Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет инфокоммуникаций

Кафедра защиты информации

ПРОТИВОДЕЙСТВИЕ УТЕЧКЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Минск БГУИР 2018

УДК 004.056(076.5)
ББК 32.973.26-018.2я73
П83

А в т о р ы:

Т. В. Борботько, О. В. Бойправ, В. Е. Морозов, А. В. Дрозд

Р е ц е н з е н т ы:

кафедра автоматизированных систем управления войсками
учреждения образования «Военная академия Республики Беларусь»
(протокол №3 от 04.02.2018);

заведующий кафедрой телекоммуникационных систем
учреждения образования «Белорусская государственная академия связи»
кандидат технических наук, доцент С. И. Половеня

Противодействие утечке конфиденциальной информации. Лабора-
П 83 торный практикум : пособие / Т. В. Борботько [и др.]. – Минск : БГУИР, 2018. – 188 с. : ил.
ISBN 978-985-543-422-2.

Состоит из шести лабораторных работ, каждая из которых содержит краткие теоретические сведения, описание хода выполнения лабораторного задания, перечень задач для самостоятельной работы, вопросы для самоконтроля, ответы на которые оцениваются программной экспертной системой.

УДК 004.056(076.5)
ББК 32.973.26-018.2я73

ISBN 978-985-543-422-2

СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА №1
УСТАНОВКА И ПЕРВООЧЕРЕДНАЯ НАСТРОЙКА ПРОГРАММНОГО КОМПЛЕКСА SEARCHINFORM

Цель: освоить основные приемы использования программного комплекса SearchInform.

1.1. Теоретическая часть

1. Ознакомиться с приемами использования эмулятора виртуального компьютера VMware Player.
2. Ознакомиться с основными характеристиками операционной системы Windows Server 2003.
3. Ознакомиться с разделами 1–3 руководства аудитора безопасности системы SearchInform.

1.2. Лабораторное задание

1. Установить программный комплекс VMware Player. Рекомендуется установить VMware-player-6.0.7, предназначенный для бесплатного использования в личных целях. Плеер доступен для скачивания по ссылке http://www.vmware.com/ru/products/player. Установка предполагает использование на основном компьютере операционных систем семейства Windows.

В указанную преподавателем папку скопировать образ компьютера с операционной системой Windows Server и установленной системой SearchInform (папка VMwareSI).

Запустить VMware Player, окно которого показано на рис. 1.1.

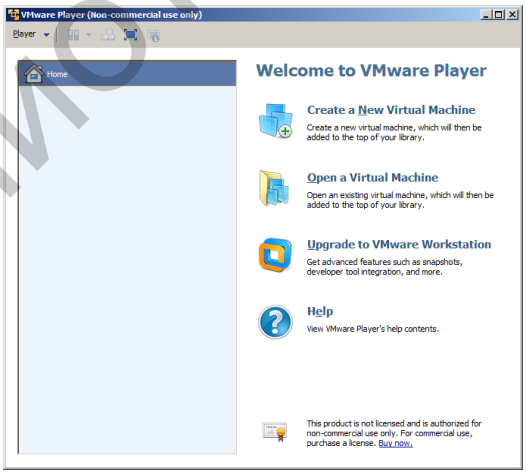


Рис. 1.1. Окно VMware Player

Используя VMware Player, в соответствии с рис. 1.2–1.4 запустить виртуальный компьютер. В дальнейшем вся работа выполняется только на виртуальном компьютере, окно которого показано на рис. 1.5. На выданном преподавателем образе компьютера использованы следующие пароли: 1111, 13, Admin.

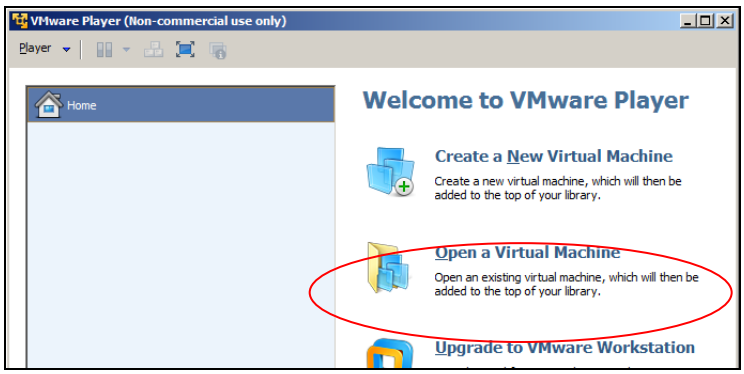


Рис. 1.2. Открытие файла образа

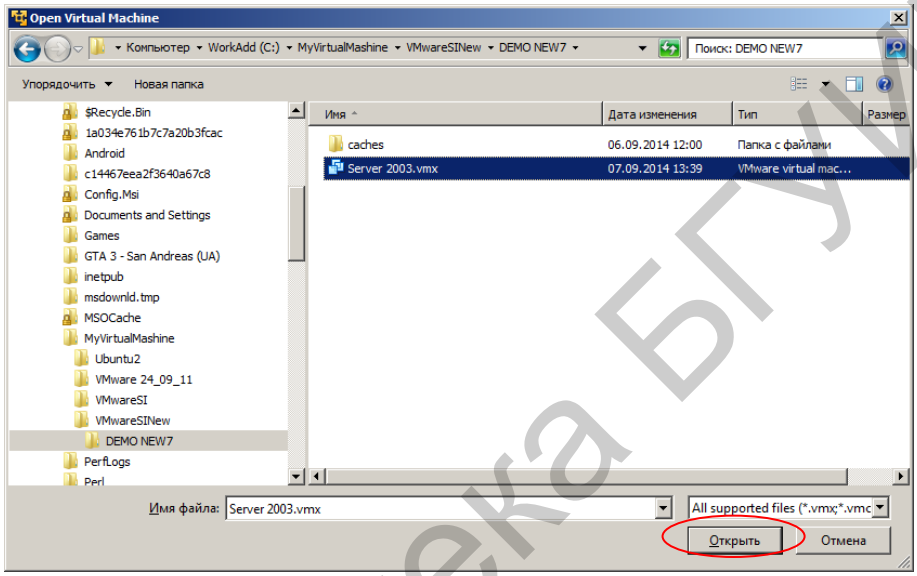


Рис. 1.3. Выбор файла образа

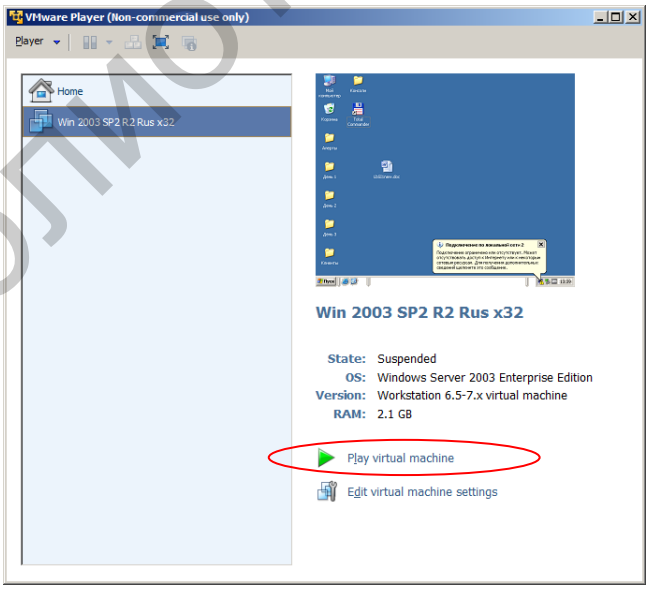


Рис. 1.4. Запуск виртуального компьютера

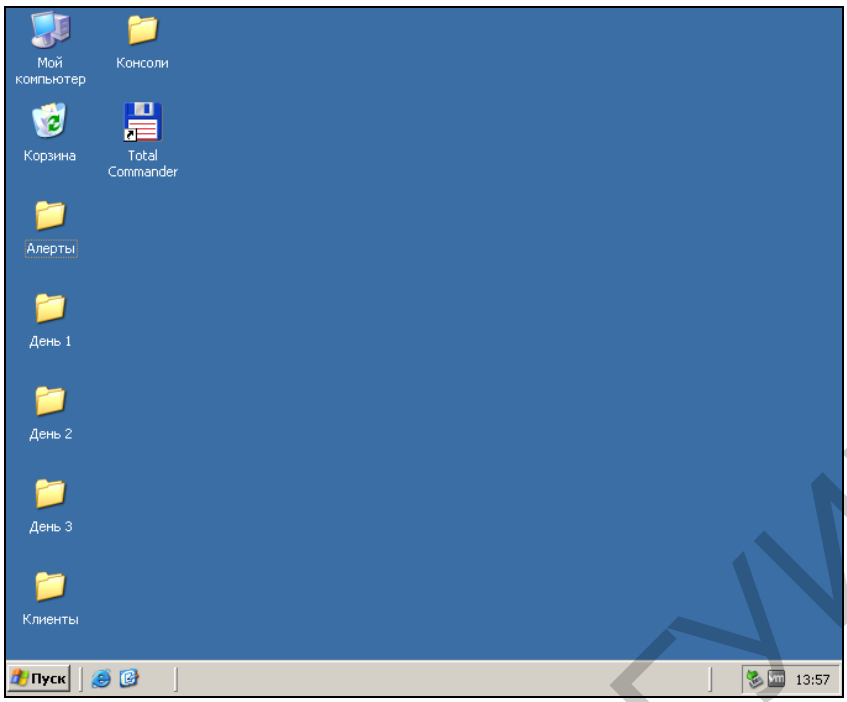


Рис. 1.5. Окно виртуального компьютера

Рекомендуется установить на виртуальном компьютере разрешение экрана 1152×864.

2. Установить собственный пароль на учетную запись администратора операционной системы Windows Server. Для этого выполнить следующее.

В соответствии с рис. 1.6–1.8 следует запустить оснастку управления компьютером.

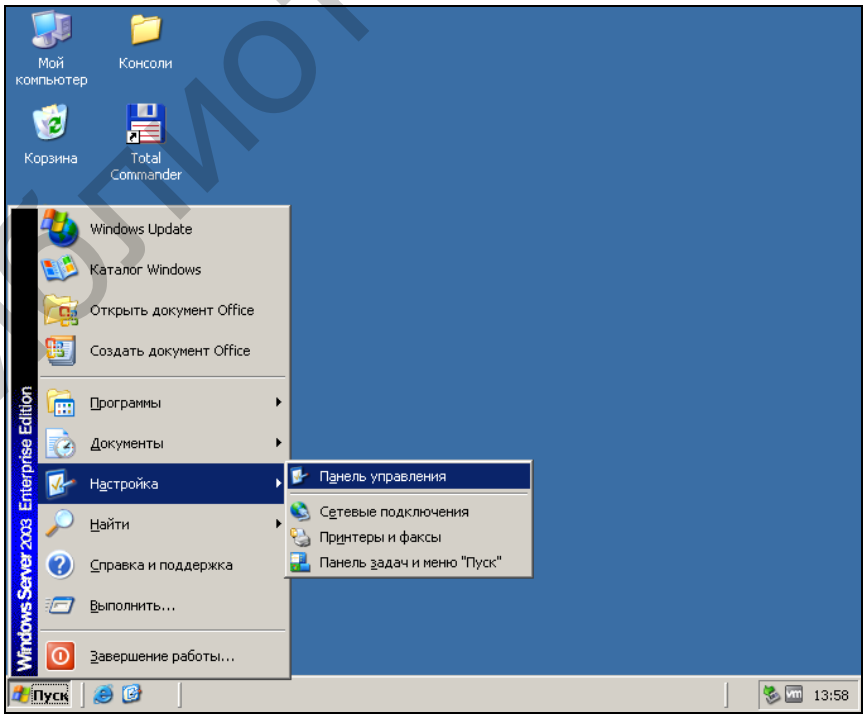


Рис. 1.6. Запуск панели управления

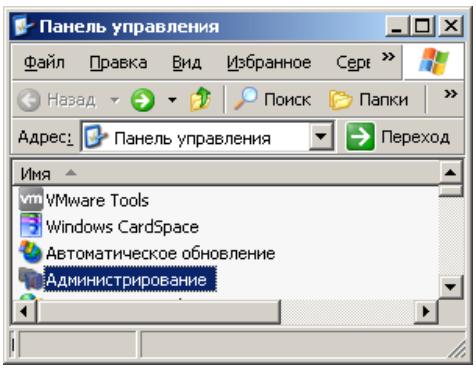


Рис. 1.7. Запуск оснастки администрирования

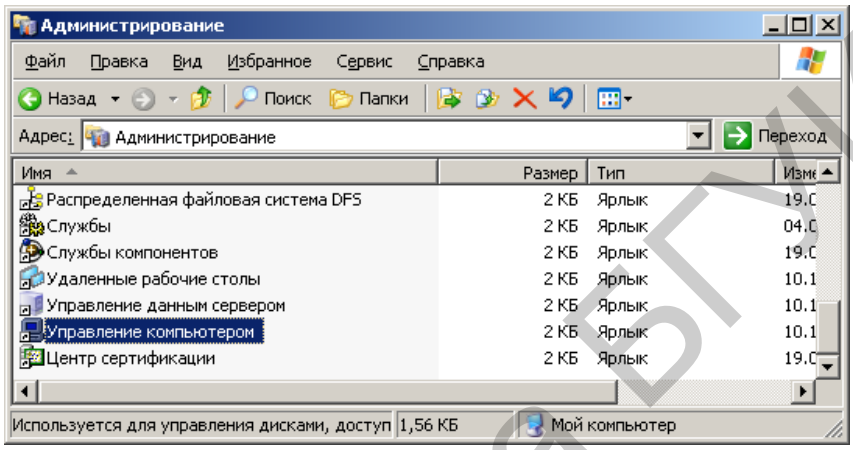


Рис. 1.8. Запуск оснастки управления компьютером

В соответствии с рис. 1.9–1.11 входим в режим изменения парольных данных администратора системы.

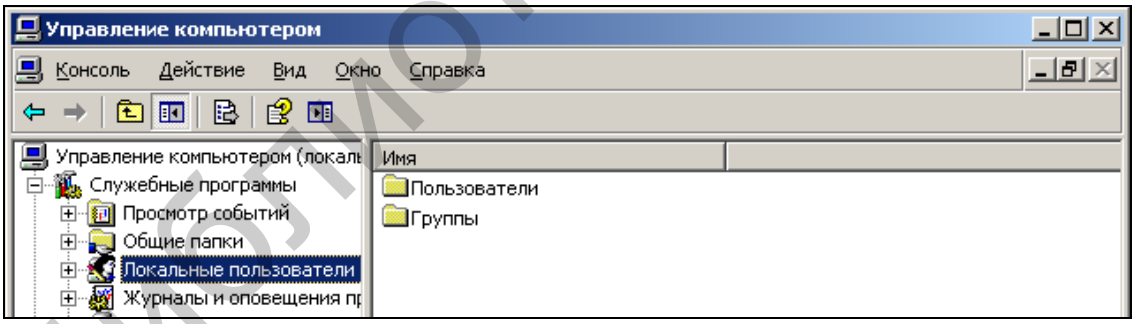


Рис. 1.9. Переход к режиму изменения параметров локальных пользователей

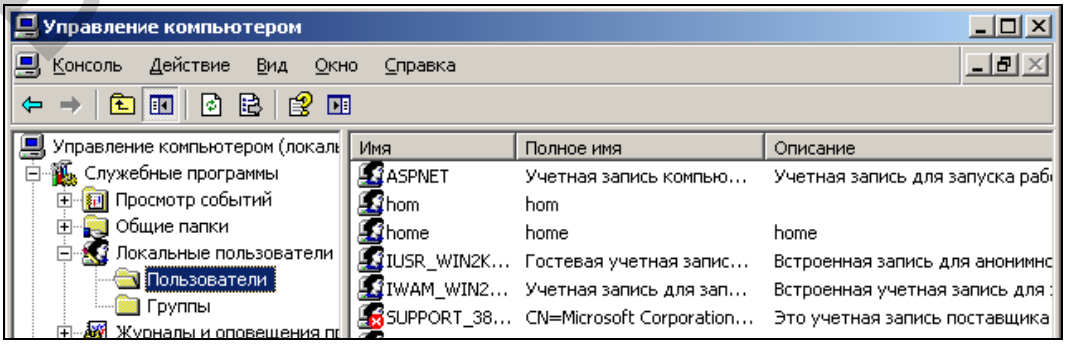


Рис. 1.10. Окно редактирования параметров локальных пользователей

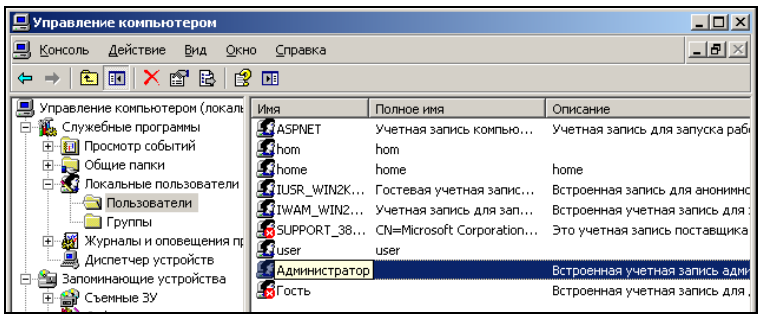


Рис. 1.11. Вход в режим редактирования параметров администратора системы

В соответствии с рис. 1.12–1.16 устанавливаем пароль для учетной записи пользователя «Администратор» (для учебных целей рекомендуется устанавливать простые пароли – 1111, 1234 и т. д.).

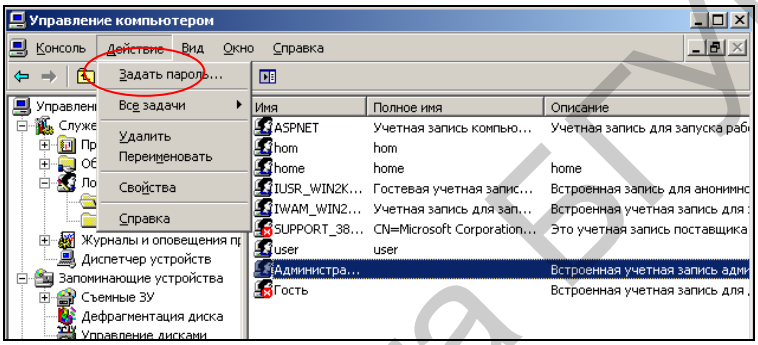


Рис. 1.12. Вход в режим редактирования парольных данных

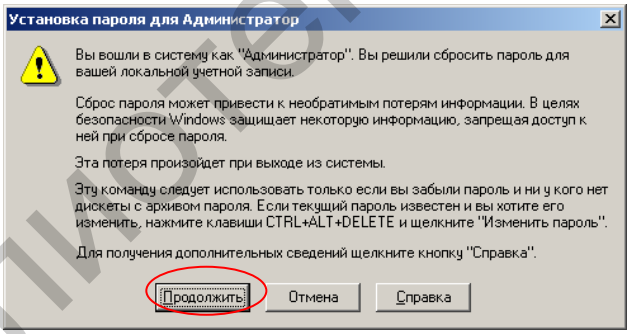


Рис. 1.13. Первый этап изменения парольных данных

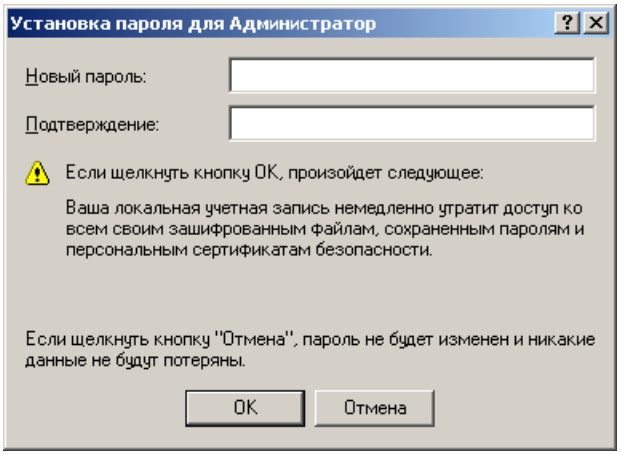


Рис. 1.14. Окно ввода парольных данных

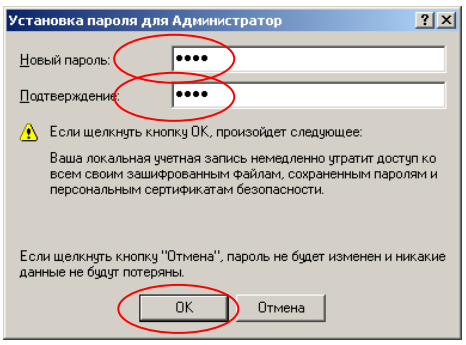


Рис. 1.15. Ввод собственных парольных данных

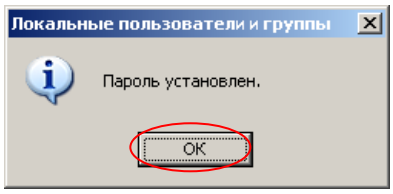


Рис. 1.16. Индикация установки пароля

В соответствии с рис. 1.17–1.19 изменяем свойства учетной записи администратора.

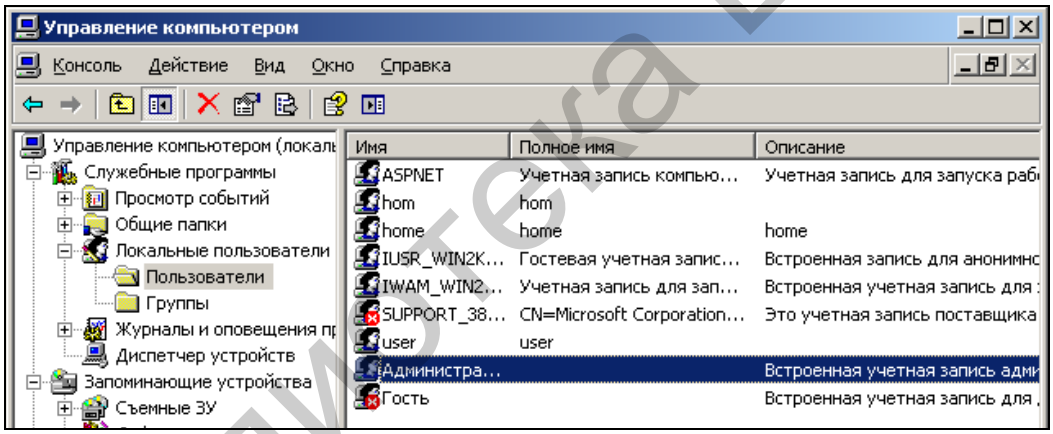


Рис. 1.17. Переход к редактированию параметров парольных данных

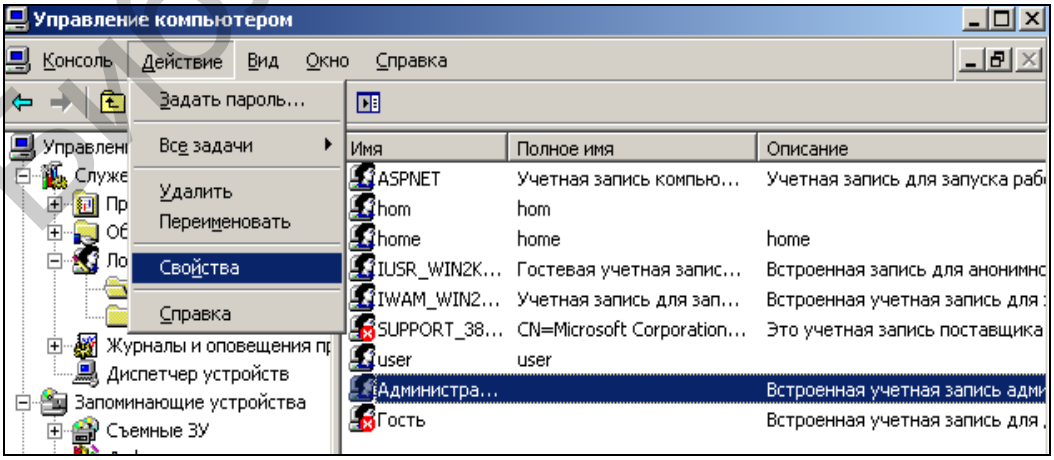


Рис. 1.18. Вызов меню изменения свойств учетной записи

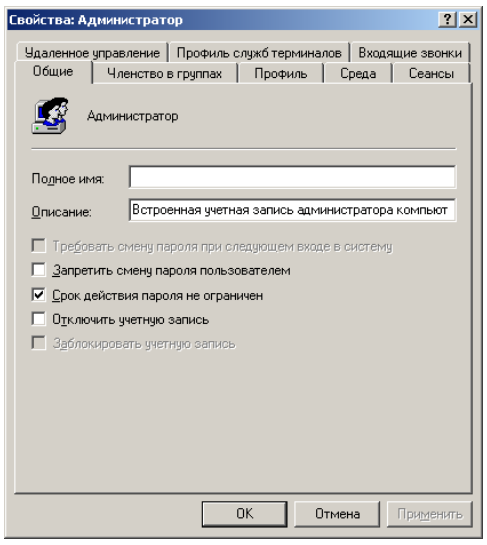


Рис. 1.19. Изменение параметров учетной записи

Выйти из режима редактирования параметров виртуального компьютера. В соответствии с рис. 1.20–1.23 перезагрузить виртуальный компьютер.

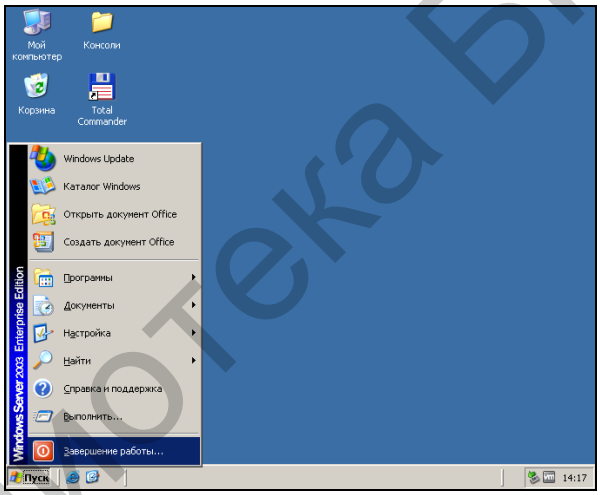


Рис. 1.20. Первый этап перезагрузки

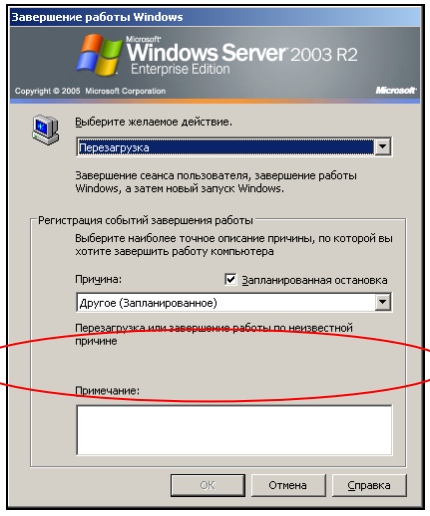


Рис. 1.21. Второй этап перезагрузки

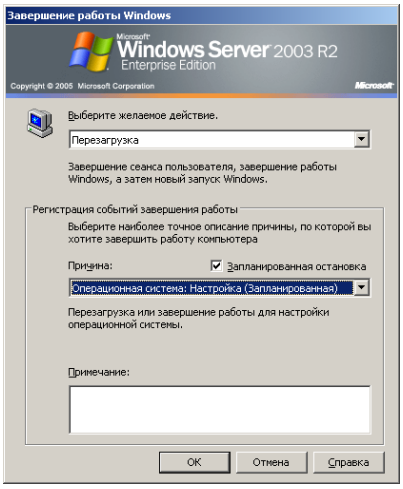


Рис. 1.22. Третий этап перезагрузки

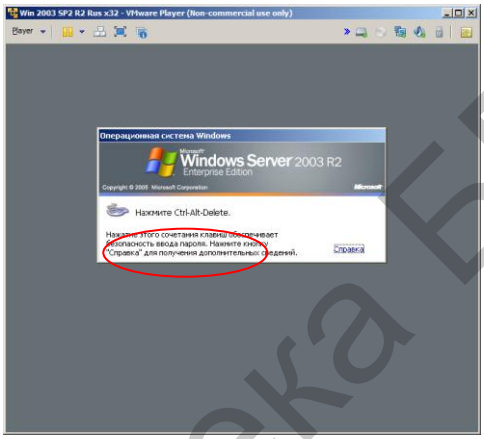


Рис. 1.23. Четвертый этап перезагрузки

Особенность перезагрузки виртуального компьютера заключается в том, что нажатие комбинации клавиш Ctrl+Alt+Delete сначала обрабатывается операционной системой основного компьютера, а уже потом виртуального. Поэтому после нажатия Ctrl+Alt+Delete сначала необходимо закрыть появившееся окно на основном компьютере, а после этого, в соответствии с рис. 1.24, войти в систему, используя новые учетные данные.

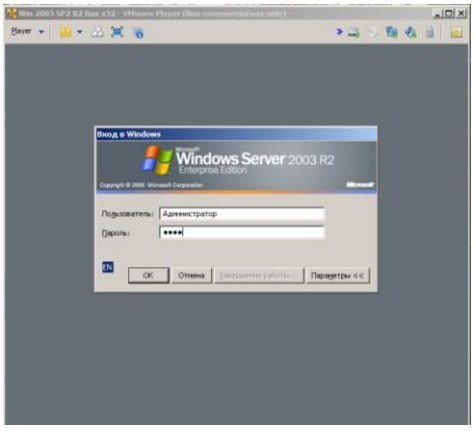


Рис. 1.24. Вход в виртуальную систему с использованием собственных учетных данных

3. С использованием встроенных средств защиты SearchInform изменить пароли доступа к консолям основных серверов (по умолчанию пароль Admin). Для этого выполнить следующее.

Открыть расположенную на рабочем столе папку «Консоли».

С помощью соответствующего ярлыка запустить консоль Search Server (рис. 1.25).

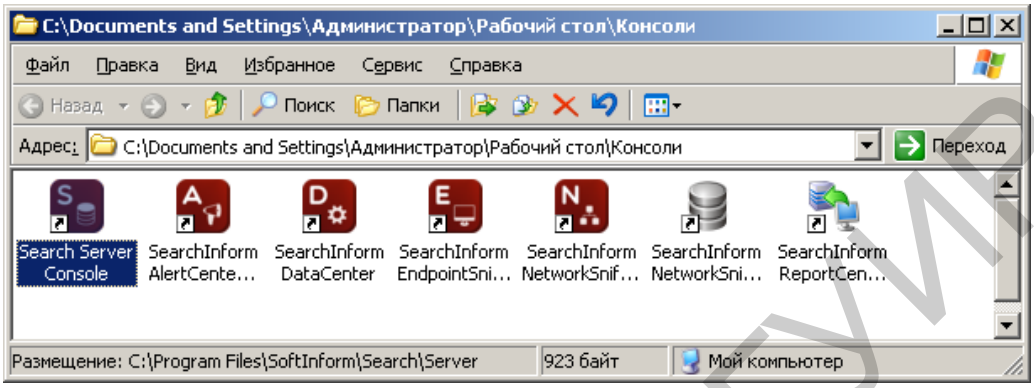


Рис. 1.25. Запуск консоли Search Server

В соответствии с рис. 1.26–1.28 войти в консоль Search Server.

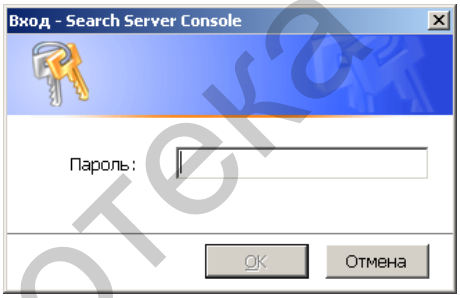


Рис. 1.26. Окно запроса пароля консоли Search Server

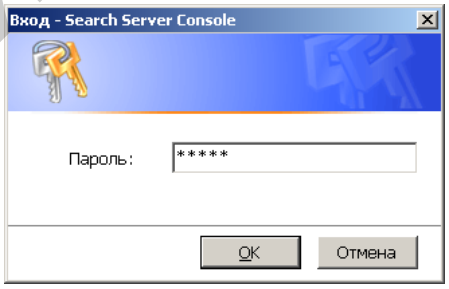


Рис. 1.27. Ввод стандартного пароля Admin в консоль Search Server

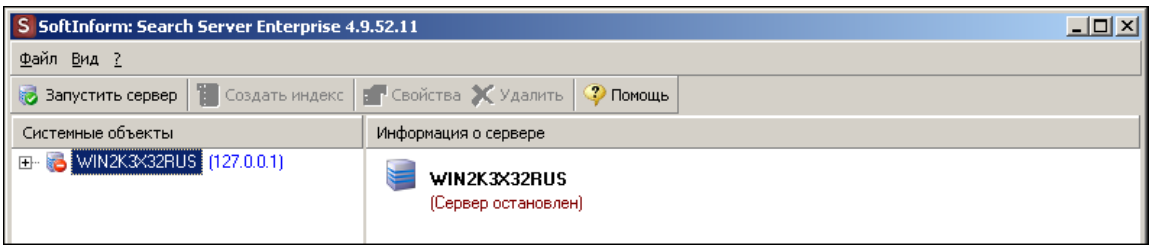


Рис. 1.28. Окно консоли Search Server

В соответствии с рис. 1.29 и 1.30 задать новый пароль консоли Search Server. В примере, показанном на рис. 1.30, использован пароль 123456. При этом была выбрана необязательная опция «Показывать пароль». Также отметим, что в поле «Пароль» (см. рис. 1.30) вводится старый пароль Admin.

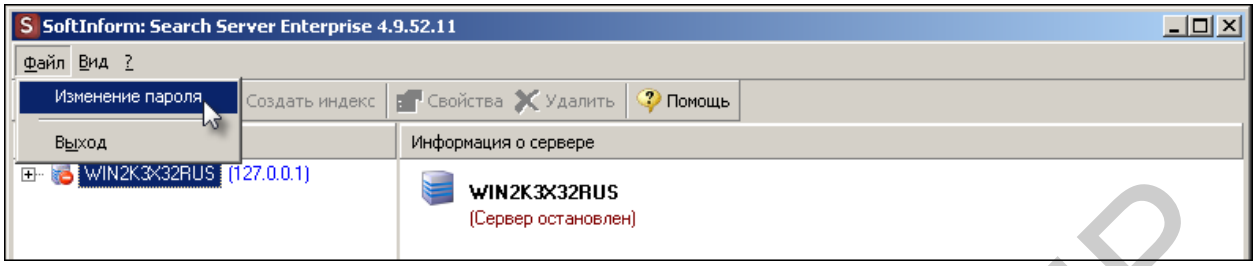


Рис. 1.29. Использование меню изменения пароля консоли Search Server

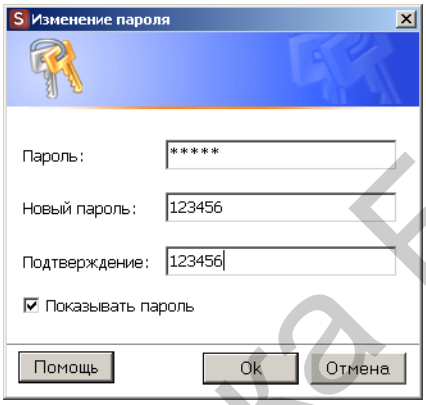


Рис. 1.30. Ввод парольных данных консоли Search Server

Закрыть консоль Search Server.

С помощью соответствующего ярлыка, размещенного в папке «Консоли», запустить консоль SearchInform DataCenter.

В соответствии с рис. 1.31 и 1.32 войти в консоль SearchInform DataCenter.

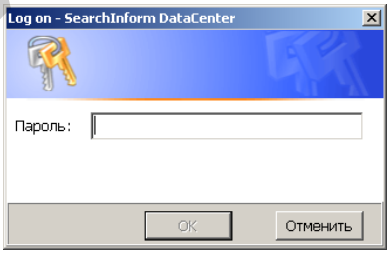


Рис. 1.31. Окно запроса пароля консоли SearchInform DataCenter

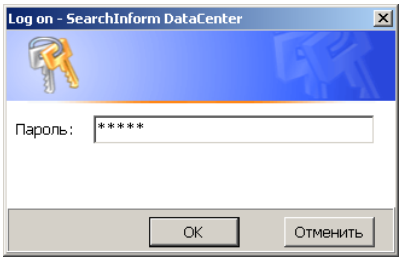


Рис. 1.32. Ввод стандартного пароля Admin в консоль SearchInform DataCenter

В соответствии с рис. 1.33–1.36 задать новый пароль консоли SearchInform DataCenter. В примере, показанном на рис. 1.35, использован пароль 123456. При этом была выбрана необязательная опция «Показывать пароль».

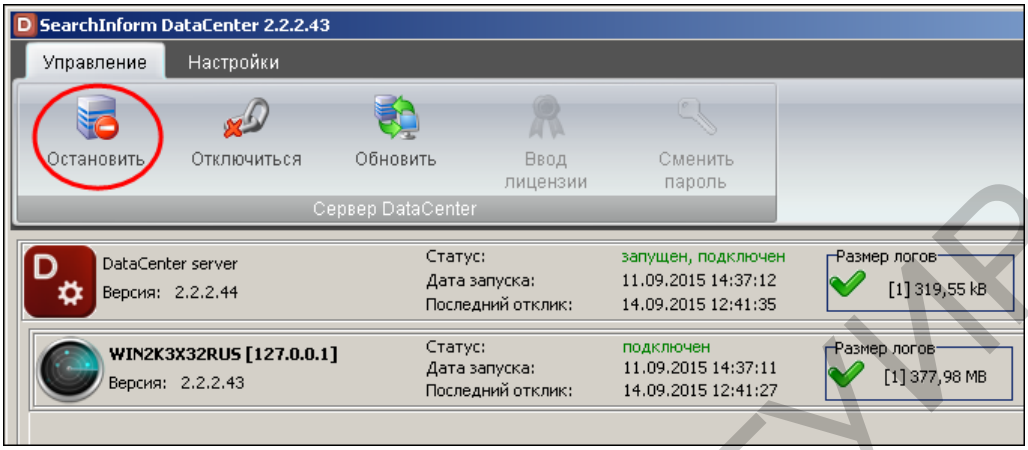


Рис. 1.33. Остановка SearchInform DataCenter

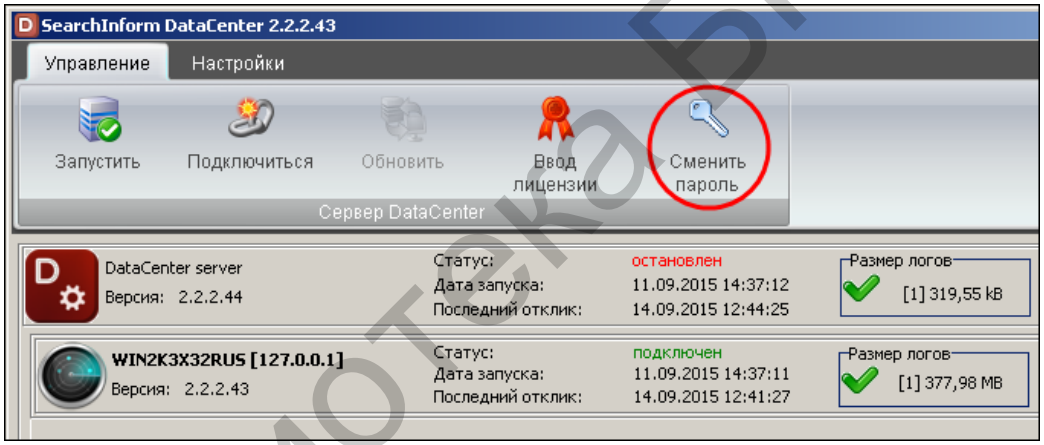


Рис. 1.34. Использование кнопки изменения пароля SearchInform DataCenter

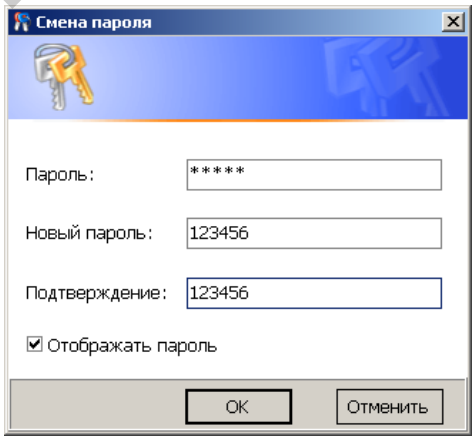


Рис. 1.35. Ввод парольных данных консоли DataCenter

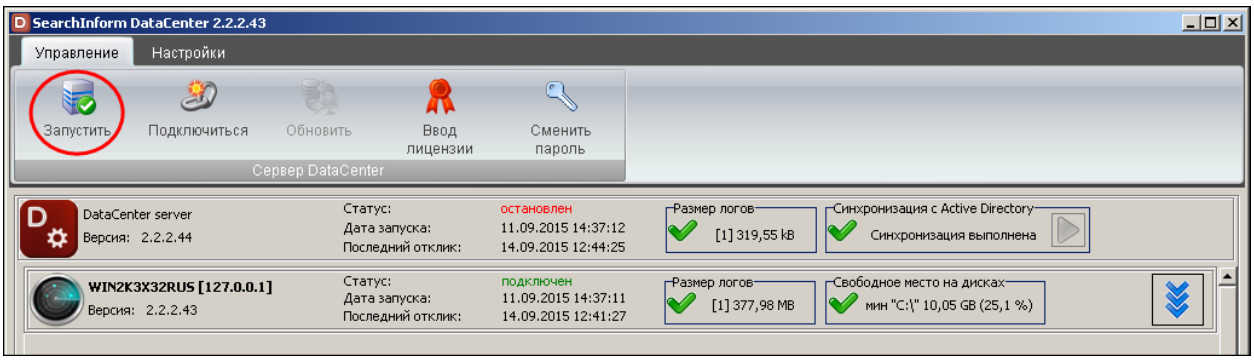


Рис. 1.36. Запуск SearchInform DataCenter

Закрыть консоль DataCenter.

С помощью соответствующего ярлыка, размещенного в папке «Консоли», запустить консоль SearchInform EndpointSniffer.

По аналогии с рис. 1.31 и 1.32 войти в консоль SearchInform EndpointSniffer.

В соответствии с рис. 1.37 и 1.35 задать новый пароль консоли EndpointSniffer.

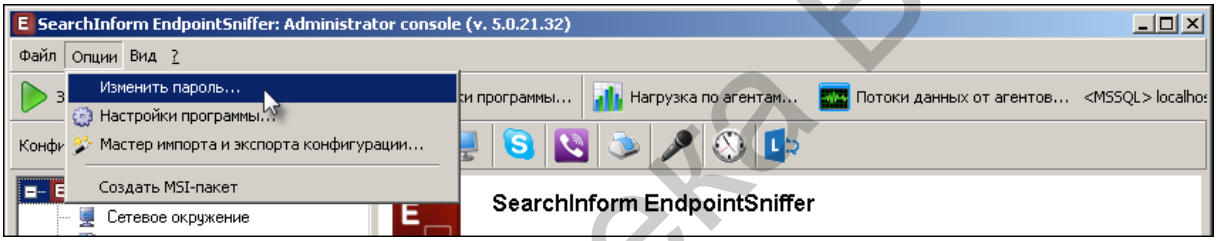


Рис. 1.37. Использование меню изменения пароля консоли EndpointSniffer

Закрыть консоль EndpointSniffer.

С помощью соответствующего ярлыка, размещенного в папке «Консоли», запустить SearchInform NetworkSniffer.

По аналогии с рис. 1.31 и 1.32 войти в NetworkSniffer.

В соответствии с рис. 1.38 и 1.35 задать новый пароль NetworkSniffer.

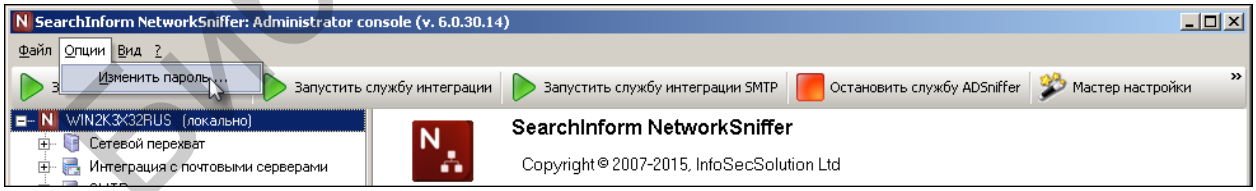


Рис. 1.38. Использование меню изменения пароля консоли NetworkSniffer

Закрыть консоль NetworkSniffer.

С помощью соответствующего ярлыка, размещенного в папке «Консоли», запустить SearchInform ReportCenter Console.

По аналогии с рис. 1.31 и 1.32 войти в SearchInform ReportCenter Console.

В соответствии с рис. 1.39 и 1.35 задать новый пароль SearchInform ReportCenter Console.

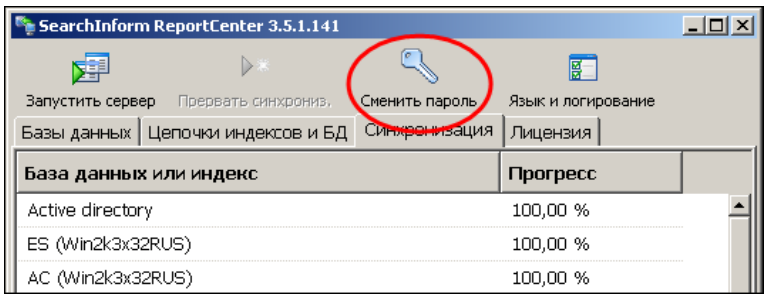


Рис. 1.39. Использование кнопки изменения пароля консоли ReportCenter

Закрыть консоль ReportCenter.

Открыть находящуюся на рабочем столе папку «Клиенты» (рис. 1.40) и с помощью ярлыка «SearchInform AlertCenter Client» запустить соответствующую службу. Окно службы показано на рис. 1.41.

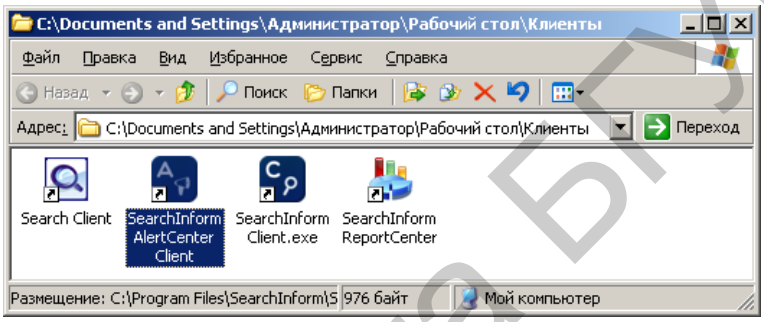


Рис. 1.40. Окно папки «Клиенты»

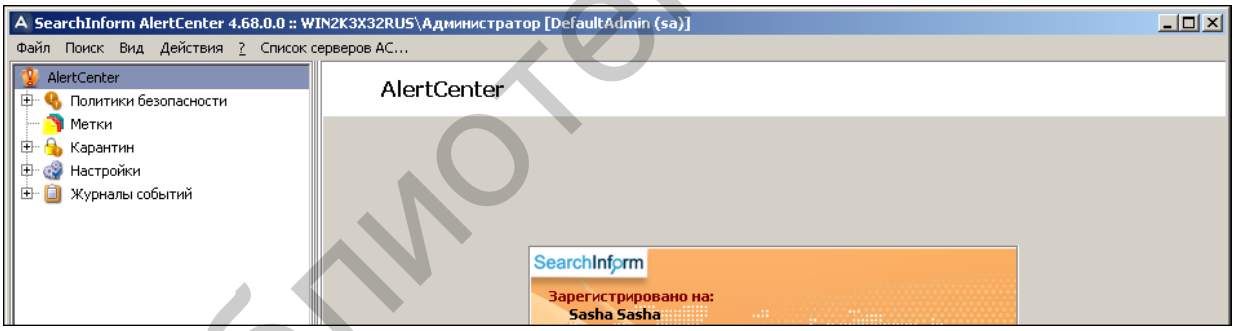


Рис. 1.41. Окно службы AlertCenter Client

В соответствии с рис. 1.42–1.46 установить пароль на использование службы «SearchInform AlertCenter Client».

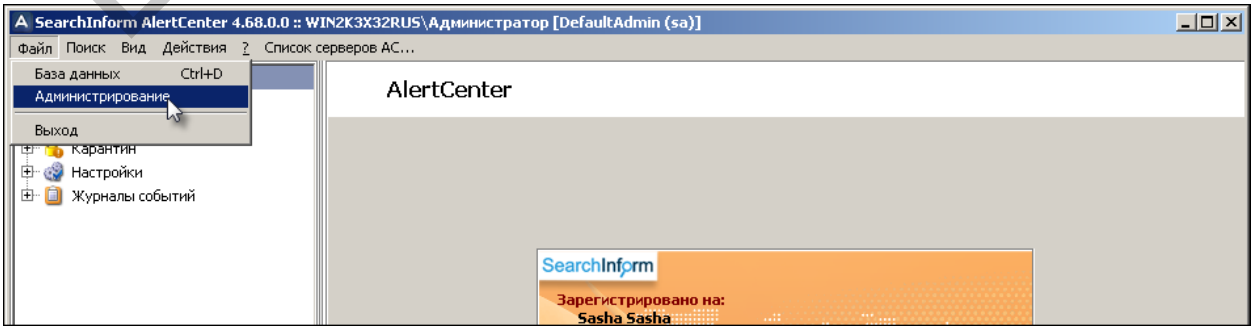


Рис. 1.42. Использование меню администрирования службы AlertCenter Client

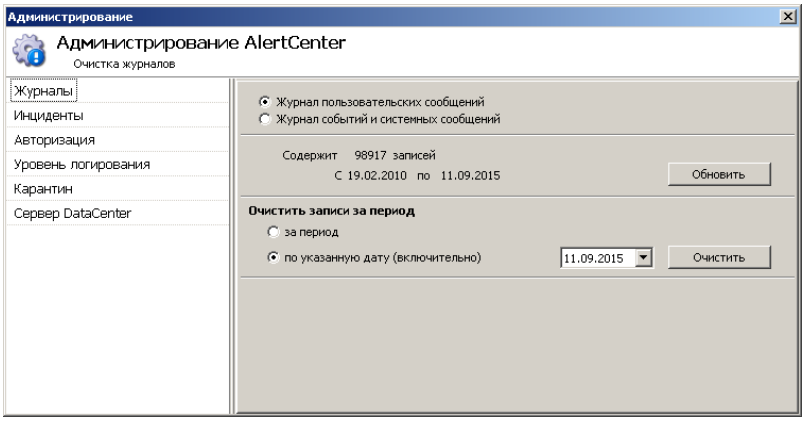


Рис. 1.43. Окно администрирования AlertCenter Client

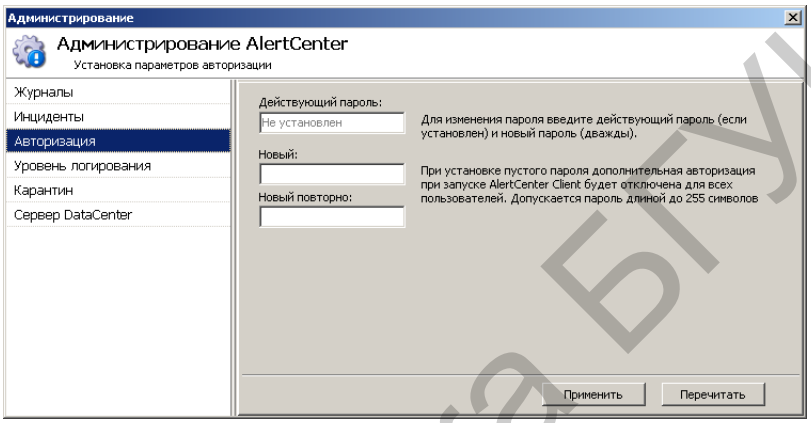


Рис. 1.44. Выбор опции авторизации AlertCenter Client

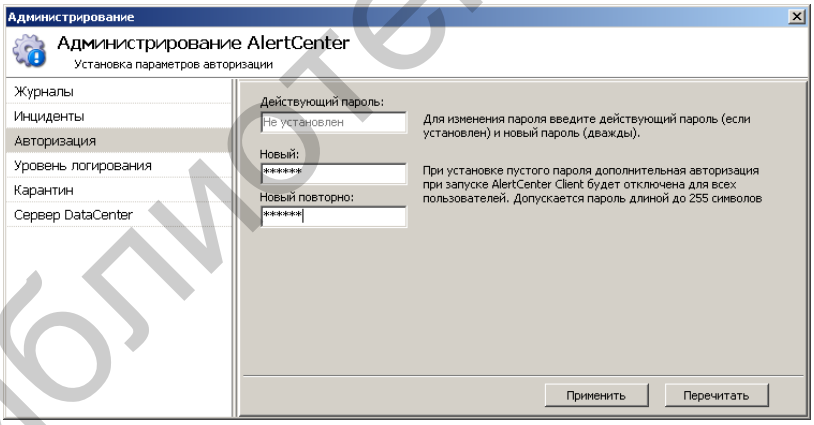


Рис. 1.45. Установка пароля AlertCenter Client

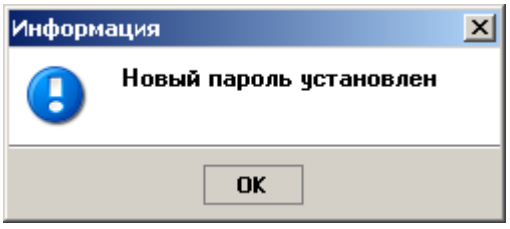


Рис. 1.46. Окно подтверждения установки пароля AlertCenter Client

Закрыть окно службы AlertCenter Client.

4. Ограничить права доступа пользователей к индексам Search Server. Для этого выполнить следующее.

С помощью соответствующего ярлыка, размещенного в папке «Консоли», запустить консоль Search Server. При необходимости ввести пароль.

В соответствии с рис. 1.47 запустить сервер.

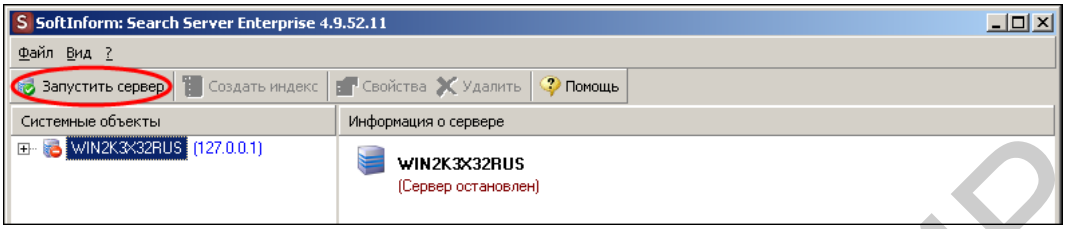


Рис. 1.47. Запуск сервера Search Server

В соответствии с рис. 1.48 выбрать индекс и нажать кнопку «Свойства».

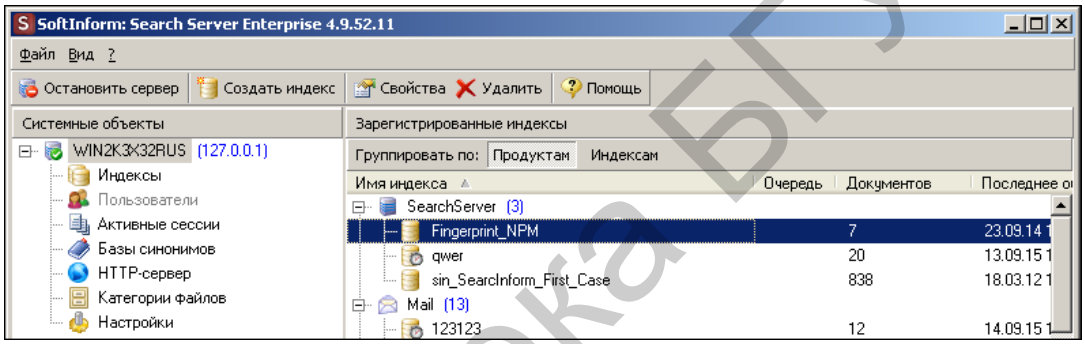


Рис. 1.48. Переход в редактирование свойств индекса

В соответствии с рис. 1.49–1.56 установить возможность доступа к данному индексу только пользователям операционной системы, которые относятся к группе «Администраторы».

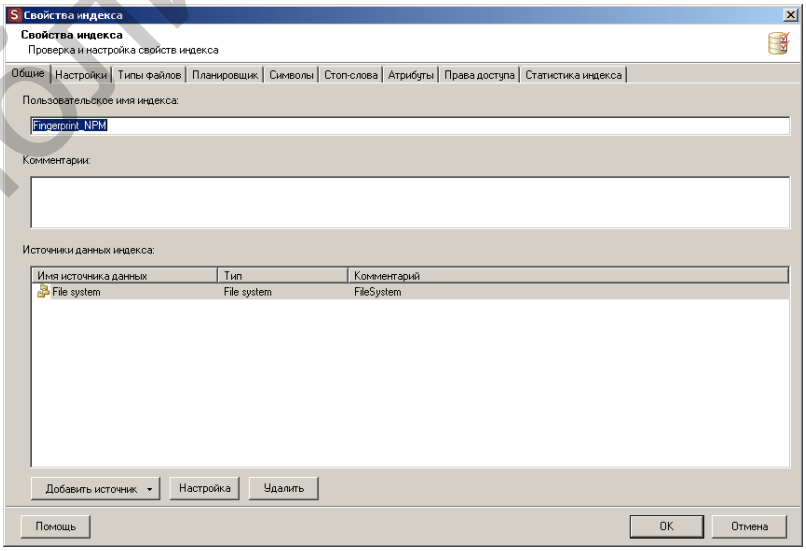


Рис. 1.49. Окно свойств индекса

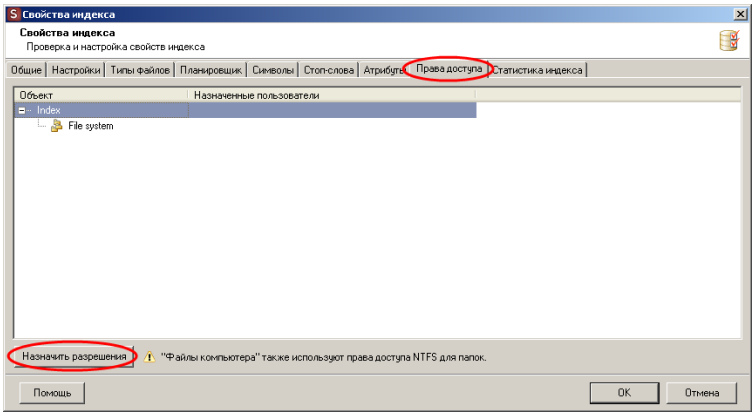


Рис. 1.50. Переход в редактирование прав доступа к индексу

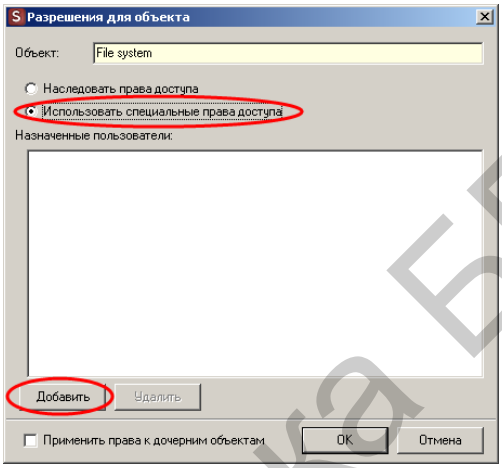


Рис. 1.51. Переход в редактирование списка пользователей индекса

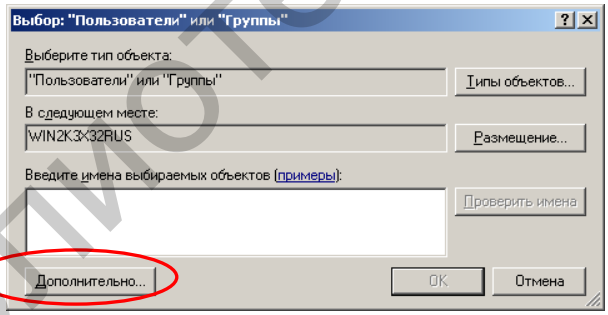


Рис. 1.52. Первый этап поиска пользователей

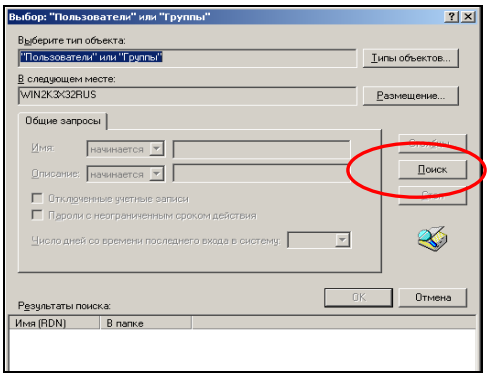


Рис. 1.53. Второй этап поиска пользователей

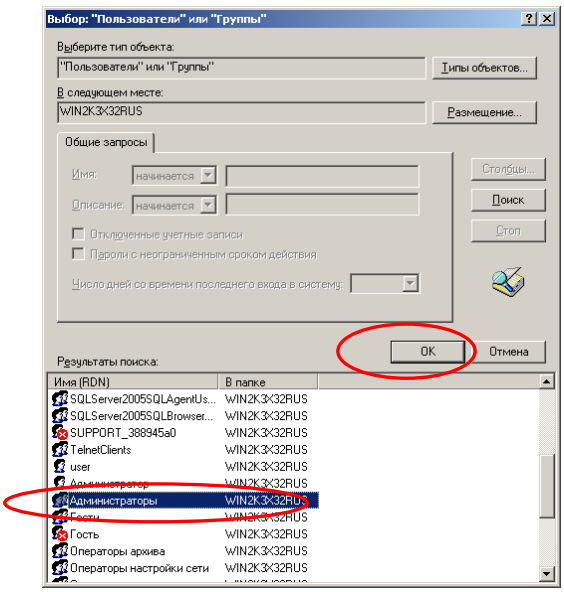


Рис. 1.54. Выбор группы «Администраторы»

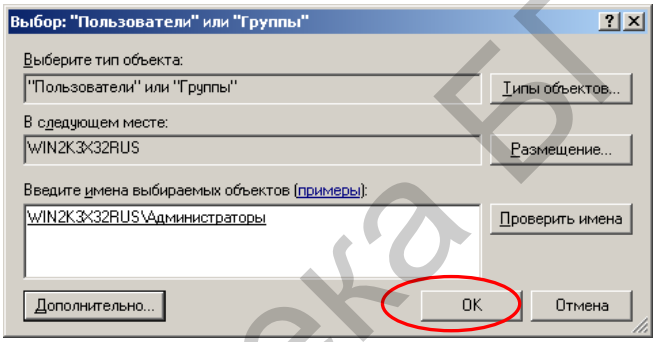


Рис. 1.55. Подтверждение выбора группы «Администраторы»

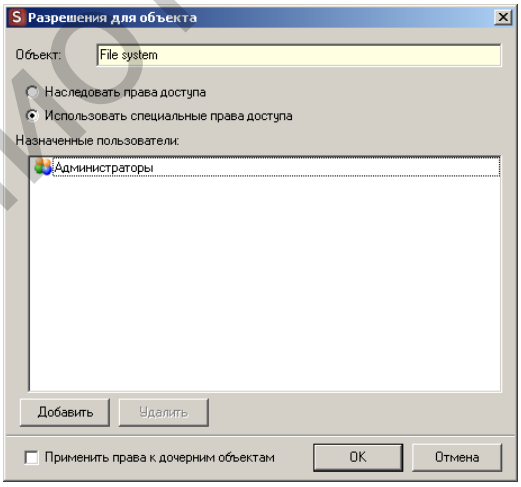


Рис. 1.56. Индикация возможности доступа
к индексу группе «Администраторы»

Закрыть консоль Search Server.

5. Управление пользователями системных служб SearchInform.

Установить, что служба AlertCenter работает от имени пользователя «Администратор». Для этого выполнить следующее.

Открыть окно панели управления ОС Windows Server (команды Пуск→Настройка→Панель управления).

В соответствии с рис. 1.57 запустить оснастку «Администрирование».

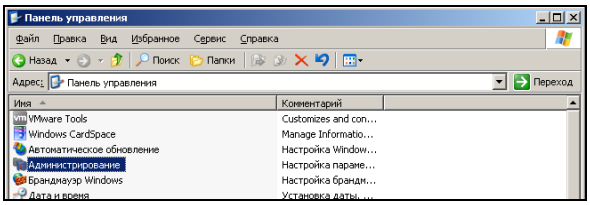


Рис. 1.57. Выбор оснастки «Администрирование»

В новом окне, показанном на рис. 1.58, запустить компонент «Службы».

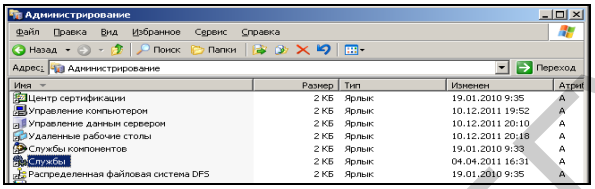


Рис. 1.58. Выбор компонента «Службы»

В соответствии с рис. 1.59 вызвать контекстное меню службы SearchInform AlertCenter server.

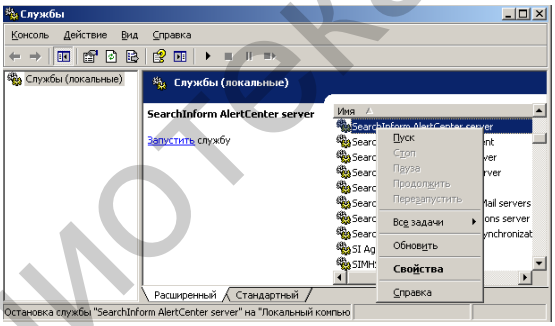


Рис. 1.59. Вызов контекстного меню службы SearchInform AlertCenter server

В контекстном меню выбрать команду «Свойства». В окне, показанном на рис. 1.60, перейти на вкладку «Вход в систему» (рис. 1.61).

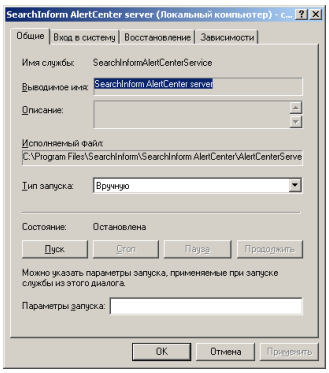


Рис. 1.60. Окно свойств службы, вкладка «Общие»

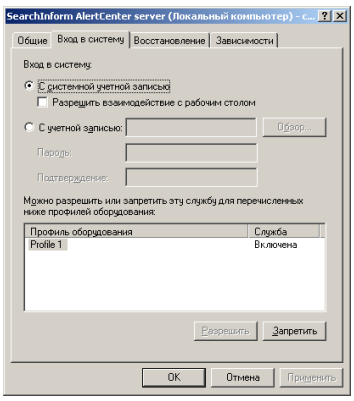


Рис. 1.61. Окно свойств службы, вкладка «Вход в систему»

Следовать инструкциям, показанным на рис. 1.62–1.70.

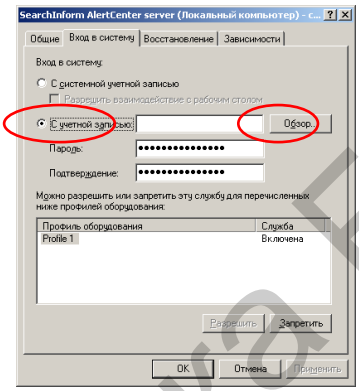


Рис. 1.62. Первый этап выбора пользователя «Администратор»

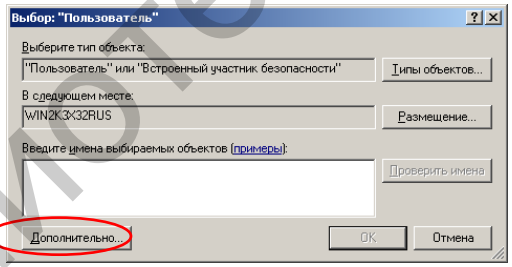


Рис. 1.63. Второй этап выбора пользователя «Администратор»

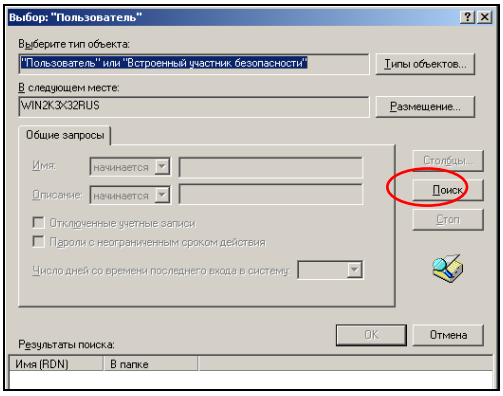


Рис. 1.64. Третий этап выбора пользователя «Администратор»

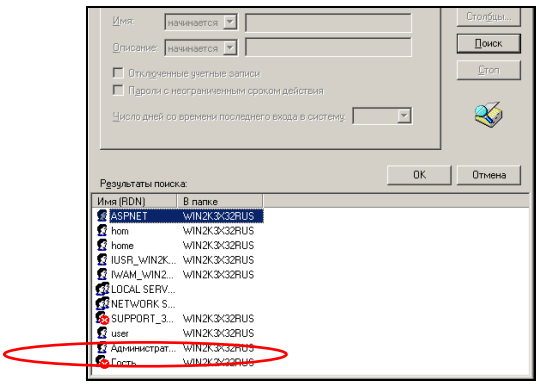


Рис. 1.65. Четвертый этап выбора пользователя «Администратор»

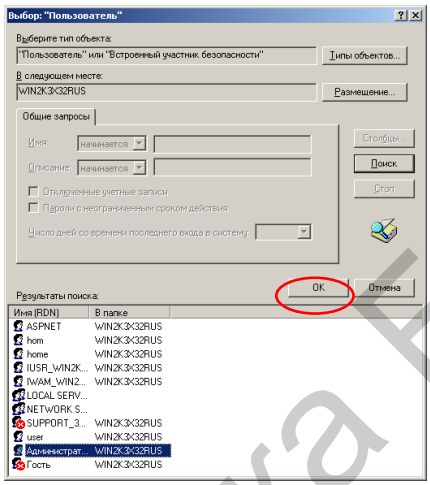


Рис. 1.66. Пятый этап выбора пользователя «Администратор»

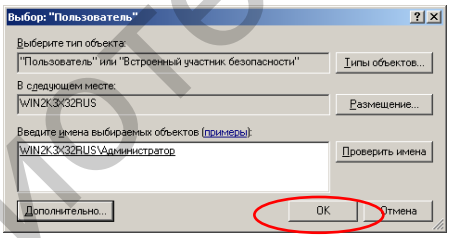
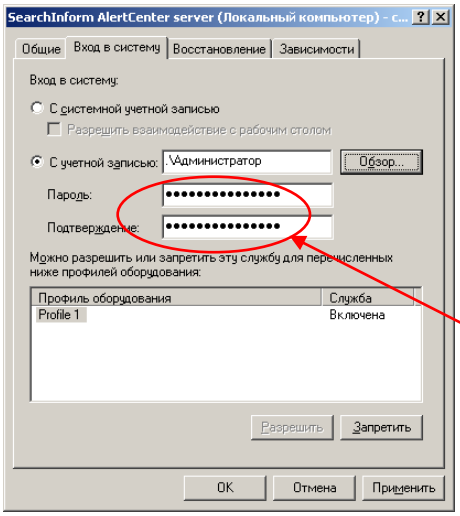


Рис. 1.67. Подтверждение выбора пользователя «Администратор»



Необходимо ввести пароль администратора

Рис. 1.68. Ввод парольных данных пользователя «Администратор»

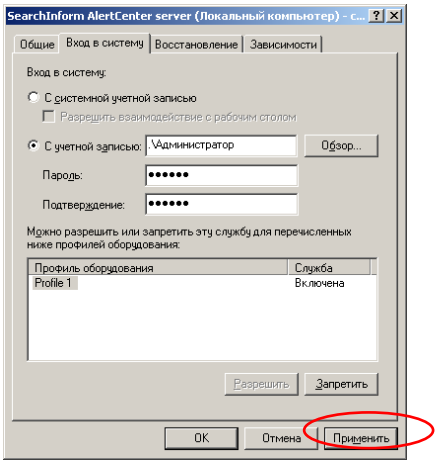


Рис. 1.69. Окончание ввода парольных данных пользователя «Администратор»

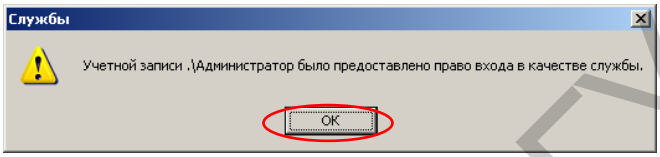


Рис. 1.70. Подтверждение входа в систему службы SearchInform AlertCenter server от имени пользователя «Администратор»

Закрыть окна «Службы» и «Администрирование».

При необходимости (уточнить у преподавателя) по аналогии с SearchInform AlertCenter установить, что службы SearchInform DataCenter: agent, DataCenter: server, DeviceSniffer Server, SearchInform NetworkSniffer, SearchInform NetworkSniffer Mail servers integration, SearchInform Regular Expressions server, SearchInform ReportCenter: synchronization service, SoftInform Search Server, SQL Server (MSSQLSERVER), SQL Server VSS Writer также работают от имени пользователя «Администратор».

Если предыдущий пункт не выполнялся (службы не работают в режиме «Администратор»), то установить, что служба SearchInform AlertCenter server работает с системной учетной записью (рис. 1.71).

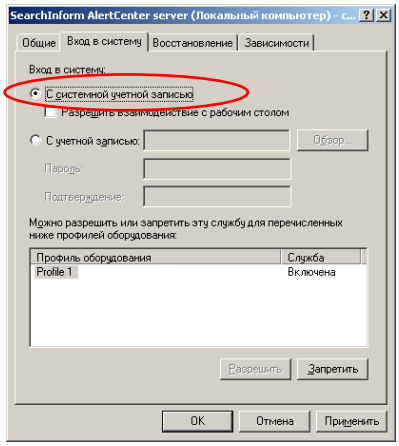


Рис. 1.71. Установка входа в систему службы SearchInform AlertCenter server с системной учетной записью

6. Настроить параметры функционирования SearchInform AlertCenter. Для этого выполнить следующее.

Запустить консоль «SearchInform AlertCenter Console». При необходимости ввести пароль (пароль по умолчанию Admin).

В соответствии с рис. 1.72 и 1.73 проверить соединение с базой данных.

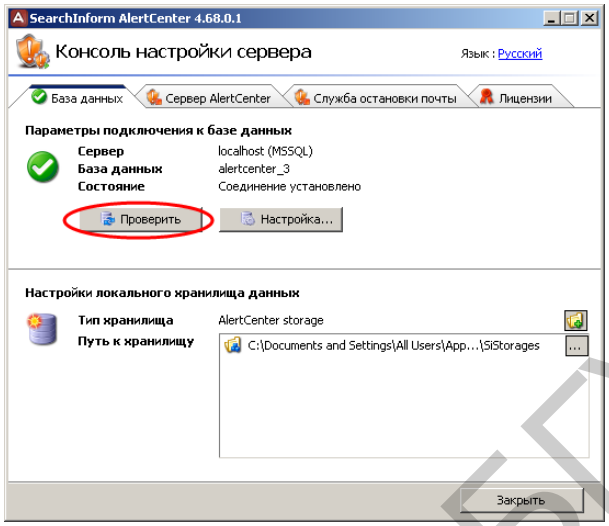


Рис. 1.72. Проверка соединения с базой данных

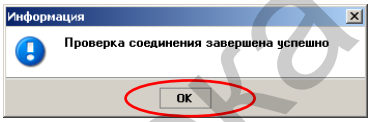


Рис. 1.73. Индикация успешного соединения с базой данных

В соответствии с рис. 1.74–1.76 просмотреть параметры соединения с системой управления базами данных.

Проверить соединения с базами данных, перечисленными в списке (рис. 1.74). Для этого следует из списка выбрать базу данных и нажать кнопку «Проверить подключение».

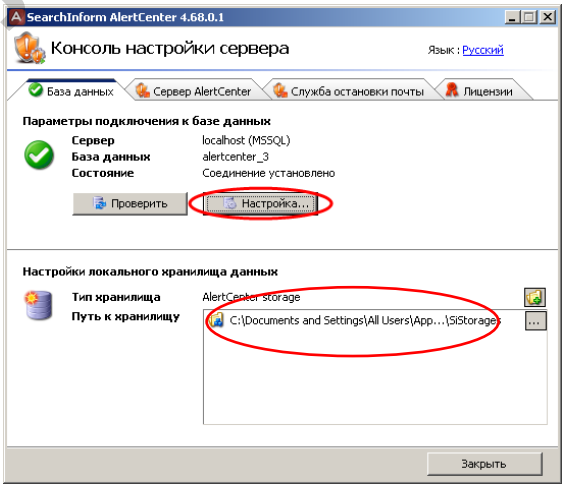


Рис. 1.74. Вход в режим настройки соединения с базой данных

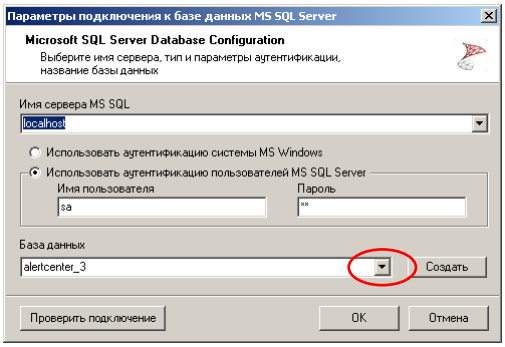


Рис. 1.75. Окно настройки соединения с базой данных

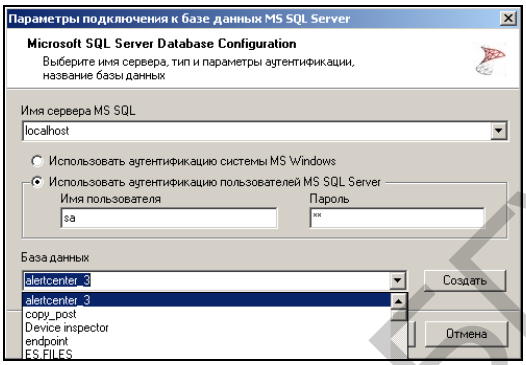


Рис. 1.76. Выбор базы данных для соединения

Выбрав базу данных alertcenter_3 и нажав кнопку «ОК» (см. рис. 1.75, 1.76), выйти из режима настроек подключения.

В соответствии с рис. 1.77 и 1.78 установить уровень логирования сервера AlertCenter.

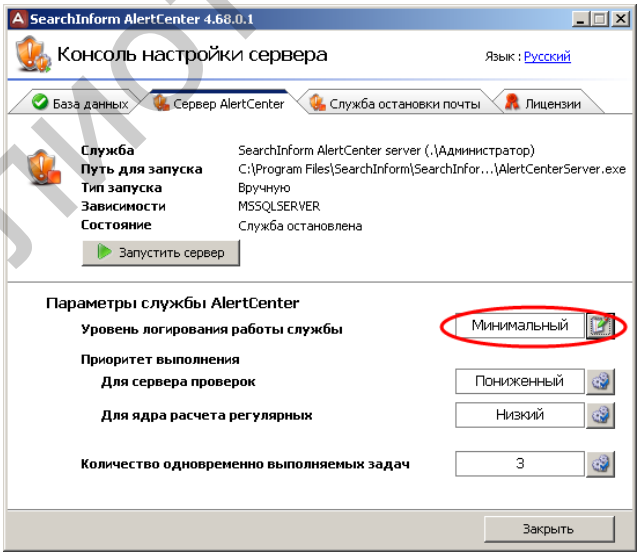


Рис. 1.77. Вход в настройку режима логирования

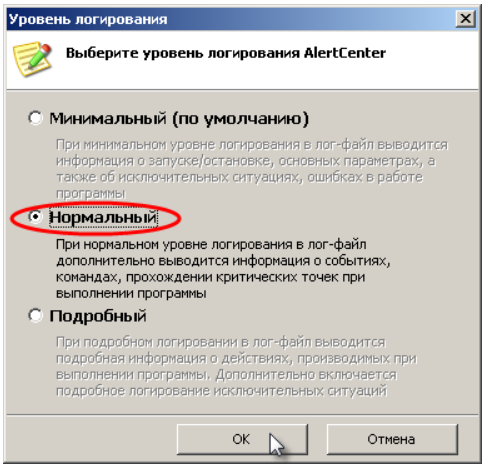


Рис. 1.78. Выбор уровня логирования

В соответствии с рис. 1.79 и 1.80 запустить сервер и закрыть консоль AlertCenter.

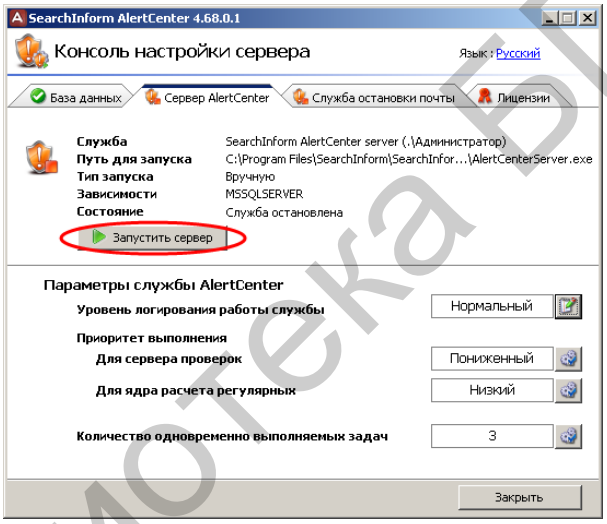


Рис. 1.79. Запуск сервера AlertCenter

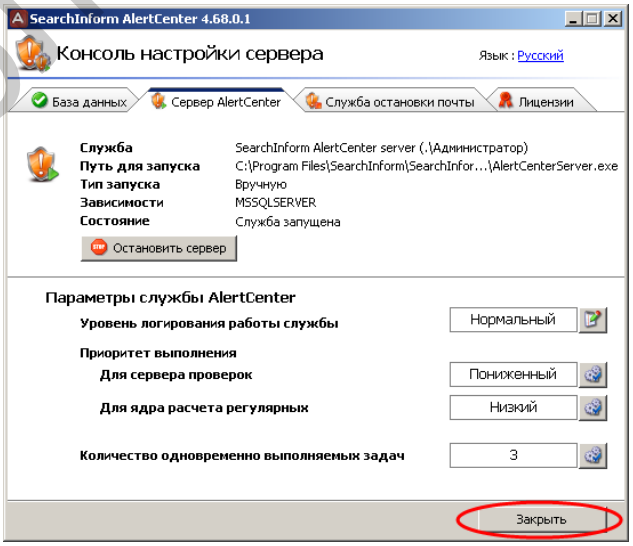


Рис. 1.80. Индикация запуска сервера AlertCenter

7. Настроить системную службу SearchInform DataCenter: agent. Для этого выполнить следующее.

Войдя в режим настроек операционной системы, запустить оснастку «Службы» и в соответствии с рис. 1.81–1.84 установить автоматический запуск службы SearchInform DataCenter: agent при загрузке операционной системы.

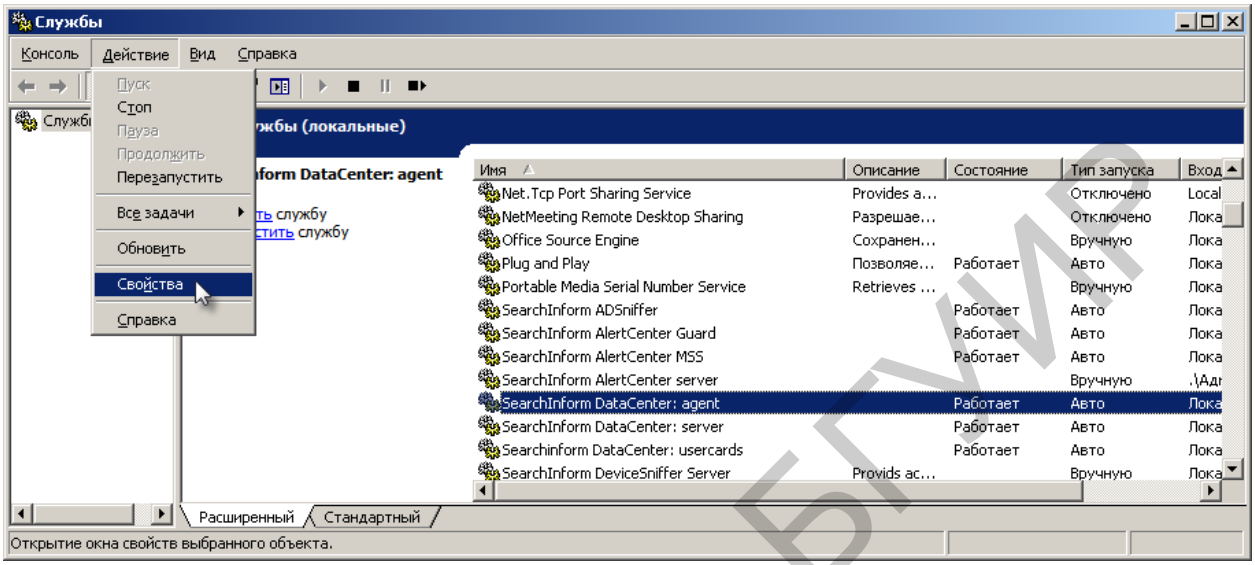


Рис. 1.81. Первый этап установки автоматического запуска SearchInform DataCenter : agent

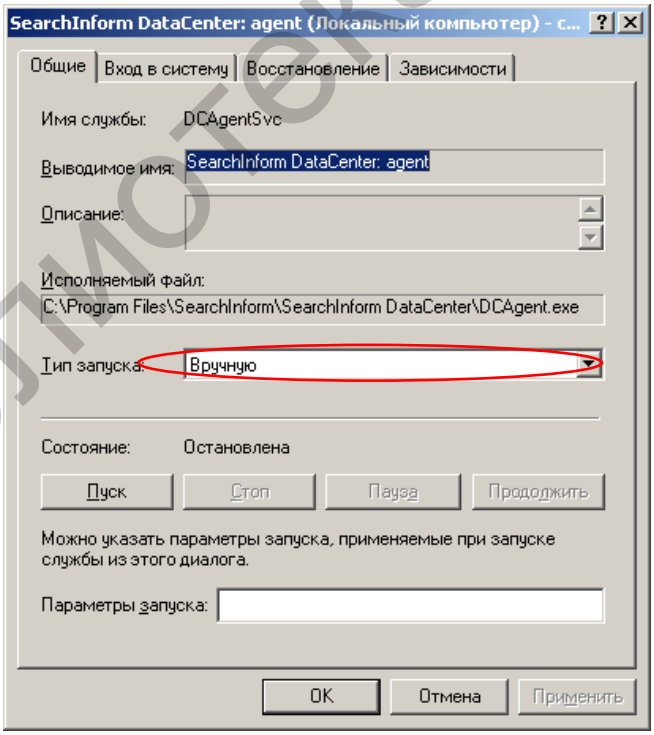


Рис. 1.82. Второй этап установки автоматического запуска SearchInform DataCenter: agent

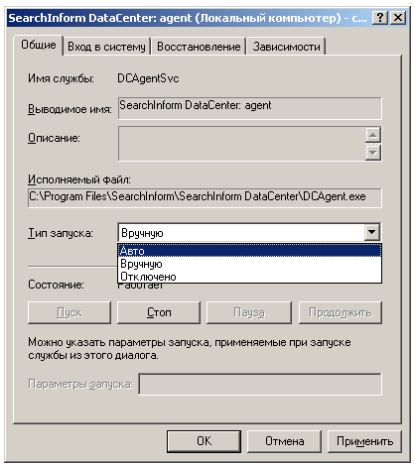


Рис. 1.83. Третий этап установки автоматического запуска SearchInform DataCenter: agent

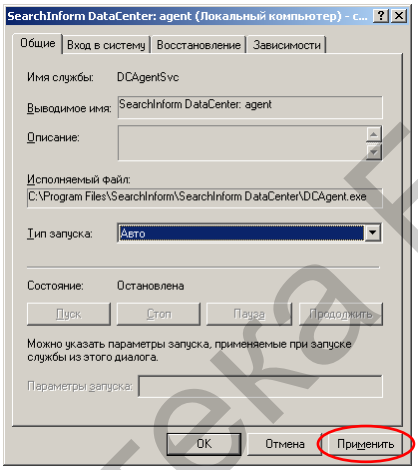


Рис. 1.84. Четвертый этап установки автоматического запуска SearchInform DataCenter: agent

В соответствии с рис.1.85 и 1.86 принудительно запустить службу SearchInform DataCenter : agent и выйти из режима управления «Службы операционной системы».

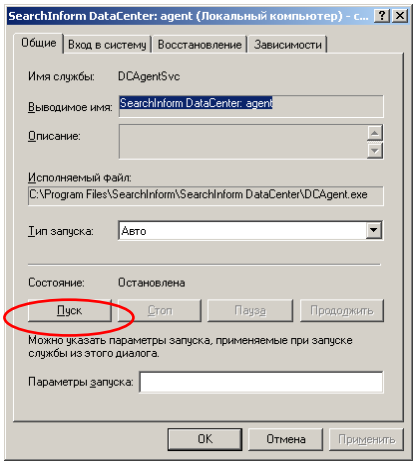


Рис. 1.85. Первый этап принудительного запуска службы SearchInform DataCenter: agent

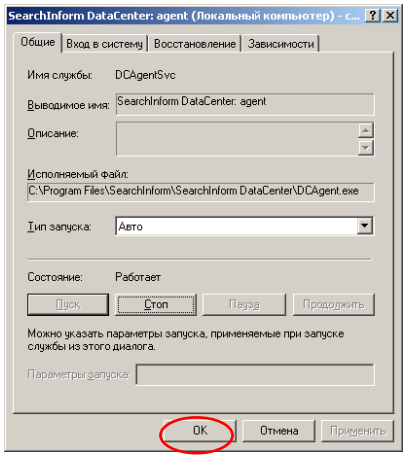


Рис. 1.86. Второй этап принудительного запуска службы SearchInform DataCenter: agent

8. Настроить параметры функционирования SearchInform EndpointSniffer. Для этого выполнить следующее.

Открыть консоль SearchInform DataCenter.

В соответствии с рис. 1.87 и 1.88 убедиться, что SearchInform EndpointSniffer не функционирует. Отметим, что в зависимости от предварительных настроек детализация параметров DataCenter может осуществляться не на вкладке «Управление» (см. рис. 1.87), а на вкладке «Настройки».

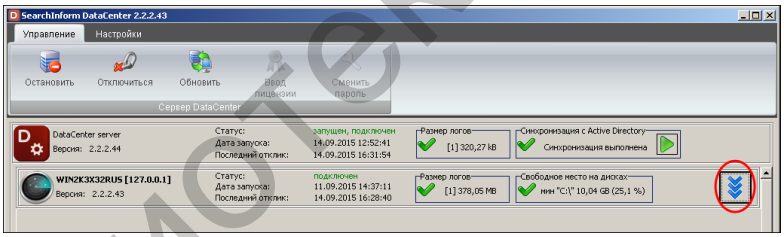


Рис. 1.87. Консоль DataCenter

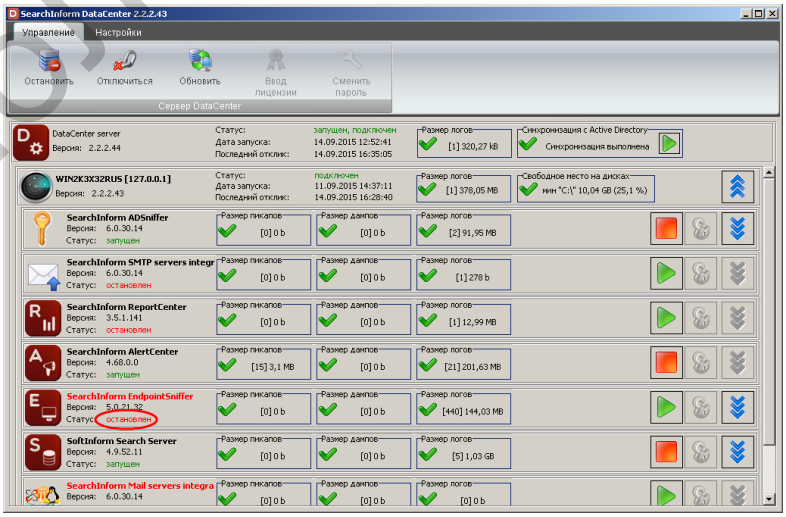


Рис. 1.88. Детализация параметров консоли DataCenter

Закрыть консоль SearchInform DataCenter.

Войти в режим управления «Службы операционной системы» и в соответствии с рис. 1.89–1.91 установить автоматический запуск службы SearchInform EndpointSniffer при загрузке операционной системы.

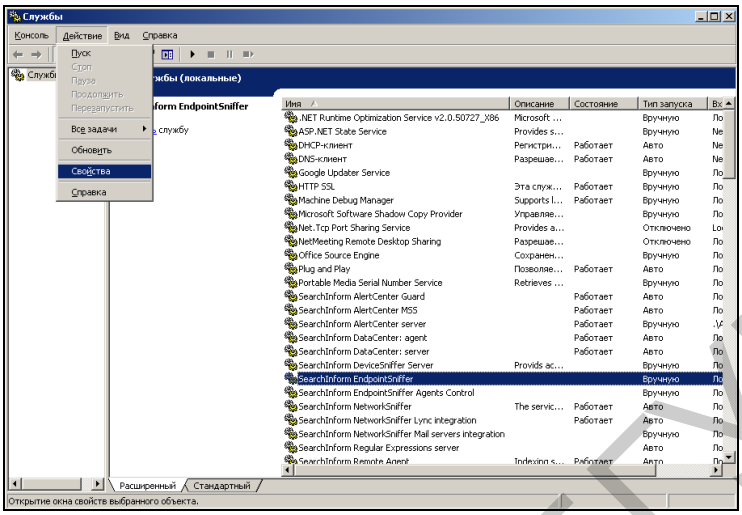


Рис. 1.89. Первый этап установки автоматического запуска SearchInform EndpointSniffer

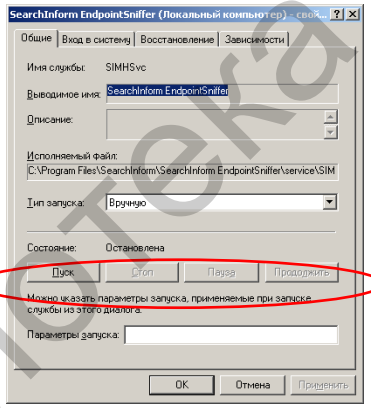


Рис. 1.90. Второй этап установки автоматического запуска SearchInform EndpointSniffer

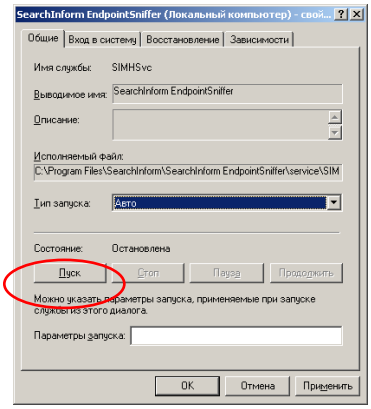


Рис. 1.91. Третий этап установки автоматического запуска SearchInform EndpointSniffer

В соответствии с рис. 1.92, 1.93 принудительно запустить службу SearchInform EndpointSniffer и выйти из режима управления «Службы операционной системы».

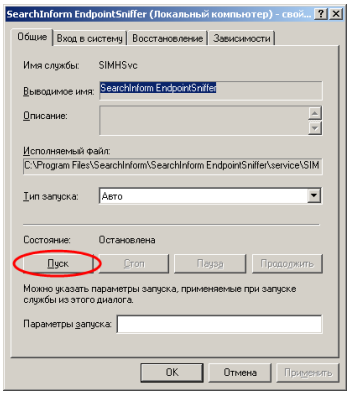


Рис. 1.92. Первый этап принудительного запуска службы SearchInform EndpointSniffer

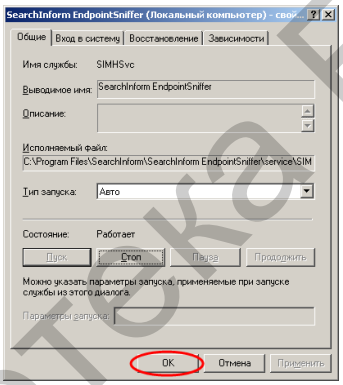


Рис. 1.93. Второй этап принудительного запуска службы SearchInform EndpointSniffer

Закрыть консоль управления «Службы операционной системы».
Завершить работу с виртуальным компьютером.

1.3. Задание для самостоятельной работы

1. Установить новый пароль на консоль SearchInform AlertCenter.
2. Установить новый пароль на остальные консоли и клиенты SearchInform.
3. Убедиться, что после перезагрузки виртуального компьютера служба SearchInform EndpointSniffer запускается в автоматическом режиме.
4. Остановить сервер AlertCenter.

1.4. Контрольные вопросы

1. Для чего необходим перехват всех документов, покидающих периметр организации, независимо от каналов, по которым это делается?

2. Требуется ли системный администратор в штате службы информационной безопасности и почему?

3. По каким схемам можно включить контур информационной безопасности в сеть предприятия?

4. Какая из схем подключения наиболее оптимальна при наличии технической возможности?

5. Перечислите основные аппаратные требования для штатного функционирования операционной системы Windows Server 2003.

6. Как установить пароль для пользователя «Администратор» Windows Server?

7. Как изменить параметры учетной записи в Windows Server?

8. Как установить пароль на консоль Search Server?

9. Как установить пароль на консоль DataCenter?

10. Как установить пароль на консоль EndpointSniffer?

11. Как установить пароль на консоль NetworkSniffer?

12. Как установить пароль на консоль ReportCenter?

13. Как установить пароль на службу AlertCenter?

14. Что такое индекс?

15. Как разграничить права доступа к индексам?

ЛАБОРАТОРНАЯ РАБОТА №2
ПРИНЦИПЫ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО КОМПЛЕКСА SEARCHINFORM ДЛЯ МОНИТОРИНГА УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

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

2.1. Теоретическая часть

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 и др.);

– веб-клиентов (передача данных по протоколу HTTP в социальные сети, форумы, блоги);

– ftp-клиентов;

– Skype (голосовых и текстовых сообщений, а также переданных файлов);

– записи на внешние устройства (Flash-носители, CD/DVD-диски, внешние жесткие диски и др.);

– печати на принтере;

– облачных хранилищ;

– Microsoft Lync (голосовых и текстовых сообщений);

– Viber (голосовых и текстовых сообщений).

Кроме этого, существует возможность выявления конфиденциальной информации на компьютерах пользователей, мониторинга изображений на дисплее пользователя, а также перехвата нажатий клавиш и записи посредством микрофона.

