КАЗАНСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

ИНСТИТУТ ФИЗИКИ

Кафедра Радиофизики

П. А. Корчагин, А. И. Сулимов

МОНИТОРИНГ ЭКРАНОВ ПОЛЬЗОВАТЕЛЕЙ И ПОИСК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Методические указания к выполнению лабораторной работы

Казань – 2022

УДК 681.322

Принято на заседании кафедры радиофизики

Протокол № 10 от 14 сентября 2021 года

Рецензент

кандидат физико-математических наук,

доцент кафедры радиоастрономии КФУ

Е. Ю. Зыков

Корчагин П. А., Сулимов А. И.

Мониторинг экранов пользователей и поиск конфиденциальной информации. Методические указания к выполнению лабораторной работы / П. А.Корчагин, А. И. Сулимов. – Казань: Казан. ун-т, 2022. – 38с.

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

Содержание

Лабораторная работа

Настройка программного комплекса SearchInform для контроля содержимого экранов пользователей и поиска конфиденциальной информации без проведения синтаксического анализа

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

Теоретические сведения

1. Ознакомиться с разделами 1-5 руководства аудитора безопасности системы SearchInform.
2. Ознакомиться со справочными материалами EndpointSniffer Console, SearchInform MonitorSniffer Client, AlertCenter Client.

Ход выполнения работы

1. Подготовительные работы:

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

– Выполнить задание лабораторной работы №2.

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

2. Реализация оперативного контроля за действиями пользователей:

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

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

– В соответствии с рис. 1-4 проверить подключение агента SearchInform MonitorSniffer Client к базе данных.

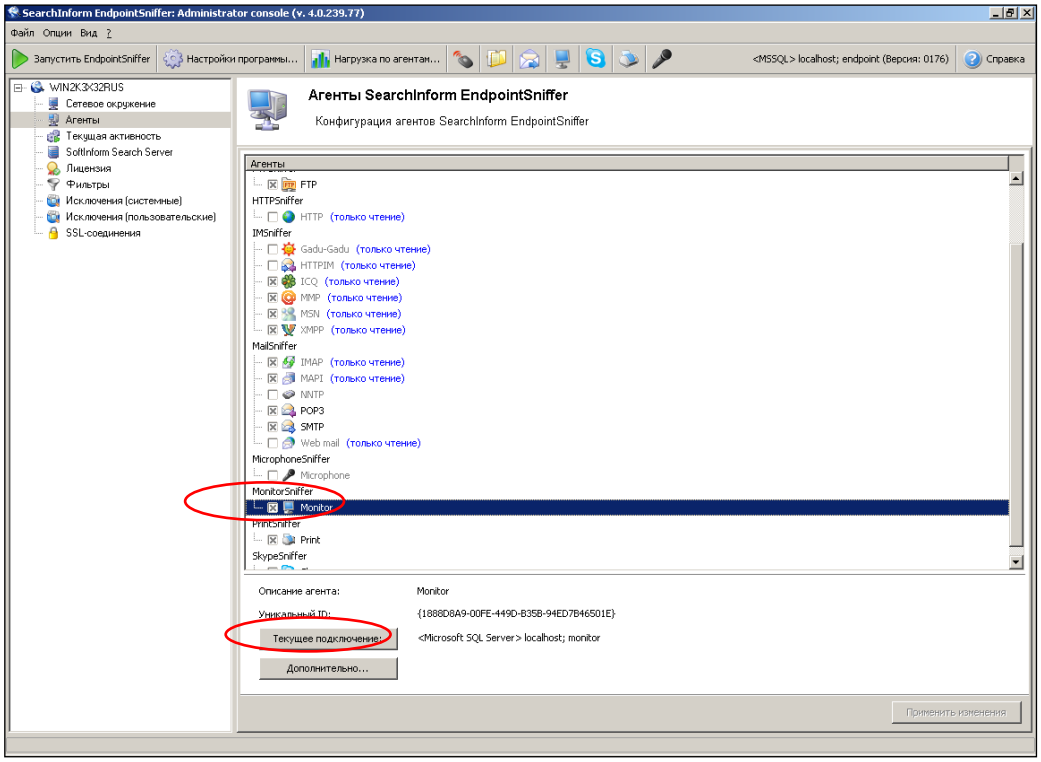

Рис. 1. Вход в режим просмотра параметров текущего подключения

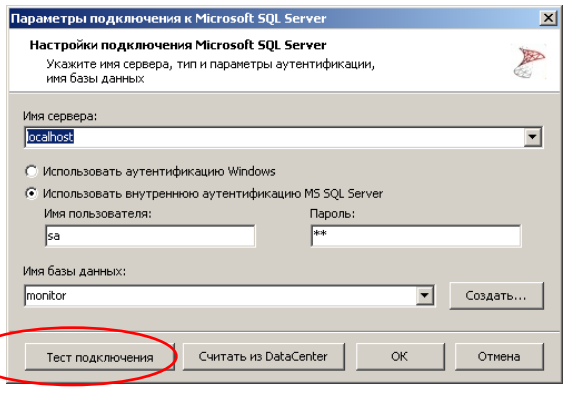

Рис. 2. Тестирование подключения к базе данных

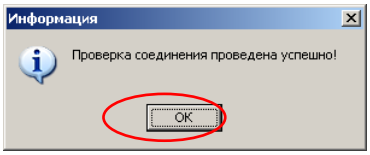

Рис. 3. Индикация успешного подключения

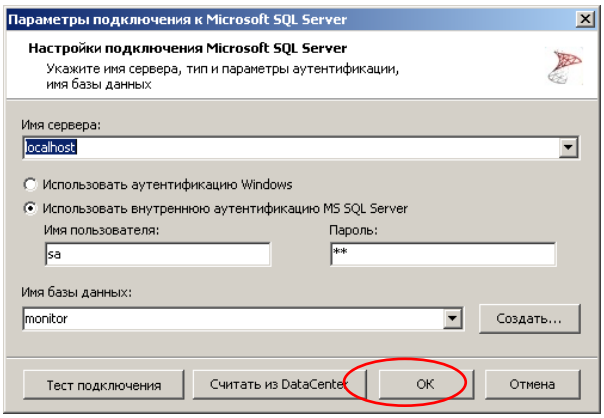

Рис. 4. Выход из режима просмотра параметров подключения

– В соответствии с рис. 5-6 войти в режим редактирования настроек мониторинга изображений на экране и запущенных процессов на компьютере пользователя.

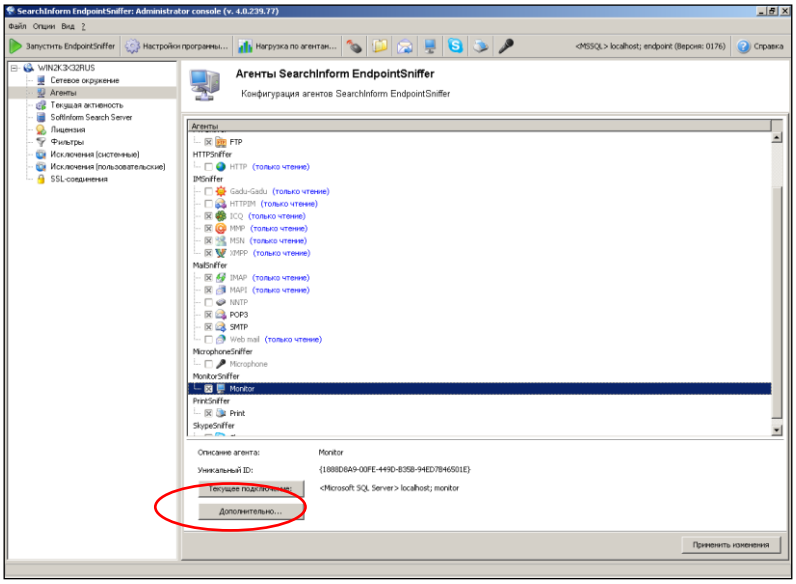

Рис. 5. Вход в режим редактирования параметров мониторинга экрана и запущенных процессов

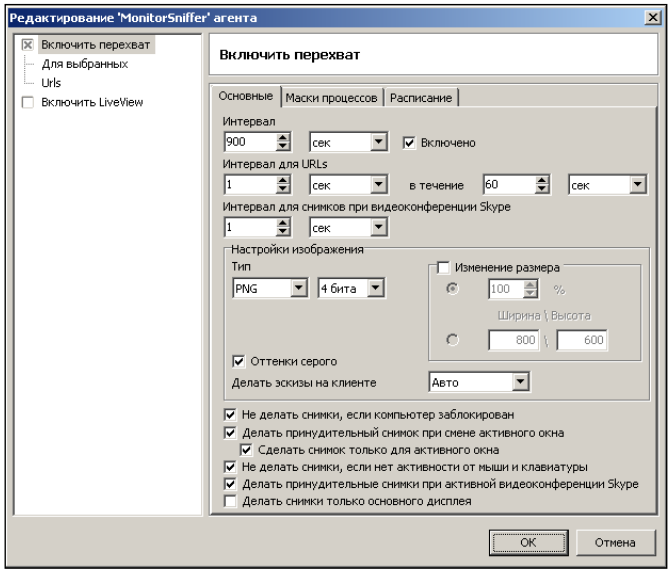

Рис. 6. Окно редактирования параметров мониторинга с первоначальными установками

– В соответствии с рис. 7-10 изменить параметры мониторинга.

