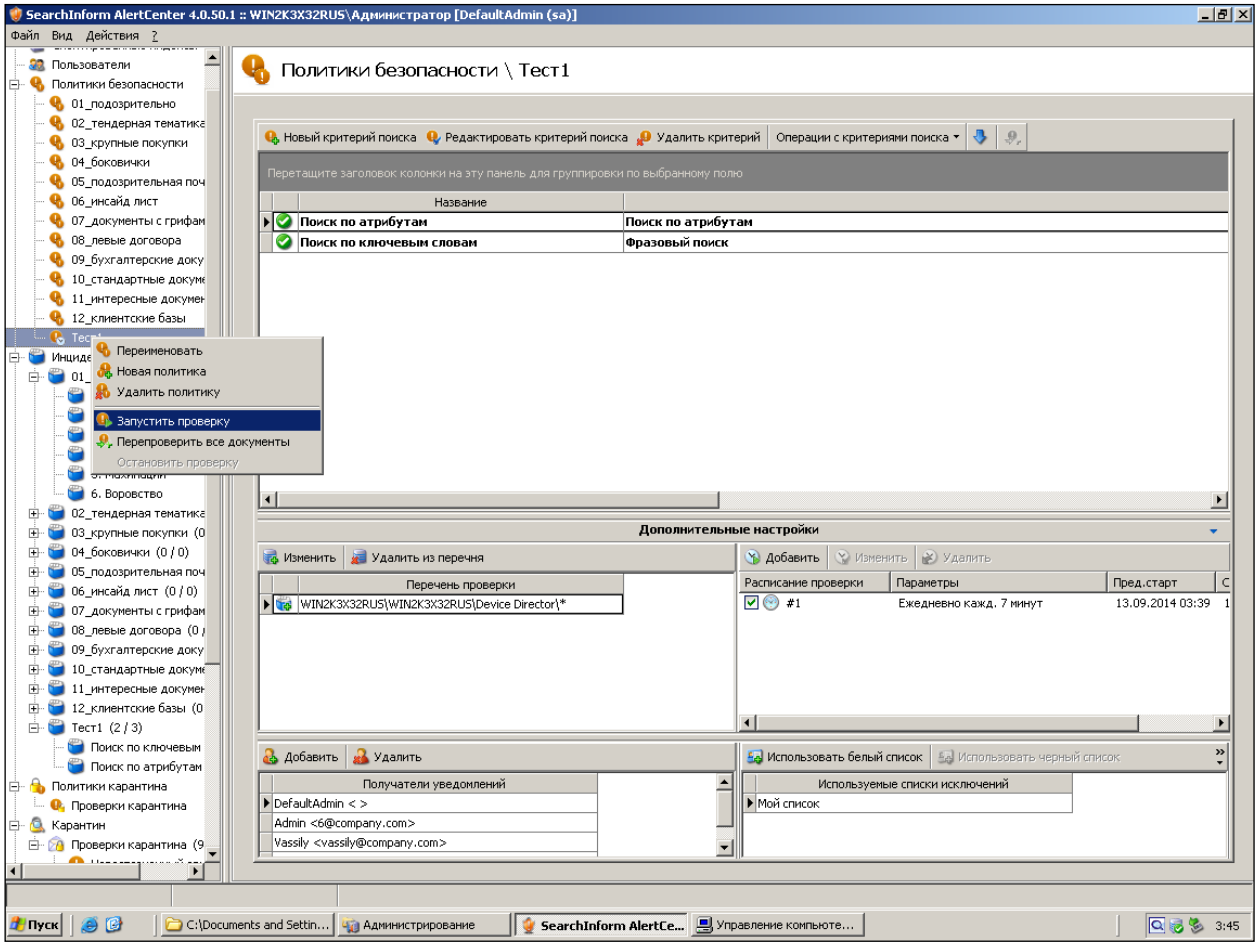

Рис.120 Принудительный запуск проверки политики «Тест1»

– В соответствии с рис. 121 отключить выполнение расписания политик безопасности «Тест1».

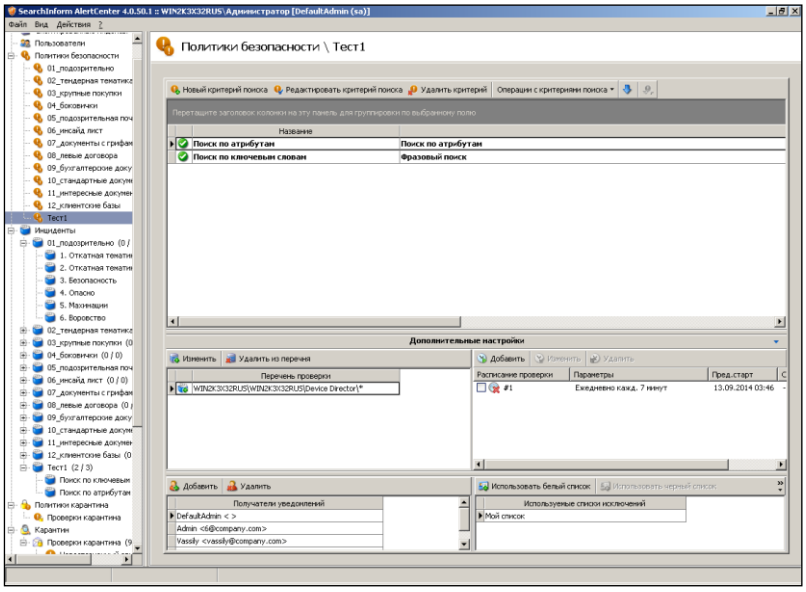

Рис. 121 Отключение выполенния расписания политики «Тест1»

- Закрыть окно AlertCenter Client.

- Завершить работу с виртуальным компьютером.

Задание для самостоятельной работы

- Отключить выполнения расписания политики «05_подозрительная почта».

- Сформировать параметры собственной политики безопасности, которые должны включать в себя: расписание проверки, список индексов для проверки, перечень белых списков, несколько простейших критериев поиска конфиденциальной информации.

- Согласовать параметры политики безопасности с преподавателем.

- Реализовать политику безопасности.

- Просмотреть перечень выявленных нарушений.

Контрольные вопросы

1. Зачем нужна фильтрация по прокси-серверам?
2. Зачем нужна фильтрация по почтовым серверам?
3. Чем отличается создание индекса от монтирования индекса?
4. Какие виды поиска рекомендуются для структурированных документов?
5. Какие виды поиска рекомендуются для не структурированных документов?
6. Что такое фильтр ограничений по перехвату?
7. Что такое «белый список»?
8. Как используется «разрешающий белый список»?
9. Как используется «запрещающий белый список»?
10. Чем отличается глобальный фильтр от фильтра по протоколам?
11. Зачем подключать AlertCenter к индексам?
12. Какой должен быть интервал обновления индексов?
13. Почему нужно отключать выполнение расписания политики?
14. Что такое активный индекс?
15. Что такое доступный индекс?