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, DeviceSniffer, CloudSniffer, LyncSniffer, ViberSniffer, KeyloggerSniffer, MicrophoneSniffer. 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, а также базам данных отдельных модулей перехвата. Для индексации данных используется компонент SoftInform Search Server. Оповещение о найденных кон-

фиденциальных данных, т. е. о выявленном факте утечки, реализуется с помощью компонента AlertCenter.

Отметим, что во многих организациях есть пользователи, документы которых должны быть исключены из перехвата. Для исключения перехвата следует использовать фильтры SearchInform EndpointSniffer Administrator Console и SearchInform NetworkSniffer Administrator Console. Фильтры по пользователям особенно актуальны для сервера NetworkSniffer, который управляет компонентами MailSniffer, IMSniffer, HTTPSniffer, FTPSniffer и CloudSniffer. Перехват идет на уровне сетевых адаптеров и по умолчанию перехватываются документы всех пользователей. Фильтры по пользователям не настолько важны для остальных компонентов, 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, которые присутствуют в подобных документах. Распознать неструктурированную конфиденциальную информацию сложнее. Для этого следует проанализировать смысл текста документа.

Поиск конфиденциальной информации осуществляется с помощью SearchInform Client, 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 и 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 и 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.

2. Расширенный поиск по техническим параметрам документа.

3. Поиск нераспознанных документов, т. е. таких, из которых не удалось извлечь текст.

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

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

6. 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 ско-

рость 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.

7. Статистические запросы – выявление инцидентов на основании количественных показателей.

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 компонентами SearchInform Client и AlertCenter.

Примечание. Подробная информация о настройках поиска содержится в руководстве аудитора безопасности системы SearchInform, а также в процедурных справках SoftInform Search, SearchInform Client, AlertCenter, EndpointSniffer, NetworkSniffer.

2.2. Лабораторное задание

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. С помощью ярлыка SearchInform AlertCenter Console, в соответствии с рис. 2.1 и 2.2, запустить сервер AlertCenter и закрыть окно консоли. При необходимости ввести пароль.

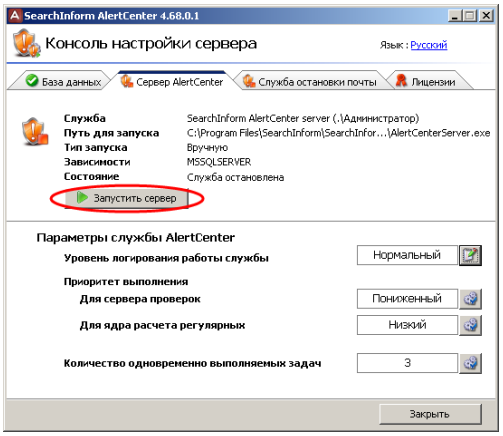


Рис. 2.1. Запуск сервера AlertCenter

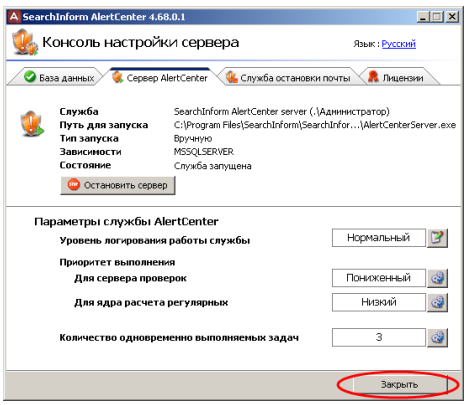


Рис. 2.2. Индикация функционирования сервера AlertCenter

С помощью соответствующего ярлыка запустить SearchInform NetworkSniffer Administrator Console, окно которого показано на рис. 2.3. Отметим, что в процессе запуска может потребоваться ввод парольных данных, установленных в предыдущей лабораторной работе.

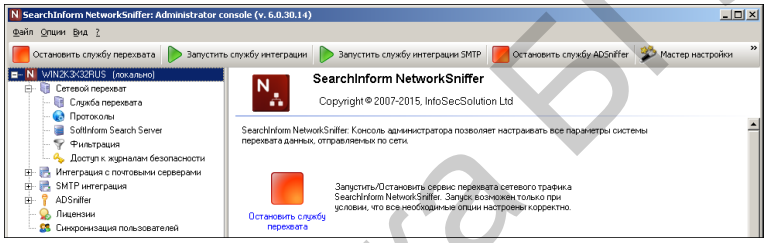


Рис. 2.3. SearchInform NetworkSniffer Administrator Console

В соответствии с рис. 2.4 и 2.5 провести редактирование фильтра перехвата информации. После редактирования будут перехватываться данные пользователей ivanov, bublik и konev для всх контролируемых протоколов.

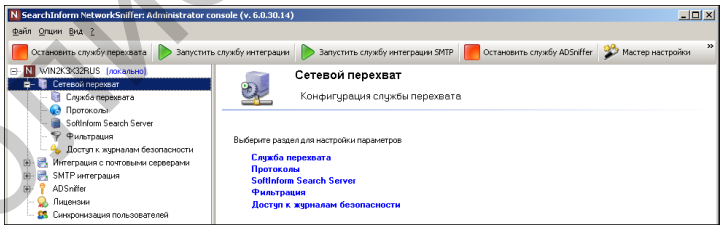


Рис. 2.4. Открытие ветви «Сетевой перехват»

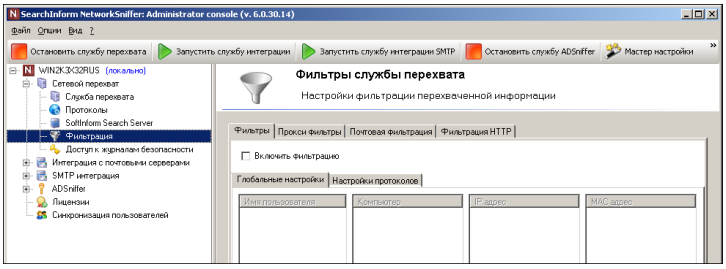


Рис. 2.5. Переход в режим редактирования фильтров
для всех контролируемых протоколов

В соответствии с рис. 2.6–2.11 добавить фильтр, разрешающий перехват данных пользователя ivanov для всех контролируемых протоколов.

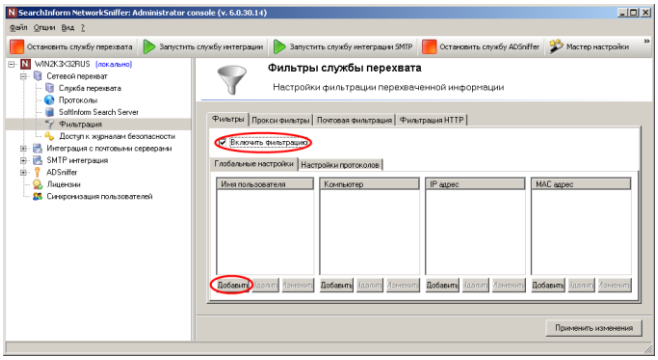


Рис. 2.6. Вход в режим добавления фильтра для всех контролируемых протоколов

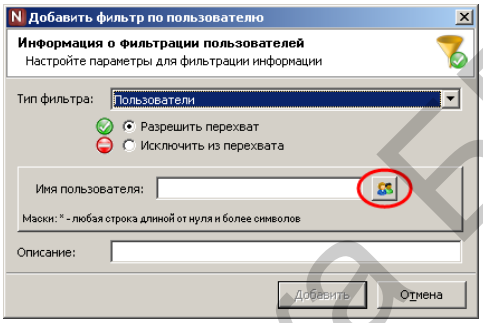


Рис. 2.7. Вход в режим выбора пользователей для разрешающего фильтра

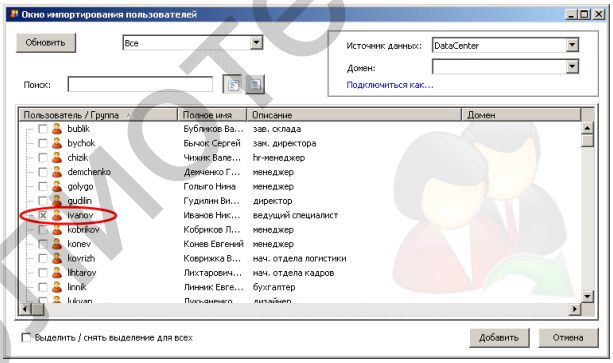


Рис. 2.8. Окно выбора пользователей для фильтра

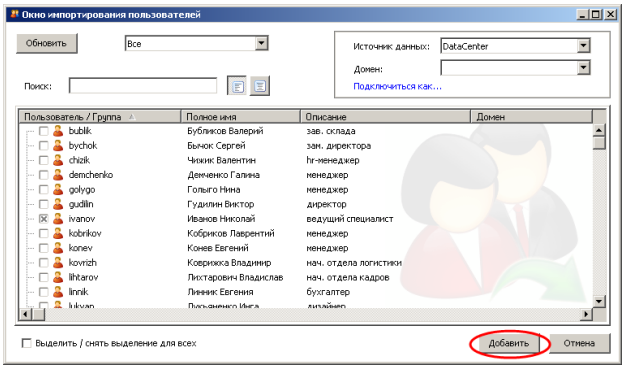


Рис. 2.9. Подтверждение выбора пользователей для фильтрации

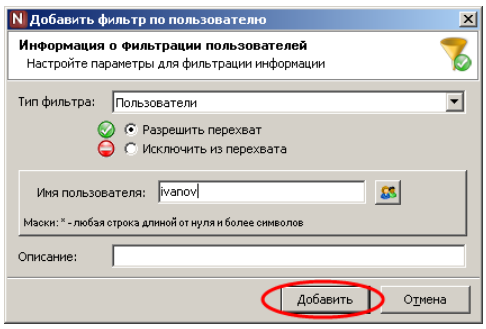


Рис. 2.10. Подтверждение настройки фильтра

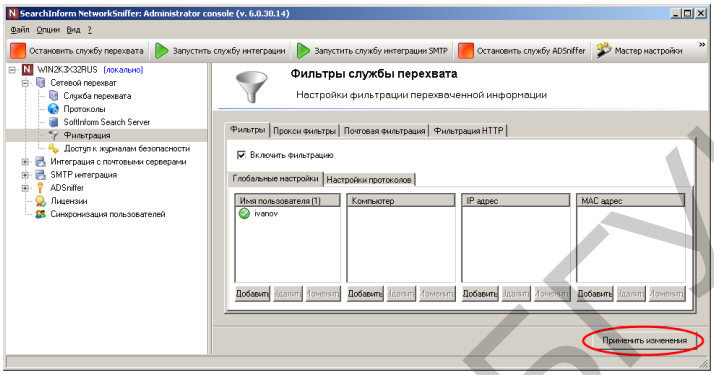


Рис. 2.11. Индикация разрешающих фильтров по пользователям для всех контролируемых протоколов

По аналогии с добавлением пользователя ivanov добавить пользователей bublik и konev. В соответствии с рис. 2.12 и 2.13 удалить фильтр, разрешающий перехват данных пользователя konev для всех контролируемых протоколов.

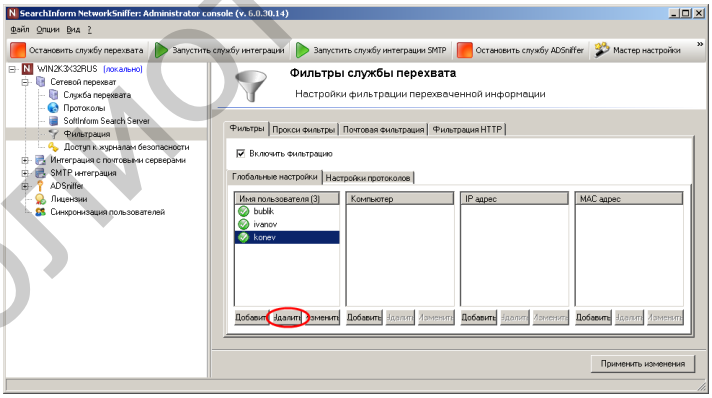


Рис. 2.12. Удаление разрешающего фильтра по пользователю konev для всех контролируемых протоколов

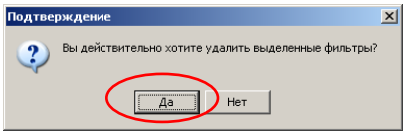


Рис. 2.13. Подтверждение удаления фильтра

В соответствии с рис. 2.14–2.20 настроить фильтрацию перехватываемых данных по сетевой маске и MAC-адресам для всех контролируемых протоко-

лов. 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».

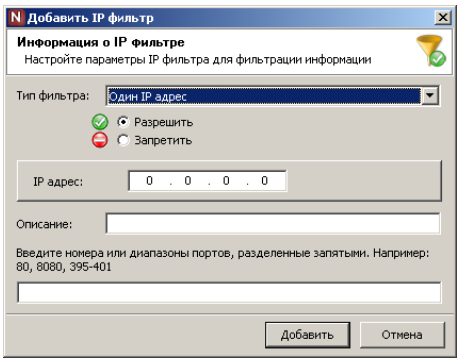


Рис. 2.14. Первый этап добавления разрешающей фильтрации по параметрам сети

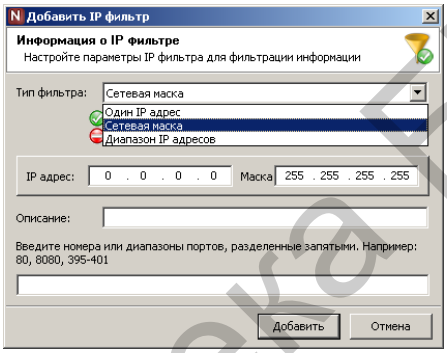


Рис. 2.15. Выбор опции «Сетевая маска»

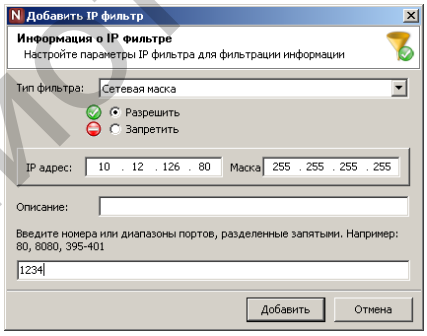


Рис. 2.16. Указание сетевой маски и прослушиваемых портов

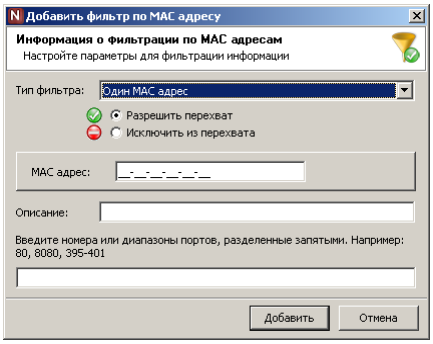


Рис. 2.17. Первый этап добавления разрешающей фильтрации по MAC-адресам

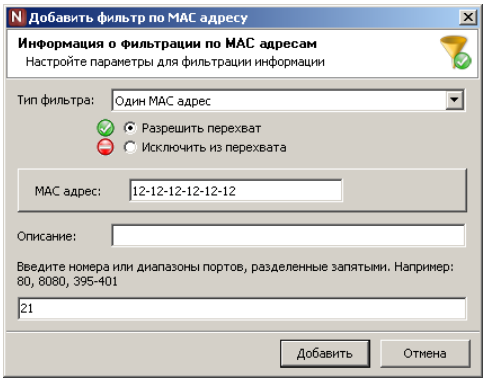


Рис. 2.18. Указание MAC-адреса и прослушиваемых портов

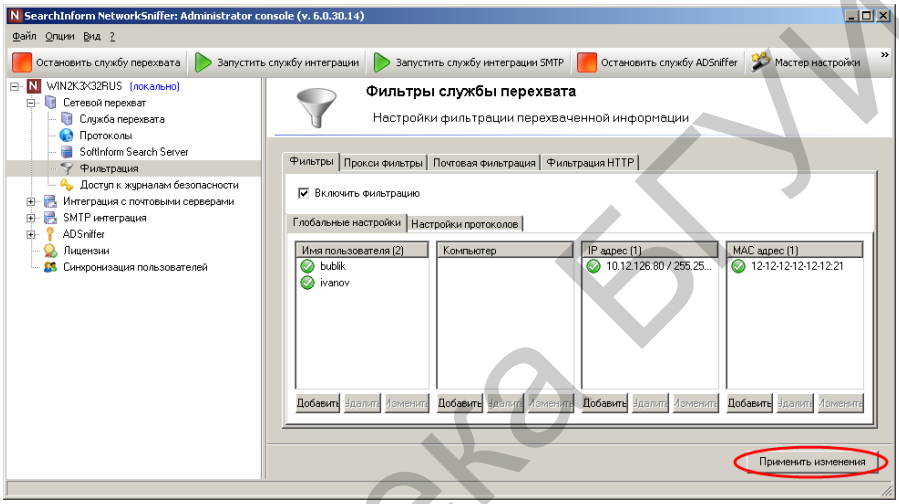


Рис. 2.19. Подтверждение добавления фильтров по IP- и MAC-адресам для всех контролируемых протоколов

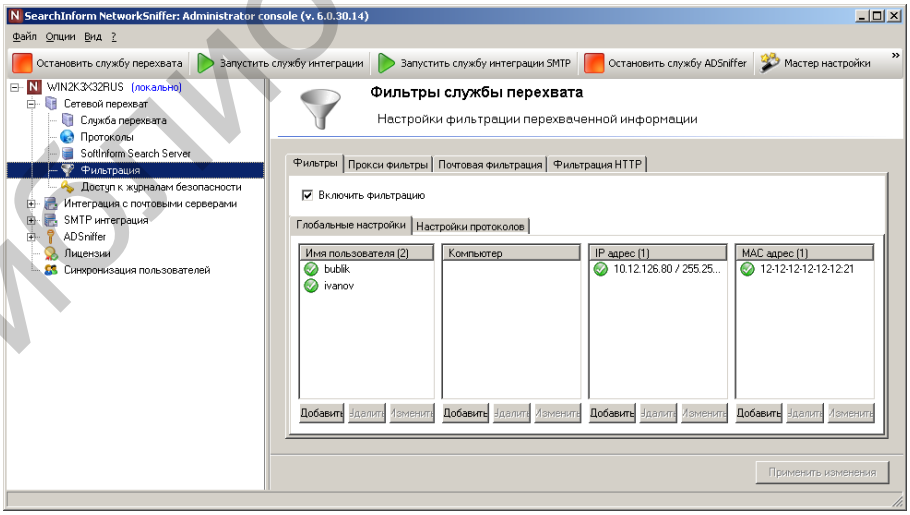


Рис. 2.20. Индикация фильтров для всех контролируемых протоколов

В соответствии с рис. 2.21 настроить фильтр, запрещающий перехват данных по протоколу HTTP для пользователя ivanov.

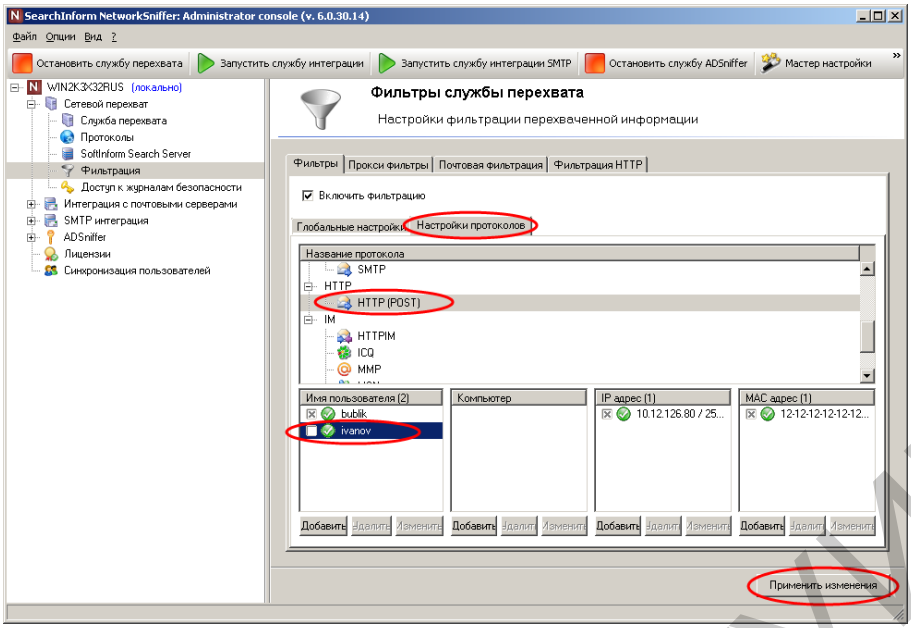


Рис. 2.21. Отмена разрешающего фильтра по протоколу HTTP для пользователя ivanov

В соответствии с рис. 2.22–2.26 настроить фильтр, разрешающий перехват данных по протоколу POP3 для пользователя polyk.

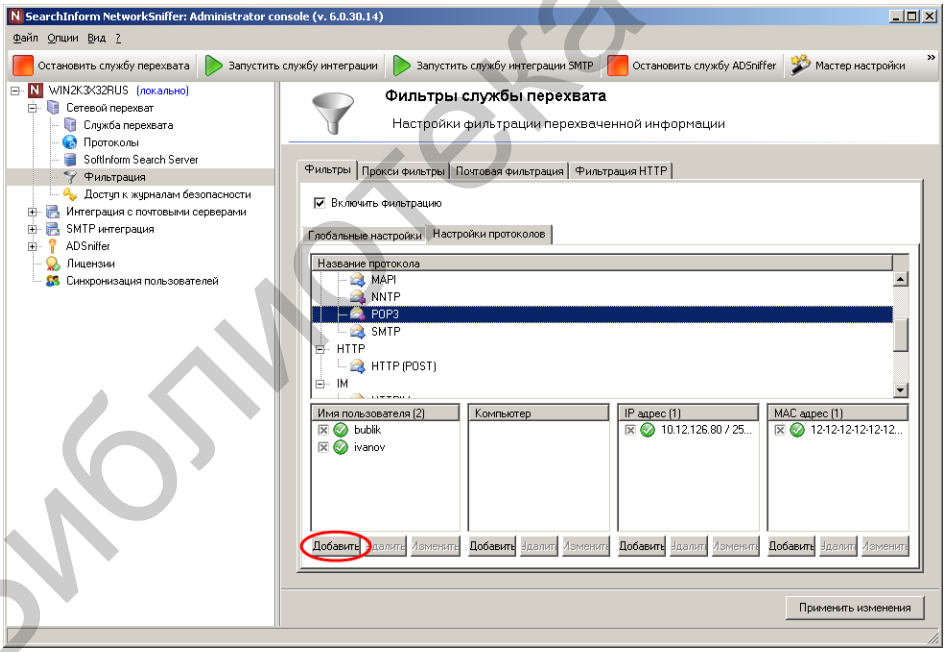


Рис. 2.22. Вход в режим добавления нового фильтра пользователей по протоколу POP3

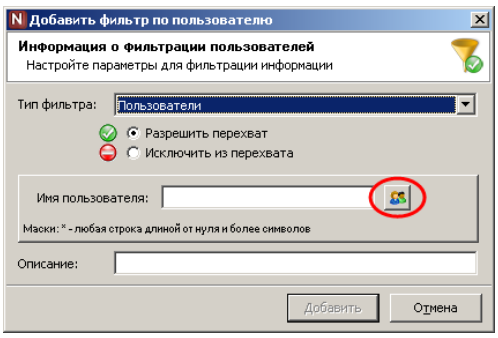


Рис. 2.23. Вход в режим выбора пользователей

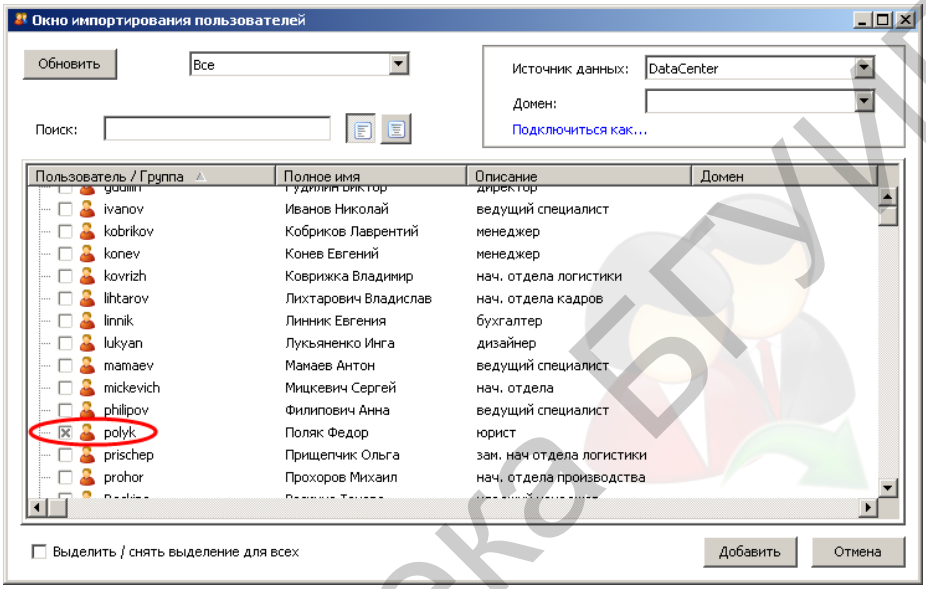


Рис. 2.24. Выбор пользователя polyk

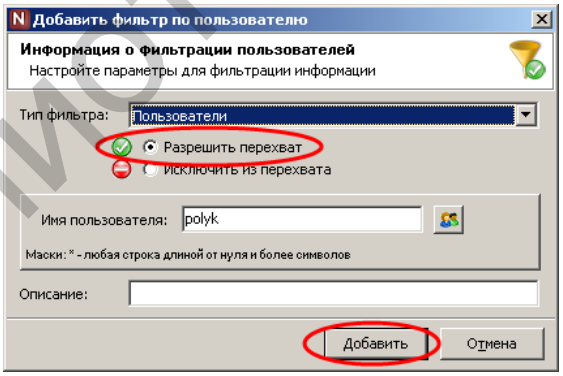


Рис. 2.25. Выбор разрешающего фильтра

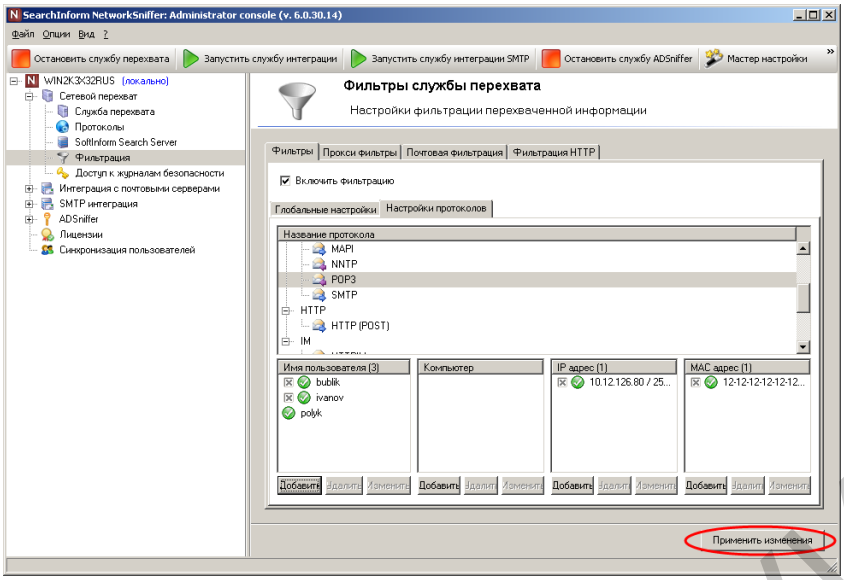


Рис. 2.26. Подтверждение добавления нового разрешающего фильтра

В соответствии с рис. 2.27–2.31 настроить прокси-фильтр.

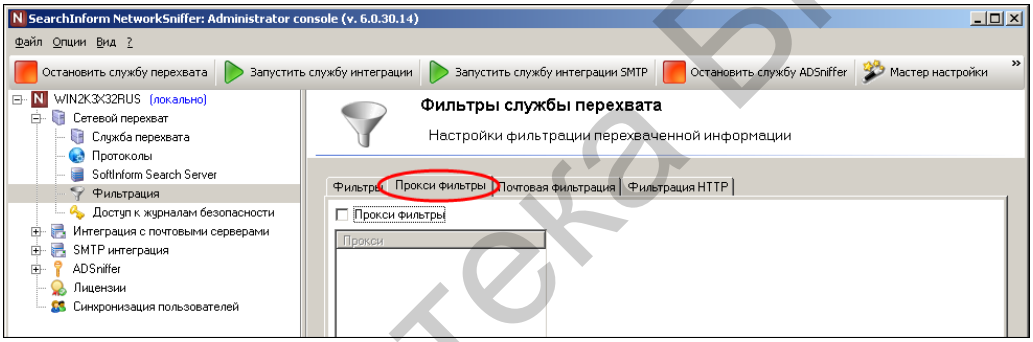


Рис. 2.27. Переход к настройкам фильтрации по прокси-серверам

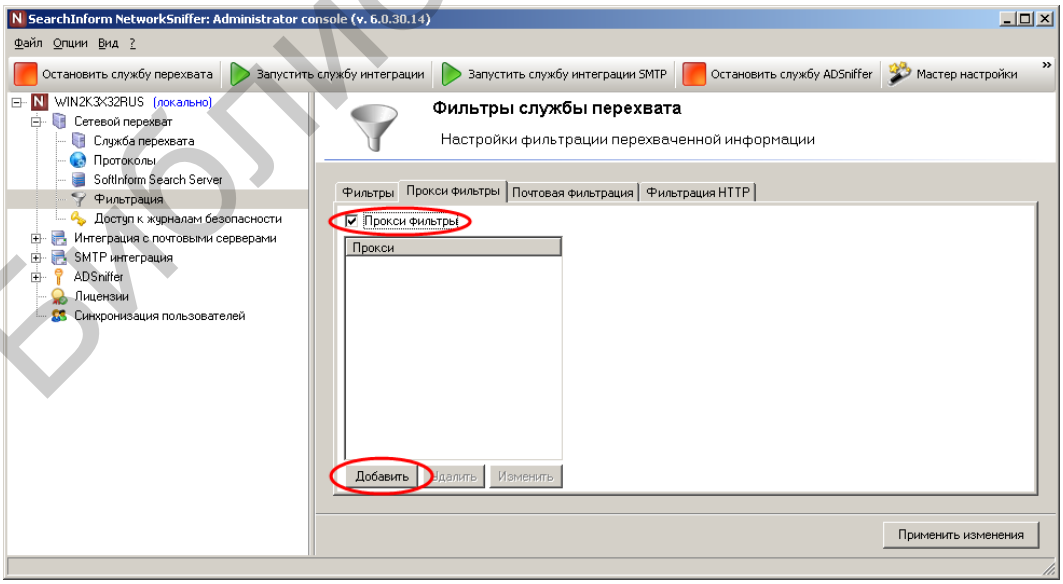


Рис. 2.28. Первый этап добавления прокси-фильтра

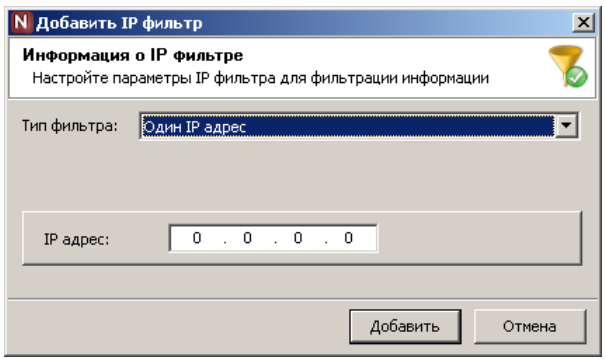


Рис. 2.29. Окно ввода параметров прокси-сервера

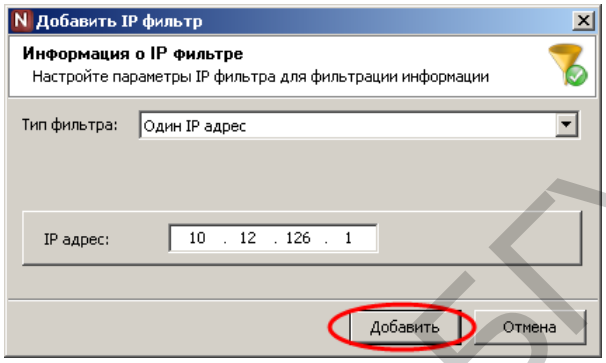


Рис. 2.30. Добавление параметров прокси-сервера

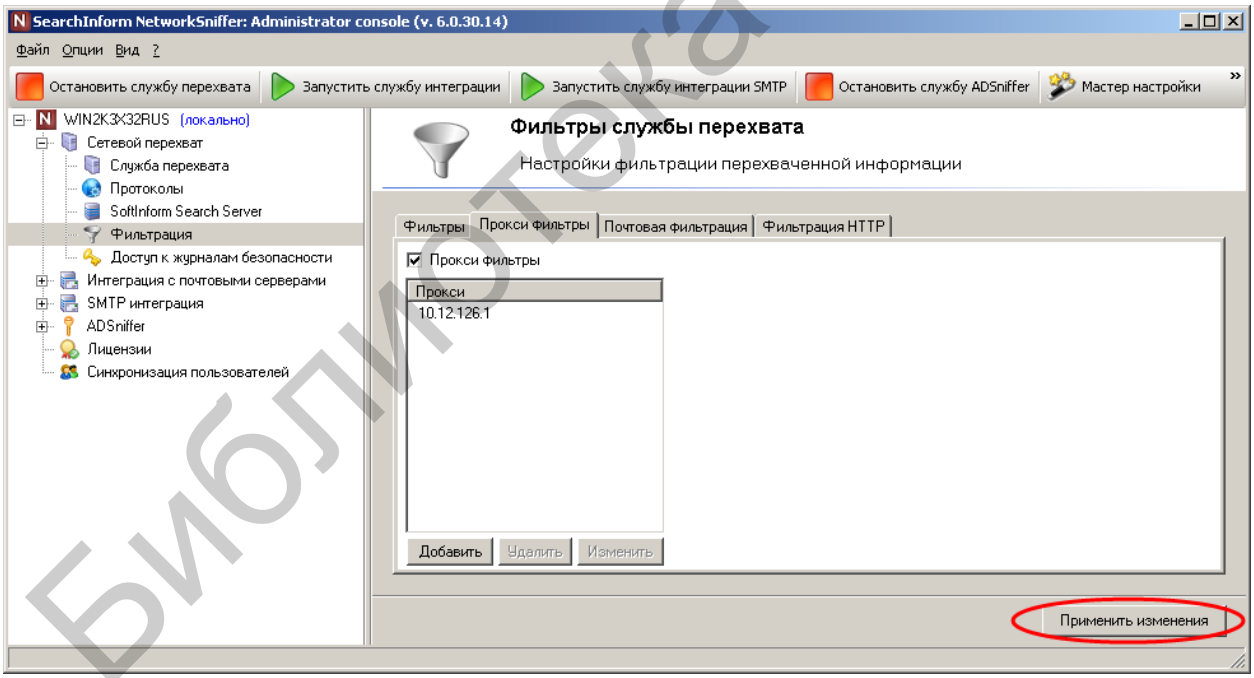


Рис. 2.31. Подтверждение параметров прокси-сервера

В соответствии с рис. 2.32–2.34 удалить прокси-фильтр.

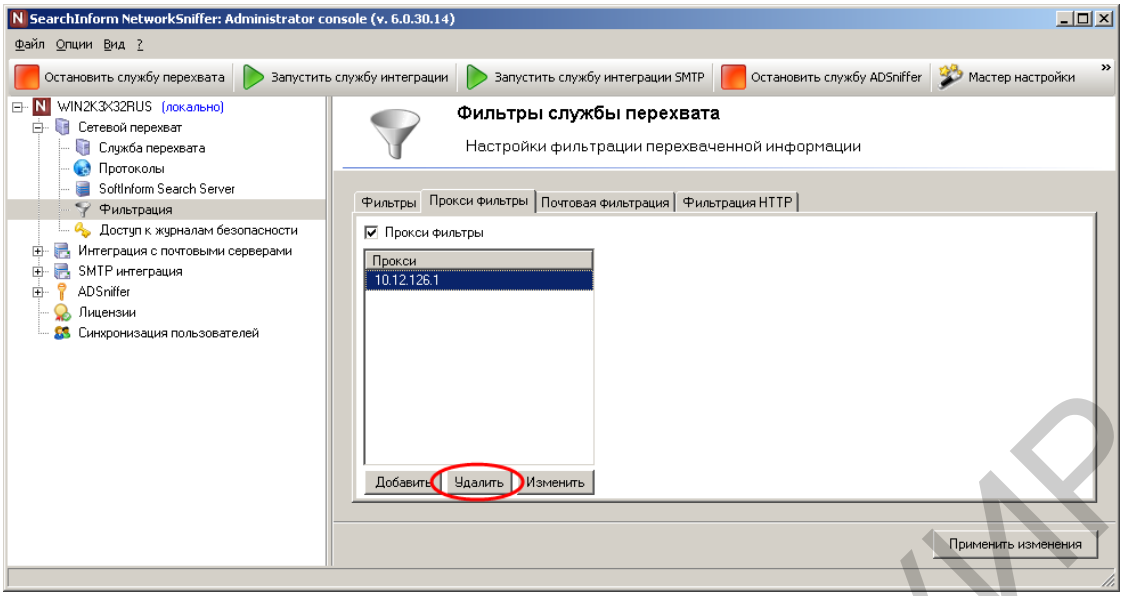


Рис. 2.32. Выбор прокси-фильтра для удаления

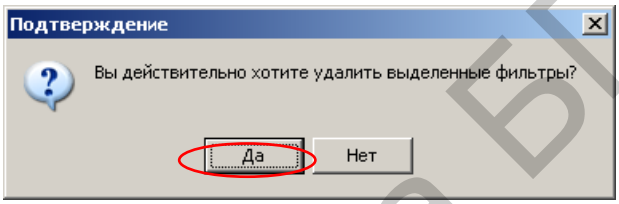


Рис. 2.33. Подтверждение удаления фильтра

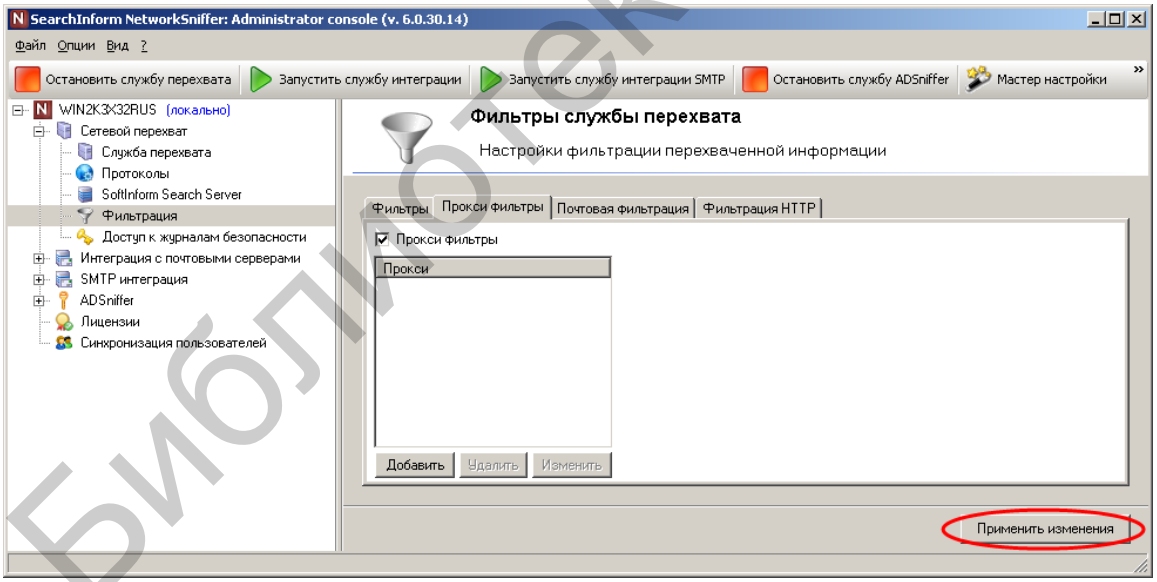


Рис. 2.34. Подтверждение настроек по удалению фильтра

В соответствии с рис. 2.35–2.37 создать фильтр по почтовым адресам для сообщений, имеющих размер более 10 000 байт.

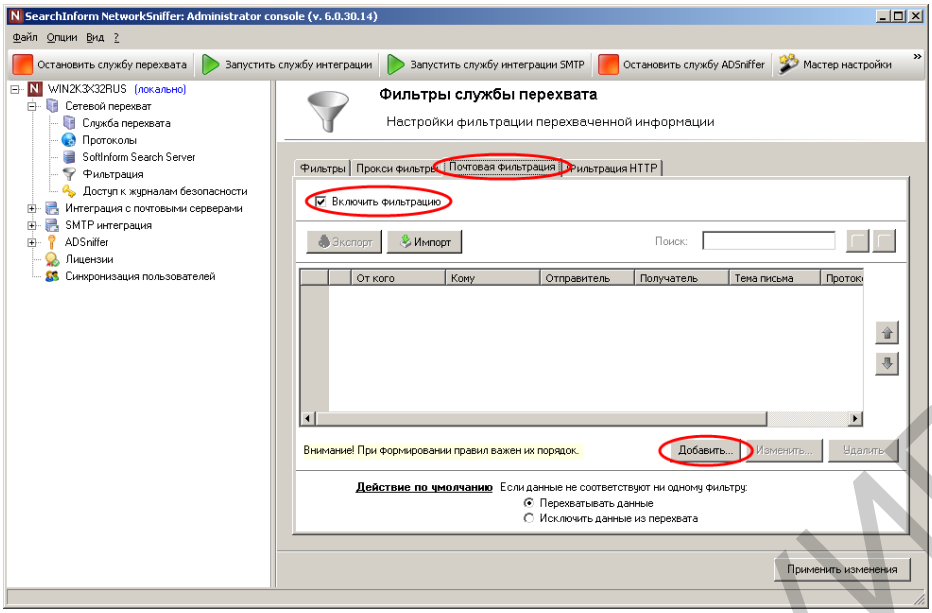


Рис. 2.35. Вход в режим добавления фильтра по почтовым адресам

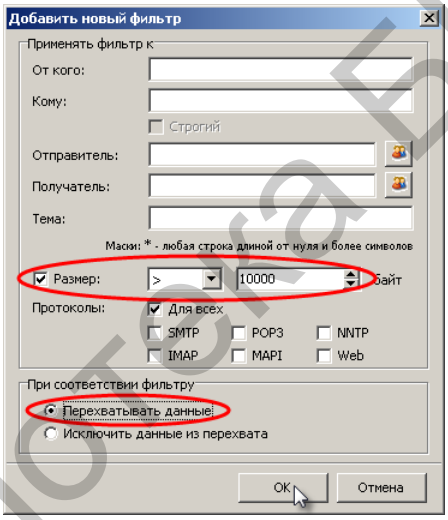


Рис. 2.36. Установка размера сообщения

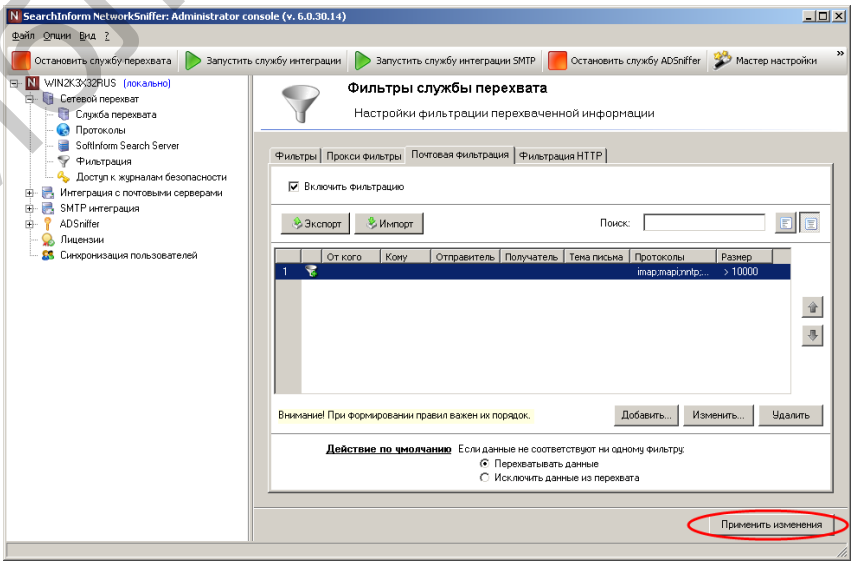


Рис. 2.37. Индикация установленного фильтра по почтовым адресам

В соответствии с рис. 2.38–2.44 указать соответствие пользователя 123 почтовому адресу 123@ukr.net.

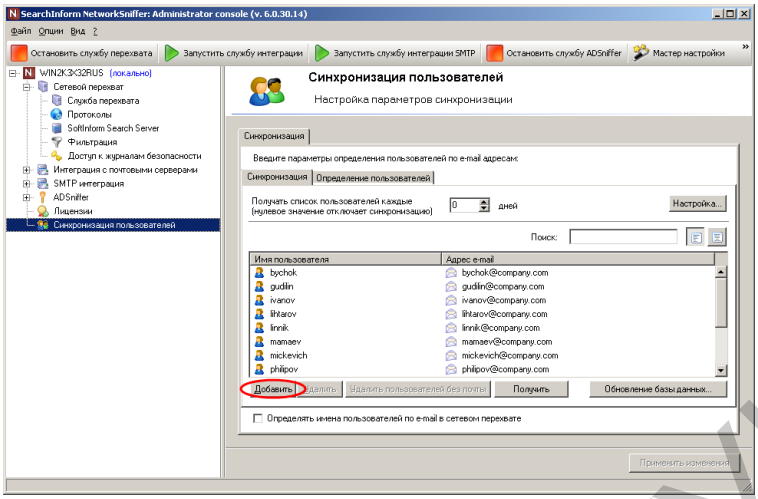


Рис. 2.38. Добавление пользователя

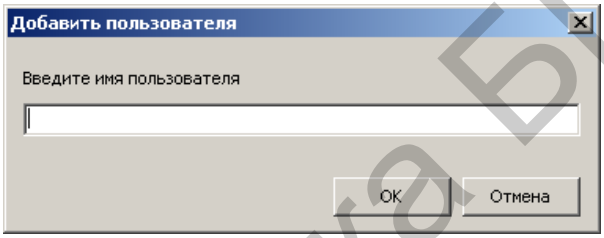


Рис. 2.39. Ввод имени пользователя

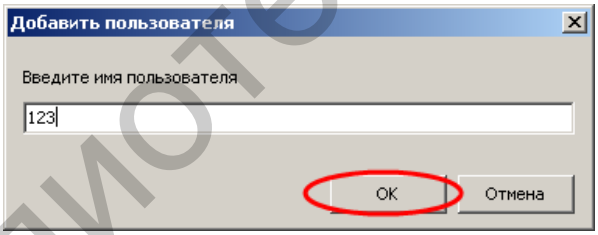


Рис. 2.40. Подтверждение имени пользователя

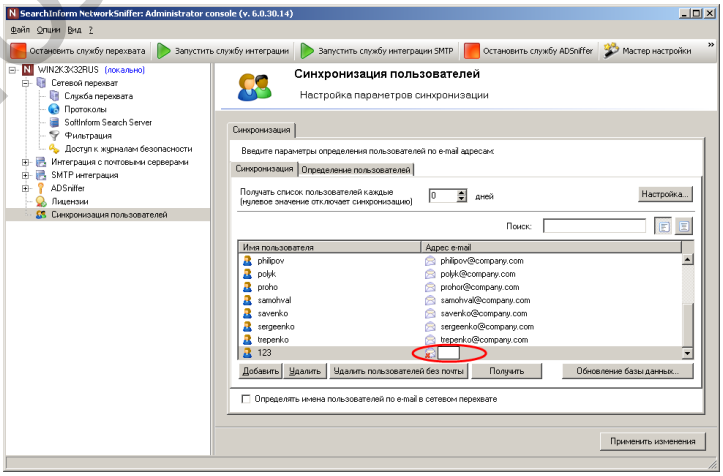


Рис. 2.41. Поле ввода почтового адреса

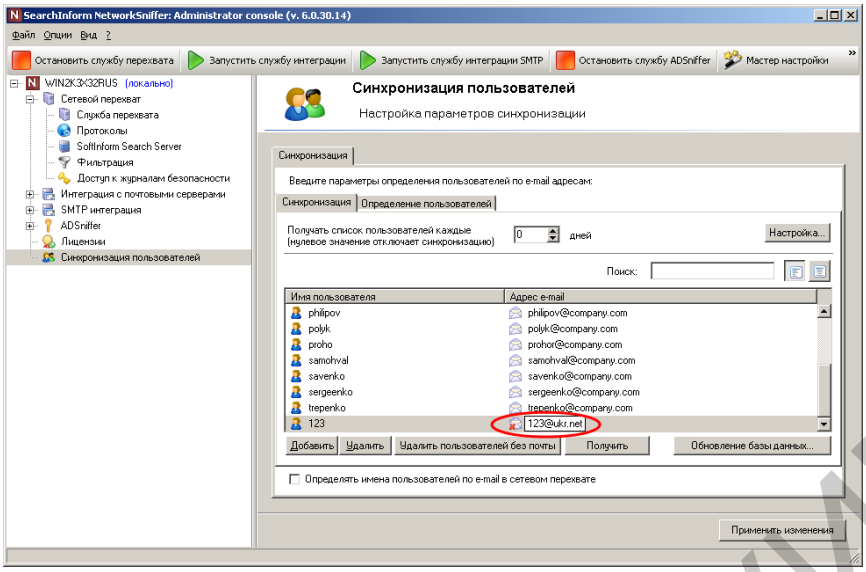


Рис. 2.42. Ввод почтового адреса

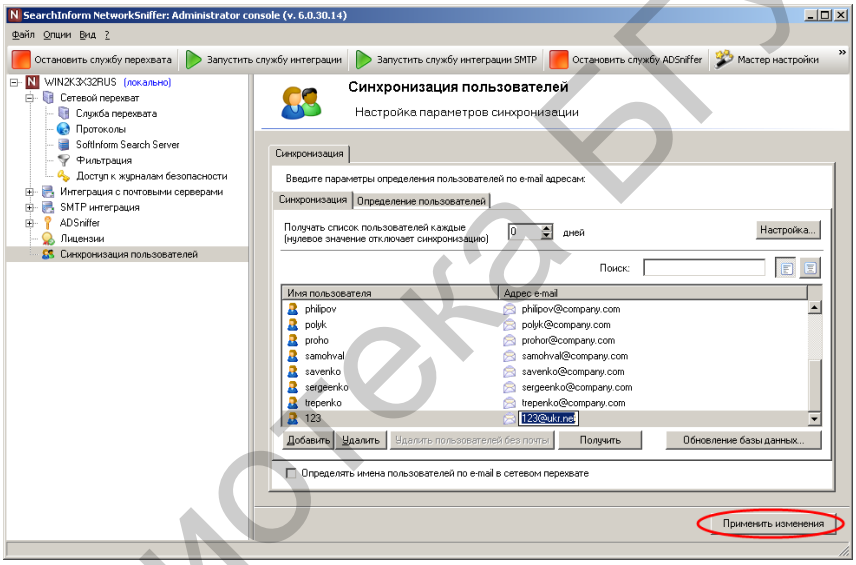


Рис. 2.43. Подтверждение соответствия адреса пользователю

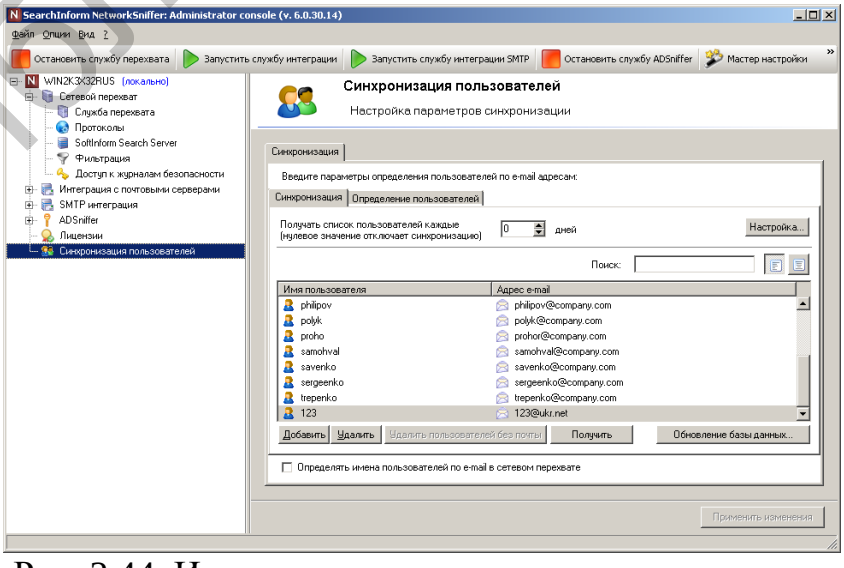


Рис. 2.44. Индикация установленного соответствия

В соответствии с рис. 2.45–2.48 создать список определения масок почтовых адресов пользователей.

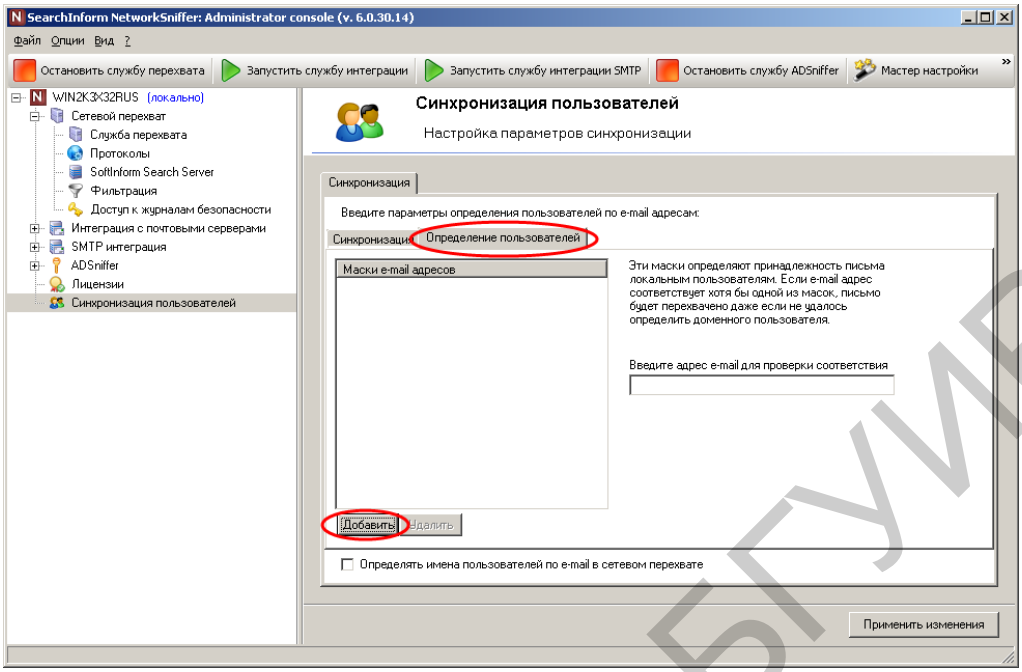


Рис. 2.45. Добавление маски

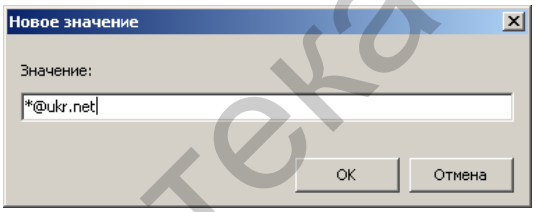


Рис. 2.46. Ввод маски *@ukr.net

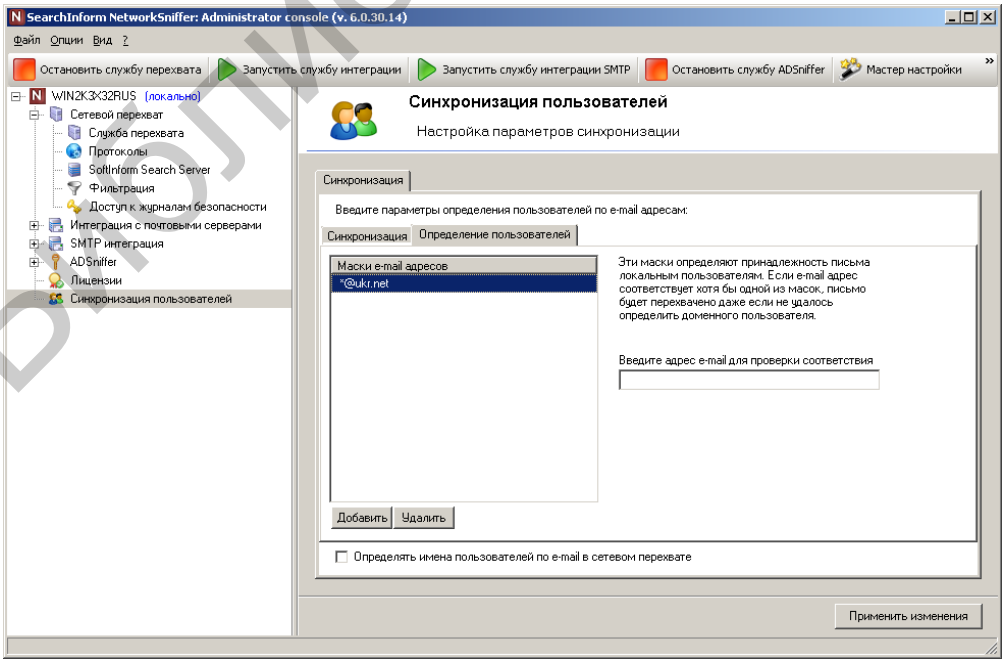


Рис. 2.47. Индикация введенной маски

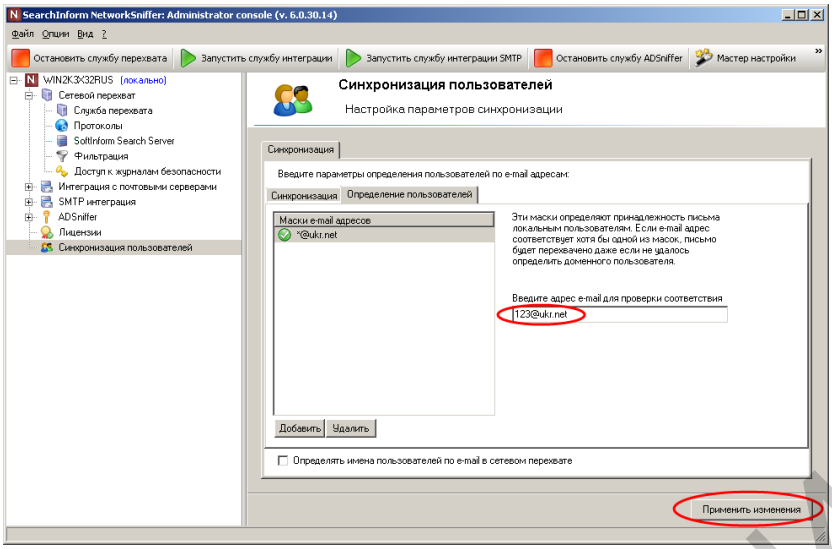


Рис. 2.48. Проверка введенной маски и применение исправлений

В соответствии с рис. 2.49–2.51 создать фильтр по почте пользователей, определив поиск наличия в теме письма слова «коррупция».

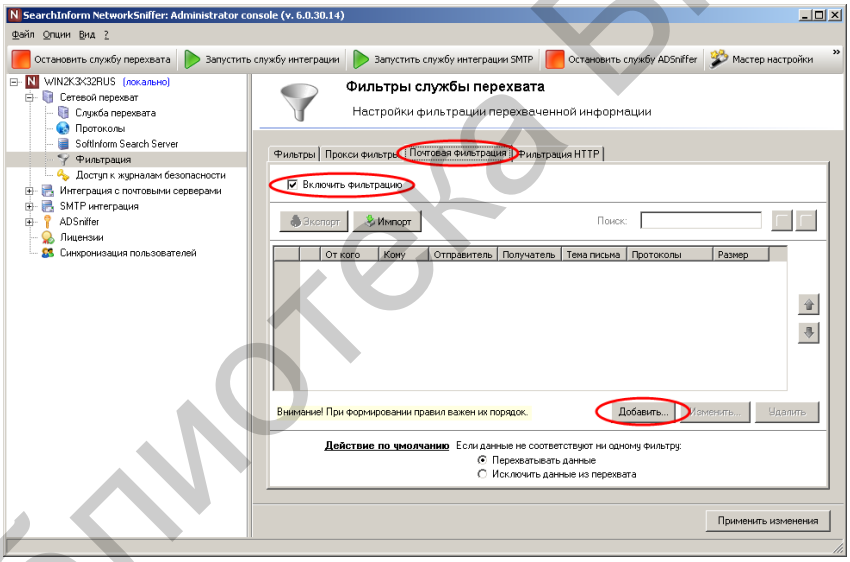


Рис. 2.49. Переход к созданию фильтра

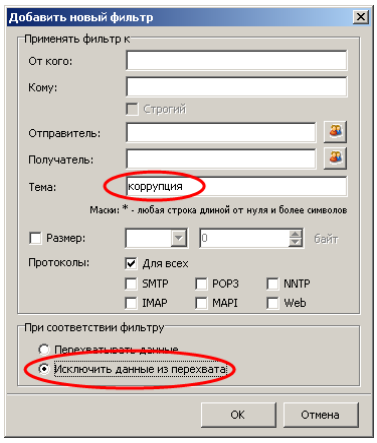


Рис. 2.50. Определение параметров фильтра

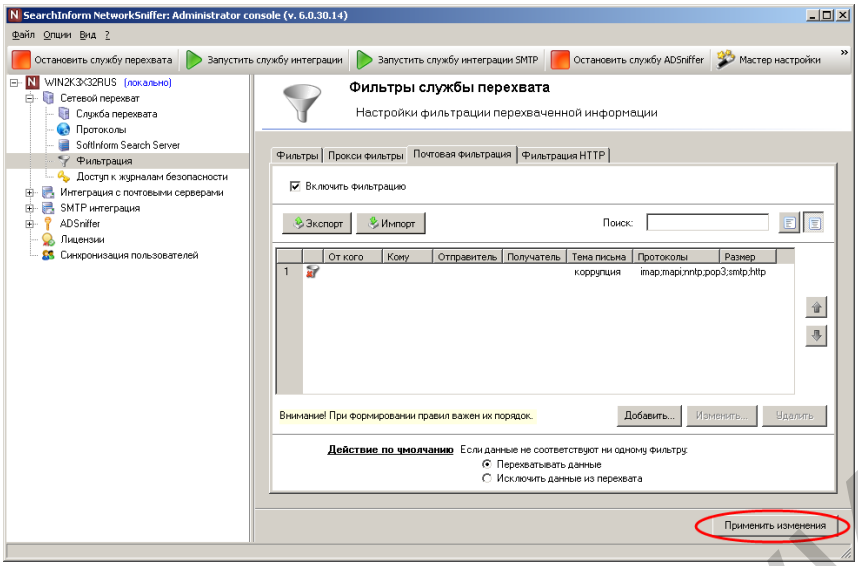


Рис. 2.51. Индикация успешного создания фильтра

В соответствии с рис. 2.52–2.54 создать фильтр по протоколу HTTP, определив поиск наличия в содержимом слова «взятка».

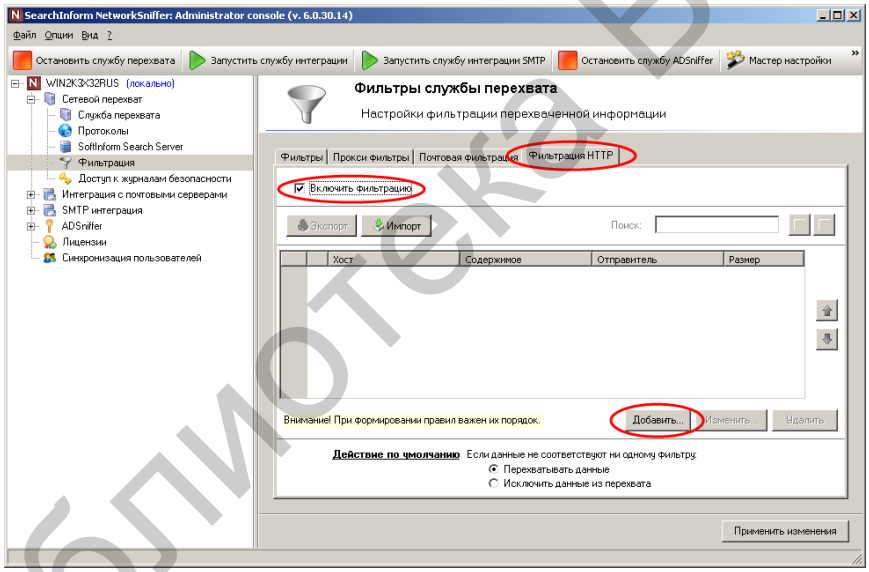


Рис. 2.52. Переход к созданию фильтра

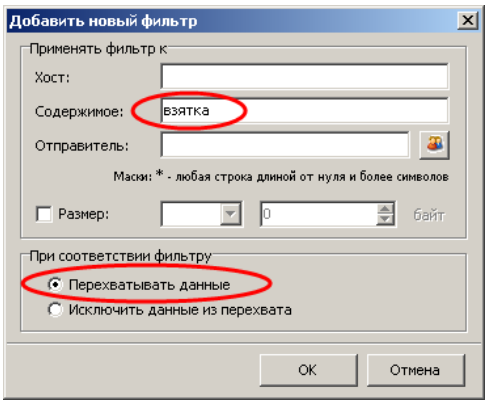


Рис. 2.53. Создание фильтра

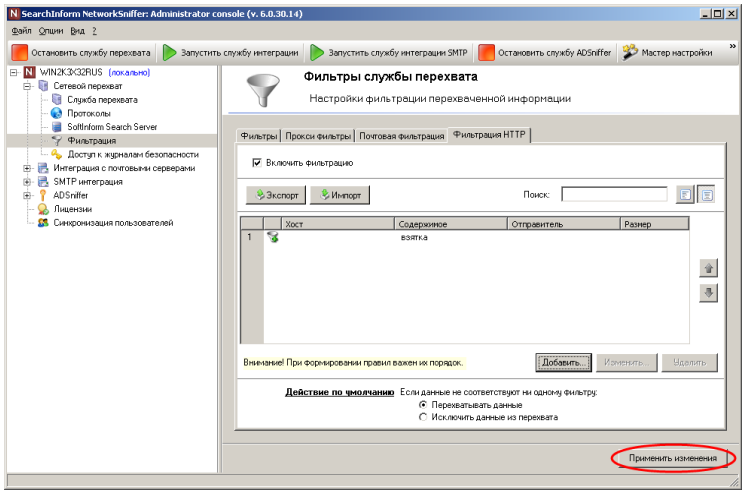


Рис. 2.54. Индикация успешного создания фильтра

Закрыть окно консоли SearchInform NetworkSniffer. Открыть окно консоли SearchInform EndpointSniffer (рис. 2.55).

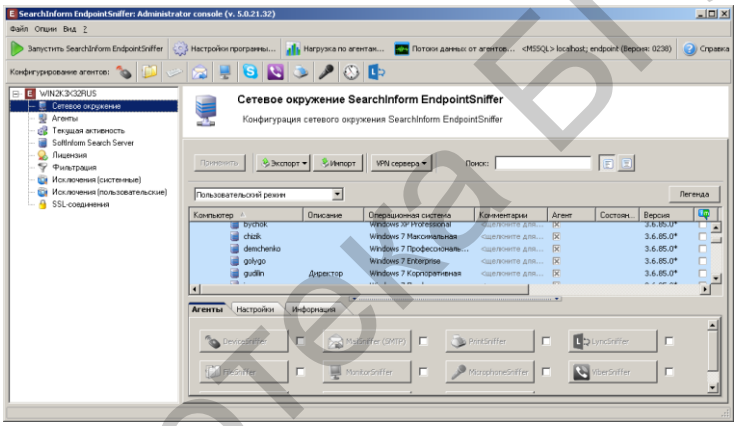


Рис. 2.55. Окно SearchInform EndpointSniffer

В соответствии с рис. 2.56–2.60 удалить из фильтрации по всем протоколам данные пользователя «Админ».

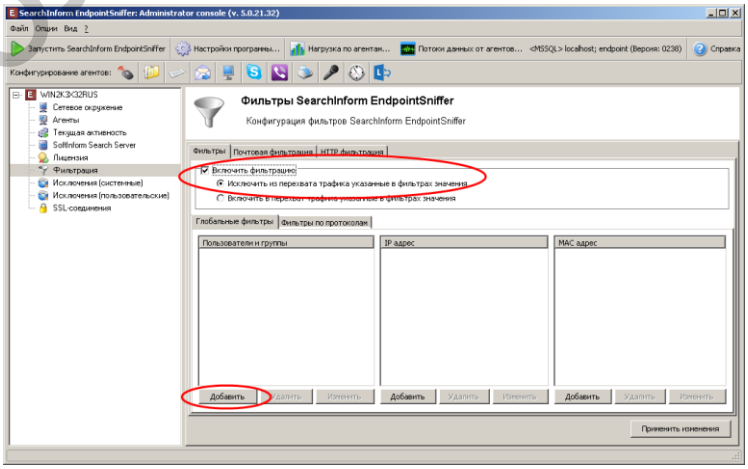


Рис. 2.56. Добавление фильтра по всем протоколам

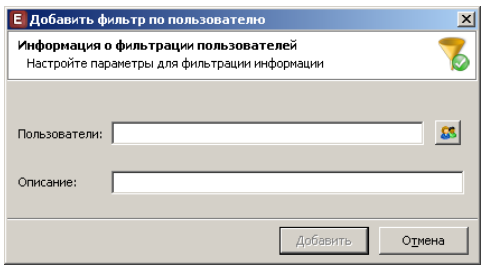


Рис. 2.57. Окно ввода имени пользователя

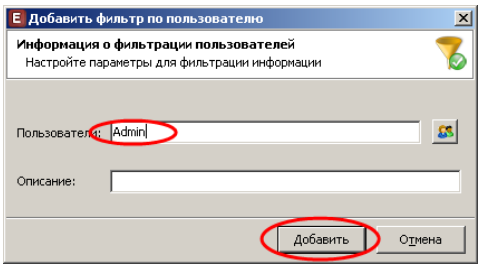


Рис. 2.58. Ввод имени пользователя

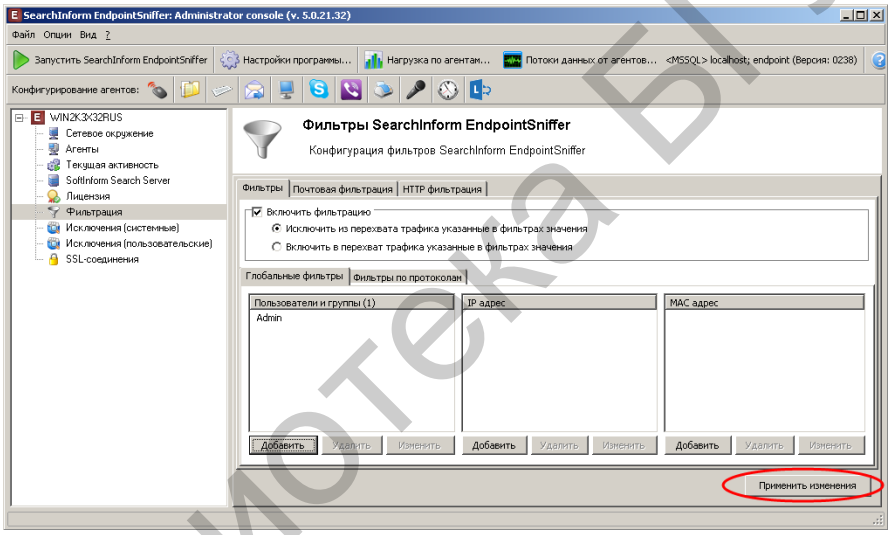


Рис. 2.59. Подтверждение добавления фильтра по всем протоколам

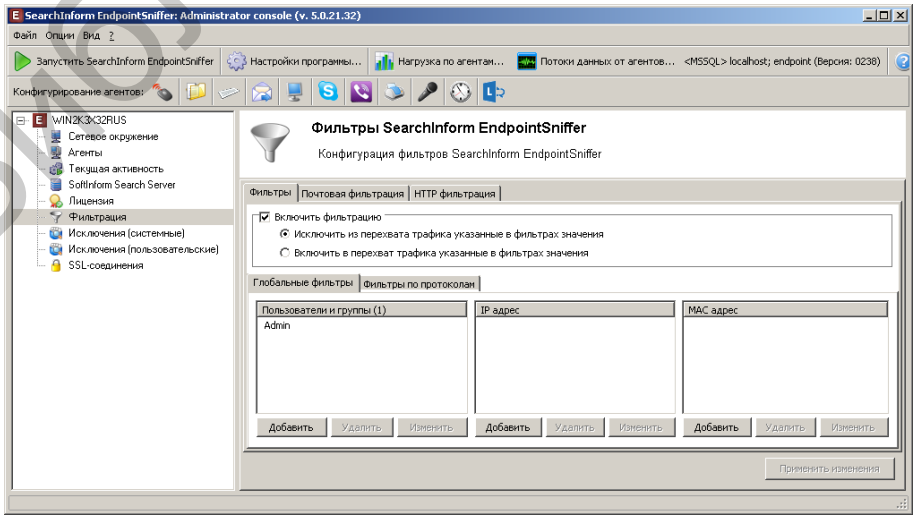


Рис. 2.60. Индикация созданного фильтра по всем протоколам

В соответствии с рис. 2.61–2.67 создать фильтр MonitorSniffer для пользователя ivanov. Фильтрация осуществляется с 10.00 до 23.00, кроме субботы и воскресенья.

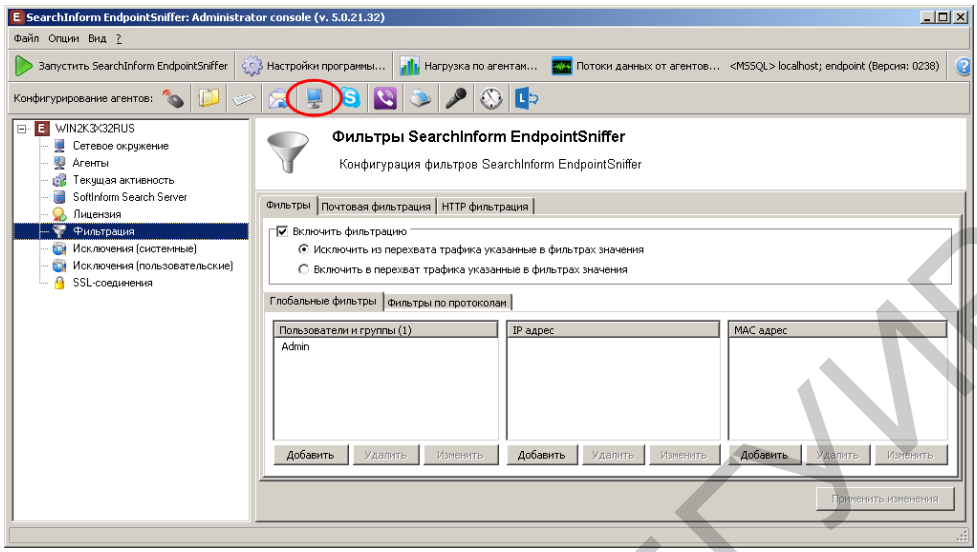


Рис. 2.61. Переход в режим создания фильтра монитора

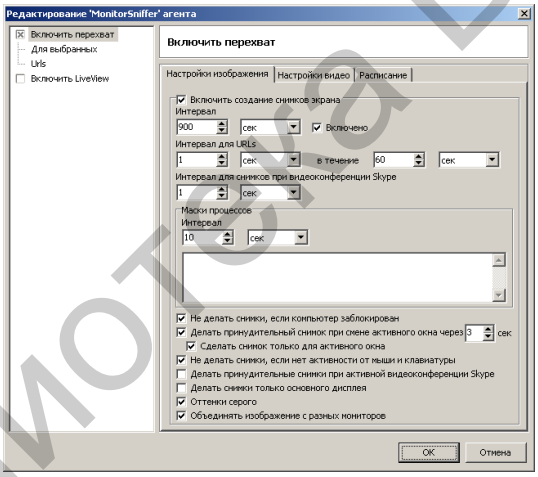


Рис. 2.62. Окно создания фильтра монитора

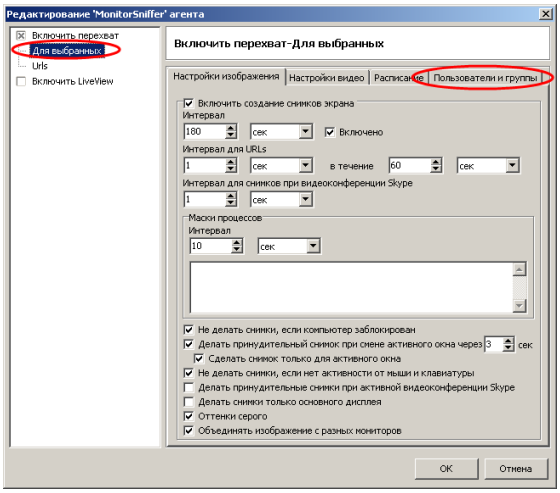


Рис. 2.63. Переход в режим создания фильтра монитора для пользователей

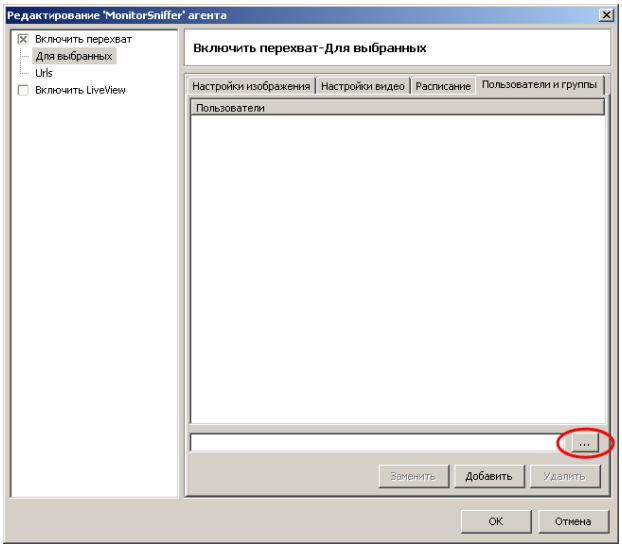


Рис. 2.64. Переход в режим выбора имен пользователей для фильтра монитора

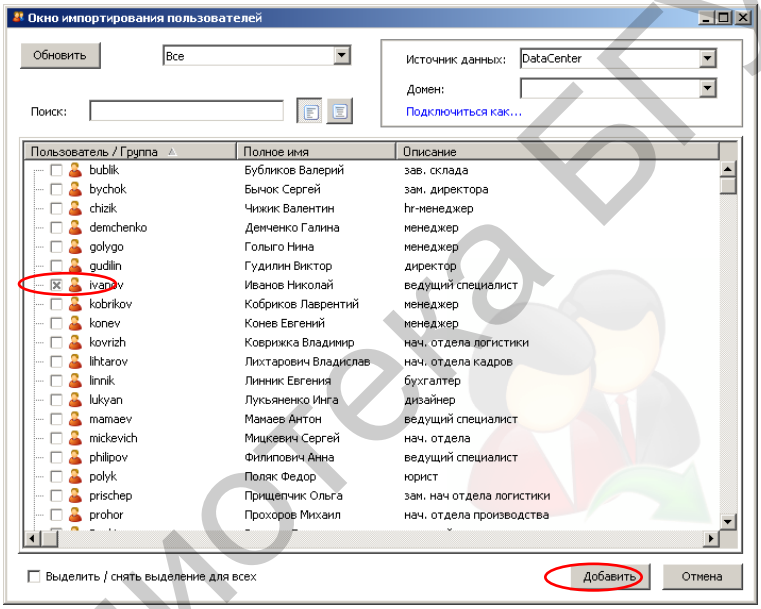


Рис. 2.65. Задание имени пользователя для фильтра монитора

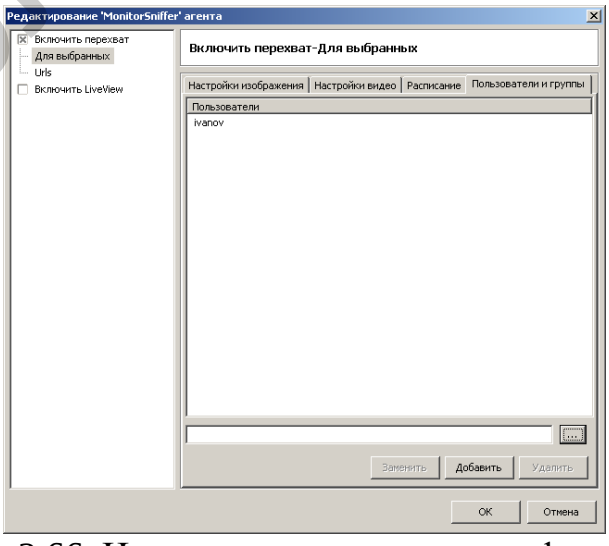


Рис. 2.66. Индикация пользователя в фильтре

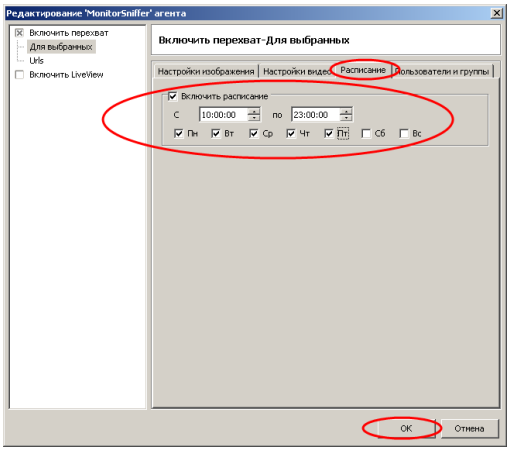


Рис. 2.67. Создание расписания в фильтре

Закрыть окно консоли SearchInform EndpointSniffer. Открыть окно консоли SearchInform NetworkSniffer (рис. 2.68).

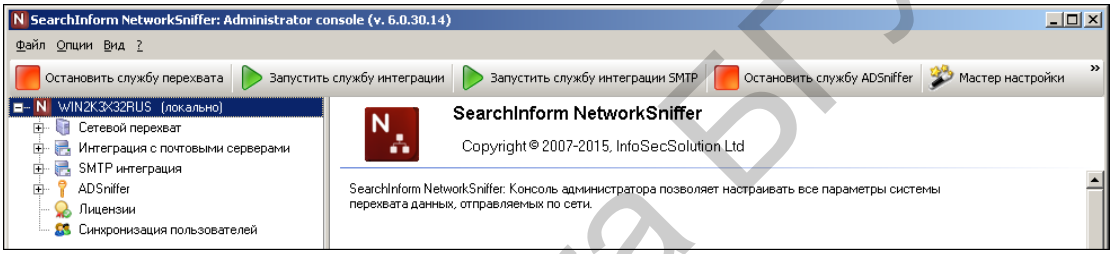


Рис. 2.68. Окно консоли NetworkSniffer

В соответствии с рис. 2.69–2.74 настроить расписание обновления индексов Network_POST. Предусмотреть обновление индексов через каждые 5 мин.

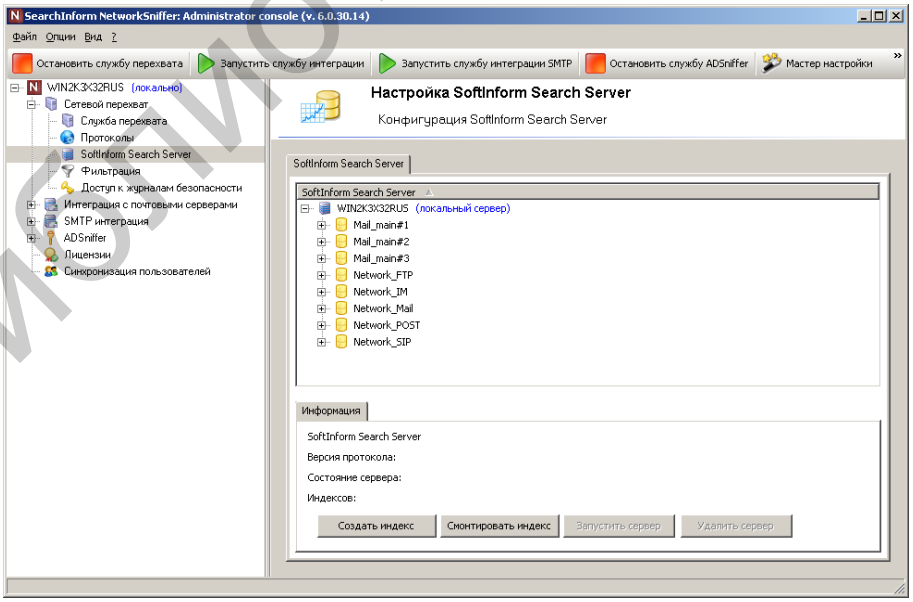


Рис. 2.69. Окно редактирования параметров индексов

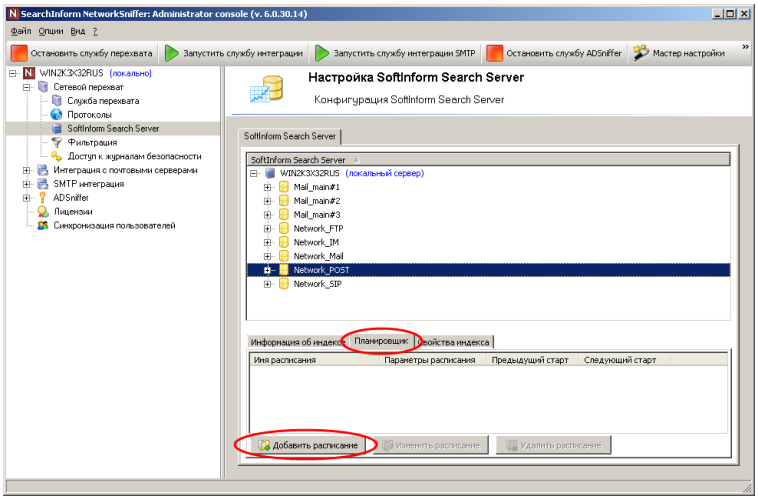


Рис. 2.70. Добавление расписания для индекса Network_POST

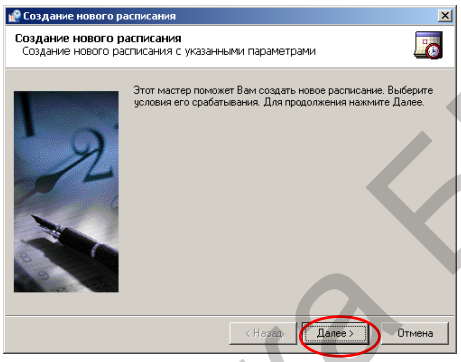


Рис. 2.71. Первый этап создания расписания

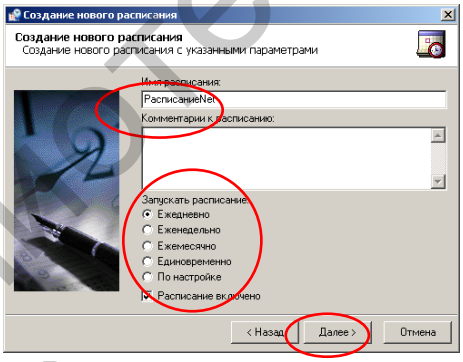


Рис. 2.72. Второй этап создания расписания

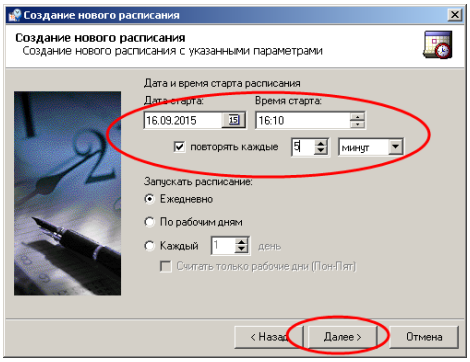


Рис. 2.73. Третий этап создания расписания

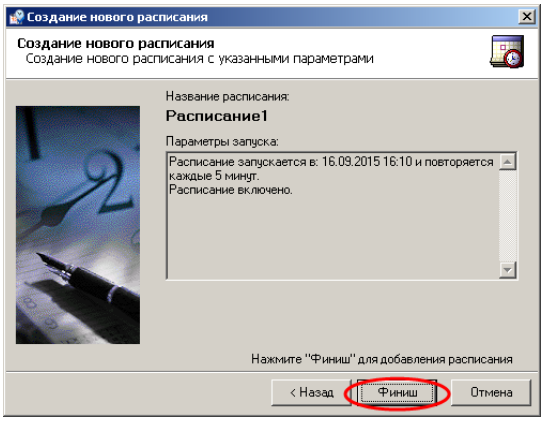


Рис. 2.74. Заключительный этап создания расписания

Закрыть окно NetworkSniffer Administrator Console.

Открыть окно AlertCenter Client. В соответствии с рис. 2.75 открыть ветвь «Политики безопасности».

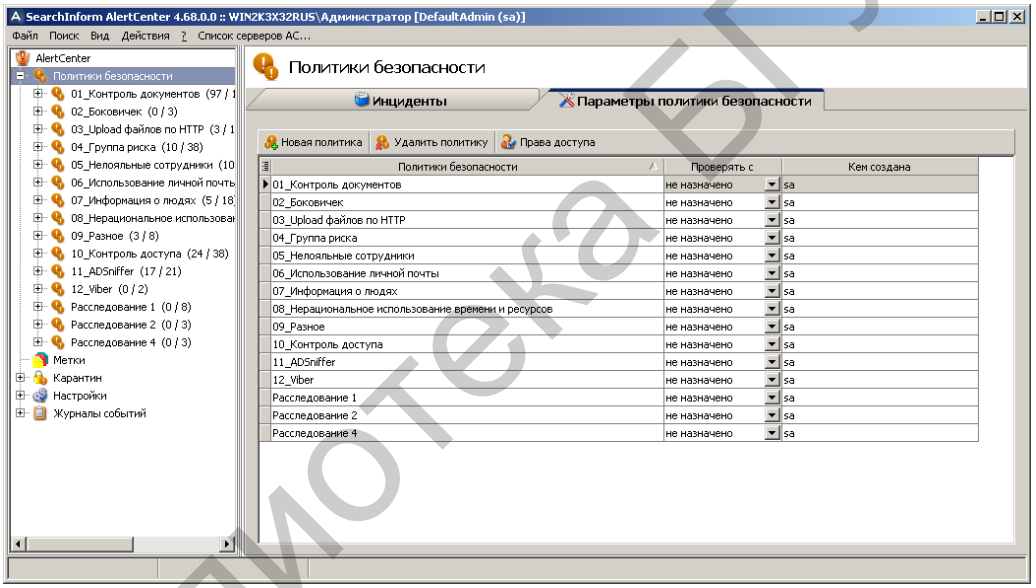


Рис. 2.75. Ветвь «Политики безопасности»

В соответствии с рис. 2.76–2.87 изменить параметры политики безопасности «06_использование личной почты». Предусмотреть использование индексов MailSniffer, отправку сообщений пользователю Admin, начало проверки индексов 16.09.2015, проверку индексов (ежедневно, только по рабочим дням, через каждые 20 мин). Исключить из проверки группу «Лояльные сотрудники».