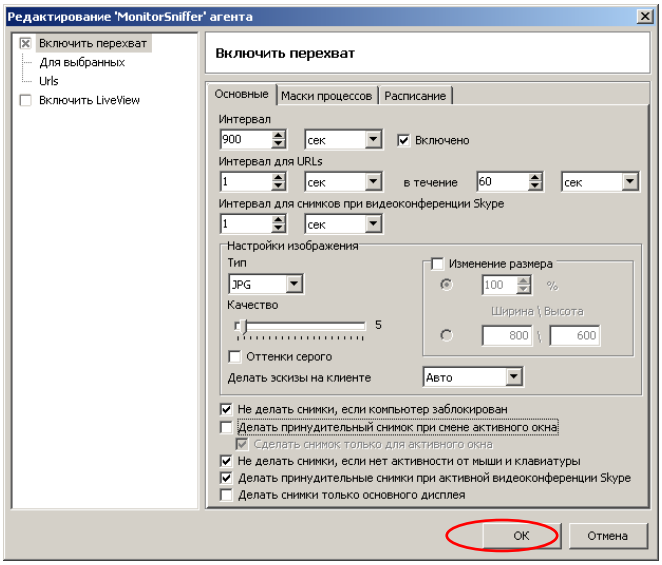

Рис. 7. Изменения качества снимка экрана

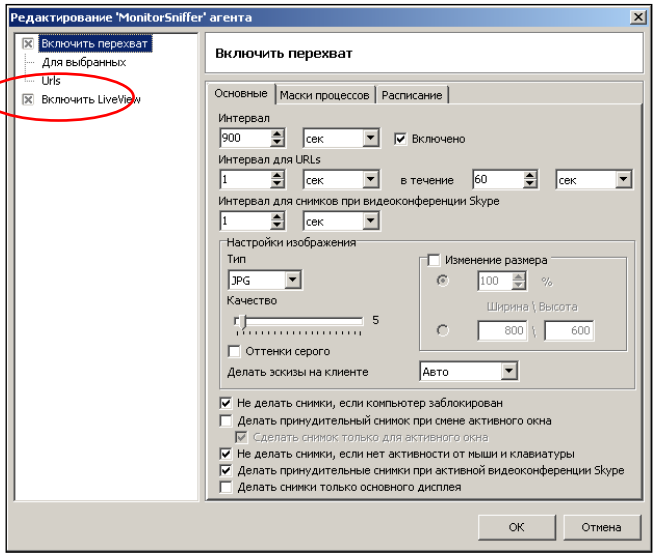

Рис. 8. Включение режима оперативного контроля экрана

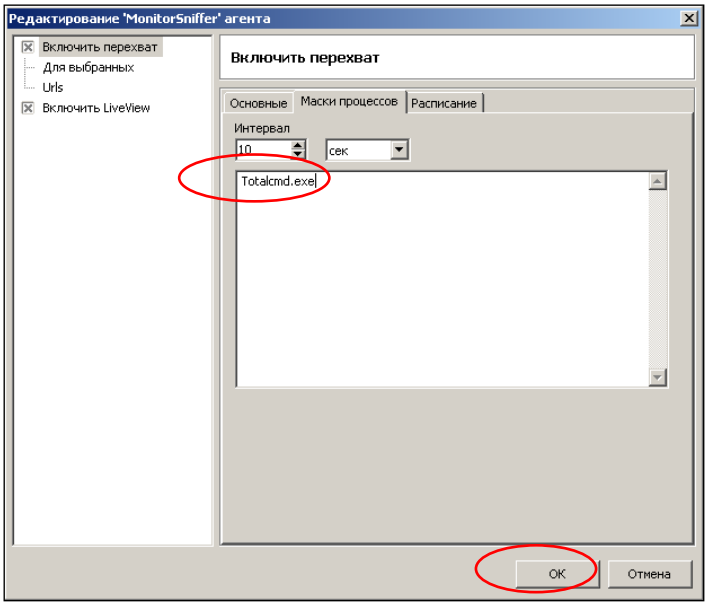

Рис. 9. Определение маски процесса

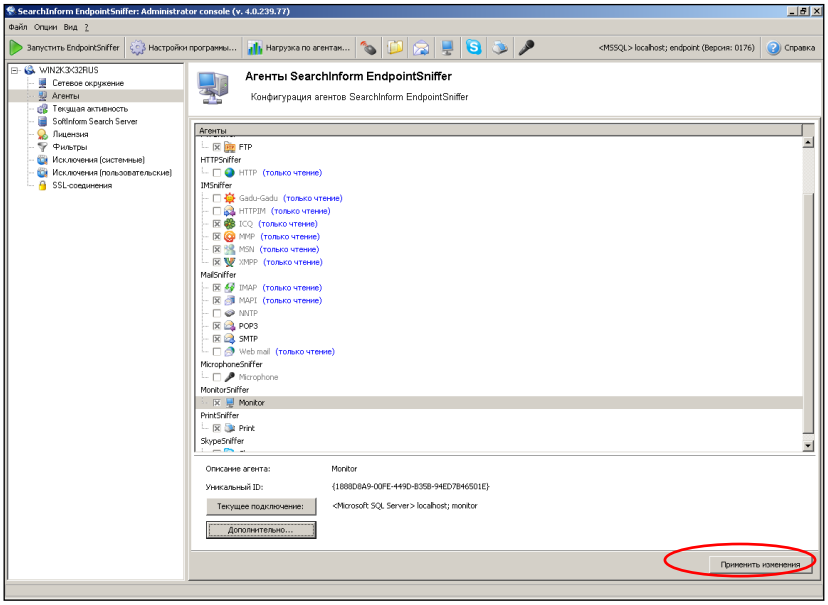

Рис. 10. Подтверждение измененных параметров мониторинга

– В соответствии с рис. 11-12 запустить сервер SearchInform EndpointSniffer

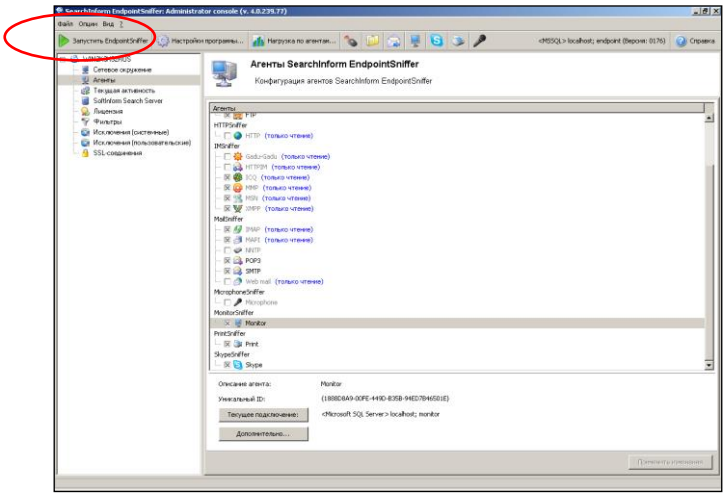

Рис. 11. Запуск сервера SearchInform EndpointSniffer

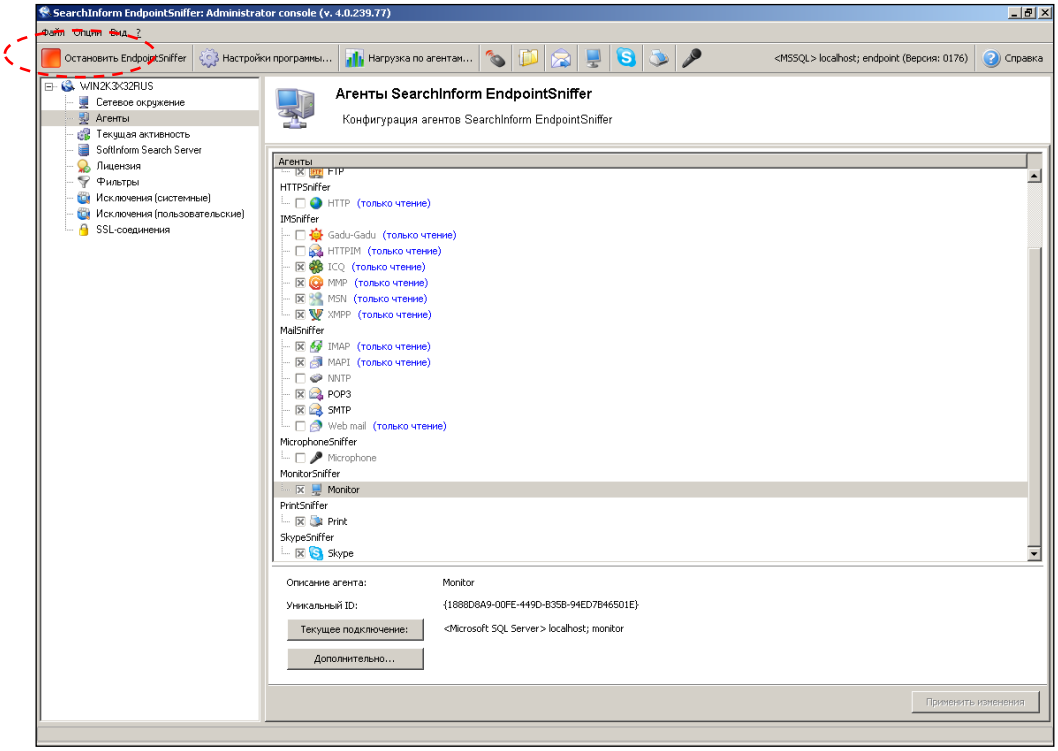

Рис. 12. Индикация функционирования сервера SearchInform EndpointSniffer

– Закрыть окно серверного приложения SearchInform EndpointSniffer.

– С помощью соответствующего ярлыка запустить SearchInform MonitorSniffer Client, окно которого показано на рис. 13.

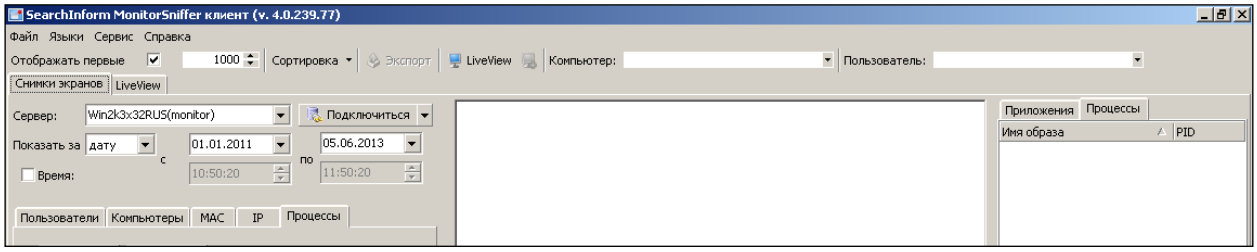

Рис. 13. Окно SearchInform MonitorSniffer Client

– В соответствии с рис. 14-15 подключиться к базе данных перехваченных снимков экрана, отредактировать временной интервал сохраненных изображений и произвести поиск всех хранящихся снимков экрана за 1-2 прошедших года. Зафиксировать время выполнения поиска.

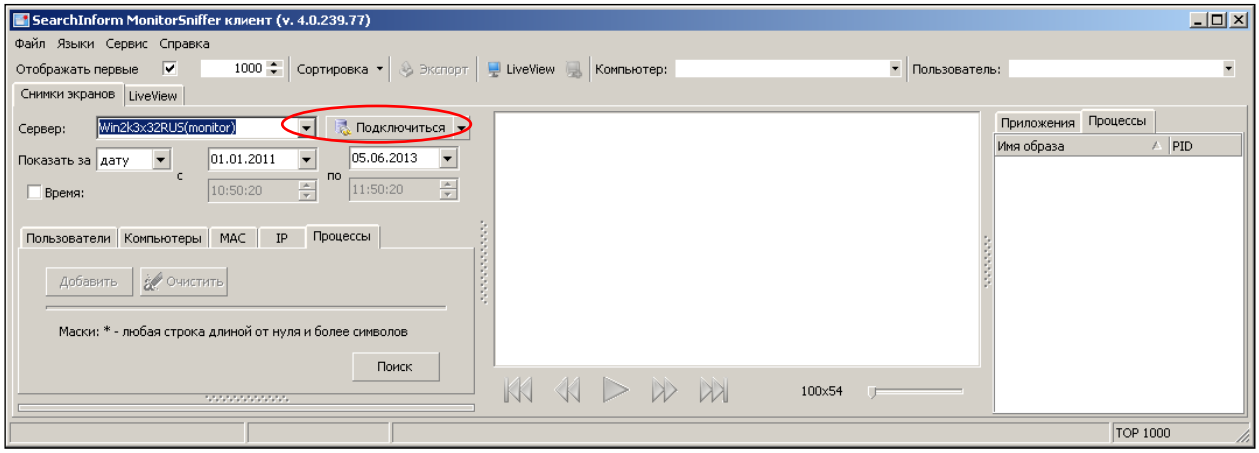

Рис. 14. Подключение MonitorSniffer Client к базе данных снимков экрана

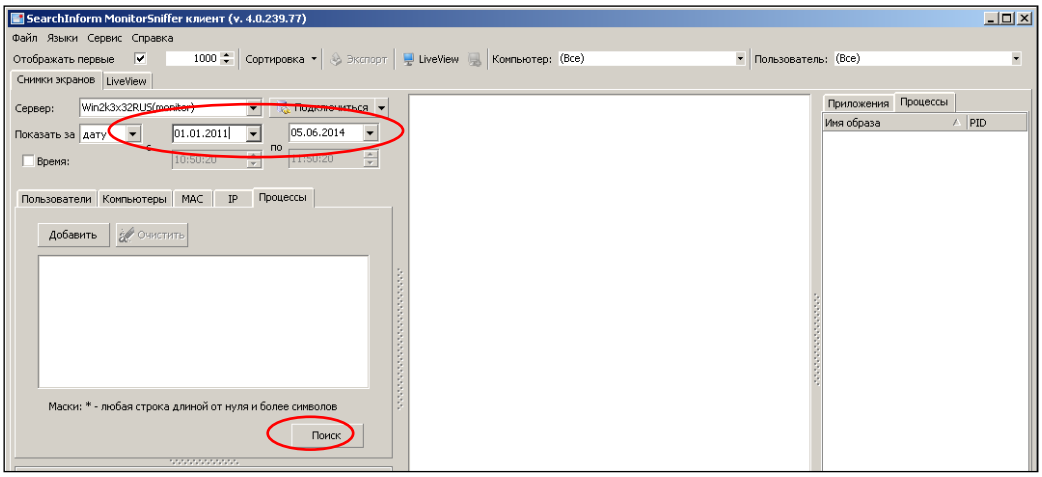

Рис. 15. Редактирование временного интервала поиска снимков

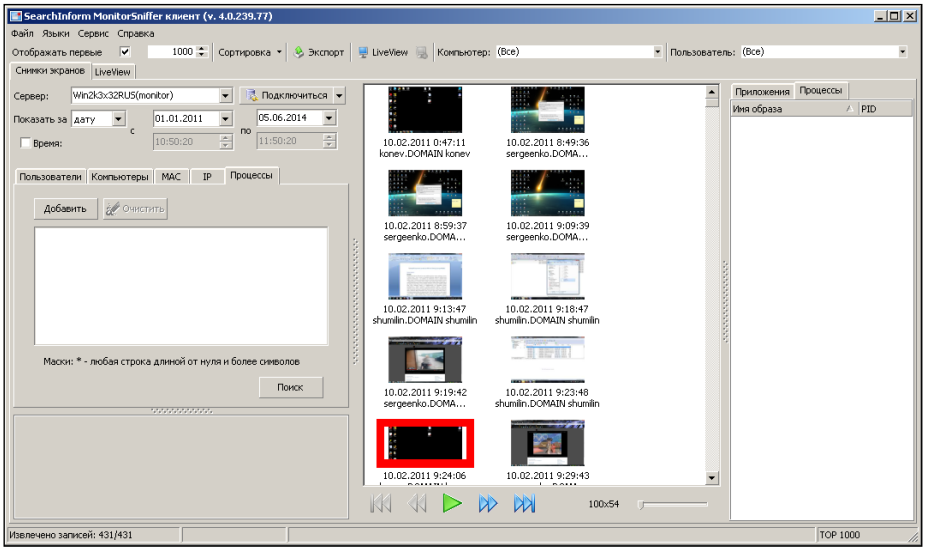

Рис. 16. Индикация сохраненных снимков экрана

– В соответствии с рис. 17-19 просмотреть снимок экрана и перечень процессов, запущенных в момент записи снимка.

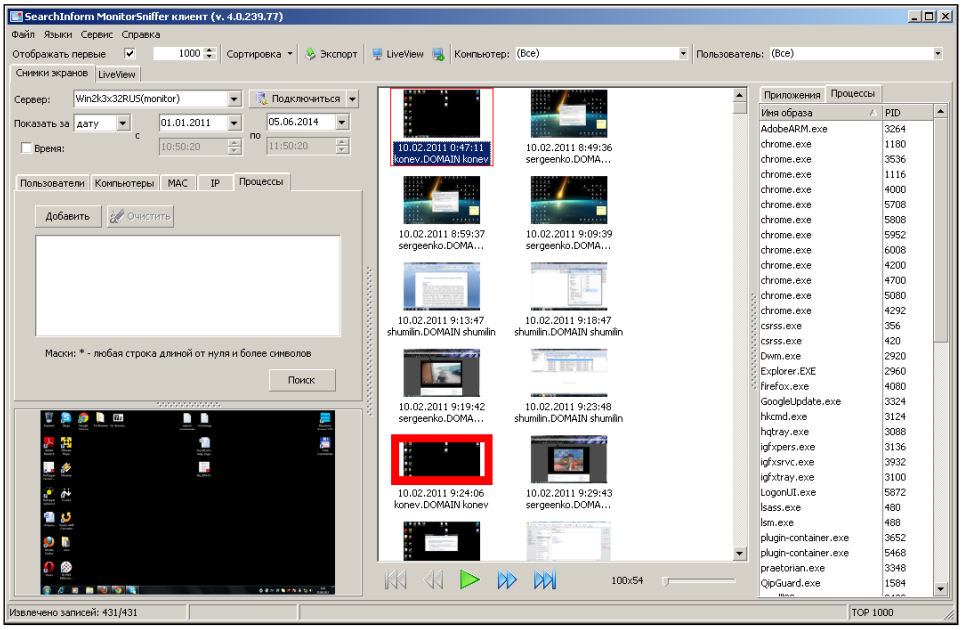

Рис. 17. Выбор снимка

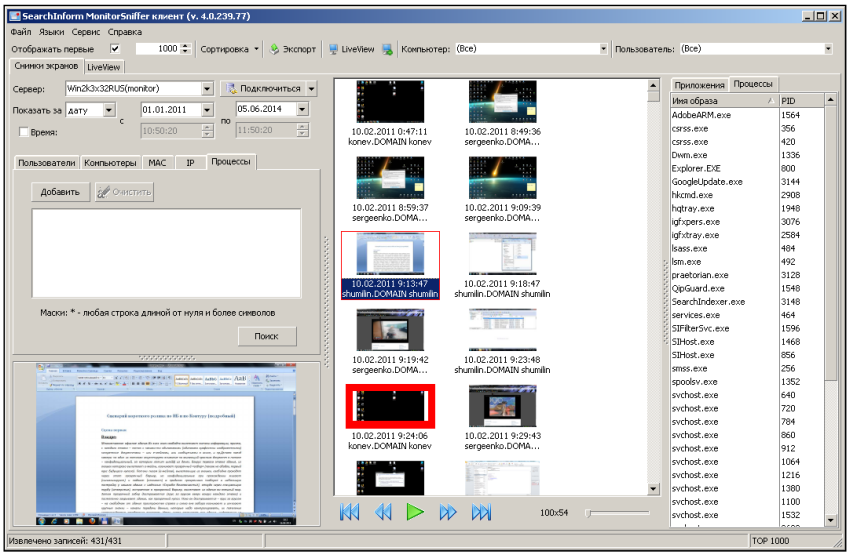

Рис. 18. Показ выбранного снимка при одинарном клике мышкой на миниатюре

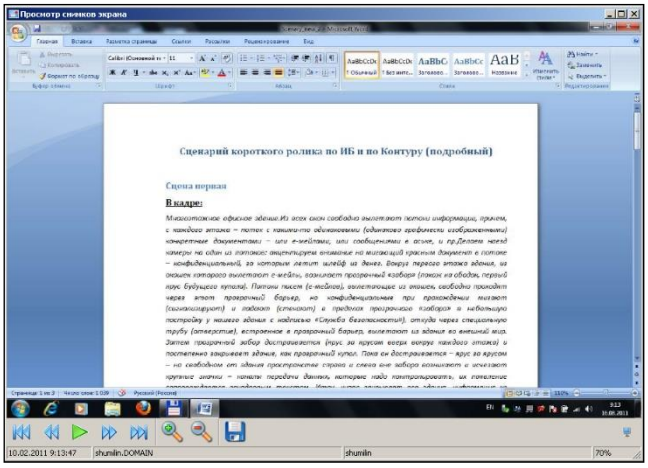

Рис. 19. Отображение выбранного снимка при двойном клике мышкой на миниатюре

– В соответствии с рис. 20-21 просмотреть свойства снимка экрана.

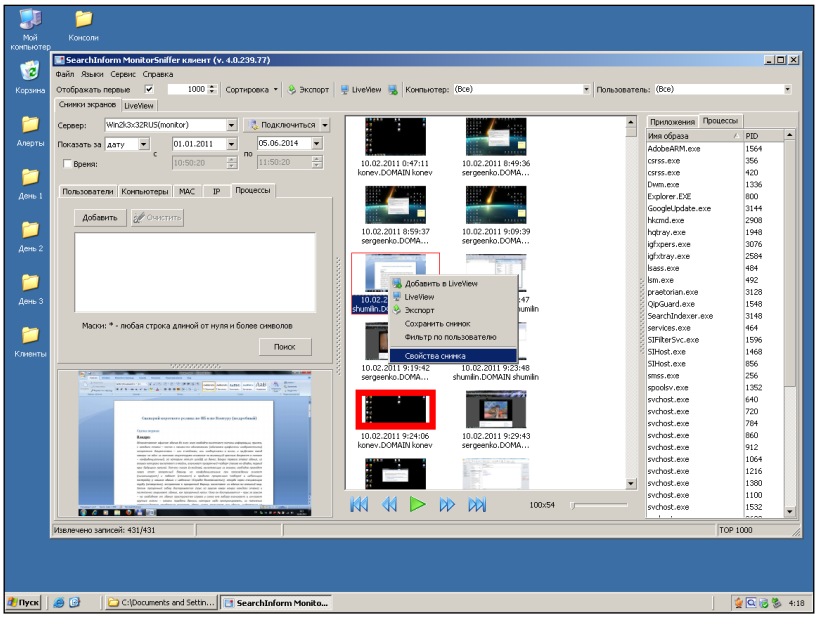

Рис. 20. Выбор опции «Свойства экрана» из контекстного меню снимка

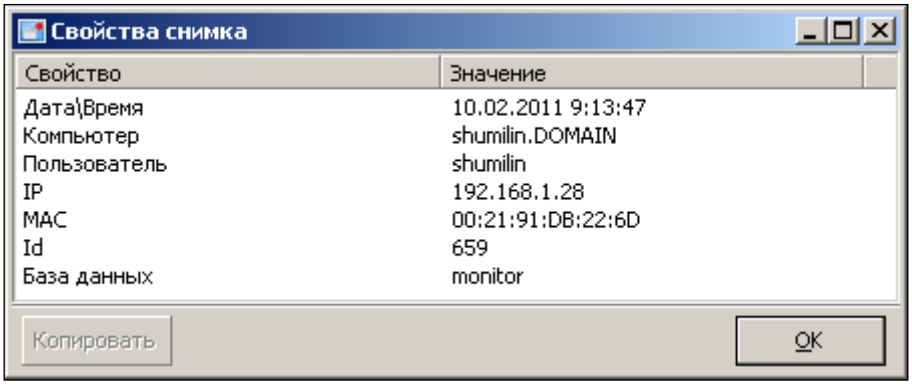

Рис. 21. Окно просмотра инормации о снимке экрана

– В соответствии с рис. 22-24 экспортировать снимок экрана в графический файл.

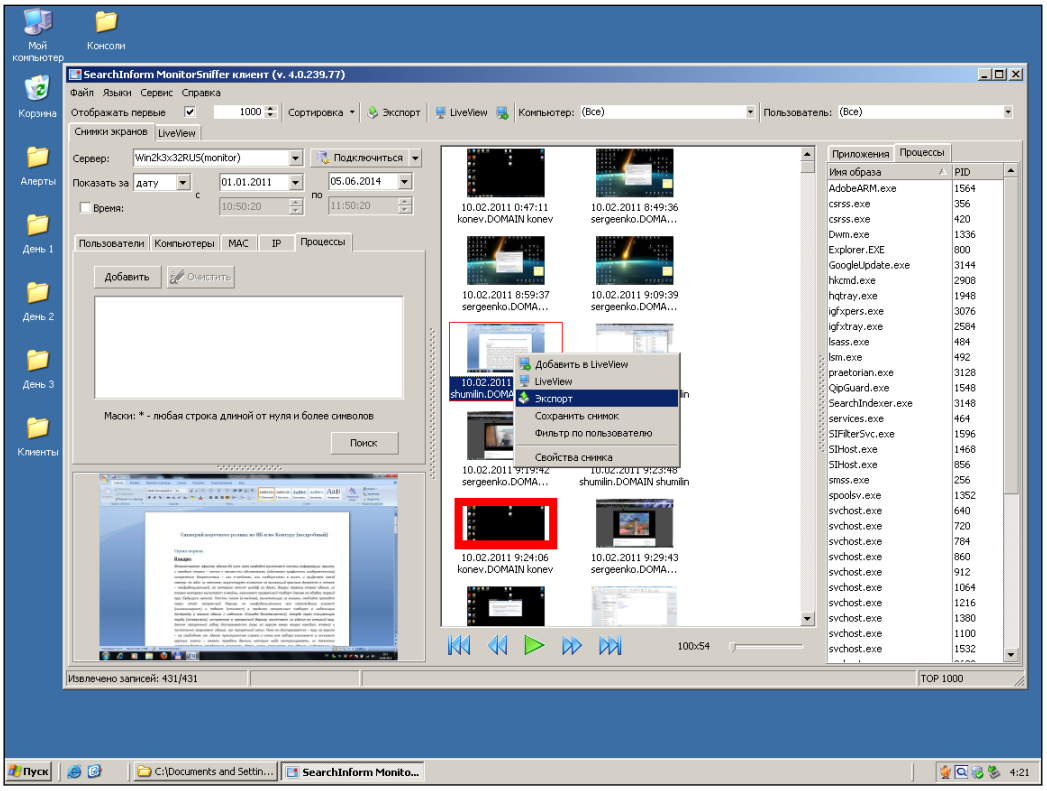

Рис. 22. Выбор опции «Экспорт» из контекстного меню снимка

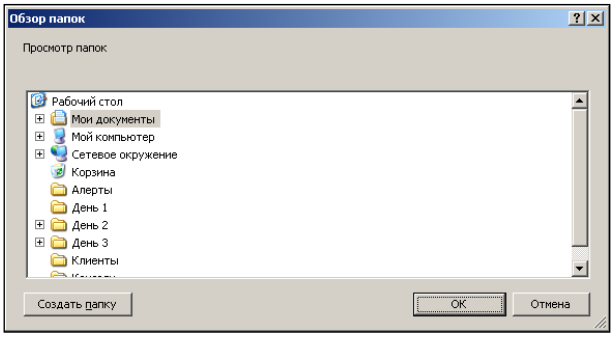

Рис. 23. Выбор места сохранения файла

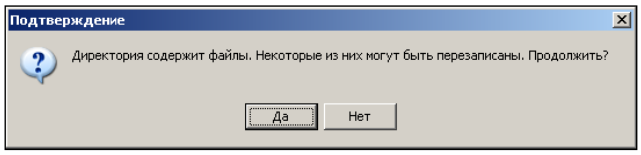

Рис. 24. Запрос подтверждения экспорта

– В соответствии с рис. 25-26 просмотреть несколько снимков экрана в виде диафильма. Данная опция применяется для быстрой предварительной оценки содержимого снимков экрана.

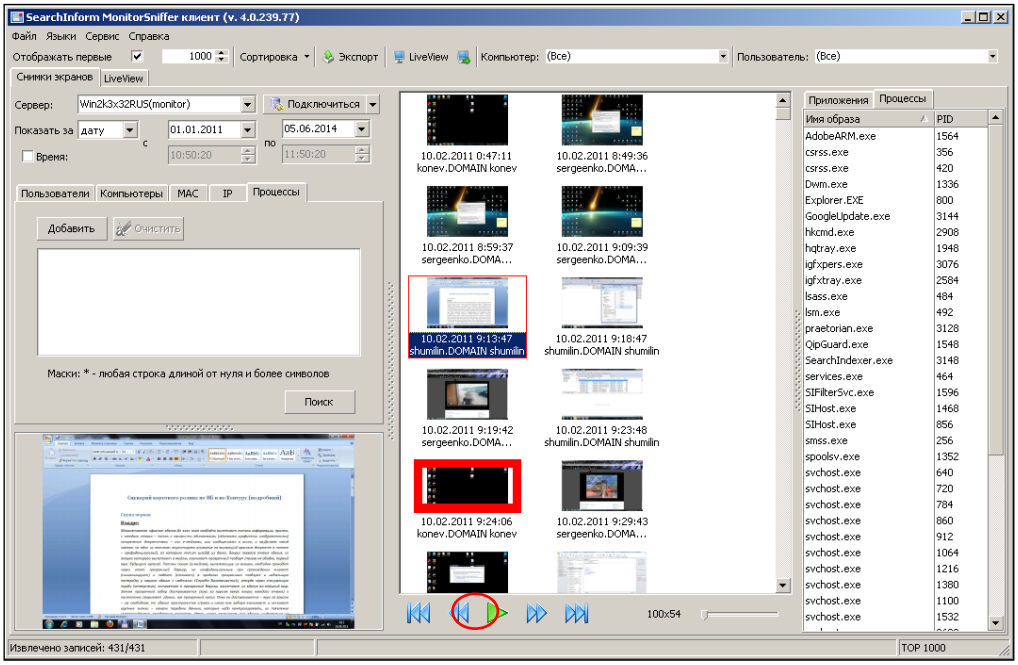

Рис. 25. Запуск диафильма

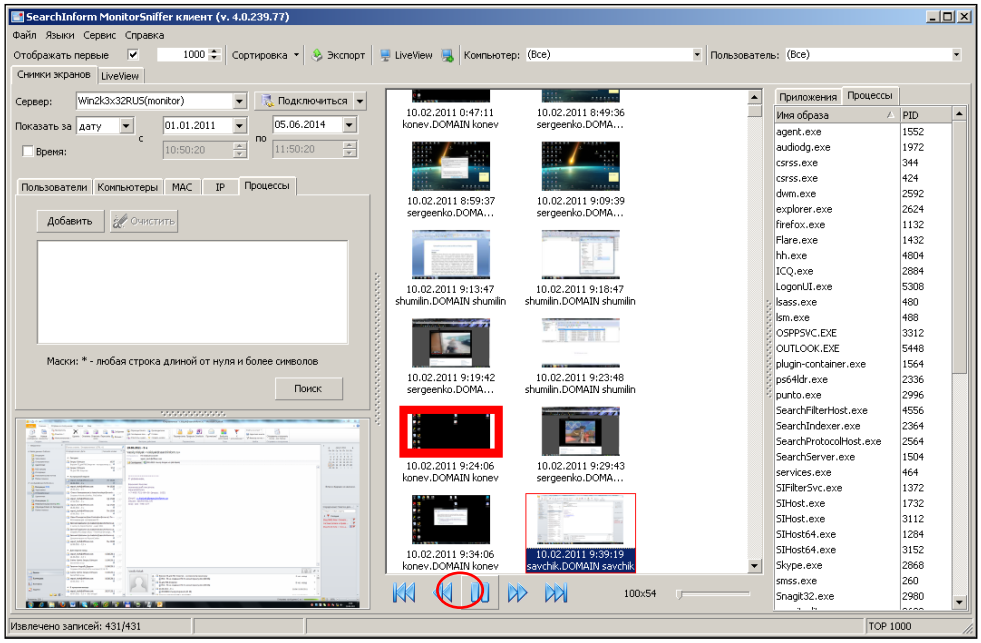

Рис. 26. Останов диафильма

– В соответствии с рис. 27-30 произвести поиск снимков экрана по имени компьютера. Заметим, что в соответствии с рис. 28 в окне выбора имени компьютера также отображаются соответствующие IP- и MAC-адреса. Зафиксировать время выполнения поиска.