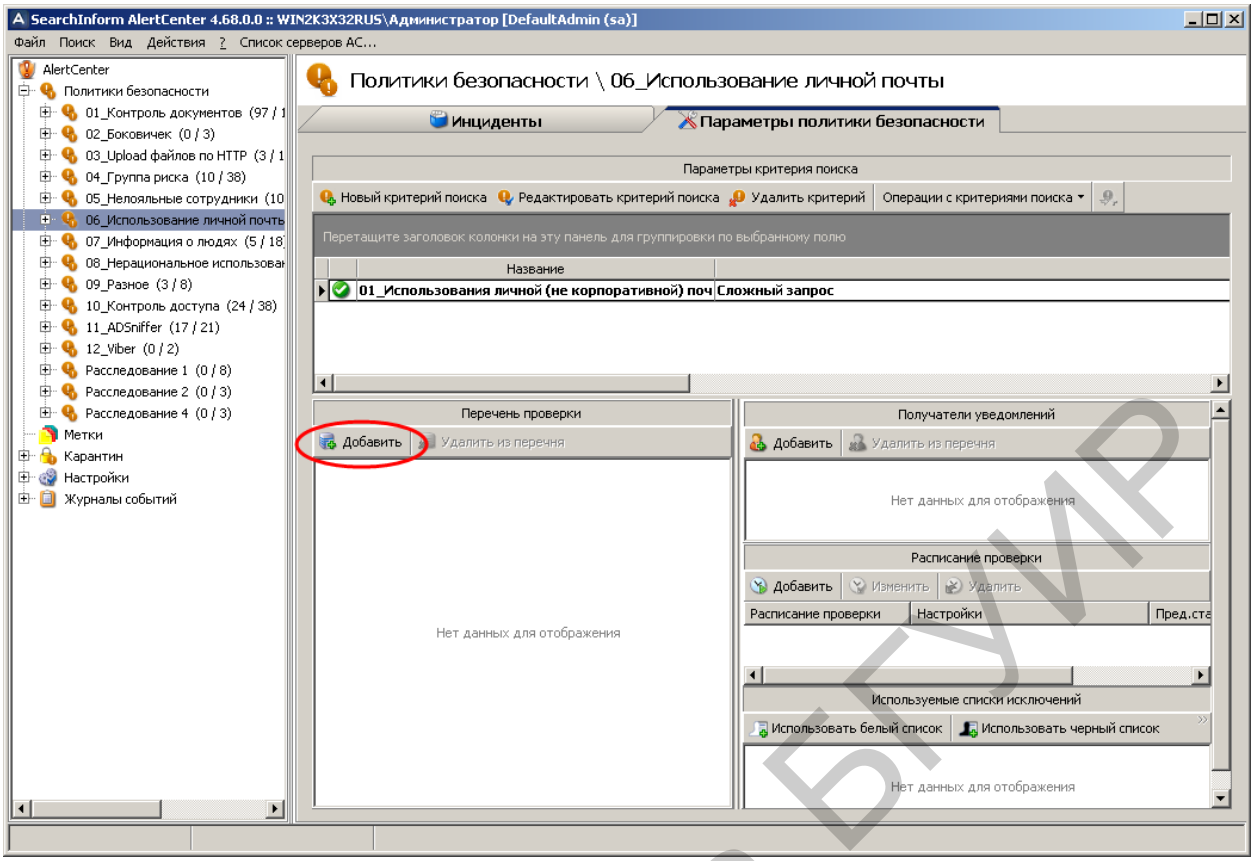


Рис. 2.76. Переход к настройке используемых индексов/баз данных

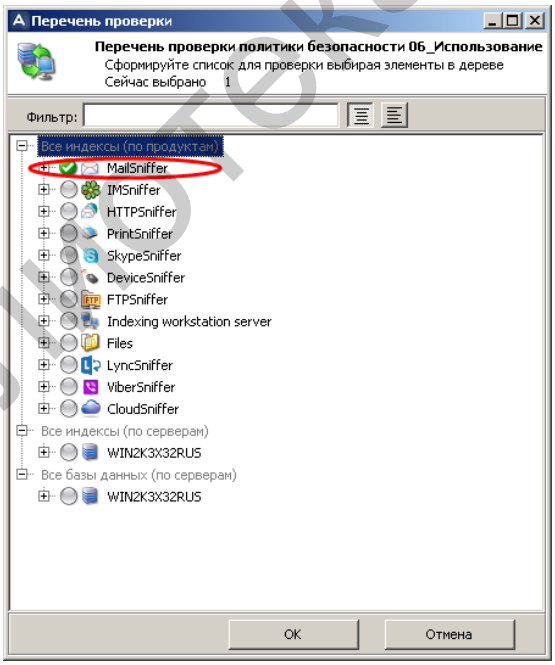


Рис. 2.77. Выбор индексов

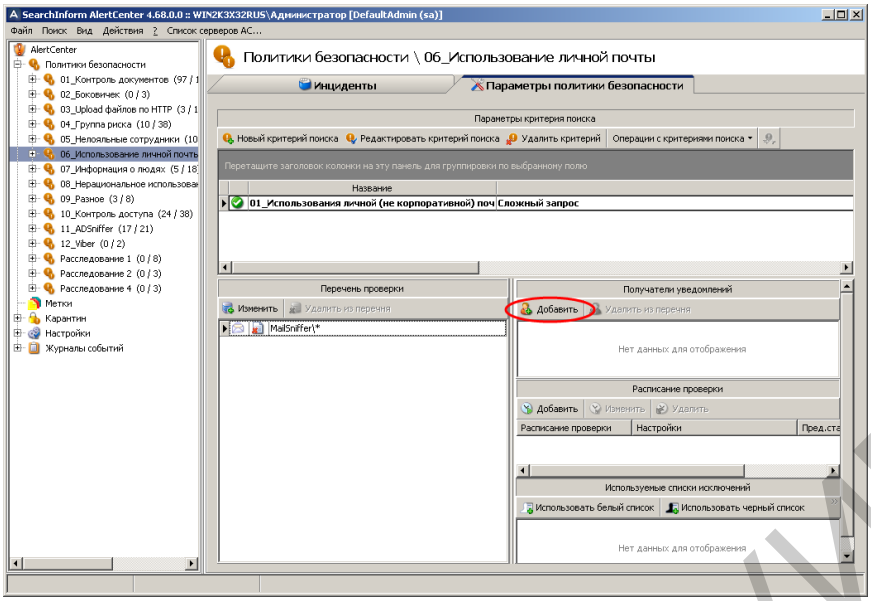


Рис. 2.78. Переход к настройке получателей уведомлений

Рис. 2.79. Выбор получателей уведомлений

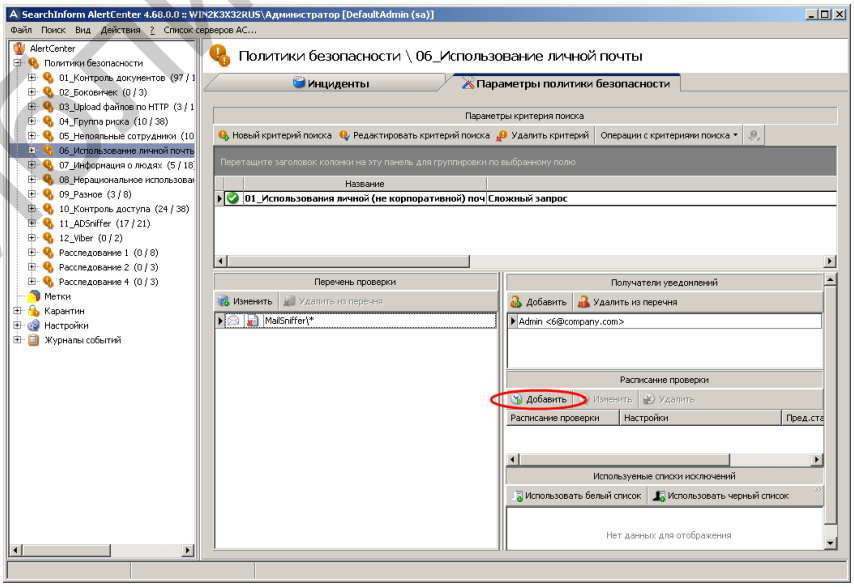


Рис. 2.80. Переход к настройке расписания

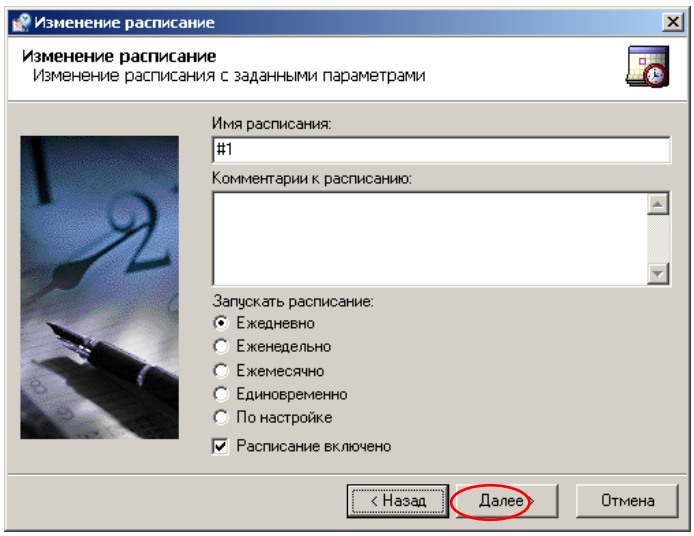


Рис. 2.81. Первый этап создания расписания

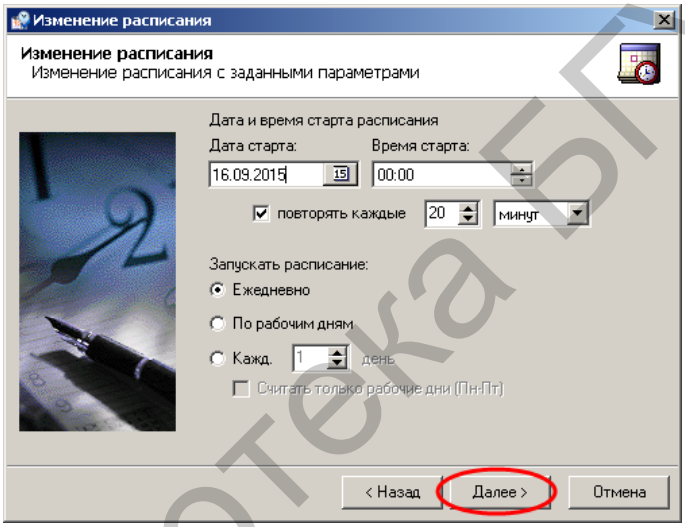


Рис. 2.82. Второй этап создания расписания

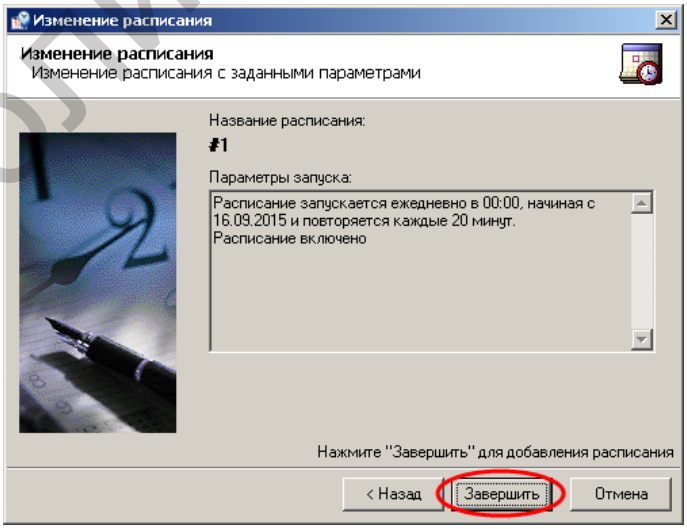


Рис. 2.83. Третий этап создания расписания

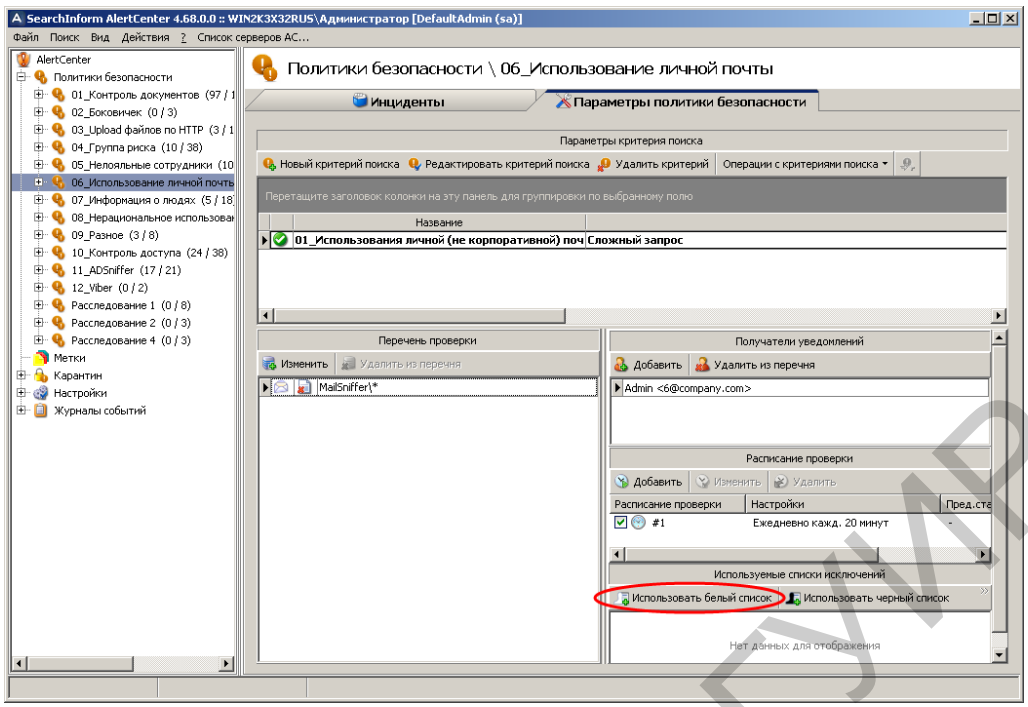


Рис. 2.84. Переход к использованию «белых списков»

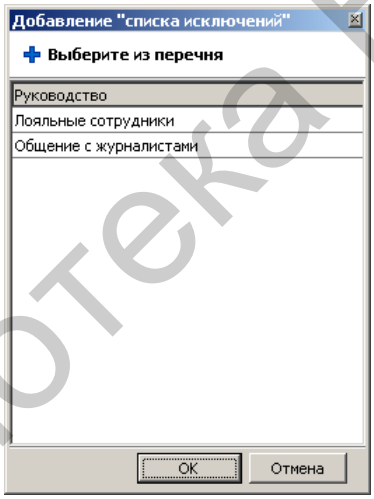


Рис. 2.85. Перечень доступных «белых списков»

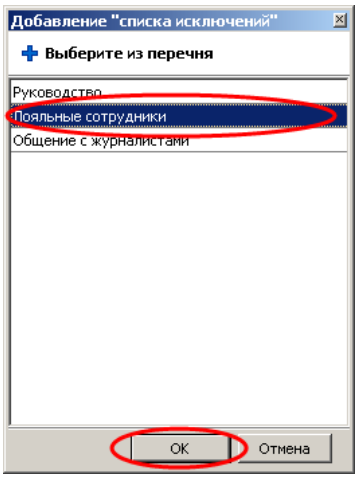


Рис. 2.86. Выбор «белого списка»

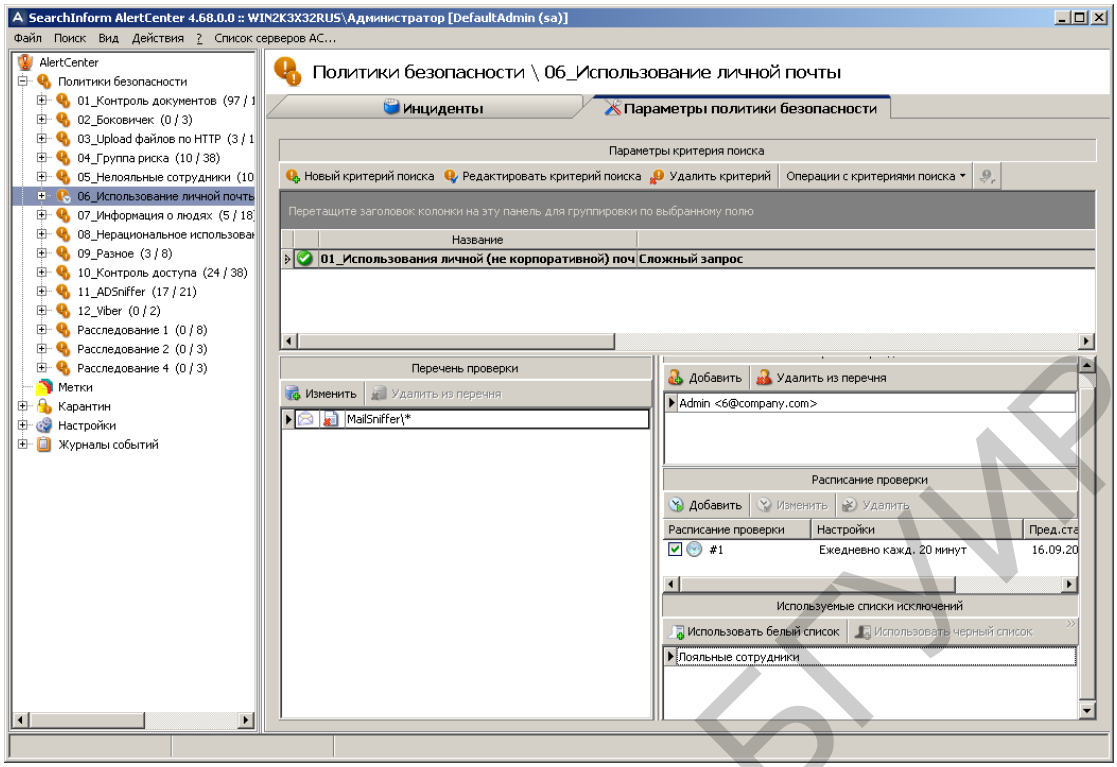


Рис. 2.87. Индикация параметров политики безопасности «06_Использование личной почты»

В соответствии с рис. 2.88 убедиться в наличии выявленных нарушений (инцидентов) политики «05_подозрительная почта».

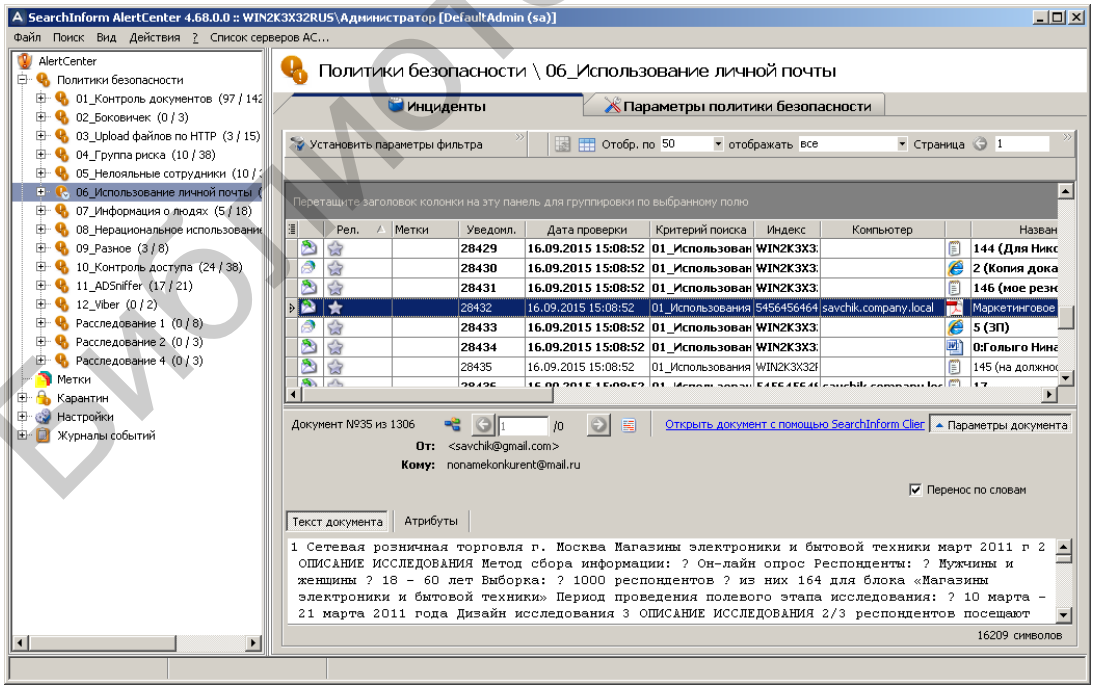


Рис. 2.88. Просмотр выявленых нарушений политики «05_подозрительная почта»

В соответствии с рис. 2.89–2.91 отредактировать белый список «Лояльные сотрудники». Добавить в него пользователя «linnik».

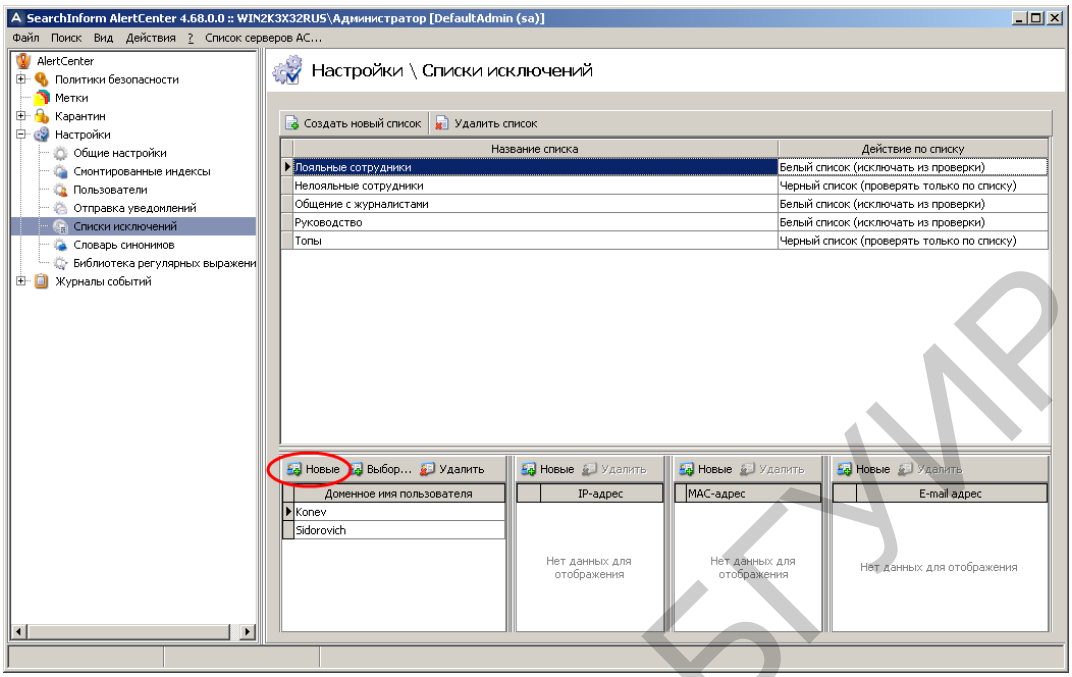


Рис. 2.89. Вход в режим добавления нового пользователя

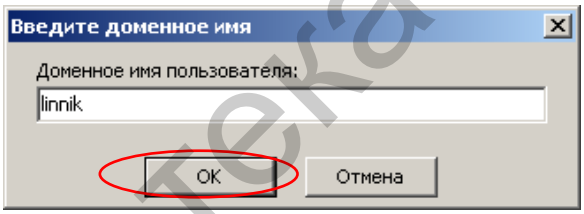


Рис. 2.90. Ввод имени пользователя

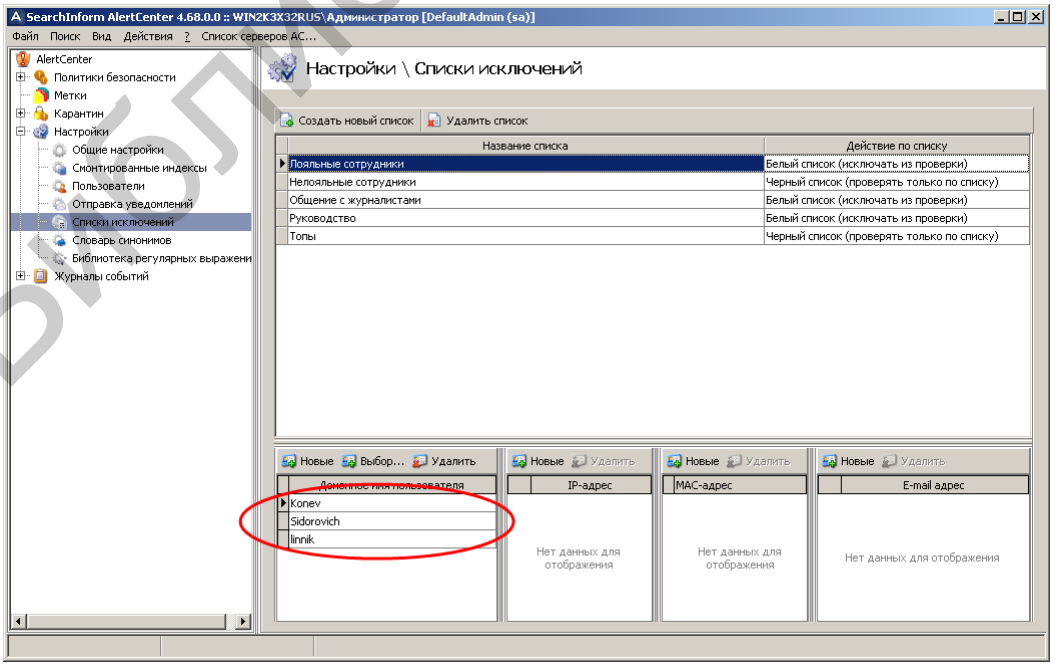


Рис. 2.91. Индикация пользователей в белом списке «Лояльные сотрудники»

В соответствии с рис. 2.92–2.97 создать белый список «Мой список», добавить в него пользователя «Администратор».

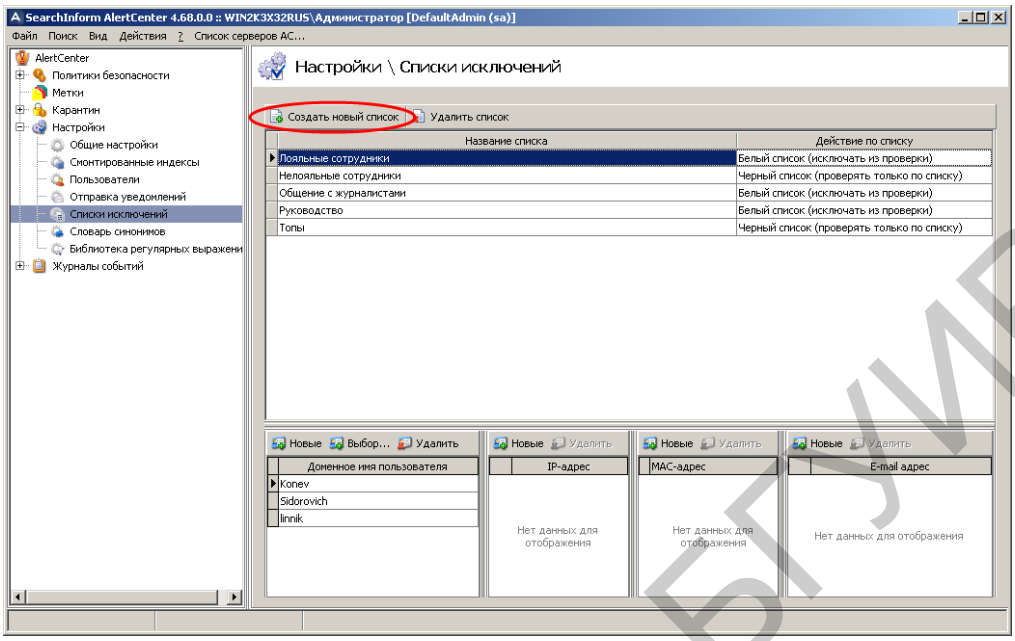


Рис. 2.92. Первый этап создания нового белого списка

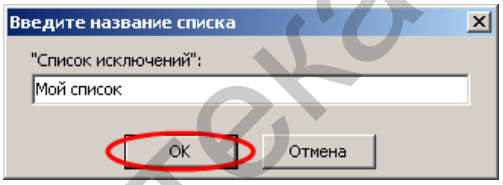


Рис. 2.93. Указание имени списка

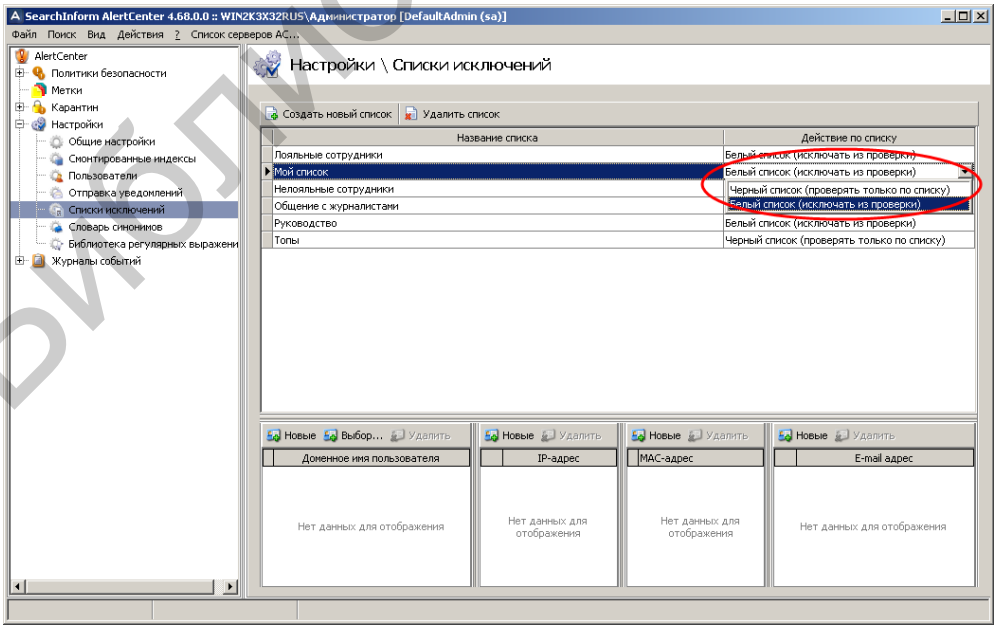


Рис. 2.94. Выбор типа списка

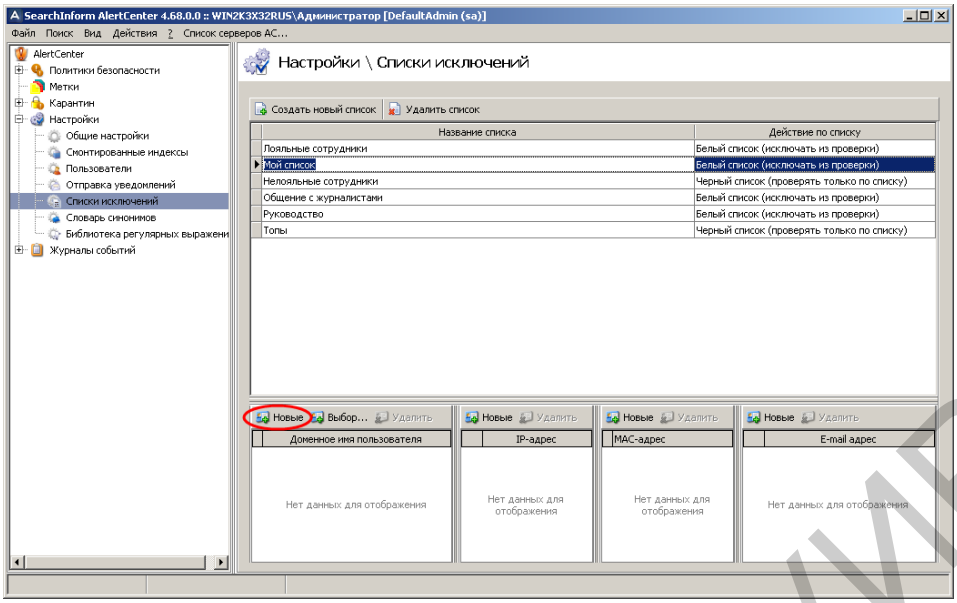


Рис. 2.95. Первый этап добавления нового пользователя в список

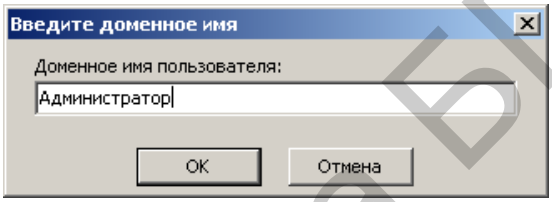


Рис. 2.96. Указание имени добавляемого пользователя

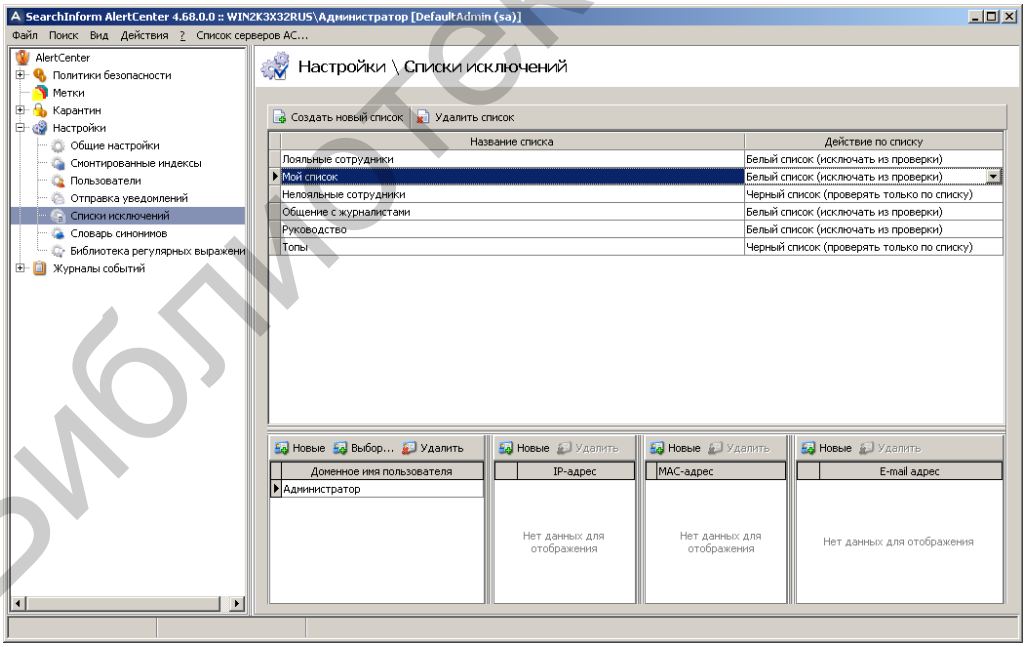


Рис. 2.97. Индикация параметров созданного списка «Мой список»

В соответствии с рис. 2.98–2.100 создать новую политику безопасности с названием «Тест1».

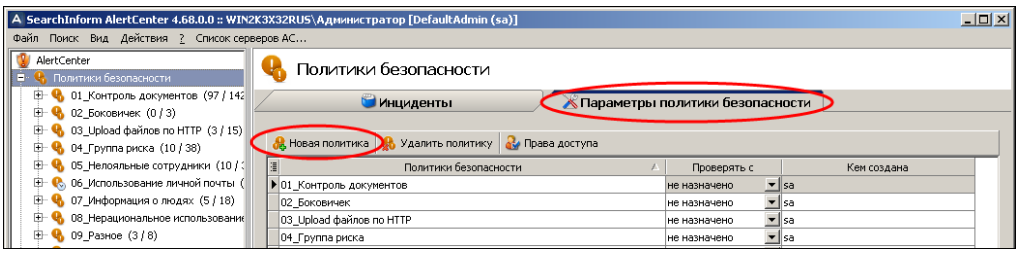


Рис. 2.98. Вход в режим создания новой политики

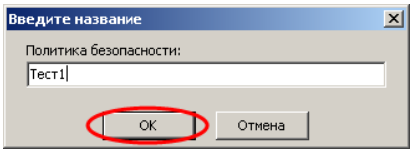


Рис. 2.99. Указание имени политики

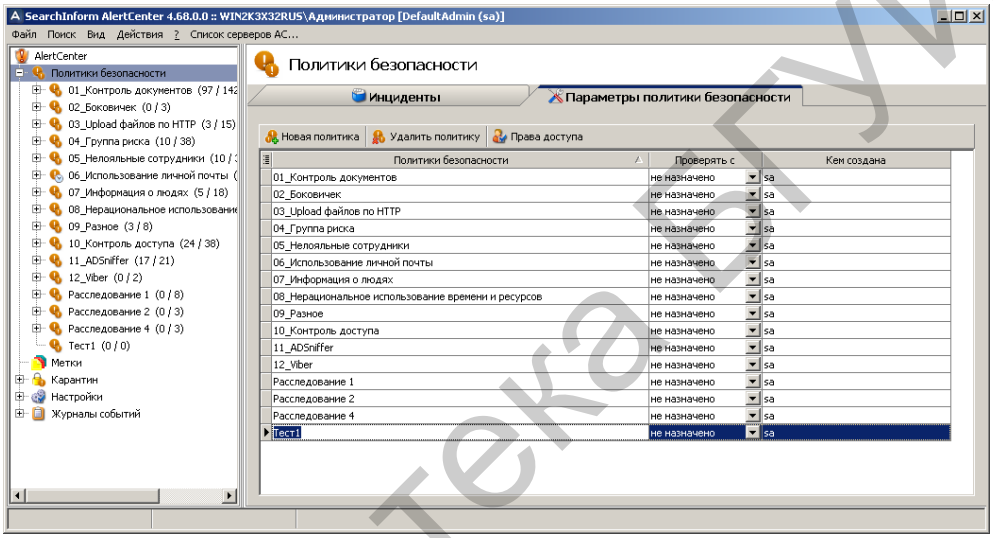


Рис. 2.100. Индикация созданной политики

В соответствии с рис. 2.101–2.105 добавить в политику «Тест1» поиск по ключевым словам и поиск по атрибутам перехваченных данных.

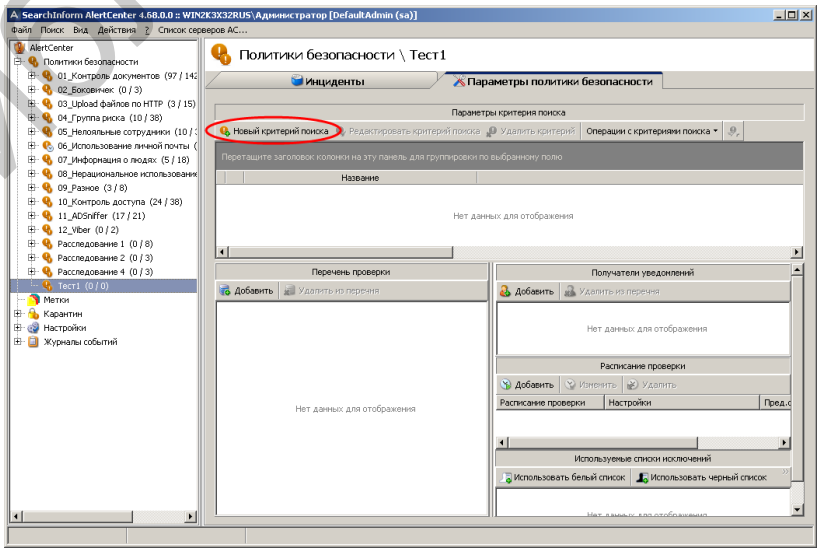


Рис. 2.101. Вход в режим создания критериев поиска

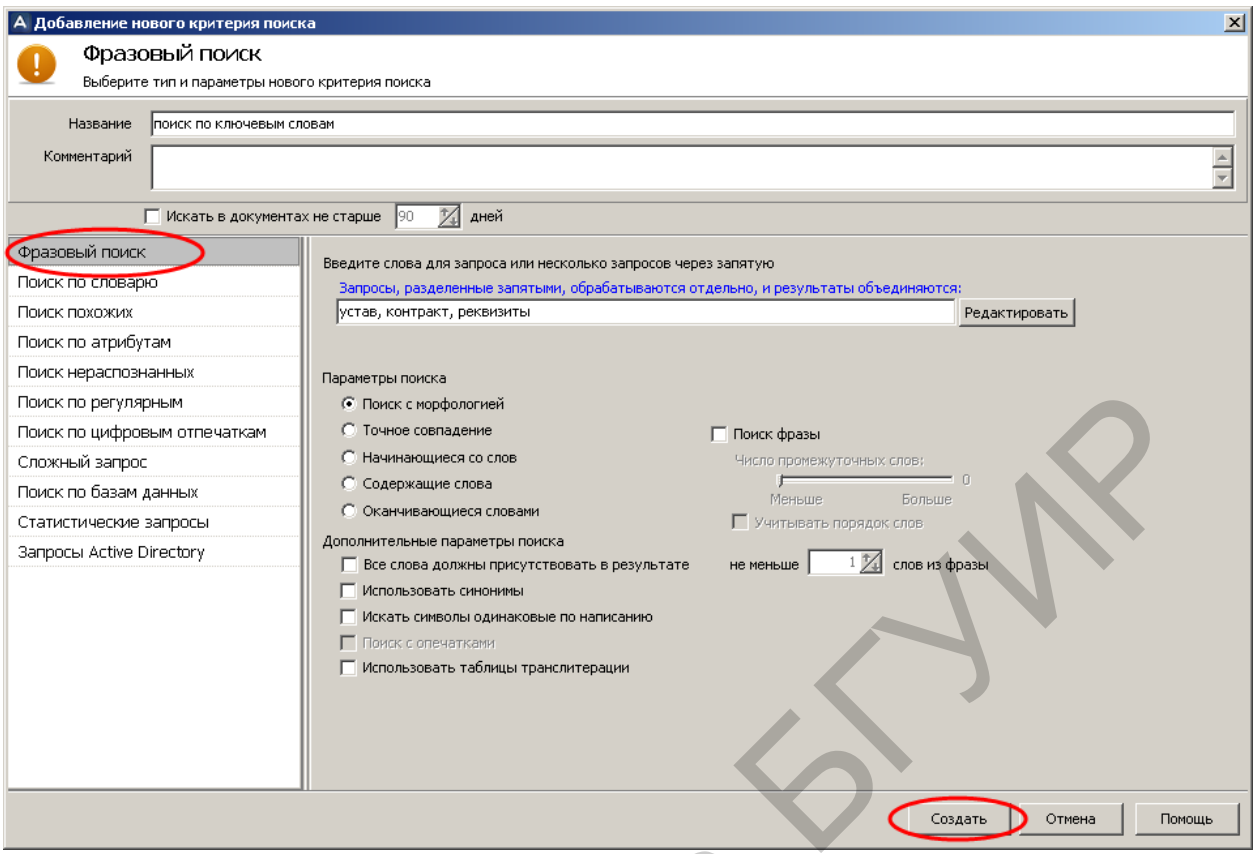


Рис. 2.102. Указание параметров поиска по ключевым словам

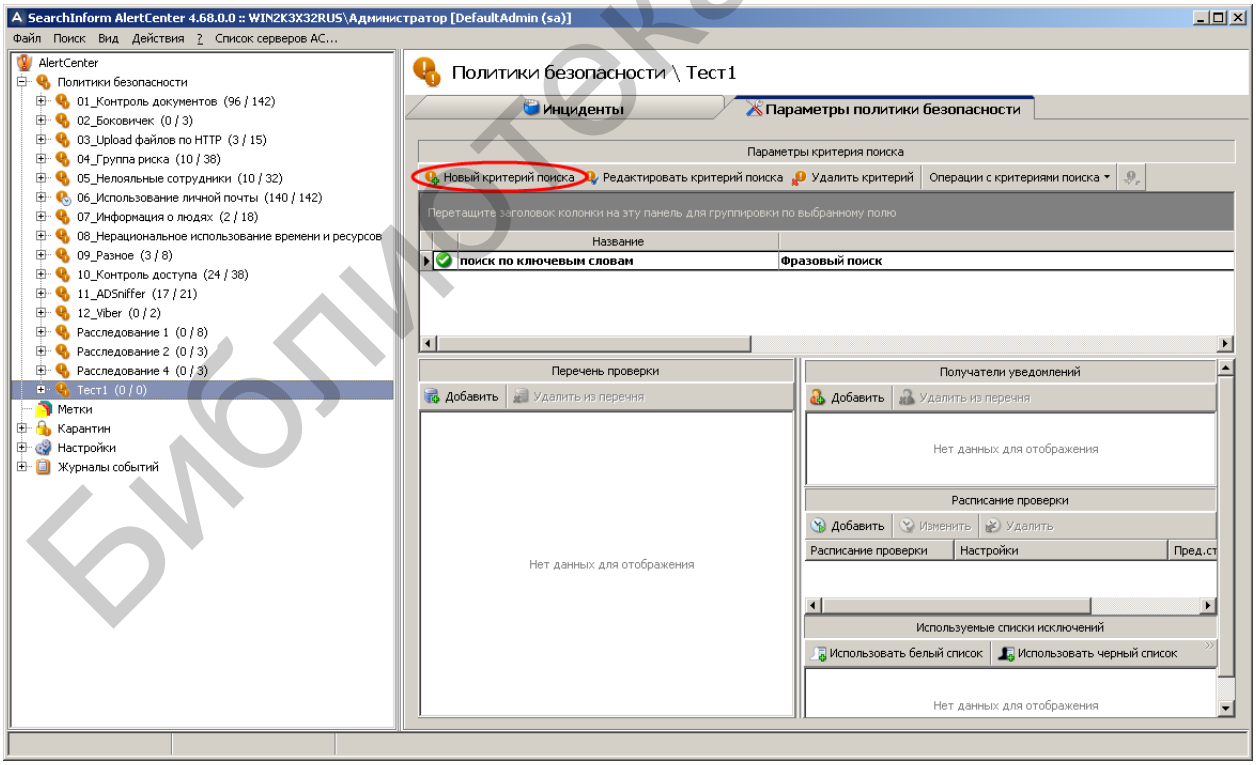


Рис. 2.103. Добавление второго поискового запроса

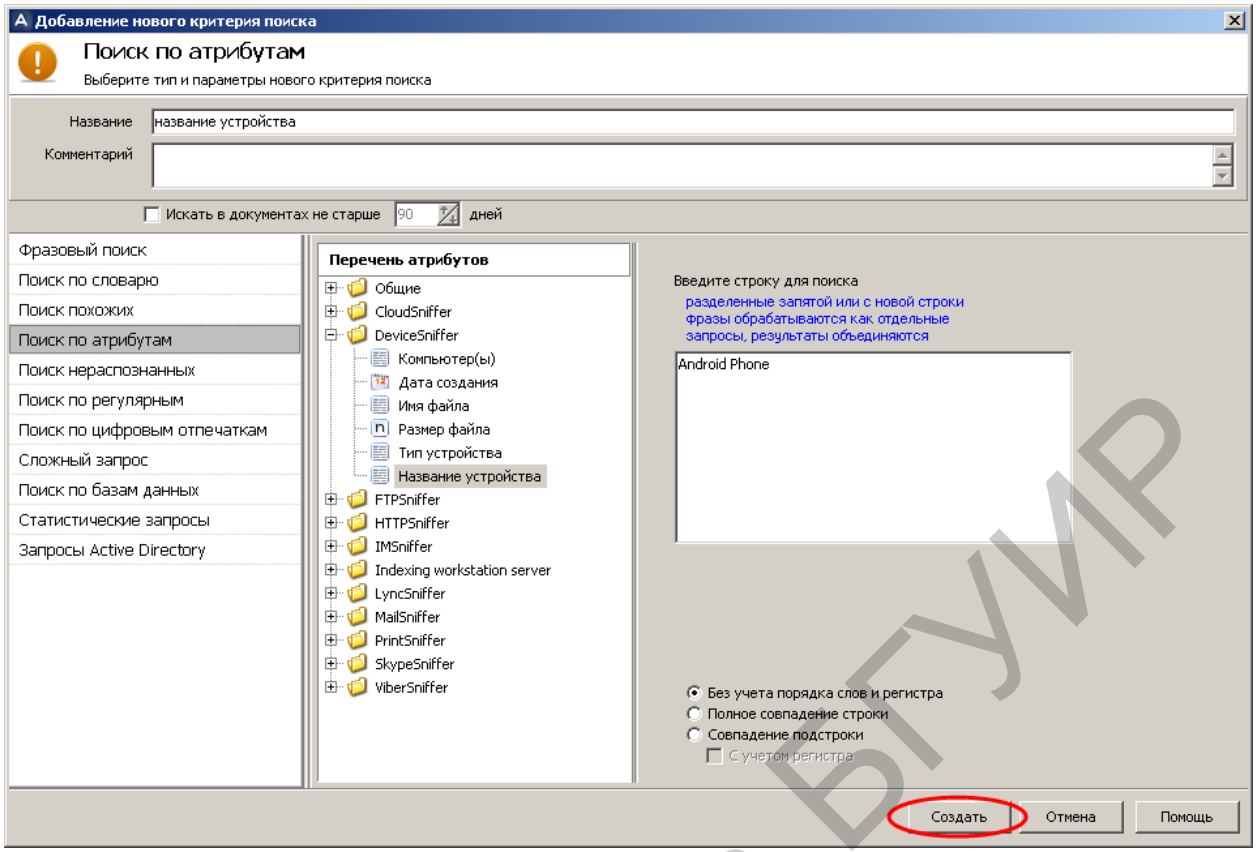


Рис. 2.104. Указание параметров поиска по атрибутам

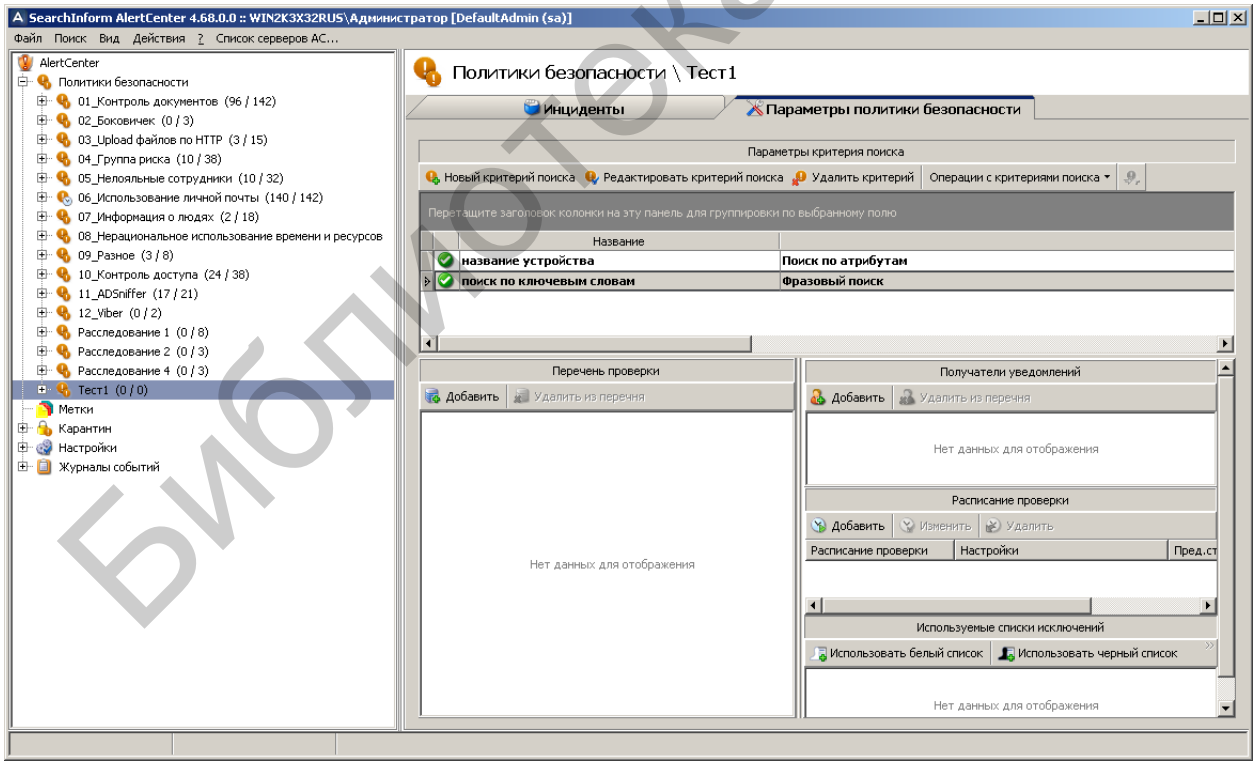


Рис. 2.105. Индикация созданных поисковых запросов

В соответствии с рис. 2.106–2.117 следует добавить в политику «Тест1» список проверяемых индексов, расписание проверки, список получателей уведомлений о нарушениях и список исключений пользователей.

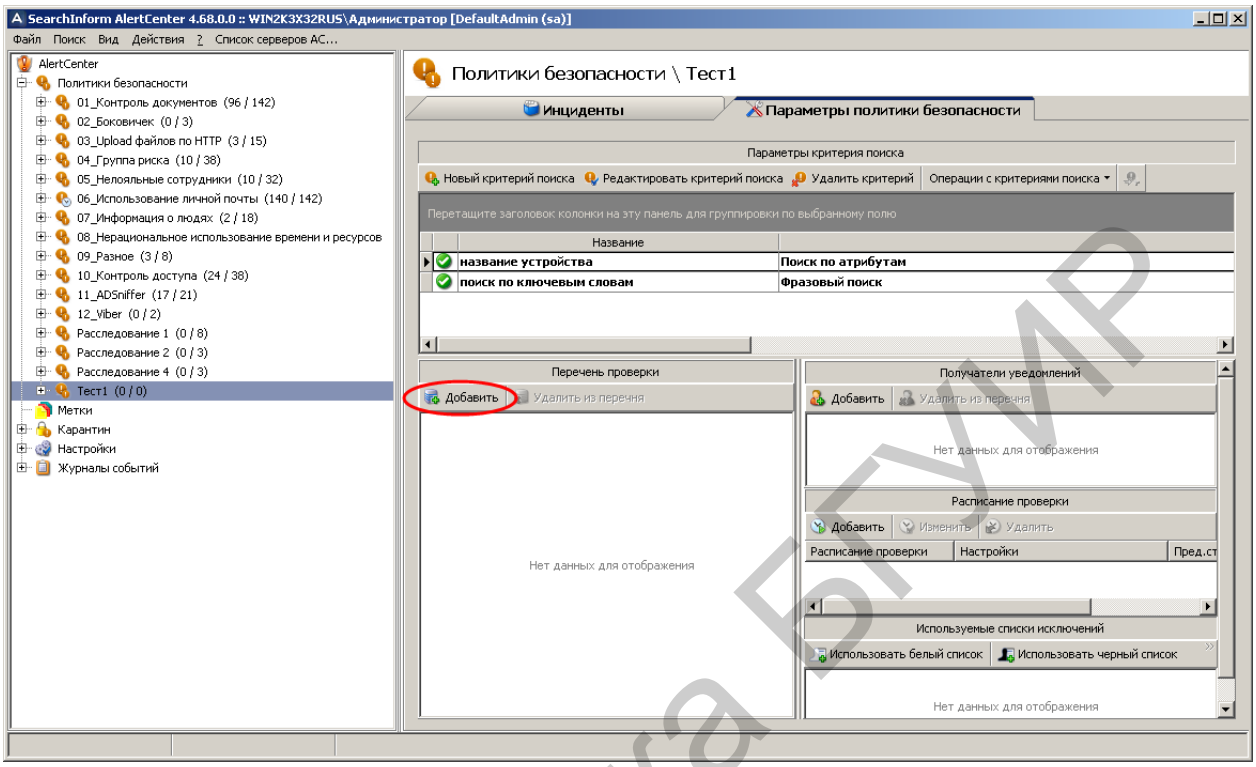


Рис. 2.106. Вход в режим добавления индексов
(для выделения нескольких критериев поиска используйте клавиши Ctrl и Shift)

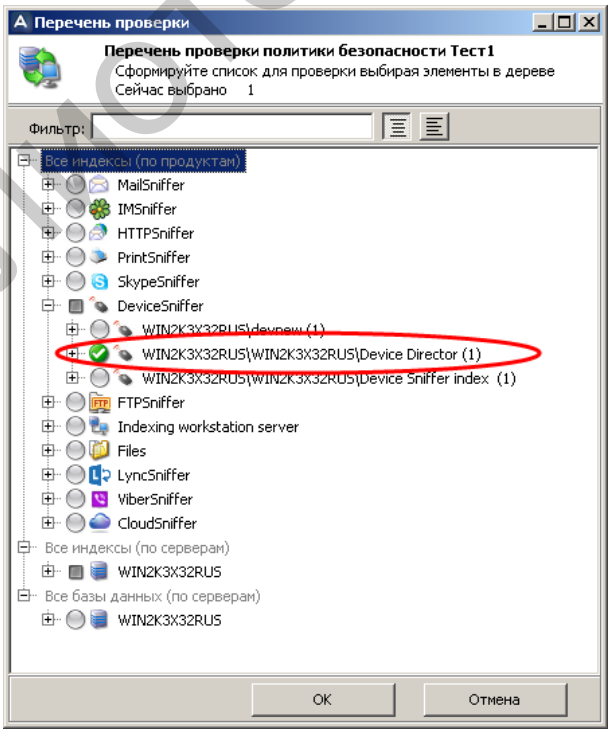


Рис. 2.107. Окно добавления имен индексов

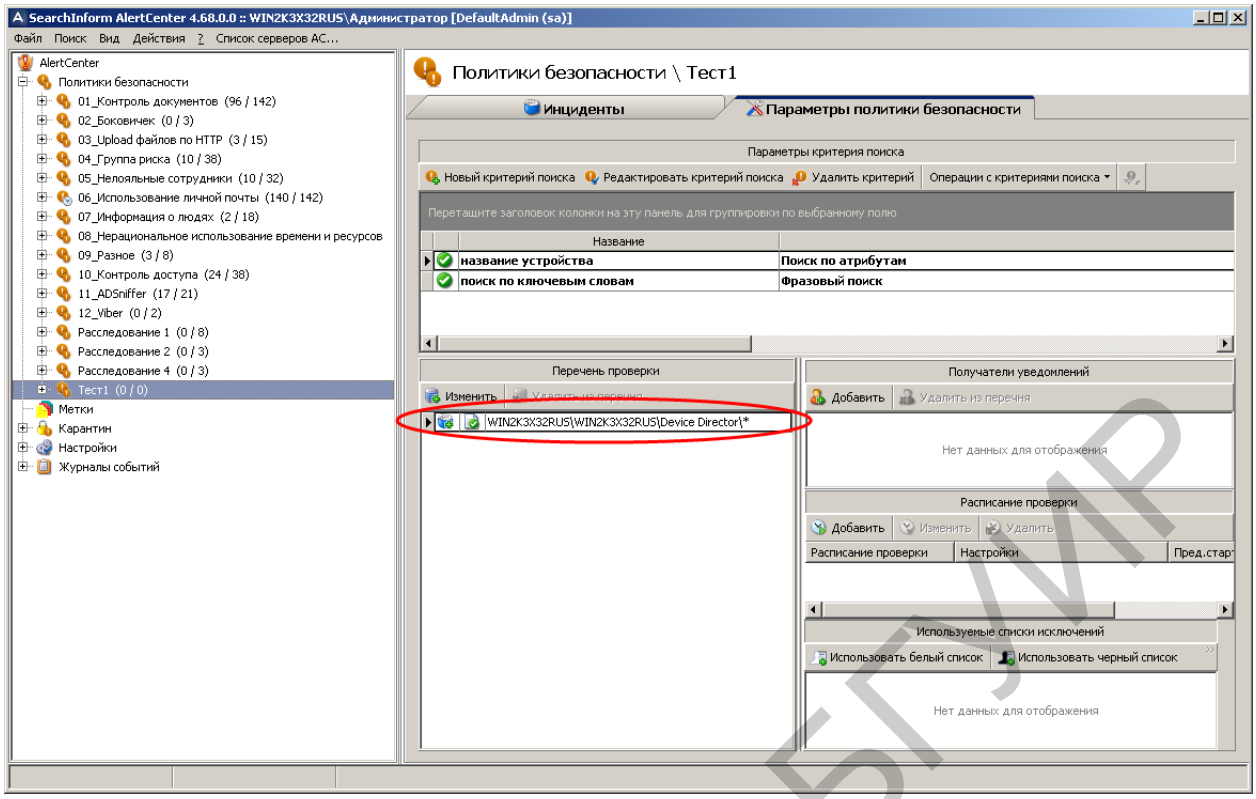


Рис. 2.108. Индикация выбранных индексов

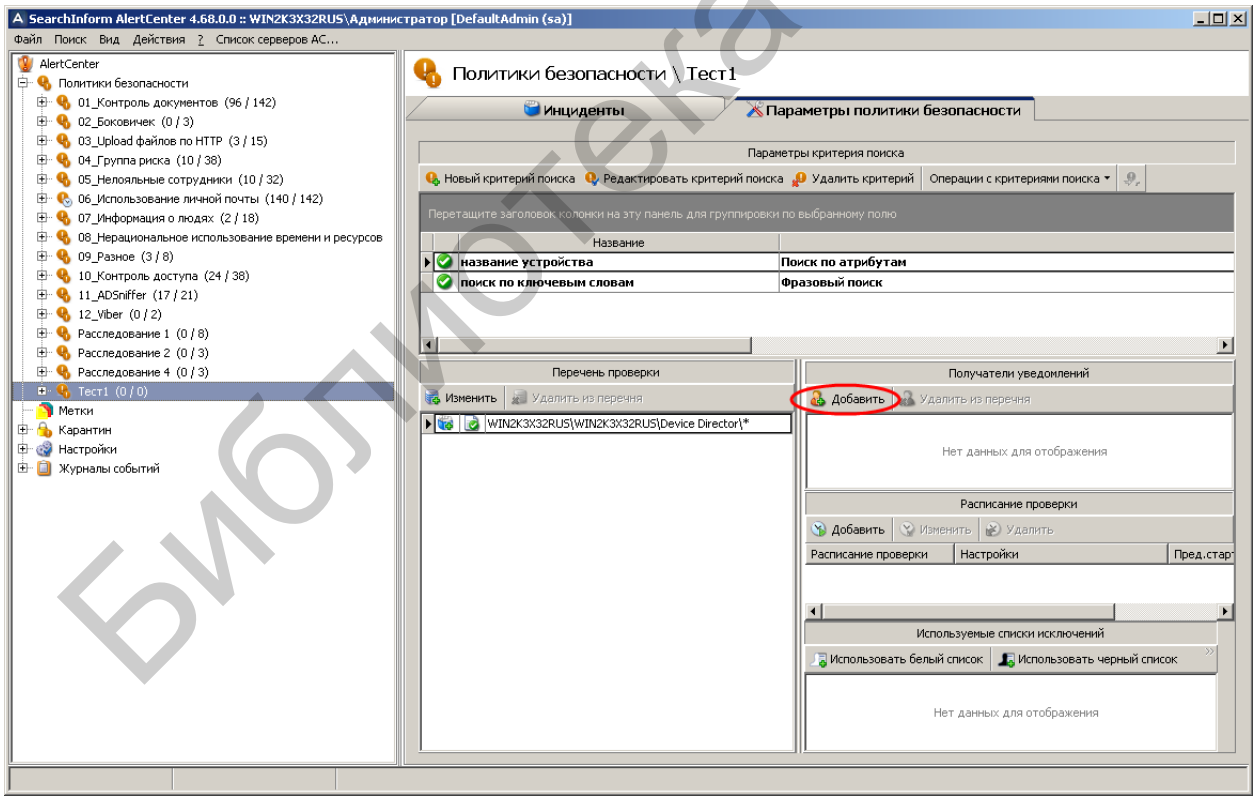


Рис. 2.109. Первый этап формирования списка получателей уведомлений о нарушениях политики безопасности «Тест1»

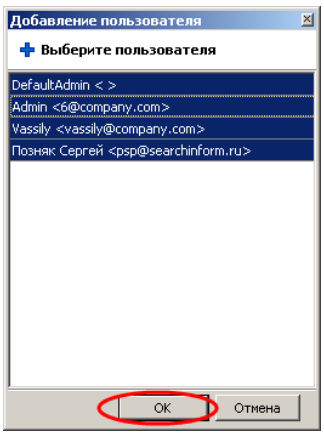


Рис. 2.110. Выбор имен получателей

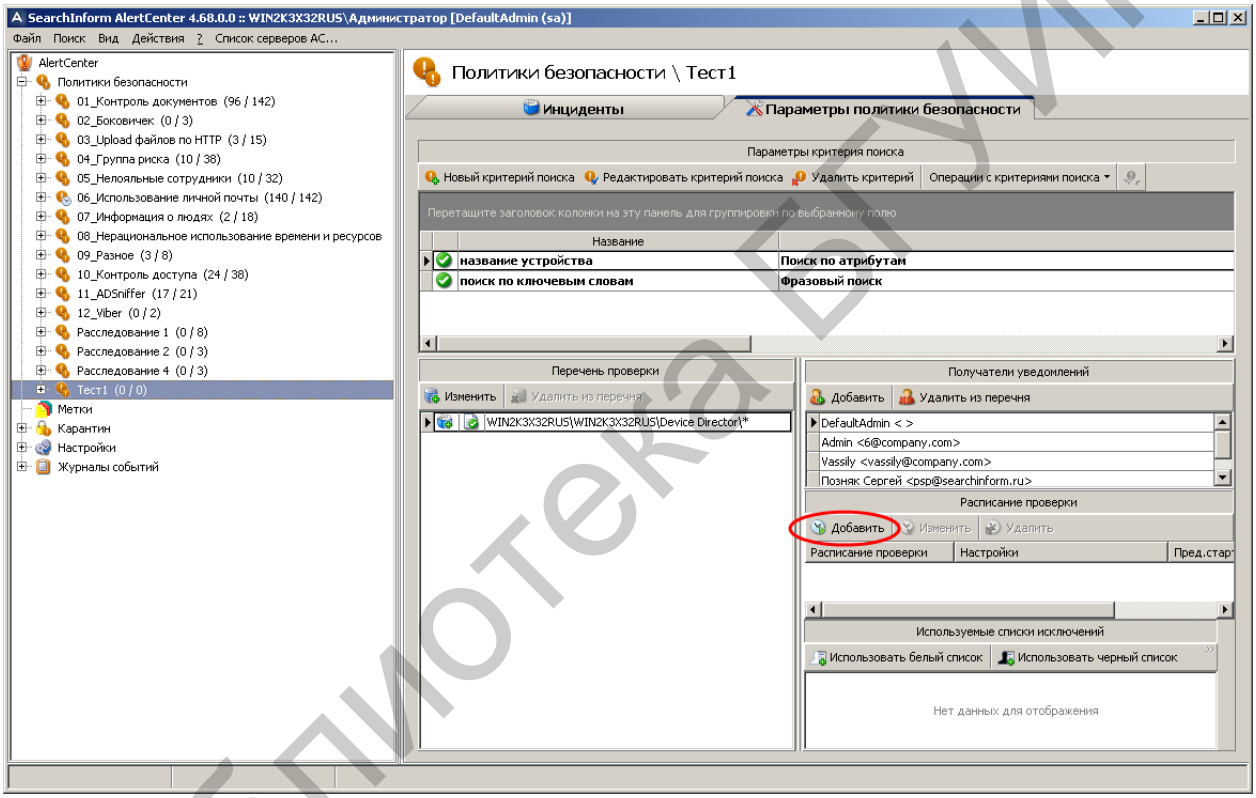


Рис. 2.111. Добавление нового расписания проверок индексов

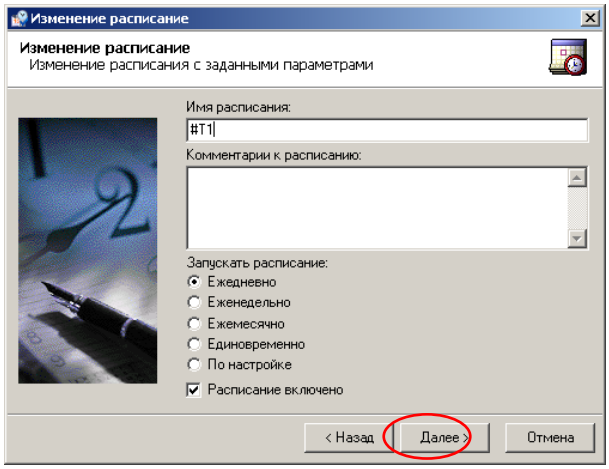


Рис. 2.112. Первый этап формирования расписания проверок индексов

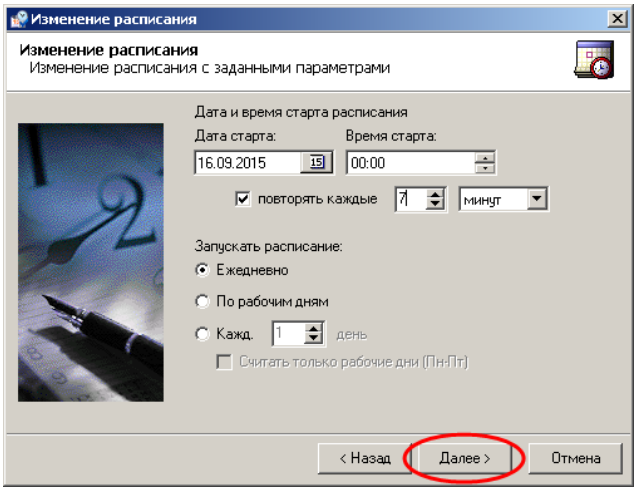


Рис. 2.113. Второй этап формирования расписания проверок индексов (частота проверки – 7 мин)

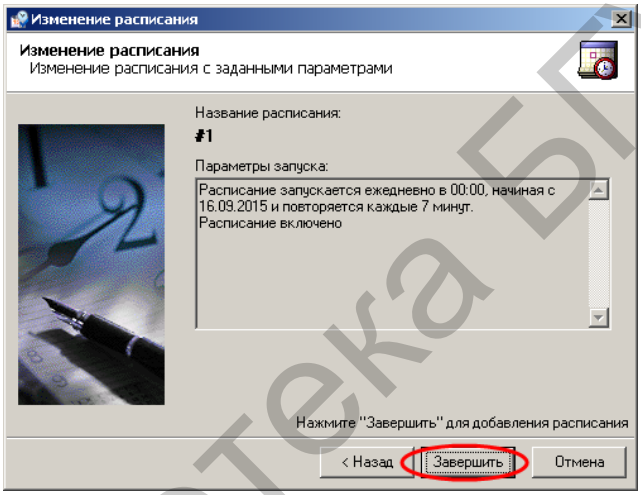


Рис. 2.114. Заключительный этап формирования расписания проверок индексов

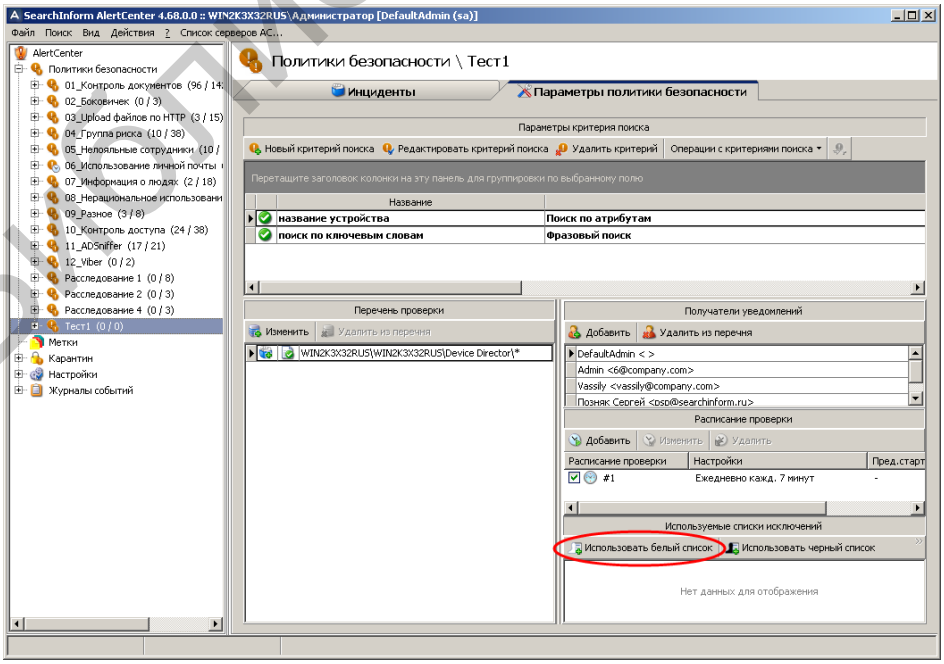


Рис. 2.115. Первый этап добавления списка исключений в политику «Тест1»

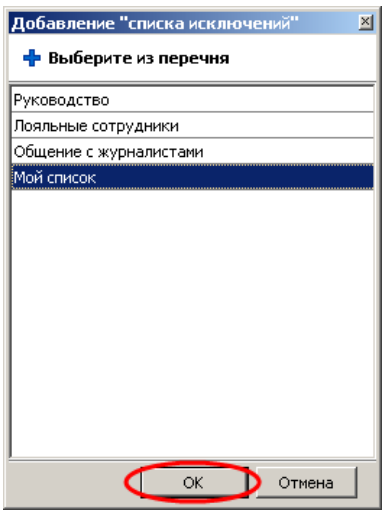


Рис. 2.116. Второй этап добавления списка «Мой список» в политику «Тест1»

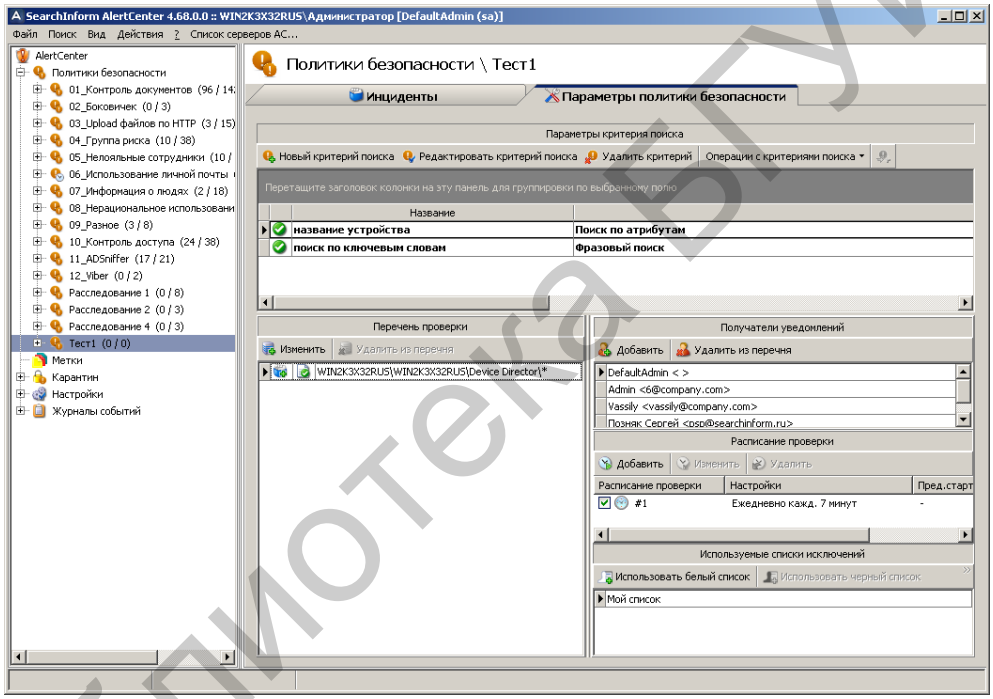


Рис. 2.117. Отображение параметров политики безопасности «Тест1»

В соответствии с рис. 2.118 просмотреть инциденты, связанные с нарушением политики безопасности «Тест1». Проверка автоматически произведется через 7 мин после окончания формирования политики, или в соответствии с рис. 2.119 можно запустить проверку принудительно. Просмотр осуществляется на вкладке «Инциденты».

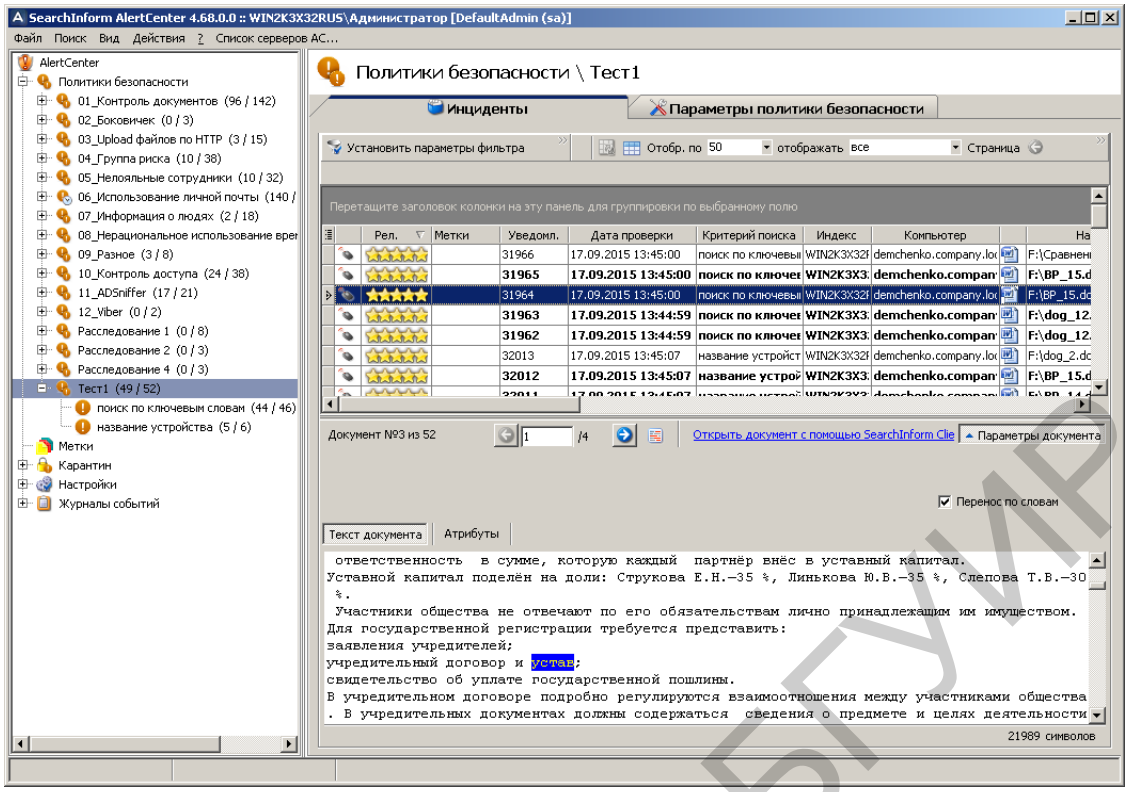


Рис. 2.118. Проверка выявленных нарушений

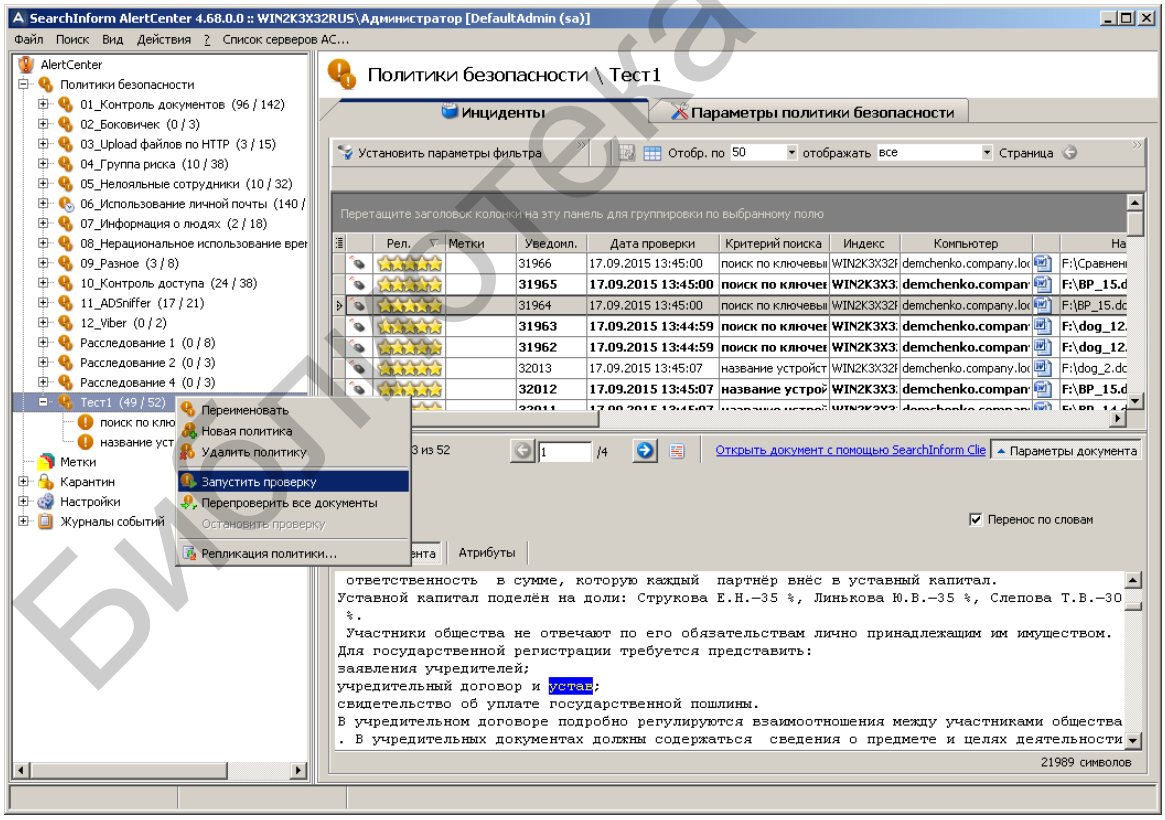


Рис. 2.119. Принудительный запуск проверки политики «Тест1»

В соответствии с рис. 2.120 отключить выполнение расписания политик безопасности «Тест1».

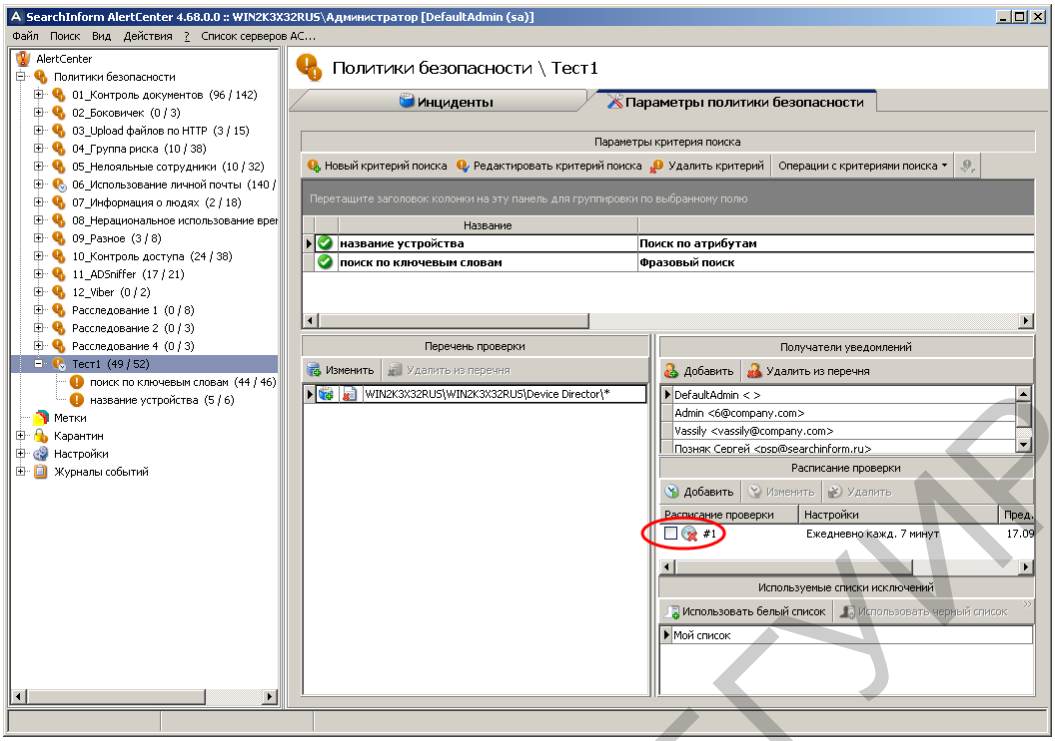


Рис. 2.120. Отключение выполнения расписания политики «Тест1»

Закрыть окно AlertCenter Client. Завершить работу с виртуальным компьютером.

2.3. Задание для самостоятельной работы

1. Отключить выполнение расписания политики «06_Использование личной почты».
2. Сформировать параметры собственной политики безопасности, которые должны включать в себя: расписание проверки, список индексов/баз данных для проверки, перечень списков исключений, несколько простейших критериев поиска конфиденциальной информации.
3. Согласовать параметры политики безопасности с преподавателем.
4. Реализовать политику безопасности.
5. Просмотреть перечень выявленных нарушений.

2.4. 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 неструктурированных документов?
6. Что такое фильтр ограничений по перехвату?
7. Что такое «список исключений»?
8. Как используется «белый список»?

ЛАБОРАТОРНАЯ РАБОТА №3
НАСТРОЙКА ПРОГРАММНОГО КОМПЛЕКСА SEARCHINFORM ДЛЯ КОНТРОЛЯ СОДЕРЖИМОГО ЭКРАНОВ ПОЛЬЗОВАТЕЛЕЙ И ПОИСКА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ БЕЗ ПРОВЕДЕНИЯ СИНТАКСИЧЕСКОГО АНАЛИЗА

Цель: освоить основные приемы реализации периодического и оперативного контроля экранов пользователей, а также методы формирования критериев поиска конфиденциальной информации «по атрибутам» и «нераспознанных».

3.1. Теоретическая часть

1. Ознакомиться с разделами 1–5 руководства аудитора безопасности системы SearchInform.

2. Ознакомиться со справочными материалами SearchInform EndpointSniffer, SearchInform Client, SearchInform AlertCenter.

3.2. Лабораторное задание

1. В соответствии с методическими указаниями лабораторной работы №1 запустить виртуальный компьютер с установленным программным комплексом SearchInform. Установить на виртуальном компьютере дату 22.09.2015.

2. Убедиться в том, что сервер AlertCenter работает, в противном случае его следует запустить с помощью консоли SearchInform AlertCenter Console.

Открыть окно консоли SearchInform EndpointSniffer. При необходимости следует ввести пароль, заданный в предыдущих лабораторных работах.

В соответствии с рис. 3.1–3.4 проверить подключение агента MonitorSniffer к базе данных.

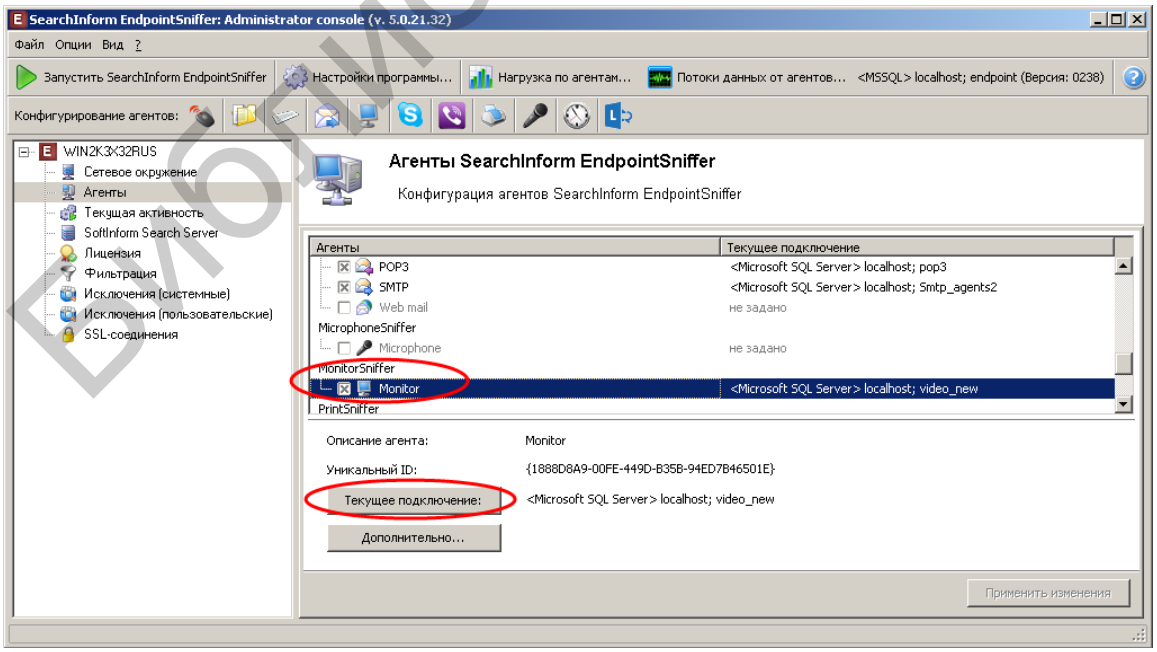


Рис. 3.1. Вход в режим просмотра параметров текущего подключения

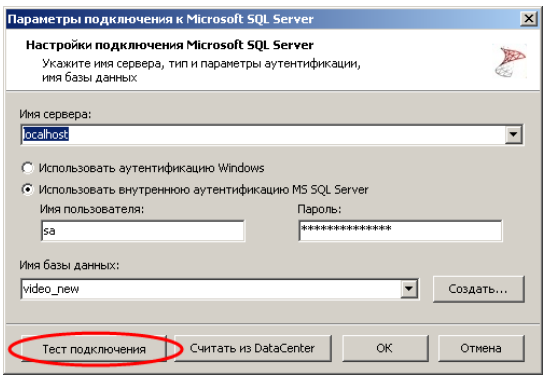


Рис. 3.2. Тестирование подключения к базе данных

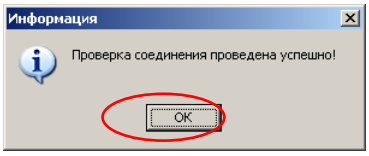


Рис. 3.3. Индикация успешного подключения

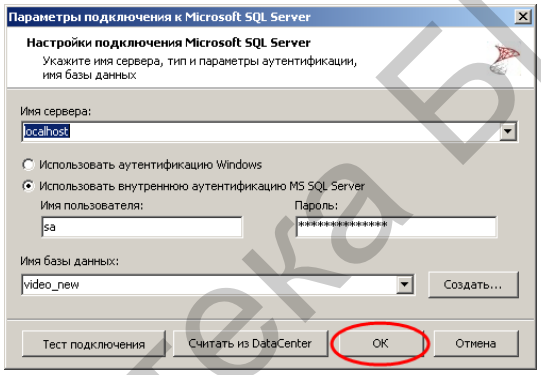


Рис. 3.4. Выход из режима просмотра параметров подключения

В соответствии с рис. 3.5 и 3.6 войти в режим редактирования настроек мониторинга изображений на экране и запущенных процессов на компьютере пользователя.

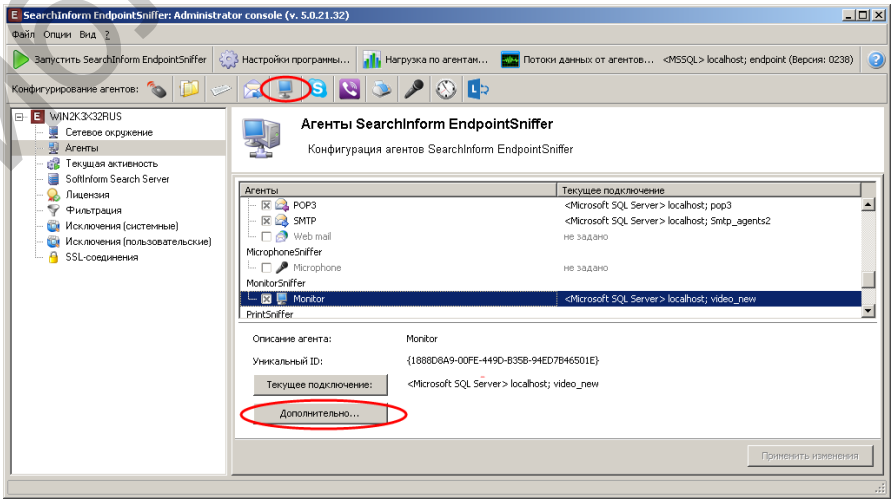


Рис. 3.5. Вход в режим редактирования параметров мониторинга экрана и запущенных процессов

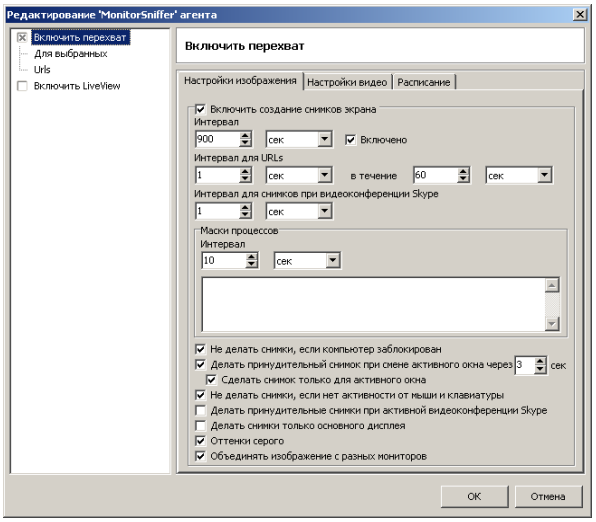


Рис. 3.6. Окно редактирования параметров мониторинга с первоначальными установками

В соответствии с рис. 3.7–3.10 изменить параметры мониторинга.

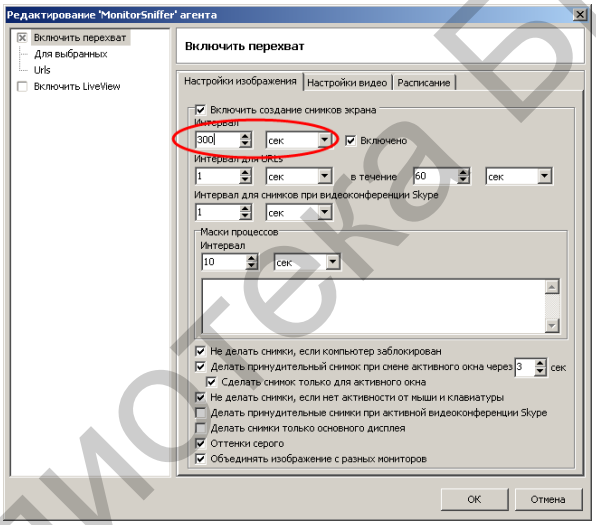


Рис. 3.7. Изменение интервала снятия снимков экрана

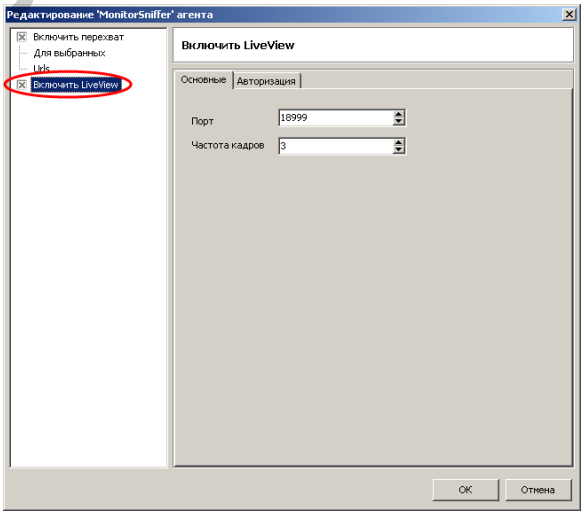


Рис. 3.8. Включение режима оперативного контроля экрана

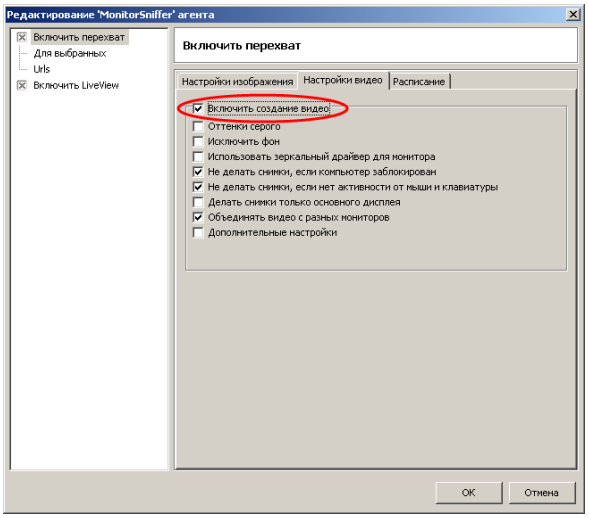


Рис. 3.9. Включение режима записи видео

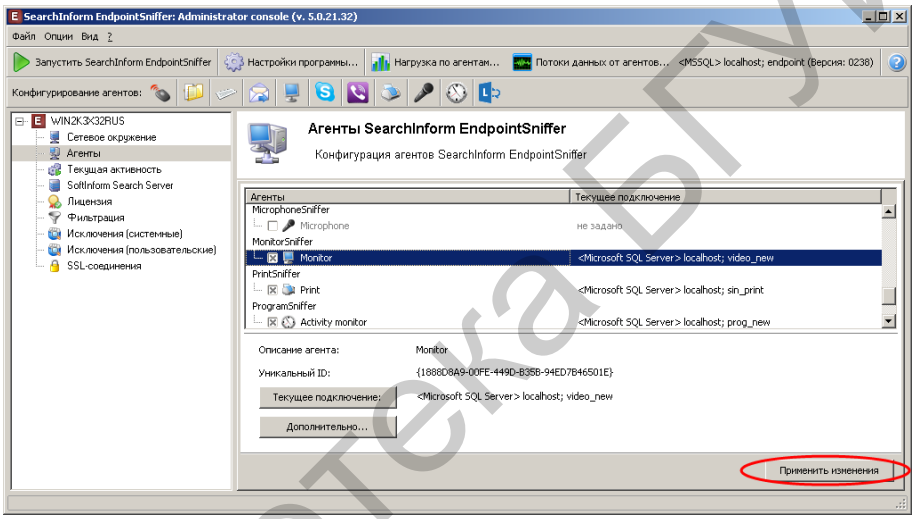


Рис. 3.10. Подтверждение измененных параметров

В соответствии с рис. 3.11 и 3.12 запустить сервер SearchInform EndpointSniffer.

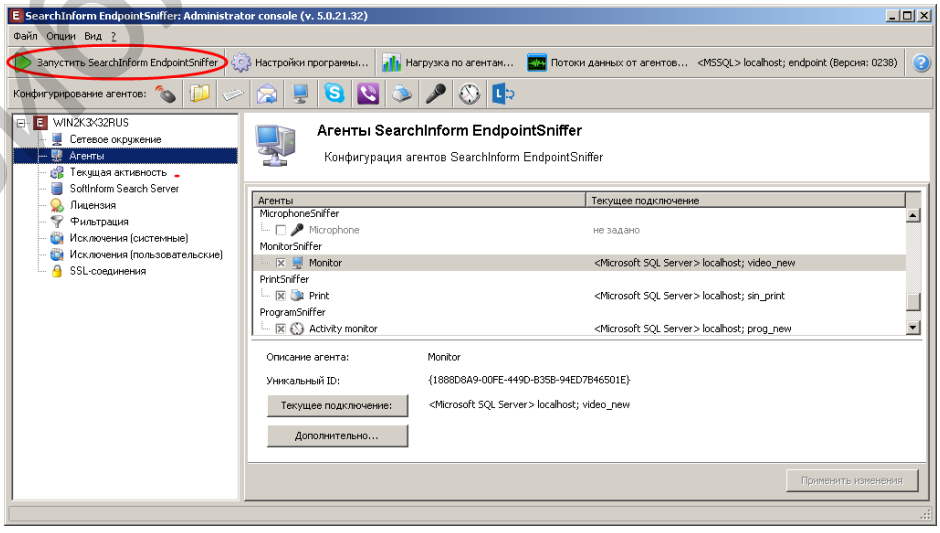


Рис. 3.11. Запуск сервера SearchInform EndpointSniffer

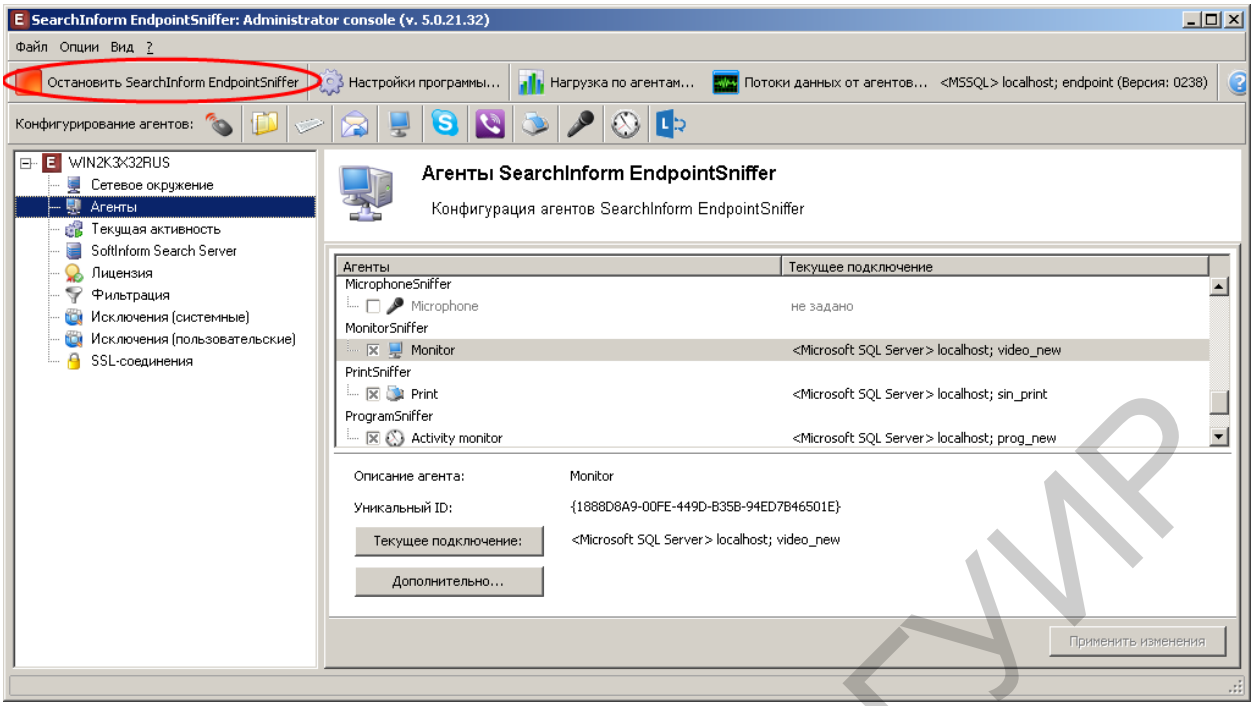


Рис. 3.12. Индикация функционирования сервера SearchInform EndpointSniffer

Закрыть окно серверного приложения SearchInform EndpointSniffer. С помощью соответствующего ярлыка запустить SearchInform Client, окно которого показано на рис. 3.13.

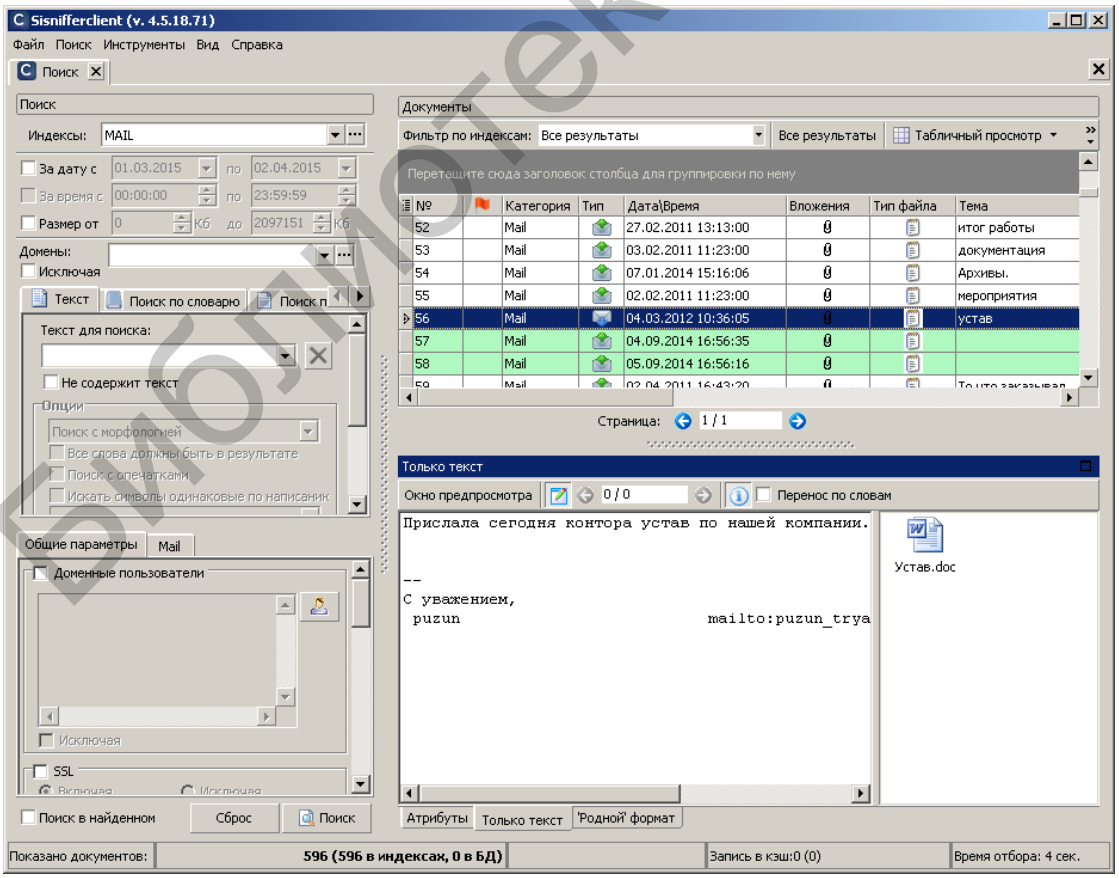


Рис. 3.13. Окно SearchInform Client

В соответствии с рис. 3.14 и 3.15 подключиться к базе данных перехваченных снимков экрана, отредактировать временной интервал сохраненных изображений и произвести поиск всех хранящихся снимков экрана за 1–2 прошедших года (рис. 3.16). Зафиксировать время выполнения поиска.