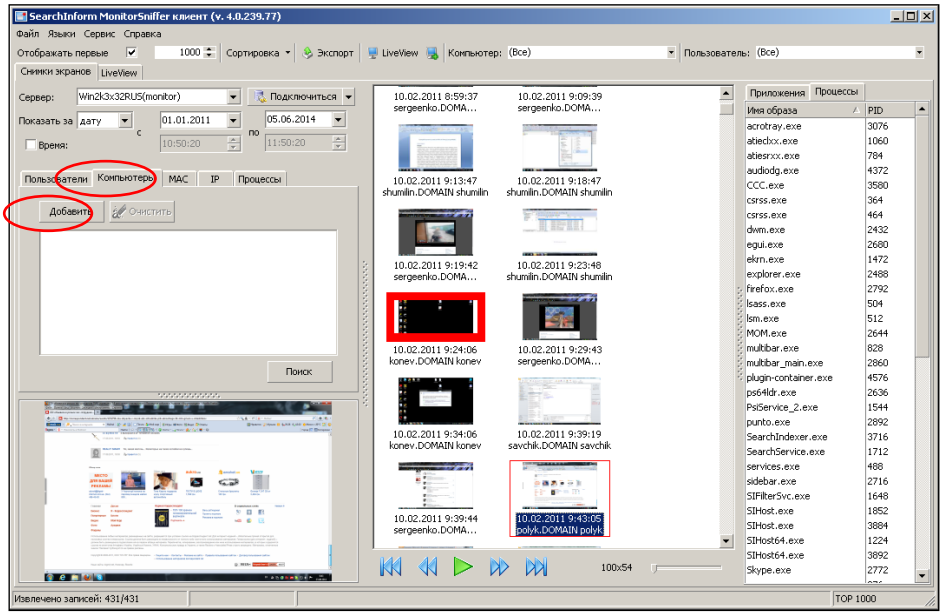

Рис. 27. Вход в режим выбора имени компьютера

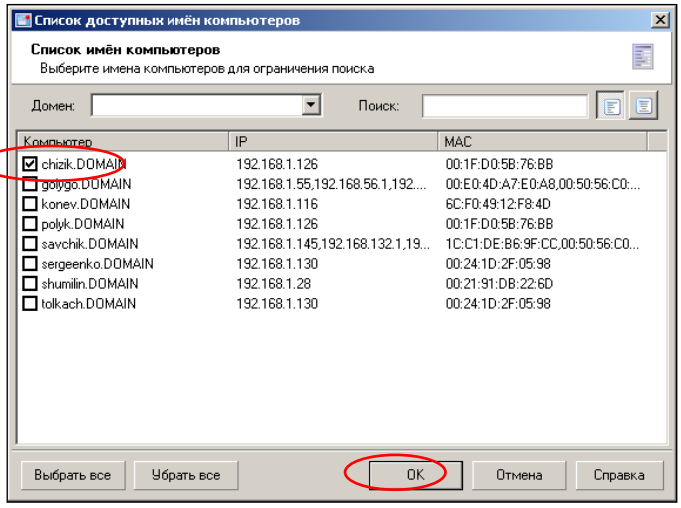

Рис. 28. Выбор имени компьютера

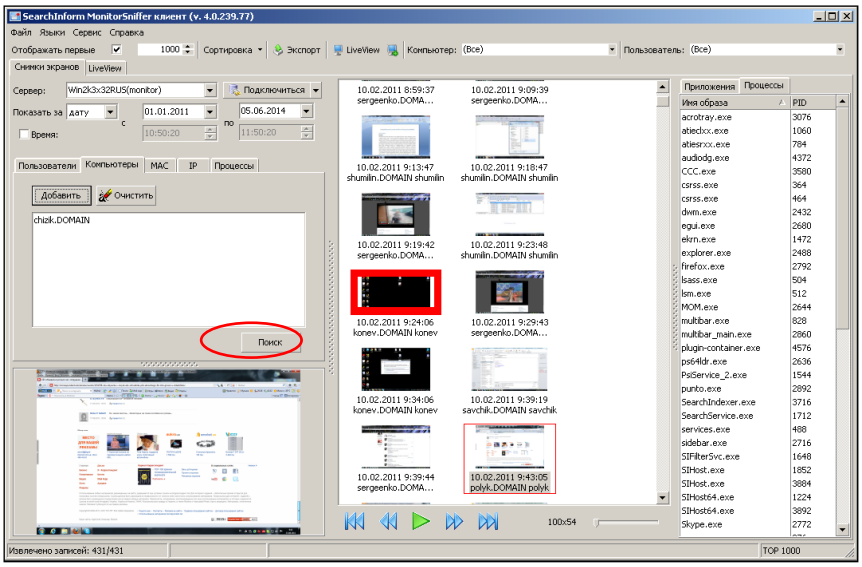

Рис. 29. Поиск снимков по имени компьютера

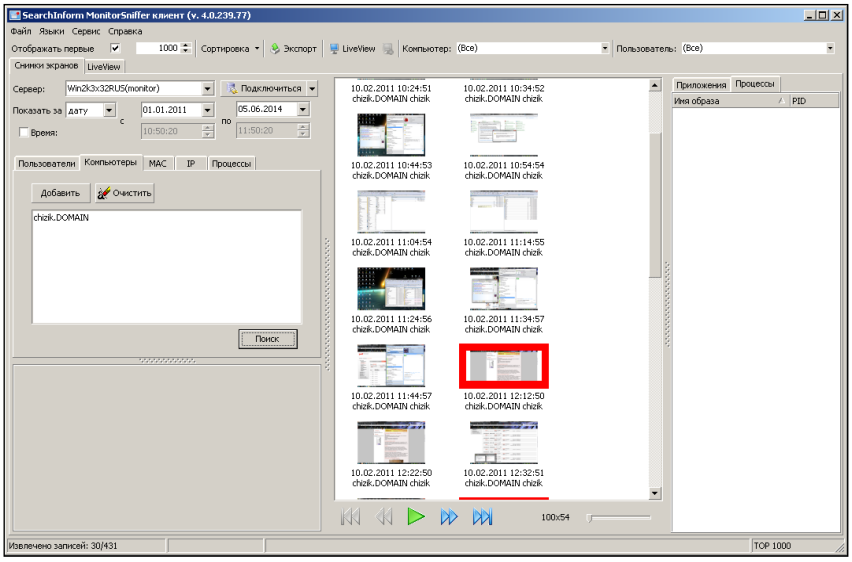

Рис. 30. Отображение результатов поиска снимков по имени компьютера

– В соответствии с рис. 31-32 очистить маску поиска. Заметим, что после очистки маски поиска в окне результатов продолжают оставаться старые данные. Для обновления данного окна следует нажать кнопку «Поиск».

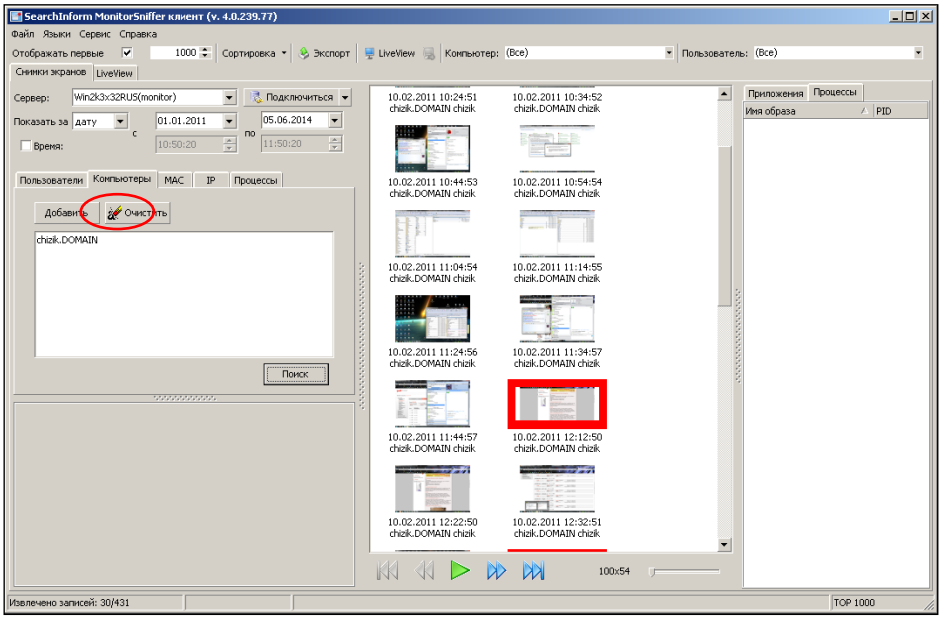

Рис. 31. Выбор опции очистки маски поиска

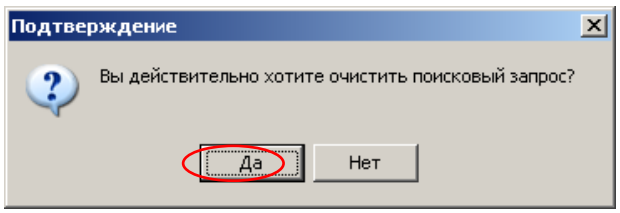

Рис. 32. Подтверждение очистки

– Найти перечень запущенных процессов в момент времени, который соответствует снимку экрана, показанному на рис. 33. Экспортировать данный снимок в графический файл. Также определить MAC и IP-адреса соответствующего компьютера.

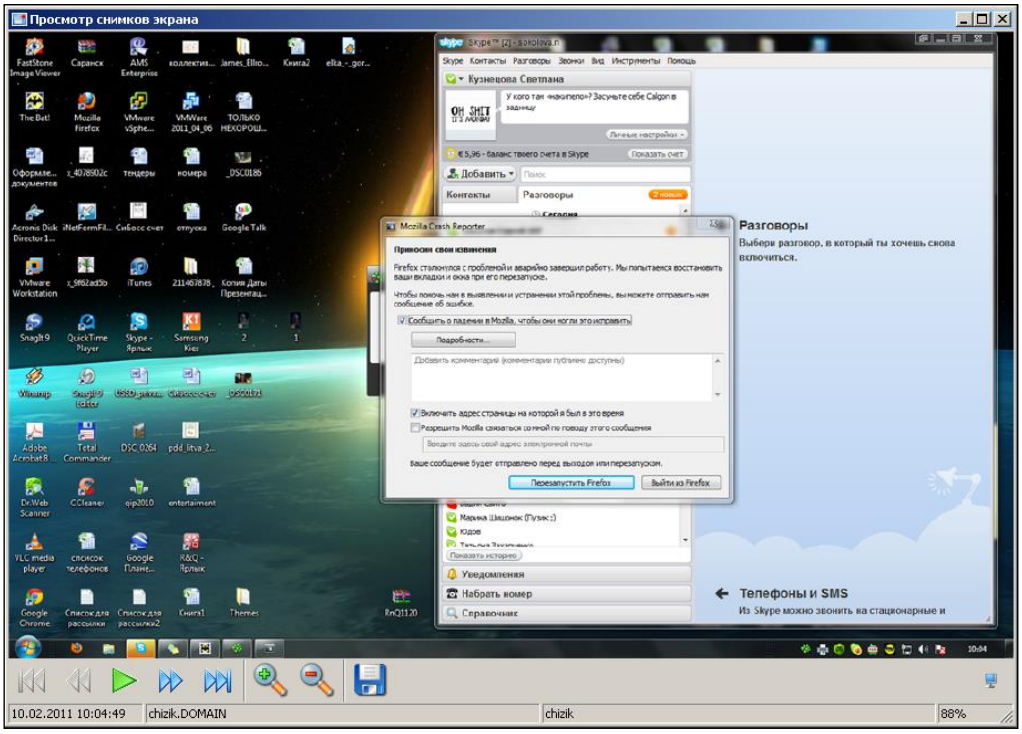

Рис. 33. Задание для поиска

– 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 MonitorSniffer Client.

3. Поиск 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». Добавить 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. 34.

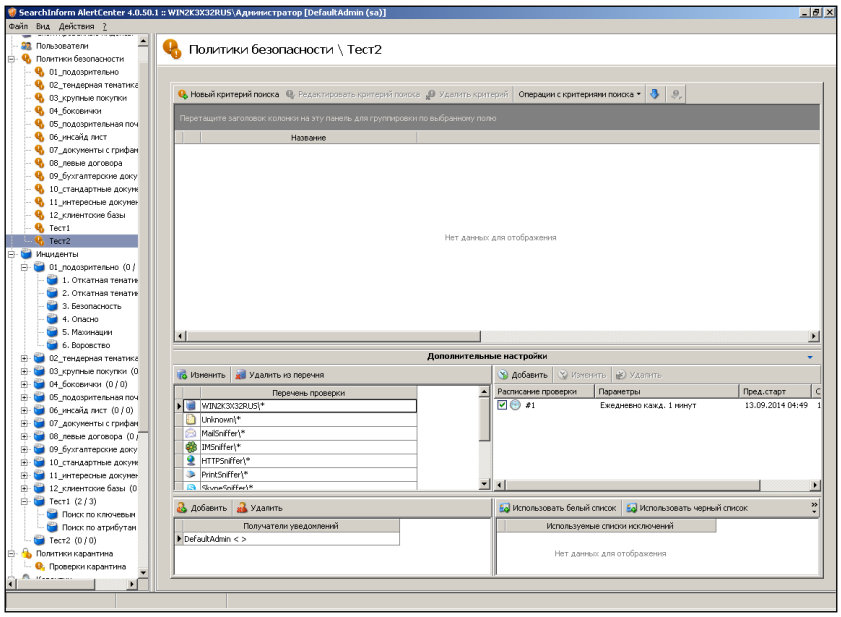

Рис. 34. Окно политики безопасности Тест2

– Через несколько минут после создания политики Тест2 в перечне инцидентов убедиться, что список соответствующих инцидентов пуст (рис.35).

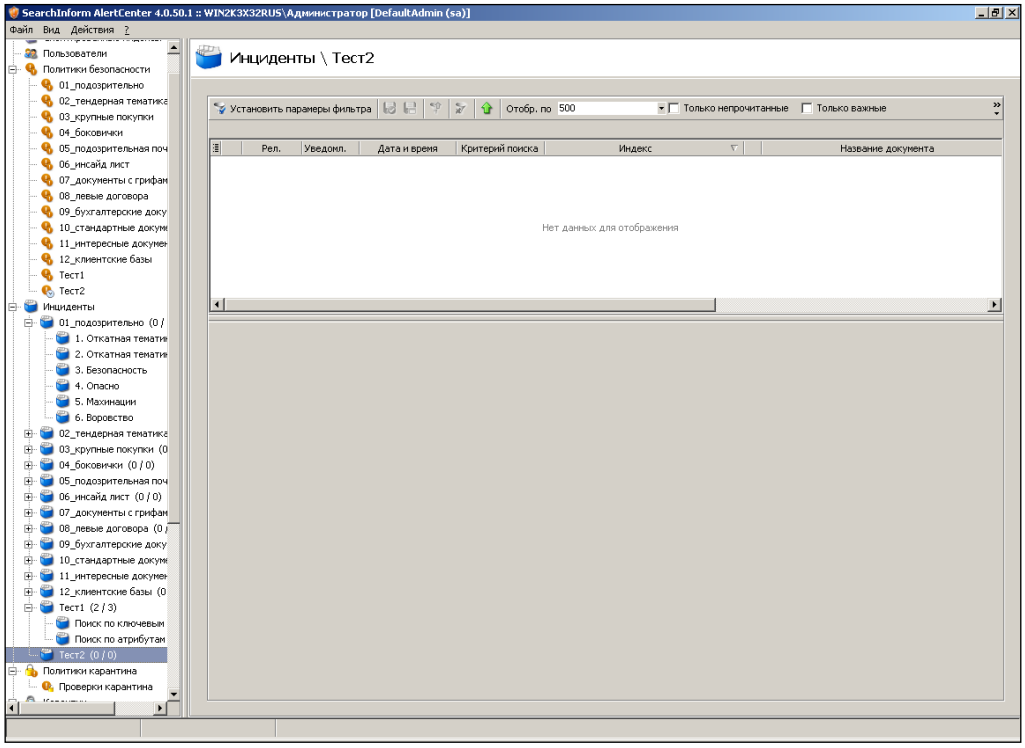

Рис. 35. Индикация пустого списка инцидентов политики «Тест2»

– В соответствии с рис. 36 создать критерий «АтрибутДатаПерехвата», предусматривающий поиск документов, дата модификации которых не больше трех лет и одного дня.

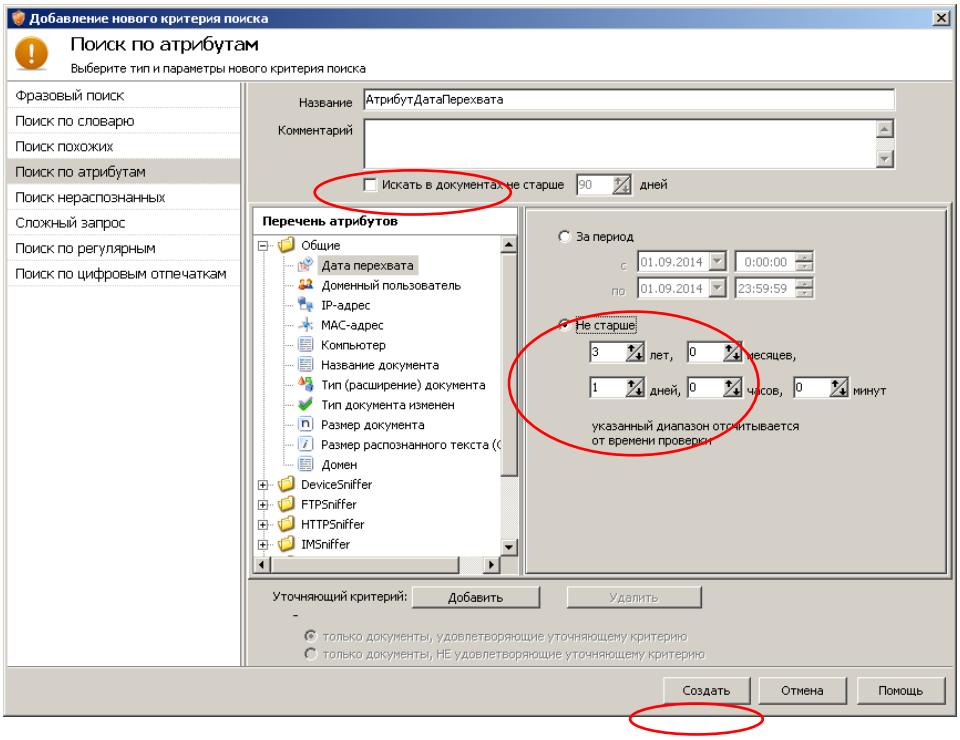

Рис. 36. Создание критерия «АтрибутДатаПерехвата»

– Через несколько минут после создания критерия убедиться, что в списке инцидентов появились соответствующее уведомления. При этом сигнализируется о том, что число инцидентов превышает максимально допустимое. (рис. 37).

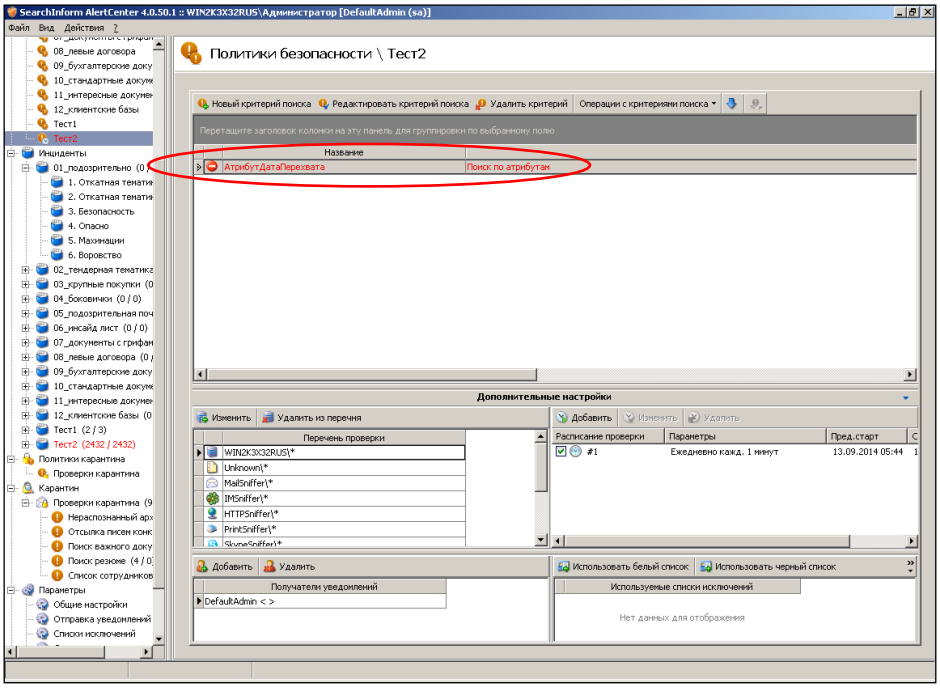

Рис. 37. Индикация инцидентов по критерию «АтрибутИзменен»

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

– В соответствии с рис. 38 создать критерий для поиска текстовой информации в графических файлах. При этом в графическом файле должно быть распознано не менее 10 символов текста.

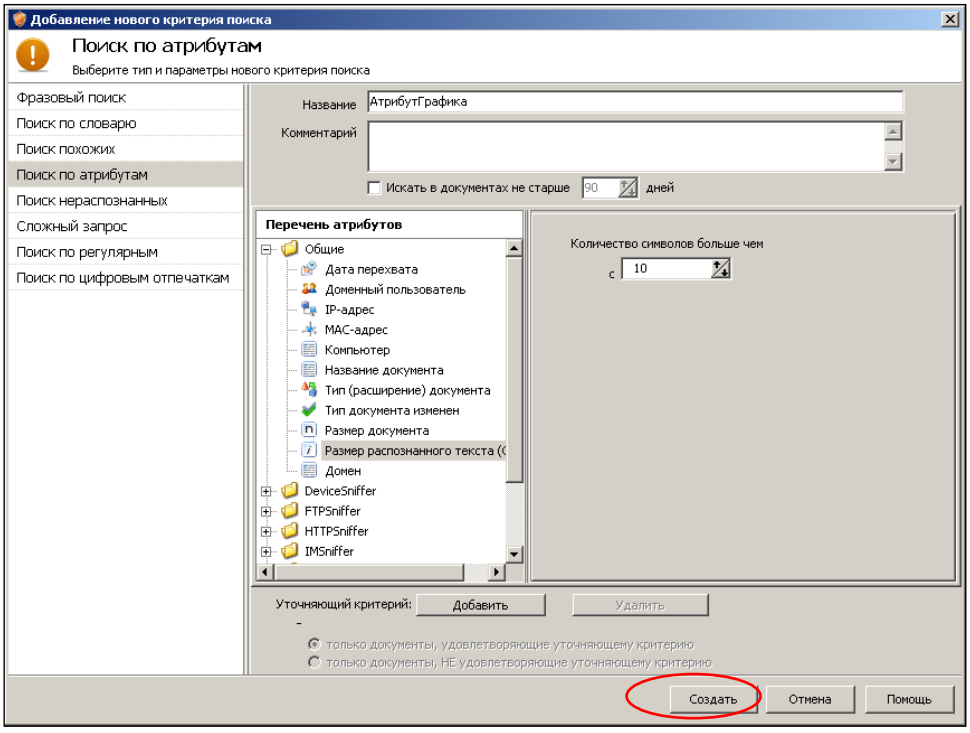

Рис. 38. Первый этап создания критерия «АтрибутГрафика»

– В соответствии с рис. 39 запустить критерий «АтрибутГрафика» на выполнение.

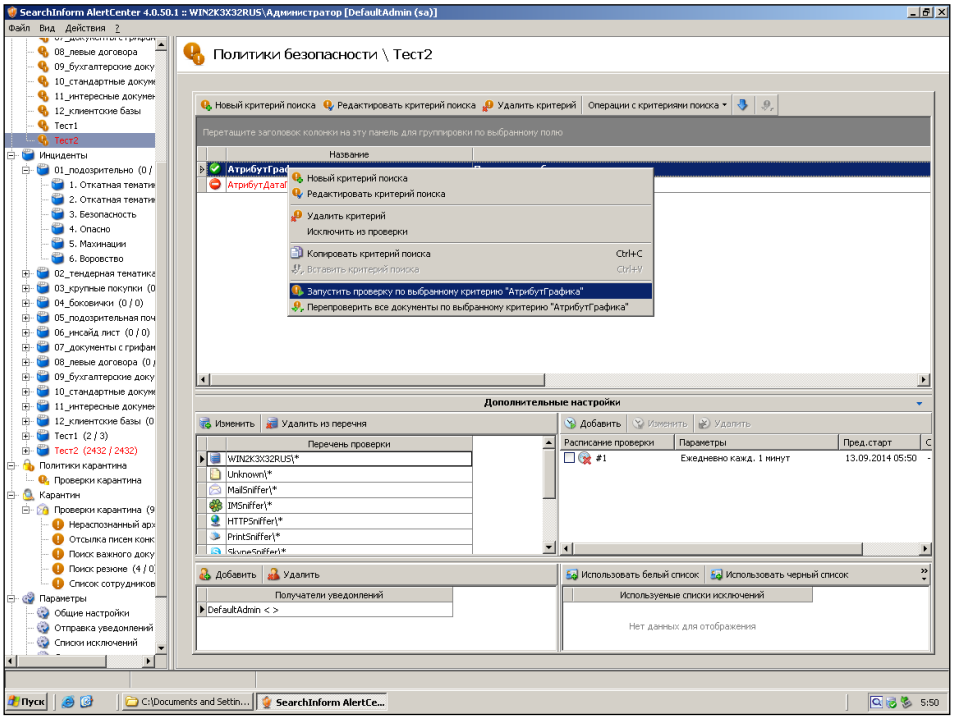

Рис. 39. Запуск критерия критерия «АтрибутГрафика»

– После выполнения критерия убедиться, что в списке инцидентов появились соответствующее уведомления (рис. 40).

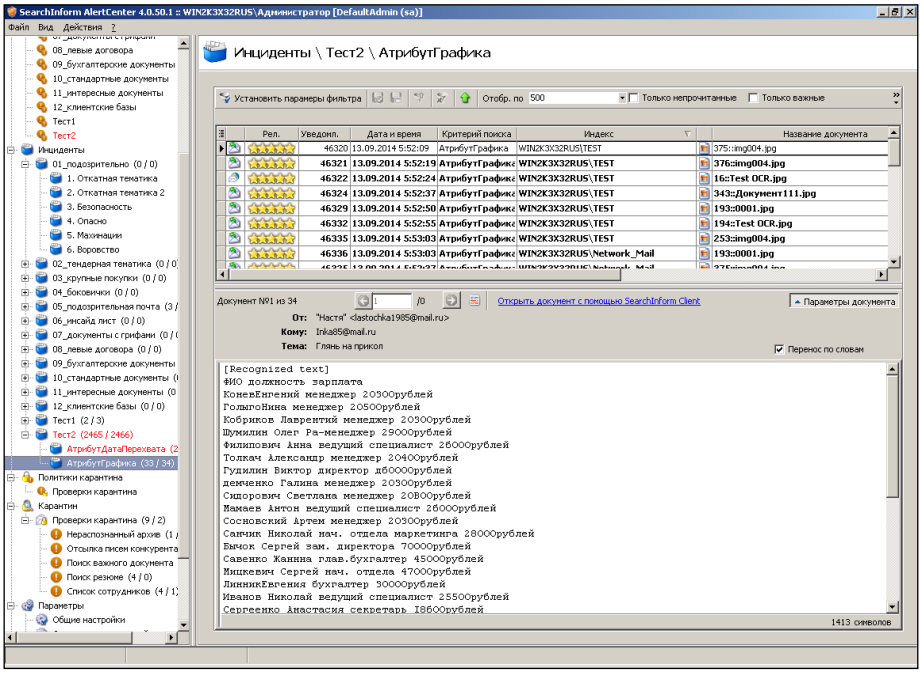

Рис. 40. Индикация инцидентов по критерию «АтрибутГрафика»

– В соответствии с рис. 41 создать критерий для поиска исходящих шифрованных электронных писем. Отметим, что опция «Шифрованное сообщение» находится в разделе «MailSniffer».

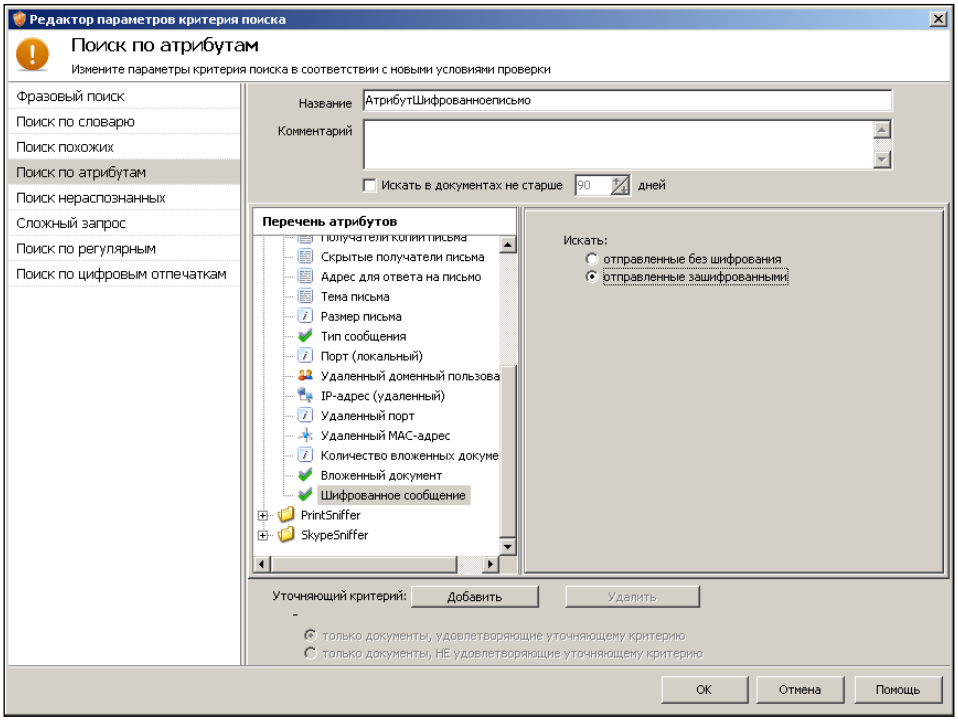

Рис. 41. Создание критерия «АтрибутШифрованноеписьмо»

– В соответствии с рис. 42 запустить принудительное выполнения критерия поиска «АтрибутШифрованноеписьмо». Зафиксировать время выполнения поиска. Убедиться в результативности поиска (рис. 43).