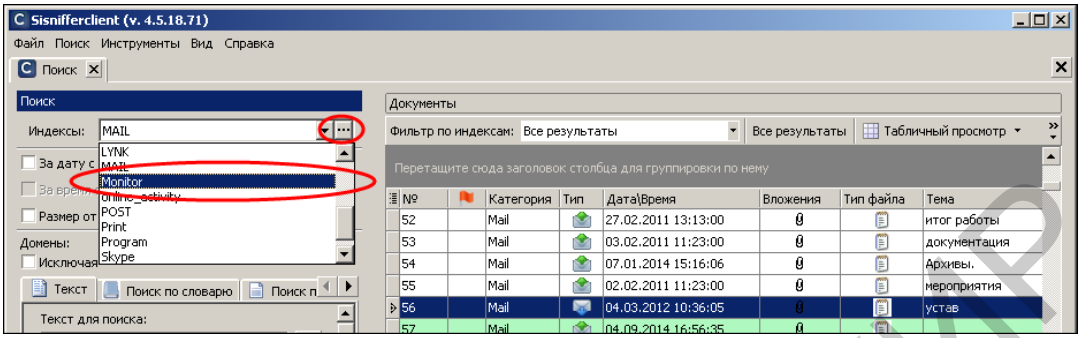


Рис. 3.14. Подключение к базе данных снимков экрана

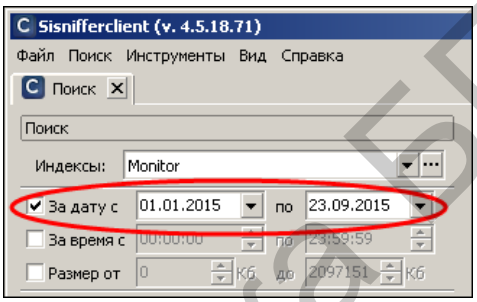


Рис. 3.15. Редактирование временного интервала поиска

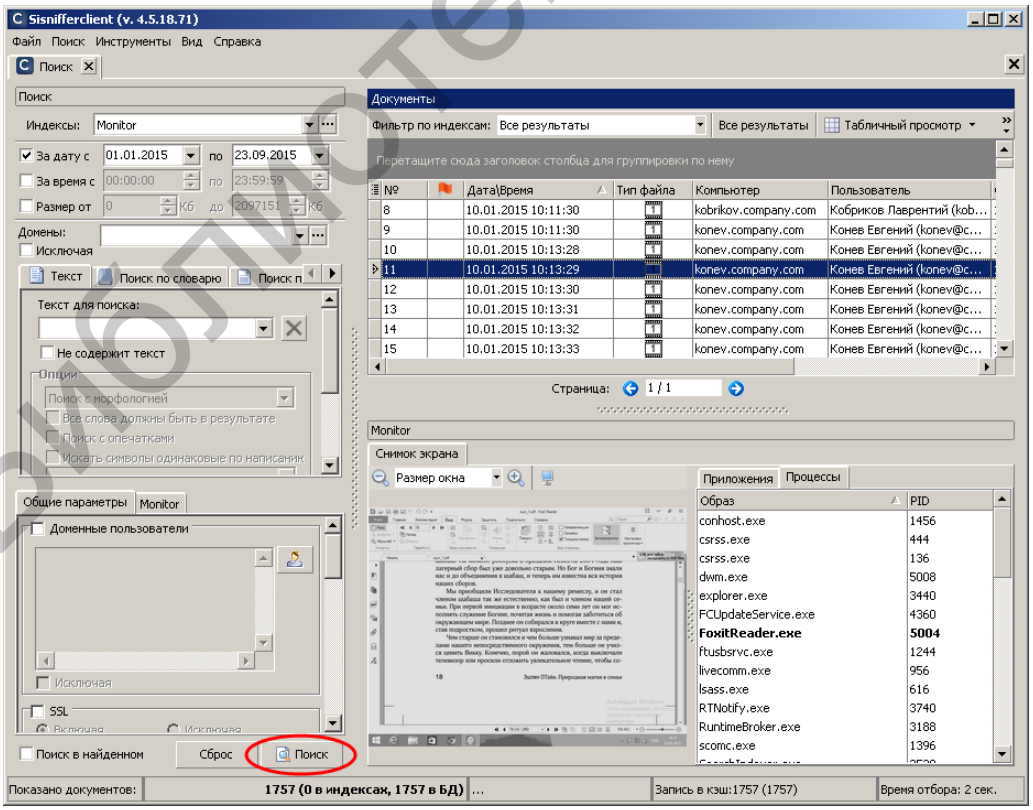


Рис. 3.16. Результат поиска снимков экрана

В соответствии с рис. 3.17–3.20 просмотреть снимок экрана и перечень процессов, запущенных в момент записи снимка.

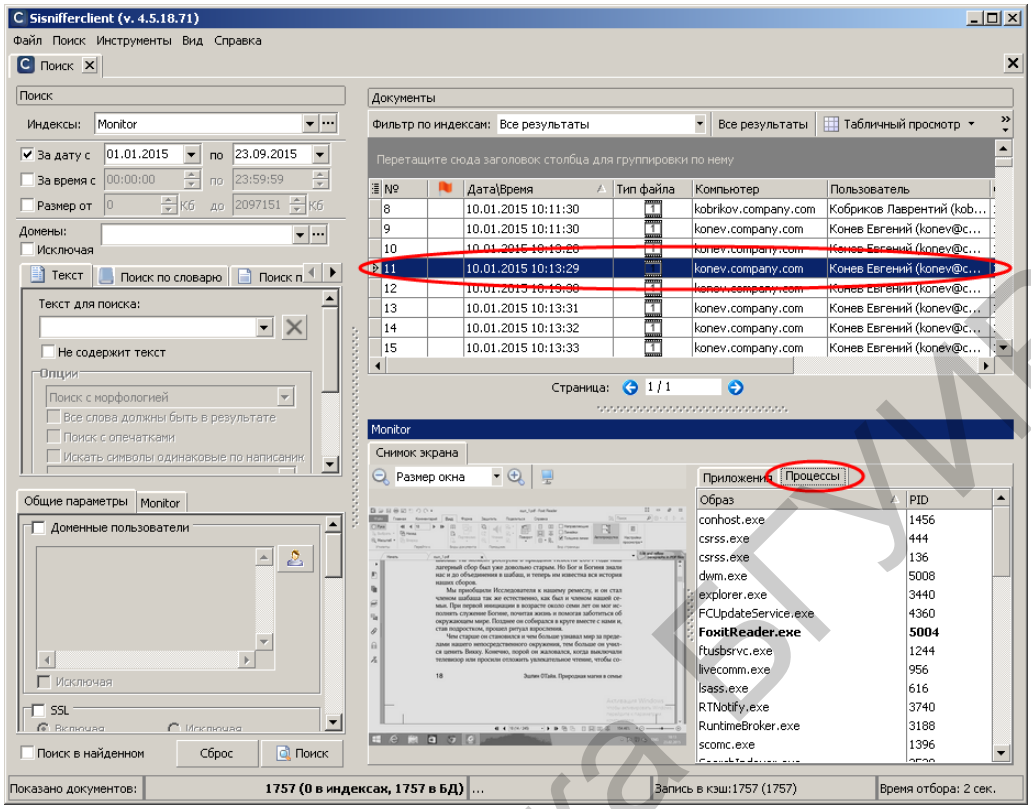


Рис. 3.17. Выбор снимка

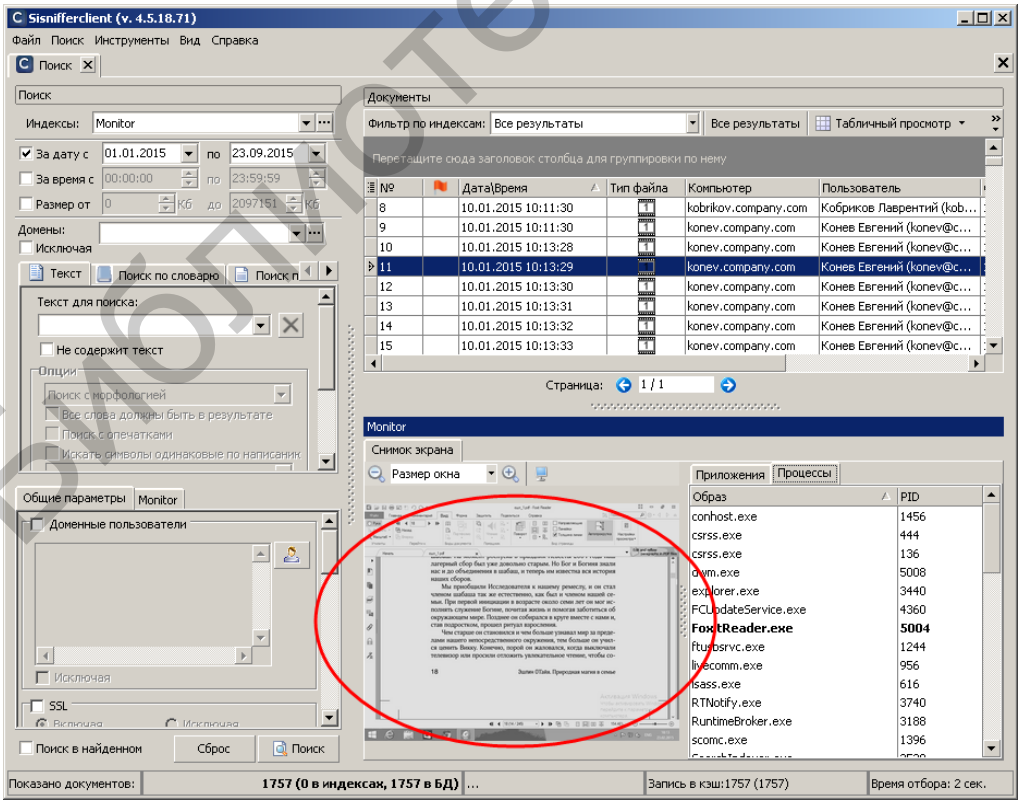


Рис. 3.18. Показ эскиза выбранного снимка

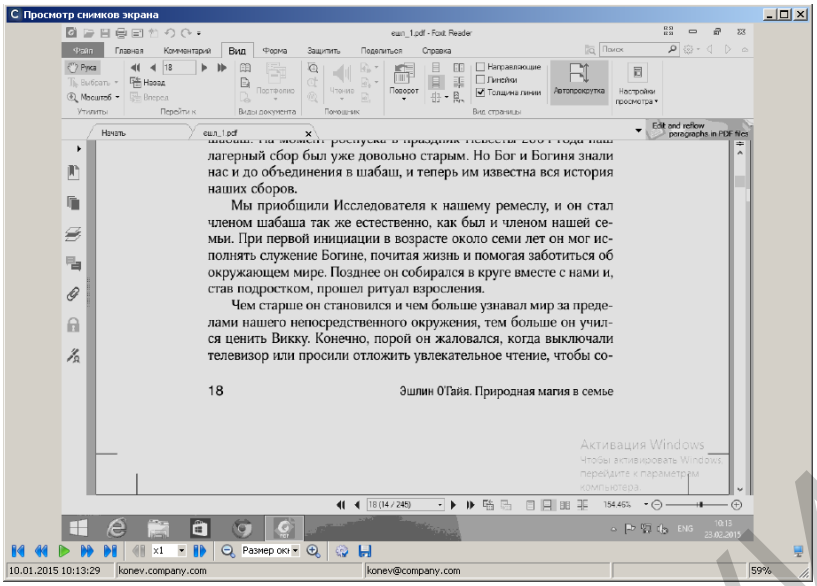


Рис. 3.19. Отображение выбранного снимка при двойном щелчке левой кнопкой мыши на эскизе

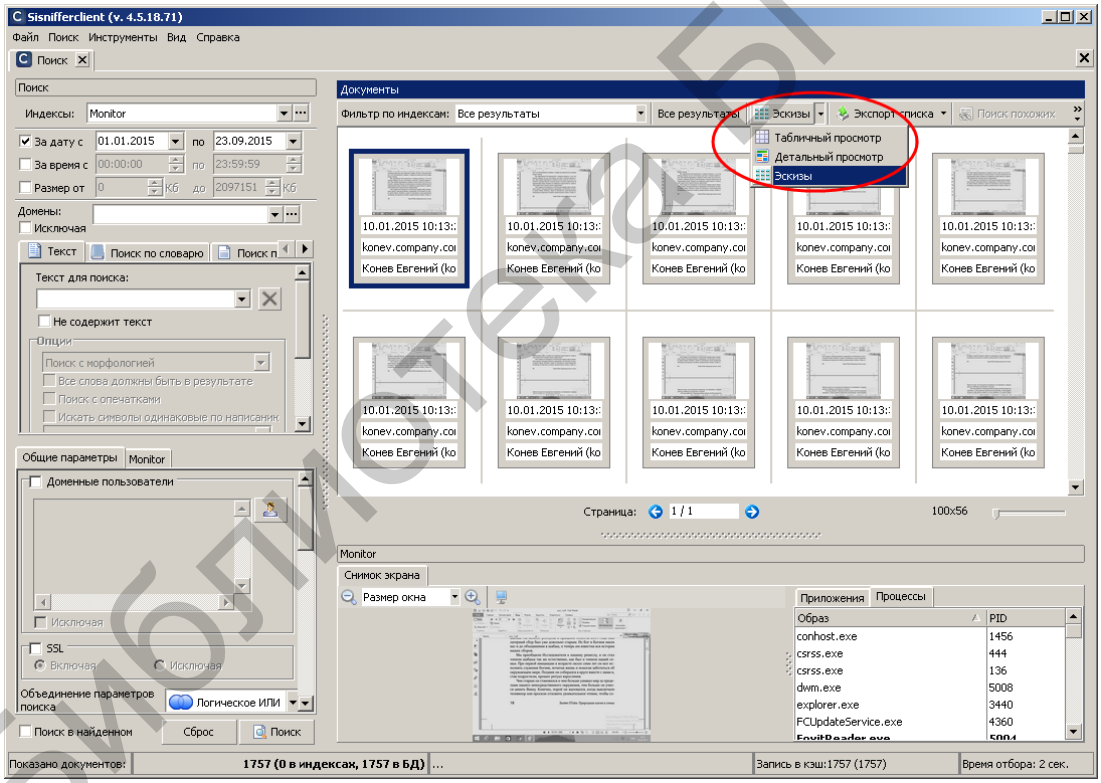


Рис. 3.20. Отображение снимков в виде эскизов

В соответствии с рис. 3.21–3.23 экспортировать снимок экрана в графический файл.

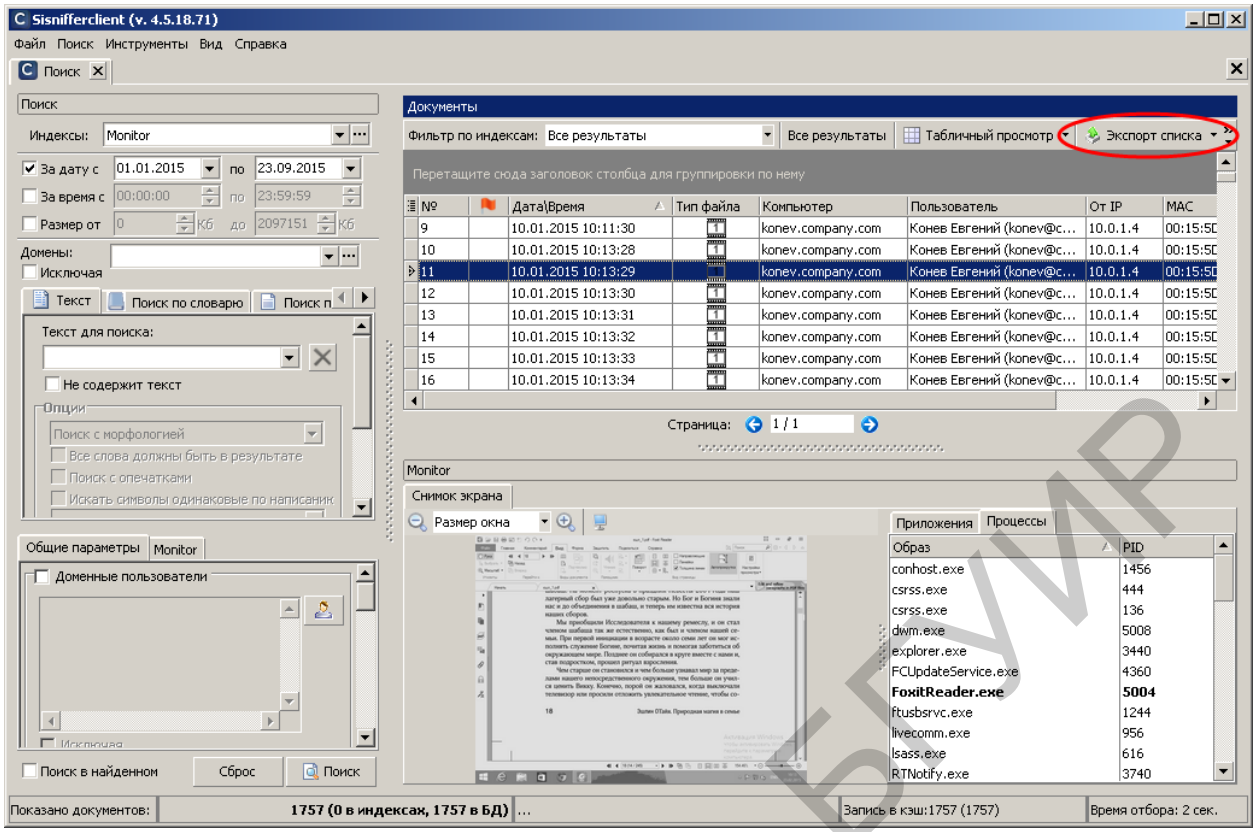


Рис. 3.21. Выбор опции «Экспорт списка»

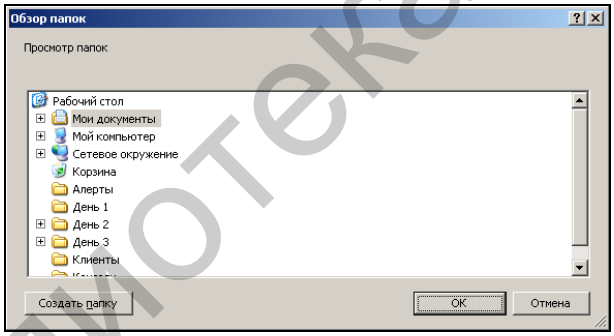


Рис. 3.22. Выбор места сохранения файла

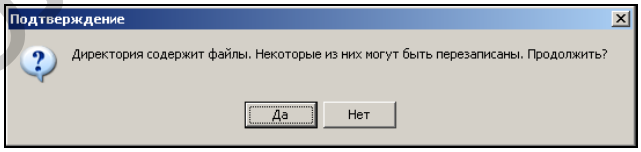


Рис. 3.23. Запрос подтверждения экспорта

В соответствии с рис. 3.24–3.26 просмотреть видеозапись содержимого экрана.

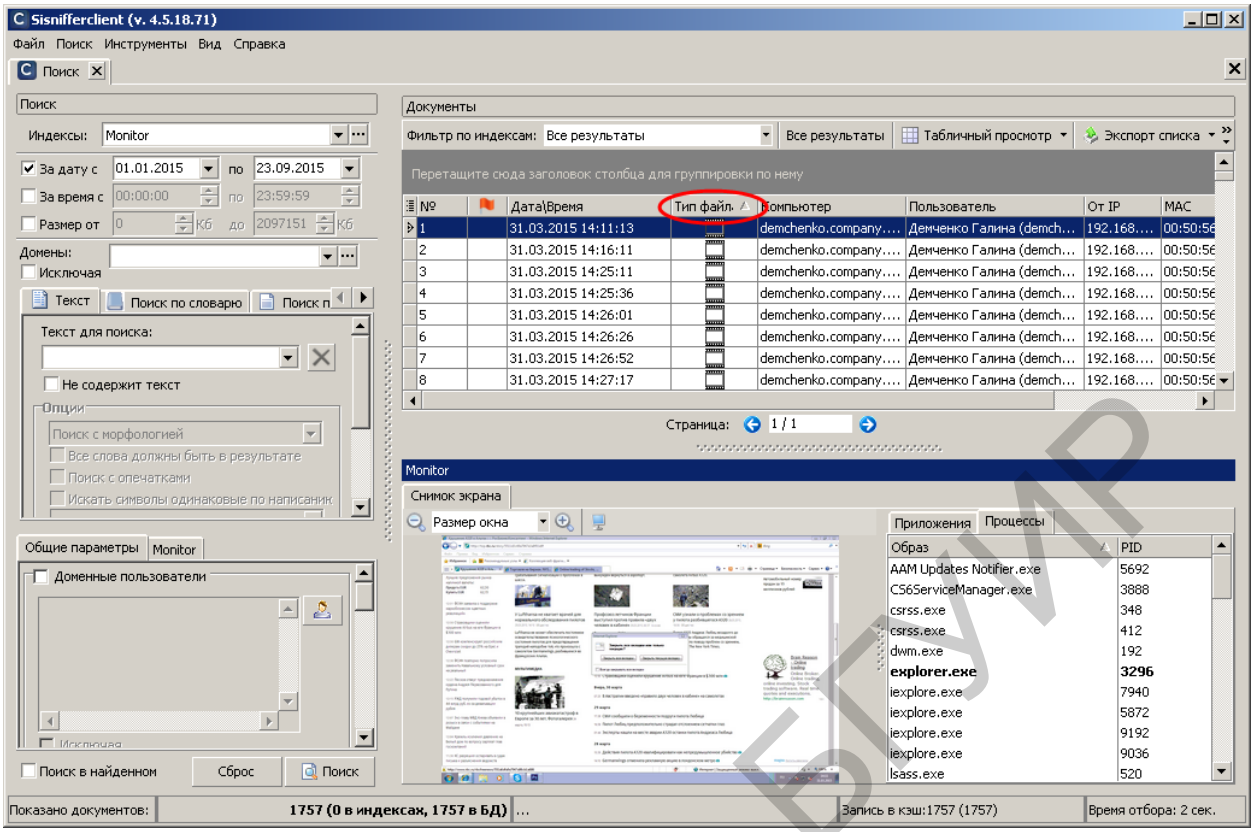


Рис. 3.24. Сортировка записей по типу файла

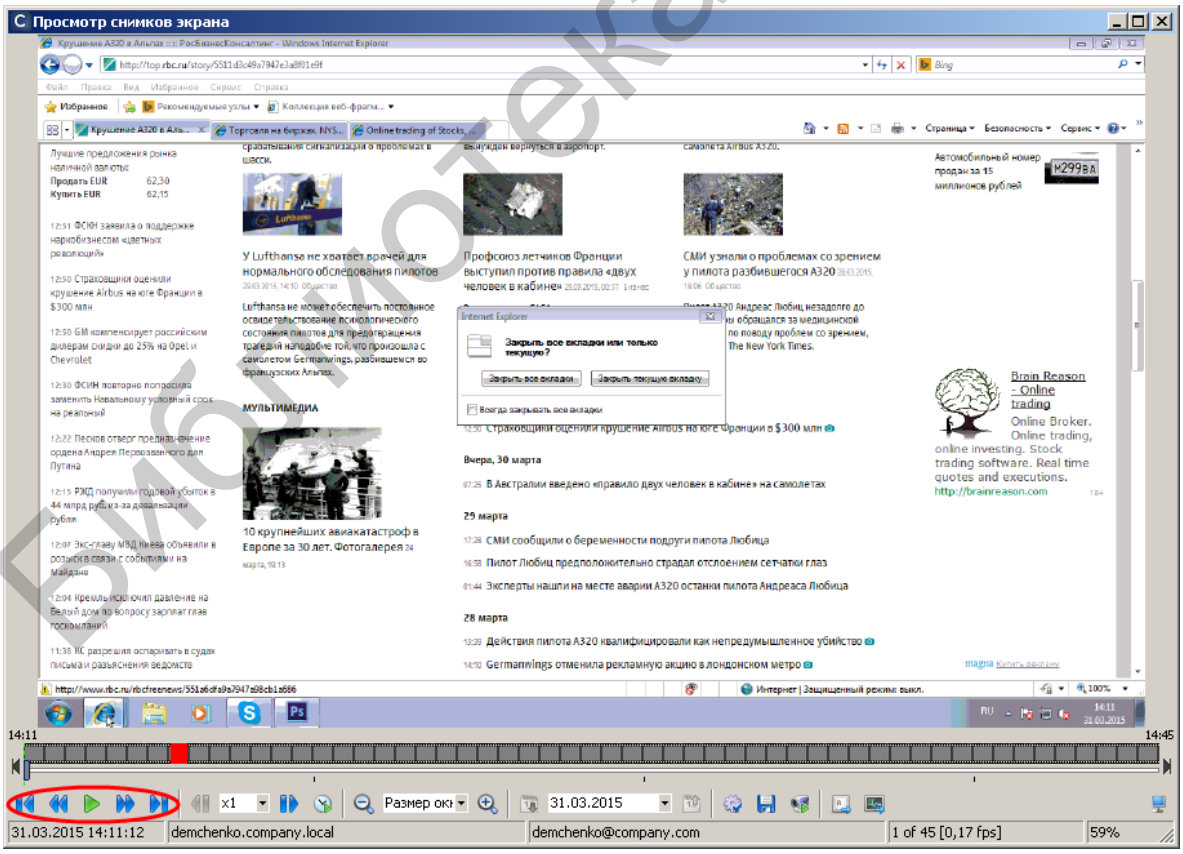


Рис. 3.25. Отображение выбранной видеозаписи при двойном щелчке левой кнопкой мыши на эскизе

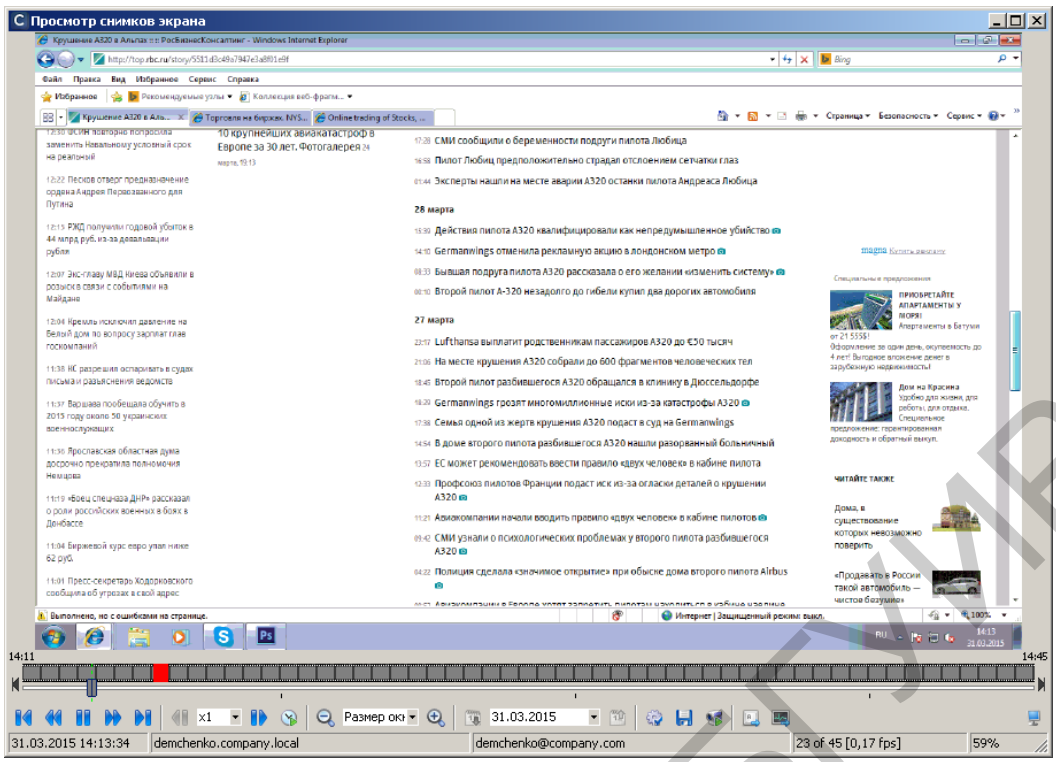


Рис. 3.26. Просмотр видеозаписи

В соответствии с рис. 3.27–3.30 произвести поиск снимков экрана по имени компьютера. Заметим, что в соответствии с рис. 3.28 в окне выбора имени компьютера также отображаются соответствующие IP- и MAC-адреса. Зафиксировать время выполнения поиска.

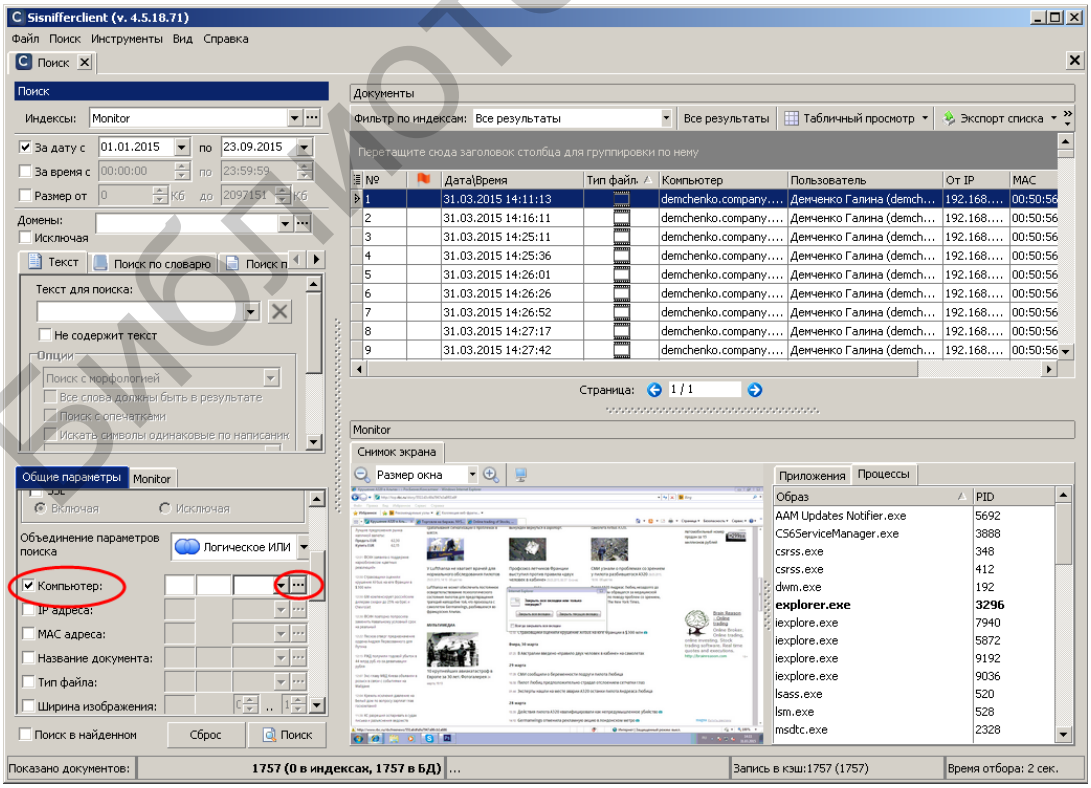


Рис. 3.27. Вход в режим выбора имени компьютера

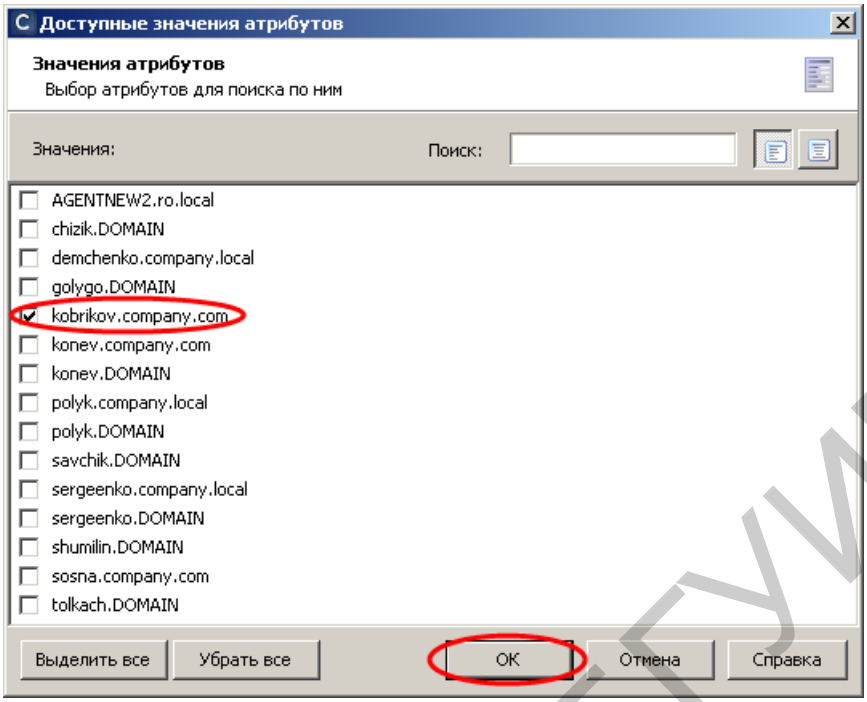


Рис. 3.28. Выбор имени компьютера

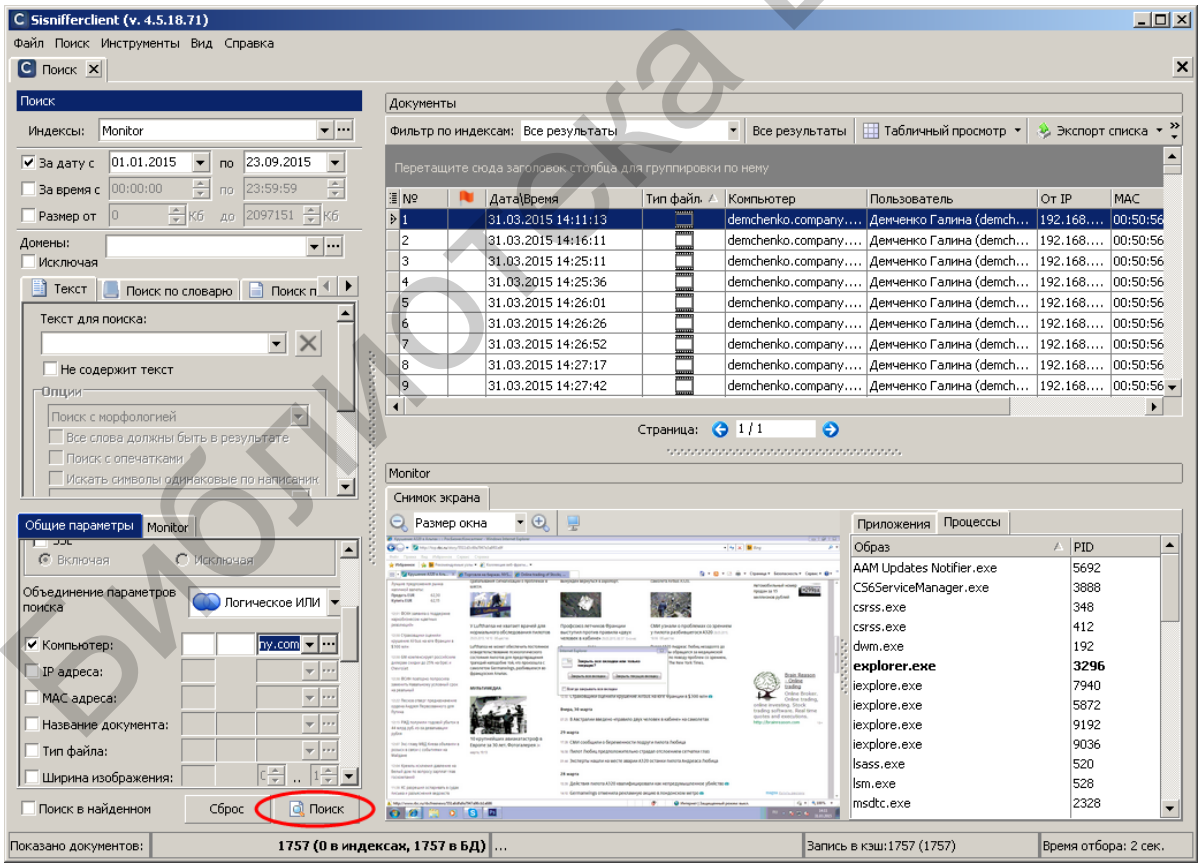


Рис. 3.29. Поиск снимков по имени компьютера

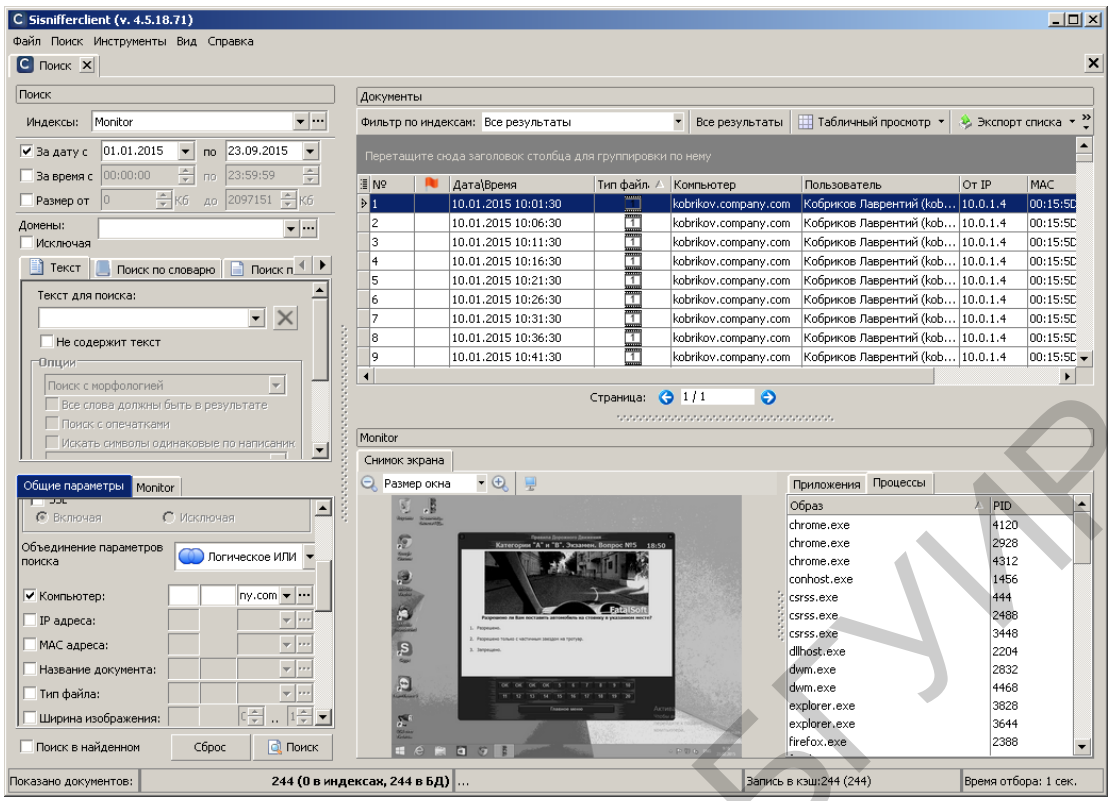


Рис. 3.30. Отображение результатов поиска снимков по имени компьютера

В соответствии с рис. 3.31 и 3.32 сбросить параметры поиска. Заметим, что после очистки маски поиска в окне результатов продолжают оставаться старые данные. Для обновления данного окна следует нажать кнопку «Поиск».

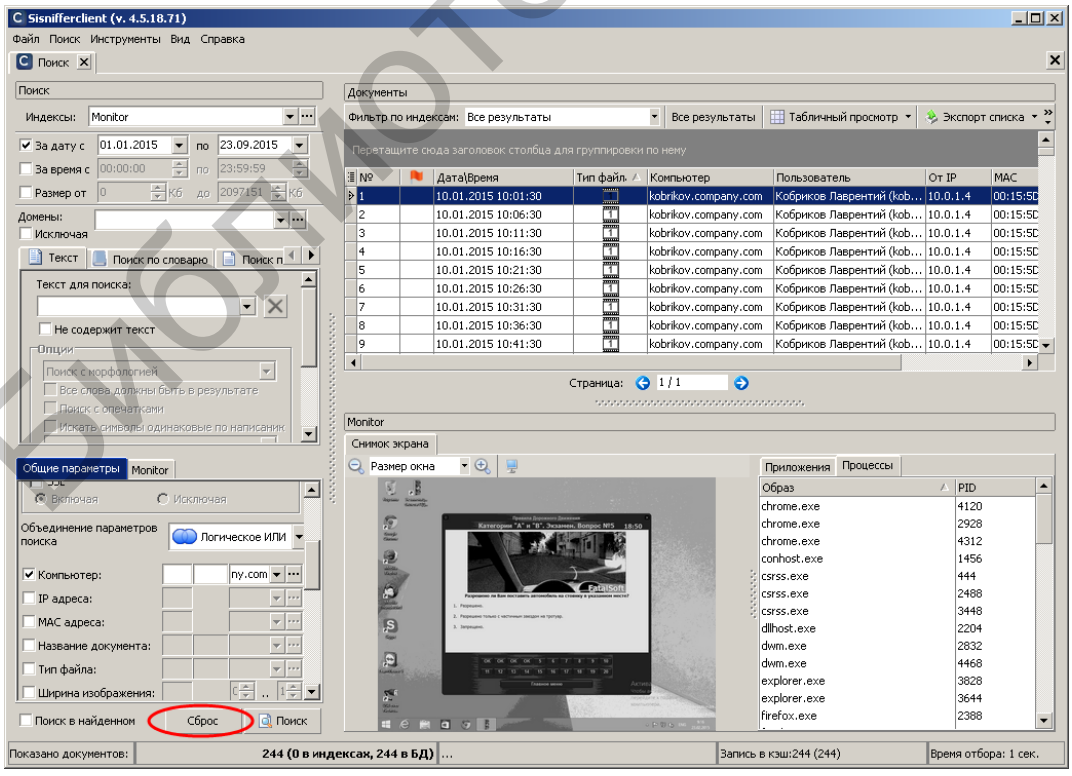


Рис. 3.31. Выбор опции очистки маски поиска

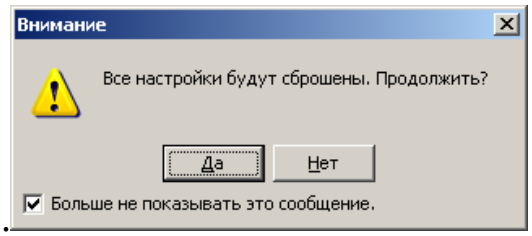


Рис. 3.32. Подтверждение очистки

Найти перечень запущенных процессов в момент времени, который соответствует снимку экрана, показанному на рис. 3.33. Экспортировать данный снимок в графический файл. Также определить MAC- и IP-адреса соответствующего компьютера.

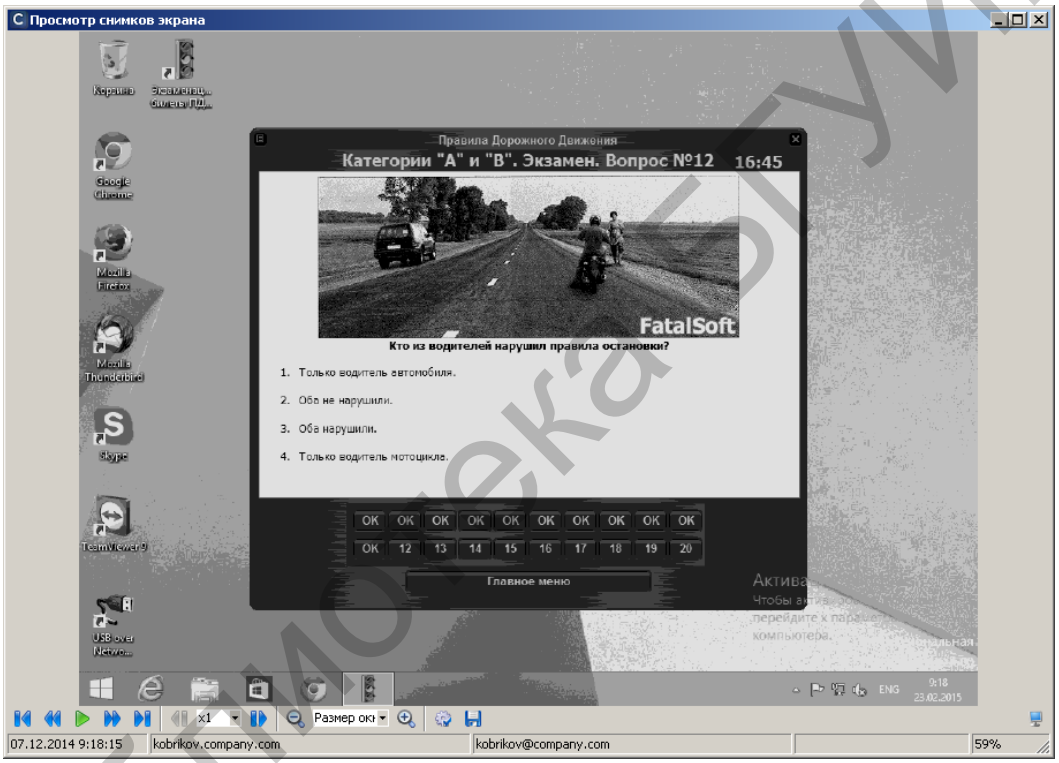


Рис. 3.33. Задание для поиска

Отметим, что методика поиска снимка экрана по MAC- и IP-адресам отличается от поиска по имени компьютера только использованием вкладок MAC и IP. Закрыть окно SearchInform Client.

3. Для поиска конфиденциальной информации без проведения синтаксического анализа открыть окно AlertCenter Client.

В соответствии с методическими указаниями лабораторной работы №2 создать новую политику безопасности с названием «Тест2». Включить в политику все доступные поисковые индексы сервера. Добавить и включить расписание, предусматривающее ежедневные, повторяющиеся каждую минуту проверки. Проверки должны начинаться с началом текущего занятия. Получать уведомления должен пользователь DefaultAdmin. Окно политики показано на рис. 3.34.

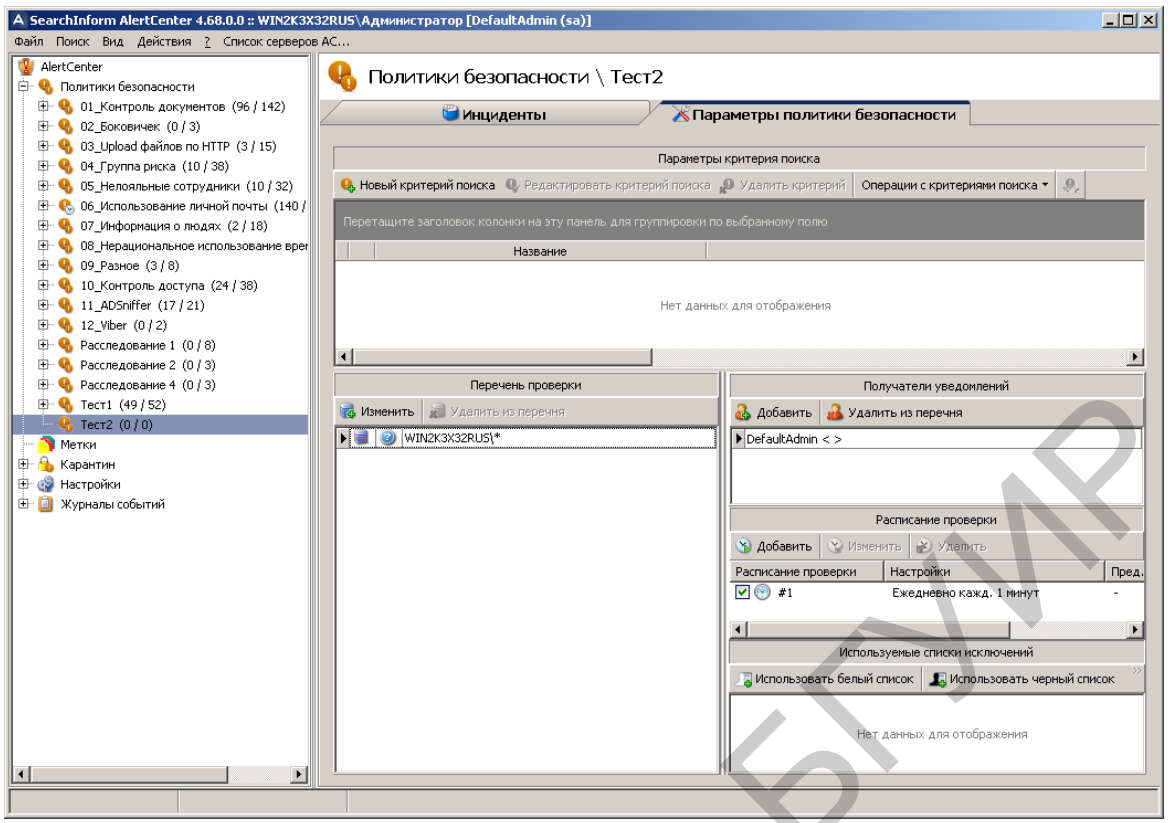


Рис. 3.34. Окно политики безопасности «Тест2»

Через несколько минут после создания политики «Тест2» в перечне инцидентов убедиться, что список соответствующих инцидентов пуст (рис. 3.35).

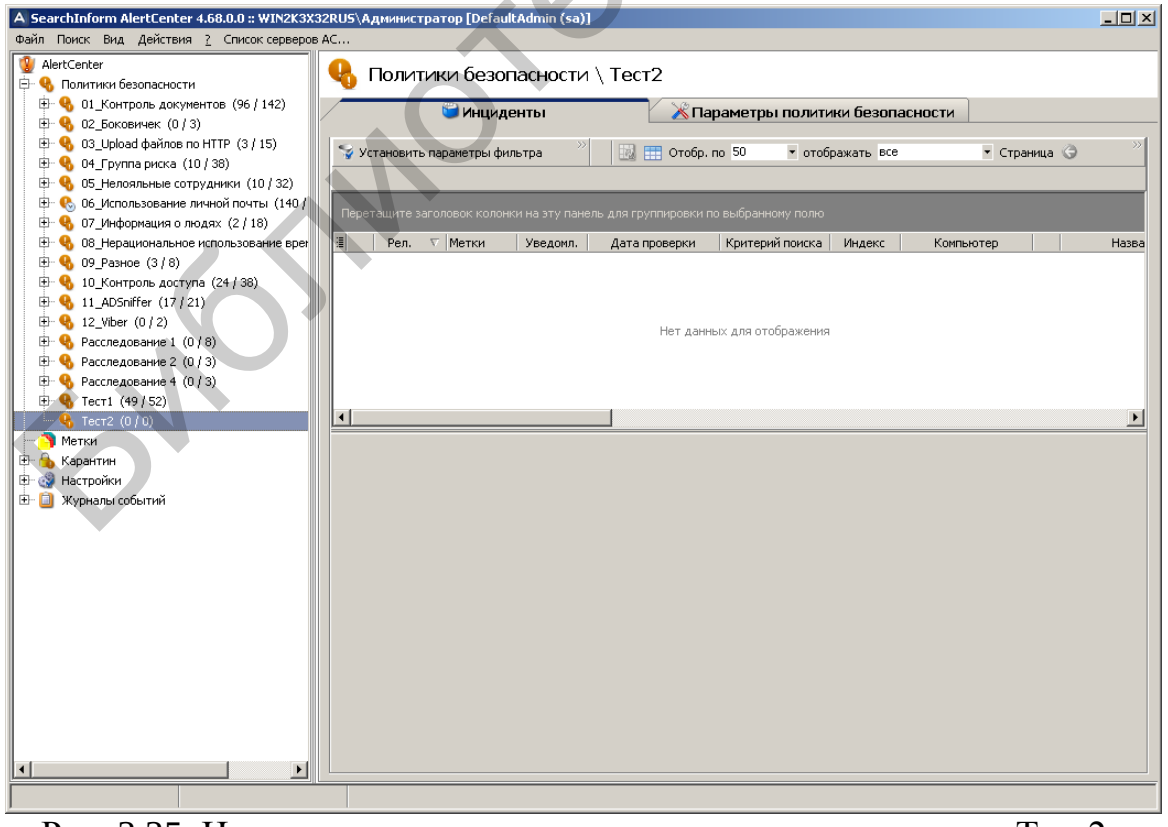


Рис. 3.35. Индикация пустого списка инцидентов политики «Тест2»

В соответствии с рис. 3.36 создать критерий «АтрибутДатаПерехвата», предусматривающий поиск документов, дата модификации которых не больше года и одного дня.

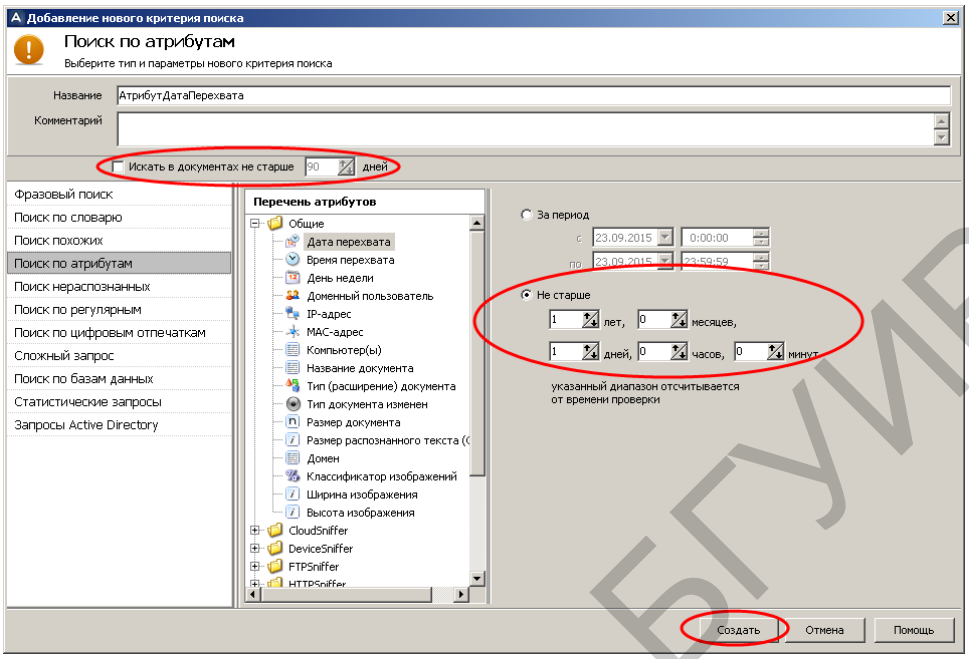


Рис. 3.36. Создание критерия «АтрибутДатаПерехвата»

Через несколько минут после создания критерия убедиться, что в списке инцидентов появились соответствующие уведомления. При этом сигнализируется о том, что число инцидентов превышает максимально допустимое (рис. 3.37).

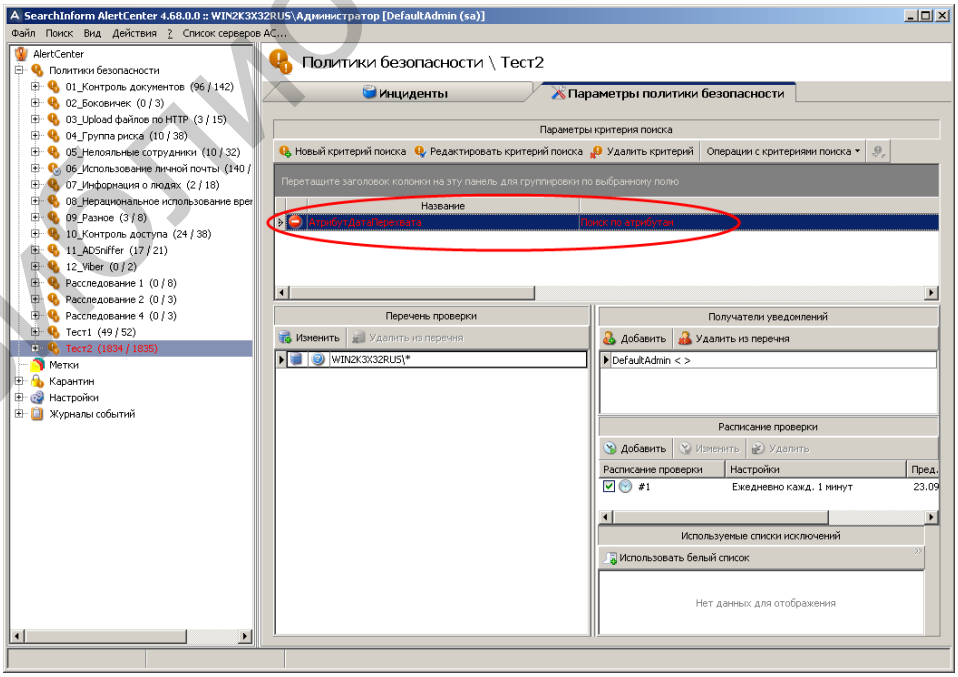


Рис. 3.37. Индикация превышения инцидентов по критерию «АтрибутДатаПерехвата»

В дальнейшем для повышения оперативности проверки созданных критериев следует отключить выполнение расписания. Запуск критериев будет осуществляться в ручном режиме.

В соответствии с рис. 3.38 создать критерий для поиска текстовой информации в графических файлах. При этом в графическом файле должно быть распознано не менее 10 символов текста.

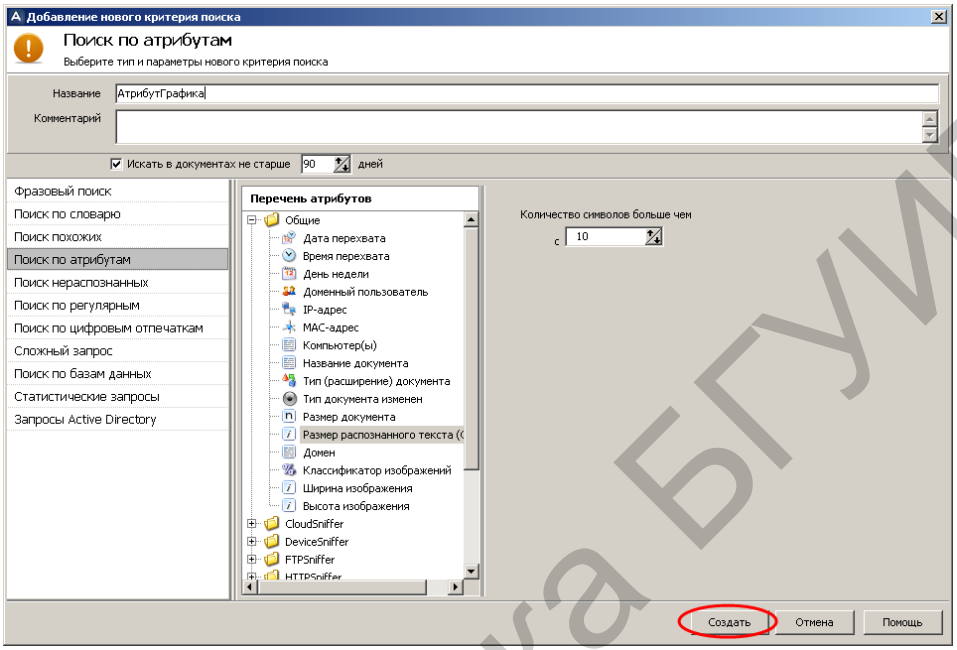


Рис. 3.38. Первый этап создания критерия «АтрибутГрафика»

В соответствии с рис. 3.39 запустить критерий «АтрибутГрафика» на выполнение.

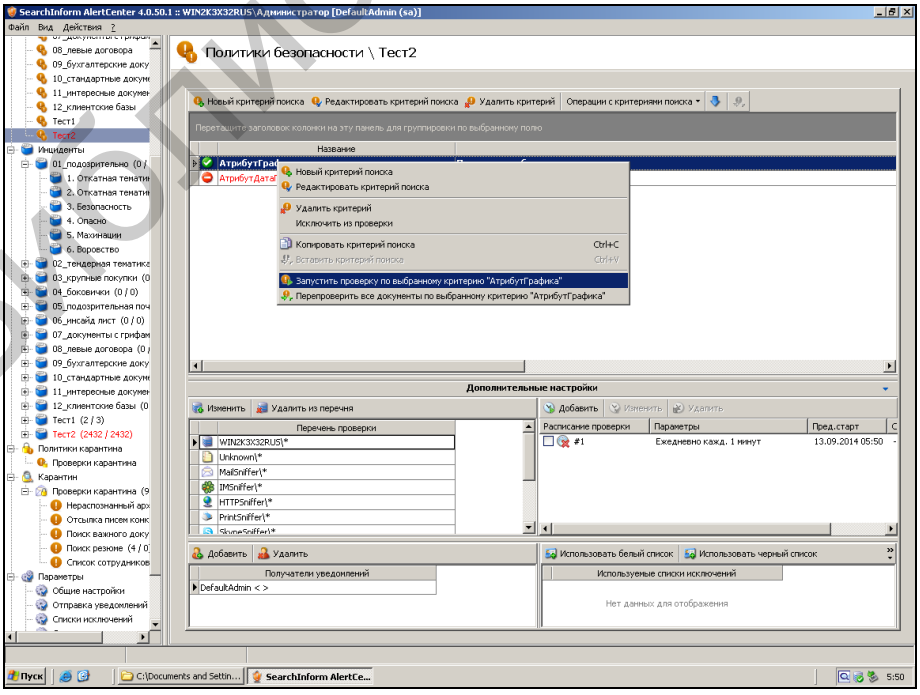


Рис. 3.39. Запуск критерия «АтрибутГрафика»

После выполнения критерия убедиться, что в списке инцидентов появились соответствующие уведомления (рис. 3.40).

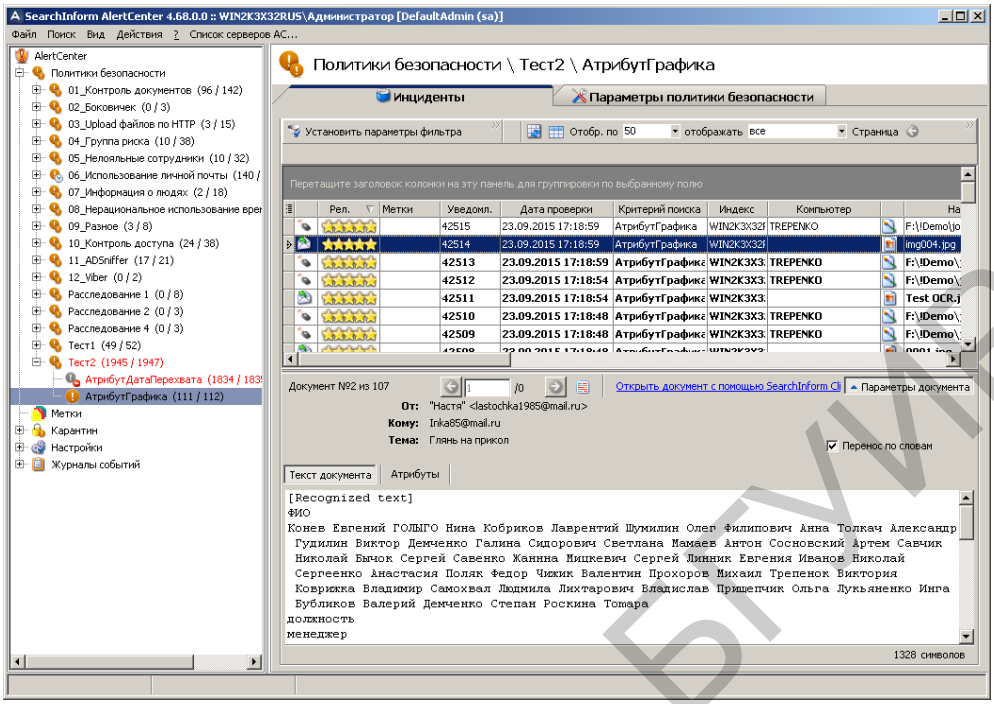


Рис. 3.40. Индикация инцидентов по критерию «АтрибутГрафика»

В соответствии с рис. 3.41 создать критерий для поиска исходящих шифрованных электронных писем. Отметим, что опция «Шифрованное сообщение» находится в разделе «MailSniffer».

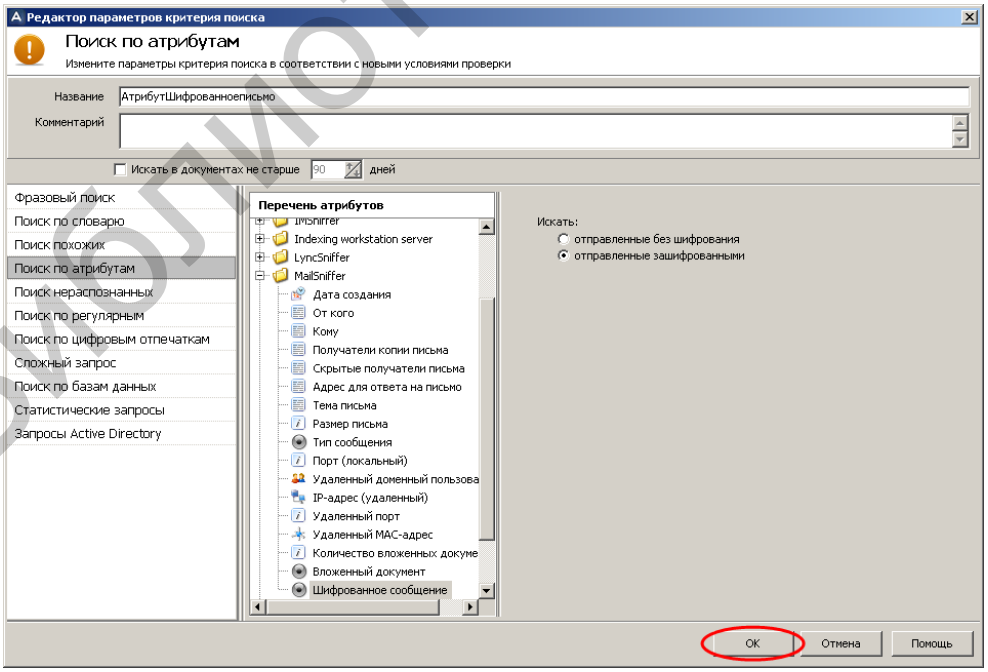


Рис. 3.41. Создание критерия «АтрибутШифрованноеписьмо»

В соответствии с рис. 3.42 запустить принудительное выполнение критерия поиска «АтрибутШифрованноеписьмо». Зафиксировать время выполнения поиска. Убедиться в результативности поиска (рис. 3.43).

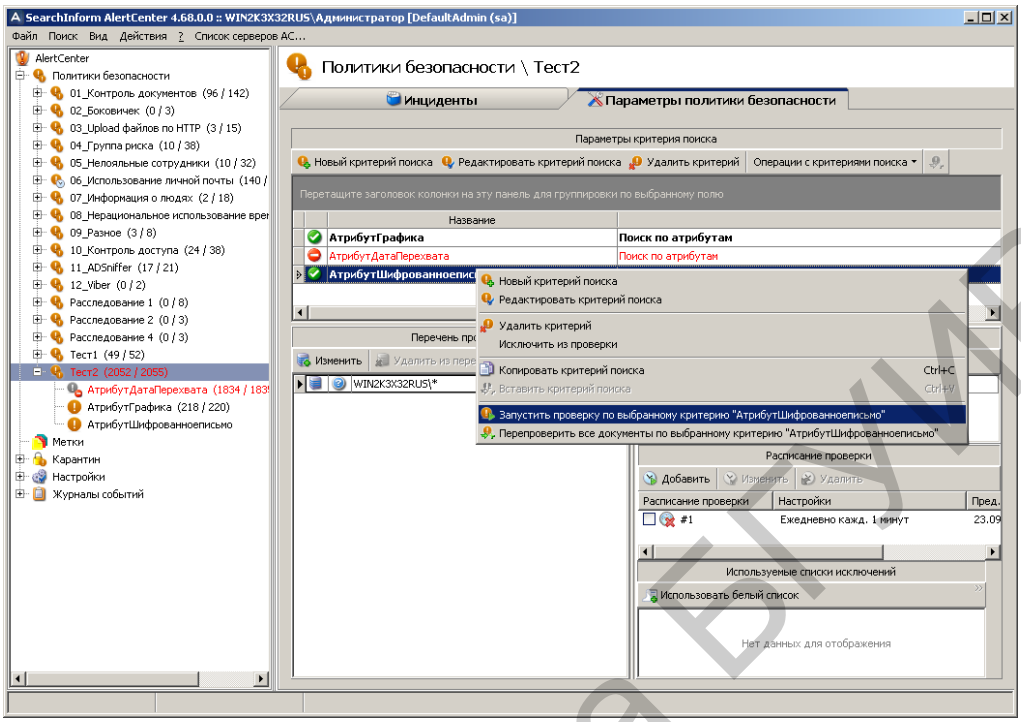


Рис. 3.42. Принудительный запуск проверки критерия «АтрибутШифрованноеписьмо»

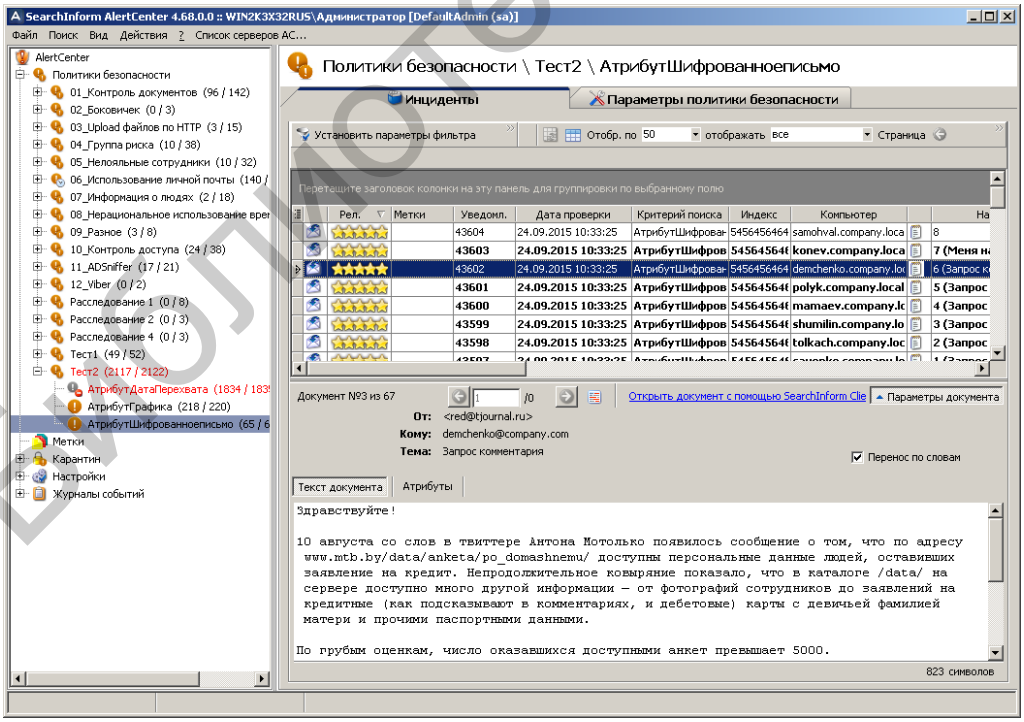


Рис. 3.43. Индикация инцидентов по критерию «АтрибутШифрованноеписьмо»

В соответствии с рис. 3.44 и 3.45 создать критерий для поиска файлов, переданных не позже чем 3 года и 1 месяц назад по протоколу HTTP методом Post. Создаваемый критерий будет содержать в себе дополнительный уточняющий критерий.

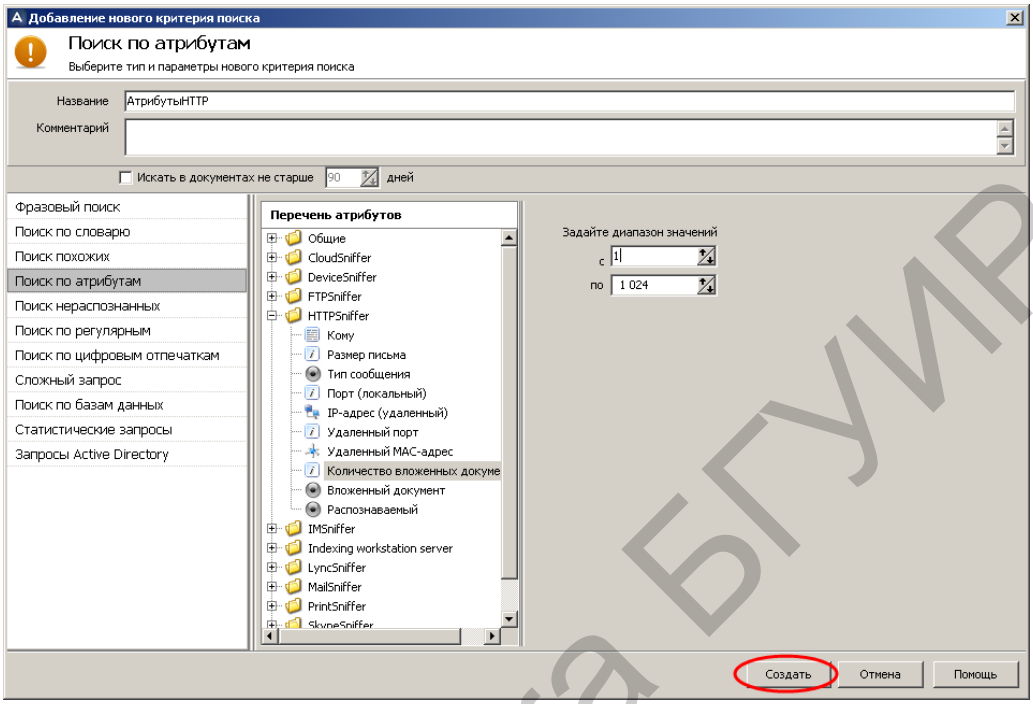


Рис. 3.44. Создание критерия «АтрибутHTTP»

Запустить принудительное выполнение критерия поиска «АтрибутHTTP» и убедиться в его результативности. Зафиксировать время выполнения поиска.

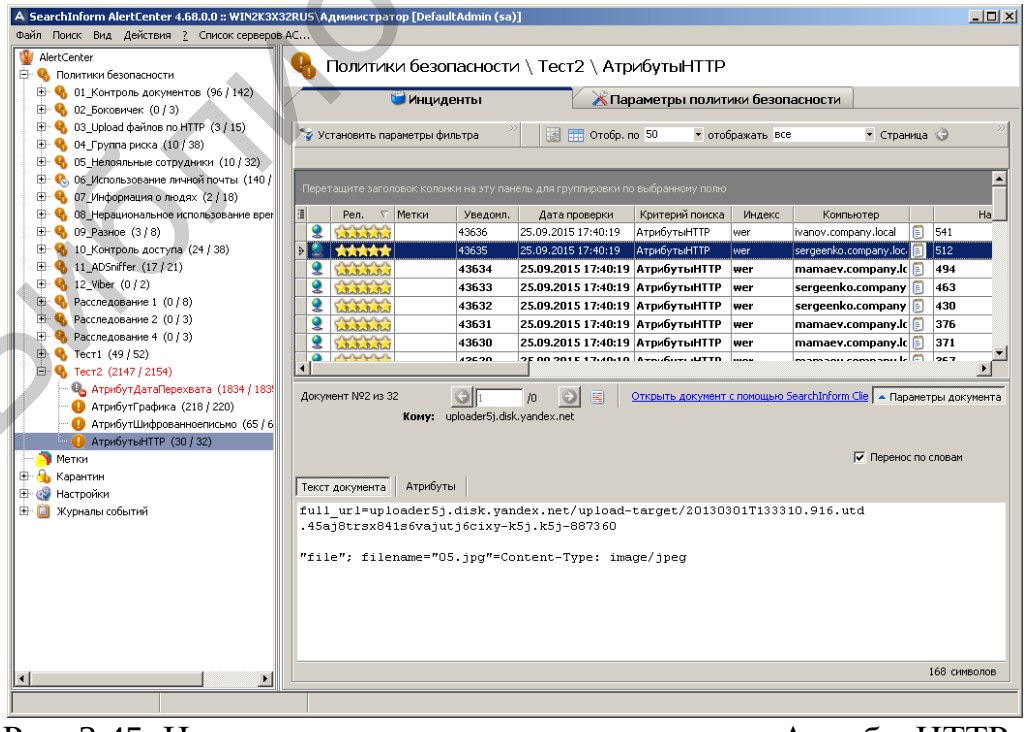


Рис. 3.45. Индикация инцидентов по критерию «АтрибутHTTP»

В соответствии с рис. 3.46 и 3.47 создать критерий для поиска файлов, имеющих размер от 1 МБ до 2 ГБ.

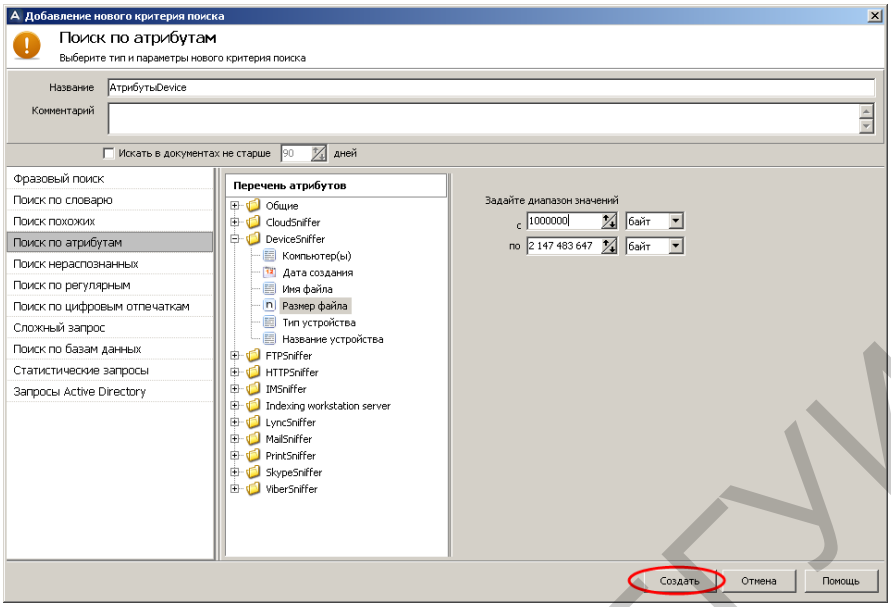


Рис. 3.46. Создание критерия «АтрибутDevice»

Запустить принудительное выполнение критерия поиска «АтрибутDevice» и убедиться в его результативности. Зафиксировать время выполнения поиска.

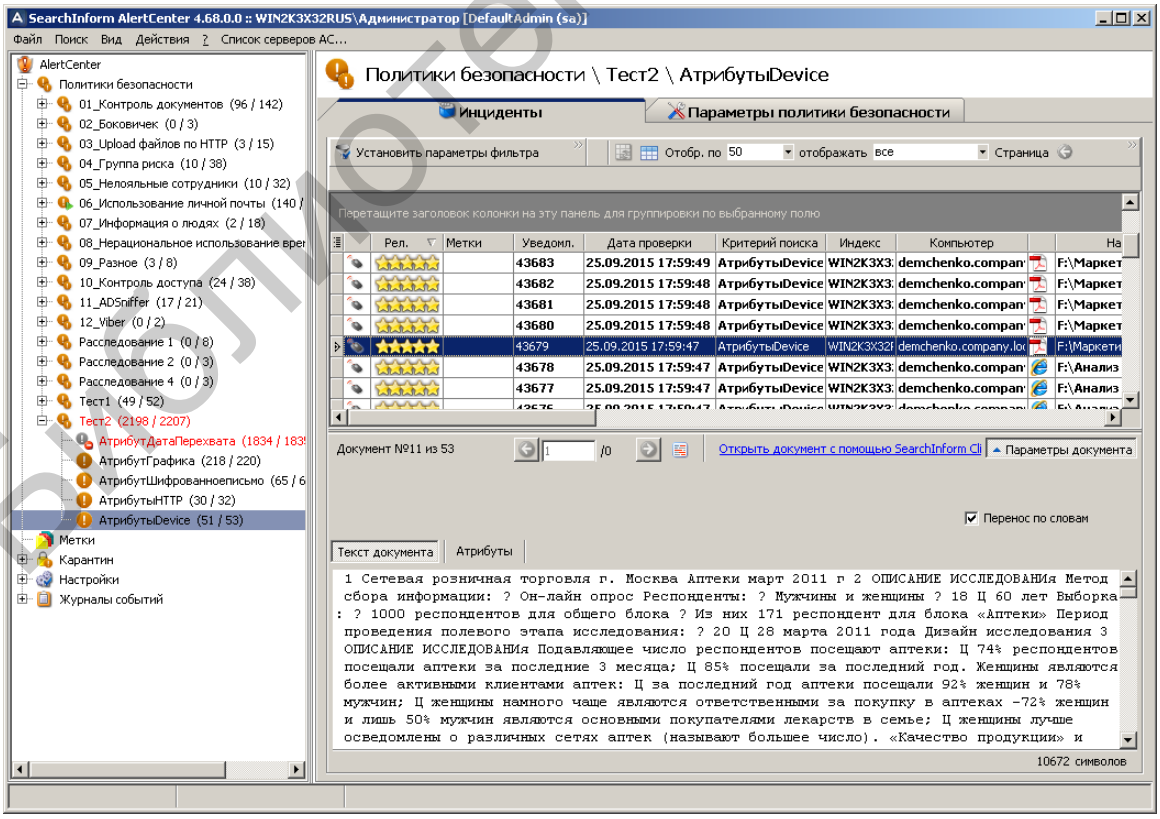


Рис. 3.47. Третий этап создания критерия «АтрибутDevice»

В соответствии с рис. 3.48 создать критерий для поиска файлов, переданных на принтер, при количестве копий меньше 3.

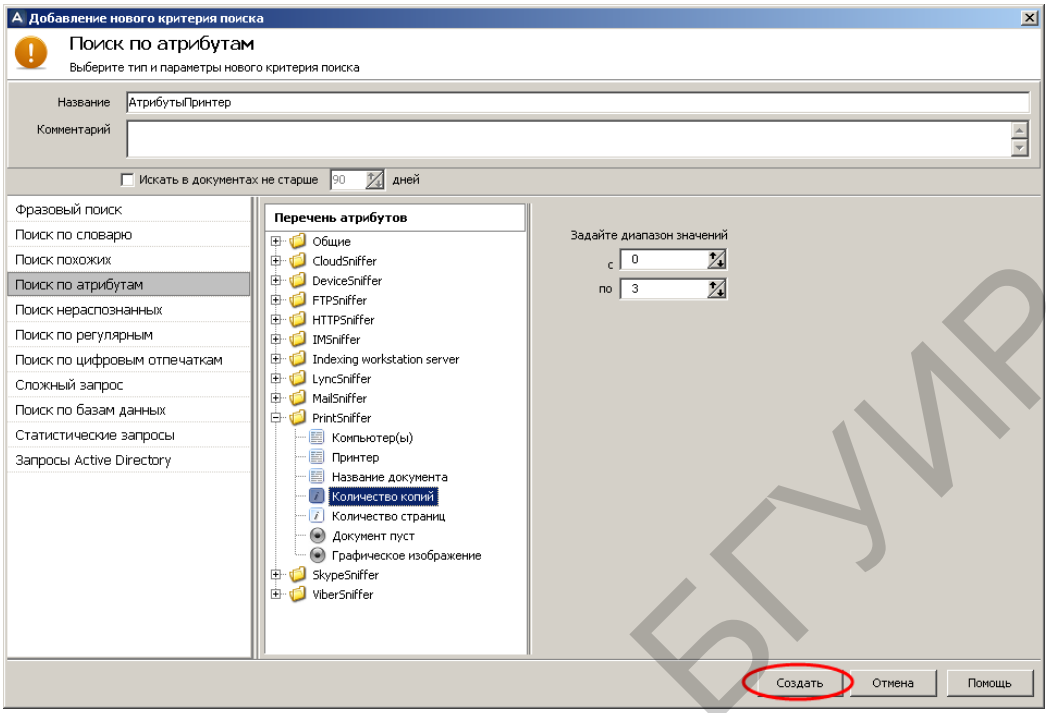


Рис. 3.48. Создание критерия «АтрибутПринтер»

Запустить принудительное выполнение критерия поиска «АтрибутПринтер» и убедиться в его результативности (рис. 3.49). Зафиксировать время выполнения поиска.

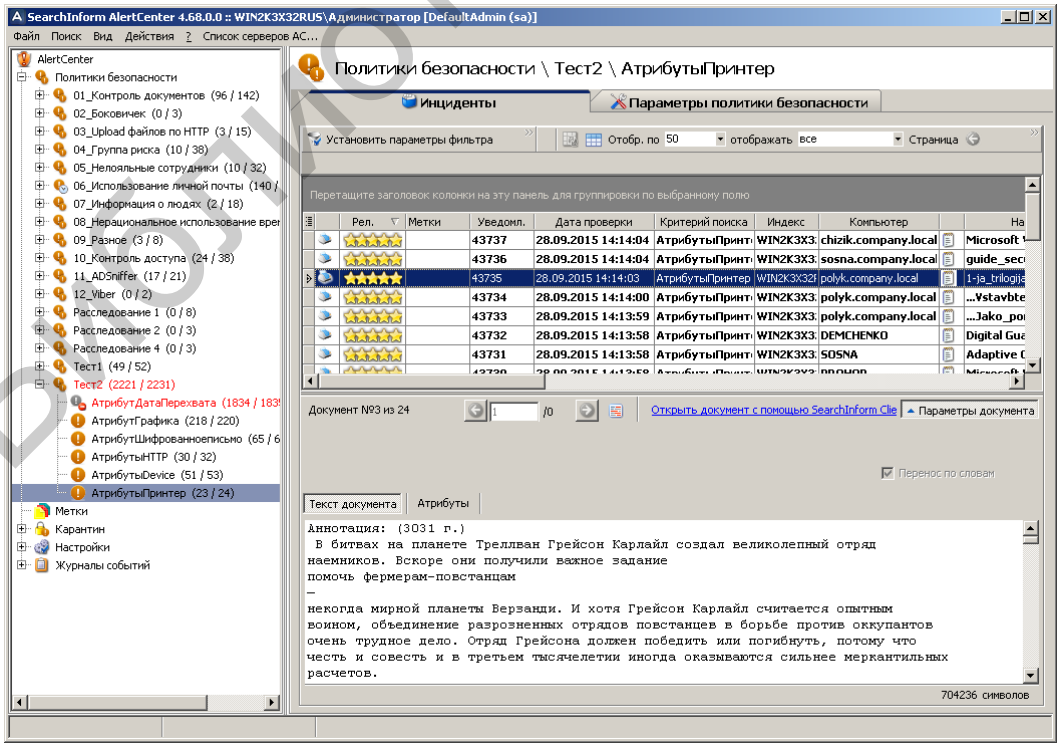


Рис. 3.49. Индикация инцидентов по критерию «АтрибутПринтер»

В соответствии с рис. 3.50 создать критерий для поиска документов, защищенных паролем.

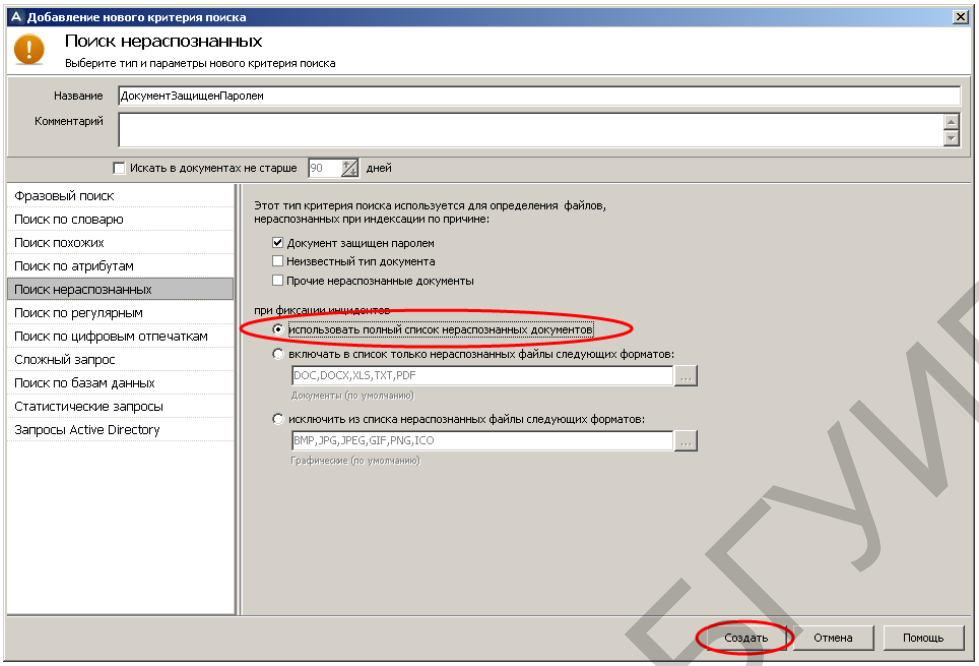


Рис. 3.50. Создание критерия «ВсеНераспознанныеДокументы»

Запустить принудительное выполнение критерия поиска «ДокументЗащищенПаролем» и убедиться в его результативности (рис. 3.51). Зафиксировать время выполнения поиска.

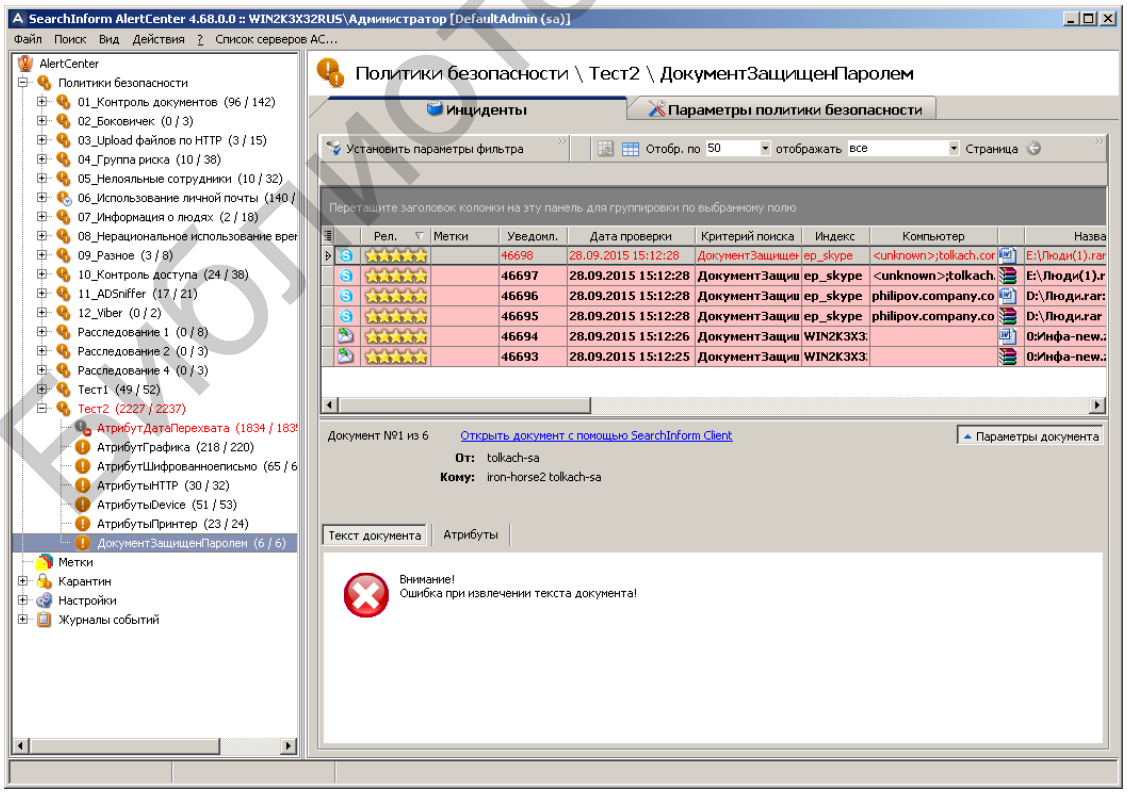


Рис. 3.51. Индикация инцидентов по критерию «ДокументЗащищенПаролем»

В соответствии с рис. 3.52 создать критерий для поиска нераспознанных doc-файлов.

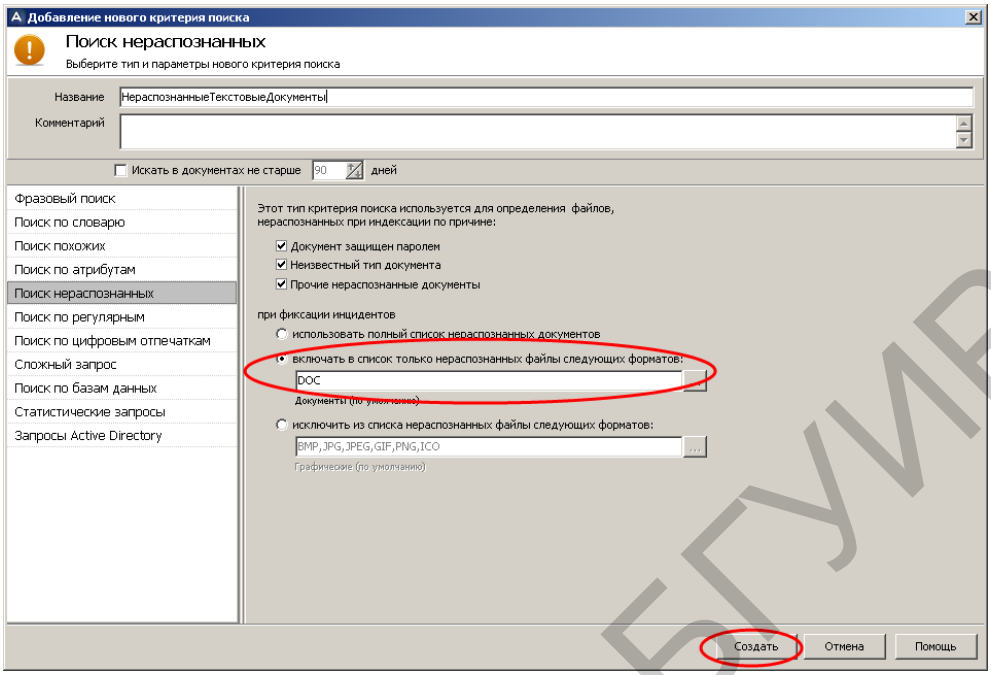


Рис. 3.52. Создание критерия «НераспознанныеТекстовыеДокументы»

Запустить принудительное выполнение критерия поиска «НераспознанныеТекстовыеДокументы» и убедиться в его результативности (рис. 3.53). Зафиксировать время выполнения поиска.

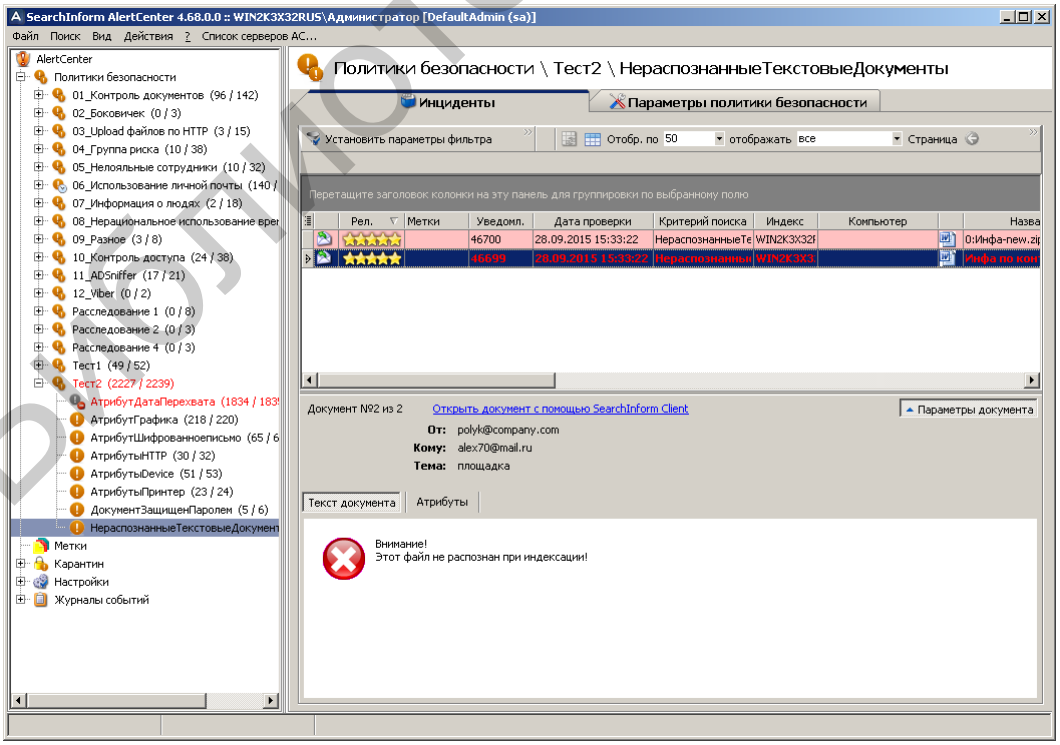


Рис. 3.53. Индикация инцидентов по критерию «НераспознанныеТекстовыеДокументы»

В соответствии с рис. 3.54 создать критерий для поиска нераспознанных файлов, исключив при этом файлы в форматах bmp, pdf и doc.

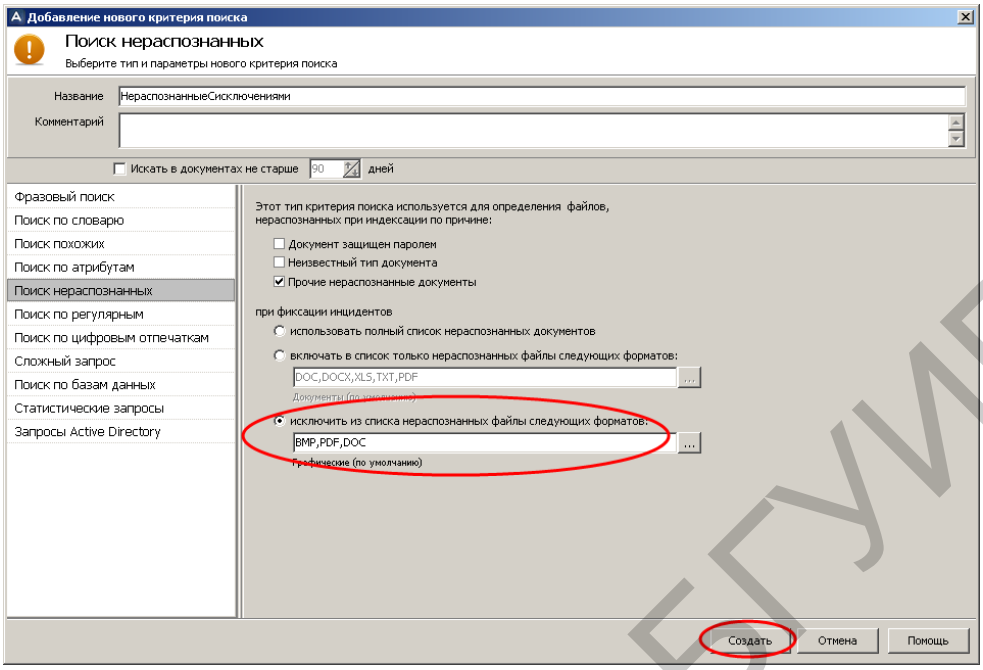


Рис. 3.54. Создание критерия «НераспознанныеСисключениями»

Запустить принудительное выполнение критерия поиска «НераспознанныеСисключениями» и убедиться в его результативности (рис. 3.55). Зафиксировать время выполнения поиска.

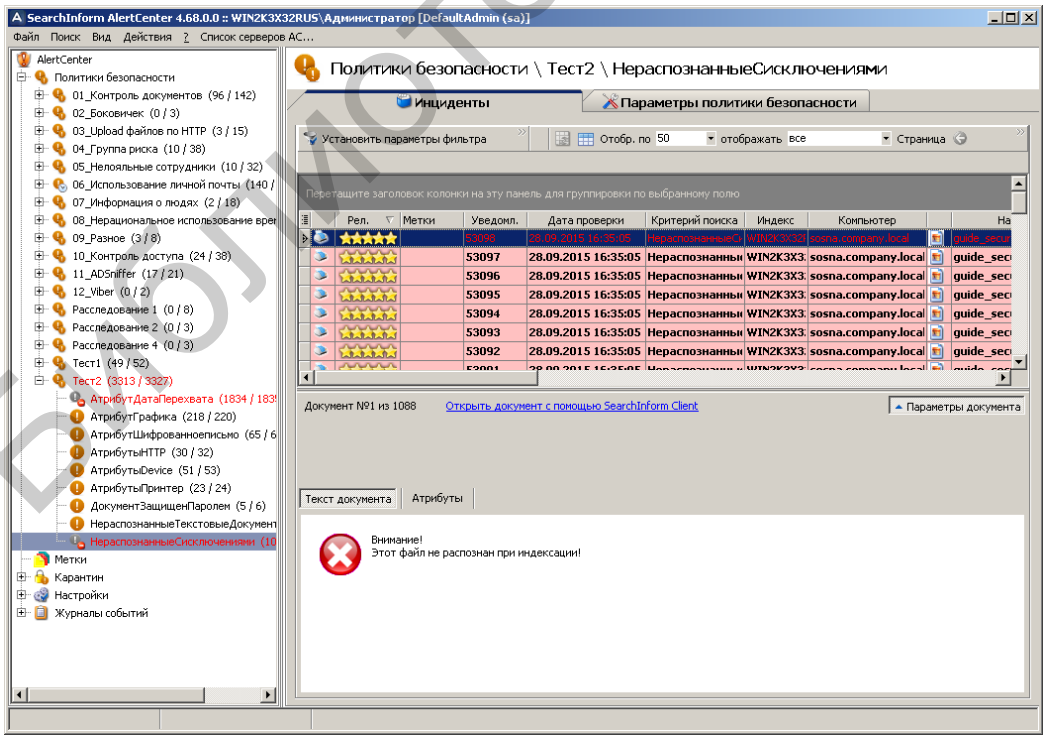


Рис. 3.55. Индикация инцидентов по критерию «НераспознанныеСисключениями»

В соответствии с рис. 3.56 и 3.57 отфильтровать инциденты по критерию «НераспознанныеСисключениями», оставив файлы, переданные на съемные носители.

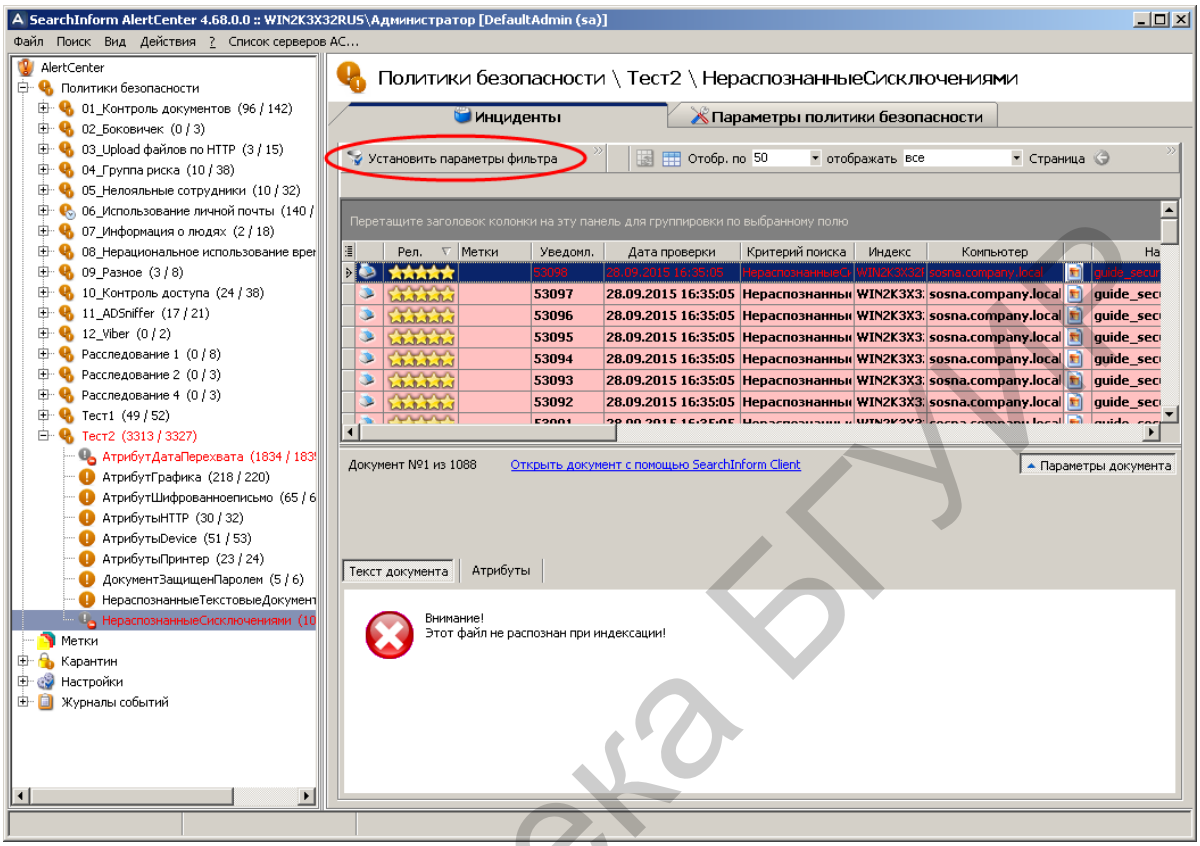


Рис. 3.56. Первый этап создания фильтра

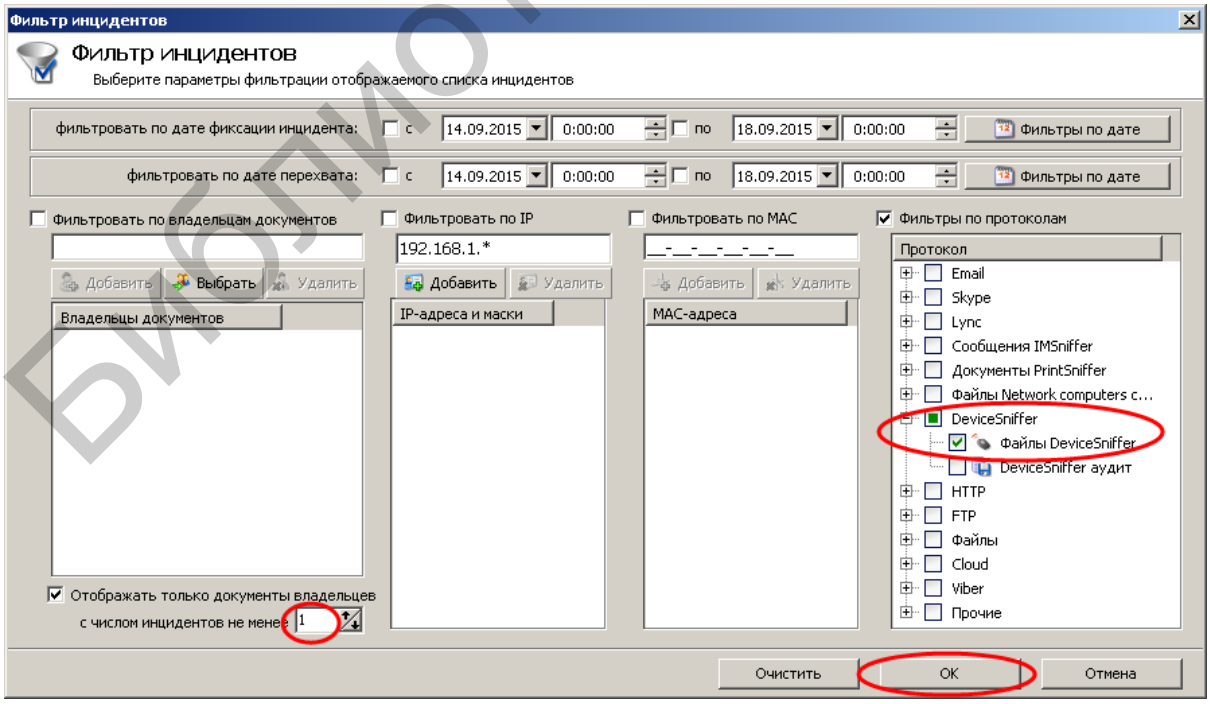


Рис. 3.57. Второй этап создания фильтра

Результат применения фильтра показан на рис. 3.58.

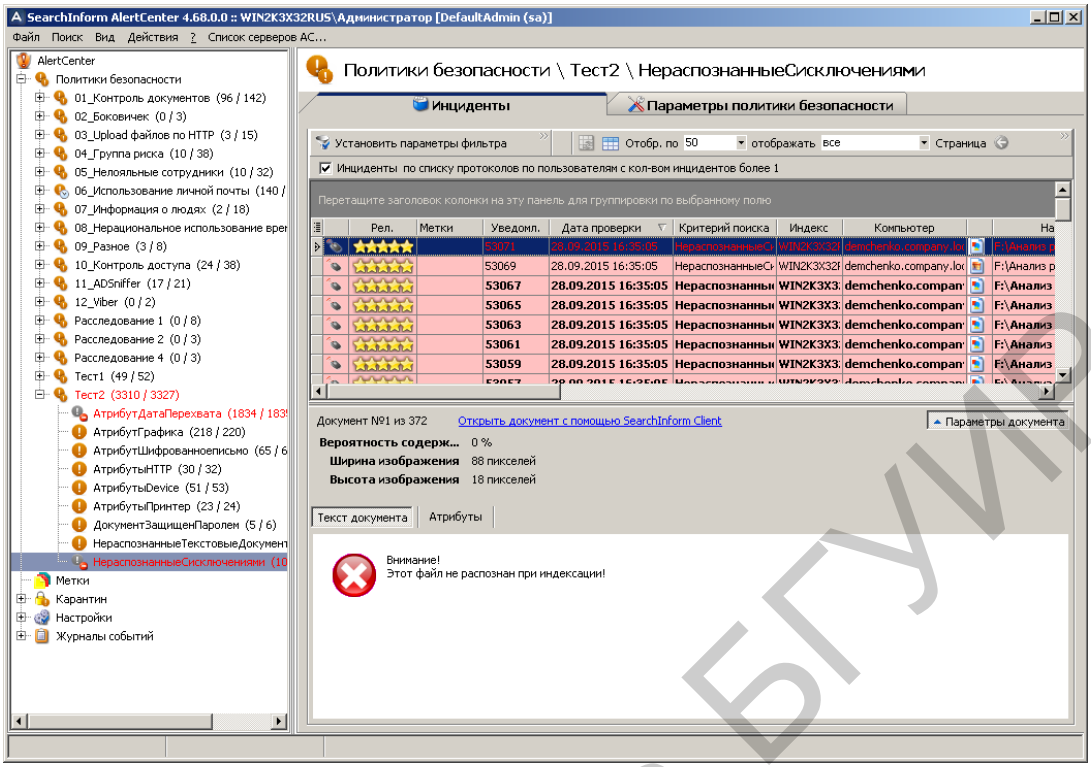


Рис. 3.58. Результат фильтрации

Определить запрос с максимальным/минимальным временем выполнения.
Закрыть окно AlertCenter Client.
Завершить работу с виртуальным компьютером.

3.3. Задание для самостоятельной работы

1. Базируясь на MAC-адресе, IP-адресе или имени пользователя, заданного преподавателем, проконтролировать содержимое перехваченных снимков экранов на предмет выявления содержимого определенной тематики. Примерный перечень вариантов тематик поиска:

– обсуждение поведения руководства организации;
– использование социальных сетей в рабочее время;
– использование Skype в рабочее время;
– использование ICQ в рабочее время;
– изучение программного комплекса SearchInform;
– использование почтовых клиентов для переписки с пользователем leo;
– обсуждение видеоаппаратуры;
– обсуждение стоимости проживания туристов.

2. Провести поиск информации, переданной по электронной почте по адресу ivnic@gmail.com.

3. Определить адрес электронной почты пользователя bublik и произвести поиск писем, которые были переданы с этого адреса и содержали вложенные файлы.

3.4. Контрольные вопросы

1. Почему количество снимков экрана, отфильтрованных по определенному IP-адресу, может отличаться от количества снимков, отфильтрованных по MAC-адресу, который соответствует определенному IP?

2. Зачем кроме фильтрации снимков экрана по именам пользователя нужна фильтрация по IP- и MAC-адресам?

3. Почему на данном виртуальном компьютере при текущей конфигурации программного комплекса SearchInform нельзя реализовать оперативный контроль за экраном пользователя?

4. Какие типы файлов может распознать программный комплекс SearchInform?

5. Какой смысл вкладывается в понятие распознавания текстовых файлов?

6. К каким действиям можно привязать включение снятия скриншотов?

7. Как изменить частоту кадров для режима видеозаписи?

8. Каково назначение опции LiveView агента MonitorSniffer?

9. Можно ли с помощью программного комплекса SearchInform произвести поиск данных, переданных по протоколу http, базируясь на IP-адресе получателя?

10. Можно ли с помощью программного комплекса SearchInform отсортировать данные, переданные на flash-носитель, от данных, переданных на компакт-диск?

11. Можно ли с помощью программного комплекса SearchInform произвести поиск данных, переданных с помощью чата Skype?

12. Можно ли с помощью программного комплекса SearchInform произвести поиск данных, переданных по протоколу ftp, базируясь на направлении передачи?

13. Можно ли с помощью программного комплекса SearchInform произвести поиск данных, переданных по протоколу http, базируясь на направлении передачи?

14. Можно ли с помощью программного комплекса SearchInform произвести поиск данных, переданных по электронной почте с использованием скрытых копий?

ЛАБОРАТОРНАЯ РАБОТА №4
НАСТРОЙКА ПРОГРАММНОГО КОМПЛЕКСА SEARCHINFORM ДЛЯ ПОИСКА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОСНОВЕ ПОДОБИЯ ТЕКСТОВЫХ ФРАГМЕНТОВ. ЧАСТЬ 1

Цель: освоить основные приемы формирования поисковых запросов конфиденциальной информации на основе критериев подобия текста.

4.1. Теоретическая часть

1. Ознакомиться с разделами 1–5 руководства аудитора безопасности системы SearchInform.

2. Ознакомиться со справочными материалами AlertCenter Client.

4.2. Лабораторное задание

1. В соответствии с методическими указаниями лабораторной работы №1 запустить виртуальный компьютер с установленным программным комплексом SearchInform. Установить на виртуальном компьютере дату 1.09.2012.

Выполнить задания лабораторных работ №2, 3.

В дальнейшем предусматривается, что студент освоил методику настроек SearchInform в объеме предыдущих лабораторных работ.

Убедиться в том, что сервер AlertCenter работает, в противном случае его следует запустить с помощью консоли SearchInform AlertCenter Console.

Открыть окно AlertCenter Client.

Использовав соответствующую консоль, убедиться в том, что сервер AlertCenter запущен. В противоположном случае запустить сервер.

2. В соответствии с методическими указаниями лабораторной работы №2 создать новую политику безопасности с названием «Тест3». Включить в политику все доступные поисковые индексы DeviceSniffer и MailSniffer. Получать уведомления должен пользователь DefaultAdmin. Окно политики показано на рис. 4.1.

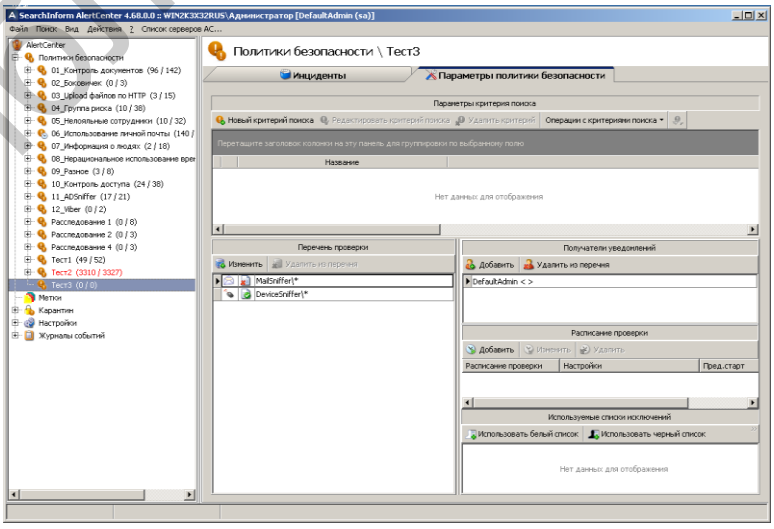


Рис. 4.1. Окно политики безопасности «Тест3»

3. Сформировать критерий «Поиск похожих». Для этого выполнить следующее.

В соответствии с рис. 4.2 создать критерий для поиска файлов, содержимое которых как минимум на 10 % релевантно тексту:

«УСТАВ

ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

СТАТЬЯ 1. ОБЩИЕ ПОЛОЖЕНИЯ

СТАТЬЯ 2. ЦЕЛИ И ВИДЫ ДЕЯТЕЛЬНОСТИ ОБЩЕСТВА

СТАТЬЯ 3. УЧАСТНИКИ ОБЩЕСТВА. ПРАВА И ОБЯЗАННОСТИ УЧАСТНИКОВ

СТАТЬЯ 4. ВЫХОД (ИСКЛЮЧЕНИЕ) УЧАСТНИКА ИЗ ОБЩЕСТВА

СТАТЬЯ 5. УСТАВНЫЙ ФОНД И ИМУЩЕСТВО ОБЩЕСТВА

СТАТЬЯ 6. ПЕРЕХОД ДОЛИ (ЧАСТИ ДОЛИ) УЧАСТНИКА В УСТАВНОМ ФОНДЕ К ДРУГОМУ ЛИЦУ

СТАТЬЯ 7. ОБРАЩЕНИЕ ВЗЫСКАНИЯ НА ДОЛЮ (ЧАСТЬ ДОЛИ) УЧАСТНИКА В УСТАВНОМ ФОНДЕ ОБЩЕСТВА

СТАТЬЯ 8. УСЛОВИЯ И ПОРЯДОК РАСПРЕДЕЛЕНИЯ ПРИБЫЛИ И УБЫТКОВ ОБЩЕСТВА

СТАТЬЯ 9. ОТВЕТСТВЕННОСТЬ ОБЩЕСТВА И ЕГО УЧАСТНИКОВ

СТАТЬЯ 10. ОРГАНЫ УПРАВЛЕНИЯ И КОНТРОЛЯ ОБЩЕСТВА

СТАТЬЯ 11. УЧЁТ И ОТЧЁТНОСТЬ В ОБЩЕСТВЕ

СТАТЬЯ 12. ФИЛИАЛЫ И ПРЕДСТАВИТЕЛЬСТВА

СТАТЬЯ 13. АФФИЛИРОВАННЫЕ ЛИЦА ОБЩЕСТВА. ЗАИНТЕРЕСОВАННОСТЬ АФФИЛИРОВАННЫХ ЛИЦ В СОВЕРШЕНИИ ОБЩЕСТВОМ СДЕЛКИ

СТАТЬЯ 14. РЕОРГАНИЗАЦИЯ И ЛИКВИДАЦИЯ ОБЩЕСТВА

ПОДПИСИ УЧАСТНИКОВ:»

Отметим, что данный текст необходимо ввести в поле «Текст для поиска».

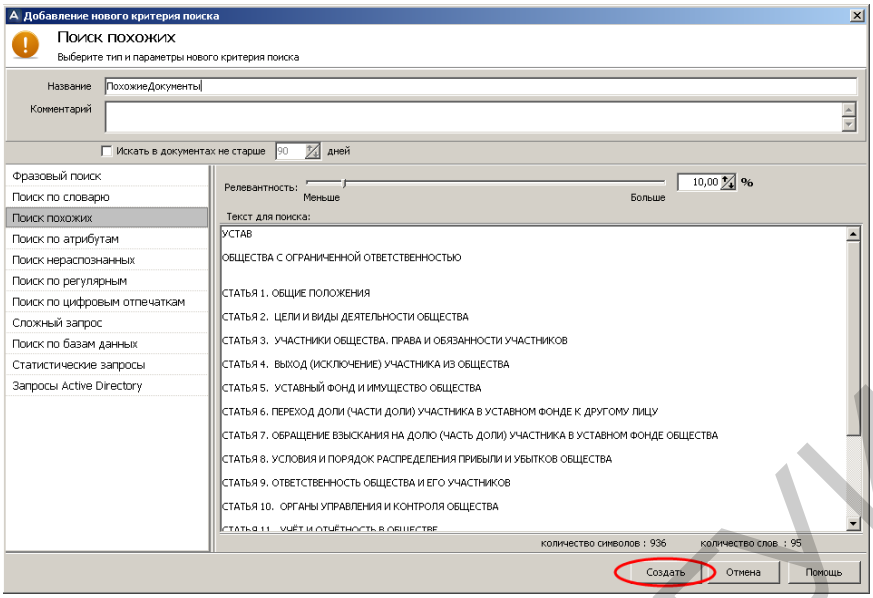


Рис. 4.2. Создание критерия «ПохожиеДокументы»

Запустить принудительное выполнение критерия поиска «ПохожиеДокументы» и убедиться в его результативности (рис. 4.3). Зафиксировать время выполнения поиска.

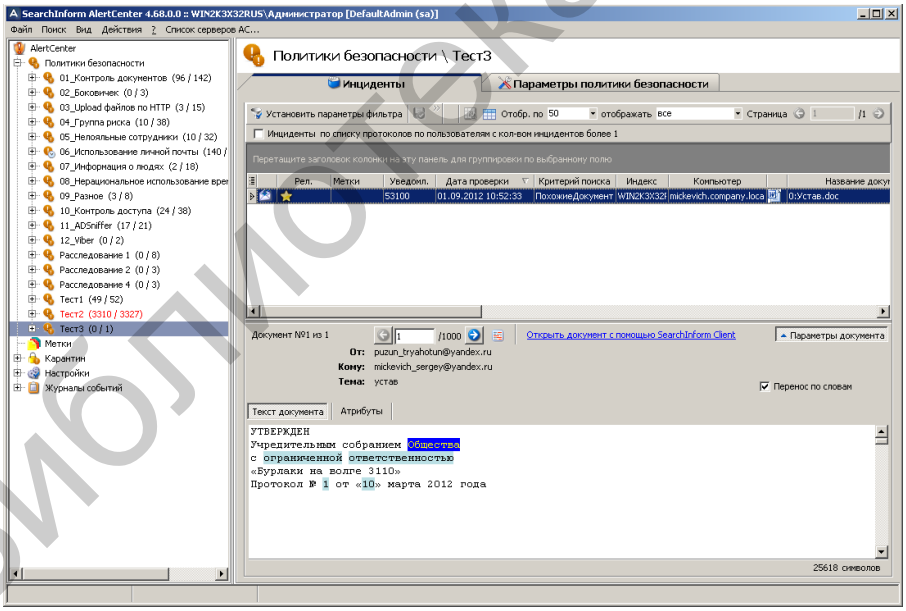


Рис. 4.3. Индикация инцидентов по критерию «ПохожиеДокументы»

Исследовать влияние «релевантности» поискового запроса и искомого текста на эффективность метода поиска похожих документов. Для этого следует:

1. Увеличить на 1 % степень релевантности критерия «ПохожиеДокументы».

2. Запустить принудительное выполнение критерия «ПохожиеДокументы», согласившись при этом на очистку инцидентов (рис. 4.4).

3. Убедиться в результативности поиска.

4. Повторять этапы 1–3 до тех пор, пока в результатах поиска не будет зафиксировано ни одного инцидента. Зафиксировать максимальную степень релевантности.

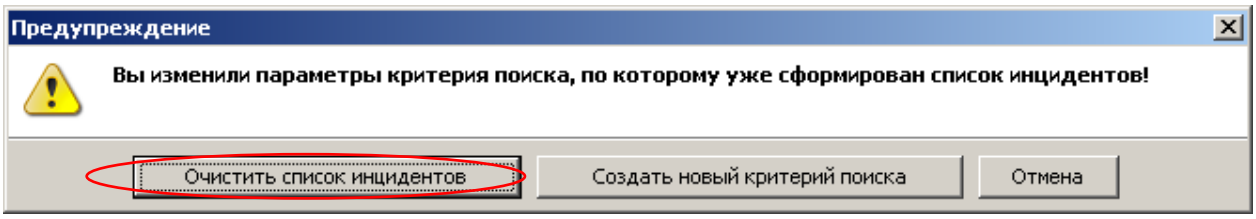


Рис. 4.4. Запрос на очистку списка инцидентов

Удалить политику безопасности «Тест2».

Формирование критерия «Поиск по цифровым отпечаткам» на основании имеющейся библиотеки цифровых отпечатков выполнить следующим образом. В соответствии с рис. 4.5 создать критерий для поиска файлов цифровых отпечатков, которые как минимум на 40 % релевантны образцам.

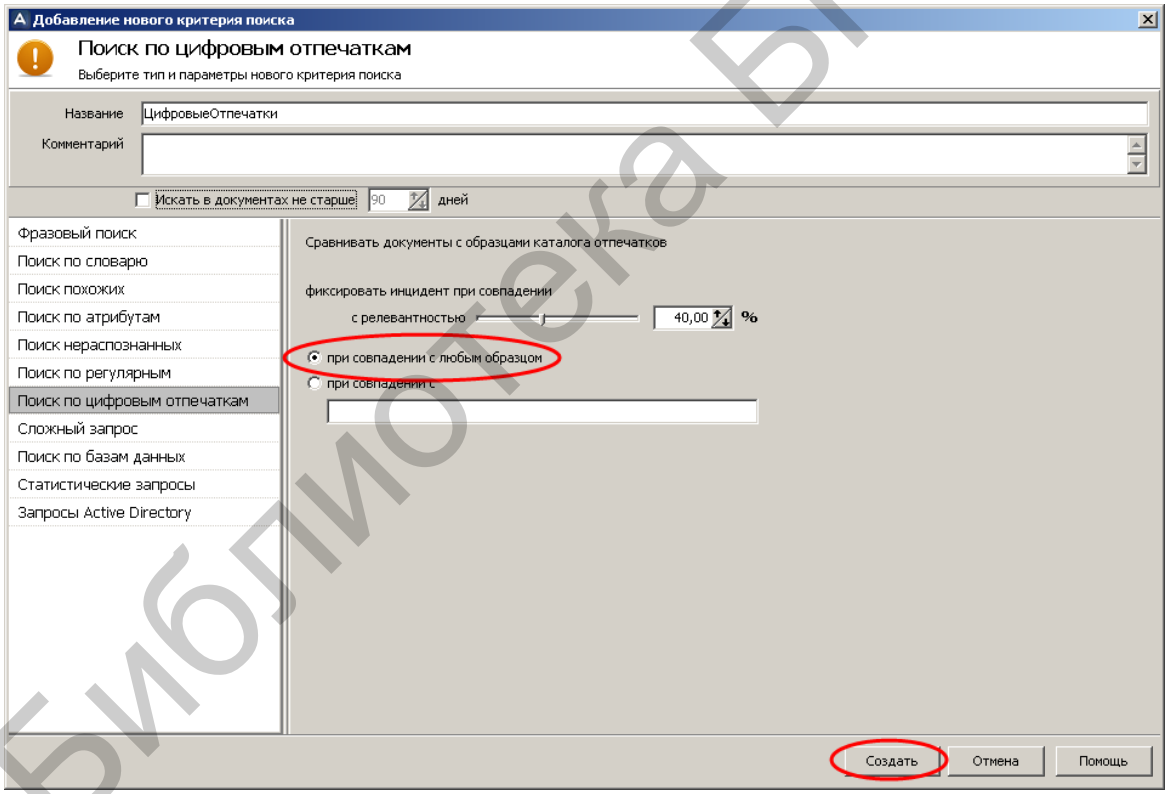


Рис. 4.5. Создание критерия «ЦифровыеОтпечатки»

Запустить принудительное выполнение критерия поиска «ЦифровыеОтпечатки». В случае когда время выполнения полной проверки достаточно большое, можно прервать проверку. Для этого можно воспользоваться инструкциями (рис. 4.6, 4.7).

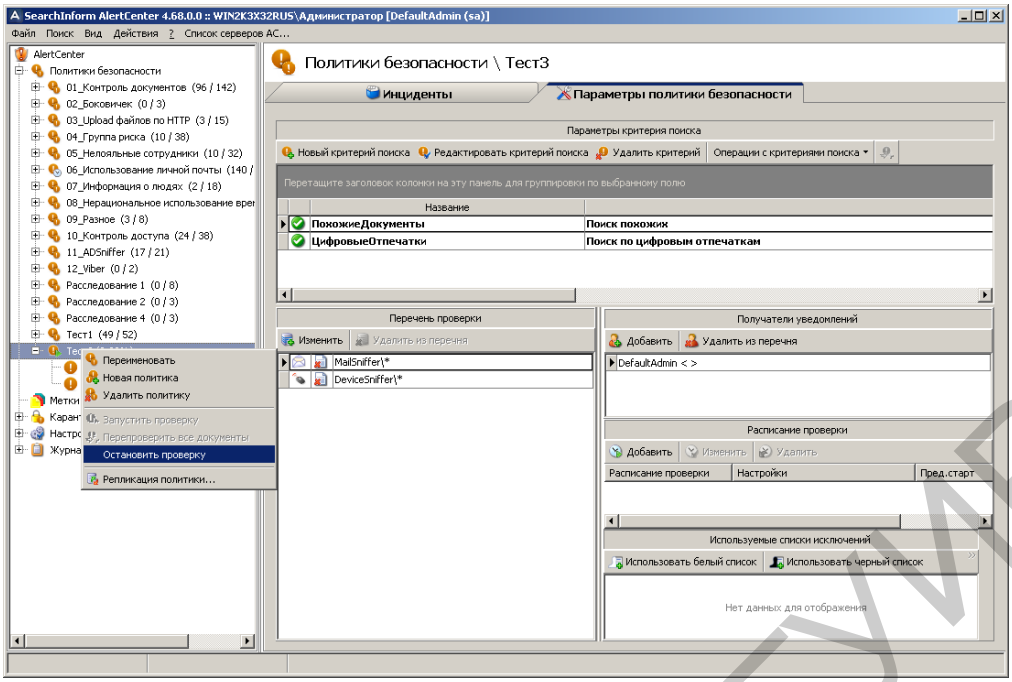


Рис. 4.6. Выбор контекстного меню остановки проверки

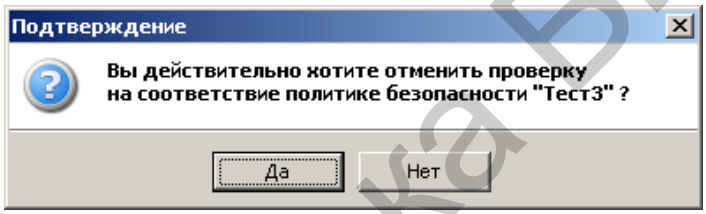


Рис. 4.7. Подтверждение остановки проверки

Убедиться в результативности проверки (рис. 4.8).

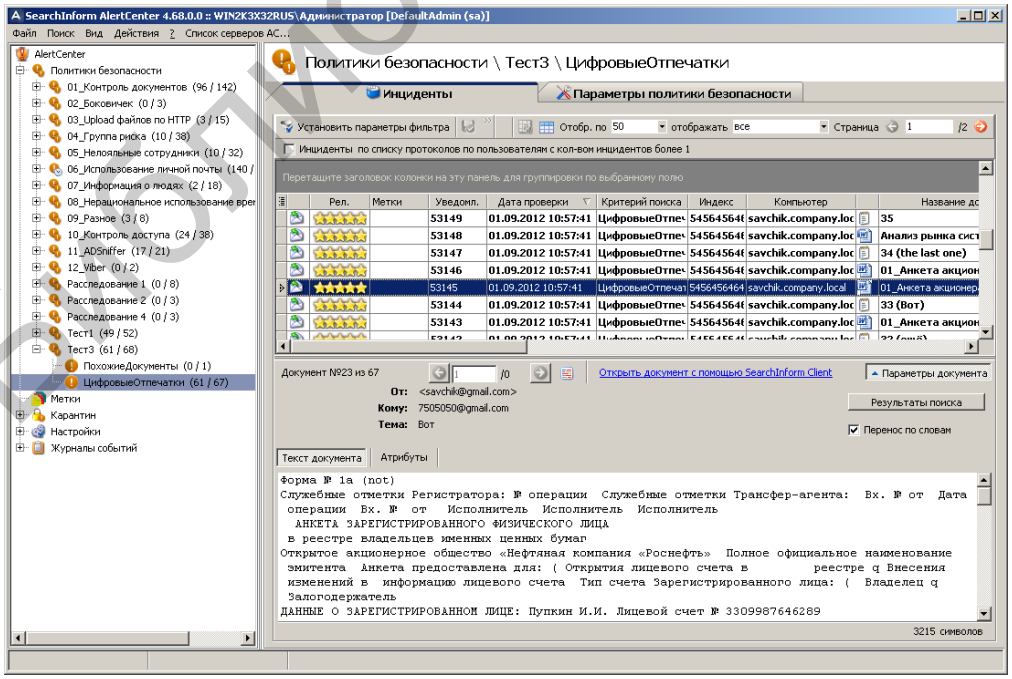


Рис. 4.8. Индикация инцидентов по критерию «ЦифровыеОтпечатки»

Формирование критерия «Поиск по цифровым отпечаткам» на основании нового каталога цифровых отпечатков выполнить следующим образом. В корне диска «С:» создать каталог «Отпечатки».

Копировать в каталог «Отпечатки» файл, соответствующий одному из перехваченных документов, например «plan_po_marketingy.doc», находящийся в каталоге «С:\Исходные базы_2010\маркетинговые планы и исследования».

Создать в каталоге «Отпечатки» файл 1.rtf и записать в него следующий текст: «Критерием эффективности управления дебиторской задолженностью определен критерий максимизации прибыли, сопутствующей кредитованию покупателей рынка «B2B», т. е. дистрибьюторов и розничных магазинов. Следствием эффективного управления дебиторской задолженностью является увеличение чистой прибыли и положительного чистого денежного потока, что ценно для всех основных акционерных групп компании: учредителей, инвесторов, потребителей, поставщиков, персонала и государства. Это означает, что менеджмент компании должен профессионально владеть всеми аспектами эффективного управления дебиторской задолженностью. Это обеспечивает обучение на этом семинаре, который отражает авторскую технологию, примененную многократно на практике и обеспечившую впечатляющие результаты».

В соответствии с рис. 4.9–4.18 создать новый каталог индексов образцов цифровых отпечатков.

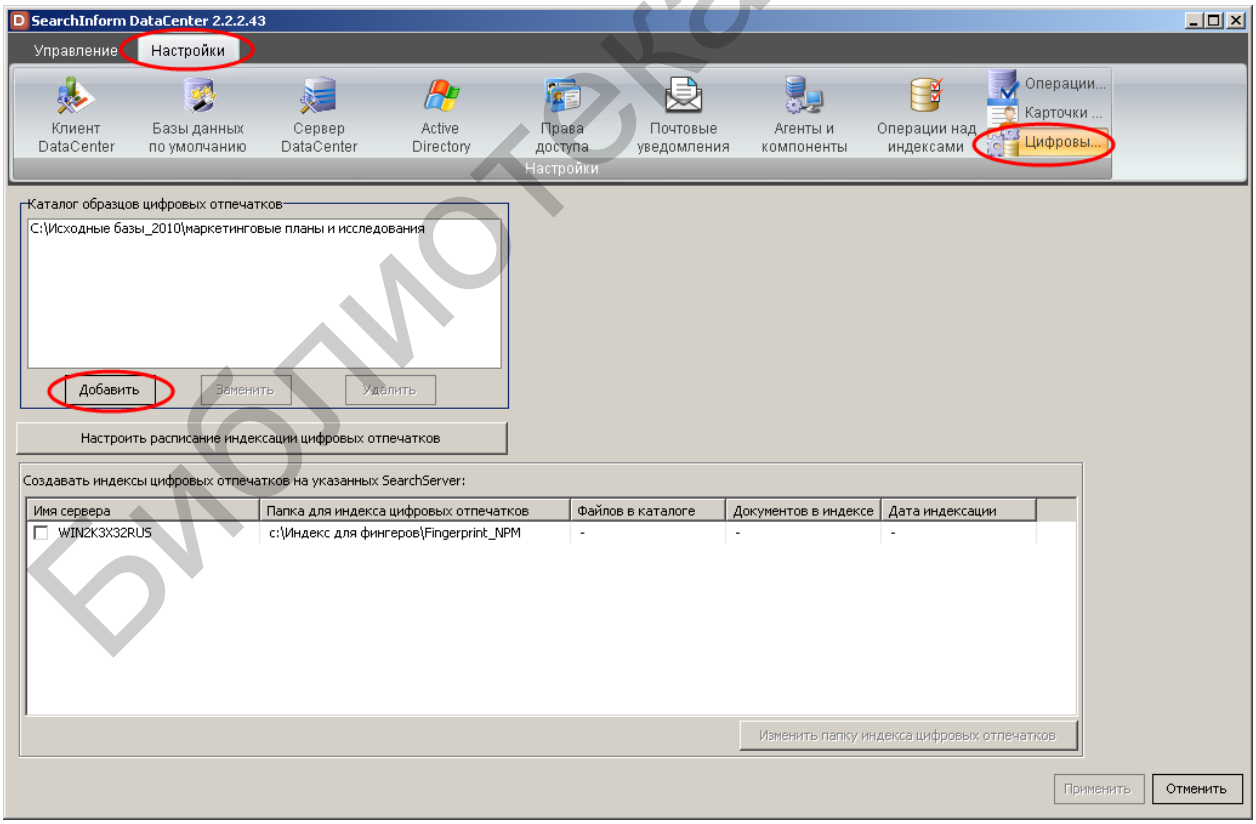


Рис. 4.9. Добавление нового каталога на вкладке «Цифровые отпечатки» в DataCenter

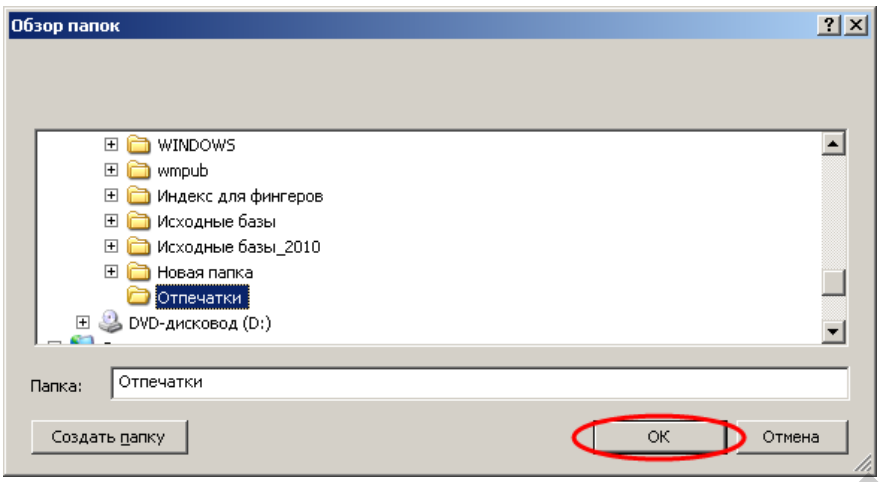


Рис. 4.10. Добавление предварительно созданной папки «Отпечатки»

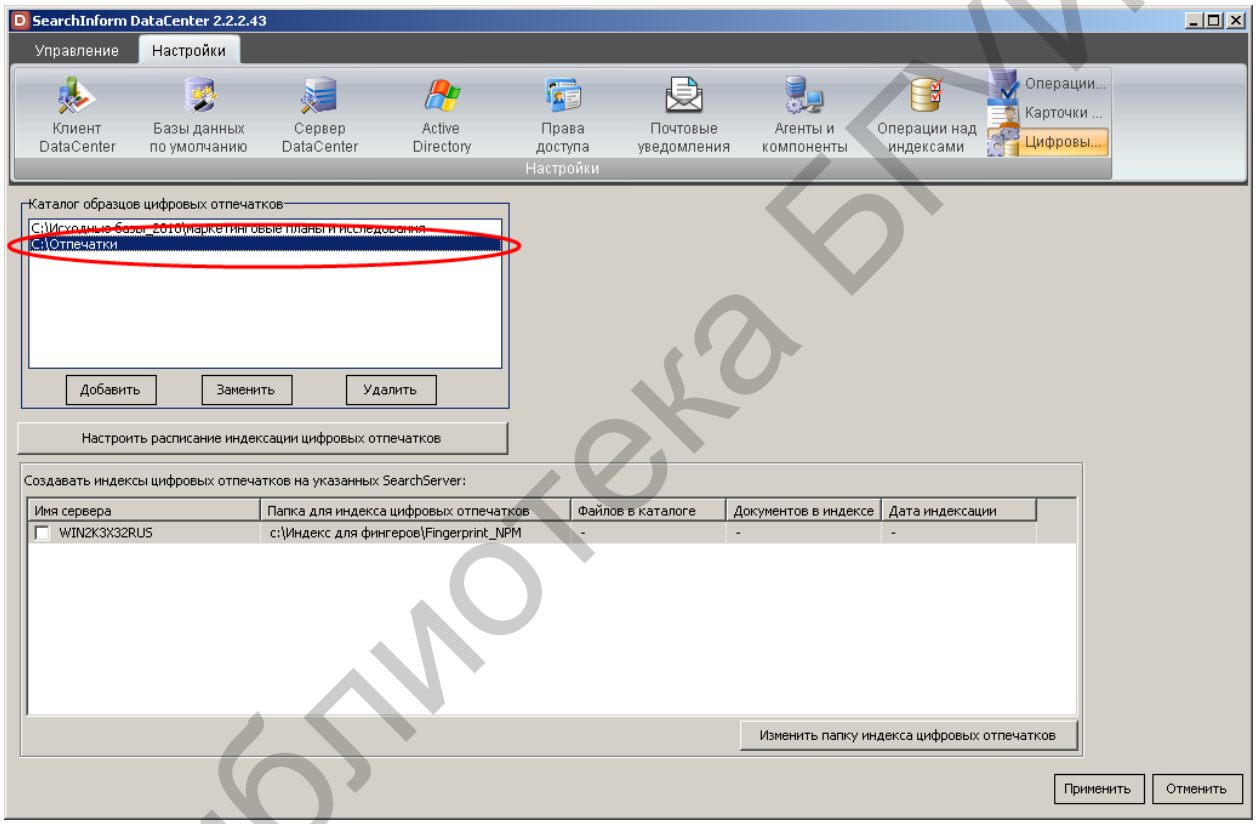


Рис. 4.11. Индикация успешного добавления каталога

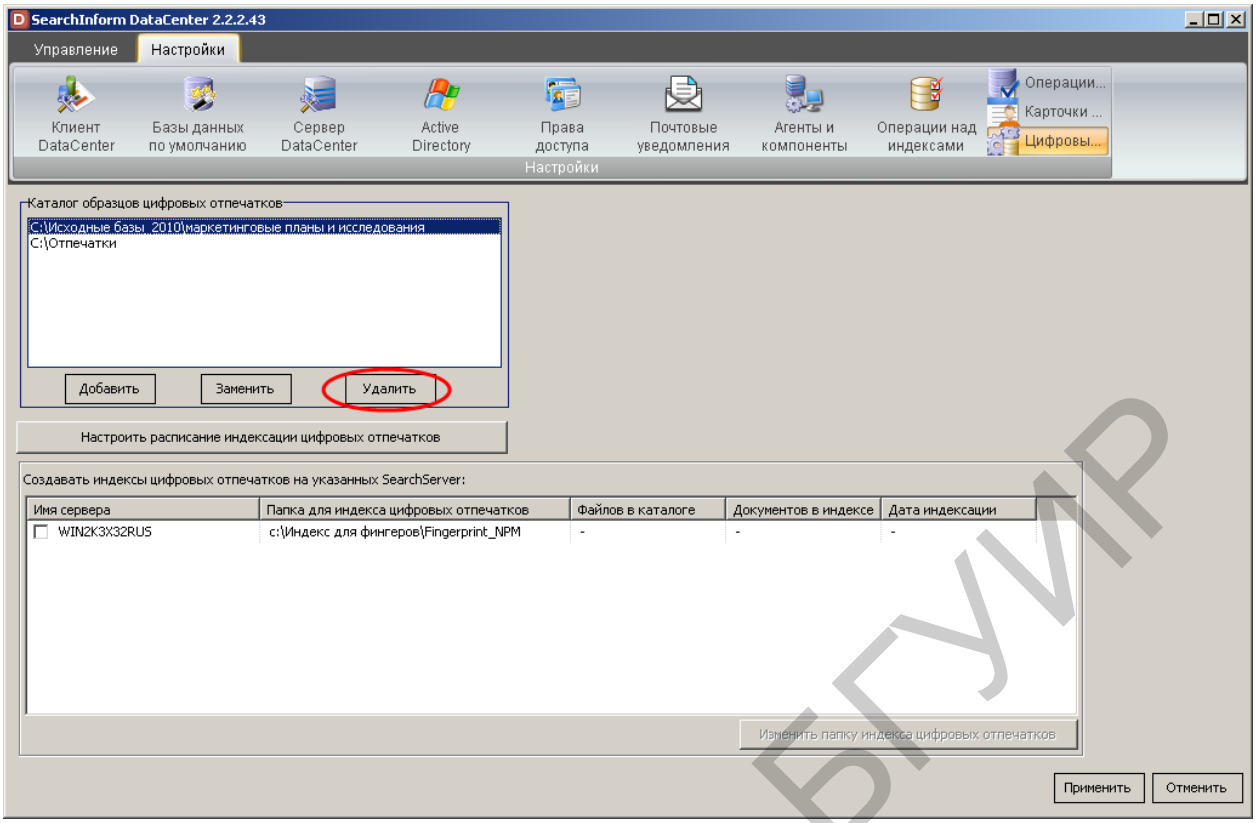


Рис. 4.12. Удаление старого каталога
«C:\Исходные базы_2010\маркетинговые планы и исследования»

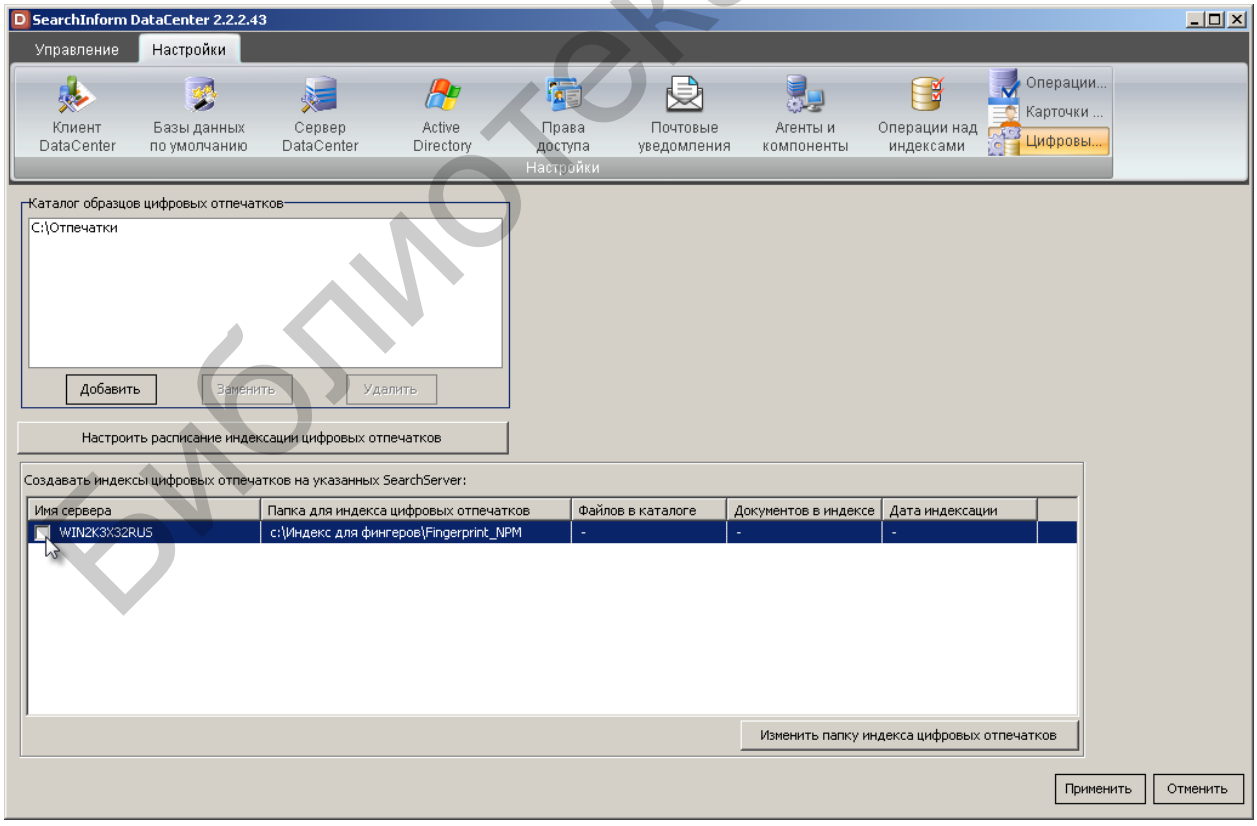


Рис. 4.13. Выбор сервера, который будет создавать
индекс цифровых отпечатков

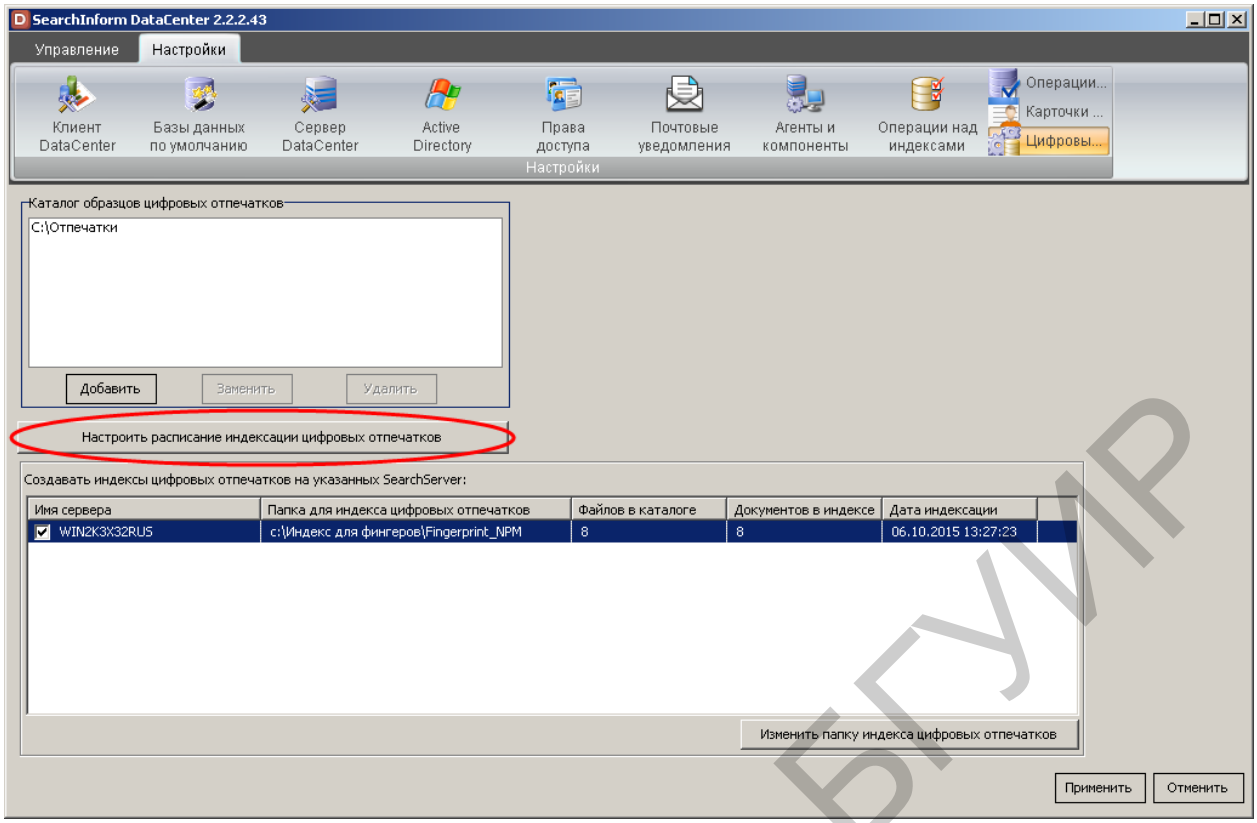


Рис. 4.14. Переход к настройке расписания индексации цифровых отпечатков

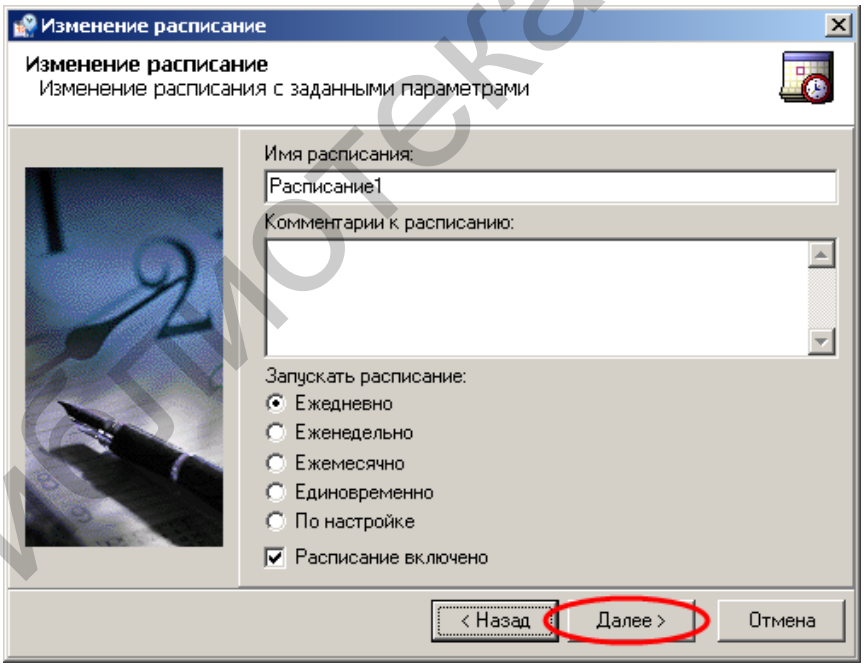


Рис. 4.15. Первый этап настройки расписания

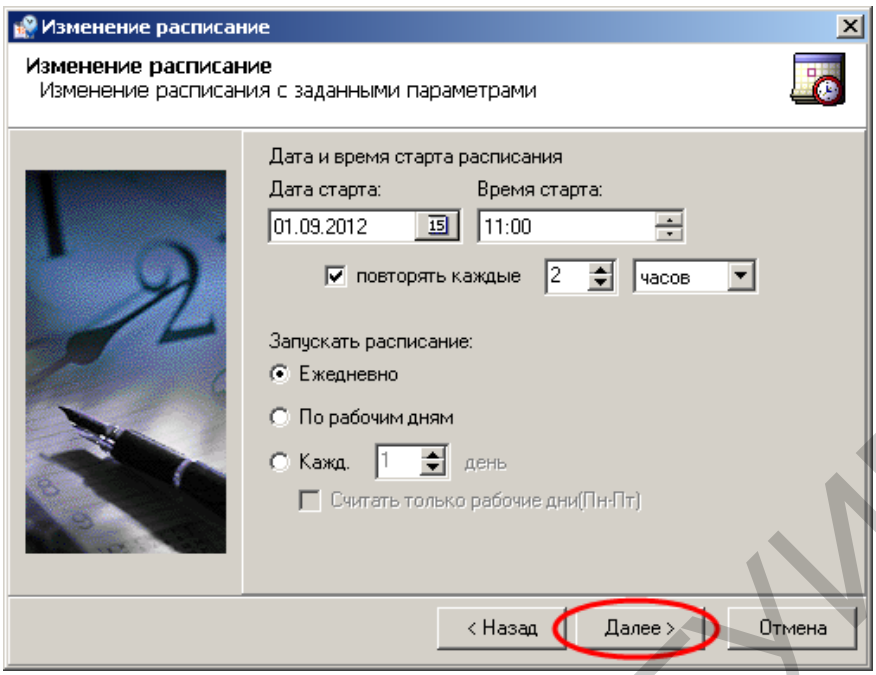


Рис. 4.16. Второй этап настройки расписания

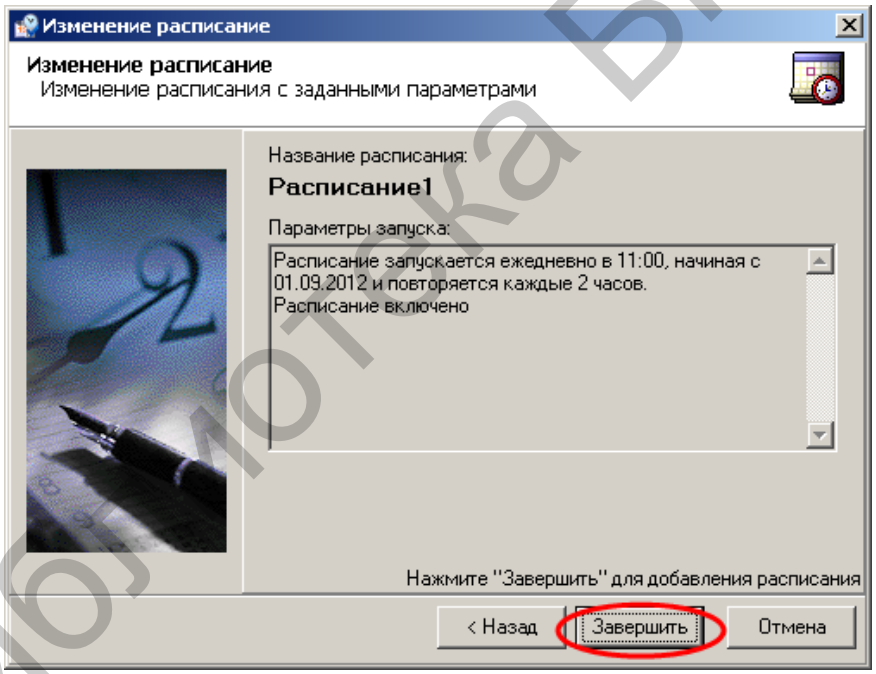


Рис. 4.17. Третий этап настройки расписания

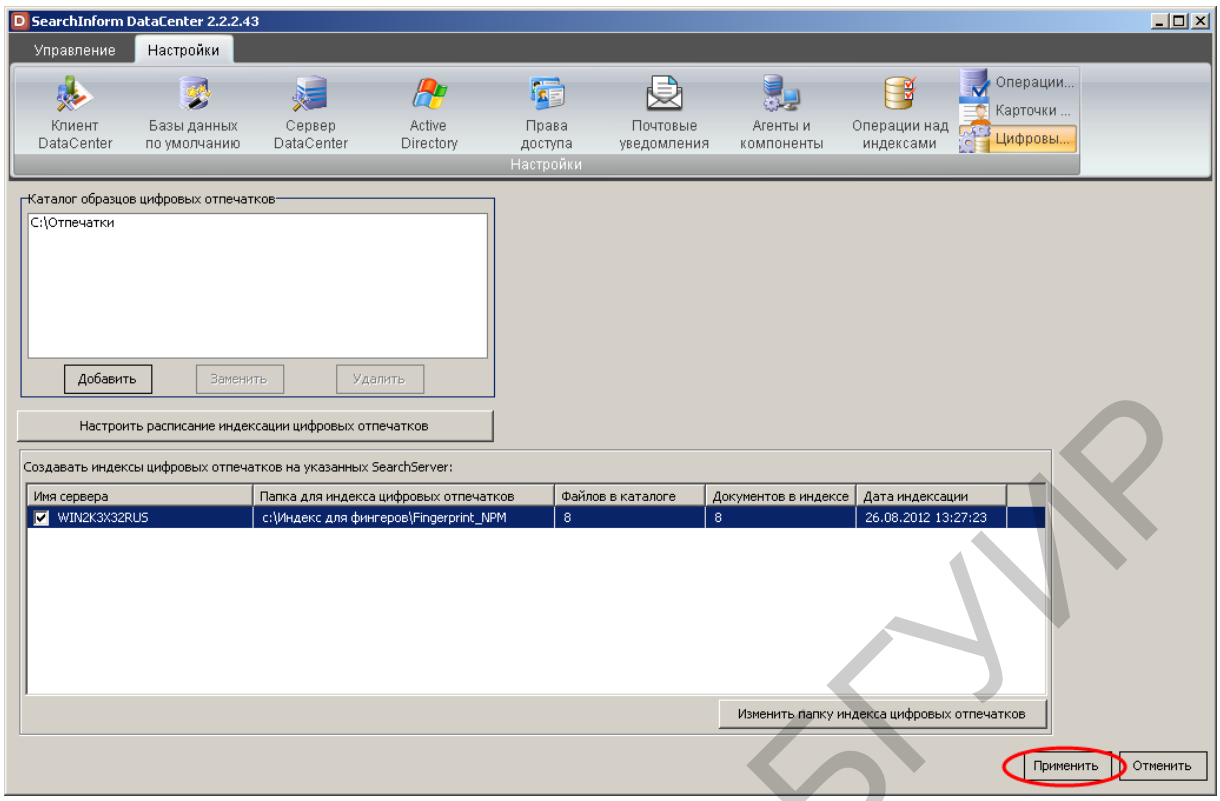


Рис. 4.18. Подтверждение всех произведенных изменений

При необходимости можно произвести индексацию цифровых отпечатков, не дожидаясь обновления по расписанию, в соответствии с рис. 4.19–4.21.

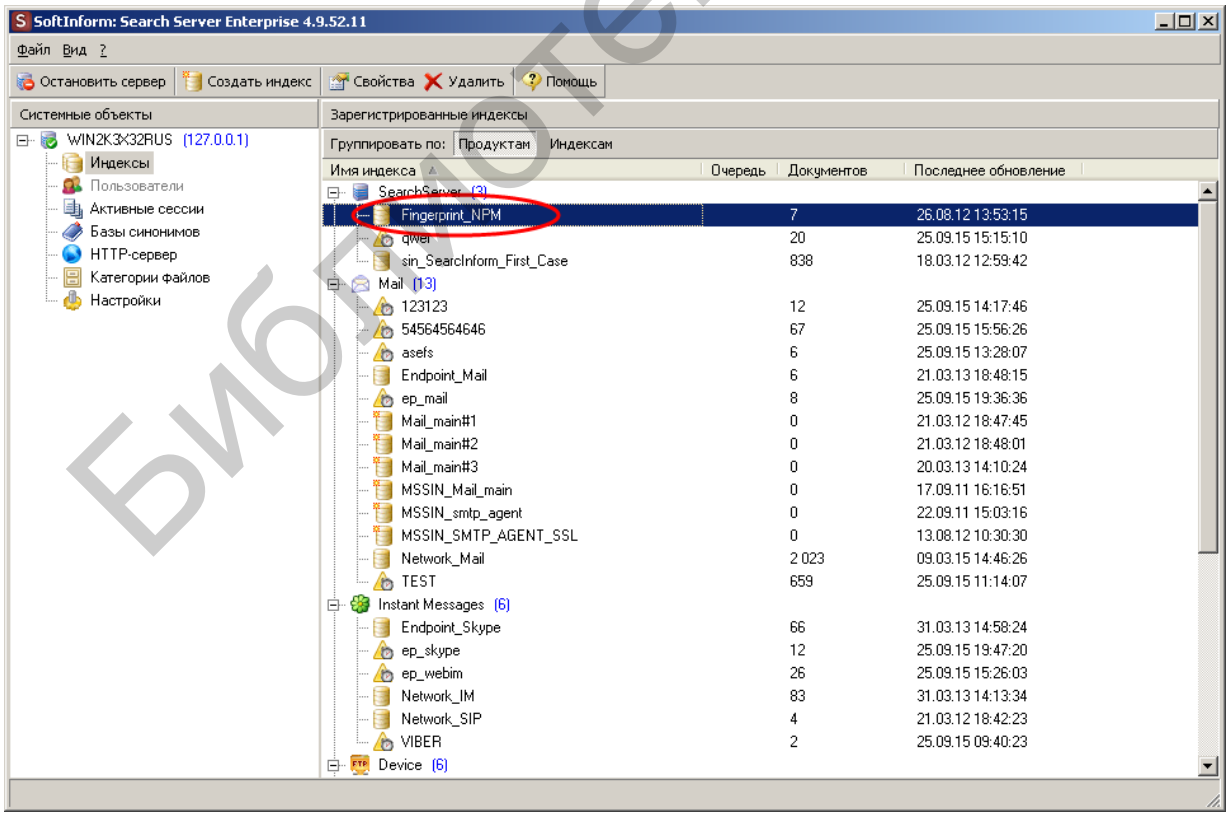


Рис. 4.19. Выбор индекса цифровых отпечатков

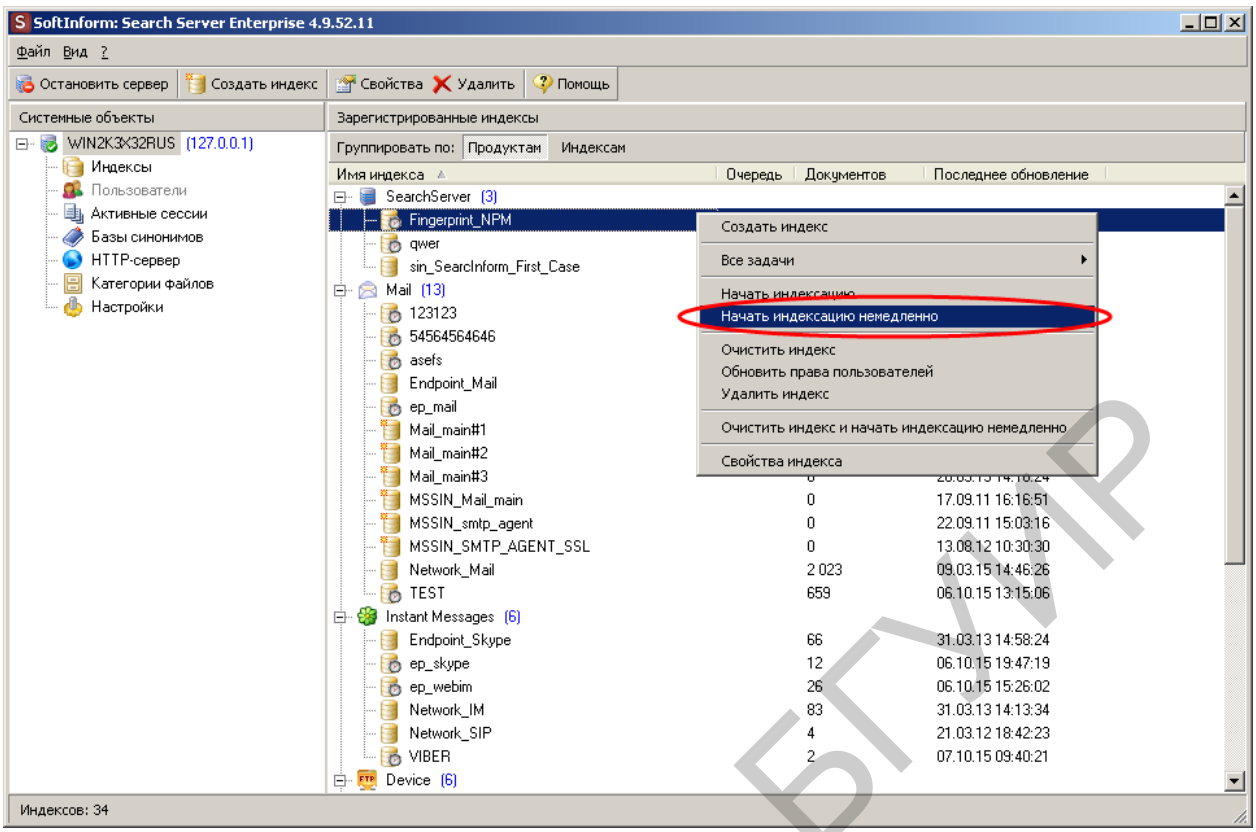


Рис. 4.20. Запуск процесса немедленной индексации

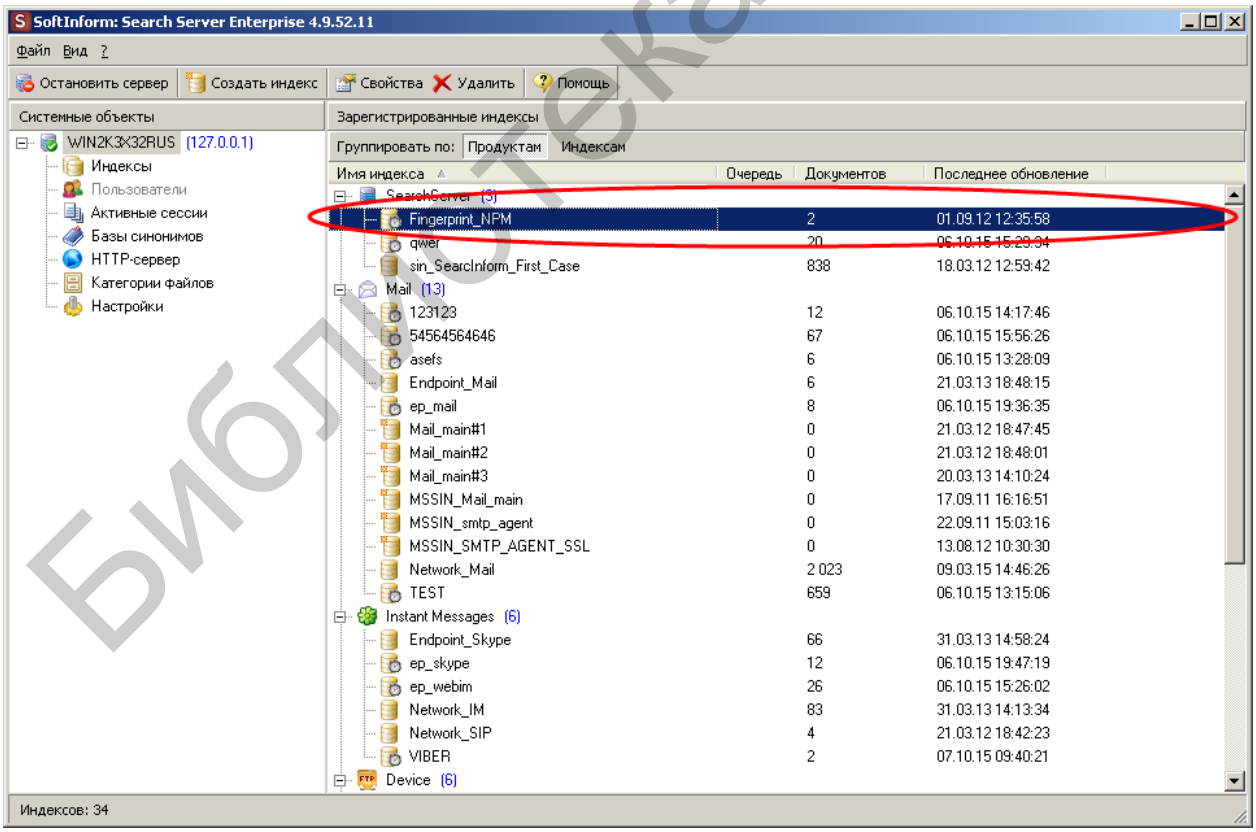


Рис. 4.21. Индикация успешно выполненной индексации

В связи с изменением каталога цифровых отпечатков необходимо произвести переиндексацию индексов с перехваченными данными в соответствии с рис. 4.22–4.24.

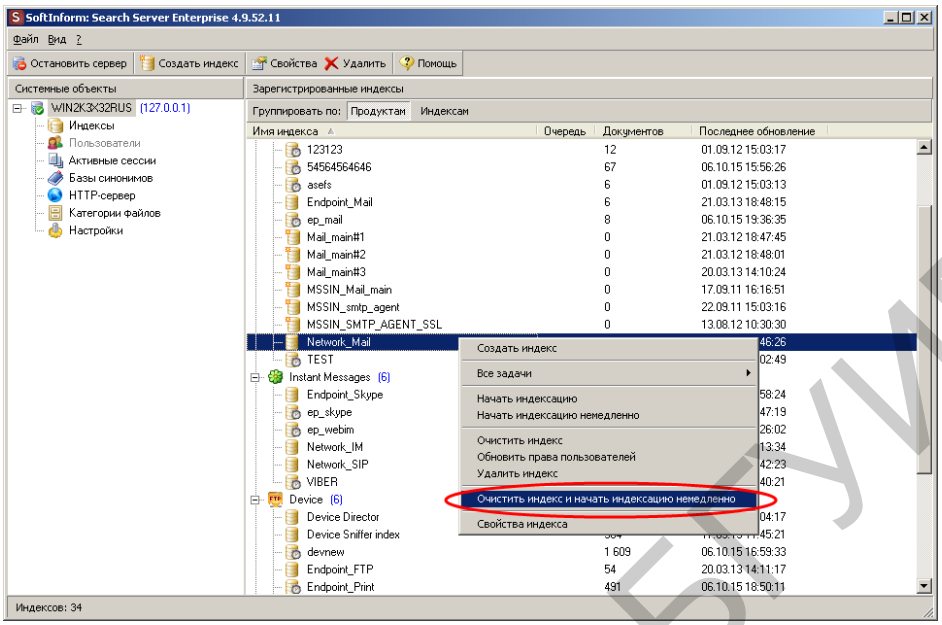


Рис. 4.22. Выбор опции «Очистить индекс и начать индексацию немедленно»

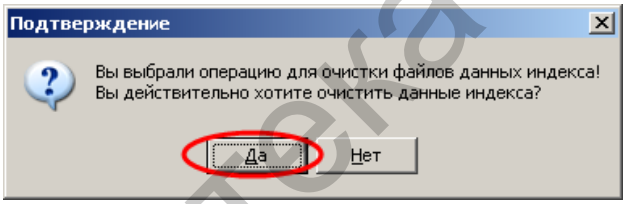


Рис. 4.23. Подтверждение очистки индекса

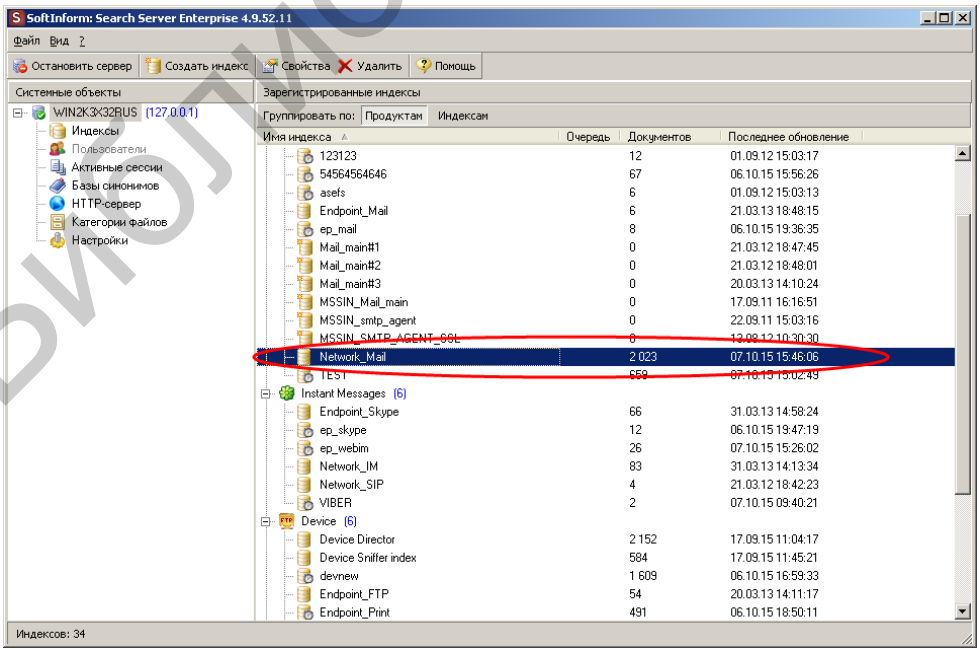


Рис. 4.24. Индикация завершенного процесса индексации

В соответствии с рис. 4.25, 4.26 запустить проверку правильности функционирования созданного индекса цифровых отпечатков.

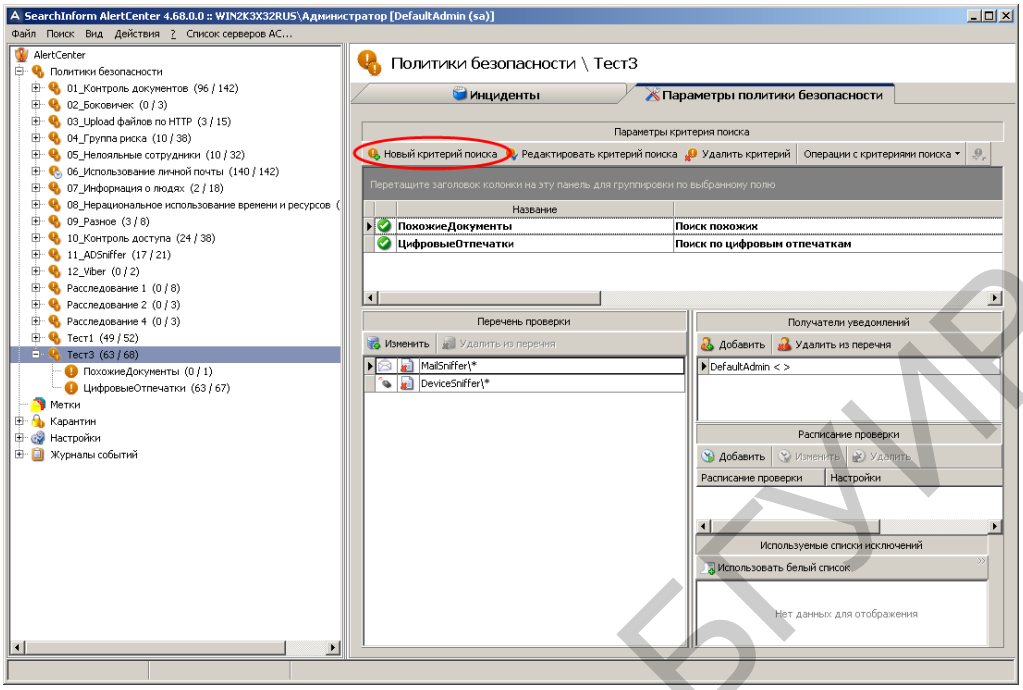


Рис. 4.25. Создание нового критерия поиска

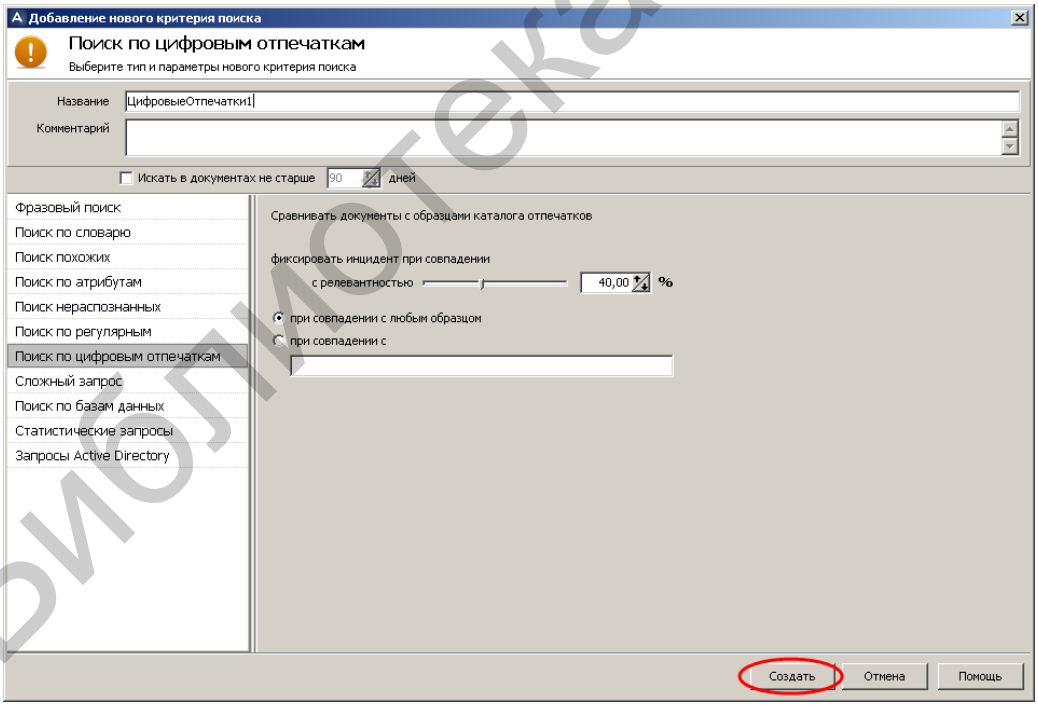


Рис. 4.26. Указание параметров поиска по цифровым отпечаткам

В соответствии с рис. 4.27–4.30 произвести индивидуальные настройки перечня проверки для созданного критерия.

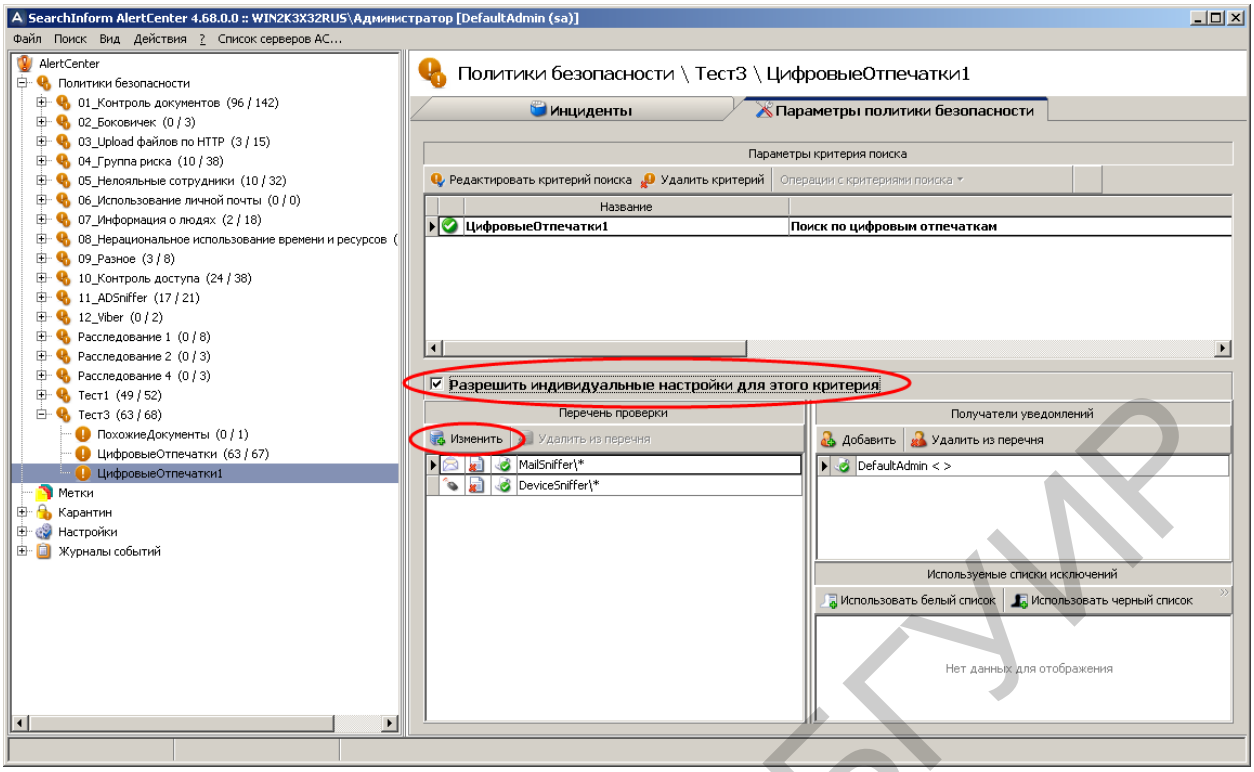


Рис. 4.27. Включение индивидуальных настроек для критерия поиска

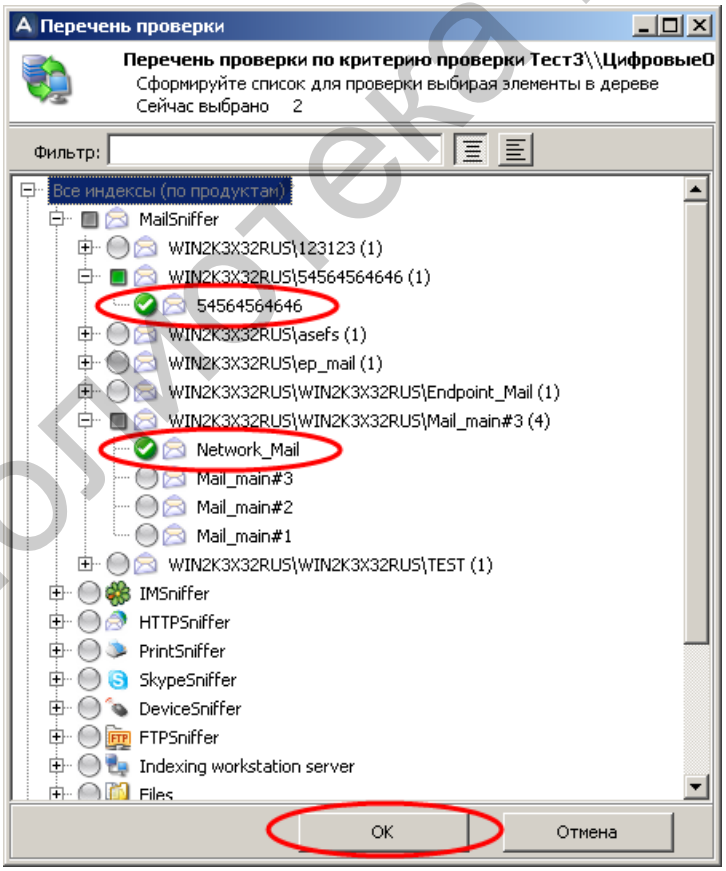


Рис. 4.28. Выбор двух индексов MailSniffer и отключение индекса DeviceSniffer

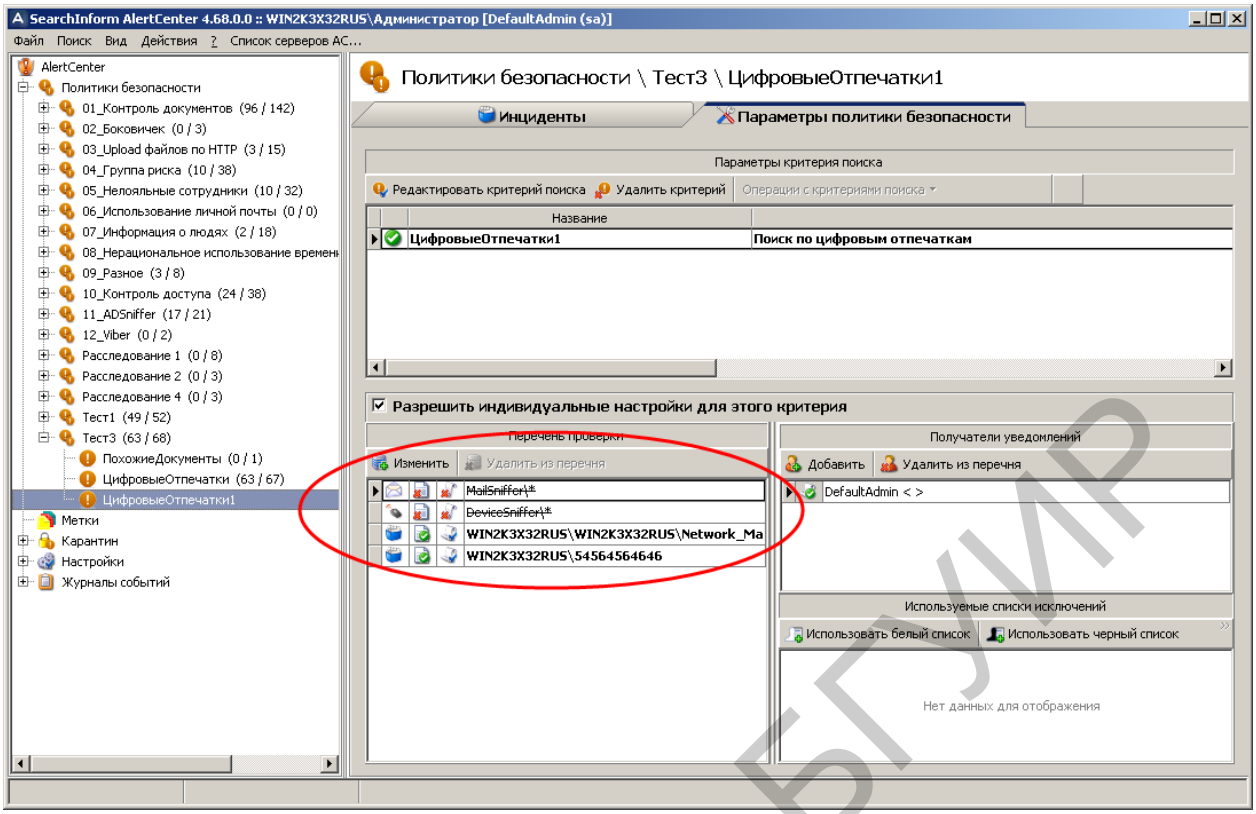


Рис. 4.29. Индикация изменений перечня проверки

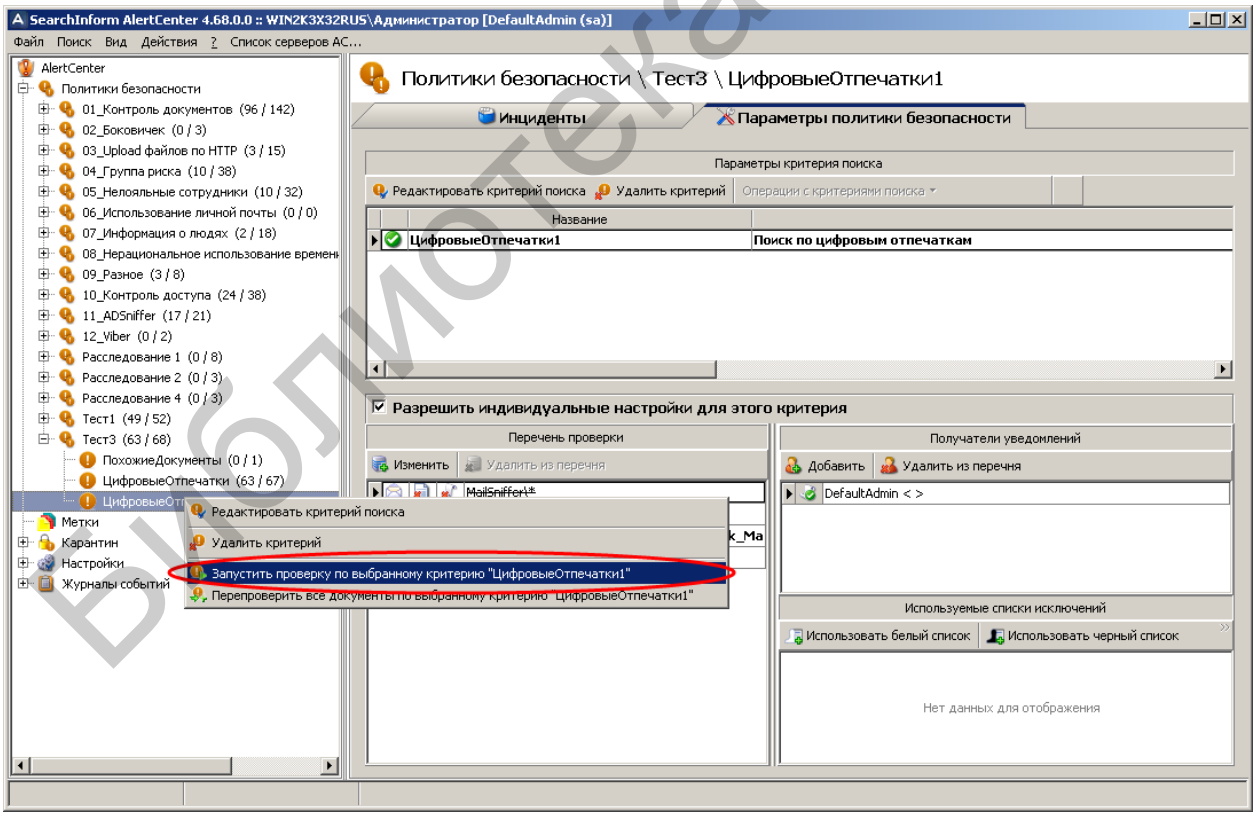


Рис. 4.30. Запуск проверки по созданному критерию

В соответствии с рис. 4.31–4.35 запустить проверку по совпадению с документом «1.rtf».