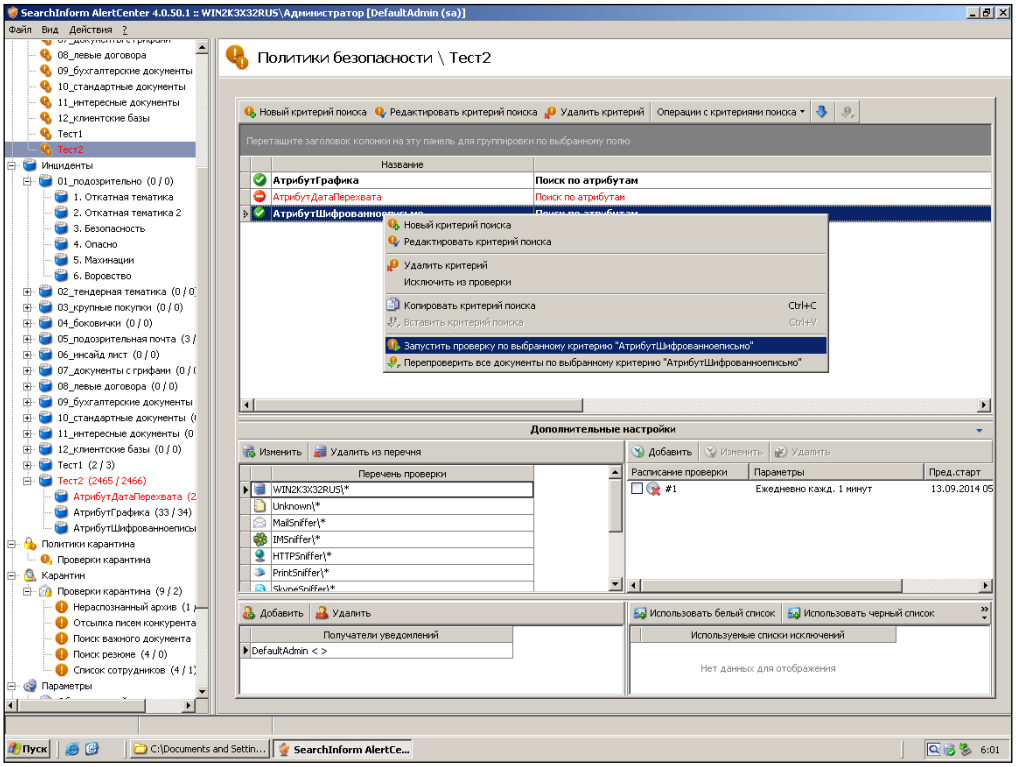

Рис. 42. Принудительный запуск проверки критерия «АтрибутШифрованноеписьмо»

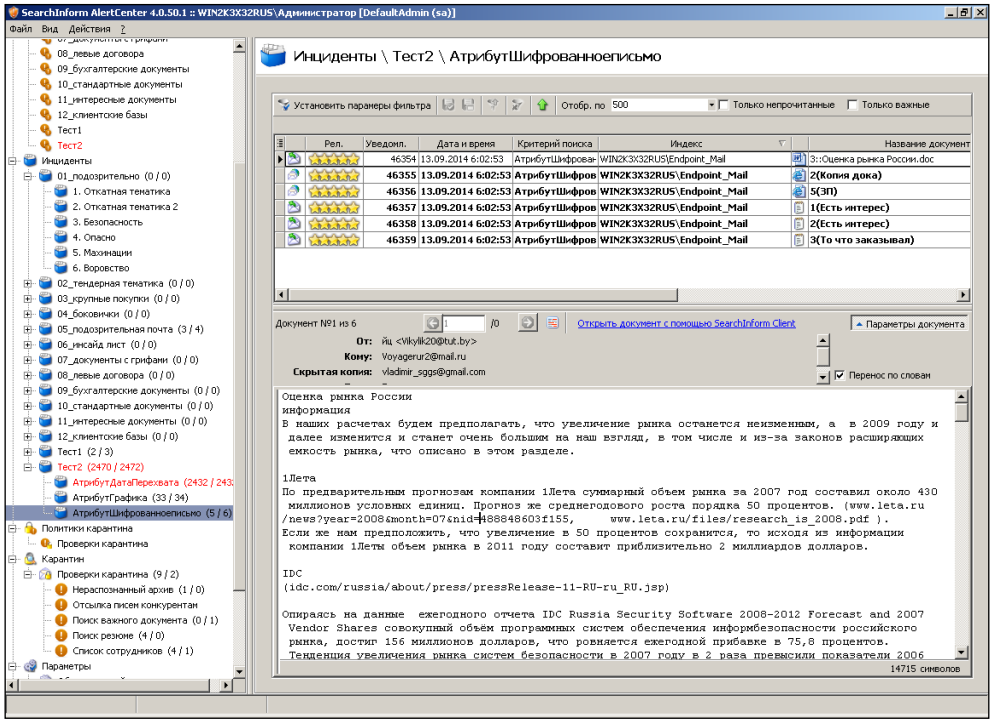

Рис. 43. Индикация инцидентов по критерию «АтрибутШифрованноеписьмо»

– В соответствии с рис. 44-46 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.

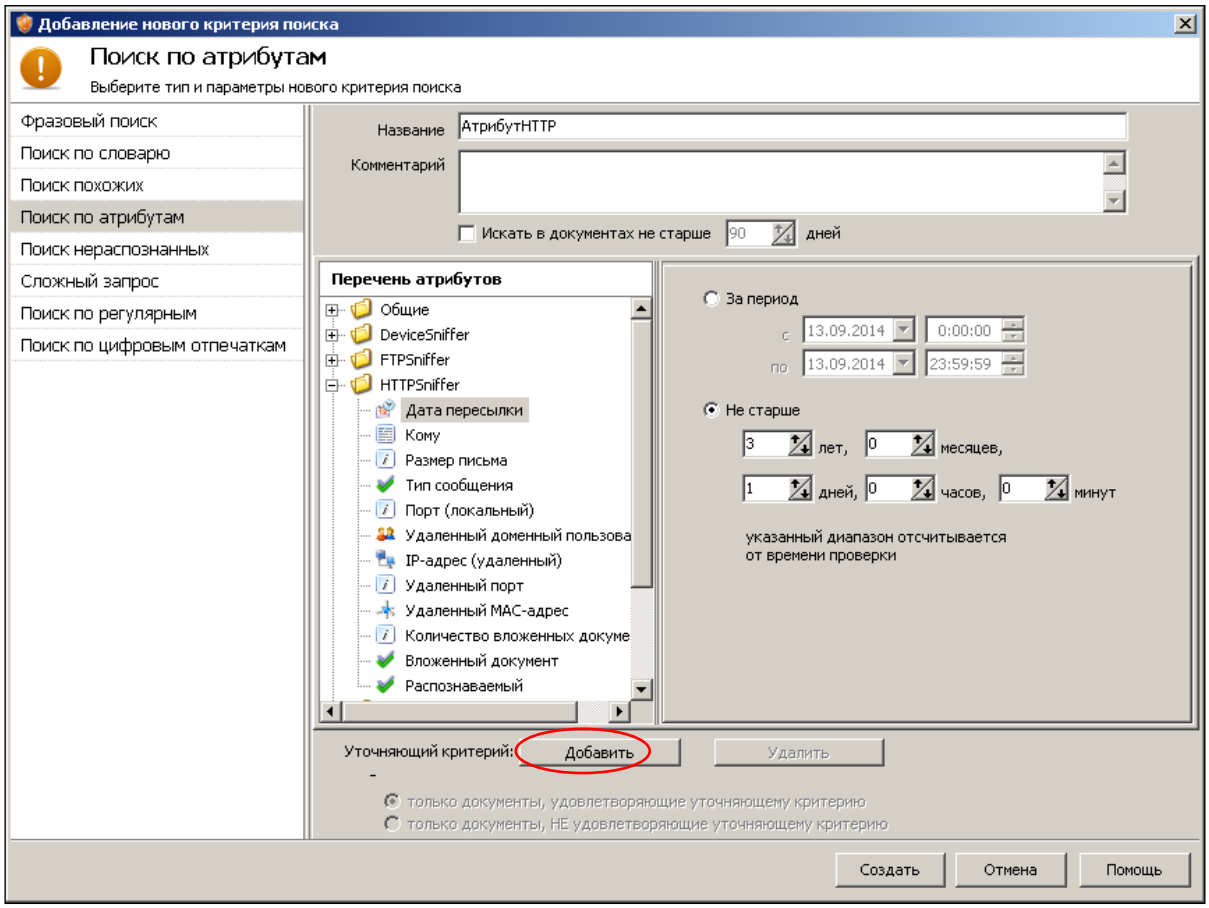

Рис. 44. Первый этап создания критерия «АтрибутHTTP»

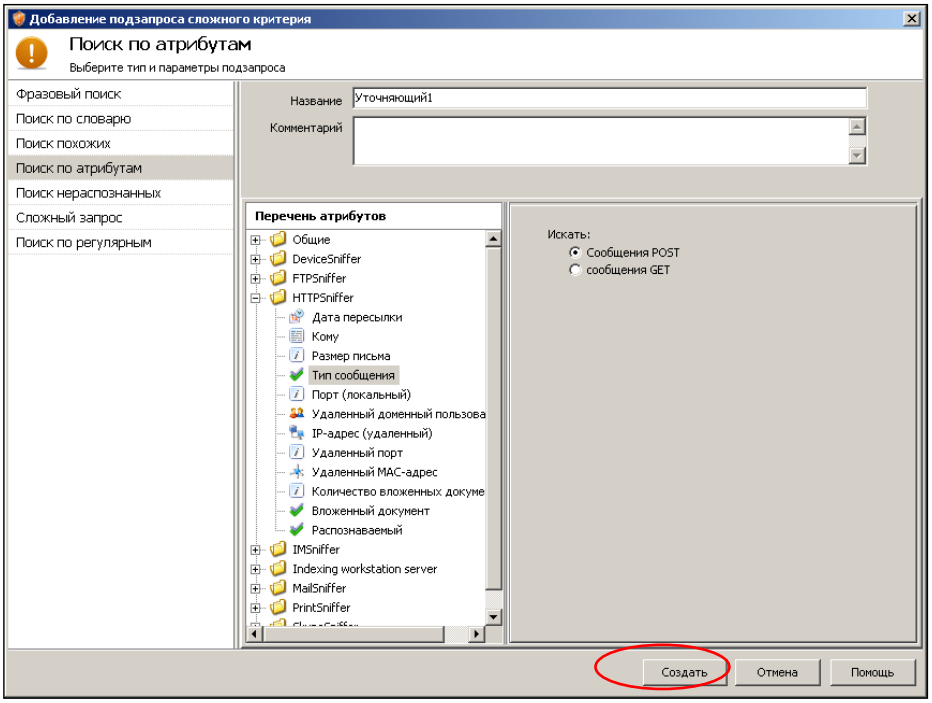

Рис. 45. Второй этап создания критерия «АтрибутHTTP» (создание уточняющего критерия «Уточняющий1»)

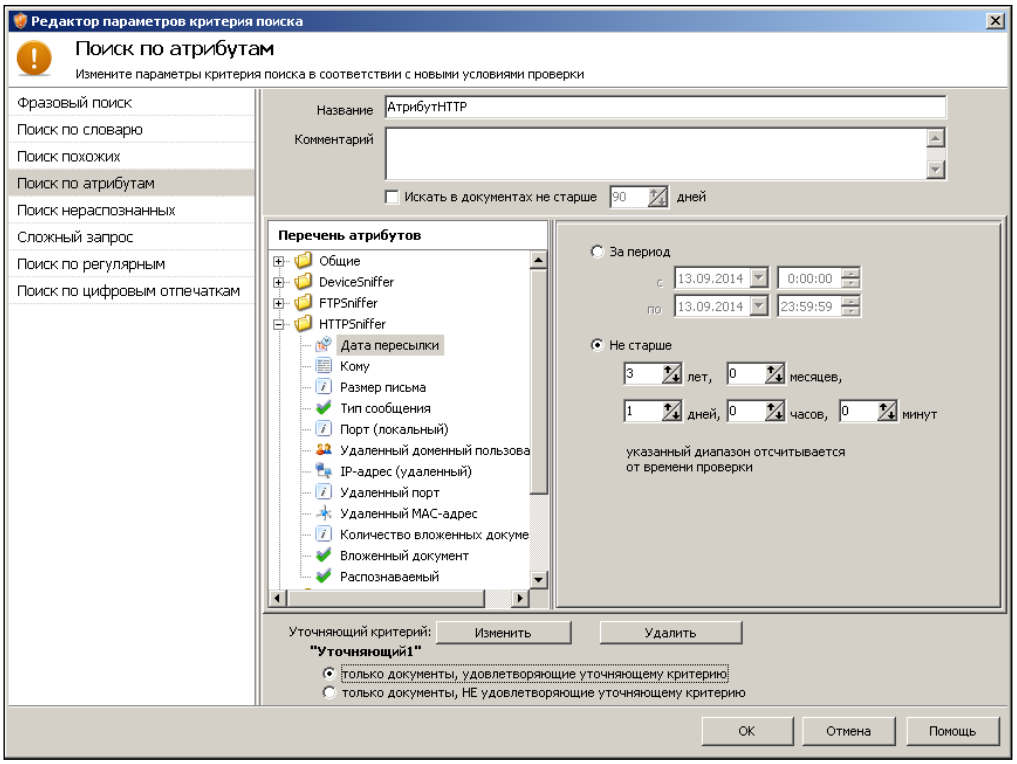

Рис. 46. Третий этап создания критерия «АтрибутHTTP»

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

– В соответствии с рис. 47-49 создать критерий для поиска файлов, переданных на съемные носители не позже чем 3 года и 1 месяц назад и имеющих размер до 2ГБ.