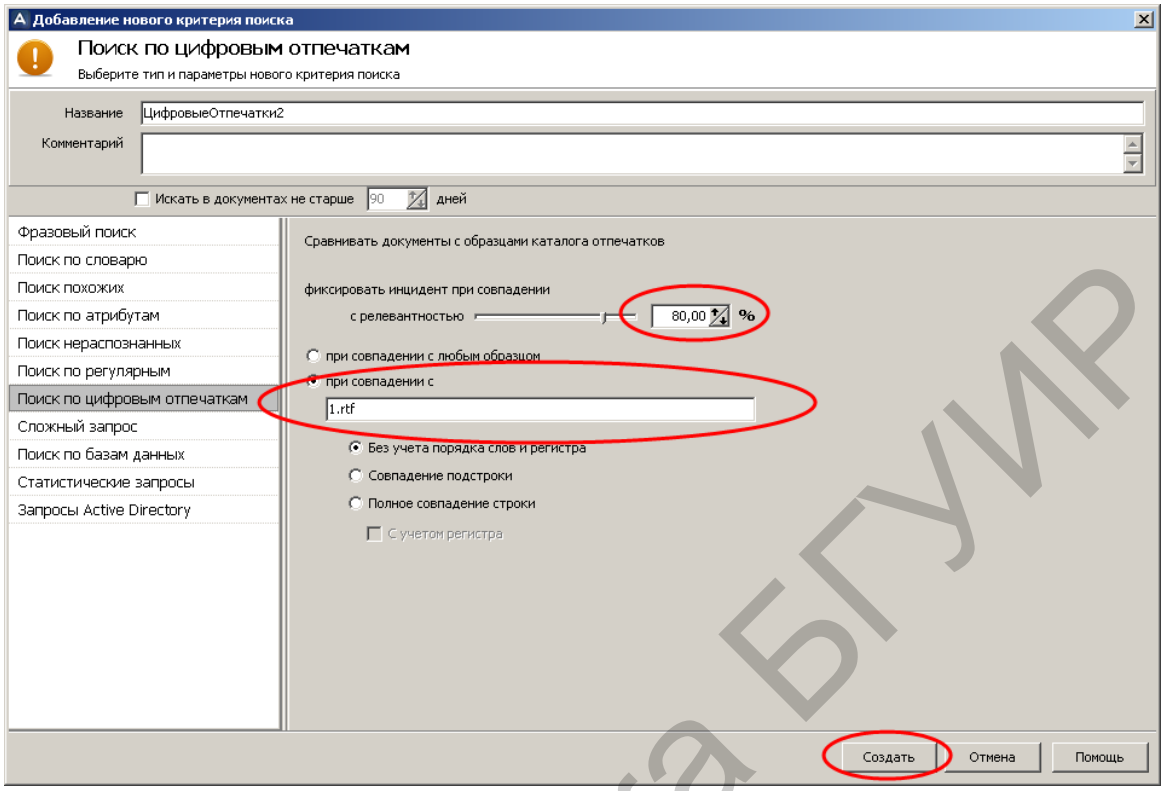


Рис. 4.31. Указание параметров поиска

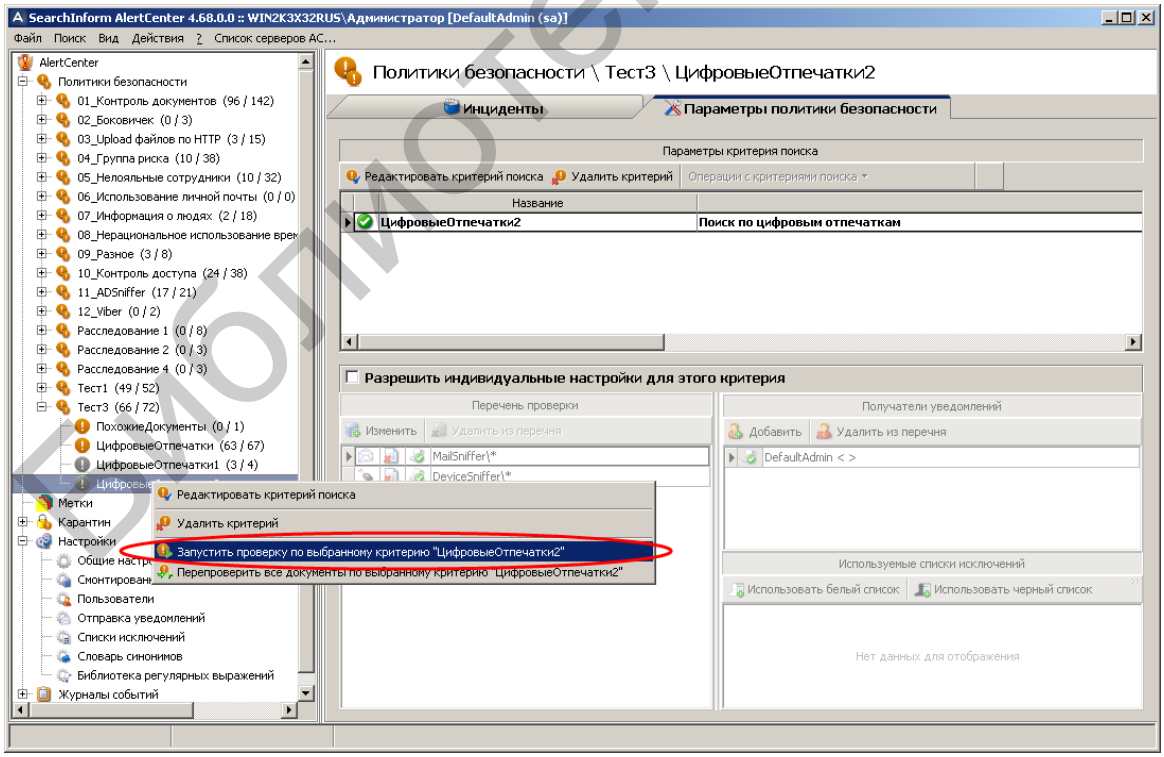


Рис. 4.32. Запуск проверки

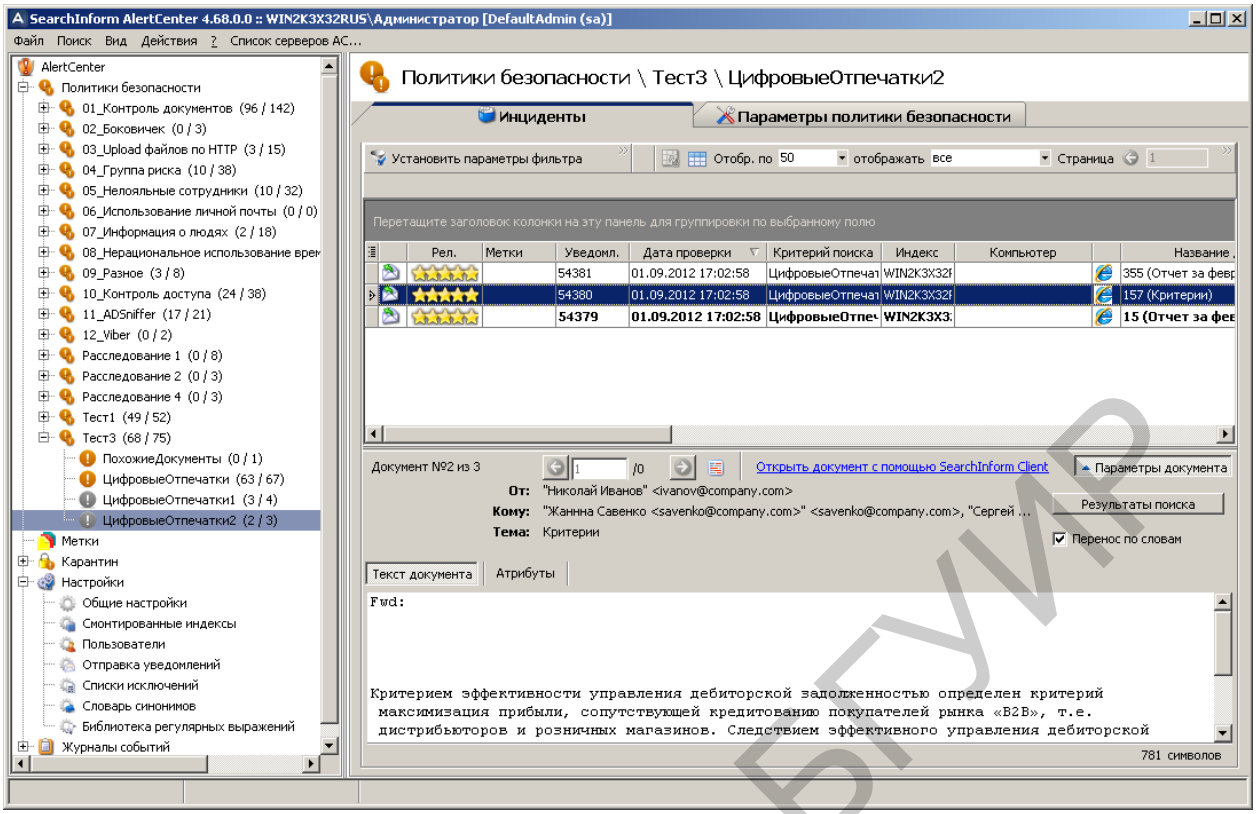


Рис. 4.33. Индикация результатов проверки

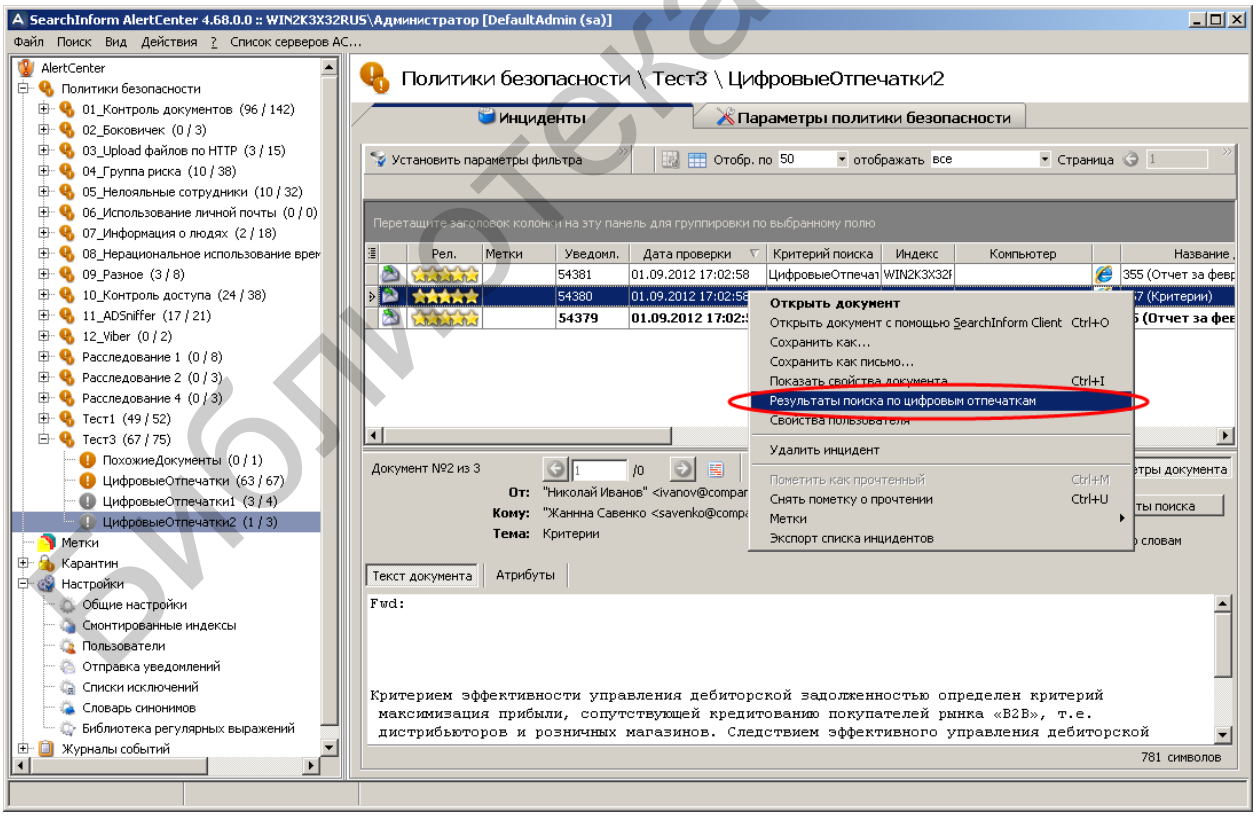


Рис. 4.34. Переход к режиму просмотра результатов поиска по цифровым отпечаткам

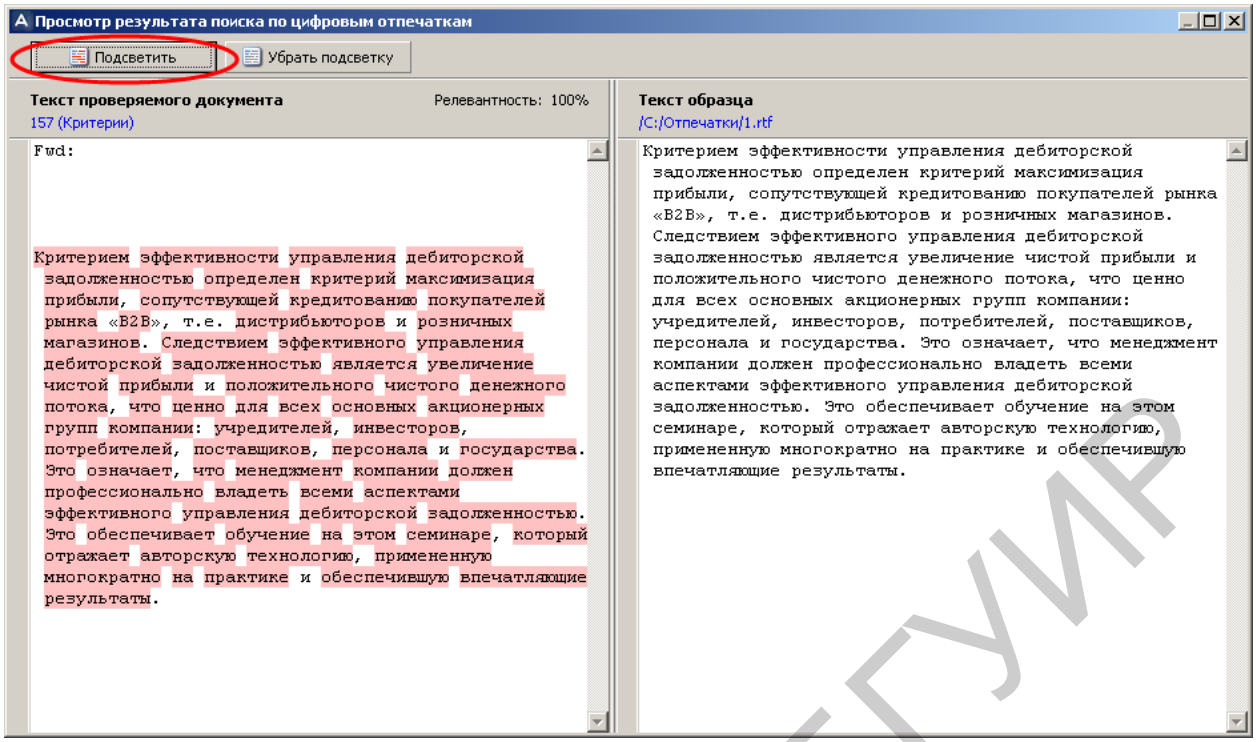


Рис. 4.35. Подсветка текста, совпадающего с образцом

Формирование сложных запросов

В соответствии с рис. 4.36–4.47 создать сложный запрос для поиска электронных писем, отправленных не позже 3 лет и 1 дня назад по адресу «linnik@company.com», в котором содержится следующий список сотрудников компании: «Гудилин Виктор, Бычок Сергей, Савенко Жанна, Мицкевич Сергей, Линник Евгения, Филипович Анна, Мамаев Антон, Самохвал Людмила, Иванов Николай, Лихтарович Владислав, Сергеенко Анастасия, Поляк Федор, Прохоров Михаил, Трепенок Виктория, Коврижка Владимир, Прищепчик Ольга, Чижик Валентин, Лукьяненко Инга, Бубликов Валерий, Шумилин Олег, Титовец Григорий, Савчик Николай, Конев Евгений, Толкач Александр, Демченко Галина, Сосновский Артем, Голыго Нина, Кобриков Лаврентий, Сидорович Светлана».

Отметим, что формируемый сложный запрос представляет собой строку «A and B and C», где A – псевдоним критерия поиска по времени отправления, B – псевдоним критерия поиска по адресу получателя, а C – псевдоним критерия поиска похожих. При этом в качестве критерия C будет использован ранее сформированный критерий «Список сотрудников», предназначенный для поиска всех документов, содержащих список сотрудников компании. Критерии A и B следует сформировать самостоятельно, приняв, что текущая дата 1.09.2012. Напомним, что необходимо установить эту дату в качестве текущей на виртуальном компьютере.

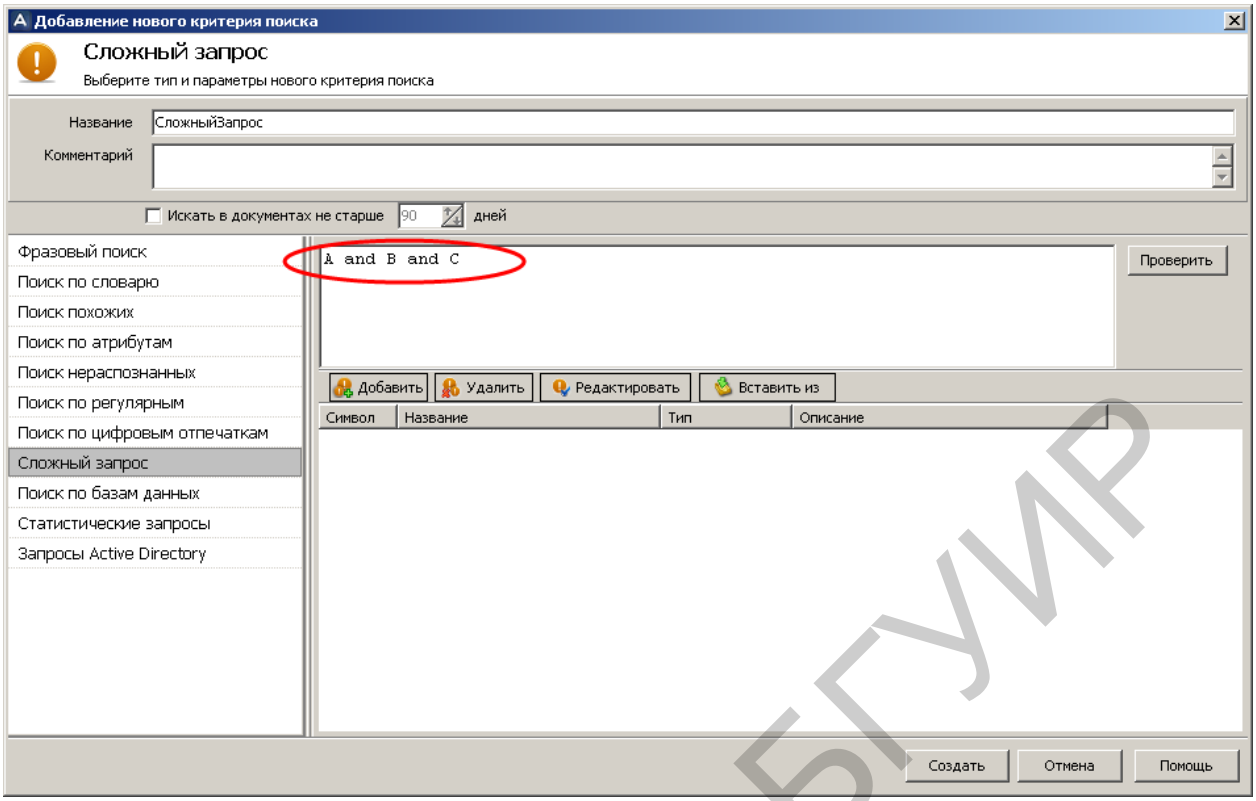


Рис. 4.36. Первый этап создания критерия «СложныйЗапрос»

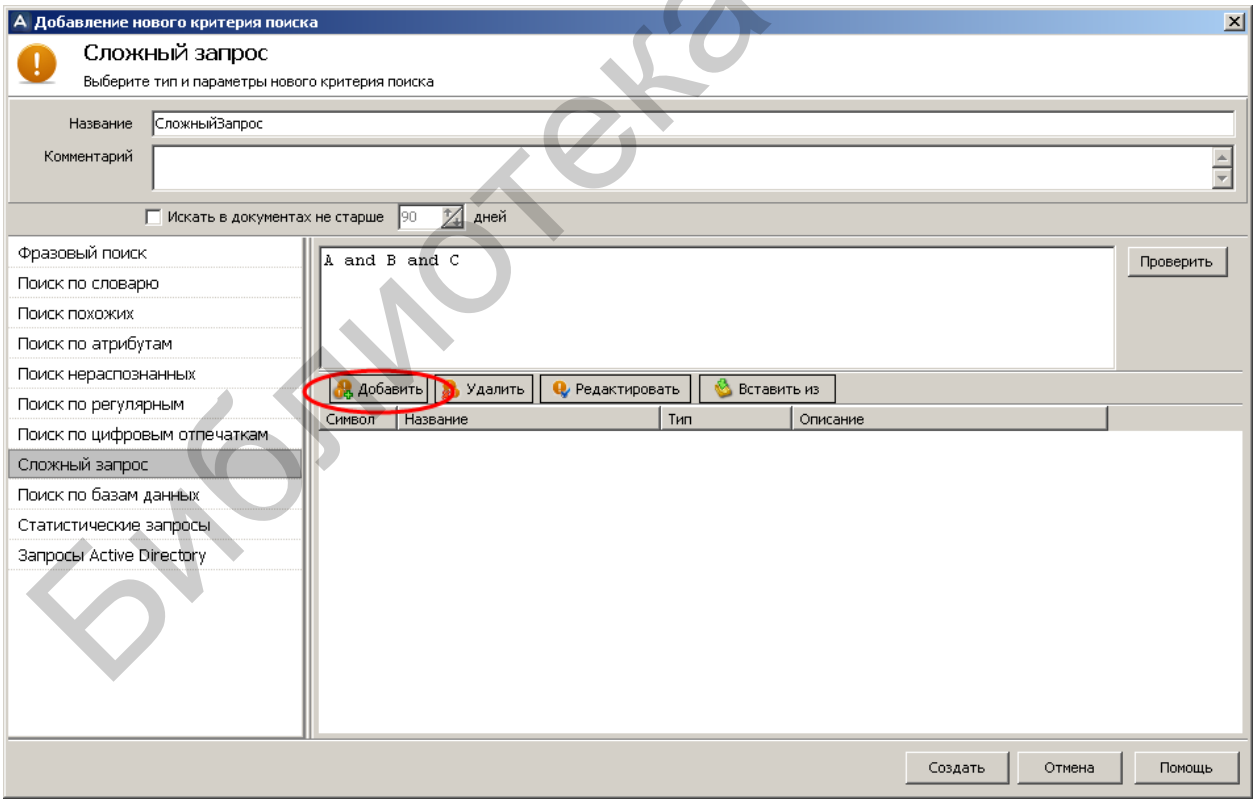


Рис. 4.37. Добавление критерия с псевдонимом A

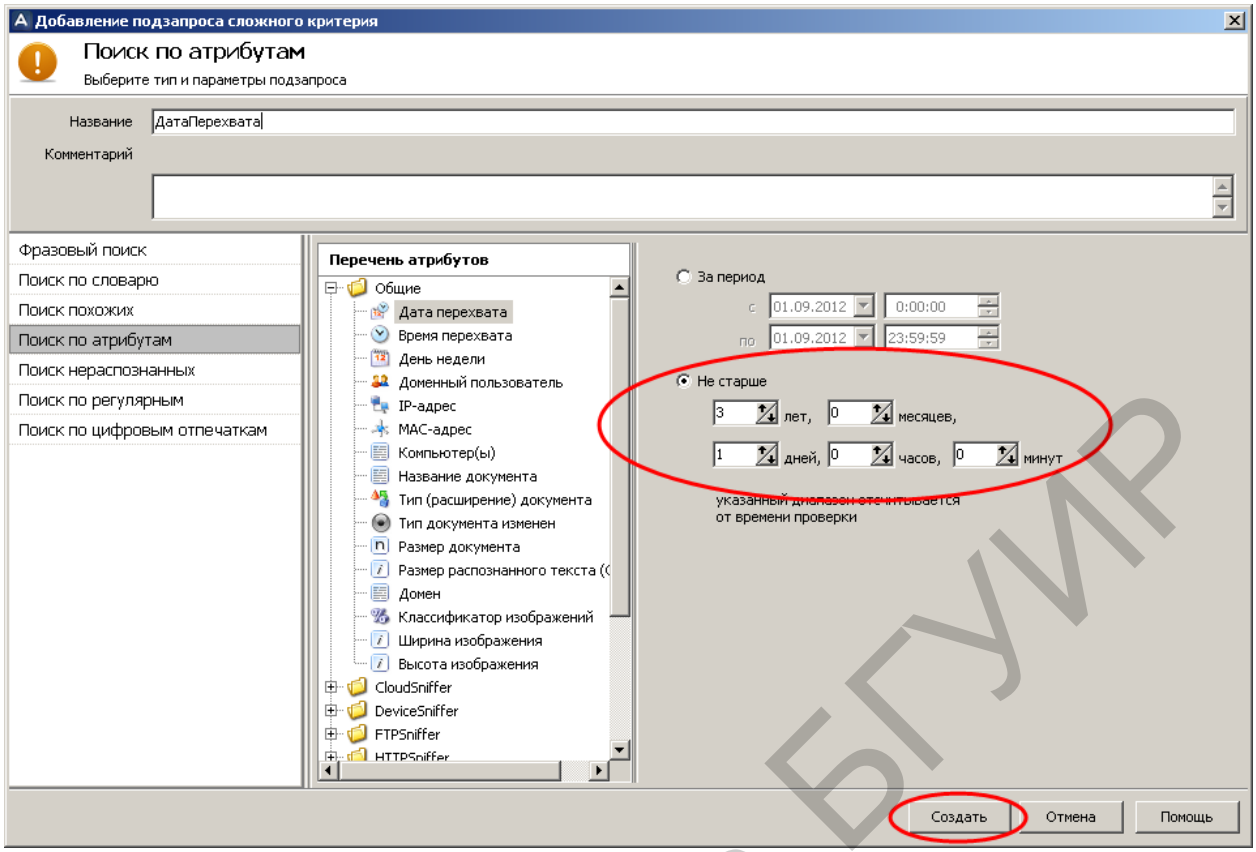


Рис. 4.38. Определение времени отправки письма

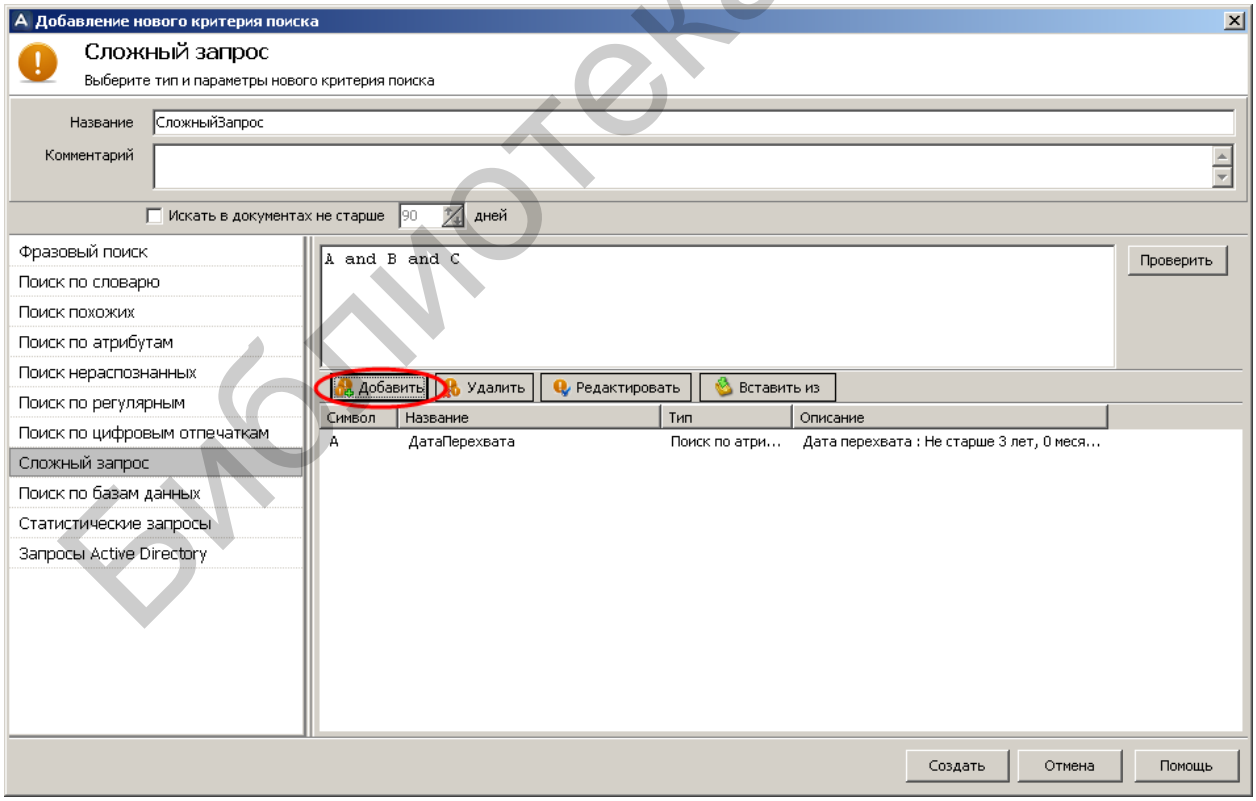


Рис. 4.39. Добавление критерия с псевдонимом B

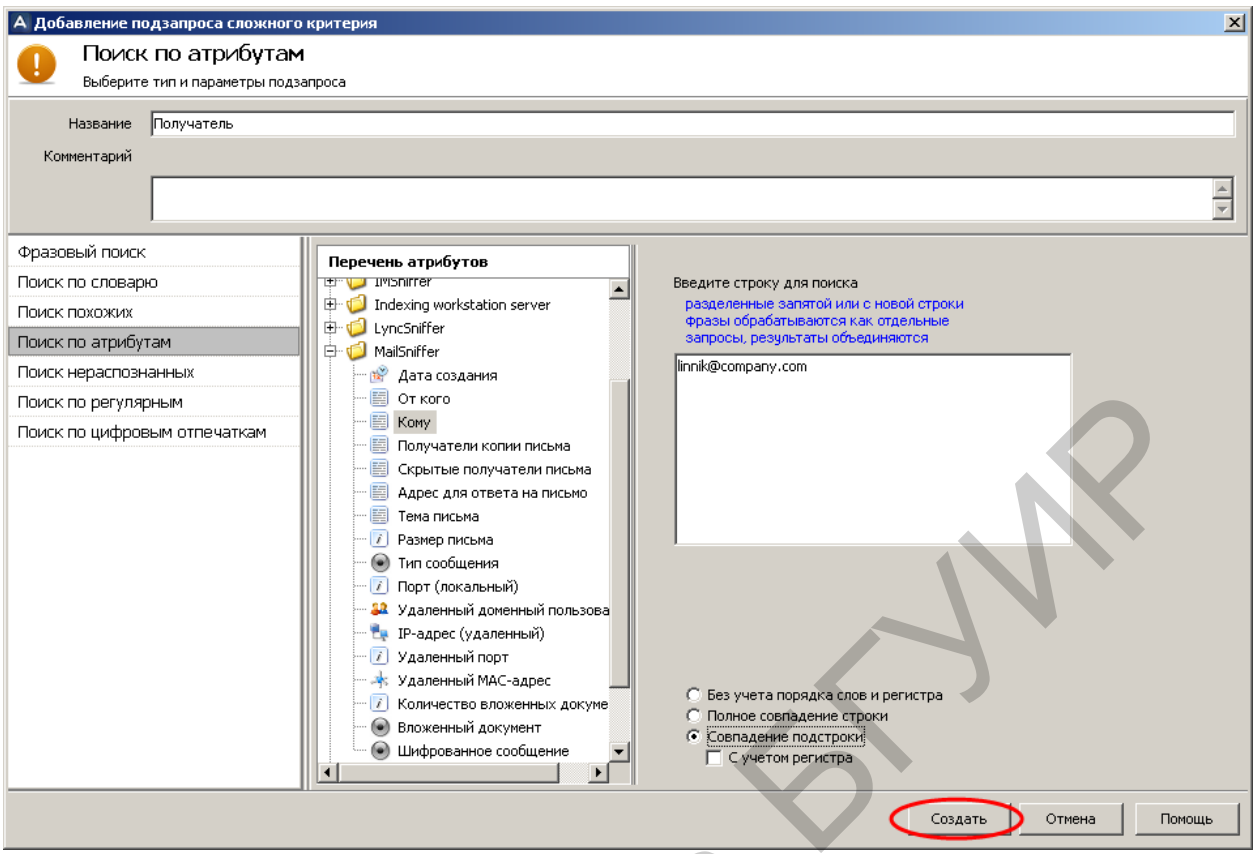


Рис. 4.40. Указание адреса получателя

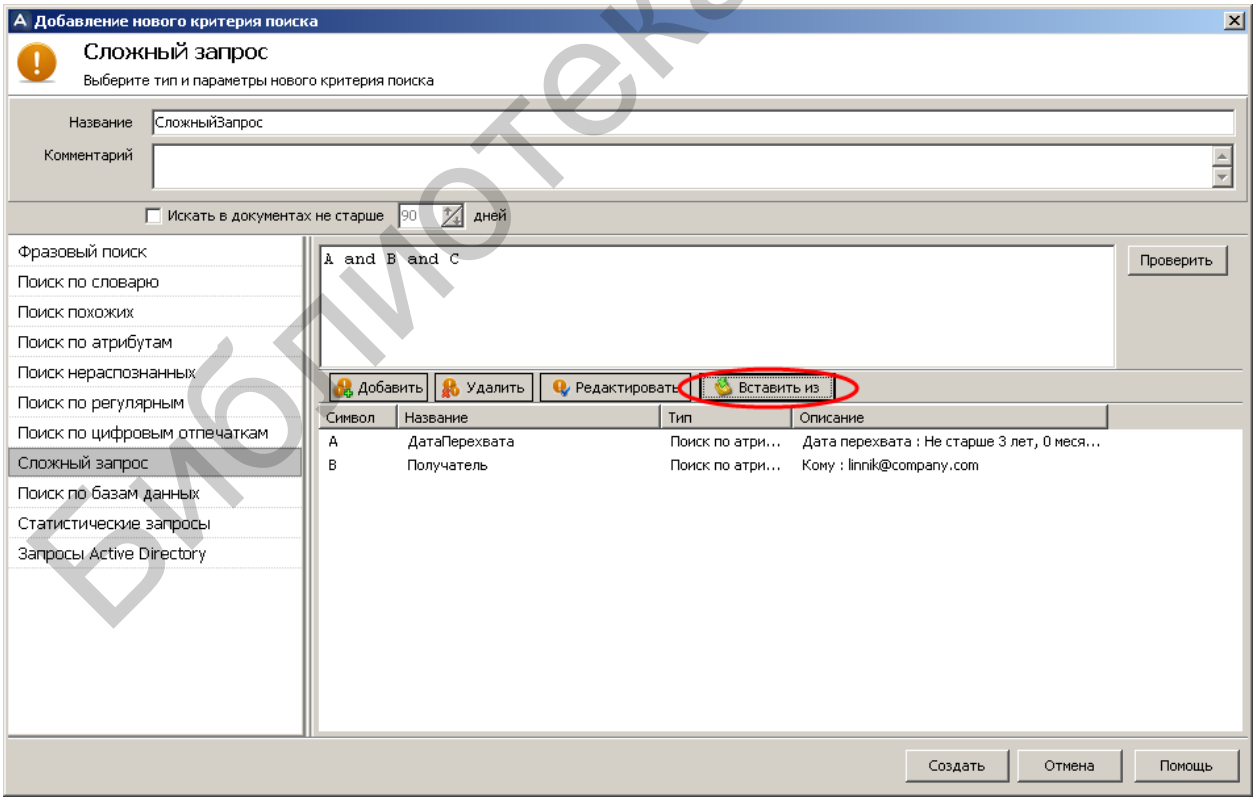


Рис. 4.41. Вход в режим вставки в сложный запрос готового критерия

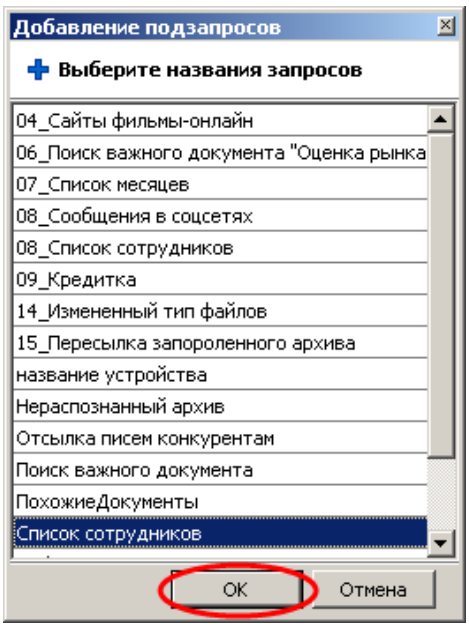


Рис. 4.42. Выбор критерия для вставки

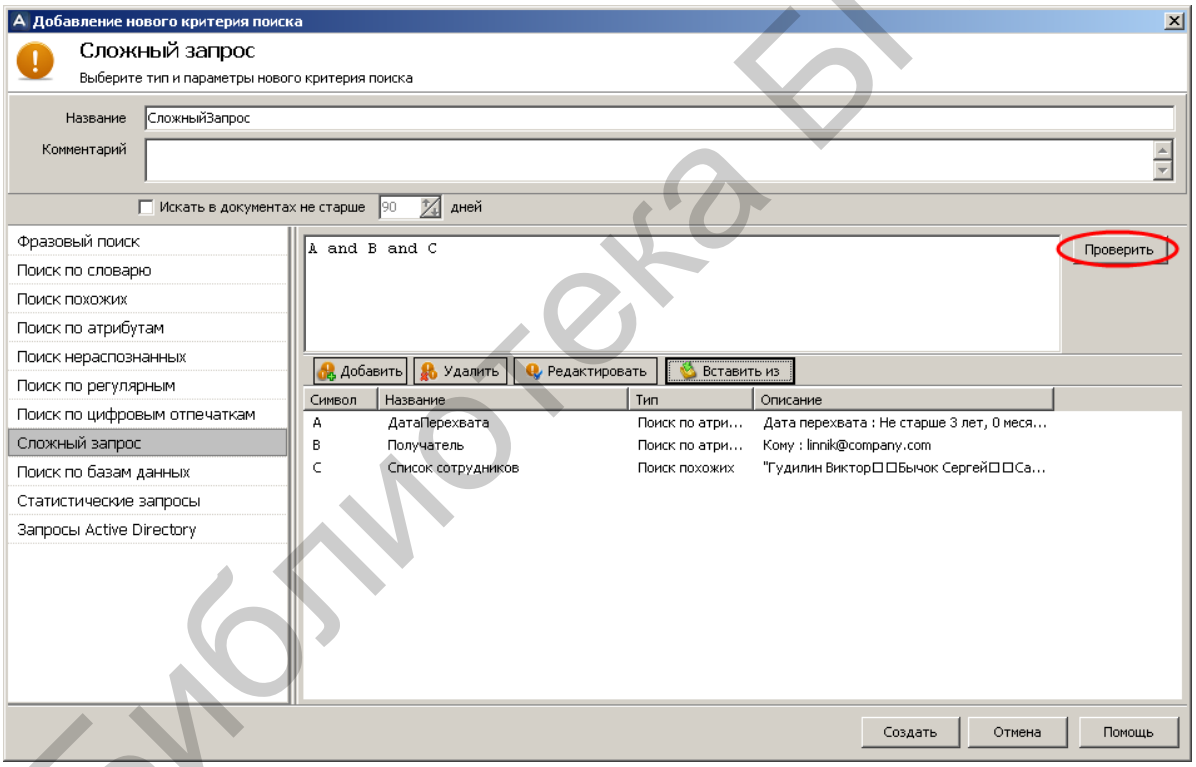


Рис. 4.43. Запуск проверки синтаксиса сложного запроса

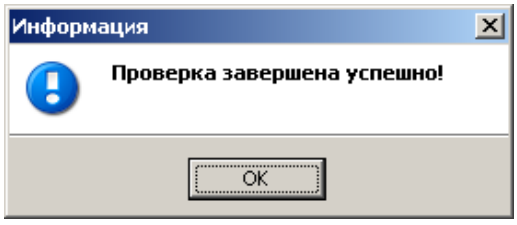


Рис. 4.44. Индикация успешной проверки

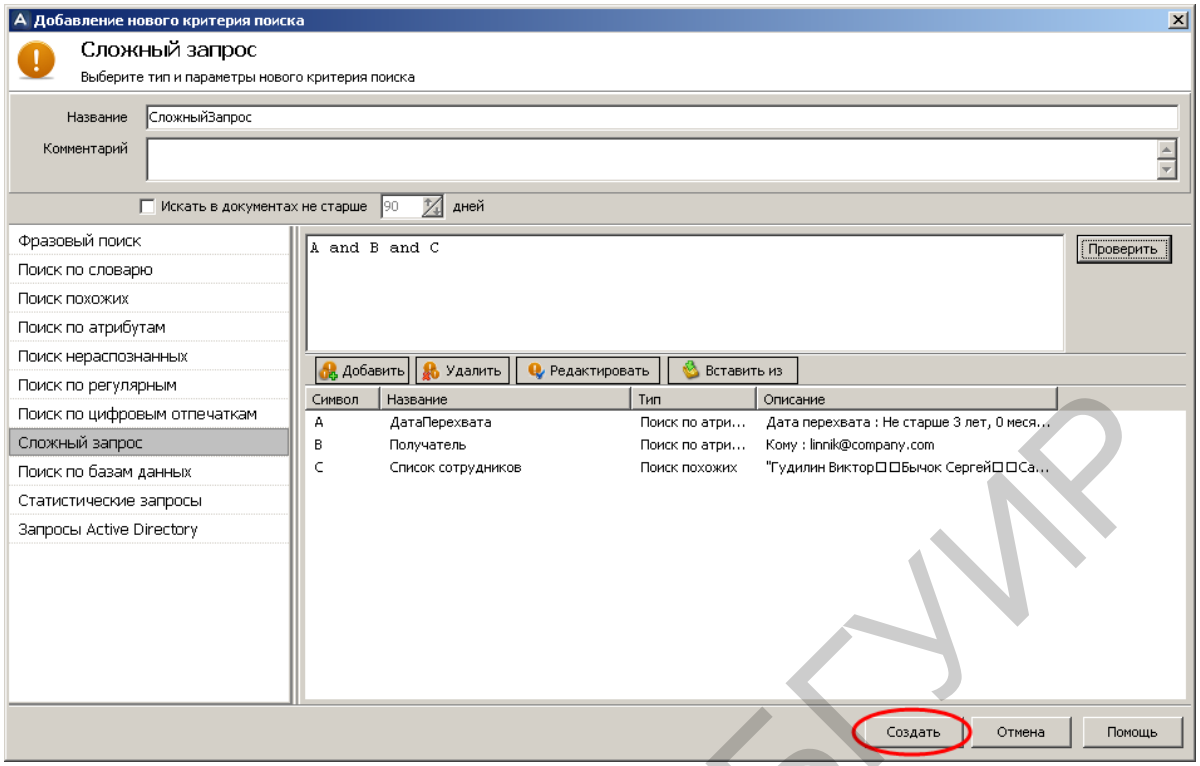


Рис. 4.45. Последний этап создания критерия «СложныйЗапрос»

Запустить принудительное выполнение критерия поиска «СложныйЗапрос» и убедиться в его результативности (см. рис. 4.46). Зафиксировать время выполнения поиска.

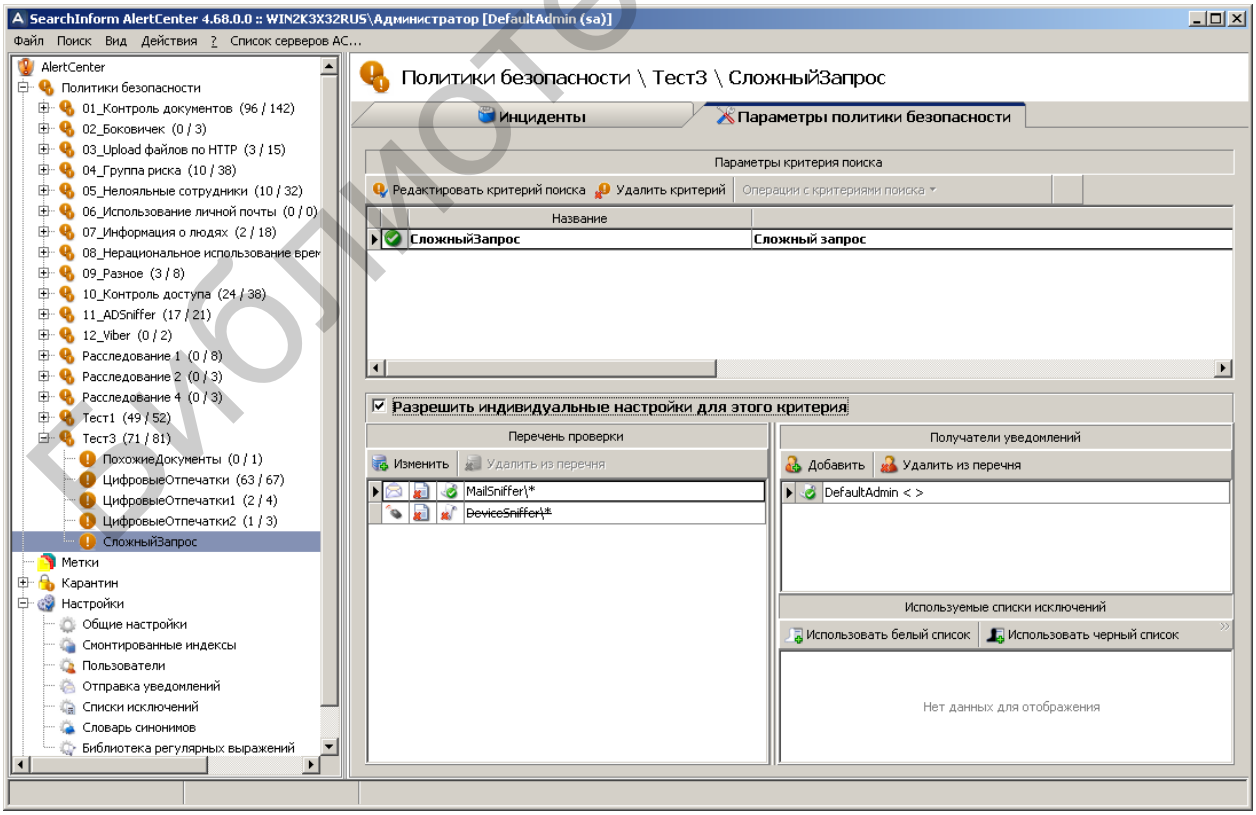


Рис. 4.46. Индикация критерия «СложныйЗапрос»

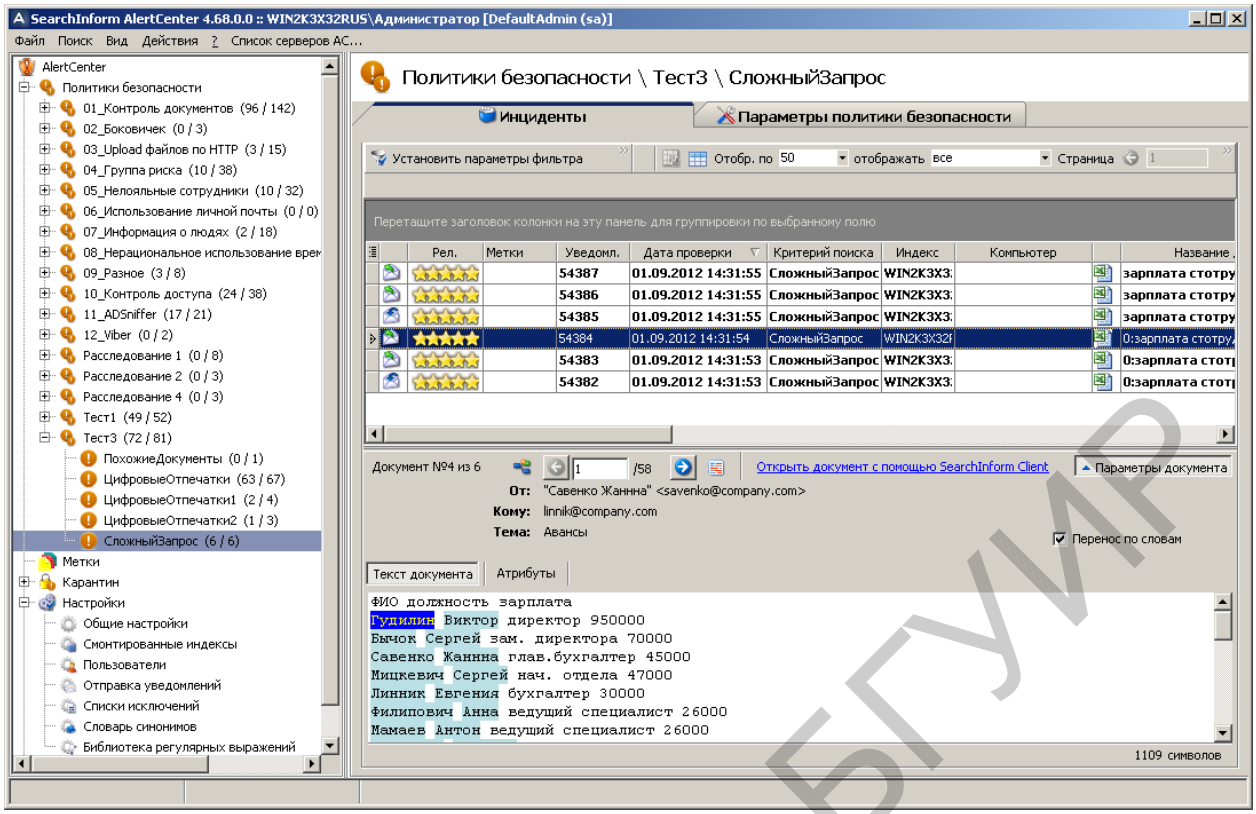


Рис. 4.47. Индикация инцидентов по критерию «СложныйЗапрос»

Определить запрос с максимальным/минимальным временем выполнения.
Закрыть окно AlertCenter Client.
Завершить работу с виртуальным компьютером.

4.3. Задание для самостоятельной работы

1. Использовав критерий «Поиск похожих», найти документ, заданный преподавателем.

2. Использовав критерий «По цифровым отпечаткам» и имеющиеся каталоги цифровых отпечатков, найти документ, заданный преподавателем.

3. Добавить в существующий каталог цифровых отпечатков новый образец и, использовав критерий «По цифровым отпечаткам», найти документ, соответствующий добавленному образцу.

4. Создать новый каталог цифровых отпечатков и, использовав критерий «По цифровым отпечаткам», найти некоторый документ, заданный преподавателем.

5. Использовав сложный запрос, состоящий из критерия поиска по атрибутам и критерия поиска по цифровым отпечаткам, найти электронные письма, отправленные с адреса «savenko@company.com», в котором содержится список сотрудников компании.

4.4. Контрольные вопросы

1. Влияют ли пробелы между словами в запросе на результаты поиска по критерию «Поиск похожих»?
2. Какие документы целесообразно искать с помощью критерия «Поиск похожих»?
3. Какие документы целесообразно искать с помощью критерия «По цифровым отпечаткам»?
4. Для чего применяется каталог образцов?
5. Что значит оператор and?
6. Что значит оператор or?
7. Что значит оператор not?
8. Как добавить новый отпечаток в существующий каталог образцов?
9. В чем разница между каталогом образцов и каталогом индексов?
10. Что такое стоп-слова?
11. Как снять цифровой отпечаток из текста в графическом файле?
12. Можно ли снять цифровой отпечаток из pdf-файла?
13. Можно ли снять цифровой отпечаток из java-файла?
14. Какие документы нецелесообразно искать с помощью критерия «По цифровым отпечаткам»?
15. Как объединяются простые запросы в сложные?
16. Как проверить синтаксис сложного запроса?

ЛАБОРАТОРНАЯ РАБОТА №5
НАСТРОЙКА ПРОГРАММНОГО КОМПЛЕКСА SEARCHINFORM ДЛЯ ПОИСКА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОСНОВЕ ПОДОБИЯ ТЕКСТОВЫХ ФРАГМЕНТОВ. ЧАСТЬ 2

Цель: освоить основные приемы формирования поисковых запросов конфиденциальной информации на основе подобия текстовых фрагментов.

5.1. Теоретическая часть

1. Ознакомиться с разделами 1–5 руководства аудитора безопасности системы SearchInform.
2. Ознакомиться со справочными материалами AlertCenter Client.

5.2. Лабораторное задание

В соответствии с методическими указаниями лабораторной работы №1 запустить виртуальный компьютер с установленным программным комплексом SearchInform. Выполнить задания лабораторных работ №2–4. В дальнейшем предусматривается, что студент освоил методику настроек SearchInform в объеме предыдущих лабораторных работ.

Убедиться в том, что сервер AlertCenter работает, в противном случае его следует запустить с помощью консоли SearchInform AlertCenter Console.

Открыть окно AlertCenter Client. В соответствии с методическими указаниями лабораторной работы №2 создать новую политику безопасности с названием «Тест4». Включить в политику только поисковые индексы DeviceSniffer и MailSniffer. Получать уведомления должен пользователь DefaultAdmin. Окно политики показано на рис. 5.1.

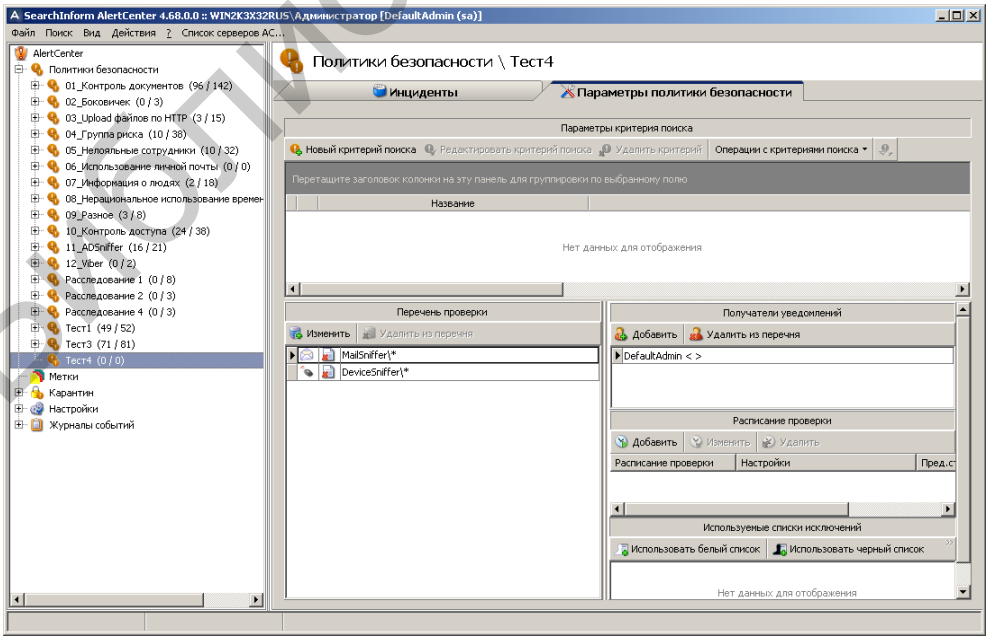


Рис. 5.1. Окно политики безопасности «Тест4»

Формирование критерия «Фразовый поиск»

Формирование данного критерия рассмотрим на примере поиска в перехваченных документах информации, касающейся Республики Бурятия.

В соответствии с рис. 5.2 создать критерий, предусматривающий точное совпадение хотя бы одного слова поискового запроса с одним из слов перехваченного документа.

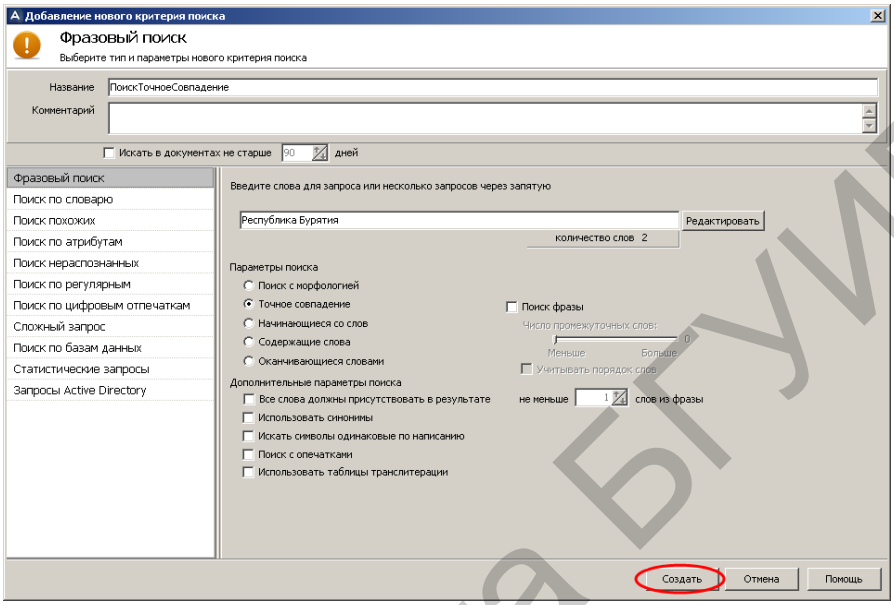


Рис. 5.2. Создание критерия «ПоискТочноеСовпадение»

Запустить принудительное выполнение критерия поиска «ПоискТочноеСовпадение» и убедиться в его результативности (рис. 5.3). Определить сколько целевых и сколько нецелевых документов содержится в результатах поиска.

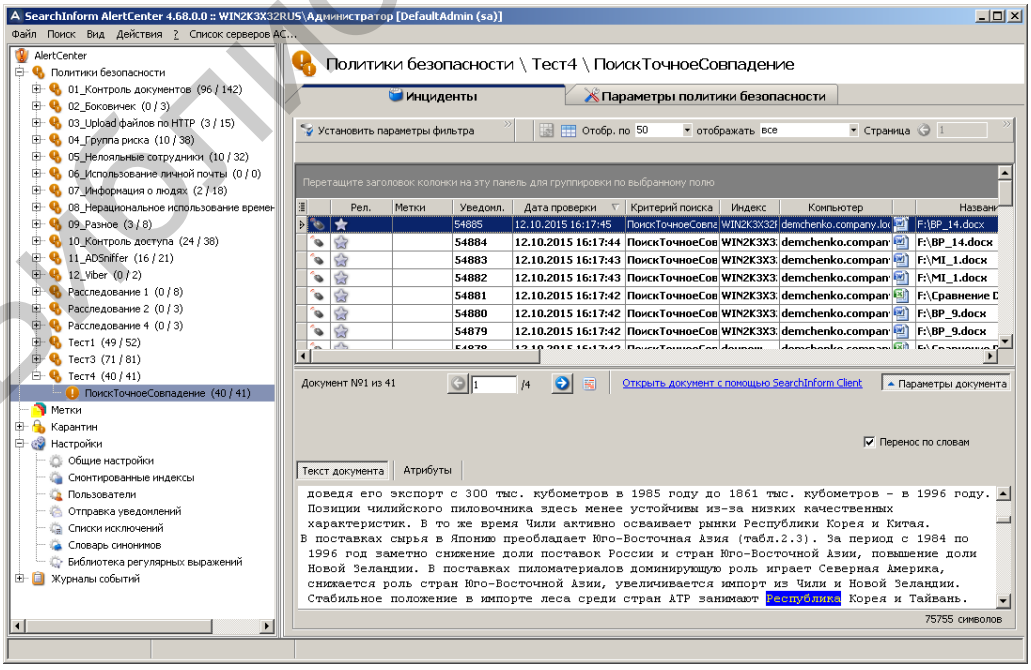


Рис. 5.3. Индикация инцидентов по критерию «ПоискТочноеСовпадение»

Уточнить результаты поиска за счет того, что в найденном документе должны присутствовать все слова запроса. Для этого следует создать новый критерий поиска «ПоискТочноеСовпадениеВсеСлова», окно которого показано на рис. 5.4.

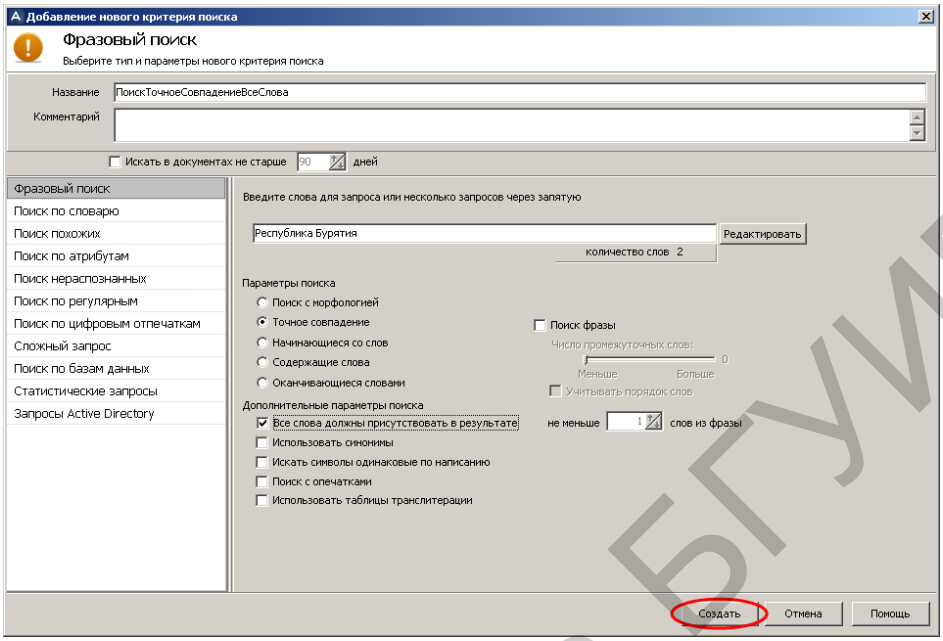


Рис. 5.4. Создание критерия «ПоискТочноеСовпадениеВсеСлова»

Запустить принудительное выполнение критерия поиска «ПоискТочное-СовпадениеВсеСлова» и убедиться в его результативности (рис. 5.5). Отметим, что количество найденных документов сократилось в 10 раз.

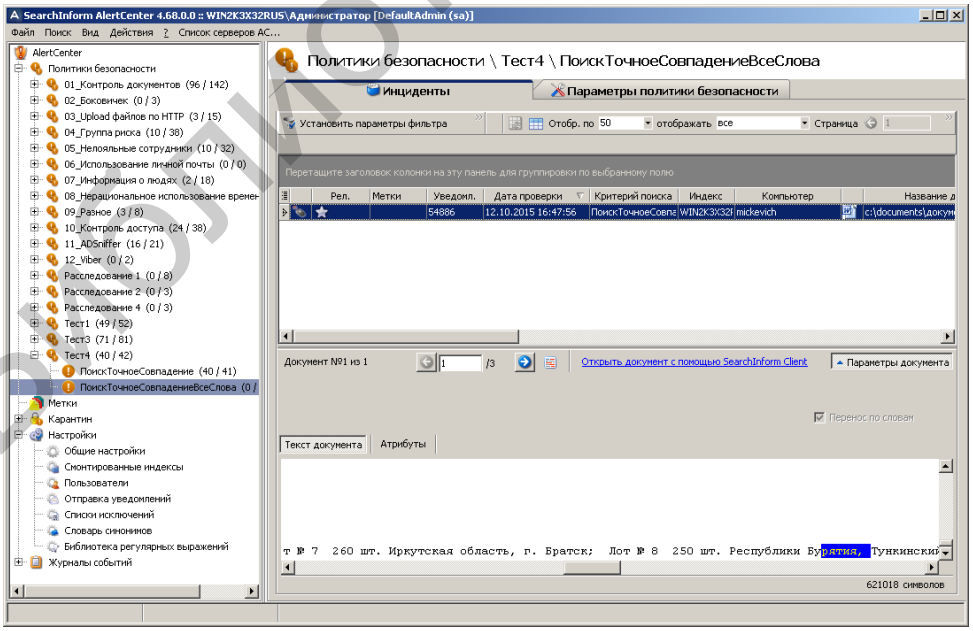


Рис. 5.5. Индикация инцидентов по критерию «ПоискТочноеСовпадениеВсеСлова»

Расширить поиск за счет изменения опции «Точное совпадение» на «Поиск с морфологией». Для этого создадим новый, показанный на рис. 5.6, критерий «ПоискМорфология».

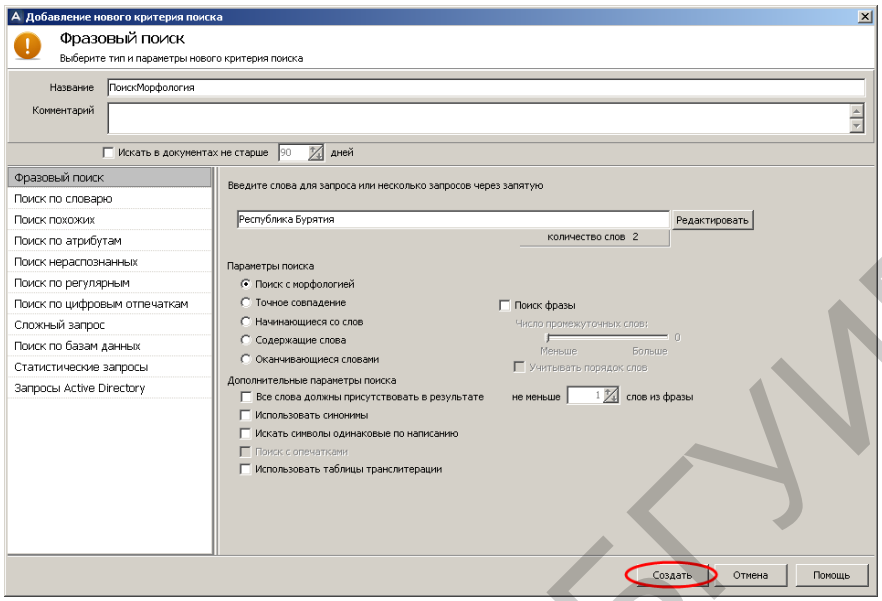


Рис. 5.6. Создание критерия «ПоискМорфология»

Запустить принудительное выполнение критерия поиска «ПоискМорфология» и убедиться в его результативности (рис. 5.7). Отметим, что количество найденных документов выросло до 77.

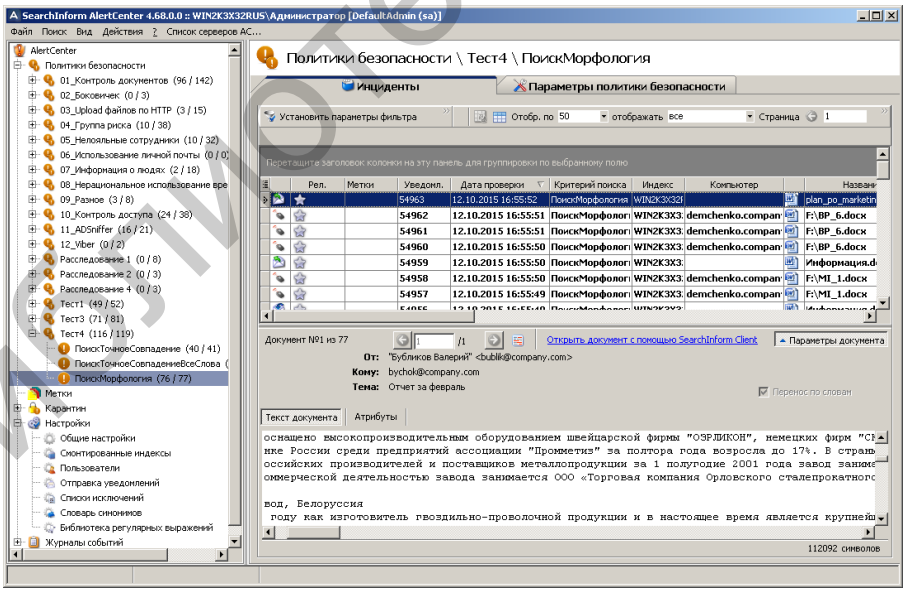


Рис. 5.7. Индикация инцидентов по критерию «ПоискМорфология»

Исследуем, как изменятся результаты поиска, за счет того что в найденном документе должны присутствовать все слова запроса. Для этого следует создать новый критерий поиска «ПоискМорфологияВсеСлова», окно которого показано на рис. 5.8.

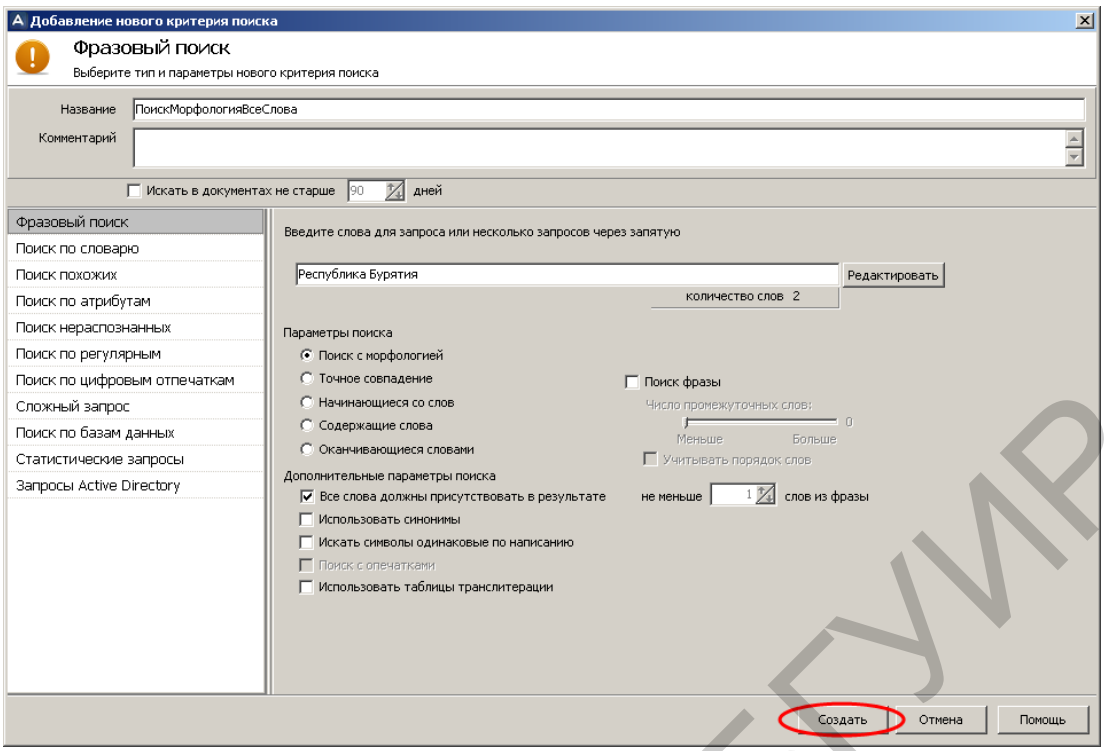


Рис. 5.8. Создание критерия «ПоискМорфологияВсеСлова»

Запустить принудительное выполнение критерия поиска «ПоискМорфологияВсеСлова» и убедиться в его результативности (рис. 5.9). Отметим, что количество найденных документов уменьшилось с 77 до 5.

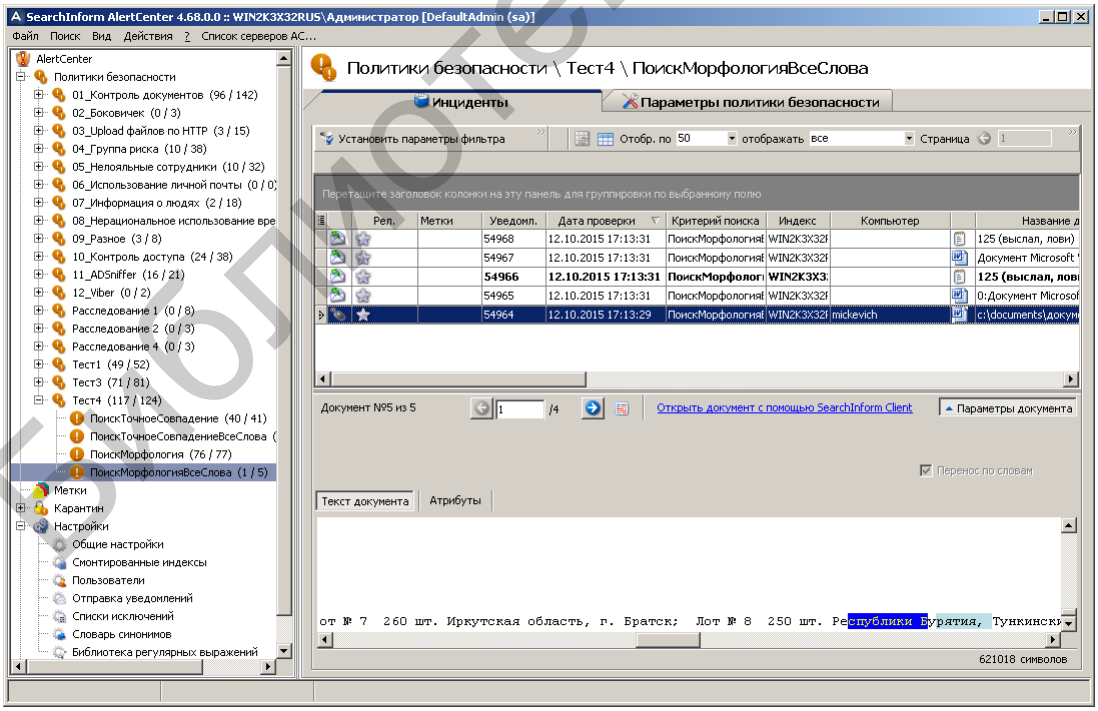


Рис. 5.9. Индикация инцидентов по критерию «ПоискМорфологияВсеСлова»

Уточнить результаты поиска за счет того, что в найденных документах могут быть искомые слова, в которых использованы совпадающие по написанию буквы

русского и латинского алфавитов. Для этого создадим новый, показанный на рис. 5.10, критерий поиска «ПоискМорфологияВсеСловаОдинаковыеСимволы».

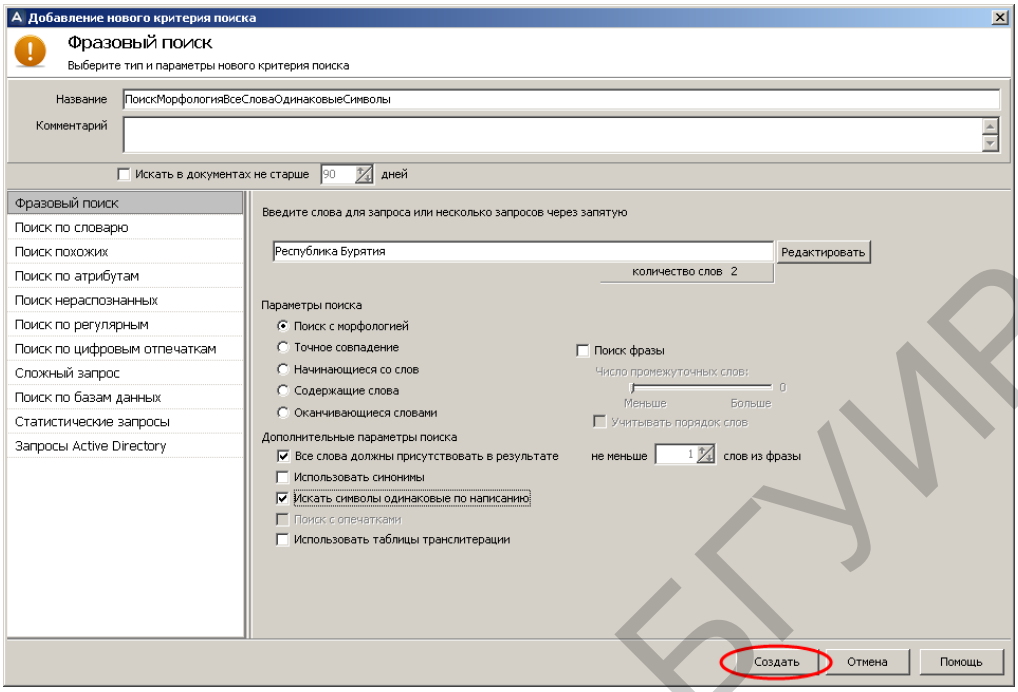


Рис. 5.10. Создание критерия «ПоискМорфологияВсеСловаОдинаковыеСимволы»

Запустить принудительное выполнение критерия поиска «ПоискМорфологияВсеСловаОдинаковыеСимволы» и убедиться в его результативности (рис. 5.11).

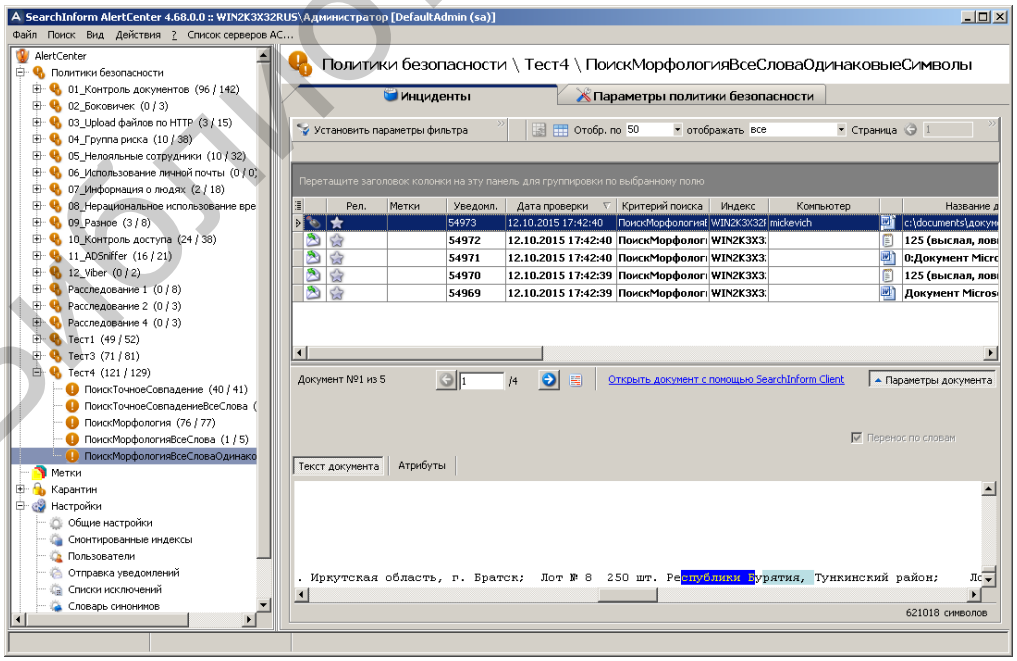


Рис. 5.11. Индикация инцидентов по критерию «ПоискМорфологияВсеСловаОдинаковыеСимволы»

Уточнить результаты поиска за счет того, что в искомых документах могут быть как одинаковые символы, так и опечатки. Кроме этого, в искомом документе должны быть все слова запроса. Для этого следует создать новый, показанный на рис. 5.12, критерий поиска «ПоискТочноеСовпадение1».

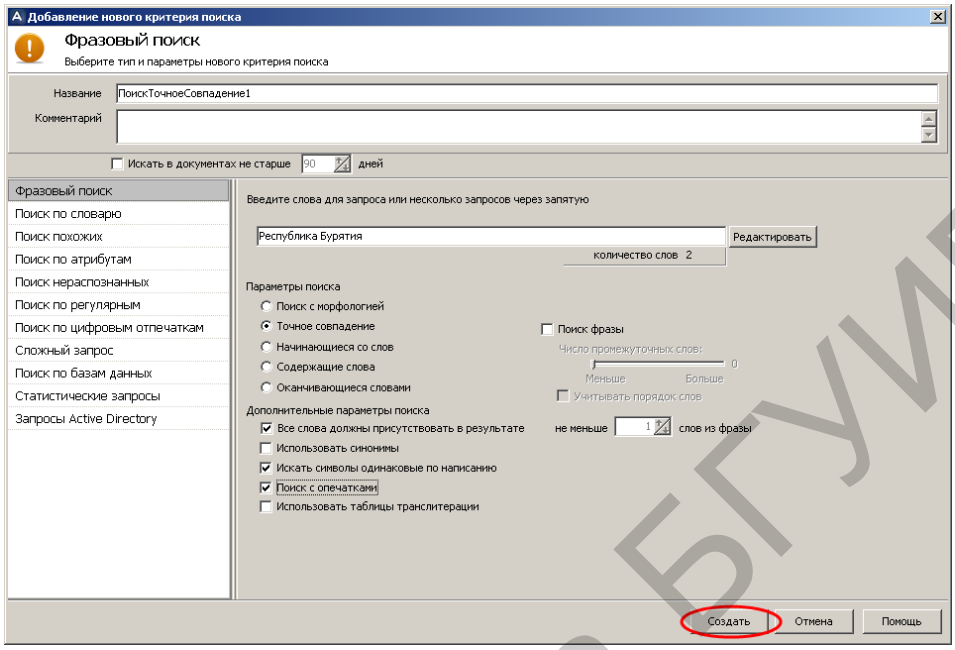


Рис. 5.12. Создание критерия «ПоискТочноеСовпадение1»

Запустить принудительное выполнение критерия поиска «ПоискТочноеСовпадение1» и убедиться в его результативности (рис. 5.13). Определить сколько целевых и нецелевых документов содержится в результатах поиска. Сравнить результаты запросов «ПоискТочноеСовпадение1» и «ПоискТочноеСовпадениеВсеСлова».

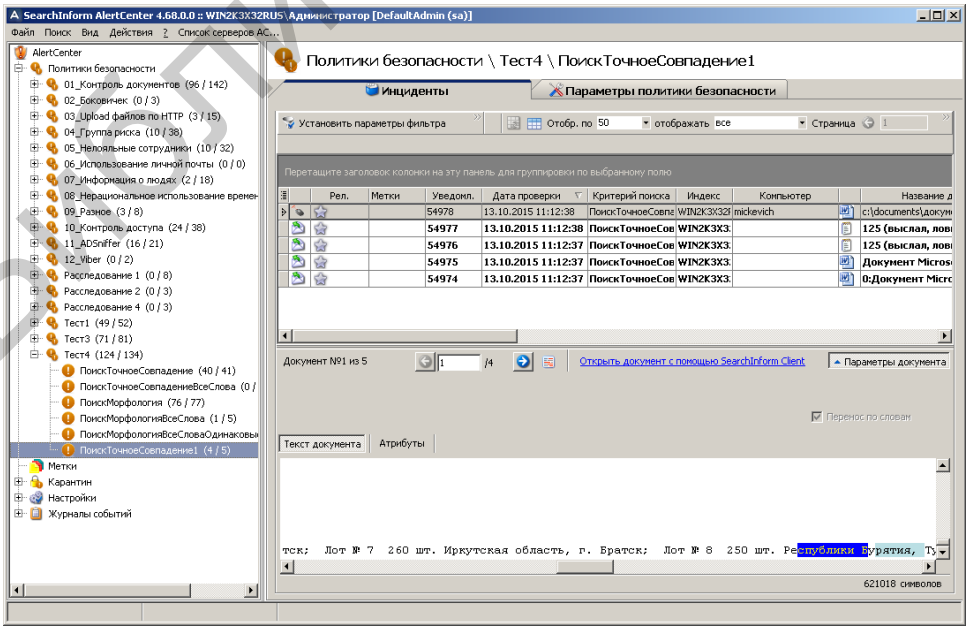


Рис. 5.13. Индикация инцидентов по критерию «ПоискТочноеСовпадение1»

Уточнить результаты поиска за счет замены опции «Точное совпадение» на опцию «Содержащие слова». Для этого создадим новый критерий поиска «ПоискСодержащиеСлова», окно которого показано на рис. 5.14.

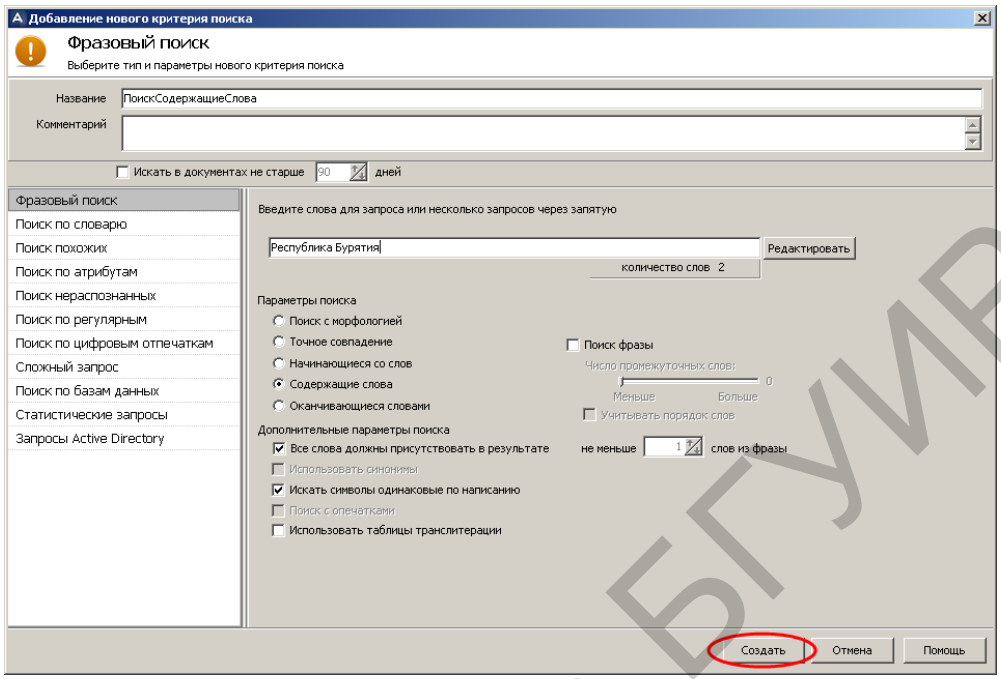


Рис. 5.14. Создание критерия «ПоискСодержащиеСлова»

Запустить принудительное выполнение критерия поиска «ПоискСодержащиеСлова» и убедиться в его результативности (рис. 5.15).

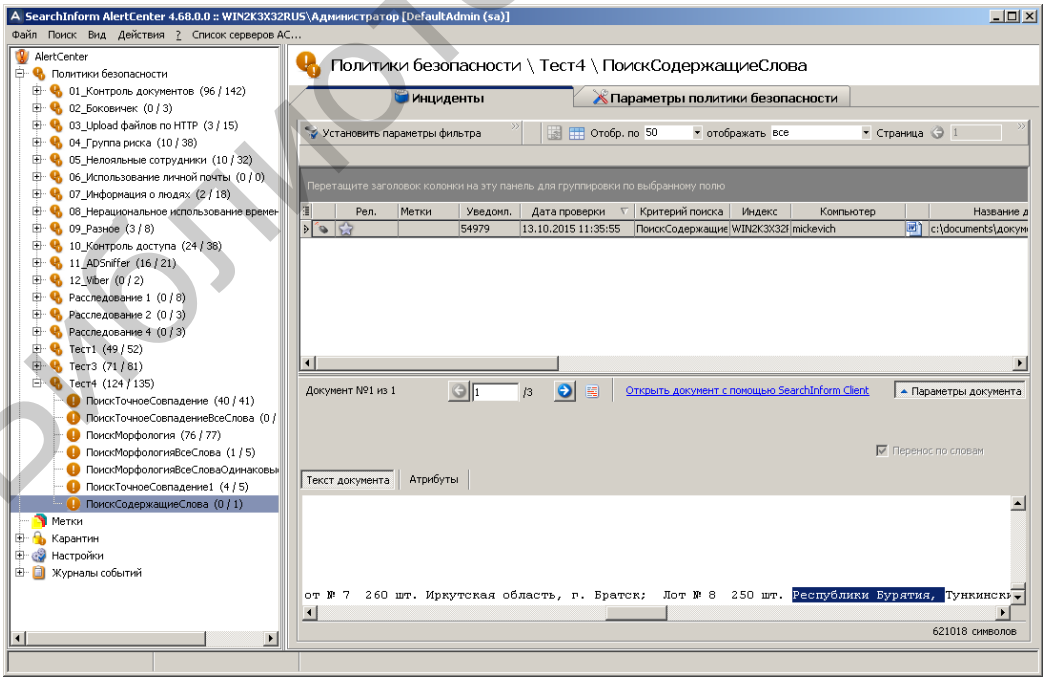


Рис. 5.15. Индикация инцидентов по критерию «ПоискСодержащиеСлова»

Исследовать результативность поиска за счет того, что в искомых документах могут присутствовать синонимы слов запроса. Для этого создадим новый критерий поиска «ПоискМорфологияСинонимы», окно которого показано на рис. 5.16.

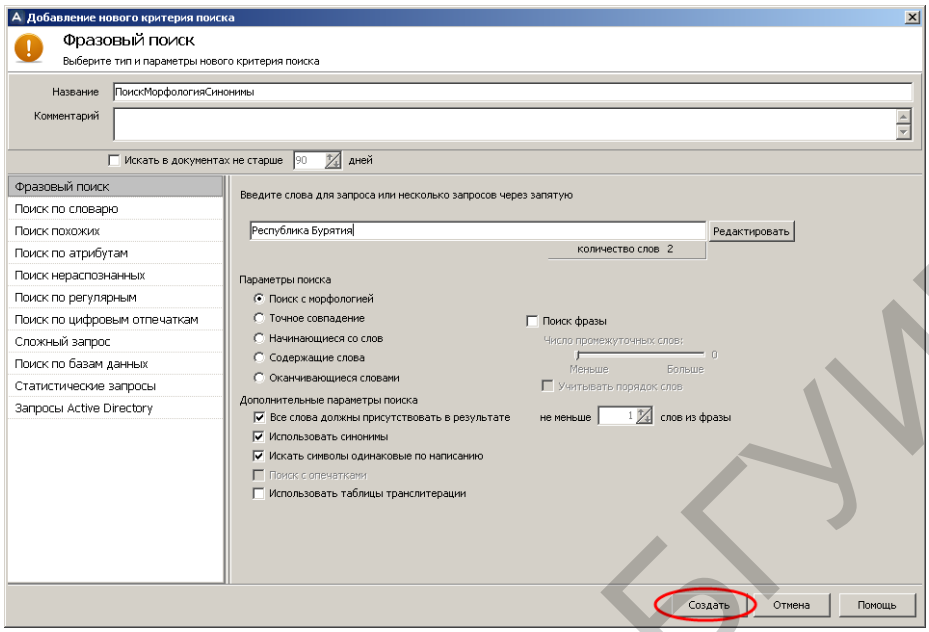


Рис. 5.16. Создание критерия «ПоискМорфологияСинонимы»

Запустить принудительное выполнение критерия поиска «ПоискМорфологияСинонимыОпечатки» и убедиться в его результативности (рис. 5.17). Определить сколько целевых и нецелевых документов содержится в результатах поиска. Кроме этого, следует определить, насколько изменились результаты относительно подобных, но не использующих синонимов критериев «ПоискМорфологияВсеСловаОдинаковыеСимволы» и «ПоискСодержащиеСлова».

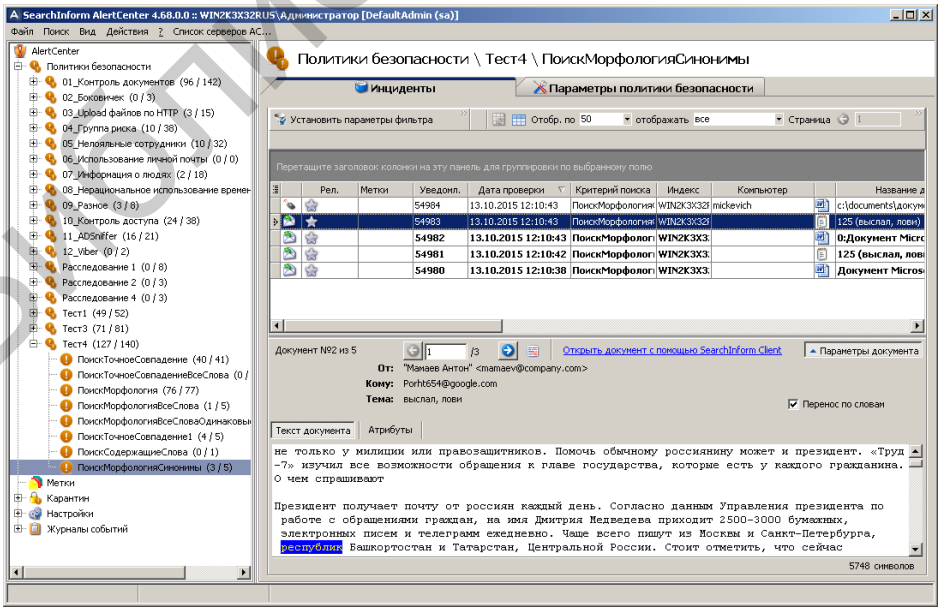


Рис. 5.17. Индикация инцидентов по критерию «ПоискМорфологияСинонимыОпечатки»

В соответствии с рис. 5.18 и 5.19 определим наличие в словаре синонимов используемого в запросе слова «республика».

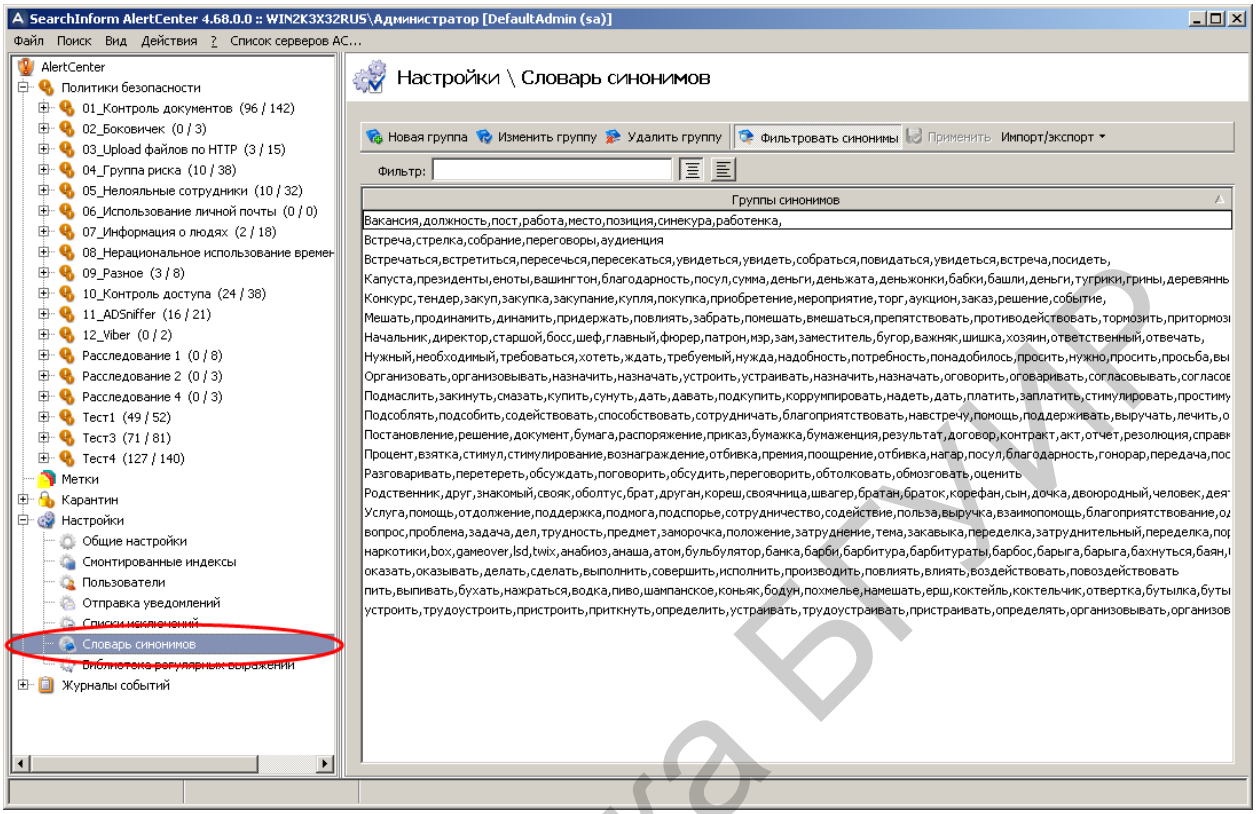


Рис. 5.18. Переход к просмотру словаря синонимов

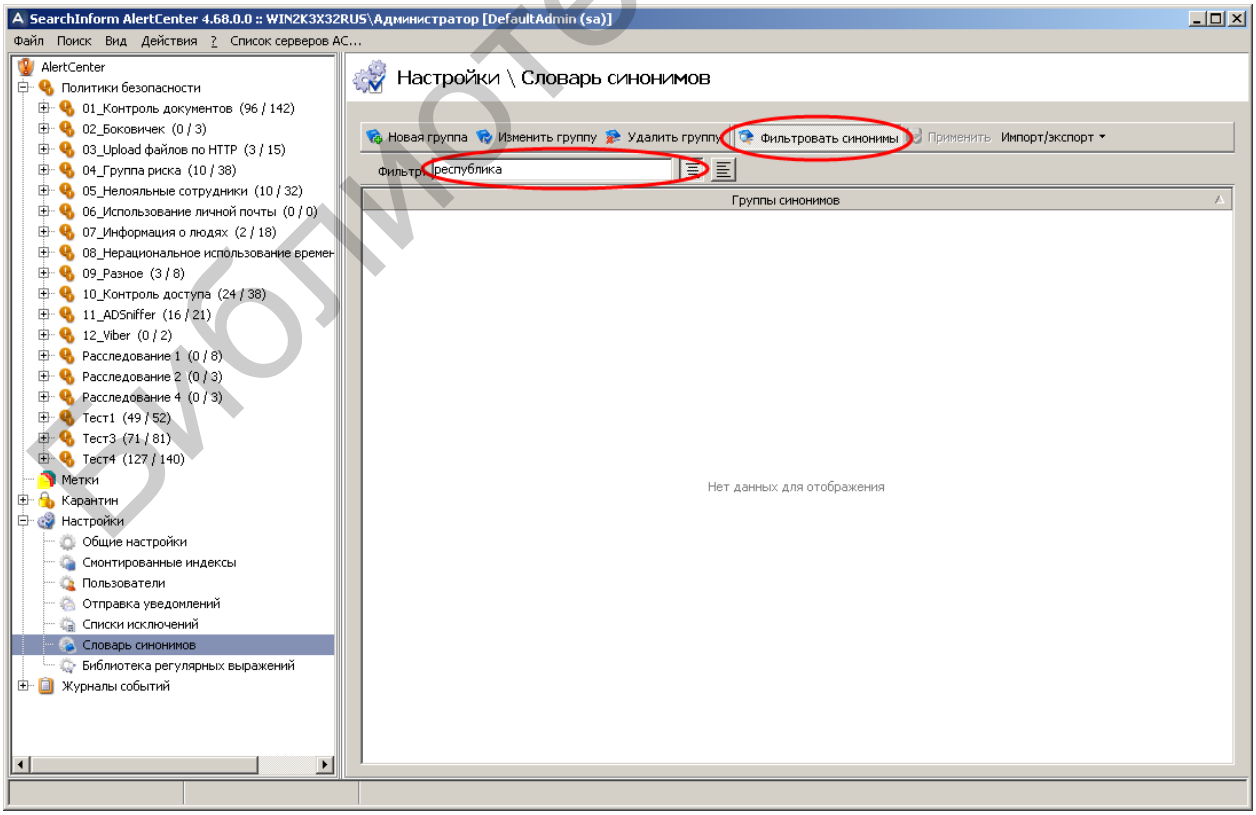


Рис. 5.19. Поиск в словаре синонимов слова «республика»

В соответствии с рис. 5.20–5.23 добавить в словарь такие синонимы слова «республика», как «государство», «держава», «страна».

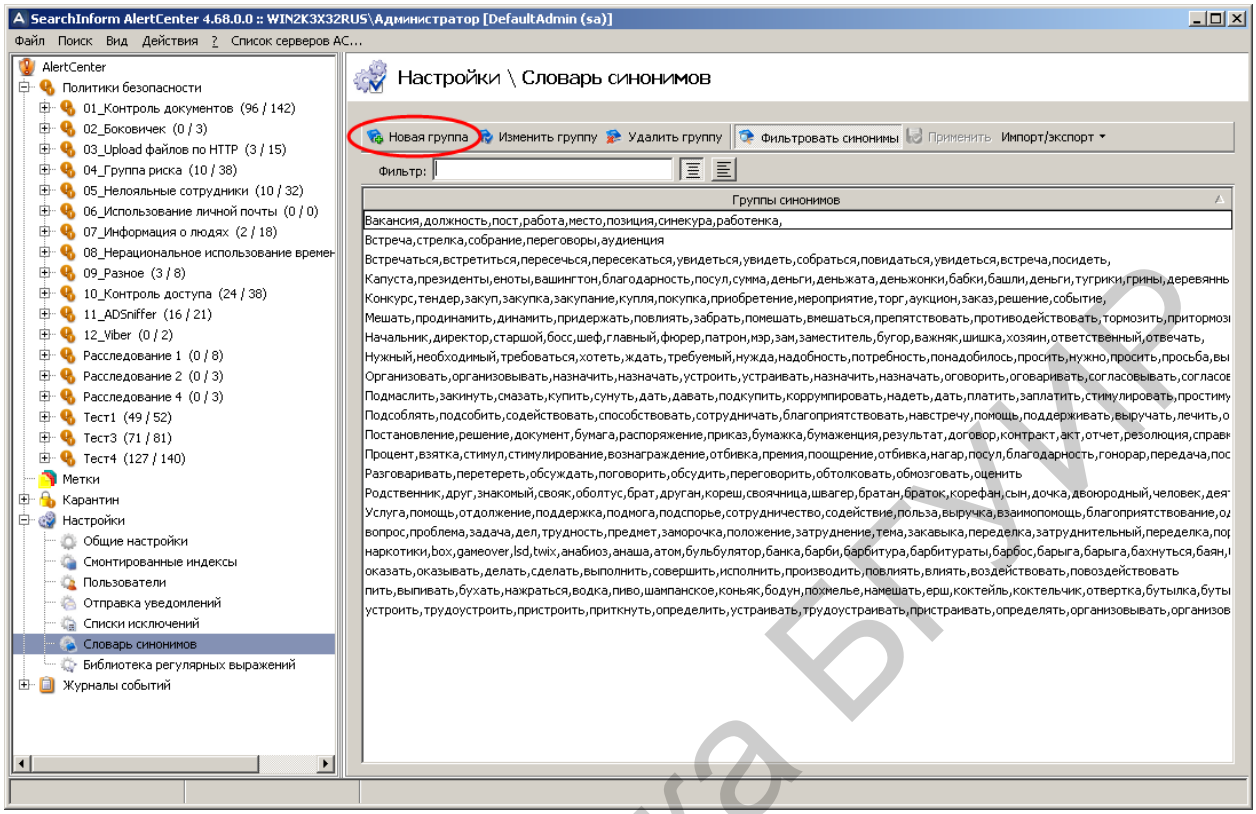


Рис. 5.20. Создание новой группы синонимов

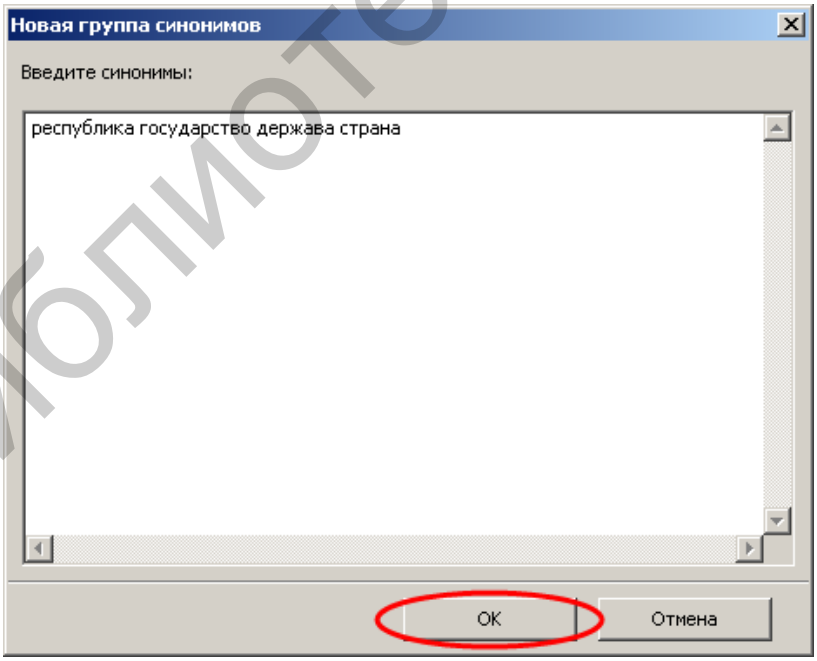


Рис. 5.21. Ввод слов-синонимов

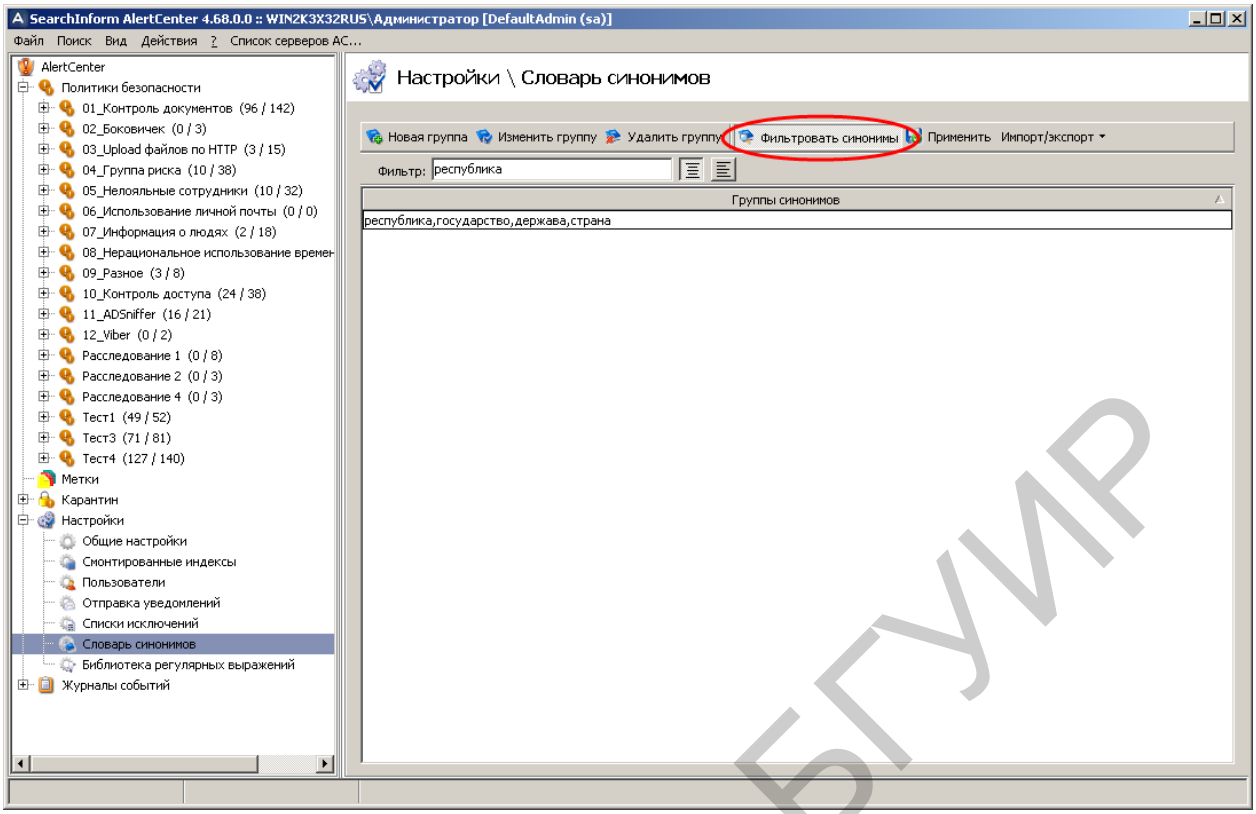


Рис. 5.22. Просмотр синонимов

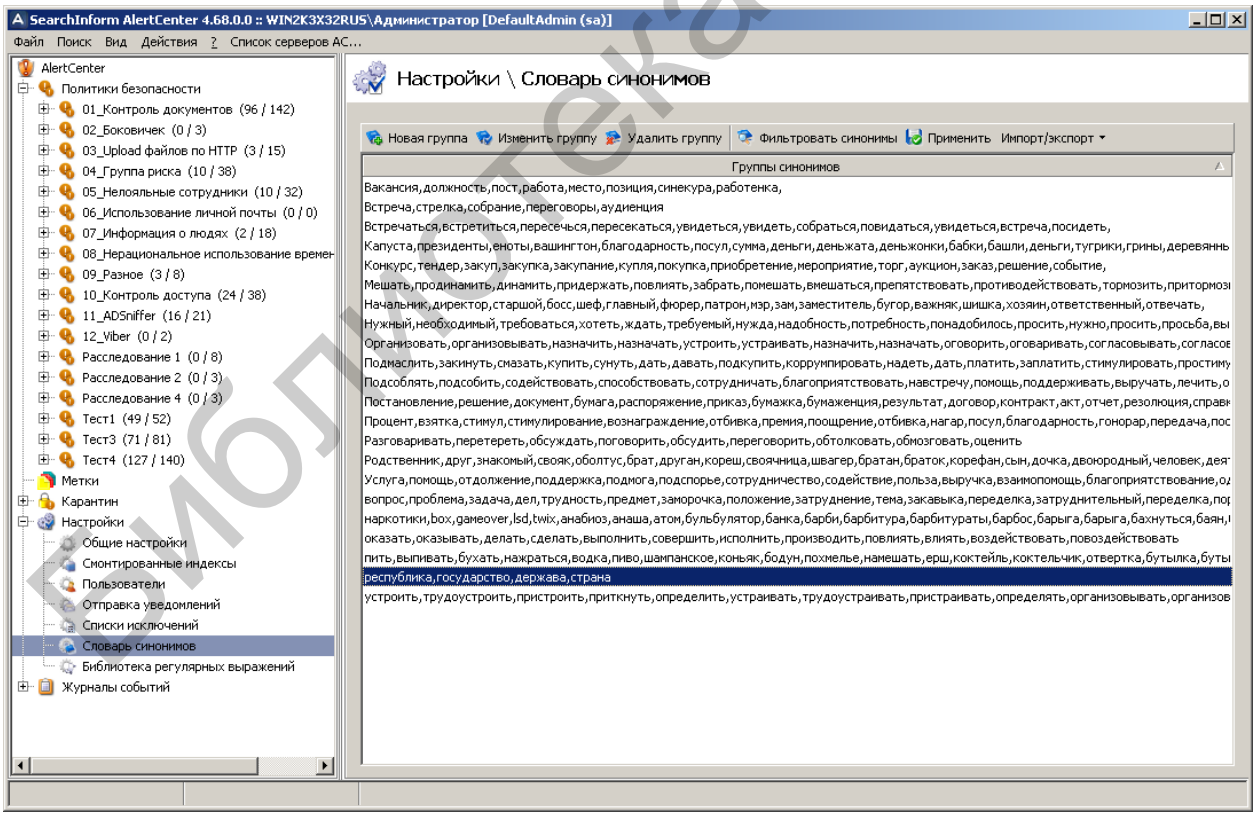


Рис. 5.23. Дополненный словарь синонимов

Рассмотреть изменения результатов поиска с применением синонимов за счет дополнения словаря синонимов. Для этого создать два новых критерия по-

иска «ПоискМорфологияСинонимыПлюс» и «ПоискМорфологияСинонимы-ПлюсВсеСлова», окна которых показаны на рис. 5.24, 5.25.

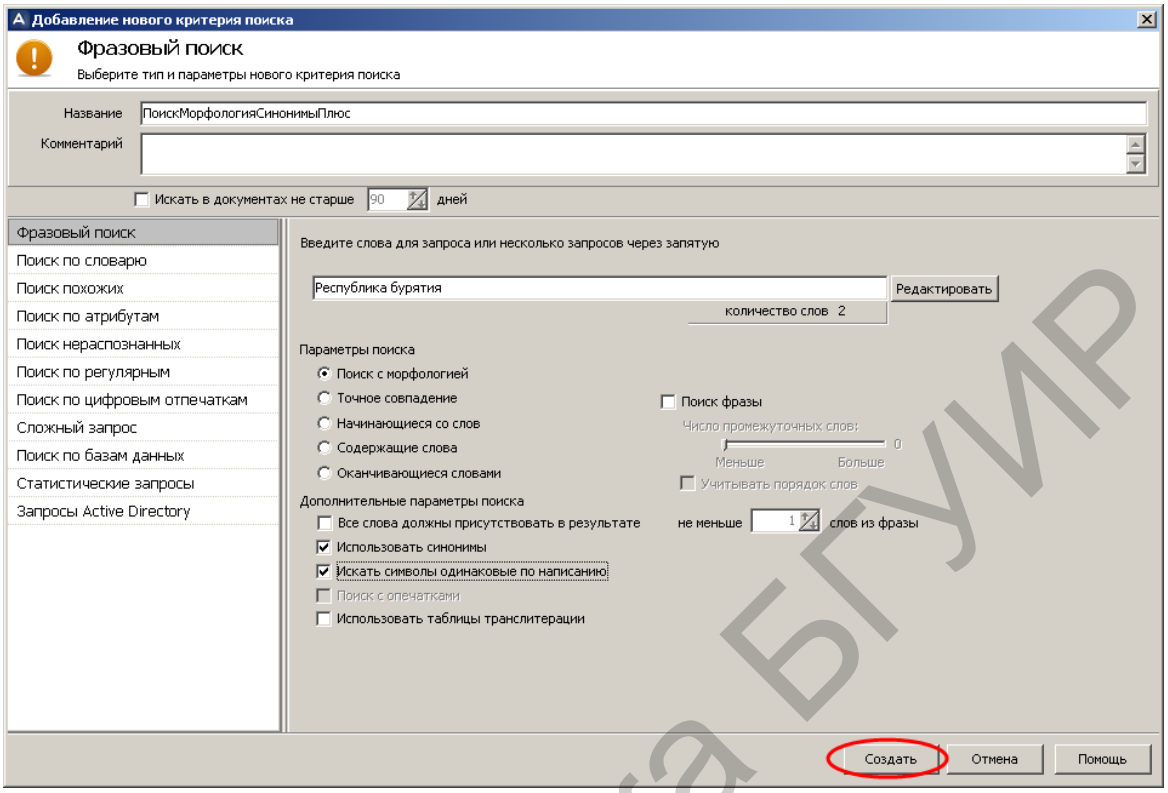


Рис. 5.24. Создание критерия «ПоискМорфологияСинонимыПлюс»

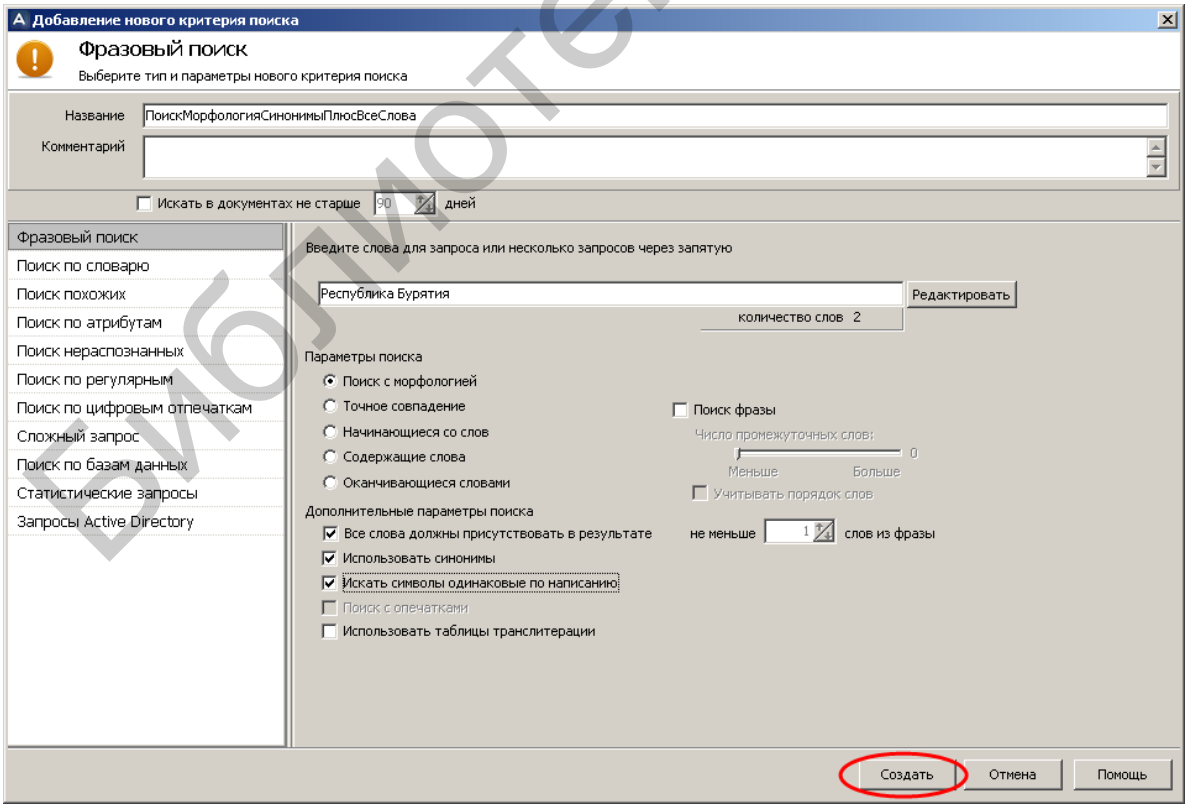


Рис. 5.25. Создание критерия «ПоискМорфологияСинонимыПлюсВсеСлова»

Запустить принудительное выполнение критериев поиска «ПоискМорфологияСинонимыПлюс» и «ПоискМорфологияСинонимыПлюсВсеСлова» и убедиться в их результативности (рис. 5.26, 5.27). Определить, сколько целевых и нецелевых документов содержится в результатах поиска. Кроме этого, следует определить, какой из критериев поиска более результативен и насколько целесообразно использование поиска с учетом синонимов.

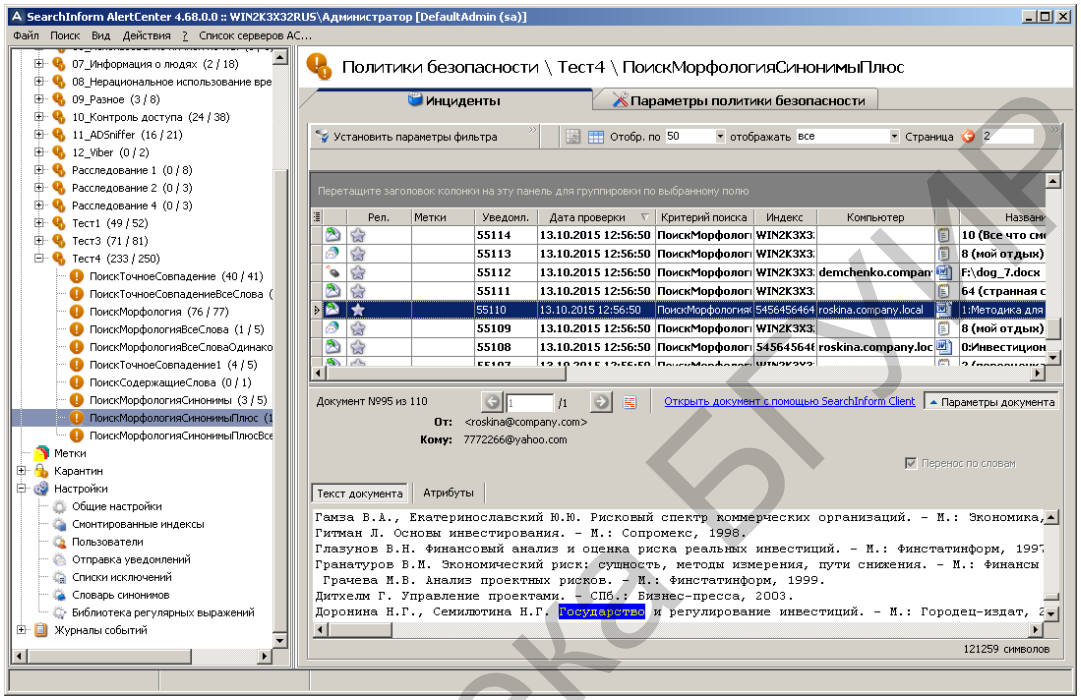


Рис. 5.26. Индикация инцидентов по критерию «ПоискМорфологияСинонимыПлюс»

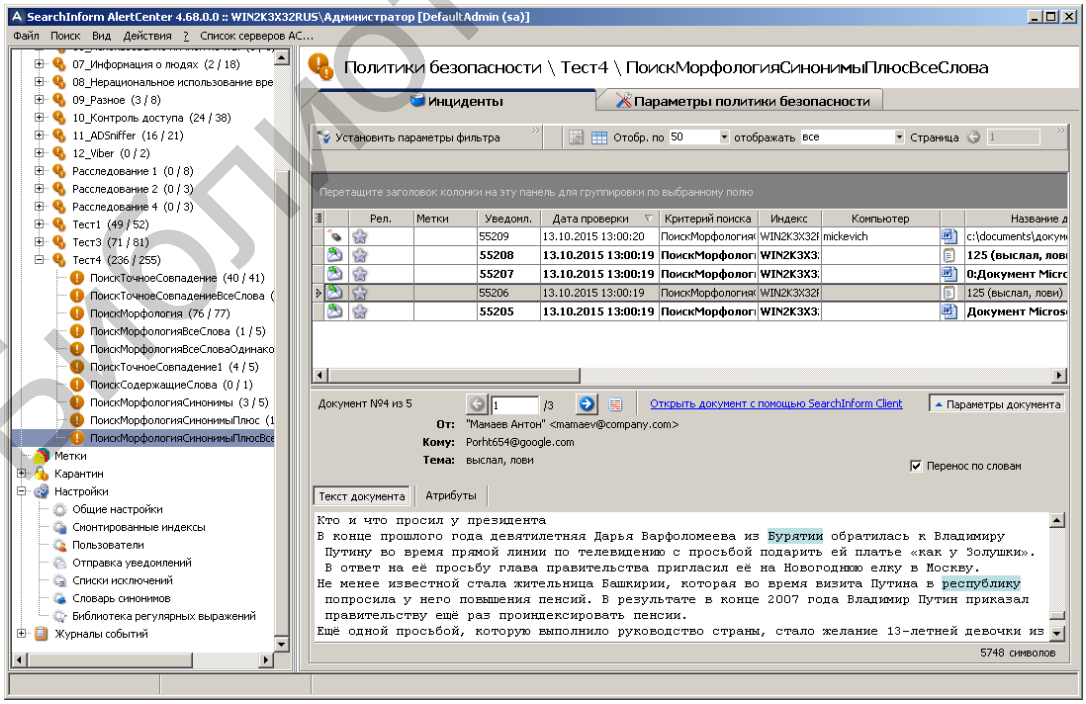


Рис. 5.27. Индикация инцидентов по критерию «ПоискМорфологияСинонимыПлюсВсеСлова»

Уточнить результаты поиска за счет использования опции «Поиск фразы». Для этого следует создать, показанный на рис. 5.28, новый критерий поиска «ПоискМорфологияСинонимыПлюсФраза».

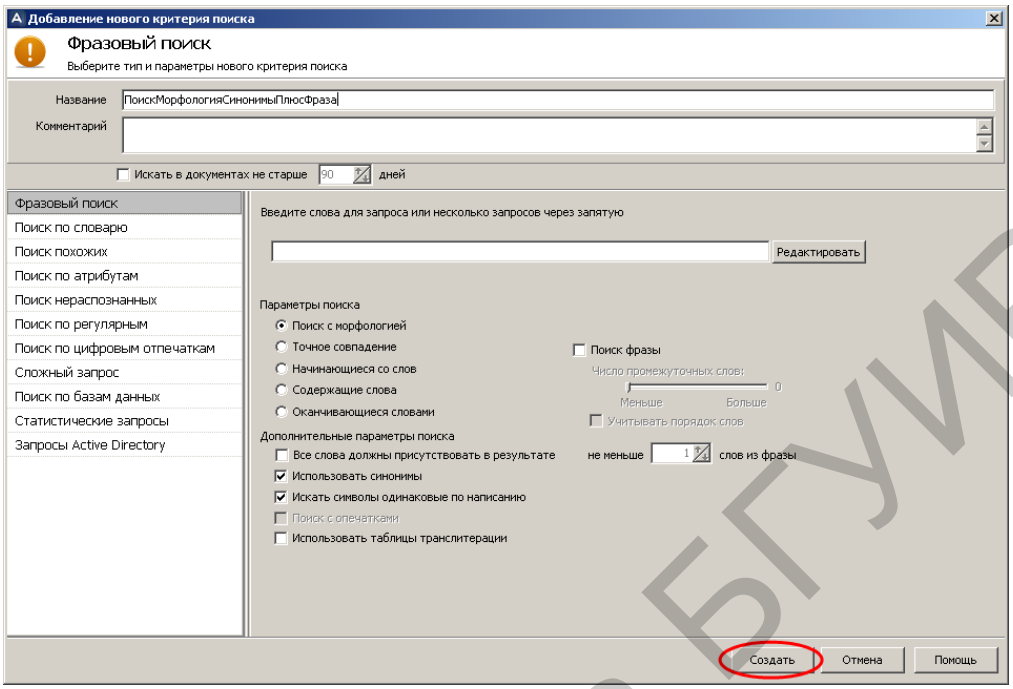


Рис. 5.28. Создание критерия «ПоискМорфологияСинонимыПлюсФраза»

Запустить принудительное выполнение критерия поиска «ПоискМорфологияСинонимыПлюсФраза» и определить его результативность (рис. 5.29). Определить целесообразность использования опции «Поиск фразы» для коротких поисковых запросов.

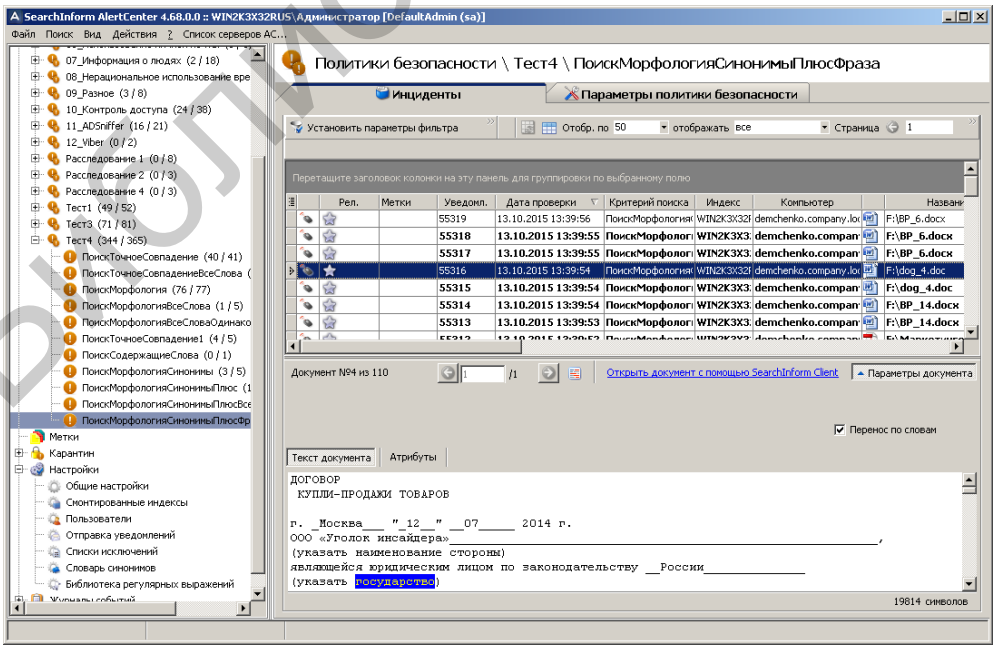


Рис. 5.29. Индикация инцидентов по критерию «ПоискМорфологияСинонимыПлюсФраза»

Исследовать эффективность фразового поиска при использовании длинных поисковых запросов, содержащих фразы, которые могут быть разделены текстовыми фрагментами. Для этого создадим новый критерий поиска «ПримерПоискФразы», окно которого показано на рис. 5.30. Поисковый запрос представляет собой текст: «Благодарим Вас за внимание, оказанное Компании Софтинформ! Образец заявки в приложении!».

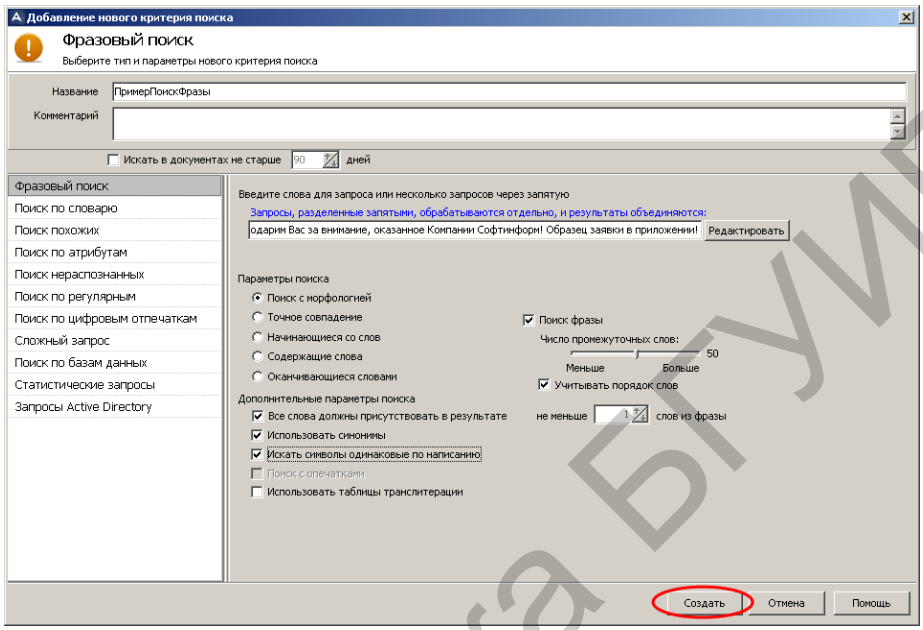


Рис. 5.30. Создание критерия «ПримерПоискФразы»

Запустить принудительное выполнение критерия поиска «ПримерПоискФразы» и убедиться в его результативности (рис. 5.31). Определить сколько целевых и нецелевых документов содержится в результатах поиска.

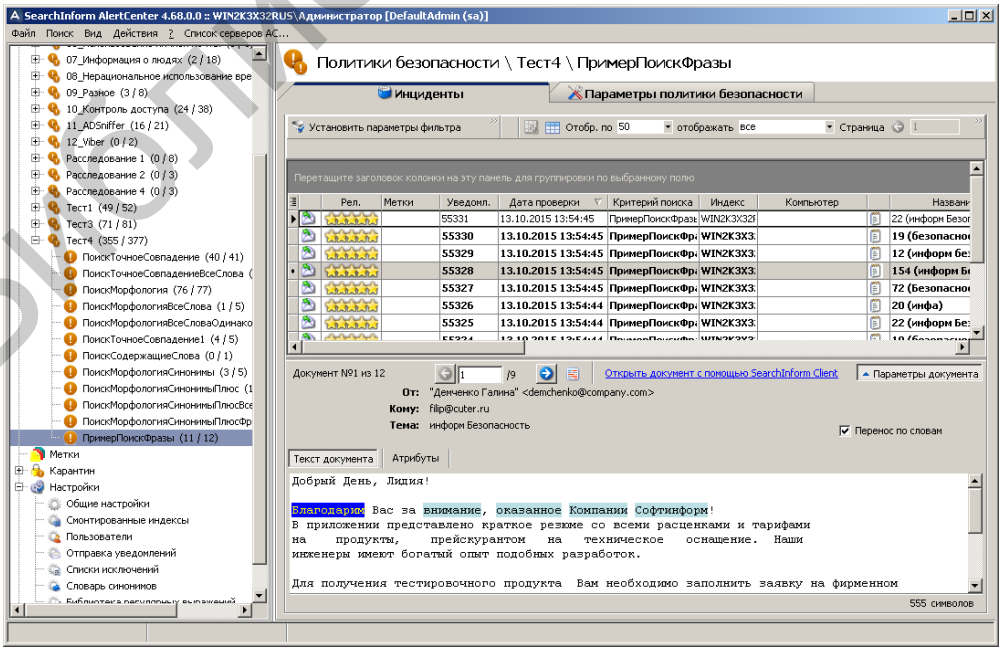


Рис. 5.31. Индикация инцидентов по критерию «ПримерПоискФразы»

Формирование критерия «Поиск по регулярным» рассмотрим на примерах поиска в перехваченных документах информации, соответствующей регулярным выражениям.

В соответствии с рис. 5.32 создать критерий для поиска документов, содержащих хотя бы одну фамилию с инициалами.

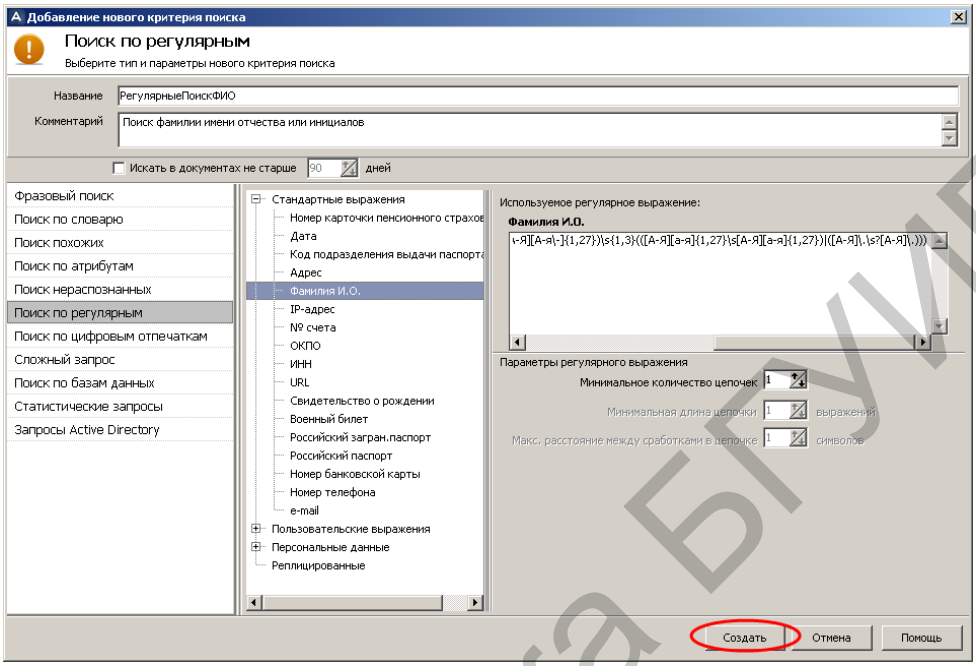


Рис. 5.32. Создание критерия «РегулярныйПоискФИО»

Для поиска по регулярным выражениям и цифровым отпечаткам в проверяемых индексах должна быть включена опция хранения текстов. В соответствии с рис. 5.33–5.36 включить хранение текстов в индексах из перечня проверки.

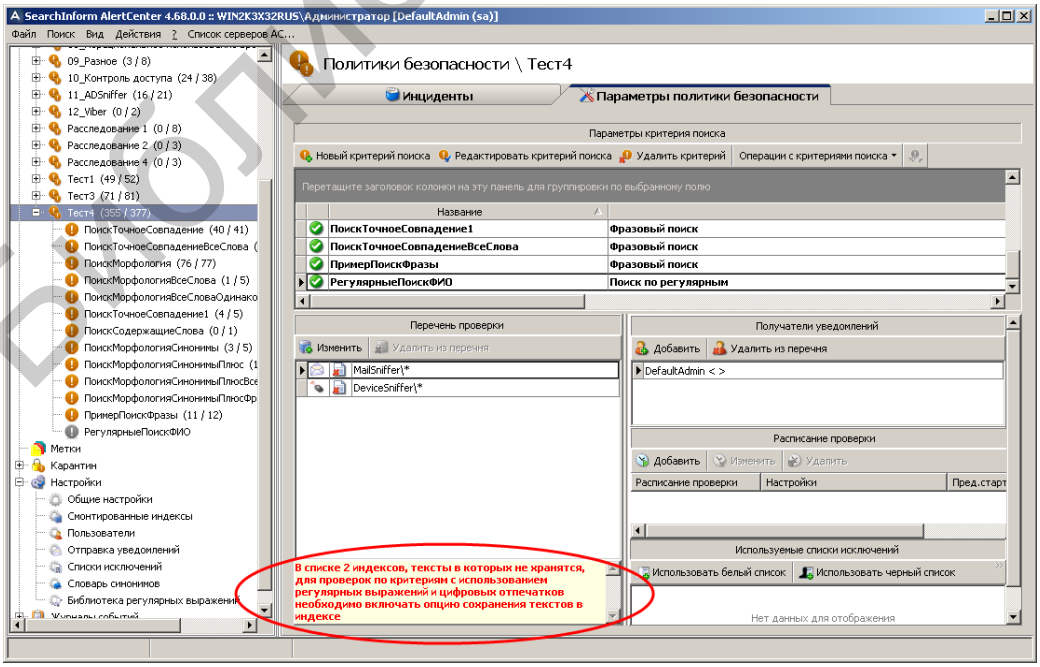


Рис. 5.33. Индикация предупреждения

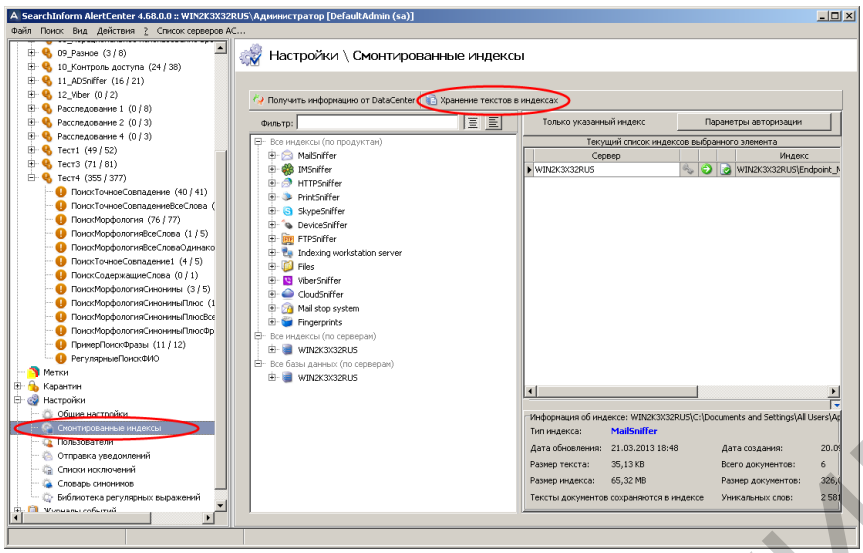


Рис. 5.34. Выбор опции «Хранение текстов в индексах»

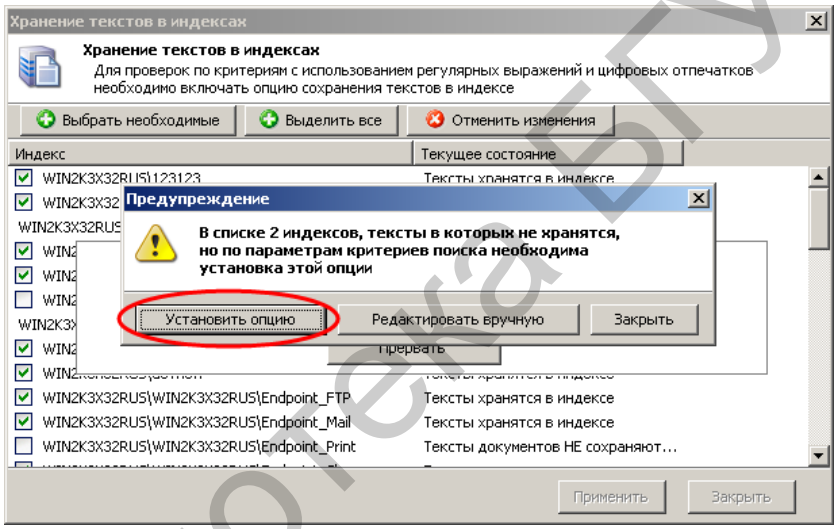


Рис. 5.35. Автоматический выбор индексов, используемых в созданных критериях поиска

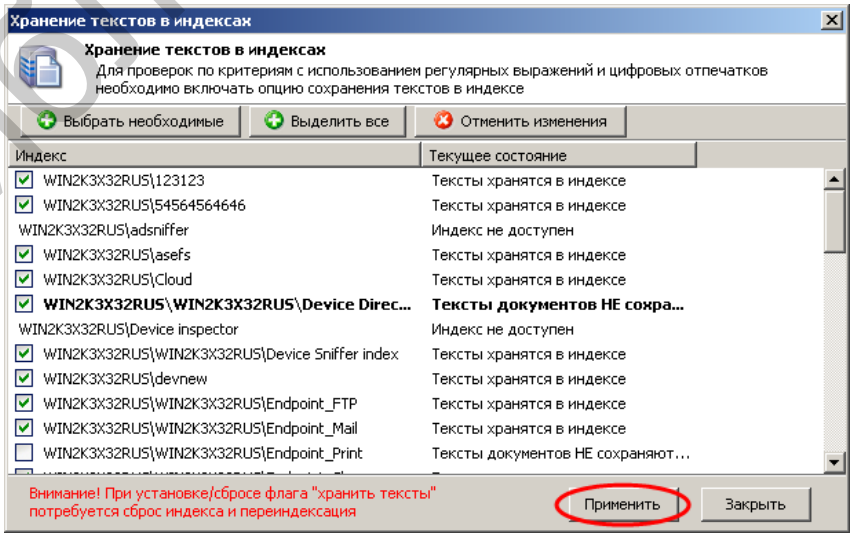


Рис. 5.36. Применение изменений

Запустить принудительное выполнение критерия поиска «РегулярныйПоискФИО» и оценить его результативность (рис. 5.37).

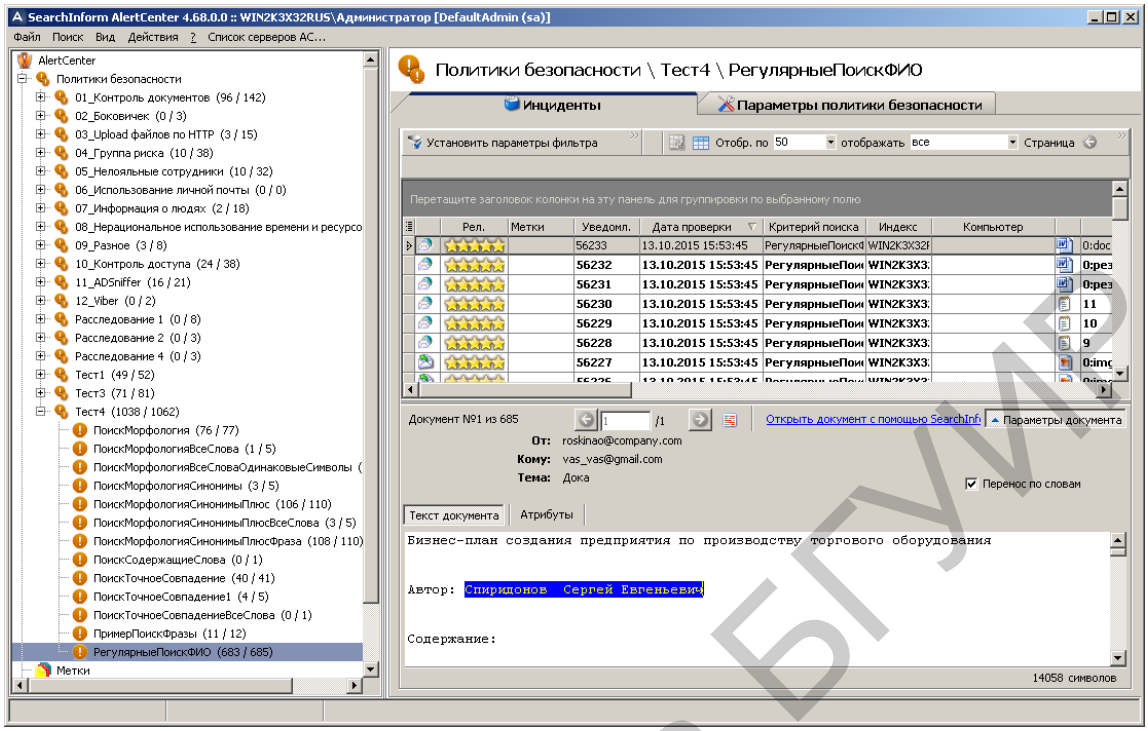


Рис. 5.37. Индикация инцидентов по критерию «РегулярныйПоискФИО»

В соответствии с рис. 5.38 создать критерий для поиска документов, содержащих как минимум пять фамилий с инициалами.

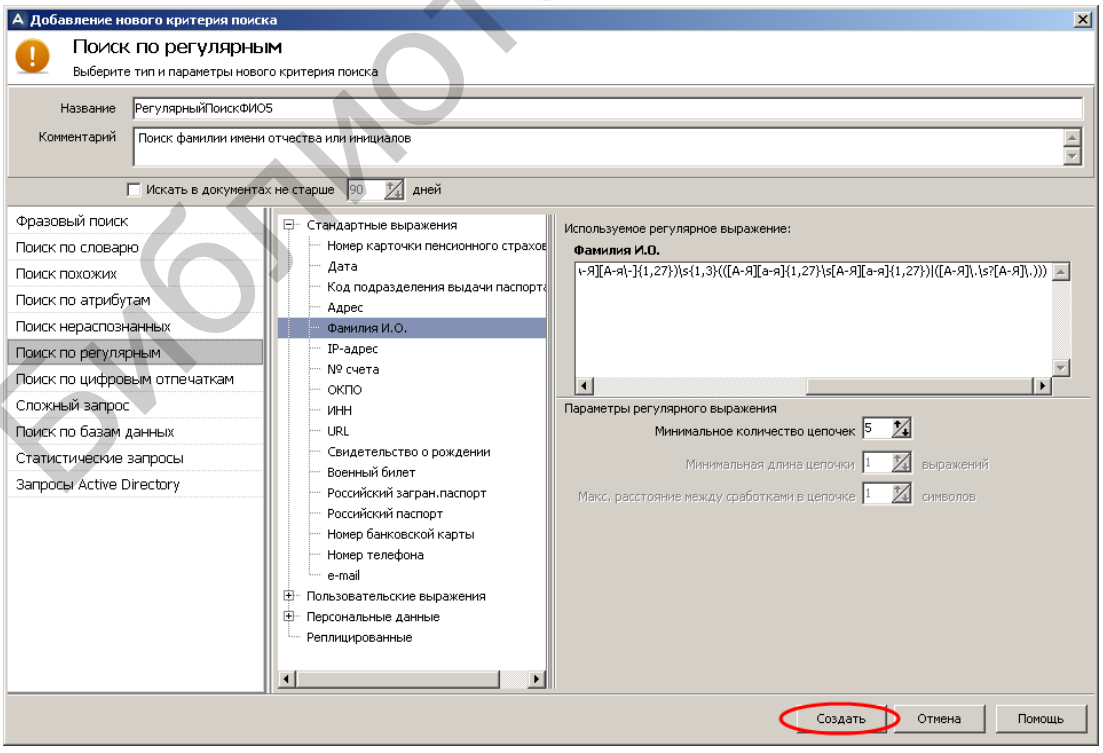


Рис. 5.38. Создание критерия «РегулярныйПоискФИО5»

Запустить принудительное выполнение критерия поиска «РегулярныйПоискФИО5» и оценить его результативность (рис. 5.39).

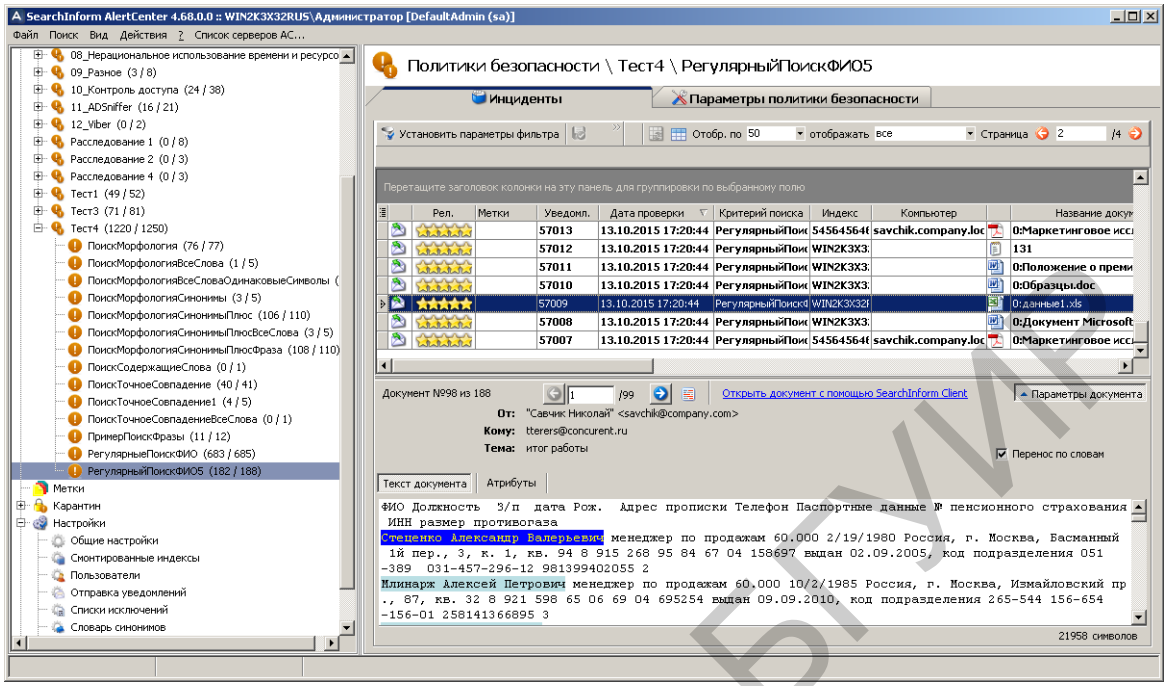


Рис. 5.39. Индикация инцидентов по критерию «РегулярныйПоискФИО5»

Выполнив инструкции рис. 5.40–5.44, убедиться в том, что найденный по критерию «РегулярныйПоискФИО5» документ с названием «0:plan_po_marketingy.doc», владельцем которого является пользователь «bublik@company.com», входит в результаты поиска по критерию «РегулярныйПоискФИО».

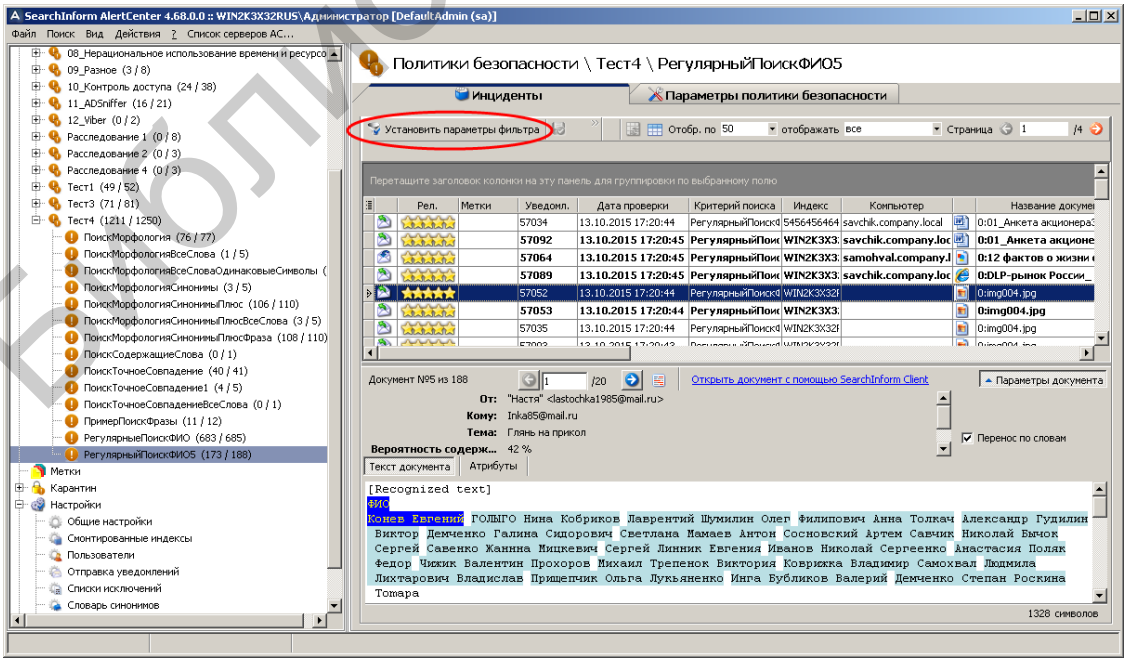


Рис. 5.40. Индикация параметров найденного документа
и вход в режим установки фильтра

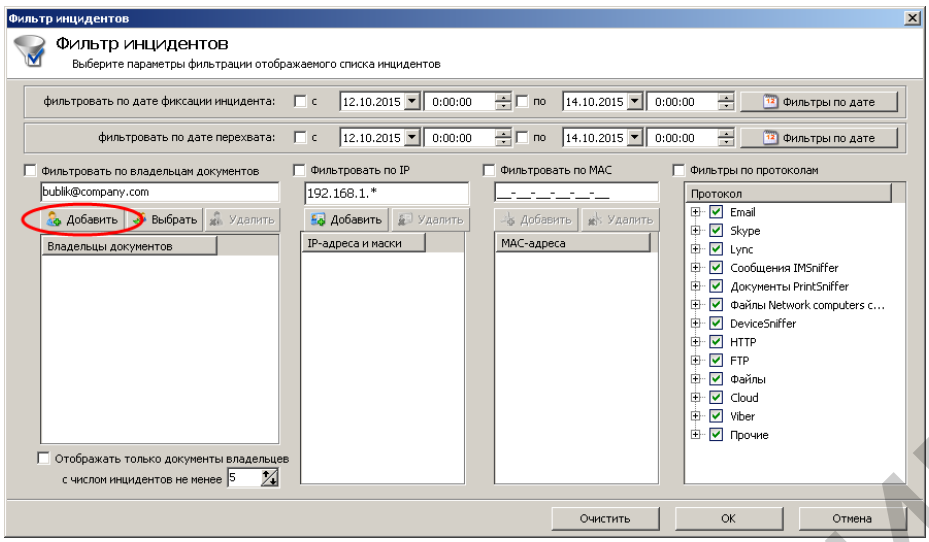


Рис. 5.41. Добавление имени владельца

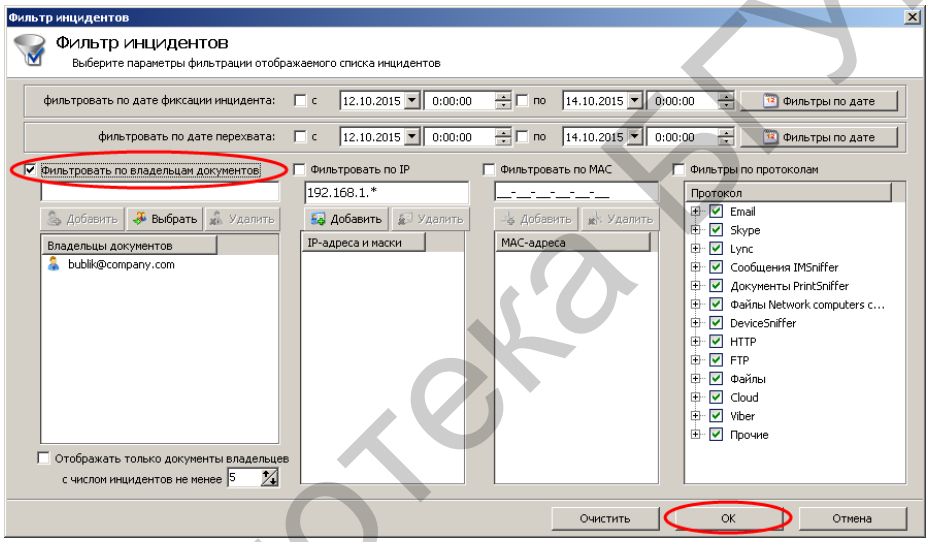


Рис. 5.42. Установка фильтрации по имени владельца «bublik@company.com»

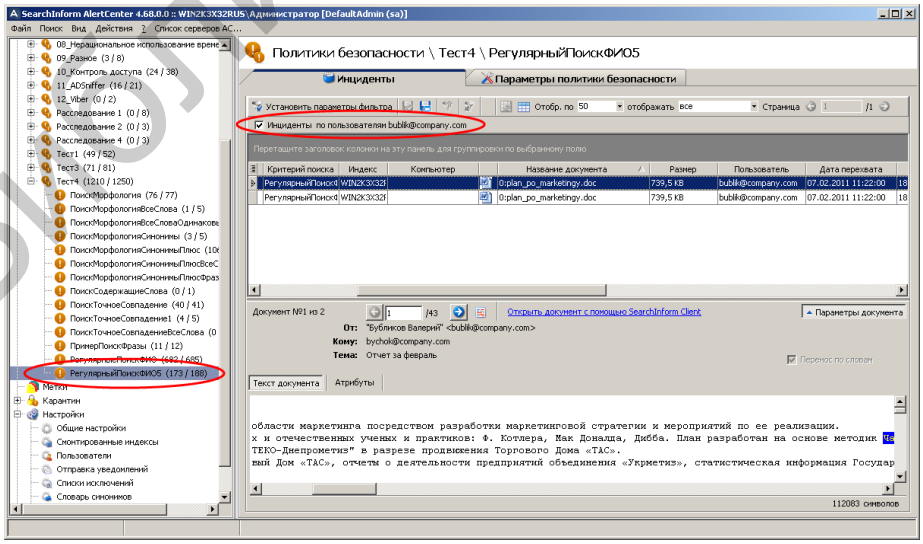


Рис. 5.43. Применение фильтра по владельцу «bublik@company.com» для результатов поиска по критерию «РегулярныйПоискФИО5»

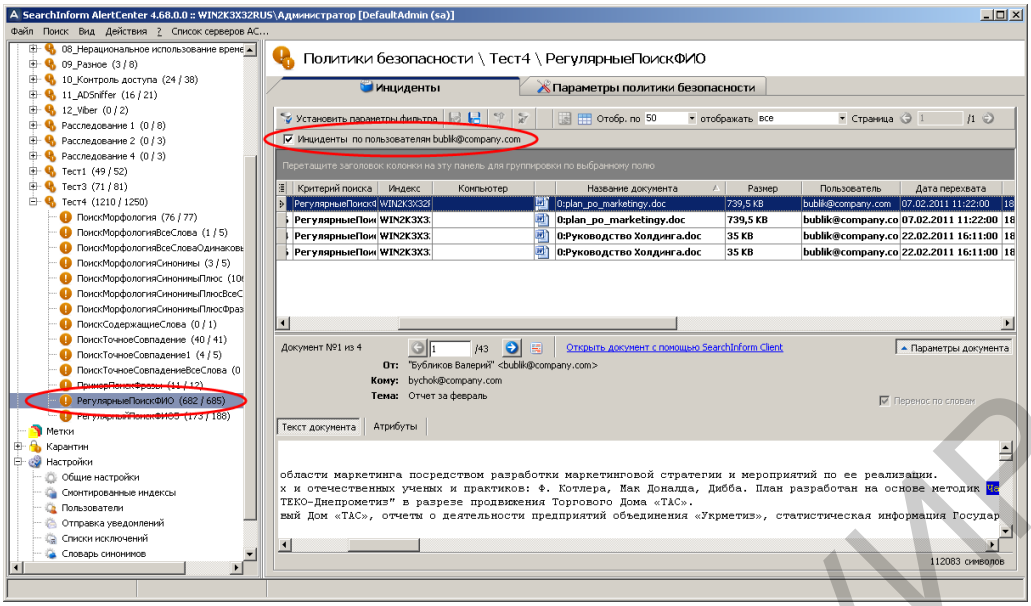


Рис. 5.44. Применение фильтра по владельцу «bublik@company.com» для результатов поиска по критерию «РегулярныйПоискФИО» и отображение искомого документа «0:plan_po_marketingy.doc»

Отменить применение фильтра «Инциденты по пользователю bublik@company.com». Определить наиболее эффективный запрос для поиска в перехваченных документах информации, касающейся Республики Бурятия.

Выполнив инструкции рис. 5.45–5.54, создать новое регулярное выражение «ФамилияАдрес», предназначенное для поиска фамилии, инициалов и электронного адреса. При этом выражение «ФамилияАдрес» должно располагаться в группе «Персональные данные» и состоять из библиотечных выражений «Фамилия И.О.» и «e-mail».

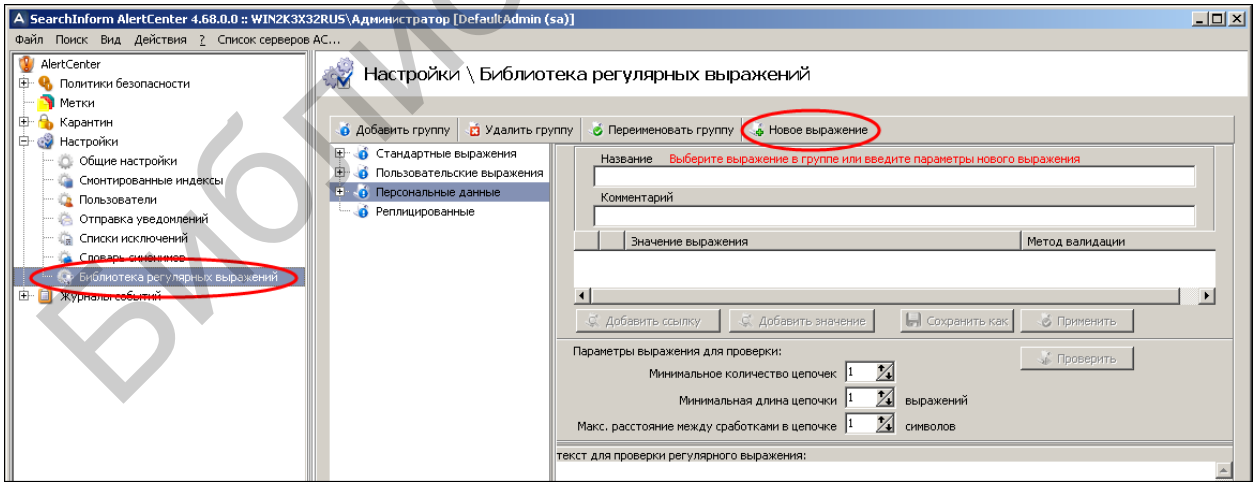


Рис. 5.45. Вход в режим создания регулярного выражения «ФамилияАдрес»

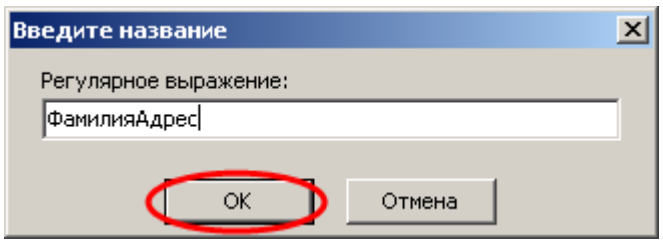


Рис. 5.46. Ввод назнавания регулярного выражения

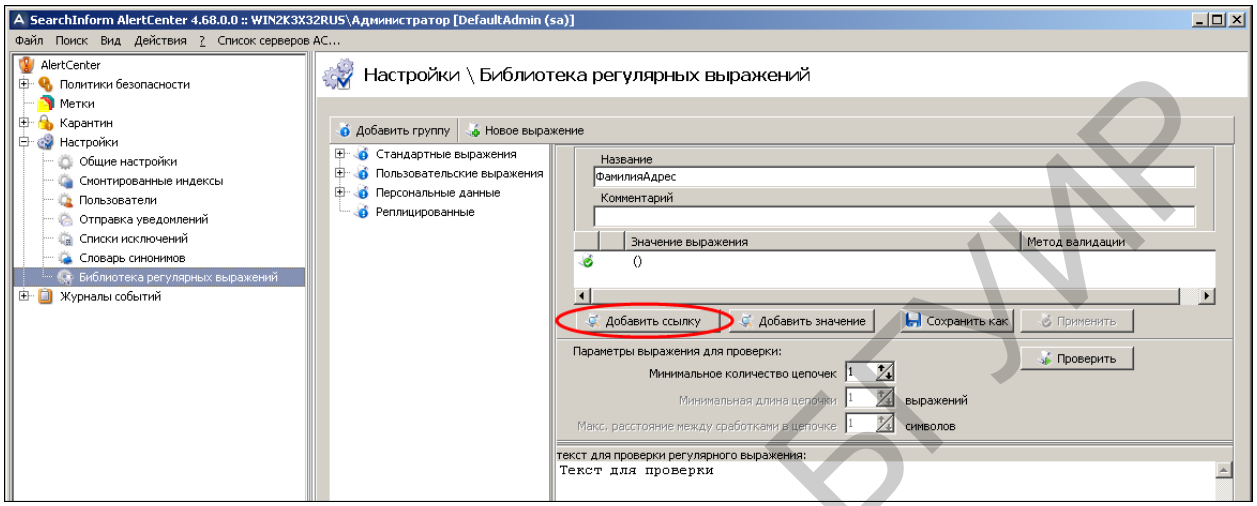


Рис. 5.47. Добавление первой ссылки

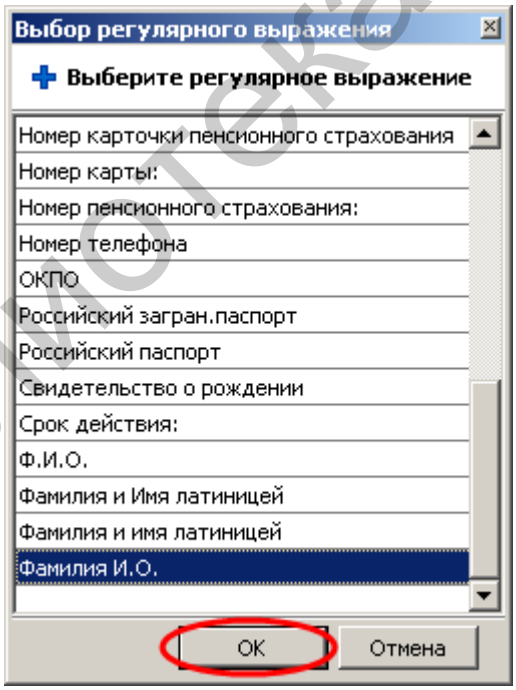


Рис. 5.48. Выбор ссылки «Фамилия И.О.»

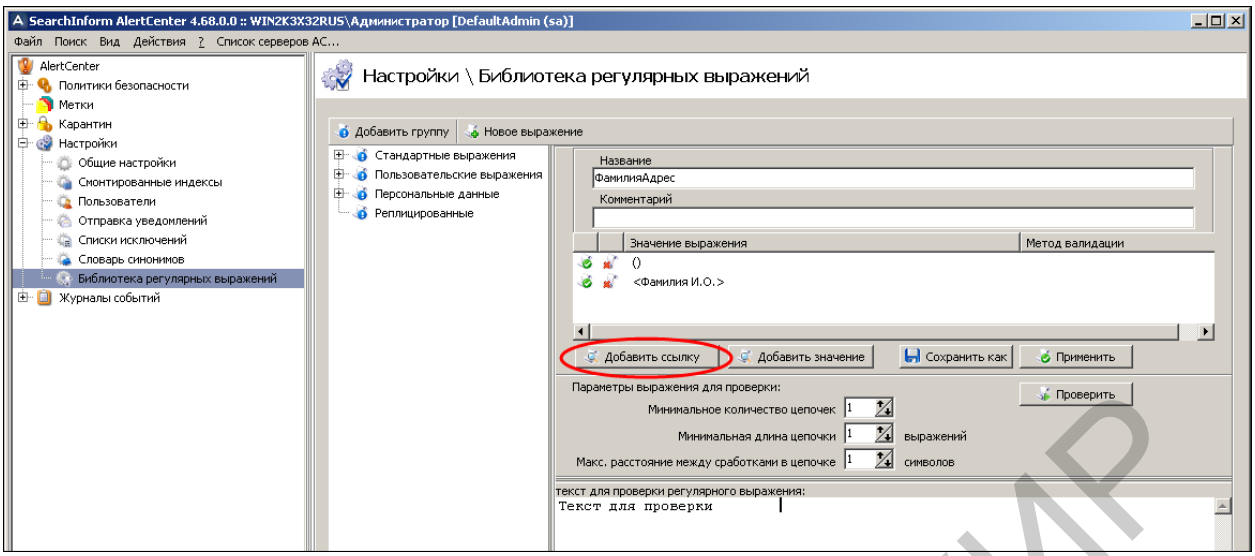


Рис. 5.49. Добавление второй ссылки

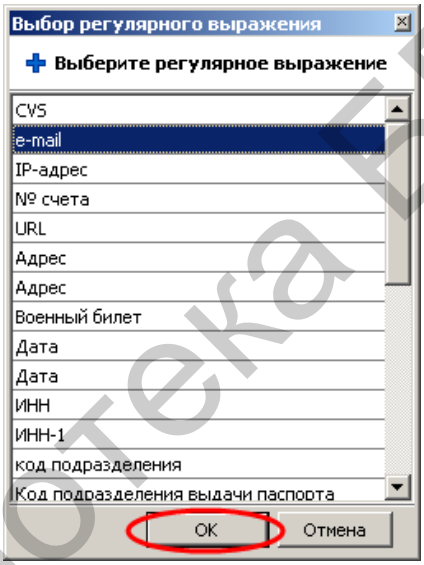


Рис. 5.50. Выбор ссылки «e-mail»

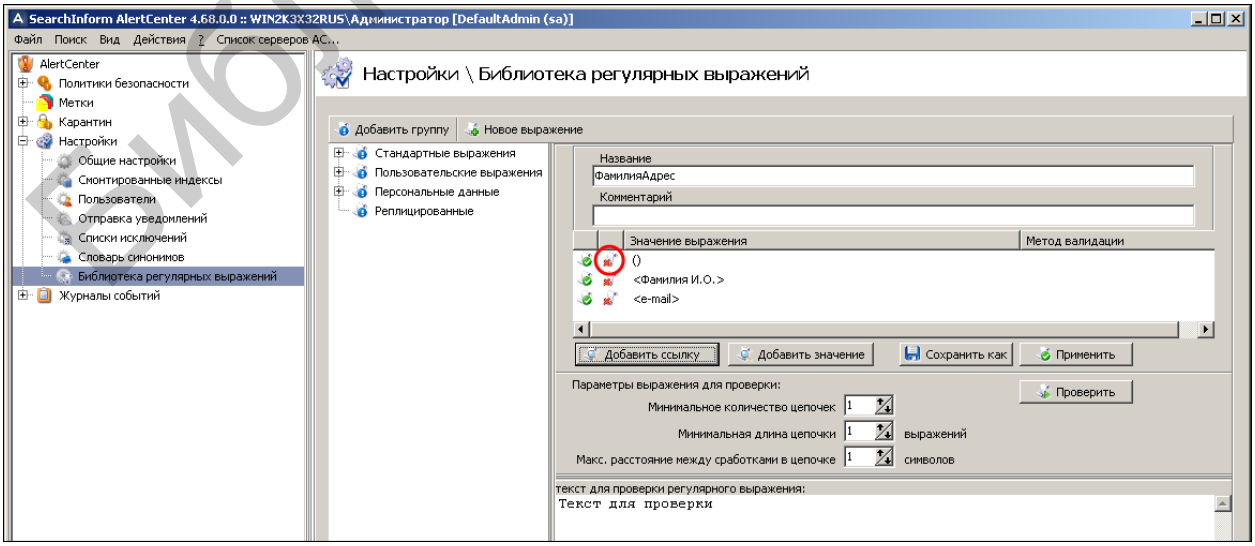


Рис. 5.51. Удаление пустого значения

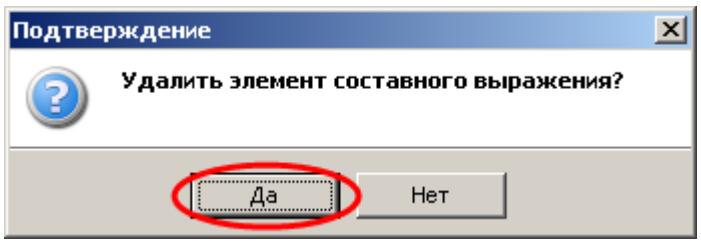


Рис. 5.52. Подтверждение удаления

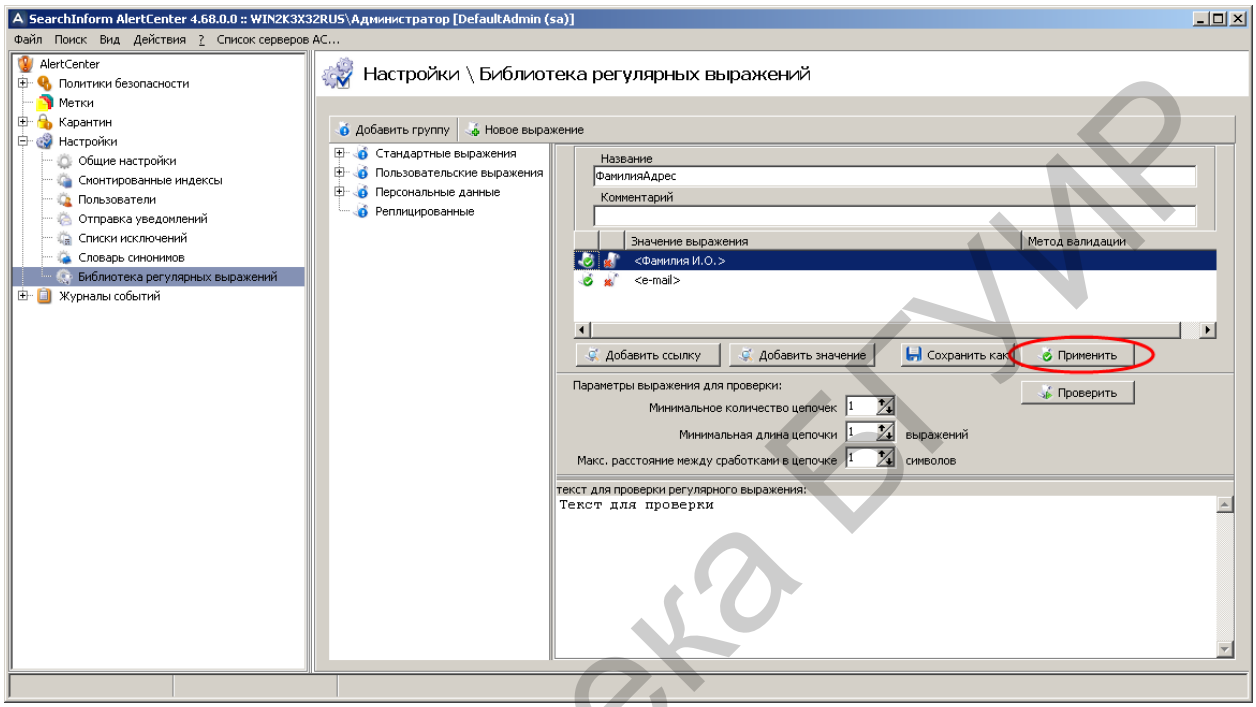


Рис. 5.53. Сохранение выражения «ФамилияАдрес»

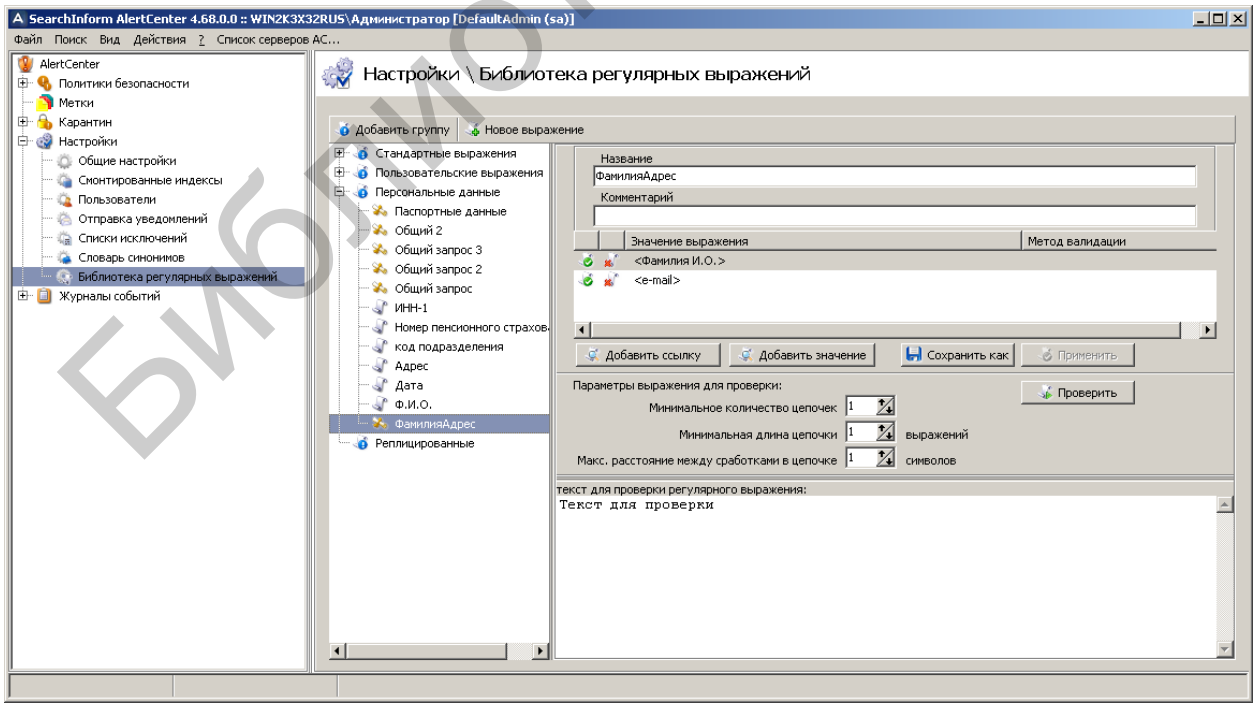


Рис. 5.54. Отображние созданного выражения «ФамилияАдрес»

В соответствии с рис. 5.55 на основе регулярного выражения «ФамилияАдрес» создать критерий для поиска документов, содержащих фамилию, инициалы и электронный адрес.

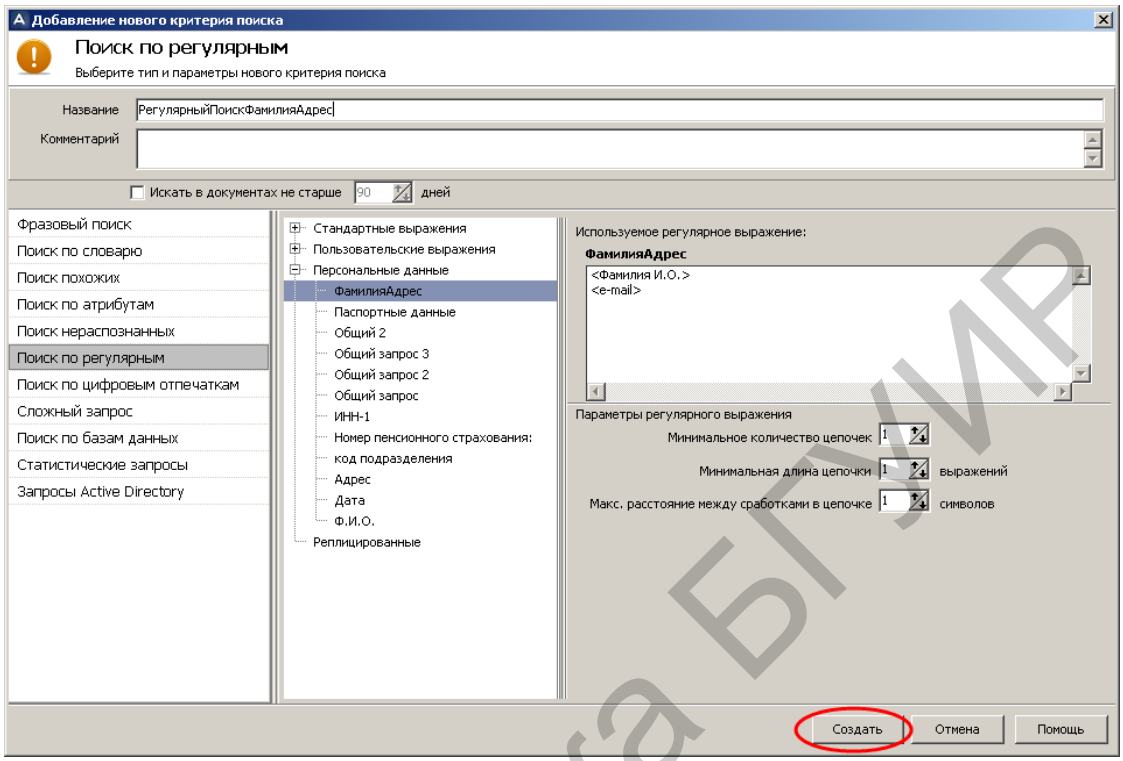


Рис. 5.55. Содание критерия «РегулярныйПоискФамилияАдрес»

Запустить принудительное выполнение критерия поиска «РегулярныйПоискФамилияАдрес» и оценить его результативность (рис. 5.56).

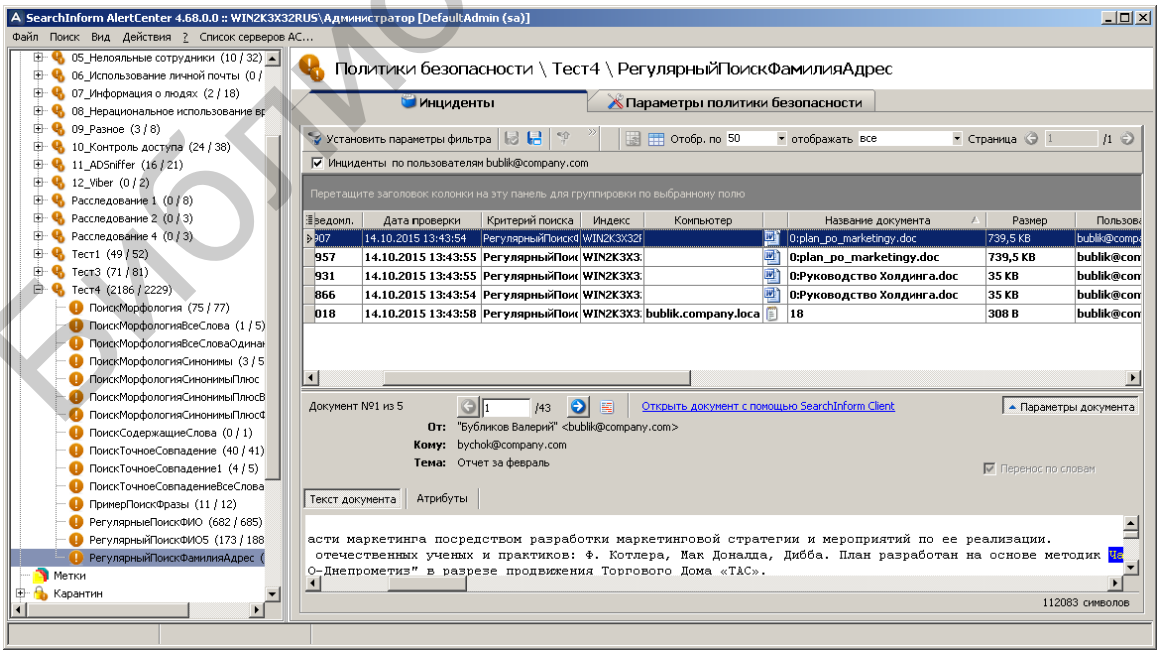


Рис. 5.56. Индикация инцидентов по критерию «РегулярныйПоискФамилияАдрес»

Попробовать уточнить результаты поиска. Для этого в соответствии с рис. 5.57 и 5.58 следует изменить параметры критерия «РегулярныйПоиск-ФамилияАдрес».

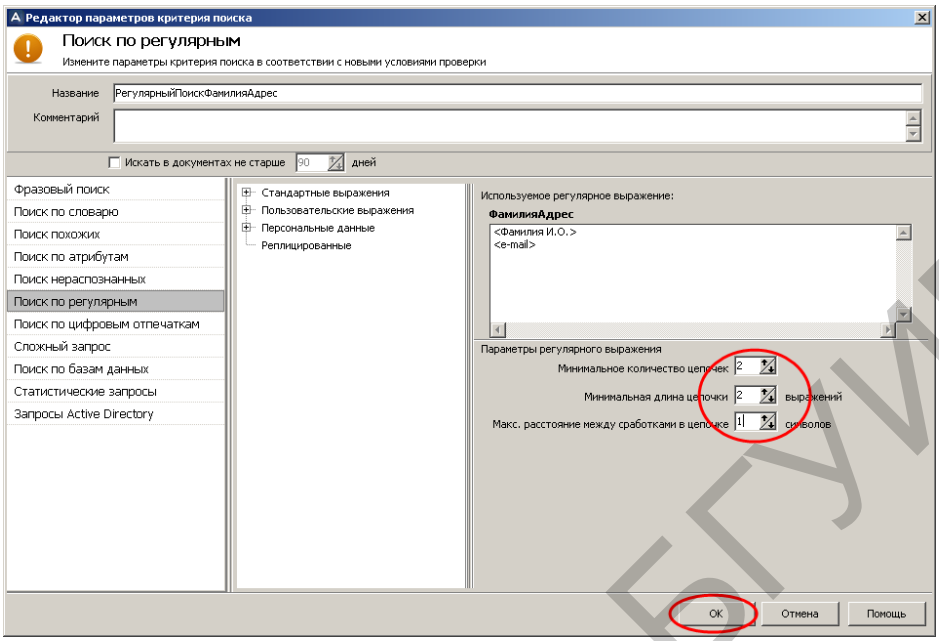


Рис. 5.57. Редактирование критерия «РегулярныйПоискФамилияАдрес»

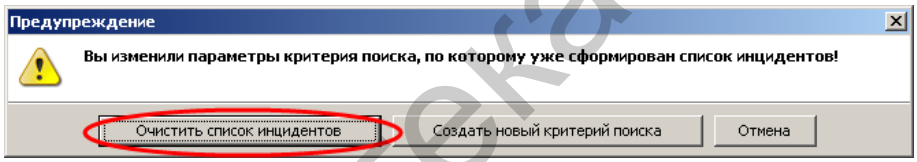


Рис. 5.58. Подтверждение результатов редактирования

Запустить принудительное выполнение отредактированного критерия поиска «РегулярныйПоискФамилияАдрес» и оценить его результативность (рис. 5.59).

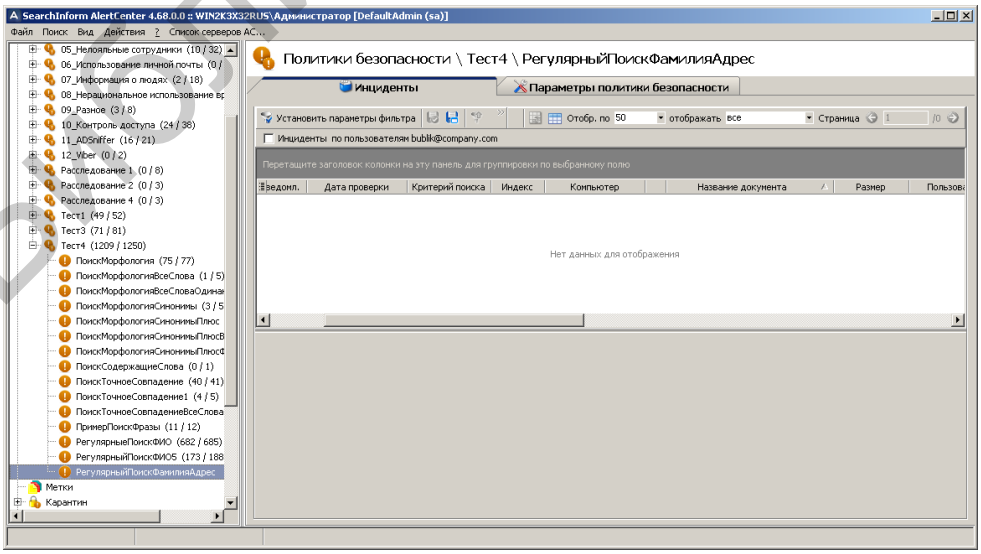


Рис. 5.59. Индикация инцидентов по отредактированному критерию «РегулярныйПоискФамилияАдрес»

Попробовать расширить результаты поиска. Для этого в соответствии с рис. 5.60 следует изменить параметры критерия «РегулярныйПоискФамилияАдрес».

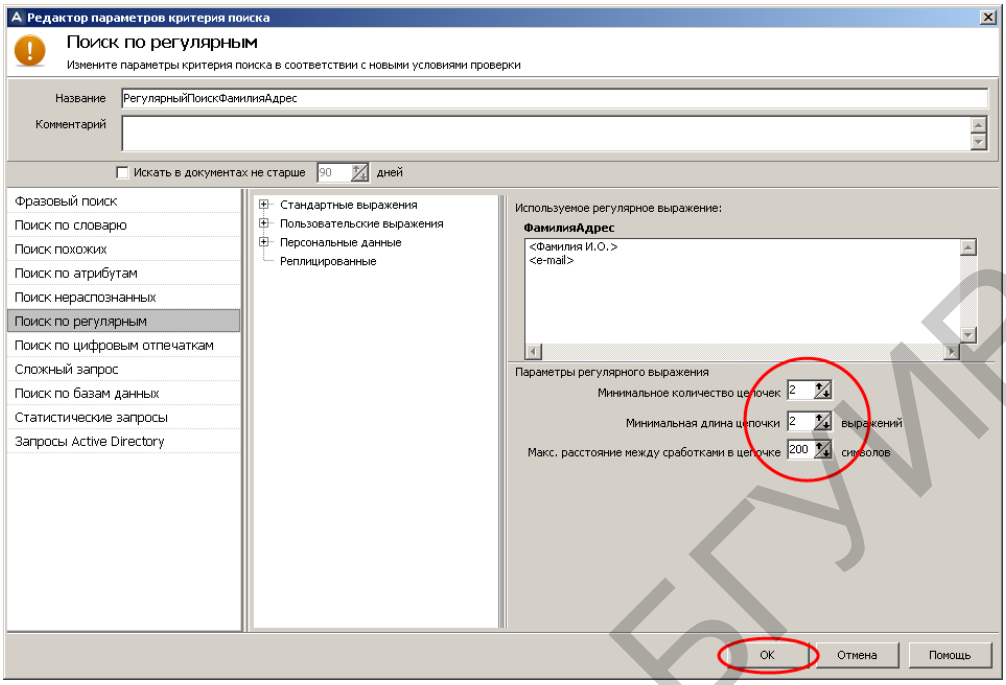


Рис. 5.60. Второе редактирование критерия «РегулярныйПоискФамилияАдрес»

Запустить принудительное выполнение вновь отредактированного критерия поиска «РегулярныйПоискФамилияАдрес» и оценить его результативность (рис. 5.61).

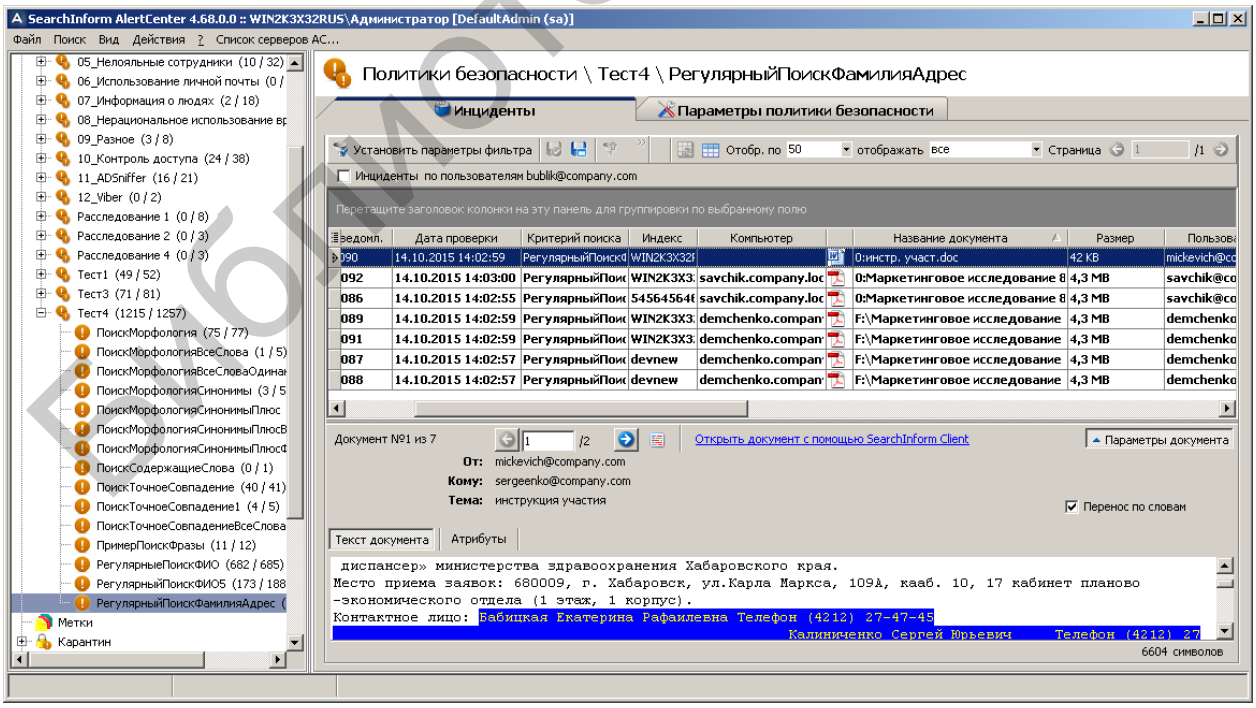


Рис. 5.61. Индикация инцидентов по отредактированному критерию «РегулярныйПоискФамилияАдрес»

Определить параметры критерия «РегулярныйПоискФамилияАдрес», которые отвечают наиболее точному результату поиска.

Закрыть окно AlertCenter Client.

Завершить работу с виртуальным компьютером.

5.3. Задание для самостоятельной работы

1. Удалить в окне инцидентов фильтр «Инциденты по пользователю bublik».
2. Используя имеющуюся библиотеку регулярных выражений, с помощью критерия «Поиск по регулярным» найти документы, в которых содержится фамилия, инициалы, номер банковской карты и номер телефона. Определить параметры критерия, которые отвечают наиболее точному результату поиска.
3. С помощью критерия «Фразовый поиск» найти документы, которые содержат информацию, касающуюся банковской деятельности. Определить параметры критерия, которые отвечают наиболее точному результату поиска.
4. Используя имеющуюся библиотеку регулярных выражений, с помощью критерия «Поиск по регулярным» найти документы, в которых содержится информация, заданная преподавателем. Определить параметры критерия, которые отвечают наиболее точному результату поиска.
5. С помощью критерия «Фразовый поиск» найти документы, в которых содержится информация, заданная преподавателем. Определить параметры критерия, которые отвечают наиболее точному результату поиска.

5.4. Контрольные вопросы

1. Чем отличается опция «Поиск с морфологией» от опции «Точное совпадение»?
2. Назовите два случая, в которых использование опции «Использовать синонимы» не приносит результатов.
3. Каково назначение опции «Искать символы одинаковые по написанию»?
4. В каких случаях целесообразно использование опции «Поиск фразы»?
5. Зачем необходимо настраивать параметр «Расстояние между словами» в опции «Поиск фразы»?
6. Каково назначение поля «Фильтр» в «Словаре синонимов»?
7. Зачем в поисковом запросе используется символ «,»?
8. Каково назначение опции «Минимальное количество цепочек» в критерии «Поиск по регулярным»?
9. Каково назначение опции «Минимальная длина цепочки» в критерии «Поиск по регулярным»?
10. Каково назначение опции «Максимальная длина пробелов в цепочке» в критерии «Поиск по регулярным»?
11. В чем разница между функциональностью кнопок «Добавить ссылку» и «Добавить значение» окна «Библиотека регулярных выражений»?
12. Почему в окне «Выбор регулярного выражения» могут присутствовать несколько одинаковых названий регулярных выражений?

ЛАБОРАТОРНАЯ РАБОТА №6
ФОРМИРОВАНИЕ РЕГУЛЯРНЫХ ВЫРАЖЕНИЙ И НАСТРОЙКА СИСТЕМЫ ПЕРЕХВАТА ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

Цель: освоить принципы формирования регулярных выражений для поиска конфиденциальной информации и овладеть методикой настройки системы перехвата программного комплекса SearchInform.

6.1. Теоретическая часть

Регулярные выражения – технология поиска текстовых фрагментов в электронных документах, соответствующих определенным шаблонам (образцам). Другими словами, данная технология заключается в том, что в документе производится поиск текстовых фрагментов, которые отвечают заданным шаблонам. В простейшем случае шаблон поиска состоит исключительно из символов, к которым относятся буквы, арабские цифры и некоторые знаки препинания. Например, для поиска в документе текста «привет» можно использовать шаблон «привет». Однако по причине ограниченности возможностей поиска простейшие образцы, как правило, не используются. На практике в состав шаблонов кроме символов включают специальные символы, основным назначением которых является указание элементов, управляющих процессом поиска, и определение непечатаемых символов. Например, для поиска в документе отдельного слова «привет» следует использовать образец (\sпривет\s). Назначение наиболее применяемых спецсимволов приведено в табл. 6.1.

Таблица 6.1

Перечень спецсимволов

Спецсимвол	Назначение	Спецсимвол	Назначение
\t	Табуляция	[	Начало символьного класса
\s	Пробел	]	Конец символьного класса
\d	Цифра	{	Начало квантификатора
\D	Все что угодно, но не цифра	}	Конец квантификатора
\b	Начало или конец слова	?	Один любой символ
$	Конец строки	|	Альтернатива
^	Начало строки	+	Объединение
\w	Буква	(	Начало группировки
*	Любая последовательность символов	)	Конец группировки

Как видно из табл. 6.1, существуют спецсимволы, такие как «(», «)», «[», «]», «{», «}», которые могут потенциально использоваться как обычные. В таких случаях им должен предшествовать знак «\». Например, для поиска текста «[123]» можно использовать образец «\[123\]». При этом для представления в образце символа «\» следует записать «\\».

Основными управляющими элементами поиска являются символьные классы, квантификаторы, группировки и альтернативы.

Символьный класс представляет собой конечный набор символов. Он ограничивается квадратными скобками и содержит перечисление символов, которые можно вместо него подставить. Заменяется он всего на один символ, входящий в это перечисление. Примеры:

[абвгде] – простое перечисление символов.

[а-яА-Я] – все русские буквы.

[0-9a-z] – цифры и строчная латиница.

[^0-9] – все символы, кроме цифр.

Отметим, что в символьном классе (внутри квадратных скобок) знак «-» используется для указания диапазонов символов, а знак «^» обозначает символ, который отсутствует в данном перечислении. Фактически префикс «^» инвертирует список. Вместо того чтобы перечислять символы, принадлежащие классу, мы перечисляем символы, не входящие в него.

Группировки используются, когда необходимо обрабатывать результат частями. Например, при обработке ссылок в HTML-документе удобно отдельно обрабатывать текст, ссылки и URL. Группировки заключаются в круглые скобки.

Квантификаторы показывают, сколько раз может повторяться предыдущий символ (символьный класс, альтернатива и т. д.). Ограничиваются парой фигурных скобок. Примеры:

\w{3} – три латинских буквы.

\d{1, 3} – одна, две или три цифры.

[а-яА-Я]{3, } – русское слово длинной три символа и более.

Квантификаторы с одним параметром называются точными и указывают точное количество повторений.

Квантификаторы с двумя аргументами называются конечными и указывают конечный диапазон, в котором варьируется количество повторений.

Квантификаторы без второго параметра (но с запятой) называются бесконечными и ограничивают количество повторений лишь снизу.

Альтернативы нужны, когда необходимо объединить несколько правил в одно. При этом совпадение засчитывается, когда есть совпадение хотя бы с одним правилом. Желательно альтернативы заключать внутрь группировки (круглые скобки). Правила, входящие в вариант, разделяются вертикальной чертой «|». Примеры:

(жы|шы) – или «жы» или «шы»

([a-zA-Z]+|[а-яА-Я]+) – или слово на латинице, или русское.

В данном примере продемонстрирована альтернатива в группировке. В принципе, альтернатива может существовать и вне группировки, но так возникает больше ошибок.

Рассмотрим несколько примеров записей образцов регулярных выражений.

Пример №1

Поиск в тексте номеров телефонов, т. е. строки типа «+7-924-111-11-34». Предлагаемый шаблон – «\+[0-9-]+».

Принцип поиска: находим строку, которая начинается со знака «+», за которым следует неограниченное количество цифр, или знака «-».

Пояснения частей шаблона:

1. \+ – явно указываем, что первым символом должен быть плюс. Поскольку символ «+» относится к спецсимволам, то он экранирован с помощью \.

2. [0-9-] – квантификатор, указывающий на цифры от 0 до 9 или знак «-».

3. «+» – в данном случае знак плюса выполняет роль спецсимвола объединения.

Пример №2

Поиск в тексте адресов электронной почты, т. е. строки «1w1@qw12.1we.ex».

Предлагаемый шаблон – «[\w\d-.]+@([\w\d-]+(\.[\w\-]+)+)».

Пояснения частей шаблона:

1. [\w\d-.]+ – эта часть описывает адрес электронной почты до знака «@». В соответствии со стандартом здесь могут быть любые буквы (\w), цифры от нуля до девяти (\d), знак «-» и точка. После описания символьного класса нужно поставить спецсимвол «+», иначе под данную часть шаблона будут попадать одиночные символы.

2. @ – электронный адрес почты не может быть без знака «@», поэтому нам необходимо его описать.

3. ([\w\d-]+(\.[\w\-]+)+) – запись доменной части электронного адреса почты, которая начинается группой латинских букв или цифр, продолжается знаком «.» и заканчивается группой латинских букв.

Пример №3

Поиск в тексте ссылок на интернет-ресурсы, т. е. строк типа «http://www.12weer.ex» или «ftp://2weer.ex».