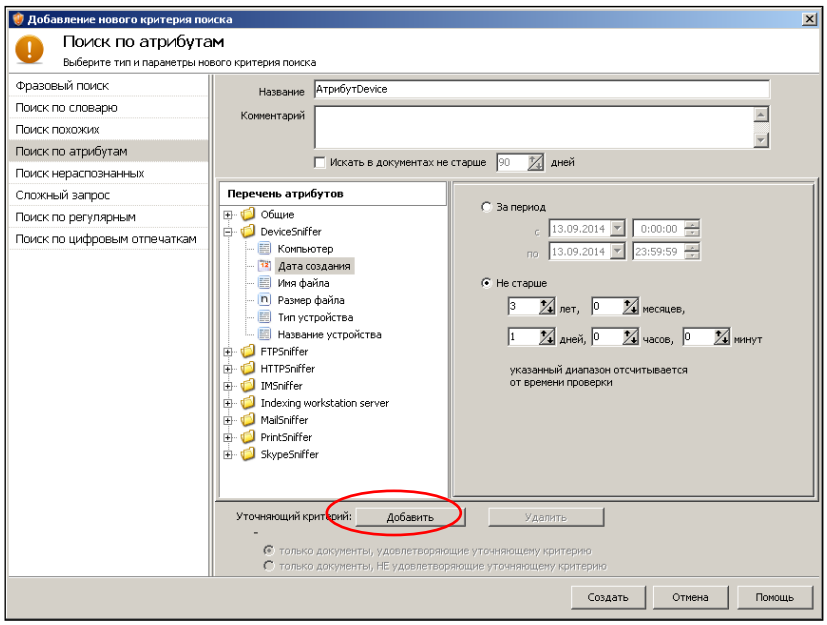

Рис. 47. Первый этап создания критерия «АтрибутDevice»

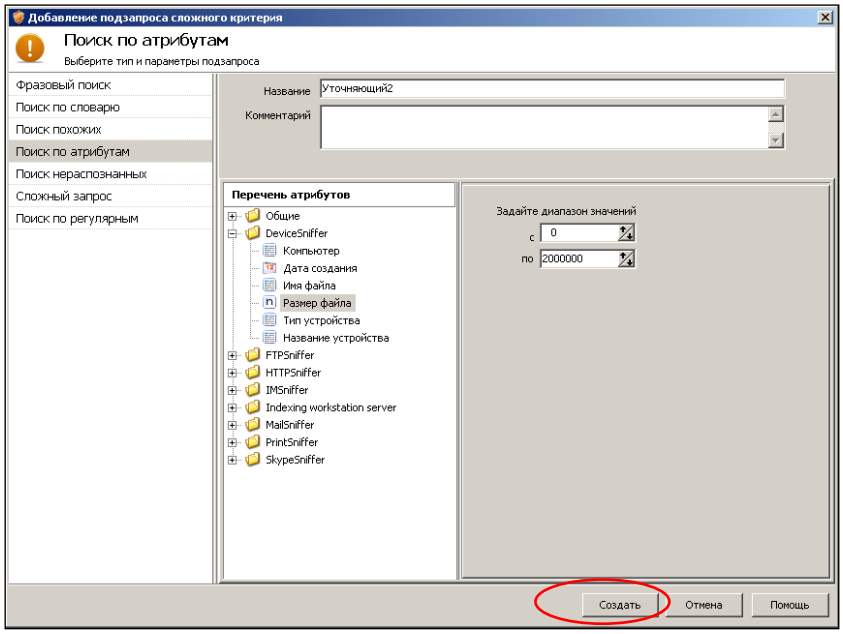

Рис. 48. Второй этап создания критерия «АтрибутDevice»

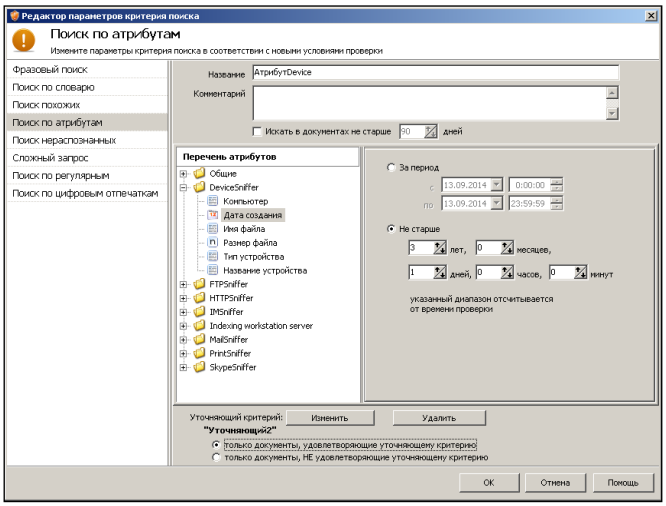

Рис. 49. Третий этап создания критерия «АтрибутDevice»

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

– В соответствии с рис. 50 создать критерий для поиска файлов, переданных на принтер, при количестве копий меньше 3.

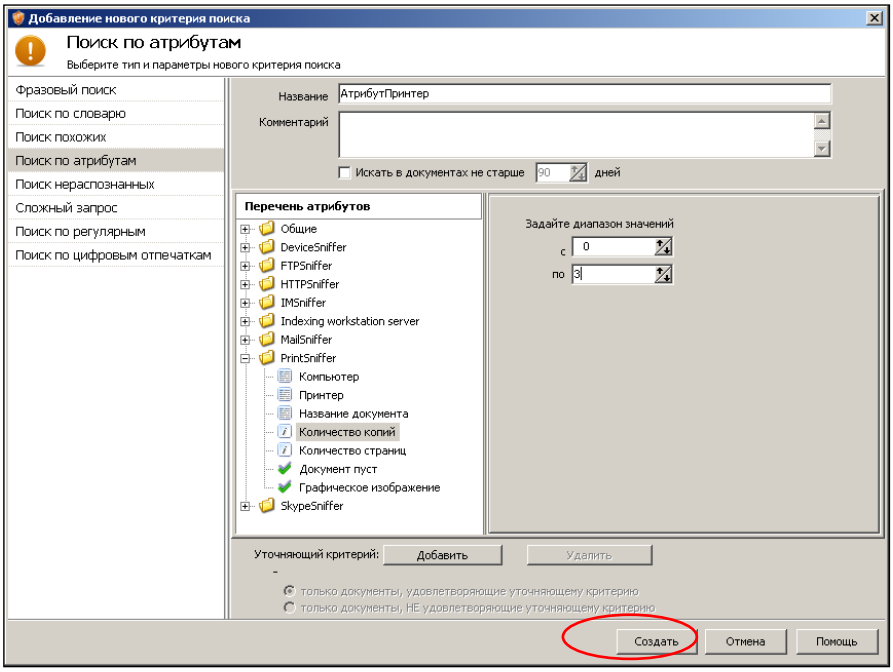

Рис. 50. Создание критерия «АтрибутПринтер»

– Запустить принудительное выполнения критерия поиска «АтрибутПринтер» и убедиться в его результативности (рис. 51). Зафиксировать время выполнения поиска.

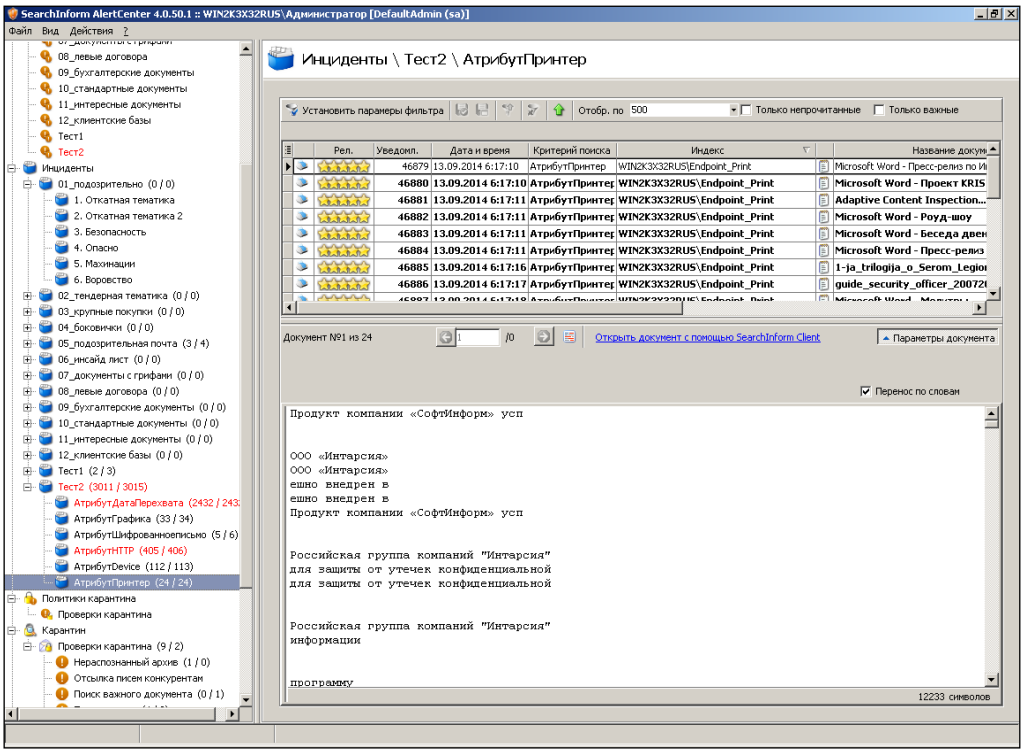

Рис. 51. Индикация инцидентов по критерию «АтрибутПринтер»

– В соответствии с рис. 52 создать критерий для поиска всех файлов, тип которых не распознан.

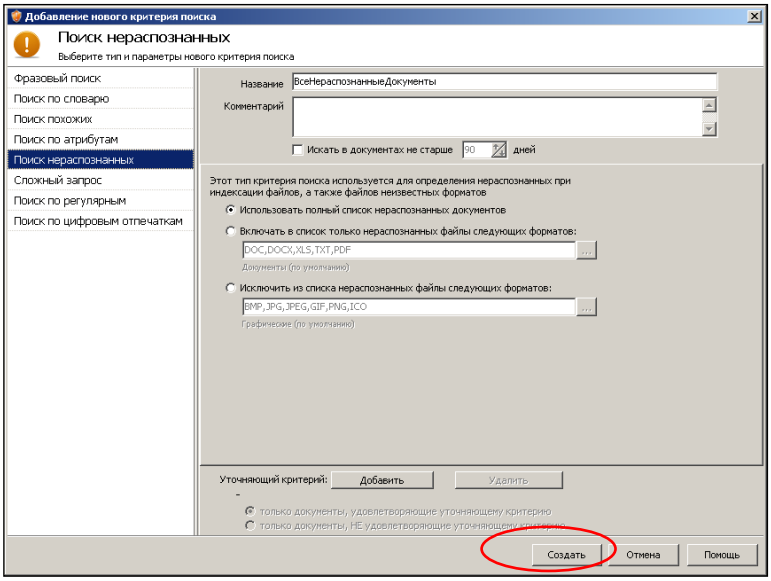

Рис. 52. Создание критерия «ВсеНераспознанныеДокументы»

– Запустить принудительное выполнения критерия поиска «ВсеНераспознанныеДокументы» и убедиться в его результативности (рис. 53). Зафиксировать время выполнения поиска.

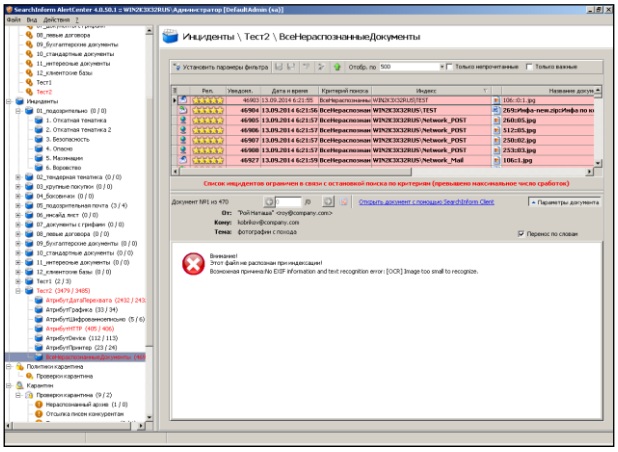

Рис. 53. Индикация инцидентов по критерию «ВсеНераспознанныеДокументы»

– В соответствии с рис. 54 создать критерий для поиска не распознанных doc-файлов.

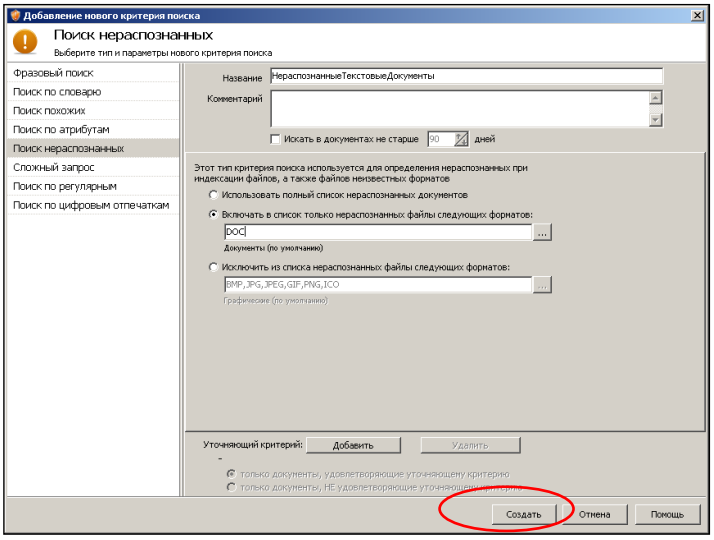

Рис. 54. Создание критерия «НераспознанныеТекстовыеДокументы»

– Запустить принудительное выполнения критерия поиска «НераспознанныеТекстовыеДокументы» и убедиться в его результативности (рис. 55). Зафиксировать время выполнения поиска.

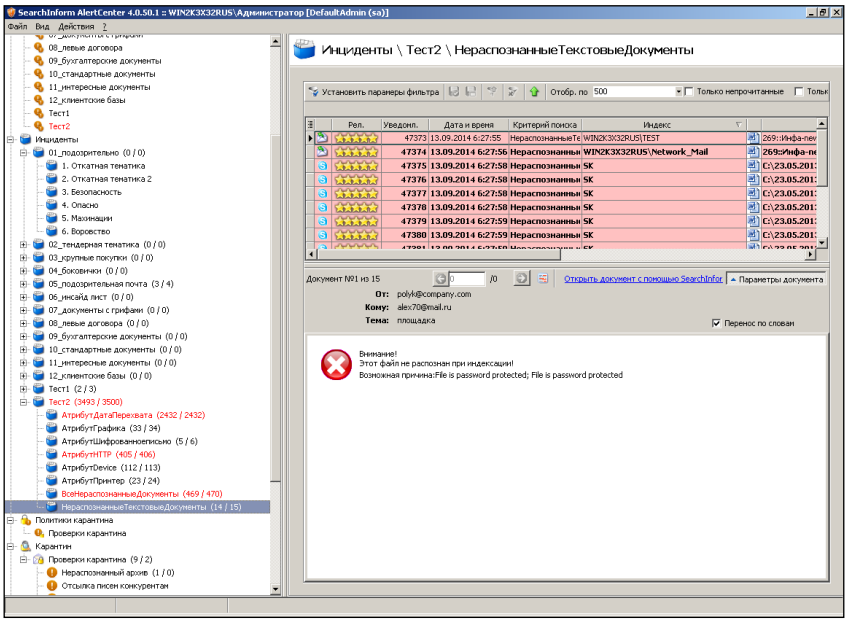

Рис. 55. Индикация инцидентов по критерию «НераспознанныеТекстовыеДокументы»

– В соответствии с рис. 56 создать критерий для поиска не распознанных файлов, исключив при этом файлы в форматах bmp, pdf и doc.