Предлагаемый шаблон – «(http|ftp)://([\w\d-]+(\.[\w\d\-]+)+)(([\w\d\-=\?\\\./]+)+)*».

Пояснения частей шаблона.

1. (http|ftp):// – эта часть описывает возможные протоколы. Любой адрес для обращения к узлу с помощью протокола http или ftp должен начинаться с http:// или ftp:// соответственно. В скобках сначала указывается приставка http, затем вертикальная черта, которая соответствует логическому ИЛИ, и уже после нее вторая возможная приставка – ftp. В итоге наш шаблон будет срабатывать как на ссылки ftp-ресурсов, так и http.

2. ([\w\d-]+(\.[\w\d\-]+)+) – таким образом можно описать адрес узла. Данная конструкция будет одинаково хорошо срабатывать и на адреса ви-

да http://192.168.0.1, т. е. и на IP-адрес, и на символьные адреса. Скобками группируем условия, т. к. если просто написать диапазон литералов в одном классе и поставить метасимвол +, то выражение не будет правильно работать.

3. (([\w\d\-=\?\\\./]+)+)* – поскольку ссылка может вести на конкретный файл, то мы обязаны это предусмотреть. В пути могут присутствовать различные символы: «/», «?», «=». Поскольку часть из них является спецсимволами, то их нужно экранировать, поставив перед ними еще один слеш.

Настройки системы перехвата

Ознакомиться с разделом 6 руководства аудитора безопасности системы SearchInform.

6.2. Лабораторное задание

1. В соответствии с методическими указаниями лабораторной работы №1 запустить виртуальный компьютер с установленным программным комплексом SearchInform.

Выполнить задания лабораторных работ №2–5.

В дальнейшем предусматривается, что студент освоил методику настроек SearchInform в объеме предыдущих лабораторных работ.

Убедиться в том, что сервер AlertCenter работает, в противном случае его следует запустить с помощью консоли SearchInform AlertCenter Console.

Открыть окно AlertCenter Client.

Формирование регулярных выражений

В соответствии с рис. 6.1–6.3 создать в библиотеке регулярных выражений новую группу с названием «Тестовые выражения».

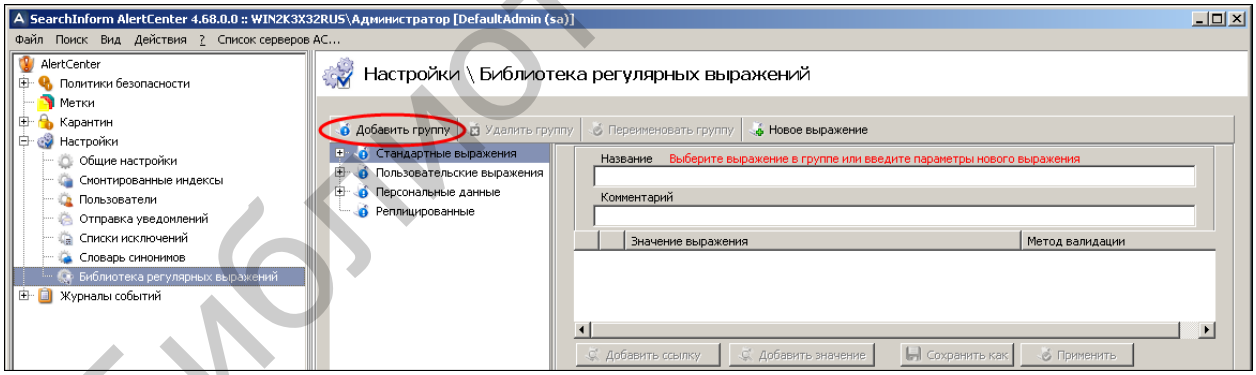


Рис. 6.1. Запрос на создание новой группы регулярных выражений

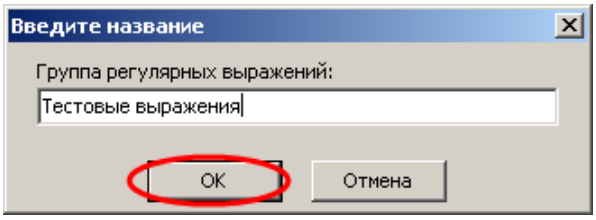


Рис. 6.2. Ввод имени группы

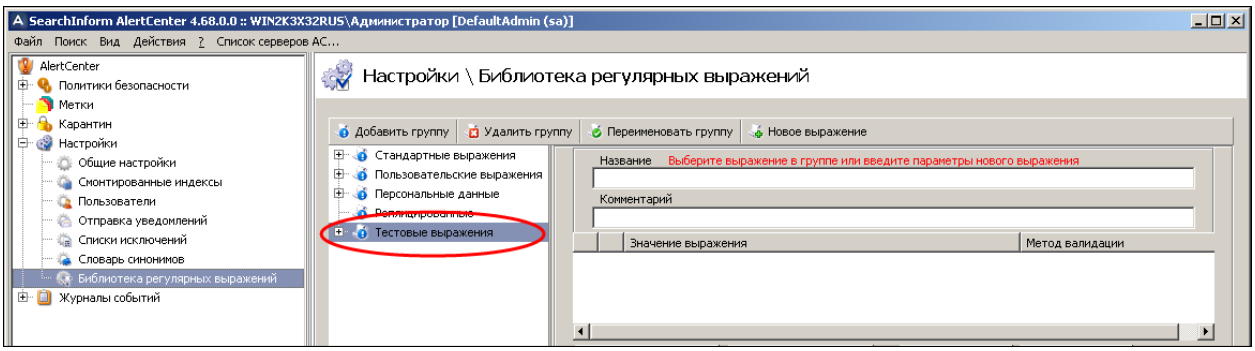


Рис. 6.3. Индикация созданной группы регулярных выражений

В соответствии с рис. 6.4–6.10 в группу «Тестовые выражения» добавить новое регулярное выражение «Новое 1», предназначенное для поиска документов, содержащих номера телефонов, т. е. строки типа «+7-924-111-11-34» (см. задачу примера №1). Текст регулярного выражения: \+[0-9-]+.

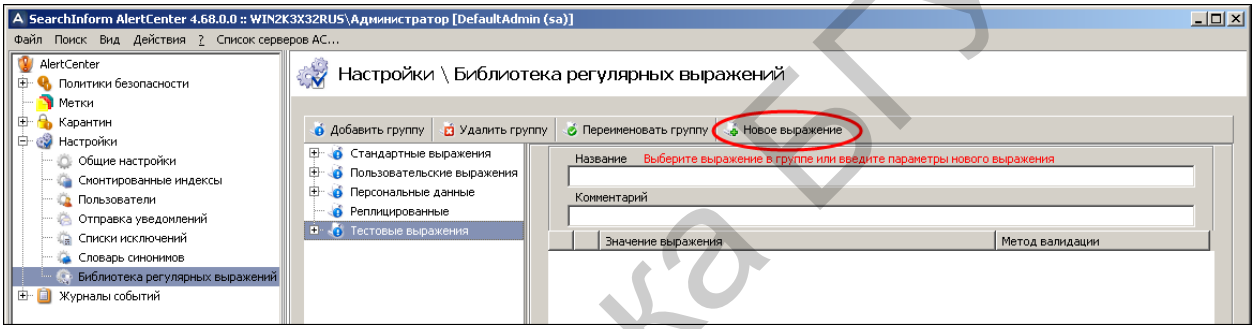


Рис. 6.4. Запрос на создание нового регулярного выражения

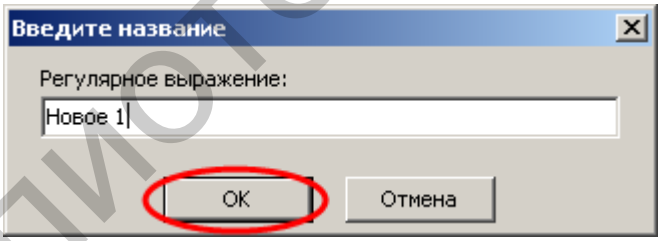


Рис. 6.5. Определение названия регулярного выражения

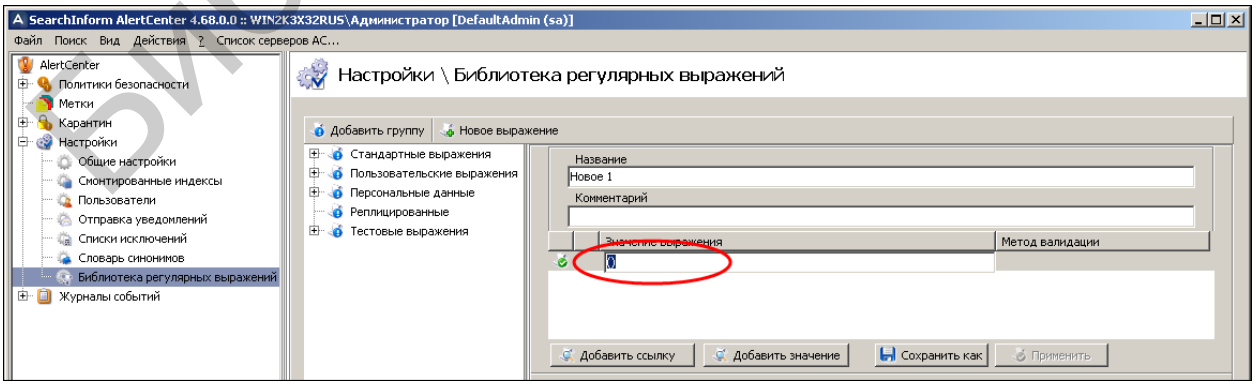


Рис. 6.6. Вход в режим записи текста выражения

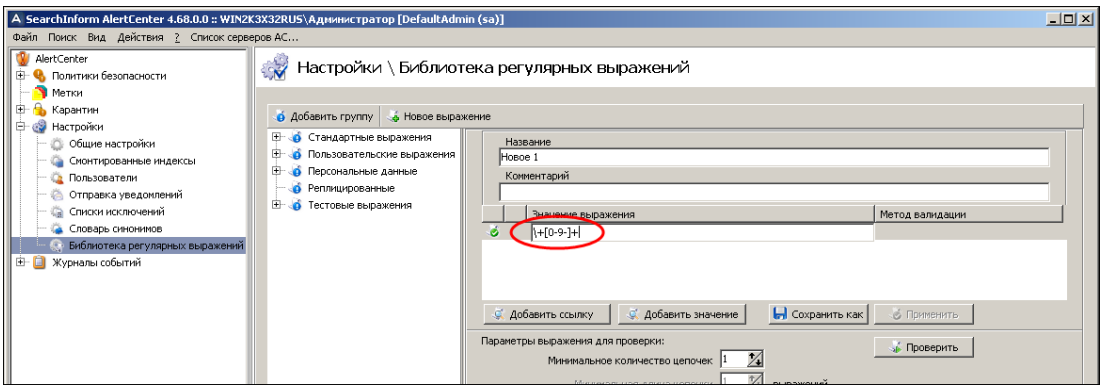


Рис. 6.7. Ввод текста выражения
(после ввода текста следует нажать клавишу Enter)

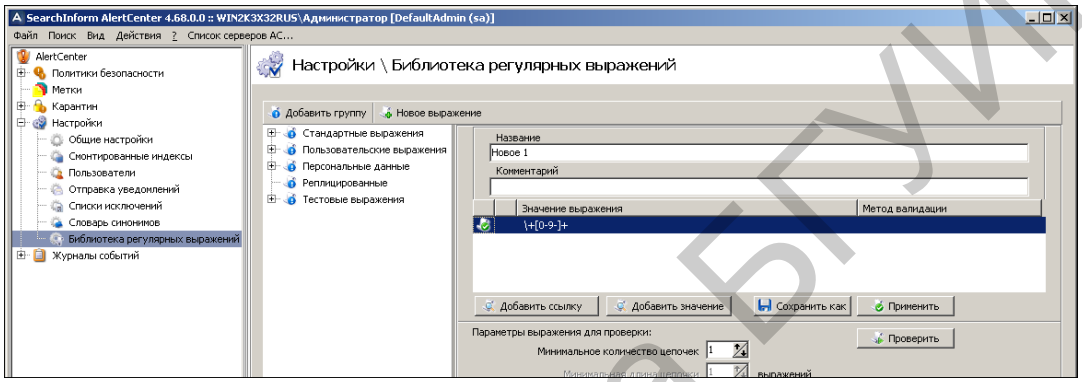


Рис. 6.8. Индикация текста выражения

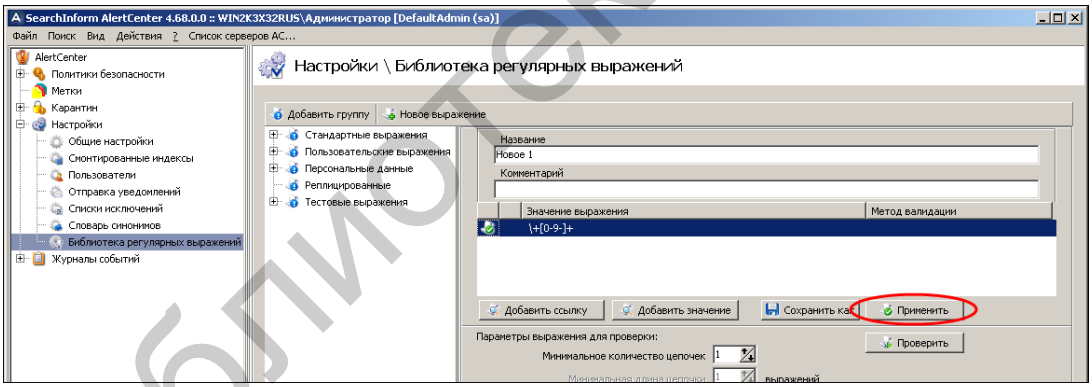


Рис. 6.9. Запись выражения

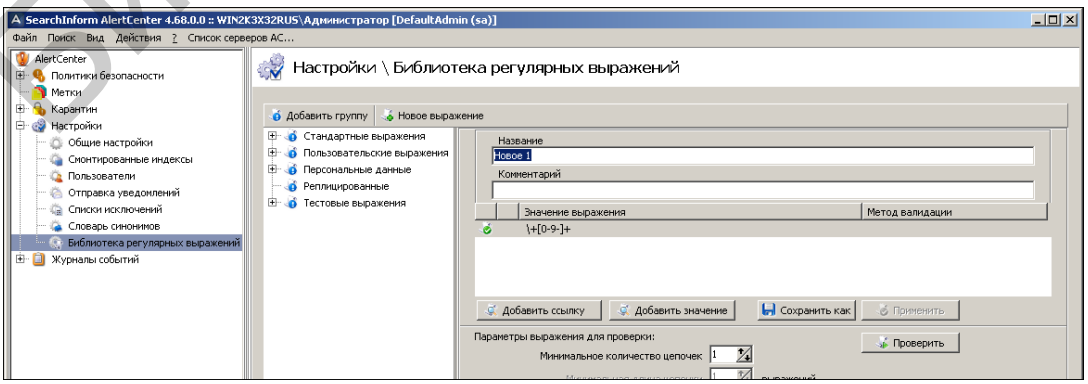


Рис. 6.10. Сформированное регулярное выражение «Новое 1»

В соответствии с рис. 6.11–6.14 проверить функциональность выражения «Новое 1» на следующем текстовом фрагменте: «В соответствии с рис. 1– в группу «Тестовые выражения» добавить новое регулярное выражение «Новое 1», предназначенное для поиска документов, содержащих номера телефонов, т. е. строки типа «+7-924-111-11-34» (Задача примера №1)».

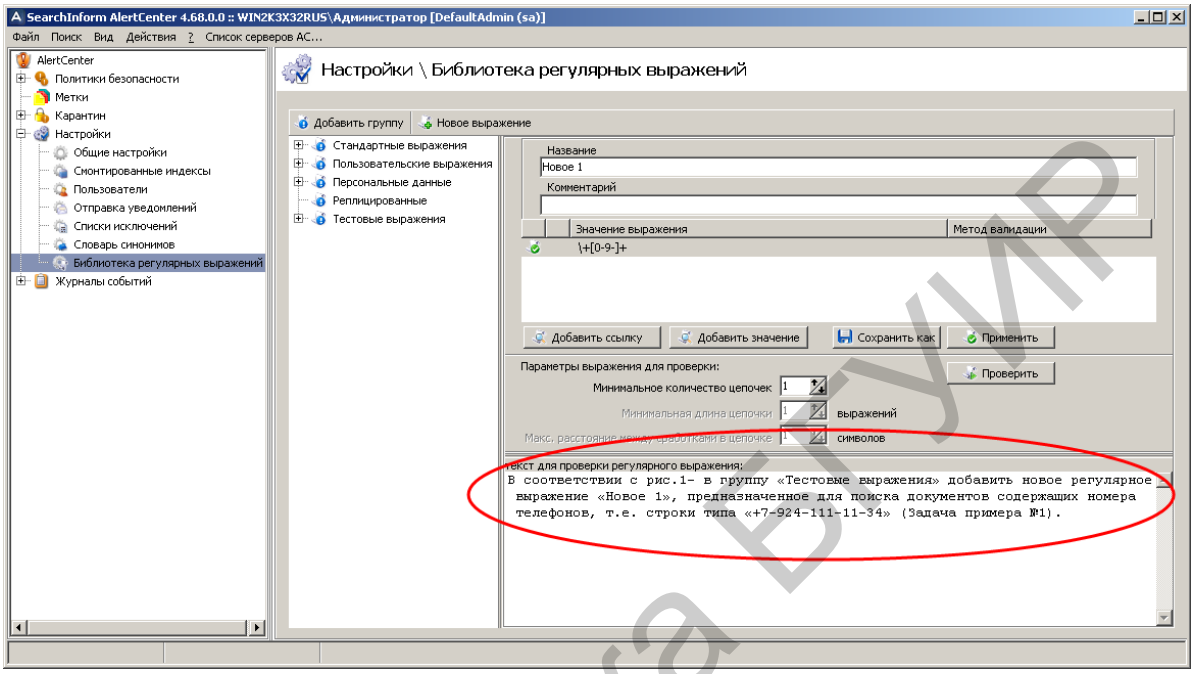


Рис. 6.11. Ввод проверочного текста

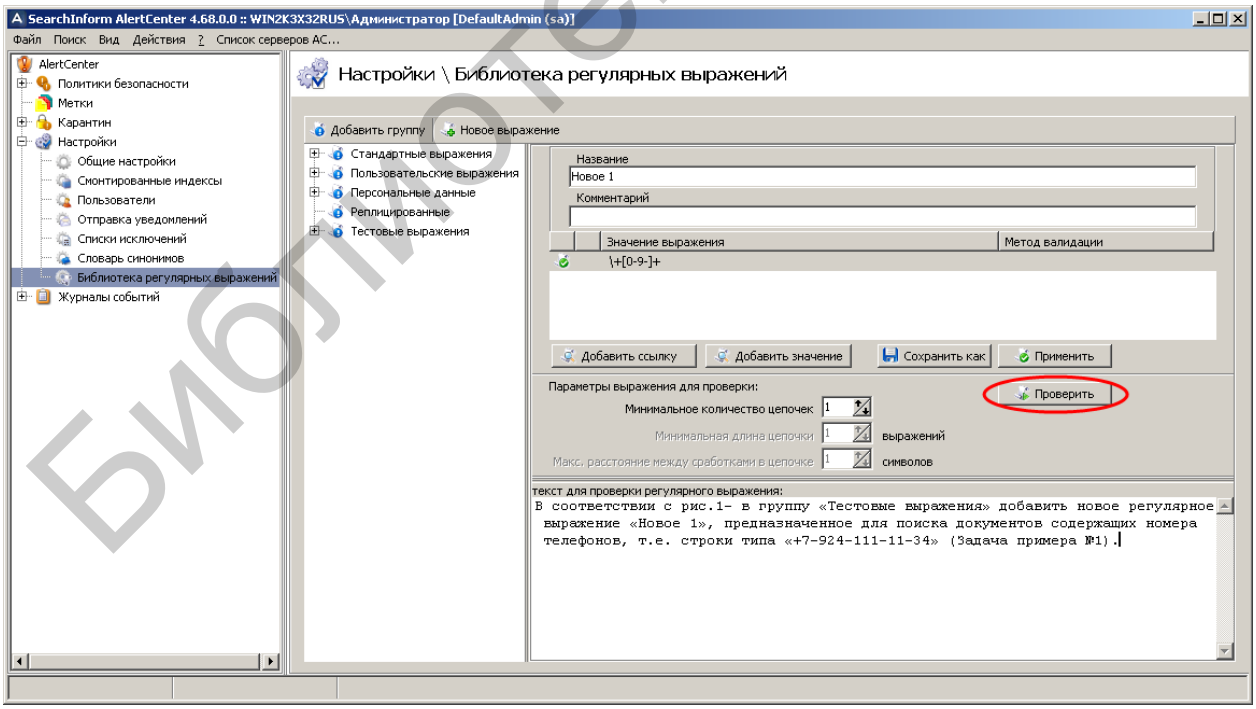


Рис. 6.12. Инициализация проверки

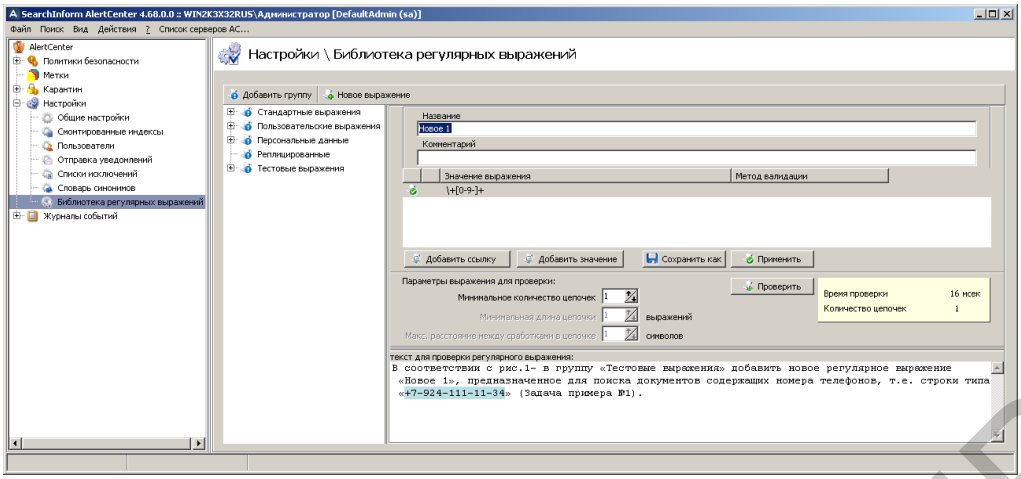


Рис. 6.13. Индикация результатов проверки

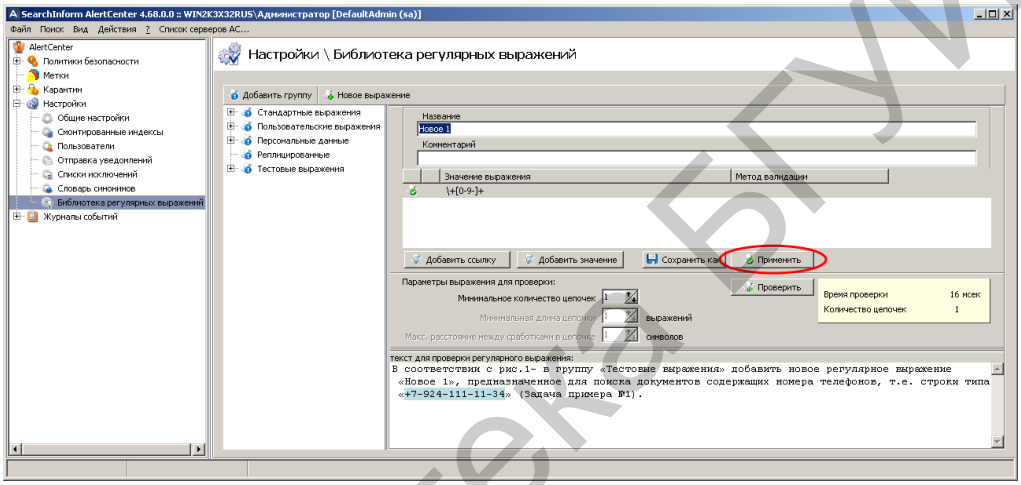


Рис. 6.14. Подтверждение редактирования выражения

В соответствии с рис. 6.15 и 6.16 проверить функциональность выражения «Новое 1», создав и выполнив соответствующий поисковый критерий. Отметим, что все поисковые критерии следует создавать в политике безопасности «Тест4».

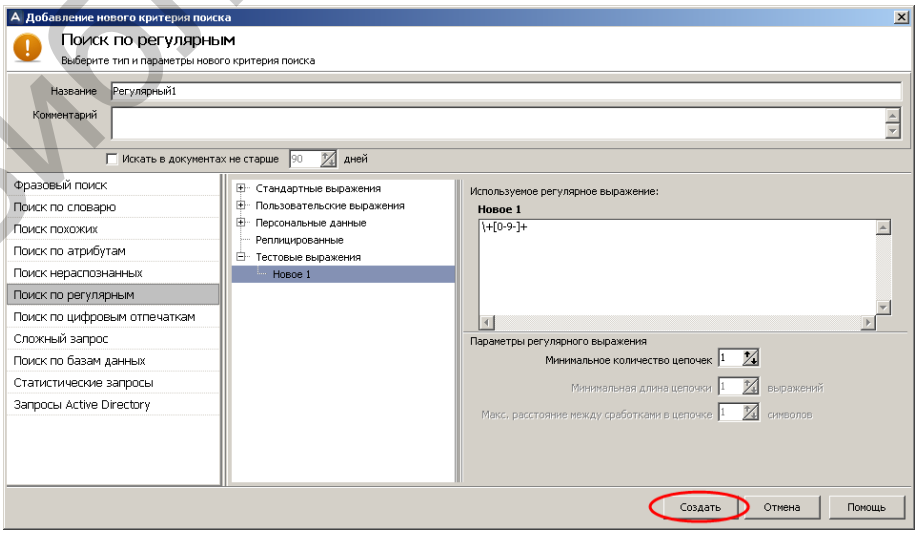


Рис. 6.15. Создание критерия «Регулярный1»

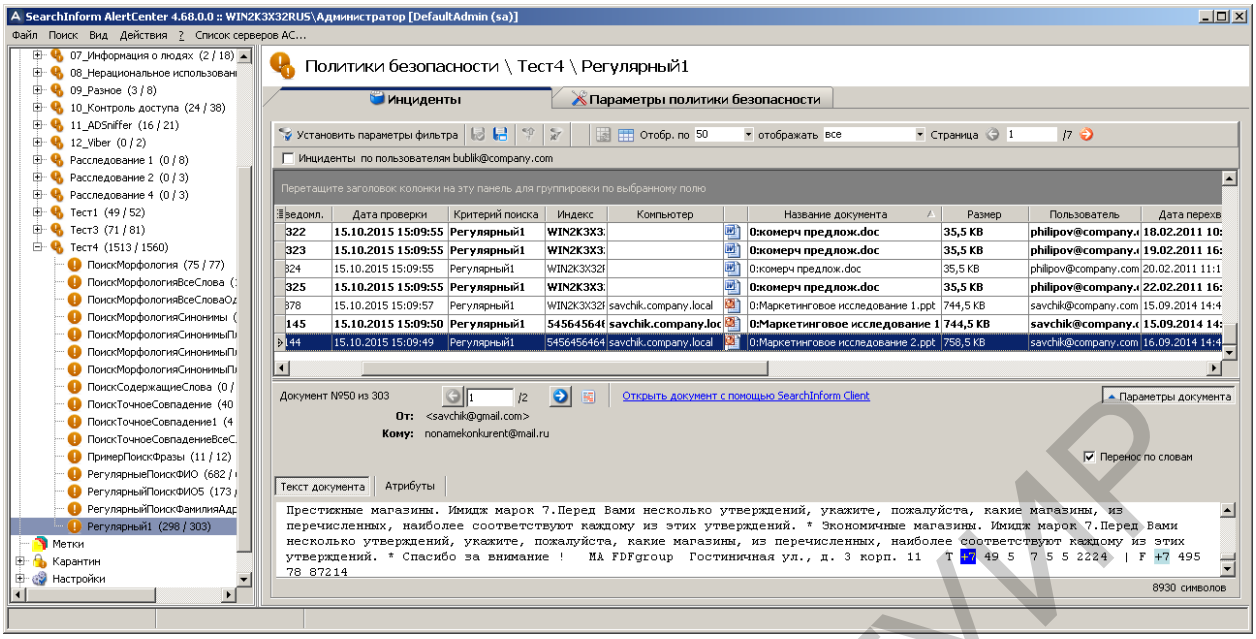


Рис. 6.16. Индикация инцидентов по критерию «Регулярный1»

Задание 1. Создать регулярное выражение для поиска документов, соответствующих примеру №2. Произвести поиск, сформировав соответствующий поисковый критерий. Отметим, что все регулярные выражения следует создавать в группе «Тестовые выражения».

Задание 2. Создать регулярное выражение для поиска документов, в которых содержатся цифры. Произвести поиск, сформировав соответствующий поисковый критерий.

Текст регулярного выражения: -?\d+.

Задание 3. Создать регулярное выражение для поиска документов, в которых содержится дробное число (число, содержащее целую и дробную часть, разделенную точкой или запятой). Произвести поиск, сформировав соответствующий поисковый критерий.

Текст регулярного выражения: \d+)([.,])(\d+.

Задание 4. Создать регулярное выражение для поиска документов, в которых содержится определение ссылки в виде http://www.rambler.ru, ftp://rambler.ru, www.rambler.ru. Произвести поиск, сформировав соответствующий поисковый критерий.

Текст регулярного выражения:

((http|ftp)://([\w\d]+(\.[\w\d\]+)+)(([\w\d\=\?\\\./]+)+))|(([\w\d]+(\.[\w\d\]+)+)(([\w\d\=\?\\\./]+)+)).

Задание 5. Создать регулярное выражение для поиска документов, в которых содержится 20-значный номер банковского счета. Произвести поиск, сформировав соответствующий поисковый критерий.

Текст регулярного выражения: \b(\d{20})\b.

Задание 6. Создать регулярное выражение для поиска документов, в которых содержатся имена текстовых файлов. Произвести поиск, сформировав

соответствующий поисковый критерий. Отметим, что запись «(?i)» указывает на нечуствительность к регистру. Текст регулярного выражения: (?i).txt.

2. Выполнить настройку сетевого соединения между виртуальным и основным компьютерами следующим образом. В соответствии с рис. 6.17–6.23 настроить параметры сетевых соединений виртуального компьютера.

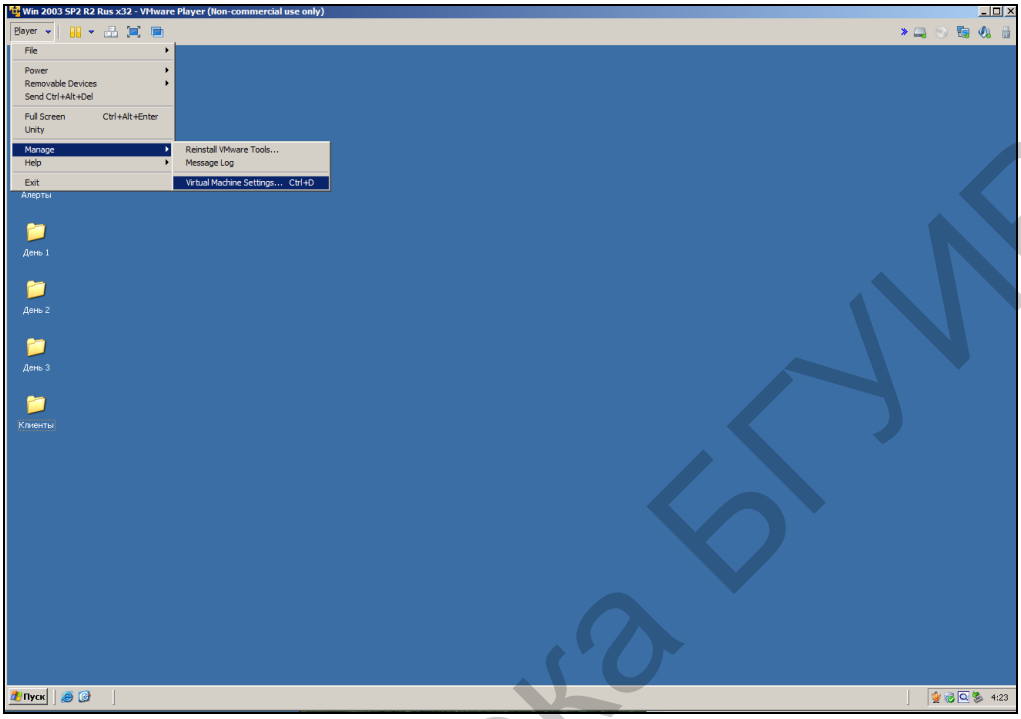


Рис. 6.17. Вход в режим редактирования настроек виртуального компьютера

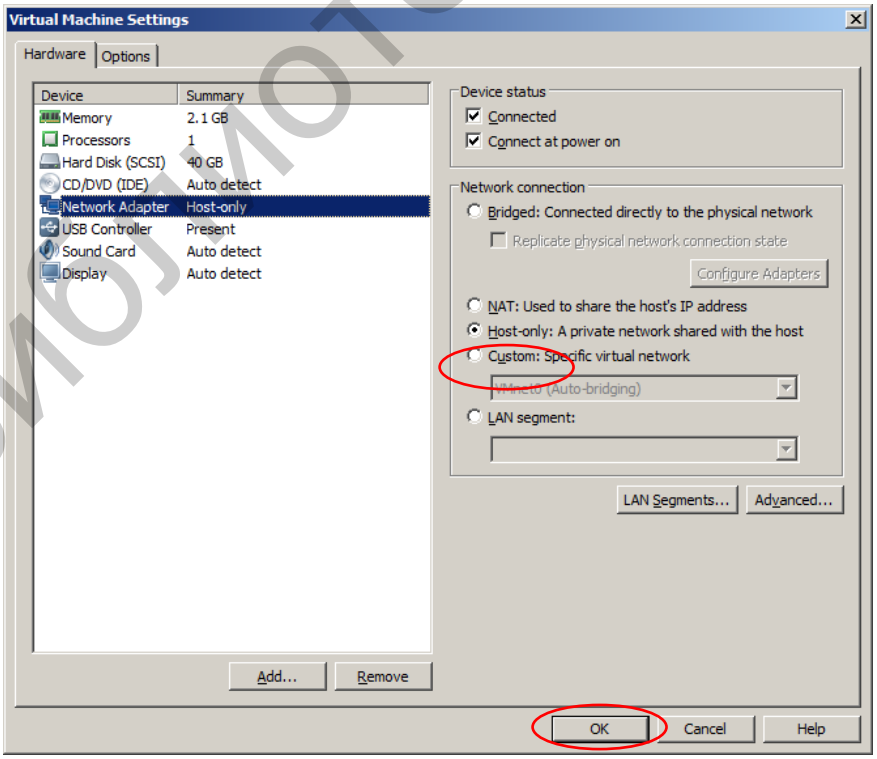


Рис. 6.18. Настройка сетевого адаптера виртуального компьютера

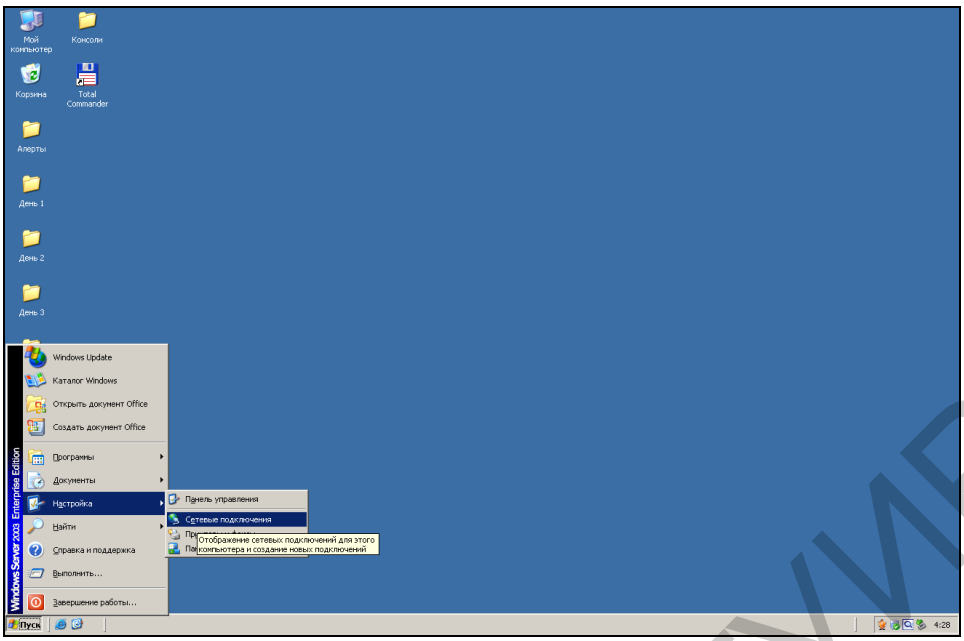


Рис. 6.19. Вход в режим редактирования сетевых подключений виртуального компьютера

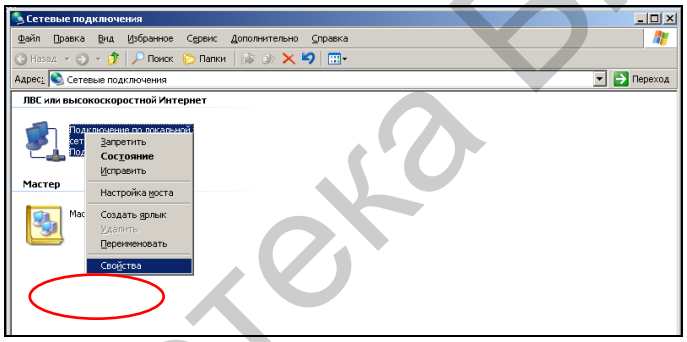


Рис. 6.20. Вход в режим изменения свойств сетевых соединений ОС виртуального компьютера

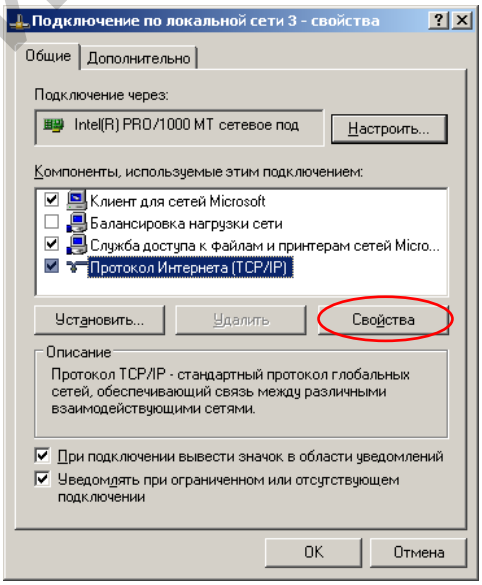


Рис. 6.21. Окно изменения свойств протокола TCP/IP ОС виртуального компьютера

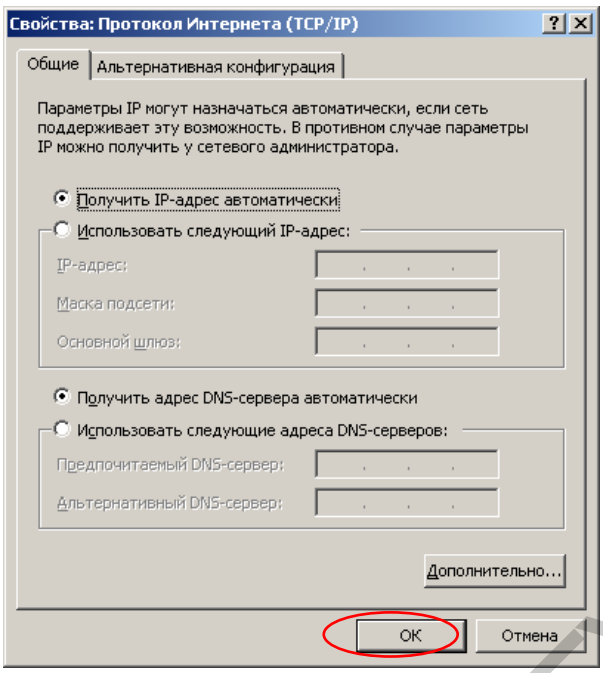


Рис. 6.22. Настройка протокола TCP/IP ОС виртуального компьютера

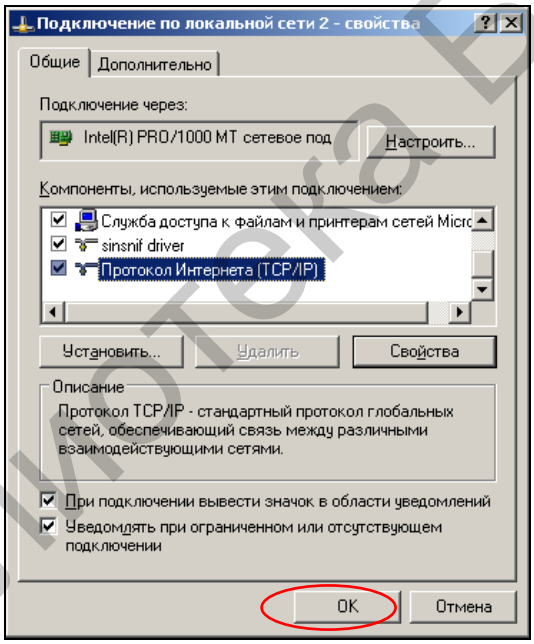


Рис. 6.23. Подтверждение настроек

На виртуальном компьютере откройте консоль «Администрирование». Для этого последовательно выполните команды: Пуск→Настройка→Панель управления→Администрирование.

В соответствии с рис. 6.24 откройте консоль «Локальная политика безопасности».

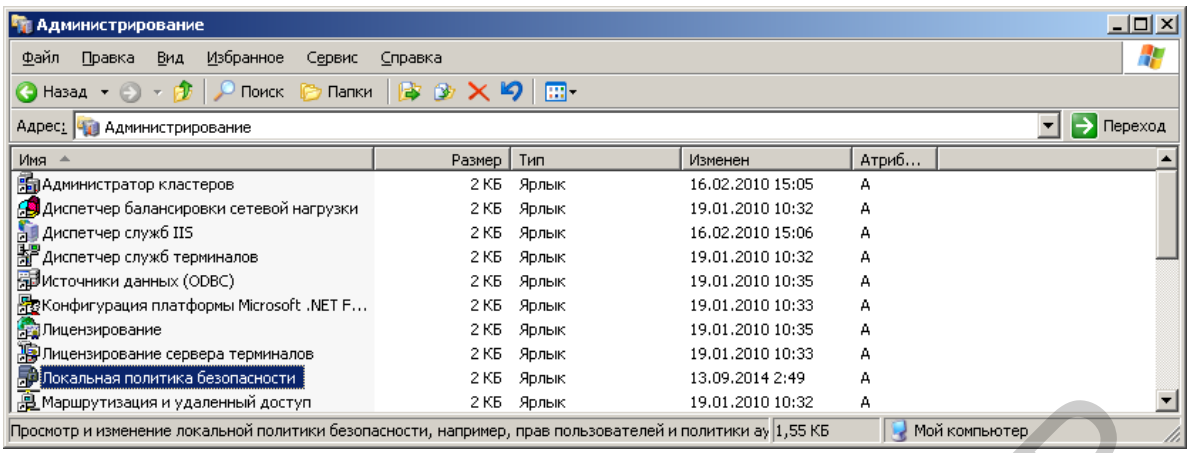


Рис. 6.24. Запуск консоли «Локальная политика безопасности»

В соответствии с рис. 6.25–6.32 настройте права доступа к сетевым ресурсам виртуального компьютера.

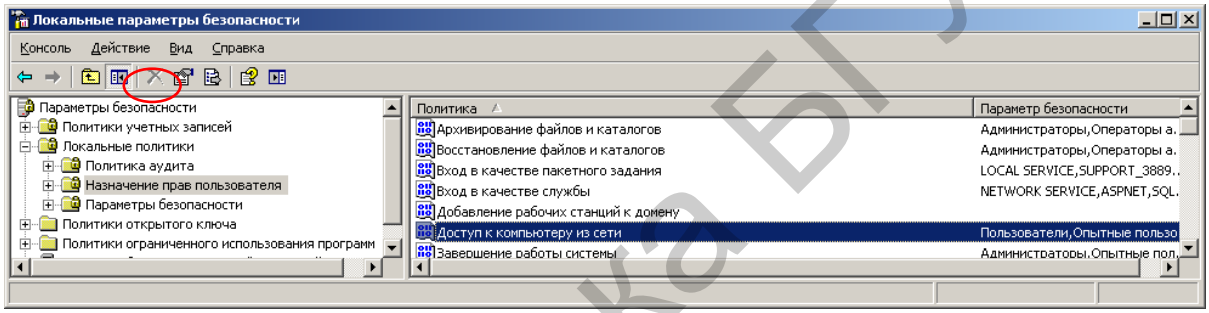


Рис. 6.25. Редактирование прав доступа к комьютеру из сети в окне «Локальные параметры безопасности» ОС виртуального компьютера

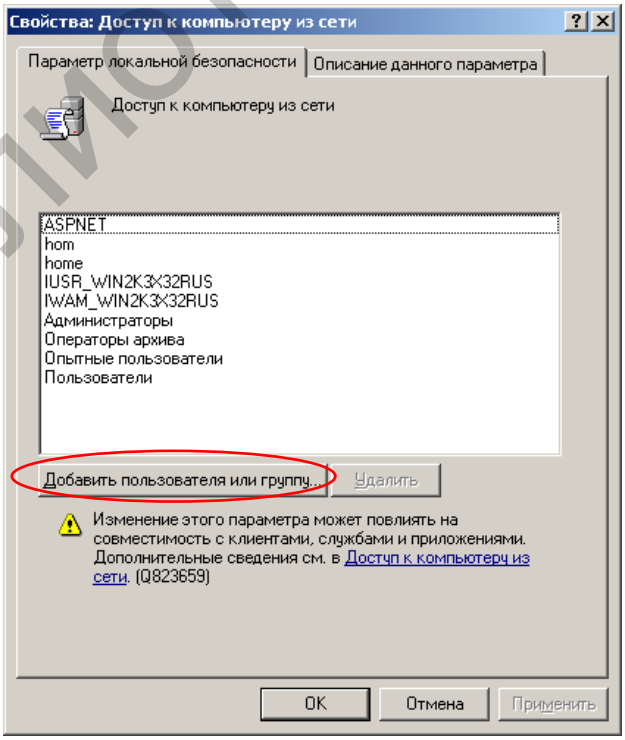


Рис. 6.26. Первый этап добавления пользователя «Все»

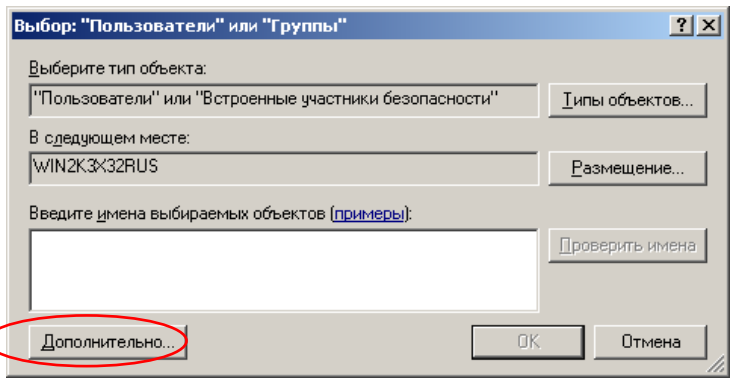


Рис. 6.27. Второй этап добавления пользователя «Все»

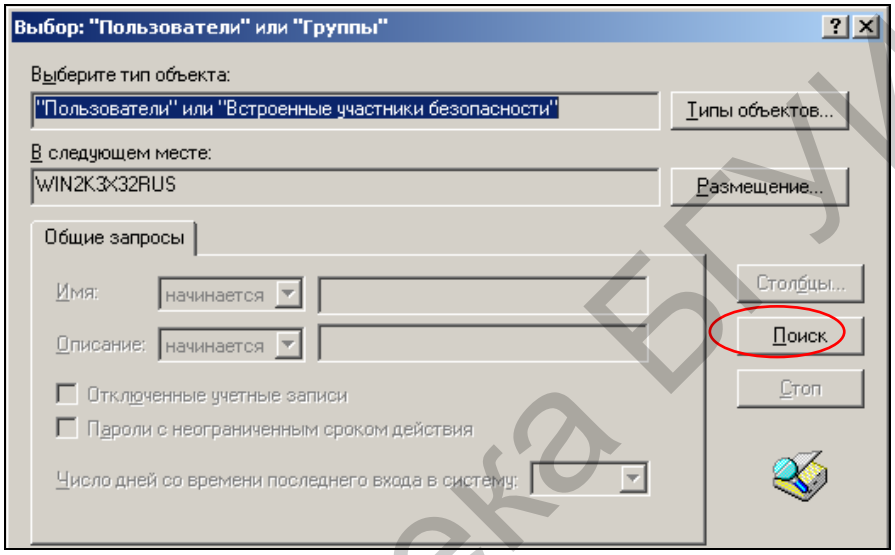


Рис. 6.28. Третий этап добавления пользователя «Все»

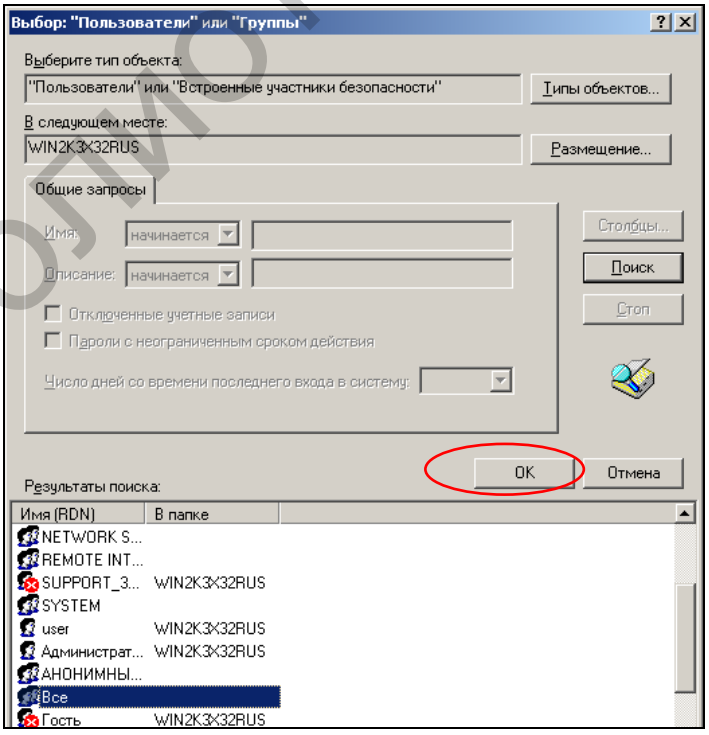


Рис. 6.29. Четвертый этап добавления пользователя «Все»

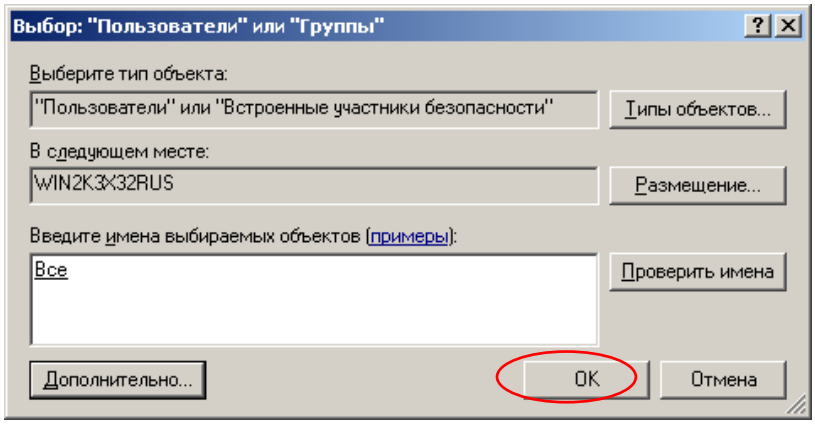


Рис. 6.30. Пятый этап добавления пользователя «Все»

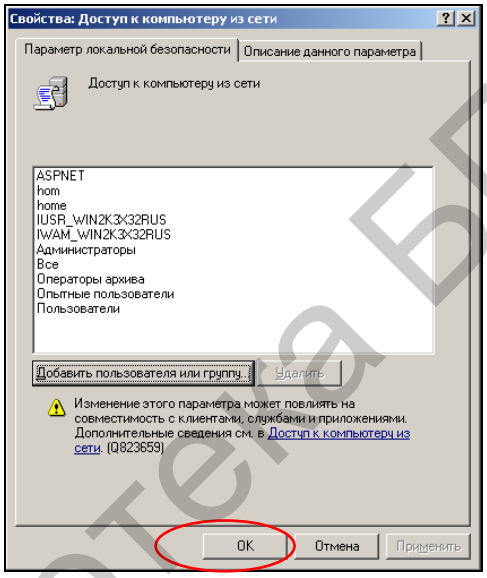


Рис. 6.31. Шестой этап добавления пользователя «Все»

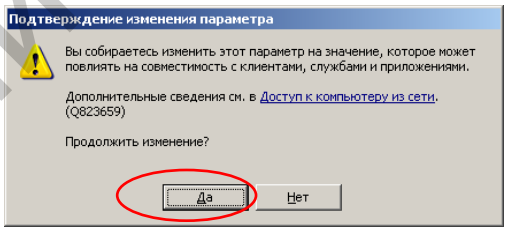


Рис. 6.32. Заключительный этап добавления пользователя «Все»

Закрыть окно «Локальные параметры безопасности».

На виртуальном компьютере войти в режим редактирования настроек брандмауэра Windows (соответствующий ярлык находится в панели управления).

В соответствии с рис. 6.33 отключить брандмауэр виртуального компьютера.

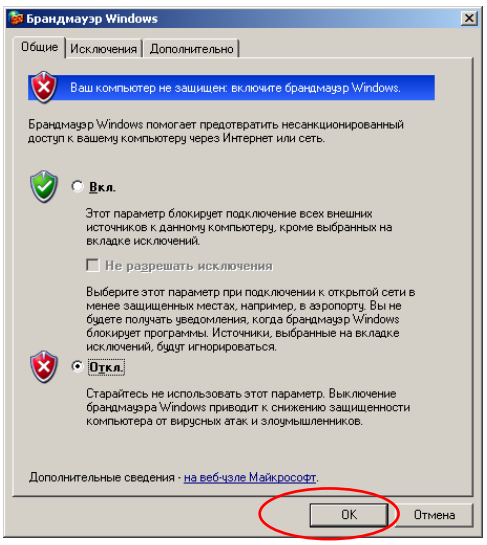


Рис. 6.33. Отключение брандмауэра ОС виртуального компьютера

Отключить брандмауэр ОС основного компьютера.

Войти в режим просмотра сетевых подключений основного компьютера.

В соответствии с рис. 6.34 и 6.35 убедиться в наличии сетевых подключений виртуального компьютера к основному. В данном случае подразумевается, что основной компьютер работает под управлением ОС Windows 7.

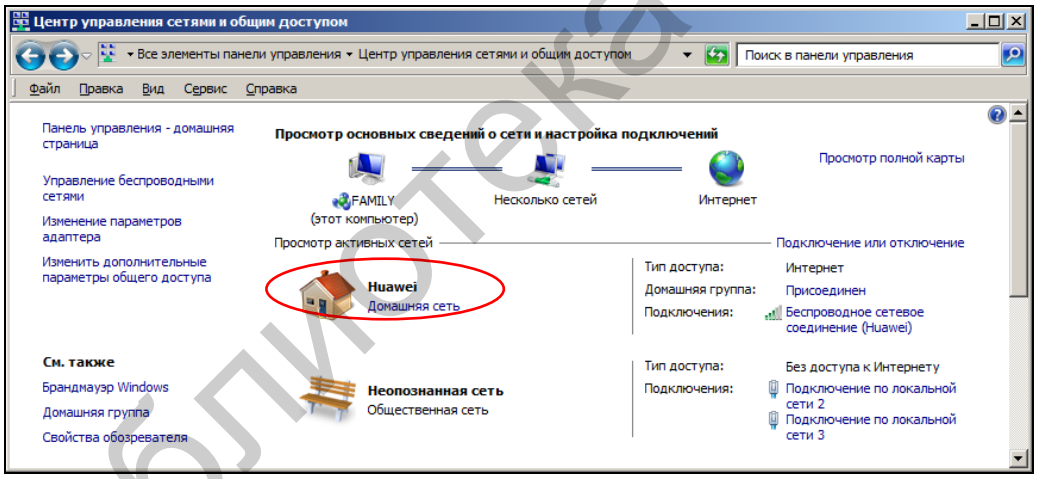


Рис. 6.34. Сетевые подключения основного компьютера

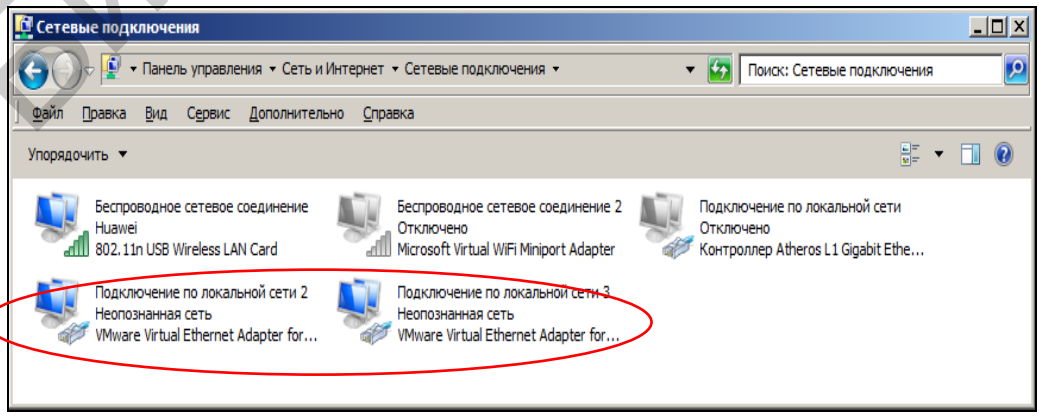


Рис. 6.35. Сетевые подключения основного и виртуального компьютера

В соответствии с рис. 6.36 и 6.37 определить IP-адреса основного и виртуального компьютера. Для этого необходимо воспользоваться командной строкой основного и виртуального компьютера.

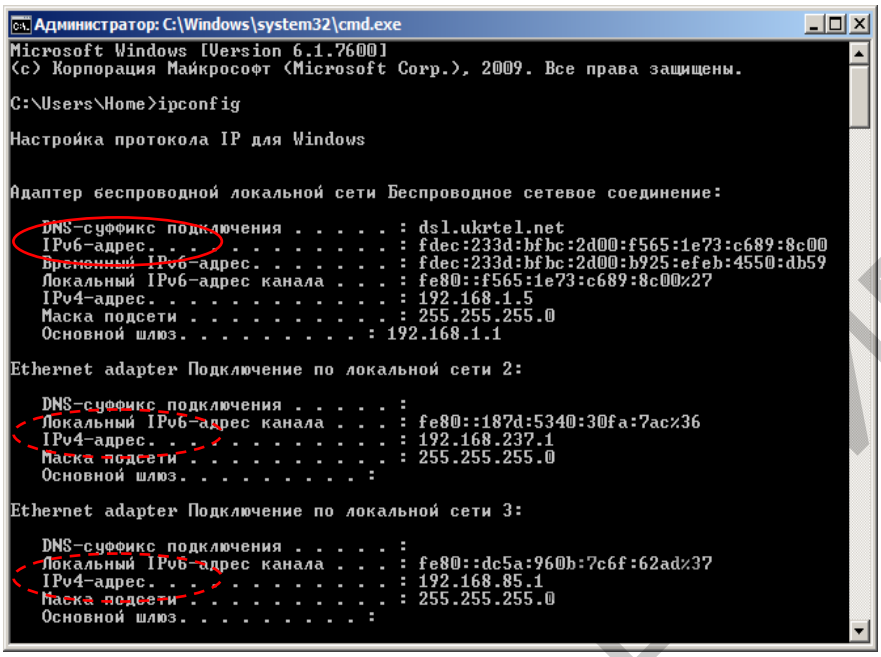


Рис. 6.36. Определение IP-адресов основного компьютера

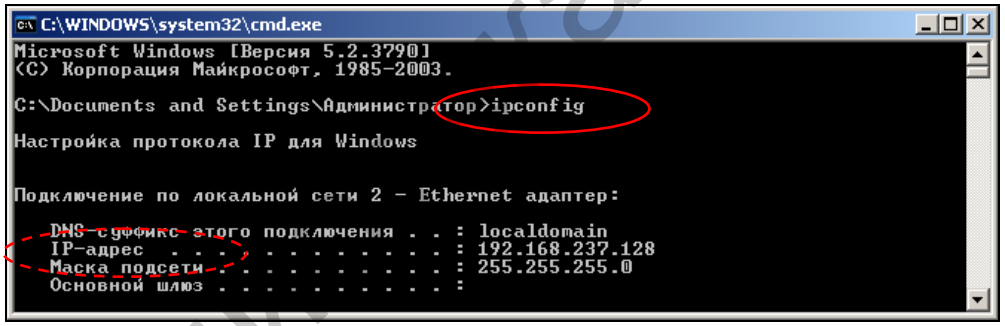


Рис. 6.37. Определение IP-адреса виртуального компьютера

В соответствии с рис. 6.38 и 6.39 убедиться в работоспособности сети между виртуальным и основным компьютером.

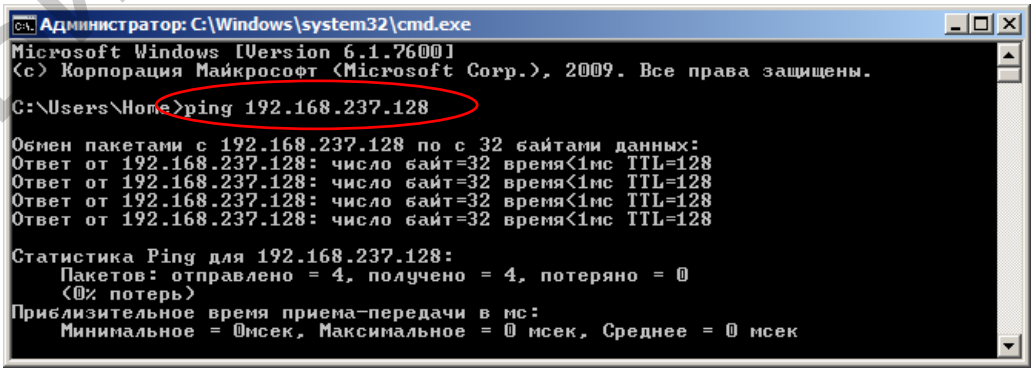


Рис. 6.38. Запуск проверки сети с основного компьютера

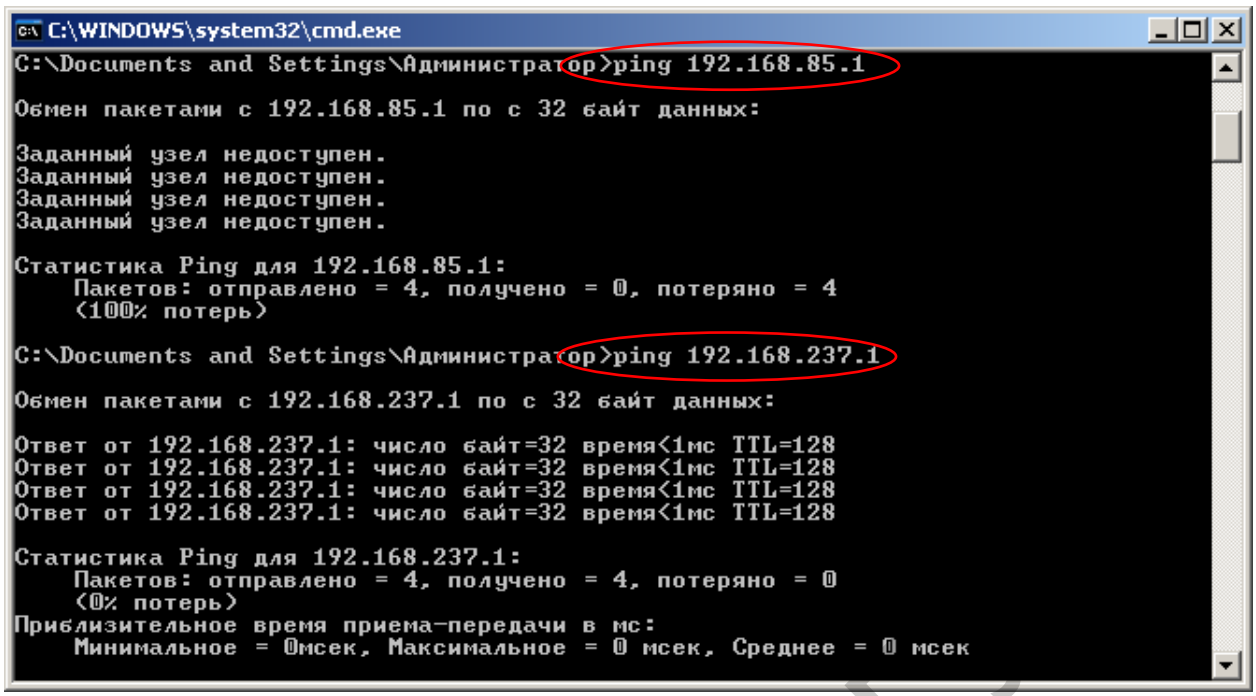


Рис. 6.39. Запуск проверки сети с виртуального компьютера

Таким образом, основной компьютер доступен с виртуального по IP-адресу 192.168.237.1, а виртуальный компьютер доступен с основного по IP-адресу 192.168.237.128.

В соответствии с рис. 6.40 и 6.41 настроить веб-сервер основного компьютера. Убедиться в том, что веб-сервер запущен. Отметим, что использование веб-серверов не является обязательным условием для настройки службы перехвата программного комплекса SearchInform. Однако в противном случае несколько теряется наглядность полученных результатов.

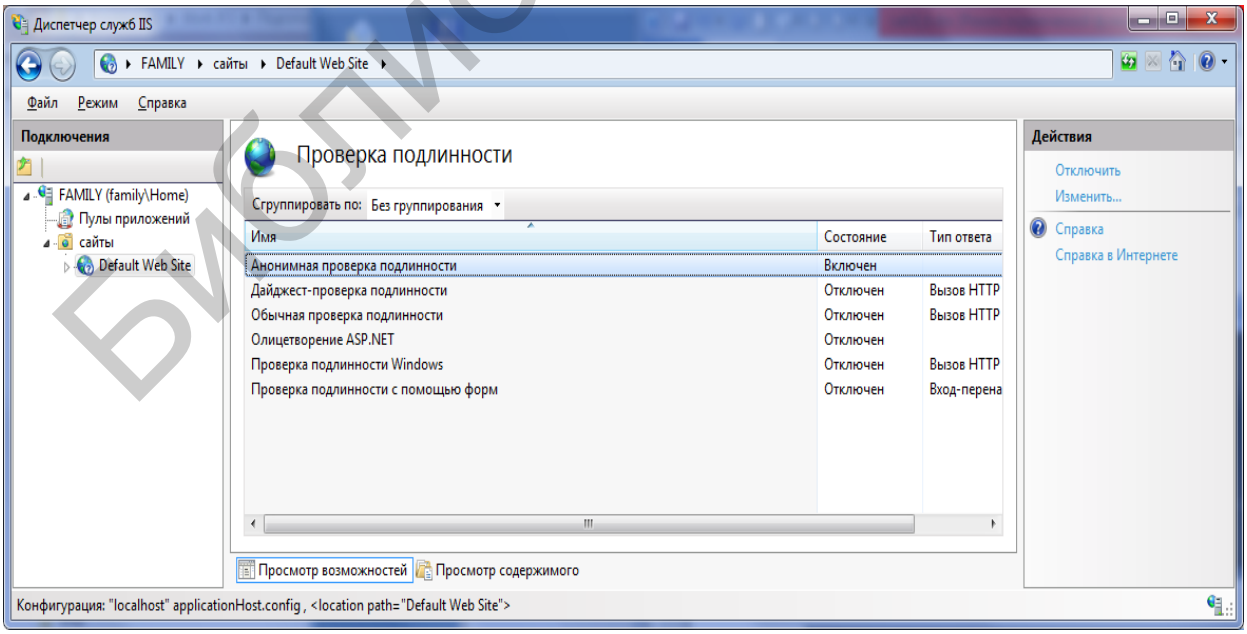


Рис. 6.40. Первый этап настройки веб-сервера основного компьютера

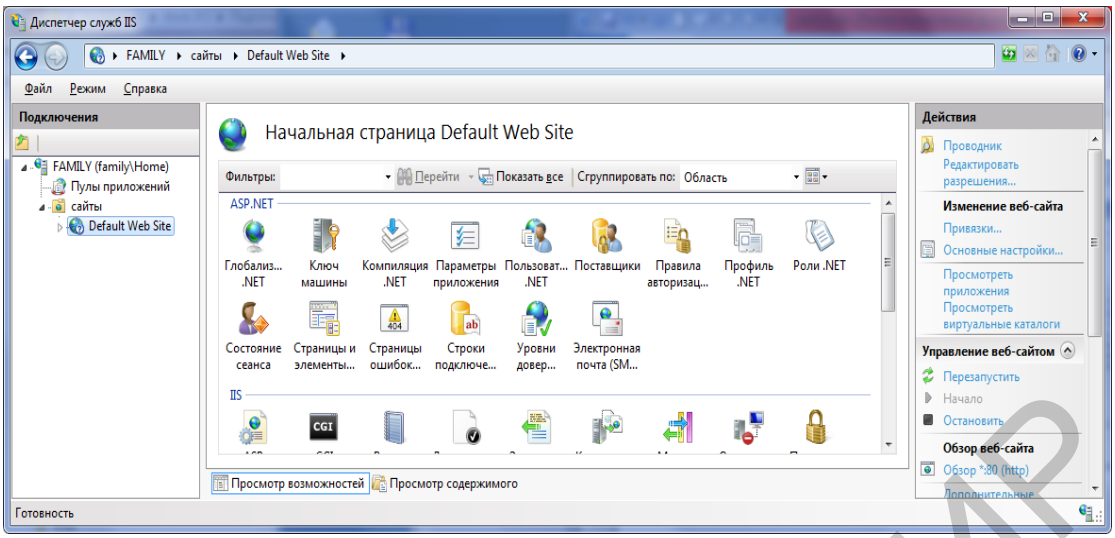


Рис. 6.41. Второй этап настройки веб-сервера основного компьютера

В соответствии с рис. 6.42 настроить сетевые подключения браузеров основного и виртуального компьютера.

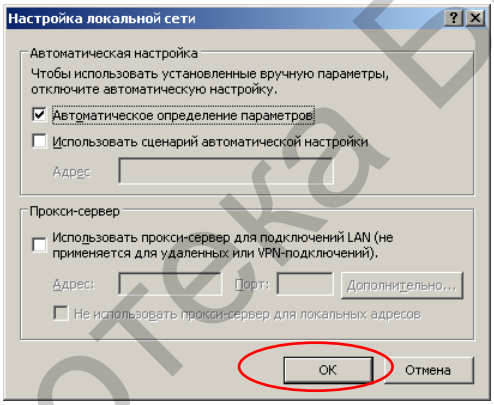


Рис. 6.42. Настройка сетевых подключений браузера

В соответствии с рис. 6.43 с помощью браузера виртуального компьютера проверить доступность веб-сервера основного компьютера.

Рис. 6.43. Отображение начальной страницы веб-сайта основного компьютера

В соответствии с рис. 6.44–6.46 настроить веб-сервер виртуального компьютера.

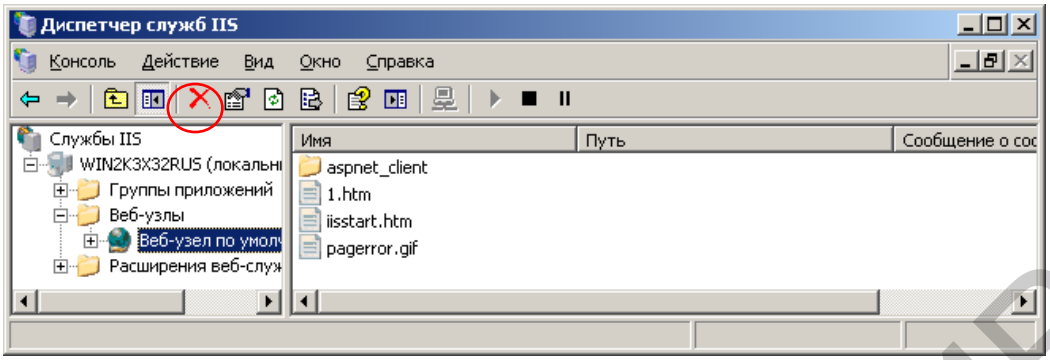


Рис. 6.44. Вход в режим изменения свойств веб-сервера виртуального компьютера

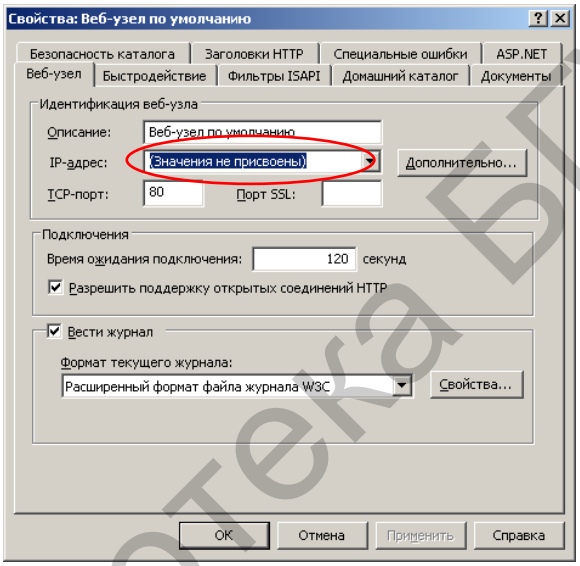


Рис. 6.45. Первый этап добавления IP-адреса

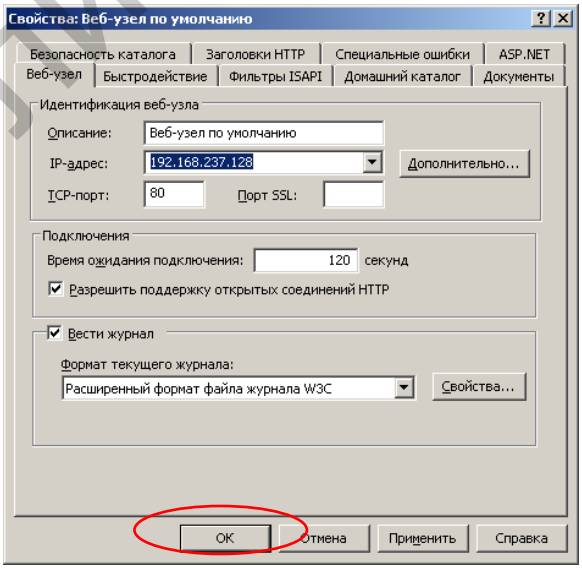


Рис. 6.46. Второй этап добавления IP-адреса

Перезапустить веб-сервер виртуального компьютера.

В соответствии с рис. 6.47, запустив браузер основного компьютера, убедиться в доступности веб-сервера виртуального компьютера.

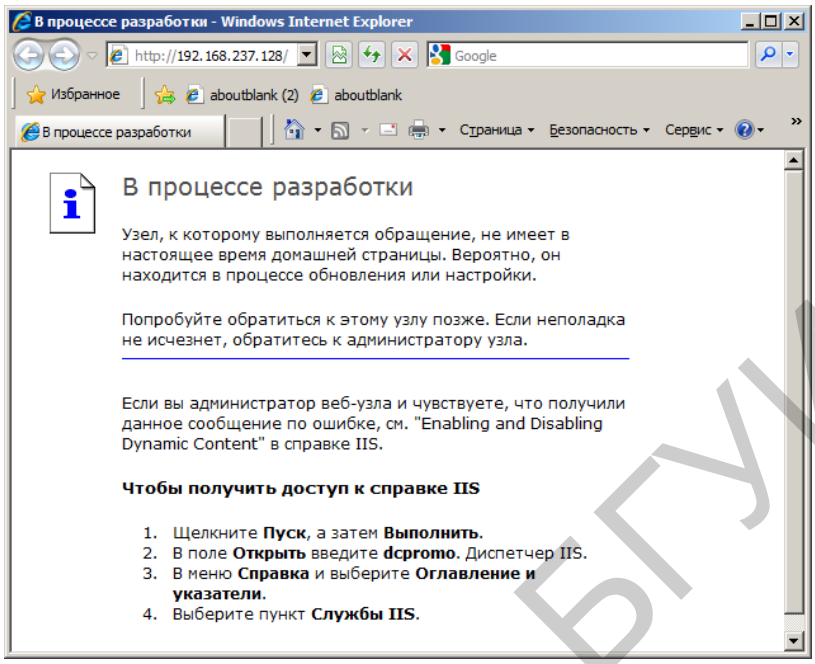


Рис. 6.47. Первоначальная страница сайта виртуального компьютера

В соответствии с рис. 6.48 убедиться, что службой перехвата контролируется сетевой адаптер, используемый для связи с виртуальным компьютером.

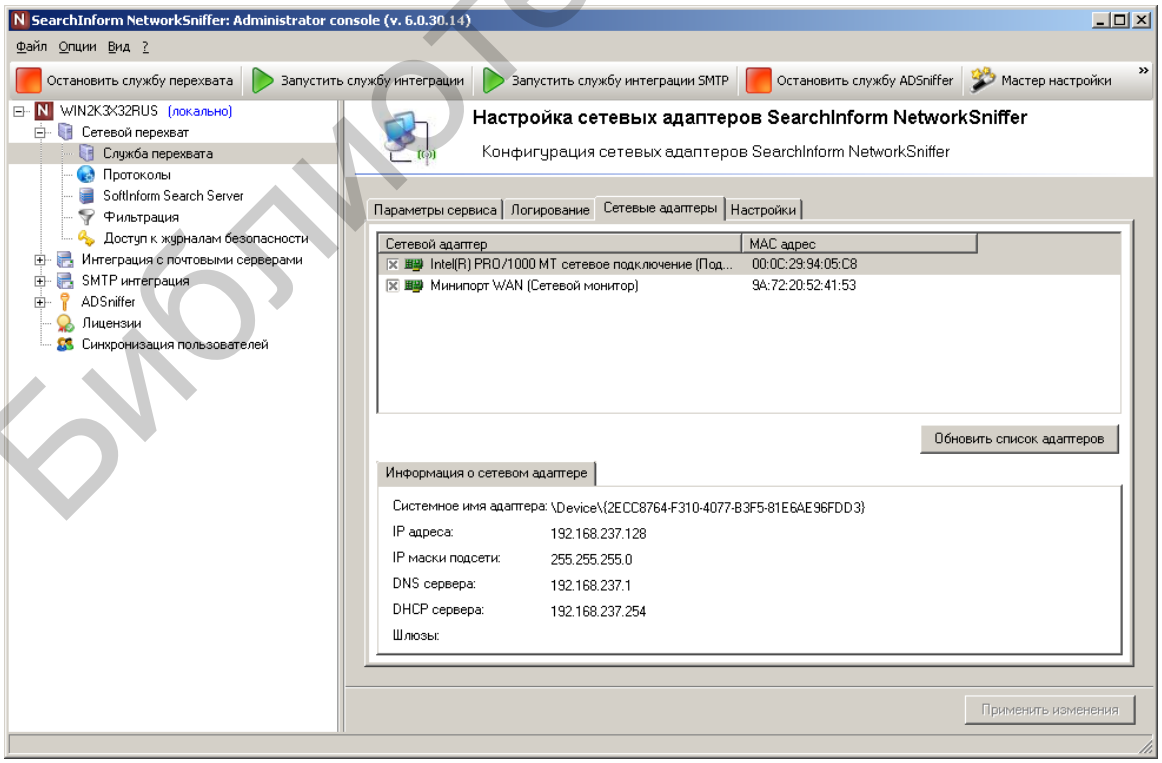


Рис. 6.48. Индикация контролируемых сетевых адаптеров

В соответствии с рис. 6.49 и 6.50 выключить фильтрацию службы перехвата.

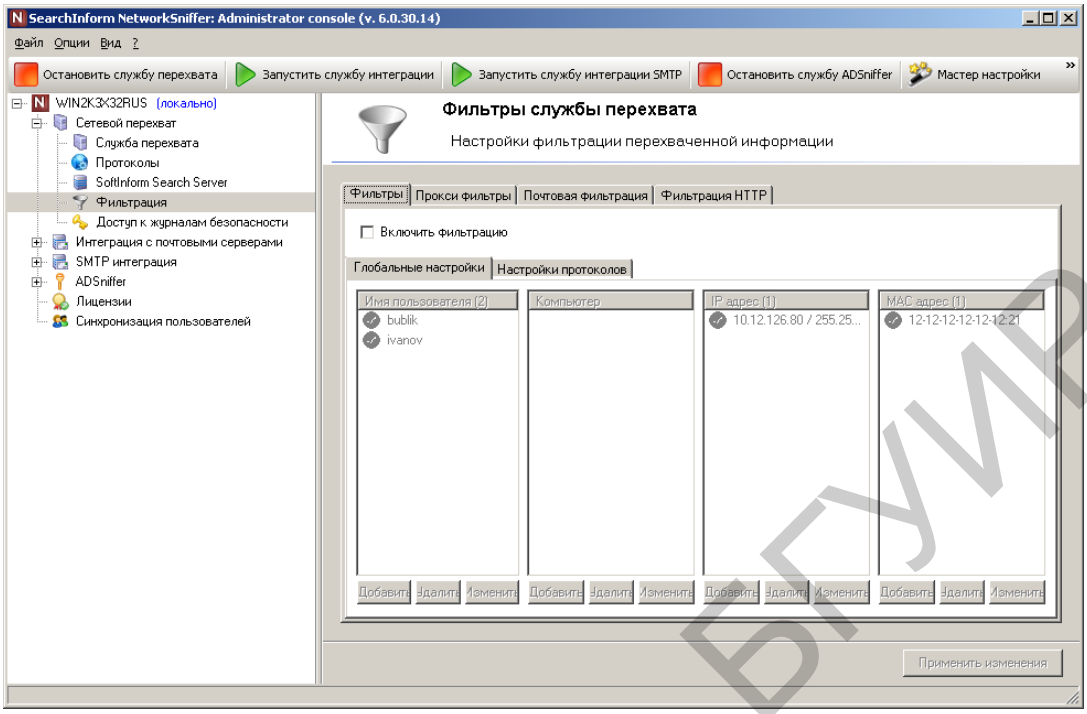


Рис. 6.49. Выключение общей фильтрации

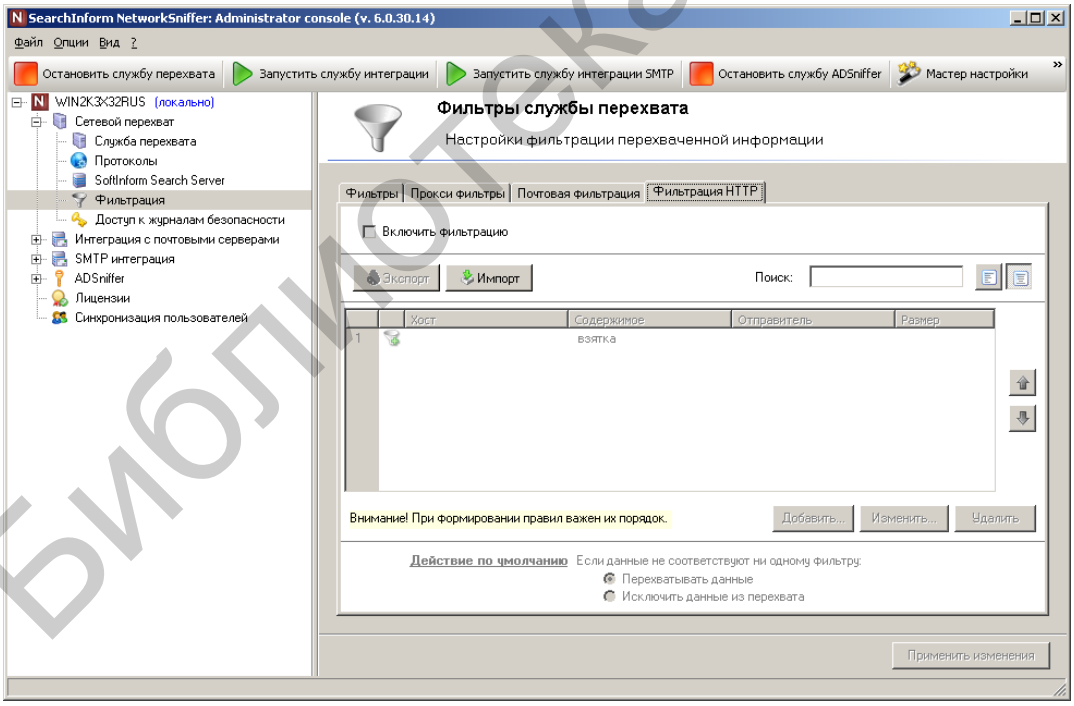


Рис. 6.50. Выключение фильтрации HTTP

Создать новую политику безопасности «Тест5» и добавить в нее индекс «NetworkPost». В соответствии с рис. 6.51 создать новый критерий, предусматривающий поиск информации, переданной по сети по протоколу HTTP методом POST не позже одного дня назад.

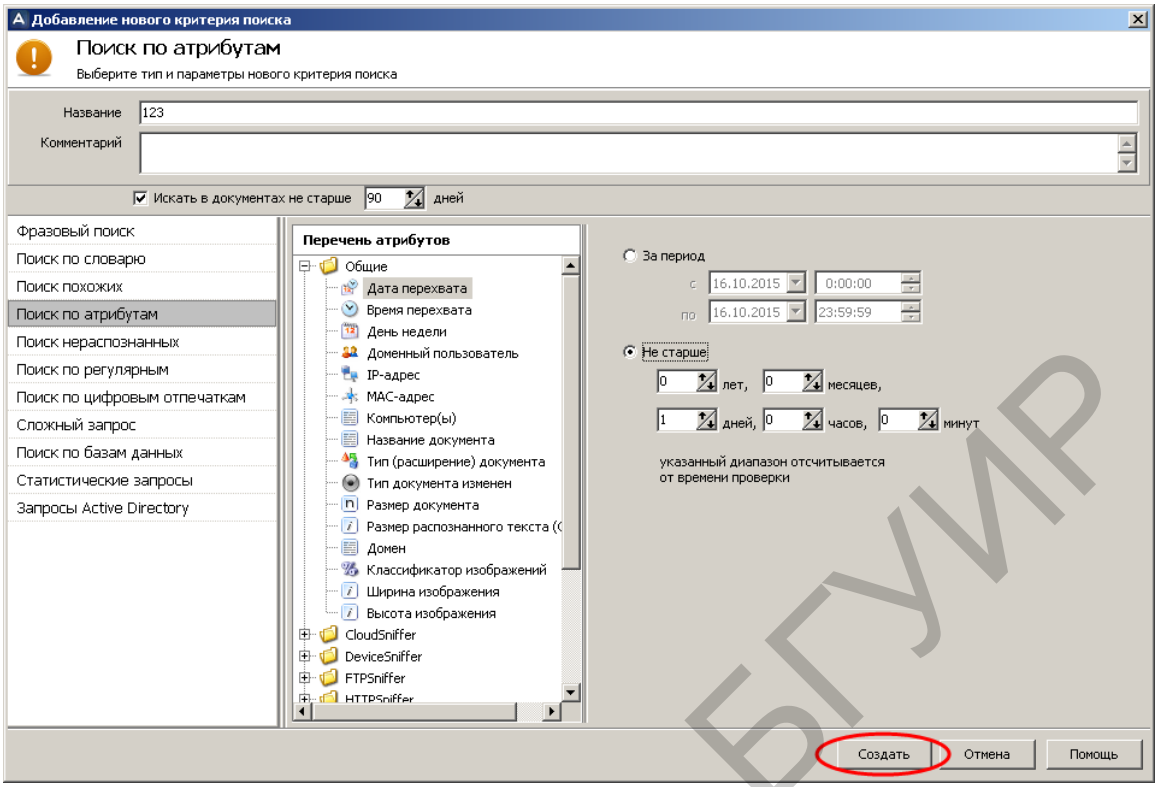


Рис. 6.51. Создание критерия поиска «123»

На виртуальном компьютере создать текстовый документ с названием «1.htm». Открыв документ «1.htm» программой «Блокнот», записать в него текст, показанный на рис. 6.52. После этого документ следует сохранить и закрыть.

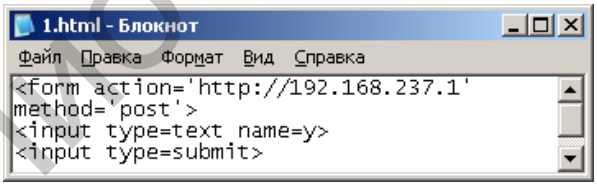


Рис. 6.52. Код веб-страницы

В соответствии с рис. 6.53 и 6.54, открыв документ «1.htm» с помощью браузера, передать на основной компьютер по протоколу HTTP методом POST текст «Hello World!». Если после подачи запроса окно браузера соответствует рис. 6.55, значит, текст был успешно передан.

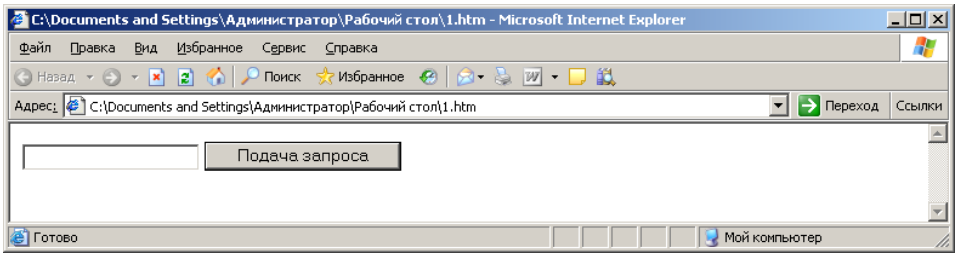


Рис. 6.53. Окно веб-страницы

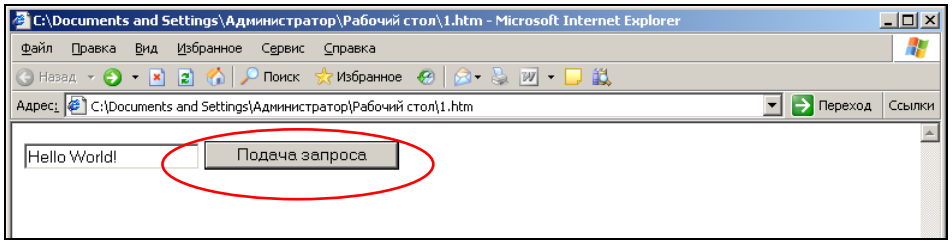


Рис. 6.54. Передача запроса

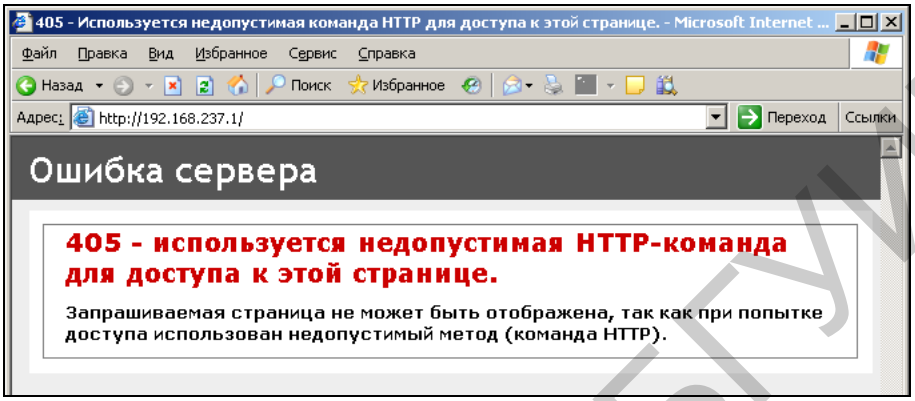


Рис. 6.55. Индикация успешной передачи текста

В соответствии с рис. 6.56 с помощью консоли Search Server Console провести обновление индекса Network_POST.

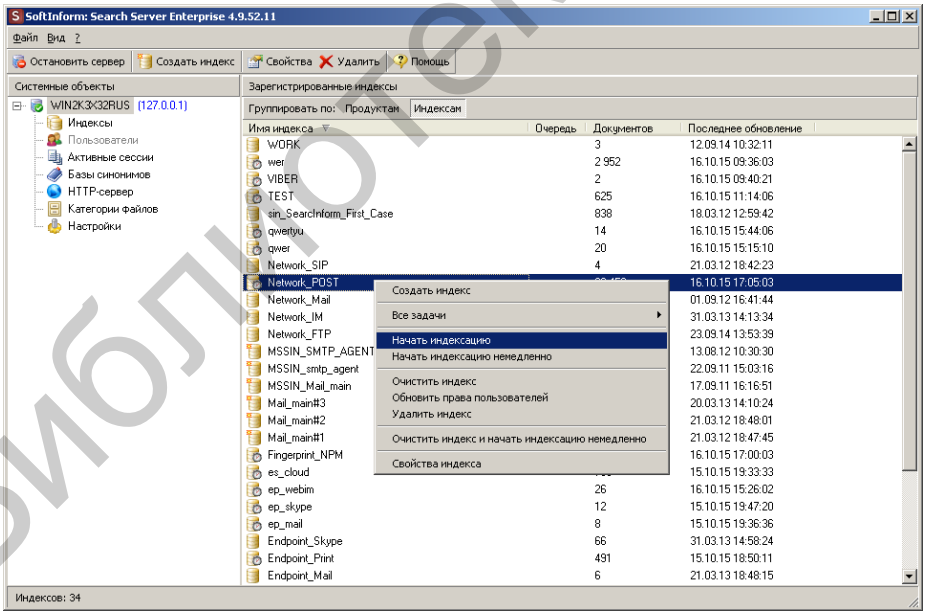


Рис. 6.56. Обновление индекса Network_POST

Запустив принудительное выполнение критерия поиска «123», убедиться в его результативности (рис. 6.57), т. е. в том, что данные, переданные по сети из виртуального компьютера, перехвачены.

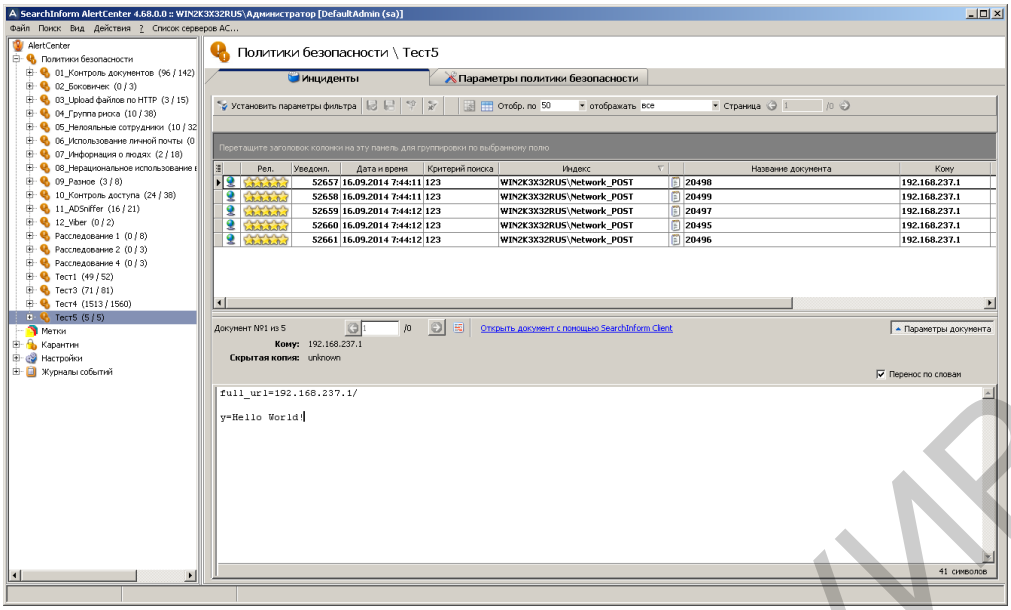


Рис. 6.57. Индикация инцидентов по критерию «123»

Закрыть окно AlertCenter Client.

Завершить работу с виртуальным компьютером.

6.3. Задание для самостоятельной работы

1. Используя регулярные выражения, произвести поиск документов, в которых содержатся как минимум 3 слова, состоящие из 10 символов кириллицы.
2. Используя регулярные выражения, произвести поиск документов, в которых содержатся названия файлов в форматах doc и txt.
3. Передать по сети между виртуальным и основным компьютером текстовую информацию, в которой содержатся номера групп студентов вашего факультета. Перехватить эту информацию. Используя регулярные выражения, произвести поиск соответствующих.
4. Используя регулярные выражения, произвести поиск документов, в которых упоминаются номера автомобилей.

6.4. Контрольные вопросы

1. Что такое шаблон регулярного выражения?
2. Зачем в регулярных выражениях используются спецсимволы?
3. Что такое квантификатор?
4. Что такое символьный класс?
5. Что значит шаблон \d{5}?
6. Что значит шаблон \w{1,5}?
7. Что значит шаблон [а-я]{1, }?
8. Как в шаблоне определить пробел?
9. Как в шаблоне определить отдельное слово?
10. Как в шаблоне определить нечувствительность к регистру?
11. Как в шаблоне определить альтернативу?
12. Как в шаблоне определить группировку?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Руководство аудитора безопасности системы SearchInform. – М. : Сёрчинформ, 2016. – 5 с.

2. Процедурная справка SoftInform Search. SearchInform. – М. : Сёрчинформ, 2016. – 40 с.

3. Процедурная справка SearchInform Client. SearchInform. – М. : Сёрчинформ, 2016. – 40 с.

4. Процедурная справка AlertCenter. SearchInform. – М. : Сёрчинформ, 2016. – 46 с.

5. Процедурная справка EndpointSniffer. SearchInform. – М. : Сёрчинформ, 2016. – 90 с.

6. Процедурная справка NetworkSniffer. SearchInform. – М. : Сёрчинформ, 2016. – 47 с.

7. KIB_description [Электронный ресурс]. – 2018. – Режим доступа : https://static.searchinform.ru/uploads/sites/1/2016/07/KIB_description.pdf.

8. Техническая поддержка VMware. Начальное руководство. – М. : VMware, Inc., 2012. – 29 с.

Св. план 2018, поз. 44

Учебное издание

Борботько Тимофей Валентинович
Бойправ Ольга Владимировна
Морозов Виктор Егорович
Дрозд Алексей Валерьевич

ПРОТИВОДЕЙСТВИЕ УТЕЧКЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

ПОСОБИЕ

Редактор *Е. С. Юрец*
Корректор *Е. И. Герман*
Компьютерная правка, оригинал-макет *О. И. Толкач*

Подписано в печать 06.07.2018. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 11,16. Уч.-изд. л. 11,8. Тираж 30 экз. Заказ 103.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6