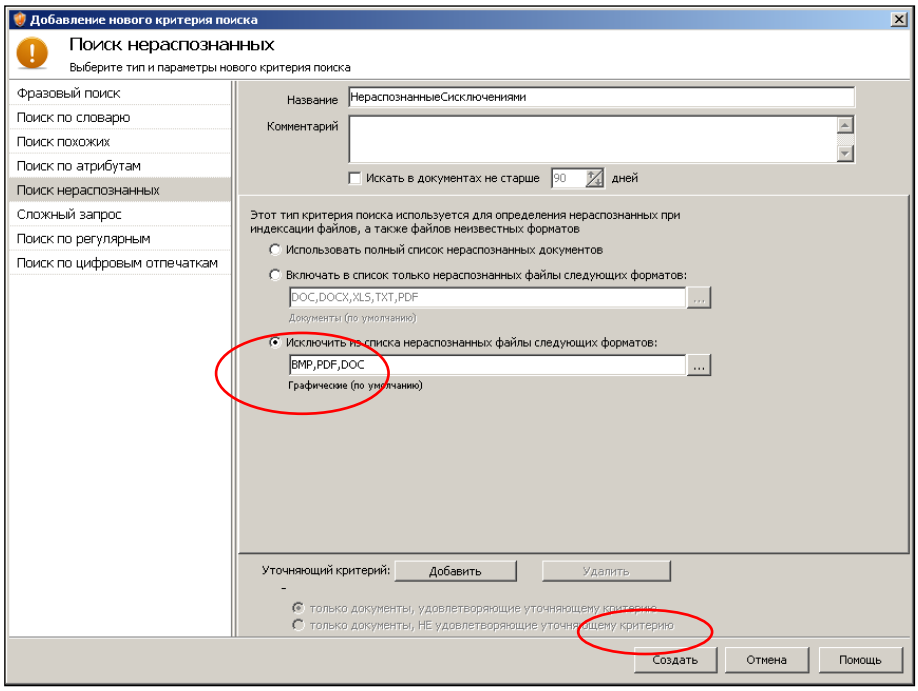

Рис. 56. Создание критерия «НераспознанныеСисключениями»

– Запустить принудительное выполнения критерия поиска «НераспознанныеСисключениями» и убедиться в его результативности (рис. 57). Зафиксировать время выполнения поиска.

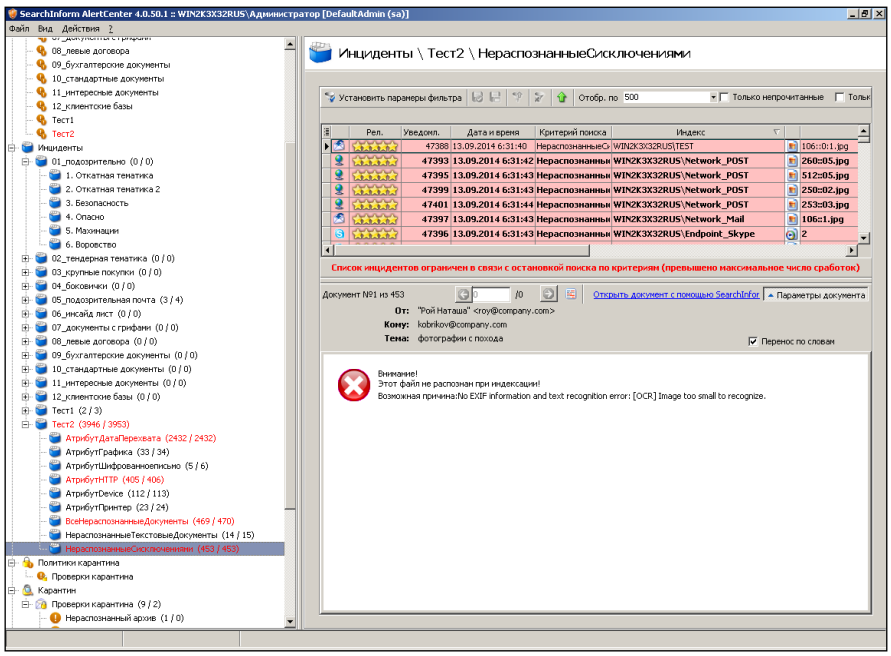

Рис. 57. Индикация инцидентов по критерию «НераспознанныеСисключениями»

– В соответствии с рис. 58-59 отфильтровать инциденты по критерию «НераспознанныеСисключениями», оставив файлы, переданные на съемные носители.

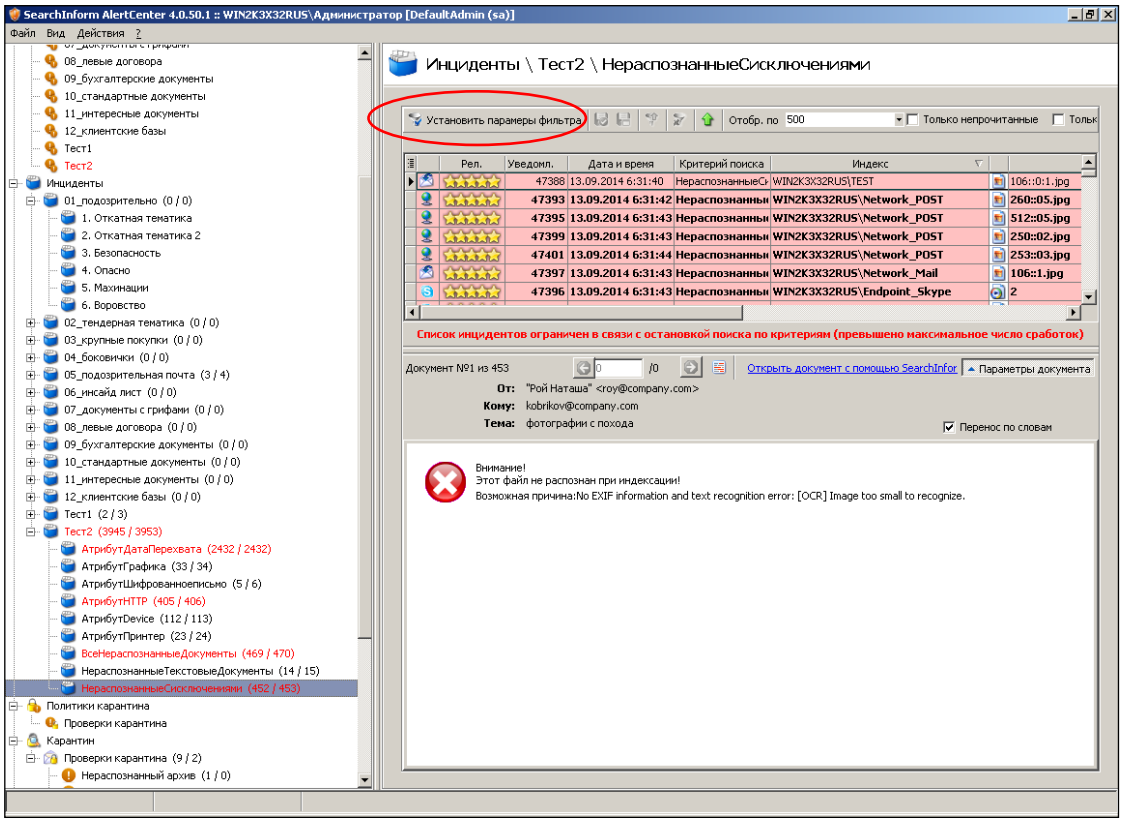

Рис. 58. Первый этап созндания фильтра

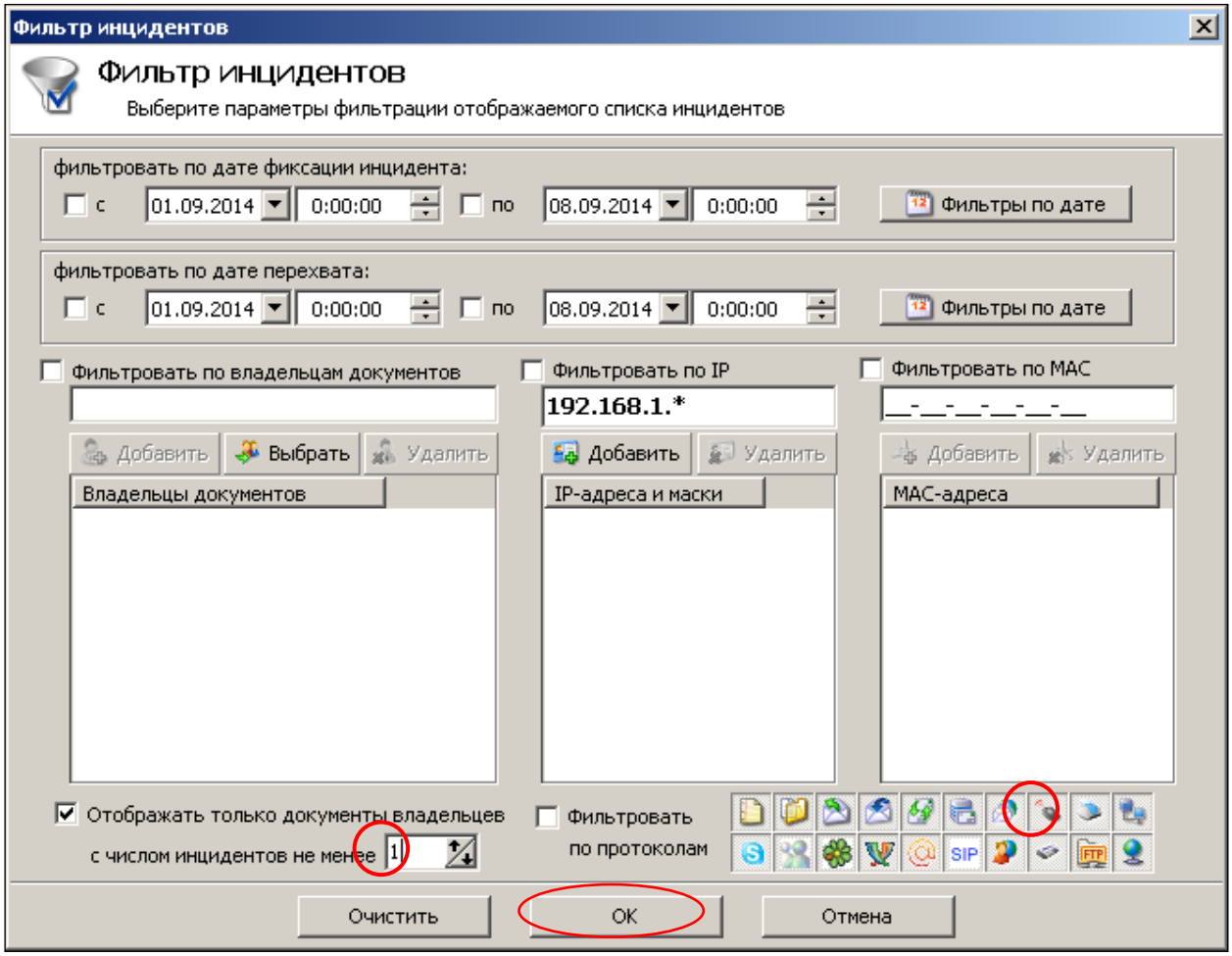

Рис. 59. Второй этап созндания фильтра

– Результат применения фильтра показан на рис. 60.

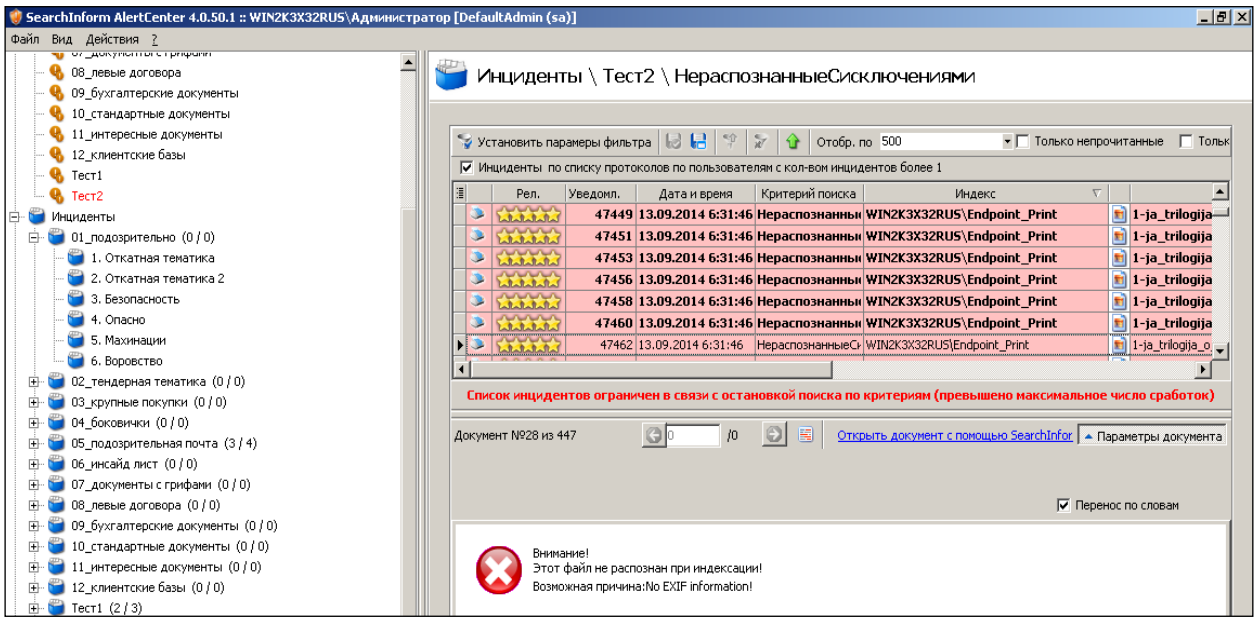

Рис. 60. Результат фильтрации

– Определить запрос с максимальным/минимальным временем выполнения.

– Закрыть окно AlertCenter Client.

– Завершить работу с виртуальным компьютером.

Задание для самостоятельной работы

- 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.

- Произвести поиск информации переданных по электронной почте по адресу voyagerur2@mail.ru.

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

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. Как изменить качество снимков экрана?
7. Какое назначение опции LiveView агента MonitorSniffer?
8. Можно ли с помощью программного комплекса SearchInform произвести поиск данных, переданных по протоколу http, базируясь на IP-адресе получателя?
9. Можно ли с помощью программного комплекса SearchInform отсортировать данные, переданные на flash-носитель от данных переданных на компакт диск?
10. Можно ли с помощью программного комплекса SearchInform произвести поиск данных, переданных с помощью чата Skype?
11. Можно ли с помощью программного комплекса SearchInform произвести поиск данных, переданных по протоколу ftp, базируясь на направлении передачи?
12. Можно ли с помощью программного комплекса SearchInform произвести поиск данных, переданных по протоколу http, базируясь на направлении передачи?
13. Зачем нужны уточняющие критерии?
14. Сколько уточняющих критериев можно использовать в одном запросе?